API Reference

AWS Network Firewall

API Version 2020-11-12

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Network Firewall: API Reference

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Welcome **1**
Actions **3**
AcceptNetworkFirewallTransitGatewayAttachment 6
Request Syntax 6
Request Parameters 6
Response Syntax 7
Response Elements 7
Errors 8
See Also 8
AssociateAvailabilityZones 10
Request Syntax 10
Request Parameters 10
Response Syntax 12
Response Elements 12
Errors 13
See Also 14
AssociateFirewallPolicy 16
Request Syntax 16
Request Parameters 16
Response Syntax 18
Response Elements 18
Errors 19
See Also 20
AssociateSubnets 22
Request Syntax 22
Request Parameters 22
Response Syntax 24
Response Elements 24
Errors 25
See Also 26
CreateFirewall 28
Request Syntax 28
Request Parameters 29
Response Syntax 33

Response Elements ... 35
Errors ... 35
See Also ... 36
CreateFirewallPolicy ... 38
Request Syntax ... 38
Request Parameters ... 39
Response Syntax ... 41
Response Elements ... 42
Errors ... 42
See Also ... 43
CreateRuleGroup ... 45
Request Syntax ... 45
Request Parameters ... 48
Response Syntax ... 52
Response Elements ... 53
Errors ... 54
See Also ... 55
CreateTLSInspectionConfiguration ... 56
Request Syntax ... 56
Request Parameters ... 57
Response Syntax ... 59
Response Elements ... 60
Errors ... 61
See Also ... 62
CreateVpcEndpointAssociation ... 63
Request Syntax ... 63
Request Parameters ... 63
Response Syntax ... 65
Response Elements ... 65
Errors ... 66
See Also ... 67
DeleteFirewall ... 69
Request Syntax ... 69
Request Parameters ... 69
Response Syntax ... 70
Response Elements ... 72

Errors ... 73
See Also ... 74
DeleteFirewallPolicy ... 75
Request Syntax ... 75
Request Parameters ... 75
Response Syntax ... 76
Response Elements ... 76
Errors ... 77
See Also ... 78
DeleteNetworkFirewallTransitGatewayAttachment ... 79
Request Syntax ... 79
Request Parameters ... 79
Response Syntax ... 79
Response Elements ... 80
Errors ... 81
See Also ... 81
DeleteResourcePolicy ... 83
Request Syntax ... 83
Request Parameters ... 83
Response Elements ... 83
Errors ... 83
See Also ... 84
DeleteRuleGroup ... 86
Request Syntax ... 86
Request Parameters ... 86
Response Syntax ... 87
Response Elements ... 88
Errors ... 88
See Also ... 89
DeleteTLSInspectionConfiguration ... 91
Request Syntax ... 91
Request Parameters ... 91
Response Syntax ... 92
Response Elements ... 92
Errors ... 93
See Also ... 94

DeleteVpcEndpointAssociation ... 95
Request Syntax ... 95
Request Parameters ... 95
Response Syntax ... 95
Response Elements ... 96
Errors ... 97
See Also ... 98
DescribeFirewall ... 99
Request Syntax ... 99
Request Parameters ... 99
Response Syntax ... 100
Response Elements ... 101
Errors ... 103
See Also ... 103
DescribeFirewallMetadata ... 105
Request Syntax ... 105
Request Parameters ... 105
Response Syntax ... 105
Response Elements ... 106
Errors ... 107
See Also ... 108
DescribeFirewallPolicy ... 109
Request Syntax ... 109
Request Parameters ... 109
Response Syntax ... 110
Response Elements ... 111
Errors ... 112
See Also ... 113
DescribeFlowOperation ... 114
Request Syntax ... 114
Request Parameters ... 114
Response Syntax ... 115
Response Elements ... 116
Errors ... 118
See Also ... 119
DescribeLoggingConfiguration ... 120

Request Syntax ... 120
Request Parameters ... 120
Response Syntax ... 121
Response Elements ... 121
Errors ... 122
See Also ... 123
DescribeResourcePolicy ... 124
Request Syntax ... 124
Request Parameters ... 124
Response Syntax ... 124
Response Elements ... 124
Errors ... 125
See Also ... 126
DescribeRuleGroup ... 127
Request Syntax ... 127
Request Parameters ... 127
Response Syntax ... 128
Response Elements ... 132
Errors ... 133
See Also ... 134
DescribeRuleGroupMetadata ... 135
Request Syntax ... 135
Request Parameters ... 135
Response Syntax ... 136
Response Elements ... 136
Errors ... 138
See Also ... 139
DescribeRuleGroupSummary ... 140
Request Syntax ... 140
Request Parameters ... 140
Response Syntax ... 141
Response Elements ... 141
Errors ... 142
See Also ... 143
DescribeTLSInspectionConfiguration ... 145
Request Syntax ... 145

Request Parameters 145
Response Syntax 146
Response Elements 147
Errors 149
See Also 149
DescribeVpcEndpointAssociation 151
Request Syntax 151
Request Parameters 151
Response Syntax 151
Response Elements 152
Errors 153
See Also 153
DisassociateAvailabilityZones 155
Request Syntax 155
Request Parameters 155
Response Syntax 157
Response Elements 157
Errors 158
See Also 159
DisassociateSubnets 161
Request Syntax 161
Request Parameters 161
Response Syntax 162
Response Elements 163
Errors 164
See Also 165
GetAnalysisReportResults 166
Request Syntax 166
Request Parameters 166
Response Syntax 168
Response Elements 168
Errors 169
See Also 170
ListAnalysisReports 172
Request Syntax 172
Request Parameters 172

Response Syntax 173
Response Elements 174
Errors 174
See Also 175
ListFirewallPolicies 176
Request Syntax 176
Request Parameters 176
Response Syntax 177
Response Elements 177
Errors 178
See Also 178
ListFirewalls 180
Request Syntax 180
Request Parameters 180
Response Syntax 181
Response Elements 181
Errors 182
See Also 183
ListFlowOperationResults 184
Request Syntax 184
Request Parameters 184
Response Syntax 186
Response Elements 187
Errors 189
See Also 190
ListFlowOperations 191
Request Syntax 191
Request Parameters 191
Response Syntax 193
Response Elements 193
Errors 194
See Also 195
ListRuleGroups 196
Request Syntax 196
Request Parameters 196
Response Syntax 197

Response Elements 198
Errors 198
See Also 199
ListTagsForResource 200
Request Syntax 200
Request Parameters 200
Response Syntax 201
Response Elements 201
Errors 202
See Also 203
ListTLSInspectionConfigurations 204
Request Syntax 204
Request Parameters 204
Response Syntax 205
Response Elements 205
Errors 206
See Also 206
ListVpcEndpointAssociations 208
Request Syntax 208
Request Parameters 208
Response Syntax 209
Response Elements 209
Errors 210
See Also 211
PutResourcePolicy 212
Request Syntax 212
Request Parameters 212
Response Elements 214
Errors 214
See Also 215
RejectNetworkFirewallTransitGatewayAttachment 216
Request Syntax 216
Request Parameters 216
Response Syntax 217
Response Elements 217
Errors 218

See Also ... 219
StartAnalysisReport ... 220
Request Syntax ... 220
Request Parameters ... 220
Response Syntax ... 221
Response Elements ... 221
Errors ... 221
See Also ... 222
StartFlowCapture ... 224
Request Syntax ... 224
Request Parameters ... 225
Response Syntax ... 226
Response Elements ... 227
Errors ... 227
See Also ... 228
StartFlowFlush ... 230
Request Syntax ... 230
Request Parameters ... 230
Response Syntax ... 232
Response Elements ... 232
Errors ... 233
See Also ... 234
TagResource ... 235
Request Syntax ... 235
Request Parameters ... 235
Response Elements ... 236
Errors ... 236
See Also ... 237
UntagResource ... 238
Request Syntax ... 238
Request Parameters ... 238
Response Elements ... 239
Errors ... 239
See Also ... 240
UpdateAvailabilityZoneChangeProtection ... 241
Request Syntax ... 241

Request Parameters 241
Response Syntax 243
Response Elements 243
Errors 244
See Also 245
UpdateFirewallAnalysisSettings 247
Request Syntax 247
Request Parameters 247
Response Syntax 248
Response Elements 249
Errors 250
See Also 251
UpdateFirewallDeleteProtection 252
Request Syntax 252
Request Parameters 252
Response Syntax 253
Response Elements 254
Errors 255
See Also 256
UpdateFirewallDescription 257
Request Syntax 257
Request Parameters 257
Response Syntax 258
Response Elements 259
Errors 260
See Also 261
UpdateFirewallEncryptionConfiguration 262
Request Syntax 262
Request Parameters 262
Response Syntax 263
Response Elements 264
Errors 265
See Also 266
UpdateFirewallPolicy 268
Request Syntax 268
Request Parameters 269

Response Syntax ... 271
Response Elements ... 272
Errors ... 273
See Also ... 274
UpdateFirewallPolicyChangeProtection ... 275
Request Syntax ... 275
Request Parameters ... 275
Response Syntax ... 276
Response Elements ... 277
Errors ... 278
See Also ... 279
UpdateLoggingConfiguration ... 280
Request Syntax ... 280
Request Parameters ... 281
Response Syntax ... 282
Response Elements ... 282
Errors ... 283
See Also ... 284
UpdateRuleGroup ... 286
Request Syntax ... 286
Request Parameters ... 289
Response Syntax ... 293
Response Elements ... 294
Errors ... 294
See Also ... 295
UpdateSubnetChangeProtection ... 297
Request Syntax ... 297
Request Parameters ... 297
Response Syntax ... 298
Response Elements ... 299
Errors ... 300
See Also ... 301
UpdateTLSInspectionConfiguration ... 302
Request Syntax ... 302
Request Parameters ... 303
Response Syntax ... 305

Response Elements 306
Errors 307
See Also 308
Data Types 309
ActionDefinition 312
Contents 312
See Also 312
Address 313
Contents 313
See Also 313
AnalysisReport 315
Contents 315
See Also 316
AnalysisResult 317
Contents 317
See Also 318
AnalysisTypeReportResult 319
Contents 319
See Also 320
Attachment 321
Contents 321
See Also 322
AvailabilityZoneMapping 323
Contents 323
See Also 323
AvailabilityZoneMetadata 324
Contents 324
See Also 324
AZSyncState 325
Contents 325
See Also 325
CapacityUsageSummary 326
Contents 326
See Also 326
CheckCertificateRevocationStatusActions 327
Contents 327

See Also 328
CIDRSummary 329
Contents 329
See Also 329
CustomAction 331
Contents 331
See Also 332
Dimension 333
Contents 333
See Also 333
EncryptionConfiguration 334
Contents 334
See Also 334
Firewall 336
Contents 336
See Also 341
FirewallMetadata 342
Contents 342
See Also 343
FirewallPolicy 344
Contents 344
See Also 346
FirewallPolicyMetadata 348
Contents 348
See Also 348
FirewallPolicyResponse 350
Contents 350
See Also 352
FirewallStatus 353
Contents 353
See Also 354
Flow 356
Contents 356
See Also 358
FlowFilter 359
Contents 359

See Also ... 360
FlowOperation ... 361
Contents ... 361
See Also ... 361
FlowOperationMetadata ... 363
Contents ... 363
See Also ... 364
FlowTimeouts ... 365
Contents ... 365
See Also ... 365
Header ... 366
Contents ... 366
See Also ... 368
Hits ... 370
Contents ... 370
See Also ... 370
IPSet ... 371
Contents ... 371
See Also ... 371
IPSetMetadata ... 372
Contents ... 372
See Also ... 372
IPSetReference ... 373
Contents ... 373
See Also ... 373
LogDestinationConfig ... 374
Contents ... 374
See Also ... 375
LoggingConfiguration ... 377
Contents ... 377
See Also ... 377
MatchAttributes ... 378
Contents ... 378
See Also ... 379
PerObjectStatus ... 380
Contents ... 380

See Also 380
PolicyVariables 382
Contents 382
See Also 382
PortRange 383
Contents 383
See Also 383
PortSet 384
Contents 384
See Also 384
PublishMetricAction 385
Contents 385
See Also 385
ReferenceSets 386
Contents 386
See Also 386
RuleDefinition 387
Contents 387
See Also 388
RuleGroup 389
Contents 389
See Also 390
RuleGroupMetadata 391
Contents 391
See Also 391
RuleGroupResponse 392
Contents 392
See Also 396
RuleOption 397
Contents 397
See Also 397
RulesSource 399
Contents 399
See Also 400
RulesSourceList 401
Contents 401

See Also 402
RuleSummary 403
Contents 403
See Also 403
RuleVariables 405
Contents 405
See Also 405
ServerCertificate 406
Contents 406
See Also 406
ServerCertificateConfiguration 407
Contents 407
See Also 408
ServerCertificateScope 409
Contents 409
See Also 410
SourceMetadata 411
Contents 411
See Also 411
StatefulEngineOptions 413
Contents 413
See Also 414
StatefulRule 415
Contents 415
See Also 416
StatefulRuleGroupOverride 417
Contents 417
See Also 417
StatefulRuleGroupReference 418
Contents 418
See Also 419
StatefulRuleOptions 420
Contents 420
See Also 420
StatelessRule 421
Contents 421

See Also ... 421
StatelessRuleGroupReference ... 423
Contents ... 423
See Also ... 423
StatelessRulesAndCustomActions ... 424
Contents ... 424
See Also ... 424
SubnetMapping ... 425
Contents ... 425
See Also ... 425
Summary ... 426
Contents ... 426
See Also ... 426
SummaryConfiguration ... 427
Contents ... 427
See Also ... 427
SyncState ... 428
Contents ... 428
See Also ... 429
Tag ... 430
Contents ... 430
See Also ... 430
TCPFlagField ... 432
Contents ... 432
See Also ... 432
TlsCertificateData ... 434
Contents ... 434
See Also ... 435
TLSInspectionConfiguration ... 436
Contents ... 436
See Also ... 436
TLSInspectionConfigurationMetadata ... 437
Contents ... 437
See Also ... 437
TLSInspectionConfigurationResponse ... 439
Contents ... 439

See Also 441
TransitGatewayAttachmentSyncState 442
Contents 442
See Also 443
UniqueSources 444
Contents 444
See Also 444
VpcEndpointAssociation 445
Contents 446
See Also 447
VpcEndpointAssociationMetadata 449
Contents 449
See Also 449
VpcEndpointAssociationStatus 450
Contents 450
See Also 450
Common Parameters 451
Common Errors 454

Welcome

This is the API Reference for AWS Network Firewall. This guide is for developers who need detailed information about the Network Firewall API actions, data types, and errors.

The REST API requires you to handle connection details, such as calculating signatures, handling request retries, and error handling. For general information about using the AWS REST APIs, see AWS APIs.

To view the complete list of AWS Regions where Network Firewall is available, see Service endpoints and quotas in the *AWS General Reference*.

To access Network Firewall using the IPv4 REST API endpoint: `https://network-firewall.<region>.amazonaws.com`

To access Network Firewall using the Dualstack (IPv4 and IPv6) REST API endpoint: `https://network-firewall.<region>.aws.api`

Alternatively, you can use one of the AWS SDKs to access an API that's tailored to the programming language or platform that you're using. For more information, see AWS SDKs.

For descriptions of Network Firewall features, including and step-by-step instructions on how to use them through the Network Firewall console, see the Network Firewall Developer Guide.

Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for Amazon Virtual Private Cloud (Amazon VPC). With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect. Network Firewall uses rules that are compatible with Suricata, a free, open source network analysis and threat detection engine. AWS Network Firewall supports Suricata version 7.0.3. For information about Suricata, see the Suricata website and the Suricata User Guide.

You can use Network Firewall to monitor and protect your VPC traffic in a number of ways. The following are just a few examples:

- Allow domains or IP addresses for known AWS service endpoints, such as Amazon S3, and block all other forms of traffic.
- Use custom lists of known bad domains to limit the types of domain names that your applications can access.

- Perform deep packet inspection on traffic entering or leaving your VPC.
- Use stateful protocol detection to filter protocols like HTTPS, regardless of the port used.

To enable Network Firewall for your VPCs, you perform steps in both Amazon VPC and in Network Firewall. For information about using Amazon VPC, see Amazon VPC User Guide.

To start using Network Firewall, do the following:

1. (Optional) If you don't already have a VPC that you want to protect, create it in Amazon VPC.
2. In Amazon VPC, in each Availability Zone where you want to have a firewall endpoint, create a subnet for the sole use of Network Firewall.
3. In Network Firewall, define the firewall behavior as follows:
   a. Create stateless and stateful rule groups, to define the components of the network traffic filtering behavior that you want your firewall to have.
   b. Create a firewall policy that uses your rule groups and specifies additional default traffic filtering behavior.
4. In Network Firewall, create a firewall and specify your new firewall policy and VPC subnets. Network Firewall creates a firewall endpoint in each subnet that you specify, with the behavior that's defined in the firewall policy.
5. In Amazon VPC, use ingress routing enhancements to route traffic through the new firewall endpoints.

After your firewall is established, you can add firewall endpoints for new Availability Zones by following the prior steps for the Amazon VPC setup and firewall subnet definitions. You can also add endpoints to Availability Zones that you're using in the firewall, either for the same VPC or for another VPC, by following the prior steps for the Amazon VPC setup, and defining the new VPC subnets as VPC endpoint associations.

This document was last published on September 4, 2025.

Actions

The following actions are supported:

- AcceptNetworkFirewallTransitGatewayAttachment
- AssociateAvailabilityZones
- AssociateFirewallPolicy
- AssociateSubnets
- CreateFirewall
- CreateFirewallPolicy
- CreateRuleGroup
- CreateTLSInspectionConfiguration
- CreateVpcEndpointAssociation
- DeleteFirewall
- DeleteFirewallPolicy
- DeleteNetworkFirewallTransitGatewayAttachment
- DeleteResourcePolicy
- DeleteRuleGroup
- DeleteTLSInspectionConfiguration
- DeleteVpcEndpointAssociation
- DescribeFirewall
- DescribeFirewallMetadata
- DescribeFirewallPolicy
- DescribeFlowOperation
- DescribeLoggingConfiguration
- DescribeResourcePolicy
- DescribeRuleGroup
- DescribeRuleGroupMetadata
- DescribeRuleGroupSummary
- DescribeTLSInspectionConfiguration
- DescribeVpcEndpointAssociation

- DisassociateAvailabilityZones
- DisassociateSubnets
- GetAnalysisReportResults
- ListAnalysisReports
- ListFirewallPolicies
- ListFirewalls
- ListFlowOperationResults
- ListFlowOperations
- ListRuleGroups
- ListTagsForResource
- ListTLSInspectionConfigurations
- ListVpcEndpointAssociations
- PutResourcePolicy
- RejectNetworkFirewallTransitGatewayAttachment
- StartAnalysisReport
- StartFlowCapture
- StartFlowFlush
- TagResource
- UntagResource
- UpdateAvailabilityZoneChangeProtection
- UpdateFirewallAnalysisSettings
- UpdateFirewallDeleteProtection
- UpdateFirewallDescription
- UpdateFirewallEncryptionConfiguration
- UpdateFirewallPolicy
- UpdateFirewallPolicyChangeProtection
- UpdateLoggingConfiguration
- UpdateRuleGroup
- UpdateSubnetChangeProtection
- UpdateTLSInspectionConfiguration

AcceptNetworkFirewallTransitGatewayAttachment

Accepts a transit gateway attachment request for Network Firewall. When you accept the attachment request, Network Firewall creates the necessary routing components to enable traffic flow between the transit gateway and firewall endpoints.

You must accept a transit gateway attachment to complete the creation of a transit gateway-attached firewall, unless auto-accept is enabled on the transit gateway. After acceptance, use DescribeFirewall to verify the firewall status.

To reject an attachment instead of accepting it, use RejectNetworkFirewallTransitGatewayAttachment.

> **Note**
>
> It can take several minutes for the attachment acceptance to complete and the firewall to become available.

Request Syntax

```
{
   "TransitGatewayAttachmentId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

TransitGatewayAttachmentId

Required. The unique identifier of the transit gateway attachment to accept. This ID is returned in the response when creating a transit gateway-attached firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

Required: Yes

Response Syntax

```
{
   "TransitGatewayAttachmentId": "string",
   "TransitGatewayAttachmentStatus": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TransitGatewayAttachmentId

The unique identifier of the transit gateway attachment that was accepted.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

TransitGatewayAttachmentStatus

The current status of the transit gateway attachment. Valid values are:

- `CREATING` - The attachment is being created
- `DELETING` - The attachment is being deleted
- `DELETED` - The attachment has been deleted
- `FAILED` - The attachment creation has failed and cannot be recovered
- `ERROR` - The attachment is in an error state that might be recoverable
- `READY` - The attachment is active and processing traffic
- `PENDING_ACCEPTANCE` - The attachment is waiting to be accepted
- `REJECTING` - The attachment is in the process of being rejected
- `REJECTED` - The attachment has been rejected

Type: String

Valid Values: `CREATING | DELETING | DELETED | FAILED | ERROR | READY | PENDING_ACCEPTANCE | REJECTING | REJECTED`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AssociateAvailabilityZones

Associates the specified Availability Zones with a transit gateway-attached firewall. For each Availability Zone, Network Firewall creates a firewall endpoint to process traffic. You can specify one or more Availability Zones where you want to deploy the firewall.

After adding Availability Zones, you must update your transit gateway route tables to direct traffic through the new firewall endpoints. Use DescribeFirewall to monitor the status of the new endpoints.

Request Syntax

```
{
   "AvailabilityZoneMappings": [
      {
         "AvailabilityZone": "string"
      }
   ],
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZoneMappings

Required. The Availability Zones where you want to create firewall endpoints. You must specify at least one Availability Zone.

Type: Array of AvailabilityZoneMapping objects

Required: Yes

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "AvailabilityZoneMappings": [
      {
         "AvailabilityZone": "string"
      }
   ],
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AvailabilityZoneMappings

The Availability Zones where Network Firewall created firewall endpoints. Each mapping specifies an Availability Zone where the firewall processes traffic.

Type: Array of AvailabilityZoneMapping objects

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AssociateFirewallPolicy

Associates a FirewallPolicy to a Firewall.

A firewall policy defines how to monitor and manage your VPC network traffic, using a collection of inspection rule groups and other settings. Each firewall requires one firewall policy association, and you can use the same firewall policy for multiple firewalls.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyArn": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyArn": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

AssociateSubnets

Associates the specified subnets in the Amazon VPC to the firewall. You can specify one subnet for each of the Availability Zones that the VPC spans.

This request creates an AWS Network Firewall firewall endpoint in each of the subnets. To enable the firewall's protections, you must also modify the VPC's route tables for each subnet's Availability Zone, to redirect the traffic that's coming into and going out of the zone through the firewall endpoint.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetMappings": [
      {
         "IPAddressType": "string",
         "SubnetId": "string"
      }
   ],
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

SubnetMappings

The IDs of the subnets that you want to associate with the firewall.

Type: Array of SubnetMapping objects

Required: Yes

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetMappings": [
      {
         "IPAddressType": "string",
         "SubnetId": "string"
      }
   ],
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

SubnetMappings

The IDs of the subnets that are associated with the firewall.

Type: Array of SubnetMapping objects

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateFirewall

Creates an AWS Network Firewall Firewall and accompanying FirewallStatus for a VPC.

The firewall defines the configuration settings for an AWS Network Firewall firewall. The settings that you can define at creation include the firewall policy, the subnets in your VPC to use for the firewall endpoints, and any tags that are attached to the firewall AWS resource.

After you create a firewall, you can provide additional settings, like the logging configuration.

To update the settings for a firewall, you use the operations that apply to the settings themselves, for example UpdateLoggingConfiguration, AssociateSubnets, and UpdateFirewallDeleteProtection.

To manage a firewall's tags, use the standard AWS resource tagging operations, ListTagsForResource, TagResource, and UntagResource.

To retrieve information about firewalls, use ListFirewalls and DescribeFirewall.

To generate a report on the last 30 days of traffic monitored by a firewall, use StartAnalysisReport.

Request Syntax

```
{
   "AvailabilityZoneChangeProtection": boolean,
   "AvailabilityZoneMappings": [
      {
         "AvailabilityZone": "string"
      }
   ],
   "DeleteProtection": boolean,
   "Description": "string",
   "EnabledAnalysisTypes": [ "string" ],
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "FirewallName": "string",
   "FirewallPolicyArn": "string",
   "FirewallPolicyChangeProtection": boolean,
   "SubnetChangeProtection": boolean,
   "SubnetMappings": [
      {
```

```
            "IPAddressType": "string",
            "SubnetId": "string"
        }
    ],
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ],
    "TransitGatewayId": "string",
    "VpcId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZoneChangeProtection

Optional. A setting indicating whether the firewall is protected against changes to its Availability Zone configuration. When set to TRUE, you cannot add or remove Availability Zones without first disabling this protection using UpdateAvailabilityZoneChangeProtection.

Default value: FALSE

Type: Boolean

Required: No

AvailabilityZoneMappings

Required. The Availability Zones where you want to create firewall endpoints for a transit gateway-attached firewall. You must specify at least one Availability Zone. Consider enabling the firewall in every Availability Zone where you have workloads to maintain Availability Zone isolation.

You can modify Availability Zones later using AssociateAvailabilityZones or DisassociateAvailabilityZones, but this may briefly disrupt traffic. The `AvailabilityZoneChangeProtection` setting controls whether you can make these modifications.

Type: Array of AvailabilityZoneMapping objects

Required: No

DeleteProtection

A flag indicating whether it is possible to delete the firewall. A setting of `TRUE` indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to `TRUE`.

Type: Boolean

Required: No

Description

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EnabledAnalysisTypes

An optional setting indicating the specific traffic analysis types to enable on the firewall.

Type: Array of strings

Valid Values: `TLS_SNI | HTTP_HOST`

Required: No

EncryptionConfiguration

A complex type that contains settings for encryption of your firewall resources.

Type: EncryptionConfiguration object

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

FirewallPolicyArn

The Amazon Resource Name (ARN) of the FirewallPolicy that you want to use for the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FirewallPolicyChangeProtection

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

Required: No

SubnetChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

Required: No

SubnetMappings

The public subnets to use for your Network Firewall firewalls. Each subnet must belong to a different Availability Zone in the VPC. Network Firewall creates a firewall endpoint in each subnet.

Type: Array of SubnetMapping objects

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

TransitGatewayId

Required when creating a transit gateway-attached firewall. The unique identifier of the transit gateway to attach to this firewall. You can provide either a transit gateway from your account or one that has been shared with you through AWS Resource Access Manager.

> **Important**
>
> After creating the firewall, you cannot change the transit gateway association. To use a different transit gateway, you must create a new firewall.

For information about creating firewalls, see CreateFirewall. For specific guidance about transit gateway-attached firewalls, see Considerations for transit gateway-attached firewalls in the *AWS Network Firewall Developer Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-[0-9a-z]+$`

Required: No

VpcId

The unique identifier of the VPC where Network Firewall should create the firewall.

You can't change this setting after you create the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: No

Response Syntax

```
{
   "Firewall": {
      "AvailabilityZoneChangeProtection": boolean,
      "AvailabilityZoneMappings": [
         {
            "AvailabilityZone": "string"
         }
      ],
      "DeleteProtection": boolean,
      "Description": "string",
      "EnabledAnalysisTypes": [ "string" ],
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "NumberOfAssociations": number,
      "SubnetChangeProtection": boolean,
      "SubnetMappings": [
         {
            "IPAddressType": "string",
            "SubnetId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "TransitGatewayId": "string",
```

```
        "TransitGatewayOwnerAccountId": "string",
        "VpcId": "string"
    },
    "FirewallStatus": {
        "CapacityUsageSummary": {
            "CIDRs": {
                "AvailableCIDRCount": number,
                "IPSetReferences": {
                    "string" : {
                        "ResolvedCIDRCount": number
                    }
                },
                "UtilizedCIDRCount": number
            }
        },
        "ConfigurationSyncStateSummary": "string",
        "Status": "string",
        "SyncStates": {
            "string" : {
                "Attachment": {
                    "EndpointId": "string",
                    "Status": "string",
                    "StatusMessage": "string",
                    "SubnetId": "string"
                },
                "Config": {
                    "string" : {
                        "SyncStatus": "string",
                        "UpdateToken": "string"
                    }
                }
            }
        },
        "TransitGatewayAttachmentSyncState": {
            "AttachmentId": "string",
            "StatusMessage": "string",
            "TransitGatewayAttachmentStatus": "string"
        }
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewall

The configuration settings for the firewall. These settings include the firewall policy and the subnets in your VPC to use for the firewall endpoints.

Type: Firewall object

FirewallStatus

Detailed information about the current status of a Firewall. You can retrieve this for a firewall by calling DescribeFirewall and providing the firewall name and ARN.

The firewall status indicates a combined status. It indicates whether all subnets are up-to-date with the latest firewall configurations, which is based on the sync states config values, and also whether all subnets have their endpoints fully enabled, based on their sync states attachment values.

Type: FirewallStatus object

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateFirewallPolicy

Creates the firewall policy for the firewall according to the specifications.

An AWS Network Firewall firewall policy defines the behavior of a firewall, in a collection of stateless and stateful rule groups and other settings. You can use one firewall policy for multiple firewalls.

Request Syntax

```
{
   "Description": "string",
   "DryRun": boolean,
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "FirewallPolicy": {
      "PolicyVariables": {
         "RuleVariables": {
            "string" : {
               "Definition": [ "string" ]
            }
         }
      },
      "StatefulDefaultActions": [ "string" ],
      "StatefulEngineOptions": {
         "FlowTimeouts": {
            "TcpIdleTimeoutSeconds": number
         },
         "RuleOrder": "string",
         "StreamExceptionPolicy": "string"
      },
      "StatefulRuleGroupReferences": [
         {
            "DeepThreatInspection": boolean,
            "Override": {
               "Action": "string"
            },
            "Priority": number,
            "ResourceArn": "string"
         }
      ],
```

```
        "StatelessCustomActions": [
           {
              "ActionDefinition": {
                 "PublishMetricAction": {
                    "Dimensions": [
                       {
                          "Value": "string"
                       }
                    ]
                 }
              },
              "ActionName": "string"
           }
        ],
        "StatelessDefaultActions": [ "string" ],
        "StatelessFragmentDefaultActions": [ "string" ],
        "StatelessRuleGroupReferences": [
           {
              "Priority": number,
              "ResourceArn": "string"
           }
        ],
        "TLSInspectionConfigurationArn": "string"
     },
     "FirewallPolicyName": "string",
     "Tags": [
        {
           "Key": "string",
           "Value": "string"
        }
     ]
  }
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Description

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: ^.*$

Required: No

DryRun

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to TRUE, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to FALSE, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to FALSE, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

EncryptionConfiguration

A complex type that contains settings for encryption of your firewall policy resources.

Type: EncryptionConfiguration object

Required: No

FirewallPolicy

The rule groups and policy actions to use in the firewall policy.

Type: FirewallPolicy object

Required: Yes

FirewallPolicyName

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

Response Syntax

```
{
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
      "ConsumedStatelessRuleCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string",
      "FirewallPolicyStatus": "string",
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicyResponse

The high-level properties of a firewall policy. This, along with the FirewallPolicy, define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy.

Type: FirewallPolicyResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateRuleGroup

Creates the specified stateless or stateful rule group, which includes the rules for network traffic inspection, a capacity setting, and tags.

You provide your rule group specification in your request using either `RuleGroup` or `Rules`.

Request Syntax

```
{
   "AnalyzeRuleGroup": boolean,
   "Capacity": number,
   "Description": "string",
   "DryRun": boolean,
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "RuleGroup": {
      "ReferenceSets": {
         "IPSetReferences": {
            "string" : {
               "ReferenceArn": "string"
            }
         }
      },
      "RulesSource": {
         "RulesSourceList": {
            "GeneratedRulesType": "string",
            "Targets": [ "string" ],
            "TargetTypes": [ "string" ]
         },
         "RulesString": "string",
         "StatefulRules": [
            {
               "Action": "string",
               "Header": {
                  "Destination": "string",
                  "DestinationPort": "string",
                  "Direction": "string",
                  "Protocol": "string",
                  "Source": "string",
                  "SourcePort": "string"
```

```
            },
            "RuleOptions": [
               {
                  "Keyword": "string",
                  "Settings": [ "string" ]
               }
            ]
         }
      ],
      "StatelessRulesAndCustomActions": {
         "CustomActions": [
            {
               "ActionDefinition": {
                  "PublishMetricAction": {
                     "Dimensions": [
                        {
                           "Value": "string"
                        }
                     ]
                  }
               },
               "ActionName": "string"
            }
         ],
         "StatelessRules": [
            {
               "Priority": number,
               "RuleDefinition": {
                  "Actions": [ "string" ],
                  "MatchAttributes": {
                     "DestinationPorts": [
                        {
                           "FromPort": number,
                           "ToPort": number
                        }
                     ],
                     "Destinations": [
                        {
                           "AddressDefinition": "string"
                        }
                     ],
                     "Protocols": [ number ],
                     "SourcePorts": [
                        {
```

```
                                "FromPort": number,
                                "ToPort": number
                            }
                        ],
                        "Sources": [
                            {
                                "AddressDefinition": "string"
                            }
                        ],
                        "TCPFlags": [
                            {
                                "Flags": [ "string" ],
                                "Masks": [ "string" ]
                            }
                        ]
                    }
                }
            }
        ]
    }
},
"RuleVariables": {
    "IPSets": {
        "string" : {
            "Definition": [ "string" ]
        }
    },
    "PortSets": {
        "string" : {
            "Definition": [ "string" ]
        }
    }
},
"StatefulRuleOptions": {
    "RuleOrder": "string"
}
},
"RuleGroupName": "string",
"Rules": "string",
"SourceMetadata": {
    "SourceArn": "string",
    "SourceUpdateToken": "string"
},
"SummaryConfiguration": {
```

```
        "RuleOptions": [ "string" ]
    },
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ],
    "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AnalyzeRuleGroup

Indicates whether you want Network Firewall to analyze the stateless rules in the rule group for rule behavior such as asymmetric routing. If set to TRUE, Network Firewall runs the analysis and then creates the rule group for you. To run the stateless rule group analyzer without creating the rule group, set `DryRun` to TRUE.

Type: Boolean

Required: No

Capacity

The maximum operating resources that this rule group can use. Rule group capacity is fixed at creation. When you update a rule group, you are limited to this capacity. When you reference a rule group from a firewall policy, Network Firewall reserves this capacity for the rule group.

You can retrieve the capacity that would be required for a rule group before you create the rule group by calling CreateRuleGroup with `DryRun` set to TRUE.

> **Note**
>
> You can't change or exceed this capacity when you update the rule group, so leave room for your rule group to grow.

Capacity for a stateless rule group

For a stateless rule group, the capacity required is the sum of the capacity requirements of the individual rules that you expect to have in the rule group.

To calculate the capacity requirement of a single rule, multiply the capacity requirement values of each of the rule's match settings:

- A match setting with no criteria specified has a value of 1.
- A match setting with `Any` specified has a value of 1.
- All other match settings have a value equal to the number of elements provided in the setting. For example, a protocol setting ["UDP"] and a source setting ["10.0.0.0/24"] each have a value of 1. A protocol setting ["UDP","TCP"] has a value of 2. A source setting ["10.0.0.0/24","10.0.0.1/24","10.0.0.2/24"] has a value of 3.

A rule with no criteria specified in any of its match settings has a capacity requirement of 1. A rule with protocol setting ["UDP","TCP"], source setting ["10.0.0.0/24","10.0.0.1/24","10.0.0.2/24"], and a single specification or no specification for each of the other match settings has a capacity requirement of 6.

Capacity for a stateful rule group

For a stateful rule group, the minimum capacity required is the number of individual rules that you expect to have in the rule group.

Type: Integer

Required: Yes

Description

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to TRUE, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to FALSE, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to FALSE, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

EncryptionConfiguration

A complex type that contains settings for encryption of your rule group resources.

Type: EncryptionConfiguration object

Required: No

RuleGroup

An object that defines the rule group rules.

> **Note**
>
> You must provide either this rule group setting or a Rules setting, but not both.

Type: RuleGroup object

Required: No

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: ^[a-zA-Z0-9-]+$

Required: Yes

Rules

A string containing stateful rule group rules specifications in Suricata flat format, with one rule per line. Use this to import your existing Suricata compatible rule groups.

> **Note**
>
> You must provide either this rules setting or a populated `RuleGroup` setting, but not both.

You can provide your rule group specification in Suricata flat format through this setting when you create or update your rule group. The call response returns a RuleGroup object that Network Firewall has populated from your string.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000000.

Required: No

SourceMetadata

A complex type that contains metadata about the rule group that your own rule group is copied from. You can use the metadata to keep track of updates made to the originating rule group.

Type: SourceMetadata object

Required: No

SummaryConfiguration

An object that contains a `RuleOptions` array of strings. You use `RuleOptions` to determine which of the following RuleSummary values are returned in response to `DescribeRuleGroupSummary`.

- `Metadata` - returns
- `Msg`
- `SID`

Type: SummaryConfiguration object

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: Yes

Response Syntax

```
{
   "RuleGroupResponse": {
      "AnalysisResults": [
         {
            "AnalysisDetail": "string",
            "IdentifiedRuleIds": [ "string" ],
            "IdentifiedType": "string"
         }
      ],
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
```

```
        "RuleGroupId": "string",
        "RuleGroupName": "string",
        "RuleGroupStatus": "string",
        "SnsTopic": "string",
        "SourceMetadata": {
           "SourceArn": "string",
           "SourceUpdateToken": "string"
        },
        "SummaryConfiguration": {
           "RuleOptions": [ "string" ]
        },
        "Tags": [
           {
              "Key": "string",
              "Value": "string"
           }
        ],
        "Type": "string"
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroupResponse

The high-level properties of a rule group. This, along with the RuleGroup, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Type: RuleGroupResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it

has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateTLSInspectionConfiguration

Creates an AWS Network Firewall TLS inspection configuration. Network Firewall uses TLS inspection configurations to decrypt your firewall's inbound and outbound SSL/TLS traffic. After decryption, Network Firewall inspects the traffic according to your firewall policy's stateful rules, and then re-encrypts it before sending it to its destination. You can enable inspection of your firewall's inbound traffic, outbound traffic, or both. To use TLS inspection with your firewall, you must first import or provision certificates using ACM, create a TLS inspection configuration, add that configuration to a new firewall policy, and then associate that policy with your firewall.

To update the settings for a TLS inspection configuration, use UpdateTLSInspectionConfiguration.

To manage a TLS inspection configuration's tags, use the standard AWS resource tagging operations, ListTagsForResource, TagResource, and UntagResource.

To retrieve information about TLS inspection configurations, use ListTLSInspectionConfigurations and DescribeTLSInspectionConfiguration.

For more information about TLS inspection configurations, see Inspecting SSL/TLS traffic with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

Request Syntax

```
{
   "Description": "string",
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "TLSInspectionConfiguration": {
      "ServerCertificateConfigurations": [
         {
            "CertificateAuthorityArn": "string",
            "CheckCertificateRevocationStatus": {
               "RevokedStatusAction": "string",
```

```
                "UnknownStatusAction": "string"
            },
            "Scopes": [
                {
                    "DestinationPorts": [
                        {
                            "FromPort": number,
                            "ToPort": number
                        }
                    ],
                    "Destinations": [
                        {
                            "AddressDefinition": "string"
                        }
                    ],
                    "Protocols": [ number ],
                    "SourcePorts": [
                        {
                            "FromPort": number,
                            "ToPort": number
                        }
                    ],
                    "Sources": [
                        {
                            "AddressDefinition": "string"
                        }
                    ]
                }
            ],
            "ServerCertificates": [
                {
                    "ResourceArn": "string"
                }
            ]
        }
    ]
  },
  "TLSInspectionConfigurationName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Description

A description of the TLS inspection configuration.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EncryptionConfiguration

A complex type that contains optional AWS Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an AWS owned key that AWS owns and manages for you. You can use either the AWS owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see Encryption at rest with AWS Key Managment Service in the *Network Firewall Developer Guide*.

Type: EncryptionConfiguration object

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

TLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with TLSInspectionConfigurationResponse, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

AWS Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see Inspecting SSL/TLS traffic with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

Type: TLSInspectionConfiguration object

Required: Yes

TLSInspectionConfigurationName

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

Response Syntax

```
{
   "TLSInspectionConfigurationResponse": {
      "CertificateAuthority": {
         "CertificateArn": "string",
         "CertificateSerial": "string",
         "Status": "string",
         "StatusMessage": "string"
      },
      "Certificates": [
         {
            "CertificateArn": "string",
            "CertificateSerial": "string",
            "Status": "string",
            "StatusMessage": "string"
         }
      ],
```

```
        "Description": "string",
        "EncryptionConfiguration": {
           "KeyId": "string",
           "Type": "string"
        },
        "LastModifiedTime": number,
        "NumberOfAssociations": number,
        "Tags": [
           {
              "Key": "string",
              "Value": "string"
           }
        ],
        "TLSInspectionConfigurationArn": "string",
        "TLSInspectionConfigurationId": "string",
        "TLSInspectionConfigurationName": "string",
        "TLSInspectionConfigurationStatus": "string"
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the TLSInspectionConfiguration, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

Type: TLSInspectionConfigurationResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the TLS inspection configuration. The token marks the state of the TLS inspection configuration resource at the time of the request.

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration

hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateVpcEndpointAssociation

Creates a firewall endpoint for an AWS Network Firewall firewall. This type of firewall endpoint is independent of the firewall endpoints that you specify in the `Firewall` itself, and you define it in addition to those endpoints after the firewall has been created. You can define a VPC endpoint association using a different VPC than the one you used in the firewall specifications.

Request Syntax

```
{
   "Description": "string",
   "FirewallArn": "string",
   "SubnetMapping": {
      "IPAddressType": "string",
      "SubnetId": "string"
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "VpcId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Description

A description of the VPC endpoint association.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

SubnetMapping

The ID for a subnet that's used in an association with a firewall. This is used in CreateFirewall, AssociateSubnets, and CreateVpcEndpointAssociation. AWS Network Firewall creates an instance of the associated firewall in each subnet that you specify, to filter traffic in the subnet's Availability Zone.

Type: SubnetMapping object

Required: Yes

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

VpcId

The unique identifier of the VPC where you want to create a firewall endpoint.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: Yes

Response Syntax

```
{
   "VpcEndpointAssociation": {
      "Description": "string",
      "FirewallArn": "string",
      "SubnetMapping": {
         "IPAddressType": "string",
         "SubnetId": "string"
      },
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "VpcEndpointAssociationArn": "string",
      "VpcEndpointAssociationId": "string",
      "VpcId": "string"
   },
   "VpcEndpointAssociationStatus": {
      "AssociationSyncState": {
         "string" : {
            "Attachment": {
               "EndpointId": "string",
               "Status": "string",
               "StatusMessage": "string",
               "SubnetId": "string"
            }
         }
      },
      "Status": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

VpcEndpointAssociation

The configuration settings for the VPC endpoint association. These settings include the firewall and the VPC and subnet to use for the firewall endpoint.

Type: VpcEndpointAssociation object

VpcEndpointAssociationStatus

Detailed information about the current status of a VpcEndpointAssociation. You can retrieve this by calling DescribeVpcEndpointAssociation and providing the VPC endpoint association ARN.

Type: VpcEndpointAssociationStatus object

Errors

For information about the errors that are common to all actions, see Common Errors.

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.

- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteFirewall

Deletes the specified Firewall and its FirewallStatus. This operation requires the firewall's `DeleteProtection` flag to be `FALSE`. You can't revert this operation.

You can check whether a firewall is in use by reviewing the route tables for the Availability Zones where you have firewall subnet mappings. Retrieve the subnet mappings by calling DescribeFirewall. You define and update the route tables through Amazon VPC. As needed, update the route tables for the zones to remove the firewall endpoints. When the route tables no longer use the firewall endpoints, you can remove the firewall safely.

To delete a firewall, remove the delete protection if you need to using UpdateFirewallDeleteProtection, then delete the firewall by calling DeleteFirewall.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "Firewall": {
      "AvailabilityZoneChangeProtection": boolean,
      "AvailabilityZoneMappings": [
         {
            "AvailabilityZone": "string"
         }
      ],
      "DeleteProtection": boolean,
      "Description": "string",
      "EnabledAnalysisTypes": [ "string" ],
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "NumberOfAssociations": number,
      "SubnetChangeProtection": boolean,
      "SubnetMappings": [
         {
            "IPAddressType": "string",
            "SubnetId": "string"
         }
```

```
        ],
        "Tags": [
           {
              "Key": "string",
              "Value": "string"
           }
        ],
        "TransitGatewayId": "string",
        "TransitGatewayOwnerAccountId": "string",
        "VpcId": "string"
     },
     "FirewallStatus": {
        "CapacityUsageSummary": {
           "CIDRs": {
              "AvailableCIDRCount": number,
              "IPSetReferences": {
                 "string" : {
                    "ResolvedCIDRCount": number
                 }
              },
              "UtilizedCIDRCount": number
           }
        },
        "ConfigurationSyncStateSummary": "string",
        "Status": "string",
        "SyncStates": {
           "string" : {
              "Attachment": {
                 "EndpointId": "string",
                 "Status": "string",
                 "StatusMessage": "string",
                 "SubnetId": "string"
              },
              "Config": {
                 "string" : {
                    "SyncStatus": "string",
                    "UpdateToken": "string"
                 }
              }
           }
        },
        "TransitGatewayAttachmentSyncState": {
           "AttachmentId": "string",
           "StatusMessage": "string",
```

```
            "TransitGatewayAttachmentStatus": "string"
        }
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewall

A firewall defines the behavior of a firewall, the main VPC where the firewall is used, the Availability Zones where the firewall can be used, and one subnet to use for a firewall endpoint within each of the Availability Zones. The Availability Zones are defined implicitly in the subnet specifications.

In addition to the firewall endpoints that you define in this `Firewall` specification, you can create firewall endpoints in `VpcEndpointAssociation` resources for any VPC, in any Availability Zone where the firewall is already in use.

The status of the firewall, for example whether it's ready to filter network traffic, is provided in the corresponding FirewallStatus. You can retrieve both the firewall and firewall status by calling DescribeFirewall.

Type: Firewall object

FirewallStatus

Detailed information about the current status of a Firewall. You can retrieve this for a firewall by calling DescribeFirewall and providing the firewall name and ARN.

The firewall status indicates a combined status. It indicates whether all subnets are up-to-date with the latest firewall configurations, which is based on the sync states config values, and also whether all subnets have their endpoints fully enabled, based on their sync states attachment values.

Type: FirewallStatus object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

UnsupportedOperationException

The operation you requested isn't supported by Network Firewall.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteFirewallPolicy

Deletes the specified FirewallPolicy.

Request Syntax

```
{
   "FirewallPolicyArn": "string",
   "FirewallPolicyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallPolicyName

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: ^[a-zA-Z0-9-]+$

Required: No

Response Syntax

```
{
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
      "ConsumedStatelessRuleCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string",
      "FirewallPolicyStatus": "string",
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicyResponse

The object containing the definition of the FirewallPolicyResponse that you asked to delete.

Type: FirewallPolicyResponse object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

UnsupportedOperationException

The operation you requested isn't supported by Network Firewall.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteNetworkFirewallTransitGatewayAttachment

Deletes a transit gateway attachment from a Network Firewall. Either the firewall owner or the transit gateway owner can delete the attachment.

> **Important**
>
> After you delete a transit gateway attachment, raffic will no longer flow through the firewall endpoints.

After you initiate the delete operation, use DescribeFirewall to monitor the deletion status.

Request Syntax

```
{
   "TransitGatewayAttachmentId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

TransitGatewayAttachmentId

Required. The unique identifier of the transit gateway attachment to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

Required: Yes

Response Syntax

```
{
```

```
    "TransitGatewayAttachmentId": "string",
    "TransitGatewayAttachmentStatus": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TransitGatewayAttachmentId

The ID of the transit gateway attachment that was deleted.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

TransitGatewayAttachmentStatus

The current status of the transit gateway attachment deletion process.

Valid values are:

- `CREATING` - The attachment is being created
- `DELETING` - The attachment is being deleted
- `DELETED` - The attachment has been deleted
- `FAILED` - The attachment creation has failed and cannot be recovered
- `ERROR` - The attachment is in an error state that might be recoverable
- `READY` - The attachment is active and processing traffic
- `PENDING_ACCEPTANCE` - The attachment is waiting to be accepted
- `REJECTING` - The attachment is in the process of being rejected
- `REJECTED` - The attachment has been rejected

Type: String

Valid Values: `CREATING | DELETING | DELETED | FAILED | ERROR | READY | PENDING_ACCEPTANCE | REJECTING | REJECTED`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteResourcePolicy

Deletes a resource policy that you created in a PutResourcePolicy request.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

ResourceArn

The Amazon Resource Name (ARN) of the rule group or firewall policy whose resource policy you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidResourcePolicyException

The policy statement failed validation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRuleGroup

Deletes the specified RuleGroup.

Request Syntax

```
{
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

RuleGroupArn

The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

> **Note**
>
> This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS` | `STATEFUL`

Required: No

Response Syntax

```
{
   "RuleGroupResponse": {
      "AnalysisResults": [
         {
            "AnalysisDetail": "string",
            "IdentifiedRuleIds": [ "string" ],
            "IdentifiedType": "string"
         }
      ],
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "RuleGroupStatus": "string",
```

```
        "SnsTopic": "string",
        "SourceMetadata": {
           "SourceArn": "string",
           "SourceUpdateToken": "string"
        },
        "SummaryConfiguration": {
           "RuleOptions": [ "string" ]
        },
        "Tags": [
           {
              "Key": "string",
              "Value": "string"
           }
        ],
        "Type": "string"
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroupResponse

The high-level properties of a rule group. This, along with the RuleGroup, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Type: RuleGroupResponse object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

UnsupportedOperationException

The operation you requested isn't supported by Network Firewall.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteTLSInspectionConfiguration

Deletes the specified TLSInspectionConfiguration.

Request Syntax

```
{
   "TLSInspectionConfigurationArn": "string",
   "TLSInspectionConfigurationName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

TLSInspectionConfigurationName

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "TLSInspectionConfigurationResponse": {
      "CertificateAuthority": {
         "CertificateArn": "string",
         "CertificateSerial": "string",
         "Status": "string",
         "StatusMessage": "string"
      },
      "Certificates": [
         {
            "CertificateArn": "string",
            "CertificateSerial": "string",
            "Status": "string",
            "StatusMessage": "string"
         }
      ],
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "TLSInspectionConfigurationArn": "string",
      "TLSInspectionConfigurationId": "string",
      "TLSInspectionConfigurationName": "string",
      "TLSInspectionConfigurationStatus": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the TLSInspectionConfiguration, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

Type: TLSInspectionConfigurationResponse object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteVpcEndpointAssociation

Deletes the specified VpcEndpointAssociation.

You can check whether an endpoint association is in use by reviewing the route tables for the Availability Zones where you have the endpoint subnet mapping. You can retrieve the subnet mapping by calling DescribeVpcEndpointAssociation. You define and update the route tables through Amazon VPC. As needed, update the route tables for the Availability Zone to remove the firewall endpoint for the association. When the route tables no longer use the firewall endpoint, you can remove the endpoint association safely.

Request Syntax

```
{
   "VpcEndpointAssociationArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "VpcEndpointAssociation": {
```

```
        "Description": "string",
        "FirewallArn": "string",
        "SubnetMapping": {
           "IPAddressType": "string",
           "SubnetId": "string"
        },
        "Tags": [
           {
              "Key": "string",
              "Value": "string"
           }
        ],
        "VpcEndpointAssociationArn": "string",
        "VpcEndpointAssociationId": "string",
        "VpcId": "string"
    },
    "VpcEndpointAssociationStatus": {
        "AssociationSyncState": {
           "string" : {
              "Attachment": {
                 "EndpointId": "string",
                 "Status": "string",
                 "StatusMessage": "string",
                 "SubnetId": "string"
              }
           }
        },
        "Status": "string"
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

VpcEndpointAssociation

The configuration settings for the VPC endpoint association. These settings include the firewall and the VPC and subnet to use for the firewall endpoint.

Type: VpcEndpointAssociation object

VpcEndpointAssociationStatus

Detailed information about the current status of a VpcEndpointAssociation. You can retrieve this by calling DescribeVpcEndpointAssociation and providing the VPC endpoint association ARN.

Type: VpcEndpointAssociationStatus object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFirewall

Returns the data objects for the specified firewall.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: ^[a-zA-Z0-9-]+$

Required: No

Response Syntax

```
{
   "Firewall": {
      "AvailabilityZoneChangeProtection": boolean,
      "AvailabilityZoneMappings": [
         {
            "AvailabilityZone": "string"
         }
      ],
      "DeleteProtection": boolean,
      "Description": "string",
      "EnabledAnalysisTypes": [ "string" ],
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "NumberOfAssociations": number,
      "SubnetChangeProtection": boolean,
      "SubnetMappings": [
         {
            "IPAddressType": "string",
            "SubnetId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "TransitGatewayId": "string",
      "TransitGatewayOwnerAccountId": "string",
      "VpcId": "string"
```

```
    },
    "FirewallStatus": {
       "CapacityUsageSummary": {
          "CIDRs": {
             "AvailableCIDRCount": number,
             "IPSetReferences": {
                "string" : {
                   "ResolvedCIDRCount": number
                }
             },
             "UtilizedCIDRCount": number
          }
       },
       "ConfigurationSyncStateSummary": "string",
       "Status": "string",
       "SyncStates": {
          "string" : {
             "Attachment": {
                "EndpointId": "string",
                "Status": "string",
                "StatusMessage": "string",
                "SubnetId": "string"
             },
             "Config": {
                "string" : {
                   "SyncStatus": "string",
                   "UpdateToken": "string"
                }
             }
          }
       },
       "TransitGatewayAttachmentSyncState": {
          "AttachmentId": "string",
          "StatusMessage": "string",
          "TransitGatewayAttachmentStatus": "string"
       }
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewall

The configuration settings for the firewall. These settings include the firewall policy and the subnets in your VPC to use for the firewall endpoints.

Type: Firewall object

FirewallStatus

Detailed information about the current status of a Firewall. You can retrieve this for a firewall by calling DescribeFirewall and providing the firewall name and ARN.

The firewall status indicates a combined status. It indicates whether all subnets are up-to-date with the latest firewall configurations, which is based on the sync states config values, and also whether all subnets have their endpoints fully enabled, based on their sync states attachment values.

Type: FirewallStatus object

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFirewallMetadata

Returns the high-level information about a firewall, including the Availability Zones where the Firewall is currently in use.

Request Syntax

```
{
   "FirewallArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

Response Syntax

```
{
   "Description": "string",
   "FirewallArn": "string",
   "FirewallPolicyArn": "string",
   "Status": "string",
   "SupportedAvailabilityZones": {
      "string" : {
         "IPAddressType": "string"
      }
   },
```

```
    "TransitGatewayAttachmentId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Description

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Status

The readiness of the configured firewall to handle network traffic across all of the Availability Zones where you have it configured. This setting is `READY` only when the `ConfigurationSyncStateSummary` value is `IN_SYNC` and the `Attachment Status` values for all of the configured subnets are `READY`.

Type: String

Valid Values: `PROVISIONING | DELETING | READY`

SupportedAvailabilityZones

The Availability Zones that the firewall currently supports. This includes all Availability Zones for which the firewall has a subnet defined.

Type: String to AvailabilityZoneMetadata object map

TransitGatewayAttachmentId

The unique identifier of the transit gateway attachment associated with this firewall. This field is only present for transit gateway-attached firewalls.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFirewallPolicy

Returns the data objects for the specified firewall policy.

Request Syntax

```
{
   "FirewallPolicyArn": "string",
   "FirewallPolicyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallPolicyName

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: ^[a-zA-Z0-9-]+$

Required: No

Response Syntax

```
{
   "FirewallPolicy": {
      "PolicyVariables": {
         "RuleVariables": {
            "string" : {
               "Definition": [ "string" ]
            }
         }
      },
      "StatefulDefaultActions": [ "string" ],
      "StatefulEngineOptions": {
         "FlowTimeouts": {
            "TcpIdleTimeoutSeconds": number
         },
         "RuleOrder": "string",
         "StreamExceptionPolicy": "string"
      },
      "StatefulRuleGroupReferences": [
         {
            "DeepThreatInspection": boolean,
            "Override": {
               "Action": "string"
            },
            "Priority": number,
            "ResourceArn": "string"
         }
      ],
      "StatelessCustomActions": [
         {
            "ActionDefinition": {
               "PublishMetricAction": {
                  "Dimensions": [
                     {
                        "Value": "string"
                     }
                  ]
               }
```

```
            },
            "ActionName": "string"
         }
      ],
      "StatelessDefaultActions": [ "string" ],
      "StatelessFragmentDefaultActions": [ "string" ],
      "StatelessRuleGroupReferences": [
         {
            "Priority": number,
            "ResourceArn": "string"
         }
      ],
      "TLSInspectionConfigurationArn": "string"
   },
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
      "ConsumedStatelessRuleCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string",
      "FirewallPolicyStatus": "string",
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicy

The policy for the specified firewall policy.

Type: FirewallPolicy object

FirewallPolicyResponse

The high-level properties of a firewall policy. This, along with the FirewallPolicy, define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy.

Type: FirewallPolicyResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFlowOperation

Returns key information about a specific flow operation.

Request Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowOperationId": "string",
   "VpcEndpointAssociationArn": "string",
   "VpcEndpointId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

VpcEndpointId

A unique identifier for the primary endpoint associated with a firewall.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Required: No

Response Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowOperation": {
```

```
        "FlowFilters": [
           {
              "DestinationAddress": {
                 "AddressDefinition": "string"
              },
              "DestinationPort": "string",
              "Protocols": [ "string" ],
              "SourceAddress": {
                 "AddressDefinition": "string"
              },
              "SourcePort": "string"
           }
        ],
        "MinimumFlowAgeInSeconds": number
     },
     "FlowOperationId": "string",
     "FlowOperationStatus": "string",
     "FlowOperationType": "string",
     "FlowRequestTimestamp": number,
     "StatusMessage": "string",
     "VpcEndpointAssociationArn": "string",
     "VpcEndpointId": "string"
  }
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FlowOperation

Returns key information about a flow operation, such as related statuses, unique identifiers, and all filters defined in the operation.

Type: FlowOperation object

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

FlowOperationStatus

Returns the status of the flow operation. This string is returned in the responses to start, list, and describe commands.

If the status is `COMPLETED_WITH_ERRORS`, results may be returned with any number of `Flows` missing from the response. If the status is `FAILED`, `Flows` returned will be empty.

Type: String

Valid Values: `COMPLETED | IN_PROGRESS | FAILED | COMPLETED_WITH_ERRORS`

FlowOperationType

Defines the type of `FlowOperation`.

Type: String

Valid Values: `FLOW_FLUSH | FLOW_CAPTURE`

FlowRequestTimestamp

A timestamp indicating when the Suricata engine identified flows impacted by an operation.

Type: Timestamp

StatusMessage

If the asynchronous operation fails, Network Firewall populates this with the reason for the error or failure. Options include `Flow operation error` and `Flow timeout`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9- ]+$`

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

VpcEndpointId

A unique identifier for the primary endpoint associated with a firewall.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeLoggingConfiguration

Returns the logging configuration for the specified firewall.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "EnableMonitoringDashboard": boolean,
   "FirewallArn": "string",
   "LoggingConfiguration": {
      "LogDestinationConfigs": [
         {
            "LogDestination": {
               "string" : "string"
            },
            "LogDestinationType": "string",
            "LogType": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EnableMonitoringDashboard

A boolean that reflects whether or not the firewall monitoring dashboard is enabled on a firewall.

Returns TRUE when the firewall monitoring dashboard is enabled on the firewall. Returns FALSE when the firewall monitoring dashboard is not enabled on the firewall.

Type: Boolean

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

LoggingConfiguration

Defines how AWS Network Firewall performs logging for a Firewall.

Type: LoggingConfiguration object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeResourcePolicy

Retrieves a resource policy that you created in a PutResourcePolicy request.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

ResourceArn

The Amazon Resource Name (ARN) of the rule group or firewall policy whose resource policy you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "Policy": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Policy

The IAM policy for the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 395000.

Pattern: `.*\S.*`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRuleGroup

Returns the data objects for the specified rule group.

Request Syntax

```
{
   "AnalyzeRuleGroup": boolean,
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AnalyzeRuleGroup

Indicates whether you want Network Firewall to analyze the stateless rules in the rule group for rule behavior such as asymmetric routing. If set to TRUE, Network Firewall runs the analysis.

Type: Boolean

Required: No

RuleGroupArn

The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

> **Note**
>
> This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

Response Syntax

```
{
   "RuleGroup": {
      "ReferenceSets": {
         "IPSetReferences": {
            "string" : {
               "ReferenceArn": "string"
            }
         }
      },
      "RulesSource": {
```

```
        "RulesSourceList": {
           "GeneratedRulesType": "string",
           "Targets": [ "string" ],
           "TargetTypes": [ "string" ]
        },
        "RulesString": "string",
        "StatefulRules": [
           {
              "Action": "string",
              "Header": {
                 "Destination": "string",
                 "DestinationPort": "string",
                 "Direction": "string",
                 "Protocol": "string",
                 "Source": "string",
                 "SourcePort": "string"
              },
              "RuleOptions": [
                 {
                    "Keyword": "string",
                    "Settings": [ "string" ]
                 }
              ]
           }
        ],
        "StatelessRulesAndCustomActions": {
           "CustomActions": [
              {
                 "ActionDefinition": {
                    "PublishMetricAction": {
                       "Dimensions": [
                          {
                             "Value": "string"
                          }
                       ]
                    }
                 },
                 "ActionName": "string"
              }
           ],
           "StatelessRules": [
              {
                 "Priority": number,
                 "RuleDefinition": {
```

```
                    "Actions": [ "string" ],
                    "MatchAttributes": {
                       "DestinationPorts": [
                          {
                             "FromPort": number,
                             "ToPort": number
                          }
                       ],
                       "Destinations": [
                          {
                             "AddressDefinition": "string"
                          }
                       ],
                       "Protocols": [ number ],
                       "SourcePorts": [
                          {
                             "FromPort": number,
                             "ToPort": number
                          }
                       ],
                       "Sources": [
                          {
                             "AddressDefinition": "string"
                          }
                       ],
                       "TCPFlags": [
                          {
                             "Flags": [ "string" ],
                             "Masks": [ "string" ]
                          }
                       ]
                    }
                 }
              }
           ]
        }
     },
     "RuleVariables": {
        "IPSets": {
           "string" : {
              "Definition": [ "string" ]
           }
        },
        "PortSets": {
```

```
            "string" : {
               "Definition": [ "string" ]
            }
         }
      },
      "StatefulRuleOptions": {
         "RuleOrder": "string"
      }
   },
   "RuleGroupResponse": {
      "AnalysisResults": [
         {
            "AnalysisDetail": "string",
            "IdentifiedRuleIds": [ "string" ],
            "IdentifiedType": "string"
         }
      ],
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "RuleGroupStatus": "string",
      "SnsTopic": "string",
      "SourceMetadata": {
         "SourceArn": "string",
         "SourceUpdateToken": "string"
      },
      "SummaryConfiguration": {
         "RuleOptions": [ "string" ]
      },
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
```

```
        "Type": "string"
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroup

The object that defines the rules in a rule group. This, along with RuleGroupResponse, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

AWS Network Firewall uses a rule group to inspect and control network traffic. You define stateless rule groups to inspect individual packets and you define stateful rule groups to inspect packets in the context of their traffic flow.

To use a rule group, you include it by reference in an Network Firewall firewall policy, then you use the policy in a firewall. You can reference a rule group from more than one firewall policy, and you can use a firewall policy in more than one firewall.

Type: RuleGroup object

RuleGroupResponse

The high-level properties of a rule group. This, along with the RuleGroup, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Type: RuleGroupResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve

the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRuleGroupMetadata

High-level information about a rule group, returned by operations like create and describe. You can use the information provided in the metadata to retrieve and manage a rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Request Syntax

```
{
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

RuleGroupArn

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

> **Note**
>
> This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

Response Syntax

```
{
   "Capacity": number,
   "Description": "string",
   "LastModifiedTime": number,
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "StatefulRuleOptions": {
      "RuleOrder": "string"
   },
   "Type": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Capacity

The maximum operating resources that this rule group can use. Rule group capacity is fixed at creation. When you update a rule group, you are limited to this capacity. When you reference a rule group from a firewall policy, Network Firewall reserves this capacity for the rule group.

You can retrieve the capacity that would be required for a rule group before you create the rule group by calling CreateRuleGroup with `DryRun` set to `TRUE`.

Type: Integer

Description

Returns the metadata objects for the specified rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

LastModifiedTime

A timestamp indicating when the rule group was last modified.

Type: Timestamp

RuleGroupArn

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

StatefulRuleOptions

Additional options governing how Network Firewall handles the rule group. You can only use these for stateful rule groups.

Type: StatefulRuleOptions object

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

> **Note**
>
> This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS | STATEFUL`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRuleGroupSummary

Returns detailed information for a stateful rule group.

For active threat defense AWS managed rule groups, this operation provides insight into the protections enabled by the rule group, based on Suricata rule metadata fields. Summaries are available for rule groups you manage and for active threat defense AWS managed rule groups.

To modify how threat information appears in summaries, use the `SummaryConfiguration` parameter in UpdateRuleGroup.

Request Syntax

```
{
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

RuleGroupArn

Required. The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Type

The type of rule group you want a summary for. This is a required field.

Valid value: `STATEFUL`

Note that `STATELESS` exists but is not currently supported. If you provide `STATELESS`, an exception is returned.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

Response Syntax

```
{
   "Description": "string",
   "RuleGroupName": "string",
   "Summary": {
      "RuleSummaries": [
         {
            "Metadata": "string",
            "Msg": "string",
            "SID": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Description

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Summary

A complex type that contains rule information based on the rule group's configured summary settings. The content varies depending on the fields that you specified to extract in your SummaryConfiguration. When you haven't configured any summary settings, this returns an empty array. The response might include:

- Rule identifiers
- Rule descriptions
- Any metadata fields that you specified in your SummaryConfiguration

Type: Summary object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeTLSInspectionConfiguration

Returns the data objects for the specified TLS inspection configuration.

Request Syntax

```
{
   "TLSInspectionConfigurationArn": "string",
   "TLSInspectionConfigurationName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

TLSInspectionConfigurationName

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "TLSInspectionConfiguration": {
      "ServerCertificateConfigurations": [
         {
            "CertificateAuthorityArn": "string",
            "CheckCertificateRevocationStatus": {
               "RevokedStatusAction": "string",
               "UnknownStatusAction": "string"
            },
            "Scopes": [
               {
                  "DestinationPorts": [
                     {
                        "FromPort": number,
                        "ToPort": number
                     }
                  ],
                  "Destinations": [
                     {
                        "AddressDefinition": "string"
                     }
                  ],
                  "Protocols": [ number ],
                  "SourcePorts": [
                     {
                        "FromPort": number,
                        "ToPort": number
                     }
                  ],
                  "Sources": [
                     {
                        "AddressDefinition": "string"
                     }
                  ]
               }
            ],
            "ServerCertificates": [
               {
                  "ResourceArn": "string"
               }
            ]
```

```
            }
        ]
    },
    "TLSInspectionConfigurationResponse": {
        "CertificateAuthority": {
            "CertificateArn": "string",
            "CertificateSerial": "string",
            "Status": "string",
            "StatusMessage": "string"
        },
        "Certificates": [
            {
                "CertificateArn": "string",
                "CertificateSerial": "string",
                "Status": "string",
                "StatusMessage": "string"
            }
        ],
        "Description": "string",
        "EncryptionConfiguration": {
            "KeyId": "string",
            "Type": "string"
        },
        "LastModifiedTime": number,
        "NumberOfAssociations": number,
        "Tags": [
            {
                "Key": "string",
                "Value": "string"
            }
        ],
        "TLSInspectionConfigurationArn": "string",
        "TLSInspectionConfigurationId": "string",
        "TLSInspectionConfigurationName": "string",
        "TLSInspectionConfigurationStatus": "string"
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with TLSInspectionConfigurationResponse, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

AWS Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see Inspecting SSL/TLS traffic with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

Type: TLSInspectionConfiguration object

TLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the TLSInspectionConfiguration, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

Type: TLSInspectionConfigurationResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the TLS inspection configuration. The token marks the state of the TLS inspection configuration resource at the time of the request.

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeVpcEndpointAssociation

Returns the data object for the specified VPC endpoint association.

Request Syntax

```
{
   "VpcEndpointAssociationArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "VpcEndpointAssociation": {
      "Description": "string",
      "FirewallArn": "string",
      "SubnetMapping": {
         "IPAddressType": "string",
         "SubnetId": "string"
      },
      "Tags": [
         {
```

```
            "Key": "string",
            "Value": "string"
         }
      ],
      "VpcEndpointAssociationArn": "string",
      "VpcEndpointAssociationId": "string",
      "VpcId": "string"
   },
   "VpcEndpointAssociationStatus": {
      "AssociationSyncState": {
         "string" : {
            "Attachment": {
               "EndpointId": "string",
               "Status": "string",
               "StatusMessage": "string",
               "SubnetId": "string"
            }
         }
      },
      "Status": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

VpcEndpointAssociation

The configuration settings for the VPC endpoint association. These settings include the firewall and the VPC and subnet to use for the firewall endpoint.

Type: VpcEndpointAssociation object

VpcEndpointAssociationStatus

Detailed information about the current status of a VpcEndpointAssociation. You can retrieve this by calling DescribeVpcEndpointAssociation and providing the VPC endpoint association ARN.

Type: VpcEndpointAssociationStatus object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateAvailabilityZones

Removes the specified Availability Zone associations from a transit gateway-attached firewall. This removes the firewall endpoints from these Availability Zones and stops traffic filtering in those zones. Before removing an Availability Zone, ensure you've updated your transit gateway route tables to redirect traffic appropriately.

> **Note**
>
> If `AvailabilityZoneChangeProtection` is enabled, you must first disable it using UpdateAvailabilityZoneChangeProtection.

To verify the status of your Availability Zone changes, use DescribeFirewall.

Request Syntax

```
{
   "AvailabilityZoneMappings": [
      {
         "AvailabilityZone": "string"
      }
   ],
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZoneMappings

Required. The Availability Zones to remove from the firewall's configuration.

Type: Array of AvailabilityZoneMapping objects

Required: Yes

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "AvailabilityZoneMappings": [
      {
         "AvailabilityZone": "string"
      }
   ],
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AvailabilityZoneMappings

The remaining Availability Zones where the firewall has endpoints after the disassociation.

Type: Array of AvailabilityZoneMapping objects

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateSubnets

Removes the specified subnet associations from the firewall. This removes the firewall endpoints from the subnets and removes any network filtering protections that the endpoints were providing.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetIds": [ "string" ],
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

SubnetIds

The unique identifiers for the subnets that you want to disassociate.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^subnet-[0-9a-f]+$`

Required: Yes

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
```

```
    "SubnetMappings": [
       {
          "IPAddressType": "string",
          "SubnetId": "string"
       }
    ],
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

SubnetMappings

The IDs of the subnets that are associated with the firewall.

Type: Array of SubnetMapping objects

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAnalysisReportResults

The results of a COMPLETED analysis report generated with StartAnalysisReport.

For more information, see AnalysisTypeReportResult.

Request Syntax

```
{
   "AnalysisReportId": "string",
   "FirewallArn": "string",
   "FirewallName": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AnalysisReportId

The unique ID of the query that ran when you requested an analysis report.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: \S+

Required: Yes

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Response Syntax

```
{
   "AnalysisReportResults": [
      {
         "Domain": "string",
         "FirstAccessed": number,
         "Hits": {
            "Count": number
         },
         "LastAccessed": number,
         "Protocol": "string",
         "UniqueSources": {
            "Count": number
         }
      }
   ],
   "AnalysisType": "string",
   "EndTime": number,
   "NextToken": "string",
   "ReportTime": number,
   "StartTime": number,
   "Status": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AnalysisReportResults

Retrieves the results of a traffic analysis report.

Type: Array of AnalysisTypeReportResult objects

AnalysisType

The type of traffic that will be used to generate a report.

Type: String

Valid Values: `TLS_SNI` | `HTTP_HOST`

EndTime

The date and time, up to the current date, from which to stop retrieving analysis data, in UTC format (for example, `YYYY-MM-DDTHH:MM:SSZ`).

Type: Timestamp

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

ReportTime

The date and time the analysis report was ran.

Type: Timestamp

StartTime

The date and time within the last 30 days from which to start retrieving analysis data, in UTC format (for example, `YYYY-MM-DDTHH:MM:SSZ`.

Type: Timestamp

Status

The status of the analysis report you specify. Statuses include `RUNNING`, `COMPLETED`, or `FAILED`.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAnalysisReports

Returns a list of all traffic analysis reports generated within the last 30 days.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: ^[a-zA-Z0-9-]+$

Required: No

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: [0-9A-Za-z:\/+=]+$

Required: No

Response Syntax

```
{
   "AnalysisReports": [
      {
         "AnalysisReportId": "string",
         "AnalysisType": "string",
         "ReportTime": number,
         "Status": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AnalysisReports

The `id` and `ReportTime` associated with a requested analysis report. Does not provide the status of the analysis report.

Type: Array of AnalysisReport objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFirewallPolicies

Retrieves the metadata for the firewall policies that you have defined. Depending on your setting for max results and the number of firewall policies, a single call might not return the full list.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

Response Syntax

```
{
   "FirewallPolicies": [
      {
         "Arn": "string",
         "Name": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicies

The metadata for the firewall policies. Depending on your setting for max results and the number of firewall policies that you have, this might not be the full list.

Type: Array of FirewallPolicyMetadata objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFirewalls

Retrieves the metadata for the firewalls that you have defined. If you provide VPC identifiers in your request, this returns only the firewalls for those VPCs.

Depending on your setting for max results and the number of firewalls, a single call might not return the full list.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string",
   "VpcIds": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

VpcIds

The unique identifiers of the VPCs that you want Network Firewall to retrieve the firewalls for. Leave this blank to retrieve all firewalls that you have defined.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: No

Response Syntax

```
{
   "Firewalls": [
      {
         "FirewallArn": "string",
         "FirewallName": "string",
         "TransitGatewayAttachmentId": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewalls

The firewall metadata objects for the VPCs that you specified. Depending on your setting for max results and the number of firewalls you have, a single call might not be the full list.

Type: Array of FirewallMetadata objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFlowOperationResults

Returns the results of a specific flow operation.

Flow operations let you manage the flows tracked in the flow table, also known as the firewall table.

A flow is network traffic that is monitored by a firewall, either by stateful or stateless rules. For traffic to be considered part of a flow, it must share Destination, DestinationPort, Direction, Protocol, Source, and SourcePort.

Request Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowOperationId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "VpcEndpointAssociationArn": "string",
   "VpcEndpointId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

VpcEndpointId

A unique identifier for the primary endpoint associated with a firewall.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Required: No

Response Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowOperationId": "string",
   "FlowOperationStatus": "string",
   "FlowRequestTimestamp": number,
   "Flows": [
      {
         "Age": number,
         "ByteCount": number,
         "DestinationAddress": {
            "AddressDefinition": "string"
         },
         "DestinationPort": "string",
         "PacketCount": number,
```

```
            "Protocol": "string",
            "SourceAddress": {
               "AddressDefinition": "string"
            },
            "SourcePort": "string"
         }
      ],
      "NextToken": "string",
      "StatusMessage": "string",
      "VpcEndpointAssociationArn": "string",
      "VpcEndpointId": "string"
   }
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

FlowOperationStatus

Returns the status of the flow operation. This string is returned in the responses to start, list, and describe commands.

If the status is `COMPLETED_WITH_ERRORS`, results may be returned with any number of `Flows` missing from the response. If the status is `FAILED`, `Flows` returned will be empty.

Type: String

Valid Values: `COMPLETED | IN_PROGRESS | FAILED | COMPLETED_WITH_ERRORS`

FlowRequestTimestamp

A timestamp indicating when the Suricata engine identified flows impacted by an operation.

Type: Timestamp

Flows

Any number of arrays, where each array is a single flow identified in the scope of the operation. If multiple flows were in the scope of the operation, multiple `Flows` arrays are returned.

Type: Array of Flow objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

StatusMessage

If the asynchronous operation fails, Network Firewall populates this with the reason for the error or failure. Options include `Flow operation error` and `Flow timeout`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9- ]+$`

VpcEndpointAssociationArn

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

VpcEndpointId

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFlowOperations

Returns a list of all flow operations ran in a specific firewall. You can optionally narrow the request scope by specifying the operation type or Availability Zone associated with a firewall's flow operations.

Flow operations let you manage the flows tracked in the flow table, also known as the firewall table.

A flow is network traffic that is monitored by a firewall, either by stateful or stateless rules. For traffic to be considered part of a flow, it must share Destination, DestinationPort, Direction, Protocol, Source, and SourcePort.

Request Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowOperationType": "string",
   "MaxResults": number,
   "NextToken": "string",
   "VpcEndpointAssociationArn": "string",
   "VpcEndpointId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FlowOperationType

An optional string that defines whether any or all operation types are returned.

Type: String

Valid Values: `FLOW_FLUSH | FLOW_CAPTURE`

Required: No

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

VpcEndpointId

A unique identifier for the primary endpoint associated with a firewall.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Required: No

Response Syntax

```
{
   "FlowOperations": [
      {
         "FlowOperationId": "string",
         "FlowOperationStatus": "string",
         "FlowOperationType": "string",
         "FlowRequestTimestamp": number
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FlowOperations

Flow operations let you manage the flows tracked in the flow table, also known as the firewall table.

A flow is network traffic that is monitored by a firewall, either by stateful or stateless rules. For traffic to be considered part of a flow, it must share Destination, DestinationPort, Direction, Protocol, Source, and SourcePort.

Type: Array of FlowOperationMetadata objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.

- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRuleGroups

Retrieves the metadata for the rule groups that you have defined. Depending on your setting for max results and the number of rule groups, a single call might not return the full list.

Request Syntax

```
{
   "ManagedType": "string",
   "MaxResults": number,
   "NextToken": "string",
   "Scope": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

ManagedType

Indicates the general category of the AWS managed rule group.

Type: String

Valid Values: `AWS_MANAGED_THREAT_SIGNATURES | AWS_MANAGED_DOMAIN_LISTS | ACTIVE_THREAT_DEFENSE`

Required: No

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

Scope

The scope of the request. The default setting of `ACCOUNT` or a setting of `NULL` returns all of the rule groups in your account. A setting of `MANAGED` returns all available managed rule groups.

Type: String

Valid Values: `MANAGED | ACCOUNT`

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

Response Syntax

```
{
   "NextToken": "string",
```

```
    "RuleGroups": [
       {
          "Arn": "string",
          "Name": "string"
       }
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

RuleGroups

The rule group metadata objects that you've defined. Depending on your setting for max results and the number of rule groups, this might not be the full list.

Type: Array of RuleGroupMetadata objects

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

Retrieves the tags associated with the specified resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

You can tag the AWS resources that you manage through AWS Network Firewall: firewalls, firewall policies, and rule groups.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

ResourceArn

The Amazon Resource Name (ARN) of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a

`NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Tags

The tags that are associated with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTLSInspectionConfigurations

Retrieves the metadata for the TLS inspection configurations that you have defined. Depending on your setting for max results and the number of TLS inspection configurations, a single call might not return the full list.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "TLSInspectionConfigurations": [
      {
         "Arn": "string",
         "Name": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

TLSInspectionConfigurations

The TLS inspection configuration metadata objects that you've defined. Depending on your setting for max results and the number of TLS inspection configurations, this might not be the full list.

Type: Array of TLSInspectionConfigurationMetadata objects

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListVpcEndpointAssociations

Retrieves the metadata for the VPC endpoint associations that you have defined. If you specify a fireawll, this returns only the endpoint associations for that firewall.

Depending on your setting for max results and the number of associations, a single call might not return the full list.

Request Syntax

```
{
   "FirewallArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

If you don't specify this, Network Firewall retrieves all VPC endpoint associations that you have defined.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

MaxResults

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "VpcEndpointAssociations": [
      {
         "VpcEndpointAssociationArn": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a

`NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `[0-9A-Za-z:\/+=]+$`

VpcEndpointAssociations

The VPC endpoint assocation metadata objects for the firewall that you specified. If you didn't specify a firewall, this is all VPC endpoint associations that you have defined.

Depending on your setting for max results and the number of firewalls you have, a single call might not be the full list.

Type: Array of VpcEndpointAssociationMetadata objects

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutResourcePolicy

Creates or updates an IAM policy for your rule group, firewall policy, or firewall. Use this to share these resources between accounts. This operation works in conjunction with the AWS Resource Access Manager (RAM) service to manage resource sharing for Network Firewall.

For information about using sharing with Network Firewall resources, see Sharing Network Firewall resources in the *AWS Network Firewall Developer Guide*.

Use this operation to create or update a resource policy for your Network Firewall rule group, firewall policy, or firewall. In the resource policy, you specify the accounts that you want to share the Network Firewall resource with and the operations that you want the accounts to be able to perform.

When you add an account in the resource policy, you then run the following Resource Access Manager (RAM) operations to access and accept the shared resource.

- GetResourceShareInvitations - Returns the Amazon Resource Names (ARNs) of the resource share invitations.
- AcceptResourceShareInvitation - Accepts the share invitation for a specified resource share.

For additional information about resource sharing using RAM, see AWS Resource Access Manager User Guide.

Request Syntax

```
{
   "Policy": "string",
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Policy

The IAM policy statement that lists the accounts that you want to share your Network Firewall resources with and the operations that you want the accounts to be able to perform.

For a rule group resource, you can specify the following operations in the Actions section of the statement:

- network-firewall:CreateFirewallPolicy
- network-firewall:UpdateFirewallPolicy
- network-firewall:ListRuleGroups

For a firewall policy resource, you can specify the following operations in the Actions section of the statement:

- network-firewall:AssociateFirewallPolicy
- network-firewall:ListFirewallPolicies

For a firewall resource, you can specify the following operations in the Actions section of the statement:

- network-firewall:CreateVpcEndpointAssociation
- network-firewall:DescribeFirewallMetadata
- network-firewall:ListFirewalls

In the Resource section of the statement, you specify the ARNs for the Network Firewall resources that you want to share with the account that you specified in `Arn`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 395000.

Pattern: `.*\S.*`

Required: Yes

ResourceArn

The Amazon Resource Name (ARN) of the account that you want to share your Network Firewall resources with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidResourcePolicyException

The policy statement failed validation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RejectNetworkFirewallTransitGatewayAttachment

Rejects a transit gateway attachment request for Network Firewall. When you reject the attachment request, Network Firewall cancels the creation of routing components between the transit gateway and firewall endpoints.

Only the firewall owner can reject the attachment. After rejection, no traffic will flow through the firewall endpoints for this attachment.

Use DescribeFirewall to monitor the rejection status. To accept the attachment instead of rejecting it, use AcceptNetworkFirewallTransitGatewayAttachment.

> **Note**
>
> Once rejected, you cannot reverse this action. To establish connectivity, you must create a new transit gateway-attached firewall.

Request Syntax

```
{
   "TransitGatewayAttachmentId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

TransitGatewayAttachmentId

Required. The unique identifier of the transit gateway attachment to reject. This ID is returned in the response when creating a transit gateway-attached firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

Required: Yes

Response Syntax

```
{
   "TransitGatewayAttachmentId": "string",
   "TransitGatewayAttachmentStatus": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TransitGatewayAttachmentId

The unique identifier of the transit gateway attachment that was rejected.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

TransitGatewayAttachmentStatus

The current status of the transit gateway attachment. Valid values are:

- `CREATING` - The attachment is being created
- `DELETING` - The attachment is being deleted
- `DELETED` - The attachment has been deleted
- `FAILED` - The attachment creation has failed and cannot be recovered
- `ERROR` - The attachment is in an error state that might be recoverable
- `READY` - The attachment is active and processing traffic
- `PENDING_ACCEPTANCE` - The attachment is waiting to be accepted
- `REJECTING` - The attachment is in the process of being rejected
- `REJECTED` - The attachment has been rejected

For information about troubleshooting endpoint failures, see Troubleshooting firewall endpoint failures in the *AWS Network Firewall Developer Guide*.

Type: String

Valid Values: `CREATING | DELETING | DELETED | FAILED | ERROR | READY | PENDING_ACCEPTANCE | REJECTING | REJECTED`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartAnalysisReport

Generates a traffic analysis report for the timeframe and traffic type you specify.

For information on the contents of a traffic analysis report, see AnalysisReport.

Request Syntax

```
{
   "AnalysisType": "string",
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AnalysisType

The type of traffic that will be used to generate a report.

Type: String

Valid Values: `TLS_SNI | HTTP_HOST`

Required: Yes

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "AnalysisReportId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AnalysisReportId

The unique ID of the query that ran when you requested an analysis report.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `\S+`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartFlowCapture

Begins capturing the flows in a firewall, according to the filters you define. Captures are similar, but not identical to snapshots. Capture operations provide visibility into flows that are not closed and are tracked by a firewall's flow table. Unlike snapshots, captures are a time-boxed view.

A flow is network traffic that is monitored by a firewall, either by stateful or stateless rules. For traffic to be considered part of a flow, it must share Destination, DestinationPort, Direction, Protocol, Source, and SourcePort.

> **Note**
>
> To avoid encountering operation limits, you should avoid starting captures with broad filters, like wide IP ranges. Instead, we recommend you define more specific criteria with `FlowFilters`, like narrow IP ranges, ports, or protocols.

Request Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowFilters": [
      {
         "DestinationAddress": {
            "AddressDefinition": "string"
         },
         "DestinationPort": "string",
         "Protocols": [ "string" ],
         "SourceAddress": {
            "AddressDefinition": "string"
         },
         "SourcePort": "string"
      }
   ],
   "MinimumFlowAgeInSeconds": number,
   "VpcEndpointAssociationArn": "string",
   "VpcEndpointId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FlowFilters

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: Array of FlowFilter objects

Required: Yes

MinimumFlowAgeInSeconds

The reqested `FlowOperation` ignores flows with an age (in seconds) lower than `MinimumFlowAgeInSeconds`. You provide this for start commands.

> **Note**
>
> We recommend setting this value to at least 1 minute (60 seconds) to reduce chance of capturing flows that are not yet established.

Type: Integer

Required: No

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

VpcEndpointId

A unique identifier for the primary endpoint associated with a firewall.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FlowOperationId": "string",
   "FlowOperationStatus": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

FlowOperationStatus

Returns the status of the flow operation. This string is returned in the responses to start, list, and describe commands.

If the status is `COMPLETED_WITH_ERRORS`, results may be returned with any number of `Flows` missing from the response. If the status is `FAILED`, `Flows` returned will be empty.

Type: String

Valid Values: `COMPLETED | IN_PROGRESS | FAILED | COMPLETED_WITH_ERRORS`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartFlowFlush

Begins the flushing of traffic from the firewall, according to the filters you define. When the operation starts, impacted flows are temporarily marked as timed out before the Suricata engine prunes, or flushes, the flows from the firewall table.

> **Important**
>
> While the flush completes, impacted flows are processed as midstream traffic. This may result in a temporary increase in midstream traffic metrics. We recommend that you double check your stream exception policy before you perform a flush operation.

Request Syntax

```
{
   "AvailabilityZone": "string",
   "FirewallArn": "string",
   "FlowFilters": [
      {
         "DestinationAddress": {
            "AddressDefinition": "string"
         },
         "DestinationPort": "string",
         "Protocols": [ "string" ],
         "SourceAddress": {
            "AddressDefinition": "string"
         },
         "SourcePort": "string"
      }
   ],
   "MinimumFlowAgeInSeconds": number,
   "VpcEndpointAssociationArn": "string",
   "VpcEndpointId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZone

The ID of the Availability Zone where the firewall is located. For example, `us-east-2a`.

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: String

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FlowFilters

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: Array of FlowFilter objects

Required: Yes

MinimumFlowAgeInSeconds

The reqested `FlowOperation` ignores flows with an age (in seconds) lower than `MinimumFlowAgeInSeconds`. You provide this for start commands.

Type: Integer

Required: No

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

VpcEndpointId

A unique identifier for the primary endpoint associated with a firewall.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Pattern: `^vpce-[a-zA-Z0-9]*$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FlowOperationId": "string",
   "FlowOperationStatus": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

FlowOperationStatus

Returns the status of the flow operation. This string is returned in the responses to start, list, and describe commands.

If the status is `COMPLETED_WITH_ERRORS`, results may be returned with any number of `Flows` missing from the response. If the status is `FAILED`, `Flows` returned will be empty.

Type: String

Valid Values: `COMPLETED | IN_PROGRESS | FAILED | COMPLETED_WITH_ERRORS`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

Adds the specified tags to the specified resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

You can tag the AWS resources that you manage through AWS Network Firewall: firewalls, firewall policies, and rule groups.

Request Syntax

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

ResourceArn

The Amazon Resource Name (ARN) of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Tags

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

Removes the tags with the specified keys from the specified resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

You can manage tags for the AWS resources that you manage through AWS Network Firewall: firewalls, firewall policies, and rule groups.

Request Syntax

```
{
   "ResourceArn": "string",
   "TagKeys": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

ResourceArn

The Amazon Resource Name (ARN) of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

TagKeys

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^.*$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateAvailabilityZoneChangeProtection

Modifies the `AvailabilityZoneChangeProtection` setting for a transit gateway-attached firewall. When enabled, this setting prevents accidental changes to the firewall's Availability Zone configuration. This helps protect against disrupting traffic flow in production environments.

When enabled, you must disable this protection before using AssociateAvailabilityZones or DisassociateAvailabilityZones to modify the firewall's Availability Zone configuration.

Request Syntax

```
{
   "AvailabilityZoneChangeProtection": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AvailabilityZoneChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

Required: Yes

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "AvailabilityZoneChangeProtection": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AvailabilityZoneChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallAnalysisSettings

Enables specific types of firewall analysis on a specific firewall you define.

Request Syntax

```
{
   "EnabledAnalysisTypes": [ "string" ],
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

EnabledAnalysisTypes

An optional setting indicating the specific traffic analysis types to enable on the firewall.

Type: Array of strings

Valid Values: `TLS_SNI | HTTP_HOST`

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
```

```
    "EnabledAnalysisTypes": [ "string" ],
    "FirewallArn": "string",
    "FirewallName": "string",
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EnabledAnalysisTypes

An optional setting indicating the specific traffic analysis types to enable on the firewall.

Type: Array of strings

Valid Values: `TLS_SNI | HTTP_HOST`

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallDeleteProtection

Modifies the flag, `DeleteProtection`, which indicates whether it is possible to delete the firewall. If the flag is set to TRUE, the firewall is protected against deletion. This setting helps protect against accidentally deleting a firewall that's in use.

Request Syntax

```
{
   "DeleteProtection": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

DeleteProtection

A flag indicating whether it is possible to delete the firewall. A setting of TRUE indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to TRUE.

Type: Boolean

Required: Yes

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "DeleteProtection": boolean,
```

```
    "FirewallArn": "string",
    "FirewallName": "string",
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

DeleteProtection

A flag indicating whether it is possible to delete the firewall. A setting of TRUE indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to TRUE.

Type: Boolean

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallDescription

Modifies the description for the specified firewall. Use the description to help you identify the firewall when you're working with it.

Request Syntax

```
{
   "Description": "string",
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Description

The new description for the firewall. If you omit this setting, Network Firewall removes the description for the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "Description": "string",
```

```
    "FirewallArn": "string",
    "FirewallName": "string",
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Description

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallEncryptionConfiguration

A complex type that contains settings for encryption of your firewall resources.

Request Syntax

```
{
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

EncryptionConfiguration

A complex type that contains optional AWS Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an AWS owned key that AWS owns and manages for you. You can use either the AWS owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see Encryption at rest with AWS Key Managment Service in the *Network Firewall Developer Guide*.

Type: EncryptionConfiguration object

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
```

```
    "EncryptionConfiguration": {
       "KeyId": "string",
       "Type": "string"
    },
    "FirewallArn": "string",
    "FirewallName": "string",
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EncryptionConfiguration

A complex type that contains optional AWS Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an AWS owned key that AWS owns and manages for you. You can use either the AWS owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see Encryption at rest with AWS Key Managment Service in the *Network Firewall Developer Guide*.

Type: EncryptionConfiguration object

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.

- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallPolicy

Updates the properties of the specified firewall policy.

Request Syntax

```
{
   "Description": "string",
   "DryRun": boolean,
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "FirewallPolicy": {
      "PolicyVariables": {
         "RuleVariables": {
            "string" : {
               "Definition": [ "string" ]
            }
         }
      },
      "StatefulDefaultActions": [ "string" ],
      "StatefulEngineOptions": {
         "FlowTimeouts": {
            "TcpIdleTimeoutSeconds": number
         },
         "RuleOrder": "string",
         "StreamExceptionPolicy": "string"
      },
      "StatefulRuleGroupReferences": [
         {
            "DeepThreatInspection": boolean,
            "Override": {
               "Action": "string"
            },
            "Priority": number,
            "ResourceArn": "string"
         }
      ],
      "StatelessCustomActions": [
         {
            "ActionDefinition": {
               "PublishMetricAction": {
```

```
                    "Dimensions": [
                       {
                          "Value": "string"
                       }
                    ]
                 }
              },
              "ActionName": "string"
           }
        ],
        "StatelessDefaultActions": [ "string" ],
        "StatelessFragmentDefaultActions": [ "string" ],
        "StatelessRuleGroupReferences": [
           {
              "Priority": number,
              "ResourceArn": "string"
           }
        ],
        "TLSInspectionConfigurationArn": "string"
    },
    "FirewallPolicyArn": "string",
    "FirewallPolicyName": "string",
    "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Description

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to `TRUE`, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to `FALSE`, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to `FALSE`, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

EncryptionConfiguration

A complex type that contains settings for encryption of your firewall policy resources.

Type: EncryptionConfiguration object

Required: No

FirewallPolicy

The updated firewall policy to use for the firewall. You can't add or remove a TLSInspectionConfiguration after you create a firewall policy. However, you can replace an existing TLS inspection configuration with another `TLSInspectionConfiguration`.

Type: FirewallPolicy object

Required: Yes

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallPolicyName

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

Response Syntax

```
{
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
```

```
        "ConsumedStatelessRuleCapacity": number,
        "Description": "string",
        "EncryptionConfiguration": {
           "KeyId": "string",
           "Type": "string"
        },
        "FirewallPolicyArn": "string",
        "FirewallPolicyId": "string",
        "FirewallPolicyName": "string",
        "FirewallPolicyStatus": "string",
        "LastModifiedTime": number,
        "NumberOfAssociations": number,
        "Tags": [
           {
              "Key": "string",
              "Value": "string"
           }
        ]
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicyResponse

The high-level properties of a firewall policy. This, along with the FirewallPolicy, define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy.

Type: FirewallPolicyResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the

operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallPolicyChangeProtection

Modifies the flag, `ChangeProtection`, which indicates whether it is possible to change the firewall. If the flag is set to TRUE, the firewall is protected from changes. This setting helps protect against accidentally changing a firewall that's in use.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyChangeProtection": boolean,
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

FirewallPolicyChangeProtection

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

Required: Yes

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
```

```
    "FirewallArn": "string",
    "FirewallName": "string",
    "FirewallPolicyChangeProtection": boolean,
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

FirewallPolicyChangeProtection

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateLoggingConfiguration

Sets the logging configuration for the specified firewall.

To change the logging configuration, retrieve the LoggingConfiguration by calling DescribeLoggingConfiguration, then change it and provide the modified object to this update call. You must change the logging configuration one LogDestinationConfig at a time inside the retrieved LoggingConfiguration object.

You can perform only one of the following actions in any call to `UpdateLoggingConfiguration`:

- Create a new log destination object by adding a single `LogDestinationConfig` array element to `LogDestinationConfigs`.
- Delete a log destination object by removing a single `LogDestinationConfig` array element from `LogDestinationConfigs`.
- Change the `LogDestination` setting in a single `LogDestinationConfig` array element.

You can't change the `LogDestinationType` or `LogType` in a `LogDestinationConfig`. To change these settings, delete the existing `LogDestinationConfig` object and create a new one, using two separate calls to this update operation.

Request Syntax

```
{
   "EnableMonitoringDashboard": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "LoggingConfiguration": {
      "LogDestinationConfigs": [
         {
            "LogDestination": {
               "string" : "string"
            },
            "LogDestinationType": "string",
            "LogType": "string"
         }
      ]
   }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

EnableMonitoringDashboard

A boolean that lets you enable or disable the detailed firewall monitoring dashboard on the firewall.

The monitoring dashboard provides comprehensive visibility into your firewall's flow logs and alert logs. After you enable detailed monitoring, you can access these dashboards directly from the **Monitoring** page of the Network Firewall console.

Specify `TRUE` to enable the the detailed monitoring dashboard on the firewall. Specify `FALSE` to disable the the detailed monitoring dashboard on the firewall.

Type: Boolean

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: ^[a-zA-Z0-9-]+$

Required: No

LoggingConfiguration

Defines how Network Firewall performs logging for a firewall. If you omit this setting, Network Firewall disables logging for the firewall.

Type: LoggingConfiguration object

Required: No

Response Syntax

```
{
   "EnableMonitoringDashboard": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "LoggingConfiguration": {
      "LogDestinationConfigs": [
         {
            "LogDestination": {
               "string" : "string"
            },
            "LogDestinationType": "string",
            "LogType": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EnableMonitoringDashboard

A boolean that reflects whether or not the firewall monitoring dashboard is enabled on a firewall.

Returns TRUE when the firewall monitoring dashboard is enabled on the firewall. Returns FALSE when the firewall monitoring dashboard is not enabled on the firewall.

Type: Boolean

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

LoggingConfiguration

Defines how AWS Network Firewall performs logging for a Firewall.

Type: LoggingConfiguration object

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

LogDestinationPermissionException

Unable to send logs to a configured logging destination.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRuleGroup

Updates the rule settings for the specified rule group. You use a rule group by reference in one or more firewall policies. When you modify a rule group, you modify all firewall policies that use the rule group.

To update a rule group, first call DescribeRuleGroup to retrieve the current RuleGroup object, update the object as needed, and then provide the updated object to this call.

Request Syntax

```
{
   "AnalyzeRuleGroup": boolean,
   "Description": "string",
   "DryRun": boolean,
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "RuleGroup": {
      "ReferenceSets": {
         "IPSetReferences": {
            "string" : {
               "ReferenceArn": "string"
            }
         }
      },
      "RulesSource": {
         "RulesSourceList": {
            "GeneratedRulesType": "string",
            "Targets": [ "string" ],
            "TargetTypes": [ "string" ]
         },
         "RulesString": "string",
         "StatefulRules": [
            {
               "Action": "string",
               "Header": {
                  "Destination": "string",
                  "DestinationPort": "string",
                  "Direction": "string",
                  "Protocol": "string",
```

```
                "Source": "string",
                "SourcePort": "string"
            },
            "RuleOptions": [
                {
                    "Keyword": "string",
                    "Settings": [ "string" ]
                }
            ]
        }
    ],
    "StatelessRulesAndCustomActions": {
        "CustomActions": [
            {
                "ActionDefinition": {
                    "PublishMetricAction": {
                        "Dimensions": [
                            {
                                "Value": "string"
                            }
                        ]
                    }
                },
                "ActionName": "string"
            }
        ],
        "StatelessRules": [
            {
                "Priority": number,
                "RuleDefinition": {
                    "Actions": [ "string" ],
                    "MatchAttributes": {
                        "DestinationPorts": [
                            {
                                "FromPort": number,
                                "ToPort": number
                            }
                        ],
                        "Destinations": [
                            {
                                "AddressDefinition": "string"
                            }
                        ],
                        "Protocols": [ number ],
```

```
                        "SourcePorts": [
                           {
                              "FromPort": number,
                              "ToPort": number
                           }
                        ],
                        "Sources": [
                           {
                              "AddressDefinition": "string"
                           }
                        ],
                        "TCPFlags": [
                           {
                              "Flags": [ "string" ],
                              "Masks": [ "string" ]
                           }
                        ]
                     }
                  }
               }
            ]
         }
      },
      "RuleVariables": {
         "IPSets": {
            "string" : {
               "Definition": [ "string" ]
            }
         },
         "PortSets": {
            "string" : {
               "Definition": [ "string" ]
            }
         }
      },
      "StatefulRuleOptions": {
         "RuleOrder": "string"
      }
   },
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Rules": "string",
   "SourceMetadata": {
      "SourceArn": "string",
```

```
        "SourceUpdateToken": "string"
    },
    "SummaryConfiguration": {
        "RuleOptions": [ "string" ]
    },
    "Type": "string",
    "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

AnalyzeRuleGroup

Indicates whether you want Network Firewall to analyze the stateless rules in the rule group for rule behavior such as asymmetric routing. If set to TRUE, Network Firewall runs the analysis and then updates the rule group for you. To run the stateless rule group analyzer without updating the rule group, set `DryRun` to TRUE.

Type: Boolean

Required: No

Description

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to TRUE, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to FALSE, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to FALSE, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

EncryptionConfiguration

A complex type that contains settings for encryption of your rule group resources.

Type: EncryptionConfiguration object

Required: No

RuleGroup

An object that defines the rule group rules.

> **Note**
>
> You must provide either this rule group setting or a `Rules` setting, but not both.

Type: RuleGroup object

Required: No

RuleGroupArn

The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Rules

A string containing stateful rule group rules specifications in Suricata flat format, with one rule per line. Use this to import your existing Suricata compatible rule groups.

> **Note**
>
> You must provide either this rules setting or a populated `RuleGroup` setting, but not both.

You can provide your rule group specification in Suricata flat format through this setting when you create or update your rule group. The call response returns a RuleGroup object that Network Firewall has populated from your string.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000000.

Required: No

SourceMetadata

A complex type that contains metadata about the rule group that your own rule group is copied from. You can use the metadata to keep track of updates made to the originating rule group.

Type: SourceMetadata object

Required: No

SummaryConfiguration

Updates the selected summary configuration for a rule group.

Changes affect subsequent responses from DescribeRuleGroupSummary.

Type: SummaryConfiguration object

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

> **Note**
>
> This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS` | `STATEFUL`

Required: No

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

Response Syntax

```
{
   "RuleGroupResponse": {
      "AnalysisResults": [
         {
            "AnalysisDetail": "string",
            "IdentifiedRuleIds": [ "string" ],
            "IdentifiedType": "string"
         }
      ],
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
      "EncryptionConfiguration": {
         "KeyId": "string",
         "Type": "string"
      },
      "LastModifiedTime": number,
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "RuleGroupStatus": "string",
      "SnsTopic": "string",
      "SourceMetadata": {
         "SourceArn": "string",
         "SourceUpdateToken": "string"
      },
      "SummaryConfiguration": {
         "RuleOptions": [ "string" ]
      },
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
```

```
        ],
        "Type": "string"
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroupResponse

The high-level properties of a rule group. This, along with the RuleGroup, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Type: RuleGroupResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateSubnetChangeProtection

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetChangeProtection": boolean,
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

SubnetChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

Required: Yes

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
```

```
    "SubnetChangeProtection": boolean,
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

SubnetChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

UpdateToken

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateTLSInspectionConfiguration

Updates the TLS inspection configuration settings for the specified TLS inspection configuration. You use a TLS inspection configuration by referencing it in one or more firewall policies. When you modify a TLS inspection configuration, you modify all firewall policies that use the TLS inspection configuration.

To update a TLS inspection configuration, first call DescribeTLSInspectionConfiguration to retrieve the current TLSInspectionConfiguration object, update the object as needed, and then provide the updated object to this call.

Request Syntax

```
{
   "Description": "string",
   "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
   },
   "TLSInspectionConfiguration": {
      "ServerCertificateConfigurations": [
         {
            "CertificateAuthorityArn": "string",
            "CheckCertificateRevocationStatus": {
               "RevokedStatusAction": "string",
               "UnknownStatusAction": "string"
            },
            "Scopes": [
               {
                  "DestinationPorts": [
                     {
                        "FromPort": number,
                        "ToPort": number
                     }
                  ],
                  "Destinations": [
                     {
                        "AddressDefinition": "string"
                     }
                  ],
                  "Protocols": [ number ],
                  "SourcePorts": [
```

```
                        {
                           "FromPort": number,
                           "ToPort": number
                        }
                     ],
                     "Sources": [
                        {
                           "AddressDefinition": "string"
                        }
                     ]
                  }
               ],
               "ServerCertificates": [
                  {
                     "ResourceArn": "string"
                  }
               ]
            }
         ]
      },
      "TLSInspectionConfigurationArn": "string",
      "TLSInspectionConfigurationName": "string",
      "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

Description

A description of the TLS inspection configuration.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EncryptionConfiguration

A complex type that contains the AWS KMS encryption configuration settings for your TLS inspection configuration.

Type: EncryptionConfiguration object

Required: No

TLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with TLSInspectionConfigurationResponse, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

AWS Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see Inspecting SSL/TLS traffic with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

Type: TLSInspectionConfiguration object

Required: Yes

TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

TLSInspectionConfigurationName

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the TLS inspection configuration. The token marks the state of the TLS inspection configuration resource at the time of the request.

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

Response Syntax

```
{
   "TLSInspectionConfigurationResponse": {
      "CertificateAuthority": {
         "CertificateArn": "string",
         "CertificateSerial": "string",
```

```
            "Status": "string",
            "StatusMessage": "string"
        },
        "Certificates": [
            {
                "CertificateArn": "string",
                "CertificateSerial": "string",
                "Status": "string",
                "StatusMessage": "string"
            }
        ],
        "Description": "string",
        "EncryptionConfiguration": {
            "KeyId": "string",
            "Type": "string"
        },
        "LastModifiedTime": number,
        "NumberOfAssociations": number,
        "Tags": [
            {
                "Key": "string",
                "Value": "string"
            }
        ],
        "TLSInspectionConfigurationArn": "string",
        "TLSInspectionConfigurationId": "string",
        "TLSInspectionConfigurationName": "string",
        "TLSInspectionConfigurationStatus": "string"
    },
    "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the TLSInspectionConfiguration, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

Type: TLSInspectionConfigurationResponse object

UpdateToken

A token used for optimistic locking. Network Firewall returns a token to your requests that access the TLS inspection configuration. The token marks the state of the TLS inspection configuration resource at the time of the request.

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors.

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The AWS Network Firewall API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
>
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- ActionDefinition
- Address
- AnalysisReport
- AnalysisResult
- AnalysisTypeReportResult
- Attachment
- AvailabilityZoneMapping
- AvailabilityZoneMetadata
- AZSyncState
- CapacityUsageSummary
- CheckCertificateRevocationStatusActions
- CIDRSummary
- CustomAction
- Dimension
- EncryptionConfiguration
- Firewall
- FirewallMetadata
- FirewallPolicy
- FirewallPolicyMetadata
- FirewallPolicyResponse

- FirewallStatus
- Flow
- FlowFilter
- FlowOperation
- FlowOperationMetadata
- FlowTimeouts
- Header
- Hits
- IPSet
- IPSetMetadata
- IPSetReference
- LogDestinationConfig
- LoggingConfiguration
- MatchAttributes
- PerObjectStatus
- PolicyVariables
- PortRange
- PortSet
- PublishMetricAction
- ReferenceSets
- RuleDefinition
- RuleGroup
- RuleGroupMetadata
- RuleGroupResponse
- RuleOption
- RulesSource
- RulesSourceList
- RuleSummary
- RuleVariables
- ServerCertificate

- ServerCertificateConfiguration
- ServerCertificateScope
- SourceMetadata
- StatefulEngineOptions
- StatefulRule
- StatefulRuleGroupOverride
- StatefulRuleGroupReference
- StatefulRuleOptions
- StatelessRule
- StatelessRuleGroupReference
- StatelessRulesAndCustomActions
- SubnetMapping
- Summary
- SummaryConfiguration
- SyncState
- Tag
- TCPFlagField
- TlsCertificateData
- TLSInspectionConfiguration
- TLSInspectionConfigurationMetadata
- TLSInspectionConfigurationResponse
- TransitGatewayAttachmentSyncState
- UniqueSources
- VpcEndpointAssociation
- VpcEndpointAssociationMetadata
- VpcEndpointAssociationStatus

ActionDefinition

A custom action to use in stateless rule actions settings. This is used in CustomAction.

Contents

PublishMetricAction

Stateless inspection criteria that publishes the specified metrics to Amazon CloudWatch for the matching packet. This setting defines a CloudWatch dimension value to be published.

You can pair this custom action with any of the standard stateless rule actions. For example, you could pair this in a rule action with the standard action that forwards the packet for stateful inspection. Then, when a packet matches the rule, Network Firewall publishes metrics for the packet and forwards it.

Type: PublishMetricAction object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Address

A single IP address specification. This is used in the MatchAttributes source and destination specifications.

Contents

AddressDefinition

Specify an IP address or a block of IP addresses in Classless Inter-Domain Routing (CIDR) notation. Network Firewall supports all address ranges for IPv4 and IPv6.

Examples:

- To configure Network Firewall to inspect for the IP address 192.0.2.44, specify `192.0.2.44/32`.
- To configure Network Firewall to inspect for IP addresses from 192.0.2.0 to 192.0.2.255, specify `192.0.2.0/24`.
- To configure Network Firewall to inspect for the IP address 1111:0000:0000:0000:0000:0000:0000:0111, specify `1111:0000:0000:0000:0000:0000:0000:0111/128`.
- To configure Network Firewall to inspect for IP addresses from 1111:0000:0000:0000:0000:0000:0000:0000 to 1111:0000:0000:0000:ffff:ffff:ffff:ffff, specify `1111:0000:0000:0000:0000:0000:0000:0000/64`.

For more information about CIDR notation, see the Wikipedia entry Classless Inter-Domain Routing.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `^([a-fA-F\d:\.]+($|/\d{1,3}))$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AnalysisReport

A report that captures key activity from the last 30 days of network traffic monitored by your firewall.

You can generate up to one report per traffic type, per 30 day period. For example, when you successfully create an HTTP traffic report, you cannot create another HTTP traffic report until 30 days pass. Alternatively, if you generate a report that combines metrics on both HTTP and HTTPS traffic, you cannot create another report for either traffic type until 30 days pass.

Contents

AnalysisReportId

The unique ID of the query that ran when you requested an analysis report.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `\S+`

Required: No

AnalysisType

The type of traffic that will be used to generate a report.

Type: String

Valid Values: `TLS_SNI | HTTP_HOST`

Required: No

ReportTime

The date and time the analysis report was ran.

Type: Timestamp

Required: No

Status

The status of the analysis report you specify. Statuses include `RUNNING`, `COMPLETED`, or `FAILED`.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AnalysisResult

The analysis result for Network Firewall's stateless rule group analyzer. Every time you call CreateRuleGroup, UpdateRuleGroup, or DescribeRuleGroup on a stateless rule group, Network Firewall analyzes the stateless rule groups in your account and identifies the rules that might adversely effect your firewall's functionality. For example, if Network Firewall detects a rule that's routing traffic asymmetrically, which impacts the service's ability to properly process traffic, the service includes the rule in a list of analysis results.

The `AnalysisResult` data type is not related to traffic analysis reports you generate using StartAnalysisReport. For information on traffic analysis report results, see AnalysisTypeReportResult.

Contents

AnalysisDetail

Provides analysis details for the identified rule.

Type: String

Required: No

IdentifiedRuleIds

The priority number of the stateless rules identified in the analysis.

Type: Array of strings

Required: No

IdentifiedType

The types of rule configurations that Network Firewall analyzes your rule groups for. Network Firewall analyzes stateless rule groups for the following types of rule configurations:

- `STATELESS_RULE_FORWARDING_ASYMMETRICALLY`

  Cause: One or more stateless rules with the action `pass` or `forward` are forwarding traffic asymmetrically. Specifically, the rule's set of source IP addresses or their associated port numbers, don't match the set of destination IP addresses or their associated port numbers.

To mitigate: Make sure that there's an existing return path. For example, if the rule allows traffic from source 10.1.0.0/24 to destination 20.1.0.0/24, you should allow return traffic from source 20.1.0.0/24 to destination 10.1.0.0/24.

- `STATELESS_RULE_CONTAINS_TCP_FLAGS`

  Cause: At least one stateless rule with the action `pass` or`forward` contains TCP flags that are inconsistent in the forward and return directions.

  To mitigate: Prevent asymmetric routing issues caused by TCP flags by following these actions:

  - Remove unnecessary TCP flag inspections from the rules.
  - If you need to inspect TCP flags, check that the rules correctly account for changes in TCP flags throughout the TCP connection cycle, for example `SYN` and `ACK` flags used in a 3-way TCP handshake.

Type: String

Valid Values: `STATELESS_RULE_FORWARDING_ASYMMETRICALLY` | `STATELESS_RULE_CONTAINS_TCP_FLAGS`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AnalysisTypeReportResult

The results of a `COMPLETED` analysis report generated with StartAnalysisReport.

For an example of traffic analysis report results, see the response syntax of GetAnalysisReportResults.

Contents

Domain

The most frequently accessed domains.

Type: String

Required: No

FirstAccessed

The date and time any domain was first accessed (within the last 30 day period).

Type: Timestamp

Required: No

Hits

The number of attempts made to access a observed domain.

Type: Hits object

Required: No

LastAccessed

The date and time any domain was last accessed (within the last 30 day period).

Type: Timestamp

Required: No

Protocol

The type of traffic captured by the analysis report.

Type: String

Required: No

UniqueSources

The number of unique source IP addresses that connected to a domain.

Type: UniqueSources object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Attachment

The definition and status of the firewall endpoint for a single subnet. In each configured subnet, Network Firewall instantiates a firewall endpoint to handle network traffic.

This data type is used for any firewall endpoint type:

- For `Firewall.SubnetMappings`, this `Attachment` is part of the `FirewallStatus` sync states information. You define firewall subnets using `CreateFirewall` and `AssociateSubnets`.
- For `VpcEndpointAssociation`, this `Attachment` is part of the `VpcEndpointAssociationStatus` sync states information. You define these subnets using `CreateVpcEndpointAssociation`.

Contents

EndpointId

The identifier of the firewall endpoint that Network Firewall has instantiated in the subnet. You use this to identify the firewall endpoint in the VPC route tables, when you redirect the VPC traffic through the endpoint.

Type: String

Required: No

Status

The current status of the firewall endpoint instantiation in the subnet.

When this value is `READY`, the endpoint is available to handle network traffic. Otherwise, this value reflects its state, for example `CREATING` or `DELETING`.

Type: String

Valid Values: `CREATING | DELETING | FAILED | ERROR | SCALING | READY`

Required: No

StatusMessage

If Network Firewall fails to create or delete the firewall endpoint in the subnet, it populates this with the reason for the error or failure and how to resolve it. A `FAILED` status indicates a

non-recoverable state, and a ERROR status indicates an issue that you can fix. Depending on the error, it can take as many as 15 minutes to populate this field. For more information about the causes for failiure or errors and solutions available for this field, see Troubleshooting firewall endpoint failures in the *Network Firewall Developer Guide*.

Type: String

Required: No

SubnetId

The unique identifier of the subnet that you've specified to be used for a firewall endpoint.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^subnet-[0-9a-f]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AvailabilityZoneMapping

Defines the mapping between an Availability Zone and a firewall endpoint for a transit gateway-attached firewall. Each mapping represents where the firewall can process traffic. You use these mappings when calling CreateFirewall, AssociateAvailabilityZones, and DisassociateAvailabilityZones.

To retrieve the current Availability Zone mappings for a firewall, use DescribeFirewall.

Contents

AvailabilityZone

The ID of the Availability Zone where the firewall endpoint is located. For example, `us-east-2a`. The Availability Zone must be in the same Region as the transit gateway.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `\S+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AvailabilityZoneMetadata

High-level information about an Availability Zone where the firewall has an endpoint defined.

Contents

IPAddressType

The IP address type of the Firewall subnet in the Availability Zone. You can't change the IP address type after you create the subnet.

Type: String

Valid Values: `DUALSTACK | IPV4 | IPV6`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AZSyncState

The status of the firewall endpoint defined by a `VpcEndpointAssociation`.

Contents

Attachment

The definition and status of the firewall endpoint for a single subnet. In each configured subnet, Network Firewall instantiates a firewall endpoint to handle network traffic.

This data type is used for any firewall endpoint type:

- For `Firewall.SubnetMappings`, this `Attachment` is part of the `FirewallStatus` sync states information. You define firewall subnets using `CreateFirewall` and `AssociateSubnets`.
- For `VpcEndpointAssociation`, this `Attachment` is part of the `VpcEndpointAssociationStatus` sync states information. You define these subnets using `CreateVpcEndpointAssociation`.

Type: Attachment object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CapacityUsageSummary

The capacity usage summary of the resources used by the ReferenceSets in a firewall.

Contents

CIDRs

Describes the capacity usage of the CIDR blocks used by the IP set references in a firewall.

Type: CIDRSummary object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CheckCertificateRevocationStatusActions

Defines the actions to take on the SSL/TLS connection if the certificate presented by the server in the connection has a revoked or unknown status.

Contents

RevokedStatusAction

Configures how Network Firewall processes traffic when it determines that the certificate presented by the server in the SSL/TLS connection has a revoked status.

- **PASS** - Allow the connection to continue, and pass subsequent packets to the stateful engine for inspection.
- **DROP** - Network Firewall closes the connection and drops subsequent packets for that connection.
- **REJECT** - Network Firewall sends a TCP reject packet back to your client. The service closes the connection and drops subsequent packets for that connection. `REJECT` is available only for TCP traffic.

Type: String

Valid Values: `PASS | DROP | REJECT`

Required: No

UnknownStatusAction

Configures how Network Firewall processes traffic when it determines that the certificate presented by the server in the SSL/TLS connection has an unknown status, or a status that cannot be determined for any other reason, including when the service is unable to connect to the OCSP and CRL endpoints for the certificate.

- **PASS** - Allow the connection to continue, and pass subsequent packets to the stateful engine for inspection.
- **DROP** - Network Firewall closes the connection and drops subsequent packets for that connection.
- **REJECT** - Network Firewall sends a TCP reject packet back to your client. The service closes the connection and drops subsequent packets for that connection. `REJECT` is available only for TCP traffic.

Type: String

Valid Values: `PASS | DROP | REJECT`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CIDRSummary

Summarizes the CIDR blocks used by the IP set references in a firewall. Network Firewall calculates the number of CIDRs by taking an aggregated count of all CIDRs used by the IP sets you are referencing.

Contents

AvailableCIDRCount

The number of CIDR blocks available for use by the IP set references in a firewall.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 1000000.

Required: No

IPSetReferences

The list of the IP set references used by a firewall.

Type: String to IPSetMetadata object map

Required: No

UtilizedCIDRCount

The number of CIDR blocks used by the IP set references in a firewall.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 1000000.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

CustomAction

An optional, non-standard action to use for stateless packet handling. You can define this in addition to the standard action that you must specify.

You define and name the custom actions that you want to be able to use, and then you reference them by name in your actions settings.

You can use custom actions in the following places:

- In a rule group's StatelessRulesAndCustomActions specification. The custom actions are available for use by name inside the `StatelessRulesAndCustomActions` where you define them. You can use them for your stateless rule actions to specify what to do with a packet that matches the rule's match attributes.
- In a FirewallPolicy specification, in `StatelessCustomActions`. The custom actions are available for use inside the policy where you define them. You can use them for the policy's default stateless actions settings to specify what to do with packets that don't match any of the policy's stateless rules.

Contents

ActionDefinition

The custom action associated with the action name.

Type: ActionDefinition object

Required: Yes

ActionName

The descriptive name of the custom action. You can't change the name of a custom action after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9]+$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Dimension

The value to use in an Amazon CloudWatch custom metric dimension. This is used in the `PublishMetrics` CustomAction. A CloudWatch custom metric dimension is a name/value pair that's part of the identity of a metric.

AWS Network Firewall sets the dimension name to `CustomAction` and you provide the dimension value.

For more information about CloudWatch custom metric dimensions, see Publishing Custom Metrics in the Amazon CloudWatch User Guide.

Contents

Value

The value to use in the custom metric dimension.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-_ ]+$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EncryptionConfiguration

A complex type that contains optional AWS Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an AWS owned key that AWS owns and manages for you. You can use either the AWS owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see Encryption at rest with AWS Key Managment Service in the *Network Firewall Developer Guide*.

Contents

Type

The type of AWS KMS key to use for encryption of your Network Firewall resources.

Type: String

Valid Values: `CUSTOMER_KMS | AWS_OWNED_KMS_KEY`

Required: Yes

KeyId

The ID of the AWS Key Management Service (KMS) customer managed key. You can use any of the key identifiers that KMS supports, unless you're using a key that's managed by another account. If you're using a key managed by another account, then specify the key ARN. For more information, see Key ID in the *AWS KMS Developer Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.*\S.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

Firewall

A firewall defines the behavior of a firewall, the main VPC where the firewall is used, the Availability Zones where the firewall can be used, and one subnet to use for a firewall endpoint within each of the Availability Zones. The Availability Zones are defined implicitly in the subnet specifications.

In addition to the firewall endpoints that you define in this `Firewall` specification, you can create firewall endpoints in `VpcEndpointAssociation` resources for any VPC, in any Availability Zone where the firewall is already in use.

The status of the firewall, for example whether it's ready to filter network traffic, is provided in the corresponding FirewallStatus. You can retrieve both the firewall and firewall status by calling DescribeFirewall.

Contents

FirewallId

The unique identifier for the firewall.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

The relationship of firewall to firewall policy is many to one. Each firewall requires one firewall policy association, and you can use the same firewall policy for multiple firewalls.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

SubnetMappings

The primary public subnets that Network Firewall is using for the firewall. Network Firewall creates a firewall endpoint in each subnet. Create a subnet mapping for each Availability Zone where you want to use the firewall.

These subnets are all defined for a single, primary VPC, and each must belong to a different Availability Zone. Each of these subnets establishes the availability of the firewall in its Availability Zone.

In addition to these subnets, you can define other endpoints for the firewall in `VpcEndpointAssociation` resources. You can define these additional endpoints for any VPC, and for any of the Availability Zones where the firewall resource already has a subnet mapping. VPC endpoint associations give you the ability to protect multiple VPCs using a single firewall, and to define multiple firewall endpoints for a VPC in a single Availability Zone.

Type: Array of SubnetMapping objects

Required: Yes

VpcId

The unique identifier of the VPC where the firewall is in use.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: Yes

AvailabilityZoneChangeProtection

A setting indicating whether the firewall is protected against changes to its Availability Zone configuration. When set to `TRUE`, you must first disable this protection before adding or removing Availability Zones.

Type: Boolean

Required: No

AvailabilityZoneMappings

The Availability Zones where the firewall endpoints are created for a transit gateway-attached firewall. Each mapping specifies an Availability Zone where the firewall processes traffic.

Type: Array of AvailabilityZoneMapping objects

Required: No

DeleteProtection

A flag indicating whether it is possible to delete the firewall. A setting of `TRUE` indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to `TRUE`.

Type: Boolean

Required: No

Description

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EnabledAnalysisTypes

An optional setting indicating the specific traffic analysis types to enable on the firewall.

Type: Array of strings

Valid Values: `TLS_SNI | HTTP_HOST`

Required: No

EncryptionConfiguration

A complex type that contains the AWS KMS encryption configuration settings for your firewall.

Type: EncryptionConfiguration object

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

FirewallPolicyChangeProtection

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: No

NumberOfAssociations

The number of `VpcEndpointAssociation` resources that use this firewall.

Type: Integer

Required: No

SubnetChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to TRUE.

Type: Boolean

Required: No

Tags

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

TransitGatewayId

The unique identifier of the transit gateway associated with this firewall. This field is only present for transit gateway-attached firewalls.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-[0-9a-z]+$`

Required: No

TransitGatewayOwnerAccountId

The AWS account ID that owns the transit gateway. This may be different from the firewall owner's account ID when using a shared transit gateway.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallMetadata

High-level information about a firewall, returned by operations like create and describe. You can use the information provided in the metadata to retrieve and manage a firewall.

Contents

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

TransitGatewayAttachmentId

The unique identifier of the transit gateway attachment associated with this firewall. This field is only present for transit gateway-attached firewalls.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^tgw-attach-[0-9a-z]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallPolicy

The firewall policy defines the behavior of a firewall using a collection of stateless and stateful rule groups and other settings. You can use one firewall policy for multiple firewalls.

This, along with FirewallPolicyResponse, define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy.

Contents

StatelessDefaultActions

The actions to take on a packet if it doesn't match any of the stateless rules in the policy. If you want non-matching packets to be forwarded for stateful inspection, specify `aws:forward_to_sfe`.

You must specify one of the standard actions: `aws:pass`, `aws:drop`, or `aws:forward_to_sfe`. In addition, you can specify custom actions that are compatible with your standard section choice.

For example, you could specify `["aws:pass"]` or you could specify `["aws:pass", “customActionName”]`. For information about compatibility, see the custom action descriptions under CustomAction.

Type: Array of strings

Required: Yes

StatelessFragmentDefaultActions

The actions to take on a fragmented UDP packet if it doesn't match any of the stateless rules in the policy. Network Firewall only manages UDP packet fragments and silently drops packet fragments for other protocols. If you want non-matching fragmented UDP packets to be forwarded for stateful inspection, specify `aws:forward_to_sfe`.

You must specify one of the standard actions: `aws:pass`, `aws:drop`, or `aws:forward_to_sfe`. In addition, you can specify custom actions that are compatible with your standard section choice.

For example, you could specify `["aws:pass"]` or you could specify `["aws:pass", “customActionName”]`. For information about compatibility, see the custom action descriptions under CustomAction.

Type: Array of strings

Required: Yes

PolicyVariables

Contains variables that you can use to override default Suricata settings in your firewall policy.

Type: PolicyVariables object

Required: No

StatefulDefaultActions

The default actions to take on a packet that doesn't match any stateful rules. The stateful default action is optional, and is only valid when using the strict rule order.

Valid values of the stateful default action:

- aws:drop_strict
- aws:drop_established
- aws:alert_strict
- aws:alert_established

For more information, see Strict evaluation order in the *AWS Network Firewall Developer Guide*.

Type: Array of strings

Required: No

StatefulEngineOptions

Additional options governing how Network Firewall handles stateful rules. The stateful rule groups that you use in your policy must have stateful rule options settings that are compatible with these settings.

Type: StatefulEngineOptions object

Required: No

StatefulRuleGroupReferences

References to the stateful rule groups that are used in the policy. These define the inspection criteria in stateful rules.

Type: Array of StatefulRuleGroupReference objects

Required: No

StatelessCustomActions

The custom action definitions that are available for use in the firewall policy's `StatelessDefaultActions` setting. You name each custom action that you define, and then you can use it by name in your default actions specifications.

Type: Array of CustomAction objects

Required: No

StatelessRuleGroupReferences

References to the stateless rule groups that are used in the policy. These define the matching criteria in stateless rules.

Type: Array of StatelessRuleGroupReference objects

Required: No

TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallPolicyMetadata

High-level information about a firewall policy, returned by operations like create and describe. You can use the information provided in the metadata to retrieve and manage a firewall policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy.

Contents

Arn

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

Name

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallPolicyResponse

The high-level properties of a firewall policy. This, along with the FirewallPolicy, define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy.

Contents

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

> **Note**
>
> If this response is for a create request that had `DryRun` set to `TRUE`, then this ARN is a placeholder that isn't attached to a valid resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FirewallPolicyId

The unique identifier for the firewall policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

FirewallPolicyName

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

ConsumedStatefulRuleCapacity

The number of capacity units currently consumed by the policy's stateful rules.

Type: Integer

Required: No

ConsumedStatelessRuleCapacity

The number of capacity units currently consumed by the policy's stateless rules.

Type: Integer

Required: No

Description

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EncryptionConfiguration

A complex type that contains the AWS KMS encryption configuration settings for your firewall policy.

Type: EncryptionConfiguration object

Required: No

FirewallPolicyStatus

The current status of the firewall policy. You can retrieve this for a firewall policy by calling DescribeFirewallPolicy and providing the firewall policy's name or ARN.

Type: String

Valid Values: `ACTIVE | DELETING | ERROR`

Required: No

LastModifiedTime

The last time that the firewall policy was changed.

Type: Timestamp

Required: No

NumberOfAssociations

The number of firewalls that are associated with this firewall policy.

Type: Integer

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallStatus

Detailed information about the current status of a Firewall. You can retrieve this for a firewall by calling DescribeFirewall and providing the firewall name and ARN.

The firewall status indicates a combined status. It indicates whether all subnets are up-to-date with the latest firewall configurations, which is based on the sync states config values, and also whether all subnets have their endpoints fully enabled, based on their sync states attachment values.

Contents

ConfigurationSyncStateSummary

The configuration sync state for the firewall. This summarizes the `Config` settings in the `SyncStates` for this firewall status object.

When you create a firewall or update its configuration, for example by adding a rule group to its firewall policy, Network Firewall distributes the configuration changes to all Availability Zones that have subnets defined for the firewall. This summary indicates whether the configuration changes have been applied everywhere.

This status must be `IN_SYNC` for the firewall to be ready for use, but it doesn't indicate that the firewall is ready. The `Status` setting indicates firewall readiness. It's based on this setting and the readiness of the firewall endpoints to take traffic.

Type: String

Valid Values: `PENDING | IN_SYNC | CAPACITY_CONSTRAINED`

Required: Yes

Status

The readiness of the configured firewall to handle network traffic across all of the Availability Zones where you have it configured. This setting is `READY` only when the `ConfigurationSyncStateSummary` value is `IN_SYNC` and the `Attachment Status` values for all of the configured subnets are `READY`.

Type: String

Valid Values: `PROVISIONING | DELETING | READY`

Required: Yes

CapacityUsageSummary

Describes the capacity usage of the resources contained in a firewall's reference sets. Network Firewall calculates the capacity usage by taking an aggregated count of all of the resources used by all of the reference sets in a firewall.

Type: CapacityUsageSummary object

Required: No

SyncStates

Status for the subnets that you've configured in the firewall. This contains one array element per Availability Zone where you've configured a subnet in the firewall.

These objects provide detailed information for the settings `ConfigurationSyncStateSummary` and `Status`.

Type: String to SyncState object map

Required: No

TransitGatewayAttachmentSyncState

The synchronization state of the transit gateway attachment. This indicates whether the firewall's transit gateway configuration is properly synchronized and operational. Use this to verify that your transit gateway configuration changes have been applied.

Type: TransitGatewayAttachmentSyncState object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Flow

Any number of arrays, where each array is a single flow identified in the scope of the operation. If multiple flows were in the scope of the operation, multiple `Flows` arrays are returned.

Contents

Age

Returned as info about age of the flows identified by the flow operation.

Type: Integer

Required: No

ByteCount

Returns the number of bytes received or transmitted in a specific flow.

Type: Long

Required: No

DestinationAddress

A single IP address specification. This is used in the MatchAttributes source and destination specifications.

Type: Address object

Required: No

DestinationPort

The destination port to inspect for. You can specify an individual port, for example `1994` and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: No

PacketCount

Returns the total number of data packets received or transmitted in a flow.

Type: Integer

Required: No

Protocol

The protocols to inspect for, specified using the assigned internet protocol number (IANA) for each protocol. If not specified, this matches with any protocol.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 12.

Pattern: `^.*$`

Required: No

SourceAddress

A single IP address specification. This is used in the MatchAttributes source and destination specifications.

Type: Address object

Required: No

SourcePort

The source port to inspect for. You can specify an individual port, for example `1994` and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FlowFilter

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Contents

DestinationAddress

A single IP address specification. This is used in the MatchAttributes source and destination specifications.

Type: Address object

Required: No

DestinationPort

The destination port to inspect for. You can specify an individual port, for example 1994 and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: No

Protocols

The protocols to inspect for, specified using the assigned internet protocol number (IANA) for each protocol. If not specified, this matches with any protocol.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 12.

Pattern: `^.*$`

Required: No

SourceAddress

A single IP address specification. This is used in the MatchAttributes source and destination specifications.

Type: Address object

Required: No

SourcePort

The source port to inspect for. You can specify an individual port, for example 1994 and you can specify a port range, for example 1990:1994. To match with any port, specify ANY.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: ^.*$

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FlowOperation

Contains information about a flow operation, such as related statuses, unique identifiers, and all filters defined in the operation.

Flow operations let you manage the flows tracked in the flow table, also known as the firewall table.

A flow is network traffic that is monitored by a firewall, either by stateful or stateless rules. For traffic to be considered part of a flow, it must share Destination, DestinationPort, Direction, Protocol, Source, and SourcePort.

Contents

FlowFilters

Defines the scope a flow operation. You can use up to 20 filters to configure a single flow operation.

Type: Array of FlowFilter objects

Required: No

MinimumFlowAgeInSeconds

The reqested `FlowOperation` ignores flows with an age (in seconds) lower than `MinimumFlowAgeInSeconds`. You provide this for start commands.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FlowOperationMetadata

An array of objects with metadata about the requested `FlowOperation`.

Contents

FlowOperationId

A unique identifier for the flow operation. This ID is returned in the responses to start and list commands. You provide to describe commands.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

FlowOperationStatus

Returns the status of the flow operation. This string is returned in the responses to start, list, and describe commands.

If the status is `COMPLETED_WITH_ERRORS`, results may be returned with any number of `Flows` missing from the response. If the status is `FAILED`, `Flows` returned will be empty.

Type: String

Valid Values: `COMPLETED | IN_PROGRESS | FAILED | COMPLETED_WITH_ERRORS`

Required: No

FlowOperationType

Defines the type of `FlowOperation`.

Type: String

Valid Values: `FLOW_FLUSH | FLOW_CAPTURE`

Required: No

FlowRequestTimestamp

A timestamp indicating when the Suricata engine identified flows impacted by an operation.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FlowTimeouts

Describes the amount of time that can pass without any traffic sent through the firewall before the firewall determines that the connection is idle and Network Firewall removes the flow entry from its flow table. Existing connections and flows are not impacted when you update this value. Only new connections after you update this value are impacted.

Contents

TcpIdleTimeoutSeconds

The number of seconds that can pass without any TCP traffic sent through the firewall before the firewall determines that the connection is idle. After the idle timeout passes, data packets are dropped, however, the next TCP SYN packet is considered a new flow and is processed by the firewall. Clients or targets can use TCP keepalive packets to reset the idle timeout.

You can define the `TcpIdleTimeoutSeconds` value to be between 60 and 6000 seconds. If no value is provided, it defaults to 350 seconds.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Header

The basic rule criteria for AWS Network Firewall to use to inspect packet headers in stateful traffic flow inspection. Traffic flows that match the criteria are a match for the corresponding StatefulRule.

Contents

Destination

The destination IP address or address range to inspect for, in CIDR notation. To match with any address, specify `ANY`.

Specify an IP address or a block of IP addresses in Classless Inter-Domain Routing (CIDR) notation. Network Firewall supports all address ranges for IPv4 and IPv6.

Examples:

- To configure Network Firewall to inspect for the IP address 192.0.2.44, specify `192.0.2.44/32`.
- To configure Network Firewall to inspect for IP addresses from 192.0.2.0 to 192.0.2.255, specify `192.0.2.0/24`.
- To configure Network Firewall to inspect for the IP address 1111:0000:0000:0000:0000:0000:0000:0111, specify `1111:0000:0000:0000:0000:0000:0000:0111/128`.
- To configure Network Firewall to inspect for IP addresses from 1111:0000:0000:0000:0000:0000:0000:0000 to 1111:0000:0000:0000:ffff:ffff:ffff:ffff, specify `1111:0000:0000:0000:0000:0000:0000:0000/64`.

For more information about CIDR notation, see the Wikipedia entry Classless Inter-Domain Routing.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

DestinationPort

The destination port to inspect for. You can specify an individual port, for example 1994 and you can specify a port range, for example 1990:1994. To match with any port, specify ANY.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: ^.*$

Required: Yes

Direction

The direction of traffic flow to inspect. If set to ANY, the inspection matches bidirectional traffic, both from the source to the destination and from the destination to the source. If set to FORWARD, the inspection only matches traffic going from the source to the destination.

Type: String

Valid Values: FORWARD | ANY

Required: Yes

Protocol

The protocol to inspect for. To specify all, you can use IP, because all traffic on AWS and on the internet is IP.

Type: String

Valid Values: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP | HTTP2 | QUIC

Required: Yes

Source

The source IP address or address range to inspect for, in CIDR notation. To match with any address, specify ANY.

Specify an IP address or a block of IP addresses in Classless Inter-Domain Routing (CIDR) notation. Network Firewall supports all address ranges for IPv4 and IPv6.

Examples:

- To configure Network Firewall to inspect for the IP address 192.0.2.44, specify `192.0.2.44/32`.
- To configure Network Firewall to inspect for IP addresses from 192.0.2.0 to 192.0.2.255, specify `192.0.2.0/24`.
- To configure Network Firewall to inspect for the IP address 1111:0000:0000:0000:0000:0000:0000:0111, specify `1111:0000:0000:0000:0000:0000:0000:0111/128`.
- To configure Network Firewall to inspect for IP addresses from 1111:0000:0000:0000:0000:0000:0000:0000 to 1111:0000:0000:0000:ffff:ffff:ffff:ffff, specify `1111:0000:0000:0000:0000:0000:0000:0000/64`.

For more information about CIDR notation, see the Wikipedia entry Classless Inter-Domain Routing.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

SourcePort

The source port to inspect for. You can specify an individual port, for example 1994 and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Hits

Attempts made to a access domain.

Contents

Count

The number of attempts made to access a domain.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IPSet

A list of IP addresses and address ranges, in CIDR notation. This is part of a RuleVariables.

Contents

Definition

The list of IP addresses and address ranges, in CIDR notation.

Type: Array of strings

Length Constraints: Minimum length of 1.

Pattern: `^.*$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IPSetMetadata

General information about the IP set.

Contents

ResolvedCIDRCount

Describes the total number of CIDR blocks currently in use by the IP set references in a firewall. To determine how many CIDR blocks are available for you to use in a firewall, you can call `AvailableCIDRCount`.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 1000000.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IPSetReference

Configures one or more IP set references for a Suricata-compatible rule group. This is used in CreateRuleGroup or UpdateRuleGroup. An IP set reference is a rule variable that references resources that you create and manage in another AWS service, such as an Amazon VPC prefix list. Network Firewall IP set references enable you to dynamically update the contents of your rules. When you create, update, or delete the resource you are referencing in your rule, Network Firewall automatically updates the rule's content with the changes. For more information about IP set references in Network Firewall, see Using IP set references in the *Network Firewall Developer Guide*.

Network Firewall currently supports Amazon VPC prefix lists and resource groups in IP set references.

Contents

ReferenceArn

The Amazon Resource Name (ARN) of the resource that you are referencing in your rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LogDestinationConfig

Defines where AWS Network Firewall sends logs for the firewall for one log type. This is used in LoggingConfiguration. You can send each type of log to an Amazon S3 bucket, a CloudWatch log group, or a Firehose delivery stream.

Network Firewall generates logs for stateful rule groups. You can save alert, flow, and TLS log types.

Contents

LogDestination

The named location for the logs, provided in a key:value mapping that is specific to the chosen destination type.

- For an Amazon S3 bucket, provide the name of the bucket, with key `bucketName`, and optionally provide a prefix, with key `prefix`.

  The following example specifies an Amazon S3 bucket named `DOC-EXAMPLE-BUCKET` and the prefix `alerts`:

  ```
  "LogDestination": { "bucketName": "DOC-EXAMPLE-BUCKET", "prefix":
  "alerts" }
  ```

- For a CloudWatch log group, provide the name of the CloudWatch log group, with key `logGroup`. The following example specifies a log group named `alert-log-group`:

  ```
  "LogDestination": { "logGroup": "alert-log-group" }
  ```

- For a Firehose delivery stream, provide the name of the delivery stream, with key `deliveryStream`. The following example specifies a delivery stream named `alert-delivery-stream`:

  ```
  "LogDestination": { "deliveryStream": "alert-delivery-stream" }
  ```

Type: String to string map

Key Length Constraints: Minimum length of 3. Maximum length of 50.

Key Pattern: `^[0-9A-Za-z.\-_@\/]+$`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Value Pattern: `[\s\S]*$`

Required: Yes

LogDestinationType

The type of storage destination to send these logs to. You can send logs to an Amazon S3 bucket, a CloudWatch log group, or a Firehose delivery stream.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 30.

Pattern: `[0-9A-Za-z]+`

Valid Values: `S3 | CloudWatchLogs | KinesisDataFirehose`

Required: Yes

LogType

The type of log to record. You can record the following types of logs from your AWS Network Firewall stateful engine.

- `ALERT` - Logs for traffic that matches your stateful rules and that have an action that sends an alert. A stateful rule sends alerts for the rule actions DROP, ALERT, and REJECT. For more information, see StatefulRule.
- `FLOW` - Standard network traffic flow logs. The stateful rules engine records flow logs for all network traffic that it receives. Each flow log record captures the network flow for a specific standard stateless rule group.
- `TLS` - Logs for events that are related to TLS inspection. For more information, see Inspecting SSL/TLS traffic with TLS inspection configurations in the *Network Firewall Developer Guide*.

Type: String

Valid Values: `ALERT | FLOW | TLS`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LoggingConfiguration

Defines how AWS Network Firewall performs logging for a Firewall.

Contents

LogDestinationConfigs

Defines the logging destinations for the logs for a firewall. Network Firewall generates logs for stateful rule groups.

Type: Array of LogDestinationConfig objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MatchAttributes

Criteria for Network Firewall to use to inspect an individual packet in stateless rule inspection. Each match attributes set can include one or more items such as IP address, CIDR range, port number, protocol, and TCP flags.

Contents

DestinationPorts

The destination port to inspect for. You can specify an individual port, for example 1994 and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

This setting is only used for protocols 6 (TCP) and 17 (UDP).

Type: Array of PortRange objects

Required: No

Destinations

The destination IP addresses and address ranges to inspect for, in CIDR notation. If not specified, this matches with any destination address.

Type: Array of Address objects

Required: No

Protocols

The protocols to inspect for, specified using the assigned internet protocol number (IANA) for each protocol. If not specified, this matches with any protocol.

Type: Array of integers

Valid Range: Minimum value of 0. Maximum value of 255.

Required: No

SourcePorts

The source port to inspect for. You can specify an individual port, for example 1994 and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

If not specified, this matches with any source port.

This setting is only used for protocols 6 (TCP) and 17 (UDP).

Type: Array of PortRange objects

Required: No

Sources

The source IP addresses and address ranges to inspect for, in CIDR notation. If not specified, this matches with any source address.

Type: Array of Address objects

Required: No

TCPFlags

The TCP flags and masks to inspect for. If not specified, this matches with any settings. This setting is only used for protocol 6 (TCP).

Type: Array of TCPFlagField objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PerObjectStatus

Provides configuration status for a single policy or rule group that is used for a firewall endpoint. Network Firewall provides each endpoint with the rules that are configured in the firewall policy. Each time you add a subnet or modify the associated firewall policy, Network Firewall synchronizes the rules in the endpoint, so it can properly filter network traffic. This is part of a SyncState for a firewall.

Contents

SyncStatus

Indicates whether this object is in sync with the version indicated in the update token.

Type: String

Valid Values: `PENDING | IN_SYNC | CAPACITY_CONSTRAINED`

Required: No

UpdateToken

The current version of the object that is either in sync or pending synchronization.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyVariables

Contains variables that you can use to override default Suricata settings in your firewall policy.

Contents

RuleVariables

The IPv4 or IPv6 addresses in CIDR notation to use for the Suricata `HOME_NET` variable. If your firewall uses an inspection VPC, you might want to override the `HOME_NET` variable with the CIDRs of your home networks. If you don't override `HOME_NET` with your own CIDRs, Network Firewall by default uses the CIDR of your inspection VPC.

Type: String to IPSet object map

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Key Pattern: `^[A-Za-z][A-Za-z0-9_]*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PortRange

A single port range specification. This is used for source and destination port ranges in the stateless rule MatchAttributes, `SourcePorts`, and `DestinationPorts` settings.

Contents

FromPort

The lower limit of the port range. This must be less than or equal to the `ToPort` specification.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: Yes

ToPort

The upper limit of the port range. This must be greater than or equal to the `FromPort` specification.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PortSet

A set of port ranges for use in the rules in a rule group.

Contents

Definition

The set of port ranges.

Type: Array of strings

Length Constraints: Minimum length of 1.

Pattern: `^.*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PublishMetricAction

Stateless inspection criteria that publishes the specified metrics to Amazon CloudWatch for the matching packet. This setting defines a CloudWatch dimension value to be published.

Contents

Dimensions

Type: Array of Dimension objects

Array Members: Fixed number of 1 item.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReferenceSets

Contains a set of IP set references.

Contents

IPSetReferences

The list of IP set references.

Type: String to IPSetReference object map

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Key Pattern: `^[A-Za-z][A-Za-z0-9_]*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleDefinition

The inspection criteria and action for a single stateless rule. AWS Network Firewall inspects each packet for the specified matching criteria. When a packet matches the criteria, Network Firewall performs the rule's actions on the packet.

Contents

Actions

The actions to take on a packet that matches one of the stateless rule definition's match attributes. You must specify a standard action and you can add custom actions.

> **Note**
>
> Network Firewall only forwards a packet for stateful rule inspection if you specify `aws:forward_to_sfe` for a rule that the packet matches, or if the packet doesn't match any stateless rule and you specify `aws:forward_to_sfe` for the `StatelessDefaultActions` setting for the FirewallPolicy.

For every rule, you must specify exactly one of the following standard actions.

- **aws:pass** - Discontinues all inspection of the packet and permits it to go to its intended destination.
- **aws:drop** - Discontinues all inspection of the packet and blocks it from going to its intended destination.
- **aws:forward_to_sfe** - Discontinues stateless inspection of the packet and forwards it to the stateful rule engine for inspection.

Additionally, you can specify a custom action. To do this, you define a custom action by name and type, then provide the name you've assigned to the action in this `Actions` setting. For information about the options, see CustomAction.

To provide more than one action in this setting, separate the settings with a comma. For example, if you have a custom `PublishMetrics` action that you've named `MyMetricsAction`, then you could specify the standard action `aws:pass` and the custom action with `["aws:pass", "MyMetricsAction"]`.

Type: Array of strings

Required: Yes

MatchAttributes

Criteria for Network Firewall to use to inspect an individual packet in stateless rule inspection. Each match attributes set can include one or more items such as IP address, CIDR range, port number, protocol, and TCP flags.

Type: MatchAttributes object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleGroup

The object that defines the rules in a rule group. This, along with RuleGroupResponse, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

AWS Network Firewall uses a rule group to inspect and control network traffic. You define stateless rule groups to inspect individual packets and you define stateful rule groups to inspect packets in the context of their traffic flow.

To use a rule group, you include it by reference in an Network Firewall firewall policy, then you use the policy in a firewall. You can reference a rule group from more than one firewall policy, and you can use a firewall policy in more than one firewall.

Contents

RulesSource

The stateful rules or stateless rules for the rule group.

Type: RulesSource object

Required: Yes

ReferenceSets

The list of a rule group's reference sets.

Type: ReferenceSets object

Required: No

RuleVariables

Settings that are available for use in the rules in the rule group. You can only use these for stateful rule groups.

Type: RuleVariables object

Required: No

StatefulRuleOptions

Additional options governing how Network Firewall handles stateful rules. The policies where you use your stateful rule group must have stateful rule options settings that are compatible

with these settings. Some limitations apply; for more information, see Strict evaluation order in the *AWS Network Firewall Developer Guide*.

Type: StatefulRuleOptions object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleGroupMetadata

High-level information about a rule group, returned by ListRuleGroups. You can use the information provided in the metadata to retrieve and manage a rule group.

Contents

Arn

The Amazon Resource Name (ARN) of the rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

Name

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleGroupResponse

The high-level properties of a rule group. This, along with the RuleGroup, define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Contents

RuleGroupArn

The Amazon Resource Name (ARN) of the rule group.

> **Note**
>
> If this response is for a create request that had `DryRun` set to `TRUE`, then this ARN is a placeholder that isn't attached to a valid resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

RuleGroupId

The unique identifier for the rule group.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

AnalysisResults

The list of analysis results for `AnalyzeRuleGroup`. If you set `AnalyzeRuleGroup` to `TRUE` in CreateRuleGroup, UpdateRuleGroup, or DescribeRuleGroup, Network Firewall analyzes the rule group and identifies the rules that might adversely effect your firewall's functionality. For example, if Network Firewall detects a rule that's routing traffic asymmetrically, which impacts the service's ability to properly process traffic, the service includes the rule in the list of analysis results.

Type: Array of AnalysisResult objects

Required: No

Capacity

The maximum operating resources that this rule group can use. Rule group capacity is fixed at creation. When you update a rule group, you are limited to this capacity. When you reference a rule group from a firewall policy, Network Firewall reserves this capacity for the rule group.

You can retrieve the capacity that would be required for a rule group before you create the rule group by calling CreateRuleGroup with `DryRun` set to `TRUE`.

Type: Integer

Required: No

ConsumedCapacity

The number of capacity units currently consumed by the rule group rules.

Type: Integer

Required: No

Description

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EncryptionConfiguration

A complex type that contains the AWS KMS encryption configuration settings for your rule group.

Type: EncryptionConfiguration object

Required: No

LastModifiedTime

The last time that the rule group was changed.

Type: Timestamp

Required: No

NumberOfAssociations

The number of firewall policies that use this rule group.

Type: Integer

Required: No

RuleGroupStatus

Detailed information about the current status of a rule group.

Type: String

Valid Values: `ACTIVE | DELETING | ERROR`

Required: No

SnsTopic

The Amazon Resource Name (ARN) of the Amazon Simple Notification Service SNS topic that's used to record changes to the managed rule group. You can subscribe to the SNS topic to receive notifications when the managed rule group is modified, such as for new versions and for

version expiration. For more information, see the Amazon Simple Notification Service Developer Guide..

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

SourceMetadata

A complex type that contains metadata about the rule group that your own rule group is copied from. You can use the metadata to track the version updates made to the originating rule group.

Type: SourceMetadata object

Required: No

SummaryConfiguration

A complex type containing the currently selected rule option fields that will be displayed for rule summarization returned by DescribeRuleGroupSummary.

- The `RuleOptions` specified in SummaryConfiguration
- Rule metadata organization preferences

Type: SummaryConfiguration object

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Type: String

Valid Values: `STATELESS` | `STATEFUL`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleOption

Additional settings for a stateful rule. This is part of the StatefulRule configuration.

Contents

Keyword

The keyword for the Suricata compatible rule option. You must include a `sid` (signature ID), and can optionally include other keywords. For information about Suricata compatible keywords, see Rule options in the Suricata documentation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `.*`

Required: Yes

Settings

The settings of the Suricata compatible rule option. Rule options have zero or more setting values, and the number of possible and required settings depends on the `Keyword`. For more information about the settings for specific options, see Rule options.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 8192.

Pattern: `.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

RulesSource

The stateless or stateful rules definitions for use in a single rule group. Each rule group requires a single `RulesSource`. You can use an instance of this for either stateless rules or stateful rules.

Contents

RulesSourceList

Stateful inspection criteria for a domain list rule group.

Type: RulesSourceList object

Required: No

RulesString

Stateful inspection criteria, provided in Suricata compatible rules. Suricata is an open-source threat detection framework that includes a standard rule-based language for network traffic inspection.

These rules contain the inspection criteria and the action to take for traffic that matches the criteria, so this type of rule group doesn't have a separate action setting.

> **Note**
>
> You can't use the `priority` keyword if the `RuleOrder` option in StatefulRuleOptions is set to `STRICT_ORDER`.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000000.

Required: No

StatefulRules

An array of individual stateful rules inspection criteria to be used together in a stateful rule group. Use this option to specify simple Suricata rules with protocol, source and destination, ports, direction, and rule options. For information about the Suricata `Rules` format, see Rules Format.

Type: Array of StatefulRule objects

Required: No

StatelessRulesAndCustomActions

Stateless inspection criteria to be used in a stateless rule group.

Type: StatelessRulesAndCustomActions object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RulesSourceList

Stateful inspection criteria for a domain list rule group.

For HTTPS traffic, domain filtering is SNI-based. It uses the server name indicator extension of the TLS handshake.

By default, Network Firewall domain list inspection only includes traffic coming from the VPC where you deploy the firewall. To inspect traffic from IP addresses outside of the deployment VPC, you set the `HOME_NET` rule variable to include the CIDR range of the deployment VPC plus the other CIDR ranges. For more information, see RuleVariables in this guide and Stateful domain list rule groups in AWS Network Firewall in the *Network Firewall Developer Guide*.

Contents

GeneratedRulesType

Whether you want to allow or deny access to the domains in your target list.

Type: String

Valid Values: `ALLOWLIST | DENYLIST`

Required: Yes

Targets

The domains that you want to inspect for in your traffic flows. Valid domain specifications are the following:

- Explicit names. For example, `abc.example.com` matches only the domain `abc.example.com`.
- Names that use a domain wildcard, which you indicate with an initial `'.'`. For example, `.example.com` matches `example.com` and matches all subdomains of `example.com`, such as `abc.example.com` and `www.example.com`.

Type: Array of strings

Required: Yes

TargetTypes

The protocols you want to inspect. Specify `TLS_SNI` for `HTTPS`. Specify `HTTP_HOST` for `HTTP`. You can specify either or both.

Type: Array of strings

Valid Values: `TLS_SNI | HTTP_HOST`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleSummary

A complex type containing details about a Suricata rule. Contains:

- `SID`
- `Msg`
- `Metadata`

Summaries are available for rule groups you manage and for active threat defense AWS managed rule groups.

Contents

Metadata

The contents of the rule's metadata.

Type: String

Required: No

Msg

The contents taken from the rule's msg field.

Type: String

Required: No

SID

The unique identifier (Signature ID) of the Suricata rule.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleVariables

Settings that are available for use in the rules in the RuleGroup where this is defined. See CreateRuleGroup or UpdateRuleGroup for usage.

Contents

IPSets

A list of IP addresses and address ranges, in CIDR notation.

Type: String to IPSet object map

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Key Pattern: `^[A-Za-z][A-Za-z0-9_]*$`

Required: No

PortSets

A list of port ranges.

Type: String to PortSet object map

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Key Pattern: `^[A-Za-z][A-Za-z0-9_]*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServerCertificate

Any AWS Certificate Manager (ACM) Secure Sockets Layer/Transport Layer Security (SSL/TLS) server certificate that's associated with a ServerCertificateConfiguration. Used in a TLSInspectionConfiguration for inspection of inbound traffic to your firewall. You must request or import a SSL/TLS certificate into ACM for each domain Network Firewall needs to decrypt and inspect. AWS Network Firewall uses the SSL/TLS certificates to decrypt specified inbound SSL/TLS traffic going to your firewall. For information about working with certificates in AWS Certificate Manager, see Request a public certificate or Importing certificates in the *AWS Certificate Manager User Guide*.

Contents

ResourceArn

The Amazon Resource Name (ARN) of the AWS Certificate Manager SSL/TLS server certificate that's used for inbound SSL/TLS inspection.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServerCertificateConfiguration

Configures the AWS Certificate Manager certificates and scope that Network Firewall uses to decrypt and re-encrypt traffic using a TLSInspectionConfiguration. You can configure `ServerCertificates` for inbound SSL/TLS inspection, a `CertificateAuthorityArn` for outbound SSL/TLS inspection, or both. For information about working with certificates for TLS inspection, see Using SSL/TLS server certficiates with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

> **Note**
>
> If a server certificate that's associated with your TLSInspectionConfiguration is revoked, deleted, or expired it can result in client-side TLS errors.

Contents

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the imported certificate authority (CA) certificate within AWS Certificate Manager (ACM) to use for outbound SSL/TLS inspection.

The following limitations apply:

- You can use CA certificates that you imported into ACM, but you can't generate CA certificates with ACM.
- You can't use certificates issued by AWS Private Certificate Authority.

For more information about configuring certificates for outbound inspection, see Using SSL/TLS certificates with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

For information about working with certificates in ACM, see Importing certificates in the *AWS Certificate Manager User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

CheckCertificateRevocationStatus

When enabled, Network Firewall checks if the server certificate presented by the server in the SSL/TLS connection has a revoked or unkown status. If the certificate has an unknown or revoked status, you must specify the actions that Network Firewall takes on outbound traffic. To check the certificate revocation status, you must also specify a `CertificateAuthorityArn` in ServerCertificateConfiguration.

Type: CheckCertificateRevocationStatusActions object

Required: No

Scopes

A list of scopes.

Type: Array of ServerCertificateScope objects

Required: No

ServerCertificates

The list of server certificates to use for inbound SSL/TLS inspection.

Type: Array of ServerCertificate objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServerCertificateScope

Settings that define the Secure Sockets Layer/Transport Layer Security (SSL/TLS) traffic that Network Firewall should decrypt for inspection by the stateful rule engine.

Contents

DestinationPorts

The destination ports to decrypt for inspection, in Transmission Control Protocol (TCP) format. If not specified, this matches with any destination port.

You can specify individual ports, for example 1994, and you can specify port ranges, such as `1990:1994`.

Type: Array of PortRange objects

Required: No

Destinations

The destination IP addresses and address ranges to decrypt for inspection, in CIDR notation. If not specified, this matches with any destination address.

Type: Array of Address objects

Required: No

Protocols

The protocols to inspect for, specified using the assigned internet protocol number (IANA) for each protocol. If not specified, this matches with any protocol.

Network Firewall currently supports only TCP.

Type: Array of integers

Valid Range: Minimum value of 0. Maximum value of 255.

Required: No

SourcePorts

The source ports to decrypt for inspection, in Transmission Control Protocol (TCP) format. If not specified, this matches with any source port.

You can specify individual ports, for example 1994, and you can specify port ranges, such as `1990:1994`.

Type: Array of PortRange objects

Required: No

Sources

The source IP addresses and address ranges to decrypt for inspection, in CIDR notation. If not specified, this matches with any source address.

Type: Array of Address objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SourceMetadata

High-level information about the managed rule group that your own rule group is copied from. You can use the the metadata to track version updates made to the originating rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup.

Contents

SourceArn

The Amazon Resource Name (ARN) of the rule group that your own rule group is copied from.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

SourceUpdateToken

The update token of the AWS managed rule group that your own rule group is copied from. To determine the update token for the managed rule group, call DescribeRuleGroup.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulEngineOptions

Configuration settings for the handling of the stateful rule groups in a firewall policy.

Contents

FlowTimeouts

Configures the amount of time that can pass without any traffic sent through the firewall before the firewall determines that the connection is idle.

Type: FlowTimeouts object

Required: No

RuleOrder

Indicates how to manage the order of stateful rule evaluation for the policy. `STRICT_ORDER` is the recommended option, but `DEFAULT_ACTION_ORDER` is the default option. With `STRICT_ORDER`, provide your rules in the order that you want them to be evaluated. You can then choose one or more default actions for packets that don't match any rules. Choose `STRICT_ORDER` to have the stateful rules engine determine the evaluation order of your rules. The default action for this rule order is `PASS`, followed by `DROP`, `REJECT`, and `ALERT` actions. Stateful rules are provided to the rule engine as Suricata compatible strings, and Suricata evaluates them based on your settings. For more information, see Evaluation order for stateful rules in the *AWS Network Firewall Developer Guide*.

Type: String

Valid Values: `DEFAULT_ACTION_ORDER | STRICT_ORDER`

Required: No

StreamExceptionPolicy

Configures how Network Firewall processes traffic when a network connection breaks midstream. Network connections can break due to disruptions in external networks or within the firewall itself.

- `DROP` - Network Firewall fails closed and drops all subsequent traffic going to the firewall. This is the default behavior.

- `CONTINUE` - Network Firewall continues to apply rules to the subsequent traffic without context from traffic before the break. This impacts the behavior of rules that depend on this context. For example, if you have a stateful rule to `drop http` traffic, Network Firewall won't match the traffic for this rule because the service won't have the context from session initialization defining the application layer protocol as HTTP. However, this behavior is rule dependent—a TCP-layer rule using a `flow:stateless` rule would still match, as would the `aws:drop_strict` default action.
- `REJECT` - Network Firewall fails closed and drops all subsequent traffic going to the firewall. Network Firewall also sends a TCP reject packet back to your client so that the client can immediately establish a new session. Network Firewall will have context about the new session and will apply rules to the subsequent traffic.

Type: String

Valid Values: `DROP | CONTINUE | REJECT`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRule

A single Suricata rules specification, for use in a stateful rule group. Use this option to specify a simple Suricata rule with protocol, source and destination, ports, direction, and rule options. For information about the Suricata `Rules` format, see Rules Format.

Contents

Action

Defines what Network Firewall should do with the packets in a traffic flow when the flow matches the stateful rule criteria. For all actions, Network Firewall performs the specified action and discontinues stateful inspection of the traffic flow.

The actions for a stateful rule are defined as follows:

- **PASS** - Permits the packets to go to the intended destination.
- **DROP** - Blocks the packets from going to the intended destination and sends an alert log message, if alert logging is configured in the Firewall LoggingConfiguration.
- **ALERT** - Sends an alert log message, if alert logging is configured in the Firewall LoggingConfiguration.

  You can use this action to test a rule that you intend to use to drop traffic. You can enable the rule with `ALERT` action, verify in the logs that the rule is filtering as you want, then change the action to `DROP`.
- **REJECT** - Drops traffic that matches the conditions of the stateful rule, and sends a TCP reset packet back to sender of the packet. A TCP reset packet is a packet with no payload and an RST bit contained in the TCP header flags. REJECT is available only for TCP traffic. This option doesn't support FTP or IMAP protocols.

Type: String

Valid Values: `PASS | DROP | ALERT | REJECT`

Required: Yes

Header

The stateful inspection criteria for this rule, used to inspect traffic flows.

Type: Header object

Required: Yes

RuleOptions

Additional options for the rule. These are the Suricata `RuleOptions` settings.

Type: Array of RuleOption objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRuleGroupOverride

The setting that allows the policy owner to change the behavior of the rule group within a policy.

Contents

Action

The action that changes the rule group from `DROP` to `ALERT`. This only applies to managed rule groups.

Type: String

Valid Values: `DROP_TO_ALERT`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRuleGroupReference

Identifier for a single stateful rule group, used in a firewall policy to refer to a rule group.

Contents

ResourceArn

The Amazon Resource Name (ARN) of the stateful rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

DeepThreatInspection

AWS Network Firewall plans to augment the active threat defense managed rule group with an additional deep threat inspection capability. When this capability is released, AWS will analyze service logs of network traffic processed by these rule groups to identify threat indicators across customers. AWS will use these threat indicators to improve the active threat defense managed rule groups and protect the security of AWS customers and services.

> **Note**
>
> Customers can opt-out of deep threat inspection at any time through the AWS Network Firewall console or API. When customers opt out, AWS Network Firewall will not use the network traffic processed by those customers' active threat defense rule groups for rule group improvement.

Type: Boolean

Required: No

Override

The action that allows the policy owner to override the behavior of the rule group within a policy.

Type: StatefulRuleGroupOverride object

Required: No

Priority

An integer setting that indicates the order in which to run the stateful rule groups in a single FirewallPolicy. This setting only applies to firewall policies that specify the `STRICT_ORDER` rule order in the stateful engine options settings.

Network Firewall evalutes each stateful rule group against a packet starting with the group that has the lowest priority setting. You must ensure that the priority settings are unique within each policy.

You can change the priority settings of your rule groups at any time. To make it easier to insert rule groups later, number them so there's a wide range in between, for example use 100, 200, and so on.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRuleOptions

Additional options governing how Network Firewall handles the rule group. You can only use these for stateful rule groups.

Contents

RuleOrder

Indicates how to manage the order of the rule evaluation for the rule group. `DEFAULT_ACTION_ORDER` is the default behavior. Stateful rules are provided to the rule engine as Suricata compatible strings, and Suricata evaluates them based on certain settings. For more information, see Evaluation order for stateful rules in the *AWS Network Firewall Developer Guide*.

Type: String

Valid Values: `DEFAULT_ACTION_ORDER | STRICT_ORDER`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRule

A single stateless rule. This is used in StatelessRulesAndCustomActions.

Contents

Priority

Indicates the order in which to run this rule relative to all of the rules that are defined for a stateless rule group. Network Firewall evaluates the rules in a rule group starting with the lowest priority setting. You must ensure that the priority settings are unique for the rule group.

Each stateless rule group uses exactly one `StatelessRulesAndCustomActions` object, and each `StatelessRulesAndCustomActions` contains exactly one `StatelessRules` object. To ensure unique priority settings for your rule groups, set unique priorities for the stateless rules that you define inside any single `StatelessRules` object.

You can change the priority settings of your rules at any time. To make it easier to insert rules later, number them so there's a wide range in between, for example use 100, 200, and so on.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: Yes

RuleDefinition

Defines the stateless 5-tuple packet inspection criteria and the action to take on a packet that matches the criteria.

Type: RuleDefinition object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRuleGroupReference

Identifier for a single stateless rule group, used in a firewall policy to refer to the rule group.

Contents

Priority

An integer setting that indicates the order in which to run the stateless rule groups in a single FirewallPolicy. Network Firewall applies each stateless rule group to a packet starting with the group that has the lowest priority setting. You must ensure that the priority settings are unique within each policy.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: Yes

ResourceArn

The Amazon Resource Name (ARN) of the stateless rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRulesAndCustomActions

Stateless inspection criteria. Each stateless rule group uses exactly one of these data types to define its stateless rules.

Contents

StatelessRules

Defines the set of stateless rules for use in a stateless rule group.

Type: Array of StatelessRule objects

Required: Yes

CustomActions

Defines an array of individual custom action definitions that are available for use by the stateless rules in this `StatelessRulesAndCustomActions` specification. You name each custom action that you define, and then you can use it by name in your StatelessRule RuleDefinition `Actions` specification.

Type: Array of CustomAction objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SubnetMapping

The ID for a subnet that's used in an association with a firewall. This is used in CreateFirewall, AssociateSubnets, and CreateVpcEndpointAssociation. AWS Network Firewall creates an instance of the associated firewall in each subnet that you specify, to filter traffic in the subnet's Availability Zone.

Contents

SubnetId

The unique identifier for the subnet.

Type: String

Required: Yes

IPAddressType

The subnet's IP address type. You can't change the IP address type after you create the subnet.

Type: String

Valid Values: `DUALSTACK | IPV4 | IPV6`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Summary

A complex type containing summaries of security protections provided by a rule group.

Network Firewall extracts this information from selected fields in the rule group's Suricata rules, based on your SummaryConfiguration settings.

Contents

RuleSummaries

An array of RuleSummary objects containing individual rule details that had been configured by the rulegroup's SummaryConfiguration.

Type: Array of RuleSummary objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SummaryConfiguration

A complex type that specifies which Suricata rule metadata fields to use when displaying threat information. Contains:

- `RuleOptions` - The Suricata rule options fields to extract and display

These settings affect how threat information appears in both the console and API responses. Summaries are available for rule groups you manage and for active threat defense AWS managed rule groups.

Contents

RuleOptions

Specifies the selected rule options returned by DescribeRuleGroupSummary.

Type: Array of strings

Valid Values: `SID | MSG | METADATA`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SyncState

The status of the firewall endpoint and firewall policy configuration for a single VPC subnet. This is part of the FirewallStatus.

For each VPC subnet that you associate with a firewall, AWS Network Firewall does the following:

- Instantiates a firewall endpoint in the subnet, ready to take traffic.
- Configures the endpoint with the current firewall policy settings, to provide the filtering behavior for the endpoint.

When you update a firewall, for example to add a subnet association or change a rule group in the firewall policy, the affected sync states reflect out-of-sync or not ready status until the changes are complete.

Contents

Attachment

The configuration and status for a single firewall subnet. For each configured subnet, Network Firewall creates the attachment by instantiating the firewall endpoint in the subnet so that it's ready to take traffic.

Type: Attachment object

Required: No

Config

The configuration status of the firewall endpoint in a single VPC subnet. Network Firewall provides each endpoint with the rules that are configured in the firewall policy. Each time you add a subnet or modify the associated firewall policy, Network Firewall synchronizes the rules in the endpoint, so it can properly filter network traffic.

Type: String to PerObjectStatus object map

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

A key:value pair associated with an AWS resource. The key:value pair can be anything you define. Typically, the tag key represents a category (such as "environment") and the tag value represents a specific value within that category (such as "test," "development," or "production"). You can add up to 50 tags to each AWS resource.

Contents

Key

The part of the key:value pair that defines a tag. You can use a tag key to describe a category of information, such as "customer." Tag keys are case-sensitive.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^.*$`

Required: Yes

Value

The part of the key:value pair that defines a tag. You can use a tag value to describe a specific value within a category, such as "companyA" or "companyB." Tag values are case-sensitive.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `^.*$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

TCPFlagField

TCP flags and masks to inspect packets for, used in stateless rules MatchAttributes settings.

Contents

Flags

Used in conjunction with the `Masks` setting to define the flags that must be set and flags that must not be set in order for the packet to match. This setting can only specify values that are also specified in the `Masks` setting.

For the flags that are specified in the masks setting, the following must be true for the packet to match:

- The ones that are set in this flags setting must be set in the packet.
- The ones that are not set in this flags setting must also not be set in the packet.

Type: Array of strings

Valid Values: `FIN | SYN | RST | PSH | ACK | URG | ECE | CWR`

Required: Yes

Masks

The set of flags to consider in the inspection. To inspect all flags in the valid values list, leave this with no setting.

Type: Array of strings

Valid Values: `FIN | SYN | RST | PSH | ACK | URG | ECE | CWR`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

TlsCertificateData

Contains metadata about an AWS Certificate Manager certificate.

Contents

CertificateArn

The Amazon Resource Name (ARN) of the certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

CertificateSerial

The serial number of the certificate.

Type: String

Required: No

Status

The status of the certificate.

Type: String

Required: No

StatusMessage

Contains details about the certificate status, including information about certificate errors.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9- ]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with TLSInspectionConfigurationResponse, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration.

AWS Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see Inspecting SSL/TLS traffic with TLS inspection configurations in the *AWS Network Firewall Developer Guide*.

Contents

ServerCertificateConfigurations

Lists the server certificate configurations that are associated with the TLS configuration.

Type: Array of ServerCertificateConfiguration objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TLSInspectionConfigurationMetadata

High-level information about a TLS inspection configuration, returned by `ListTLSInspectionConfigurations`. You can use the information provided in the metadata to retrieve and manage a TLS configuration.

Contents

Arn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

Name

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the `TLSInspectionConfiguration`, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling `DescribeTLSInspectionConfiguration`.

Contents

TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

TLSInspectionConfigurationId

A unique identifier for the TLS inspection configuration. This ID is returned in the responses to create and list commands. You provide it to operations such as update and delete.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

TLSInspectionConfigurationName

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

CertificateAuthority

Contains metadata about an AWS Certificate Manager certificate.

Type: TlsCertificateData object

Required: No

Certificates

A list of the certificates associated with the TLS inspection configuration.

Type: Array of TlsCertificateData objects

Required: No

Description

A description of the TLS inspection configuration.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

EncryptionConfiguration

A complex type that contains the AWS KMS encryption configuration settings for your TLS inspection configuration.

Type: EncryptionConfiguration object

Required: No

LastModifiedTime

The last time that the TLS inspection configuration was changed.

Type: Timestamp

Required: No

NumberOfAssociations

The number of firewall policies that use this TLS inspection configuration.

Type: Integer

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

TLSInspectionConfigurationStatus

Detailed information about the current status of a TLSInspectionConfiguration. You can retrieve this for a TLS inspection configuration by calling DescribeTLSInspectionConfiguration and providing the TLS inspection configuration name and ARN.

Type: String

Valid Values: `ACTIVE | DELETING | ERROR`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TransitGatewayAttachmentSyncState

Contains information about the synchronization state of a transit gateway attachment, including its current status and any error messages. Network Firewall uses this to track the state of your transit gateway configuration changes.

Contents

AttachmentId

The unique identifier of the transit gateway attachment.

Type: String

Required: No

StatusMessage

A message providing additional information about the current status, particularly useful when the transit gateway attachment is in a non-`READY` state.

Valid values are:

- `CREATING` - The attachment is being created
- `DELETING` - The attachment is being deleted
- `DELETED` - The attachment has been deleted
- `FAILED` - The attachment creation has failed and cannot be recovered
- `ERROR` - The attachment is in an error state that might be recoverable
- `READY` - The attachment is active and processing traffic
- `PENDING_ACCEPTANCE` - The attachment is waiting to be accepted
- `REJECTING` - The attachment is in the process of being rejected
- `REJECTED` - The attachment has been rejected

For information about troubleshooting endpoint failures, see Troubleshooting firewall endpoint failures in the *AWS Network Firewall Developer Guide*.

Type: String

Required: No

TransitGatewayAttachmentStatus

The current status of the transit gateway attachment.

Valid values are:

- `CREATING` - The attachment is being created
- `DELETING` - The attachment is being deleted
- `DELETED` - The attachment has been deleted
- `FAILED` - The attachment creation has failed and cannot be recovered
- `ERROR` - The attachment is in an error state that might be recoverable
- `READY` - The attachment is active and processing traffic
- `PENDING_ACCEPTANCE` - The attachment is waiting to be accepted
- `REJECTING` - The attachment is in the process of being rejected
- `REJECTED` - The attachment has been rejected

Type: String

Valid Values: `CREATING | DELETING | DELETED | FAILED | ERROR | READY | PENDING_ACCEPTANCE | REJECTING | REJECTED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UniqueSources

A unique source IP address that connected to a domain.

Contents

Count

The number of unique source IP addresses that connected to a domain.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VpcEndpointAssociation

A VPC endpoint association defines a single subnet to use for a firewall endpoint for a `Firewall`. You can define VPC endpoint associations only in the Availability Zones that already have a subnet mapping defined in the `Firewall` resource.

> **Note**
>
> You can retrieve the list of Availability Zones that are available for use by calling `DescribeFirewallMetadata`.

To manage firewall endpoints, first, in the `Firewall` specification, you specify a single VPC and one subnet for each of the Availability Zones where you want to use the firewall. Then you can define additional endpoints as VPC endpoint associations.

You can use VPC endpoint associations to expand the protections of the firewall as follows:

- **Protect multiple VPCs with a single firewall** - You can use the firewall to protect other VPCs, either in your account or in accounts where the firewall is shared. You can only specify Availability Zones that already have a firewall endpoint defined in the `Firewall` subnet mappings.
- **Define multiple firewall endpoints for a VPC in an Availability Zone** - You can create additional firewall endpoints for the VPC that you have defined in the firewall, in any Availability Zone that already has an endpoint defined in the `Firewall` subnet mappings. You can create multiple VPC endpoint associations for any other VPC where you use the firewall.

You can use AWS Resource Access Manager to share a `Firewall` that you own with other accounts, which gives them the ability to use the firewall to create VPC endpoint associations. For information about sharing a firewall, see `PutResourcePolicy` in this guide and see Sharing Network Firewall resources in the *AWS Network Firewall Developer Guide*.

The status of the VPC endpoint association, which indicates whether it's ready to filter network traffic, is provided in the corresponding VpcEndpointAssociationStatus. You can retrieve both the association and its status by calling DescribeVpcEndpointAssociation.

Contents

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

SubnetMapping

The ID for a subnet that's used in an association with a firewall. This is used in CreateFirewall, AssociateSubnets, and CreateVpcEndpointAssociation. AWS Network Firewall creates an instance of the associated firewall in each subnet that you specify, to filter traffic in the subnet's Availability Zone.

Type: SubnetMapping object

Required: Yes

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

VpcId

The unique identifier of the VPC for the endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: Yes

Description

A description of the VPC endpoint association.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

VpcEndpointAssociationId

The unique identifier of the VPC endpoint association.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

VpcEndpointAssociationMetadata

High-level information about a VPC endpoint association, returned by `ListVpcEndpointAssociations`. You can use the information provided in the metadata to retrieve and manage a VPC endpoint association.

Contents

VpcEndpointAssociationArn

The Amazon Resource Name (ARN) of a VPC endpoint association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VpcEndpointAssociationStatus

Detailed information about the current status of a VpcEndpointAssociation. You can retrieve this by calling DescribeVpcEndpointAssociation and providing the VPC endpoint association ARN.

Contents

Status

The readiness of the configured firewall endpoint to handle network traffic.

Type: String

Valid Values: `PROVISIONING | DELETING | READY`

Required: Yes

AssociationSyncState

The list of the Availability Zone sync states for all subnets that are defined by the firewall.

Type: String to AZSyncState object map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signing AWS API requests in the *IAM User Guide*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Elements of an AWS API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see AWS services that work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400