



Panduan Developer

# AWS Manajer Keamanan Jaringan



# AWS Manajer Keamanan Jaringan: Panduan Developer

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

---

# Table of Contents

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| Apa itu Manajer Keamanan AWS Jaringan? .....                                                 | 1  |
| Bagaimana AWS Sekilas tentang Network Security Manager bekerja .....                         | 1  |
| Fitur dari AWS Manajer Keamanan Jaringan .....                                               | 1  |
| Kasus penggunaan .....                                                                       | 2  |
| Layanan terkait .....                                                                        | 3  |
| Mengakses AWS Manajer Keamanan Jaringan .....                                                | 4  |
| Harga .....                                                                                  | 4  |
| Apakah Anda pengguna baru? .....                                                             | 5  |
| Bagaimana AWS Network Security Manager bekerja .....                                         | 6  |
| AWS Model sumber daya Manajer Keamanan Jaringan .....                                        | 6  |
| AWS Siklus hidup sumber daya Manajer Keamanan Jaringan, penggabungan, dan sinkronisasi ..... | 7  |
| Draf dan siklus hidup aktif .....                                                            | 7  |
| Penentuan versi .....                                                                        | 8  |
| Priority-based penggabungan kebijakan .....                                                  | 9  |
| Penemuan sumber daya dengan AWS Config .....                                                 | 10 |
| Sinkronisasi dan remediasi .....                                                             | 11 |
| Akun administrator dan anggota .....                                                         | 13 |
| Service-linked peran .....                                                                   | 13 |
| Menyiapkan Manajer Keamanan AWS Jaringan .....                                               | 14 |
| Pilih model organisasi Anda .....                                                            | 14 |
| Menyiapkan untuk penggunaan akun tunggal .....                                               | 14 |
| Menyiapkan untuk penggunaan multi-akun dengan AWS Organizations .....                        | 15 |
| Membuat AWS Akun administrator Manajer Keamanan Jaringan .....                               | 16 |
| Buat identitas IAM dengan AWS IZIN Manajer Keamanan Jaringan .....                           | 17 |
| Mendaftar untuk Akun AWS .....                                                               | 19 |
| Penggunaan AWS Manajer Keamanan Jaringan di Wilayah yang dinonaktifkan secara default .....  | 19 |
| Tutorial: Menyebarkan perlindungan keamanan jaringan pertama Anda .....                      | 20 |
| Prasyarat .....                                                                              | 20 |
| Langkah 1: Buat aturan .....                                                                 | 21 |
| Langkah 2: Buat template .....                                                               | 22 |
| Langkah 3: Buat kebijakan .....                                                              | 23 |
| Langkah 4: Buat ruang lingkup .....                                                          | 24 |

|                                                                  |    |
|------------------------------------------------------------------|----|
| Langkah 5: Buat dan publikasikan penyebaran .....                | 24 |
| Langkah 6: Memantau status sinkronisasi .....                    | 25 |
| Langkah 7: Bersihkan .....                                       | 26 |
| Langkah selanjutnya .....                                        | 27 |
| Mengelola firewall dan layanan keamanan .....                    | 28 |
| Mengelola ACL web untuk WAF AWS .....                            | 28 |
| AWS Konsep WAF .....                                             | 28 |
| Buat Cepat untuk AWS WAF .....                                   | 32 |
| Proses pembuatan standar untuk AWS WAF .....                     | 36 |
| Mengelola perlindungan DDoS untuk Shield Advanced AWS .....      | 42 |
| Buat Cepat untuk AWS Shield Advanced .....                       | 43 |
| Proses pembuatan standar untuk AWS Shield Advanced .....         | 46 |
| AWS Manajer Keamanan Jaringan dan Manajer Firewall .....         | 51 |
| Koeksistensi dengan AWS Firewall Manager .....                   | 51 |
| Prioritas selama remediasi .....                                 | 51 |
| Migrasi yang direncanakan dari AWS Firewall Manager .....        | 51 |
| Keamanan .....                                                   | 53 |
| Perlindungan data .....                                          | 54 |
| Enkripsi saat diam .....                                         | 55 |
| Enkripsi saat bergerak .....                                     | 55 |
| Manajemen kunci .....                                            | 55 |
| Manajemen identitas dan akses .....                              | 55 |
| Audiens .....                                                    | 56 |
| Mengautentikasi dengan identitas .....                           | 56 |
| Mengelola akses menggunakan kebijakan .....                      | 57 |
| Bagaimana AWS Manajer Keamanan Jaringan bekerja dengan IAM ..... | 59 |
| Identity-based contoh kebijakan .....                            | 65 |
| Pemecahan masalah .....                                          | 70 |
| Service-linked peran .....                                       | 72 |
| Service-linked izin peran .....                                  | 73 |
| Membuat peran tertaut layanan .....                              | 83 |
| Mengedit peran yang ditautkan ke layanan .....                   | 83 |
| Menghapus peran yang ditautkan ke layanan .....                  | 84 |
| Wilayah yang Didukung .....                                      | 84 |
| Validasi kepatuhan .....                                         | 85 |
| Ketahanan .....                                                  | 85 |

|                                                             |      |
|-------------------------------------------------------------|------|
| Keamanan Infrastruktur .....                                | 86   |
| Praktik terbaik keamanan .....                              | 86   |
| Kontrol pencegahan .....                                    | 86   |
| Kontrol detektif .....                                      | 87   |
| Memantau AWS Manajer Keamanan Jaringan .....                | 88   |
| Memantau status sinkronisasi .....                          | 88   |
| Operasi status sinkronisasi .....                           | 88   |
| Memahami nilai status sinkronisasi .....                    | 89   |
| Memahami stempel waktu evaluasi .....                       | 89   |
| Cross-account visibilitas .....                             | 89   |
| Mendiagnosis sumber daya yang tidak sinkron .....           | 90   |
| CloudTrail log .....                                        | 90   |
| AWS Informasi Manajer Keamanan Jaringan di CloudTrail ..... | 91   |
| Contoh: CreatePolicy acara .....                            | 92   |
| Kuota .....                                                 | 95   |
| Kuota sumber daya .....                                     | 95   |
| Kuota komposisi sumber daya .....                           | 95   |
| Kuota konfigurasi lingkup .....                             | 96   |
| Kuota akun administrator .....                              | 96   |
| Kuota pagination API .....                                  | 96   |
| Penyesuaian kuota .....                                     | 97   |
| Riwayat dokumen .....                                       | 98   |
| .....                                                       | xcix |

# Apa itu AWS Manajer Keamanan Jaringan?

Dengan AWS Network Security Manager, Anda dapat menentukan dan menerapkan perlindungan keamanan jaringan secara terpusat — seperti aturan WAF AWS dan AWS Shield Advanced — di satu atau beberapa akun dan sumber daya di organisasi Anda. Alih-alih bekerja dengan masing-masing sumber daya secara individual, Anda mendefinisikan objek kebijakan yang dapat digunakan kembali (aturan, templat, dan kebijakan) sekali dan menerapkannya dalam skala besar, dengan pemantauan berkelanjutan untuk mendeteksi dan memulihkan penyimpangan kebijakan.

## Bagaimana AWS Sekilas tentang Network Security Manager bekerja

Anda menentukan satu set objek kebijakan hierarkis dan menerapkannya ke cakupan yang ditargetkan. Objek kebijakan tingkat terendah adalah aturan. Anda dapat mengelompokkan aturan ke dalam templat, yang dapat Anda gabungkan ke dalam kebijakan dengan resolusi konflik berbasis prioritas. Anda kemudian memilih akun dan sumber daya untuk dilindungi dengan cakupan, dan menerapkan kebijakan Anda dengan menerbitkan penerapan.

Setelah penerapan, Manajer Keamanan AWS Jaringan terus memantau lingkungan cakupan dan kebijakan yang diterapkan untuk memeriksa apakah mereka cocok dengan definisi yang dimaksud. Jika tidak, Manajer Keamanan AWS Jaringan dapat secara opsional memulihkan sumber daya yang melayang dari konfigurasi yang dimaksud. Untuk detail selengkapnya tentang model sumber daya, siklus hidup, dan arsitektur, lihat. [Bagaimana AWS Network Security Manager bekerja](#)

## Fitur dari AWS Manajer Keamanan Jaringan

- Support untuk beberapa jenis firewall — AWS Network Security Manager mendukung AWS WAF untuk konfigurasi ACL web dan grup aturan. Jenis sumber daya yang dilindungi mencakup CloudFront distribusi Amazon, Application Load Balancer, dan tahapan Amazon API Gateway. AWS Network Security Manager juga mendukung AWS Shield Advanced untuk perlindungan DDoS dari CloudFront distribusi Amazon, Application Load Balancers, Classic Load Balancers, dan alamat IP Elastis.
- Konfigurasi keamanan yang dapat digunakan kembali — Tentukan objek kebijakan sekali sebagai aturan, kelompokkan ke dalam templat, dan buat cakupan untuk menargetkan sumber daya. Gunakan kembali aturan, templat, dan cakupan di beberapa kebijakan dan penerapan.

- **Priority-based penggabungan kebijakan** — Ketika beberapa kebijakan melindungi sumber daya yang sama, Manajer Keamanan AWS Jaringan menggabungkan konfigurasinya berdasarkan prioritas kebijakan, memberikan resolusi konflik yang dapat diprediksi.
- **Single-account dan dukungan multi-administrator** - Gunakan Manajer Keamanan AWS Jaringan dalam satu akun atau tentukan beberapa akun administrator, masing-masing dengan tingkat prioritas. Ketika kebijakan administrator tumpang tindih, Manajer Keamanan AWS Jaringan menyelesaikan konflik berdasarkan prioritas administrator terlebih dahulu, kemudian dengan prioritas kebijakan dalam setiap akun.
- **Draf dan status Aktif** - Setiap sumber daya Manajer Keamanan AWS Jaringan, termasuk aturan, templat, kebijakan, cakupan, dan penerapan, mendukung status Draf dan Aktif. Simpan sumber daya sebagai Draf tanpa memengaruhi perlindungan langsung, lalu publikasikan saat siap untuk menegakkannya.
- **Snapshot berversi** - Setiap sumber daya Manajer Keamanan AWS Jaringan, termasuk aturan, templat, kebijakan, cakupan, dan penerapan, mendukung snapshot bernomor versi yang tidak dapat diubah. Gunakan pembuatan versi untuk mempertahankan konfigurasi sumber daya Manajer Keamanan AWS Jaringan yang diketahui baik.
- **Protected-resource diagnostik sinkronisasi** — Untuk setiap sumber daya dalam lingkup, lihat setelan mana yang tidak sinkron dan alasannya, dengan pengaturan yang diharapkan dibandingkan dengan nilai aktual untuk setiap bidang konfigurasi.
- **Remediasi otomatis** — Secara opsional memungkinkan Manajer Keamanan AWS Jaringan untuk secara otomatis memulihkan sumber daya yang tidak sinkron dan menyelaraskannya dengan konfigurasi yang dimaksud tanpa intervensi manual.
- **Natural-language pembuatan aturan** - Gunakan `GenerateRuleConfiguration` operasi untuk mendeskripsikan aturan dalam bahasa sederhana dan menerima konfigurasi JSON yang sesuai, yang didukung oleh Amazon Bedrock.

## Kasus penggunaan

Berikut ini adalah kasus penggunaan umum untuk AWS Network Security Manager:

- **Menerapkan aturan AWS WAF dasar di semua akun** — Tentukan kumpulan grup aturan AWS WAF yang harus digunakan oleh setiap aplikasi yang menghadap ke internet, lalu terapkan di seluruh organisasi Anda. AWS Manajer Keamanan Jaringan secara otomatis menerapkan aturan ke sumber daya dalam lingkup baru saat masuk ke ruang lingkup.

- Buat aturan AWS WAF kustom atau pengecualian khusus di seluruh sumber daya tertentu — Tentukan seperangkat aturan AWS WAF yang hanya berlaku untuk kumpulan sumber daya tertentu. Set ini dapat berupa unit bisnis atau aplikasi tertentu yang Anda identifikasi berdasarkan ID AWS akun, OU, tag, atau Nama Sumber Daya Amazon (ARN).
- Verifikasi perlindungan DDoS pada sumber daya yang menghadap ke internet — Buat kebijakan AWS Shield Advanced yang mencakup jenis sumber daya publik dan terapkan di seluruh organisasi sehingga sumber daya penting mengaktifkan perlindungan DDoS.
- Mendeteksi dan memulihkan penyimpangan konfigurasi — Gunakan pemantauan status sinkronisasi untuk mengidentifikasi sumber daya yang konfigurasi firewallnya telah melayang dari status yang diinginkan, dan secara opsional mengaktifkan remediasi otomatis untuk mengembalikannya ke kepatuhan.
- Delegasikan manajemen keamanan ke beberapa tim — Tentukan beberapa akun administrator dengan tingkat prioritas yang berbeda dan akses cakupan ke akun tertentu, unit organisasi, atau jenis firewall, yang memungkinkan tim mengelola kebijakan keamanan mereka sendiri dalam batas-batas yang ditentukan.

## Layanan terkait

- AWS WAF — Gunakan AWS WAF untuk melindungi aplikasi web dan API Anda dari eksploitasi web umum dan bot yang mungkin memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. AWS Network Security Manager menggunakan AWS WAF untuk membuat dan mengelola ACL web dan grup aturan untuk sumber daya dalam satu akun atau di seluruh akun di organisasi Anda.
- AWS Shield Advanced — Layanan perlindungan DDoS terkelola yang menyediakan perlindungan yang diperluas untuk aplikasi Anda yang sedang berjalan. AWS Network Security Manager menggunakan Shield Advanced untuk memberikan perlindungan DDoS untuk sumber daya dalam satu akun atau di seluruh akun di organisasi Anda.
- AWS Organizations — Membantu Anda mengelola dan mengatur lingkungan secara terpusat saat Anda tumbuh dan meningkatkan sumber daya Anda AWS. AWS Network Security Manager mewajibkan AWS Organizations untuk mengelola perlindungan di seluruh akun anggota.
- AWS Config — Layanan yang memungkinkan Anda menilai, mengaudit, dan mengevaluasi konfigurasi sumber daya Anda. AWS Network Security Manager menggunakan perekam AWS Config terkait layanan untuk menemukan sumber daya di akun anggota Anda.

# Mengakses AWS Manajer Keamanan Jaringan

Anda dapat mengakses AWS Network Security Manager melalui antarmuka berikut:

## AWS Konsol Manajemen

Antarmuka berbasis web untuk mengelola sumber daya Manajer Keamanan AWS Jaringan.

Buka konsol Manajer Keamanan AWS Jaringan di <https://console.aws.amazon.com/network-security-manager/>.

## AWS Antarmuka Baris Perintah (AWS CLI)

Memberikan perintah untuk operasi Manajer Keamanan AWS Jaringan. Untuk informasi selengkapnya, lihat Referensi [Perintah AWS CLI](#).

## AWS SDK

AWS menyediakan SDK yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman. SDK menyediakan cara mudah untuk membuat akses terprogram ke Manajer Keamanan AWS Jaringan. Untuk informasi lebih lanjut, lihat [Alat untuk Amazon Web Services](#).

## AWS API Manajer Keamanan Jaringan

REST API yang menggunakan JSON melalui HTTPS. Format titik akhir API adalah `network-security-manager.{region}.api.aws`. Untuk informasi selengkapnya, lihat [Referensi API AWS Network Security Manager](#).

Untuk memulai dengan AWS Network Security Manager, lihat [Menyiapkan Manajer Keamanan AWS Jaringan](#) dan [Tutorial: Menyebarkan perlindungan keamanan jaringan pertama Anda](#).

## Harga

Anda membayar untuk setiap sumber daya dalam lingkup yang dipantau dan dilindungi oleh Manajer Keamanan AWS Jaringan. Biaya tambahan berlaku untuk layanan keamanan dasar yang Anda gunakan, seperti AWS WAF dan AWS Shield Advanced. Untuk informasi harga terperinci, lihat [harga Manajer Keamanan AWS Jaringan](#) di AWS situs web.

## Apakah Anda pengguna baru?

Jika Anda adalah pengguna pertama kali AWS Network Security Manager, kami sarankan Anda membaca topik berikut secara berurutan:

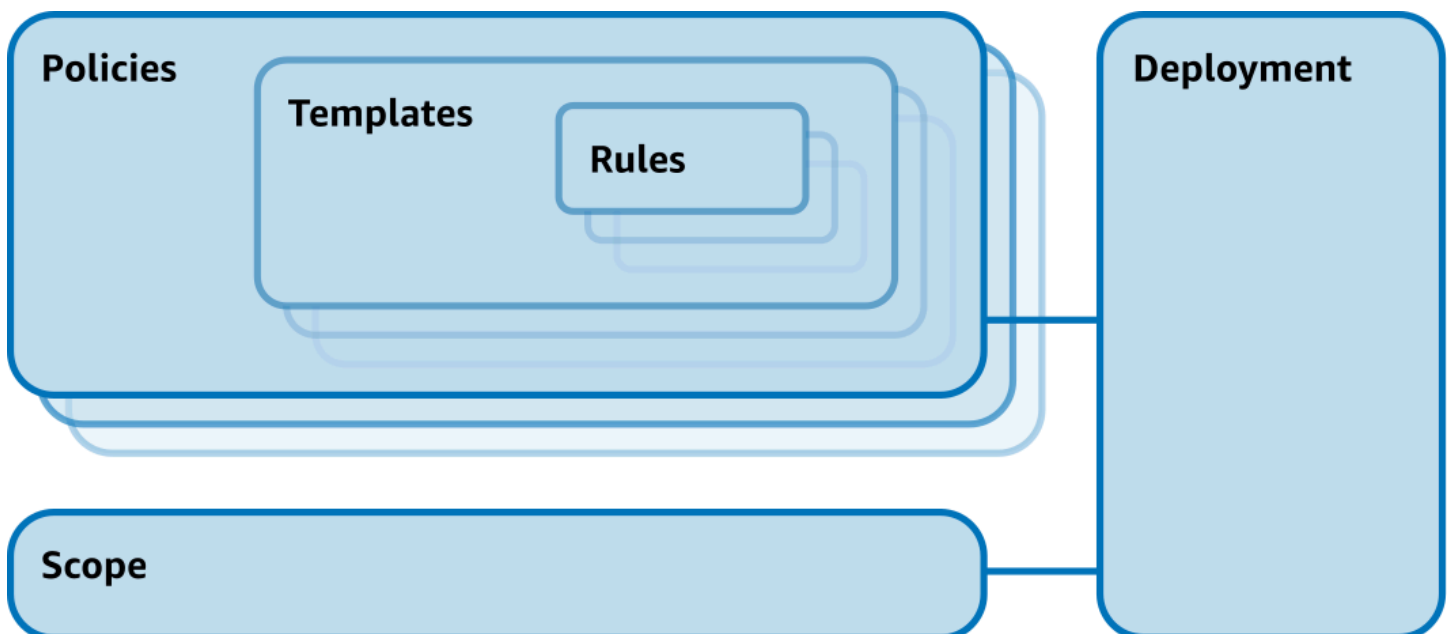
1. [Bagaimana AWS Network Security Manager bekerja](#)— Pelajari tentang model sumber daya, status siklus hidup, penggabungan kebijakan, dan sinkronisasi.
2. [Menyiapkan Manajer Keamanan AWS Jaringan](#)— Lengkapi prasyarat untuk menggunakan AWS Network Security Manager.
3. [Tutorial: Menyebarakan perlindungan keamanan jaringan pertama Anda](#)— Berjalanlah melalui tutorial ujung ke ujung yang membuat penerapan pertama Anda.

# Bagaimana AWS Manajer Keamanan Jaringan bekerja

Gunakan model sumber daya Manajer Keamanan AWS Jaringan untuk merancang dan mengelola perlindungan keamanan jaringan untuk sumber daya dalam satu akun atau di beberapa akun di organisasi Anda. Bab ini menjelaskan lima jenis sumber daya, bagaimana mereka membentuk hierarki, dan konsep-konsep kunci yang mengatur perilaku mereka.

## AWS Model sumber daya Manajer Keamanan Jaringan

AWS Network Security Manager menggunakan lima jenis sumber daya yang diatur dalam hierarki komposisi:



Sumber daya saling mereferensikan ke atas melalui hierarki. Aturan digunakan dalam templat dan kebijakan. Template, aturan, atau keduanya digunakan dalam kebijakan. Lingkup mereferensikan sumber daya yang dilindungi kebijakan dalam penerapan.

Bagian berikut menjelaskan setiap jenis sumber daya dalam hierarki.

Aturan — Unit atom konfigurasi keamanan jaringan. Ada dua jenis aturan — aturan inspeksi lalu lintas dan aturan konfigurasi firewall. Inspeksi lalu lintas berfokus pada bagaimana layanan keamanan menangani lalu lintas. Aturan konfigurasi menentukan operasi sistem di luar inspeksi lalu lintas. Struktur aturan bervariasi menurut jenis firewall.

**Template** — Kelompok aturan yang dipesan dan dapat digunakan kembali untuk satu jenis firewall. Gunakan templat untuk mengemas aturan terkait bersama-sama dan membagikannya di beberapa kebijakan. Template bersifat opsional.

**Kebijakan** — Menggabungkan serangkaian templat dan aturan yang diurutkan dengan pengaturan penegakan untuk jenis firewall. Setiap kebijakan membawa prioritas (angka yang lebih rendah menunjukkan prioritas yang lebih tinggi). Ketika beberapa kebijakan melindungi sumber daya yang sama, prioritas menentukan bagaimana konflik diselesaikan. Untuk aturan inspeksi lalu lintas, prioritas menentukan urutan di mana aturan dikumpulkan. Untuk aturan konfigurasi firewall, prioritas menentukan konfigurasi mana yang berlaku untuk setiap sumber daya dan kebijakan dalam cakupannya.

**Lingkup** — Pilihan deklaratif di mana perlindungan berlaku. Lingkup menentukan jenis sumber daya mana yang harus dilindungi, dan Anda dapat memfilter sumber daya secara opsional berdasarkan tag atau atribut konfigurasi. Dalam mode multi-akun, ruang lingkup juga menentukan akun atau OU mana yang akan disertakan atau dikecualikan. Dalam mode akun tunggal, ruang lingkup berlaku untuk akun itu sendiri. Mode lingkup diperbaiki saat Anda membuatnya. Anda tidak dapat mengganti ruang lingkup antara mode multi-akun dan akun tunggal di kedua arah, sehingga cakupan multi-akun tidak akan pernah menjadi cakupan akun tunggal, atau sebaliknya.

**Deployment** - Mengikat satu atau beberapa kebijakan ke ruang lingkup. Menerbitkan penyebaran mengaktifkan penegakan hukum. AWS Manajer Keamanan Jaringan menemukan sumber daya dalam ruang lingkup, menghitung konfigurasi yang dimaksudkan, dan secara opsional memulihkan sumber daya yang tidak sinkron.

Untuk batas komposisi sumber daya, lihat [Kuota](#).

## AWS Siklus hidup sumber daya Manajer Keamanan Jaringan, penggabungan, dan sinkronisasi

Bagian berikut menjelaskan perilaku dan mekanisme yang mengatur cara sumber daya Manajer Keamanan AWS Jaringan beroperasi setelah Anda membuatnya.

### Draf dan siklus hidup aktif

Setiap sumber daya Manajer Keamanan AWS Jaringan — termasuk aturan, templat, kebijakan, cakupan, dan penerapan — memiliki status Draf atau Aktif:

- **Aktif** — Status default. Sumber daya diterbitkan dan tersedia untuk digunakan. Sumber daya lain dapat mereferensikannya, dan penerapan yang menyertakannya menegakkan konfigurasinya.
- **Draf** — Sumber daya disimpan tetapi belum aktif. Sumber daya draf tidak ditegakkan dan tidak dapat direferensikan oleh sumber daya lain. Saat Anda membuat atau memperbarui sumber daya, pilih Simpan draf agar tetap dalam status draf.

Secara default, Manajer Keamanan AWS Jaringan membuat sumber daya sebagai Aktif. Untuk membuat sumber daya sebagai Draft menggunakan API, setel `isPublished` parameter ke `false` dalam operasi buat atau perbarui.

Saat Anda memperbarui sumber daya, skenario berikut berlaku:

| Keadaan saat ini | Tindakan           | Hasil                                                                  |
|------------------|--------------------|------------------------------------------------------------------------|
| Draf             | Pilih Simpan draf  | Perbarui draf (tetap Draf)                                             |
| Draf             | Pilih Publikasikan | Publikasikan draf (menjadi Aktif)                                      |
| Aktif            | Pilih Publikasikan | Perbarui dan tetap aktif (Aktif)                                       |
| Aktif            | Pilih Simpan draf  | Buat hamparan draf (menjadi Draf dengan sumber daya Aktif di bawahnya) |

`hasPublishedVersion` Bidang muncul di daftar dan mendapatkan tanggapan. Bidang ini memberi tahu Anda apakah sumber daya Aktif yang diterbitkan ada di bawah draf. Ketika sumber daya memiliki status Draf dan `hasPublishedVersion: true`, draf yang tertunda berada di atas sumber daya Aktif yang diterbitkan secara langsung.

Anda tidak dapat menghapus sumber daya Aktif yang referensi sumber daya Aktif lainnya.

## Penentuan versi

Setiap sumber daya Manajer Keamanan AWS Jaringan — termasuk aturan, templat, kebijakan, cakupan, dan penerapan — dapat dibuat versi. Untuk membuat versi sumber daya Aktif, pilih sumber daya, pilih Tindakan, lalu pilih Buat snapshot berversi. Versi tidak dibuat secara otomatis pada setiap pembaruan.

### AWS CLI alternatif

Anda juga dapat membuat versi menggunakan operasi `Create{Resource}Snapshot` API pada sumber daya Aktif.

Properti versi kunci:

- Setiap versi memiliki nomor unik (bilangan bulat berurutan) dan ARN yang memenuhi syarat versi (misalnya,). `arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`
- Versi tidak dapat diubah. Mereka tidak dapat diperbarui.
- Anda dapat membuat hingga 10 versi per sumber daya.
- Versi dapat diberi tag.

Gunakan versi untuk mempertahankan varian konfigurasi yang diinginkan. Untuk memutar kembali sumber daya, baca versi, lalu perbarui sumber daya langsung dengan konfigurasi versi yang diinginkan.

## Priority-based penggabungan kebijakan

Ketika beberapa kebijakan melindungi sumber daya yang sama, AWS Network Security Manager menggabungkan konfigurasinya menjadi satu hasil. Angka prioritas yang lebih rendah menunjukkan prioritas yang lebih tinggi (prioritas 1 lebih diutamakan daripada prioritas 2). Ketika AWS Network Security Manager menggabungkan kebijakan yang berisi aturan inspeksi lalu lintas, prioritas menentukan urutan di mana aturan digabungkan. Untuk aturan konfigurasi firewall, kebijakan prioritas tinggi menentukan konfigurasi mana yang berlaku.

AWS Manajer Keamanan Jaringan mengevaluasi prioritas pada dua tingkat, dalam urutan ini:

1. Prioritas administrator — Manajer Keamanan AWS Jaringan mengevaluasi prioritas administrator terlebih dahulu. Setiap administrator organisasi diberi prioritas, seperti yang dijelaskan dalam [the section called “Akun administrator dan anggota”](#). Ketika AWS Network Security Manager menggabungkan kebijakan, itu memberi peringkat kebijakan administrator lebih tinggi daripada kebijakan akun tunggal akun anggota itu sendiri. Jika kebijakan administrator dan kebijakan akun tunggal akun anggota berlaku untuk sumber daya dan konflik, konfigurasi kebijakan administrator

akan menang. Akun anggota tidak dapat memilih keluar, mengganti, atau membebaskan dirinya dari kebijakan administrator.

2. Prioritas kebijakan — Dalam setiap akun, Manajer Keamanan AWS Jaringan kemudian menggunakan prioritas kebijakan untuk menyelesaikan konflik yang tersisa. Nilai prioritas kebijakan adalah bilangan bulat mulai dari 1 dan harus unik per akun.

Anda menetapkan prioritas administrator dengan `priority` bidang yang diperlukan pada `PutAdminAccount` operasi, bilangan bulat dari 1 hingga 10. Nilai prioritas adalah unik, sehingga dua administrator tidak pernah berbagi prioritas dan tidak diperlukan tie-breaking. Untuk informasi selengkapnya, lihat [Referensi API AWS Network Security Manager](#).

Hasil gabungan dari semua kebijakan yang berlaku untuk sumber daya adalah konfigurasi firewall yang efektif. AWS Network Security Manager menghitung konfigurasi ini, membandingkannya dengan konfigurasi sumber daya yang sebenarnya, dan melaporkan perbedaan apa pun sebagai status sinkronisasi.

Ketika kebijakan bertentangan, Manajer Keamanan AWS Jaringan membandingkan setiap atribut dan menerapkan nilai dari kebijakan prioritas yang lebih tinggi. Jika kebijakan prioritas lebih tinggi tidak menentukan atribut, nilai kebijakan prioritas rendah akan berlaku. Sumber daya yang cocok dengan konfigurasi efektif adalah `IN_SYNC`. Sumber daya yang dilindungi oleh kebijakan prioritas rendah yang pengaturannya diganti oleh laporan kebijakan prioritas lebih tinggi sebagai `OUT_OF_SYNC` untuk penerapan dengan prioritas lebih rendah. Ini adalah perilaku yang diharapkan, bukan kegagalan.

## Penemuan sumber daya dengan AWS Config

AWS Manajer Keamanan Jaringan menemukan sumber daya yang dilindungi di akun Anda menggunakan perekam AWS konfigurasi Config terkait layanan. Perekam ini dibuat secara otomatis di setiap akun saat akun tersebut memasuki ruang lingkup penerapan. Tidak seperti AWS Firewall Manager, Anda tidak perlu melakukan pengaturan tambahan apa pun. AWS Penggunaan Config oleh AWS Network Security Manager tidak dibebankan kepada pelanggan AWS Network Security Manager.

Karakteristik utama dari perekam terkait layanan:

- Itu dinamai `AWSConfigurationRecorderForNetworkSecurityManager`.
- Ini terpisah dari perekam konfigurasi yang dikelola pelanggan di akun.
- Ini hanya mencatat jenis sumber daya yang relevan dengan cakupan dan penerapan aktif Anda.

- Anda tidak perlu mengatur AWS Config atau membuat perekam konfigurasi. AWS Manajer Keamanan Jaringan mengelola ini secara otomatis. AWS Penggunaan Config oleh AWS Network Security Manager tidak dibebankan kepada pelanggan.
- Anda tidak dapat memodifikasi atau menghapus perekam saat sedang digunakan. AWS Network Security Manager mengelola siklus hidupnya secara otomatis.

Anda tidak perlu mengaktifkan atau mengkonfigurasi AWS Config secara manual agar AWS Network Security Manager berfungsi. Layanan menangani penemuan sumber daya secara otomatis setelah Anda memublikasikan penerapan.

## Sinkronisasi dan remediasi

Penegakan di Manajer Keamanan AWS Jaringan tidak sinkron dan akhirnya konsisten. Setelah Anda memublikasikan penerapan, atau saat sumber daya berubah, tahapan berikut akan terjadi:

1. Penemuan sumber daya — Manajer Keamanan AWS Jaringan menemukan sumber daya dalam ruang lingkup menggunakan perekam AWS Config terkait layanan.
2. Perhitungan konfigurasi — Untuk setiap sumber daya yang ditemukan, AWS Network Security Manager menghitung konfigurasi firewall yang efektif dengan menggabungkan semua kebijakan yang berlaku berdasarkan prioritas.
3. Evaluasi sinkronisasi — Manajer Keamanan AWS Jaringan membandingkan konfigurasi efektif dengan konfigurasi aktual sumber daya dan mencatat status sinkronisasi.
4. Remediasi (opsional) — Jika Anda menetapkan `remediationEnabled` kebijakan, AWS Network Security Manager mengoreksi sumber daya yang tidak sinkron agar sesuai dengan konfigurasi yang efektif.

Setiap tahap asinkron. Konsekuensi untuk alur kerja Anda:

- Ada penundaan antara penerbitan penyebaran dan sumber daya menjadi dilindungi.
- Ada penundaan antara membuat sumber daya baru dalam ruang lingkup dan dilindungi.
- `Last CheckedStempel` waktu pada entri status sinkronisasi memberi tahu Anda kapan Manajer Keamanan AWS Jaringan terakhir mengevaluasi sumber daya.

Remediasi dan pembersihan sumber daya adalah pengaturan tingkat kebijakan. Anda mengonfigurasi masing-masing per kebijakan di `policyConfiguration` objek.

## `remediationEnabled`

Menentukan apakah Manajer Keamanan AWS Jaringan secara otomatis memulihkan sumber daya yang tidak sesuai. Saat Anda mengaktifkan setelan ini, AWS Network Security Manager mengoreksi sumber daya yang tidak sinkron agar sesuai dengan konfigurasi yang efektif.

## `resourcesCleanUp`

Menentukan apakah AWS Network Security Manager secara otomatis menghapus sumber daya yang dibuat ketika mereka tidak lagi diperlukan. AWS Network Security Manager menghapus firewall yang dibuat saat Anda menghapus penyebaran, atau ketika akun atau sumber daya keluar dari cakupan.

Pengaturan `remediationEnabled` dan `resourcesCleanUp` pengaturan keduanya default ke `false`. AWS Network Security Manager tidak memperbaiki atau membersihkan sumber daya sampai Anda mengaktifkan pengaturan ini. `policyConfigurationObjek` juga berlaku `wafConfig`, yang berlaku untuk kebijakan AWS WAF. Untuk informasi selengkapnya, lihat [Referensi API AWS Network Security Manager](#).

Saat sumber daya tidak sinkron, status sinkronisasi menyertakan alasan tidak sinkron dengan detail per setelan yang menunjukkan nilai yang diharapkan dibandingkan dengan nilai aktual. Alasannya diatur ke dalam kategori berikut:

- `missingFirewall`— Tidak ada perlindungan firewall yang terkait dengan sumber daya.
- `invalidFirewall`— Firewall ada tetapi konfigurasinya berbeda dari konfigurasi yang efektif. Ini termasuk enam ember `detail:incorrectSingleValueConfigurations`, `missingAppendableConfigurationValues`, `incorrectAppendableConfigurationOrder`, `missingMergeableConfigurationValues`, dan `unexpectedMergeableConfigurationValues`.

Jika remediasi diaktifkan tetapi Manajer Keamanan AWS Jaringan tidak dapat memperbaiki sumber daya, `remediationIssues` bidang menyediakan `issueType`, `message` menjelaskan masalah, dan `correctiveAction` menyarankan cara mengatasinya.

AWS Network Security Manager tidak mengevaluasi pengaturan yang tidak dikelola. Jika bidang tidak muncul dalam aturan kontribusi apa pun, Manajer Keamanan AWS Jaringan mengabaikannya selama evaluasi sinkronisasi.

## Akun administrator dan anggota

AWS Network Security Manager menggunakan model manajemen lintas akun yang dibangun di atas AWS Organizations:

- Akun Administrator — Akun tempat Anda membuat dan mengelola sumber daya Manajer Keamanan AWS Jaringan (aturan, templat, kebijakan, cakupan, dan penerapan). Anda menetapkan satu atau lebih akun administrator, masing-masing dengan prioritas dari 1 hingga 10.
- Akun anggota — Akun tempat Manajer Keamanan AWS Jaringan menemukan sumber daya, mengevaluasi status sinkronisasi, dan secara opsional memperbaiki konfigurasi yang tidak sinkron. AWS Manajer Keamanan Jaringan bertindak dalam akun anggota melalui peran terkait layanan. Untuk informasi selengkapnya, lihat [the section called “Service-linked peran”](#).

Anda dapat secara opsional mencakup setiap administrator ke subset akun, OU, dan jenis firewall. Gunakan kemampuan ini untuk mendelegasikan pengelolaan area tertentu ke tim yang berbeda.

AWS Network Security Manager adalah layanan regional. Anda membuat sumber daya dan penerapan per Wilayah tanpa dependensi lintas wilayah.

## Service-linked peran

AWS Manajer Keamanan Jaringan menggunakan peran terkait layanan IAM yang diberi nama `AWSServiceRoleForNetworkSecurityManager` untuk bertindak di akun anggota organisasi Anda atas nama Anda. Peran ini mempercayai kepala `network-security-manager.amazonaws.com` layanan. Ini menggunakan kebijakan yang `NetworkSecurityManagerServiceRolePolicy` AWS dikelola.

AWS Network Security Manager membuat peran ini secara otomatis saat Anda mengaktifkan layanan, sehingga tidak ada pengaturan manual. Peran ini memungkinkan Manajer Keamanan AWS Jaringan mengelola perlindungan AWS WAF dan AWS Shield Advanced, menemukan sumber daya yang dilindungi melalui AWS Config, dan melakukan operasi lintas akun. Lihat informasi yang lebih lengkap di [the section called “Service-linked peran”](#).

# Pengaturan AWS Manajer Keamanan Jaringan

Dengan AWS Network Security Manager, Anda dapat bekerja dalam dua model organisasi. Gunakan secara langsung dalam satu akun, atau gunakan dengan AWS Organizations untuk mengelola perlindungan di beberapa akun. Langkah-langkah pengaturan tergantung pada model yang Anda pilih.

## Topik

- [Pilih model organisasi Anda](#)
- [Menyiapkan untuk penggunaan akun tunggal](#)
- [Menyiapkan untuk penggunaan multi-akun dengan AWS Organizations](#)
- [Membuat AWS Akun administrator Manajer Keamanan Jaringan](#)
- [Buat identitas IAM dengan AWS Izin Manajer Keamanan Jaringan](#)
- [Penggunaan AWS Manajer Keamanan Jaringan di Wilayah yang dinonaktifkan secara default](#)

## Pilih model organisasi Anda

Pilih dari model organisasi berikut:

- **Single-account**— Gunakan Manajer Keamanan AWS Jaringan untuk melindungi sumber daya dalam satu akun. Anda tidak memerlukan AWS Organizations atau akun administrator. Buat identitas IAM dengan izin Manajer Keamanan AWS Jaringan dan mulai gunakan layanan secara langsung. AWS Manajer Keamanan Jaringan secara otomatis membuat peran terkait layanan di akun Anda.
- **Multi-account**— Gunakan AWS Network Security Manager with AWS Organizations untuk melindungi sumber daya di beberapa akun. Mode ini memerlukan pengaturan AWS Organizations, mengaktifkan akses tepercaya, dan membuat akun administrator.

## Menyiapkan untuk penggunaan akun tunggal

Untuk menggunakan AWS Network Security Manager dalam satu akun, buat identitas IAM dengan izin yang sesuai dan mulailah menggunakan layanan secara langsung. Anda tidak perlu membuat akun administrator. AWS Manajer Keamanan Jaringan secara otomatis membuat peran terkait

layanan di akun Anda di latar belakang. Loncat ke [the section called “Buat identitas IAM dengan AWS IZIN Manajer Keamanan Jaringan”](#).

## Menyiapkan untuk penggunaan multi-akun dengan AWS Organizations

Untuk mengelola perlindungan di beberapa akun, buat keanggotaan dan konfigurasi AWS Organizations yang diperlukan.

1. Pilih akun yang akan digunakan sebagai administrator Manajer Keamanan AWS Jaringan untuk organisasi — Ini adalah akun tempat Anda membuat dan mengelola sumber daya Manajer Keamanan AWS Jaringan.
2. Verifikasi keanggotaan organisasi — Jika akun yang Anda pilih belum menjadi anggota organisasi, mintalah untuk bergabung. Ikuti panduan di [Mengundang AWS akun untuk bergabung dengan organisasi Anda](#) di Panduan Pengguna AWS Organizations.
3. Aktifkan semua fitur di organisasi Anda — AWS Organizations memiliki dua set fitur yang tersedia: fitur penagihan terkonsolidasi dan semua fitur. Untuk menggunakan AWS Network Security Manager, organisasi Anda harus diaktifkan untuk semua fitur. Jika organisasi Anda dikonfigurasi hanya untuk penagihan gabungan, ikuti panduan di [Mengaktifkan semua fitur di organisasi Anda di Panduan Pengguna AWS Organizations](#).
4. Aktifkan akses tepercaya untuk AWS Network Security Manager — Aktifkan akses tepercaya untuk AWS Network Security Manager in AWS Organizations. Dengan mengaktifkan akses tepercaya, Manajer Keamanan AWS Jaringan dapat membuat peran terkait layanan di akun anggota dan mengelola sumber daya atas nama mereka.
5. Daftarkan akun administrator yang didelegasikan — Daftarkan akun pilihan Anda sebagai administrator yang didelegasikan untuk Manajer Keamanan AWS Jaringan di Organizations AWS . Gunakan akun manajemen Organisasi untuk menyelesaikan langkah ini.

### Multi-account perlindungan dinonaktifkan saat mematikan akses tepercaya

Jika Anda menonaktifkan akses tepercaya untuk AWS Network Security Manager di AWS Organizations, atau Anda membatalkan pendaftaran akun administrator yang didelegasikan, AWS Network Security Manager akan menetapkan cakupan dan penerapan multi-akun ke DISABLED status dan membersihkan perlindungan yang dikelola.

# Membuat AWS Akun administrator Manajer Keamanan Jaringan

Langkah ini hanya berlaku untuk mode multi-akun. Hanya akun manajemen organisasi yang dapat membuat akun administrator Manajer Keamanan AWS Jaringan.

Setelah menyelesaikan penyiapan Organizations, daftarkan akun Anda sebagai administrator AWS Network Security Manager. Anda dapat melakukan ini dari konsol atau antarmuka baris AWS perintah (AWS CLI).

Saat Anda membuat akun administrator, Manajer Keamanan AWS Jaringan secara otomatis membuat peran terkait layanan di semua akun di organisasi Anda. Dengan peran ini, Manajer Keamanan AWS Jaringan menemukan sumber daya dan mengelola perlindungan di akun anggota.

Dengan AWS Network Security Manager, Anda dapat memiliki beberapa administrator yang mengelola sumber daya firewall organisasi Anda. Jika ingin menggunakan beberapa administrator di organisasi, Anda dapat menerapkan kondisi lingkup administratif ke setiap administrator untuk menentukan sumber daya yang dapat mereka kelola. Ini memberi Anda fleksibilitas untuk memiliki peran administrator yang berbeda dalam organisasi Anda dan membantu Anda mempertahankan prinsip akses yang paling tidak istimewa. Misalnya, satu administrator dapat mengelola satu set unit organisasi (OU). Administrator lain hanya dapat mengelola jenis kebijakan tertentu.

Untuk jumlah maksimum administrator yang dapat Anda miliki per organisasi, lihat [Kuota](#).

## Registrasi wilayah

Anda mendaftarkan akun administrator Manajer Keamanan AWS Jaringan di satu AWS Wilayah. Untuk menggunakan Manajer Keamanan AWS Jaringan di Wilayah tambahan, ulangi langkah ini di setiap Wilayah.

Untuk membuat akun administrator menggunakan konsol

1. Buka konsol Manajer Keamanan AWS Jaringan di <https://console.aws.amazon.com/network-security-manager/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih Tambahkan administrator.
4. Pilih akun dan masukkan nilai prioritas (1 hingga 10).
5. Pilih Tambahkan administrator untuk mengonfirmasi.

Untuk membuat akun administrator menggunakan AWS CLI

Panggil PutAdminAccount operasi. Anda harus memberikan nilai prioritas (1 hingga 10).

Contoh AWS CLI berikut mendaftarkan akun sebagai administrator Manajer Keamanan AWS Jaringan dengan prioritas 1:

```
aws network-security-manager put-admin-account \  
  --account-id 123456789012 \  
  --priority 1
```

Anda dapat menunjuk beberapa akun administrator, masing-masing dengan prioritas yang berbeda. Secara opsional, Anda dapat membatasi setiap administrator ke akun tertentu, OU, atau jenis firewall dengan memberikan adminScope parameter.

Untuk menghapus akun administrator menggunakan konsol

 Multi-account perlindungan dinonaktifkan saat menghapus administrator

Saat Anda menghapus akun administrator, Manajer Keamanan AWS Jaringan menetapkan cakupan dan penerapan multi-akun ke DISABLED status dan membersihkan perlindungan yang dikelolanya.

1. Buka konsol Manajer Keamanan AWS Jaringan di <https://console.aws.amazon.com/network-security-manager/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih akun administrator yang ingin Anda hapus.
4. Pilih Hapus administrator.
5. Untuk mengonfirmasi, pilih Konfirmasi penghapusan administrator.

## Buat identitas IAM dengan AWS Izin Manajer Keamanan Jaringan

Untuk menggunakan AWS Network Security Manager, Anda memerlukan identitas IAM (pengguna atau peran) dengan izin untuk memanggil operasi Manajer Keamanan AWS Jaringan. Tindakan IAM menggunakan awalnnetwork-security-manager.

Contoh berikut kebijakan IAM berisi tiga pernyataan. Pernyataan pertama memberikan akses penuh ke semua operasi Manajer Keamanan AWS Jaringan. Pernyataan kedua memberikan izin AWS Organizations dan AWS WAF tambahan yang dibutuhkan AWS Network Security Manager. AWS Network Security Manager menggunakan izin ini untuk mengidentifikasi akun dan unit organisasi (OU) di organisasi Anda dan untuk mencantumkan grup aturan WAF yang tersedia dan produk terkelola. Izin ini juga memungkinkan AWS Network Security Manager mengaktifkan akses tepercaya dan mendaftarkan administrator yang didelegasikan di Organizations AWS . Pernyataan ketiga memberikan `iam:CreateServiceLinkedRole` izin yang dibutuhkan Manajer Keamanan AWS Jaringan untuk membuat peran terkait layanan, yang diperlukan untuk penggunaan akun tunggal dan multi-akun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "network-security-manager:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:DescribeAllManagedProducts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*"
    }
  ]
}
```

```
}
```

Untuk penggunaan produksi, kami sarankan Anda hanya memberikan izin minimum yang diperlukan. Untuk informasi selengkapnya, lihat [the section called “Manajemen identitas dan akses”](#).

## Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat [Memulai dengan Akun AWS](#) di Panduan AWS Account Management Referensi.

## Penggunaan AWS Manajer Keamanan Jaringan di Wilayah yang dinonaktifkan secara default

Untuk menggunakan Manajer Keamanan AWS Jaringan di Wilayah yang dinonaktifkan secara default, Anda harus mengaktifkan Wilayah untuk akun manajemen organisasi Anda dan akun administrator Manajer Keamanan AWS Jaringan. Untuk informasi tentang Wilayah yang dinonaktifkan secara default dan cara mengaktifkannya, lihat [Mengelola AWS Wilayah](#) di Referensi AWS Umum.

Untuk mengaktifkan Wilayah yang dinonaktifkan

Untuk akun manajemen Organizations dan akun administrator AWS Network Security Manager, ikuti panduan di [Mengaktifkan Wilayah](#) di Referensi AWS Umum.

# Terapkan perlindungan keamanan jaringan pertama Anda

Tutorial ini memandu Anda melalui penerapan ACL web AWS WAF menggunakan konsol AWS Network Security Manager. Anda menyelesaikan langkah-langkah berikut:

1. Buat aturan
2. Buat template
3. Buat kebijakan
4. Buat ruang lingkup
5. Membuat dan mempublikasikan penyebaran
6. Memantau status sinkronisasi

Dalam tutorial ini, Anda membuat ACL web AWS WAF yang melindungi Application Load Balancers di seluruh akun yang Anda pilih. Proses ini sebagian besar identik untuk semua layanan keamanan dan firewall yang didukung oleh AWS Network Security Manager.

Waktu untuk menyelesaikan: sekitar 10 menit

Biaya: Tutorial ini menggunakan AWS layanan yang mungkin dikenakan biaya. Untuk harga saat ini, lihat [harga Manajer Keamanan AWS Jaringan](#) di AWS situs web.

## Prasyarat

Sebelum memulai, verifikasi bahwa Anda memenuhi persyaratan berikut:

- Langkah-langkah persiapan yang diselesaikan seperti yang dijelaskan dalam [Menyiapkan Manajer Keamanan AWS Jaringan](#).
- AWS Identitas dan Manajemen Akses (IAM) and Access Management (IAM) dengan izin Manajer Keamanan AWS Jaringan.
- AWS Organisasi Organizations dengan semua fitur diaktifkan dan akun administrator AWS Network Security Manager yang ditunjuk (diperlukan untuk penerapan multi-akun).
- Akses ke konsol Manajer Keamanan AWS Jaringan.

## Langkah 1: Buat aturan

Aturan adalah blok bangunan konfigurasi keamanan Anda. Pada langkah ini, Anda membuat dua aturan AWS WAF: satu yang menetapkan tindakan default dan satu yang menetapkan konfigurasi visibilitas. Tindakan Default dan VisibilityConfig merupakan bidang wajib untuk ACL web AWS WAF.

Untuk membuat aturan Tindakan Default, ikuti langkah-langkah berikut:

1. Buka konsol Manajer Keamanan AWS Jaringan di <https://console.aws.amazon.com/network-security-manager/>.
2. Di panel navigasi, pilih Ikhtisar.
3. Pada halaman Ikhtisar, pilih Buat aturan.
4. Untuk nama Aturan, masukkan nama deskriptif, seperti `my-default-action-rule`.
5. Di bagian Definisi aturan, untuk jenis Firewall, pilih AWS WAF.
6. Untuk Pilih jenis aturan, pilih Konfigurasi.
7. Pilih Sisipkan jenis konfigurasi, lalu pilih Tindakan Default. Editor JSON muncul dengan konfigurasi default.
8. Di editor JSON, hapus Block bagian dan simpan hanya Allow bagian itu.
9. Pilih Buat aturan.

Untuk membuat VisibilityConfig aturan, ikuti langkah-langkah ini:

1. Di panel navigasi, pilih Ikhtisar.
2. Pada halaman Ikhtisar, pilih Buat aturan.
3. Untuk nama Aturan, masukkan nama deskriptif, seperti `my-visibility-config-rule`.
4. Di bagian Definisi aturan, untuk jenis Firewall, pilih AWS WAF.
5. Untuk Pilih jenis aturan, pilih Konfigurasi.
6. Pilih Sisipkan jenis konfigurasi, lalu pilih VisibilityConfig. Editor JSON muncul dengan konfigurasi default.
7. Pilih Buat aturan.

### AWS CLI alternatif

Anda juga dapat membuat aturan dengan AWS CLI:

```
aws network-security-manager create-rule \  
  --rule-name "my-default-action-rule" \  
  --firewall-type WAF \  
  --rule-type CONFIGURATION \  
  --configuration '{"DefaultAction": {"Allow": {}}}' \  
  --is-published true  
  
aws network-security-manager create-rule \  
  --rule-name "my-visibility-config-rule" \  
  --firewall-type WAF \  
  --rule-type CONFIGURATION \  
  --configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true, \  
    "CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \  
  --is-published true
```

## Langkah 2: Buat template

Template mengelompokkan satu atau beberapa aturan untuk digunakan kembali di seluruh kebijakan. Pada langkah ini, Anda membuat template yang menyertakan aturan dari Langkah 1:

1. Di panel navigasi, pilih Ikhtisar.
2. Pada halaman Ikhtisar, pilih Buat template.
3. Untuk nama Template, masukkan nama deskriptif, seperti `my-waf-template`.
4. Untuk jenis Firewall, pilih AWS WAF.
5. Di bagian Aturan, pilih Tambahkan aturan dan pilih aturan yang Anda buat di Langkah 1.
6. Pilih Buat templat.

### AWS CLI alternatif

Anda juga dapat membuat template dengan AWS CLI:

```
aws network-security-manager create-template \  
  --template-name "my-waf-template" \  
  --firewall-type WAF \  
  --associated-rule-list '[{"ruleIdentifier": "rule-arn-from-step-1"}]' \  
  --is-published true
```

```
--is-published true
```

## Langkah 3: Buat kebijakan

Kebijakan menggabungkan templat dengan pengaturan penegakan hukum. Pada langkah ini, Anda membuat kebijakan yang mereferensikan template Anda dan mengaktifkan remediasi otomatis:

1. Di panel navigasi, pilih Ikhtisar.
2. Pada halaman Ikhtisar, pilih Buat kebijakan.
3. Untuk nama Kebijakan, masukkan nama deskriptif, seperti `my-waf-policy`.
4. Untuk jenis Firewall, pilih AWS WAF.
5. Di bagian Prioritas kebijakan, kebijakan yang ada dan prioritasnya ditampilkan. Tinjau prioritas kebijakan baru. Jika Anda perlu menyesuaikannya, pilih bidang prioritas dan ubah nilainya menjadi 1 atau nomor prioritas yang tidak digunakan.
6. Di bagian Templat dan aturan, pilih Tambahkan templat dan pilih templat yang Anda buat di Langkah 2.
7. Untuk Remediasi, pilih Diaktifkan.
8. Untuk resolusi ACL web pelanggan yang ada, pilih Tidak ada remediasi.
9. Pilih Buat kebijakan.

### AWS CLI alternatif

Anda juga dapat membuat kebijakan dengan AWS CLI:

```
aws network-security-manager create-policy \  
  --policy-name "my-waf-policy" \  
  --firewall-type WAF \  
  --priority 1 \  
  --associated-template-and-rule-list '[{"templateIdentifier": "template-arn-  
from-step-2"}]' \  
  --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":  
false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \  
  --is-published true
```

## Langkah 4: Buat ruang lingkup

Lingkup menentukan di mana perlindungan Anda berlaku. Pada langkah ini, Anda membuat cakupan yang menargetkan Application Load Balancers di akun Anda:

1. Di panel navigasi, pilih Ikhtisar.
2. Pada halaman Ikhtisar, pilih Buat ruang lingkup.
3. Untuk nama Scope, masukkan nama deskriptif, seperti `my-alb-scope`.
4. (Opsional) Di bagian Pemilihan unit akun dan organisasi, untuk Pilih metode pengendalian ruang lingkup administratif, pilih Lingkup untuk seluruh AWS Organisasi (semua OU dan akun). Lewati langkah ini untuk penerapan akun tunggal.
5. Di bagian Resources, untuk tipe Resource, pilih Application Load Balancer.
6. Pilih Buat ruang lingkup.

### AWS CLI alternatif

Anda juga dapat membuat cakupan dengan AWS CLI:

```
aws network-security-manager create-scope \  
  --scope-name "my-alb-scope" \  
  --scope-configuration '{  
    "accountFilter": {"includeAll": {}},  
    "resourceScopes": {  
      "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {  
        "includeAll": true  
      }  
    }  
  }' \  
  --is-published true
```

## Langkah 5: Buat dan publikasikan penyebaran

Penerapan mengikat kebijakan ke ruang lingkup dan mengaktifkan penegakan hukum. Untuk membuat dan mempublikasikan penerapan:

1. Di panel navigasi, pilih Ikhtisar.

2. Pada halaman Ikhtisar, pilih Buat penyebaran.
3. Untuk nama Deployment, masukkan nama deskriptif, seperti. `my-first-deployment`
4. Di bagian Kebijakan, pilih Tambahkan kebijakan dan pilih kebijakan yang Anda buat di Langkah 3.
5. Di bagian Cakupan, pilih Tambahkan cakupan dan pilih cakupan yang Anda buat di Langkah 4.
6. Pilih Buat penerapan.

AWS Manajer Keamanan Jaringan mulai menemukan sumber daya dan menerapkan perlindungan. Proses ini tidak sinkron dan mungkin memakan waktu beberapa menit untuk menyelesaikannya.

#### AWS CLI alternatif

Anda juga dapat membuat dan mempublikasikan penerapan dengan AWS CLI:

```
aws network-security-manager create-deployment \  
  --deployment-name "my-first-deployment" \  
  --associated-policy-list '[{"policyIdentifier": "policy-arn-from-step-3"}]' \  
  \  
  --associated-scope-list '[{"scopeIdentifier": "scope-arn-from-step-4"}]' \  
  --deployment-configuration '{"enableCrossAccountVisibility": true}' \  
  --is-published true
```

## Langkah 6: Memantau status sinkronisasi

Setelah Anda mempublikasikan penerapan, Manajer Keamanan AWS Jaringan menemukan sumber daya dan menyinkronkan konfigurasinya. Untuk memantau status setiap sumber daya:

1. Di panel navigasi, pilih Ikhtisar.
2. Pilih tab Deployment.
3. Pilih penerapan yang Anda buat di Langkah 5.
4. Pilih tab Sinkronisasi.
5. Tinjau status sinkronisasi untuk setiap sumber daya:
  - **IN\_SYNC** - Konfigurasi sumber daya cocok dengan pengaturan perlindungan yang Anda inginkan.
  - **OUT\_OF\_SYNC** — Konfigurasi sumber daya tidak cocok. AWS Manajer Keamanan Jaringan memulihkan ini secara otomatis saat remediasi diaktifkan.

- NOT\_APPLICABLE — Sumber daya berada dalam cakupan tetapi tidak dapat dievaluasi oleh penerapan ini.

#### AWS CLI alternatif

Anda juga dapat memeriksa status sinkronisasi dengan AWS CLI:

```
aws network-security-manager list-resource-synchronization-statuses \
  --deployment-identifier "deployment-arn-from-step-5"
```

## Langkah 7: Bersihkan

Jika Anda tidak lagi membutuhkan sumber daya yang Anda buat, hapus sumber daya tersebut dalam urutan terbalik untuk menghentikan penegakan hukum dan menghapus perlindungan dari sumber daya dalam lingkup:

Urutan terbalik penting karena sumber daya ini saling merujuk. Untuk melihat apa yang terkait dengan sumber daya sebelum Anda menghapusnya, hubungi ListResourceAssociations ARN sumber daya tersebut. Ini mengembalikan ARN dan jenis sumber daya masing-masing sumber daya terkait. Untuk informasi selengkapnya, lihat [Referensi API AWS Network Security Manager](#).

1. Di panel navigasi, pilih Ikhtisar. Pilih tab Deployment. Pilih penerapan Anda, pilih Tindakan, lalu pilih Hapus.
2. Pilih tab Scopes. Pilih cakupan Anda, pilih Tindakan, lalu pilih Hapus.
3. Pilih tab Kebijakan. Pilih kebijakan Anda, pilih Tindakan, lalu pilih Hapus.
4. Pilih tab Template. Pilih template Anda, pilih Tindakan, lalu pilih Hapus.
5. Pilih tab Aturan. Pilih aturan Anda, pilih Tindakan, lalu pilih Hapus.

#### AWS CLI alternatif

Sebelum Anda menghapus sumber daya, periksa asosiasinya untuk merencanakan urutan penghapusan:

```
aws network-security-manager list-resource-associations \
```

```
--resource-arn "resource-arn"
```

Jika sumber daya masih memiliki asosiasi, hapus atau hapus sumber daya terkait terlebih dahulu.

Anda dapat menghapus sumber daya dengan AWS CLI dalam urutan terbalik:

```
aws network-security-manager delete-deployment \  
  --deployment-identifier "deployment-arn"  
  
aws network-security-manager delete-scope \  
  --scope-identifier "scope-arn"  
  
aws network-security-manager delete-policy \  
  --policy-identifier "policy-arn"  
  
aws network-security-manager delete-template \  
  --template-identifier "template-arn"  
  
aws network-security-manager delete-rule \  
  --rule-identifier "rule-arn"
```

## Langkah selanjutnya

Sekarang setelah Anda memiliki penerapan yang berfungsi, jelajahi cara-cara berikut untuk memperluas perlindungan keamanan jaringan Anda:

- Pelajari tentang model sumber daya dan siklus hidup di [Bagaimana AWS Network Security Manager bekerja](#)
- Gunakan draft/publish alur kerja untuk melakukan perubahan tahap sebelum diterapkan. Untuk informasi selengkapnya, lihat [the section called “Draf dan siklus hidup aktif”](#).
- Buat snapshot untuk mempertahankan konfigurasi yang diketahui baik. Untuk informasi selengkapnya, lihat [the section called “Penentuan versi”](#).
- Gunakan GenerateRuleConfiguration untuk membuat aturan dari deskripsi bahasa alami. Untuk informasi selengkapnya, lihat [Referensi API AWS Network Security Manager](#).
- Jelajahi pengelolaan perlindungan AWS WAF dan AWS Shield Advanced di seluruh organisasi Anda. Lihat informasi yang lebih lengkap di [Mengelola firewall dan layanan keamanan](#).

# Mengelola firewall dan layanan keamanan

Dengan AWS Network Security Manager, Anda menentukan dan menerapkan kebijakan keamanan untuk beberapa firewall dan layanan keamanan. Meskipun elemen umum menjangkau portofolio keamanan AWS jaringan, ada variasi penting yang perlu Anda tangani dalam Manajer Keamanan AWS Jaringan.

Untuk setiap layanan keamanan jaringan yang didukung, subbagian berikut menjelaskan elemen dan langkah unik untuk Quick Create dan proses pembuatan detail standar.

## Mengelola ACL web untuk AWS WAF

Dengan AWS Network Security Manager, Anda mengonfigurasi dan menerapkan daftar kontrol akses web AWS WAF (ACL web) secara terpusat di seluruh akun dan sumber daya di organisasi Anda. Anda dapat menentukan aturan AWS Network Security Manager untuk AWS WAF, mengelompokkannya ke dalam templat perlindungan, dan menerapkannya dalam skala besar melalui kebijakan dan penerapan AWS Network Security Manager.

## AWS Konsep WAF

Konsep berikut khusus untuk menggunakan AWS Network Security Manager dengan AWS WAF. Untuk informasi selengkapnya tentang cara kerja Manajer Keamanan AWS Jaringan, lihat [Bagaimana AWS Network Security Manager bekerja](#).

## AWS Jenis aturan WAF

Untuk AWS WAF, aturan adalah salah satu dari dua jenis:

- **INSPEKSI** - Berisi definisi grup aturan menggunakan `PreProcessFirewallManagerRuleGroups` (aturan yang berjalan sebelum aturan yang ditentukan pelanggan) atau `PostProcessFirewallManagerRuleGroups` (aturan yang berjalan setelahnya).
- **KONFIGURASI** - Berisi pengaturan konfigurasi ACL web tunggal. Konfigurasi JSON harus berisi persis satu kunci tingkat atas yang cocok dengan pengaturan yang didukung (misalnya `Description`, `DefaultAction`, `VisibilityConfig`, `LoggingConfiguration`, `CaptchaConfig`, `AssociationConfig`, `OnSourceDDoSProtectionConfig`, `TokenDomains`, atau `MonetizationConfig`).

Sebagian besar pengaturan konfigurasi ACL web sesuai dengan parameter operasi AWS WAFCreateWebACL. Untuk informasi selengkapnya tentang pengaturan ini dan definisinya, lihat [CreateWebACL di Referensi](#) API AWS WAF.

Pengecualiannya adalah LoggingConfiguration, yang Anda konfigurasikan secara terpisah. Untuk informasi selengkapnya, lihat [the section called “Pencatatan log”](#).

## AWS Penggabungan kebijakan WAF

Untuk AWS WAF, setiap pengaturan konfigurasi menggunakan salah satu strategi penggabungan berikut:

### SingleValue

Pengaturan yang hanya dapat memiliki satu nilai. Kebijakan prioritas tertinggi menang.

Nilai prioritas adalah unik, sehingga dua kebijakan tidak dapat menentukan nilai yang berbeda pada prioritas yang sama. Untuk informasi selengkapnya tentang

cara Manajer Keamanan AWS Jaringan menyelesaikan prioritas, lihat [the section called “Priority-based penggabungan kebijakan”](#) Pengaturan berikut menggunakan

SingleValue:DefaultAction,VisibilityConfig,CaptchaConfig,ChallengeConfig,OnSourceD danDescription.

### Tambahkan (dan AppendAndSort)

Entri dari semua kebijakan ditambahkan ke daftar dalam urutan prioritas.

TokenDomains dan DataProtectionConfig.DataProtections gunakan Append. PreProcessFirewallManagerRuleGroups dan

PostProcessFirewallManagerRuleGroups gunakan AppendAndSort, yang menambahkan grup aturan dari semua kebijakan dan mengurutkannya berdasarkan prioritas. Urutan penting karena AWS WAF mengevaluasi kelompok aturan secara berurutan.

### Gabungkan

Entri dari semua kebijakan bergabung menjadi satu set, terlepas dari prioritasnya.

CustomResponseBodies dan AssociationConfig.RequestBody gunakan Merge.

Strategi Append, AppendAndSort, dan Merge menghapus entri duplikat. Ketika dua kebijakan memberikan kontribusi konfigurasi yang identik, AWS Network Security Manager menyimpan entri dari kebijakan prioritas yang lebih tinggi. Oleh karena itu, konfigurasi efektif berisi satu salinan entri itu, bukan satu salinan per kebijakan kontribusi.

## Resolusi ACL web yang ada

Gunakan `existingCustomerWebACLResolution` setelan pada kebijakan AWS WAF untuk menentukan cara Manajer Keamanan AWS Jaringan menangani sumber daya yang sudah memiliki ACL web yang dikelola pelanggan:

- **RETROFIT**— Perbarui ACL web Anda yang ada untuk menyelaraskan dengan konfigurasi yang efektif.
- **OVERRIDE\_ASSOCIATION**— Kaitkan ACL web yang dikelola oleh Manajer Keamanan AWS Jaringan dengan sumber daya sebagai gantinya.
- **NO\_REMEDIATION**— Jangan memperbaiki jika ACL web Anda ada.

## Pencatatan lalu lintas ACL web

Anda mengontrol pencatatan ACL web dengan `LoggingConfiguration` pengaturan pada kebijakan. AWS Network Security Manager menerapkan pengaturan ini menggunakan `PutLoggingConfiguration` operasi AWS WAF. Anda dapat menentukan satu tujuan logging per web ACL. Untuk informasi selengkapnya, lihat [PutLoggingConfiguration](#) di Referensi API AWS WAF.

Setiap ACL web dalam lingkup yang dikelola kebijakan mengirimkan lognya ke tujuan yang ditentukan kebijakan. Ini memberi Anda pencatatan terpusat di seluruh akun di organisasi Anda. Gunakan untuk mendapatkan informasi terperinci tentang lalu lintas yang dianalisis oleh ACL web Anda di seluruh organisasi.

Untuk pencatatan terpusat di beberapa akun, Anda dapat mengirim log ke bucket Amazon S3 atau aliran pengiriman Amazon Data Firehose. Setiap jenis tujuan memerlukan konfigurasi tambahan, yang harus Anda selesaikan sebelum Manajer Keamanan AWS Jaringan dapat mengelola pencatatan AWS WAF di seluruh sumber daya dan akun dalam cakupan Anda. Nama tujuan harus dimulai dengan `aws-waf-logs-`.

## Amazon Data Firehose

Buat aliran pengiriman dengan karakteristik sebagai berikut:

- Dibuat menggunakan akun administrator AWS Network Security Manager
- Nama yang dimulai dengan `aws-waf-logs-`, misalnya `aws-waf-logs-network-security-manager-central`
- Sebuah PUT sumber

- Dibuat di Wilayah tempat Anda beroperasi, atau di Wilayah AS Timur (Virginia N.) jika Anda mengambil log untuk Amazon CloudFront

Sebelum Anda menggunakan aliran pengiriman, uji untuk mengonfirmasi bahwa ia memiliki throughput yang cukup untuk log organisasi Anda. Untuk informasi selengkapnya, lihat [Membuat aliran pengiriman Amazon Data Firehose di Panduan](#) Pengembang Amazon Data Firehose.

## Amazon S3

Buat bucket mengikuti panduan Amazon S3 di Panduan Pengembang AWS WAF. Anda juga harus mengonfigurasi bucket dengan izin yang memungkinkan pengiriman log untuk menulis ke sana. Kebijakan bucket berikut memberikan izin tersebut.

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForNetworkSecurityManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix"
    },
    {
      "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/"
    },
    {
      "Sid": "AWSLogDeliveryFullControlNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/"
    },
    {
      "Sid": "AWSLogDeliveryFullControlNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/"
    }
  ]
}
```

Ganti *bucket-suffix* dengan akhiran nama bucket Anda sendiri, dan ganti *policy-id* dengan ID kebijakan Anda.

 CloudWatch Log hanya mendukung penggunaan akun tunggal

Jika Anda menggunakan Manajer Keamanan AWS Jaringan di beberapa akun, Anda tidak dapat menggunakan grup CloudWatch log Amazon Log sebagai tujuan pencatatan. Grup log harus berada di AWS akun yang sama dan Wilayah yang sama dengan ACL web. Untuk penerapan multi-akun, gunakan bucket Amazon S3 atau aliran pengiriman Amazon Data Firehose sebagai gantinya.

## Buat Cepat untuk AWS WAF

Dengan Quick Create, Anda menentukan dan menerapkan perlindungan AWS WAF dalam satu alur kerja terpandu. Gunakan Quick Create saat Anda ingin menyiapkan perlindungan ACL web lengkap dari aturan melalui penerapan dalam satu sesi.

Untuk menentukan dan menerapkan perlindungan AWS WAF dengan Quick Create, selesaikan prosedur berikut secara berurutan.

Untuk membuat kebijakan dan menambahkan perlindungan

1. Buka konsol Manajer Keamanan AWS Jaringan di <https://console.aws.amazon.com/network-security-manager/>.
2. Di panel navigasi, pilih Ikhtisar.
3. Di kanan atas halaman Ikhtisar, pilih Buat dan terapkan cepat. Halaman Quick create and deploy muncul dengan beberapa panel.
4. Di panel Detail kebijakan, untuk Nama, masukkan nama kebijakan. (Opsional) Untuk Deskripsi, masukkan deskripsi.
5. Di panel Define protections, pilih jenis firewall yang ingin Anda gunakan. Pilih AWS WAF. Subpanel Templat dan aturan muncul, tempat Anda dapat menambahkan aturan atau templat.
6. Untuk menambahkan aturan, pilih Tambah atau kelola aturan. Di jendela yang muncul, untuk Pilih jenis aturan, pilih salah satu dari berikut ini:
  - AWS Aturan Terkelola - Tabel menunjukkan semua Aturan AWS Terkelola yang didukung AWS WAF.

- Aturan — Tabel menunjukkan grup aturan AWS WAF yang Anda miliki, selain Aturan AWS Terkelola.

Pilih kotak centang untuk aturan yang ingin ditambahkan ke kebijakan Anda. Kemudian pilih Tambahkan aturan.

7. Untuk menambahkan templat, pilih Tambahkan templat. Di jendela Add templates yang muncul, tabel menampilkan template yang tersedia. Pilih templat yang Anda inginkan, bersama dengan versi yang akan disertakan dalam kebijakan. Kemudian pilih Tambahkan templat.

## Untuk mengonfigurasi kebijakan

1. Tinjau pilihan Anda di tabel Template dan aturan. Bilangan bulat di kolom Posisi menentukan urutan evaluasi aturan dan templat. Untuk mengubah urutan evaluasi, pilih nilai posisi di kolom Posisi. Gunakan panah untuk mengubah nilainya. Untuk menerima perubahan, pilih Konfirmasi. Untuk mengembalikan perubahan, pilih Batal.
2. Di bawah Konfigurasi kebijakan di panel Tentukan perlindungan, tentukan tindakan otomatis yang diambil Manajer Keamanan AWS Jaringan dalam cakupan yang ditargetkan:
  - Remediasi menerapkan kebijakan yang ditetapkan untuk sumber daya apa pun yang status keamanannya tidak disinkronkan dengan status yang diinginkan yang dijelaskan dalam Manajer Keamanan AWS Jaringan.
  - Pembersihan sumber daya menghapus firewall yang dibuat Manajer Keamanan AWS Jaringan untuk sumber daya saat penerapan dihapus, atau ketika akun atau sumber daya berada di luar cakupan.
  - Resolusi WebACL pelanggan yang ada menentukan cara menyelesaikan konflik antara kebijakan yang Anda definisikan dan apa yang mungkin sudah diterapkan. Dari menu, pilih salah satu opsi berikut:
    - Tidak ada remediasi yang melewati remediasi pada sumber daya apa pun yang sudah memiliki ACL web.
    - Override asosiasi menggantikan ACL web yang ada dengan AWS Network Security Manager yang dibuat web ACL.
    - Retrofit memperbaiki aturannya ke setiap ACL web yang ada dan menjaga ACL web terkait dengan sumber daya.
3. Di panel Prioritas kebijakan, tetapkan prioritas. AWS Manajer Keamanan Jaringan mengevaluasi kebijakan sesuai dengan prioritas mereka untuk menyelesaikan konflik. Posisi yang lebih

rendah (bilangan bulat bawah) memiliki prioritas yang lebih tinggi. Untuk mengedit prioritas, pilih nilai Posisi. Kemudian naikan dengan panah, atau masukkan nilai secara langsung. Untuk mengonfirmasi pilihan, pilih Konfirmasi. Untuk membuang perubahan, pilih Batal.

## Untuk mengatur ruang lingkup

1. Di panel Setel cakupan, tentukan kumpulan aset yang diterapkan kebijakan tersebut. Untuk nama Scope, masukkan nama. (Opsional) Untuk Deskripsi, masukkan deskripsi.

2.

### Multi-account modus saja

Langkah ini hanya berlaku untuk mode multi-akun. Dalam mode multi-akun, gunakan sub-panel pemilihan Akun dan unit organisasi untuk memilih akun atau OU mana yang akan disertakan atau dikecualikan. Dalam mode akun tunggal, sub-panel ini tidak muncul di konsol, jadi lewati langkah ini.

Di sub-panel pemilihan unit akun dan organisasi, pilih salah satu opsi berikut:

- Ruang lingkup untuk seluruh AWS organisasi. Tidak diperlukan definisi lebih lanjut.
  - Ruang lingkup untuk seluruh AWS Organisasi tetapi tidak termasuk OU dan akun tertentu. Subpanel unit Organisasi dan sub-panel Akun muncul. Untuk mengecualikan unit organisasi, pilih Tambah OU. Pilih unit organisasi di pohon organisasi, lalu pilih Tambah OU. Untuk mengecualikan akun individual, pilih Tambah akun. Pilih akun di pohon organisasi, lalu pilih Tambah akun.
  - Jangan lingkup ke seluruh AWS Organisasi, dan hanya menyertakan OU dan akun tertentu. Gunakan mekanisme Add OU dan Add account yang sama untuk menyertakan unit organisasi dan akun yang Anda inginkan.
3. Di sub-panel Resources, untuk tipe Resource, pilih semua atau jenis sumber daya AWS WAF tertentu. Pilihannya adalah satu atau lebih dari yang berikut:
    - Penyeimbang Beban Aplikasi
    - API REST Amazon API Gateway
    - CloudFront Distribusi

### CloudFront Persyaratan wilayah

Untuk melindungi sumber daya CloudFront Distribusi, gunakan Wilayah AS Timur (Virginia Utara) (us-east-1).

### Jenis sumber daya global dan regional

Anda dapat memilih jenis sumber daya global (CloudFront Distribusi) atau jenis sumber daya regional (Application Load Balancer dan Amazon API Gateway REST API), tetapi tidak keduanya. Setelah memilih jenis sumber daya, Anda tidak dapat beralih antara CloudFront Distribusi dan tipe sumber daya regional saat memperbarui konfigurasi.

### Sumber daya yang tidak dikelola CloudFront

AWS Network Security Manager tidak mengelola CloudFront distribusi yang menggunakan paket harga CloudFront flat-rate atau CloudFront distribusi pementasan. Sumber daya ini muncul di luar sinkronisasi.

4. Untuk setiap jenis sumber daya yang dipilih, pilih salah satu opsi yang saling eksklusif berikut:
  - Sertakan semua sumber daya
  - Sertakan sumber daya tertentu
  - Kecualikan sumber daya tertentu
5. Jika Anda memilih Sertakan sumber daya tertentu, pilih salah satu jenis ekspresi berikut, lalu buat kombinasi tag atau ARN yang sesuai:
  - Kriteria tunggal
  - Cocokkan semua kriteria (DAN)
  - Cocokkan kriteria apa pun (OR)
  - TIDAK

Semua jenis sumber daya memiliki kriteria inklusi Tag dan ARN. Jika Anda memilih Tag, masukkan Kunci dan Nilai opsional. Anda dapat mengidentifikasi beberapa tag. Jika jenis sumber daya Anda adalah Application Load Balancer, kriteria Konfigurasi tambahan akan muncul. Dalam Konfigurasi, pilih Skema, yang memiliki opsi Internet-facing atau Internal.

## Untuk meninjau dan menerapkan kebijakan

1. Di panel Tinjau dan terapkan, untuk nama Deployment, masukkan nama. (Opsional) Untuk Deskripsi, masukkan deskripsi. Untuk menentukan apakah konten penerapan Anda terlihat oleh akun lain di organisasi Anda, pilih Aktifkan visibilitas lintas akun untuk penerapan ini.
2. (Opsional) Untuk menambahkan tag ke sumber daya Anda, pilih Tambahkan tag baru, lalu masukkan kombinasi Kunci dan Nilai opsional.
3. Untuk menjalankan apa yang Anda tentukan, pilih Buat dan terapkan. Ketika proses selesai, halaman Deployment muncul, di mana Anda dapat melihat detail dari apa yang dibuat.

### Penerapan mungkin dikenakan biaya

Penyebaran menciptakan layanan keamanan jaringan dan melampirkannya ke sumber daya yang dilindungi. AWS Manajer Keamanan Jaringan mengenakan biaya untuk sumber daya yang dilindungi. Layanan keamanan itu sendiri melindungi sumber daya, yang menimbulkan biaya tambahan. Sebelum Anda menerapkan, tinjau [halaman penetapan harga Manajer Keamanan AWS Jaringan dan halaman harga AWS WAF](#).

## Proses pembuatan standar untuk AWS WAF

Dengan proses pembuatan standar, Anda membuat setiap komponen AWS WAF—aturan, templat, kebijakan, cakupan, dan penerapan—secara individual untuk kontrol penuh. Gunakan pendekatan ini ketika Anda ingin membuat komponen yang dapat digunakan kembali dan menggabungkannya sesuai kebutuhan.

Kebijakan AWS WAF Manajer Keamanan AWS Jaringan dapat berisi aturan dan templat. Saat menerapkan kebijakan tersebut, AWS Network Security Manager akan membuat ACL web di setiap akun dalam lingkup.

### Untuk membuat aturan (konsol)

1. Masuk ke AWS Management Console menggunakan akun administrator AWS Network Security Manager, lalu buka konsol AWS Network Security Manager di <https://console.aws.amazon.com/network-security-manager/>.

### Penyiapan akun administrator

Untuk informasi tentang menyiapkan akun administrator Manajer Keamanan AWS Jaringan, lihat [Menyiapkan Manajer Keamanan AWS Jaringan](#).

2. Di panel navigasi, pilih AWS Network Security Manager, lalu Ikhtisar.
3. Di panel Ikhtisar, pilih Buat aturan. Masukkan nama deskriptif, lalu masukkan Deskripsi opsional.
4. Di panel Rule definition, untuk tipe Firewall, pilih AWS WAF.
5. Untuk Jenis aturan, pilih Inspeksi atau Konfigurasi.

Jika Anda memilih Inspeksi, panel editor JSON bernama Tentukan referensi grup aturan muncul dengan opsi berikut:

- Sisipkan template - Pilih template JSON untuk aturan Pertama (pra-proses) atau aturan Terakhir (pasca-proses). Ketika Anda membuat pilihan, AWS Network Security Manager menyisipkan JSON yang sesuai ke editor, bersama dengan ikon peringatan jika input diperlukan untuk melengkapi template.
- Sisipkan grup aturan - Menyajikan daftar pilihan yang didorong oleh tiga opsi:
  - Grup aturan Aturan AWS Terkelola (AMR)
  - Grup aturan kustom yang ada
  - Grup aturan AWS Marketplace

AWS Network Security Manager menyajikan grup aturan yang terkait dengan pilihan Anda, dan Anda dapat memilih satu instance untuk dimasukkan. Setelah Anda membuat pilihan, pilih Pilih grup aturan. AWS Network Security Manager menyisipkan referensi ke aturan inspeksi dengan sintaks yang benar ke editor JSON.

- Sisipkan dengan AI — Membuka jendela overlay bernama AI configuration generator. Gunakan alat ini untuk menjelaskan aturan Anda dalam bahasa sederhana, dan Manajer Keamanan AWS Jaringan menghasilkan JSON terkait di editor. Anda kemudian dapat meninjau kode yang dihasilkan dan memilih untuk menerima, memodifikasi, atau menghapus output.
6. (Opsional) Setelah definisi aturan JSON Anda selesai, Anda dapat mengaitkan tag dengan aturan Anda. Pilih Tambahkan tag baru, lalu masukkan Kunci dan Nilai opsional.
  7. Saat Anda menyelesaikan definisi, pilih Simpan draf untuk menyimpan objek yang tidak aktif dan berpotensi tidak lengkap, atau Buat aturan.

 Nama ACL Web bersifat permanen

Anda tidak dapat mengubah nama ACL web setelah Anda membuatnya. Jika Anda memperbarui nama kebijakan, AWS Network Security Manager tidak memperbarui nama ACL web terkait. Agar AWS Network Security Manager membuat ACL web dengan nama yang berbeda, Anda harus membuat kebijakan baru.

### Untuk membuat template (konsol)

Template merakit aturan dalam urutan prioritas untuk evaluasi dalam kebijakan. Anda dapat mengatur jenis aturan Anda ke dalam pengelompokan yang selaras dengan tujuan keamanan Anda. Anda juga dapat membiarkan tim yang berbeda membangun pernyataan kontrol keamanan yang selaras dengan tanggung jawab dan keterampilan mereka.

1. Pada halaman Ikhtisar, di panel Ikhtisar, pilih Buat template. Pada halaman Buat template, masukkan nama Template, masukkan Deskripsi opsional, dan pilih jenis Firewall (dalam hal ini, AWS WAF).
2. Ketika Anda memilih jenis Firewall, panel Aturan akan muncul. Pilih salah satu dari dua tombol Tambahkan aturan untuk membuka daftar aturan yang tersedia. Pilih kotak centang di sebelah kiri nama aturan untuk menambahkannya ke template. Untuk memilih versi aturan tertentu, pilih bidang Versi aturan. Jika beberapa versi tersedia, pilih versi yang Anda inginkan, lalu pilih Konfirmasi.
3. (Opsional) Buat tag untuk template. Setelah selesai, pilih Simpan draf atau Buat templat. Untuk terus membuat kebijakan, pilih Buat templat.

### Untuk membuat kebijakan (konsol)

Ini adalah langkah terakhir dari definisi kebijakan dan persiapan untuk penyebaran.

1. Pada halaman Ringkasan, di panel Ikhtisar, pilih Buat kebijakan. Pada halaman Buat kebijakan, masukkan Nama dan Deskripsi opsional, lalu pilih jenis Firewall (dalam hal ini, AWS WAF).
2. Di panel Prioritas kebijakan, tetapkan prioritas. AWS Manajer Keamanan Jaringan mengevaluasi kebijakan sesuai dengan prioritas mereka untuk menyelesaikan konflik. Posisi yang lebih rendah (bilangan bulat bawah) memiliki prioritas yang lebih tinggi. Untuk mengedit prioritas,

pilih nilai Posisi. Kemudian naikan dengan panah, atau masukkan nilai secara langsung. Untuk mengonfirmasi pilihan, pilih Konfirmasi. Untuk membuang perubahan, pilih Batal.

3. Di panel konfigurasi Kebijakan, tentukan tindakan otomatis yang diambil Manajer Keamanan AWS Jaringan dalam cakupan yang ditargetkan:
  - Remediasi menerapkan kebijakan yang ditetapkan untuk sumber daya apa pun yang status keamanannya tidak disinkronkan dengan status yang diinginkan yang dijelaskan dalam Manajer Keamanan AWS Jaringan.
  - Pembersihan sumber daya menghapus firewall yang dibuat Manajer Keamanan AWS Jaringan untuk sumber daya saat penerapan dihapus, atau ketika akun atau sumber daya berada di luar cakupan.
  - Resolusi WebACL pelanggan yang ada menentukan cara menyelesaikan konflik antara kebijakan yang Anda definisikan dan apa yang mungkin sudah diterapkan. Dari menu, pilih salah satu opsi berikut:
    - Tidak ada remediasi yang melewati remediasi pada sumber daya apa pun yang sudah memiliki ACL web.
    - Override asosiasi menggantikan ACL web yang ada dengan AWS Network Security Manager yang dibuat web ACL.
    - Retrofit memperbaiki aturannya ke setiap ACL web yang ada dan menjaga ACL web terkait dengan sumber daya.
4. Setelah pengaturan konfigurasi ini selesai, pilih aturan dan templat yang ingin ditambahkan ke kebijakan. Di panel Templat dan aturan, pilih Tambahkan aturan atau Tambahkan templat untuk mengisi kebijakan. Kedua proses membuka jendela yang beroperasi dengan cara yang sama seperti proses pemilihan aturan yang dijelaskan sebelumnya di bagian ini.

Untuk membuat ruang lingkup (konsol)

1. Anda dapat memulai langkah ini dari halaman Ikhtisar atau dari area lain di dalam alat. Di panel Rincian cakupan, masukkan nama Lingkup dan Deskripsi opsional.

2. 

 Multi-account modus saja

Langkah ini hanya berlaku untuk mode multi-akun. Dalam mode multi-akun, gunakan sub-panel pemilihan Akun dan unit organisasi untuk memilih akun atau OU mana yang akan

disertakan atau dikecualikan. Dalam mode akun tunggal, sub-panel ini tidak muncul di konsol, jadi lewati langkah ini.

Di panel pemilihan unit akun dan organisasi, pilih salah satu dari tiga metode untuk mengendalikan ruang lingkup administratif:

- Lingkup untuk seluruh AWS Organisasi (semua OU dan akun) - Tidak diperlukan definisi lebih lanjut.
  - Cakupan untuk seluruh AWS Organisasi tetapi tidak termasuk OU dan akun tertentu — Dua sub-panel muncul, satu untuk unit Organisasi dan satu untuk Akun. Pilih Tambahkan OU untuk membuka jendela Tambah OU, pilih unit organisasi yang Anda butuhkan dari pohon organisasi, lalu pilih Tambah OU. Untuk menambahkan akun individual, di sub-panel Akun, pilih Tambah akun, pilih akun dari pohon organisasi, lalu pilih Tambah akun.
  - Jangan mencakup seluruh AWS Organisasi, hanya sertakan OU dan akun tertentu — Gunakan sub-panel yang sama untuk menambahkan OU atau akun dengan mekanisme yang sama yang dijelaskan untuk opsi sebelumnya.
3. Selanjutnya, pilih sumber daya di sub-panel Sumber Daya. Di kotak pemilihan Jenis sumber daya, pilih semua atau jenis sumber daya AWS WAF tertentu. Untuk AWS WAF, opsinya adalah salah satu atau semua hal berikut:
- Penyeimbang Beban Aplikasi
  - API REST Amazon API Gateway
  - CloudFront Distribusi

#### CloudFront Persyaratan wilayah

Untuk melindungi sumber daya CloudFront Distribusi, gunakan Wilayah AS Timur (Virginia Utara) (us-east-1).

#### Jenis sumber daya global dan regional

Anda dapat memilih jenis sumber daya global (CloudFront Distribusi) atau jenis sumber daya regional (Application Load Balancer dan Amazon API Gateway REST API), tetapi tidak keduanya. Setelah memilih jenis sumber daya, Anda tidak dapat beralih antara CloudFront Distribusi dan tipe sumber daya regional saat memperbarui konfigurasi.

 Sumber daya yang tidak dikelola CloudFront

AWS Network Security Manager tidak mengelola CloudFront distribusi yang menggunakan paket harga CloudFront flat-rate atau CloudFront distribusi pementasan. Sumber daya ini muncul di luar sinkronisasi.

4. Untuk setiap jenis sumber daya yang dipilih, pilih salah satu opsi yang saling eksklusif berikut:
  - Sertakan semua sumber daya
  - Sertakan sumber daya tertentu
  - Kecualikan sumber daya tertentu
5. Jika Anda memilih Sertakan sumber daya tertentu, pilih salah satu jenis ekspresi berikut:
  - Kriteria tunggal
  - Cocokkan semua kriteria (DAN)
  - Cocokkan kriteria apa pun (OR)
  - TIDAK
6. Setiap jenis ekspresi mendukung kriteria inklusi tunggal atau ganda dan ARN, sehingga Anda dapat membangun kombinasi tag atau ARN. Semua jenis sumber daya mendukung kriteria inklusi Tag dan ARN. Jika Anda memilih Tag, identifikasi Kunci dan Nilai opsional. Anda dapat mengidentifikasi beberapa tag.
7. Untuk Application Load Balancer, kriteria Konfigurasi tambahan muncul. Dalam Konfigurasi, Anda dapat mengatur Skema dengan opsi Internet-facing atau Internal.

Untuk membuat penerapan (konsol)

Penerapan mengikat kebijakan Anda ke ruang lingkup dan mengaktifkan penegakan hukum, yang menyebabkan Manajer Keamanan AWS Jaringan menerapkan aturan AWS WAF Anda ke sumber daya dalam lingkup.

1. Pada halaman Ikhtisar, di panel Ikhtisar, pilih Buat penerapan. Anda juga dapat memulai langkah ini dari area lain di dalam alat.
2. Pilih kebijakan yang ingin Anda terapkan.
3. Pilih cakupan yang menentukan akun dan sumber daya tempat Manajer Keamanan AWS Jaringan menerapkan kebijakan tersebut.

4. Untuk nama Deployment, masukkan nama. (Opsional) Untuk Deskripsi, masukkan deskripsi.
5. (Opsional) Untuk membuat penyebaran terlihat oleh akun lain di organisasi Anda, pilih Aktifkan visibilitas lintas akun untuk penerapan ini.
6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru, lalu masukkan kombinasi Kunci dan Nilai opsional.
7. Pilih Buat dan terapkan. Halaman Deployment muncul, di mana Anda dapat melihat detail dari apa yang dibuat Manajer Keamanan AWS Jaringan.

 **Penerapan mungkin dikenakan biaya**

Penyebaran menciptakan layanan keamanan jaringan dan melampirkannya ke sumber daya yang dilindungi. AWS Manajer Keamanan Jaringan mengenakan biaya untuk sumber daya yang dilindungi. Layanan keamanan itu sendiri melindungi sumber daya, yang menimbulkan biaya tambahan. Sebelum Anda menerapkan, tinjau [halaman penetapan harga Manajer Keamanan AWS Jaringan](#) dan [halaman harga AWS WAF](#).

## Mengelola perlindungan DDoS untuk AWS Shield Advanced

Dengan AWS Network Security Manager, Anda mengonfigurasi dan menerapkan perlindungan AWS Shield Advanced secara terpusat di seluruh akun dan sumber daya di organisasi Anda. Anda dapat menentukan kebijakan perlindungan DDoS dan menegakkannya dalam skala besar melalui kebijakan dan penerapan Manajer Keamanan AWS Jaringan.

 **AWS Manajer Keamanan Jaringan ditagih secara terpisah**

AWS Network Security Manager bukan bagian dari penawaran AWS Shield Advanced. Untuk informasi selengkapnya tentang harga, lihat harga [Manajer Keamanan AWS Jaringan](#) dan [harga AWS Shield Advanced](#).

 **AWS Langganan Shield Advanced**

Ketika penerapan aktif menyertakan akun dalam cakupannya, Manajer Keamanan AWS Jaringan berlangganan akun tersebut ke AWS Shield Advanced. AWS Manajer Keamanan Jaringan tidak membatalkan langganan saat akun meninggalkan ruang lingkup atau saat

Anda menghapus penerapan. Untuk membatalkan langganan AWS Shield Advanced, lihat [Berlangganan AWS Shield Advanced](#) di Panduan Pengembang AWS WAF.

## Buat Cepat untuk AWS Shield Advanced

Dengan Quick Create, Anda menentukan dan menerapkan perlindungan AWS Shield Advanced dalam satu alur kerja terpandu. Gunakan Quick Create saat Anda ingin mengatur perlindungan DDoS dari kebijakan melalui penerapan dalam satu sesi.

Untuk menentukan dan menerapkan perlindungan AWS Shield Advanced dengan Quick Create, selesaikan prosedur berikut secara berurutan.

Untuk membuat kebijakan dan mengonfigurasi perlindungan

Selesaikan langkah-langkah berikut:

1. Buka konsol Manajer Keamanan AWS Jaringan di <https://console.aws.amazon.com/network-security-manager/>.
2. Di panel navigasi, pilih Ikhtisar.
3. Pada halaman Ikhtisar, pilih Quick create and deploy. Halaman Quick create and deploy muncul dengan beberapa panel.
4. Di panel Detail kebijakan, untuk Nama, masukkan nama kebijakan. (Opsional) Untuk Deskripsi, masukkan deskripsi.
5. Di panel Define protections, pilih jenis firewall yang ingin Anda gunakan. Pilih AWS Shield Advanced.
6. Di bawah Konfigurasi kebijakan di panel Tentukan perlindungan, tentukan tindakan otomatis yang diambil Manajer Keamanan AWS Jaringan dalam cakupan yang ditargetkan:
  - Remediasi menerapkan kebijakan yang ditetapkan untuk sumber daya apa pun yang status keamanannya tidak sesuai dengan status yang diinginkan yang dijelaskan oleh Manajer Keamanan AWS Jaringan.
  - Pembersihan sumber daya menghapus perlindungan DDoS yang dibuat oleh Manajer Keamanan AWS Jaringan untuk sumber daya saat penerapan dihapus, atau ketika akun atau sumber daya berada di luar cakupan.

- Resolusi DDoS pelanggan yang ada menentukan cara menyelesaikan konflik antara kebijakan yang Anda definisikan dan apa yang mungkin sudah diterapkan. Dari menu, pilih salah satu opsi berikut:
    - Tidak ada remediasi yang melewati remediasi pada sumber daya apa pun yang sudah memiliki perlindungan DDoS.
    - Asosiasi penggantian menggantikan perlindungan DDoS yang ada dengan perlindungan DDoS yang dibuat oleh Manajer Keamanan AWS Jaringan.
    - Retrofit memperbaiki aturannya ke setiap perlindungan DDoS yang ada dan menjaga perlindungan DDoS yang terkait dengan sumber daya.
7. Di panel Prioritas kebijakan, tetapkan prioritas. AWS Manajer Keamanan Jaringan mengevaluasi kebijakan sesuai dengan prioritas mereka untuk menyelesaikan konflik. Posisi yang lebih rendah (bilangan bulat bawah) memiliki prioritas yang lebih tinggi.

Untuk mengedit prioritas, pilih nilai Posisi. Kemudian naikan dengan panah, atau masukkan nilai secara langsung. Untuk mengonfirmasi pilihan, pilih Konfirmasi. Untuk membuang perubahan, pilih Batal.

Untuk mengatur ruang lingkup

Selesaikan langkah-langkah berikut:

1. Di panel Setel cakupan, tentukan kumpulan aset yang diterapkan kebijakan tersebut. Untuk nama Scope, masukkan nama. (Opsional) Untuk Deskripsi, masukkan deskripsi.

2.

 Multi-account modus saja

Langkah ini hanya berlaku untuk mode multi-akun. Dalam mode multi-akun, gunakan sub-panel pemilihan Akun dan unit organisasi untuk memilih akun atau OU mana yang akan disertakan atau dikecualikan. Dalam mode akun tunggal, sub-panel ini tidak muncul di konsol, jadi lewati langkah ini.

Di sub-panel pemilihan unit akun dan organisasi, pilih salah satu opsi berikut:

- Ruang lingkup untuk seluruh AWS organisasi. Tidak diperlukan definisi lebih lanjut.
- Ruang lingkup untuk seluruh AWS Organisasi tetapi tidak termasuk OU dan akun tertentu. Subpanel unit Organisasi dan sub-panel Akun muncul. Untuk mengecualikan unit organisasi,

pilih Tambah OU. Pilih unit organisasi di pohon organisasi, lalu pilih Tambah OU. Untuk mengecualikan akun individual, pilih Tambah akun. Pilih akun di pohon organisasi, lalu pilih Tambah akun.

- Jangan lingkup ke seluruh AWS Organisasi, dan hanya menyertakan OU dan akun tertentu. Gunakan mekanisme Add OU dan Add account yang sama untuk menyertakan unit organisasi dan akun yang Anda inginkan.
3. Di sub-panel Sumber Daya, untuk jenis Sumber Daya, pilih semua atau jenis sumber daya AWS Shield Advanced tertentu. Pilihannya adalah satu atau lebih dari yang berikut:
- Penyeimbang Beban Aplikasi
  - CloudFront Distribusi
  - Classic Load Balancer
  - Alamat IP elastis
4. Untuk setiap jenis sumber daya yang dipilih, pilih salah satu opsi yang saling eksklusif berikut:
- Sertakan semua sumber daya
  - Sertakan sumber daya tertentu
  - Kecualikan sumber daya tertentu
5. Jika Anda memilih Sertakan sumber daya tertentu, pilih salah satu jenis ekspresi berikut, lalu buat kombinasi tag atau ARN yang sesuai:
- Kriteria tunggal
  - Cocokkan semua kriteria (DAN)
  - Cocokkan kriteria apa pun (OR)
  - TIDAK

Semua jenis sumber daya memiliki kriteria inklusi Tag dan ARN. Jika Anda memilih Tag, masukkan Kunci dan Nilai opsional. Anda dapat mengidentifikasi beberapa tag.

#### CloudFront Persyaratan wilayah

Untuk melindungi sumber daya CloudFront Distribusi, gunakan Wilayah AS Timur (Virginia Utara) (us-east-1).

Untuk meninjau dan menerapkan kebijakan

Selesaikan langkah-langkah berikut:

1. Di panel Tinjau dan terapkan, untuk nama Deployment, masukkan nama. (Opsional) Untuk Deskripsi, masukkan deskripsi. Untuk menentukan apakah konten penerapan Anda terlihat oleh akun lain di organisasi Anda, pilih Aktifkan visibilitas lintas akun untuk penerapan ini.
2. (Opsional) Untuk menambahkan tag ke sumber daya Anda, pilih Tambahkan tag baru, lalu masukkan kombinasi Kunci dan Nilai opsional.
3. Untuk membuat dan menerapkan kebijakan dan cakupan, pilih Buat dan terapkan. Ketika proses selesai, halaman Deployment muncul, di mana Anda dapat melihat detail dari apa yang dibuat Manajer Keamanan AWS Jaringan.

 **Penerapan mungkin dikenakan biaya**

Penyebaran menciptakan layanan keamanan jaringan dan melampirkannya ke sumber daya yang dilindungi. AWS Manajer Keamanan Jaringan mengenakan biaya untuk sumber daya yang dilindungi. Layanan keamanan itu sendiri melindungi sumber daya, yang menimbulkan biaya tambahan. Sebelum menerapkan, tinjau halaman penetapan harga [AWS Network Security Manager](#) dan halaman harga [AWS Shield Advanced](#).

## Proses pembuatan standar untuk AWS Shield Advanced

Dengan proses pembuatan standar, Anda menyiapkan setiap komponen AWS Shield Advanced — kebijakan, cakupan, dan penerapan — secara individual untuk kontrol penuh. Gunakan pendekatan ini ketika Anda ingin membuat komponen yang dapat digunakan kembali dan menggabungkannya sesuai kebutuhan.

Kebijakan AWS Shield Advanced sederhana dan tidak berisi aturan, grup aturan, atau templat. Saat Anda menerapkan kebijakan tersebut, AWS Network Security Manager akan membuat perlindungan AWS Shield Advanced DDoS di setiap akun dalam lingkup. Untuk informasi tentang cara kerja Manajer Keamanan AWS Jaringan, lihat [Bagaimana AWS Network Security Manager bekerja](#).

Untuk membuat kebijakan (konsol)

Selesaikan langkah-langkah berikut:

1. Masuk ke AWS Management Console menggunakan akun administrator AWS Network Security Manager, lalu buka konsol AWS Network Security Manager di <https://console.aws.amazon.com/network-security-manager/>.



#### Penyiapan akun administrator

Untuk informasi tentang menyiapkan akun administrator Manajer Keamanan AWS Jaringan, lihat [Menyiapkan Manajer Keamanan AWS Jaringan](#).

2. Di panel navigasi, pilih AWS Network Security Manager, lalu Ikhtisar.
3. Di panel Ikhtisar, pilih Buat kebijakan. Masukkan Nama dan Deskripsi opsional, lalu pilih jenis Firewall (dalam hal ini, AWS Shield Advanced).
4. Di panel Prioritas kebijakan, tetapkan prioritas. AWS Manajer Keamanan Jaringan mengevaluasi kebijakan sesuai dengan prioritas mereka untuk menyelesaikan konflik. Posisi yang lebih rendah (bilangan bulat bawah) memiliki prioritas yang lebih tinggi.

Untuk mengedit prioritas, pilih nilai Posisi. Kemudian naikkan dengan panah, atau masukkan nilai secara langsung. Untuk mengonfirmasi pilihan, pilih Konfirmasi. Untuk membuang perubahan, pilih Batal.

5. Di panel konfigurasi Kebijakan, tentukan tindakan otomatis yang diambil Manajer Keamanan AWS Jaringan dalam cakupan yang ditargetkan:
  - Remediasi menerapkan kebijakan yang ditetapkan untuk sumber daya apa pun yang status keamanannya tidak sesuai dengan status yang diinginkan yang dijelaskan oleh Manajer Keamanan AWS Jaringan.
  - Pembersihan sumber daya menghapus perlindungan DDoS yang dibuat oleh Manajer Keamanan AWS Jaringan untuk sumber daya saat penerapan dihapus, atau ketika akun atau sumber daya berada di luar cakupan.
  - Resolusi DDoS pelanggan yang ada menentukan cara menyelesaikan konflik antara kebijakan yang Anda definisikan dan apa yang mungkin sudah diterapkan. Dari menu, pilih salah satu opsi berikut:
    - Tidak ada remediasi yang melewati remediasi pada sumber daya apa pun yang sudah memiliki perlindungan DDoS.
    - Asosiasi penggantian menggantikan perlindungan DDoS yang ada dengan perlindungan DDoS yang dibuat oleh Manajer Keamanan AWS Jaringan.

- Retrofit memperbaiki aturannya ke setiap perlindungan DDoS yang ada dan menjaga perlindungan DDoS yang terkait dengan sumber daya.

Untuk membuat ruang lingkup (konsol)

Selesaikan langkah-langkah berikut:

1. Di panel Rincian cakupan, masukkan nama Lingkup dan Deskripsi opsional.

2.

 **Multi-account modus saja**

Langkah ini hanya berlaku untuk mode multi-akun. Dalam mode multi-akun, gunakan sub-panel pemilihan unit Akun dan organisasi untuk memilih akun atau OU mana yang akan disertakan atau dikecualikan. Dalam mode akun tunggal, sub-panel ini tidak muncul di konsol, jadi lewati langkah ini.

Di panel pemilihan unit akun dan organisasi, pilih salah satu dari tiga metode untuk mengendalikan ruang lingkup administratif:

- Lingkup untuk seluruh AWS Organisasi (semua OU dan akun) - Tidak diperlukan definisi lebih lanjut.
  - Cakupan untuk seluruh AWS Organisasi tetapi tidak termasuk OU dan akun tertentu — Dua sub-panel muncul, satu untuk unit Organisasi dan satu untuk Akun. Pilih Add OU untuk membuka jendela Add OU, pilih unit organisasi yang Anda butuhkan, lalu pilih Tambah OU. Untuk menambahkan akun individual, di sub-panel Akun, pilih Tambah akun, pilih akun, lalu pilih Tambah akun.
  - Jangan lingkup ke seluruh AWS Organisasi, hanya sertakan OU dan akun tertentu — Gunakan sub-panel yang sama untuk menambahkan OU atau akun.
3. Selanjutnya, pilih sumber daya di sub-panel Sumber Daya. Di kotak pemilihan Jenis sumber daya, pilih semua atau jenis sumber daya AWS Shield Advanced tertentu. Untuk AWS Shield Advanced, pilihannya adalah salah satu atau semua hal berikut:
- Penyeimbang Beban Aplikasi
  - CloudFront Distribusi
  - Classic Load Balancer
  - Alamat IP elastis

4. Untuk setiap jenis sumber daya yang dipilih, pilih salah satu opsi yang saling eksklusif berikut:
  - Sertakan semua sumber daya
  - Sertakan sumber daya tertentu
  - Kecualikan sumber daya tertentu
5. Jika Anda memilih Sertakan sumber daya tertentu, pilih salah satu jenis ekspresi berikut:
  - Kriteria tunggal
  - Cocokkan semua kriteria (DAN)
  - Cocokkan kriteria apa pun (OR)
  - TIDAK
6. Setiap jenis ekspresi mendukung kriteria inklusi tunggal atau ganda dan ARN, sehingga Anda dapat membangun kombinasi tag atau ARN. Semua jenis sumber daya mendukung kriteria inklusi Tag dan ARN. Jika Anda memilih Tag, identifikasi Kunci dan Nilai opsional. Anda dapat mengidentifikasi beberapa tag.

 CloudFront Persyaratan wilayah

Untuk melindungi sumber daya CloudFront Distribusi, gunakan Wilayah AS Timur (Virginia Utara) (`us-east-1`).

Untuk membuat penerapan (konsol)

Penerapan mengikat kebijakan Anda ke ruang lingkup dan mengaktifkan penegakan hukum. AWS Network Security Manager kemudian menerapkan perlindungan AWS Shield Advanced DDoS Anda ke sumber daya dalam lingkup.

Selesaikan langkah-langkah berikut:

1. Pada halaman Ikhtisar, di panel Ikhtisar, pilih Buat penerapan.
2. Pilih kebijakan yang ingin Anda terapkan.
3. Pilih cakupan yang menentukan akun dan sumber daya tempat Manajer Keamanan AWS Jaringan menerapkan kebijakan tersebut.
4. Untuk nama Deployment, masukkan nama. (Opsional) Untuk Deskripsi, masukkan deskripsi.

5. (Opsional) Untuk membuat penerapan terlihat oleh akun lain di organisasi Anda, pilih Aktifkan visibilitas lintas akun untuk penerapan ini.
6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru, lalu masukkan kombinasi Kunci dan Nilai opsional.
7. Pilih Buat dan terapkan. Halaman Deployment muncul, di mana Anda dapat melihat detail dari apa yang dibuat Manajer Keamanan AWS Jaringan.

 Penerapan mungkin dikenakan biaya

Penyebaran menciptakan layanan keamanan jaringan dan melampirkannya ke sumber daya yang dilindungi. AWS Manajer Keamanan Jaringan mengenakan biaya untuk sumber daya yang dilindungi. Layanan keamanan itu sendiri melindungi sumber daya, yang menimbulkan biaya tambahan. Sebelum menerapkan, tinjau halaman harga [AWS Network Security Manager](#) dan halaman harga [AWS Shield Advanced](#).

# AWS Manajer Keamanan Jaringan dan AWS Firewall Manager

AWS Network Security Manager adalah layanan yang menggantikan AWS Firewall Manager. Keduanya adalah layanan yang sepenuhnya terpisah, masing-masing dengan kemampuan unik dan model harga yang berbeda. Jika saat ini Anda menggunakan AWS Firewall Manager, Anda tidak perlu mengambil tindakan apa pun—firewall dan kebijakan yang ada terus berfungsi. Bab ini menjelaskan bagaimana kedua layanan hidup berdampingan, cara kerja prioritas saat Anda menggunakan keduanya, dan bagaimana migrasi akan bekerja saat tersedia.

AWS Network Security Manager dan AWS Firewall Manager beroperasi berdampingan dan independen satu sama lain. Pada titik tertentu, AWS Firewall Manager akan berhenti dijual dan kemudian berhenti beroperasi.

## Koeksistensi dengan AWS Firewall Manager

AWS Network Security Manager tidak memengaruhi firewall yang Anda buat dengan AWS Firewall Manager kecuali Anda memulai tindakan untuk mengubahnya. Firewall dan kebijakan yang Anda buat dengan AWS Firewall Manager terus beroperasi kecuali Anda menghentikannya. Ini benar bahkan setelah AWS Firewall Manager dihentikan.

## Prioritas selama remediasi

Sementara kedua layanan beroperasi, Anda dapat mengambil tindakan yang memengaruhi firewall yang Anda buat dengan AWS Firewall Manager. Saat Anda membuat kebijakan Manajer Keamanan AWS Jaringan, Anda menerapkannya ke cakupan, yang merupakan sekumpulan sumber daya target. Jika cakupan tersebut mencakup sumber daya yang sudah ditangani oleh kebijakan AWS Firewall Manager, AWS Network Security Manager akan diutamakan selama remediasi. Dalam hal ini, kebijakan dan cakupan Manajer Keamanan AWS Jaringan mengesampingkan AWS firewall dan kebijakan Firewall Manager yang ada. Perilaku spesifik tergantung pada opsi resolusi yang Anda pilih.

## Migrasi yang direncanakan dari AWS Firewall Manager

Migrasi dari AWS Firewall Manager ke AWS Network Security Manager mengkonsolidasikan manajemen firewall Anda ke dalam satu layanan dan memungkinkan Anda menggunakan

kemampuannya. Migrasi direncanakan tetapi belum tersedia. Ketika migrasi tersedia, Anda akan dapat memindahkan kebijakan AWS Firewall Manager Anda ke AWS Network Security Manager. Migrasi akan membutuhkan tindakan baru di kedua layanan yang belum ada.

Proses yang direncanakan akan menyalin kebijakan yang dipilih dari AWS Firewall Manager, mentransfernya ke AWS Network Security Manager, dan menerjemahkannya ke dalam struktur kebijakan baru. Proses ini tidak memengaruhi kebijakan asli Anda atau firewall terkait di AWS Firewall Manager.

# Keamanan di AWS Manajer Keamanan Jaringan

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program Kepatuhan Program [AWS Kepatuhan Program AWS](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Manajer Keamanan AWS Jaringan, lihat [AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan](#) .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Manajer Keamanan AWS Jaringan. Topik berikut menunjukkan cara mengonfigurasi Manajer Keamanan AWS Jaringan untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Manajer Keamanan AWS Jaringan Anda.

## Topik

- [Perlindungan data di AWS Manajer Keamanan Jaringan](#)
- [Identitas dan manajemen akses untuk AWS Manajer Keamanan Jaringan](#)
- [Menggunakan peran terkait layanan untuk AWS Manajer Keamanan Jaringan](#)
- [Validasi kepatuhan untuk AWS Manajer Keamanan Jaringan](#)
- [Ketahanan di AWS Manajer Keamanan Jaringan](#)
- [Keamanan Infrastruktur di AWS Manajer Keamanan Jaringan](#)
- [Praktik terbaik keamanan untuk AWS Manajer Keamanan Jaringan](#)

# Perlindungan data di AWS Manajer Keamanan Jaringan

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Manajer Keamanan AWS Jaringan. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ Privasi Data AWS](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Pusat Peraturan Umum Perlindungan Data \(GDPR\)](#).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan logging aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Network Security Manager atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan

untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

## Enkripsi saat diam

AWS Network Security Manager mengenkripsi semua data saat istirahat menggunakan AWS kunci Key Management Service (AWS KMS). Service-managed Kunci KMS melindungi konfigurasi sumber daya, status penerapan, dan data sinkronisasi Anda. Anda tidak perlu mengkonfigurasi atau mengelola kunci ini.

## Enkripsi saat bergerak

AWS Network Security Manager mengenkripsi semua data dalam perjalanan menggunakan Transport Layer Security (TLS). Semua permintaan API memerlukan TLS 1.2 atau yang lebih baru. Koneksi ke titik akhir API Manajer Keamanan AWS Jaringan menggunakan HTTPS secara eksklusif.

## Manajemen kunci

AWS Network Security Manager menggunakan kunci AWS KMS yang dikelola layanan untuk enkripsi saat istirahat. Anda tidak dapat memberikan kunci KMS Anda sendiri saat ini.

## Identitas dan manajemen akses untuk AWS Manajer Keamanan Jaringan

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Manajer Keamanan AWS Jaringan. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

### Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Manajer Keamanan Jaringan bekerja dengan IAM](#)

- [Identity-based contoh kebijakan untuk AWS Manajer Keamanan Jaringan](#)
- [Pemecahan masalah AWS Identitas dan akses Manajer Keamanan Jaringan](#)

## Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Pemecahan masalah AWS Identitas dan akses Manajer Keamanan Jaringan](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana AWS Manajer Keamanan Jaringan bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Identity-based contoh kebijakan untuk AWS Manajer Keamanan Jaringan](#))

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensial identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

## Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

## Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center.

## Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

## Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

## Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya.

AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

## Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

## Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

## Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

## Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

## Bagaimana AWS Manajer Keamanan Jaringan bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke AWS Network Security Manager, pelajari fitur IAM apa yang tersedia untuk digunakan dengan AWS Network Security Manager.

| Fitur IAM                                | AWS Dukungan Manajer Keamanan Jaringan |
|------------------------------------------|----------------------------------------|
| <a href="#">Identity-based kebijakan</a> | Ya                                     |
| <a href="#">Resource-based kebijakan</a> | Tidak                                  |
| <a href="#">Tindakan kebijakan</a>       | Ya                                     |
| <a href="#">Sumber daya kebijakan</a>    | Ya                                     |
| <a href="#">Kunci kondisi kebijakan</a>  | Ya                                     |
| <a href="#">ACL</a>                      | Tidak                                  |

| Fitur IAM                                    | AWS Dukungan Manajer Keamanan Jaringan |
|----------------------------------------------|----------------------------------------|
| <a href="#">ABAC (tanda dalam kebijakan)</a> | Ya                                     |
| <a href="#">Kredensial sementara</a>         | Ya                                     |
| <a href="#">Izin principal</a>               | Ya                                     |
| <a href="#">Peran layanan</a>                | Ya                                     |
| <a href="#">Service-linked peran</a>         | Ya                                     |

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Manajer Keamanan AWS Jaringan dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

## Identity-based kebijakan untuk AWS Manajer Keamanan Jaringan

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkannya atau ditolakannya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

## Resource-based kebijakan dalam AWS Manajer Keamanan Jaringan

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan

oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

AWS Network Security Manager tidak mendukung kebijakan berbasis sumber daya.

## Tindakan kebijakan untuk AWS Manajer Keamanan Jaringan

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Manajer Keamanan AWS Jaringan, lihat [Tindakan yang Ditetapkan oleh Manajer Keamanan AWS Jaringan](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan di Manajer Keamanan AWS Jaringan menggunakan awalan berikut sebelum tindakan:

```
network-security-manager
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [  
    "network-security-manager:action1",  
    "network-security-manager:action2"  
]
```

AWS Network Security Manager mendefinisikan tindakan IAM di seluruh jenis sumber dayanya. Ini termasuk membuat, membaca, memperbarui, dan menghapus (CRUD) operasi untuk aturan,

template, kebijakan, cakupan, dan penerapan, bersama dengan snapshot, tagging, administratif, status sinkronisasi, dan operasi asosiasi sumber daya.

## Sumber daya kebijakan untuk AWS Manajer Keamanan Jaringan

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (\*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar tipe sumber daya Manajer Keamanan AWS Jaringan dan ARNnya, lihat [Sumber Daya yang Ditentukan oleh Manajer Keamanan AWS Jaringan di Referensi](#) Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang Ditentukan oleh Manajer Keamanan AWS Jaringan](#).

AWS Network Security Manager mendefinisikan tipe sumber daya IAM untuk setiap sumber dayanya (aturan, templat, kebijakan, ruang lingkup, dan penerapan), ditambah jenis snapshot untuk masing-masing sumber daya (misalnya,). `rule-snapshot` Format ARN adalah:

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}
```

Draf ARN menambahkan :DRAFT dan snapshot ARN menambahkan nomor versi (misalnya,). :3

Draf bukan tipe sumber daya IAM yang terpisah. Untuk otorisasi, draf diperlakukan sebagai anak dari sumber daya aktifnya, yang merupakan orang tua. ARN :DRAFT yang memenuhi syarat memberi wewenang terhadap sumber daya aktif, jadi izin untuk bertindak berdasarkan draf berasal dari izin untuk bertindak atas sumber daya aktif tersebut.

Snapshot berbeda dari draf. Setiap snapshot adalah tipe sumber daya IAM-nya sendiri, jadi ARN yang memenuhi syarat versi memberi otorisasi terhadap jenis sumber daya snapshot tersebut secara langsung, bukan terhadap sumber daya aktif induk.

## Kunci kondisi kebijakan untuk AWS Manajer Keamanan Jaringan

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Manajer Keamanan AWS Jaringan, lihat [Kunci Kondisi untuk Manajer Keamanan AWS Jaringan](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang Ditentukan oleh Manajer Keamanan AWS Jaringan](#).

AWS Network Security Manager mendukung kunci kondisi tag AWS global berikut untuk kontrol akses berbasis atribut (ABAC):

- `aws:ResourceTag/${TagKey}`
- `aws:RequestTag/${TagKey}`
- `aws:TagKeys`

Tag-based tombol kondisi berlaku untuk sumber daya aktif dan snapshot. Sumber daya draf tidak dapat diberi tag dan tidak mendukung `aws:ResourceTag` kondisi.

## ACL di AWS Manajer Keamanan Jaringan

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

AWS Network Security Manager tidak mendukung daftar kontrol akses (ACL).

## ABAC dengan AWS Manajer Keamanan Jaringan

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

AWS Network Security Manager mendukung kontrol akses berbasis atribut menggunakan ketiga kunci kondisi tag AWS global. Anda dapat membatasi akses ke sumber daya Manajer Keamanan AWS Jaringan berdasarkan tag yang dilampirkan pada sumber daya tersebut.

## Menggunakan kredensial sementara dengan AWS Manajer Keamanan Jaringan

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

## Cross-service izin utama untuk AWS Manajer Keamanan Jaringan

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

## Peran layanan untuk AWS Manajer Keamanan Jaringan

Mendukung peran layanan: Ya

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

### Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas Manajer Keamanan AWS Jaringan. Edit peran layanan hanya jika Manajer Keamanan AWS Jaringan memberikan panduan untuk melakukannya.

## Service-linked peran untuk AWS Manajer Keamanan Jaringan

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

AWS Manajer Keamanan Jaringan menggunakan peran terkait layanan untuk beroperasi di akun anggota organisasi Anda. AWS Network Security Manager membuat peran terkait layanan secara otomatis saat Anda mengaktifkan layanan. Peran tersebut memberikan izin kepada Manajer Keamanan AWS Jaringan untuk mengelola sumber daya AWS WAF dan AWS Shield Advanced. Peran ini juga memberikan akses ke AWS Config untuk penemuan sumber daya dan izin untuk melakukan operasi lintas akun.

Untuk detail tentang membuat dan mengelola peran terkait layanan Manajer Keamanan AWS Jaringan, lihat [the section called “Service-linked peran”](#)

## Identity-based contoh kebijakan untuk AWS Manajer Keamanan Jaringan

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Manajer Keamanan AWS Jaringan. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) di Panduan Pengguna IAM](#).

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Manajer Keamanan AWS Jaringan, termasuk format ARN untuk setiap jenis sumber daya, lihat [Tindakan, Sumber Daya, dan Kunci Kondisi untuk Manajer Keamanan AWS Jaringan](#) di Referensi Otorisasi Layanan.

## Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan AWS Konsol Manajer Keamanan Jaringan](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [Read-only akses ke AWS Manajer Keamanan Jaringan](#)
- [Mengelola aturan dan template saja](#)

## Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Manajer Keamanan AWS Jaringan di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber

daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

## Menggunakan AWS Konsol Manajer Keamanan Jaringan

Untuk mengakses konsol AWS Network Security Manager, Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Manajer Keamanan AWS Jaringan di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk mengakses konsol AWS Network Security Manager, prinsipal memerlukan izin minimum untuk `network-security-manager:Get*` tindakan `network-security-manager:List*` dan tindakan.

## Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

## Read-only akses ke AWS Manajer Keamanan Jaringan

Kebijakan berikut memberikan akses hanya-baca utama ke semua sumber daya Manajer Keamanan AWS Jaringan. Ini berguna untuk auditor atau peran pemantauan yang perlu melihat konfigurasi dan status sinkronisasi tanpa membuat perubahan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-manager:Get*",
        "network-security-manager:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

## Mengelola aturan dan template saja

Kebijakan berikut memungkinkan prinsipal untuk membuat, memperbarui, dan menghapus aturan dan templat, tanpa memberikan akses ke kebijakan, cakupan, atau penerapan. Ini berguna untuk tim yang membuat konfigurasi keamanan tetapi tidak mengontrol penegakan hukum.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-manager:CreateRule",
        "network-security-manager:GetRule",
        "network-security-manager:UpdateRule",
        "network-security-manager>DeleteRule",
        "network-security-manager:ListRules",
        "network-security-manager:CreateRuleSnapshot",
        "network-security-manager:ListRuleSnapshots",
        "network-security-manager>CreateTemplate",
        "network-security-manager:GetTemplate",
        "network-security-manager:UpdateTemplate",

```

```
        "network-security-manager:DeleteTemplate",
        "network-security-manager:ListTemplates",
        "network-security-manager:CreateTemplateSnapshot",
        "network-security-manager:ListTemplateSnapshots",
        "network-security-manager:TagResource",
        "network-security-manager:UntagResource",
        "network-security-manager:ListTagsForResource"
    ],
    "Resource": "*"
}
]
```

## Pemecahan masalah AWS Identitas dan akses Manajer Keamanan Jaringan

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Network Security Manager dan IAM.

### Topik

- [Saya tidak berwenang untuk melakukan tindakan di AWS Manajer Keamanan Jaringan](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses saya AWS Sumber daya Manajer Keamanan Jaringan](#)

### Saya tidak berwenang untuk melakukan tindakan di AWS Manajer Keamanan Jaringan

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya `my-example-widget` rekaan, tetapi tidak memiliki izin `network-security-manager:GetWidget` rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
network-security-manager:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `network-security-manager:GetWidget`.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

## Saya tidak berwenang untuk melakukan `iam:PassRole`

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Manajer Keamanan AWS Jaringan.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Manajer Keamanan AWS Jaringan. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

## Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses saya AWS Sumber daya Manajer Keamanan Jaringan

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah AWS Network Security Manager mendukung fitur-fitur ini, lihat [Bagaimana AWS Manajer Keamanan Jaringan bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

## Menggunakan peran terkait layanan untuk AWS Manajer Keamanan Jaringan

AWS Manajer Keamanan Jaringan menggunakan peran [terkait layanan](#) IAM. Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke Manajer Keamanan AWS Jaringan. Service-linked peran telah ditentukan sebelumnya oleh Manajer Keamanan AWS Jaringan dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Network Security Manager lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Network Security Manager mendefinisikan izin dari peran layanannya yang terkait. Kecuali ditentukan lain, hanya Manajer Keamanan AWS Jaringan yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin. Anda tidak dapat melampirkan kebijakan izin tersebut ke entitas IAM lainnya.

Anda dapat menghapus peran terkait layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Manajer Keamanan AWS Jaringan Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang bekerja dengan IAM](#) dan cari layanan yang menyertakan Ya di kolom peran. Service-linked Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

## Service-linked izin peran untuk AWS Manajer Keamanan Jaringan

AWS Network Security Manager menggunakan peran terkait layanan bernama.

`AWSServiceRoleForNetworkSecurityManager` Peran terkait layanan ini mempercayai kepala `network-security-manager.amazonaws.com` layanan untuk mengambil peran tersebut.

Kebijakan izin peran bernama `NetworkSecurityManagerServiceRolePolicy` adalah kebijakan AWS terkelola yang memungkinkan Manajer Keamanan AWS Jaringan menyelesaikan tindakan pada sumber daya yang ditentukan.

Kebijakan kepercayaan berikut memungkinkan kepala `network-security-manager.amazonaws.com` layanan untuk mengambil peran.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "network-security-manager.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

### Note

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [izin Service-linked peran](#) di Panduan Pengguna IAM.

## Detail izin

AWS Manajer Keamanan Jaringan memerlukan setiap grup izin untuk melindungi dan menemukan sumber daya di seluruh akun dan organisasi Anda. Kebijakan `NetworkSecurityManagerServiceRolePolicy` terkelola memberikan izin berikut, dikelompokkan berdasarkan layanan:

- **wafv2**— Buat, baca, perbarui, dan hapus grup aturan ACL web dan Firewall Manager. Kaitkan dan pisahkan ACL web dengan sumber daya yang dilindungi. Mengelola konfigurasi pencatatan ACL web dan kebijakan izin grup aturan. Tag dan untag sumber daya. Validasi AWS Network Security Manager web ACL dan konfigurasi aturan.
- **shield**— Buat, jelaskan, daftar, dan hapus perlindungan AWS Shield Advanced. Buat dan jelaskan langganan AWS Shield Advanced.
- **elasticloadbalancing**— Jelaskan Penyeimbang Beban Aplikasi dan tag. Membuat, menghapus, dan mengatur asosiasi ACL web pada Application Load Balancers.
- **cloudfront**— Dapatkan dan daftar CloudFront distribusi, konfigurasi, dan tag Amazon. Mengaitkan dan memisahkan ACL web distribusi. Baca asal-usul VPC.
- **apigateway**— Baca API REST Amazon API Gateway API, tahapan, dan tag. Atur ACL web pada tahap API.
- **ec2**— Baca ACL dan asosiasi web instans Akses Terverifikasi Amazon EC2. Jelaskan alamat IP Elastis untuk perlindungan AWS Shield Advanced.
- **cognito-idp,apprunner, appsyncamplify, dan bedrock-agentcore** — Baca asosiasi ACL web untuk kumpulan pengguna Amazon Cognito, layanan AWS App Runner , API AWS AppSync GraphQL, AWS Amplify aplikasi, dan gateway AWS Amazon AgentCore Bedrock sehingga Manajer Keamanan Jaringan dapat menemukan sumber daya yang dilindungi.
- **config**— Pilih konfigurasi sumber daya dan kelola perekam AWS Config konfigurasi terkait layanan yang digunakan Manajer Keamanan AWS Jaringan untuk menemukan sumber daya dalam cakupan.
- **organizations**— Baca organisasi, akun, akar, unit organisasi, dan administrator yang didelegasikan sehingga Manajer Keamanan AWS Jaringan dapat beroperasi di seluruh organisasi Anda.
- **logs**— Buat, baca, perbarui, hapus, dan daftar pengiriman log untuk pencatatan ACL web.
- **s3**— Dapatkan dan letakkan kebijakan bucket di bucket Amazon S3 yang namanya dimulai `aws-waf-logs-` sehingga log ACL web dapat dikirimkan.
- **iam**— Buat peran terkait layanan yang diperlukan AWS Shield Advanced, AWS Config, dan AWS WAF, dengan cakupan kunci kondisi. `iam:AWSServiceName`

JSON berikut menunjukkan kebijakan `NetworkSecurityManagerServiceRolePolicy` izin lengkap.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "LogsGeneral",
    "Effect": "Allow",
    "Action": [
      "logs:ListLogDeliveries",
      "logs:CreateLogDelivery",
      "logs:GetLogDelivery",
      "logs:UpdateLogDelivery",
      "logs>DeleteLogDelivery"
    ],
    "Resource": "*"
  },
  {
    "Sid": "S3LogBucketGeneral",
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketPolicy",
      "s3:PutBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::aws-waf-logs-*"
  },
  {
    "Sid": "CloudfrontVpcOriginAccess",
    "Effect": "Allow",
    "Action": [
      "cloudfront:GetVpcOrigin"
    ],
    "Resource": "arn:aws:cloudfront::*:vpccorigin/*"
  },
  {
    "Sid": "ConfigUnscoped",
    "Effect": "Allow",
    "Action": [
      "config:SelectResourceConfig"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DescribeOrganizationUnScoped",
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeOrganization",
```

```

        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
},
{
    "Sid": "DescribeAccountScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeAccount",
    "Resource": "arn:aws:organizations::*:account/o-*/*"
},
{
    "Sid": "DescribeOrganizationUnitScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeOrganizationalUnit",
    "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
},
{
    "Sid": "ListDelegatedAdministratorsScoped",
    "Effect": "Allow",
    "Action": "organizations:ListDelegatedAdministrators",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "network-security-manager.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "LoadBalancerNonMutationApiAccess",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeWebACLAssociation"
    ],
    "Resource": "*"
},

```

```

{
  "Sid": "LoadBalancerGetWebACLScoped",
  "Effect": "Allow",
  "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
  "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
},
{
  "Sid": "CloudFrontDistributionNonMutationApiAccess",
  "Effect": "Allow",
  "Action": [
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListTagsForResource"
  ],
  "Resource": "arn:aws:cloudfront:*:*:distribution/*"
},
{
  "Sid": "ApiGatewayStageNonMutationApiAccess",
  "Effect": "Allow",
  "Action": "apigateway:GET",
  "Resource": [
    "arn:aws:apigateway:*:*/restapis",
    "arn:aws:apigateway:*:*/restapis/*/stages",
    "arn:aws:apigateway:*:*/restapis/*/stages/*",
    "arn:aws:apigateway:*:*/tags/*"
  ]
},
{
  "Sid": "Wafv2General",
  "Effect": "Allow",
  "Action": [
    "wafv2:TagResource",
    "wafv2:ListResourcesForWebACL",
    "wafv2:AssociateWebACL",
    "wafv2:ListTagsForResource",
    "wafv2:UntagResource",
    "wafv2:GetWebACL",
    "wafv2:DisassociateFirewallManager",
    "wafv2>DeleteWebACL",
    "wafv2:DisassociateWebACL",
    "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
    "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
  ],
  "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
}

```

```

},
{
  "Sid": "Wafv2WebAclAndRuleGroupMutation",
  "Effect": "Allow",
  "Action": [
    "wafv2:UpdateWebACL",
    "wafv2:CreateWebACL",
    "wafv2:DeleteFirewallManagerRuleGroups",
    "wafv2:PutFirewallManagerRuleGroups"
  ],
  "Resource": [
    "arn:aws:wafv2:*:*:/webacl/*",
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*",
    "arn:aws:wafv2:*:*:global/managedruleset/*",
    "arn:aws:wafv2:*:*:regional/managedruleset/*",
    "arn:aws:wafv2:*:*:global/ipset/*",
    "arn:aws:wafv2:*:*:regional/ipset/*",
    "arn:aws:wafv2:*:*:global/regexpatternset/*",
    "arn:aws:wafv2:*:*:regional/regexpatternset/*"
  ]
},
{
  "Sid": "Wafv2Logging",
  "Effect": "Allow",
  "Action": [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource": "arn:aws:wafv2:*:*:/webacl/*"
},
{
  "Sid": "Wafv2ListLogging",
  "Effect": "Allow",
  "Action": "wafv2:ListLoggingConfigurations",
  "Resource": "*"
},
{
  "Sid": "Wafv2ListWebACLs",
  "Effect": "Allow",
  "Action": "wafv2:ListWebACLs",
  "Resource": "*"
},

```

```

{
  "Sid": "Wafv2PermissionPolicy",
  "Effect": "Allow",
  "Action": [
    "wafv2:PutPermissionPolicy",
    "wafv2:GetPermissionPolicy",
    "wafv2>DeletePermissionPolicy"
  ],
  "Resource": [
    "arn:aws:wafv2::*:global/rulegroup/*",
    "arn:aws:wafv2::*:regional/rulegroup/*"
  ]
},
{
  "Sid": "Wafv2WebaclDescribe",
  "Effect": "Allow",
  "Action": "wafv2:GetWebACLForResource",
  "Resource": "arn:aws:wafv2::*:*/webacl/*"
},
{
  "Sid": "CloudFrontListDistributions",
  "Effect": "Allow",
  "Action": [
    "cloudfront:ListDistributionsByWebACLId",
    "cloudfront:ListDistributions"
  ],
  "Resource": "*"
},
{
  "Sid": "CloudFrontDistributionMutation",
  "Effect": "Allow",
  "Action": [
    "cloudfront:AssociateDistributionWebACL",
    "cloudfront:DisassociateDistributionWebACL"
  ],
  "Resource": "arn:aws:cloudfront::*:distribution/*"
},
{
  "Sid": "ElbWebAclRemediationScoped",
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:CreateWebACLAssociation",
    "elasticloadbalancing>DeleteWebACLAssociation"
  ],

```

```

    "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
  },
  {
    "Sid": "ElbSetWebAcl",
    "Effect": "Allow",
    "Action": "elasticloadbalancing:SetWebACL",
    "Resource": "*"
  },
  {
    "Sid": "ApiGatewayWebAclRemediation",
    "Effect": "Allow",
    "Action": "apigateway:SetWebACL",
    "Resource": "arn:aws:apigateway:*::/restapis/*/stages/*"
  },
  {
    "Sid": "CognitoWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "cognito-idp:GetWebACLForResource",
      "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AppRunnerWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "apprunner:DescribeWebAclForService",
      "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": "*"
  },
  {
    "Sid": "VerifiedAccessWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "ec2:GetVerifiedAccessInstanceWebAcl",
      "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AppSyncWebAclIntegration",
    "Effect": "Allow",

```

```

    "Action": [
      "appsync:GetWebACLForResource",
      "appsync:ListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AmplifyWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "amplify:GetWebACLForResource",
      "amplify:ListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ShieldGeneral",
    "Effect": "Allow",
    "Action": [
      "shield:CreateProtection",
      "shield:DeleteProtection",
      "shield:DescribeProtection",
      "shield:ListProtections",
      "shield:CreateSubscription",
      "shield:DescribeSubscription",
      "shield:GetSubscriptionState",
      "ec2:DescribeAddresses",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ShieldSlrCreation",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "shield.amazonaws.com"
      }
    }
  }
},
{

```

```

    "Sid": "AllowConfigRecorderList",
    "Effect": "Allow",
    "Action": "config:ListConfigurationRecorders",
    "Resource": "*"
  },
  {
    "Sid": "AllowPutServiceLinkedConfigRecorder",
    "Effect": "Allow",
    "Action": "config:PutServiceLinkedConfigurationRecorder",
    "Resource": "*"
  },
  {
    "Sid": "AllowConfigRecorderScopedAccess",
    "Effect": "Allow",
    "Action": [
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus",
      "config>DeleteServiceLinkedConfigurationRecorder",
      "config:AssociateResourceTypes",
      "config:DisassociateResourceTypes"
    ],
    "Resource": "arn:aws:config:*:*:configuration-recorder/*"
  },
  {
    "Sid": "AllowCreateConfigServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam:*:*:role/aws-service-role/config.amazonaws.com/*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "config.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowListActionsForAgentCoreGateway",
    "Effect": "Allow",
    "Action": [
      "bedrock-agentcore:GatewayListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowGetActionForAgentCoreGateway",

```

```

    "Effect": "Allow",
    "Action": [
        "bedrock-agentcore:GatewayGetWebACLForResource"
    ],
    "Resource": "arn:aws:bedrock-agentcore:*:*:gateway/*"
},
{
    "Sid": "WafV2LoggingSlrCreation",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam:*:*:role/aws-service-role/wafv2.amazonaws.com/*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "wafv2.amazonaws.com"
        }
    }
}
]
}

```

## Membuat peran terkait layanan untuk AWS Manajer Keamanan Jaringan

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan AWS Network Security Manager, AWS Network Security Manager akan membuat peran terkait layanan untuk Anda. Tidak ada langkah manual untuk dilakukan.

Jika Anda menghapus peran terkait layanan ini dan kemudian perlu membuatnya lagi, Manajer Keamanan AWS Jaringan akan membuat ulang peran tersebut saat berikutnya Anda menggunakan layanan. Anda tidak perlu mengambil tindakan apa pun.

Untuk informasi selengkapnya, silakan lihat [Membuat peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Menyunting peran terkait layanan untuk AWS Manajer Keamanan Jaringan

Anda tidak dapat mengubah izin peran `AWSServiceRoleForNetworkSecurityManager` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM.

Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Menghapus peran terkait layanan untuk AWS Manajer Keamanan Jaringan

Jika Anda tidak perlu lagi menggunakan AWS Network Security Manager, kami sarankan Anda menghapus peran `AWSServiceRoleForNetworkSecurityManager` terkait layanan.

Sebelum Anda menghapus peran terkait layanan, bersihkan sumber daya yang dikelola Manajer Keamanan AWS Jaringan. Nonaktifkan Manajer Keamanan AWS Jaringan dan hapus kebijakan dan cakupan sehingga tidak ada sumber daya yang dikelola Manajer Keamanan AWS Jaringan yang tetap ada di akun Anda. Anda kemudian dapat menghapus peran secara manual.

### Note

Jika Manajer Keamanan AWS Jaringan menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, pilih Peran.
3. Di kotak pencarian, masukkan `AWSServiceRoleForNetworkSecurityManager`, lalu pilih peran.
4. Pilih Hapus.
5. Untuk mengonfirmasi penghapusan, masukkan nama peran, lalu pilih Hapus.

Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Wilayah yang Didukung untuk AWS Peran terkait layanan Manajer Keamanan Jaringan

AWS Manajer Keamanan Jaringan mendukung penggunaan peran terkait layanan di semua AWS Wilayah tempat Manajer Keamanan AWS Jaringan tersedia.

## Validasi kepatuhan untuk AWS Manajer Keamanan Jaringan

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi Anda ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat [mendaftar untuk AWS \(lanjutan\)](#) atau [mengaktifkan fitur lanjutan untuk lingkungan](#) Anda AWS .

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#) .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat [Dokumentasi AWS Keamanan](#).

## Ketahanan di AWS Manajer Keamanan Jaringan

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Selain infrastruktur AWS global, AWS Network Security Manager menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

# Keamanan Infrastruktur di AWS Manajer Keamanan Jaringan

Sebagai layanan terkelola, AWS Network Security Manager dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper [Amazon Web Services: Overview of Security Processes](#).

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Network Security Manager melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal IAM. Atau Anda dapat menggunakan [AWS Security Token Service](#) (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

## Praktik terbaik keamanan untuk AWS Manajer Keamanan Jaringan

Praktik terbaik berikut membantu Anda mempertahankan konfigurasi AWS Network Security Manager yang aman.

### Kontrol pencegahan

- Gunakan hak istimewa IAM -- Berikan hanya izin yang diperlukan untuk setiap pengguna atau peran untuk melakukan tugas Manajer Keamanan AWS Jaringan mereka. Gunakan kunci kondisi IAM untuk membatasi akses ke sumber daya tertentu bila memungkinkan.
- Gunakan peran terkait layanan - Manajer Keamanan AWS Jaringan menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Peran ini memiliki izin yang telah ditentukan sebelumnya yang mencakup akses minimum yang diperlukan.
- Konfigurasi cakupan dengan hati-hati -- Tentukan konfigurasi lingkup yang hanya menargetkan akun dan jenis sumber daya yang memerlukan perlindungan. Cakupan yang terlalu luas dapat menyebabkan penegakan hukum yang tidak diinginkan.

## Kontrol detektif

- Aktifkan AWS CloudTrail CloudTrail pencatatan -- merekam semua panggilan API Manajer Keamanan AWS Jaringan. Tinjau log ini untuk mengaudit siapa yang membuat perubahan pada konfigurasi keamanan Anda dan kapan.
- Pantau status sinkronisasi - Periksa status sinkronisasi penerapan Anda secara teratur untuk mengidentifikasi sumber daya yang tidak sinkron dengan postur keamanan yang Anda inginkan.

# Memantau AWS Manajer Keamanan Jaringan

Monitoring AWS Network Security Manager membantu Anda memahami apakah sumber daya Anda dilindungi sebagaimana dimaksud. AWS Network Security Manager menyediakan kemampuan pemantauan berikut:

- API status sinkronisasi - Kueri status perlindungan sumber daya individual di seluruh penerapan Anda.
- AWS CloudTrail- Rekam semua panggilan API Manajer Keamanan AWS Jaringan untuk audit, kepatuhan, dan pemecahan masalah operasional.

## Memantau status sinkronisasi

Cara utama untuk memantau apakah sumber daya Anda dilindungi adalah melalui API status sinkronisasi. AWS Network Security Manager mengevaluasi setiap sumber daya dalam lingkup dan mencatat apakah konfigurasi firewall aktualnya cocok dengan konfigurasi yang dimaksud.

## Operasi status sinkronisasi

AWS Network Security Manager menyediakan dua operasi untuk query status sinkronisasi:

### ListResourceSynchronizationStatuses

Mengembalikan status per sumber daya untuk penerapan tertentu. Membutuhkan `deploymentIdentifier` parameter. Filter secara opsional berdasarkan `synchronizationStatus` (IN\_SYNC, OUT\_OF\_SYNC, atau NOT\_APPLICABLE).

### ListAggregateResourceSynchronizationStatuses

Mengembalikan status agregat per sumber daya di semua penerapan Anda. Filter secara opsional oleh `synchronizationStatus`. Operasi ini menunjukkan hasil gabungan dari semua kebijakan yang berlaku untuk setiap sumber daya.

Kedua operasi mendukung pagination dengan `maxResults` (1 hingga 100) dan `nextToken`.

## Memahami nilai status sinkronisasi

### IN\_SYNC

Konfigurasi firewall sumber daya yang sebenarnya cocok dengan konfigurasi efektif yang dihitung dari semua kebijakan yang berlaku.

### OUT\_OF\_SYNC

Konfigurasi sumber daya yang sebenarnya berbeda dari konfigurasi yang efektif.

`outOfSyncReasons` bidang ini menyediakan detail per pengaturan yang menunjukkan nilai yang diharapkan versus nilai aktual.

### TIDAK\_BERLAKU

Akun sumber daya dan jenis sumber daya berada dalam cakupan, tetapi sumber daya itu sendiri tidak cocok dengan filter lingkup (misalnya, filter tag mengecualikannya). Tidak diperlukan tindakan.

Jika sumber daya tidak muncul di hasil sama sekali, jenis akun atau sumber daya tidak berada dalam cakupan penerapan. Periksa konfigurasi cakupan Anda.

## Memahami stempel waktu evaluasi

Setiap entri status sinkronisasi mencakup dua stempel waktu:

- `evaluatedAt`- Ketika Manajer Keamanan AWS Jaringan terakhir mengevaluasi konfigurasi sumber daya. `evaluatedAt` nilai basis menunjukkan bahwa evaluasi belum berjalan untuk perubahan terbaru.
- `updatedAt`- Ketika catatan status sinkronisasi itu sendiri terakhir berubah. Jika `updatedAt` lebih tua dari `evaluatedAt`, statusnya sudah stabil sejak evaluasi terakhir.

## Cross-account visibilitas

Ketika beberapa administrator melindungi sumber daya yang sama, visibilitas ke status sinkronisasi agregat bergantung pada `enableCrossAccountVisibility` pengaturan pada setiap penerapan.

- Jika semua penerapan yang mencakup sumber daya mengaktifkan visibilitas lintas akun, administrator mana pun dapat melihat status agregat lengkap dan alasan tidak sinkron.

- Jika ada penyebaran yang menonaktifkan visibilitas lintas akun, administrator lain akan melihat NOT\_VISIBLE penanda alih-alih alasan terperinci. Ini menunjukkan bahwa administrator lain juga melindungi sumber daya tetapi belum berbagi visibilitas.

## Mendiagnosis sumber daya yang tidak sinkron

Ketika sumber daya melaporkan OUT\_OF\_SYNC, outOfSyncReasons bidang mengidentifikasi perbedaan konfigurasi tertentu. Alasan tingkat atas adalah salah satu dari:

- missingFirewall- Tidak ada perlindungan firewall yang terkait dengan sumber daya.
- invalidFirewall- Firewall ada tetapi konfigurasinya tidak sesuai dengan harapan. Perbedaan spesifik tercantum dalam ember yang dikategorikan.

Jika remediasi diaktifkan tetapi tidak dapat memperbaiki sumber daya, remediationIssues bidang tersebut memberikan correctiveAction panduan tentang cara menyelesaikan masalah secara manual. Remediasi adalah pengaturan tingkat kebijakan yang dimatikan secara default. Untuk informasi selengkapnya, lihat [the section called “Sinkronisasi dan remediasi”](#).

Beberapa penerapan dengan konfigurasi berbeda dapat menargetkan sumber daya yang sama. Dalam hal ini, status sinkronisasi per-penyebaran dapat OUT\_OF\_SYNC sedangkan status sinkronisasi agregat adalah IN\_SYNC. Ini adalah perilaku yang diharapkan, bukan kegagalan. Pengaturan kebijakan prioritas lebih tinggi diutamakan selama penggabungan. Akibatnya, sumber daya cocok dengan konfigurasi efektif, meskipun tidak cocok dengan konfigurasi penerapan prioritas rendah.

## Pencatatan log AWS Panggilan API Manajer Keamanan Jaringan dengan AWS CloudTrail

AWS Network Security Manager terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap semua panggilan API untuk AWS Network Security Manager sebagai peristiwa manajemen. Panggilan yang diambil termasuk panggilan dari konsol AWS Network Security Manager dan panggilan terprogram ke operasi AWS Network Security Manager API.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Manajer Keamanan AWS Jaringan. Jika

Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di Riwayat acara. Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS CloudTrail](#).

## AWS Informasi Manajer Keamanan Jaringan di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Manajer Keamanan AWS Jaringan, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan Riwayat CloudTrail acara](#).

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Manajer Keamanan AWS Jaringan, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi. Ini mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)

Semua operasi Manajer Keamanan AWS Jaringan dicatat oleh CloudTrail. Operasi publik meliputi:

- Membuat, membaca, memperbarui, dan menghapus (CRUD) operasi untuk aturan, template, kebijakan, cakupan, dan penerapan
- Operasi snapshot
- Operasi penandaan
- Operasi akun administrator
- Operasi status sinkronisasi
- Operasi asosiasi sumber daya
- Operasi pembuatan aturan

Setiap entri acara mencakup informasi berikut:

- Sumber acara: `network-security-manager.amazonaws.com`
- Nama acara, yang merupakan nama operasi API (misalnya, `CreatePolicy` atau `ListDeployments`)
- Sumber daya yang terpengaruh, diidentifikasi oleh ARN dan jenis sumber daya

Read-only operasi (seperti `GetPolicy`, `ListRules`, dan `ListResourceSynchronizationStatuses`) dicatat dengan `readOnly: true` dan tidak termasuk elemen respons. Operasi mutasi mencakup parameter permintaan dan elemen respons.

#### Note

CloudTrail menyunting bidang sensitif dari catatan peristiwa. Misalnya, CloudTrail menyunting prompt parameter dalam `GenerateRuleConfiguration` operasi.

## Contoh: CreatePolicy acara

Contoh berikut menunjukkan entri CloudTrail log untuk `CreatePolicy` operasi.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:my-session",
    "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/AdminRole",
        "accountId": "123456789012",
        "userName": "AdminRole"
      },
      "attributes": {
        "creationDate": "2026-08-10T18:22:41Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}
```

```

},
"eventTime": "2026-08-10T18:24:03Z",
"eventSource": "network-security-manager.amazonaws.com",
"eventName": "CreatePolicy",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.44",
"userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
"requestParameters": {
  "clientToken": "550e8400-e29b-41d4-a716-446655440001",
  "policyName": "production-web-acl-policy",
  "firewallType": "WAF",
  "priority": 1,
  "associatedTemplateAndRuleList": [
    {
      "templateIdentifier": "arn:aws:network-security-manager:us-
east-1:123456789012:template:t1a2b3c4d5"
    }
  ],
  "policyConfiguration": {
    "remediationEnabled": true,
    "resourcesCleanUp": false,
    "wafConfig": {
      "existingCustomerWebACLResolution": "RETROFIT",
      "conflictResolution": "MERGE_WHERE_APPLICABLE"
    }
  },
  "isPublished": true
},
"responseElements": {
  "policyId": "p9z8y7x6w5v4u3t2",
  "policyArn": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
  "policyName": "production-web-acl-policy",
  "status": "ACTIVE",
  "version": "1"
},
"requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
"eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
"readOnly": false,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::NetworkSecurityManager::Policy",

```

```
      "ARN": "arn:aws:network-security-manager:us-  
east-1:123456789012:policy:p9z8y7x6w5v4u3t2"  
    }  
  ],  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "123456789012",  
  "eventCategory": "Management"  
}
```

# AWS Kuota Manajer Keamanan Jaringan

Anda Akun AWS memiliki kuota default berikut untuk AWS Network Security Manager. Kecuali dinyatakan lain, setiap kuota adalah per akun, per Wilayah.

## Kuota sumber daya

Tabel berikut mencantumkan jumlah maksimum sumber daya Manajer Keamanan AWS Jaringan yang dapat Anda buat per akun di setiap Wilayah.

| Sumber daya              | Kuota bawaan | Dapat Disesuaikan |
|--------------------------|--------------|-------------------|
| Aturan per akun          | 200          | Tidak             |
| Templat per akun         | 100          | Tidak             |
| Kebijakan per akun       | 100          | Tidak             |
| Cakupan per akun         | 100          | Tidak             |
| Penerapan per akun       | 100          | Tidak             |
| Snapshot per sumber daya | 10           | Tidak             |

## Kuota komposisi sumber daya

Tabel berikut mencantumkan kuota untuk bagaimana sumber daya AWS Network Security Manager mereferensikan satu sama lain dalam hierarki sumber daya.

| Kuota                                                   | Nilai        |
|---------------------------------------------------------|--------------|
| Aturan per template                                     | 1 hingga 50  |
| Templat per kebijakan AWS WAF                           | 1 hingga 2   |
| Aturan dan templat digabungkan sesuai kebijakan AWS WAF | 1 hingga 100 |

| Kuota                                                    | Nilai            |
|----------------------------------------------------------|------------------|
| Templat atau aturan sesuai kebijakan AWS Shield Advanced | 0 (harus kosong) |
| Kebijakan per penerapan                                  | 1 hingga 2       |
| Cakupan per penerapan                                    | 1 (tepat satu)   |

## Kuota konfigurasi lingkup

Tabel berikut mencantumkan kuota untuk ekspresi konfigurasi lingkup.

| Kuota                                          | Nilai |
|------------------------------------------------|-------|
| Cakupan jenis sumber daya per lingkup          | 20    |
| Kedalaman ekspresi lingkup (tingkat bersarang) | 2     |
| Luas ekspresi lingkup (kriteria per level)     | 20    |

## Kuota akun administrator

Tabel berikut mencantumkan kuota untuk tingkat prioritas akun administrator AWS Network Security Manager.

| Kuota                           | Nilai       |
|---------------------------------|-------------|
| Tingkat prioritas administrator | 1 sampai 10 |

## Kuota pagination API

Tabel berikut mencantumkan batas pagination untuk operasi List.

| Kuota                                                  | Nilai |
|--------------------------------------------------------|-------|
| Hasil maksimal per halaman ( <code>maxResults</code> ) | 100   |
| Hasil minimum per halaman ( <code>maxResults</code> )  | 1     |

## Penyesuaian kuota

Kuota yang tercantum di bagian sebelumnya adalah tetap dan tidak dapat ditingkatkan saat ini.

# Riwayat dokumen untuk AWS Panduan Pengembang Manajer Keamanan Jaringan

Tabel berikut menjelaskan rilis dokumentasi untuk AWS Network Security Manager.

| Perubahan                  | Deskripsi                                                    | Tanggal         |
|----------------------------|--------------------------------------------------------------|-----------------|
| <a href="#">Rilis awal</a> | Rilis awal Panduan Pengembang Manajer Keamanan AWS Jaringan. | Agustus 1, 2026 |

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.