を使用した堅牢なネットワーク設計 AWS Control Tower

AWS 規範ガイダンス

AWS 規範ガイダンス: を使用した堅牢なネットワーク設計 AWS Control Tower

Table of Contents

序章 1
前提条件 1
一元化されたネットワークアカウント 1
堅牢なネットワーク設定 3
IPAM 4
IPAM を委任 4
IPAM 階層を設計 5
IPAM を設定 5
VPC を設定 7
ファイアウォール VPC 7
インバウンド VPC 7
アウトバウンド VPC 8
VPC フローログ 8
ネットワーク ACL 設定 8
一元化されたファイアウォール 8
ファイアウォールルールグループ 9
ファイアウォールポリシー 9
ファイアウォール 8
ファイアウォールのログ記録 10
トランジットゲートウェイの設定 10
エンドポイントの設定 11
ゲートウェイエンドポイント 12
インターフェイスエンドポイント 12
アーキテクチャ 12
分散型 DNS および Route 53 プロファイル 13
Route 53 プロファイル 14
AWS WAF 15
目的 16
リソース 17
寄稿者 18
ドキュメント履歴 19
..... xx

AWS Control Tower を使用した堅牢なネットワーク設計

Amazon Web Services (寄稿者)

2024 年 9 月 (ドキュメント履歴)

セキュリティは、あらゆる組織にとって重要な役割を果たします。アプリケーションセキュリティの主な要素の 1 つはネットワークです。ネットワークの抜け穴は、サイバー犯罪者がアプリケーションを侵害し、システムを制御するためのさまざまな手段を生み出す可能性があります。このガイドでは、AWS Control Tower を使用して AWS Organizations レベルでネットワークを設計する際のベストプラクティスをいくつか定義します。ネットワーク設計の目的は、管理の容易化、セキュリティの向上、AWS クラウド でホストされているアプリケーションの保護を実現することです。この目的を達成するために、ネットワーク設計には、インターネットに出入りするトラフィックを、AWS 内の単一の一元化されたネットワークアカウントを経由して検査、フィルタリング、ログ記録する仕組みが含まれます。

対象となるアプローチでは、3 つの仮想プライベートクラウド (VPC) を持つ一元化されたネットワークアカウントを使用します。スポーク VPC およびインターネットからのインバウンドトラフィックとアウトバウンドトラフィックは、AWS WAF と AWS Network Firewall によってフィルタリングされます。また、トラフィックのルーティングは AWS Transit Gateway および VPC エンドポイントによってサポートされます。

前提条件

- アクティブな AWS アカウント
- AWS Control Tower のセットアップ
- トランジットゲートウェイの知識
- ネットワークとネットワークセキュリティに関する知識

一元化されたネットワークアカウント

組織のネットワーク全体を管理する場合は、ネットワークコンポーネントやネットワークサービスの管理専用となる別のアカウントを用意することをお勧めします。まず、ネットワークチームはネットワークサービスを管理するためのアカウント (ネットワークアカウント) の作成を依頼します。新しいアカウントを作成したら、そのアカウント番号を控えておきます。次に、Amazon Virtual Private Cloud (Amazon VPC) の IP Address Manager (IPAM) の管理権限を、AWS Control Tower 管理アカウ

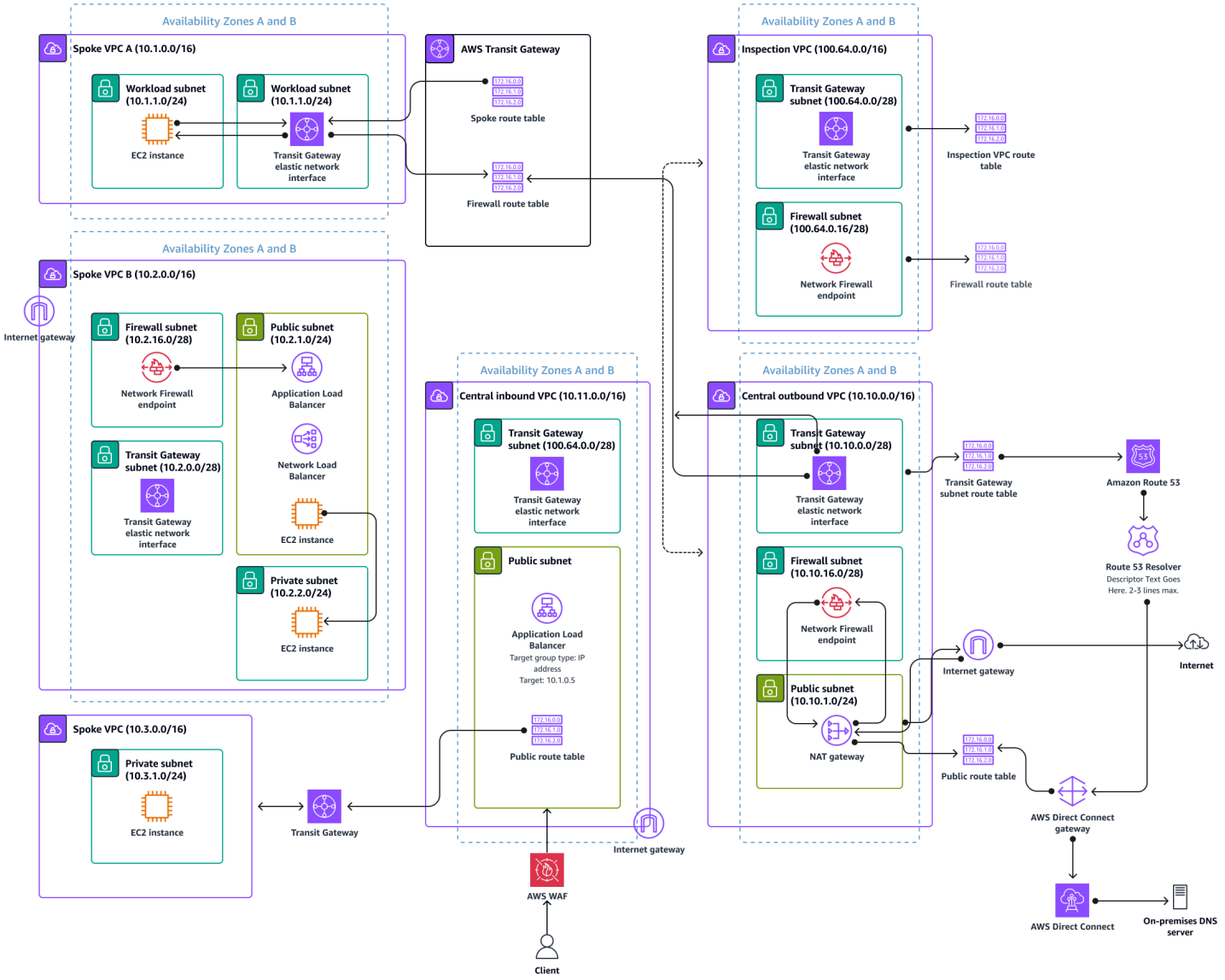
ントからネットワークアカウントに変更します。変更時には、IPAM でアカウントの詳細を指定します。

新しく作成したこのアカウントが、一元化されたネットワークアカウントとなり、次のネットワークサービスを管理します。

- IPAM
- VPC の設定
- ネットワークアクセスコントロールリスト (ACL)
- 一元化されたネットワークファイアウォール
- AWS Transit Gateway
- VPC エンドポイント設定
- 一元化された DNS 管理
- 一元化されたインバウンドトラフィック
- AWS WAF

堅牢なネットワーク設定

次の図は、組織に侵入する悪意のあるトラフィックをフィルタリングし、インターネットやインターネット上の特定のサイトに到達することを想定していないトラフィックをブロックすることによってネットワークを保護するために、理想的なネットワークがどのように構築されるべきかを示しています。また、このネットワークは、組織のセキュリティ要件に基づいて、組織内のトラフィックを制御することもできます。



組織によってホストされるサービスに送信されるすべてのインバウンドトラフィックは、トラフィックが Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに到達する AWS WAF AWS Network Firewall 前に、 によってフィルタリングされます。組織から送信されるすべてのアウトバウンドトラフィックは、送信先に到達する前に、まず Network Firewall によってフィルタリングされ

ます。Amazon Route 53 はすべての DNS 解決を管理し、DNS ログをクエリするためのソースを提供します。 AWS Transit Gateway エラスティックネットワークインターフェイスは、一元化されたネットワークを提供するのに役立ちます。

トピック

- IPAM
- VPC を設定
- ネットワーク ACL 設定
- 一元化されたネットワークファイアウォール
- トランジットゲートウェイの設定
- VPC エンドポイントの設定
- 分散型 DNS および Route 53 プロファイル
- AWS WAF

IPAM

Amazon VPC IP Address Manager (IPAM) は、組織のすべてのパブリック IP アドレスとプライベート IP アドレスを管理するのに役立つ AWS 機能です。IPAM は、IP アドレスをさまざまなビジネスユニットと特定の に分類します AWS リージョン。IPAM は、既に使用中の IP アドレスと未使用の残りの IP アドレスを追跡します。また、IP アドレスの重複を回避し、選択したネットマスクに基づいて特定の CIDR ブロックを VPC に割り当てるのにも役立ちます。

IPAM を委任

デフォルトでは、組織の IPAM 設定は AWS Control Tower 管理アカウントで利用できます。ネットワークアカウントから IPAM を管理するには、 AWS Control Tower 管理アカウントからネットワークアカウントに IPAM 管理を委任します。

1. AWS Control Tower 管理アカウントで、Amazon VPC サービスに移動します。
2. Amazon VPC IP Address Manager を開きます。
3. 左側のペインで、組織設定を選択します。
4. [編集] を選択し、アカウント作成時に控えておいたネットワークアカウント番号を入力します。
5. 変更を保存します。

委任を設定すると、その詳細がネットワークアカウントの IPAM 組織設定に反映されます。

IPAM 階層を設計

IPAM を設定する前に、以下の基準に基づいて組織に必要な構造を分析します。

- IPAM が使用する CIDR ブロック
- IPAM を介してネットワークアカウントを設定する必要があるビジネスユニット
- この IPAM で管理 AWS リージョン される

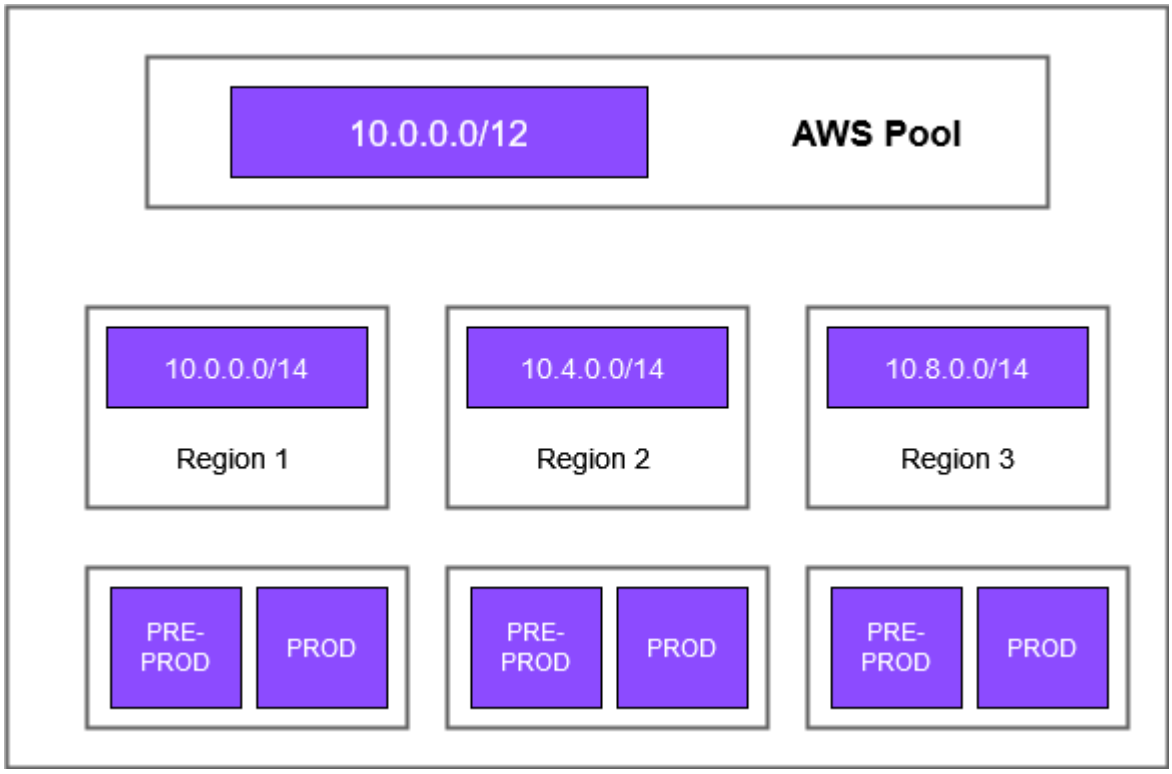
IPAM を設定

以下を実行して IPAM を設定します。

1. を開き AWS マネジメントコンソール、Amazon VPC IP Address Manager コンソールに移動します。
2. IPAM を作成します。名前、オペレーション AWS リージョン、説明を入力します。

   IPAM が作成されると、次の 2 つのスコープが含まれます。

   - パブリック: パブリック CIDR ブロックの設定と使用に使用される
   - プライベート: プライベート CIDR ブロックの設定と使用に使用される
3. 最上位の IPAM プールを作成します。次の図では、最上位プールは AWS Pool です。



4. 下位レベルのプールを作成します。
   - リージョン用のプール
   - リージョン内の本番稼働前用と本番稼働用のプール

   プールには、必ず適切なスコープを指定してください。一般的には、自社のパブリック CIDR ブロックからパブリック IP アドレスを使用してサービスをホストする場合を除き、ほとんどのネットワークでプライベートスコープを使用することをお勧めします。
5. AWS Resource Access Manager () を使用して、IPAM を他の AWS Organizations 組織単位 (OU) アカウントと共有しますAWS RAM。リソースを作成する各アカウントと IPAM を共有します。これらのアカウントは、組織のネットワーク範囲にあり、最上位の IPAM プールの一部である必要があります。

すべての VPC を作成するときは、IPAM ベースの VPC 作成を使用することをお勧めします。これにより、新しい VPC の CIDR ブロックが既存の VPC と衝突しないようにできます。新しい VPC は、あらかじめ設定したプール設定を使用して作成されます。

VPC を設定

VPC は、従来のデータセンターネットワークに似 AWS た の論理的に分離されたネットワークです。通常、堅牢なネットワークには、ネットワークアカウントに 3 つの異なる VPC が含まれます。

- ファイアウォール VPC
- インバウンド VPC
- アウトバウンド VPC

これらの各 VPC は、特定の目的のために指定されています。このガイドで説明されているものを除き、アプリケーションやその他のサービスをこれらの VPC にデプロイしないでください。

これらの VPC を作成する際は、[VPC のみ] オプションを選択します。次に、[IPAM が割り当てられた IPv4 CIDR ブロック] オプションを選択し、関連する IPAM プールを選択したうえで、適切なネットマスクを入力します。

ファイアウォール VPC

ファイアウォール VPC は、 AWS Network Firewallを使用したファイアウォールの作成と設定専用の VPC です。ファイアウォール VPC 内に、次の 6 つのプライベートサブネットを作成します。

- Transit Gateway アタッチメント専用の 3 つのサブネット
- ファイアウォール専用の 3 つのサブネット

インバウンド VPC

ネットワークアカウントを設定する際は、 AWSでホストされているサービスに送信されるトラフィックを考慮してください。インバウンド VPC では、Application Load Balancer をホストします。また、セキュリティを侵害する可能性のある悪意のあるアクティビティを防ぐために、組織の標準的な AWS WAF ファイアウォールやその他のセキュリティ関連サービスを設定します。インバウンド VPC で、次の 6 つのサブネットを作成します。

- Application Load Balancer をホストするための 3 つのパブリックサブネット
- インバウンド VPC の CIDR ブロック以外の他のネットワーク CIDR ブロックに対して、ファイアウォールへのルーティングを設定するための 3 つの Transit Gateway アタッチメントサブネット

アウトバウンド VPC

アウトバウンド VPC は、ネットワークアカウントから送信されるトラフィックを制御します。アウトバウンド VPC では、次の 6 つのサブネットを作成します。

- 3 つの異なるアベイラビリティーゾーンに設けた 3 つのパブリックサブネット (各サブネットに NAT ゲートウェイを作成)。
- 3 つのアベイラビリティーゾーンに設けた 3 つのプライベートサブネット (各サブネットには、それぞれのパブリックサブネットに作成された NAT ゲートウェイ ID への 0.0.0.0/0 ルートを含むようにルートテーブルを設定)。トランジットゲートウェイをプライベートサブネットにアタッチ。

プライベートホストゾーンをアウトバウンド VPC に関連付けます。

VPC フローログ

今後の分析のためにネットワークインターフェイスへのすべてのリクエストを記録するには、[VPC フローログ] を設定します。詳細については、「Amazon VPC ドキュメント」および「Patterns」の「Configure VPC Flow Logs for centralization across AWS アカウント」を参照してください。

ネットワーク ACL 設定

ネットワークアクセスコントロールリスト (ネットワーク ACL) は、Application Load Balancer に到達するトラフィックが分散サービス拒否攻撃 (DDoS) やその他の悪意のあるアクティビティを試みた場合に備えて、インバウンドトラフィックとアウトバウンドトラフィックの両方を検証するステートレスなサービスです。

IP アドレスまたは CIDR ブロックへのアクセスを防ぐには、ネットワーク ACL のインバウンドセクションとアウトバウンドセクションの両方に拒否ルールを追加します。ネットワーク ACL では、ルール番号がトラフィックの評価において、重要な役割を果たします。拒否ルールには、必ず適切なルール番号を付けてください。ネットワーク ACL の詳細については、「AWS Documentation」を参照してください。

一元化されたネットワークファイアウォール

ファイアウォール VPC AWS Network Firewall にデプロイします。この VPC は、送信元から送信先へのトラフィックとインターネットからのトラフィックを検査するファイアウォールをホストすることで重要な役割を果たします。

ファイアウォールルールグループ

ファイアウォール VPC からインターネット AWS マネージドルール 、およびインターネットから VPC に流れるトラフィックをモニタリングおよび管理するために、カスタムルールを定義するか、既存の を使用します。要件に基づいて、ステートフルルールまたはステートレスルールを作成します。

- ステートフルルール – パケットを検査する際に、トラフィックフローの方向やパケットに関連するその他のトラフィック承認状況が考慮されます。

  このルールグループは、Suricata 互換侵入防止システム (IPS) の要件に準拠しています。詳細については「Network Firewall ドキュメント」を参照してください。

  また、Network Firewall ではドメイントラフィックのフィルタリングもサポートしています。リストに記載された特定のドメインへのトラフィックは、標準ネットワーク属性に基づいて定義されたルールによってモニタリングされ、トラフィックフローが制御されます。
- ステートレスルール – Network Firewall のステートレスルールエンジンは、ステートレスルールグループ用に各パケットを個別に分析します。ネットワーク用のファイアウォールは、トラフィックの方向やその他の関連するパケットなどのコンテキストを考慮しません。
- AWS マネージドルール ルールグループ – Network Firewall を使用すると、 AWS マネージドルール ルールグループにアクセスできます。これらのプリセットされた使用可能なルールのコレクションは、up-to-date新しい脆弱性や脅威に基づいてルールグループ AWS を更新します。

ファイアウォールポリシー

ファイアウォールポリシーを作成します。ファイアウォールポリシーは、アタッチするルールに基づいて、ファイアウォールのモニタリングと保護の動作を定義します。これらのルールは、 によって提供されるマネージドルール、 AWS または作成したカスタムステートフルルールまたはステートレスルールにすることができます。

ファイアウォール

ファイアウォール VPC で、定義したファイアウォールポリシーを使用してファイアウォールを作成します。ファイアウォール専用の 3 つのサブネット (トランジットゲートウェイ用のサブネットではないもの) を選択します。ファイアウォールを作成したら、Network Firewall によって作成される VPC エンドポイントを書き留めます。

これらのエンドポイントにトラフィックをルーティングするように、ファイアウォール VPC のトランジットゲートウェイサブネットの送信先 0.0.0.0/0 を設定します。エンドポイントを設定する際は、各トランジットゲートウェイサブネットが対応するファイアウォールエンドポイントサブネットと一致していることを確認してください。適切なサブネットマッピングにより、トラフィックのルーティングと検査の高可用性を確保できます。

ファイアウォールのログ記録

ネットワークファイアウォールによってブロックされたトラフィックを分析するために、ファイアウォールのログ記録を有効にします。ファイアウォールのログ記録により、不正なアクティビティを特定できるだけでなく、VPC 内外で発生しているその他のアクティビティを分析することもできます。

トランジットゲートウェイの設定

最も多くの AWS リソース AWS リージョン がプロビジョニングされるか、アプリケーションがデプロイされる で、ネットワークアカウントにトランジットゲートウェイを作成します。トランジットゲートウェイを作成する際は、デフォルトのルートテーブルの伝播と関連付けをクリアします。代わりに、VPC の種類に基づいて、特定のトランジットゲートウェイルートテーブルにルートをアタッチおよび伝播させます。

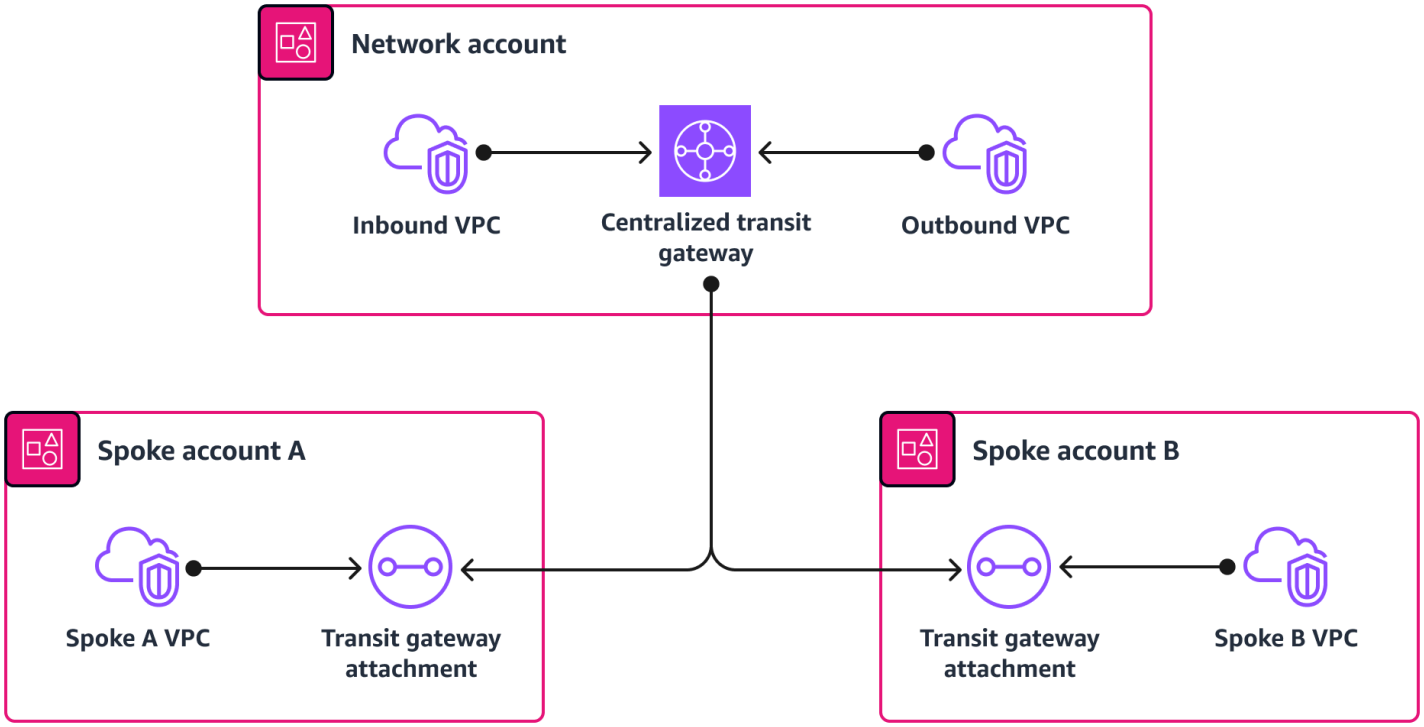
このトランジットゲートウェイでは、次の 3 つのトランジットゲートウェイルートテーブルを作成します。

- Inbound VPC トランジットゲートウェイルートテーブル:
  - 関連付け – アウトバウンド VPC とファイアウォール VPC を除く、トラフィックを検査する必要があるすべての VPC アタッチメント。
  - 伝播 — 送信先 0.0.0.0/0 をファイアウォール VPC アタッチメントに向ける静的ルート。
- ファイアウォール検査トランジットゲートウェイルートテーブル:
  - 関連付け — ファイアウォール VPC ゲートウェイアタッチメント。
  - 伝播 — ファイアウォール VPC トランジットゲートウェイルートテーブルで、ファイアウォール VPC から各 VPC アタッチメントにトラフィックをルーティングするように伝播を設定する。検査後にトラフィックをインターネットにルーティングする場合は、送信先 0.0.0.0/0 をアウトバウンド VPC に向ける静的ルートを追加する。
- Outbound トランジットゲートウェイルートテーブル:
  - 関連付け — このルートテーブルにアウトバウンド VPC アタッチメントを関連付ける。

- 伝播 — 送信先 `0.0.0.0/0` をファイアウォール VPC ゲートウェイアタッチメントに向ける静的ルートを作成する。

> **Note**
>
> ネットワークアカウントは、ネットワーク関連のサービスやコンポーネントを設定するための専用アカウントです。このネットワークアカウントには、それ以外のアプリケーションやサービスをデプロイしないでください。

次の図は、子アカウントの VPC からのトラフィックが、一元化されたネットワークアカウントとインターネットまたはその他の VPC との間でどのようにルーティングされるかを示しています。



VPC エンドポイントの設定

VPC エンドポイントはアウトバウンド VPC にのみ作成されます。アウトバウンド VPC は、組織内のすべての VPCs が AWS のサービス 安全に到達するためのソースとして機能します。これにより、VPC エンドポイントの管理が容易になります。また、個々の VPC に複数のエンドポイントを作成する代わりに、単一の送信元エンドポイントを使用するため、コストの最適化にもつながります。

ゲートウェイエンドポイント

ゲートウェイ VPC エンドポイントは、VPC にインターネットゲートウェイや NAT ゲートウェイを必要とせずに、Amazon Simple Storage Service (Amazon S3) および Amazon DynamoDB への信頼性の高い接続を提供します。ゲートウェイエンドポイントは、他のタイプの VPC エンドポイントとは異なり、 AWS PrivateLinkを使用しません。ゲートウェイエンドポイントは無料で提供されます。安全なチャネルを介してスポーク VPC から Amazon S3 と DynamoDB にアクセスする必要がある場合は、ゲートウェイエンドポイントを使用することをお勧めします。

インターフェイスエンドポイント

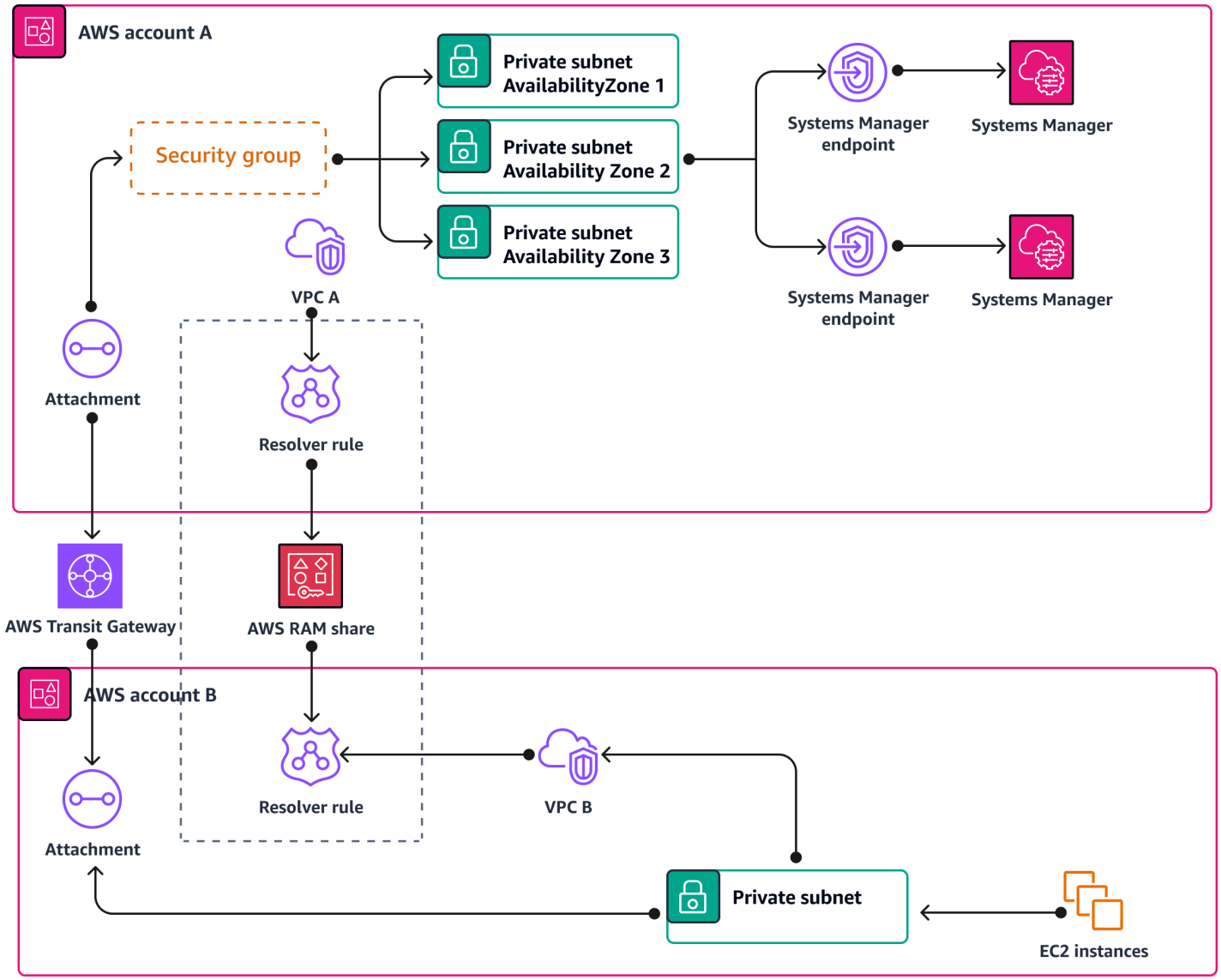
インターフェイスエンドポイントは、 のサービスと AWS エンドポイント間のプライベート通信を確立するのに役立ちます AWS PrivateLink。

アウトバウンド VPC では、必要な VPC エンドポイントを作成します。Amazon S3 と DynamoDB については、個々の VPC にゲートウェイエンドポイントを作成します。一般的に使用される VPC エンドポイントには、次のものがあります。

- Amazon S3 Control
- DynamoDB
- AWS Systems Manager

アーキテクチャ

次の図は、一元化された VPC エンドポイントを使用して、EC2 インスタンスまたは他の AWS アカウント のサービスでホスト AWS のサービス されているアプリケーションがどのように到達するかを示しています。このアーキテクチャでは、別のアカウントの VPC B の EC2 インスタンスが、VPC A で作成された VPC エンドポイントを使用して Systems Manager セッションを解決できます。



この構成では、VPC エンドポイントが組織全体で使用できる単一の一元化されたネットワークアカウントでホストされいるため、コスト削減に役立ちます。VPC エンドポイントは、1 つのアカウントから作成および管理できます。

分散型 DNS および Route 53 プロファイル

分散型 DNS アーキテクチャでは、組織はそれぞれの 内にプライベートホストゾーンを作成し AWS アカウント 、必要な VPCs。このアプローチには以下の利点があります。

- 管理の分離
- インシデント発生時の影響範囲の縮小

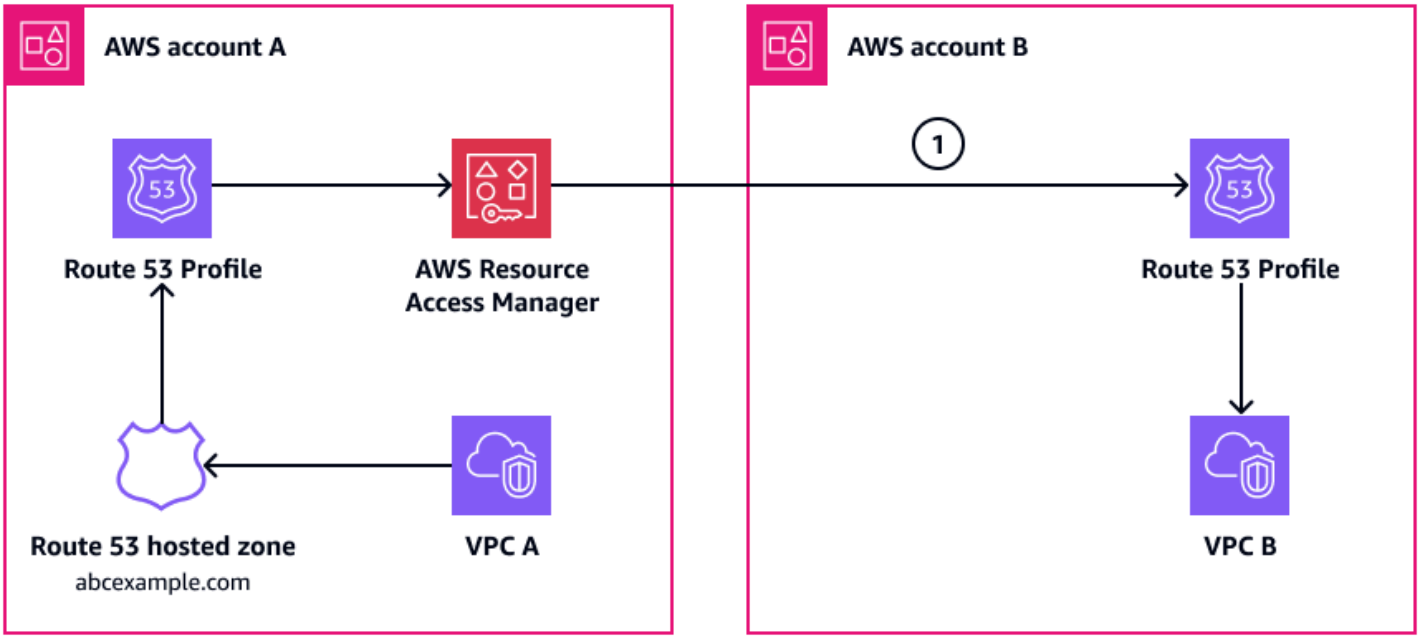
- 一元化された権限に依存することなく、チームがホストゾーンと関連付けられた VPC を個別に管理できるため、運用の柔軟性が向上

Route 53 プロファイル

Amazon Route 53 プロファイルは、異なる AWS アカウント間でホストゾーン、リゾルバー転送ルール、Route 53 DNS ファイアウォールルールの管理と共有を効率化します。これらのリソースを 1 つのソースから管理することで、運用上のオーバーヘッドを削減できます。

また、他のアカウントが作成したホストゾーンを関連付けることもできます。たとえば、オンプレミスサーバーを指すプライベートホストゾーンを設定する必要がある場合は、プライベートホストゾーンを 1 つの に作成 AWS アカウント し、Route 53 プロファイルに関連付けることができます。同じホストゾーン設定が別のアカウントで必要な場合は、プロファイルをそのアカウントと共有し、必要な VPC を関連付けます。これにより、複数のアカウント間で DNS 解決が可能になり、各アカウントでホストゾーンの設定を複製する必要はありません。

次の図は、Route 53 Profile Sharing AWS Resource Access Manager (AWS RAM) の設定を示しています。Route 53 プロファイルは、単一のアカウント、 AWS Organizations の組織単位、または組織全体で共有できます。



この図表は、次のワークフローを示しています:

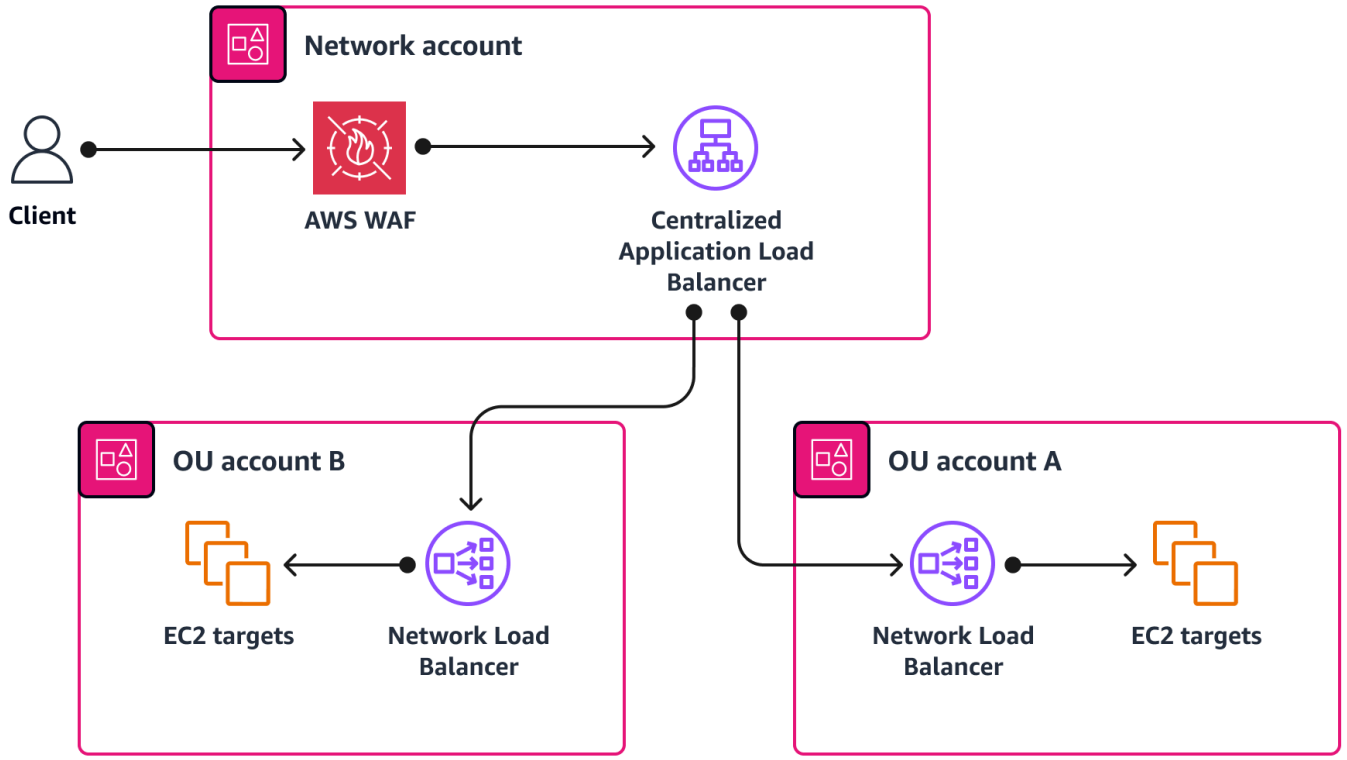
1. Route 53 プロファイルは、アカウント A からアカウント B に共有されています。

> **Note**
>
> 分散型 DNS と Route 53 プロファイルを使用する場合は、同じホストゾーン設定をアカウントまたは VPC 間で重複しないようにすることをお勧めします。

AWS WAF

をソース AWS WAF として使用して、クロスサイトスクリプティング、SQL インジェクション、DDoS などの脆弱性攻撃からアプリケーションを保護することができます。堅牢なネットワークアプローチを実現するには、Application Load Balancer AWS WAF の前に を設定し、組織全体で従うべき AWS WAF ルールを定義します。これにより、組織全体でホストされているサービスに到達するトラフィックがセキュリティのベストプラクティスを満たし、トラフィックが組織の環境に入る前にセキュリティがチェックされます。

次の図は、ネットワークアカウントの Application Load Balancer AWS WAF を通過するインバウンドトラフィックを示しています。ネットワークアカウントからは、そのトラフィックが OU アカウントの Network Load Balancer または Application Load Balancer にルーティングされ、ターゲット EC2 インスタンスに送信されます。



目標と利点

このガイドの設定セットを実装することで、次の結果を実現できます。

- 組織全体の CIDR を管理する Amazon VPC IP Address Manager (IPAM)
- AWS Transit Gateway で設定されたハブアンドスポークネットワーキングモデル
- トラフィックを検査するためのネットワークファイアウォール
- ネットワークファイアウォール内の一元化されたインバウンドエンドポイントを介した、すべてのアプリケーションの単一のエントリポイント
- インターネットトラフィックの単一の VPC 出口
- DNS 解決を管理できる単一の場所
- 組織全体のセキュリティの向上
- 組織全体のトラフィックのルーティングを制御できる単一の場所
- VPC エンドポイントへの安全なアクセス

リソース

- IPAM ドキュメント
- 「IP Address Management for AWS Control Tower」(ブログ記事)
- 「Securely scale multi-account architecture with AWS Network Firewall and AWS Control Tower」(ブログ記事)
- 「Simplify DNS management in a multi-account environment with Route 53 Resolver」(ブログ記事)
- 「Customizing AWS Control Tower」(ワークショップ)
- 「Extending your Landing Zone: Networking」(ワークショップ)

寄稿者

このガイドの寄稿者は次のとおりです。

- T.V.R.L.Phani Kumar Dadi (コンサルタント – DevOps、AWS)
- Chintamani Aphale (リードコンサルタント、AWS)
- Jagdish Komakula (シニアリードコンサルタント、AWS)
- Pratap Kumar Nanda (リードコンサルタント – DevOps、AWS)
- Pradip kumar Pandey (リードコンサルタント – DevOps、AWS)
- Aarti Rajput (リードコンサルタント、AWS)
- Mayuri Shinde (コンサルタント – DevOps、AWS)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
情報を削除	集中型 DNS と集中型インバウンドトラフィックに関するセクションを削除しました。	2024 年 9 月 30 日
の情報を追加しました。	分散型 DNS と Amazon Route 53 プロファイルに関するセクションを追加しました。	2024 年 9 月 20 日
初版発行	—	2023 年 12 月 27 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。