Cisco Secure Firewall Management Center での DIA を使用したインターネットへのアプリケーション トラフィックのルーティング

2025 年 9 月

ダイレクト インターネット アクセスを使用したブランチからインターネットへのアプリケーション トラフィックのルーティング

従来のネットワーク展開では一般に、境界ファイアウォールと暗号化された VPN トンネルを使用して、すべてのインターネットトラフィックが中央サイトを通過するようにルーティングされます。これにより、遅延、パケット損失、コストの増加、および管理の複雑化が発生する可能性があります。

Cisco Secure Firewall の主要な SD-WAN 機能であるダイレクト インターネット アクセス（DIA）は、中央サイトをバイパスして、ブランチオフィスのアプリケーション トラフィックをインターネットに直接ルーティングすることで、これらの課題に対処します。DIA は、ポリシーベース ルーティング（PBR）を使用して、ネットワーク、ポート、ユーザーグループ、アプリケーション、セキュリティグループタグ（SGT）などの属性に基づいてトラフィックを識別し、転送することで、遅延を短縮し、ユーザー体験を向上させます。このアプローチでは、ブランチファイアウォールでローカルインターネット出口ポイントを有効にすることで、ネットワーク管理が簡素化され、帯域幅の消費が削減され、パフォーマンスが向上します。

PBR を使用してトラフィックを誘導する方法には以下があります。

- 送信元 IP アドレスベースのルーティング（バージョン 7.1 以降）
- アプリケーション認識型ルーティング（バージョン 7.1 以降）
- パスモニタリングを使用したアプリケーション認識型ルーティング
  - IP ベース（バージョン 7.2 以降）
  - HTTP ベース（バージョン 7.4 以降）
- アイデンティティベースのルーティング（AD ユーザー、ユーザーグループ、および SGT）（バージョン 7.4 以降）

ダイレクト インターネット アクセスを使用する利点

- 遅延、パケット損失、およびジッターを減らすことにより、インターネット速度とブランチオフィスのユーザー体験を向上させます。
- 中央サイトでの帯域幅使用量を削減します。
- リアルタイム評価指標に基づいてダイナミックなパス選択を行うインテリジェント アプリケーション ルーティングを有効にします。これにより、手動の操作は不要になります。
- リンクの正常性およびネットワークの状態に基づいてアプリケーション トラフィックを誘導します。

ダイレクト インターネット アクセスを設定するためのワークフロー

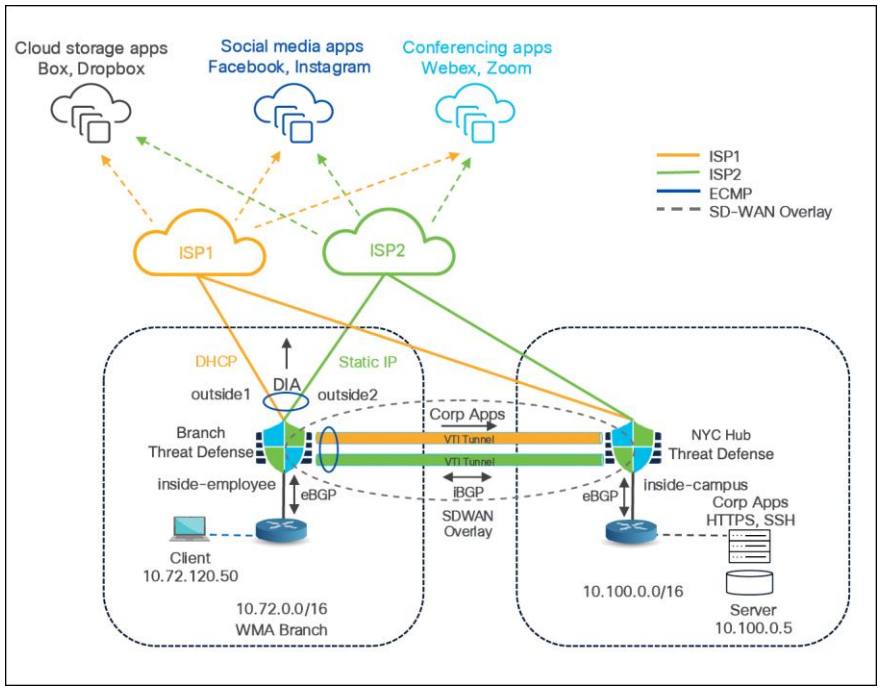
ダイレクト インターネット アクセスの設定

この例では、PBR ルーティングに Firepower 1120（WMA-FW-01）を使用して、ウースター、MA（WMA）の SD-WAN ブランチを使用します。次の 2 つの WAN インターフェイスがあります。

- ISP1 の outside1
- ISP2 の outside2

LAN に接続されているインターフェイスは **inside-employee** です。

理解しやすいように、この例ではニューヨーク市、NY（NYC）のハブデバイスのみを使用しています。



ECMP ゾーンの作成

ECMP ゾーンを作成して、出力インターフェイス間でトラフィックの負荷を分散します。

ステップ 1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2. デバイス（WMA-FW-01）の横にある [編集（Edit）] アイコンをクリックします。

ステップ 3. [ルーティング（Routing）] タブをクリックします。

ステップ 4. [ECMP] をクリックします。

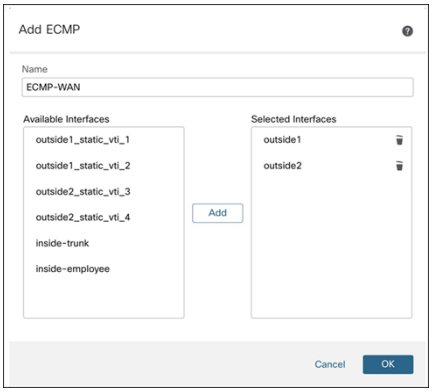
ステップ 5. [Add] をクリックします。

ステップ 6. [ECMPの追加（Add ECMP）] ダイアログボックスに、ECMP ゾーンの名前を入力します。

この例では、ECMP ゾーンは **ECMP-WAN** です。

ステップ 7. ECMP ゾーンの [使用可能なインターフェイス（Available Interfaces）] リストでインターフェイスを選択し、[追加（Add）] をクリックします。

この例では、選択された出力インターフェイスは **outside1** および **outside2** です。



ステップ 8. [OK] をクリックします。

[ECMP] ページに、新しく作成された ECMP ゾーンが表示されます。

ステップ 9. [保存（Save）] をクリックします。

手順 1 ～ 9 を繰り返して、デバイスの 4 つのスタティック VTI を使用する別の ECMP ゾーン（**ECMP-VTI**）を作成します。この ECMP ゾーンは、これらの VTI 間のトラフィック負荷を共有します。選択する必要があるデバイスの 4 つのスタティック VTI は、次のとおりです。

- outside1_static_vti_1（outside1 インターフェイスを使用する SVTI から NYC へのハブ）
- outside1_static_vti_2（outside1 インターフェイスを使用する SVTI から NNJ へのハブ）
- outside2_static_vti_3（outside2 インターフェイスを使用する SVTI から NNJ へのハブ）
- outside2_static_vti_4（outside2 インターフェイスを使用する SVTI から NYC へのハブ）

インターフェイスでのパスモニタリングの設定

ステップ 1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2. デバイス（**WMA-FW-01**）の横にある [編集（Edit）] アイコンをクリックします。

ステップ 3. [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4. インターフェイス（**outside1**）の横にある [編集（Edit）] アイコンをクリックします。

ステップ 5. [パスモニタリング（Path Monitoring）] タブをクリックします。

ステップ 6. [IPベースのパスモニタリングの有効化（Enable IP based Path Monitoring）] チェックボックスをオンにします。

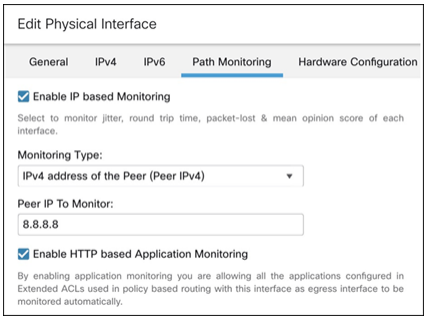
ステップ 7. [モニタリングタイプ（Monitoring Type）] ドロップダウンリストから、該当するオプションを選択します。

この例では、[ピアのIPv4アドレス（ピアIPv4）（IPv4 address of the Peer (Peer IPv4)）] オプションを選択します。

注： デバイスが PBR のメトリックを収集できるように、ピアに到達できることを確認します。

ステップ 8. [モニターするピアIP（Peer IP To Monitor）] フィールドで、ピアデバイスの IP アドレスを入力します。

この例の IP アドレスは **8.8.8.8** です。



ステップ 9. [OK] をクリックします。

手順 1 ～ 9 を繰り返して、デバイスの **outside2** インターフェイスでのパスモニタリングを設定します。

DNS サーバー グループ オブジェクトの作成

信頼できる DNS サーバーを設定する前に、1 つ以上の DNS サーバーグループを作成する必要があります。DNS サーバーグループは、Threat Defense デバイスがこれらの承認済みサーバーからの DNS 応答を信頼できるようにするために、信頼できる DNS サーバー内に定義されます。

前提条件

- DNS サーバーに接続するインターフェイスがあることを確認します。
- 管理対象デバイスに、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあることを確認します。

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. 左側のペインで [Network] をクリックします。

ステップ 3. [ネットワークの追加（Add Network）] をクリックして、ドロップダウンリストから [オブジェクトの追加（Add Object）] を選択します。

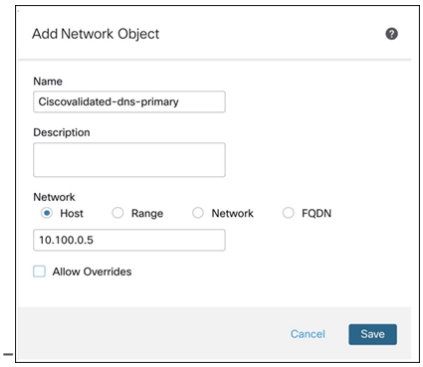
ステップ 4. [名前（Name）] フィールドに、DNS サーバーオブジェクトの名前を入力します。

この例では、**Ciscovalidated-dns-primary** と **Ciscovalidated-dns-secondary** の 2 つの DNS サーバーオブジェクトを作成します。

ステップ 5. [ホスト（Host）] オプションボタンを選択して、DNS サーバーの IP アドレスを入力します。

この例では、DNS サーバーの IP アドレスは次のとおりです。

- **Ciscovalidated-dns-primary**：**10.100.0.5**
- **Ciscovalidated-dns-secondary**：**10.200.0.5**



ステップ 6. [保存（Save）] をクリックします。

信頼された **DNS** サーバーの設定

Threat Defense デバイスが承認済み DNS サーバーからの DNS 応答をスヌープできるように、設定した DNS サーバーグループを信頼できる DNS サーバーとして定義する必要があります。

ステップ 1. [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択します。

ステップ 2. Threat Defense ポリシーを作成または編集します。

ステップ 3. この例では、Threat Defense ポリシーは **Threat-defense-setting-policy** であり、**WMA-FW-01** デバイスに割り当てられています。

ステップ 4. 左側のペインで [DNS] をクリックします。

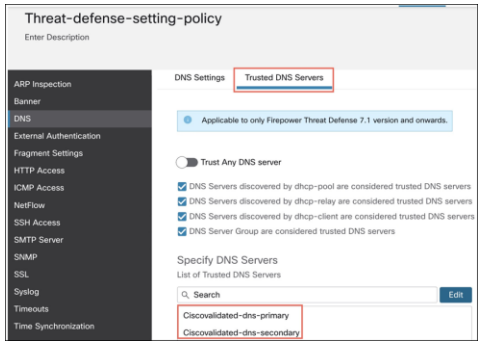
ステップ 5. [信頼できるDNSサーバー（Trusted DNS Servers）] タブをクリックします。

ステップ 6. [DNSサーバーの指定（Specify DNS Servers）] で [編集（Edit）] をクリックします。

ステップ 7. [DNSサーバーの選択（Select DNS Servers）] ダイアログボックスで、必要なホストオブジェクトを選択し、[追加（Add）] をクリックして、[選択済みDNSサーバー（Selected DNS Servers）] リストに追加します。

この例では、**Ciscovalidated-dns-primary** と **Ciscovalidated-dns-secondary** の 2 つの DNS サーバーオブジェクトを選択します。

ステップ 8. [保存（Save）] をクリックします。DNS サーバーが、[信頼されたDNSサーバー（Trusted DNS Servers）] ページに表示されます。



拡張 **ACL** オブジェクトの設定

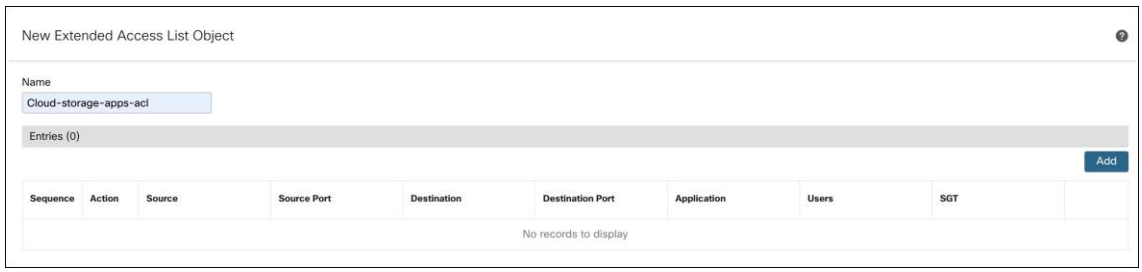
Threat Defense デバイスの拡張 ACL を設定して、PBR を使用してさまざまな出力インターフェイスを介してアプリケーショントラフィックをインターネットに転送する必要があります。

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. 左側のペインで、[アクセスリスト（Access Lists）] > [拡張（Extended）] をクリックします。

ステップ 3. [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。

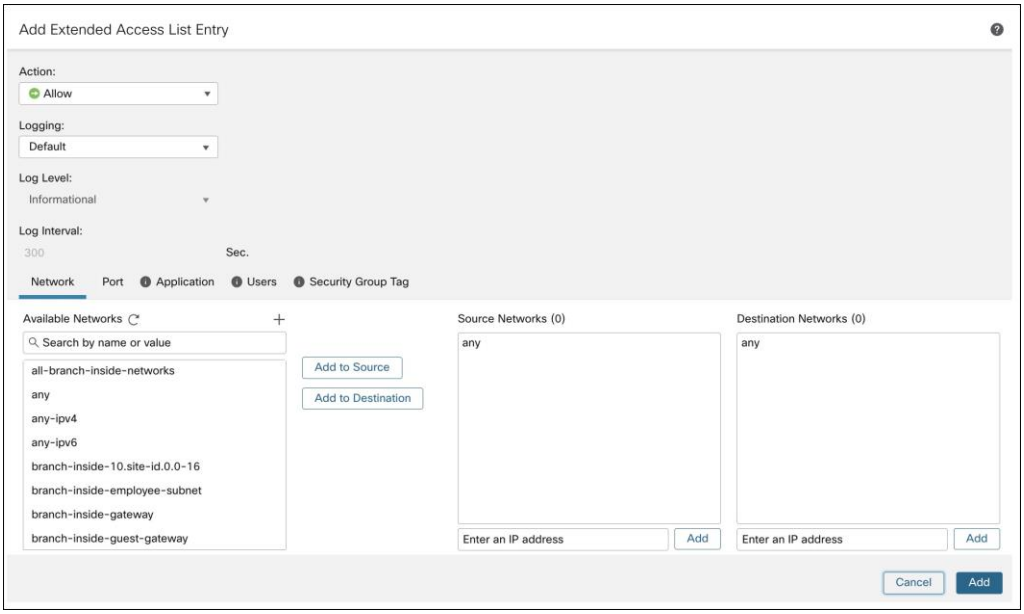
ステップ 4. [新規拡張ACLオブジェクト（New Extended ACL Object）] ダイアログボックスで、次のパラメータを設定します。



i. [名前（Name）] フィールドにオブジェクトの名前を入力します。

ii. [追加（Add）] をクリックして、新しい拡張アクセスリストを作成します。

iii. [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、パラメータを設定します。

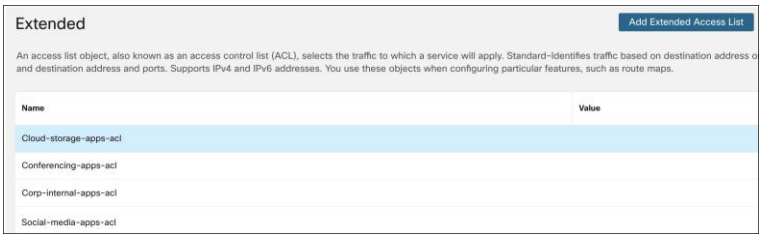


iv. [アクション（Action）] ドロップダウンリストから、[許可（Allow）] を選択します。

v. [ネットワーク（Network）]、[ポート（Port）]、[アプリケーション（Application）]、[ユーザー（Users）]、または [セキュリティグループタグ（Security Group Tag）] タブをクリックし、必要なアクセス制御プロパティを選択します。

vi. [追加（Add）] をクリックします。

ステップ 5. [保存（Save）] をクリックします。拡張 ACL が、[拡張ACL（Extended ACL）] ページに表示されます。



例 1:

Box や Dropbox などのクラウド ストレージ アプリケーション用の拡張 ACL を作成します。

[新規拡張ACLオブジェクト（New Extended ACL Object）] ダイアログボックスで、次のパラメータを設定します。

a. [名前（Name）] フィールドに、オブジェクトの名前（**Cloud-storage-apps-acl**）を入力します。

b. [追加（Add）] をクリックして、新しい拡張アクセスリストを作成します。

c. [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、パラメータを設定します。

d. [アクション（Action）] ドロップダウンリストから、[許可（Allow）] を選択します。

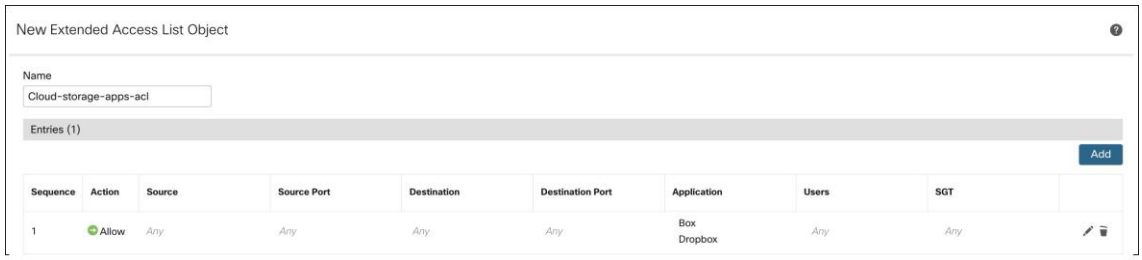
e. [Network] タブをクリックします。

f. デフォルトでは、[送信元ネットワーク（Source Network）] と [接続先ネットワーク（Destination Network）] は [すべて（any）] です。

g. [Application] タブをクリックします。[使用可能なアプリケーション（Available Applications）] リストで、[Box] と [Dropbox] を検索します。

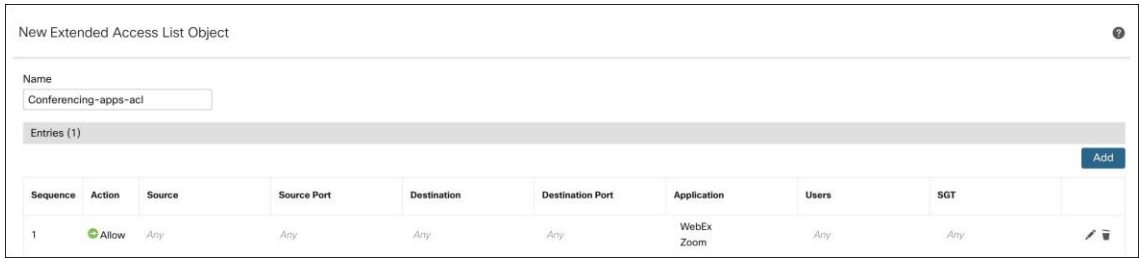
h. [Box] と [Dropbox] を選択し、[ルールに追加（Add to Rule）] をクリックします。

i. [保存（Save）] をクリックします。



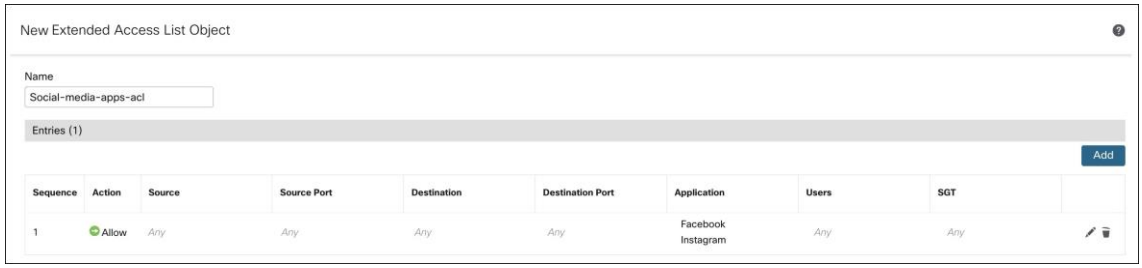
例 2：

例 1 の手順を繰り返し、**Webex** や **Zoom** などの会議アプリケーション用の拡張 ACL（**Conferencing-apps-acl**）を作成します。



例 3：

例 1 の手順を繰り返し、**Facebook** や **Instagram** などのソーシャル メディア アプリケーション用の拡張 ACL（**Social-media-apps-acl**）を作成します。



例 4：

ブランチ LAN 内のアプリケーションにアクセスするための拡張 ACL（**Corp-internal-apps-acl**）を作成します。

[新規拡張ACLオブジェクト（New Extended ACL Object）] ダイアログボックスで、次のパラメータを設定します。

a. [名前（Name）] フィールドに、オブジェクトの名前（**Corp-internal-apps-acl**）を入力します。

b. [追加（Add）] をクリックして、新しい拡張アクセスリストを作成します。

c. [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、パラメータを設定します。

d. [アクション（Action）] ドロップダウンリストから、[許可（Allow）] を選択します。

e. [Network] タブをクリックします。

f. [送信元ネットワーク（Source Network）] では、WMA ブランチの内部ネットワークオブジェクトを追加する必要があります。

g. 必要なら、[使用可能なネットワーク（Available Networks）] の横にある [+] をクリックして、ネットワークオブジェクトを作成します。この例では、**WMA-inside-10.72.0.0-16** で、IP アドレスは **10.72.0.0/16** です。

h. [使用可能なネットワーク（Available Networks）] で、**WMA-inside-10.72.0.0-16** を検索します。

i. [Add to Source] をクリックします。

j. [接続先ネットワーク（Destination networks）] では、NYC ハブおよび NNJ ハブの内部ネットワークオブジェクトを追加します。

k. 必要なら、[使用可能なネットワーク（Available Networks）] の横にある [+] をクリックして、ネットワークオブジェクトを作成します。この例では、**NNJ-inside-10.200.0.0-16**（IP アドレス **10.200.0.0/16**）と、**NYC-inside-10.100.0.0-16**（IP アドレス **10.100.0.0/16**）です。

l. [使用可能なネットワーク（Available Networks）] で、**NNJ-inside-10.200.0.0-16** と **NYC-inside-10.100.0.0-16** を検索します。

m. [接続先に追加（Add to Destination）] をクリックします。

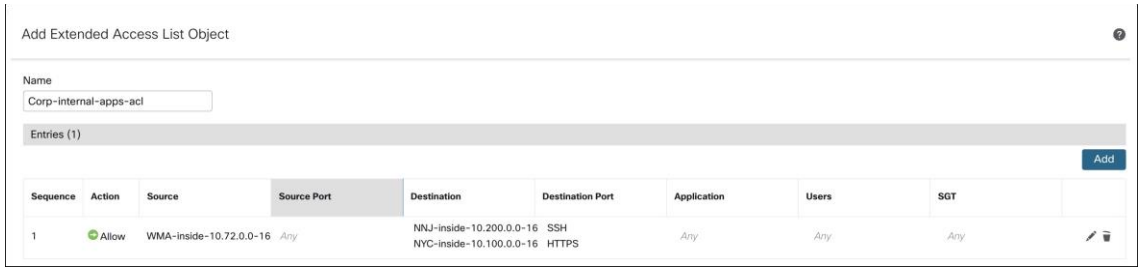
n. [ポート（Port）] タブをクリックします。

o. [使用可能なポート（Available Ports）] リストで、**SSH** と **HTTPS** を検索します。

p. [接続先に追加（Add to Destination）] をクリックします。

q. [使用可能なアプリケーション（Available Applications）] リストで **SSH** と **HTTPS** を検索し、[ルールに追加（Add to Rule）] をクリックします。

r. [保存（Save）] をクリックします。



インターフェイスの優先順位の設定

ステップ 1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2. デバイス（WMA-FW-01）の横にある [編集（Edit）] アイコンをクリックします。

ステップ 3. [ルーティング（Routing）] タブをクリックします。

ステップ 4. 左側のペインで、[ポリシーベースルーティング（Policy Based Routing）] をクリックします。

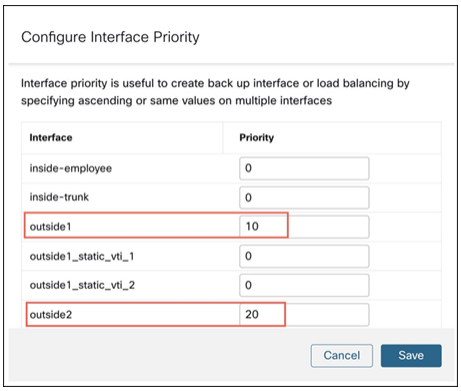
ステップ 5. [インターフェイスの優先順位の設定（Configure Interface Priority）] をクリックします。

ステップ 6. [インターフェイスの優先順位の設定（Configure Interface Priority）] ダイアログボックスで、インターフェイスに対して優先順位番号を指定します。

トラフィックは、優先度が最も低いインターフェイスに最初にルーティングされます。インターフェイスが使用できない場合、トラフィックは次に優先順位値が低いインターフェイスに転送されます。すべてのインターフェイスで優先度値が同じである場合、トラフィックはインターフェイス間で分散されます。

この例では、outside1 インターフェイスの優先順位は 10 で、outside2 インターフェイスの優先順位は 20 です。

ステップ 7. [保存（Save）] をクリックします。



ポリシー ベース ルーティング ポリシーの設定

ステップ 1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2. デバイス（WMA-FW-01）の横にある [編集（Edit）] アイコンをクリックします。

ステップ 3. [ルーティング（Routing）] タブをクリックします。

ステップ 4. 左側のペインで、[ポリシーベースルーティング（Policy Based Routing）] をクリックします。

ステップ 5. [追加（Add）] をクリックします。

ステップ 6. [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストからインターフェイスを選択します。

> **注：** ドロップダウンには、論理名を持ち、グローバル仮想ルータに属するインターフェイスのみが表示されます。

この例では、入力インターフェイスは **inside-employee** です。

ステップ 7. [追加（Add）] をクリックして、ポリシーの一致基準と転送アクションを指定します。

ステップ 8. [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、以下のパラメータを設定します。

i. [一致ACL（Match ACL）] ドロップダウンから、拡張 ACL を選択します。

ii. [送信先（Send To）] ドロップダウンリストから、[出力インターフェイス（Egress Interfaces）] を選択します。

iii. [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから、[インターフェイスプライオリティ（Interface Priority）]、[順序（Order）]、[最小ジッター（Minimal Jitter）]、[最大平均オピニオン評点（Maximum Mean Opinion Score）]、[最小ラウンドトリップ時間（Minimal Round Trip Time）]、または [最小パケット損失（Minimal Packet Loss）] の内のいずれかを選択します。以下に例を示します。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、インターフェイスの横にある [+] をクリックして、選択した出力インターフェイスを追加します。

v. [保存（Save）] をクリックします。

ステップ 9. デバイスに PBR ポリシーを展開します。

例 1:

優先順位の低い出力インターフェイスを介してクラウド ストレージ アプリケーション トラフィックを転送するように、PBR ポリシーを設定します。

ステップ 1. [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから **inside-employee** を選択します。

ステップ 2. [追加（Add）] をクリックします。

ステップ 3. [転送アクションの追加（Add Forwarding Actions）] ***ダイアログ***ボックスで、以下のパラメータを設定します。

i. [一致ACL（Match ACL）] ドロップダウンリストから、**Cloud-storage-apps-acl** を選択します。

ii. [送信先（Send To）] ドロップダウンリストから、[出力インターフェイス（Egress Interfaces）] を選択します。

iii. [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [インターフェイスプライオリティ（Interface Priority）] を選択します。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、**outside1** および **outside2** の横にある [+] をクリックします。

v. [保存（Save）] をクリックします。

例 2 :

RTT が最短の出力インターフェイスを介してソーシャル メディア アプリケーション トラフィックを転送するように、PBR ポリシーを設定します。

ステップ 1. [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから **inside-employee** を選択します。

ステップ 2. [追加（Add）] をクリックします。

ステップ 3. [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、以下のパラメータを設定します。

i. [一致ACL（Match ACL）] ドロップダウンリストから、**Social-media-apps-acl** を選択します。

ii. [送信先（Send To）] ドロップダウンリストから、[出力インターフェイス（Egress Interfaces）] を選択します。

iii. [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから、[最短ラウンドトリップ時間（Minimal Round Trip Time）] を選択します。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、**outside1** および **outside2** の横にある [+] をクリックします。

v. [保存（Save）] をクリックします。

例 3 :

ジッターが最小の出力インターフェイスを介して会議アプリケーション トラフィックを転送するように、PBR ポリシーを設定します。

ステップ 1. [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから **inside-employee** を選択します。

ステップ 2. [追加（Add）] をクリックします。

ステップ 3. [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、以下のパラメータを設定します。

i. [一致ACL（Match ACL）] ドロップダウンリストから、**Conferencing-apps-acl** を選択します。

ii. [送信先（Send To）] ドロップダウンリストから、[出力インターフェイス（Egress Interfaces）] を選択します。

iii. [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから、[最小ジッター（Minimal Jitter）] を選択します。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、**outside1** および **outside2** の横にある [+] をクリックします。

v. [保存（Save）] をクリックします。

例 4：

複数の出力 VTI トンネルインターフェイス間で ECMP を使用して企業のアプリケーション トラフィックを転送するように、PBR ポリシーを設定します。

ステップ 1. [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから **inside-employee** を選択します。

ステップ 2. [追加（Add）] をクリックします。

ステップ 3. [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、以下のパラメータを設定します。

i. [一致ACL（Match ACL）] ドロップダウンリストから、**Corp-internal-apps-acl** を選択します。

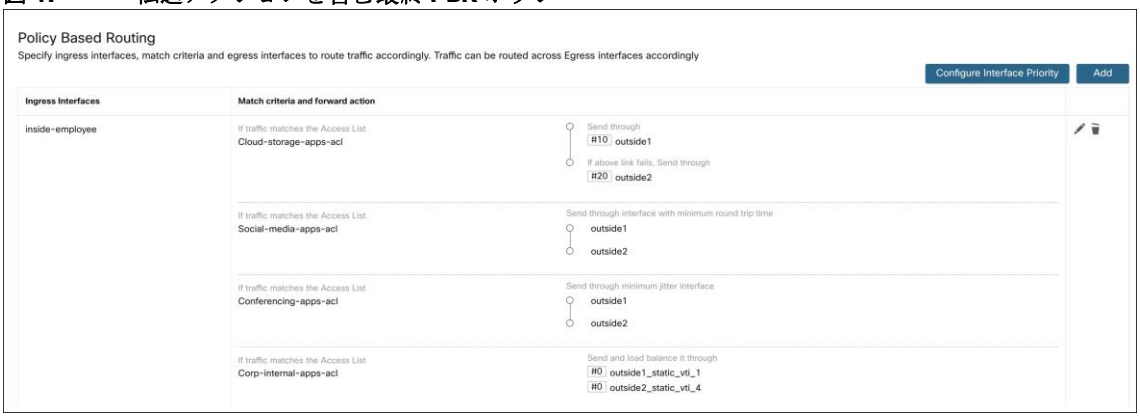
ii. [送信先（Send To）] ドロップダウンリストから、[出力インターフェイス（Egress Interfaces）] を選択します。

iii. [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [インターフェイスプライオリティ（Interface Priority）] を選択します。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、**outside1_static_vti_1** および **outside2_static_vti_4** の横にある [+] をクリックします。これらはニューヨーク市、NY（NYC）ハブデバイスで終了する VTI です。

v. [保存（Save）] をクリックします。

図 1.　　転送アクションを含む最終 PBR ポリシー



設定の確認

Management Center またはデバイス CLI を使用して設定を確認できます。

Management Center を使用してデバイス設定を表示するには、次の手順を実行します。

ステップ 1.　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

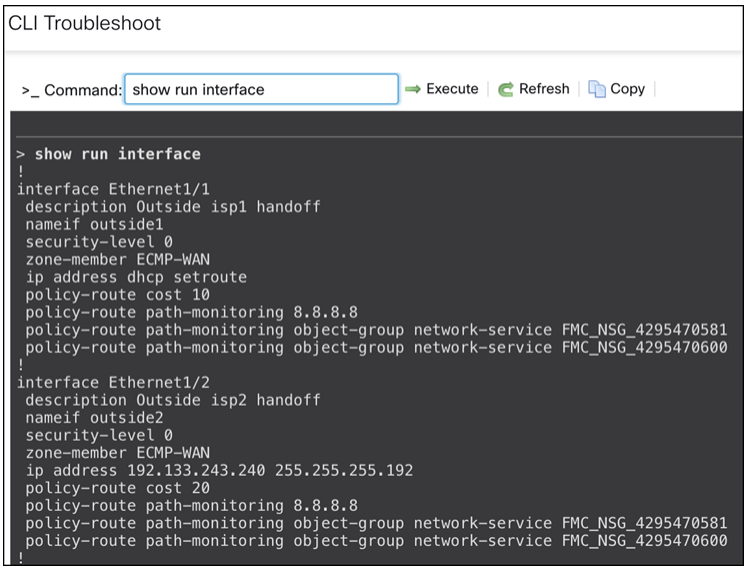
ステップ 2.　[デバイス（Device）] タブをクリックします。

ステップ 3.　[全般（General）] カードの [CLI] をクリックします。

ステップ 4.　[CLIのトラブルシュート（CLI Troubleshoot）] ダイアログボックスで、[コマンド（Command）] フィールドに以下のコマンドを入力し、[実行（Execute）] をクリックします。

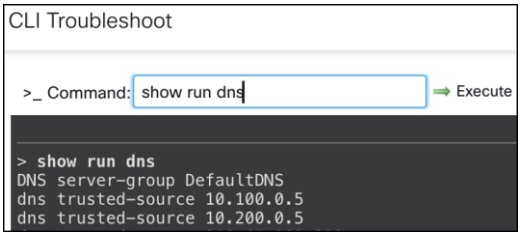
インターフェイス構成の確認

`show run interface` コマンドを実行して、デバイスのインターフェイス構成を表示します。



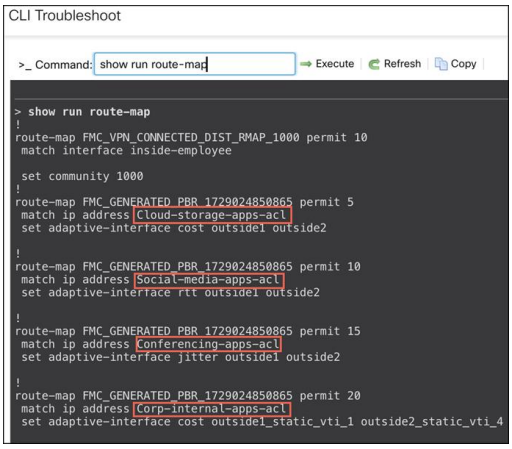
DNS 設定の確認

`show run interface` コマンドを実行して、デバイスのインターフェイス構成を表示します。



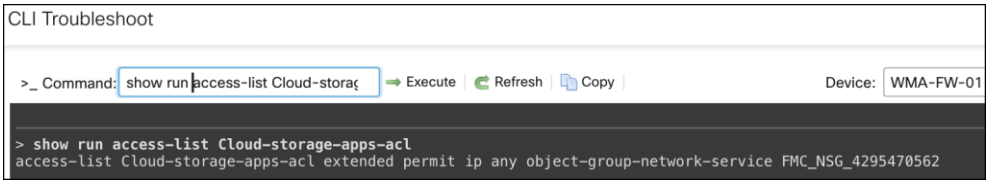
ルートマップ設定の確認

`show run route-map` コマンドを実行して、デバイスのルートマップを表示します。

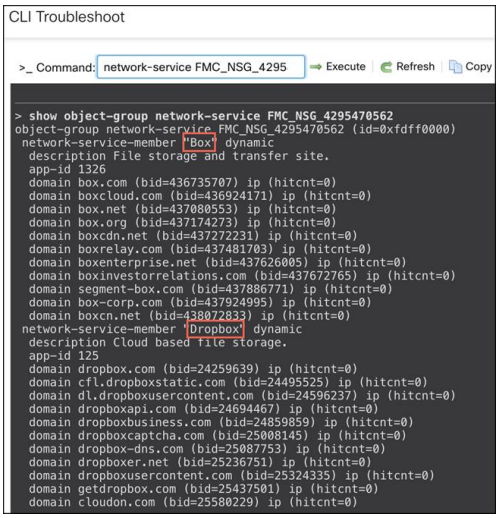


アクセスリストおよびネットワーク サービス グループ設定の確認

`show run access list <access list_name>` コマンドを実行して、アクセスリストの詳細を表示します。

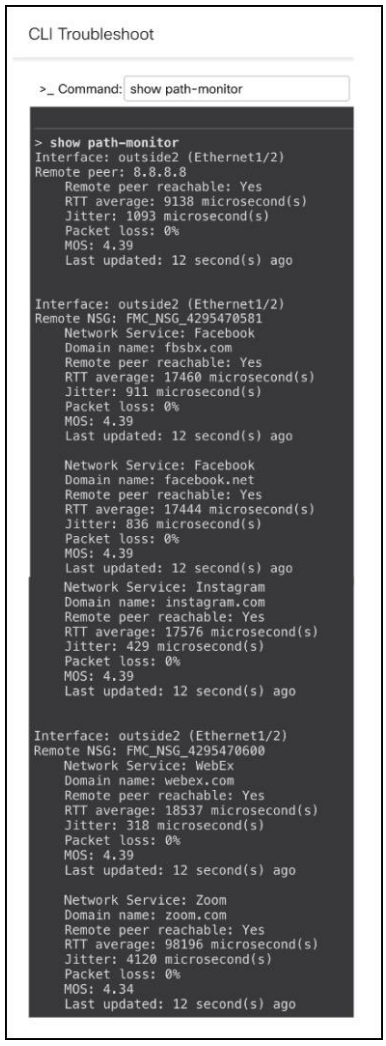


`show object-group network-service <network-service-groups-name>` コマンドを実行して、NSG 設定を表示します。`<network-service-groups-name>` は、アクセスリストに関する上記の **show** コマンドで確認できます。



パスモニタリング設定の確認

`show path-monitor` コマンドを実行して、パスモニタリング設定を表示します。



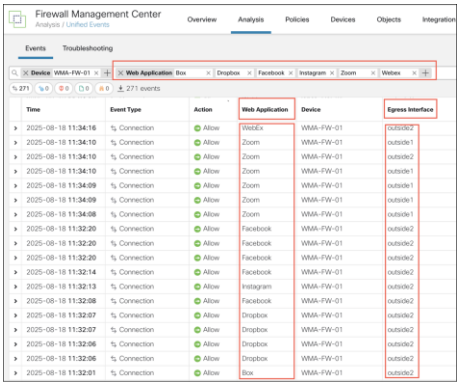
アプリケーション トラフィック フローの確認

ステップ 1. [分析（Analysis）] > [統合イベント（Unified Events）] を選択します。

ステップ 2. [列ピッカー（Column Picker）] アイコンを使用して列をカスタマイズします。[Webアプリケーション（Web Application）] と [出力インターフェイス（Egress Interface）] を選択し、[適用（Apply）] をクリックします。

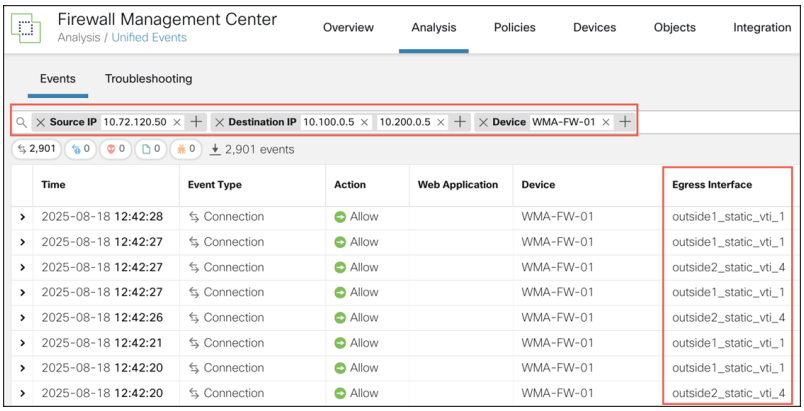
ステップ 3. 確認しやすいように列の順序を変更します。

ステップ 4. [Webアプリケーション（Web Application）] フィルタ内で、[Box]、[Dropbox]、[Facebook]、[Instagram]、[WebEx]、[Zoom] を入力し、[適用（Apply）] をクリックします。このページには、PBR ポリシーで定義したさまざまなアプリケーションの、Threat Defense デバイスにより選択された出力インターフェイスが表示されます。



ステップ 5. [Webアプリケーション（Web Application）] フィルタを削除します。

ステップ 6. フィルタ内で、[送信元IP（Source IP）] に **10.72.120.50（WMA-inside-nw）**、[宛先IP（Destination IP）] に **10.100.0.5（NYC-internal-nw）**および **10.200.0.5（NNJ-internal-nw）**を追加して、WMA LAN から NYC ハブおよび NNJ ハブへのトラフィックのイベントを表示します。



SD-WAN トポロジとアプリケーション トラフィックのモニター

SD-WAN サマリーダッシュボード（[概要（Overview ）]、[ダッシュボード（Dashboards）]、[SD-WANサマリー（SD-WAN Summary）]）を使用して、SD-WAN トポロジとそのアプリケーション トラフィックをモニターできます。このダッシュボードは、次の操作に役立ちます。

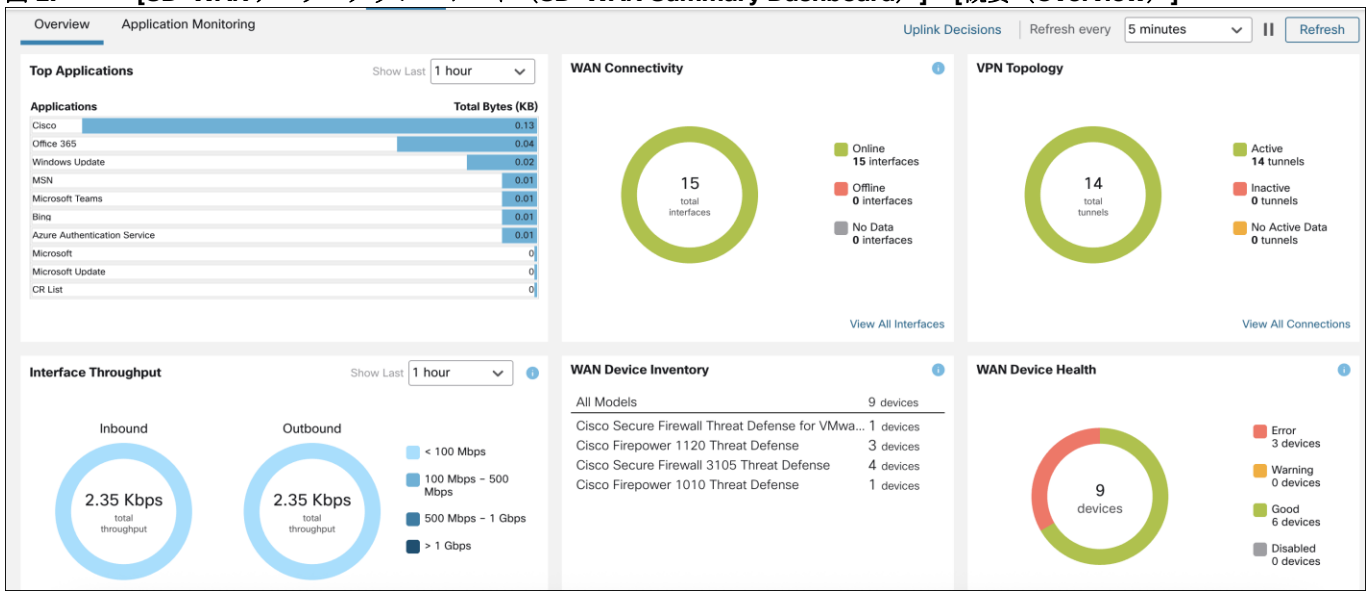
- アンダーレイおよびオーバーレイトポロジの問題を特定する。
- 既存の [ヘルスモニタリング（Health Monitoring）]、[デバイス管理（Device Management）]、および [サイト間モニタリング（Site-to-Site Monitoring）] ページを使用して、VPN の問題をトラブルシューティングする。
- WAN インターフェイスのアプリケーション パフォーマンス メトリックをモニターする。Threat Defense は、これらのメトリックに基づいてアプリケーション トラフィックを誘導します。

[概要（Overview）] セクションには、次のウィジェットがあります。

- **トップアプリケーション**：スループットに応じてランク付けされた上位 10 個のアプリケーションが表示されます。
- **WAN 接続**：WAN インターフェイスのステータスに関する統合情報が表示されます。
- **VPN トポロジ**：サイト間 VPN トンネルのステータスの概要が表示されます。
- **インターフェイス スループット**：WAN インターフェイスのネットワーク全体のスループット使用率に関する情報が表示されます。

- **デバイスインベントリ**：すべての管理対象 WAN デバイスを一覧表示し、モデルに従ってグループ化します。
- **WAN デバイスの正常性**：WAN デバイスの正常性に応じてデバイス数を表示します。

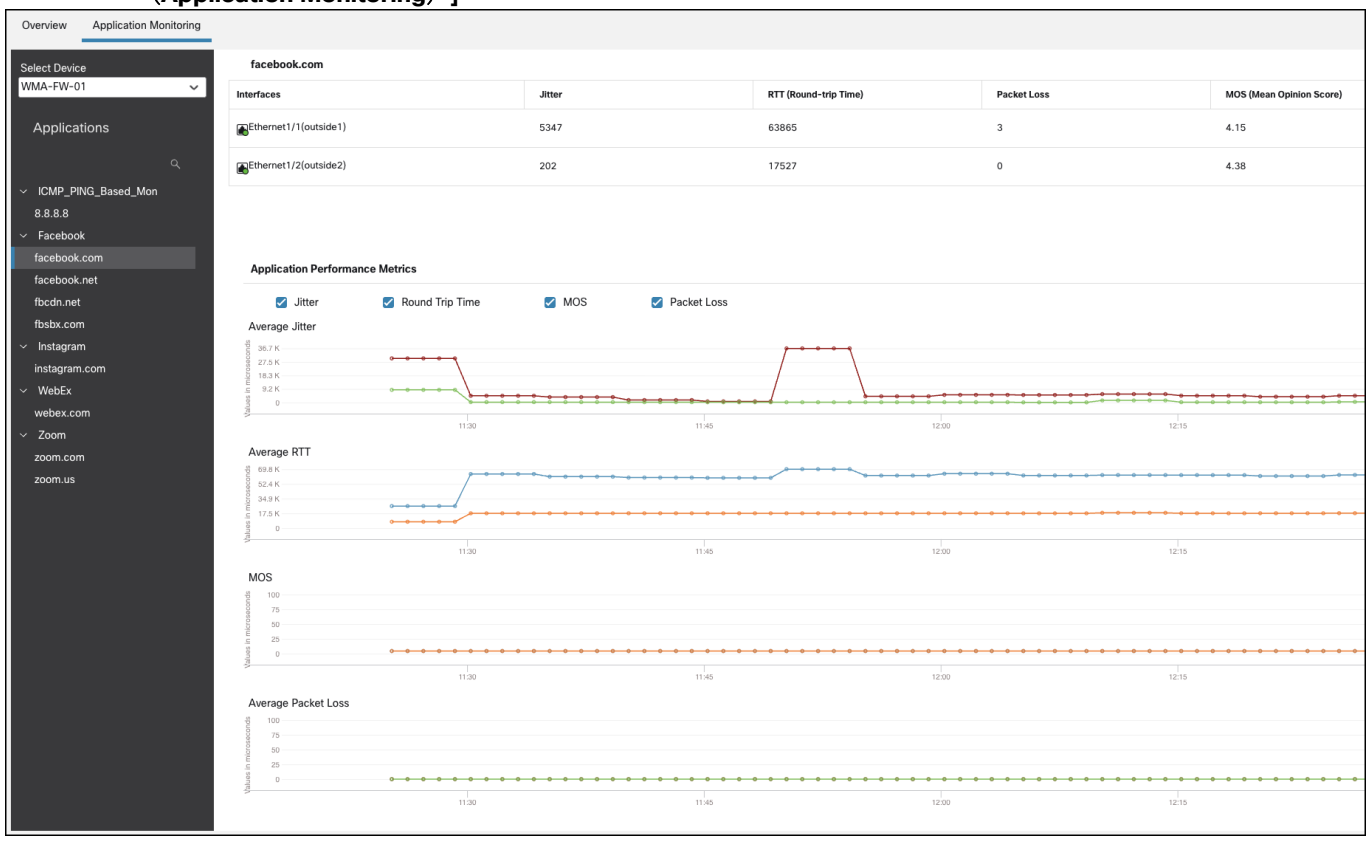
図 2.　　[SD-WANサマリーダッシュボード（SD-WAN Summary Dashboard）] > [概要（Overview）]



ダッシュボードの [アプリケーション モニタリング（Application Monitoring）] セクションでは、WAN デバイスを選択することで、対応する WAN インターフェイスのアプリケーション パフォーマンス メトリックを表示できます。これらのメトリックには、ジッター、ラウンドトリップ時間（RTT）、平均オピニオン評点（MOS）、パケット損失が含まれます。

ダッシュボードの詳細については、https://secure.cisco.com/secure-firewall/docs/sd-wan-summary-dashboard を参照してください。

図 3.　　[SD-WANサマリーダッシュボード（SD-WAN Summary Dashboard）] > [アプリケーション モニタリング（Application Monitoring）]



SD-WAN 設計およびその他のユースケースの詳細については、『Cisco Secure Firewall Threat Defense SD-WAN 設計および展開ガイド』を参照してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。