セキュリティ グループとルールの作成

セキュリティグループルール

このセクションでは、クラウドネットワーク コントローラのホーム リージョンおよび非ホーム リージョンで Cisco Catalyst 8000V を有効にして AWS でプログラムするセキュリティ グループ ルールについて説明します。

（注） 外部ネットワークは、「クラウドコントローラ起動時のクラウド形成テンプレート」から取得され、クラウド ネットワーク コントローラまたは Cisco Catalyst 8000V にアクセスするネットワークです。

クラウドネットワーク コントローラの起動後に AWS で作成されたセキュリティ グループ ルール

1. **セキュリティグループ**：uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   目的：Cisco クラウド ネットワーク コントローラ管理インターフェイスに接続します。

   インバウンドルール

   1. ルール *1*：（クラウド ネットワーク コントローラへの HTTPS アクセス）

      送信元：外部ネットワーク

      接続先: クラウド ネットワーク コントローラ

      プロトコル- TCP

      ポート – 443

   2. ルール *2*：（デフォルトのルールは、セキュリティグループ内のすべてのトラフィックを許可することです）（このルールは、将来、クラスタとして複数のクラウドネットワークコントローラに使用されます。現在、このルールは、セキュリティ グループに接続されているコントローラ NIC が 1 つしかないため、使用されません。）

セキュリティ グループとルールの作成

送信元：uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

接続先：クラウド ネットワーク コントローラ

プロトコル - 全て

ポート - 全て

3. ルール *3*：（クラウド ネットワーク コントローラへの HTTP アクセス）

送信元：外部ネットワーク

接続先: クラウド ネットワーク コントローラ

プロトコル – TCP

ポート – 80

（注） このルールは、クラウドネットワーク コントローラへのHTTPアクセスに対して有効になっています。HTTPアクセスは、クラウドネットワーク コントローラの通信ポリシーを使用して無効にできます。

4. ルール *4*：

送信元：外部ネットワーク

接続先：クラウド ネットワーク コントローラ

プロトコル – ICMP

ポート：全て

5. ルール *5*：（Kafka ルール）

送信元：外部ネットワーク

接続先：クラウド ネットワーク コントローラ

プロトコル – TCP

ポート：9095

6. ルール *6*：（クラウド ネットワーク コントローラへの ssh アクセス）

送信元：外部ネットワーク

接続先：クラウド ネットワーク コントローラ

プロトコル – TCP

ポート – 22

アウトバウンドルール

1. ルール *1*：（クラウド ネットワーク コントローラからのアウトバウンド通信に必要）

送信元：クラウド ネットワーク コントローラ

セキュリティ グループとルールの作成

接続先：0/0

プロトコル - 全て

ポート - 全て

（注） このルールは、クラウドネットワークコントローラがCiscoライセンスサーバー、DNS、NTPなどの外部サービスにアクセスするために必要です。

2. *ルール 2*：（セキュリティ グループ内の全てのトラフィックを許可するデフォルトルール）

送信元：クラウド ネットワーク コントローラ

接続先：uni/tn-infra/cloudapp-cloud-infra / cloudepg-controllers

プロトコル- 全て

ポート：全て

（注） このルールは、上記で説明したセキュリティ グループ内の全ての着信を許可するルールに似ています。現在は使用されていません。

2. セキュリティグループ：capic-rCAPICInfra SecurityGroup

これは、Cisco Catalyst 8000V が展開されるとすぐにインターフェイスから切り離され、インターフェイスは同じルール セットとこのセキュリティ グループを使用して uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers-infra-nic に接続されますはクラウドにそのまま残されます。

目的：このセキュリティ グループは、クラウド ネットワーク コントローラのインフラ インターフェイスに接続されます。これは、複数のクラウド ネットワーク コントローラ インスタンスをサポートする場合にクラスタリングに使用されます。

（注） このインフラ インターフェイスは外部に公開されず、柔軟性 IP は接続されません。全てのトラフィックは、セキュリティ グループと VPC 内でのみ許可されます。このルールは現在使用されていません。

インバウンドルール

1. *ルール 1*：

送信元：0/0

接続先：クラウド ネットワーク コントローラ

プロトコル – 全て

セキュリティ グループとルールの作成

ポート – 全て

アウトバウンドルール

1. ルール *1* :

   送信元：クラウド ネットワーク コントローラ

   接続先：0/0

   プロトコル – 全て

   ポート：全て

Cisco Catalyst 8000V をホームリージョンと非ホームリージョンに展開した後、ホームリージョンセキュリティグループ **cloudepg-controllers** でクラウドネットワークコントローラ用に作成されたルール

（注） **uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers** セキュリティ グループの場合、クラウド ネットワーク コントローラの起動時に展開されたルールに加えて、次のルールが追加されます。これらのルールは、Cisco Catalyst 8000V を自宅および自宅以外の地域に展開した後に追加されます。これらのルールは、クラウド ネットワーク コントローラ が Cisco Catalyst 8000V を管理するために必要です。

1. **セキュリティグループ** : uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   Cisco Catalyst 8000V を有効にした後、追加のインバウンドルールは作成されません。

   アウトバウンドルール

   1. ルール *1* :（このルールは、自宅以外の地域の Cisco Catalyst 8000V ごとに追加されます）。

      送信元：クラウド ネットワーク コントローラ

      接続先：Cisco Catalyst 8000V プライベート IP

      プロトコル- TCP

      ポート 22

   2. ルール *2* :（このルールは、各地域の Cisco Catalyst 8000V ごとに追加されます）。

      送信元：クラウド ネットワーク コントローラ

      宛先: /uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra-csr: < **CAT8KV-NAME** > : interface: 3.

      プロトコル- 全て

      ポート：全て

セキュリティ グループとルールの作成

3. *ルール 1*：（このルールは、自宅以外の地域の Cisco Catalyst 8000V ごとに追加されます）。

   送信元：クラウド ネットワーク コントローラ

   接続先：Cisco Catalyst 8000V プライベート IP

   プロトコル- TCP

   ポート- 830

4. *ルール 4*：（このルールは、非ホーム リージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

   送信元：クラウド ネットワーク コントローラ

   接続先：非ホーム リージョン Cisco Catalyst 8000V プライベート IP

   プロトコル- 全て

   ポート - 全て

5. *ルール 5*：

   送信元：クラウド ネットワーク コントローラ

   接続先：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra -routers

   プロトコル- TCP

   ポート- 830

6. *ルール 6*：

   送信元：クラウド ネットワーク コントローラ

   接続先：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra -routers

   プロトコル- TCP

   ポート- 22

2. **セキュリティ グループ**：capic-uni/tn-infra/cloudapp-cloud -infra/cloudepg-controllers-infra-nic

   目的：このセキュリティ グループは、クラウド ネットワーク コントローラのインフラ インターフェイスに接続されます。

（注） このインターフェイスは外部に公開されず、柔軟性 IP は接続されません。全てのトラフィックは、セキュリティ グループと VPC 内でのみ許可されます。

インバウンドルール

1. *ルール 1*：（クラウド ネットワーク コントローラ：デフォルト ルール）

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers- infra -nic

セキュリティ グループとルールの作成

接続先：クラウド ネットワーク コントローラ

プロトコル – 全て

ポート：全て

アウトバウンドルール

1. *ルール 1*：

送信元：クラウド ネットワーク コントローラ

接続先：/uni/tn-infra/cloudapp-cloud -infra/cloudepg-controllers-infra-nic

プロトコル – 全て

ポート – 全て

Cisco Catalyst 8000V のホームリージョンで作成されたセキュリティグループとルール

1. **セキュリティ グループ**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

インバウンドルール

1. *ルール 1*：

送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

接続先：Cisco Catalyst 8000V

プロトコル – TCP

ポート 22

2. *ルール* 2：（*Netconf*）

送信元：クラウドネットワークコントローラのパブリック IP

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 830

3. *ルール 3*：（これは、非ホーム リージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

送信元：リモート Cisco Catalyst 8000V プライベート IP

接続先：Cisco Catalyst 8000V

プロトコル – 全て

ポート - 全て

4. *ルール 4*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

セキュリティ グループとルールの作成

プロトコル- TCP

ポート- 22

5. *ルール 5*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 80

6. *ルール 6*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 443

7. *ルール 7*：

送信元：クラウドネットワークコントローラのパブリック IP

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 22

8. *ルール 8*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

プロトコル- ICMP

9. *ルール 9*：（このルールは、Cisco Catalyst 8000V 間の通信を有効にするために必要です）。

送信元：/uni/tn -infra/cloudapp-cloud-infra/cloudepg-infra-routers

接続先：Cisco Catalyst 8000V

プロトコル- 全て

ポート - 全て

10. *ルール 10*：

送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

接続先：Cisco Catalyst 8000V

プロトコル- TCP

セキュリティ グループとルールの作成

ポート- 830

アウトバウンドルール

1. *ルール 1*：（このルールは、非ホーム リージョンの Cisco Catalyst 8000V ごとにプライベート IP を持つ 2 つのインターフェイス用に作成されます）。

   送信元: Cisco Catalyst 8000V

   接続先：リモート（非ホームリージョン）Cisco Catalyst 8000V プライベート IP

   プロトコル- 全て

   ポート - 全て

2. *ルール 2*：（このルールは、Cisco Catalyst 8000V（ホーム リージョンと非ホームリージョンの両方）インターフェイス 3-Gig4 ごとに 1 つ作成されます。）

   送信元: Cisco Catalyst 8000V

   接続先：/uni/tn-infra/cloudapp-cloud/-infra/cloudepg-infra-csr：<CAT8KV_NAME> ：interface：3

   プロトコル – 全て

   ポート - 全て

3. *ルール 3*：

   送信元: Cisco Catalyst 8000V

   接続先：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

   プロトコル- 全て

   ポート - 全て

4. *ルール 4*：

   送信元: Cisco Catalyst 8000V

   接続先：0.0.0.0/0

   プロトコル- 全て

   ポート - 全て

5. *ルール 5*：（リモートリージョン Cisco Catalyst 8000V の gig4 インターフェイスのプライベート IP アドレスごとに 1 つのルールが作成されます）

   送信元: Cisco Catalyst 8000V

   接続先：リモートリージョン Cisco Catalyst 8000V Gig4（Interface-3）プライベート IP

2. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra-csr: < **CAT8KV_NAME** _NONHOME>: interface: 2

セキュリティ グループとルールの作成

（注） 非ホーム リージョン Cisco Catalyst 8000V インターフェイス 2 ごとに 1 つのセキュリティ グループが作成されます。このセキュリティグループは現在使用されておらず、将来の目的のために作成されています。

インバウンドルール

1. *ルール 1*：（自宅以外の地域の Cisco Catalyst 8000V ごとに 1 つ）

   送信元：非ホームリージョン Cisco Catalyst 8000V インターフェイス 2 プライベート IP

   プロトコル- 全て

   ポート：全て

2. *ルール 2*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）

   送信元：uni/tn-infra /cloudapp -cloud- infra/cloudepg-infra-csr：**<CAT8KV_NAME>** ：interface：2

   プロトコル- 全て

   ポート - 全て

3. **セキュリティ グループ**- uni/tn-dmmy/cloudapp-dmmy/cloudepg-CAPIC_INTERNAL_EP_SG_DEFAULT

   目的- インフラで作成された未使用のセキュリティ グループ。EPG にセグメント化されるまでエンドポイントを配置するデフォルトのセキュリティグループ。

4. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >: interface: 3

（注） ホーム リージョンの Catalyst 8000V インターフェイス3（Gig4）ごとに 1 つのセキュリティ グループが作成されます。これは、それぞれのローカルリージョン Cisco Catalyst 8000V インターフェイス 3（Gig4）に接続されます。

インバウンドルール

1. *ルール 1*：（このようなルールは 8 個あります）

   送信元：リモート Cisco Catalyst 8000V のプライベート IP（各リモート Cisco Catalyst 8000V のインターフェイスごとに 1 つ）

   プロトコル- 全て

   ポート - 全て

2. *ルール 2*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）（インターフェイスごとに 2 つの Cisco Catalyst 8000V があるため、このようなルールは 4 つになります）。

セキュリティ グループとルールの作成

送信元：uni/tn-infra /cloudapp -cloud- infra/cloudepg-infra-csr：**<HOME and NON HOME REGION CAT8KV_NAME>** ：interface: 1

プロトコル- 全て

ポート - 全て

3. ルール *3*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）（インターフェイスごとに 2 つの Cisco Catalyst 8000V があるため、このようなルールは 4 つになります）。

   送信元：/uni/tn-infra/ cloudapp-cloud-infra/cloudepg-infra-csr<<**HOME and NON HOME REGION CAT8KV_NAME>**>: interface: 2

   プロトコル- 全て

   ポート - 全て

4. ルール *4*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）（インターフェイスごとに 2 つの Cisco Catalyst 8000V があるため、このようなルールは 4 つになります）。

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr<<**HOME and NON HOME REGION CAT8KV_NAME>**: interface: 3

   プロトコル- 全て

   ポート - 全て

5. ルール *5*：

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

   プロトコル- 全て

   ポート - 全て

6. ルール *6*：

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   プロトコル- 全て

   ポート - 全て

アウトバウンドルール

1. ルール *1*：

   接続先：外部ネットワーク

   プロトコル – 全て

   ポート - 全て

2. ルール *2*：

   接続先：インターフェイス 3（Gig4）のリモート Cisco Catalyst 8000V プライベート IP（非ホームリージョンの Cisco Catalyst 8000V ごとに 1 つ）

   プロトコル- 全て

セキュリティ グループとルールの作成

ポート - 全て

3. *ルール 3*：（自宅と自宅以外の両方の地域で Cisco Catalyst 8000V ごとに 1 つ作成）

   送信元：/uni/tn -infra/ cloudapp -cloud -infra/ cloudepg -infra -csr：**<CAT8KV_NAME >** ：interface：3

   プロトコル- 全て

   ポート - 全て

5. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >: interface: 2 (Cisco Catalyst 8000V ごとに 1 つ)

   インバウンドルール

   1. *ルール 1*：（Cisco Catalyst 8000V ごとに 1 つ作成）

      送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >:Interface: 2

      プロトコル- 全て

      ポート - 全て

   2. *ルール 2*：（リモートリージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

      送信元：Cisco Catalyst 8000V のリモート プライベート IP

      プロトコル- 全て

      ポート - 全て

   アウトバウンドルール

   1. *ルール 1*：

      接続先：インターフェイス 2（Gig3）およびインターフェイス 3（Gig4）のプライベート IP のリモート Cisco Catalyst 8000V

      プロトコル – 全て

      ポート - 全て

   2. *ルール 2*：（このルールは、ホームリージョンと非ホームリージョンの両方の Cisco Catalyst 8000V に追加されます）。

      接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface：2

      プロトコル- 全て

      ポート - 全て

   3. ルール 3：（このルールは、ホームリージョンと非ホームリージョンの両方の Cisco Catalyst 8000V に追加されます）。

セキュリティ グループとルールの作成

接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface：3

プロトコル- 全て

ポート - 全て

4. *ルール 4*：

接続先：0/0

プロトコル- 全て

ポート - 全て

6. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >: interface: 1 (Cisco Catalyst 8000V ごとに 1 つ)

インバウンドルール

1. ルール 1：（自宅および自宅以外の地域の Cisco Catalyst 8000V を含む Cisco Catalyst 8000V インターフェイス 1 ごとに 1 つのルールが作成されます）。

送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >:Interface: 1

プロトコル- 全て

ポート - 全て

2. *ルール 2*：（リモート リージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

送信元：リモート リージョン Cisco Catalyst 8000V インターフェイス 1（Gig2）のリモート プライベート IP

プロトコル- 全て

ポート - 全て

アウトバウンドルール

1. *ルール 1*：

接続先：インターフェイス 3（Gig4）およびインターフェイス 1（Gig2）のリモート リージョン Cisco Catalyst 8000V プライベート IP

プロトコル – 全て

ポート - 全て

2. *ルール 2*：

接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface: 1

プロトコル- 全て

ポート - 全て

セキュリティ グループとルールの作成

3. *ルール 3*：

   接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface：3

   プロトコル- 全て

   ポート - 全て

4. *ルール 4*：

   接続先：0/0

   プロトコル- 全て

   ポート - 全て

Cisco Catalyst 8000V の非ホーム リージョンでは、セキュリティ グループとルールは、ホーム リージョンの上記のセクションで説明したものと同様ですが、次の例外があります。セキュリティ グループを接続先として使用する代わりに、一部のルールにはクラウド ネットワーク コントローラの特定の IP アドレス。

セキュリティ グループとルールの作成

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。