



オンボーディングとファイアウォールイネーブルメント

この章では、Cisco N9300 シリーズ スマート スイッチでレイヤ 4 ～ レイヤ 7 サービス アクセラレーションをセットアップ方法について説明します。

トラブルシューティング情報については、「[Cisco N9300 Series Smart Switches Troubleshooting](#)」を参照してください。

- [レイヤ 4 ～ レイヤ 7 サービス アクセラレーションのセットアップ](#) (1 ページ)
- [DPU へ通信をリダイレクトします](#) (11 ページ)

レイヤ 4 ～ レイヤ 7 サービス アクセラレーションのセットアップ

ライセンス要件

サービス アクセラレーション機能を使用するには、Premier ライセンス階層である必要があります。レイヤ 4 のステートフル セグメンテーション機能およびセキュリティ ユースケースには、別途 Cisco Hypershield ライセンスが必要です。

レイヤ 4 - レイヤ 7 サービス アクセラレーションのワークフロー

DPU で提供されるレイヤ 4 - レイヤ 7 サービス アクセラレーション機能を有効にするには、次の手順を実行します。

1. スイッチにソフトウェアをインストールして、スイッチを起動します。
2. VRF メンバーと VRF コンテキストおよびレイヤ 3 インターフェイスを構成します。
3. Hypershield 送信元インターフェイスのループバック インターフェイスを構成します。
4. サービス アクセラレーション機能を有効にする
5. Hypershield Security Cloud Control からトークンを要求します。

6. Hypershield に接続するための構成を追加します。
7. 必要な VRF のトラフィックのトラフィック インспекションを構成します。
8. ファイアウォール サービス機能を有効にします。

注意事項と制約事項

VRF の使用と IP アドレスの構成に関する推奨事項

推奨事項は、VRF の使用と予約済みの IP アドレス範囲に関するガイダンスを提供します。

- VRF-lite を活用トラフィックを分離し、リダイレクションのために各 VRF のトラフィックを特定の DPU に割り当てます。
- DPU によるフィルタリングが必要なトラフィックには、（デフォルトの VRF に加えて）1 つまたは複数の VRF を割り当てます。
- IP アドレス範囲 169.254.xx は使用しないでください。スイッチ内の DPU との通信に使用されます。
- 通常の IP アドレス要件（mgmt0 IP など）に加えて、Cisco N9300 シリーズ スマート スイッチで実行されている Hypershield Agent のループバック IP アドレスを割り当てる必要があります。

ファイアウォール サービス構成に関する制約事項と考慮事項

これらの制限と考慮事項は、ファイアウォール サービスを運用するための制限事項とベストプラクティスに対処し、トラフィック インспекションの動作、プロトコルの相互作用、およびサービス アクセラレーション VRF 機能に対応します。

- Hypershield 管理トラフィックは、デフォルトの VRF を使用します。サービス ファイアウォールでトラフィック インспекションのデフォルト VRF および管理 VRF を構成することはできません。
- Hypershield への接続には前面パネル インターフェイスを使用する必要がありますが、mgmt0 インターフェイスを使用することはできません。
- ループバック インターフェイスがサービス インスタンスの送信元インターフェイスとして使用されると、ループバック IP アドレスは、エージェントと Hypershield 間の通信以外の目的には使用できません。

このループバック IP アドレスは、スイッチで実行されている制御プロトコルに再利用することはできません。ループバック IP アドレスが送信元として指定されている場合、NXOS CLI から ICMP エコーを使用して他の接続先への到達可能性をテストしようとすると失敗します。

代わりにトラブルシューティング コマンドを活用、Hypershield Agent と Hypershield Controller 間の接続を確認します。詳細については、「[Cisco N9300 シリーズ スマート スイッチのトラブルシューティング](#)」を参照してください。

- サービス ファイアウォールの構成で VRF が構成されている場合（つまり、VRF が通信フィルタリングの対象）で、サービスファイアウォールが「インサービス」でない場合、この VRF によってルーティングされる IPv4 および IPv6 トラフィックは、サービス ファイアウォールが「サービス中」です（当該トラフィックを許可するセキュリティルールが設定されるまで）。



(注) Cisco N9300 スマート スイッチのスーパーバイザ宛での、サービス アクセラレーション用に構成された VRF の制御プロトコル トラフィックは検査 されません。そのため、サービス ファイアウォールが「インサービス」であるかどうか、およびセキュリティルールが構成されているかどうかに関係なく、ドロップされません。

- ファイアウォール サービスは、マルチキャスト トラフィック、ローカル スイッチ宛でのトラフィック、スーパーバイザから発信されるトラフィック、BFD エコー パケット、デフォルトおよび管理 VRF、ならびにサービス ファイアウォールに追加されていない VRF を検査し ません。
- サービス ファイアウォールが「インサービス」状態ではなく、DPU でトラフィックを検査する準備が できていない 場合、レイヤ 3 ルーティングプロトコルはグレースフル挿入と削除 (GIR) の動作を保証します。

これを実現するために、サービス アクセラレーション VRF は、ルート アドバタイズメントの動作を変更して、ネットワークからスイッチを分離します。この機能をサポートするプロトコルは、Border Gateway Protocol (BGP) および Open Shortest Path First (OSPF) を含みます。

サービスファイアウォールが使用可能になり、「サービス中」状態になると、プロトコルは通常のルート アドバタイズメント動作を再開します。

これらの機能は、Cisco Nexus NX- OSリリース 10.5 (3s) F では使用でき ません。

- VRF 間フローはサポートされていません : フィルタリングされるトラフィックは、同じ VRF からスマート スイッチに出入りする必要があります。
- Cisco Nexus NX- OS リリース 10.5 (3s) F は、レイヤ 3 物理インターフェイスとポート チャネル、および物理とポート チャネル サブインターフェイスのみをサポートします。レイヤ 3 物理インターフェイスでは、着信トラフィックのみがサポートされます。
- 冗長性、ステートフル フェールオーバーなどの高可用性機能はサポートされていません。トラフィック分散に ECMP を使用する場合、トラフィックがスイッチに対して対称的に送信されていることを確認する必要があります。
- アクセスまたはトランクポート、ネットワーク間の VLAN 拡張、MAC アドレス テーブル管理などのレイヤ 2 機能はサポート されません。
- ルートマップで構成されたインポートまたはエクスポートポリシーを使用した異なる VRF 間でのルート交換を可能にする VRF 共有機能はサポートされて いません。

- 2つのデバイス間のリンクを単一のポート チャンネルとして扱うことができる仮想ポート チャンネル (vPC) は、サポートされません。
 - スイッチ仮想インターフェイス (SVI) はサポートされません。トラフィックのルーティングにレイヤ 3 インターフェイスを使用できます。
 - シームレスなフェールオーバーを提供する Hot Standby Router Protocol (HSRP) プロトコルと Virtual Router Redundancy Protocol (VRRP) プロトコルはサポートされません。
 - VXLAN および EVPN 機能 はサポートされていません。
 - **feature service-acceleration** コマンドは、ハードウェア集約型の機能です。有効にすると、NXOSはDPUの電源を投入しますが、これには時間がかかります。その結果、NXOSは、DPUの電源が完全にオンになって端末状態に達するまで、**no feature service-acceleration** コマンドの実行を防止します。次のステートメントが当てはまります：
 - **feature service-acceleration** コマンドは、システム内のすべての DPU の電源がオンになるまで無効にできません。
 - **feature service-acceleration** コマンドは、いったん無効にした場合、スイッチのリブート後にのみ再度有効にできます。
- configure replace** 機能を使用する場合（「[構成の置換の実行](#)」を参照）、**configure replace** の成功は、サービスアクセラレーションが有効または無効に設定された構成のタイミングに依存することがあります。
- Hypershield Agent から Hypershield システムへの管理トラフィックは、IPv6 経由ではサポートされていません。

VRF をインターフェイスへの構成と割り当て

インターフェイスで VRF を構成するには、次の作業を行います。

手順

ステップ 1 **vrf context vrf-name** コマンドを使用して新しい VRF を作成します。

例：

```
switch# configure terminal
switch(config)#vrf context red
switch(config)#vrf context blue
switch(config)#vrf context green
switch(config-vrf)# exit
```

ステップ 2 **interface interface-typeslot/port** コマンドを使用して、レイヤ 3 インターフェイスを構成します。

例：

```
switch# configure terminal
switch(config)# interface ethernet 1/1
```

ステップ 3 `vrf member vrf-name` コマンドを使用して、VRF をインターフェイスに割り当てます。

例：

```
switch(config-if)# vrf member red
```

これにより、インターフェイスに構成されている既存の IPv4/IPv6 アドレスが削除されます。

ステップ 4 `ip address ip-address/length` コマンドを使用してインターフェイスの IP アドレスを構成します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。

例：

```
switch(config-if)# ip address 192.0.2.1/16
```

例

VRF コンテキストとレイヤ 3 インターフェイス構成を確認します。

```
switch# show run
..
vrf context red
vrf context green
vrf context blue
!
!
switch# show run interface 1/1
interface Ethernet1/1
    vrf member red
    ip address 192.0.2.1/16
    no shutdown
<...etc...>
...!
```

ループバック インターフェイスを作成します。

ループバック インターフェイスを作成し、このループバックループバック インターフェイスをサービス システムの Hypershield 構成の Hypershield エージェントに関連付けるには、次の作業を実行します。

手順

ステップ 1 `interface loopback instance` コマンドを使用して、Hyper Shield 送信元インターフェイスのループバック インターフェイスを作成します。

例：

```
switch(config)# interface loopback 100
switch(config-if)#
```

ステップ 2 `ip address ip-address/length` コマンドを使用してインターフェイスの IP アドレスを構成します。

例：

```
switch(config-if)# ip address 192.0.2.1/32
```

IP アドレスの詳細については、『[Cisco Nexus 9000 Series NX-OS ユニキャスト回送構成ガイド](#)』を参照してください。

ip-address/length : ループバックの IP アドレスを設定します

(注)

Hyperレート エージェントの IP アドレスの長さとして /32 を構成する必要があります。

(注)

Hyperレート エージェントから ハイパー シールド システム への管理トラフィックは、IPv6 経由ではサポートされていません。

例

ループバック インターフェイスの構成の確認。

```
switch# show run
!
interface loopback100
  ip address 192.0.2.1/32
```

サービス販売促進を有効化

スイッチの DPU への電源投入を有効にするには、次の作業を実行します。

手順

feature service-acceleration コマンドを有効にして、DPU の電源を投入します。

例 :

```
Switch(config)# feature service-acceleration
```

feature service-acceleration コマンドが構成されていない場合、DPU の電源はオフになります。スイッチは NXOS スイッチとして機能します。

(注)

機能サービス アクセラレーションを有効にすると、DPU に電力が供給されます。ただし、構成を決定するには、DPU にリダイレクトする VRF トラフィックを定義する必要があります。「[ファイアウォール サービスへの通信リダイレクションの VRF を構成します。](#) (10 ページ)」を参照してください。

サービス販売促進の確認

このタスクを実行して、サービス アクセラレーションの有効化を確認します。

手順

ステップ 1 `show run service-acceleration | grep feature` コマンドを使用して、サービス アクセラレーション ステータスを確認します。

例：

```
switch# show run service-acceleration | grep feature

feature service-acceleration
```

ステップ 2 インターフェイスのステータスを表示するには、`show interfaces brief` コマンドを活用。

例：

```
Switch# show interface brief
..!
-----
Service          VLAN    Type Mode   Status Reason          Speed    Port
Ethernet
-----
SEth1/1          --      eth  routed up    none          200G (D) --
SEth1/2          --      eth  routed up    none          200G (D) --
SEth1/3          --      eth  routed up    none          200G (D) --
SEth1/4          --      eth  routed up    none          200G (D) --
```

機能のサービス アクセラレーションを有効にすると、すべての DPU の電源がオンになります。

例

`show module` コマンドを使用して、DPU の電源がオンでオンラインであることを確認できます。

```
switch# show module
Mod Ports      Module-Type      Model      Status
-----
1    24    24x40/100G QSFP28 Ethernet Module  N9324C-SE1U  ok
27    0    Virtual Supervisor Module  N9324C-SE1U  active
*
```

<...snip...>

```
* this terminal session
Mod DPU    Module-Type      Model      Status
-----
1    1    DPU              N9324C-SE1U-DPU  ok
1    2    DPU              N9324C-SE1U-DPU  ok
1    3    DPU              N9324C-SE1U-DPU  ok
1    4    DPU              N9324C-SE1U-DPU  ok

Mod DPU    Sw      Hw      Serial-Num  Online Diag Status
-----
1    1    1.5.3.s  1.0      FDO285215F3  Pass
1    2    1.5.3.s  1.0      FDO285215F4  Pass
1    3    1.5.3.s  1.0      FDO285215F5  Pass
1    4    1.5.3.s  1.0      FDO285215F6  Pass
```

サービス アクセラレーション機能を無効にする

手順

no feature service-acceleration コマンドを使用して、スイッチのサービス アクセラレーション機能とレイヤ 4 ～ 7 サービスを無効にして、DPU 電源オフ状態で機能させます。

例：

```
Switch(config)# no feature service-acceleration
```

(注)

(無効にした後に) この機能を再度有効にする場合は、Cisco N9300 スマート スイッチをリロードする必要があります。

Cisco N9300 スマート スイッチを Hypershield に登録する

Hypershield からワンタイム パスワード (OTP) トークンを取得する必要があります。トークンには、Hypershield に到達する方法に関する情報が含まれています。

スイッチと Hypershield 間の通信を確立するには、このトークンをスイッチに入力する必要があります。

手順

service system hypershield register otp コマンドを使用して、取得したトークンでスイッチと Hypershield 間の通信を確立します。

例：

```
Switch# service system hypershield register 34C58A...
```

EXEC レベルでこのコマンドを実行します。

otp：トークン文字列を示します（最大サイズは 4094）。トークンを引用符なしで入力します。

Hypershield の接続状態を確認する

手順

show service-acceleration status details コマンドを使用して、接続のステータスを確認します。

例：

```
switch# show service-acceleration status details

Service System: hypershield
Source Interface: loopback100 (192.0.2.1/32)
Agent Status: firewall-ready, redirect-installed
Agent Health Status: failed (Error: dial unix /run/agw.sock: connect: connection refused)
Controller Connection Status: success

[...]
```

ハイパーシールド接続の構成

に接続し、Cisco N9300 スマート スイッチの Hypershield エージェントと Hypershield システム間の接続を確立するには、次のタスクを実行します。

手順

ステップ 1 `service system hypershield` コマンドを有効にして、Hypershield インスタンスを設定します。

例：

```
Switch(config)# service system hypershield
```

ステップ 2 `source-interface` コマンドを構成して、IP アドレスを持つループバック インターフェイスを Hypershield エージェントに割り当てます。

例：

```
Switch(config-svc-sys)# source-interface loopback 100
```

ループバック IP アドレスは、デフォルトの VRF で構成する必要があります。[ループバック インターフェイスを作成します。](#) (5 ページ) を参照してください。

(注)

システムが自動的に構成をブロックするため、デフォルトの VRF をサービス アクセラレーション VRF として構成することはできません。

例

例は、サービス アクセラレーション機能の構成を示しています。

```
switch# show run service-acceleration
!
feature service-acceleration
service system hypershield register 34C58A...
!
service system hypershield
```

ファイアウォール サービスへの通信リダイレクションの VRF を構成します。

```
source-interface loopback 100
...!
```

ファイアウォールサービスへの通信リダイレクションのVRFを構成します。

通信をファイアウォールする必要がある VRF を指定するには、次の作業を実行します。

手順

ステップ 1 `service firewall` コマンドを有効にします。

例：

```
Switch(config-svc-sys)# service firewall
```

ステップ 2 `vrf vrf-name` コマンドを使用して、ファイアウォール サービスによって検査されるように VRF 内の通信をリダイレクトするように、サービス ファイアウォールの下に VRF を構成します。

例：

```
Switch(config-svc-sys-fw)# vrf red module-affinity dynamic
```

`module-affinity dynamic` が使用されている場合、スイッチは、どの DPU が VRF の通信を検査する必要があるかを決定します。VRF コンテキストおよびその他の必要なネットワーク構成が、通常どおりスイッチに入力されます。

ステップ 3 (オプション) `module-affinity` コマンドを使用して、VRF 内の通信をその DPU 内のファイアウォール サービスで検査する必要があることを示すため、特定の DPU 番号を構成します。

例：

```
Switch(config-svc-sys-fw)# blue module-affinity 1
```

VRF ブルーの通信は DPU1 によって検査されます。

これは、DPU への通信リダイレクト用の VRF の構成例です。

```
Switch(config-svc-sys)# service firewall
Switch(config-svc-sys-fw)# vrf red module-affinity dynamic
Switch(config-svc-sys-fw)# vrf blue module-affinity 1
```

例

この例は、ファイアウォールを有効にしたサービスアクセラレーションを示しています。

```
switch# show run service-acceleration
!
```

```
feature service-acceleration
service system hypershield register 34C58A...
!
service system hypershield

source-interface loopback 100
service firewall
  vrf blue module-affinity 1
  vrf red module-affinity dynamic
```

サービス ファイアウォールのインサービスであるトラフィック検査を有効にする

in-service コマンドは、サービス ファイアウォール機能を有効にし、DPU によるトラフィック検査を許可します。

no service firewall no in-service コマンドを使用して、ファイアウォール機能のメンテナンスモードをトリガー、サービス ファイアウォール DPU と VRF ピニングを変更することもできます。

手順

in-service コマンドを有効にして、サービス ファイアウォールが特定のトラフィックをリダイレクトできるようにします。

例：

```
Switch(config-svc-sys-fw)# in-service
```

DPU へ通信をリダイレクトします

手順

VRF のステータスを表示するには、**show service-acceleration status details** コマンドを使用します。

例：

この例は、ファイアウォールサービスが「アウトオブサービス」状態になっていることを示しています。

```
switch# show service-acceleration status details
Service System: hypershield
Source Interface: Lo100 (192.0.2.1/9)
Agent Status: firewall-disable
Controller Connection Status: init
Services:
Firewall: out-of-service
  VRF          Operational State      Affinity
=====
```

blue	isolated	n/a
red	isolated	n/a

サービス ファイアウォールのインサービス機能を確認する

手順

ステップ 1 `show service-acceleration status details` コマンドを活用、モジュールアフィニティを使用した VRF のステータスを表示します。

例：

この例は、「サービス内」状態のファイアウォールサービスと、ファイアウォールに対応する VRF を示しています。

```
switch# show service-acceleration status details
Service System: hypershield
Source Interface: Lo100 (192.0.2.1/8)
Agent Status: firewall-ready,redirect-installed
Controller Connection Status: success
Services:
  Firewall: in-service
```

VRF	Operational State	Affinity
blue	forwarding ready	1
red	forwarding ready	3

ステップ 2 コマンド `show service-acceleration redirect-policy brief` を活用、トラフィックを VRF から DPU にリダイレクトするためのサービスイーサネット サブインターフェイスを識別します。

例：

```
switch# show system internal service-acceleration redirect-policy brief
```

VRF	AF Type	Interface[Status]	Affinity	Redirect Status
blue	IPv4	SEth1/3.11[UP]	1	Enabled
red	IPv4	SEth1/1.10[UP]	3	Enabled
blue	IPv6	SEth1/3.11[UP]	1	Enabled
red	IPv6	SEth1/1.10[UP]	3	Enabled

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。