



ファーストホップセキュリティ

この章は、次の項で構成されています。

- [ファーストホップセキュリティについて \(1 ページ\)](#)
- [ACI FHS の導入 \(2 ページ\)](#)
- [注意事項と制約事項 \(2 ページ\)](#)
- [APIC GUI を使用して FHS の設定 \(3 ページ\)](#)
- [NX-OS CLI を使用した FHS の設定 \(4 ページ\)](#)
- [FHS スイッチ iBASH コマンド \(10 ページ\)](#)
- [REST API を使用して apic 内で FHS の設定 \(15 ページ\)](#)

ファーストホップセキュリティについて

ファーストホップセキュリティ (FHS) 機能では、レイヤ2リンク上でより優れた IPv4 と IPv6 のリンクセキュリティおよび管理が可能になります。サービスプロバイダ環境で、これらの機能は重複アドレス検出 (DAD) とアドレス解像度 (AR) などのアドレス割り当てや派生操作が、より緊密に制御可能です。

次のサポートされている FHS 機能はプロトコルをセキュアにして、ファブリックリーフスイッチにセキュアなエンドポイントデータベースを構築するのに役立ち、MIM 攻撃や IP の盗難などのセキュリティ盗難を軽減するために使用されます。

- **ARP 検査**：ネットワーク管理者は、無効な MAC アドレスから IP アドレスへのバインディングがある ARP パケットを代行受信、記録、およびドロップすることができます。
- **ND 検査**：レイヤ2 ネイバーテーブルでステートレス自動設定アドレスのバインディングを学習し、保護します。
- **DHCP 検査**：信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- **RA ガード**：ネットワーク管理者は、不要または不正なルータアドバタイズメント (RA) ガードメッセージをブロックまたは拒否できます。
- **IPv4 および IPv6 ソースガード**—不明なソースからのデータトラフィックをすべてブロックします。

- **信頼制御**：信頼できる送信元はその企業の管理制御下にあるデバイスです。これらのデバイスには、ファブリック内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、ホストポートは信頼できない送信元として扱われます。

FHS 機能は、次のセキュリティ対策を提供します。

- **ロールの適用**：信頼できない主催者が、そのロールの有効範囲を超えるメッセージを送信することを防ぎます。
- **バインディングの適用**：アドレスの盗難を防止します。
- **DoS 攻撃の軽減対策**：悪意あるエンドポイントを防ぎ、データベースが操作サービスを提供することを停止するポイントにエンドポイントデータベースを成長させます。
- **プロキシ サービス**：アドレス解決の効率を高めるため一部のプロキシ サービスを提供します。

FHS 機能は、テナントブリッジドメイン (BD) ごとに有効になっています。ブリッジドメインとして、単一または複数のリーフスイッチで展開可能で、FHS 脅威の制御と軽減のメカニズムは単一のスイッチと複数のスイッチのシナリオにも対応できます。

ACI FHS の導入

ほとんどの FHS 機能はツーステップ傾向で設定されています。最初に機能の動作を説明するポリシーを定義し、次にこのポリシーを「ドメイン」に適用します (テナントブリッジドメインまたはテナントエンドポイントグループになる)。異なる動作を定義する別のポリシーは、さまざまな交差ドメインに適用できます。特定のポリシーを使用する決定は、ポリシーを適用するもっとも明確なドメインで行われます。

ポリシーのオプションは、[Tenant_name]>[Networking]>[Protocol Policies]>[First Hop Security] タブの下にある Cisco APIC GUI から定義できます。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- リリース 3.1 (1) より、仮想エンドポイント (AV のみ) で FHS はサポートされています。
- FHS は、VLAN と VXLAN の両方のカプセル化でサポートされています。
- **[ダウン]** 状態の FHS バインディング表データベースでセキュリティ保護されたエンドポイント エントリは、タイムアウトから **18 時間** 後に消去されます。エントリが学習する前面パネルポートがリンク ダウンする場合、エントリは **[ダウン]** 状態に移動します。この **18 時間** ウィンドウの中で、エンドポイントが別のロケーションに移動し別のポートで確認される場合、エンドポイントが他のポートから到達可能な限り移行され、エントリはグレースフルに **[ダウン]** 状態から **[REACHABLE/STALE]** に移行します。

- IP 発信元ガードが有効な時、IP 送信元アドレスとして Ipv6 リンク ローカルアドレスを使用して供給される Ipv6 トラフィックは、IP 送信元ガード施行を受けません（例：送信元 MAC の施行 <=> IP 調査機能によりセキュリティ保護された送信元 IP バインディング）。バインディング チェック障害に関係なく、デフォルトでこのトラフィックが許可されません。
- L3Out インターフェイスでは、FHS はサポートされていません。
- TOR に基づいて N9K-M12PQ では FHS はサポートされていません。
- ACI マルチサイトの FHS はサイトのローカル機能であるため、APIC クラスタからサイトでのみ有効にできます。また、ACI マルチサイトの FHS は、BD や EPG がサイトローカルであり、サイト上でストレッチしない場合にのみ動作します。ストレッチ BD または EPG の FHS セキュリティを有効にすることはできません。
- レイヤ 2 専用ブリッジ ドメインでは、FHS はサポートされていません。
- FHS の有効化機能ではトラフィックが 50 秒間中断することがあります。これは、BD 内の EP がフラッシュされ、BD 内の EP ラーニングが 50 秒間無効になるためです。

APIC GUI を使用して FHS の設定

始める前に

- テナントとブリッジ ドメインが設定されています。

ステップ 1 メニューバーで、[テナント]>[Tenant_name]をクリックします。[ナビゲーション]ペインで、[ポリシー]>[プロトコル]>[最初のホップセキュリティ]をクリックします。[最初のホップセキュリティ]を右クリックして[機能ポリシーの作成]を開き、次の操作の実行します。

- a) [名前] フィールドにホップセキュリティ セキュリティ ポリシーの名前を入力します。
- b) [IP 検査]、[送信元ガード]、[ルータ アドバタイズメント] フィールドが有効になっていることを確認し、[提出]をクリックします。

ステップ 2 [ナビゲーション] ペインで、[最初のホップセキュリティ]を展開し、[制御ポリシーの信頼]を右クリックして[信頼制御ポリシーの作成]を開いて次のアクションを実行します。

- a) [名前] フィールドに信頼制御ポリシーの名前を入力します。
- b) ポリシーで許可する機能を選択し、[提出]をクリックします。

ステップ 3 (オプション) EPG に信頼制御ポリシーを適用するには、[Navigation] ペインで、[Application Profiles]>[ApplicationProfile_name]>[Application EPGs]を展開し、[Application EPG_name]をクリックして、次の操作を行います。

- a) [作業] ペインで、[全般] タブをクリックします。
- b) [FHS 信頼制御ポリシー] の下矢印をクリックして、以前作成したポリシーを選択し、[提出]をクリックします。

- ステップ 4 [ナビゲーション] ペインで、[ブリッジ ドメイン]>[ブリッジ ドメイン名] を展開して、[アドバンスド/トラブルシューティング] タブをクリックして、次のアクションを実行します。
- [ホップの最初のセキュリティ ポリシー] フィールドで、作成したポリシーを選択し、[提出] をクリックします。これで FHS 設定を完了します。

NX-OS CLI を使用した FHS の設定

始める前に

- テナントとブリッジ ドメインが設定されています。

ステップ 1 configure

コンフィギュレーション モードに入ります。

例 :

```
apic1# configure
```

ステップ 2 FHS ポリシーを設定します。

例 :

```
apic1(config)# tenant coke
apic1(config-tenant)# first-hop-security
apic1(config-tenant-fhs)# security-policy poll
apic1(config-tenant-fhs-secpol)#
apic1(config-tenant-fhs-secpol)# ip-inspection-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# source-guard-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# router-advertisement-guard-admin-status enabled
apic1(config-tenant-fhs-secpol)# router-advertisement-guard
apic1(config-tenant-fhs-raguard)#
apic1(config-tenant-fhs-raguard)# managed-config-check
apic1(config-tenant-fhs-raguard)# managed-config-flag
apic1(config-tenant-fhs-raguard)# other-config-check
apic1(config-tenant-fhs-raguard)# other-config-flag
apic1(config-tenant-fhs-raguard)# maximum-router-preference low
apic1(config-tenant-fhs-raguard)# minimum-hop-limit 10
apic1(config-tenant-fhs-raguard)# maximum-hop-limit 100
apic1(config-tenant-fhs-raguard)# exit
apic1(config-tenant-fhs-secpol)# exit
apic1(config-tenant-fhs)# trust-control tcpoll
apic1(config-tenant-fhs-trustctrl)# arp
apic1(config-tenant-fhs-trustctrl)# dhcpv4-server
apic1(config-tenant-fhs-trustctrl)# dhcpv6-server
apic1(config-tenant-fhs-trustctrl)# ipv6-router
apic1(config-tenant-fhs-trustctrl)# router-advertisement
apic1(config-tenant-fhs-trustctrl)# neighbor-discovery
apic1(config-tenant-fhs-trustctrl)# exit
apic1(config-tenant-fhs)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# first-hop-security security-policy poll
apic1(config-tenant-bd)# exit
```

```
apicl(config-tenant)# application ap1
apicl(config-tenant-app)# epg epg1
apicl(config-tenant-app-epg)# first-hop-security trust-control tcpoll
```

ステップ3 FHS の設定例を示します。

例：

```
leaf4# show fhs bt all
```

Legend:

```
TR      : trusted-access          UNRES : unresolved          Age    : Age
since creation
UNTR    : untrusted-access       UNDTR  : undetermined-trust  CRTNG  : creating
UNKNW   : unknown               TENTV  : tentative          INV    : invalid
NDP     : Neighbor Discovery Protocol STA    : static-authenticated  REACH  : reachable
INCOMP  : incomplete           VERIFY : verify             INTF   : Interface
TimeLeft : Remaining time since last refresh LM     : lla-mac-match       DHCP   :
```

EPG-Mode:

```
U : unknown   M : mac     V : vlan     I : ip
BD-VNID      BD-Vlan      BD-Name
15630220     3             t0:bd200
```

Origin	IP	MAC	INTF	EPG(sclass) (mode)	Trust-lvl	State
Age	TimeLeft					
ARP	192.0.200.12	D0:72:DC:A0:3D:4F	eth1/1	epg300(49154) (V)	LM,TR	STALE
00:04:49	18:08:13					
ARP	172.29.205.232	D0:72:DC:A0:3D:4F	eth1/1	epg300(49154) (V)	LM,TR	STALE
00:03:55	18:08:21					
ARP	192.0.200.21	D0:72:DC:A0:3D:4F	eth1/1	epg300(49154) (V)	LM,TR	REACH
00:03:36	00:00:02					
LOCAL	192.0.200.1	00:22:BD:F8:19:FF	vlan3	LOCAL(16387) (I)	STA	REACH
04:49:41	N/A					
LOCAL	fe80::200	00:22:BD:F8:19:FF	vlan3	LOCAL(16387) (I)	STA	REACH
04:49:40	N/A					
LOCAL	2001:0:0:200::1	00:22:BD:F8:19:FF	vlan3	LOCAL(16387) (I)	STA	REACH
04:49:39	N/A					

信頼レベルは次のとおりです。

- **TR** : 信頼されています。エンドポイントが、信頼設定が有効になっている EPG から学習されたときに表示されます。
- **UNTR** : 信頼できません。エンドポイントが、信頼設定が有効になっていない EPG から学習されたときに表示されます。
- **UNDTR** : 未定。DHCP サーバーブリッジドメイン (BD) がリモートリーフにあり、DHCP クライアントがローカルリーフにある DHCP リレートポロジの場合に表示されます。この状況では、ローカルリーフは、DHCP サーバー BD が信頼 DHCP を有効にしているかどうかを認識しません。

ステップ4 さまざまなタイプと理由の例とともに違反を表示します。

例 :

```
leaf4# show fhs violations all
```

Violation-Type:

```
POL : policy      THR : address-theft-remote
ROLE : role       TH  : address-theft
INT  : internal
```

Violation-Reason:

```
IP-MAC-TH  : ip-mac-theft          OCFG_CHK  : ra-other-cfg-check-fail    ANC-COL
: anchor-collision
PRF-LVL-CHK : ra-rtr-pref-level-check-fail INT-ERR   : internal-error                    TRUST-CHK
: trust-check-fail
SRV-ROL-CHK : srv-role-check-fail    ST-EP-COL : static-ep-collision              LCL-EP-COL
: local-ep-collision
MAC-TH      : mac-theft              EP-LIM    : ep-limit-reached                 MCFG-CHK
: ra-managed-cfg-check-fail
HOP-LMT-CHK : ra-hoplimit-check-fail MOV-COL   : competing-move-collision         RTR-ROL-CHK
: rtr-role-check-fail
IP-TH       : ip-theft
```

EPG-Mode:

```
U : unknown    M : mac    V : vlan    I : ip
```

```
BD-VNID      BD-Vlan      BD-Name
15630220     3             t0:bd200
```

```
-----
| Type | Last-Reason | Proto | IP           | MAC           | Port   | EPG(sclass) (mode) |
Count |
-----
| THR  | IP-TH       | ARP   | 192.0.200.21 | D0:72:DC:A0:3D:4F | tunnel5 | epg300(49154) (V) | 21
|
```

Table Count: 1

ステップ5 FHS 設定の表示:

例 :

```
swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security binding-table
```

Pod/Node State	Type	Family	IP Address	MAC Address	Interface	Level
1/102 reach	local	ipv4	192.0.200.1	00:22:BD:F8:19:FF	vlan3	static- authenticated
1/102 reach	local	ipv6	fe80::200	00:22:BD:F8:19:FF	vlan3	static- authenticated
1/102 reach	local	ipv6	2001:0:0:200::1	00:22:BD:F8:19:FF	vlan3	static- authenticated
1/101 stale	arp	ipv4	192.0.200.23	D0:72:DC:A0:02:61	eth1/2	lla-mac-match , untrusted-access
1/101 reach	local	ipv4	192.0.200.1	00:22:BD:F8:19:FF	vlan3	static- authenticated

```

able
1/101 nd ipv6 fe80::d272:dcff:fea0 D0:72:DC:A0:02:61 eth1/2 lla-mac-match
reach :261 ,untrusted-
able
1/101 nd ipv6 2001:0:0:200::20 D0:72:DC:A0:02:61 eth1/2 access
stale lla-mac-match
,untrusted-
1/101 nd ipv6 2001::200:d272:dcff: fea0:261 D0:72:DC:A0:02:61 eth1/2 access
stale lla-mac-match
,untrusted-
1/101 local ipv6 fe80::200 00:22:BD:F8:19:FF vlan3 static-
reach authenticated
able
1/101 local ipv6 2001:0:0:200::1 00:22:BD:F8:19:FF vlan3 static-
reach authenticated
able
1/103 local ipv4 192.0.200.1 00:22:BD:F8:19:FF vlan4 static-
reach authenticated
able
1/103 local ipv6 fe80::200 00:22:BD:F8:19:FF vlan4 static-
reach authenticated
able
1/103 local ipv6 2001:0:0:200::1 00:22:BD:F8:19:FF vlan4 static-
reach authenticated
able
1/104 arp ipv4 192.0.200.10 F8:72:EA:AD:C4:7C eth1/1 lla-mac-match
stale ,trusted-access
1/104 arp ipv4 172.29.207.222 D0:72:DC:A0:3D:4C eth1/1 lla-mac-match
stale ,trusted-access
1/104 local ipv4 192.0.200.1 00:22:BD:F8:19:FF vlan4 static-
reach authenticated
able
1/104 nd ipv6 fe80::fa72:eaff:fead F8:72:EA:AD:C4:7C eth1/1 lla-mac-match
stale :c47c ,trusted-access
1/104 nd ipv6 2001:0:0:200::10 F8:72:EA:AD:C4:7C eth1/1 lla-mac-match
stale ,trusted-access
1/104 local ipv6 fe80::200 00:22:BD:F8:19:FF vlan4 static-
reach authenticated
able
1/104 local ipv6 2001:0:0:200::1 00:22:BD:F8:19:FF vlan4 static-
reach authenticated
able

```

Pod/Node	Type	IP Address	Creation TS	Last Refresh TS
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----

NX-OS CLI を使用した FHS の設定

```

1/102    local    192.0.200.1          2017-07-20T04:22:38.000+00:00  2017-07-20T04:22:38.000+00:00
1/102    local    fe80::200            2017-07-20T04:22:56.000+00:00  2017-07-20T04:22:56.000+00:00
1/102    local    2001:0:0:200::1     2017-07-20T04:22:57.000+00:00  2017-07-20T04:22:57.000+00:00
1/101    arp      192.0.200.23        2017-07-27T10:55:20.000+00:00  2017-07-27T16:07:24.000+00:00
1/101    local    192.0.200.1          2017-07-27T10:48:09.000+00:00  2017-07-27T10:48:09.000+00:00
1/101    nd       fe80::d272:dcff:fea0  2017-07-27T10:52:16.000+00:00  2017-07-27T16:04:29.000+00:00
        :261
1/101    nd       2001:0:0:200::20    2017-07-27T10:57:32.000+00:00  2017-07-27T16:07:24.000+00:00
1/101    nd       2001::200:d272:dcff:  2017-07-27T11:21:45.000+00:00  2017-07-27T16:07:24.000+00:00
        fea0:261
1/101    local    fe80::200            2017-07-27T10:48:10.000+00:00  2017-07-27T10:48:10.000+00:00
1/101    local    2001:0:0:200::1     2017-07-27T10:48:11.000+00:00  2017-07-27T10:48:11.000+00:00
1/103    local    192.0.200.1          2017-07-26T22:03:56.000+00:00  2017-07-26T22:03:56.000+00:00
1/103    local    fe80::200            2017-07-26T22:03:57.000+00:00  2017-07-26T22:03:57.000+00:00
1/103    local    2001:0:0:200::1     2017-07-26T22:03:58.000+00:00  2017-07-26T22:03:58.000+00:00
1/104    arp      192.0.200.10        2017-07-27T11:21:13.000+00:00  2017-07-27T16:05:48.000+00:00
1/104    arp      172.29.207.222      2017-07-27T11:54:48.000+00:00  2017-07-27T16:06:38.000+00:00
1/104    local    192.0.200.1          2017-07-27T10:49:13.000+00:00  2017-07-27T10:49:13.000+00:00
1/104    nd       fe80::fa72:eaff:fead  2017-07-27T11:21:13.000+00:00  2017-07-27T16:06:43.000+00:00
        :c47c
1/104    nd       2001:0:0:200::10    2017-07-27T11:21:13.000+00:00  2017-07-27T16:06:19.000+00:00
1/104    local    fe80::200            2017-07-27T10:49:14.000+00:00  2017-07-27T10:49:14.000+00:00
1/104    local    2001:0:0:200::1     2017-07-27T10:49:15.000+00:00  2017-07-27T10:49:15.000+00:00

```

swtb23-ifc1#

swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics arp

```

Pod/Node      : 1/101
Request Received : 4
Request Switched : 2
Request Dropped : 2
Reply Received  : 257
Reply Switched  : 257
Reply Dropped   : 0

```

```

Pod/Node      : 1/104
Request Received : 6
Request Switched : 6
Request Dropped : 0
Reply Received  : 954
Reply Switched  : 954
Reply Dropped   : 0

```

swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics dhcpv4

```

Pod/Node      : 1/102
Discovery Received : 5
Discovery Switched : 5
Discovery Dropped : 0
Offer Received    : 0
Offer Switched    : 0
Offer Dropped     : 0
Request Received   : 0
Request Switched   : 0
Request Dropped    : 0
Ack Received       : 0
Ack Switched       : 0
Ack Dropped        : 0
Nack Received      : 0
Nack Switched     : 0

```

```
Nack Dropped : 0
Decline Received : 0
Decline Switched : 0
Decline Dropped : 0
Release Received : 0
Release Switched : 0
Release Dropped : 0
Information Received : 0
Information Switched : 0
Information Dropped : 0
Lease Query Received : 0
Lease Query Switched : 0
Lease Query Dropped : 0
Lease Active Received : 0
Lease Active Switched : 0
Lease Active Dropped : 0
Lease Unassignment Received : 0
Lease Unassignment Switched : 0
Lease Unassignment Dropped : 0
Lease Unknown Received : 0
Lease Unknown Switched : 0
Lease Unknown Dropped : 0
```

```
swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics neighbor-discovery
Pod/Node : 1/101
Neighbor Solicitation Received : 125
Neighbor Solicitation Switched : 121
Neighbor Solicitation Dropped : 4
Neighbor Advertisement Received : 519
Neighbor Advertisement Switched : 519
Neighbor Advertisement Drop : 0
Router Solicitation Received : 4
Router Solicitation Switched : 4
Router Solicitation Dropped : 0
Router Adv Received : 0
Router Adv Switched : 0
Router Adv Dropped : 0
Redirect Received : 0
Redirect Switched : 0
Redirect Dropped : 0

Pod/Node : 1/104
Neighbor Solicitation Received : 123
Neighbor Solicitation Switched : 47
Neighbor Solicitation Dropped : 76
Neighbor Advertisement Received : 252
Neighbor Advertisement Switched : 228
Neighbor Advertisement Drop : 24
Router Solicitation Received : 0
Router Solicitation Switched : 0
Router Solicitation Dropped : 0
Router Adv Received : 53
Router Adv Switched : 6
Router Adv Dropped : 47
Redirect Received : 0
Redirect Switched : 0
Redirect Dropped : 0
```

FHS スイッチ iBASH コマンド

ステップ1 BD の FHS 機能設定と、EPG の信頼コントロール ポリシー設定を表示する show コマンド:

例:

```
leaf4# show fhs features all
```

```

BD-VNID          BD-Vlan          BD-Name
15630220         4                t0:bd200

Feature Policy:
  Feature    Family    Protocol    Operational-State    Options
ipinspect   IPV4      ARP         UP                   stalelifetime: 180s
ipinspect   IPV4      DHCP        UP                   -
ipinspect   IPV4      LOCAL       UP                   -
ipinspect   IPV4      STATIC      UP                   -
ipinspect   IPV6      ND          UP                   stalelifetime: 180s
ipinspect   IPV6      DHCP        UP                   -
ipinspect   IPV6      LOCAL       UP                   -
ipinspect   IPV6      STATIC      UP                   -
raguard     IPV6      -           UP                   ManagedCfgFlag: on
                                           OtherCfgFlag: on
                                           maxHopLimit: 15
                                           minHopLimit: 3
                                           routerPref: medium
-----
Trust Policy:
Epg-id          Epg-type          Epg-name
49154           Ckt-Vlan          epg300
  Trust-Attribute    Operational-State
PROTO-ARP           UP
PROTO-ND            UP
DHCPV4-SERVER       UP
DHCPV6-SERVER       UP
ROUTER              UP

```

ステップ2 FHS のセキュリティ保護されたエンドポイントのデータベースを表示する show コマンド:

例:

```

leaf1# show fhs bt
all      data      dhcpv4    local    static
arp      detailed  dhcpv6    nd       summary

leaf1# show fhs bt all

Legend:
DHCP      : dhcp-assigned          TR      : trusted-access          UNRES : unresolved
Age       : Age since creation      CRTNG   : creating                 TENTV  : tentative
VERIFY   : verify                    UNDR    : undetermined-trust     INV    : invalid
NDP      : Neighbor Discovery Protocol  STA     : static-authenticated  REACH  : reachable
LM       : lla-mac-match        UNKNW   : unknown                   INTF   : Interface
TimeLeft : Remaining time since last refresh  INCMP   : incomplete           UNTR   :
untrusted-access

```

```
EPG-Mode:
  U : unknown   M : mac   V : vlan   I : ip

BD-VNID      BD-Vlan      BD-Name
15630220     3             t0:bd200
```

Origin	IP	MAC	INTF	EPG(sclass) (mode)	Trust-lvl
State	Age	TimeLeft			
ARP	192.0.200.23	D0:72:DC:A0:02:61	eth1/2	epg200(32770) (V)	LM,UNTR
STALE	00:07:47	00:01:33			
LOCAL	192.0.200.1	00:22:BD:F8:19:FF	vlan3	LOCAL(16387) (I)	STA
REACH	00:14:58	N/A			
NDP	fe80::d272:dcff:fea0:261	D0:72:DC:A0:02:61	eth1/2	epg200(32770) (V)	LM,UNTR
STALE	00:10:51	00:00:47			
NDP	2001:0:0:200::20	D0:72:DC:A0:02:61	eth1/2	epg200(32770) (V)	LM,UNTR
STALE	00:05:35	00:00:42			
LOCAL	fe80::200	00:22:BD:F8:19:FF	vlan3	LOCAL(16387) (I)	STA
REACH	00:14:58	N/A			
LOCAL	2001:0:0:200::1	00:22:BD:F8:19:FF	vlan3	LOCAL(16387) (I)	STA
REACH	00:14:57	N/A			

```
leaf1# show fhs bt summary all
```

```
-----
                          FHS Binding Table Summary
-----
BD-Vlan: 3          BD-Name: t0:bd200
  Total number of ARP entries      : 1
  Total number of DHCPv4 entries   : 0
  Total number of ND entries       : 2
  Total number of DHCPv6 entries   : 0
  Total number of Data entries     : 0
  Total number of Static entries   : 0
  Total number of Local entries    : 3
  Total number of entries          : 6
-----
Total entries across all BDs matching given filters
  Total number of ARP entries      : 1
  Total number of DHCPv4 entries   : 0
  Total number of ND entries       : 2
  Total number of DHCPv6 entries   : 0
  Total number of Data entries     : 0
  Total number of Static entries   : 0
  Total number of Local entries    : 3
  Total number of entries          : 6
-----
```

ステップ3 FHS エンドポイントの違反を表示する show コマンド:

例:

```
leaf1# show fhs violations all
```

```
Violation-Type:
  POL : policy      THR : address-theft-remote
  ROLE : role       TH  : address-theft
  INT  : internal

Violation-Reason:
  IP-MAC-TH : ip-mac-theft
  OCFG_CHK  : ra-other-cfg-check-fail
  ANC-COL   :
```

```

: anchor-collision
PRF-LVL-CHK : ra-rtr-pref-level-check-fail   INT-ERR   : internal-error           TRUST-CHK
: trust-check-fail
SRV-ROL-CHK : srv-role-check-fail           ST-EP-COL : static-ep-collision      LCL-EP-COL
: local-ep-collision
MAC-TH      : mac-theft                       EP-LIM    : ep-limit-reached         MCFG-CHK
: ra-managed-cfg-check-fail
HOP-LMT-CHK : ra-hoplimit-check-fail        MOV-COL   : competing-move-collision RTR-ROL-CHK
: rtr-role-check-fail
IP-TH       : ip-theft

```

Trust-Level:

```

TR   : trusted-access      UNTR  : untrusted-access      UNDTR  : undetermined-trust
INV  : invalid             STA   : static-authenticated    LM     : lla-mac-match
DHCP : dhcp-assigned

```

EPG-Mode:

```

U : unknown   M : mac   V : vlan   I : ip

```

```

BD-VNID      BD-Vlan      BD-Name
15630220     4              t0:bd200

```

Type	Last-Reason	Proto	IP	MAC	Port
EPG(sclass) (mode)	Trust-lvl	Count			
TH	IP-TH	ND	2001:0:0:200::20	D0:72:DC:A0:3D:4F	eth1/1
epg300 (49154) (V)	LM,UNTR	2			
POL	HOP-LMT-CHK	RD	fe80::fa72:eaff:fead:c47c	F8:72:EA:AD:C4:7C	eth1/1
epg300 (49154) (V)	LM,TR	2			

Table Count: 2

ステップ4 FHS コントロール パケット 転送カウンタを表示する show コマンド:

例:

```

leaf1# show fhs counters
all   arp   dhcpv4  dhcpv6  nd
leaf4# show fhs counters all

```

```

BD-VNID      BD-Vlan      BD-Name
15630220     4              t0:bd200

```

Counter Type	Received	Switched	Dropped
Arp Request	6	6	0
Arp Reply	94	94	0
Dhcpv4 Ack	0	0	0
Dhcpv4 Decline	0	0	0
Dhcpv4 Discover	0	0	0
Dhcpv4 Inform	0	0	0
Dhcpv4 Leaseactive	0	0	0
Dhcpv4 Leasequery	0	0	0
Dhcpv4 Leaseunassigned	0	0	0
Dhcpv4 Leaseunknown	0	0	0
Dhcpv4 Nack	0	0	0
Dhcpv4 Offer	0	0	0
Dhcpv4 Release	0	0	0
Dhcpv4 Request	0	0	0
Dhcpv6 Advertise	0	0	0
Dhcpv6 Confirm	0	0	0
Dhcpv6 Decline	0	0	0

Dhcipv6 Informationreq		0		0		0	
Dhcipv6 Rebind		0		0		0	
Dhcipv6 Reconfigure		0		0		0	
Dhcipv6 Relayforw		0		0		0	
Dhcipv6 Relayreply		0		0		0	
Dhcipv6 Release		0		0		0	
Dhcipv6 Renew		0		0		0	
Dhcipv6 Reply		0		0		0	
Dhcipv6 Request		0		0		0	
Dhcipv6 Solicit		0		0		0	

Nd Na		18		18		0	
Nd Ns		26		22		4	
Nd Ra		11		6		5	
Nd Redirect		0		0		0	
Nd Rs		0		0		0	

ステップ5 NxOS メモリから FHS のセキュリティ保護されたエンドポイントのデータベースを表示します。

例:

```
leaf1# vsh -c 'show system internal fhs bt'
```

```
Binding Table has 7 entries, 4 dynamic
```

Codes:

```
L - Local           S - Static           ND - Neighbor Discovery   ARP - Address Resolution Protocol
DH4 - IPv4 DHCP     DH6 - IPv6 DHCP       PKT - Other Packet       API - API created
```

Preflevel flags (prlvl):

```
0001: MAC and LLA match      0002: Orig trunk          0004: Orig access
0008: Orig trusted trunk     0010: Orig trusted access 0020: DHCP assigned
0040: Cga authenticated     0080: Cert authenticated  0100: Statically assigned
```

EPG types:

```
V - Vlan Based EPG      M - MAC Based EPG      I - IP Based EPG
```

Code	Network Layer Address		Link Layer Address		Interface		Vlan
EPg	prlvl Age		Time left				
ARP	172.29.207.222		d0:72:dc:a0:3d:4c		Eth1/1		4
0x40000c002 (V)	0011 29 s		157 s				
L	192.0.200.1		00:22:bd:f8:19:ff		Vlan4		4
0x400004003 (I)	0100 55 mn						
ARP	192.0.200.10		f8:72:ea:ad:c4:7c		Eth1/1		4
0x40000c002 (V)	0011 156 s		30 s				
L	2001:0:0:200::1		00:22:bd:f8:19:ff		Vlan4		4
0x400004003 (I)	0100 55 mn						
ND	2001:0:0:200::10		f8:72:ea:ad:c4:7c		Eth1/1		4
0x40000c002 (V)	0011 143 s		47 s				
L	fe80::200		00:22:bd:f8:19:ff		Vlan4		4
0x400004003 (I)	0100 55 mn						
ND	fe80::fa72:eaff:fead:c47c		f8:72:ea:ad:c4:7c		Eth1/1		4
0x40000c002 (V)	0011 176 s		11 s				

ステップ6 NX-OS FHS プロセス内蔵メモリから FHS 機能の設定を表示します。

例:

```
leaf4# vsh -c 'show system internal fhs pol'
```

```

Target          Type Policy          Feature          Target-Range Sub-Feature
epg 0x40000c002 EPG  epg 0x40000c002 Trustctrl       vlan 4         Device-Roles: DHCPv4-Server,
DHCpV6-Server, Router

vlan 4          VLAN vlan 4          IP inspect      vlan all       Protocols: ARP ND
DHCpV6,        VLAN vlan 4          RA guard        vlan all       Protocols: ARP, DHCPv4, ND,
vlan 4          VLAN vlan 4          M-Config-flag:Enable,On
Router-Pref:medium
O-Config-flag:Enable,On,

```

ステップ7 NX-OS 共有データベースから FHS のセキュリティ保護されたエンドポイントのデータベースを表示します。

例:

```
leaf1# vsh -c 'show system internal fhs sdb bt'
```

```

Preflevel flags (preflvl):
0001: MAC and LLA match      0002: Orig trunk           0004: Orig access
0008: Orig trusted trunk    0010: Orig trusted access  0020: DHCP assigned
0040: Cga authenticated     0080: Cert authenticated   0100: Statically assigned

Origin      Zone ID      L3 Address      MAC Address      VLAN ID  EPG
ID          IF-name      Preflvl  State
-----
ARP         0x4         172.29.207.222  d0:72:dc:a0:3d:4c  4
0x40000c002 Eth1/1      0011  STALE
L          0x4         192.0.200.1    00:22:bd:f8:19:ff  4
0x400004003 Vlan4      0100  REACHABLE
ARP         0x4         192.0.200.10   f8:72:ea:ad:c4:7c  4
0x40000c002 Eth1/1      0011  REACHABLE
L          0x4         2001:0:0:200::1 00:22:bd:f8:19:ff  4
0x400004003 Vlan4      0100  REACHABLE
ND         0x4         2001:0:0:200::10 f8:72:ea:ad:c4:7c  4
0x40000c002 Eth1/1      0011  STALE
L          0x80000004 fe80::200     00:22:bd:f8:19:ff  4
0x400004003 Vlan4      0100  REACHABLE
ND         0x80000004 fe80::fa72:eaff:fead:c47c f8:72:ea:ad:c4:7c  4
0x40000c002 Eth1/1      0011  STALE

```

ステップ8 NxOS 共有データベースから FHS 機能の設定を表示します。

例:

```
leaf1# vsh -c 'show system internal fhs sdb pol'
```

```

Policies:

IP inspect      Vlan 4          Protocols:ARP DHCPv4 ND DHCPv6
RA guard        Vlan 4          Min-HL:3 Max-HL:15 M-Config-Flag:enable,on
O-Config-Flag:enable,on Router-Pref:medium
Trustctrl       Epg 0x40000c002 Vlan:4
Device-Roles:DHCPv4-Server DHCPv6-Server Router
Protocols:ARP ND

```

ステップ9 セキュリティ保護されたデータベース エンドポイント エントリを消去する show コマンド:

例:

```
leaf1# vsh -c 'clear system internal fhs bt ipv4 172.29.207.222'
```

REST API を使用して apic 内で FHS の設定

始める前に

- テナントおよびブリッジ ドメインは設定しておく必要があります。

FHS と信頼制御ポリシーを設定します。

例 :

```
<polUni>
  <fvTenant name="Coke">
    <fhsBDPol name="bdpol5" ipInspectAdminSt="enabled-ipv6" srcGuardAdminSt="enabled-both"
raGuardAdminSt="enabled" status="">
      <fhsRaGuardPol name="raguard5" managedConfigCheck="true" managedConfigFlag="true"
otherConfigCheck="true" otherConfigFlag="true" maxRouterPref="medium" minHopLimit="3" maxHopLimit="15"
status=""/>
    </fhsBDPol>
    <fvBD name="bd3">
      <fvRsBDToFhs tnFhsBDPolName="bdpol5" status=""/>
    </fvBD>
  </fvTenant>
</polUni>

<polUni>
<fvTenant name="Coke">
  <fhsTrustCtrlPol name="trustctrl5" hasDhcpv4Server="true" hasDhcpv6Server="true"
hasIpv6Router="true" trustRa="true" trustArp="true" trustNd="true" />
  <fvAp name="wwwCokecom3">
    <fvAEPg name="test966">
      <fvRsTrustCtrl tnFhsTrustCtrlPolName="trustctrl5" status=""/>
    </fvAEPg>
  </fvAp>
</fvTenant>
</polUni>
```


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。