P コマンド

この章では、P で始まる Cisco NX-OS TrustSec コマンドについて説明します。

permit

セキュリティ グループ アクセス コントロール リスト（SGACL）に許可ルールを設定するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

構文の説明

all	すべてのトラフィックを指定します。
icmp	インターネット制御メッセージ プロトコル（ICMP）トラフィックを指定します。
igmp	インターネット グループ管理プロトコル（IGMP）トラフィックを指定します。
ip	IP トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	ユーザ データグラム プロトコル（UDP）トラフィックを指定します。
dest	宛先ポート番号を指定します。
dst	宛先ポート番号を指定します。
src	送信元ポート番号を指定します。
eq	ポート番号と同等の番号を指定します。
gt	ポート番号より大きい番号を指定します。
lt	ポート番号より小さい番号を指定します。
neq	ポート番号と同等ではない番号を指定します。
port-number	TCP または UDP のポート番号。指定できる範囲は 0 ～ 65535 です。
range	TCP または UDP のポート範囲を指定します。
port-number1	範囲の開始ポート。指定できる範囲は 0 ～ 65535 です。
port-number2	範囲の終了ポート。指定できる範囲は 0 ～ 65535 です。
log	（任意）この設定に一致するパケットをログに記録することを指定します。

デフォルト

なし

コマンド モード

ロールベース アクセス コントロール リスト（RBACL）

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

RBACL ロギングをイネーブルにするには、VLAN での RBACL ポリシーの強制をイネーブルにする必要があります。また **cts role-based counters enable** コマンドを使用して Cisco TrustSec カウンタをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SGACL に許可アクションを追加し、RBACL ログをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# permit icmp log
switch(config-rbacl)#
```

次に、SGACL から許可ルールを削除する例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no permit icmp log
switch(config-rbacl)#
```

関連コマンド

コマンド	説明
cts role-based access-list	Cisco TrustSec SGACL を設定します。
cts role-based counters	RBACL カウンタをイネーブルにします。
deny	SGACL に拒否アクションを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

policy

Cisco TrustSec デバイス識別情報または Security Group Tag（SGT; セキュリティ グループ タグ）を使用して、インターフェイス上に Cisco TrustSec 認証ポリシーを手動で設定するには、**policy** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

policy {**dynamic identity** *device-id* | **static sgt** *sgt-value* [**trusted**]}

no policy {**dynamic** | **static**}

構文の説明

dynamic identity	Cisco TrustSec デバイス識別情報を使用してダイナミック ポリシーを指定します。
device-id	Cisco TrustSec デバイス識別情報。デバイス識別情報は、大文字と小文字を区別して指定します。
static sgt	SGT を使用してスタティック ポリシーを指定します。
sgt-value	Cisco TrustSec SGT。形式は、**0x***hhhh* です。範囲は 0x2 ～ 0xffef です。
trusted	（任意）インターフェイス上で受信したトラフィックに SGT が設定されている場合、タグを上書きしません。

コマンド デフォルト

なし

コマンド モード

Cisco TrustSec 手動コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown** と **no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、インターフェイスにダイナミック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、手動で設定したダイナミック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、インターフェイスにスタティック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、手動で設定したスタティック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec 手動コンフィギュレーションモードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

propagate-sgt

レイヤ 2 Cisco TrustSec インターフェイス上でセキュリティ グループ タグ（SGT）伝搬をイネーブルにするには、**propagate-sgt** コマンドを使用します。SGT 伝搬をディセーブルにするには、このコマンドの **no** 形式を使用します。

propagate-sgt

no propagate-sgt

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

手動設定がインターフェイスでイネーブルにされている場合、イネーブルになります。

手動設定がインターフェイスでディセーブルにされている場合、ディセーブルになります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

インターフェイスに接続しているピア デバイスで SGT がタグ付けされた Cisco TrustSec パケットを制御できない場合は、そのインターフェイスで SGT 伝搬機能をディセーブルにすることができます。

このコマンドを使用したあと、設定を有効にするには、**shutdown** と **no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SGT 伝搬をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、SGT 伝搬をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# propagate-sgt
```

```
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec 手動設定をイネーブルにします。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。