show vlan group から switchport port-security violation まで

- single-connection, 2 ページ
- source, 3 ページ
- ssh, 5 ページ
- switchport port-security, 12 ページ

single-connection

単一の TCP 接続を使用したすべての TACACS パケットの同じサーバへの送信をイネーブルにするには、TACACS+ サーバ コンフィギュレーション モードで **single-connection** コマンドを使用します。 この機能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。

single-connection

no single-connection

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

TACACS パケットは単一の TCP 接続では送信されません。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

single-connection コマンドを使用して、単一の TCP 接続を介してすべての TACACS パケットを同じサーバに向けて多重化します。

例

次に、単一の TCP 接続を介して、すべての TACACS パケットを TACACS サーバに向けて多重化する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、config server tacacs モードを開始します。

source

送信元アドレスに順次番号を付けるには、IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション モードで **source** コマンドを使用します。 シーケンスを削除するには、このコマンドの **no** 形式を使用します。

source *sequence interface* **track** *track-number*

no source *sequence*

構文の説明

sequence	シーケンス番号を割り当てます。
interface	インターフェイスのタイプと番号
track *track-number*	トラック番号を使用して送信元アドレスをトラッキングします。

コマンド デフォルト

トラック ステータスは常にアップ状態です。

コマンド モード

IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション（config-ikev2-flexvpn）

コマンド履歴

リリース	変更内容
15.2(1)T	このコマンドが導入されました。
Cisco IOS XE Release 3.7S	このコマンドが、Cisco IOS XE Release 3.7S に統合されました。

使用上のガイドライン

このコマンドをイネーブルにする前に、**crypto ikev2 client flexvpn** コマンドを設定する必要があります。

シーケンス番号が一番小さいものが送信元アドレスで、これに対しては送信元 IP アドレスがトンネル インターフェイスのトンネル VRF で使用可能な場合だけ、トラック オブジェクトがアップ状態になります。 送信元に対してセッションがアップ状態である場合、その送信元は「現在アクティブな送信元」と呼ばれます。

（注） このコマンドが変更された結果、アクティブなセッションが終了されます。

例

次に、スタティック ピアを定義する例を示します。

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# source 1 Ethernet 0/1 track 11
```

関連コマンド

コマンド	説明
crypto ikev2 client flexvpn	IKEv2 FlexVPN クライアント プロファイルを定義します。

ssh

リモート ネットワーキング デバイスとの暗号化されたセッションを開始するには、特権 EXEC モードまたはユーザ EXEC モードで **ssh** コマンドを使用します。

ssh [**-v** {**1**| **2**}| **c** {**3des**| **aes128-cbc**| **aes192-cbc**| **aes256-cbc**}| **-l** *userid*| **-l** *userid:vrfname number ip-address ip-address*| **-l** *userid:rotary number ip-address*| **-m** {**hmac-md5**| **hmac-md5-96**| **hmac-sha1**| **hmac-sha1-96**}| **-o numberofpasswordprompts** *n*| **-p** *port-num*] {**ip-addr**| **hostname**} [**command**| **-vrf**]

構文の説明

-v	（任意）サーバに接続するために使用する、セキュア シェル（SSH）のバージョンを指定します。 • **1**：SSH バージョン 1 を使用して接続します。 • **2**：SSH バージョン 2 を使用して接続します。

-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc }	（任意）データの暗号化に使用する暗号化アルゴリズムとして、データ暗号規格（DES）、トリプルDES（3DES）、高度暗号化規格（AES）のいずれかを指定します。サポートされているAESアルゴリズムは、aes128-cbc、aes192-cbc、およびaes256-cbcです。 • SSHバージョン1を使用するには、ルータで暗号化イメージを実行していなければいけません。暗号化を含むCiscoソフトウェアイメージは、指定子「k8」（DES）または「k9」（3DES）を持ちます。 • SSHバージョン2は、aes128-cbc、aes192-cbc、aes256-cbcおよび3des-cbc暗号化アルゴリズムだけをサポートしています。SSHバージョン2は、3DESイメージでのみサポートされています。 • **-c**キーワードを指定しない場合、ネゴシエーション中にリモート ネットワーキング デバイスは、サポートされているすべてのクリプトアルゴリズムを送信します。 • **-c**キーワードを設定しても、指定した引数（des、3des、aes128-cbc、aes192-cbc、aes256-cbcのいずれか）をサーバがサポートしていない場合、リモート ネットワーキング デバイスは接続を閉じます。
-l *userid*	（任意）SSHサーバを実行しているリモートネットワーキングデバイスにログインするときに使用するユーザIDを指定します。ユーザIDを省略すると、デフォルトとして現在のユーザIDが使用されます。

-l *userid* **:** *vrfname number ip-address*	（任意）*userid* フィールドにポート情報を含めることで、リバース SSH を設定するときにユーザ ID を指定します。 • **:**：**ポート番号と端末 IP アドレスがユーザ ID に続くことを示します。** • vrfname：ユーザ固有の VRF。 • *number*：端末または補助回線番号。 • *ip-address*：ターミナル サーバの IP アドレス。 （注） *userid* フィールドにポート情報を含めることでリバース SSH を設定する場合（各端末または補助回線を別々のコマンド コンフィギュレーション行にリストする長いメソッドよりも簡単なメソッド）、*userid* 引数と **:** *number ip-address* デリミタおよび引数を使用する必要があります。vrfname を使用することで、SSH は VRF インスタンスにアドレスが存在するホストとのセッションを確立できます。
-l *userid* **:rotary** *number ip-address*	（任意）端末回線がリバース SSH のロータリー グループの下でグループ化されることを指定します。 • **:**：ロータリー グループ番号と端末 IP アドレスが続くことを示します。 • *number* ：端末または補助回線番号。 • *ip-address*：ターミナル サーバの IP アドレス。 （注） *userid* フィールドにロータリー情報を含めることでリバース SSH を設定する場合（各端末または補助回線を別々のコマンド コンフィギュレーション行にリストする長いプロセスよりも簡単なプロセス）、*userid* 引数および **:rotary{** *number} {ip-address}* デリミタおよび引数を使用する必要があります。

-m {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**	（任意）ハッシュされたメッセージ認証コード（HMAC）アルゴリズムを指定します。 • SSH バージョン 1 では、HMAC がサポートされていません。 • **-m** キーワードを指定しない場合、ネゴシエーション中にリモート ネットワーキング デバイスは、サポートされているすべての HMAC アルゴリズムを送信します。**-m** キーワードを設定しても、指定した引数（hmac-md5、hmac-md5-96、hmac-sha1、および hmac-sha1-96）をサーバがサポートしていない場合、リモート デバイスは接続を閉じます。
-o numberofpasswordprompts *n*	（任意）セッションを終了するまでにソフトウェアが生成するパスワードプロンプトの回数を指定します。SSH サーバが、試行回数に制限を適用する場合もあります。サーバによって設定された制限が **-o numberofpasswordprompts** キーワードで市営された値を下回る場合、サーバによって設定された制限が優先されます。デフォルトの試行回数は 3 回です。これは、Cisco IOS SSH サーバのデフォルトでもあります。指定できる値の範囲は、1 ～ 5 です。
-p *port-num*	（任意）リモート ホストの目的のポート番号を示します。デフォルトのポート番号は 22 です。
ip-addr | *hostname*	リモート ネットワーキング デバイスの IPv4 または IPv6 アドレスまたはホスト名を指定します。
command	（任意）リモート ネットワーキング デバイスで実行する Cisco IOS コマンドを指定します。リモート ホストが Cisco IOS ソフトウェアを実行していない場合、これはリモート ホストによって認識される任意のコマンドで構いません。コマンドにスペースが含まれる場合、コマンドを引用符で囲む必要があります。

-vrf	（任意）SSH クライアント側機能に VRF 認識を追加します。 クライアントの VRF インスタンス名は、正しいルーティングテーブルを検索し接続を確立するために、IP アドレスで指定されます。

コマンド デフォルト

コマンドが使用されない場合、暗号化セッションは存在しません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.1(3)T	このコマンドが導入されました。
12.2(8)T	IPv6 アドレスのサポートが追加されました。
12.0(21)ST	IPv6 アドレスのサポートが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	IPv6 アドレスのサポートが Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	IPv6 アドレスのサポートが Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX	このコマンドが Cisco IOS Release 12.2(17a)SX に統合されました。
12.3(7)T	このコマンドは、セキュア シェル バージョン 2 をサポートするように拡張されました。 **-c** キーワードは、aes128-cbc、aes192-cbc、および aes256-cbc 暗号アルゴリズムのサポートを含めるために拡張されました。 **-m** キーワードが、アルゴリズム hmac-md5、hmac-md5-96、hmac-sha1、および hmac-sha1-96 とあわせて追加されました。 **-v** キーワードと引数**1** および **2** が追加されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.3(11)T	**-l** *userid* **:** *number ip-address* および **-l** *userid* **: rotary** *number ip-address* キーワードと引数オプションが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。

リリース	変更内容
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.3(7)JA	このコマンドが、Cisco IOS Release 12.3(7)JA に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.0(32)SY	このコマンドが、Cisco IOS Release 12.0(32)SY に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	**-l** *userid* **:** *vrfname number ip-address* キーワードと引数および *-vrf* キーワードが追加されました。
Cisco IOS XE Release 2.4	このコマンドは、Cisco ASR 1000 シリーズルータで導入されました。

使用上のガイドライン

ssh コマンドを使用することで、Cisco ルータは別の Cisco ルータまたは SSH バージョン 1 またはバージョン2サーバを実行しているデバイスとの間に、安全で暗号化された接続を確立できます。この接続は、接続が暗号化されている点を除き、アウトバウンド Telnet 接続の機能と同様です。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

（注） SSH バージョン 1 は、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェア イメージでだけサポートされます。 DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。 3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。

- SSH バージョン 2 は、aes128-cbc、aes192-cbc、および aes256-cbc 暗号化アルゴリズムだけをサポートしています。 SSH バージョン 2 は、3DES イメージでのみサポートされています。
- SSH バージョン 1 では、HMAC アルゴリズムがサポートされていません。

次に、ローカル ルータとリモート ホスト HQhost の間で安全なセッションを開始し、**show users** コマンドを実行する例を示します。 **show users** コマンドの結果は、HQhost にログインしている有効なユーザのリストです。 リモート ホストは、ユーザ adminHQ を認証するために、adminHQ パスワードを要求します。 認証ステップが成功すると、リモート ホストは、**show users** コマンドの結果をローカル ルータに返してから、セッションを閉じます。

```
ssh -l adminHQ HQhost "show users"
```

次に、ローカル ルータとエッジ ルータ HQedge の間で安全なセッションを開始し、**show ip route** コマンドを実行する例を示します。 この例では、エッジ ルータはユーザを認証するために、

adminHQ パスワードを要求します。 認証ステップが成功すると、エッジ ルータは、**show ip route** コマンドの結果をローカル ルータに返します。

```
ssh -l adminHQ HQedge "show ip route"
```

次に、3DES を使用して HQedge ルータと安全なリモート コマンド接続を開始する SSH クライアントの例を示します。 HQedge で稼働している SSH サーバは、標準の認証方式を使用して HQedge ルータの admin7 ユーザのセッションを認証します。 認証が機能するためには、HQedge ルータで SSH がイネーブルになっている必要があります。

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

次に、**show running-config** コマンドを実行するための、ローカル ルータとアドレス 3ffe:1111:2222:1044::72 のリモート IPv6 ルータとの間の安全なセッションの例を示します。 この例では、リモート IPv6 ルータはユーザを認証するために、adminHQ パスワードを要求します。 認証ステップが成功すると、リモート IPv6 ルータは、**show unning-config** コマンドの結果をローカル ルータに返してから、セッションを閉じます。

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```

（注） 最後の例では、IPv6 アドレス 3ffe:1111:2222:1044::72 にマップするホスト名が使用される可能性があります。

次に、クリプト アルゴリズム aes256-cbc と hmac-sha1-96 の HMAC を使用する SSH バージョン 2 セッションの例を示します。 ユーザ ID は user2、IP アドレスは 10.76.82.24 です。

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -1 user2 10.76.82.24
```

次に、SSH クライアントでリバース SSH が設定されている例を示します。

```
ssh -l lab:1 router.example.com
```

次のコマンドは、リバース SSH がロータリー グループの最初の空き回線に接続されることを表示します。

```
ssh -l lab:rotary1 router.example.com
```

関連コマンド

コマンド	説明
ip ssh	ルータに SSH サーバの制御パラメータを設定します。
show ip ssh	SSH のバージョンおよび設定データを表示します。
show ssh	SSH サーバ接続のステータスを表示します。

switchport port-security

インターフェイスでポート セキュリティをイネーブルにするには、インターフェイス コンフィギュレーション モードで **switchport port-security** コマンドを使用します。 ポート セキュリティ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。

switchport port-security

no switchport port-security

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートがリリース 12.2(17d)SXB に拡張されました。
12.2(18)SXE	Supervisor Engine 720 でこのコマンドが次のように変更されました。 • リリース 12.2(18)SXE 以降のリリースでは、トランクでポート セキュリティがサポートされます。 • リリース 12.2(18)SXE 以降のリリースでは、802.1Q トンネル ポートでポート セキュリティがサポートされます。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

ポート セキュリティを設定するときには、次の注意事項に従ってください。

- リリース 12.2(18)SXE 以降のリリースでは、トランクでポート セキュリティがサポートされます。
- リリース 12.2(18)SXE よりも前のリリースでは、トランクでポート セキュリティはサポートされません。

- リリース 12.2(18)SXE 以降のリリースでは、802.1Q トンネル ポートでポート セキュリティがサポートされます。
- リリース 12.2(18)SXE よりも前のリリースでは、802.1Q トンネル ポートでポート セキュリティはサポートされません。
- セキュア ポートは、スイッチド ポート アナライザ（SPAN）の宛先ポートにできません。
- セキュア ポートは、EtherChannel に所属できません。
- セキュア ポートはトランク ポートにはできません。
- セキュア ポートは 802.1X ポートにはできません。 セキュア ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。 802.1x 対応ポートをセキュア ポートに変更しようとしても、エラー メッセージが表示され、セキュリティ設定は変更されません。

例

次に、ポート セキュリティをイネーブルにする例を示します。

```
Router(config-if)#
switchport port-security
```

次に、ポート セキュリティをディセーブルにする例を示します。

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定情報を表示します。