showvlangroupthroughswitchportport-security violation

single-connection

To enable all TACACS packets to be sent to the same server using a single TCP connection, use the **single-connection**command in TACACS+ server configuration mode. To disable this feature, use the **no** form of this command.

single-connection

no single-connection

Syntax Description

This command has no arguments or keywords.

Command Default

TACACS packets are not sent on a single TCP connection.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **single-connection** command to multiplex all TACACS packets to the same server over a single TCP connection.

Examples

The following example shows how to multiplex all TACACS packets over a single TCP connection to the TACACS server:

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

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

source

To sequentially number the source address, use the **source** command in IKEv2 FlexVPN client profile configuration mode. To remove the sequence, use the **no** form of this command.

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

no source *sequence*

Syntax Description

sequence	Assigns a sequence number.
interface	Interface type and number.
track *track-number*	Tracks the source address with a track number.

Command Default

The track status is always up.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

The source address is the one with the lowest sequence number for which track object is in the UP state only if the source IP address is available in the tunnel VRF of the tunnel interface. If a session is UP for a source, the source is said to be a "Current active source".

Note Any changes to this command terminates the active session.

Examples

The following example shows how to define a static peer:

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

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in user EXEC or privileged EXEC mode.

ssh [**-v** {**1**| **2**}| **-c** {**aes128-ctr**| **aes192-ctr**| **aes256-ctr**| **aes128-cbc**| **3des**| **aes192-cbc**| **aes256-cbc**}| **-l** *user-id*| **-l** *user-id*:*vrf-name number ip-address ip-address*| **-l** *user-id*:*rotary number ip-address*| **-m** {**hmac-md5-128**| **hmac-md5-96**| **hmac-sha1-160**| **hmac-sha1-96**}| **-o numberofpasswordprompts** *n* | **-p** *port-num*] {*ip-addr* |*hostname* [**command**| **-vrf**]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. • **1**--Connects using SSH Version 1. • **2**--Connects using SSH Version 2.
-c {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des | aes192-cbc | aes256-cbc}	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms are **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, and **aes256-cbc**. • To use SSH Version 1, you must have an encryption image running on the device. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES). • SSH Version 2 supports only the following crypto algorithms: **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, **aes256-cbc**, and **3des**. SSH Version 2 is supported only in 3DES images. • If you do not specify the **-c** keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the**-c** keyword and the server does not support the argument that you have shown (**des**, **3des**, **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, or **aes256-cbc**), the remote networking device closes the connection.

-l *user-id*	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
-l *user-id* **:** *vrf-namenumber ip-address*	(Optional) Specifies the user ID when configuring reverse SSH by including port information in the *user-id* field. • **:** --Signifies that a VRF name, number, and terminal IP address will follow the user ID. • *vrf-name* --User-specific VRF. • *number* --Terminal or auxiliary line number. • *ip-address* --IP address of the terminal server. **Note** The *user-id* argument and **:** *number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including port information in the *user-id* field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line).The VRF name allows SSH to establish sessions with hosts whose addresses are in a VRF instance.
-l *user-id* **:rotary** *number ip-address*	(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH. • **:rotary** --Signifies that a rotary group number and terminal IP address will follow. • *number* --Terminal or auxiliary line number. • *ip-address* --IP address of the terminal server. **Note** The *user-id* argument and the **:rotary** *number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the *user-id* field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).

-m {**hmac-md5-128** | **hmac-md5-96** | **hmac-sha1-160** | **hmac-sha1-96**}	(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm. • SSH Version 1 does not support HMACs. • If you do not specify the **-m** keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the **-m** keyword and the server does not support the algorithm that you have shown (**hmac-md5-128**, **hmac-md5-96**, **hmac-sha1-160**, and **hmac-sha1-96**), the remote device closes the connection.
-o numberofpasswordprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswordprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p *port-num*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
ip-addr | *hostname*	Specifies the IPv4 or IPv6 address or hostname of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.
-vrf	(Optional) Adds VRF awareness to SSH client-side functionality. The VRF instance name in the client is provided with the IP address to look up the correct routing table and establish a connection.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(8)T	This command was modified. Support for IPv6 addresses was added.
12.0(21)ST	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.3(7)T	This command was modified to include Secure Shell Version 2 support. The **-c** keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The **-m** keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The **-v**keyword and **1** and **2** arguments were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **-l** *userid***:***number ip-address and* **-l** *userid***:rotary** *number ip-address* keyword and argument options were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The**-l** *userid***:***vrfname number ip-address* keyword and argument options were added
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.3(2)S	This command was modified. SSH version 2 supports counter-based AES encryption for 128-, 192-, and 256-bit key length.
Cisco IOS XE Release 3.9S	This command was modified. SSH version 2 supports counter-based AES encryption for 128-, 192-, and 256-bit key length.

Release	Modification
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **ssh** command enables a Cisco device to make a secure, encrypted connection to another Cisco device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Note SSH Version 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

- SSH Version 2 supports only the following crypto algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

Examples

The following example illustrates the initiation of a secure session between the local device and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local device and will then close the session.

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

The following example illustrates the initiation of a secure session between the local device and the edge device HQedge to run the **show ip route** command. In this example, the edge device prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge device will return the result of the **show ip route** command to the local device.

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

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge device. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge device using standard authentication methods. The HQedge device must have SSH enabled for authentication to work.

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

The following example shows a secure session between the local device and a remote IPv6 device with the address 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF to run the **show running-config** command. In this example, the remote IPv6 device prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 device will return the result of the **show running-config** command to the local device and will then close the session.

```
Device# ssh -l adminHQ 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF "show running-config"
```

The following example shows an SSH Version 2 session using the crypto algorithm aes256-ctr and an HMAC of hmac-sha1-96. The user ID is user2 and the IP address is 10.76.82.24.

```
Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24
```

The following example shows how to configure reverse SSH on the SSH client:

```
Device# ssh -l lab:1 device.example.com
```

The following command shows how to connect reverse SSH to the first free line in the rotary group:

```
Device# ssh -l lab:rotary1 device.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the device.
show ip route	Displays the contents of the routing table.
show ip ssh	Displays the version and configuration data for SSH.
show running-config	Displays the contents of the running configuration file.
show ssh	Displays the status of SSH server connections.
show users	Displays information about the active lines on a device.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in interface configuration mode. To disable port security, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on nonnegotiating trunks. • With Release 12.2(18)SXE and later releases, port security is supported on IEEE 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on nonnegotiating trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on IEEE 802.1Q tunnel ports.
- Port security does not support Switch Port Analyzer (SPAN) destination ports.
- Port security does not support EtherChannel port-channel interfaces.
- With Cisco IOS Release 12.2(33)SXH and later releases, you can configure port security and 802.1X port-based authentication on the same port. With releases earlier than Cisco IOS Release 12.2(33)SXH:
  - If you try to enable 802.1X port-based authentication on a secure port, an error message appears and 802.1X port-based authentication is not enabled on the port.

- If you try to enable port security on a port configured for 802.1X port-based authentication, an error message appears and port security is not enabled on the port.

Examples

This example shows how to enable port security:

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

This example shows how to disable port security:

```
Device(config-if)# no switchport port-security
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.