VPN Troubleshooting for Firepower Threat Defense

This chapter describes Firepower Threat Defense VPN troubleshooting tools and debug information.

System Messages

The Message Center is the place to start your troubleshooting. This feature allows you to view messages that are continually generated about system activities and status. To open the Message Center, click **System Status**, located to the immediate right of the **Deploy** button in the main menu. See System Messages for details on using the Message Center.

VPN System Logs

You can enable system logging (syslog) for Firepower Threat Defense devices. Logging information can help you identify and isolate network or device configuration problems. When you enable VPN logging, these syslogs are sent from Firepower Threat Defense devices to the Firepower Management Center for analysis and archiving.

Any VPN syslogs that are displayed have a default severity level 'ERROR' or higher (unless changed). VPN logging is managed through Firepower Threat Defense platform settings. You can adjust the message severity level by editing the **VPN Logging Settings** in the Firepower Threat Defense platform settings policy for targeted devices (**Platform Settings** > **Syslog** > **Logging Setup**). See About Configuring Syslog for details on enabling VPN logging, configuring syslog servers, and viewing the system logs.

Note VPN syslogs are automatically enabled to be sent to the Firepower Management Center by default whenever a device is configured with site-to-site or remote access VPNs.

Viewing VPN System Logs

The Firepower System captures event information to help you to gather additional information about the source of your VPN problems. Any VPN syslogs that are displayed have a default severity level 'ERROR' or higher (unless changed). By default the rows are sorted by the **Time** column.

You must be an Admin user in a leaf domain to perform this task.

Before you begin

Enable VPN logging by checking the **Enable Logging to FMC** check box in the Firepower Threat Defense platform settings (**Devices** > **Platform Settings** > **Syslog** > **Logging Setup**). See About Configuring Syslog for details on enabling VPN logging, configuring syslog servers, and viewing the system logs.

Procedure

Step 1   Choose **Devices** > **VPN** > **Troubleshooting**.

Step 2   You have the following options:

- Search — To filter current message information, click **Edit Search**.
- View — To view VPN details associated with the selected message in the view, click **View**.
- View All — To view VPN details for all messages in the view, click **View All**.
- Delete — To delete selected messages from the database, click **Delete** or click **Delete All** to delete all the messages.

Debug Commands

This section explains how you use debug commands to help you diagnose and resolve VPN-related problems. Not all available debug commands are described in this section. Commands are included here based on the their usefulness in assisting you to diagnose VPN-related problems.

Usage Guidelines   Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with the Cisco Technical Assistance Center (TAC). Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

You can view debug output in a CLI session only. Output is directly available when connected to the Console port, or when in the diagnostic CLI (enter **system support diagnostic-cli**). You can also view output from the regular Firepower Threat Defense CLI using the **show console-output** command.

To show debugging messages for a given feature, use the **debug** command. To disable the display of debug messages, use the **no** form of this command. Use **no debug all** to turn off all debugging commands.

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description	*feature*	Specifies the feature for which you want to enable debugging. To see available features, use the **debug ?** command for CLI help.
	subfeature	(Optional) Depending on the feature, you can enable debug messages for one or more subfeatures. Use ? to see the available subfeatures.
	level	(Optional) Specifies the debugging level. The level might not be available for all features. Use ? to see the available levels.

Command Default

The default debugging level is 1.

Example

With multiple sessions running on a remote access VPN, troubleshooting can be difficult given the size of the logs. You can use the **debug webvpn condition** command to set up filters to target your debug process more precisely.

debug webvpn condition {**group** *name* | **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

Where:

- **group** *name* filters on a group policy (not a tunnel group or connection profile).

- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] filters on the public IP address of the client. The subnet mask (for IPv4) or prefix (for IPv6) is optional.

- **reset** resets all filters. You can use the **no debug webvpn condition** command to turn off a specific filter.

- **user** *name* filters by username.

If you configure more than one condition, the conditions are conjoined (ANDed), so that debugs are shown only if all conditions are met.

After setting up the condition filter, use the base **debug webvpn** command to turn on the debug. Simply setting the conditions does not enable the debug. Use the **show debug** and **show webvpn debug-condition** commands to view the current state of debugging.

The following shows an example of enabling a conditional debug on the user jdoe.

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Related Commands	Command	Description
	show debug	Shows the currently active debug settings.
	undebug	Disables debugging for a feature. This command is a synonym for **no debug**.

debug aaa

See the following commands for debugging configurations or settings associated with authentication, authorization, and accounting (AAA, pronounced "triple A").

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description		
	aaa	Enables debugging for AAA. Use ? to see the available subfeatures.
	accounting	(Optional) Enables AAA accounting debugging.
	authentication	(Optional) Enables AAA authentication debugging.
	authorization	(Optional) Enables AAA authorization debugging.
	common	(Optional) Specifies the AAA common debug level. Use ? to see the available levels.
	internal	(Optional) Enables AAA internal debugging.
	shim	(Optional) Specifies the AAA shim debug level. Use ? to see the available levels.
	url-redirect	(Optional) Enables AAA url-redirect debugging.

Command Default	The default debugging level is 1.

Related Commands	Command	Description
	show debug aaa	Shows the currently active debug settings for AAA.
	undebug aaa	Disables debugging for AAA. This command is a synonym for **no debug aaa**.

debug crypto

See the following commands for debugging configurations or settings associated with crypto.

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description		
	crypto	Enables debugging for *crypto*. Use ? to see the available subfeatures.

ca	(Optional) Specifies the PKI debug levels. Use ? to see the available subfeatures.
condition	(Optional) Specifies the IPsec/ISAKMP debug filters. Use ? to see the available filters.
engine	(Optional) Specifies the crypto engine debug levels. Use ? to see the available levels.
ike-common	(Optional) Specifies the IKE common debug levels. Use ? to see the available levels.
ikev1	(Optional) Specifies the IKE version 1 debug levels. Use ? to see the available levels.
ikev2	(Optional) Specifies the IKE version 2 debug levels. Use ? to see the available levels.
ipsec	(Optional) Specifies the IPsec debug levels. Use ? to see the available levels.
condition	(Optional) Specifies the Crypto Secure Socket API debug levels. Use ? to see the available levels.
vpnclient	(Optional) Specifies the EasyVPN client debug levels. Use ? to see the available levels.

Command Default   The default debugging level is 1.

Related Commands

Command	Description
show debug crypto	Shows the currently active debug settings for crypto.
undebug crypto	Disables debugging for crypto. This command is a synonym for **no debug crypto**.

debug crypto ca

See the following commands for debugging configurations or settings associated with crypto ca.

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description

crypto ca	Enables debugging for *crypto ca*. Use ? to see the available subfeatures.
cluster	(Optional) Specifies the PKI cluster debug level. Use ? to see the available levels.
cmp	(Optional) Specifies the CMP transactions debug level. Use ? to see the available levels.
messages	(Optional) Specifies the PKI Input/Output message debug level. Use ? to see the available levels.
periodic-authentication	(Optional) Specifies the PKI periodic-authentication debug level. Use ? to see the available levels.

scep-proxy	(Optional) Specifies the SCEP proxy debug level. Use ? to see the available levels.
server	(Optional) Specifies the local CA server debug level. Use ? to see the available levels.
transactions	(Optional) Specifies the PKI transaction debug level. Use ? to see the available levels.
trustpool	(Optional) Specifies the trustpool debug level. Use ? to see the available levels.
1-255	(Optional) Specifies the debugging level.

Command Default The default debugging level is 1.

Related Commands

Command	Description
show debug crypto ca	Shows the currently active debug settings for crypto ca.
undebug	Disables debugging for crypto ca. This command is a synonym for **no debug crypto ca**.

debug crypto ikev1

See the following commands for debugging configurations or settings associated with Internet Key Exchange version 1 (IKEv1).

debug *crypto ikev1* [*timers*] [*1-255*]

Syntax Description

ikev1	Enables debugging for *ikev1*. Use ? to see the available subfeatures.
timers	(Optional) Enables debugging for IKEv1 timers.
1-255	(Optional) Specifies the debugging level.

Command Default The default debugging level is 1.

Related Commands

Command	Description
show debug crypto ikev1	Shows the currently active debug settings for IKEv1.
undebug crypto ikev1	Disables debugging for IKEv1. This command is a synonym for **no debug crypto ikev1**.

debug crypto ikev2

See the following commands for debugging configurations or settings associated with Internet Key Exchange version 2 (IKEv2).

debug *crypto ikev2* [*ha* | *platform* | *protocol* | *timers*]

Syntax Description	*ikev2*	Enables debugging *ikev2*. Use ? to see the available subfeatures.
	ha	(Optional) Specifies the IKEv2 HA debug level. Use ? to see the available levels.
	platform	(Optional) Specifies the IKEv2 platform debug level. Use ? to see the available levels.
	protocol	(Optional) Specifies the IKEv2 protocol debug level. Use ? to see the available levels.
	timers	(Optional) Enables debugging for IKEv2 timers.

Command Default	The default debugging level is 1.

Related Commands	Command	Description
	show debug crypto ikev2	Shows the currently active debug settings for IKEv2.
	undebugcrypto ikev2	Disables debugging for IKEv2. This command is a synonym for **no debug crypto ikev2**.

debug crypto ipsec

See the following commands for debugging configurations or settings associated with IPsec.

debug *crypto ipsec* [*1-255*]

Syntax Description	*ipsec*	Enables debugging for *ipsec*. Use ? to see the available subfeatures.
	1-255	(Optional) Specifies the debugging level.

Command Default	The default debugging level is 1.

Related Commands	Command	Description
	show debug crypto ipsec	Shows the currently active debug settings for IPsec.
	undebugcrypto ipsec	Disables debugging for IPsec. This command is a synonym for **no debug crypto ipsec**.

debug ldap

See the following commands for debugging configurations or settings associated with LDAP (Lightweight Directory Access Protocol).

debug *ldap* [*1-255*]

Syntax Description	*ldap*	Enables debugging for LDAP. Use ? to see the available subfeatures.

1-255	(Optional) Specifies the debugging level.

Command Default　The default debugging level is 1.

Related Commands

Command	Description
show debug ldap	Shows the currently active debug settings for LDAP.
undebugldap	Disables debugging for LDAP. This command is a synonym for **no debug ldap**.

debug ssl

See the following commands for debugging configurations or settings associated with SSL sessions.

debug *ssl* [*cipher* | *device*] [*1-255*]

Syntax Description

ssl	Enables debugging for SSL. Use ? to see the available subfeatures.
cipher	(Optional) Specifies the SSL cipher debug level. Use ? to see the available levels.
device	(Optional) Specifies the SSL device debug level. Use ? to see the available levels.
1-255	(Optional) Specifies the debugging level.

Command Default　The default debugging level is 1.

Related Commands

Command	Description
show debug ssl	Shows the currently active debug settings for SSL.
undebug ssl	Disables debugging for SSL. This command is a synonym for **no debug ssl**.

debug webvpn

See the following commands for debugging configurations or settings associated with WebVPN.

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description

webvpn	Enables debugging for WebVPN. Use ? to see the available subfeatures.
anyconnect	(Optional) Specifies the WebVPN AnyConnect debug level. Use ? to see the available levels.
chunk	(Optional) Specifies the WebVPN chunk debug level. Use ? to see the available levels.

cifs	(Optional) Specifies the WebVPN CIFS debug level. Use ? to see the available levels.
citrix	(Optional) Specifies the WebVPN Citrix debug level. Use ? to see the available levels.
compression	(Optional) Specifies the WebVPN compression debug level. Use ? to see the available levels.
condition	(Optional) Specifies the WebVPN filter conditions debug level. Use ? to see the available levels.
cstp-auth	(Optional) Specifies the WebVPN CSTP authentication debug level. Use ? to see the available levels.
customization	(Optional) Specifies the WebVPN customization debug level. Use ? to see the available levels.
failover	(Optional) Specifies the WebVPN failover debug level. Use ? to see the available levels.
html	(Optional) Specifies the WebVPN HTML debug level. Use ? to see the available levels.
javascript	(Optional) Specifies the WebVPN Javascript debug level. Use ? to see the available levels.
kcd	(Optional) Specifies the WebVPN KCD debug level. Use ? to see the available levels.
listener	(Optional) Specifies the WebVPN listener debug level. Use ? to see the available levels.
mus	(Optional) Specifies the WebVPN MUS debug level. Use ? to see the available levels.
nfs	(Optional) Specifies the WebVPN NFS debug level. Use ? to see the available levels.
request	(Optional) Specifies the WebVPN request debug level. Use ? to see the available levels.
response	(Optional) Specifies the WebVPN response debug level. Use ? to see the available levels.
saml	(Optional) Specifies the WebVPN SAML debug level. Use ? to see the available levels.
session	(Optional) Specifies the WebVPN session debug level. Use ? to see the available levels.
task	(Optional) Specifies the WebVPN task debug level. Use ? to see the available levels.

transformation	(Optional) Specifies the WebVPN transformation debug level. Use ? to see the available levels.
url	(Optional) Specifies the WebVPN URL debug level. Use ? to see the available levels.
util	(Optional) Specifies the WebVPN utility debug level. Use ? to see the available levels.
xml	(Optional) Specifies the WebVPN XML debug level. Use ? to see the available levels.

Command Default   The default debugging level is 1.

Related Commands

Command	Description
show debug webvpn	Shows the currently active debug settings for WebVPN.
undebug webvpn	Disables debugging for WebVPN. This command is a synonym for **no debug webvpn**.