Implement Platform Settings for VPN Troubleshooting

Contents

Introduction Prerequisites Requirements Components Used Firewall Management Center Firewall Threat Defense

Introduction

This document describes how to easily organize and identify VPN debug logs using Secure Firewall Management Center and Secure Firewall Threat Defense.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Management Center (FMC)
- Basic understanding of navigating the FMC GUI and FTD CLI
- Existing policy assignment for Platform Settings

Components Used

The information in this document is based on these software versions and hardware versions:

- Firewall Management Center version 7.3
- Firewall Threat Defense version 7.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Firewall Management Center

Navigate to Devices > Platform Settings.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices Objects	Integration		
				Device Management	VPN	Troubleshoot	
Summer Dechboord				Device Upgrade	Site To Site	File Download	
Summary Dashboard twitch detries Provides a summary of activity on the appliance	1 1			NAT	Remote Access	Threat Defense CLI	
				QoS	Dynamic Access Policy	Packet Tracer	
Network × Threats Intrusion Events	Status	Geolocation	QoS	Platform Settings	Troubleshooting	Packet Capture	
				FlexConfig			
				Certificates			

Click the pencil between the copy and delete icon.

þ	Firewall Management Center Devices / Platform Settings	Overview	Analysis	Policies	Devices	Objects	Integration	
P	Natform Settings					Device Type		Status
	Production Settings					Threat Defense		Targeting 1 devices

Navigate to Syslogin the left column of options and ensure Enable Logging, and Send debug messages as syslog are enabled. Additionally, ensure the Memory Size of the Internal Buffer is set with a value that is adequate for troubleshooting purposes.



Click Logging Destinations and then click +Add.

Firewall Management	nt Center	Overview	Analysis	Policies	Devices	Objects	Integ	ration		
Production Settings Enter Description										
ARP Inspection	Logging Setup	Logging	Destinations	Email Setu	p Event L	ists Rat	e Limit	Syslog Settings	Syslog Servers	
Banner DNS										
External Authentication	Logging Destin	nation				Sy	slog from	All Event Class		Syslog from spe
Fragment Settings									No records to display	
HTTP Access										
ICMP Access										
SSH Access										
SMTP Server										
SNMP										
SSL										
Syslog										
Timeouts										
Time Synchronization										
Time Zone										
UCAPL/CC Compliance										
Performance Profile										

In this section, the logging destination is a preference of the administrator and Internal Buffer is used. Change Event Class to Filter on Severity and debugging. Once this is completed, click +Add and choose webvpn, vpn, auth, and caall with Syslog severity of debugging. This step allows the administrator to filter these debug outputs to a specific syslog message of 711001. These can be modified depending type of troubleshooting. However, the ones chosen in this example cover the most commonly encountered Site-to-Site, Remote Access, and AAA VPN-related issues.

ARP Inspection Banner	Logging Setup	Logging Destinations	Edit Logging Filter			• · •		0	-
DNS External Authentication Fragment Settings HTTP Access	Logging Destination	n	Logging Destination Event Class	Internal Buffer Filter on Severity	•	debugging	•	+ Add	og from sp øpridebug
ICMP Access SSH Access SMTD Senser			Event Class webypn		Syslog) Severity ging		/1	
SNMP SSL			vpn auth		debug; debug;	ging ging		/i /i	
Syslog Timeouts Time Synchronization			ca		debug	aing		/1	
Time Zone UCAPL/CC Compliance Performance Profile							Cancel	ОК	

Create event classes and filters for the debugs.

Warning: This changes the Buffer Logging Level to debugging and logs debugging events for the classes specified to the internal buffer. It is recommended to use this logging method for troubleshooting purposes, and not for long-term use.

Choose Save in the top right, and then Deploythe configuration changes.

Firewall Management	nt Center	Overview Ana	lysis Policies	Devices Objects	Integration		
Production Settings Enter Description							
ARP Inspection	Logging Setup	Logging Destin	ations Email Setup	Event Lists Ra	ite Limit Syslog Settings	Syslog Servers	
Banner DNS							
External Authentication	Logging Destinat	tion		s	yslog from All Event Class		Syslog from spe
Fragment Settings	Internal Buffer			F	Iter on Severity:debugging		webvpn:debuggi
HTTP Access							
ICMP Access							
SSH Access							
SMTP Server							
SNMP							
SSL							
Syslog							
Timeouts							
Time Synchronization							
Time Zone							
UCAPL/CC Compliance							
Performance Profile							

Firewall Threat Defense

Navigate to the FTD CLI and issue the command show logging setting. The settings here reflect the changes made on the FMC. Ensure the debug-trace logging is enabled, and the buffer logging matches the classes and logging level specified.



is applied. This triggers a logging debug-trace notice, letting the administrator know that these debugs are redirected. In order to view these debugs, issue the command show log | in 711001. This syslog ID now only contains relevant VPN debugs as applied by the administrator. Existing logs can be cleared with a clear logging buffer.

FTD72# debug webvpn anyconnect 255 INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and wi 'INFO: debug webvpn anyconnect enabled at level 255. 'FTD72# show log | in 711001

Shows all VPN debugs are being redirected to syslog 711001.