Konfigurieren von BFD in Secure Firewall Threat Defense über die Benutzeroberfläche

Inhalt

Einleitung Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird die Konfiguration des BFD-Protokolls in Secure Firewall Management Center (FMC) mit Version 7.3 und höher beschrieben.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Border Gateway Protocol (BGP)-Protokoll
- Bidirectional Forwarding Detection (BFD)-Konzepte

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure FMC Virtual Version 7.3.1
- BGP in Cisco Secure Firewall Threat Defense (FTD) mit Cisco Secure FMC mit Version 7.3 und höher konfiguriert

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

BFD ist ein Erkennungsprotokoll, das entwickelt wurde, um eine schnelle Erkennung von Pfadausfällen für alle Medientypen, Kapselungen, Topologien und Routing-Protokolle zu ermöglichen.

Konfigurieren

Informationen zu BFD-Konfigurationen in FMC mit Version 7.3 und höher finden Sie in den folgenden Schritten.

Schritt 1: Navigieren Sie zum Devicesund klicke auf die Schaltfläche Device Management-Taste.

Firewall Mana Overview / Dashboa	gement Center rds / Dashboard	Overview Analysis	Policies	Devices 1 Objects	Integration		
Summary Dashb Provides a summary of activity on t Network Threats	DOARD (switch dashboard) the appliance Intrusion Events	Status × Geolocation	QoS	Device Management Device Upgrade NAT QoS Platform Settings	2 VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	
Appliance Status			- x	FlexConfig Certificates		=	Current Session
Normai (D)		Criscal (3)		Name IPv4 Address IPv6 Address Model Versions Software Rule Update Geolocation Update VDB	FMC-HackTZ 10.88.243.103 Disabled Secure Finewall Management Center for 7.3.1 2023-07-12-001-vrt 2023-07-10-101 368	r VMware	Username
Product Updates			- ×	 RSS Feed - Unable to d 	nable to download feed	- ×	 System Load
Туре	Current	Latest				c	
Geolocation Update Local Geolocation Update Rule Update Local Rule Update Software							CPU 0 CPU 1 CPU 2
2 Devices VDB 1 Management Center							Memory Load Avg
Disk Usage			- ×				
By Category: https://10.88.243.103/ddd/#Senso	rList						

Bild 1. FMC-Dashboard:

Schritt 2: Wählen Sie das Gerät aus, das Sie für das BFD-Protokoll konfigurieren möchten.

þ	Firewall Management Center Devices / Device Management	Overview A	Analysis Policie	s Devices	Objects Ir	ntegration	
View B All (r: Group • 2) • Error (0) • Warning (0) •	● Offline (0) ● Nor	mal (2) 🗢 Depic	ryment Pending (0)	 Upgrade ((2) • Snort 3 (2)	
Collapse	LAI						
	Name		Model		Version	Chassis	Licenses
	 Ungrouped (2) 						
	SF3130-A Snort 3 10.88.146.203 - Routed		Firewall 3	130 Threat Defense	7.3.1	Manage	Essentials, IPS (2 more)
	SF3130-8 Short 3 10.88.146.205 - Routed		Firewall 3	130 Threat Defense	7.3.1	Manage	Essentials, IPS (2 more)

für das das BFD-Protokoll konfiguriert werden soll. Erstellen Sie eine neue Vorlage, indem Sie auf die Schaltfläche + -Taste.

Firewall Managemen Devices / Secure Firewall Ro	nt Center ^{uting}	Overview				Objects			
SF3130-A Cisco Secure Firewall 3130 Threat I Device Routing Interfac	Defense ves Inline Sets	DHCP							
Manage Virtual Routers Global Virtual Router Properties	Bidirection Single-Hop	nal Forwa Multi-Hop	arding De	etection	Routing	(BFD)			
ECMP					Add BFL	D Single-Ho	ib D	v	
	1000				Interface			_	
OSPF					BGP			v 1	
OSPFv3					Terretete	la ma			
EIGRP					Select	Name			
					 Template 	Name is manda			
Policy Based Routing									
							Cancel	OK	
IPv4							Carroer		
IPv6									
Static Route									
 Multicast Routing 									
IGMP							There are	no BFD records /	
PIM									
Multicast Routes									
Multicast Boundary Filter									
General Settings									

Schritt 5: Geben Sie der Vorlage einen Namen, und konfigurieren Sie die für den BFD gewünschten Parameter. Klicken Sie anschließend auf Speichern.

Devices / Secure Firewall Ro			
SF3130-A Cisco Secure Finewall 3130 Threat I Device Routing Interfac			
	Bidirectional Forwarding Detec	tion Routing (BFD) Add BFD Template Object	
		Name* Template Type: Single-Hop Multi-Hop Echo: disabled	
		Interval Authentication Interval Type: None	
		Multiplier:	
		Minimum Transmit: Minimum Receive:	

Abbildung 4: Schnittstellenauswahl.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.