

Configurazione di BFD in Secure Firewall Threat Defense con GUI

Sommario

[Introduzione](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare il protocollo BFD in Centro gestione firewall protetto (FMC) con versione 7.3 e successive.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo BGP (Border Gateway Protocol)
- Nozioni base sul rilevamento dell'inoltro bidirezionale (BFD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure FMC Virtual versione 7.3.1
- BGP configurato in Cisco Secure Firewall Threat Defense (FTD) con Cisco Secure FMC in esecuzione versione 7.3 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

BFD è un protocollo di rilevamento progettato per fornire tempi di rilevamento degli errori dei percorsi di inoltro rapido per tutti i tipi di supporti, incapsulamenti, topologie e protocolli di routing.

Configurazione

Fare riferimento a questi passaggi per le configurazioni BFD in FMC con versioni 7.3 e successive.

Passaggio 1. Passare alla **Devices** nella parte superiore e fare clic sul pulsante **Device Management** pulsante.

Firewall Management Center
Overview / Dashboards / Dashboard

Overview Analysis Policies **Devices** 1 Objects Integration

Summary Dashboard [\[refresh dashboard\]](#)
Provides a summary of activity on the appliance

Network Threats Intrusion Events Status X Geolocation QoS

Appliance Status

Normal (2) Critical (3)

Product Updates

Type	Current	Latest
Geolocation Update		
Local Geolocation Update	2023-07-10-101	2023-07-10-101
Rule Update		
Local Rule Update	2023-07-12-001-vrt	2023-07-12-001-vrt
Software		
1 Management Center	7.3.1	7.3.1
2 Devices	7.3.1	7.3.1
VDB		
1 Management Center	368	368

Disk Usage

By Category:

Appliance Information

Name	FMC-HackTZ
IPv4 Address	10.88.243.103
IPv6 Address	Disabled
Model	Secure Firewall Management Center for VMware
Versions	
Software	7.3.1
Rule Update	2023-07-12-001-vrt
Geolocation Update	2023-07-10-101
VDB	368

RSS Feed - Unable to download feed

Unable to download feed

Current Session

Username
admin

System Time

System Time
Uptime
Boot Time

System Load

CPU 0
CPU 1
CPU 2
CPU 3
Memory
Load Avg

<https://10.88.243.103/ddd/#SensorList>

Immagine 1. Dashboard FMC.

Passaggio 2. Scegliere il dispositivo che si desidera configurare per il protocollo BFD.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (2) Snort 3 (2)

Collapse All

Name	Model	Version	Chassis	Licenses
Ungrouped (2)				
SF3130-A Snort 3 10.88.146.203 - Routed	Firewall 3130 Threat Defense	7.3.1	Manage	Essentials, IPS (2 more...)
SF3130-B Snort 3 10.88.146.205 - Routed	Firewall 3130 Threat Defense	7.3.1	Manage	Essentials, IPS (2 more...)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).