

قفن ربع Syslog ل FTD تانايب ةهجاو نيوكت VPN

تايوتحمل

[قمدقمل](#)

[قيساسال تابلطتمل](#)

[تابلطتمل](#)

[قمدختسمل تانوكمل](#)

[قيساسا تامولعم](#)

[يطي طختل مسرل](#)

[نيوكتلا](#)

[قحصلال نمققحتلا](#)

[قلص تاذا تامولعم](#)

قمدقمل

قفن VPN ربع لسري syslog ل ردصمك نراق تايطعم Cisco FTD لكشي نأ فيك ققيشو اذه فصري

قيساسال تابلطتمل

تابلطتمل

قيلاتلا عيضاوملاب قفرعم كيدل نوكت ناب Cisco يصوت

- Cisco Secure Firewall Threat Defense (FTD) ىلع Syslog نيوكت
- Syslog قماع
- Cisco نم (FMC) نمالا عيامل رادج قراذ زكرم

قمدختسمل تانوكمل

قغيص زاهجو عيچمرب اذه ىلع ققيشو اذه يف قمولعمل تسسأ

- Cisco FTD، رادصال 7.3.1
- Cisco FMC، رادصال 7.3.1

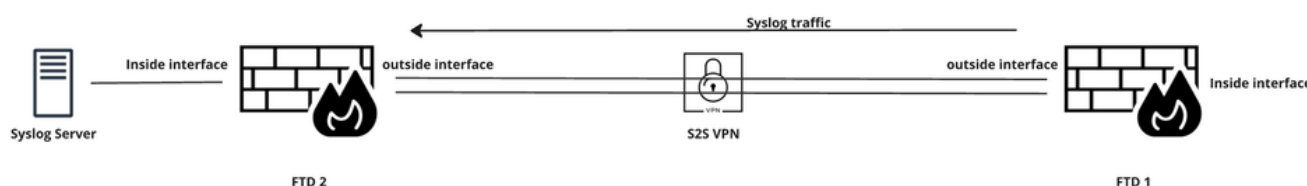
اذه عاشن! مت. تاسسؤم وأ تاغومجم وأ نييدرف نيمدختسم ياب قطبترم دنتسمل اذه يف اهيل! راشمل IP نيوانعو تاكشبشال نوكت ال: قيليوسمل اءال خإ قيلمعم قئييب يف مادختسالل ايرصحن نيوكتلا

نيوكتب دنتسمل اذه يف قمدختسمل ازهجالا عيمج تاندب. قصاخ قيلمعم قئييب يف قئوجولملا ازهجالا نم دنتسمل اذه يف قءراولاملا عمل عاشن! مت رما يال لمحتمل ريئاتلل كمهف نم دكاتف، ليغشتلا ديق كفتكشبش تنك اذ. (يضارتفا) حوسمم

قيساسا تامولعم

ىل قفن VPN ربع تلسرأ نوكتي نأ syslog ل ردصمك FTD نم نراق تايطعمل نم دحاو لمعتسي نأ لح ققيشو اذه فصري ديعب عقوم يف دجاوتي نوكتي نأ لدان syslog

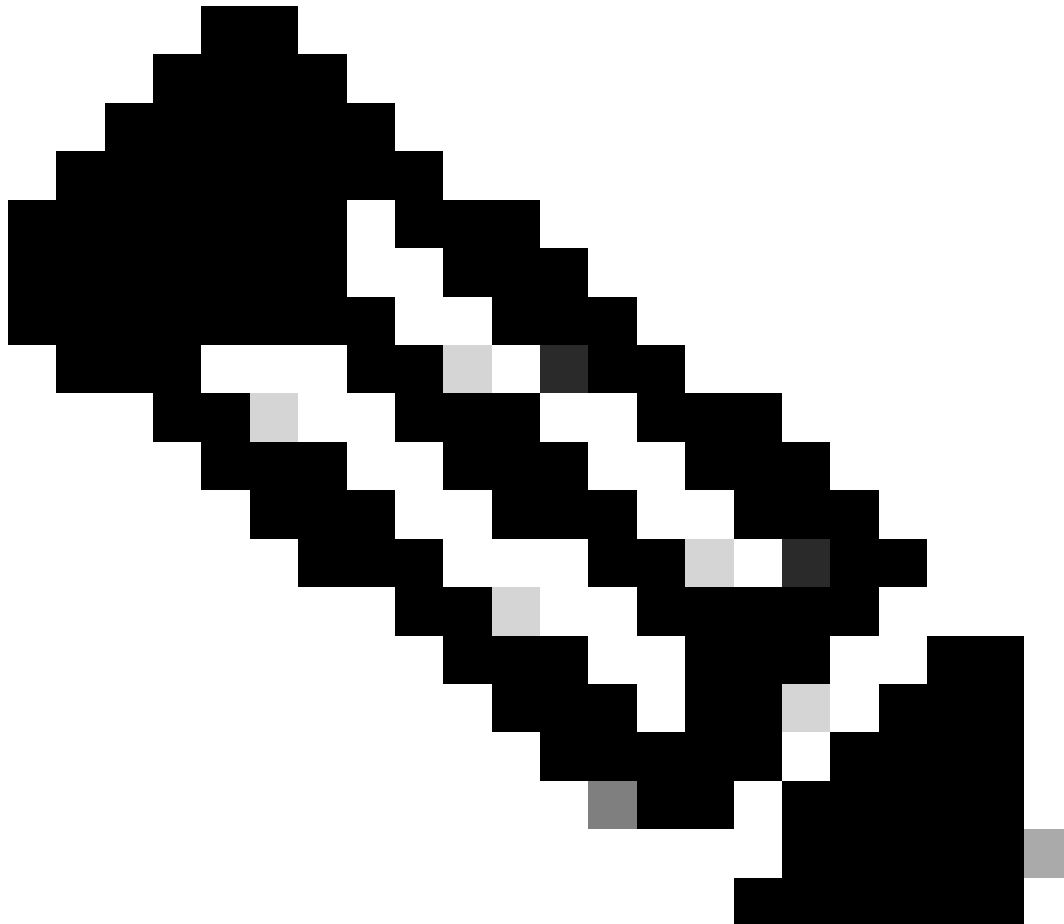
يطي طختل مسرل



قكشبش لل يطيطختل مسرل

رمال قيبطت كنكمي، قفنل ربع اهل اسرل متي يتل syslog رورم كرح رصم انم متي يتل هجاولا ديدحتل
management-access ربع Flex Config.

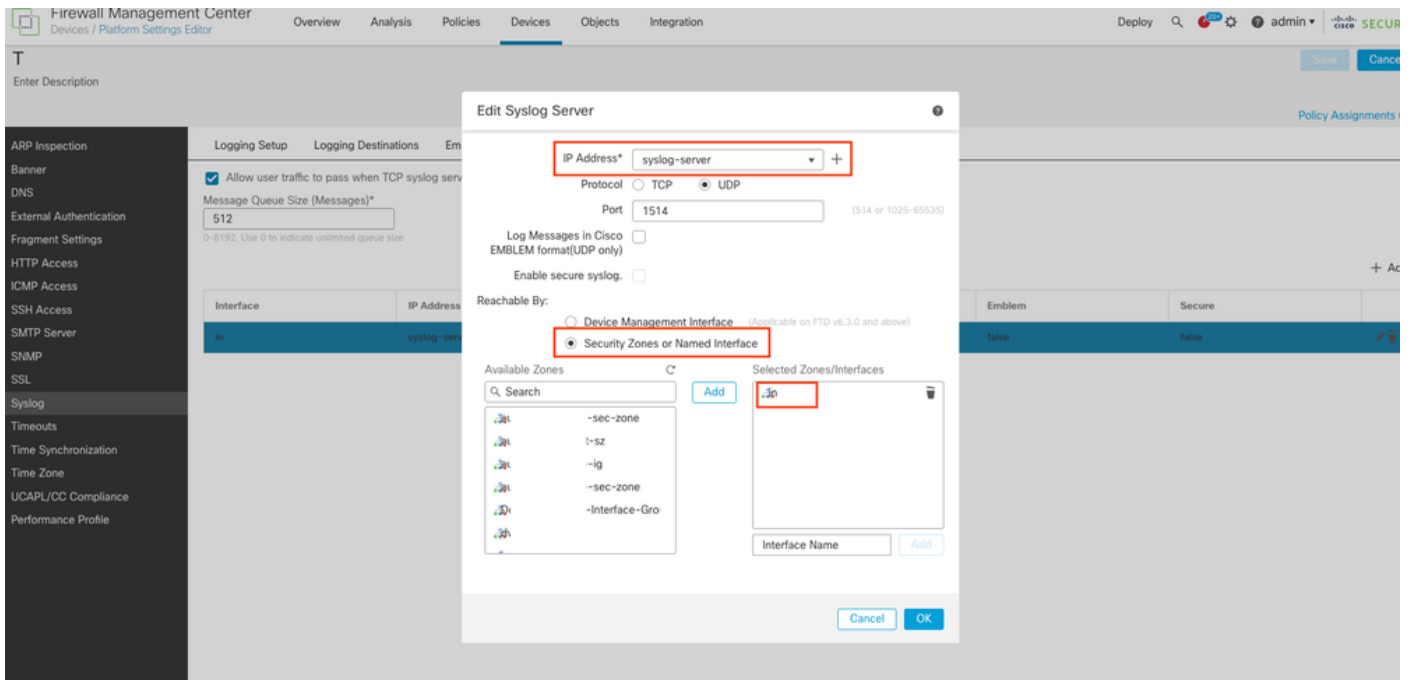
قفن لال خ نم اهل اسرل متي يتل Syslog لئ اسرل رصم هجاوك قرادلل ىل لوصولا هجاو مادختساب طقف رمال اذه حمسي ال
ربع و قفنل لمك SSL VPN و VPN ليمع مادختس دنع Ping و SSH ربع تانايبل هجاوب لاصلتال اب اضي نكل و VPN،
عقوم ىل عقوم نم IPsec قفن



طقف هجاو قرادلل لوصولا هجاو ديدحت كنكمي: عظام

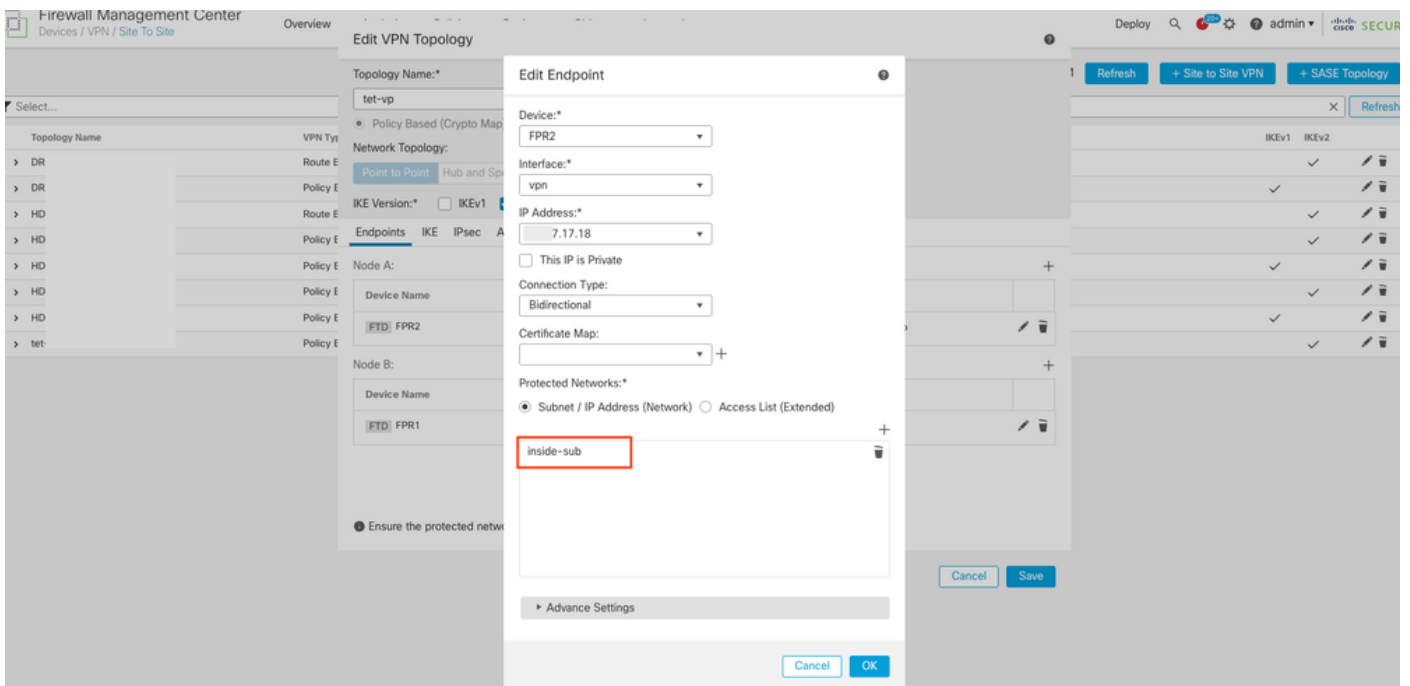
نيوكتل

قطانم ديدحت نم دكأت FTD ل ساسال ماظنل تاداع > هجال نمض syslog نيوكتب مق 1.
هجاو رتخاو syslog مداخ نيوكت اناثا هجال قرادل هجاو نم الدب قامسمال هجاو راخ و نامال
syslog رورم كرح رصم ديدحتل قرادلل لوصولا



Syslog مداخل نيوكت

2. هاهن ةطقنل ةي محمل تاكلشل نمض ةرادإلإ لوصول ةهجاو ةكبش ةفاضل نم دكأت 2. (ةدقع > VPN ططخم > عقوم لىا عقوم > زهجالأ تحت).



ةي محمل تاكلشل نيوكت

3. نيوكت VPN تاكلش و لوصول-ةرادإلإ ةهجاو ةكبش ني ب ةي وهلل NAT نيوكت نم دكأت 3. مسق نمض ةهجاو ةهجاو ل راسم ل شحب ذيفنت راخي ديدحت بجي. (VPN رورم ةكرحل NAT عئاش NAT ةدعاق نم مدقتم).

نيوكت في ةدحمل ةهجاو لال خ نم تانايل ل رورم ةكرحل FTD ل سري، راسم ل نع شحب نودب. هيجوتل لودج هلقوي ام نع رظنل لضغب nat.

Rules													
Filter by Device Filter Rules													
1 Rule Selected Select Bulk Action													
	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
NAT Rules Before													
☒	1	↔	Static	in	out	inside-sub	syslog_server_subnet		inside-sub	syslog_server_subnet		Do not use route-lookup no-proxy-arp	
Auto NAT Rules													
NAT Rules After													

nat ةي وه ليكشت

4. وي رانيسال اذه ي (ف) <interface name> management-access ني وكت نآل كنكمي . FlexConfig نئاك > نئالك ايراد > تانئالك تحت (management-access inside).

ني وكت لارشن وفدهتسم ل زاوجل FlexConfig جهن يلع اهنيني عتب مق

AAA Server

Access List

Address Pools

Application Filters

AS Path

BFD Template

Cipher Suite List

Community List

DHCP IPv6 Pool

Distinguished Name

DNS Server Group

External Attributes

File List

FlexConfig

FlexConfig Object

Text Object

Geolocation

Interface

Key Chain

Network

PKI

Policy List

Port

Prefix List

Route Map

Security Intelligence

Sinkhole

FlexConfig Object

FlexConfig Object in

Name

Name

Description

Description

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert

Deployment: Everytime

Type: Append

management-access inside

Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Cancel Save

FlexConfig ني وكت

ةحصل نم ققحتل

ةرادال ال لوصول ني وكت

<#root>

firepower#

show run | in management-access

management-access inside

Syslog: ني وكت

<#root>

firepower#

show run logging

logging enable
logging timestamp
logging trap debugging
logging FMC MANAGER_VPN_EVENT_LIST

logging host inside 192.168.17.17 17/1514

logging debug-trace persistent
logging permit-hostdown
logging class vpn trap debugging

VPN: قفن ربع Syslog رورم ةكرح لاسرا متي

<#root>

FTD 2:

firepower#

show conn

36 in use, 46 most used

Inspect Snort:

preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP vpn 192.168.17.17:1514 inside 10.17.17.18:514, idle 0:00:02, bytes 35898507, flags -

FTD 1:

firepower#

show conn

6 in use, 9 most used

Inspect Snort:

preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP server 192.168.17.17:1514 vpn 10.17.17.18:514, idle 0:00:00, bytes 62309790, flags -

firepower#

show crypto ipsec sa

interface: vpn

Crypto map tag: CSM_vpn_map, seq num: 1, local addr: 17.xx.xx.18

access-list CSM_IPSEC_ACL_2 extended permit ip 10.17.17.0 255.255.255.0 192.168.17.0 255.255.255.0
Protected vrf (ivrf):

local ident (addr/mask/prot/port): (10.17.17.0/255.255.255.0/0/0)

-----> Inside interface subnet

remote ident (addr/mask/prot/port): (192.168.17.0/255.255.255.0/0/0)

-----> Syslog server subnet

current_peer: 17.xx.xx.17

#pkts encaps: 309957, #pkts encrypt: 309957, #pkts digest: 309957

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 309957, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#TFC rcvd: 0, #TFC sent: 0

#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0

#send errors: 0, #recv errors: 0

قُلُوص تاذ تاملول عم

- [FMC ربح FTD ىلع ليجس تللا نيوك ت](#)
- [FMC قطس اوب قرا دملال FTD ىلع VPN ةكبش ىلالا عقوم لال نيوك ت](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا