

# قفن رباعي FTD ل Syslog تانايي جوانين وكت VPN

## تايي وتحمل

[قمدقمل](#)

[قيس اس الاتابل طتملا](#)

[تابل طتملا](#)

[قمدخت سملاتانوكملا](#)

[قيس اس اتمامولعم](#)

[يطي طخت لامس دلا](#)

[نيوكتل](#)

[فحصلانم قفتحتل](#)

[قلص تاذ اتمامولعم](#)

## قمدقمل

قفن رباعي لسرى syslog ل ردمصمك نراق تايي طمعم Cisco FTD لکشى نا فيك ققيشو اذه فصي.

## قيس اس الاتابل طتملا

[تابل طتملا](#)

هييلاتلا عييض او ملاب فقرعم كييدل نوكت نا ب Cisco يصوص:

- Cisco Secure Firewall Threat Defense (FTD)
- Syslog
- Cisco FMC (نـمـ) نـمـ الـيـامـحـلـ رـادـجـ قـرـادـ زـكـرـمـ
- قمدخت سملاتانوكملا

غـيـصـ زـاهـجـوـ ذـيـحـمـرـبـ اـذـهـ ىـلـعـ فـقـيـشـوـ اـذـهـ يـفـ قـهـولـعـمـلـاـ نـسـسـاـ

- Cisco FTD، 7.3.1
- Cisco FMC، 7.3.1

اـذـهـ ئـاشـنـاـ هـتـ بـتـاسـسـؤـمـ وـأـتـاعـوـمـجـمـ وـأـنـيـدرـفـ نـيـمـدـخـتـسـمـ يـأـبـ قـطـبـتـرـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ اـهـيـلـ إـلـاـ IPـ نـيـوـانـعـوـ تـاـكـبـشـلـاـ نـوـكـتـ الـ:ـ يـقـيلـوـسـمـلـاـ ئـالـاـ

هيـيلـمـعـمـ ئـيـيـبـ يـفـ مـادـخـتـسـلـاـ اـذـهـ يـفـ قـدـحـوـمـلـاـ قـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ قـدـراـوـلـاـ تـاـمـوـلـعـلـاـ ئـاشـنـاـ هـتـ

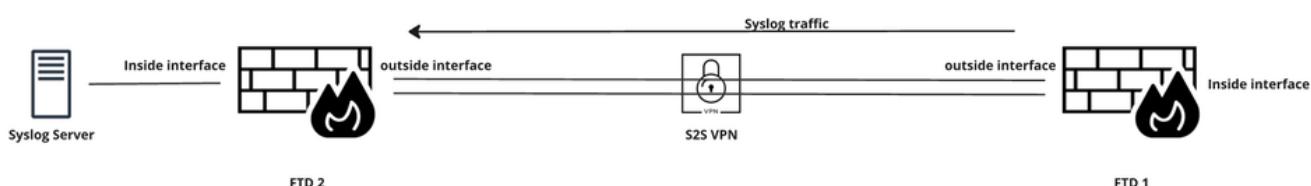
نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ قـمـدـخـتـسـمـلـاـ ذـيـحـمـجـ تـأـدـبـ بـفـصـاخـ ئـيـيـبـ يـفـ قـدـحـوـمـلـاـ قـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ قـدـراـوـلـاـ تـاـمـوـلـعـلـاـ ئـاشـنـاـ هـتـ رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ،ـ لـيـغـشـتـلـاـ دـيـقـ لـكـتـكـبـشـ تـنـاـكـ اـذـهـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ.

## قيس اس اتمامولعم

قـفـنـ ربـاعـيـ لـسـرـىـ syslogـ لـ رـدـصـمـكـ FTDـ نـمـ نـراقـ تـايـيـ طـعـمـلـاـ نـمـ دـحـ اوـ لـمـعـتـسـيـ نـاـ لـحـ فـقـيـشـوـ اـذـهـ فـصـيـ

ديـعـبـ عـقـومـ يـفـ دـجـاوـتـيـ نـوـكـيـ نـاـ لـدانـ.

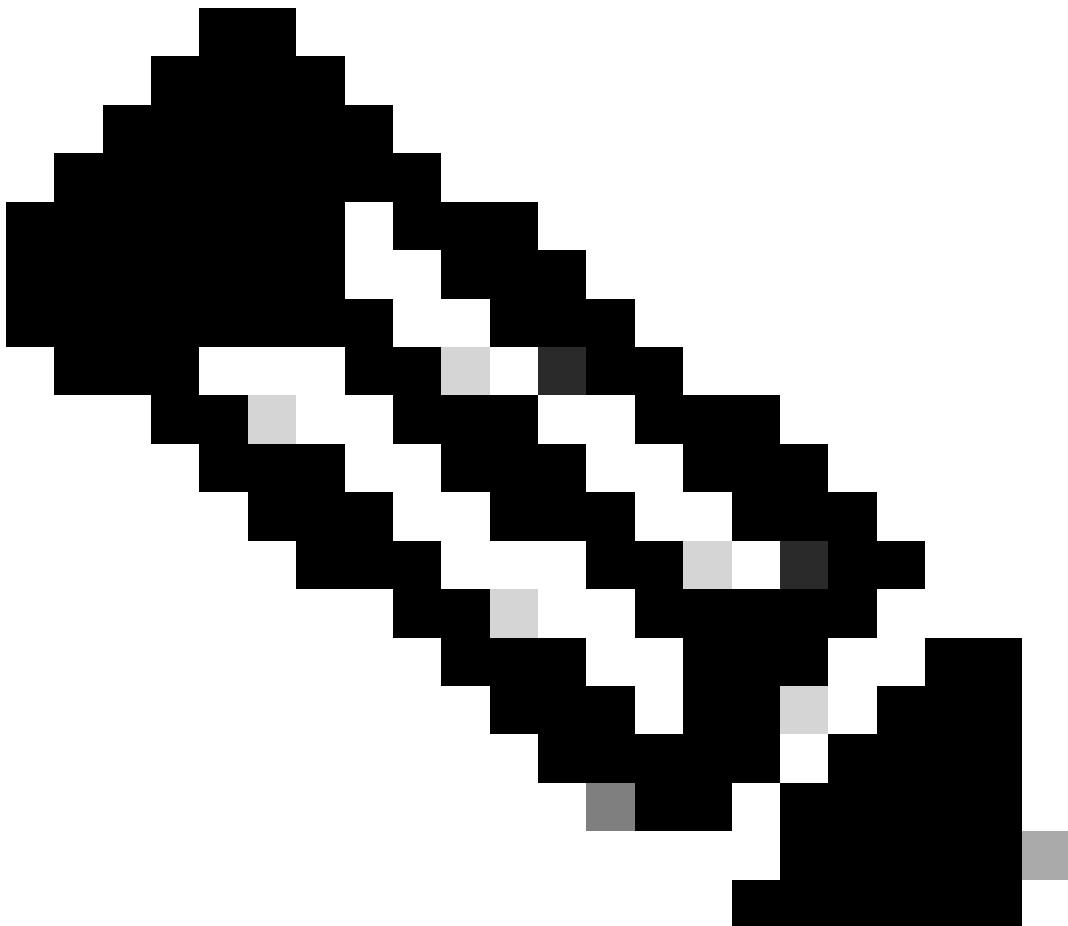
[يـطـيـ طـخـتـلـاـ مـسـرـلـاـ](#)



كـبـشـلـلـ يـطـيـ طـخـتـلـاـ مـسـرـلـاـ

رمألا قييىبىطت ئىنكمىي ،قىفنلىا رباع اهلاسرا مەتىي يىتلارو مرئىخ ردىصمىم اهنم مەتىي يىتلارا ۋەچاولى دىدجىتلىك management-access Flex Config.

قىفنلىا لالخ نم اهلاسرا مەتىي يىتلار Syslog لىئاسىرلى ردىصم ۋەچاولى ئىلە لۇصۇلما ۋەچاولى مادختىسىنى طقىف رمألا اذە حەمسىي ال VPN و اقىفنلىا لەمەك VPN و SSL VPN لىيەم مادختىسى دىن دىن Ping و SSH ربعتانايىبىلارا ۋەچاولى اپلىرىنىڭلۇ ،اضىيأننىڭلۇ ،عقوم ئىلە عقوم نم IPsec قىفنلىا



طقىف ئەدھار و ئەرادي-لۇصۇ و ئەھجاو دىدجىت ئىنكمىي : ئەظحالىم.

## نېوكتلى

قطانىم دىدجىت نم دىكأت FTD ل يىس اسألا ماظنلى تادادعى > ۋەچاولى نەمەن syslog نېوكتلى مۇق. ئەھجاو رەتىخاولى syslog مەداخ نېوكت ئانىڭ ئەزىز ۋەچاولى ئەرادي ۋەچاولى ئامسىملا ۋەچاولى رايىخ و ئەنام ئەلارو مرئىخ ردىصم syslog دىدجىتلى ئەرادي-لۇصۇلارا.

The screenshot shows the 'Edit Syslog Server' dialog box. The 'IP Address\*' field is set to 'syslog-server'. The 'Protocol' section has 'TCP' as the selected option. The 'Port' field is set to '1514'. Under 'Reachable By:', the 'Security Zones or Named Interface' radio button is selected. In the 'Available Zones' list, there are several entries: '-sec-zone', 'l-sz', '-ig', '-sec-zone', and '-Interface-Gro'. The 'Selected Zones/Interfaces' list contains a single entry: 'lo'. The 'OK' button at the bottom right is highlighted.

## مداخنیوکت Syslog

ةياهن ةطقنل ةيمحملا تاكبشلا نمض ۀرادإا ىلإ لوصولا ٰههجاو ٰكبش ٰفاضا نم دكأت. 2. ٰدقع > VPN ططخم > عقوم ىلإ عقوم > ٰزهجأا تتح).

Topology Name:  
tet-vp

Device:  
FPR2

Interface:  
vpn

IP Address:  
7.17.18

This IP is Private

Connection Type:  
Bidirectional

Certificate Map:  
[empty dropdown]

Protected Networks:  
 Subnet / IP Address (Network)  Access List (Extended)

inside-sub

Cancel Save

ةيەمەنە تاکبىشلانى يوقت

نيوكت يف ٽددحملا ٽهجاولالا لالخ نم تانايبلارورم ٽكرح FTD لسري ،راسملانع ثحب نودب nat، هيجوتلاللودج هلوقي ام نع رظنلاضغب.

Rules												
Filter by Device Filter Rules												
1 Rule Selected	Select Bulk Action											
Original Packet Translated Packet												
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
<input checked="" type="checkbox"/>	1	Static	in	out	inside-sub	syslog_server_subnet	Inside-sub	syslog_server_subnet	route-lookup no-proxy-arp			
<b>NAT Rules Before</b>												
<b>Auto NAT Rules</b>												
<b>NAT Rules After</b>												

نويوكت لىكشت nat

ویرانیسلا اذه يف) management-access <interface name> نويوكت نآلا كنكمي . management-access inside ( تانىاكل ئارادا > نئاكلا تحت FlexConfig .

نويوكتلا رشن و فدهتسمل زاهجلى FlexConfig جىل عاھن يي عتب مق.

The screenshot shows the 'Objects / Object Management' section of the Juniper Network Manager. On the left, there's a sidebar with various network objects like AAA Server, Access List, Address Pools, etc. The 'FlexConfig Object' under 'FlexConfig' is selected. A modal window titled 'Add FlexConfig Object' is open, showing the configuration for the 'management\_access\_object'. The 'Name' field is set to 'management\_access\_object' and the 'Description' field is 'For Syslog'. The 'Deployment' dropdown is set to 'Everytime' and the 'Type' dropdown is set to 'Append'. Below these fields, there's a rich text area containing the configuration: 'management-access inside'. At the bottom of the modal, there are 'Cancel' and 'Save' buttons. To the right of the modal, a list of other FlexConfig objects is visible.

نويوكت FlexConfig

## ةحصـلـا نـم قـقـحتـلـا

ةرـادـإـلـا إـلـا لـوـصـولـا نـيـوـكـتـ:

```
<#root>
firepower#
show run | in management-access

management-access inside
```

نـيـوـكـتـ Syslog:

```

<#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

```

ي م ت ا س ا ل ا ح ك ر ة ف ن ر ب ع Syslog R o r m V P N :

```

<#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
```

## قلىص تاذت امولع

- [ربع FTD ىل لىچ سىتلانى يوكىت](#)
- [فەطس اوپ قرادىملا FTD ىل لىچ سىتلانى يوكىت](#)

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).