

FMC في NetFlow نيوكت

تايوت حمل

[قمدم](#)

[ةيساسأل تابلطم](#)

[تابلطم](#)

[ةمدختسم تانوكم](#)

[ةيساسأ تامولعم](#)

[NetFlow في عمجم ةفاض](#)

[NetFlow ل تانايبل رورم ةكرح ةئف ةفاض](#)

[اهالص او عاخذأل فاشكتسا](#)

[ةلص تاذ تامولعم](#)

ةمدقم

يذل Cisco نم نمأل ةيامل رادج ةرادك زكرم في NetFlow نيوكت ةيفي ك دن تسم ل اذه فص ي
ثدأل وأ 7.4 رادصل ل لغشي.

ةيساسأل تابلطم

تابلطم

ةيلال عيضاوم ل اب ةفرعم كيدل نوكت نأ Cisco ي صوت:

- Cisco نم (FMC) نمأل ةيامل رادج ةرادك زكرم
- Cisco نم (FTD) ةيامل رادج ديدهت نع نمأل عافدل
- NetFlow لوكوتورب

ةمدختسم تانوكم

ةيلال ةيدامل تانوكم ل او جم اربل تارادصل ل دن تسم ل اذه في ةدراول تامولعمل دن تست:

- v7.4.1 ليغش تب VMWare ل نمأل ةيامل رادج ةرادك زكرم موقوي
- v7.4.1 نمأل ةيامل رادج ليغش

ةصاخ ةي لمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجالا عيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكأتف ، ليغشتلا ديقتك تكبش

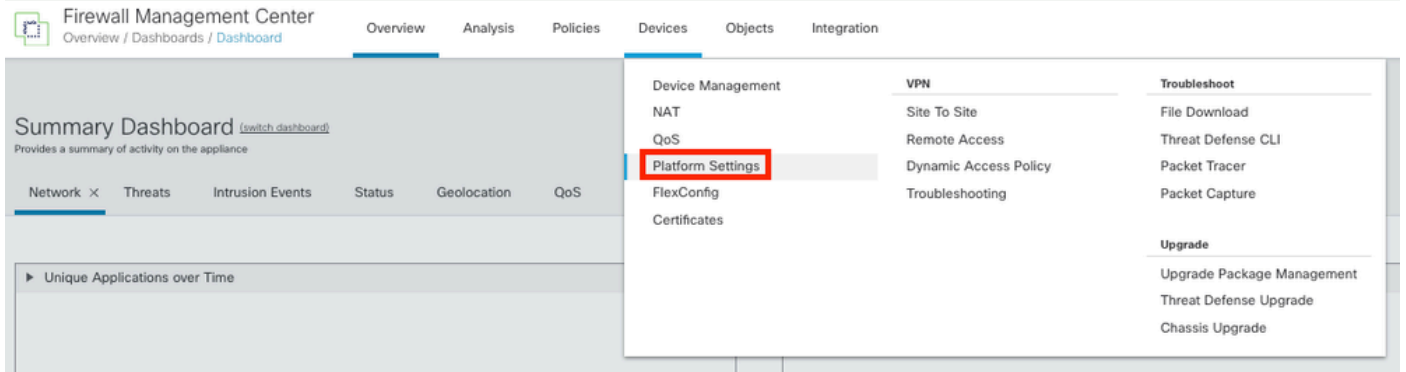
ةيساسا تامولعمل

دنتسمل اذهل ةصاخلا تابلطتملا نمضتت

- لىل رادصا و 7.4 رادصا ال Cisco Secure Firewall Threat Defense
- لىل رادصا و 7.4 رادصا ال لمعي يذلا Cisco نم نم ال ةيامل رادج ةرادك زكرم

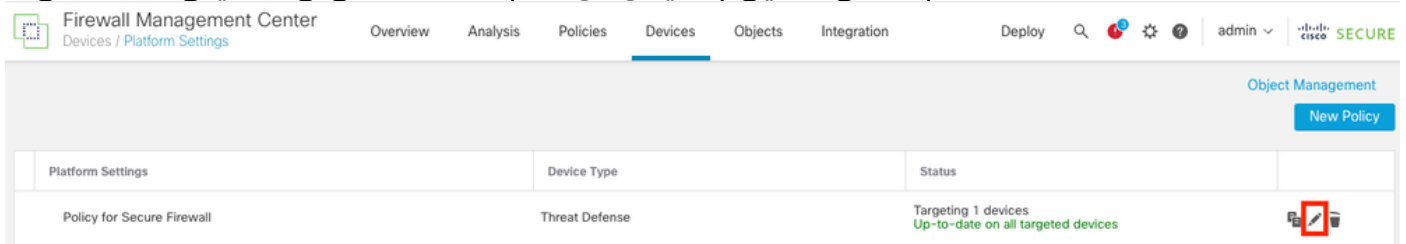
NetFlow يف عمجم ةفاضل

يساسالا ماظنلا تاداعل > ةزهجالا يلى لقتنا 1. ةوطخل



يساسالا ماظنلا تاداعل يلى لوصول

ةبقارملا زاهجل ني عمل يساسالا ماظنلا تاداعل چهن ريرحت 2. ةوطخل



چهنلا رادصا

NetFlow رتخأ 3. ةوطخل



Policy for Secure Firewall

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Interface

Inspect Enabled

NetFlow تاداع | لى لوصول

NetFlow تاناى ب ريدصت نيكمتل قفدتلا ريدصت ليوحت نيكمت 4. ةوطخال

Policy for Secure Firewall

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Enable Flow Export

Active Refresh Interval (1-60)

minutes

Delay Flow Create (1-180)

seconds

Template Timeout Rate (1-3600)

minutes

Collector

Traffic Class

NetFlow نيكمت

عجم ةفاضل قوف رقنا 5 ةوطخلا

Policy Assignments (1)

Add Collector

Add Traffic Class

ةفاضل عجم

عمجم ىل ع UDP ذفنمو، NetFlow شادحاً عمجم ب صاخلا عمجم ل فيضم ل IP نئاك رتخاً 6. ةوطخل ل لوصول ب جي يتل ةهجال ةومجم رتخاو، هيل NetFlow مزح لاسرا ب جي يذلا تانايل ل قوف روناو، اهلا ل نم تانايل عمجم:

Add Collector

Host
Netflow_Collector

Port (1-65535)
2055

Available Interface Groups (1)
Netflow_Export

Selected Interface Groups (0)

Add

Select at least one interface group.

Cancel OK

تانايل عمجم تاداع

NetFlow ل تانايل رورم ةكرح ةئف ةفاضل

تانايل رورم ةكرح ةئف ةفاضل قوف رونا 1. ةوطخل

Enable Flow Export

Active Refresh Interval (1-60) minutes
1

Delay Flow Create (1-180) seconds
30

Template Timeout Rate (1-3600) minutes
30

Host	Interface Groups	Port
Netflow_Collector	Netflow_Export	2055

Add Collector

Add Traffic Class

No traffic class records.

رورم ل ةكرح ةئف ةفاضل

ةمئاق، NetFlow شادحاً قباطت نأ ب جي يتل رورم ل ةكرح ةئف ل مسالا لقح لخدأ 2. ةوطخل يتل رورم ل ةكرح قباطت نأ ب جي يتل رورم ل ةكرح ةئف ل ديحتل (ACL) لوصول ل في م كحتل يتل ةفلتخم ل NetFlow شادحاً ب صاخلا راي تخال تاناخ دح، NetFlow شادحاً ل اهطاق تال متي

قفاوم قوف رقناو عيمجتلا تاودأ ىلا اهلا سارا ديرت:

Add Traffic Class



Name
Netflow_class

Type
 Access List Default

Access List Object
Netflow_ACL

Event Types

Collector	All	Created	Denied	Updated	Torn Down
Netflow_Collector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel OK

تانايبلا رورم ةكرف ةئف تادادع

اهحال صاوا عا طخال فاشكتسا

رم اوألا رطس ةهجاو نم نيوكتلا نم ققحتلا كنكمي 1. ةوطخلا

معدب ةصاخلا (CLI) رم اوألا رطس ةهجاو ىلا لخدأ، FTD ب ةصاخلا (CLI) رم اوألا رطس ةهجاو نم 1.1. ماطنلا:

```
>system support diagnostic-cli
```

1.2: ةسايسلا ةطيرخ نيوكت صرحف

```
<#root>
```

```
firepower#show running-config policy-map  
!  
policy-map type inspect dns preset_dns_map  
parameters  
message-length maximum client auto
```

```
message-length maximum 512
no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class_snmp
inspect snmp

class Netflow_class_Netflow_ACL
```

```
flow-export event-type all destination 192.168.31.1
```

```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. ري دصت-قفدت ني وكت نم ققحت:

```
<#root>
```

```
firepower#show running-config flow-export
```

```
flow-export destination Inside 192.168.31.1 2055
```

هه اوله عومجم يف اهنيوكت مت يتلله هه اوله مسا وه "Inside"، لاثملا اذه يف: عهظالم
لله NetFlow_Export م ست يتلله

(ACL) لوصول يف مكحتله عمئاقل لوصول تارم ددع نم ققحتله 2. عوطخله

<#root>

```
firepower#show access-list Netflow_ACL
access-list Netflow_ACL; 1 elements; name hash: 0xbad5d4bf
access-list Netflow_ACL line 1 extended permit ip object Inside_Network any (
hitcnt=44
) 0xb704fc5b
access-list Netflow_ACL line 1 extended permit ip 10.1.2.0 255.255.255.0 any (
hitcnt=44
) 0xb704fc5b
```


NetFlow تادادع نم ققحتلا 3. ةوطخلا

<#root>

firepower#show flow-export counters

destination: Inside 192.168.31.1 2055

Statistics:

packets sent	101
--------------	-----

Errors:

block allocation failure	0
--------------------------	---

invalid interface	0
-------------------	---

template send failure	0
-----------------------	---

no route to collector	0
-----------------------	---

failed to get lock on block	0
-----------------------------	---

source port allocation failure	0
--------------------------------	---

ةلص تاذا تامولعم

- [7.4 رادصلا، Cisco نم نم آلا ةي امحلا رادج ةرادا زكرم زاغ نيوكت ليلد](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
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 دن ت س م ل ا