

# ةزهجأ ىلع NAP تاسايس ةنراقم ةيفيك FirePOWER

## تاوت حمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[NAP نيوكت نم ققحتلا](#)

## ةمدقملا

FirePOWER (FMC) ةرادا زكرم اهردي يتلا FirePOWER ةزهجأ (NAP) ةفلتخملا ةكبشلا ليلحت تاسايس ةنراقم ةيفيك دننستسما اذه حضوي

## ةيساسألا تابلطتملا

## تابلطتملا

ةيلالاتلا عيضاوملاب ةفرعم كيذل نوكت نأ Cisco ي صوت

- ردصملا حوتفم ريخشلا ةفرعم
- Firepower (FMC) ةرادا زكرم
- Firepower Threat Defense (FTD)

## ةمدختسملا تانوكملا

ةيلالاتلا ةيداملا تانوكملا وجماربال تارادصا ىلا دننستسما اذه في ةدراولا تامولعملا دننستس

- Firepower تاصنم عيجم ىلع ةلاقملا هذه قبطنت
- نم 6.4.0 رادصا لا لغشي يذلا Cisco نم FirePOWER (FTD) ديدهت دض عافدلا جمانرب  
جمانربلا
- Firepower Management Center Virtual (FMC) يذلا 6.4.0 رادصا لا لغشي يذلا

## ةيساسأ تامولعم

ىلا ةكبشلا كرحم جاتحي، ءارجا اذهب مايق لل. ةكبشلا مزح في اهنم و لا لغتسالا تايلمع ىلع روثلل طمنلا ةقبطام تاينقت ريخشلا مدختسي  
لحارملا ب رمت نأ نكمي وينطول للمعلا جمانرب ةدعاسمب ةيلمعلا هذه متتو. ةنراقملا هذه ءارجا اهلاخ نم نكمي ةقيرطب اهداع لمثل ةكبش مزح  
ةيلالاتلا ثالثل:

- زيمرتلا ك ف
- عيبطت
- قسبم زيهدت

في رمتسي م، ىلوالا ثالثل TCP/IP تاقبطل لاخ نم مزحلا زيمرت ك فب الوأ ماظنلا موقبي: لحارم في مزحل ةكبشلا ليلحت ةسايس ءعلا  
لوكتوربال دودش فاشتكاو ةقسسما ءعلا و اعيا عيبطتلا.

ننستسي ئر نينتي فظو ةقسسما تاجلا عملا رفوت:

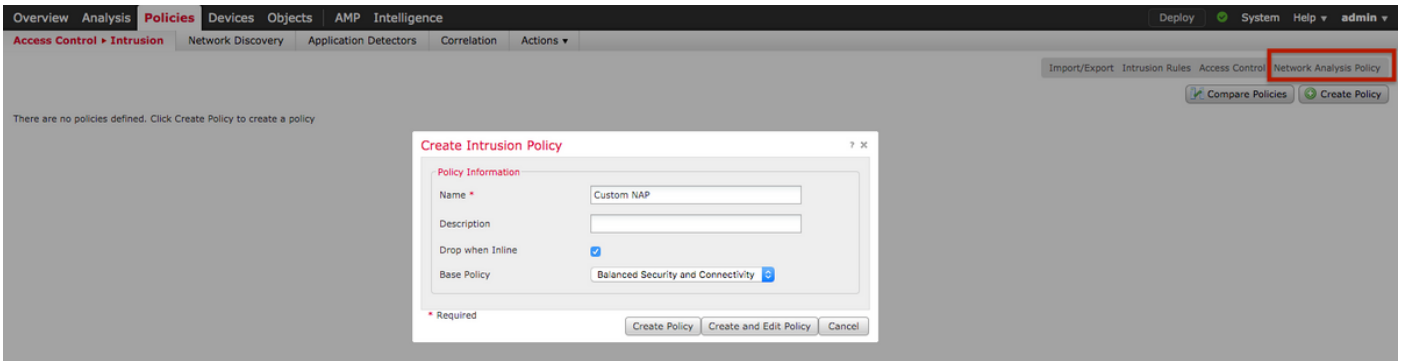
- شيفت التال نم ديزمل رورملا ةكرح عيبطت
- لوكوتوربولل ةذاشل التالاجلا ىلع فرعتلا

فشكللا ءارجال جلا عملل قعباس قنيعم تارايخ ماحتقالا قساييس دعاوق ضعب ببلطنتت: **ةظحالم**

لوصحلل <https://www.snort.org/> عقوملا ةرايز يجري ،ردصملا جوتفم Snort جم انرب لوج تامولعم ىلع لوصحلل

## NAP نيوكت نم ققحتلا

(FMC) ةيساسالا ةرادالا يف مكحتلا ةدحوتاسايس ىلا لقتنا ،اهريحت وأ ةيماحلا ةوقب ةصاخلا (NAP) مكحتلا ىوتسم ةيماح تاسايس ءاشنال ةروصولا يف حضورم وه امك ،نم ائلا ىولعل انكرلا يف ةكبشلل ليحت ةسايس رايج قوف رقتنا مث ،لفطتلا > لوصولا يف مكحتلا



Network Analysis Policy	Inline Mode	Status	Last Modified
Test1	Yes	No access control policies use this policy. Policy not applied on any devices	2019-12-30 02:13:49 Modified by "admin"
Test2*	Yes	You are currently editing this policy. No access control policies use this policy. Policy not applied on any devices	2019-12-30 02:14:24 Modified by "admin"

(NAP) (ACP)

> (ACP) . .

ACP :

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions ▼

## Test

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#)

Rules Security Intelligence HTTP Responses Logging **Advanced**

### General Settings

Maximum URL characters to store in connection events 1024

Allow an Interactive Block to bypass blocking for (seconds) 600

Retry URL cache miss lookup Yes

Inspect t

#### Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined [Balanced Security and Connectivity](#)

Intrusion Policy Variable Set [Default-Set](#)

Network Analysis Rules [No Custom Rules](#) [Network Analysis Policy List](#)

Default Network Analysis Policy [Balanced Security and Connectivity](#)

[Revert to Defaults](#) [OK](#) [Cancel](#)

### Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined [Balanced Security and Connectivity](#)

Intrusion Policy Variable Set [Default Set](#)

Default Network Analysis Policy [Balanced Security and Connectivity](#)

عظالم : ةكبشلا ليلحت .

### ةكبشلا ليلحت ةسايس ةنراقم (NAP)

يف ةزيملا هذه دعاست نأ نكميو ، اهؤارج مت يتلا تاريخي غتلاب ةينطول لمعلل جمارب ةسايس ةنراقم نكميو جمارب ةنراقم ريراقت دادع اضيأ نكمي ، كلذلى ةفاضلابو . اهحاصل او اهئاطخ اف اشكست او تالكشملا ديدحت هسفن تقولا يف اهريصتو ةينطول لمعلل .

ىلعأ يف ةكبشلا ليلحت جهن رايخ قوف رقنا ، كلذ دعب . لفطتلا > لوصول يف مكحتلا > ةسايسلا ىلى لقتنا نميال يولعل بانجال يف ةسايسلا ةنراقم بيوبتلا ةمالع ةدهاشم كنكمي NAP ةسايس ةحفص تحت . نيمللا ةروصولا يف حضورم وه امك :

Deploy ✔ System Help ▼ admin ▼

Object Management Access Control Intrusion

Compare Policies + Create Policy

Last Modified	
2019-12-30 01:58:08 Modified by "admin"	
2019-12-30 01:58:59 Modified by "admin"	

ننريغتم في فكبشلال ليلحت جهن ةنراقم رفوتت

- ةنطوال لمعال ططخل نيتفلتخم نيتسايس نيب
- ةنطوال فيكتال ططخة سايس سفنل نيتفلتخم نيحيقنت نيب

### Select Comparison

Compare Against

✔ Other Policy
Other Revision

Policy A

NAP1one (2019-11-27 14:22:32 by admin)
▼

Policy B

NAP1one (2019-11-27 14:22:32 by admin)
▼

OK
Cancel

ريدصت نكممي امك، ةنطوال لمعال ططخل نيتددخم نيتسايس نيب رطسب رطاس ةنراقم ةنراقم ال ةذفان رفوت ةروصلال في حضورم وه امك، نيميالال عا في ةنراقم ريرقت بيوبتال ةمالع نم ريرقتك جهنلال سفن

Back Comparison Report New Comparison

Previous Next (Difference 1 of 114)

Test1 (2019-12-30 02:13:49 by admin)	Test2 (2019-12-30 02:14:24 by admin)
<b>Policy Information</b>	
Name: Test1	Name: Test2
Modified: 2019-12-30 02:13:49 by admin	Modified: 2019-12-30 02:14:24 by admin
Base Policy: Connectivity Over Security	Base Policy: Maximum Detection
<b>Settings</b>	
<b>Checksum Verification</b>	
ICMP Checksums: Enabled	ICMP Checksums: Disabled
IP Checksums: Enabled	IP Checksums: Drop and Generate Events
TCP Checksums: Enabled	TCP Checksums: Drop and Generate Events
UDP Checksums: Enabled	UDP Checksums: Disabled
<b>DCE/RPC Configuration</b>	
<b>Servers</b>	
default	
SMB Maximum AndX Chain: 3	SMB Maximum AndX Chain: 5
RPC over HTTP Server Auto-Detect Ports: Disabled	RPC over HTTP Server Auto-Detect Ports: 1024-65535
TCP Auto-Detect Ports: Disabled	TCP Auto-Detect Ports: 1024-65535
UDP Auto-Detect Ports: Disabled	UDP Auto-Detect Ports: 1024-65535
SMB File Inspection Depth: 16384	SMB File Inspection Depth:
<b>Packet Decoding</b>	
Detect Invalid IP Options: Disable	Detect Invalid IP Options: Enable
Detect Obsolete TCP Options: Disable	Detect Obsolete TCP Options: Enable
Detect Other TCP Options: Disable	Detect Other TCP Options: Enable
Detect Protocol Header Anomalies: Disable	Detect Protocol Header Anomalies: Enable
<b>DNS Configuration</b>	
Detect Obsolete DNS RR Types: No	Detect Obsolete DNS RR Types: Yes
Detect Experimental DNS RR Types: No	Detect Experimental DNS RR Types: Yes
<b>FTP and Telnet Configuration</b>	
<b>FTP Server</b>	
default	

امك ، بولطم الة عجارم ال فرعم ديحتل ة عجارم ال راىخ راىخ| نكمي ، اهسفن NAP ة سايس نم ني رادصا ني ب ة نراقم لل ة روصلا يف حضورم وه

## Select Comparison ? X

Compare Against: Other Revision

Policy: Test1 (2019-12-30 02:13:49 by admin)

Revision A: 2019-12-30 02:13:49 by admin

Revision B: 2019-12-30 01:58:08 by admin

OK
Cancel

Back

Previous Next (Difference 1 of 13)

Comparison Report New Comparison

Test1 (2019-12-30 02:13:49 by admin)	
<b>Policy Information</b>	
Modified	2019-12-30 02:13:49 by admin
Base Policy	Connectivity Over Security
<b>Settings</b>	
CSP Configuration Disabled	
DCE/RPC Configuration	
Servers	
default	
RPC over HTTP Server Auto-Detect Ports	Disabled
TCP Auto-Detect Ports	Disabled
UDP Auto-Detect Ports	Disabled
HTTP Configuration	
Servers	
default	
Ports	80, 443, 1220, 1741, 2301, 3
Server Flow Depth	300
SSL Configuration	
Ports	443, 465, 563, 636, 989, 992
TCP Stream Configuration	
Servers	
default	
Perform Stream Reassembly on Client Ports	21, 23, 25, 42, 53, 80, 135, 1
Perform Stream Reassembly on Client Services	CYS, DCE/RPC, DNS, , HTTP,
Perform Stream Reassembly on Both Ports	5000, 9800, 9111

Test1 (2019-12-30 01:58:08 by admin)	
<b>Policy Information</b>	
Modified	2019-12-30 01:58:08 by admin
Base Policy	Balanced Security and Connec
<b>Settings</b>	
DCE/RPC Configuration	
Servers	
default	
RPC over HTTP Server Auto-Detect Ports	1024-65535
TCP Auto-Detect Ports	1024-65535
UDP Auto-Detect Ports	1024-65535
HTTP Configuration	
Servers	
default	
Ports	80, 443, 1220, 1741, 2301, 2
Server Flow Depth	500
SSL Configuration	
Ports	443, 465, 563, 636, 989, 992
TCP Stream Configuration	
Servers	
default	
Perform Stream Reassembly on Client Ports	21, 23, 25, 42, 53, 135, 136,
Perform Stream Reassembly on Client Services	CYS, DCE/RPC, DNS, , IMAP,
Perform Stream Reassembly on Both Ports	80, 443, 465, 636, 992, 993,
Perform Stream Reassembly on Both Services	HTTP

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