

# Firepower تانايب راسم عاڤخأ فاشكتسأ ةماع ةرظن :اهحالصإو

## تايوتحمل

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تانايبل راسم ةيرامعم ةماع ةرظن](#)

[ASA \(SFR ةدحو\) FirePOWER تامدخل يساسأل ماظنلا عم](#)

[Virtual FTD و ASA500-X ةصنم يلغ Firepower ديدهت دض عافدلا](#)

[SSP تاصنم يلغ FTD](#)

[Firepower 9300 و 4100 ةزهجأ](#)

[Firepower 2100 ةزهجأ](#)

[اهحالصإو Firepower تانايب راسم عاڤخأ فاشكتسأل اهب يصوملا ةيلمعل](#)

[FTD ربع ةمزحلل يلغفل راسملا](#)

[تروشلا ةمزح راسم](#)

[مزحلل جورخل او لوخدلا](#)

[DAQ Firepower ةقبط](#)

[ةينمأل تارابختسالا](#)

[لوصولا يف مكحتلا ةسايس](#)

[SSL جهن](#)

[ةطشنلا ةقداصملا](#)

[ماحتقالا ةسايس](#)

[ةكبشلا ليحت ةسايس](#)

[ةلص تاذا تامولعم](#)

## ةمدقملا

ديدهت نع عافدلا زاهج ناك اذا ام يلغ ةعرب فبرعتلا يف ةدعاسملا وه ليلدلا اذه نم ضرغلل ببستت FirePOWER تامدخ عم (ASA) فيكتلل لباقلا نامأل زاهج وأ (FTD) ةيرانلا ةقاولا بةصاخلا (تانوكملا) نوكملا قيقيضت يف دعاست امك . ةكبشلا رورم ةكرح عم ةلكشم يف زكرم كارش لباق اعمج بجي يتلا تانايبل او اهي في قيقتحلتا بجي يتلا FirePOWER Cisco نم (TAC) ةينقتلا ةدعاسملا

اهحالصإو Firepower تانايب راسم عاڤخأ فاشكتسأ ةلسلس تالاقم عيمجب ةمئاق

ةمزحلا لخدم :اهحالصإو Firepower تانايب راسم عاڤخأ فاشكتسأ نم 1 ةلحرملا

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html>

DAQ ةقبط :اهحالصإو Firepower تانايب راسم عاڤخأ فاشكتسأ نم 2 ةلحرملا

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html>

نامأل اءكذ :اهحالصإو Firepower تانايب راسم عاڤخأ فاشكتسأ نم 3 ةلحرملا

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html>

في مكحتل ةسايس :اهالصل او Firepower تانايب راسم عاطخأ فاشكتسأ نم 4 ةلجرمل لوصول

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html>

SSL جهن :اهالصل او Firepower تانايب راسم عاطخأ فاشكتسأ نم 5 ةلجرمل

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html>

ةطشنل ةقداصلم :اهالصل او Firepower تانايب راسم عاطخأ فاشكتسأ نم 6 ةلجرمل

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html>

ماحتقالا جهن :اهالصل او Firepower تانايب راسم عاطخأ فاشكتسأ نم 7 ةلجرمل

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html>

ةكبشل ليلحت جهن :اهالصل او Firepower تانايب راسم عاطخأ فاشكتسأ نم 8 ةلجرمل

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html>

## ةيساسأل اابلطتمل

- ASA و FTD تاصلنم ل يساسأ مهف هيدل صخشلا نأ ةلاقملا هذه ضررتفت .
  - بولطم ريغ هنأ نم مغرلا يلع ،حتوفملا ردصلم ل سخش نع ةفرعملاب يصوي .
- ،تيتثلا ونيوكتلا ةلدا كلذ في امب ، FirePOWER قئاثوب ةلماك ةمئاق يلع لوصولل ،  
قئاثولل راسم [طاطخم](#) ةحفص ةرايز يجرى .

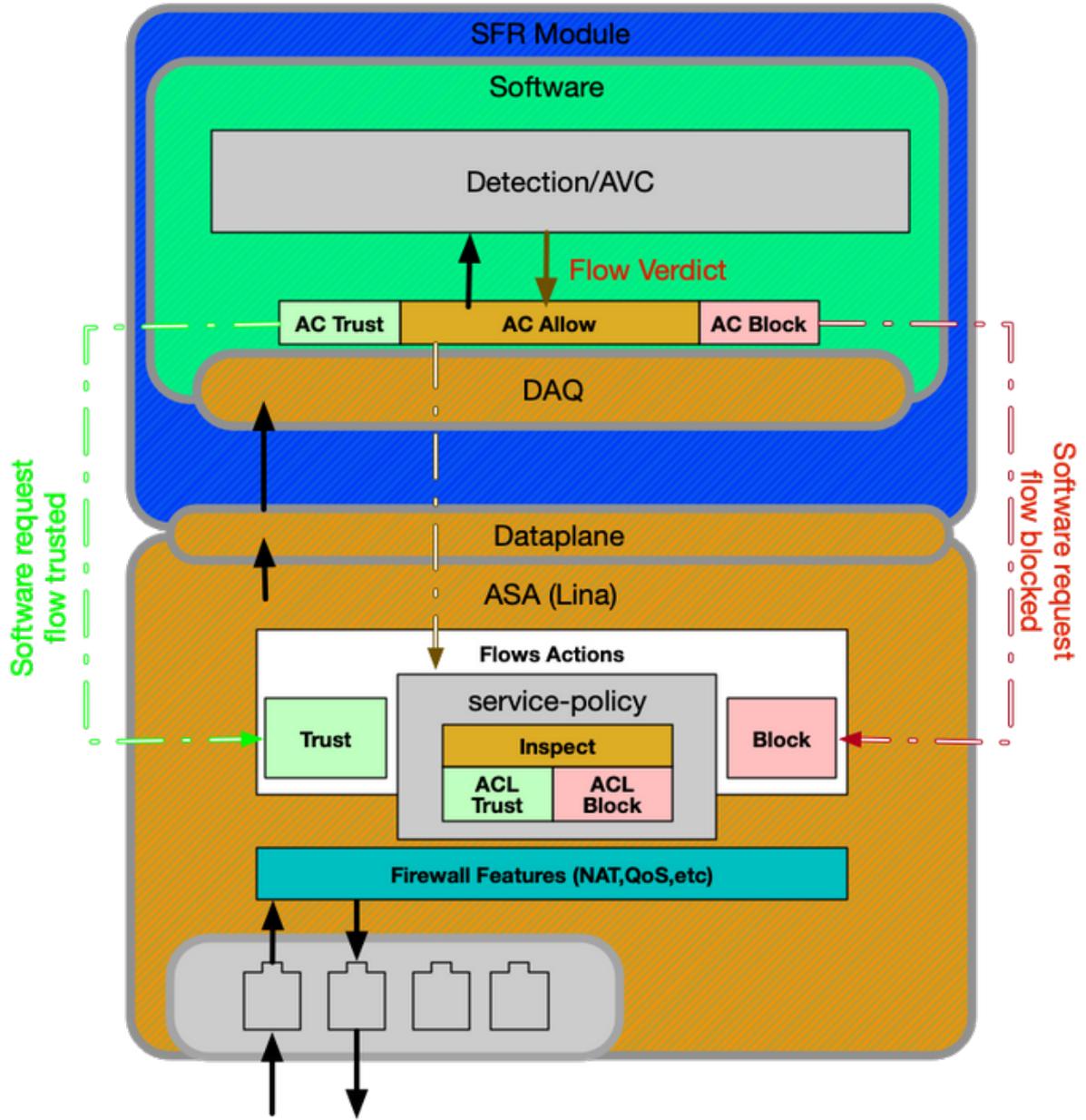
## تانايب راسم ل ةيرامعم ةرظن

عضوعم FirePOWER تاصلنم نم ديدعلل ةينبلا تانايب راسم لىلا يلاتلا مسقلا رظني زاهاك اذام ديدحت ةيفيك لىلا كلذ دعب لقتننس ،رابتعالا في ةيرامعمل ةسدنهل ال ما رورملا ةكرح قفدت عنم في FirePOWER .

الو ةميدقلا 8000 و 7000 Firepower ةلسلسلا ةزهجأ ةلاقملا هذه يطغت ال :**ةظالم** هذه فاشكتسأ لوح تامولعمل نم ديزمل (FTD ريغ) NGIPS يرهظلا يساسأل ماظنلا انب ةصاخلا [TechNotes](#) ةحفص ةرايز يجرى ،اهالصل او ةمظنألا .

## ASA عم (SFR ةدحو) FirePOWER تامدخل يساسأل ماظنلا عم

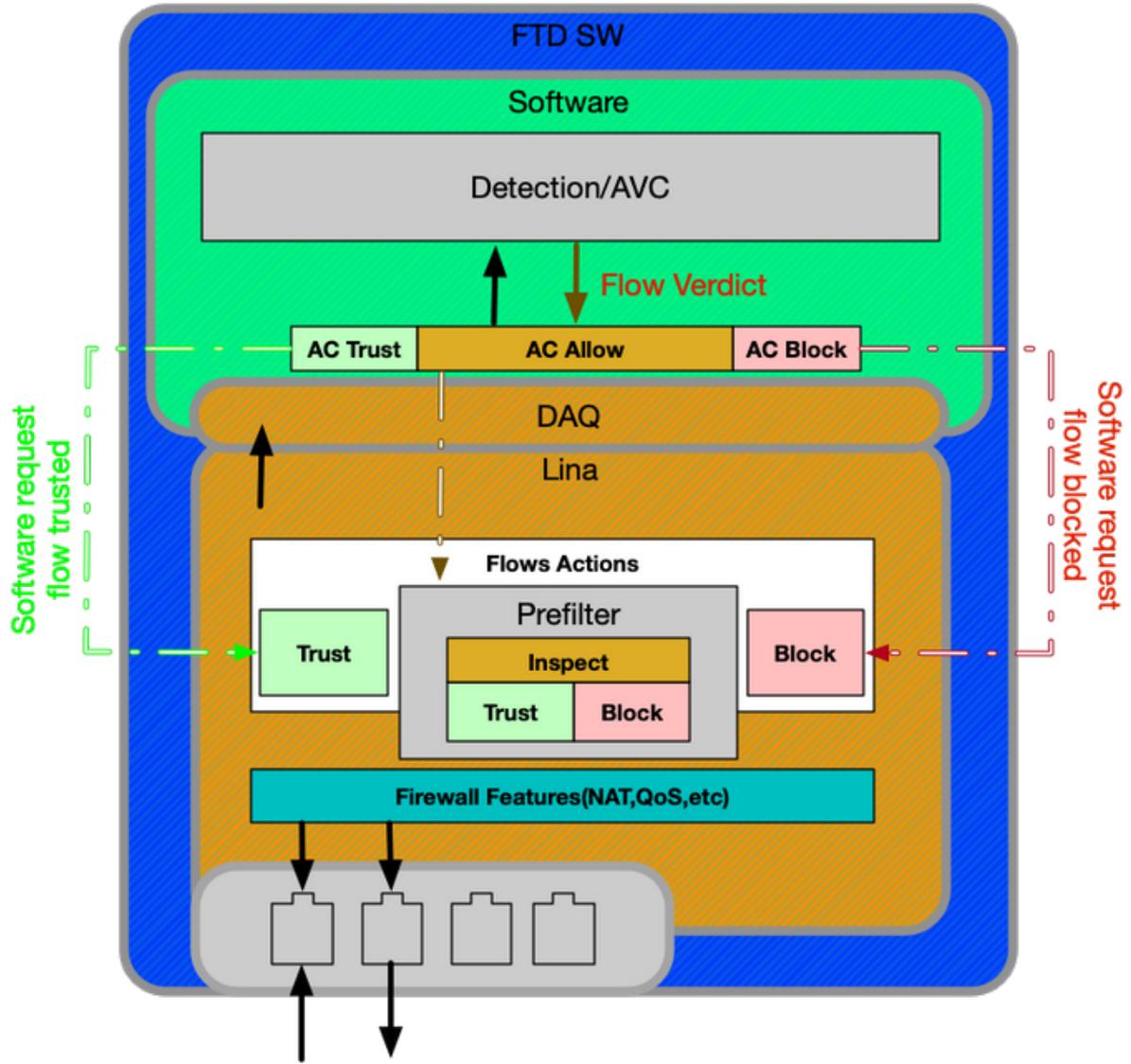
زاهاك يساسأل في اذه SFR ةدحو مساب FirePOWER تامدخل يساسأل ماظنلا لىلا اضيأ راشيو ةصنم ASA 5500-X لىلا لمعي يضارتفا .



ةيظمن ال SFR ةدحو لى اهل اسرا متي يتل تانايا لى رورم ةكح ASA لى ةمدخل جهن ددحي تانايا لى لوصحل كرحمب لاصتال لاهم ادختسا متي يتل او تانايا لى وتسم ةقبط كانه اهمه ف ريخش لل نكمي ةقيرطب مزحلل ةمحرتل همدختسا متي يذلاو، FirePOWER (DAQ).

## Virtual ASA500-X و Firepower ةصنم لى دى دعت دض عافدل FTD

FirePOWER و Lina (ASA) نم لك لى يوتحت ةدحو ةروص نم يس اساسا ل FTD ماظن نوكتي ةيلعاف رثكأ تالاصتإ كانه نأ وه ةصنم ةدحو SFR عم ASA ني بو اذه ني بس يئرلا قرفلا ني لina و snort.

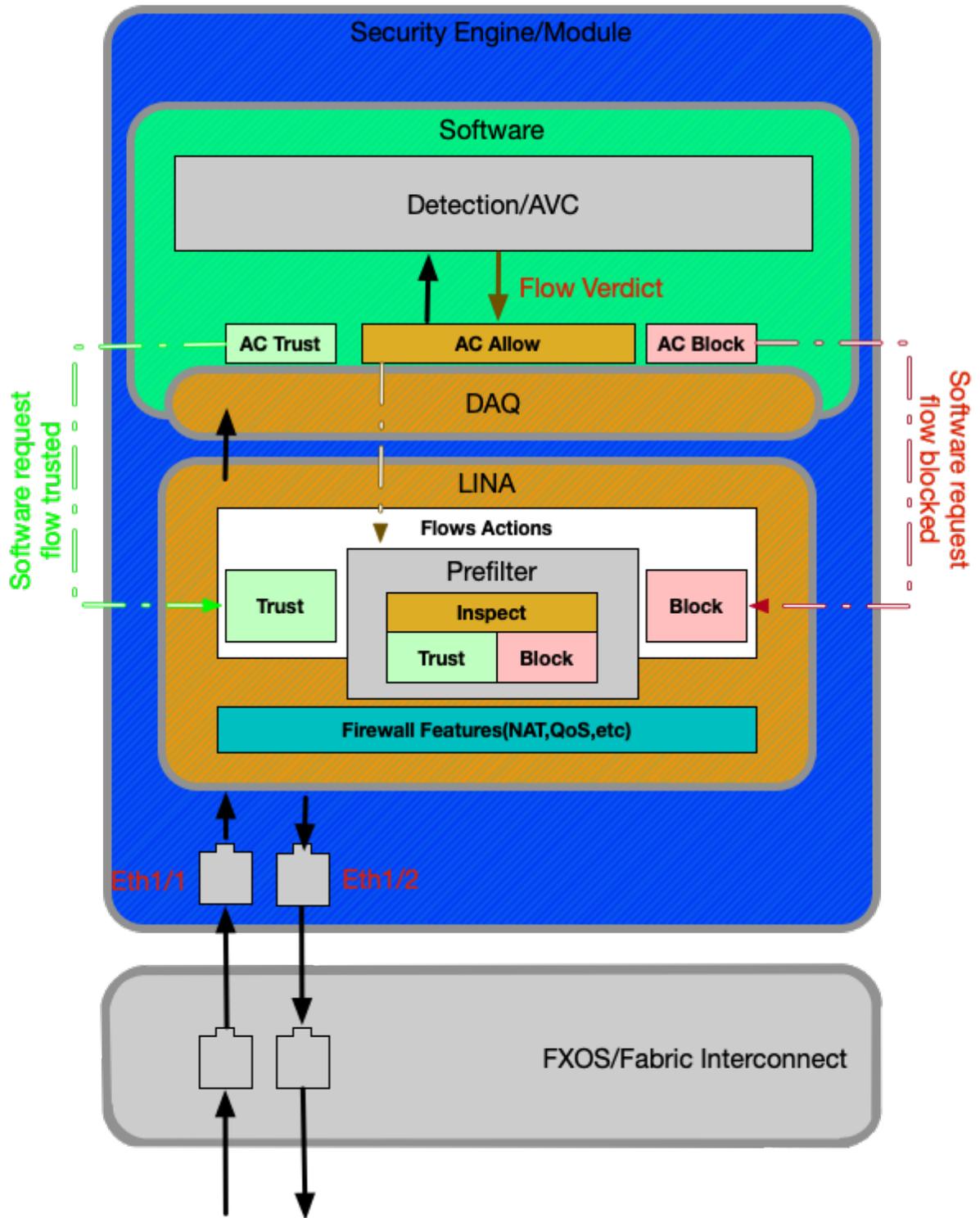


## FTD تاصنم يلع SSP

يوليغشتلا ماظنلا قوف FTD جمانرب لمعي، (SSP) نامألا تامدخل ةيساسألا ةمظنألا زرط ي ف  
 ماظن نع قرابع وه، (FXOS مساب اراصتخا فورعمل) Firepower Xsible Operation System  
 فرعت ةفلتخم تاقيبطت ةفاضتساو لكيهال ةزهجأ ةرادال مدختسي (OS) يساسأ لئغشت  
 ةيقتنملا ةزهجال مساب.

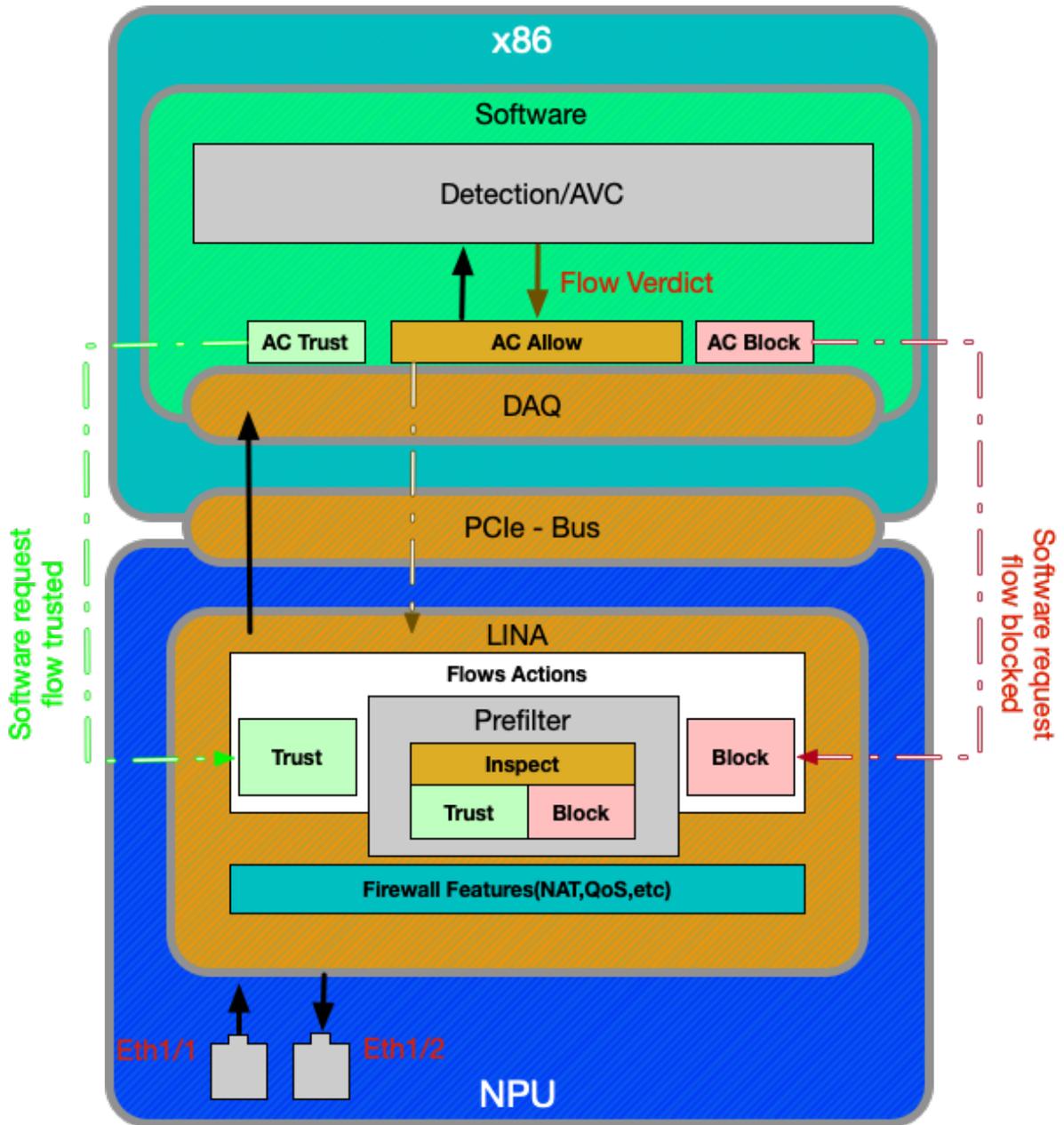
امك، زرطال ربع تافالتخال ضعب كانه، (SSP) نامألا ةقبط لوكتوربل يساسألا ماظنلا لخاد  
 هاندا فاصوألا ةينايبلا موسرلا ي ف حضوم وه.

## Firepower 9300 و 4100 ةزهجأ



ةطساوب جارخإلاو لاخدإلا مزح عم لماعتلا متي، Firepower 9300 و 4100 ةساسألا ةمظنألا ىلع  
 متي (يچيسننلا ينيبلا لاصتالا) FXOS تباثلا جم انربلا ةطساوب هليغشت متي لوح م  
 دعب (ةلاحلا هذه ي ف) ي قطنملا زاھجلا ىلا ةنعملا تاهجاو لا ىلا مزحلا لاسرا ك لذ دعب  
 SSP ريغ FTD تاصنم ىلع لاجلا وه امك اهسفن يه مزحلا ةجلاعم نوكت، كلذ

## ةزهجأ Firepower 2100



ب ةصاخلا ريغ FTD ةسساسألا ةمظنألا اريثك هبشي لكشب Firepower 2100 زاغلا لمعي عمو 4100 و 9300 نيزارطلا يف ةدوجوملا ينيبالا ةينيبالا لاصتا ةقبط يلع يوتحي الو SSP. ةرئادلا دوجو وهو الأ، رخألا ةزهجألاب ةنراقم 2100 ةلسلسلا ةزهجأ يف ريبك قرف كانه، كلذ يلع (LINA) ةيديلقنلا ASA تازيم عي مج ليغشت متي (ASIC) قي بطتلاب ةصاخلا ةجمدملا ةيفصتو، snort) يلاتلا ليجلا نم (NGFW) ةي امحلا رادج تازيم عي مج ليغشت متي امك، ASIC و Snort و Lina اهب لصتت يتلا ةقيرطلا. ةيديلقنلا x86 ةينيبالا يلع (كلذ يلا امو، URL ناونع ربع Peripheral Component Interconnect Express (PCIe) لالخ نم يه يساسألا ماظنلا اذه يلع رشابملا لوصولا مدختست يتلا رخألا ةسساسألا ةمظنألاب ةنراقم، مزحلا راطتنا ةمئاق ريخشلا يتح راطتنا ةمئاق يف مزحلا عضول (DMA) ةركاذلا يلا.

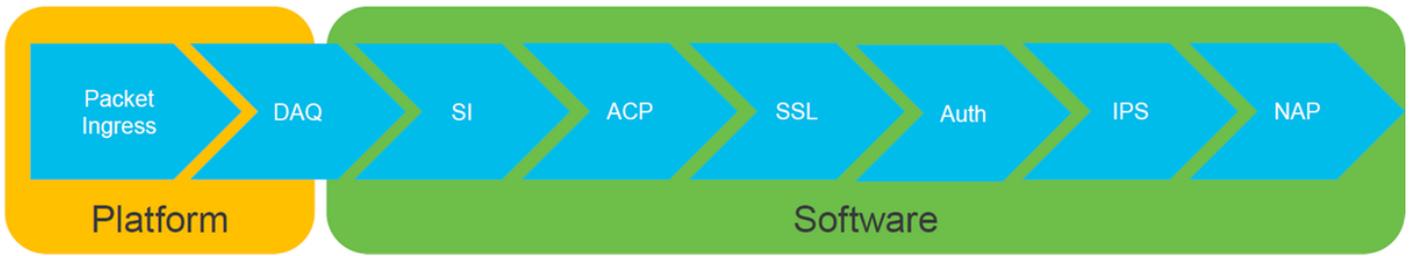
ب ةصاخلا ريغ FTD ةمظنألا عاطخأ فاشكتسال اهسفن بيلاسألا عابتا متيس: **ةظحالم SSP** يساسألا ماظنلا يلع اهجالصا و SSP.

## تانايب راسم عاطخأ فاشكتسال اهب يصوصملا ةي لمعلا اهجالصا و Firepower

تانايبالا راسم ةينيبالا يلا ةفاضلاب ةديرفلا رورملا ةكرح ديدحت ةيفيك انيطغ دقو نألا

طاقس إنكمي يتلا ءدءملا نكامألا إلا نألا رظنن اننإف، FirePOWER تاصنم يف يساسألا يتلاو، تانايبال راسم تالاقم يف اهتيطغت متي ءيساسأ تانوكم ءينامث كانه. اهيف مزحلا ءلمءملا مزحلا طاقسإ تايلمء ءيءءل يءنم لكشب اهءالءا ءاطءألا فاشكءسأ نكمي يلى ام ريباءءلا هءه لمءءو:

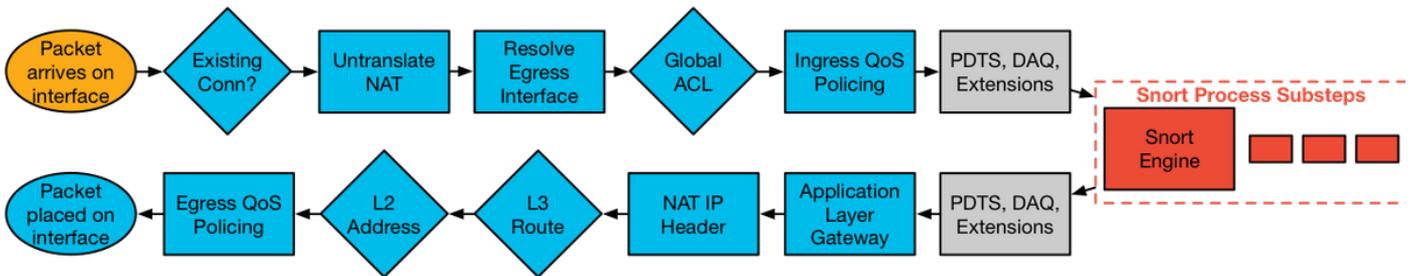
1. ءمزحلا لءءم
2. ءاقبء DAQ Firepower
3. ءينمألا تارابءءسإلا
4. لوصولا يف مءءءلا ءسايء
5. ءهن SSL
6. ءطءننلا ءقءاصملا تازيم
7. ءءاوق (ءسءلا ءسايء IPS)
8. (ءكبءل لبق ام ءلاءم تاءاءء) ءكبءل لءلءء ءهن



هءو ىلء FirePOWER ءلاءم يف تايلمءلا بءترب ءءرم ريب ءانوكملا هءه: ءطءالم اهءالءا ءاطءألا فاشكءسالا هب ىصولملا لمءل ريسل اءفوءب ءولمءه انءلوء، ءقءلا ءمزحلا طاءءم يلىءل راسم لل هانءأ يءىضوءءلا مسرلا ءءار.

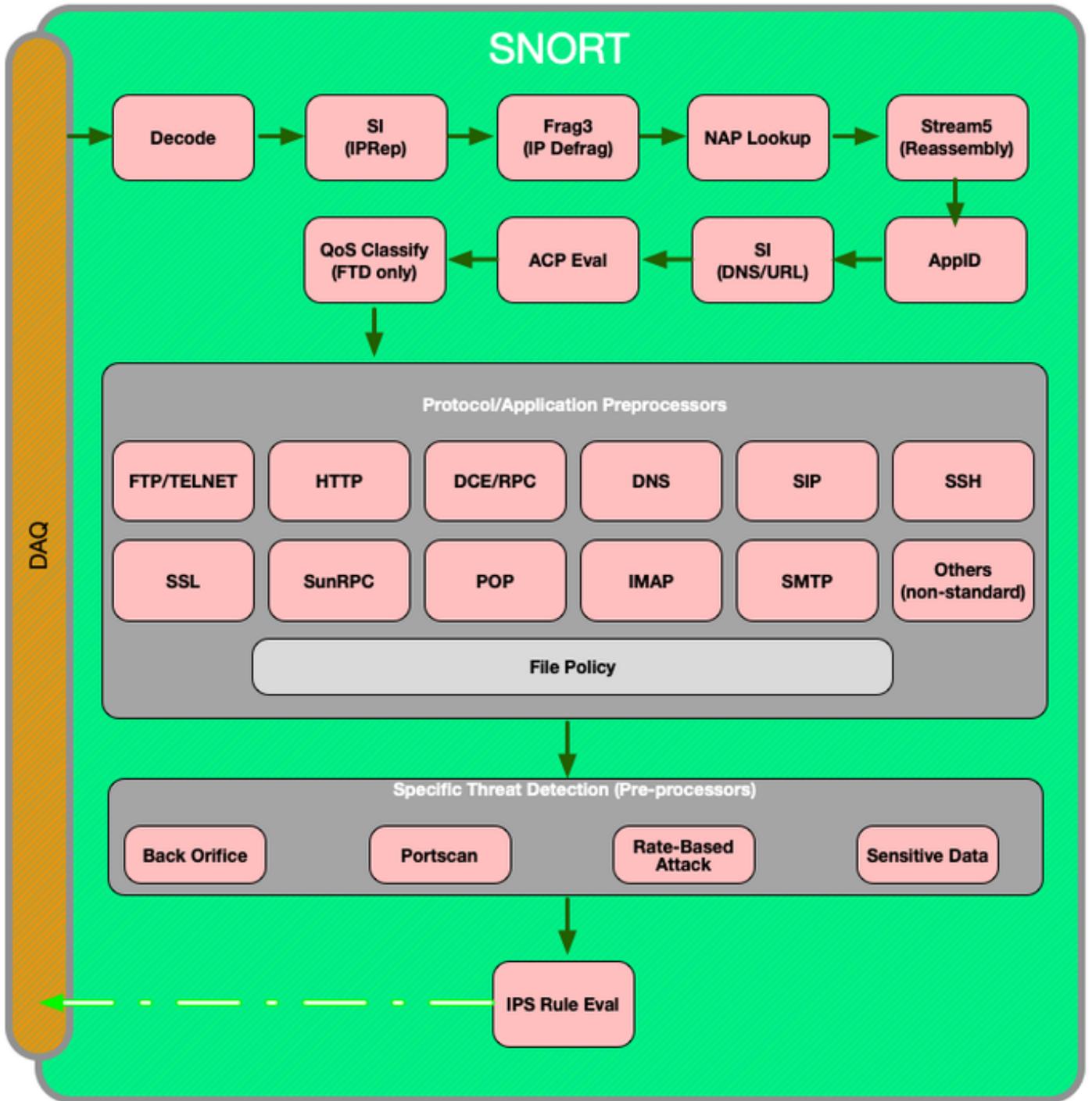
## FTD ربع ءمزحلا لىءءل راسملا

FTD لالء اهزايءءا ءنء ءمزحلا لىءءل راسملا يلاءل يءىضوءءلا مسرلا ءضوي.



## ءروشلا ءمزح راسم

ريبءشلا كءم لالء نم ءمزحلا راسم يلاءل يءىضوءءلا مسرلا ءضوي.



## مراحل جورخلاو لوخدلا

تايلمع ي ا ثودج مدع نم دكأتلا يه اهجالص او تانا ي ب ل ا راسم ءاطخ ا فاشك تس ا واطخ ي لو ا دع ب ، لخدت ال اهنكلو لخدت ةمزل ا تناك اذا . ةمزل ا ةجالعمل جورخلا و لوخدلا ةلحرم ي ف طاقس ا راسم لخد ام ناكم ي ف زا هجال ةطساوب اهطاقس ا متي ةمزل ا نا نم دكأتلا كنكم ي كل ذ تانا ي ب ل ا .

FirePOWER ةمظنا ي ل ا هجورخو مزل ا لوخد ءاطخ ا فاشك تس ا ةي فيك ي ل ا [ءلاقملا](#) هذه قرطتت اهجالص او .

# DAQ Firepower ةقبط

فأشكتسأ يف ةيولاتلا ةوطخلال نإف ،هأجتإلإ سئل نكلو هأجتإلإ ديق ةمزحلأ نأ ديدحت مت إذا باسكتك) FirePOWER DAQ ةقبط يف نوكت نأ بجي أهألصلإو تانايبلأ راسم ءاطخأ رملأ ناك إذا وشيتفتلل FirePOWER لىل ةيئعملأ رورملا ةكرح لاسرأ نم دكأتلل (تانايبلأ أهليدعت وأ أهطاقسلأ مت إذا ،كلذك

ةطساوب رورملا ةكرحل ةيولوالأ ةجلاعملأ ءاطخأ فأشكتسأ ةيئفك يف [ةلاقملا](#) هذه شحتب ءهألصلإو زاهجال ربع هكلست يذلا راسملا لىل ةفاصلأب FirePOWER

الوؤسم FirePOWER نوكت ناك إذا ام ديدحتل امامت FirePOWER زاهج زواجت ةيئفك يطغي امك رورملا ةكرح ةلكشم نع

## ةيئمألا تارابختسلأ

ةلهس يوتسملأ اذه يف لتكلأ .رورملا ةكرح صرخل FirePOWER لخد نوكت لوأ وه نامألا ءاكذو (GUI) ةيموسرلا مدختسملأ ةهجاو لىل ءكذ ديدحت نكميو .انكمم ليجستلا ماد ام ديدحتل ادج يف مكحتلا > تاسايسلا لىل لاقتنال لال خ نم (FMC) لوصولأ يف مكحتلا ءدحوب ءصاخلا جهنلأ بناجب دوجوملا ريرحتلا زمر قوف رقتلا دعب .لوصولأ يف مكحتلا ءسايس > لوصولأ نامألا تامولعم بيوبتلا ءمالع لىل لقتنأ ،شحتبلا ديق

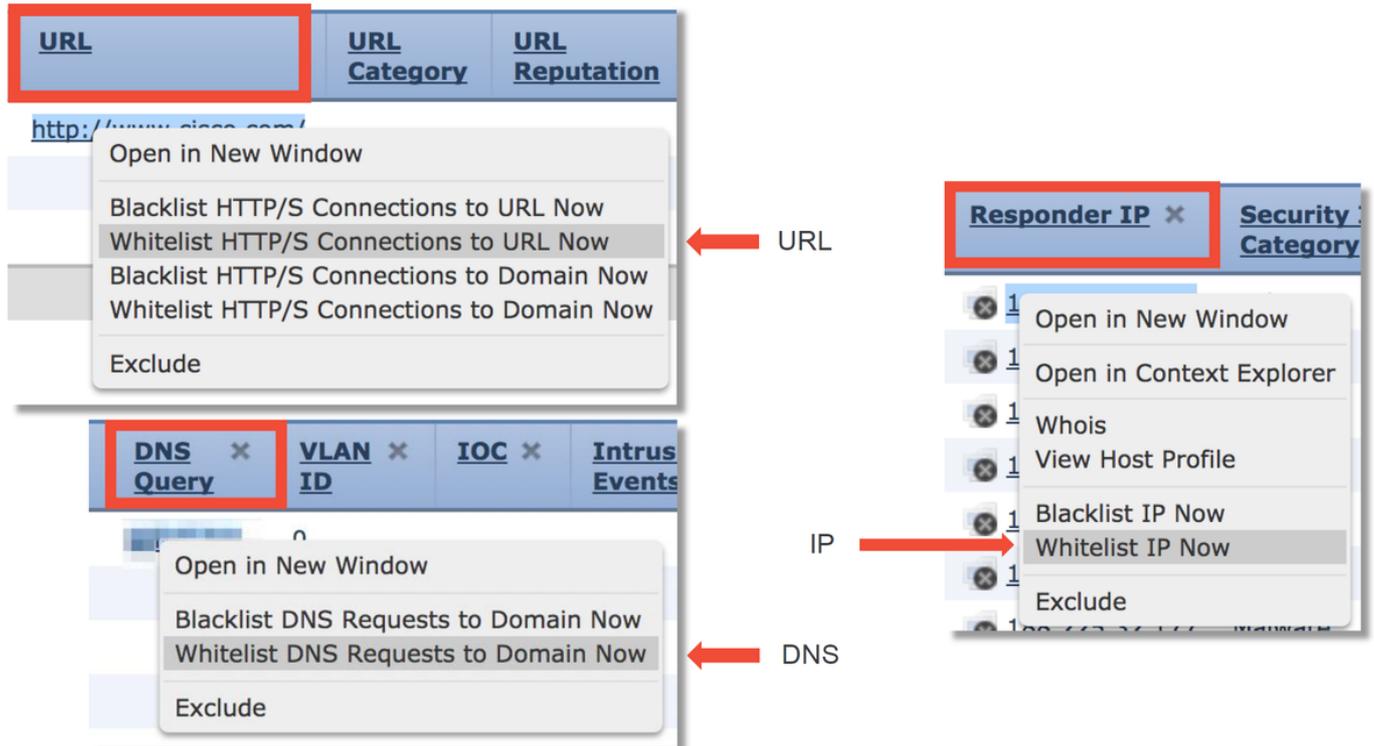
The screenshot shows the 'Security Intelligence' tab in the FMC interface. The 'DNS Policy' is set to 'Default DNS Policy'. The 'Whitelist (2)' section contains two entries: 'Global Whitelist (Any Zone)' under 'Networks' and 'Global Whitelist for URL (Any Zone)' under 'URLs'. The 'Blacklist (30)' section is expanded, showing a list of categories and their corresponding 'Logging' status. The 'Networks' section has 'Logging enabled' checked, while the 'URLs' section has 'Logging disabled' checked. A red arrow points to the 'Logging enabled' checkbox, another red arrow points to the 'Logging disabled' checkbox, and a third red arrow points to the 'DNS Policy' dropdown menu in the top right corner.

Category	Logging Status
Networks	Logging enabled
Attackers (Any Zone)	X
Bogon (Any Zone)	X
Bots (Any Zone)	X
CnC (Any Zone)	X
Dga (Any Zone)	X
Exploitkit (Any Zone)	X
Malware (Any Zone)	X
Open_proxy (Any Zone)	X
Phishing (Any Zone)	X
Response (Any Zone)	X
Spam (Any Zone)	X
Suspicious (Any Zone)	X
Tor_exit_node (Any Zone)	X
Global Blacklist (Any Zone)	X
URLs	Logging disabled
my_custom_url (Any Zone)	X
Global Blacklist for URL (Any Zone)	X
URL Attackers (Any Zone)	X
URL Bogon (Any Zone)	X
URL Bots (Any Zone)	X
URL CnC (Any Zone)	X
URL Dga (Any Zone)	X
URL Exploitkit (Any Zone)	X
URL Malware (Any Zone)	X
URL Open_proxy (Any Zone)	X
URL Open_relay (Any Zone)	X
URL Phishing (Any Zone)	X
URL Response (Any Zone)	X
URL Spam (Any Zone)	X
URL Suspicious (Any Zone)	X
URL Tor_exit_node (Any Zone)	X

شادحاً > تالاصتالال > ليلحتلالا تحت نامألا ءاكذ شادحاً ضرع كنكمي ، ليجستال ني كمت درجمب رورملا ءكرح عنم ببس احضاو نوئي نأ بجي . نامألا ءاكذ

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

DNS مالعسا وأ URL وأ IP ليلع نامألا سواملا رزب رقنلال كنكمي ، ءعيرس في فخت ءوطخك ءاضيبلا تانايبلا راخي رايتخاو "نامألا تامولعم" ءزيم ءطساوب هرطح متي يذلا



تنك اذوا ، ءادوسلال ءمئاقلال ليلع حيجص ريغ لكشب ءعضومت ام ائيش نأ في كشت تنك اذوا طبارلال ليلع Cisco Talos عم ءرشابم ءركذت حتف كنكمي ، ءعمسلال ريغت بلط في بغرت ليلال:

[https://www.talosintelligence.com/reputation\\_center/support](https://www.talosintelligence.com/reputation_center/support)

نم لاخدا ءلازا ام برو هرطح متي ام نع ءالبال TAC لىل تانايبلا ريفوت اضيأ كنكمي ءادوسلال ءمئاقلال

ءاحالساو "نامألا تامولعم" نوكم ءاطخأ فاشك تسأ لوح ءيليصفت تامولعم ليلع لوصحلل ءلصلال تاذا ءاحالساو تانايبلا راسم ءاطخأ فاشك تسأ [ءلاقم](#) ءعءارم ءاچرلا

## لوصول في مكحتلال ءسايس

ءليلال ءوطخلال نإف ، رورملا ءكرح رطحب موقت ال "نامألا تامولعم" ءزيم نأ ديحت مت اذوا ام ءفرعمل ءاحالساو "لوصول في مكحتلال ءسايس" ءعاق ءاطخأ فاشك تسأ يه ءهب لوصولل رورملا ءكرح طاقساب موقت "رطحلال" ءارء نمضتت يتلا ءعاقولل اذوا تنك اذوا

ءهذل كنكمي ، امومع . ءببتلاب طاقتلالال وأ "firewall-engine-debug" رمألا ماخذتسا ءدبب لوصول

بابسأ يألو، رورملا ةكرح اهرضت يتلا ةدعاقلا يه ام كربختو اروف باوجلل كي طعت نا تاودالا

- ةكرح عنمت يتلا ةدعاقلا ةفرعمل Firepower CLI لىل ع ااطخأل حيحصت ليغشتب مق رادج ماظنل معد > : يتلا رمأل لال خ نم (تامل عمل نم نكمم ددع ربكأ لاخذإ نم دكأت) رورملا ااطخأل حيحصت-كرحملا-ةياملح

• ليحلحتلل TAC لىل ااطخأل حيحصت جارخا ريفوت نكمي

يتلا رورملا ةكرحل ةدعاقلا مييقت فصت يتلا، ةيجذوملل تاجرحملا ضعب يلي اميف "حامسلا" اارجال عم لوصولو يف مكحتلا ةدعاق قباطت

```
> system support firewall-engine-debug
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.51
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 New session
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload
0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 pending rule order 3, 'block urls', URL
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676,
payload 2655, client 638, misc 0, user 9999997, url http://www.cisco.com/, xff
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0: DataMessaging_GetURLData: Returning URL_BCTYPE
for www.cisco.com
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 rule order 3, 'block urls', URL Lookup Success:
http://www.cisco.com/ waited: 0ms
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 no match rule order 3, 'block urls',
url=(http://www.cisco.com/) c=4 r=96
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 match rule order 4, 'inspect it all', action Allow
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 File policy verdict is Type, Malware, and Capture
```

مل وا، اهتقباطم مت يتلا (AC) لوصولو يف مكحتلا دعاقو نم يا ديحت لىل ارداق نكت مل اذا تاودالا مادختساب ةلكشملا يه ددرتملا رايتلا ةسايس تناك اذا ام ديحت لىل ارداق نكت يف مكحتلا ةسايس ااطخا فاشكتسال ةيساسال تاوطخل ضعب يلي اميف، هالع اءراول تايلمع/تارييغت بلطتت اهنال لوال رايل تسيلا تارايل هذه نا طحال) اهالصلو لوصولو (ةسايسلل رشن

- "رطح" اارجال عم دعاقو يال ليحستلا نيكمم
- عاشناب كلذ دعب مق، اهرطح متي و رورملا ةكرحل لاصلتالا اادحأ يرت ال لازت ال تنك اذا فيفخت ةوطخك ةينعمل رورملا ةكرحل ةقت ةدعاق
- نأ يف كشت لازت ال كنكل ةلكشملا لحت ال لازت ال رورملا ةكرحل ةقتلا ةدعاق تنك اذا مكحتلل غراف ديدج جهن عاشناب مق، كلذ دعب، ااطخ لىل ةدوجوم ددرتملا رايتلا ةسايس "رورملا ةكرحل لك رطح" ريفيضا رتفا اارجال مادختساب، نكمأ ن لوصولو يف

## Check logging for block rules

#	Name	Sou... Zon...	Dest Zon...	Sou... Net...	Dest Net...	VLA...	Use...	App...	Sou...	Des...	URLs	ISE... Attr...	Acti...					
▼ Mandatory - My AC Policy (1-2)																		
1	block with logging	any	any	any	any	any	any	YouTube	any	any	any	any	Block					0
2	block no logging	any	any	any	any	any	any	YouTube	any	any	any	any	Block					0

↓ Add trust rule

1	Trust traffic	any	any	192.	any	any	any	any	any	any	any	any	Trust					0
2	block with logging	any	any	any	any	any	any	YouTube	any	any	any	any	Block					0
3	block no logging	any	any	any	any	any	any	YouTube	any	any	any	any	Block					0

↓ Create blank AC policy

#	Name	Sour... Zones	Dest Zones	Sour... Netw...	Dest Netw...	VLAN...	Users	Appli...	Sour...	Dest ...	URLs	ISE/... Attri...	Action					
▼ Mandatory - Test - No rules (-)																		
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>																		
▼ Default - Test - No rules (-)																		
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>																		
Default Action												Intrusion Prevention: Balanced Security and Connectivity						

اهالصالو لوصولاب مكحتلا ةسايس اطاخا فاشكتسا لوح ةلصم تامولعم يلعل لوصولل ةلصلل اذاهالصالو تانايلبال راسم اطاخا فاشكتسا [قلاقم](#) ةعجارم اچارلا.

## SSL جهن

يللي اميف رورملا ةكرح رظح ماق دق نوكي نأ لمحتحملا نمف ،مادختسالال ديقي SSL جهن ناك اذا اهلصالو SSL ةسايس اطاخا فاشكتسال ةسايسال اوطلخال ضعب:

- 'يضارتفالال اچارلال' كلذيف امب ،دعاوقلال عيمجل ليحستلال نيكتمت

#	Name	Sour... Zones	Dest Zones	Source Netw...	Dest Netw...	VLA...	Us...	Appli...	Sour...	Dest ...	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DnD banking	any	any	any	any	any	any	any	any	any	Financial Services (Any Reputatio	any	Do not decrypt
2	decrypt outbound suspicious	inside	outside	any	any	any	any	any	any	any	Any (Reputations 1-2)	any	Decrypt - Resign

**Editing Rule - DnD banking**

Name: DnD banking  Enabled Move

Action: Do not decrypt

**Logging**

Log at End of Connection Enable Logging

Send Connection Events to:

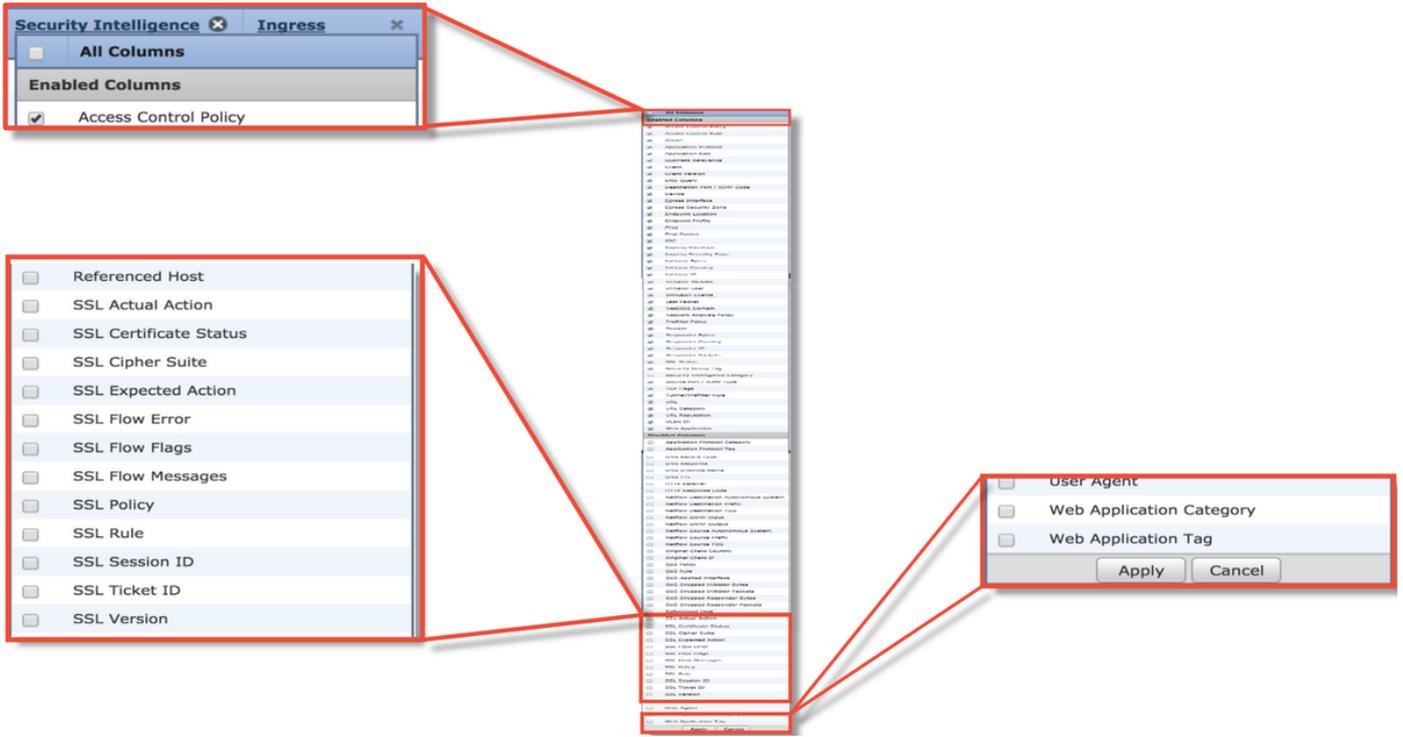
Event Viewer

Syslog Select a Syslog Alert Configuration...

SNMP Trap Select an SNMP Alert Configuration...

Save Cancel

- رظحل راخي نييعت مت اذا ام ةفرعمل ريفشتلال اغلال اچارل بيوبتلال ةمالع نم ققحت رورملا ةكرح
- مسالال يف 'SSL' يللي يوتحت يتلال لوقحلال ةفاك نم ققحت ،"الاصلتال اچارل" مسق يف اچارل" ضراع يف مهنكتمت بجيو يضارتفال لكشب نيمدختسمال مظعم ليطعت متي دومع مساي اراوجب دوجومال بيلصلال قوف رقنلاب "الاصلتال"



Connection Events [\[switch workflow\]](#)  
 Connections with Application Details > [Table View of Connection Events](#)  
 Search Constraints (Edit Search Save Search)

**SSL Blocking flow**

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country
2017-05-30 13:09:23	2017-05-30 13:09:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:53	2017-05-30 13:08:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:23	2017-05-30 13:08:24	Block	SSL Block	192.16			
2017-05-30 13:08:19	2017-05-30 13:08:20	Block	SSL Block	192.16			
2017-05-30 13:07:53	2017-05-30 13:07:54	Block	SSL Block	192.16			
2017-05-30 13:07:23	2017-05-30 13:07:24	Block	SSL Block	192.16			

**Cause of the SSL failure**

SSL Status	SSL Flow Error	SSL Actual Action	SSL Expected Action	SSL Certificate Status	SSL Version
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLsv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLsv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLsv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLsv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLsv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	decrypt (Resign)	Decrypt (Resign)	Valid	TLsv1.2

**SSL flow flags for what happened with flow**

SSL Rule	SSL Session ID	SSL Ticket ID	SSL Flow Flags	SSL Flow Messages
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE

- في فخت ةوطخك يضا رتفا ءارچك ريفشتلا ك ف مدع عم ةغراف SSL ةسايس ءاشنإ
- في فخت ةوطخك لوصولو ي ف مكحتلا جهن نم SSL جهن ةلازا مدقتم بيوبتلا ةمالع ي ف كلذ نييعت مت

لاصتالا اءا ءلا سارنا نكميو ، رورملا ءكرح طاقساب موقوي IT ب صا ءال SSL جهن نا ي ف هبتشي TAC. ءلا جهنلا نيوكت ءلا ءفاضالاب

ءارءلا ، ءالصالو SSL ةسايس ءاطءا فاشكتسا لو ء لي صا فتلا نم ءيزم ءل ء لوصءلل ءلصال اءالصالو تانا يبال راسم ءاطءا فاشكتسا [ءلاقم](#) ءعءارم

## ءطشنلا ءقءاصملا

رورملا ءكرح طاقساب ءل ءرءقلا ءطشنلا ءقءاصملا ل نو كي ، ءيوهلا جهن ي ف ما ءءتسال اءن

اهس فن ةطشننلا ةقداصملا ةزيم رثؤت نا نكمي. أطخ ثودح ةلاح يف اهب حامسلا بجي يتلا ،مدختسم ةقداصم ىلا انتجاح ديدحت مت اذا هنأل HTTP/HTTPS رورم ةكرح عيمج ىلع ةرشابم رثؤت نا يغبني ال ةطشننلا ةقداصملا نا ينعي اذهو. طقف HTTP لوكوتورب ربع اذه لك ثدحي ةددحم دعاوق كيدل نكت مل ام (كلذ ىلا امو ICMP و DNS لثم) ىرخألا ةكبشلا تامدخ ىلع نيمدختسملل نكمي الو ،مدختسملا ىلع انا رب رطحل ىلع موقت لوصولا يف مكحتلل ةلكشم اذه نوكتي نل ،كلذ عمو. FTD ىلع ةطشننلا ةقداصملا تامدخ لالخنم ةقداصملا ةقداصملا ىلع نيمدختسملا ةردق مدعل ةجيتن نكلو ،ةطشننلا ةقداصملا ةزيم ةرشابم مهيلىل قداصملا ريغ نيمدختسملا عنمي جهن دوجوو.

مادختساب ةيوهال جهن نمض ةدعاق يلىطعت يف ةعيرسلا فيفختلا تاوطخ ىدح لثمتت "ةطشننلا ةقداصملا" ءارج.

مادختسا "رايخ ىلع يوتحت ال "ةلماخل ةقداصملا" ءارج عم دعاوق يلى نا نم اضيأ دكأت هصحف مت يذلا "مدختسملا ديدحت نم ةلماخل ةقداصملا نكمتت مل اذا ةطشننلا ةقداصملا

**Editing Rule - Passive**

Name: Passive  Enabled Move

Action: Passive Authentication Realm: my-realm Authentication Type: HTTP Basic

Zones Networks VLAN Tags Ports Realm & Settings

Realm \* my-realm Make sure passive auth rules don't fall back to active auth

Use active authentication if passive authentication cannot identify user

\* Required Field

Save Cancel

Action	Auth Type	
Active Authentication	NTLM	
Active Authentication	Kerberos	
Active Authentication	HTTP Negotiate	
Active Authentication	HTTP Response Pa	
Active Authentication	HTTP Basic	
Passive Authentication	none	

**Remove or disable active auth rules**

**Identity Policy Settings**

Identity Policy: None

**Or remove identity from Advanced tab of ACP**

[قلاقم](#) ةعجارم ءاجرلا ،اهحالصاو ةطشننلا ةقداصملا ءاطخأ فاشكتسا لوح ليصافتلا نم ديزم ةلصللا تاذاهحالصاو تانايبلا راسم ءاطخأ فاشكتسا

## ماحتقالا ةسايس

نكمي ةكبشلا ريخأت يف ببستلا وأ رورملا ةكرح طاقسإ ىلا للستلا ةسايس يدؤت دق مكحتلا ةسايس نمض ةيلالتلا ةثالثلا نكامأل دحأ يف للستلا ةسايس مادختسا لوصولاب:

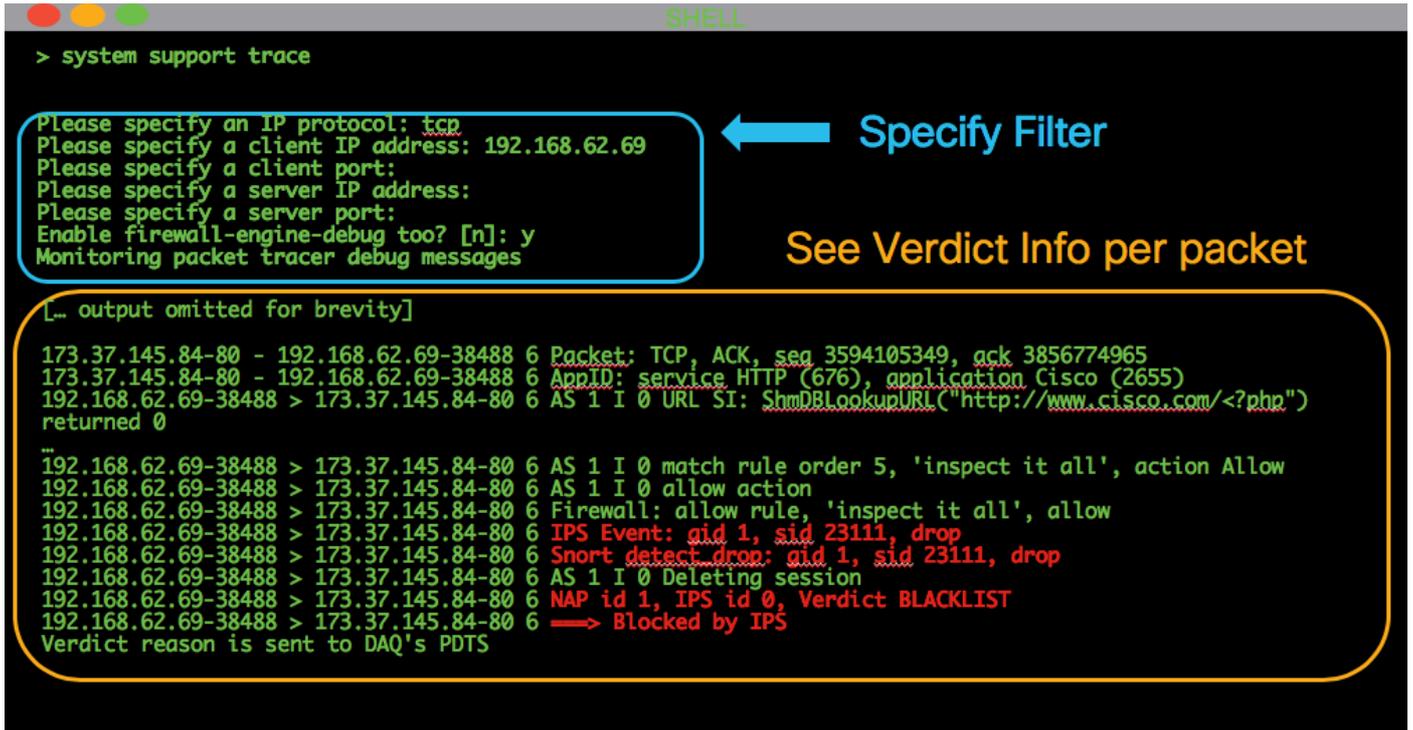
- "صحف" بيوبتلا ةمالع نمض ،لوصولاب مكحتلا ةدعاق يف
  - يضارتفالا ءارجإل يف
  - > قارتخال تاسايسو ةكبشلا ليلحت مسق يف ،ةمدقتم تاراخي بيوبتلا ةمالع يف
- لوصولا يف مكحتلا ةدعاق ديدحت لبق ةمدختسملا قارتخال ةسايس

ةحفص ىلا لقتنا ،رورملا ةكرح رطحب موقت ماحتقالا ةسايس ةدعاق تناك اذا ام ةفرعمل ةقيرط رفوت (FMC) ةيساسألا ةرادإل يف مكحتلا ةدحو يف ثادحألا > ماحتقالا > ليلحت عالطالا يجري .ثادحألا يف ةكراشملا ةفيضملا ةزهجالا لوح تامولعم للستلا ثادحأ لودج ضرع

ةق لعتم ل تامول عم ل اب ةق لعتم ل ا ه ا ل ص و ا ت ا ن ا ي ب ل ا ر ا س م ا ط ا خ ا ف ا ش ك ت س ا ة ل ا ق م ي ل ع  
ب ش د ل ل ل ي ل ح ت ب .

موق ي (IPS) م ا ح ت ق ا ل ا ة س ا ي س ع ي ق و ت ن ا ك ا ذ ا ا م د ي د ح ت ل ا ه ب ي ص و م ل ا ي ل و ا ل ا ة و ط خ ل ل ل ث م ت  
ة ص ا خ ل ل (CLI) ر م ا و ا ل ر ط س ة ه ج ا و ن م م ا ط ن ل ل م ع د ع ب ت ت > ة ز ي م م ا د خ ت س ا ي ف ر و ر م ل ا ة ك ر ح ر ط ح ب  
م ن ا م ك ، e n g i n e - d e b u g - e r a d j u s t م ا ح ل ر ا د ج ة ه ب ا ش م ق ي ر ط ب ا ذ ه ا ط ا خ ا ل ا ح ي ح ص ت ر م ل م ع ي . F T D ب  
ع ب ت ت ل ل ب ن ا ج ب ة ي ا م ح ل ل ر ا د ج ك ر ح م ا ط ا خ ا ح ي ح ص ت ن ي ك م ت ر ا ي خ ك ل ل ح ي ت ي .

ت ر ه ظ ا ث ي ح م ا ط ن ل ل م ع د ع ب ت ت ة ا د ا م ا د خ ت س ا ل ا ل ا ث م ي ل ا ت ل ل ي ح ي ض و ت ل ل م س ر ل ا ح ض و ي  
ف ر ع م ل ل م ل ي ص ا ف ت ل ل ع ي م ج ك ح ن م ي ا ذ ه و . ل ف ط ت ل ل ة د ع ا ق ب ب س ب ة م ز ح ل ل ر ط ح م ت ه ن ا ة ج ي ت ن ل ل  
I P S ف ر ع م و ( ة ك ب ش ل ل ل ي ل ح ت ج ه ن ) N A P ف ر ع م و ( ع ي ق و ت ل ل ف ر ع م ) S I D ف ر ع م و ( G I D ) ة و م ج م ل  
ه ذ ه ر و ر م ل ا ة ك ر ح ع ن م ت ي ت ل ل ة د ع ا ق ل ل / ج ه ن ل ل ي ل ع ا ل ط ا ل ا ك ن ك م ي ي ت ح .

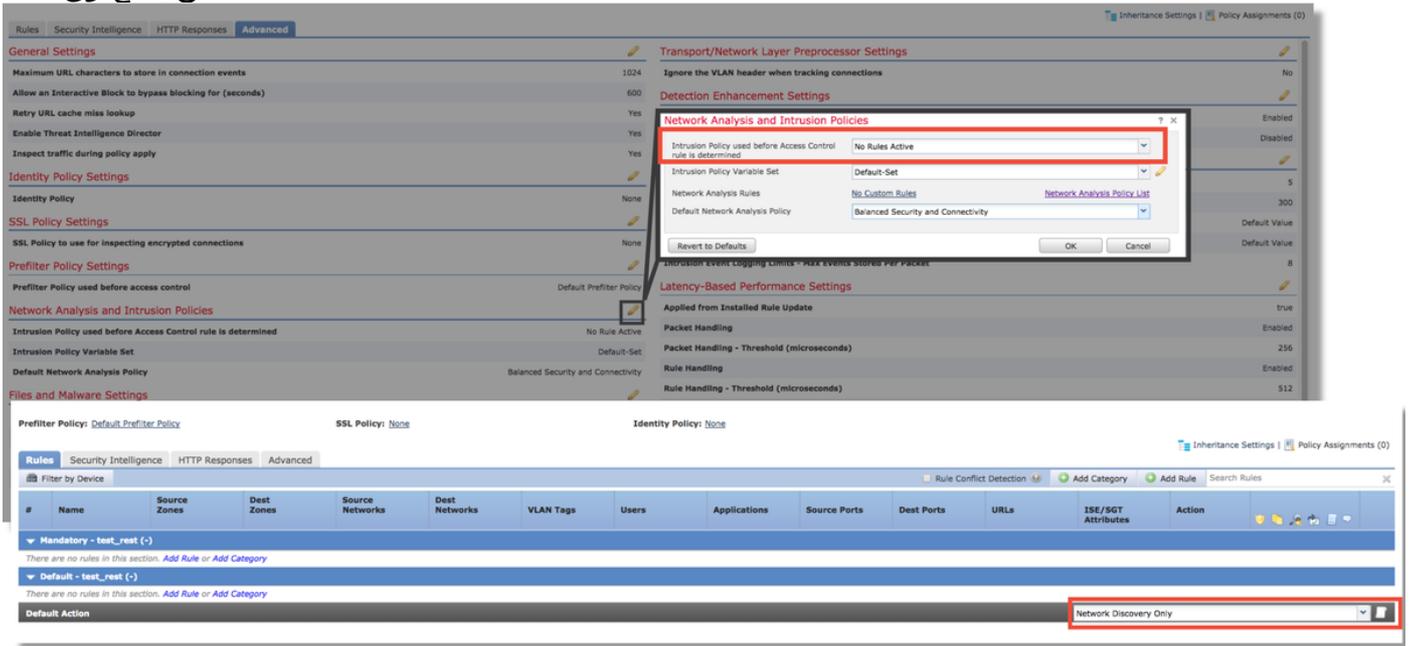


م ت ي ه ن ا ي ف ك ش ت ك ن ك ل و ، ع ب ت ت ل ل ا ج ا ر خ ا ر ط ح ب م و ق ت I P S ن ا د ي د ح ت ي ل ع ا ر د ا ق ن ك ت م ل ا ذ ا  
ع ن م ة س ا ي س ل ا د ب ت س ا ك ن ك م ي ف ، ة ص ص خ م ل ل و ص و ل ا ع ن م ة س ا ي س ب ب س ب I P S ط ا ق س ا  
ت ا س ا ي س ي ه ه ذ ه " ن ا م ا ل ا ر ب ع ل ا ص ت ا ل ا " ج ه ن و ا " ن ز ا و ت م ل ل ا ص ت ا ل ا و ن ا م ا ل a " ج ه ن ب ل و ص و ل ا  
م ت ن م و ، ة ل ك ش م ل ل ا ح ي ل ع ل م ع ي ه ن ا ف ، ر ي ي غ ت ل ل ا ذ ه ا ر ج ا م ت ا ذ ا C i s c o . ا ه ر ف و ت ي ت ل ل م ا ح ت ق ا ل ا  
م ت ا ذ ا T A C ل ب ق ن م ا ج ع ز م ا ق ب س م م د خ ت س م ل ا ص ص خ م ل م ا ح ت ق ا ل ا ج ه ن ن و ك ي ن ا ن ك م ي  
ي ض ا ر ت ف a ل ا د ا د ع ا ل ر ي ي غ ت ة ل و ا ح م ك ن ك م ي ف ، ل ع ف ل ا ب ة ي ض ا ر ت ف a ل a C i s c o ة س ا ي س م ا د خ ت س ا  
ق ي ي ض ت ي ف د ع ا س ت د ق ك ل ذ ل ، ل ق ا د ع ا و ق ي ل ع ي و ت ح ت د ع a و ق ل ل ه ذ ه ن ا ل ا ن ا م ل ل ق ا ج ه ن ي ل ل  
م ت ، ة ن ز ا و ت م ة س ا ي س م د خ ت س ت ت ن ا و ر و ر م ل ا ة ك ر ح ر ط ح م ت ا ذ ا ، ل ا ث م ل ل ي ب س ي ل ع . ق ا ط ن ل ل  
ن و ك ي ن ا ل م ت ح م ل ن م ف ، ة ل ك ش م ل ل ل و ز ت و ن ا م a ل ا ة س ا ي س ر ب ع ل ا ص ت a ل a ي ل ل ا ي د ب ت ل a ب م و ق ت  
ت a ل ف a ل l ا ه ن ي ي ع ت م ت ي م ل ي ت l l ر و ر م l a ة ك ر ح ط ق س ت ة ن ز ا و ت م l a ة س a ي س l l ا ي ف د ع a ق ك a ن ه  
ن a م a l a ة س a ي س ر ب ع ل a ص ت a l a ي ف .

ل ت ك ت ا ي ن ا ك م ا ع ي م ج ة ل ا ز ا ل " ل و ص و ل a ب م ك ح ت l a ج ه ن " ن م ض ة ي ل a ت l l ت a ر ي ي غ ت l l a ع a ر ج a ن ك م ي  
ن a م a l a ة ي ل a ع f ر ي ي غ ت م د ع l l ت a ر ي ي غ ت l l a ن م ن ك م م ر د ق ل ق a ع a ر ج a ب ي ص و ي ) " ل ل س ت l l a ج ه ن ص ح ف  
I P S ل ي ط ع ت ن م a ل د ب ، ة ي ن ع م l l ر و ر م l a ة ك ر ح ل ة ف د ه ت س م د د ر ت م ر a ي ت د ع a و ق ع ض و ب ي ص و ي a ذ l  
ف ( ا ه ل م ك a ب ة س a ي س l l ا ي ف :

- ر و ر م ة ك ر ح ق ب ا ط ت ي ت l l a ( د ع a و ق l l a ) ة د ع a ق l l a ط ق ف ( و ا ) ل و ص و ل a ب م ك ح ت l l a د ع a و ق ع ي م ج ي ف  
" ص ح ف " ب ي و ب ت l l a ة م a ل ع ن م ل ل س ت l l a ة س a ي س ة ل a ز a ب م ق ، ( ر ث ا ت ت ي ت l l a و ة ن ي ع م  
ج ه ن > ق a ر ت خ a l a ت a س a ي س و ة ك ب ش l l a ل ي ل ح ت ي ف ، ة م د ق ت م ت a ر a ي خ ب ي و ب ت l l a ة م a ل ع ي ف

دجوت ال" جهنلا رتخأ، لوصولاي ف مكحتلا دعاق مسق ديدحت لبق مدختسملا قارتخالال "ةطشن دعواق".



اهحالصإو ةكبشلا ليلحت جهن عاطخأ فاشكتسأ ل مدقتف ،دعب ةلكشملا اذه لحي مل اذا

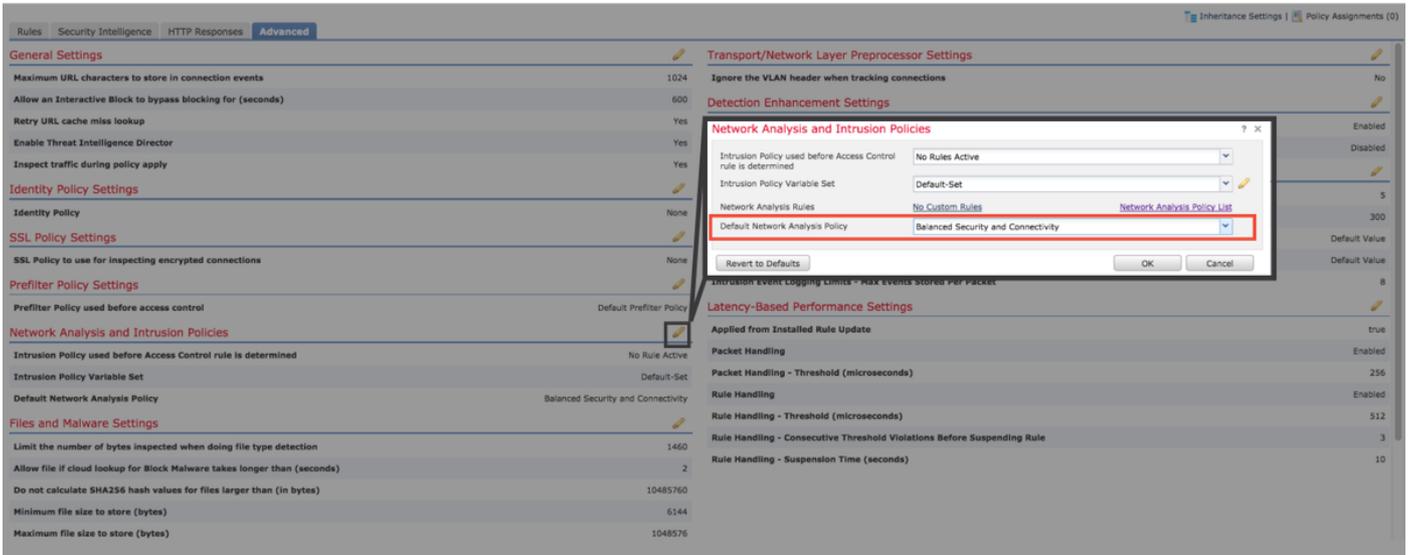
ةعجارم عاجرلا ،اهحالصإو "للستلا ةسايس" ةزيم عاطخأ فاشكتسأ لوح ليصافتلا نم ديزملا ةلصللا تاذ اهلحالصإو تانايبلا راسم عاطخأ فاشكتسأ [ةلاقم](#).

## ةكبشلا ليلحت ةسايس

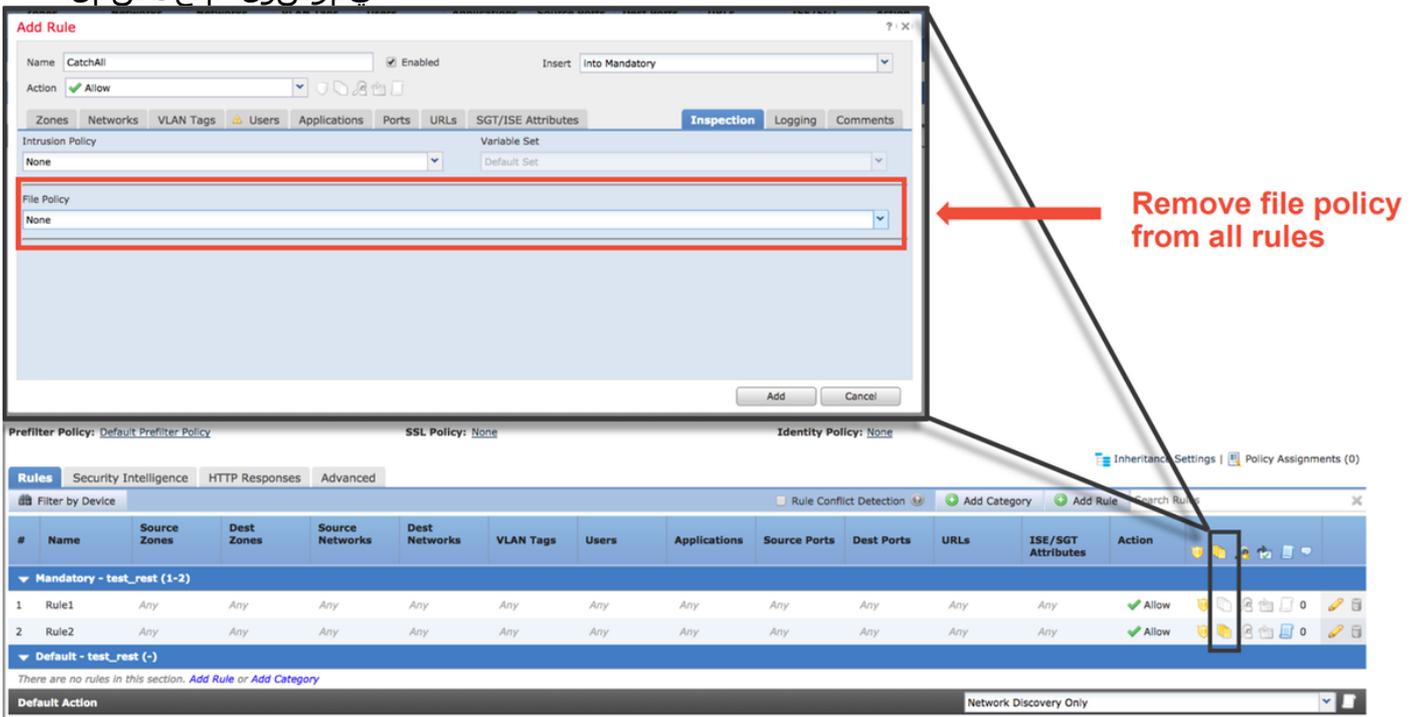
نكمي يتلاو ، FirePOWER ل قبسملال جلاعملال تاداعل ىلع (NAP) ةكبشلا ليلحت جهن يتحي اهلحالصإو عاطخأ فاشكتسال اهب ىصوملا ىلوالا ووطخلال دعت .رورملا ةكرح طاقسإ اهضعبل يف لثمتت يتلاو ،اهحالصإو IPS عاطخأ فاشكتسال ةبسنلاب لالجال وه امك اهسفن يه رورم ةكرح عنمي يذلا مداخلاي ف دجوي ام ىلع روثعال ةلواحمل ماظنلال معد بقعت > ةادأ مادختسإ اذاللا هذه لوح تامولعملال نم ديزم ىلع لوصولال هالعأ "ماحتقالا ةسايس" مسق عاجر .تانايبلا مادختسالال لاثمو .

ةعرسلال هجو ىلع ينطولا لمعلال جمانربب ةقلعتملا ةلمتحملا تالكشملا فيفخت لجا نم ةليللال تاوطخلال ذيفنت نكمي:

- جهنل اذه لدبتسا ،صصخملال مكحتلا ىوتسم ةيماح جمانرب مادختسإ ةلاح يف "نامال ربع لاصلتال" جهن وأ "نينزاوتملا لاصلتال او نامال"



- تايفضارت فالال دحأ لى NAP نيفي عت نم دكأت ،"ةصصخم دعاقوق" يأ مادختس إ قلاح يف هالعا ةروكذمل
- جهنك اتقوم هتلازال نكمي ، فلم جهن مدختست لوصولا يف مكحتل دعاقوق نم يأتناك اذا هجاويف سكعنت نل يتلواويف لخلال فرطال لىل ع قبسمل لجالعمل اتاداعل نيكمت فلم ةيموسرللا مدختسمل



ةكبشلال لىلحت ةسايس اطاخأ فاشكتسأ لوح لىلصافتلال نم ديزملا ةعجارم نكمي قلاقملا هذه يف اهالصالو

## ةلص تاذا تاملولعم

FirePOWER قئاثول تاطابترا

<https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا