

# لا اثم و ةي طم ن ل ا CX/FirePOWER ة دح و عم ASA ل ص و م ن ي و ك ت CWS

## ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ي س ا س ا ت ا م و ل ع م](#)

[ق ا ط ن ل ا](#)

[م ا د خ ت س ا ل ا ة ل ا ح](#)

[ة ي س ي ئ ر ل ا ط ا ق ن ل ا](#)

[ن ي و ك ت ل ا](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[CWS و ASA ل ر و ر م ل ا ة ك ر ح ق ف د ت](#)

[CX/FirePower و ASA ن م ل ك ل ر و ر م ل ا ة ك ر ح ق ف د ت](#)

[ت ا ن ي و ك ت ل ا](#)

[ل ك د ا ع ب ت س ا و \(TCP/80\) ت ن ر ت ن ا ل ا ب ة ط ب ت ر م ل ا ب ي و ر و ر م ت ا ك ر ح ل ك ة ق ب ا ط م ل ل و ص و ل ا ة م ئ ا ق ة ي ل خ ا د ل ا ر و ر م ل ا ت ا ك ر ح](#)

[\(TCP/443\) ت ن ر ت ن ا ل ا ب ة ط ب ت ر م ل ا HTTPS ر و ر م ت ا ك ر ح ع ي م ج ة ق ب ا ط م ل ل و ص و ل ا ة م ئ ا ق](#)

[ة ي ل خ ا د ل ا ر و ر م ل ا ت ا ك ر ح ع ي م ج د ا ع ب ت س ا و](#)

[HTTPS و ب ي و ر و ر م ت ا ك ر ح ل ك د ا ع ب ت س ا و ، ة ي ل خ ا د ل ا ر و ر م ل ا ة ك ر ح ل ك ة ق ب ا ط م ل ل و ص و ل ا ة م ئ ا ق](#)

[ي ر خ ا ل ا ذ ف ا ن م ل ا ع ي م ج و ت ن ر ت ن ا ل ا ب ة ط ب ت ر م ل ا](#)

[CX/FirePower و CWS ن م ل ك ل ت ا ن ا ي ا ب ل ا ر و ر م ة ك ر ح ة ق ب ا ط م ل ة ئ ف ل ا ة ط ي ر خ ن ي و ك ت](#)

[ة ئ ف ل ا ت ا ط ط خ م ب ت ا ع ا ر ج ا ل ا ن ا ر ق ا ل ة س ا ي س ل ا ة ط ي ر خ ن ي و ك ت](#)

[ة ه ج ا و ل ا ي ل ع CWS و CX/FirePower ل م ا ع ل ك ش ب ج ه ن ل ا ط ي ش ن ت](#)

[\(ق ر ف ا ل\) ASA ي ل ع CWS ن ي ك م ت](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

[ا ه ج ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

## ة م د ق م ل ا

ة د ح و عم Cisco Adaptive Security Appliance (ASA) ة د ح و م ا د خ ت س ا ة ي ف ي ك د ن ت س م ل ا ا ذ ه ف ص ي Cisco Cloud ل ص و م و ، ي ل ل ا ل ا ل ي ج ل ا ن م ة ي ا م ح ل ا ر ا د ج م س ا ب ا ض ي ا ة ف و ر ع م ل ا ، Context Aware (CX)، Web Security (CWS).

## ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

### ت ا ب ل ط ت م ل ا

ك ي د ل ن و ك ي ن ا ب Cisco ي ص و ت

- (ي ن ا ج م ص ي خ ر ت) ASA ي ل ع 3DES/AES ص ي خ ر ت
- ب و ل ط م ل ا ن ي م د خ ت س م ل ا د د ع ل CWS م ا د خ ت س ا ل ح ل ا ص CWS ص ي خ ر ت / ة م د خ
- ة ق د ا ص م ل ا ح ا ت ف م ء ا ش ن ا ل ScanCenter ل خ د م ي ل ا ل و ص و ل ا

## ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ن ي ع م ة ي د ا م ت ا ن و ك م و ج م ا ر ب ت ا ر ا د ص ا ي ل ع د ن ت س م ل ا ا ذ ه ر ص ت ق ي ا ل

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ء ا ش ن ا م ت ن ت ا ك ا ذ ا . ( ي ض ا ر ت ف ا ) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ج ا ل ا ع ي م ج ت ا د ب ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ة ر ش ا ب م ك ت ك ب ش

## ة ي س ا س ا ت ا م و ل ع م

### ق ا ط ن ل ا

ة ي ل ا ت ل ا ت ا ج ت ن م ل ا و ة ي ن ق ت ل ا ت ا ل ا ج م د ن ت س م ل ا ا ذ ه ح ض و ي

- ة ي ا م ح ر ا د ج ن ا م ا Cisco ASA 5500-X Series Adaptive Security ة ل د ع م ل ا ن ا م ا ل ا ة ز ه ج ا ر ف و ت ق ا ر ت خ ا ل ا ع ن م و ت ن ر ت ن ا ل ا
- ع ي م ج ي ف ل ي د ع ت ل ل ب ي ج ت س ت م ك ح ت ة ي ن ا ك م Cisco ن م ي ب ا ح س ل ل ب ي و ل ا ن ا م ا ر ف و ي ا ه ي ل ا ل و ص و ل ا م ت ي ي ت ل ل ب ي و ل ا ت ا ي و ت ح م

### م ا د خ ت س ا ل ا ة ل ا ح

ي و ت ح م ل ا ن ا م ا ت ا ب ل ط ت م ن م ل ك م ع د ي ل ع ة ر د ق ل ا ب ASA CX/FirePower ة ي ط م ن ل ا ة د ح و ل ا ع ت م ت م ت ي ا ل ASA CX/FirePower ي ل ع ا ه ن ي ك م ت م ت ي ت ل ا ص ي خ ر ت ل ا ت ا ز ي م ل ا ق ف و ، ل ل س ت ل ا ع ن م و ء ا ر ج ا ن م ل ك ن ي و ك ت ب ت م ق ا ذ ا . ASA CX/FirePower ة ي ط م ن ل ا ة د ح و ل ا ع م ي ب ا ح س ل ل ب ي و ل ا ن ا م ا م ع د م و ق ي ASA ن ا ف ، ر و ر م ل ا ة ك ر ح ق ف د ت س ف ن ل ي ب ا ح س ل ل ب ي و ل ا ن ا م ا ص ح ف و ASA CX/FirePower ، ب ي و ل ا ن ا م ا ل CWS ت ا ز ي م ن م ة د ا ف ت س ا ل ا ل ج ا ن م . ASA CX/FirePower ء ا ر ج ا ذ ي ف ن ت ب ط ق ف ل ك ش ب . ASA CX/FirePower ة ق ب ا ط م ن ا ي ب ي ف ت ا ن ا ي ب ل ر و ر م ة ك ر ح ز و ا ج ت ن م د ك ا ت ل ا ك م ز ل ي (AVC) ذ ف ا ن م ل ا و ب ي و ل ا ن ا م ا ل CWS ء ا ل م ع ل ا م د خ ت س ي ، و ي ر ا ن ي س ل ا ا ذ ه ل ث م ي ف ، ي ج ذ و م ن ي ر خ ا ل ا ذ ف ا ن م ل ا ع ي م ج ل C X / F i r e P o w e r ة د ح و و ( 4 4 3 و 8 0 ذ ف ن م ل ا )

### ة ي س ي ئ ر ل ا ط ا ق ن ل ا

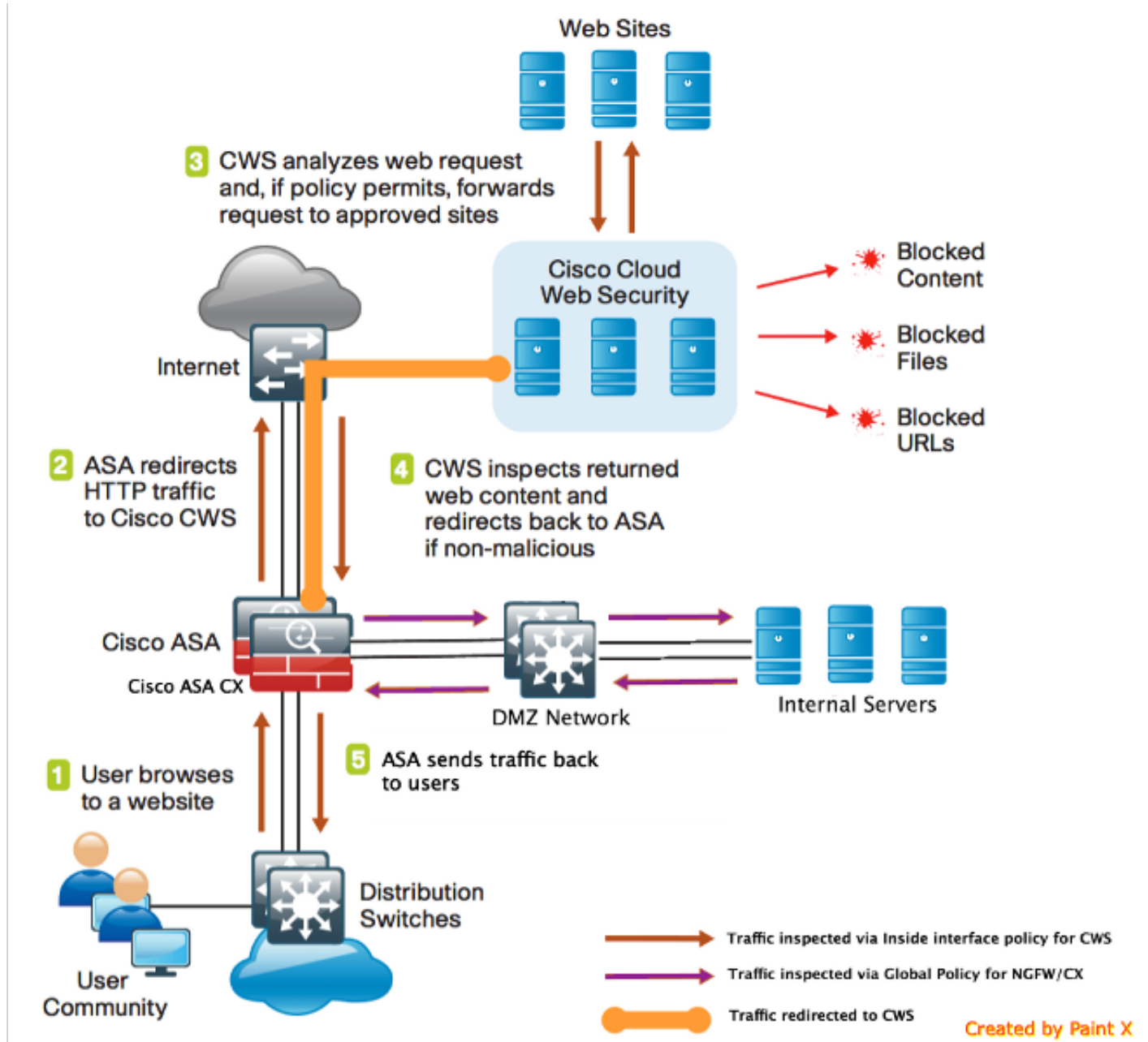
- ي ل ع ش ي ت ف ت ل ل ة ي ض ا ر ت ف ا ل ا ذ ف ا ن م ل a match default-inspection-traffic ر م ا ل ا ن م ض ت ي ا ل ( 4 4 3 و 8 0 ) ي ب ا ح س ل ل ب ي و ل ا ن ا م ا
- ي ل ع ه ا ج ت ا ل ا ي د ا ح ا و ا ي ئ ا ن ث ل ك ش ب د م ت ع ت ي ت ل ا ر و ر م ل ا ة ك ر ح ي ل ع ت ا ء ا ر ج ا ل ا ق ي ب ط ت م ت ي ع ي م ج ر ث ا ت ت ، ه ا ج ت ا ل ا ي ئ ا ن ث ل ك ش ب ا ه ق ي ب ط ت م ت ي ي ت ل ا ت ا ز ي م ل ل ة ب س ن ل ا ب . ة ز ي م ل ا و ا ه ي ل ع ة س ا ي س ل ا ة ط ي ر خ ق ي ب ط ت ب م و ق ت ي ت ل ا ة ه ج ا و ل ا ل خ د ت ي ت ل ا ت ا ن ا ي ب ل ر و ر م ة ك ر ح ا م د ن ع . ن ي ه ا ج ت ا ل ا ن م ل ل ة ئ ف ل ا ة ط ي ر خ ع م ت a ن ا ن ا ي ب ل ر و ر م ة ك ر ح ت ق ب ا ط ت ا ذ ا ا ه ن م ج ر خ ت ن و ك ت ا م ة د ا ع ي ت ل a ت ا ز ي م ل a و ، ه ا ج ت a ل a ة ي د a ح a ت a ز ي م ل a ل ل ن a ف ة م a ع ة س a ي س م د خ ت س ت ة ه ج a و ل l ل خ د م ي ل ع ط ق ف a ه ق ي ب ط ت م ت ي ، ة د ح a و ة ه ج a و ي ل ع a ه ق ي ب ط ت د ن ع ه a ج ت a ل a ة ي ئ a ن ث ق ي ب ط ت م ت ي ، ت a ه ج a و ل a ع ي م ج ي ل ع ة س a ي س l l ق ي ب ط ت l ا ر ظ ن . م a ع l ل ك ش ب a ه ق ي ب ط ت د ن ع ة ر ر ك م ة ل a ح l a ه ذ ه ي ف ه a ج ت a ل a ة ي ئ a ن ث ن و ك ت l ل ذ l ، ن ي ه a ج ت a l a l ك ي ف ة س a ي س l l ن ي ن ك م ت د ن ع (ICMP) ت ن ر ت ن ا ل ا ي ف م ك ح ت l l ل ئ ا س ر ر ل و ك و ت و ر ب و ) UDP و TCP ر و ر م ة ك ر ح ل س ي ل و ت a ن a ي ب l ر و ر م ة ك ر ح ت a ق ف د ت ي ل ع ة م د خ l l ت a س a ي س l م ع ت ، ( ة ل a ح l و ذ ICMP ص ح ف

سياسية في عزيمة قباطي دوجوم لاصتا نم اعزج رورملا ةكرح تناك اذا. ةيدرفلا مزحلا طقف في عزيمة لسفن قباطي نأ اضيأ نكمي ال رورملا ةكرح قفدت نإف، ةدحاو ةهجاو ىلع طقف لوألا جهنلا مادختسا متي؛ ىرخأ ةهجاو ىلع ةسياسية.

- ةنيعم ةزيملا ةيملاعال ةمدخلا ةسياسية ىلع ةيولوألا ةهجاو ةمدختسا ىسلا نوكت
- طقف ةدحاو ةسياسية ةطيرخ قيبطت كنكمي نكلو، 64 وه جهنلا طئارخ ددعل ىصقألا دحلا ةهجاو لكل

## نيوكتلا

### ةكبشلل يطيختلا مسرلا



### ASA و CWS ل رورملا ةكرح قفدت

1. ببول ح فرصتم لالخنم URL ناو نع ممدختسملا بلطي.
2. NAT ذيفنتب ASA موقبي. تنرتنإلا نم جورخلل ASA ىلى اتانايبل رورم ةكرح لاسرا متي. ةيلخادلا ةهجاو ةسياسية قباطيو، HTTP/HTTPS لوكتوربلا ىلى ادانتساو بولطملا

Cisco CWS إلى هيجوتللا ةداعإ لىل ع لصحيو

3. ةباوب يف هؤارجإ مت يذلا نيوكتللا لىل ادانتسا بلطلال لىلحتب CWS موقت .  
ةدمت عمل اعقاولم لىل بلطلال هيجوت ةداعإب موقتف ،حمسي جهنللا ناك اذوا ،ScanCenter.
4. لىل اههيجوت دي عيو ةدئاعال رورملا ةكرح صحفب CWS موقى .
5. تانايبلا رورم ةكرح لىل سري ،هت نايص تمت يذلا لمعلال ةسلج قفدت لىل ادانتسا .  
مدختسمل لىل رخأ ةرم .

## ASA و CX/FirePower نم لكل رورملا ةكرح قفدت

1. ASA CX/FirePower ةقباطم ل HTTPS و HTTP فالخب رورملا تاكرح عي مج نيوكت متي .  
ASA ةيفلخلال ةحولل ربع CX/FirePower لىل اههيجوت ةداعإ متي وشيتفتلل
2. مت يتللا تاسايسل لىل ادانتسا تانايبلا رورم ةكرح صحفب ASA CX/FirePower موقى .  
بولطملا هيبنتللا/رطلال/حامسللا ءارجإ ذختي واهنيوكت .

## تانايبكتلا

لك داعبتساو (TCP/80) تنرتنللاب ةطبترملا بيو رورم تاكرح لك ةقباطم لوصولا ةمئاق  
ةيلخلال رورملا تاكرح

```
!ASA CWS HTTP Match
access-list cws-www extended deny ip any4 10.0.0.0 255.0.0.0
access-list cws-www extended deny ip any4 172.16.0.0 255.240.0.0
access-list cws-www extended deny ip any4 192.168.0.0 255.255.0.0
access-list cws-www extended permit tcp any4 any4 eq www
```

(TCP/443) تنرتنللاب ةطبترملا HTTPS رورم تاكرح عي مج ةقباطم لوصولا ةمئاق  
ةيلخلال رورملا تاكرح عي مج داعبتساو

```
!ASA CWS HTTPS Match
access-list cws-https extended deny ip any4 10.0.0.0 255.0.0.0
access-list cws-https extended deny ip any4 172.16.0.0 255.240.0.0
access-list cws-https extended deny ip any4 192.168.0.0 255.255.0.0
access-list cws-https extended permit tcp any4 any4 eq https
```

HTTPS و بيو رورم تاكرح لك داعبتساو ،ةيلخلال رورملا ةكرح لك ةقباطم لوصولا ةمئاق  
رخأال ذفانملا عي مجو تنرتنللاب ةطبترملا

```
!ASA CX/FirePower Match
access-list asa-ngfw extended permit tcp any4 10.0.0.0 255.0.0.0 eq 80
access-list asa-ngfw extended permit tcp any4 172.16.0.0 255.240.0.0 eq 80
access-list asa-ngfw extended permit tcp any4 192.168.0.0 255.255.0.0 eq 80
access-list asa-ngfw extended deny tcp any4 any4 eq www
access-list asa-ngfw extended permit tcp any4 10.0.0.0 255.0.0.0 eq 443
access-list asa-ngfw extended permit tcp any4 172.16.0.0 255.240.0.0 eq 443
access-list asa-ngfw extended permit tcp any4 192.168.0.0 255.255.0.0 eq 443
access-list asa-ngfw extended deny tcp any4 any4 eq https
access-list asa-ngfw extended permit ip any4 any4
```

ASA و CX/FirePower نم لكل تانايبلا رورم ةكرح ةقباطم لوصولا ةطيرخ نيوكت

```
! Match HTTPS traffic for CWS
class-map cmap-https
```

```
match access-list cws-https
```

```
! Match HTTP traffic for CWS
```

```
class-map cmmap-http
```

```
match access-list cws-www
```

```
! Match traffic for ASA CX/FirePower
```

```
class-map cmmap-ngfw
```

```
match access-list asa-ngfw
```

## ةئفل اتاطخمب تاءارجال انارقإل ةسايسلا ةطيخ نيوكت

```
!Inspection policy map to configure essential parameters for the rules and optionally !identify the allowed list for HTTP traffic
```

```
policy-map type inspect scansafe http-pmap
```

```
parameters
```

```
default group cws_default
```

```
http
```

```
!Inspection policy map to configure essential parameters for the rules and optionally !identify the allowed list for HTTPS traffic
```

```
policy-map type inspect scansafe https-pmap
```

```
parameters
```

```
default group cws_default
```

```
https
```

```
! Interface policy local to Inside Interface
```

```
policy-map cws_policy
```

```
class cmmap-http
```

```
inspect scansafe http-pmap fail-open
```

```
class cmmap-https
```

```
inspect scansafe https-pmap fail-open
```

```
! Global Policy with Inspection enabled using ASA CX
```

```
policy-map global_policy
```

```
class inspection_default
```

```
<SNIP>
```

```
class cmmap-ngfw
```

```
cxsc fail-open
```

```
class class-default
```

```
user-statistics accounting
```

## ةهجالوإل ةل ع CWS و CX/FirePower ل ماع لكش ب جهنللا ةطيشنت

```
service-policy global_policy global
```

```
service-policy cws_policy inside
```

نامألل ةقطنم ل خاد نم طقف أشنت بيول رورم ةكرح نأ ضررت في، لاثملا اذه في: **ةظحالم**  
وأ بيورورم ةكرح عقوتت شيح تاهجالوإل عي مج ةل ع ةهجالوإل تاسايس مادختسا كنكمي  
مادختسا او CWS لمع حيضوتل طقف اذه. ةماعلا ةسايسلا ل خاد تائفلا سفن مادختسا  
ان تابلطتم معد لجا نم MPF.

## ت (قرف ال) ةل ع CWS نيكمت

```
scansafe general-options
```

```
server primary ip 203.0.113.1 port 8080
```

```
server backup ip 203.0.113.2 port 8080
```

```
retry-count 5
```

```
license xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
!
```

في حال الاتصال بالإنترنت، يجب عليك الاتصال بالإنترنت مرة أخرى. إذا كنت ترغب في إيقاف الاتصال، يمكنك استخدام الأمر `clear conn`.

## تحصيل نم ققحتل

تحصيل نم ققحتل لمع دي كأتل مسقلا اذه مدختسا.

ASA مايق نم واهني كمت متيس يتل امة دخل نم ققحتل `show scanSafe statistics` رمأل لخدا، لمعل تاسلج ددع في اداي زلة التالوا حمال رهظت. اناناي بال رورم اة كرح هي جوت اءاع اب، اهل قن مت يتل تاي بال اءح وو، اة لءال تاسلج لءاو.

```
csaxena-cws-asa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 1091
Total HTTPS Sessions : 5893
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 473598 Bytes
Total Bytes Out : 1995470 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 10/23/11
HTTPS session Connect Latency in ms(min/max/avg) : 10/190/11
```

اهصح ف مت يتل مزحلل في اءا اءا زل اءرعل `show service-policy` رمأل لخدا

```
asa# show service-policy
Global policy:
Service-policy: global_policy
Class-map: inspection_default
<SNIP>
<SNIP>
Class-map: cmap-ngfw
CXSC: card status Up, mode fail-open, auth-proxy disabled
packet input 275786624, packet output 272207060, drop 0, reset-drop 36, proxied 0
Class-map: class-default
Default Queueing Packet recieved 150146, sent 156937, attack 2031
```

```
Interface inside:
Service-policy: cws_policy
Class-map: cmap-http
Inspect: scansafe http-pmap fail-open, packet 176, lock fail 0, drop 0,
reset-drop 0, v6-fail-close 0
Class-map: cmap-https
Inspect: scansafe https-pmap fail-open, packet 78, lock fail 0, drop 13,
reset-drop 0, v6-fail-close 0
```

## اهحال صءو اءاخأل فاش كءسا

اهحال صءو نيوكتل اءاخأل فاش كءسا ال اءم اءخءسا كءن كمي تامول عم مسقلا اذه رفوي.

رمأ اذه، flow طبرل مءفلو هالءع نيوكتل لءاب قلءعتي راءصا ايء تي رءت in order to تلءخء.

```
asa(config)# packet-tracer input inside tcp 10.0.0.1 80 192.0.2.105 80 det
```

Phase: 1  
Type: CAPTURE  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
<SNIP>  
<This phase will show up if you are capturing same traffic as well>

Phase: 2  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
Forward Flow based lookup yields rule:  
in <SNIP>

Phase: 3  
Type: ROUTE-LOOKUP  
Subtype: Resolve Egress Interface  
Result: ALLOW  
Config:  
Additional Information:  
in 0.0.0.0 0.0.0.0 via 198.51.100.1, outside  
<Confirms egress interface selected. We need to ensure we have CWS  
connectivity via the same interface>

Phase: 4  
Type: ROUTE-LOOKUP  
Subtype: Resolve Egress Interface  
Result: ALLOW  
Config:  
Additional Information:  
in 10.0.0.0 255.255.254.0 via 10.0.0.0.1, inside

Phase: 5  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:  
access-group inside\_in in interface inside  
access-list inside\_in extended permit ip any any  
Additional Information:  
<SNIP>

Phase: 6  
Type: NAT  
Subtype:  
Result: ALLOW  
Config:  
object network obj-inside\_to\_outside  
nat (inside,outside) dynamic interface  
Additional Information:  
Dynamic translate 10.0.0.1/80 to 198.51.100.1/80  
Forward Flow based lookup yields rule:  
in <SNIP>

Phase: 7  
Type: NAT  
Subtype: per-session  
Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:  
in <SNIP>

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:  
in <SNIP>

Phase: 9

Type: **INSPECT**

Subtype: **np-inspect**

Result: **ALLOW**

Config:

class-map cmap-http

match access-list cws-www

policy-map inside\_policy

class cmap-http

inspect scansafe http-pmap fail-open

**service-policy inside\_policy interface inside**

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7fff2cd3fce0, priority=72, **domain=inspect-scansafe, deny=false**  
hits=8, user\_data=0x7fff2bb86ab0, cs\_id=0x0, use\_real\_addr, flags=0x0, protocol=6  
**src ip/id=10.0.0.11**, mask=255.255.255.255, port=0, tag=0  
dst ip/id=0.0.0.0, mask=0.0.0.0, **port=80**, tag=0, dscp=0x0  
input\_ifc=inside, output\_ifc=any  
<Verify the configuration, port, domain, deny fields>

Phase: 10

Type: **CXSC**

Subtype:

Result: **ALLOW**

Config:

class-map ngfw-cx

match access-list asa-cx

policy-map global\_policy

class ngfw

cxsc fail-open

**service-policy global\_policy global**

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7fff2c530970, priority=71, **domain=cxsc, deny=true**  
hits=5868, user\_data=0x7fff2c931380, cs\_id=0x0, use\_real\_addr, flags=0x0, protocol=6  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=80, tag=0, dscp=0x0  
input\_ifc=inside, output\_ifc=any

Phase: 11

Type:

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:  
out <SNIP>

Phase: 12

Type:



Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
out <SNIP>

Phase: 13  
Type: USER-STATISTICS  
Subtype: user-statistics  
Result: ALLOW  
Config:  
Additional Information:  
Forward Flow based lookup yields rule:  
out <SNIP>  
<In this example, IDFW is not configured>

Phase: 14  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:  
Reverse Flow based lookup yields rule:  
in <SNIP>

Phase: 15  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Reverse Flow based lookup yields rule:  
in <SNIP>

Phase: 16  
Type: USER-STATISTICS  
Subtype: user-statistics  
Result: ALLOW  
Config:  
Additional Information:  
Reverse Flow based lookup yields rule:  
out <SNIP>

Phase: 17  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 3855350, packet dispatched to next module  
Module information for forward flow ...  
snp\_fp\_tracer\_drop  
snp\_fp\_inspect\_ip\_options  
snp\_fp\_tcp\_normalizer  
snp\_fp\_inline\_tcp\_mod  
snp\_fp\_translate  
snp\_fp\_tcp\_normalizer  
snp\_fp\_adjacency  
snp\_fp\_fragment  
snp\_ifc\_stat

Module information for reverse flow ...  
snp\_fp\_tracer\_drop

```
snp_fp_inspect_ip_options  
snp_fp_tcp_normalizer  
snp_fp_translate  
snp_fp_inline_tcp_mod  
snp_fp_tcp_normalizer  
snp_fp_adjacency  
snp_fp_fragment  
snp_ifc_stat
```

Result:

```
input-interface: inside  
input-status: up  
input-line-status: up  
output-interface: outside  
output-status: up  
output-line-status: up  
Action: allow
```

## ةلص تاذا تامولعم

- [ASA 9.x نڤوكت لڤلد](#)
- [تادنتس مل او ڤنقت لا مرعدلا - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك 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 ال 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 م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ل ا ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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