ASA met CX/FirePower Module en Configuratievoorbeeld van CWS-connector

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) kunt gebruiken met de module Context Aware (CX), ook bekend als de Next Generation Firewallondersteuning en Cisco Cloud Web Security (CWS) Connector.

Voorwaarden

Vereisten

Cisco raadt u aan:

- 3DES/AES-licentie op ASA (gratis licentie)

- Geldige CWS-service/licentie voor gebruik van CWS voor het vereiste aantal gebruikers
- Toegang tot ScanCenter Portal voor het genereren van de verificatie-toets

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Toepassingsgebied

In dit document worden deze gebieden van technologie en producten beschreven:

- Cisco ASA 5500-X Series adaptieve security applicaties biedt beveiliging tegen firewalls en inbraakpreventie op internet.
- Cisco Cloud Web Security biedt granulaire controle over alle webinhoud die benaderd wordt.

Case gebruiken

De ASA CX/FirePower-module heeft de mogelijkheid om zowel de Content Security als de Inbraakpreventievereisten te ondersteunen, afhankelijk van de licentiefuncties die op de ASA CX/FirePower zijn ingeschakeld. Cloud Web security wordt niet ondersteund met de ASA CX/FirePower-module. Als u zowel de ASA CX/FirePOWER-actie als de Cloud Web Security inspectie voor dezelfde verkeersstroom configureren voert de ASA alleen de ASA CX/FirePower-actie uit. Om de CWS-functies voor Web Security te kunnen gebruiken, moet u ervoor zorgen dat het verkeer niet wordt gepasseerd in het wedstrijdoverzicht van ASA CX/FirePower. Meestal zullen klanten in zo'n scenario CWS gebruiken voor Web Security en AVC (poort 80 en 443) en CX/FirePower Module voor alle andere poorten.

Belangrijkste punten

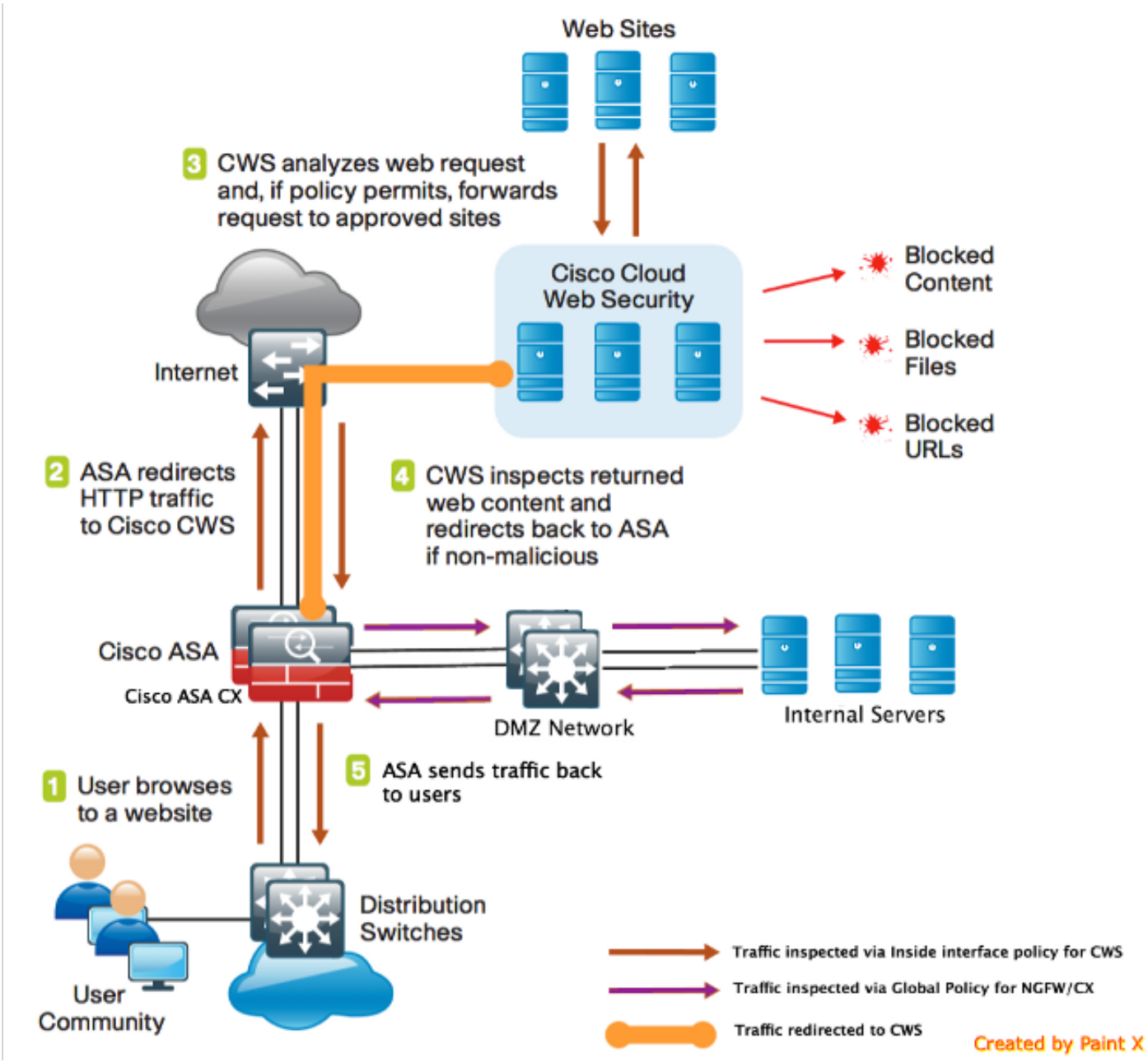
- De **standaard inspectie-verkeer** opdracht **maken** geen gebruik van de standaardpoorten voor de Cloud Web Security inspectie (80 en 443).
- Handelingen worden toegepast op verkeer dat tweezijdig of eenzijdig afhankelijk is van het kenmerk. Voor functies die bidirectioneel worden toegepast, wordt al het verkeer dat de interface ingaat of verlaat waarop u de beleidskaart toepast, beïnvloed als het verkeer de class map voor beide richtingen aanpast. Wanneer je een mondiaal beleid gebruikt, zijn alle kenmerken eenrichtings; kenmerken die gewoonlijk bidirectioneel zijn wanneer ze op één interface worden toegepast , zijn alleen van toepassing op de ingang van elke interface wanneer ze mondiaal worden toegepast . Omdat het beleid op alle interfaces wordt toegepast, wordt het beleid in beide richtingen toegepast, zodat in dit geval tweerichtingsaliteit overbodig is.
- Voor TCP- en UDP-verkeer (en Internet Control Message Protocol (ICMP), wanneer u een

stateful ICMP-inspectie toestaat), werkt het servicebeleid op verkeersstromen en niet alleen op afzonderlijke pakketten. Als het verkeer deel uitmaakt van een bestaande verbinding die een eigenschap in een beleid op één interface aanpast, kan de verkeersstroom niet dezelfde eigenschap in een beleid op een andere interface evenaren; alleen het eerste beleid wordt gebruikt .

- Het beleid van de interfacedienst heeft voorrang op het mondiale dienstenbeleid voor een bepaalde eigenschap.
- Het maximum aantal beleidskaarten is 64, maar je kunt slechts één beleidskaart per interface toepassen.

Configureren

Netwerkdiagram



Traffic Flow voor de ASA en CWS

1. De gebruiker vraagt de URL via de webbrowser.
2. Het verkeer wordt naar de ASA gestuurd om het internet te verlaten. ASA voert de vereiste NAT uit en is gebaseerd op het protocol HTTP/HTTPS, op overeenkomsten met het interne interfacebeleid en wordt opnieuw gericht naar Cisco CWS.
3. CWS analyseert het verzoek op basis van de configuratie die in het ScanCenter-portal is uitgevoerd en indien het beleid toestaat, stuurt u het verzoek naar goedgekeurde locaties.
4. CWS inspecteert het geretourneerde verkeer en wijst hetzelfde terug op ASA.
5. Op basis van de onderhouden sessiestroom stuurt ASA het verkeer terug naar de gebruiker.

Traffic Flow voor de ASA en CX/FirePower

1. Alle andere verkeer dan HTTP en HTTPS is geconfigureerd om aan de ASA CX/FirePower-inspectie te voldoen voor inspectie en wordt opnieuw naar CX/FirePower over de ASA-backplane geleid.
2. De ASA CX/FirePower inspecteert het verkeer op basis van de geconfigureerde beleidslijnen en neemt de vereiste toestaan/blokkeren/waarschuwende actie.

Configuraties

Toegangslijst met alle gelijk te stellen internet Bond Web (TCP/80) verkeer en sluit al intern verkeer uit

```
!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
```

Toegangslijst met alle HTTPS-verbindingen (TCP/443) die voldoen aan alle interne verkeer

```
!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
```

Toegangslijst voor alle interne verkeer, met uitzondering van alle internetgebonden web- en HTTPS-verkeer en alle andere poorten

```
!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
```

Klasse Map configuratie aan verkeer aangepast voor CWS en CX/FirePOWER

```
! Match HTTPS traffic for CWS
class-map cmap-https
match access-list cws-https

! Match HTTP traffic for CWS
class-map cmap-http
match access-list cws-www

! Match traffic for ASA CX/FirePower
class-map cmap-ngfw
match access-list asa-ngfw
```

Policy Map Configuration voor het koppelen van acties met klaskaarten

```
!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 cmap-http
inspect scansafe http-pmap fail-open
class cmap-https
inspect scansafe https-pmap fail-open

! Global Policy with Inspection enabled using ASA CX
policy-map global_policy
class inspection_default
<SNIP>
class cmap-ngfw
cxsc fail-open
class class-default
user-statistics accounting
```

Mondiaal beleid voor CX/FirePOWER en CWS op de interface activeren

```
service-policy global_policy global
service-policy cws_policy inside
```

> **Opmerking:** In dit voorbeeld wordt aangenomen dat internetverkeer alleen van binnen de veiligheidszone afkomstig is. U kunt interfacebeleid op alle interfaces gebruiken waar u web verkeer verwacht of dezelfde klassen binnen het globale beleid gebruikt. Dit is alleen maar om de werking van CWS en het gebruik van MPF aan te tonen teneinde onze behoefte te ondersteunen.

CWS op de ASA inschakelen (geen verschil)

```
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 xxxxxxxxxxxxxxxxxxxxxxxxxxxx
!
```

Om ervoor te zorgen dat alle verbindingen het nieuwe beleid gebruiken, moet u de huidige verbindingen loskoppelen zodat ze weer met het nieuwe beleid kunnen worden verbonden. Zie de **heldere verbinding** of de **duidelijke lokaal-host** opdrachten.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Voer de opdracht **show scansafe statistics in** om de dienst te controleren die wordt ingeschakeld en om de ASA om te leiden. De volgende pogingen tonen de toename in aantal sessies, huidige sessies, en bytes overgebracht.

```
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
```

Voer de opdracht **showservice-beleid in** om de stappen in geïnspecteerde pakketten te zien

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Om problemen met de bovenstaande configuratie op te lossen en de pakketstroom te begrijpen, voert u deze opdracht in:

```
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
```

Gerelateerde informatie

- ASA 9900x-configuratiegids
- Technische ondersteuning en documentatie – Cisco Systems