Esempio di configurazione di ASA con modulo CX/FirePower e connettore CWS

Sommario

Introduzione

In questo documento viene descritto come usare Cisco Adaptive Security Appliance (ASA) con il modulo Context Aware (CX), noto anche come Next Generation Firewall, e Cisco Cloud Web Security (CWS) Connector.

Prerequisiti

Requisiti

Cisco raccomanda:

- Licenza 3DES/AES su ASA (licenza gratuita)
- Servizio/licenza CWS valido per utilizzare CWS per il numero richiesto di utenti
- Accesso al portale ScanCenter per generare la chiave di autenticazione

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Ambito

Questo documento illustra le seguenti aree di tecnologia e prodotti:

- Cisco ASA serie 5500-X Adaptive Security Appliance fornisce la sicurezza del firewall ai margini di Internet e la prevenzione delle intrusioni.
- Cisco Cloud Web Security fornisce un controllo granulare su tutto il contenuto Web a cui si accede.

Scenario d'uso

Il modulo ASA CX/FirePower è in grado di supportare i requisiti di sicurezza dei contenuti e di prevenzione delle intrusioni, a seconda delle funzionalità di licenza abilitate su ASA CX/FirePower. Cloud Web Security non è supportato con il modulo ASA CX/FirePower. Se si configura sia l'azione ASA CX/FirePower che l'ispezione Cloud Web Security per lo stesso flusso di traffico, l'ASA esegue solo l'azione ASA CX/FirePower. Per utilizzare le funzionalità di CWS per Web Security, è necessario verificare che il traffico venga ignorato nell'istruzione match per ASA CX/FirePower. In questo scenario, i clienti utilizzano in genere CWS per Web Security e AVC (porte 80 e 443) e il modulo CX/FirePower per tutte le altre porte.

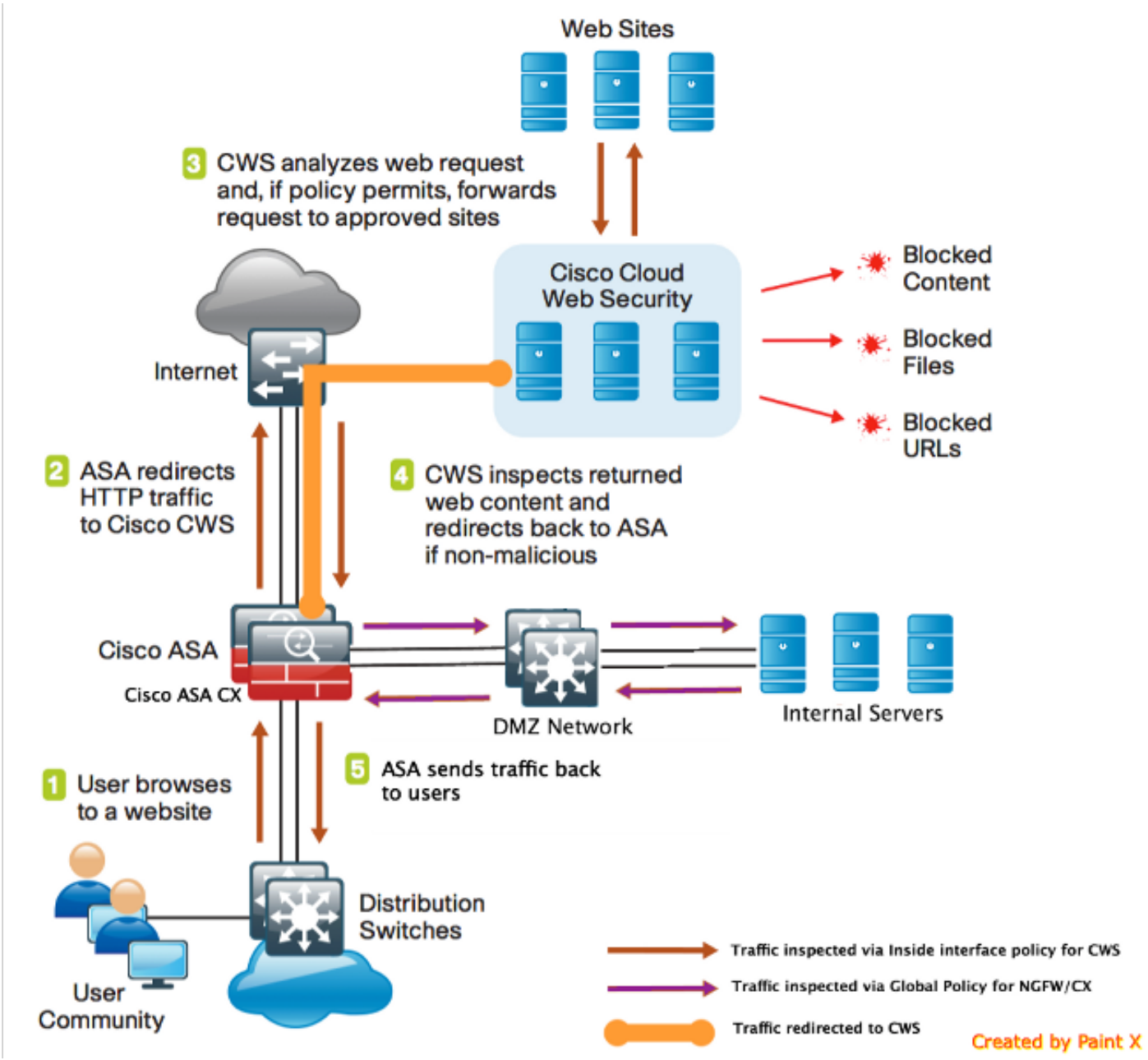
Punti chiave

- Il comando **match default-Inspection-traffic** non include le porte predefinite per l'ispezione di Cloud Web Security (80 e 443).
- Le azioni vengono applicate al traffico in modo bidirezionale o unidirezionale a seconda della funzionalità. Per le funzionalità applicate in modo bidirezionale, tutto il traffico in entrata o in uscita dall'interfaccia a cui si applica la mappa dei criteri viene influenzato se il traffico corrisponde alla mappa delle classi per entrambe le direzioni. Quando si utilizza un criterio globale, tutte le funzionalità sono unidirezionali; le funzioni che normalmente sono bidirezionali quando applicate a una singola interfaccia si applicano solo all'ingresso di ciascuna interfaccia quando applicate globalmente. Poiché il criterio viene applicato a tutte le interfacce, viene applicato in entrambe le direzioni, pertanto in questo caso la bidirezionalità è ridondante.

- Per il traffico TCP e UDP (e il protocollo ICMP (Internet Control Message Protocol) quando si abilita l'ispezione ICMP stateful), le policy del servizio funzionano sui flussi di traffico e non solo sui singoli pacchetti. Se il traffico fa parte di una connessione esistente che corrisponde a una funzionalità di un criterio su un'interfaccia, tale flusso di traffico non può corrispondere alla stessa funzionalità di un criterio su un'altra interfaccia; viene utilizzato solo il primo criterio.
- I criteri dei servizi di interfaccia hanno la precedenza sui criteri dei servizi globali per una determinata funzionalità.
- Il numero massimo di mappe criteri è 64, ma è possibile applicare una sola mappa criteri per interfaccia.

Configurazione

Esempio di rete



Flusso del traffico per l'ASA e il CWS

1. L'utente richiede l'URL tramite il browser Web.
2. Il traffico viene inviato all'appliance ASA per uscire da Internet. L'ASA esegue il NAT richiesto e, in base al protocollo HTTP/HTTPS, corrisponde ai criteri dell'interfaccia interna e viene reindirizzata a Cisco CWS.
3. CWS analizza la richiesta in base alla configurazione eseguita nel portale ScanCenter e, se i criteri lo consentono, inoltra la richiesta ai siti approvati.
4. CWS controlla il traffico restituito e lo reindirizza all'ASA.
5. In base al flusso di sessione mantenuto, l'ASA invia il traffico all'utente.

Flusso del traffico per ASA e CX/FirePower

1. Tutto il traffico diverso da HTTP e HTTPS è configurato in modo da corrispondere ad ASA CX/FirePower per l'ispezione e viene reindirizzato a CX/FirePower sul backplane ASA.
2. ASA CX/FirePower controlla il traffico in base alle policy configurate ed esegue l'azione di autorizzazione/blocco/avviso richiesta.

Configurazioni

Elenco degli accessi per trovare la corrispondenza con tutto il traffico Web associato a Internet (TCP/80) ed escludere tutto il traffico interno

```
!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
```

Elenco accessi per trovare la corrispondenza con tutto il traffico HTTPS (TCP/443) associato a Internet ed escludere tutto il traffico interno

```
!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
```

Elenco degli accessi per trovare la corrispondenza con tutto il traffico interno, escludere tutto il traffico Web e HTTPS associato a Internet e tutte le altre porte

```
!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
```

Configurazione mappa classi per la corrispondenza del traffico per CWS e 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
```

Configurazione mappa criteri per associare azioni a mappe classi

```
!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
```

Attivazione globale di regole per CX/FirePower e CWS sull'interfaccia

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

> **Nota:** Nell'esempio si presume che il traffico Web provenga solo dall'interno dell'area di sicurezza. È possibile utilizzare i criteri di interfaccia su tutte le interfacce in cui si prevede il traffico Web o utilizzare le stesse classi all'interno del criterio globale. Questo è solo per dimostrare il funzionamento di CWS e l'uso di MPF per sostenere il nostro requisito.

Abilitare CWS sull'appliance ASA (nessuna differenza)

```
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
!
```

Per garantire che tutte le connessioni utilizzino il nuovo criterio, è necessario disconnettere le connessioni correnti in modo che possano riconnettersi al nuovo criterio. Vedere i comandi **clear conn** o **clear local-host**.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Immettere il comando **show scansafe statistics** per verificare che il servizio sia abilitato e che l'ASA reindirizzi il traffico. I tentativi successivi mostrano l'incremento nel numero di sessioni, sessioni correnti e byte trasferiti.

```
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
```

Immettere il comando **show service-policy** per verificare gli incrementi dei pacchetti ispezionati

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per risolvere i problemi relativi alla configurazione indicata sopra e capire il flusso del pacchetto, immettere questo comando:

```
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
```

Informazioni correlate

- Guida alla configurazione di ASA 9.x
- Documentazione e supporto tecnico – Cisco Systems