Ejemplo de Configuración de ASA con Módulo CX/FirePower y Conector CWS

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Alcance
caso de uso
Puntos clave
Configurar
Diagrama de la red
Flujo de tráfico para ASA y CWS
Flujo de tráfico para ASA y CX/FirePower
Configuraciones
Lista de acceso para hacer coincidir todo el tráfico web enlazado a Internet (TCP/80) y excluir todo el tráfico interno
Lista de acceso para hacer coincidir todo el tráfico HTTPS (TCP/443) enlazado a Internet y excluir todo el tráfico interno
Lista de acceso para coincidir con todo el tráfico interno, excluya todo el tráfico web y HTTPS vinculado a Internet y todos los demás puertos
Configuración de mapa de clase para hacer coincidir el tráfico tanto para CWS como para CX/FirePower
Configuración de Policy Map para Asociar Acciones con Mapas de Clase
Activar la política globalmente para CX/FirePower y CWS en la interfaz
Habilitar CWS en ASA (sin diferencias)
Verificación
Troubleshoot
Información Relacionada

Introducción

Este documento describe cómo utilizar Cisco Adaptive Security Appliance (ASA) con el módulo Context Aware (CX), también conocido como firewall de última generación, y el conector Cisco Cloud Web Security (CWS).

Prerequisites

Requirements

Cisco recomienda que tenga:

- Licencia 3DES/AES en ASA (licencia gratuita)
- Licencia/servicio CWS válido para utilizar CWS para el número necesario de usuarios
- Acceso a ScanCenter Portal para generar la clave de autenticación

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Alcance

Este documento muestra estas áreas de tecnología y productos:

- Los dispositivos de seguridad adaptable Cisco ASA serie 5500-X proporcionan seguridad de firewall de la frontera de Internet y prevención de intrusiones.
- Cisco Cloud Web Security proporciona un control granular de todo el contenido web al que se accede.

caso de uso

El módulo ASA CX/FirePower tiene la capacidad de admitir tanto el requisito de seguridad de contenido como de prevención de intrusiones, según las funciones de licencia habilitadas en ASA CX/FirePower. Cloud Web Security no es compatible con el módulo ASA CX/FirePower. Si configura la acción ASA CX/FirePower y la inspección de Cloud Web Security para el mismo flujo de tráfico, ASA solo realiza la acción ASA CX/FirePower. Para aprovechar las funciones de CWS para Web Security, debe asegurarse de que el tráfico se omite en la sentencia match para ASA CX/FirePower. Normalmente, en este escenario, los clientes utilizarán CWS para Web Security y AVC (puertos 80 y 443) y el módulo CX/FirePower para todos los demás puertos.

Puntos clave

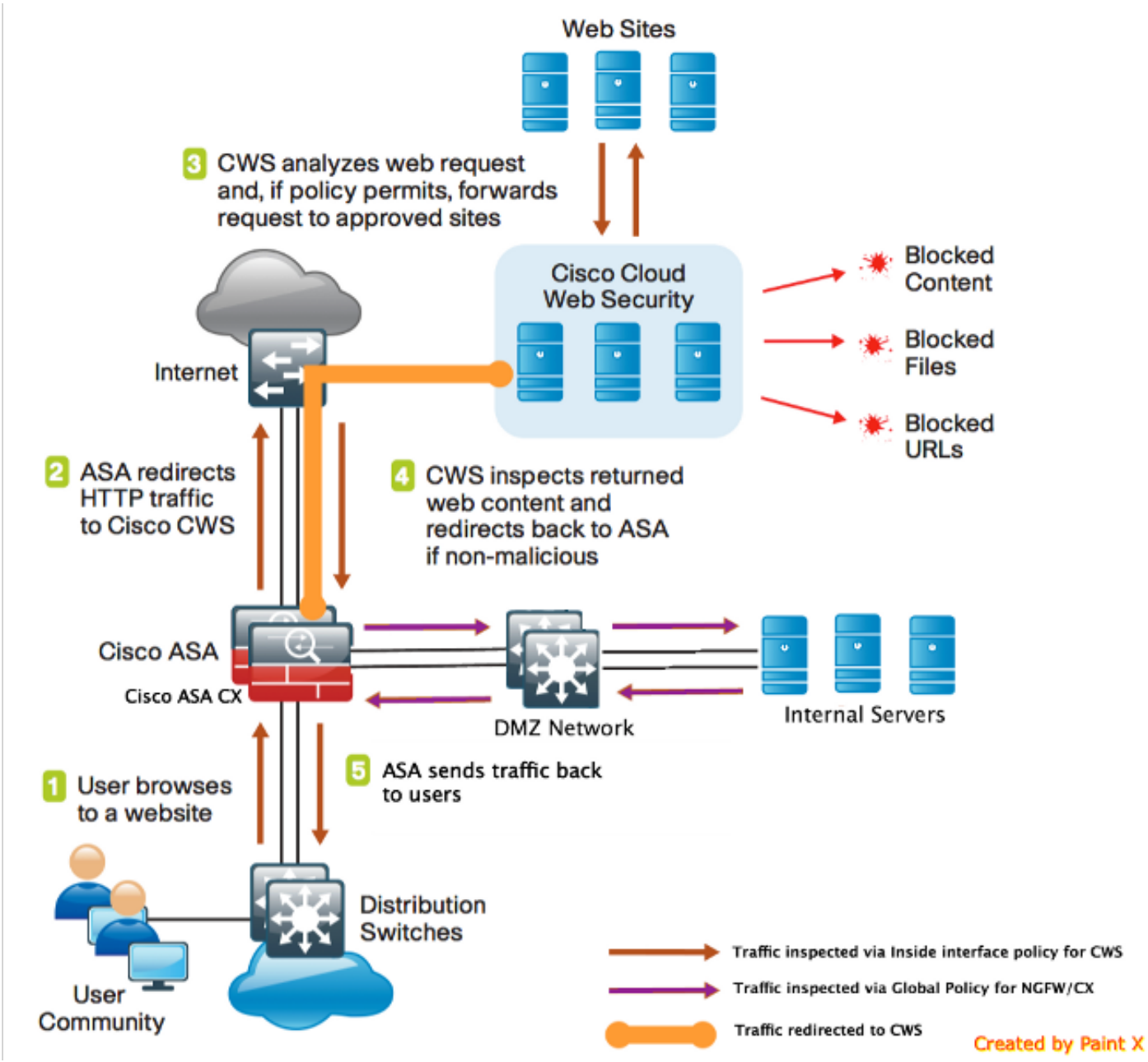
- El **comando match default-inspection-traffic** no incluye los puertos predeterminados para la inspección de Cloud Web Security (80 y 443).
- Las acciones se aplican al tráfico de forma bidireccional o unidireccional según la función. Para las funciones que se aplican bidireccionalmente, todo el tráfico que entra o sale de la interfaz a la que se aplica el policy map se ve afectado si el tráfico coincide con el class map para ambas direcciones. Cuando utiliza una política global, todas las funciones son unidireccionales; las funciones que normalmente son bidireccionales cuando se aplican a una sola interfaz sólo se aplican a la entrada de cada interfaz cuando se aplican globalmente. Debido a que la política se aplica a todas las interfaces, la política se aplica en ambas direcciones, por lo que la bidireccionalidad en este caso es redundante.
- Para el tráfico TCP y UDP (y el protocolo de mensajes de control de Internet (ICMP) cuando

se habilita la inspección ICMP con estado), las políticas de servicio funcionan en los flujos de tráfico y no sólo en los paquetes individuales. Si el tráfico es parte de una conexión existente que coincide con una función en una política en una interfaz, ese flujo de tráfico tampoco puede coincidir con la misma función en una política en otra interfaz; sólo se utiliza la primera política.

- Las políticas de servicio de interfaz tienen prioridad sobre la política de servicio global para una función determinada.
- El número máximo de mapas de política es 64, pero sólo puede aplicar un mapa de política por interfaz.

Configurar

Diagrama de la red



Flujo de tráfico para ASA y CWS

1. El usuario solicita la URL a través del navegador web.
2. El tráfico se envía al ASA para salir de Internet. El ASA realiza la NAT necesaria y se basa en el protocolo HTTP/HTTPS, coincide con la política de interfaz interna y se redirige a Cisco CWS.
3. CWS analiza la solicitud basándose en la configuración realizada en el portal de ScanCenter y, si la política lo permite, reenvía la solicitud a los sitios aprobados.
4. CWS inspecciona el tráfico devuelto y redirige lo mismo a ASA.
5. Según el flujo de sesión mantenido, ASA envía el tráfico de vuelta al usuario.

Flujo de tráfico para ASA y CX/FirePower

1. Todo el tráfico que no sea HTTP y HTTPS se configura para que coincida con ASA CX/FirePower para su inspección y se redirige a CX/FirePower a través de la placa de interconexiones ASA.
2. ASA CX/FirePower inspecciona el tráfico en función de las políticas configuradas y realiza la acción necesaria para permitir/bloquear/alertar.

Configuraciones

Lista de acceso para hacer coincidir todo el tráfico web enlazado a Internet (TCP/80) y excluir todo el tráfico 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
```

Lista de acceso para hacer coincidir todo el tráfico HTTPS (TCP/443) enlazado a Internet y excluir todo el tráfico 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
```

Lista de acceso para coincidir con todo el tráfico interno, excluya todo el tráfico web y HTTPS vinculado a Internet y todos los demás puertos

```
!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
```

Configuración de mapa de clase para hacer coincidir el tráfico tanto para CWS como para 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
```

Configuración de Policy Map para Asociar Acciones con Mapas de Clase

```
!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
```

Activar la política globalmente para CX/FirePower y CWS en la interfaz

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

> **Nota:** En este ejemplo, se asume que el tráfico web se origina solamente desde dentro de la zona de seguridad. Puede utilizar políticas de interfaz en todas las interfaces en las que espere tráfico web o utilizar las mismas clases dentro de la política global. Esto es sólo para demostrar el funcionamiento de CWS y el uso de MPF para apoyar nuestro requerimiento.

Habilitar CWS en ASA (sin diferencias)

```
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
!
```

Para asegurarse de que todas las conexiones utilicen la nueva política, debe desconectar las conexiones actuales para que puedan volver a conectarse con la nueva política. Vea los comandos **clear conn** o clear local-host.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Ingrese el comando **show scansafe statistics** para verificar el servicio que se debe habilitar y que ASA redirige el tráfico. Los intentos posteriores muestran el incremento en los recuentos de sesiones, las sesiones actuales y los bytes transferidos.

```
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
```

Ingrese el comando **show service-policy** para ver los incrementos en los paquetes inspeccionados

```
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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para resolver cualquier problema relacionado con la configuración anterior y comprender el flujo de paquetes, ingrese este 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
```

Información Relacionada

- Guía de configuración de ASA 9.x
- Soporte Técnico y Documentación - Cisco Systems