Exemple de configuration d'ASA avec module CX/FirePower et connecteur CWS

Contenu

Introduction

Ce document décrit comment utiliser l'appareil de sécurité adaptatif Cisco (ASA) avec le module Context Aware (CX), également appelé pare-feu de nouvelle génération, et le connecteur Cisco Cloud Web Security (CWS).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez :

- Licence 3DES/AES sur ASA (licence gratuite)

- Service/licence CWS valide pour utiliser CWS pour le nombre d'utilisateurs requis
- Accès au portail ScanCenter pour générer la clé d'authentification

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Informations générales

Portée

Ce document présente les domaines technologiques et les produits suivants :

- Les appareils de sécurité adaptatifs de la gamme Cisco ASA 5500-X assurent la sécurité du pare-feu de périphérie Internet et la prévention des intrusions.
- Cisco Cloud Web Security offre un contrôle granulaire sur l'ensemble du contenu Web accessible.

cas d’utilisation

Le module ASA CX/FirePower est capable de prendre en charge les exigences de sécurité du contenu et de prévention des intrusions, en fonction des fonctionnalités de licence activées sur ASA CX/FirePower. La solution de sécurité Web dans le cloud n'est pas prise en charge avec le module ASA CX/FirePower. Si vous configurez l'action ASA CX/FirePower et l'inspection Cloud Web Security pour le même flux de trafic, l'ASA exécute uniquement l'action ASA CX/FirePower. Afin de tirer parti des fonctionnalités CWS pour la sécurité Web, vous devez vous assurer que le trafic est ignoré dans l'instruction de correspondance pour ASA CX/FirePower. En règle générale, dans un tel scénario, les clients utilisent CWS pour la sécurité Web et AVC (ports 80 et 443) et le module CX/FirePower pour tous les autres ports.

Points clés

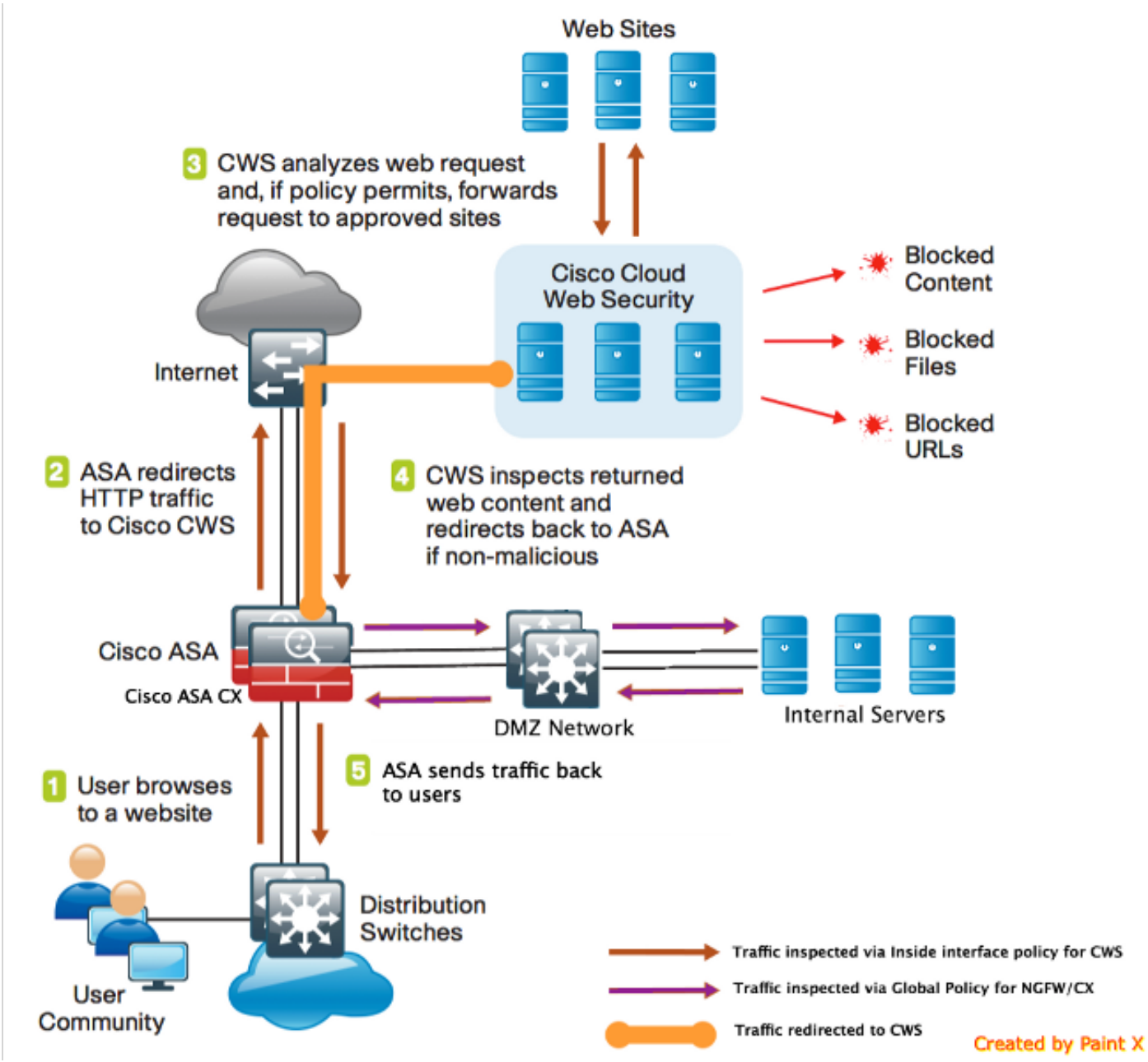
- La commande **match default-inspection-traffic** n'inclut pas les ports par défaut pour l'inspection Cloud Web Security (80 et 443).
- Les actions sont appliquées au trafic qui dépend de la fonction de manière bidirectionnelle ou unidirectionnelle. Pour les fonctionnalités appliquées de manière bidirectionnelle, tout le trafic entrant ou sortant de l'interface à laquelle vous appliquez la carte de stratégie est affecté si le trafic correspond à la carte de classe pour les deux directions. Lorsque vous utilisez une stratégie globale, toutes les fonctionnalités sont unidirectionnelles ; les fonctions qui sont normalement bidirectionnelles lorsqu'elles sont appliquées à une seule interface s'appliquent uniquement à l'entrée de chaque interface lorsqu'elles sont appliquées globalement. Étant donné que la stratégie est appliquée à toutes les interfaces, elle est appliquée dans les deux directions, de sorte que la bidirectionnalité est redondante dans ce cas.
- Pour le trafic TCP et UDP (et ICMP (Internet Control Message Protocol) lorsque vous activez

l'inspection ICMP dynamique), les politiques de service fonctionnent sur les flux de trafic et pas seulement sur les paquets individuels. Si le trafic fait partie d'une connexion existante qui correspond à une fonctionnalité d'une stratégie sur une interface, ce flux de trafic ne peut pas également correspondre à la même fonctionnalité dans une stratégie sur une autre interface ; seule la première stratégie est utilisée.

- Les stratégies de service d'interface ont priorité sur la stratégie de service globale pour une fonction donnée.
- Le nombre maximal de cartes de stratégie est de 64, mais vous ne pouvez appliquer qu'une seule carte de stratégie par interface.

Configuration

Diagramme du réseau



Flux de trafic pour ASA et CWS

1. L'utilisateur demande l'URL via le navigateur Web.
2. Le trafic est envoyé à l'ASA pour sortir d'Internet. L'ASA effectue la NAT requise et en fonction du protocole HTTP/HTTPS, correspond à la stratégie d'interface interne et est redirigé vers Cisco CWS.
3. CWS analyse la demande en fonction de la configuration effectuée dans le portail ScanCenter et, si la stratégie le permet, transmet la demande aux sites approuvés.
4. CWS inspecte le trafic retourné et redirige le trafic vers ASA.
5. En fonction du flux de session maintenu, ASA renvoie le trafic à l'utilisateur.

Flux de trafic pour ASA et CX/FirePower

1. Tout le trafic autre que HTTP et HTTPS est configuré pour correspondre à ASA CX/FirePower pour inspection et est redirigé vers CX/FirePower sur le fond de panier ASA.
2. ASA CX/FirePower inspecte le trafic en fonction des politiques configurées et prend les mesures d'autorisation/de blocage/d'alerte requises.

Configurations

Liste d'accès correspondant à tout le trafic Internet (TCP/80) et excluant tout le trafic interne

```
!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
```

Liste d'accès correspondant à tout le trafic HTTPS lié à Internet (TCP/443) et excluant tout le trafic interne

```
!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
```

Liste d'accès correspondant à tout le trafic interne, excluant tout le trafic Web et HTTPS lié à Internet et tous les autres ports

```
!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
```

Configuration de la carte de classe pour faire correspondre le trafic pour CWS et 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
```

Configuration de la carte de stratégie pour associer des actions à des mappages de classes

```
!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
```

Activer la stratégie globale pour CX/FirePower et CWS sur l'interface

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

> **Note**: Dans cet exemple, il est supposé que le trafic Web provient uniquement de l'intérieur de la zone de sécurité. Vous pouvez utiliser des stratégies d'interface sur toutes les interfaces sur lesquelles vous attendez du trafic Web ou utiliser les mêmes classes dans la stratégie globale. Il s'agit simplement de démontrer le fonctionnement de CWS et l'utilisation de MPF afin de répondre à nos besoins.

Activer CWS sur l'ASA (aucune différence)

```
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
!
```

Afin de vous assurer que toutes les connexions utilisent la nouvelle stratégie, vous devez déconnecter les connexions actuelles afin qu'elles puissent se reconnecter à la nouvelle stratégie. Reportez-vous aux commandes **clear conn** ou **clear local-host**.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Entrez la commande **show scansafe statistics** afin de vérifier le service à activer et que l'ASA redirige le trafic. Les tentatives suivantes montrent l'incrément dans le nombre de sessions, les sessions en cours et les octets transférés.

```
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
```

Entrez la commande **show service-policy** afin de voir les incréments dans les paquets inspectés

```
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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de résoudre les problèmes liés à la configuration ci-dessus et de comprendre le flux de

paquets, entrez cette commande :

```
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
```

Informations connexes

- Guide de configuration ASA 9.x
- Support et documentation techniques - Cisco Systems