Konfigurationsbeispiel für ASA mit CX/FirePower-Modul und CWS Connector

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Umfang
Anwendungsfall
Wichtigste Punkte
Konfigurieren
Netzwerkdiagramm
Datenverkehrsfluss für ASA und CWS
Datenverkehrsfluss für ASA und CX/FirePower
Konfigurationen
Zugriffsliste zum Zuordnen des gesamten Internet-Bound-Web-Datenverkehrs (TCP/80) und Ausschließen des gesamten internen Datenverkehrs
Zugriffsliste für vollständigen Internet-Bound-HTTPS-Datenverkehr (TCP/443) und Ausschluss des gesamten internen Datenverkehrs
Zugriffsliste für den gesamten internen Datenverkehr, Ausschluss des gesamten Internet- und HTTPS-Datenverkehrs und aller anderen Ports
Klassenzuordnungskonfiguration zur Anpassung des Datenverkehrs für CWS und CX/FirePower
Richtlinienzuordnungskonfiguration, um Aktionen Klassenzuordnungen zuzuordnen
Globale Aktivierung der Richtlinie für CX/FirePower und CWS auf der Schnittstelle
CWS auf der ASA aktivieren (kein Unterschied)
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die Verwendung der Cisco Adaptive Security Appliance (ASA) mit dem Context Aware (CX)-Modul, auch als Firewall der nächsten Generation bezeichnet, und dem Cisco Cloud Web Security (CWS) Connector.

Voraussetzungen

Anforderungen

Cisco empfiehlt Folgendes:

- 3DES/AES-Lizenz auf ASA (kostenlose Lizenz)
- Gültiger CWS-Service/-Lizenz zur Verwendung von CWS für die erforderliche Anzahl von Benutzern
- Zugriff auf das ScanCenter-Portal zum Generieren des Authentifizierungsschlüssels

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Umfang

Dieses Dokument zeigt die folgenden Bereiche der Technologie und Produkte:

- Die Cisco Adaptive Security Appliances der Serie ASA 5500-X bieten Sicherheit und Intrusion Prevention für die Internet-Edge-Firewall.
- Cisco Cloud Web Security bietet eine präzise Kontrolle aller Webinhalte, auf die zugegriffen wird.

Anwendungsfall

Das ASA CX/FirePOWER-Modul kann sowohl die Inhaltssicherheit als auch die Intrusion Prevention-Anforderung unterstützen, abhängig von den auf der ASA CX/FirePower aktivierten Lizenzfunktionen. Cloud Web Security wird vom ASA CX/FirePower-Modul nicht unterstützt. Wenn Sie sowohl die ASA CX/FirePower-Aktion als auch die Cloud Web Security-Prüfung für denselben Datenverkehrsfluss konfigurieren, führt die ASA nur die ASA CX/FirePower-Aktion aus. Um die CWS-Funktionen für Web Security nutzen zu können, müssen Sie sicherstellen, dass der Datenverkehr in der Match-Anweisung für ASA CX/FirePower umgangen wird. In einem solchen Szenario verwenden Kunden normalerweise CWS für Web Security und AVC (Port 80 und 443) sowie CX/FirePower-Module für alle anderen Ports.

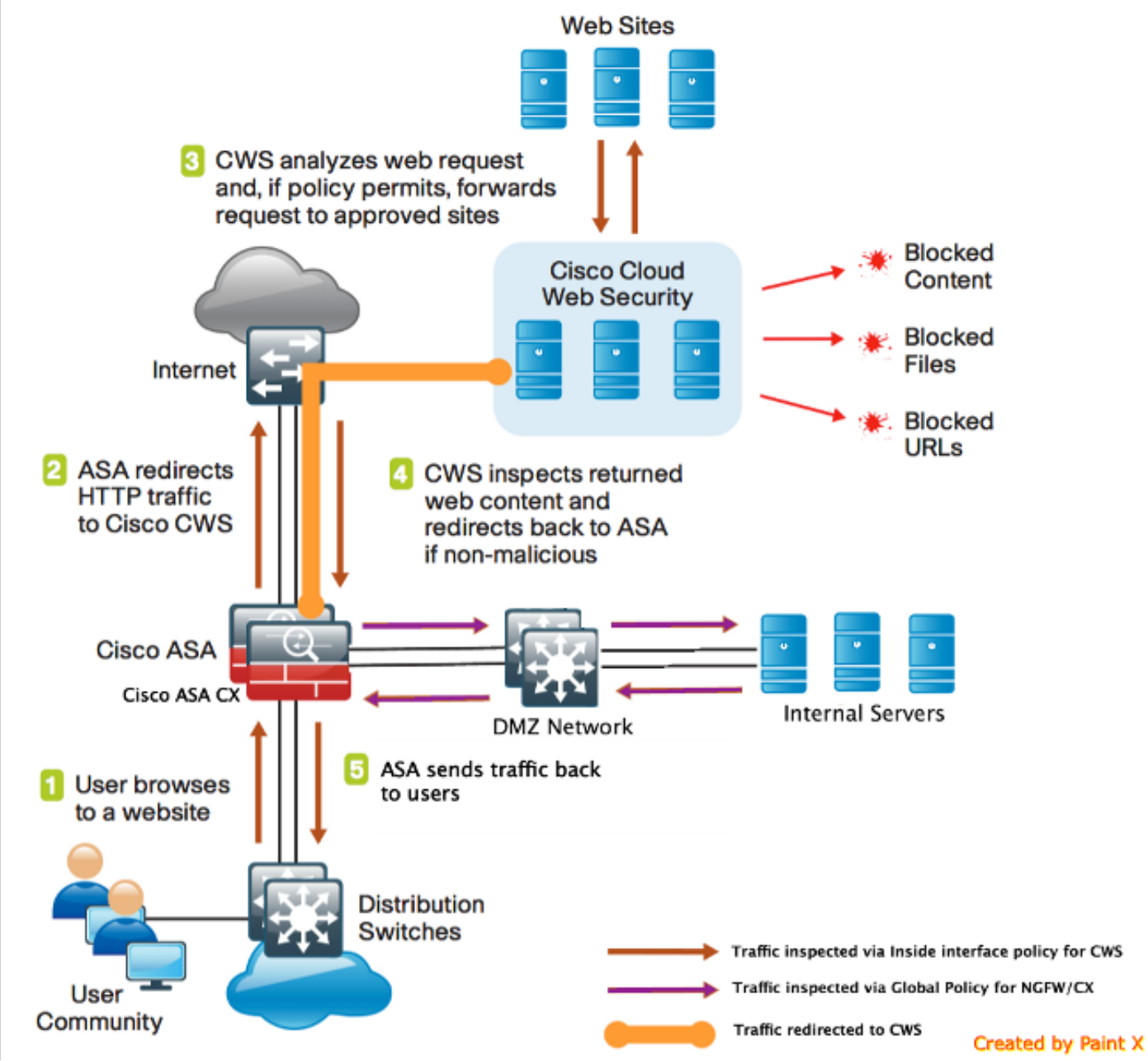
Wichtigste Punkte

- Der Befehl **match default-Inspection-traffic** enthält keine Standardports für die Cloud Web Security Inspection (80 und 443).
- Aktionen werden je nach Funktion auf bidirektionalen oder unidirektionalen Datenverkehr angewendet. Bei Funktionen, die bidirektional angewendet werden, ist der gesamte Datenverkehr, der in die Schnittstelle, auf die Sie die Richtlinienzuordnung anwenden, eingeht oder diese verlässt, davon betroffen, wenn der Datenverkehr mit der Klassenzuordnung für beide Richtungen übereinstimmt. Wenn Sie eine globale Richtlinie verwenden, sind alle Funktionen unidirektional. Funktionen, die normalerweise bidirektional sind, wenn sie auf eine einzige Schnittstelle angewendet werden, gelten nur für den Eingang jeder Schnittstelle, wenn

diese global angewendet wird. Da die Richtlinie auf alle Schnittstellen angewendet wird, wird die Richtlinie in beide Richtungen angewendet, sodass Bidirektionalität in diesem Fall redundant ist.
- Bei TCP- und UDP-Datenverkehr (und Internet Control Message Protocol (ICMP), wenn Sie Stateful ICMP Inspection aktivieren) werden die Service-Richtlinien nicht nur auf einzelnen Paketen, sondern auf Datenverkehrsflüssen ausgeführt. Wenn der Datenverkehr Teil einer bestehenden Verbindung ist, die mit einer Funktion in einer Richtlinie auf einer Schnittstelle übereinstimmt, kann dieser Datenverkehrsfluss nicht auch mit derselben Funktion in einer Richtlinie auf einer anderen Schnittstelle übereinstimmen. Es wird nur die erste Richtlinie verwendet.
- Schnittstellen-Dienstrichtlinien haben Vorrang vor der globalen Dienstrichtlinie für eine bestimmte Funktion.
- Die maximale Anzahl von Richtlinienzuordnungen beträgt 64, Sie können jedoch nur eine Richtlinienzuordnung pro Schnittstelle anwenden.

Konfigurieren

Netzwerkdiagramm



Datenverkehrsfluss für ASA und CWS

1. Der Benutzer fordert die URL über den Webbrowser an.
2. Datenverkehr wird an die ASA gesendet, um ins Internet zu gehen. Die ASA führt eine erforderliche NAT durch und basiert auf dem HTTP/HTTPS-Protokoll, stimmt mit der internen Schnittstellenrichtlinie überein und wird an Cisco CWS umgeleitet.
3. CWS analysiert die Anfrage basierend auf der Konfiguration im ScanCenter-Portal und leitet die Anfrage an genehmigte Standorte weiter, wenn die Richtlinie dies zulässt.
4. CWS überprüft den zurückgegebenen Datenverkehr und leitet ihn an ASA weiter.
5. Basierend auf dem aufrechtzuerhaltenden Sitzungsfluss sendet ASA Datenverkehr zurück an den Benutzer.

Datenverkehrsfluss für ASA und CX/FirePower

1. Der gesamte Datenverkehr außer HTTP und HTTPS wird so konfiguriert, dass er der ASA CX/FirePower zur Überprüfung entspricht, und wird über die ASA-Rückwandplatine an

CX/FirePower umgeleitet.
2. Die ASA CX/FirePower prüft den Datenverkehr anhand der konfigurierten Richtlinien und ergreift die erforderlichen Zulassungs-/Block-/Warnaktionen.

Konfigurationen

Zugriffsliste zum Zuordnen des gesamten Internet-Bound-Web-Datenverkehrs (TCP/80) und Ausschließen des gesamten internen Datenverkehrs

```
!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
```

Zugriffsliste für vollständigen Internet-Bound-HTTPS-Datenverkehr (TCP/443) und Ausschluss des gesamten internen Datenverkehrs

```
!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
```

Zugriffsliste für den gesamten internen Datenverkehr, Ausschluss des gesamten Internet- und HTTPS-Datenverkehrs und aller anderen 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
```

Klassenzuordnungskonfiguration zur Anpassung des Datenverkehrs für CWS und 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
```

Richtlinienzuordnungskonfiguration, um Aktionen Klassenzuordnungen zuzuordnen

```
!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
```

Globale Aktivierung der Richtlinie für CX/FirePower und CWS auf der Schnittstelle

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

> **Hinweis**: In diesem Beispiel wird davon ausgegangen, dass der Webdatenverkehr nur von innerhalb der Sicherheitszone stammt. Sie können Schnittstellenrichtlinien auf allen Schnittstellen verwenden, für die Sie Internetdatenverkehr erwarten, oder Sie verwenden dieselben Klassen innerhalb der globalen Richtlinie. Dies dient lediglich dazu, die Funktionsweise von CWS und die Verwendung von MPF zu demonstrieren, um unsere Anforderungen zu erfüllen.

CWS auf der ASA aktivieren (kein Unterschied)

```
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
!
```

Um sicherzustellen, dass alle Verbindungen die neue Richtlinie verwenden, müssen Sie die aktuellen Verbindungen trennen, damit sie erneut eine Verbindung mit der neuen Richtlinie herstellen können. Siehe **clear conn** oder **clear local-host**-Befehle.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Geben Sie den Befehl **show scansafe statistics** ein, um zu überprüfen, ob der zu aktivierende Dienst von der ASA umgeleitet wird. Die nachfolgenden Versuche zeigen die Erhöhung der Anzahl der Sitzungen, der aktuellen Sitzungen und der übertragenen Bytes an.

```
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
```

Geben Sie den Befehl **show service-policy** ein, um die Inkremente in untersuchten Paketen anzuzeigen.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Geben Sie den folgenden Befehl ein, um Probleme im Zusammenhang mit der oben genannten Konfiguration zu beheben und den Paketfluss zu verstehen:

```
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
```

Zugehörige Informationen

- ASA 9.x-Konfigurationsleitfaden
- Technischer Support und Dokumentation - Cisco Systems