帶CX/FirePower模組和CWS聯結器的ASA配置示例

目錄

簡介

本檔案介紹如何將思科調適型安全裝置(ASA)與情景感知(CX)模組（也稱為下一代防火牆）和思科雲網路安全(CWS)聯結器配合使用。

必要條件

需求

思科建議您：

- ASA上的3DES/AES許可證（免費許可證）
- 有效的CWS服務/許可證，可為所需數量的使用者使用CWS
- 訪問ScanCenter門戶以生成身份驗證金鑰

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

範圍

本檔案介紹下列技術和產品領域：

- Cisco ASA 5500-X系列自適應安全裝置提供網際網路邊緣防火牆安全和入侵防禦。
- 思科雲網路安全對訪問的所有網路內容提供精細控制。

使用案例

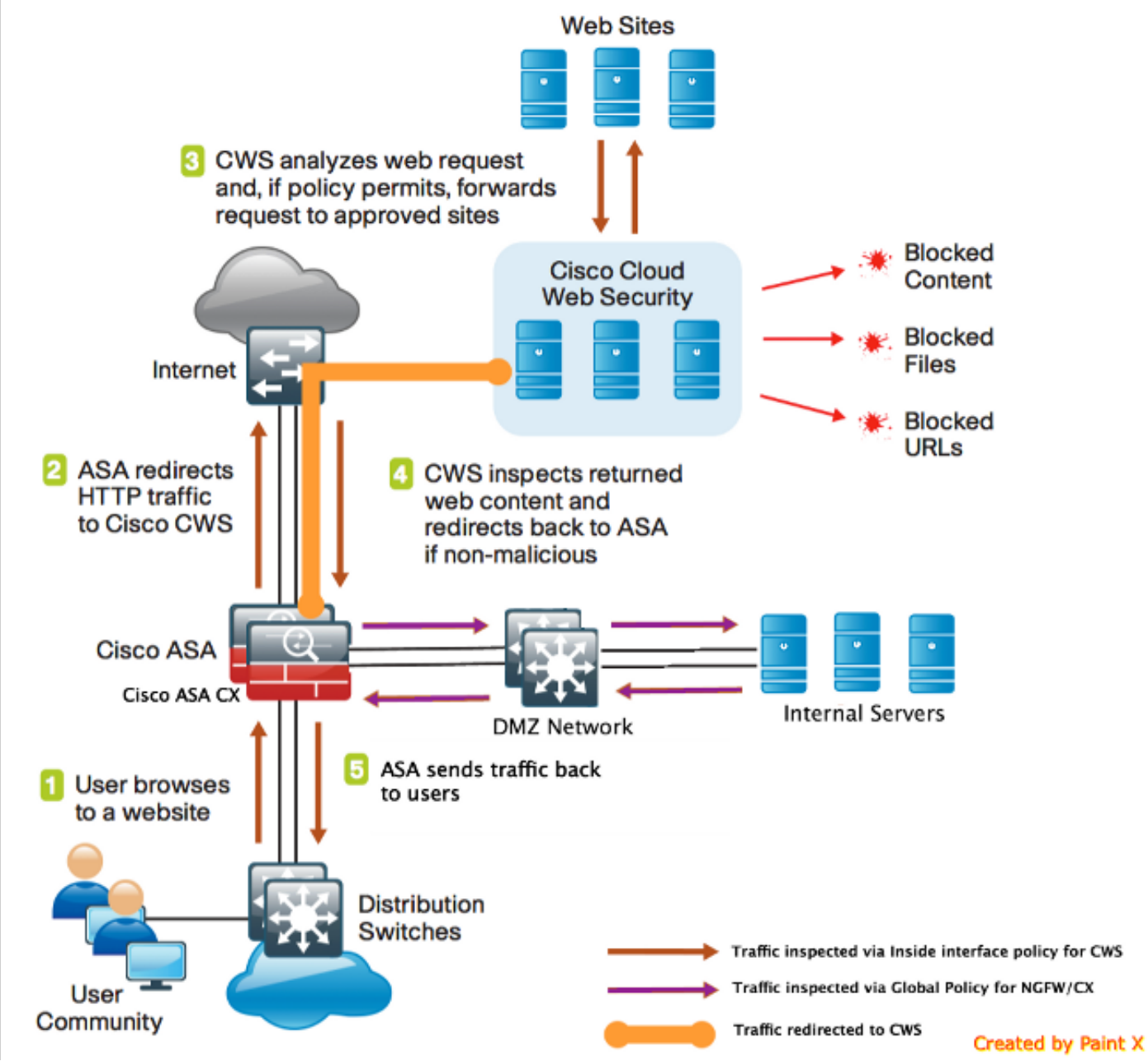
ASA CX/FirePower模組能夠支援內容安全和入侵防禦要求，具體取決於ASA CX/FirePower上啟用的許可證功能。ASA CX/FirePower模組不支援雲網路安全。如果為同一流量配置ASA CX/FirePower操作和雲網路安全檢測，則ASA僅執行ASA CX/FirePower操作。為了利用CWS功能實現網路安全，您需要確保在ASA CX/FirePower的match語句中繞過流量。通常，在這種情況下，客戶會將CWS用於Web安全和AVC（埠80和443），將CX/FirePower模組用於所有其他埠。

要點

- match default-inspection-traffic 命令不包括雲網路安全檢測（80和443）的預設埠。
- 操作將應用到雙向或單向依賴此功能的流量。對於雙向應用的功能，如果兩個方向的流量與類對映匹配，則所有進入或退出應用策略對映的介面的流量都會受到影響。使用全域性策略時，所有功能都是單向的；在應用於單個介面時通常為雙向的功能僅在全域性應用時應用於每個介面的入口。由於策略應用於所有介面，因此策略在兩個方向上都應用，因此在這種情況下，雙向性是多餘的。
- 對於TCP和UDP流量(以及啟用有狀態ICMP檢測時的網際網路控制訊息通訊協定(ICMP))，服務原則會對流量執行，而不僅僅是單個封包執行。如果流量是現有連線的一部分，該連線匹配一個介面上的某個策略中的功能，則該流量也不能與另一個介面上的某個策略中的相同功能匹配；僅使用第一個策略。
- 對於給定功能，介面服務策略優先於全域性服務策略。
- 策略對映的最大數量為64，但每個介面只能應用一個策略對映。

設定

網路圖表



ASA和CWS的流量

1. 使用者通過Web瀏覽器請求URL。
2. 流量傳送到ASA以通過Internet傳輸。ASA執行所需的NAT並基於協定HTTP/HTTPS，與內部介面策略匹配並重定向到Cisco CWS。
3. CWS根據在ScanCenter門戶中完成的配置分析請求，如果策略允許，則將請求轉發到已批准的站點。
4. CWS檢查返回的流量並將其重定向到ASA。
5. 根據維護的會話流，ASA將流量傳送回使用者。

ASA和CX/FirePower的流量

1. 除HTTP和HTTPS之外的所有流量都配置為與ASA CX/FirePower匹配以進行檢測，並重定向至ASA背板上的CX/FirePower。
2. ASA CX/FirePower根據配置的策略檢查流量，並採取所需的allow/block/alert操作。

組態

匹配所有網際網路繫結Web(TCP/80)流量並排除所有內部流量的訪問清單

```
!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
```

匹配所有網際網路繫結HTTPS(TCP/443)流量並排除所有內部流量的訪問清單

```
!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
```

匹配所有內部流量的訪問清單，排除所有網際網路繫結Web和HTTPS流量以及所有其他埠

```
!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
```

用於匹配CWS和CX/FirePower流量的類對映配置

```
! 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
```

將操作與類對映關聯的策略對映配置

```
!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
```

為介面上的CX/FirePower和CWS全域性啟用策略

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

> **附註**：在此範例中，假設網路流量僅源自安全區域內部。可以在所有預期有Web流量的介面上使用介面策略，也可以在全域性策略中使用相同的類。這只是為了說明CWS的運行情況，以及MPF的使用，以支援我們的要求。

在ASA上啟用CWS（無差異）

```
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
!
```

為確保所有連線都使用新策略，您需要斷開當前連線，以便它們可以重新連線新策略。請參閱 **clear conn** 或**clear local-host** 命令。

驗證

使用本節內容，確認您的組態是否正常運作。

輸入**show scansafe statistics**命令以驗證要啟用的服務以及ASA是否重定向流量。後續嘗試顯示會話計數、當前會話和傳輸的位元組數的增量。

```
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
```

輸入show service-policy命令以檢視檢查的封包中的增量

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要排除與上述組態相關的所有問題並了解封包流量，請輸入以下命令：

```
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
```

相關資訊

- [ASA 9.x配置指南]
- [技術支援與文件 - Cisco Systems]