带CX/FirePower模块和CWS连接器的ASA配置示例

目录

简介

本文档介绍如何将思科自适应安全设备(ASA)与情景感知(CX)模块（也称为下一代防火墙）和思科云网络安全(CWS)连接器配合使用。

先决条件

要求

Cisco 建议您：

- ASA上的3DES/AES许可证（免费许可证）
- 有效的CWS服务/许可证，用于为所需数量的用户使用CWS
- 访问ScanCenter门户以生成身份验证密钥

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

范围

本文档显示以下技术和产品领域：

- Cisco ASA 5500-X系列自适应安全设备提供互联网边缘防火墙安全和入侵防御。
- 思科云网络安全对访问的所有网络内容提供精细控制。

使用案例

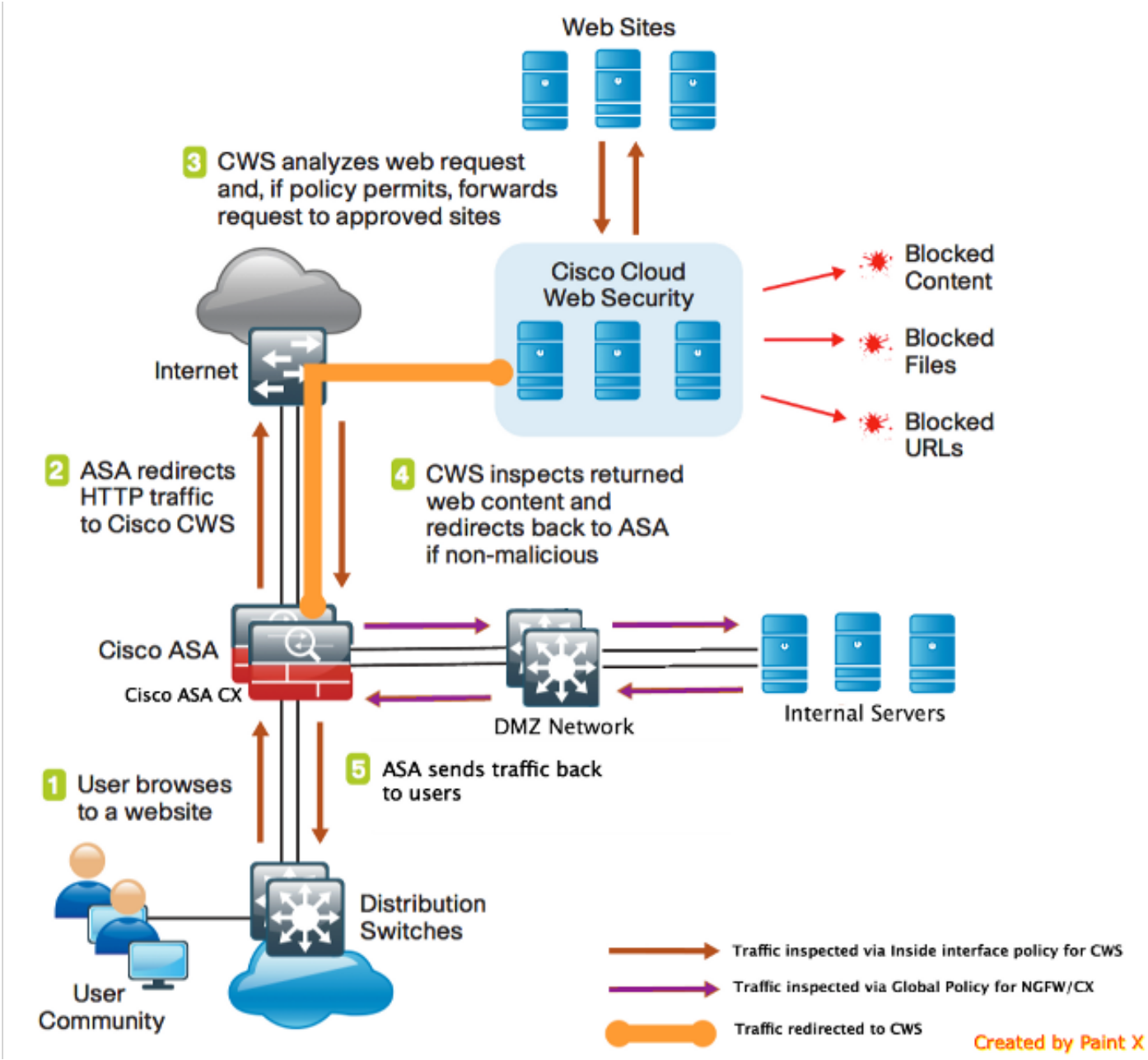
ASA CX/FirePower模块能够同时支持内容安全和入侵防御要求，具体取决于ASA CX/FirePower上启用的许可证功能。ASA CX/FirePower模块不支持云网络安全。如果为同一流量同时配置ASA CX/FirePower操作和云网络安全检查，则ASA仅执行ASA CX/FirePower操作。为了利用CWS功能实现网络安全，您需要确保在ASA CX/FirePower的match语句中绕过流量。通常，在这种情况下，客户将使用CWS进行网络安全和AVC（端口80和443），而CX/FirePower模块用于所有其他端口。

要点

- match default-**inspection-traffic命令不**包括云网络安全检测（80和443）的默认端口。
- 操作根据功能双向或单向应用于流量。对于双向应用的功能，如果流量与两个方向的类映射匹配，则进入或退出应用策略映射的接口的所有流量都会受到影响。使用全局策略时，所有功能都是单向的；应用于单个接口时通常是双向的功能仅应用于全局应用时每个接口的入口。由于策略应用于所有接口，因此该策略在两个方向上都应用，因此本例中的双向性是冗余的。
- 对于TCP和UDP流量(以及启用状态ICMP检测时的互联网控制消息协议(ICMP))，服务策略在流量上运行，而不仅仅是单个数据包。如果流量是现有连接的一部分，该连接与一个接口上策略中的功能匹配，则该流量也不能与另一个接口上策略中的相同功能匹配；仅使用第一个策略。
- 对于给定功能，接口服务策略优先于全局服务策略。
- 策略映射的最大数量为64，但每个接口只能应用一个策略映射。

配置

网络图



ASA和CWS的流量

1. 用户通过Web浏览器请求URL。
2. 流量发送到ASA以通过Internet。ASA执行所需的NAT，并根据协议HTTP/HTTPS与内部接口策略匹配，然后被重定向到Cisco CWS。
3. CWS根据在ScanCenter门户中完成的配置分析请求，如果策略允许，则将请求转发到已批准的站点。
4. CWS会检查返回的流量并将其重定向到ASA。
5. 根据维护的会话流，ASA将流量发回给用户。

ASA和CX/FirePower的流量

1. 除HTTP和HTTPS之外的所有流量都配置为与ASA CX/FirePower匹配以进行检查，并通过ASA背板重定向到CX/FirePower。
2. ASA CX/FirePower根据配置的策略检查流量并采取所需的允许/阻止/警报操作。

配置

匹配所有互联网绑定Web(TCP/80)流量并排除所有内部流量的访问列表

```
!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
```

匹配所有互联网绑定HTTPS(TCP/443)流量并排除所有内部流量的访问列表

```
!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
```

匹配所有内部流量、排除所有互联网绑定的Web和HTTPS流量以及所有其他端口的访问列表

```
!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
```

匹配CWS和CX/FirePower流量的类映射配置

```
! 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
```

将操作与类映射关联的策略映射配置

```
!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
```

全局激活接口上CX/FirePower和CWS的策略

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

> **注意：**在本例中，假设网络流量仅来自安全区域内部。您可以在预期网络流量的所有接口上使用接口策略，或在全局策略中使用相同的类。这只是为了演示CWS的功能和MPF的使用，以支持我们的要求。

在ASA上启用CWS（无差异）

```
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
!
```

为了确保所有连接都使用新策略，您需要断开当前连接，以便它们能重新连接新策略。请参见**clear conn**或clear **local-host**命令。

验证

使用本部分可确认配置能否正常运行。

输入**show scansafe statistics**命令以验证要启用的服务以及ASA重定向流量。后续尝试显示会话计数、当前会话和传输的字节的增量。

```
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
```

输入show service-policy命令，以查看检查的数据包的增量

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

要排除与上述配置相关的任何问题并了解数据包流，请输入以下命令：

```
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
```

相关信息

- [ASA 9.x配置指南]
- [技术支持和文档 - Cisco Systems]