与CX/FirePower模块和CWS连接器配置示例的ASA

目录

简介

本文描述如何以上下文意识(CX)亦称模块、下一代防火墙和Cisco Cloud Web安全(CWS)连接器使用Cisco可适应安全工具(ASA)。

先决条件

要求

Cisco 建议您：

- 3DES/AES在ASA (自由许可证)的许可证
- 有效CWS服务/许可证使用CWS用户所需数量
- 对生成认证密钥的ScanCenter门户的访问

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

本文显示这些技术领域和产品：

- Cisco ASA 5500-X系列可适应安全工具提供互联网边缘防火墙安全和入侵防御。
- Cisco Cloud Web安全提供对访问的所有Web内容的粒状控制。

使用案例

ASA CX/FirePower模块有功能支持两个内容安全和入侵防御需求，从属在启用的许可证功能于ASA CX/FirePower。Cloud Web安全不用ASA CX/FirePower模块支持。如果配置ASA CX/FirePower操作和Cloud Web安全检查同一通信流的， ASA只进行ASA CX/FirePower操作。为了利用Web安全的CWS功能，您在ASA的CX/FirePower匹配语句需要保证流量绕过。一般，在这种情况下，客户将使用CWS Web安全和AVC (端口80和443)和CX/FirePower模块其他端口。

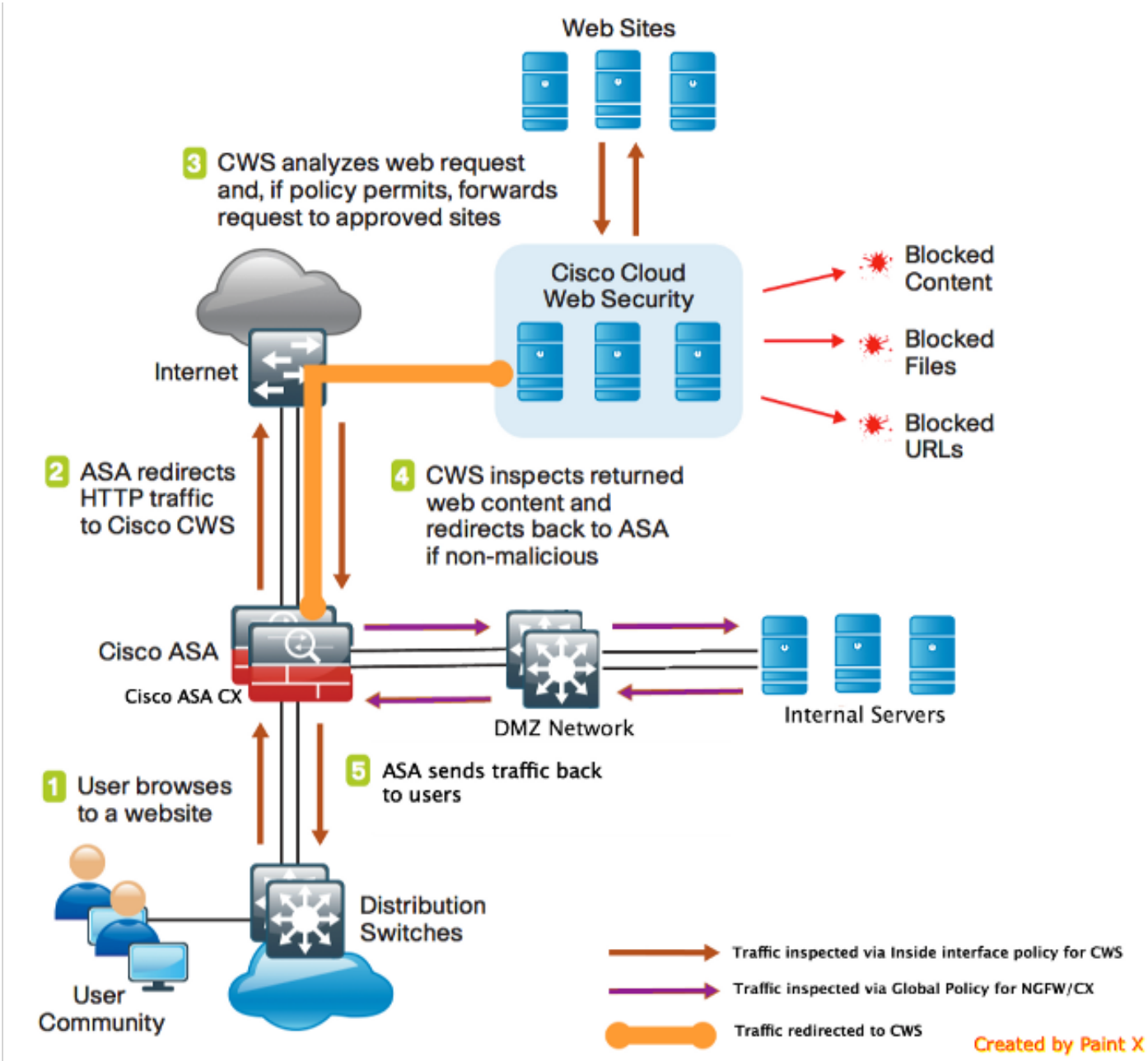
关键点

- **匹配默认检查流量**命令不包括Cloud Web安全检查的默认端口(80和443)。
- 操作应用对流量双向或unidirectionally从属在功能。对于应用双向的功能，进入或退出的所有流量您应用策略映射的接口受影响，如果流量匹配两个方向的类映射。当您使用一项全局策略时所有功能是单向的;通常双向，当应用对单个接口的功能只适用对每个接口入口，当应用全局。由于策略应用对所有接口，策略在两个方向应用，因此bidirectionality在这种情况下冗余。
- 对于TCP和UDP流量(和互联网控制消息协议(ICMP)，当您启用有状态的ICMP检查)时，服务策略起作用不仅通信流和单个数据包。如果流量是匹配在一项策略的一个功能在一个接口现有连接的一部分，该通信流不能也匹配在一项策略的同一个功能在另一个接口;使用仅第一项策略。

- 接口服务策略优先于一个给的功能的全球服务服务策略。
- 策略映射最大是64，但是您能只应用每个接口一个策略映射。

配置

网络图



ASA和CWS的通信流

1. 用户请求URL通过Web浏览器。

2. 流量发送对ASA出去互联网。ASA执行需要的NAT和根据协议HTTP/HTTPS，配比对内部接口策略并且重新定向对Cisco CWS。

3. CWS解析根据配置的请求执行在门户的ScanCenter和，如果策略允许，寄请求给已批准站点。

4. CWS检查返回的流量并且重定向同样对ASA。

5. 基于维护的会话流， ASA送回流量到用户。

ASA和CX/FirePower的通信流

1. 除HTTP和HTTPS之外的所有流量配置匹配检查的ASA CX/FirePower和重定向对在ASA背板的CX/FirePower。

2. ASA CX/FirePower检查根据策略的流量配置并且采取需要的准许/块/警报行动。

配置

匹配所有互联网限制Web (TCP/80)流量和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
```

匹配所有互联网限制HTTPS (TCP/443)流量和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
```

匹配所有内部流量的访问列表，排除所有互联网限制Web和HTTPS流量和其他端口

```
!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的流量的类映射配置

```
! 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
```

连结操作的策略映射配置与类映射

```
!Inspection policy map to configure essential parameters for the rules and
optionally !identify the whitelist 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 whitelist 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
```

激活策略全局CX/FirePower和CWS的在接口

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

> Note:在本例中，假设， Web流量从安全区里边仅起源。您能使用在您期待Web流量或使用在全局策略内的同班的所有接口的接口策略。这是为了展示作用CWS和使用MPF为了支持我们的需求。

在ASA (没有差异)的Enable (event) CWS

```
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
!
```

为了保证所有连接使用新的策略，您需要断开连接当前连接，因此他们能重新连接与新的策略。请参阅clear conn或清除local-host命令。

验证

使用本部分可确认配置能否正常运行。

输入statistics命令显示的scansafe为了验证启用的服务，并且ASA重定向流量。随后的尝试显示在会话计数、当前转接的会话和字节的增量。

```
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policy命令的show service为了发现在被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。

为了排除故障与上述配置涉及的所有问题和了解数据包流，请输入此命令：

```
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