Exemplo de configuração do ASA com módulo CX/FirePower e conector CWS

Contents

Introduction

Este documento descreve como usar o Cisco Adaptive Security Appliance (ASA) com o módulo Context Aware (CX), também conhecido como firewall de próxima geração, e o Cisco Cloud Web Security (CWS) Connector.

Prerequisites

Requirements

A Cisco recomenda que você:

- Licença 3DES/AES no ASA (licença gratuita)
- Serviço/licença CWS válido para usar o CWS para o número necessário de usuários
- Acesso ao Portal do ScanCenter para gerar a chave de autenticação

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

Escopo

Este documento mostra as seguintes áreas de tecnologia e produtos:

- Os dispositivos de segurança adaptável Cisco ASA 5500-X Series fornecem segurança de firewall de borda da Internet e prevenção contra invasões.
- O Cisco Cloud Web Security oferece controle granular sobre todo o conteúdo da Web acessado.

caso de uso

O módulo ASA CX/FirePower tem a capacidade de oferecer suporte aos requisitos de segurança de conteúdo e prevenção contra invasões, dependendo dos recursos de licença habilitados no ASA CX/FirePower. O Cloud Web Security não é compatível com o módulo ASA CX/FirePower. Se você configurar a ação ASA CX/FirePower e a inspeção do Cloud Web Security para o mesmo fluxo de tráfego, o ASA executará apenas a ação ASA CX/FirePower. Para aproveitar os recursos do CWS para o Web Security, é necessário garantir que o tráfego seja ignorado na instrução de correspondência do ASA CX/FirePower. Normalmente, nesse cenário, os clientes usarão o CWS para segurança da Web e o módulo AVC (portas 80 e 443) e CX/FirePower para todas as outras portas.

Principais pontos

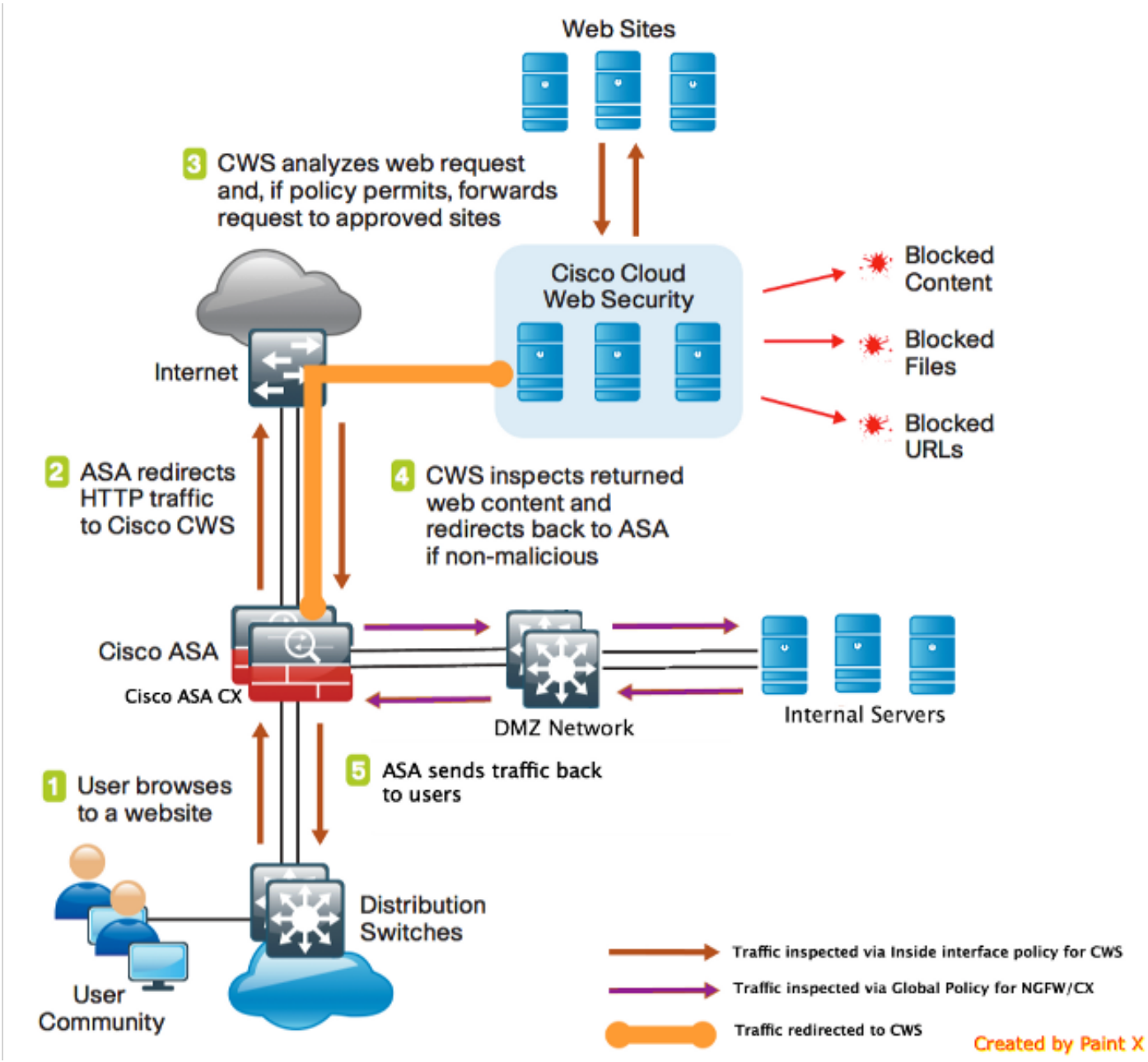
- O comando **match default-inspection-traffic** não inclui as portas padrão para a inspeção Cloud Web Security (80 e 443).
- As ações são aplicadas ao tráfego de forma bidirecional ou unidirecional, dependendo do recurso. Para recursos que são aplicados bidirecionalmente, todo o tráfego que entra ou sai da interface à qual você aplica o mapa de política é afetado se o tráfego corresponder ao mapa de classe para ambas as direções. Quando você usa uma política global, todos os recursos são unidirecionais; os recursos que normalmente são bidirecionais quando aplicados a uma única interface aplicam-se somente à entrada de cada interface quando aplicados globalmente. Como a política é aplicada a todas as interfaces, a política é aplicada em ambas as direções, portanto, a bidirecionalidade nesse caso é redundante.
- Para tráfego TCP e UDP (e Internet Control Message Protocol (ICMP) quando você habilita a

inspeção de ICMP stateful), as políticas de serviço operam em fluxos de tráfego e não apenas em pacotes individuais. Se o tráfego fizer parte de uma conexão existente que corresponda a um recurso em uma política em uma interface, esse fluxo de tráfego também não poderá corresponder ao mesmo recurso em uma política em outra interface; somente a primeira política é usada.

- As políticas de serviço de interface têm precedência sobre a política de serviço global para um determinado recurso.
- O número máximo de mapas de política é 64, mas você só pode aplicar um mapa de política por interface.

Configurar

Diagrama de Rede



Fluxo de tráfego para o ASA e o CWS

1. O usuário solicita o URL através do navegador da Web.
2. O tráfego é enviado ao ASA para sair pela Internet. O ASA executa o NAT necessário e baseado no protocolo HTTP/HTTPS, corresponde à política de interface interna e é redirecionado para o Cisco CWS.
3. O CWS analisa a solicitação com base na configuração feita no portal do ScanCenter e, se a diretiva permitir, encaminha a solicitação para sites aprovados.
4. O CWS inspeciona o tráfego retornado e redireciona o mesmo para o ASA.
5. Com base no fluxo de sessão mantido, o ASA envia o tráfego de volta ao usuário.

Fluxo de tráfego para o ASA e o CX/FirePower

1. Todo o tráfego que não seja HTTP e HTTPS é configurado para corresponder ao ASA CX/FirePower para inspeção e é redirecionado para CX/FirePower sobre o painel traseiro ASA.
2. O ASA CX/FirePower inspeciona o tráfego com base nas políticas configuradas e toma a ação de permissão/bloqueio/alerta necessária.

Configurações

Lista de acesso para corresponder a todo o tráfego da Web vinculado à Internet (TCP/80) e excluir todo o tráfego interno

```
!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
```

Lista de acesso para corresponder a todo o tráfego HTTPS (TCP/443) vinculado à Internet e excluir todo o tráfego interno

```
!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
```

Lista de acesso para corresponder a todo o tráfego interno, excluir todo o tráfego Web e HTTPS vinculado à Internet e todas as outras portas

```
!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
```

Configuração de mapa de classe para corresponder o tráfego para CWS e 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
```

Configuração do mapa de política para associar ações a mapas de classe

```
!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
```

Ative globalmente a política para CX/FirePower e CWS na interface

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

> **Note**: Neste exemplo, supõe-se que o tráfego da Web seja originado somente de dentro da zona de segurança. Você pode usar políticas de interface em todas as interfaces nas quais espera tráfego da Web ou usar as mesmas classes na política global. Isso é apenas para demonstrar o funcionamento do CWS e o uso do MPF para atender a nosso requisito.

Ativar o CWS no ASA (sem diferença)

```
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
!
```

Para garantir que todas as conexões usem a nova política, você precisa desconectar as conexões atuais para que possam se reconectar à nova política. Consulte os comandos **clear conn** ou **clear local-host**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Insira o comando **show scansafe statistics** para verificar o serviço a ser ativado e se o ASA redireciona o tráfego. Tentativas subsequentes mostram o aumento nas contagens de sessão, sessões atuais e bytes transferidos.

```
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
```

Insira o comando **show service-policy** para ver os incrementos em pacotes inspecionados

```
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
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para solucionar qualquer problema relacionado à configuração acima e entender o fluxo do pacote, insira este comando:

```
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
```

Informações Relacionadas

- Guia de configuração do ASA 9.x
- Suporte Técnico e Documentação - Cisco Systems