CWs no tráfego ASA aos servidores internos obstruídos

Índice

Introdução

Este documento descreve um problema comum encontrado quando você configura a Segurança da Web da nuvem de Cisco (CWs) (conhecido previamente como ScanSafe) em versões 9.0 e mais recente adaptáveis das ferramentas de segurança de Cisco (ASA).

Com CWs, o ASA reorienta transparentemente o HTTP e o HTTPS selecionados a um servidor proxy CWs. Os administradores têm a capacidade para permitir, obstruir, ou advertir utilizadores finais a fim protegê-los do malware com a configuração apropriada das políticas de segurança no portal CWs.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destas configurações:

- Cisco ASA através de CLI e/ou do Security Device Manager adaptável (ASDM)
- Cisco nubla-se a Segurança da Web em Cisco ASA

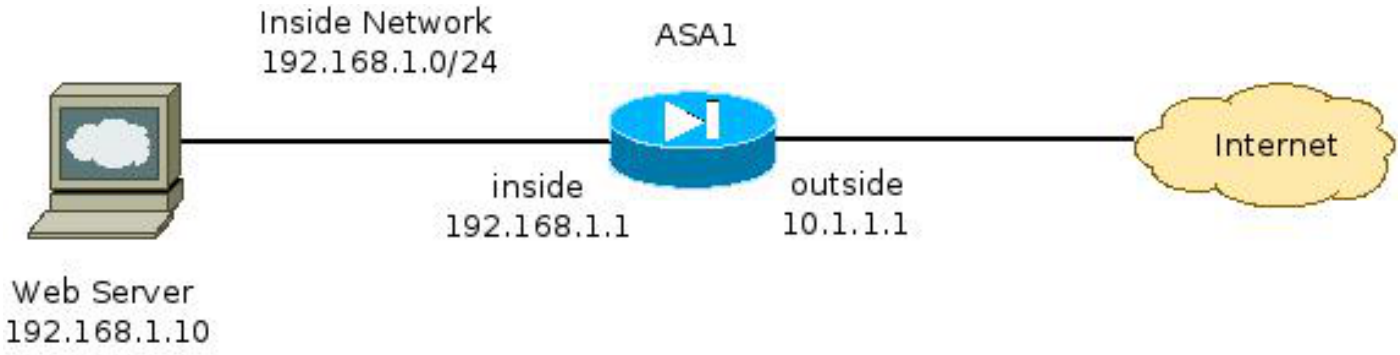
Componentes Utilizados

A informação neste documento é baseada em Cisco ASA.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede



Problema

Um problema comum encontrado quando você configura Cisco CWs no ASA ocorre quando os servidores de Web internos se tornam inacessíveis com o ASA. Por exemplo, está aqui uma configuração de exemplo que corresponde à topologia ilustrada na seção anterior:

```
hostname ASA1
!
<snip>
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
<snip>
object network inside-network
 subnet 192.168.1.0 255.255.255.0
object network web-server
 host 192.168.1.10
!
<snip>
access-list outside_access_in permit tcp any host 192.168.1.10 eq www
access-list outside_access_in permit tcp any host 192.168.1.10 eq https
access-list http-traffic extended permit tcp any any eq www
access-list https-traffic extended permit tcp any any eq https
!
<snip>
scansafe general-options
 server primary fqdn proxy193.scansafe.net port 8080
 server backup fqdn proxy1363.scansafe.net port 8080
 retry-count 5
 license <license key>
```

```
!
<snip>
object network inside-network
 nat (inside,outside) dynamic interface
object network web-server
 nat (inside,outside) static 10.1.1.10
!
access-group outside_access_in in interface outside
!
<snip>
class-map http-class
 match access-list http_traffic
class-map https-class
 match access-list https_traffic
!
policy-map type inspect scansafe http-pmap
 parameters
 http
policy-map type inspect scansafe https-pmap
 parameters
 https
!
policy-map outside-policy
class http-class
 inspect scansafe http-pmap fail-close
class https-class
 inspect scansafe https-pmap fail-close
!
service-policy outside-policy interface inside
```

Com este confguration, o servidor de Web interno da parte externa que se usa o endereço IP 10.1.1.10 pôde tornar-se inacessível. Esta edição pode ser causada por razões múltiplas, como:

- O tipo de índice hospedado no servidor de Web.
- O certificado do Secure Socket Layer (SSL) do servidor de Web não é confiado pelo servidor proxy CWs.

Solução

O índice hospedado em todos os server internos é considerado geralmente de confiança. Daqui, não é necessário fazer a varredura do tráfego para estes server com CWs. Você pode tráfego da branco-lista a tais servidores internos com esta configuração:

```
ASA1(config)# object-group network ScanSafe-bypass
ASA1(config-network-object-group)# network-object host 192.168.1.10
ASA1(config-network-object-group)# exit
ASA1(config)# access-list http_traffic line 1 deny tcp
  any object-group ScanSafe-bypass eq www
ASA1(config)# access-list https_traffic line 1 deny tcp
  any object-group ScanSafe-bypass eq https
```

Com esta configuração, o tráfego ao servidor de Web interno em 192.168.1.10 nas portas TCP 80 e 443 é reorientado já não aos servidores proxy CWs. Se há os servidores múltiplos do este datilografam dentro a rede, você podem adicionar-los ao objeto-grupo nomeado ScanSafe-desvio.

Configuração final

Está aqui um exemplo da configuração final:

```
hostname ASA1
!
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/3
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  management-only
  no nameif
  no security-level
  no ip address
!
object network inside-network
  subnet 192.168.1.0 255.255.255.0
object network web-server
  host 192.168.1.10
object-group network ScanSafe-bypass
  network-object host 192.168.1.10
!
access-list outside_access_in permit tcp any host 192.168.1.10 eq www
access-list outside_access_in permit tcp any host 192.168.1.10 eq https
access-list http_traffic deny tcp any object-group ScanSafe-bypass eq www
access-list http-traffic extended permit tcp any any eq www
access-list https_traffic deny tcp any object-group ScanSafe-bypass eq https
access-list https-traffic extended permit tcp any any eq https
!
scansafe general-options
  server primary fqdn proxy193.scansafe.net port 8080
  server backup fqdn proxy1363.scansafe.net port 8080
  retry-count 5
  license <license key>
!
pager lines 24mtu outside 1500
mtu inside 1500
no asdm history enable
arp timeout 14400
!
object network inside-network
  nat (inside,outside) dynamic interface
object network web-server
  nat (inside,outside) static 10.1.1.10
!
access-group outside_access_in in interface outside
!
route outside 0.0.0.0 0.0.0.0 10.1.1.254 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
!
class-map http-class
  match access-list http_traffic
class-map https-class
  match access-list https_traffic
!
policy-map type inspect scansafe
  http-pmap
  parameters
    http
policy-map type inspect scansafe https-pmap
  parameters
    https
!
policy-map inside-policy
class http-class
  inspect scansafe http-pmap fail-close
class https-class
  inspect scansafe https-pmap fail-close
!
service-policy inside-policy interface inside
```

Informações Relacionadas

- Manual de configuração rápida do conector de Cisco ASA
- Guia de configuração de CLI de Cisco ASA 9.0
- Suporte Técnico e Documentação - Cisco Systems