CWS en el tráfico ASA a los servidores internos bloqueados

Contenido

Introducción

Este documento describe un problema común encontrado cuando usted configura la Seguridad de la red de la nube de Cisco (CWS) (conocido previamente como ScanSafe) en las versiones adaptantes 9.0 de los dispositivos de seguridad de Cisco (ASA) y posterior.

Con el CWS, el ASA transparente reorienta el HTTP y el HTTPS seleccionados a un servidor proxy del CWS. Los administradores tienen la capacidad de permitir, de bloquear, o de advertir a los usuarios finales para protegerlos contra el malware con la configuración apropiada de las políticas de seguridad en el portal del CWS.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de estas configuraciones:

- Cisco ASA vía CLI y/o el Administrador de dispositivos de seguridad adaptante (ASDM)
- Seguridad de la red de la nube de Cisco en Cisco ASA

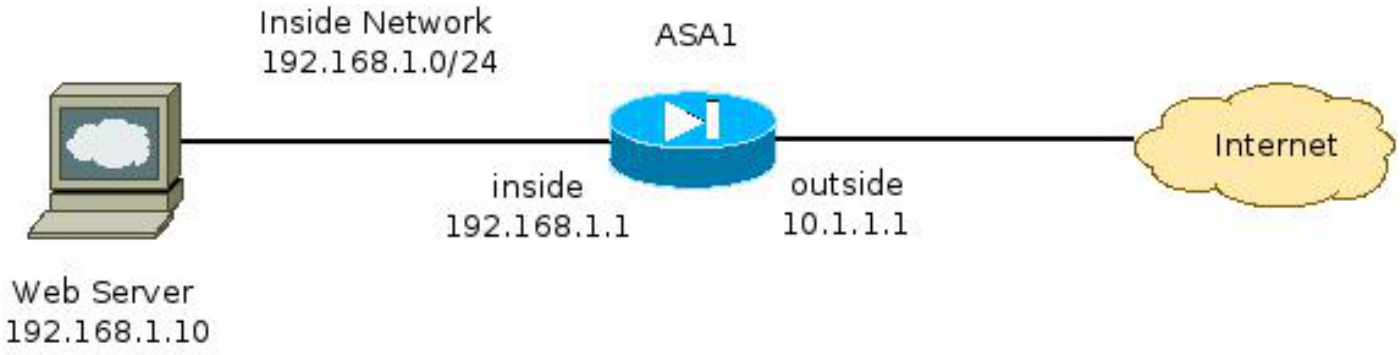
Componentes Utilizados

La información en este documento se basa en Cisco ASA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red



Problema

Un problema común encontrado cuando usted configura el CWS de Cisco en el ASA ocurre cuando los servidores Web internos hacen inaccesibles con el ASA. Por ejemplo, aquí está una configuración de muestra que corresponde a la topología ilustrada en la sección 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
```

Con este confguration, el servidor Web interno del exterior que utiliza la dirección IP 10.1.1.10 pudo hacer inaccesible. Este problema se puede causar por las razones múltiples, por ejemplo:

- El tipo de contenido recibido en el servidor Web.
- El certificado del Secure Socket Layer (SSL) del servidor Web no es confiado en por el servidor proxy del CWS.

Solución

El contenido recibido en cualquier servidor interno generalmente se considera digno de confianza. Por lo tanto, no es necesario analizar el tráfico a estos servidores con el CWS. Usted puede tráfico de la blanco-lista a tales servidores internos con esta configuración:

```
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
```

Con esta configuración, el tráfico al servidor Web interno en 192.168.1.10 en los puertos TCP 80 y 443 se reorienta no más a los servidores proxy del CWS. Si hay los servidores múltiples de este teclean adentro la red, usted pueden agregarlos al objeto-grupo nombrado ScanSafe-puente.

Configuración final

Aquí está un ejemplo de la configuración 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
```

Información Relacionada

- Guía de configuración rápida del conector de Cisco ASA
- Guía de configuración CLI de Cisco ASA 9.0
- Soporte Técnico y Documentación - Cisco Systems