CWS на трафике ASA к заблокированным внутренним серверам

Содержание

Введение

Этот документ описывает типичную проблему, с которой встречаются при настройке Облачной веб-безопасности (CWS) Cisco (ранее известный как ScanSafe) на устройствах адаптивной защиты Cisco (ASA) Версии 9.0 и позже.

С CWS ASA прозрачно перенаправляет, выбрал HTTP и HTTPS к прокси-серверу CWS. У администраторов есть способность позволить, заблокировать, или предупредить конечных пользователей для защиты их от вредоносного ПО с соответствующей конфигурацией политики безопасности на портале CWS.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с этими конфигурациями:

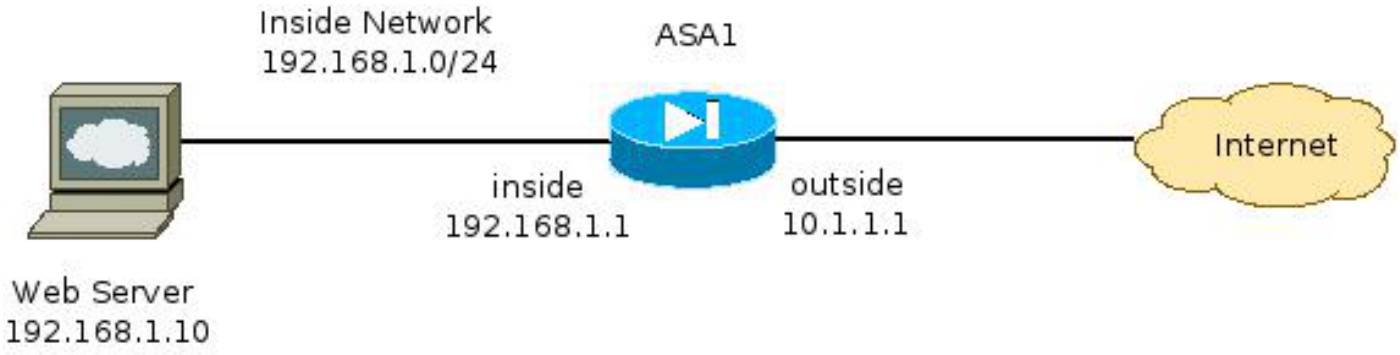
- ASA Cisco через CLI и/или Менеджер устройств адаптивной безопасности (ASDM) (ASDM)
- Облачная веб-безопасность Cisco на ASA Cisco

Используемые компоненты

Сведения в этом документе основываются на ASA Cisco.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Схема сети



Проблема

Типичная проблема встретилась при настройке CWS Cisco на ASA, происходит, когда внутренние веб-серверы становятся недоступными через ASA. Например, вот пример конфигурации, который соответствует топологии, проиллюстрированной в предыдущем разделе:

```
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
```

С этим confguration внутренний веб-сервер снаружи этого использует IP-адрес **10.1.1.10**, мог бы стать недоступным. Эта проблема может быть вызвана множественными причинами, такими как:

- Тип содержания размещен на Web-сервере.
- Сертификату Протокола SSL Web-сервера не доверяет прокси-сервер CWS.

Решение

Содержание, размещенное на любом внутреннем сервере (серверах), обычно считают защищенным. Следовательно, необязательно для сканирования трафика к этим серверам с CWS. Можно добавить трафик в белый список к таким внутренним серверам с этой конфигурацией:

```
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
```

С этой конфигурацией трафик к внутреннему веб-серверу в **192.168.1.10** на портах TCP **80** и **443** больше не перенаправляется к прокси-серверам CWS. Если существуют несколька адресов серверов этого типа в сети, можно добавить их к object-group, названному **обходом ScanSafe**.

Окончательная конфигурация

Вот пример окончательной конфигурации:

```
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
```

Дополнительные сведения

- Руководство по быстрой настройке разъёма Cisco ASA
- Руководство конфигурации интерфейса командой строки Cisco ASA 9.0
- Cisco Systems – техническая поддержка и документация