Blockierter CWS auf ASA-Datenverkehr zu internen Servern

Inhalt

Einführung

Dieses Dokument beschreibt ein häufig auftretendes Problem bei der Konfiguration von Cisco Cloud Web Security (CWS) (früher ScanSafe genannt) auf Cisco Adaptive Security Appliances (ASAs) Version 9.0 und höher.

Mit CWS leitet die ASA ausgewählte HTTP- und HTTPS-Verbindungen transparent an einen CWS-Proxyserver um. Administratoren können Endbenutzer zulassen, blockieren oder vor Malware warnen, um sie mithilfe der entsprechenden Konfiguration von Sicherheitsrichtlinien im CWS-Portal vor Malware zu schützen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über die folgenden Konfigurationen zu verfügen:

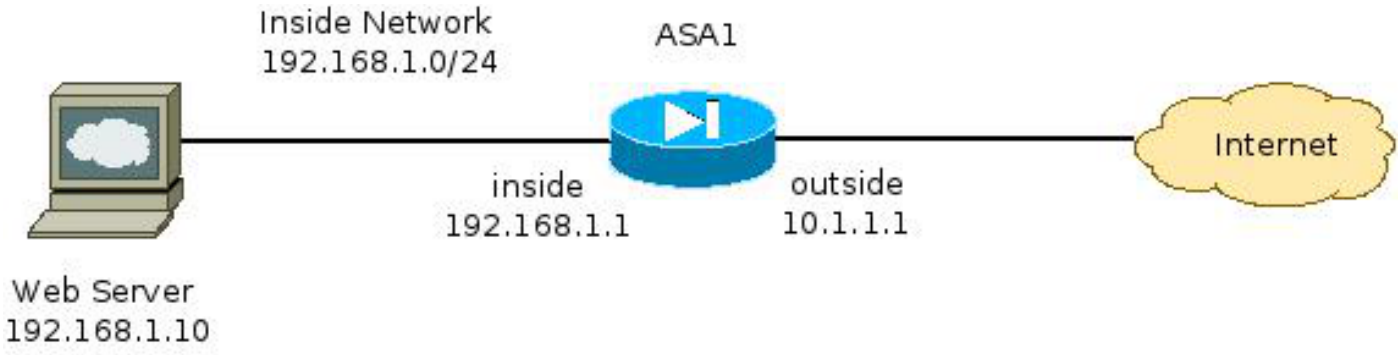
- Cisco ASAs über CLI und/oder Adaptive Security Device Manager (ASDM)
- Cisco Cloud Web Security auf Cisco ASAs

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco ASAs.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm



Problem

Ein häufiges Problem tritt bei der Konfiguration von Cisco CWS auf der ASA auf, wenn auf die internen Webserver nicht über die ASA zugegriffen werden kann. Hier ist beispielsweise eine Beispielkonfiguration, die der im vorherigen Abschnitt dargestellten Topologie entspricht:

```
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
```

Bei dieser Konfiguration kann der interne Webserver von außen, der die IP-Adresse **10.1.1.10** verwendet, nicht mehr zugänglich sein. Dieses Problem kann aus mehreren Gründen auftreten:

- Der Inhaltstyp, der auf dem Webserver gehostet wird.
- Das SSL-Zertifikat (Secure Socket Layer) des Webservers wird vom CWS-Proxyserver nicht als vertrauenswürdig eingestuft.

Lösung

Inhalte, die auf internen Servern gehostet werden, gelten im Allgemeinen als vertrauenswürdig. Daher ist es nicht erforderlich, den Datenverkehr zu diesen Servern mit CWS zu prüfen. Mit der folgenden Konfiguration können Sie Datenverkehr zu diesen internen Servern der Zulassungsliste hinzufügen:

```
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
```

Bei dieser Konfiguration wird der Datenverkehr zum internen Webserver unter **192.168.1.10** an den TCP-Ports **80** und **443** nicht mehr an die CWS-Proxyserver umgeleitet. Wenn im Netzwerk mehrere Server dieses Typs vorhanden sind, können Sie diese der Objektgruppe **ScanSafe-bypass** hinzufügen.

Endgültige Konfiguration

Hier ein Beispiel für die endgültige Konfiguration:

```
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
!
pager lines 24 mtu 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
```

Zugehörige Informationen

- Cisco ASA Connector - Kurzreferenz
- Konfigurationsleitfaden für die CLI von Cisco ASA 9.0
- Technischer Support und Dokumentation - Cisco Systems