CWS sul traffico ASA verso i server interni bloccato

Sommario

Introduzione

Questo documento descrive un problema comune riscontrato durante la configurazione di Cisco Cloud Web Security (CWS) (precedentemente noto come ScanSafe) su Cisco Adaptive Security Appliance (ASA) versione 9.0 e successive.

Con CWS, l'ASA reindirizza in modo trasparente i protocolli HTTP e HTTPS selezionati a un server proxy CWS. Gli amministratori possono consentire, bloccare o avvisare gli utenti finali per proteggerli dal malware con la configurazione appropriata dei criteri di sicurezza sul portale CWS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle seguenti configurazioni:

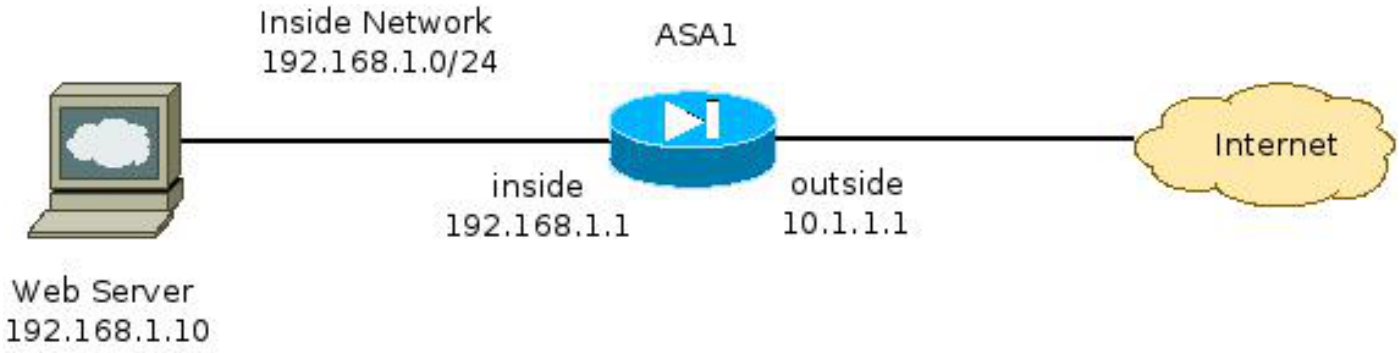
- Cisco ASA tramite CLI e/o Adaptive Security Device Manager (ASDM)
- Cisco Cloud Web Security su Cisco ASA

Componenti usati

Le informazioni di questo documento si basano sulle appliance Cisco ASA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete



Problema

Un problema comune riscontrato quando si configura Cisco CWS sull'appliance ASA si verifica quando i server Web interni non sono più accessibili tramite l'appliance ASA. Di seguito è riportato un esempio di configurazione che corrisponde alla topologia illustrata nella sezione precedente:

```
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 questa configurazione, il server Web interno dall'esterno che utilizza l'indirizzo IP **10.1.1.10** potrebbe diventare inaccessibile. Questo problema può essere causato da più motivi, ad esempio:

- Tipo di contenuto ospitato nel server Web.
- Il certificato SSL (Secure Sockets Layer) del server Web non è considerato attendibile dal server proxy CWS.

Soluzione

Il contenuto ospitato su qualsiasi server interno è in genere considerato attendibile. Non è quindi necessario eseguire la scansione del traffico verso questi server con CWS. È possibile aggiungere il traffico a tali server interni all'elenco dei server consentiti con la seguente configurazione:

```
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 questa configurazione, il traffico diretto al server Web interno all'indirizzo **192.168.1.10** sulle porte TCP **80** e **443** non viene più reindirizzato ai server proxy CWS. Se nella rete sono presenti più server di questo tipo, è possibile aggiungerli al gruppo di oggetti denominato **ScanSafe-bypass**.

Configurazione finale

Di seguito è riportato un esempio della configurazione finale:

```
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
```

Informazioni correlate

- Guida alla configurazione rapida di Cisco ASA Connector
- Guida alla configurazione della CLI di Cisco ASA 9.0
- Documentazione e supporto tecnico – Cisco Systems