내부 서버에 대한 ASA 트래픽의 CWS 차단됨

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliances) 버전 9.0 이상에서 Cisco CWS(ScanSafe)를 구성할 때 발생하는 일반적인 문제에 대해 설명합니다.

CWS를 사용하면 ASA는 선택한 HTTP 및 HTTPS를 CWS 프록시 서버로 투명하게 리디렉션합니다.관리자는 최종 사용자를 CWS 포털에서 적절한 보안 정책 컨피그레이션으로 악성코드로부터 보호하기 위해 허용, 차단 또는 경고할 수 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 컨피그레이션에 대해 알고 있는 것이 좋습니다.

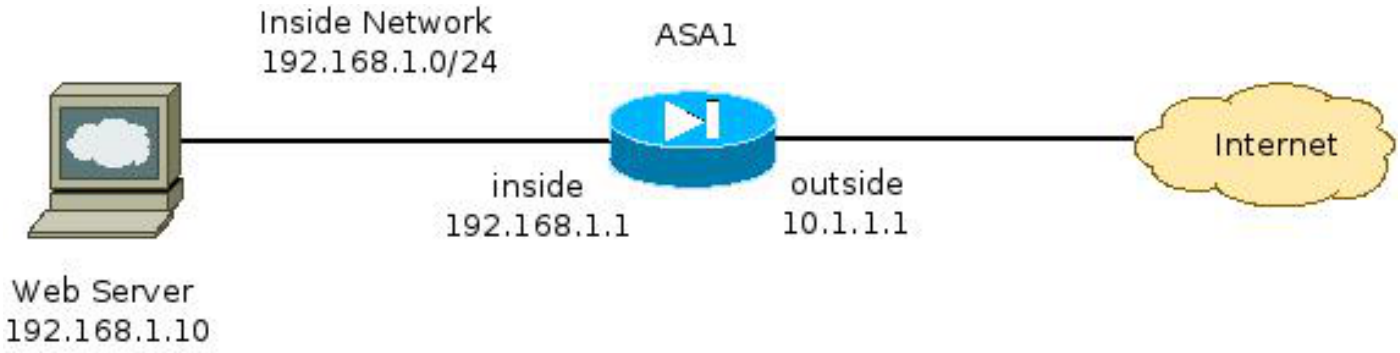
- CLI 및/또는 ASDM(Adaptive Security Device Manager)을 통한 Cisco ASA
- Cisco ASA의 Cisco Cloud Web Security

사용되는 구성 요소

이 문서의 정보는 Cisco ASA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램



문제

ASA에서 Cisco CWS를 구성할 때 발생하는 일반적인 문제는 내부 웹 서버가 ASA를 통해 액세스할 수 없게 될 때 발생합니다.예를 들어, 다음은 이전 섹션에서 설명한 토폴로지에 해당하는 샘플 컨피그레이션입니다.

```
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
```

이 컨피그레이션을 사용하면 IP 주소 **10.1.1.10**을 사용하는 외부의 내부 웹 서버에 액세스할 수 없게 됩니다.이 문제는 다음과 같은 여러 가지 이유로 인해 발생할 수 있습니다.

- 웹 서버에서 호스팅되는 콘텐츠의 유형입니다.
- 웹 서버의 SSL(Secure Socket Layer) 인증서가 CWS 프록시 서버에서 신뢰되지 않습니다.

솔루션

내부 서버에서 호스팅되는 컨텐츠는 일반적으로 신뢰할 수 있는 것으로 간주됩니다.따라서 CWS를 사용하여 이러한 서버에 대한 트래픽을 스캔할 필요가 없습니다.다음 컨피그레이션을 사용하여 이러한 내부 서버에 트래픽을 허용 목록에 추가할 수 있습니다.

```
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
```

이 컨피그레이션을 사용하면 TCP 포트 **80** 및 **443**에서 **192.168.1.10**의 내부 웹 서버에 대한 트래픽이 더 이상 CWS 프록시 서버로 리디렉션되지 않습니다.네트워크에 이 유형의 서버가 여러 개 있는 경우 ScanSafe**-bypass**라는 객체 그룹에 서버를 추가할 수 있습니다.

최종 구성

다음은 최종 구성의 예입니다.

```
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
```

관련 정보

- Cisco ASA Connector 빠른 구성 가이드
- Cisco ASA 9.0 CLI 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems