Escenarios de configuración de la Administración de IPS en un módulo ips 5500x

Contenido

Introducción

Este documento provee escenarios de configuración de un módulo de Sistemas de Prevención de Intrusos (IPS) de Adaptive Security Appliance (ASA) 5500x.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Módulos ASA 5500x IPS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Módulos ASA 5500x IPS

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedente

Con la introducción del ASA 5500x y la implementación del software del IPS, hay cambios fundamentales a la manera que se permite a la Administración de IPS comportarse.

1. El IPS puede utilizar solamente la interfaz de la Administración 0/0 para el Acceso de administración externo.
2. Si el ASA tiene un **nameif** asignado a la Administración 0/0, el IPS debe tener un direccionamiento en la misma subred como el **nameif**.
3. Usted no puede quitar el comando de la **Administración-solamente de la** interfaz de la Administración 0/0 del ASA.
4. Si el ASA intenta rutear el tráfico con el **nameif de la Administración** con la declaración de la “Administración-solamente”, el ASA cae el tráfico.
5. Si no hay **nameif** asignado a la Administración 0/0, el IPS funciona semejantemente a la interfaz de administración avanzada de los módulos del módulo de Servicios de seguridad del examen y de la prevención (AIP-SSM).

Estos comportamientos inhiben las comunicaciones del IPS a las redes externas que pasan con el ASA si hay un **nameif** en la interfaz de la Administración 0/0. El ASA cae las conexiones que pasan a través de otras interfaces como tráfico del por--cuadro porque la dirección IP pertenece a la subred del **nameif de la** “Administración”. Esto puede también causar los problemas porque el IPS necesita los gateways externo para rutear el tráfico correctamente al ASA.

Prefacio

El módulo ips en el ASA 5500X utiliza la interfaz de la Administración 0/0 para comunicar con el mundo exterior. Este documento proporciona la información sobre cómo configurar esta interfaz en los entornos múltiples.

Los escenarios Allto incluyen este Esquema de dirección básico:

- Interfaz exterior ASA: 203.0.113.1/24
- Interfaz interior ASA: 198.51.100.1/24
- Interfaz de administración ASA: 192.0.2.1/24
- Direccionamiento de la Administración de IPS: 192.0.2.2/24

Los escenarios Allto asumen que la interfaz interior y la Administración 0/0 están conectadas con el mismo Switch.

Nota: Si hay un **nameif** assisgned a la interfaz de la Administración 0/0 ASA, un dispositivo de la capa 3 con las interfaces en los redes secundarios del **nameif del** “interior” y de la “Administración” se requiere. El IPS también requiere que el default gateway para el IPS esté situado en ese dispositivo de la capa 3.

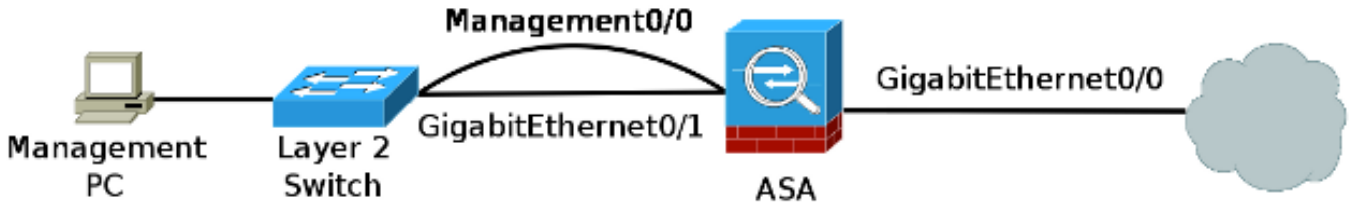
Escenarios

Escenario 1

Mejor práctica para la configuración de la Administración IPS y ASA

1. La Administración IPS y ASA no puede ambos ser accedida a través de la interfaz de la Administración 0/0.
2. No debe haber **nameif** asignado a la interfaz de la Administración 0/0 ASA. Acceden a la Administración ASA en las interfaces del transporte del tráfico.
3. El IPS se da una dirección IP accesible del **nameif del** “interior”.
4. El acceso del “interior” ocurre a través del Switch o del router, sin la implicación del ASA.
5. Para permitir la Administración del exterior, crear una traducción de dirección de red estática (NAT) para la dirección IP del sensor, o definir el **puerto que remite al** puerto apropiado (la redirección de puerto se utiliza en este ejemplo).

En este escenario, las comunicaciones de Administración de IPS a la red externa se comportan similar a cualquier otro host en la red interna. Esto se utiliza para las actualizaciones de firma, la correlación global, y las peticiones de la licencia del servicio IPS.



Configuración:

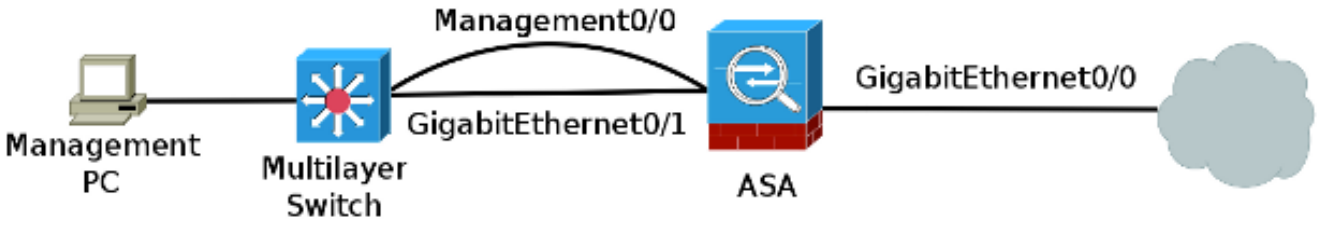
```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 no nameif security-level 0 management-only !! same-security-traffic
permit inter-interface same-security-traffic permit intra-interface object network IPS-
management host 198.51.100.2 object network ASA-inside host 198.51.100.1 object network ASA-
outside host 203.0.113.1 object-group service HTTP service-object tcp-udp destination eq www
service-object tcp destination eq https access-list global_access extended permit ip any any
access-list global_access_1 remark Allow IPS management out through to the internet. access-list
global_access_1 extended permit object-group HTTP object IPS-management any nat (inside,outside)
source dynamic IPS-management IPS-management interface nat (inside,outside) static IPS-
management ASA-outside service tcp 443 65432 !! Use of an ephemeral port allows for the use of
common ports for other !! network applications. This also conceals the actual management port by
making it !! not well known. ASA# show module ips details | include Mgmt Mgmt IP addr:
198.51.100.2 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 198.51.100.1 Mgmt Access List:
0.0.0.0/0 Mgmt web ports: 443 Mgmt TLS enabled: true
```

Escenario 2

La Administración de IPS está en la misma subred como el nameif de la “Administración” y está en una red de la capa 3

1. Señale el gateway del IPS a una interfaz de la capa 3 en la red con excepción del IP del **nameif de la** Administración ASA. Este dispositivo debe soportar la encaminamiento entre ambas subredes; por ejemplo, `192.0.2.2/24,192.0.2.254`.
2. Cree una Static ruta en la interfaz interior del ASA para señalar el tráfico a la dirección IP de la interfaz de la capa 3; por ejemplo, `rutee 192.0.2.2 interior 255.255.255.255 192.0.1.254`.
3. Aseegurese todo el Access Control List (ACL) y las reglas NAT se aplican a la dirección IP de la Administración de IPS.

En esta configuración, el IPS envía los pedidos las actualizaciones de la **correlación**, las peticiones de la **licencia** y las **actualizaciones de firma globales IPS al** default gateway (`192.0.2.254`), y se traduce a la dirección externa. Las rutas de tráfico de retorno detrás vía la ruta del interior y se remiten al dispositivo de la capa 3 que contiene una interfaz en el interior y las redes de administración.



Configuración:

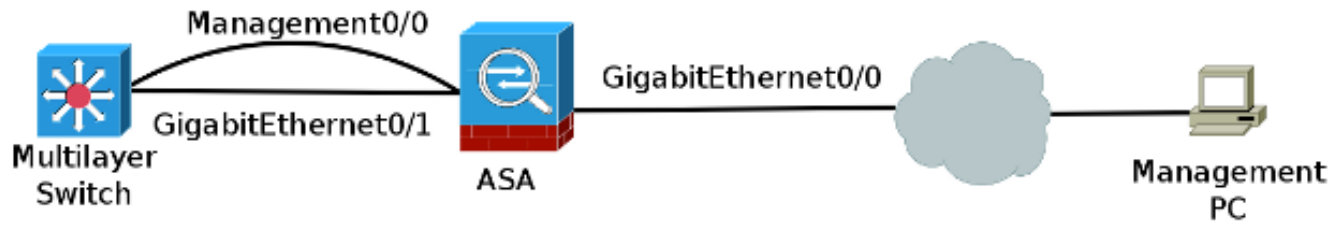
```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 100 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 nameif management security-level 0 ip address 192.0.2.1 255.255.255.0 !!
same-security-traffic permit inter-interface same-security-traffic permit intra-interface
object-group service HTTP service-object tcp-udp destination eq www service-object tcp
destination eq https access-list global_access extended permit ip any any access-list
global_access_1 remark Allow IPS management out through to the internet. access-list
global_access_1 extended permit object-group HTTP host 192.0.2.2 any route inside 192.0.2.2
255.255.255.255 198.51.100.254 1 ASA# show module ips details | include Mgmt Mgmt IP addr:
192.0.2.2 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 192.0.2.254 Mgmt Access List: 0.0.0.0/0
Mgmt web ports: 443 Mgmt TLS enabled: true
```

Escenario 3

La Administración de IPS es necesaria de la interfaz exterior y hay un nameif de la "Administración"

1. Señale el gateway del IPS a una interfaz de la capa 3 en la red con excepción del IP del **nameif de la** Administración ASA. Este dispositivo debe soportar la encaminamiento entre ambas subredes.
2. Cree una Static ruta en la interfaz interior del ASA para señalar el tráfico a la dirección IP de la interfaz de la capa 3.
3. Aseegurese todas las reglas ACL y NAT aplicarse a la dirección IP de la Administración de IPS.

Todo es lo mismo que arriba, a menos que un ACL se deba escribir para permitir que un host del exterior maneje el IPS.



Configuración:

```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 nameif management security-level 0 ip address 192.0.2.1 255.255.255.0
management-only !! same-security-traffic permit inter-interface same-security-traffic permit
intra-interface object network ASA-management host 192.0.2.1 object network ASA-inside host
198.51.100.1 object network IPS-management host 192.0.2.2 object-group service HTTP service-
object tcp-udp destination eq www service-object tcp destination eq https access-list
global_access extended permit ip any any access-list global_access_1 remark Allow IPS management
out through to the internet. access-list global_access_1 extended permit object-group HTTP
object IPS-management any object-group service MGMT_SERVICES service-object tcp-udp destination
eq http service-object tcp destination eq https service-object tcp destination eq ssh access-
list outside_access_in line 1 remark Allow outside management to IPS. access-list
outside_access_in line 2 extended permit object-group MGMT_SERVICES host 203.0.113.1 object IPS-
management access-group outside_access_in in interface outside nat (inside,outside) source
dynamic IPS-management IPS-management interface route inside 192.0.2.2 255.255.255.255
198.51.100.254 1 ASA# show module ips details | include Mgmt Mgmt IP addr: 192.0.2.2 Mgmt
Network mask: 255.255.255.0 Mgmt Gateway: 192.0.2.254 Mgmt Access List: 0.0.0.0/0 Mgmt web
ports: 443 Mgmt TLS enabled: true
```

Situación 4

Túnel IPsec conectado directamente con el ASA

1. La terminación de un túnel VPN al ASA tiene el mismo efecto que la Administración de la interfaz en la cual usted termina el VPN.
2. Una vez que usted ha puesto su VPN, usted necesita escribir una ruta de la interfaz en la cual el VPN termina al Next-Hop a un gateway interno de la capa 3.
3. La Administración de IPS también necesita señalar a un gateway que no resida en el ASA, solamente al interior el **nameif de la** “Administración”.
4. Si no hay dispositivos de la capa 3 detrás del ASA, usted debe quitar el **nameif de la** “Administración” y el IP Address en la Administración 0/0 ASA, y después ingresa el IPS en la subred del **nameif del** “interior”.

El tráfico de administración que sale del IPS trabaja lo mismo que en una red sin la conexión VPN. Sin embargo, el Acceso de administración se debe dirigir de la red en la cual el VPN termina.

Configuración:

```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 nameif management security-level 0 ip address 192.0.2.1 255.255.255.0
management-only !! same-security-traffic permit inter-interface same-security-traffic permit
intra-interface object network ASA-management host 192.0.2.1 object network ASA-inside host
198.51.100.1 object network IPS-management host 192.0.2.2 object-group service
```

DM_INLINE_SERVICE_1 service-object tcp-udp destination eq www service-object tcp destination eq https access-list global_access extended permit ip any any access-list global_access_1 remark Allow IPS management out through to the internet. access-list global_access_1 extended permit object-group DM_INLINE_SERVICE_1 object IPS-management any no pager logging enable ip local pool vpn 198.51.100.3-198.51.100.49 mask 255.255.255.0 icmp unreachable rate-limit 1 burst-size 1 icmp permit any outside icmp permit any inside access-group global_access_1 global route outside 0.0.0.0 0.0.0.0 203.0.113.2 route inside 192.0.2.2 255.255.255.255 198.51.100.254 1 dynamic-access-policy-record DfltAccessPolicy description "access" webvpn svc ask enable default svc user-identity default-domain LOCAL aaa authentication ssh console LOCAL http server enable http 0.0.0.0 0.0.0.0 outside crypto ipsec ikev1 transform-set tranny esp-aes esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac crypto ipsec security-association lifetime kilobytes 20000 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5 crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map outside_map interface outside crypto map inside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map inside_map interface inside crypto ca trustpoint ASDM_TrustPoint0 enrollment self subject-name CN=ciscoasa proxy-ldc-issuer crl configure crypto ca certificate chain ASDM_TrustPoint0 crypto isakmp identity address crypto ikev2 remote-access trustpoint ASDM_TrustPoint0 crypto ikev1 enable outside crypto ikev1 enable inside crypto ikev1 policy 5 authentication pre-share encryption aes hash md5 group 2 lifetime 86400 ssh 0.0.0.0 0.0.0.0 outside ssh timeout 60 console timeout 0 dhcp-client client-id interface outside ssl trust-point ASDM_TrustPoint0 inside ssl trust-point ASDM_TrustPoint0 outside webvpn port 8080 enable outside enable inside dtls port 8080 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 2 anyconnect profiles ANYconnect disk0:/anyconnect.xml anyconnect enable group-policy DfltGrpPolicy attributes vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless address-pools value vpn webvpn anyconnect profiles value ANYconnect type user ASA# **show module ips detail | include Mgmt** Mgmt IP addr: 192.0.2.2 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 192.0.2.254 Mgmt Access List: 0.0.0.0/0 Mgmt web ports: 443 Mgmt TLS enabled: true

Información Relacionada

- Cómo verificar las alertas del examen y de la firma del tráfico IPS
- Soporte Técnico y Documentación - Cisco Systems