Cenários de configuração do Gerenciamento de IPS em um módulo ips 5500x

Índice

Introdução

Este documento fornece cenários de configuração em um módulo de Intrusion Preventions Systems (IPS) no Adaptive Security Appliance (ASA) 5500x.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Módulos ips ASA 5500x

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Módulos ips ASA 5500x

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

Background

Com a introdução do ASA 5500x e a implementação de software do IPS, há umas alterações fundamentais à maneira que é permitido ao Gerenciamento de IPS se comportar.

1. O IPS pode somente usar a relação do Gerenciamento 0/0 para o acesso de gerenciamento externo.
2. Se o ASA tem um **nameif** atribuído ao Gerenciamento 0/0, o IPS deve ter um endereço na mesma sub-rede como o **nameif**.
3. Você não pode remover o comando do **Gerenciamento-somente da** relação do Gerenciamento 0/0 do ASA.
4. Se o ASA tenta distribuir o tráfego com o **nameif do Gerenciamento** com a indicação do “Gerenciamento-somente”, o ASA deixa cair o tráfego.
5. Se não há nenhum **nameif** atribuído ao Gerenciamento 0/0, o IPS funciona similarmente à interface de gerenciamento avançada dos módulos do módulo de Serviços de segurança da inspeção e da prevenção (AIP-SSM).

Estes comportamentos inibem comunicações do IPS às redes externas que passam com o ASA se há um **nameif na** relação do Gerenciamento 0/0. O ASA deixa cair as conexões que passam através de outras relações como o tráfego da através--caixa porque o endereço IP de Um ou Mais Servidores Cisco ICM NT pertence à sub-rede do **nameif do** “Gerenciamento”. Isto pode igualmente causar problemas porque o IPS precisa gateways externos a fim distribuir corretamente o tráfego ao ASA.

Prefácio

O módulo ips no ASA 5500X usa a relação do Gerenciamento 0/0 para comunicar-se com o mundo exterior. Este documento fornece a informação em como estabelecer esta relação em ambientes múltiplos.

Todos os cenários incluem este esquema de endereço básico:

- Interface externa ASA: 203.0.113.1/24
- Interface interna ASA: 198.51.100.1/24
- Interface de gerenciamento ASA: 192.0.2.1/24
- Endereço do Gerenciamento de IPS: 192.0.2.2/24

Todos os cenários supõem que a interface interna e o Gerenciamento 0/0 estão conectados ao mesmo interruptor.

Nota: Se há um **nameif** assisgned à relação do Gerenciamento 0/0 ASA, um dispositivo da camada 3 com relações em sub-redes do **nameif do** “interior” e do “Gerenciamento” está exigido. O IPS igualmente exige que o gateway padrão para o IPS esteja ficado situado nesse dispositivo da camada 3.

Encenações

Cenário 1

Melhor prática para a instalação do Gerenciamento IPS e ASA

1. O Gerenciamento IPS e ASA não pode ambos ser alcançado através da relação do Gerenciamento 0/0.
2. Não deve haver nenhum **nameif** atribuído à relação do Gerenciamento 0/0 ASA. O Gerenciamento ASA é alcançado em relações do rolamento do tráfego.
3. O IPS é dado um endereço IP de Um ou Mais Servidores Cisco ICM NT alcançável do **nameif do** “interior”.
4. O acesso do “interior” ocorre através do interruptor ou do roteador, sem participação do ASA.
5. A fim permitir o Gerenciamento da parte externa, criar uma tradução de endereço da rede estática (NAT) para o endereço IP de Um ou Mais Servidores Cisco ICM NT do sensor, ou definir a **porta que envia à** porta apropriada (o redirecionamento de porta é usado neste exemplo).

Nesta encenação, as comunicações de Gerenciamento de IPS à rede externa comportam-se similar a todo o outro host na rede interna. Isto é usado para atualizações de assinatura, a correlação global, e do serviço IPS pedidos da licença.

Configuração:

```
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
```

Cenário 2

O Gerenciamento de IPS está na mesma sub-rede como o nameif do “Gerenciamento” e está em uma rede da camada 3

1. Aponte o gateway do IPS a uma relação da camada 3 na rede a não ser o IP do **nameif do** Gerenciamento ASA. Este dispositivo deve apoiar o roteamento entre ambas as sub-redes; por exemplo, `192.0.2.2/24,192.0.2.254`.
2. Crie uma rota estática na interface interna do ASA para apontar o tráfego ao endereço IP de Um ou Mais Servidores Cisco ICM NT da relação da camada 3; por exemplo, `distribua 192.0.2.2 interno 255.255.255.255 192.0.1.254`.
3. Certifique-se que todo o Access Control List (ACL) e regras NAT aplique ao endereço IP de Um ou Mais Servidores Cisco ICM NT do Gerenciamento de IPS.

Nesta configuração, o IPS envia pedidos para atualizações **globais da correlação**, **licencia** pedidos e **atualizações de assinatura IPS ao** gateway padrão (`192.0.2.254`), e é traduzido ao endereço exterior. As rotas de tráfego de retorno para trás através da rota do interior e são

enviadas ao dispositivo da camada 3 que abriga uma relação no interior e nas redes de gerenciamento.

Configuração:

```
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
```

Cenário 3

O Gerenciamento de IPS é precisado da interface externa e há um nameif do “Gerenciamento”

1. Aponte o gateway do IPS a uma relação da camada 3 na rede a não ser o IP do **nameif do** Gerenciamento ASA. Este dispositivo deve apoiar o roteamento entre ambas as sub-redes.
2. Crie uma rota estática na interface interna do ASA para apontar o tráfego ao endereço IP de Um ou Mais Servidores Cisco ICM NT da relação da camada 3.
3. Certifique-se de todas as regras ACL e NAT aplicar-se ao endereço IP de Um ou Mais Servidores Cisco ICM NT do Gerenciamento de IPS.

Tudo é o mesmo que acima, a não ser que um ACL deva ser escrito para permitir que um host da parte externa controle o IPS.

Configuração:

```
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
```

Encenação 4

Túnel de IPsec conectado diretamente ao ASA

1. A terminação de um túnel VPN ao ASA tem o mesmo efeito que o Gerenciamento da relação em que você termina o VPN.
2. Uma vez que você setup seu VPN, você precisa de escrever uma rota da relação em que o VPN termina ao salto seguinte a um gateway interno da camada 3.
3. O Gerenciamento de IPS igualmente precisa de apontar a um gateway que não resida no ASA, mas ao interior o **nameif do** “Gerenciamento”.
4. Se não há nenhum dispositivo da camada 3 atrás do ASA, você deve remover o **nameif do** “Gerenciamento” e o endereço IP de Um ou Mais Servidores Cisco ICM NT no Gerenciamento 0/0 ASA, e incorpora então o IPS à sub-rede do **nameif do** “interior”.

O tráfego de gerenciamento que sae do IPS trabalha o mesmos que em uma rede sem a conexão de VPN. Contudo, o acesso de gerenciamento deve ser endereçado da rede em que o VPN termina.

Configuração:

```
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
```

Informações Relacionadas

- Como verificar alertas da inspeção e da assinatura do tráfego IPS
- Suporte Técnico e Documentação - Cisco Systems