Scénarios de configuration de Gestion IPS sur un module 5500x IPS

Contenu

Introduction

Ce document fournit des scénarios de configuration sur un module des systèmes des préventions des intrusions 5500x de l'appliance de sécurité adaptable (ASA) (IPS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modules ASA 5500x IPS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Modules ASA 5500x IPS

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Fond

Avec l'introduction de l'ASA 5500x et l'implémentation de logiciel d'IPS, il y a les modifications fondamentales à la manière on permet qu'à la Gestion IPS pour se comporter.

1. L'IPS peut seulement utiliser l'interface de la Gestion 0/0 pour l'accès externe de Gestion.
2. Si l'ASA a un **nameif** assigné à la Gestion 0/0, l'IPS doit avoir une adresse dans le même sous-réseau que le **nameif**.
3. Vous ne pouvez pas retirer la commande **réservée à la Gestion de l'**interface de la Gestion 0/0 de l'ASA.
4. Si les essais ASA pour conduire le trafic par le **nameif de Gestion** avec la déclaration « réservée à la Gestion », l'ASA relâche le trafic.
5. S'il n'y a aucun **nameif** assigné à la Gestion 0/0, les fonctions IPS pareillement à l'interface de gestion de modules d'Advanced Inspection and Prevention Security Services Module (AIP SSM).

Ces comportements empêchent des transmissions de l'IPS aux réseaux externes qui traversent l'ASA s'il y a un **nameif** sur l'interface de la Gestion 0/0. L'ASA relâche les connexions qui traversent d'autres interfaces comme trafic d'à travers-le-case parce que l'adresse IP appartient au sous-réseau de **nameif de** « Gestion ». Ceci peut également poser des problèmes parce que l'IPS a besoin de passerelles externes afin de conduire le trafic correctement à l'ASA.

Préface

Le module IPS sur l'ASA 5500X emploie l'interface de la Gestion 0/0 pour communiquer avec le monde extérieur. Ce document fournit des informations sur la façon dont installer cette interface dans de plusieurs environnements.

Tous les scénarios incluent ce schéma de base d'adresse :

- ASA en dehors d'interface : 203.0.113.1/24
- Interface interne ASA : 198.51.100.1/24
- Interface de gestion ASA : 192.0.2.1/24
- Adresse de Gestion IPS : 192.0.2.2/24

Tous les scénarios supposent que l'interface interne et la Gestion 0/0 sont connectées au même commutateur.

Remarque: S'il y a un **nameif** assisgned à l'interface de la Gestion 0/0 ASA, un périphérique de la couche 3 avec des interfaces dans des sous-réseaux de **nameif de** « intérieur » et de « Gestion » est exigé. L'IPS exige également que la passerelle par défaut l'IPS se trouvent sur ce périphérique de la couche 3.

Scénarios

Scénario 1

Pratique recommandée pour l'installation de la Gestion IPS et ASA

1. La Gestion IPS et ASA ne peut pas chacun des deux être accédée à par l'interface de la Gestion 0/0.
2. Il ne devrait y avoir aucun **nameif** assigné à l'interface de la Gestion 0/0 ASA. La Gestion ASA est accédée à sur des interfaces d'incidence du trafic.
3. L'IPS est indiqué une adresse IP accessible du **nameif de** « intérieur ».
4. Access du « intérieur » se produit par le commutateur ou le routeur, sans implication de l'ASA.
5. Afin de permettre la Gestion de l'extérieur, créer une traduction d'adresses de réseau statique (NAT) pour l'adresse IP de capteur, ou définir la **transmission du port au** port approprié (la redirection de port est utilisée dans cet exemple).

Dans ce scénario, les transmissions de Gestion IPS au réseau extérieur se comporte semblable à n'importe quel autre hôte sur le réseau intérieur. Ceci est utilisé pour des mises à jour de signature, la corrélation globale, et des demandes de permis de service IPS.

Configuration :

```
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
```

Scénario 2

La Gestion IPS est dans le même sous-réseau que le nameif de « Gestion » et est dans un réseau de la couche 3

1. Indiquez la passerelle de l'IPS une interface de la couche 3 dans le réseau autre que l'IP de **nameif de** Gestion ASA. Ce périphérique doit prendre en charge le routage entre les deux sous-réseaux ; par exemple, `192.0.2.2/24,192.0.2.254`.
2. Créez une artère statique sur l'interface interne de l'ASA pour indiquer le trafic l'adresse IP d'interface de la couche 3 ; par exemple, `conduisez 192.0.2.2 intérieur 255.255.255.255 192.0.1.254`.
3. Assurez-vous que toute la liste de contrôle d'accès (ACL) et règles NAT appliquez à l'adresse IP de la Gestion IPS.

Dans cette configuration, l'IPS envoie des demandes des mises à jour de **corrélation**, des demandes de **permis** et des mises à jour **globales de signature IPS à la** passerelle par défaut (`192.0.2.254`), et est traduit à l'adresse d'extérieur. Renvoyez les artères de trafic de retour par l'intermédiaire de l'artère d'intérieur et êtes expédié au périphérique de la couche 3 qui loge une interface dans l'intérieur et les réseaux de gestion.

Configuration :

```
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
```

Scénario 3

La Gestion IPS est nécessaire de l'interface extérieure et il y a un nameif de « Gestion »

1. Indiquez la passerelle de l'IPS une interface de la couche 3 dans le réseau autre que l'IP de **nameif de** Gestion ASA. Ce périphérique doit prendre en charge le routage entre les deux sous-réseaux.
2. Créez une artère statique sur l'interface interne de l'ASA pour indiquer le trafic l'adresse IP d'interface de la couche 3.
3. Veillez tous les ACL et règles NAT pour s'appliquer à l'adresse IP de la Gestion IPS.

Tout est identique comme ci-dessus, à moins qu'un ACL doive être écrit pour permettre à un hôte de l'extérieur pour gérer l'IPS.

Configuration :

```
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
```

Scénario 4

Tunnel d'IPSec directement connecté à l'ASA

1. L'arrêt d'un tunnel VPN à l'ASA a le même effet que la Gestion de l'interface sur laquelle vous terminez le VPN.
2. Une fois que vous avez installé votre VPN, vous devez écrire une artère de l'interface sur

laquelle le VPN se termine au prochain-saut à une passerelle interne de la couche 3.

3. La Gestion IPS doit également indiquer une passerelle qui ne réside pas sur l'ASA, mais l'intérieur le **nameif de** « Gestion ».
4. S'il n'y a aucun périphérique de la couche 3 derrière l'ASA, vous devez retirer le **nameif de** « Gestion » et l'adresse IP sur la Gestion 0/0 ASA, et puis écrivez l'IPS dans le sous-réseau de **nameif de** « intérieur ».

Le trafic d'administration qui laisse l'IPS fonctionne les mêmes que dans un réseau sans connexion VPN. Cependant, l'accès de Gestion doit être adressé du réseau sur lequel le VPN se termine.

Configuration :

```
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
```

Informations connexes

- Comment vérifier des alertes d'inspection et de signature du trafic IPS

- Support et documentation techniques - Cisco Systems