5500x IPS モジュールの IPS 管理設定シナリオ

目次

概要

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）5500x 侵入防御システム（IPS）モジュールの設定シナリオについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA 5500x IPS モジュール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ASA 5500x IPS モジュール

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ASA 5500x を導入して IPS のソフトウェアを実装すると、IPS 管理で許可されている動作方法が大きく変更されます。

1. IPS は、外部管理アクセス用に管理 0/0 インターフェイスのみを使用できます。
2. ASA に管理 0/0 に割り当てられた **nameif** がある場合、IPS は同じサブネット内に **nameif** のアドレスを持つ必要があります。
3. ASA の管理 0/0 インターフェイスから、**management-only** コマンドを削除することはできません。
4. ASA が「management-only」ステートメントを使用して、**management nameif** からトラフィックをルーティングしようとすると、ASA でトラフィックがドロップされます。
5. 管理 0/0 に **nameif** が割り当てられていない場合、IPS は Advanced Inspection and Prevention Security Services Module（AIP-SSM）モジュール管理インターフェイスと同様に機能します。

これらの動作により、管理 0/0 インターフェイスに **nameif** がある場合は ASA をパススルーする IPS から外部ネットワークへの通信が阻害されます。 ASA は、through-the-box トラフィックとして他のインターフェイスをパススルーする接続をドロップします。これは、IP アドレスが「管理」**nameif** サブネットに属しているためです。 また、これにより、トラフィックを ASA に適切にルーティングするための外部ゲートウェイが IPS に必要になるため、問題が発生します。

はじめに

ASA 5500X の IPS モジュールは、管理 0/0 インターフェイスを使用して外部と通信します。 このドキュメントでは、さまざまな環境におけるこのインターフェイスの設定方法について説明します。

全シナリオに、次の基本アドレス スキームが含まれています。

- ASA 外部インターフェイス： 203.0.113.1/24
- ASA 内部インターフェイス： 198.51.100.1/24
- ASA 管理インターフェイス： 192.0.2.1/24
- IPS 管理アドレス： 192.0.2.2/24

全シナリオで、内部インターフェイスと管理 0/0 が同じスイッチに接続されていることが想定されています。

注: nameif が ASA 管理 0/0 インターフェイスに割り当てられている場合、「内部」および「管理」**nameif** サブネットワークを備えたレイヤ 3 デバイスが必要です。 IPS ではまた、レイヤ 3 デバイスに配置する IPS のデフォルト ゲートウェイが必要です。

シナリオ

シナリオ 1

IPS 管理と ASA 管理のセットアップにおけるベスト プラクティス

1. IPS 管理と ASA 管理は、いずれも管理 0/0 インターフェイス経由でアクセスできません。
2. **nameif** は ASA 管理 0/0 インターフェイスに割り当てられません。 ASA 管理は、トラフィック ベアリング インターフェイスからアクセスできます。
3. IPS には、「内部」**nameif** からアクセスできる IP アドレスが割り当てられます。

4. 「内部」からのアクセスは、ASA が関与することなく、スイッチまたはルータを通じて行われます。
5. 外部からの管理を可能にするには、センサの IP アドレスのスタティック NAT を作成するか、または適切なポートに**ポート フォワーディング**を定義します（この例では、ポート リダイレクションが使用されています）。

このシナリオでは、外部ネットワークへの IPS 管理通信は、内部ネットワークの他のホストと同様に動作します。 これは、シグニチャ アップデート、グローバル相関、IPS サービス ライセンスのリクエストに使用されます。

設定：

```
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
```

シナリオ 2

IPS 管理が「管理」nameif として同じサブネット内に存在し、レイヤ 3 ネットワークにある場合

1. IPS のゲートウェイを、ASA 管理 **nameif** IP ではなく、ネットワーク内のレイヤ 3 インターフェイスにポイントさせます。 このデバイスでは、 192.0.2.2/24,192.0.2.254 などの両方のサブネット間のルーティングをサポートする必要があります。
2. ASA の内部インターフェイスにスタティック ルートを作成し、トラフィックを route inside 192.0.2.2 255.255.255.255 192.0.1.254 1 などのレイヤ 3 インターフェイス IP アドレスにポイントさせます。
3. すべてのアクセス コントロール リスト（ACL）と NAT ルールが、IPS 管理の IP アドレスに適用されていることを確認します。

この設定では、IPS は **グローバル相関**のアップデート、**ライセンス** リクエスト、**IPS シグニチャ** アップデートのリクエストをデフォルト ゲートウェイ（192.0.2.254）に送信し、外部アドレスに変換します。 トラフィック ルートは内部ルートを経由して戻り、内部および管理ネットワーク内のインターフェイスを有するレイヤ 3 デバイスに転送されます。

設定：

```
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
```

シナリオ 3

IPS 管理が外部インターフェイスから必要で、「管理」nameif がある場合

1. IPS のゲートウェイを、ASA 管理 **nameif** IP ではなく、ネットワーク内のレイヤ 3 インターフェイスにポイントさせます。 このデバイスは、両方のサブネット間のルーティングをサポートする必要があります。
2. ASA の内部インターフェイスにスタティック ルートを作成し、トラフィックをレイヤ 3 インターフェイスの IP アドレスにポイントさせます。
3. すべての ACL と NAT ルールが、IPS 管理の IP アドレスに適用されていることを確認します。

ACL を書き込み、外部からホストで IPS を管理できるほかは、前述の手順と同じです。

設定：

```
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
```

シナリオ 4

ASA に直接接続されている IPSec トンネル

1. VPN トンネルから ASA への終端には、VPN を終端するインターフェイスからの管理と同じ効果があります。
2. VPN をセットアップしたら、VPN をネクストホップと内部レイヤ 3 ゲートウェイに終端するインターフェイスからルートを書き込みます。
3. IPS 管理では、ASA になく、「管理」**nameif** 内部にあるゲートウェイにポイントさせる必要があります。
4. ASA にレイヤ 3 デバイスがない場合は、「管理」**nameif** と ASA 管理 0/0 の IP アドレスを削除して、「内部」**nameif** サブネットの IPS を入力する必要があります。

IPS を離れる管理トラフィックは、VPN 接続なしでもネットワーク内で同様に機能します。 ただし、管理アクセスについては VPN を終端するネットワークから対処する必要があります。

設定：

```
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
```

関連情報

- IPS トラフィックのインスペクションとシグニチャ アラートの確認方法
- テクニカルサポートとドキュメント - Cisco Systems