ASA 5500-X IPS モジュールのインターネットアクセス

目次

概要

新しい適応型セキュリティ アプライアンス（ASA）5500-X 侵入防御システム（IPS）モジュールは、その設計により、Management 0/0 ポートでの through-the-box トラフィックを許可しません。 このため、IPS が ASA の管理インターフェイスの IP アドレスをデフォルト ゲートウェイとして使用するように設定すると、その他のインターフェイスの背後にあるホストからセンサーを管理したり、それにアクセスしたりできなくなります。 また、センサーはインターネットに達することができなくなります。

このドキュメントでは、ASA 経由でインターネットにアクセスするように、新しい ASA 5500-X IPS モジュールを設定する方法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 5500-X 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 5500-X IPS モジュール

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

機能情報

5512-5555 アプライアンスは IPS とシームレスに統合しており、ソフトウェア モジュールとして動作します。 IPS 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。 現在、Management 0/0 ポートは、ASA 5500-X シリーズのデバイスで through-the-box トラフィックを許可しません。 この問題は、とくに Management 0/0 インターフェイスを IPS のデフォルト ゲートウェイとして設定しているとき、使いやすさに影響します。

トラブルシューティング方法

前提条件：

IPS 機能ライセンスが ASA にインストールされている必要があります。 IPS モジュールを有効にするためにこれが必要となります。 これを確認するには、**show version** コマンドを ASA で使用します。 「**IPS Module: Enabled**」が **show version** の出力に表示されることを確認してください。

```
ASA(config)# show module

           Mod Card Type                                    Model              Serial No.
           --- -------------------------------------------- ------------------ -----------
             0 ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC ASA5515            FCH1549776V
           ips ASA 5515-X IPS Security Services Processor   ASA5515-IPS        FCH1549776V

           Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
           --- --------------------------------- ------------ ------------ ---------------
             0 503d.e59d.90a0 to 503d.e59d.90a7  1.0          2.1(9)8      8.6(1)
           ips 503d.e59d.909e to 503d.e59d.909e  N/A          N/A          7.1(4)E4

           Mod SSM Application Name           Status           SSM Application Version
           --- ------------------------------ ---------------- --------------------------
           ips IPS                            Up               7.1(4)E4

           Mod Status             Data Plane Status     Compatibility
           --- ------------------ --------------------- -------------
             0 Up Sys             Not Applicable
           ips Up                 Up

           Mod License Name   License Status  Time Remaining
           --- -------------- --------------- ---------------
           ips IPS Module     Enabled         perpetual
```

回避策

IPS モジュールがインターネットにアクセスできるようにするには（自動更新や Global Correlation などのために）、ASA の Management 0/0 ポートをレイヤ 3 デバイスに接続します

。

たとえば、ASA 内のルータか ASA にローカルのルータの空きポートに Management 0/0 ポートを接続できます。 ルータは、ASA の内部インターフェイスをポイントするデフォルト ゲートウェイを含むことができるようになります。 次の手順を実行します。

1. ASA の Management 0/0 ポートをレイヤ 3 デバイスに接続します。 また、ASA の内部インターフェイスとこのレイヤ 3 デバイスとの間で接続を確立します。
2. IPS モジュールの Management IP アドレスを設定します。 このアドレスが ASA Management インターフェイス IP アドレスと同じサブネット上にあることを確認します。 この例では、ASA の Management0/0 インターフェイスに 10.1.1.1 が、IPS Management インターフェイスに 10.1.1.2 が割り当てられます。
3. 上記のレイヤ 3 デバイスとして、IPS モジュールでデフォルト ゲートウェイを設定します。 適切なルートまたはデフォルトゲートウェイをレイヤ 3 デバイスで相応に設定し、ASA の内部インターフェイスに必要なトラフィックを転送する必要があります。
4. スタティック ルートを ASA で設定し、リターン トラフィックがこのレイヤ 3 デバイスを介して IPS モジュールに達するようにします。

トポロジ：

設定例：

ルータ：

```
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
end
!
interface GigabitEthernet0/1
 ip address 10.1.1.3 255.255.255.0
 duplex auto
 speed auto
end
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA 5515：

```
ASA# show running-config
: Saved
:
ASA Version 8.6(1)2
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif internet
 security-level 0
 ip address 172.16.103.73 255.255.255.0
!
interface Management0/0
 nameif management
```

```
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
object network obj-10.0.0.0
 subnet 10.1.0.0 255.255.0.0
!
object network obj-10.0.0.0
 nat (inside,internet) dynamic interface
!
route internet 0.0.0.0 0.0.0.0 172.16.103.64 1
!--- Route configured to reach the ips module through the internal router route inside 10.1.1.2
255.255.255.255 192.168.1.2 1
```

ASA 5515-IPS：

```
sensor#show configuration
! ------------------------------
! Current configuration last modified Sun Sep 18 00:06:25 2012
! ------------------------------
! Version 7.1(4)! Host:
!     Realm Keys          key1.0
! Signature Definition:!     Signature Update    S615.0   2012-01-03
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
!--- The management IP address is set. host-ip 10.1.1.2/24,10.1.1.3 !--- The access-list is set
to allow management from the 10.0.0.0/8 network. access-list 10.0.0.0/8 dns-primary-server
enabled !--- The DNS server IP address is set. address 8.8.8.8 exit exit exit
```

IPS のために Management 0/0 ポートで through-the-box トラフィックを許可するように求める機能要求が上がっています。

詳細については、 Cisco Bug ID CSCua67798（登録ユーザ専用）： ENH ASA 5500-X -「管理ポートにおける through-the-box トラフィックの許可」を参照してください。

FAQ

Q： ネットワーク内のレイヤ 3 デバイスをデフォルト ゲートウェイがポイントするようにしていません。 IPS はどのようにインターネットに達することができますか。

A： その他の設計については、ドキュメント /c/en/us/support/docs/security/ips-sensor-software-version-71/113690-ips-config-mod-00.html。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems