ASA 5500-X IPS模块的Enable (event)互联网访问

目录

简介

根据设计，新的可适应安全工具(ASA) 5500-X入侵预防系统(IPS)模块不允许在Management0/0端口的通过这方框流量。所以，如果IPS设置使用ASA的管理接口的IP地址作为默认网关，然后传感器不可能从在其他接口后的主机被管理或访问。并且，传感器不能到达互联网。

本文解释如何设置新的ASA 5500-X IPS模块通过ASA访问互联网。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA 5500-X IPS模块

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 5500-X IPS模块

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能信息

5512-5555个设备无缝地集成与IPS，运行作为软件模块。IPS管理接口共享与ASA的Management0/0接口。目前， Management0/0端口不允许在ASA的通过这方框流量5500-X系列设备。特别是当Management0/0接口设置作为IPS的时，默认网关此问题影响易用。

故障排除方法

前提条件：

在ASA安装的IPS功能许可证。这要求启用IPS模块。使用**show version命令**在ASA，这可以验证。检查**IPS模块：启用**在**show version输出**。

```
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
```

解决方法

为了使IPS模块访问互联网(例如自动更新、全局相关性等等)，请连接ASA的Management0/0端口对第3层设备。

例如， Management0/0端口可以连接到路由器的空闲端口内部或本地对ASA。路由器能，反过来，有指向ASA的里面/内部接口的默认网关。完成这些步骤：

1. 连接ASA的Management0/0端口对第3层设备。并且， ASA的内部接口的之间建立连接和此第3层设备。
2. 配置IPS模块的管理IP地址。确保此地址在相同子网作为ASA管理接口IP地址。在示例中，10.1.1.1分配到ASA和10.1.1.2的Management0/0接口对IPS管理接口。
3. 配置在IPS模块的默认网关作为以上提到的第3层设备。在第3层设备必须相应地设置适当的路由或默认网关转发必要的流量到ASA的里面/内部接口。

4. 配置在ASA的静态路由，以便回程数据流通过此第3层设备到达IPS模块。

拓扑：

配置示例：

路由器：

```
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
```

功能请求被上升了允许在Management0/0端口的通过这方框流量IPS的。

可以找到详细信息此处：Cisco Bug ID CSCua67798 (仅限注册用户) ：ENH ASA 5500-X -允许在管理端口的通过这方框流量

FAQ

问：我没有一第3层设备在网络点里面默认网关。IPS如何能到达互联网？

回答:参考其他设计的本文：/c/en/us/support/docs/security/ips-sensor-software-version-71/113690-ips-config-mod-00.html。

相关信息

- 技术支持和文档 - Cisco Systems