Enable Internet Access for ASA 5500−X IPS Module

Document ID: 113691

Contributed by Thulasi Shankar and David Houck, Cisco TAC Engineers.
Sep 25, 2012

Contents

Introduction

As per design, the new Adaptive Security Appliance (ASA) 5500−X Intrusion Preventions Systems (IPS) modules does not permit through−the−box traffic on the Management 0/0 port. Therefore, if the IPS is set to use the IP address of the management interface of the ASA as the default gateway, then the sensor cannot be managed or accessed from hosts behind other interfaces. Also, the sensor will not be able to reach the Internet.

This document explains how to set up the new ASA 5500−X IPS modules to access the Internet via the ASA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ASA 5500−X IPS modules

Components Used

The information in this document is based on these software and hardware versions:

- ASA 5500−X IPS modules

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Feature Information

The 5512−5555 appliances are seamlessly integrated with IPS, which runs as a software module. The IPS Management interface shares the Management 0/0 interface with the ASA. Currently, the Management 0/0 port does not allow through−the−box traffic in the ASA 5500−X series of devices. This issue impacts the ease of use, especially when the Management 0/0 interface is set as the default gateway for the IPS.

Troubleshooting Methodology

Prerequisites:

IPS feature license installed on the ASA. This is required to enable the IPS module. This can be verified using the **show version** command on the ASA. Check for **IPS Module: Enabled** in the **show version** output.

```
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
```

Workaround

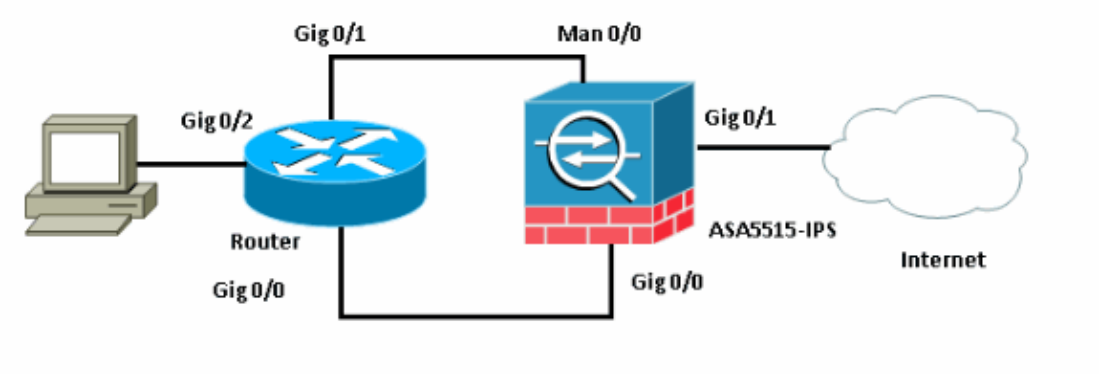
In order to enable the IPS module to access the Internet (for example for auto−updates, Global Correlation, etc.), connect the Management 0/0 port on the ASA to a Layer 3 device.

For example, the Management 0/0 port can be connected to a free port on a router internal or local to the ASA. The router, in turn, can have the default gateway which points to the inside/internal interface of the ASA. Complete these steps:

1. Connect the Management 0/0 port of the ASA to the Layer 3 device. Also, establish connectivity between an internal interface of the ASA and this Layer 3 device.
2. Configure the Management IP address for the IPS module. Make sure this address is on the same subnet as the ASA Management interface IP address. In the example, 10.1.1.1 has been assigned to the Management0/0 interface of the ASA and 10.1.1.2 to the IPS Management interface.

3. Configure the default gateway on the IPS module as the Layer 3 device mentioned above. Appropriate routes or default−gateway must be set accordingly on the Layer 3 device to forward the necessary traffic to the inside/internal interface of the ASA.
4. Configure a static route on the ASA so that the return traffic reaches the IPS module through this Layer 3 device.

Topology:



Sample configuration:

Router:

```
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
```

A feature request has been raised to permit through-the-box traffic on the Management 0/0 port for the IPS.

The details can be found here: Cisco bug ID CSCua67798 (registered customers only) : ENH ASA 5500-X - To permit through-the-box traffic on management port

FAQ

Q: I do not have a Layer 3 device inside the network point the default gateway to. How can the IPS reach the Internet?

A: Refer to this document for other designs:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_tech_note09186a0080bd5d03.shtml.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 25, 2012 Document ID: 113691