Getting Started with Your Cisco IPS

I Introduction

This paper explains the basics of intrusion prevention systems (IPSs) and guides you through getting started with the Cisco® ASA 5500 Series IPS Solution. This paper is geared toward Cisco partners, Cisco customers, or anyone who needs a basic understanding of the Cisco ASA 5500 Series IPS Solution.

The purpose of IPS technology is to look at all data inside network packets to determine if malicious traffic exists within those packets. If an IPS determines that malicious traffic exists within those packets, it will immediately drop the traffic and stop the attack; in less-critical situations, the IPS may just generate an alert to let you know that suspicious traffic was found on your network.

A Cisco IPS will protect your network by making sure:

- Traffic inspected is compliant with TCP/IP.
- All network flows have been correctly built.
- Any attempts to subvert your security device are recognized and stopped.
- Any attempts to compromise your network devices with malicious software are stopped.
- Any new day-zero exploits are stopped.
- Network traffic behaving outside the scope of normal behavior is recognized and stopped.

Deploying a Cisco ASA 5500 Series IPS Solution is a simple, straightforward process that requires four fundamental steps.

- Where to deploy the Cisco ASA 5500 Series IPS Solution
- How to configure and license the ASA
- How to configure the IPS
- How to license, configure, and monitor solution using Cisco IPS Manager Express

II Where to deploy the Cisco ASA 5500 Series IPS Solution

The Cisco ASA 5500 Series IPS Solution needs to be placed in your network at the location where it can provide the maximum amount of protection. For example, if you have different segments defined in your network, such as a segment for users and a separate segment for Web servers and mail servers, where would it make most sense to put your ASA? If you put it between the server segment and the user segment, there is no protection between your users and the Internet. If you put the ASA between your users and the Internet, it is possible that users could plug an infected PC into the network, which makes the server segment vulnerable to infection.

For small and medium-sized businesses (SMBs) or small commercial enterprises, it usually makes sense to place the ASA where the Internet connects to your network and then use it to segment the rest your network. This effectively allows you to protect all areas of your network.

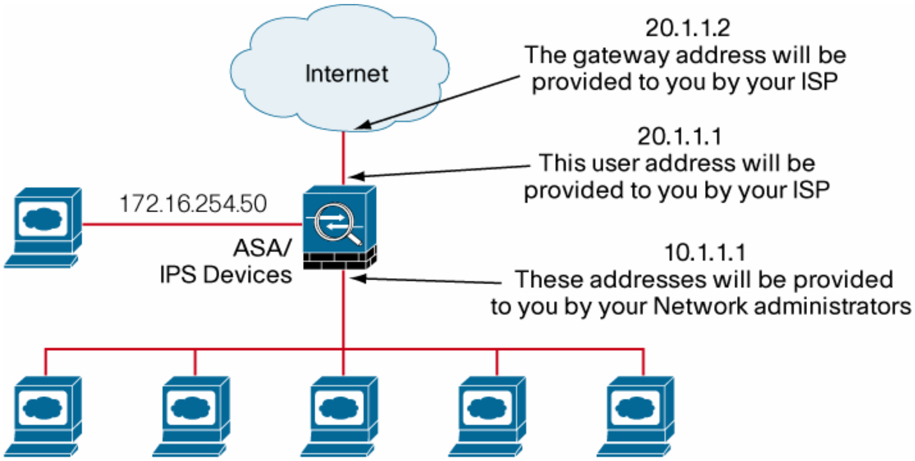
III How to configure and license the ASA

This section explains how to install and configure the Cisco ASA 5500 Series using a single network segment between the Internet and your company network. Installing the ASA in your network is a straightforward process. Both the ASA and the IPS management applications provide easy-to-use wizards to assist you with this installation.

Step 1:

Plug the ASA into the network where you have decided it provides the highest level of security. In this installation setup, the ASA will be put between your Internet edge and a commercial or SMB customer network, as shown in the following illustration.

Figure 1.


Internet
20.1.1.2
The gateway address will be provided to you by your ISP
20.1.1.1
This user address will be provided to you by your ISP
172.16.254.50
ASA/
IPS Devices
10.1.1.1
These addresses will be provided to you by your Network administrators

Step 2:

You must put a management IP address on the ASA, so you can access it using the management application. Connect a console cable to the ASA and take the following steps. You can use any address recommended by your network administrator; in this example, we will use 172.16.254.50.

The task is to enter your license information into your ASA. Press the return key and enter the command **enable**, then press the “Enter” key when asked for a password. At the “#” prompt, enter the command activation key xxxxxxxxxxxxxxx (where the x’s represent your license key).

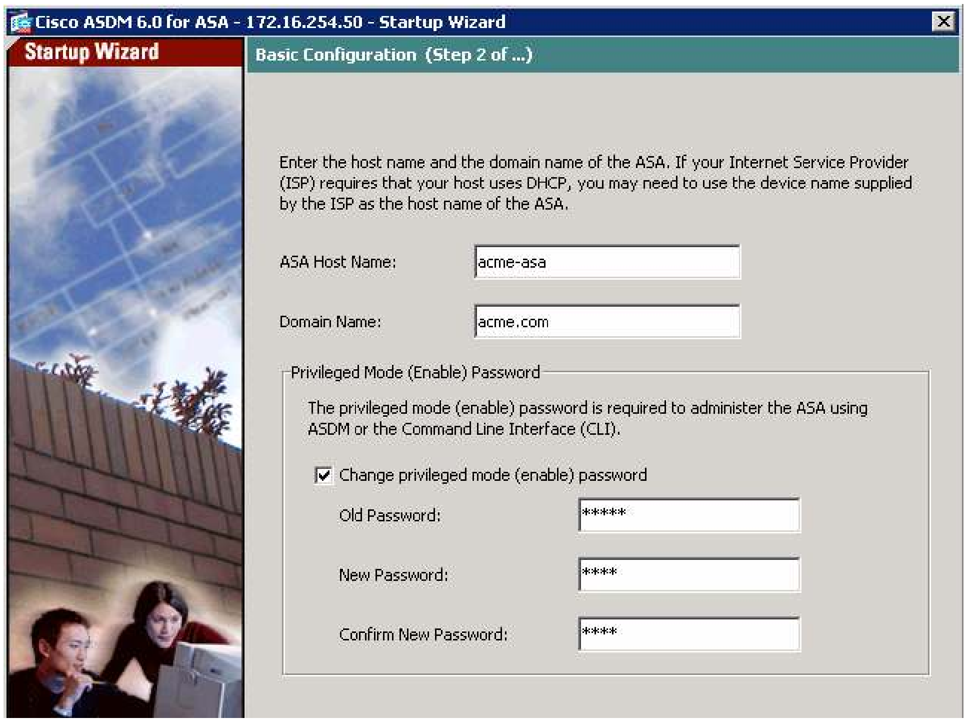
```
ciscoasa# conf t
ciscoasa(config)# interface Management0/0
ciscoasa(config-if)# nameif management
INFO: Security level for "management" set to 0 by default.
ciscoasa(config-if)# ip address 172.16.254.50 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config)# http server ena
ciscoasa(config)# http 0.0.0.0 0.0.0.0 management
ciscoasa(config)# asdm image disk0:/asdm-603.bin
ciscoasa(config)#
```

Step 3.

To access the ASA, use a PC on the management network and enter https://172.16.254.50. Click “Startup Wizard.” Select “Modify Existing Configuration” and click “Next.”

Enter a host name and a domain name. The host name can be anything alphanumeric; the domain name should be the company’s domain. In this case, **acme-asa** was used for the host name and **acme.com** for the domain name.

An “enable password” protects the privileged mode of your ASA, so you should enter a secret password that will need to be used to gain access to the device. Click “Next.”



Cisco ASDM 6.0 for ASA - 172.16.254.50 - Startup Wizard

Startup Wizard

Basic Configuration (Step 2 of ...)

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name: acme-asa

Domain Name: acme.com

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

☑ Change privileged mode (enable) password

Old Password: *****

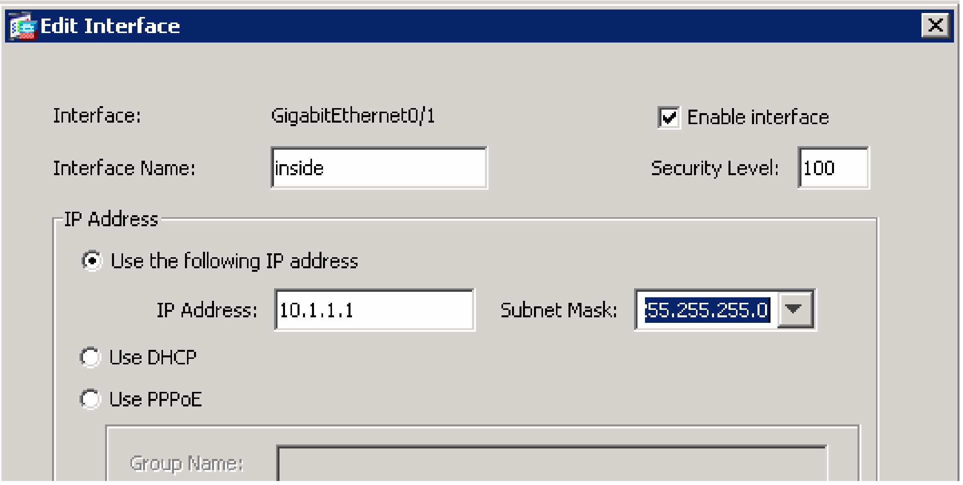
New Password: ****

Confirm New Password: ****

In the next panel you can enter auto-update information, which can fetch updates to your ASA software. This will be left blank for this installation.

The next panel configures your interface, which is connected to the Internet. Click “Enable Interface,” and enter **outside** for the interface name. Enter the IP address **20.1.1.1** with a subnet mask of **255.255.255.0**. Your outside interface will have a security level of 0, which means this interface is not trusted and no traffic will be allowed in unless the firewall is configured to allow traffic.

The next panel allows you to configure the inside interface that connects the company network to the Internet. Highlight “GigabitEthernet 0/1” and select “Edit.” In the resulting screen, check the “Enable interface” box and enter **inside** as the interface name. Click the “Use the following IP address” radio button and enter **10.1.1.1** as the address and **255.255.255.0** as the subnet mask. Enter a security level of 100, which indicates that the inside interface is the trusted segment of your firewall.



Edit Interface

Interface: GigabitEthernet0/1

☑ Enable interface

Interface Name: inside

Security Level: 100

IP Address

● Use the following IP address

IP Address: 10.1.1.1

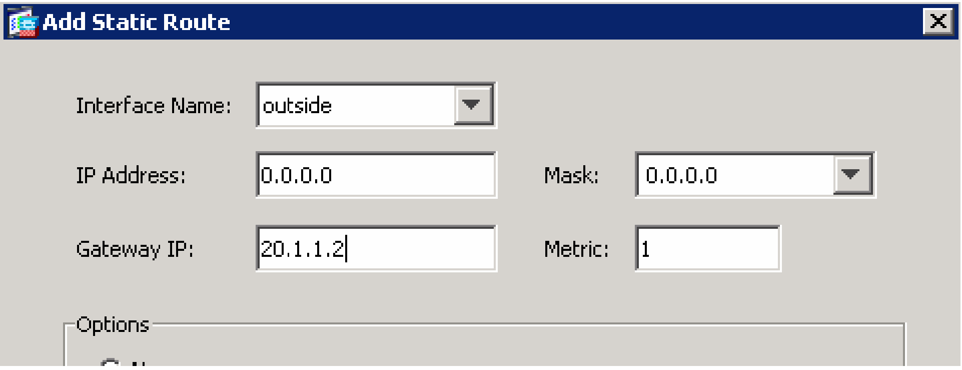
Subnet Mask: 255.255.255.0

○ Use DHCP

○ Use PPPoE

Group Name:

The next panel allows you to configure a metric called a default route. This simply tells your ASA the address of the device that is connecting you to the Internet. As you can see from the topology illustration, we are using **20.1.1.2** as the gateway address and a subnet mask of **255.255.255.0.** Enter an IP address of **0.0.0.0**, a mask of **0.0.0.0**, and a gateway IP address of **20.1.1.2.** This tells the ASA that it will route all traffic not destined for your company network to the Internet. Click “OK,” and then click “Next.”



Add Static Route

Interface Name: outside

IP Address: 0.0.0.0

Mask: 0.0.0.0

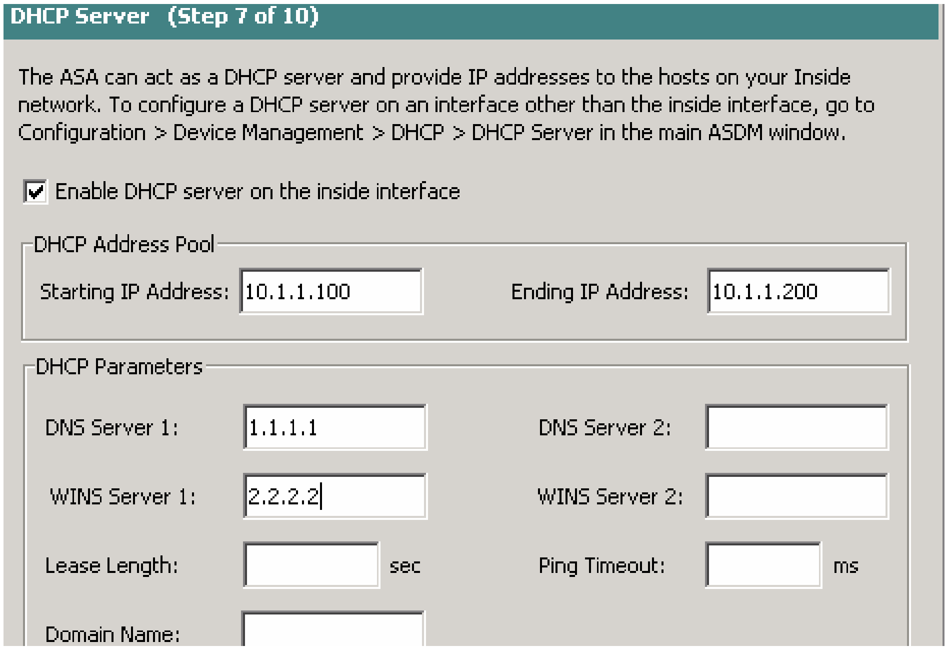
Gateway IP: 20.1.1.2

Metric: 1

Options

The next panel allows you to configure your ASA as a DHCP server. This will allow your ASA to dynamically hand out addresses to any PCs requesting an address from your company network. If the PCs on your network already have IP addresses, you can click “Next” on this panel. For this configuration, we will tell the ASA that it will automatically configure new PCs with an address range from 10.1.1.100 to 10.1.1.200. DNS and WINS addresses vary from location to location; for this exercise we will enter fake addresses.

Click the “Enable DHCP server on the inside interface” box. Enter **10.1.1.100** as the starting IP address, **10.1.1.200** as the ending IP address, **1.1.1.1** as DNS Server 1, and **2.2.2.2** as WINS Server 1. Click “Next.”



DHCP Server (Step 7 of 10)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your Inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

☑ Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 10.1.1.100   Ending IP Address: 10.1.1.200

DHCP Parameters

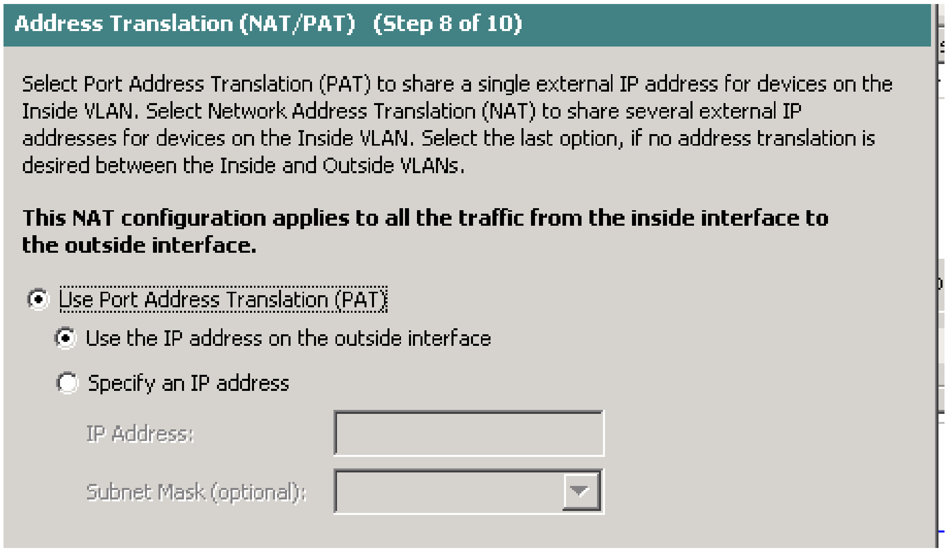
DNS Server 1: 1.1.1.1   DNS Server 2:

WINS Server 1: 2.2.2.2   WINS Server 2:

Lease Length: sec   Ping Timeout: ms

Domain Name:

The next panel lets you define how the Internet will view your IP addresses as unique routable addresses and port numbers. In this example, we are using the default, which tells the ASA to use the outside IP address for unique routable address mapping.



Address Translation (NAT/PAT) (Step 8 of 10)

Select Port Address Translation (PAT) to share a single external IP address for devices on the Inside VLAN. Select Network Address Translation (NAT) to share several external IP addresses for devices on the Inside VLAN. Select the last option, if no address translation is desired between the Inside and Outside VLANs.

This NAT configuration applies to all the traffic from the inside interface to the outside interface.

● Use Port Address Translation (PAT)

● Use the IP address on the outside interface

○ Specify an IP address

IP Address:

Subnet Mask (optional):

The next panel allows you to configure your ASA to use the management GUI. We already completed this step through the console port when we put a management IP address on this device. Click “Next.”

The next panel shows you the commands that will be put on your ASA. Click “Finish” and your ASA is now operational, allowing traffic to go from your company network to the Internet and back, but blocking potentially malicious traffic that is sourced from the Internet.

After you click “Next,” you will be prompted for the new password that you entered while running the wizard. After you enter that password, you will be reconnected to the graphical management application.

The ASA is now configured.

IV How to Configure the IPS

Now that the ASA has been configured, there are a few more steps to license and configure the IPS.

- Configure management addresses and information on the IPS.
- License the IPS and install current signature information.
- Configure the ASA to send data to the IPS to be evaluated for network threats.

From the ASA console, enter **session 1**. This will bring you to the IPS CLI. The default username and password combination is **cisco/cisco**. You will be prompted to change your password before you can continue.

After the password has been changed, you will be presented with a “#” prompt from the IPS. Enter the command **setup** to do the initial configuration of the IPS. Sample values entered in this configuration are **acme-ip** for the sensor name, and **172.16.254.50 1/24** and **172.16.254.1** for IP addressing. We apply an access list allowing management from any PCs on the management subnet by entering **0.0.0.0/0**. Following is a sample of the setup utility using the suggested configuration values.

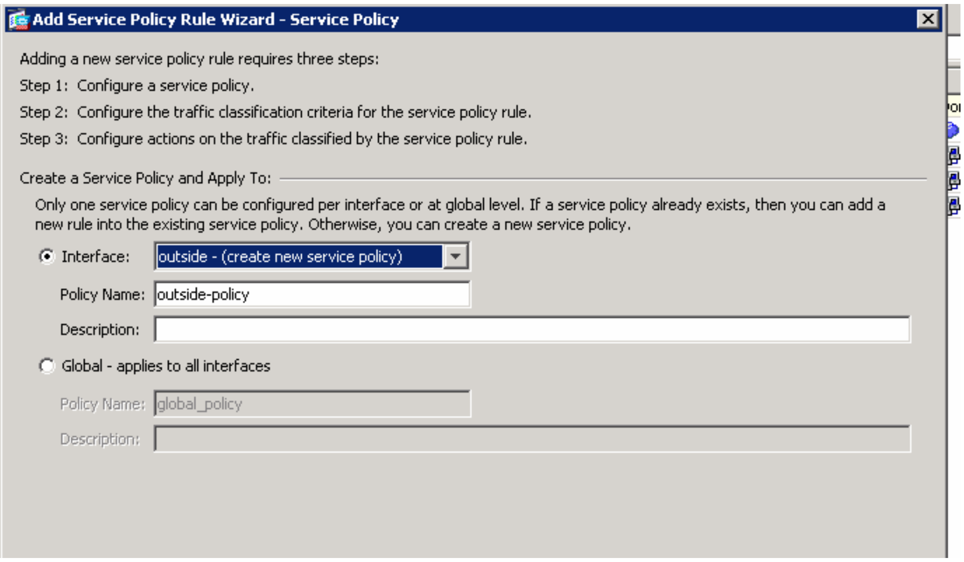
```
sensor# setup
 --- Basic Setup ---
 --- System Configuration Dialog ---
Current time: Mon Mar 10 23:10:37 2008
Enter host name[sensor]: acme-aip
Enter IP interface[192.168.1.2/24,192.168.1.1]:
172.16.254.51/24,172.16.254.1
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 0.0.0.0/0
Permit:
Modify system clock settings?[no]:
The following configuration was entered.
.
.
.
[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 2

--- Configuration Saved ---
```

Enabling the IPS

Now that the ASA and the IPS are configured and operational, you must configure the ASA to send traffic to the IPS for inspection. This is done by creating a service policy using Cisco Adaptive Security Device Manager (ASDM).

Using your Web browser, log into ASDM by entering the command **https://172.16.254.50/**. Browse to Panel Configuration > Firewall > Service Policy Rules and take the following steps.

Click the "+" icon to create a new policy. Select the "Interface" radio button, and "outside" from the drop-down menu. Click "Next."



Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

● Interface: outside - (create new service policy)

Policy Name: outside-policy

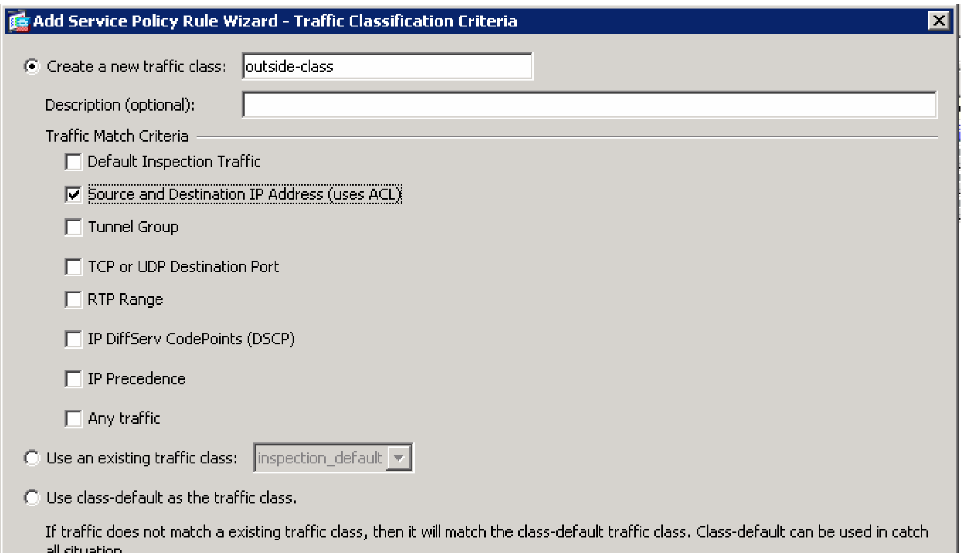
Description:

○ Global - applies to all interfaces

Policy Name: global_policy

Description:

Check the "Source and Destination IP Address" box and click "Next."



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: outside-class

Description (optional):

Traffic Match Criteria

□ Default Inspection Traffic

☑ Source and Destination IP Address (uses ACL)

□ Tunnel Group

□ TCP or UDP Destination Port

□ RTP Range

□ IP DiffServ CodePoints (DSCP)

□ IP Precedence

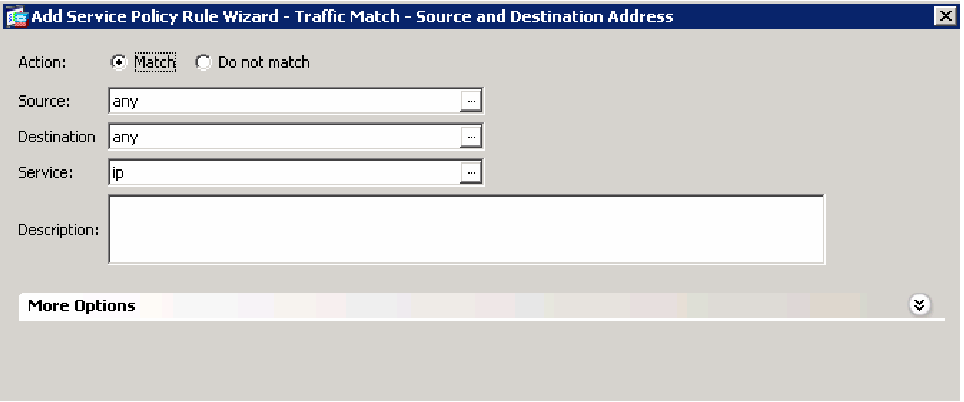
□ Any traffic

○ Use an existing traffic class: inspection_default

○ Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation

Configure the policy to manage any any ip, and click "Next."



Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ● Match ○ Do not match

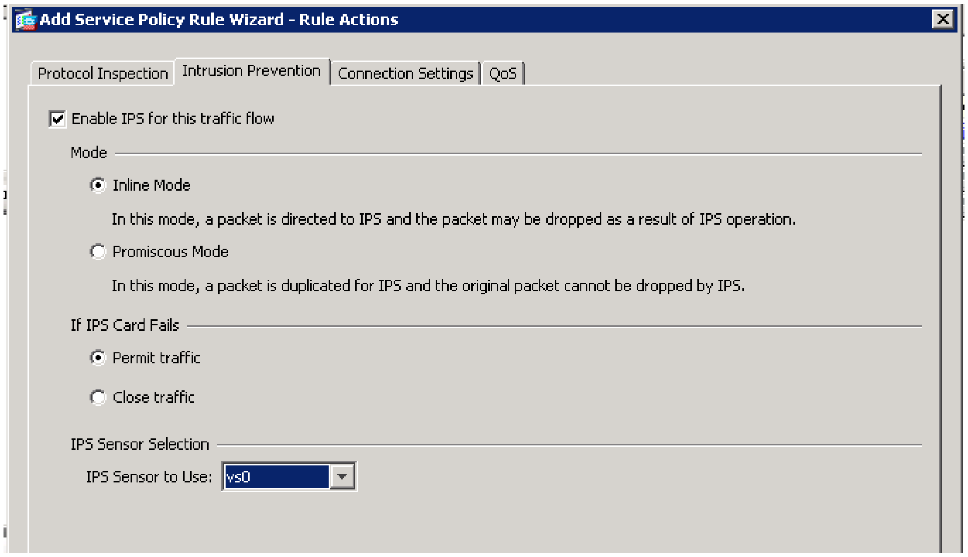
Source: any

Destination any

Service: ip

Description:

Click the tab labeled “Intrusion Prevention.” Check the “Enable IPS for this traffic flow” box. From the pull-down menu labeled “IPS Sensor to Use,” select “vs0.”



Add Service Policy Rule Wizard - Rule Actions

☑ Enable IPS for this traffic flow

Mode

● Inline Mode

In this mode, a packet is directed to IPS and the packet may be dropped as a result of IPS operation.

○ Promiscous Mode

In this mode, a packet is duplicated for IPS and the original packet cannot be dropped by IPS.

If IPS Card Fails

● Permit traffic

○ Close traffic

IPS Sensor Selection

IPS Sensor to Use: vs0

Click “Finish,” then click “Apply” to enable the new policy.

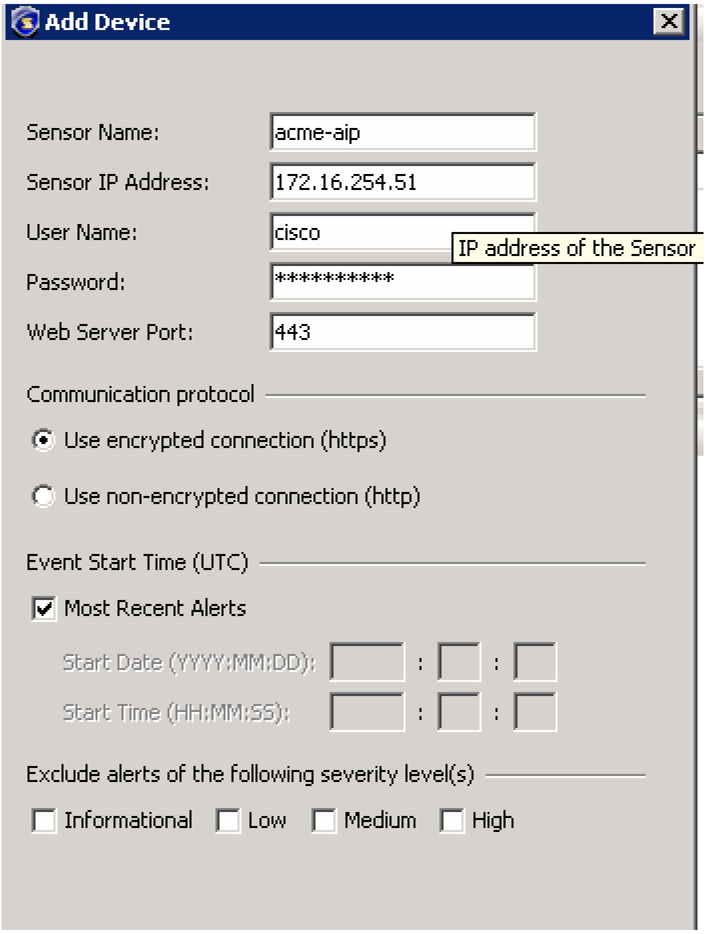
V How to License, Configure, and Monitor Your Cisco ASA 5500 Series IPS Solution Using Cisco IPS Manager Express

The first step is to install Cisco IPS Manager Express on the workstation from which you plan to manage your Cisco ASA 5500 Series IPS Solution.

Note: This workstation must be in the same management subnet as the IPS, so it should have an IP address starting with 172.16.254.X. Using workstations in other subnets is beyond the scope of this document.

To download Cisco IPS Manager Express, go to http://www.cisco.com/go/ips and follow the links to the download page.

Click the IPS Manager Express installer. An icon labeled “Cisco IME” will be displayed on your desktop. Click that icon to launch Cisco IPS Manager Express. From the Home > Devices > Device List panel, click the icon to add a new IPS. Use the values from the previous section to fill in the device panel.



Add Device

Sensor Name: acme-aip

Sensor IP Address: 172.16.254.51

User Name: cisco

Password: **********

Web Server Port: 443

Communication protocol

● Use encrypted connection (https)

○ Use non-encrypted connection (http)

Event Start Time (UTC)

☑ Most Recent Alerts

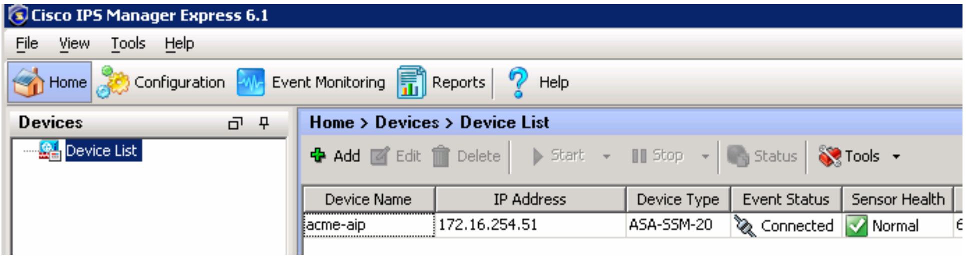
Start Date (YYYY:MM:DD): __ : __ : __

Start Time (HH:MM:SS): __ : __ : __

Exclude alerts of the following severity level(s)

□ Informational □ Low □ Medium □ High

You will be presented with a dialog box confirming the trusted certificate from the IPS. Click "Accept" to continue. You will see the device displayed in the IPS Manager Express device list.



Home > Devices > Device List

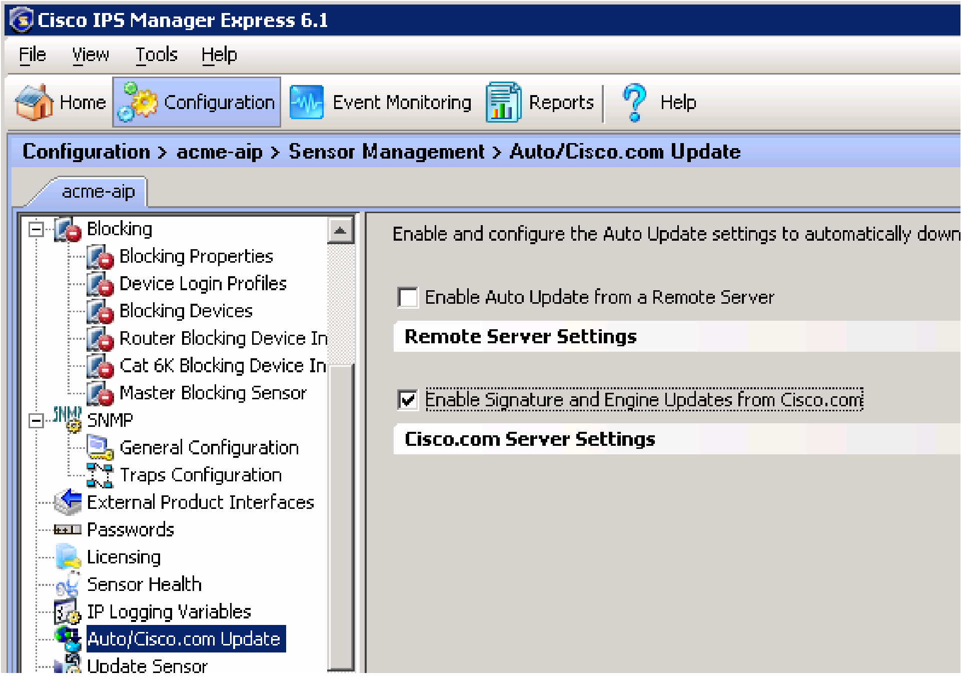
Device Name	IP Address	Device Type	Event Status	Sensor Health
acme-aip	172.16.254.51	ASA-SSM-20	Connected	✓ Normal

The last task to be completed is to use IPS Manager Express to license your sensor. Replace your IPS license on the desktop of the management workstation. From the Configuration > acme-aip > Sensor Management > Licensing panel, select "Update from license file" and browse to the license located on the desktop of the management workstation. Click "Update license." When the update is completed, you must install the current IPS signature file from Cisco.com.

Again, browse to http://www.cisco.com/go/ips and follow the download links. Click on the "Cisco Intrusion Detection System" link. Click on the "Latest Security Upgrades" link. Click on the most current signature file and download the file to the desktop of your management workstation.

Browse to the Cisco IPS Manager Express panel labeled Configuration > acme-aip > Sensor Management > Update Sensor. Click the button next to "Update is located on this client," and browse to the signature file that you just downloaded.

To ensure that all new updates are automatically installed on your IPS device, browse to the IPS Manager Express panel labeled Configuration > acme-aip > Sensor Management > Auto/Cisco.com Update and check the “Enable Signature and Engine Updates from Cisco.com” box.



Configuration > acme-aip > Sensor Management > Auto/Cisco.com Update

Enable and configure the Auto Update settings to automatically down

☐ Enable Auto Update from a Remote Server

Remote Server Settings

☑ Enable Signature and Engine Updates from Cisco.com

Cisco.com Server Settings

Your ASA 5500 Series IPS Solution is now in place, providing firewall and IPS security for your network. If you need assistance with any of the steps in this document, please contact the Cisco Technical Assistance Center.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-464689-00 04/08