INGRAM MICRO

Cisco ASA 5500 LAB Guide

Ingram Micro

4/1/2009

The following LAB Guide will provide you with the basic steps involved in performing some fundamental configurations on a Cisco ASA 5500 series security appliance.

Table of Contents

Initial Configuration Command Line Dialogue	Page 03
Restoring the ASA to Factory Default Configuration	Page 07
Exploring ASDM	Page 09
Initial ASA Configuration	Page 11
Configuring the 8 Port Switch	Page 22
Configuring NAT	Page 24
Configuring the Firewall	Page 30
Web Filtering	Page 35
Configuring Site to Site VPN	Page 40
Remote Access VPN	Page 46
Easy VPN Remote	Page 54

Initial Configuration Command Line Dialogue

When the ASA does not have a preexisting configuration, you will have the option to set up an initial configuration by following a set of interactive commands. Start the ASA, and when it is finished booting you will see the initial configuration dialogue script.

Select yes by hitting enter to configure the ASA via interactive prompts.

```
COM4 - PuTTY

  If you require further assistance please contact us by
  sending email to export@cisco.com.
  ******************************** Warning ********************************

Copyright (c) 1996-2006 by Cisco Systems, Inc.

                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

Configuration has non-ASCII characters and will be ignored.

Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Pre-configure Firewall now through interactive prompts [yes]? y
```

There are two options when configuring the firewall mode: routed and transparent. Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire" and is not seen as a router hop to connected devices. The security appliance connects the same network on its inside and outside interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network; IP readdressing is unnecessary. In routed mode, the security appliance can perform NAT between connected networks, and can use OSPF or RIP.

Select “transparent” as the firewall mode for this portion of the lab.

```
COM4 - PuTTY
  sending email to export@cisco.com.
  ******************************** Warning ********************************

Copyright (c) 1996-2006 by Cisco Systems, Inc.

                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

Configuration has non-ASCII characters and will be ignored.

Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Pre-configure Firewall now through interactive prompts [yes]? y
Firewall Mode [Routed]: transparent
```

For security reasons and for remote access to the ASA, you will need to configure a password for the appliance. This password will be the Privileged Exec level password for the appliance.

Configure the password and allow password recovery.

```
COM4 - PuTTY
  ****************************** Warning ******************************

Copyright (c) 1996-2006 by Cisco Systems, Inc.

                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

Configuration has non-ASCII characters and will be ignored.

Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Pre-configure Firewall now through interactive prompts [yes]? y
Firewall Mode [Routed]: transparent
Enable password [<use current password>]: cisco
Allow password recovery [yes]? y
```

Configure the time and date settings for the appliance. The correct time is an important factor for Syslog time stamps, certificate time stamps, logging of audit and messaging data, etc.

```
COM4 - PuTTY
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

Configuration has non-ASCII characters and will be ignored.

Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Pre-configure Firewall now through interactive prompts [yes]? y
Firewall Mode [Routed]: transparent
Enable password [<use current password>]: cisco
Allow password recovery [yes]? y
Clock (UTC):
  Year [2008]:
  Month [Sep]:
  Day [10]:
  Time [10:48:01]:
```

Configure the IP address and network mask of the management interface. Give the ASA a hostname and domain. Configure the IP address of the management station. For this lab, we are configuring the following:

Management IP Address: *10.10.10.1*
Management Network Mask: *255.255.255.0*
Host Name: *ASALab*
Domain: *Pod1*
IP Address of Host Running Device Manager: *10.10.10.100**

* It is important to ensure that you statically assign the IP address of your device management station to reflect this setting.

```
COM4 - PuTTY
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

Configuration has non-ASCII characters and will be ignored.

Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Pre-configure Firewall now through interactive prompts [yes]? y
Firewall Mode [Routed]: transparent
Enable password [<use current password>]: cisco
Allow password recovery [yes]? y
Clock (UTC):
  Year [2008]:
  Month [Sep]:
  Day [10]:
  Time [10:48:01]:
Management IP address: 10.10.10.1
Management network mask: 255.255.255.0
Host name: ASALab
Domain name: Pod1
IP address of host running Device Manager: 10.10.10.100
```

Verify and write to flash.

```
COM4 - PuTTY
Allow password recovery [yes]? y
Clock (UTC):
  Year [2008]:
  Month [Sep]:
  Day [10]:
  Time [10:48:01]:
Management IP address: 10.10.10.1
Management network mask: 255.255.255.0
Host name: ASALab
Domain name: Pod1
IP address of host running Device Manager: 10.10.10.100

The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 10:48:01 Oct 19 2008
Firewall Mode: Transparent
Management IP address: 10.10.10.1
Management network mask: 255.255.255.0
Host name: ASALab
Domain name: Pod1
IP address of host running Device Manager: 10.10.10.100

Use this configuration and write to flash? y
```

You will notice that the security level of the inside interface is set by default. This is actually setting the security level of VLAN 1, and not a specific interface.

You will also notice that the HTTP server has not been enabled on the appliance. In order to connect to the ASA via ASDM, the HTTP server will need to be enabled.

```
COM4 - PuTTY
The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 10:48:01 Sep 10 2008
Firewall Mode: Transparent
Management IP address: 10.10.10.1
Management network mask: 255.255.255.0
Host name: ASALab
Domain name: Pod1
IP address of host running Device Manager: 10.10.10.100

Use this configuration and write to flash? y
INFO: Security level for "inside" set to 100 by default.
INFO: Security level for "inside" set to 100 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: 7853c9a2 b1f1c54f b2ee0b9b 92a1fb2a

1779 bytes copied in 1.390 secs (1779 bytes/sec)



Type help or '?' for a list of available commands.
ASALab>
```

Enter Privileged Exec mode and enable the HTTP server by entering the *http server enable* command.

```
COM4 - PuTTY

Use this configuration and write to flash? y
INFO: Security level for "inside" set to 100 by default.
INFO: Security level for "inside" set to 100 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: 7853c9a2 b1f1c54f b2ee0b9b 92a1fb2a

1779 bytes copied in 1.390 secs (1779 bytes/sec)



Type help or '?' for a list of available commands.
ASALab> ena
Password: *****
ASALab# config t
ASALab(config)# http server enable
ASALab(config)#
```

From here, you can continue to configure the ASA 5505 from the command line. It is not necessary to go through the initial configuration dialogue every time you set up an ASA. If you like, you can opt out of the script by entering "*no*" when you're asked if you want to configure the firewall through interactive prompts.

Because we want to continue the lab by configuring the ASA from ASDM, we will want to restore the factory default configuration.

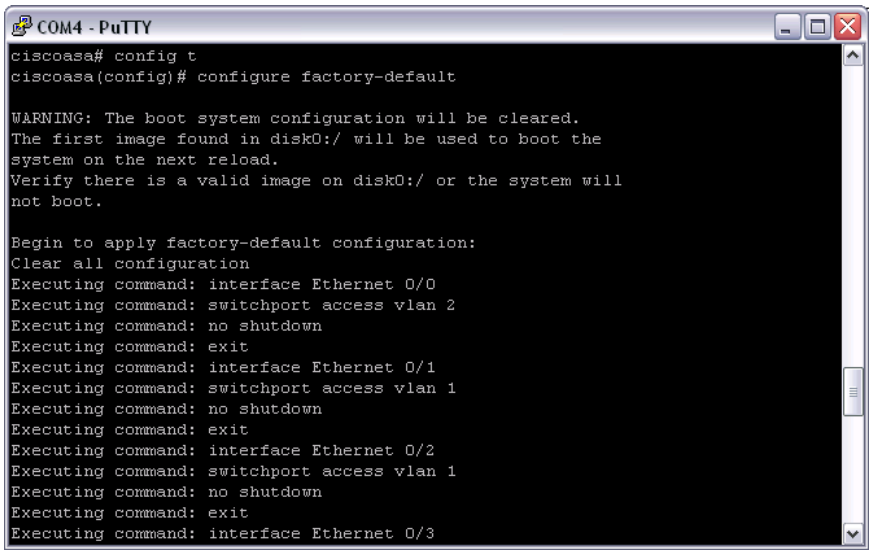
Restoring the ASA to Factory Default Configuration

The ASA 5505 is shipped with a factory default configuration, which consists of the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. The VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- A default route derived from DHCP.
- All inside IP addresses are translated when accessing the outside using interface PAT.
- By default, inside users can access the outside with an access list, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the security appliance, so a PC connecting to the VLAN 1 interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

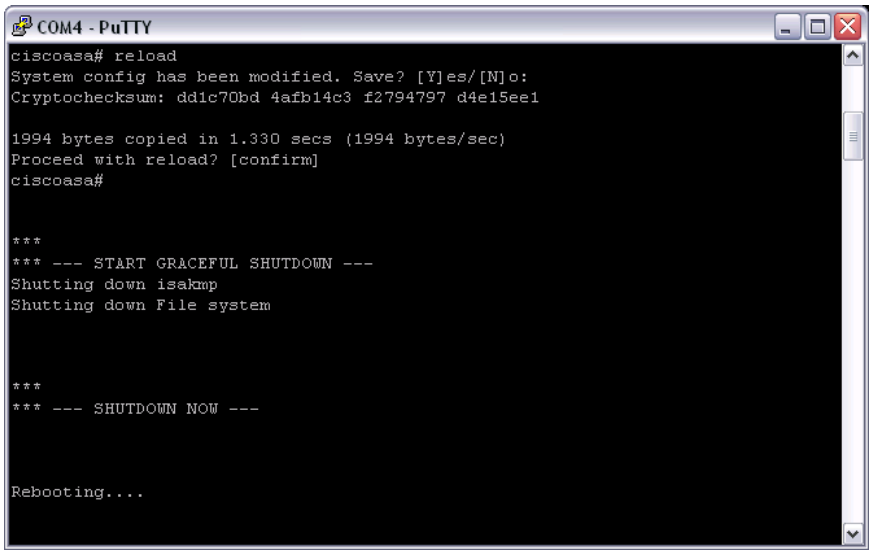
If you need to revert back to these changes after a configuration, you can do so by entering the *configure factory-default* command.

Reset the ASA to factory default by entering Configuration mode and entering the *configure factory-default* command.



You can then save the configuration by entering the *write memory* command, or by entering the *reload* command and selecting the *yes* option to save the changed configuration.

Save the configuration and reload the ASA.



Now that the default configuration has been restored to the ASA, we will begin configuration from ASDM.

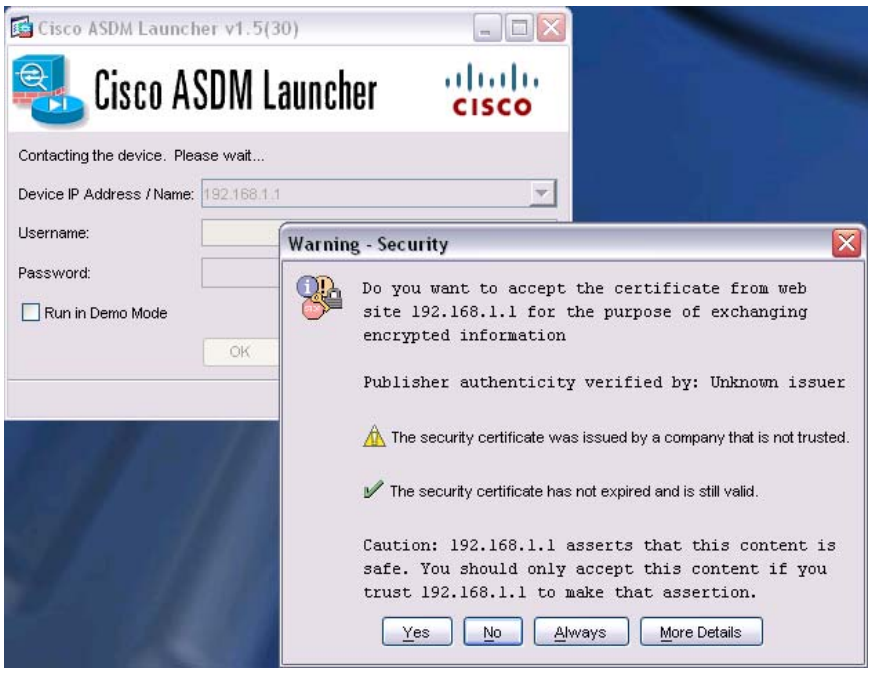
Exploring ASDM

Plug your laptop into one of the E0/1 - E0/7 switch ports on the ASA, and set your network adapter to obtain an IP address via DHCP. If you are running wireless, you may need to turn off your wireless adapter to avoid any routing table conflicts on your laptop.

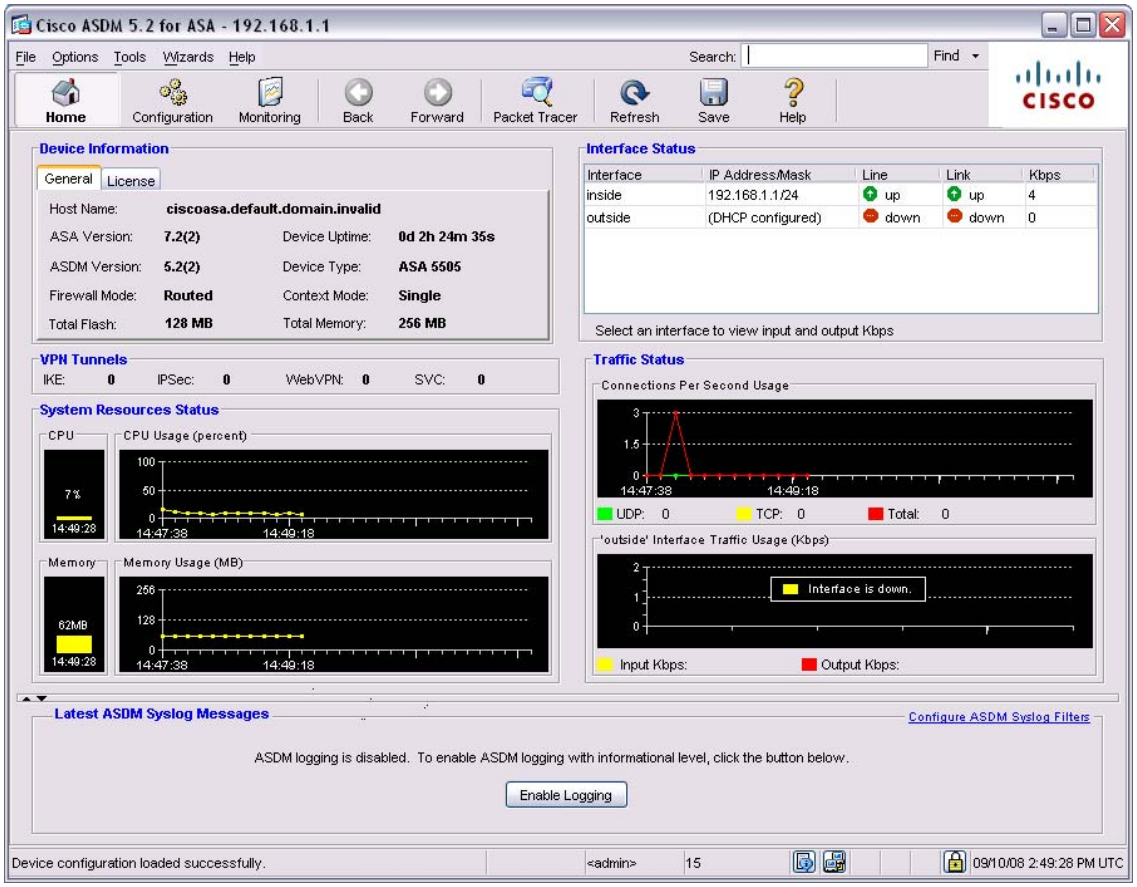
Launch the Cisco Adaptive Security Device Manager from Start > Programs.

When ASDM loads, connect to the default IP address of the appliance (192.168.1.1). By default, the username is blank and the password is *cisco*.

Accept the security certificate by selecting *Always* in the Security Warning dialogue box.



When ASDM loads, you will be brought to the Home screen of the application.



Along the top, you will see the following buttons:

- **Home** – brings you to the main ASDM screen. From here you will have a general overview of the device including device information, license information, interface status, VPN tunnel information, system resource status, traffic status, and recent Syslog messages.
- **Configuration** – brings you to the configuration screen of ASDM. From here you will have the option to configure interfaces, security policies, NAT, VPN, Cisco Secure Desktop, routing, and global options. You will also have access to various configuration wizards.
- **Monitoring** – Brings you to the device monitoring screen. From here you can monitor interfaces, routing, VPN, security properties, and access logs.
- **Back** – brings you back one navigation screen.
- **Forward** – brings you forward one navigation screen.
- **Packet Tracer** – Allows you to specify interfaces and trace packets as they traverse the device.
- **Refresh** – Loads the current configuration from the device.
- **Save** – Saves the current configuration to the device.
- **Help** – Gives you access to a TAC database of configuration information.

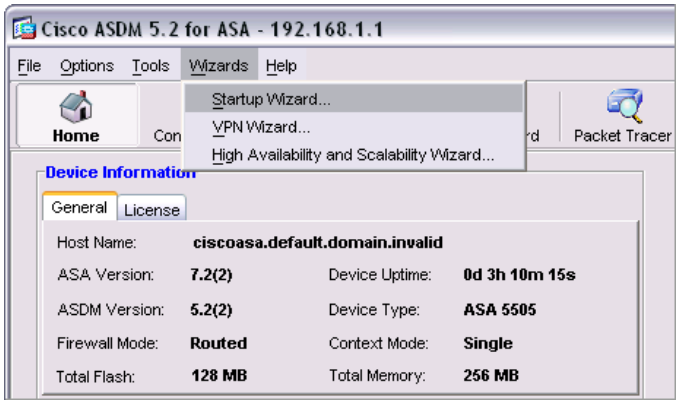
At this time, spend time navigating ASDM to become familiar with the screens and available options.

Initial ASA Configuration

Now that we are familiar with ASDM, we'll spend some time using the application to configure the appliance.

Because the configuration is presently set to factory default, there are some basic configuration changes that need to be made. We will set up the basic configuration from the Startup Wizard.

From ASDM, click Wizards > Startup Wizard



Step 1 will ask you if you would like to modify the existing configuration, or if you would like to reset the appliance to factory default.

Since we've already set the box to factory default, we will proceed by selecting the *Modify Existing Configuration* option. When you are done, click *Next*.

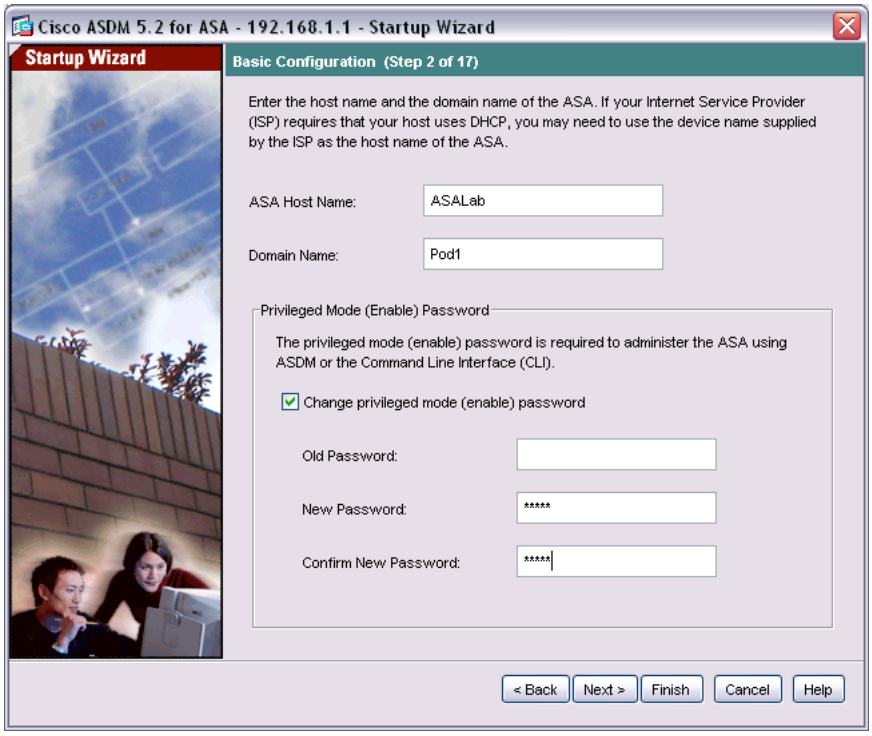
Step 2 will ask us to provide a hostname, domain name, and Privileged Exec level passwords for the appliance.

Enter the following information:
Hostname – *ASALab*
Domain – *Pod1*

Since the default password is *cisco*, we will not be changing it in this lab.

The hostname is the name used to identify the appliance. It will appear in the command line prompt.
The domain name will be appended to all unqualified domain names.

When you've entered the information, click *Next*.



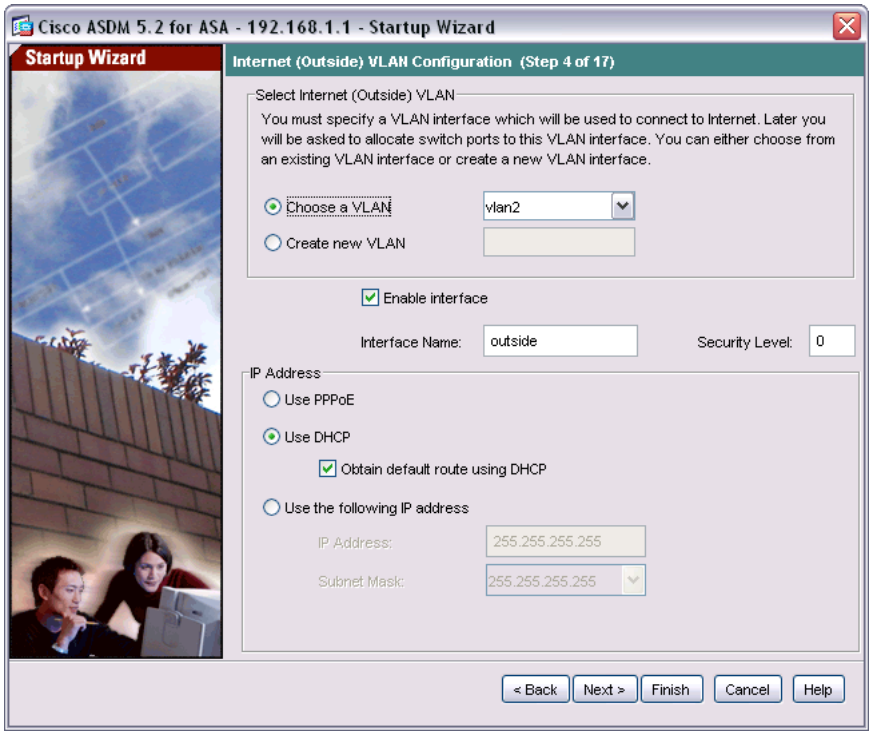
Step 3 will ask you if you would like to configure an Auto Update Server.

The Auto Update specification allows the Auto Update server to either push configuration information to the security appliance, or to pull configuration information by causing the security appliance to periodically poll the Auto Update server. The Auto Update server can also send a command to the security appliance to send an immediate polling request at any time.

For the purpose of this lab, we will not be configuring an Auto Update Server. Click *Next* to continue.

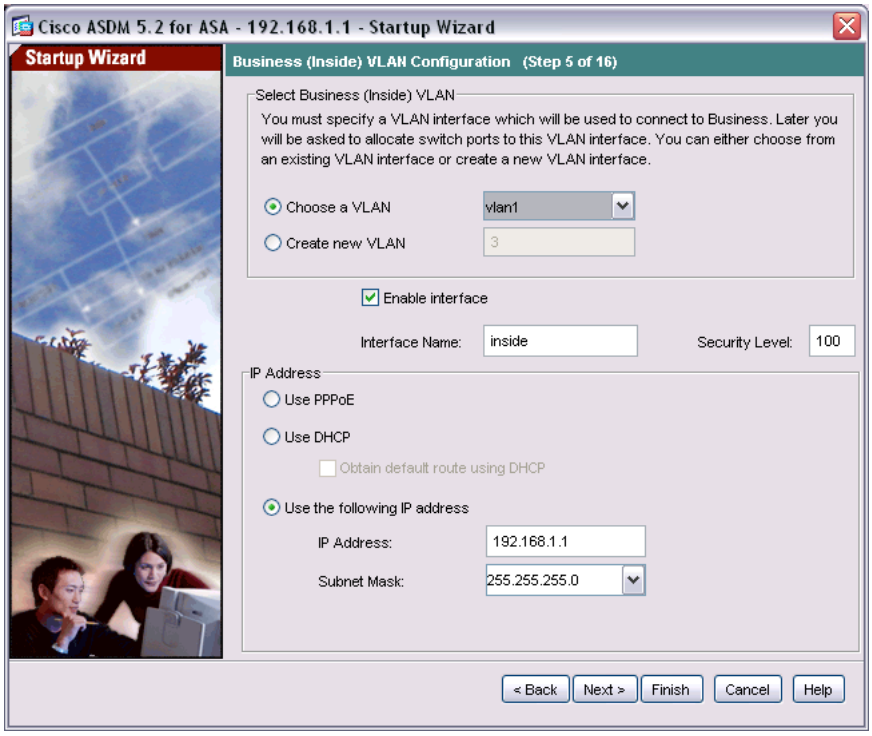
Step 4 will ask you to configure the Outside interface.

The Outside interface is the untrusted interface that connects to the Internet, and is identified by the VLAN a particular interface belongs to. Untrusted interfaces are assigned a security level of 0. By default, the ASA 5505's configuration specifies that VLAN 2 is an untrusted VLAN with a security level of 0, and applies these settings to E0/0. Verify the settings are correct and that the Outside interface is configured to accept an IP address via DHCP, and then click next.



Step 5 will ask you to configure the Inside interface.

Inside interfaces are the trusted interfaces belonging to your network, and are also identified by the VLAN a particular interface belongs to. Trusted interfaces are assigned a security level of 100. By default, the ASA 5505's configuration specifies that VLAN 1 is a trusted VLAN with a security level of 100, and applies these settings to interfaces E0/1 – E0/7. Verify the settings are correct and that the Inside interface is configured to have an IP address of 192.168.1.1 with a mask of 255.255.255.0.



NOTE: I've found IP address configuration in the startup wizard to be a bit finicky. If you change the IP address of the Inside VLAN, you will lose connectivity to ASDM. What you will need to do is statically assign an IP address to your network adapter, and then go in to CLI and change the address of the HTTP server using this command:

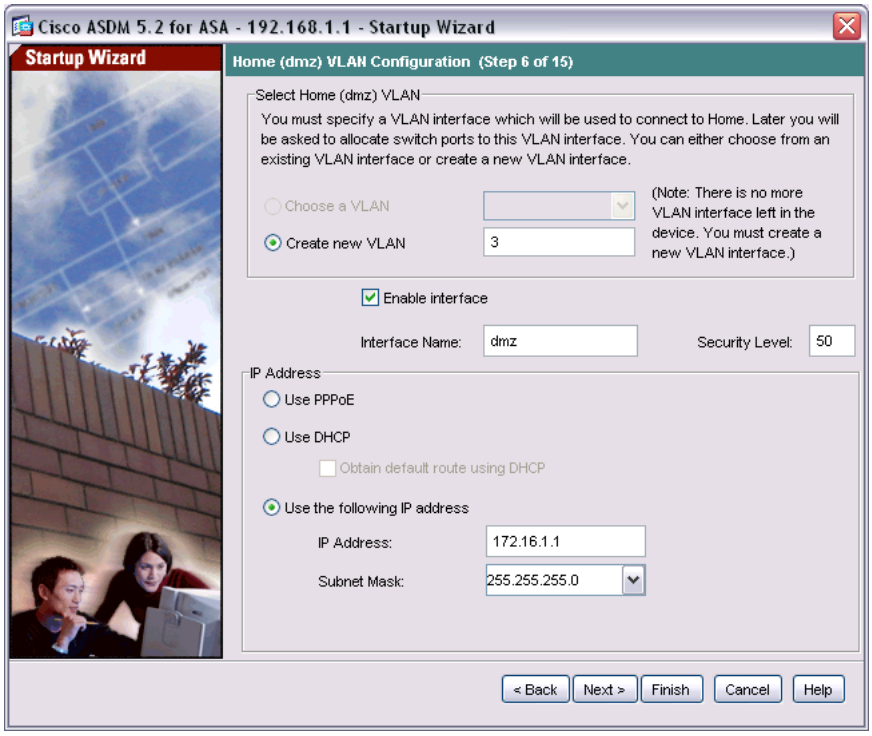
ASA(config)#http [IP address] [subnet mask] inside

Step 6 will ask you to configure a DMZ.

Since both default VLANs have been assigned to the Outside and Inside interfaces, we will need to create a new VLAN. Accept the default VLAN of *3*, and then *enable* the interface by clicking the radio button. Accept the default security level of 50. Security levels will be discussed in the next few steps.

Assign the DMZ an IP address of *172.16.1.1* with a mask of *255.255.255.0*.

Verify your settings and click *Next*.

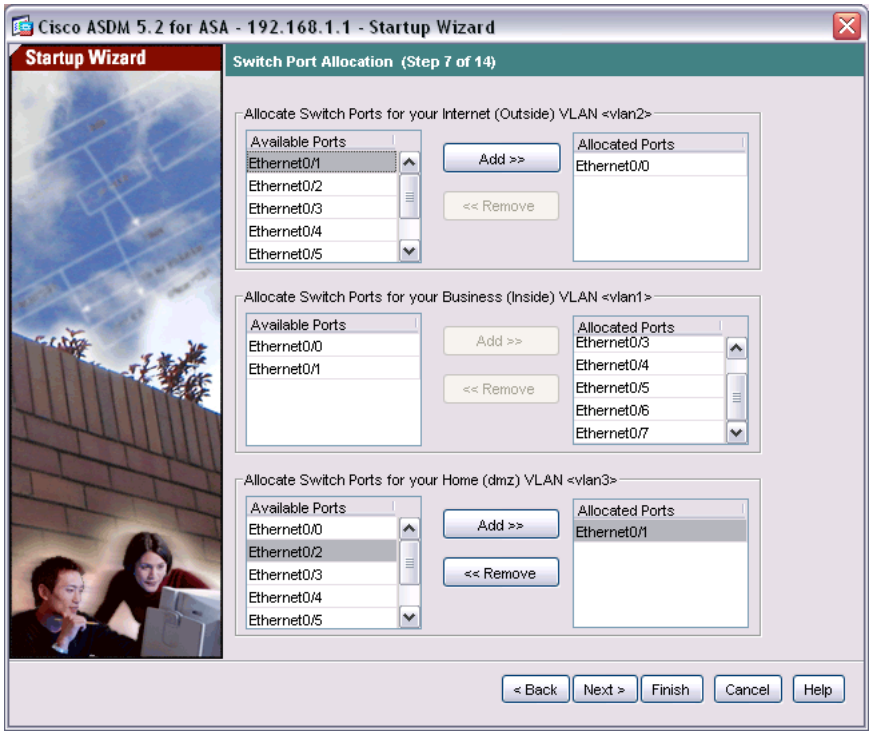


Step 7 will ask you to configure additional switch ports.

On this screen, you will see which switch ports belong to which VLANs. Here you can add or remove interfaces under each configured VLAN.

You should notice that VLAN 3, which is our newly created DMZ VLAN, does not have any interfaces assigned to it. Select interface *E0/1*, and assign it to *VLAN 3* (the DMZ VLAN).

Click *Next* when you are done.



Step 8 will ask you to set up the General Interface Configuration.

In the ASA 5505's default configuration, the DMZ is seen as a home network, with the Outside interface being the Internet connection, and the Inside interface a business network. By design, an interface with a high security level can communicate down to an interface with a lower security level, but not vice versa.

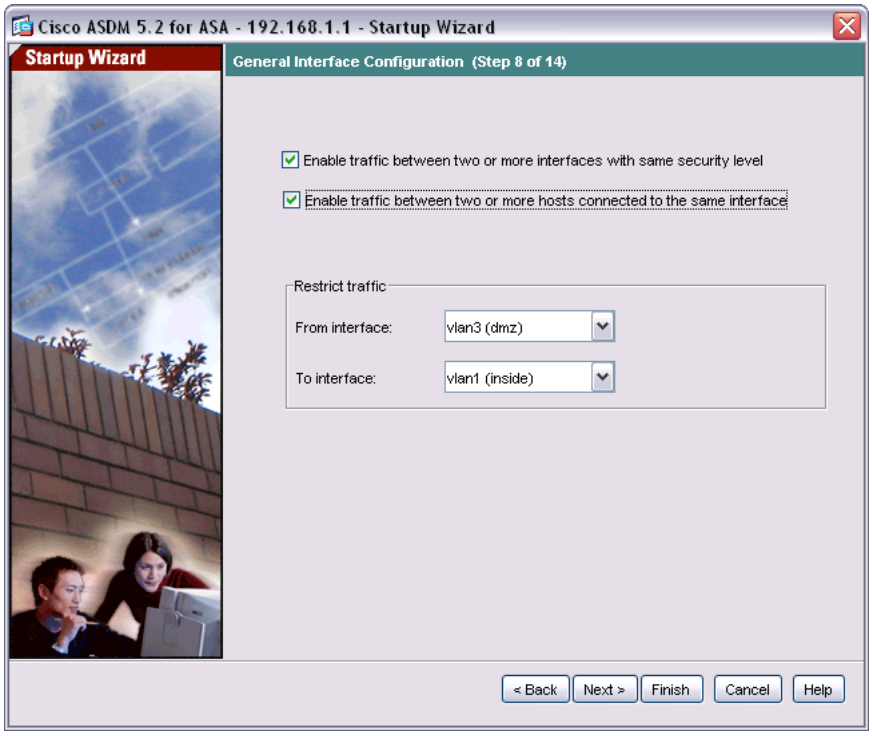
The default security level for the DMZ is 50. This means that the Inside interface (security level of 100) can initiate communication to the DMZ and the Outside interface (security level of 0), the DMZ can initiate communication to the Outside interface but not the Inside interface, and the Outside interface cannot initiate communication to either the Inside interface or the DMZ.

On the General Interface Configuration you can control how interfaces with different security level interact.

Check the options to *enable traffic between 2 or more interfaces with the same security level*, and to *enable traffic between 2 or more hosts connected to the same interface*.

Restricted traffic is not an optional configuration. If you only have a restricted license, you must restrict from one interface to any of the other interfaces. Typically, this is the traffic from the DMZ to the inside interface, but any pair can be chosen. The Restrict Traffic area fields are hidden if you have a full license or if the device is in transparent mode. Restrict traffic from *VLAN 3* to *VLAN 1*.

When you are complete, click *Next*.

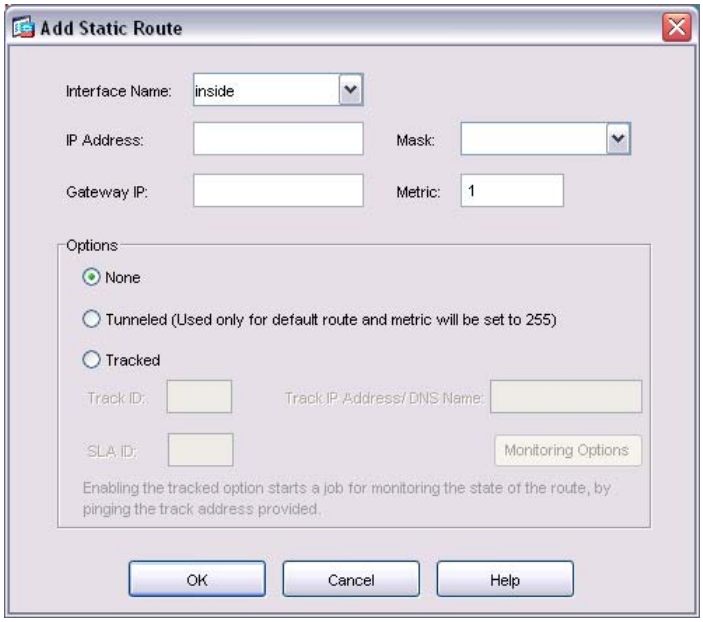


Step 9 will ask you to configure static routes.

The static routes configured here will use the Outside interface to send all traffic to the next hop. If you want to configure a default route, you can set the IP address and network mask to 0.0.0.0.

For the lab, we will be configuring a default route.

Click the *Add* button.



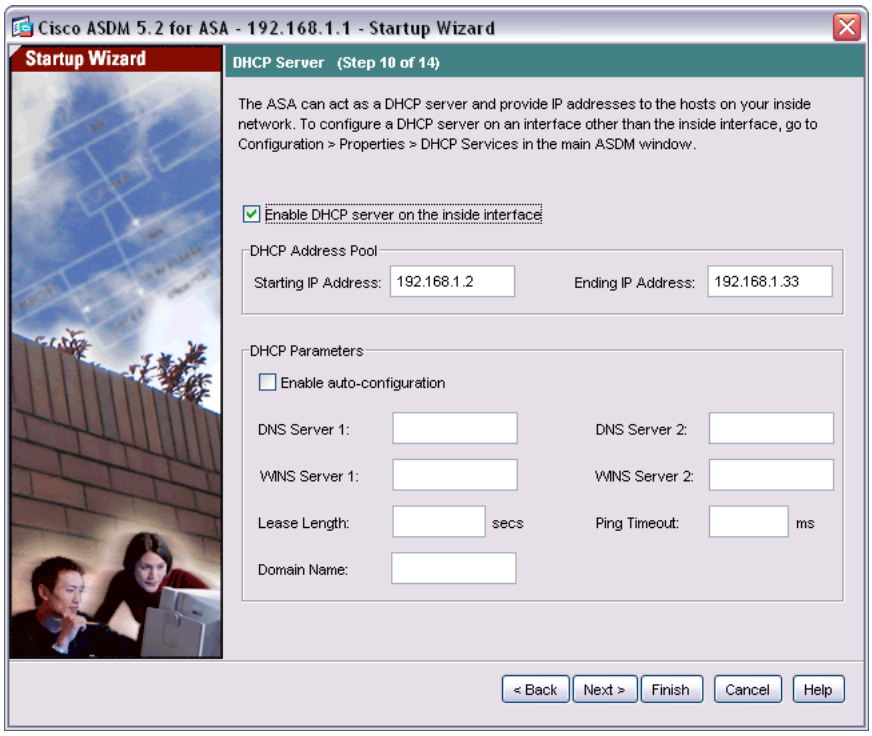
Enter the following configuration options:

Interface Name: *Inside*
IP Address: *0.0.0.0*
Mask: *0.0.0.0*
Gateway IP: *[variable depending on your gateway. I will be using 192.168.10.1]*
Metric: *1*
Options: *None*

Click on *OK*, and then click *Next*.

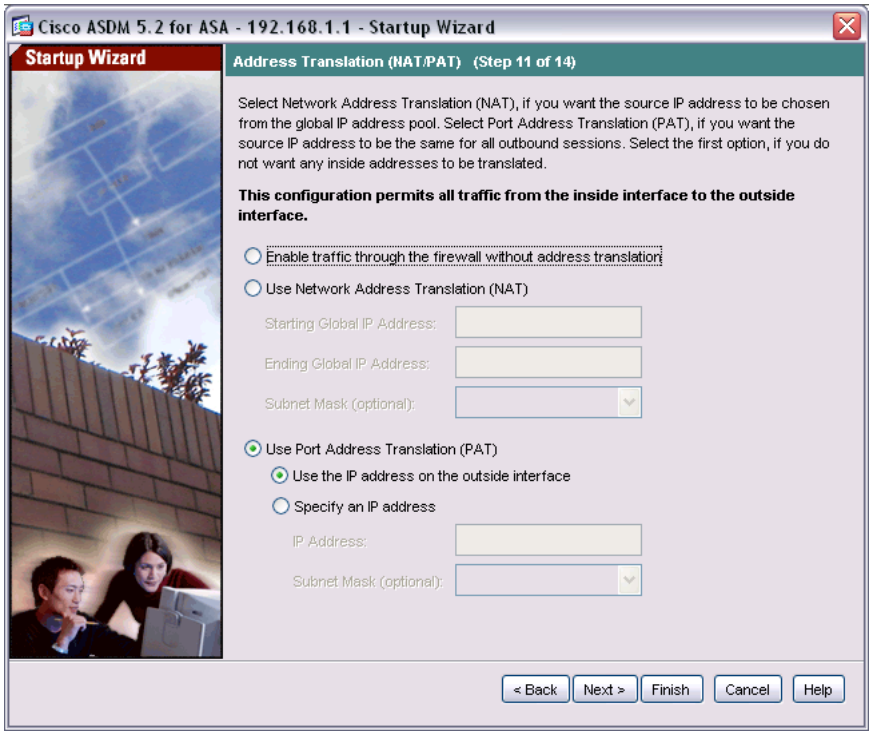
Step 10 will ask you to configure a DHCP server.

In this step, we will configure the DHCP settings of the ASA server. Since we currently have no reason to change the settings, select the default values and click *Next*.



Step 11 will ask you to configure NAT/PAT.

At this time we will not be setting up Network Address Translation, but we will be configuring Port Address Translation. Verify the options to configure PAT are selected, and then click *Next*.



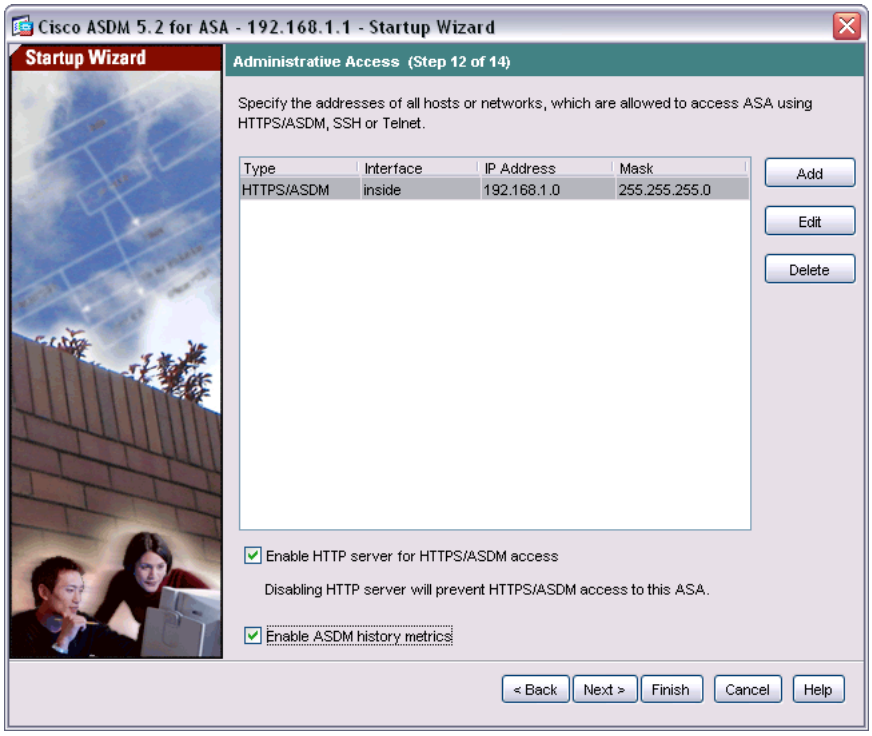
Step 12 will ask you to configure administrative access.

Here you can configure an IP address range or a specific host for ASDM administrative permissions to the appliance.

If you want to maintain the appliance via ASDM, you will need to make sure the *Enable HTTP server for HTTPS/ASDM access* box is checked.

Check the box to enable *ASDM History Metrics*. History metrics will keep a history of various statistics, which can be displayed by ASDM on any Graph/Table. If you do not enable history metrics, you can only monitor statistics in real time. Enabling history metrics lets you view statistics graphs from the last 10 minutes, 60 minutes, 12 hours, and 5 days.

Accept the default IP range of *192.168.1.0* with a mask of *255.255.255.0*, and click *Next*.



Step 13 will ask you to Configure Easy VPN.

We will not be configuring Easy VPN at this time, so click *Next*.

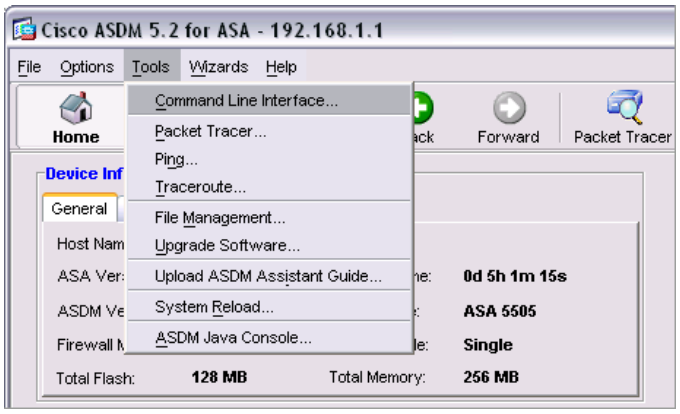
Step 14 will ask you to verify the configuration, and then send your changes to the ASA.

Click *Finish* when you have completed the verification.

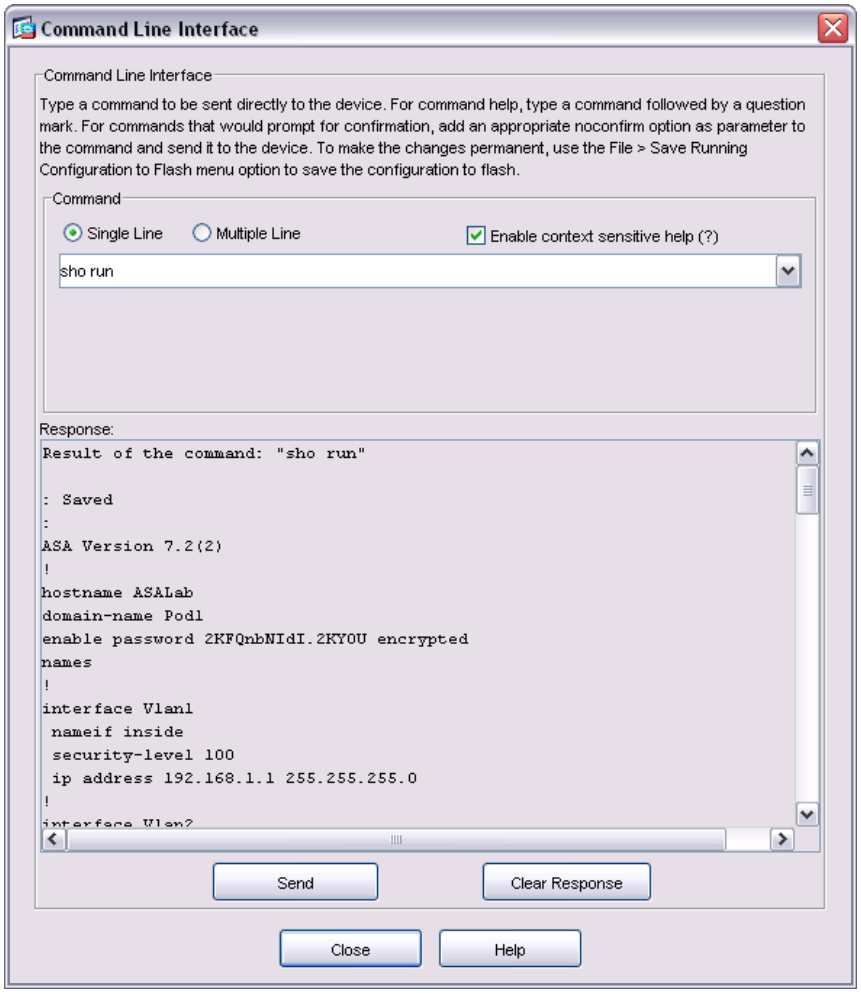
When you are prompted for a username and password, use the following credentials:
Username: *[blank]*
Password: *cisco*

These parameters were configured during the Startup Wizard.

To see the changes you've made, click Tools > Command Line Interface



In the dialogue box, enter the command *sho run*. This will display the running configuration on the box.



You have now completed the Startup Wizard.

Configuring The 8 Port Switch

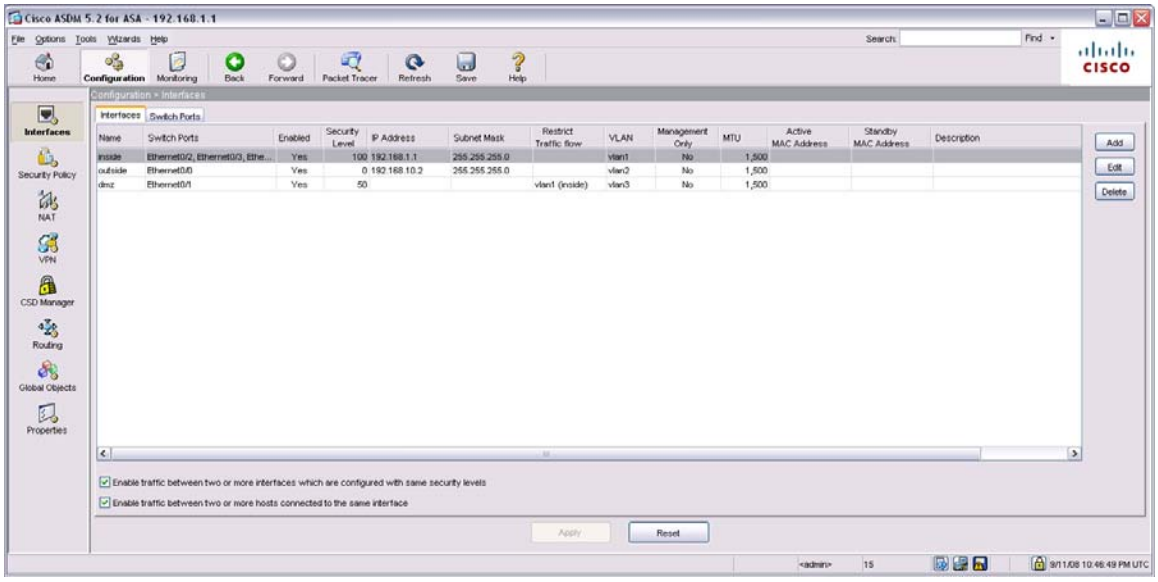
The ASA 5505 supports a built in switch. There are two different kinds of interfaces you will need to configure:

1. **Physical interfaces** – The 5505 has eight switch ports, two of which are PoE ports. This switching is done in hardware at layer 2.

2. **Logical VLAN interfaces** – The 5505 supports a variable number of VLANs depending on your license and the firewall mode. If you're operating in transparent mode, you have a maximum of 2 allowable VLANs. If you are operating in routed mode, you can configure up to 3 VLANs with the Base license, and 20 VLANs with the Security Plus License.

If you are unsure of which license you have, click the *Home* button on the navigation pane, and click the *License* tab.

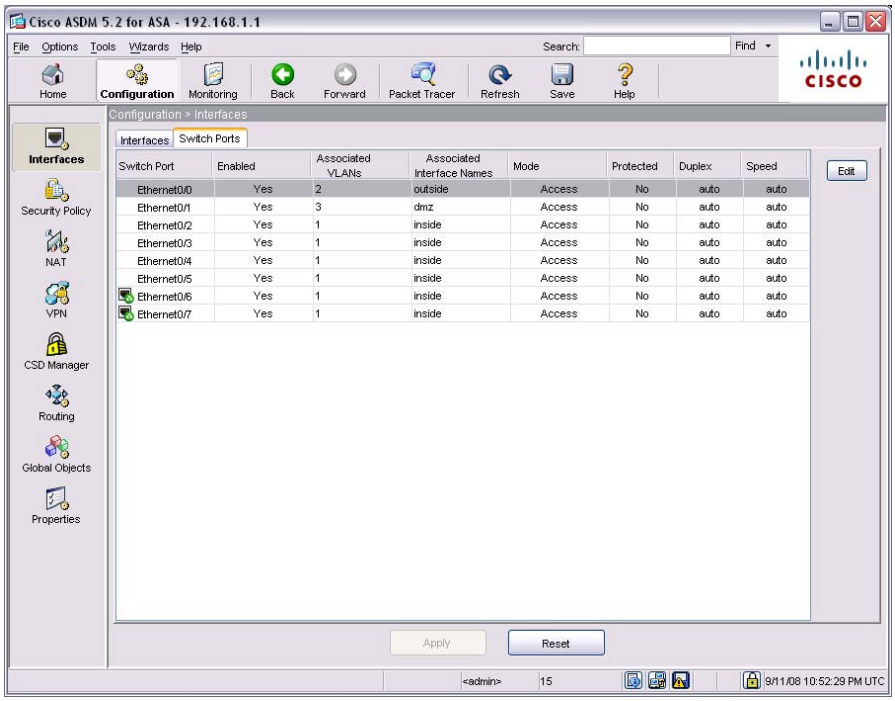
Some of the VLANs and interfaces have already been configured in the Startup Wizard. If you click the Interfaces button on the navigation pane, you can view or make changes to your configuration.



You will see two tabs on the Interfaces page: Interfaces and Switch Ports.

The Interfaces tab gives you an idea of which VLAN, security level, and IP address belong to a particular interface. You can add or edit the interfaces by clicking the appropriate buttons on the right.

The Switch Ports tab gives you information on a per interface basis, as well as speed and duplex information for each physical interface.



You can also edit the properties of an interface by clicking the *Edit* button.

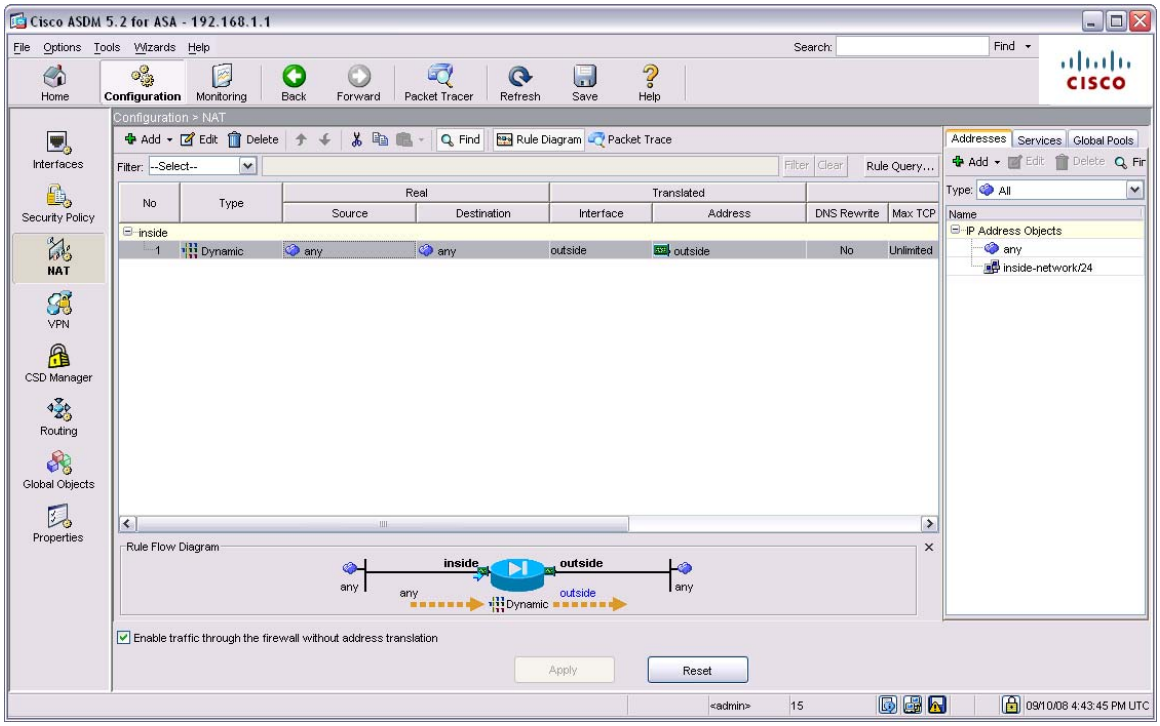
Since all of the switching was preconfigured, you have completed this section of the lab.

Configuring NAT

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. NAT is composed of two steps: the process by which a real address is translated into a mapped address, and the process to undo translation for returning traffic.

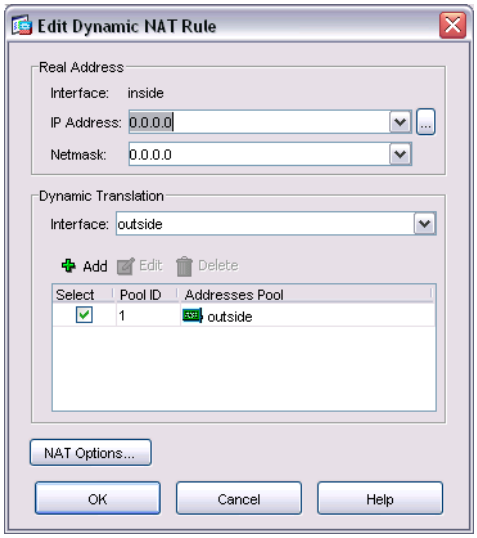
In the Startup Wizard, we configured PAT. In this lab we will be configuring NAT.

Start by clicking the *Configure* button, and then clicking the *NAT* button.

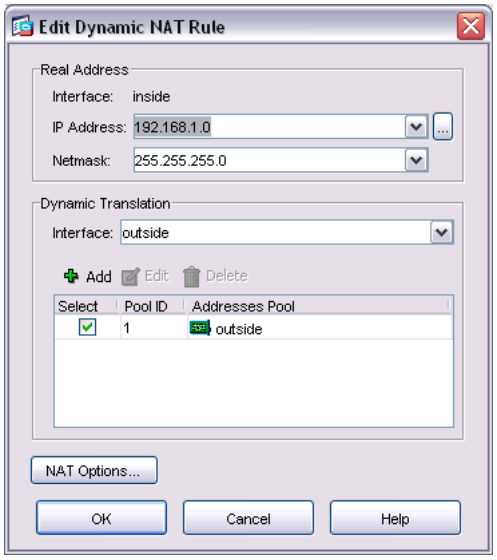


You will see the default NAT rule on the screen.

We will want to add an entry for the Inside VLAN. Click the default NAT rule, and then click the *Edit* button.

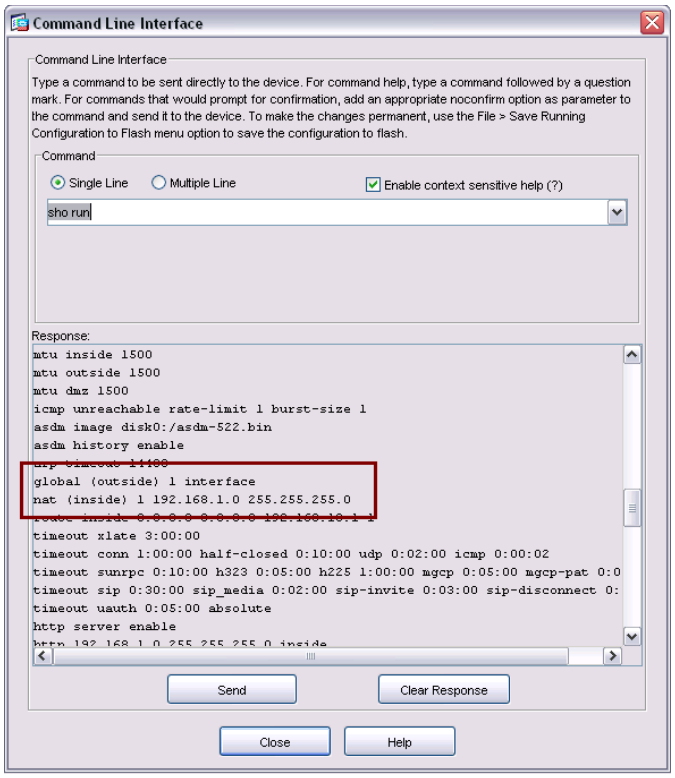


Change the Inside address to reflect that of your network (in this lab 192.168.1.0 with a subnetmask of 255.255.255.0). When you are done, click *OK*.



Now click *Apply* at the bottom of the ASDM screen.

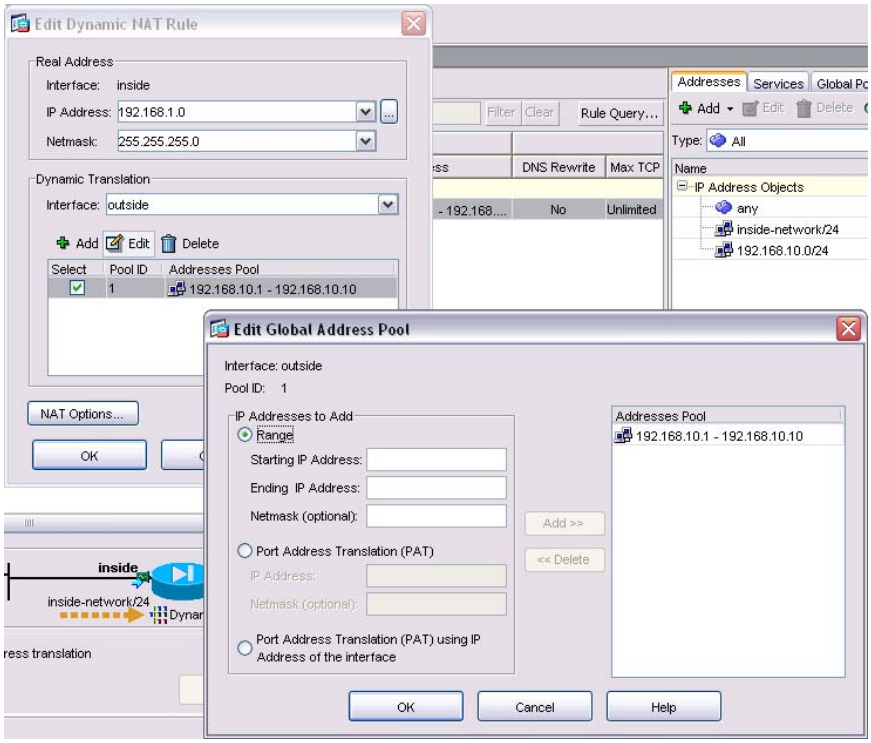
Click Tools > Command Line, and enter the command *sho run* to see what changes you have made.



You should notice that we have successfully created one half of the NAT translation configuration by identifying the Inside VLAN's addresses. Now we need to identify the Outside Global addresses.

Go back to the NAT rule you just created. Click the *Edit* button.

Under Dynamic Translation, select the Outside interface and click *Edit*. This will bring up a new window where you can edit the translation rules.



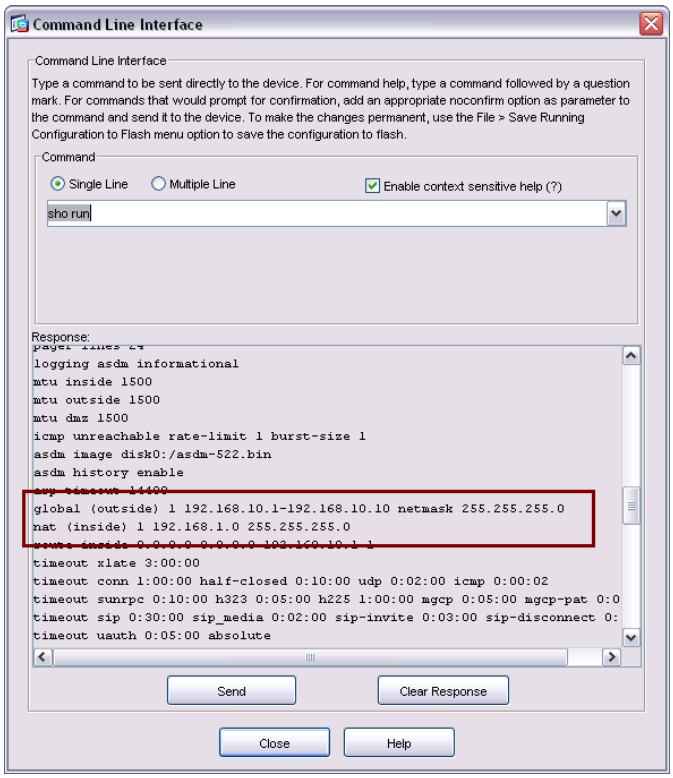
Enter the global IP address Range. In the Lab, we will be using 192.168.10.2 – 192.168.10.10 with a subnetmask of 255.255.255.0.

When you are done, click the *Add* button.

Remove the generic Outside interface address pool by highlighting it, and selecting the *Delete* option.

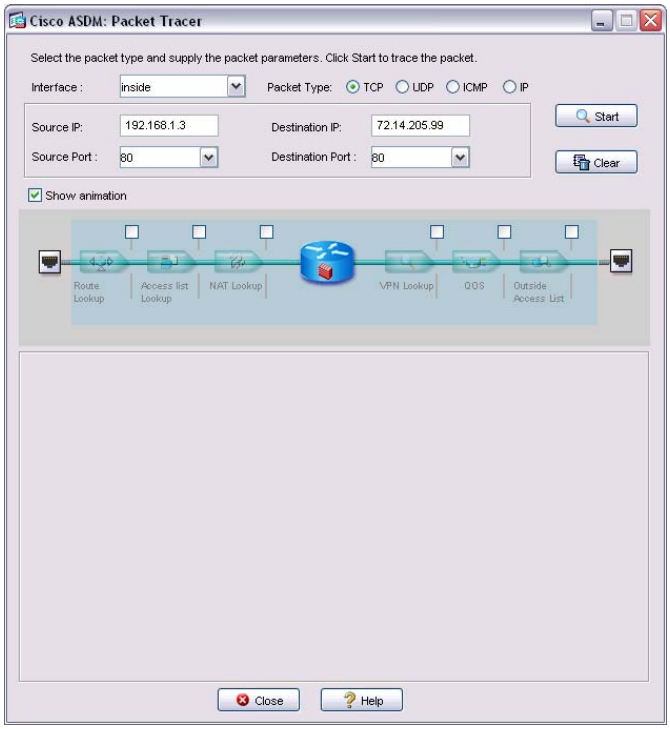
When you are done, click *Apply*.

If you go back to Tools > Command Line and execute the *sho run* command, you will now see the complete NAT configuration.



If you are in an environment with an outside connection, you can test NAT by utilizing ASDM's Packet Tracer application.

Click on *Packet Tracer* to bring up the application.



You will want to run a test from the Inside interface. Enter the source IP address of your machine, and a reachable destination address (72.14.205.99 is www.google.com). Packet tracer will follow your packets through the flow of the network, and report back if there are any problems. You will know if you have configured NAT incorrectly because Packet Tracer will show you a packet drop happening at the NAT stage of the trace.

NOTE: If you're doing a packet trace, make sure the traffic type you're attempting to send is permitted by the firewall. If it is not, you will see the flow dropped by an ACL configuration.

You have now completed the NAT configuration.

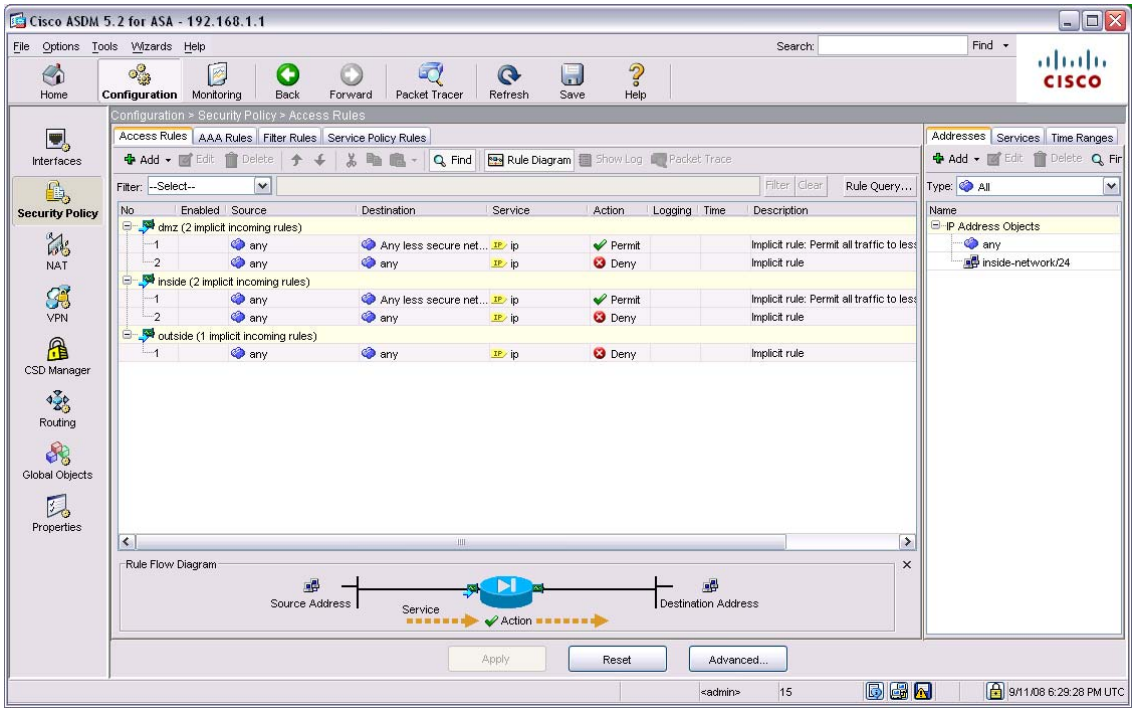
Configuring the Firewall

By default on the security appliance, traffic from a higher security level (for example, Inside) can access a lower security level (for example, Outside): there is an implicit access list on the inside interface allowing all outbound IP traffic from the inside network. (The security appliance denies traffic destined for the inside network from the outside network using the Adaptive Security Algorithm. The Adaptive Security Algorithm is a stateful approach to security. Every inbound packet is checked against the Adaptive Security Algorithm and against connection state information in memory.) The implicit access list appears in ASDM, but you cannot edit it. To limit outbound traffic, you can add an access list (in which case, the implicit access list is removed).

Every inbound packet is checked using the Adaptive Security Algorithm unless a connection is already established. By default on the security appliance, no traffic can pass through the firewall unless you add an access list to allow it.

To allow traffic that is normally denied by the Adaptive Security Algorithm, you can add an access list; for example, you can allow public access to a web server on a DMZ network by adding an access list to the outside interface.

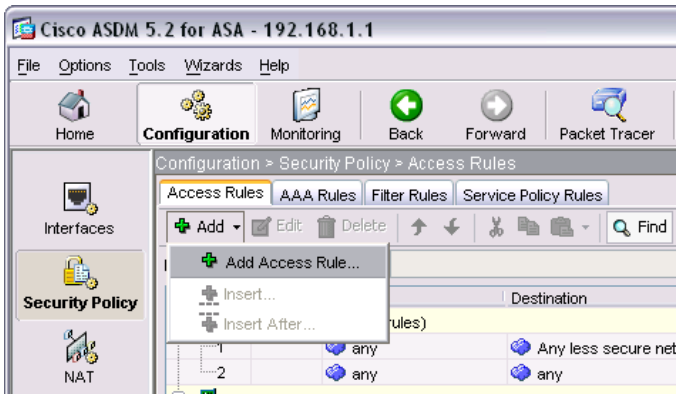
Check the implicit rules by clicking *Security Policy* on the navigation pane.



Here you can see how access lists have been created to manipulate the behaviour of traffic flowing from a VLAN with one security level to another. If you want to see how these access lists behave, you can test them in Packet tracer. You will need an external connection to test packet flow with Packet tracer.

For the sake of this lab, let's assume you had an FTP server residing on the DMZ. In order for the FTP server to be accessible from the outside world, we would need to add an access list to the configuration.

Start by clicking *Add*, and then selecting *Add Access Rule*.



What we are trying to do is create an ACL that will permit traffic from the Outside interface to a particular host on the DMZ. Let's assume our FTP server is residing at 172.16.1.100, and we want to configure the ACL for FTP in active mode.

In the Add Access Rule dialogue box, configure the following parameters:

Interface and Action

Interface – *outside*
Direction – *incoming*
Action – *permit*

Source

Source – *any*

Destination

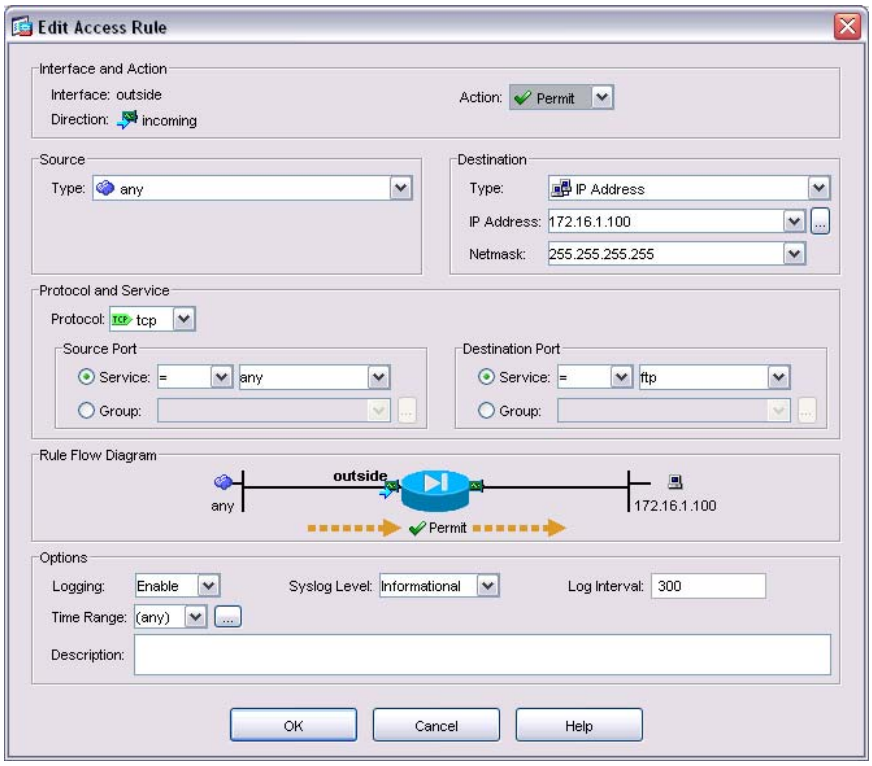
Type – *IP address*
IP Address –*172.16.1.100*
Netmask – *255.255.255.255*

Protocol and Service

Protocol – *tcp*
Source Port
Service – = *any*
Destination Port
Service – = *ftp*

Options

Logging – *enable*
Syslog Level – *informational*
Log Interval – *300*



When you are done, click *OK* and then *Apply*.

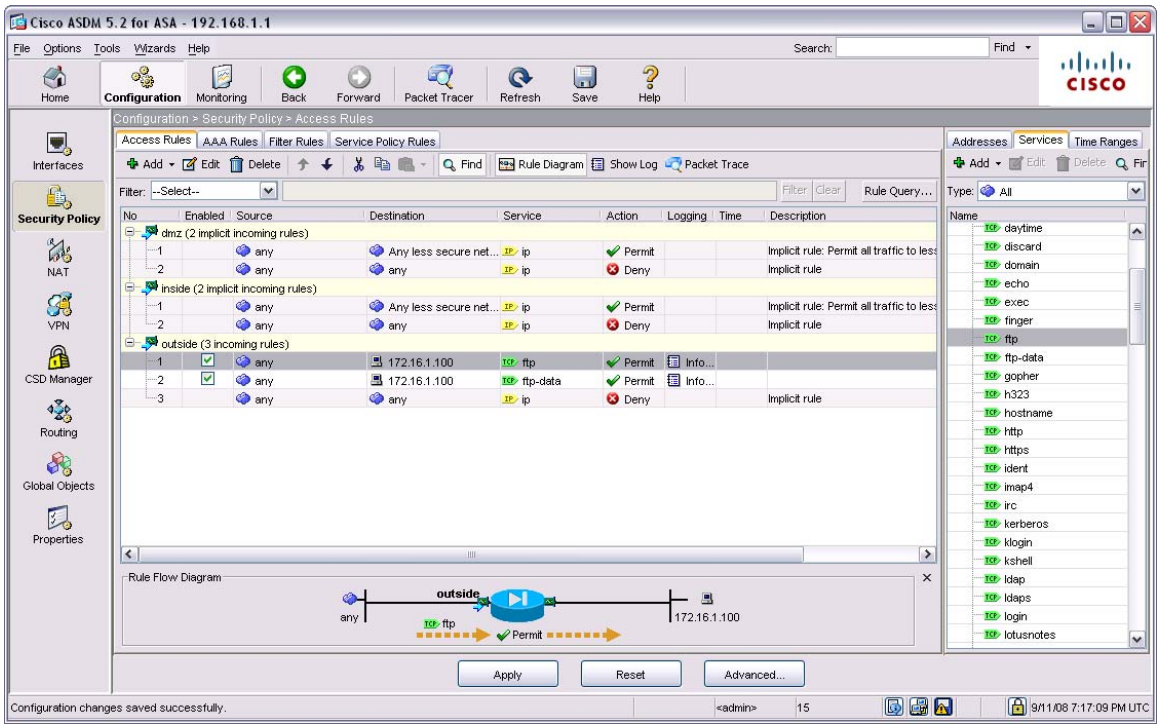
When FTP is operating in active mode, it uses port 21 for control and port 20 for data. We have completed the portion of the access list that permits control information, but what about data?

Go back and create a new access rule. The parameters for the new access list will be exactly the same as the one you have just created, but instead of a destination port service of *ftp*, we will select the *ftp-data* service.

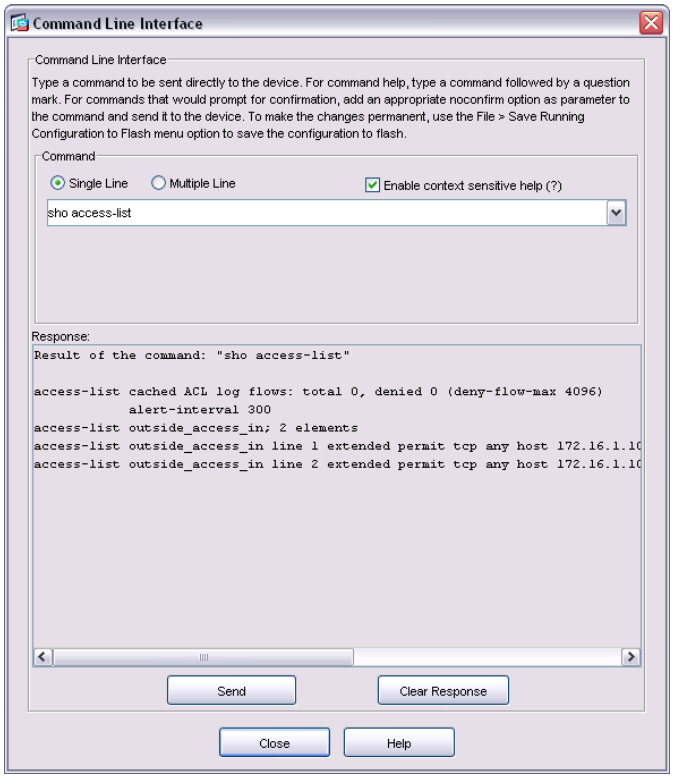
Click on *OK* and then *Apply* when you are done.

NOTE: Creating a rule by itself will NOT permit traffic to a DMZ. Either NAT has to be configured, or NAT has to be disabled on the DMZ. The ASA is heavily reliant on NAT to get traffic through the firewall.

You should now see two new access lists applied to the Outside interface.



Click on Tools > Command Line and enter the command *sho access-list* to review your changes. Optionally, your changes can be viewed with the *sho run* command.



As a recap, here is what we have configured:

1. We have created an access list that permits FTP traffic from the Outside interface to an FTP server on the DMZ (172.16.1.100/24).

2. We have identified that any source protocol can access the FTP server, and have permitted these sources to access the FTP control and data protocols at 172.16.1.100.

3. We have enabled logging.

You have now configured basic firewalling.

Web Filtering

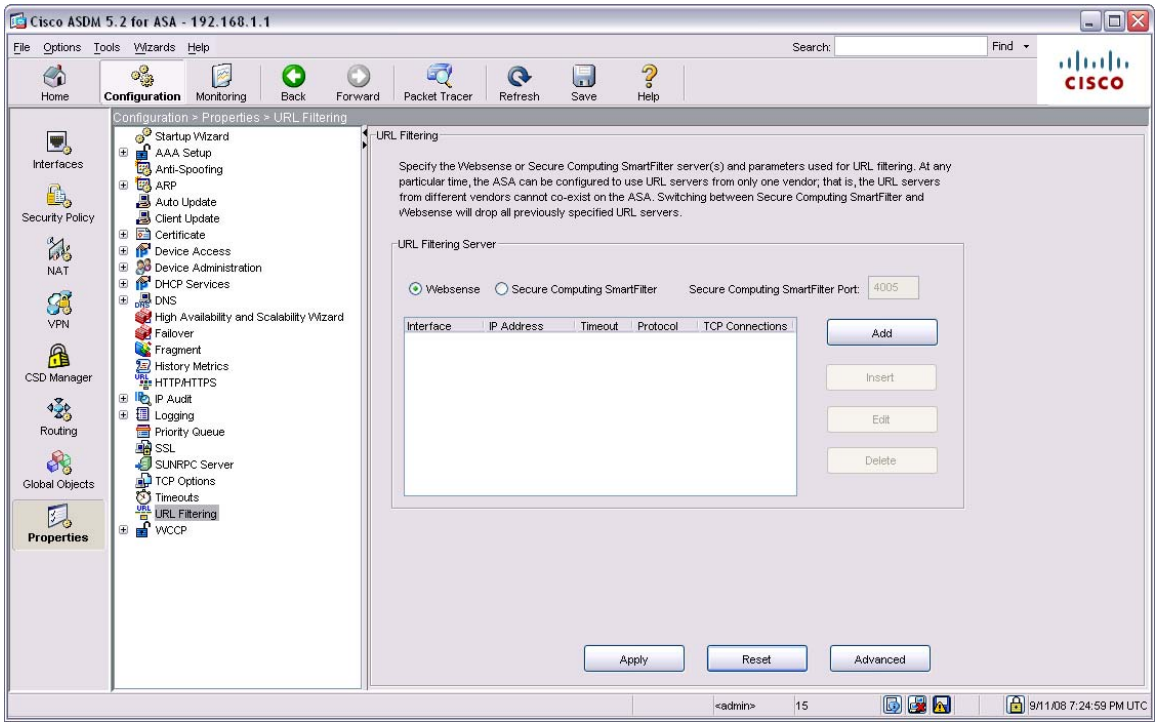
The firewall configuration on the ASA via ASDM is quite extensive, and goes far beyond the simple access list we've created for FTP. The next feature you will configure is URL filtering.

The ASA 5505 supports URL filtering by tying in functionality with either a Websense or Secure Computing SmartFilter server. URL filtering can be leveraged to control internet usage by blocking access to particular sites or web applications.

When filtering is enabled and a request for content is directed through the security appliance, the request is sent to the content server and to the filtering server at the same time. If the filtering server allows the connection, the security appliance forwards the response from the content server to the originating client. If the filtering server denies the connection, the security appliance drops the response and sends a message or return code indicating that the connection was not successful.

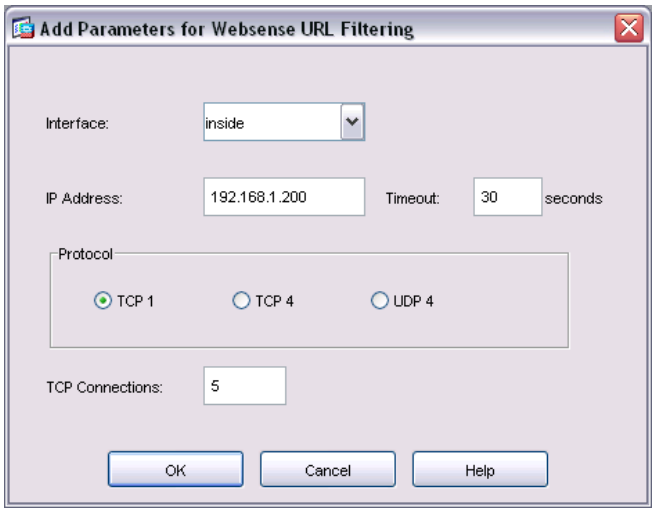
The first step to creating a web filter is to identify the filtering server.

Click on *Properties* in the left hand navigation panel, and then click *URL Filtering*.



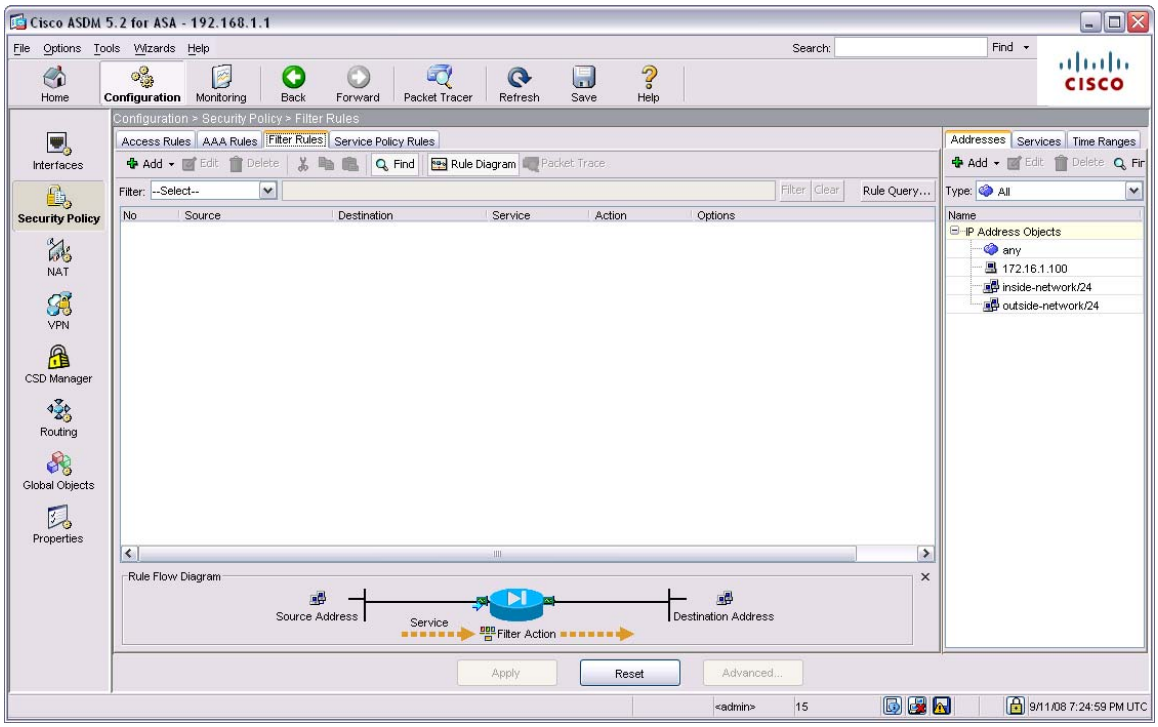
Click the *Add* button to add a filtering server. When the dialogue box comes up, add the following information for your server:

Interface – *inside*
IP Address – *192.168.1.200*
Timeout – *30*
Protocol – *TCP*
TCP Connections – *5*



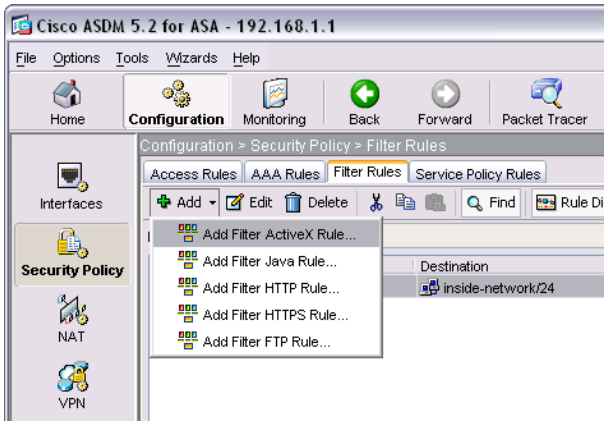
When you are done, click *OK*, and then *Apply*.

Go back to the *Secuirty Policies* screen, and click the *Filter Rules* tab.



We are going to set up a web filter to prohibit ActiveX from the Outside interface to the Inside interface. Instead of blocking entire websites because of content, we are going to filter specific web applications (in this case, ActiveX) from the ASA.

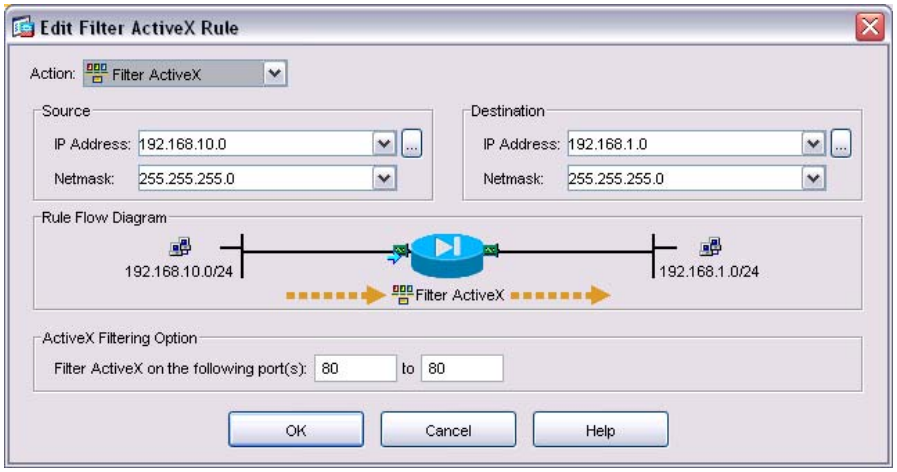
Click on the *Add* button, and select the *Add Filter for ActiveX* Rule option.



We will now set up the rule prohibiting access to ActiveX on the Inside interface from the Outside interface.

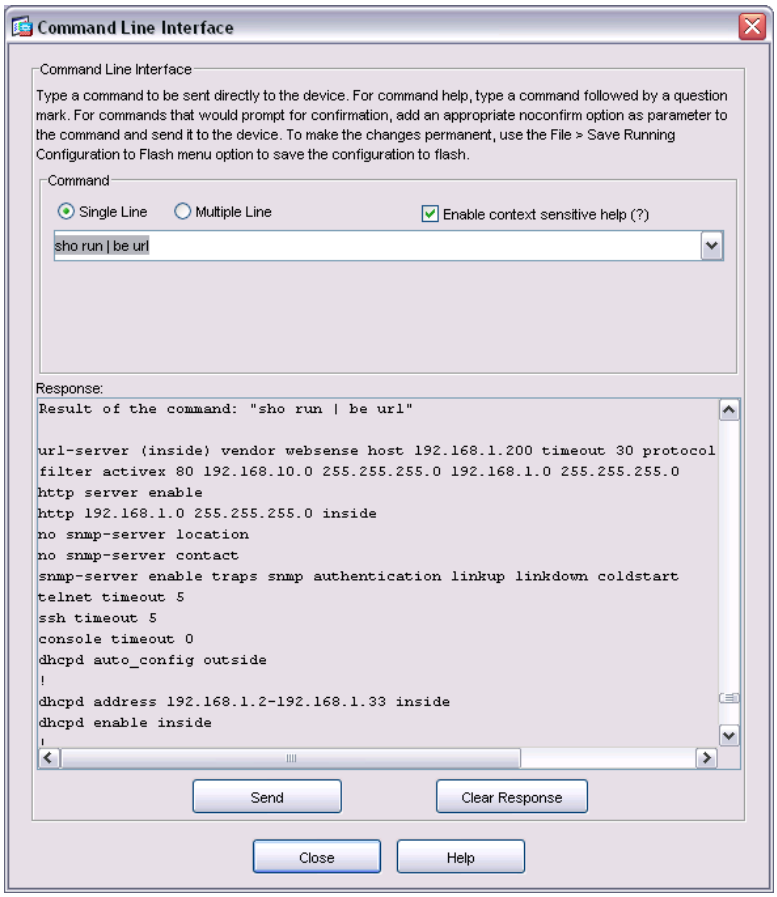
In the Edit Filter dialogue box, configure the following:

Action: *Filter ActiveX*
Source: *click the … box next to the IP Address field and select Outside Network*
Destination: *click the … box next to the IP Address field and select Inside Network*
Filter ActiveX on the following ports: *80 to 80*

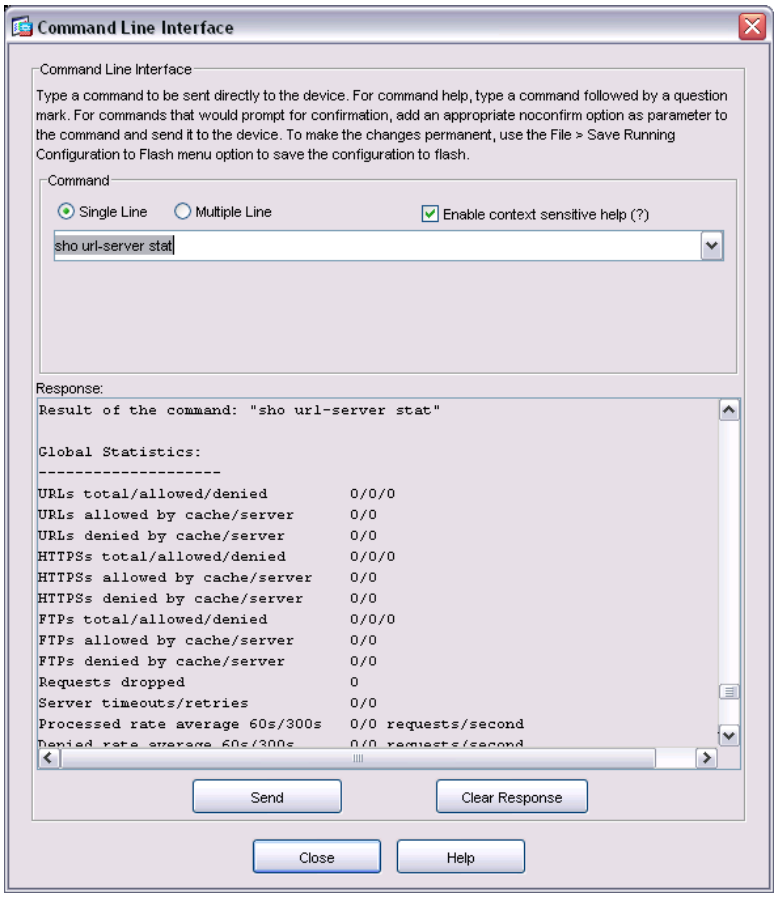


When you are done, click *OK*, and then *Apply*.

If you want to view your changes in CLI, click Tools > Command Line, and enter the command *sho run | be url*.



To view statistics on your URL filtering server, click Tools > Command Line, and enter the command *sho url-server stat*.



You have now completed the process to configure Web filtering.

Configuring Site to Site VPN

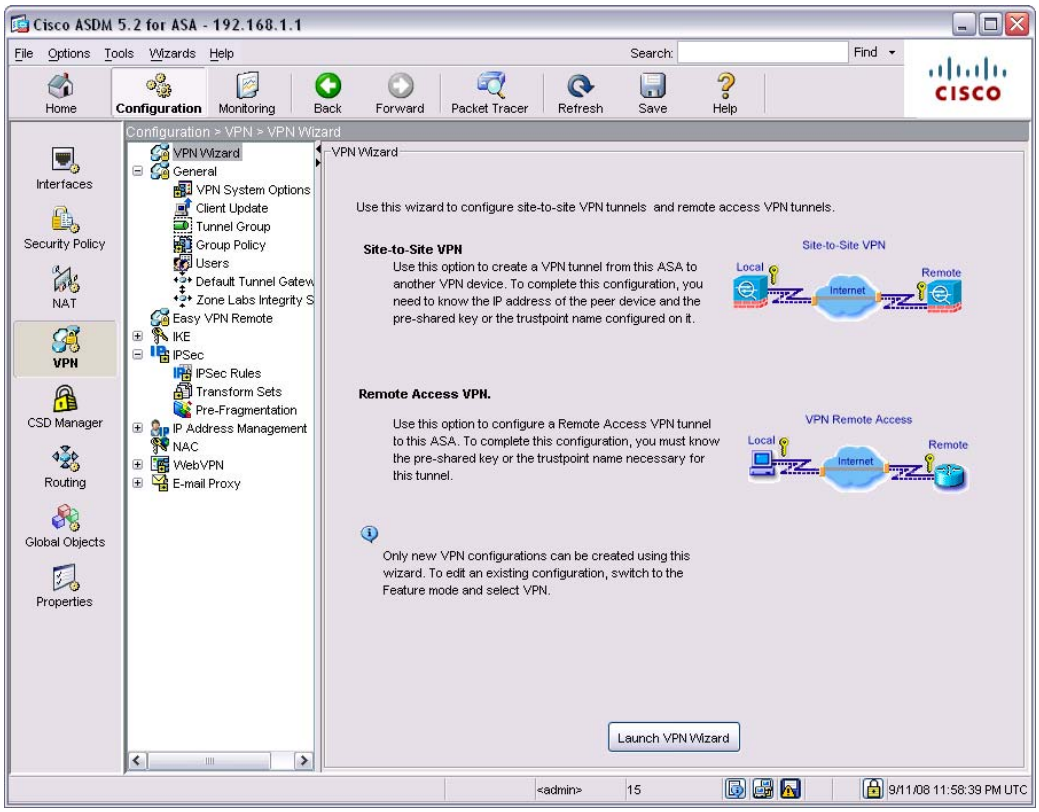
The ASA 5505 can create a virtual private network by creating a secure connection across a TCP/IP network (i.e. the Internet). This secure connection is called a tunnel, and the ASA 5505 will use tunneling protocols to negotiate security parameters and manage packets while in transit.

With ASDM, you can use a VPN wizard to configure either of the following types of VPN:

1. **Site to Site** – creates a LAN to LAN VPN configuration, which is used between two IPSec gateways.

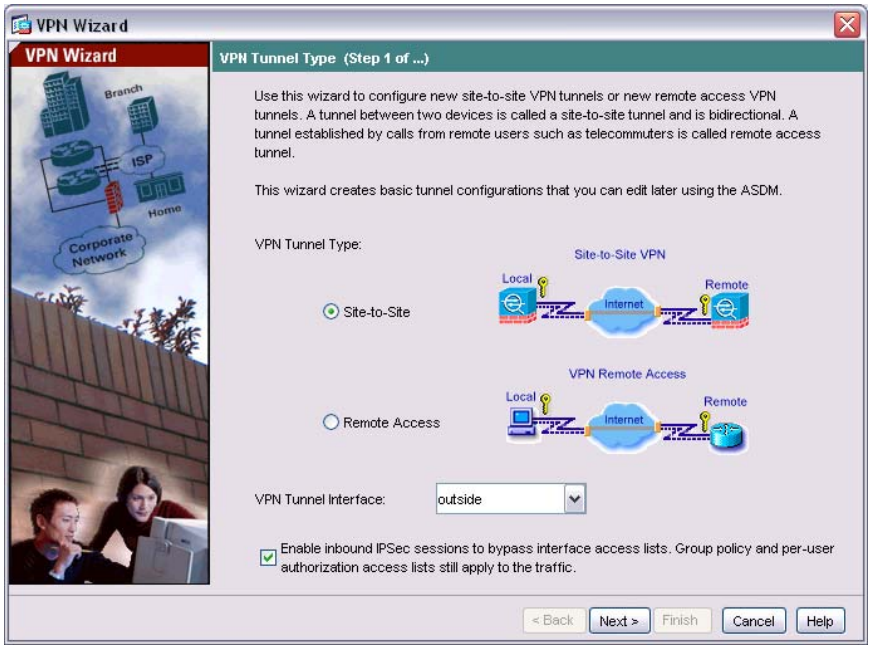
2. **Remote Access** – creates an endpoint to LAN VPN configuration for clients.

To set up a new VPN, click the *VPN* button in the navigation pane on the left, and then click *VPN Wizard*.



Click the *Launch VPN Wizard* button.

Step 1 will ask you to select the type of VPN you would like to configure. Since we will be creating a site to site VPN for this lab, select the option for a site to site setup and then click *Next*.



Step 2 will ask you to configure information for the remote side of the connection.

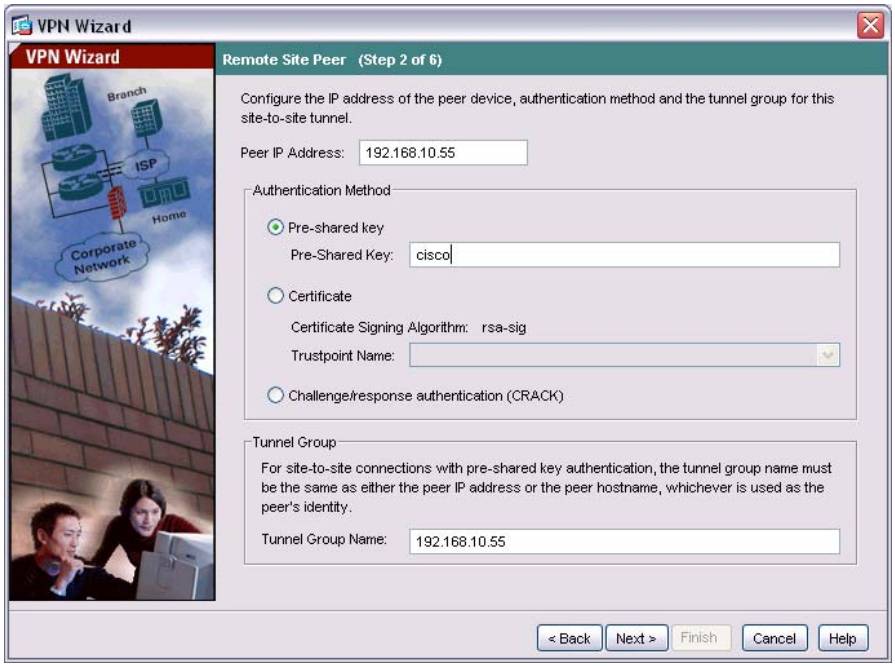
For this lab, configure the following options:

Peer IP Address: *192.168.10.55*
Authentication Method: *preshared key*
Preshared Key: *cisco*
Tunnel Group Name: *192.168.10.55*

What we are doing is identifying the device on the other end of the tunnel, setting a preshared key which will be used for authentication, and naming the tunnel group.

Using a preshared key is a quick and easy way to set up communication with remote peers. Each pair of IPSec peers must exchange preshared keys to establish secure tunnels.

The tunnel group name will create a record containing connection properties for this tunnel. This tunnel group can identify AAA servers, a default group policy, and IKE attributes.



When you are done, click *Next*.

Step 3 will ask you to configure the IKE policy. IKE is the security negotiation protocol that lets two hosts agree on how to build an IPSec SA (security association). IKE is broken into 2 phases (the first phase creates a tunnel to protect further IKE messages, and the second phase creates a tunnel to protect data). To create the policy for Phase 1, we need three pieces of information:

1. An encryption method – The options are DES, 3DES, AES-128, AES-192, and AES-256. The number specifies how long the keys are in bits.

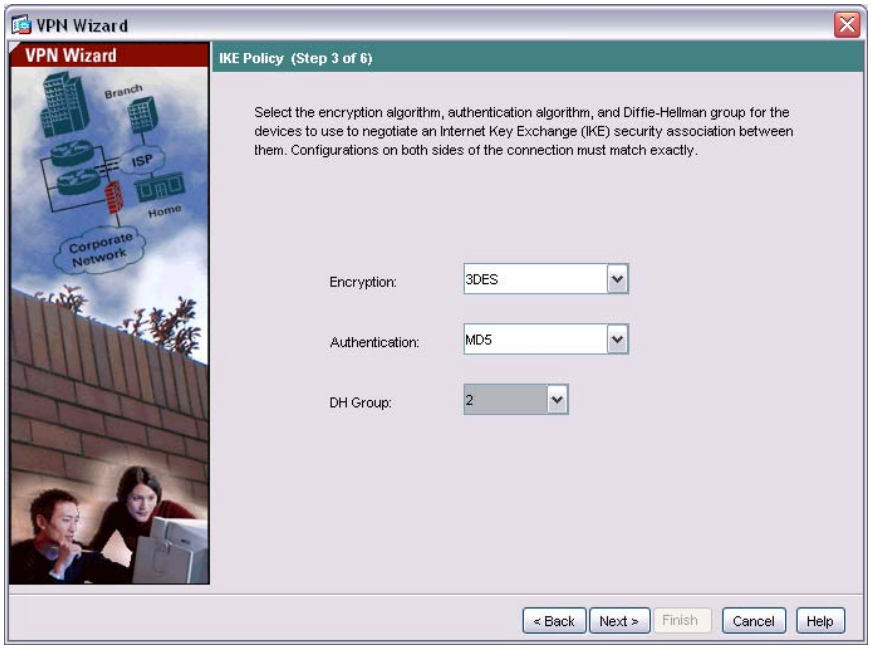
2. An authentication method – The options are SHA or MD5, and both are hash algorithms. SHA is considered more secure, but MD5 is faster.

3. A Diffie-Hellman group to establish the strength of the encryption key – This algorithm is used to derive a shared secret between two peers without actually transmitting it to each other. The options are 1, 2, 5, or 7.

For this lab, configure the following:

Encryption: *3DES*
Authentication: *MD5*
DH group: *2*

The decision to uses these properties is usually governed by a corporate security policy. Remember, the stronger the encryption, authentication, and DH groups, the greater the processing requirement is for the security appliance.



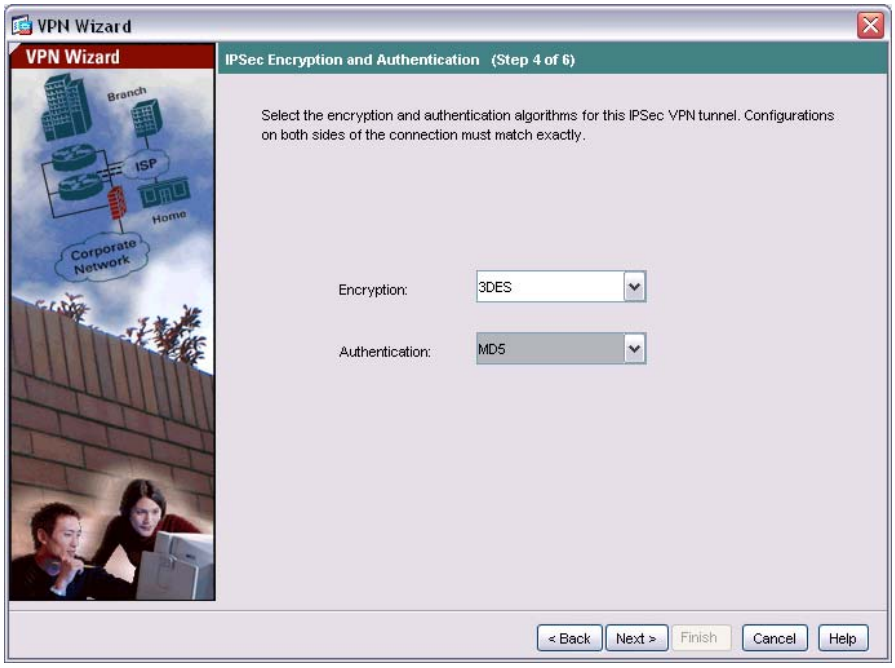
When you are done, click *Next*.

Step 4 will ask you to select the IPSec Encryption and Authentication settings. These settings will configure IKE for Phase 2, and require two pieces of information:

1. Encryption method – The options are DES, 3DES, AES-128, AES-192, and AES-256

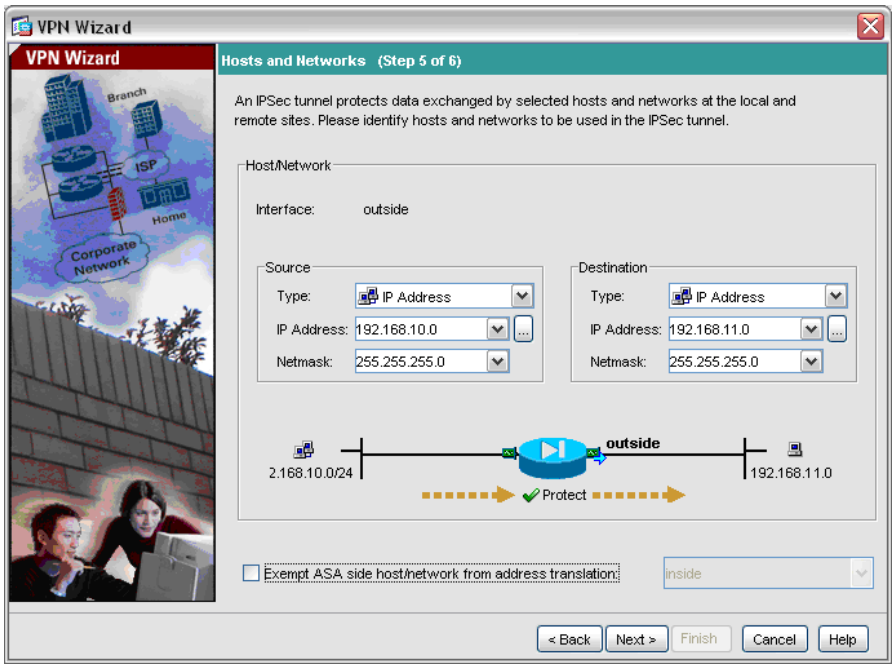
2. Authentication method – The options are SHA or MD5

For this lab we will be using *3DES* and *MD5*.



When you are done, click *Next*.

Step 5 will ask you to identify hosts and networks that can use this IPSec tunnel. Since we are setting up a site to site VPN and we only want to grant VPN access to those two sites, configure the source and destination to be your two IPSec endpoints.



Earlier in the lab we configured our Outside interface to obtain an IP address via DHCP. On the remote side of this configuration, our peer would have to identify our interface by our hostname.

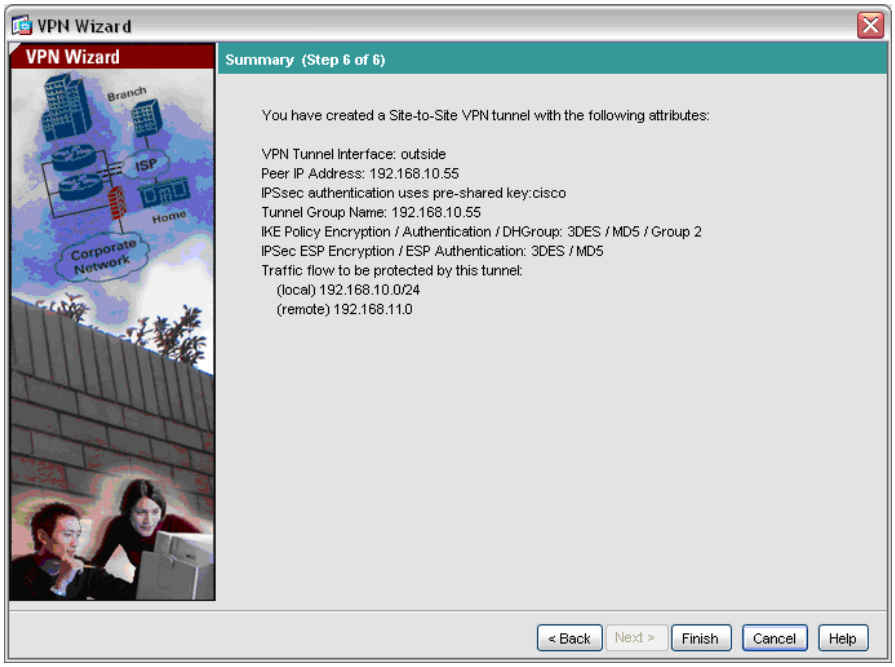
Configure the local side of the connection by entering an IP address of *192.168.1.0/24* in the IP address and netmask fields. Optionally, you can select the inside interface by clicking the ellipsis button.

Configure the remote side of the connection by entering the IP address of the remote network (*192.168.11.0/24*) in the IP address and netmask fields.

The “Exempt ASA side host network from address translation” check box allows traffic to flow through the ASA without address translation.

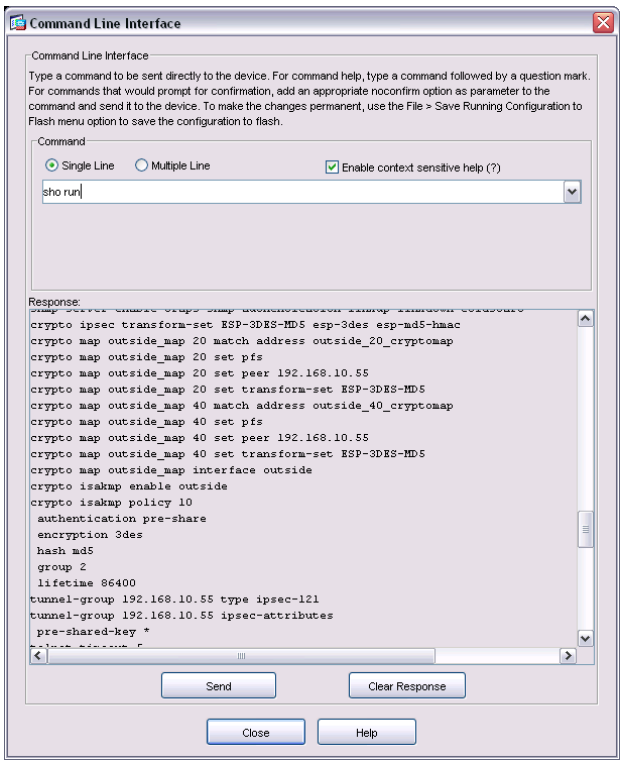
When you are done, click *Next*.

Step 6 will ask you to review your configuration. When you are done, click Finish



If you need to make changes to your settings after the VPN Configuration Wizard, you can do so on the VPN screen.

If you would like to verify your settings in CLI, click Tools > Command Line. Notice the new access lists permitting you access to 192.168.11.0, and the new crypto map statements associated with the newly configured VPN.

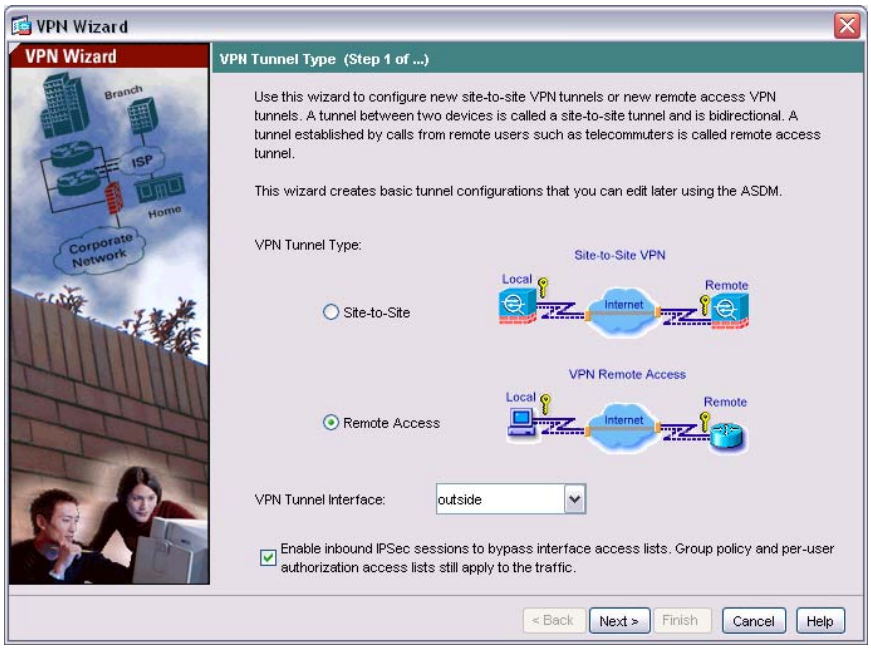


You have now completed the site to site VPN configuration.

Remote Access VPN

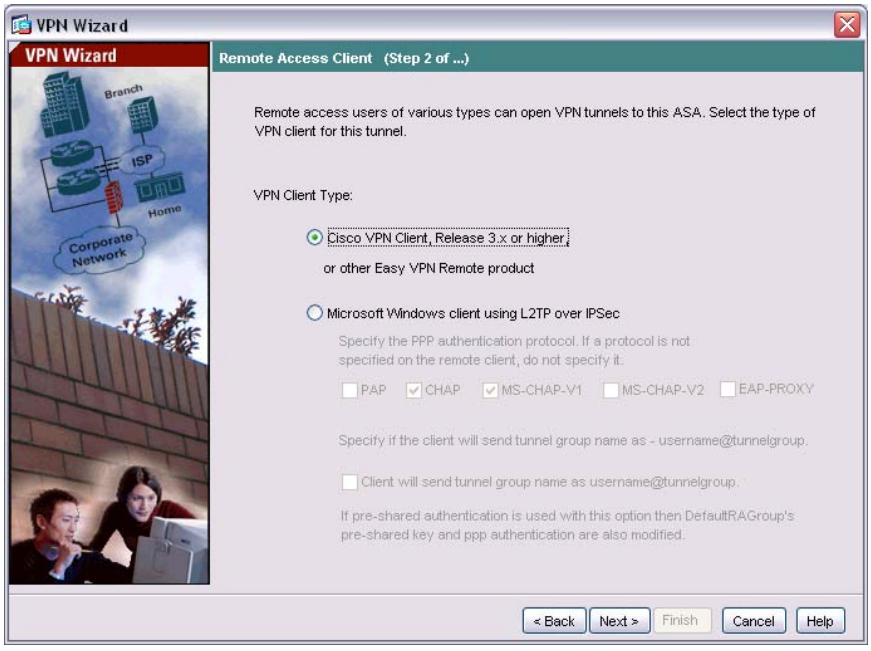
Like a site to site VPN, a remote access VPN is designed to create a secure tunnel for communications. A remote access VPN will create a configuration that achieves secure remote access for VPN clients, such as mobile users.

To begin, relaunch the VPN Wizard, selecting the VPN type as Remote Access in **Step 1**.



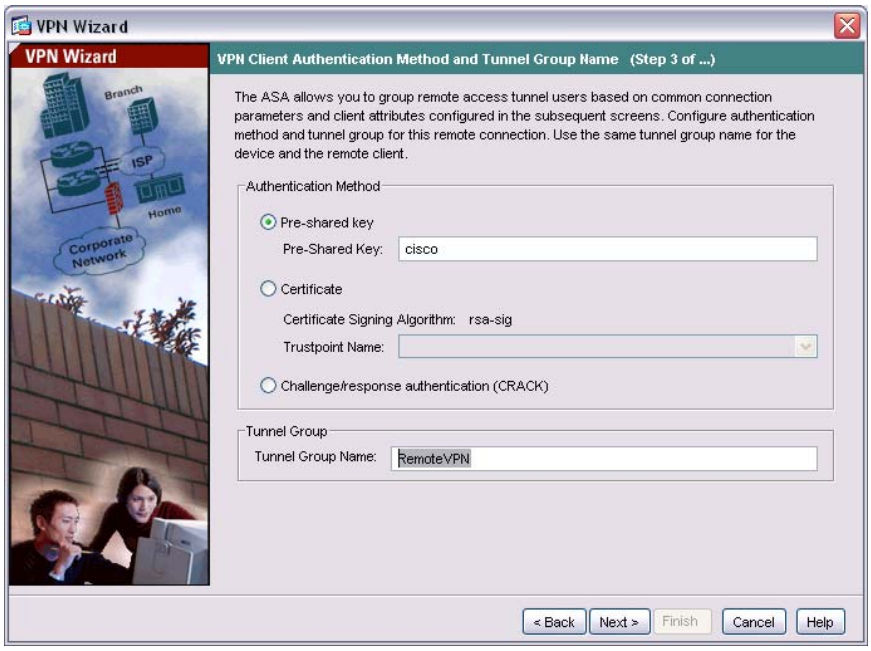
Click *Next* to continue.

Step 2 will ask you to select the type of VPN client to be used by remote users. For this lab, select *Cisco VPN Client*, and click *Next*.



Step 3 will ask you to configure the authentication method and tunnel group name. Since we don't have a certificate server, select *Pre-shared Key* as the authentication method. Enter the key: *cisco*.

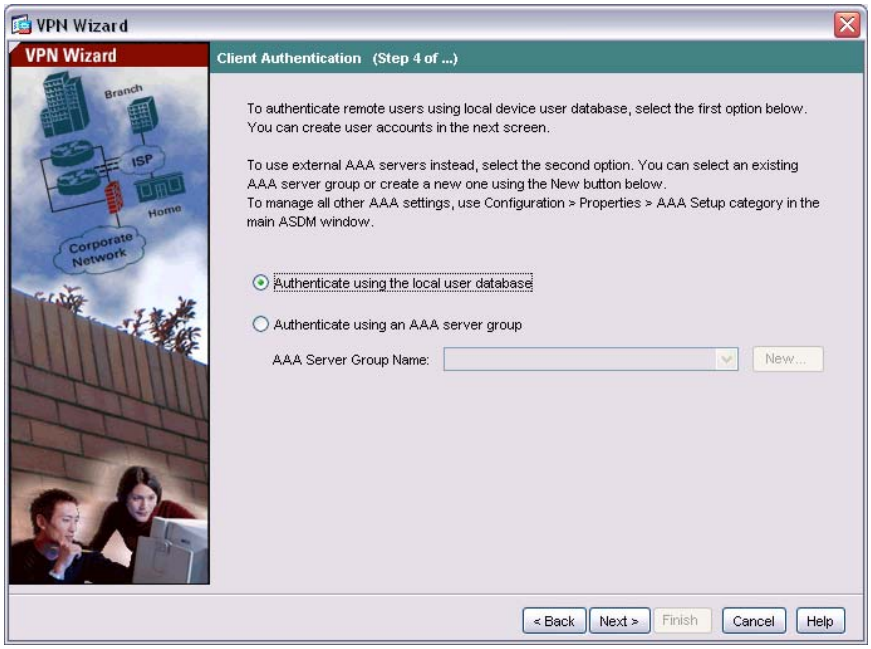
Enter the tunnel name: *RemoteVPN*



Click *Next* when you are done.

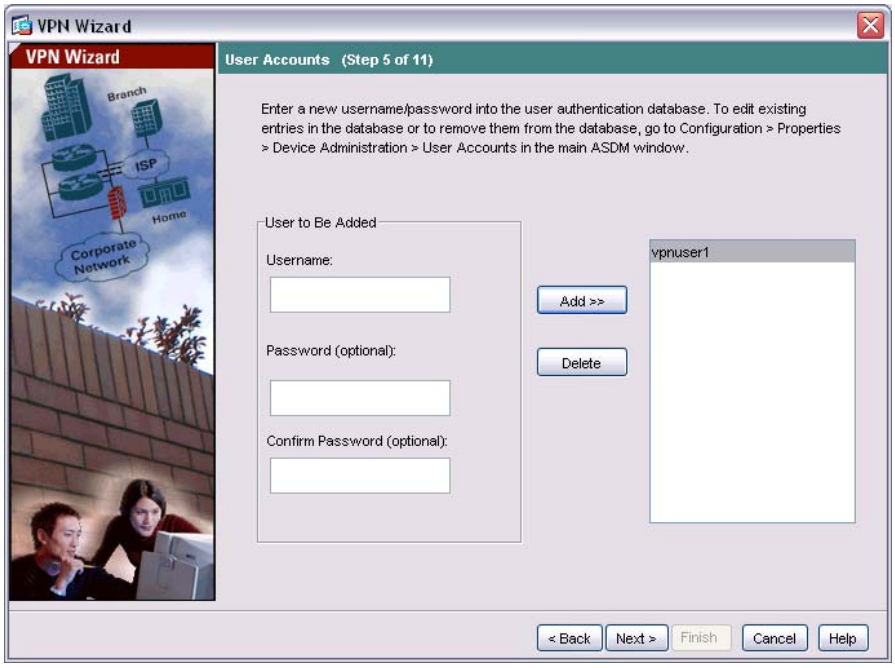
Step 4 will ask you to select a user authentication method. Users can be authenticated by a local database, or by using external AAA servers.

Since we don't presently have an AAA server, select the *local user database* radio button, and click *Next*.



Step 5 will ask you to create user accounts. This is the local database that will be used for user authentication.

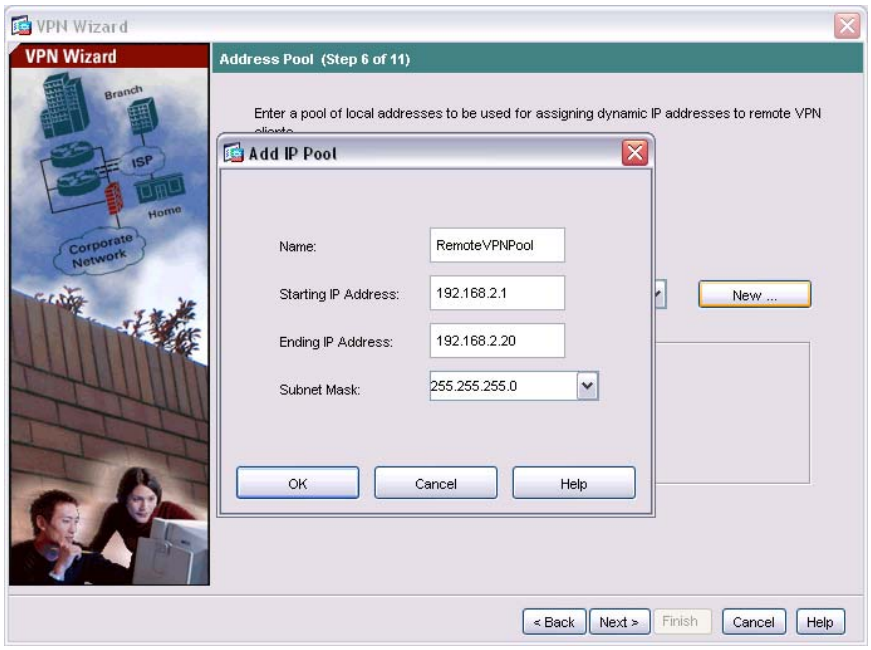
Enter a username of *vpnuser1* and a password of *cisco*, then click Add. Click *Next* to continue.



Step 6 will ask you to enter an address pool. For remote clients to gain access to the network, you need to configure a pool of addressed that can be assigned to VPN clients as they are successfully connected.

Click the New button to create a new pool.

Enter a pool name of RemoteVPNPool, and a range of 192.168.2.1/24-192.168.2.20/24.



Click *OK*, and then *Next* to continue.

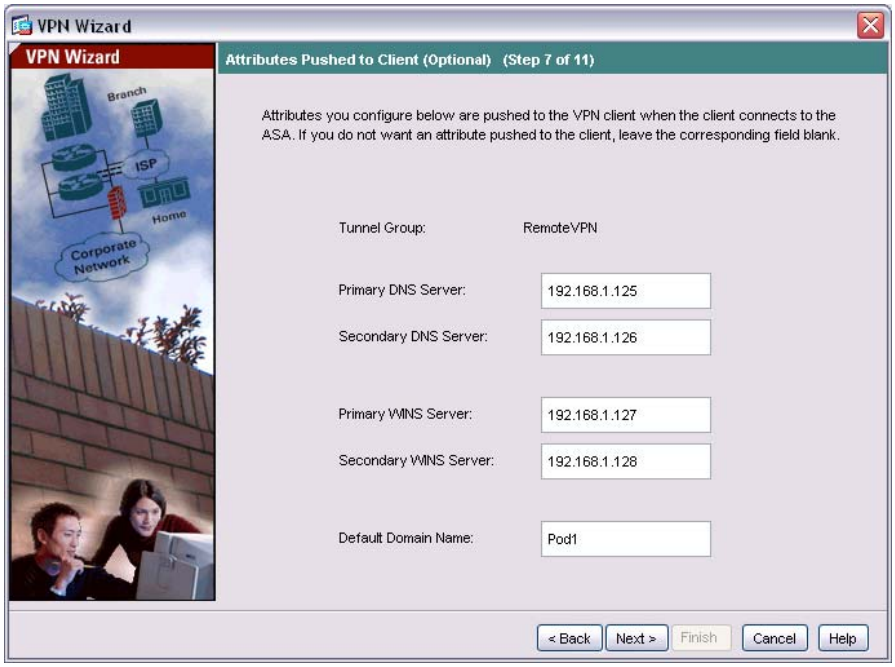
Step 7 will ask you to configure attributes to push out to clients. Each remote client will need a basic network configuration including things like DNS and WINS servers.

For the lab, let's assume we have the following servers:

DNS 1 – *192.168.1.125*
DNS 2 – *192.169.1.126*

WINS 1 – *192.168.1.127*
WINS 2 – *192.168.1.128*

We will also use the domain name of *Pod1.*



Click *Next* to continue.

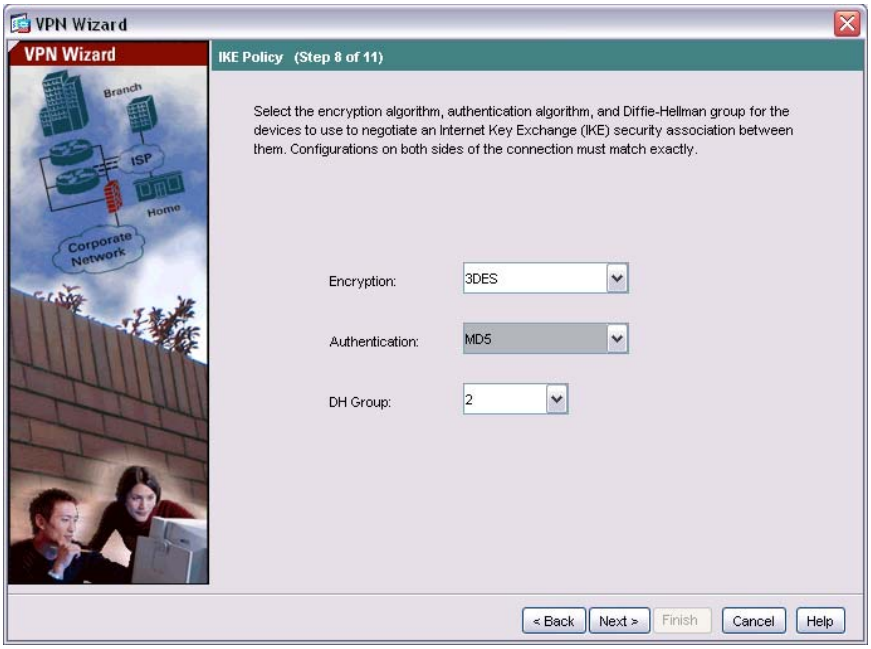
Steps 8-9 will ask you to configure the IKE policy and IPSec encryption and authentication methods. Since we've gone over this in the last VPN example, configure the following:

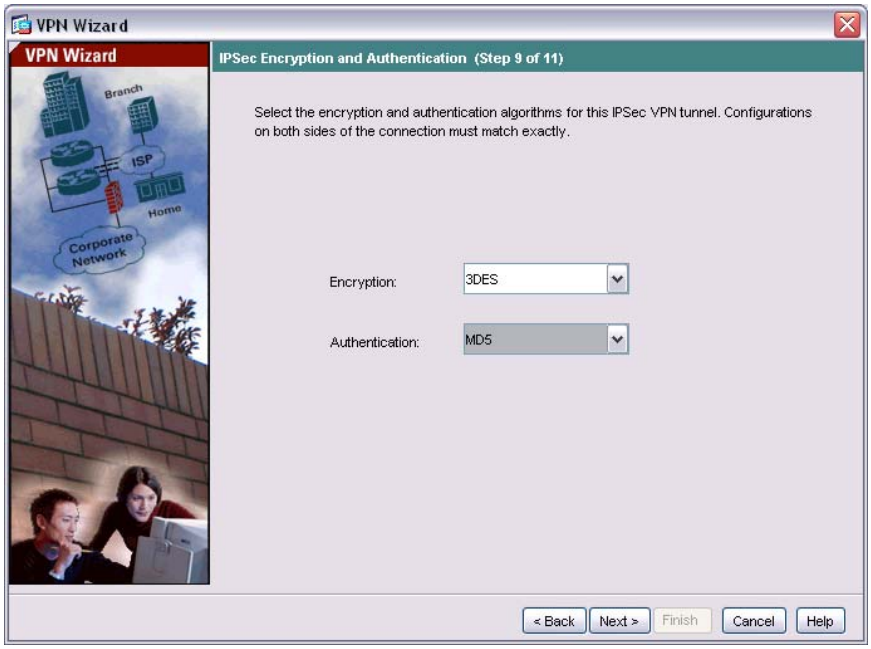
IKE Policy

Encryption: *3DES*
Authentication: *MD5*
DH group: *2*

IPSec Encryption and Authentication

Encryption: *3DES*
Authentication: *MD5*





Click *Next* to continue.

Step 10 will ask you to configure any address translation exemptions and split tunneling. Split tunneling allows remote users to access a VPN at the same time they are connected to a LAN. The NAT exception will expose all or part of a network to your remote users.

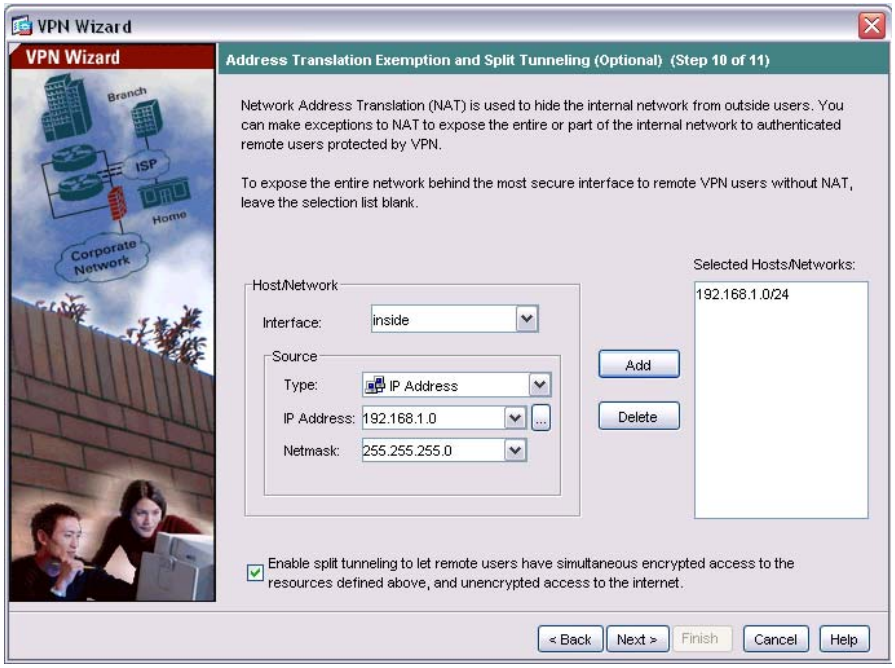
Since we want our users to see the entire Inside network, add the Inside network to the list of exceptions by entering the following information:

Interface – *Inside*
Source Type – *IP address*
Source IP Address – *192.168.1.0*

Source Netmask – *255.255.255.0*

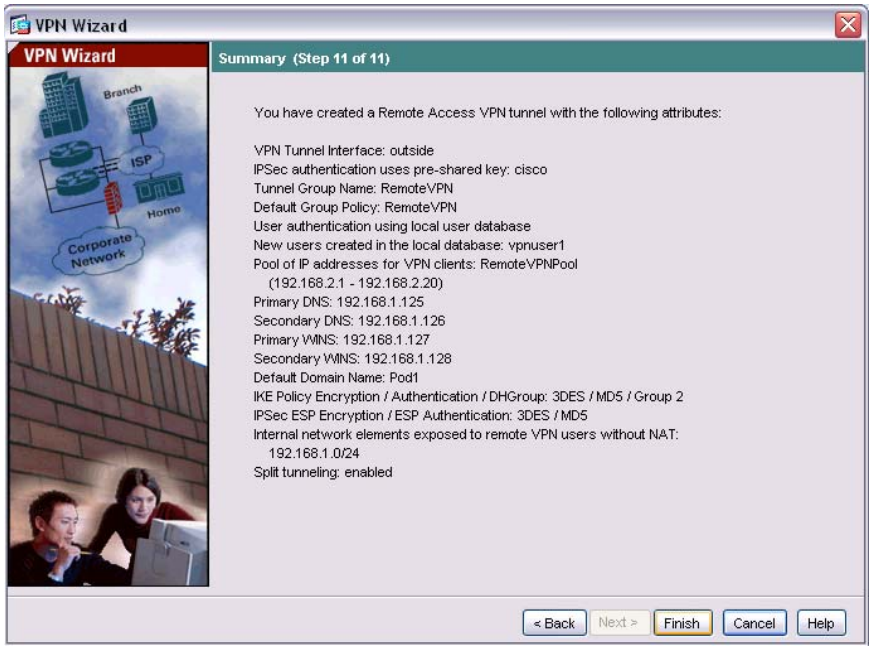
When you are complete, click *Add*.

Since we also want our users to be able to use split tunneling, check the checkbox allowing them to do so.



Click *Next* when you are complete.

Step 11 will ask you to verify the configuration. Click Finish to complete the Wizard.



If you get a warning about the RemoteVPN group not existing, don’t panic. Complete the configuration and you will see the group has been added to the Group Policy list.

You have now completed the Remote VPN configuration.

Easy VPN Remote

A Cisco Easy VPN hardware device enables companies with multiple locations to establish secure connectivity with minimal configuration. Cisco Easy VPN consists of appliances with one of two roles: clients and servers.

A Cisco Easy VPN server is responsible for pushing out security policies to remote sites so a remote site has up to date policies before the connection is established.

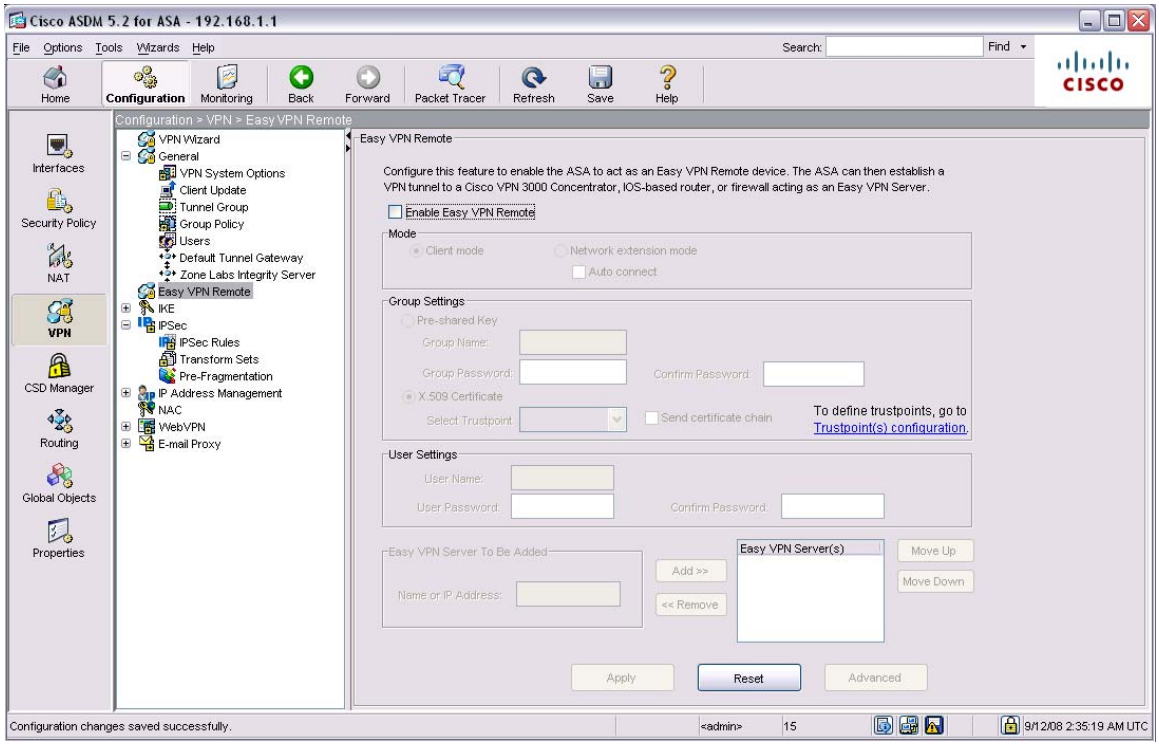
A Cisco Easy VPN client would maintain a minimal VPN configuration, and would use this configuration to connect to an Easy VPN server to pull down a complete configuration.

Cisco Easy VPN simplifies configuration by:

- Eliminating the need for hosts at remote site to run a VPN client
- Storing security policies on a centralized server, pushing them out to remote hardware clients when a VPN connection is established
- Minimizing the number of local configuration parameters

Since the 5505 is a relatively small device, we will be configuring it as a client in this lab.

To begin, click *VPN* in the left-hand navigation pane, and the click *Easy VPN Remote*.



Check the enable *Easy VPN Remote* checkbox to begin the configuration.

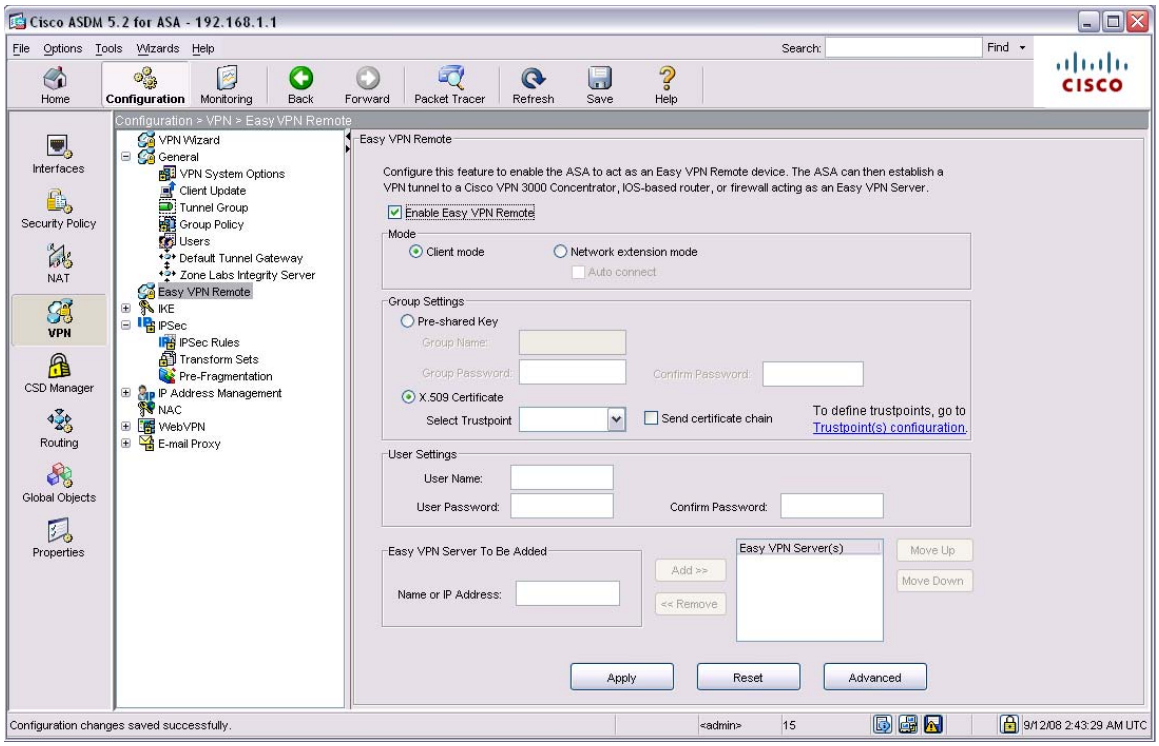
NOTE: because of design, an ASA 5505 cannot run different types of tunnels if it is running Easy VPN Remote. You will not be able to make changes to IPSec or remote access VPNs while Easy VPN Remote is enabled.

Easy VPN Remote can operate in one of two modes: client and network extension modes.

Client mode isolates all devices on the client network from those on the enterprise network. The Easy VPN client will perform PAT for all VPN traffic for its inside hosts.

Network extension mode makes the inside interface and all inside hosts routable across the tunnel and on the enterprise network.

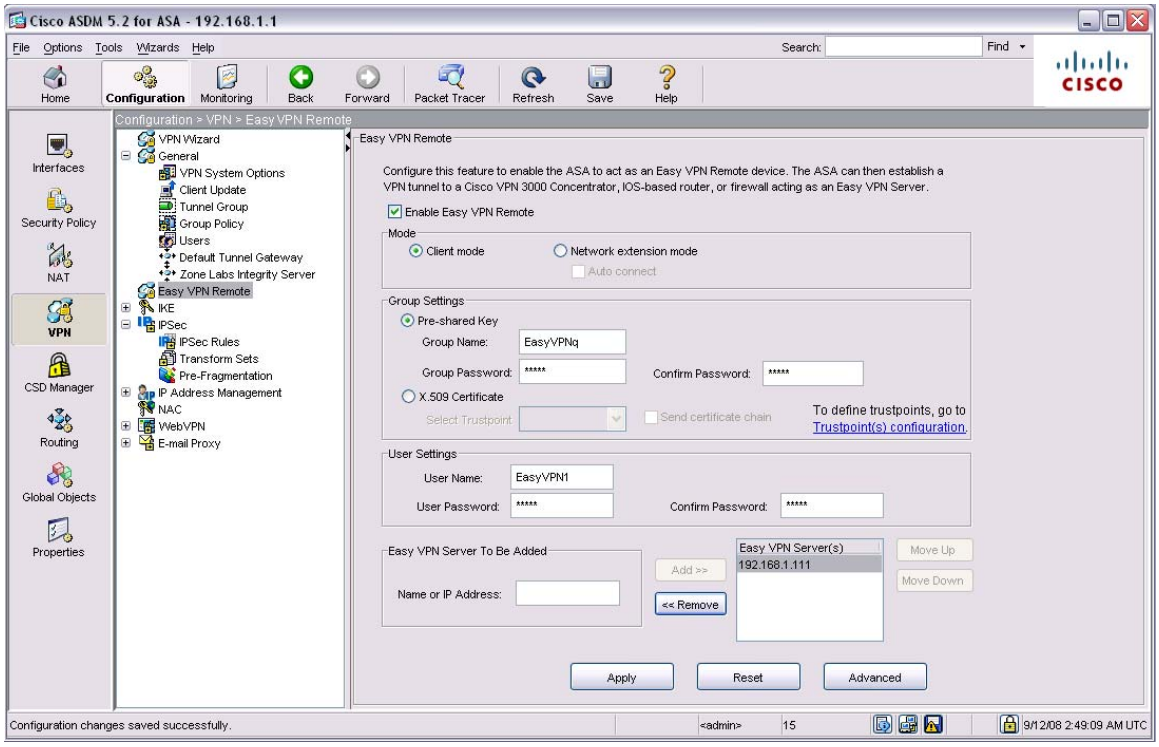
For the purpose of this lab, we will be configuring Easy VPN Remote to operate in client mode.



In the *Group Setting*, select the option for a *pre-shared key*. Specify a group name of *EasyVPN*, and a group password of *cisco*.

Under *User Settings*, specify the username and password to be used by the ASA 5505 when establishing a connection. We will be using *EasyVPN1* with a password of *cisco*.

In the last option, specify an *Easy VPN server* to connect to. In this lab we will be using *192.168.1.111*. When you are done, click the *Add* button.



That's all there is to configuring Easy VPN.

When you are done this section, make sure you uncheck the *Enable Easy VPN Remote* box.