**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.



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.



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.



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.



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.



Verify and write to flash.



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.



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



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.

🔂 Cisco ASDM 5.2 for ASA - 192.168.1.1	-	
<u>File Options Tools Wizards Help</u>	Search: Find -	1
Home Configuration Monitoring Back Forward Packet Trac	icer Refresh Save Help	sco
Device Information	Interface Status	
General License Host Name: ciscoasa.default.domain.invalid	Interface IP Address/Mask Line Link Kbp inside 192.168.1.1/24 Oup Oup 4	s
ASA Version:     7.2(2)     Device Uptime:     0d 2h 24m 35s       ASDM Version:     5.2(2)     Device Type:     ASA 5505       Firewall Mode:     Routed     Context Mode:     Single       Total Flash:     128 MB     Total Memory:     256 MB	Select an interface to view input and output Kbps	
VPN Tunnels IKE: 0 IPSec: 0 WebVPN: 0 SVC: 0	Traffic Status Connections Per Second Usage	
CPU Usage (percent) 7% 14:49:28 14:49:28 CPU Usage (percent) 100 100 100 100 100 100 100 10	1.5 0 14:49:38 ■ UDP: 0 • UDP: 0 • TCP: 0 • Outside' Interface Traffic Usage (Kbps)	
Memory         Memory         Second S	Interface is down.	
ASDM logging is disabled. To enable ASDM logging	Configure ASDM System g with informational level, click the button below. a Logging	Filters –
Device configuration loaded successfully.	<admin> 15 🐻 🖼 🙆 09/10/08 2:49</admin>	:28 PM UTC

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

	Cisco ASD	M 5.2	for ASA	- 192	.168.1.1		
File	Options	Tools	Wizards	Help			
	ổ Home	Con	<u>S</u> tartuj ⊻PN V	oVViza √izard.	rd		rd Packet Tracer
	Device Info	ormatio License	High A	vailabi	lifty and Scalability	Wizard	
	Host Nam	e:	ciscoas	a.defa	ult.domain.inva	lid	
	ASA Vers	sion:	7.2(2)		Device Uptime	e Od 3h 1	0m 15s
	ASDM Ve	rsion:	5.2(2)		Device Type:	ASA 55	05
	Firewall M	lode:	Routed		Context Mode	Single	
	Total Flash	h:	128 MB		Total Memory:	256 MB	

**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.

🖆 Cisco ASDM 5.2 for ASA - 192.168.1.1 - Startup Wizard				X	
Startup Wizard	Basic Configuration (Step	2 of 17)			
KE	Enter the host name and th (ISP) requires that your hos by the ISP as the host name	e domain name st uses DHCP, e of the ASA.	e of the ASA. If your int you may need to use th	ernet Service Provider ne device name supplied	
S ST	ASA Host Name:	ASALab			
	Domain Name:	Pod1			
	Privileged Mode (Enable) The privileged mode (e ASDM or the Command ✔ Change privileged	Password — nable) passwo I Line Interface mode (enable)	ord is required to admin (CLI). password	ister the ASA using	
	Old Password:				
TH	New Password:		****		
	Confirm New Pass	word:	*****		
	L				
			< Back Next > Fi	nish Cancel Hel	a a

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.

📴 Cisco ASDM 5.2 for AS	A - 192.168.1.1 - Startup Wiza	ard 🛛 🔀
Startup Wizard	Internet (Outside) VLAN Configu	ration (Step 4 of 17)
A TEL	Select Internet (Outside) VLAN You must specify a VLAN interfa will be asked to allocate switch p an existing VLAN interface or cre	ace which will be used to connect to Internet. Later you borts to this VLAN interface. You can either choose from eate a new VLAN interface.
1 h los	Choose a VLAN	vlan2
	◯ Create new VLAN	
and a second	Enable interfa	ce
FILTE THE	Interface Name:	outside Security Level: 0
	IP Address	
THUM	<ul> <li>Use DHCP</li> </ul>	
TTT	☑ Obtain default route	using DHCP
- 1-1-	OUse the following IP address	
A	IP Address:	255.255.255.255
	Subnet Mask:	255.255.255.255
		< Back Next > Finish Cancel Help

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.

📴 Cisco ASDM 5.2 for AS/	A - 192.168.1.1 - Startup Wizard 🛛 🛛 🛛 🕅
Startup Wizard	Business (Inside) VLAN Configuration (Step 5 of 16)
A B L	Select Business (Inside) VLAN You must specify a VLAN interface which will be used to connect to Business. Later you will be asked to allocate switch ports to this VLAN interface. You can either choose from an existing VLAN interface or create a new VLAN interface.
and the second	Choose a VLAN     Vlan1
	Create new VLAN 3
and the second	Enable interface
THE THE	Interface Name: inside Security Level: 100
	Address     Use PPPoE
THUM	O Use DHCP
T	Obtain default route using DHCP
The	O Use the following IP address
A	IP Address: 192.168.1.1
Co Un	Subnet Mask: 255.255.0
	< Back Next > Finish Cancel Help

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.

📴 Cisco ASDM 5.2 for AS/	192.168.1.1 - Startup Wizard 🛛 🛛 🔀
Startup Wizard	Home (dmz) VLAN Configuration (Step 6 of 15)
HE	Select Home (dmz) VLAN You must specify a VLAN interface which will be used to connect to Home. Later you will be asked to allocate switch ports to this VLAN interface. You can either choose from an existing VLAN interface or create a new VLAN interface.
10 4X	Choose a VLAN VLAN Interface left in the
	Create new VLAN     3     device. You must create a     new VLAN interface.)
and a second	Enable interface
THE THE	Interface Name: dmz Security Level: 50
	Use PPPoE
THUM	O Use DHCP
TIT	Obtain default route using DHCP
TITI	Use the following IP address
A	IP Address: 172.16.1.1
	Subnet Mask: 255.255.0
	< Back Next > Finish Cancel Help

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.

😼 Cisco ASDM 5.2 for AS	- 192.168.1.1 - Startup Wizard 🛛 🛛 👔
Startup Wizard	Switch Port Allocation (Step 7 of 14)
10/200	Allocate Switch Ports for your Internet (Outside) VLAN <vlan2></vlan2>
	Available Ports Allocated Ports
K VAV	Ethernet0/1 Add >> Ethernet0/0
	Ethernet0/2
1 hours	Ethernet0/3
	Ethernet0/4
	Ethernet0/5
E a m	Allocate Switch Ports for your Business (Inside) VLAN <vlan1></vlan1>
Ferting Ve	Allocated Ports
-1-1-	Ethernet0/4
	<< Remove Ethernet0/5
LINING	Ethernet0/6
	Ethernet0/7
	Allocate Switch Ports for your Home (dmz) VLAN <vlan3>          Available Ports       Add &gt;&gt;         Ethernet0/0       Add &gt;&gt;         Ethernet0/2       I         Ethernet0/4          Ethernet0/4</vlan3>
	< Back Next > Finish Cancel Help

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.

📴 Cisco ASDM 5.2 for ASA	192.168.1.1 - Startup Wizard	X
Startup Wizard	General Interface Configuration (Step 8 of 14)	
	Enable traffic between two or more interfaces with same security level Enable traffic between two or more hosts connected to the same interface   Restrict traffic   From interface:   vlan3 (dmz)   To interface:     vlan1 (inside)	
	< Back Next > Finish Cancel Hel	q

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.

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

Click the Add button.

Interface Name:	inside	~		
IP Address:		Mask:		~
Gateway IP:		Metric:	1	
Options				
100 C				
<ul> <li>None</li> </ul>				
<ul> <li>None</li> <li>Tunneled (I</li> </ul>	Jsed only for defa	ult route and metric v	will be set to	255)
None     Tunneled (I     Tracked	Jsed only for defa	ult route and metric v	vill be set to	255)
None     Tunneled (I     Tracked     TrackID:	Jsed only for defa	ult route and metric v ack IP Address/DNS	will be set to	255)
None     Tunneled (I     Tracked     Track.ID:     SLA.ID:	Jsed only for defa	uit route and metric v ack IP Address/DNS	will be set to Name: Mo	255) nitoring Option

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*.

🔁 Cisco ASDM 5.2 for AS	4 - 192.168.1.1 - Startup Wizard 🛛 🛛 🔀
Startup Wizard	DHCP Server (Step 10 of 14)
A TOTAL	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 > Properties > DHCP Services in the main ASDM window.
Stores and the	✓ Enable DHCP server on the inside interface
	DHCP Address Pool
11	Starting IP Address: 192.168.1.2 Ending IP Address: 192.168.1.33
Service In	
124	DHCP Parameters
	Enable auto-configuration
THUM	DNS Server 1: DNS Server 2:
THI	VMINS Server 1: VMINS Server 2:
T	Lease Length: secs Ping Timeout: ms
	Domain Name:
	< Back Next > Finish Cancel Help

**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*.

📴 Cisco ASDM 5.2 for AS/	A - 192.168.1.1 - Startup Wizard 🛛 🕅
Startup Wizard	Address Translation (NAT/PAT) (Step 11 of 14)
HE	Select Network Address Translation (NAT), if you want the source IP address to be chosen from the global IP address pool. Select Port Address Translation (PAT), if you want the source IP address to be the same for all outbound sessions. Select the first option, if you do not want any inside addresses to be translated.
and the	This configuration permits all traffic from the inside interface to the outside interface.
	Enable traffic through the firewall without address translation
and the second	O Use Network Address Translation (NAT)
TAT ST	Starting Global IP Address:
	Ending Global IP Address:
	Subnet Mask (optional):
THUM	● Use Port Address Translation (PAT)
TIT	<ul> <li>Use the IP address on the outside interface</li> </ul>
TTTT	O Specify an IP address
A	IP Address:
	Subnet Mask (optional):
	< Back Next > Finish Cancel Help

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.

📴 Cisco ASDM 5.2 for ASA	192.168.1.1	l - Startup W	izard		
Startup Wizard	Administrative	Access (Step	12 of 14)		
Print 1	Specify the addro HTTPS/ASDM, SS	esses of all host 3H or Telnet.	s or networks, which	are allowed to access A	ASA using
K VAV	Туре	Interface	IP Address	Mask	Add
SAV /	HTTPS/ASDM	inside	192.168.1.0	255.255.255.0	
The second se					Edit
					Delete
The Th					
- 6	🗹 Enable HTTP	server for HTTF	S/ASDM access		
	Disabling HT	IP server will pr	event HTTPS/ASDM a	ccess to this ASA.	
	🔽 Enable ASDN	A history metrics			
			< Back	lext > Finish Car	cel Help

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

5	Cisco ASD	M 5.2	for ASA - '	192.16	8.1.1			
File	Options	<u>T</u> ools	<u>W</u> izards <u>H</u>	lelp		_		
		Cor	nmand Line In	terface		b		- 🔿
	Home	Pac	ket Tracer			ack	Forward	Packet Tracer
Г	Device Inf	Pi <u>n</u> g	y					
	General	Tra	ceroute					
	General	File	Management					1
	Host Nam	Upg	grade Softwa	re				
	ASA Ver:	Uple	oad ASDM As	sistant C	}uide…	he:	0d 5h 1m 15	s
	ASDM Ve	Sys	stem <u>R</u> eload			k	ASA 5505	
	Firewall N	<u>A</u> SI	DM Java Cons	ole		le:	Single	
	Total Flash	h:	128 MB	1	lotal Memo	ry:	256 MB	

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

Command Line	Interface			
-Command Line Inter	face			
Type a command to mark. For commands the command and so Configuration to Flas	be sent directly to the dev s that would prompt for co end it to the device. To ma sh menu option to save the	ice. For comm infirmation, add ke the change: configuration	and help, type a command followed by d an appropriate noconfirm option as pa s permanent, use the File > Save Runnir to flash.	a question rameter to ng
<ul> <li>Single Line</li> </ul>	O Multiple Line		Enable context sensitive help (?)	
sho run				~
Response:				
: Saved : ASA Version 7.	.2(2)			
hostname ASALs	аb			
domain-name Po enchle nessuo	odl od 2KROphNIdi 2KVO	lengrente	a	
names	ta zhrqiibwiai.zhio	, encrypce.	-	
1				
interface Vlar	11			
security-leve	≗ ⊳1 100			
ip address 19	92.168.1.1 255.255	.255.0		
1				
interfore Vier	n?			
	Send		Clear Response	
	Clos	:e	Help	

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.

🗟 Cisco ASDN	15.2 for AS	A - 192.168	3.1.1								
ile Options ]	ools <u>W</u> izards	s <u>H</u> elp					Search:			Find 👻	
्री Home	Configuration	Monitorin	g Back	Forward	Racket Trace	Refresh		<b>?</b> Help			cisco
Device Infor	mation					Interface Stat	tus				
General Li	cense					Interface	IP Addre	ess/Mask	Line	Link	Kbps
Encryption	3DES-AE	s	Inside Hosts:	10		dmz	no ip ad	ldress	😑 down	😑 down	0
Enilouper	Dicabled		VDN Deers	40		inside	192.168	3.1.1/24	🖸 up	🖸 up	4
VLANs:	3, DMZ R	, testricted	Max Physical	Biesblad		outside	192.168	3.10.2/24	📟 down	😑 down	0
License:	Base		Entrainingenso.	Disabled							
WebVPN Pe	eers: 2		Trunk Ports:	0		Select an inte	rface to view	/ input and ou	utput Kbps		
VPN Tunnel	s					Traffic Statu	s				
IKE: 0	IPSec:	0 V	VebVPN: 0	SVC:	0	Connections	Per Second I	Usage			
22:42:39 Memory 73M9 22:42:39	19:21:39 Memory Usage 256 128 0 19:21:39	19.23 (MB) 19.23	:19 1	9:24:59	22:42:29	'outside' Inter	rface Traffic L ne 'outside' Int s:	Jsage (Kbps) Inter erface Traffi	rface is down. c Usage (Kbps), utput Kbps:	refreshed e	very 10 secon
Latest AS	UM Syslog M	ASDM	logging is disable	ed. To enable	ASDM logging v	vith informational	level, click th	e button belo	w.	figure ASDM	<u>Syslog Filters</u> -
						<admin></admin>	15	6	3 🔼	9/11/0	18 10:42:39 PM

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.

Options Ic	ools <u>Wi</u> zards	Help										Search		Find +	
Home	Configuration	Monitoring Back	Forward	Packet Tra	cer Refresh	Save Help									CISCO
	Configuratio	on > Interfaces													
	Interfaces	Switch Ports													
erfaces	Name	Switch Ports	Enabled	Security	P Address	Subnet Mask	Restrict Tratlic from	VLAN	Management	MTU	Active MAC Address	Standby MAC Address	Description		441
G.	inside	Ethernet0/2, Ethernet0/3, Ethe	. Yes	100	192.168.1.1	255,255,255.0	Tractic now	vtant	No	1,500	MAG Address	MANC ACCRESS			400
rity Policy	outside	Ethernet0/0	Ves	0	192 168 10.2	255 255 255 0		vlen2	No	1,500					EoR
и.	dmz	Ethernet0/1	Yes	50	0		vlant (inside)	vfan3	No	1,500					Delete
3															
PN															
-															
anager															
rager S															
anager Eng															
anagar Sing															
tanager															
Anager															
kanager Ling Objects Pettes	c						8								2
Manager Ading Coljects	¢.]						8								3
Manager 23 20 20 20 20 20 20 20 20 20 20 20 20 20	<	traffic between two or more inte	rfaces which	ch are config	ured with same se e interface	curty levels	- 10 -								6
Annager Atrager Atrag (Objects Cojects	4. V Enable V Enable	Staffic between two or more inte Staffic between two or more ince	rfaces which	ch are config id to the same	ured with same se a interface	curty levels	, til Addity :		Reset	1					4

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.

🔤 Cisco ASDM	5.2 for ASA - 192	2.168.1.1							_ 0
Eile Options Tu Con Home	Configuration Mo	itoring Back	O Forward	Packet Tracer Refe	Search:	? Help		Find -	cisco
_	Configuration > In	terfaces	_	_	_	_	_		_
Interfaces	Interfaces Swith Switch Port	ch Ports Enabled	Associated	Associated	Mode	Protected	Dunlex	Speed	
C.		Lindologi	VLANs	Interface Names	mode	110100104	Dapies	opeca	Edit
<u> </u>	EthernetU/U	Yes	2	outside	Access	NO	auto	auto	-
Security Policy	EthernetU/1	Yes	3	amz	Access	NO	auto	auto	_
310	Ethernet0/2	Yes	1	inside	Access	NO	auto	auto	_
100	Ethernet0/3	Vec	4	inside	Access	No	auto	auto	_
NAT	Ethernet0/4	Vec	4	inside	Access	No	auto	auto	-
C <sup>2</sup>	Ethernet0/S	Vec	4	inside	Access	No	auto	auto	_
VPN	Ethernet0/7	Ves	4	inside	Access	No	auto	auto	-
Routing Routing Global Objects Properties									
				Apply	Reset				
							1		

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.

🔁 Cisco ASDM 5	5.2 for AS	A - 192.168.1.1									_ 🗆 🛛
File Options Too	ols <u>W</u> izard	s <u>H</u> elp						Search:		Find 👻	1.1
Home C	onfiguratic	Monitoring	O Back	Forward P	acket Tracer Ref	Yesh Save	<b>?</b> Help				CISCO
	Configurat	ion > NAT								1	
	🔂 Add 🗸	Edit <u> </u> Delet	e ↑ ↓	🔏 🛍 💼	👻 🔍 Find 🔛 F	Rule Diagram 📿 Pack	et Trace			Addresses Serv	rices Global Pools
Interfaces	Filter:Se	lect 💌						Filter Clear	Rule Query	💠 Add 👻 🎬 Ed	t 🔟 Delete 🔍 Fir
<u>A</u>	No	Type		R	Real		Translated			Type: 🏈 All	~
Security Policy		1160	5	Source	Destination	Interface	Address	DNS Rev	write Max TCP	Name	
210	-inside	111 Dynamic	i anv		anv	outside	5 outside	No	Unlimited	anv	ecis
NAT		11 C J Hanno								inside-r	network/24
07											
VPN											
CSD Manager											
120											
Routing											
<u>8</u>											
Global Objects											
Properties	<			- Ш					>		
	Rule Flov	v Diagram			inside 🥂	outside	La		×		
				any							
				an an	iy	outside	Louity				
										<u>p</u>	
	Enable 1	rattic through the tir	ewall withou	a address trans	aation						
						Apply	Reset				
							<admin></admin>	15	🕟 🛃 🗗	<b>)</b> 🙆 09.	10/08 4:43:45 PM UTC

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.

📴 Edit Dyna	amic NAT Rule	×
Real Addre	355	
Interface	: inside	
IP Addres	ss: 0.0.0.0	
Netmask:	0.0.0.0	
Dynamic Tr	ranslation	
Interface	: outside 💌	
🔂 Add	📷 Edit 💼 Delete	
Select	1 Addresses Pool	
NAT Optio	ns	
ОК	Cancel Help	

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*.

둴 Edit Dynam	nic NAT Rule	×
_Real Address		1
Interface:	inside	
IP Address:	192.168.1.0	
Netmask:	255.255.255.0	
∟ ⊢Dynamic Tran	slation	1
Interface: c	utside	
🗣 Add 🍯	🕈 Edit  💼 Delete	
Select F	Pool ID Addresses Pool	
1	web outside	
NAT Options	···	
ок	Cancel Help	

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.

🔂 Command Line Interface
Command Line Interface Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Confirm and to Filerborneus under to come the confirmation to face the followed by the followed by the confirmation to the send the confirmation to the confirmation to the send to the device. To make the changes permanent, use the File > Save Running
Command Command
sho run
Response: mtu inside 1500 mtu outside 1500 mtu dmz 1500 icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-522.bin asdm history enable
global (outside) 1 interface nat (inside) 1 92.168.1.0 255.255.255.0
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:0 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0: timeout uauth 0:05:00 absolute http server enable to server enable Send Clear Response
Close Help

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.

Interface:	nside					Addresses Services Global
IP Address:	192.168.1.0	¥	Filte	r Clear Rul	e Query	💠 Add 👻 🛒 Edit  👚 Delete
Netmask:	255.255.255.0	~				Type: 🍳 All
-Dynamic Trans	lation		ISS	DNS Rewrite	Max TCP	Name
Interface: ou	.tside	N	102.169	No	Unlimited	Address Objects
			- 132.100	140	Orininicou	inside-network/24
💠 Add 🙋	Edit Delete		_			
Select P	ol ID Addresse:	s Pool				
NAT Options.		j Edit Global Address Po Interface: outside Pool ID: 1 IP Addresses to Add	pol	1	Address	es Pool
NAT Options.		J Edit Global Address Printerface: outside Pool ID: 1 P Addresses to Add Range Starting IP Address:	pol	]	Address	es Pool
NAT Options.		J Edit Global Address Printerface: outside Pool ID: 1 IP Addresses to Add Range Starting IP Address: Ending IP Address:	Jool		Address	es Pool
NAT Options.		Edit Global Address Printerface: outside Pool ID: 1 IP Addresses to Add Range Starting IP Address: Ending IP Address: Netmask (optional):		Add >>	Address Address	es Pool 68.10.1 - 192.168.10.10
NAT Options. OK		Edit Global Address Printerface: outside     Pool ID: 1     P Addresses to Add     Range     Starting IP Address:     Ending IP Address:     Netmask (optional):     O Port Address Translatio	n (PAT)	Add >>	Address 192.1	es Pool
NAT Options. OK		J Edit Global Address Pu Interface: outside Pool ID: 1 IP Addresses to Add Range Starting IP Address: Ending IP Address: Netmask (optional): P Address Translatio IP Address:	n (PAT)	Add >> << Delete	Address	es Pool
NAT Options.		J Edit Global Address Ponterface: outside Pool ID: 1 P Addresses to Add T Addresses to Add T Address: Ending IP Address: Netmask (optional): P Address: P Address: Netmask (optional): P Address: P Addr	n (PAT)	Add >> << Delete	Address	es Pool ( 68.10.1 - 192.168.10.10

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.

Command Line Interface
Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.
Single Line     Muttiple Line     Enable context sensitive help (?)
sho run
Response'
pageing asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500 icmp upreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
asdm history enable
global (outside) 1 192.168.10.1-192.168.10.10 netmask 255.255.255.0 nat (inside) 1 192.168.1.0 255.255.255.0
timeout x1ate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:0 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0: timeout uauth 0:05:00 absolute
Close Help

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.

Cisco ASDM:	Packet Tracer	
Select the pack	et type and supply the packet parameters. Click Start to trace the packet.	
Interface :	inside Packet Type:  TCP UDP ICMP	90
Source IP:	192.168.1.3 Destination IP: 72.14.205.99	Q Start
Source Port :	80 Destination Port : 80 💌	Clear
Show anima	tion	
Route	Access list NAT Lookup 005	Outside
Lookup	Lookup 1	1 Access List 1
	Close 7 Help	

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 <u>www.google.com</u>). 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.

🔂 Cisco ASDM	5.2 for ASA - 192.168.1.1
<u>File</u> Options <u>T</u> o	ools <u>Wi</u> zards <u>H</u> elp
් Home	Configuration Monitoring Back Forward Packet Tracer
	Configuration > Security Policy > Access Rules
	Access Rules AAA Rules Filter Rules Service Policy Rules
Interfaces	🗣 Add 🗸 📷 Edit 🏢 Delete 🎓 🗲 🛛 👗 🛍 🏙 🤟 🔍 Find
A	I 🖶 Add Access Rule
Security Policy	Insert Destination
	Insert After ules)
68	🔷 Any less secure ne
NAT	2 🏟 any 🏟 any

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* 

Interface and Action Interface: outside Direction: 🎺 incoming	Action: 🖌 Permit
Source Type: 🏟 any	Destination Type: P Address V IP Address: 172.16.1.100 V
Protocol: tcp V Source Port Service: any V Group: Rule Flow Diagram	Destination Port
Options Logging: Enable Systog Level: Informat	ional 🔽 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.

Cisco ASDM 5	5.2 for ASA	192.16	8.1.1												_ 🗆 🛛
File Options Too	ols <u>W</u> izards	Help									Searcl	h:		Find 👻	1.1
Home C	ogg Configuration	Monitorin	ig Back	Forward	I Packet Tr	racer	<b>R</b> efresh	<b>I</b> Save	<b>?</b> Help						cisco
Home C Interfaces Security Policy WPN CSD Manager CSD Manager CSD Manager CSD Manager CSD Manager Properties	Configuration Configuration Access Rule Riter:Selec No Selec No 	Monton: 1 Securi 2 Edt 1 2 Enabled 1 2 (2 implicit of ( 6 (2 implicit of ( 6 (2 implicit of ( 7 ( 7 ( 7 ( 7 ( 7 ( 7 ( 7 ( 7	g Back y Policy - Acou des Fitter Rules Source coorning rules any any any any any any any any	Forward sees Rules es Service 5 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	i         Packet Ti           Policy Rules	Find     Find     Cure net	Refresh	save ram ☐ Show ✓ Per ③ Der ④ Der ④ Der	leip	Packet Trac Iging Time	e Description Implicit rule Implicit rule Implicit rule	ear Rule Quer	AA Y Typ Na less x	ddresses Servic Add - Edit Constant See All See All See Constant See Constant Se	5 Time Ranges.
Configuration change	es saved succ	essfully.					Apply	Rese	t	Adv <adm< td=""><td>/anced</td><td>6</td><td></td><td>9/1</td><td>1/08 7:17:09 PM UTC</td></adm<>	/anced	6		9/1	1/08 7:17:09 PM UTC
									_						

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.

🖻 Command Line Interface
Command Line Interface Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.
Command     Single Line Multiple Line Enable context sensitive help (?)     sho access-list
Response: Result of the command: "sho access-list" access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list outside_access_in; 2 elements access-list outside_access_in line 1 extended permit tcp any host 172.16.1.1( access-list outside_access_in line 2 extended permit tcp any host 172.16.1.1(

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* 

📑 Add Parameters for	r Websense URL Filtering 🛛 🔀
Interface:	inside
IP Address:	192.168.1.200 Timeout: 30 seconds
Protocol	
⊙ TCP 1	O TCP 4 O UDP 4
TCP Connections:	5
ок	Cancel Help

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

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

Cisco ASDM	5.2 for ASA	- 192.168.1	.1										_ 🗆 🖂
File Options To	ols <u>W</u> izards	Help								Search:		Find 🔹	1.1
	00		0	0		Q		2					CISCO
Home	Configuration	Monitoring	Back	Forward	Packet Tracer	Refresh	Save	Help					cisco
	Configuratio	n > Security P	olicy > Filter	r Rules		_	_		_	_	_		
	Access Rul	es AAA Rules	Filter Rules	Service Polic	y Rules							Addresses Serv	ices Time Ranges
Interfaces	🔂 Add 🗸	Edit D	elete 🐰 I		ind 🔛 Rule Di	agram 🗬 Pac	ket Trace					💠 Add 👻 🌃 Edi	t 🏢 Delete 🔍 Fir
<u>A</u>	Filter:Sele	ect	~							Filter Clear	Rule Query	Type: 🏈 All	~
Security Policy	No	Source		Destination	0	Service	Action		Options			Name	
31.												P Address Obj	ects
NAT												- 🖪 172.16.	1.100
<b>1</b>												inside-r	network/24
See												outside	-network/24
VPIN													
6													
CSD Manager													
120													
Routing													
<b>A</b>													
Global Objects													
Properties													
Toponico	<										>		
	Rule Flow	Diagram									×		
				-⊢ 4					- 🚅				
			Source A	Address	Service	Eiter Action		D	estination Address				
						- The Action							
						Apply	Res	set	Advanced.				
									<admin></admin>	15	li 😼 🛃	9/	11/08 7:24:59 PM UTC

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* 

Source			Destination		
IP Address:	192.168.10.0	<b>.</b>	IP Address:	192.168.1.0	~
Netmask:	255.255.255.0	~	Netmask:	255.255.255.0	~
		Fitter	ActiveX ====		
ActiveX Filteri	ng Option				

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.

💁 Command Line	Interface				×
-Command Line Inter	face				
Type a command to mark. For commands the command and se Configuration to Flas ┌Command	be sent directly to the dev s that would prompt for co and it to the device. To mal h menu option to save the	ice. For comman nfirmation, add a ke the changes p configuration to	3 help, type a comm n appropriate nocon ermanent, use the F flash.	and followed by a qua ifirm option as parame file > Save Running	estion eter to
📀 Single Line	O Multiple Line		Enable context se	nsitive help (?)	
sho run   be url					<b>~</b>
Response:					
url-server (in filter activex http server en http 192.168.1 no snmp-server	side) vendor webs : 80 192.168.10.0 2 able .0 255.255.255.0 : · location	ense host 19 255.255.255.	2.168.1.200 ti 0 192.168.1.0	imeout 30 protoc 255.255.255.0	201
snmp-server en telnet timeout ssh timeout 5 console timeou	able traps snmp av . 5 t 0	athenticatio	n linkup linko	down coldstart	
dhcpd auto_con !	fig outside				
dhcpd address dhcpd enable i	192.168.1.2-192.10 nside	58.1.33 insi	de		
۱ ۲	Ш				>
	Send		Clear Response	e	
	Clos	•	Help		

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

Command Line Interface	
Command Line Interface	
Command Line interface	- Four-second labola dama a second della constitue
mark. For command to be send during device mark. For commands that would prompt for con the command and send it to the device. To make Configuration to Flash menu option to save the o	e. For command negr, type a command followed by a question firmation, add an appropriate noconfirm option as parameter to e the changes permanent, use the File > Save Running configuration to flash.
Command	
Single Line O Multiple Line	Enable context sensitive help (?)
sho url-server stat	~
Response:	
Result of the command: "sho url-	server stat"
Global Statistics:	
URLs total/allowed/denied	0/0/0
URLs allowed by cache/server	0/0
URLs denied by cache/server	0/0
HTTPSs total/allowed/denied	0/0/0
HTTPSs allowed by cache/server	0/0
HTTPSs denied by cache/server	0/0
FTPs total/allowed/denied	0/0/0
FTPs allowed by cache/server	0/0
FTPs denied by cache/server	0/0
Requests dropped	0
Server timeouts/retries	0/0
Processed rate average 60s/300s	0/0 requests/second
Denied rote overege file/300c	0/0 remissive/second
Send	Clear Response
Class	

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:

- 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.

🖬 VPN Wizard		X
VPN Wizard	Remote Site Peer (Step 2 of 6)	
Branch	Configure the IP address of the peer device, authentication method and the tunnel group for thi site-to-site tunnel. Peer IP Address: 192.168.10.55	s
	Authentication Method	1
Home	• Pre-shared key	
Corporate	Pre-Shared Key: cisco	
Cather to	○ Certificate	
The second second	Certificate Signing Algorithm: rsa-sig	-
	Trustpoint Name:	<u>e</u>
274UIII	Challenge/response authentication (CRACK)	
TIT	Tunnel Group	
-6-	For site-to-site connections with pre-shared key authentication, the tunnel group name mus be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.	t
	Tunnel Group Name: 192,168.10.55	
	Sack Next > Finish Cancel	Help

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.

🖬 VPN Wizard		×	
VPN Wizard	IKE Policy (Step 3 of 6) Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.		
Corporate Network	Encryption: Authentication: DH Group:	3DES v MD5 v	
		< Back Next > Finish Cancel Help	

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.

🔁 VPN Wizard	X
VPN Wizard	IPSec Encryption and Authentication (Step 4 of 6)
VPN Wizard	IPSec Encryption and Authentication (Step 4 of 6)         Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.         Encryption:       3DES         Authentication:       MD5
	Rack Nexts Finish Cancel Hein

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.

📑 VPN Wizar d	
VPN Wizard	Hosts and Networks (Step 5 of 6)
Branch ISP Home Corporate Network	An IPSec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPSec tunnel.  Host/Network Interface: outside Source Destination
c.esta	Type: 🙀 IP Address 💌 Type: 🙀 IP Address 💌
	IP Address:       192.168.10.0       IP Address:       192.168.11.0       III         Netmask:       255.255.255.0       IIII       Netmask:       255.255.255.0
	2.158:10.0/24
	Exempt ASA side host/hetwork from address translation
	< Back Next > Finish Cancel Help

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.

🗟 Command Line Interface 🛛 🛛 🔀
Command Line Interface Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for continmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash meru option to save the configuration to flash.
Command  Constant Interview Provide Line  Context sensitive help (?)  Sho run
Response.
crypto map outside_map 20 set pfs crypto map outside_map 20 set peer 192.168.10.55 crypto map outside_map 20 set transform=set ESP=3DES=MD5 crypto map outside_map 40 match address outside_40_cryptomap crypto map outside_map 40 set pfs crypto map outside_map 40 set peer 192.168.10.55 crypto map outside_map 40 set transform=set ESP=3DES=MD5
crypto hap outside_hap interface outside crypto isakmp enable outside crypto isakmp policy 10 authentication pre=share encryption 3des hash md5 group 2 lifetime 86400
tunnel-group 192.168.10.55 type 1psec-121 tunnel-group 192.168.10.55 ipsec-attributes pre-shared-key * * * * * * * * * * * * * * * * * * *
Close Help

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.

📴 VPN Wizard			
VPN Wizard	VPN Tunnel Type (Step 1 of)		
Brandh Frank Frank Home	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.		
Corporate Network	VPN Tunnel Type: Site-to-Site VPN		
CONT - ENG	Site-to-Site		
	Remote Access		
6.2-	VPN Tunnel Interface:		
	Enable inbound IPSec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.		
	< Back Next > Finish Cancel Help		

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

📴 VPN Wizard		
VPN Wizard	VPN Client Authentication Method	and Tunnel Group Name (Step 3 of)
Branch	The ASA allows you to group remot parameters and client attributes con method and tunnel group for this rer device and the remote client.	e access tunnel users based on common connection igured in the subsequent screens. Configure authentication lote connection. Use the same tunnel group name for the
	Authentication Method	
Home	Pre-shared key	
Corporate	Pre-Shared Key: cisco	
centre	O Certificate	
J. J. Mark	Certificate Signing Algorithm	rsa-sig
	Trustpoint Name:	
CTUUM III	O Challenge/response authent	cation (CRACK)
TTT	Tunnel Group	
	Tunnel Group Name: Remote V	PN
		< Back Next > Finish Cancel Help

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*.

📴 VPN Wizard	
VPN Wizard	Client Authentication (Step 4 of)
Brandh Frandh Frandh Frandh Home Comporte	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, use Configuration > Properties > AAA Setup category in the main ASDM window.
Network	Authenticate using the local user database     Authenticate using an AAA server group     AAA Server Group Name:     New
	< Back Next > Finish Cancel Help

**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.

🔁 VPN Wizard		×
VPN Wizard	User Accounts (Step 5 of 11)	
Branch	Enter a new username/password into the entries in the database or to remove the > Device Administration > User Account	he user authentication database. To edit existing m from the database, go to Configuration > Properties ts in the main ASDM window.
Homo	User to Be Added	
Corporate Network	Username:	vpnuser1
	Password (optional):	Add >> Delete
6	Confirm Password (optional):	
		<back next=""> Finish Cancel Help</back>

**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.

VPN Wizard			$\overline{\mathbf{X}}$
VPN Wizard Branch SP Home	Address Pool (Step 6 of 11)	sses to be used for assigning dynam	iic IP addresses to remote VPN
Corporato Network	Name: Starting IP Address: Ending IP Address: Subnet Mask:	RemoteVPNPool       192.168.2.1       192.168.2.20       255.255.255.0       Cancel	New
		< Back Next >	Finish Cancel Help

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.

🚰 VPN Wizard		$\overline{\mathbf{X}}$		
VPN Wizard	Attributes Pushed to Client (Optional) (	Step 7 of 11)		
Branch	Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.			
Corporate }	Tunnel Group:	RemoteVPN		
Network	Primary DNS Server:	192.168.1.125		
- Alle	Secondary DNS Server:	192.168.1.126		
The	Primary WINS Server:	192.168.1.127		
TH	Secondary WINS Server:	192.168.1.128		
	Default Domain Name:	Pod1		
		< Back Next > Finish Cancel Help		

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* 

🚰 VPN Wizard			
VPN Wizard	IKE Policy (Step 8 of 11)		
Branch Branch ISP Home	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.		
Corporate Network	Encryption: 3DES		
	Authentication: MD5		
-6			
	< Back Next > Finish Cancel Help		
🔄 VPN Wizard			
VPN Wizard	IPSec Encryption and Authentication (Step 9 of 11)		
Branch	Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.		
Corporate Network			
THE THE	Encryption: JUES		
	Authentication: MD5		
0.A-			

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.

< Back Next > Finish Cancel Help

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.

📴 VPN Wizard		
VPN Wizard	Address Translation Exemption and Split Tunneling (Optional)	(Step 10 of 11)
Brandh (SP) Home	Network Address Translation (NAT) is used to hide the internal netw can make exceptions to NAT to expose the entire or part of the inter remote users protected by VPN. To expose the entire network behind the most secure interface to re leave the selection list blank.	vork from outside users. You nal network to authenticated mote VPN users without NAT,
Corporate Network		Selected Hosts/Networks:
	Interface: inside Source Type: IP Address IP Address: 192.168.1.0 IN Netmask: 255.255.255.0 IN Enable split tunneling to let remote users have simultaneous end resources defined above, and unencrypted access to the interf	192.168.1.0/24

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.

🔂 Cisco ASDM 5.2 for ASA - 192.168.1.1		🛛 🔀
File Options Tools Wizards Help	Search:	Find +
Home Configuration Monitoring Back Fo	ward Packet Tracer Retresh Save Help	CISCO
Configuration > VFN > Easy VFN Remote         Interfaces         Interfaces         Security Policy         NAT         Image: CSD Manager         CSD Manager         CSD Manager         CSD Manager         Colobal Objects         Image: Properties	Easy VPN Remote Configure this feature to enable the ASA to act as an Easy VPN Remote device. The ASA can then establish a VPN turnel to a Close VPN 3000 Concentrator, IOS-based router, or firewall acting as an Easy VPN Server.	
Configuration changes saved successfully.	<admin> 15 😡 🖼</admin>	9/12/08 2:35:19 AM UTC

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.

🖾 Cisco ASDM 5.2 for ASA - 192.168.1.1				
Elle Options Tools Witzards Help Search Find •				
Hone Configuration Montpring Back Forward Packet Tracer Refresh Save Help	ISCO			
Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN > Easy VPN Remote         Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN > Easy VPN Remote         Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN > Easy VPN Remote         Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN > Easy VPN Remote         Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN > Easy VPN Remote         Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN > Easy VPN Remote         Image: Configuration = VPN > Easy VPN Remote       Configuration = VPN Package         Image: VPN Remote       Image: VPN Remote         Image: VPN Remote       Configuration = VPN Package         Image: VPN Remote       Image: VPN Remote         Image: VPN Remote       Configuration = VPN Package         Image: VPN Remote       Image: VPN Remote         Image: VPN Remote       Configuration = VPN Package         Image: VPN Remote       Image: VPN Remote         Image: VPN Remote       Configuration = VPN Package         Image: VPN Remote       Image: VPN Remote         Image: VPN				
Configuration changes saved successfully. 4admin> 15 🔯 🛃 🔊 😭 sh1206 2:43:29 AM UTC				

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.

🖾 Cisco ASDM 5.2 for ASA - 192.168.1.1		_ 🗆 🔀
File Options Tools Wizards Help Search:	Find 👻	deale
Home Configuration Monitoring Back Forward Packet Tracer Refresh Save Help		cisco
Configuration > VPN > Easy VPN Remote         Interfaces         Interfac	A then establish a y VPN Server.	
Configuration changes saved successfully. <a href="https://www.saved-successfully.com"></a> 15	💿 🛃 🔂 🔒 9/12/0	08 2:49:09 AM UTC

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.