Configuring a Cisco ASA 5505

December 2008

Rob Denney

Contents

Introduction

"More robust and flexible than the Cisco PIX Firewall, the Cisco ASA 5500 Series Adaptive Security Appliances are purpose-built security solutions … A core component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers both IPsec and Secure Socket Layer (SSL) VPN connectivity." [(1)] The Cisco ASA 5500 Series device offers advanced firewall, virtual private networking, content security, and intrusion detection in a single device.

This paper will be focusing on the Cisco ASA 5505 series adaptive security appliance (with base license) and its incorporation into a small business or Home Network. Specifically, it will look at the initial configuration of network address translation and access policies, configuring VLANs and ports, and device administration. It will also look at the configuration of more advanced features such as a basic AAA server in Windows 2008 and its configuration in the device, TCP options, anti-spoofing, and service policies to do such things as limiting the transfer speed of an interface. A central focus of this paper will be on implementing a demilitarized zone. All examples and screenshots were performed using ASDM version 5.2 and ASA version 7.2.

Overview of Device Features

Differences between Base License and Security Plus License

The 5500 series comes in a variety of models but we are going to be focusing on the 5505 model, released in 2006. The 5505 model comes in two separate licenses. These licenses are the base and the security plus. Both offer 150 megabits per second throughput, a maximum of 25 SSL VPN user sessions, and a maximum encrypted VPN throughput of 100 megabits per second. However, the security plus license has additional features. For example, it supports up to 25,000 maximum firewall connections whereas the base license only supports a maximum of 10,000. It also supports a maximum of 25 site-to-site and remote access VPN sessions and the base license supports a maximum of 10. It should be noted that both licenses initially only support two VPN connections [(2)]. The security plus license also allows for a maximum of 20 virtual interfaces, commonly referred to as VLANs, with trunking enabled, and the base license supports a maximum of three. Unfortunately, neither of the licenses supports intrusion prevention, content security (which includes antivirus, anti spyware, and file blocking), or VPN clustering and load balancing.

A major difference between the two licenses is that the base license does not allow traffic to be forwarded from one VLAN to another; this restriction is removed in the security plus license. However, the base license does allow that particular VLAN to respond to requests. Another way of explaining this restriction is that there are two normal zones and one restricted zone that can only communicate with one of the other zones [(2)]. This can potentially create problems when trying to implement a demilitarized zone (also known as a DMZ) as will be discussed in a later section.

This device also implements URL Filtering, Secure Desktop, IP Auditing, and can use certificates for identification.

Initial configuration

The initial configuration of the device is rather straightforward. An easy method for accessing the configuration page is by opening a web browser and pointing it to 192.168.1.1. This is the device's default internal address. It will initially ask you for a username and password. There is no username or password. Successful authentication will take you to a web page were you have two options. The first option is to go on the Cisco ASDM as a local application. This option downloads the ASDM Software and installs it, allowing you to access it from the desktop and also manage multiple Security Appliances. The second option is to run the ASDM as a java applet. The startup wizard can be run from this page or by entering the ASDM itself.

Startup Wizard

The startup wizard consists of thirteen steps:

Step 1

Asks if you would like to modify an existing configuration or if you would like to reset the configuration to factory defaults.

Step 2

Asks you to enter the ASA host name as well as domain name; it allows you to enable a privileged mode password which is then required to administer the device using the ASDM or command line interface. For this example, the host name is 'ciscoasa' and the domain name is 'house.local'.

Step 3

Allows an auto update server to be enabled. This is disabled for the following examples.

Step 4

Configures the Internet, or 'Outside', VLAN configuration. It offers the choice of which VLAN will be used to connect to the Internet, allows you to name the interface, set the security level (which should be zero), and allows you to specify how to obtain an IP address. These examples use DHCP to obtain an IP address, but for ease of explanation, the IP will be 71.57.38.231 or 68.60.231.174 (depending on the image).

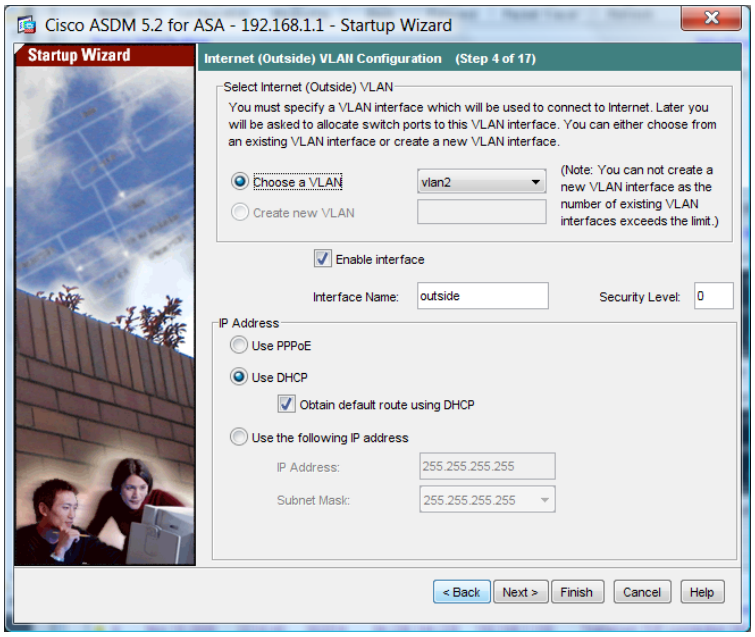

Figure 1 – Step 4 of the Startup Wizard

Step 5

Allows you to configure the same options as in Step 4, though this time they are for the business, or 'Inside', VLAN. These examples use an internal IP range of 192.168.1.0 and a subnet mask of 255.255.255.0. The device has an inside IP address of 192.168.1.1. The security level for this interface is 100.

Step 6

Allows you to configure same options as steps four and five. However, this time they are for a home, or 'DMZ', VLAN configuration. The DMZ in the following examples will be 192.168.10.0 with a subnet mask of 255.255.255.0 with the device having an IP address of a 192.168.10.1. The security level for this interface is 50.

Step 7

Allows you to configure switch port allocation. This lets you choose which ports are allocated to what VLAN.

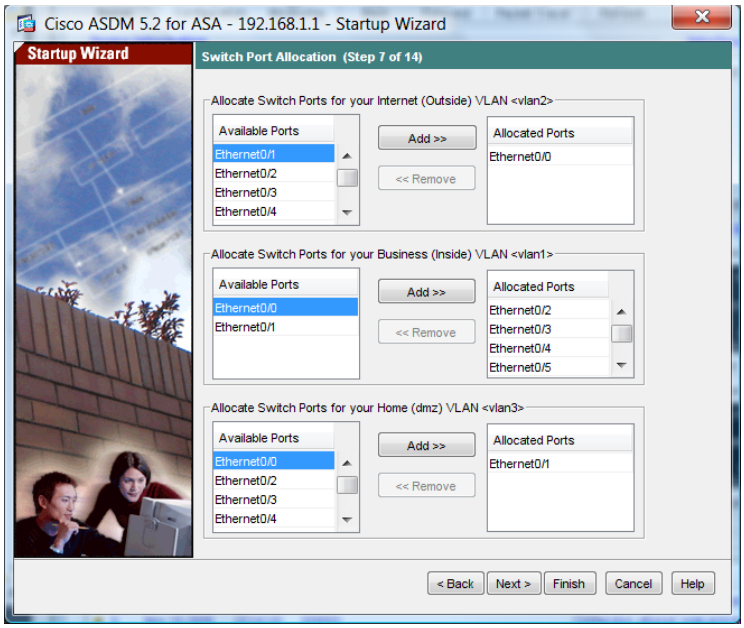

Figure 2 – Step 7 of the Startup Wizard

Step 8

Gives you two options. First option is to enable traffic between two or more interfaces with the same security level:

> By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same security interfaces provides the following benefits:
>
> - You can configure more than 101 communicating interfaces.
>
> If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).
>
> - You want traffic to flow freely between all same security interfaces without access lists. (3)

The second option is to enable traffic between two or more hosts connected to the same interface. This enables traffic to enter and exit the same interface (4). As mentioned earlier, the base license forces traffic to be restricted from one VLAN to another VLAN. For initial configuration, just make sure that you do not restrict traffic from the inside VLAN to the outside VLAN. Different configurations of this option will be discussed in the DMZ section.

Step 9

Allows you to edit the static route table.

Step 10

Allows you to enable and configure a DHCP server for the inside network. This device was configured to be a DHCP server with an address pool starting at 192.168.1.2 and ending at 192.168.1.30.

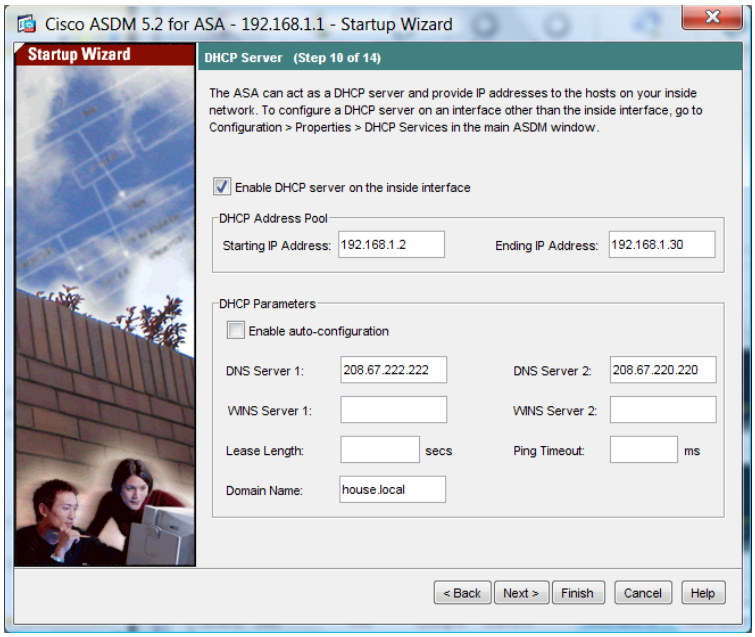

Figure 3 – Step 10 of the Startup Wizard

Step 11

Allows you to begin configuration of address translation using network address translation (NAT) or port address translation (PAT). There is also an option to disable address translation. If an internal client wishes to access the internet when using network address translation, its internal address is mapped to an external address owned by the organization. The range of valid IP addresses is designated at this step. However, if you do not own a range of IP addresses you will want to use port address translation. This functions similar to as network address translation. Instead of mapping an internal client's address to an external address selected from a pool, the device will map the connection to a specific port using the IP address on the outside interface.

Step 12

Configures administrative access to the device. It should be noted that if you disable the HTTP server, you will not be able to access the device using HTTPS or the ASDM.

Step 13

Used for Easy VPN remote configuration.

Once you've finished running the startup wizard, the commands will be sent to the device. If at a later point you wish to change the device access configuration, you may do so by going to the *Configuration* panel, followed by *Properties*, *Device Access*, and lastly *HTTPS/ASDM*.

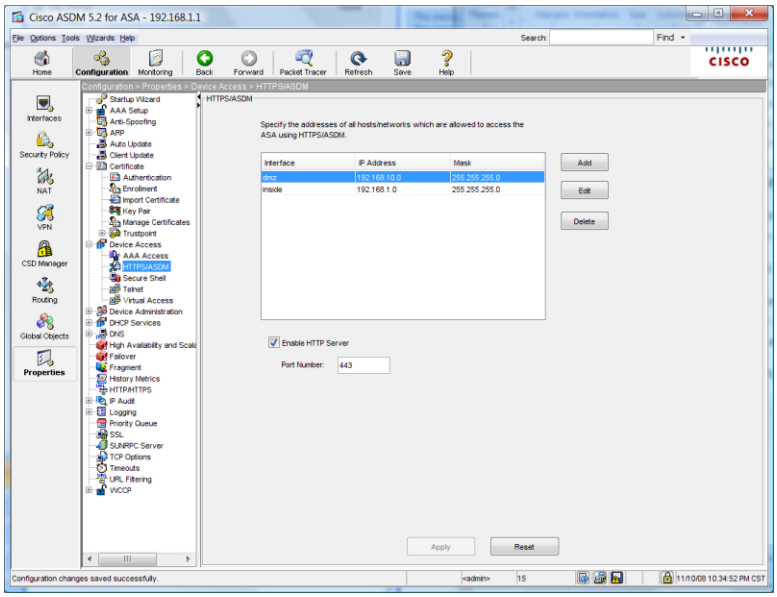

Figure 4 - HTTPS/ASDM Device Access

Device Access is also at the point which you are able to limit the access type (SSH, Telnet, ASDM, HTTP, AAA) and also limit what IP addresses or IP address ranges are allowed to access the device.

Setting up VLANs and Ports

The initial configuration of the device gives the user two VLANs, inside and outside. The base license, as is being used in these examples, allows for a third VLAN to be configured. This VLAN will be labeled as the 'DMZ'. To add a VLAN, go to the *Configuration* panel and then *Interfaces* and click 'Add'. The following display will appear:

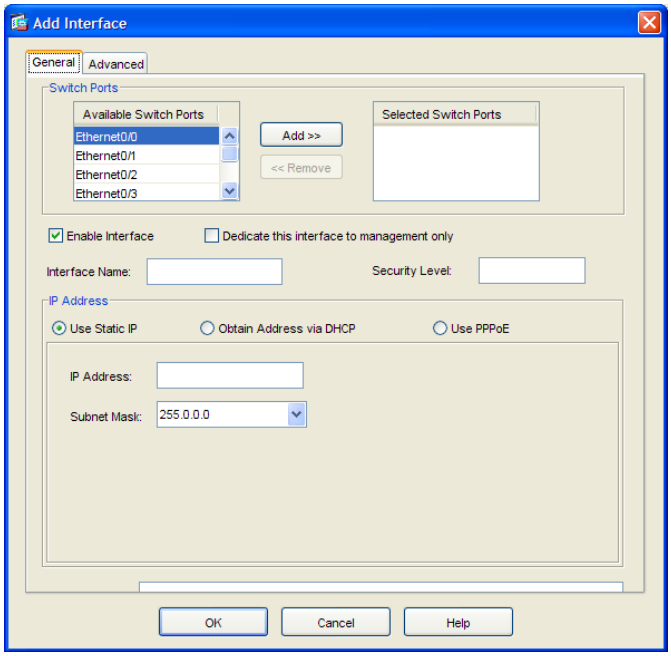

Figure 5 – Adding an Interface and selecting Switch ports

From here, you can enable/disable the interface, name it, set the security level, set the IP address of the device on the interface, and also select which physical ports will be implemented on this interface. The 'Advanced' tab allows you to set the MTU, MAC address, as well as where to block traffic from. The base license *requires* one of the three VLANs to block traffic from another zone. The example DMZ uses Ethernet0/1, while the Outside uses Ethernet0/0, and the Inside has Ethernet0/2 through Ethernet 0/7.

Going to the 'Switch Ports' tab gives the user a different view of the ports as well as the ability to edit further settings. These settings include changing the port to Trunk access mode (not allowed with the base license), changing the duplex, changing the speed, and lastly the isolation mode (restricting traffic from being forwarded from one isolated port to another on the same VLAN). The icons next to Ethernet0/6 and Ethernet 0/7 signify that those ports support PoE (Power over Ethernet).

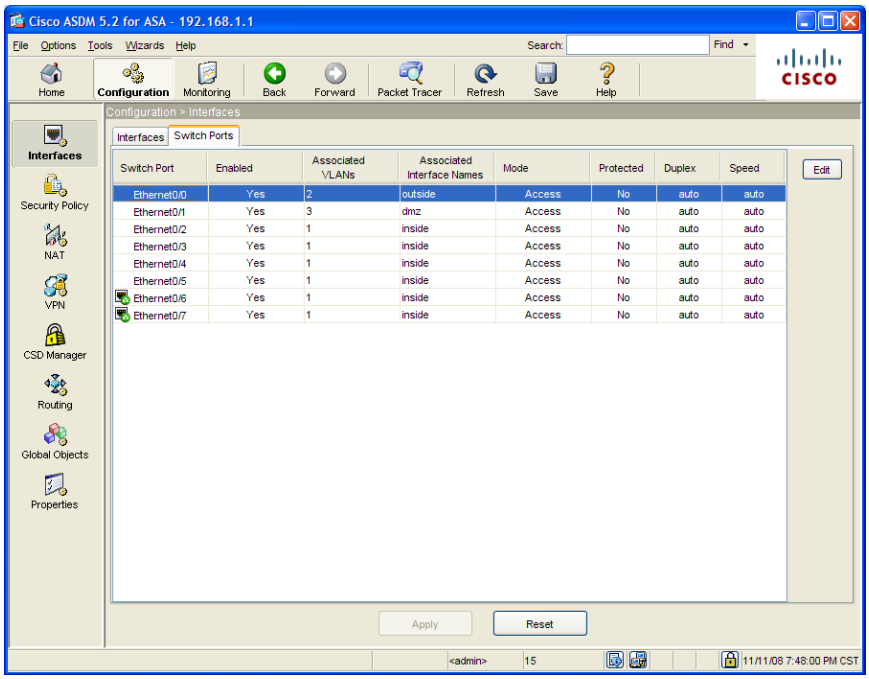

Figure 7 – Interface Switch Ports Overview

Security levels

Security levels are an important concept of Cisco devices. These levels range from 0-100 (0 being the lowest, 100 being the highest). An easy way of thinking about security levels of an interface is to think of it as a percentage of trust. An inside network may be trusted all of the time. It will be given a security level of 100. A DMZ, on the other hand, should not be trusted all of the time as it can be vulnerable to the outside network. We can give this interface a security level of 50. The outside network should never be trusted. It will be given a security level of 0. By default, traffic is allowed to flow from a trusted source to a less trusted source but the inverse is not true.

Access Policies

The access control lists define what type of traffic or who can enter or exit through the device. An access policy serves a similar function to a firewall rule, and each interface has its own lists for incoming and outgoing traffic.

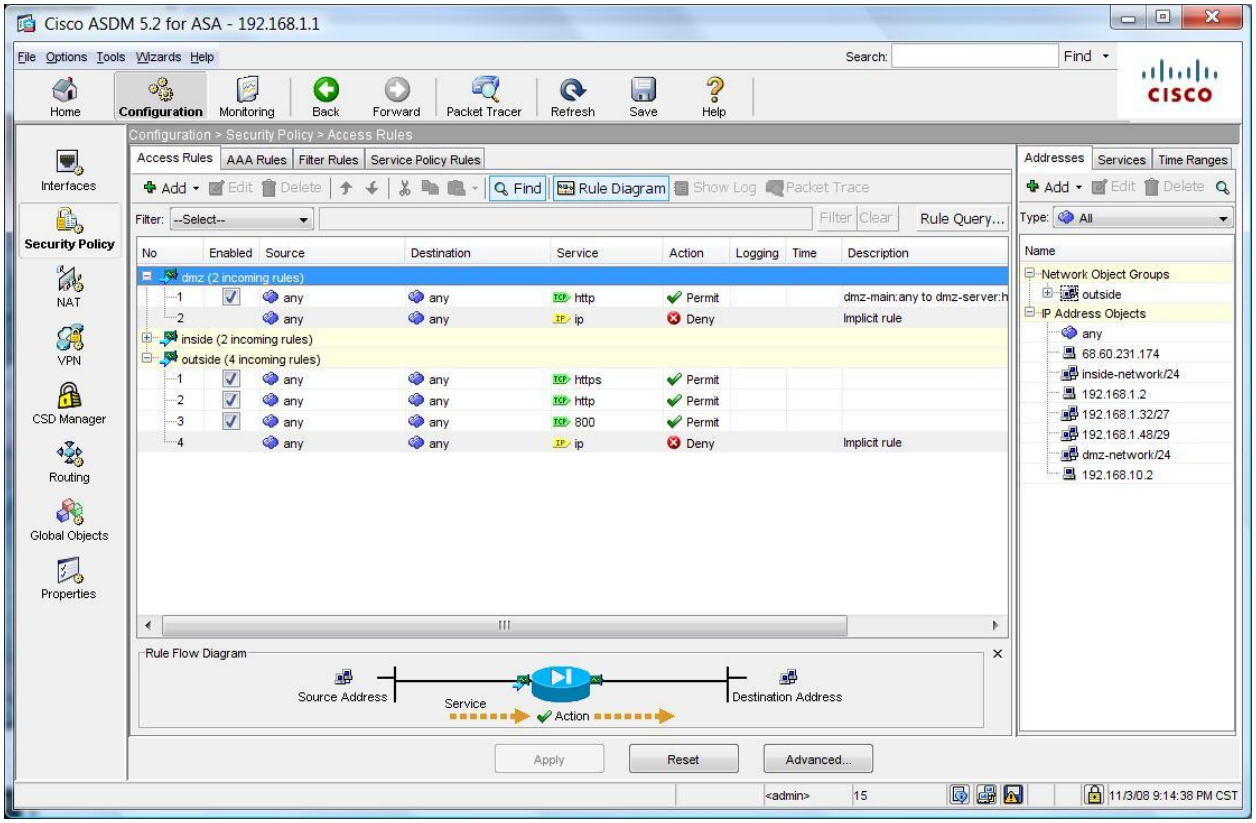

Figure 8 – Access Rules Overview

Figure 8 shows the ASDM view of the *Access Rules*. These access rules can be viewed and modified in the *Access Rules* tab of *Security Policy* under the *Configuration*. Each interface has its own implicit rules for both incoming and outgoing traffic. The incoming rules deny all traffic of any type to any destination. The outgoing default rule also denies all traffic. These default rules are only implemented should an additional rule for that interface be added. For example, if you do not configure a rule for outgoing connections on the Inside network all traffic is allowed. However, if you add a rule that allows HTTP traffic to exit the network, *only* HTTP traffic will be allowed outside unless more rules are configured. As a result, it should be noted that outgoing connection rules will not be listed unless a rule in addition to the default rule is added.

How to Add Policies

The addition and modification of access rules is easy via the ASDM. Choose ‘Add’ then ‘Access Rule’. The following screen will appear:

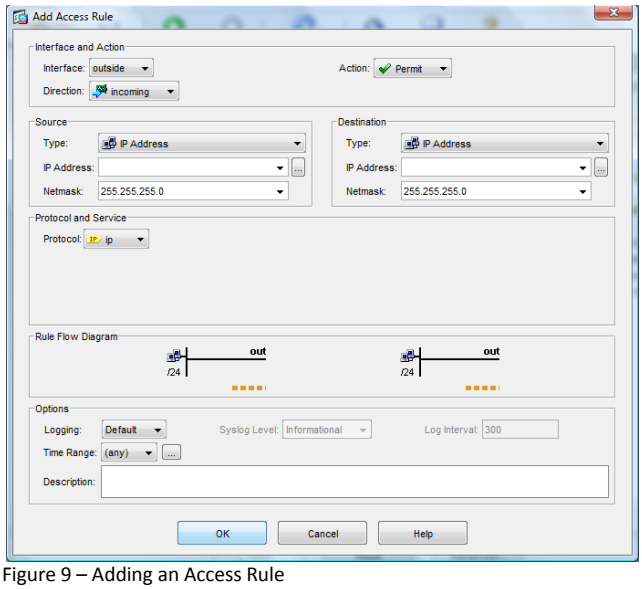

Figure 9 – Adding an Access Rule

From this screen, you choose the interface that you wish the rule to apply. Next, choose the direction of traffic that the rule applies to (incoming or outgoing) and an action (Permit or Deny). The source and destination can be "any", "IP address" (including netmask), an interface IP, or a defined network object. You can also choose the protocol (IP, TCP, UDP) and specific service. The services can be chosen from a predefined list or by typing in the ports. Further options include logging, the time range desired for the rule to be active, and/or a description.

Example Inside Policies

To perform even the most simple of operations on the internet (web page browsing) on the Inside network, two rules must be configured: the first rule must allow DNS queries. The second must allow HTTP (a third rule would be required for HTTPS).

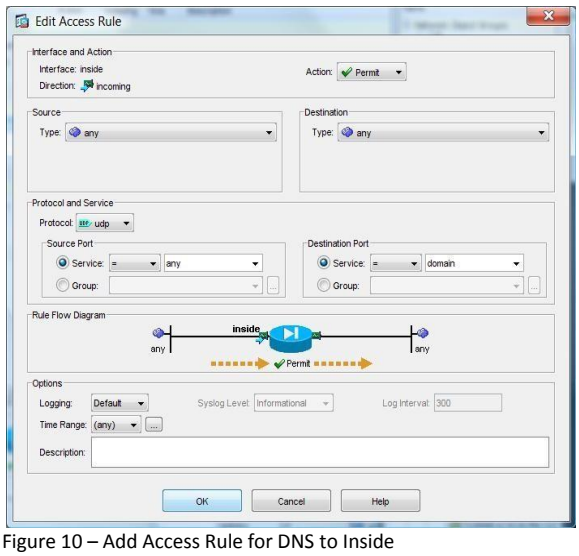

Figure 10 – Add Access Rule for DNS to Inside

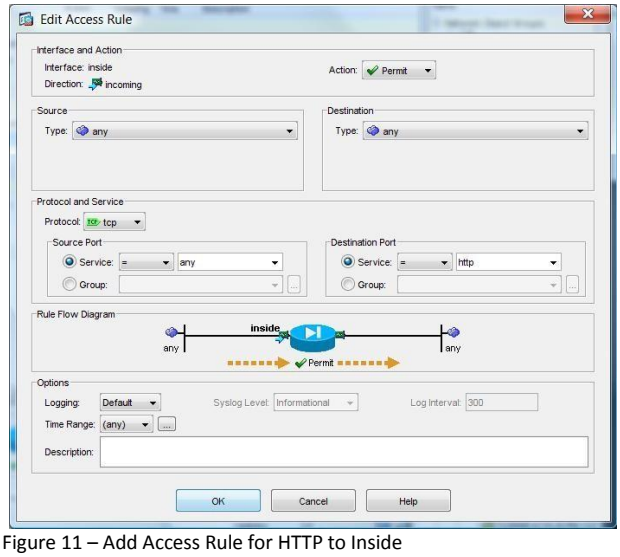

Figure 11 – Add Access Rule for HTTP to Inside

Example DMZ Policies

For a home or small business DMZ, not much should need to be permitted. It largely depends on the running servers. For example, if a web server is running, HTTP/HTTPS should be enabled. The same should happen for any e-mail related services (i.e. SMTP).

The following is an example of an access rule allowing HTTP access to the web server in the DMZ. It allows any source to send TCP traffic from any port to port 80 (HTTP) of 192.168.10.2 in the DMZ.

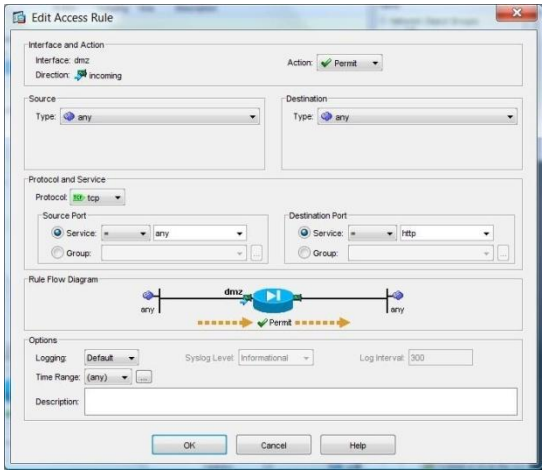

Figure 12 – Add Access Rule for HTTP to DMZ

Example Outside Policies

The Outside interface will require the same access rules as the DMZ for services that you want to be publically accessible.

NAT Policies

Network Address/Port Address Translation (NAT/PAT) is extremely important for any user who does not directly connect his/her computer to a modem. NAT is used to allow many other computers behind the routing device access the internet using the external address without giving away the identity of the host. This is done by modifying the source and destination information of packets and maintaining a list of connections.

How to Add NAT Policies

NAT Policies can be added, edited, or removed from the *Configuration -> NAT* panel. Select 'Add' and choose the type of policy you want to add. There are multiple options: Static NAT Rule, Dynamic NAT Rule, NAT Exempt Rule, Identity NAT Rule, Static Policy NAT Rule, and Dynamic Policy NAT Rule. Static rules map a private address to an external address one-to-one. Dynamic rules map a single address to a pool of addresses.

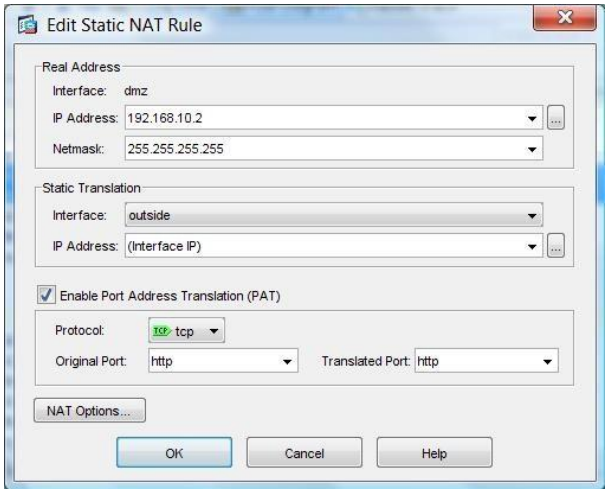

Figure 13 – Editing a Static NAT Rule

Demilitarized Zone (DMZ)

"DMZ (Demilitarized Zone) is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. A DMZ adds an additional layer of security to an organization's Local Area Network (LAN). An external attacker can only access equipment that is in the DMZ, rather than the whole of the network" [5]. There are two commonly used structures for a DMZ. The first (shown in Figure 14) is using a single firewall. The firewall sits between the external router and the internal network. It separates the DMZ from the rest of the LAN. The other structure uses two firewalls. The first firewall filters all traffic only permitting the traffic which is allowed for the internal and DMZ networks. The other firewall filters traffic to only allow traffic that originates from the DMZ. This is a more secure method of deploying a DMZ [6]. However, for ease of creation, we will use the first method.

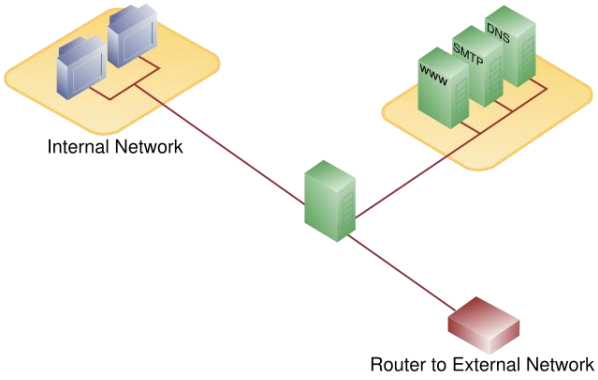

Figure 14 – Example DMZ Configuration [7]

There are three requirements when configuring the ASA for a DMZ deployment [8]:

- Internal clients need to be able to communicate with devices on the internet.
- Internal clients need to be able to communicate with the DMZ web server.
- External clients need to be able to communicate with the DMZ web server.

The base license of the Cisco device does not allow all of the VLANs to communicate with each other. This can present a problem when attempting to configure a DMZ as it must be on its own VLAN. There are only two methods possible when using this device. These are: DMZ->Inside traffic is restricted and Outside->Inside traffic is restricted.

DMZ->Inside Restricted

My initial attempt to create a workable DMZ with the restrictions involved restricting traffic from the DMZ VLAN to the Inside VLAN. This restriction must be set in the *Interfaces* panel. Once this has been done and the traffic flow restricted, the next step was to create the necessary NAT policies:

- Traffic coming from the internet to the external address port 80 is translated to the web server in the DMZ on port 80.
- Traffic coming from the DMZ VLAN to port 80 is translated to the web server in the DMZ on port 80.
- Traffic coming from the Inside VLAN to port 80 is translated to the external address port 80.
- Traffic coming from the internet to the external address port 21 is translated to the FTP server in the DMZ on port 21.
- Traffic coming from the DMZ VLAN to port 21 is translated to the FTP server in the DMZ on port 21.
- Traffic coming from the Inside VLAN to port 21 is translated to the external address port 21.

In addition to the preceding rules, rules to access the internal routers from the outside were also to be programmed:

- Traffic coming from the internet to the external address over port 800 is translated to an internal address of 192.168.1.2 on port 80.
- Traffic coming from the DMZ to the external address over port 800 is translated to an internal address of 192.168.1.2 on port 80.
- Traffic coming from the Inside VLAN to the external address over port 800 is translated to an internal address of 192.168.1.2 on port 80.

These rules were more so to prove that the internal network can still be accessed, given the proper instructions. However, these rules should not be implemented in a production environment; they create an unnecessary risk to the network.

At the start, this setup appeared to work with the exception of the DMZ being unable to initiate communication to the Inside VLAN.

I attempted to verify that this setup worked at a later point and found that it was not performing as it was earlier. This was more of an error on my part, not realizing that the web browser I was using was simply caching the appropriate web pages and redisplaying them without trying to pull new information.

Summary

The first attempt at creating a workable DMZ did not work as intended. While clients on the internet were able to access the content of the web server as well as the FTP server, clients on the Inside VLAN could not. The DMZ itself could not access its own web pages unless it used the external IP address or simply "localhost". The method used to try to circumvent the restrictions of the license was to redirect all requests from the Inside VLAN to the external address and have the DMZ respond to those requests. Ideally, the device would have known to respond back to the inside client. It was smart enough to realize what I was attempting to do and would log an error message related to the restriction.

As stated on the Cisco website, "[w]ith the Base platform, communication between the DMZ VLAN and the Inside VLAN is restricted: the Inside VLAN is permitted to send traffic to the DMZ VLAN, but the DMZ VLAN is not permitted to send traffic to the Inside VLAN. The Security Plus license removes this limitation, thus enabling a full DMZ configuration." [(9)]

However, the DMZ *can* respond to requests from the Inside. The ability to solely respond to requests and not initiate could have an effect on things like backups, email, etc. Of course, the whole point of a DMZ is so that outsiders can access it but the DMZ itself cannot access the internal network. To access things like a backup server you would likely have to set up more routing through something such as an application server.

Email and databases may also be problematic. The email server in the DMZ would serve only to pass email through to the internal network. However, with the restriction of not being able to initiate connections to the inside network, programs like *Exchange* would have to be able to "pull" mail instead of have it pushed into the Inside. With this in mind, if you run a local copy of the database inside the DMZ, it would be possible to perform backups if you have some sort of replication/sync initiated from a database on the inside network. This does nothing for the contents of the database if the DMZ web server is compromised; it only allows for backups. However, this is an increased security risk. When there is a database server allowed (whether inside the DMZ or not), if you break the DMZ server it's only a matter of time until you can get access to the database. All that must be done in either situation is to then attack the database server or brute force the password. If the SQL server is in the DMZ, it can be brute forced or perhaps the files can be copied off the server then brute forced. If it's not in the DMZ you can still try to exploit it over the allowed connection from the web server.

This method acts more like what some routers refer to as a "DMZ host" [(6)]. The difference between a true DMZ and a "DMZ host" is that only the select ports are forwarded and it cannot be more than a single host. This may be a viable method for creating a DMZ, though it is not ideal and has limitations.

Outside->Inside Restricted

A DMZ that cannot initiate connections to an internal network would hinder its usefulness. Armed with this and some other information on security allows us to use another method for configuring the DMZ. An outsider should hardly ever be able to access internal resources. This leads to configuring the device to restrict traffic from the Outside to the Inside. An outsider cannot initiate connections to an internal resource. However, a user on the internal network can still access outside resources (such as web pages, FTP sites, etc.). The traffic flow must be restricted from the *Interfaces* panel. If the proper

interface does not have the traffic restricted already, it would be simple to save the configuration file, edit the appropriate line, and reapply the configuration from the factory defaults.

Table 1 – Differences between DMZ configuration for no forward command

Original Section (DMZ->Inside Restricted)	Modified Section (Outside->Inside Restricted)
interface Vlan1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 ! interface Vlan2 nameif outside security-level 0 ip address dhcp setroute ! interface Vlan3 **no forward interface Vlan1** nameif dmz security-level 50 ip address 192.168.10.1 255.255.255.0	interface Vlan1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 ! interface Vlan2 **no forward interface Vlan1** nameif outside security-level 0 ip address dhcp setroute ! interface Vlan3 nameif dmz security-level 50 ip address 192.168.10.1 255.255.255.0

Once this has been done, the appropriate NAT policies can be created (for the example):

- Traffic coming from the internet to the external address on port 80 is translated to the web server in the DMZ on port 80.
- Traffic coming from the internet to the external address on port 21 is translated to the FTP server in the DMZ on port 21.
- Traffic coming from the inside to the external address on port 80 is translated to the web server in the DMZ on port 80.
- Traffic coming from the inside to the external address on port 21 is translated to the FTP server in the DMZ on port 21.
- Traffic coming from the DMZ to the external address on port 80 is translated to the FTP server in the DMZ on port 80.
- Traffic coming from the inside to any address on the DMZ network over any port is translated to the correct address and port (static rule).
- Traffic coming from the DMZ to any address on the inside network over any port is translated to the correct address and port (static rule).

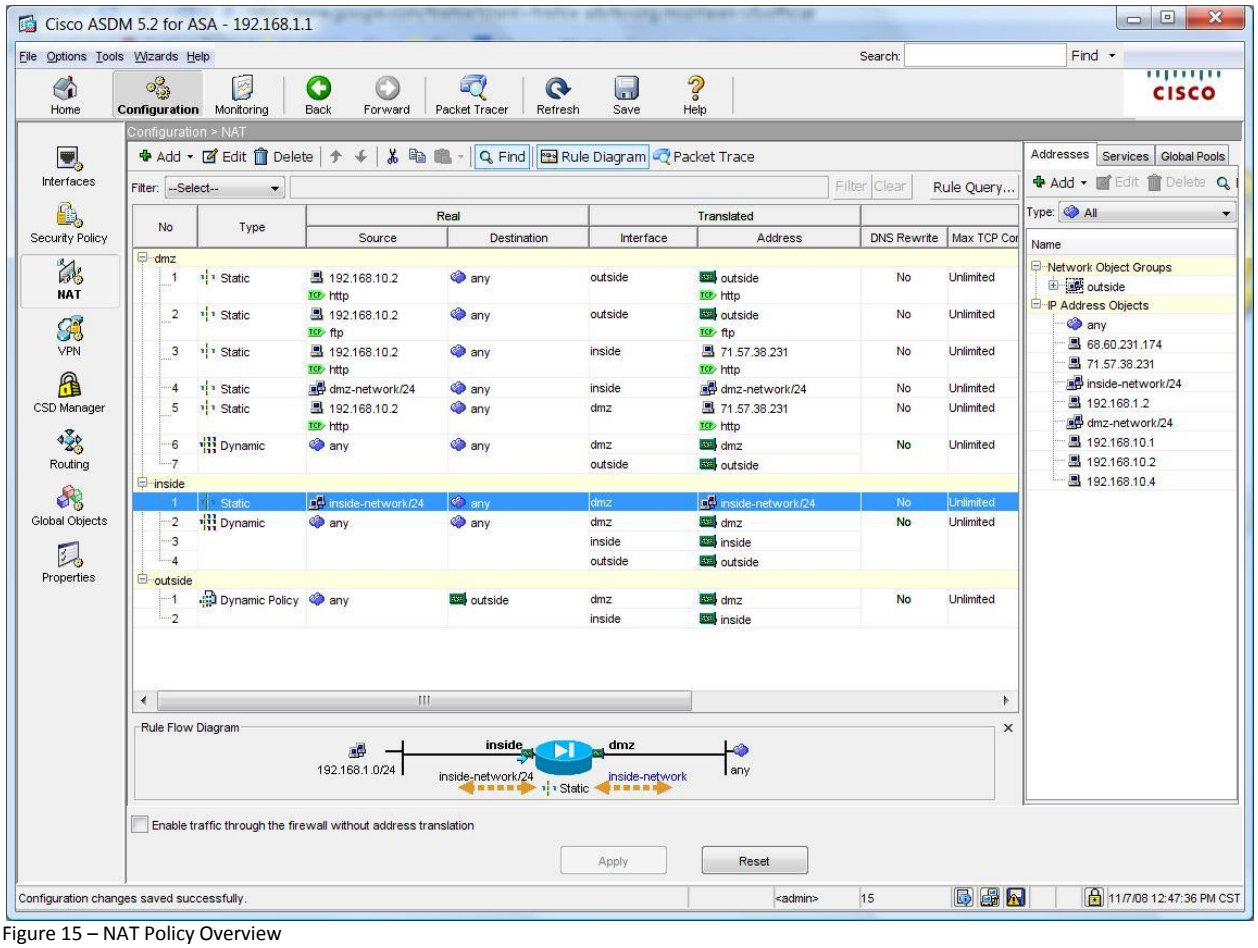

Figure 15 – NAT Policy Overview

The last two rules listed are necessary otherwise you will not be able to communicate between the inside and the DMZ. Events will be listed in the log file informing you that there is no translation group for the communication.

Summary

The second method of configuring a DMZ using the base license was far more successful in terms of its usefulness for its function. The DMZ is separated from the Inside LAN, but it can still communicate with it for functions such as database access, email access, or backups. The internal clients can easily access the DMZ servers for updating or viewing their content.

There is one significant disadvantage to this method: connections coming from external connections cannot reach the inside LAN if they were not initiated by a host within the LAN. This alone is not necessarily a bad thing, as it is not recommended to allow unrequested connections from the internet. However, one of the marketing points of this device is its VPN capabilities:

> "Extend your network with secure, flexible, seamless remote access. Cisco ASA 5500 Series, Cisco's premier VPN solution, offers unmatched clientless portal capability and cross-platform full-tunnel client for up to 10,000 simultaneous SSL or true IPsec connections in one device - all protected by world-class firewall services and much more." (10)

This feature is rendered largely useless by disabling incoming connections in the manner described earlier. This would render most, if not all, of the similar methods of viewing internal content remotely (GoToMyPC, Remote Desktop, etc.) unusable. While home users would most likely not be as concerned about this, many small businesses who employ users around the country or allow them to work at home may be concerned about the lack of this feature.

Authentication, Authorization, Accounting (AAA)

Purpose of AAA

"AAA [pronounced 'triple A'] provides the primary framework to set up access control on a router or access server. It is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way to perform authentication, authorization, and accounting services" [(11)].

Authentication: Who are you?

Authentication is a method for identifying oneself by the use of credentials. Possible credentials can be, for example: passwords, one-time tokens, or certificates [(12)].

Authorization: What can you do?

Authorization refers to the granting of privileges to a user (or other object). It is "based on their authentication, what privileges they are requesting, and the current system state. Authorization may be based on restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user" [(12)].

Accounting: What did you do?

Accounting refers to tracking and/or logging of network resources utilized by users. This information generally contains the identity of the user (username, IP, etc.), service used, time used, and time ended [(12)].

RADIUS

RADIUS (Remote Authentication Dial in user Service) is a protocol used to implement centralized AAA. It is "often used by ISPs, Wireless Networks, integrated e-mail services, Access Points, Network Ports, Web Servers or any provider needing a well supported AAA server [and] is commonly used by ISPs and corporations managing access to the Internet or internal networks employing a variety of networking technologies, including modems, DSL, wireless and VPNs" [(13)].

It is in competition with TACACS+ (a later and incompatible version of TACACS).

Table 2 – Differences between RADIUS and TACACS+ [(14)]

RADIUS	TACACS+
RADIUS uses UDP.	TACACS+ uses TCP.
RADIUS encrypts only the password in the access-request packet; less secure.	TACACS+ encrypts the entire body of the packet; more secure.
RADIUS combines authentication and	TACACS+ uses the AAA architecture, which

authorization.	separates authentication, authorization, and accounting.
Industry standard (created by Livingston).	Cisco Proprietary.
RADIUS does not support ARA access, Net BIOS Frame Protocol Control protocol, NASI, and X.25 PAD connections.	TACACS+ offers multiprotocol support.
RADIUS does not allow users to control which commands can be executed on a router.	TACACS+ provides two ways to control the authorization of router commands: on a per-user or per-group basis.

"Although TACACS+ is considered to be more versatile, RADIUS is the AAA protocol of choice for enterprise ISPs because it uses fewer CPU cycles and is less memory intensive." [(14)]

It should be noted that RADIUS combines Authentication and Authorization.

Setting up a RADIUS server Windows Server 2008 Standard

AAA can be implemented in a variety of protocols including RADIUS, Diameter, TACACS, and TACACS+. For this example, a RADIUS server will be configured in Windows Server 2008 Standard. As AAA is not the focus of this paper, it will be a very basic example used only for demonstration.

The first step is to install the Network Policy and Access Services. This is a logical grouping of several functions, including Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP). The NPS is an updated version of Microsoft's implementation of a RADIUS server and proxy and is the selection that should be chosen. It performs all of the functions of RADIUS and also can function as a Network Access Protection (NAP) policy server [(15)].

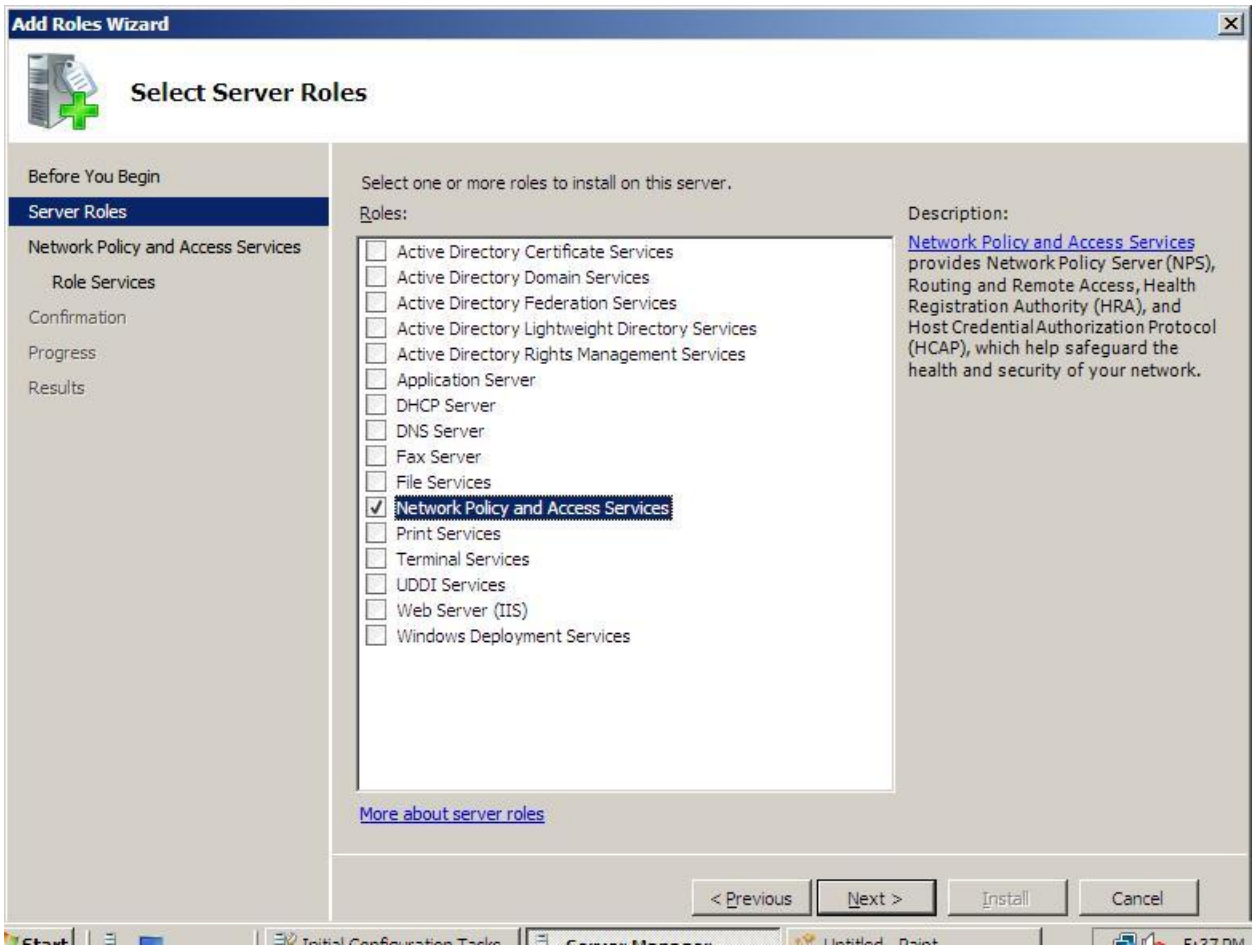

Figure 16 – Installing NPAS in Windows 2008 Server

Once NPS is installed:

- Open the NPS management console
- Expand RADIUS Clients and Servers
- Right-click RADIUS Clients
- Select New RADIUS Client
- Enable the client and fill out the appropriate information.

  The friendly name is simply an easy way to remember the name for the device used by the administrator. The address is the IP address of the Cisco device, and the Vendor name is Cisco. It would be best to generate a shared secret instead of manually creating one. An automatically generated secret would likely be more complicated and harder to guess.

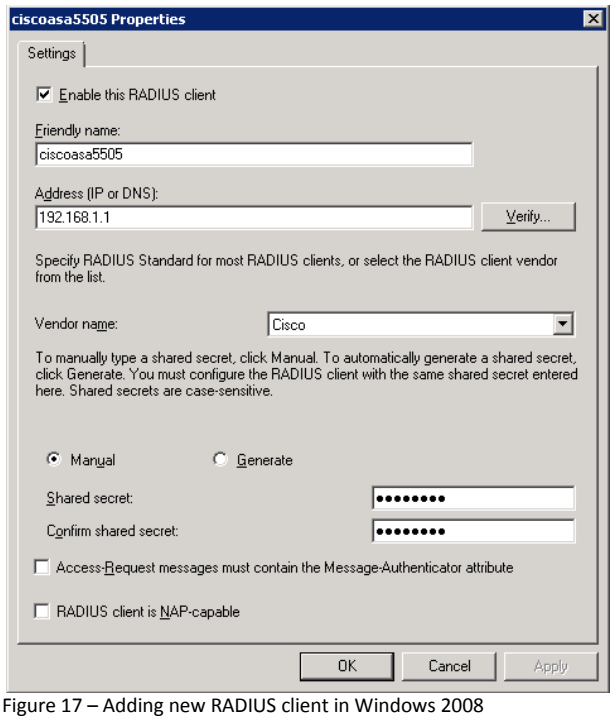

Figure 17 – Adding new RADIUS client in Windows 2008

Expanding *Policies* reveals several options. We won't modify *Connection Request Policies*, but check to ensure that the default "Use Windows authentication for all users" is enabled. Next, right-click *Network Policies* and select 'New'.

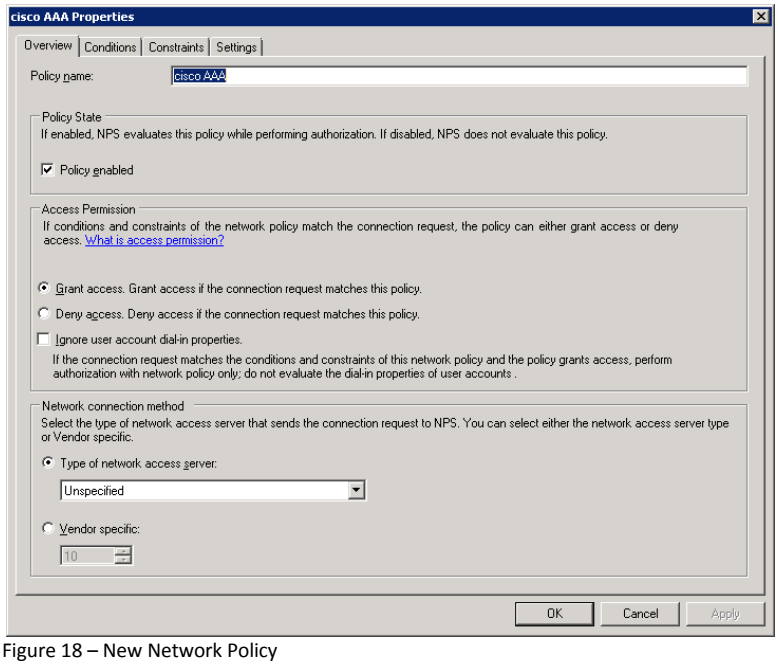

Figure 18 – New Network Policy

For this example, the policy was simply named "cisco-AAA". It was also enabled and the policy was set to "grant access" as long as the connection matches the policy. Entering the *Conditions* tab allows us to modify the type of conditions required for access to be granted.

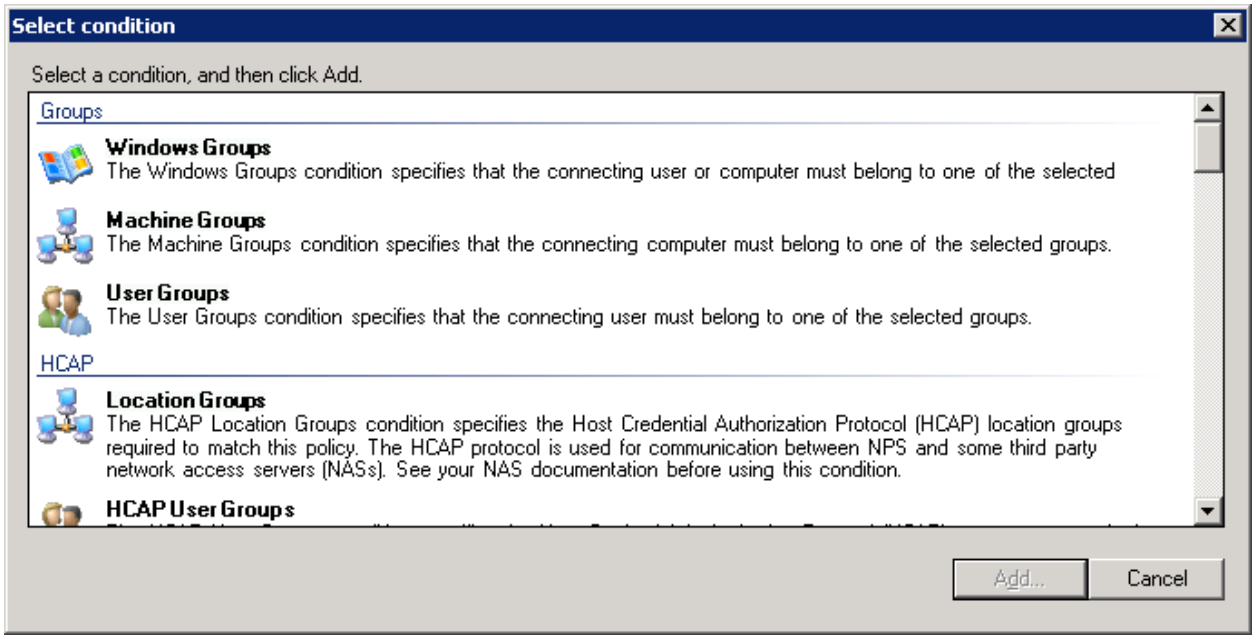

Figure 19 – Possible Conditions for Network Policy

These conditions include which group the user belongs to, the health status of the device, the time of day, and many others. For this example, we are only requiring that the user is a member of the Administrators group of the server. You may change the authentication methods or constraints if desired (being mindful that it may affect the following settings).

The *Settings* tab allows us to specify some features specific to the device. First, we click on 'Standard'. Add a new attribute and set it to 'Service-type'. When it asks you to enter the type, select 'Login' and close the prompts. Next, add a Vendor-specific attribute: select 'Cisco', then 'Cisco-AV-Pair'. Select 'Add' and enter "shell:priv-lvl=15" [(16)]. Lastly, close out the prompts and finish the wizard.

By default, log files for authentication and accounting are stored in "C:\Windows\system32\LogFiles".

Setting up the ASA 5505 to use AAA

The first thing to be configured on the device is the AAA Server groups. From the *Configuration* panel, select *Properties -> AAA Setup -> AAA Server Groups*. From here, add a new server group. For our configuration, it has been named "win2008". Set the protocol to RADIUS, Accounting Mode to Single, and Reactivation Mode to Timed. Now the servers must be added to this group. Our setup has only one server. It is in the Inside interface, has an IP address of 192.168.1.7, is using UDP port 1645-46 (though RADIUS officially has ports 1812-13 [(17)]), and the server secret key generated in Windows 2008 is entered at this screen.

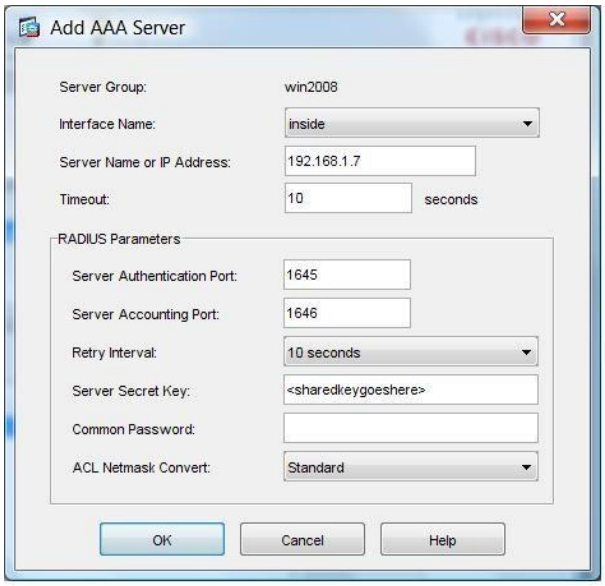

Figure 20 – Add a new AAA server

Figure 21 – Test newly added AAA server

You can now test this configuration by clicking the 'Test' button.

Device Administration

After validating the information for the RADIUS server, you can now configure the device to require authentication from the RADIUS server for specific types of device administration. This would be valuable if you wish to allow certain members of your IT team access to the device but to also have individual accounts with different access levels and more accountability. From the *Configuration* panel, select *Properties -> Device Access -> AAA Access*.

You can enable whichever you choose for authentication. I chose to enable it for SSH access as I do not allow telnet access. I could easily have enabled it for HTTP/ASDM as well. It should be noted that you must switch the server group from LOCAL to your newly created group, which, in this case, was win2008.

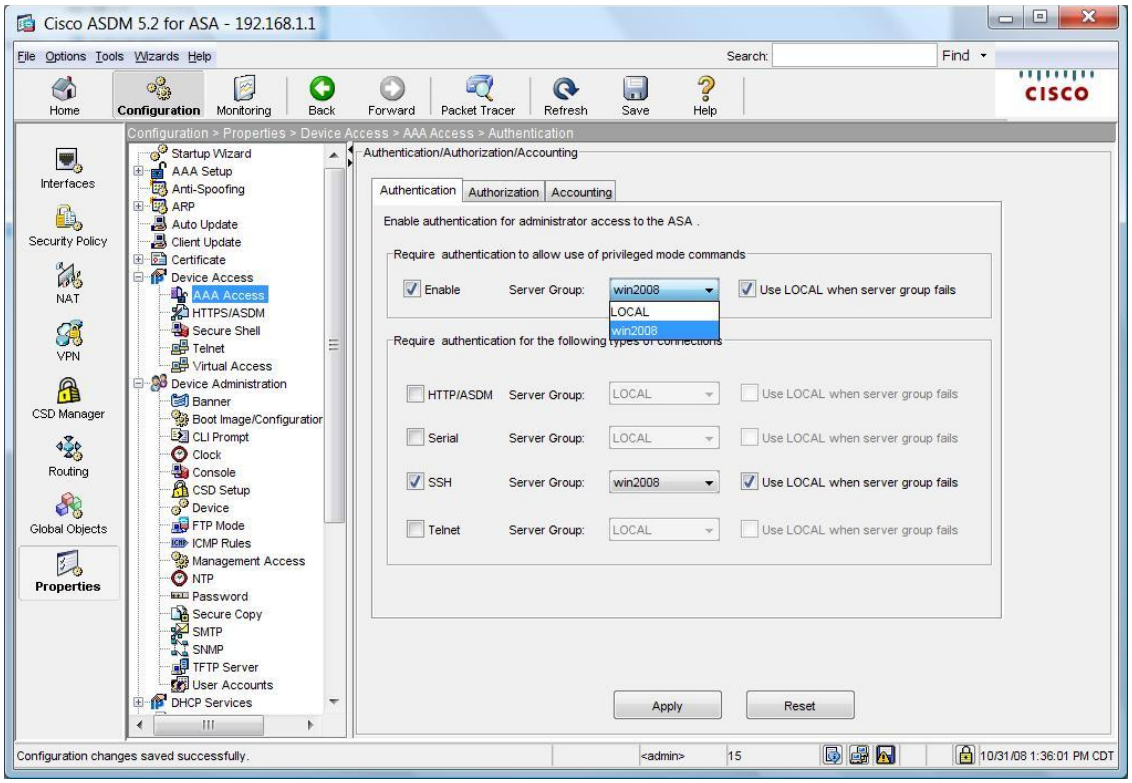

Figure 22 – Device access using AAA

For Accounting, I enabled it for all user activity, as well as SSH and Telnet connections (to log attempts).

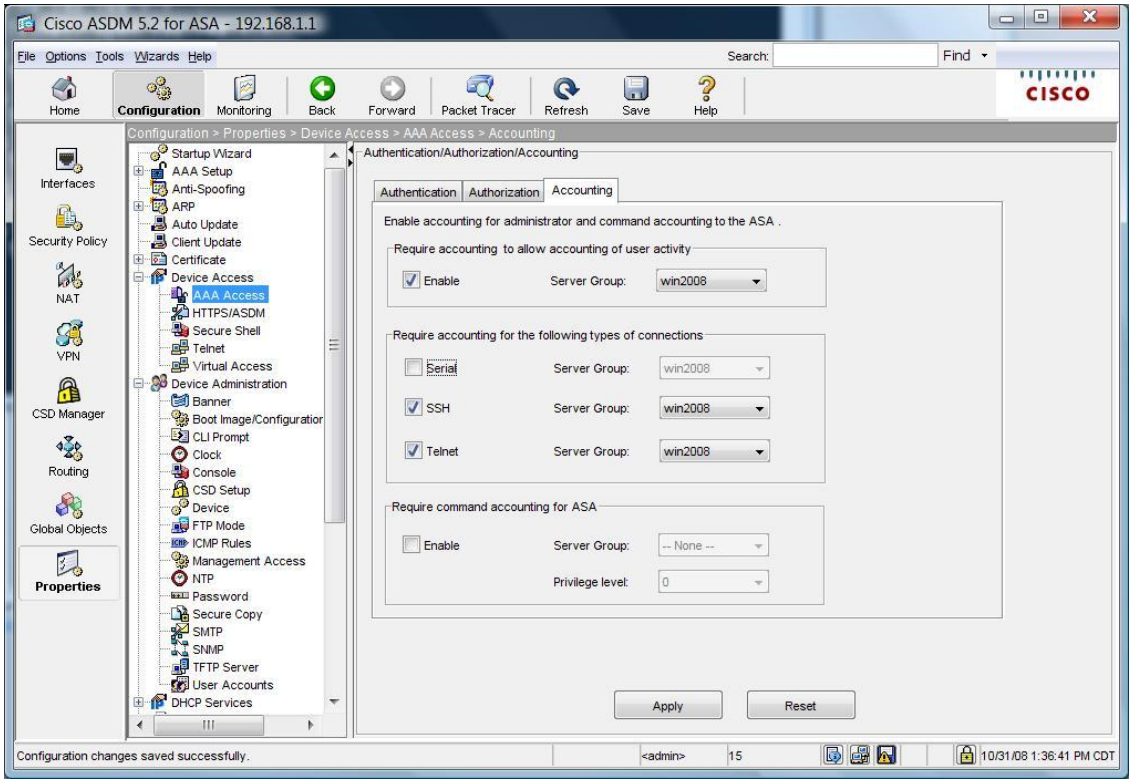

Figure 23 – Device accounting using AAA

I did not configure any Authorization, as I could not use Windows Server 2008 for that purpose as configured.

Example on How to Limit and/or Log Access to Web Pages

Another interesting ability of AAA is that you can log and limit access to resources. For example, this can be done to web pages. It is a fairly simple process for authentication:

- Open the *Security Policy* panel from within *Configuration.*
- Select the *AAA Rules* tab.
- Select 'Add' -> 'Authentication Rule'.
- Select the interface you wish the rule to apply (inside for this example).
- Change the AAA Server Group (win2008 for this example).
- Leave the source and destination alone.
- Change the Protocol to TCP, and the destination port to HTTP.
- Click OK.

HTTPS Login

When users now attempt to visit a webpage, they must enter their credentials in a web page form (if Secure HTTP is enabled via the *Advanced* options) or a pop-up login.

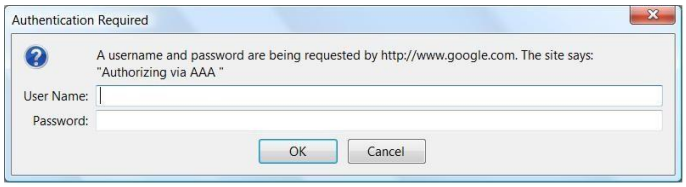

Figure 24 – Login form not using Secure HTTP

Figure 25 – Using Secure HTTP

AAA prompts

The prompts shown on these forms can be changed in Configuration -> Properties -> AAA Setup -> Auth Prompt. The prompt is currently set to "Authorizing via AAA" as shown above, though this is technically inaccurate as it is authenticating.

HTTP Logging

The accounting for HTTP transactions is configured through a nearly identical rule except you must choose Add -> Accounting Rule. The log files are located on the AAA server and entries look like the following:

```
192.168.1.1,unknown,12/01/2008,17:09:25,IAS,WIN2008,5,0,14,66.235.139.70,16,80,4
0,2,42,1140,43,1726,44,79F82CEA,46,29,49,0,4,192.168.1.1,4108,192.168.1.1,4116,9
,4128,ciscoasa5505,5000,ip:source-port=49809,5000,ip:destination-
port=80,5000,ip:source-ip=192.168.1.2,5000,ip:destination-
ip=66.235.139.70,4154,Use Windows authentication for all users,4136,4,4142,0
```

```
192.168.1.1,unknown,12/01/2008,17:09:25,IAS,WIN2008,5,0,14,128.242.186.208,16,80
,40,2,42,26498,43,1259,44,45AF29EE,46,19,49,0,4,192.168.1.1,4108,192.168.1.1,411
6,9,4128,ciscoasa5505,5000,ip:source-port=49829,5000,ip:destination-
port=80,5000,ip:source-ip=192.168.1.2,5000,ip:destination-
ip=128.242.186.208,4154,Use Windows authentication for all users,4136,4,4142,0
```

Miscellaneous Features

The Cisco ASA 5500 series comes with a variety of security features. Many are listed in the Properties panel. Some of the security features are *ICMP Rules*, *TCP Options*, *Anti-Spoofing*, and *Service Policies*.

ICMP Rules

Most people might prefer they aren't known to the internet. This is where ICMP rules are beneficial. With these rules, ICMP requests can be accepted or rejected on different interfaces. For example, you can enable ICMP echo requests on the Outside interface to allow your external address to be pingable.

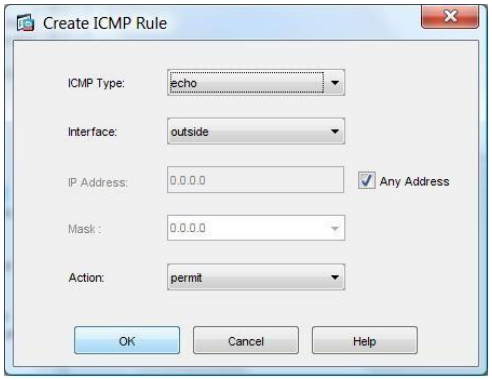

Figure 26 – Create ICMP Rule

ICMP Types include: any, alternate-address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute, and unreachable. *ICMP Rules* can be found under *Device Administration*.

TCP Options

The *TCP Options* pane allows you to specify parameters for TCP connections.

TCP Resets

TCP Resets allow an inappropriate TCP connection to be reset. According to RFC3360, "as a general rule, reset (RST) must be sent whenever a segment arrives which apparently is not intended for the current connection. A reset must not be sent if it is not clear that this is the case" [(18)]. The Cisco ASA 5505 allows the administrator to specify when to allow TCP Resets to be sent. These settings are for when traffic is denied due to AAA settings or ACLs. This is particularly useful for inbound traffic with IDENT connections. "When you send a TCP RST (reset flag in the TCP header) to the denied host, the RST stops the incoming IDENT process so that you do not have to wait for IDENT to time out. Waiting for IDENT to time out can cause traffic to slow because outside hosts keep retransmitting the SYN until the IDENT times out, so the **service resetinbound** command might improve performance" [(19)]. With outbound

connections, this option is enabled by default. It can be disabled during periods of heavy traffic to reduce CPU load. If TCP Resets are not sent, these packets are silently discarded [19].

Anti-Spoofing

What is spoofing

Spoofing is when a packet pretends to have a source address that is not their own. This allows people to gain unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine. It can also be used for Denial of Service attacks to prevent the victim from tracing and stopping the DoS [20].

How does Cisco's Anti-Spoofing protect against it?

The Cisco device employs an anti-spoofing feature by making sure the source IP address is coming in on the appropriate source interface. "If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the security appliance drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the security appliance drops the packet because the matching route (the default route) indicates the outside interface" [19].

Service Policy

Example on limiting transfer speeds

Service policies can be created to perform specific restrictions or inspections on traffic. For example, bandwidth can be limited. Here is an example on how to limit incoming HTTP bandwidth from the Security Policy -> Service Policy panel:

First, create a new Service Policy

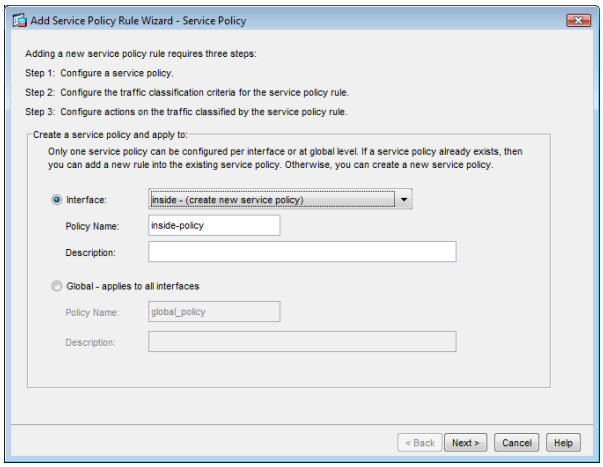

Figure 27 – Adding a new Service Policy

Then, select the type of traffic to monitor

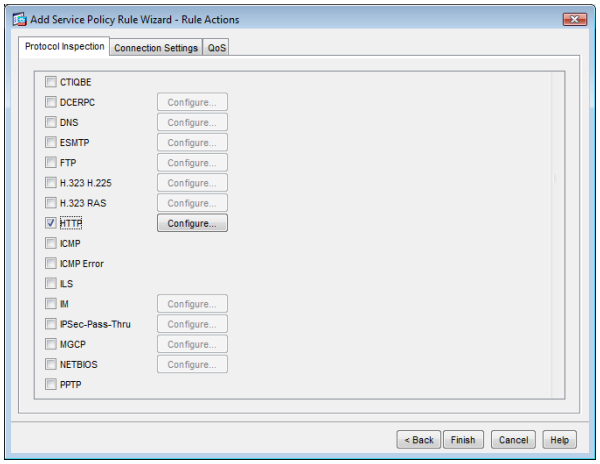

Figure 28 – Selecting protocol to inspect

Finally, configure bandwidth and actions (note that it the direction is set to output for inbound traffic)

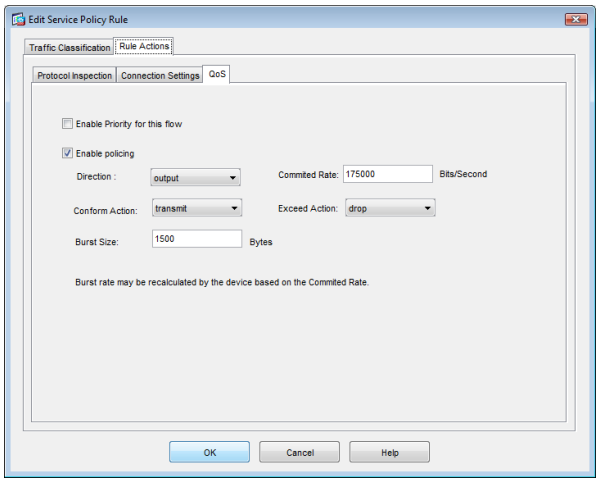

Figure 29 – QoS to limit input speed

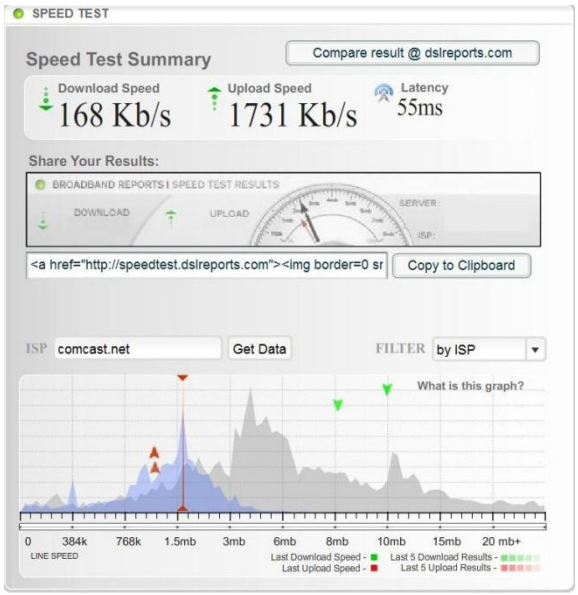

Figure 30 – Results of implemented Bandwidth policy

It is unusual to note that when configuring this policy the direction of the traffic was “input” and the outgoing traffic rate slowed. When the traffic was set to “output”, the incoming traffic was slowed. This rule had the traffic speed set to 175,000 bits, or around 170 kilobits, so the rule was fairly accurate. The latency was not affected and traffic not part of the HTTP protocol continued to flow at normal speeds.

Conclusion

The Cisco ASA 5505 is a versatile device capable of running many of the network services required by small businesses and tech-savvy home users. Its modular design, strong capabilities out-of-the-box, and ease of configuration make it a worthwhile investment for those concerned about the cost, time, and expertise required for enhancing an existing network or creating a new one with more complex and numerous hardware devices, such as its predecessors: the Cisco PIX, Cisco IDP 4200, and the Cisco VPN 3000 Series Concentrators [21]. However, the base license is limited in functionality. The security plus license would be required for the full use of a demilitarized zone along with VPN connections, increased VLANs, and increased firewall connections.

This page was left intentionally blank.

Works Cited

1. **Cisco Systems, Inc.** WHITEPAPER: CONVERGED VS. DEDICATED APPLIANCE. *Cisco Systems, Inc.* [Online] 2005. [Cited: November 14, 2008.] www.cisco.com/application/pdf/en/us/guest/products/ps6120/c1244/cdccont_0900aecd80282f76.pdf.

2. —. Cisco ASA 5500 Series Adaptive Security Appliances Models Comparison. *Cisco Systems, Inc.* [Online] 2008. [Cited: November 14, 2008.] http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html.

3. —. Cisco Security Appliance Command Line Configuration Guide, Version 7.2 - Configuring Interface Parameters. *Cisco Systems, Inc.* [Online] 2008. [Cited: November 15, 2008.] http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/intparam.html.

4. —. ASDM 5.2 User Guide - Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance. *Cisco Systems, Inc.* [Online] 2008. [Cited: November 15, 2008.] http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/user/guide/ifcs5505.html.

5. —. DMZ - Ciscowiki. *Cisco Support Wiki.* [Online] August 2008. [Cited: November 18, 2008.] http://supportwiki.cisco.com/ViewWiki/index.php/DMZ.

6. **Wikipedia.** DMZ (computing). *Wikipedia, the Free Encyclopedia.* [Online] November 24, 2008. [Cited: November 20, 2008.] http://en.wikipedia.org/wiki/Demilitarized_zone_(computing).

7. **Viento, Sangre.** DMZ (computing). *Wikipedia, the free encyclopedia.* [Online] May 14, 2008. [Cited: November 20, 2008.] http://upload.wikimedia.org/wikipedia/commons/6/6f/DMZ_network_diagram_1_firewall.svg.

8. **Cisco Systems, Inc.** Cisco ASA 5505 Getting Started Guide Software Version 7.2. San Jose : s.n., 2006, pp. 6-5.

9. —. Cisco ASA 5505 Getting Started Guide, Version 7.2 - Planning for a VLAN Configuration. *Cisco Systems, Inc.* [Online] 2008. [Cited: November 15, 2008.] http://www.cisco.com/en/US/docs/security/asa/asa72/getting_started/asa5505/quick/guide/vlans.html.

10. —. Cisco ASA 5500 Series Adaptive Security Appliances. *Cisco Systems, Inc.* [Online] 2008. [Cited: November 15, 2008.] http://www.cisco.com/en/US/products/ps6120/.

11. —. AAA - Ciscowiki. *Cisco Support Wiki.* [Online] May 21, 2008. [Cited: November 18, 2008.] http://supportwiki.cisco.com/ViewWiki/index.php/AAA.

12. **Wikipedia.** AAA protocol. *Wikipedia, the Free Encyclopedia.* [Online] November 21, 2008. [Cited: November 24, 2008.] http://en.wikipedia.org/wiki/AAA_protocol.

13. —. RADIUS. *Wikipedia, the free encyclopedia.* [Online] October 10, 2008. [Cited: November 22, 2008.] http://en.wikipedia.org/wiki/RADIUS.

14. **Cisco Systems, Inc.** Cisco AAA Case Study Overview. *Cisco Systems, Inc.* [Online] 2008. [Cited: November 16, 2008.] http://www.ciscosystems.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/aaasub/C262C1.html.

15. **Microsoft Corporation.** Network Policy and Access Services. *Microsoft TechNet: Resources for IT Professionals.* [Online] 2008. [Cited: November 13, 2008.] http://technet.microsoft.com/en-us/library/cc754521.aspx.

16. **Blindhog.net.** Cisco AAA login authentication with Radius (MS IAS). *Blindhog.net.* [Online] March 7, 2007. [Cited: November 8, 2008.] http://www.blindhog.net/cisco-aaa-login-authentication-with-radius-ms-ias/.

17. **IBM Corporation.** RADIUS. *Internet Security Systems.* [Online] 2008. [Cited: November 9, 2008.] http://www.iss.net/security_center/advice/Reference/Networking/RADIUS/default.htm.

18. **Floyd, S.** Inappropriate TCP Resets Considered Harmful. *Information-Technology Promotion Agency - Japan.* [Online] August 2002. [Cited: October 29, 2008.] http://www.ipa.go.jp/security/rfc/RFC3360EN.html.

19. **Cisco Systems, Inc.** Preventing Network Attacks. *Cisco Systems, Inc.* [Online] 2008. [Cited: October 28, 2008.] http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/user/guide/protect.html.

20. **Tanase, Matthew.** IP Spoofing: An Introduction. *SecurityFocus.* [Online] March 11, 2003. [Cited: November 4, 2008.] http://www.securityfocus.com/infocus/1674.