SANS Institute
InfoSec Reading Room

Transparent (Layer 2) Firewalls: A look at 2 Vendor Offerings: Juniper and Cisco

Transparent (Layer 2) Firewalls: A look at 2 Vendor Offerings: Juniper and Cisco

GIAC GCFW Gold Certification

Author: Matt Austin, net2004eng@yahoo.com

Adviser: Rick Wanner

Accepted: 2008-12-11

Contents

Table of Figures and Tables

1. Abstract

The focus of this paper is to demystify and review how to configure and deploy Juniper and Cisco firewalls in transparent mode. Firewalls configured in transparent mode are also sometimes referred to as bridging, layer-2 or stealth firewalls since they operate at layer 2 of the OSI reference model (Tanase, 2003). Not nearly as popular as layer 3 firewalls (Tyson, 2008), transparent firewalls can offer a wide array of benefits for any organization. So you may be asking yourself, "Why use a transparent firewall?" Well, transparent firewalls can offer solutions to networks where address space is limited, or separation of duties between network and security teams preclude the use of a dynamic routing protocol on security equipment such as your firewall (Tanase, 2003). Some corporations may also find benefits in deploying a transparent firewall in their wireless segments (Koth-arsa,K.., Sanguanpong, S..,Phonphoem,A.., 2008), or for guest networks as well. These are just some of the scenarios where a corporation might find use in deploying a transparent firewall, and the hope is for readers to conjure up other ways they might be able to find benefits in using a transparent firewall in their own network.

2. Introduction

Firewalls are an integral part of any Defense in Depth strategy (May, C..,

Hammerstein, J.., Mattson, J.. Rush, K.., 2008). Presently, firewalls are typically used to provide egress (outgoing) and ingress (incoming) filtering of traffic, whether they are deployed on the perimeter or inside of your network (Chapple, 2003). Although firewalls are not an end all be all, they do provide a preliminary level of mitigation to risk (risk being attackers on the Internet, or anyplace else for that matter) when deployed properly. Firewalls come in many shapes and forms ranging from Web Based Firewalls, Proxy Firewalls, Unified Threat Management (UTM) Devices, and Stateful firewalls (SearchNetworking.com, 2008). Each type has its own strengths and weaknesses, and every organization or individual should consider the specific role they plan to utilize their firewall in, prior to purchasing one.

This paper will provide configuration parameters for both the Juniper and Cisco firewalls, including rulebase configuration, troubleshooting and device hardening. This paper is meant to provide some further insight to those interested in Layer 2 Firewall's, and should not be considered an endorsement plug for either of the vendors referenced in this paper. I chose these vendors in specific since it seems that in my experience, the majority of corporations are using one of these two vendors in their own corporate environments. Both of these vendors have also been rated highly in the Gartner Enterprise Firewall Magic Quadrant, with Juniper recognized as a leader and Cisco being a significant challenger (Young,G.., Pescatore, J.., 2007).

3. Network Design

I will be utilizing the same design and firewall rulebase for each of the firewalls that will be examined. I've included three diagrams below in order to help assist the reader. The first diagram (1. Network Design) consists of the network design which will be referenced throughout this paper. The second (2. Hosts/Networks/Servers) and third (3. Rules to govern user access) diagrams consist of a list of servers and hosts that I will be defining access for, and the general rule definitions we will be applying to each network segment.

1. Network Design

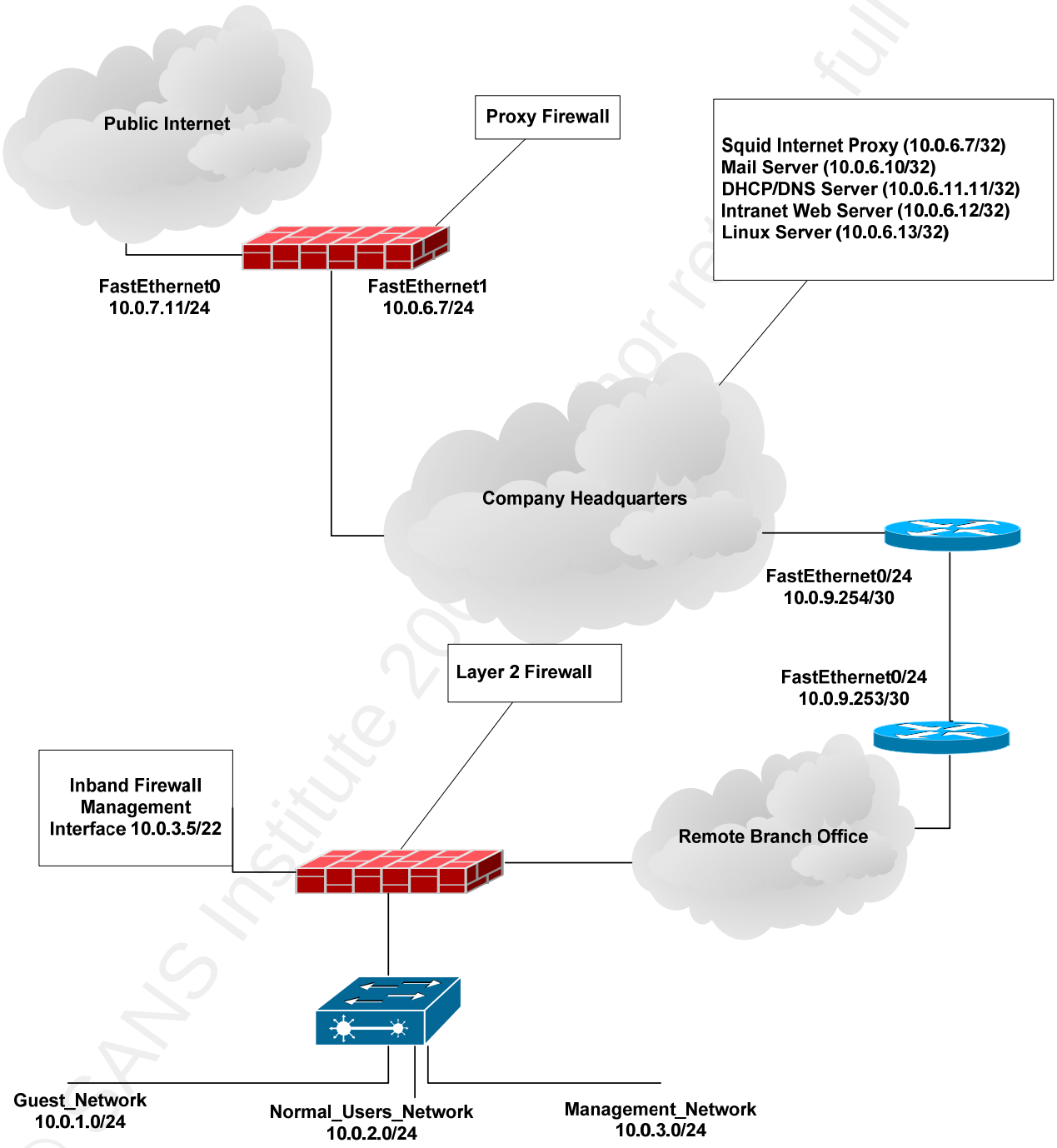


Figure: Reference Network Architecture

2. Hosts/Networks/Servers

Servers/Hosts	Hostname	IP Address or Network	Services Provided
Firewall Management	sans_fw_mgt1.gold.paper	10.0.3.5	TCP22 - SSH, TCP443 - HTTPS
Mail Server (FreeBSD)	mail.gold.paper	10.0.6.10	TCP25 - SMTP, TCP22 - SSH
DNS Server (FreeBSD)	dns1.gold.paper	10.0.6.11	TCP53/UDP53 -DNS
Intranet Web Server (OpenBSD)	web.gold.paper	10.0.6.12	TCP80 - HTTP
Linux Server (Debian Server)	linux.gold.paper	10.0.6.13	TCP22 - SSH, UDP69 - TFTP, TCP80 - HTTP
Squid Internet Proxy (CentOS)	web_proxy.gold.paper	10.0.6.7	TCP3128 - HTTP, TCP443 - HTTPS, TCP22 - SSH
Guest_Network		10.0.1.0/24	
Normal_Users_Network		10.0.2.0/24	
Management_Network		10.0.3.0/24	
Corporate_LAN_Network		10.0.6.0/24	

Table: Hosts, Networks, and Servers

3. Rules to govern user access

Network Name	Source	Destination	Service	Allow/Deny/Log
Guest_Network Rules				
	10.0.1.0/24	10.0.6.7	Squid Proxy -TCP3128	Allow/Log
	10.0.1.0/24	ANY	ALL	Deny/Log
Normal_Users Network Rules				
	10.0.2.0/24	10.0.6.7	Squid Proxy -TCP3128	Allow/Log
	10.0.2.0/24	10.0.6.11	TCP53/UDP53 -DNS	Allow/Log
	10.0.2.0/24	10.0.6.10	TCP25 - SMTP	Allow/Log
	10.0.2.0/24	10.0.6.12	TCP80 - HTTP	Allow/Log
	10.0.2.0/24	ANY	ALL	Deny
Management_Network Rules				
	10.0.3.0/24	10.0.3.5	TCP22 - SSH, TCP443 - HTTPS	Allow/Log
	10.0.3.0/24	10.0.6.10	TCP25 - SMTP, TCP22 - SSH	Allow/Log
	10.0.3.0/24	10.0.6.11	TCP53/UDP53 -DNS	Allow/Log
	10.0.3.0/24	10.0.6.12	TCP80 - HTTP	Allow/Log
	10.0.3.0/24	10.0.6.13	TCP22 - SSH, UDP69 - TFTP, TCP80 - HTTP	Allow/Log
	10.0.3.0/24	10.0.6.7	Squid Proxy -TCP3128, TCP22 - SSH	Allow/Log
	10.0.3.0/24	ANY	ALL	Deny

Table: Access Rules

4. Juniper SSG

4.1. Introduction to the Juniper SSG5

Juniper Networks acquired the Netscreen product line in early 2004 (Juniper Networks, Inc., 2004), out of which the current Secure Services Gateway (SSG) arose. Since this acquisition, a number of appliance based firewalls have been offered by Juniper Networks, of which we will be focusing specifically on their SSG5 platform. This appliance is a stateful firewall built primarily for small to medium sized businesses, but since the code base (ScreenOS) is supported across their entire firewall product line, the larger Enterprise models can support this configuration as well. I'll provide a brief overview of some of the key features

and terminologies associated with Juniper Firewalls, and then elaborate on how to configure the device as a transparent firewall. Lastly, some of the methods available for troubleshooting via the command line will be featured.

4.2. Configuration Parameters necessary for Transparent/Bridge Mode (CLI)

Juniper firewalls introduce a few unique concepts which pertain to their firewall line of products. Prior to discussing the configuration parameters in depth, it's best to get familiar with many of the terms you will see used quite often when people reference Juniper firewalls. Some of these security components are: interfaces, zones, and virtual routers. The physical interface provides connections to specific subnets, for instance a private (your protected network) and public (ISP you connect to on the edge) network. Zones are logical groups which consist of subnets and interfaces. Virtual routers consist of a logical routing construct within the firewall itself (Juniper Networks Inc., 2007). The order of operations when configuring a Juniper firewall is as follows (you can use the pre-defined settings or create your own to suit your environment):

1. Create Virtual Router

2. Add Zone to the Virtual Router

3. Add interface to the Zone

4. Assign an IP address to the Interface

By default, much of this is already pre-configured out of the box. This may not be suitable for your network environment, and many of the settings will have to be changed in order to have a functional firewall in your network. Now let's delve into the objectives necessary in order to get your Juniper up and running as a transparent firewall.

Routing functions performed by the Juniper firewall are done via virtual routers. ScreenOS uses 2 predefined virtual routers, a trust-vr and an untrust-vr. The untrust-vr is typically used for the unprotected zones, where the trust-vr is used for routing in all of your protected zones (Juniper Networks, Inc., 2006). This will remain as default, so nothing needs to be configured for this. Now I will begin by walking you through the process of logging in, changing the default administrative password, and configuring the other parameters that will make the firewall operational in transparent mode. The information provided in this paper will show you how to do this via the command line - while connected via the console.

The first step in configuring the device will require resetting the configuration back to its default settings. This is done by entering the serial number of the device for the login-id and password (see diagram “4A” below).

4A. Reset the Juniper SSG5 to Factory Default Settings

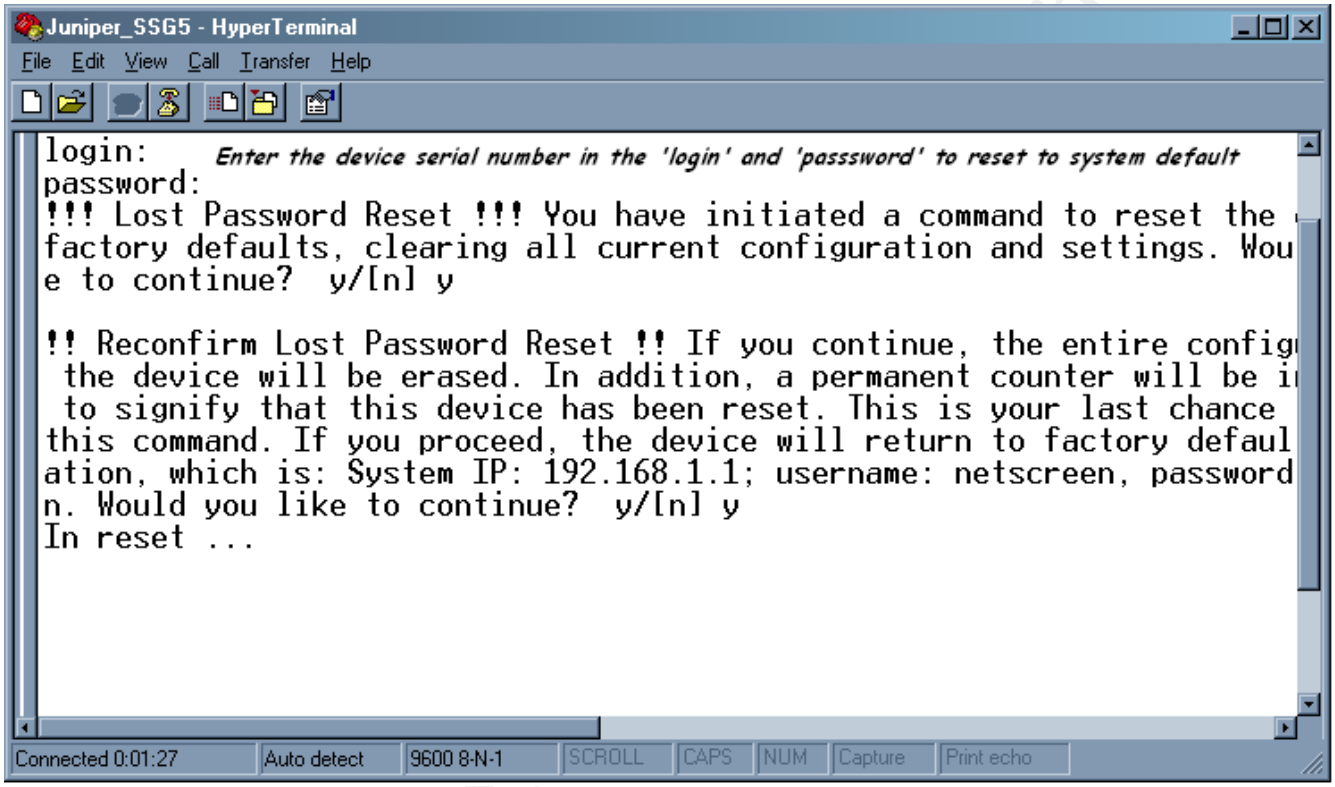


Figure: Juniper Factory Reset

After initially logging in, change the default administrative login ID and password to what you would like. Here the new admin name is 'austinm' who has a local password of 'G!@c_g0ld_p@p3R'. I like to get into the habit of periodically saving my configuration after making changes, so that way if I am arbitrarily disconnected, all my changes aren't lost.

Define the new Administrative Username and Password

set admin name austinm [Define the new admin ID]

set admin password G!@c_g0ld_p@p3R [Set the admin's password]

save [Save the changes to the configuration]

To define the hostname and domain for the firewall, enter the following commands:

Define the hostname and domain

set hostname sans_fw_mgt1 [Define a hostname for the firewall]
set domain gold.paper [Define the domain for the firewall]
save [Save the changes to the configuration]

We are now to the point where we can configure the management settings for the transparent firewall. The management settings will allow you to monitor and connect to the device to make configuration changes and to troubleshoot client connectivity. I'll discuss the commands which are necessary to achieving this in the next few paragraphs.

When using a Juniper firewall in transparent mode, the virtual "vlan1" interface is used for all management functions (Juniper Networks, Inc., 2006). The management IP address is defined by using "set interface vlan1 ip 10.0.3.3/22" and you will need to enable management via that same ip address by setting "set interface vlan1 manageable". The security administrator also needs to define what services will be used to manage the device (ssh, ssl, and ping) when it is operating inline. In addition, I like to "unset" the other services which are not allowed for managing the firewall (web[http], telnet and snmp v1/v2), since they use clear-

text data transmissions. In any instance it is best to try to avoid using these protocols, and instead use a secure alternative such as ssh or ssl, to manage your security infrastructure devices. In order to report on Up/Down status for the firewall, we allow "ping" as a management protocol as well.

Defining the Management Interface, and management options

set interface vlan1 ip 10.0.3.5/22	[Define an IP address for device management]
set interface vlan1 ip manageable	[Allow the device to be managed by the IP you provided]
set interface vlan1 manage ssh	[Allow SSH Management]
set interface vlan1 manage ssl	[Allow SSL Management]
set interface vlan1 manage ping	[Allow ping Management]
unset interface vlan1 manage web	[Disallow HTTP Management]
unset interface vlan1 manage telnet	[Disallow Telnet Management]
unset interface vlan1 manage snmp	[Disallow SNMP Management]
save	[Save the changes to the configuration]

There are 3 other options that should be defined as well: the allowed management ip addresses/network, the self-logging settings, and the method the firewall will use in order to

locate the destination MAC addresses for ARP traffic. The “set admin-manager-ip 10.0.3.0 255.255.255.0” command defines what ip address, or networks, are allowed to manage the device. If someone attempts to connect to the firewall via ssh, and they are connecting from a 10.0.5.9 address, they will be denied access since their network ip address does not fall into the range of addresses which are allowed to manage the device. This traffic can be logged locally (denied and successful connections) by using the “set firewall log-self” command.

Allowing Administrative Users and Self Logging

set admin manager-ip 10.0.3.0 255.255.255.0 [Define the network or host, which is allowed to manage the firewall]

set firewall log-self [Tell the firewall to log traffic which is sent to the device itself]

save [Save the changes to the configuration]

Since this is a transparent firewall, we will need to address how the firewall will respond to ARP traffic it receives for the local network. By default, the firewall is configured to flood all ARP queries it receives, out all network interfaces, in an effort to solicit an ARP reply from the destination machine (Juniper Networks Inc., 2006). This is done when the firewall does not know where the destination MAC address resides (such as which interface it should send traffic out of for the destination MAC address), since it is not in the firewalls MAC address table. When an ARP reply is received, the firewall notes which interface the reply was

received on, and adds an entry in its forwarding table containing the ARP address and interface it was received on. When using the ARP/Traceroute option, a few additional actions take place. Please see the following numbered list for more information (Cameron,R..,Woodberg,B..,Krishnamurthy Madwachar,M..Swarm,M..,Wyler,N.R..,Albers,M..,Bonnell,R.., 2007):

1. MAC address in the initial ARP request is recorded and then the packet is dropped.

2. The Firewall then generates 2 packets: ARP query packet and another for traceroute.

3. The ARP query replaces the source MAC address from the initial packet and instead uses the MAC address of the the VLAN1 interface.

4. The traceroute packet is an ICMP echo request with a TTL of 1.

5. The 2 generated packets are then flooded out to all interfaces, except the one which generated the initial packet.

6. If a reply is found on a device in the same subnet that the packet was originally received in, it learns that MAC and forwards traffic to the applicable interface. If the IP address for the MAC address exists in a different subnet, the trace-route packet returns with the IP address and MAC that the traffic must pass through, and now knows to forward the traffic through that

path.

The ARP/Traceroute method is considered a more secure broadcast method since the initial packet is not flooded out all interfaces. The traceroute option is turned on by default (Cameron,R.et al., 2007).

Address Resolution Protocol Discovery

set interface vlan1 broadcast arp trace-route [Specify that the firewall should use 'arp trace-route' for ARP discovery]

save [Save the changes to the configuration]

There are some other settings that should be noted, which are applicable when the firewall is configured for transparent mode. The first command, "set interface vlan1 bypass-others-ipsec" allows a device to pass IPSec traffic without attempting to terminate it (Juniper Networks Inc., 2006). We would have to build rules to allow this from a source to a specific destination address, but we define this since we will not be creating an IPSec tunnel to the firewall itself. The second command, "unset interface vlan1 bypass-non-ip" prevents non-IP based traffic, such as Appletalk or IPX, from being allowed through the firewall (Juniper Networks Inc., 2006).

Allow IPSEC traffic to pass and disallow non-IP based traffic

set interface vlan1 bypass-others-ipsec [Allow IPSEC traffic to pass through the firewall]

unset interface vlan1 bypass-non-ip [Prevent non-IP based traffic from traversing the firewall]

save [Save the changes to the configuration]

Now onto putting the interfaces into the layer-2 zones they are required to be in for transparent configuration. The first 2 commands put the ethernet0 and ethernet1 interfaces into 2 of the 3 pre-defined layer-2 zones of “V1-Untrust” and “V1-Trust”, the other pre-defined zone “V1-DMZ will not be used (Juniper Networks Inc., 2006). The “V1-Untrust” zone will represent the corporate facing interface, where the “V1-Trust”zone will represent the branch office facing interface. You can create your own zones if you would like, but since these are available by default, I find using these makes configuration tasks a bit easier. The other 2 commands set the interface speed to 100mb and full duplex mode.

Defining the zone membership, speed and duplex settings for the interfaces

set interface "ethernet0/0" zone "V1-Untrust" [Specify which physical interface will be in the layer-2 Untrust zone]

set interface "ethernet0/1" zone "V1-Trust" [Specify which physical interface will be in the layer-2 Trust zone]

set interface ethernet0/0 phy full 100mb [Set the physical interface to Full Duplex and

100mb]

set interface ethernet0/1 phy full 100mb [Set the physical interface to Full Duplex and 100mb]

save [Save the changes to the configuration]

In order to manage the Juniper firewall device via Secure Shell version 2 (SSHv2), there are a couple of commands that we need to enter. You can either enable SSH version 1 or version 2, but not both. Due to the well known vulnerabilities in SSHv1 (Department of Energy, 2001), we will use version 2 on our firewall. There are 2 commands required for this feature to be set and enabled. Also, we enabled Secure Copy (SCP), which can be used to securely transfer files to and from the firewall. SCP uses SSH as its underlying protocol to accomplish this (Pechanec, 2007).

Enable Secure Shell version 2 (SSHv2) management feature and Secure Copy (SCP)

set ssh version v2 [Specify which SSH version will be used for administrative connections – SSH Version 2 is the default]

set ssh enable [Enable the SSH protocol on the firewall]

set scp enable [Allow SCP to be used to transfer files to the firewall]

save [Save the changes to the configuration]

The last piece of the general configuration is to initiate the “unset” command on all other interfaces, and the default bridge group (bgroup0). This puts the interfaces in what Juniper refers to as the “null zone”. The null zone is a placeholder for interfaces that are not

currently bound to a zone (Cameron,R., et al., 2007), and essentially not in use. This helps to clean up much of the default configuration parameters that have been left over. The only thing we have left to complete at this point is to configure our policies for the rulebase, and to discuss some of the options available to us as far as troubleshooting is concerned.

Put unused interfaces into the Null Zone

unset interface bgroup0 port ethernet0/2 [Take the ethernet0/2 interface out of the bridge mode group, since it will not be used]

unset interface bgroup0 port ethernet0/3 [Take the ethernet0/3 interface out of the bridge mode group, since it will not be used]

unset interface bgroup0 port ethernet0/4 [Take the ethernet0/4 interface out of the bridge mode group, since it will not be used]

unset interface bgroup0 port ethernet0/5 [Take the ethernet0/5 interface out of the bridge mode group, since it will not be used]

unset interface bgroup0 port ethernet0/6 [Take the ethernet0/6 interface out of the bridge mode group, since it will not be used]

unset interface wireless0/0 ip [Disable the wireless interface, since we will not be using it]

unset interface bgroup0 ip [Disable the bridge group interface. The other interfaces must be removed from the bridge group, before disabling the bridge group]

unset interface bgroup0 zone [Disable the zone associated with the bridge group]

unset interface wireless0/0 zone [Disable the zone associated with the wireless

zone]

unset interface bri0/0 zone [Disable the zone associated with the bri zone]

save [Save the changes to the configuration]

We can now focus on building our firewall rulebase. The first thing we need to do is to remove the default policy applied from the default configuration. The "unset" command below does this for us:

unset policy id 1 [Remove the default policy]

Now we are in a position to begin configuring our new policy; let's look at how we will accomplish this by illustrating in a few examples. In section 3 "Network Design", the third image provided "3. Rules to govern user access", gives us a guideline concerning what rules we will be creating for each network segment. In the final rulebase, we will have fewer rules to cover all the access depicted, since we will be using groups to consolidate much of this. When a firewall processes rules in the rulebase, it starts with the rules at the top of the rulebase and works down the list, until a match is made and either traffic is allowed, dropped or rejected based on the action. Traffic matches are typically based on the following criteria: source port, source ip address, destination port, and destination ip address; and depending on what other features are purchased or come bundled with the firewall (IPS, AV, or Content Filtering), it may or may not go through a few other checks as well. An example of this would

be filtering the download of all .EXE files sent via HTTP. Juniper Deep Inspection examines Layer 3 and Layer 4 packet headers, as well as Layer 7 application content and protocol characteristics in an effort to detect and prevent any attacks or anomalous behavior that might be present (Juniper Networks Inc., 2006b).

Below I have provided an example of how to create a custom service for web access (for the Squid Proxy) and group for DNS (DNS_UDP_and_TCP). When defining the group, you first need to define the service you want to use (we used custom names here) and then add them to the group name individually.

Creating custom services and service groups on a Juniper SSG5

set service "Squid_Proxy_Port" protocol tcp src-port 1-65535 dst-port 3128-3128 [Define the custom service for “Squid_Proxy_Port”specifying that this is for the tcp protocol, and any source port in the range of 1-65535 is allowed to connect to the destination port of 3128]

set service "DNS_TCP" protocol tcp src-port 1-65535 dst-port 53-53 [Define the custom service for “DNS_TCP”specifying that this is for the tcp protocol, and any source port in the range of 1-65535 is allowed to connect to the destination port of 53]

set service "DNS_UDP" protocol udp src-port 1-65535 dst-port 53-53 [Define the custom service for “DNS_UDP”specifying that this is for the udp protocol, and any source port in the

range of 1-65535 is allowed to connect to the destination port of 53]

set group service "DNS_UDP_and_TCP" add "DNS_TCP" [Define the group "DNS_UDP_and_TCP"and add the custom service of "DNS_TCP"to it]

set group service "DNS_UDP_and_TCP" add "DNS_UDP" [Define the group "DNS_UDP_and_TCP"and add the custom service of "DNS_UDP"to it]

Now onto creating an address object that resides in the "V1-Untrust" the "V1-Trust" zones. When defining new address objects, you need to specify which zone they belong in. So, if we have devices that reside on our protected network, we will have to define it as belonging in that specific zone. The same goes for those objects that reside in the untrusted zone as well.

Creating custom host and network objects, as well as an EXAMPLE "global" object

set address "V1-Untrust" "Mail_Server_10.0.6.10" 10.0.6.10 255.255.255.255 [Here we create a new address, which will reside in the Untrust zone, with a name of "Mail_Server_10.0.6.10". Since this is a single host, we specify the IP address with host subnet mask of 255.255.255.255]

set address "V1-Untrust" "Corporate_LAN_10.0.6.0" 10.0.6.0 255.255.255.0 [Here we create

a new address, which will reside in the Untrust zone, with a name of "Corporate_LAN_10.0.6.0" . Since this is a network object, we specify the subnet mask for it as 255.255.255.0]

set address "V1-Trust" "Guest_Network_10.0.1.0" 10.0.1.0 255.255.255.0 [Here we create a new address, which will reside in the Trust zone this time, with a name of "Guest_Network_10.0.1.0". Since this is a network object, we specify the subnet mask for it as 255.255.255.0]

A full description of all objects created for our rulebase/policy can be found in Appendices A1, A2 and A3. Now that the rules have been created, let's look at some methods used in order to help in troubleshooting connectivity and to validate the device configuration.

4.3. Troubleshooting techniques (Debug, Show and Snoop)

Some Useful Juniper CLI Commands:

---

get config [This command will display the current running configuration on the Juniper Firewall]

get interface [This displays the interfaces, the status (up/down), Zone, IP Address, Name, etc...]

trace-route "ip address" [To perform trace-route to xxx destination]

get policy [To display the current Juniper Policy]

get system [This is great for obtaining the device Serial Number,Software Version,Date and Time, etc...]

WHAT TO USE, SNOOP OR DEBUG?

Snoop provides a layer 2 through layer 4 view of the packet as it comes in and out of the NetScreen interface. You can filter a packet based on source and/or destination IP, source and/or destination port, protocol, and ethernet type, including VLAN tags, and ARPs. Snoop can capture information like frag flags, sequence number, acknowledgement number, TTL, and TOS bit, source and destination IP and port information, as well as ARP request and reply information (Cameron,R.et al., 2007).

Debug flow on the other hand provides information about the packet as it traverses through the interfaces of the NetScreen device. This will take you through the entire flow of

the packet inside the Juniper device. It also provides policy id, session id, source and destination IP and port information, and next hop routes, or where the packet actually came from (Cameron,R.et al., 2007).

NOTE: Juniper has a variety of documents online that cover this in more thorough detail. I recommend that you take a look at their site for more information if you need further assistance. I also provided some of these links in the references section.

SNOOP COMMANDS

set console dbuf [Sends snoop output to dbuf buffer (on by default)]

snoop [Starts the snoop capture]

snoop off [Turns snoop capture off]

snoop info [Displays current snoop status]

snoop detail [Enables full packet logging]

snoop filter [Allows you to filter what gets captured]

clear db [Clears the debug memory buffer]

get dbuf stream [Displays output for analysis]

get dbuf info [This will display what your buffer size is]

SNOOP EXAMPLE:

1. Send snoop output to dbug buffer. Even though this is on by default, this ensures that no-one changed it before you:

set console dbuf

2. Define your snoop filter. Here we are filtering for traffic from source address: 10.0.3.3 (ip src-ip 10.0.3.3), to destination address: 10.0.6. (dst-ip 10.0.6.7), for traffic on TCP (ip-proto 6) port 3128 (dst-port 3128):

snoop filter ip src-ip 10.0.3.3 dst-ip 10.0.6.7 dst-port 3128 ip-proto 6

3. Verify your snoop filter was created successfully (You can define multiple snoop filters and activate one or many at once):

snoop info

4. Enable your snoop filter:

snoop filter id "number of your snoop filter you just created" on

5. Clear the debug buffer - in case something was previously captured

clear dbuf

6. Enable snoop, type "y" to continue

snoop [press Enter]

7. After testing is complete, disable snoop:

snoop off [press Enter]

8. Turn off your filter:

snoop filter id "number of your snoop filter you just created" off

9. View the contents from your snoop capture:

get dbuf stream

10. When you are done, clear or transfer the data via tftp to another location for analysis:

11a. Clearing the Buffer

clear dbuf [press Enter]

11b.Transfer data via tftp to another location for analysis (NOTE: Ensure you have a tftp server installed on the destination machine you would like to transfer the file to). This is taking the contents from the Debug Buffer and sending it to the TFTP Server at "10.0.6.13" with the destination file name of "snoop_capture" and traffic will be originating from the "ethernet0/0" interface.

get dbuf stream > tftp 10.0.6.13 snoop_capture from ethernet0/0

DEBUG EXAMPLE:

1. Send debug output to dbug buffer. Even though this is on by default, this ensures that no-one changed it before you:

set console dbuf

2. Define your debug flow filter. Here we are filtering for traffic from source address: 10.0.3.13

(ip src-ip 10.0.3.13), to destination address: 10.0.6.10 (dst-ip 10.0.6.10), for traffic on port 25 (dst-port 25):

set ffilter src-ip 10.0.3.13 dst-ip 10.0.6.10 dst-port 25

3. Verify the flow filter has been created:

get ffilter

4. Clear the debug buffer - in case something was previously captured

clear dbuf

5. Turn on the debug flow:

debug flow [basic | all | drop]

6. When the traffic has flowed through the firewall, and you need to review the debug output, do the following:

undebug all [pressEnter]

7. If you are done with your flow filter, remove it by issuing the following command:

unset ffilter "id number of filter"

8. To obtain the output from the debug, issue the following command:

get dbuf stream

9. When you are done, clear or transfer the data via tftp to another location for analysis:

10a. Clearing the Buffer

clear dbuf [pressEnter]

10b.Transfer data via tftp to another location for analysis (NOTE: Ensure you have a tftp server installed on the destination machine you would like to transfer the file to). This is taking the contents from the Debug Buffer and sending it to the TFTP Server at "10.0.6.13" with the destination file name of "debug_capture" and traffic will be originating from the "ethernet0/0" interface.

get dbuf stream > tftp 10.0.6.13 debug_capture from ethernet0/0

NOTE: You can use the debug commands to analyze virtually anything on your firewall. Both debug and snoop can be very cpu intensive, so try to be as specific as possible when defining your filters. Also be sure to turn off snoop and debug when you are through with your capture.

4.4. Final Notes on the Juniper SSG5

We've covered a wide variety of options for the Juniper SSG firewall when it is configured to operate as a transparent firewall. There are many more features available, but since this firewall isn't the sole topic of this paper, we didn't cover all the features available for the Juniper firewall. The online documentation is a rich resource for more information about the SSG product and is available online at no cost. This being said, I highly recommend that those who are interested in more information about the product features to consult the online documentation for more specific information.

Other features, such as the built-in IPS (SCREENs) settings can be configured to alert on and prevent network attacks, reconnaissance detection, and to perform rudimentary content filtering (Cameron,R.et al., 2007). These settings are configured specifically for each Zone on the firewall, so if you decide you would like to perform filtering for all traffic coming from the Internet to your network, you can enable this in the Internet facing Zone. This does increase processing time and utilizes more system resources, but the benefits typically outweigh the drawbacks to using such features. This is something each organization needs to determine for themselves.

As far as enterprise management goes, Juniper also offers the Network and Security

Manager (NSM) for managing all enterprise firewalls, Intrusion Detection and Prevention (IDP) devices, routers, switches and soon the Secure Access Gateway (SSL VPN) devices as well (Juniper Networks Inc., 2008) . The NSM is advantageous to those organizations which have a large number of Juniper devices to manage. From one central location, you can perform role-based administrative access to all Juniper infrastructure gear, and do all changes from one location. For anyone who has tried to manage a large number of firewalls without a central management platform, you can understand the benefits of using a device like the NSM.I provided some screenshots and a further explanation of the NSM in Appendix A3.

5. Cisco ASA 5505

5.1. Introduction to Cisco ASA 5505

Cisco Systems, Inc. has been a prominent world leader in network technology for over 2 decades. Founded in 1984 (Cisco Systems Inc., 2008a), they have grown to become a leading provider for router and switch technology, and continue to forge ahead with other cutting edge products in the wireless and security markets. Cisco acquired the PIX Firewall when they purchased Network Translation - in November of 1995 (Coile, 2003) - and have since been more actively involved in building a competitive security portfolio of products.

This portion of the paper will focus on the Cisco Adaptive Security Appliance (ASA), which is to replace the Cisco PIX Appliance, which has reached end-of-sale/end-of-life (Cisco Systems Inc., 2008b).

5.2. Configuration Parameters necessary for Transparent/Bridge Mode (CLI)

Cisco ASA and PIX devices utilize security levels, which range from 0 (lowest) to 100 (highest), which are assigned to each network interface. The lower the security level, for instance 0, the less secure the interface is presumed to be. So by default, Cisco assigns the outside interface a security level of 0, while the inside interface is assigned a security level of 100. Also by default, traffic is allowed to traverse the firewall from a higher security interface to a lower security interface. Traffic from a lower security level interface (such as the outside interface at 0) is not allowed to pass to a higher security interface (such as the inside interface with a security level of 100) (Cisco Systems Inc., 2008d). We will be using access-lists to define what traffic is allowed to traverse from the "inside" interface to the "outside" interface.

Before starting, another important point to bring up is the various configuration modes available when configuring a Cisco device. I've included a diagram (Cisco Systems Inc., 2008e) below to help you get started with learning the configuration modes, since we will be entering and exiting these modes quite often. All commands I display will assume the

reader is in privileged exec mode, and has logged into the firewall successfully already. I'll provide directives in the paper to help the reader along, for those unfamiliar with configuring Cisco devices.

Table 5A: Cisco Command Mode Summary

Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	Switch>	Enter logout or quit.	Use this mode to: 1.Change terminal settings. 2.Perform basic tests. 3.Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Switch#	Enter disable or exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.

Global configuration	While in privileged EXEC mode, enter the configure command.	Switch(config)#	To exit to privileged EXEC mode, enter exit or end, or press Ctrl-Z.	Use this mode to configure parameters that apply to the entire switch.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Switch(config-if)#	To exit to global configuration mode, enter exit. To return to privileged EXEC mode, press Ctrl-Z or enter end.	Use this mode to configure parameters for the Ethernet interfaces.

Table: Cisco Command Mode Summary

In order to configure the Cisco ASA as a transparent firewall, we will initiate the following command "firewall transparent" from global configuration mode. The Cisco ASA can be configured as either a transparent mode firewall or a routed mode firewall (Cisco Systems Inc., 2008f). By default, it is configured to operate in routed mode. Once you change the mode, the running configuration is cleared and the firewall must be reloaded. At which point we can begin configuring other parameters on our firewall which pertain to transparent operation.

Placing the ASA in Transparent Mode

configuration terminal [Enter global configuration mode]

firewall transparent [Configure the ASA for Transparent mode]

end [Exit configuration mode]

reload [Reboot the firewall to make the changes permanent]

After the firewall has reloaded, we can configure passwords for basic authentication. When configuring Cisco devices you have 2 passwords to configure; the login (User EXEC) and enable (Privileged EXEC) passwords. We also will be defining a local user database to restrict which administrators are authorized to login and manage the device.

After entering global configuration mode, we change the login password to "User_EXEC_P@55w0rd", which by default is “cisco” (depending on what version of code you are running)(Cisco Systems Inc., 2008g). We then change the previously unset privileged exec password to "Priv_EXEC_P@55w0rd". Exit out of the current configuration mode by typing "end" from our global configuration session, and you will return to privileged exec mode. We will save the running configuration to the startup configuration "copy running-configuration startup-configuration", so next time the device is rebooted, the changes we made will remain intact. Just like the "save" command when using Juniper devices, if we forget to save the configuration and the device is inadvertently rebooted, all our changes will be lost. Another method is to use the "write memory" command which accomplishes the same

thing, and saves on a little typing. I like to make a habit of doing this frequently as well (I will use both commands: "write memory" and “copy running-configuration startup-configuration" interchangeably in this paper). So for the time being, anyone who attempts to login to the device will be required to enter 2 passwords for access - one for normal User access and another for Privileged access.

Create User and Privileged EXEC Passwords

(Remember, all commands will take into account that the user has already entered privileged EXEC mode with level 15 access rights)

configure terminal [Enter global configuration mode]

passwd User_EXEC_P@55w0rd [Define the User login password]

enable password Priv_EXEC_P@55w0rd [Define the Privileged mode password]

end [Exit configuration mode]

copy running-configuration startup-configuration [Save the changes that were made to the running configuration (active configuration) to the startup configuration (which is loaded on system start)]

Now let’s define the local user database in order to define a more restrictive access policy. When creating a user-id, you can specify what level of access the user has

been granted. We will grant the user "austinm" full access rights (privilege 15). There are 16 privilege levels, with level 15 being the most privileged and level 0 being the lowest. You can customize these levels by defining what commands are allowed to be ran from which specific access levels (for example you could create a custom level 5 which would allow users with this privilege level to initiate "configure", "ping" or "route" commands) (Cisco Systems, Inc., 2008h).

Once the user has been defined we need to apply user authentication and authorization controls. Cisco uses triple AAA services, which respectively stand for: Authentication, Authorization and Accounting. The only 2 options that we will be using are authentication and authorization. We require the username/password combination to be validated by the local user database prior to allowing access to either enable mode or access to the device via ssh.

Local Admin Account Creation and Authentication Requirements

configure terminal [Enter global configuration mode]

username austinm password G!@c_g0ld_p@p3R privilege 15 [Define a local administrator “austinm”with a password of “G!@c_g0ld_p@p3R”and with the highest privilege level of 15]

aaa authentication enable console LOCAL [Define local authentication to be required for enable mode access. The local user database will be used for authentication]

aaa authentication ssh console LOCAL [Define local authentication to be required for ssh access. The local user database will be used for authentication]

end [Exit configuration mode]

write memory [Save the configuration changes. Write memory is the same as initiating the “copy running-configuration startup-configuration]

Below you will find the appropriate commands to use for configuring the hostname on the ASA and the domain name for the device.

Define Cisco ASA Hostname and Domain

configuration terminal [Enter global configuration mode]

hostname sans-fw-mgt1 [Define a hostname for the firewall]

domain-name giac.gold [Define the domain for the firewall]

end [Exit configuration mode]

write memory [Save the device configuration]

In order to manage the ASA, we must assign an IP address to the device in global configuration mode. The security appliance uses this IP address as the source address

for packets that originate on the security appliance, such as system messages or AAA communications. The IP address, must be on the same network as the downstream and upstream routers, and cannot use a host address mask (255.255.255.255) (Cisco Systems Inc., 2008).

Define the Management IP Address

configuration terminal	[Enter global configuration mode]
ip address 10.0.3.5 255.255.252.0	[Define the management IP address]
end	[Exit configuration mode]
write memory	[Save the device configuration]

Since we are using SSH version 2 to manage the firewall, we will need to define what hosts/networks are allowed to connect via SSH. A RSA key pair needs to be generated in order to support this, as well as to support SSL and IPSEC connections. When users connect via SSH from the 10.0.3.0/24 network for administration, they will need to use this key. Ensure that you have defined the domain name and hostname for the ASA prior to initiating this command.

Configure and Enable SSH Management Access

conf t [Enter global configuration mode]

crypto key generate rsa modulus 2048 [Here we generate a RSA key, which is sent to the SSH server, by the client to encrypt the SSH session key. This is required for SSH.]

ssh 10.0.3.0 255.255.255.0 inside [Define what host/network is allowed to access the ASA via SSH, and via what interface]

ssh version 2 [Enable SSH Version 2 Management]

end [Exit configuration mode]

copy run start [Save the device configuration]

With the Cisco ASA Firewall, you are limited to using only 2 interfaces for passing traffic when the device is operating in transparent mode. Since the management interface has already been configured, we can configure these 2 interfaces now. The Virtual Local Area Network (VLAN) interfaces must be configured first. We will create 2 VLANs: 2 and 3, and then assign the VLANs to our physical interfaces. Once we enter VLAN configuration mode, we need to name the interfaces by using the "nameif" command, and then have to define the security level for each specific VLAN "security-level" (we discussed the security levels previously, but as a reminder, a security level of 100 is considered the most secure, where 0 is the least secure). After doing this, we issue the command "no

shutdown" which changes the administrative status of the VLAN from Down to Up.

VLAN Configuration and naming the interfaces

config t	[Enter global configuration mode]
interface Vlan2	[Enter VLAN 2 Configuration Mode]
nameif inside	[Provide a name for the interface]
security-level 100	[Define the security level for the VLAN -100 is highest]
no shutdown	[Set the interface to be administratively 'UP']
exit	[Exit out of VLAN2 Configuration Mode]
interface Vlan3	[Enter VLAN 2 Configuration Mode]
nameif outside	[Provide a name for the interface]
security-level 0	[Define the security level for the VLAN - 0 is the least trusted]
no shutdown	[Set the interface to be administratively 'UP']
end	[Exit configuration mode]
write mem	[Save the device configuration]

Once the VLANs have been configured, we need to assign the 2 physical network interfaces to these VLANs. In order to do this, just issue the "switchport access vlan "the VLAN number that you want to put the interface in"" to put the physical interface in the VLAN you want. I also added a description to each interface (I encourage the reader to use descriptions in their own configurations as well, in order to document what has been done and why).

Placing the Physical Interfaces in their respective VLAN

conf t	[Enter global configuration mode]
interface ethernet0/1	[Enter ethernet0/1 configuration mode]
description Inside Interface - Protected Network	[Provide a description for the interface]
switchport access vlan 2	[Assign vlan2 to the interface]
no shutdown	[Set the interface to be administratively 'UP']
exit	[Exit out of ethernet0/1configuration mode]
interface ethernet0/0	[Enter ethernet0/0 configuration mode]
description Outside Interface - Corporate Network	[Provide a description for the interface]

switchport access vlan 3 [Assign vlan3 to the interface]

no shutdown [Set the interface to be administratively 'UP']

end [Exit configuration mode]

write mem [Save the device configuration]

ARP Spoofing is a method used by attackers to impersonate other hosts or routers on a network; ARP Inspection helps to prevent this (Cisco Systems Inc., 2008j). Cisco firewalls use 2 methods for dealing with ARP traffic; they can either flood or not flood the ARP packet out all interfaces. If neither the MAC nor IP address is found in the ARP table on the firewall, the firewall can flood the ARP packet out all interfaces in order to discover the host. If you select to not flood the packet, a static mapping will need to be present for the packet to be passed. We will keep the default, which is to flood, but depending on the network environment, you may want to set up static ARP entries on your firewall instead, which is more secure, but can be an administrative nightmare to maintain.

Enable ARP Inspection

configuration terminal [Enter global configuration mode]

arp-inspection inside enable flood [Enable arp inspection on the inside interface]

arp-inspection outside enable flood [Enable arp inspection on the outside interface]

end [Exit configuration mode]

write mem [Save the device configuration]

Let's now look at how to configure object-groups and service-objects for use in our rulebase (Cisco Systems Inc., 2008k). Just as I did in the Juniper SSG section, I will provide examples of how to create a host and service object, as well as one firewall rule. All other rules can be found in "Appendix B2 – Layer-2 Cisco Configuration Explained".

For the Juniper SSG5, we created services for the Squid Proxy and DNS; let's do the same here. Like most of the other configuration tasks, we create these while in global configuration mode. For all object-groups, you will need to specify "object-group", then whether you would like to define a group of "icmp-type", "network", "protocol" or "service". We will be defining a service object, which is used for defining TCP/UDP ports/services. Next you need to specify the name of the object, in our case "Squid_Proxy_Port" and "DNS_UDP_and_TCP", and lastly the protocol or protocols that this will cover "tcp" and "tcp-udp" ,respectively. Once you enter the object configuration mode, you must specify the destination port, or range of ports, for this object to match. Since Squid by default uses port 3128, we will define this port to be used in our "Squid_Proxy_Port" object. For DNS, "domain" is a pre-defined service name, and we will select this in order to match on any TCP/UDP port

53 packets. When specifying an ACL entry, you must also specify the protocol; we went ahead and created a protocol object group "TCP_and_UDP" which covers both tcp and udp, for usage with DNS traffic.

Creating custom services and service groups on a Cisco ASA

configuration terminal [Enter global configuration mode]

object-group service Squid_Proxy_Port tcp [Define a tcp service object group for the custom “Squid_Proxy_Port”]

description Squid Proxy Service [Give a description for the service]

port-object eq 3128 [Define what the port for our service will be]

exit [Exit object-group configuration mode]

object-group service DNS_UDP_and_TCP tcp-udp [Define a tcp and udp service object group for the custom “DNS_UDP_and_TCP”group]

description DNS Services for TCP and UDP [Give a description for the service]

port-object eq domain [Define what the port for our service will be. Here we are using the pre-defined service name for DNS.]

exit [Exit object-group configuration mode]

object-group protocol TCP_and_UDP [Define a tcp and udp protocol object group for

the custom “TCP_and_UDP”protocol group]

protocol-object tcp [Use the pre-defined protocol for tcp “tcp”]

protocol-object udp [Use the pre-defined protocol for udp “udp”]

end [Exit configuration mode]

write config [Save the device configuration]

In order to create host/network objects we follow pretty much the same steps as we performed in our last task of creating service groups, but we instead use the "network" object-group option. Let's look at our first example, we are creating a custom network object for our management network, and naming it as such "Management_Network_10.0.3.0". We provide an adequate description for the object, and then define the network address with the following "network-object 10.0.3.0 255.255.255.0". You may also add a host address here as well. For instance, if you wanted to create an object containing a host ip address of "1.1.1.1" you could enter "network-object 1.1.1.1 255.255.255.255" or "network-object host 1.1.1.1" as well. You are able to add both the host and network entry in one object-group, under separate line entries. Next we look at how we can nest other object groups. By using the same process as before, you just need to add the previously created network object-groups by name, using the "group-object" command. I know some of you may be thinking that this looks like we are creating a bigger headache than necessary (adding groups to groups, all these port objects,

etc...), but this can really help in minimizing the rules in your rulebase. In the long run, this will actually make life much easier administrative wise, so long as someone takes the time to document it!

Creating custom host and network objects

configuration terminal [Enter global configuration mode]

object-group network Management_Network_10.0.3.0 [Create a network object for the Management Network]

description Network Management Network [Provide a description for the group]

network-object 10.0.3.0 255.255.255.0 [Define the actual network IP address and subnet mask]

exit [Exit object-group configuration mode]

object-group network Remote_Site_Networks [Create a network object for all the remote site networks]

description 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24 [Provide a description for the group]

group-object Management_Network_10.0.3.0 [Add the object that was defined for the Management Network]

group-object Normal_Users_Network_10.0.2.0 [Add the object that was defined for the

Normal Users Network]

group-object Guest_Network_10.0.1.0 [Add the object that was defined for the Guest Network]

end [Exit configuration mode]

write config [Save the device configuration]

Now let's configure our rulebase, which will consist of a named access list applied to our Ethernet interfaces. Keep in mind that 2 types of access lists may be used when configuring a Cisco transparent firewall. One type can be for IP based traffic, and one can be for non-IP traffic, called an Ethertype access list (Cisco Systems Inc., 2008l). You may have one of each applied to an interface (so 2 total applied to one interface), but since we don't plan on allowing IPX, Appletalk, or any other non-IP based traffic, we will only be using the IP based access list. All our access lists will be “extended named access lists”, which allow us to specify the source and destination IP addresses. After entering global configuration mode, we need to type in "access-list", and then the name we want to use for the access list, here being "inside_to_outside" (which I am using to depict the direction that this access list will be applied for). Next we specify that this will be an "extended" access-list, and we would like to "permit" traffic. We then have to specify the protocol object group we previously created "TCP_and_UDP", followed by the source group "Remote_Site_Networks"

(IP Range/Group initiating traffic), then the destination "DNS_Server_10.0.6.11" (IP Range/Group receiving traffic), and finally the service "DNS_UDP_and_TCP" and we'll specify that we want to log on this rule.

Building the Access Control List

configure terminal [Enter global configuration mode]

access-list inside_to_outside extended permit object-group TCP_and_UDP object-group Remote_Site_Networks object-group DNS_Server_10.0.6.11 object-group DNS_UDP_and_TCP log [This creates our first entry in the access-list. We use a named access list of “inside_to_outside”which indicates the direction that this traffic is to filter. Since we are defining a source and destination in our access-list, we must use an “extended”access-list. We want to allow the traffic, so we add the “permit” statement. Next step is to specify the protocol to use, but instead of an individual protocol such as icmp/udp/tcp, I will use the protocol group, “TCP_and_UDP” which covers both the tcp and udp protocols for us. Next we define the source of the traffic, and the “Remote_Site_Networks”object will be used; and we will follow with the destination server object we created, “DNS_Server_10.0.6.11”. Next we define the service(s) allowed, “DNS_UDP_and_TCP”and lastly we will enable logging “log” for this rule.]

Lastly, we have to apply our completed ACL to an interface, via an access-

group, in order to enforce our policy. If you fail to perform this task, the access-list will not be enforced on the firewall. First we have to enter the interface configuration by issuing "interface ethernet0/1" and "interface ethernet0/0" respectively. After, use the "access-group" command followed by the named access control list we created, and apply the ACL in the direction "in" we expect to inspect traffic from (so inside_to_outside will be inspecting traffic which is coming into [ingress] the interface we named "inside" earlier, from the Remote Network Side). We then specify the interface we named earlier "interface inside".

Applying the Access Lists

conf t	[Enter global configuration mode]
interface ethernet0/1	[Enter ethernet0/1 configuration mode]
access-group inside_to_outside in interface inside	[Apply the access-list – via the access-group command – to the interface]
end	[Exit configuration mode]
interface ethernet0/0	[Enter ethernet0/0 configuration mode]
access-group outside_to_inside in interface outside	[Apply the access-list – via the access-group command – to the interface]

end [Exit configuration mode]

write config [Save the device configuration]

Now that we have successfully built a transparent firewall, let's look at some ways we can to troubleshoot and verify the configuration of our firewall. I've included a short list of some helpful debug and show commands, and have a more exhaustive list provided in the URL reference below.

5.3. Troubleshooting techniques (Debug and Show)

Useful Cisco ASA CLI Debug and Show Commands:

debug mac-address-table [Enables debugging messages for the MAC Address Table]

debug arp-inspection [Debugs ARP inspection for ARP Spoofing]

show running-config [Show the running configuration. This may be abbreviated with "sh run"]

show run object-group [To view all the object groups that have been created]

show firewall [Validate what mode the firewall is running in - your output should

indicate Transparent]

show version [Validate what version your running, how much memory you have, the serial number, among many other useful items]

show conn all [Display all connections to and in the firewall state table]

show interfaces [View interface statistics, as to the traffic sent/received, whether an interface is up/down]

show logging all [Displays all system log message IDs, along with whether they are enabled or disabled (Cisco Systems Inc., 2008j)]

show mac-address-table [Display all MAC Address entries on the Firewall]

show access-lists [Display all access-lists for discrepancies]

5.4. Final Notes on the Cisco ASA 5505

Configuring the Cisco ASA for transparent mode operation is a pretty straightforward process. Just like the Juniper configuration, only 2 physical interfaces can be used to configure a Cisco firewall in transparent mode. Also briefly covered are some of the methods available to use for troubleshooting connectivity to and through the firewall.

Some of the additional features - such as virtualization with contexts - are not available

in the ASA 5505 model (Cisco Systems Inc., 2008m). For a small home or branch office, you may not require many of the additional features such as virtualization with multiple contexts, but that is for each company to decide on their own. I strongly encourage those considering purchasing an ASA 5505 to consult the Model Comparison Guide (Cisco Systems Inc., 2008m), prior to making a purchase.

Cisco offers the Cisco Security Manager platform for managing Cisco routers, switches, IDS/IPS and firewalls. Similar to the Juniper NSM, you can manage all your devices from this platform, by providing IOS/OS updates, signature updates for IDS/IPS, VPN Management, etc...As with the Juniper NSM, I provided some screenshots below for those who would like an introduction to the CSM.

Summary

This paper has covered 2 prominent firewall vendors, with a discussion and guide to configuring the devices in transparent mode. The reason I focused on these 2 vendor devices is because both are deployed in many corporate network environments, they require only 2 physical interfaces and an IP address on the device for management purposes. The network management IP address must be on the same subnet that you are bridging though. If cost is a problem for your organization, you might want to consider some of the Open Source options

(*BSD, and many Linux flavors) that are freely available (Adamo, Massimiliano., Tablo, Mauro., 2005); if not, you might want to look into CheckPoint (both with and without Nokia Hardware) (CheckPoint Software Technologies LTD., 2008), or other higher end models from Cisco and Juniper. As with anything you're deploying, you should consider the skillset of your administrative staff when making a purchase, since you want them to be able to configure, support and troubleshoot the device you're deploying.

Let's discuss a few of the caveats associated with deploying Cisco and Juniper transparent firewalls. Neither support running a dynamic routing protocol, since it is bridging traffic. You can configure the firewall to pass routing protocols such as BGP, OSPF, and RIP, but the device itself cannot participate in the routing process. You are unable to use the firewall for NAT/PAT functions either, since it is not a layer 3 device in your network. Troubleshooting can be made difficult, depending on the size of your network, since there is no layer-3 hop (remember traffic is being bridged) to identify your firewall in the network. If you're looking to bridge 2 different networks, the use of a transparent firewall can be ruled out as well, since the management ip address must be on the same subnet as the 2 interconnecting devices. The firewall is still vulnerable to attacks, since it does have an IP address on the subnet it's deployed on.

It is much easier to introduce a transparent firewall into your network, rather than

having to readdress your network infrastructure to accommodate a layer-3 firewall, which can be administratively intensive (Tanase, 2003). The transparent firewall may also be introduced into environments where your network team may want to use routing protocols to pass traffic, but the firewall team doesn't support routing protocols on their devices. With a transparent firewall, you can choose to have them route the way they want, and allow the routing protocols to traverse the firewall, but not participate in the routing process itself. The firewall still performs stateful inspection on packets it receives, but is not seen as a layer-3 network device like firewalls deployed in more traditional roles.

Depending on the goals your organization is looking to achieve by deploying a firewall, there are strong arguments for and against transparent firewalls. I've only discussed a few arguments for and against them, and after deploying a few myself, I can see the reasoning why an organization might want to deploy one in their network, and why they might not. Just like all security technologies, firewalls have come a long way and rather than just being a stateful layer 3/4 filtering device, they can now support such features as web filtering, IDS/IPS functionality, anti-virus and SPAM mitigation, to name a few. As the field advances, not just firewalls, but routers and other network devices have already begun to support these same features as well (Cisco and Juniper to mention 2). I hope the reader found this paper of use, and if there are any questions related to using this technology, I'd be glad to answer any

questions that you might have.

8. References

Tanase, Matthew. (2003, October 15). Security Focus: Transparent, Bridging Firewall Devices. Retrieved December 4, 2008, Web site: http://www.securityfocus.com/infocus/1737

Tyson, Jeff. (2008). How OSI Works. HowStuffWorks.com. Retrieved December 5, 2008, from Web Site: http://computer.howstuffworks.com/osi.htm

Koth-arsa,K.., Sanguanpong, S..,Phonphoem,A..(2008, January 23). Transparent Firewall for Wireless Network. Retrieved December 4, 2008, from Web Site: http://www.apan.net/meetings/hawaii2008/presentations/security/kasom.ppt

Chapple, Mike. (2003, March 4). SearchSecurity.com. Egress Filtering. Retrieved December 4, 2008, from Web Site: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci883409,00.html#

SearchNetworking.com. (2008, January 2). SearchNetworking.com. Introduction to firewalls: Types of firewall. Retrieved December 4, 2008, from Web Site: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1282044,00.html

Young, G.., Pescatore, J.. (2007, September 13). Gartner: Magic Quadrant for Enterprise Network Firewalls, 2H07 [ID Number: G00151129].

Juniper Networks, Inc. (2006b). Technical Documentation: ScreenOS Software Documentation: Concepts & Examples ScreenOS Reference Guide: Vol 4, Attack Detection and Defense Mechanisms. Retrieved 2008, December 1, from Juniper Networks Inc. Web Site: http://www.juniper.net/techpubs/software/screenos/screenos5.4.0/CE_v4.pdf

Juniper Networks, Inc. (2004, February 9). Juniper Networks, Inc. To Acquire Netscreen Technologies Inc.. Retrieved 2008, October 16, from Juniper Networks Inc. Web site: http://www.juniper.net/company/presscenter/pr/2004/pr-040209.html

Juniper Networks, Inc. (2007). Configuring Juniper Networks Firewall/IPSec VPN Products Student Guide, Revision 6.a. USA: Juniper Networks, Inc..

Juniper Networks, Inc. (2006, July 31). Technical Documentation: ScreenOS Software Documentation: Concepts & Examples ScreenOS Reference Guide: Vol 2, Fundamentals. Retrieved 2008, December 1, from Juniper Networks Inc. Web Site: http://www.juniper.net/techpubs/software/screenos/screenos5.4.0/CE_v2.pdf

Cameron,R..,Woodberg,B..,Krishnamurthy Madwachar,M..Swarm,M..,Wyler,N.R..,Albers,M..,Bonnell,R.. (2007). Configuring Juniper Networks NetScreen & SSG Firewalls. Rockland,MA: Syngress Publishing Inc..

Department of Energy, (2001, October 16). M-017: Multiple SSH Version 1 Vulnerabilities. Retrieved October 23, 2008, Web site: http://www.ciac.org/ciac/bulletins/m-017.shtml

Pechanec, Jan (2007, July 9). How the SCP protocol works - Jan Pechanec's weblog [Web]. Retrieved December 5, 2008, from Web Site: http://blogs.sun.com/janp/entry/how_the_scp_protocol_works

Juniper Networks, Inc. (2008). Juniper Networks. Network and Security Manager - Control Network Security Management. Retrieved December 4, 2008, from Web Site: http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/netscreen_security_manager/index.html

Cisco Systems Inc. (2008a). News@Cisco -> Fact Sheet. Retrieved October 23, 2008, from Cisco Fact Sheet Web site: http://newsroom.cisco.com/dlls/corpinfo/factsheet.html

Coile, Brantley, (2003). Configuring L2TP Connections. A History of the PIX. Retrieved December 3, 2008, from Web Site: http://home.cfl.rr.com/dealgroup/pix/pix_page_history.htm

Cisco Systems Inc. (2008b). Cisco PIX 500 Series Security Appliances: End-of-Life and End-of-Sales. Retrieved October 23, 2008, from End-of-Life and End-of-Sale Notices, Web Site: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_eol_notices_list.html

Cisco Systems Inc. (2008c). Cisco ASA Getting Started Guide, 8.0 – Configuring the Adaptive Security Appliance. Retrieved October 27, 2008, from Configuring the Adaptive Security Appliance, Web Site: http://www.cisco.com/en/US/docs/security/asa/asa80/getting_started/asa5500/quick/guide/setup.html

Cisco Systems Inc. (2008d). Cisco Security Appliance Command Line Configuration Guide, Version 7.1 – Configuring Interface Parameters. Retrieved December 3, 2008, from Web Site: http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/intparam.html

Cisco Systems, Inc. (2008e). Catalyst 2950 Desktop Switch Software Configuration Guide, 12.1 (9) EA1 - Cisco Systems. Using the Command Line Interface. Retrieved: October 25, 2008, from Using the Command Line Interface, Web site: http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swcli.html

Cisco Systems Inc. (2008f). Cisco Security Appliance Command Line Configuration Guide,

Version 7.2 – Firewall Mode Overview. Retrieved December 3, 2008, from Web Site: http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/fwmode.html

Cisco Systems Inc. (2008g). Cisco Security Appliance Command Line Configuration Guide, Version 7.1 – Monitoring and Troubleshooting. Retrieved December 2, 2008, from Web Site: http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/trouble.html#wp1058131

Cisco Systems, Inc. (2008h). How to assign Privilege Levels with TACACS+ and RADIUS - Cisco Systems. Retrieved: October 26, 2008, from Web Site: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008009465c.shtml

Cisco Systems Inc. (2008i, September 26).PIX/ASA: Transparent Firewall Configuration Example. Retrieved December 4, 2008, from Web Site: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a008089f467.shtml

Cisco Systems, Inc. (2008j) Cisco Security Appliance Command Line Configuration Guide, Version 7.2: Configuring ARP Inspection and Bridging Parameters. Retrieved: October 26, 2008, from Web Site: http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/bridgarp.html

Cisco Systems Inc. (2008k, September 26). Using and Configuring PIX/ASA/FWSM Object Groups. Retrieved December 3, 2008, from Web Site: www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a00800d641d.shtml

Cisco Systems Inc. (2008l). Cisco Security Appliance Command Line Configuration Guide,

Version 8.0 - Permitting or Denying Network Access. Retrieved: December 1, 2008, from Web Site: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/nwaccess.html

Cisco Systems Inc. (2008m). Cisco ASA 5500 Series Adaptive Security Appliances. Retrieved December 3, 2008, from Web Site: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

Adamo, Massimiliano., Tablo, Mauro. (2005, December). Linux vs. OpenBSD - A Firewall Performance Test. Retrieved December 3, 2008, from Web Site http://www.usenix.org/publications/login/2005-12/pdfs/adamo.pdf

CheckPoint Software Technologies LTD. (2008). CheckPoint Software: VPN-1 Power VSX. Retrieved December 3, 2008, from Web Site: http://www.checkpoint.com/products/vpn-1_power_vsx/

Appendix A1: Juniper Final Configuration

```
get conf
Total Config size 5914:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set service "Squid_Proxy_Port" protocol tcp src-port 1-65535 dst-port 3128-3128
set service "DNS_UDP" protocol udp src-port 1-65535 dst-port 53-53
set service "DNS_TCP" protocol tcp src-port 1-65535 dst-port 53-53
set alg appleichat enable
unset alg appleichat re-assembly enable
set alg sctp enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "austinm"
set admin password "nDG8KGrlJ9yOczXHysXOZBItD0PAHn"
```

```
set admin auth web timeout 10
set admin auth dial-in timeout 3
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
```

```
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface ethernet0/0 phy full 100mb
set interface ethernet0/1 phy full 100mb
set interface "bri0/0" zone "Null"
set interface "ethernet0/0" zone "V1-Untrust"
set interface "ethernet0/1" zone "V1-Trust"
set interface "wireless0/0" zone "Null"
set interface "bgroup0" zone "Null"
set interface vlan1 ip 10.0.4.251/29
set interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface vlan1 ip manageable
set flow tcp-mss
unset flow no-tcp-seq-check
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set domain gold.paper
set hostname sans_fw_mgt1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "V1-Trust" "Guest_VLAN_10.0.5.0" 10.0.5.0 255.255.255.128
```

```
set address "V1-Trust" "Management_Network_10.0.4.0" 10.0.4.0 255.255.255.128
set address "V1-Trust" "Normal_Users_VLAN_10.0.3.0" 10.0.3.0 255.255.255.128
set address "V1-Untrust" "Corporate_LAN_10.0.6.0" 10.0.6.0 255.255.255.0
set address "V1-Untrust" "DNS_Server_10.0.6.11" 10.0.6.11 255.255.255.255
set address "V1-Untrust" "Intranet_Web_Server_10.0.6.12" 10.0.6.12 255.255.255.255
set address "V1-Untrust" "Linux_TFTP_10.0.6.13" 10.0.6.13 255.255.255.255
set address "V1-Untrust" "Mail_Server_10.0.6.10" 10.0.6.10 255.255.255.255
set address "V1-Untrust" "Squid_Proxy_10.0.6.7" 10.0.6.7 255.255.255.255
set group address "V1-Trust" "Management_Normal_Networks"
set group address "V1-Trust" "Management_Normal_Networks" add "Management_Network_10.0.4.0"
set group address "V1-Trust" "Management_Normal_Networks" add "Normal_Users_VLAN_10.0.3.0"
set group address "V1-Trust" "Remote_Site_Networks"
set group address "V1-Trust" "Remote_Site_Networks" add "Guest_VLAN_10.0.5.0"
set group address "V1-Trust" "Remote_Site_Networks" add "Management_Network_10.0.4.0"
set group address "V1-Trust" "Remote_Site_Networks" add "Normal_Users_VLAN_10.0.3.0"
set group service "DNS_UDP_and_TCP"
set group service "DNS_UDP_and_TCP" add "DNS_TCP"
set group service "DNS_UDP_and_TCP" add "DNS_UDP"
set group service "TFTP_SSH_HTTP"
set group service "TFTP_SSH_HTTP" add "HTTP"
set group service "TFTP_SSH_HTTP" add "SSH"
set group service "TFTP_SSH_HTTP" add "TFTP"
set ike respond-bad-spi 1
set ike ikev2 ike-sa-soft-lifetime 60
```

```
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set url protocol websense
exit
set policy id 1 from "V1-Untrust" to "V1-Trust"  "Any" "Any" "ANY" deny log
set policy id 1
exit
set policy id 2 from "V1-Trust" to "V1-Untrust"  "Management_Normal_Networks" "DNS_Server_10.0.6.11" "DNS_UDP_and_TCP" permit log
set policy id 2
exit
set policy id 3 from "V1-Trust" to "V1-Untrust"  "Remote_Site_Networks" "Squid_Proxy_10.0.6.7" "Squid_Proxy_Port" permit log
set policy id 3
```

```
exit
set policy id 4 from "V1-Trust" to "V1-Untrust"  "Management_Normal_Networks" "Mail_Server_10.0.6.10" "SMTP" permit log
set policy id 4
exit
set policy id 5 from "V1-Trust" to "V1-Untrust"  "Management_Normal_Networks" "Intranet_Web_Server_10.0.6.12" "HTTP" permit log
set policy id 5
exit
set policy id 6 from "V1-Trust" to "V1-Untrust"  "Management_Network_10.0.4.0" "Squid_Proxy_10.0.6.7" "SSH" permit log
set policy id 6
exit
set policy id 7 from "V1-Trust" to "V1-Untrust"  "Management_Network_10.0.4.0" "Linux_TFTP_10.0.6.13" "TFTP_SSH_HTTP" permit log
set policy id 7
exit
set policy id 8 from "V1-Trust" to "V1-Untrust"  "Any" "Any" "ANY" deny log
set policy id 8
exit
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set ssh enable
set scp enable
set config lock timeout 5
unset license-key auto-update
set wlan 0 channel auto
set wlan 1 channel auto
```

```
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
sans_fw_mgt1->     get conf
Total Config size 6095:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set service "Squid_Proxy_Port" protocol tcp src-port 1-65535 dst-port 3128-3128
set service "DNS_TCP" protocol tcp src-port 1-65535 dst-port 53-53
set service "DNS_UDP" protocol udp src-port 1-65535 dst-port 53-53
set alg appleichat enable
unset alg appleichat re-assembly enable
set alg sctp enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
```

```
set admin name "austinm"
set admin password "nDG8KGrlJ9yOczXHysXOZBItD0PAHn"
set admin manager-ip 10.0.3.0 255.255.255.0
set admin auth web timeout 10
set admin auth dial-in timeout 3
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface ethernet0/0 phy full 100mb
set interface ethernet0/1 phy full 100mb
set interface "bri0/0" zone "Null"
set interface "ethernet0/0" zone "V1-Untrust"
set interface "ethernet0/1" zone "V1-Trust"
```

```
set interface "wireless0/0" zone "Null"
set interface "bgroup0" zone "Null"
set interface vlan1 ip 10.0.3.5/22
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface vlan1 ip manageable
unset interface vlan1 manage telnet
unset interface vlan1 manage snmp
unset interface vlan1 manage web
set flow tcp-mss
unset flow no-tcp-seq-check
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set domain gold.paper
set hostname sans_fw_mgt1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "V1-Trust" "Guest_Network_10.0.1.0" 10.0.1.0 255.255.255.0
set address "V1-Trust" "Management_Network_10.0.3.0" 10.0.3.0 255.255.255.0
set address "V1-Trust" "Normal_Users_Network_10.0.2.0" 10.0.2.0 255.255.255.0
set address "V1-Untrust" "Corporate_LAN_10.0.6.0" 10.0.6.0 255.255.255.0
set address "V1-Untrust" "DNS_Server_10.0.6.11" 10.0.6.11 255.255.255.255
set address "V1-Untrust" "Intranet_Web_Server_10.0.6.12" 10.0.6.12 255.255.255.255
set address "V1-Untrust" "Linux_TFTP_10.0.6.13" 10.0.6.13 255.255.255.255
set address "V1-Untrust" "Mail_Server_10.0.6.10" 10.0.6.10 255.255.255.255
set address "V1-Untrust" "Squid_Proxy_10.0.6.7" 10.0.6.7 255.255.255.255
set group address "V1-Trust" "Management_Normal_Networks"
set group address "V1-Trust" "Management_Normal_Networks" add "Management_Network_10.0.3.0"
set group address "V1-Trust" "Management_Normal_Networks" add "Normal_Users_Network_10.0.2.0"
set group address "V1-Trust" "Remote_Site_Networks"
set group address "V1-Trust" "Remote_Site_Networks" add "Guest_Network_10.0.1.0"
set group address "V1-Trust" "Remote_Site_Networks" add "Management_Network_10.0.3.0"
```

```
set group address "V1-Trust" "Remote_Site_Networks" add "Normal_Users_Network_10.0.2.0"
set group service "DNS_UDP_and_TCP"
set group service "DNS_UDP_and_TCP" add "DNS_TCP"
set group service "DNS_UDP_and_TCP" add "DNS_UDP"
set group service "TFTP_SSH_HTTP"
set group service "TFTP_SSH_HTTP" add "HTTP"
set group service "TFTP_SSH_HTTP" add "SSH"
set group service "TFTP_SSH_HTTP" add "TFTP"
set ike respond-bad-spi 1
set ike ikev2 ike-sa-soft-lifetime 60
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set url protocol websense
exit
set policy id 1 from "V1-Untrust" to "V1-Trust"  "Any" "Any" "ANY" deny log
set policy id 1
exit
set policy id 2 from "V1-Trust" to "V1-Untrust"  "Management_Normal_Networks" "DNS_Server_10.0.6.11" "DNS_UDP_and_TCP" permit log
set policy id 2
exit
set policy id 3 from "V1-Trust" to "V1-Untrust"  "Remote_Site_Networks" "Squid_Proxy_10.0.6.7" "Squid_Proxy_Port" permit log
set policy id 3
```

```
exit
set policy id 4 from "V1-Trust" to "V1-Untrust"  "Management_Normal_Networks" "Mail_Server_10.0.6.10" "SMTP" permit log
set policy id 4
exit
set policy id 5 from "V1-Trust" to "V1-Untrust"  "Management_Normal_Networks" "Intranet_Web_Server_10.0.6.12" "HTTP" permit log
set policy id 5
exit
set policy id 6 from "V1-Trust" to "V1-Untrust"  "Management_Network_10.0.3.0" "Squid_Proxy_10.0.6.7" "SSH" permit log
set policy id 6
exit
set policy id 7 from "V1-Trust" to "V1-Untrust"  "Management_Network_10.0.3.0" "Linux_TFTP_10.0.6.13" "TFTP_SSH_HTTP" permit log
set policy id 7
exit
set policy id 8 from "V1-Trust" to "V1-Untrust"  "Any" "Any" "ANY" deny log
set policy id 8
exit
set firewall log-self
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set ssh enable
set scp enable
set config lock timeout 5
unset license-key auto-update
set wlan 0 channel auto
set wlan 1 channel auto
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
exit
set vrouter "untrust-vr"
exit
```

```
set vrouter "trust-vr"
exit
sans_fw_mgt1->
```

Appendix A2: Layer-2 Juniper Configuration Explained

Explanation of Command Line Arguments that were added/changed/removed:

set admin name austinm	(This defines the new administrator username)
set admin password G!@c_g0ld_p@p3R	(This will define the new administrator's password)
set hostname sans_fw_mgt1	(Defines the hostname for the device)
set domain gold.paper	(Define the domain name for the device)
set interface vlan1 ip 10.0.3.5/22	(Define an IP Address for Management purposes - only for Transparent Mode configuration)
set interface vlan1 ip manageable	(Sets the IP Address for VLAN1 to be its management IP Address)
set interface vlan1 manage ssh	(Allow management via the SSH service)
set interface vlan1 manage ssl	(Allow management via the SSL service)
set interface vlan1 manage ping	(Allow device to respond to ping)
set interface vlan1 broadcast arp trace-route	
set interface vlan1 bypass-others-ipsec	(Allows IPSec traffic to pass through the firewall, if allowed by a rule.)
unset interface vlan1 bypass-non-ip	(Prevents non-IP traffic to pass through a Juniper firewall in Transparent mode, with the exception of ARP)
unset interface vlan1 manage web	(Removes the ability to manage the firewall via http)
unset interface vlan1 manage telnet	(Removes the ability to manage the firewall via telnet)
unset interface vlan1 manage snmp	(Removes the ability to manage the firewall via snmp)
set admin manager-ip 10.0.3.0 255.255.255.0	(Specifies IP address or networks, which are allowed to connect to the management interface)
set firewall log-self	(Log traffic sent to the firewall IP itself. This consists of snmp, ping's, ssh, etc...)
set interface "ethernet0/0" zone "V1-Untrust"	(Adds interface ethernet0/0 to the V1-Untrust Zone)
set interface "ethernet0/1" zone "V1-Trust"	(Adds interface ethernet0/1 to the V1-Trust Zone)
set interface ethernet0/0 phy full 100mb	(Statically defines speed and duplex for Ethernet0/0)
set interface ethernet0/1 phy full 100mb	(Statically defines speed and duplex for Ethernet0/1)
set ssh version v2	(Utilize SSH version 2, rather than version 1. You can only use 1 of the 2)
set ssh enable	(Enable SSH for system management)
set scp enable	(Enable Secure Copy in order to transfer files to/from the firewall using the SSH protocol)
unset interface bgroup0 port ethernet0/2	(Remove the ability to bridge interface ethernet0/2. You can bridge multiple interfaces so they behave as one.)

unset interface bgroup0 port ethernet0/3	(Remove the ability to bridge interface ethernet0/3. You can bridge multiple interfaces so they behave as one.)
unset interface bgroup0 port ethernet0/4	(Remove the ability to bridge interface ethernet0/4. You can bridge multiple interfaces so they behave as one.)
unset interface bgroup0 port ethernet0/5	(Remove the ability to bridge interface ethernet0/5. You can bridge multiple interfaces so they behave as one.)
unset interface bgroup0 port ethernet0/6	(Remove the ability to bridge interface ethernet0/6. You can bridge multiple interfaces so they behave as one.)
unset interface wireless0/0 ip	(Removes default IP settings for wireless connectivity)
unset interface bgroup0 ip	(Remove default IPaddress originally assigned to the Bridge Group)
unset interface bgroup0 zone	(Removes zone membership for Bridge Group Interface)
unset interface wireless0/0 zone	(Removes zone membership for Wireless Interface)
unset interface bri0/0 zone	(Removes zone membership for the bri0/0 interface)
unset policy id 1	(Removes the default firewall policy (the term rule is synonymous with policy in Juniper talk) allowing full access)

Services Defined (All others are pre-defined)

set service "Squid_Proxy_Port" protocol tcp src-port 1-65535 dst-port 3128-3128	Service created for Squid Default port "3128"
set service "DNS_TCP" protocol tcp src-port 1-65535 dst-port 53-53	Serivce for TCP DNS - We defined TCP DNS since a UDP DNS message is limited to 512 bytes long
set service "DNS_UDP" protocol udp src-port 1-65535 dst-port 53-53	Service for UDP DNS - Normal lookups (nslookup, dig, host) for the most part
set group service "DNS_UDP_and_TCP" add "DNS_TCP"	Adding the DNS_TCP service to the DNS group
set group service "DNS_UDP_and_TCP" add "DNS_UDP"	Adding the DNS_UDP service to the DNS group
set group service "TFTP_SSH_HTTP" add "TFTP"	Add the TFTP Service (UDP69) which is a pre-defined service to our "TFTP_SSH_HTTP" group
set group service "TFTP_SSH_HTTP" add "SSH"	Add the SSH Service (TCP22) which is a pre-defined service to our "TFTP_SSH_HTTP" group
set group service "TFTP_SSH_HTTP" add "HTTP"	Add the HTTP Service (TCP80) which is a pre-defined service to our "TFTP_SSH_HTTP" group

Hosts/Networks and Group Definitions

set address "V1-Trust" "Normal_Users_Network_10.0.2.0" 10.0.2.0 255.255.255.0	Address definition for the Normal Users Network of 10.0.2.0/24 in the V1-Trust Zone
set address "V1-Trust" "Management_Network_10.0.3.0" 10.0.3.0 255.255.255.0	Address definition for the Management Network of 10.0.3.0/24 in the V1-Trust Zone
set address "V1-Trust" "Guest_Network_10.0.1.0" 10.0.1.0 255.255.255.0	Address definition for the Guest Network of 10.0.1.0/24 in the V1-Trust Zone

set address "V1-Untrust" "Corporate_LAN_10.0.6.0" 10.0.6.0 255.255.255.0	Address definition for the Corporate LAN of 10.0.6.0/24 in the V1-Untrust Zone
set address "V1-Untrust" "DNS_Server_10.0.6.11" 10.0.6.11 255.255.255.255	Address definition for the DNS Server at 10.0.6.11 in the V1-Untrust Zone
set address "V1-Untrust" "Squid_Proxy_10.0.6.7" 10.0.6.7 255.255.255.255	Address definition for the Squid Proxy Server at 10.0.6.7 in the V1-Untrust Zone
set address "V1-Untrust" "Mail_Server_10.0.6.10" 10.0.6.10 255.255.255.255	Address definition for the Mail Server at 10.0.6.10 in the V1-Untrust Zone
set address "V1-Untrust" "Intranet_Web_Server_10.0.6.12" 10.0.6.12 255.255.255.255	Address definition for the Intranet Web Server at 10.0.6.12 in the V1-Untrust Zone
set address "V1-Untrust" "Linux_TFTP_10.0.6.13" 10.0.6.13 255.255.255.255	Address definition for the Linux TFTP Server at 10.0.6.13 in the V1-Untrust Zone
set group address "V1-Trust" "Management_Normal_Networks" add "Normal_Users_Network_10.0.2.0"	Create the "Management_Normal_Networks" group and add the Normal Users VLAN object to it
set group address "V1-Trust" "Management_Normal_Networks" add "Management_Network_10.0.3.0"	Create the "Management_Normal_Networks" group and add the Management Network object to it
set group address "V1-Trust" "Remote_Site_Networks" add "Normal_Users_Network_10.0.2.0"	Create the "Remote_Site_Networks" group and add the Normal Users VLAN object to it
set group address "V1-Trust" "Remote_Site_Networks" add "Management_Network_10.0.3.0"	Create the "Remote_Site_Networks" group and add the Management Network object to it
set group address "V1-Trust" "Remote_Site_Networks" add "Guest_Network_10.0.1.0"	Create the "Remote_Site_Networks" group and add the Guest VLAN object to it

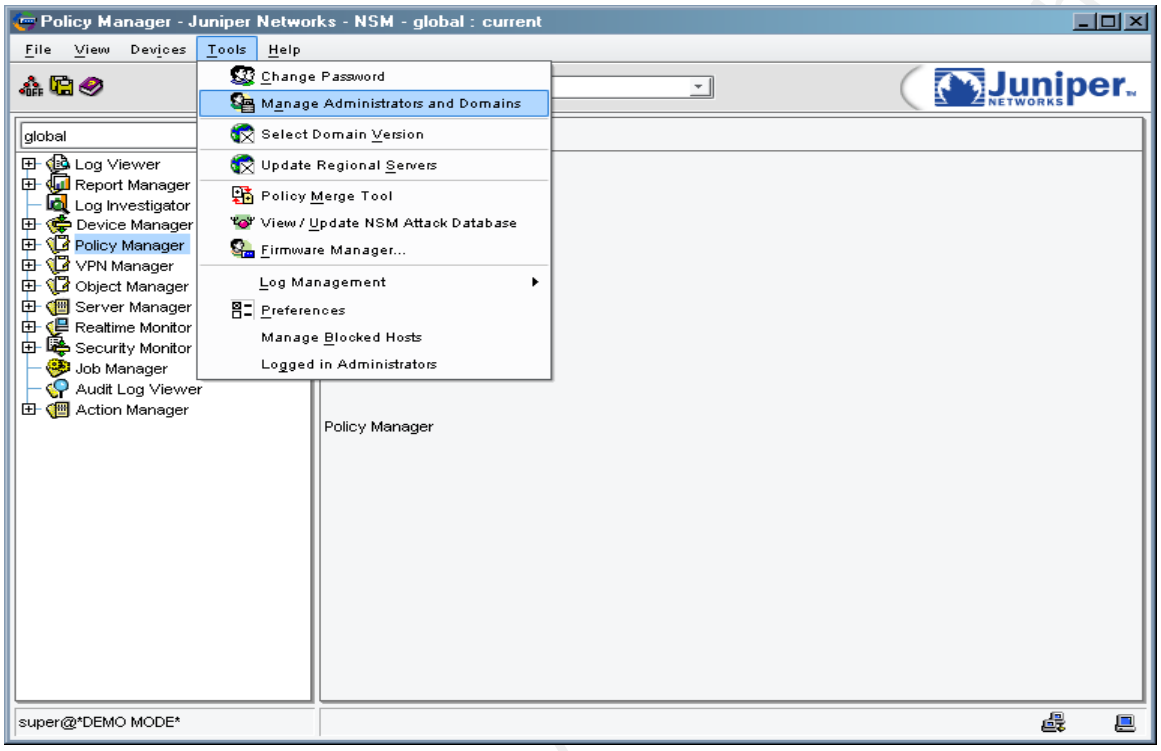
Active Rulebase

set policy id 1 from "V1-Untrust" to "V1-Trust" "ANY" "ANY" "ANY" deny log	Deny any traffic sourced from the Untrust Zone with a Destination of the Trust Zone
set policy id 2 from "V1-Trust" to "V1-Untrust" "Management_Normal_Networks" "DNS_Server_10.0.6.11" "DNS_UDP_and_TCP" permit log	Allow our Management networks to perform DNS queries to our DNS server, log this as well
set policy id 3 from "V1-Trust" to "V1-Untrust" "Remote_Site_Networks" "Squid_Proxy_10.0.6.7" "Squid_Proxy_Port" permit log	Allow our Remote Site Networks group to access the squid proxy for web access, log it as well (you might consider not logging http traffic if you anticipate a high volume of traffic)
set policy id 4 from "V1-Trust" to "V1-Untrust" "Management_Normal_Networks" "Mail_Server_10.0.6.10" "SMTP" permit log	Allow our Management and Normal user networks to connect to the mail server in order to send mail, log traffic as well
set policy id 5 from "V1-Trust" to "V1-Untrust" "Management_Normal_Networks" "Intranet_Web_Server_10.0.6.12" "HTTP" permit log	Allow our Management and Normal user networks to connect to the Intranet Webserver in order to view corporate headlines for employees, log traffic as well
set policy id 6 from "V1-Trust" to "V1-Untrust" "Management_Network_10.0.3.0" "Squid_Proxy_10.0.6.7" "SSH" permit log	Allow only the Management Network to connect via SSH to the Squid Proxy for administration, log this access
set policy id 7 from "V1-Trust" to "V1-Untrust" "Management_Network_10.0.3.0" "Linux_TFTP_10.0.6.13" "TFTP_SSH_HTTP" permit log	Allow only the Management Network to connect via SSH, and HTTP to the designated multi purpose TFTP server. This rule will also allow router and switch configuration files to be sent to the server for backup and auditing purposes.
set policy id 8 from "V1-Trust" to "V1-Untrust" "ANY" "ANY" "ANY" deny log	Deny any traffic not explicitly permitted

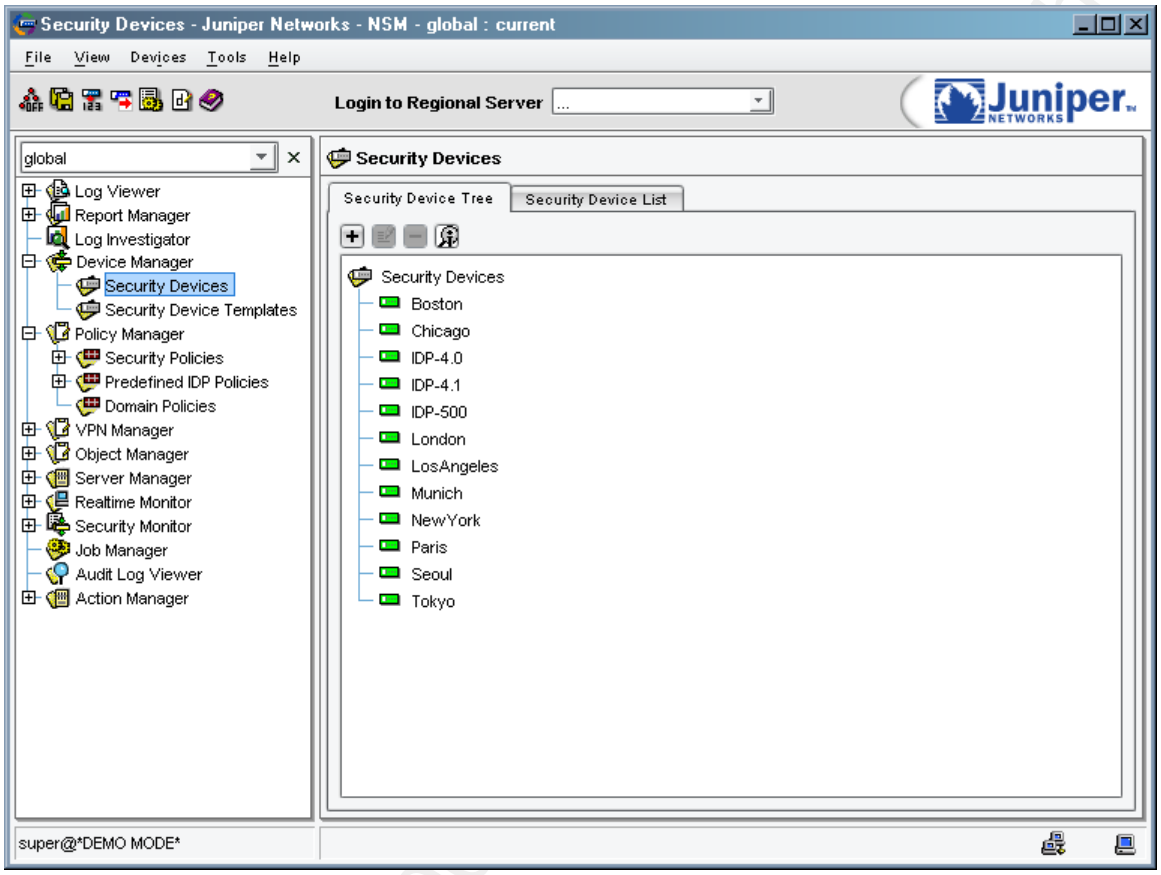
Appendix A3: Juniper NSM

The Juniper Network Security Manager (NSM) allows security administrators to centrally manage virtually all Juniper devices from one platform. You are able to house firmware versions for device updates, provide global objects for use across all your devices (great for common rules and objects used throughout your network), and define role based access to allow granular access to only specific resources that you may want to provide access to (for instance, log viewing capabilities only for Auditor access). The NSM provides a wide variety of options for those looking to gain a foothold on their network/security infrastructure.

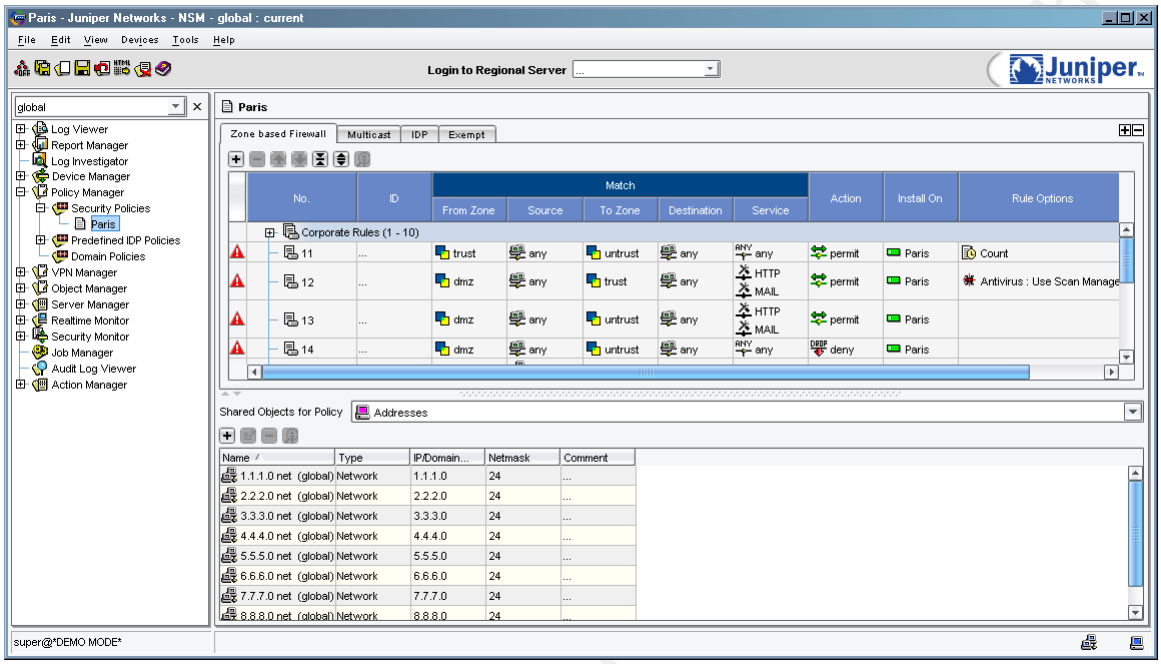
After initially logging in to the Juniper NSM, you may select the following menu option to add new devices to be managed “Tools ->Manage Administrators and Domains”



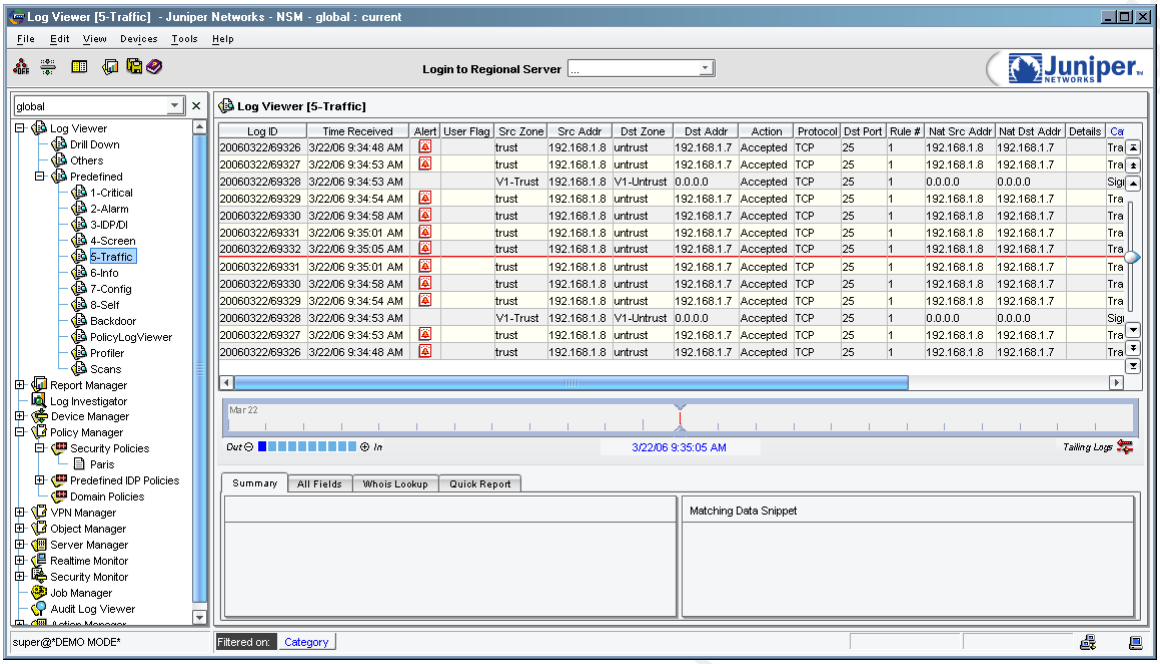
Under “Security Devices” you can define the settings for your device: IP Addresses, SNMP settings, administrator access, etc…This is where you would add a new firewall for your organization, and assign a policy to the device.



As for defining the firewall policy, you can do this by accessing “Policy Manager -> Security Policies.” If you have any global domain policies (policies that are defined under the “global” domain, which are applicable to the devices you choose) you can view these here as well.



The last part I am going to briefly cover is the traffic log viewer “Log Viewer -> Predefined -> Traffic.” From this option, you can view all the rules which you currently log on for the domain you are in. This will show you the zones the traffic traversed, source/destination IP addresses, service and the timestamp for the traffic.



I only provided a very brief overview of some of the options available to you in NSM. Juniper provides an exhaustive amount of options available to the security administrator via NSM. The Security Manager can be run on Solaris or Red Hat Linux server platforms (please see the release notes for specifics concerning specifications). For those managing a large amount of Juniper devices in their organization, I strongly encourage you to look into what this product has to offer for your organization.

Appendix B1: Cisco Final Configuration

Cisco Final Configuration for Layer 2 Firewall

```
: Saved
:
ASA Version 7.2(3)
!
firewall transparent
hostname sans-fw-mgt1
domain-name giac.gold
enable password Ctc8IVa8CxYZQbPa encrypted
names
!
interface Vlan1
 no nameif
 no security-level
!
interface Vlan2
 nameif inside
 security-level 100
!
interface Vlan3
 nameif outside
 security-level 0
!
interface Ethernet0/0
 description Outside Interface - Corporate Network
 switchport access vlan 3
!
interface Ethernet0/1
```

```
 description Inside Interface - Protected Network
 switchport access vlan 2
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 shutdown
!
passwd DXkE2Ge44h8jN886 encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name giac.gold
object-group service Squid_Proxy_Port tcp
 description Squid Proxy Service
 port-object eq 3128
object-group service DNS_UDP_and_TCP tcp-udp
 description DNS Services for TCP and UDP
 port-object eq domain
object-group protocol TCP_and_UDP
 description TCP and UDP Services
```

```
 protocol-object tcp
 protocol-object udp
object-group service HTTP tcp
 description Hyper Text Transfer Protocol
 port-object eq www
object-group service SMTP tcp
 description Simple Mail Transport Protocol
 port-object eq smtp
object-group service TFTP udp
 description TFTP Service for File Transfer
 port-object eq tftp
object-group service SSH_HTTP tcp
 description SSH and HTTP Services
 port-object eq ssh
 port-object eq www
object-group icmp-type ping
 description Allow Ping for Management Networks
 icmp-object echo
 icmp-object echo-reply
object-group network Normal_Users_Network_10.0.2.0
 description Normal User Access
 network-object 10.0.2.0 255.255.255.0
object-group network Corporate_LAN_10.0.6.0
 description Corporate Network
 network-object 10.0.6.0 255.255.255.0
object-group network Guest_Network_10.0.1.0
 description Normal Network Access
 network-object 10.0.1.0 255.255.255.0
object-group network Management_Network_10.0.3.0
 description Network Management Network
 network-object 10.0.3.0 255.255.255.0
object-group network Remote_Site_Networks
 description 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24
```

```
 group-object Management_Network_10.0.3.0
 group-object Normal_Users_Network_10.0.2.0
 group-object Guest_Network_10.0.1.0
object-group network Management_Normal_Networks
 description Normal User and Management Networks
 group-object Management_Network_10.0.3.0
 group-object Normal_Users_Network_10.0.2.0
object-group network Mail_Server_10.0.6.10
 description Internal SMTP Mail Server
 network-object host 10.0.6.10
object-group network Squid_Proxy_10.0.6.7
 description Squid Proxy Server
 network-object host 10.0.6.7
object-group network DNS_Server_10.0.6.11
 description DNS Server for all clients
 network-object host 10.0.6.11
object-group network Intranet_Web_Server_10.0.6.12
 description Intranet Web Server
 network-object host 10.0.6.12
object-group network Linux_TFTP_10.0.6.13
 description Host for TFTP, SSH and HTTP
 network-object 10.0.6.13 255.255.255.255
access-list inside_to_outside extended permit tcp object-group Remote_Site_Networks object-group Squid_Proxy_10.0.6.7 object-group Squid_Proxy_Port log
access-list inside_to_outside extended permit tcp object-group Management_Normal_Networks object-group Mail_Server_10.0.6.10 object-group SMTP log
access-list inside_to_outside extended permit tcp object-group Management_Normal_Networks object-group Intranet_Web_Server_10.0.6.12 object-group HTTP
log
access-list inside_to_outside extended permit tcp object-group Management_Network_10.0.3.0 object-group Squid_Proxy_10.0.6.7 eq ssh log
access-list inside_to_outside extended permit tcp object-group Management_Network_10.0.3.0 object-group Linux_TFTP_10.0.6.13 object-group SSH_HTTP log
access-list inside_to_outside extended permit udp object-group Management_Network_10.0.3.0 object-group Linux_TFTP_10.0.6.13 object-group TFTP log
access-list inside_to_outside extended deny ip any any log
access-list outside_to_inside extended deny ip any any log
pager lines 24
mtu inside 1500
mtu outside 1500
```

```
ip address 10.0.3.5 255.255.252.0
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group inside_to_outside in interface inside
access-group outside_to_inside in interface outside
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 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
aaa authentication enable console LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh 10.0.3.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
```

```
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
arp-inspection inside enable flood
arp-inspection outside enable flood
username austinm password dvdf.CB7MK/P25gh encrypted privilege 15
prompt hostname context
Cryptochecksum:e4543b96e5bbf39779a930fdfd0d5fdd
: end
sans-fw-mgt1(config)#
```

Appendix B2: Layer-2 Cisco Configuration Explained

Command	Explanation	Mode Issued In
Explanation of Command Line Arguments that were added/changed/removed:		
firewall transparent	(Place the Cisco ASA into Transparent Firewall Mode - remember to reboot after)	Global
passwd User_EXEC_P@55w0rd	(Set the login password.)	Global
enable password Priv_EXEC_P@55w0rd	(Set the enable password for Privileged Exec Access.)	Global
username austinm password G!@c_g0ld_p@p3R privilege 15	(Define user "austinm" with a password of "G!@c_g0ld_p@p3R" with level 15 privilege)	Global
aaa authentication enable console LOCAL	(Require the user to be authenticated locally when entering "enable" mode)	Global
aaa authentication ssh console LOCAL	(Require user authentication when connecting via SSH)	Global
hostname sans-fw-mgt1	(Create the hostname for the Firewall - Required for SSH access)	Global
domain-name giac.gold	(Define the Doman Name for the firewall - Required for SSH access)	Global
ip address 10.0.3.5 255.255.252.0	(Define the Management IP Address for the Firewall)	Global
interface Vlan2	(Enter VLAN 2 Configuration Mode)	Global
nameif inside	(Provide a name "inside" for the Vlan2 interface)	Interface-Mode
security-level 100	(Define the security-level for the VLAN - 100 is the highest security level)	Interface-Mode
no shutdown	(Set VLAN 2 as administratively UP)	Interface-Mode
interface Vlan3	(Enter VLAN 3 Configuration Mode)	Global
nameif outside	(Provide a name "outside" for the Vlan3 interface)	Interface-Mode
security-level 0	(Define the security-level for the VLAN - 0 is the lowest security level)	Interface-Mode
no shutdown	(Set VLAN 3 as administratively UP)	Interface-Mode
interface ethernet0/1	(Enter interface "ethernet0/1" configuration mode)	Global
description Inside Interface - Protected Network	(Provide a description of the function for this interface)	Interface-Mode
switchport access vlan 2	(Assign the physical interface to VLAN2 - The Inside Interface)	Interface-Mode
no shutdown	(Set "ethernet0/1" as administratively UP)	Interface-Mode
interface ethernet0/0	(Enter interface "ethernet0/0" configuration mode)	Global

description Outside Interface - Corporate Network	(Provide a description of the function for this interface)	Interface-Mode
switchport access vlan 3	(Assign the physical interface to VLAN3 - The Outside Interface)	Interface-Mode
no shutdown	(Set "ethernet0/0" as administratively UP)	Interface-Mode
crypto key generate rsa modulus 2048	(Generates a Key for use when IPSEC,SSH, and SSL Connections are made to the firewall)	Global
ssh 10.0.3.0 255.255.255.0 inside	(Define what hosts/network are allowed to connect to the ASA via SSH)	Global
ssh version 2	(Specify the SSH version allowed)	Global
arp-inspection inside enable flood	(Enable ARP Inspection on the inside interface, and allow addresses to be learned by flooding)	Global
arp-inspection outside enable flood	(Enable ARP Inspection on the outside interface, and allow addresses to be learned by flooding)	Global

Services Groups Defined

object-group service Squid_Proxy_Port tcp	(Define a tcp service object-group for the Squid Proxy Port (3128))	Global
description Squid Proxy Service	(Provide a description for the service)	Object-Mode
port-object eq 3128	(Specify what port it equals - 3128)	Object-Mode
object-group service DNS_UDP_and_TCP tcp-udp	(Define a tcp/udp service object-group for DNS)	Global
description DNS Services for TCP and UDP	(Provide a description for the service)	Object-Mode
port-object eq domain	(Specify what port it equals - domain [pre-defined as domain for UDP/TCP53)	Object-Mode
object-group protocol TCP_and_UDP	(Define a protocol object-group for TCP and UDP)	Global
description TCP and UDP Services	(Provide a description for this protocol)	Object-Mode
protocol-object tcp	(Define the object for TCP)	Object-Mode
protocol-object udp	(Define the object for UDP)	Object-Mode
object-group service HTTP tcp	(Define a tcp service object-group for HTTP)	Global
description Hyper Text Transfer Protocol	(Provide a description for the service)	Object-Mode
port-object eq www	(Specify what port it equals - www [pre-defined as www for TCP port 80)	Object-Mode
object-group service SMTP tcp	(Define a tcp service object-group for SMTP - mail)	Global
description Simple Mail Transport Protocol	(Provide a description for the service)	Object-Mode
port-object eq smtp	(Specify what port it equals - smtp [pre-defined as smtp for TCP port 25)	Object-Mode
object-group service TFTP udp	(Define a udp service object-group for TFTP - Trivial File Transfer Protocol)	Global
description TFTP Service for File Transfer	(Provide a description for the service)	Object-Mode

port-object eq tftp	(Specify what port it equals - tftp [pre-defined as tftp for UDP port 69)	Object-Mode
object-group service SSH_HTTP tcp	(Define a tcp service object-group for SSH and HTTP)	Global
description SSH and HTTP Services	(Provide a description for the service)	Object-Mode
port-object eq ssh	(Specify what port it equals - ssh [pre-defined a ssh for TCP port 22)	Object-Mode
port-object eq www	(Specify what port it equals - www [pre-defined as www for TCP port 80)	Object-Mode
object-group icmp-type ping	(Define a icmp service object-group for ping)	Global
description Allow Ping for Management Networks	(Provide a description for the protocol)	Object-Mode
icmp-object echo	(Specify the icmp type you would like to define, here we set echo)	Object-Mode
icmp-object echo-reply	(Specify the icmp type you would like to define, here we set echo-reply)	Object-Mode

Hosts/Networks and Group Definitions

object-group network Management_Network_10.0.3.0	(Create the network object to be used in the ACL, for the Management Network)	Global
description Network Management Network	(Provide a description for the Network Object)	Object-Mode
network-object 10.0.3.0 255.255.255.0	(Define the network address for our object)	Object-Mode
object-group network Normal_Users_Network_10.0.2.0	(Create the network object to be used in the ACL, for the Normal Users Network)	Global
description Normal User Access	(Provide a description for the Network Object)	Object-Mode
network-object 10.0.2.0 255.255.255.0	(Define the network address for our object)	Object-Mode
object-group network Guest_Network_10.0.1.0	(Create the network object to be used in the ACL, for the Guest Network)	
description Normal Network Access	(Provide a description for the Network Object)	
network-object 10.0.1.0 255.255.255.0	(Define the network address for our object)	
object-group network Corporate_LAN_10.0.6.0	(Create the network object to be used in the ACL, for the Corporate LAN)	Global
description Corporate Network	(Provide a description for the Network Object)	Object-Mode
network-object 10.0.6.0 255.255.255.0	(Define the network address for our object)	Object-Mode
object-group network Remote_Site_Networks	(Create the network group to be used in the ACL, for All the Remote Networks)	Global
description 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24	(Provide a description for the Network Object)	Object-Mode
group-object Management_Network_10.0.3.0	(Add the already defined Network Object for the Management Network)	Object-Mode
group-object Normal_Users_Network_10.0.2.0	(Add the already defined Network Object for the Normal User Network)	Object-Mode
group-object Guest_Network_10.0.1.0	(Add the already defined Network Object for the Guest VLAN)	Object-Mode
object-group network Management_Normal_Networks	(Create the network object to be used in the ACL, for the Management and Normal Networks)	Global

description Normal User and Management Networks	(Provide a description for the Network Object)	Object-Mode
group-object Normal_Users_Network_10.0.2.0	(Add the already defined Network Object for the Normal User Network)	Object-Mode
group-object Management_Network_10.0.3.0	(Add the already defined Network Object for the Management Network)	Object-Mode
object-group network Mail_Server_10.0.6.10	(Create the network object to be used in the ACL, for the Mail Server)	Global
description Internal SMTP Mail Server	(Provide a description for the Mail Server)	Object-Mode
network-object host 10.0.6.10	(Define the network address for our object)	Object-Mode
object-group network Squid_Proxy_10.0.6.7	(Create the network object to be used in the ACL, for the Squid Proxy Server)	Global
description Squid Proxy Server	(Provide a description for the Squid Web Proxy Server)	Object-Mode
network-object host 10.0.6.7	(Define the network address for our object)	Object-Mode
object-group network DNS_Server_10.0.6.11	(Create the network object to be used in the ACL, for the DNS Server)	Global
description DNS Server for all clients	(Provide a description for the DNS Server)	Object-Mode
network-object host 10.0.6.11	(Define the network address for our object)	Object-Mode
object-group network Intranet_Web_Server_10.0.6.12	(Create the network object to be used in the ACL, for the Intranet Web Server)	Global
description Intranet Web Server	(Provide a description for the Intranet Web Server)	Object-Mode
network-object host 10.0.6.12	(Define the network address for our object)	Object-Mode
object-group network Linux_TFTP_10.0.6.13	(Create the network object to be used in the ACL, for the Linux Server)	Global
description Host for TFTP, SSH and HTTP	(Provide a description for the Linux Server)	Object-Mode
network-object 10.0.6.13 255.255.255.255	(Specify the ip address for the Linux Server)	Object-Mode

Access Lists Defined

access-list inside_to_outside extended permit tcp object-group Remote_Site_Networks object-group Squid_Proxy_10.0.6.7 object-group Squid_Proxy_Port log	Global
access-list inside_to_outside extended permit tcp object-group Management_Normal_Networks object-group Mail_Server_10.0.6.10 object-group SMTP log	Global
access-list inside_to_outside extended permit tcp object-group Management_Normal_Networks object-group Intranet_Web_Server_10.0.6.12 object-group HTTP log	Global
access-list inside_to_outside extended permit tcp object-group Management_Network_10.0.3.0 object-group Squid_Proxy_10.0.6.7 eq ssh log	Global
access-list inside_to_outside extended permit tcp object-group Management_Network_10.0.3.0 object-group Linux_TFTP_10.0.6.13 object-group SSH_HTTP log	Global
access-list inside_to_outside extended permit udp object-group Management_Network_10.0.3.0 object-group Linux_TFTP_10.0.6.13 object-group TFTP log	Global

access-list inside_to_outside extended deny ip any any log		Global
access-list outside_to_inside extended deny ip any any log		

Applying the access-list via the access-group statement

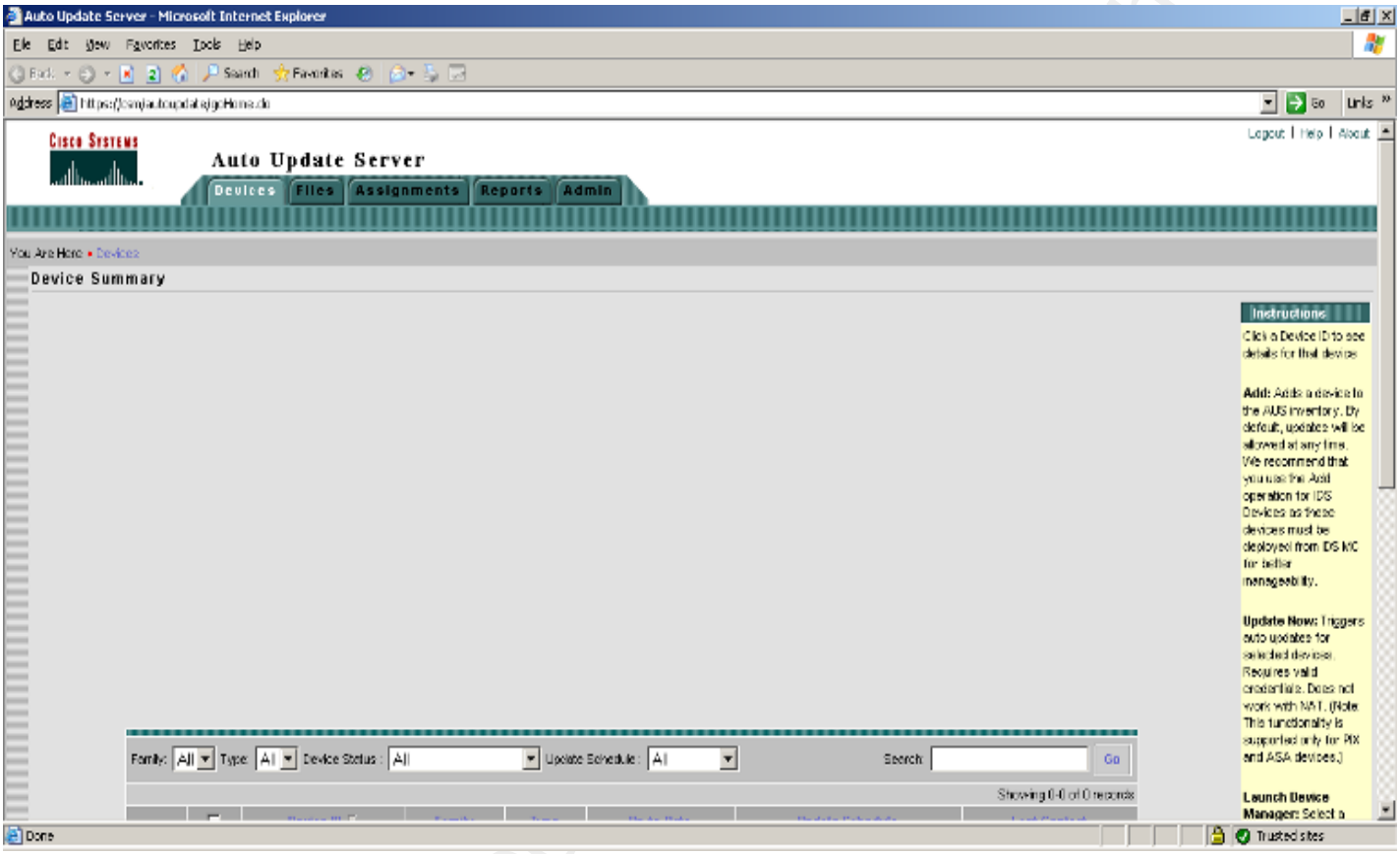
interface ethernet0/1	(Enter interface "ethernet0/1" configuration mode)	Global
access-group inside_to_outside in interface inside	(Apply the access-list we defined above, via the access-group command, to the inside interface	Interface-Mode
interface ethernet0/0	(Enter interface "ethernet0/0" configuration mode)	Global
access-group outside_to_inside in interface outside	(Apply the access-list we defined above, via the access-group command, to the outside interface	Interface-Mode

Appendix B3: Cisco Security Manager

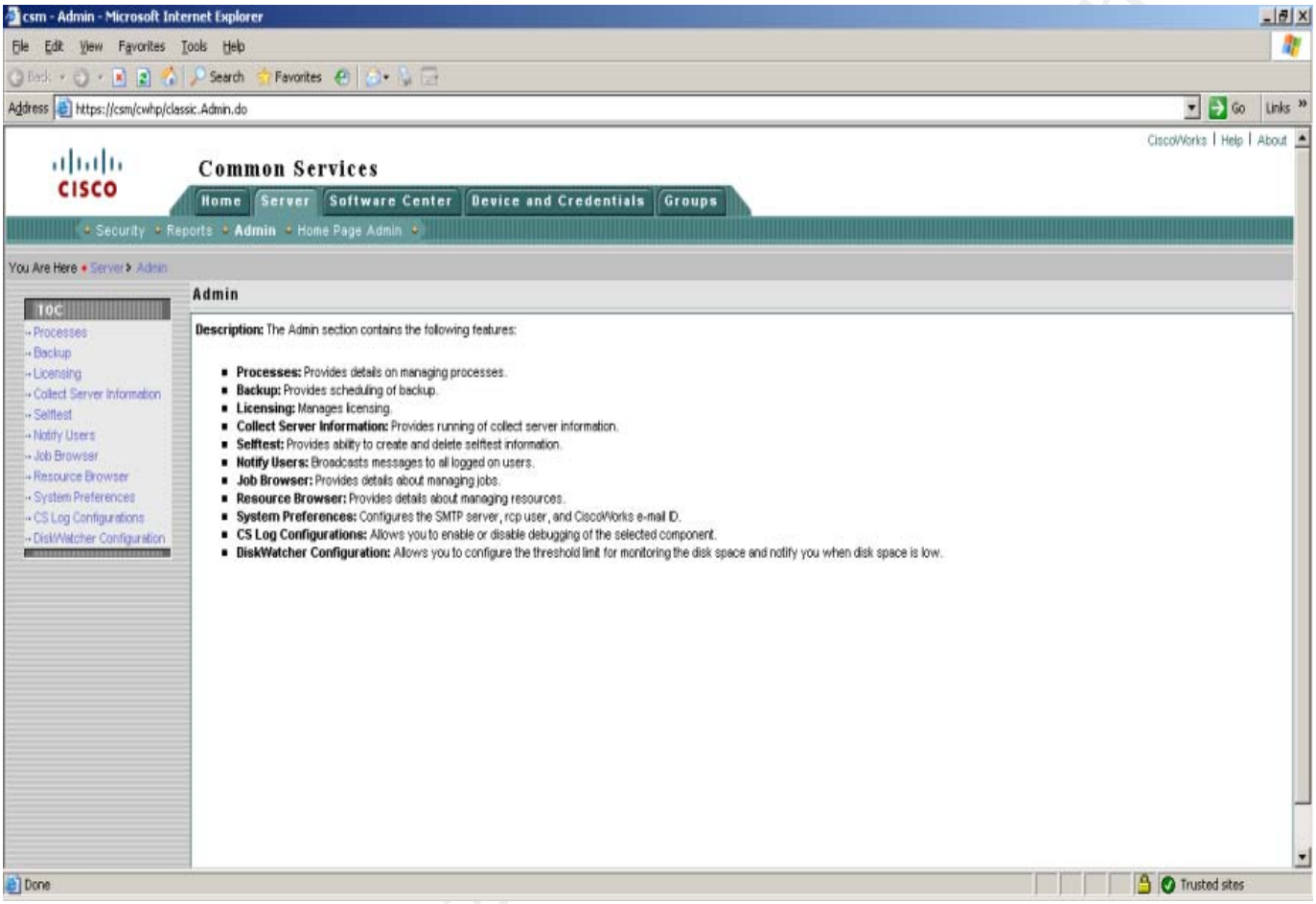
The Cisco Security Manager is a GUI management platform built to configure and support Cisco security features (for example: firewall feature set on Cisco Routers) across a wide variety of Cisco's products. CSM is a great tool for configuring VPN's, firewall policies, and updating IPS signatures on your devices. The CSM integrates tightly with other Cisco Management platforms as well, enabling role-based access (with the Cisco Access Control Server), event monitoring, analyses and response (with Cisco Security Monitoring, Analysis, and Response system).

After initially logging into the CSM web interface, your presented with 3 options (this is assuming all components were selected during the installation): Cisco Security Manager Client Installer, Auto Update Server, and Server Administration. The Security Manager Client allows administrators to securely connect to the CSM to perform administration functions. The Auto Update Server can be configured to automatically update devices with configuration parameters the administrator defines, and will provide information on conflicts (for example, overlapping firewall rules). Server Administration allows you to define security settings for the server itself (backups, audit reports, etc...), as well as manage device licensing and IPS signatures.

Below is a screenshot of the “Auto Update Server”Since this is a new install, there are currently no managed devices, but this is where you add them.



When you select the “Server Administration”option, you are taken to the screen below, where you can configure many options specific to the server.



As with the Juniper NSM, you have plenty of options available to you from the Cisco Security Manager for managing your Cisco based network. The server can be installed on Windows Server 2003, and supports connectivity via Internet Explorer and Firefox browsers. I encourage those who are interested in this management platform to use the URL I provided below as a starting point for finding out more detailed information about the product.

Additional Juniper Links:

Product Data Sheets:

http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_5_slash_ssg_20/index.html

Network and Security Manager

http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/netscreen_security_manager/index.html

ScreenOS version 6.0 Software Documentation

http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/

Additional Cisco Links:

Cisco Security Manager

http://www.cisco.com/en/US/products/ps6498/index.html

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/data_sheet_c78-458677-00_ps6498_Products_Data_Sheet.html

ASA Product Comparison Sheet

http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

Cisco Security Appliance Command Reference, Version 7.2

http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/cmd_ref.html

Last Updated: June 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced