Forcepoint NGFW System Engineer Lab Guide

June 14, 2019

Lab 0:

Contents

Lab 0: Contents

List of Figures

Introduction

Welcome to the Forcepoint NGFW System Engineer course! This course and its associated labs are designed to provide the student with a deep level of knowledge regarding all aspects of a Forcepoint NGFW environment. Network and security administrators, integrators and partners will learn how to install, configure, maintain and troubleshoot the Forcepoint NGFW and its associated management platform, the SMC.

The course starts by having you install the Management and Log servers, the two most commonly used components of the architecture. After these are licensed,

The course simulates a three (3) site environment, one as the Headquarters and two remote offices, Atlanta and Paris. You will first install the SMC, which will manage the entire environment. After that, you will configure and deploy one other firewall for the Headquarters location. As a slight variation on firewall deployments, you will deploy a Master Engine at the Paris location, which can host virtual firewalls - common in MSSP environments.

Lab 0: List of Figures

LAB 1

SMC Installation and Deployment

Getting Started

The first step in deploying a Forcepoint NGFW infrastructure is installing the Security Management Center, or the SMC. The SMC is made of processes that collectively manage and monitor your Forcepoint NGFW deployment. Before the firewall engines can be defined and managed, the SMC must be installed and properly configured.

In this lab, you will install the SMC on a Linux server. You will then install the licenses for the SMC and the firewall engines. This lab, and the labs that follow, will simulate distributed environment, where some of the firewalls are not at the same site as the SMC. To accommodate the remotely managed environment, you will configure locations and contact addresses so that remote firewalls can communicate with the SMC, which is being protected by a firewall.

At the conclusion of this lab, the SMC will be ready for further configuration as you deploy your distributed firewall environment.

1.1 Installing the SMC Software

In this exercise, you will install the Management Server and Log Server components on the same Linux server. The SMC will be located behind the HQ, or Helsinki, firewall.

1. From the **Main Menu** running in the command prompt on the **Landing Machine**, select option 1 for the **Helsinki SMC**

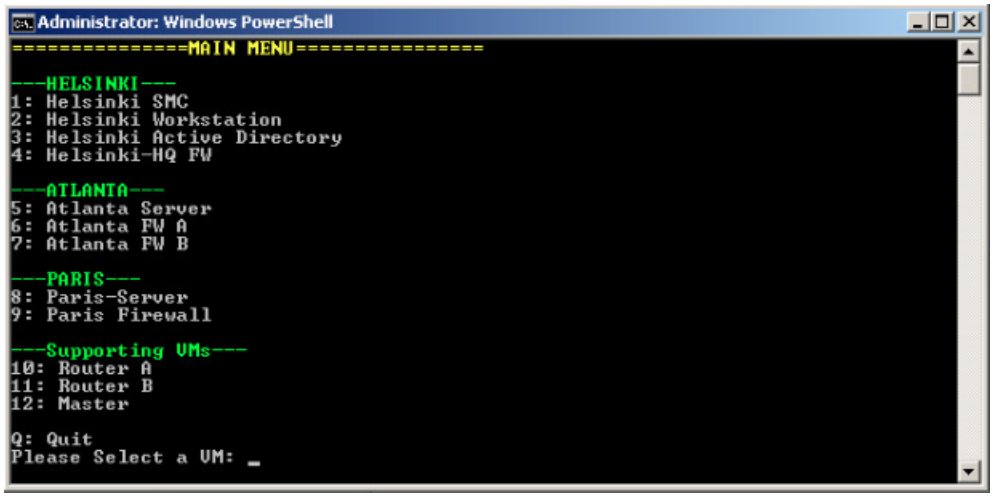


Figure 1.1: Opening a Console to SMC

2. On the desktop, click the **Terminal** icon to open a Linux command prompt

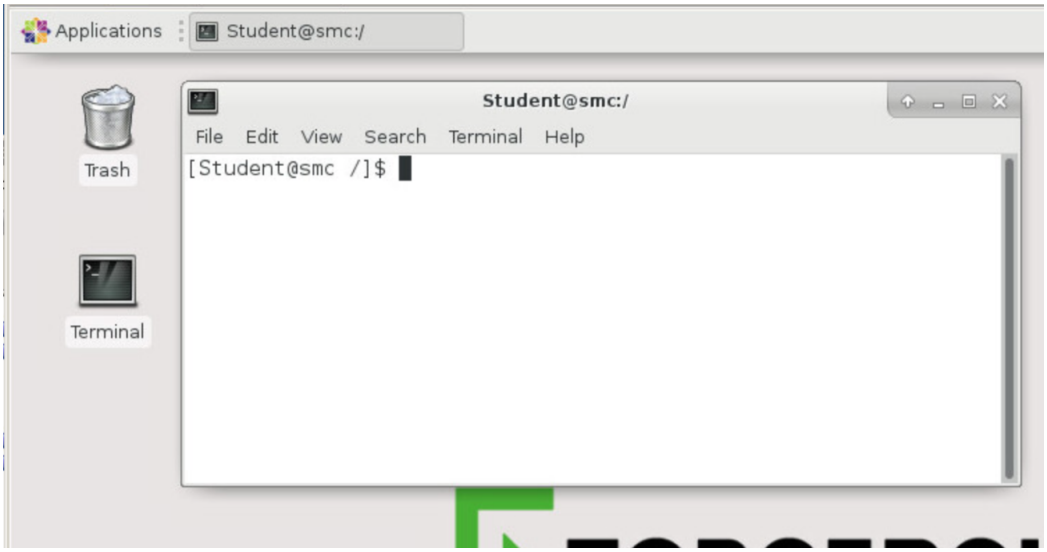


Figure 1.2: Opening a Linux Command Prompt

3. At the prompt, type `cd Downloads`, press **Enter**
4. To install the SMC software on Linux, you must be the superuser. To log in as root, the superuser, type `su` and press **Enter**
5. When prompted for the password, enter `Forcepoint1!`

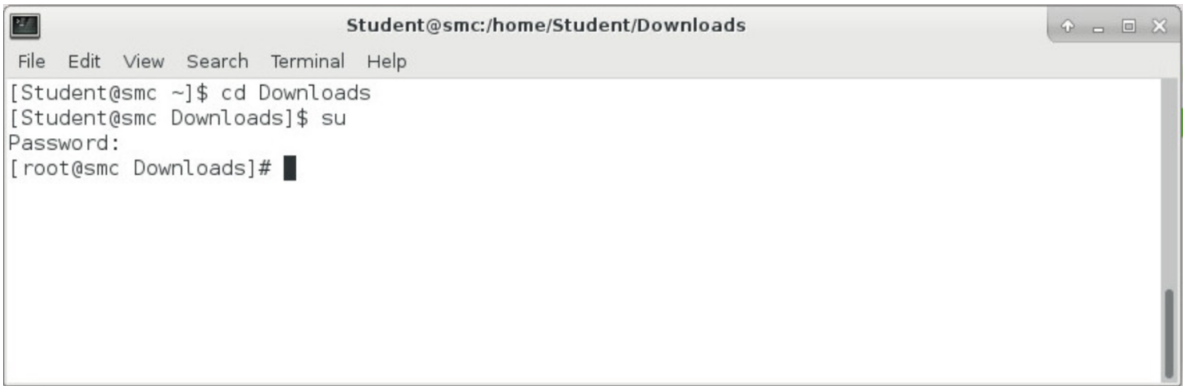


Figure 1.3: Preparing to Install the SMC

6. Type `cd Downloads` and press **Enter** to change into the Downloads directory
7. Type `ls` to list the files in the directory
8. To unzip the SMC software, type `unzip smc_6.6.1_10714_linux.zip` The SMC software unpacks

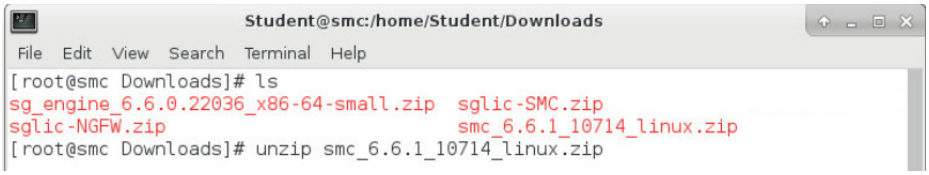


Figure 1.4: Unpacking the SMC Software

TIP: When typing long names, enter the first few characters of the name and press **Tab** to complete the name.

9. When the SMC software has finished unpacking, type `cd smc_6.6.1_10714_linux/Linux-x64` and press **Enter**. This will change into the directory where the installer executable is located
10. At the command prompt, type `./setup.sh` and press **Enter**
11. The setup script will run, and you will be presented with the figure below

Figure 1.5: SMC Installation Start

12. Click **OK**
13. In the screen that follows, click **Next**
14. Accept the license agreement by selecting **I accept the terms of the License Agreement**. Click **Next**

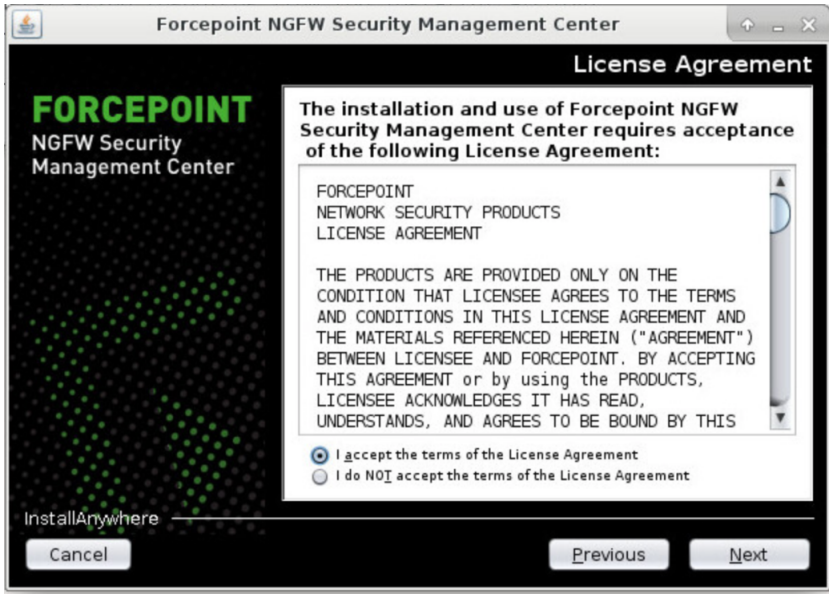


Figure 1.6: Accepting the License Agreement

15. You are now prompted for the path in which the SMC software is installed. Click **Next**
16. Next you are prompted to ensure that `/etc/hosts` is configured correctly for name resolution, you may click **Next**
17. Accept the default for the shortcuts directory by clicking **Next**
18. At this point, you are prompted to select which management components to install. Select **Typical**. This will install the Management and Log servers

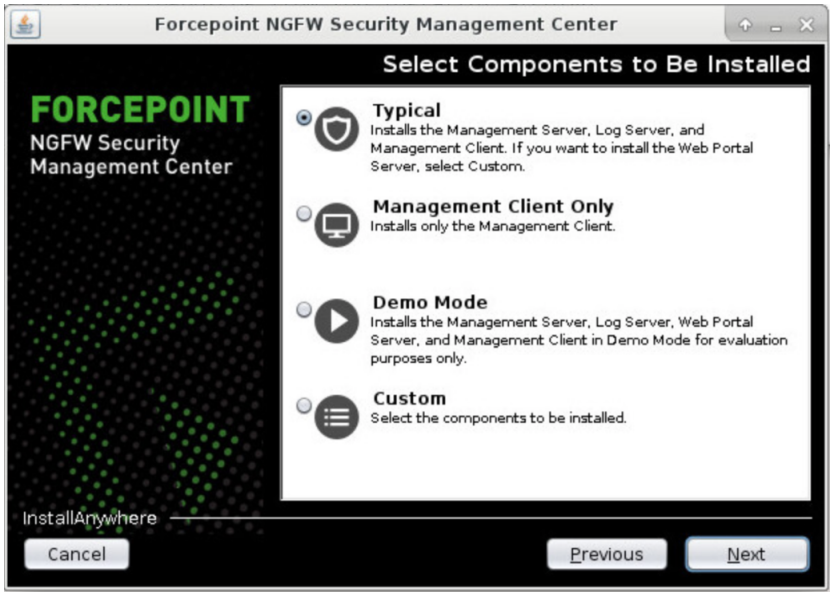


Figure 1.7: Typical SMC Installation

19. Click **Next**
20. Ensure that the IP address selected is **172.31.200.101** as the IP for the Management and Log servers. This is the IP address of the Linux server and the IP to which the SMC license is bound
21. Click **Next**
22. Deselect **256-Bit Security Strength** and make sure that **Install as a Service** is selected. Click **Next**

Figure 1.8: Selecting Management IP Address

23. You are now prompted to create a superuser for the SMC. Enter the following
    - **User Name**: `root`
    - **Password**: `Forcepoint1!`

Figure 1.9: Entering the Superuser Credentials

24. Click **Next**
25. For the Log Server configuration, ensure that the IP address is selected as **172.31.200.101** and that **Install the Log Server as a Service** is selected. Click **Next**

Figure 1.10: Log Server Installation Configuration

26. Accept the default Log Files directory by clicking **Next**
27. Click **Install** at the Pre-Installation Summary. The SMC will now be installed
28. When the installation completes, click **Done**

Figure 1.11: Completed SMC Installation

1.2 Logging Into the SMC

Now that the SMC software is installed, you must log in to continue the configuration. In this exercise, you will log in as the Superuser and complete the SMC installation by applying the licenses.

1. From the same Terminal you used previously, type the following command, `/usr/local/forcepoint/smc/bin/sgClient.sh &` and press **Enter**
2. The SMC Client log in prompt appears. Click the arrow to the right of **172.31.200.101**

Figure 1.12: Opening the SMC Client

3. When prompted, click **Accept** to accept the SMC key fingerprint

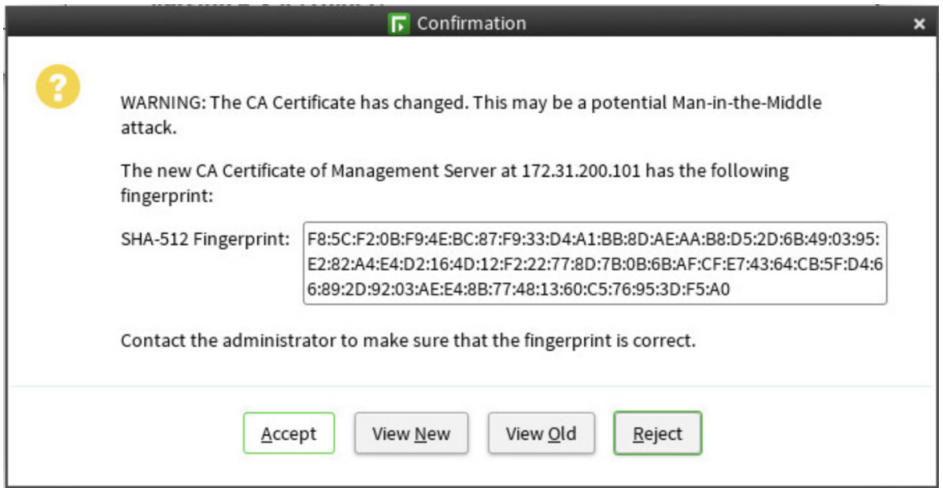


Figure 1.13: Accepting the SMC Key Fingerprint

4. When prompted, enter the following credentials for the SMC Superuser
   - **User Name**: root
   - **Password**: Forcepoint1!
5. Click **Log On**. You are now logged into the SMC and ready to continue the configuration

1.3 Installing SMC and Engine Licenses

So far you have unpacked the SMC software, run the installer, and provided the configuration details for the SMC. Now that you are logged in, the next step is to install the licenses for the Management and Log servers, which collectively form the SMC.

1. From the SMC client, click **Menu** from the toolbar at the top and browse to **System Tools** → **Install Licenses**

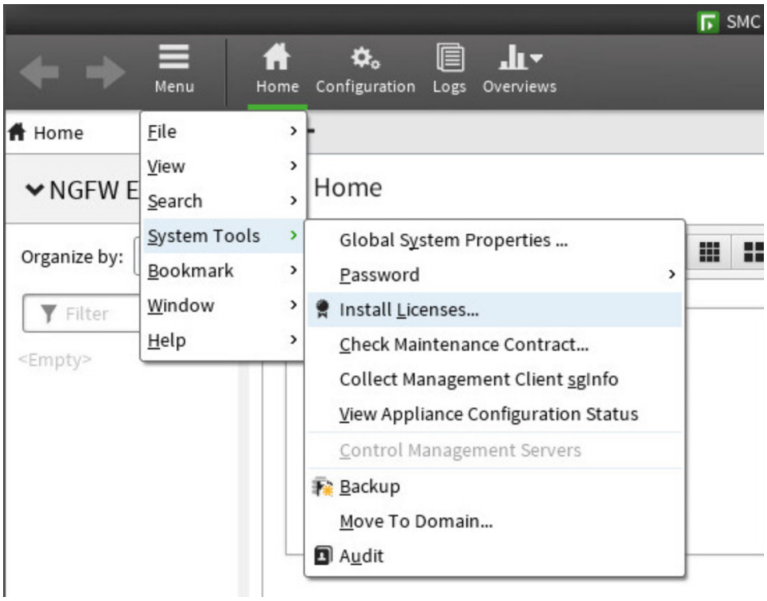


Figure 1.14: License Installation Menu Selection

2. In the window that appears, use the drop down menu and browse to \ → **home** → **Student** → **Downloads** and select **sglic-SMC.zip**. Click **Install**

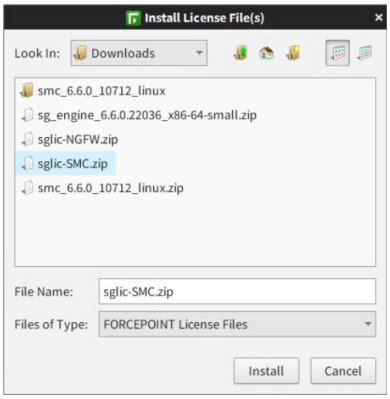


Figure 1.15: Installing SMC Licenses

3. To install the engine licenses that will be used for the NGFWs that you will install later, click **Menu** from the toolbar at the top and browse to **System Tools** → **Install Licenses**
4. In the window that appears, use the drop down menu and browse to \→ **home** → **Student** → **Downloads** and select **sglic-NGFW.zip**. Click **Install**

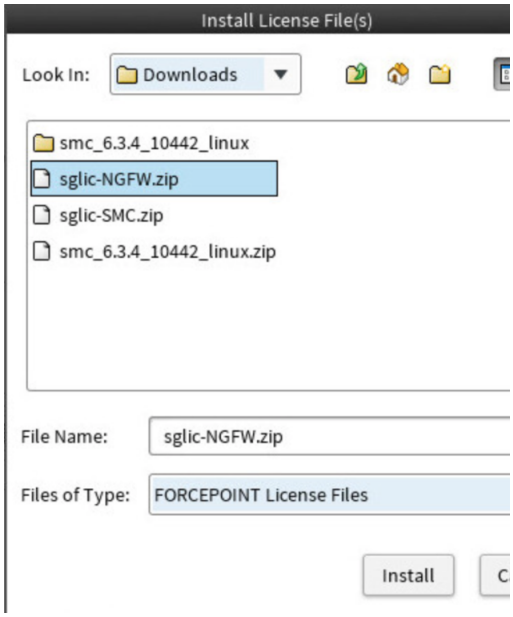
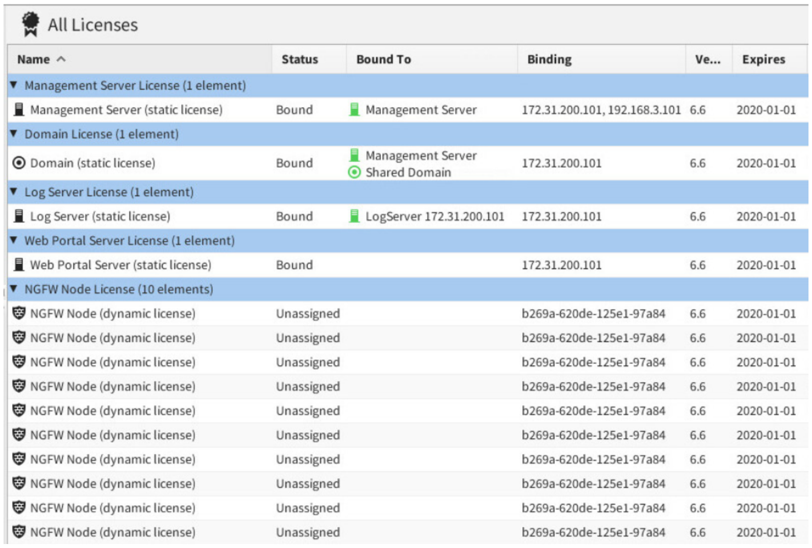


Figure 1.16: Installing the Engine Licenses

1.4 Verifying the License Installation

Now that the licenses have been installed, you will now verify the successful installation of the licenses.

1. From the **Home** view, click **Configuration** in the Menu toolbar. The **Configuration** view opens
2. In the tree view on the left, browse to **Administration** → **Licenses** → **All Licenses**



All Licenses

Name	Status	Bound To	Binding	Ve...	Expires
▼ Management Server License (1 element)					
Management Server (static license)	Bound	Management Server	172.31.200.101, 192.168.3.101	6.6	2020-01-01
▼ Domain License (1 element)					
Domain (static license)	Bound	Management Server Shared Domain	172.31.200.101	6.6	2020-01-01
▼ Log Server License (1 element)					
Log Server (static license)	Bound	LogServer 172.31.200.101	172.31.200.101	6.6	2020-01-01
▼ Web Portal Server License (1 element)					
Web Portal Server (static license)	Bound		172.31.200.101	6.6	2020-01-01
▼ NGFW Node License (10 elements)					
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01
NGFW Node (dynamic license)	Unassigned		b269a-620de-125e1-97a84	6.6	2020-01-01

Figure 1.17: Verified License Installation

Summary

In this lab, you have successfully installed and licensed the SMC. This is the first step in any deployment. The stage is now set to further configure the SMC to manage a distributed NGFW environment.

LAB 2

Single Firewall Installation

Getting Started

Now that the SMC is installed, it is time to deploy the firewall at the Headquarters location. This will be a single node firewall in front of the SMC, and it will perform NAT. In later labs, you will create a policy that allows for the centralized, and secure, management of remote firewalls.

2.1 Define a New Single Firewall

The first step in deploying a new firewall is to first define it in the SMC. In this exercise, you will define a new single firewall, with three (3) interfaces, two will be external interfaces, connected to different ISPs, and the third interface will be for the Helsinki (Headquarters) network.

1. From the **Home** view, click the gear icon next to **NGFW Engines** and browse to **New** → **Firewall** → **Single Firewall**. The **Single Firewall (Edit)** tab opens

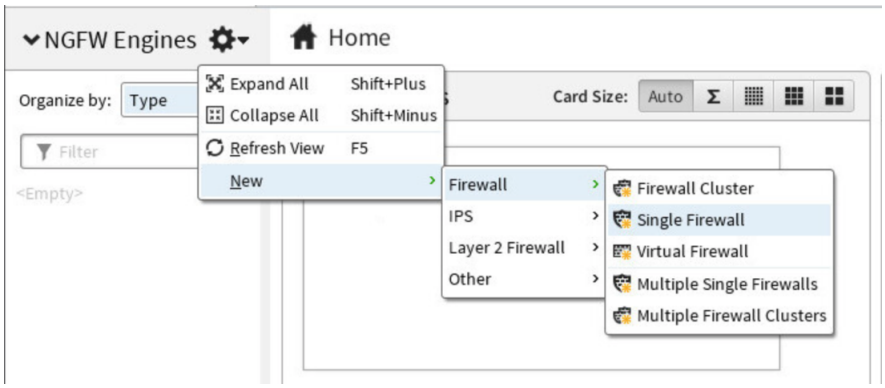


Figure 2.1: Creating a New Single Firewall

2. Under the **General** section, in the **Name** field, enter **Helsinki-HQ FW**
3. In the **Log Server** field, ensure that **Log Server 172.31.200.101** is selected
4. Next to the **DNS IP Addresses** field, click **Add** and select **IP Address**
5. In the dialog that appears, enter **8.8.8.8** and click **OK**

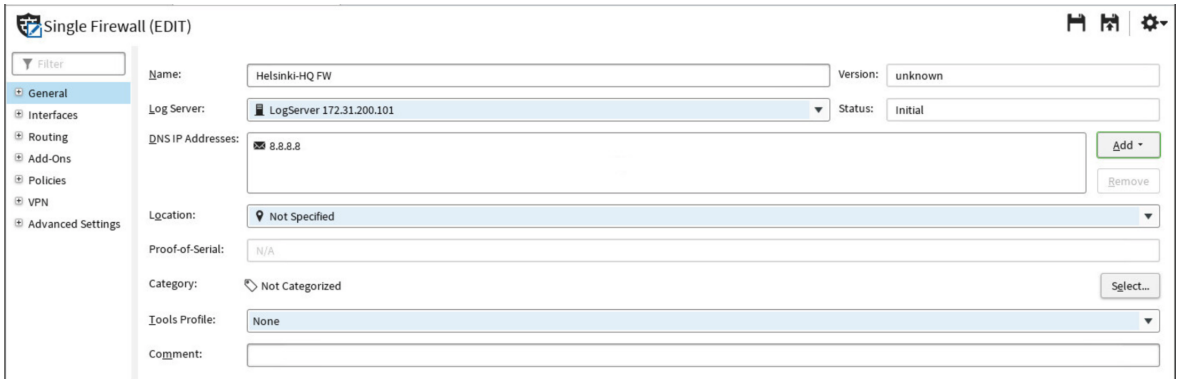


Figure 2.2: Helsinki-HQ FW General Properties

2.2 Define Physical Interfaces

The first step in configuring a Forcepoint NGFW is to define the physical interfaces. After the Physical Interfaces are defined, you will add IP addresses to them in the next exercise.

2.2.1 Define Interface 0

1. On the left side, click on **Interfaces**
2. In the upper right of the client, click the **New** icon and select **Layer 3 Interface**. The Layer 3 Physical Interface properties opens
3. Verify that the **Interface ID** is set to **0**
4. Click the **Zone** drop down menu, and select **Internal**
5. Click the **LLDP Mode** drop down menu, and select **Receive Only**
6. In the comment field, enter **HQ Internal**

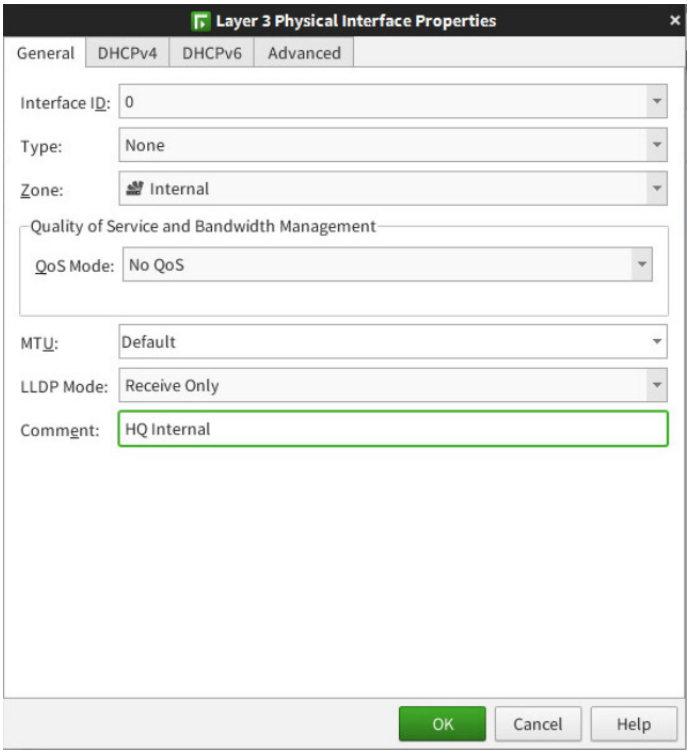


Figure 2.3: Interface 0 Properties

7. Click **OK**. The Layer 3 Physical Interface Properties dialog closes

2.2.2 Define Interface 1

1. Click thew **New** icon and select **Layer 3 Physical Interface**. The Layer 3 Physical Interface Properties opens
2. Verify that the **Interface ID** is set to **1**
3. Click the **Zone** drop down menu and select **External**
4. Click the **LLDP Mode** drop down menu, and select **Receive Only**
5. In the **Comment** field, enter **ISP A External**

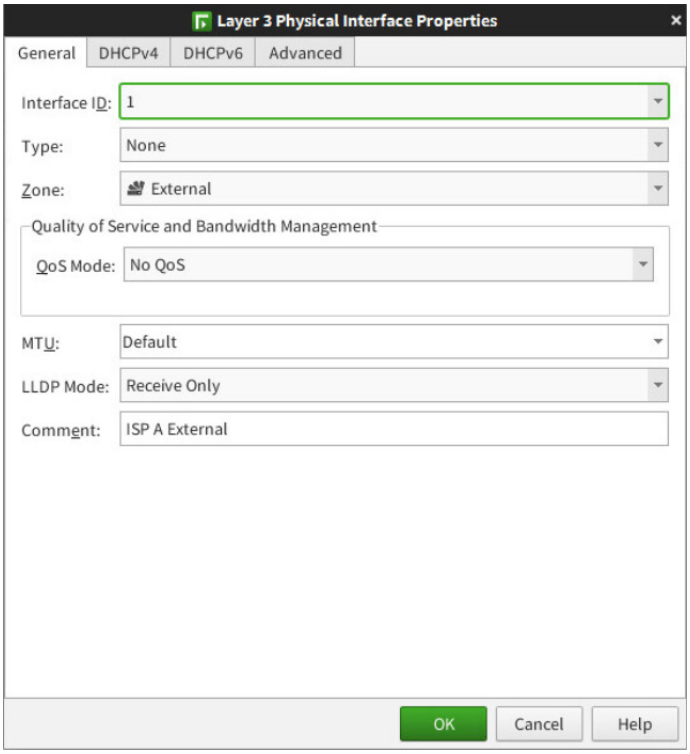


Figure 2.4: Interface 1 Properties

6. Click **OK**. The Layer 3 Physical Interface Properties dialog closes

2.2.3 Define Interface 2

1. Click thew **New** icon and select **Layer 3 Physical Interface**. The Layer 3 Physical Interface Properties opens
2. Verify that the **Interface ID** is set to **2**
3. Click the **Zone** drop down menu and select **External**
4. Click the **LLDP Mode** drop down menu, and select **Receive Only**
5. In the **Comment** field, enter **ISP B External**

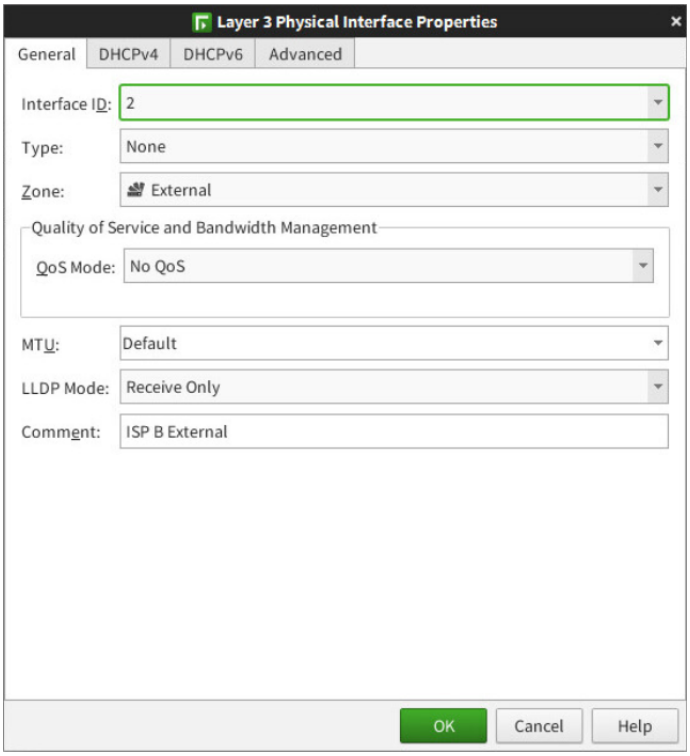


Figure 2.5: Interface 2 Properties

2.3 Configure IP Addresses on Physical Interfaces

The Physical Interfaces are now defined. At this point, you will assign IP addresses to the interfaces. The HQ Internal (Interface 0) will be the HQ private network.

2.3.1 Add IP Address for Interface 0

1. Right-click on **Interface 0** and browse to **New** → **IPv4 Address**. The IP Address Properties for Interface #0 opens
2. In the drop down menu, make sure that the IP Address type is set to **Static**
3. In the **IPv4 Address** field, enter **172.31.200.1**
4. Click in the **Netmask** field. The subnet mask, network address, and the broadcast addresses are populated automatically

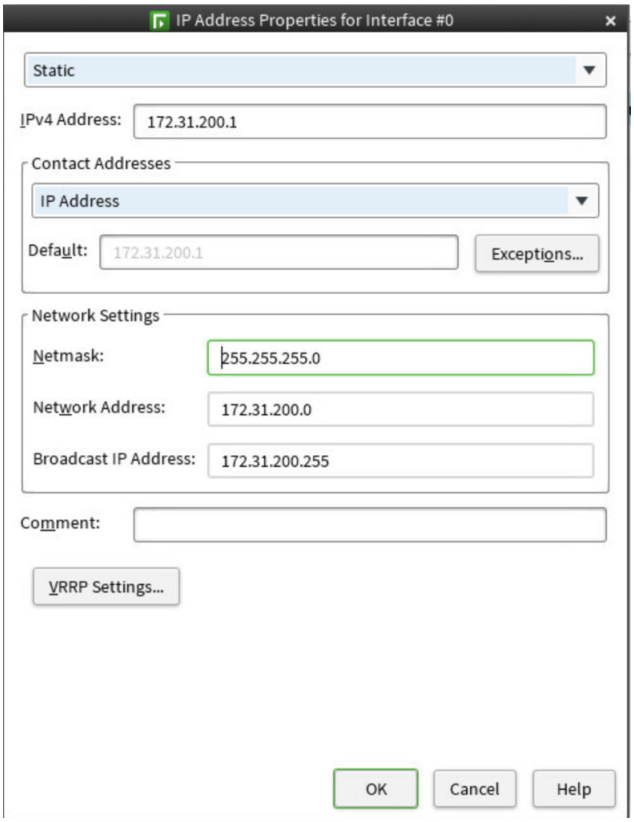


Figure 2.6: IP Address for Interface 0

5. Click **OK**. The IP Address Properties for Interface #0 closes

2.3.2 Add IP Address for Interface 1

1. Right-click on **Interface 1** and browse to **New** → **IPv4 Address**. The IP Address Properties for Interface #1 opens
2. In the drop down menu, make sure that the IP Address type is set to **Static**
3. In the **IPv4 Address** field, enter **172.31.1.254**
4. Click in the **Netmask** field. The subnet mask, network address, and the broadcast addresses are populated automatically

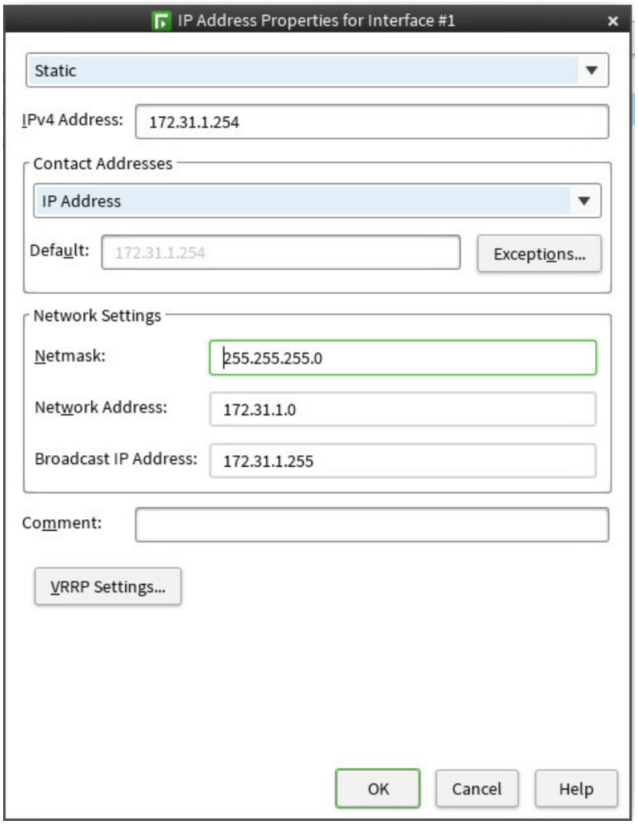


Figure 2.7: IP Address for Interface 1

5. Click **OK**. The IP Address Properties for Interface #1 closes

2.3.3 Add IP Address for Interface 2

1. Right-click on **Interface 2** and browse to **New** → **IPv4 Address**. The IP Address Properties for Interface #2 opens
2. In the drop down menu, make sure that the IP Address type is set to **Static**
3. In the **IPv4 Address** field, enter **10.1.1.254**
4. Click in the **Netmask** field. The subnet mask, network address, and the broadcast addresses are populated automatically

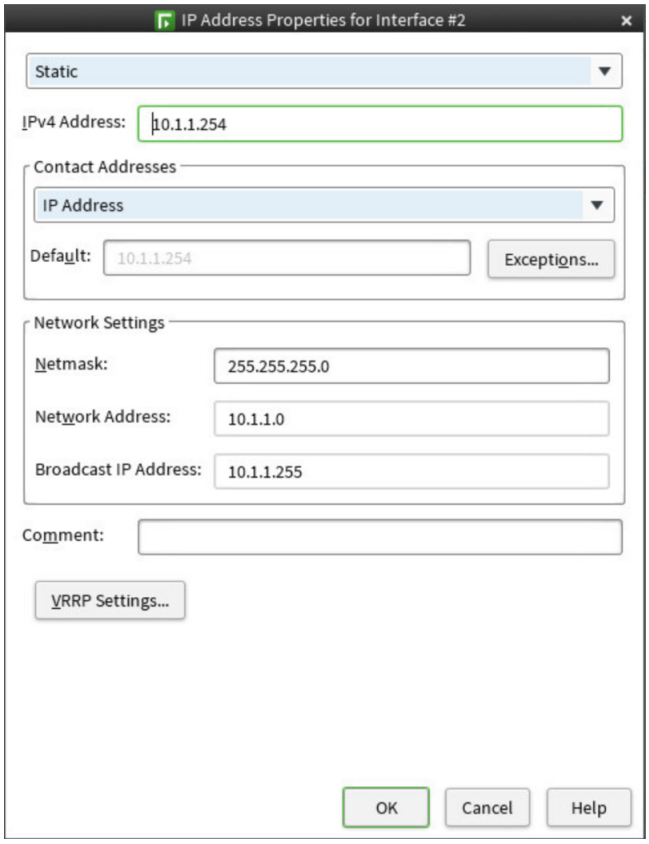


Figure 2.8: IP Address for Interface 2

5. Click **OK**. The IP Address Properties for Interface #2 closes

2.4 Configure Interface Options

In the NGFW, there are options that must be selected for the interfaces you created in the last exercise. Most importantly, this exercise will guide you through selecting the management interface.

1. In the tab where your Single Firewall is still open for editing, expand **Interfaces** on the left side and select **Interface Options**
2. In the **Control Interface** section, in the **Primary** field, leave the interface set to **Interface 0 (172.31.200.1)**
3. In the **IPv4 Identity for Authentication Requests** field, use the drop-down menu and select **Interface 1 (172.31.200.1)** **NOTE**: The Identity for Authentication Requests is the IP that is present to external authentication servers. The IP is used as an identifier only, as such packets are still routed according to the routing table.
4. In the **IPv4 Source for Authentication Requests**, choose the interface the firewall uses for send authentication requests by leaving it set to **According to Routing**
5. Set **Default IP for Outgoing Traffic** to **Interface 1 (172.31.1.254)** Your configured Interface Options should appear as in the figure below

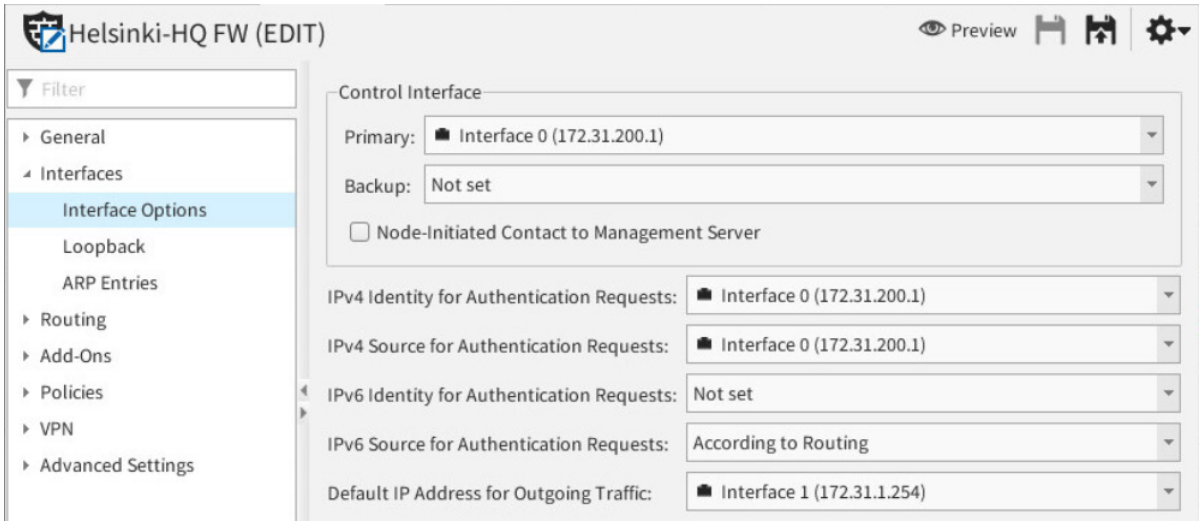


Figure 2.9: completed Interface Option Configuration

6. Click the **Save** icon in the upper right corner to save the Helsinki-HQ FW firewall
7. You may now close the tab where the **Helsinki-HQ FW** is open for editing

2.5 Establishing Trust with the SMC

Now that the firewall has been defined in the SMC, you can save the initial configuration of the firewall. The information contained in this configuration will be used to establish a trust relationship between the SMC and the Engine (firewall). In this exercise, you will save the Initial Configuration and use a console to configure the Engine for initial contact with the SMC.

2.5.1 Saving the Initial Configuration

1. From the **Home** view, in the tree view on the left, expand **Firewalls**
2. Right-click on **Helsinki-HQ FW** and browse to **Configuration** → **Save Initial Configuration**

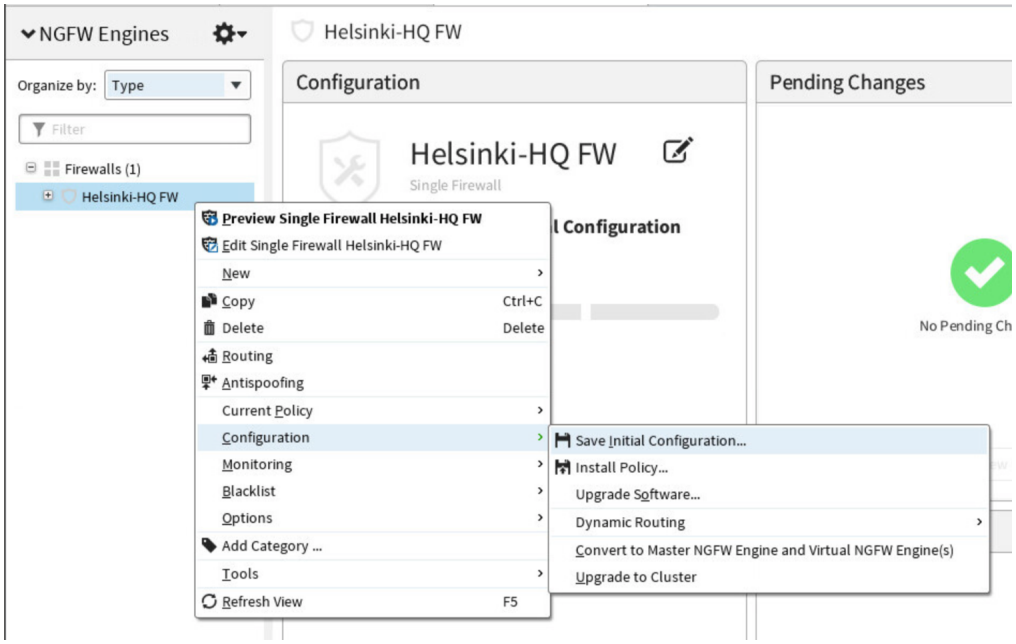


Figure 2.10: Saving the Initial Configuration

3. On the window that appears, click **View Details**
4. Leave this window open or write down the **One Time Password**. This will be needed for the Engine configuration

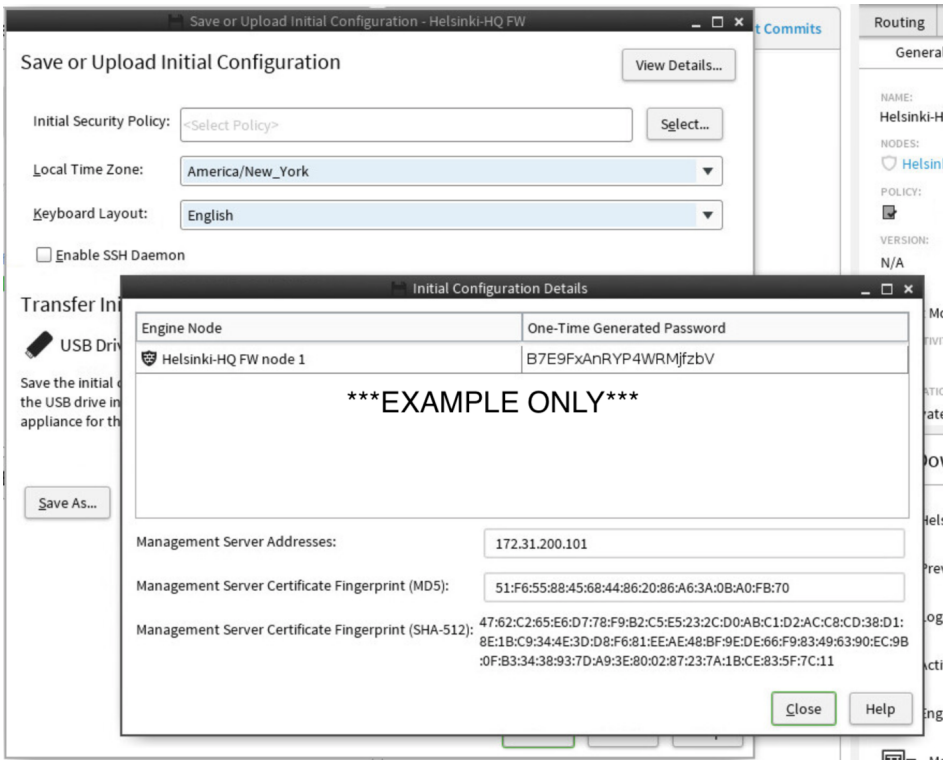


Figure 2.11: Viewing Initial Configuration Details

2.5.2 Configuring the Engine for SMC Contact

So far you have gotten the information from the SMC to establish a trust relationship with the SMC - the One Time Password. This is used on the Engine as a way of identifying itself to the SMC. In this exercise, you will open a console to the Engine

and configuring to contact the SMC.

1. Using the **Main Menu** from the **Landing Machine**, open a console to **Helsinki-HQ FW**

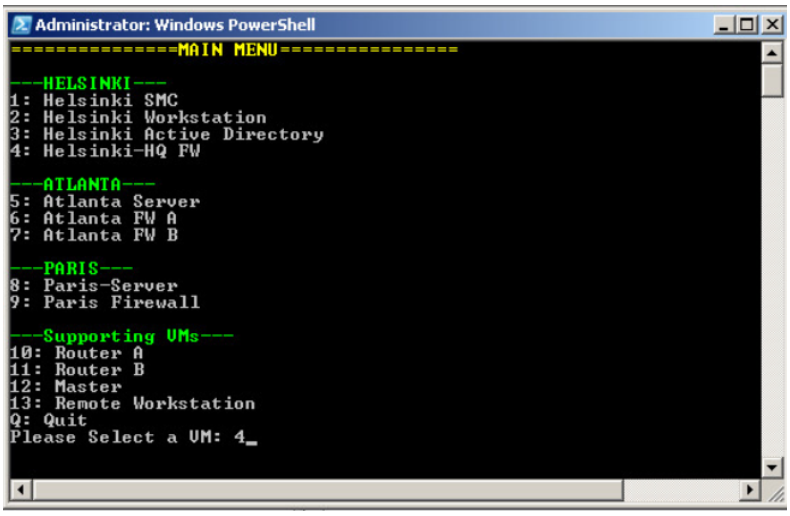


Figure 2.12: Opening a Console to HQ Firewall

2. In the window that appears, click inside. Press **Enter** to activate the console
3. Stop the browser-based configuration by entering **Y**, when prompted. The console configuration wizard starts

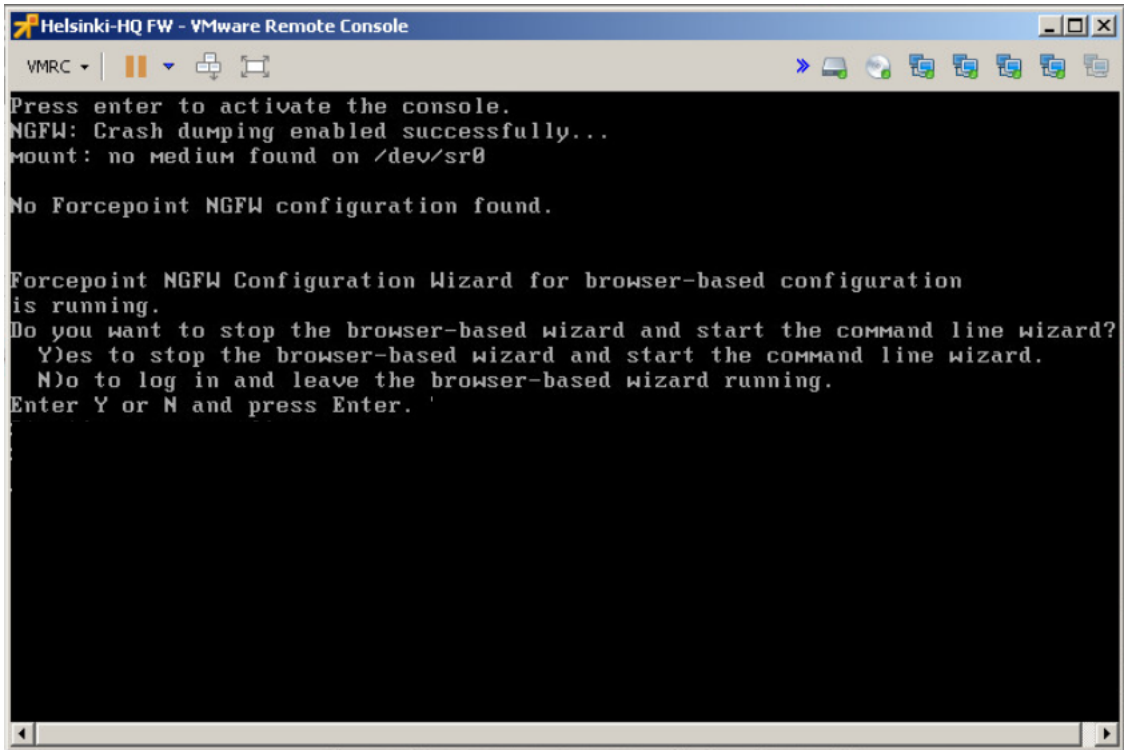


Figure 2.13: First Engine Login

4. When prompted to select the **Role**, press **Enter**. You are now prompted to select the role.
5. Select **Firewall/VPN** by pressing **Enter**

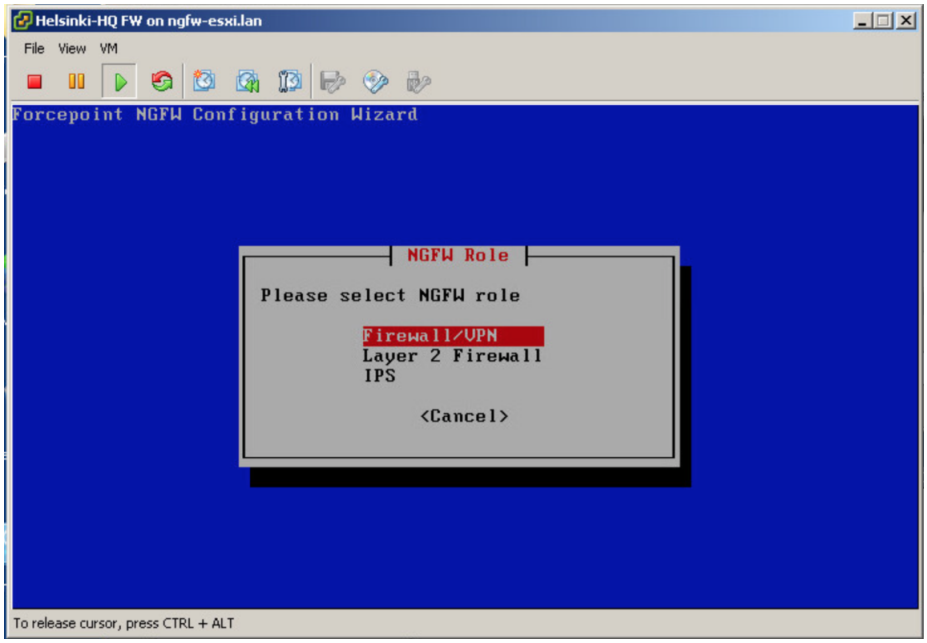


Figure 2.14: Selecting Engine Role

6. On the **Welcome** screen, use the **Tab** key, tab over to **Next**, and press **Enter**
7. In the **Configure OS Settings**, enter the following values

   NOTE: Use the **Enter** key to select a setting to change, use the **Space bar** to check a box, and the **Tab** or arrow keys to move from field to field.

   - **Keyboard layout**: US English
   - **Local timezone**: US/Eastern

     TIP: Press **U** and the selection will jump to time zones starting with US.

   - **Hostname**: HQ-Firewall
   - **Root password**: Pass1234
8. Using the **Space bar**, select **Enable SSH daemon**

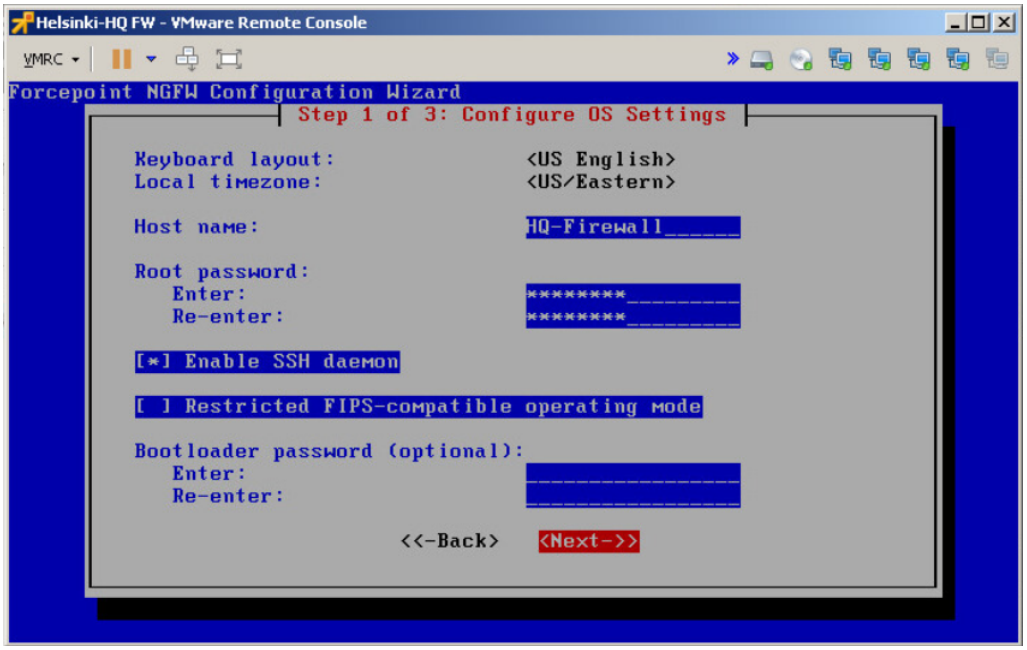


Figure 2.15: Completed HQ Firewall OS Settings

9. Using the **Tab** key, move to **Next** and press **Enter**
10. In the **Configure Network Interfaces** screen, leave eth0 set as the **Mgmt** (Management) interface. Tab down to **Next**

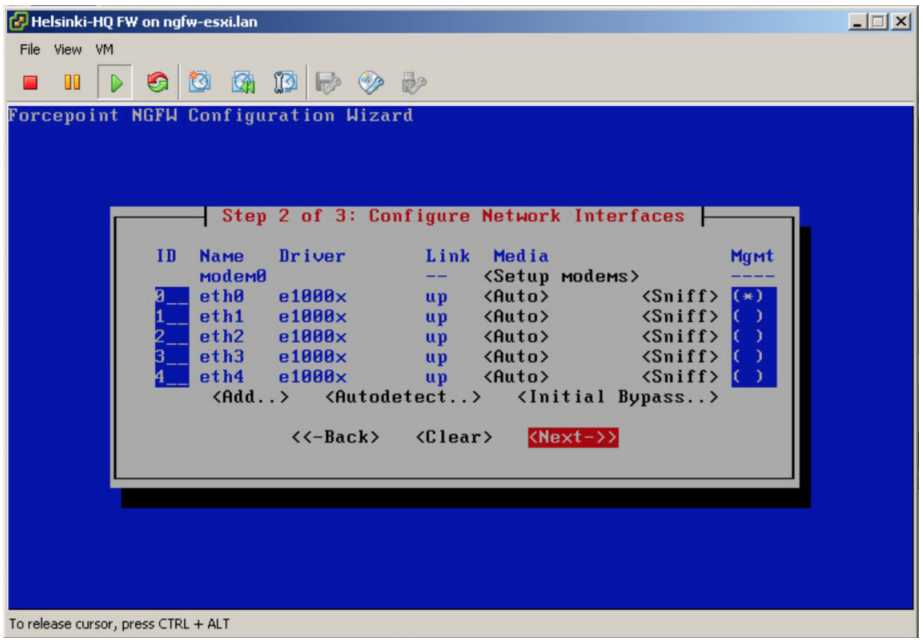


Figure 2.16: Network Interface Configuration Wizard

11. Using the Tab or Arrow Keys, move down to **Enter node IP address manually**, and enter the following values
    - **IP address**: 172.31.200.1
    - **Netmask/Prefix Length**: 24

NOTE: As the SMC is located on a directly connected network, no gateway IP address is required.

12. Using the Tab or Arrow Keys, move down to **Contact** and press the **Space Bar** to select it
13. Arrow down to the **Management Server** field, and enter the following values
    - **IP address**: 172.31.200.101
    - **One-time password**: Enter the one time password generated in **Step 4** from the **Saving the Initial Configuration** section above
14. Arrow or Tab down to **256-bit security** and press the **Space bar** to deselect it
15. Arrow or Tab down to **Finish** Your completed Engine initial configuration should appear as in the figure below

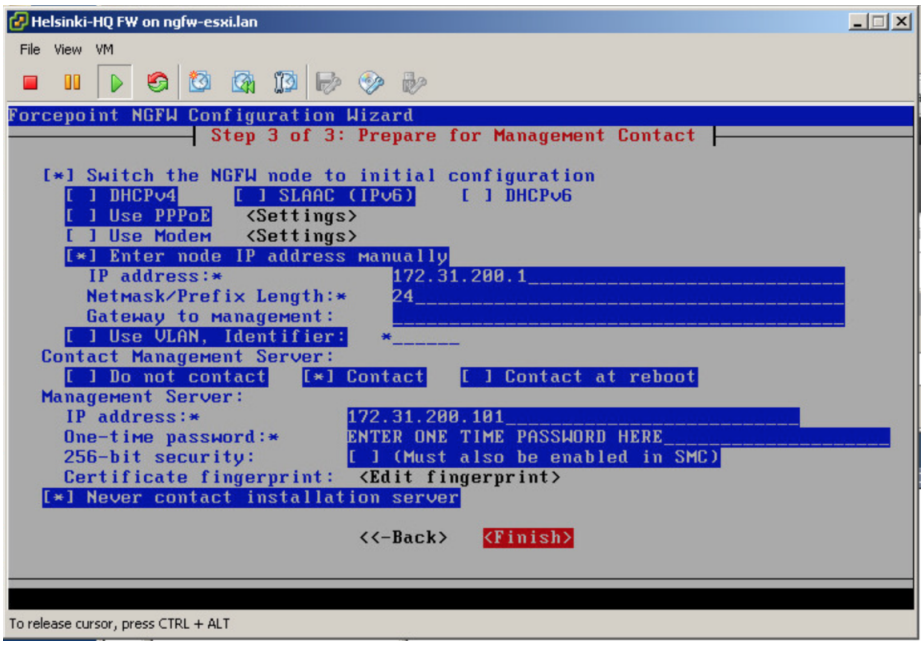


Figure 2.17: Completed HQ Firewall Initial Configuration

16. When presented with the **Fingerprint Verification**, press **Enter** to accept the Management Server certificate fingerprint

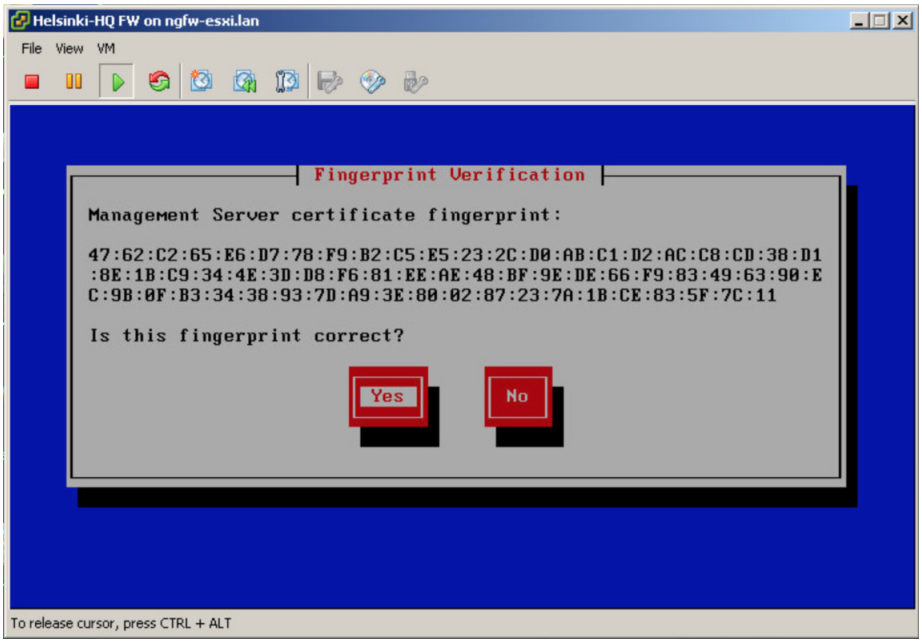


Figure 2.18: Management Server Certificate Fingerprint

17. After this, you should receive a message that contact with the Management Server was successful, and after 5 seconds, the login prompt will be presented

    NOTE: If contact fails, and you receive a message in relation to the One-time Password being incorrect, it is not necessary to restart the installation wizard. Log in as **root** with **Pass1234** as the password and run **sg-contact-mgmt** followed by the One-time Password. It is also possible to create a new One-time Password by right-clicking on the Engine → **Configuration** → **Save Initial Configuration**. You will then receive a new One-time Password. Run the following `sg-contact-mgmt <YOUR ONE TIME PASSWORD>`

18. In the Management Client, you may now close the window where your One-time Password was available for viewing

19. To verify that the Management Server Contact was successful, click the **Home** button and note that the color of the Engine has changed from white to orange, letting you know that contact was successful

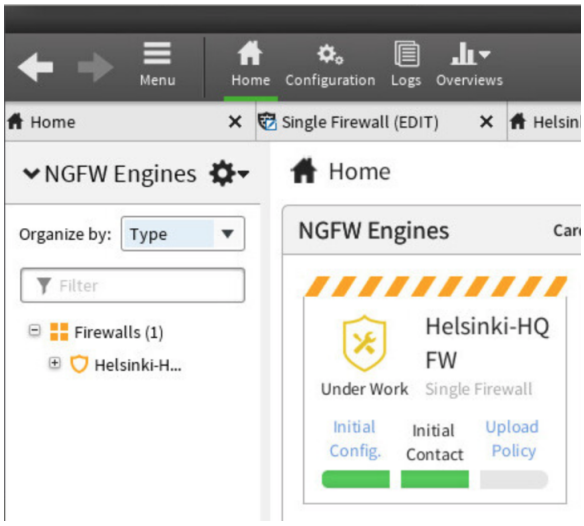


Figure 2.19: Successful Management Contact SMC View

NOTE: The status of the Engine will not be green until a policy is successfully uploaded in a later lab.

2.6 Bind a License to the Engine

In order for a policy to be installed, you must bind a license to the engine. In this exercise, you will bind one of the NGFW licenses to the Single Firewall you just created.

1. From the Management Client, click the **Configuration** button in the tool bar at the top. The Configuration View opens
2. In the tree view on the left, browse to **Administration** → **Licenses** → **NGFW Engines**
3. In the pane on the right, right-click the first **NGFW Node (dynamic license)** and select **Bind**. The Select License Binding dialog opens
4. Click on **Helsinki-HQ FW node 1**

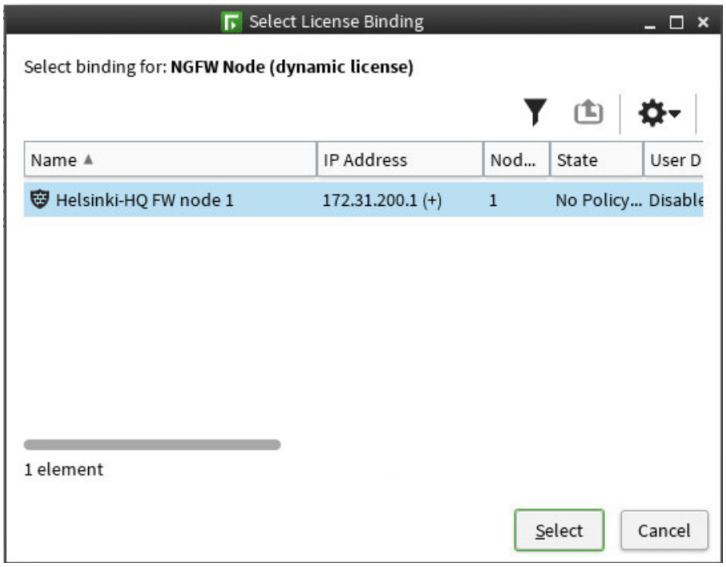


Figure 2.20: Binding a License to Helsinki-HQ FW

5. Click **Select**. The Select License Binding dialog closes. A message appears letting you know that the license was successfully bound to the engine

Summary

In this lab you have taken the first steps in deploying your distributed firewall environment. You first configured the Engine in the SMC, which gave you a one-time password for use in establishing trust between the SMC and Engine. You then configured the Engine itself using the terminal-based installation wizard. At the conclusion of the lab, you used the one-time password to contact the Management Server. The status of the new Engine in the SMC changed as a visual indication that trust between the SMC and the Engine was successful. You are now ready to further configure the Engine and, later, upload a security policy.

LAB 3

Configuring Basic Routing

3.1 Getting Started

Now that the Helsinki-HQ FW has contacted the management server, you are ready to take the next step, which to is define a router. The router object allows you to define a default route that the firewall will use when sending traffic to the internet. The type of route that you will be defining is a static route, that is a route that has been manually defined.

In this lab, you will define the router that will be used as the default route. By doing this exercise, you are moving closer to being able to manage a distributed environment by defining a path for computers and servers located behind this firewall to reach the internet. Also, this exercise makes it possible for remote firewalls to reach the SMC.

3.2 Define a Router

To define routes, you can use a Router element or simply enter an IP address.

1. From the **Home** view, right-click the **Configuration** and select **Open in New Tab**. The **Configuration** view opens
2. On the left side, browse to **Network Elements** → **Routers**
3. Right-click on **Routers** and select **New Router**

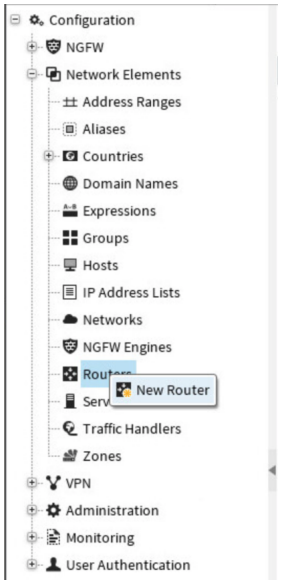


Figure 3.1: Defining a New Router - Helsinki

4. Configure the Router with the following properties:
   - Name: **Helsinki ISP A Router**
   - IPv4 Address: **172.31.1.1**

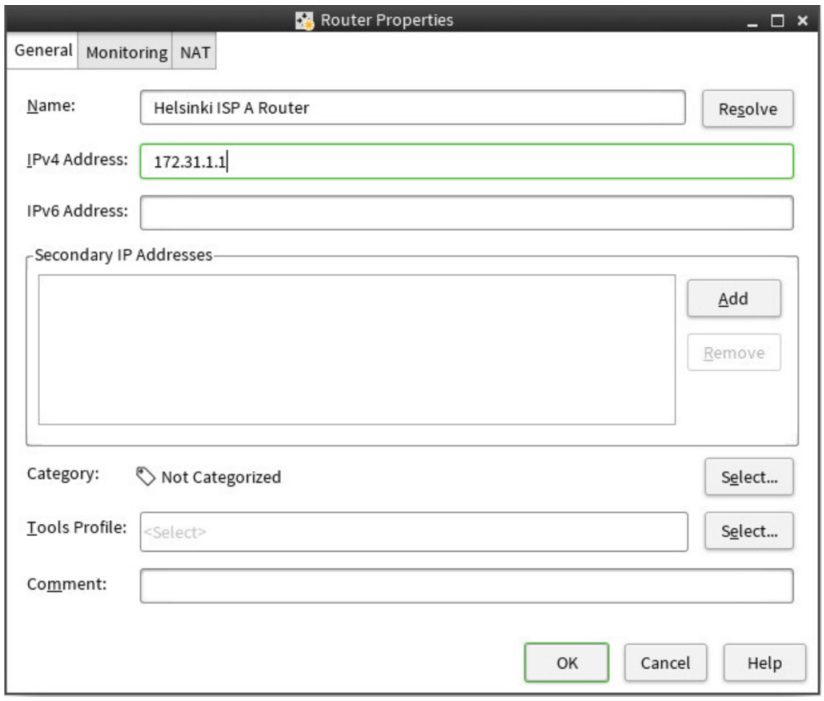


Figure 3.2: Helsinki ISP A Router Properties

5. Click **OK**. The Router Properties closes

3.3 Create a Default Route

Now you will create a default route to direct any traffic not destined to your own networks to the route of last resort - the Internet.

1. From the tab where the **Home** view is open, right-click **Helsinki-HQ FW** and select **Edit Single Firewall Helsinki-HQ FW**
2. On the left side, click on **Routing**
3. Under **Interface 1** in the pane on the right, right-click on **network-172.31.1.0/24: 172.31.1.0/24** and select **Add Router**

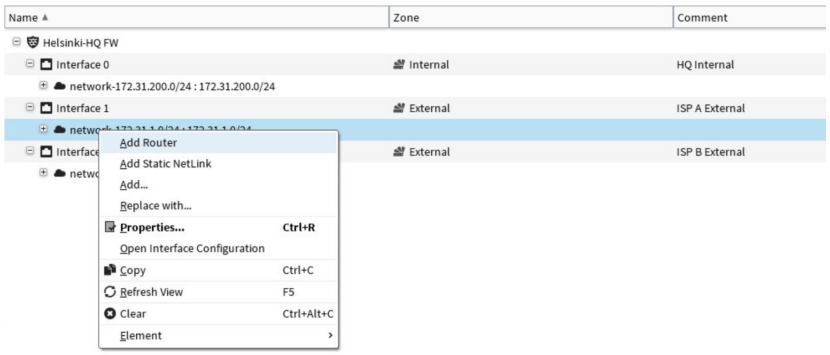


Figure 3.3: Adding Default Route for Helsinki-HQ FW

4. In the **Select Elements** dialog that opens, click on the **Helsinki ISP A Router**, and click **Add**. Click **OK**. The Select Elements dialog closes
5. Expand **Interface 1** and browse to **Helsinki ISP A Router**
6. Right-click on **Helsinki ISP A Router** and select **Set as Default Route**

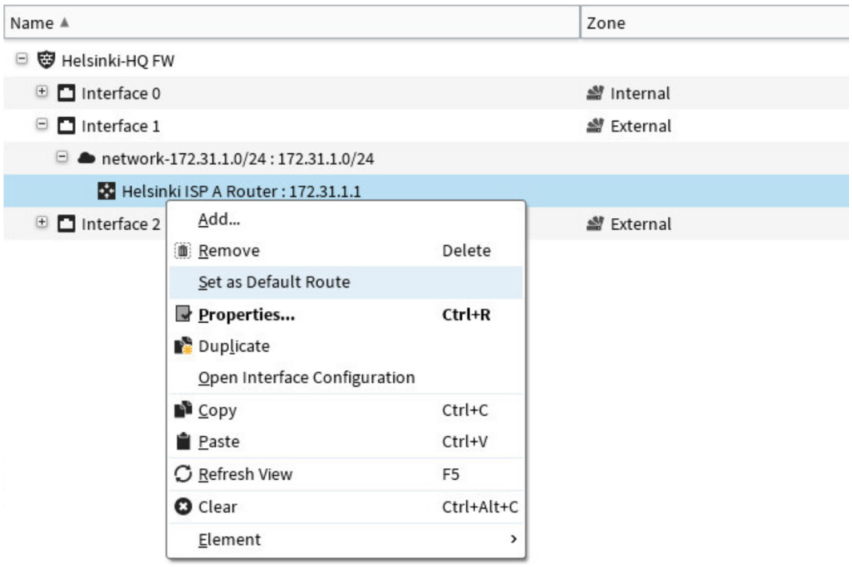


Figure 3.4: Setting the Helsinki-HQ FW Default Route

7. Click the **Expand all** icon (just above the **Name** column). The routing definition should look as in the figure below

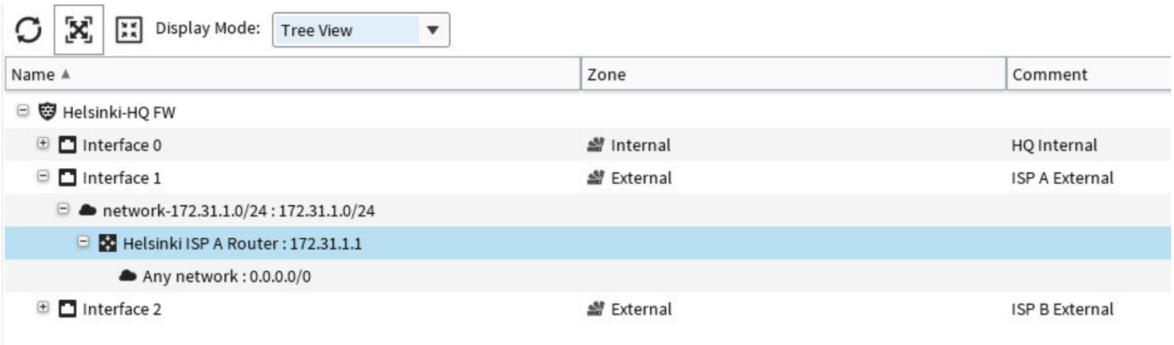


Figure 3.5: Completed Helsinki Routing View

8. In the upper right-hand corner of the Engine editor, click the **Save** button to store the changes you have just made. You may now close the tab where the **Helsinki-HQ FW** is open for editing

3.4 Summary

You have now defined the default route for the Helsinki-HQ FW. Now the Engine has a default route to the internet. This default route will get traffic from the internal network to the Internet, and, more importantly, this will allow traffic from the SMC to communicate with other firewalls that you will deploy in the labs to come.

LAB 4

NGFW Policies and Policy Templates

Getting Started

So far you have installed the SMC, defined the HQ firewall, and created a default route. The next step before you can start installing remote Engines (firewalls) is to create a security policy. To make the task of managing a distributed firewall environment easier, you will create a policy template that will be used on all Engines under management. This template will contain rules that should will be used on all Engines.

After creating the template, you will create a security policy for the Helsinki-HQ FW. This policy will contain access and NAT rules that will allow the SMC to communicate with all Engines, regardless of their physical location. As part of this, also create NAT rules that will translate traffic to and from the Internet.

At the end of this lab, the security policy rules will be in place so that remote Engines can be deployed and managed.

4.1 Creating a Policy Template

Policy Templates allow you to create a set of security policy rules that can be used on all engines, regardless of their network configurations. When changes are required that effect your entire environment, there is only one set of rules, the template, that need to be changed. In this exercise, you will create a policy template that has a rule to enforce logging and block common social media applications.

1. In the Management Client, click the **Configuration** icon. The Configuration view opens
2. From the tree view on the left, browse to **NGFW** → **Policies** → **Firewall Policies**
3. On the right side of the Management Client, click **New** and select **Firewall Policy Template**. The Firewall Template Policy Properties opens

Figure 4.1: New Firewall Policy Template

4. In the **Name** field, enter **Global Firewall Template**

5. In the **Template** pane, click on the **Firewall Template**

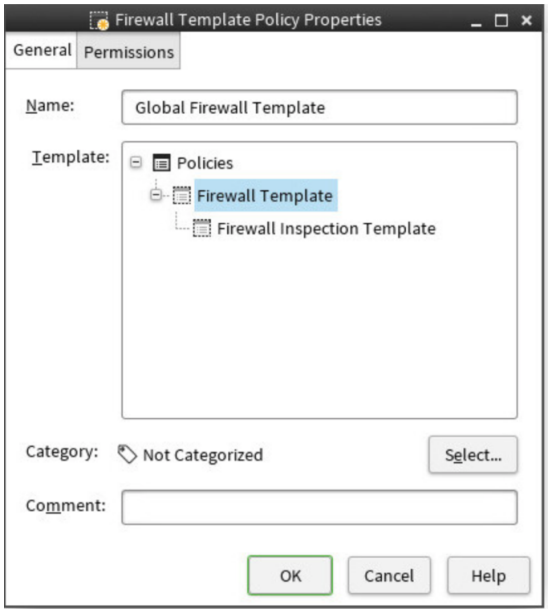


Figure 4.2: Global Firewall Template Properties

6. Click **OK**. The **Global Firewall Template** opens for editing

4.1.1 Add a Template Rule for Logging

The first rule you are going to add is a Continue rule that will ensure that all connections on all firewalls are being logged. The rule will preclude the need to enable logging on every rule individually.

TIP: While doing this lab, finding objects and services can be made easier by clicking in a cell and entering part of name or number that you are attempting to find. A list of matching objects appears, allowing you to select the appropriate one.

1. Double-click the green Insert Point, **IPv4 Insert Point - add rules here**. An empty rule appears

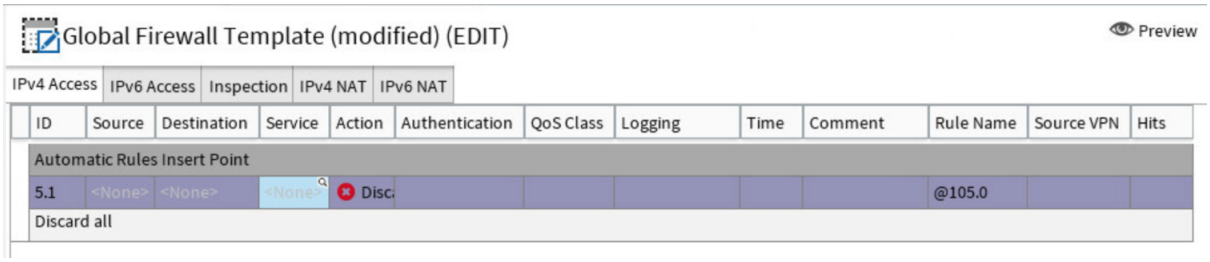


Figure 4.3: New Empty Template Rule

2. Configure the rules as follows:
   - **Source**: Right-click and select **ANY**
   - **Destination**: Right-click and select **ANY**
   - **Service**: Right-click and select **ANY**
   - **Action**: Right-click and select **Continue**
   - **Logging**: Right-click and select **Edit Logging**. The **Logging - Select Rule Options** dialog opens
3. Check the box for **Override Settings Inherited from Continue Rule(s)**

4. Use the **Logging Level** drop-down menu and select **Stored**
5. Use the **Connection Closing** drop-down menu and select **Log Accounting Information**
6. Check the for **Override Recording Settings Inherited from Continue Rule(s)**
7. Use the drop-down menu and set **Log Network Applications** to **Enforced**

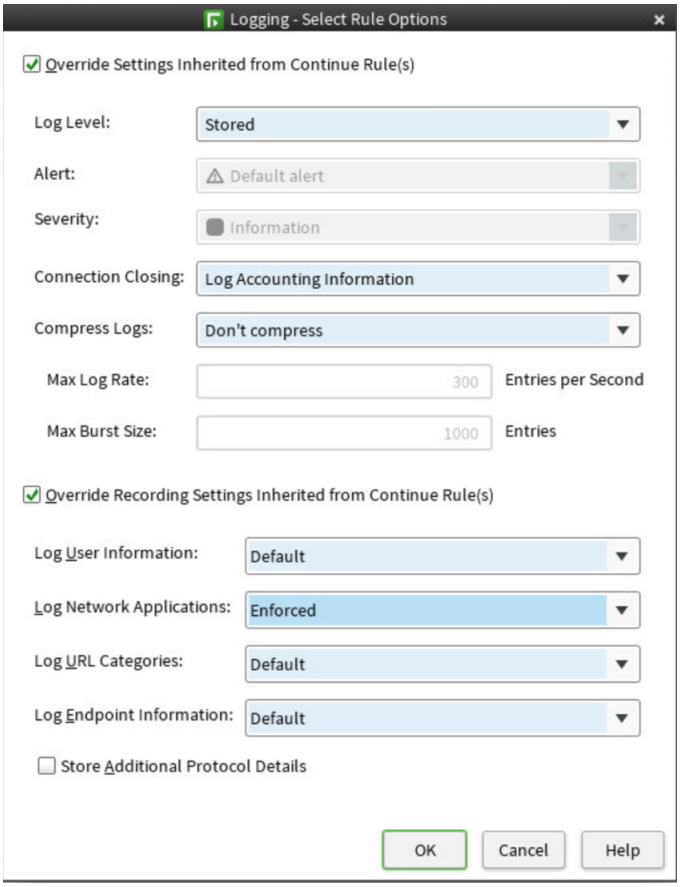


Figure 4.4: Global Template Logging Options

8. Click **OK**. The Logging Options dialog closes. Your completed Continue Rule for logging should appear as in the figure below

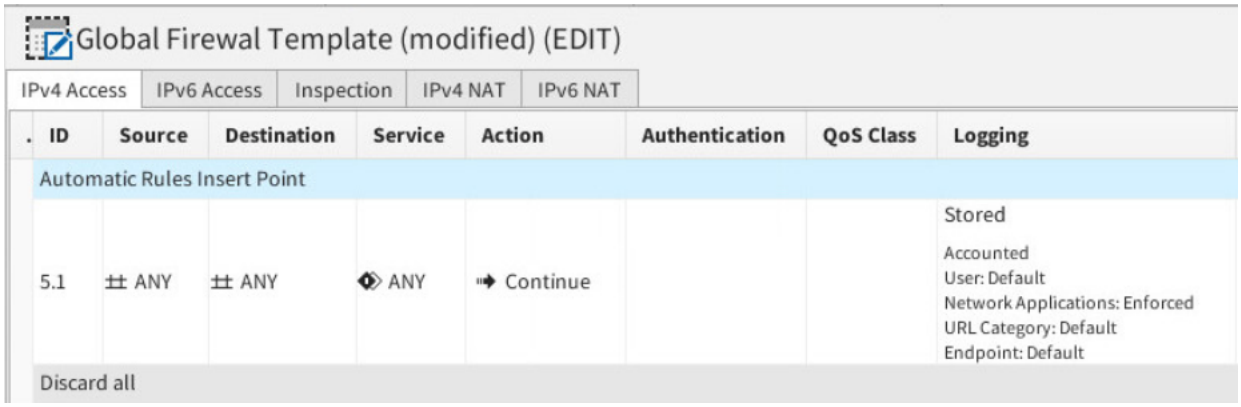


Figure 4.5: Completed Logging Continue Rule - Global Template

4.1.2 Add a Rule to Block Social Media Network Applications

The next rule you add will be to block social media network applications. In this exercise, you will block Facebook, Twitter, and Google Hangouts.

1. Right-click in the **ID** column of the rule you created above, and select **Add Rule After**. A new blank rule appears
2. Configure the rule with the following values
   - **Source**: Right-click and select **ANY**
   - **Destination**: Right-click and select **ANY**
   - **Service**: Click into the cell and type `Facebook`. Select the **Facebook** network application from the list. Repeat this step for **Twitter** and **Snapchat**

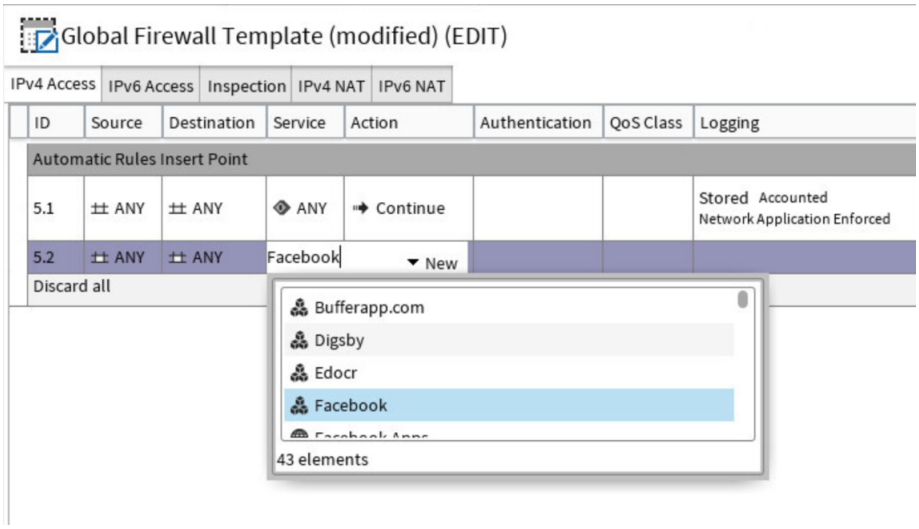


Figure 4.6: Blocking Facebook - Global Template

- **Action**: Right-click and select **Discard**. Your completed rule should look as in the figure below

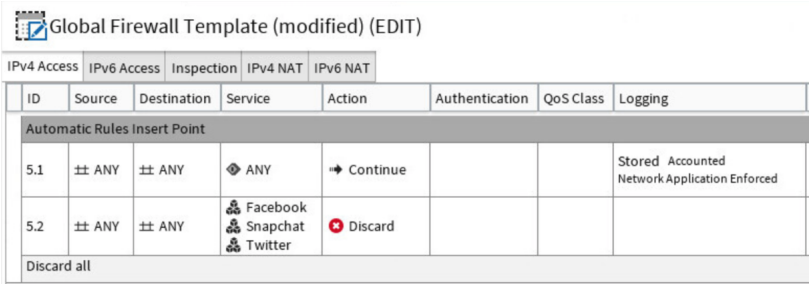


Figure 4.7: Blocking Social Media Applications

4.1.3 Add a Template IPv4 Access Rule Insert Point

Because you are creating a template, upon which other policies will be based, you must now create an Insert Point where the rules from the child policies will be inserted in the template. In this exercise, you will place the Insert Point after the last rule you created in the previous exercise. This means that the two template rules you created will be processed then the rules from policies based on this template. The Insert Point ensures that the rules are processed in the correct order.

1. Right-click in the **ID** column of rule **5.2** and select **Add Insert Point After**. The Insert Point dialog opens
2. In the field provided for the Insert Point name, enter **Local Firewall Policy Rules**

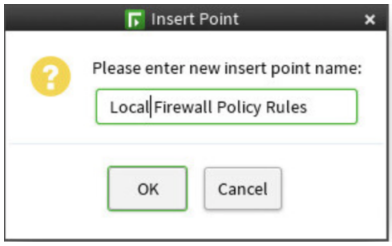


Figure 4.8: Naming the Insert Point

3. Click **OK**. The Insert Point dialog closes
4. Click the **Save** button. Your completed Global Template IPv4 Access Rules should appear as in the figure below

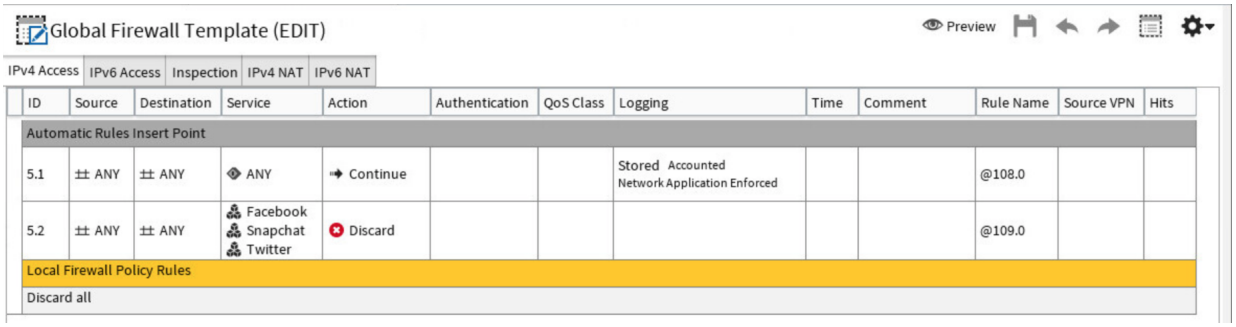


Figure 4.9: Completed Global Template

4.1.4 Add a Template IPv4 NAT Rule Insert Point

Just as you did in the last exercise, you must also create an Insert Point for NAT rules.

1. With the **Global Firewall Template** still open for editing, click on the **IPv4 NAT** tab
2. Right-click on the rule, **IPv4 NAT Insert Point - add rules here** and select **Add Insert Point**. The Insert Point dialog opens
3. In the field provided, enter **Local Firewall NAT Rules**
4. Click **OK**. The Insert Point dialog closes
5. Click the **Save** button. Your completed Global Template IPv4 NAT rule Insert Point should appear as in the figure below

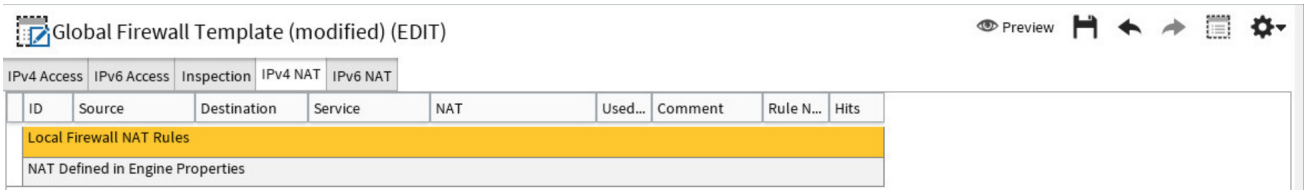


Figure 4.10: Global Template NAT Insert Point

6. Click the **Save** icon to save your work on the policy. You may close the tab where the template is open for editing

Summary

In this lab, you have created a policy template that will ensure all firewalls under management have the same core set of rules. Should any changes be required for the entire managed firewall environment, one only had to adjust the template and

install the policies. Write once, use everywhere. This will put you in a position to deploy other firewalls in remote locations and manage them. In the next lab, you will create Locations and Contact Addresses, and policy rules that will allow traffic between the SMC and the remote firewalls.

LAB 5

Distributed System Configuration

Getting Started

In the previous lab, you installed and licensed the SMC. In the labs that follow, you will be configuring and deploying firewalls. One of those is local to the SMC, and the others are in remote locations, Atlanta and Paris. Because the SMC is on a directly connected network to the Headquarters location, the SMC and the Headquarters firewall will communicate using their real IP addresses. For the firewalls at the Atlanta and Paris locations, they will be communicating with the SMC *through* the Headquarters firewall, meaning that the remote firewalls will have to use the NAT IP of the management server.

In this lab, you will ensure that firewalls, local or remote to the SMC, are using the correct IP addresses for communication with the SMC. To do this, you will configure locations and contact IP addresses that define the correct IP addresses to use for Management and Logging communications.

As part of this lab, you will also enable Webstart on the Management Server. Enabling this feature allows anyone with a web browser to download the management client. This avoids the need to install the management client locally, and it ensures that you will always be using to correct version of the client.

5.1 Create a Location

Built into the SMC is a default location, called *Default*. Anything that is part of the Default location uses the real IP of the SMC, 172.31.200.101, for management and logging communication. For firewalls or other managed objects that are remote to the SMC will use the NAT IP of the SMC, 172.31.1.101.

A location can be thought of as a point of view. From the point of view the Default location, real IPs are used. You will now create a Remote location and define that IPs that will be used for Management and Logging communications from its point of view.

1. From the **Home** view in the Management Client, click the **Configuration** icon. The Configuration view opens
2. On the left side, browse to **Administration** → **Other Elements** → **Locations**

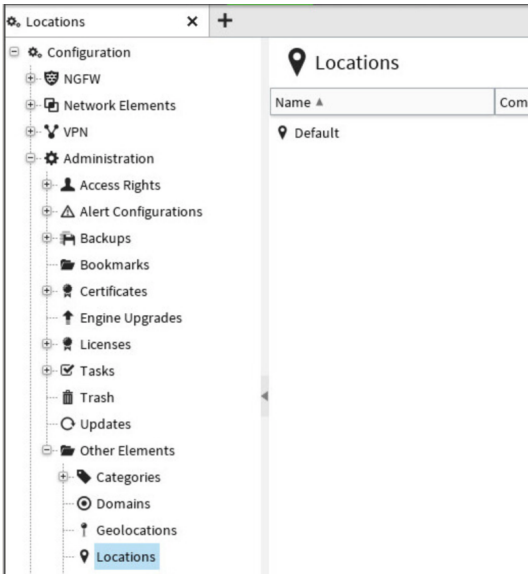


Figure 5.1: Browsing to Locations

3. In the upper right corner, click the **New** icon and select **Location**. The Location Properties opens
4. In the **Name** field, enter **Remote**

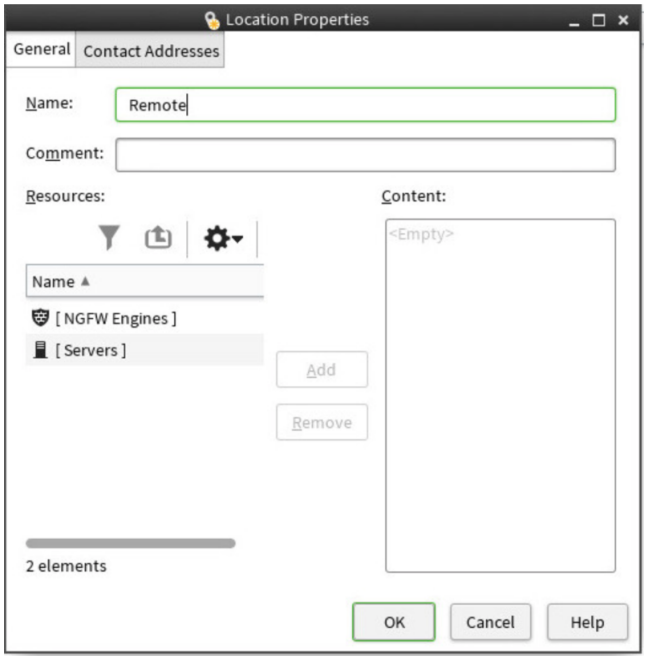


Figure 5.2: Remote Location Properties

5. Click **OK**. The Remote Location Properties closes

5.2 Configure Contact Addresses for the Management and Log Servers

Now that you have configured a location, you will now configure that IP address that is used for the Management and Log servers from the perspective of the *Remote* location.

1. In the Menu toolbar, click the **Home** icon. The Home View opens

2. On the left, click **Others**

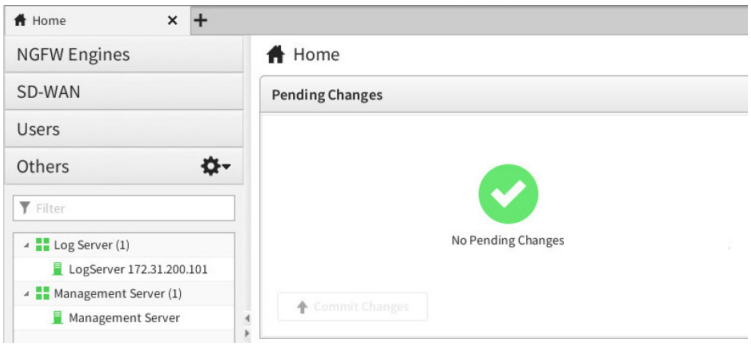


Figure 5.3: The “Others“ View

3. Right-click on the **Management** server, and select **Properties**

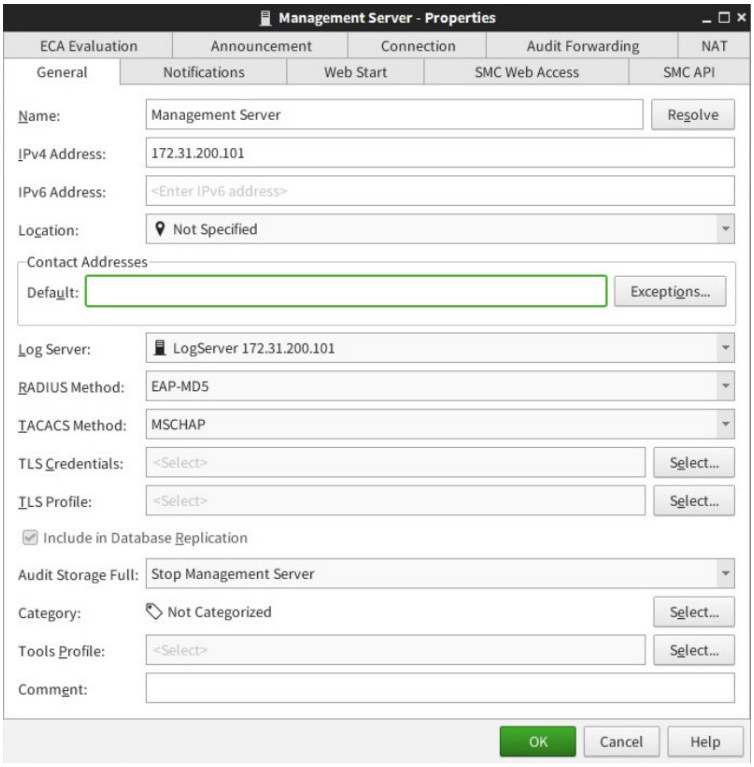


Figure 5.4: Management Server Properties

4. Click **Exceptions**. The Exceptions editor opens
5. Click **Add**. The Select Elements dialog opens

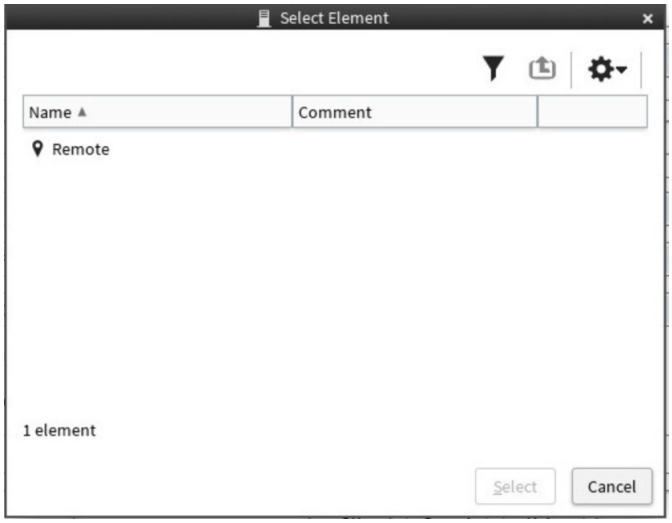


Figure 5.5: Selecting the Remote Location

6. Click on the **Remote** location, and then click **Select**. The Select Elements dialog closes
7. In the Exceptions Editor, enter **172.31.1.101** in the **Contact Addresses** field

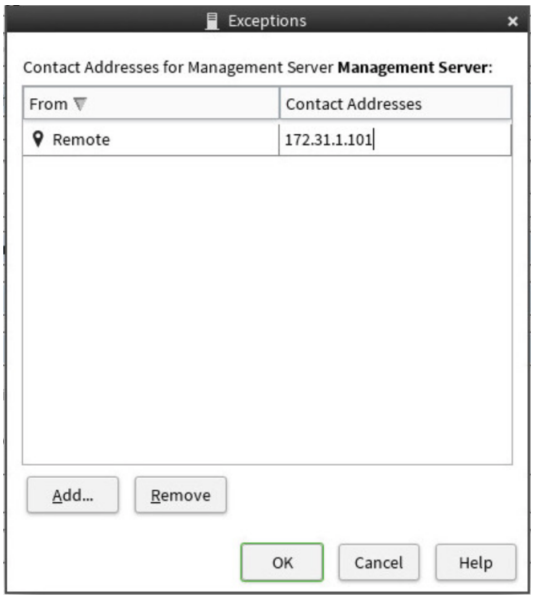


Figure 5.6: Completed Exception for Management Server

8. Click **OK**. The Exception Editor closes
9. Click **OK**. The Management Server properties closes

NOTE: You may receive a duplicate IP address warning. This simply lets you know that there is another object with the same IP address. This does not represent a conflict. You may click **Yes**.

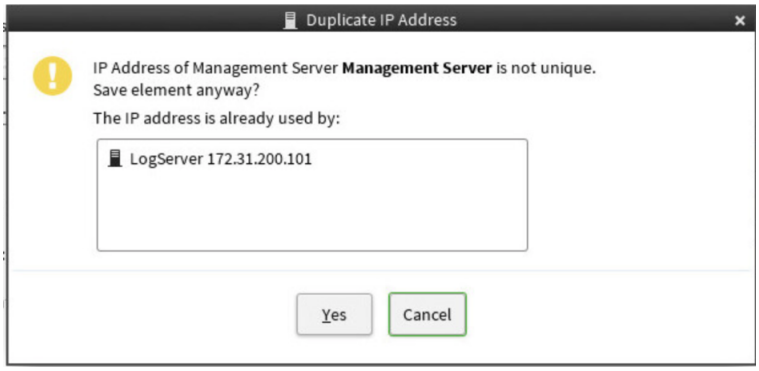


Figure 5.7: Non-Unique IP Warning

Now that you have configured the Contact IP address for the Management Server from the perspective of Remote location, you will now do the same for the Log Server.

1. From the **Home** view, right-click on the **Log** server and select **Properties**. The Log Server Properties opens

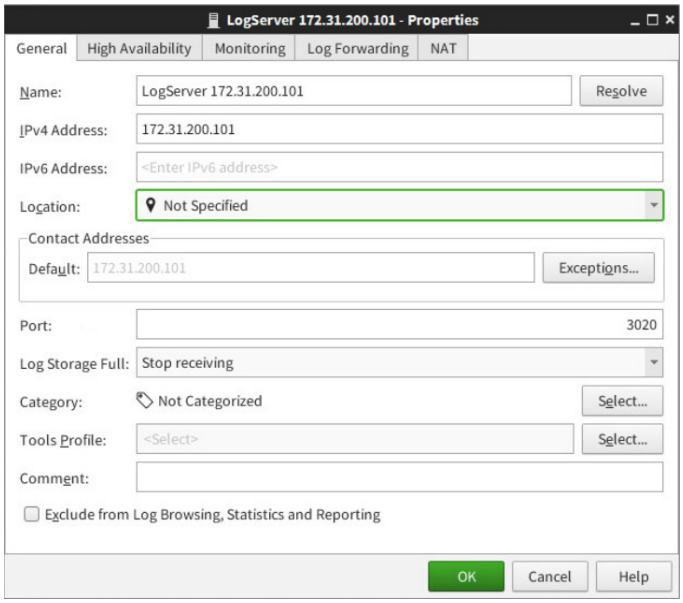


Figure 5.8: Log Server Properties

2. Click **Exceptions**. The Exception editor opens
3. Click **Add** and select the **Remote** location. Click **Select**. The Select Elements dialog closes
4. In the Exceptions Editor, enter **172.31.1.101** in the **Contact Addresses** field

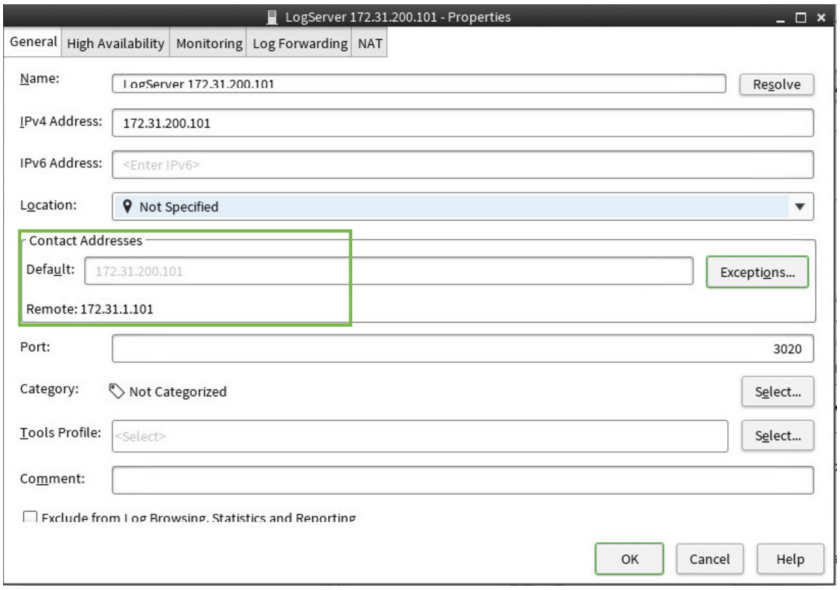


Figure 5.9: Completed Exception for Log Server

5. Click **OK**. The Exception Editor closes
6. Click **OK** to close the Log Server properties

5.3 Enable the Remote Web Access

To make deployment of the Management Client easier, you will now enable the SMC Web Access on the Management Server. This will allow you to run the Management Client inside your browser as a Web application. This eliminates the need to install it on your local machine.

1. From the **Home** view, on the left side, navigate to the **Others** section
2. Right-click on the **Management** server and select **Properties**. The Management Server properties opens
3. Click on the **SMC Web Access** tab
4. Check the **Enable** checkbox
5. In the **Hostname** field, enter **smc.webaccess.com**
6. In the **Port Number** field, enter **8080**
7. In the **Server Credentials** field, click on **Select**
8. The **Select** window will open, click on the tool icon then **New** → **TLS Credentials**
9. The New TLS Credentials window will open.
10. In the **Name** field enter **smc.webaccess.com** and repeat the same for the **Common Name** field.

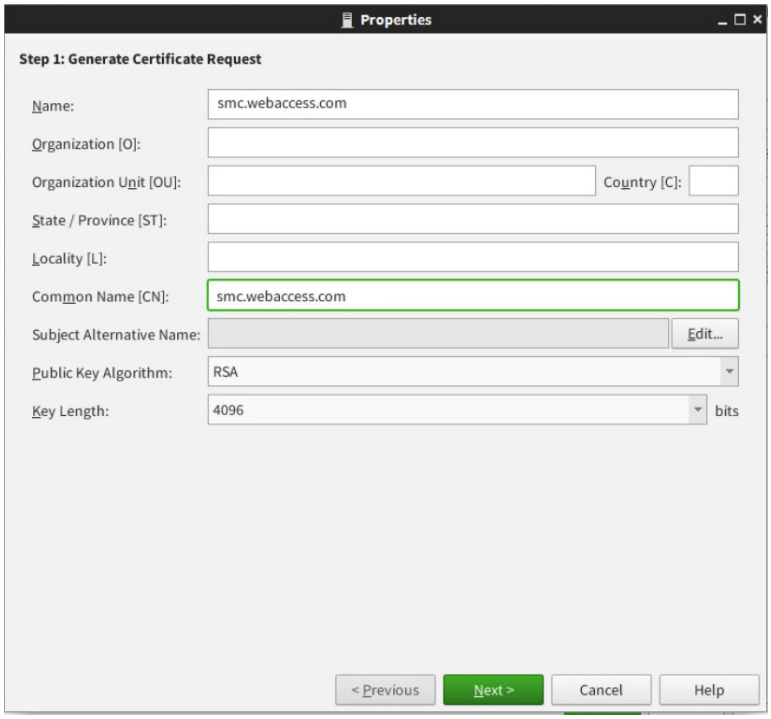


Figure 5.10: New TLS Credentials Certificate Step 1

11. Click on **Next**
12. In the **Step 2** page, select the Option **Sign with Internal CA**

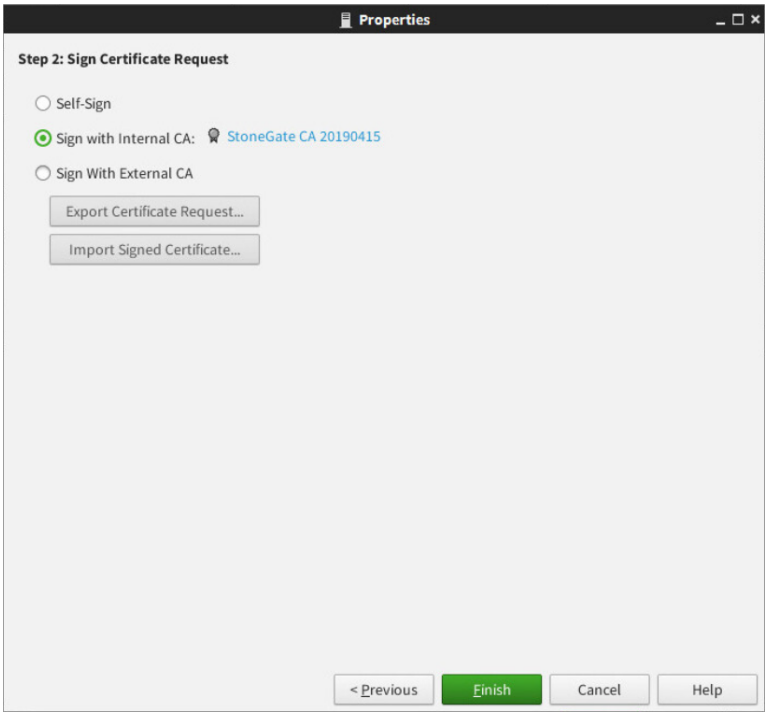


Figure 5.11: New TLS Credentials Certificate Step 2

13. Click on **Finish**
14. In the Select Element window, select the newly created **smc.webaccess.com** TLS Credentials and click on **Select**

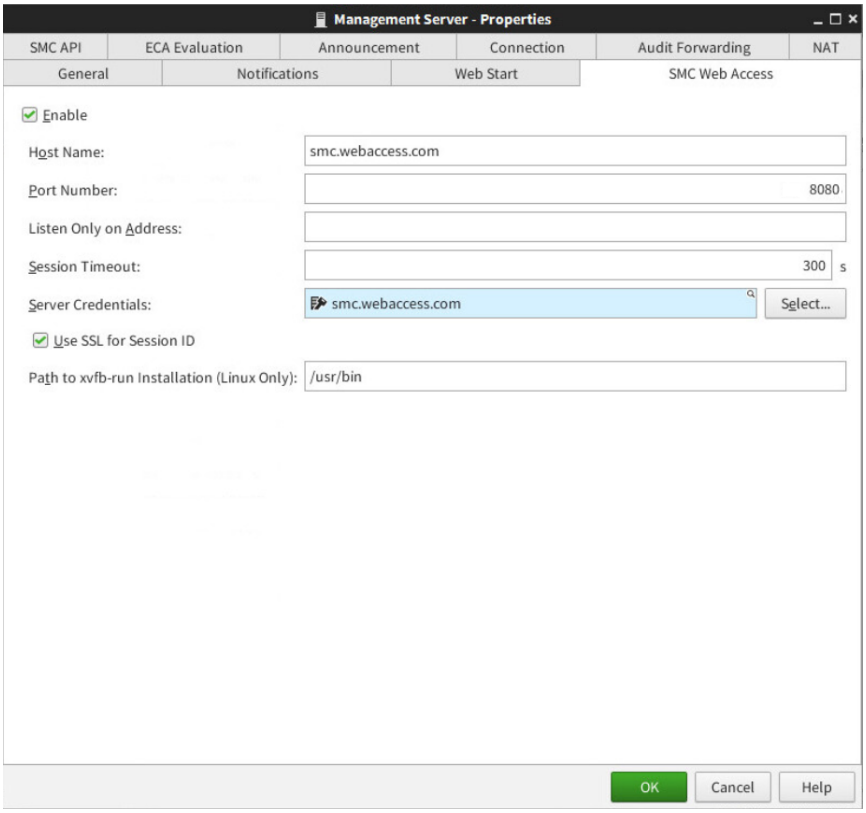


Figure 5.12: SMC Web Access Configured

15. Click **OK**. The Management Server properties closes

NOTE: You may receive a duplicate IP address warning. This simply lets you know that there is another object with the same IP address. This does not represent a conflict. You may click **Yes**.

5.4 Create the Helsinki HQ Policy Access Rules

You have just completed the Global Firewall Template, upon which all of your other policies will be based. You have also created locations and contact IP addresses that define the proper addresses to be used for system communications. In this exercise, you will create the policy specific to the Helsinki-HQ FW. These rules will permit management connections through the Helsinki-HQ FW to the SMC so that remote firewalls can be managed.

1. In the tab where **Firewall Policies** is still open, right-click on the **Global Firewall Template** you created in the last lab and select **New** → **Firewall Policy**. The **Firewall Policy Properties** opens

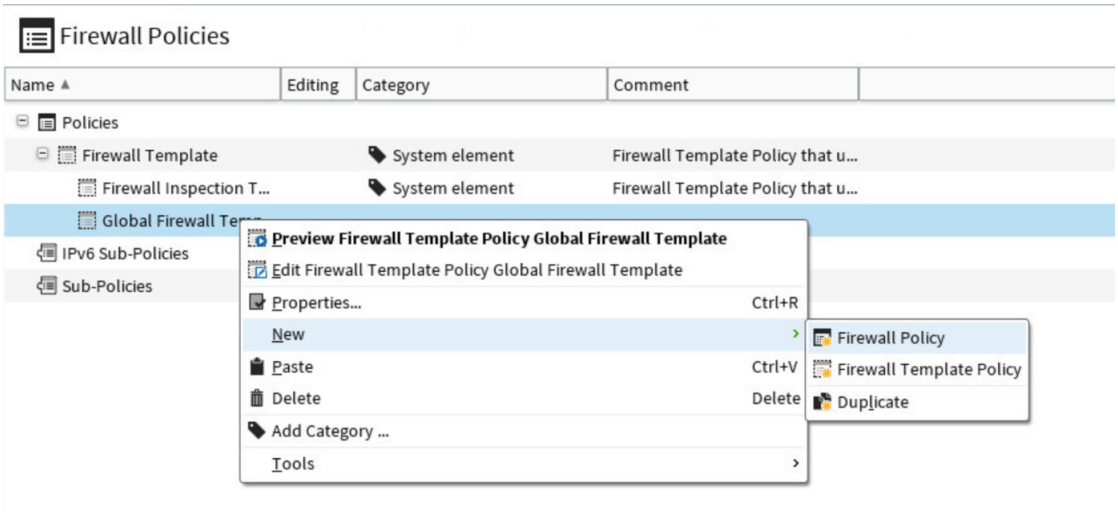


Figure 5.13: Creating a New Firewall Policy - Helsinki-HQ FW

2. In the **Name** field, enter **HQ Policy**
3. Make sure that the **Global Firewall Template** is selected

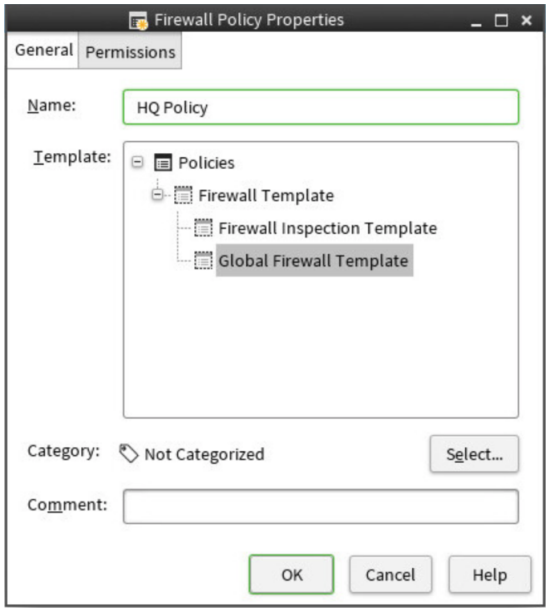


Figure 5.14: HQ Policy Properties

4. Click **OK**. The **HQ Policy** opens for editing

5.4.1 Create a Group Object for Remote Firewalls

In this exercise, you will create a Group Object that contains the firewalls that you will remotely manage. In the labs that follow, you will add two (2) firewalls to this group.

1. In the tree view on the left side, browse to **Network Elements** → **Groups**
2. Click the **New** icon and select **Group**. The Group Properties dialog opens

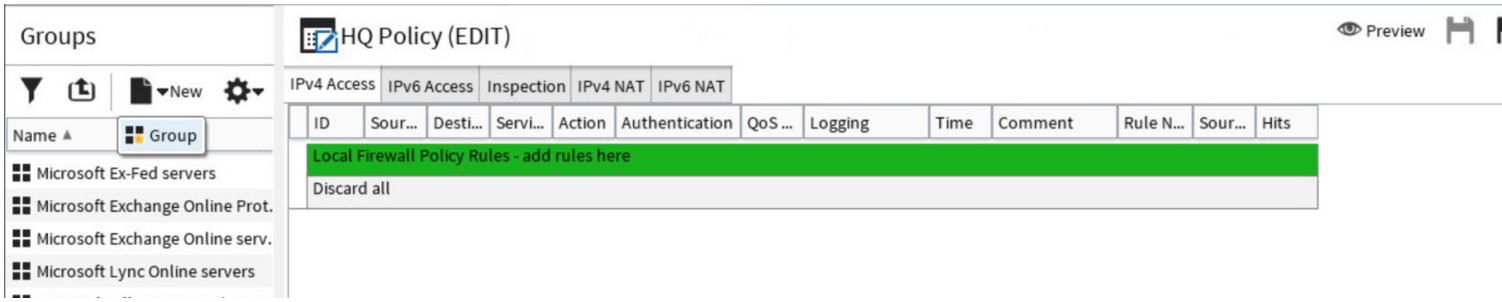


Figure 5.15: Defining a New Group Object

3. In the **Name** Field, enter **Global Firewalls**
4. Click **OK**. The Group Properties closes

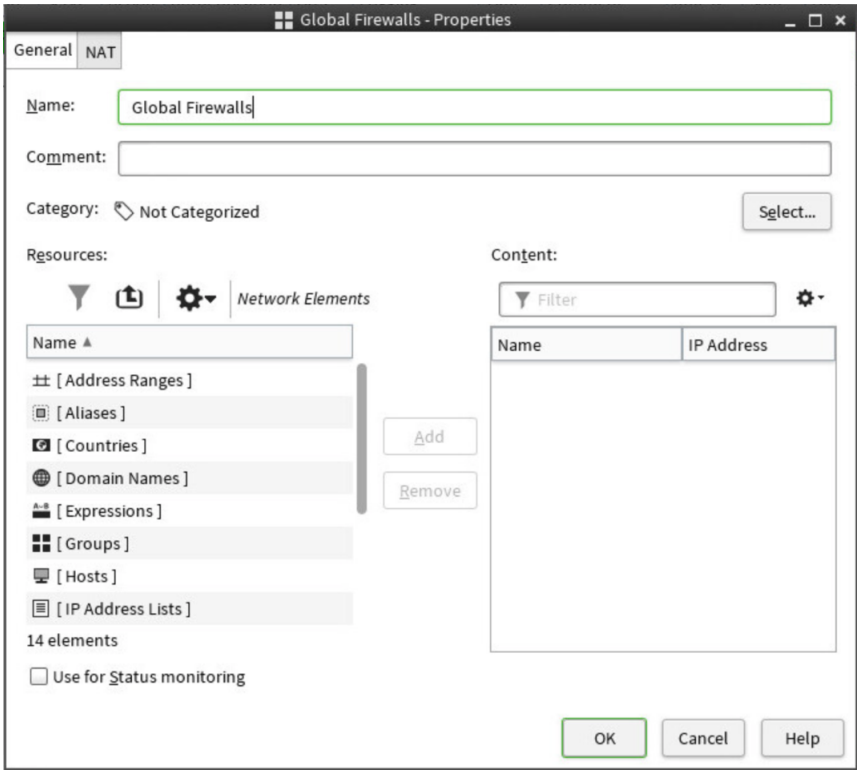


Figure 5.16: Global Firewalls Group Properties

NOTE: The Global Firewalls group is empty right now. When you define the remote firewalls later, you will add those firewalls to this group object.

5.4.2 Create an Expression

In this exercise, you will create an Expression that defines the “Internet“ as being *not* the Helsinki internal network, 172.31.200.0/24. This will be used in the firewall policy rules.

1. In the tree view on the left, navigate to **Network Elements** → **Expressions**

   TIP: Use the icon in the figure below to navigate the tree view

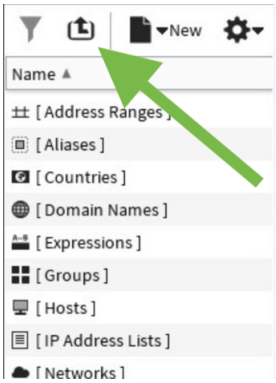


Figure 5.17: Navigating the Object Tree View

2. Click the **New** icon and select **Expression**. The Expression Properties dialog opens
3. In the **Name** field, enter **not Helsinki Internal Networks**
4. Click the negate icon, which looks like this: ˜ This symbol means **not** or negate
5. Click the **Add Element** icon. The Select Element dialog opens
6. Browse to **Network Elements** → **Networks** and select **network-172.31.200.0/24**

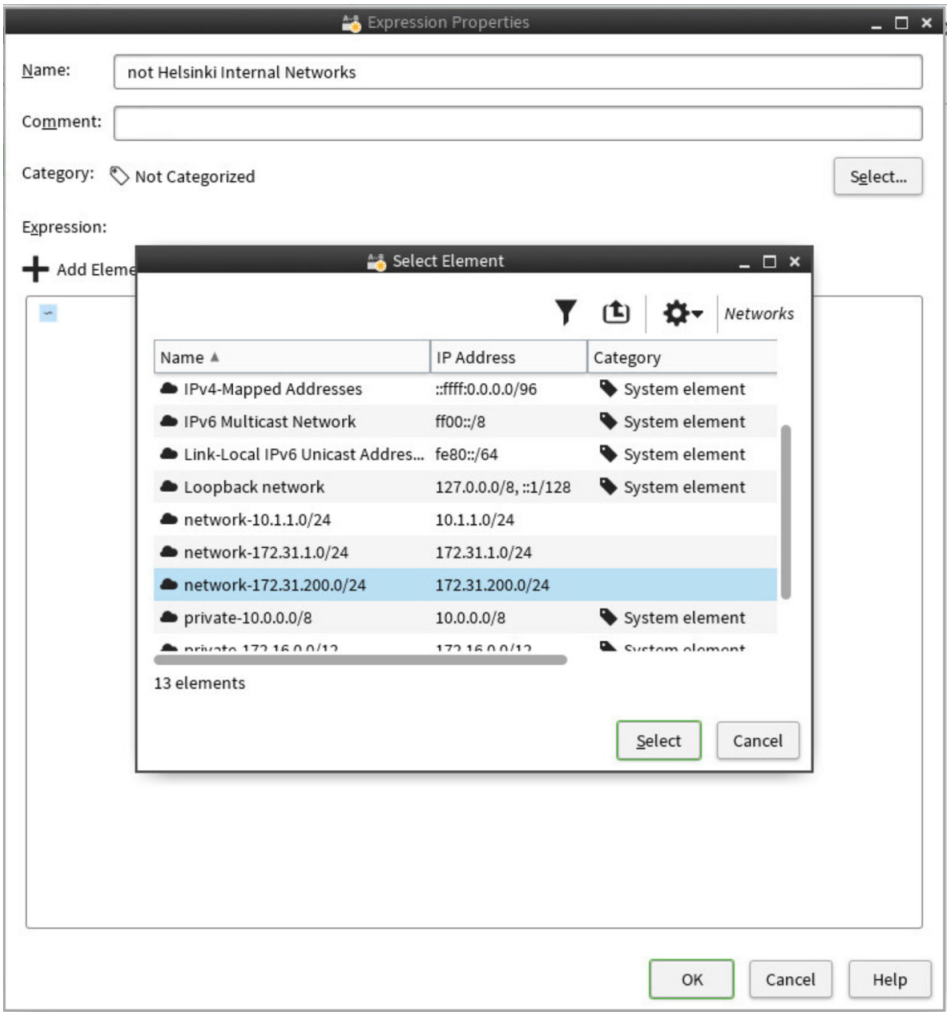


Figure 5.18: Helsinki Not Internal Expression

7. Click **Select**. The Select Element dialog closes. You fully configured expression should appear as in the figure below

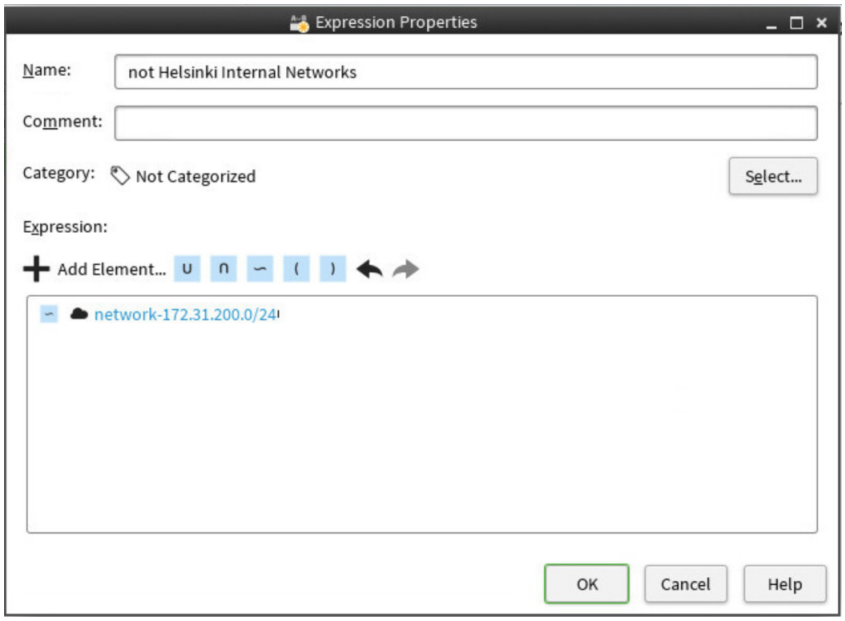


Figure 5.19: Fully Configured Not Helsinki Network Expression

8. Click **OK**. The Expression Properties closes

5.4.3 Create the Management/Log Server NAT Address

In this exercise, you will create a host object that represents the public address of the Management and Log servers (remember that the Management and Log Servers are installed on the same server). This host object will be used to allow traffic from the Internet to be NATed to the real IP of the Management Server.

1. In the tree view on the left, navigate to **Network Elements** → **Hosts**
2. Click the **New** icon and select **Host**. The Host Properties opens
3. In the **Name** field, enter **Management Server (NAT)**
4. In the **IPv4 Address** field, enter **172.31.1.101**
5. Click **OK**. The Host Properties closes. Your fully configured host should appear as in the figure below

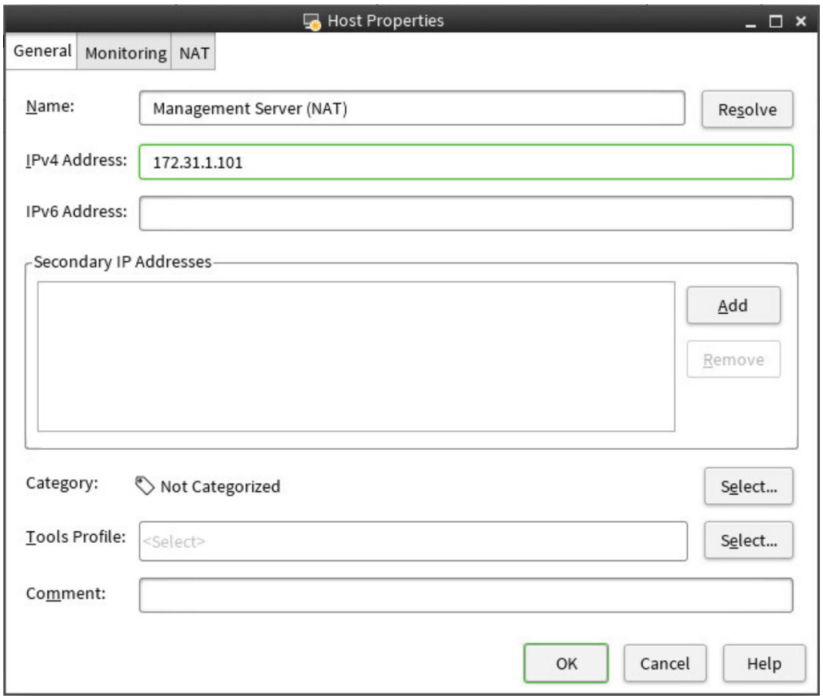


Figure 5.20: Management Server NAT Host Object

5.4.4 Create an Access Rule for Management Client Traffic and Other Services

In this exercise you will create rules that permit traffic from Global Firewalls to the SMC. **NOTE**: In this rule, there are additional services such as SSH, Ping, HTTP, HTTPS, and HTTP proxy that are needed for other services that are needed for the purposes of these labs.

1. In the Policy Editor, double-click on the green insert point, **Local Firewall Policy Rules - add rules here**. A new empty rule is added
2. Configure the rule as follows:
   - **Source**: click into the **Source** cell and type `not h` A list of matching objects appears. Select **not Helsinki Internal Networks**

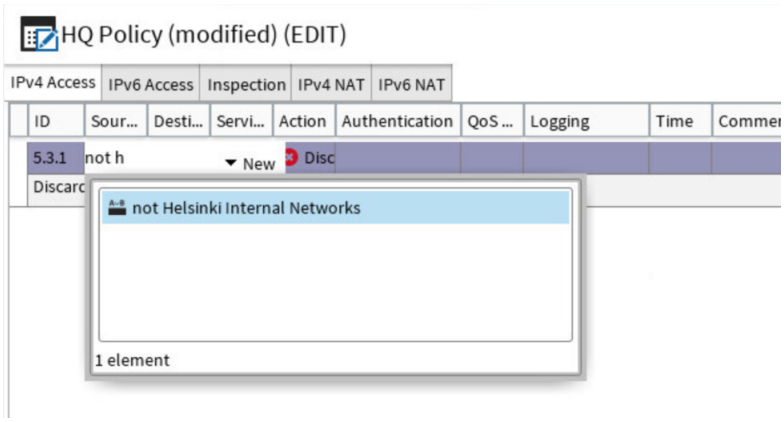


Figure 5.21: Type-ahead Searching - HQ Policy

   - **Destination**: click into the **Destination** cell and type `172.31.1.101` Select the **Management Server (NAT)** host
   - **Service**: Click into the **Service** cell and configure the following
     (a) Type 22 and select **SSH**

(b) Type `8080` and select **HTTP proxy**

NOTE: There is no HTTP proxy running. You are simply allowing port 8080 for remote access to the Management client, which will be covered later.

(c) Type `DNS` and select **DNS** from the list. This service group contains DNS UDP and DNS TCP

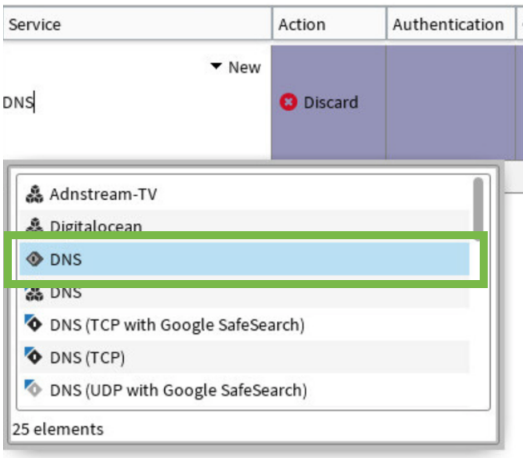


Figure 5.22: Selecting the Correct DNS Service

(d) Type `80` and select **HTTP**
(e) Type `21` and select **FTP**
(f) Type `443` and select **HTTPS**
(g) Type `ping` and select **Ping**. Please refer to the figure below to select the correct service group

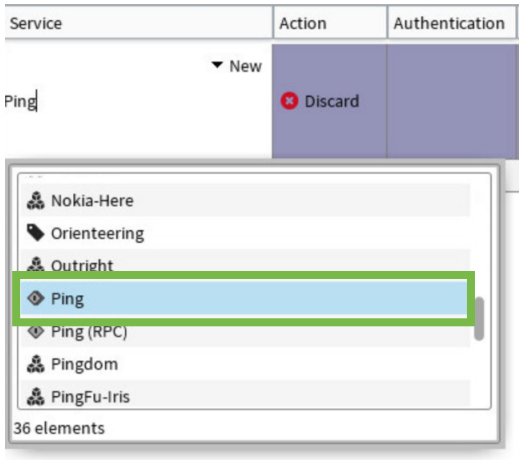


Figure 5.23: Selecting the Ping Service Group

(h) Type `sg client` and select **SG Client to Log**
(i) Repeat the last step, this time selecting **SG Client to Management**

- **Action**: Right-click and select **Allow**. Your completed rule should appear as in the figure below

5.5.3.5	not Helsinki Internal Networks	Management Server (NAT)	DNS FTP HTTP HTTP proxy HTTPS Ping SG Client to Log SG Client to Management SSH	Allow

Figure 5.24: Completed SMC Client to Management Rule

5.4.5 Create an Access Rule for Management Server to Global Firewalls

In this exercise, you will add a rule that permits the Management Server to control and get information from the firewall Engines.

1. Right-click in the **ID** column of the second rule, and select **Add Rule After**. A new empty rule is added
2. Configure the new rule as follows:
   (a) **Source**: Type `Management Ser` and select **Management Server**
   (b) **Destination**: Type `Global` and select **Global Firewalls**
   (c) **Service**: Click into the **Service** cell and add the following services
      - Type `sg con` and select **SG Control**
      - Type `sg manage` and select **SG Management to Firewall**
   (d) **Action**: Right-click and select **Allow**. Your completed rule should appear as in the figure below

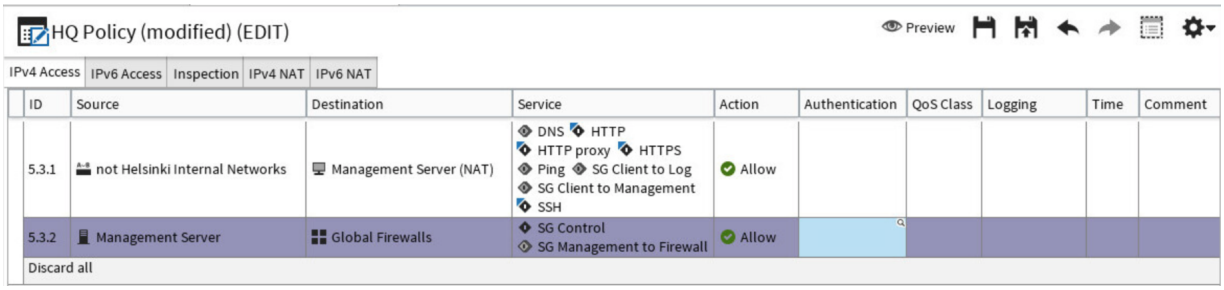


Figure 5.25: Completed Management to Firewall Rule

5.4.6 Create an Access Rule for Global Firewalls to Management Server

In the last exercise, you permitted the Management Server to communicate to the Global Firewalls. You will now add a rule that permits the Global Firewalls to send management and log related information to the Management and Log Servers (installed on the same server).

1. Right-click in the **ID** column of the last rule, and select **Add Rule After**. A new empty rule is added
2. Configure the new rules as follows:
   - **Source**: Type `Global` and select **Global Firewalls**
   - **Destination**: Type `Management Ser` and select **Management Server (NAT)**
   - **Service**: Click into the **Service** cell and add the following services
     (a) Type `sg engine` and select **SG Engine to Log**
     (b) Repeat the previous step and select **SG Engine to Management**
   - **Action**: Right-click and select **Allow**. Your completed rule should appear as in the figure below

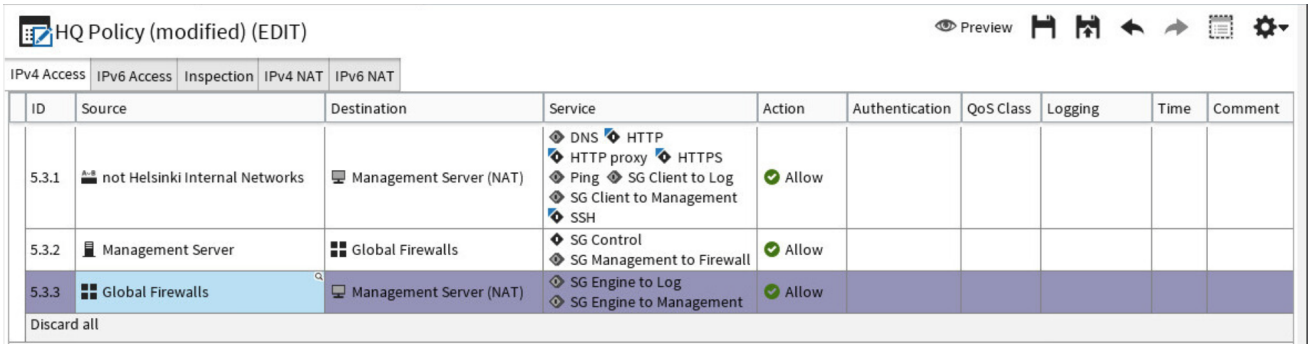


Figure 5.26: Completed Firewall to Management Rule

5.4.7 Create an Access Rule Allowing Internal Network to Internet

You now have all of the rules in place for allowing Management and Logging connections to and from your remote firewalls. Now you will create a rule that allows traffic from the Helsinki internal network to the internet. For now, we will allow all traffic out.

1. Right-click in the **ID** column of the first rule, and select **Add Rule After**. A new empty rule is added
2. Configure the new rule as follows:
   (a) **Source**: in the tree view on the left, navigate to **Network Elements** → **Networks**. Drag and drop the **network-172.31.200.0/24** in the **Source** cell
   (b) **Destination**: in the tree view on the left, navigate to **Network Elements** → **Expressions**. Drag and drop the expression you created above, **not Helsinki Internal Networks** into the **Destination** cell
   (c) **Service**: Right-click and set to **ANY**
   (d) **Action**: Right-click and select **Allow**. Your completed rule should appear as in the figure below

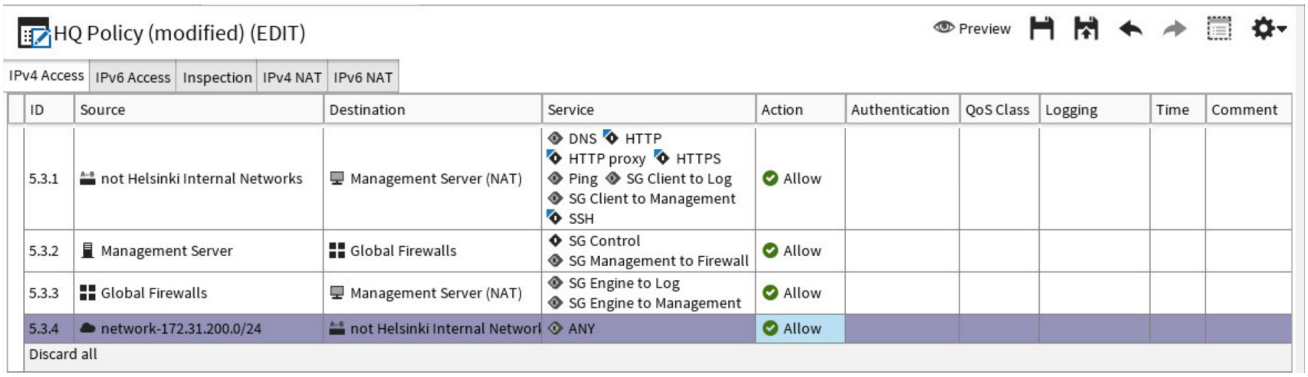


Figure 5.27: Completed Internal Network to Internet Rule

NOTE: In this last exercise, you used the drag and drop method of populating cells to get you familiar with both ways of creating rules.

5.5 Defining HQ Policy NAT Rules

So far you have been working with Access Rules. However, to get traffic from the Public side of the firewall to the Private side, you will need to write NAT rules. In this exercise, you will create two (2) NAT rules, one NATing traffic from the Internet to the Management Server and one NATing internal network traffic to the Internet.

5.5.1 Create a Static Destination NAT rule for the Management Server

The first thing you must do is create a rule that NATs traffic destined for 172.31.1.101 (the NAT IP of the Management Server) to the real IP of the Management Server. This is known as a Static Destination NAT.

1. With the Policy Editor still open, click on the **IPv4 NAT** tab
2. Double-click the insert point, **Local Firewall NAT Rules - add rules here**. A new empty rule appears
3. Configure the new rule as follows:
   - **Source**: in the tree view on the left, navigate to **Network Elements** → **Expressions**. Drag and drop **not Helsinki Internal Networks** to the **Source** cell
   - **Destination**: type `Management` and select **Management Server (NAT)**
   - **Service**: leave this set to **ANY**
   - **NAT**: in the **NAT** cell, right-click and select **Edit NAT**. The Network Address Translation dialog opens

(a) Click on the **Destination Translation** tab
(b) Check the box next to **Translate Destination**
(c) Next to the **Translated** field, click **Select**. The Select Element dialog opens
(d) Browse to **Network Elements** → **Servers**

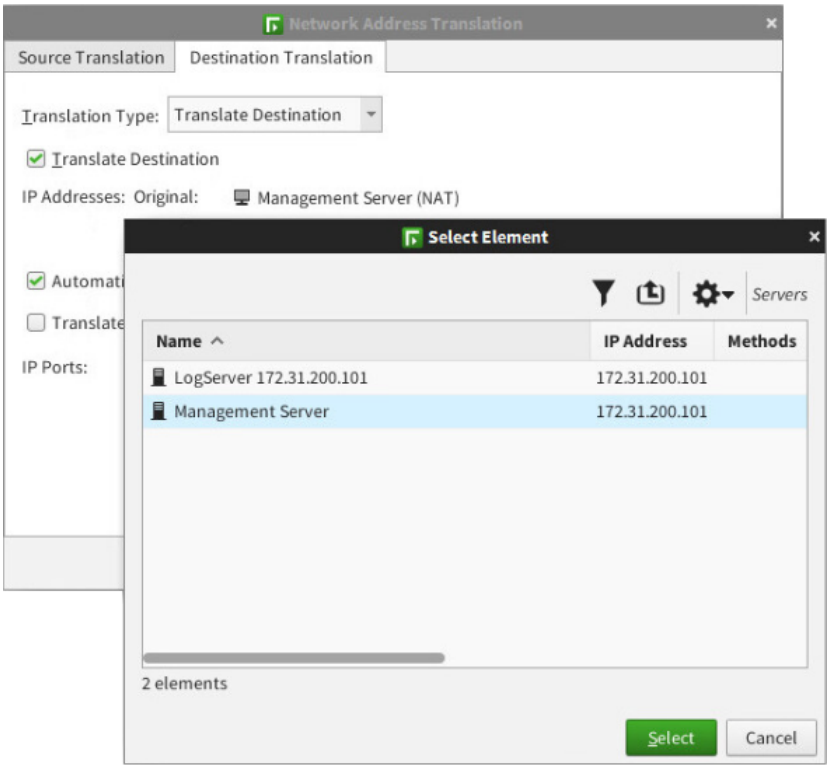


Figure 5.28: Select the Management Server for NAT Destination

(e) Click on **Management Server** and click **Select**. The Select Element dialog closes
(f) Make sure that **Automatic Proxy ARP (Recommended)** is checked

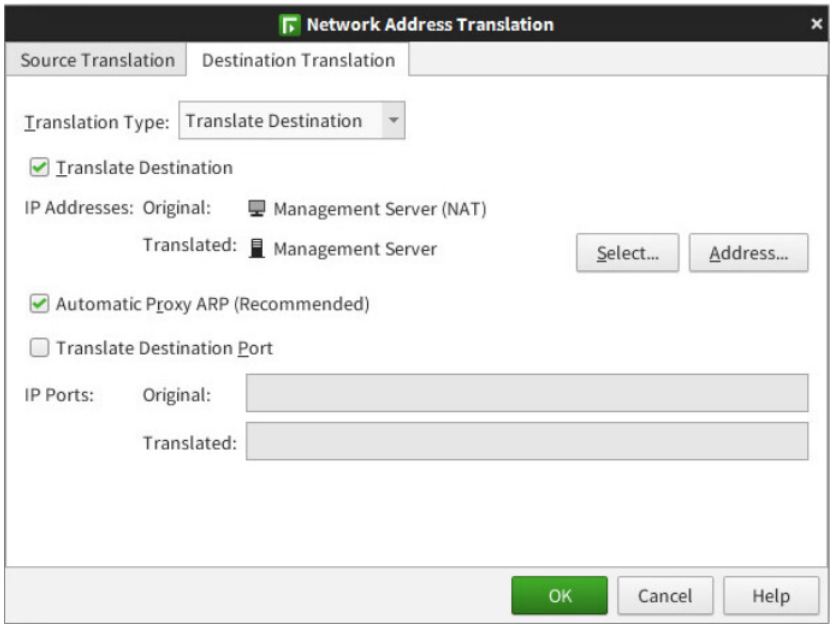


Figure 5.29: Management Server Destination NAT Properties

(g) Click **OK**. Your completed Management Server Destination NAT rule should appear as in the figure below

Figure 5.30: Completed Management Server NAT Rule

5.5.2 Create a Static Source NAT for the Management Server

You will now create a rule that NATs outgoing traffic from the Management Server to its public IP address, 172.31.1.101. This rule is required so that responses to the Firewalls are coming from the correct IP address.

1. Right-click in the **ID** column of the rule you just created and select **Add Rule Before**. A new empty rule appears
2. Configure the new rule as follows::
   - **Source**: type `mangement` and select **Management Server**
   - **Destination**: type `Global` and select **Global Firewalls**
   - **Service**: right-click and select **ANY**
   - **NAT**: in the **NAT** cell, right-click and select **Edit NAT**. The Network Address Translation dialog opens
     (a) In the **Translation Type** drop-down menu, select **Static**
     (b) Next to the **Translated** field, click **Select**. The Select Elements dialog box opens
     (c) Browse to **Network Elements** → **Hosts** and select **Management Server (NAT)**
     (d) Leave **Automatic Proxy ARP (Recommended)** checked

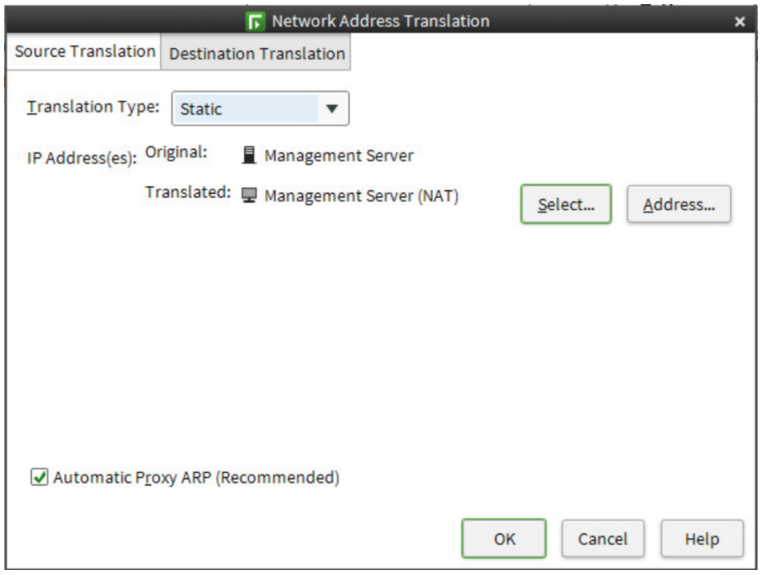


Figure 5.31: Static Source NAT Rule for Management Server

- Click **OK**. The Network Address Translation dialog closes

5.5.3 Create a Dynamic Source NAT Rule for the Internal Network

The rule you just created NATs connections destined for the Management Server's NAT address to its real, or private, IP address. The rule you will create in this exercise will NAT all connections from the internal network to the Internet. This is a Dynamic Source NAT rule.

1. Right-click in the **ID** column of the last rule and select **Add Rule After**. A new empty rule appears
2. Configure the rule as follows:
   - **Source**: from the tree view on the left, navigate to **Network Elements** → **Networks**. Drag and drop **network-172.31.200.0/24** into the **Source** cell
   - **Destination**: type `not h` and select **not Helsinki Internal Networks**
   - **Service**: leave this set to **ANY**
   - **NAT**: in the **NAT** cell, right-click and select **Edit NAT**. The Network Address Translation dialog opens
     (a) On the **Source Translation** tab, use the **Translation Type** drop-down menu and select **Dynamic**
     (b) Next to the **IP Address Pool** field, click **Address**. The Enter IP Address(es) dialog opens
     (c) In the field provided, enter **172.31.1.60**. Click **OK**. The Enter IP Address(es) dialog closes

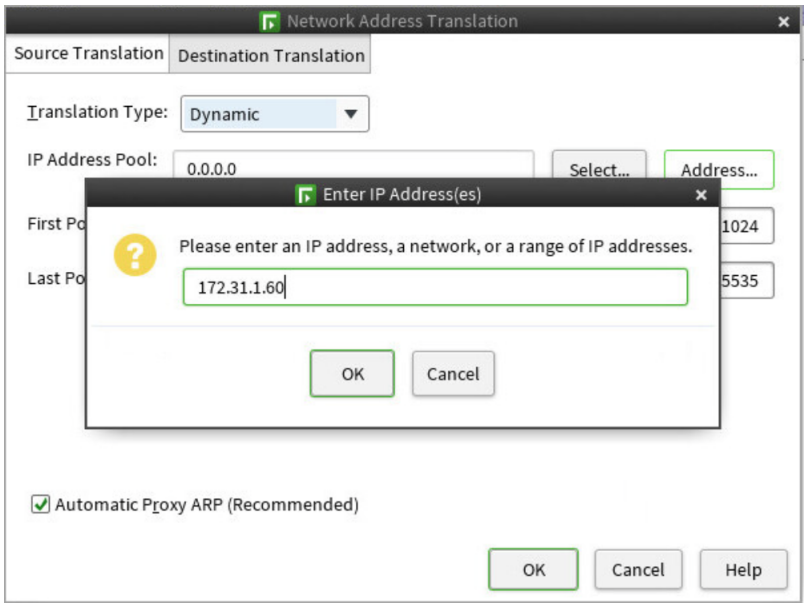


Figure 5.32: Dynamic Source NAT IP Address - HQ Policy

(d) Leave **Automatic Proxy ARP (Recommended)** checked

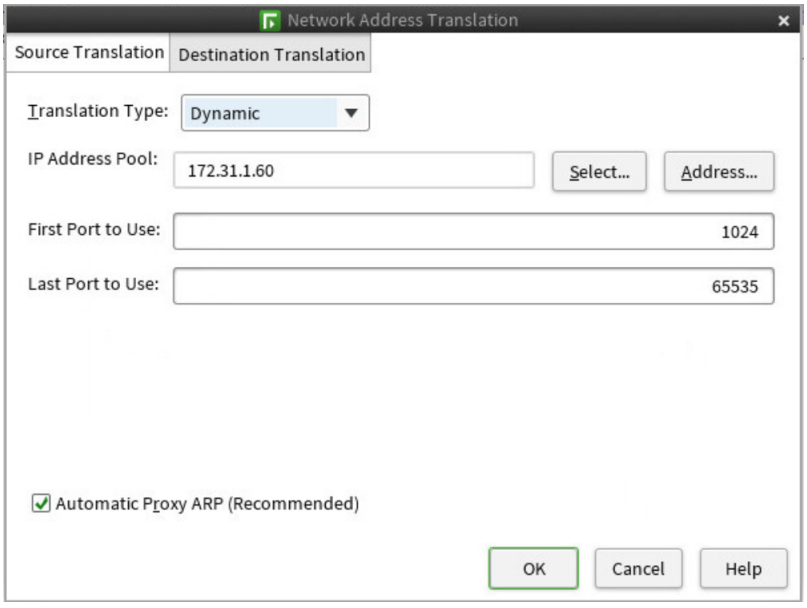


Figure 5.33: Dynamic Source NAT Properties - HQ Policy

- Click **OK**. Your completed Dynamic Source NAT rule should appear as in the figure below

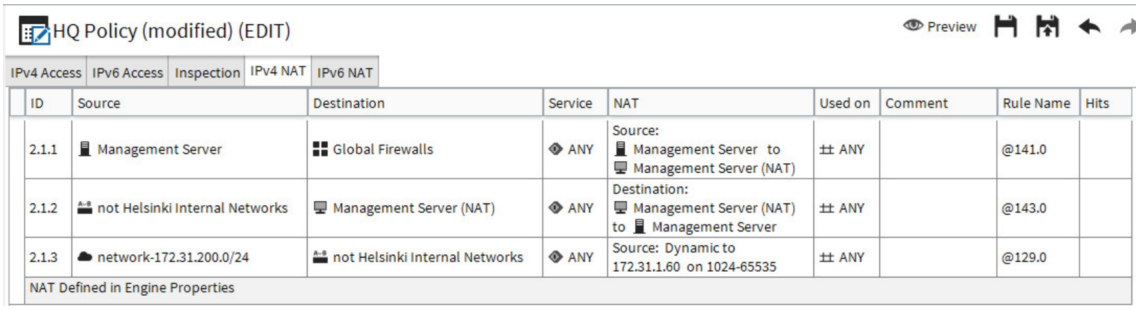


Figure 5.34: Completed Dynamic Source NAT Rule - HQ Policy

3. Click the **Save** icon. Your completed NAT rules should appear as in the figure below

5.6 Installing the HQ Policy on Helsinki-HQ FW

Now you are ready to upload the policy to the firewall. You have defined the firewall, established trust with the engine, bound the license, and defined the firewall policy. In this exercise, you will upload the policy you created above to the Engine and test it.

5.6.1 Uploading the Firewall Policy

1. With the Policy Editor still open, click the **Save and Install** button. The Upload Policy Task Properties dialog appears
2. On the left, click on **Helsinki-HQ FW** and click **Add**

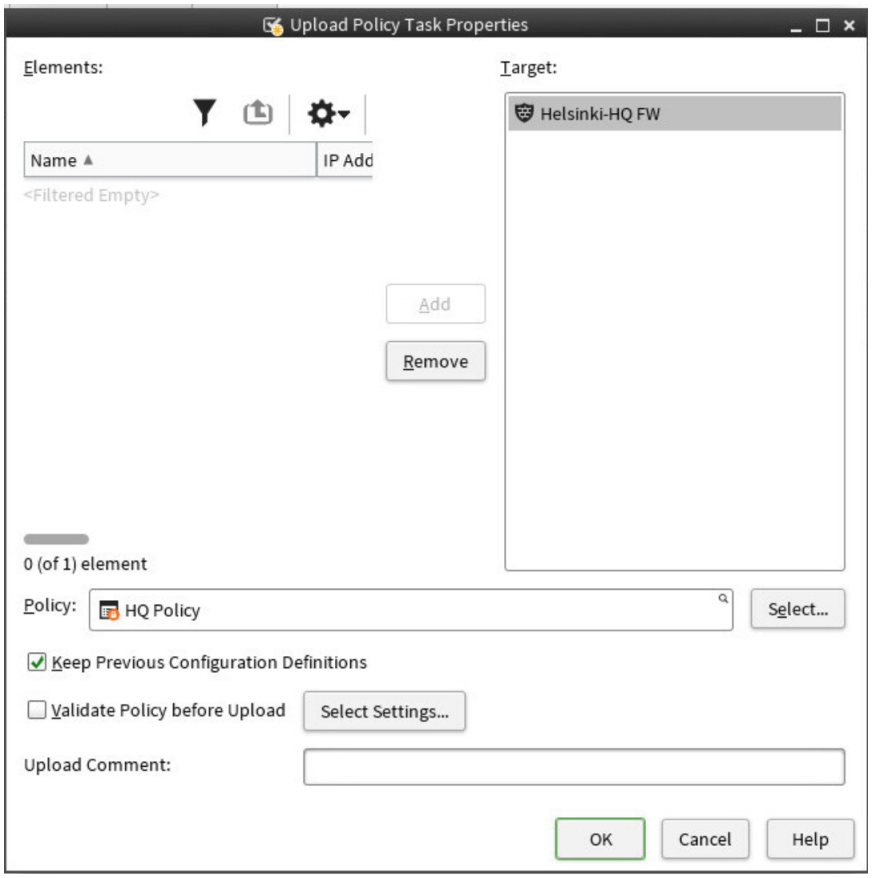


Figure 5.35: Policy Upload Task Properties

3. Click **OK**. The policy upload begins. When it is complete, you may close the tab where the upload has finished

   NOTE: You may receive some warnings at the bottom of the policy upload task. This is related to the fact that there are no firewalls in in Global Firewalls group. You will add firewalls to that Group in later labs.

5.7 Testing the Policy

You have now installed the firewall policy. You will now perform a very simple test to ensure the Management Server can reach the Internet. More complex testing will be done when the other firewalls are deployed in Lab 6.

1. On the desktop of the **HQ SMC** virtual machine, where you have been working, open a terminal by double-clicking the **Terminal** icon
2. At the command prompt, type `ping www.google.com` You should receive replies

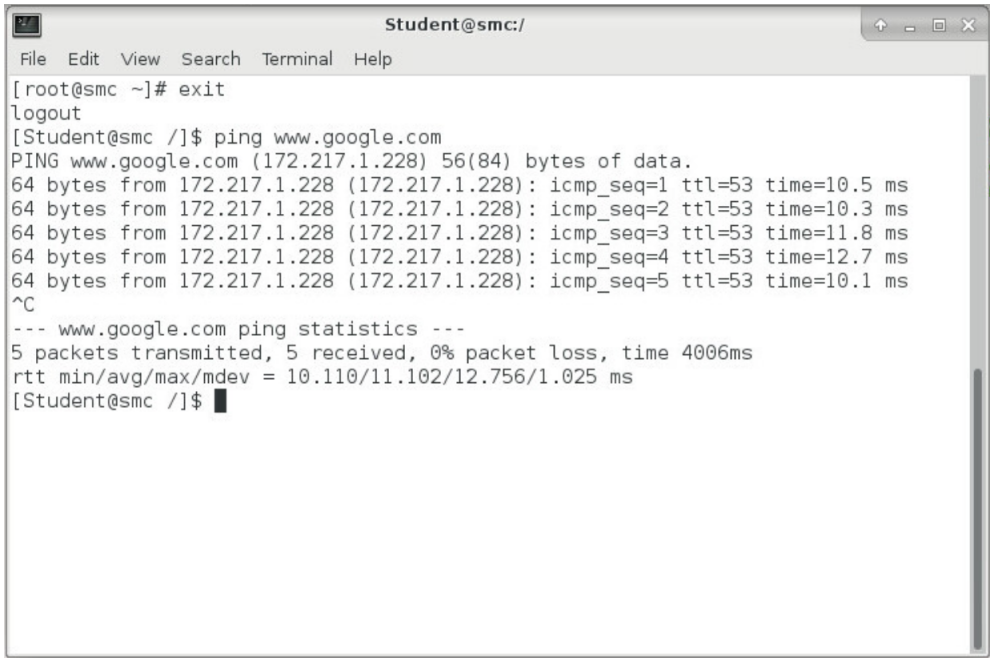


Figure 5.36: Echo Replies - Testing the HQ Policy

Summary

In this lab, you have configured Locations and Contact IP addresses so that the remote firewalls use the correct IP address when communicating with the Management and Log Servers. Because the Management Server itself has a private IP address, the Contact IP Address ensures that the remote firewalls use a public address to reach it. To further enable remote management, you also enabled Web Start so that administrators have access to the Management Server, at home or in the office.

LAB 6

NGFW Clustering

6.1 Getting Started

A firewall cluster consists of one to 16 firewall nodes. The multiple engine nodes form a firewall cluster that functions as one virtual entity. The functioning of all nodes is synchronized so that the cluster operates correctly and efficiently. The nodes exchange status information constantly to prevent connections from getting lost. If a firewall node becomes unavailable, the other nodes of the cluster are immediately informed of this, and the traffic is reallocated appropriately. The exchange of information between clustered nodes is synchronized through a heartbeat network using mainly multicast transmissions. For efficient synchronization between the nodes of a cluster, communication links dedicated to the management of node activity are recommended.

The Management Server also has a dedicated connection to each of the nodes to guarantee efficient management of the individual nodes. The management connections are authenticated and protected.

6.2 Defining a firewall cluster

1. Click the **Configuration** icon in the toolbar. The **Configuration** view opens

Figure 6.1: Toolbar Configuration Selection

2. Right-click **NGFW Engines** and select **New** → **Firewall** → **Firewall Cluster**. The engine editor opens

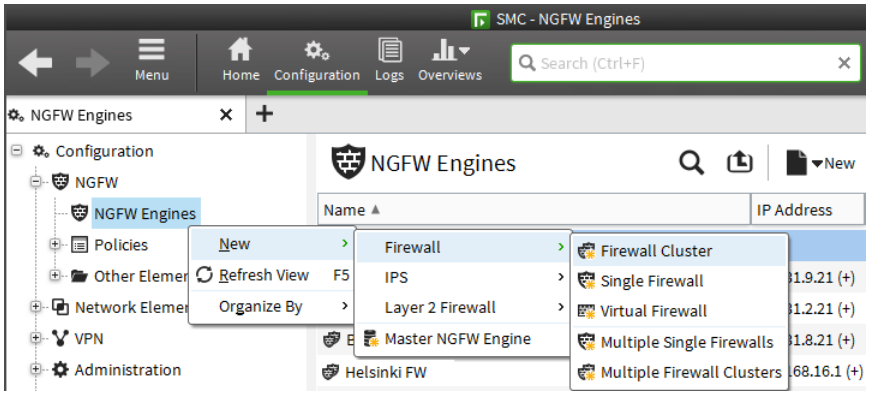


Figure 6.2: New Firewall Cluster Selection

3. Name the firewall cluster **Atlanta FW Cluster**. The **Log Server** (IP Address 172.31.200.101) is already selected
4. Click the **Add** button next to the **DNS IP Addresses** field and select **IP Address**. The Add IP Address dialog opens
5. In the field provided, enter **8.8.8.8**
6. In the **Location** field, use the drop-down menu and select **Remote**

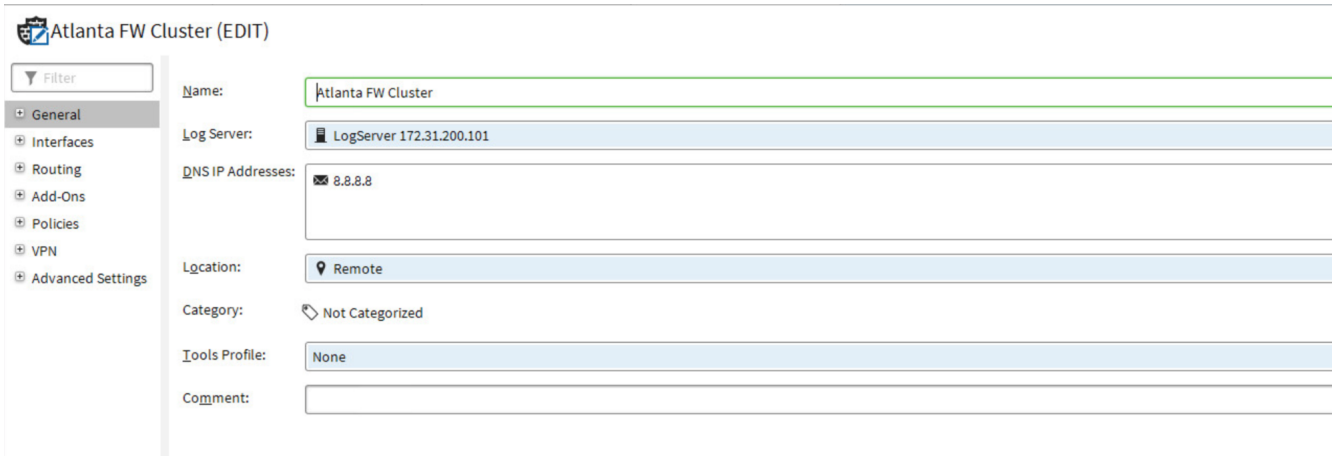


Figure 6.3: New Cluster General Properties

7. Expand **General** select **Clustering** and check that the clustering mode is set to **Balancing**

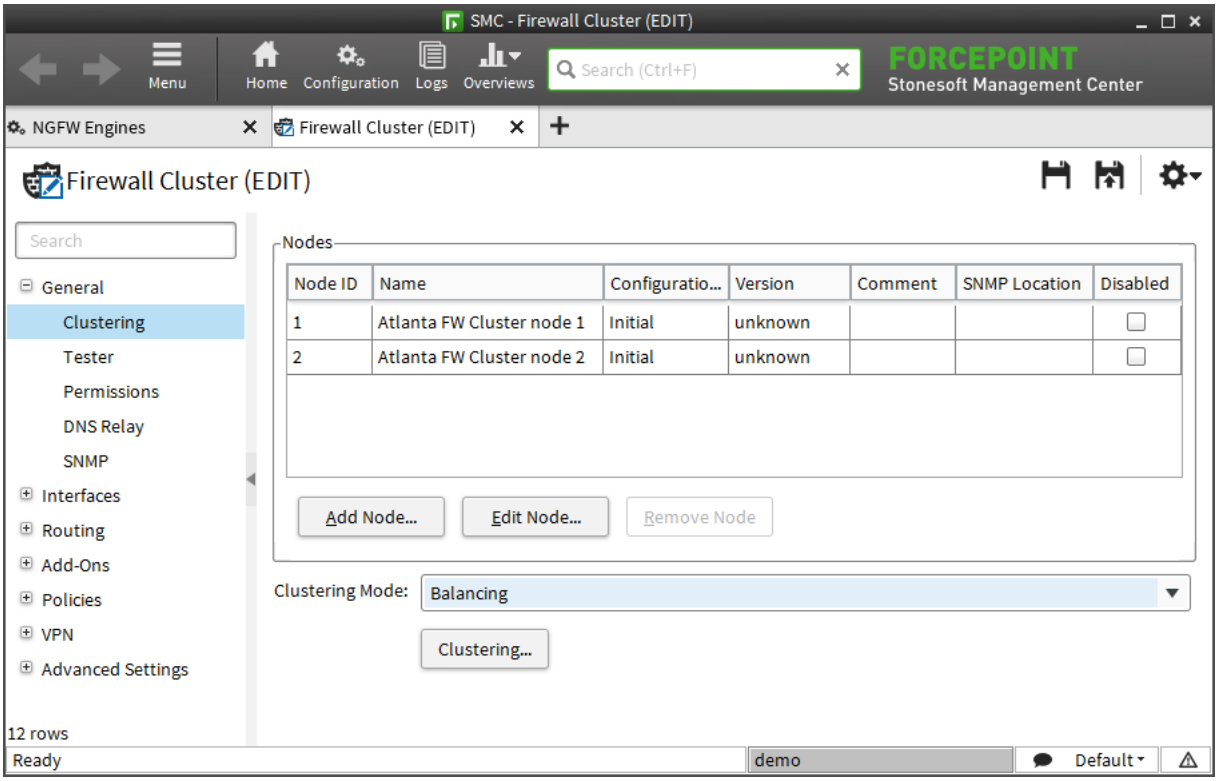


Figure 6.4: Verification of Clustering Mode

6.3 Defining Physical Interfaces

The first step in configuring firewall cluster interfaces is to define the physical interfaces. You will define four physical interfaces for your cluster:

- **Interface ID 0**: for the internal network
- **Interface ID 1**: for the connections to ISP A and the primary control connection to the Management Server
- **Interface ID 2**: for the connection to ISP B and the backup control connection to the Management Server
- **Interface ID 3**: for the heartbeat communication between the nodes

6.3.1 Define Interface ID 0

1. From the Engine Editor, select **Interfaces**
2. Right-click **New** → **Layer 3 Physical Interface**. The Layer 3 Physical Interface Properties dialog box opens

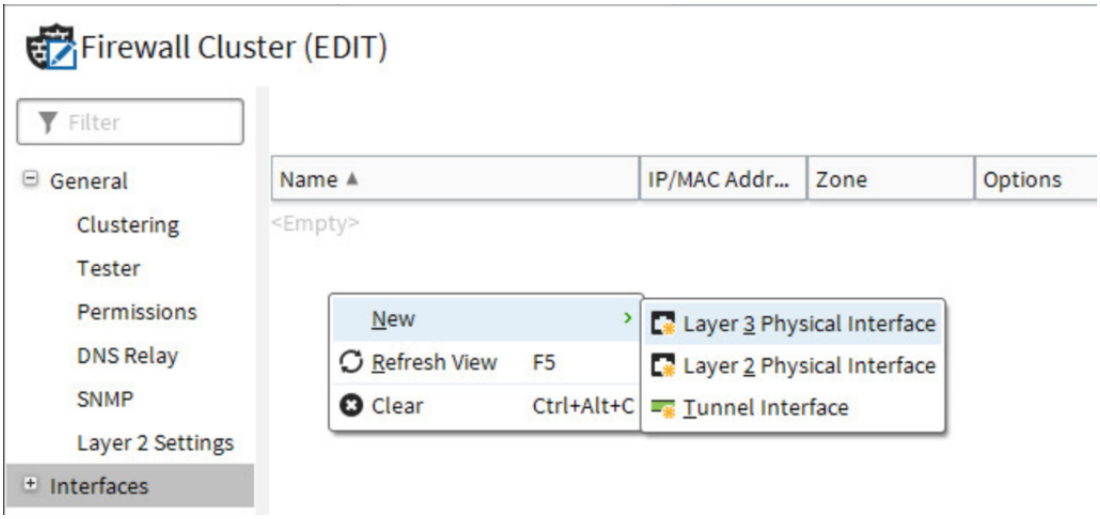


Figure 6.5: Defining a New Physical Interface

3. Select **Interface ID 0** and define the following settings:
   - CVI Mode: **Packet Dispatch**
   - MAC Address: **00:00:5e:00:aa:02**
   - LLDP Mode: **Reveiver Only**
   - Comment: **Atlanta Internal Network**

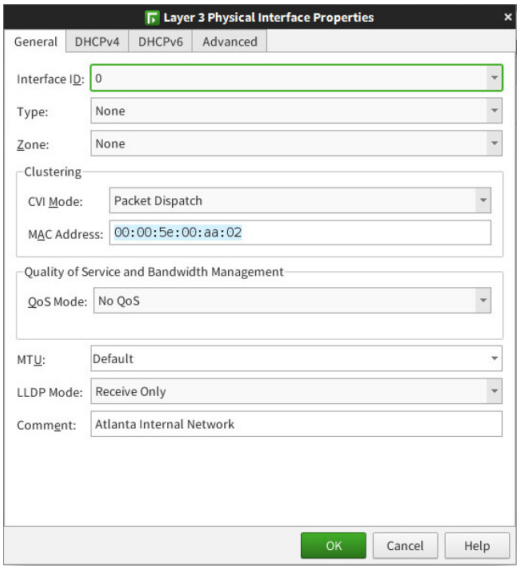


Figure 6.6: Physical Interface 0 Properties

4. Click **OK**

6.3.2 Define Interface ID 1

1. Right-click **Interfaces** and select **New** → **Layer 3 Physical Interface**. The Layer 3 Physical Interface Properties dialog box opens
2. Select **Interface ID 1** and define the following settings
   - CVI Mode: **Packet Dispatch**

- MAC Address: **00:00:5e:00:bb:02**
- LLDP Mode: **Reveiver Only**
- Comment: **External ISP A and Primary Control**

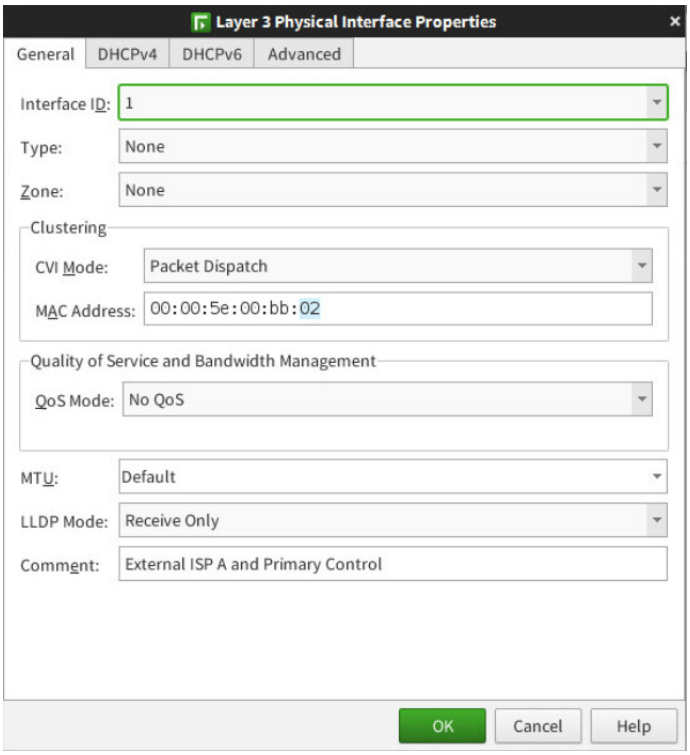


Figure 6.7: Physical Interface 1 Properties

3. Click **OK**

6.3.3 Define Interface ID 2

1. Right-click **Interfaces** and select **New** → **Layer 3 Physical Interface**. The Layer 3 Physical Interface Properties dialog box opens
2. Select **Interface ID 2** and define the following settings:
   - CVI Modes: **Packet Dispatch**
   - MAC Address: **00:00:5e:00:cc:02**
   - LLDP Mode: **Reveiver Only**
   - Comment: **External ISP B and Control Backup**

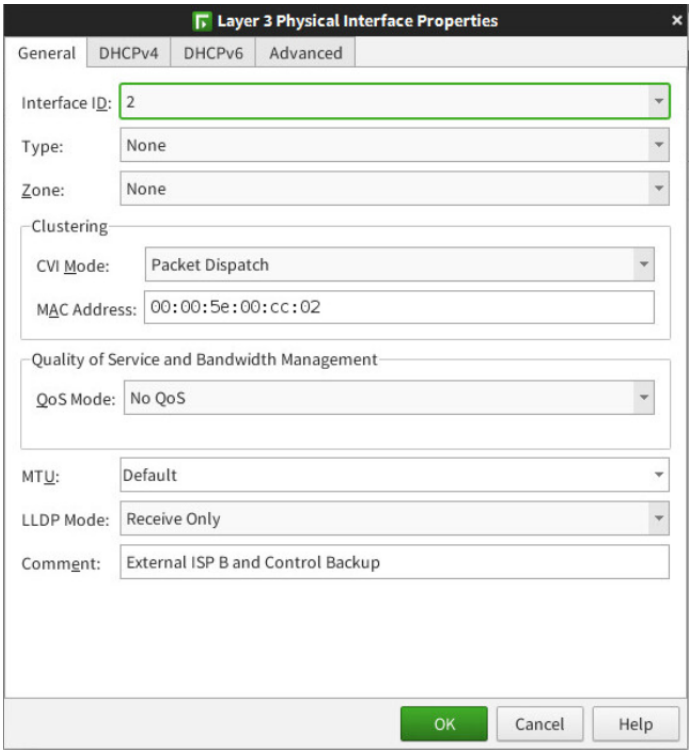


Figure 6.8: Physical Interface 2 Properties

- Click **OK**

Both heartbeat and state synchronization (which take place on the same interface) are time critical communications. Network latency from other traffic may interfere with these crucial communications. Using a dedicated network for the heartbeat communications is recommended.

6.3.4 Define Interface ID 3

1. Right-click **Interfaces** and select **New** → **Layer 3 Physical Interface**. The Layer 3 Physical Interface Properties dialog box opens
2. Select **Interface ID 3** and define the following settings:
   - CVI Mode: **None**
   - LLDP Mode: **Receiver Only**
   - Comment: **Heartbeat**

Figure 6.9: Physical Interface 3 Properties

3. Click **OK**

After you have defined the physical interfaces for the cluster, you are ready to configure Cluster Virtual IP Addresses (CVIs) and Node Dedicated IP Addresses (NDIs) on the physical interfaces.

6.4 Define CVIs and NDIs for Interface 0

1. Right-click **Interface 0** and select **New** → **IPv4 Address**. The **Interface Properties for Interface 0** dialog box opens
2. Define the following setting under **Cluster Virtual IP Address**:
   - IPv4 Address: **192.168.2.1**
3. Define the following settings under **Node Dedicated IP Address**:
   - Node 1 IPv4 Address: **192.168.2.21**
   - Node 2 IPv4 Address: **192.168.2.22**

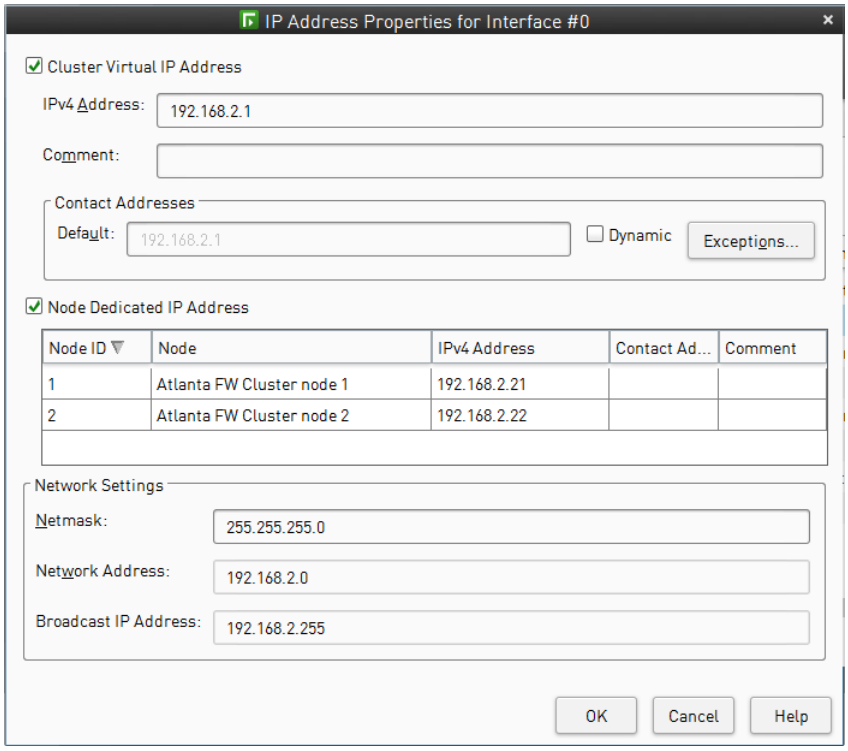


Figure 6.10: IPv4 Addresses for Interface 0

4. Click **OK**

6.5 Define CVIs and NDIs for Interface 1

1. Right-click **Interface 1** and select **New** → **IPv4 Address**. The **Interface Properties for Interface 1** dialog box opens
2. Define the following setting under **Cluster Virtual IP Address**:
   - IPv4 Address: **172.31.2.254**
3. Define the following settings under **Node Dedicated IP Address**:
   - Node 1 IPv4 Address: **172.31.2.21**
   - Node 2 IPv4 Address: **172.31.2.22**

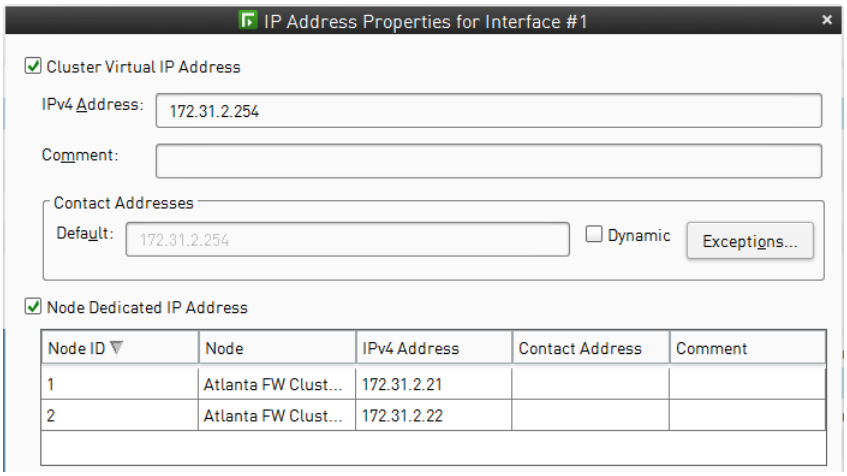


Figure 6.11: IPv4 Addresses for Interface 1

4. Click **OK**

6.6 Define CVIs and NDIs for Interface 2

1. Right-click **Interface 2** and select **New** → **IPv4 Address**. The **Interface Properties for Interface 2** dialog box opens
2. Define the following setting under **Cluster Virtual IP Address**:
   - IPv4 Address: **10.1.2.254**
3. Define the following settings under **Node Dedicated IP Address**:
   - Node 1 IPv4 Address: **10.1.2.21**
   - Node 2 IPv4 Address: **10.1.2.22**

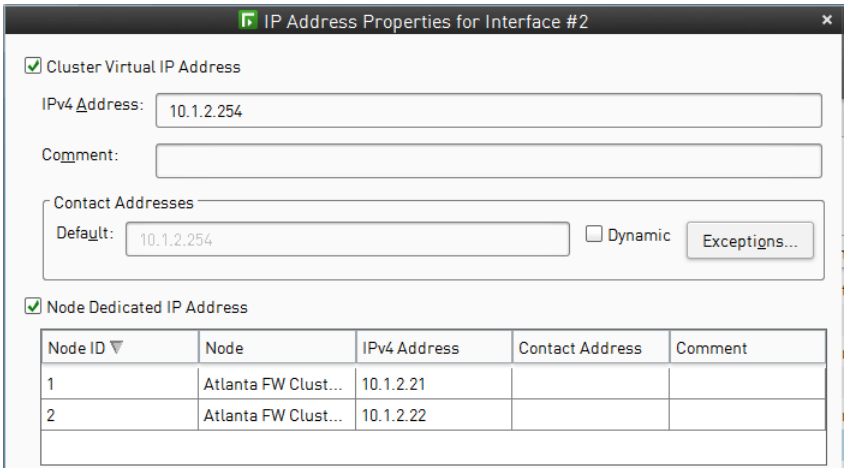


Figure 6.12: IPv4 Addresses for Interface 2

4. Click **OK**

6.7 Define NDIs for Interface 3

This interface is used for the heartbeat connection between nodes, so it only needs Node Dedicated IP Addresses.

1. Right-click **Interface 3** and select **New** → **IPv4 Address**. The **Interface Properties for Interface 3** dialog box opens.
2. Deselect **Cluster Virtual IP Address** and define the following settings under **Node Dedicated IP Address**:
   - Node 1 IPv4 Address: **10.42.2.21**
   - Node 2 IPv4 Address: **10.42.2.22**
3. Click **OK**

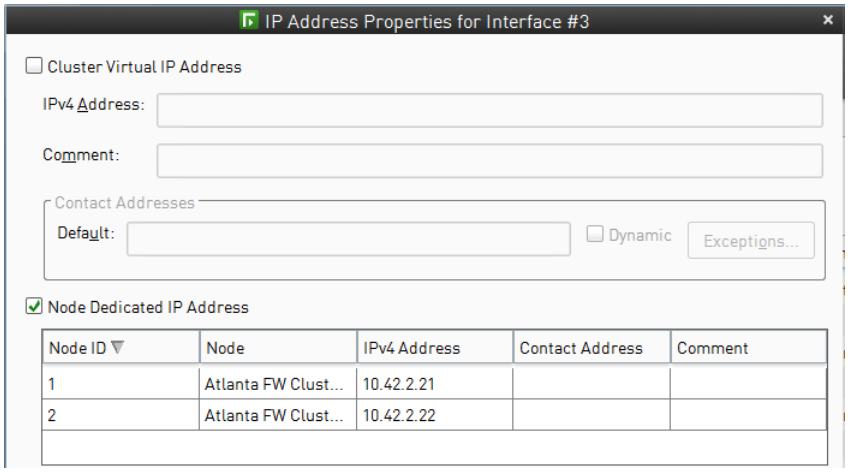


Figure 6.13: IPv4 Addresses for Interface 3

6.8 Define Interface Options

Now that you have defined the physical interfaces and assigned IP addresses to them, you must define the correct options for each interface.

1. From the **Engine Editor**, in the **Interface Menu**, expand the **Interfaces** tree and select **Interface Options**. The Interface Options dialog box opens
2. Configure the following settings for interface options:
   - Primary Control Interface: **Interface 1**
   - Backup Control Interface: **Interface 2**
   - Primary Heartbeat Interface: **Interface 3**
   - Backup Heartbeat Interface: **Interface 0**
   - IPv4 Identity for Authentication Requests: **Interface 0**
   - IPv4 Source for Authentication Requests: **Interface 0**
   - IPv6 Identity for Authentication Requests: **Interface 0**
   - IPv6 Source for Authentication Requests: **Not Set**
   - Default IP Address for Outgoing Traffic: **According to Routing**
3. Click **Save**. The completed Firewall Cluster Interface configuration should appear as in the figure below

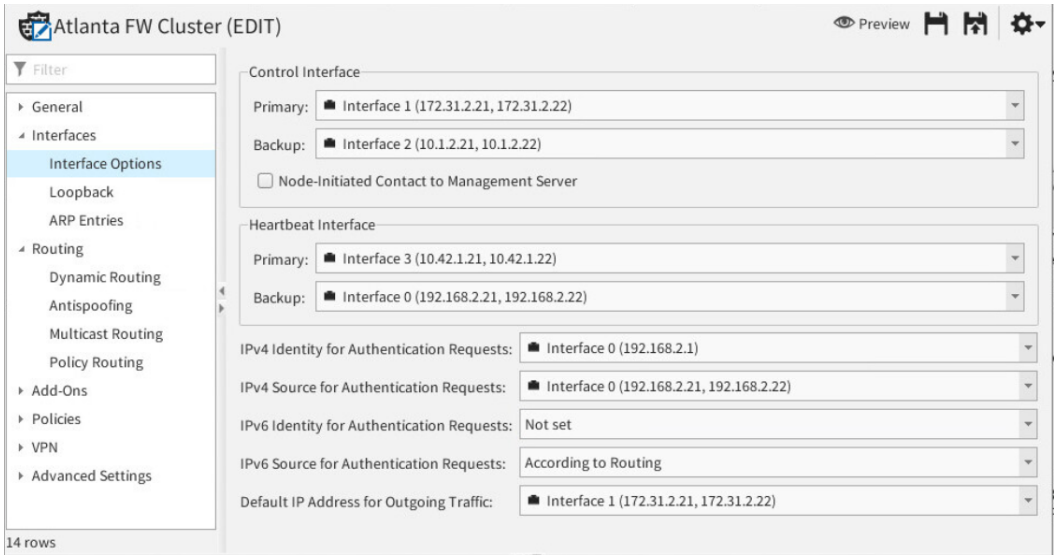


Figure 6.14: Completed Interface Options Selection

4. You might see the errors below, which can be safely ignored. The license and the routing configuration will be addressed in a later lab

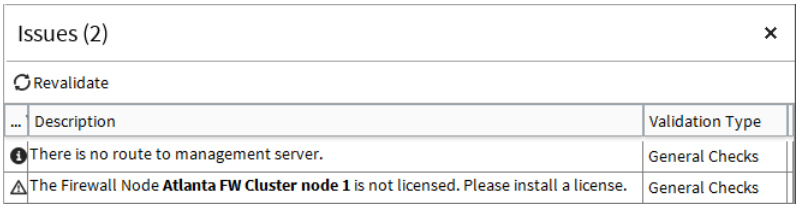


Figure 6.15: New Cluster Validation Errors

5. You may close the tab where the Engine is open for editing

6.9 Finish the Configuration

The firewall cluster you just defined now appears under **NGFW Engines** in the **Configuration** view.

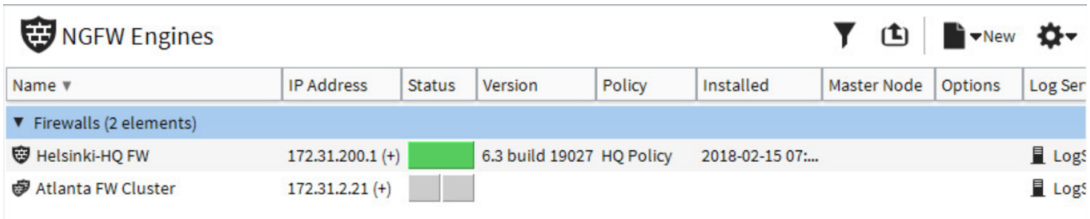


Figure 6.16: Configuration View Firewalls

6.10 Save the Initial Configuration

Now that you have defined the properties of your firewall cluster, you are ready to save the configuration information so that you can begin installing the firewall engines. In this task, you create the required configuration files that the engine needs during the next phase of the installation. When you save the initial configuration, the Management Server also creates a one-time password that the engine uses to obtain the configuration for each node in the cluster.

1. In the **Configuration** view, right-click **Atlanta FW Cluster** → **Configuration** → **Save Initial Configuration**. The **Initial Configuration** dialog box opens

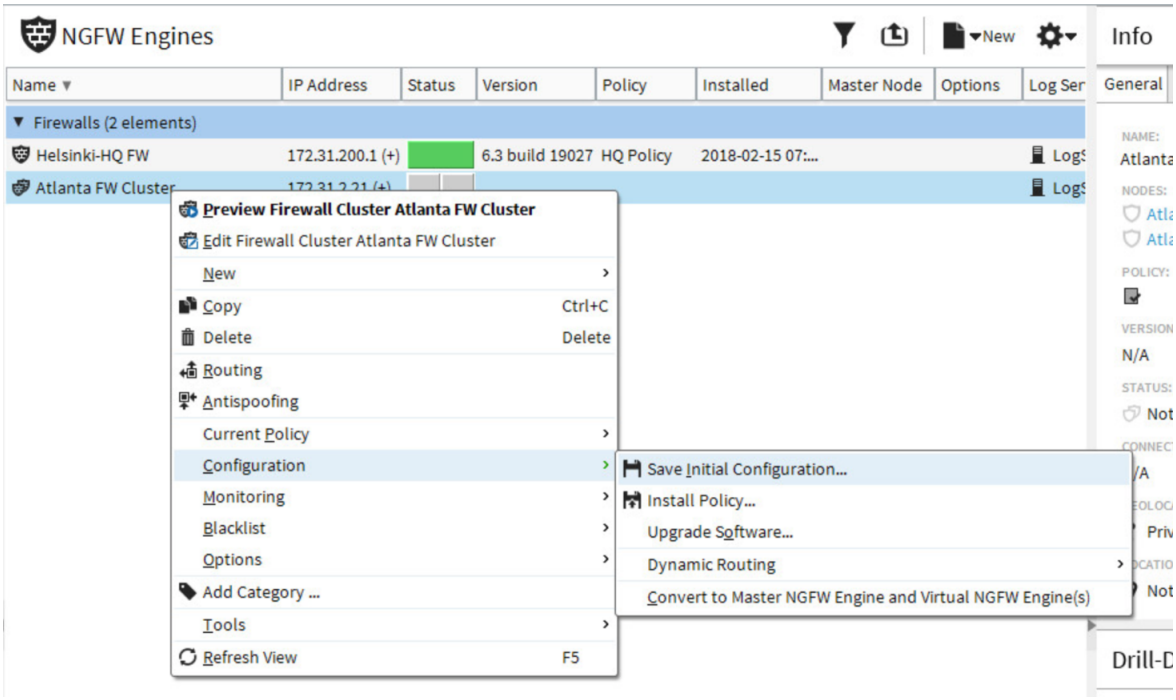


Figure 6.17: Saving the Initial Firewall Configuration

2. Click **View Details**

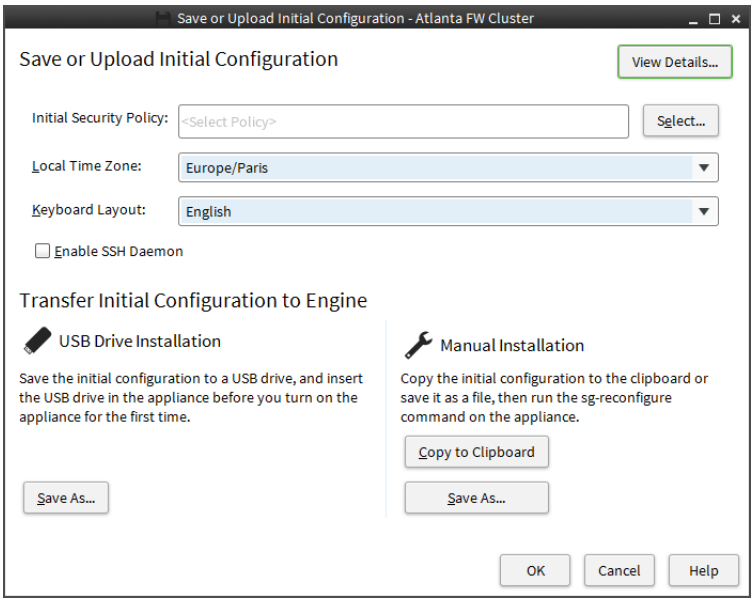


Figure 6.18: Initial Configuration Details

3. Write down the one-time passwords that were generated for each node

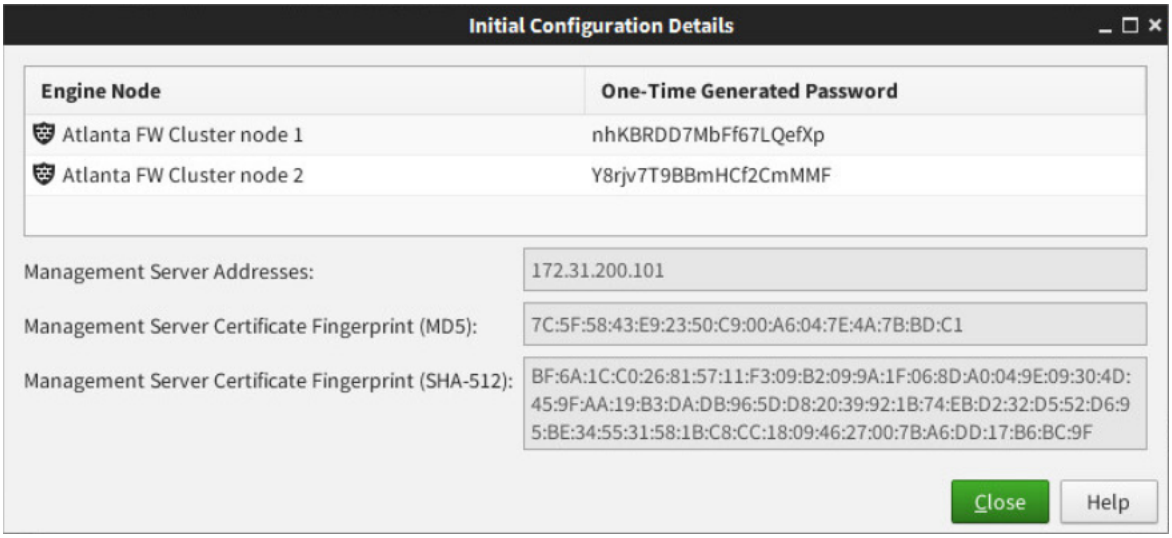


Figure 6.19: Node One Time Passwords

NOTE: Do not close the dialog box. It shows the fingerprint of the Management Server's certificate and the one-time password. If you accidentally close the dialog box, repeat the procedure to create a new initial configuration with a new one-time password.

TIP: You can use the Initial Configuration dialog box as a reference as you type the one-time password or copy and paste the one-time password into the engine console. If copying and pasting does not work, you can use your phone camera.

6.11 Add Atlanta FW Cluster to Global Firewalls Group

In **Lab2**, you created a Global Firewall group object that will contain all of you remote firewalls. Before you can contact the Management Server to establish trust, you must add the Atlanta FW Cluster to that group and upload the policy. This will allow connections from the Atlanta FW Cluster through to the Management and Log Servers.

1. Right-click the **Home** icon in the toolbar, and select **Open in New Tab**. The Home view opens
2. Right-click on **Helsinki-HQ FW** and browse to **Current Policy** → **Edit**. The policy editor opens

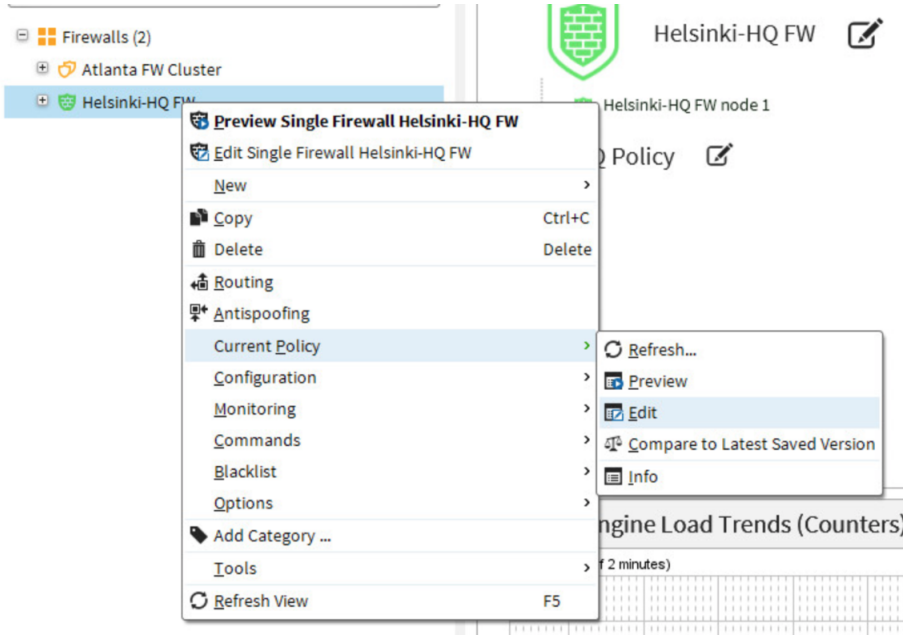


Figure 6.20: Editing HQ Policy - Global Firewalls Group

3. Right-click on **Global Firewalls** in the policy and select **Properties**. The Global Firewalls group object properties opens
4. Under the **Resources** section, click on **NGFW Engines** and click on **Atlanta FW Cluster**
5. Click **Add**
6. Click **OK**. Your completed **Global Firewalls** group should appear as in the figure below

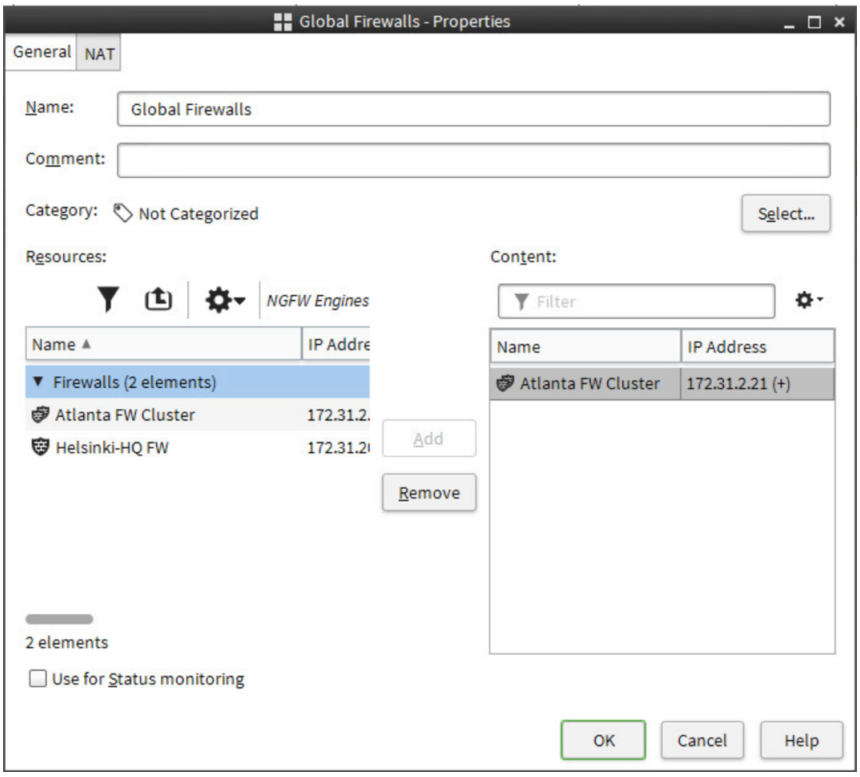


Figure 6.21: Adding Atlanta FW Cluster to Global Firewalls

7. Click the **Save and Install...** button. The HQ Policy uploads. When the upload is complete, you may close the **Upload Policy: HQ Policy** tab
8. Close the tab where the **HQ Policy** is open for editing

6.12 Configure the Engine on an NGFW Appliance

NGFW appliances have the engine software pre-installed. However, there are settings that you must configure on the engine's command line.

1. Using the **Main Menu** on the **Landing Machine**, open a console to **Atlanta FW A**

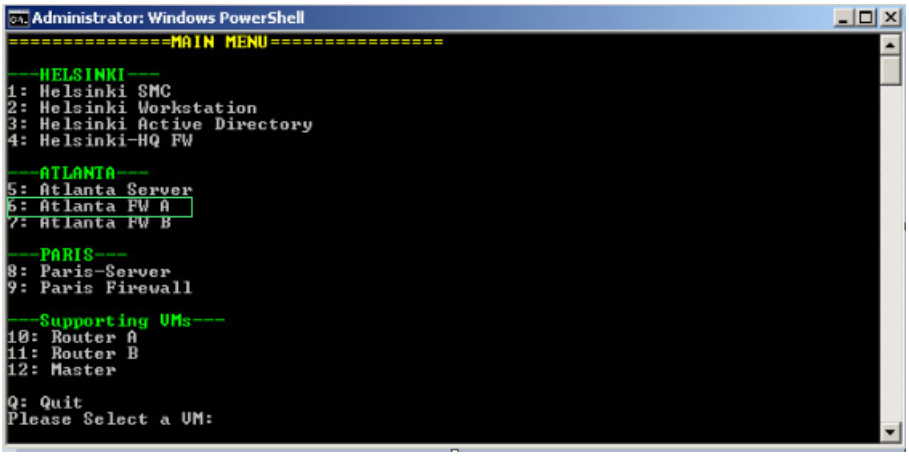


Figure 6.22: Console to Atlanta FW A

2. Press **Enter** to active the console. Enter **Y**and then **Enter** to start the Configuration Wizard

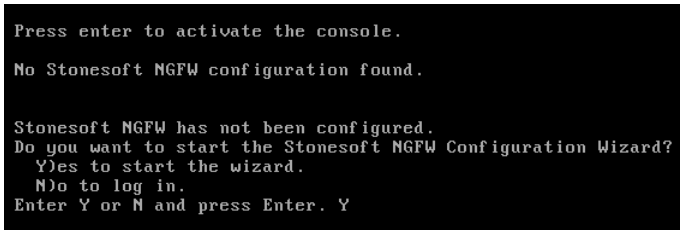


Figure 6.23: Activating the Engine Console

3. Highlight **Role** and press **Enter** to select the role for the NGFW Engine
4. Highlight **Firewall/VPN** and press **Enter**. The role-specific Configuration Wizard starts

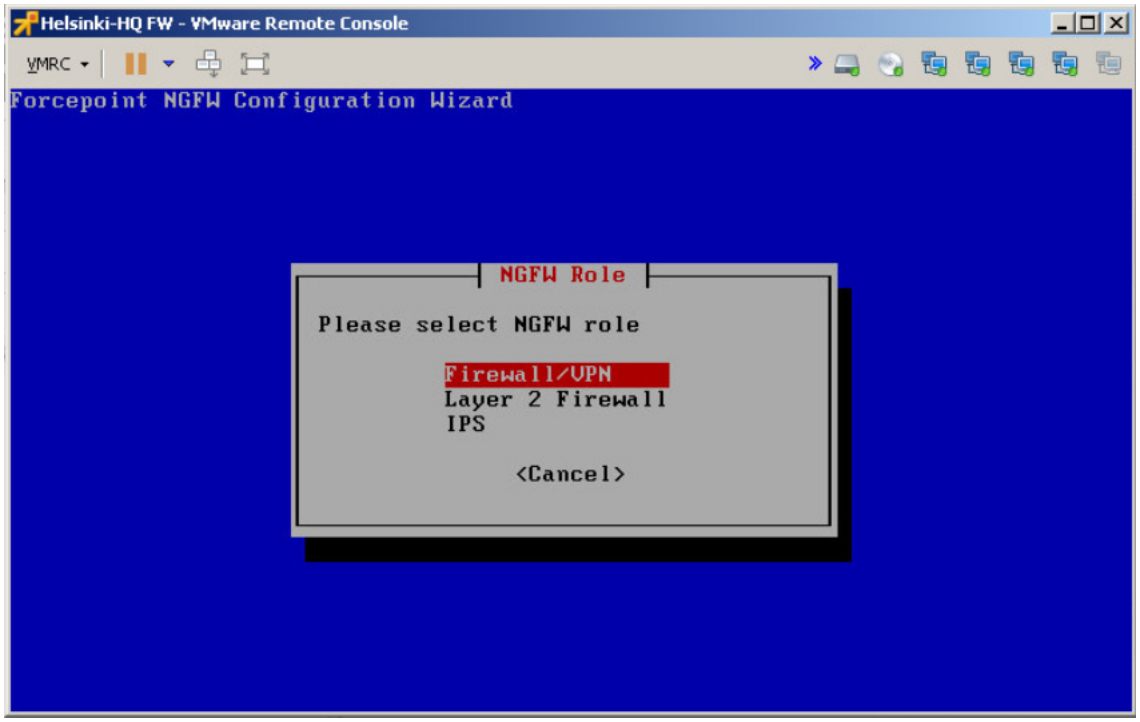


Figure 6.24: Selecting the FW/VPN Role

5. Select Next and press Enter to continue. The OS Settings screen opens

Figure 6.25: Configuring OS Settings

6. Highlight the entry field for **Keyboard Layout** using the arrow keys and press **Enter**. The Select Keyboard Layout screen opens
7. Highlight US English and press Enter
8. Highlight the entry field for **Local Timezone** and press **Enter**. The Select Timezone screen opens
9. Select **Local Timezone**, scroll to **US/Eastern** and press **Enter**. The **Select Timezone** screen closes
10. Enter the correct **Host Name** (for example, Atlanta-FW-1 or Atlanta-FW-2)
11. Enter and confirm **Pass1234** as the root password. This is the only account for command line access to the engine
12. Select **Enable SSH Daemon** by pressing the space bar
13. Highlight **Next** and press **Enter**. The Configure Interfaces screen opens

6.13 Configure Network Interfaces

1. Select **Autodetect** and press **Enter**. The interfaces are shown with the IDs associated with each network interface
2. Make sure that the **Mgmt** column is selected for **eth1**

   If necessary, highlight the **Mgmt** column for eth1 and press the space bar. An asterisk (*) fills the brackets

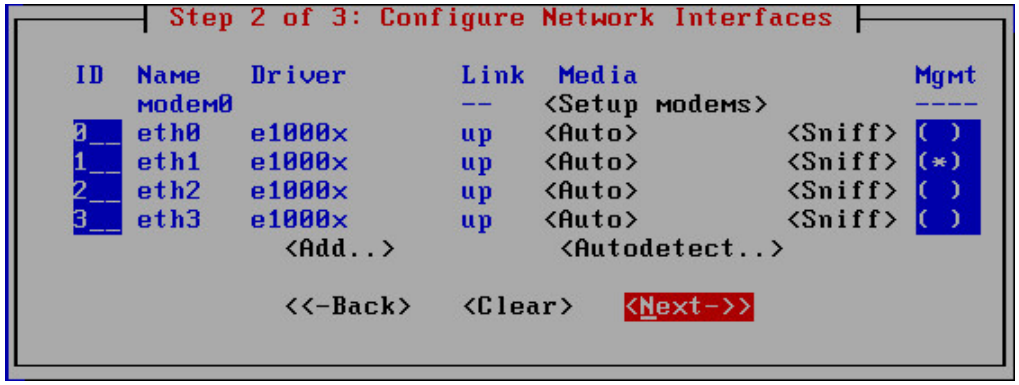


Figure 6.26: Network Interface Configuration

TIP: The Sniff option is available in case you have trouble connecting to the Management Server after the configuration is complete. It allows you to troubleshoot and detect whether you have assigned your Interface IDs correctly.

3. Select **Next** and press **Enter**. The Prepare for Management Contact dialog box opens

6.14 Contact the Management Server

1. Select **Switch Firewall node to initial configuration**
2. Select **Enter Node IP Address Manually** and enter the following IP Address settings:
   - IP Address: **172.31.2.21** (or **172.31.2.22 for Node 2**)
   - Netmask: **255.255.255.0**
   - Gateway to Management: **172.31.2.1**
3. Highlight **Contact** and press the space bar. An asterisk (*) fills the brackets
4. Enter the **IP Address** of the Management Server **172.31.1.101**

   NOTE: You are using the external IP address of the Management Server, as opposed to its real IP address because this firewall is remote.

5. Enter the **One-time Password** you generated in the Management Client
6. Highlight **256-bit security** and press the space bar to clear the selection
7. Highlight **Finish** and press**Enter**

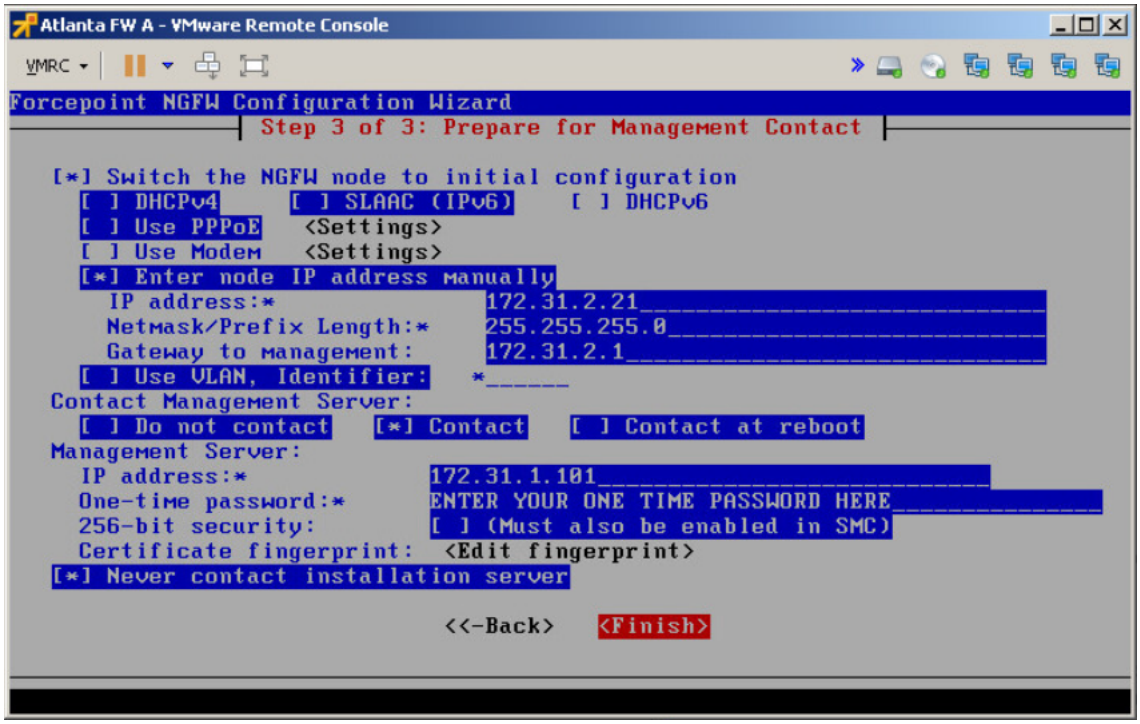


Figure 6.27: Management Server Contact Details

8. Accept the Management Server certificate fingerprint

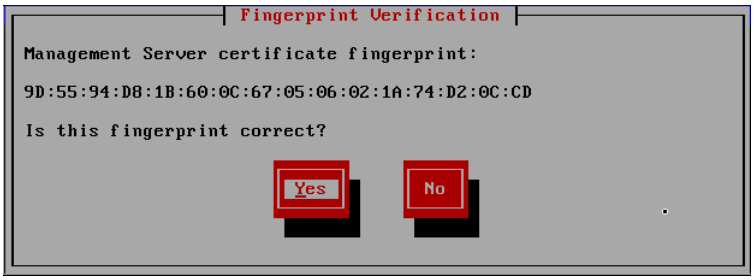


Figure 6.28: Management Server key Fingerprint

The node connects to the Management Server. A message indicating that the initial contact has succeeded appears.

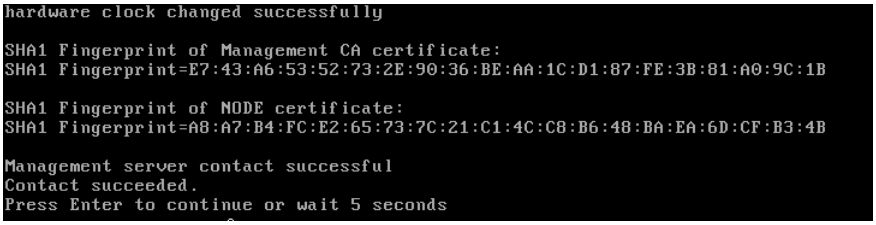


Figure 6.29: Successful Management Contact Confirmation

When the engine has successfully contacted the Management Server, it appears in the No Policy Installed state in the Home view in the Management Client. The Connectivity tab also shows the status of the node as gray.

NOTE: If the contact fails, log on to the firewall console, type **sg-reconfigure** and check the settings.

6.15 Make Initial Contact with the Atlanta-FW2 Appliance

1. Open a virtual console to **Atlanta-FW2**
2. Repeat these steps for Atlanta-FW2 Virtual Appliance using the following values:
   - IP Address: **172.31.2.22**
   - Netmask: **255.255.255.0**

6.16 Bind Licenses

1. In the Management Client, click the tab where the **Configuration** view is open
2. Browse to **Administration** → **Licenses** → **NGFW Engines**. A list of NGFW Node licenses is displayed

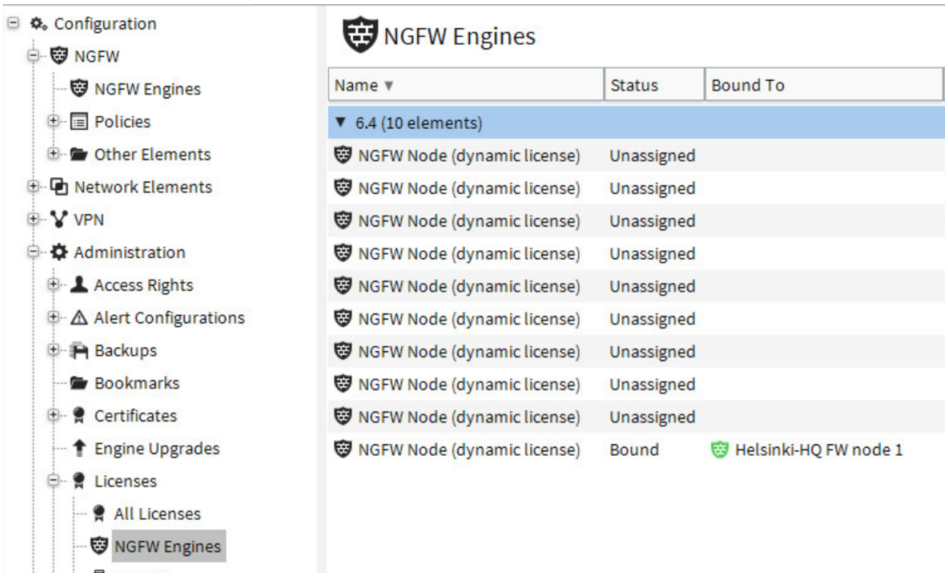


Figure 6.30: License Administration View

3. Right-click a **NGFW Node** license and select **Bind**. The **Select License Binding** dialog box opens
4. Select the node to which you want to bind the license and click **Select**. The license is bound to the selected node. You will see a dialog box which says “Install the policy on Atlanta FW Cluster to activate the new license“. This will be done in the next section
5. Repeat these steps to bind a license to Atlanta FW Cluster node 2

6.17 Create a Default Route For Atlanta FW Cluster

As you did in **Lab 3**, you will now create a router for Atlanta FW Cluster and adding to the routing view. This will provide a default route that the firewall can use when sending traffic outbound.

6.17.1 Define a Router

1. From the **Home** view, right-click the **Configuration** icon in the toolbar and select **Open in New Tab**. The **Configuration** view opens
2. On the left side, browse to **Network Elements** → **Routers**

3. Right-click on **Routers** and select **New Router**. The Router Properties dialog opens
4. Configure the Router with the following properties:
   - Name: **Atlanta ISP A Router**
   - IPv4 Address: **172.31.2.1**

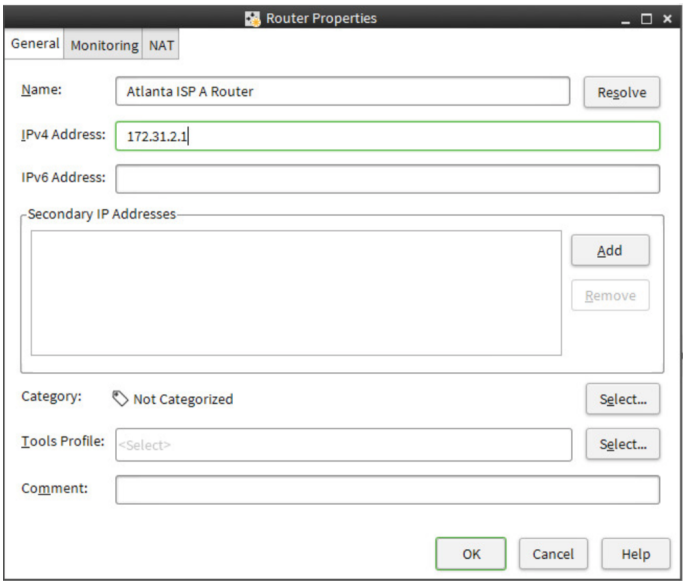


Figure 6.31: Atlanta ISP A Router Properties

5. Click **OK**. The Router Properties closes

6.17.2 Create a Default Route

Now you will create a default route to direct any traffic not destined to your own networks to the route of last resort - the Internet.

1. From the tab where the **Home** view is open, right-click **Atlanta FW Cluster** and select **Edit Firewall Cluster Atlanta FW Cluster**
2. On the left side, click on **Routing**
3. Under **Interface 1** in the pane on the right, right-click on **network-172.31.2.0/24: 172.31.2.0/24** and select **Add Router**

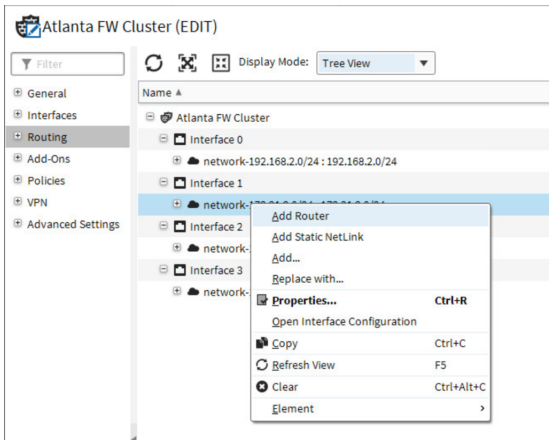


Figure 6.32: Adding Default Route for Atlanta FW Cluster

4. In the **Select Elements** dialog that opens, click on the **Atlanta ISP A Router**, and click **Add**. Click **OK**. The Select Elements dialog closes
5. Expand **Interface 1** and browse to **Atlanta ISP A Router**
6. Right-click on **Atlanta ISP A Router** and select **Set as Default Route**

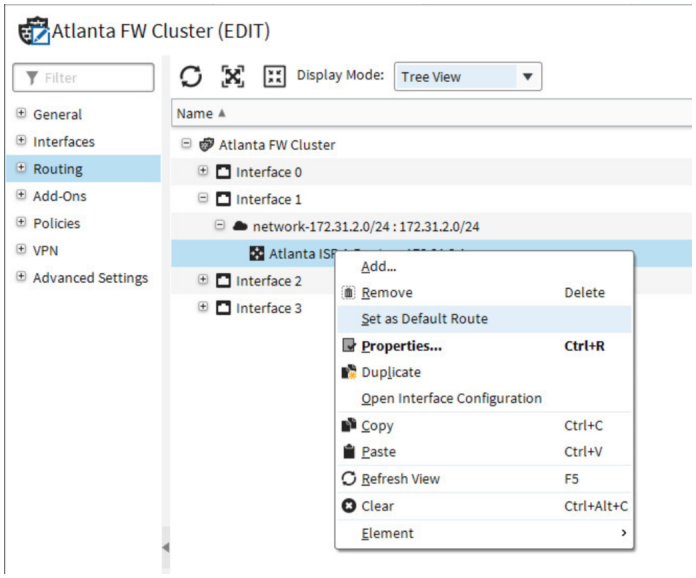


Figure 6.33: Setting the Atlanta FW Cluster Default Route

7. Click the **Expand all** icon (just above the **Name** column). The routing definition should look as in the figure below

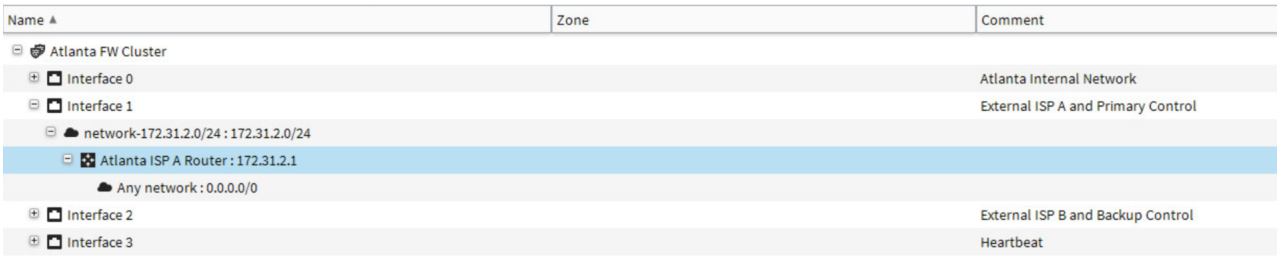


Figure 6.34: Completed Atlanta FW Cluster Routing View

8. In the upper right-hand corner of the Engine editor, click the **Save** button to store the changes you have just made. You may now close the tab where the **Atlanta FW Cluster** is open for editing

6.18 Define a Policy for Atlanta FW Cluster

Now that the Atlanta FW Cluster has been defined, you will now create a firewall policy based on the template you created in Lab 2.

6.18.1 Create the Atlanta Policy

1. In the tab where the **Configuration** view is open, in the tree view, browse to **NGFW** → **Policies** → **Firewall Policies**
2. Right-click on **Global Firewall Template** and select **New** → **Firewall Policy**. The Firewall Policy Properties opens

3. In the **Name** field, enter **Atlanta Policy**

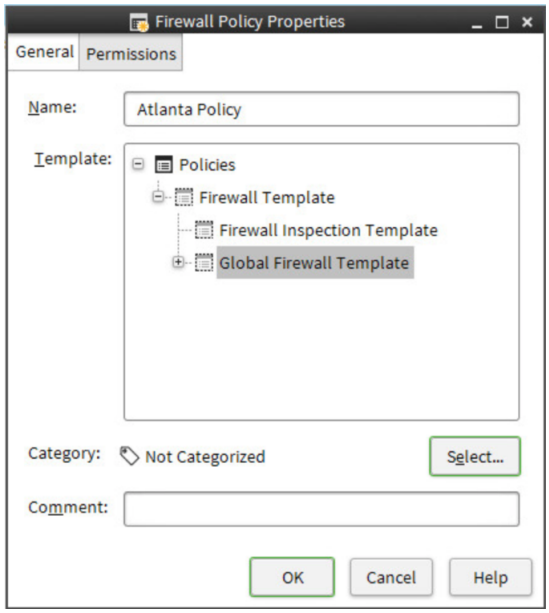


Figure 6.35: Atlanta Policy Properties

4. Click **OK**. The Firewall Policy Properties dialog closes. The Atlanta Policy opens for editing

6.18.2 Create an Expression

1. Browse to **Network Elements** in the Resources list on the left.
2. Navigate to **Network Elements** → **Expressions**

   TIP: Use the icon in the figure below to navigate the tree view

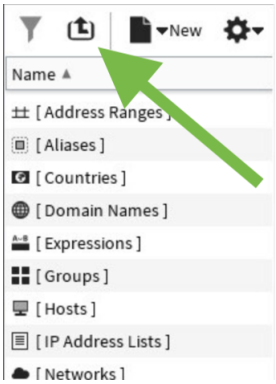


Figure 6.36: Navigating the Object Tree View

3. Click the **New** icon and select **Expression**. The Expression Properties dialog opens
4. In the **Name** field, enter **not Atlanta Internal Networks**
5. Click the **Negation** (˜)
6. Click the **Add Element** icon. The Select Element dialog opens
7. Browse to **Network Elements** → **Networks** and select **network-192.168.2.0/24**

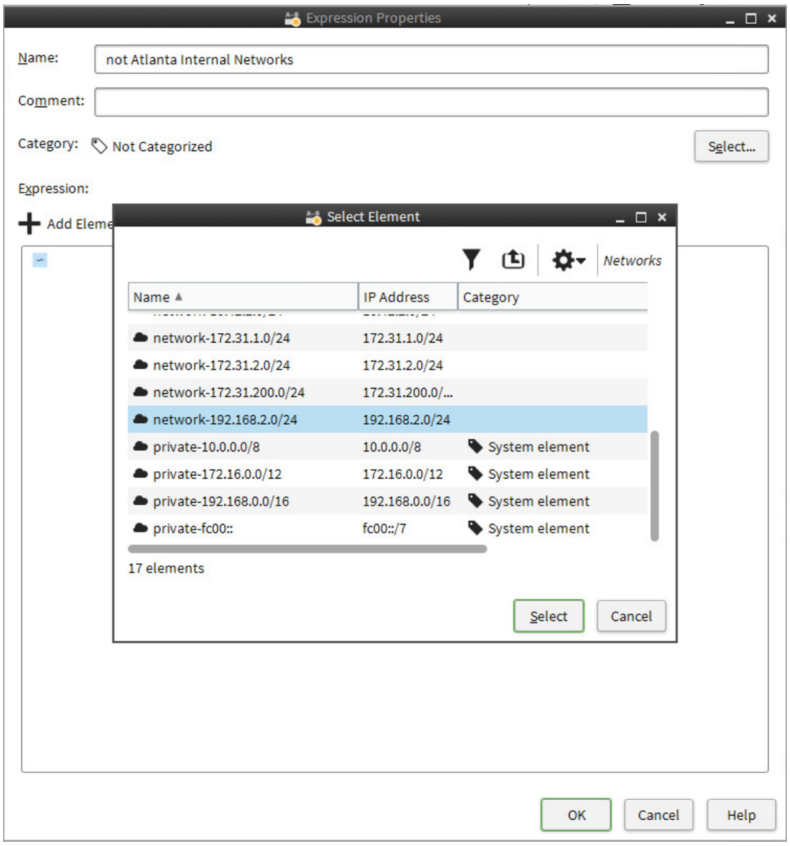


Figure 6.37: Not Atlanta Internal Expression

8. Click **Select**. The Select Element dialog closes. You fully configured expression should appear as in the figure below

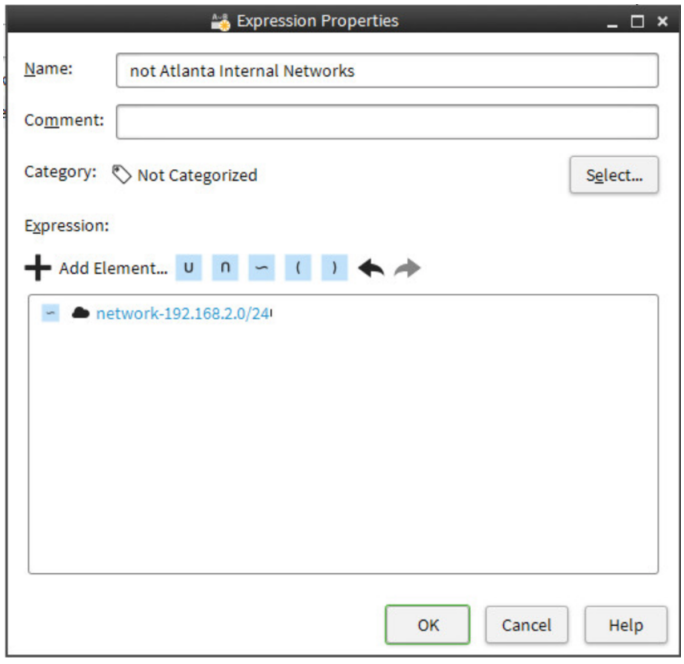


Figure 6.38: Fully Configured Not Atlanta Network Expression

9. Click **OK**. The Expression Properties closes

6.18.3 Add a Rule to Allow Access to the Internet

You have now created the policy and created an Expression that you will use next. You will now create an access rule that permits traffic to the Internet from the Atlanta Internal Network.

1. In the Tab where the Atlanta policy is opened for editing, double-click on the green insert point, **Local Firewall Policy Rules - add rules here**. A new empty rule appears
2. Configure the new rule as follows:
   - **Source**: type `192.168.2.` and select **network-192.168.2.0/24**
   - **Destination**: type `not Atlanta` and select **not Atlanta Internal Networks**
   - **Service**: right-click and set to **ANY**
   - **Action**: right-click and select **Allow**
3. Click the **Save** icon. Your completed Access Rule should appear as in the figure below

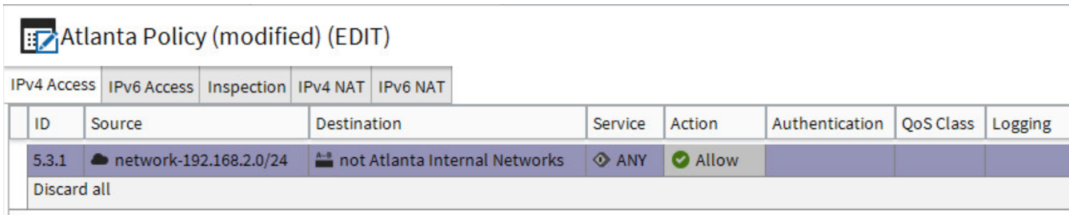


Figure 6.39: Completed IPv4 Access Rule - Atlanta Policy

NOTE: In later labs, you will increase the security of this policy. This rule will allow for general testing.

6.18.4 Create Hosts for Atlanta Web Server

You will now configure two hosts - the Atlanta Web server and the Atlanta Web Server (NAT). These will be used in the rules you will configure below.

1. Browse to **Network Elements** in the Resources list
2. Right-click **Hosts** and select **New Host**. The Host Properties dialog box opens
3. Configure the Host element with the following properties:
   - **Name**: Atlanta Web Server
   - **IPv4 address**: 192.168.2.101
4. Click **OK**
5. Create another new Host element and configure it with the following properties:
   - **Name**: Atlanta Web Server (NAT)
   - **IPv4 Address**: 172.31.2.101

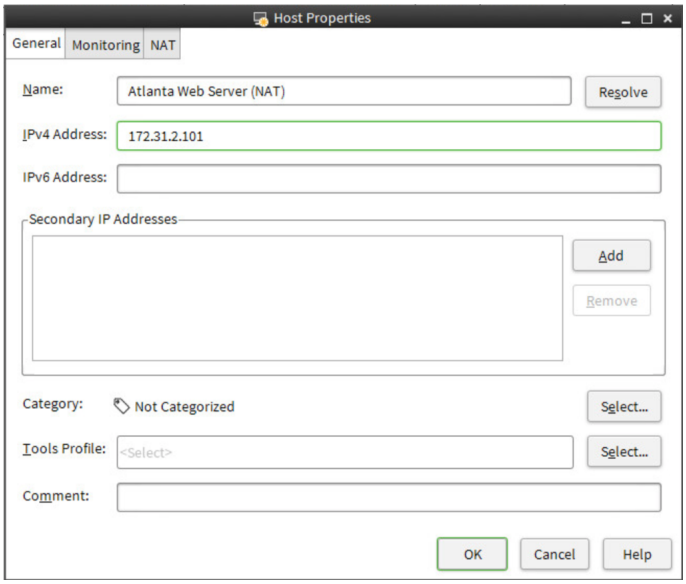


Figure 6.40: Defining Atlanta Web Server Host

6. Click **OK**. The Host Properties closes

6.18.5 Add a Rule for Inbound Traffic to Atlanta Sever

Behind the Atlanta FW Cluster, there is a server that hosts an FTP site as well as a web server. You will now create a host and an access rule to permit these connections.

1. Right-click in the **ID** column of the rule you just created and select **Add Rule Before**. A new empty rule appears
2. Drag and drop **not Atlanta Internal Networks** from the **Destination** cell of the rule below into the **Source** cell of the new rule
3. In the **Destination** cell, type `Atlanta` and select **Atlanta Web Server (NAT)**
4. In the **Service** cell, type `21` and select **FTP**
5. Again in the **Service** cell, type `80` and select **HTTP**
6. Again in the **Service** cell, type `22` and select **SSH**
7. Again in the **Service** cell, type `Ping` and select the protocol
8. Right-click in the **Action** cell, and select **Allow**. Your completed Access rule should appear as in the figure below

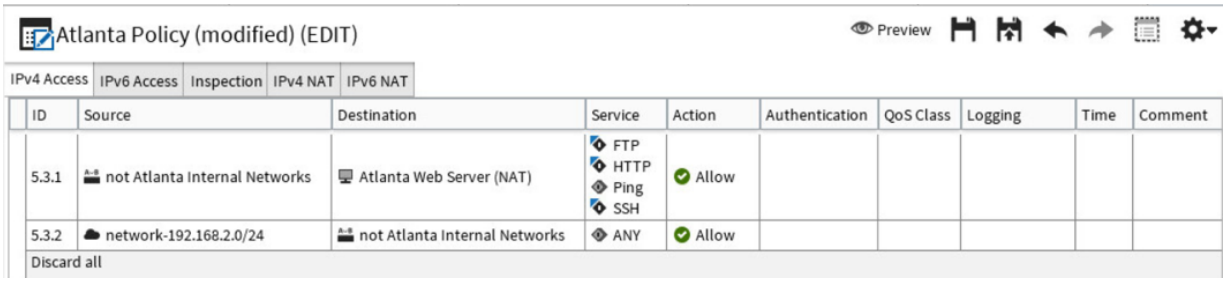


Figure 6.41: Rule to Allow Access to Atlanta Server

6.18.6 Add a Static NAT for the Atlanta Web Server

0.6 The last exercise is to add a static NAT rule that will translate traffic from the Internet to the private IP address of the Atlanta Web Server, 192.168.2.101.

1. Click on the **IPv4 NAT** tab
2. Double-click on the green insert point, **Local Firewall NAT Rules - add rules here**. A new empty rule appears
3. Configure the new rule as follows:
   - **Source**: type `not Atl` and select **not Atlanta Internal Networks**
   - **Destination**: type **Atlanta** and select **Atlanta Web Server (NAT)**
   - **Service**: right-click and set to **ANY**
   - **NAT**: right-click in the **NAT** cell and select **Edit NAT**. Configure NAT as follows:
     (a) Click on the **Destination Translation** tab
     (b) In the **Translate Destination** drop-down list, select **Translate Destination**
     (c) Check the box next to **Translate Destination**
     (d) Click **Select** next to the **Translated** field, and browse to **Network Elements** → **Hosts**
     (e) Click on **Atlanta Web Server** and click **Select**. The Select Element dialog closes
     (f) Make sure that **Automatic Proxy ARP (Recommended)** is checked

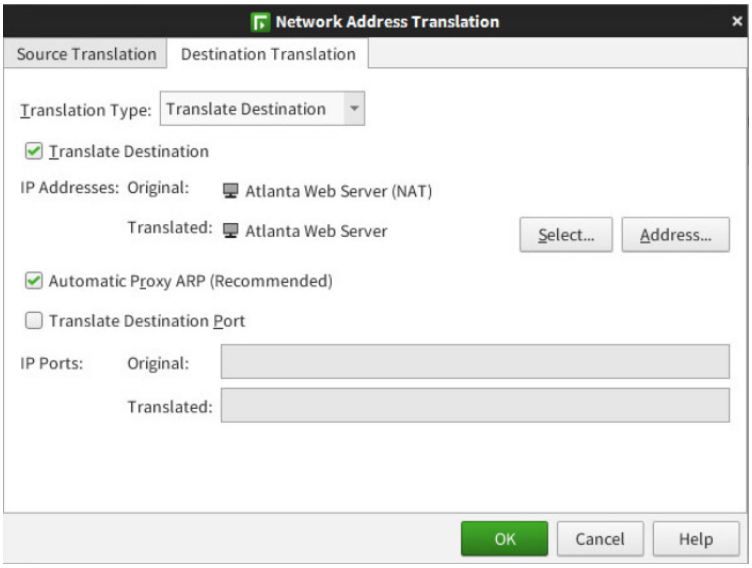


Figure 6.42: Completed NAT Translation for Atlanta Web Server

- Click **OK**. Your completed Static Destination NAT rule should appear as in the figure below

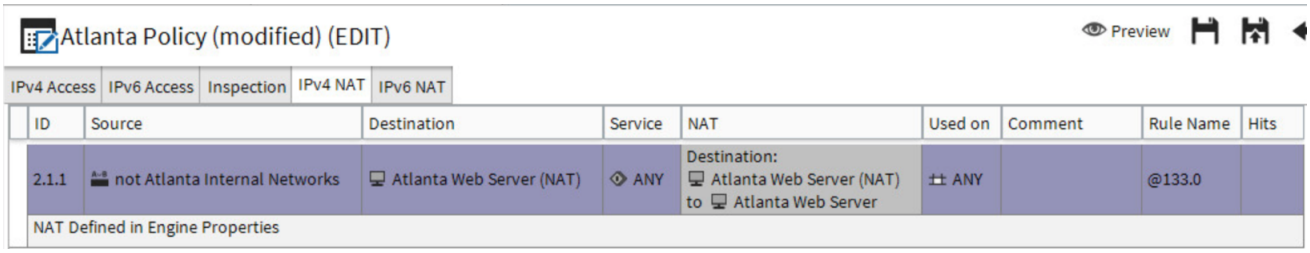


Figure 6.43: Completed Destination NAT for Atlanta Web Server

6.19 Install the Atlanta Policy and Test

Now that the policy is configured, you have a rule that permits traffic out from the internal network, a rule that permits traffic to the public IP of the web server, and a NAT rule that translates the public IP of the web server to its real IP. You will now install the new policy and test connectivity to the web server.

6.19.1 Install the Policy

1. With the **Atlanta Policy** still open for editing, click the **Save and Install** button. The Upload Policy Task Properties opens
2. Click on **Atlanta FW Cluster** and click **Add**

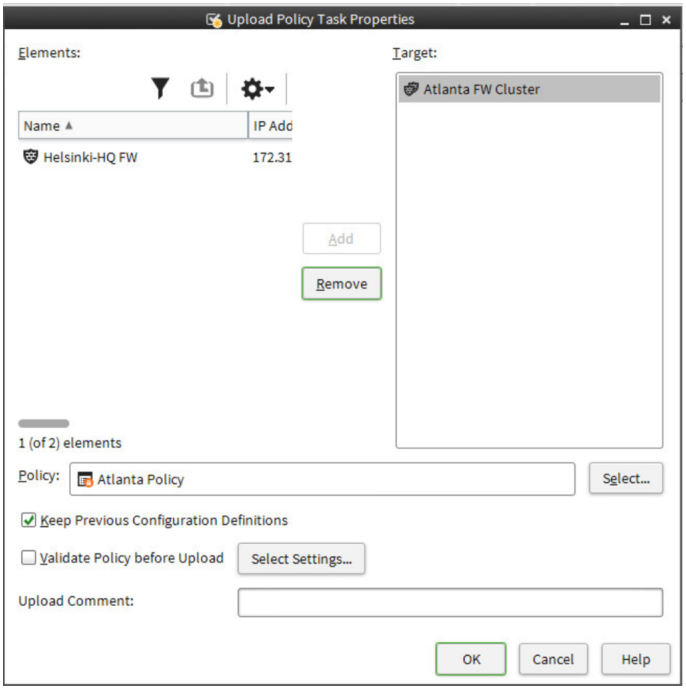


Figure 6.44: Uploading Atlanta Policy

3. Click **OK**. The policy upload begins. When complete, you may close the Upload Policy tab
4. From the Menu Bar, click the **Home** icon and verify that the **Atlanta FW Cluster** has turned green

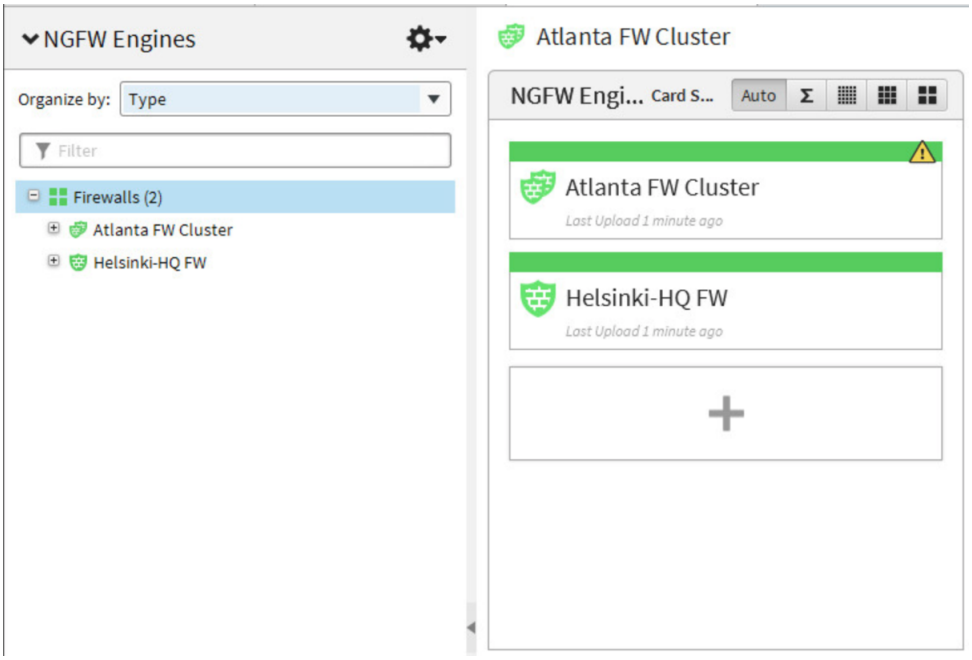


Figure 6.45: Atlanta FW Cluster Successful Policy Installation

6.19.2 Test the Atlanta Policy

You are now ready to test connectivity through the Atlanta FW Cluster by accessing the Atlanta web site. This test will ensure that the access rules permit traffic on HTTP and that the NATing to the private IP address of the web server is being done correctly.

1. On the desktop of **HQ SMC**, double-click the **Firefox** icon
2. In the URL bar, enter `http://server-1.atlanta.com` and press enter. The Atlanta web page is displayed

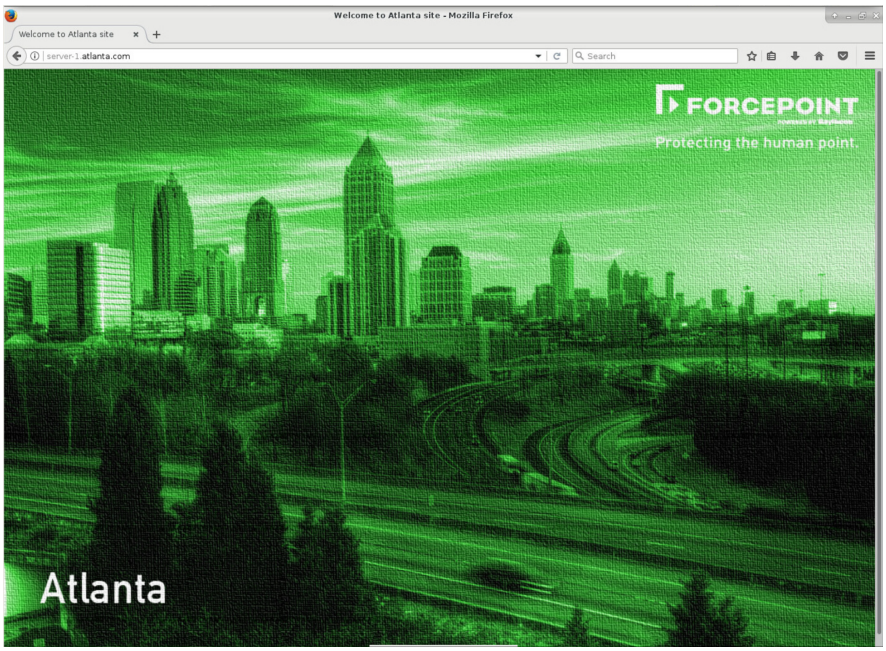


Figure 6.46: Atlanta Web Page - Policy Testing

6.20 Summary

During this lab you have created a two (2) node firewall cluster, configured its routing, and created a firewall policy that allows traffic outbound and allows traffic inbound to the Atlanta web server. The configuration of the firewall cluster provided high-availability and load balancing for Internet traffic. In the next lab, you will configure Multi-Link which will give you high-availability at the level of the ISP.

LAB 7

Outbound Traffic Management - Multi-Link

7.1 Getting Started

Traditionally, connections provided by Internet Service Providers (ISPs) have been a single point of failure for corporate communications. Forcepoint's SD-WAN technology provides both high availability and load balancing between multiple network links (NetLinks). Load balancing between ISPs increases the overall throughput of your network, as it becomes easier to avoid congestion situations. For each new connection request, the firewall can select the fastest route for the connection amongst the available links. Multi-Link technology can be used for both outbound and inbound connections. This lab concentrates on outbound load balancing. You will create the NetLink and Router elements and configured the routing for the Multi-Link configuration. Then you will create an Outbound Multi-Link element and configure NAT rules to define which traffic is load-balanced using the NetLinks.

In Lab 6, you created a Router element for the ISP A connection (the default route) and configured routing for a single-ISP environment. However, the network scenario includes two ISP connections. You will now create another Router element and two NetLink elements and configure the routing so that traffic can be routed through the two ISP connections.

When the Multi-Link configuration is completed and tested for Atlanta Firewall, you will configure the Multi-Link feature for the Helsinki firewall. This is a necessary step before you can setup a full Multi-Link VPN between Atlanta Firewall and Helsinki firewall in lab 8.

7.2 Define the ISP B Router

In this exercise, you will define the Router element to represent the ISP B router for Atlanta FW.

7.2.1 Define the ISP B Router for Atlanta FW

1. Click the tab where the **Configuration** view is open
2. Browse to **Network Elements**, right-click **Routers**, and select **New Router**. The Router Properties dialog box opens
3. Configure the Router with the following properties:
   - Name: **Atlanta ISP B Router**
   - IPv4 Address: **10.1.2.1**
4. Click **OK**

NOTE: You might see a warning about duplicate IP addresses with the ISP A or ISP B Firewall element. You can safely ignore this warning and click **OK**.

7.3 Define NetLinks

NetLinks represent ISP connections or any other communication links, such as leased lines, xDSL, or dialup modems.In this exercise, the NetLinks represent the connections to the ISP A and ISP B Routers. You will also use the NetLinks you create in this exercise later to configure outbound traffic balancing in Outbound Load Balancing.

7.3.1 Define Netlinks for Atlanta FW

1. Right-click **Traffic Handlers** and select **New** → **Static NetLink**. The Static NetLink Properties dialog box opens
2. Create a NetLink element for ISP A with the following **General** properties:
   - Name: **Atlanta ISP A Netlink**
   - Gateway: Select **Atlanta ISP A Router** from the list
   - Network: Click **Select** and select **network-172.31.2.0/24**.
   - Provider Name: **ISP A**
   - Download Speed: Type **100.0** and select **Mbit/s** in the unit of measurement selector on the right
   - Upload Speed: Repeat the same action as in previous step

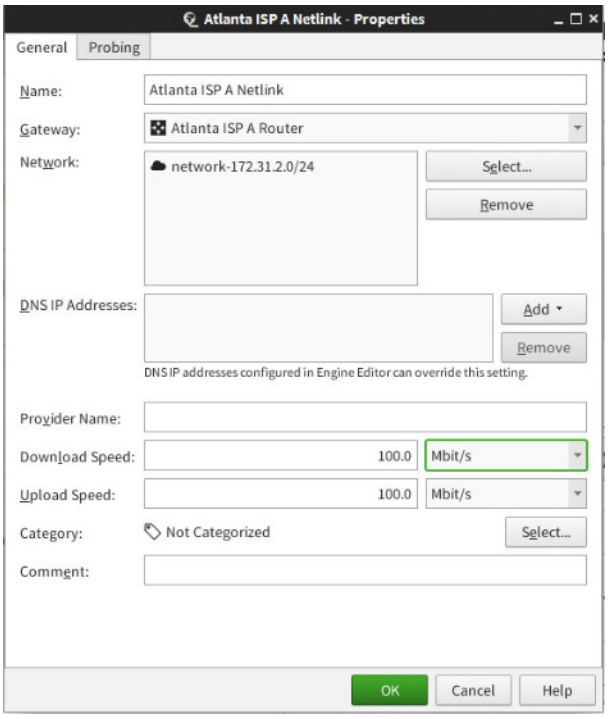


Figure 7.1: Atlanta ISP A Netlink Properties

NOTE: If the correct router does not appear in the list, click **Select**, browse to **Network Elements** → **Routers**, and select **Atlanta ISP A Router.**

3. Click the **Probing** tab
4. Click **Add** and enter **8.8.8.8** as the Probe IP Address **NOTE**: The probe address is needed for NetLinks in standby mode and in inbound load balancing between NetLinks.

Figure 7.2: Configuring Netlink Probing Address

5. Click **OK**.
6. Repeat these steps to create a NetLink element for ISP B with the following properties:
   - Name: **Atlanta ISP B Netlink**
   - Gateway: **Atlanta ISP B Router**
   - Network:**network-10.1.2.0/24**
   - Provider Name: **ISP B**
   - Download Speed: Type **1.0** and select **Mbit/s** in the unit of measurement selector on the right
   - Upload Speed: Repeat the same action as in previous step
   - Probe IP Address: **8.8.8.8**

7.4 Configure Routing for Multi-Link

You must now edit the routing to define which traffic is routed through which NetLink. You do this by adding the NetLinks to the Routing tree under the appropriate interfaces. There is no need to remove the single-ISP configuration, although you do not need it in this lab environment. Having both types of routes is a valid configuration and may sometimes be required by some features that cannot use Multi-Link.

7.4.1 Define Multi-Link Routing for Atlanta

1. Click the tab where the **Atlanta FW Cluster** element is open for editing. Select **Routing**

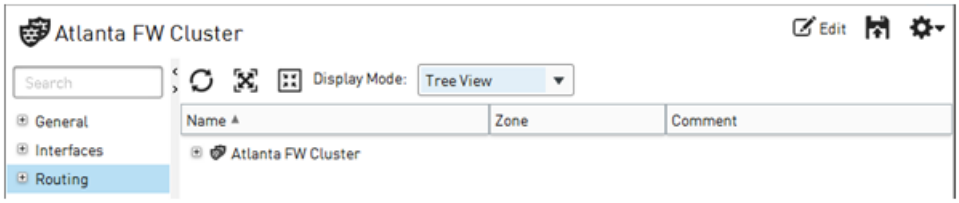


Figure 7.3: Atlanta FW Cluster Routing - Multi-Link

2. Right click the network beneath **Interface 1** and select **Add Static Netlink**

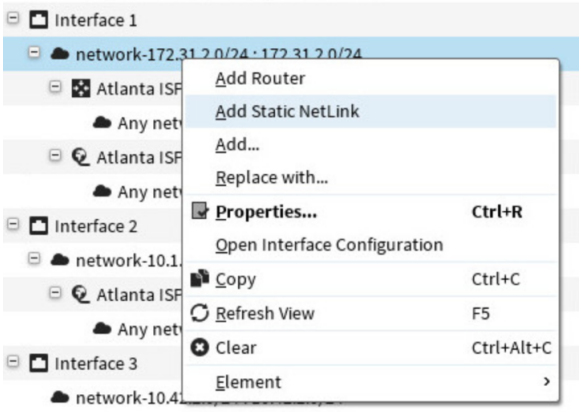


Figure 7.4: Adding a Static Netlink to Routing

3. Add **Atlanta ISP A NetLink** to the **Content** pane. Click **OK**
4. Right-click **Atlanta ISP A NetLink** and click **Set as Default Route**
5. Right-click the network beneath **Interface 2** and select **Add Static Netlink**
6. Add **Atlanta ISP B** to the **Content** pane. Click **OK**
7. Right-click **Atlanta ISP B** NetLink and click **Set as Default Route**
8. Click **Save**
9. Click the **Expand all** icon. The routing definition should should appear as in the figure below

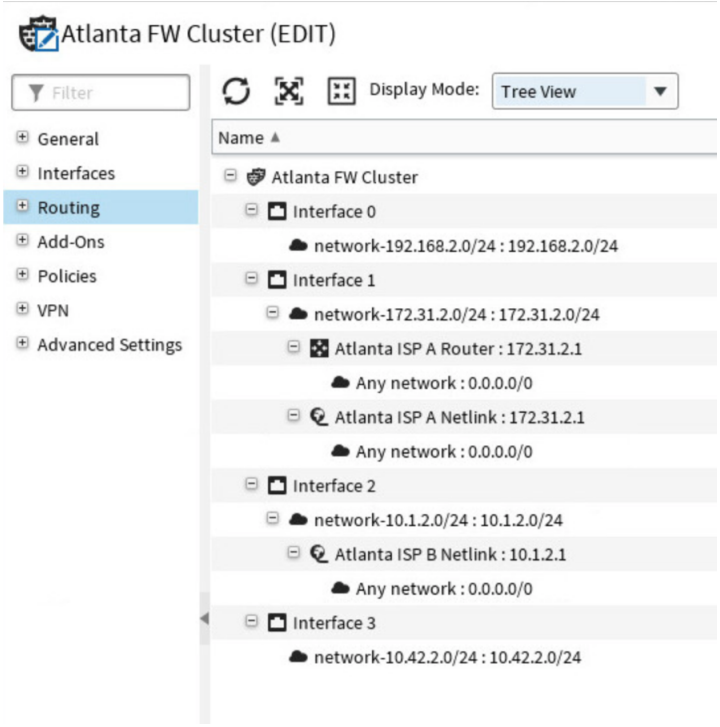


Figure 7.5: Completed Netlink Routing Configuration

7.5 Define an Outbound Multi-Link Element

An Outbound Multi-Link element is used for balancing outbound traffic between different ISPs. The balancing decision (the selection of the link for a given connection) is based on either Round Trip Time or ratio.

7.5.1 Define an Outbound Multi-Link Element for Atlanta

1. Click the **Configuration** and browse to **Network Elements**
2. Right-click **Traffic Handlers** and select **New** → **Outbound Multi-Link.** The **Outbound Multi-Link Properties** dialog box opens
3. Enter **Atlanta Outbound Multi-Link** as the Name
4. Click **Add**. The **Multi-Link Member** dialog box opens
5. Define the Multi-Link Member with the following properties:
   - NetLink: **Atlanta ISP A Netlink**
   - Selected Range: **172.31.2.60-172.31.2.60** (entering the same address in both fields defines a single IP address instead of an address range)

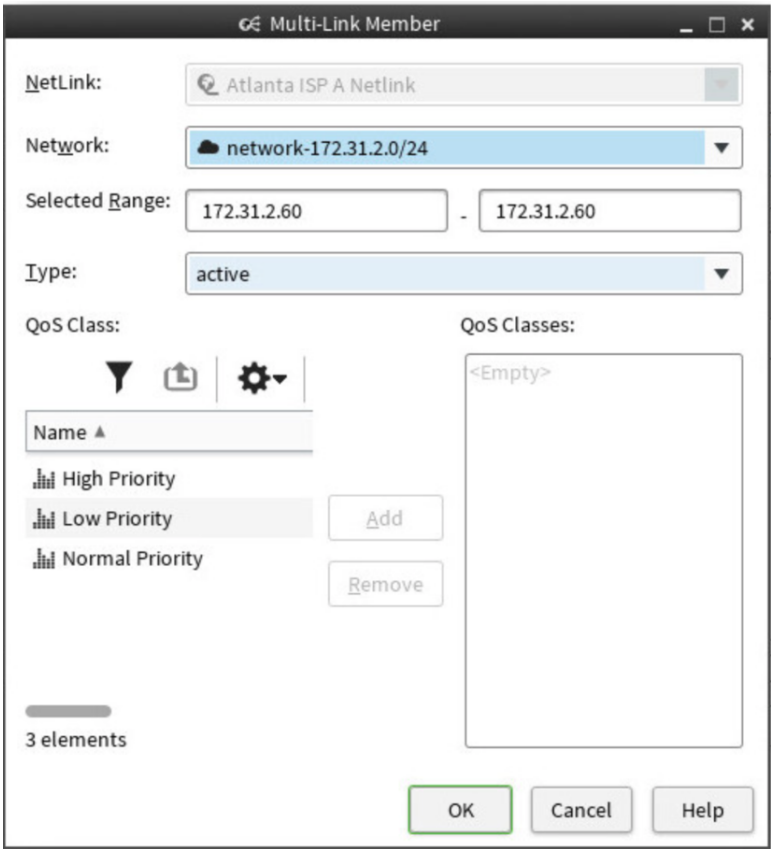


Figure 7.6: Completed ISP A Multi-Link Member

NOTE: The Selected Range setting defines which IP addresses are used for handling outbound load balancing on this NetLink. The range is used for NATing the source IP addresses on the selected NetLink for outbound load balancing. Although it is possible to define a network range, in most cases it is better to use a single IP address.

6. Click **OK**
7. Repeat the steps above to add another Multi-Link Member with the following properties:
   - NetLink: **Atlanta ISP B Netlink**
   - Selected Range: **10.1.2.60-10.1.2.60**
8. Click **OK** to save the **Atlanta Outbound Multi-Link** element

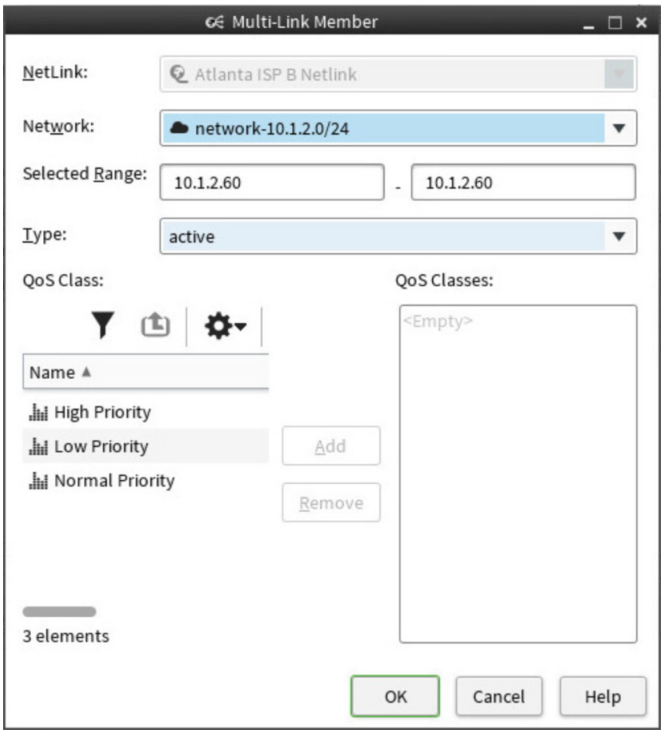


Figure 7.7: Completed ISP B Multi-Link Member

7.6 Create an Outbound Load Balancing NAT Rule

Now that you have defined an Outbound Multi-Link element that includes the NetLinks, you are ready to create an outbound load balancing NAT rule. This rule dynamically balances connections between the NetLinks in the Outbound Multi-Link for traffic that matches the rule.

7.6.1 Defining NAT Rules for Atlanta

1. Click the tab where the **Atlanta Policy** is open for editing
2. Click the **IPv4 NAT** tab
3. Right-click in the **ID** column of your Static Destination NAT rule, and select **Add Rule After**
4. Configure the new rule as follows:
   - Source: **network-192.168.2.0/24**
   - Destination: **not Atlanta Internal Networks**
   - Service: **ANY**
5. Double-click the **NAT cell**. The **Network Address Translation** dialog box opens
6. Under the Source Translation Tab, select **Dynamic** for the **Translation Type**
7. Click **Select** and browse to **Network Elements** → **Traffic Handlers**
8. Select the **Atlanta Outbound Multi-Link** element and click **Select**

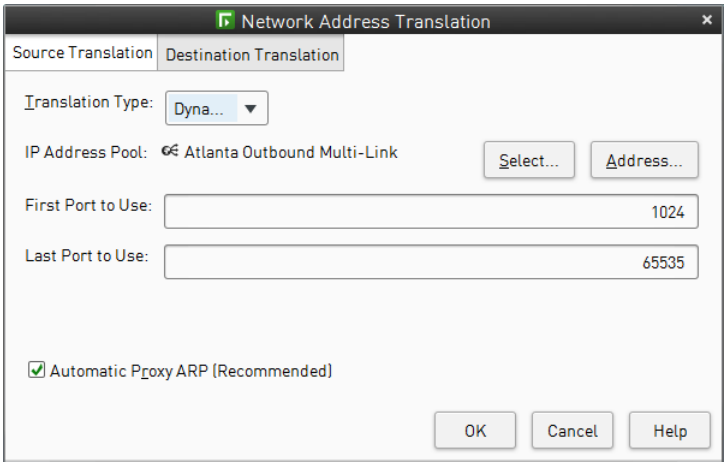


Figure 7.8: Multi-Link NAT Rule Creation

9. Click **OK**. The completed IPv4 NAT rules should appear as in the figure below:

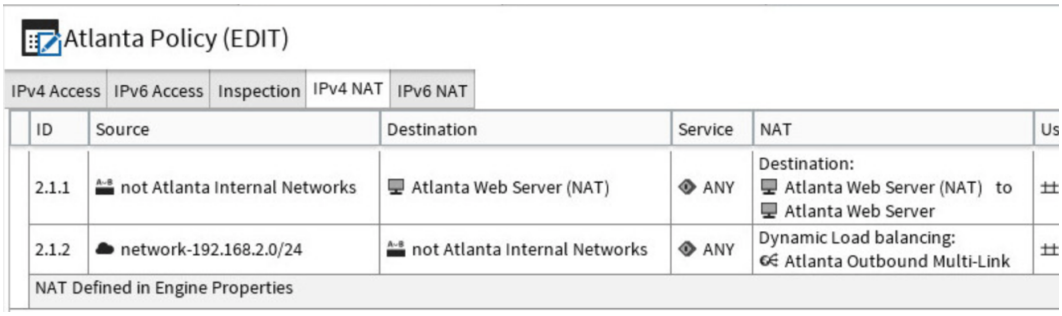


Figure 7.9: Completed Outbound Multi-Link NAT Rule

10. **Save and install** the policy
11. Close the **Upload Policy** Atlanta Policy: tab when the policy upload is completed

7.7 Testing Multi-Link

To test how outbound load balancing between ISPs works, you will connect to an HTTP server through your firewall cluster. In the Logs view, you can follow which ISP is actually chosen by the load-balanced routing.

1. From the **Home** view, right-click on **Atlanta FW Cluster** and browse to **Monitoring** → **Logs by Sender**. The Logs View opens

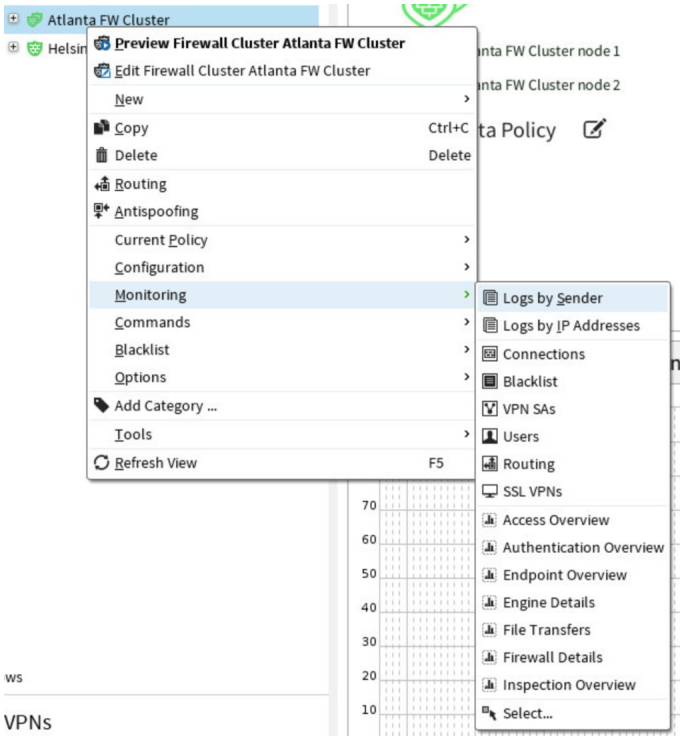


Figure 7.10: Logs by Sender - Multi-Link Testing

2. Click the **Current Events** (play button) icon in the toolbar

Figure 7.11: Current Events Button - Log Browser

3. Using the **Main Menu** from the **Landing Machine**, open a console to the **Atlanta-Server**

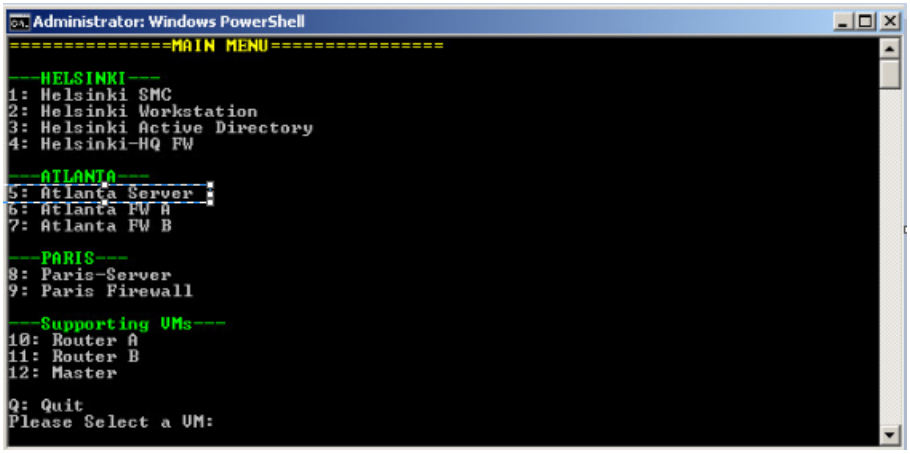


Figure 7.12: Console to Atlanta-Server

4. From **Atlanta-Server**, double-click the **Firefox** icon on the desktop
5. Enter the address `http://server-1.helsinki.com` in the URL field. The Helsinki Website page is displayed

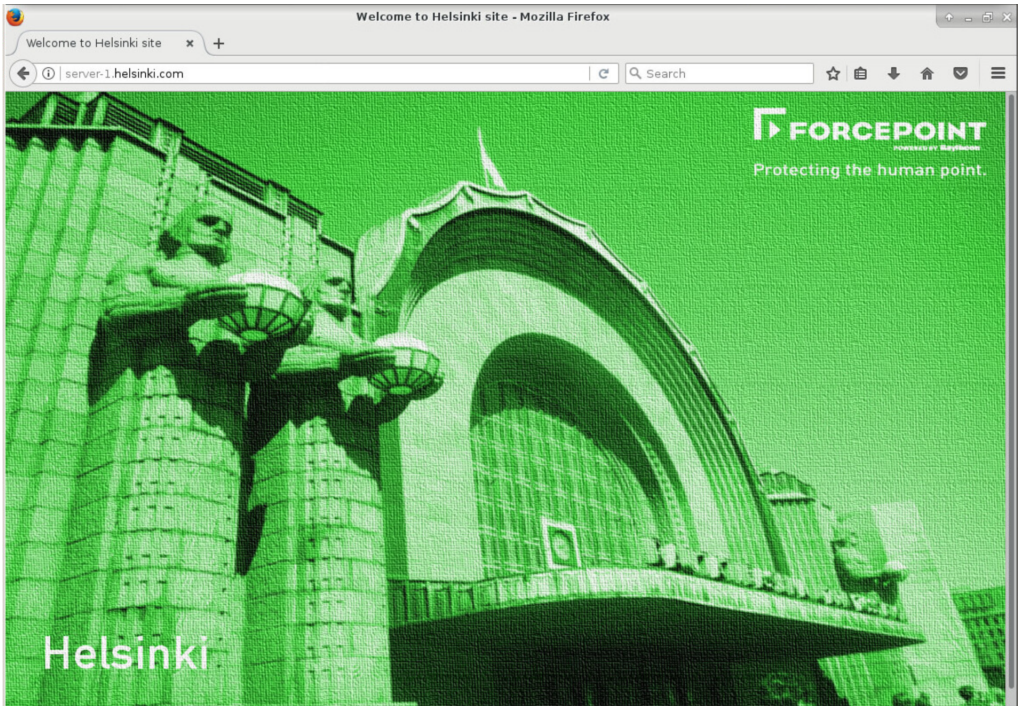
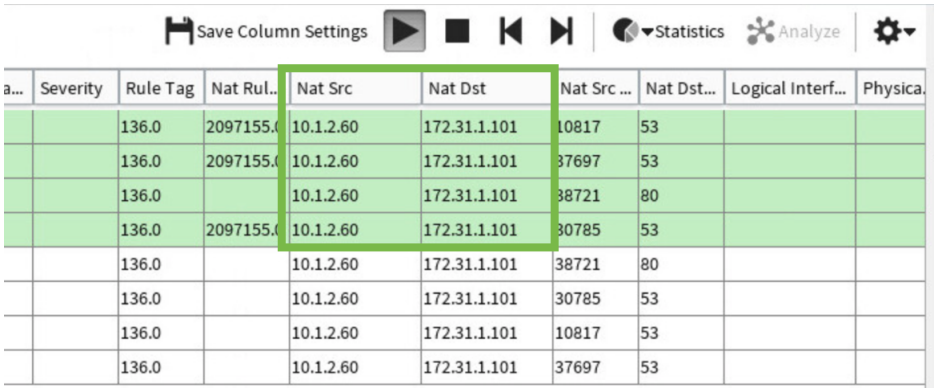


Figure 7.13: Helsinki Web Site - Multi-Link Testing

6. Check the **Nat Src** column in the **Logs** view to see which NetLink is selected



a...	Severity	Rule Tag	Nat Rul..	Nat Src	Nat Dst	Nat Src ...	Nat Dst...	Logical Interf...	Physica.
		136.0	2097155.(	10.1.2.60	172.31.1.101	10817	53		
		136.0	2097155.(	10.1.2.60	172.31.1.101	37697	53		
		136.0		10.1.2.60	172.31.1.101	38721	80		
		136.0	2097155.(	10.1.2.60	172.31.1.101	30785	53		
		136.0		10.1.2.60	172.31.1.101	38721	80		
		136.0		10.1.2.60	172.31.1.101	30785	53		
		136.0		10.1.2.60	172.31.1.101	10817	53		
		136.0		10.1.2.60	172.31.1.101	37697	53		

Figure 7.14: Examining NAT Source for Multi-Link

7. Make a note of which ISP was used. In this example, it is ISP B

7.8 Simulate an ISP Failure

Netlinks, like firewall engines, can be taken off-line. A use case for this would be in a case where ISP maintenance was required. In this exercise, you will force a Netlink off-line and see how the Outbound Multi-Link responds to the ISP being unavailable.

1. From the tab where the **Home** view is open, click on **SD-WAN** on the left side of the client window
2. Expand **Branches** and then right click on **Atlanta FW Cluster**

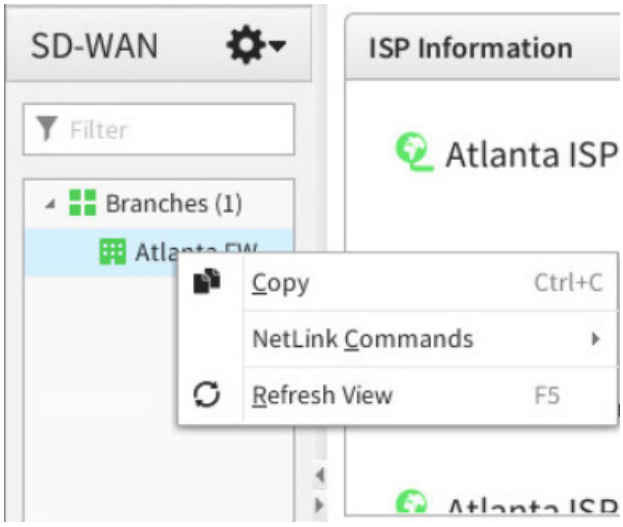


Figure 7.15: View of Branches

3. From the exercise above, you saw that the connection was NATed to ISP B. Move the mouse over **Netlink Commands**, then move on **Atlanta ISP B Netlink** and click on **Force NetLink Disable**. A new tab opens, disabling the Netlink. You may close this tab. In case from the exercise above the connection was NATted to ISP A then perfom the same operation with **ISP A Netlink**.
4. In the tab where the Log Browser is still open, click the **Current Events** button (play button)
5. From the console you have open to **Atlanta-Server**, use Firefox and go to `http://server-1.helsinki.com`

   NOTE: Hold down the **Shift** key to reload this page. It could be cached.
6. Return to the Management Client and look at the logs. You should see that the **Nat Src** field has changed to ISP A

Rule Tag	Nat Rul...	Nat Src	Nat Dst
136.0	2097155.0	172.31.2.60	72.31.1.101
136.0	2097155.0	172.31.2.60	72.31.1.101
136.0		172.31.2.60	72.31.1.101
136.0	2097155.0	172.31.2.60	72.31.1.101
136.0		172.31.2.60	72.31.1.101
136.0		172.31.2.60	72.31.1.101
136.0		172.31.2.60	72.31.1.101
136.0		172.31.2.60	72.31.1.101

Figure 7.16: Change in NAT Source after ISP Failure

7. From the **Home** view, under the **SD-WAN** section on the left, expand **Branches** and then right click on **Atlanta FW Cluster**, move the mouse over **Netlink Commands**, then move on **Atlanta ISP B Netlink** and **Reset NetLink State to Auto**. A new tab opens, and the operation completes. You may close this tab. The Netlink state returns to green

7.9 Configure Multilink for Helsinki-HQ FW

In the lab 8, you will configure a Multi-Link VPN between Helsinki and Atlanta Firewalls. To fully benefit of the Multi-Link VPN capability of the NGFW, it is necessary to have Outbound Multi-Link configured for the firewalls at both end of the VPN. To configure the Outbound Multi-link for the **Helsinki-HQ FW** you will be using a slightly different approach than the one used for the configuration of the **Atlanta FW**.

7.9.1 Create a new route to internet for Helsinki FW

In this exercise you will create a new default route for **Helsinki-HQ FW** to direct any traffic not destined to your internal networks. Once the new route is created you will be proposed with an automatic Multi-link setup.

1. From the **Home** view, right-click on **Helsinki-HQ FW** and select **Edit Single Firewall Helsinki-HQ FW**
2. On the left side, click on **Routing**
3. In the **Routing Tools** panel at the bottom, in the **Default Route** tab, enter **10.1.1.1** which is the IP address of the default gateway for the **Helsinki-HQ FW** second external interface
4. Click **Add**
5. The system detected that a second default route is being added and it provides the options to update the two routers element routing the traffic to internet to netlink elements. In the confirmation dialog that pops up, select **Multilink**
6. Click the **Expand all** icon (just above the Name column). The routing definition should look as in the figure below.

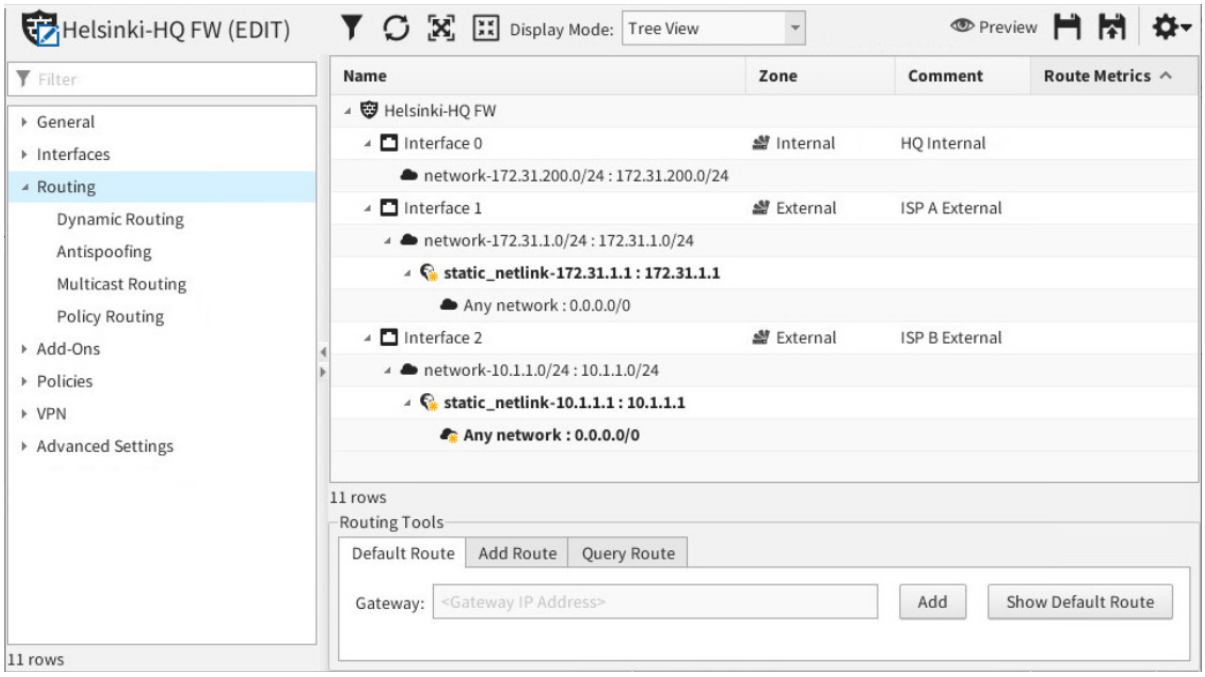


Figure 7.17: Helsinki Routing view

7. Click on the **Save** icon.

7.9.2 Update the Netlinks properties for Helsinki FW

In this section you will update the properties of each **Helsinki**'s netlink in order to include the bandwidth information that will be used to collect information about traffic figures.

1. In the routing view right-click on the **static_netlink-172.31.1.1: 172.31.1.1** and select **Properties**. The netlink properties window will open.
2. Modify the following fields:
   - Download Speed: Type **100.0** and select **Mbit/s** in the unit of measurement selector on the right
   - Upload Speed: Repeat the same action as in previous step

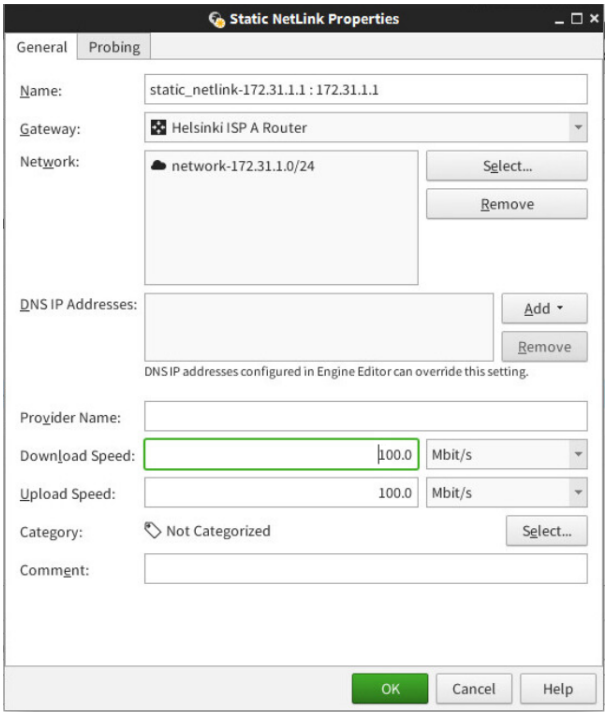


Figure 7.18: Netlink Parameters

3. Repeat the same steps for the **static_netlink-10.1.1.1: 10.1.1.1**
4. Click on the **Save** icon.

7.9.3 Define an Outbound Multi-Link Element for Helsinki

1. Click the **Configuration** and browse to **Network Elements**
2. Right-click **Traffic Handlers** and select **New** → **Outbound Multi-Link.** The **Outbound Multi-Link Properties** dialog box opens
3. Enter **Helsinki Outbound Multi-Link** as the Name
4. Click **Add** in the Multi-Link Members section. The **Multi-Link Member** dialog box opens
5. Define the Multi-Link Member with the following properties:
   - NetLink: **static_netlink-172.31.1.1: 172.31.1.1**
   - Selected Range: **172.31.1.60-172.31.1.60** (entering the same address in both fields defines a single IP address instead of an address range)

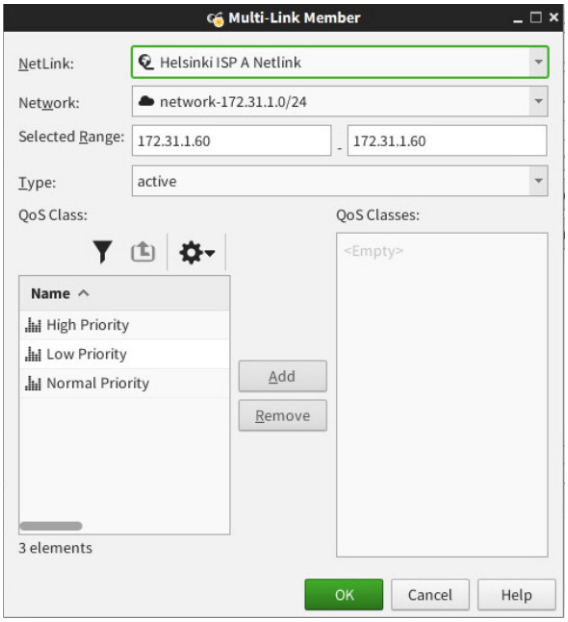


Figure 7.19: Completed ISP A Multi-Link Member

NOTE: The Selected Range setting defines which IP addresses are used for handling outbound load balancing on this NetLink. The range is used for NATing the source IP addresses on the selected NetLink for outbound load balancing. Although it is possible to define a network range, in most cases it is better to use a single IP address.

6. Click **OK**
7. Repeat the steps above to add another Multi-Link Member with the following properties:
   - NetLink: **static_netlink-10.1.1.1: 10.1.1.1**
   - Selected Range: **10.1.1.60-10.1.1.60**
8. Click **OK** to save the **Helsinki Outbound Multi-Link** element

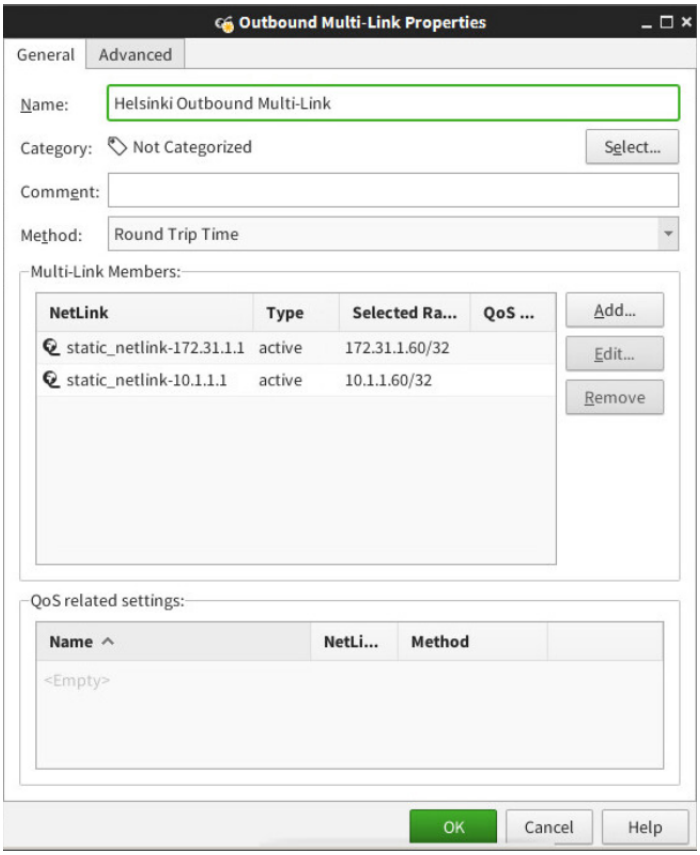


Figure 7.20: Helsinki Outbound Multi-Link

7.9.4 Defining Outbound Multi-Link NAT Rules for Helsinki-HQ FW

1. Click the tab where the **HQ Policy** is open for editing
2. Click the **IPv4 NAT** tab
3. Find the Rule that matches the Outbound traffic from your internal Network (Last rule in the policy), right-click in the **NAT** column and click on **Edit NAT**

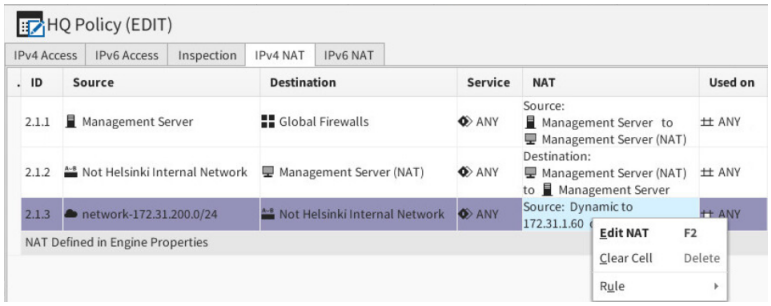


Figure 7.21: Edit Existing NAT Rule

4. Configure the new NAT properties as follows:
   - Under the Source Translation Tab,
   - Click **Select** and browse to **Network Elements** → **Traffic Handlers**
   - Select the **Helsinki Outbound Multi-Link** element and click **Select**

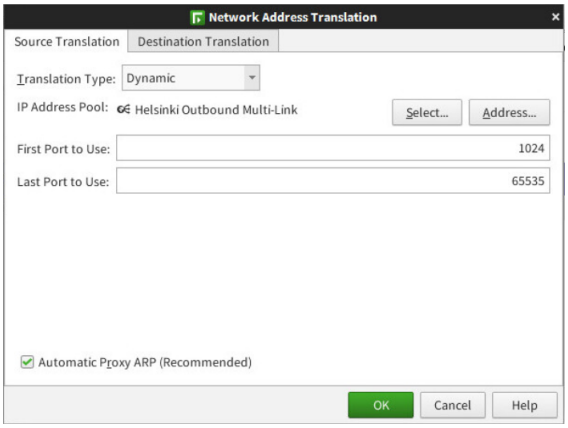


Figure 7.22: Multi-Link NAT Rule Creation

- Click **OK**.

The completed IPv4 NAT rules should appear as in the figure below:

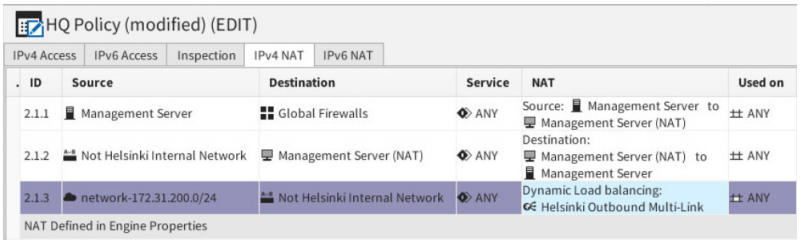


Figure 7.23: Completed Outbound Multi-Link NAT Rule

5. **Save and install** the policy
6. Close the **Upload Policy** HQ Policy: tab when the policy upload is completed

7.10 Summary

In this lab exercise, you have configured Multi-Link to load-balance outbound traffic between two ISP connections for the Atlanta FW Cluster and Helsinki FW. Furthermore, you have verified how the ISP failover and recovery function properly. Next, you will configure a Virtual Private Network (VPN) and use Multi-Link to provide high availability for connections between Atlanta network and the Helsinki Headquarters network.

LAB 8

Policy-Based VPN

8.1 Getting Started

In the previous lab, you configured Outbound Multi-Link for load balancing outbound traffic between multiple ISP links. Now you will configure a VPN and use Multi-Link to provide high availability for connections to the VPN.

Using multiple links for VPN traffic between security gateways offers alternative routes for the traffic, minimizing the effects of ISP service breaks. All VPN traffic is distributed between the active communication links based on connection performance measurements. This way, the firewall can select the route with the best throughput to balance VPN traffic dynamically. The VPN traffic balancing decisions are made separately from decisions on other traffic. When there are multiple links between each security gateway, a logical tunnel can be established between each pair of endpoints. Thus, the use of multiple links enables recovering VPN connections that are lost due to link failure or Internet service breaks.

8.2 Verify Atlanta FW Cluster VPN Settings

When new Firewall elements are created, the VPN Gateway element for the engine is automatically created. The VPN Gateway settings are configured in the VPN section of the Engine Editor.

1. Click the tab where the **Atlanta FW Cluster** is open for editing and browse to **VPN** to review the VPN Gateway configuration
2. If the **Atlanta FW Cluster** is not open for editing in another tab, right-click on the **Atlanta FW Cluster** from the **Home** view and select **Edit Firewall Cluster Atlanta FW Cluster**
3. Browse to **VPN** → **End-Points**. The endpoints configuration should look like the illustration below

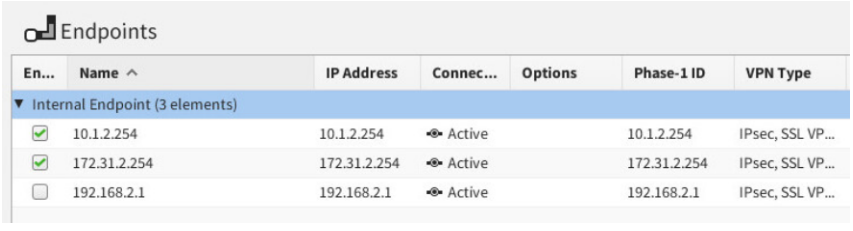


Figure 8.1: Endpoints Configuration

4. Browse to **VPN** → **Sites**. The Sites definition should appear as in the figure below:

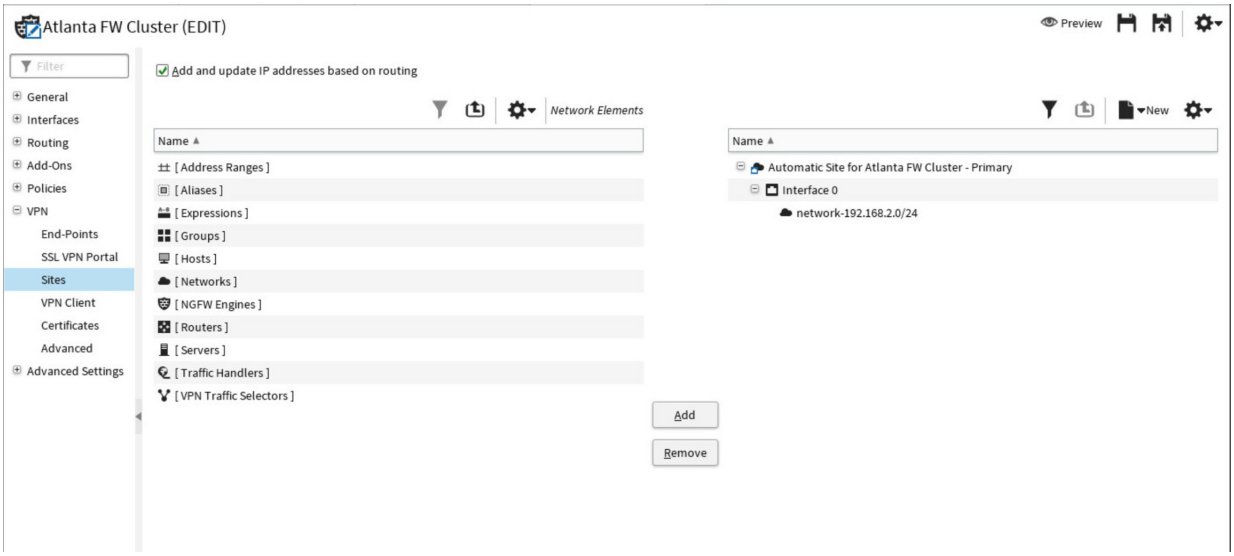


Figure 8.2: VPN Sites Configuration

8.3 Change the Site Definition for Helsinki-HQ FW

By default, the SMC will exclude the network on which the Management Server resides. To ensure that we have the proper site definition, follow the steps below.

NOTE: This step may not always be necessary. In this particular lab environment, changing the site definition was required.

1. From the **Home** view, right-click on **Helsinki-HQ FW** and select **Edit Single Firewall Helsinki-HQ FW**. The Engine Editor opens
2. On the left, browse to **VPN** → **Endpoints**. Verify that both **172.31.1.254** and **10.1.1.254** are checked
3. On the left, click on **Sites**
4. Uncheck the box for **Add and update IP Addresses based on routing**
5. At the top, click the **New** icon and select **Site**. The Site Properties window opens
6. In the **Name** field, enter **HKI-Site**
7. In the Network Elements pane, browse to **Networks** and select **network-172.31.200.0/24** and click the **Add** button
8. Click **OK**. The Site Properties window closes
9. Click **Save** button. You may close the tab where the Engine is open for editing

Your completed Helsinki-HQ FW site definition should appear as in the figure below:

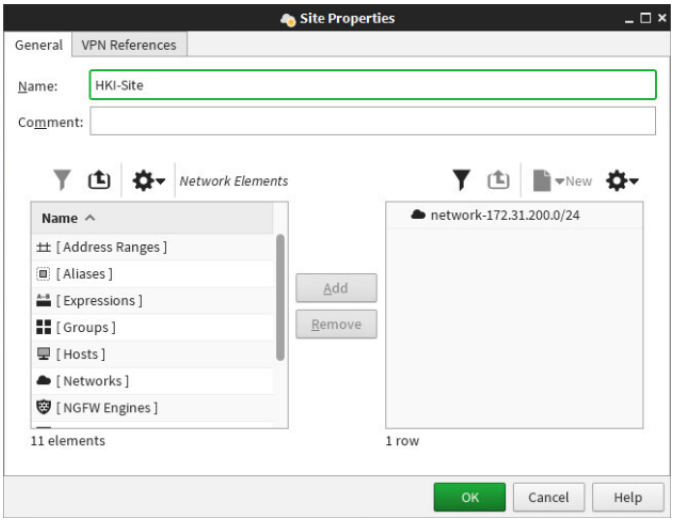


Figure 8.3: Helsinki-HQ FW Site Definition

8.4 Define the VPN Topology

The VPN Gateway elements are visible in the VPN configuration context under the VPN gateway branch. They represent firewalls in VPNs and are used to build the VPN topology.

1. From the toolbar, right-click the **Configuration** icon and select **Open in New Tab**. The Configuration view opens
2. In the tree view, browse to **SD-WAN** → **Policy-Based VPNs**
3. Right-click on **Policy-Based VPNs** and select **New Policy-Based VPN**. The Policy-Based VPN Properties dialog box opens

Figure 8.4: Creating a New Policy-Based VPN

4. In the **Name** field, enter **HQ-ATL VPN**

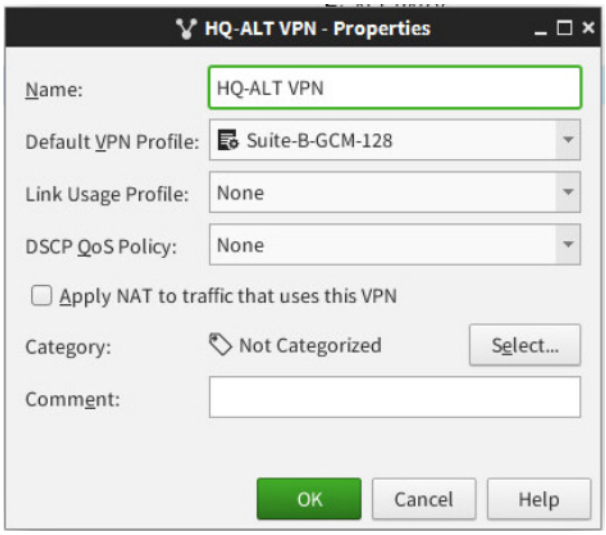


Figure 8.5: New VPN Properties

5. Click **OK**. The Policy-Based VPN Properties dialog closes. The VPN editor opens
6. Browse to **Gateways** in the **Resources list**
7. Drag and drop **Atlanta FW Cluster - Primary** to **Satellite Gateways**
8. Drag and drop **Helsinki-HQ FW - Primary** to **Central Gateways**

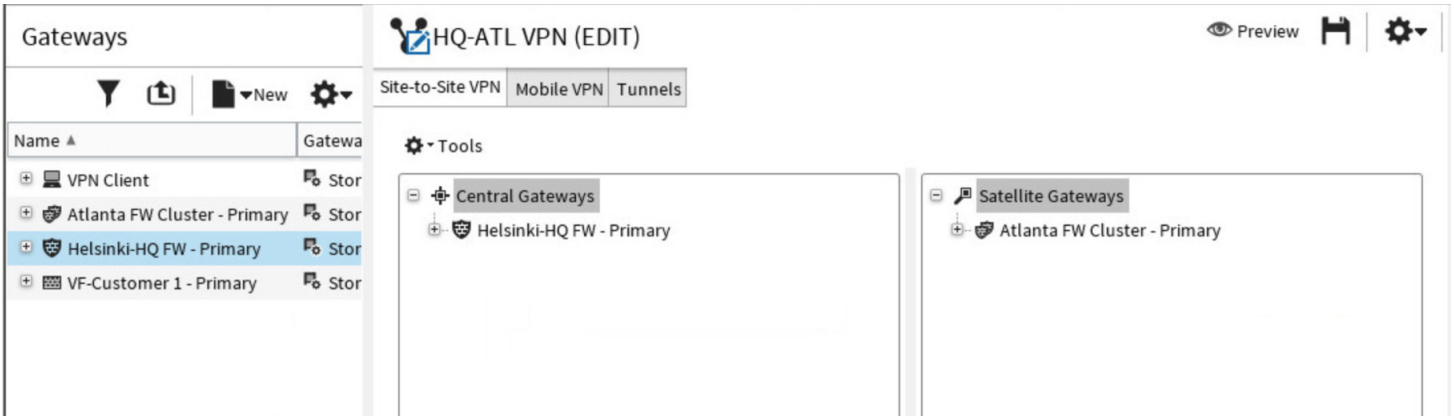


Figure 8.6: HQ-ATL VPN Topology

9. Click the **Save** icon in the toolbar

8.5 View the VPN Tunnels

1. Click the **Tunnels** tab and check the tunnels that have been generated
2. Click the **Gateway** <-> **Gateway** tunnel between **Atlanta FW Cluster** and **Helsinki-HQ FW** to view the associated **Endpoint** <-> **Endpoint** tunnels

Figure 8.7: Endpoint-to-Endpoint Tunnels

8.6 Create VPN Rules

After you have added your gateway to the VPN, you must now create rules on both the Atlanta FW Cluster and the Helsinki-HQ FW. These rules will allow traffic between the internal networks of both firewalls, encrypted by IPSec.

8.6.1 Create VPN Access Rules for Atlanta FW Cluster

1. From the **Home** view, right-click on the **Atlanta FW Cluster** and browse to **Current Policy** → **Edit**. The Atlanta Policy opens for editing
2. Right-click in the **ID** cell of the first rule, and select **Add Rule Before**. A new empty rule appears
3. Configure the new rule with the following values:
   - **Source**: type `network-192.168` and select **network-192.168.2.0/24**
   - **Destination**: type `network-172.31.` and select **network-172.31.200.0/24**
   - **Service**:
     - type `80` and select **HTTP**
     - type `21` and select **FTP**
     - type `echo req` and select **Ping**
   - **Action**: right-click in the **Action** cell, and select **Allow**.
   - Then right-click in the **Action** cell and select **Edit Options**. The Select Rule Action Options dialog box opens.
   - In the **VPN Action** field, select **Enforce VPN**
   - In the **VPN** field, select the **HQ-ATL VPN** element.

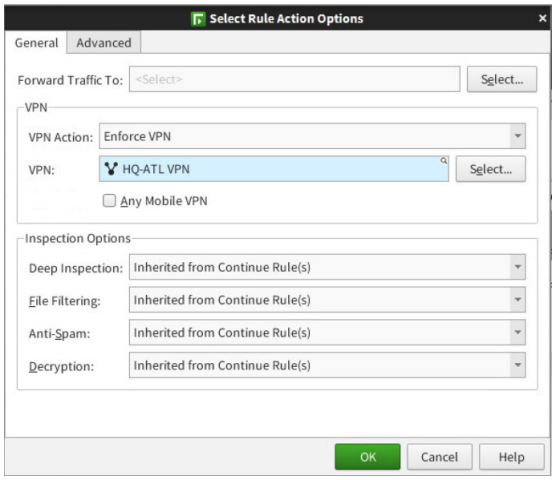


Figure 8.8: Enforcing the HQ-ATL VPN

- Click **OK**. The Select Rule Action Options dialog box closes

4. Right-click in the **ID** cell of the rule you just created and select **Copy Rule**
5. Right-click in the **ID** column of the same rule and select **Paste**. The rule is pasted below
6. In the rule that pasted, right-click in the **Source** and **Destination** cells and select **Clear Cell**
7. Drag **network-172.31.200.0/24** from the **Destination** cell from the rule above into the **Source** cell
8. Drag **network-192.168.2.0/24** from the **Source** cell from the rule above into the **Destination** cell. Your completed VPN rules for the **Atlanta FW Cluster** should appear as in the figure below:

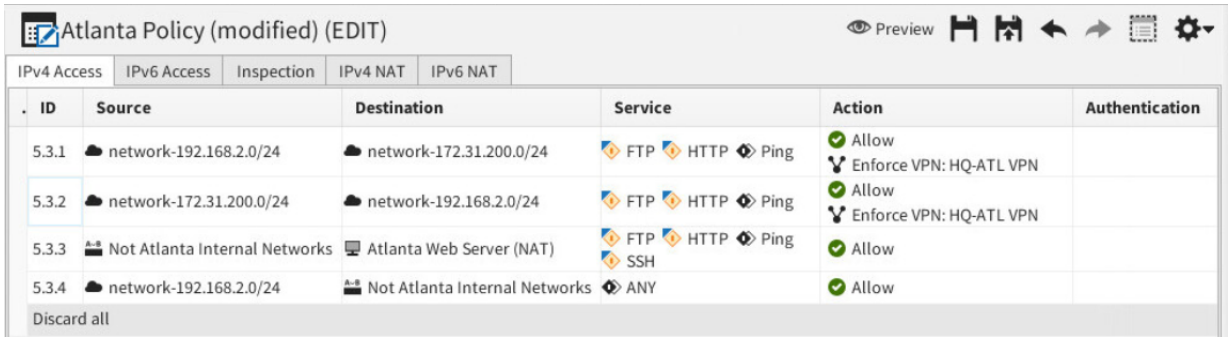


Figure 8.9: Completed Atlanta FW Cluster VPN Rules

9. Click in the **ID** cell of the first VPN rule. Hold down the **Shift** key, and click in the **ID** cell of the rule below. Both rules are highlighted. Right-click and select **Copy Rule**
10. Click the **Save and Install** icon. When the policy upload completes, close the policy upload tab. Close the tab where the **Atlanta Policy** is open for editing

8.6.2 Create VPN Access Rules for Helsinki-HQ FW

You will now add access rules that permit VPN traffic through the Helsinki-HQ FW.

1. From the **Home** view, right-click on **Helsinki-HQ FW** and browse to **Current Policy** → **Edit**. The HQ Policy opens for editing
2. Right-click in the **ID** cell of the rule permitting traffic from **Global Firewalls** to **Management Server (NAT)**, and select **Paste**

3. The two rules you copied from the **Atlanta Policy** are pasted into the **HQ Policy**. Your completed VPN rules for the **HQ Policy** should appear as in the figure below:

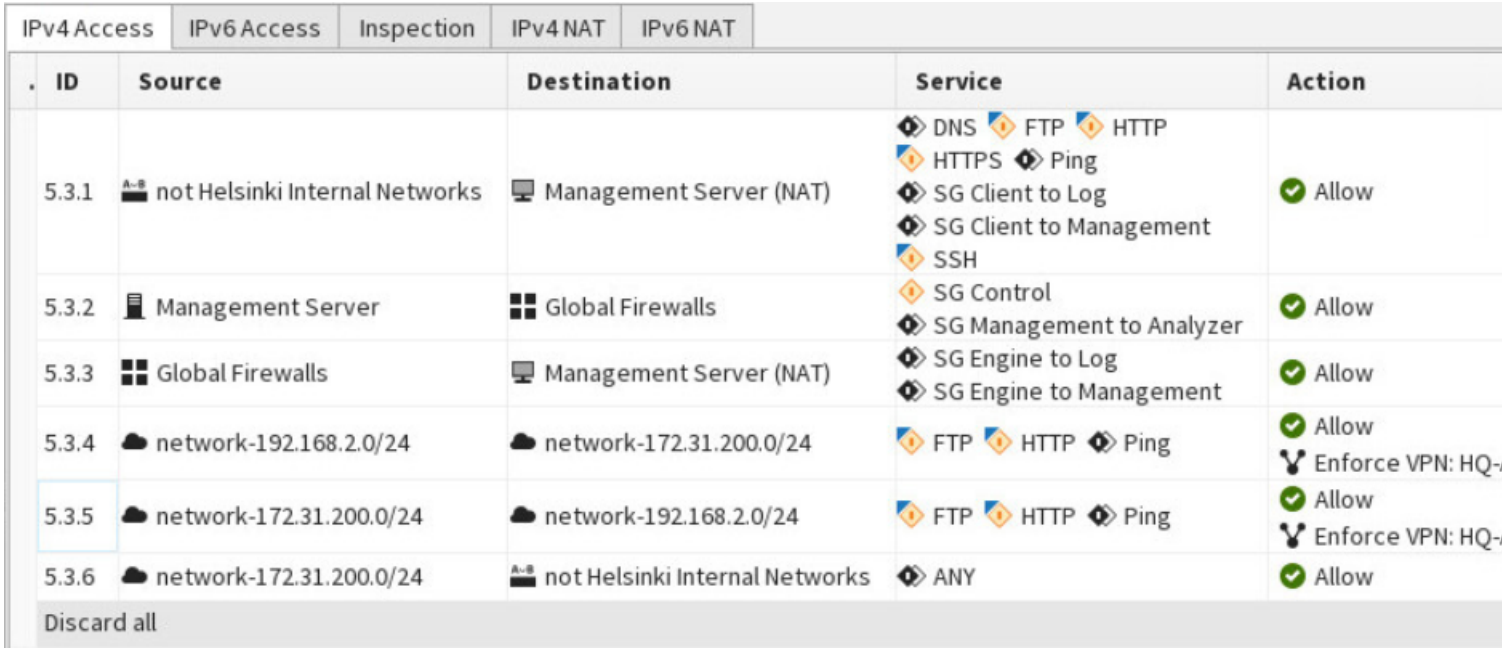


Figure 8.10: VPN Rules for Helsinki

4. Click the **Save and Install** icon. When the policy upload completes, close the policy upload tab. Close the tab where the **HQ Policy** is open for editing

8.7 Test Your Multi-Link VPN

Now that you have created a Multi-Link VPN and the necessary VPN Access rules, you can test how the firewall handles VPN traffic using multiple endpoints by downloading a file from your partner site.

1. From the **Home** view, right-click on **Atlanta FW Cluster** and browse to **Monitoring** → **Logs by Sender**. The Log browser opens
2. In the **Query** panel on the right, use the drop-down menu, and click **Select**
3. In the dialog that opens, scroll down and select the **VPN** logging context

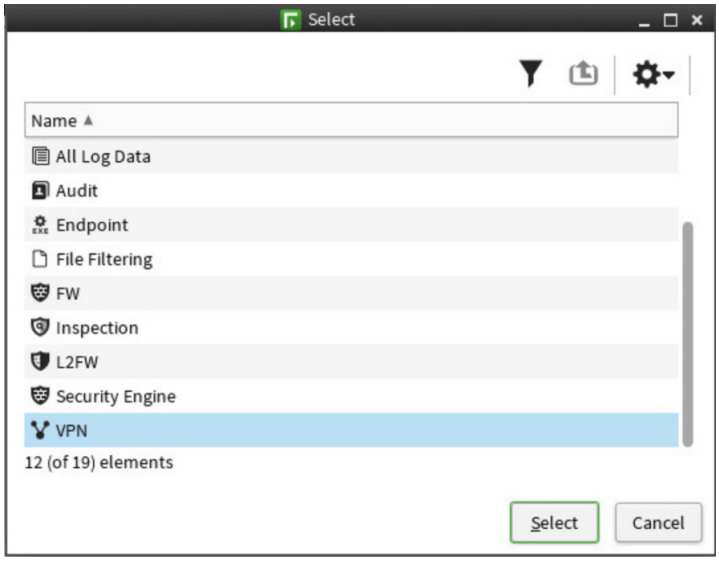
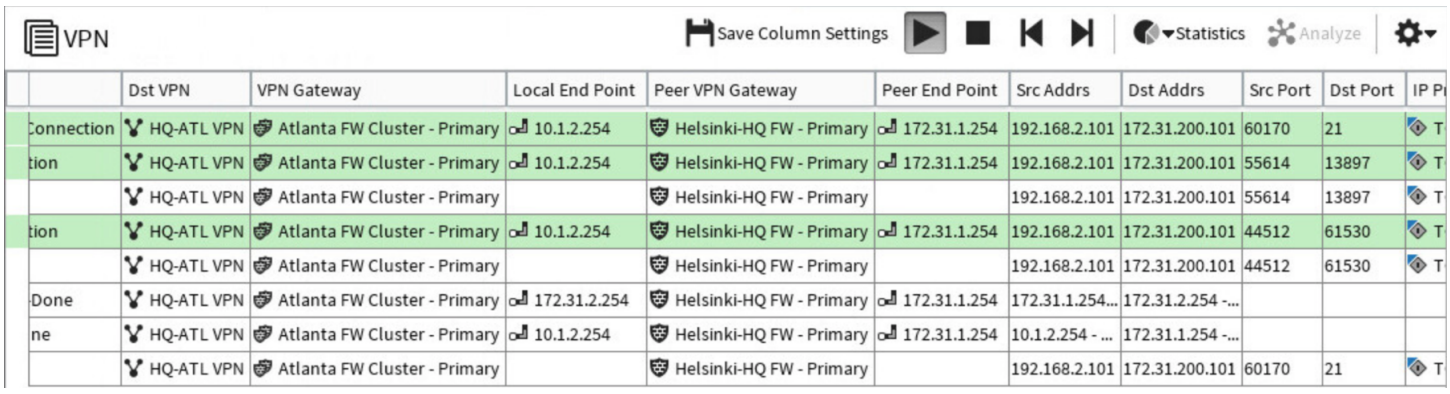


Figure 8.11: Selecting the VPN Logging Context

4. Click **Select**. The Select dialog box closes
5. In the **Query** panel, click **Apply**
6. Click the **Current Events** button in the logging toolbar
7. Using the **Main Menu** from the **Landing Machine**, open a console to **Atlanta-Server**
8. Open a **Terminal** you opened earlier, type `ping 172.31.200.105` This is the internal IP address of the HQ Active Directory server
9. From the **Atlanta Server**, double-click the **Firefox** icon
10. In the URL bar, enter `ftp://172.31.200.101`
11. Click the **pub** directory and then click **bigfile_100M**. The file downloads
12. Return to the **HQ SMC**. Look at the **Log** browser and you should see something similar to this:



	Dst VPN	VPN Gateway	Local End Point	Peer VPN Gateway	Peer End Point	Src Addrs	Dst Addrs	Src Port	Dst Port	IP P
Connection	HQ-ATL VPN	Atlanta FW Cluster - Primary	10.1.2.254	Helsinki-HQ FW - Primary	172.31.1.254	192.168.2.101	172.31.200.101	60170	21	T
tion	HQ-ATL VPN	Atlanta FW Cluster - Primary	10.1.2.254	Helsinki-HQ FW - Primary	172.31.1.254	192.168.2.101	172.31.200.101	55614	13897	T
	HQ-ATL VPN	Atlanta FW Cluster - Primary		Helsinki-HQ FW - Primary		192.168.2.101	172.31.200.101	55614	13897	T
tion	HQ-ATL VPN	Atlanta FW Cluster - Primary	10.1.2.254	Helsinki-HQ FW - Primary	172.31.1.254	192.168.2.101	172.31.200.101	44512	61530	T
	HQ-ATL VPN	Atlanta FW Cluster - Primary		Helsinki-HQ FW - Primary		192.168.2.101	172.31.200.101	44512	61530	T
Done	HQ-ATL VPN	Atlanta FW Cluster - Primary	172.31.2.254	Helsinki-HQ FW - Primary	172.31.1.254	172.31.1.254...	172.31.2.254 -...			
ne	HQ-ATL VPN	Atlanta FW Cluster - Primary	10.1.2.254	Helsinki-HQ FW - Primary	172.31.1.254	10.1.2.254 - ...	172.31.1.254 -...			
	HQ-ATL VPN	Atlanta FW Cluster - Primary		Helsinki-HQ FW - Primary		192.168.2.101	172.31.200.101	60170	21	T

Figure 8.12: VPN Logging Context

13. Click the tab where the **Home** view is open and expand the **SDWAN** section on the left hand side.
14. Expand the Policy-Based VPN tree and click **HQ-ATL VPN**. Detailed Multi-Link tunnel status information appears.
Note: If the view is empty, on the main tool bar, click **Menu** → **View** → **Layout** → **Reset Layout**

15. Expand the **Helsinki - HQ FW - Primary - Atlanta FW Cluster - Primary** in the the Tunnels Pane to see which Multi-link Tunnel is used (Status Online)

16. In the Main Menu, open a console and select the Router currently routing the VPN traffic.

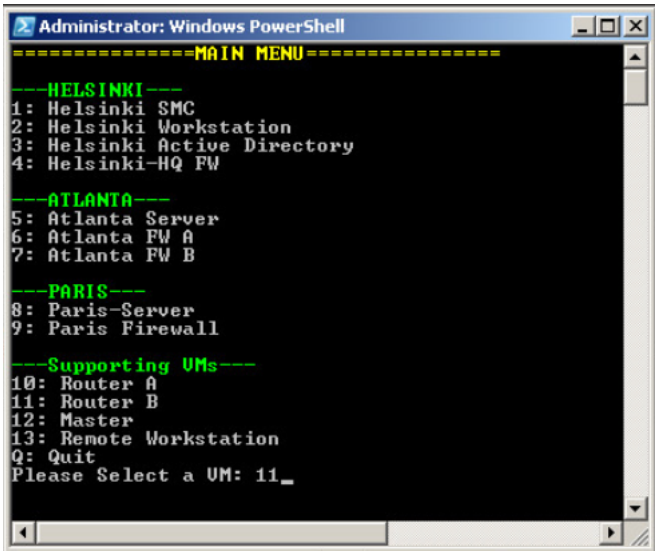


Figure 8.13: Console to the Router

17. Switch off the routers by clicking on the Suspend button in the VMware menu bar.

Figure 8.14: Suspend button

18. From the Atlanta Server, in the Firefox URL bar, enter `ftp://172.31.200.101`

19. Click **bigfile_1000M** in the web browser and select Save to download the file.

20. In the SDWAN dashboard in the Home view, check the Tunnels Pane to see which Multi-link Tunnel is now used.

21. When you have completed the lab, switch the router on by clicking the Power on button in the menu bar of the Router VM.

8.8 Summary

In this lab, you configured a Multi-Link VPN to ensure that the VPN connection to your partner is available without interruptions at all times. You have now set up a reliable network infrastructure with the required redundancy features.

LAB 9

Authentication and User Identification

Getting Started

User Authentication and User Identity are two concepts that are related to each other in that the information they use comes from a directory server, most often Active Directory. With user information available to the firewall, decisions can be made about access control with user identity, and users a required to prove their identity through authenticaion.

Users and user groups can be used in the source and destination of access control rules. In that scenario, the user is resolved to an IP address. The IP address of the user can be sent to the firewall, directly, using Forcepoint User Identification or, as in this lab, the Endpoint Context Agent. The Endpoint Context Agent provides the IP address of the user as well as information about the applications, or programs, running on the endpoint. In this respect, the Endpoint Context Agent can provide more information that Forcepoint User Identification alone. The primary difference is that Forcepoint User Identification identifies users at the network level, whereas ECA identifies users at the level of the endpoint.

In this lab, you will integrate Active Directory with the SMC, allowing you to use user information in the source and destination columns of access rules and use the same user information for authentication. You will then install the Endpoint Context Agent and block specific applications from running on the endpoint.

9.1 Integrate Active Directory with the SMC

In this exercise, you will create a new Active Directory Server element and supply the appropriate credentials, allowing the SMC and Active Directory to communicate.

1. From the **Home** view, click on the **Configuration** icon in the menu bar. The Configuration view opens
2. Browse to **Network Elements** → **Servers**

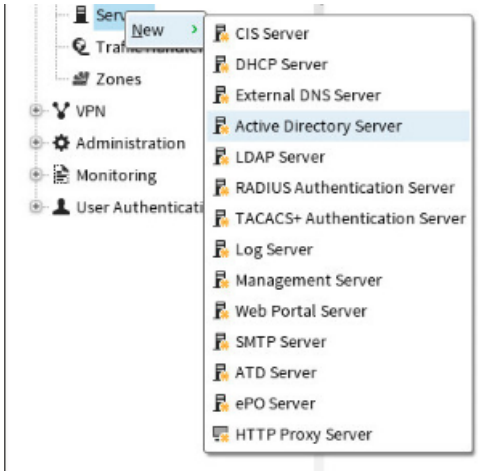


Figure 9.1: Creating a New Active Directory Server

3. Right-click on **Servers** and select **New** → **Active Directory Server**. The Active Directory Server Properties opens
4. Configure the Active Directory Server with the following values:
   - **Name**: HQ AD
   - **IP Address**: 172.31.200.105
   - **LDAP on Port**: 389
   - **Base DN**: `dc=helsinki,dc=com`
   - **BIND User ID**: `cn=Jim,cn=Users,dc=helsinki,dc=com`
   - **BIND Password**: Forcepoint1!
5. Click on the **Authentication** tab
6. Check the box for **Use Network Policy Server Method (NPS)**
7. Leave the **Port Number** set to **1812**
8. Enter `Forcepoint1!` as the **Shared Secret**

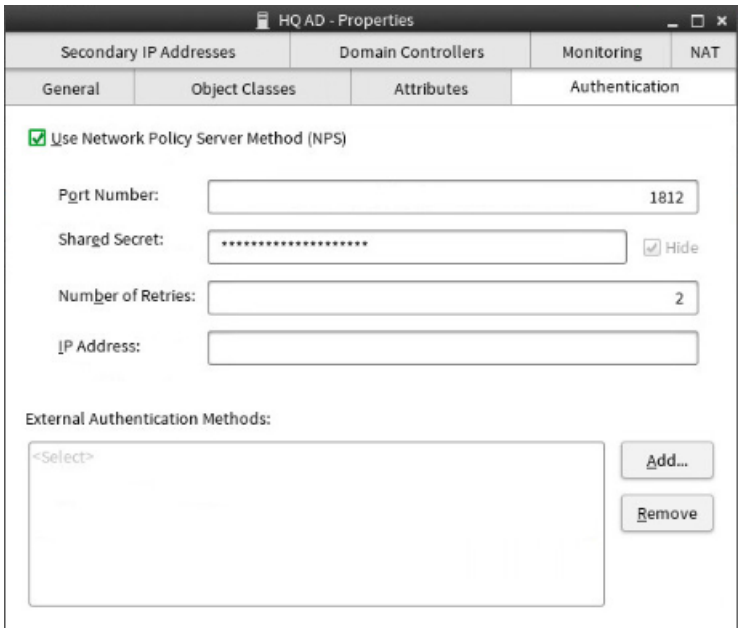


Figure 9.2: NPS Authentication Settings

9. Switch back to the **General** tab and click the **Check Connectivity** button. A message appears indicating that the connection was successful. Click **OK**

10. Click **OK**. Your completed Active Directory Server should appear as in the figure below:

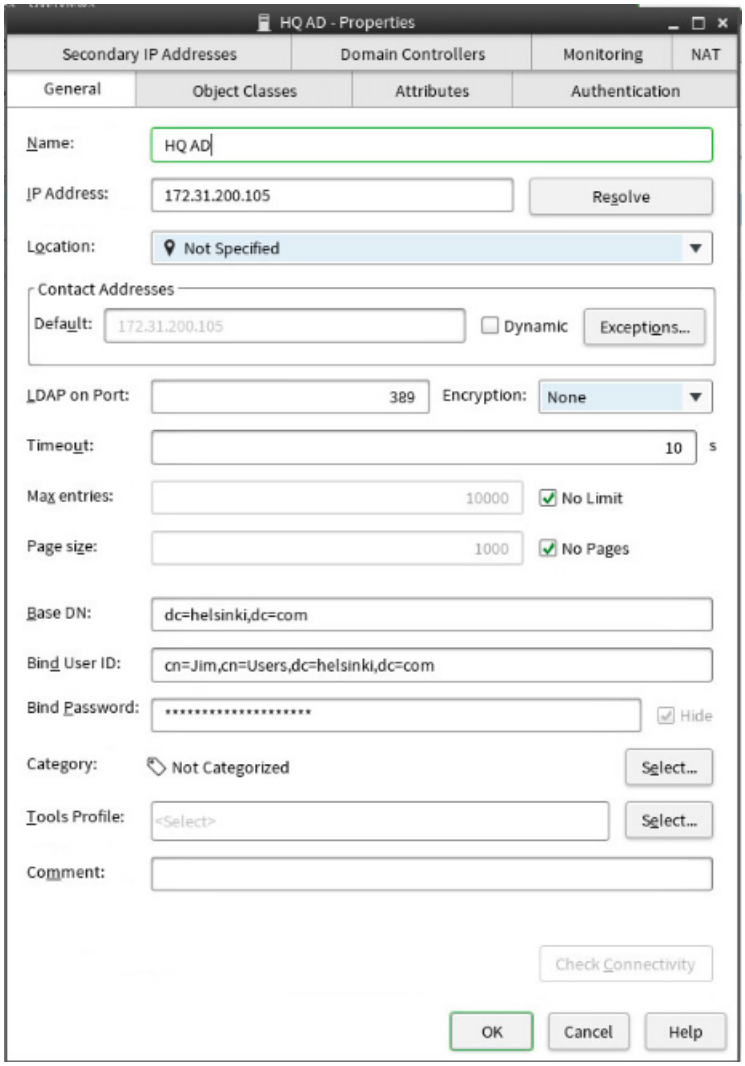


Figure 9.3: Completed Active Directory Server Element

9.2 Add a New LDAP Domain

Now that the Active Directory has been integrated, you are now ready to add the LDAP domain that Active Directory controls. This will allow you to browse through the AD forrest and have access to users and user groups.

1. From the same **Configuration** view, use the **Resources** tree on the left, and browse to **User Authentication** → **Users**

2. Right-click on **Users** and select **New External LDAP Domain**

3. In the **Name** field, enter `helsinki.com`

4. Check the box for **Default LDAP Domain**

5. In the **Servers** pane, click on **HQ AD** and click the **Add** button. HQ AD now appears in the **Bound Servers** pane

6. Click on the **Default Authentication** tab

7. Click the **Select** button next to the **Default Authentication** field. The Select Element dialog box opens
8. Click on **Network Policy Server** and click **Select**. The Select Element dialog closes

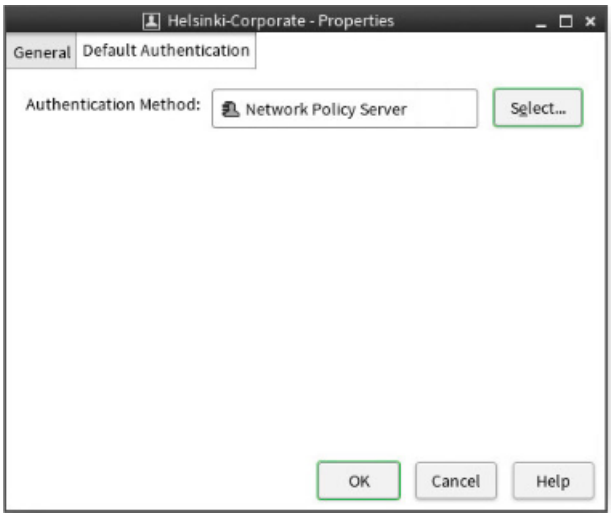


Figure 9.4: Default Authentication Selection of NPS

9. Click **OK**. Your completed LDAP Domain properties should appear as in the figure below:

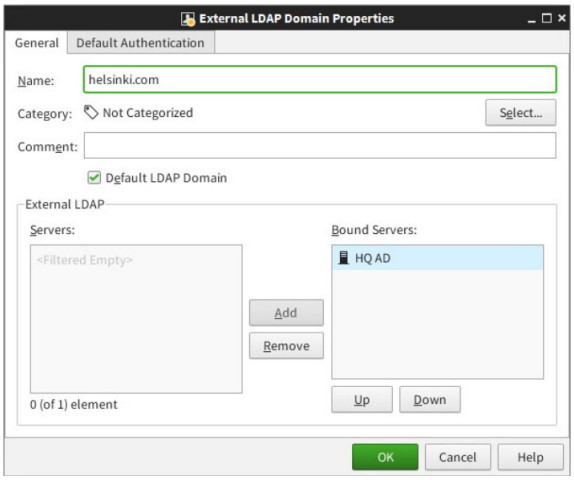


Figure 9.5: Completed Helsinki-Corporate Domain Properties

9.3 Configure ECA for the SMC and Engine

You are now ready to take the next step for User Identification and endpoint application control. To do this, you will import the CA Certificate of the Active Directory Server into the SMC. This will then be used to create an Endpoint Context Agent configuration file that is used for the installation of the Endpoint Context Agent on a domain computer.

9.3.1 Create a New Trusted CA with the AD CA Certificate

1. From the same **Configuration** view, use the **Resources** tree on the left and browse to **Administration** → **Certificates** → **Certificate Authorities** → **Trusted Certificate Authorities**
2. Right-click on **Trusted Certificate Authorities** and select **New** → **Trusted Certificate Authority**. The Trusted Certificate Authority Properties opens

3. In the **Name** field, enter **HQ CA**
4. Click on the **Certificate** tab
5. At the bottom, click the **Import** button. The Import Certificate dialog box opens
6. Use the drop-down menu for **Look in** and navigate to \ → `home` → `Student` → `Desktop`
7. Click on **HQ-CA.crt** and click **Open**. The Certificate appears

Figure 9.6: Imported AD CA Certificate

8. Click **OK**. The Trusted Certificate Authorities Properties closes

9.3.2 Create an ECA Configuration

You will now create an ECA Configuration. This configuration will be used to activate ECA on the firewall side. This will be used by the firewall to create an ECA configuration file that the endpoint will use during the agent installation.

1. Still in the **Configuration** view, browse to **NGFW** → **Other Elements** → **Engine Properties** → **ECA Configurations**
2. Right-click on **ECA Configurations** and select **New** → **New ECA Configuration**. The ECA Configuration Properties opens
3. In the **Name** field, enter **HQ-ECA-Config**
4. Click the **Add** button. The Select Element dialog box opens
5. Locate the **HQ CA** and click **Select**. The Select Element dialog closes

   TIP: Type part of the name (e.g. HQ) and the HQ CA will appear
6. Click **OK**. Your completed ECA Configuration should appear as in the figure below:

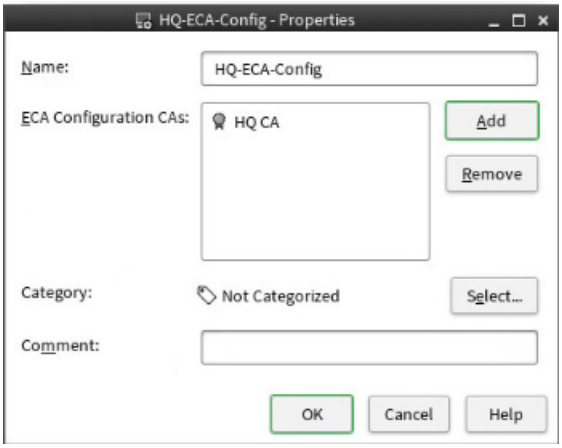


Figure 9.7: Completed ECA Configuration

9.3.3 Configure Helsinki-HQ FW for ECA

Now that you have created the ECA Configuration file, you must now apply this to the firewall. Once it is applied to the firewall, you will be able to create the endpoint ECA configuration file that is used on the endpoint during the installation of the Endpoint Context Agent.

1. From the same **Configuration** view, use the **Resources** tree and browse to **NGFW** → **NGFW Engines**
2. Right-click on **Helsinki-HQ FW** and select **Edit Single Firewall Helsinki-HQ FW**. The firewall properties opens
3. On the left, expand **Add-Ons** and click on **Endpoint Integration**
4. Use the **Endpoint Service** drop-down menu, and select **Forcepoint Endpoint Context Agent (ECA)**
5. Click **Select** next to the **ECA Configuration** field. The Select Element dialog box opens
6. Click on **HQ-ECA-Config** and click **Select**
7. In the **Source Network** pane, click **Add**. The Select Element dialog box opens
8. Click on **Zones** and then click on **Internal** and click **Select**. The Select Element dialog box closes
9. Click **Add** next to the **Listening Interfaces** pane. The Select Element dialog box opens
10. Click **Interfaces**. Click on **Interface 0 (172.31.200.1)** and click **Select**. The Select Element dialog box closes
11. Leave the **Listening Port** set to **9111**

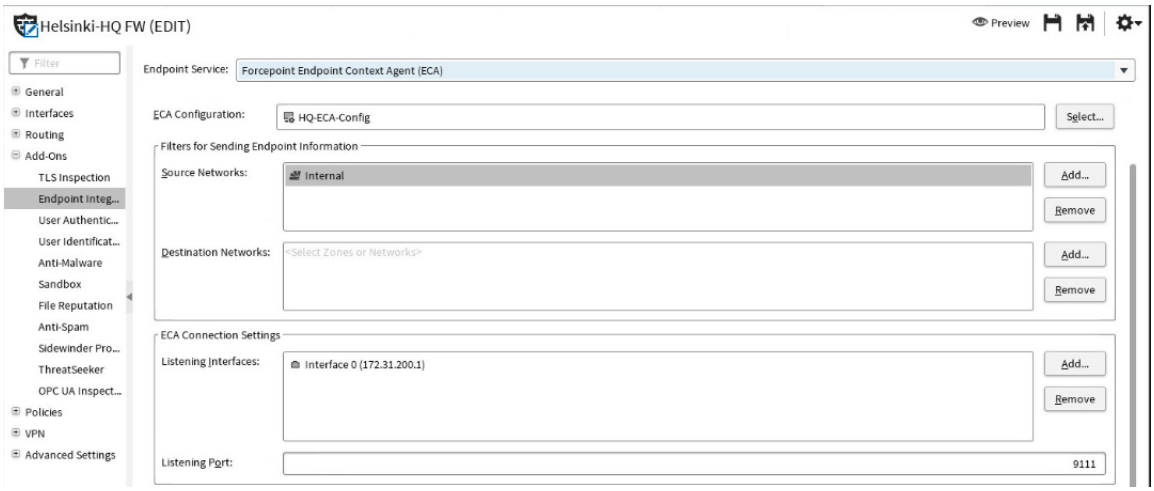


Figure 9.8: Engine Properties with ECA Configured

12. Click the **Save** icon
13. At the bottom of the engine editor, click the **Export Configuration for Endpoint Clients**. The HQ-ECA-Config - Properites dialog box opens
14. Click **Browse** and browse to \ → `home` → `Student` → `Desktop`. Click **OK**. The Export File dialog box closes

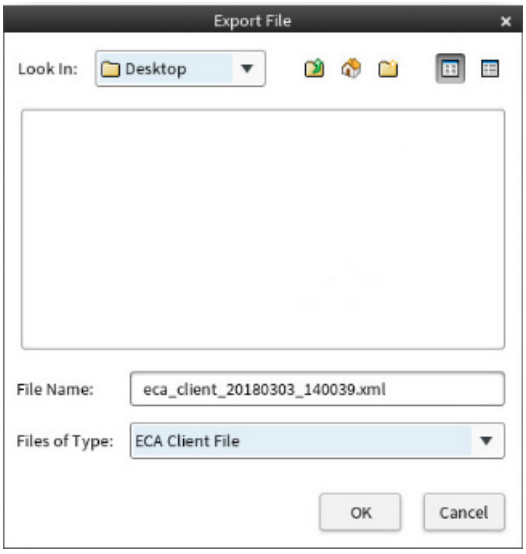


Figure 9.9: Saving the ECA Client Configuration

15. Click **Export**. The HQ-ECA-Config - Properties dialog box closes

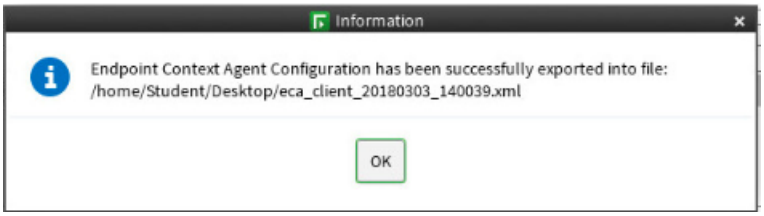


Figure 9.10: Successful Export of ECA Client Configuration

16. Click **OK** to close the dialog indicating the successful export of the client ECA configuration file
17. Click **Save and Install**. You may close the tab where the Engine is open for editing

9.4 Install ECA on the Helsinki Workstation

At this point, Active Directory has been integrated with the SMC giving you access to users and user groups that you will use later. You have also configured the Engine to receive and send information to the Endpoing Context Agent. The CA certificate of Active Directory has been imported so that the client certificates issued by Active Directory's certificate auto-enrollment will be trusted. It is now time to install the Endpoint Context Agent on the endpoint.

9.4.1 Download the ECA Client Configuration File to the Helsinki Workstation

1. Using the **Main Menu** from the **Landing Machine**, open a console to the **Helsinki Workstation**

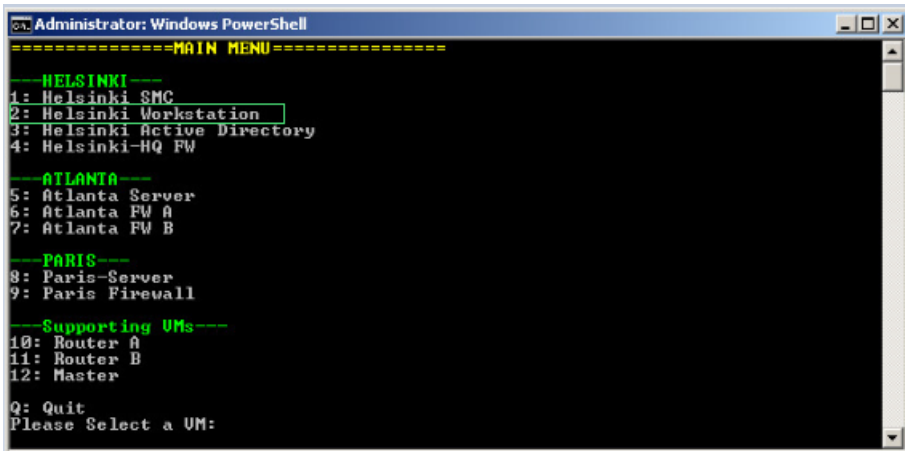


Figure 9.11: Opening a Console to Helsinki Workstation

2. At top of the console window, click on **VMRC** and then click on **Send Ctrl+Alt+Del**
3. Click **Switch User** and then select **Other**
4. At the login prompt, log in with the user **HKI-Wrk1\Administrator**. Enter `Forcepoint1!` as the password

   NOTE: The ECA client must be installed as the local Administrator
5. On the taskbar, click the Documents folder

Figure 9.12: Opening Explorer to Download ECA Configuration

6. In the navigation bar at the top, click and enter `ftp://Student@172.31.200.101` and press **Enter**

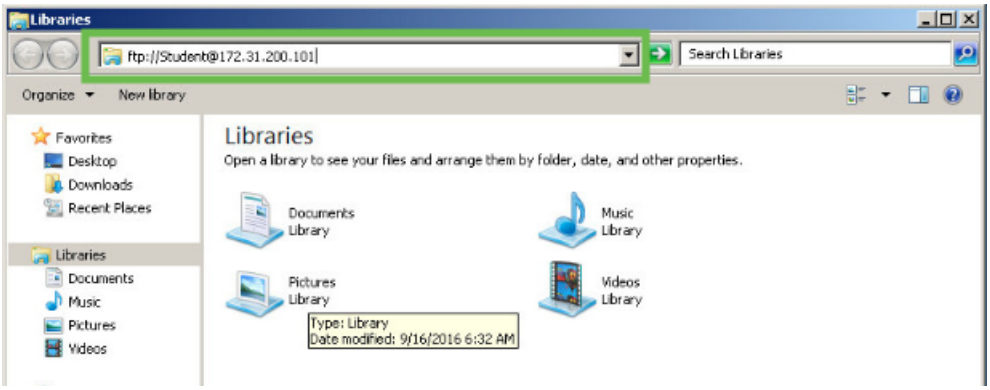


Figure 9.13: Downloading the ECA Configuration

7. When prompted, enter `Forcepoint1!` as the password
8. Browse to the **Desktop** folder. Drag and drop the ECA xml file to the Desktop of the Windows workstation. You may close the Explorer window
9. Click on the file you just downloaded and rename it **eca.conf**

   NOTE: This is a required step for any ECA deployment and is not specific to these labs
10. On the Desktop of the Windows workstation, there is a folder labeled **ForcepointOneEndpointPackage**

11. In that folder, double click on **WebsenseEndpointPackageBuilder.exe**

    NOTE: Forcepoint One Endpoint is the newest Endpoint solution that allows the administrator to incorporate all Forcepoint Endpoint agents in one installation. In the following steps we will configure the Forcepoint One Endpoint to install only the ECA Client.

12. Unselect the **Forcepoint Web Security Endpoint checkbox**

13. Once the Endpoint builder is launched, enable the checkbox for **Forcepoint Endpoint Context Agent** and click on **Next**

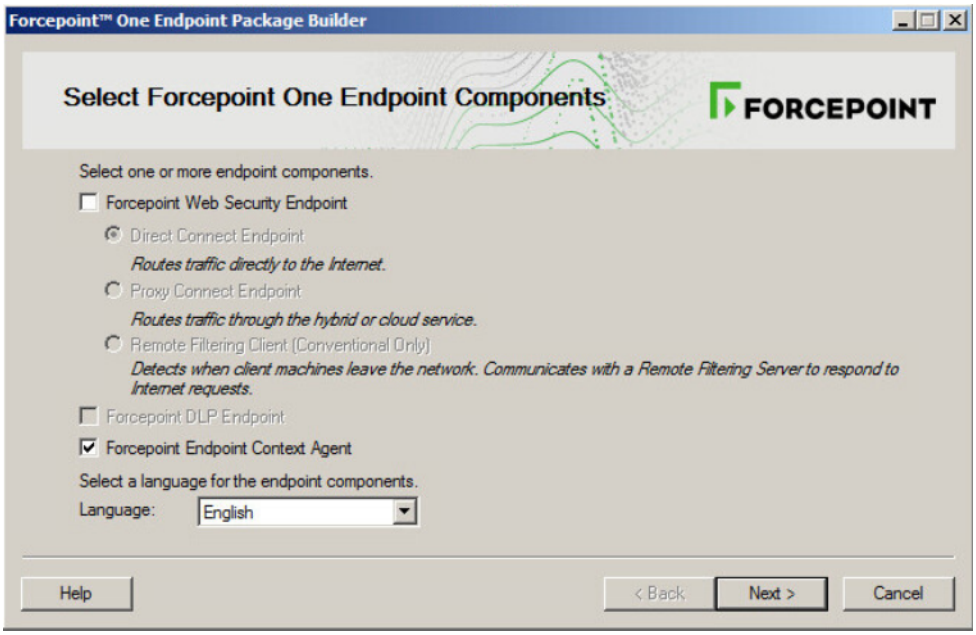


Figure 9.14: Selecting ECA in the Builder

14. In the installation settings, select **Windows 64-bit** as Operating System and provide `Forcepoint1!` as password. Leave the rest of the fields as they are. Click on **Next**.

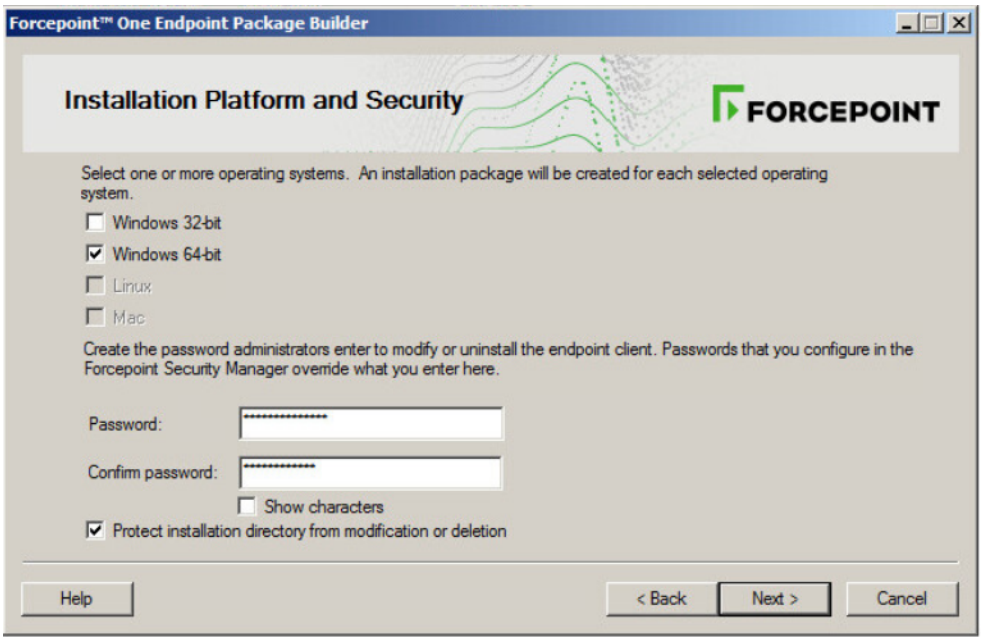


Figure 9.15: Installation settings for the ECA builder

15. In the installation Path window, select the default location and click on **Next**

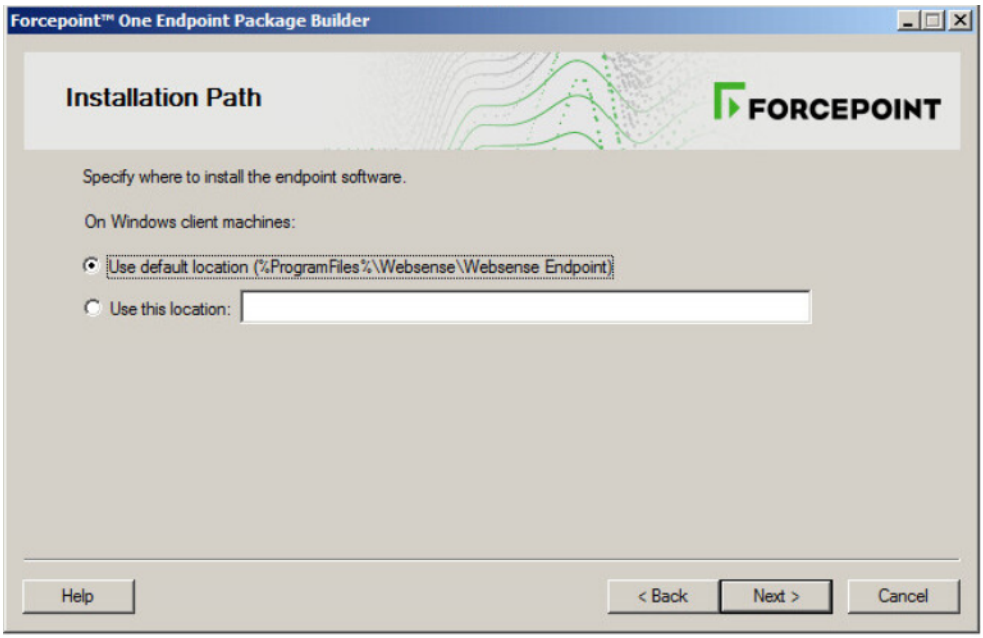


Figure 9.16: Installation Path for the ECA builder

16. In the profile Path window, click **Browse** and access the **Desktop** folder. Select the **eca.conf** file that you copied and click **Open**

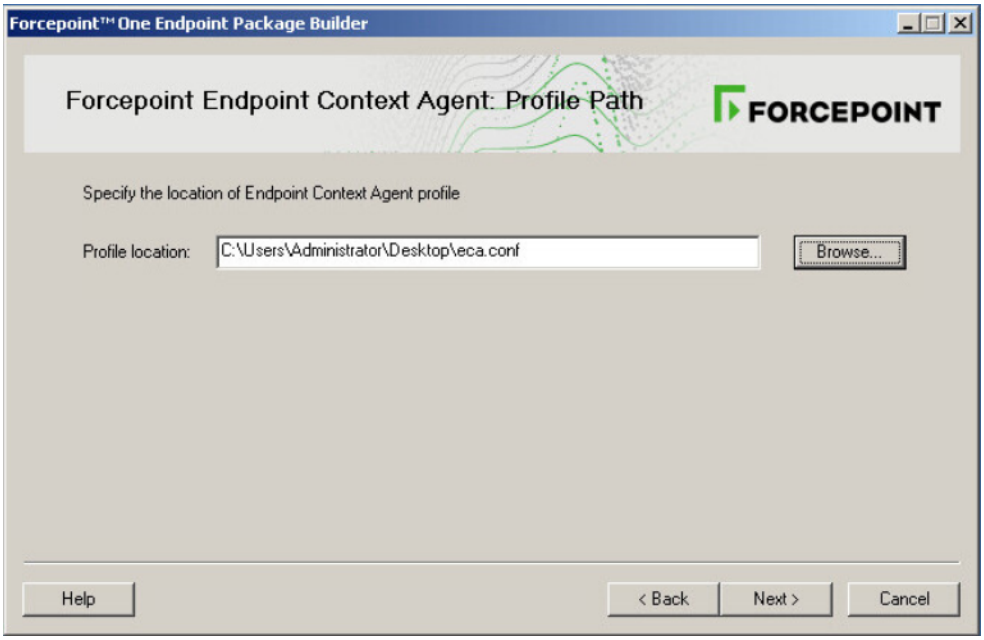


Figure 9.17: ECA conf file location

17. Click **Next**
18. Click **Browse** and select the **Desktop** as Save location. Click **OK**

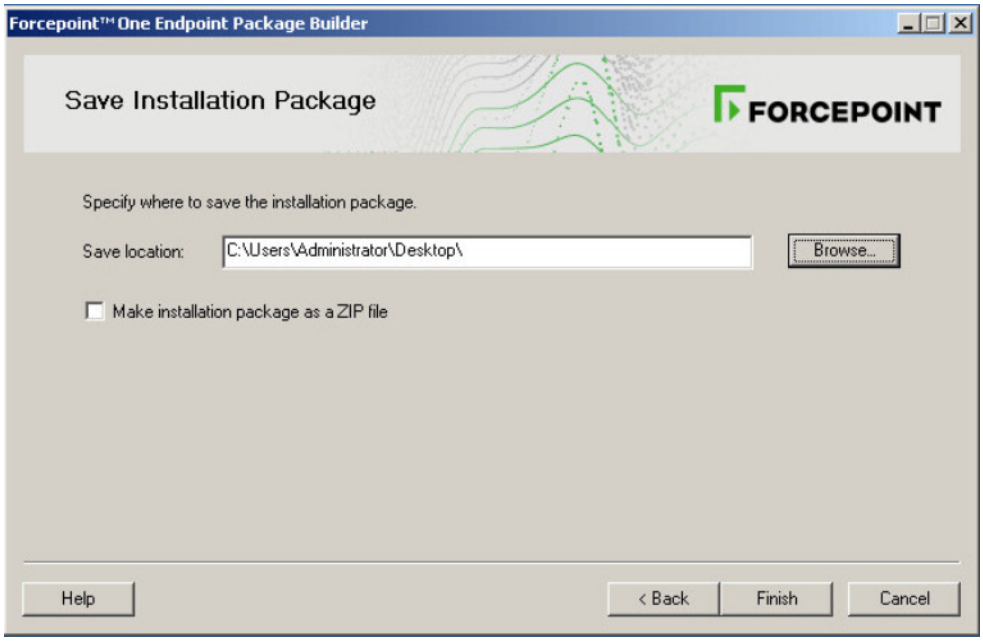


Figure 9.18: ECA builder save location

19. Click **Finish**. The installation package for ECA is created on the Desktop

20. Double-click the **FORCEPOINTONEENDPOINT-x64** installer on the Desktop. The installation begins

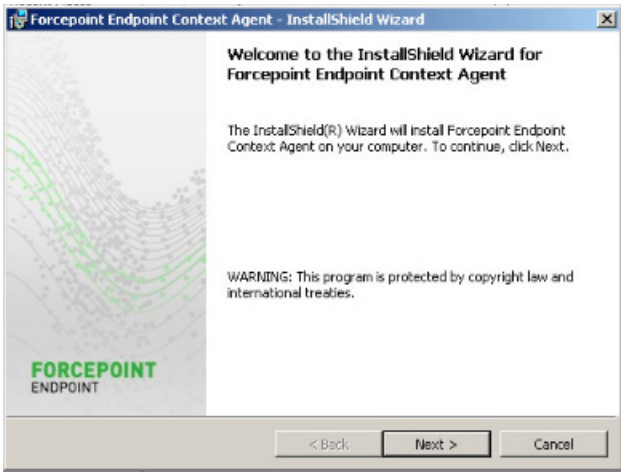


Figure 9.19: Launching the ECA Installer

21. Click **Next**
22. Accept the license agreement by selecting **I accept the terms in the subscription agreement**. Click **Next**
23. Use the default **Destination folder** and click **Next**
24. Click **Install**
25. When the installation is complete, click **Finish**
26. Wait a few moments, and click into the Task Tray, hover over the Forcepoint icon and verify that ECA agent is properly running

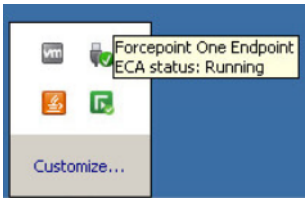


Figure 9.20: Installed and Configured ECA

27. If no Forcepoint icon appears, click **Customize** in the Task Tray and select **Always show all icons and notifications on the taskbar**. Click **OK**

Figure 9.21: Customize the Task Tray for ECA

9.5 Verify ECA Connectivity Using the Logs

In the last exercise, you were able to see that the ECA was properly configured by looking at its icon in the Task Tray. Now you will use the logs to verify that the ECA has connected to the Engine.

1. Using the **Main Menu** from the **Landing Machine**, switch back to the console window for **HQ SMC**
2. In the Management Client, right-click on the **Logs** icon on the **Menu** toolbar, and select **Open in New Tab**. The Log Browser opens
3. In the **Query Panel** on the right, use the drop-down menu and select the **Endpoint** logging context

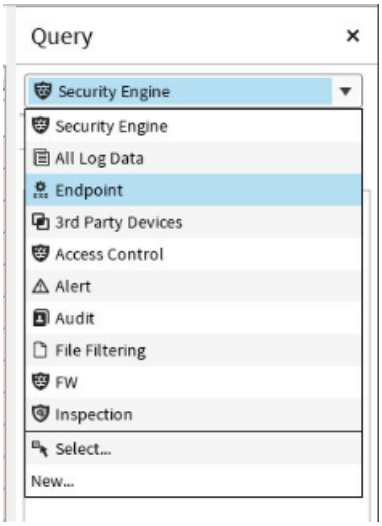


Figure 9.22: Endpoint Logging Context

4. Click **Apply**

5. Scroll through the logs and locate the **ECA_Metadata_Connected**

Figure 9.23: Endpoint Metadata Received

9.6 Blocking Internet Explorer on the Endpoint

Now that the ECA is configured and it has established contact with the Engine, you can now write rules to block users from accessing services, network applications, and the use of programs running on the endpoint. In this exercise, you will write a rule that blocks a user from using Internet Explorer. This exercise will combine User Identification and endpoint application control in the same rule.

9.6.1 Adjust the Logging in the HQ Policy for ECA

ECA is now connected, which means that you can start logging user activity and endpoint applications. To do this, you will first need to enable some additional logging in the HQ Policy.

1. From the **Home** view, right-click on the **Helsinki-HQ FW** and select **Current Policy** → **Edit**. The Policy Editor opens
2. Right-click in the **ID** column of the first rule and select **Add Rule Before**. A new empty rule appears
3. Configure the new rule as follows:
    - **Source**: Right-click and set to **ANY**
    - **Destination**: Right-click and set to **ANY**
    - **Service**: Right-click and set to **ANY**
    - **Action**: Right-click and select **Continue**
4. Right-click in the **Logging** cell and select **Edit Logging**. The Logging - Select Rule Options dialog box opens
5. Check the box next to **Override Recording Settings Inherited from Continue Rule(s)**
6. Configure the logging as follows:
    - **Log Level**: Stored
    - **Log User Information**: Enforced
    - **Log Network Applications**: Enforced
    - **Log URL Categories**: Default
    - **Log Endpoint Information**: Enforced
7. Click **OK**. Your adjusted logging options should appear as in the figure below:

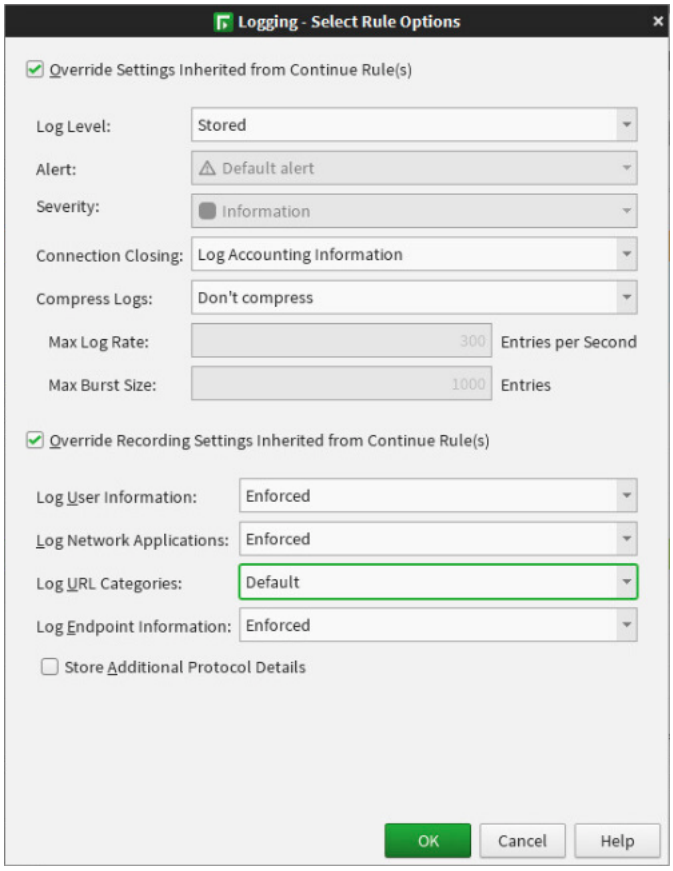


Figure 9.24: Adjusted Logging Options for Endpoint Information

9.6.2 Create a Rule to Block Internet Explorer on the Endpoint

In the last section you adjusted the logging in the HQ Policy to log endpoint information. You did not change the Global Firewall Template because ECA is only being used by the Helsinki-HQ FW. As the logging has been adjusted to log endpoint information, you can now create the rule that blocks Internet Explorer on the endpoint and view it in the log browser.

1. In the tab where the **HQ Policy** is open for editing, right-click in the **ID** cell of the last rule that permits the 172.31.200.0/24 network to the internet and select **Add Rule Before**. A new blank rule appears
2. In the **Source** cell, use the **Resources** tree on the left and browse to **Endpoint Information** → **All Endpoint Applications**
3. Type `internet`. A list of endpoint applications appears with `internet` in the name
4. Click on **Internet Explorer 10**. Hold down the **Shift** key, and click on the last instance of **Internet Explorer**

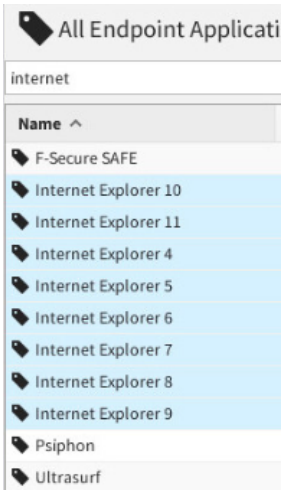


Figure 9.25: Selecting All ECA Internet Explorer Versions

5. Click on your selection and drag it into the **Source** cell
6. Drag and drop **not Helsinki Internal Networks** from the rule below into the **Destination** cell of the new rule
7. Right-click in the **Service** cell and select **HTTP** and **HTTPS**
8. Right-click in the **Action** cell and select **Edit Options**. The Select Rule Action Options dialog box opens
9. Click on the **Response** tab and check the box for **Override Settings Inherited from Continue Rules**
10. Click **Select** next to the **User Response** field. The Select User Response dialog box opens
11. Click on **Default User Response** and click **Select**. The Select User Response dialog box closes

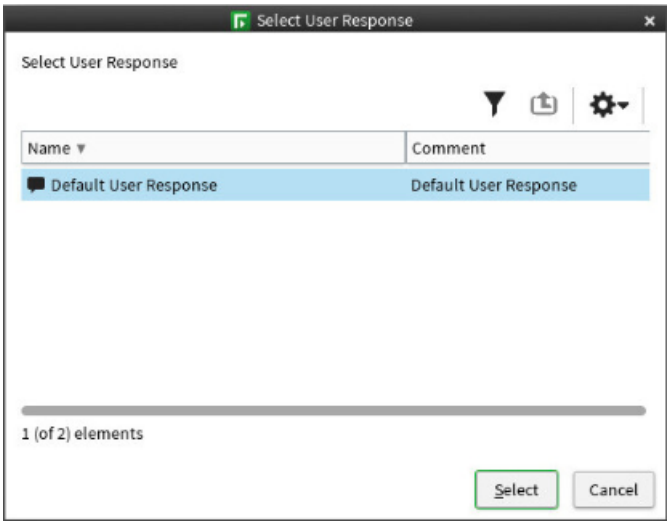


Figure 9.26: Selecting Default User Response for ECA Rule

12. Click **OK**. The Select Rule Action Options closes. Your fully configured rule to block the Internet Explorer executable on the endpoint should appear as in the figure below:

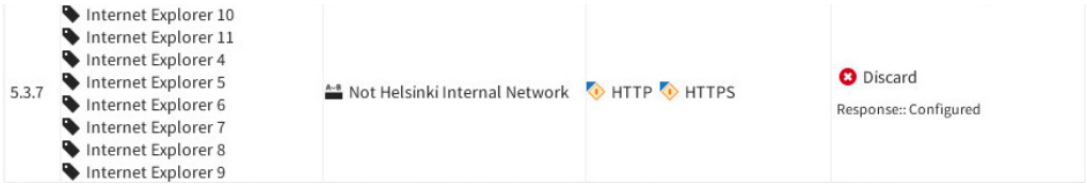


Figure 9.27: Completed Internet Explorer ECA Rule

13. Click the **Save and Install** icon. The policy upload begins

9.7 Test the ECA Rule to Block Internet Explorer

The Helsinki-HQ Firewall has now been configured with the ECA and a rule to block Internet Explorer rom running on the endpoint. In this exercise, you will use the Helsinki Workstation, where the ECA is installed, to attempt a connection to the internet using Internet Explorer.

1. Using the **Main Menu** from the **Landing Machine**, open a console to the **Helsinki Workstation** (if one is not already open)
2. Click the **Start** button, and select **Log Off**. The Administrator is logged off

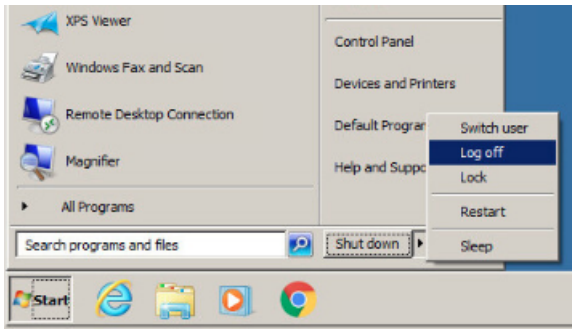


Figure 9.28: Switching Users on Helsinki Workstation

3. In the console window for **Helsinki Workstation**, click **VMRC** and select **Send Crtl+Alt+Del**
4. Click **Switch User** and then click **Other User**
5. Log in with user **Jim** and Password `Forcepoint1!`
6. In the task bar, click the **Internet Explorer**. The Internet Explorer web browser opens. You should receive the following response:

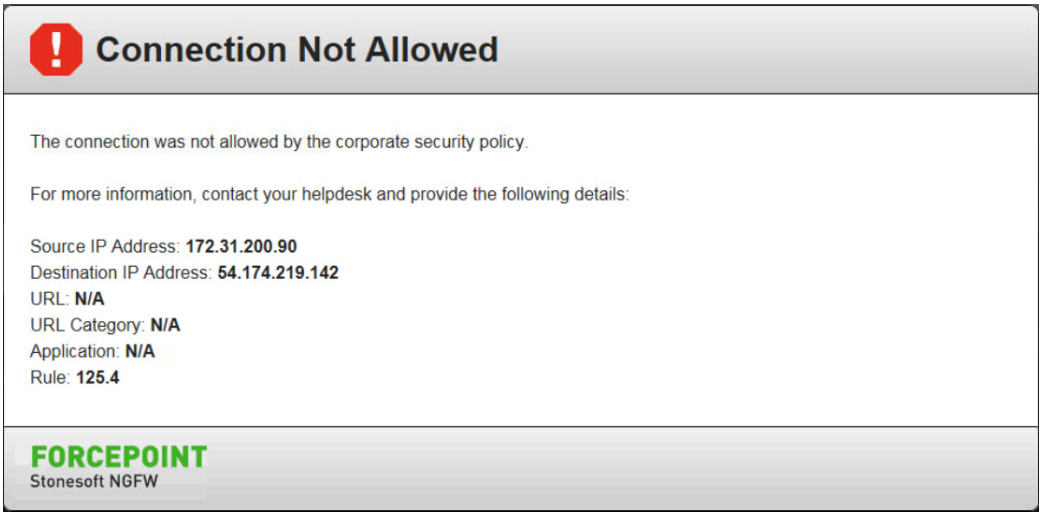


Figure 9.29: Blocked Usage of Internet Explorer

7. You may close the Internet Explorer browser window

9.7.1 Use the Logs to View the Blocked Internet Explorer Usage Attempt

You will now use the log browser to view the logs that were generated by a user's attempt to use Internet Explorer.

1. With the Logs View still open, use the drop-down menu in the **Query** panel, and select **Endpoint**

   NOTE: If the Endpoint logging context does not appear in the list, click **Select** at the bottom of the list and locate the Endpoint logging context

2. Click **Apply**. Endpoint log entries are displayed

3. Locate the **Endpoint Application** column, and verify that entries similar to the following exist:

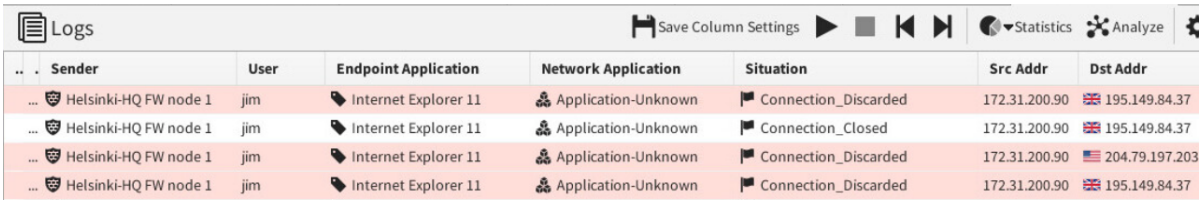


Figure 9.30: Blocked Internet Explorer Client Executable

9.7.2 Add User, Application, and Client Application Columns to Logging View

In order to view information about applications, users, and client applications in the logging view, you will use the column selection to add these columns to your logging view. You will then save these selections for future use.

1. In the **Logs** view, use the drop-down menu in the **Query** panel, and select **Security Engine**

2. Right-click on any column header and select **Column Selection**. The Column Selection dialog box opens

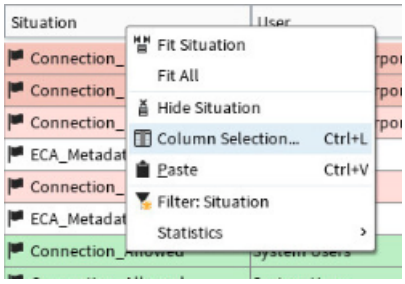


Figure 9.31: Logging Column Selection

3. On the left, click **All Fields**
4. Type `user`. Drag and drop the **User** field into the column on the right under **Situation**
5. Click the “X“ after the word **user** to clear your search

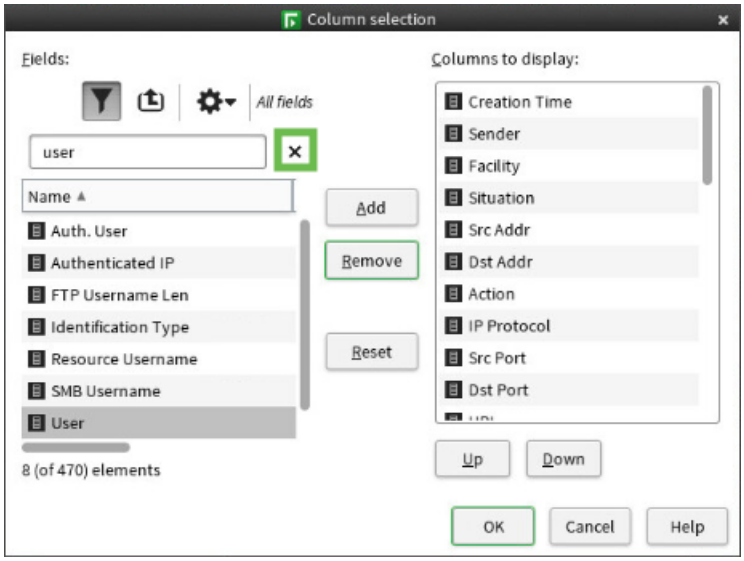


Figure 9.32: Column Selection Dialog

6. Now type `Endpoint`. Drag and drop **Endpoint Application** after **User** on the right
7. Repeat the last two steps for **Network Application**.
8. Click **OK**. Your completed logs view should appear as in the figure below:

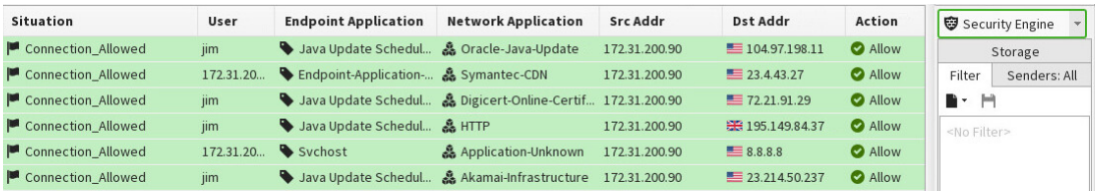


Figure 9.33: Customized Logs View

9. Click the **Save Column Settings** button to save your customized logging view

9.8 Create a Rule to Block a User from Accessing a Network Application

You have now seen that the ECA can prevent an executable on the endpoint from reaching the network. You will now use the user information provided by the ECA to block a user from accessing a network application, LinkedIn.

1. With the **HQ Policy** still open for editing, right-click in the **ID** cell of the rule that blocks the use of Internet Explorer and select **Add Rule Before**. A new empty rule is added
2. Use the **Resource** tree on the left and browse to **Users** → **helsinki.com** → **helsinki** → **Users** and drag **Jim** into the **Source** cell
3. Drag **not Helsinki Internal Networks** from the rule below into the **Destination** cell
4. Click in the **Service** cell and type `Linked` and select the **LinkedIn** network application from the list
5. Right-click in the **Action** cell and select **Discard**
6. Right-click in the **Logging** column and select **Edit Logging**. The Logging - Select Rule Options dialog box opens
7. Check **Override Settings Inherited From Continue Rule(s)**
8. Use the drop-down box and select **Stored** for the **Log Level**
9. Set **Connection Closing** to **Log Accounting Information**
10. Click **OK**. The Logging - Select Rule Options dialog box closes. Your fully configured rule should appear as in the figure below:

Figure 9.34: Blocking LinkedIn for User Jim

11. Click **Save and Install**. The policy upload begins

9.8.1 Test Access to LinkedIn from the Helsinki Workstation

1. Switch back to the console for the **Helsinki Workstation**
2. Click the **Google Chrome** icon in the task bar. Google Chrome opens
3. In the URL bar, enter `http://www.linkedin.com`. Access is blocked

9.8.2 Use the Logs to Verify Blocked Access to LinkedIn

1. Switch back to the **HQ SMC** console where the log browser is still open
2. In the **Query** panel, use the drop-down menu to select the **Security Engine** logging context. Click **Apply**
3. Right-click on the column header for **Network Application** and select **Filter: Network Application**. The Filter Properties opens
4. Click in the empty pane and type `LinkedIn`. Double-click the LinkedIn network application from the list

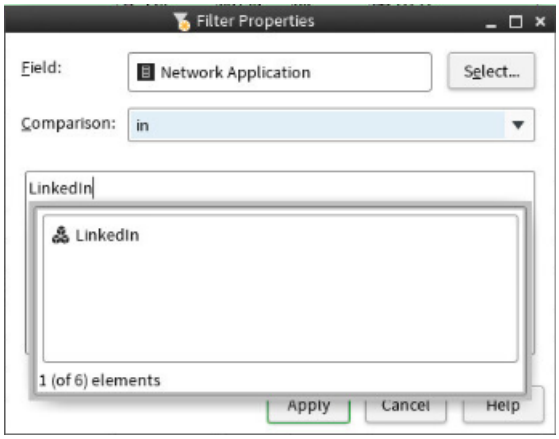


Figure 9.35: Creating a Network Application Filter

5. Double-click on the ebay network application. Click **Apply**. The Filter Properties closes
6. Click **Apply** in the **Query** panel. A list of matching connections is displayed. Your view should appear as in the figure below:

Situation	User	Endpoint Application	Network Appl...	Src Addr	Dst Addr	Action
Connection_Allowed	jim	Google Chrome	Google	172.31.200.90	172.217.1.238	Allow
Connection_Discarded	jim	Google Chrome	LinkedIn	172.31.200.90	108.174.10.10	Discard
Connection_Discarded	jim	Google Chrome	LinkedIn	172.31.200.90	108.174.10.10	Discard
Connection_Discarded	jim	Google Chrome	LinkedIn	172.31.200.90	108.174.10.10	Discard

Figure 9.36: Log Entries for Blocked LinkedIn Access Attempts

Summary

In this lab you have integrated Active Directory with the SMC to provide visibility into user activity as well a information about executables running on the endpoint. You have seen how to configure rules to user identity information and information obtained from the ECA to make access control decisions. As an extension of the exercises you performed in this lab, you now have the information from Active Directory that will be used in the next lab to authenticate mobile VPN users.

LAB 10

Mobile VPN

10.1 Getting Started

Remote users need to connect securely to the corporate network. This requires robust encryption and reliable user authentication methods to prevent unauthorized access to corporate resources. The Forcepoint VPN Client offers remote users access to corporate networks through a native Windows Graphical User Interface. Once installed on a laptop or desktop computer, the Forcepoint VPN Client software receives its settings in a configuration file it downloads from the VPN gateway. This way, Mobile VPN connections automatically comply with the corporate security policy and users do not have to change any settings when changes are made in the VPN gateway's configuration.

10.2 Create an Address Range Element

A new address range element is needed to define the range of IP addresses that the DHCP server assigns to VPN Clients so that the addresses can be entered into the VPN gateway's configuration.

1. Click the tab where the **Configuration** view is open. If necessary you can open a new Configuration view by clicking the Configuration icon in the menu bar.
2. Browse to **Network Elements** → **Address Ranges** and select **New Address Range**. The **Address Range Properties** dialog box opens

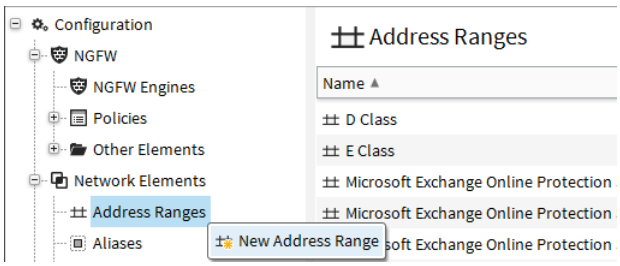


Figure 10.1: Address Range Properties

3. Define the following properties:
   - **Name**: Helsinki mVPN DHCP range
   - **IP Range**: 172.31.200.30 - 172.31.200.40

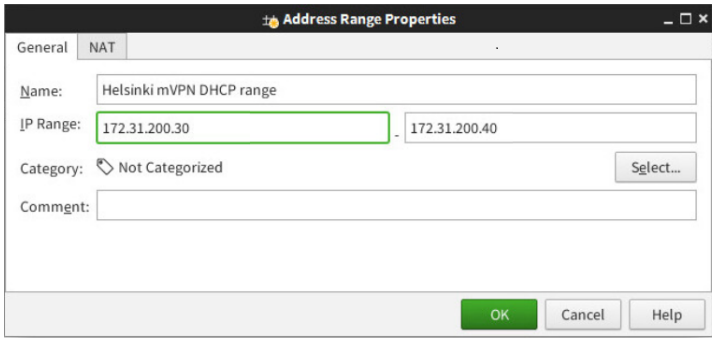


Figure 10.2: Helsinki DHCP Range Properties

4. Click **OK**.

10.3 Configure the DHCP Server

In this section we will configure the Helsinki-HQ FW to provide DHCP services from its internal Interface. DHCP server is important because it will be used to provide Virtual IP addresses to the Mobile VPN clients.

1. Click the **Helsinki-HQ FW (EDIT)** tab where the **Helsinki-HQ FW**is open for editing
2. Browse to **Interfaces**, right-click **Interface 0** and select **Edit Interface Properties**
3. In the Interface properties select the **DHCPv4** tab and in the **DHCP Mode** drop-down list, select **DHCPv4 Server**
4. Configure the internal DHCP server as such:
    - **DHCP Address range:** click on Select and pick the **Helsinki mVPN DHCP Range**
    - **Primary DNS Server:** Type 172.31.200.105
    - **Default Gateway:** Type 172.31.200.1
    - click **OK**

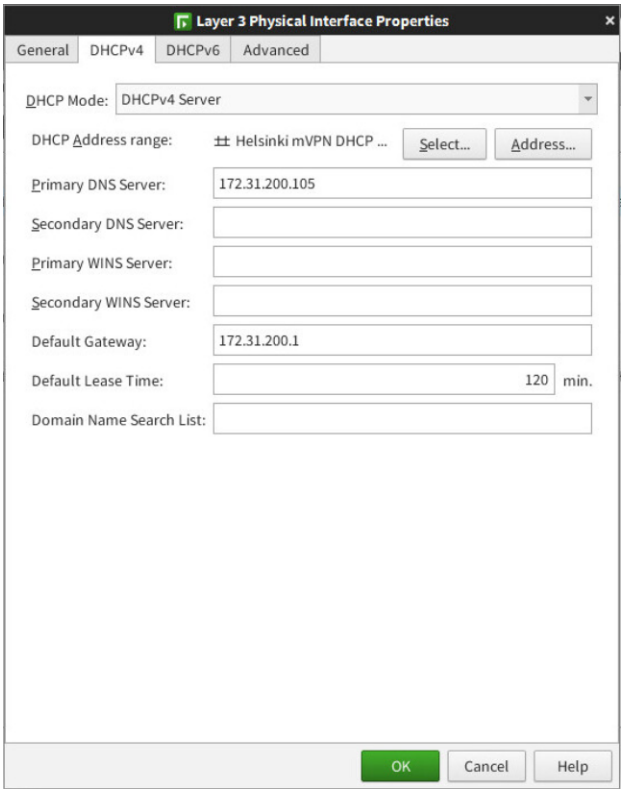


Figure 10.3: Internal DHCP Server

5. Click the **Save** icon to save the engine settings.

10.4 Configure VPN Client Address Management

DHCP for Virtual IP addresses is defined in the NGFW Engine properties in the VPN Client section. The range of IP addresses that the DHCP server assigns to VPN Clients can be entered in the Virtual IP Address configuration.

1. In the same **Helsinki-HQ FW (EDIT)** tab where the **Helsinki-HQ FW**is open for editing
2. Browse to **VPN** → **VPN Client**
3. From the **VPN Type** drop-down list, select **IPsec VPN**
4. In the **Virtual Address** pane, select **Direct** from the **DHCP Mode** drop-down list
5. In the **Interface for DHCP Relay** field, make sure that **Interface 0** is selected
6. Select **Restrict Virtual Address Ranges** and enter the following IP address range:
   - **172.31.200.30 - 172.31.200.40**
7. Select Proxy ARP and enter the following IP address range:
   - **172.31.200.30 - 172.31.200.40**

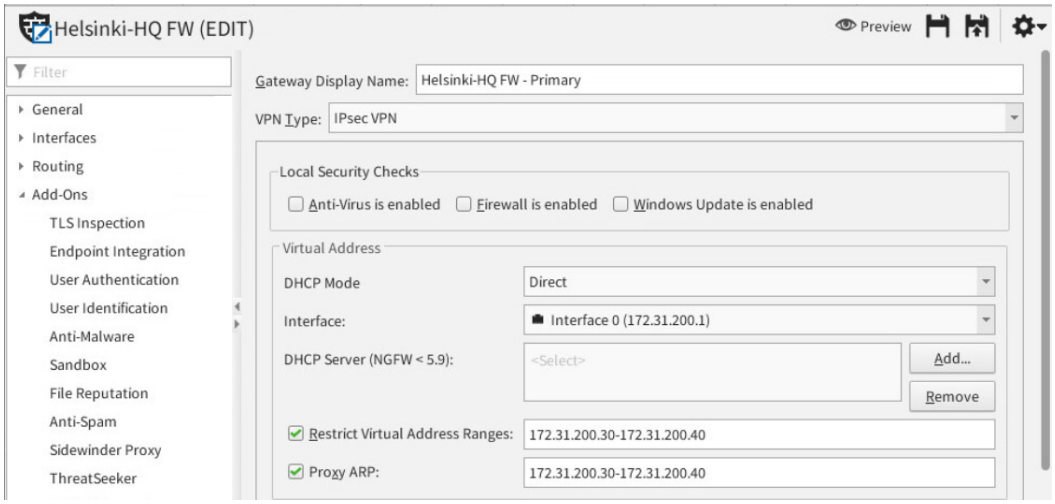


Figure 10.4: Restrict Virtual Address Ranges

8. Click **Save**

10.5 Configure the Mobile VPN

Next, you will add VPN Client access to a new Mobile VPN.

1. Click the tab where the **Configuration** view is open
2. Browse to **SD-WAN** → **Policy Based VPNs**
3. Right-click **Policy Based VPNs** and select **New Policy-Based VPN**. The **VPN Properties** dialog box opens
4. In the **Name** field, enter **Helsinki-HQ Mobile VPN**
5. Select **VPN-A Suite** as the **Default VPN Profile**

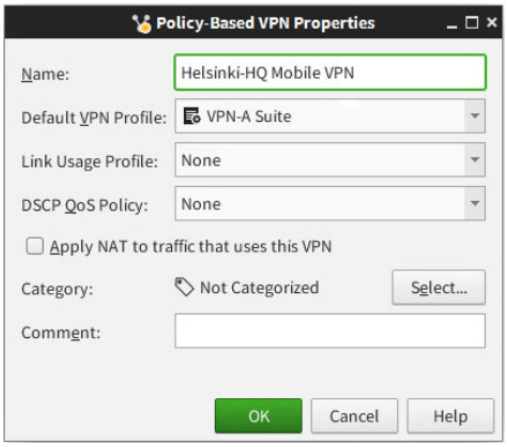


Figure 10.5: Helsinki-HQ Mobile VPN Properties

6. Click **OK**. The VPN opens for editing in a new tab
7. Click the **Mobile VPN** tab
8. From the **Select the engine that provides Mobile VPN Access** drop-down list, select **Select Gateways below**

9. Drag and drop **Helsinki-HQ FW - Primary** to **Mobile VPN Gateways**

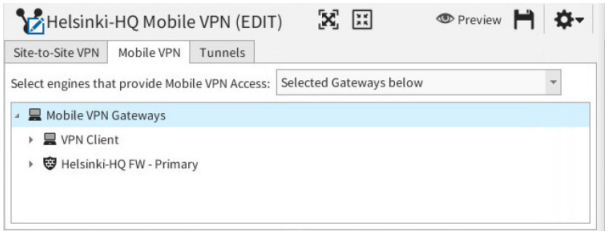


Figure 10.6: Mobile VPN Gateways

10. Click the tab where the **Tunnels** tab. The tunnel between the **Helsinki-HQ VPN Gateway** and any VPN Clients has been added to the list of tunnels

11. Click the **Gateway** <-> **Gateway** tunnel between **VPN Client** and **Helsinki-HQ FW – Primary** to view the associated **Endpoint** <-> **Endpoint** tunnels

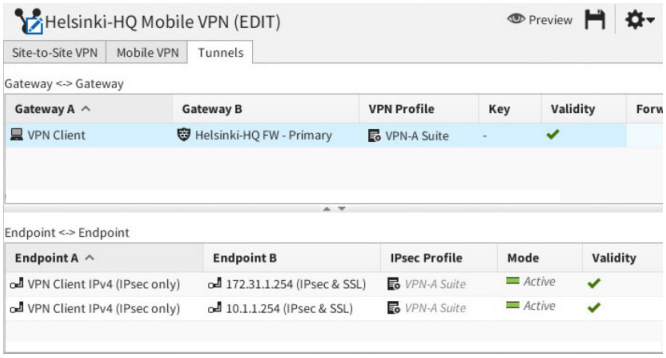


Figure 10.7: Endpoint to Endpoint Tunnels

12. In the **Gateway** <-> **Gateway** table, right-click **VPN-A Suite** and select **Properties**. The VPN A Suite Profile Properties dialog box opens

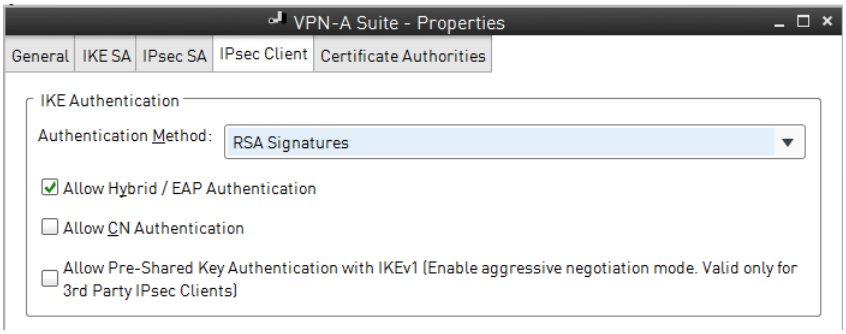


Figure 10.8: New VPN Profile Properties

13. Click the **IPsec Client** tab and select **Allow Hybrid/EAP Authentication**. This allows VPN Client users to authenticate with a password. Click **OK**

14. Click the **Save** icon

15. Close the **Helsinki-HQ Mobile VPN (EDIT)** tab

10.6 Add a Mobile VPN Access Rule

You must now add access rules that will allow Mobile VPN users to connect.

1. If the **HQ Policy** is not open for editing in another tab, from the **Home** view, right-click on the **Helsinki-HQ FW** and select **Current Policy** → **Edit**. The HQ Policy opens for editing
2. Right-click in the **ID** cell of the first rule, and select **Add Rule After**. A new empty rule appears
   - **Source**: **Helskinki mVPN DHCP Range** from **Network Elements** → **Address Ranges** in the **Resources** list
   - **Destination**: type `172.31.200.0` and select **network-172.31.200/24**
   - **Service**: ANY
3. **Action**: right-click in the **Action** cell, and select **Allow**.
4. Then right-click in the **Action** cell and select **Edit Options**. The Select Rule Action Options dialog box opens.
5. In the **VPN Action** field, select **Enforce VPN**
6. In the **VPN** field, select the **Helsinki-HQ Mobile VPN** element.
7. Click **OK**. The Select Rule Action Options dialog box closes

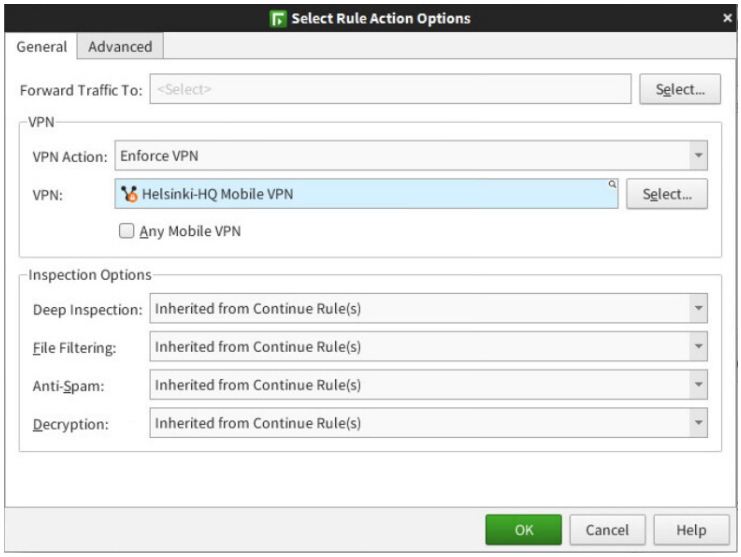


Figure 10.9: Enforcing Mobile VPN

10.7 Define Authentication Options for the Mobile VPN Access Rule

1. Double-click the **Authentication** cell. The Authentication Parameters dialog box opens

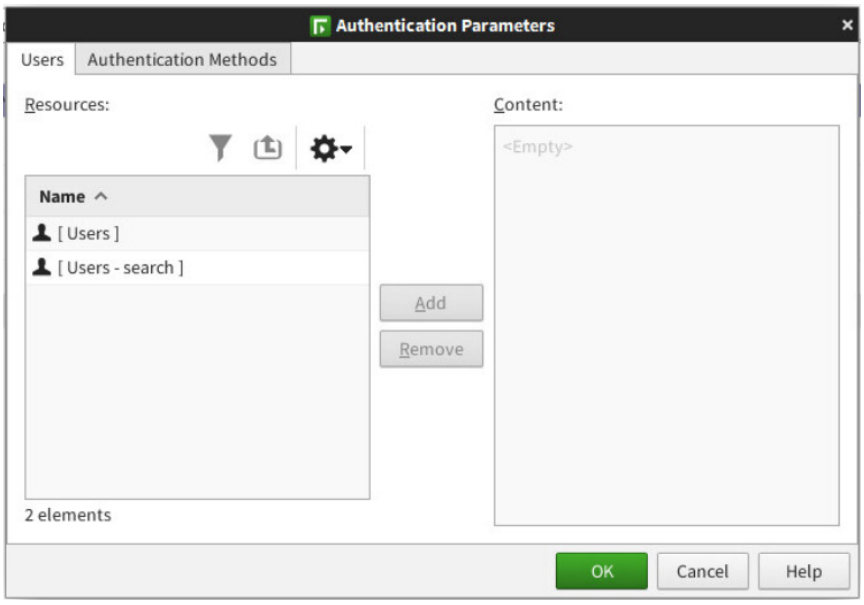


Figure 10.10: Authentication Parameters Dialog

2. Browse to **Users** → **helsinki.com** → **helsinki**
3. Select the **Users** group and click **Add**
4. Click the **Authentication Methods** tab

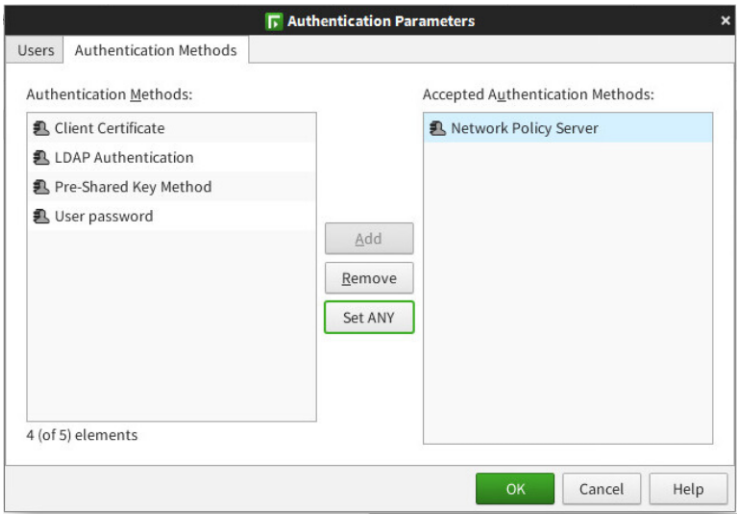


Figure 10.11: Authentication Methods Tab

5. Select **Network Policy Server** and click **Add**
6. Click **OK**. The completed Access Rules should look as in the figure below:

Figure 10.12: Completed Authentication Access Rule

7. Click the **Save and install** button. The HQ Policy uploads
8. Close the **Upload Policy: HQ Policy** tab when the policy upload is completed

10.8 Install the Forcepoint VPN Client

Next, you will install the VPN Client software to test the Mobile VPN connections. This software is located on the Remote Workstation.

1. Using the **Main Menu** from the **Landing Machine**, open a console to **Remote Workstation**
2. Select the user **Student** to Log in
3. At the password prompt, `Forcepoint1!`
4. Once logged in Click the **Folder** icon on the Start Bar and browse to **Downloads**
5. Double-click the **Forcepoint-VPN-Client-6.6.0.6605.exe** installer to begin the installation

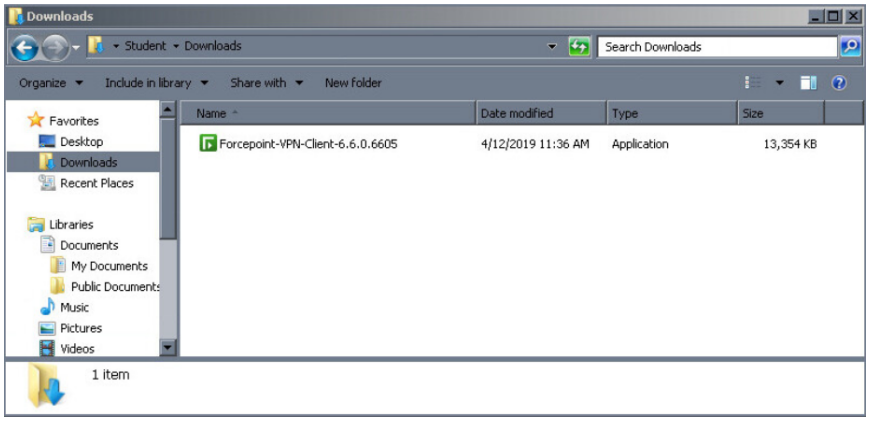


Figure 10.13: VPN Client Installer

6. Select **Run**

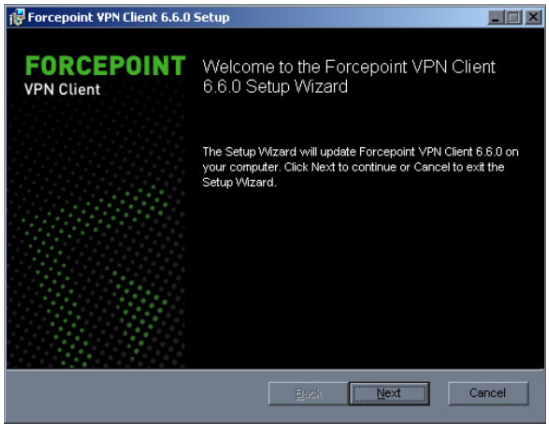


Figure 10.14: Running the VPN Client Installer

7. click **Install**
8. Select **I accept the terms in the license agreement**. Click **Next**
9. Click **Install**. The installation begins
10. Click **Close**

After the installation is complete, the Forcepoint VPN Client icon appears in the Notification area of the Windows taskbar.

10.9 Launch the Forcepoint VPN Client and connect to a New Gateway

1. Right-click the **Forcepoint VPN Client** icon in Notification area of the Windows taskbar and select **Properties**. The Forcepoint VPN Client Properties opens

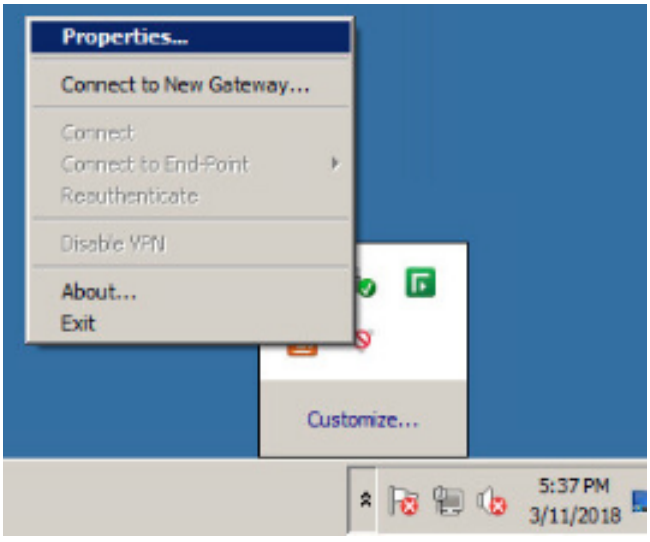


Figure 10.15: Connecting to a New Gateway

2. Click on **Connect to New Gateway**

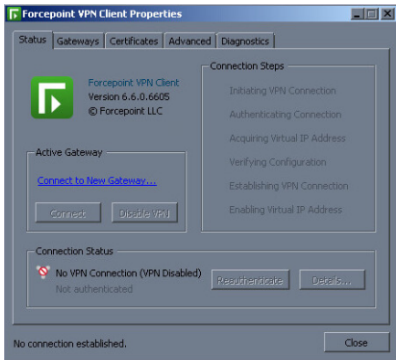


Figure 10.16: Connecting to a New VPN Gateway

3. Verify that **IPsec** is selected in the **Protocol** definition
4. Enter **172.31.1.254** as the **Host Name**
5. Leave **User Name** as Authentication method and click **OK**

Figure 10.17: New Gateway Properties

item Click **OK** to accept the firewall's certificate fingerprint and contact the VPN gateway. The **User Authentication** dialog box opens

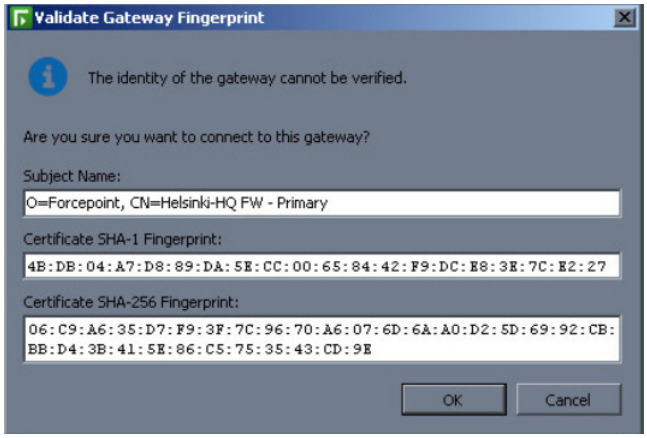


Figure 10.18: Accepting Firewall's VPN Certificate

6. Enter the following credentials:
   - **User**: bill
   - **Password**: Pass1234

   NOTE: The user, bill, comes from Active Directory. The firewall is using the interface that you selected for "Source for Authentication Requests" in the interface options and contacting Active Directory over the Policy-Based VPN you configured earlier. The firewall then communicates with the Network Policy Server installed on Active Directory to authenticate the user.
7. After entering the user name and password, the client authenticates and receives an address from the Helsinki DHCP Server. Your successful connection should appear as in the figure below:

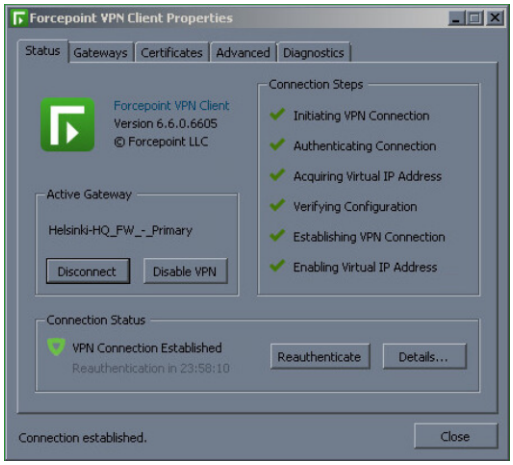


Figure 10.19: Successful VPN Client Connection

8. Select **Public network** in the Windows Set Network Location dialog and click close.

10.10 Test the VPN Client

Now that you have authenticated to the VPN, you should be able to access resources at your site. You will test this by trying to access your site's Web page.

1. Open **Google Chrome** and enter the internal IP address of the Helsinki Web Server, `http://172.31.200.101`
2. When you are done testing, **disconnect** and close the VPN from the **Status** tab because you will not need to be connected to the VPN for future labs

10.11 Summary

During this lab, you have configured secure remote access to your network using the Forcepoint VPN Client. This included the configuration of a Mobile VPN and authentication for VPN Client users, and installation of the VPN Client.

LAB 11

Using Siderwinder Proxies

Getting Started

Part of the Forcepoint NGFW's ability to deep inspect traffic is its ability to transparently proxy traffic. A proxy "intercepts" a connection and opens a new connection of the same type to the same destination. In this way, it is acting as a proxy on behalf of the original requester. This gives the firewall the ability to tightly control what happens in a given connection. Proxies are generally explicit or transparent. Explicit proxies require the client to specifically configure traffic to be sent to the address of the proxy. On the other hand, transparent proxies do not. The traffic is proxied by a firewall, for example, transparently. No configuration on the level of the client is required.

In this lab, you will configure the HTTP proxy to silently proxy HTTP traffic, while controlling specific parts of the connection. One attack type that can be easily prevented with the HTTP proxy is unicode-based attacks. To prevent these, you will create an HTTP proxy service and disallow unicode in URLs.

11.1 Enable SSM Proxies in the Engine Properties

In order to use the SSM Proxy modules with the firewall, they have to be enabled in the engine properties. In this exercise, you will edit the Atlanta FW Cluster and enable the use of the proxy modules.

1. From the **Home** view, right-click on the **Atlanta FW Cluster** and select **Edit Firewall Cluster Atlanta FW Cluster**. The Atlanta FW Cluster properties open for editing
2. Expand **Add-Ons** and click on **Sidewinder Proxies**
3. Select **Enable**
4. Click the **Save** icon to save the changes to the firewall configuration

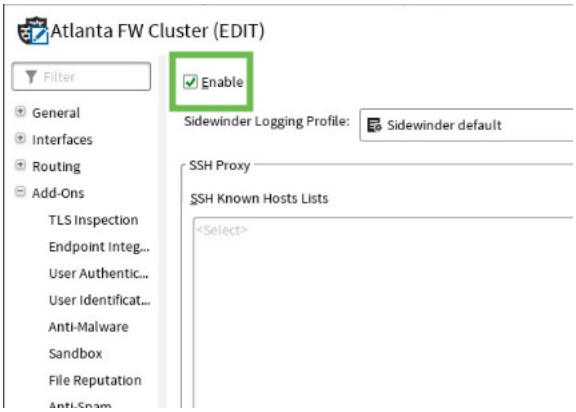


Figure 11.1: Enabling the SSM Proxies in the Engine Properties

5. You may close the tab where the engine is open for editing

11.2 Create a Custom SSM HTTP Proxy Service

In this exercise, you will create a custom SSM HTTP Proxy element that prevents the use of unicode in a URL.

1. In the tab where your **Atlanta Policy** is open for editing, switch to the **IPv4 Access Rules** tab
2. In the **Resources** panel, browse to **Services** → **With Proxy**
3. Right-click on **SSM HTTP** and browse to **New** → **Duplicate**. The TCP Service Properties dialog box opens
4. In the **Name** field, enter **SSM HTTP Atlanta**. Click on the **Protocol Parameters** tab
5. The following should be checked:
   - **Log URLs**
   - **Request Validation**
6. Expand **URL Control Options**. The following should be selected:
   - **Disallow Unicode URL Queries**
   - Use the drop-down menu and select **Block and Log** for **URL Normalization Validation**
   - Leave **Require HTTP Version**
   - **Allow HTTP Version 1.0**
   - **Allow HTTP Version 1.1**
7. Click **OK**. Your completed custom SSM HTTP Proxy Service should appear as in the figure below:

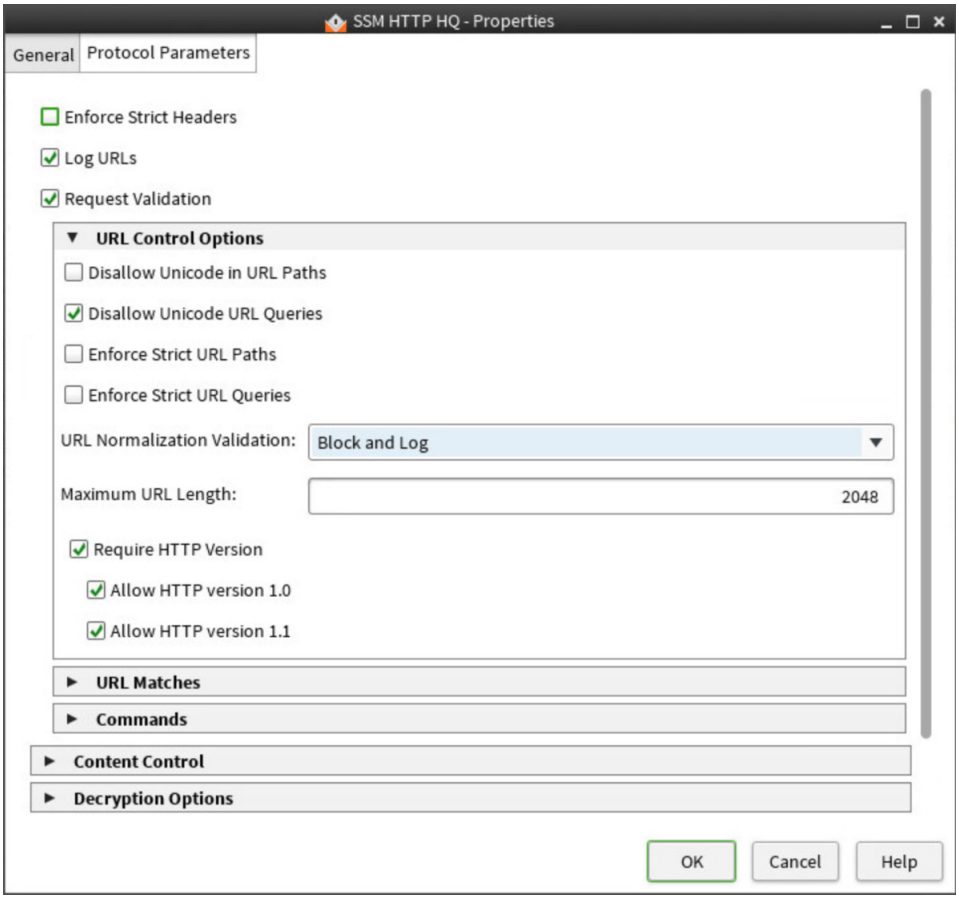


Figure 11.2: Completed Custom SSM HTTP Proxy

11.3 Create a Rule to Proxy HTTP

1. Right-click in the **ID** cell of the last rule, and select **Copy Rule**
2. Right-click in the **ID** cell of the same rule, and select **Paste**. A copy of the last rule is added. Make sure the rule is added before the last rule.
3. Click in the **Service** cell of the first two identical rules
4. Browse to **Services** → **With Proxy**
5. Drag and drop your **SSM HTTP Atlanta** element into the **Service** cell
6. Click **Save and Install**. Your completed SSM Proxy rule should appear as in the figure below:

Figure 11.3: Completed SSM HTTP Proxy Rule

11.4 Test the SSM HTTP Proxy with Unicode in a URL

To avoid the possibility that someone could use a Unicode attack in a URL, you will test the new proxy to ensure that Unicode is detected and dropped.

1. From the **Home** view, right-click the **Atlanta FW Cluster** and browse to **Monitoring** → **Logs by Sender**. The log browser opens
2. Click the **Current Events** icon (play button)
3. Using the **Main Menu** from the **Landing Machine**, open a console to the **Atlanta-Server**
4. Double-click the **Terminal** icon on the desktop. A Terminal window opens
5. At the command prompt, type `./unicode-url` and press **Enter**

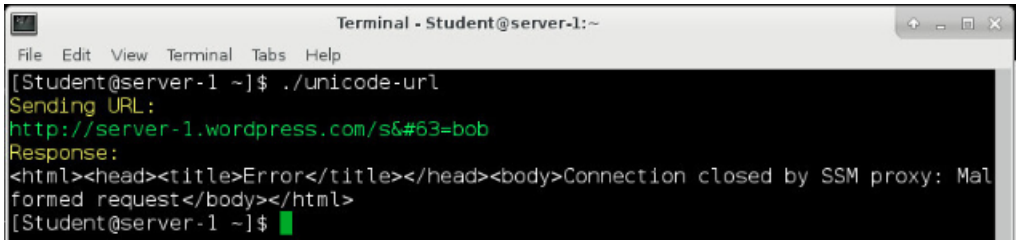


Figure 11.4: Using Curl to Encode a URL

NOTE: When this script runs, curl (a command line tool for posting information to a web server) is used to post the data portion (the part after the last slash in the URL) of the URL to the web server in a unicode format. Using a web browser would not yield the same result because web browsers interpret unicode literally.

6. Return to the Management Client and view the logs. You should see a log entry similar to the figure below:

a FW Cluster node 1	SSM Proxy	HTTP_Request-Line-Unparseable	Terminate	192.168.2.101	172.31.1.101		SSM HTTP
a FW Cluster node 1	SSM Proxy	HTTP_URL-Logged		192.168.2.101	172.31.1.101	http://server-1.wordpress.com/	SSM HTTP

Figure 11.5: Blocked Unicode in a URL

Summary

In this lab, you have created a proxy rule that ensures that Unicode is not embedded in a URL that could cause harm to your network. This proxy is transparent and had no effect on traffic that was safe, according to your security policy.

LAB 12

Using Deep Inspection

12.1 Getting Started

In this lab, you will become familiar with configuring Inspection Policies and File Filtering Policy. After each section, you will test the newly created rule against network traffic.

When anomalous traffic is detected, NGFW can be configured to trigger a response for the event in addition to logging it. There are several response mechanisms available:

- Connection termination
- Traffic recording
- Traffic blacklisting
- Different alerting channels

On the other hand, we may sometimes want to customize the rules in the Inspection Policy to produce fewer log entries than what is defined in the Inspection Policy Template. This kind of customization may be needed if you have verified that a Situation that is defined to produce a log entry in the Inspection Policy Template is in fact normal traffic in your network environment and you do not need the logs for statistical analysis later on.

The File filtering Policy allows you to restrict the file types that are allowed in and out through the firewall, and to apply malware detection to files. The following malware detection methods are supported:

- McAfee GTI (Global Threat Intelligence) file reputation
- Anti-malware scan on the NGFW Engine
- Forcepoint Advanced Malware Detection (Cloud Sandbox)

In this lab, you will first enable deep inspection for all traffic on your firewall by using the Firewall Inspection Policy template and create the Inspection Policy that will be used by your Firewall Policy. You will then customize your Inspection Policy by adding the following new rules:

- Create an Inspection rule that blocks the use of old Internet Explorer versions.
- Replace the currently used Medium-Security Inspection Policy with the High-Security Inspection Policy.
- Create an Inspection rule that cleans up log entries from anonymous FTP login attempt logs that are not needed in your environment.

In the second part of the lab, you will configure a File Filtering Policy to scans files for malware using the Anti-Malware of your firewall and prevent the download of exe files through your firewall. You will then update your Firewall Policy to send traffic to the File Filtering Policy you created.

12.2 Change Firewall Template to Enable Deep Inspection

If you use the Firewall Inspection Template as the basis for your policy, deep inspection is enabled by default for all supported protocols. Otherwise, make sure that your custom template policy directs all necessary Protocols to be inspected.

You will change the Firewall Template Policy to the Training Security Inspection Policy Template. The Training Security Inspection Policy is a custom Inspection template policy. The Training Security Inspection Policy inherits from Firewall Inspection Template and consequently enables deep inspection for all supported protocols. It also contains additional access rules necessary for the labs environment to work.

When you change the Firewall Template Policy for a Policy, the Policy cannot not be in edit mode in the Policy Editor. Therefore you must first switch the Atlanta Policy to Preview mode.

1. If the **Configuration** view is not already open in another tab, from the **Home** view, right-click the **Configuration** icon in the Menu tool bar, and select **Open in New Tab**. The Configuration view opens
2. Browse to **NGFW** → **Policies** → **Firewall Policies**
3. Click on the **Global Firewall Template** and drag it on to the **Firewall Inspection Template**
4. Click **Yes** when you receive the message that the inheritancy of the policies is changing

Figure 12.1: Inheritance Change Warning

5. The policy structure should appear as in the figure below:

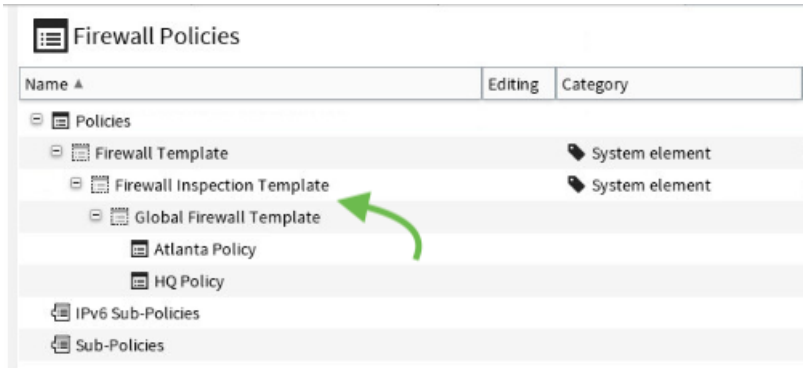


Figure 12.2: Updated Policy Structure for Firewall Inspection Template

New Inspection rules will be added to the Inspection Policy used by your Firewall Policy. The next step is to create the Inspection Policy that will be used by your Firewall Policy.

NOTE: An alternate method is to simply drag and drop your firewall policy to the Training Firewall Inspection Policy.

12.3 Create an Inspection Policy

In this exercise, you will create an Inspection Policy that inherits Inspection rules from the predefined Medium-Security Inspection Policy. In a production environment, you would directly edit the Medium-Security Inspection Policy and use the same Inspection Policy on multiple NGFW Engines. However, these lab exercises are intended to student to practice editing the Inspection

1. In the **Configuration** view, browse to **Policies** → **Inspection Policies**
2. Right-click **Inspection Policies** and select **New Inspection Policy**. The Inspection Policy Properties dialog box opens
3. Name the Inspection Policy **Atlanta Inspection Policy**
4. Browse to **Medium-Security Inspection Policy** and select it as the template for your Inspection Policy
5. Click **OK**. The **Inspection Policy** opens for editing in a new tab

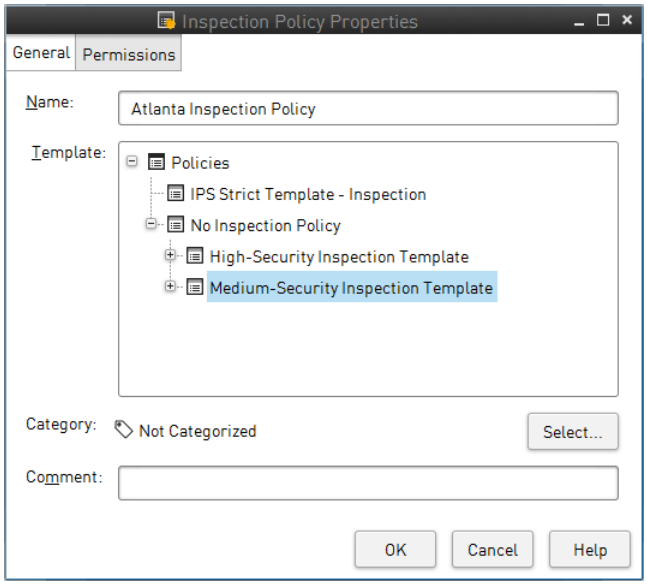


Figure 12.3: Selecting Medium Security Inspection Template

12.4 Configure an Inspection Rule to Block the Use of Old Internet Explorer Versions

You will now update your Inspection Policy and configure traffic identification rules to sends an alert and terminates the connection whenever someone uses an old version of the Internet Explorer Web browser.

1. Click the tab where **Atlanta Inspection Policy** is open for editing
2. Click the **Inspection** tab
3. Browse to **Traffic Identification** → **Browsers** → **Major Browser Versions**
4. Select the following Situations:
   - **HTTP_CSH-Internet-Explorer-2.x-Browser-Usage**
   - **HTTP_CSH-Internet-Explorer-3.x-Browser-Usage**
   - **HTTP_CSH-Internet-Explorer-4.x-Browser-Usage**
   - **HTTP_CSH-Internet-Explorer-5.x-Browser-Usage**
   - **HTTP_CSH-Internet-Explorer-6.x-Browser-Usage**

- **HTTP_CSH-Internet-Explorer-7.x-Browser-Usage**
- **HTTP_CSH-Internet-Explorer-8.x-Browser-Usage**
- **HTTP_CSH-Internet-Explorer-9.x-Browser-Usage**

NOTE: You can also start typing the Situation name and a list of matching Situations appears.

5. Right click **Edit Action** in the **Action** column. The **Select Action** dialog box opens
6. Select **Override Default Action** and set Action to **Terminate**
7. Click **OK**
8. Right click the **Logging** column and select **Edit Logging**. The **Select Logging Options** dialog box opens
9. Select **Override Default Logging Settings** and set **Log Level** to **Alert**

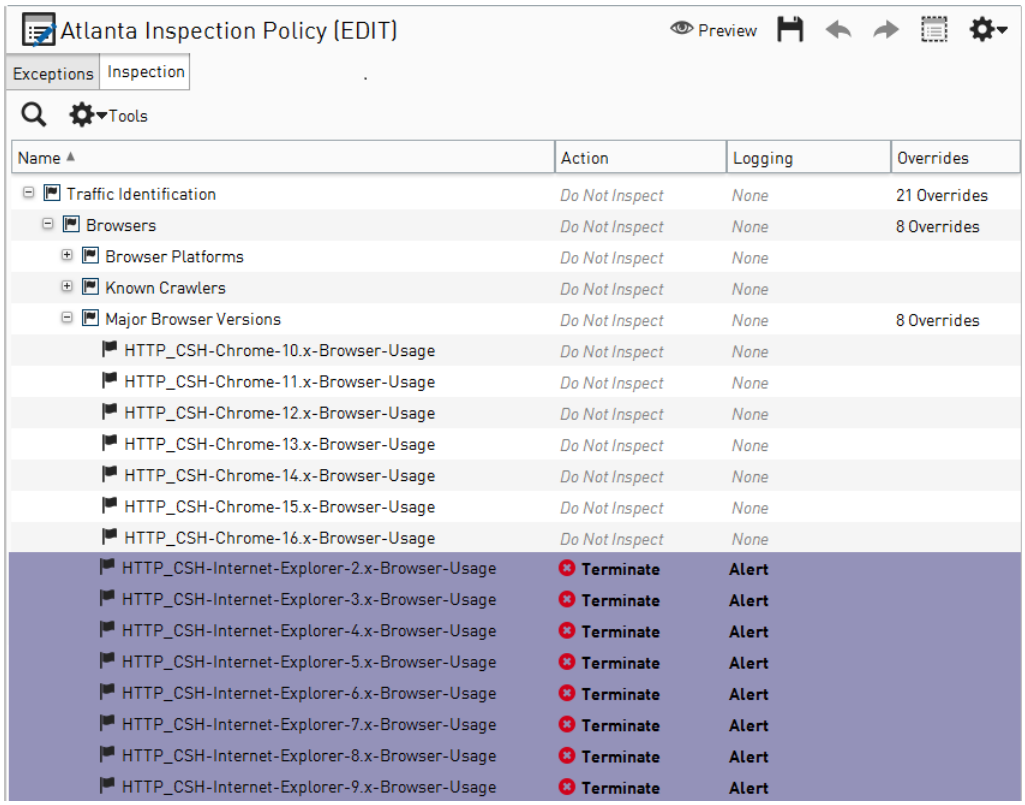


Figure 12.4: Setting IE Usage to Alert

10. Click **OK**
11. **Save** the Inspection Policy

12.5 Select the Inspection Policy in the Firewall Policy

1. Click the **Atlanta Policy** tab where the **Atlanta Policy** is open in Preview mode
2. Click the **Edit** button in the Policy toolbar
3. Click the **Inspection** tab
4. Click **Select** button for the **Inspection Policy**. The **Select Element** dialog box opens

5. Select **Atlanta Inspection Policy** and click **Select**

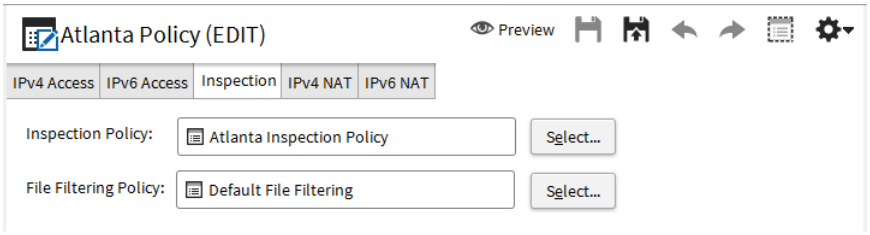


Figure 12.5: Selecting Atlanta Inspection Policy

6. Click **Save and install**
7. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

12.6 Test Internet Explorer Usage

1. Open a console to the **Master** image
2. Log on to the **Master**
   - User Name: **root**
   - Password: **Pass1234**
3. Type **cd scripts**
4. Type **./internet_explorer_traffic.sh 2**
5. Enter the following credentials to log on:
   - **Username**: `root`
   - **Password**: `Forcepoint1!`

You might see a warning message about Remote Host Identification. You can ignore that message. When this script is successful, the script will appear to "hang" after displaying "**Changing Log Levels useragent IE → 172.31.2.101**". Enter **Control-C** to kill the script when done or to retest.

Click the tab where the Logs View is open and investigate the logs for Internet Explorer Browser events. You should see that the connection matching the Situation "**HTTP_CSH-Internet-Explorer-5.x_Browser Usage**" has been terminated.

Figure 12.6: Blocked Internet Explorer Usage

12.7 Use Inspection Policy Templates

The main difference between the rules in the Medium-Security Inspection Template and the High-Security Inspection Template is in the way Inspection rules handle suspected attacks. In the High-Security Inspection Template, Suspected Attacks are terminated with an alert, whereas the Medium-Security Inspection Template only logs Suspected Attacks. You will now see how changing the template affects the handling of a Situation belonging to the Suspected Attack group.

12.8 Find Logs of Attacks

1. From the console of the **Master**, type **./openview_attack.sh 2**
2. Click the tab where the **Logs** view is open
3. Look for a log that shows a match to the Situation **HTTP_CRL-HP-OpenView-Network-Node-Manager-Ovlogin.exe-Buffer-Overflow** (see the illustration below)
4. Select the **HTTP_CRL-HP-OpenView-Network-Node-Manager-Ovlogin.exe-Buffer-Overflow** log and Click **Tool** → **Details** in the toolbar and read the information regarding the Situation In the References pane, you can see the Situation Type does this Situation belong to.
5. Click the **Record** icon in the toolbar to return to the Logs view
6. Right-click the Situation **HTTP_CRL-HP-OpenView-Network-Node-Manager-Ovlogin.exe-Buffer-Overflow** log entry and select **View Rule**

See which action is currently defined for the Situation.

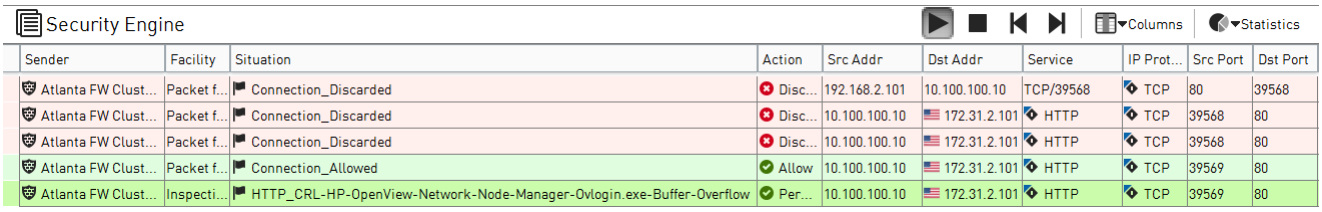


Figure 12.7: OpenView Attack Log Entry

12.9 Change the Inspection Policy Template

You will now change the Medium-Security Inspection Template to the High-Security Inspection Template and see if the Situation **HTTP_CRL-HP-OpenView-Network-Node-Manager-Ovlogin.exe-Buffer-Overflow** is handled in a different way.

1. Click the tab where **Atlanta Inspection Policy** is open for editing
2. Click **Preview** in the Policy toolbar
3. Click the tab where the **Configuration** view is open
4. Browse to **NGFW** → **Policies** → **Inspection Policies** → **Medium-Security Inspection Template** → **Atlanta Inspection Policy**
5. Right-click **Atlanta Inspection Policy** and select **Properties**
6. Click **High-Security Inspection Template** to change the template for your policy
7. Click **OK**

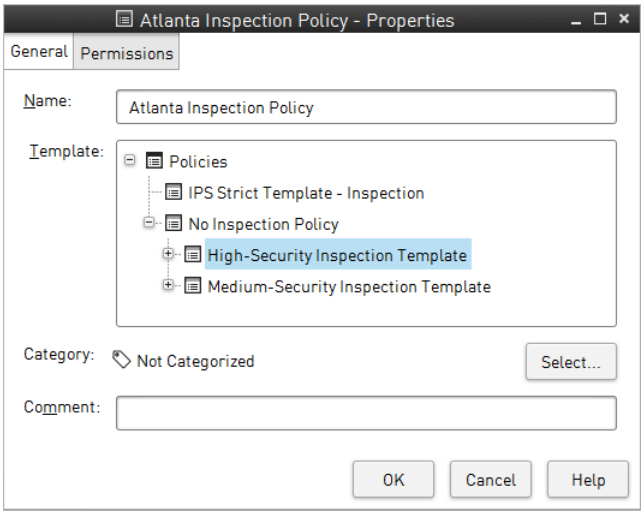


Figure 12.8: Switching to High Security Inspection Template

8. Browse to **Policies** → **Firewall Policies**
9. Right-click **Atlanta Policy** and select **Install Policy**
10. Make sure that **Atlanta** is selected as Target and click **OK** to install the policy
11. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

12.10 Test the High-Security Inspection Template

1. From the console of the **Master**, launch the **openview_attack.sh 2** script again
2. Click the tab where the **Logs** view is open and look for the Situation **HTTP_CRL-HP-OpenView-Network-Node-Manager-Ovlogin.exe-Buffer-Overflow** again
3. How is the Situation handled with the High-Security Inspection Template?

Atlanta FW Clust...	Packet f...	Connection_Allowed	Allow	10.100.100.10	172.31.2.101	HTTP	TCP
Atlanta FW Clust...	Inspecti...	HTTP_CRL-HP-OpenView-Network-Node-Manager-Ovlogin.exe-Buffer-Overflow	Ter...	10.100.100.10	172.31.2.101	HTTP	TCP

Figure 12.9: OpenView Attack Blocked Log Entry

12.11 Customize Logging

NGFW provides information on network traffic by logging events that are of interest in our network environment. It alerts administrators about suspicious events and terminates clearly bad traffic. Normally, administrators do not need to study log entries unless they want to search for some particular events in the network or want to use the log entries, for example, to create statistical reports. Some network traffic may produce a lot of log entries but be of little interest to the administrators. Instead of using log pruning filters, the administrators may decide to adjust the Inspection policy so that these log entries are not produced at all. However, before doing that the administrators should make sure that these log entries are not needed anywhere or that the log entries only concern a specific destination or source.

In this exercise, you will change the logging option to None regarding log entries about Anonymous login attempts. This lab assumes that anonymous login is allowed on the FTP server running on 192.168.2.101 and thus it is not necessary to see the logs regarding this specific FTP server. However, anonymous login attempts on any other FTP servers in the network would interest us, so the attempts on other FTP servers will still produce log entries.

12.12 Create a Rule from Logs

From the Master image, generate an excessive amount of **FTP_Anonymous_Login_Attempt** by entering **./ftp_ anonymous_login.sh 2**.

1. Click the tab where the **Logs** view is open
2. Find log entries that match the **FTP_CS-Anonymous-Login-Attempt** Situation. You should see an excessive amount of **FTP_Anonymous_Login_Attempt** log entries
3. Right-click one of the **FTP_CS-Anonymous-Login-Attempt** log entries and select **Create Rule** → **Do Not Log Connection**. The **New Rule Properties dialog** opens

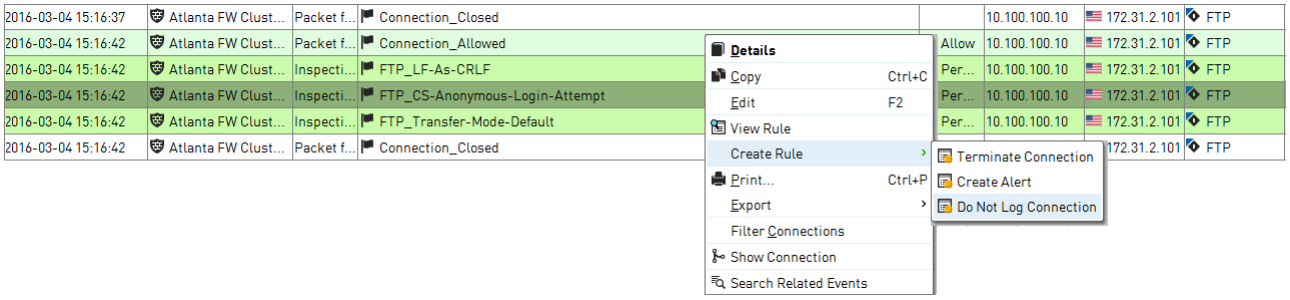


Figure 12.10: Creating a Rule from a Log Entry

4. Select **Add Rules** and click **OK**

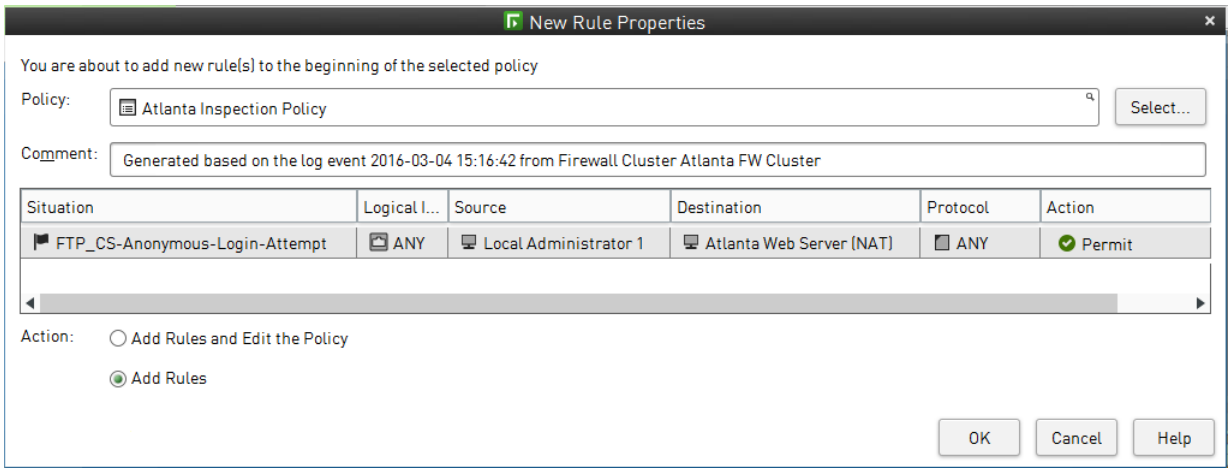


Figure 12.11: New Rule Properties - From Log Entry

5. Click the **Atlanta Inspection Policy** tab where the **Atlanta Inspection Policy** is open in Preview mode
6. Click the **Edit** button in the Policy toolbar
7. Click the **Exception** tab and change the source value to **ANY** in the new inspection exception rule

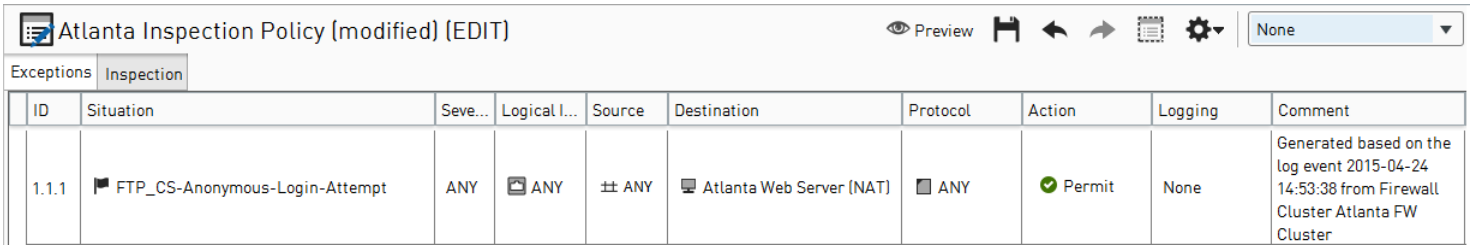


Figure 12.12: Adding New Rule to Exceptions

8. Set the log level to **None**
9. Click the **Save** icon
10. Click the tab where the **Configuration** view is open
11. Browse to **NGFW** → **Policies** → **Firewall Policies**
12. Right-click **Atlanta Policy** and select **Install Policy**
13. Make sure that **Atlanta** is selected as Target and click **OK** to install the policy
14. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed
15. Switch back to the **Logs** view and check that **FTP_CS-Anonymous-Login-Attempt** log entries are no longer shown in the logs

12.13 Summary

During this lab, you configured deep inspection for all traffic on your firewall using the Firewall inspection template for your Firewall policy. You created an Inspection Policy for your Firewall that inherits from an Inspection Policy Template and you customized it to fit your network environment. You blocked the use of old Internet Explorer versions and clean up log entries from anonymous FTP login attempt logs that are not needed in your environment.

LAB 13

Malware Detection

13.1 Getting Started

The File filtering Policy allows you to restrict the file types that are allowed in and out through the firewall, and to apply malware detection to files. In this exercise, you will first create a File filtering Policy that scans files for malware using the Anti-Malware of your firewall and prevents the download of executable files. You will then update your Firewall Policy use the File filtering Policy your created and configure an access control rule to send traffic to File Filtering Policy.

13.2 Test Access to WordPress and File Download

With File Filtering **not** currently enabled, you will test to see that you can, in fact, download a malicious file.

1. Click the tab where the **Logs** view is open. Make sure the **Network Application** and **User** columns are visible and that **Atlanta FW Cluster** is selected as the **Sender**
2. Click the **Current Events** icon in the toolbar
3. In the web browser from Atlanta's server, connect to `http://server-1.wordpress.com` The Helsinki WordPress page opens
4. In the WordPress web page, click the link '**Click to download the order form (HTTP)**' in the Free NGFW Goodies post and save the file in the root folder of your server. Open a terminal, and enter the following commands:
   - `cd Downloads`
   - `gedit order_form.docx`

Figure 13.1: Editing the Downloaded Order Form

5. Check that what you thought was a word document was in fact a malicious file
6. Close **gedit**
7. In the terminal, delete the file you downloaded by typing the following at a command prompt:
   - `rm -f order\_form.docx`

NOTE: If your test is unsuccessful, you might need to clear your browser cache.

13.3 Create File Filtering Policy

The File Filtering Policy you are going to create now contains two rule. The first rule blocks transfer of the executable files. The second rule scans files for malware file using the Anti-Malware scan detection of your firewall.

1. In the **Configuration** view, browse to **NGFW** → **Policies** → **File Filtering Policies**
2. Right-click **File Filtering Policies** and select **New File Filtering Policy**. The **File Filtering Policy Properties** dialog box opens
3. Name the File Filtering Policy **Atlanta File Filtering Policy**
4. Click **OK**. The **New File Filtering Policy** opens for editing in a new tab
5. Right-click the **Permit All** rule and select **Add Rule**
6. Configure the new rule as follows:
    - File Source: **ANY**
    - File Destination: **ANY**
    - Action: **Discard**
7. Click the **File Type** cell, browse to **File Types** → **By File Types** → **Program File** in the Resources list
8. Drag and drop **Executable** tag into the **File Type** cell
9. Right-click **Logging** cell, select **Edit Logging**. The **Logging** dialog box opens
10. Select **Override Log Settings for connection** and configure the logging options as follows:
    - Log Level: **Alert**
11. Click **OK**
12. Right-click the **ID**cell of the rule you just created and select **Add Rule After**
13. Configure the new rule as follows:
    - File Source: **ANY**
    - File Destination: **ANY**
    - File Type: **ANY**
14. Right-click **Action** cell, select **Allow After**. The **Allow After** dialog box opens
15. Select **Anti-Malware Scan**

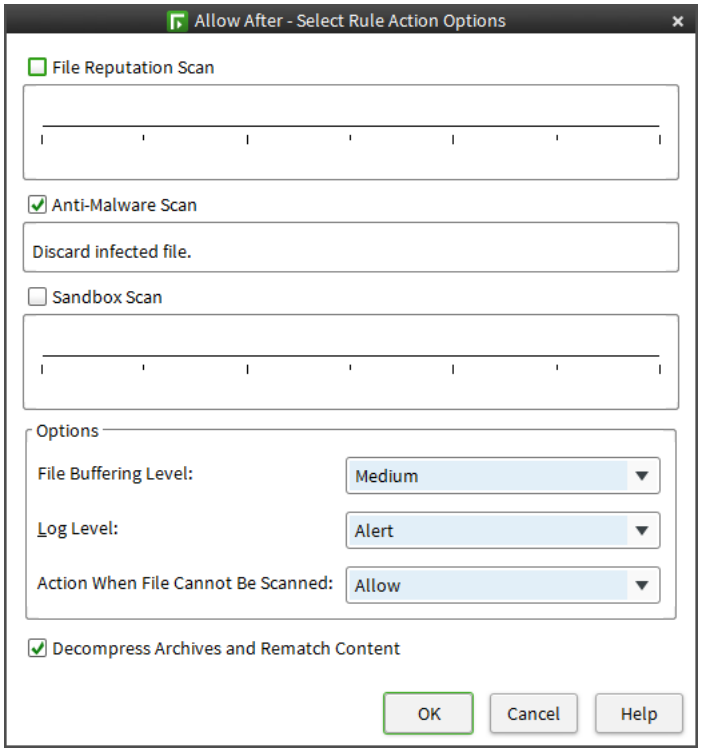


Figure 13.2: File Filtering Allow After Properties

16. Click **OK**

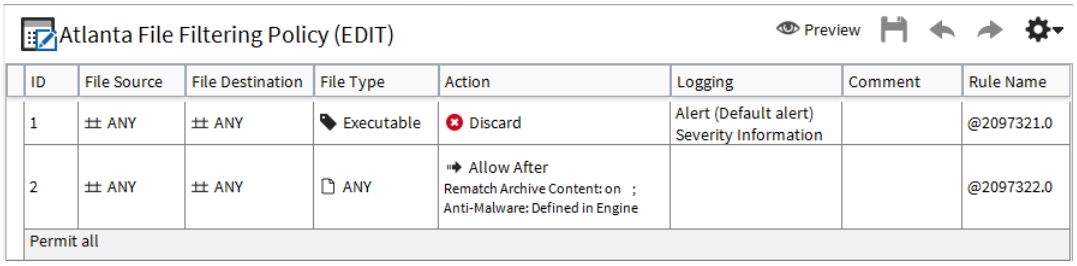


Figure 13.3: Completed File Filtering Policy

17. Click **Save**

13.4 Enable File Filtering on the Engine

In order for the firewall to block malware, the Anti-Malware feature must be enabled in the Add-Ons section of the engine properties.

1. From the **Home** view, right-click on the **Atlanta FW Cluster** and select **Edit Firewall Cluster Atlanta FW Cluster**. The Engine Editor opens
2. Click on **Add-ons** and select **Anti-Malware** Configure Anti-Malware as follows:
   - Select the**Enable** checkbox
   - Malware Log Level: **Alert**
   - Update Frequency: **When Anti-Malware Daemon Starts**
   - Malware Signature Mirror Settings: **172.31.1.101/updater/**

3. Click **Save**. The completed configuration should appear as in the figure below:

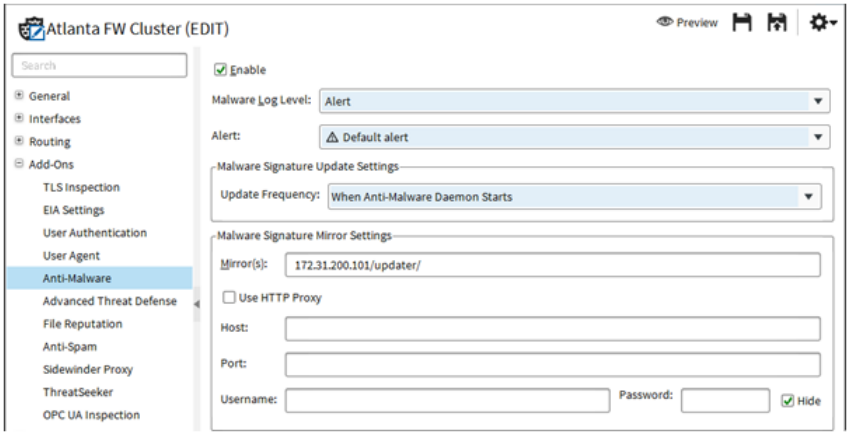


Figure 13.4: Enabling Anti-Malware on the Engine

13.5 Configure File Filtering for HTTP Traffic

The IPv4 Access rule for sending HTTP traffic to the File Filtering Policy must be added in the Atlanta Firewall Policy

1. Open the **Atlanta Policy** and click the **IPv4 Access** tab
2. Right-click the **ID** cell of the SSM Proxy rule (the rule before the last rule) and select **Add Rule Before**. A new rule is added.
3. Configure the rule with the following properties:
   - Source: **net-192.168.2.0/24**
   - Destination: **Not Atlanta Internal Network**
   - Service: **HTTP**
   - Action: **Continue**
4. Right-click **Action** cell, select **Edit Options**. The **Select Rule Action Options** dialog box opens
5. From the **File Filtering** drop-down list, select **On**
6. Click **OK**

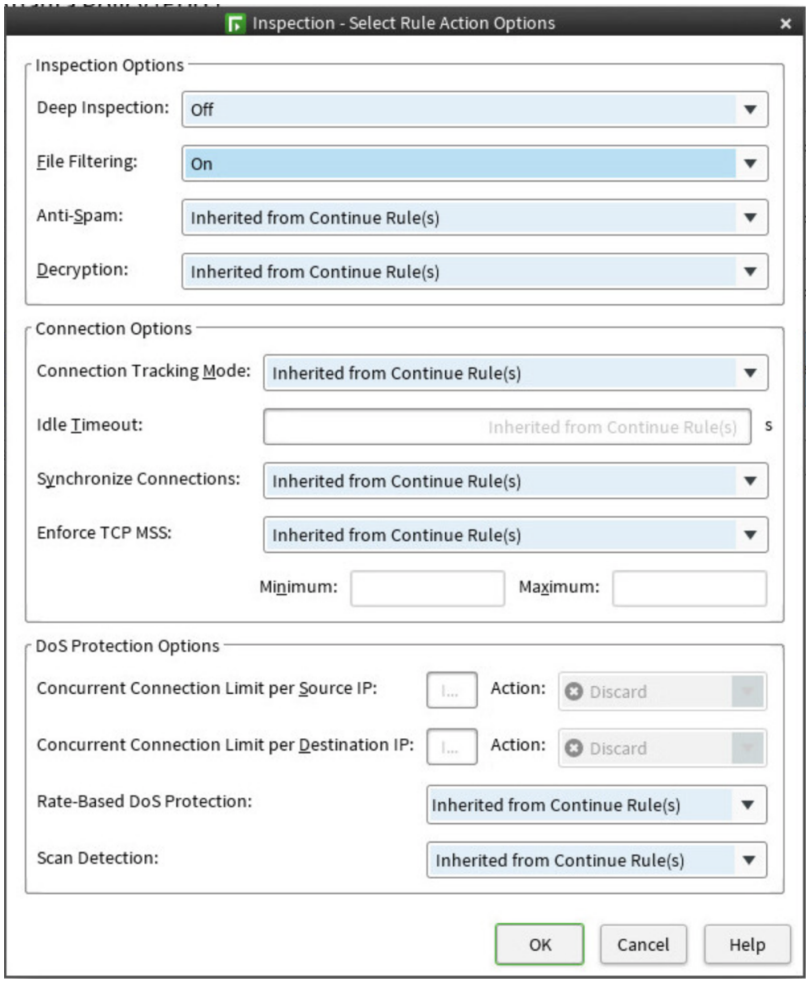


Figure 13.5: Action Options for File Filtering

7. Your completed File Filtering rule should appear as in the figure below:

5.5.3.5	network-192.168.2.0/24	Not Atlanta Internal Networks	HTTP	Continue File Filtering: on
5.5.3.6	network-192.168.2.0/24	Not Atlanta Internal Networks	SSM HTTP Atlanta	Allow
5.5.3.7	network-192.168.2.0/24	Not Atlanta Internal Networks	ANY	Allow

Figure 13.6: File Filtering Enabled in Access Rule

13.5.1 Select the File Filtering Policy in the Firewall Policy

The Atlanta Firewall Policy is updated to use the customized File filtering Policy.

1. Click the **Inspection** tab
2. Click the **Select** button for the **File Filtering Policy**. The **Select Element** dialog box opens
3. Select **Atlanta File Filtering Policy** and click **Select**

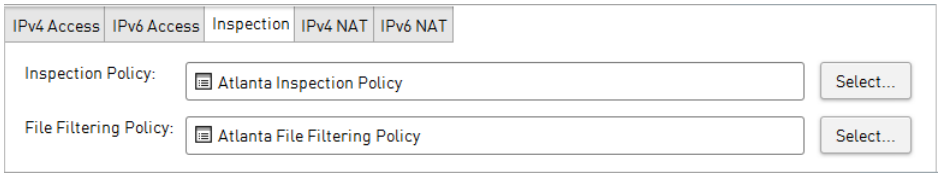


Figure 13.7: Selecting the New File Filtering Policy

4. Click the **Save and Install** icon. The **Policy Upload Task Properties** dialog box opens
5. Click **OK**
6. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

13.6 Test the File Filtering Policy

1. Click the tab where the **Logs** view is open
2. Click the **Current Events** icon in the toolbar
3. Switch back to the console for the **Atlanta Server**
4. In the web browser from Atlanta's server connect to `http://server-1.wordpress.com`
5. In the WordPress web page click the link **Click to download the order form (HTTP)** in the Free NGFW Goodies post. The download of the malicious file is now blocked.

	2016-03-04 15:36:14	Atlanta FW Clust...	Inspecti...	Connection_Allowed	Allow	192.168.2.101	172.31.200...	HTTP	TCP
	2016-03-04 15:36:14	Atlanta FW Clust...	Inspecti...	Executable File	Permit	192.168.2.101	172.31.200...	HTTP	TCP
⚠	2016-03-04 15:36:15	Atlanta FW Clust...	Inspecti...	File_Blocked	Terminate	192.168.2.101	172.31.200...	HTTP	TCP
	2016-03-04 15:36:16	Atlanta FW Clust...	Packet f...	Connection_Allowed	Allow	10.100.100.10	172.31.2.101	FTP	TCP
	2016-03-04 15:36:16	Atlanta FW Clust...	Inspecti...	FTP_LF-As-CRLF	Permit	10.100.100.10	172.31.2.101	FTP	TCP
	2016-03-04 15:36:16	Atlanta FW Clust...	Inspecti...	FTP_Transfer-Mode-Default	Permit	10.100.100.10	172.31.2.101	FTP	TCP

Figure 13.8: File Blocked Log Entry

6. In your web browser, connect to `http://172.31.1.101/download/`
7. In the web page, click on the **procexp.exe** to save the file on your server
8. Check that the Exe file download is blocked and a new **File Blocked** alert appears in the Logs view

NOTE: If your test is unsuccessful, you may need to clear the brower's cache, hold down the **Shift** key, or press **CTRL+F5**

13.7 Summary

During this lab, you configured a File Filtering Policy to scan files for malware using the Anti-Malware of your firewall and prevent the download of exe files through your firewall.

LAB 14

Custom Situations

Getting Started

Situation elements define the patterns in traffic and events in your system that you want to detect with NGFW. Situations also provide a description that is shown in the logs, and a link to relevant external information (CVE/CAN/BID) in the form of a Vulnerability element attached to the Situation. Situations have their own grouping system called Tags.

Situations are generally used for:

- Detecting malicious patterns in traffic
- Reducing the number of alert and log entries produced by matches to Situations (using Correlation Situations)
- Detecting patterns in traffic that you do not want to inspect

In this lab, you will create and test a custom Situation. You will also configure protocol validation in an Inspection rule.

14.1 Create an Inspection Policy for HQ Firewall

In this exercise, you will create an Inspection Policy that inherits Inspection rules from the predefined Medium-Security Inspection Policy. In a production environment, you would directly edit the Medium-Security Inspection Policy and use the same Inspection Policy on multiple NGFW Engines. However, these lab exercises are intended to student to practice editing the Inspection

1. In the **Configuration** view, browse to **Policies** → **Inspection Policies**
2. Right-click **Inspection Policies** and select **New Inspection Policy**. The Inspection Policy Properties dialog box opens
3. Name the Inspection Policy **HQ Inspection Policy**
4. Browse to **High-Security Inspection Policy** and select it as the template for your Inspection Policy
5. Click **OK**. The **Inspection Policy** opens for editing in a new tab

14.2 Creating Custom Situations

You will now create a custom Situation that matches if attempts are made to access the FTP server's "confidential" directory from networks other than the internal network. To detect this, you will define the following regular expression that matches if the string "confidential" (not case-sensitive) is detected in any FTP client stream: `(?i).*confidential`. The characters that make up the regular expression have the following actions:

`(?i)`	Match upper or lower case (ignore case)
`.`	Match any character
`*`	Match 0 or more times

Your custom Situation is also associated with a Situation Type. The Situation Type usually specifies the branch of the Rules tree under which the Situation is included. Here the User Defined Situations Type is chosen.

To restrict the inspection based on the traffic source, you finally need to create the Exception rule. In this rule, you will define that traffic matching the custom Situation having a source other than the Helsinki network and as destination the Natted address of the HQ-Helsinki server will be terminated.

1. Switch to the tab where **HQ Inspection Policy** is open for editing
2. In the Resources list, browse to **Situations** → **Custom Situations**
3. Right-click **Custom Situations** and select **New** → **Situation**. The Situation Properties dialog opens

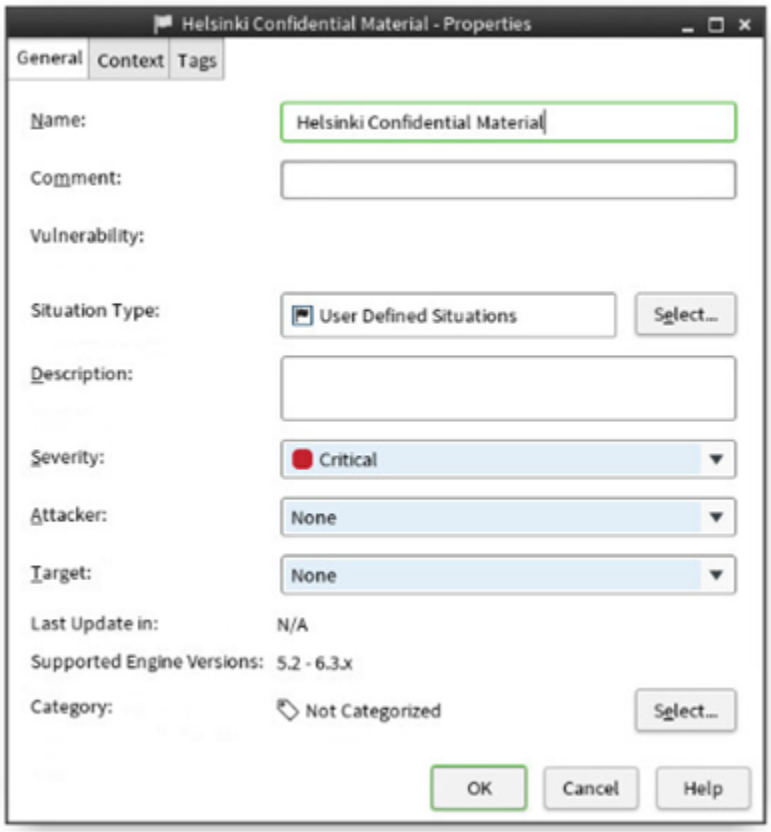


Figure 14.1: Confidential Materials Situation Properties

4. Configure the Situation with the following properties:
   - Name: **Helsinki Confidential Material**
   - Situation Type: Select **User Defined Situations**

     NOTE: Based on the Situation type, the matching Situation can be either terminated (Attacks and Successful Attacks), permitted with Stored logging entry (Suspected Attacks, Suspicious Traffic) or not inspected (Traffic Identification) by the default system template rules.
   - Description: **An attempt to access the confidential directory was detected.**
   - Severity: **Critical**
5. Switch to the **Context** tab and click **Select**. The Select Context dialog opens

6. Browse to **Protocols** → **Application Protocols** → **FTP** → **FTP Client Stream** and click **Select**
7. Enter the following Regular Expression: `(?i).*confidential`
8. Click **OK**. The Situation is created and added to the Custom Situations branch

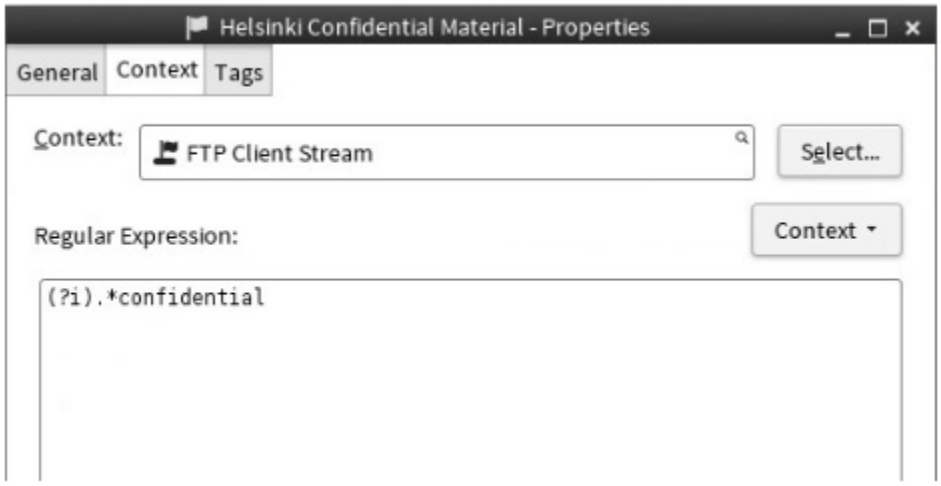


Figure 14.2: Regular Expression for Situation

NOTE: Adding a Tag to a Situation is not obligatory. However, grouping similar types of Situations under the same Tag helps you to configure rules as you can use the Tag in the rules instead of adding each Situation individually.

14.2.1 Use the Custom Situation in an Exception Rule

1. In the **Exceptions** tab of your Inspection Policy, right-click the first rule and select **Add Rule Before**
2. Click the **Situation** cell in the new rule and browse to **Custom Situations** in the Situations list
3. Drag and drop the **Helsinki Confidential Material** Situation into the **Situation** cell
4. Configure the rule with the following properties:
   - Severity: **ANY**
   - Logical interface: **ANY**
   - Source: **Not Helsinki Internal Network**
   - Destination: **Management Server (NAT)**
   - Protocol: **ANY**
   - Action: **Terminate**

14.2.2 Set Logging Options

1. Double-click the **Logging** cell.
2. Select **Override Settings Inherited from Continue Rule(s)** and change the Log Level to **Alert**.
3. Click **OK**. The new rule should appear as in the figure below:

Figure 14.3: Exception Rule for Confidential Material

4. **Save** the Inspection Policy

14.2.3 Select the HQ Inspection Policy in the HQ Firewall Policy

1. If the **HQ Policy** is not open in a tab, browse to **NGFW** → **Policies** → **Firewall Policies** → **Firewall Template** → **Firewall Inspection Template** → **Global Firewall Template** and right-click **HQ Policy** and select **Edit Firewall Policy HQ Policy**
2. Click the **Inspection** tab
3. Click **Select** button for the **Inspection Policy**. The **Select Element** dialog box opens
4. Select **HQ Inspection Policy** and click **Select**
5. Click **Save and install**
6. Close the **Upload Policy: HQ Policy** tab when the policy upload is completed

14.2.4 Test the Custom Situation

1. From **Atlanta-Server**, open **Firefox** and type `ftp://172.31.1.101`
2. Click **confidential**. You are not able to access to the confidential folder
3. Switch back to the **HQ SMC** console where the log view is open
4. View the log entries generated by your FTP traffic in the Log view

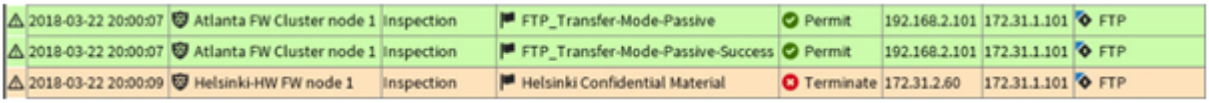


Figure 14.4: Confidential Material Access Attempt Log Entry

14.3 Use Protocol Validation

In this example, you want to detect if someone from the external network is doing DNS listing from the HQ Helsinki's DNS server and deny the DNS transfer requests. You will update the previously configured Inspection rule to detect the use of DNS transfer requests into your HQ Inspection Policy.

14.3.1 Create a Rule to Detect DNS Transfer Requests

1. In the **Exceptions** tab of your **HQ Inspection Policy**, click the **Situation** cell of the first rule that contains the **Helsinki Confidential Material**Situation
2. Start typing **DNS_Transfer-Request** and a list of matching Situations appears. Select the **DNS_Transfer-Request** situation

Figure 14.5: DNS Transfer Request Exception Rule

3. **Save** the **HQ Inspection Policy**
4. Click the tab where the **HQ Policy** is open for editing
5. Click **Save and install**

14.3.2 Test DNS Transfer Requests

1. From the**Atlanta-Server** machine, switch to a terminal window and enter **host -l training.com** on the command line.
2. In the Management Client, switch to the tab where the Logs view is open and verify that the Situation was logged properly for the test.

Figure 14.6: DNS Transfer request Terminated Log Entry

14.4 Summary

In this lab, you created a new custom Situation to detect access to a specific directory on your FTP server. You also configured protocol validation to prevent unauthorized client hosts from doing DNS listing from the HQ Helsinki's DNS server.

LAB 15

TLS Inspection

15.1 Test Anti-Malware Inspection for HTTPS Connections

1. From the **Atlanta Server**, open **Firefox** and type `https://server-1.wordpress.com` in the URL Bar
2. In the WordPress web page, click the link 'Click to download the order form (HTTPS)'. This links opens a secure connection for downloading the malicious file from the WordPress web site. If the browser shows a security exception message, add the exception. You can visualize the certificate, check the issuer and confirm the security exception.

   NOTE: In the training lab environment the certificate used for the WordPress website is a self-signed certificate.
3. **Save the file** in the root folder of your server
4. Open a console, and enter the commands:
   - `cd Downloads`
   - `gedit order\_form.docx`

Figure 15.1: Editing the Downloaded Order Form

5. Check that you succeeded in downloading the malicious file again, this time through a secure connection

NOTE: You might need to clear the browser cache and delete the user session under monitoring.

15.2 Configure TLS inspection

You will now configure decryption and inspection of the HTTPS traffic for vulnerability inspection andfor malware detection with the NGFW anti-malware.

15.2.1 Create a Custom HTTPS Service

1. Click the tab where the **Configuration** view is open and browse to **NGFW** → **Other Elements** → **Services** → **TCP**
2. Right-click **HTTPS (with decryption)** and select **New** → **Duplicate**.The **TCP Service Properties** dialog box opens

3. Name the Service **Atlanta HTTPS Custom**
4. Click the **Protocol Parameters** tab and select the following options:
   - HTTPS Decryption and inspection: **Yes**
   - Logging of Accessed URLs: **Yes**
   - Optimized Server Stream Fingerprinting: **Yes**
5. Click **OK**

15.2.2 Configuring Client Protection

The Client Protection Certificate Authority element contains the private key and certificate that the engine uses to sign the substitute certificates it generates.

1. Click the **Atlanta FW Cluster (EDIT)** tab where **Atlanta FW Cluster** is open for editing
2. Browse to **Add-Ons** → **TLS Inspection**
3. From the **Client Protection Certificate Authority** drop-down list, select **New**
4. Name it **Client Protection CA protecting Atlanta Internal Clients**
5. Set **Validity time** to **120** min
6. Click the **Certificate** tab and click **Generate**. The **Signing Certificate Details** dialog box opens
7. Define the following parameters:
   - Common Name: **clientprotection.atlanta.com**
   - Public Key Length: **2048**
   - Valid Until: Leave the default

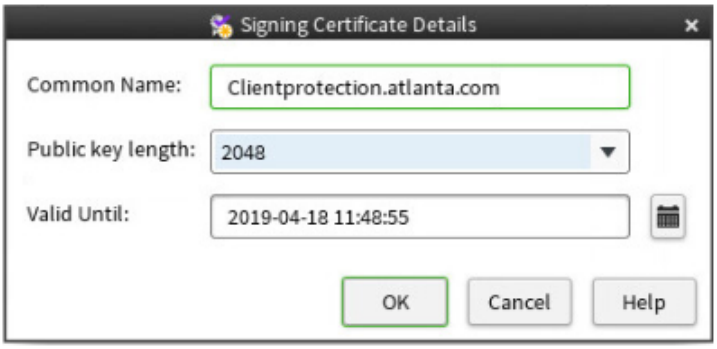


Figure 15.2: Generating Client Protection CA

8. Click **OK**
9. In the **Client Protection Certificate Authority Properties**, Click **Export**

Figure 15.3: Exporting Client Protection CA Certificate

10. In the **Export File** dialog box, browse to \ → **Home** → **Student** → **Desktop**
11. Name the file**NGFW Client Protection CA.crt**

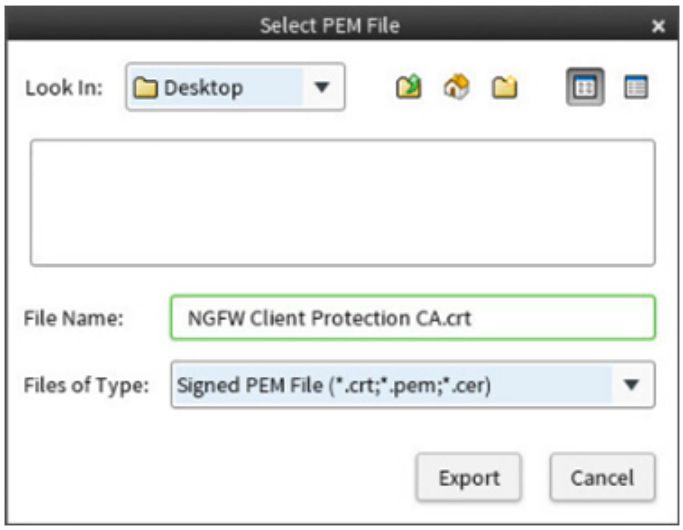


Figure 15.4: Saving the Client Protection CA Certificate

12. Click **Export** The Export File dialog box closes
13. Click **OK** to close the **Client Protection Certificate Authority** Properties
14. Select the **Client Protection CA protecting Atlanta Internal Clients**
15. Click **Save** in the Engine Editor toolbar

15.2.3 Import Client Protection CA in the Atlanta Web Browser

1. Using the **Main Menu** from the **Landing Machine**, open a console to the **Atlanta Server**
2. On the desktop, double-click the **Firefox** icon
3. In the URL bar, enter `ftp://Student@172.31.1.101` and press **Enter**
4. When prompted, enter `Forcepoint1!` as the password
5. Browse to the **Desktop** folder

6. Right Click **NGFW Client Protection CA.crt** and select **Save link as...**

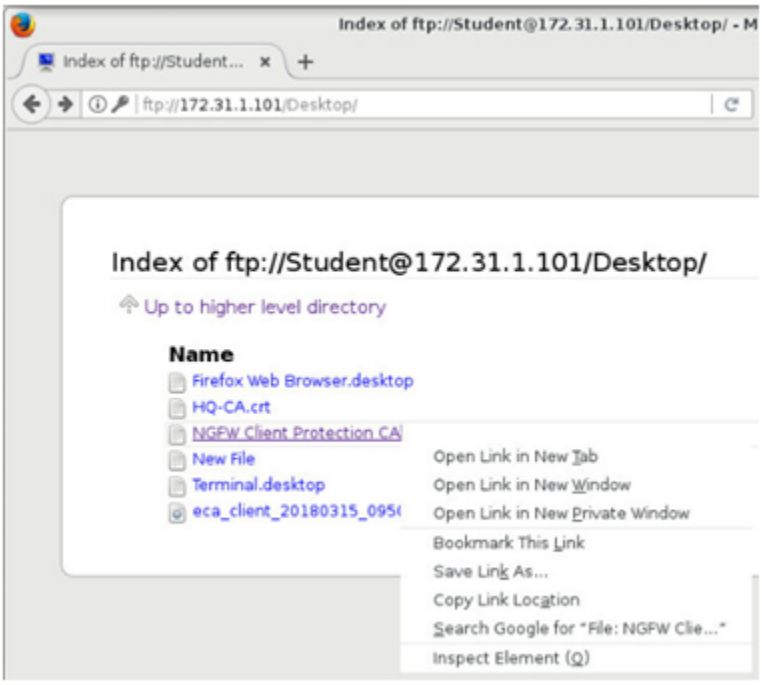


Figure 15.5: Downloading Client Protection CA

7. In the dialog box, browse to **Desktop** and click **Save**
8. Click the **Menu** icon on the top right in the Firefox application and click **Preferences**

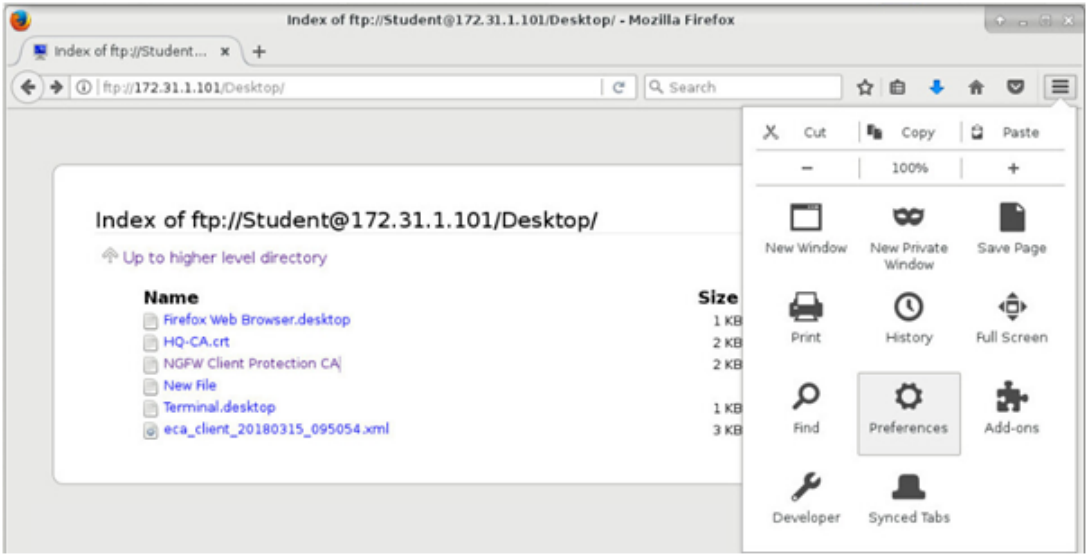


Figure 15.6: Firefox Preferences - Trusting Client Protection CA

9. In the dialog box, browse to **Advanced** → **Certificates** and click **View Certificates**

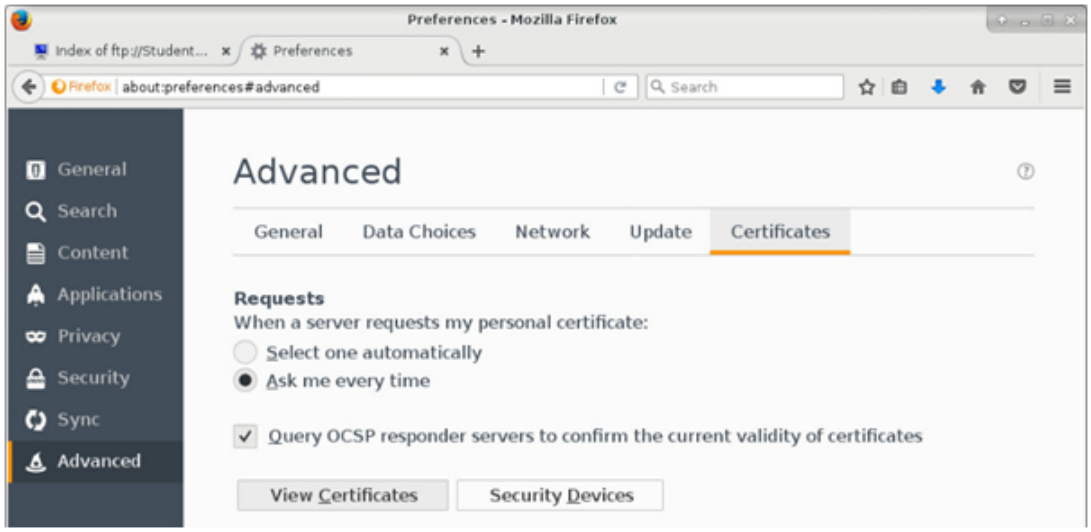


Figure 15.7: Viewing Firefox Certificates

10. Click the **Authorities** tab
11. Click **Import** in the In the **Certificate Manager** dialog box. Browse to **Desktop** and Select **NGFW Client Protection CA.crt** and Click **Open**

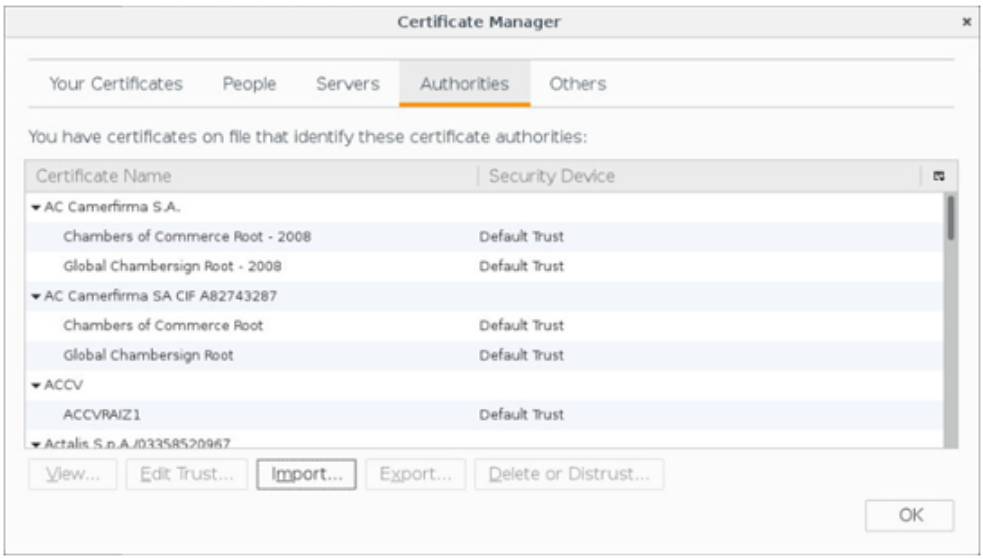


Figure 15.8: Importing the CA Certificate into Firefox

12. Select **Trust this CA to identify websites** checkbox and click **OK**
13. Click **OK** to close the **Certificate Manager** dialog box

15.2.4 Define Access Rules for Vulnerability and Anti-Malware Inspection for HTTPS Traffic

1. Click the **Atlanta Policy (EDIT)** tab where the **Atlanta Policy** is open for editing.
2. In the **IPv4 Access** Rule where File Filtering is enabled for outbound HTTP traffic, Click the **Service** cell and browse to **Services** → **TCP** in the Resources list.
3. Drag and drop the **Atlanta HTTPS Custom Service** to the **Service** cell
4. Right-click **Action** cell, select **Edit Options**. The **Select Rule Action Options** dialog box opens

5. From the **Deep Inspection** drop-down list, select **On**
6. From the **File Filtering** drop-down list, select **On**

Figure 15.9: Enabling File Filtering

7. **Save** and **Install** the policy
8. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

15.2.5 Test Certificate used for TLS Inspection

1. Open a new tab on **Firefox**
2. In the URL bar, enter **www.google.com** and press **Enter**
3. In the URL bar, click the lock icon

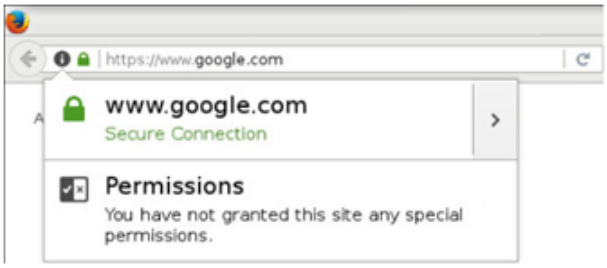


Figure 15.10: Verifying Google Certificate Validity

4. Click the arrow on the right hand side
5. Check that the certificate used was generated by the Firewall.

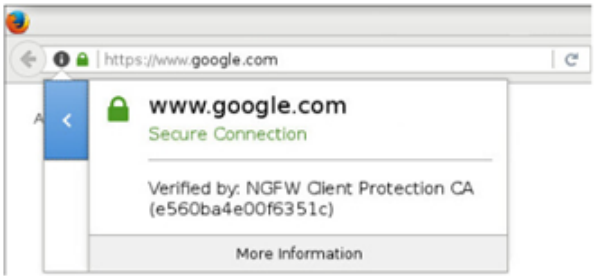


Figure 15.11: Verifying the use of NGFW CA

6. If you click **More Information**, and click **View Certificate**, you can then view the certificate and check that the certificate has `http://www.google.com` as the Common name, but its issuer is **NGFW Client Protection CA** and the Period of Validity is **one** day.

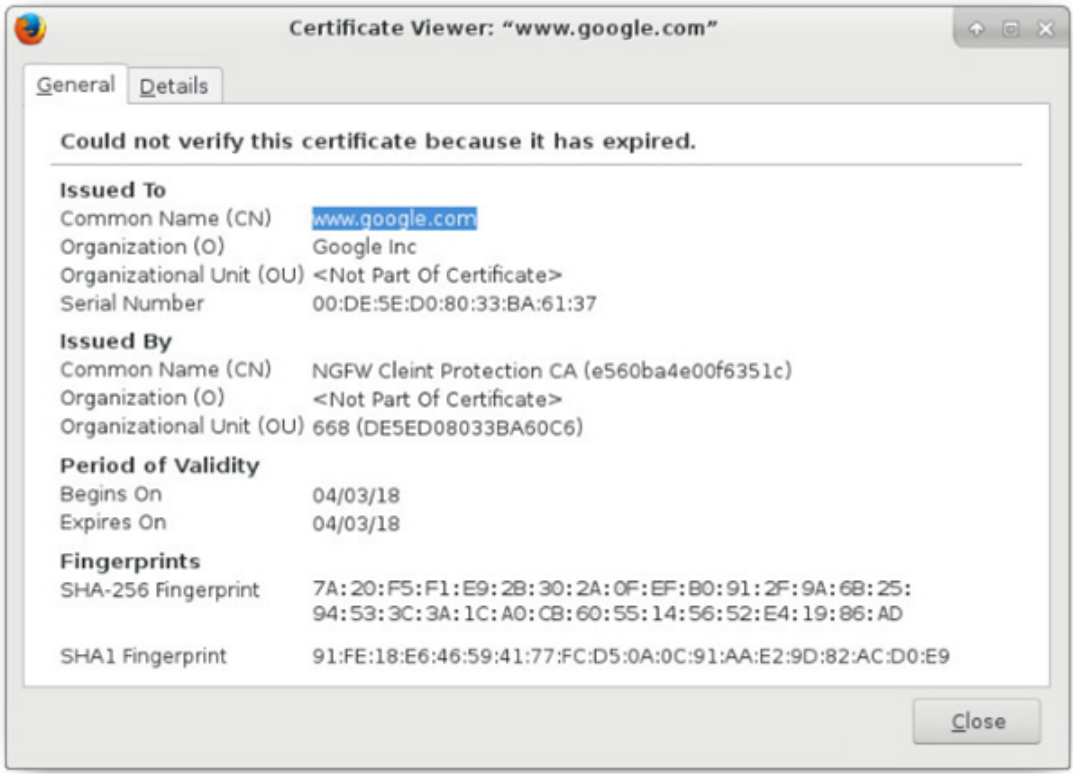


Figure 15.12: Google Certificate Details

15.3 Test Anti-Malware Inspection for HTTPS Connections

1. Using the **Main Menu** from the **Landing Machine**, open a console to the **Atlanta Server**
2. In Firefox, connect to `http://server-1.wordpress.com`
3. In the WordPress web page, click the link '**Click to download the order form (HTTPS)**' in the **NGFW Free Goodies** post
4. Verify that a new alert appears in the **Logs** view
5. Check the details of Firewall logs:
   - The connection is HTTPS on port 443, but the firewall is still able to inspect the connection because the HTTPS tunnel is terminated on the firewall
   - Anti-malware is now able to inspect the traffic for malware and the download of the EICAR file was discarded

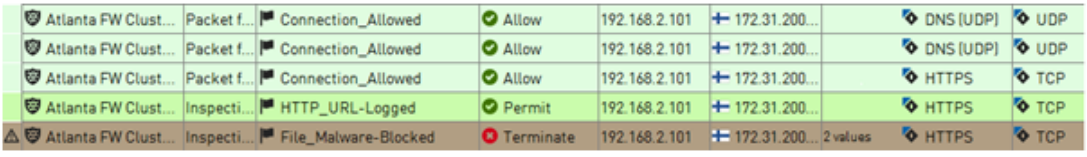


Figure 15.13: Caption

If your test is unsuccessful, you might need to clear your browser cache or use **Ctrl+F5** to force the reload of the Web page. To completely clear the web brower cache, perform the following steps:

1. Click the **Menu** icon in the top right of the Firefox application and click **Preferences**

2. Browse to **Privacy** and click **Clear all current history**
3. In the dialog box, select **Everything** as the time range to clear and make sure that **Cache** is selected
4. Click **Clear Now**

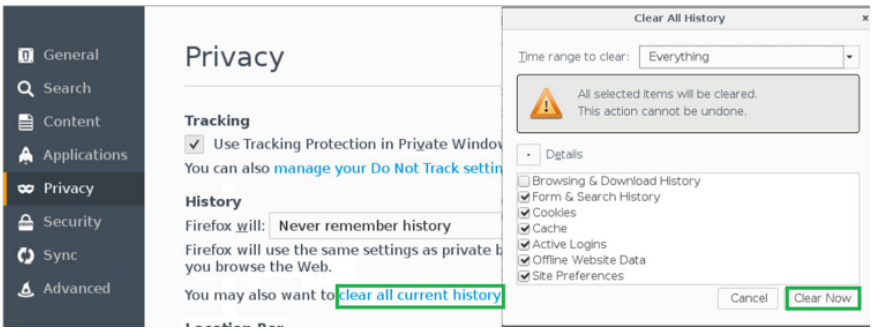


Figure 15.14: Clearing the Browser History

15.4 Summary

In this lab, you have inspected and decrypted traffic for vulnerability and malware inspection using the NGFW anti-malware.

LAB 16

Multi-Layer Deployment

16.1 Getting Started

In the lab 15, you configured the HQ Inspection Policy to detect an external host accessing a specific directory on your HQ Helsinki's FTP server and to prevent DNS listing from the HQ Helsinki's DNS server.In this lab, you will extend the protection of your HQ Helsinki Server to block these connections when originating from the internal network.

You will define a Layer 2 Interfaces for the HQ-Helsinki Firewall and a Layer 2 Interface policy that will capture traffic in the Helsinki internal network and inspect it according to the HQ Inspection Policy.

16.2 Define a Layer 2 Interfaces Policy for HQ-Helsinki Firewall

In this exercise, you will create a Layer 2 Interface Policy. The aim of this policy is to capture the traffic in the Helsinki internal network and inspect it according to the HQ Inspection Policy.

In lab 15, you configured the HQ-Helsinki Firewall to use the HQ Inspection Policy by associating it to the HQ policy. Firewall Policies and Layer 2 Interface Policy share the same Inspection Policy. You will use the Layer 2 Interface Policy Template as the basis for your HQ Layer 2 Interface Policy.

In the HQ Layer 2 Interface Policy, you will only create a continue rule to log Helsinki internal traffic. Deep inspection is enabled by the rules defined in the Layer 2 Interface Policy Template that you will select as basis for your Policy. The default action for the access control is set by the type of the Layer 2 Interface type you will choose for your Layer 2 Interface.

Later in this lab, you will define a Layer 2 Capture Interface, therefore your HQ Layer 2 Policy will allow all traffic and sent it to be deep inspected in the HQ Inspection Policy.

16.3 Define a Layer 2 Interfaces Policy for HQ-Helsinki Firewall

1. In the **Configuration** view, browse to **Policies** → **Layer 2 Interface Policies**
2. Right-click **Layer 2 Interface Policies** and select **New Layer 2 Interface Policies**. The Layer 2 Interface Policy Properties dialog box opens
3. Name the Inspection Policy **HQ Layer 2 Interface Policy**
4. Browse to **Layer 2 Interface Template** and select it as the template for your Layer 2 Interface Policy

Figure 16.1: Creating a New Layer 2 Interface Policy

5. Click **OK**. The **Layer 2 Interface Policies** opens for editing in a new tab
6. Double-click the green Insert Point, **IPv4 Insert Point - add rules here**. An empty rule appears
7. Configure the rules as follows:
    - **Source**: Right-click and select **ANY**
    - **Destination**: Right-click and select **ANY**
    - **Service**: Right-click and select **ANY**
    - **Action**: Right-click and select **Continue**
    - **Logging**: Right-click and select **Edit Logging**. The **Logging - Select Rule Options** dialog opens
8. Check the box for **Override Settings Inherited from Continue Rule(s)**
9. Use the **Logging Level** drop-down menu and select **Stored**

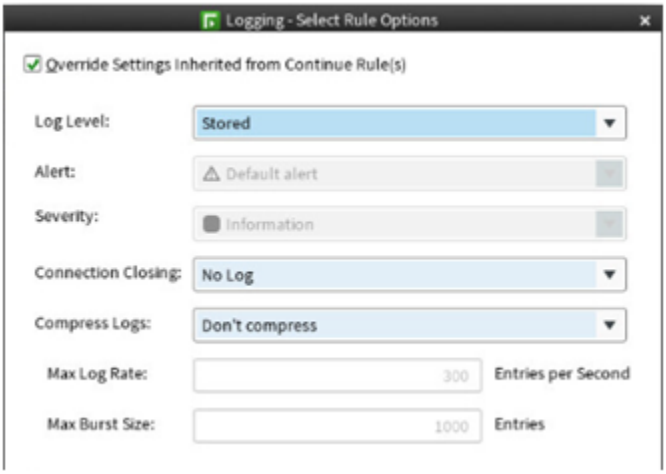


Figure 16.2: Continue Rule for Logging - Layer 2 Interface Policy

10. Click **OK**
11. Save the policy

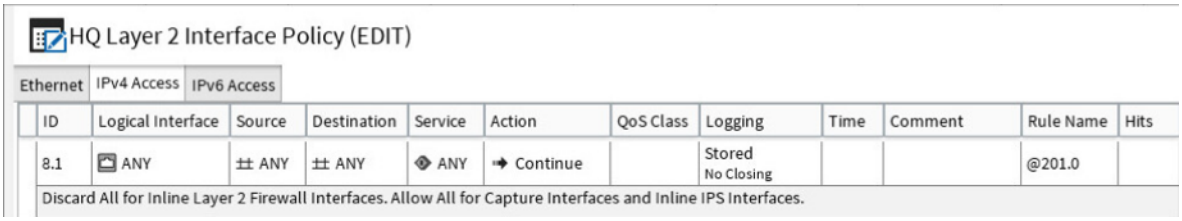


Figure 16.3: Completed Continue Rule for Logging

16.4 Define a Layer 2 Physical Interfaces for HQ-Helsinki Firewall

You will define a new Layer 2 Interface for HQ-Helsinki Firewall of the type Capture Interface.

1. Click the tab where the **HQ-Helsinki FW** is open for Editing. Alternatively, from the **Configuration** view, browse to **NGFW** → **NGFW Engines**, right-click on the **HQ-Helsinki FW** and select **Edit Single Firewall HQ-Helsinki FW**.The Engine Editor opens
2. On the left side, click on **Interfaces**
3. In the upper right of the client, click the **New** icon and select **Layer 2 Interface**. The Layer 2 Physical Interface properties opens

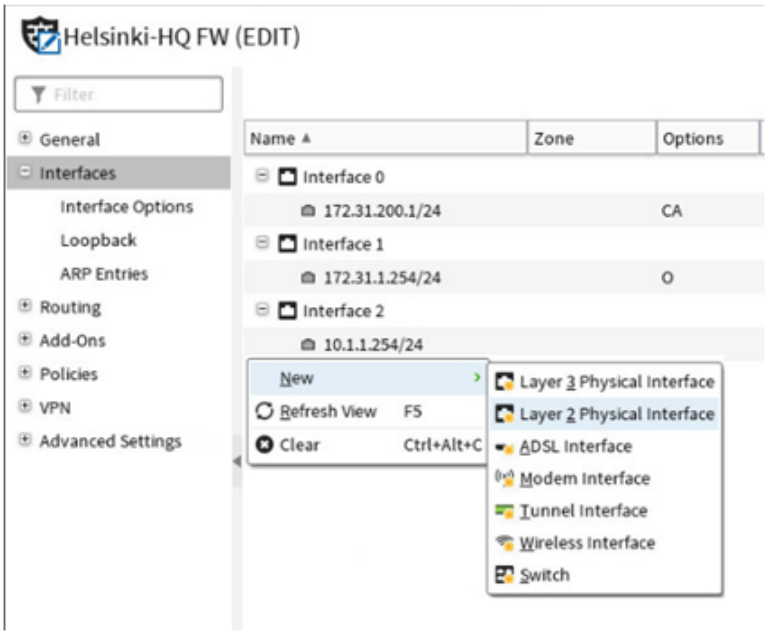


Figure 16.4: Defining a New Layer 2 Interface

4. Verify that the **Interface ID** is set to **3**
5. Click the **Type** drop-down menu and select **Capture Interface**
6. Click the **Zone** drop-down menu, and select **Internal**
7. Click the **Logical Interface** drop-down menu in the **Capture Interface Settings**. The Select Logical Interface dialog opens
8. Click **New** in the drop down menu. The Logical Interface Properties dialog opens
9. Name the logical interface **HQ Capture** and click **OK**

10. In the **Comment** field, enter **HQ Internal Capture**

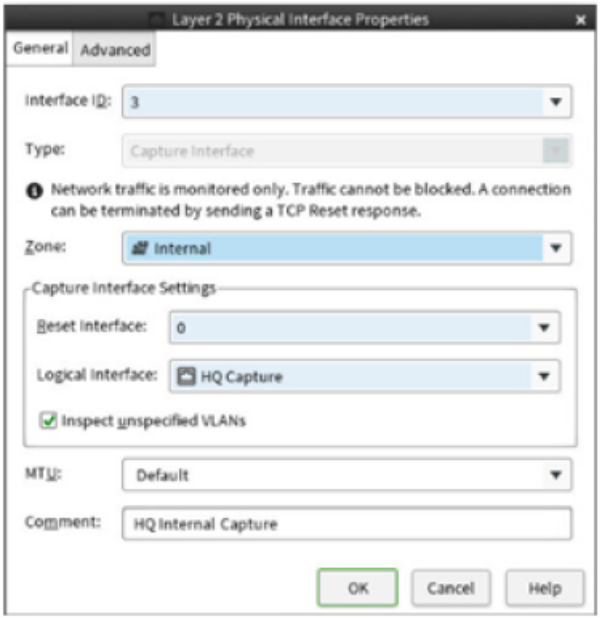


Figure 16.5: Layer 2 Physical Interface Properties

11. Click **OK**. The Physical Interface is added to the Interfaces list

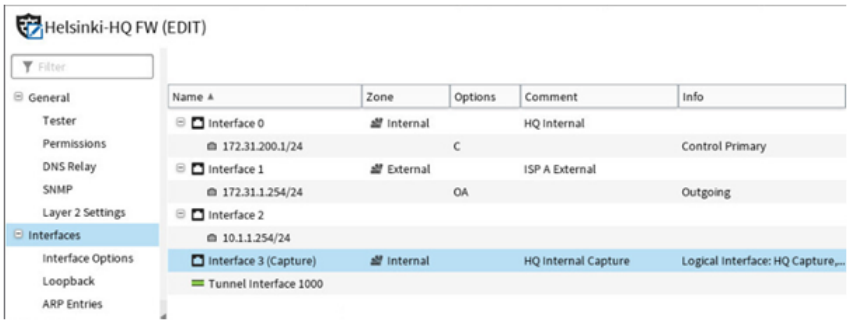


Figure 16.6: Completed Layer 2 Interface

12. Click **OK**. The Physical Interface is added to the Interfaces list
13. On the left side, click on **General** → **Layer 2 Settings**
14. Click the **Policy for Layer 2 Interface** drop down menu and click **Select**. . . The Select dialog box opens
15. Click **HQ Layer 2 Interface Policy** and click **Select**

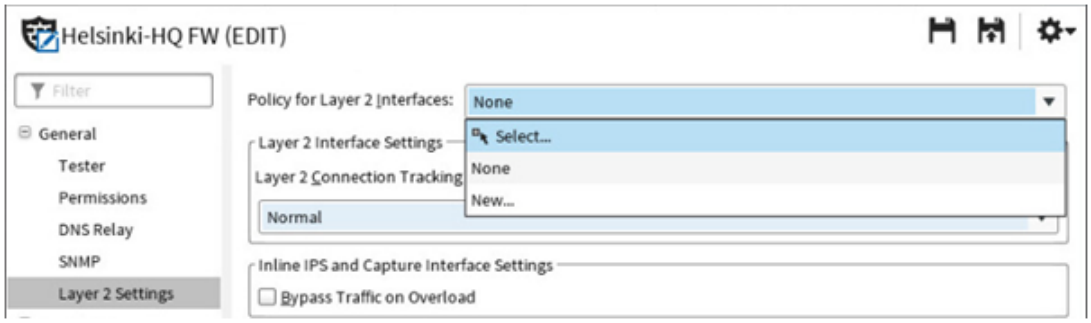


Figure 16.7: Selecting a Layer 2 Interface Policy

16. Click the **Policy for Layer 2 Connection Tracking Mode** drop down menu and click **Loose**

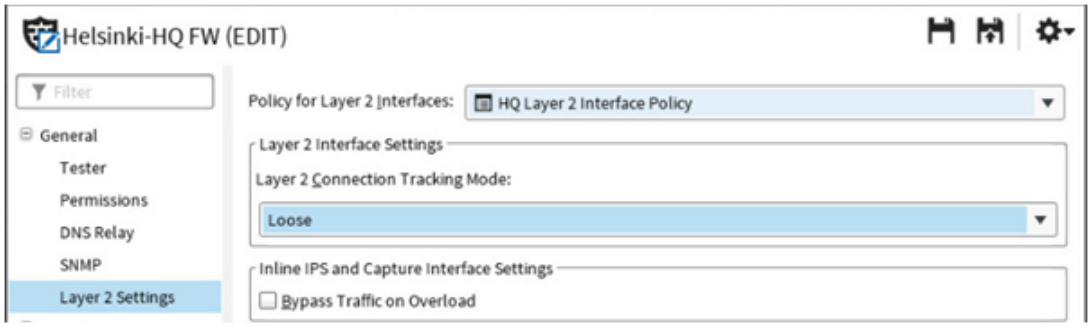


Figure 16.8: Layer 2 Interface Connection Tracking Mode

16.5 Create a Rule to monitor the Internal Access to the Confidential Material

You will now add a rule in the HQ Inspection Policy to monitor the access to the confidential Material. In this new rule you will define an Alert to be sent in case the particular situation is detected by the Inspection Policy.

1. Click the tab where your **HQ Inspection Policy** is open for editing. Alternatively from the **Configuration** view, browse to **NGFW** → **Policies** → **Inspection Policy** → **High-Security Inspection Template**, right-click on the **HQ Inspection Policy** and select **Edit Inspection Policy HQ Inspection Policy**. The Policy Editor opens
2. In the **Exceptions** tab, right-click the first rule and select **Add Rule After**
3. Configure the rule with the following properties:
   - Situation:**Helsinki Confidential Material**
   - Severity: **ANY**
   - Logical interface: **ANY**
   - Source: **network-172.31.200.0/24**
   - Destination: **Management Server**
   - Protocol: **ANY**
   - Action: **Permit**
   - Logging: **Alert**
4. Click **OK**. The new rule should appear as in the figure below

Figure 16.9: Completed Confidential Material Terminate Rule

5. **Save** the **HQ Inspection Policy**
6. Browse to **Policies** → **Firewall Policies**
7. Right-click **HQ Policy** and select **Install Policy**
8. Close the **Upload Policy: HQ Policy** tab when the policy upload is completed

16.6 Test Access to Confidential folder from the HQ Workstation

From the **HQ Workstation**, you will open Google Chrome and connect to your Helsinki FTP server internal address 172.31.200.101 and check that the access to the confidential folder is detected by your Layer 2 Interface Policy.

1. Switch back to the console for the **Helsinki Workstation**
2. Using Google Chrome, in the URL bar, enter `ftp://172.31.200.101`
3. Click **confidential**
4. Switch back to the **HQ SMC** console where the log view is open
5. View the log entries generated by your FTP traffic in the Log view

Figure 16.10: Log Entry for Detected Access to Confidential Material

NOTE: You will see the alert in the logs when access to the confidential material is detected by the layer 2 interface configured in capture mode.

16.7 Summary

In this lab, you have configured Layer 2 interfaces on an NGFW in the FW/VPN Role. This has allowed you to detect unwanted activity by monitoring network traffic, in much the same way as an IDS.

LAB 17

Forcepoint Integration

17.1 Getting Started

NGFW integrates with other Forcepoint security products and third party products to provide enhanced security.

URL filtering prevents users from accessing websites that provide content that is objectionable, potentially harmful, or not work-related. This kind of content filtering can increase network security and enforce an organization's policy on acceptable use of resources.

The URL categorizations are provided by the external Forcepoint™ ThreatSeeker Intelligence Cloud service. ThreatSeeker Intelligence Cloud (ThreatSeeker) provides categories for malicious websites and several categories for different types of non-malicious content you might want to filter or log.

17.2 Update DNS Settings on the Atlanta Server

To ensure that DNS names related to the Forcepoint cloud services resolve properly, you will now switch your DNS server from the lab DNS server to a public DNS server.

1. From the **Atlanta Server** open a command prompt by clicking, in the upper left corner of the screen, **Applications** → **Terminal**. A new command prompt opens
2. At the command prompt, type `su root` and press **Enter**
3. Enter the password `Forcepoint1!` and press **Enter**
4. Type the following command: `echo "nameserver 8.8.8.8" > /etc/resolv.conf`

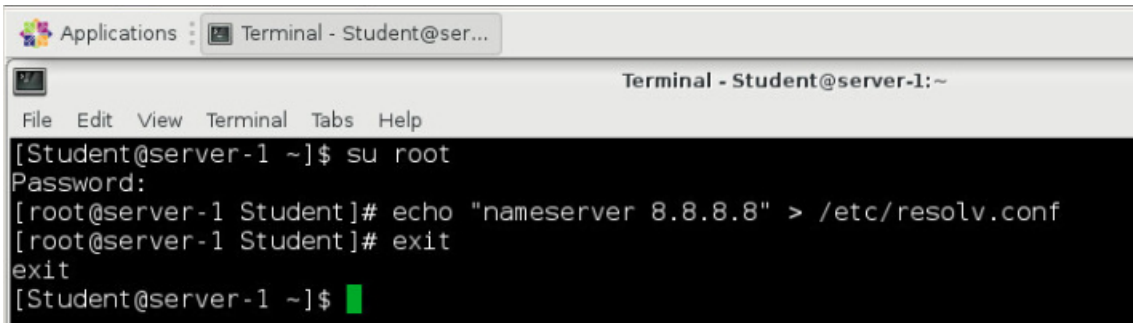


Figure 17.1: Changing the DNS Server on Atlanta Server

17.3 Enable URL Filtering on the Engine

To start using ThreatSeeker categories for URL filtering, you need to enable ThreatSeeker for the engine.

1. Click the **Atlanta FW Cluster(EDIT)** tab where the **Atlanta FW Cluster** is open for editing
2. Click on **Add-ons** and select **ThreatSeeker**
3. Check the box next to **Enable**
4. Click **Save**

17.4 Enforce logging for URL Filtering

The logging for URL category is enforced in the continue rule that will be matched before the URL Filtering rules.

1. Click the **Atlanta Policy (EDIT)** tab where the **Atlanta Policy** is open for editing
2. In the IPv4 Access Continue rule that enables TLS Inspection and File Filtering, right-click the **Logging** cell and select **Edit Logging**. The **Logging** dialog box opens
3. Select **Override Recording Settings Inherited from Continue Rule(s)**
4. Select **Enforced** in the **Log URL Categories** drop-down list

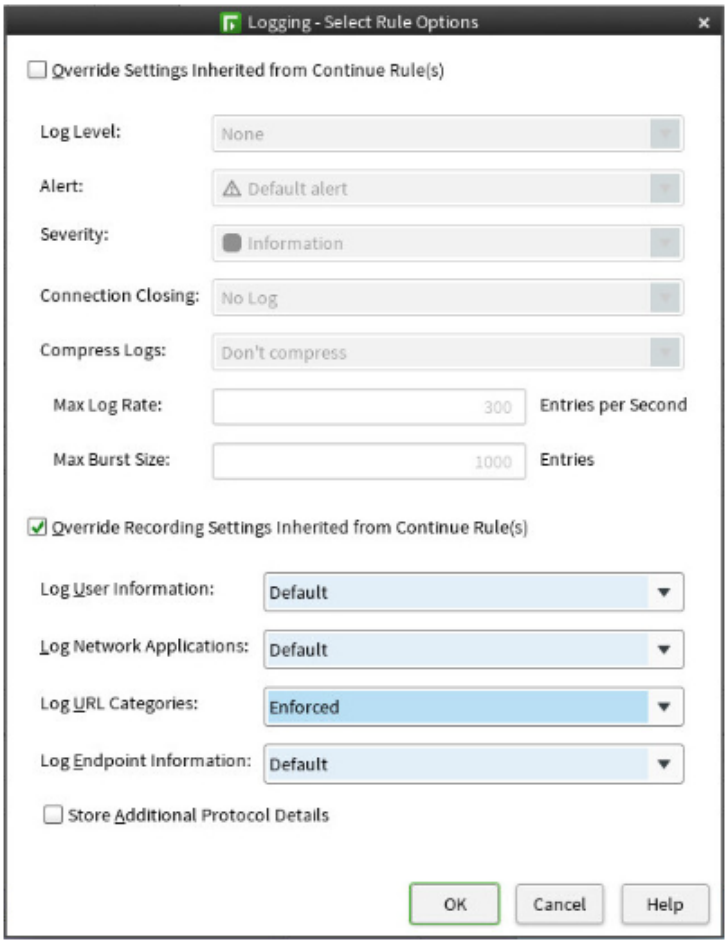


Figure 17.2: Changing Logging Options, Enforce URL Logging

5. Click **OK**

17.5 Create User Response for URL Filtering

A User Response can be configured to notify the user that a HTTP or HTTPS connection is closed by the URL filtering. The User Response will be activated in the continue rule that will be matched before the URL Filtering rules.

1. In the Continue rule where you set the logging level for URL Filtering, right-click the **Action** cell and select **Edit Options**. The Select Rule Action Options dialog box opens
2. Click on the **Response** tab and check the box for **Override Settings Inherited from Continue Rules**
3. Click **Select** next to the **User Response** field. The Select User Response dialog box opens
4. Click on **Default User Response** and click **Select**. The Select User Response dialog box closes
5. Click **OK**. The Select Rule Action Options closes

17.6 Define Access Rules to block Connections to Shopping sites

You are now going to add a rule to block access to Shopping sites using URL filtering categories provided by Forcepoint ThreatSeeker cloud service.

1. With the **Atlanta Policy** still open for editing, right-click in the **ID** cell of the continue rule you just updated and select **Add Rule After**. A new empty rule is added
2. Drag **net-192.168.2.0/24** from a rule below into the **Source** cell
3. Drag **not Atlanta Internal Networks** from the rule below into the **Destination** cell
4. Click the **Service** cell. In the resource pane, browse to **URL Category** and drag **Shopping**into the **Service** cell. The completed Access rules should appear as in the figure below:

Figure 17.3: Access Rules to Drop Shopping URL Category

5. **Save and install** the policy
6. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

17.7 Test that Access to Shopping Sites are blocked

17.7.1 Test Access to Shopping Sites from the Atlanta Server

1. Switch back to the console for the **Atlanta Server**
2. Open **Firefox**
3. In the URL bar, enter `https://www.amazon.com`. Access is blocked and you should receive the following response:

Figure 17.4: Blocked Access to Amazon.com

17.7.2 Add URL Filtering Columns to Logging View

In order to view information about URLs and URL categories in the logging view, you will add these columns to your logging view.

1. Switch back to the **HQ SMC** console where the **Log View** is still open
2. From the **Logs** view, right-click on any column header and select **Column Selection**. The Column Selection dialog box opens
3. On the left, click **All Fields**
4. Type **URL**. Drag and drop the **URL** and **URL Category** fields into the column on the right under **Situation**
5. Click the **Save Column Settings** button to save your customized logging view

17.7.3 Use the Logs to View the Blocked Shopping Sites Access Attempt

1. Right-click on the column header for **URL Category** and select **Filter: URL Category**. The Filter Properties opens
2. Click in the empty pane and type **Shopping**

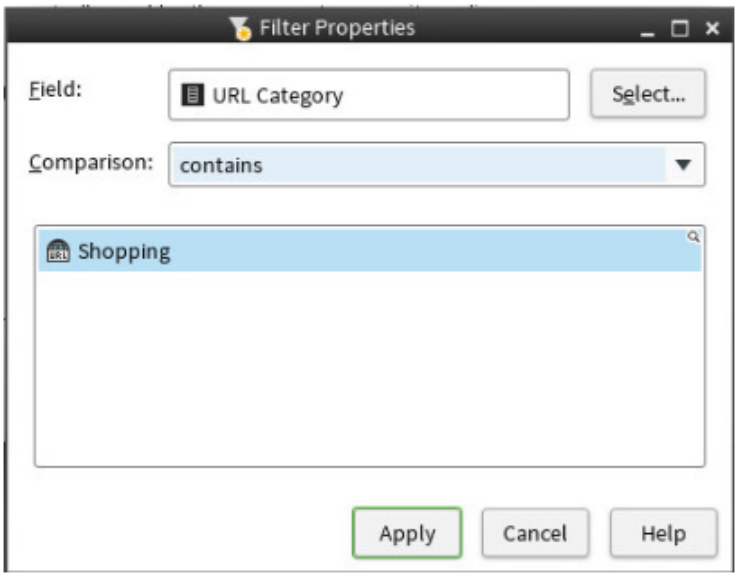


Figure 17.5: URL Category Filter for Shopping

3. Double-click on the **Shopping** URL category. Click **Apply**. The Filter Properties closes
4. Click **Apply** in the **Query** panel. A list of matching connections is displayed. A discard log should appear as in the figure below:

Figure 17.6: Blocked URL Category Log Entry

17.8 Whitelisting Shopping Sites

You will create a list of specific shopping sites that will be reached from your internal network. It is also possible to allow a specific users to access a specific shopping site if the NGFW is integrated with Active Directory using the ECA agent or the FUID agent.

1. With the **HQ Policy** still open for editing, right-click in the **ID** cell of the rule that blocks access to Shopping site and select **Add Rule Before**. A new empty rule is added
2. Drag **net-192.168.2.0/24** from a rule below into the **Source** cell
3. Drag **not Atlanta Internal Networks** from the rule below into the **Destination** cell
4. Click the **Service** cell
5. In the resource pane toolbar, click the **Up** button and browse to **URL List**
6. Right-Click the empty space and select **New URL List Application**
7. Configure the URL List Application with the following with the following properties:
   - Name: **Shopping URLs Whitelist**
   - URLs: `www.walmart.com`

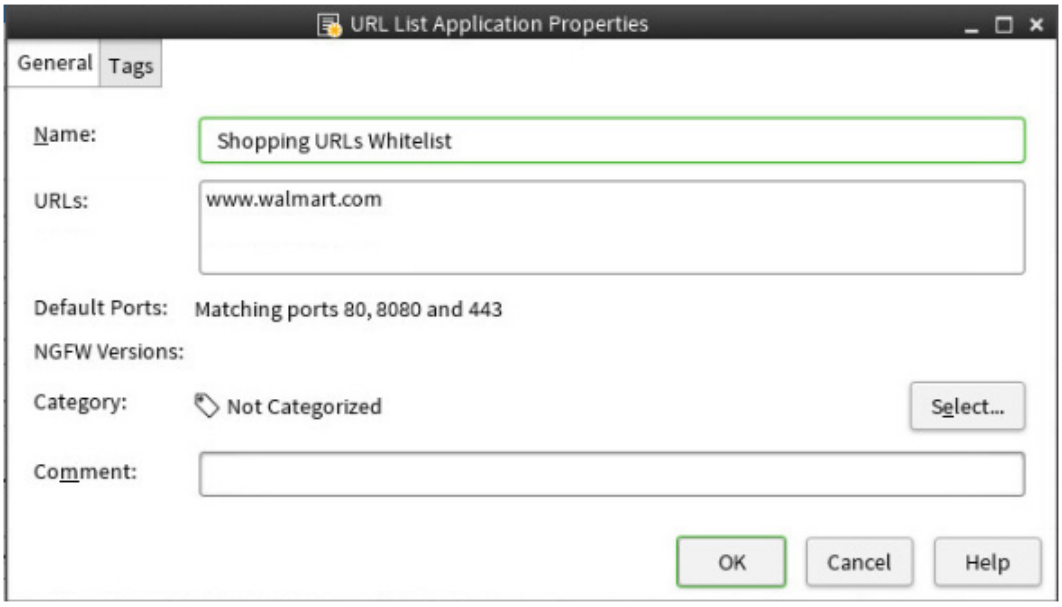


Figure 17.7: URL Whitelist Properties

8. Click **OK**
9. Drag and Drop the **Shopping URLs Whitelist** element into the **Service** cell

10. Right-click in the **Action** cell and select **Allow**. The completed Access rules should as in the figure below:

network-192.168.2.0/24	Not Atlanta internal network	Shopping URLs Whitelist	Allow
network-192.168.2.0/24	Not Atlanta internal network	Shopping	Discard

Figure 17.8: Completed Access Rules for URL Whitelisting

11. **Save and install** the policy
12. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

17.8.1 Test Access to Walmart from the Atlanta Server

1. Switch back to the console for the **Atlanta Server**
2. In Firefox, in the URL bar, enter `https://www.walmart.com`. Access is allowed.

17.9 Disable TLS inspection for URL Category

You will disable TLS inspection for banking sites to protect access to private information when an employee connects to a bank

1. With the **HQ Policy** still open for editing, right-click in the **ID** cell of the HTTP Proxy rule allowing outbound HTTP traffic and select **Add Rule Before**. A new empty rule is added
2. Drag **net-192.168.2.0/24** from a rule below into the **Source** cell
3. Drag **not Atlanta Internal Networks** from the rule below into the **Destination** cell
4. Click the **Service** cell. In the resource pane, browse to **URL category** → **Business and Economy** and drag **Financial Data and Services** into the **Service** cell
5. Right-Click the **Action** Cell and select **Allow**
6. Right-Click the **Action** Cell and select **Edit Options** The Select Rule Action Options dialog box opens
7. From the **Decryption** drop-down list, select **Disallowed**

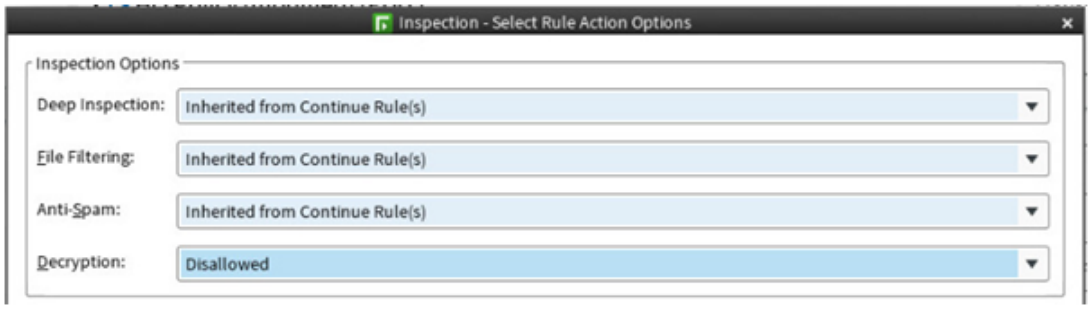


Figure 17.9: Disallowing Decryption in Action Options

8. Click **OK**. The completed Access rules should look appear as in the figure below:

network-192.168.2.0/24	Not Atlanta internal network	Shopping URLs Whitelist	Allow
network-192.168.2.0/24	Not Atlanta internal network	Shopping	Discard
network-192.168.2.0/24	Not Atlanta internal network	Financial Data and Services	Allow Decryption: Disallowed

Figure 17.10: Decryption Disallow Rule for URL Category

9. **Save and install**the policy
10. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

17.9.1 Test that Access to www.bankofamerica.com is not decrypted

1. Switch back to the console for the **Atlanta Server**
2. In Firefox, in the URL bar, enter `https://www.walmart.com`
3. In the URL bar, click the lock icon
4. Click the arrow on the right hand side
5. Check that the certificate used was generated by the Firewall

Figure 17.11: Walmart Certificate Signed By NGFW CA

6. In the URL bar, enter `https://www.bankofamerica.com`
7. In the URL bar, click the lock icon
8. Click the arrow on the right hand side
9. Check that the certificate used was generated by the original issuer

Figure 17.12: Bank of America Original Certificate

17.10 Summary

In this lab, you have used one of the Forcepoint Cloud-based Services, ThreatSeeker, to control URLs based on categories. You used various approaches to controlling URL access, such as blocking and whitelisting.