LAB 18

Optional Lab - Quality of Service

18.1 Getting Started

In normal network traffic conditions, temporary traffic peaks may occur. With most connections, slight delays are not noticeable to the user. However, some connections, such as streaming audio or video, are time-critical, and even minor delays are easily noticed in the quality of service.

Bandwidth management means creating policies that determine how the available network link capacity is divided between different types of communications, especially when the network is congested. Bandwidth management consists of guaranteeing a portion of bandwidth for a certain type of traffic or setting a limit for how much bandwidth a certain type of traffic is allowed to consume. You can use both guarantees and limits in the same QoS policy. Traffic prioritization is used to assign a priority to time-critical traffic. Normally, packets are sent out in the same order they were received regardless of the queue size. When you set priority levels for traffic, high priority packets bypass others when there is congestion and packets are queued. QoS rules are applied when traffic is exiting the firewall.

18.2 Define a QoS Policy

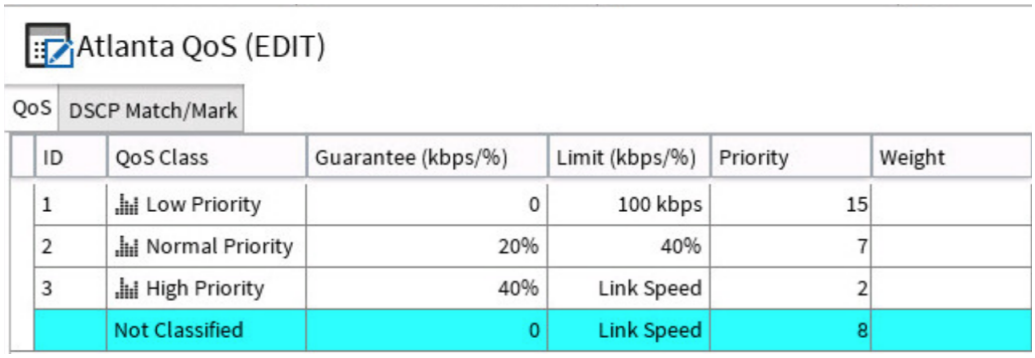
There are three default QoS classes: high priority, normal priority, and low priority. You will only use the three predefined QoS classes in this lab. Each QoS Class can appear only once in a QoS policy, so the order of the rules is not important.

1. From the **Home** view, click the **"+"** sign to open a new tab
2. Click **Configuration**. The **Configuration** pane opens
3. Browse to **NGFW** → **NGFW Engines** → **Policies** → **QoS Policies**
4. In the pane on the right, right-click and select **New QoS Policy**. The **QoS Policy Editor** opens. Name you QoS policy **Atlanta QoS**
5. Click **OK**. The **Atlanta QoS** opens for editing
6. Right-click on the **Not Classified** rule and select **Add Rule**. Configure the rule with the following values:
   - **QoS Class**: High Priority
   - **Gaurantee**: 40%
   - **Priority**: 2
7. Right-click in the **ID** column of the rule you just created and select **Add Rule Before**.
8. Configure the rule with the following values:
   - **QoS Class**: Normal Priority

- **Gaurantee**: 20%
- **Limit**: 40 %
- **Priority**: 7

9. Right-click in the **ID** column of the rule you just created and select **Add Rule Before**.
10. Configure the rule with the following values:
    - **QoS Class**: Low Priority
    - **Limit**: 100kbps
    - **Priority**: 15

    The completed QoS policy should appear as in the figure below:



ID	QoS Class	Guarantee (kbps/%)	Limit (kbps/%)	Priority	Weight
1	Low Priority	0	100 kbps	15	
2	Normal Priority	20%	40%	7	
3	High Priority	40%	Link Speed	2	
	Not Classified	0	Link Speed	8	

Figure 18.1: Completed QoS Policy

11. Click the **Save** icon to save your new QoS policy

    NOTE: In this lab, you use percentages and kbps values in the same policy to explore the capabilities of the QoS policy. In a production environment, it is not a good idea to mix the units because it makes the policy hard to read and may postpone automatic validity checks until the policy installation stage.

18.3 Organize the Policy Rules

Now that the number of policy rules is increasing, it is a good idea to organize them. In this exercize, you will create a sub-policy and create rule sections to create a more maintainable and organized policy.

1. From the **Home** view, right-click the **Atlanta FW Cluster** and select **Current Policy** → **Edit**. The **Atlanta FW Policy** opens for editing
2. Click in the **ID** column of the application rule for the **Helsinki Wordpress Website**
3. Holding down the shift key, click in the **ID** column of the last rule. Three rules are highlighted
4. Right-click in the **ID** column of the last rule, and select **Create Sub-Policy**
5. In the field of the dialog box that appears, enter **Atlanta Outbound Sub-Policy**. Click **OK**. The rules are collapsed into a jump rule
6. In the jump that is created, enter the following values:
    - Source: **net-192.168.2.0/24**
    - Destination: **not Internal Nets**

Your organized policy should appear as in the figure below

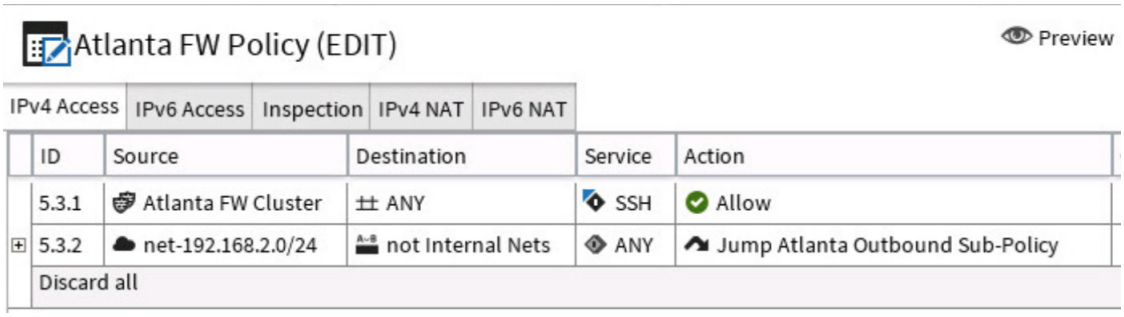


Figure 18.2: Addition of a Sub-Policy

18.4 Assigning QoS Classes to Traffic

QoS classes are linked to different types of traffic based on matches in the IPv4 Access rules. When the Access Rule matches, the QoS class specified in the QoS column of the rule is assigned to the traffic. To configure the Access Rules for QoS matches, follow the below steps.

1. With the **Atlanta FW Policy** still open for editing, right-click in the **Action** column of the jump rule you created above and select **Edit Sub-Policy Atlanta Outbound Sub-Polcy**. The policy editor opens
2. Right-click in the **ID** column of the rule that permits access the the **Helsink Wordpress Website**, and select **Copy Rule**
3. Right-click in the **ID** column of the same rule and select **Paste**
4. In the **Destination** and **Service** columns of the new rule, and select **Clear Cell**
5. In the **Destination** column of the rule, type `Paris`. In the list that appears, select **Paris Web Server (NAT)**
6. In the **Service** column, type `22`. Select **SSH** from the list that appears
7. In the **QoS Class** column, type `high` and select **High Priority**
8. Right-click in the **ID** of this rule, and select **Copy Rule**, then right-click in the **ID** column again and select **Paste**
9. Right-click in the **Destination** column and select **Clear Cell**. Right-click again and select **Set to ANY**
10. In the **Service** column of the new rule, right-click and select **Clear Cell**
11. Right-click again in the **Service** column and type `21`. Select **FTP** from the list that appears
12. Right-click in the **QoS Class** column and select **Clear Cell**. In the same cell, type `low` and select **Low Priority**
13. Right-click in the **QoS Class** column of the last rule, and type `normal` and select **Normal Priority**

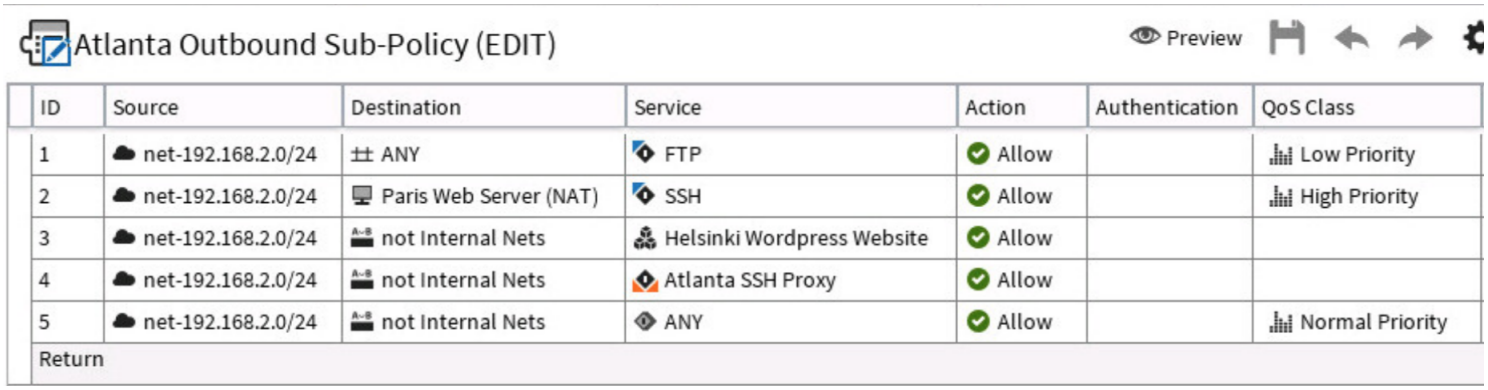


Figure 18.3: Modified Sub-Policy for QoS

14. Save your policy but do not install it. Close the tab where your policy is open for editing

18.5 Defining the QoS Settings for a Physical Interface

The firewall does not automatically know how much bandwidth its interfaces have or which QoS Policy to apply on which interface. You must define these values. Different QoS Policies can be defined for different Firewall interfaces. The requirements for external and internal interfaces are usually different. When Multi-Link is used, the link speed of external interfaces may vary.

To assign you QoS policy to a physical interface, follow the below steps.

1. Click the **Home** icon in the toolbar
2. Right-click on the **Atlanta FW Cluster** and select **Edit Firewall Cluster Atlanta FW Cluster**. The Engine Editor opens
3. On the left, click on **Interfaces**
4. Right-click on **Interface 1** and select **Edit Phyical Interface**. The Phyical Interface Properties dialog opens
5. Configure Interface 1 with the following properties:
    - QoS Mode: **Full QoS**
    - QoS Policy: **Atlanta QoS**
    - Throughput (kbps): **100000**
6. Click **OK** to close the Interface Properties
7. Click the **Save and Refresh** button to upload your QoS settings and firewall policy

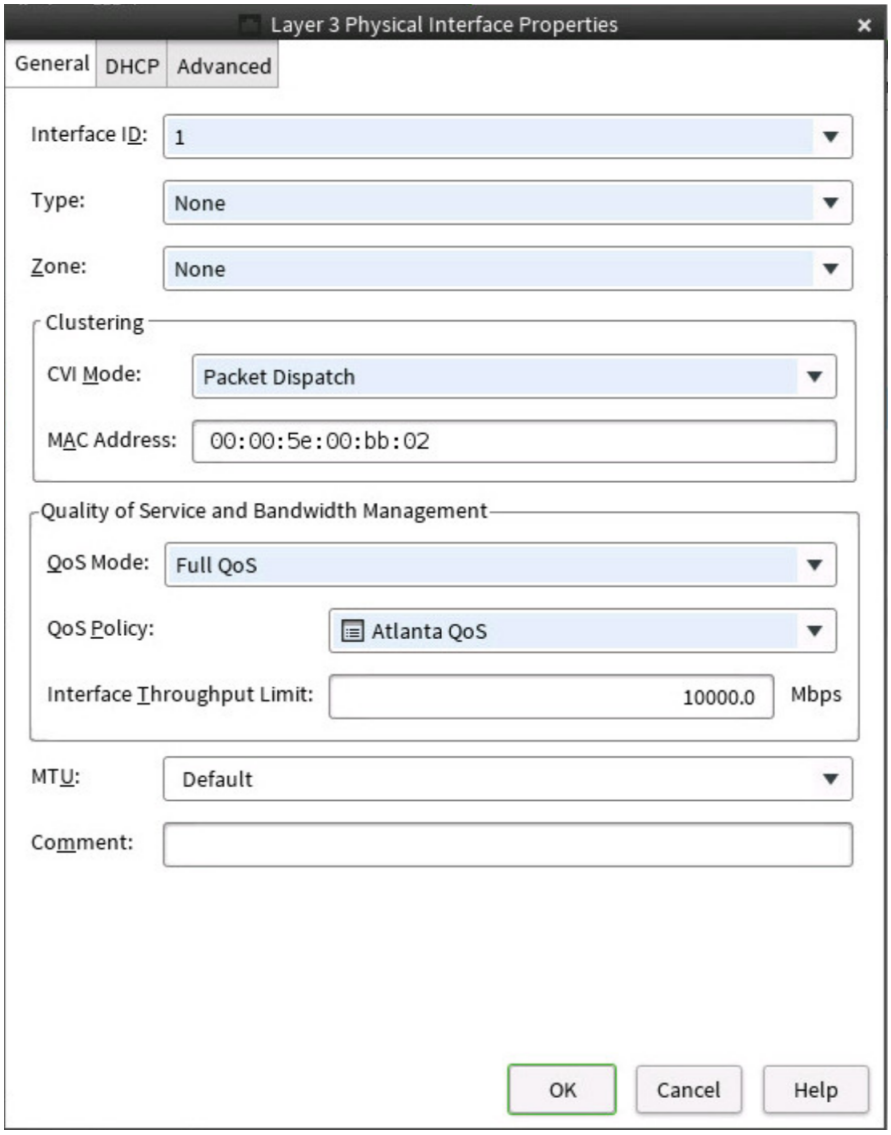


Figure 18.4: Application of QoS Policy to Interface

18.6 Testing the Outbound QoS Transfer Rate

You will now test your QoS policy by connecting to the Paris Server with **SSH** and **FTP**

18.6.1 Test the SSH Tranfer Rate with High Priority

1. Open a console to the **Atlanta-Server**, and click the **Terminal** icon on the bottom toolbar
2. Enter the following command: `scp /var/ftp/pub/bigfile_10M Student@172.31.3.101:.`
3. When you are prompted for the password, enter: **Forcepoint1!**

   NOTE: You may receive a prompt to accept the SSH key of the remote server. If you do, you may accept it.
4. Note that the transfer is fast

18.6.2 Test the FTP Transfer Rate with Low Priority

1. From the **Atlanta-Server** console click the termainal icon. At the command prompt, enter

   ```
   dd if=/dev/zero of=myfile.txt count=100 bs=1048576
   ```

2. From the **Atlanata-Server** console, open a terminal and enter `ftp 172.31.3.101`
3. Once connected, log in with the following credentials:
   - **User**: Student
   - **Password**: Forcepoint1!
4. At the ftp prompt, type `cd pub`
5. At the ftp prompt, type `hash`, followed by `put myfile.txt`
6. Note the painful slowness

18.7 Monitoring Traffic by QoS Class

Built into the SMC are monitoring tools that allow you to measure the effectiveness and performance of your QoS policy. Below are the steps for monitoring QoS.

1. Right-click the **Atlanta FW Cluster** → **Monitoring** → **Select**
2. In the window that appears, select **QoS Overview** and click the **Select** button. The **QoS Overview** opens

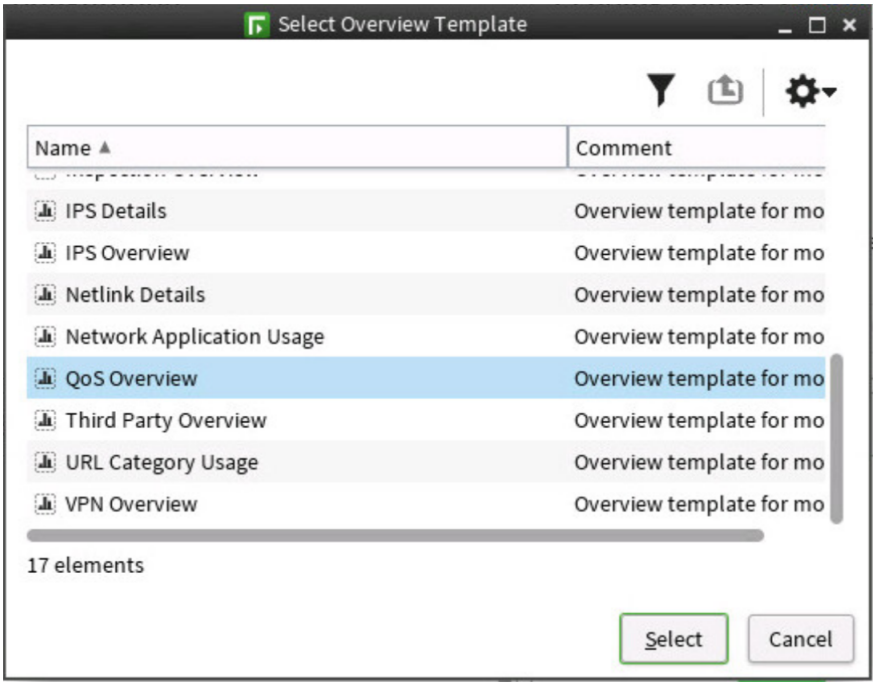


Figure 18.5: Qos Overview Selection

3. Double-click the title of any section to maximize it. Review the QoS related information. Verify that the tranfer rate matches the QoS settings you have defined

18.8 Summary

In this lab, you have configured bandwidth management and traffic prioritization to define how the available network link bandwidth is divided between different types of connections. You have created a QoS policy to make sure that important traffic is not delayed and time-critical communications have a guaranteed bandwidth.

LAB 19

Optional Lab - Inbound Traffic Management

19.1 Getting Started

As you have seen, the Forcepoint NGFW can load-balance outbound traffic using Mutli-Link. Multi-Link also provides a mechanism through which multiple IP addresses can be associated with a given domain name. Using server pools, multiple IP addresses can be associated with a given domain name such that a DNS query would return all of the IP addresses you have configured for your different ISPs.

In the event that one of the Netlinks becomes unavailable, the firewall can update the DNS record for your domain, removing the IP address associated with the failed link. In this way, the most accurate list of available IPs for a given domain is returned when a DNS query is performed.

In this lab you will configure a server pool that has two IP addresses associated with it - one from each ISP - and enable dynamic DNS updates so that in the event of a failure, the most accurate list of IP addresses is availble for your domain. To test this, you will simulate a link failure and observe the changes to the DNS record for your domain.

19.2 Define a Server Pool Element

To begin the process, you must define a server pool element. This element will be given an IP address from each of your Netlinks.

1. From the menu bar, click the **Configuration** icon and browse to **Network Elements** → **Traffic Handlers**
2. In the right-hand pane, right-click and select **New** → **Server Pool**. The Server Pool editor opens
3. In the **Name** field, enter **Atlanta Server Pool**
4. In the **External Addresses** field, click **Add**
5. In the window that appears, select **Atlanta ISP A Netlink** from the **Netlink** drop-down menu
6. In the **IP Address** field, enter **172.31.2.50**

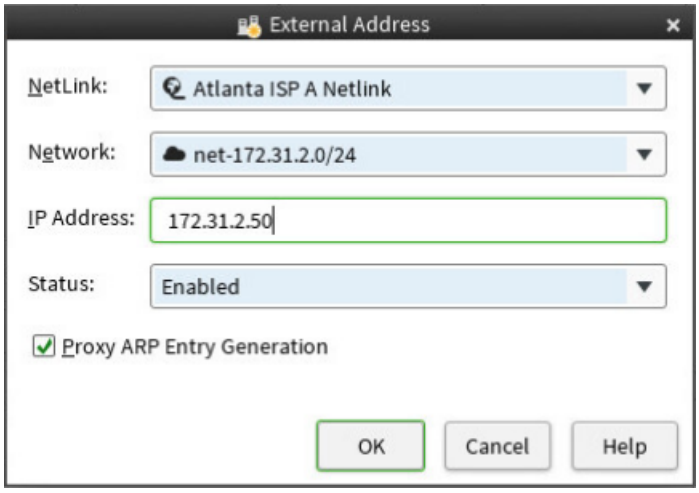


Figure 19.1: Netlink Selection for ISP A

7. Click **OK**
8. Click the **Add** button again. In the window that appears, select **Atlanta ISP B Netlink** from the **Netlink** drop-down menu
9. In the **IP Address** field, enter **10.1.2.50**

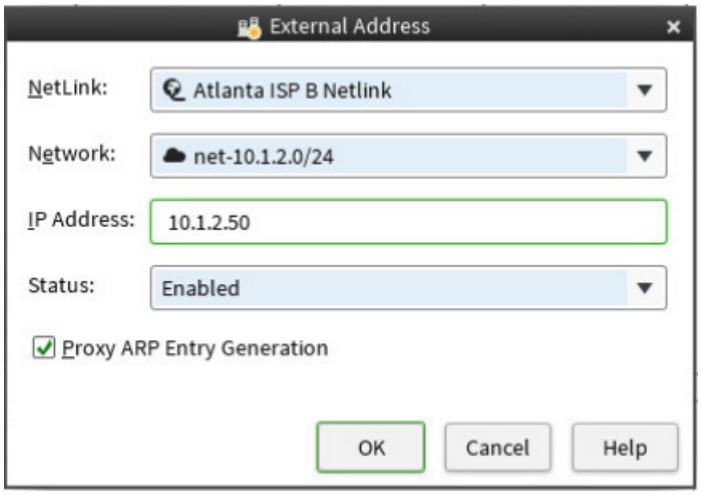


Figure 19.2: Netlink Selection for ISP B

10. Click **OK**. The External Address window closes
11. In the **Server Pool Properties** window, check the **Enable Dynamic DNS Updates** checkbox
12. In the **DNS Server** drop-down menu, select **Lab DDNS**

    NOTE: The **Lab DDNS** server is preconfigured. This is simply a DNS server based on **bind 9** or **named** that has the `allow-update` directive configured for your domain.
13. In the **Fully Qualified Domain Name** field, enter **www.atlanta.com**
14. In the **Server Pool Memebers** pane, click **Add**. The **Select Element** dialog opens
15. Browse to **Network Elements** → **Hosts**. Type the word **atlanta**
16. In the list of Atlanta related objects that appears, click on **Atlanta Web Server** and click **Select**

17. On the **Monitoring** tab, make sure the **Method** is set to **Ping**

    NOTE: This Server Pool only contains one server. If there is more than one server, the firewall will balance traffic according to the selection you make in the **Allocate Traffic to Servers by:** drop-down menu. Additionally, if there are multiple servers in the pool, the monitoring method specifies how the firewall ensures that the server pool members are up and able to receive new connections.

18. Click **OK**. Your compelted Server Pool should appear as in the figure below

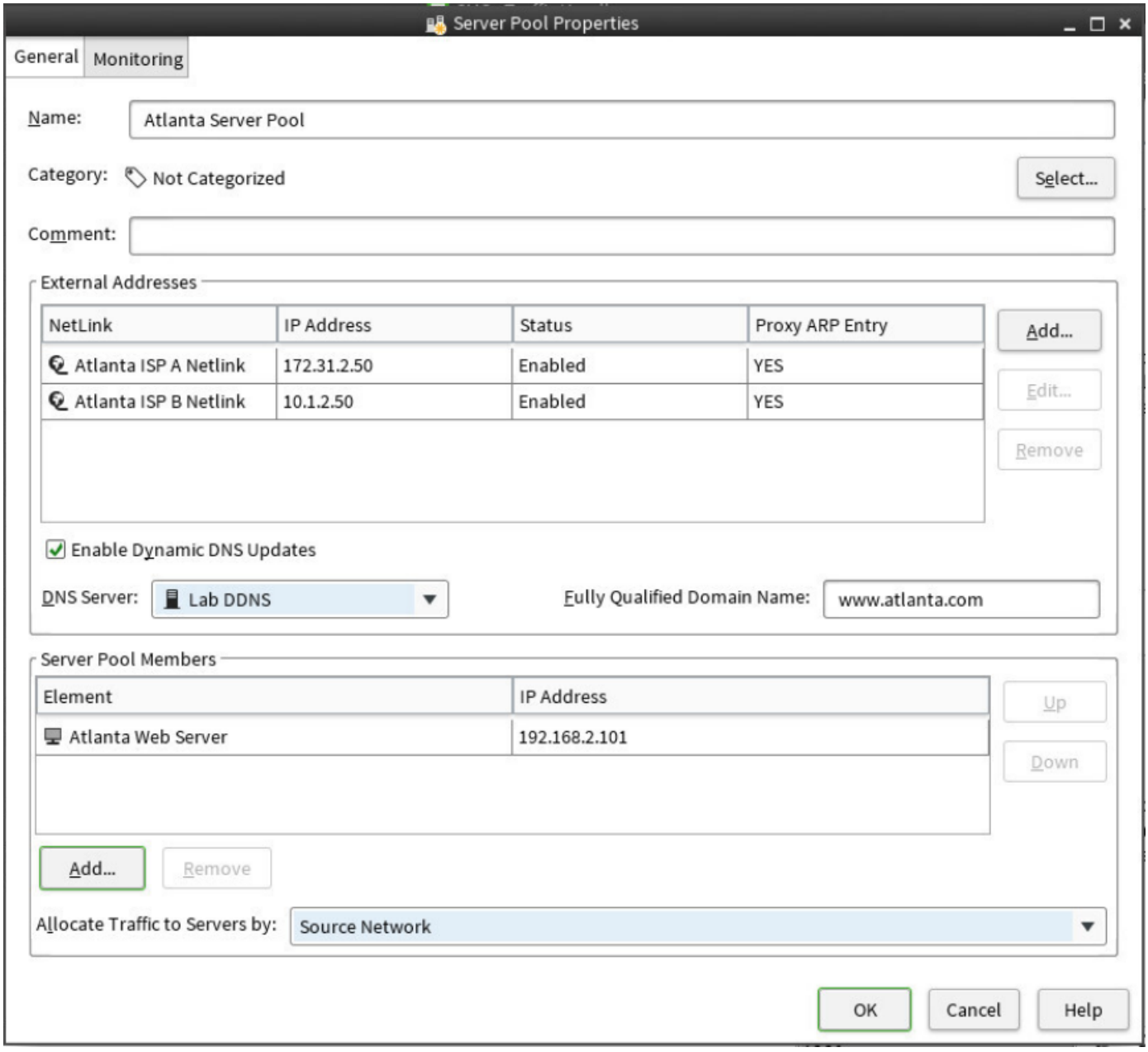


Figure 19.3: Completed Server Pool Configuration

19.3 Add an Access Rule to Allow Dynamic DNS Updates

In order for the firewall to send updates to a Dynamic DNS server, you must create an access rule that allows the firewall itself to send DNS traffic.

1. In the toolbar, click the **Home** button
2. Right-click on **Atlanta FW Cluster** and browse to **Current Policy** → **Edit**. The **Atlanta Policy** opens for editing
3. Right-click in the **ID** column of the rule that permits traffic to **Atlanta Web Server (NAT)** and select **Add Rule Before**
4. Configure the rule allowing DNS traffic from the firewall with the following values: **TIP**: Rather than browsing for the elements listed above, in any given cell, type the name of the object and a list of objects that match will appear. This saves time and makes it easier to find objects.
    - Source: **Atlanta FW Cluster**
    - Destination: **Lab DDNS**
    - Service: **DNS**
    - Action: **Allow**
5. In the **Logging** column of the rule you just created, right-click and select **Edit Logging**
6. In the window that appears, check the box beside **Overide Settings Inherited from Continue Rule**
7. Leave the **Log Level** set to **None**. Your completed rule should appear as in the figure below

Figure 19.4: Compeleted Firewall DNS Allow Rule

19.4 Add Access Rules for the Server Pool

Now that the Server Pool has been created, you must add access rules that allow traffic to it. When adding rules for Server Pools, NAT rules are not necessary. The NATing is done dynamically depending on the Server Pool member to which the inbound traffic is balanced.

1. In the tab where your policy is open for editing, right-click in the **ID** column of the rule that permits traffic to **Atlanta Web Server (NAT)** and select **Add Rule Before**
2. Configure the rule with the following values: **TIP**: Rather than browsing for the elements listed above, in any given cell, type the name of the object and a list of objects that match will appear. This saves time and makes it easier to find objects.
    - Source: **not Internal Nets**
    - Destination: **Atlanta Server Pool**
    - Service: **HTTP**
    - Action: **Allow**

    Your completed rule should appear as in the figure below

Figure 19.5: Completed Server Pool Rule

3. Click the **Save and Install** button. The policy upload begins

19.5 Test Inbound Traffic Management

So far you have configured a Server Pool that will update a dynamic DNS server should one of the ISP connections become unavailable. You will now access the Atlanta web site from the Paris site. You will then simulate a link failure by putting one of you netlinks offline and observe the changes in DNS resolution for www.atlanta.com.

1. From the **Landing Machine**, use the **vShpere Client** and open a console to the **Paris Server** VM
2. In the toolbar at the bottom, click the **Terminal** icon. A terminal window opens
3. At the command prompt, issue the following command: `watch -n 3 -x nslookup www.atlanta.com`. This will query DNS server of the Paris Server (172.31.200.101) every three seconds.
4. Note that `www.atlanta.com` resolves to two IP addresses, **172.31.2.50** and **10.1.2.50**. Leave this command running

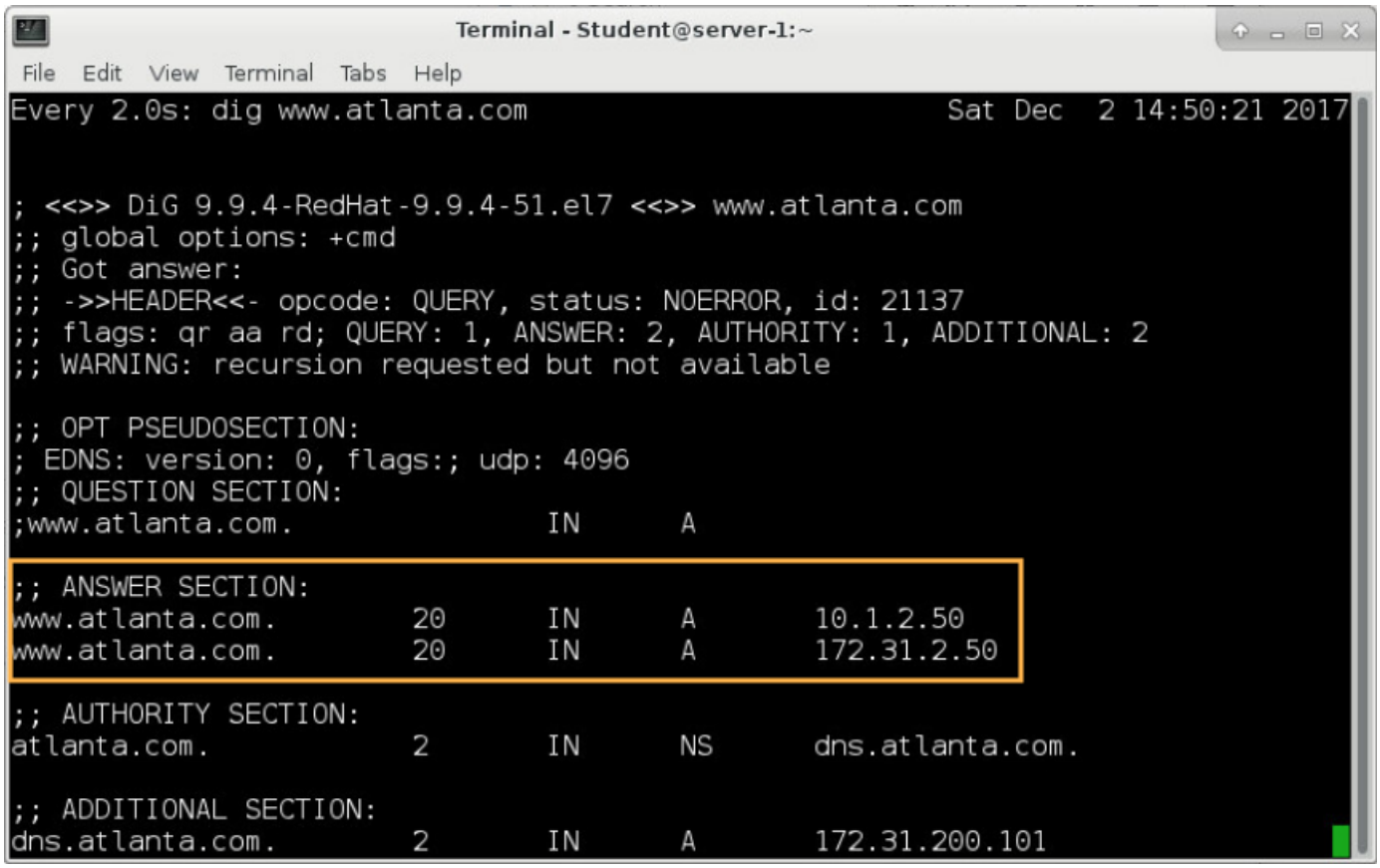


Figure 19.6: Address List for www.atlanta.com

NOTE: When DNS queries are performed, the order of the two IP addresses listed above changes. This is due to the DNS server.

5. In the **SMC Client**, right-click on the **Home** icon in the toolbar, and select **Open In New Tab**. The Home view opens
6. In the navigation column on the left of the Home view, click **Others**
7. In the **Multi-Link** section, browse to **Atlanta FW Cluster**. Click the ”+” sign to expand the available Netlinks
8. Right-click on **Atlanta ISP B Netlink** and browse to **Commands** → **Force Netlink Disable**. A new tab opens and the netlink is disabled. Click the **Close** button

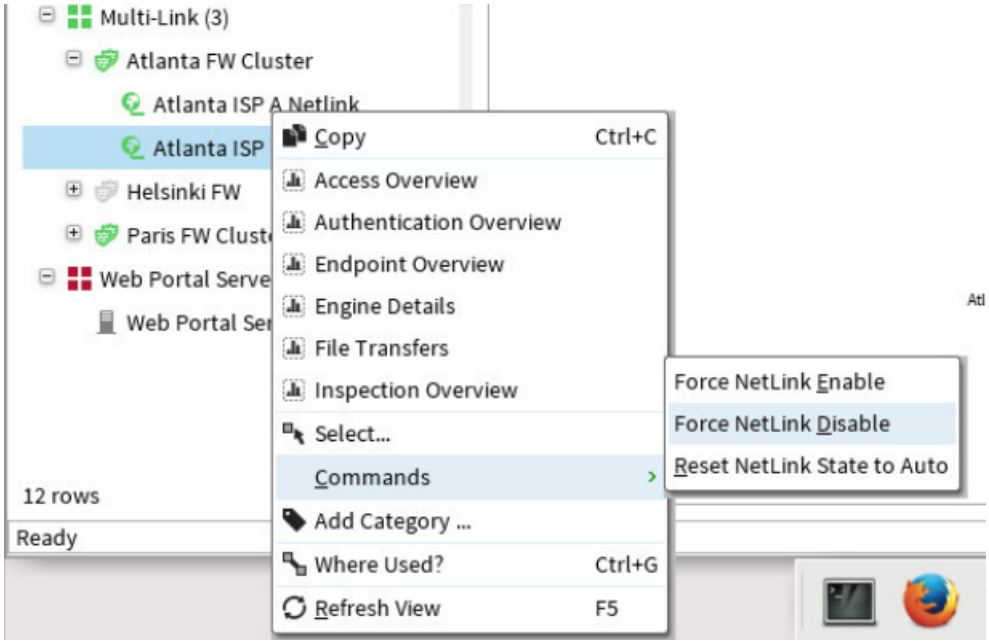


Figure 19.7: Disabling Atlanta ISP B Netlink

9. Return to the console window for the **Paris Server** where the `watch` command is still running. Note that *only* the IP address of **ISP A** is returned in the DNS query because the **Atlanta ISP B Netlink** is now disabled

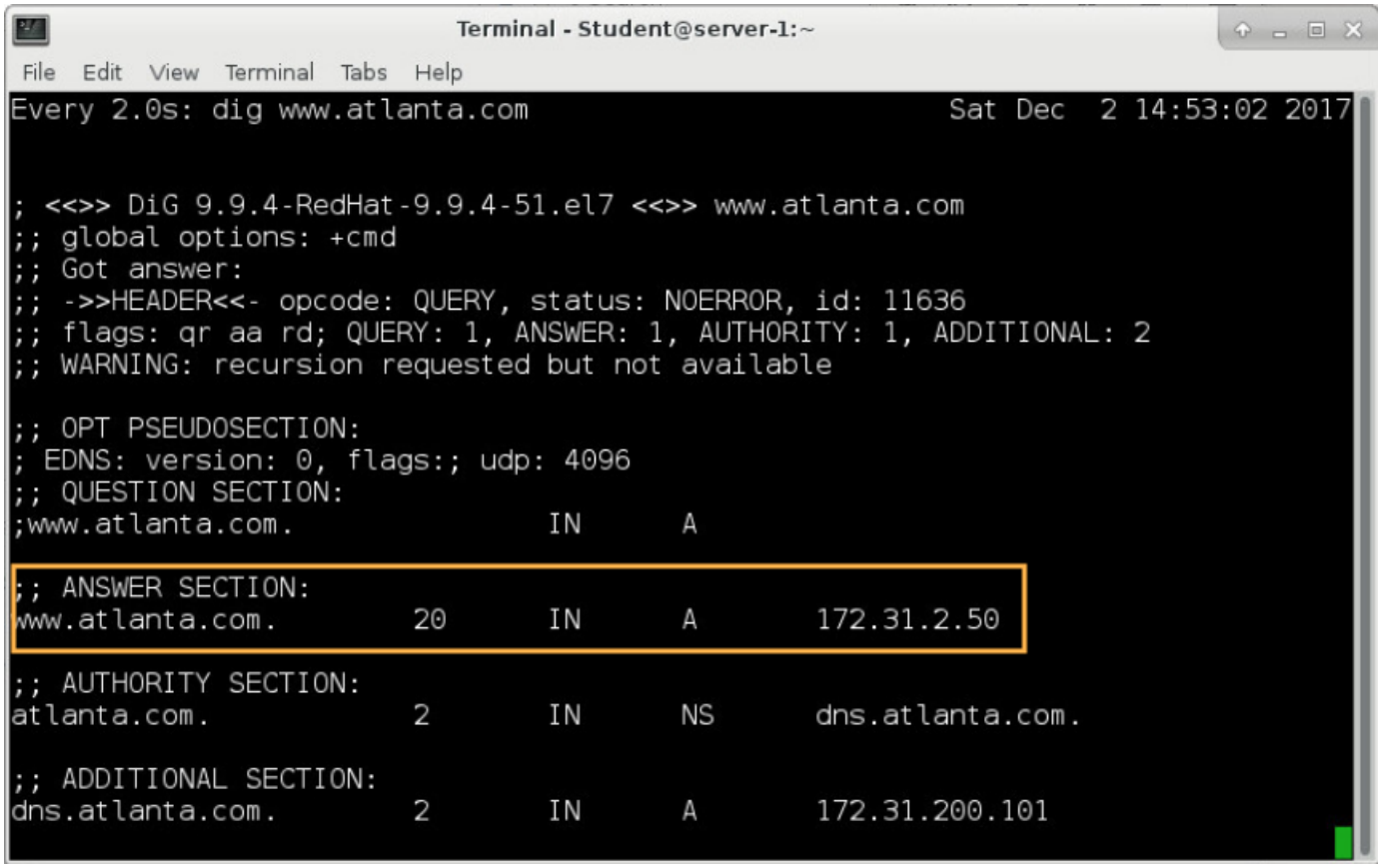


Figure 19.8: Updated Address List for www.atlanta.com

10. In the **SMC Client**, once again right-click on the **Atlanta ISP B Netlink** → **Commands** → **Reset Netlink State to**

Auto

11. Return to the console window for the **Paris Server** where the `watch` command is still running. Note that *both* the IP address of **ISP A** *and* **ISP B** are returned in the DNS query

To test how this would work when attempting to access a website, follow the steps below:

1. Return to the console window for the **Paris Server**. Click the **Firefox** icon to open a web browser
2. In the URL field, enter `http://www.atlanta.com` and press enter. The webpage for Atlanta opens
3. In the SMC Client right-click on **Atlanta ISP B Netlink** and browse to **Commands** → **Force Netlink Disable**. A new tab opens and the netlink is disabled. Click the **Close** button
4. Return to the console window for the **Paris Server**. Hold down the SHIFT key, and click the **refresh** button. The Atlanta web page is still available
5. In the **SMC Client**, once again right-click on the **Atlanta ISP B Netlink** → **Commands** → **Reset Netlink State to Auto**

19.6 Summary

In this lab, you have created a server pool that allows you to use IP addresses from your availble ISPs to reach your web server. Using the firewall's ability to update a dynamic DNS server, any link failure results in a DNS lookup that only returns the IP addresses of the links that are still available.

LAB 20

Optional Lab - SMC High Availability

20.1 Getting Started

A Management Server and a Log Server are required for configuration changes to and system monitoring of engines. Although engines work independently without the SMC according to their installed configuration, configuration changes and system monitoring are not possible without a Management Server and Log Server. The Management Server in particular is a critical component, as it is the only place where the full configuration information is stored.

You can install additional Management Servers and Log Servers. The high availability (HA) solution includes automatic incremental replication of the configuration data stored on the Management Server. This way, manual intervention is minimized, and the SMC can be fully managed and monitored without manually reinstalling and restoring a backup.

20.2 Define a New Management Server

To start the process of setting up Management Server High Availability, you must first define a new Management Server. Any newly defined Management Server is considered an additional Management server and is used for High Availability. To define a new Management Server, follow the below steps.

1. From the toolbar, click **Configuration** and browse to **Administration** → **Licenses** → **Servers** and verify that the Management Server license shows two IP addresses, **172.31.200.101** and **192.168.3.101**
2. From the same view, browse to **Network Elements** → **Servers**
3. Right-click **Servers** and browse to **New** → **Management Server**. The **Management Server Properties** opens
4. Configure the new Management Server with the following properties:
   - **Name**: HQ Backup Management
   - **IPv4 Address**: 192.168.3.101
   - **Log Server**: select **Log Server 172.31.200.101** from the drop-down list

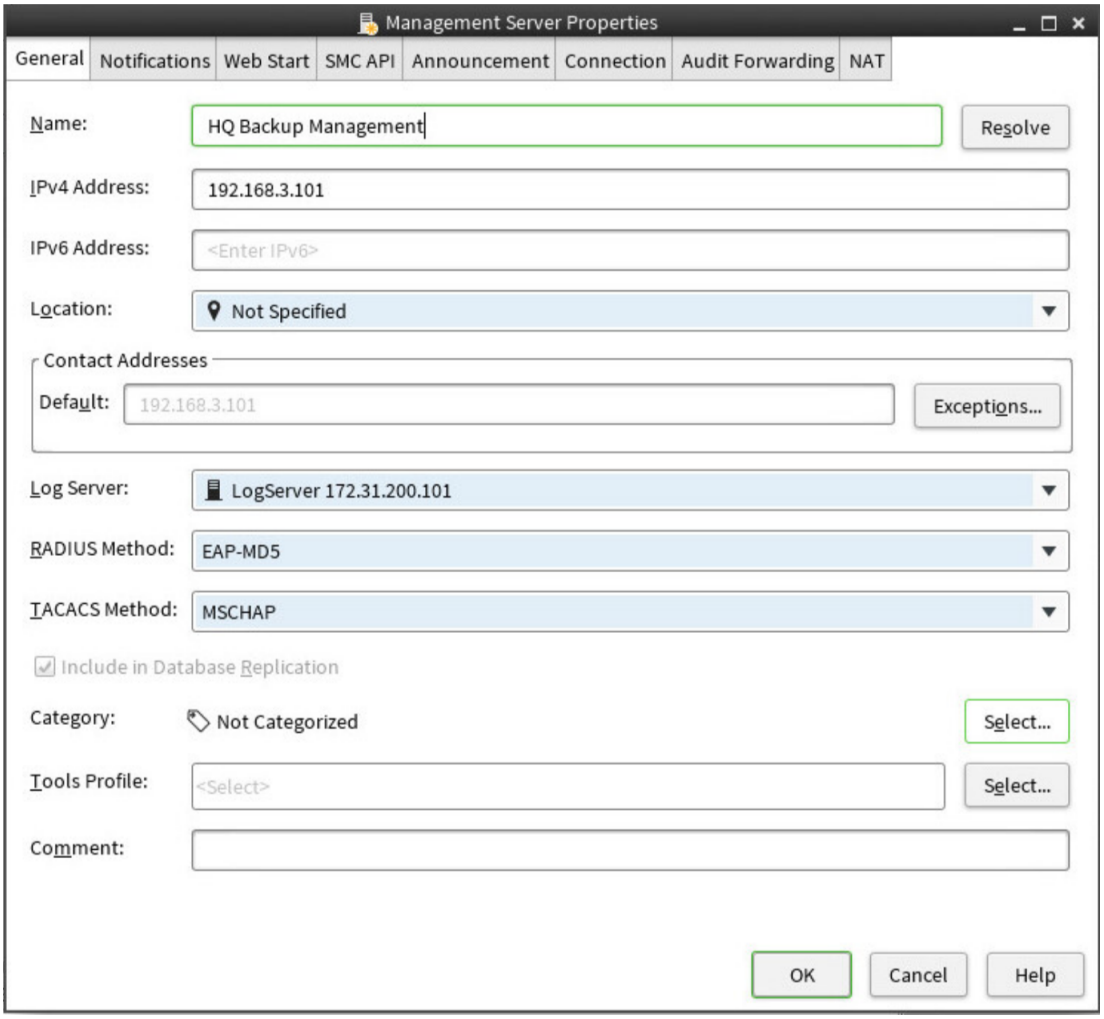


Figure 20.1: New Management Server Properties

5. Click **OK**

   NOTE: You may receive a warning that the new management server has the same IP as the Paris Web Server. This does not represent an IP conflict. This warning lets you know that there is another object with the same IP address. You may click **OK**.

6. From the same view, browse to **Administration** → **Licenses** → **Servers**. Note that the new Management Server is correctly associated with the Management server license

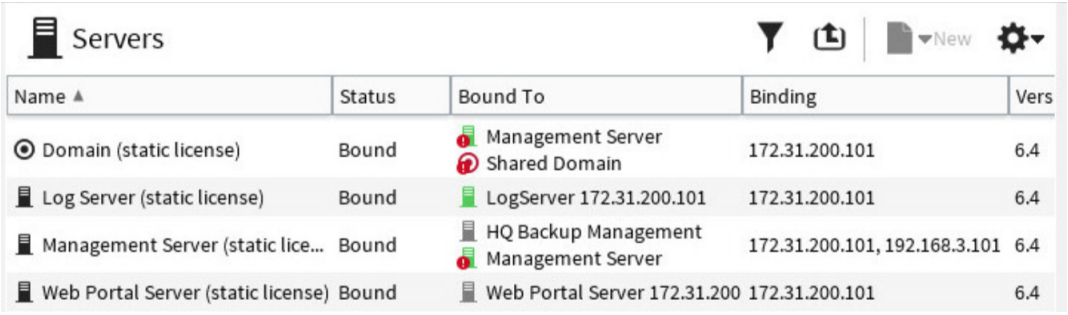


Figure 20.2: HQ Backup Management Correctly Licensed

NOTE: The red exclamation mark on the original Management Server simply means that it has not yet replicated to

the newly defined HQ Backup Management server.

20.3 Access Rules Permitting Management Communication

Because the new Management Server that we have created is at the Paris location and the Paris FW Cluster is in front of it, access rules are necessary to allow communication to the new backup Management Server. While the rules to allow this are preconfigured for this lab environment, please note these rules for future deployments. To view these rules, follow the below steps.

1. In the Management client, right-click the **Home** button and select **Open in New Tab**. The home view opens
2. Right-click the **Paris FW Cluster** and browse to **Current Policy** → **Preview**. The Paris FW Cluster policy opens in read-only mode
3. Expand the rule section **Management Rules** by click the small "**+**" sign
4. Note rules **5.4** through **5.6**. These allow communication between the primary and backup management servers so that they may replication their databases. These also allow the firewalls to communicate with the backup Management Server

Management Rules				
5.3	SMC Client	Paris Web Server	Ping SG Client to Log SG Client to Management	Allow
5.4	Management Server Paris Web Server	Management Server Paris Web Server	SG Control SG Status Monitoring	Allow
5.5	Paris Web Server	Global Firewalls	SG Management to Firewall	Allow
5.6	Global Firewalls	Paris Web Server	SG Engine to Management	Allow

Figure 20.3: Access Rules for SMC High Availability

NOTE: The **Paris Server** object is the same server that hosts the new backup management server.

20.4 Install the SMC Software on the Backup Management Server

You will now install the SMC software on the Paris Internal Server. This server will serve as the backup management server.

1. From the **Landing Machine**, use the **vSphere** client to open a console to the **Paris-Server**
2. At the bottom of the desktop, click the **Terminal** icon. A terminal opens
3. At the command prompt, type `su root`, enter the password `Forcepoint1!` and press enter
4. At the command prompt, type `cd Downloads` and press enter
5. Then type `unzip smc_6.3.0_10417_linux.zip -` and press enter. The SMC software will unpack from the zip archive
6. At the command prompt, type `cd smc_6.3.0_10417_linux/Forcepoint_SMC_Installer/Linux-x64` and press enter
7. Now type `./setup.sh` and press enter. The SMC software installation begins
8. When installation begins, select the language as **English** and press **OK**. In the next prompt, click **Next**
9. When prompted, accept the **License Agreement** and click **Next**
10. You will then be prompted for the installation directory location. You may accept the default and click **Next**. Click **Next** in the prompt that follows

11. Accept the default **Shortcuts** directory by clicking **Next**
12. When prompted for **Select Components to be Installed**, select **Custom**

Figure 20.4: Custom mode SMC Software Installation for HA

13. Click **Next**
14. When prompted for the components to install, deselect all components *except* **Management Server**

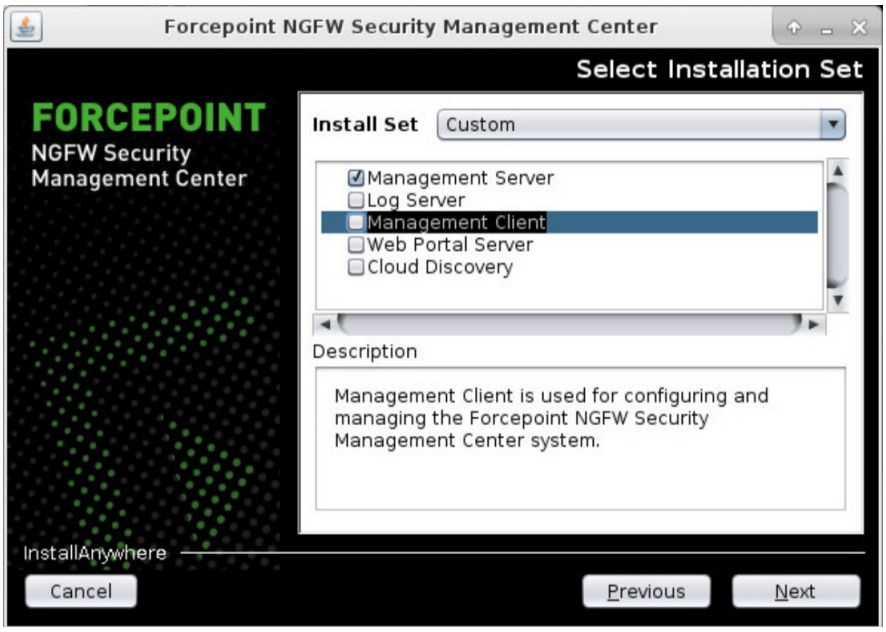


Figure 20.5: Management Server Component Selection

15. Click **Next**
16. By default, the IP address of the server is selected for the **Management Server IP Address**. Verify that it is selected as **192.168.3.101**

17. In the **Log Server IP Address** field, enter **172.31.200.101**
18. Select **Install as an Additional Management Server for High Availability**
19. Leave **Install as a Service** selected

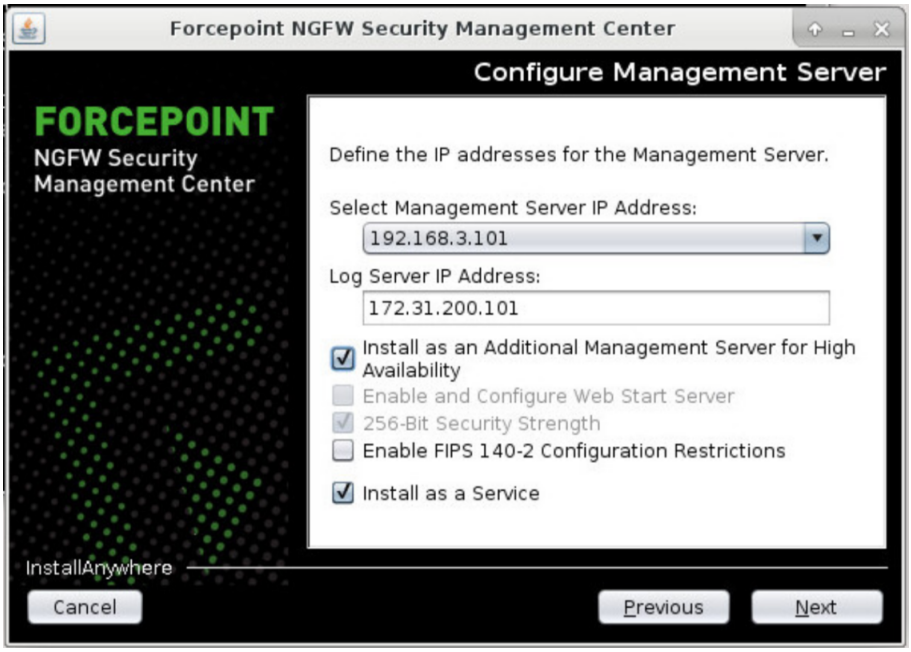


Figure 20.6: New Management Server Detailed Configuration

20. Click **Next**
21. In the **Pre-Installation Summary** prompt, press **Install**. The SMC Software installs
22. You will be prompted for the current Management Server credentials. Enter the following credentials to connect to the existing SMC:
    - **User Name**: root
    - **Password**: Pass1234
    - **Active Management Server**: 172.31.200.101
23. Click **OK**
24. When prompted, click **Accept** to accept the Management Server fingerprint

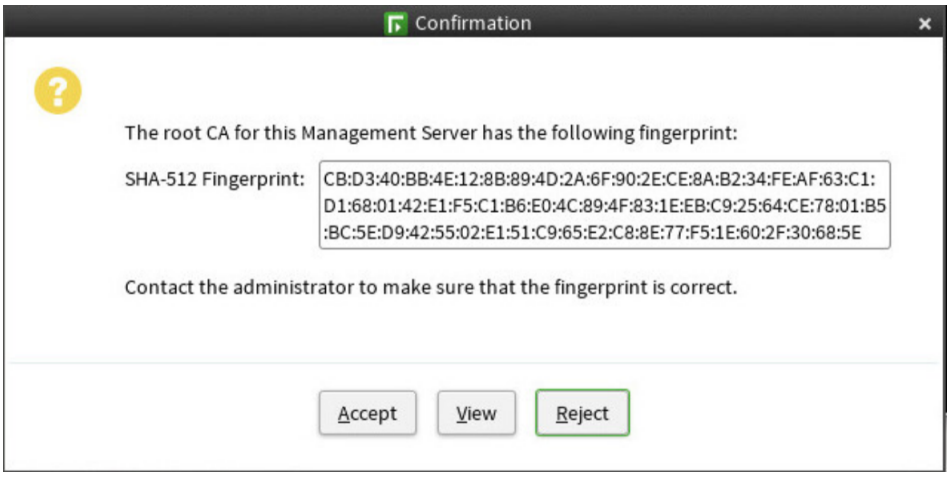


Figure 20.7: Backup Management Server Connecting to Primary SMC

25. A prompt appears, ensure that the **Use Existing Management Server** is selected
26. Click **OK**
27. A message confirming that the certificate was generated appears. Click **OK**
28. The Management Server software installation completes. Click **Done**. The installer closes

20.5 Confirm Replication of Primary SMC Database to Standby Server

After the installtion of the SMC software on the standby server, the primary management server database replicates to the newly installed backup SMC. You will now confirm that the replication was successful.

1. Using the Management Client, click on the **Menu** icon and browse to **System Tools** → **Control Management Servers**

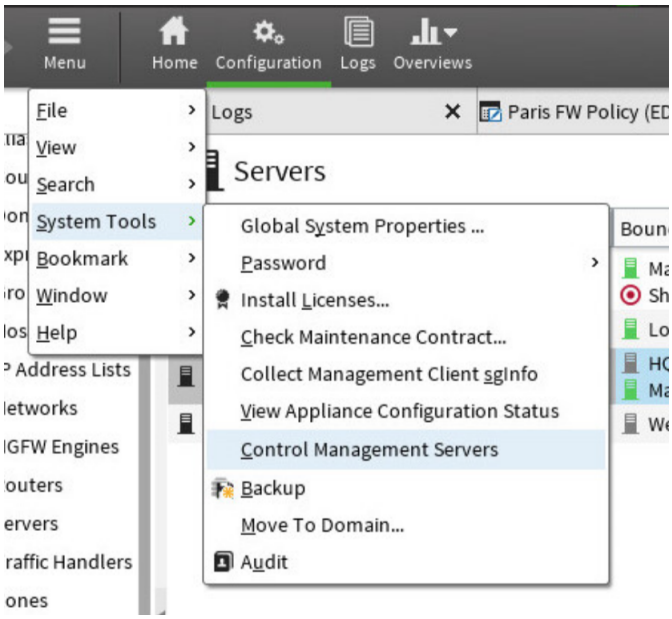


Figure 20.8: Controlling Management Servers

2. When the **Control Management Servers** dialog opens, you should see something similar to the figure below

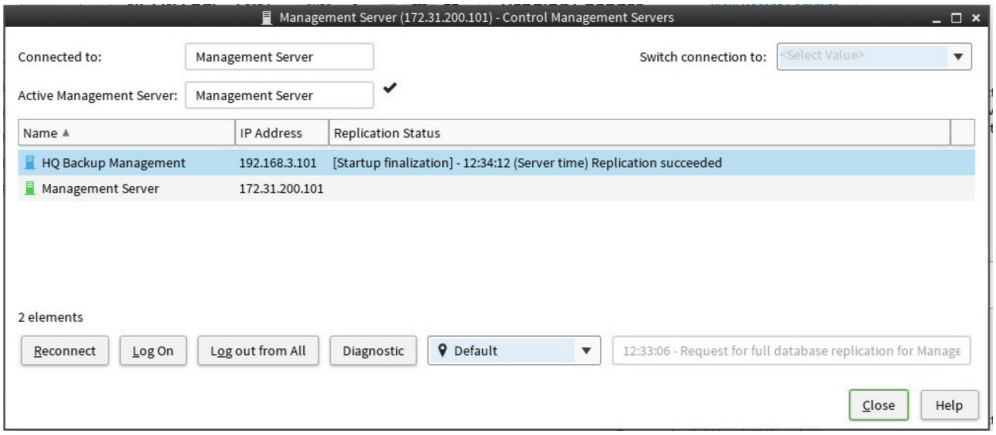


Figure 20.9: Successful Management Server Database Replication

3. Click **Close** to exit the **Control Management Servers** dialog

IMPORTANT: At this point make sure to refresh the policy on all firewalls to ensure that all firewalls under management are aware of the backup SMC

20.6 Testing Management Server Failover

To ensure that the primary management server can fail over properly in the event of a failure, you will now set the backup management server that you have created as the primary. To do this, follow the below steps.

1. Make sure that there are no policies or engines open for editing
2. Close the **Management Client**
3. From the **Landing Machine**, use **Firefox** to open a connection to the Management Server by clicking **Start Management Client**. Java Webstart downloads and runs the management client
4. When you are presented with the SMC Logon prompt, click **Add Server**. Enter the backup management server IP address, **192.168.3.101**
5. Click the "**+**" sign to add the IP address of the backup management server

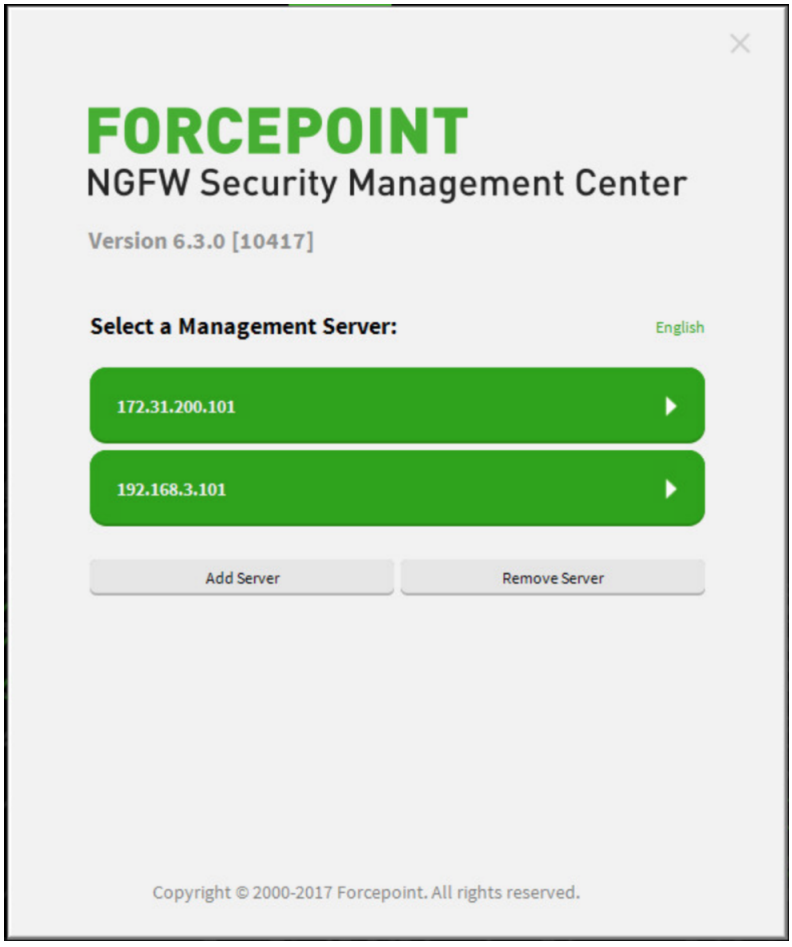


Figure 20.10: Preparing to Login to Backup Management Server

6. When the new IP is added, click the arrow on the right to login. Supply the following credentials:
   - **User**: root
   - **Password**: Pass1234
7. Click the **Logon** button. You will be logged into the **HQ Backup Management** server

8. On the toolbar at the top, click **Menu** and browse to **System Tools** → **Control Management Servers**. The **Control Management Servers** dialog opens

9. Right-click on the **HQ Backup Management** and select **Set Active**. When prompted to give full control of all domains to the **HQ Backup Management**, click **Yes**

10. A message appears confirming that the **HQ Backup Management** is now the primary management server appears. Click **OK**. The **HQ Backup Management** is now the primary management server

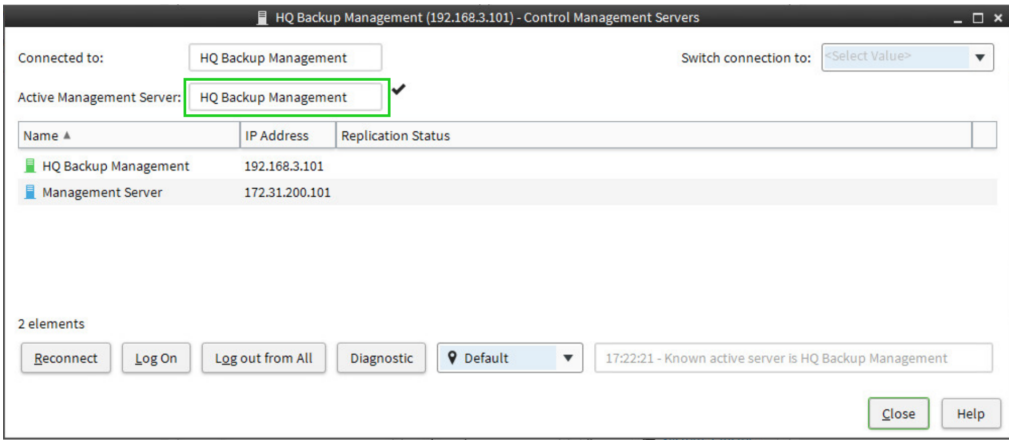


Figure 20.11: HQ Backup Management set to Primary

11. You may close the **Control Management Servers** dialog by clicking **Close**

20.7 Switch Back to Primary Management Server

Now that you have successfully switched over to the HQ Backup Management server, you must now switch control back to the primary. To do this, follow the below steps.

1. Close the **Management Client**

2. From the **Landing Machine**, use **Firefox** to open a connection to the Management Server by clicking **Start Management Client** Java Webstart downloads and runs the management client

3. Click the arrow to the right of **172.31.200.101**. The management client downloads

4. When prompted, logon to the Management Server with the following credentials:

   - **User**: root
   - **Password**: Pass1234

5. Click **Logon**. The Management Client opens and you are connected to the original Management Server

6. On the toolbar at the top, click **Menu** and browse to **System Tools** → **Control Management Servers**. The **Control Management Servers** dialog opens

7. Right-click on the **Management Server** and select **Set Active**. When prompted to give full control of all domains to the **HQ Backup Management**, click **Yes**

8. A message appears confirming that the **Management Server** is now the primary management server appears. Click **OK**. The **Management Server** is now the primary management server

20.8 Summary

In this lab, you have installed the SMC software on a server that is outside of the HQ environment and configured it as a backup maanagement server. From the HQ Management server, you have seen that once configured, the primary SMC replicates its database to the new backup. Your new backup management server is ready to be used in the event of failure or maintenance.

LAB 21

Optional Lab - Dynamic Routing

Getting Started

In this lab, BGP will be used as external gateway protocol between Atlanta Firewall and Router ISP B. You will configure Atlanta Firewall and ISP B Router as BGP Peer to distribute routing information to each other. Atlanta Firewall and Router ISP B will belong to the same autonomous system.

The route redistribution will be limited to distribute a specific route from ISP B Router to Atlanta Firewall. You are going to add a loopback address to ISP B Router and configure ISP B router to distribute the route path to reach this new network to the Atlanta Firewall using the BGP protocol.

By default, the Atlanta Firewall own traffic is routed to ISP A router, its default gateway. With the new BGP route, the connections to the loopback address of the ISP B Router from the Atlanta Firewall will be routed directly to the ISP B router.

21.1 Configure BGP for Atlanta Firewall

You will now enable the BGP protocol in the engine properties and define the autonomous system that Atlanta Firewall belongs to. Then you will update the Atlanta Firewall routing definition by adding the ISP B router as BGP Peer behind the interfaces that will propagate the new route path.

1. Click the tab where the **Atlanta FW Cluster** view is open for editing
2. Select **General** and browse to **Clustering**
3. Click **Clustering Mode** drop-down list and select **Standby**
4. Select **Routing** and browse to **Dynamic routing**
5. Select**Enabled** in the**BGP** panel
6. Click **Autonomous System** drop-down list. Click **Select.** The **Select Properties** dialog opens
7. Right-click the empty panel and select **New** → **Autonomous System**
8. Define the following settings and click **OK**
   - Name: **ISP B AS**
   - Autonomous System Number: **60000**
9. Click **Select**

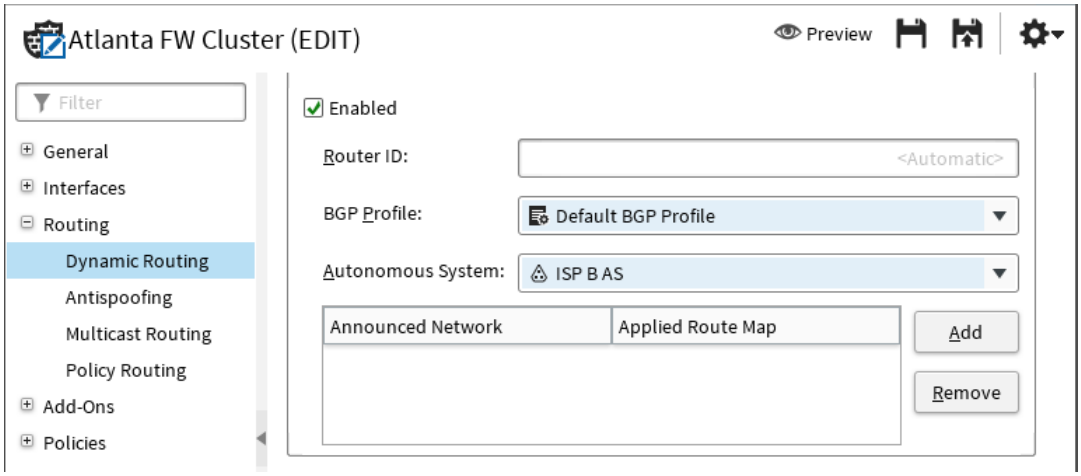


Figure 21.1: Enabling Dynamic Routing

10. Browse to **Routing**
11. Expand the **Interface 2**
12. Right-click **net-10.1.2.0/24** and select **Add BGP Peering**. The**Select Element(s)** properties opens
13. In the **Resources** pane, right-click **New BGP Peering**
14. Name the BGP Peering:**ISP B – Atlanta BGP Peering.** Click **OK**
15. Select the **ISP B - Atlanta BGP Peering** by adding the **ISP B - Atlanta BGP Peering** in the **Select Element(s)** properties. Click **OK**

    NOTE: In this exercise, Atlanta Firewall and ISP B Router will see each other as external BGP Peers even if you would normally define them as Firewall e.g. BGP Peers internal to the system.
16. Expand the **Interface 2**
17. Right-click **ISP B - Atlanta BGP Peering** and select **Add External BGP Peer.** The **Select Element(s)** properties opens
18. In the **Resources** pane, right-click **New** → **External BGP Peer**
19. Define the following settings and click **OK**
20. - Name: **ISP B BGP Peer**
    - IP Address: **10.1.2.110**
    - Autonomous System Number: **ISP B AS**
21. Add the **ISP B BGP Peer** and Click **OK**

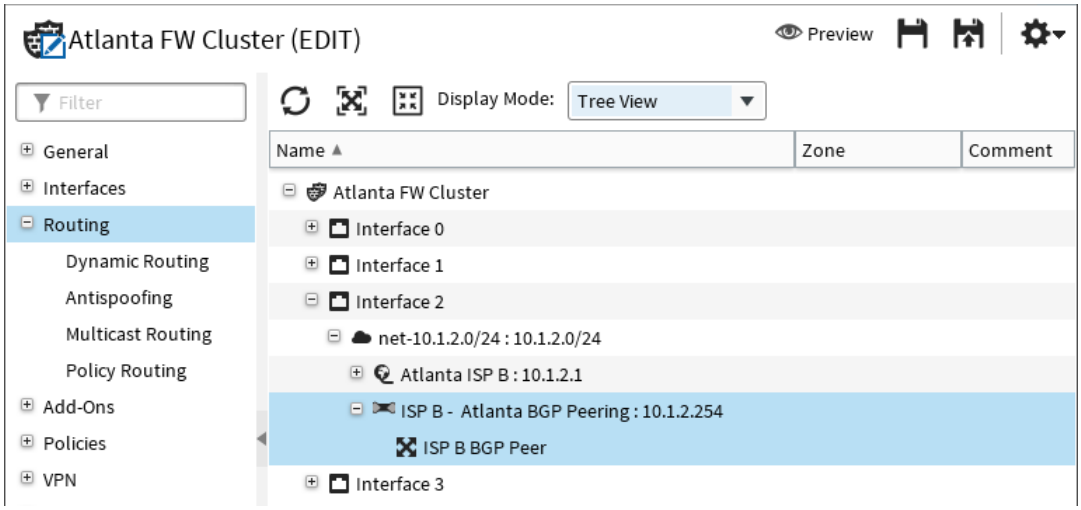


Figure 21.2: BGP Peering - Routing View

22. Browse to **Policies** → **Automatic Rules**
23. Click the **Logging Level for Automatic Rules** drop-down list
24. Click **Stored**
25. Click **Save and refresh Policy** icon in the Engine Editor Toolbar and upload the **Atlanta Policy** to the **Atlanta FW Cluster**
26. Close the **Upload Policy: Atlanta Policy** tab when the policy upload is completed

21.2 Configure a Loopback Interface for ISP B Firewall

1. In the tab where the **Configuration** view is open, browse to **NGFW** → **NGFW Engines** → **Router ISP B**
2. Right-click the **Router ISP B** and select **Edit Router ISP B** for editing the Firewall in a new tab
3. Browse to **Interfaces** → **Loopback**
4. Click **Add** below to the **Loopback Address** table
5. Type**172.16.58.101** in the new row, in the **Loopback Address** column

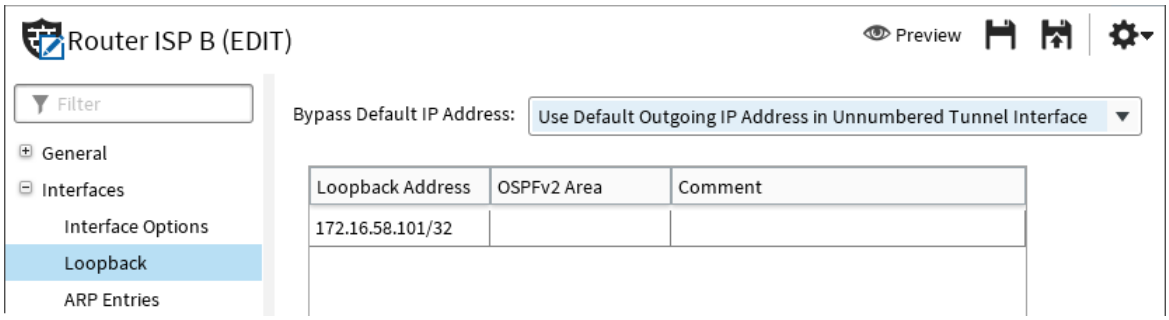


Figure 21.3: Loopback Interface Configuration for BGP

21.3 Configure BGP for ISP B Firewall

1. Browse to **Dynamic routing**
2. Select **Enabled** in the **BGP** panel
3. Click **Autonomous System** drop-down list and select **ISP B AS**
4. Click **Add** next to the **Announced Network** table
5. Right-click **Select** in the empty cell in the **Announced Network** column
6. Click **Network** and select **net-172.16.58.0/24**

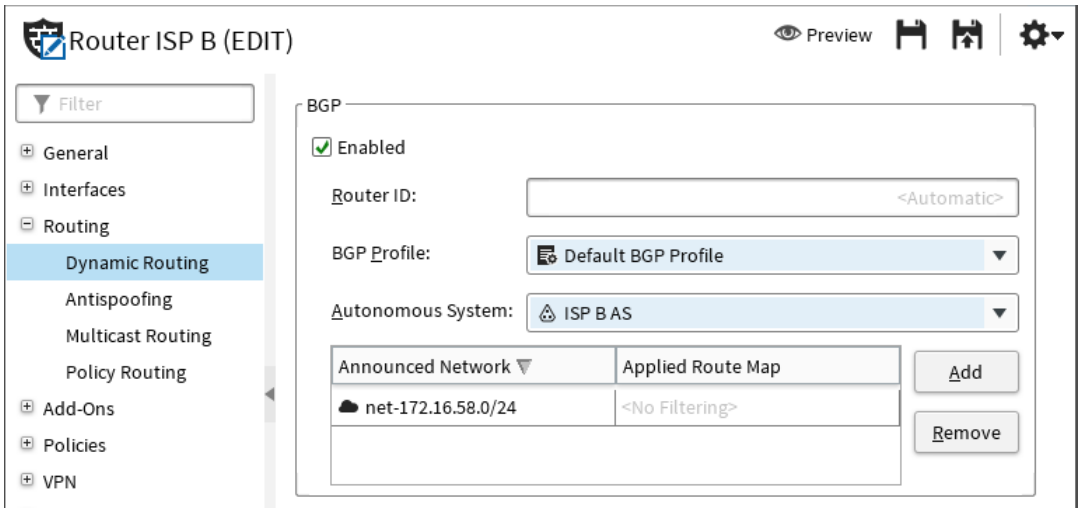


Figure 21.4: Enabling BGP on ISP B Firewall

7. Browse to **Routing**
8. Expand the **Interface 1**
9. Right-click **net-10.1.2.0/24** and select **Add BGP Peering**
10. Select the **ISP B – Atlanta BGP Peering** by adding the **ISP B – Atlanta BGP Peering** in the **Select Element(s)** properties dialog. Click **OK**
11. Expand the **Interface 1**
12. Right-click **ISP B - Atlanta BGP Peering** and select **Add Firewall**
13. Select the **Atlanta FW Cluster** by adding the **Atlanta FW Cluster** in the **Select Element(s)** properties dialog. Click **OK**

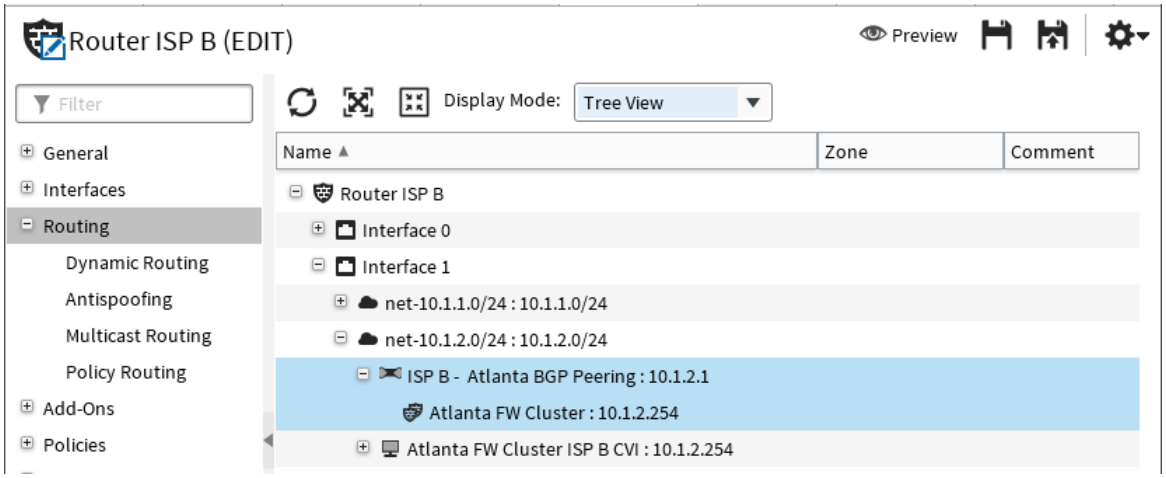


Figure 21.5: Router ISP B Routing Table - BGP

14. Browse to **Policies** → **Automatic Rules**
15. Click the **Logging Level for Automatic Rules** drop-down list
16. Click **Stored**
17. Click **Save and refresh Policy** icon in the Engine Editor Toolbar and upload the **Router Policy** to the **Router ISP B**
18. Close the **Upload Policy: Router Policy** tab when the policy upload is completed
19. Close the **Router ISP B** tab

21.4 Test the BGP Routing

Let's check that the Atlanta and ISP B Router are exchanging routing information looking at the logs generated by the BGP traffic created to update the routes. For this, we are going to create a filter combining the logging facilities related to dynamic routing and the related services. We will add the ping in the filter as we will use this service to test the connectivity.

1. Click the tab where the **Logs** view is open
2. Select **Security Engine** as log context
3. Filter the logs by selecting Atlanta and Paris firewalls as **Sender** in the **Query** Pane
4. Right-click the **Service** column and select **Filter: Service**
5. In the **Filter Properties** dialog, type
   - **OSPFIGP** in the text field and click on it
   - **BGP** in the text field and click on it
   - **Ping** in the text field and click on it. Click **Apply**
6. Right-click the **Facility** column and select **Filter: Facility**
7. In the **Filter Properties**, configure the following settings:
   - Click the **Constant** drop-down list and select **Dynamic Routing** and click **Add**
   - Click the **Constant** drop-down list and select **Syslog** and click **Add.** Click **Apply**

8. Drag and drop the **Facility** Filter on the **Service Filter** to create a combine filter with a **OR**

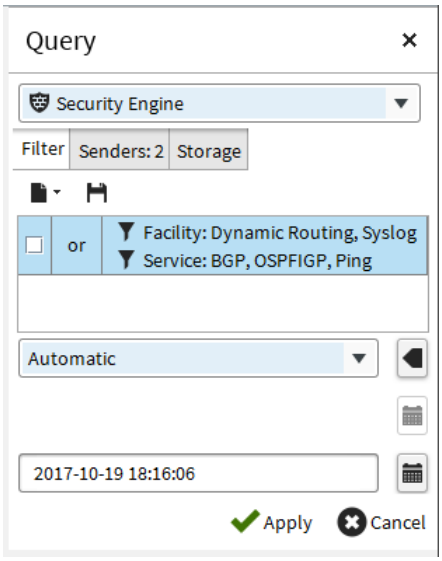


Figure 21.6: Log Filter for Testing BGP

9. Click the **Save** button. The **Filter Properties** dialog opens
10. Name the Filter **Dynamic Routing Traffic Filter**

    NOTE: Since Multilink is deployed there is a fair amount of Ping from the Atlanta Firewall nodes to 172.31.200.101 generated by the Multilink monitoring. To have a better visibility for out test, we are excluding 172.31.200.101 as destination in our filter

11. Click the **OR** in the tree and then the **&** button in the toolbar

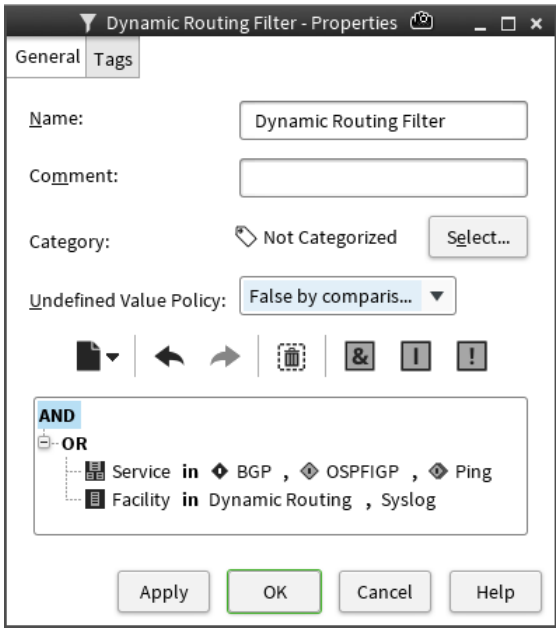


Figure 21.7: Editing the BGP Log Filter

12. Right-click **AND** in the tree and select **New** → **Filter: Dest Addr**. The **Properties dialog** opens

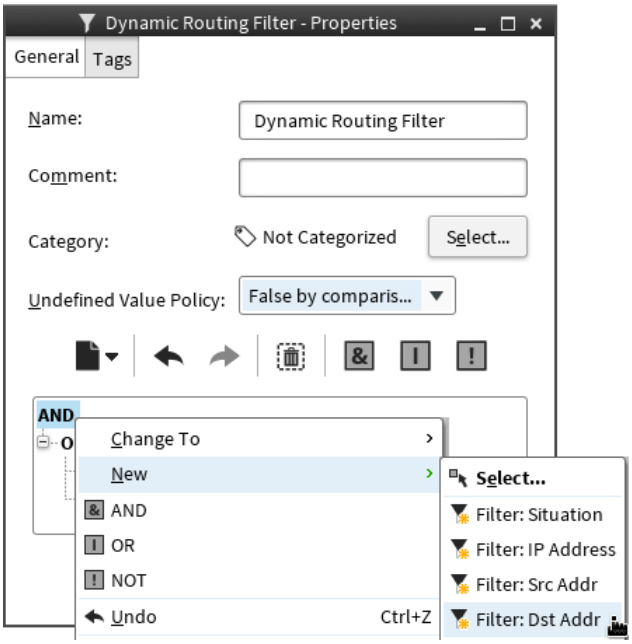


Figure 21.8: Tuning the BGP Log Filter

13. Type **172.31.200.101** in the **IP address** text field and click **Add**. Click **Apply**
14. Click the **NOT** button in the toolbar

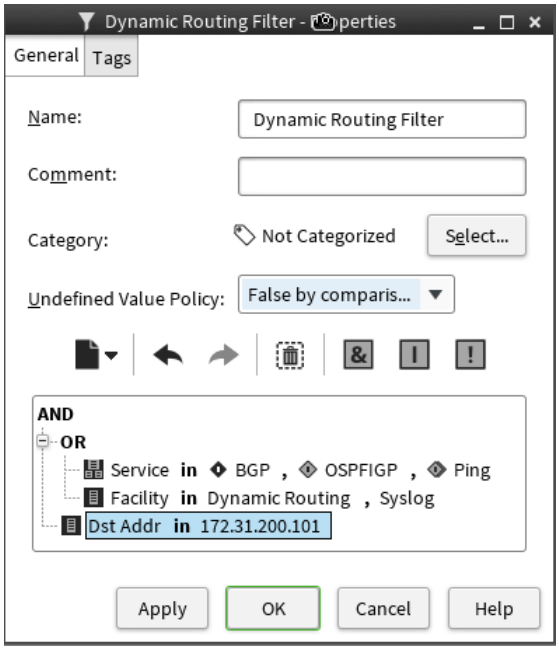


Figure 21.9: Excluding Management Traffic from BGP Filter

The filter should look like the illustration below:

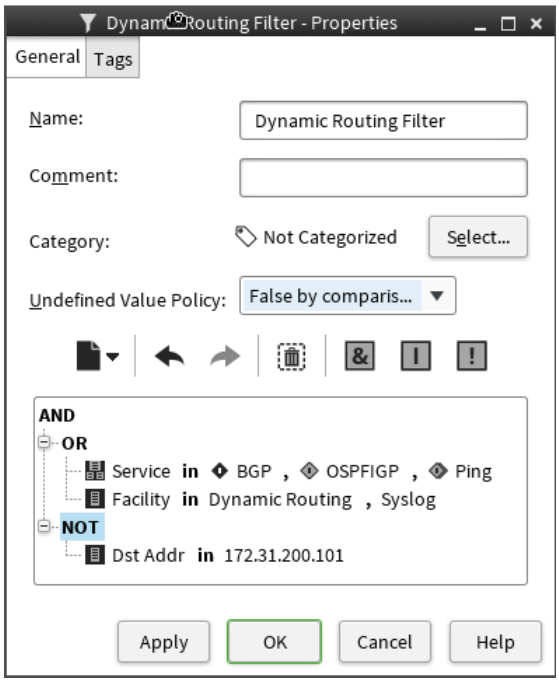


Figure 21.10: Completed BGP Log Filter

15. Click **OK**
16. Click **Apply** in the **Query** Pane
17. Click on the go to last stored record in the toolbar

Figure 21.11: Viewing BGP Related Logs 1/2

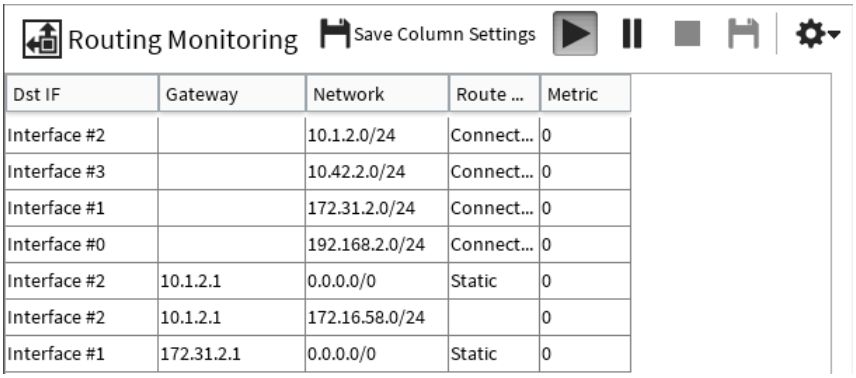
18. Move the **Information Message** column by dragging the column next to the **Situation** column
19. Check for the following logs

	Sender	Situation	Information Message	Service	Action	Src Addr	Dst Addr
	Atlanta FW Cluster node 2	Connection_Allowed		BGP	Allow	10.1.2.1	10.1.2.254
	Atlanta FW Cluster node 2	Connection_Closed	Connection was reset by server	BGP		10.1.2.1	10.1.2.254
⚠	Router ISP B node 1	Dynamic_Routing_Neighbor_UP	Neighbor 10.1.2.254 in Established state				
	Atlanta FW Cluster node 2	Connection_Allowed		BGP	Allow	10.1.2.254	10.1.2.1
⚠	Atlanta FW Cluster node 2	Dynamic_Routing_Neighbor_UP	Neighbor 10.1.2.1 recovered to Established st...				
	Router ISP B node 1		Sending restart update, 0 protocols restarting				
	Router ISP B node 1		Removing stale routes				
	Atlanta FW Cluster node 1		ROOT LOGIN on '/dev/tty1'				
	Router ISP B node 1	Connection_Allowed		Echo Req...	Allow	10.1.2.21	172.16.58.101
	Atlanta FW Cluster node 1	System_Engine-User_Command	HISTORY: PID=13018 UID=0 USER=root ping 1...				
	Atlanta FW Cluster node 1	Connection_Allowed		Echo Req...	Allow	10.1.2.21	172.16.58.101

Figure 21.12: Viewing BGP Logs 2/2

Let's now look at the Atlanta Routing Monitoring.

1. Click the tab where the **Home** view is open and expand the **NGFW Engines** section of the **Status** tree. Browse to **Firewalls** → **Atlanta FW Cluster**
2. Click **Atlanta FW Cluster** and in the **Drill-Down** pane, select **Monitoring** → **Routing**. In the **Routing monitoring** view, you can see the route that has been dynamically added with BPG



Dst IF	Gateway	Network	Route ...	Metric
Interface #2		10.1.2.0/24	Connect...	0
Interface #3		10.42.2.0/24	Connect...	0
Interface #1		172.31.2.0/24	Connect...	0
Interface #0		192.168.2.0/24	Connect...	0
Interface #2	10.1.2.1	0.0.0.0/0	Static	0
Interface #2	10.1.2.1	172.16.58.0/24		0
Interface #1	172.31.2.1	0.0.0.0/0	Static	0

Figure 21.13: Viewing Dynamically Added Routes

Finally let's check directly on the engine node the dynamic routing definition using the quagga command line.

1. Click **Home** button in the toolbar to return to the **Home** view
2. Identify the Atlanta Firewall node which is on-line
3. Open a virtual console to that Firewall node in the vSphere client
4. Log on to the Firewall node by entering the following credentials
5. - Login: **root**
   - Password: **Pass1234**
6. Enter `vtysh` to use the quagga shell
7. Enter `show ip route` to see all the routes and the protocol that provided the route path information
8. Type `show ip bgp neighbors` and check that ISP B router interface 10.1.2.1 is there
9. Type `show ip bgp` the see the routes learnt through BGP
10. Type `exit`
11. Type `ping 172.16.58.101` to test the connectivity to the ISP B Router Loopback address

The ping will go directly to ISP B with the new route instead of going to the Atlanta Firewall default route which is ISP A router. You can verify it in the Log View by checking the latest stored logs.

Note that the default routes generated by the outbound Multi-Link are matched before the routes added by the dynamic routing, even if the scope of the route is smaller. Therefore in the lab, since multilink is still configured, the outbound traffic originated from the Atlanta Server will not take into account the route added dynamically by BGP.

21.5 Using OSPFv2

In this lab, OSPFv2 is used as internal gateway protocol in the Atlanta internal network and Paris internal network. You will configure Atlanta Firewall and Paris Firewall as OSPF neighbors to distribute the routing information to each other.

The dynamic route redistribution will be limited. Atlanta Firewall will advertise the route to its internal network to Paris Firewall and vice-versa. The static routing definition will remain.

Atlanta and Paris are not physically directly connected to each other, Route-Based VPN you setup in the previous lab will be used to communicate routing information to each other using multicast.

In this configuration, Atlanta and Paris Firewalls will learn how to access to each other internal network dynamically and so the static routes we previously created to route the traffic between Paris and Atlanta internal network through. the route base VPN will not be necessary anymore.

21.6 Define an IP Address for the Tunnel Interface

The tunnel interface for your cluster has already been defined in the previous lab. Assigning an IP address to a Tunnel Interface is optional. However in this scenario we want to rely on automatic rules to allow OSPF multicast traffic through the Route-Based VPN Tunnel. For this configuration to work, we need to we need to assigned an IP address to the Tunnel Interface. If we don't assign any IP address, the default IP addresses for outgoing traffic that is defined in the Firewall Interface option will be used to initiate the multicast connection and this traffic must be manually allowed in both Atlanta and Paris Policy.

1. Click the tab where the **Atlanta FW Cluster** view is open for editing, Select **Interfaces**
2. Right-click **Tunnel Interface 1000** and select **New** → **IPv4 Address**. The **Tunnel Interface 1000** dialog box opens
3. Deselect **Node Dedicated IP Address** and define the following settings under **Cluster Virtual IP Address**:
   - IPv4 Address: **10.10.10.102**
   - Netmask: **255.255.255.0**

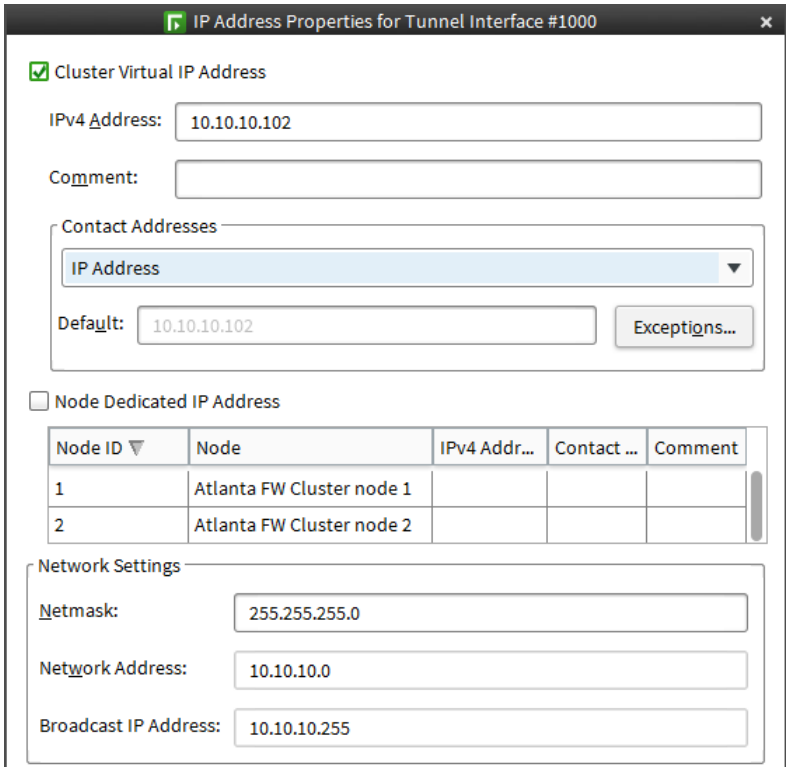


Figure 21.14: Creating a Tunnel Interface for OSPF

4. Click **OK**

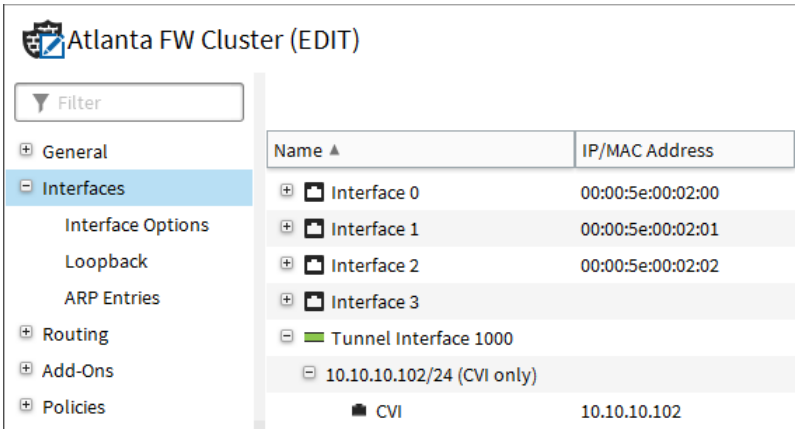


Figure 21.15: Completed Tunnel Interface Configuration

21.7 Configure OSPFv2 for Atlanta Firewall

You will now enable the OSPFv2 protocol in the engine properties. Then you will update the Atlanta Firewall routing definition by adding an OSPFv2 area behind the interfaces that will propagate route paths to the neighbor Firewall Paris. The OSPFv2 area will be common to Paris and Atlanta Firewall

The OSFPv2 area will be added behind the interface connected to the internal network as we want this interface IP address and the directly connected network to be announced. However we will prevent that this interface propagate information by selecting the passive communication mode.

The OSFPv2 area will also be added behind the Tunnel Interface to announce routes to the Atlanta Internal network to the neighbor Firewall Paris via the Route-Based VPN tunnel.

1. Browse to **Dynamic routing**
2. Select **Enabled** in the **OSPFv2** panel

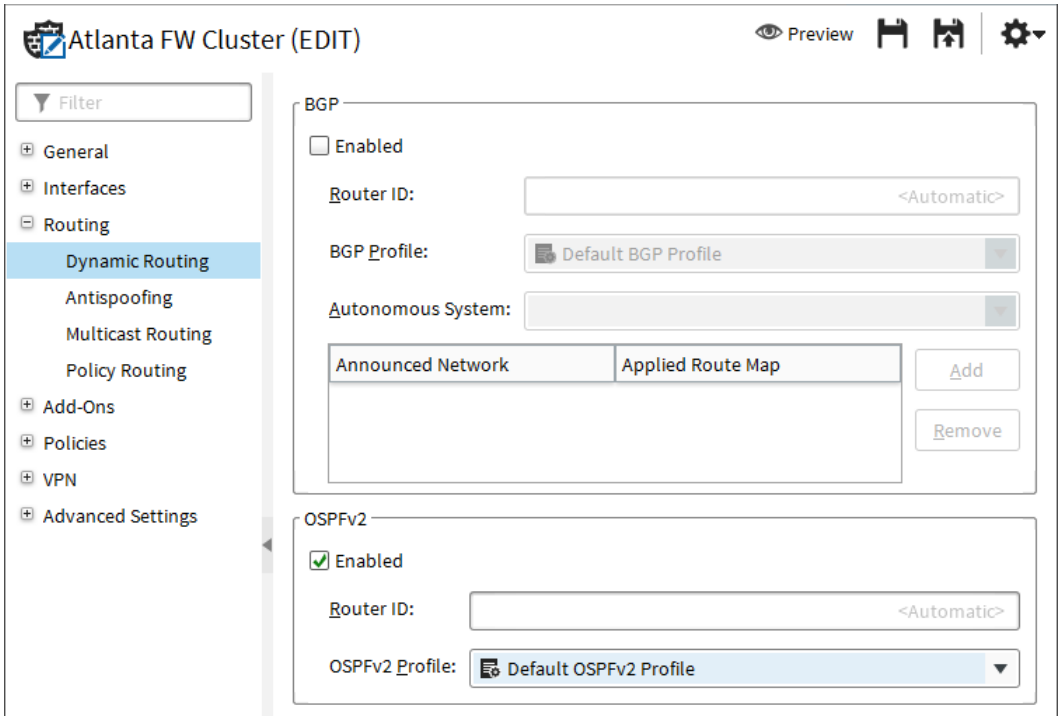


Figure 21.16: Enabling OSPF on Atlanta Firewall Cluster

3. Browse to **Routing**. The network directly connected to the tunnel interface has been added behind the Tunnel Interface in the routing view
4. Expand the **Tunnel Interface 1000**. Right-click **net-192.168.3.0/24** and select **Remove**
5. Right-click **Tunnel Interface 1000** and select **Add OSPFv2 Area.** The **Select Element(s)** properties opens
6. In the **Resources** pane, right-click **New OSPFv2 Area**
7. Define the define the following settings for the OSPFv2 Area:
   - Name: **Atlanta-Paris OSPFv2 Area**
   - Area ID: **0**
8. Click **OK**
9. Select the **Atlanta-Paris OSPFv2 Area** by adding the **Atlanta-Paris OSPFv2 Area** in the **Select Element(s)** properties. Click **OK**
10. Expand the **Interface 0**
11. Right-click **net-192.168.2.0/24** and select **Add OSPFv2 Area.** The **Select Element(s)** properties opens
12. Add the **Atlanta-Paris OSPFv2 Area** and Click **OK**
13. Click **Save** The Routing definition should look like the illustration below:

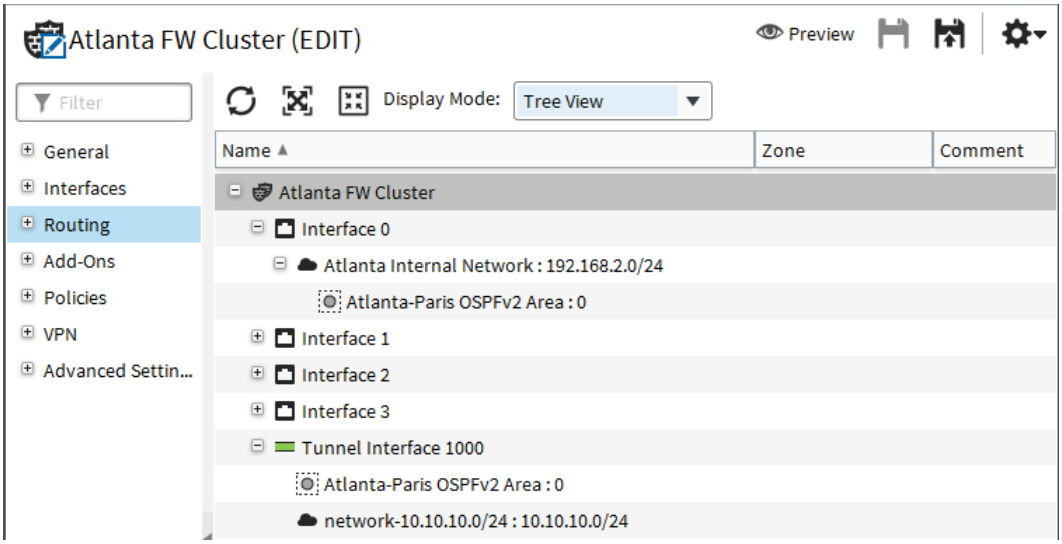


Figure 21.17: Atlanta Firewall OSPF Routing Table

14. Click **Refresh Engine Policy** icon and upload the **Atlanta Policy** to the **Atlanta FW Cluster**
15. Close the **Upload Policy: Atlanta Policy** tab when the policy upload has completed

21.8 Configure OSPFv2 for Paris Firewall

In a similar way, OSPFv2 must be configured in Paris Firewall to allow Paris and Atlanta to exchanges routing paths through the Route-Based VPN.

1. In the tab where the **Configuration** view is open, browse to **NGFW** → **NGFW Engines** → **Paris FW Cluster**
2. Right-click the **Paris FW Cluster** and select **Edit Paris FW Cluster** for editing the Firewall in a new tab
3. Select **General** and browse to **Clustering**
4. Click **Clustering Mode** drop-down list and select **Standby**
5. Browse to **Dynamic routing**
6. Select **Enabled** in the **OSPFv2** panel
7. Browse to **Routing**
8. Right-click **Tunnel Interface 1000** and select **New** → **IPv4 Address**. The **Tunnel Interface 1000** dialog box opens
9. Deselect **Node Dedicated IP Address** and define the following settings under **Cluster Virtual IP Address**:
   - IPv4 Address: **10.10.10.103**
   - Netmask: **255.255.255.0**
10. Expand the **Tunnel Interface 1000**. Right-click **net-192.168.3.101** and select **Remove**
11. Right-click **Tunnel Interface 1000** and select **Add OSPFv2 Area.** The**Select Element(s)** properties opens
12. Select the **Atlanta-Paris OSPFv2 Area** by adding the **Atlanta-Paris OSPFv2 Area** in the **Select Element(s)** properties. Click **OK**
13. Expand the **Interface 0**
14. Right-click **net-192.168.3.0/24** and select **Add OSPFv2 Area.** The **Select Element(s)** properties opens
15. Add the **Atlanta-Paris OSPFv2 Area** and Click **OK**

16. Click **Save** The Routing definition should look like the illustration below:

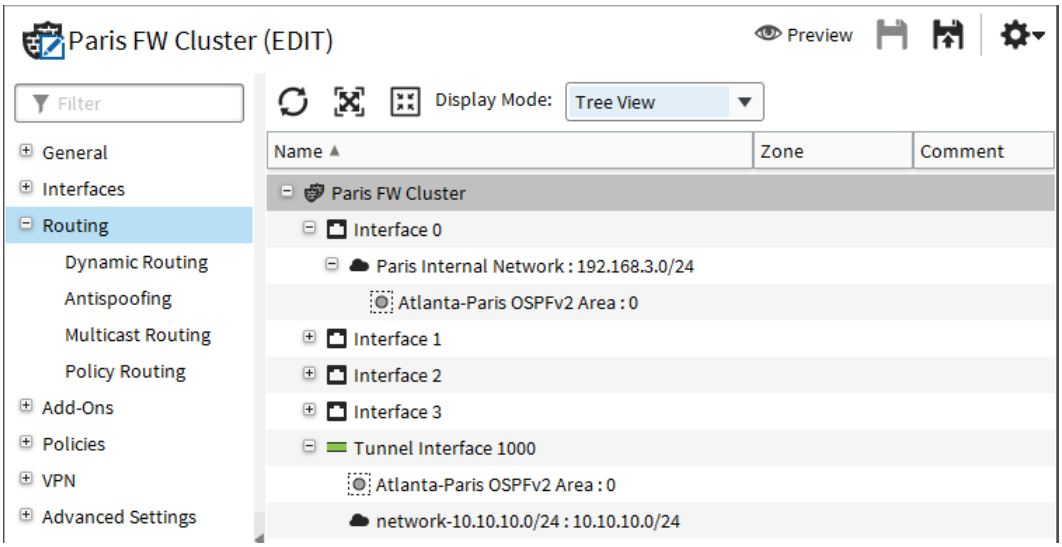


Figure 21.18: Paris FIrewall OSPF Routing Table

17. Click **Refresh Engine Policy** icon in the Engine Editor Toolbar and upload the **Paris Policy** to the **Paris FW Cluster**
18. Close the **Paris FW Cluster** tab
19. Close the **Upload Policy: Paris Policy** tab when the policy upload is completed

21.9 Test the Route-Based VPN using OSPFv2 routing

You have defined a Route-Based VPN and the traffic routed through the Route-Based VPN will be defined dynamically according to the routes exchanged using the OSPFv2 protocol.

We are now initialing a ping from the Atlanta server to the Paris Server to test the Route-Based VPN tunnel is working.

1. From **Atlanta-Server1**, start a continuous ping to Paris's web server. Open the terminal and type **ping 192.168.3.101**

Let's also check that the Atlanta and Paris Firewalls are exchanging routing information looking at the logs generated by the OSPFv2 multicast traffic created to update the routes. For this, we are going to create a filter combining Ping service and the logging facilities related to dynamic routing.

1. Click the tab where the **Logs** view is open
2. Select **Security Engine** as log context
3. Right-click **Select** in the Filter text field
4. Browse to **Filters** → **All Filters** in the **Select Filter properties** dialog. Type **Dynamic Routing Filter** and click on the element and click **Select**
5. Click **Apply** in the **Query** Pane
6. Click on the go to last stored record in the toolbar

Figure 21.19: Last Record Button: Logging Toolbar

7. Check for the following logs:

Sender	Facility	Situation	Service	Information Message
Atlanta FW Cluster node 2	Packet Filtering	FW_New-Route-Based-VPN-Connection	OSPFIGP	
Atlanta FW Cluster node 2	Dynamic Routing	Dynamic_Routing_Neighbor_UP		Neighbor 192.168.3.1 Established on vpn12:10.10.10.1(
Paris FW Cluster node 2	Dynamic Routing	Dynamic_Routing_Neighbor_UP		Neighbor 192.168.2.1 Established on vpn12:10.10.10.1(
Atlanta FW Cluster node 2	Syslog	Dynamic_Routing_Route_Deleted		Protocol ospf delete prefix 10.10.10.103/32 via :: interf
Atlanta FW Cluster node 2	Syslog	Dynamic_Routing_Route_Deleted		Protocol ospf delete prefix 192.168.3.0/24 via :: interfa
Atlanta FW Cluster node 2	Syslog	Dynamic_Routing_Route_Added		Protocol ospf add prefix 10.10.10.103/32 via :: interface
Atlanta FW Cluster node 2	Syslog	Dynamic_Routing_Route_Added		Protocol ospf add prefix 192.168.3.0/24 via :: interface=
Atlanta FW Cluster node 2	Dynamic Routing			Sending restart update, 0 protocols restarting
Atlanta FW Cluster node 2	Dynamic Routing			Removing stale routes
Atlanta FW Cluster node 2	Packet Filtering	FW_New-Route-Based-VPN-Connection	Echo Req...	

Figure 21.20: Monitoring OSPF Routings

Let's now look at the Atlanta Routing Monitoring.

1. Click the tab where the **Home** view is open and expand the **NGFW Engines** section of the **Status** tree. Browse to **Firewalls** → **Atlanta FW Cluster**
2. Click **Atlanta FW Cluster** and in the **Drill-Down** pane, select **Monitoring** → **Routing**. In the **Routing monitoring** view, you can see the routes that have been dynamically added with OSPFv2. There are the ones with the highest Metric values defined

Routing Monitoring | Save Column Settings

Creation Time	Dst IF	Gateway	Network	Route Type	Metric
			10.1.2.254/32	Static	0
			10.10.10.0/24	Static	0
	Interface #2	10.1.2.1	0.0.0.0/0	Static	0
	Interface #1	172.31.2.1	0.0.0.0/0	Static	0
	Interface #2		10.1.2.0/24	Connected	0
	Interface #3		10.42.2.0/24	Connected	0
	Interface #1		172.31.2.0/24	Connected	0
	Interface #0		192.168.2.0/24	Connected	0
			10.10.10.103/32		10
			192.168.3.0/24		20

Figure 21.21: Observing the Routing Metric for OSPF

Finally let's check directly on the engine node the routing definition using the quagga command line.

1. Click **Home** button in the toolbar to return to the **Home** view
2. Identify the Atlanta Firewall node which is on-line
3. Open a virtual console to that specific Firewall node in the vSphere client
4. Log on to the Firewall node by entering the following credentials
5. - Login: **root**
   - Password: **Pass1234**
6. Enter `vtysh` to use the quagga shell

7. Enter `show ip routes` to see all the routes and the protocol that provided the route path information
8. Type `show ip ospf neighbors` and check that Paris Firewall CVI 10.10.10.103 is there
9. Type `show ip ospf route` the see the routes learned using OSPFv2

```
SG-Quagga-Router# show ip ospf route
============ OSPF network routing table ============
N    10.10.10.103/32        [10] area: 0.0.0.0
                            directly attached to vpn12
N    192.168.2.0/24         [10] area: 0.0.0.0
                            directly attached to eth0
N    192.168.3.0/24         [20] area: 0.0.0.0
                            via 10.10.10.103, vpn12

============ OSPF router routing table =============
```

Figure 21.22: Viewing OSPF Routes at the Command Line

21.10 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 22

Optional Lab - Custom Network Applications

22.1 Getting Started

The logging of connections and activity traversing the firewall should not be limited to source, destination and port alone. It is far more useful to have additional information about network activity. Two examples of such information is URL and Application logging. In both cases, the NGFW is looking deeper into the packet to determine the URL and the network application in use. The SMC contains thousands of application signatures by default. However, in most organizations there will be custom applications for which you may wish to write your own signature. This lab will guide you through the process of obtaining more information about connections and creating a custom application signature.

22.2 Enable Connection and HTTP Request Logging for HTTP Traffic

You will now first add an Access rule to enable HTTP connection and URL logging for HTTP traffic, and then test the URL logging.

1. Click the Tab where the **Atlanta FW Policy** is open
2. Right-click the last rule allowing outbound traffic and Select **Copy Rule**
3. Right-click the last rule allowing outbound traffic and Select **Paste**
4. Configure the rule as follows:
   - Source: **net-192.168.2.0/24**
   - Destination: **not Internal Nets**
   - Service: **HTTP (with URL logging)**
   - Action: **Allow**
5. Click **OK**. The new rule should look as in the figure below:

	ID	Source	Destination	Service	Action
	5.3.1	net-192.168.2.0/24	not Internal Nets	HTTP (with URL Logging)	Allow
	5.3.2	net-192.168.2.0/24	not Internal Nets	ANY	Allow
	Discard all				

Figure 22.1: Completed URL Logging Rule

6. **Save and Install** the Policy

22.3 Test URL Logging

1. Click the Tab where the **Logs View** is open
2. Click the Tool icon and select **Column** → **Column Selection**. The Column Selection dialog opens

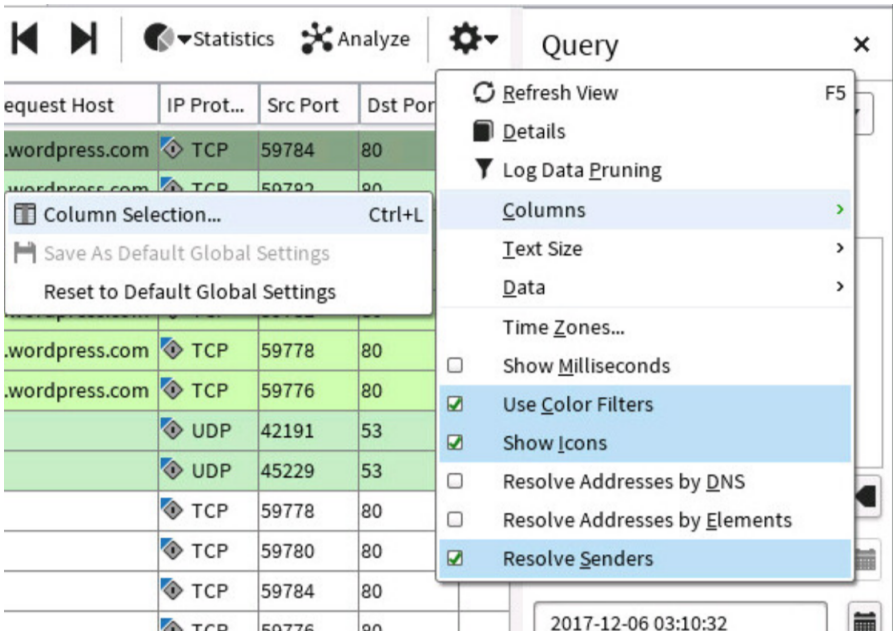


Figure 22.2: Selection of Columns

3. Select **All Fields**
4. Start typing **Application**. A list of matching log entries appears
5. Click **Network Applications** and drag and drop it after the **Service** field
6. Start typing **HTTP**. A list of matching log entries appears
7. Click **HTTP Request Host** and drag and drop it after the **Network Application** field
8. Click **OK**
9. Click the **Save Column Settings** icon in the toolbar
10. Click the **Current Events** icon in the toolbar

Figure 22.3: Current Events Toolbar Selection

11. Using the **vSphere** client on the **Landing Machine** and open a console to **Atlanta-Server**
12. Click the Firefox icon and the web browser and go to `http://server-1.wordpress.com`
13. Check the logs for allowed HTTP connections and verify that the server host name is visible in the **HTTP Request Host** log field

Situation	Action	Src Addr	Dst Addr	Service	HTTP Request Host
Connection_Allowed	Allow	192.168.3.1...	172.31.200.101	HTTP	
HTTP_URL-Logged	Permit	192.168.3.1...	172.31.200.101	HTTP	server-1.wordpress.com

Figure 22.4: HTTP Request Host Log Field

22.4 Create a Custom Application for the Helsinki Wordpress Server

1. Click the Tab where the **Atlanta FW Policy** is open
2. Click the **Service** cell of the last created rule
3. In the Resources list, right-click **Network Applications** → **New** → **Application**. The **Application Properties** dialog box opens
4. Name the Network Application **Helsinki Wordpress Website**
5. In the **Default ports** table, click the **Add Port** button and configure the following:
   - Protocol: **TCP**
   - From: **80**
   - TLS: **Forbidden**
6. In the **Default ports** table, click the **Add Port** button and configure the following:
   - Protocol: **TCP**
   - From: **443**
   - TLS: **Mandatory**
7. In the **TLS Match** field, click **Select** and select **Match_Any-Valid-Certificate**
8. Select **Application identified by TLS Match Alone**

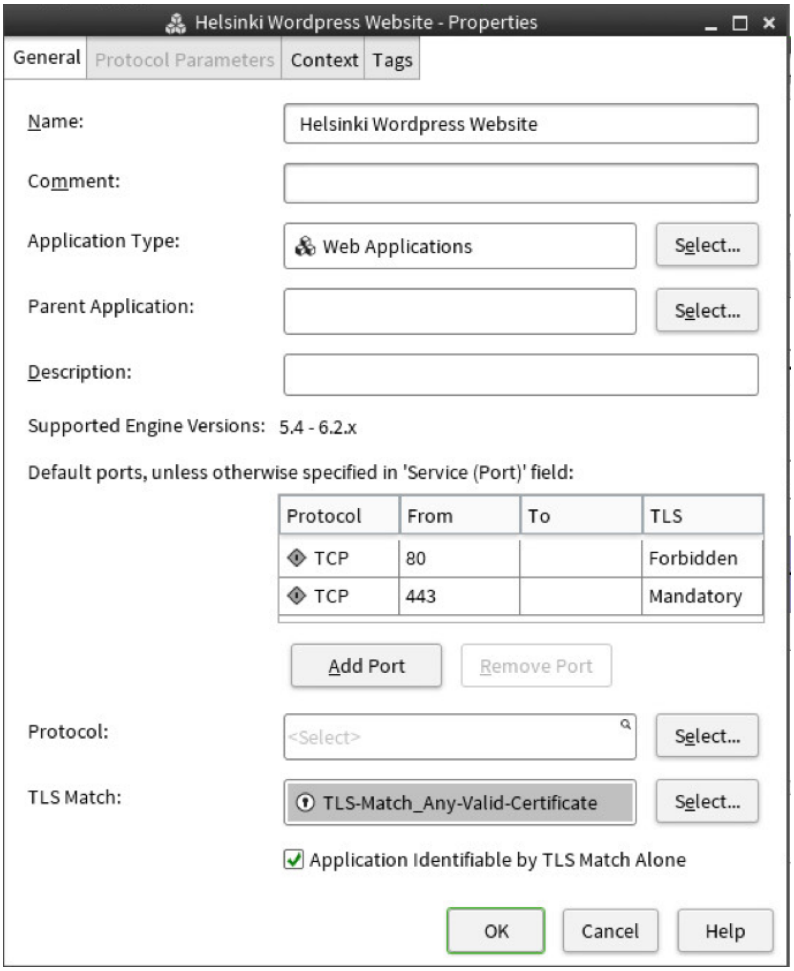


Figure 22.5: Custom Application Properties

9. Click the **Context** Tab
10. Click the **&** icon in the toolbar
11. Right-Click **& AND** → **Add** → **New Match** in the text field

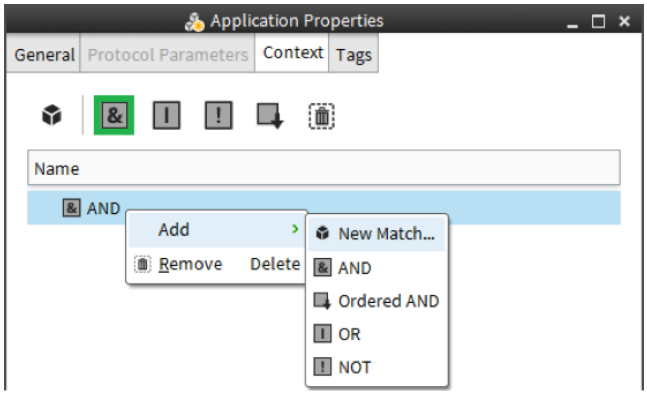


Figure 22.6: Custom Application Context Properties

12. Click **Select**. The **Select Context** dialog opens
13. Browse to **Protocols** → **Application Protocols** → **HTTP** → **HTTP Client Stream** and click **Select**

14. Enter the following Regular Expression that matches the Wordpress server host name:
    - `.*Host:\x20server-1\.wordpress\.com`

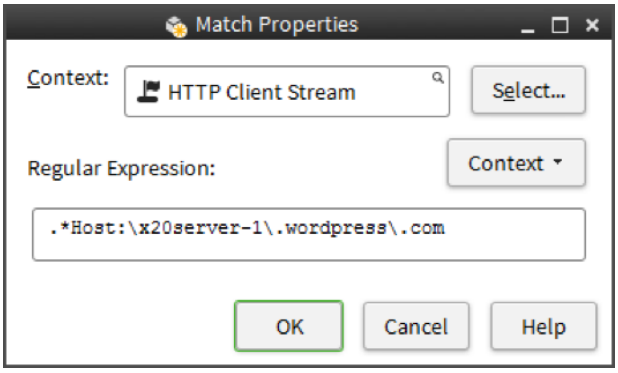


Figure 22.7: HTTP Client Stream Match Properties

15. Click **OK**
16. Click **OK**. The Network Application is created
17. Right-click the **Service** cell configured with the **HTTP (with URL logging)** service and select **Clear Cell**
18. Click the **Service** cell, start typing **Helsinki Wordpress Website** and select the element

ID	Source	Destination	Service	Action
5.3.1	net-192.168.2.0/24	not Internal Nets	Helsinki Wordpress Website	Allow

Figure 22.8: Custom Application Used in a Rule

19. **Save and Install** the Policy

22.5 Testing Application Logging

1. Click the Tab where the **Logs View** is open
2. Click the **Current Events** icon in the toolbar
3. Open the web browser on your **Atlanta-Server** and go to `http://server-1.wordpress.com`
4. Check the logs for allowed HTTP connections and verify that the **Helsinki Wordpress Application** is visible in the **Network Application** log field

Situation	Action	Src Addr	Dst Addr	Service	HTTP Request Host	Network Application
HTTP_URL-Logged	Permit	192.168.3.1...	172.31.200.101	HTTP	server-1.wordpress.com	Helsinki Wordpress Website
Connection_Allowed	Allow	192.168.3.1...	172.31.200.101	HTTP	server-1.wordpress.com	Helsinki Wordpress Website

Figure 22.9: Log Entries of Custom Application over HTTP

5. Perform a similar test for HTTPS connections and enter `https://server-1.wordpress.com` in the Atlanta Web browser

6. Verify that the **Helsinki Wordpress Application** is visible in the **Network Application** log field

Situation	Action	Src Addr	Dst Addr	Service	HTTP Request Host	Network Application
Connection_Allowed	Allow	192.168.3.1...	172.31.200.101	HTTPS		Helsinki Wordpress Website

Figure 22.10: Log Entries of Custom Application over HTTPS