



# Dell PowerConnect J-Series J-SRX100S/SU Services Gateway

Getting Started Guide



## Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Getting Started Guide

This Getting Started Guide provides instructions for basic installation and configuration of the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway.

# Document Contents

<b>1 Getting Started with the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway</b> . . . . .	<b>3</b>
<b>2 Setting Up Your Network</b> . . . . .	<b>6</b>
<b>3 Performing Advanced Network Configuration</b> . . . . .	<b>19</b>
<b>4 Enabling Security Services</b> . . . . .	<b>25</b>
<b>5 Powering Off the Device</b> . . . . .	<b>40</b>
<b>6 Support and Training Options</b> . . . . .	<b>41</b>

# 1 Getting Started with the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway

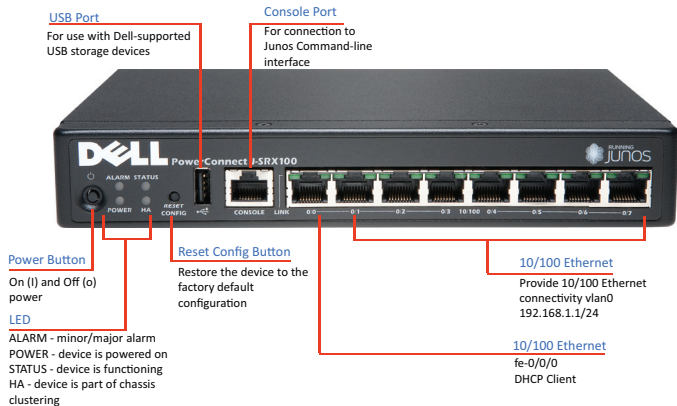
The Dell PowerConnect J-Series J-SRX100S/SU Services Gateway offers features that provide complete functionality and flexibility for delivering secure Internet and intranet access. The services gateway offers stable, reliable, and efficient IP routing in addition to switching support and LAN connectivity. The device provides firewall, anti-virus, anti-spam, anti-spyware, Web filtering, IP Security (IPsec), and virtual private network (VPN) services for small-sized and medium-sized companies. The services gateway can be connected directly to traditional private networks such as leased lines, Frame Relay, or MPLS or to the public Internet. The services gateway runs the Junos operating system (Junos OS).

This chapter provides the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway front and back panel views and the package content information.

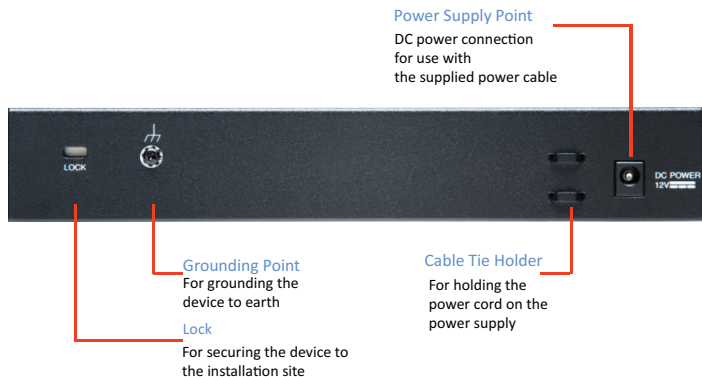
## Section 1 Contents

<b>1.1 Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Front Panel</b> . . . . .	<b>4</b>
<b>1.2 Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Back Panel</b> . . . . .	<b>4</b>
<b>1.3 Checking the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Package Contents</b> . . . . .	<b>5</b>

## 1.1 Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Front Panel



## 1.2 Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Back Panel



## 1.3 Checking the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Package Contents

Before setting up your Dell PowerConnect J-Series J-SRX100S/SU Services Gateway, verify that your package contains the following parts:

- Dell PowerConnect J-Series J-SRX100S/SU Services Gateway
- DB9 > RJ-45 cable
- Quick Start Guide
- Getting Started Guide
- Safety and Environmental Regulation Information (SERI)
- End-User License Agreement (EULA)
- Registration and Software Updates information
- Warranty and support Information (WSI)
- Open Source Code Notice

### 1.3.1 Any Items Missing?

If any items are missing from your package, contact Dell customer support at [www.support.dell.com](http://www.support.dell.com).



**NOTE:** If you have purchased a UTM subscription, the license authorization codes certificate will be shipped separately in an envelope. You will need this certificate to set up security services for your gateway.



**NOTE:** The power supply adapter and the power cord are shipped in a separate box.

## 2 Setting Up Your Network

This chapter provides preconfiguration and configuration instructions for connecting your Dell PowerConnect J-Series J-SRX100S/SU Services Gateway. Review this chapter to set up your services gateway.

### Section 2 Contents

<b>2.1 Recording Configuration Information</b> .....	<b>7</b>
<b>2.2 Connecting the Device</b> .....	<b>8</b>
<b>2.3 Verifying Internet Connectivity</b> .....	<b>10</b>
<b>2.4 Understanding the Default Configuration Settings</b> .....	<b>11</b>
<b>2.5 Verifying the System Requirements</b> .....	<b>11</b>
<b>2.6 Accessing the J-Web Interface</b> .....	<b>11</b>
<b>2.7 Configuring the Basic Settings</b> .....	<b>13</b>
<b>2.8 Verifying the Configuration</b> .....	<b>17</b>

## 2.1 Recording Configuration Information

This section provides the following information:

### 2.1.1 Registration Information

### 2.1.2 Login Information

### 2.1.3 Internet Service Provider Information

#### 2.1.1 Registration Information



**NOTE:** If you have not purchased the UTM or IDP licenses, do not proceed with the instructions provided in this section.

Use the following information when you are enabling Unified Threat Management (UTM)/Intrusion Detection and Prevention (IDP) licenses on the device.

---

<b>Serial Number</b>	Record the serial number found on the bottom of the chassis of your Dell PowerConnect J-Series J-SRX100S/SU Services Gateway.
----------------------	---

---

---

<b>Authorization Code</b>	Record the authorization code provided by Dell. <b>NOTE:</b> Use the authorization code only if you have purchased subscription licenses for UTM and IDP.
---------------------------	--

---

#### 2.1.2 Login Information

Use the following default username and password information for the first time login. Record this information for your future reference.

---

<b>Username</b>	Select an administrator account name. Default is <b>root</b> .
<b>Password</b>	Password is not required. Leave this box blank.

---

### 2.1.3 Internet Service Provider Information

Use the following information to connect to the Internet when your Internet Service Provider (ISP) provides the static settings such as IP address, Domain Name Server (DNS), and so on.



**NOTE:** Do not use this information if your ISP uses Dynamic Host Configuration Protocol (DHCP).

IF YOU CONNECT USING	PLEASE RECORD
DHCP	No information is usually required, although some providers may require a hostname. Hostname: _____

IF YOU CONNECT USING	PLEASE RECORD
Static IP	IP Address: _____
	Subnet Mask: _____
	Default Gateway: _____
	Primary DNS: _____
	DNS 2 (optional): _____
	DNS 3 (optional): _____

## 2.2 Connecting the Device

This section covers the following tasks:

### 2.2.1 Connecting the Power Cable to the Device

### 2.2.2 Connecting the Management Device

### 2.2.3 Connecting to Your Internet Service Provider



## 2.2.1 Connecting the Power Cable to the Device

To connect the power cable to the device:

1. Plug the DC connector end of the power cable in to the power connector on the back of the device.
2. Plug the AC adapter end of the power cable in to an AC power outlet. We recommend using a surge protector. Note the following indications (see **"1.1 Dell PowerConnect J-Series J-SRX100S/SU Services Gateway Front Panel"**):
  - POWER LED (green): The device is receiving power.
  - STATUS LED (green): The device is operating normally.
  - ALARM LED (amber): The device is operating normally, but a rescue configuration has not yet been set. This is not a panic condition, however.



**NOTE:** Initially, if the rescue configuration has not been set, a steadily amber ALARM LED indicates a minor alarm condition, and a steadily red ALARM LED indicates that a major alarm condition on the services gateway.

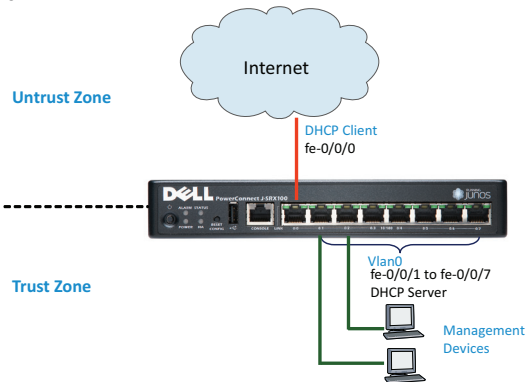


**NOTE:** You must allow the device between 5 and 7 minutes to boot fully after you have powered it on. Wait until the STATUS LED is steadily green before proceeding to **"2.2.2 Connecting the Management Device."**

## 2.2.2 Connecting the Management Device

Connect the management device to the services gateway using an RJ-45 cable (Ethernet cable) from any one of the fe-0/0/1 through fe-0/0/7 ports on the front panel to the Ethernet port on the management device.

**Figure 1: Connecting the Management Device to the Services Gateway**



After you connect the management device to the services gateway, the DHCP server process on the services gateway automatically assigns an IP address to the management device. Ensure that the management device acquires an IP address in the range of 192.168.1.2 through 192.168.1.254 from the services gateway.

**NOTE:** For the services gateway to assign an IP address to the management device, the management device must be set up to connect using DHCP.



If an IP address is not assigned to the management device, you can manually configure an IP address in the range of 192.168.1.2/24 through 192.168.1.99/24. Ensure you do not use 192.168.1.1, as this IP address is configured on the services gateway.

### 2.2.3 Connecting to Your Internet Service Provider

Connect the fe-0/0/0 port on the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway to your ISP or Internet (see **“Figure 1: Connecting the Management Device to the Services Gateway”**). The DHCP server that resides in your ISP network provides the necessary settings (such as default route, DNS, and so on) to the services gateway to connect to the Internet.



**NOTE:** If you are using a static IP address to connect to the provider’s network, do not perform **“2.3 Verifying Internet Connectivity.”** To access the Internet from your management device (workstation or laptop), you need to first configure the static IP address on the fe-0/0/0 interface and configure a default route.

## 2.3 Verifying Internet Connectivity

With a default configuration of the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway, you can access the Internet when you connect the management device into any one of the Ethernet ports (fe-0/0/1 through fe-0/0/7) and your ISP is connected to the fe-0/0/0 port. For more information on default configuration, see **“2.4 Understanding the Default Configuration Settings.”**

Now you can browse the Internet from your management device. For example, type **www.dell.com** in your browser.



**NOTE:** If you are using DHCP to verify the network settings from your service provider, verify your Internet connectivity. If you are using a static IP address to connect to the provider’s network, do not verify the internet connectivity.

## 2.4 Understanding the Default Configuration Settings

The device has the following default configuration settings when you power it on for the first time (for more information on trust and untrust zones, see “3.1 Zones and Interfaces Overview”):



### Factory Default Settings

PORT LABEL	INTERFACE	SECURITY ZONE	DHCP STATE	IP ADDRESS
0/0	fe-0/0/0	untrust	client	Unassigned
0/1 to 0/7	fe-0/0/1 to fe-0/0/7	trust	server	192.168.1.1/24

SOURCE ZONE	DESTINATION ZONE	POLICY ACTION
<b>For Security Policies</b>		
trust	untrust	permit
trust	trust	permit
untrust	trust	deny
<b>For NAT Rule</b>		
trust	untrust	source NAT to untrust zone interface

## 2.5 Verifying the System Requirements

Before you begin the setup process, verify that you have one of the following supported browsers:

ICON	ACCEPTED BROWSER	BROWSER VERSION NUMBER
	Internet Explorer	7.0 and later
	Mozilla Firefox	3.0 and later

## 2.6 Accessing the J-Web Interface

To access the J-Web interface:

1. Launch a Web browser on the management device or PC.
2. Enter **http://192.168.1.1** in the URL address box. The J-Web login page appears.
3. Specify the default username as **root**. Do not enter any value in the Password box.
4. Click **Log In**. The first time you log in, the J-Web Initial Setup page appears.



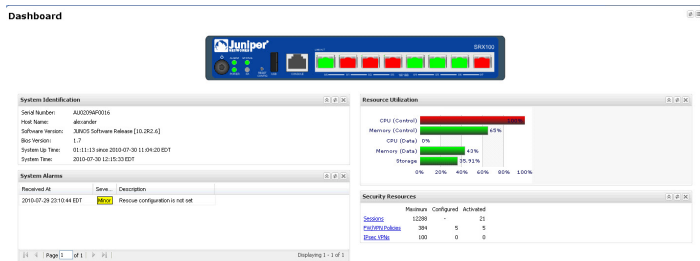
**NOTE:** The J-Web interface will take between 1 and 2 minutes for displaying the initial setup page, only Host Name and Root Password is mandatory. Other fields are optional.

The screenshot shows the J-Web configuration interface with the following sections:

- Identification:** Fields for Host Name, Domain Name, Root Password, and Verify Root Password.
- Time:** Fields for Time Zone and NTP server, with a Current System Time display.
- Network:** Fields for DNS Name Servers, Domain Search, Default Gateway, Localhost Address, and Network Address. There is also a checkbox for "Enable DHCP on fe-0/0/0.0".
- Management Access:** A section with several checkboxes: "Allow Telnet Access", "Allow J-WebSSH over Clear Text Access", "Allow J-WebSSH over Encrypted Access", and "Allow SSH Access".

5. Enter the hostname and root password. You can also configure DNS server, time zone, and so on, on this page.
6. Click **Apply**.
7. Click **Commit Options** on the top right corner and click **Commit**.

8. If you have used a static IP address to configure an IP address on your services gateway, ensure that you make the following J-Web modifications:
  - a. Clear the **Enable DHCP on fe-0/0/0.0** check box.
  - b. Enter the manual IP address provided by your ISP in the **fe-0/0/0.0** address box. The IP address must be entered in the a.b.c.d/xx format, where xx is the subnet mask.
  - c. Enter the IP address of the gateway in the Default Gateway box. Your ISP provides the IP address for the gateway.
  - d. Enter server names in the DNS name servers box. Your ISP provides the server names.
  - e. Click **Apply**. The J-Web login page appears again.
  - f. Enter the username and password and click **Log In**. After successful login, the Dashboard page appears.



9. Access the Internet from your management device.  
For example, type **www.dell.com** in your browser. This connectivity ensures that you can pass traffic through the services gateway. For more information on verification, see **“2.8 Verifying the Configuration.”**

## 2.7 Configuring the Basic Settings

This section covers the following configuration tasks:

### 2.7.1 Setting the System Hostname, Domain Name Server, and Root Authentication

### 2.7.2 Setting the Date and Time

### 2.7.3 Creating a User Account

### 2.7.4 Assigning a Static IP Address to the WAN-Facing Interface

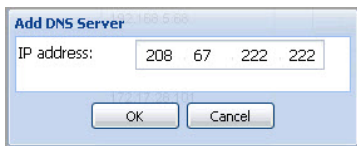
### 2.7.5 Creating a Default Route to the WAN Interface

### 2.7.6 Applying the Basic Configuration Settings

#### 2.7.1 Setting the System Hostname, Domain Name Server, and Root Authentication

If you have not configured the hostname and DNS settings in the J-Web Initial Setup page, to set or change the hostname, DNS settings, or the root authentication password:

1. Click the **Configure** tab at the top of the page and navigate to **System Properties > System Identity**.
2. Click **Edit** and enter the hostname and root password.
3. Click **Add** and enter the DNS server IP address. For example, **208.67.222.222**.



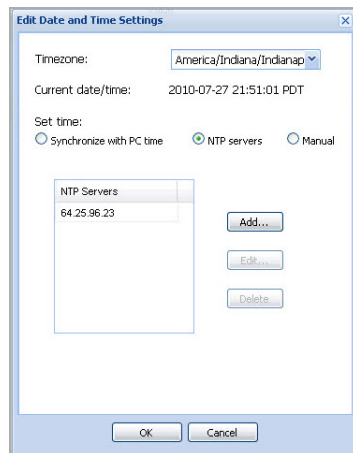
4. Click **OK** and then click **OK** again.
5. Click **Commit** to save the basic configuration.

## 2.7.2 Setting the Date and Time

You can synchronize the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway clock using three options: Manual, management device clock, or NTP Server.

To set the date and time:

1. Click the **Configure** tab at the top of the page and navigate to **System Properties > Date Time**.
2. Click **Edit** at the top right corner of the page, and then select your required time zone from the list.
3. Select the set time options in **Set time**.
4. Click **OK**.



## 2.7.3 Creating a User Account

To configure a user (other than an administrative account) and to set different permissions while accessing the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway:

1. Click the **Configure** tab at the top of the page and choose **System Properties > User Management**.
2. Click **Edit** at the top right corner of the page, and then click **Add**.
3. Enter the username and password.
4. Select the required permission from the list in Login class.
5. Click **OK**.



**Add User**

User name: lab

User Id:

Full name:

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

Login class: read-only

OK Cancel

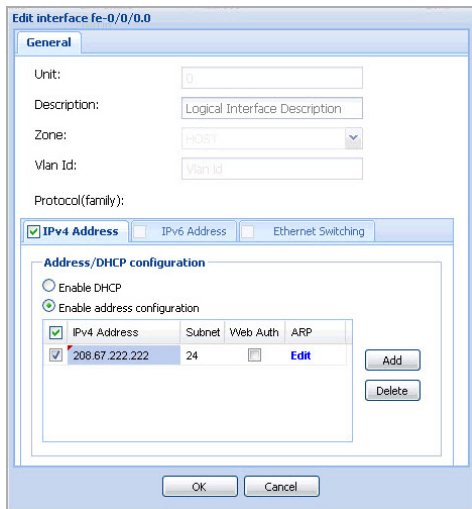
## 2.7.4 Assigning a Static IP Address to the WAN-Facing Interface

To assign a static IP address to the WAN-facing (internet) interface:

1. Click the **Configure** tab at the top of the page and navigate to **Interfaces**.
2. Expand **fe-0/0/0** and select the logical interface.
3. Click **Edit** and select the zone as **untrust** from the list.
4. Click the **IPv4 Address** tab.
5. Select **Enable address configuration** and then select the **IPv4 Address** check box.



**NOTE:** The **IPv4 Address** check box must be selected before the **Add** button is automatically enabled.



6. Click **Add** and enter the IP address and subnet mask provided by your ISP.
7. Click **OK**.

## 2.7.5 Creating a Default Route to the WAN Interface

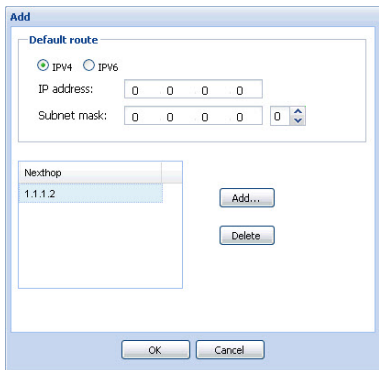
 **NOTE:** Creating a default route is required only if you have used a static IP address.

To create a default route to the WAN interface:

1. Click the **Configure** tab at the top of the page and navigate to **Routing > Static Routing**.
2. Click **Add**.
3. Enter the IP address as **0.0.0.0** and the Subnet mask as **0.0.0.0**.

 **NOTE:** While adding the next hop, the field is separated by tabs instead of dots.





4. Click **Add** in Next hop and enter the default gateway IP address provided by your ISP.
5. Click **OK**.

### 2.7.6 Applying the Basic Configuration Settings

When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, but do not take effect on the device until you commit the changes. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file.

To save the configuration, select **Commit Options** on the top right corner of the page and click **Commit**.



**NOTE:** You can commit your configuration settings at the end of each task or you can commit all the configuration settings at one time.

## 2.8 Verifying the Configuration

To verify the basic configuration, access any external website (for example, **www.dell.com**), to ensure that you are connected to the Internet.

If you are unable to connect to Internet from your management PC, verify the following:

1. In the J-Web interface, click the **Troubleshoot** tab and then click **Ping Host**.
2. Enter **www.dell.com** in Remote Host and click **Start**. If your ping is successful go to Step 3, otherwise go to Step 4.
3. Ensure the Management PC has acquired IP address (in the range 192.168.1.2 through 192.168.1.99) and DNS settings from the services gateway. If the PC acquired the correct IP address/DNS and you are still not able to access internet, go to Step 5.

4. To ensure that the services gateway has the default route (0.0.0.0) when you are using DHCP:

- a. Click the **Monitor** tab and navigate to **Routing > Route Information**.

Static Routing

Route Filter

Destination Address:  Protocol:

Next Hop Address:  Receive Protocol:

Best Route  Inactive Routes

Exact Route  Hidden Routes

Route Table:

Route Information: 28 destinations, 28 routes (27 active, 0 hold down, 1 hidden)

Static Route Address	Next Hop Type	Next Hop	Age	Protocol	Preference	Status	AS Path
10.4.0.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.5.0.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.6.128.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.9.0.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.10.0.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.13.4.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.13.10.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.34.0.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	
10.98.12.0	Router	10-000.0	1:36:22	Static	5	Active NotReachable Int Ext	

- b. Select **inet.0** from the Route Table list and then click **Generate Report**.

c. Save the report on your local disk.

5. Contact Dell customer support at [www.support.dell.com](http://www.support.dell.com).

## 3 Performing Advanced Network Configuration

This chapter provides the security zone and policies configuration instructions for connecting your Dell PowerConnect J-Series J-SRX100S/SU Services Gateway.

### Section 3 Contents

<b>3.1 Zones and Interfaces Overview</b> .....	<b>20</b>
<b>3.2 Creating a New Security Zone and Adding an Interface to the New Zone</b> .....	<b>20</b>
<b>3.3 Configuring Security Policies</b> .....	<b>22</b>
<b>3.4 Enabling Remote Access to the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway</b> .....	<b>23</b>
<b>3.5 Enabling System Services</b> .....	<b>23</b>
<b>3.6 Allowing Host Inbound Traffic</b> .....	<b>24</b>
<b>3.7 Applying the Security Policy Configuration</b> .....	<b>24</b>

### 3.1 Zones and Interfaces Overview

Zones split a network infrastructure into logical areas, each with its own set of usage rules, security services, and policies. Most networks include multiple definitions of zones, including those for trusted, untrusted, public, encrypted, and wireless traffic. The Dell PowerConnect J-Series J-SRX100S/SU Services Gateway comes preconfigured with basic zones, such as:

- Untrust zone—Zone through which you connect to the Internet.
- Trust zone—Zone that contains all the trusted local network resources.

The security features and settings that zones carry are enforced by binding one or more physical interfaces (fe-0/0/1 through fe-0/0/7) on services gateway to a zone.

### 3.2 Creating a New Security Zone and Adding an Interface to the New Zone

This example shows how to create a new zone, DMZ, and assign interface fe-0/0/2 to it. This example also shows how to make fe-0/0/2 an L3 interface and assign an IP address to it.

To create and assign an interface port to the DMZ zone:

1. Click the **Configure** tab at the top of the page, navigate to **Security > Zones/Screens**, and then click **Add**.
2. Enter the Zone name as **DMZ** and select the zone type as **security**.

The screenshot shows the 'Add Zone' configuration window. The 'Zone name' field is set to 'DMZ' and the 'Zone type' is set to 'security'. Under 'Traffic control options', 'Send RST for non matching session' is unchecked and 'Binding screen' is set to a dropdown menu. At the bottom, there are two columns: 'Available' and 'Selected'. The 'Available' column lists interfaces fe-0/0/1.0 through fe-0/0/7.0. The 'Selected' column contains fe-0/0/2.0. A double-headed arrow button is positioned between the columns, indicating the move operation.

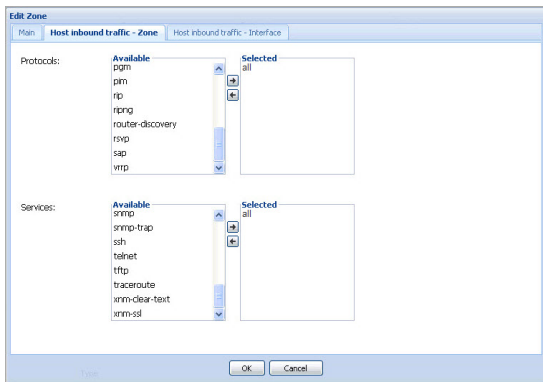
3. In the Interfaces in this zone field, move **fe-0/0/2** from the **Available** list to the **Selected** list.

- Click the **Host inbound traffic – Zone** tab.



**NOTE:** This step is optional. However, you must select the required services and protocols to enable any kind of service or protocol (DHCP, OSPF, and so on).

- Select the required services and protocols and move them to **Selected** and click **OK**.



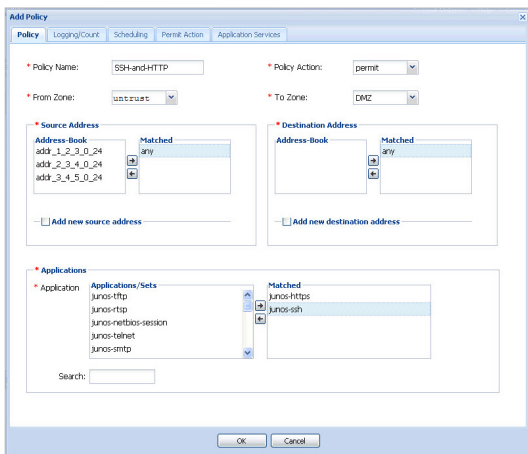
- To modify the fe-0/0/2 interface to be an L3 interface (by default, it is Layer 2):
  - Click the **Configure** tab at the top of the page and navigate to **Interfaces**.
  - Expand **fe-0/0/2**, select the logical interface (fe-0/0/2.0), and then click **Edit**.
  - Clear the **Ethernet switching** check box and select the **IPv4 Address** check box.
  - Select the **IPv4 Address** check box.
  - Click **Add** and enter the IP address.
  - Click **OK**.

### 3.3 Configuring Security Policies

Security policies provide a set of rules for transit traffic to use to identify which traffic can pass through the firewall and what actions to take on the traffic as it passes through the firewall. To assign an IP address:

For example, to define a security policy between the untrust and the DMZ zones that will allow HTTP/SSH traffic between them:

1. Click the **Configure** tab, choose **Security > Policy > FW Policies**, and then click **Add**.



2. In the Policy tab, enter the policy name and select the Policy Action as **permit** from the list.
3. In the Policy tab, select **untrust** from the list for **From Zone** and **DMZ** from the list for **To Zone**.
4. In the Source Address and Destination Address areas, move **any** to **Matched**.



**NOTE:** For any specific source or destination address, select **Add new destination address**.

5. In Applications, move **junos-https** and **junos-ssh** to **Matched** and then click **OK**.



**NOTE:** To allow HTTP/SSH traffic from the DMZ to the untrust zone, create a new policy and configure a security policy from the DMZ to the untrust zone. To perform this, follow the steps mentioned in **“3.3 Configuring Security Policies;”** however, you need select **DMZ** from the list for **From Zone** and **untrust** from the list for **To Zone**.

## 3.4 Enabling Remote Access to the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway

To manage the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway from a remote location, for example through fe-0/0/0 that is connected to your Internet Service Provider, you must:

- enable system services like HTTP/Telnet/SSH.
- allow host-inbound-traffic at the zone or specific interface level (in this case, zone is **untrust** and interface is **fe-0/0/0**).

## 3.5 Enabling System Services

To enable system services like HTTP, Telnet, and SSH:

1. Click the **Configure** tab at the top of the page, navigate to **System Properties > Management Access**. The Management Access Configuration page appears.
2. Click **Edit**.
3. Click the **Services** tab.
4. In Services, select the check box for the service that you want to enable.



**NOTE:** By default, Telnet and SSH are enabled.



5. In Enable HTTP/HTTPS, to enable HTTP/HTTPS on all available interfaces:
  - a. Click the **Enable on all interfaces** check box or
  - b. To add HTTP/HTTPS only to certain interfaces move the required interfaces to **selected interfaces**.



**NOTE:** Before enabling HTTPS access, ensure that the system date and time is set accurate.

6. Click **OK**.

### 3.6 Allowing Host Inbound Traffic

To allow host-inbound service for a zone/interface:

1. Click the **Configure** tab at the top of the page, navigate to **Security > Zones/Screens**.
2. Click the security zone that you want to modify (for example, untrust).
3. In the **Main** tab, ensure **fe-0/0/0** interface is in the **Selected** column.
4. Click the **Host inbound traffic – Zone** tab.

5. Select the required services and protocols and move them to **Selected**.
6. Optionally, to allow host inbound traffic at interface level (instead of allowing to the entire zone):
  - a. Click the **Host inbound traffic – Interface** tab.
  - b. Click on the **fe-0/0/0** interface (for this example).
  - c. Follow step 4 and step 5.
7. Click **OK**.

### 3.7 Applying the Security Policy Configuration

Once the configuration is complete, you can save the changes. To save the configuration, select **Commit Options** on the top right corner of the page and click **Commit**.



# 4 Enabling Security Services

This chapter provides the Unified Threat Management (UTM) and Intrusion Detection and Prevention (IDP) policy configuration and installation instructions for accessing your Dell PowerConnect J-Series J-SRX100S/SU Services Gateway.



**NOTE:** If you have not purchased the UTM or IDP licenses, do not proceed with the instructions provided in this chapter.

## Section 4 Contents

4.1 Activating Licenses on the Device . . . . .	26
4.2 Installing and Verifying a License . . . . .	26
4.3 Unified Threat Management . . . . .	26
4.4 Intrusion Detection and Prevention . . . . .	35

## 4.1 Activating Licenses on the Device

Before you can configure any UTM features, the UTM feature license must be installed on the device.

Follow the licensing activation instructions included with your license authorization code.

## 4.2 Installing and Verifying a License

To automatically add subscription licenses to the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway after registering, ensure that you are connected to the Internet and that DNS is configured.

To install and verify the installed license:

1. Click the **Maintain** tab at the top of the page and navigate to **Licenses**.
2. Click **Download Keys** to download the licenses automatically.
3. In the Feature Summary, check that all the licenses are installed.

Licenses				
Feature Summary				
Feature	Licenses Used	Licenses Installed	Licenses Needed	License Expires on
Kaspersky AV	0	3	0	2011-06-30
Anti Virus with Sophos Engine	0	2	0	2011-06-30
Anti-Spam	0	5	0	2011-06-30
Web Filtering	0	4	0	2011-06-30
IDP Signature	0	3	0	2011-06-30
AX411 WLAN AP	0	2	0	
Memory Upgrade	0	1	0	

Installed Licenses				
<input type="button" value="Add..."/>	<input type="button" value="Delete"/>	<input type="button" value="Display Keys..."/>		<input type="button" value="Download Keys"/>
ID	State	Version	Group	Enabled Features
<input type="checkbox"/> JUN05260100	valid	2	No group information	IDP Signature
<input type="checkbox"/> JUN05260101	valid	2	No group information	Kaspersky AV
<input type="checkbox"/> JUN05260102	valid	2	No group information	Anti-Spam
<input type="checkbox"/> JUN05260103	valid	2	No group information	Anti Virus with Sophos Engine
<input type="checkbox"/> JUN05260104	valid	2	No group information	Anti Virus with Sophos Engine
<input type="checkbox"/> JUN05260105	valid	2	No group information	Anti-Spam
<input type="checkbox"/> JUN05260106	valid	2	No group information	Web Filtering
<input type="checkbox"/> JUN05260107	valid	2	No group information	IDP Signature
<input type="checkbox"/> JUN05260108	valid	2	No group information	Anti-Spam
<input type="checkbox"/> JUN05260109	valid	2	No group information	Kaspersky AV
<input type="checkbox"/> JUN05260110	valid	2	No group information	Anti-Spam
<input type="checkbox"/> JUN05260111	valid	2	No group information	Web Filtering

## 4.3 Unified Threat Management

This section provides the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway configuration instructions for using a UTM policy to secure the network:

### 4.3.1 Enabling Anti-Virus

### 4.3.2 Enabling Web Filtering

### 4.3.3 Enabling Anti-Spam

### 4.3.4 Applying the UTM Configuration Settings

### 4.3.5 Verifying the UTM Configuration Settings

## 4.3.1 Enabling Anti-Virus

This section provides an example for configuring the full file-based anti-virus scanning feature using the default **junos-av-defaults** anti-virus profile. To enable anti-virus, you must perform the following configuration steps:

#### 4.3.1.1 Applying an Anti-Virus Profile to a UTM Policy

#### 4.3.1.2 Applying the UTM Policy to a Firewall Policy

#### 4.3.1.3 Creating an Anti-Virus Profile

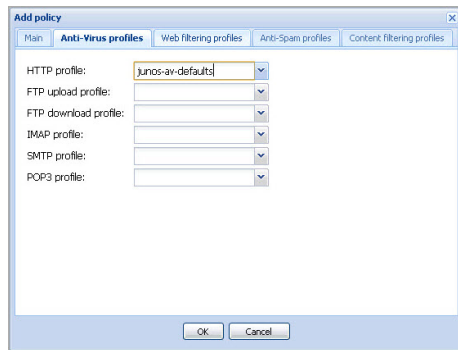
#### 4.3.1.1 Applying an Anti-Virus Profile to a UTM Policy

To apply an anti-virus profile to a UTM policy:



**NOTE:** You can either create a new UTM policy or use an existing UTM policy (if any exists) to add Anti-Virus to it. If you want to create a new anti-virus profile, see **“4.3.1.3 Creating an Anti-Virus Profile.”**

1. Click the **Configure** tab, choose **Security > Policy > UTM Policies**, and then click **Add**.
2. Click the **Main** tab and enter the policy name as **custom-utm-policy**.
3. Click the **Anti-Virus profiles** tab, select **junos-av-defaults** from the list in HTTP Profile box, and then click **OK**.

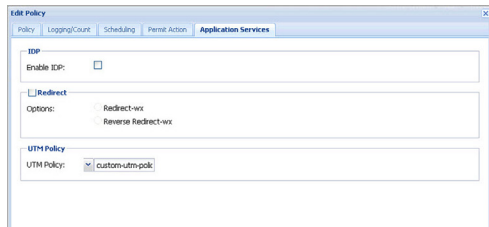


### 4.3.1.2 Applying the UTM Policy to a Firewall Policy

To inspect transit traffic and evaluate it against the anti-virus profile, you must apply the UTM policy to a firewall policy.

To apply the UTM policy to a firewall policy:

1. Click the **Configure** tab and choose **Security > Policy > FW Policies**.
2. Click **Edit** to edit an existing policy.
3. Click the **Application Services** tab.
4. In UTM Policy, select **custom-utm-policy** from the list.



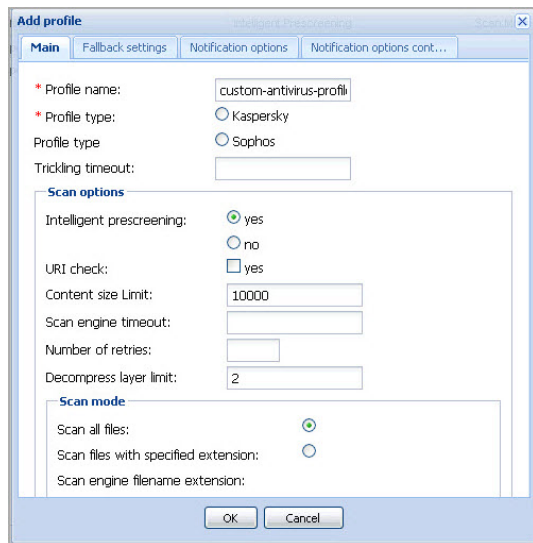
5. Click **OK**.

### 4.3.1.3 Creating an Anti-Virus Profile

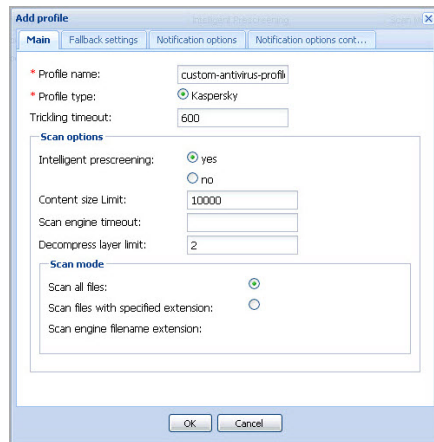
This task is optional and can be performed if you want to configure a new anti-virus profile.

To create an anti-virus profile:

1. Click the **Configure** tab and choose **Security > UTM > Anti-Virus**.
2. Click **Add** for a new anti-virus profile.



3. Do the following:
  - a. Enter a Profile name.  
For example, **custom-antivirus-profile**.
  - b. Select Profile Type as **Kaspersky**.
  - c. Enter the Trickling timeout.
4. In the Scan options, do the following:
  - a. Select the Intelligent prescreening as **yes**.
  - b. Enter the Content size Limit.
  - c. Enter the Decompress layer limit.
5. In the Scan mode, select **Scan all files**.
6. Click **OK**.



### 4.3.2 Enabling Web Filtering

This section provides an example for configuring the Web filtering feature using the default **junos-wf-cps-default** Web filtering profile. To enable Web filtering, you must perform the following configuration tasks:

#### 4.3.2.1 Applying a Web Filtering Profile to a UTM Policy

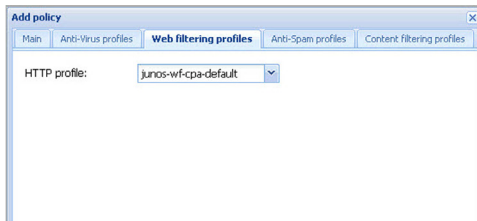
#### 4.3.2.2 Applying a UTM Policy to a Firewall Policy

#### 4.3.2.3 Creating a Web Filtering Profile

### 4.3.2.1 Applying a Web Filtering Profile to a UTM Policy

To configure the predefined Web filtering profile to use the configured UTM policy:

1. Click the **Configure** tab and choose **Security > Policy > UTM Policies**.
2. Click **Add**.
3. Click the **Main** tab and enter the policy name as **web-filtering-policy**.
4. Click the **Web filtering profiles** tab.
5. In HTTP Profile, select **junos-wf-cpa-default** from the list.



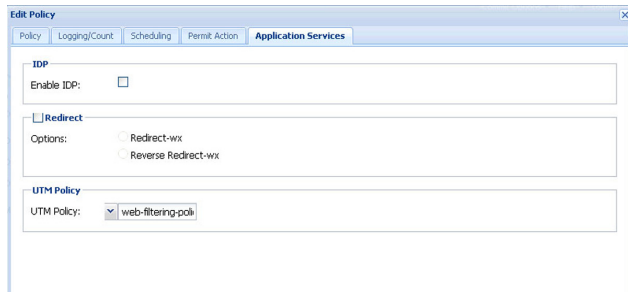
6. Click **OK**.

### 4.3.2.2 Applying a UTM Policy to a Firewall Policy

To inspect transit traffic and evaluate it against the Web filtering profile, you must apply the UTM policy to a firewall policy.

To apply a UTM policy to a firewall policy:

1. Click the **Configure** tab and choose **Security > Policy > FW Policies**.
2. Click **Edit** to edit an existing policy.
3. Click the **Application Services** tab.
4. In UTM Policy, select **web-filtering-policy** from the list.



5. Click **OK**.
6. Click **Commit Options** on the top right corner of the page and click **Commit**.



**NOTE:** If you want to create a new Web filtering profile, see [“4.3.2.3 Creating a Web Filtering Profile.”](#)

### 4.3.2.3 Creating a Web Filtering Profile

This task is optional and can be performed if you want to configure a new Web filtering profile.

To create a Web filtering profile:

1. Click the **Configure** tab and choose **Security > UTM > Web Filtering**.
2. Click **Global Options** at the top right corner of the page.
3. In Filtering type, select **Surf Control Integrated**.
4. In Surf Control Integrated Options, enter the value for Cache time out and Cache size.
5. Click **OK**.

The screenshot shows a dialog box titled "Global WF Options". It contains the following fields and options:

- URL whitelist: [text box]
- URL blacklist: [text box]
- Filtering type**
  - Surf Control Integrated:
  - WebSense Redirect:
  - Local:
- Surf Control Integrated Options**
  - Cache timeout: [text box with value 10]
  - Cache size: [text box with value 20]
  - Server host: [text box with value cpa.surfcpa.com]
  - Server port: [text box with value 9020]

Buttons: OK, Cancel

6. Click **Add** on the top right corner.
7. In the Main tab, do the following:
  - a. Enter the Profile name.  
For example, **custom-web-filtering-profile**.
  - b. Select **Permit** in default action.
  - c. Enter the timeout value.
8. Click **OK**.

### 4.3.3 Enabling Anti-Spam

This section provides an example for configuring the anti-spam feature using the default **junos-as-defaults** anti-spam profile. To enable UTM anti-spam on the Dell PowerConnect J-SRX100S/SU Services Gateway, you must perform the following tasks:

#### 4.3.3.1 Applying an Anti-Spam Profile to a UTM Policy

#### 4.3.3.2 Applying a UTM Policy to a Firewall Policy

#### 4.3.3.3 Creating an Anti-Spam Profile

### 4.3.3.1 Applying an Anti-Spam Profile to a UTM Policy

To configure the predefined anti-spam profile to use a UTM policy:

1. Click the **Configure** tab and choose **Security > Policy > UTM Policies**.
2. Click **Edit**.
3. Click the **Anti-Spam profiles** tab.



4. In SMTP profile, select **junos-as-defaults** from the list.
5. Click **OK**.



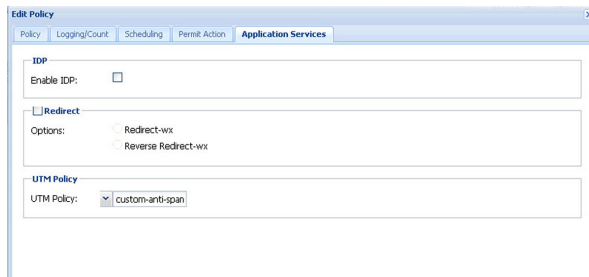
**NOTE:** If the configuration delivery status is fail, click **Details** for more information. If you want to create a new anti-spam profile, see **“4.3.3.3 Creating an Anti-Spam Profile.”**

### 4.3.3.2 Applying a UTM Policy to a Firewall Policy

To inspect transit traffic and evaluate it against the anti-spam profile, you must apply the UTM policy to a firewall policy.

To apply a UTM policy to a firewall policy:

1. Click the **Configure** tab and choose **Security > Policy > FW Policies**.
2. Click **Edit** to edit an existing policy.
3. Click the **Application Services** tab.



4. In UTM Policy, select the required UTM policy from the list.
5. Click **OK**.

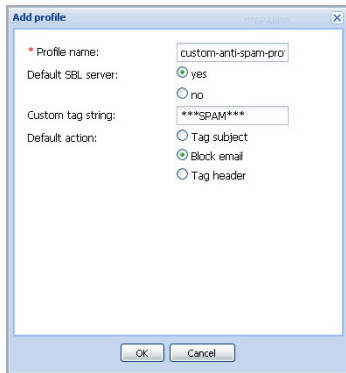


### 4.3.3.3 Creating an Anti-Spam Profile

This task is optional and can be performed if you want to configure a new anti-spam profile.

To create a new anti-spam profile:

1. Click the **Configure** tab and choose **Security > UTM > Anti-Spam**.
2. Click **Add**.



3. Enter the profile name.



**NOTE:** By default, the Default SBL server is **yes** and the Default action is **Block email**.

4. Click **OK**. The download successful message appears.
5. Click **OK**.



**NOTE:** If the configuration delivery status is Fail, click **Details** for more information.

### 4.3.4 Applying the UTM Configuration Settings

To save the UTM configuration settings, select **Commit Options** at the top right corner of the page and click **Commit**.

### 4.3.5 Verifying the UTM Configuration Settings

To verify the UTM configuration settings, perform the following tasks:

#### 4.3.5.1 Verifying an Anti-Virus Configuration

#### 4.3.5.2 Verifying a Web Filtering Configuration

#### 4.3.5.3 Verifying an Anti-Spam Configuration

### 4.3.5.1 Verifying an Anti-Virus Configuration

To verify an anti-virus configuration:

1. Click the **Monitor** tab.
2. Choose **Security > UTM > Anti-Virus**.



**NOTE:** Click the plus sign (+) to view the UTM anti-virus statistics. If you want to clear the data, click **Clear Anti-Virus Statistics**.

UTMs	
Anti-Virus	
UTM Anti-Virus	
AV Key Expire Date :	0311-06-29 20:00:00
Update Server :	http://update.suniper-updates.net(AV/SRV100)
Interval :	60
Auto Update Status :	next update in 1 minutes
Last Result :	download list file failed
AV Signature Version :	not loaded
Scan Engine Info :	
Pattern Type :	
UTM Anti-Virus Statistics	
Antivirus Statistics	
Statistics type	Counter
Intelligent_prescreening Passed :	0
Forwarded to scan engine :	
Scan Mode	Counter
Scan All	0
Scan Extension	0
Fall Back	Log and Permit Block
Engine Not Ready	0 0
Password File	0 0
Decompress Layer	0 0
Corrupt File	0 0
Out Of Resources	0 0
Timeout	0 0
Maximum Content Size	0 0
Too Many Requests	0 0
Others	0 0
<a href="#">Clear Anti-Virus Statistics</a>	

### 4.3.5.2 Verifying a Web Filtering Configuration

To verify a Web filtering configuration:

1. Click the **Monitor** tab.
2. Choose **Security > UTM > Web Filtering**.



**NOTE:** If you want to clear the data, click **Clear Web Filtering Statistics**.

UTMs		
Web Filtering		
UTM Web Filtering Statistics		
Statistics type	Counter	
Total Requests :	0	
White List Hit :	0	
Black List Hit :	0	
Queries To Server :	0	
Server Reply Permit :	0	
Server Reply Block :	0	
Custom Category Permit :	0	
Custom Category Block :	0	
Cache Hit Permit :	0	
Cache Hit Block :	0	
Web Filtering Session total :	4000	
Web Filtering Session Inuse :	0	
Fall Back	Log and Permit	Block
Default :	0	0
Timeout :	0	0
Server-Connectivity :	0	0
Too-Many-Requests :	0	0
<a href="#">Clear Web Filtering Statistics</a>		

### 4.3.5.3 Verifying an Anti-Spam Configuration

To verify an anti-spam configuration:

1. Click the **Monitor** tab.
2. Choose **Security > UTM > Anti-Spam**.



**NOTE:** If you want to clear the data, click **Clear Anti-Spam Statistics**.

UTMs		
Anti-spam		
UTM Anti-spam Status		
DNS Server Setting :		
DNS Server	IP	Source Interface
Primary	208.67.222.222	Fe-0/0/0
Secondary	192.168.5.68	Fe-0/0/1
Tertiary	192.168.60.131	Fe-0/0/2
UTM Anti-spam Statistics		
Statistics type	Counter	
Total Connections:	0	
Denied Connections :	0	
Total Greetings :	0	
Denied Greetings :	0	
Total Email Scanned :	0	
Spam Total :	0	
Spam Tagged :	0	
Spam Dropped :	0	
DNS Errors :	0	
Timeout Errors :	0	
Return Errors :	0	
Invalid Parameter Errors :	0	
Statistics Start time :	07/28/2010 22:17:04	
Statistics for the last 10 days		
Day	Permitted Emails/Spams	
	None Found	
<input type="button" value="Clear Anti-spam Statistics"/>		

## 4.4 Intrusion Detection and Prevention

This section provides the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway configuration instructions for using a predefined IDP Series policy to secure the network:

### 4.4.1 Downloading and Installing the Latest Security Package

### 4.4.2 Downloading and Installing the IDP Security Policy Templates

### 4.4.3 Loading the Policy Templates File

### 4.4.4 Configuring an Active IDP Policy

### 4.4.5 Enabling IDP Series Detection on the Existing Firewall Security Policy

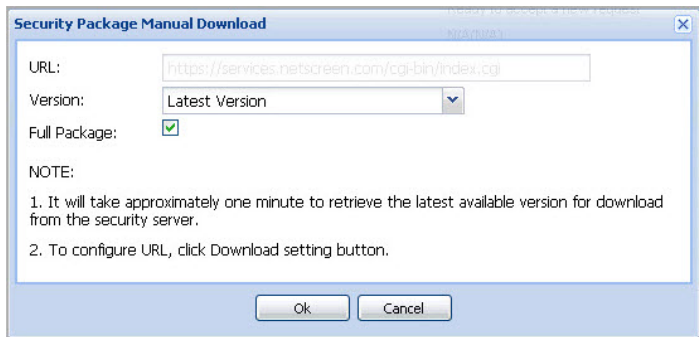
### 4.4.6 Applying the IDP Configuration Settings

### 4.4.7 Verifying the IDP Configuration Settings

### 4.4.1 Downloading and Installing the Latest Security Package

To download and install the latest security package:

1. Click the **Configure** tab and choose **Security > IDP > Signature Update**.
2. Click the **Download** tab and select **Latest Version** from the list.

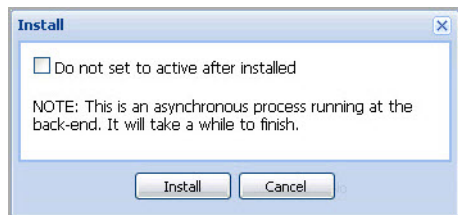


3. Select **Full Package** and click **OK**. The downloading message appears.



**NOTE:** It will take a few minutes to download. You can verify the progress of download by clicking **Check Status > Download Status**.

4. Click **OK**.
5. Click the **Install** tab in the Security IDP Signature Configuration page.



6. Click **Install**.



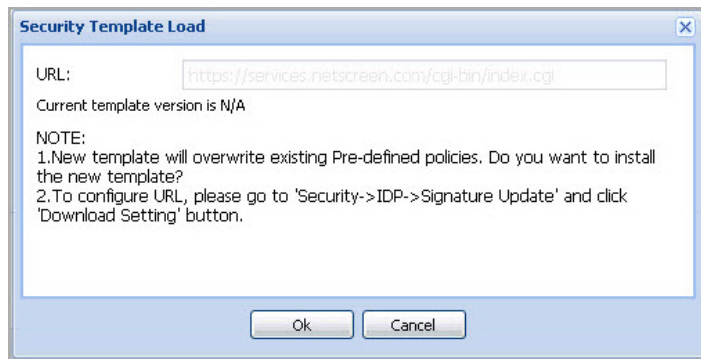
**NOTE:** The request will be processed in asynchronous mode. It will take a few minutes to install. You can verify the progress of an installation by clicking **Check Status > Install Status**.

7. Click **OK**. The installation successful message appears.
8. Click **OK**.

## 4.4.2 Downloading and Installing the IDP Security Policy Templates

To download and install the IDP security policy templates:

1. Click the **Configure** tab and choose **Security > Policy > IDP Policies**.
2. Click the **Template** tab and select **Download Template**.



3. Click **OK**.
4. Click the **Template** tab and select **Install Template**.
5. Click **OK**.



**NOTE:** You can verify the progress of a download or installation by clicking **Check Status > Download Status** or **Check Status > Install Status**.

## 4.4.3 Loading the Policy Templates File

To view all the pre-defined IDP templates available on the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway, you must load the policy templates file.

To load the policy templates file:

1. Click the **Configure** tab and choose **Security > Policy > IDP Policies**.
2. Click the **Template** tab and select **Load Template**.



**NOTE:** It will take a few minutes to load the Templates file.

3. Click **OK**.



**NOTE:** If the configuration delivery status is fail, click **Details** for more information.

## 4.4.4 Configuring an Active IDP Policy



**NOTE:** Before you use one of the predefined Junos IDP policies as an active policy, you must load the policy templates. See “**4.4.3 Loading the Policy Templates File.**”

To configure an active IDP policy:

1. Click the **Configure** tab and choose **Security > Policy > IDP Policies**.
2. Click the Recommended policy link, and then click **Activate** at the top right corner of the page.

The screenshot shows the 'IDP Policy Configuration' window with a 'Policy List' table. The table has columns for Status, Name, Type, IPS Rule Number, and Exempt Rule Number. The 'Recommended' policy is the only one with an 'Active' status.

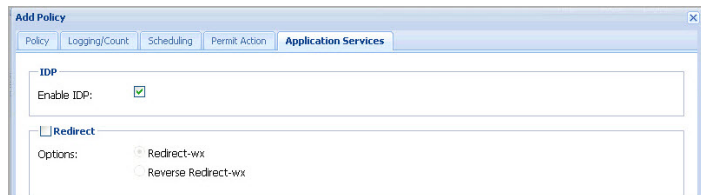
Status	Name	Type	IPS Rule Number	Exempt Rule Number
Inactive	Web_Server	pre-defined	4	0
Inactive	DMZ_Services	pre-defined	4	0
Inactive	DNS_Service	pre-defined	3	0
Inactive	File_Server	pre-defined	4	0
Inactive	Getting_Started	pre-defined	9	0
Inactive	IDP_Default	pre-defined	3	0
Active	Recommended	pre-defined	9	0

## 4.4.5 Enabling IDP Series Detection on the Existing Firewall Security Policy

To enable IDP series detection on the existing firewall security policy from the trust zone to the untrust zone:

1. Click the **Configure** tab and choose **Security > Policy > FW Policies**.
2. Click **Edit** to edit a policy.

3. Click the **Application Services** tab and select **Enable IDP**.



4. Click **OK**.

#### 4.4.6 Applying the IDP Configuration Settings

To save the IDP configuration settings, select **Commit Options** at the top right corner of the page and click **Commit**.

#### 4.4.7 Verifying the IDP Configuration Settings

To verify the IDP configuration settings:

1. Click the **Monitor** tab.
2. Choose **Security > IDP > Status**.

IDP			
Status			
<b>IDP Status</b>			
<b>Status of IDP</b>	Disabled		
<b>Up Since</b>	2010-07-28 22:14:19 EDT ( 03:02:44 ago)		
<b>Packets/Second</b>	0		
<b>Peak</b>	0 @ 2010-07-29 01:01:21 EDT		
<b>Kbits/Second</b>	0		
<b>Peak Kbits</b>	0 @ 2010-07-29 01:01:21 EDT		
<b>Latency (Microseconds)</b>	[min:0] [max:0] [avg:0]		
<b>Current Policy</b>	none		
<b>IDP Memory Statistics</b>			
PIC Name	Total IDP Data Plane Memory(MB)	Used(MB)	Available(MB)
	212	20	192

## 5 Powering Off the Device

To power off the services gateway, you can shut it down in one of the following ways:

- Graceful shutdown—Press and immediately release the **Power** button. The device begins gracefully shutting down the operating system.
- Forced shutdown—Press the **Power** button and hold it for 10 seconds. The device immediately shuts down. Press the **Power** button again to power on the device.



**NOTE:** You can reboot or halt the system in J-Web by selecting **Maintain > Reboot**.

---



## 6 Support and Training Options

This chapter provides a link to customer support and technical documentation information for the Dell PowerConnect J-Series J-SRX100S/SU Services Gateway device.

### Section 6 Contents

<b>6.1 Customer Support</b> .....	<b>42</b>
<b>6.2 Technical Documentation</b> .....	<b>42</b>

## 6.1 Customer Support

If there are any technical issues while setting up Dell PowerConnect J-Series J-SRX100S/SU Services Gateway, contact Dell customer support **[www.support.dell.com](http://www.support.dell.com)**.

## 6.2 Technical Documentation

For Technical documentation, refer to **[www.support.dell.com/manuals](http://www.support.dell.com/manuals)**.





Information in this document is subject to change without notice. All rights reserved. Reproduction of these materials in any manner whatsoever without the written permission of Juniper Networks is strictly forbidden. Trademarks used in this text: Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc. Juniper Networks® and G33® are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785. Copyright© 2010, Juniper Networks, Inc. All rights reserved. Printed in USA.

 Printed on recycled paper

Part Number 530-036103, Revision 1, August 2010