Configuration Guide

How to set up the IPsec site-to-site Tunnel between the D-Link DSR Router and the Juniper Firewall

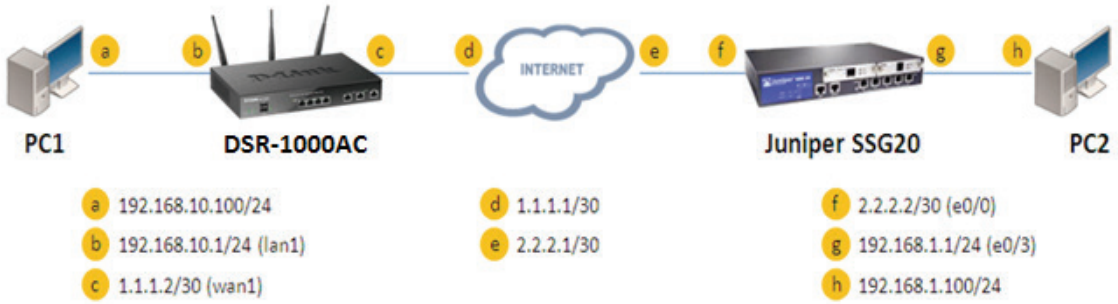
Overview

This document describes how to implement IPsec with pre-shared secrets establishing a site-to-site VPN tunnel between the D-Link DSR-1000AC and the Juniper SSG20. The screenshots in this document are from firmware version 3.10 of the DSR-1000AC and firmware version 6.3.0r24 (Released in June 2017) of the Juniper SSG20. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see in your browser.

D-Link®

Situation note

Site-to-site VPNs can be implemented in an enterprise to allow access and the exchange of data between two or more geographically separated sites or offices. Once the site-to-site VPN has been set up, the clients in the groups of the different sites can communicate as if they are on the same internal network. Because companies may have other gateways that are not D-Link products, this document can be used to create IPsec VPN tunnels between the DSR router and other existing gateway appliances.



IP addresses:
DSR WAN: **1.1.1.2/30**
DSR LAN: **192.168.10.1/24**

Juniper_SSG20 Untrust_Zone(e0/0): **2.2.2.2/30**
Juniper_SSG20 Trust_Zone(e0/3): **192.168.1.1/24**

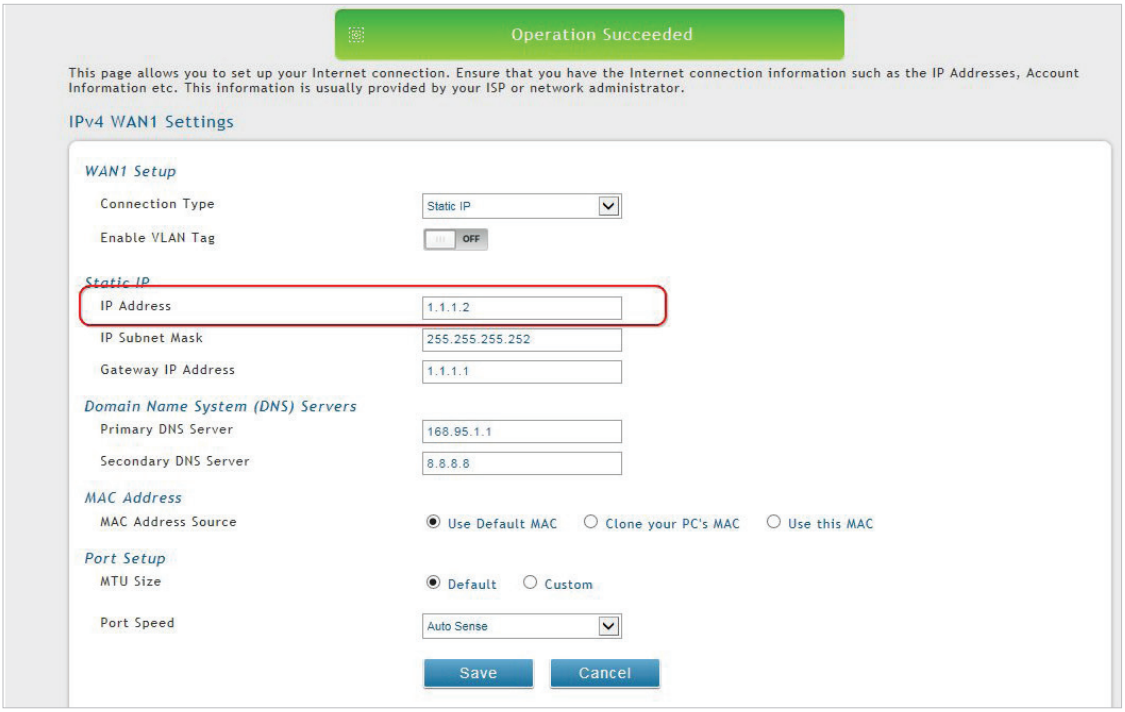
IPsec Parameters:
IPsec Mode: **Tunnel Mode**
IPsec Protocol: **ESP**
Phase1 Exchange Mode: **Main**
Phase1 Encryption: **3DES**
Phase1 Authentication: **SHA1**
Phase1 Authentication Method: **Pre-Shared Key**

Diffie-Hellman Group: **G2**
Phase1 Lifetime: **28800 sec**
Phase2 Encryption: **3DES**
Phase2 Authentication: **SHA1**
Phase2 Lifetime: **3600 sec**

Configuration Step

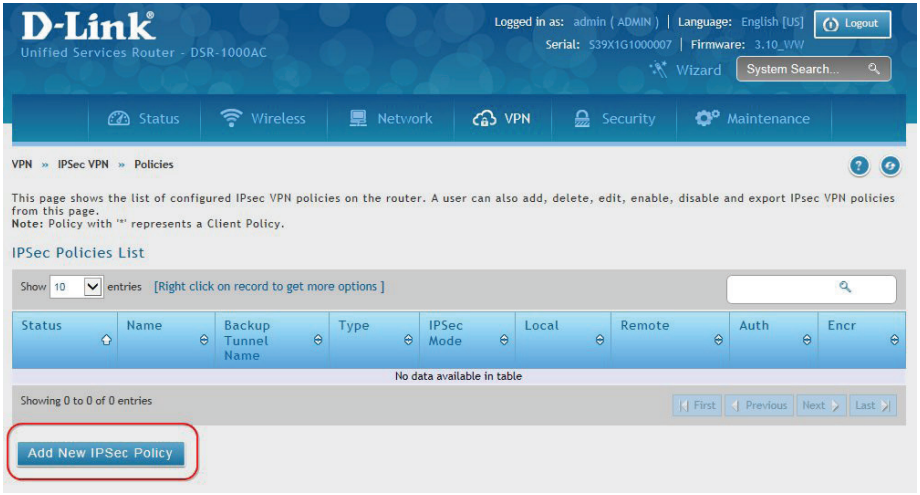
DSR Settings

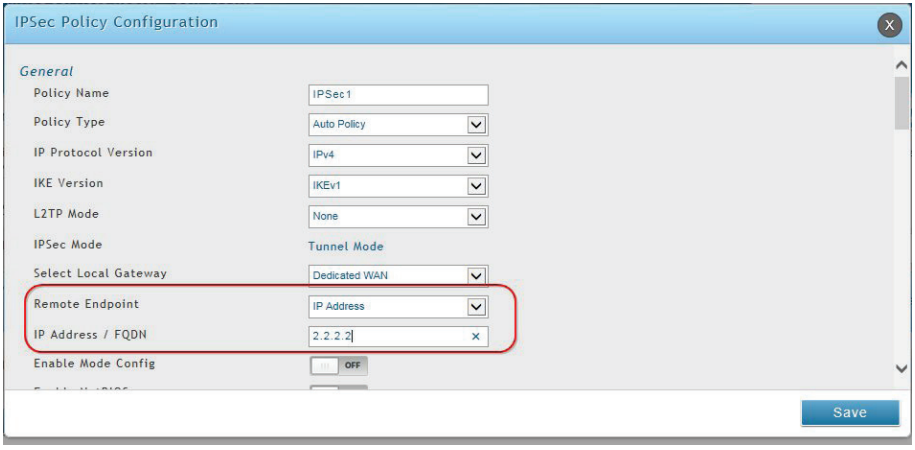
1. Set up the WAN IP address. Navigate to: Internet Settings > WAN1 Settings > WAN1 Setup.
Fill in the relevant information based on the settings of the topology. The **IP Address** of the ISP Connection Type field is the IP address of the external network connection shown as point "**c**" in the topology. Click the button "**Save**" button to complete the WAN IP address setting.

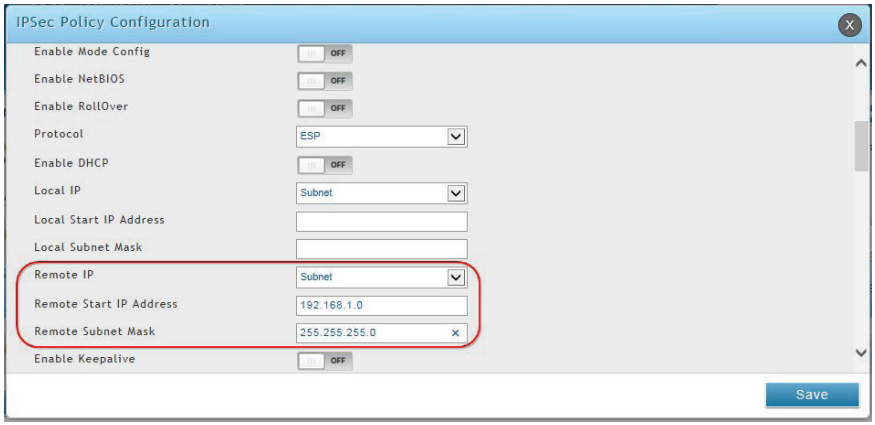


2. Set up the IPsec policy. Navigate to: VPN Settings > IPsec > IPsec Policies.

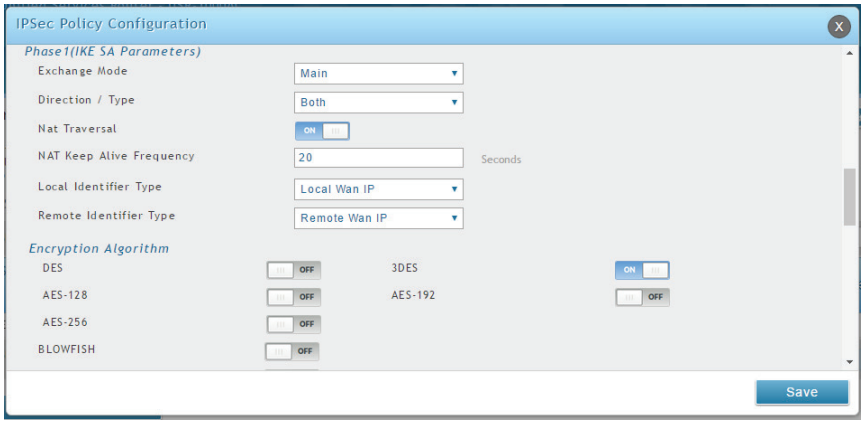
Press the "**Add New IPsec Policy**" button to create a new policy. In the General section, fill in the relevant information. The IP address of the **Remote Endpoint** refers to the external connection of the Juniper SSG20, which is shown as the point "**f**" in the topology. The internal IP address range, which is indicated by the **Local Start IP Address**, is the IP range allowed access to the remote network group over the VPN, which indicated by the IP information on **Remote Start IP Address**, is the IP range reachable through the VPN tunnel with the Juniper SSG20.

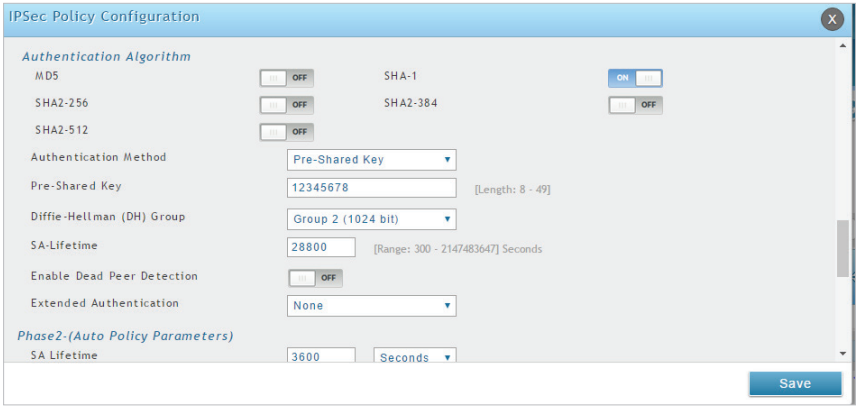




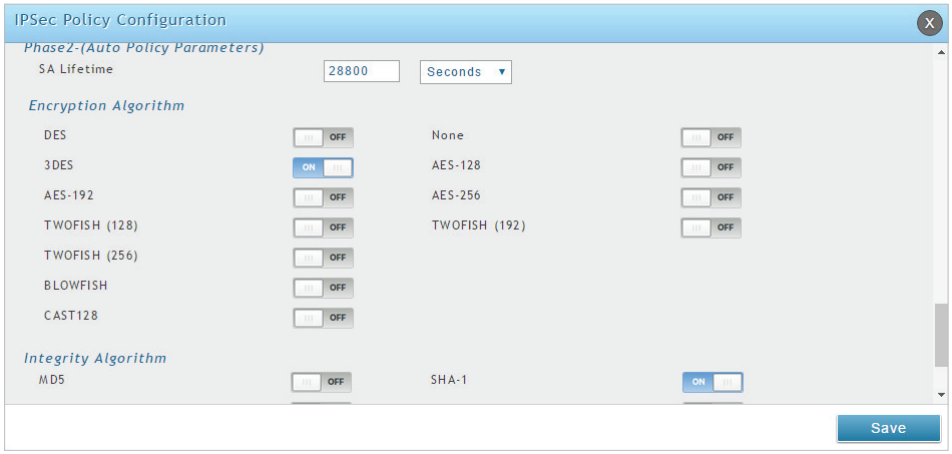


In the Phase 1 section, fill in the relevant information. Please notice that the **Pre-shared Key** must be the same as the pre-shared key that will be entered into the Juniper SSG20 later.

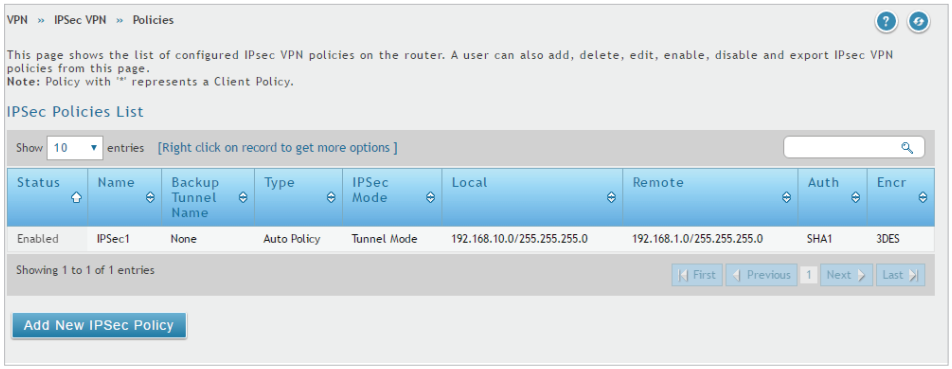




In the Phase 2 section, fill in relevant information.

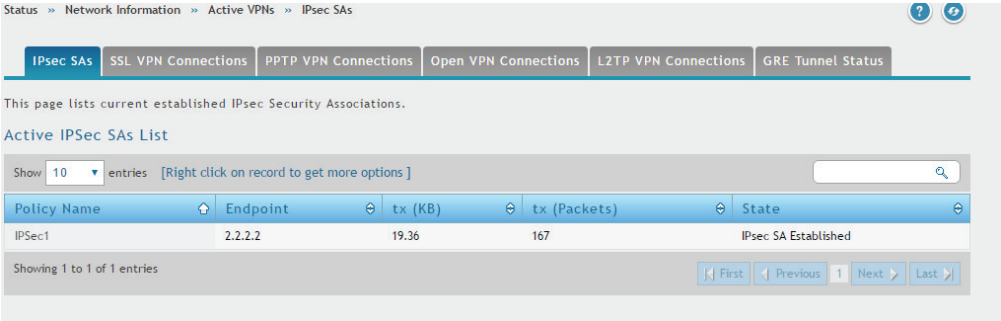


Click the "**Save**" button to complete the IPsec Policy settings.



3. Check the VPN status. Navigate to: Status > Active VPNs.

The activity will be shown in the list as the tunnel is established with the other side.

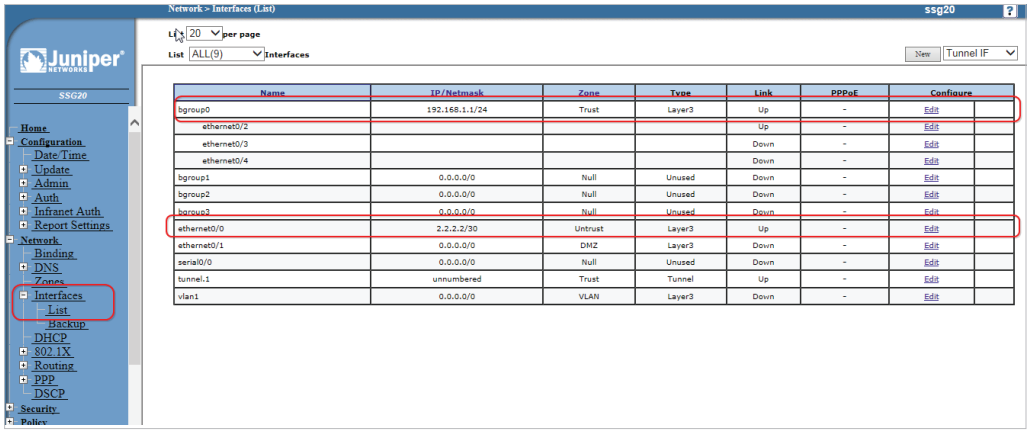


Juniper_SSG20 Settings

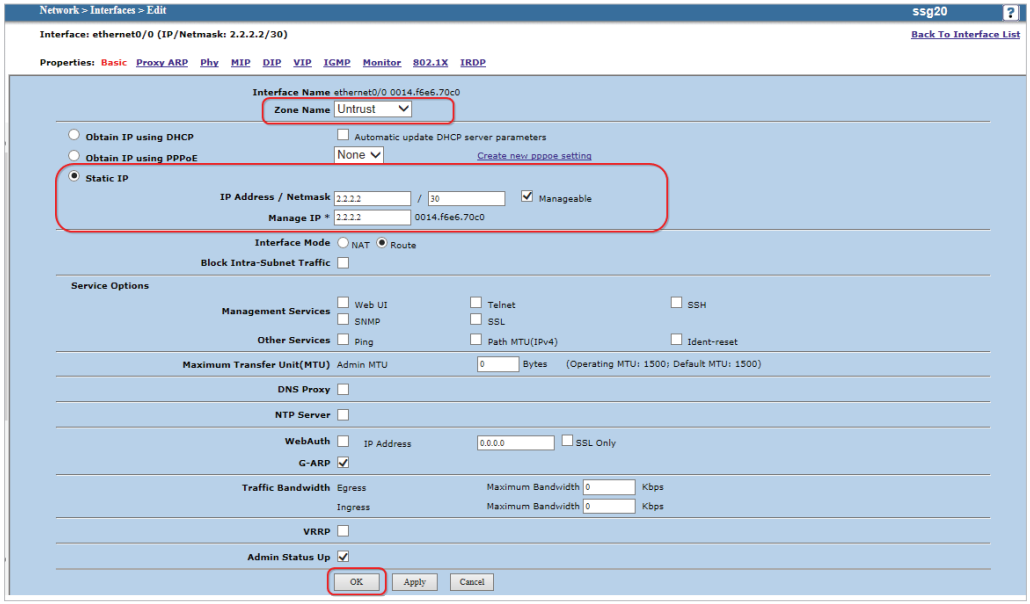
1. Set up the Untrust_Zone (WAN port) and Trust_Zone (LAN port) IP addresses.

Navigate to: Network > Interfaces > List.

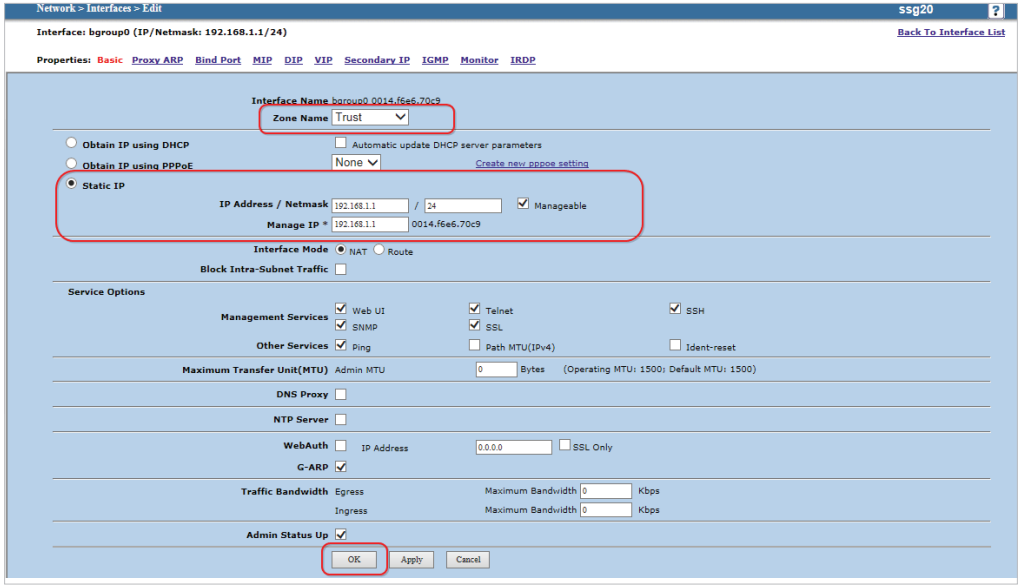
Click "**Edit**".



Configure the Untrust_Zone interface with the relevant information as below. The **IP Address/ Netmask** of the Basic tab is the IP address of external network connection, which is shown as point "f" in the topology. Click the "**OK**" button to finish this configuration.

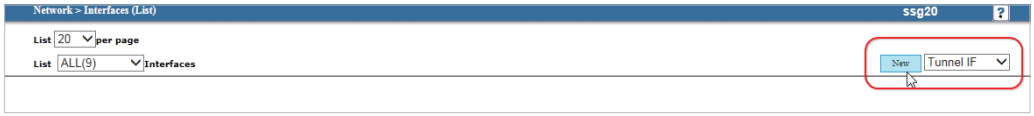


Configure Trust_Zone interface with the relevant information as below. The **IP Address/ Netmask** of the Basic tab is the IP address of the internal network connection, which is shown as point "**g**" in the topology. Click the "**OK**" button to finish this configuration.

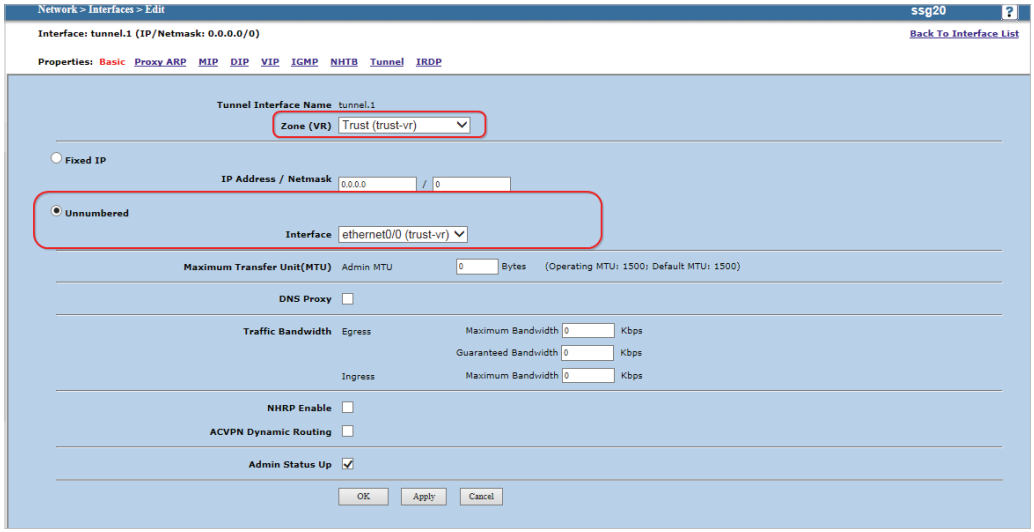


2. Add a Tunnel Interface. Navigate to: Network > Interfaces > List.

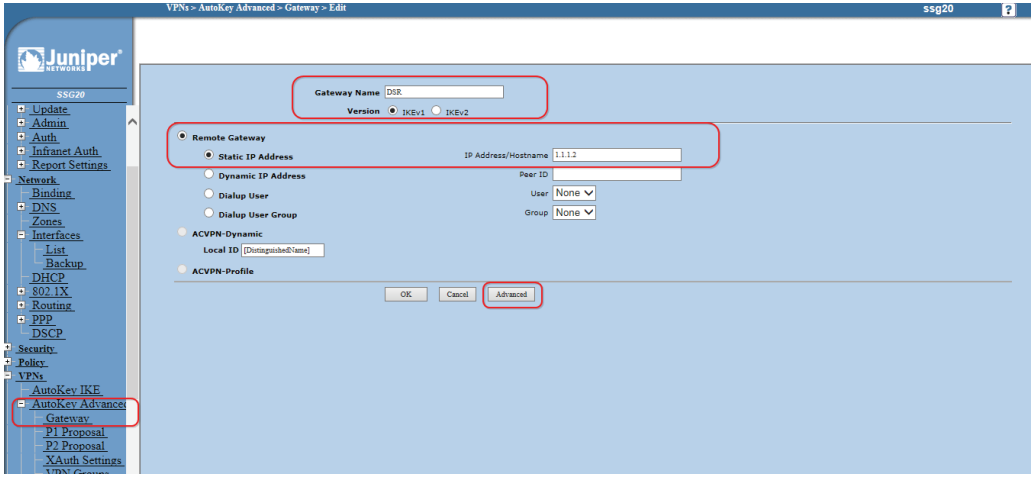
Select "**TunnelIF**" from the scroll down menu. Press the "**New**" button to create a new tunnel interface.



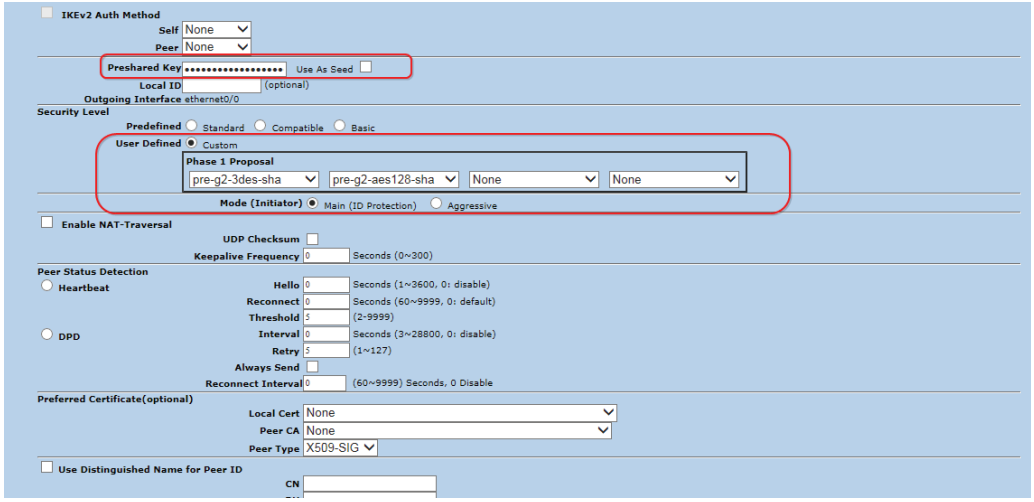
Configure the relevant settings as below.



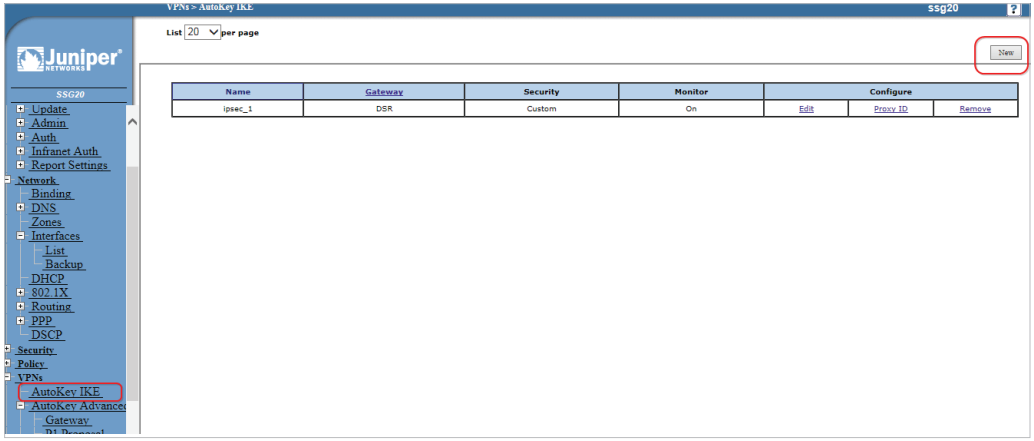
3. Add an IPsec Remote Gateway. Navigate to: VPNs > AutoKey Advanced > Gateway.
Press the "**New**" button and fill in relevant information as below.



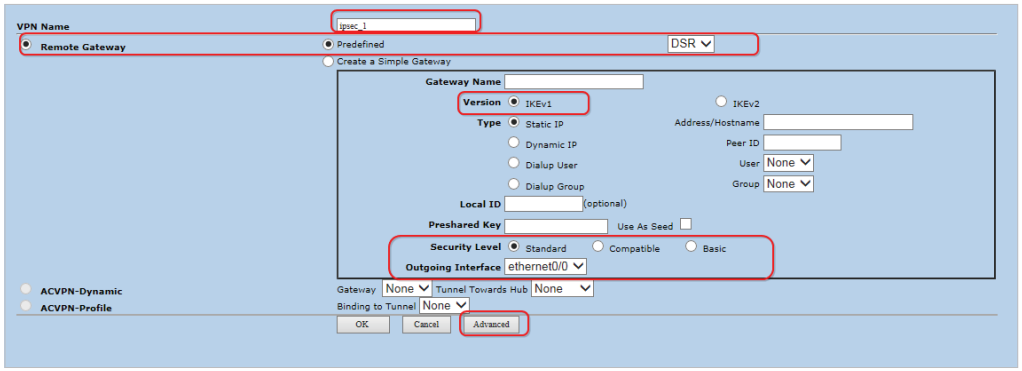
Press the "**Advanced**" button to configure the preshared key setting. Fill in the relevant information as below.
Insert the **Pre-shared Key**, which is the same as the one previously entered in the DSR-1000AC.



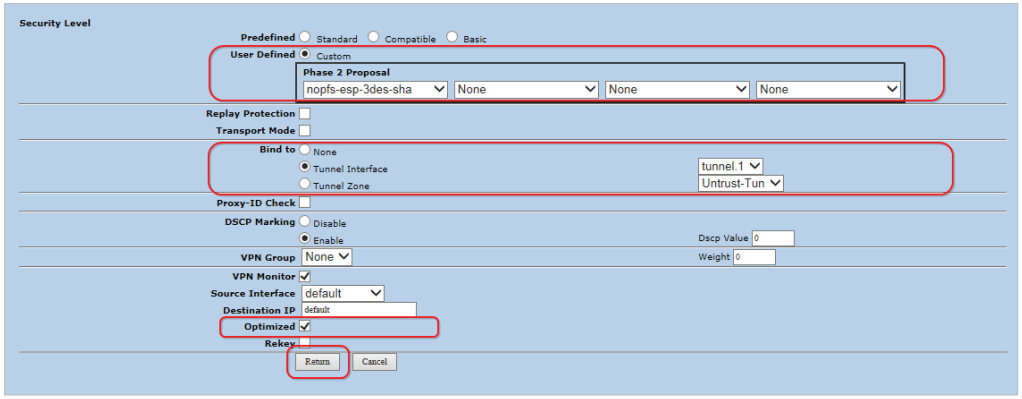
4. Create a new VPN tunnel. Navigate to: VPNs > AutoKey IKE.
Press the "**New**" button.



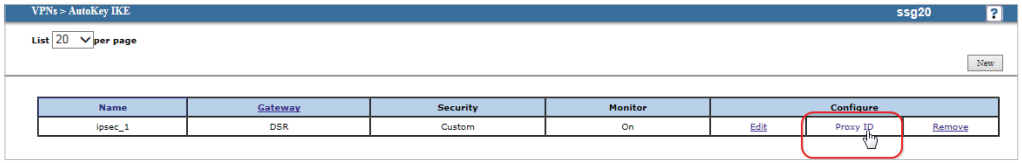
Fill in relevant information as below.



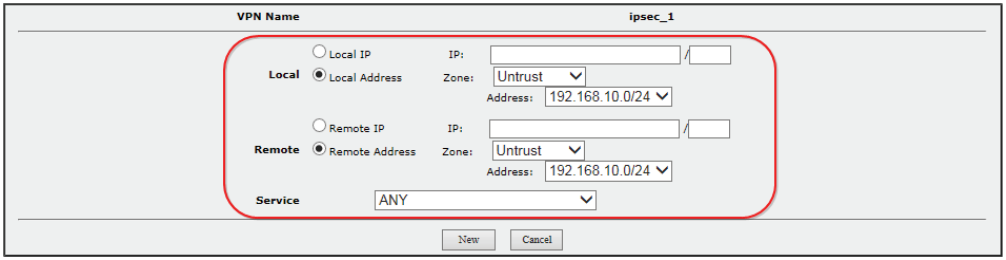
Press the "**Advanced**" button and configure the settings as below and click "**Return**".



Click "**Proxy ID**".

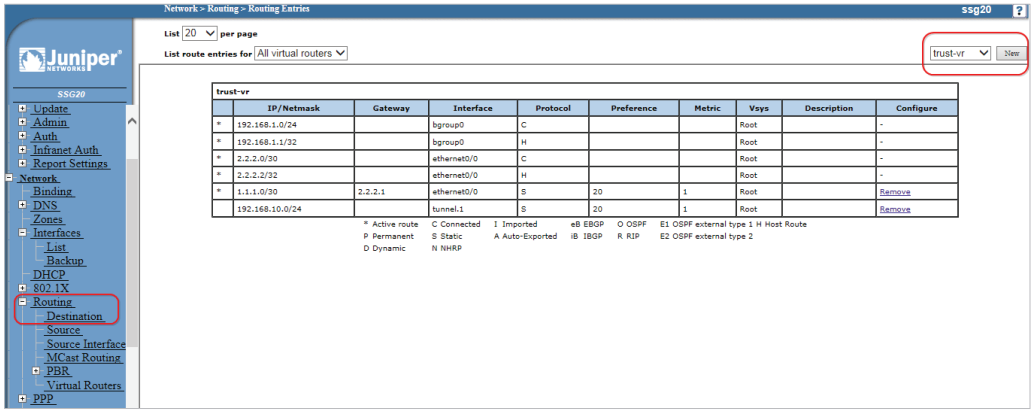


The internal IP address range, indicated by the **Local IP/ Netmask** field, is the range of addresses allowed access to the remote network over the VPN, and the remote network range, indicated by **Remote IP/ Netmask** field, is the IP address range reachable through the VPN with the DSR-1000AC.

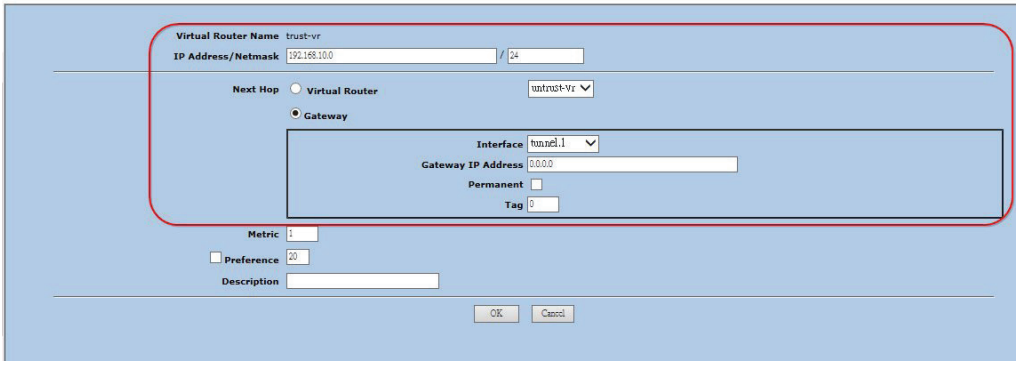


5. Create the Routings. Navigate to: Network > Routing > Destination.

Select "**trust-vt**" from the drop-down menu on the top left corner. Press the "**New**" button.



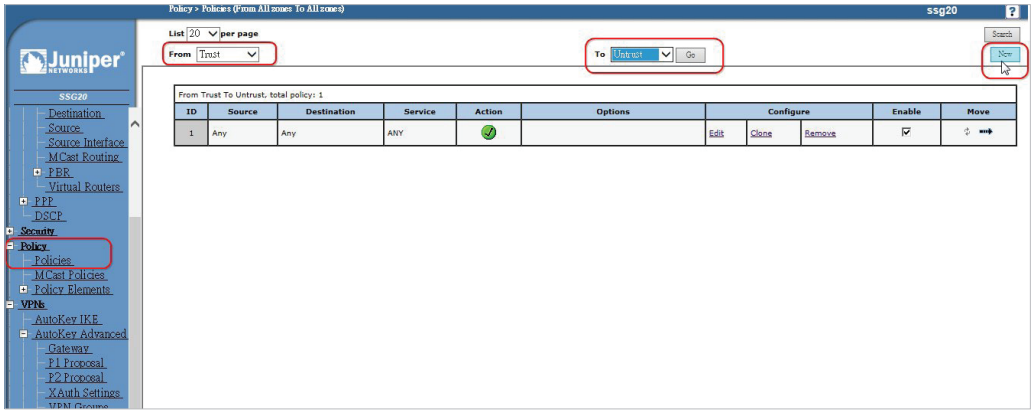
Fill in the relevant information as below.



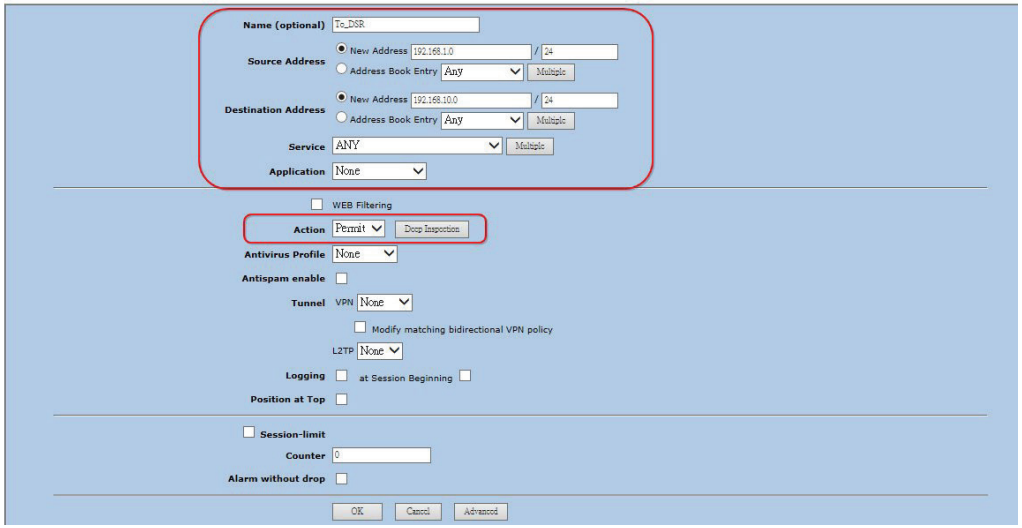
6. Set up the Policies. Navigate to: Policy> Policies.

Create the first rule. Select "**Trust**" and "**Untrust**" in the "From" and "To" drop-down menus respectively.

Press the "**New**" button.

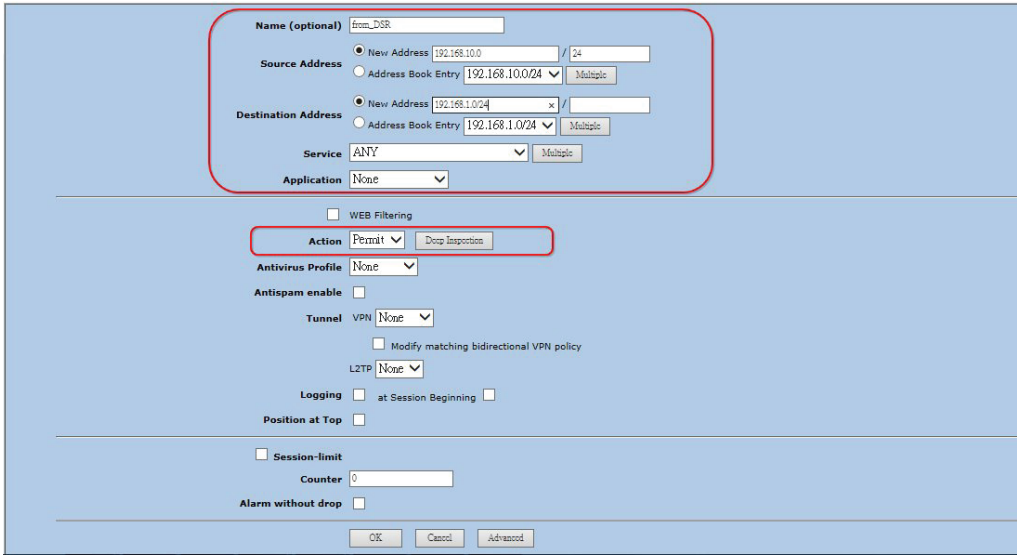


Fill in the relevant information as below.

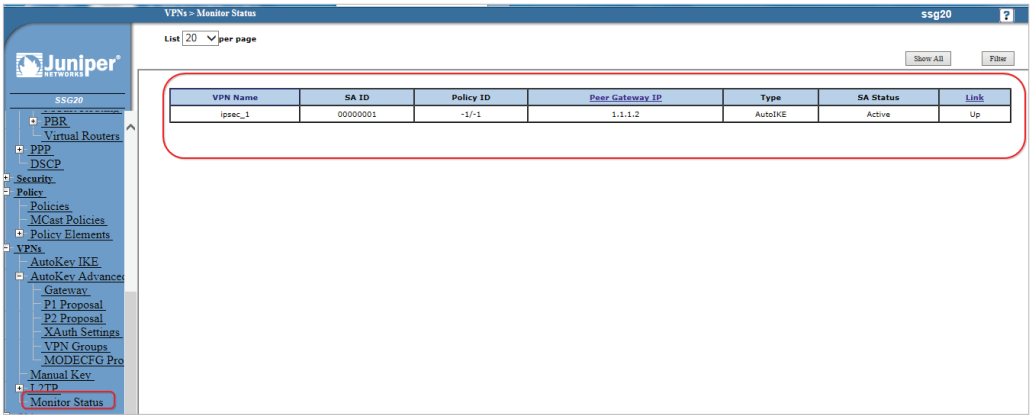


Create the second rule. Select "**Untrust**" and "**Trust**" in the "From" and "To" drop down menus respectively. Press the "**New**" button.

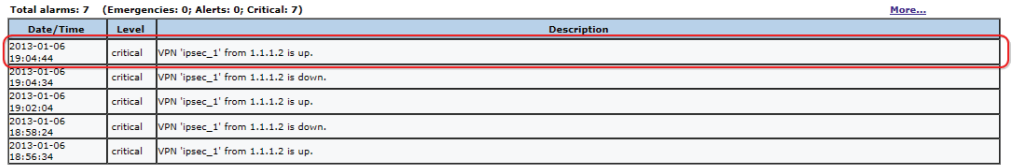
Fill in the relevant information as below.



7. Check VPN status. Navigate to: VPNs > Monitor Status.



Status logs are also viewable on the homepage.



D-Link®

Visit our website for more information
www.dlink.com