Configuration Guide

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

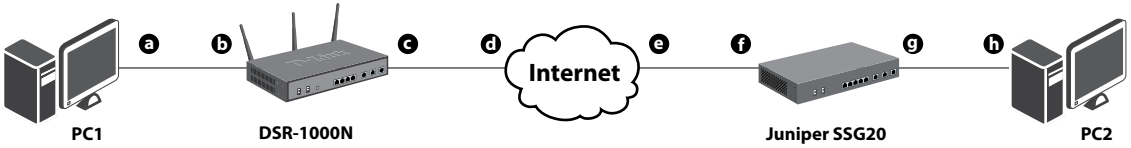
Overview

This document describes how to implement IPSec with pre-shared secrets establishing site-to-site VPN tunnel between the D-Link DSR-1000N and the Juniper SSG20. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 6.2 0r 2.0 of Juniper SSG20. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

D-Link®

Situation note

Site-to-site VPN could be implemented in an enterprise allows to access and exchange data among more than two geographical sites or offices. Once the site-to-site VPN set up, the clients in the groups of the different located sites are as in the internal networks. As companies may have other gateway appliances which are not D-Link products, this document will be useful when you intend to create IPSec VPN tunnel between DSR and other existing gateway appliance.



a 192.168.10.100/24
b 192.168.10.1/24 (LAN 1)
c 1.1.1.2/30 (WAN1)

d 1.1.1.1/30
e 2.2.2.1/30

f 2.2.2.2/30 (e0/0)
g 192.168.1.1/24 (e0/3)
h 192.168.1.100/24

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

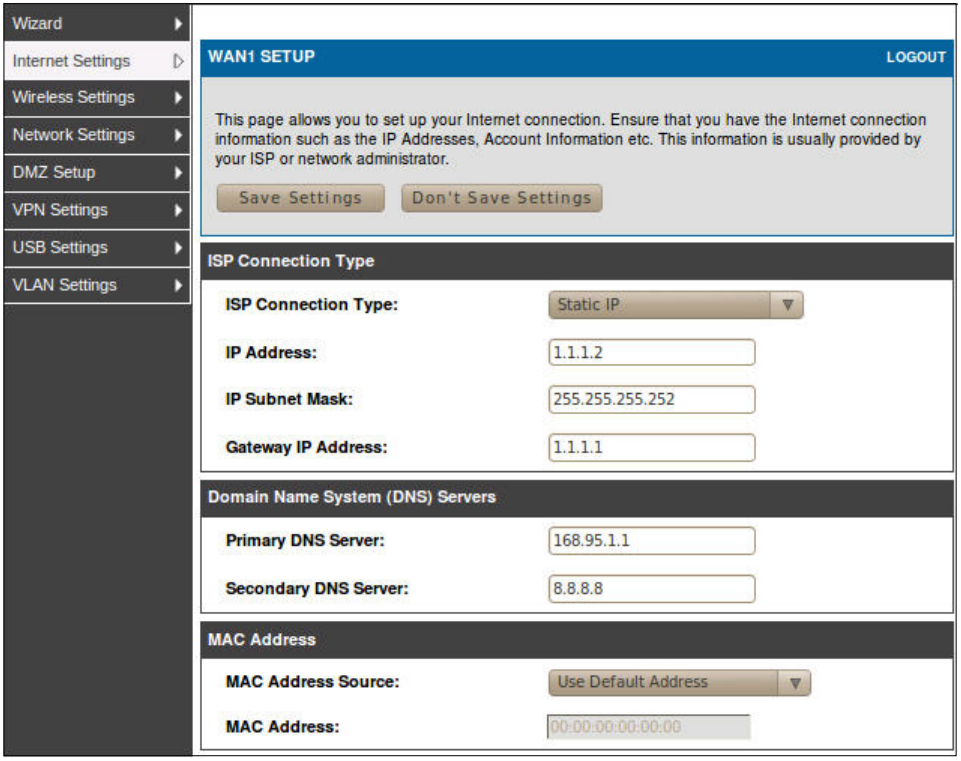
IPSec Mode: **Tunnel Mode**
IPSec Protocol: **ESP**
Phase1 Exchange Mode: **Main**
Phase1 Encryption: **3DES**
Phase1 Authentication: **SHA1**
Phase1 Authentication Method: **Pre-Shared Key**

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

Configuration Step

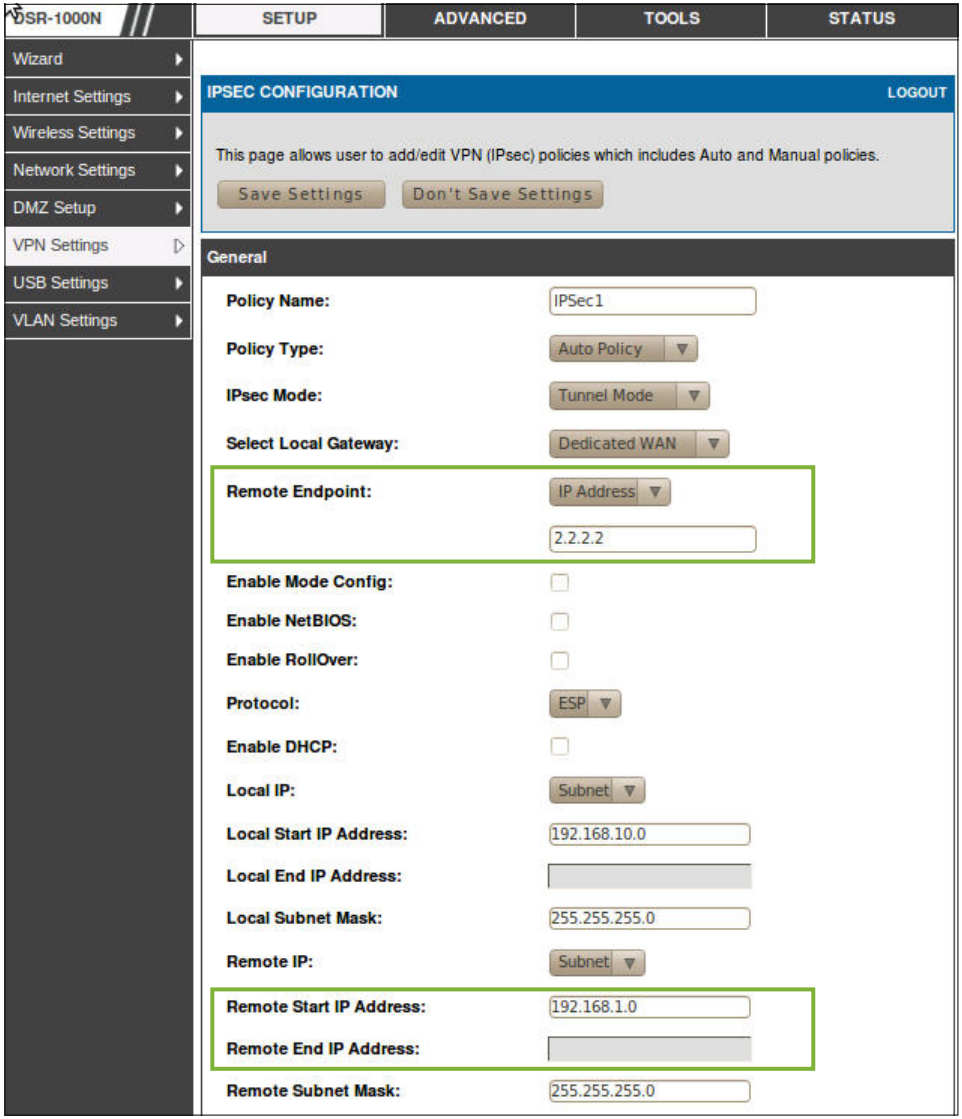
DSR Settings

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

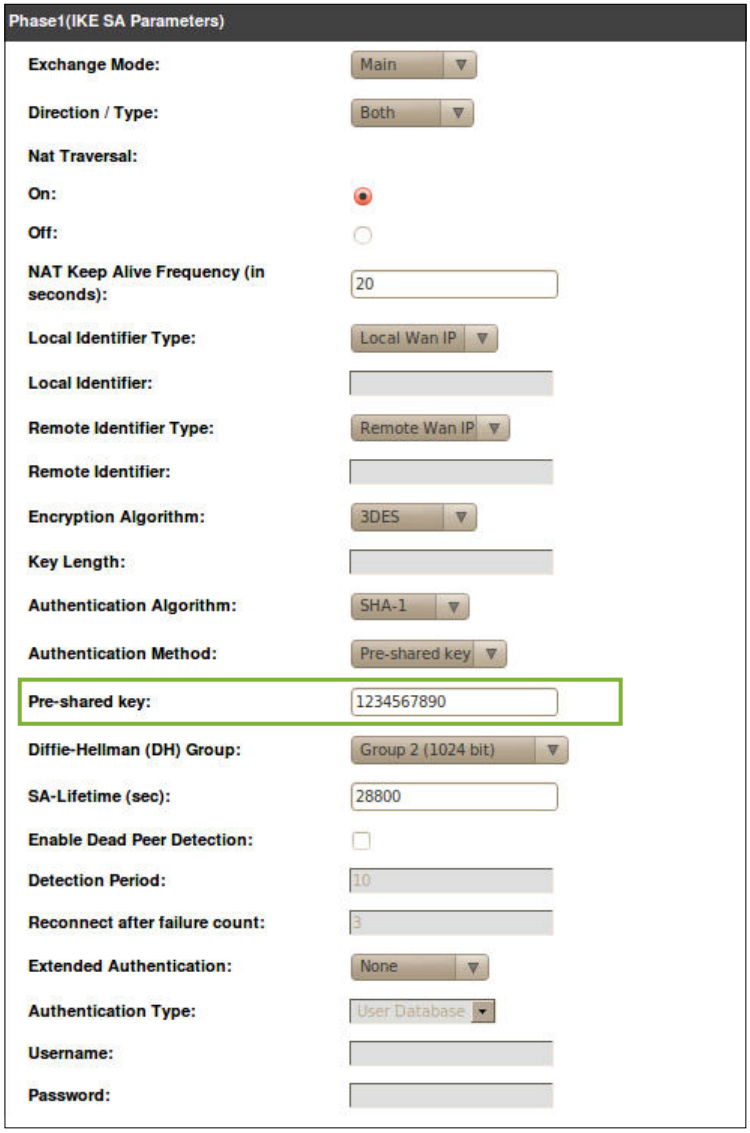


2. Set up the IPSec policy. Navigate to the VPN Settings > IPSec > IPSec Policies.

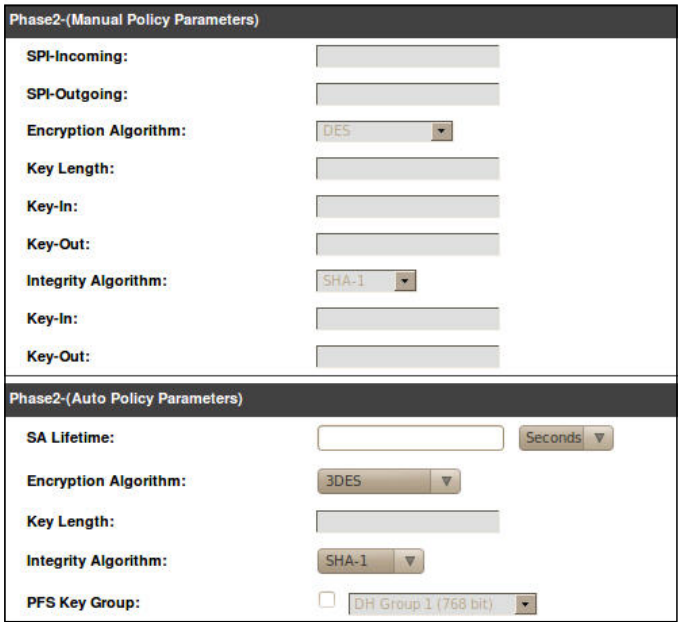
Press the button "**Add**" to increase a new policy. In General Section, fill in relative information. The IP address of Remote Endpoint refers to the external network connecting point of Juniper SSG20 which is shown as the point "**f**" on the topology. The internal network group, which indicates the IP information on Local Start IP Address, under DSR-1000N allows access to the remote network group, which indicates the IP information on Remote Start IP Address, under Juniper SSG20 through VPN tunnel.



In Phase 1 Section, fill in relative information. Please notice that the Pre-shared Key must be as same as the pre-shared key which will be inserted on Juniper SSG20 on the later step.



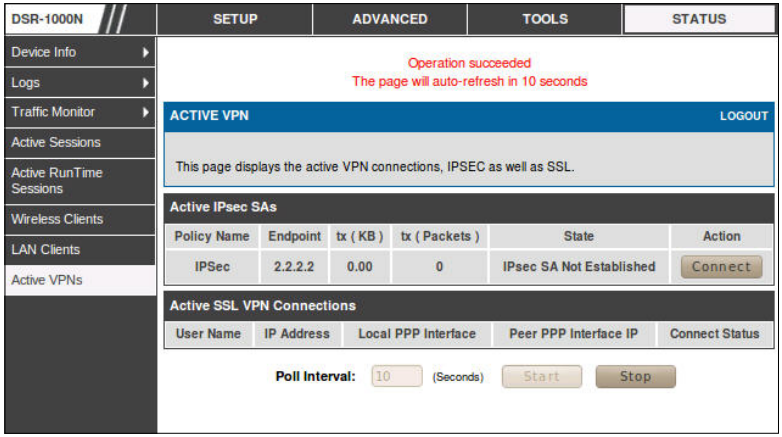
In Phase 2 Section, fill in relative information.



Click the button "**save settings**" to complete IPSec Policy settings.

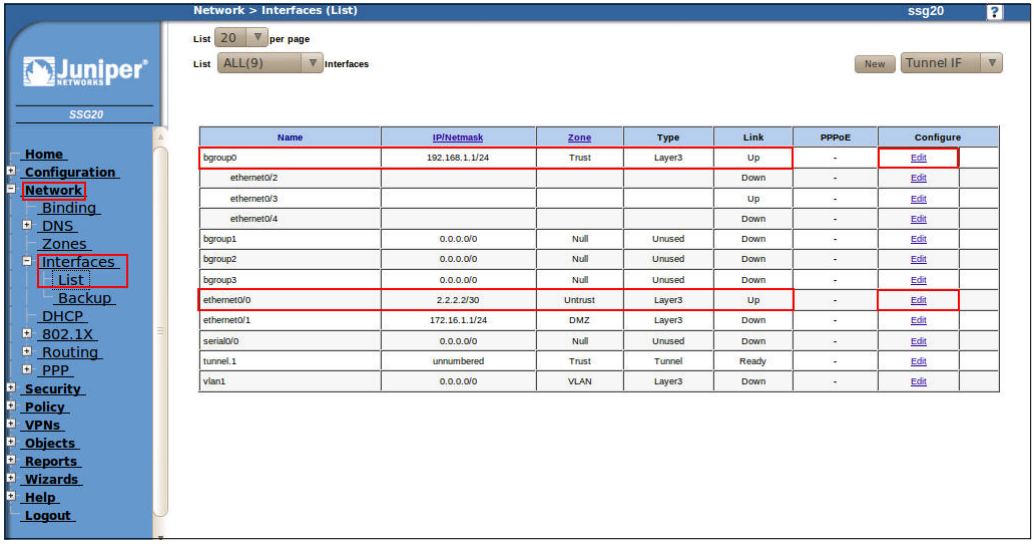
3. Check the VPN status. Navigate to the Status > Active VPNs.

The activity will be shown on the list while the tunnel is established with the other side.



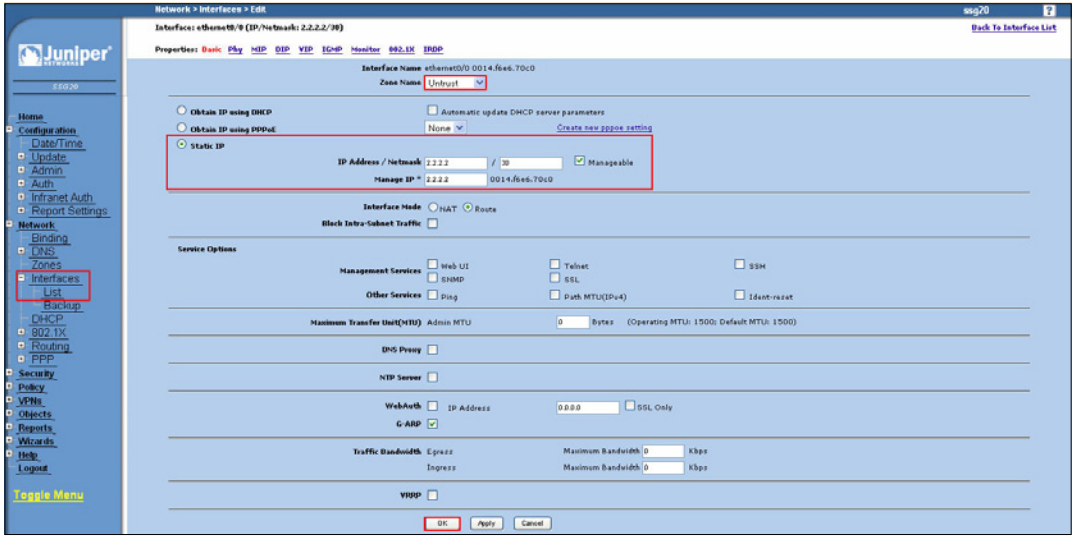
Juniper_SSG20 Settings

1. Set up the Untrust_Zone and Trust_Zone IP addresses. Navigate to the Network > Interfaces > List. Click "**Edit**".

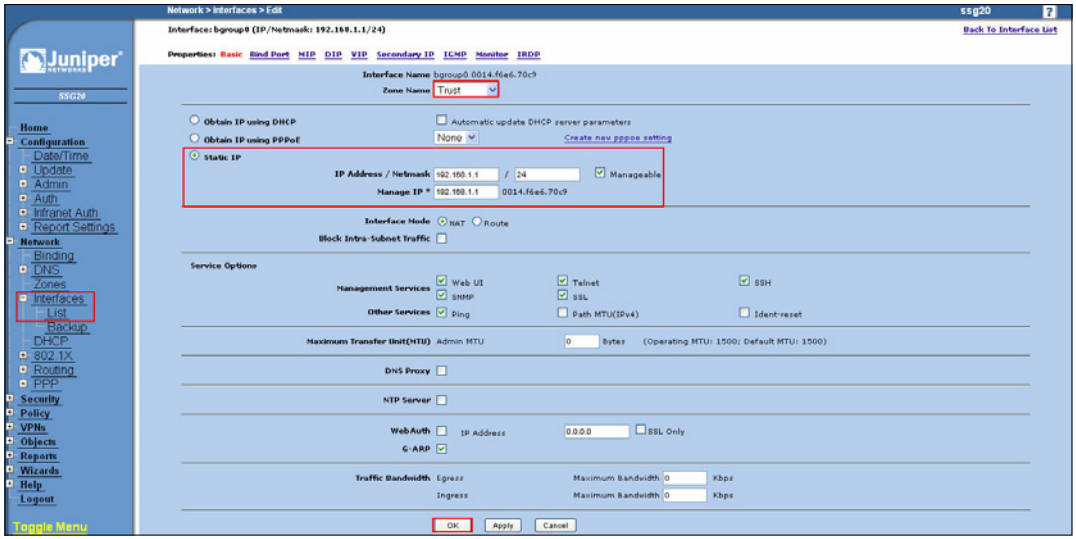


Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/2				Down	-	Edit
ethernet0/3				Up	-	Edit
ethernet0/4				Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	2.2.2.2/30	Untrust	Layer3	Up	-	Edit
ethernet0/1	172.16.1.1/24	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Trust	Tunnel	Ready	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Configure **Untrust_Zone** with relative information as below. The **IP Address/ Netmask** of Basic tab is the IP address of external network connecting point which is shown as the point "**f**" on the topology. Click the button "**OK**" to complete this setting.

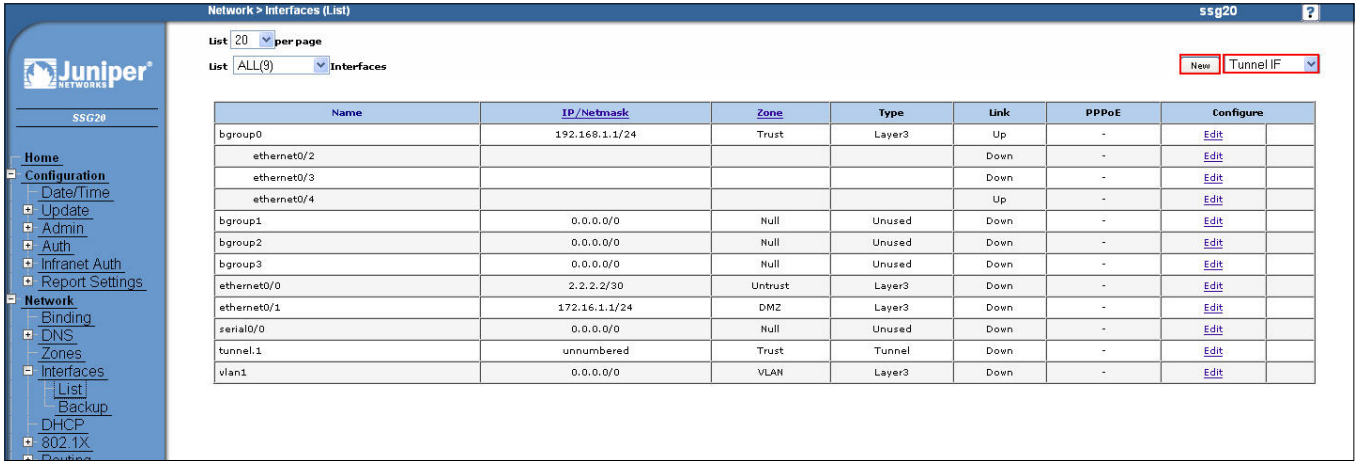


Configure **Trust_Zone** with relative information as below. The **IP Address/ Netmask** of Basic tab is the IP address of internal network connecting point which is shown as the point "**g**" on the topology. Click the button "**OK**" to complete this setting.

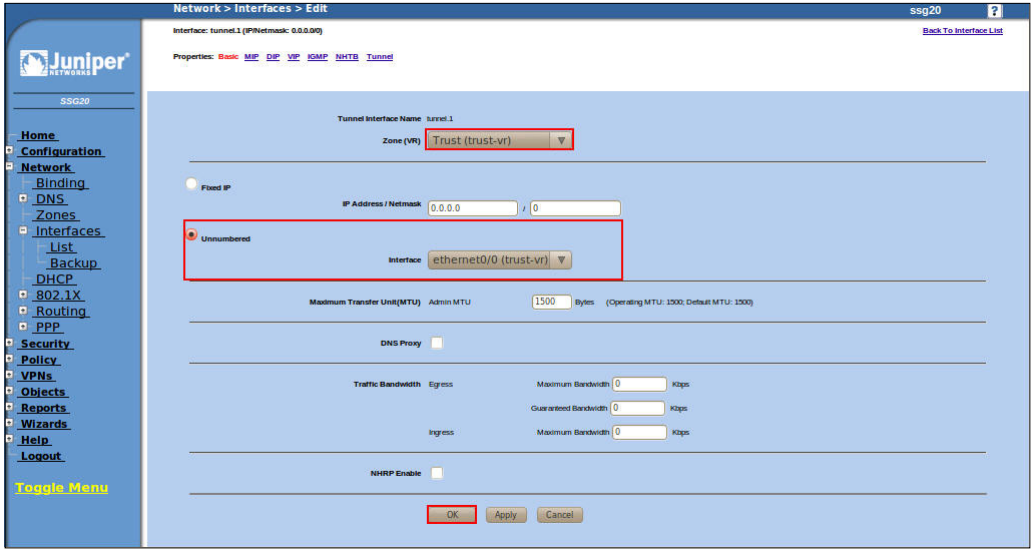


2. Add a Tunnel Interface. Navigate to the Network > Interfaces > List.

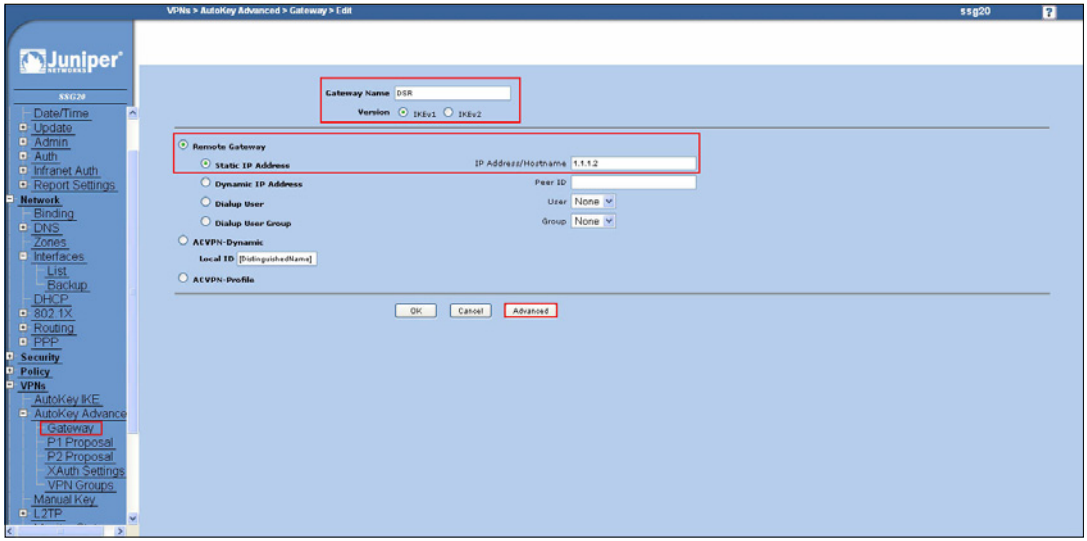
Select "**Tunnel IF**" from scroll down menu. Press the button "**New**" to increase a new tunnel interface.



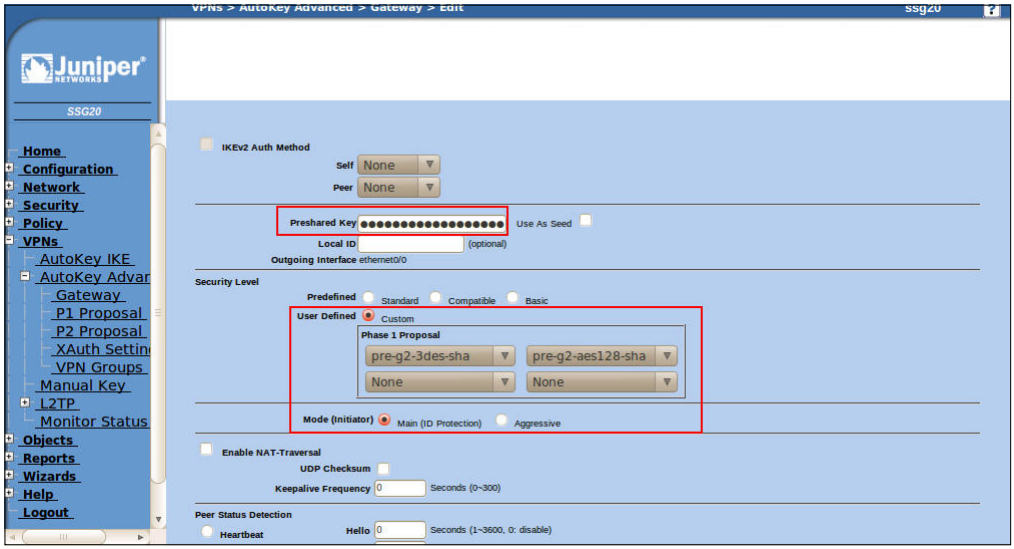
Configure relative settings as below.



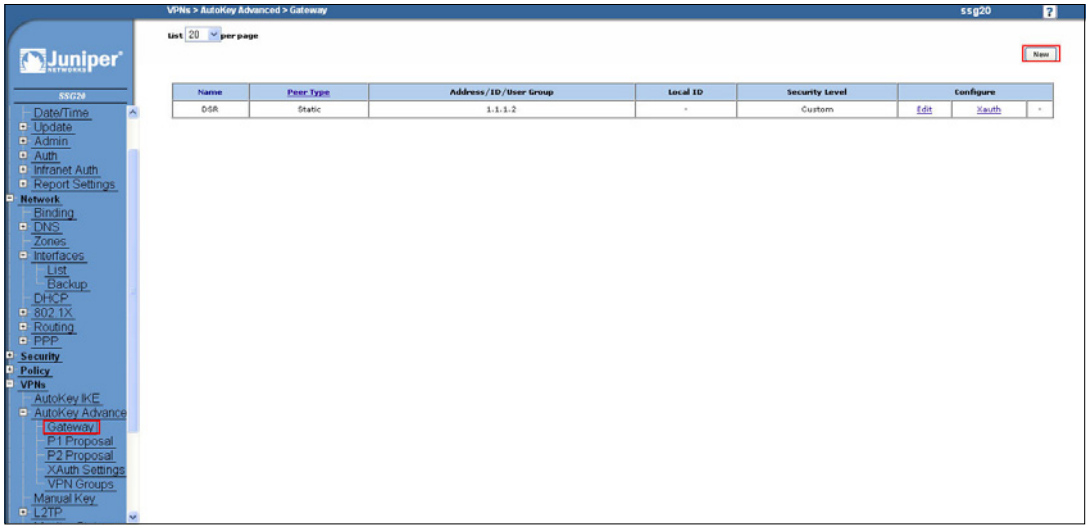
3. Add an IPSec Remote Gateway. Navigate to the VPNs > AutoKey Advanced > Gateway.
Press the button "**New**" and fill in relative information as below.



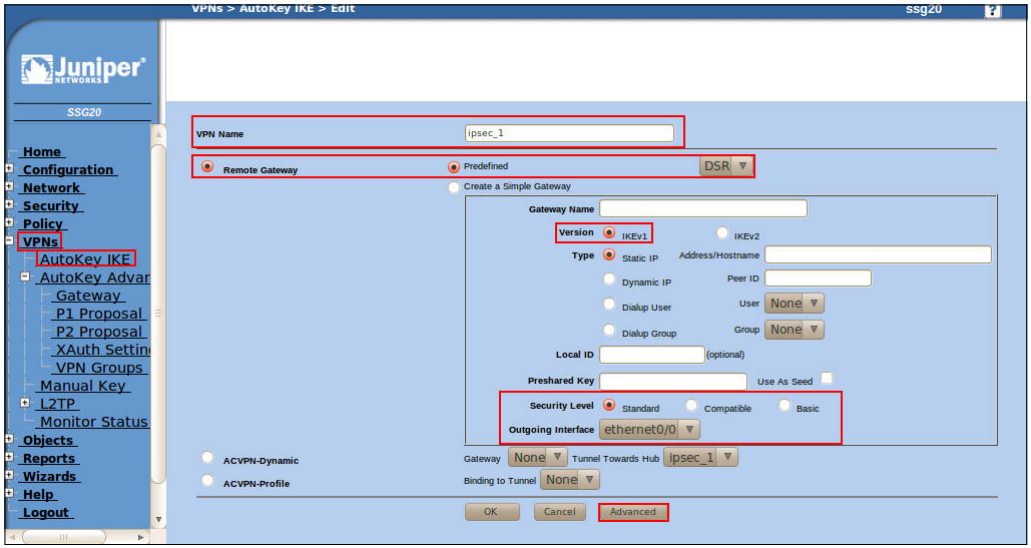
Press the button "**Advanced**" for preshared key setting. Fill in relative information as below. Insert the Pre-shared Key which is as same as the one put in DSR-1000N in the previous step.



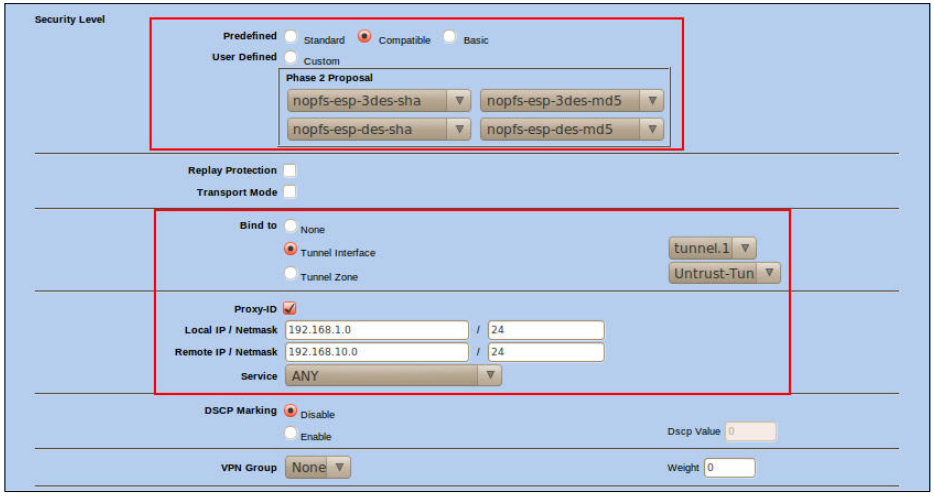
4. Create a new VPN tunnel. Navigate to VPNs > AutoKey IKE. Press the button "**New**".



Fill in relative information as below.

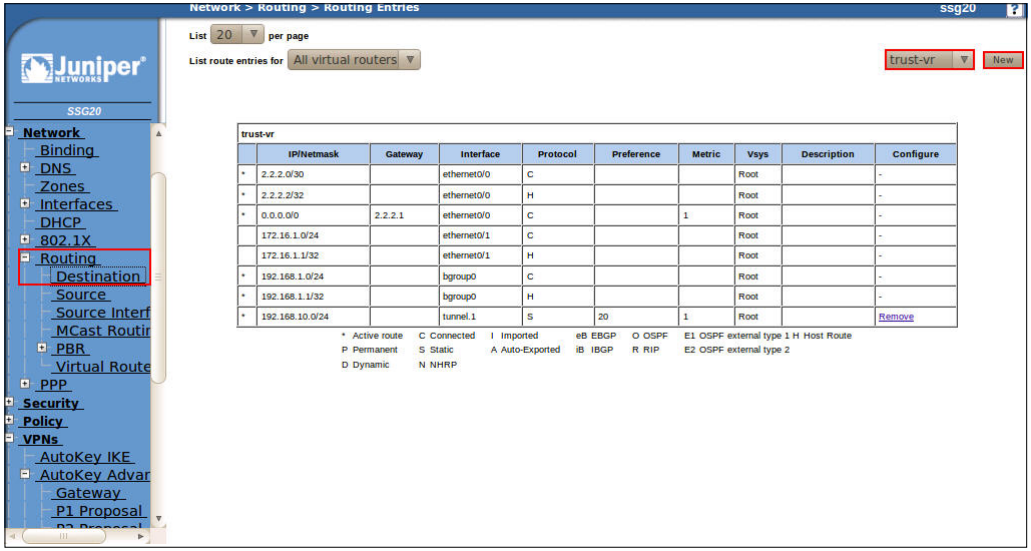


Press the button "**Advanced**" and configure settings as below. The internal network group, which is indicates the IP information on **Local IP/ Netmask**, under Juniper SSG20 allows access to the remote network group, which indicates the IP information on Remote **IP/ Netmask**, under DSR-1000N through VPN tunnel.

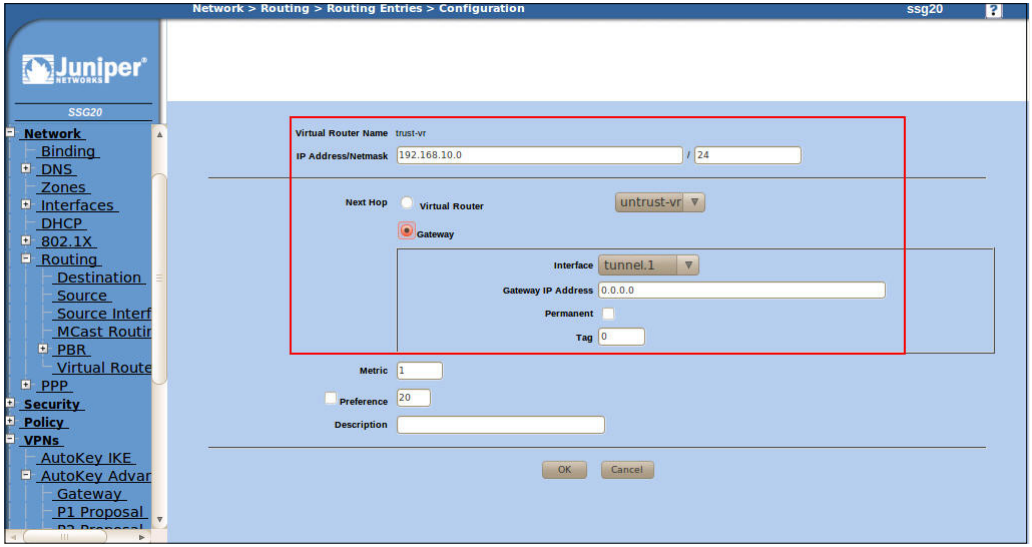


5. Create the Routings. Navigate to Network > Routing > Routing Entries.

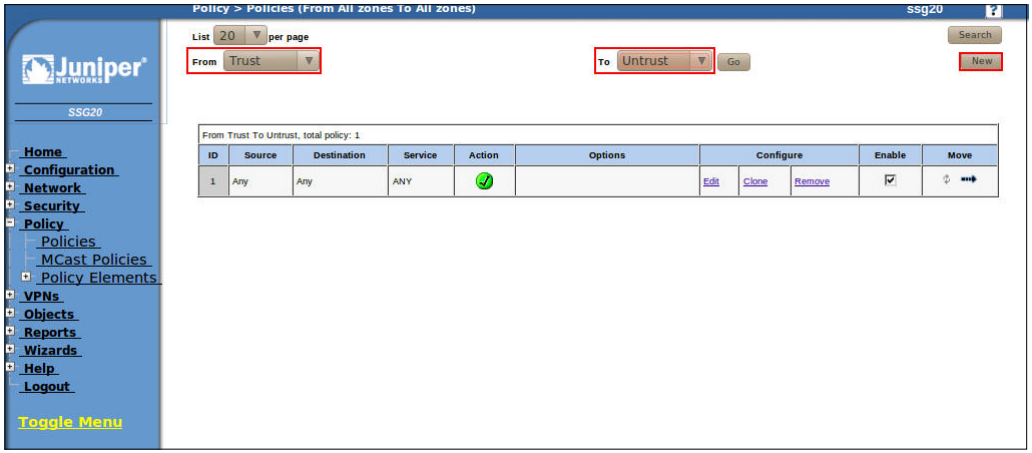
Select "**trust-vt**" from the drop down menu on the top and left corner. Press the button "**New**".



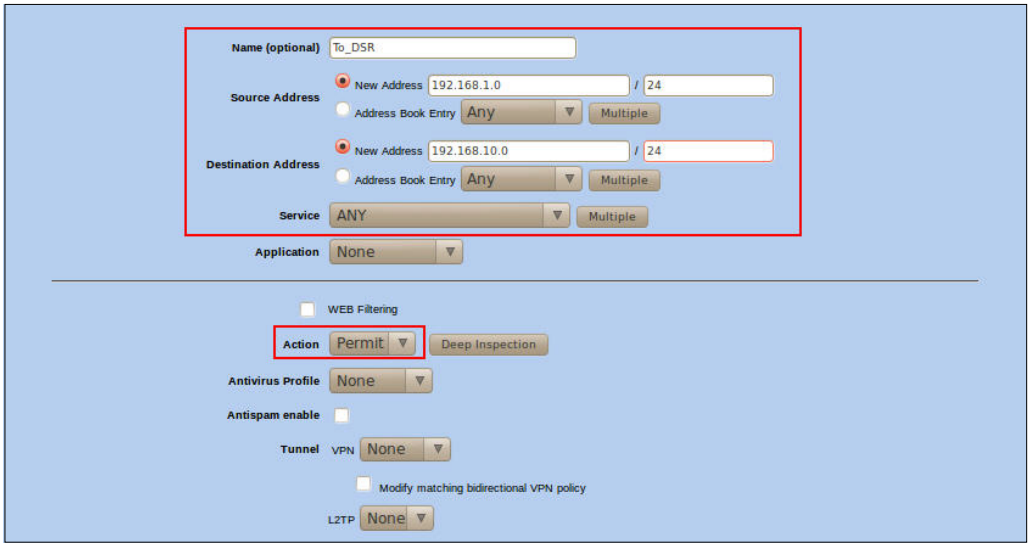
Fill in relative information as below.



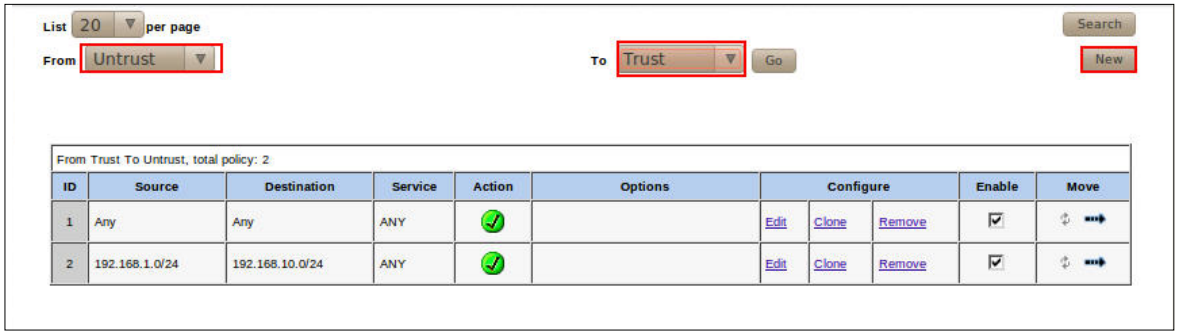
6. Set up the Policies. Navigate to Policy> Policies. Create the first rule. Select "**Trust" and "Untrust**" in the "From" and "To" drop down menus respectively. Press the button "**New**".



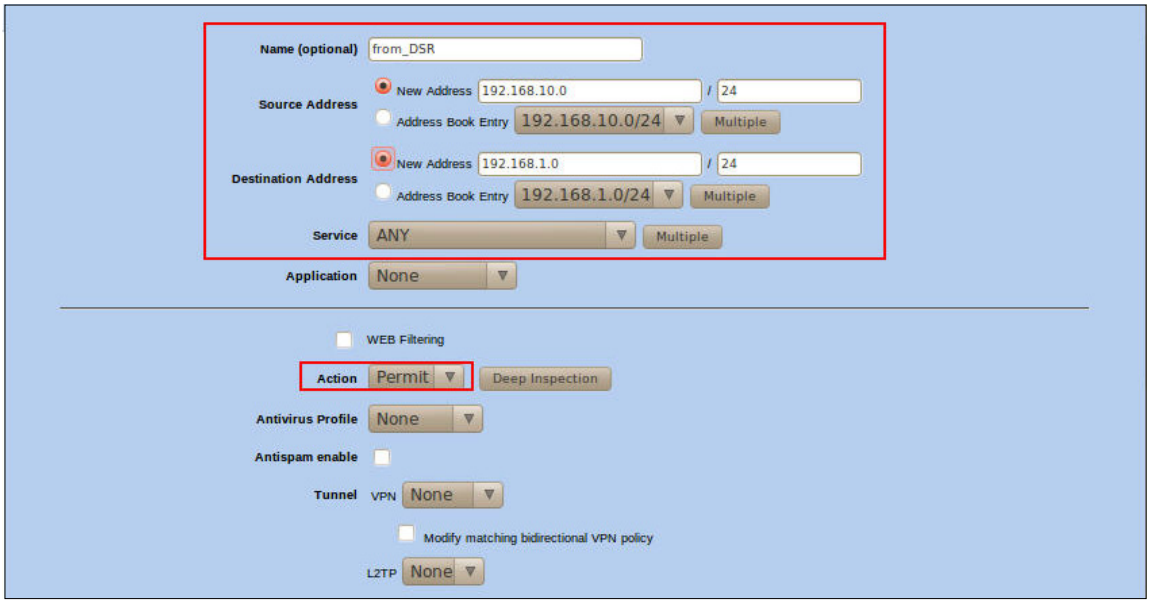
Fill in relative information as below.



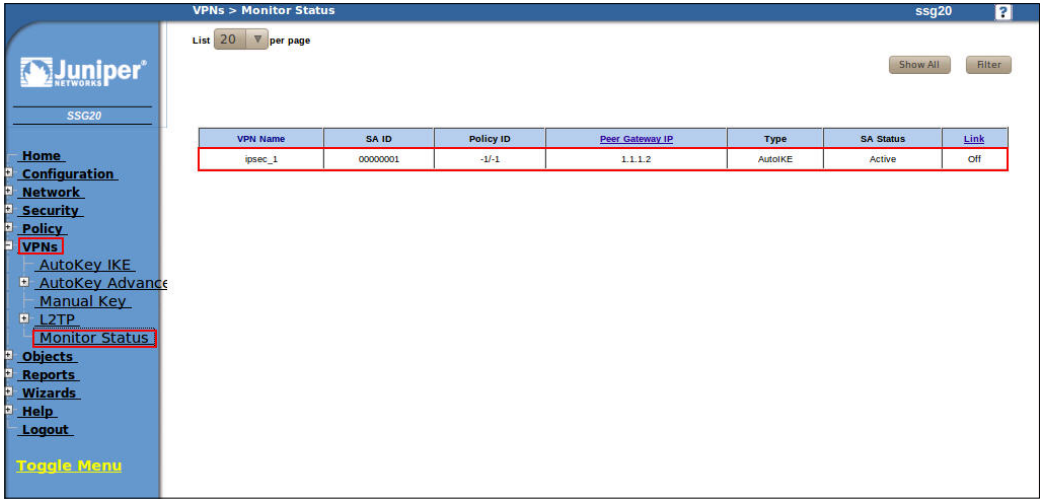
Create the second rule. Select "**Untrust" and "Trust**" in the "From" and "To" drop down menus respectively. Press the button "**New**".



Fill in relative information as below.



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



Visit our website for more information
www.dlink.com