Digi Connect® Family Application Guide

How to Create a VPN between Digi and Juniper Netscreen

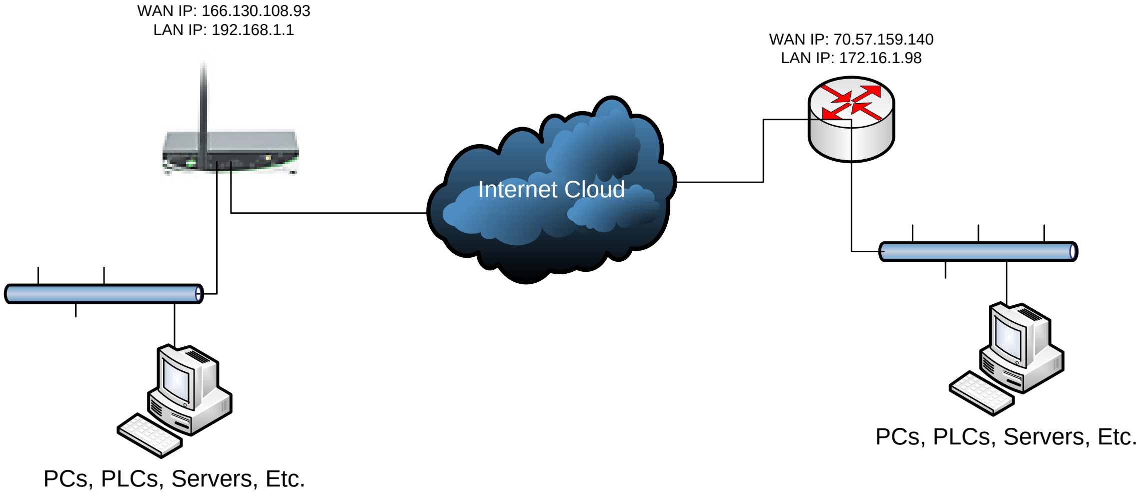
Scenario

Digi Connect family VPN router (for example ConnectPort WAN or Digi Connect WAN IA) is used for remote site connectivity. Juniper Netscreen is used at the local site for connectivity. The connection between the two networks needs to be secure for data transmission.

Theory of Operation

A location needs to be able to build a secure tunnel between the main site and a remote branch. One location has a Digi Connect router to provide primary internet connectivity. The other location uses a Juniper Netscreen for primary internet connectivity. The Digi Connect router will create a VPN tunnel to the Juniper Netscreen, creating a secure connection.

Sample Diagram



Carrier Plan and VPN Appliance Requirements

Digi Connect Router Requirements: Firmware version must be 2.8 or later. To download the latest firmware, go to http://www.digi.com/support.

GSM GPRS/EDGE APN Type needed: VPN and GRE end-points usually require static (persistent) IP addresses and must support mobile terminated data connections. If mobile termination is not an option with your current APN, you will need to acquire a new one that does support mobile termination.

CDMA networks may also require special plans to provide static IP addresses and support mobile terminated data connections.

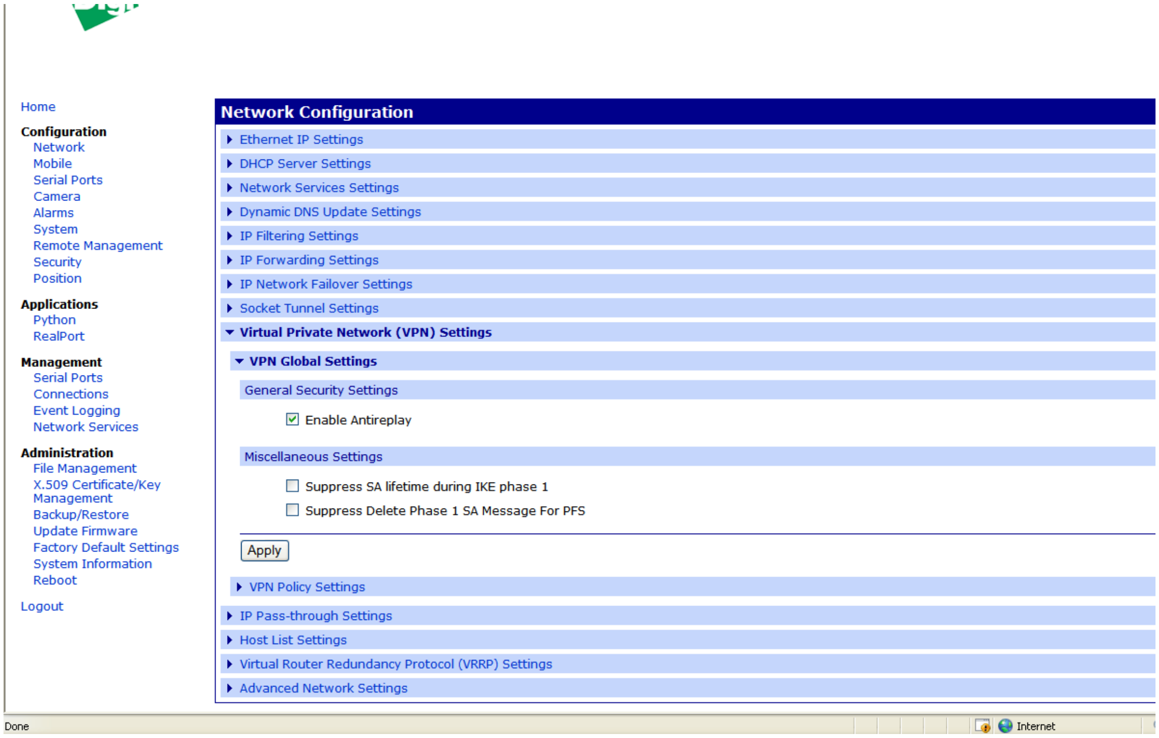
Check with your wireless provider on the available plan types.

Digi Connect Router Configuration

1. Read and follow the quick-start guide for the Digi Connect router and optionally for Digi Connectware® Manager if used.
2. Assign a static IP address to the Ethernet port (the default address is 192.168.1.1). Note the default gateway may show or change to an address such as 10.6.6.6. This is normal as it is the cellular provider's network default gateway.
3. Configure the Digi Connect router settings:

    a. VPN Global Settings

    i. Navigate to **Configuration > Network > VPN Settings** in the web interface of the unit.
    ii. Click on **VPN Global Settings**.
    iii. Click the check box for **Enable Antireplay**.
    iv. Click **Apply** to save the changes.



Home

Configuration
Network
Mobile
Serial Ports
Camera
Alarms
System
Remote Management
Security
Position

Applications
Python
RealPort

Management
Serial Ports
Connections
Event Logging
Network Services

Administration
File Management
X.509 Certificate/Key Management
Backup/Restore
Update Firmware
Factory Default Settings
System Information
Reboot

Logout

Network Configuration

- Ethernet IP Settings
- DHCP Server Settings
- Network Services Settings
- Dynamic DNS Update Settings
- IP Filtering Settings
- IP Forwarding Settings
- IP Network Failover Settings
- Socket Tunnel Settings
- Virtual Private Network (VPN) Settings
  - VPN Global Settings

    General Security Settings

    ☑ Enable Antireplay

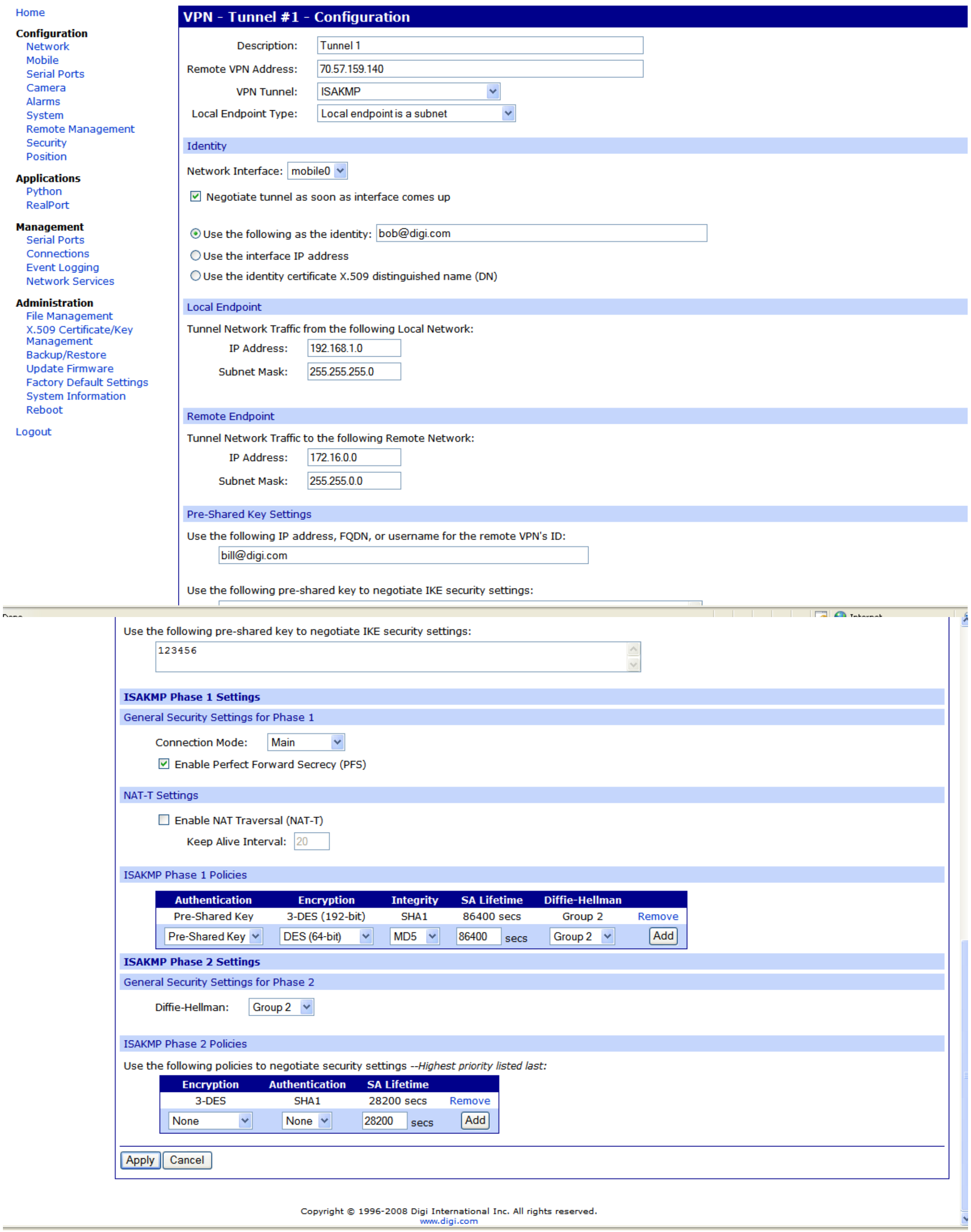
    Miscellaneous Settings

    ☐ Suppress SA lifetime during IKE phase 1
    ☐ Suppress Delete Phase 1 SA Message For PFS

    Apply
  - VPN Policy Settings
- IP Pass-through Settings
- Host List Settings
- Virtual Router Redundancy Protocol (VRRP) Settings
- Advanced Network Settings

    b. VPN Policy Settings

    i. Click on **VPN Policy Settings**.
    ii. Click on the **Add** button to setup the individual tunnel.
    iii. Fill in the appropriate information, shown in the following screenshots:



VPN - Tunnel #1 - Configuration

Description: Tunnel 1

Remote VPN Address: 70.57.159.140

VPN Tunnel: ISAKMP

Local Endpoint Type: Local endpoint is a subnet

Identity

Network Interface: mobile0

☑ Negotiate tunnel as soon as interface comes up

● Use the following as the identity: bob@digi.com

○ Use the interface IP address

○ Use the identity certificate X.509 distinguished name (DN)

Local Endpoint

Tunnel Network Traffic from the following Local Network:

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address: 172.16.0.0

Subnet Mask: 255.255.0.0

Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:

bill@digi.com

Use the following pre-shared key to negotiate IKE security settings:

Use the following pre-shared key to negotiate IKE security settings:

123456

ISAKMP Phase 1 Settings

General Security Settings for Phase 1

Connection Mode: Main

☑ Enable Perfect Forward Secrecy (PFS)

NAT-T Settings

☐ Enable NAT Traversal (NAT-T)

Keep Alive Interval: 20

ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	3-DES (192-bit)	SHA1	86400 secs	Group 2	Remove
Pre-Shared Key	DES (64-bit)	MD5	86400 secs	Group 2	Add

ISAKMP Phase 2 Settings

General Security Settings for Phase 2

Diffie-Hellman: Group 2

ISAKMP Phase 2 Policies

Use the following policies to negotiate security settings *--Highest priority listed last:*

Encryption	Authentication	SA Lifetime	
3-DES	SHA1	28200 secs	Remove
None	None	28200 secs	Add

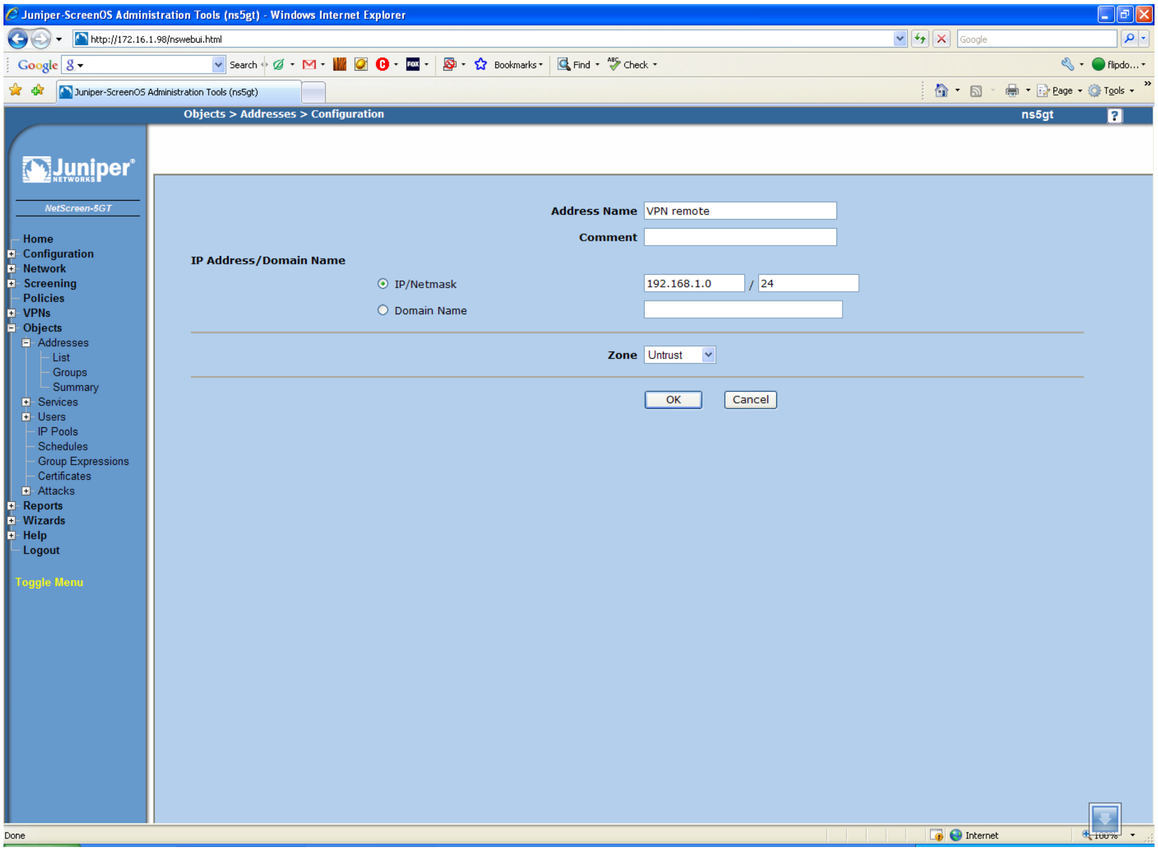
Apply Cancel

Copyright © 1996-2008 Digi International Inc. All rights reserved.
www.digi.com

iv. Click **Apply** after filling in the above information to complete the tunnel setup on the Digi Connect router.

Juniper Netscreen Configuration

1. Log into the Juniper Netscreen through its web interface.
2. Navigate to **Objects > Addresses > List** in the web interface. Select **Untrust** in the upper left hand corner, and click **New** in the upper right hand corner.
3. Fill in your Remote Site information, as shown in the screenshot below:



Address Name: VPN remote

Comment:

IP Address/Domain Name

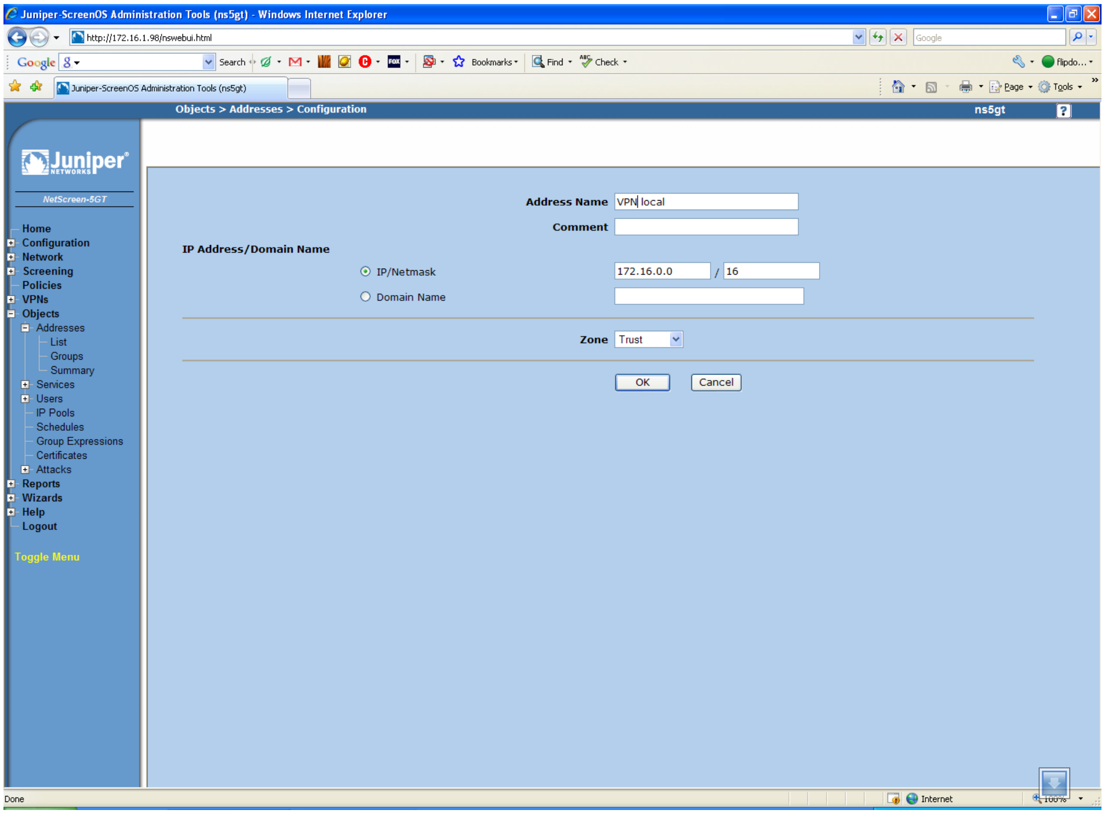
● IP/Netmask: 192.168.1.0 / 24

○ Domain Name:

Zone: Untrust

OK Cancel

4. Once this has been completed, click **Ok** to save the setting. You will then need to switch the **Untrust** option to **Trust** and perform the same settings for the Local Site information, as shown in the following screenshot:



Address Name: VPN local

Comment:

IP Address/Domain Name

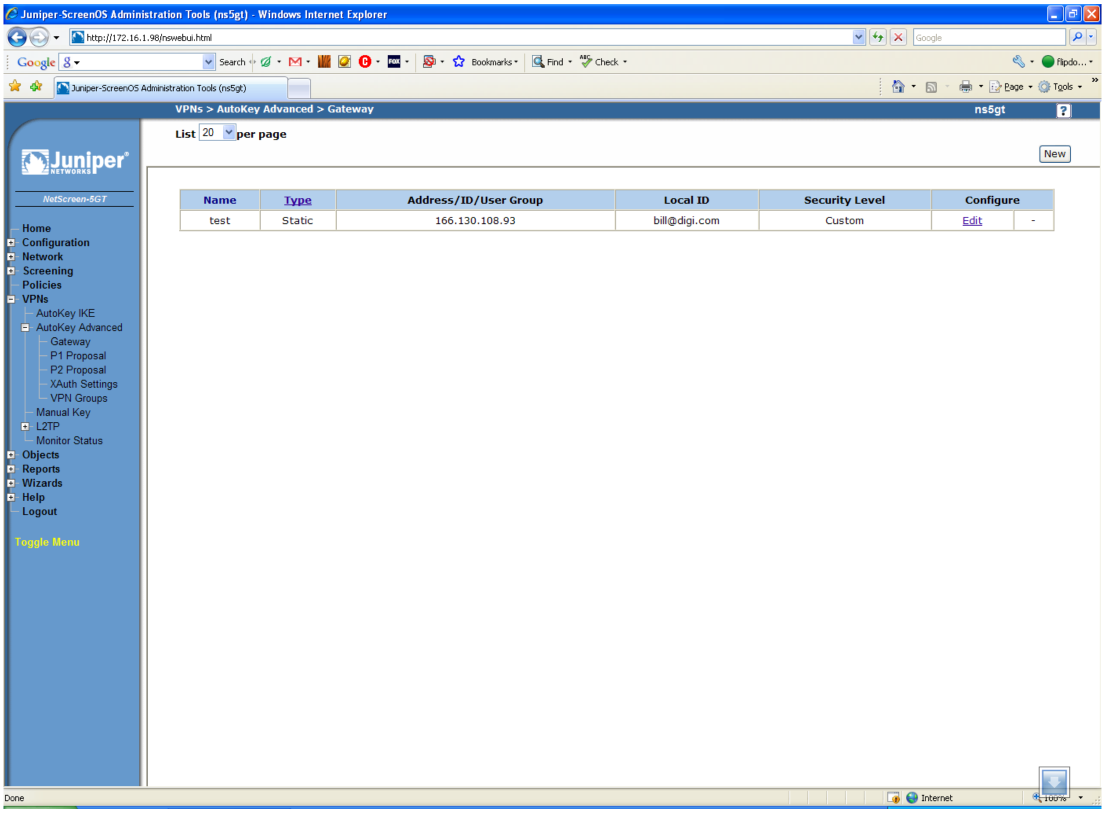
● IP/Netmask: 172.16.0.0 / 16

○ Domain Name:

Zone: Trust

OK Cancel

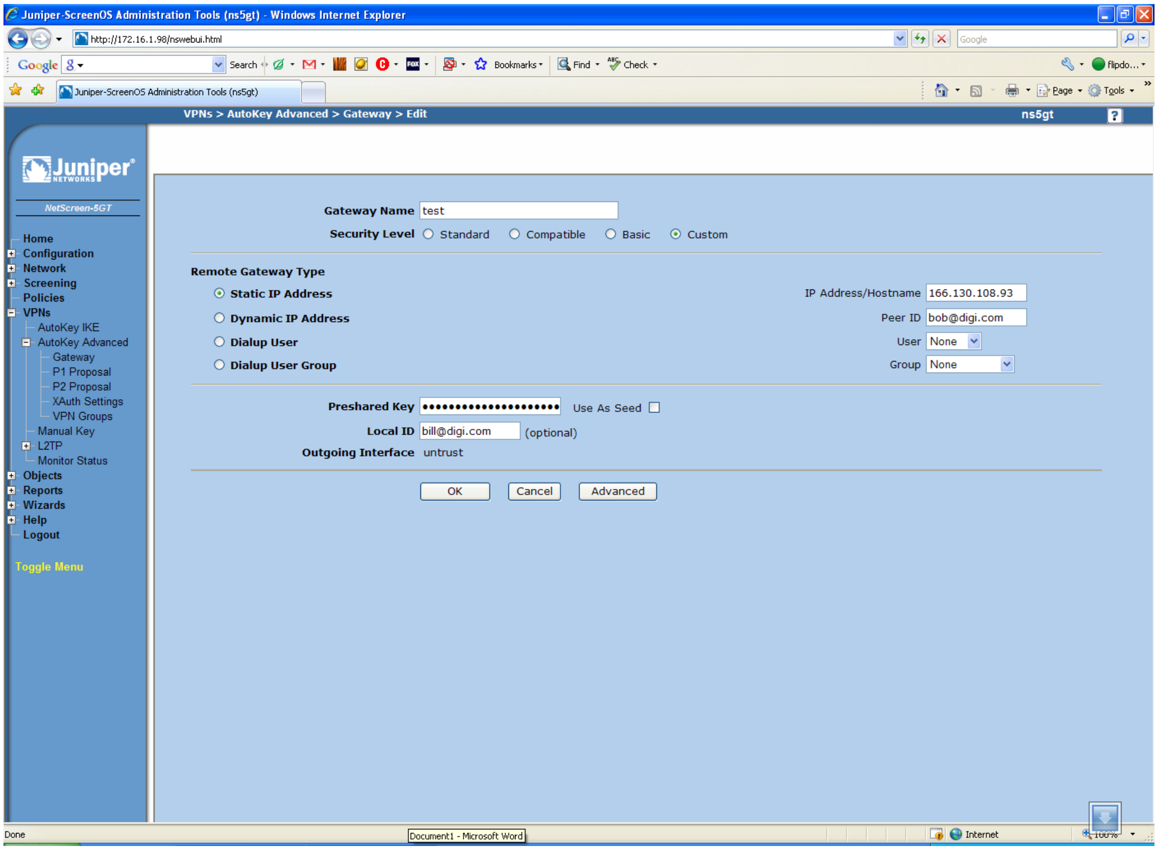
5. Navigate to **VPNs** > **AutoKey Advanced** > **Gateway:**



List 20 per page

Name	Type	Address/ID/User Group	Local ID	Security Level	Configure	
test	Static	166.130.108.93	bill@digi.com	Custom	Edit	-

6. Click **New** in the upper right hand corner and fill in the following information (shown in the following screenshot):
    a. Security Level – Custom
    b. Remote Gateway Type – Can be static or dynamic. This example will use static.
    c. IP Address/Hostname – The mobile IP or hostname of the Digi gateway.
    d. Peer ID – The ID that the Digi gateway is using.
    e. Preshared Key
    f. Local ID – The ID that the Juniper unit is using.



Juniper-ScreenOS Administration Tools (ns5gt) - Windows Internet Explorer

http://172.16.1.98/nswebui.html

VPNs > AutoKey Advanced > Gateway > Edit   ns5gt

Gateway Name: test

Security Level: ○ Standard ○ Compatible ○ Basic ● Custom

Remote Gateway Type

● Static IP Address   IP Address/Hostname: 166.130.108.93

○ Dynamic IP Address   Peer ID: bob@digi.com

○ Dialup User   User: None

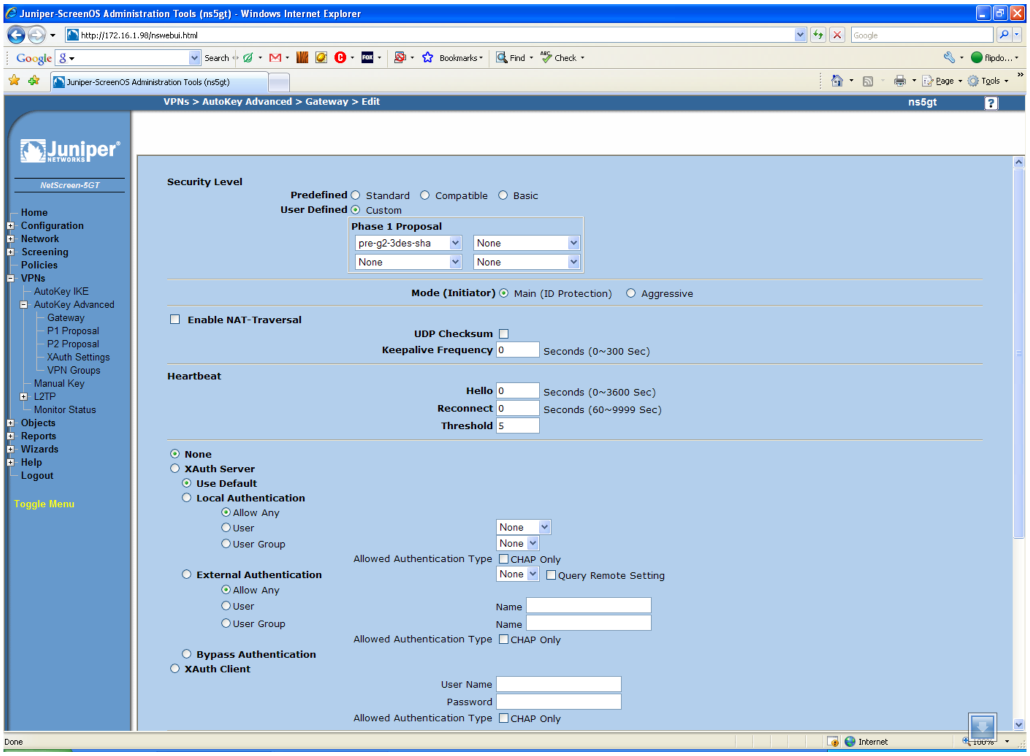
○ Dialup User Group   Group: None

Preshared Key: ••••••••••••••••••••   Use As Seed □

Local ID: bill@digi.com (optional)

Outgoing Interface: untrust

7. Click **Advanced** and fill in the following information (shown in the following screenshot):
    a. Phase 1 Proposal – pre-g2-3des-sha
    b. Mode (Initiator) - Main



Security Level

Predefined ○ Standard ○ Compatible ○ Basic

User Defined ● Custom

Phase 1 Proposal

pre-g2-3des-sha	None
None	None

Mode (Initiator) ● Main (ID Protection) ○ Aggressive

□ **Enable NAT-Traversal**

UDP Checksum □

Keepalive Frequency 0 Seconds (0~300 Sec)

Heartbeat

Hello 0 Seconds (0~3600 Sec)

Reconnect 0 Seconds (60~9999 Sec)

Threshold 5

● **None**

○ **XAuth Server**

● **Use Default**

○ **Local Authentication**

● Allow Any

○ User None

○ User Group None

Allowed Authentication Type □ CHAP Only

○ **External Authentication** None □ Query Remote Setting

● Allow Any

○ User Name

○ User Group Name

Allowed Authentication Type □ CHAP Only

○ **Bypass Authentication**

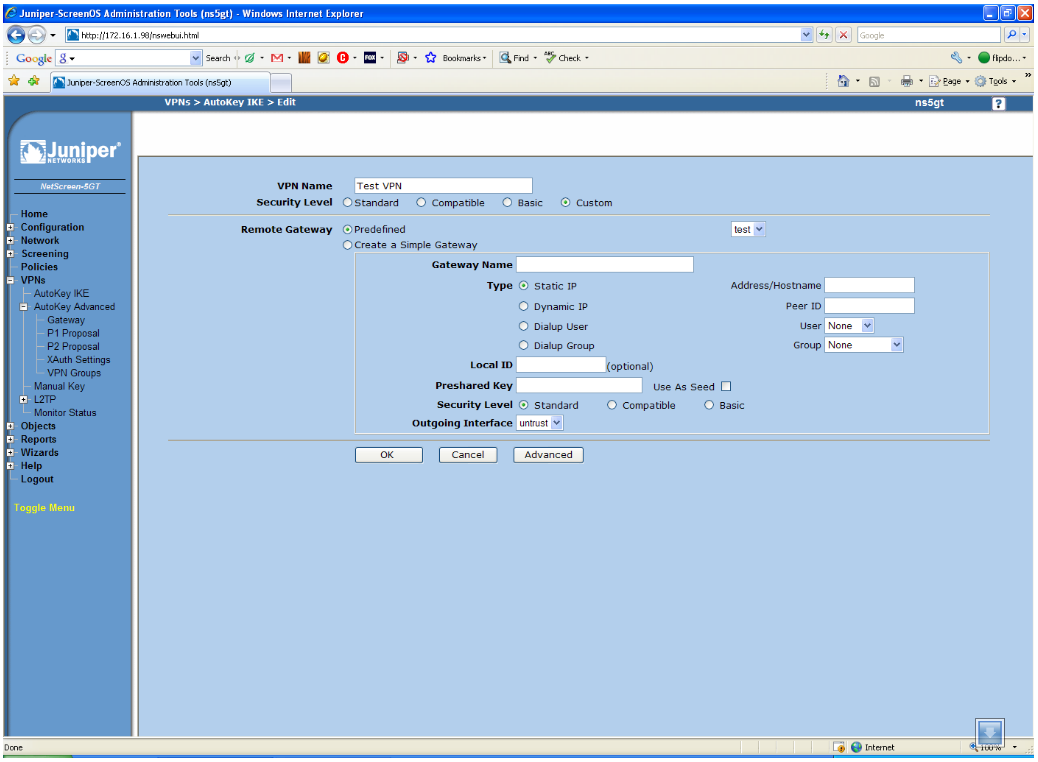
○ **XAuth Client**

User Name

Password

Allowed Authentication Type □ CHAP Only

8. Click **Return.**
9. Click **Ok**.
10. Navigate to **VPNs > AutoKey IKE** and click **New** in the upper right hand corner to get to the following screen:



VPN Name Test VPN

Security Level ○ Standard ○ Compatible ○ Basic ● Custom

Remote Gateway ● Predefined test

○ Create a Simple Gateway

Gateway Name

Type ● Static IP Address/Hostname

○ Dynamic IP Peer ID

○ Dialup User User None

○ Dialup Group Group None

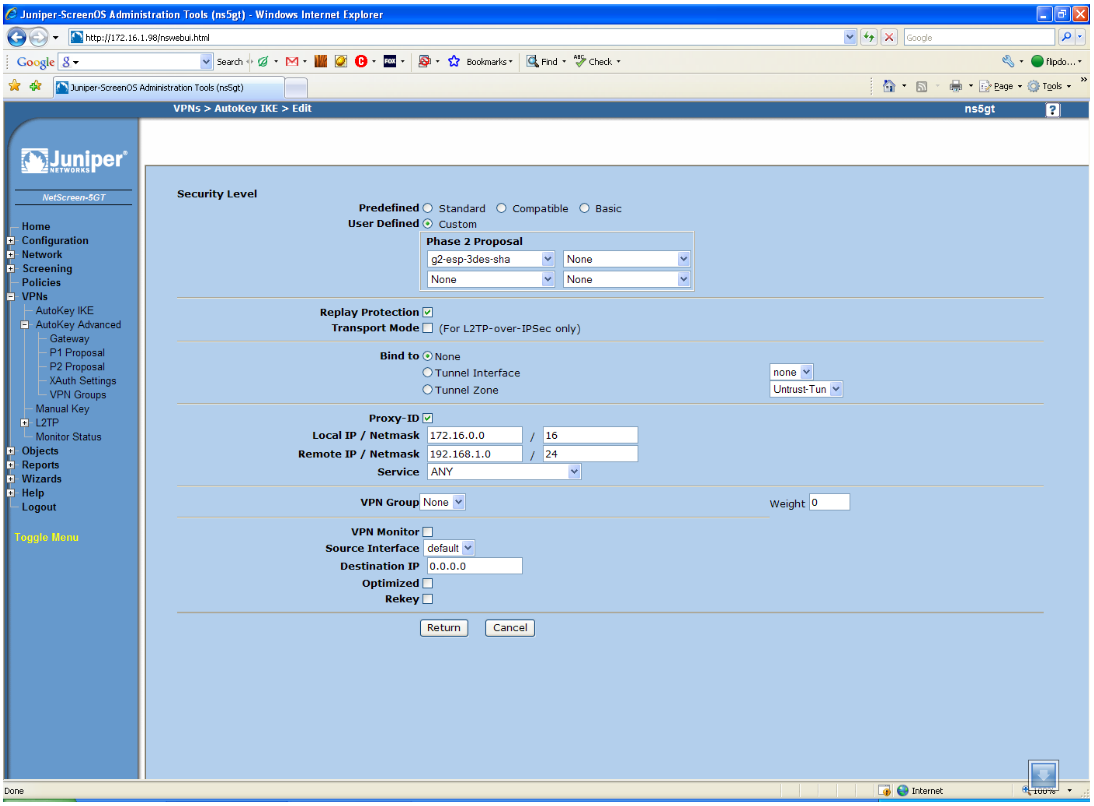
Local ID (optional)

Preshared Key Use As Seed □

Security Level ● Standard ○ Compatible ○ Basic

Outgoing Interface untrust

11. Choose the Security Level of **Custom**.
12. Under Remote Gateway, choose the option of Predefined, and select the gateway that was just setup. Click **Advanced** and fill in the following:
    a. Phase 2 Proposal – g2-esp-3des-sha
    b. Enable Replay Protection
    c. Enable Proxy-ID
        i. Local IP/Netmask – Local Subnet
        ii. Remote IP/Netmask – Remote Subnet



VPNs > AutoKey IKE > Edit   ns5gt

Security Level

Predefined	○ Standard ○ Compatible ○ Basic
User Defined	● Custom
Phase 2 Proposal	g2-esp-3des-sha, None None, None
Replay Protection	☑
Transport Mode	□ (For L2TP-over-IPSec only)
Bind to	● None ○ Tunnel Interface (none) ○ Tunnel Zone (Untrust-Tun)
Proxy-ID	☑
Local IP / Netmask	172.16.0.0 / 16
Remote IP / Netmask	192.168.1.0 / 24
Service	ANY
VPN Group	None
Weight	0
VPN Monitor	□
Source Interface	default
Destination IP	0.0.0.0
Optimized	□
Rekey	□

Return Cancel

13. Click **Return**.
14. Click **Ok**.
15. Navigate to **Policies.**
16. At the top of the page, under the **From** drop down box, select **Trust.** Under the **To** drop down box, select **Untrust**. Add the following:
    a. Source Address – Choose **Address Book Entry** and choose the local subnet that was previously setup from the drop down list.
    b. Destination Address – Choose **Address Book Entry** and choose the remote subnet that was previously setup from the drop down list.
    c. Action – Tunnel
    d. Tunnel – Choose your VPN from the list
    e. Check the box for “Modify matching bidirectional VPN policy” to automatically setup the permissions for the opposite direction.
17. Click **Ok**.

18. Move the newly created policy under the “From Trust To Untrust” section above the policy that permits any traffic. If the VPN policy is below the ‘any’ rule, it will not pass traffic through the tunnel in that direction. You may need to move the same rule under the “From Untrust To Trust” section, also.

ADDITIONAL NOTES

1. This configuration will work with Dynamic IP addresses, using hostnames established with DynDNS.org, or using the DDNS update feature of Digi Connectware® Manager. When using a Dynamic IP address, you will need to set the VPN tunnel to use **Aggressive Mode** to make the connection work.
2. This configuration will work with other VPN parameters than what is listed in the screenshots. i.e. – DES, 3DES, AES 192-bit, AES 256-bit, etc.
3. This configuration will work with other Digi Cellular products, such as the Connect WAN, Connect WAN 3G, and ConnectPort WAN VPN series of products that support VPN connections.
4. The Juniper screenshots may not reflect your specific model of Juniper VPN appliance. You may need to adjust your settings to reflect newer Juniper firmware.

Where to Get More Information

Refer to the Digi Connect router user documentation and Digi technical support website at www.digi.com/support for more information. Technical assistance is available at http://www.digi.com/support/eservice/eservicelogin.jsp.

For sales and product information, please contact Digi International at 952-912-3444 or refer to the Digi Connect wireless pages at www.digi.com.