



RSA Secured Implementation Guide VPN Products

Last Modified: March 7, 2005

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	Juniper Networks NetScreen Firewall/VPN
Version & Platform	5.x
Product Description	<p>Juniper Networks provides innovative, scalable network security solutions that allow enterprises and carriers to cost-effectively secure their networks without sacrificing performance. Providing multiple layers of defense, Juniper Networks' family of innovated security products is able to offer customers security throughout the network, ensuring that critical assets are protected by best of breed firewall, VPN and intrusion prevention solutions. The breadth of the product lines enables customers of any size to choose the solutions that best meet their needs.</p> <p>Integrated Firewall and VPN systems and appliances give customers the tools they need to protect their core network infrastructures and remote locations. By integrating robust network access control, attack containment features and secure connectivity between locations on high-performance, purpose-built appliances, Juniper Networks provides customers multiple layers of defense to keep their assets safe.</p>
Product Category	Perimeter Defense (Firewalls, VPN & Intrusion Detection)



Product Requirements

Partner Product Requirements: Juniper Networks NetScreen Firewall/VPN	
Hardware Version	NS-5XT, NS-5XP, NS-25, NS-50, NS-204 NS-208, and NS-500
Firmware Version	Screen OS 5.0 or above

Additional Software Requirements	
Application	Additional Patches
Juniper Networks NetScreen Remote	8.1 and above
Internet Browser	Netscape Communicator 4.7 and above
	Internet Explorer 5.x and above

Product Configuration

This section provides instructions for integrating the partners' product with RSA Keon. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

Overview

Juniper Networks NetScreen Firewall/VPN supports the following PKI functionality.

- Generates a public/private key pair when you create a CSR (certificate request).
- Supplies the public key as part of the certificate request in the form of a text file for transmission to a Certificate Authority (CA) for certificate enrollment (PKCS10 file).
- Supports loading the local certificate, the CA certificate, and the certificate revocation list (CRL) into the unit. You can also specify an interval for refreshing the CRL online.
- Provides certificate delivery when establishing an IPSec tunnel.
- Supports certificate path validation upward through eight levels of CA authorities in the PKI hierarchy.
- Supports the PKCS #7 cryptographic standard, which means the Juniper Networks device can accept X.509 certificates and CRL's packaged within a PKCS #7 envelope. PKCS #7 support allows you to submit multiple X.509 certificates within a single PKI request.
- You can now configure PKI to validate all the submitted certificates from the issuing CA at one time.
- Supports online CRL retrieval via LDAP or HTTP.

Integration Summary

1. PKI specific configuration.
2. VPN gateway to VPN Client specific configuration.
3. VPN gateway to VPN gateway specific configuration.
4. VPN client specific configuration.

PKI specific configuration

To use digital certificates to authenticate identity when establishing a secure VPN connection, you must first obtain and install the following:

- **Server certificate:** Also known as a local certificate, this is to be used to establish a trusted identity for the VPN gateway. This will be installed on the Juniper Networks device.
- **Trusted Root certificate:** Also known as the CA certificate, it's the certificate for the CA that issued the above certificates. This will be installed on both the Juniper Networks Remote system and the Juniper Networks device.
- **Personal certificate:** Also known as a user certificate, this is to be used to establish a trusted identity for the VPN user. This will be installed on the Juniper Networks Remote system.
- **Certificate Revocation List:** Juniper Networks and RSA Keon CA support the use of certificate distribution point (CDP) extensions and automatically retrieve the CRL via LDAP or HTTP. You can also retrieve a CRL manually and load that into the Juniper Networks device.

There are two methods of certificate enrollment for the VPN server, manual PKCS#10 enrollment and device automated SCEP enrollment. An administrator can choose their preferred enrollment method based on network connectivity to the RSA Keon CA, security concerns or convenience. Both types of enrollment are listed within this document.

Requesting a Certificate Manually

1. Requesting a Certificate Manually (Juniper Networks NetScreen Firewall/VPN)

To obtain a signed digital certificate using the manual method, you must complete several tasks in the following order:

- a) Configure default server settings.
 - b) Generate a public/private key pair.
 - c) Fill out the Certificate Request.
 - d) After you receive your signed certificate, you must load it into the Juniper Networks device along with the RSA Keon CA certificate.
2. When you request a certificate, the Juniper Networks device generates a key pair. The public key becomes incorporated in the request itself and, eventually, in the digitally signed local certificate you receive from the CA.

Note: Before generating a certificate request, make sure that you have set the system clock and assigned a host name and domain name to the Juniper Networks device.

3. Objects > Certificates > New: Enter the appropriate information, and then click **Generate**:

The screenshot shows the 'Cert New Request' page in the NetScreen NIS 100 web interface. The left sidebar contains a navigation menu with options like Home, Configuration, Network, Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main content area is titled 'Certificate Subject Information' and contains the following fields:

- Name: ns100a
- Phone: (empty)
- Unit/Department: PE
- Organization: RSA
- County/Locality: (empty)
- State: (empty)
- Country: US
- E-mail: (empty)
- IP Address: 10.100.51.21
- FQDN: ph021.securitydynamic

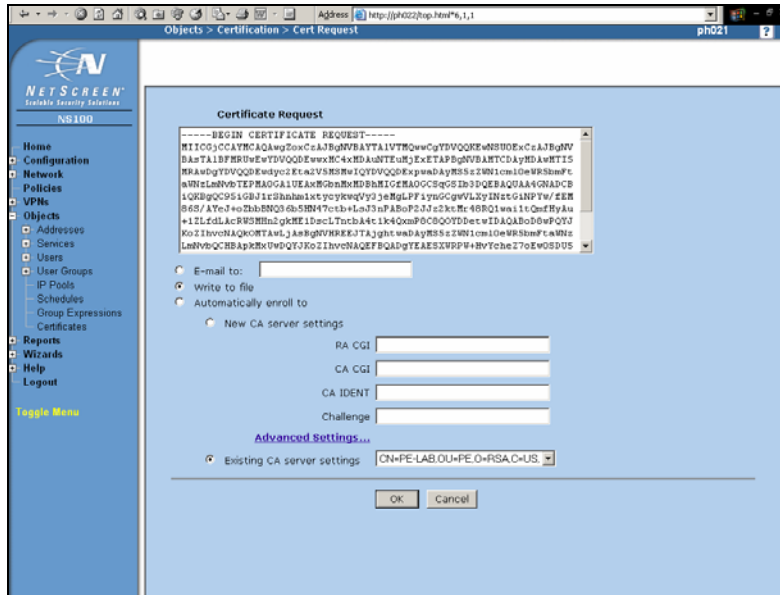
Below these fields is the 'Key Pair Information' section, which includes radio buttons for 'RSA' (selected) and 'DSA', and a dropdown menu for 'Create new key pair of' set to '1024' length. At the bottom of the form are 'Generate' and 'Cancel' buttons.

Note: If you do not include an e-mail address in the local certificate request, you cannot use an e-mail address as the local IKE ID when configuring the Juniper Networks device as a dynamic peer. Instead, you can use a fully qualified domain name (if it is in the local certificate), or you can leave the local ID field empty.

By default the Juniper Networks device sends its hostname.domainname. If you do not specify a local ID for a dynamic peer, enter the hostname.domainname of that peer on the device at the other end of the IPSec tunnel in the peer ID field.

4. The Juniper Networks device generates the PKCS #10 file and prompts you to open the file or save it to disk.
5. Open the file, and copy its contents, taking care to copy the entire text but not any blank spaces before or after the text.

Note: The certificate request must include the “-----BEGIN CERTIFICATE REQUEST-----”, and “-----END CERTIFICATE REQUEST-----” information.



6. Follow the directions in the enrollment page of your RSA Keon CA's Web site to submit the PKCS#10 request.
7. The RSA Keon CA administrator now needs to approve the certificate. When you receive the certificate copy it to a text file, and save it to your workstation. You will now need to load the certificate into the Juniper Networks device.
 - Objects > Certificates: Select Load <Cert or CRL>, and then click Browse.
 - Navigate to the directory where you stored the certificates, click Open, and then Load.
 - Perform the same steps for all your certificates (Local, CA, CRL)



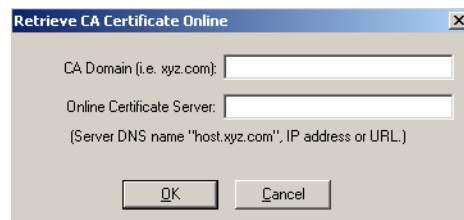
VPN Client Enrollment

There are two methods of enrollment available to the users, manual certificate enrollment, and SCEP enrollment. Each enrollment method will be described below to show configuration of both.

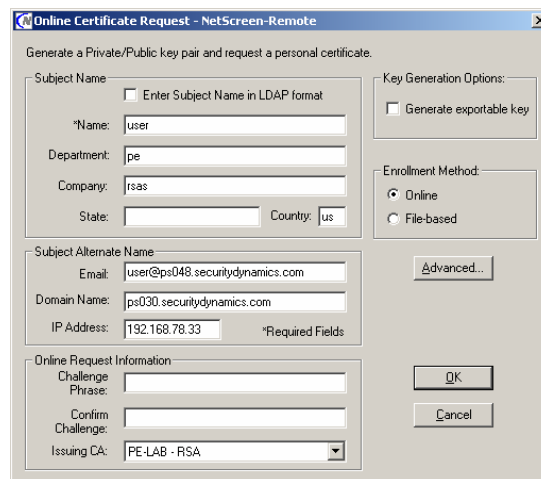
There is a known issue where SCEP enrolment will fail when using the Juniper / NetScreen Remote VPN Client version 10.1.1. For additional information please refer to the Known Issues section at the end of this document.

VPN Client SCEP Enrollment

1. Start the Certificate Manager Module by clicking Start > Programs > NetScreen-Remote > Certificate Manager.
2. Click the Root CA Certificates tab, and then click Retrieve CA Certificate to open this dialog box.



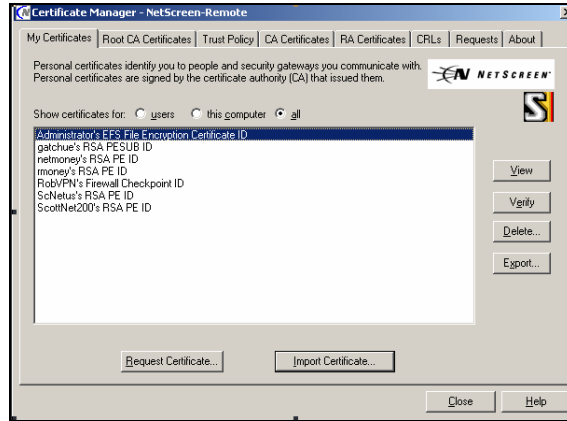
3. In the CA Domain text box, enter the CA's Nickname, e.g. PE-LAB.
4. In the Online Certificate Server field, enter the SCEP Server's URI in this format: http://<hostname>:<port>/<jurisdiction_id>/pkiclient.exe
5. When you are prompted "Are you sure you want to add this Root CA?" click Yes.
6. The CA certificate is imported into the Juniper Networks NetScreen-Remote Certificate Manager Module, and is displayed in the Root CA certificates list box if it is a self signed CA.
7. In the Certificate manager Module, click the My Certificates tab, and then click the Request Certificate tab.
8. Provide appropriate values for the fields in the Online Certificate Request dialog.



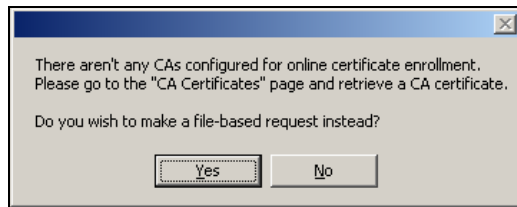
9. The Challenge Phrase is a required value that must be provided.
10. From the Issuing CA drop-down list, select the SCEP-enabled CA
11. From the Enrollment Method list, select Online.
12. Click OK. The certificate request is sent to the CA for approval.
13. Once the certificate is approved go to the request tab and select retrieve. The client certificate is then uploaded to the Juniper Networks NetScreen-Remote VPN client and will appear in the "My Certificates" list.

VPN Client Manual Enrollment

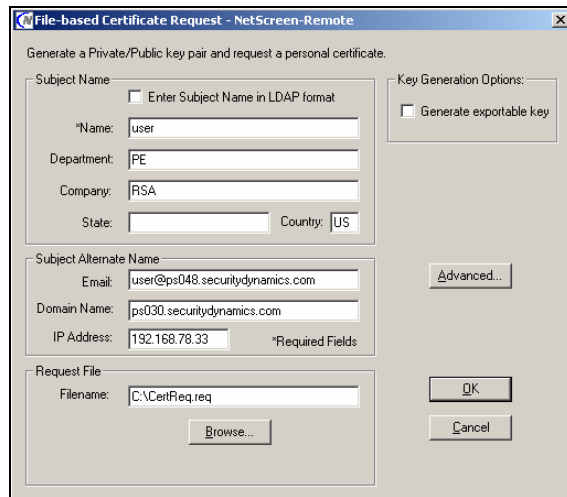
1. Start the Certificate Manager Module by clicking Start > Programs > NetScreen-Remote > Certificate Manager and select the My Certificates tab.



2. Click Request Certificate.

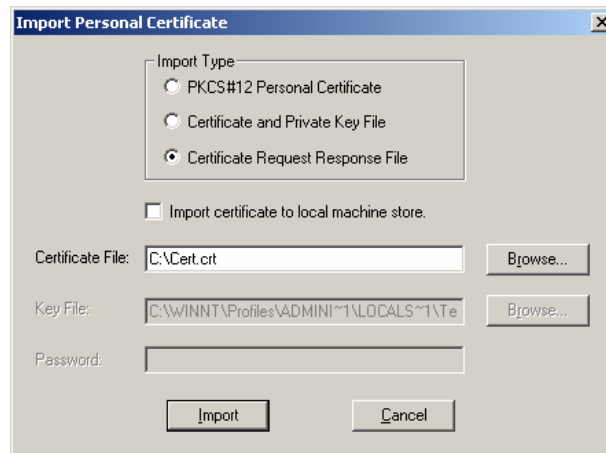


3. Click Yes to choose a file based request.
4. Provide appropriate values for the fields in the File-based Certificate Request dialog.



5. Click the Advanced button and select the Microsoft Enhanced Cryptographic Provider.
6. Click OK to generate your certificate request.
7. After your certificate has been approved save it to the client pc.

8. Get the root certificate and save that to the client pc.
9. Go to the Certificate Manager and select the My Certificates tab.
10. Click Import Certificate.



11. Select the radio button for "Certificate Request Response File" and brows to the root certificate and click Import.
12. Perform the same step as above but select the user certificate.

Configuring CRL Settings

In Phase 1 negotiations, participants check the CRL list to see if certificates received during an IKE exchange are still valid.

During configuration of the CA within the Juniper Networks device, you must enter the URI information for where the Certificate Revocation List will be published for an individual CA.

If you do not define a URI for a particular CA, the Juniper Networks device will failover to the default CRL URL address listed under Objects > Certificates > Default Cert Validation Settings.

1. Objects > Certificates (Show: CA), click on Server Settings for the certificate that was just imported. The example server certificate is PE.

Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure
PE Server Settings	23	CA	b212a1dff809d140b5b1983fe7abebbf	01-22-2006 15:36	Active	Detail, Remove

2. Enter your CRL location and the click OK.

CA Server Settings

X509 Certificate Path Validation Level

Full Partial

Certificate Revocation Settings

Check Method CRL Best Effort None

URL Address

LDAP Server

Refresh Frequency

- **X509 Cert_Path Validation Level:** Partial
- **Check Method:** CRL
- **URL Address:** <http://<hostname>:<port>/crlFileName.crl>
- **Refresh Frequency:** Daily

VPN gateway to VPN client specific configuration


To create a successful VPN tunnel, you must set up the devices on both ends of the tunnel with identical configurations.

There are five tasks involved in setting up the Juniper Networks device for an AutoKey IKE VPN tunnel using digital certificates:

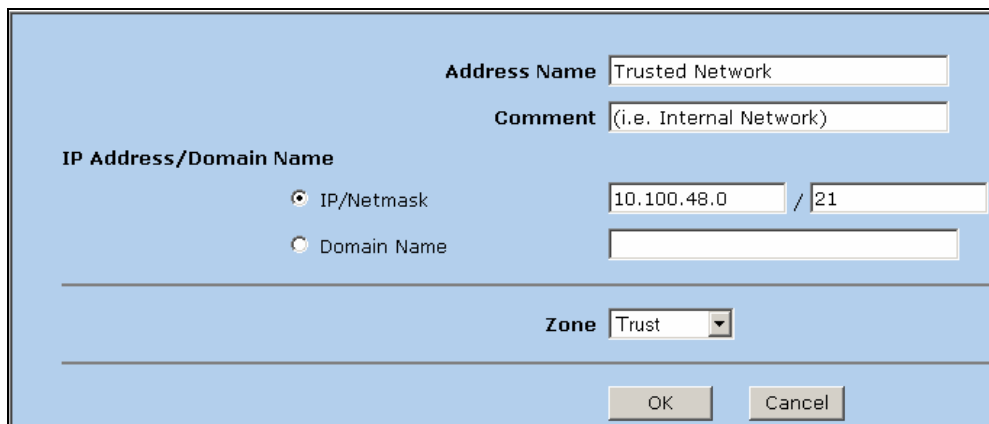
- Define the Trusted (Internal) network
- Define a User Group
- Define a Default User
- Define a Remote Gateway
- Define an AutoKey IKE VPN Tunnel
- Define a VPN Access Policy

Define the Trusted (Internal) network

1. If not already defined, enter the IP address of the Trusted (Internal) side of the Juniper Networks device. This will be the endpoint of the VPN tunnel.
2. From the Juniper Networks Administration Tool, click Objects > Addresses > Lists > Select the 'Trust' Filter from the pull down menu located at the upper left corner of the page:

Name	IP/Domain Name	Comment	Configure
Any	 0.0.0.0/0	All Addr	In Use
Dial-Up VPN	 255.255.255.255/32		In Use

3. If your Trusted (Internal) network is not defined here, click New, located in the upper right corner of the page. The Address Configuration dialog box appears.
4. Enter the following information:
 - Address Name
 - IP Address/Domain Name
 - Net Mask
 - Comment field: Optional
 - Zone: Trust

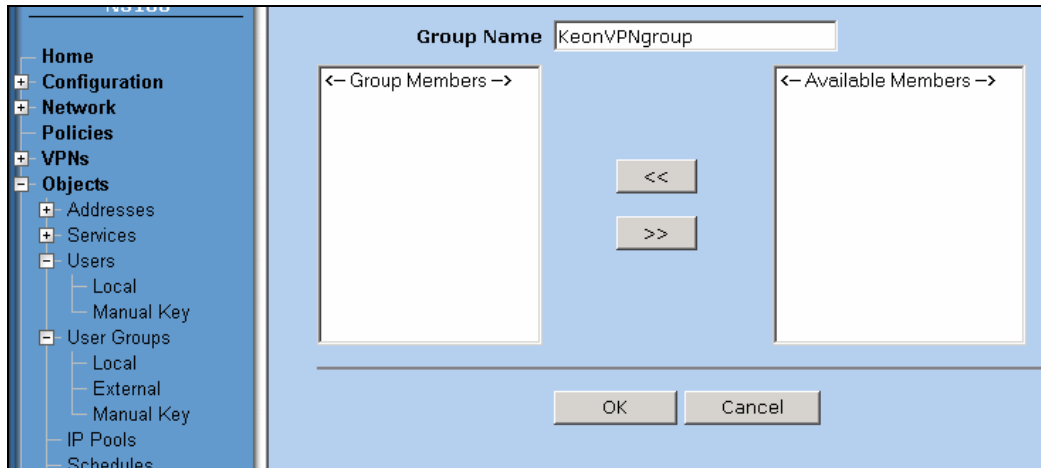


The dialog box is titled "Address Configuration" and has a light blue background. It contains the following fields and controls:

- Address Name:** A text input field containing "Trusted Network".
- Comment:** A text input field containing "(i.e. Internal Network)".
- IP Address/Domain Name:** A section with two radio buttons:
 - IP/Netmask: Two text input fields containing "10.100.48.0" and "21".
 - Domain Name: A single text input field.
- Zone:** A dropdown menu with "Trust" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Define a User Group

1. Create a Group name for your remote home users.
2. From the NetScreen Administration Tool, click Objects > User Groups > Local New.
3. Enter a group name and click OK.



4. You should now have a group defined similar to the one below.

Group Name	Group type	Members	Configure	
KeonVPNgroup	not defined	None	Edit	Remove

Define a Default User

1. Create a user name for your remote home users.
2. From the Juniper Networks Administration Tool, click Objects > Users > Local > New.
3. Enter the following information:
 - User Name
 - Select the User Group just created in the previous step.
 - Check IKE User
 - Select Use Distinguished Name For ID
 - Enter the portion of the users certificate DN that must match to authenticate.
 - Enter the number of users who can connect at one time with the matching DN.
 - Leave everything else at the default values, and click OK, located at the bottom of the page.

The screenshot shows the 'Auth/IKE/L2TP/XAuth User' configuration page. The left sidebar shows the navigation tree with 'Users' selected. The main area contains the following fields and options:

- User Name:** DefKeonPEca
- User Group:** KeonVPNgroup
- Status:** Enable, Disable
- IKE User** (Number of Multiple Logins with Same ID: 10)
- Simple Identity**
- Use Distinguished Name For ID**
 - CN:** [Empty field]
 - OU:** PE
 - Organization:** RSA
 - Location:** [Empty field]
 - State:** [Empty field]
 - Country:** US
 - E-mail:** [Empty field]
 - Container:** [Empty field]

4. You should now have an entry similar to the one below.

Name	Type	Group	Status	Identity	Configure
DefKeonPEca	IKE	KeonVPNgroup	Enabled	CN=,OU=PE,O=RSA,L=,ST=,C=US,E=	In Use

Define a Remote Gateway

Before you can set up an IKE tunnel for Dialup-to-LAN communication, you must define the remote gateway (remote computer running VPN client). This includes selecting an appropriate Phase 1 proposal for negotiating the building of the tunnel with the other end.

1. From the Juniper Networks Administration Tool, click VPN > AutoKey Advanced > Gateway > New.
2. Enter the following information:
 - Gateway Name
 - Set the Security Level to Custom
 - Remote Gateway Type to Dialup User Group
 - Select the User Group created in the previous step.

3. Click the Advanced button. Select the Phase 1 Proposals that the VPN client will need to use to connect along with the correct certificates.

4. To save the settings, click OK. The Gateway Listings page appears with the new entry.

Name	Type	IP/ID/User Group	Local ID	Security Level	Configure
KeonRemotePCs	Dialup	KeonVPNgroup	-	Custom	Edit -

Define an AutoKey IKE VPN Tunnel

Associate the remote gateway tunnel name with a Phase 2 Proposal describing how the data passing through the tunnel is to be encrypted and authorized.

1. From the Juniper Networks Administration Tool, click VPN > AutoKey IKE > New
2. Enter the following information:
 - **VPN Name:** Hostname
 - **Security Level:** Custom
 - **Remote Gateway:** Predefined and select the Gateway name

The screenshot shows the configuration interface for a new AutoKey IKE VPN tunnel. The left sidebar contains a navigation menu with options like Home, Configuration, Network, Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main configuration area includes the following fields and options:

- VPN Name:** KeonUserVPNTunnel
- Security Level:** Standard, Compatible, Basic, Custom (selected)
- Remote Gateway:** Predefined (selected), Create a Simple Gateway. Dropdown menu shows KeonRemotePCs.
- Gateway Name:** (empty text field)
- Type:** Static IP (selected), Dynamic IP, Dialup User, Dialup Group.
- IP address:** 0.0.0.0
- Peer ID:** (empty text field)
- User:** None (dropdown menu)
- Group:** KeonVPNgroup (dropdown menu)
- Local ID:** (empty text field) (optional)
- Preshared Key:** (empty text field)
- Security Level:** Standard (selected), Compatible, Basic.
- Outgoing Interface:** untrust (dropdown menu)

Buttons at the bottom include OK, Cancel, and Advanced.

3. Select Advanced and select the phase 2 proposals that the VPN clients will use.

The screenshot shows the Security Level configuration dialog box. It includes the following options and fields:

- Predefined:** Standard, Compatible, Basic (radio buttons)
- User Defined:** Custom (radio button)
- Phase 2 Proposal:**
 - Row 1: Encryption algorithm (nopfs-esp-3des-sha), Authentication algorithm (none)
 - Row 2: Encryption algorithm (none), Authentication algorithm (none)

4. Click OK to save the new entry. The updated list of AutoKey IKE VPN appears:

Name	Gateway	Security	Monitor	Configure
KeonUserVPNTunnel	KeonRemotePCs	Custom	On	Edit -

Define a VPN Access Policy

After you configure a VPN, you must define an Access Policy with the action set to *Tunnel* and associate it with the VPN tunnel.

1. From the Juniper Networks Administration Tool, Click Policy >New
2. Enter the following information:
 - **Name** (optional)
 - **Source Address:** Dial-Up VPN
 - **Destination Address:** Trusted Network
 - **Service:** ANY
 - **Action:** Tunnel
 - **VPN:** (from the drop-down list).

Use the same name that you assigned when defining the new AutoKey IKE entry in the last task. Leave the remaining fields at their default values.

3. Click OK to enter your settings.

Since the VPN Access Policy is more restrictive than the generic “Inside Any/Outside Any” Access Policy, it needs to be at the top of the list of policies. To move the Access Policy to the top of the list, click the icon in the row for the Access Policy that you want to move.

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
0	Dial-Up VPN	Trusted Network	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

4. The Juniper Networks device end of the eventual Certificate/AutoKey (IKE) VPN tunnel is complete.

VPN gateway to VPN gateway specific configuration

To create a successful VPN tunnel, you must set up the devices on both ends of the tunnel with identical configurations.

- Create a VPN gateway
- Create an AutoKey IKE entry
- Create a Policy
- Configure the second Juniper Networks box

Create a VPN gateway

1. From the main menu go to VPN – AutoKey Advanced – Gateway and click New.
2. Enter a name for the Remote Gateway.
3. Enter the IP Address of the Remote VPN server that the current Juniper Networks box will create the VPN tunnel with.

The screenshot shows a configuration dialog box for a VPN gateway. The 'Gateway Name' field contains 'ph054'. Under 'Security Level', the 'Custom' radio button is selected. The 'Remote Gateway Type' section has 'Static IP Address' selected. The 'IP Address' field contains '192.168.78.54'. The 'Peer ID' field is empty. The 'User' dropdown is set to 'None' and the 'Group' dropdown is also set to 'None'. The 'Preshared Key' field is empty. The 'Local ID' field is empty with '(optional)' next to it. The 'Outgoing Interface' is set to 'untrust'. At the bottom, there are 'OK', 'Cancel', and 'Advanced' buttons.

4. Click on the advanced button and select the Phase 1 Proposal under Security Level.

The screenshot shows the 'Security Level' configuration dialog box. Under 'Predefined', the 'Standard', 'Compatible', and 'Basic' radio buttons are unselected. Under 'User Defined', the 'Custom' radio button is selected. The 'Phase 1 Proposal' section has four dropdown menus: the first is set to 'rsa-g2-3des-md5', the second to 'none', the third to 'none', and the fourth to 'none'.

5. Select the Local Cert, Peer CA and Peer Type under Preferred Certificate.

The screenshot shows the 'Preferred Certificate' configuration dialog box. The 'Local Cert' dropdown is set to 'CN=ph021,CN=ph021.securitydynami'. The 'Peer CA' dropdown is set to 'CN=PE-LAB,OU=PE,O=RSA,C=US'. The 'Peer Type' dropdown is set to 'X509-SIG'.

6. Click Return and then OK to create the entry.

Create an AutoKey IKE entry

1. From the main menu select VPN – AutoKey IKE and click New.
2. Enter a name for the field VPN Name.
3. Select the Gateway just created in step one for the Remote Gateway.

VPN Name

Security Level Standard Compatible Basic Custom

Remote Gateway Predefined
 Create a Simple Gateway

Gateway Name

Type Static IP IP address
 Dynamic IP Peer ID
 Dialup User User
 Dialup Group Group

Local ID (optional)

Preshared Key

Security Level Standard Compatible Basic

Outgoing Interface

4. Click on Advanced.
5. Select the Phase 2 Proposal under security level, which will be used.

Security Level

Predefined Standard Compatible Basic
User Defined Custom

Phase 2 Proposal

<input type="text" value="nopfs-esp-3des-md5"/>	<input type="text" value="none"/>
<input type="text" value="none"/>	<input type="text" value="none"/>

6. Click Return and then OK.

Create a Policy

1. From the main menu select Policy.
2. Enter a Name for the VPN connection.
3. Select the address Book for the Source Address and Destination Address if they were defined. In this example we are using "Any".
4. Select the Remote VPN Gateway for the Tunnel.
5. Select Modify matching bi-directional VPN policy.

Name (optional) VPNtoVPN

Source Address

New Address

Address Book Any

Destination Address

New Address

Address Book Any

Service ANY

Action Tunnel

Tunnel VPN ph054IKE

Modify matching bidirectional VPN policy

L2TP None

OK Cancel Advanced

6. Click OK.
7. To configure the second Juniper Networks NetScreen Firewall/VPN box, you must perform the same steps on the Remote Juniper Networks box.

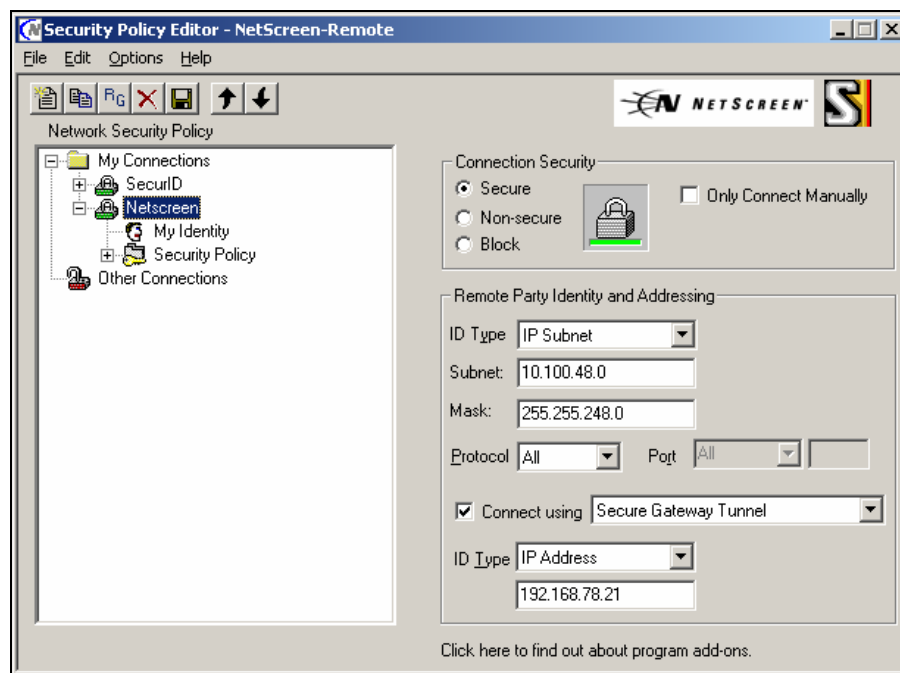
VPN Client Specific Configuration

This section explains the basics of configuring the Juniper Networks NetScreen-Remote client for IKE operation with digital certificates. There are 4 steps to setting up Juniper Networks NetScreen-Remote for an AutoKey IKE VPN tunnel:

- Create a new connection
- Configure your identity
- Define the IPSec protocols
- Initiate the connection

Creating a new connection

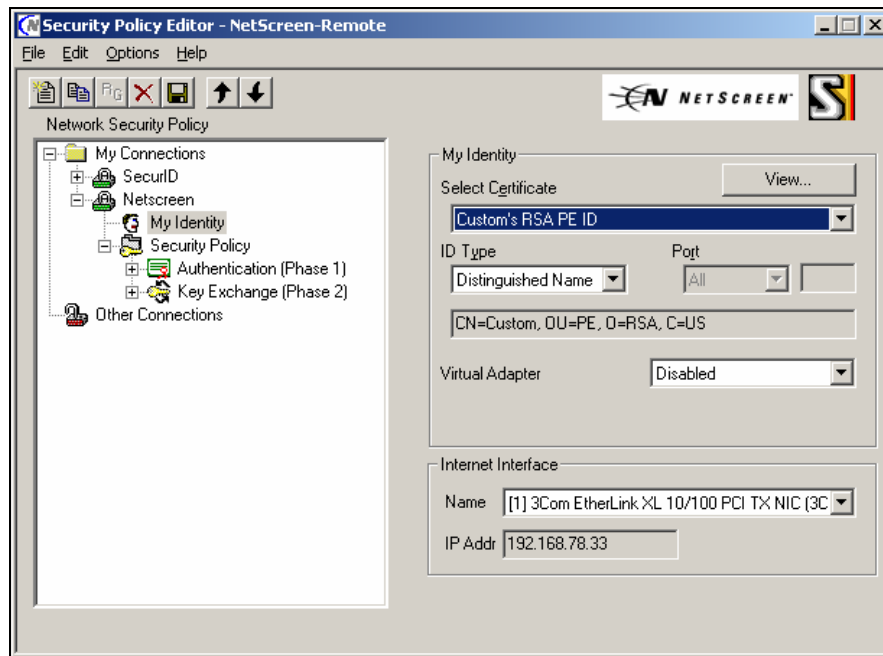
1. Double-click the Juniper Networks NetScreen-Remote icon to open the Security Policy Editor.
2. On the File menu, choose New Connection. A new connection icon appears in the Network Security Policy list.
3. Give the new Connection a unique name.



4. Under Connection Security, select Secure.
5. In the Remote Party Identity and Addressing area, select IP Subnet in the ID Type drop-down list, and type in the Subnet and Mask.
6. Define the protocol you want to use for the Connection: All, TCP, UDP, ICMP. The default is All.
7. Select 'Connect using Secure Gateway Tunnel'. The Secure Gateway Tunnel ID Type and IP Address fields become available.
8. For ID Type, select IP address from the ID Type list to identify the other party, and then enter the IP address of the Juniper Networks device. (This is the Un-trusted port IP address of the Juniper Networks device).

Configuring the identity

1. Configure your identity so that the party with whom you want to communicate can verify who you are. For this secure connection, you need to choose a digital certificate from the Certificate Manager.
2. Double-click the icon for the new connection. My Identity and Security Policy icons appear.
3. Select My Identity. The My Identity and Internet Interface areas appear.

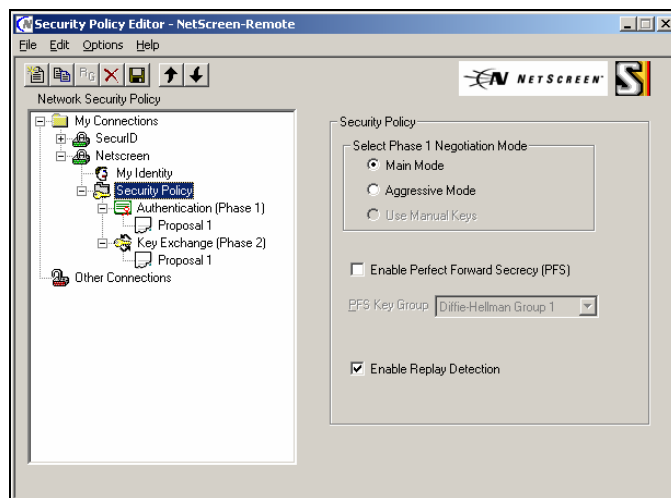


4. Select your certificate from the Select Certificate drop-down list.
5. For the ID Type, select Distinguished Name.
6. Save the entries.

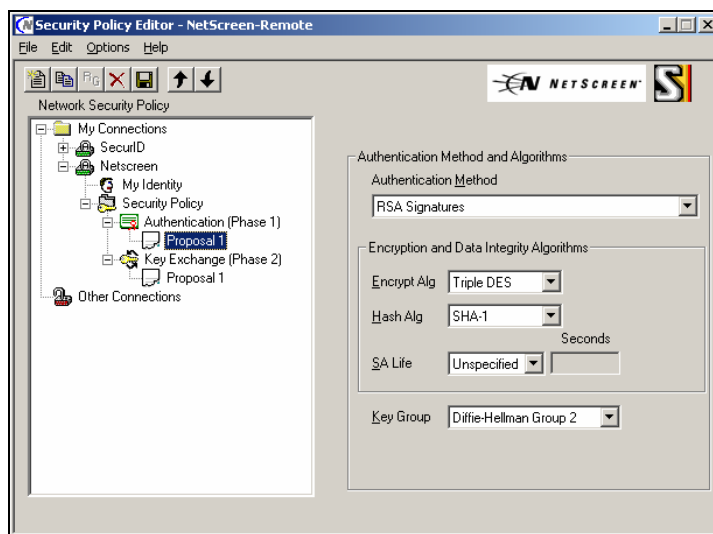
Defining the IPSec protocols

Define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

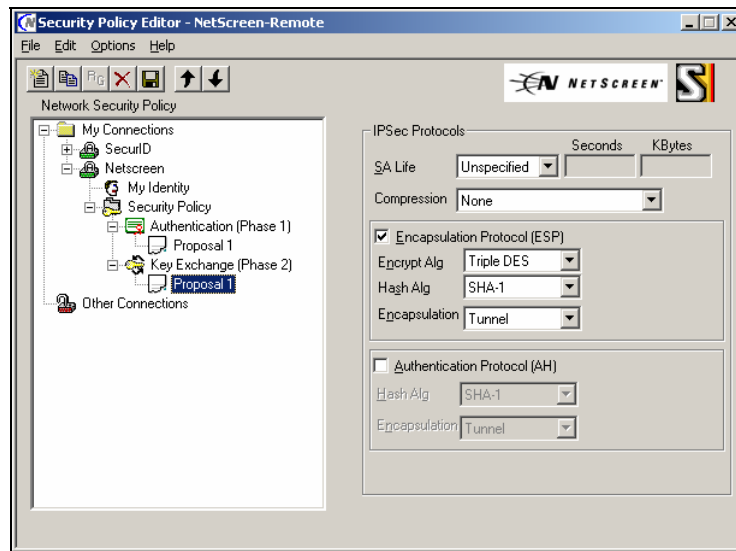
1. Double-click Security Policy in the Network Security Policy list. The Security Policy area appears on the right, and the Authentication (Phase 1) icon and Key Exchange (Phase 2) icon appear in the Network Security Policy list, as shown below.



2. Select Aggressive Mode or Main Mode in the Security Policy area.
3. Select Enable Perfect Forward Secrecy (PFS) and Enable Replay Detection if you want to employ these options. For additional information on the options available here, please refer to the Juniper NetScreen product documentation.
4. In the Network Security Policy list, double-click Authentication (Phase 1). Proposal 1 appears below the Authentication (Phase 1) icon.
5. Select Proposal 1 to display the Authentication Method and Algorithms area.



6. In the Authentication and Algorithms area, define the Encryption Algorithm, the Hash Algorithm, and the Security Association (SA) Life. Because you selected a digital certificate, RSA Signatures is what appears in the Authentication Method field. Although there is a drop-down list, no other choices are available.
7. In the Key Group drop-down list, select either Diffie-Hellman Group 1, Diffie-Hellman Group 2, or Diffie-Hellman Group 5. This must match what you set on the NetScreen device.
8. In the Network Security Policy list, double-click Key Exchange (Phase 2). Proposal 1 appears below the Key Exchange (Phase 2) icon.
9. Select Proposal 1 to display the IPSec Protocols area.



10. In the IPSec Protocols area, define the SA Life (that is, the lifetime of the Security Association) in either seconds or bytes, or leave it as Unspecified.
11. The Compression feature reduces packet sizes to expedite transmission. To enable compression, choose Deflate from the drop-down list; to disable it, choose None.
12. Other Juniper Networks products do not currently support compression. Because the devices on both ends of the VPN tunnel need to support this feature to be able to use it, leave the setting at None.
13. Select Encapsulation Protocol (ESP). Set the encapsulation method to Tunnel and set the Encrypt Alg and Hash Alg to match what you set on the Juniper Networks device.
14. Click Save on the toolbar or choose Save Changes from the File menu. The configuration for the Juniper Networks NetScreen-Remote end of an eventual VPN tunnel using a digital Certificate is complete.

Initiate a connection

With both ends of the tunnel configured, you are ready to make a secure VPN tunnel connection.

1. Launch your Web browser and enter an IP address within the network's internal subnet. Juniper Networks NetScreen-Remote, which continually checks all IP addresses that you enter, recognizes this address as the one you configured for a secure connection. It routes the transmission to the security gateway (that is, the un-trusted port of the Juniper Networks appliance and proposes the VPN tunnel connection. The Juniper Networks device responds to this proposal by checking its database until it finds the Access Policy defining the proposed connection as a VPN tunnel. With the settings at both ends in accord, Juniper Networks NetScreen-Remote and the Juniper Networks device begin using their local certificates and the specified ESP encryption and authentication algorithms to secure the connection.
2. The VPN tunnel is established.

Certification Checklist for VPN Products

Date Tested: February 24, 2005

Product	Operating System	Tested Version
RSA Keon Certificate Authority	Windows 2000 Server (SP4)	6.5.1
Juniper/NetScreen Firewall/VPN	Hardware Version 1010(0)	NS-5GT
Juniper/ NetScreen OS		5.0.0r6.1
Juniper NetScreen Remote	Windows XP Professional (SP1)	10.1.1(Build 10)

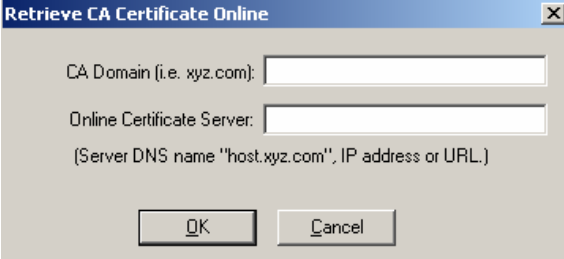
Test Case	Gateway	Client	RSA KWP	RSA SOM
Certificate Enrollment:				
P10 Certificate Request	✓	✓	N/A	N/A
P7 Response installed correctly	✓	✓	N/A	N/A
SCEP Certificate Request	✓	✗*	N/A	N/A
SCEP Response installed correctly	✓*	✗*	N/A	N/A
Importation:				
Import certificate via P12	N/A	N/A	N/A	N/A
V3 certificate installed correctly	N/A	N/A	N/A	N/A
CA Trust:				
Install v3 Root CA via cut/paste	✓	✓	N/A	N/A
Install v3 SubCA via cut/paste	✓	✓	N/A	N/A
Install v3 Root CA via SCEP	✓	✓	N/A	N/A
Install v3 SubCA via SCEP	N/A	N/A	N/A	N/A
Verify cert chain is installed	N/A	N/A	N/A	N/A
Connectivity:				
Use certificate (authentication)	✓	✓	N/A	N/A
Use certificate for IPSec tunnel	✓	✓	N/A	N/A
Advanced Connectivity:				
IP Address assignment	N/A	N/A	N/A	N/A
DNS address assignment	N/A	N/A	N/A	N/A
WINS address assignment	N/A	N/A	N/A	N/A
Access resources on network (web)	✓	✓	N/A	N/A
Status Check (w/IPSec tunnel):				
Success with a valid certificate	✓	✓	N/A	N/A
Fails - revoked certificate	✓	✓	N/A	N/A
Fails - suspended certificate	✓	✓	N/A	N/A
Success - reinstated certificate	✓	✓	N/A	N/A
Device-to-Device:				
Establish Secure Connectivity	✓	N/A	N/A	N/A

EF

✓ = Pass ✗ = Fail N/A = Non-Available Function
 ✓* or ✗* = See Known Issues

Known Issues

1. The Juniper Networks NetScreen Firewall/VPN device needs the next update filed set in the CRL. To add the next update filed to an RSA Keon CA CRL see the RSA Keon CA documentation on adding the CLR timer directive.
2. SCEP will only work at this time if Auto Vetting is turned on for the Juniper Networks NetScreen Firewall/VPN on the RSA Keon CA or you force the Juniper Networks NetScreen Firewall/VPN to use only one CN. See the RSA Keon Documentation on how to enable Auto Vetting. To force one CN on the Juniper Networks NetScreen Firewall/VPN run "set pki x raw-cn enable" from the command line of the Juniper Networks NetScreen Firewall/VPN. See the Juniper Networks NetScreen Firewall/VPN documentation for more information regarding this command or other command line functions.
3. SCEP enrolment does not work with the Juniper Networks NetScreen Remote VPN client version 10.1.1 because of a 64 character limitation in the form for the SCEP URL (Online Certificate Server field). The RSA Keon SCEP URL is typically 62 characters long before the hostname of the Certificate Authority is added. It is not known when this limitation was introduced but the 8.1 version of the client was able to enroll via SCEP.



Retrieve CA Certificate Online

CA Domain (i.e. xyz.com):

Online Certificate Server:

(Server DNS name "host.xyz.com", IP address or URL.)

OK Cancel