Juniper Networks
ScreenOS

RSA SecurID Ready Implementation Guide

Last Modified: January 31, 2012

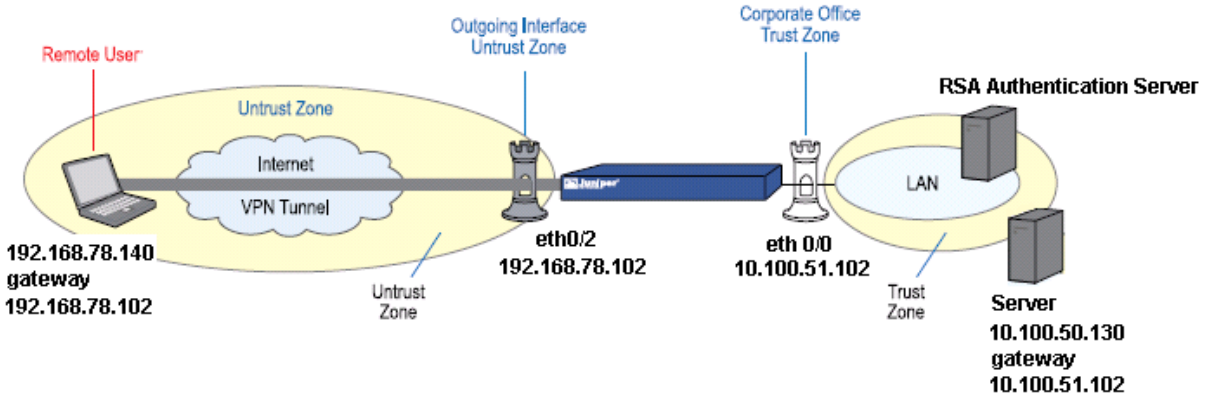
Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	ScreenOS
Version & Platform	6.3.0 r10
Product Description	ScreenOS 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, ScreenOS devices provide customers multiple layers of defense to keep their assets safe.

Solution Summary

ScreenOS can be configured to require external users to authentication using a SecurID token before access is granted to services inside the network. Internal users can be required to authenticate before accessing resources outside the network as well. Security administrators can be required to authenticate using SecurID tokens before being granted access to the ScreenOS security device's administrative interface.

RSA SecurID supported features ScreenOS 6.3.0 r10	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with the ScreenOS security device will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the ScreenOS security device to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	None stored
Node Secret	In Memory
sdstatus.12	In Memory
sdopts.rec	Not implemented

Note: The appendix of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring ScreenOS with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All ScreenOS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

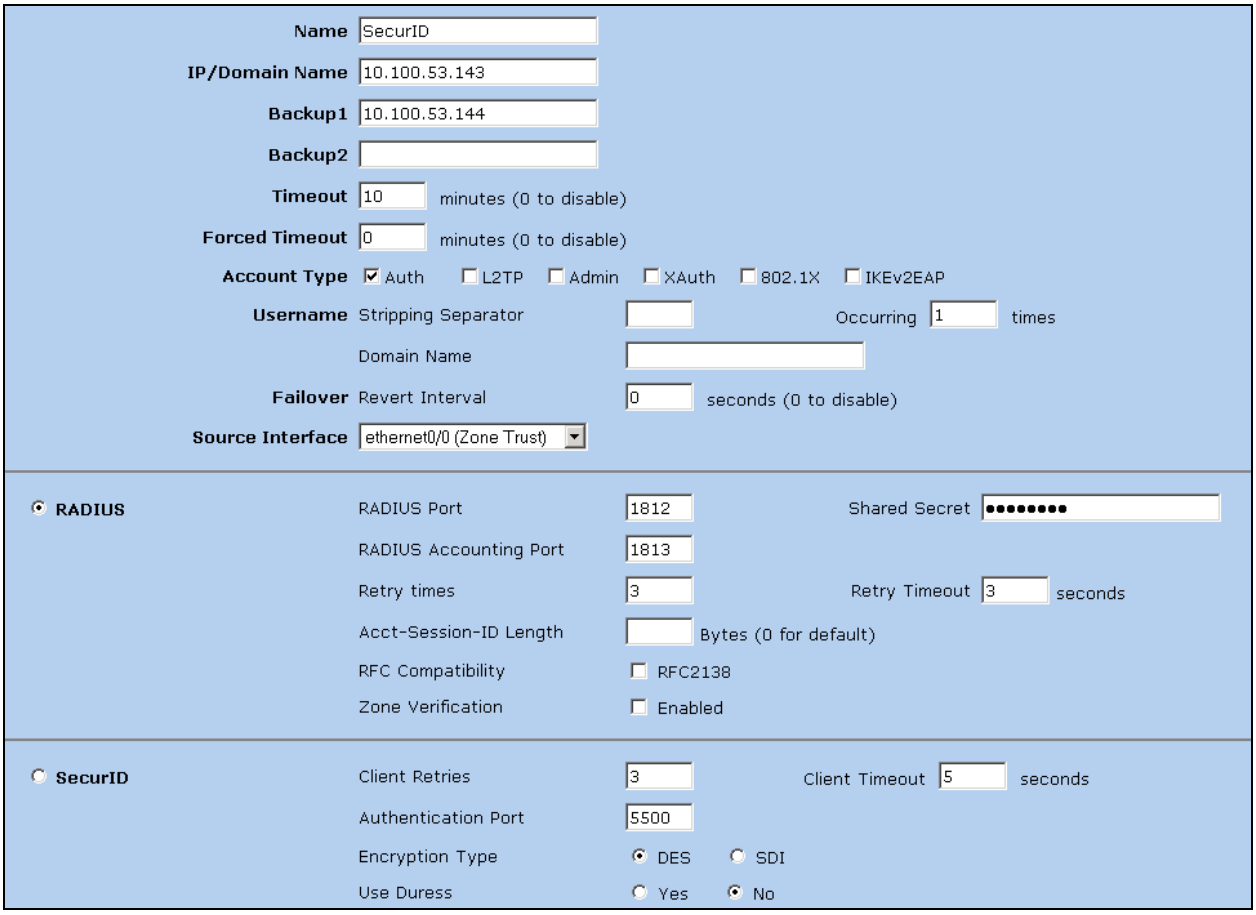
ScreenOS Configuration

Configuring Authentication Servers

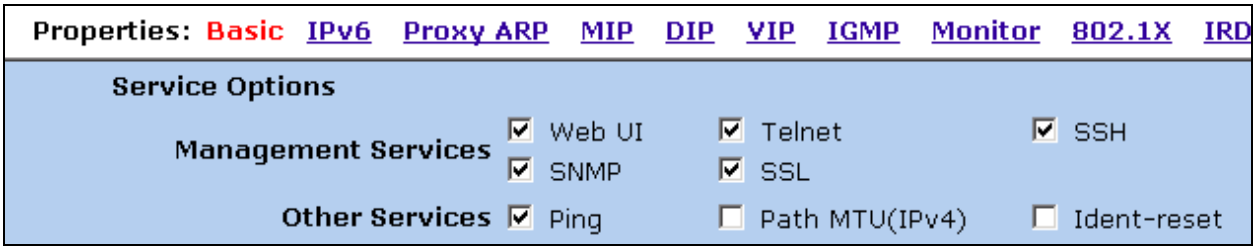
1. Browse to the Management IP address of the ScreenOS security device to access the ScreenOS configuration WebUI.
2. Navigate to **Configuration > Auth > Auth Servers** and click **New** to create a new authentication server.

3. Configure a name and enter the IP addresses or hostnames of your RSA Authentication Manager servers. Configure an account type of **Auth**, and specify a source interface. This should be the Ethernet interface on the security device that can communicate with your RSA Authentication Manager instance. Select additional Account Types depending on your requirements. Select an authentication server type of either **SecurID** or **RADIUS** and configure the SecurID or RADIUS options accordingly.

> **Note: Change Juniper's default RADIUS port to match RSA Authentication Manager's default RADIUS port of 1812.**



4. Ensure that the interface(s) for which access will be permitted are configured for the appropriate protocols. Navigate to **Network > Interfaces** and select **Edit** for the Untrust zone's interface(s) to verify that they are configured correctly.

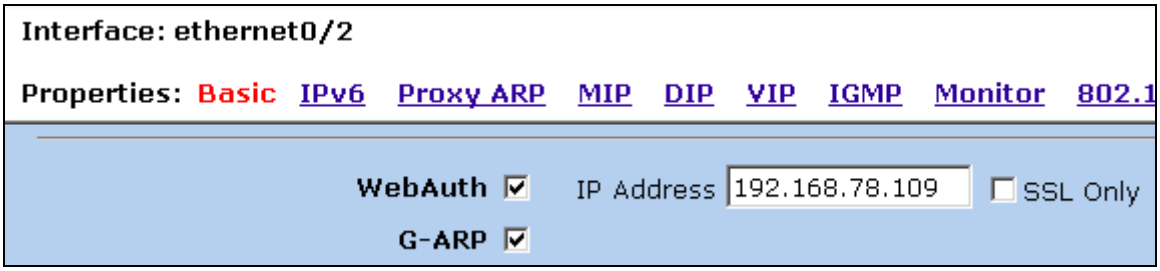


Configuring Users for WebAuth

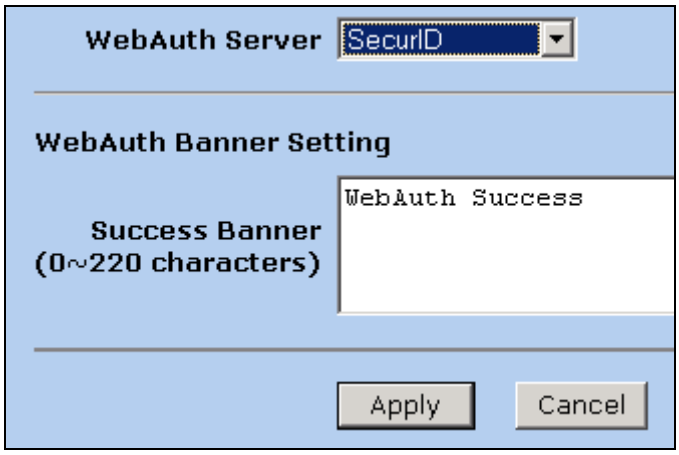
This type of authentication is also referred to as “Pre-Policy Check Authentication”. WEB Auth permits a user to be authenticated using a RSA SecurID token before being permitted access to resources in a different security zone.

> **Note: WEB Auth does not provide any mechanism for the user to perform Next Token code or new PIN mode.**

1. Define a **WebAuth** IP on the interface(s) for which WebAuth will be active. The option for this can be found on the **Basic** properties page for the interface in the ScreenOS WebUI.

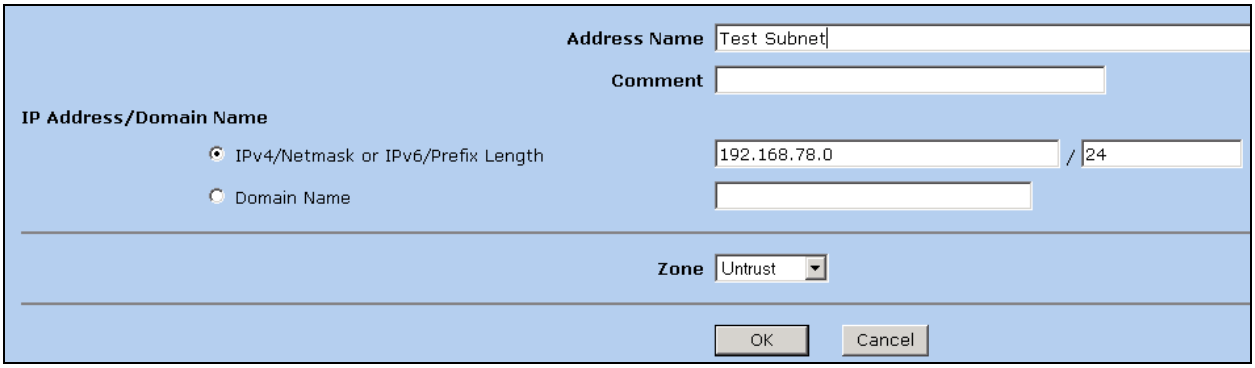


2. Navigate to **Configuration > Auth > WEB Auth** and specify the SecurID Server previously defined.

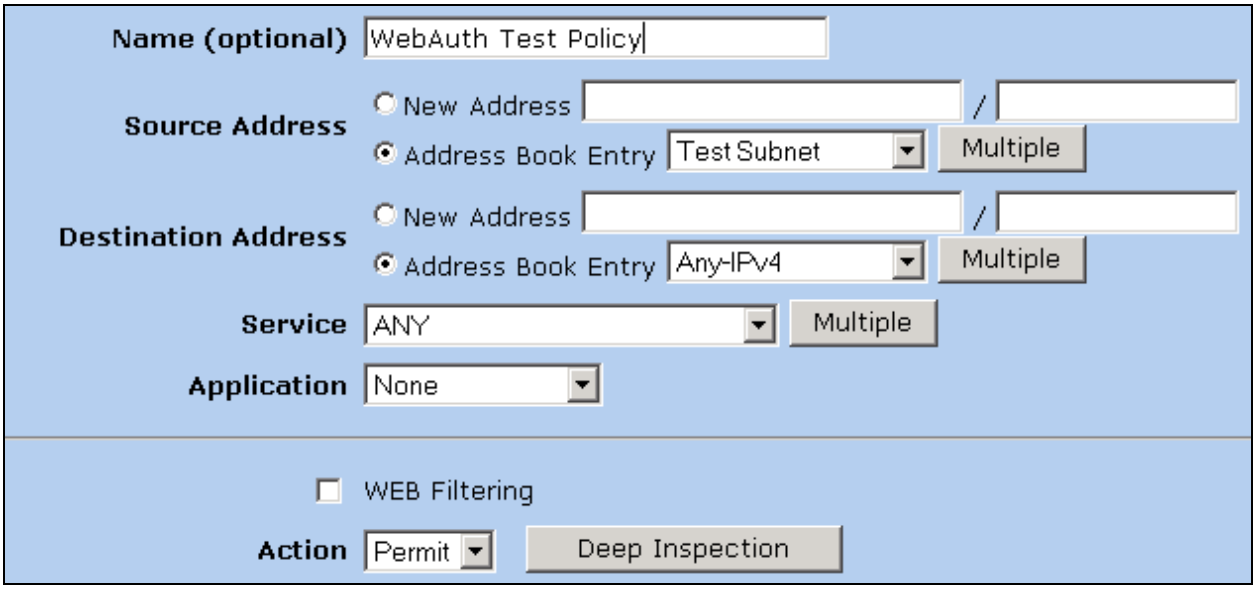


3. This example creates a policy to permit traffic from hosts in the **Untrust** security zone to any addresses in the **Trust** security zone. Begin by defining the hosts you wish to allow from the Untrust zone as a Policy Element. Navigate to **Policy > Policy Elements > Addresses > List**. Select the **Untrust** zone and click **New**.

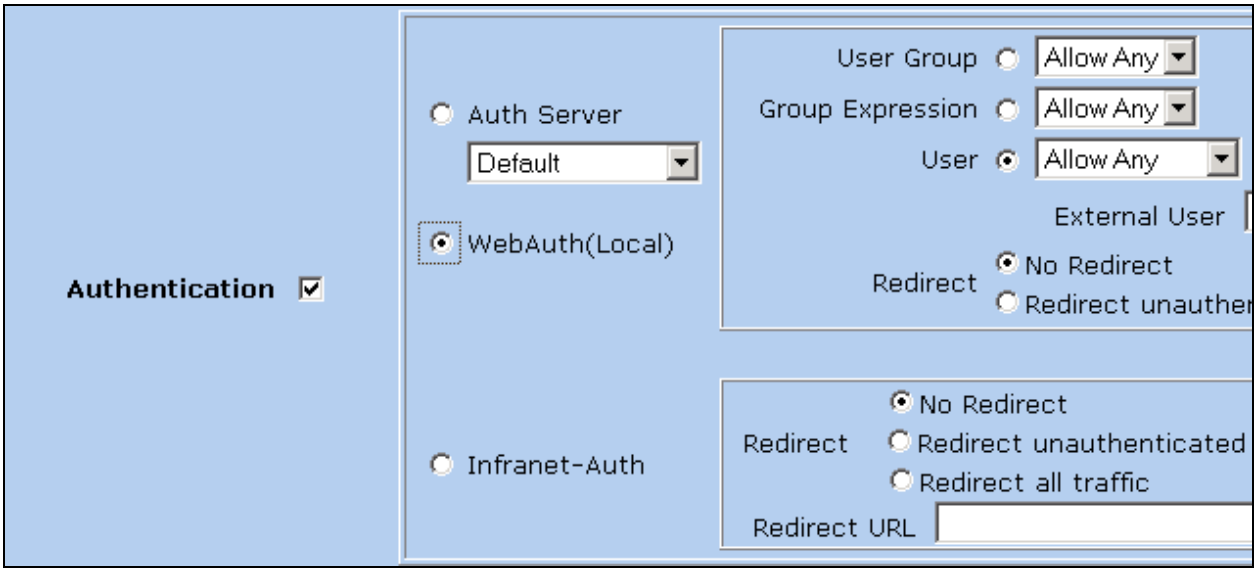
4. Fill in the appropriate fields. In this example, we define a subnet (192.168.78.0/24) in the Untrust zone. Click **OK** when finished.



5. Navigate to **Policy > Policies**. Filter the policies by selecting **From Untrust Zone** and **To Trust Zone**. Click **New** to create a new policy.
6. For the **source address**, select the address book entry created in step 4. For the **destination address**, select **Any**. For the **action** select **Permit**.



7. Click **Advanced** to access the advanced policy settings. Check the **Authentication** field and select the **WebAuth** radio button. Click **OK** to save the policy.

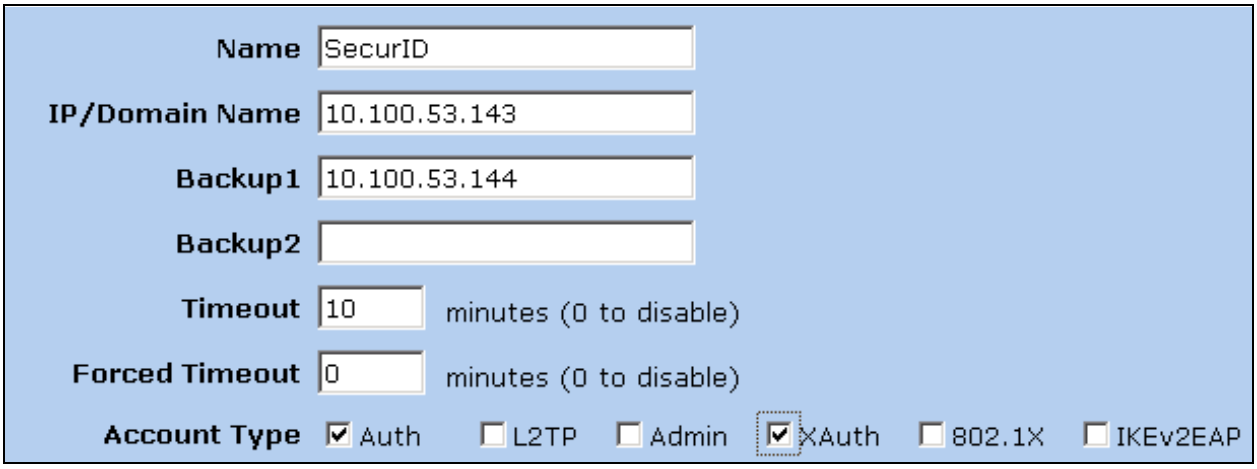


Once this policy is created, users from the designated subnet must use RSA SecurID two-factor authentication to authenticate before being permitted to reach any destination in the Trust security zone. In this example, the authentication takes place when the user browses to 192.168.78.109 using a web browser.

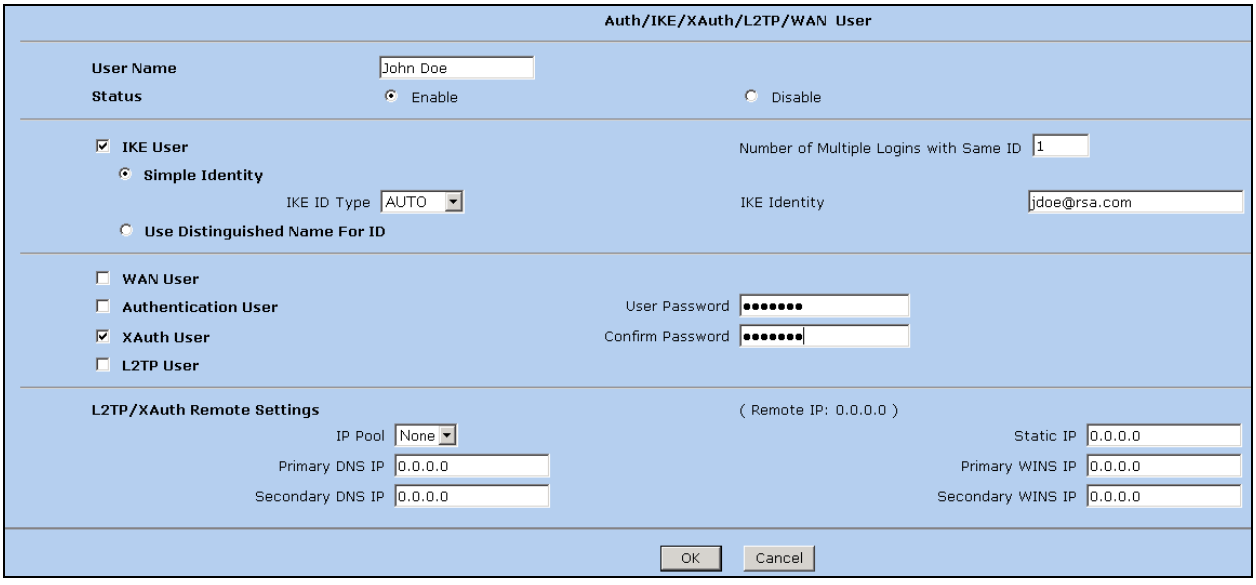
Configuring VPN Authentication

ScreenOS can be configured to use RSA SecurID to authenticate VPN tunnels that it creates for users accessing resources across security zones. In this example, we configure a per-user VPN tunnel and configure ScreenOS to authenticate the user using SecurID two-factor authentication. The NetScreen Remote VPN client is used to establish the tunnel on the client.

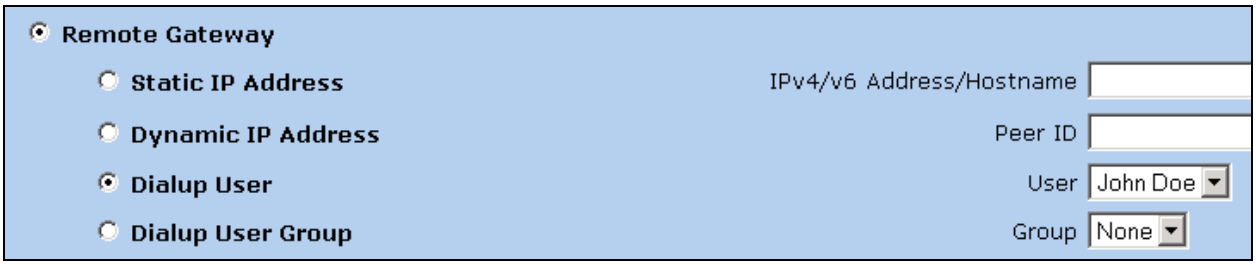
1. Log in to the ScreenOS configuration WebUI and navigate to **Configuration > Auth > Auth Servers**. Configure an Auth Server as before, only this time specify an Account Type of **XAuth**.



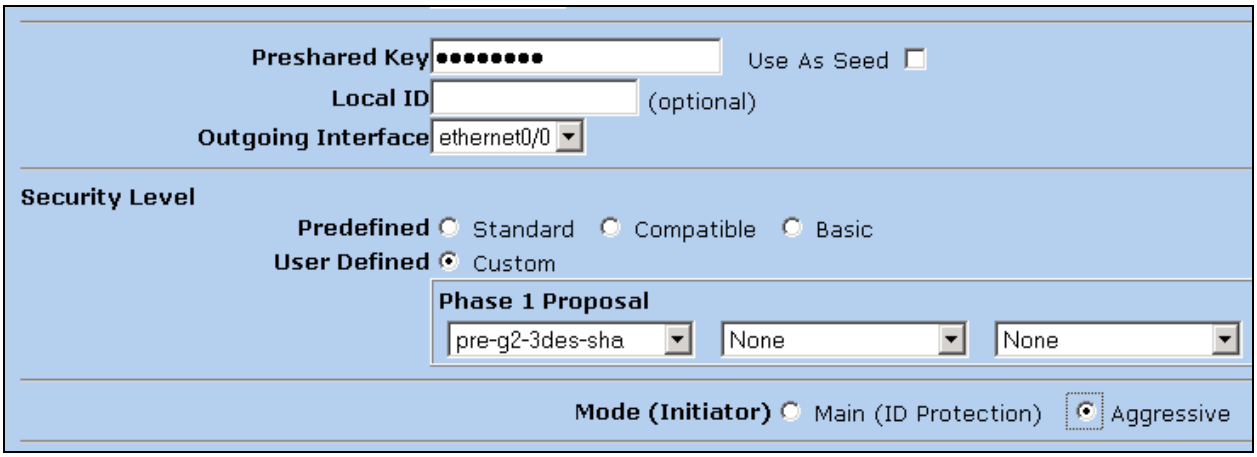
2. Create a user who will have VPN access by navigating to **Objects > Users > Local** and clicking **New** to create a new user. Select **IKE User**, choose **Simple Identity** and provide an IKE Identity for the user. Select **XAuth User**, and click **OK** to create the user object.



3. Create a new VPN Gateway by navigating to **VPNs > AutoKey Advnaced > Gateway** and clicking **New**. Give the gateway a name and select **Remote Gateway** and **Dialup User**. Select the user created in the previous step. Click **Advanced** to access the advanced gateway options.



4. Configure the IKE Security options to meet your requirements. In this example, we use a preshared key for the Phase 1 Authentication. Aggressive Mode is used because Main mode cannot operate with preshared keys. Click **Return** then **OK** when finished to create the gateway.

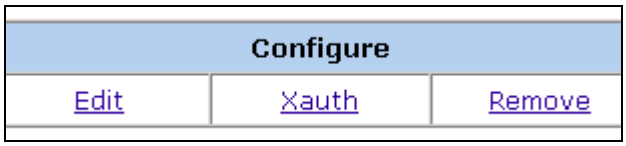


! Important: This example uses preshared keys and Aggressive Mode for demonstation purposes.

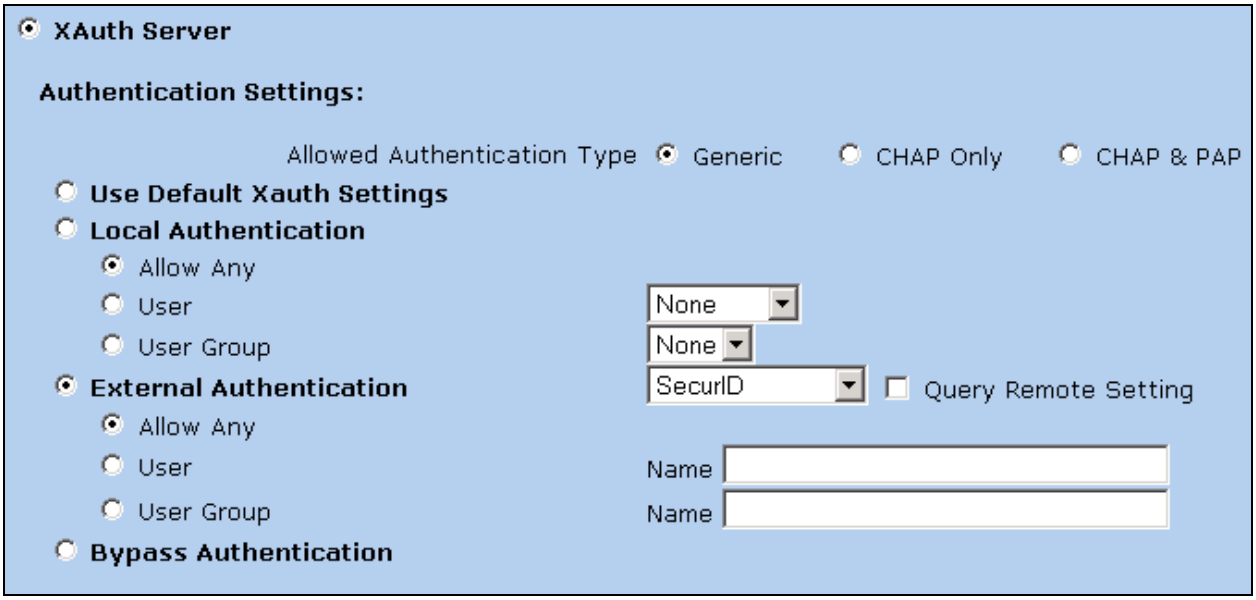
Preshared keys and Aggressive Mode contain security weaknesses that can be exploited. Production environments should always secure Phase 1 Authentication using certificate-based authentication in Main Mode.

Refer to the ScreenOS documentation for more information on securing VPN tunnel communication.

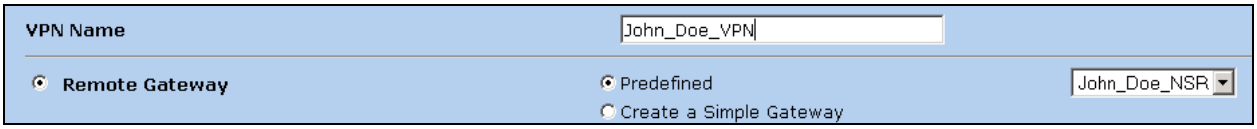
5. Click on the **Xauth** link for the newly created gateway.



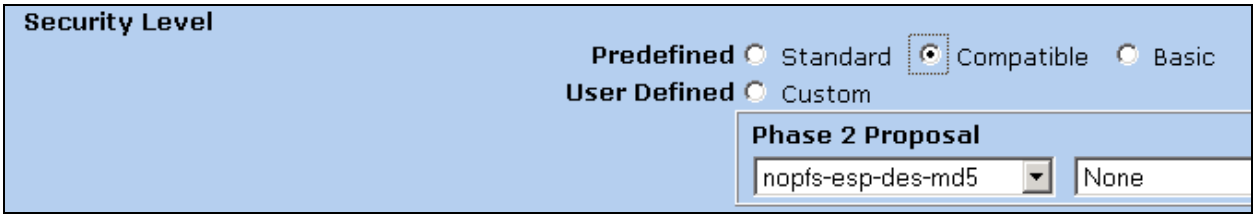
6. Choose **XAuth Server** and an Allowed Authentication Type of **Generic**. Select **External Authentication**, **Allow Any**, and choose the authentication server that was defined earlier. Click **OK** to confirm the settings.



7. Create a new VPN by navigating to **VPNs > AutoKey IKE** and clicking **New**. Give the VPN a name and choose **Remote Gateway** and **Predefined**. Select the gateway you created in the previous step. Click **Advanced** to access the advanced VPN settings.

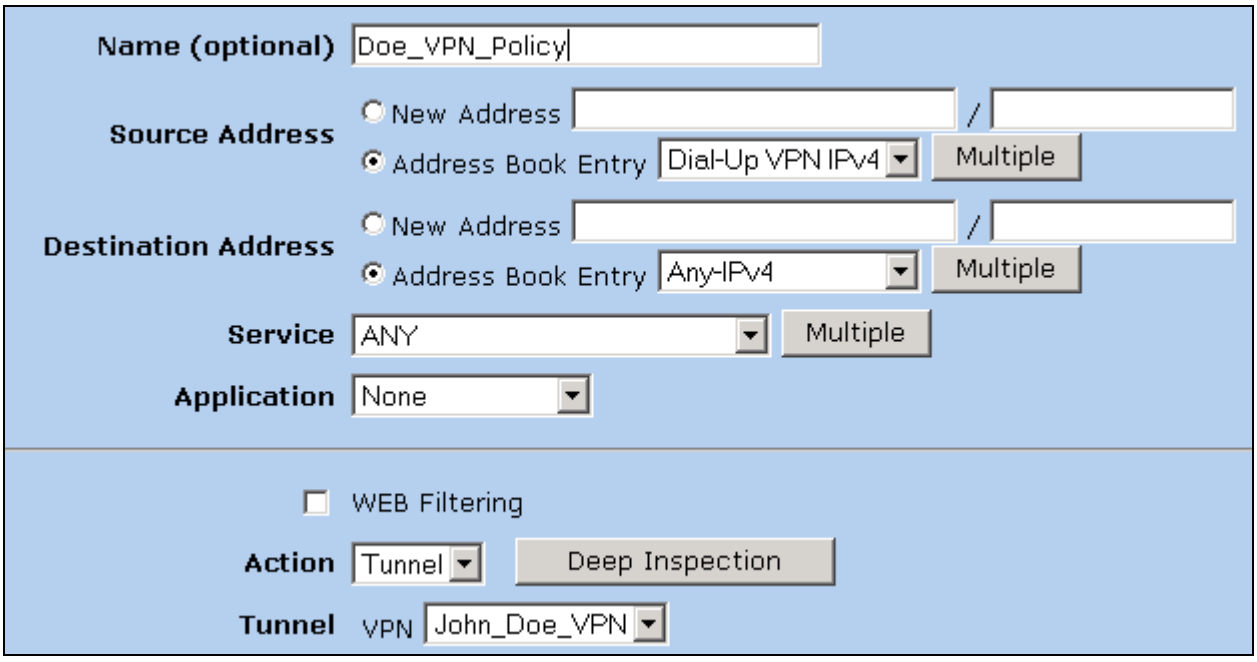


8. Choose **Compatible** for the Phase 2 Security Level. Click **Return** then **OK** to finish creating the VPN.



9. Navigate to **Policy > Policies** and filter the policies by choosing **From Untrust** and **To Trust**. Click **New** to define a new policy.

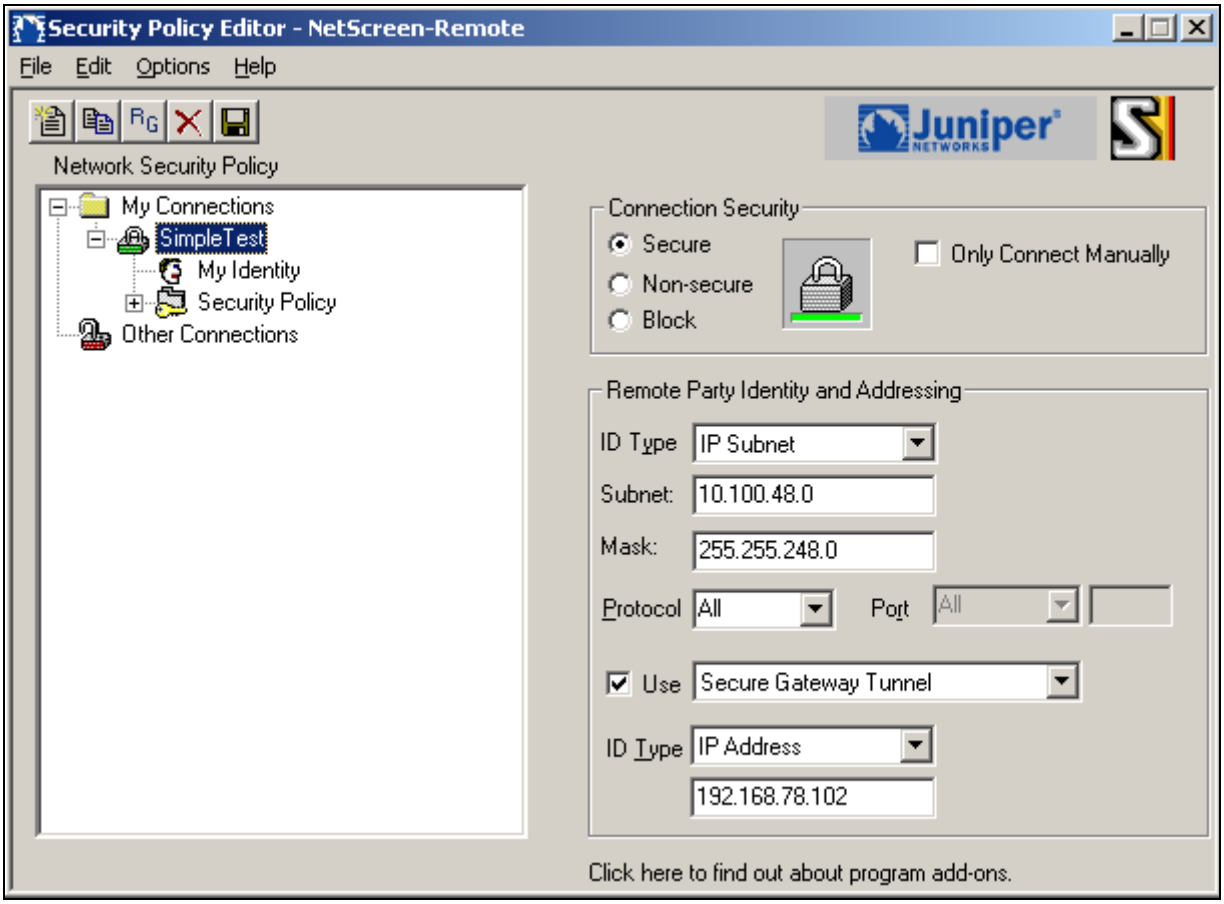
10. Give the policy a name and choose **Dial-up VPN** for the source address. Choose the address book entry in the trusted network that will be accessed by the VPN. Choose **Tunnel** for the action and select the VPN created in the previous step. Click **OK** to create the policy.



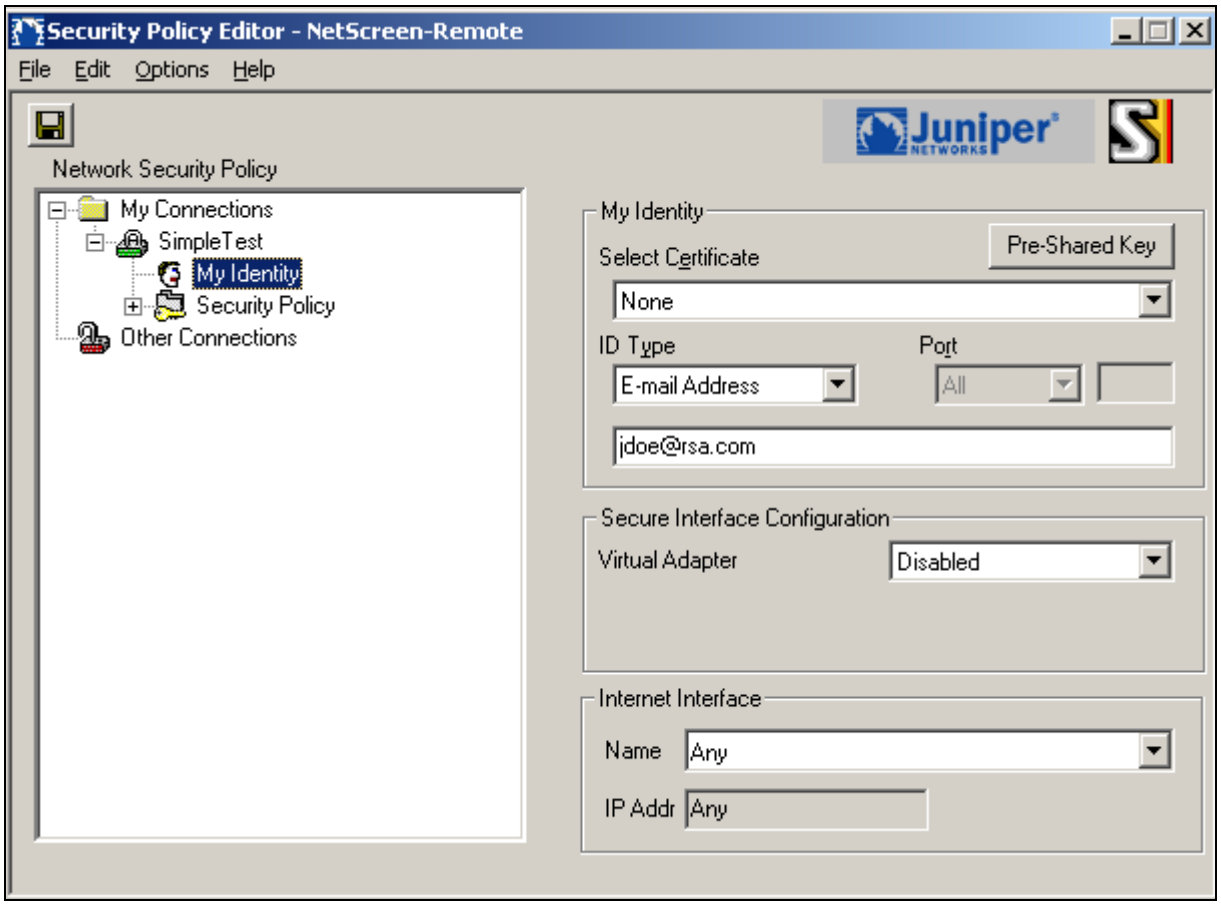
Configuring NetScreen Remote on the client

A VPN configuration must be created on the NetScreen Remote client that matches the settings we defined for the user in the previous steps. Your configuration may differ from the example below, but it is important that the remote client settings match those configured on the firewall. Refer to Juniper's documentation for ScreenOS and NetScreen Remote for detailed instructions.

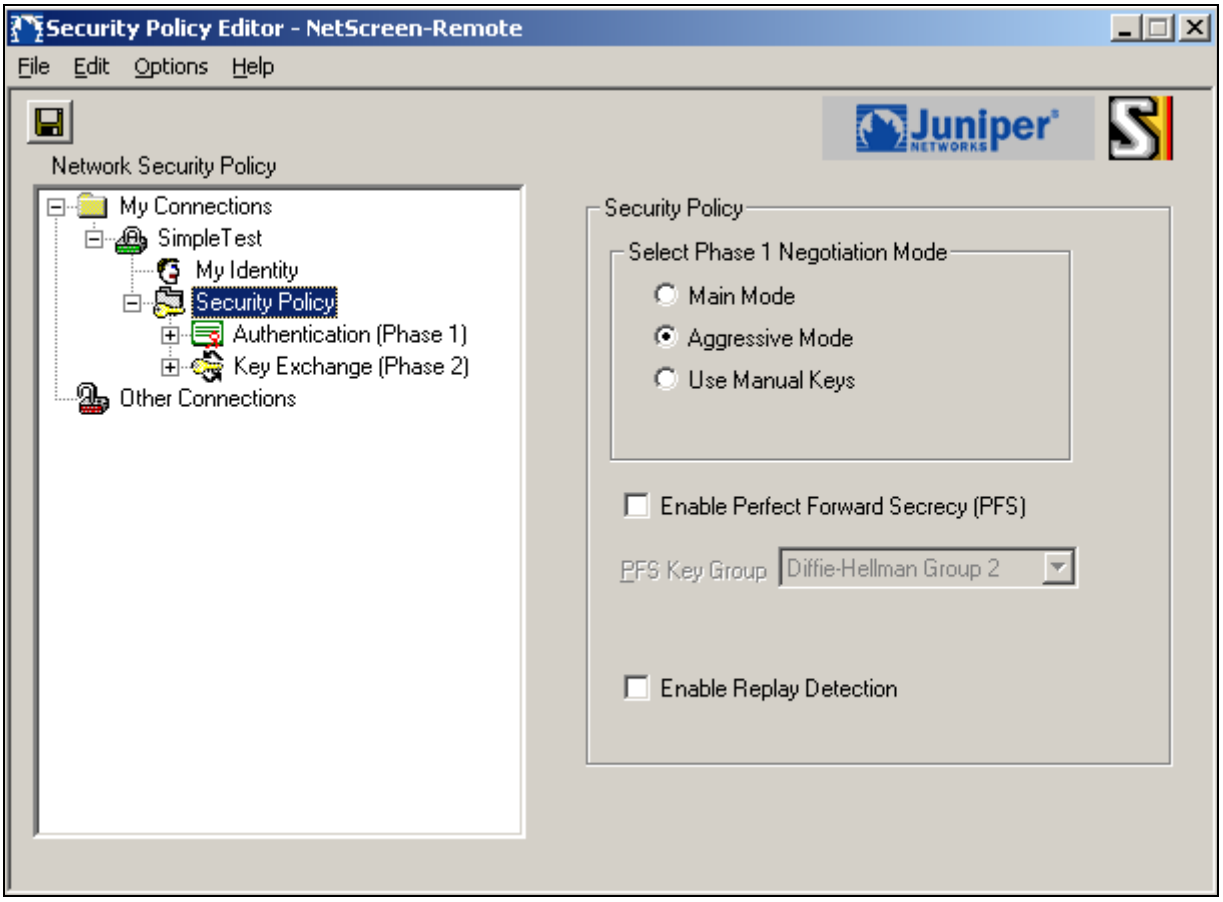
1. Create a new connection under **My Connections**. Set the Connection Security to **Secure**. ID type should be **IP Subnet** in this case. The subnet entered is that of the trusted network. Check **Use** and choose **Secure Gateway Tunnel** from the drop-down box. ID type will be **IP Address** and the value should be the IP address of the Untrust interface on the firewall.



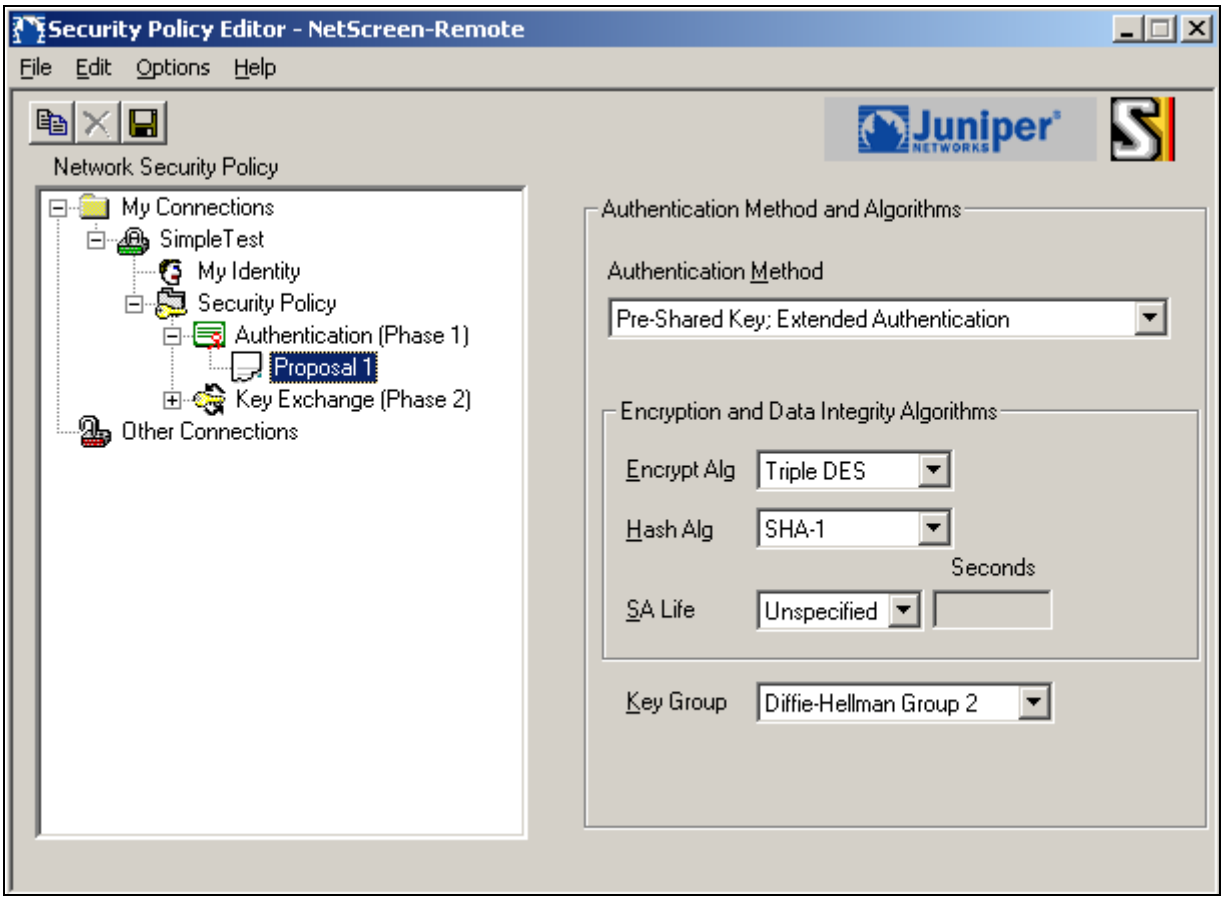
2. Select **My Identity** and supply identity details for the client. If you configured a preshared key for Phase 1 Authentication on the firewall, click the **Pre-Shared Key** button and supply that key.



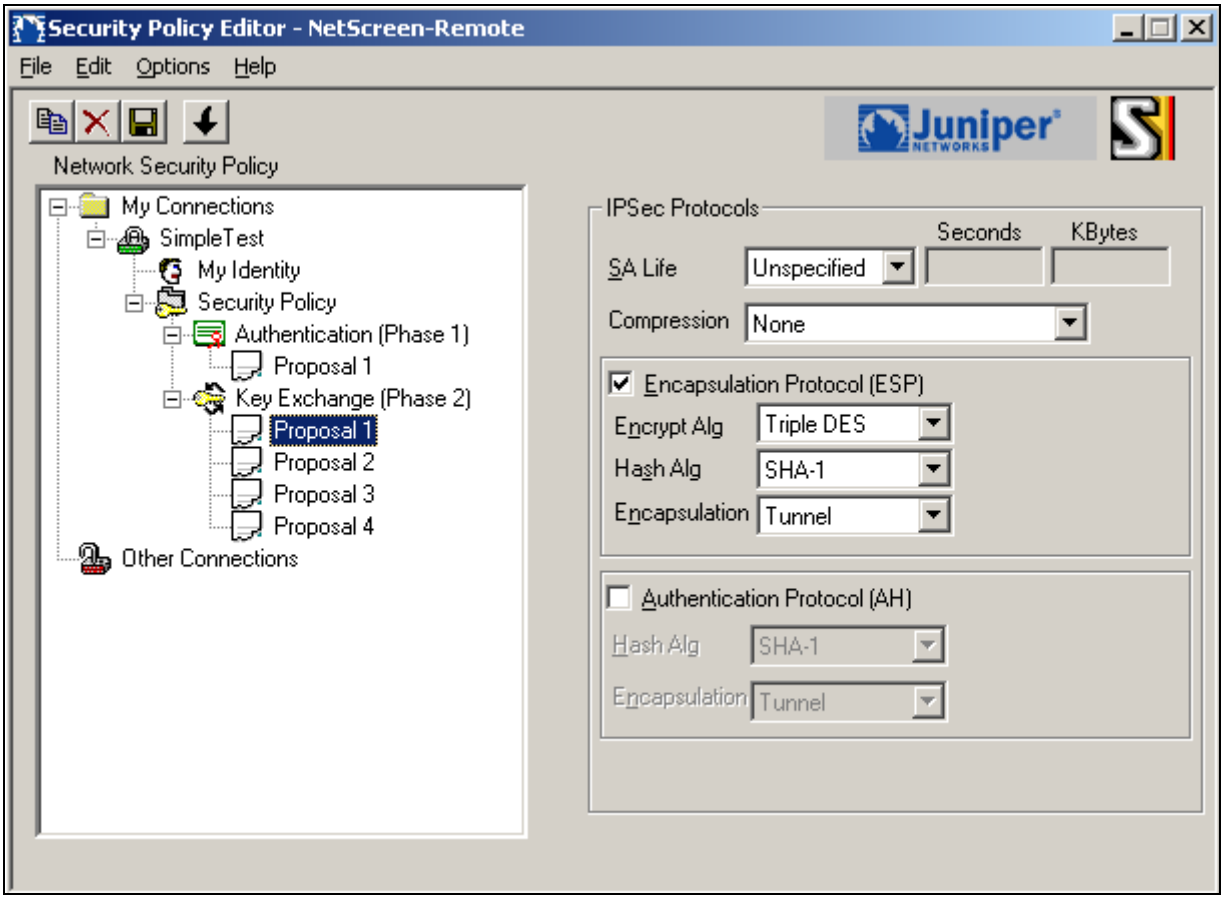
3. Select **Security Policy** and configure these settings to match those configured on the ScreenOS security device. In this example, we used a preshared key, so we must select Aggressive Mode. Our chosen methods do not support Perfect Forward Security (PFS), and we did not enable Replay Detection on the ScreenOS security device.



4. Select **Authentication (Phase 1)** and configure a proposal that matches what was configured on the ScreenOS device. In this example, we chose **pre-g2-3des-sha** as the proposal type for Phase 1, so we configure and Authentication Method of **Pre-Shared Key** with **Extended Authentication**. **Triple DES** is the encoding algorithm, **SHA-1** is the hash algorithm, and **Diffie-Hellman Group 2** is the key group. Extended authentication is needed in order to query the user for their SecurID username and passcode.



5. Select **Key Exchange (Phase 2)** and configure compatible proposals for phase 2 to match those configured on the ScreenOS device. In this example, four compatible proposals are configured. All use **Encapsulation Protocol (ESP)** and **Tunnel** encapsulation. The compatible encryption and hashing methods chose are **Triple DES / SHA-1**, **Triple DES / MD5**, **DES / SHA-1**, and **DES / MD5**.

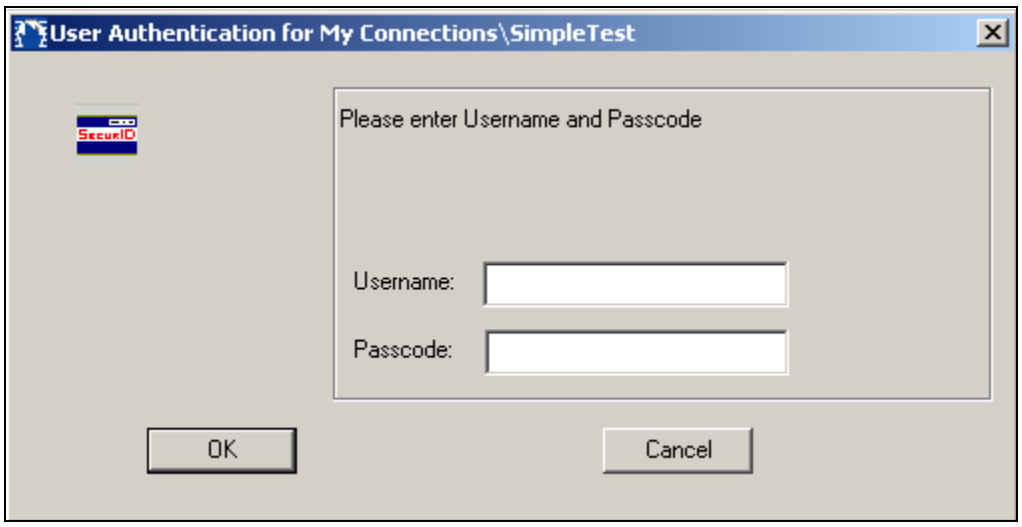


6. Save the newly created security policy.

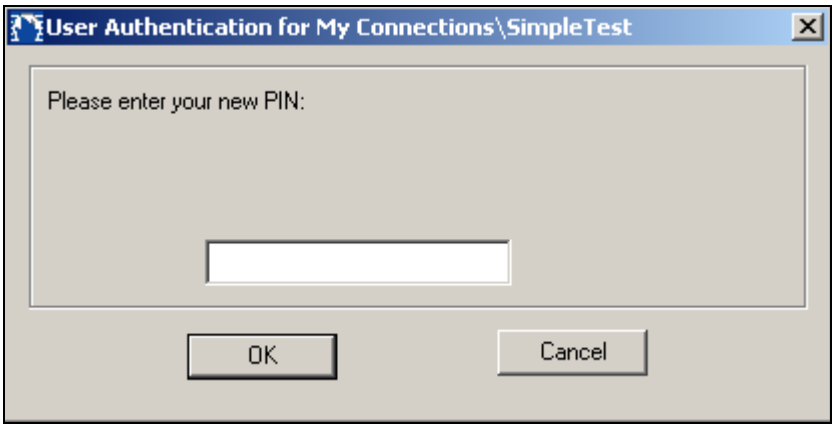
If configured correctly, a ping to any host on the trusted network will bring up an authentication dialog, where users must supply their SecurID username and passcode.

Screens

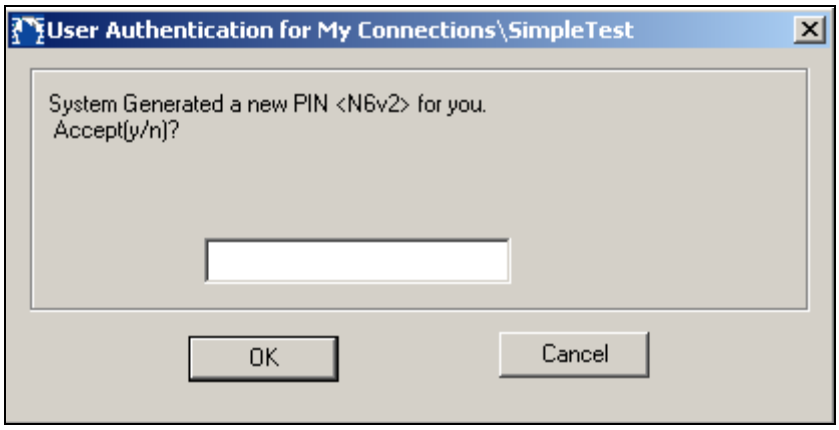
Login screen:



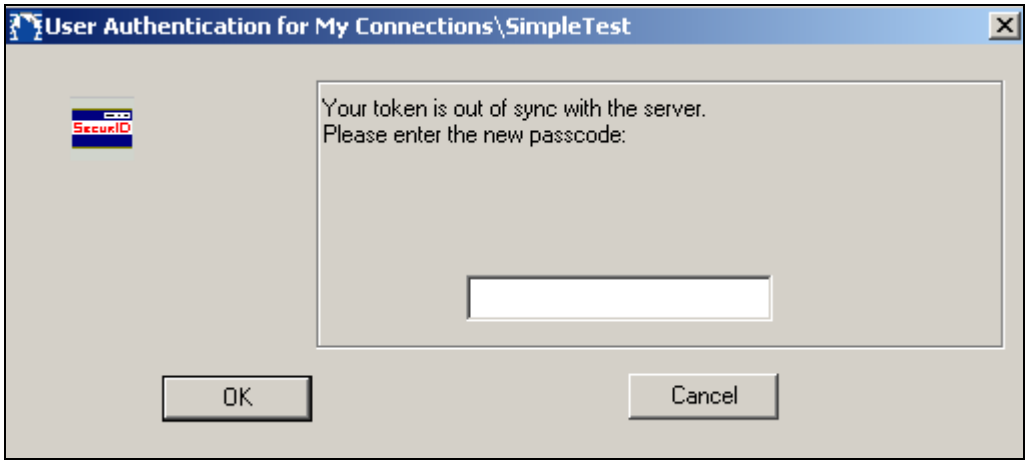
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: January 31, 2012

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP4	Windows Server 2003 SP2
Juniper ScreenOS	6.3.0 r10	Appliance
Juniper NetScreen Remote	9.0 r5	Windows Server 2003

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	✓
System Generated PIN	✓	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
Deny Numeric PIN	✓	Deny Numeric PIN	✓
Deny PIN Reuse	✓	Deny PIN Reuse	✓
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	✓
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	✗	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	✓
On-Demand New PIN	✓	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
No RSA Authentication Manager	✓	No RSA Authentication Manager	✓

MRQ

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Known Issues

WebAuth doesn't support New PIN / Next Tokencode modes

ScreenOS's WebAuth authentication method does not provide any mechanism to handle New PIN or Next Tokencode modes. This means that if a user's PIN is expired / not set or if RSA Authentication Manager requests the next tokencode from the user, instead of receiving these prompts, the user will be denied access.

Next Tokencode mode fails when using Native SecurID Protocol

Authentication fails when using the Native SecurID protocol for authentication and the user is in next tokencode mode due to an out of sync token or too many subsequent failed authentication attempts. This means that an RSA Authentication Manager administrator must synchronize the token or clear the failed login attempts to reset the user.

Note: For further information on known issues and available fixes, contact Juniper Technical Support.

Appendix

Partner Integration Details	
RSA SecurID API	Custom Build
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

To remove the node secret from the ScreenOS device, you must gain access to the CLI either via the console port, SSH, or Telnet. Log in to the console with the administrator account and execute the command:

```
delete node_secret
```