



RSA SecurID Ready Implementation Guide

Last Modified: 3/28/2003

1. Partner Information

Partner Name	Netscreen
Web Site	www.netscreen.com
Product Name	ScreenOS
Version & Platform	4.x
Product Description	<p>NetScreen Technologies Inc. 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, NetScreen 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>NetScreen 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, NetScreen provides customers multiple layers of defense to keep their assets safe.</p>
Product Category	Firewall / VPN



2. Contact Information

	Sales Contact	Support Contact
E-mail	info@netscreen.com	support@netscreen.com
Phone	408-730-6000	408-730-6768
Web	www.netscreen.com	www.netscreen.com/support/

3. Solution Summary

RSA SecurID authentication can be applied to “Auth Users”, “Xauth Users”, “L2TP Users”, and “Admin Users”.

Auth users include run-time authentication where the user is prompted for a user name and password when trying to reach a service through the firewall in-run time. Pre-check authentication, also called WEB Auth, where the user uses a WEB browser to authenticate against an address on the firewall prior to being permitted access to resources beyond the firewall.

External users can be required to authenticate using a SecurID token before access is granted to services inside the network. Internal users can be required to authenticate using a SecurID token before being granted access to resources outside the network as well. Security administrators can be required to authenticate using SecurID tokens before being granted access to the NetScreen Firewall itself.

Feature	Details
Authentication Methods Supported	Native RSA SecurID, RADIUS
RSA ACE/Agent Library Version	Version # 4.x
RSA ACE 5 Locking	No
Replica RSA ACE/Server Support	Master/Slave Only
Secondary RADIUS/TACACS+ Server Support	Yes 3 RADIUS Servers
Location of Node Secret on Client	To clear run “clear node_secret” from command prompt
RSA ACE/Server Agent Host Type	Communication server
RSA SecurID User Specification	all users
RSA SecurID Protection of Administrators	Yes

4. Product Requirements

- Hardware requirements**

NS-5XT, NS-5XP, NS-25, NS-50, NS-204, NS-208, and NS-500

- Software requirements**

Component Name: Netscreen appliance	
Operating System	Version (Patch-level)
ScreenOS	4.0.0
Web browser	Netscape Communicator 4.7 and up IE 5.x and up
Netscreen Remote	8

5. RSA ACE/Serverconfiguration

Perform the following steps to set up the Netscreen appliance as an Agent Host within the RSA ACE/Server's database.

- On the RSA ACE/Server computer, go to **Start > Programs > RSA ACE/Server**, and then **Database Administration - Host Mode**.
1. On the **Agent Host** menu, choose **Add Agent Host...**

The screenshot shows a configuration dialog box for adding an agent host. The fields are as follows:

- Name:** ph022.securitydynamics.com
- Network address:** 10.100.51.22
- Site:** (empty field) with a **Select** button to the right.
- Agent type:** A dropdown menu with **UNIX Agent** selected. Other options are **Communication Server** and **Single-Transaction Comm Server**.
- Encryption Type:** Radio buttons for **SDI** and **DES**, with **DES** selected.
- Node Secret Created:**
- Open to All Locally Known Users:**
- Search Other Realms for Unknown Users:**
- Requires Name Lock:**

At the bottom, there are two columns of buttons:

- Left column: **Group Activations...**, **Secondary Nodes...**, **Edit Agent Host Extension Data...**, **Assign Acting Servers...**
- Right column: **User Activations...**, **Delete Agent Host**, **Assign/Change Encryption Key...**, **Create Node Secret File...**

At the very bottom are **OK**, **Cancel**, and **Help** buttons.

- In **Name**, type the name of the Netscreen appliance.
- In **Network address**, type the IP address of the Netscreen appliance.
- Under **Secondary Nodes**, define all hostname/IP addresses that resolve to the Netscreen appliance.

Note: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA ACE/Server documentation for detailed information on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

6. Partner ACE/Agent configuration

This section provides instructions for integrating the partners' product with RSA SecurID. 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.

Administrative (Admin) Users

In this section we treat the configuration of Admin User authentication for the NetScreen security appliance. The configuration permits the security administrator to be authenticated using a SecurID token card before being permitted access to the NetScreen. The administration options are selected on each interface. SecurID support is available for the WEB UI, Telnet, SSL, and SCS access to the NetScreen security appliance. An administrator using any of these access methods can use SecurID to authenticate. (SSL access requires that a certificate be installed on the NetScreen security appliance first.)

NOTE: Admin user configurations do not provide any mechanism for the administrator to perform New Pin or Next Tokencode mode via the NetScreen firewall. SecurID User authentication and SecurID Admin authentication cannot be used simultaneously in a Netscreen Firewall

NetScreen Configuration

1. The NetScreen must be configured to use the ACE 5.0 Servers as Master and Slave (RSA ACE/Server 5 nomenclature is Primary and Replica, respectively). Define a new Server under “Configuration/Auth/Auth Servers” and clicking on new. Fill in the appropriate values for the RSA ACE/Servers on the resulting screen.
 - “Name” is a label used in the NetScreen firewall to refer to the RSA ACE/Server authentication server – it is NOT the name associated with a DNS entry.
 - The “IP/Domain Name” should be either the IP address or the FQDN of the primary RSA ACE/Server.
 - The “Backup1” server should be either the IP or FQDN of the replica RSA ACE/Server.
 - “Backup2” does not apply to RSA ACE/Server authentication configuration.
 - Click the button labeled “SecurID”. The default values will normally suffice unless the Authentication Port settings have been changed on the RSA ACE/Server. Leave “Encryption Type set as “DES”.

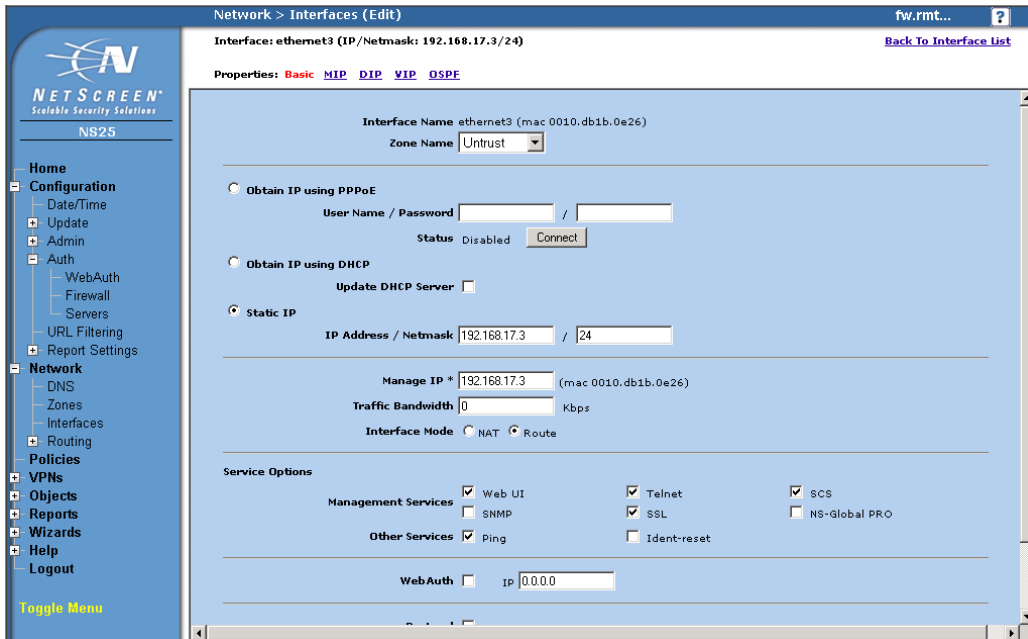
The screenshot shows the NetScreen configuration interface for defining an ACE/Server. The browser address bar shows 'http://ph022/top.html*6,1,1'. The page title is 'Configuration > Auth > Auth Servers > Edit'. The left sidebar shows the navigation menu with 'Auth' selected. The main content area contains the following fields and options:

- Name:** ACE/Servers
- IP/Domain Name:** 10.100.50.37
- Backup1:** 10.100.50.36
- Backup2:** (empty)
- Timeout:** 10 (0 to disable)
- Account Type:** Auth, IKE, L2TP, Admin, XAuth
- RADIUS:** RADIUS, Radius port: 1645, Shared Secret: (empty)
- SecurID:** SecurID, Client Retries: 3, Client Timeout: 5 seconds, Authentication Port: 5500, Encryption Type: DES, SDI, Use Duress: Yes, No
- LDAP:** LDAP, LDAP Port: 389, Common Name Identifier: cn, Distinguished Name(dn): (empty)

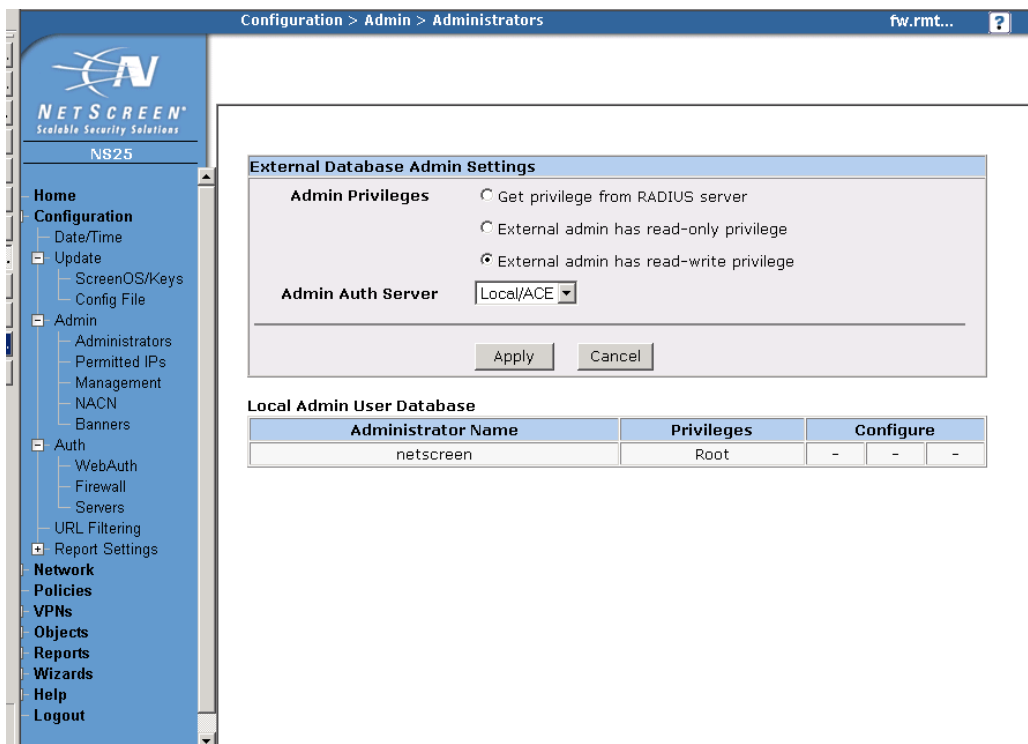
Buttons for 'OK' and 'Cancel' are located at the bottom right of the form.

Figure 1 Define ACE/Servers

2. Ensure that the interface(s) on the firewall for which administrative access will be permitted on are configured to permit administrative access. This is performed under “Network/Interfaces”. Note that SSL administrative access using SecurID authentication is possible, but it requires the loading of the appropriate certificates(s) on the firewall.



3. Once the Admin Server has been defined, go to Configuration > Admin > Administrators and select the “Local/<RSA ACE/Server name>” setting from the drop-down box. This was defined in step one above. Chose what administrative privileges you wish the RSA SecurID authenticated administrator to have.



WEB Auth Users

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 card before being permitted access to resources in a different security zone.

To get authenticated, the user points a WEB browser to an IP address on the NetScreen Firewall that has been established expressly for this purpose. An authentication dialog ensues during which the user enters their user ID and their RSA SecurID token. Once authenticated, the user can then reach services in another security zone. The need to WEB Authenticate and the IP addresses and services protected by the WEB Auth mechanism are defined in a NetScreen firewall policies. These policies specify that the user must perform a WEB authentication before being granted access.

RSA SecurID User authentication and RSA SecurID Admin authentication cannot be used simultaneously in a Netscreen Firewall. WEB Auth does not provide any mechanism for the user to perform Next Token code or new PIN mode.

1. NetScreen Configuration

The NetScreen must be configured to use the ACE 5.0 Servers as Master and Slave (RSA ACE/Server 5 nomenclature is Primary and Replica, respectively). This is achieved by defining a new Server under “Configuration/Auth/Auth Servers” and clicking on new. Fill in the appropriate values for the ACE/Servers on the resulting screen.

- “Name” is a label used in the NetScreen firewall to refer to the RSA ACE/Server– it is NOT the name associated with a DNS entry.
- The “IP/Domain Name” should be either the IP address or the FQDN of the primary RSA ACE/Server.
- The “Backup1” server should be either the IP or FQDN of the replica RSA ACE/Server.
- “Backup2” does not apply to RSA ACE/Server configuration.
- Click the button labeled “SecurID”. The default values will normally suffice unless the Authentication Port settings have been changed on the RSA ACE/Server. Leave “Encryption Type set as “DES”.

The screenshot shows the NetScreen configuration interface for defining an ACE server. The navigation tree on the left includes sections for Home, Configuration, Admin, Auth, Network, Policies, VPNS, Objects, Reports, and Wizards. The main configuration area is titled 'Configuration > Auth > Auth Servers > Edit' and shows the following fields:

Name	ACE		
IP/Domain Name	192.168.10.100		
Backup1	192.168.5.10		
Backup2			
Timeout	2 (0 to disable)		
Account Type	<input checked="" type="checkbox"/> Auth <input type="checkbox"/> L2TP <input type="checkbox"/> Admin <input type="checkbox"/> XAuth		
<input type="radio"/> RADIUS	Radius port	1645	Shared Secret
<input checked="" type="radio"/> SecurID	Client Retries	3	Client Timeout
	Authentication Port	5500	seconds
	Encryption Type	<input checked="" type="radio"/> DES <input type="radio"/> SDI	
	Use Duress	<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input type="radio"/> LDAP	LDAP Port	389	Common Name Identifier
			cn

Figure 2 DefineACEServers

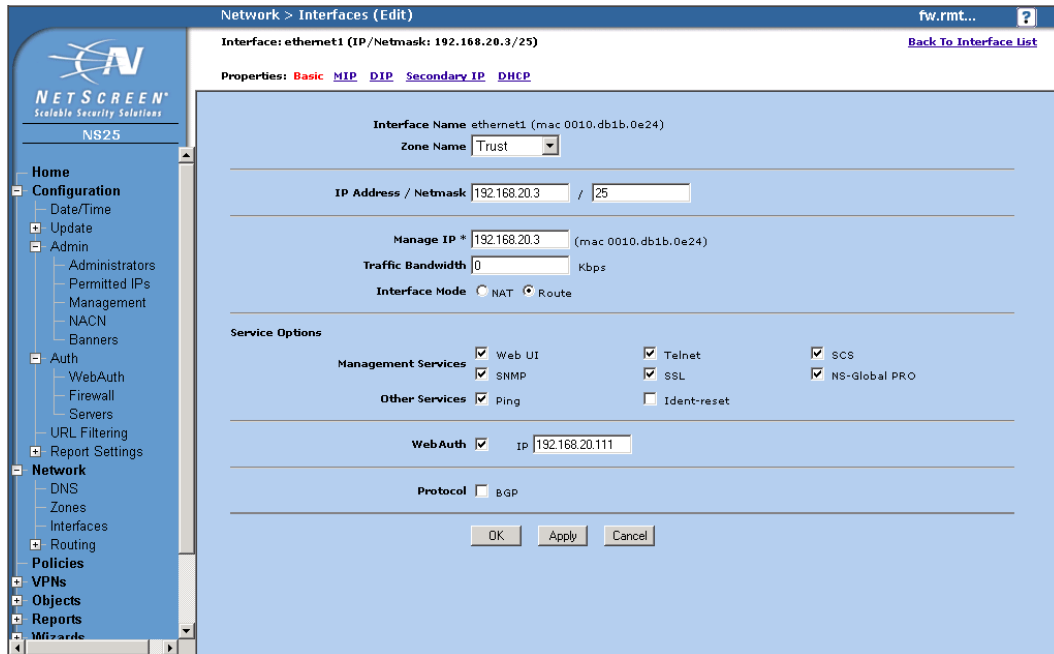
2. Once the firewall has been configured to use the RSA ACE/Servers as authentication servers, it is necessary to configure the WEB Auth access: Ensure that the ACE/Server is setup for "Auth" account types. Click on Configuration > Auth > Servers and make sure that SecurID is selected and that the Auth account type is checked:

The screenshot shows the NetScreen configuration interface for editing an authentication server. The breadcrumb path is 'Configuration > Auth > Auth Servers > Edit'. The server name is 'ACE'. The IP/Domain Name is '192.168.10.100', Backup1 is '192.168.5.10', and Backup2 is empty. The Timeout is set to '2' (0 to disable). The Account Type is 'Auth' (checked), with 'L2TP', 'Admin', and 'XAuth' unchecked. The RADIUS section is disabled. The SecurID section is active, with Client Retries set to '3', Client Timeout set to '5' seconds, and Authentication Port set to '5500'. The Encryption Type is 'DES' (selected) and 'SDI' is unselected. 'Use Duress' is set to 'No'. The LDAP section is disabled, with LDAP Port set to '389' and Common Name Identifier set to 'cn'.

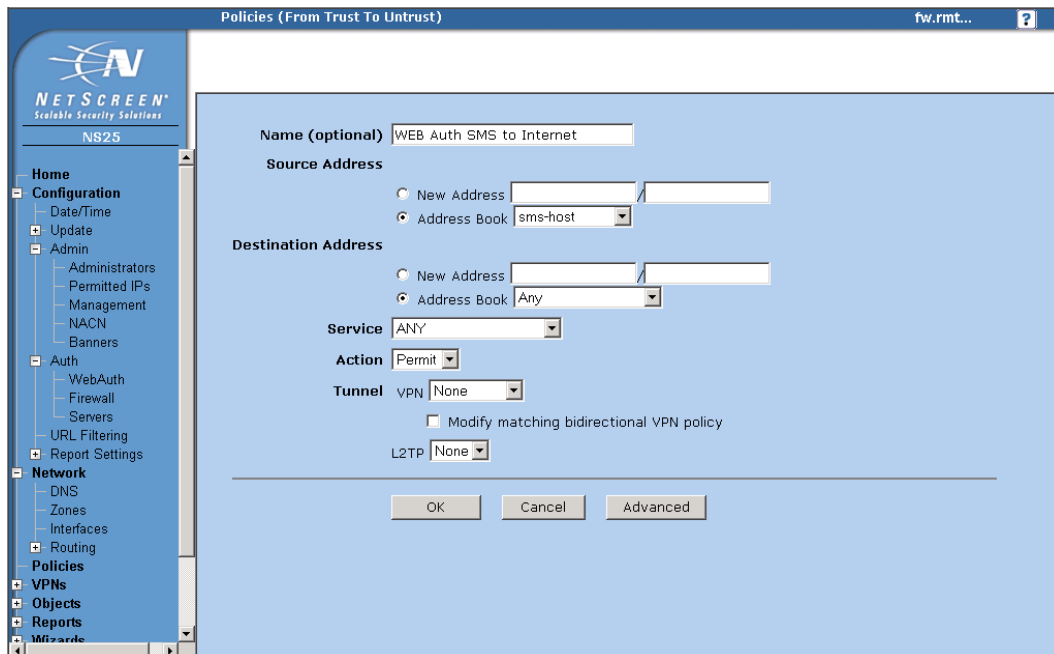
3. Enable WEB Auth on the NetScreen security appliance by clicking on Configuration > Auth > WEB Auth and specifying RSA ACE/Server defined in step one as the WEB Auth Server. You can specify a banner that the user will see upon successful authentication here as well:

The screenshot shows the NetScreen configuration interface for WebAuth. The breadcrumb path is 'Configuration > Auth > WebAuth'. The WebAuth Server is set to 'ACE'. The WebAuth Banner Setting section shows a text area for the Success Banner containing the text 'WebAuth Success'. There are 'Apply' and 'Cancel' buttons at the bottom.

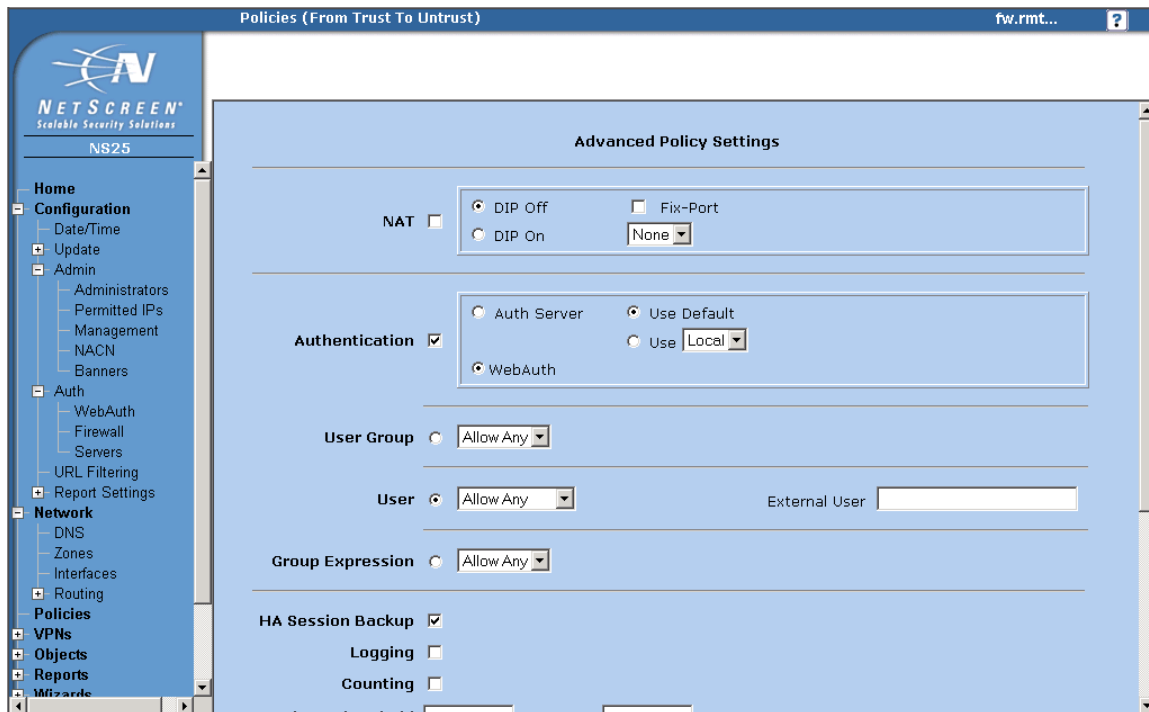
- Define an IP address on the firewall interface closest to the users you wish to authenticate. The IP address must be in the same subnet as that of the interface but it cannot be the same address as that of the interface. In this case we configure 192.168.20.111 as the WEB Auth IP address. The address of the interface is 192.168.20.3/25.



- Define a policy to permit traffic from the user to the protected resource. Here we define a policy to use WEB Auth for any traffic between "sms-host" (192.168.20.7) on the Security Zone: Trust Network and any address in the Untrust security zone. Begin as if you were defining any other policy



- Continue though by clicking on the “Advanced” button and checking the Authentication field and selecting the “WebAuth” radio button.



- Click the “Return” button and then the “OK” button to conclude.

Now the user on the host called “sms-host” must use RSA SecurID to authenticate himself before being permitted to reach any destination on the untrust security zone. The authentication takes place by the user on the sms-host pointing his WEB browser at 192.168.20.111 (or a URL containing a name that resolves to this address). The user provides his RSA SecurID user name and token code when prompted by the logon banner. Once authenticated, he can then proceed to access services on the untrust security zone.

Run-Time Auth Users

Run-Time Auth permits a user to be authenticated using an RSA SecurID token card before being permitted access to resources in a different security zone.

To get authenticated, the user attempts to access a service in another security zone that has been protected by a run-time authentication policy. An authentication dialog ensues during which the user enters their user ID and their RSA SecurID token. Once authenticated, the user can then reach services in the other security zone. The requirement to authenticate and the IP addresses and services protected by the authentication mechanism are defined in a NetScreen firewall policies. The user must be using a protocol that supports the authentication dialog: HTTP, (not HTTPS), Telnet, SSH, and FTP support run-time authentication.

RSA SecurID User authentication and RSA SecurID Admin authentication cannot be used simultaneously in a Netscreen Firewall. Run-Time Auth only provides support for Next Token Code or New PIN mode by the user using telnet.

- **NetScreen Configuration**

The NetScreen must be configured to use the ACE 5.0 Servers as Master and Slave (RSA ACE/Server 5 nomenclature is Primary and Replica, respectively). This is achieved by defining a new Server under “Configuration/Auth/Auth Servers” and clicking on new. Fill in the appropriate values for the RSA ACE/Servers on the resulting screen.

- “Name” is a label used in the NetScreen firewall to refer to the RSA ACE/Server – it is NOT the name associated with a DNS entry.
- The “IP/Domain Name” should be either the IP address or the FQDN of the primary RSA ACE/Server.
- The “Backup1” server should be either the IP or FQDN of the replica RSA ACE/Server.
- “Backup2” does not apply to RSA ACE/Server configuration.
- Click the button labeled “SecurID”. The default values will normally suffice unless the Authentication Port settings have been changed on the RSA ACE/Server. Leave “Encryption Type set as “DES”.

Configuration > Auth > Auth Servers > Edit fw.rmt...

NETSCREEN Scalable Security Solutions NS25

Home
Configuration
Date/Time
Update
Admin
Administrators
Permitted IPs
Management
NACN
Banners
Auth
WebAuth
Firewall
Servers
URL Filtering
Report Settings
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizard

Name ACE

IP/Domain Name 192.168.10.100

Backup1 192.168.5.10

Backup2

Timeout 2 (0 to disable)

Account Type Auth L2TP Admin XAuth

RADIUS Radius port 1645 Shared Secret

SecurID Client Retries 3 Client Timeout 5 seconds

Authentication Port \$500

Encryption Type DES SDI

Use Duress Yes No

LDAP LDAP Port 389 Common Name Identifier cn

Figure 3 DefineACE/Servers

- Once the firewall has been configured to use the RSA ACE/Servers as an authentication server, it is necessary to configure the Run-Time Auth access. Ensure that the RSA ACE/Server is setup for "Auth" account types. Click on Configuration > Auth > Servers and make sure that SecurID is selected and that the Auth account type is checked:

Configuration > Auth > Auth Servers > Edit

fw.rmt...

Name ACE

IP/Domain Name 192.168.10.100

Backup1 192.168.5.10

Backup2

Timeout 2 (0 to disable)

Account Type Auth L2TP Admin XAuth

RADIUS Radius port 1645 Shared Secret

SecurID Client Retries 3 Client Timeout 5 seconds

Authentication Port 5500

Encryption Type DES SDI

Use Duress Yes No

LDAP LDAP Port 389 Common Name Identifier cn

- Define a policy to permit traffic from the user to the protected resource. Here we define a policy to use run-time Auth for any traffic from any host in the untrust security zone to the "sms-host" (192.168.20.7) on the Trust security zone.

Policies (From Untrust To Trust)

fw.rmt...

Name (optional) Auth User Authentication

Source Address

New Address

Address Book Any

Destination Address

New Address

Address Book sms-host

Service ANY

Action Permit

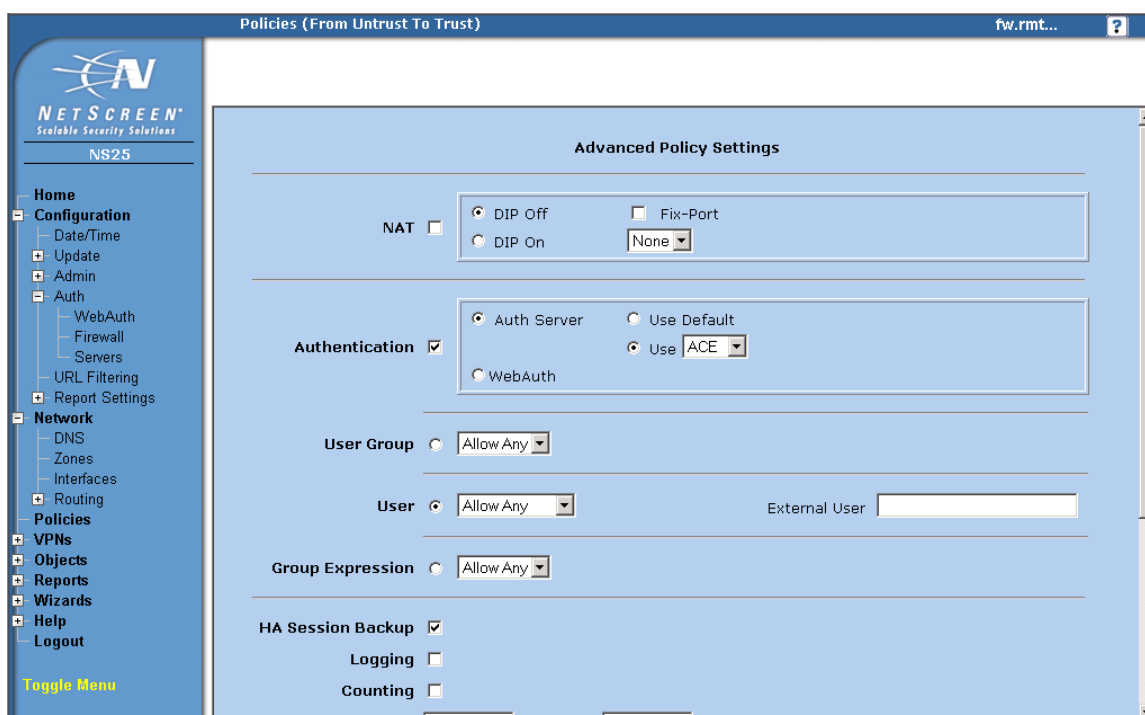
Tunnel VPN None

Modify matching bidirectional VPN policy

L2TP None

OK Cancel Advanced

- Continue building the policy by clicking on the “Advanced” button and checking the Authentication field and selecting the “Auth Server” radio button and the “Use” radio button. In the drop-down box, select the name that you gave to your RSA ACE/Server in step 1. Here we have named it “ACE” and so that is what has been selected in the drop-down box.



- Click the “Return” button and then the “OK” button to conclude.

Now any user in the untrust security zone must use RSA SecurID to authenticate himself before being permitted to reach the server called “sms-host” in the trust security zone. The authentication takes place by the user trying to access sms-host. If the user is using a protocol that supports the authentication dialog in run-time auth, he will get a log-in prompt. The user provides his RSA SecurID user name and token code when prompted by the logon banner. Once authenticated, he can then proceed to access services on the untrust security zone. The firewall will cache the user’s data that triggered the run-time auth. When the user successfully authenticates, the cached data will then be passed to the protected resource.

NetScreen Remote 8 Users

NetScreen Remote 8 permits a user to be authenticated using an RSA SecurID token card before being permitted access to resources across the VPN established between the NetScreen Remote client and the Corporate Network.

To get authenticated, the NetScreen Remote user attempts to access a service that has been protected by the NetScreen Remote software. The NetScreen Remote software then presents an authentication prompt to the remote user. An authentication dialog ensues during which the user enters their user ID and their RSA SecurID token. Once authenticated, the user can then reach services across the VPN. The requirement to authenticate and the IP addresses and services protected by the authentication mechanism are defined in a NetScreen firewall policies.

SecurID User authentication and SecurID Admin authentication cannot be used simultaneously in a Netscreen Firewall. NetScreen Remote 8 provides for full user New PIN and Next token code mode.

A. NetScreen Configuration

1. The NetScreen must be configured to use the RSA ACE 5.0 Servers as Master and Slave (RSA ACE/Server 5 nomenclature is Primary and Replica, respectively). This is achieved by defining a new Server under “Configuration/Auth/Auth Servers” and clicking on new. Fill in the appropriate values for the RSA ACE/Servers on the resulting screen.
 - “Name” is a label used in the NetScreen firewall to refer to the RSA ACE/Server – it is NOT the name associated with a DNS entry.
 - The “IP/Domain Name” should be either the IP address or the FQDN of the primary RSA ACE/Server.
 - “Backup1” server should be either the IP or FQDN of the replica RSA ACE/Server.
 - “Backup2” does not apply to ACE/Server configuration.
 - “Xauth” should be checked.
 - Click the button labeled “SecurID”. The default values will normally suffice unless the Authentication Port settings have been changed on the RSA ACE/Server. Leave “Encryption Type set as “DES”.

Configuration > Auth > Auth Servers > Edit

fw.rmt...

NETSCREEN
Scalable Security Solutions
NS25

Home
Configuration
Date/Time
Update
Admin
Auth
WebAuth
Firewall
Servers
URL Filtering
Report Settings
Network
DNS
Zones
Interfaces
Routing
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu

Name ACE

IP/Domain Name 192.168.10.100

Backup1 192.168.5.10

Backup2

Timeout 2 (0 to disable)

Account Type Auth L2TP Admin XAuth

RADIUS Radius port 1645 Shared Secret

SecurID Client Retries 3 Client Timeout 5 seconds
Authentication Port 5500

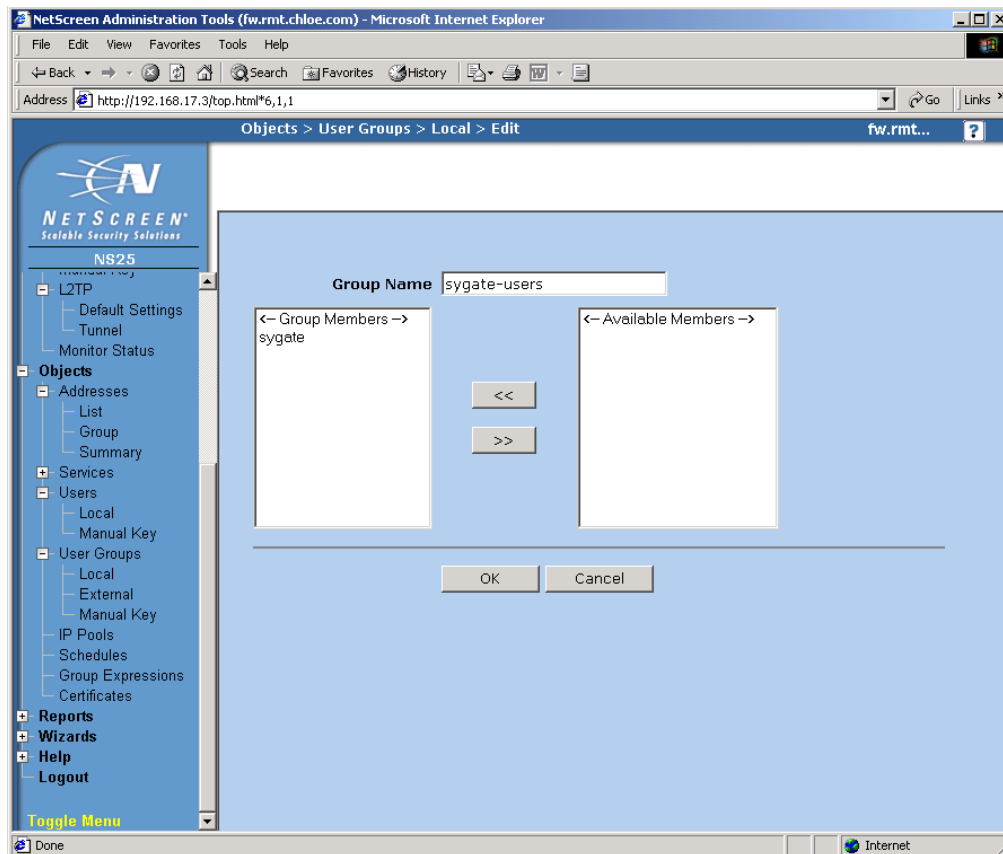
Encryption Type DES SDI

Use Duress Yes No

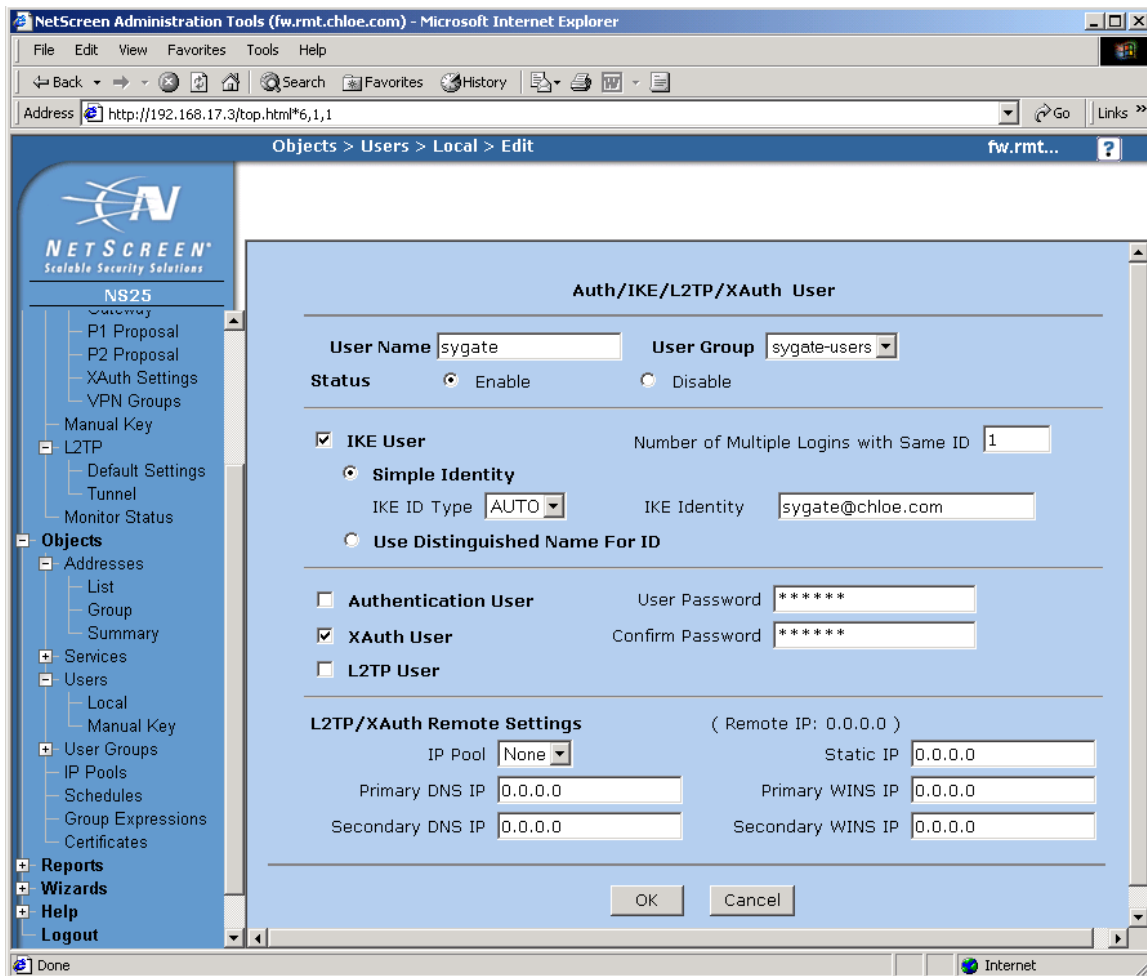
LDAP LDAP Port 389 Common Name Identifier cn

Figure 4 Define ACE/Servers

2. Once the firewall has been configured to use the RSA ACE/Servers as authentication servers, it is necessary to configure the NetScreen Remote user VPN access. Establish a User Group and create Users who will have VPN access with RSA SecurID authentication.



3. Enable the user, Choose IKE User, and select Xauth.



4. Create a VPN gateway. Under VPNs > AutoKey Advanced > Gateway select “new”. Name the gateway, select “custom” security level, select “dial-up user group” and select the group you defined earlier in the drop-down box “sygate-users”. Then click on the Advanced button.

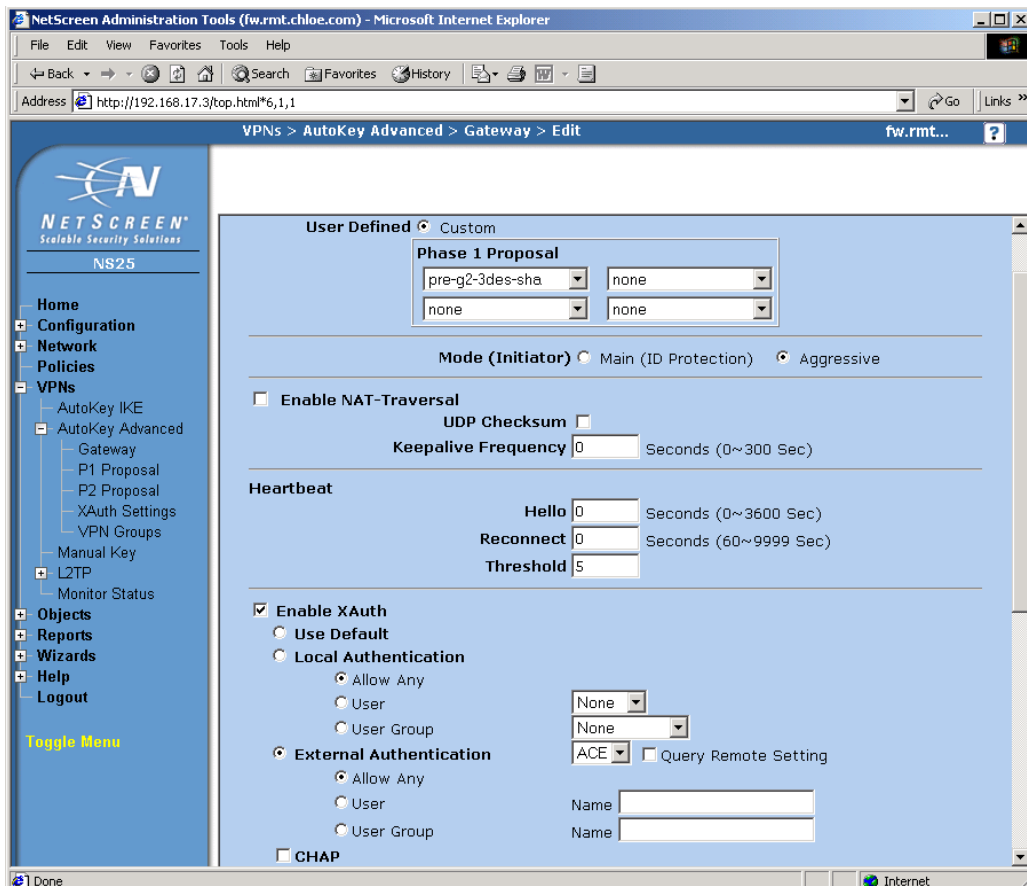
The screenshot shows the NetScreen NS100 configuration interface. The breadcrumb trail at the top reads "VPNs > AutoKey Advanced > Gateway > Edit". The left sidebar contains a navigation tree with categories: Home, Configuration, Network, Policies, VPNs (expanded), L2TP, Objects, Reports, and Wizards. Under the "VPNs" category, "AutoKey Advanced" is expanded to show "Gateway", "P1 Proposal", "P2 Proposal", "XAuth Settings", and "VPN Groups".

The main configuration area is titled "Gateway > Edit" and contains the following fields and options:

- Gateway Name:** SecurIDgateway
- Security Level:** Radio buttons for Standard, Compatible, Basic, and Custom (selected).
- Remote Gateway Type:** Radio buttons for Static IP Address, Dynamic IP Address, Dialup User, and Dialup User Group (selected).
 - Static IP Address:** IP Address: 0.0.0.0
 - Dynamic IP Address:** Peer ID: [empty]
 - Dialup User:** User: None
 - Dialup User Group:** Group: RSASecurID
- Preshared Key:** [masked with asterisks]
- Local ID:** [empty] (optional)
- Outgoing Interface:** untrust

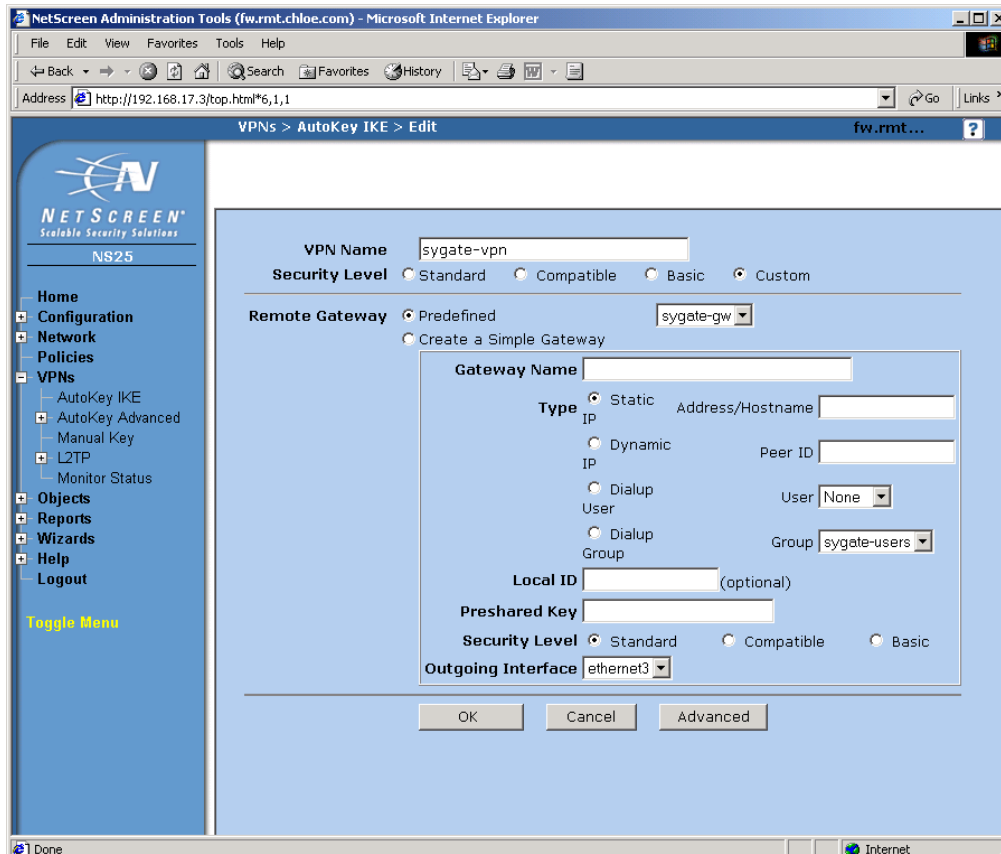
At the bottom of the configuration area are three buttons: "OK", "Cancel", and "Advanced".

- Continue building the VPN Gateway under “Advanced” by clicking on “user Defined” and selecting a series of Phase 1 Proposals. Check the Enable Xauth box. Select the External Authentication radio button and select the name given to your RSA ACE/Server.

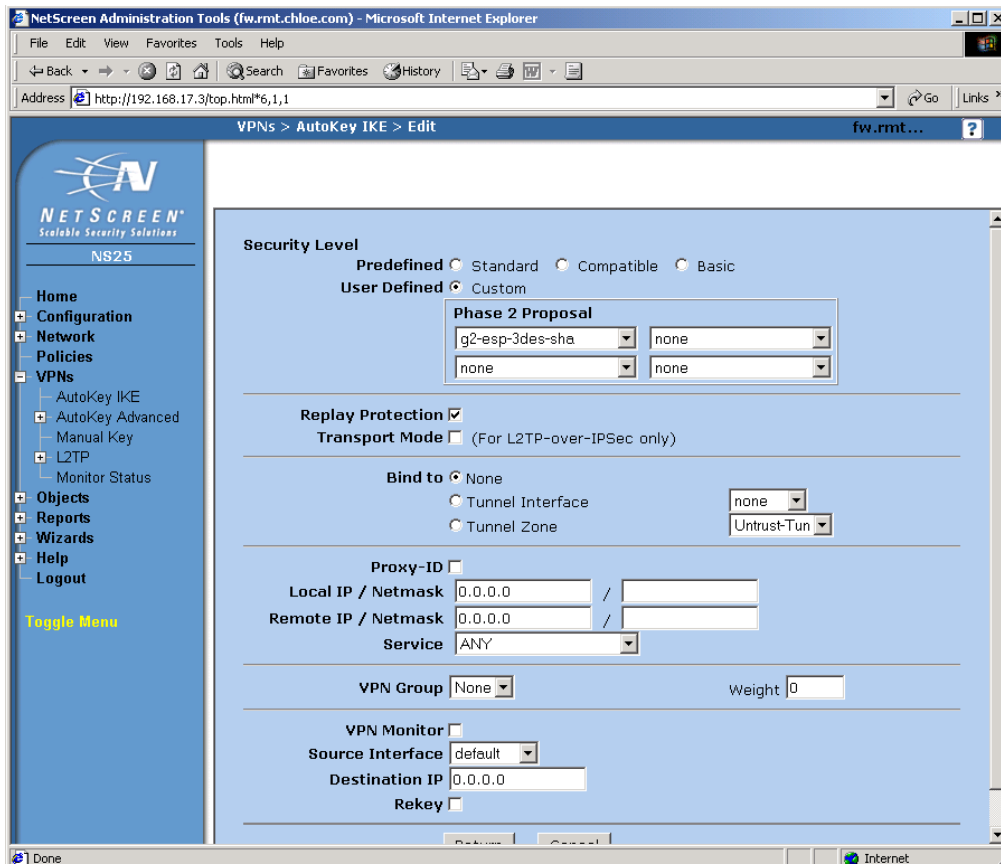


- Click the “Return” button and then the “OK” button to conclude building the Gateway

- Click VPN > AutoKey IKE. Click on the “New” button. Define a new VPN here by giving it a name, selecting “custom” for the security level, and choosing Predefined for the Remote Gateway and selecting the gateway you just defined from the drop-down box. Click on the “Advanced” button.



- Continue defining the VPN under “Advanced” by defining a Phase 2 proposal. You can turn on replay protection if you wish.



9. Create a Policy from Untrust to Trust. The source will be from the address book entry "Dial-Up VPN" and the Destination will be the trusted network. Under Action, choose tunnel. For the tunnel, choose the tunnel you defined in the prior step.

The screenshot shows the NetScreen NS100 configuration interface for creating a policy. The window title is "Policies (From Untrust To Trust)" and the user is logged in as "ph021". The left sidebar contains a navigation menu with options: Home, Configuration, Network, Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. A "Toggle Menu" link is also present. The main configuration area is titled "Name (optional)" and contains the following fields:

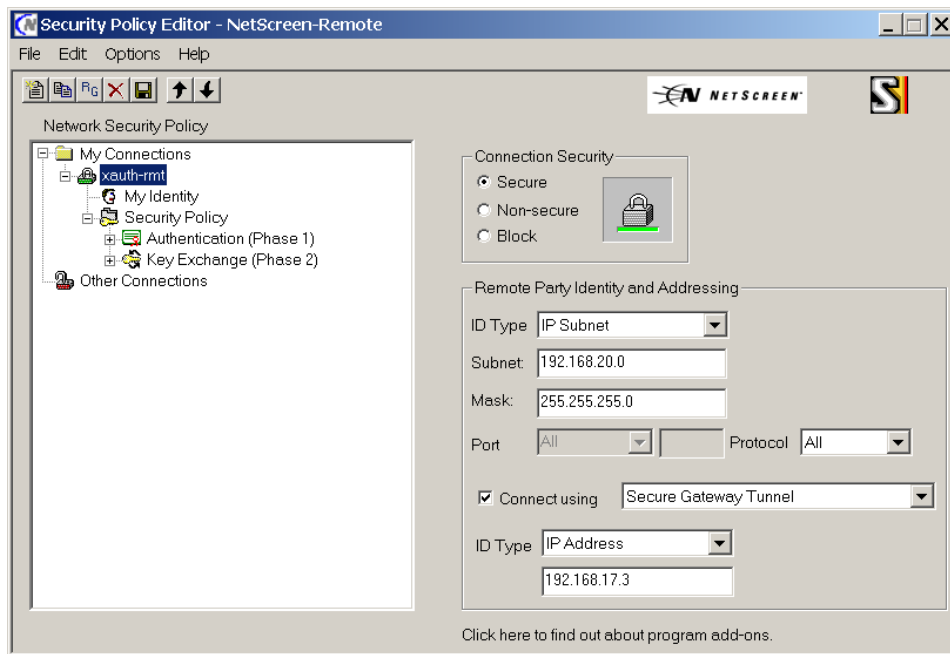
- Name (optional):** SecurIDPolicy
- Source Address:** Radio buttons for "New Address" (empty) and "Address Book" (selected). The "Address Book" dropdown is set to "Dial-Up VPN".
- Destination Address:** Radio buttons for "New Address" (empty) and "Address Book" (selected). The "Address Book" dropdown is set to "Trusted Network".
- Service:** ANY
- Action:** Tunnel
- Tunnel:** VPN, with a dropdown menu showing "rsaSecurIDvpn" selected.
- Modify matching bidirectional VPN policy
- L2TP:** None

At the bottom of the configuration area are three buttons: "OK", "Cancel", and "Advanced".

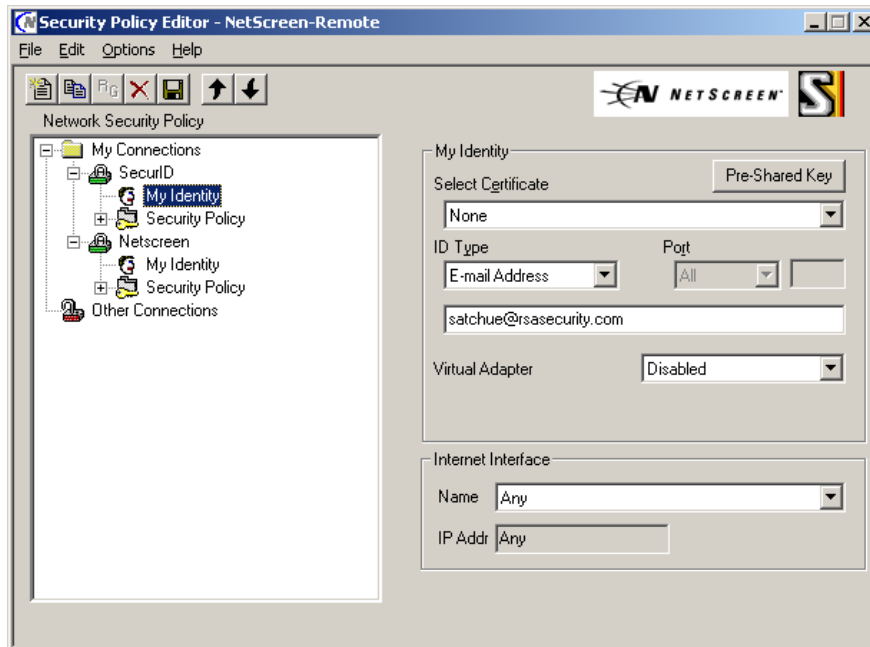
B. Netscreen Remote 8

For the NetScreen Remote 8 Client, a corresponding VPN configuration must be made. Once the NetScreen Remote 8 client has been installed, bring it up for editing by double-clicking the NetScreen Remote icon in the Microsoft Windows task bar.

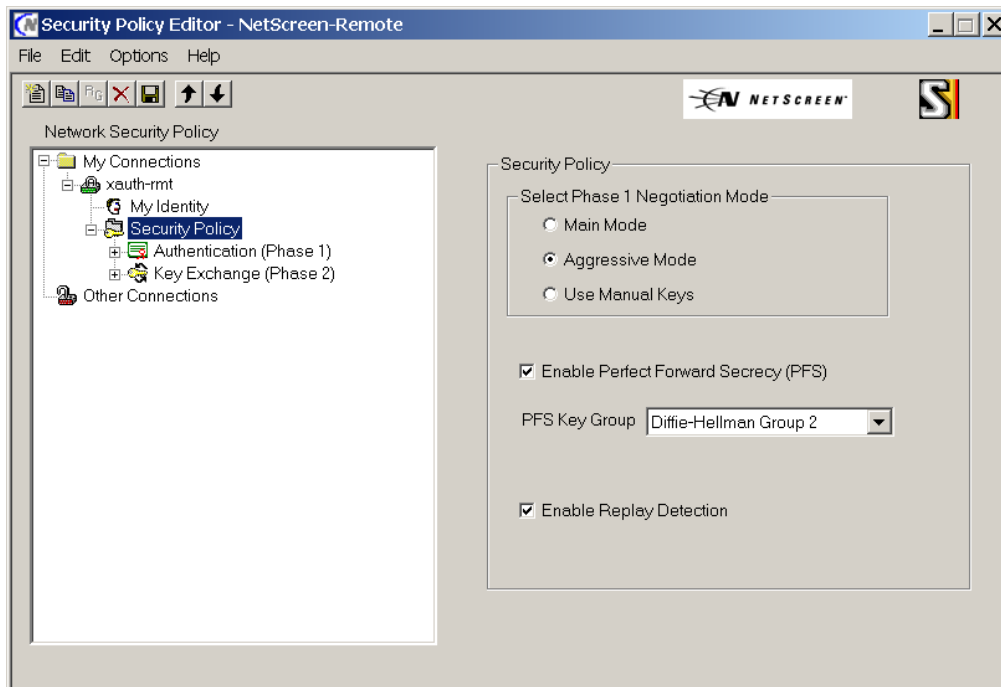
2. Create a new connection under “My Connections”. Connection security can be set to Secure. ID type should be “IP Subnet” in this case. The subnet entered is that of the trusted network – in this case 192.168.20.0 with at 255.255.255.0 subnet mask. Check connect using and chose Secure Gateway Tunnel 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 – in this case 192.168.17.3.



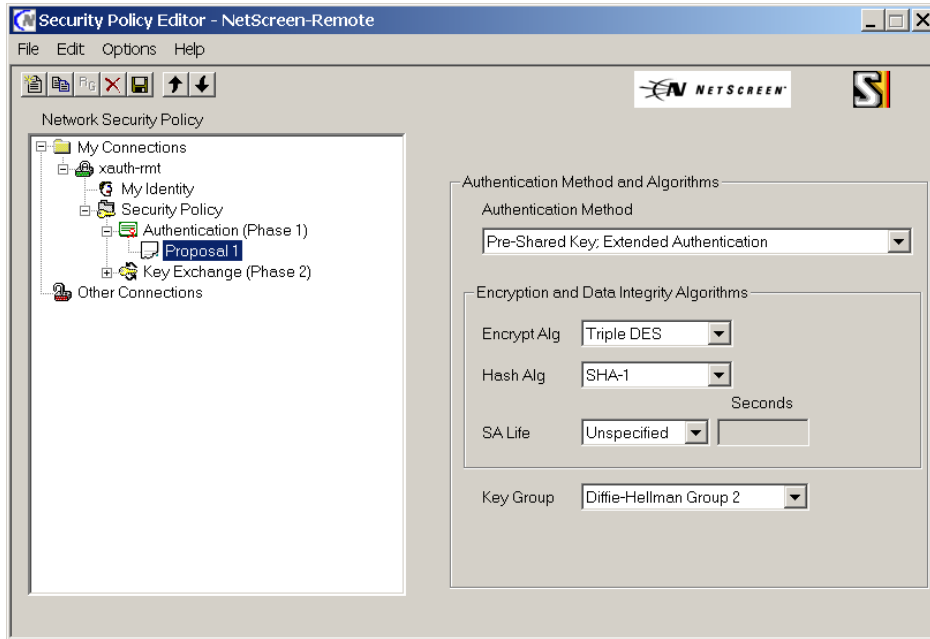
3. Under My Identity set the ID type to e-mail address and enter the same e-mail address set in part A step 3. Also set the Pre-Shared Key to match the value set in part A step 3.



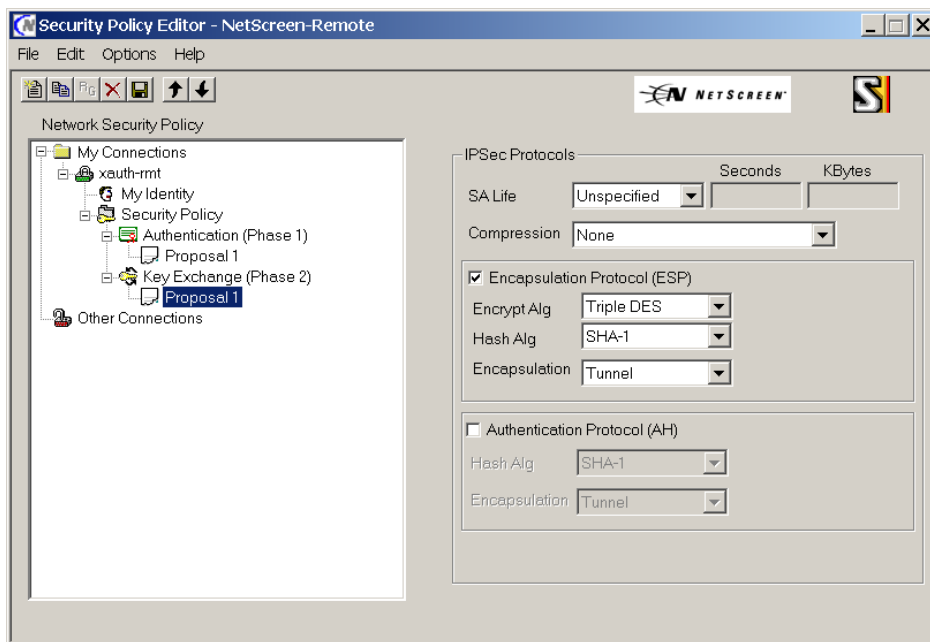
4. In the security policy tree under My Connections/Your Policy Goes Here/Security Policy, Select "Aggressive Mode", Enable Perfect Forward Security if you did so on the firewall, chose Diffie-Hellman Group 2 for the PFS key group and enable replay protection.



- Under Authentication, ensure that your setting match that in the firewall – in this example we are using Pre-shared Key, Extended Authentication, 3DES, SHA-1. We have not specified a lifetime on the client so we will be using the default lifetime on the firewall. Diffie-Hellman Group 2 is used for the key group. Xauth needs Phase 1 of IKE to complete successfully before querying the user for their User ID and Password (in this case it will be a RSA SecurID PIN + Token) hence we needed to setup Phase 1.

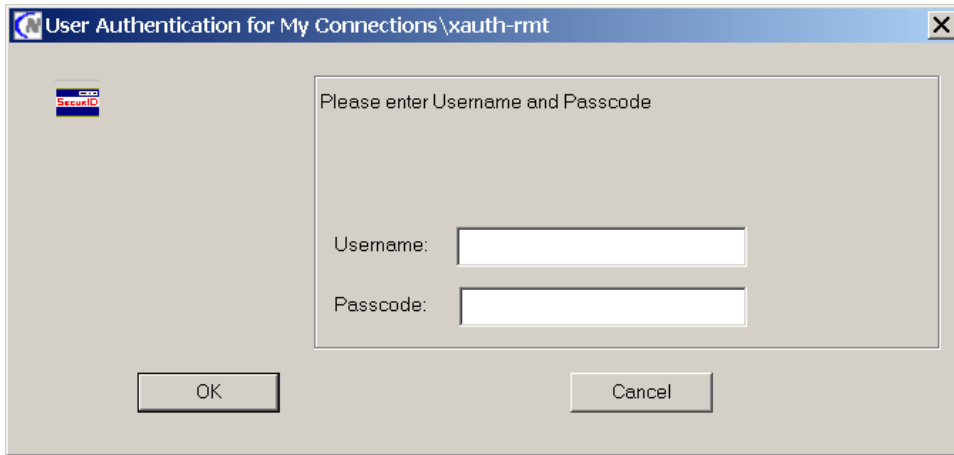


- Under Key Exchange (Phase 2), Select ESP and ensure that your phase 2 selections match what was established in the firewall – in this example we use ESP with 3DES, SHA-1, and Tunnel Encapsulation.



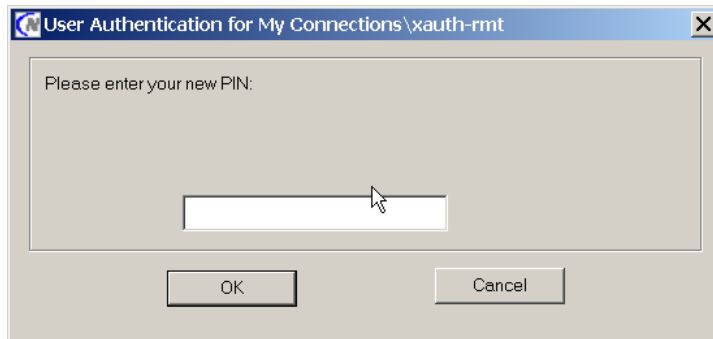
7. Save your newly created security policy.

If everything has been configured correctly, a “Ping” to any host the trusted network should bring up an authentication dialog:

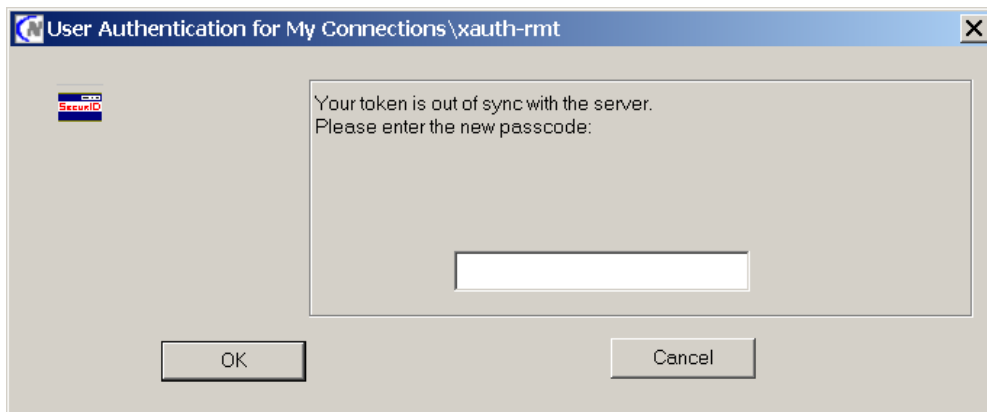


The user should enter their User ID and RSA SecurID PIN at this point and click the “OK” button.

New PIN prompt.



Next Token code prompt.



7. Certification Checklist

Date Tested: March 26, 2003

Product	Tested Version
ACE/Server	5.1
Appliance	NS-100a
ScreenOS	4.0.0r8.0
Netscreen Remote	8

Test	VPN	Telnet	Other
1st time auth. (node secret creation)	P	P	P
New PIN mode:			
System-generated			
Non-PINPAD token	P	P	N/A
PINPAD token			N/A
User-defined (4-8 alphanumeric)			
Non-PINPAD token	P	P	N/A
Password	P	P	N/A
User-defined (5-7 numeric)			
Non-PINPAD token	P	P	N/A
PINPAD token	P	P	N/A
SoftID token	P	P	N/A
Deny 4 digit PIN	P	P	N/A
Deny Alphanumeric	P	P	N/A
User-selectable			
Non-PINPAD token	P	P	N/A
PINPAD token	P	P	N/A
PASSCODE			
16 Digit PASSCODE	F*	F*	F*
4 Digit Password	P	P	N/A
Next Tokencode mode			
Non-PINPAD token	P	P	N/A
PINPAD token	P	P	N/A
Failover	P	P	P
User Lock Test (ACE Lock Function)	N/A*	N/A*	N/A*
No ACE/Server	P	P	P

SWA

N/A (N/A=Non-available function)

* See Known Issues

8. Known Issues

1. VPN access only allows 15 Character PASSCODES. Firewall authentication only allows 14 character PASSCODES
2. The Netscreen appliance only supports a Master/Slave configuration at this time.
3. Admin user configurations do not provide any mechanism for the administrator to perform New Pin or Next Tokencode mode via the NetScreen firewall
4. WEB Auth does not provide any mechanism for the user to perform Next Token code or New PIN mode.

Appendix A – Notes.

1. L2TP over IPSec using RSA SecurID server is only supported on ScreenOS 4.0.0 or higher.
2. In ScreenOS 4.0.0, authentication of users can be grouped together if using either external Radius server, or using the local database. However, the User Group functionality is not supported for LDAP and SecurID.
3. ScreenOS 1.6 did not support New Pin or Next Tokencode Mode in SecurID. Upgrade to ScreenOS 2.0 or higher for enhanced SecurID support.

Appendix B - Troubleshooting

How to debug SecurID authentication issues from within Netscreen:

From the command line interface (CLI):

```
debug secur 2 [Enter]
debug ace 2 [Enter]
debug auth 2 [Enter]
```

Run the normal authentication traffic, so the NetScreen can capture the information in the debugs. Capture the information by entering the following command:

```
get dbuf stream [Enter]
```

To turn off the debugs:

```
debug secur 0 [Enter]
debug ace 0 [Enter]
debug auth 0 [Enter]
```