



RSA SecurID Ready Implementation Guide

Last Modified: April 06, 2006

Partner Information

Product Information	
Partner Name	Nortel Networks
Web Site	www.nortelnetworks.com
Product Name	VPN Gateway 3050
Version & Platform	5.1.6.3
Product Description	The Nortel Networks VPN Gateway 3050 is a remote access security solution that extends the reach of enterprise applications and resources to remote users. The gateway performs on-the-fly content transformation to instantly convert most intranet resources into externally-viewable, secure HTML pages and employs an advanced network address and port translation (NAPT) utility to build SSL-secured VPN tunnels for client/server communications
Product Category	Perimeter Defense (VPN, Firewalls & Intrusion Detection)



Solution Summary

The Nortel Networks VPN Gateway 3050 is a remote access security solution that extends the reach of enterprise applications and resources to remote employees, partners, and customers. By using the native capability of widely deployed Web browsers, the SSL VPN Gateway offers a convenient clientless alternative for securely provisioning resources for remote users, without the need to install and manage client tunneling software on their PCs.

Due to the clientless nature of this solution, Strong two factor authentication is essential to ensure the identity of users connecting to your Enterprise from the internet. For this reason, Nortel Networks VPN Gateway 3050 provides support for the RSA Authentication Manager as a method of strong authentication for users using RSA SecurID Authentication.

For enterprises maintaining IPsec VPN environments, the Nortel VPN Gateway 3050 provides a new level of deployment flexibility and end-user support by incorporating IPsec VPN client termination to remove the network administrator's challenge of managing multiple devices to deliver both types of remote access service.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID, RADIUS
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes
Location of Node Secret on Agent	Within RSA Server configuration (See Appendix)
RSA Authentication Agent Host Type	Communication server
RSA SecurID User Specification	Designated users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: Nortel VPN Gateway 3050	
Firmware Version	5.1.6.3

Hardware Platform	
Platform	Required Patches
VPN 3050, ASA 310, ASA 410, ASA 310 FIPS	N/A

Additional Software Requirements	
Application	Additional Patches
Internet Explorer	5.0, 5.5 and 6.0

Agent Host Configuration

To facilitate communication between the Nortel VPN Gateway and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database and the RADIUS server database if using RADIUS. The Agent Host record identifies the Nortel VPN Gateway within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the Nortel VPN Gateway as Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Nortel VPN Gateway will occur.

 **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 Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product 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.

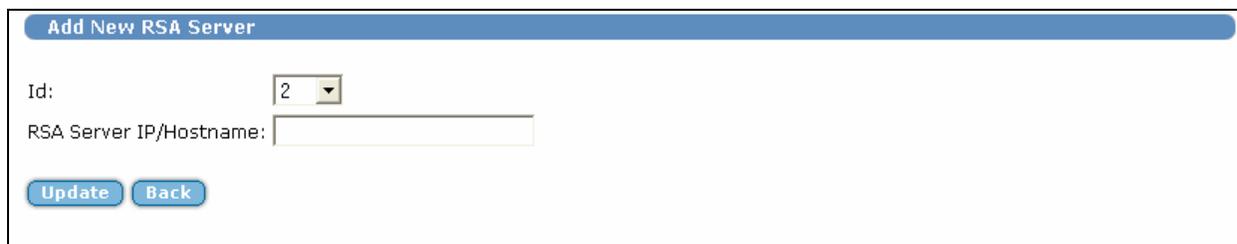
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Nortel VPN Gateway 3050 Agent configuration

Administrative tasks can be performed in the Command Line Interface (CLI) as well as the Web Administration GUI. All configuration steps and screenshots in this guide will refer to GUI administration. Please refer to Nortel Administrative documentation for more complete details on CLI and GUI Administration tasks.

Configure the RSA Server record

1. Open the Management Interface (MIP) of the Nortel VPN Gateway using a web browser. Authenticate with administrative user account and select the **Normal** administrative task set.
2. From the **SSL-VPN** admin menu select **Administration > RSA Servers** item.
3. Click the **Add New Server** button and complete the form.
4. Click **Apply** to commit changes to the IOS configuration.



 **Note: You must Update and Apply the RSA Server Group entry before you import the sdconf.rec file**

5. To import your sdconf.rec file you will return to the **RSA Servers** menu and modify the entry for the sdconf.rec file you will be adding.



6. Click **import** to upload the sdconf.rec file and then click **Apply** changes to the IOS configuration.

Creating and Configuring a SecurID User Group

1. From the admin console, expand **VPN Gateways > Group Settings > Groups**.
2. Click on the button **Add New Group**.
3. Fill out the form with the desired group name, user type and description.
4. Click **Update** and then **Apply** to add the new group to the configuration.

The screenshot shows the 'Groups' configuration page. At the top, there is a 'Domain Number' dropdown set to '1' and a 'Refresh' button. Below this is a 'Default Group' section with a dropdown set to '<unselected>' and an 'Update' button. The main section is a table titled 'Groups' with columns: Id, Name, User Type, Comment, and Actions. The table contains two rows: 1. Password Users, advanced, Users Authenticated by Static Passwords; 2. SecurID Users, advanced, Users Authenticated by RSA SecurID. Each row has 'Modify' and 'Delete' buttons. At the bottom of the table is an 'Add New Group' button.

Id	Name	User Type	Comment	Actions
1	Password Users	advanced	Users Authenticated by Static Passwords	Modify Delete
2	SecurID Users	advanced	Users Authenticated by RSA SecurID	Modify Delete

5. From the **Groups** menu on the administration console, select **Access List**.
6. Select the domain number your RSA SecurID user group resides in and then choose the RSA SecurID user group from the group list.
7. Create an appropriate Access list based on your organizations configuration. In the example below you will see we have created a generic rule allowing all access for authenticated RSA SecurID users.

The screenshot shows the 'Access Rules' configuration page. At the top, there is a 'Domain Number' dropdown set to '1' and a 'Refresh' button. To the right is a 'Group' dropdown set to '2 SecurID Users' and a 'Refresh' button. Below this is a table titled 'Access Rules' with columns: Id, Network, Service, Application, Allow, Comment, and Actions. The table contains one row: 1, *, *, *, accept, [empty], [Delete]. Below the table are 'Add Rule' and 'Update' buttons. A note at the bottom states: 'Note: You must Update in order to save changes.'

Id	Network	Service	Application	Allow	Comment	Actions
1	*	*	*	accept		Delete

8. Click **Update** to apply the Access rules.
9. Configure the user group for any necessary links or VPN Settings as required.
10. Click **Update** and then **Apply** to add the new information to the IOS configuration.

The screenshot shows the 'Apply Results' page. It features a large green text message: 'Apply Succeeded'. Below the message is a 'Back' button.

Configuring the RSA SecurID Authentication Servers

1. From the admin console, expand **VPN Gateways > Authentication > Auth Servers**.
2. Enter information for the Auth Server such as Name and Display Name. The Authentication Mechanism will be **RSA**. Then click **continue** to complete additional RSA SecurID authentication options.
3. For RSA Server Name select the name of the RSA Authentication Manager you configured in the first section of this guide. RSA Group will refer to the user group associated with users challenged by the RSA Authentication Manager.

Modify RSA Server(s)

VPN: 1
Auth Id: 2
Name: RSA SecurID
Display Name: RSA SecurID Authentication
Domain Name:

Group Authentication Servers:

Available		Selected
1 local	>> <<	

Secondary Authentication Server: <unset>
RSA Server IP/Hostname: 10.100.50.37
RSA Group: SecurID Users

Update **Back**

4. Click **Update** and then **Apply** to add the new information to the IOS configuration.

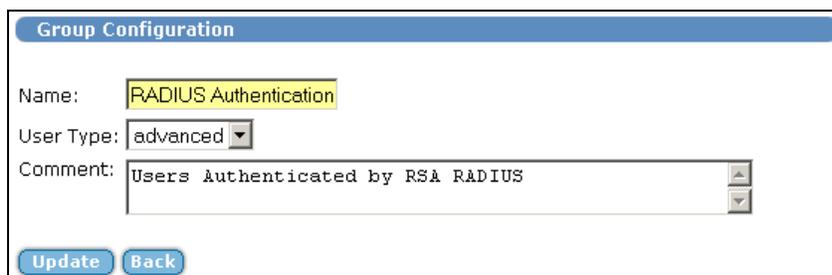
Apply Results

Apply Succeeded

Back

Creating and Configuring a RADIUS User Group

1. From the admin console, expand **VPN Gateways > Group Settings > Groups**.
2. Click on the button **Add New Group**. Fill out the form with the desired group name, user type and description.

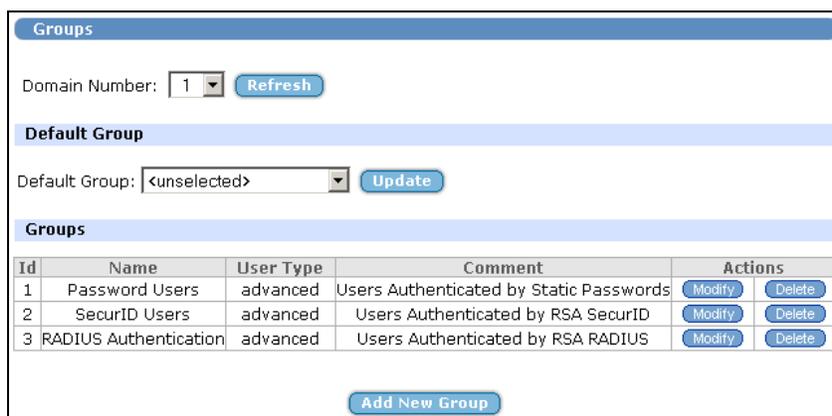


The 'Group Configuration' form contains the following fields:

- Name: RADIUS Authentication
- User Type: advanced
- Comment: Users Authenticated by RSA RADIUS

Buttons: Update, Back

3. Click **Update** and then **Apply** to add the new group to the configuration.



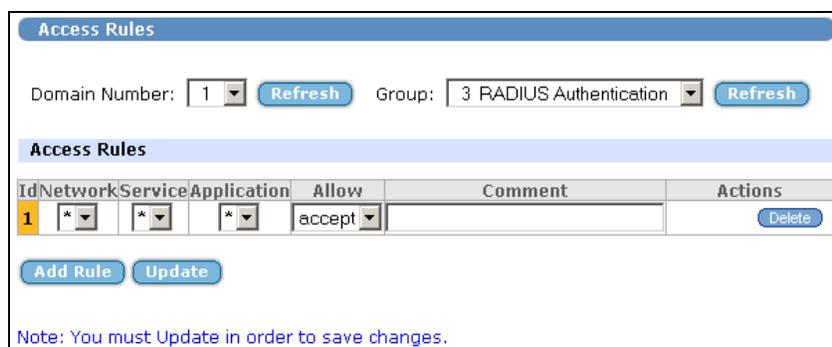
The 'Groups' screen includes:

- Domain Number: 1 (with Refresh button)
- Default Group: <unselected> (with Update button)
- A table of existing groups:

Id	Name	User Type	Comment	Actions
1	Password Users	advanced	Users Authenticated by Static Passwords	Modify Delete
2	SecurID Users	advanced	Users Authenticated by RSA SecurID	Modify Delete
3	RADIUS Authentication	advanced	Users Authenticated by RSA RADIUS	Modify Delete

Buttons: Add New Group

4. From the **Groups** menu on the administration console, select **Access List**.
5. Select the domain number your RSA RADIUS user group resides in and then choose the RSA RADIUS user group from the group list.
6. Create an appropriate Access list based on your organizations configuration. In the example below you will see we have created a generic rule allowing all access for authenticated RSA RADIUS users.



The 'Access Rules' screen includes:

- Domain Number: 1 (with Refresh button)
- Group: 3 RADIUS Authentication (with Refresh button)
- An 'Access Rules' table:

Id	Network	Service	Application	Allow	Comment	Actions
1	*	*	*	accept		Delete

Buttons: Add Rule, Update

Note: You must Update in order to save changes.

7. Click **Update** to apply the Access rules.
8. Click **Update** and then **Apply** to add the new information to the IOS configuration.

Configuring the RADIUS Authentication Servers

1. From the admin console, expand **VPN Gateways > Authentication > Auth Servers**.
2. Enter information for the Auth Server such as Name and Display Name. The Authentication Mechanism will be **RADIUS**. Then click **continue** to complete additional authentication options.
3. Enter 1872 as Vendor Id.
4. Enter 1 as Vendor type.
5. Leave timeout as default of 10 seconds.

Modify RADIUS Server(s)

VPN: 1
Auth Id: 3
Name:
Display Name:
Domain Name:

Group Authentication Servers:

Available	Selected
1 local	

Secondary Authentication Server:

Vendor Id:
Vendor Type:
Vendor Id for VPN Id:
Vendor Type for VPN Id:
Timeout: (seconds)

6. Session Timeout can be left in default state of disabled.
7. Add RADIUS Servers by clicking the **Add Server** button. Enter the IP Address, port and shared secret information for each RSA RADIUS server.

 **Note:** You can add a maximum of three RSA RADIUS servers to this authentication server list.

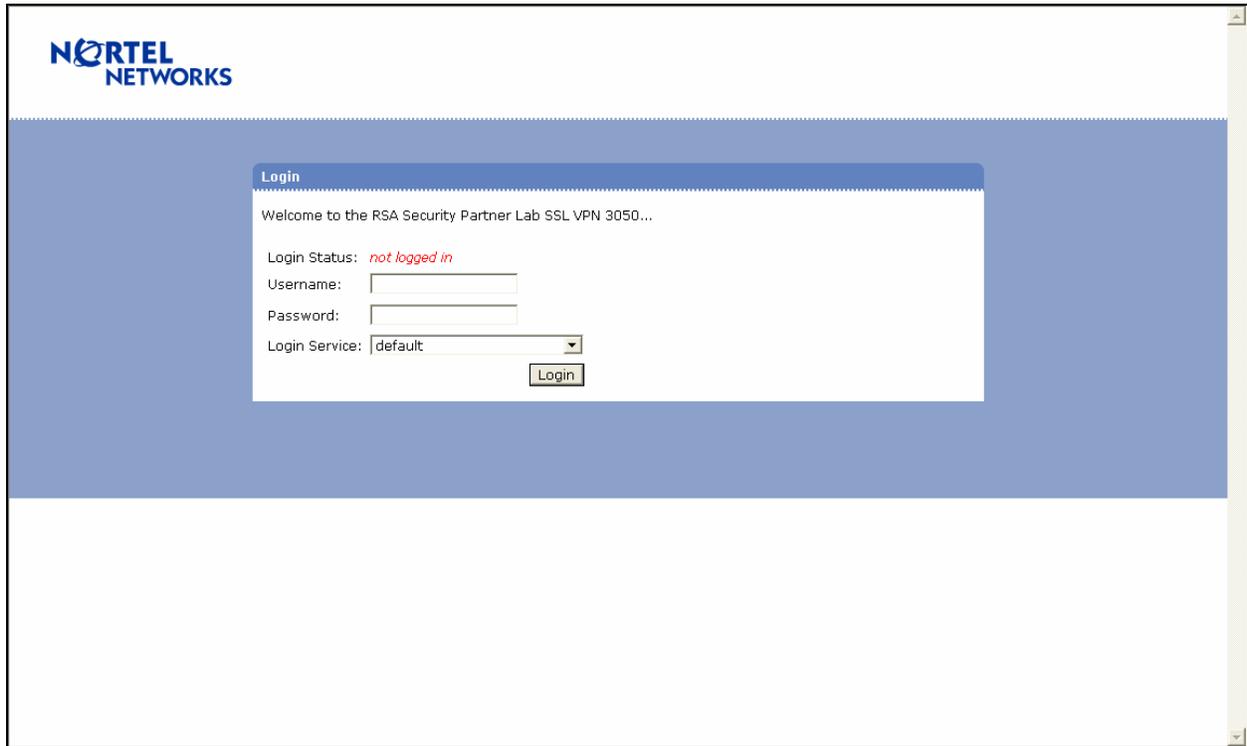
RADIUS Servers

IP Address	Port		Actions
10.100.50.37	1812	↓	<input style="border: none; background: none; border: 1px solid #4a7ebb; padding: 2px 5px;" type="button" value="Modify"/> <input style="border: none; background: none; border: 1px solid #4a7ebb; padding: 2px 5px;" type="button" value="Delete"/>
10.100.50.36	1812	↓ ↑	<input style="border: none; background: none; border: 1px solid #4a7ebb; padding: 2px 5px;" type="button" value="Modify"/> <input style="border: none; background: none; border: 1px solid #4a7ebb; padding: 2px 5px;" type="button" value="Delete"/>
10.100.50.35	1812	↑	<input style="border: none; background: none; border: 1px solid #4a7ebb; padding: 2px 5px;" type="button" value="Modify"/> <input style="border: none; background: none; border: 1px solid #4a7ebb; padding: 2px 5px;" type="button" value="Delete"/>

8. Click **Update** and then **Apply** to add the new information to the IOS configuration.

Testing the configuration

1. Open a web browser and point to the portal address. For user credentials enter a SecurID username and Passcode. From the **Login Service** list select your RSA SecurID or RSA RADIUS challenge group. Click **Login** to authenticate and enter the Portal Server.



NORTEL NETWORKS

Login

Welcome to the RSA Security Partner Lab SSL VPN 3050...

Login Status: *not logged in*

Username:

Password:

Login Service: default

 **Note: The user name does not need to exist on the VPN Gateway 3050 in order to be authenticated. The VPN Gateway 3050 will pass off authentication to the RSA Authentication Manager as a trusted authentication source.**

Certification Checklist

Date Tested: January 23, 2006

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003 Server
VPN Gateway 3050	5.1.6.3	IOS Router

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Domain Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

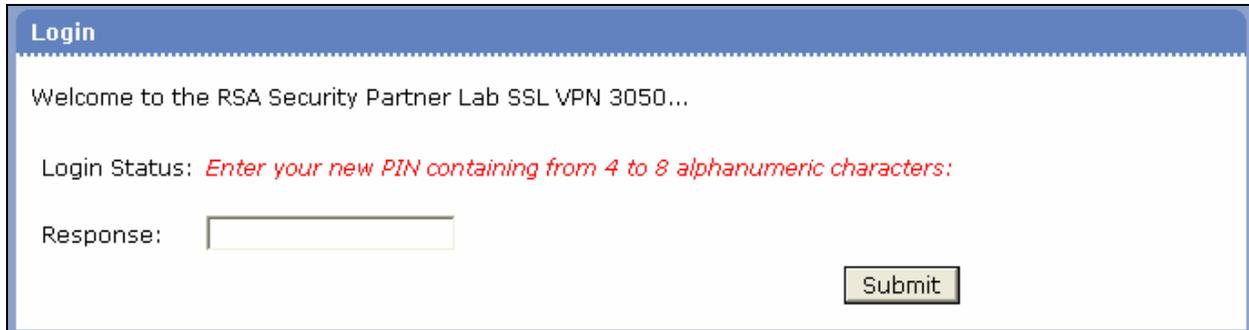
BSD

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

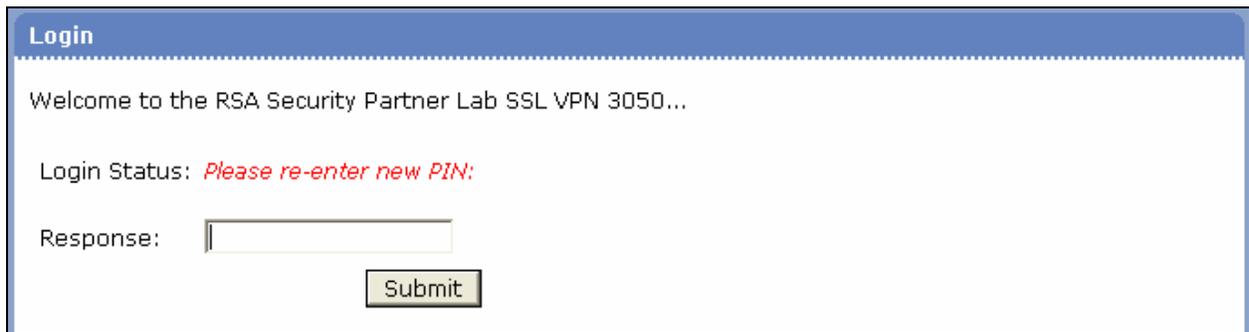
PIN Rejection: When a PIN is rejected by the Authentication Manager Server the user is questioned by the client to try a different PIN but the program flow is not intuitive.

1. The user first authenticates using either Token or Password. The user is next prompted to create a new PIN.



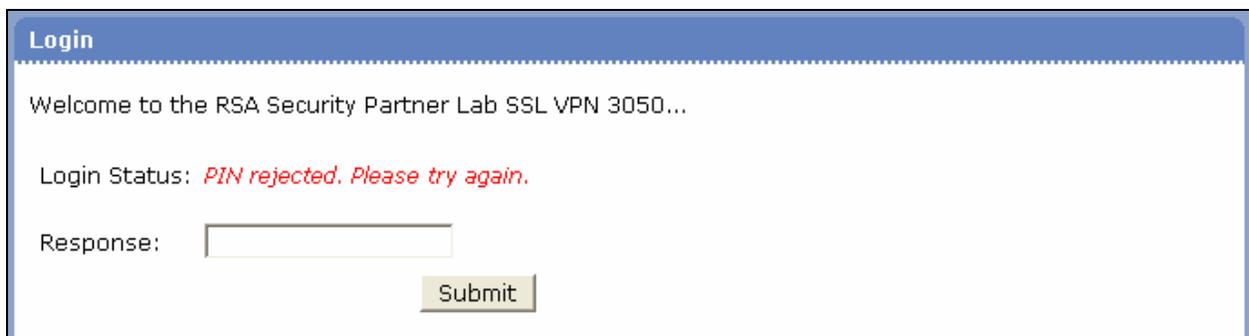
The screenshot shows a web browser window with a blue header bar containing the word "Login". Below the header, the text reads "Welcome to the RSA Security Partner Lab SSL VPN 3050...". The "Login Status:" field displays the message "Enter your new PIN containing from 4 to 8 alphanumeric characters:". Below this, the "Response:" label is followed by an empty text input field. A "Submit" button is located at the bottom right of the form area.

2. The user must re-enter the new PIN to validate input from the previous step.



The screenshot shows the same web browser window as in the previous step. The "Login Status:" field now displays the message "Please re-enter new PIN:". The "Response:" label is followed by an empty text input field. A "Submit" button is located at the bottom right of the form area.

3. If rejected, the client displays the question to the user with an empty text box for input.



The screenshot shows the same web browser window as in the previous steps. The "Login Status:" field now displays the message "PIN rejected. Please try again.". The "Response:" label is followed by an empty text input field. A "Submit" button is located at the bottom right of the form area.

- The client will accept any input by the user and then prompt for a new PASSCODE to restart the authentication process.

Login

Welcome to the RSA Security Partner Lab SSL VPN 3050...

Login Status: *Please Enter Passcode*

Response:

- The user then inputs a valid PASSCODE.

Appendix

Delete Node Secret

To remove the Node Secret from the Nortel VPN Gateway 3050, navigate to **SSL-VPN > Administration > RSA Servers** and click on the button labeled **Remove Node Secret**.

The screenshot shows the web interface of a Nortel VPN Gateway 3050. The interface is divided into several sections:

- Navigation Menu (Left):** A tree view showing the hierarchy: SSL-VPN > Administration > RSA Servers. Other options include Quick Setup, Create Portal Links, Cluster, Network, Certificates, SSL Offload, VPN Gateways, Operation, Monitor, Statistics, Users, Access List, Telnet-SSH, SSH Keys, Web, SNMP, RADIUS, and RSA Servers (highlighted).
- Page Header:** Includes tabs for SETUP, NORMAL, and EXPERT, and a History dropdown menu showing 'Administration->RSA Servers'.
- Main Content Area:**
 - Modify RSA Server:** A section with a blue header. It contains two input fields: 'Id' with the value '1' and 'RSA Server IP/Hostname' with the value '10.100.50.37'. Below these fields are three buttons: 'Update', 'Remove Node Secret' (which is being pointed to by a mouse cursor), and 'Back'.
 - Import sdconf.rec file:** A section with a blue header. It contains a 'File:' input field and a 'Browse...' button. Below this are 'Import' and 'Back' buttons.
 - Warning:** A yellow warning icon followed by the text: 'Warning: The created RSA servers should be Applied before importing th'.
 - Copyright:** 'Copyright © 2001-2005 Nortel Netw' in the bottom right corner.