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.

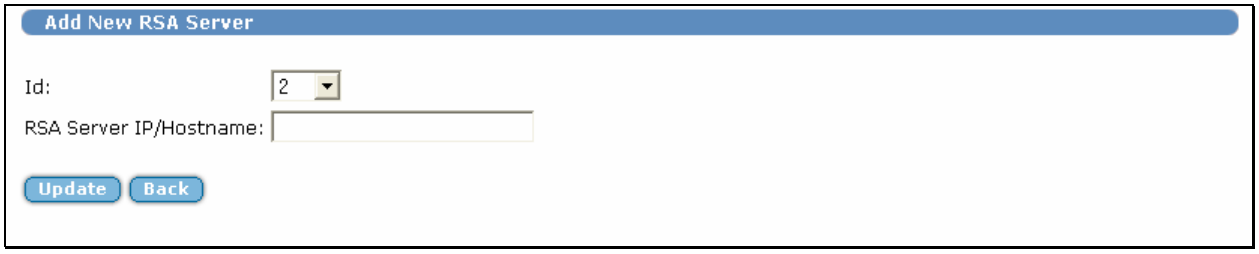
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

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.

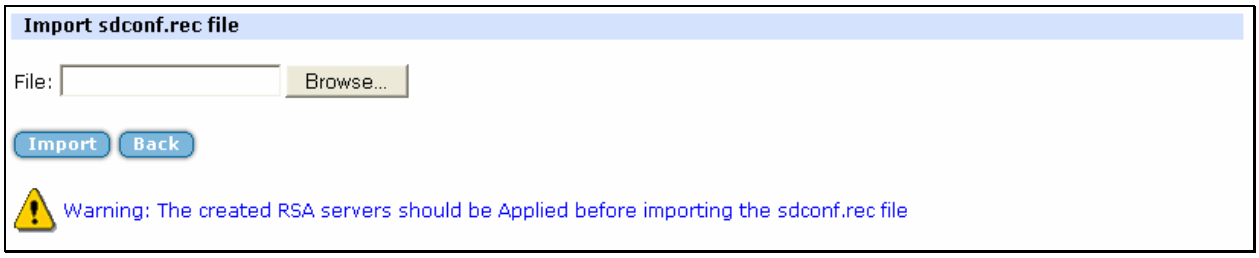
Configure the RSA Server record

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

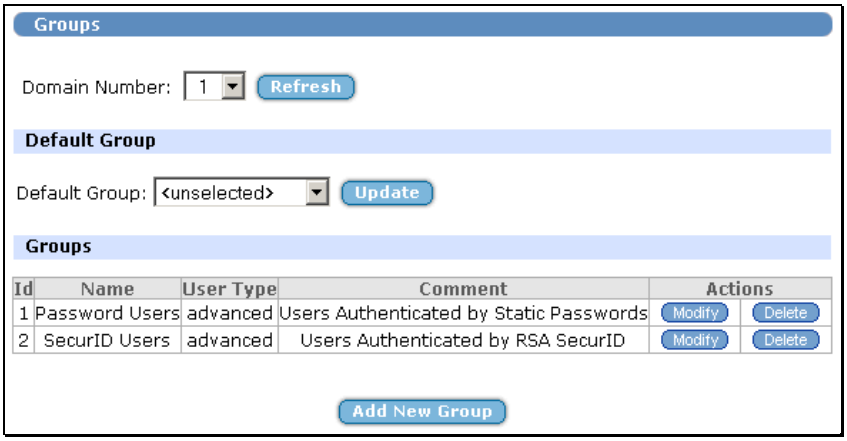
5. To import your sdconf.rec file you will return to the **RSA Servers** menu and modify the entry for the sdconf.rec file you will be adding.



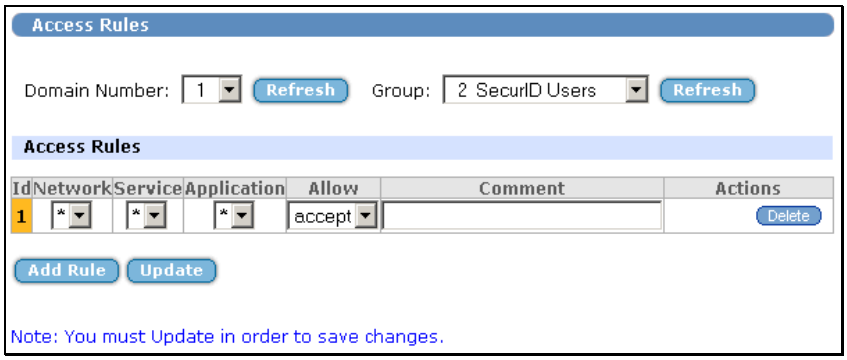
6. Click **import** to upload the sdconf.rec file and then click **Apply** changes to the IOS configuration.

Creating and Configuring a SecurID User Group

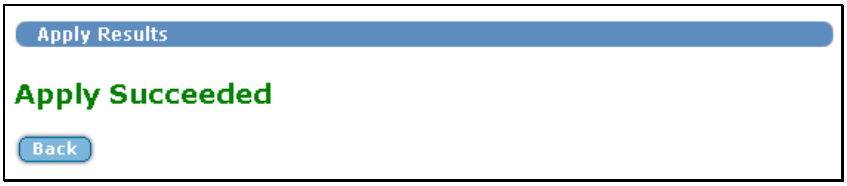
1. From the admin console, expand **VPN Gateways > Group Settings > Groups**.
2. Click on the button **Add New Group**.
3. Fill out the form with the desired group name, user type and description.
4. Click **Update** and then **Apply** to add the new group to the configuration.



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.

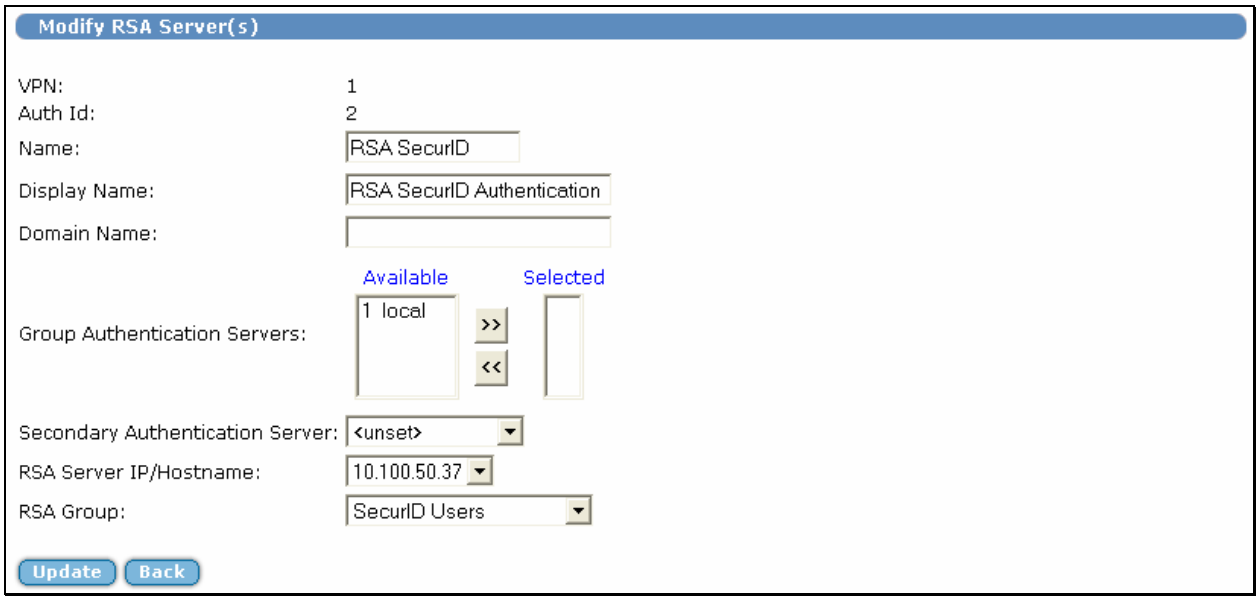


8. Click **Update** to apply the Access rules.
9. Configure the user group for any necessary links or VPN Settings as required.
10. Click **Update** and then **Apply** to add the new information to the IOS configuration.

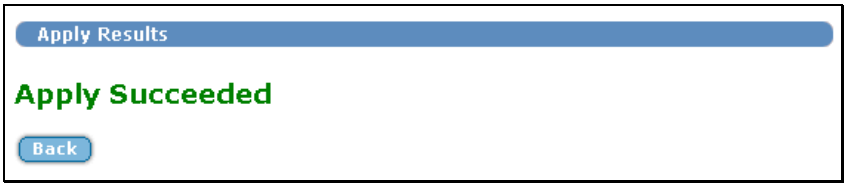


Configuring the RSA SecurID Authentication Servers

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.

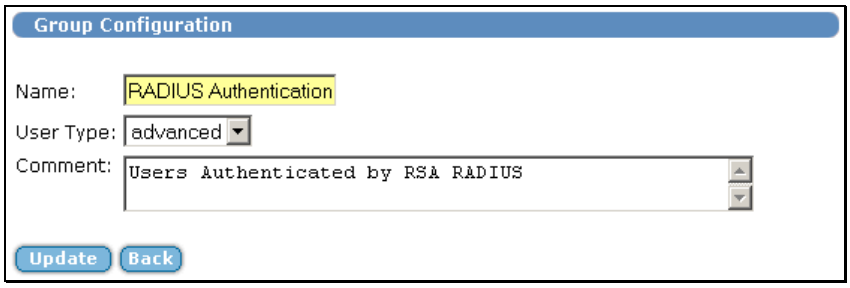


4. Click **Update** and then **Apply** to add the new information to the IOS configuration.

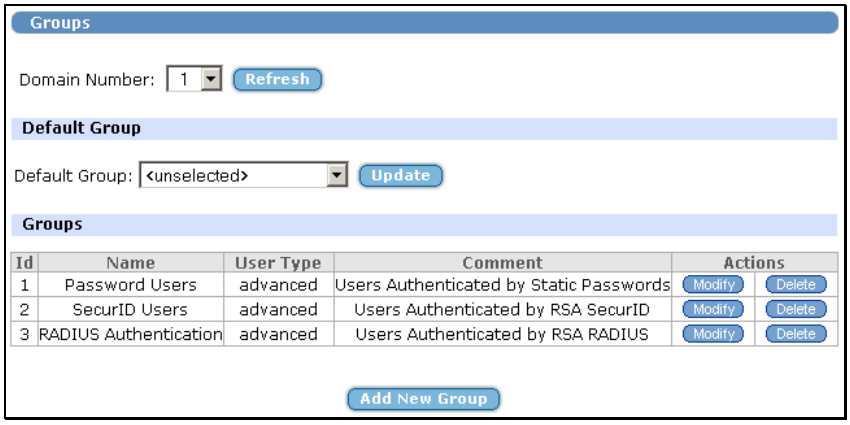


Creating and Configuring a RADIUS User Group

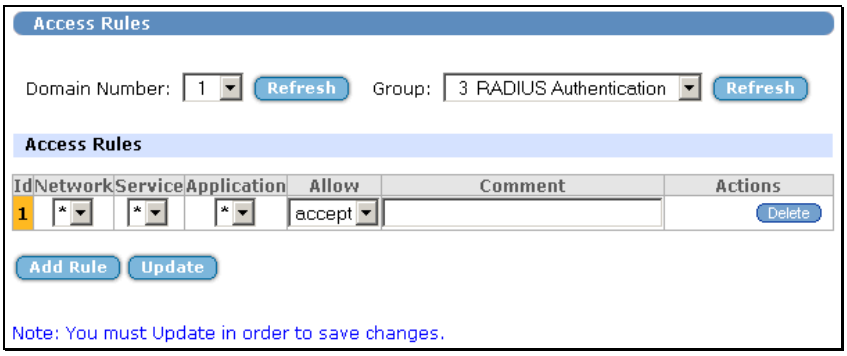
1. From the admin console, expand **VPN Gateways > Group Settings > Groups**.
2. Click on the button **Add New Group**. Fill out the form with the desired group name, user type and description.



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



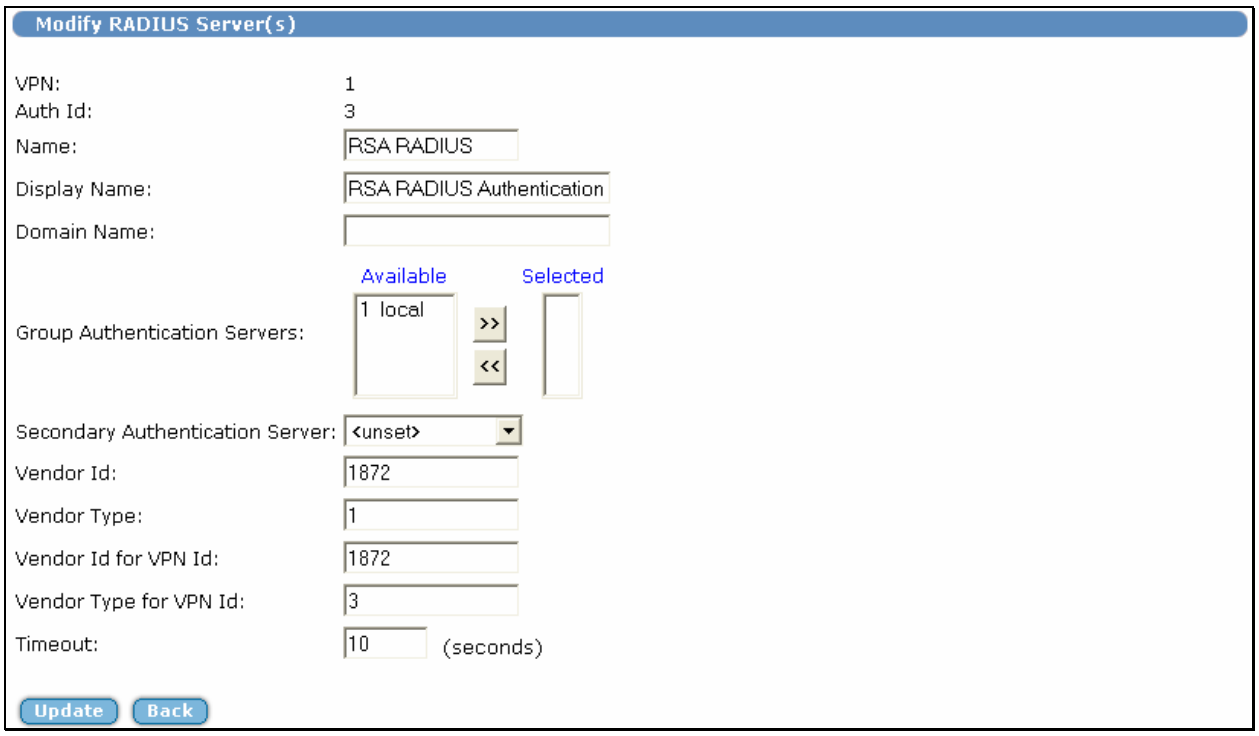
4. From the **Groups** menu on the administration console, select **Access List**.
5. Select the domain number your RSA RADIUS user group resides in and then choose the RSA RADIUS user group from the group list.
6. Create an appropriate Access list based on your organizations configuration. In the example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



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

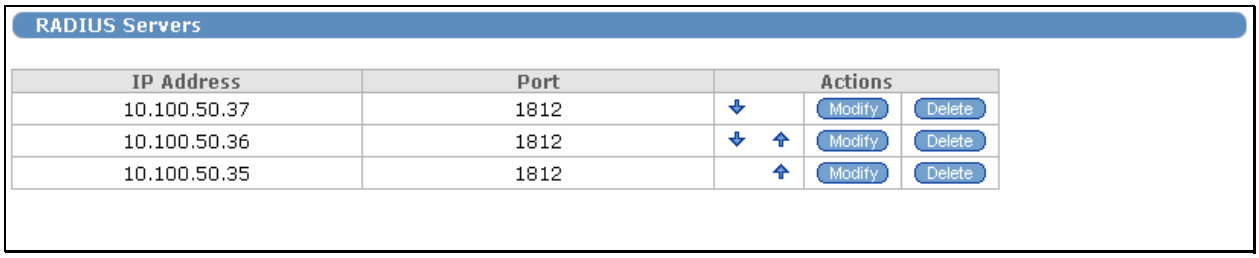
Configuring the RADIUS Authentication Servers

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.



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.

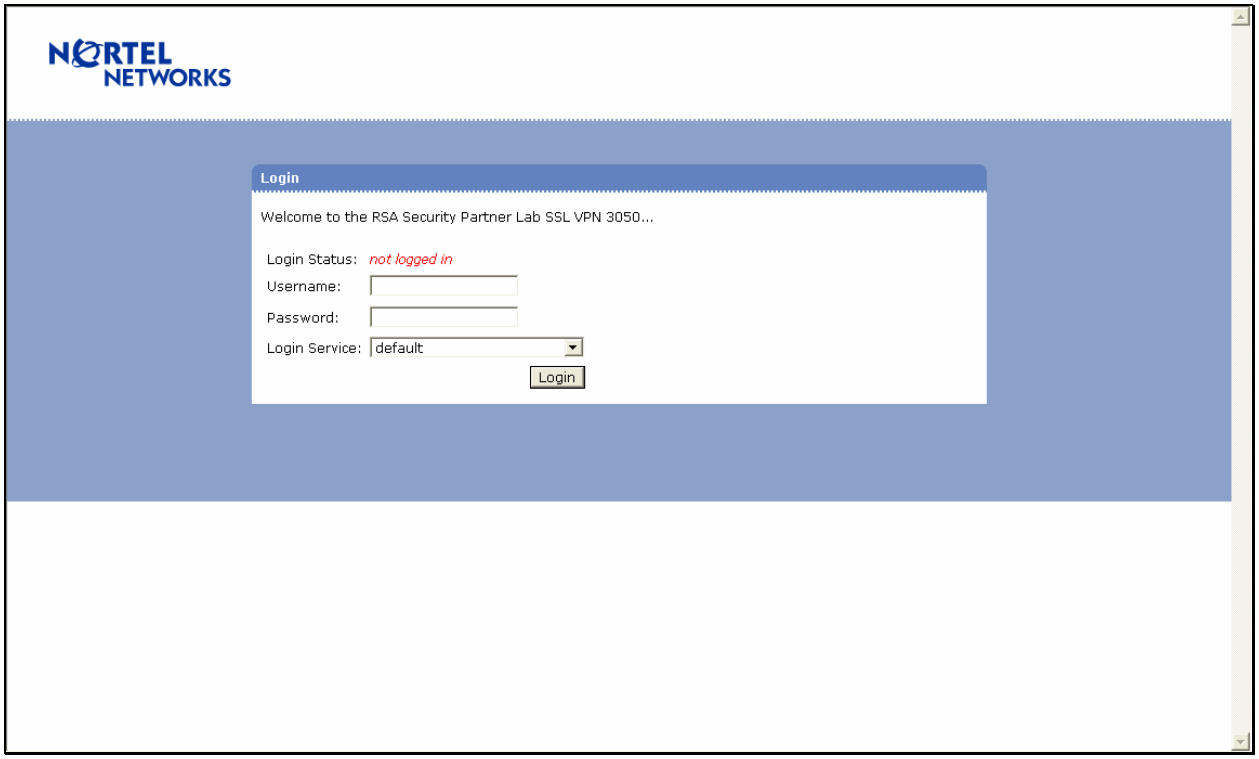
> **Note: You can add a maximum of three RSA RADIUS servers to this authentication server list.**



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.



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	✓		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)	✓
User Selectable	✓		User Selectable	✓
Deny 4 and 8 Digit PIN	✓		Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓		Deny Alphanumeric PIN	✓
PASSCODE				
16 Digit PASSCODE	✓		16 Digit PASSCODE	✓
4 Digit Password	✓		4 Digit Password	✓
Next Tokencode Mode				
Next Tokencode Mode	✓		Next Tokencode Mode	✓
Load Balancing / Reliability Testing				
Failover (3-10 Replicas)	✓		Failover	✓
Name Locking Enabled	✓		Name Locking Enabled	
No RSA Authentication Manager	✓		No RSA Authentication Manager	✓

Additional Functionality				
RSA Software Token API Functionality				
System Generated PIN	N/A		System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A		User Defined (8 Digit Numeric)	N/A
User Selectable	N/A		User Selectable	N/A
Next Tokencode Mode	N/A		Next Tokencode Mode	N/A
Domain Credential Functionality				
Determine Cached Credential State	N/A		Determine Cached Credential State	
Set Domain Credential	N/A		Set Domain Credential	
Retrieve Domain Credential	N/A		Retrieve Domain Credential	

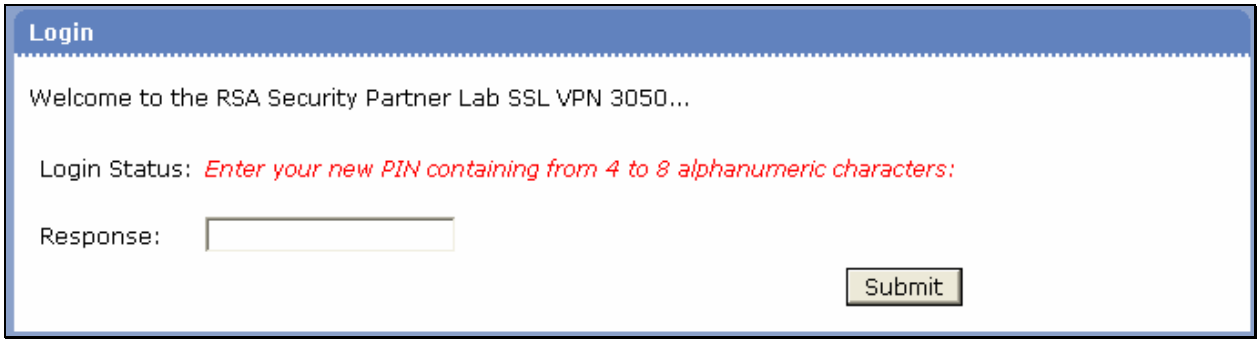
BSD

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

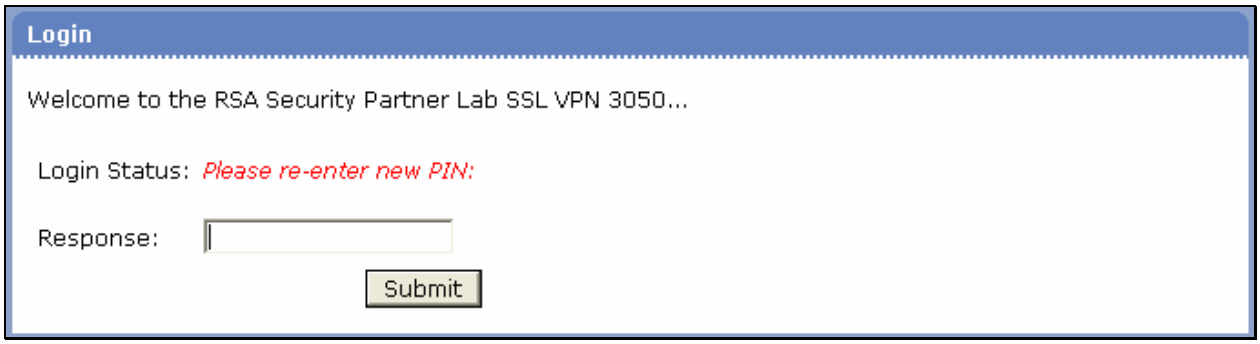
Known Issues

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.

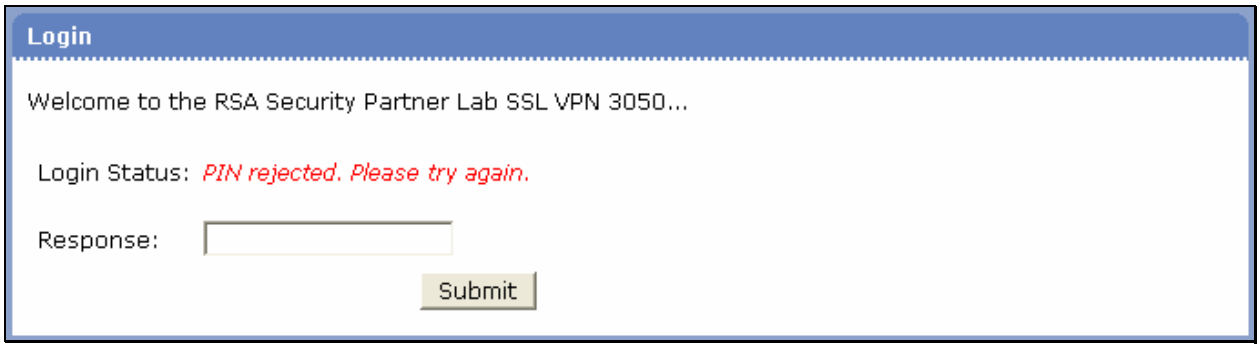
1. The user first authenticates using either Token or Password. The user is next prompted to create a new PIN.



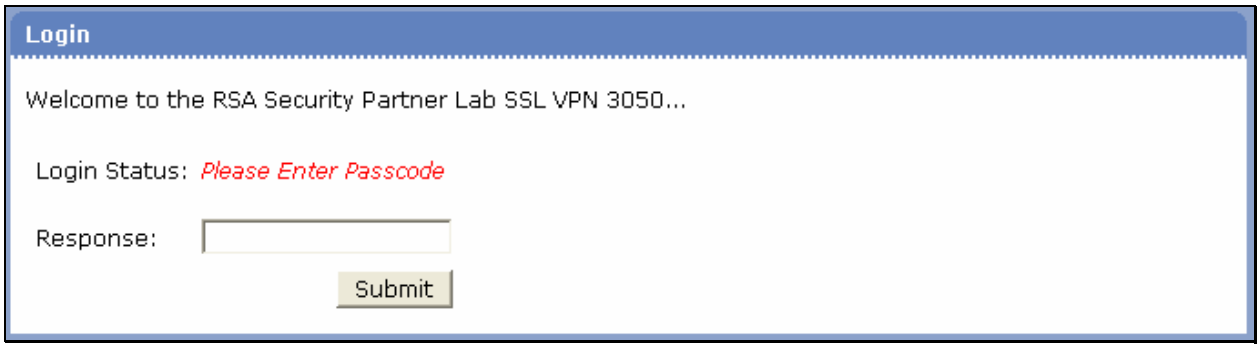
2. The user must re-enter the new PIN to validate input from the previous step.



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



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



5. 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**.