



RSA SecurID Ready Implementation Guide

Last Modified: April 25, 2005

Partner Information

Product Information	
Partner Name	Nortel Networks
Web Site	www.nortelnetworks.com
Product Name	VPN Gateway 3050
Version & Platform	5.0.3
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

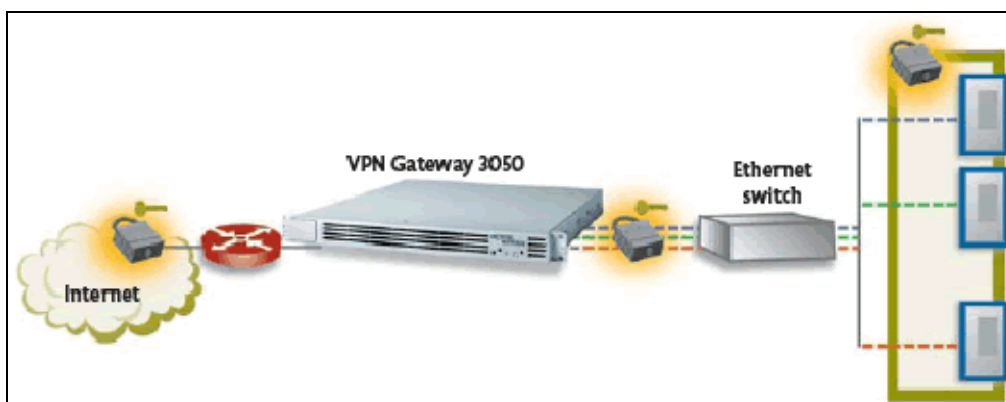
The Nortel Networks VPN Gateway 3050 is a remote access security solution that extends the reach of enterprise applications and resources to remote employees, partners, and customers. By using the native capability of widely deployed Web browsers, the SSL VPN Gateway offers a convenient clientless alternative 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.

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	5.03
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
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

* = Mandatory Function when using Native SecurID Protocols



Product Requirements

Partner Product Requirements: Nortel VPN Gateway 3050	
Firmware Version	5.0.3

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. 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.

Additional Steps for RSA Authentication Manager RADIUS Profiles

Configure a RADIUS Profile in the RSA Authentication Manager

The following steps are for administrators configuring the Nortel VPN Gateway 3050 for RSA RADIUS authentication to the RSA Authentication Manager. These steps are not necessary when using with the Native RSA SecurID authentication method.

When configuring RADIUS authentication directly to your RSA Authentication Manager, follow the steps below to configure a RADIUS Profile and assign it to your users. This configuration is basic and only details the minimum steps to get the VPN Gateway 3050 working with the RSA Authentication Manager RADIUS listener. For additional information on RADIUS Profiles, refer to your RSA Authentication Manager Administrative documentation.

1. Within the Profiles menu, select Add Profile.
2. Name your Profile to make it easily identifiable for future usage. e.g. "Nortel VPN Profile".
3. From the left menu, select Vendor-Specific.
4. Enter a string value as follows : 1872 1 "RADIUS GROUP NAME"
5. Save and Apply your changes.



Note: The string "RADIUS GROUP NAME" refers to the User Group Name configured within the VPN Gateway IOS. This string must match the group to which the RSA SecurID Challenged users belong. This string must be enclosed in double quotes and is case sensitive.

Assign RADIUS Profile to your RSA SecurID Users

1. From the user administration screen, click the button labeled **Assign Profile**.
2. Select the RADIUS profile you configured in the last section.
3. You will now see the assigned profile listed in the user information screen.
4. Save changes to this user.

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.

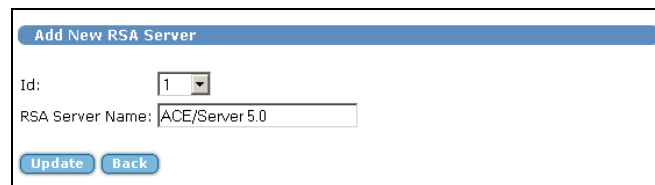
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.


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.

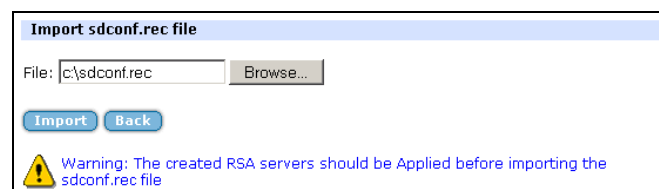
Configure the RSA Server record

1. Open your browser and point to the Management Interface (MIP) of the Nortel SSL Server. Authenticate with administrative user account and select the "Normal" administrative task set.
2. From the SSL VPN admin menu select and expand "Administration" menu and select the "RSA Servers" item.
3. Click the Add New Server button and complete the form with the RSA Authentication Manager logical name.
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, then expand Group Settings and select Groups.
2. Click on the button to add a 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' dropdown set to '<unselected>' with an 'Update' button. A table lists 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

At the bottom of the table is an 'Add New Group' button.

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 are two dropdowns: 'Domain Number' set to '1' and 'Group' set to '2 SecurID Users', each with a 'Refresh' button. Below this is a table for 'Access Rules':

ID	Network	Service	Application	Allow	Comment	Actions
1	*	*	*	accept		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.'

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 with a green message: 'Apply Succeeded'. Below the message is a 'Back' button.

Configuring the RSA SecurID Authentication Servers

1. From the admin console, expand SSL-VPN, then expand Domains, Authentication and select 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)

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

Group Authentication Servers:

Available: 1 Password
Selected:

>> <<

RSA Server Name: ACE/Server 5.0
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 SSL-VPN, then expand Domains and select Groups.
2. Click on the button to add a new group. Fill out the form with the desired group name, user type and description.

Group Configuration

Name:

User Type:

Comment:

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

Groups

Domain Number:

Default Group

Default Group:

Groups

Id	Name	User Type	Comment	Actions
1	Password Users	advanced	Users Authenticated by Static Passwords	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2	SecurID Users	advanced	Users Authenticated by RSA SecurID	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3	RADIUS Authentication	advanced	Users Authenticated by RSA RADIUS	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

4. From the Groups menu on the administration console, select Access.
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.

Access Rules

Domain Number: Group:

Access Rules

Id	Network	Service	Application	Allow	Comment	Actions
1	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="accept"/>		<input type="button" value="Delete"/>

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 SSL-VPN, then expand Domains, Authentication and select 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)

Domain: 1
Auth Id: 3
Name: RSA RADIUS
Display Name: RSA RADIUS
Domain Name:
Group Authentication Servers:

Available: 1 Password | Selected: | << >>

Vendor Id: 1872
Vendor Type: 1
Timeout: 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.

Radius Session Timeout

Session Timeout: disabled
Vendor Id: 0
Vendor Type: 0

RADIUS Servers

IP Address	Port	Shared Secret	Actions
10.100.50.37	1645	secret	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
10.100.50.36	1645	secret	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
10.100.50.35	1645	secret	<input type="button" value="Modify"/> <input 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.

The screenshot shows the Nortel Networks Security Portal login interface. At the top is the Nortel Networks logo and a background image of a person at a computer. Below the logo, it says "Welcome to the Nortel Networks Security Portal. Please login:". The login form includes a "Login Status:" field showing "not logged in", a "Username:" text input field, a "Password:" text input field, and a "Login Service:" dropdown menu currently set to "RSA SecurID Authentication". A "Login" button is located at the bottom right of the form.

NORTEL
NETWORKS


Welcome to the Nortel Networks Security Portal. Please login:

Login Status: *not logged in*

Username:

Password:

Login Service: RSA SecurID Authentication

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

Certification Checklist

Date Tested: April 25, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.0	Windows 2003 Server
VPN Gateway 3050	5.0.3	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	
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	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	

EF

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