RSA SecurID Ready Implementation Guide

Last Modified: April 6, 2005

Partner Information

Product Information	
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	Cisco IOS VPN Router
Version & Platform	12.3(13)
Product Description	Cisco IOS IPsec functionality provides network data encryption at the IP packet level, offering a robust, standards-based, security solution. IPsec provides data authentication and anti-replay services, in addition to data confidentiality services. It is the only way to implement secure VPNs. Customers can combine IPsec with other Cisco IOS Software functionality to build scalable, robust, and secure Quality of Service-aware VPNs.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)

Solution Summary

The Cisco IOS VPN software, combines IPSec VPN enhancements with robust firewall, intrusion detection, and secure administration capabilities. The VPN provides users with a complete implementation of IPSec standards, including support for DES and Triple DES encryption, and authentication through RSA SecurID authentication, and pre-shared keys via RADIUS.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Name Locking	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes/ (hardware dependent for number of servers)
Location of Node Secret on Agent	None stored
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

Product Requirements

Partner Product Requirements: Cisco IOS VPN Router	
Firmware Version	12.3(13)

Additional Software Requirements	
Application	**Additional Patches**
Cisco Secure VPN Client	4.6

Agent Host Configuration

To facilitate communication between the Cisco IOS VPN Router 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 Cisco IOS VPN Router 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, which must match the RADIUS Secret on the Cisco IOS VPN Router.

When adding the Agent Host Record, you should configure the Cisco IOS VPN Router as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Cisco IOS VPN Router 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.

Cisco IOS VPN Router

Log onto the Cisco remote access server and enter enable mode, by typing the word "enable" and giving the enable password. Then enter configuration mode by typing "config t". You are now able to enter the commands below to turn on authentication. To turn off one of the commands put the word no in front of the command line and you will turn off that line.

RADIUS configuration:

```
aaa new-model
aaa authentication login userauthen group local
aaa authorization network groupauthor local

radius-server host xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
radius-server timeout 120
radius-server key "your key"
```

VPN Policy:

```
crypto isakmp policy 3
encr 3des
authentication pre-share
group 2

crypto isakmp client configuration group vpngroup (Must match group name on vpn
client)
key password  (Must match key on vpn client)

crypto ipsec transform-set myset esp-3des esp-sha-hmac

crypto dynamic-map dymap 10
 set transform-set myset

crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dymap
```

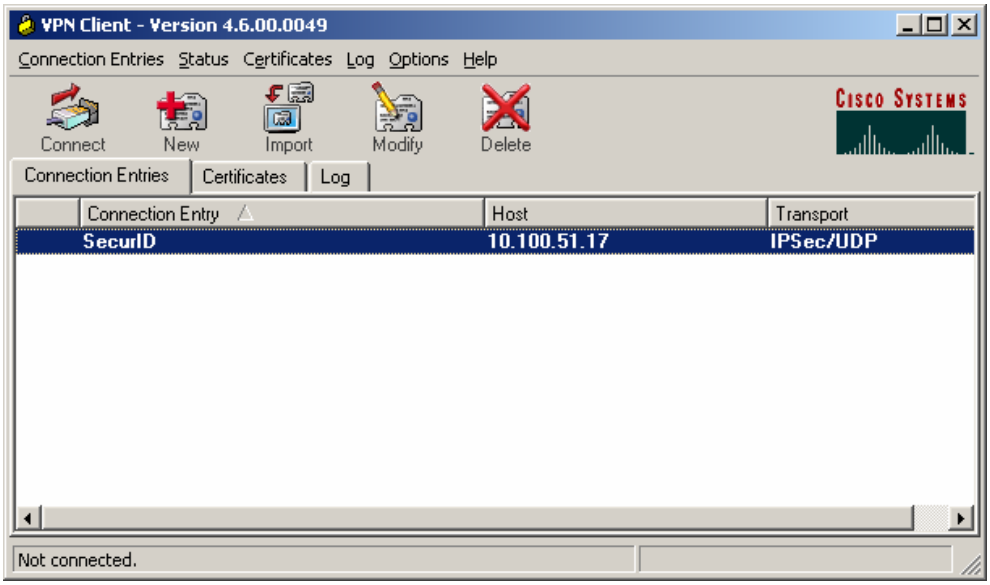
Interface configuration:

Apply the crypto map to the appropriate interface.

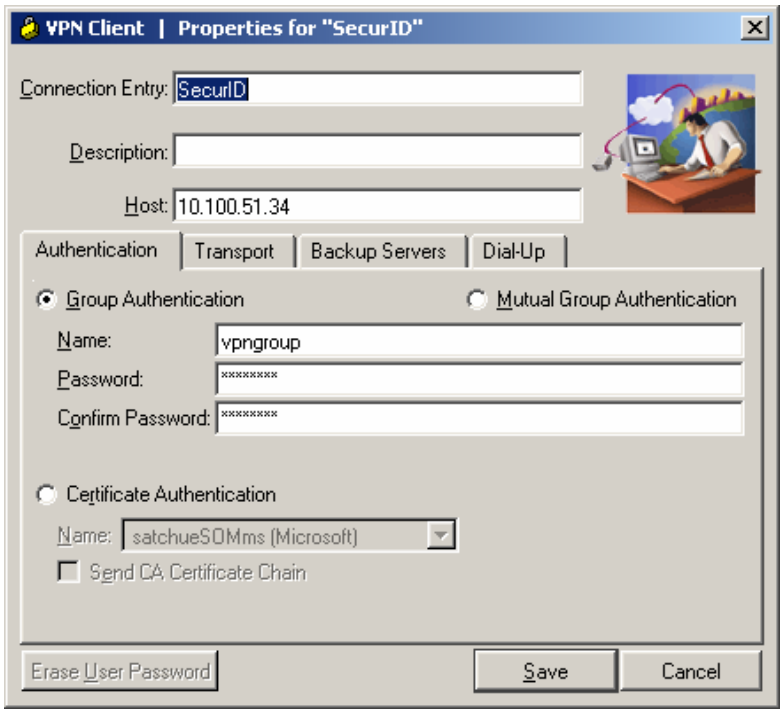
```
interface Ethernet1/0
  description connected to EthernatLAN
  crypto map clientmap
```

VPN Client Configuration

- Install the Cisco VPN client.



- Click the New button to create a RSA SecurID connection entry. Fill in the appropriate information for the connection. The group name and password must match the entry you create on the VPN server.



- Click Save.

- Highlight the connection created and click connect.
- The user will now be prompted for authentication information

Certification Checklist

Date Tested: April 4, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.0	Windows 2003
Cisco IOS VPN Router	12.3(13)	IOS
Cisco Secure VPN Client	4.6	Windows 2003

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
PASSCODE			
16 Digit PASSCODE	N/A	16 Digit PASSCODE	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	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	

SWA

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