Cisco Systems

Cisco IOS Router

RSA SecurID Ready Implementation Guide

Last Modified: March 31, 2008

Partner Information

Product Information	
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	Cisco IOS Router
Version & Platform	12.4(3)
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 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 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 Router	
Firmware Version	12.4(3)

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

Important: If you are configuring the IOS Router to use IPSec you will also need to configure the Cisco VPN client. Information on how to configure the Cisco VPN client can be found in the Cisco VPN client implementation guide located at:

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_VPN_Client_AuthMan61.pdf .

Agent Host Configuration

To facilitate communication between the Cisco IOS Router and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database and RADIUS Server database. The Agent Host record identifies the Cisco IOS 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 Router as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Cisco IOS 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 configuration:

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.

Note: For remote access use the Cisco IOS Routers configuration section.. For VPN access use the Cisco IOS VPN Router section.

Cisco IOS Routers

Note: CHAP authentication is not supported when using RSA SecurID authentication.

Tacacs+ commands

```
aaa new-model
aaa authentication login default tacacs+ line enable
aaa authentication ppp default tacacs+
tacacs-server host xxx.xxx.xxx.xxx
tacacs-server timeout 120
tacacs-server key "your key"
```

RADIUS commands

```
aaa new-model
aaa authentication login default radius line enable
aaa authentication ppp default radius
radius-server host xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646 key "your key"
radius-server timeout 120
```

Cisco IOS VPN Router

RADIUS configuration:

```
aaa new-model
aaa authentication login userauthen group radius 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 (“vpngroup” Must match the
group name set in the vpn client)
key password  (“password” Must match password set in the vpn client)
pool vpnpool  (“vpnpool” is the name of an ip pool created on the router)

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
```

The VPN Policy is an example only. You may need to make changes to it to fit your needs. For example the encr command could be set to encr aes 256.

Certification Checklist: For RSA Authentication Manager 6.x Cisco Router

Date Tested: September 29, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003
Cisco IOS VPN Router	12.4(3)	IOS

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	

BSD/SWA

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

Certification Checklist: For RSA Authentication Manager 6.x VPN

Date Tested: September 29, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003
Cisco IOS VPN Router	12.4(3)	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	

BSD/SWA

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

Certification Checklist For RSA Authentication Manager 7.x Router

Date Tested: March 31, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003 SP2
RSA RADIUS Server	7.1	Windows 2003 SP2
Cisco IOS VPN Router	12.4(3)	IOS

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)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse		PIN Reuse	
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

SWA

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

Certification Checklist For RSA Authentication Manager 7.x VPN

Date Tested: March 31, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003 SP2
RSA RADIUS Server	7.1	Windows 2003 SP2
Cisco IOS VPN Router	12.4(3)	IOS
Cisco Secure VPN Client	4.8	Windows XP Professional SP2

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)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

SWA

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

Known Issues

1. CHAP authentication is not supported when using RSA SecurID authentication