



RSA SecurID Ready Implementation Guide

Last Modified: March 27, 2008

Partner Information

Product Information	
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	ASA 5500 Series Adaptive Security Appliances
Version & Platform	7.0(1) and 7.2.(3)
Product Description	Cisco® ASA 5500 Series adaptive security appliances are purpose-built solutions that combine best-of-breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting small and medium-sized business and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)





Solution Summary

The Cisco ASA 5500 Series provides RSA SecurID authentication as one mechanism to control network activity via a RADIUS authentication and delivers flexible IPSEC or SSL VPN connectivity authentication via RADIUS or Native RSA SecurID Authentication.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, and RADIUS
List Library Version Used	5.02
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes (Dependent on Hardware)
Location of Node Secret on Agent	In flash
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	Yes, via VPN Client
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: Cisco ASA 5500	
Firmware Versions	7.0(1), 7.2(3)

Additional Software Requirements	
Application	Additional Patches
Cisco VPN Client	4.6 or higher

! Important: If you are configuring the ASA Server 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 ASA 5500 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 if using RADIUS. The Agent Host record identifies the Cisco ASA 5500 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 Cisco ASA 5500 as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Cisco ASA 5500 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.

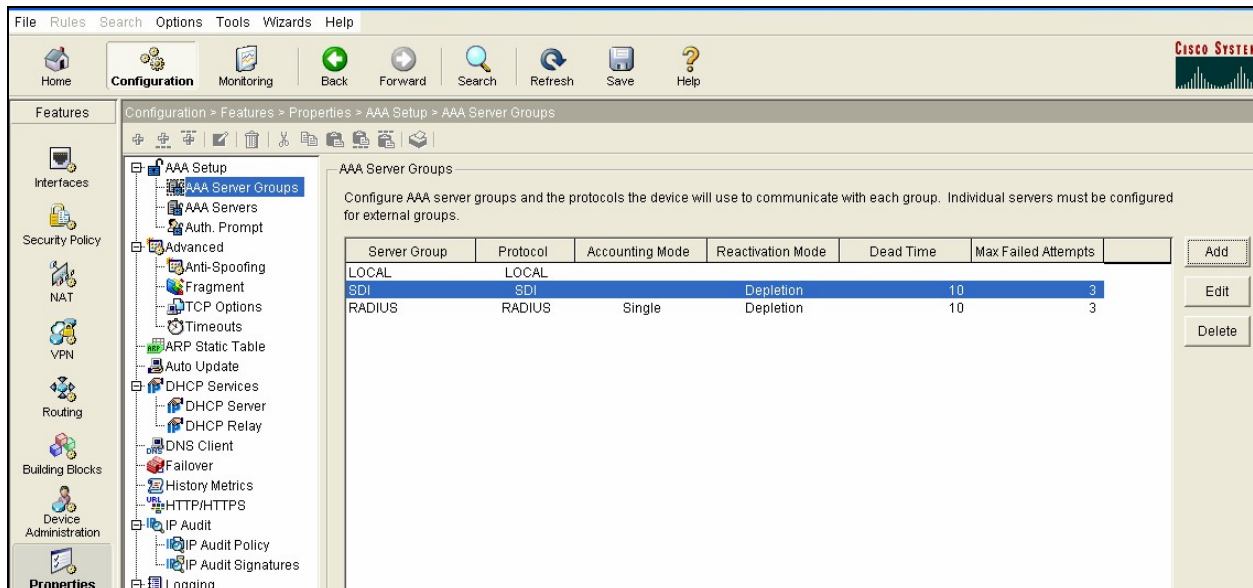
Documenting the Solution

The ASA 5500 Series Adaptive Security Appliances can authenticate to an RSA Authentication Manager in two ways. One way is via the Native RSA SecurID Authentication Protocol and the other is via RADIUS. The ASA also has three areas where RSA SecurID Authentication can be enabled. They are IPSEC VPN, Web SSL VPN and Firewall. Start the Cisco ASDM manager and go to the appropriate configuration section below for your needs.

 **Note:** Click Apply after your configuration changes when appropriate.

Authentication via RSA Native SecurID Authentication Protocol

1. Select **Configuration** from the top menu and then select **Properties** from the Features Menu on the left.
2. Select AAA Setup – AAA Server Groups.



The screenshot shows the Cisco ASDM configuration interface. The left sidebar displays the configuration tree with 'AAA Setup' expanded to 'AAA Server Groups'. The main pane shows the 'AAA Server Groups' configuration table. The table has columns for Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, and Max Failed Attempts. The 'SDI' group is selected, and the 'Add' button is visible on the right.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
SDI	SDI		Depletion	10	3
RADIUS	RADIUS	Single	Depletion	10	3

3. Click Add.



Add AAA Server Group

Configure AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group:

Protocol:

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: minutes

Max Failed Attempts:

- Server Group: Name the server group.
- Protocol: Select SDI.

 **Note:** Cisco refers to RSA SecurID authentication as “SDI”.

4. Click **OK**.
5. Select AAA Setup – AAA Servers.

The screenshot shows the Cisco Configuration Assistant interface. The breadcrumb trail is Configuration > Features > Properties > AAA Setup > AAA Servers. The main area displays the AAA Servers configuration table:

Server Group (Protocol)	Interface	Server IP Address	Timeout	
SDI (SDI)	inside	90.176.1.254	10	<input type="button" value="Add"/>
RADIUS (RADIUS)	inside	90.176.1.254	10	<input type="button" value="Edit"/>
RADIUS (RADIUS)	inside	90.176.1.4	10	<input type="button" value="Delete"/>

6. Click **Add**.



7. Select the Server Group created above for the RSA Authentication Manager "SDI" Server Group.

A screenshot of a Windows-style dialog box titled "Edit AAA Server". The dialog has a blue title bar with a close button (X). The main area is light beige and contains several configuration fields:

- Server Group:** A text field containing "SDI".
- Interface Name:** A dropdown menu with "inside" selected.
- Server IP Address:** A text field containing "90.176.1.254".
- Timeout:** A text field containing "10" followed by the label "seconds".
- SDI Parameters:** A large rectangular area containing:
 - Server Port:** A text field containing "5500".
 - Retry Interval:** A dropdown menu with "10 seconds" selected.
 - SDI Version:** A dropdown menu with "SDI version 5.0" selected.
 - Slave Server IP Address:** An empty text field.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

8. Select SDI Version 5.0 for the SDI Version. For the other parameters select the appropriate values for your servers.



Authentication via RADIUS

1. Select **Configuration** from the top menu and then select **Properties** from the Features Menu on the left.
2. Select AAA Setup – AAA Server Groups.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
SDI	SDI		Depletion	10	3
RADIUS	RADIUS	Single	Depletion	10	3

3. Click **Add**.

Configure AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group:

Protocol:

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

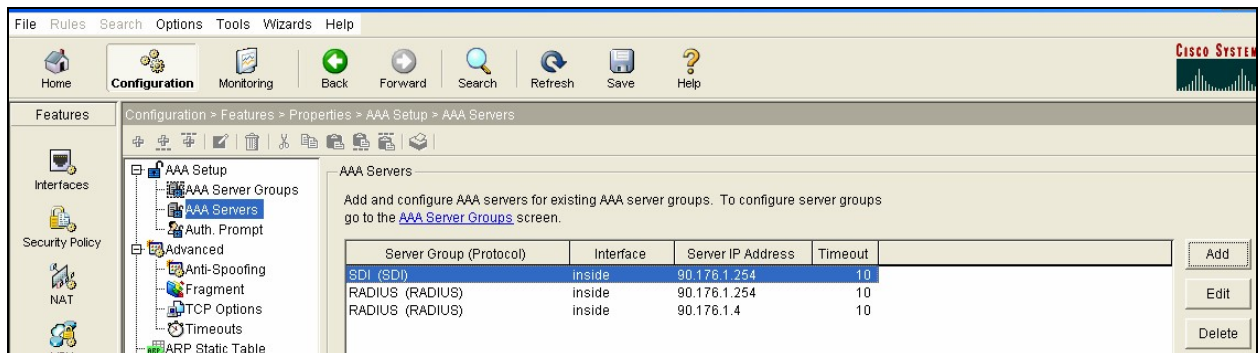
Dead Time: minutes

Max Failed Attempts:

OK Cancel Help

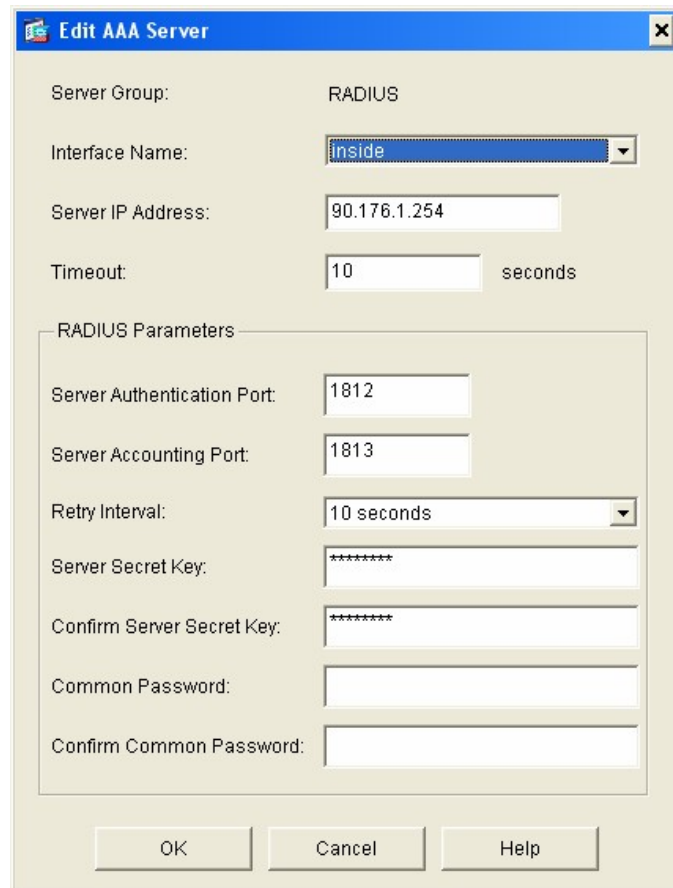
4. Name the server group and select RADIUS for the Protocol. This process can be repeated to add backup RADIUS Server.
5. Click **OK**.

6. Select AAA Setup – AAA Servers.



7. Click **Add**.

8. Select the Server Group created above for the RADIUS Server Group.



9. Select the Server Group created above for the RADIUS Server Group.

10. Enter the appropriate information for your configuration.

 **Note: The Server Secret Key needs to match the Secret Key created in the RADIUS server.**



11. Click **OK**.

IPSec VPN Configuration

1. Select **Configuration** from the top menu and then select **VPN** from the Features Menu on the left.
2. Select IP Address Management – IP Pools and add an IP pool.

The screenshot shows the RSA SecurID configuration interface. The top menu includes File, Rules, Search, Options, Tools, Wizards, and Help. The main navigation bar has icons for Home, Configuration, Monitoring, Back, Forward, Search, Refresh, Save, and Help. The left sidebar shows the Features menu with categories like Interfaces, Security Policy, NAT, VPN, Routing, and Building Blocks. The main content area is titled 'Configuration > Features > VPN > IP Address Management > IP Pools'. It displays a table for creating named IP address pools.

Pool Name	Starting Address	Ending Address	Subnet Mask	
90.176.0.0	90.176.1.60	90.176.1.70	255.252.0.0	<input type="button" value="Add"/>
				<input type="button" value="Edit"/>
				<input type="button" value="Delete"/>

3. Select IKE – Global Parameters and enable IKE access to the appropriate interface.

The screenshot shows the RSA SecurID configuration interface for the IKE Global Parameters page. The top menu and navigation bar are the same as in the previous screenshot. The left sidebar shows the Features menu with the VPN category selected. The main content area is titled 'Configuration > Features > VPN > IKE > Global Parameters'. It displays a table for enabling IKE access to interfaces.

Interface	IKE Enabled	
inside	No	<input type="button" value="Enable"/>
outside	Yes	<input type="button" value="Disable"/>

Below the table, there are checkboxes for 'Enable IPsec over NAT-T' and 'Enable IPsec over TCP'. The 'Enable IPsec over NAT-T' checkbox is checked, and the 'NAT Keepalive' is set to 20 seconds. The 'Enable IPsec over TCP' checkbox is unchecked, and the 'Enter up to 10 comma-separated TCP port values (1- 65535):' field contains the value 10000.



4. Select IKE – Policies.

Configuration > Features > VPN > IKE > Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	
10	3des	md5	2	pre-share	86400	Add
65535	3des	sha	2	pre-share	86400	Edit
						Delete

5. Click **Add** or **Edit**.

6. Create your IKE Policy with pre-shared selected for Authentication and the appropriate setting for the other parameters.

Edit IKE Policy

Priority: Authentication:

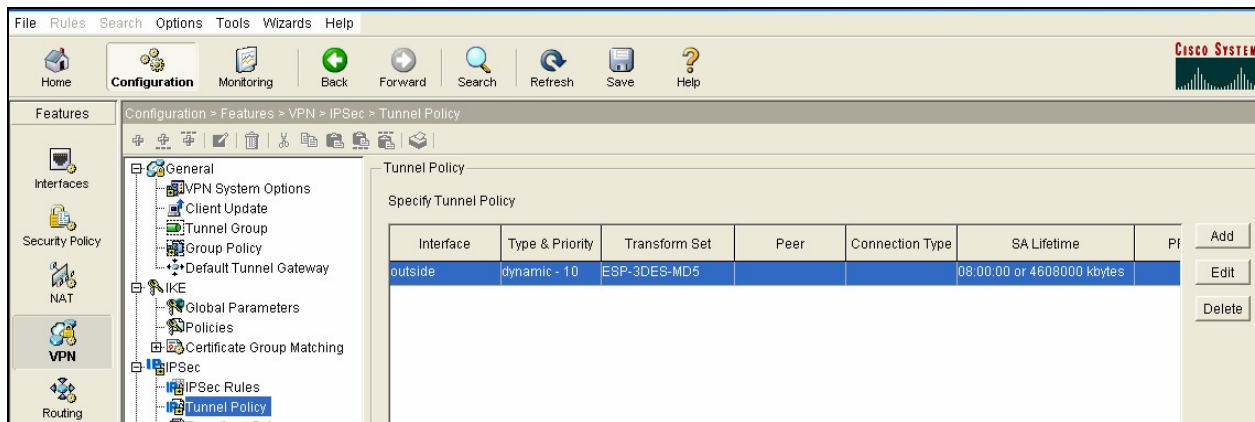
Encryption: D-H Group:

Hash: Lifetime:

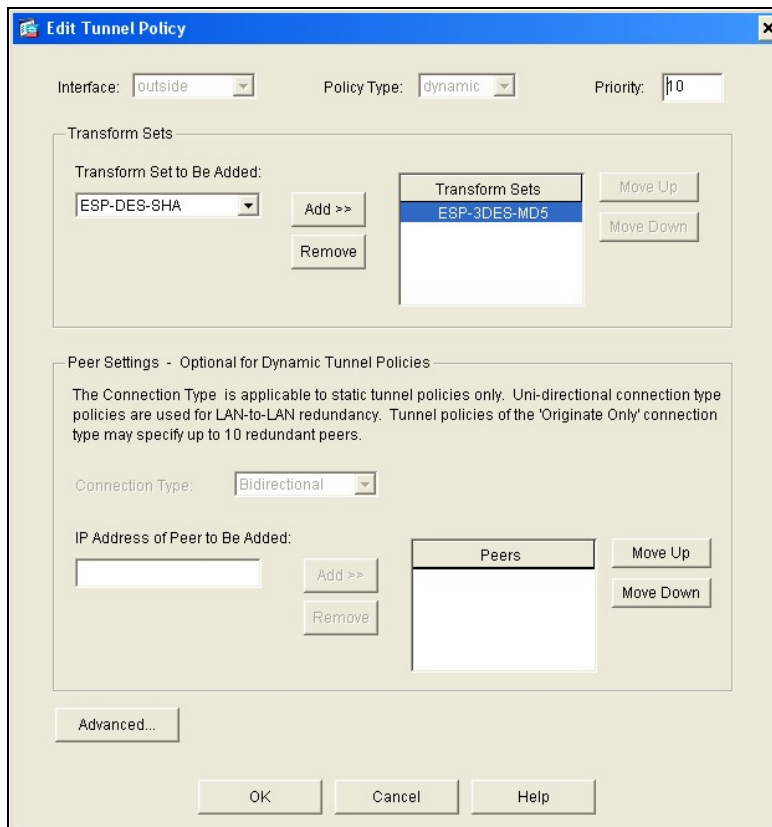
7. Click **OK**.



8. Select IPsec – Tunnel Policy.

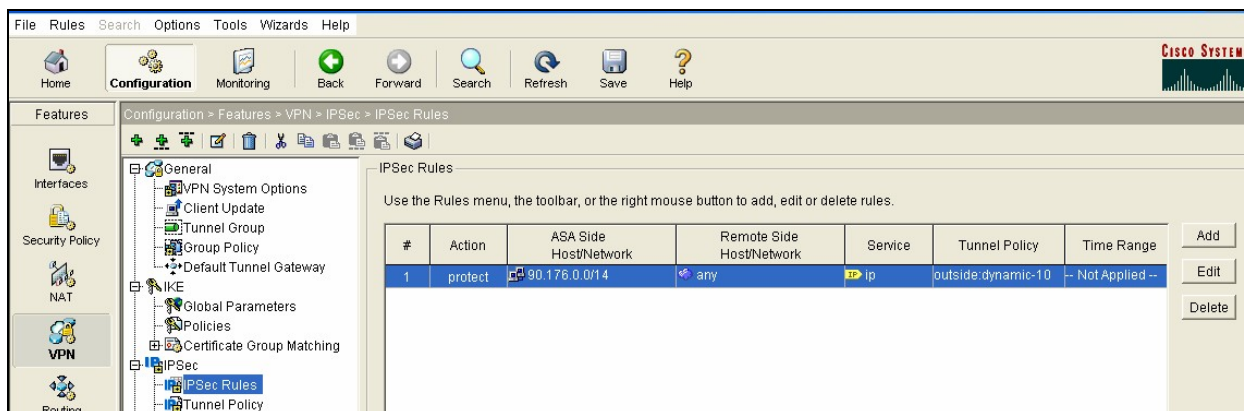


9. Select Add to add a new policy or Edit to modify an existing policy..

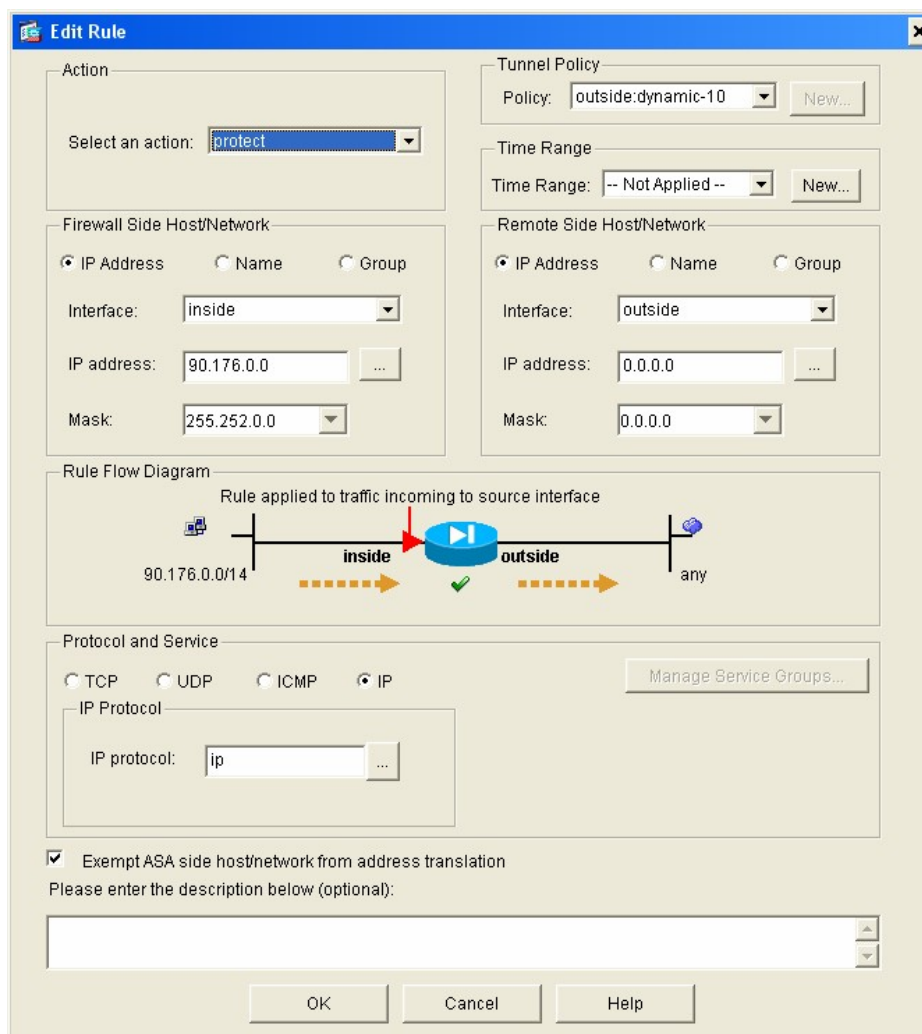


10. Click OK after selecting the appropriate settings for your policy.

11. Select IPsec – IPsec Rules.

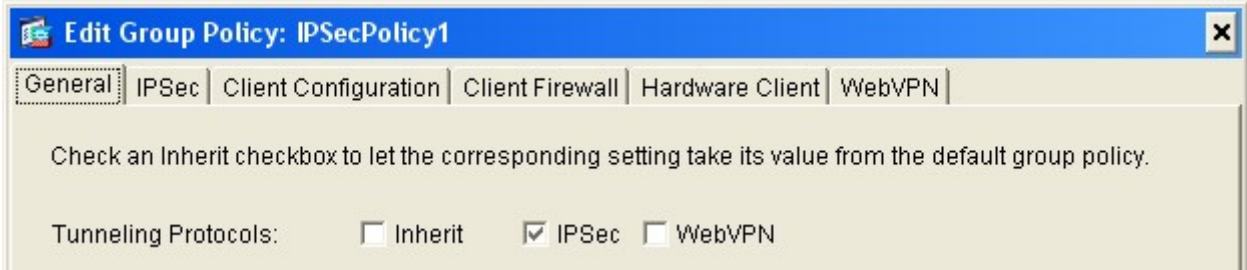


12. Click Add to add a new rule or Edit to modify an existing rule.

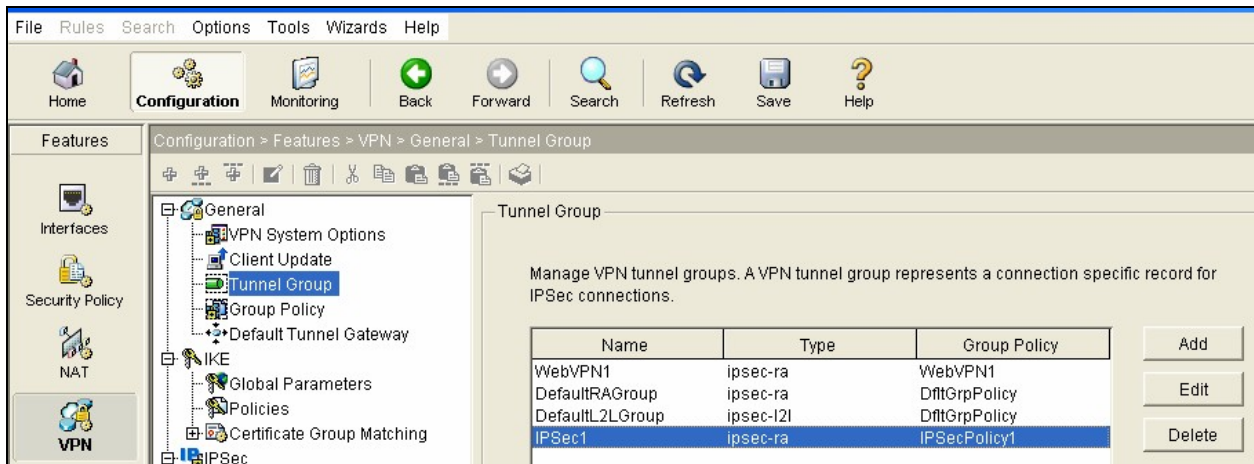




13. Select the newly created policy for the Tunnel Policy and selecting the appropriate settings for the other parameters. Click **OK**
14. Select General – Group Policy and add a group policy.



15. Check the box for IPSec and make any other configuration changes you need for your policy.
16. Click **OK**.
17. Select General – Tunnel Group.



18. Click **Add**.



Edit Tunnel Group: IPsec1 (type is ipsec-ra)

General | Client Address Assignment | IPsec | Advanced

Group Policy:

Strip the realm from username before passing it on to the AAA server

Strip the group from username before passing it on to the AAA server

To set authentication server group per interface, go to the Advanced tab.

Authentication Server Group:

Use LOCAL if Server Group fails

Authorization Server Group:

Users must exist in the authorization database to connect

Accounting Server Group:

19. Select the General tab .

- Group Policy : Select the Group Policy you created in the step above.
- Authentication Server Group: Select the Authentication Method Created, which is RSA SecurID Authentication "SDI" or RADIUS.

20. Select the Client Address Assignment tab.

- Add the appropriate ip pool.

Edit Tunnel Group: IPsec1 (type is ipsec-ra)

General | Client Address Assignment | IPsec | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

Assigned Pools

Available Pools

Assigned Pools: 90.176.0.0

OK Cancel Help



21. Select the IPsec tab.

A screenshot of a software configuration window titled "Edit Tunnel Group: IPsec1 (type is ipsec-ra)". The window has four tabs: "General", "Client Address Assignment", "IPsec", and "Advanced". The "IPsec" tab is selected. In the "IPsec" tab, there are three fields: "Pre-shared Key" with the value "password", "Trustpoint Name" with a dropdown menu showing "-- None --", and "IKE Peer ID Validation" with a dropdown menu showing "Required".

- Pre-shared Key: Enter a key. This will be the same as the group password in the Cisco VPN Client.

22. Click **OK**.

! > Important: A user who is in New-PIN mode will be asked to authenticate with their new PIN and be denied access. They will need to re-authenticate to gain access. See the second Known issue located in the Known Issues section of this guide for more information.

! > Important: The VPN client also needs to be configured for IPsec VPN access to work and the information on how to do that is documented in the Cisco VPN Client implementation guide located at http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_VPN_Client_AuthMan61.pdf.



Web SSL VPN

1. Select **Configuration** from the top menu and then select **VPN** from the Features Menu on the left.
2. Select Web VPN – WebVPN Access and enable access to the appropriate interface.

The screenshot shows the RSA SecurID configuration interface. The top menu includes File, Rules, Search, Options, Tools, Wizards, and Help. The main navigation bar has icons for Home, Configuration, Monitoring, Back, Forward, Search, Refresh, Save, and Help. The left sidebar shows a tree view of configuration categories: Interfaces, Security Policy, NAT, VPN (highlighted), Routing, Building Blocks, Device Administration, and Properties. The main content area is titled 'Configuration > Features > VPN > WebVPN > WebVPN Access'. It contains a 'WebVPN Access' configuration panel with a table and several settings.

WebVPN Access

Configure access parameters for WebVPN. (Note: The WebVPN features in this software release are currently provided as a free trial, and future major software releases will require the purchase and installation of a WebVPN feature license.)

Interface	WebVPN Enabled
inside	No
outside	Yes

Enable

Disable

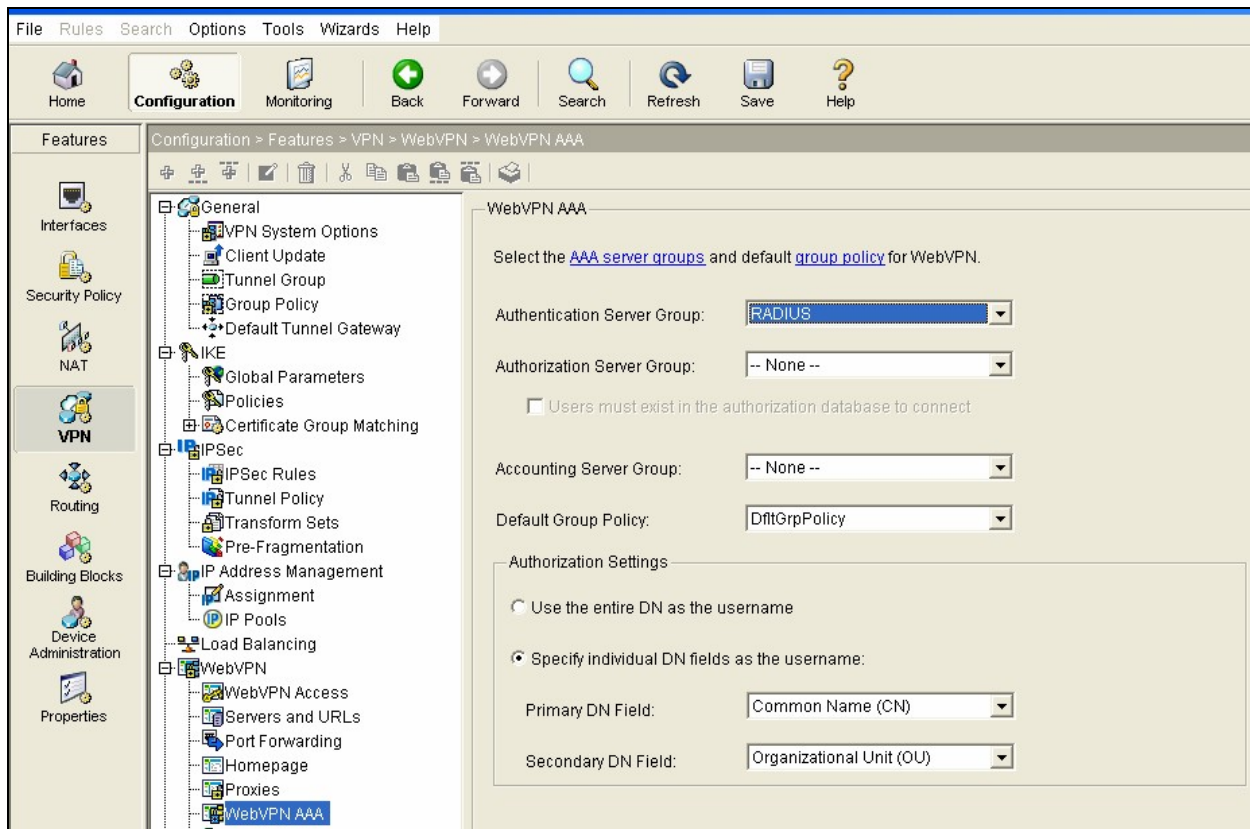
WebVPN Authentication: AAA Certificate Both

Global WebVPN Default Idle Timeout: seconds

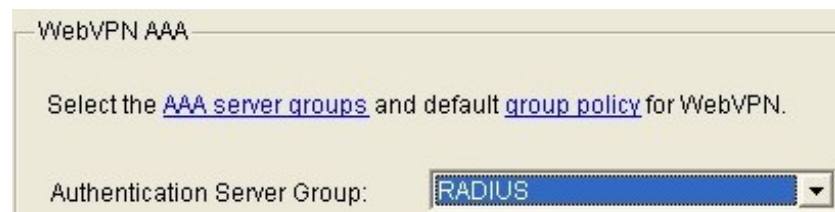
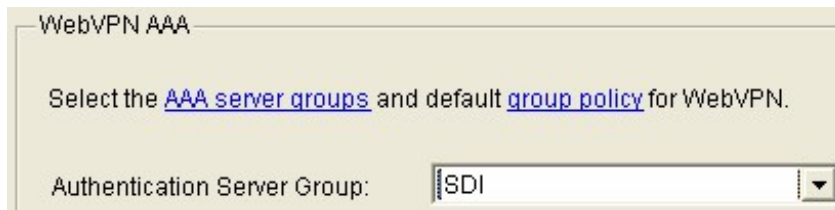
Maximum WebVPN Sessions Limit:



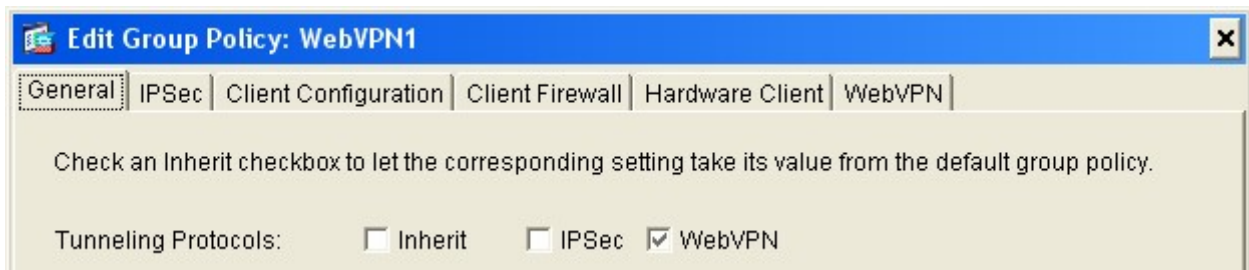
3. Select Web VPN – WebVPN AAA.



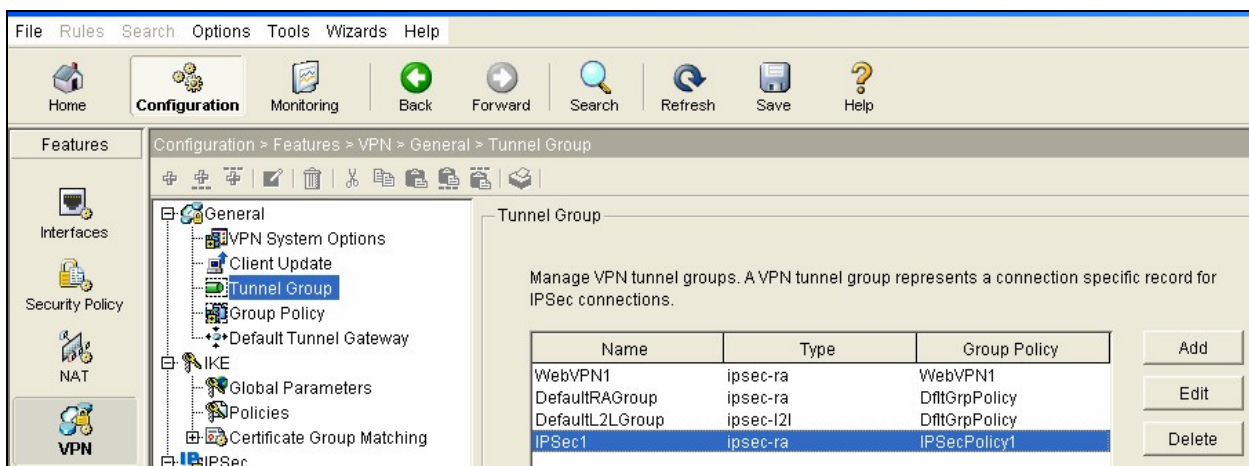
4. For Authentication Server Group select SDI or RADIUS.



5. Select General – Group Policy and add a group policy.



6. Check the box for WebVPN and make any other configuration changes you need for your policy.
7. Click **OK**.
8. Select General – Tunnel Group.



9. Click **Add**.



Edit Tunnel Group: WebVPN1 (type is ipsec-ra)

General | Client Address Assignment | IPsec | Advanced

Group Policy:

Strip the realm from username before passing it on to the AAA server

Strip the group from username before passing it on to the AAA server

To set authentication server group per interface, go to the Advanced tab.

Authentication Server Group:

Use LOCAL if Server Group fails

Authorization Server Group:

Users must exist in the authorization database to connect

Accounting Server Group:

10. Select the General tab .

- Group Policy : Select the Group Policy you created in the step above.
- Authentication Server Group: Select the Authentication Method Created, which is RSA SecurID Authentication "SDI" or RADIUS.

11. Select the Client Address Assignment tab.

- Add the appropriate ip pool.

Edit Tunnel Group: WebVPN1 (type is ipsec-ra)

General | Client Address Assignment | IPsec | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

DHCP Servers

Address Pools

To configure interface-specific address pools, go to the Advanced tab.

Available Pools

Assigned Pools

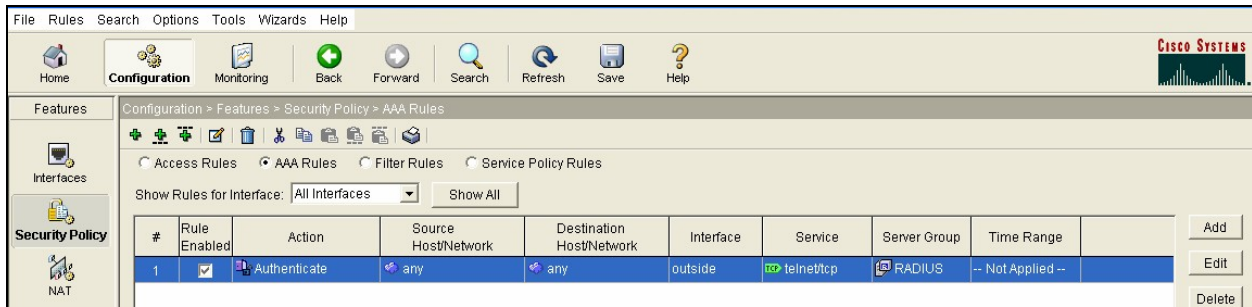
90.176.0.0



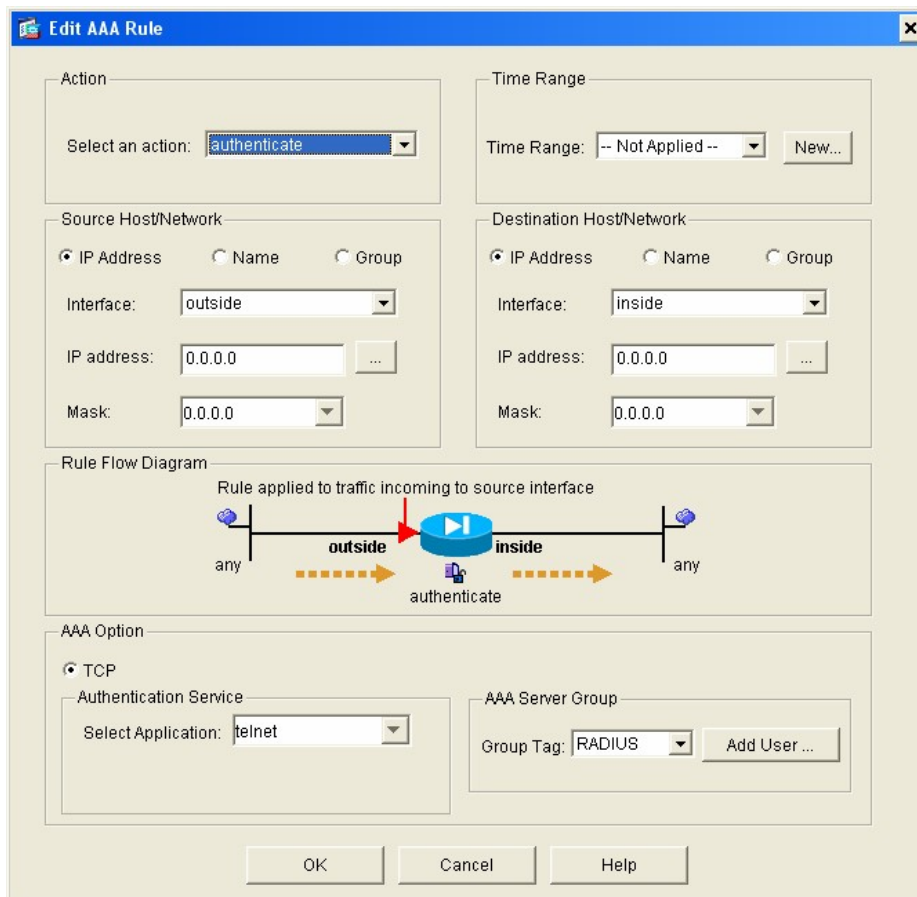
Click OK.

Firewall

1. Select **Configuration** from the top menu and then select **Security Policy** from the Features Menu on the left.
2. Select the AAA Rules radio button.



3. Click **Add**.



- Select Authenticate for Select an Action.
- Select the appropriate application under AAA Options. In this example Telnet is the application.



- Select RADIUS for the Group Tag under AAA Server Group.
 - Set the other parameters according to your policies.
4. Click **OK**.

Certification Checklist: IPSEC VPN – Authentication Manager 6.1

Date Tested: February 10, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.2	Windows 2000 SP4
RSA Remote Authentication Utility (RAU)	1.0 (Build 25)	Windows XP SP2
Cisco ASA 5500	7.2(3)	IOS
Cisco VPN Client	4.6.01.0019 and 4.8.00.0440	Windows XP SP2

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 Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input checked="" type="checkbox"/>	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"/>

CMY

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

Certification Checklist: IPSEC VPN – Authentication Manager 7.1

Date Tested: April 25, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 SP4
Cisco ASA 5500	7.2(3)	IOS
Cisco VPN Client	4.6.01.0019, 4.8.00.0440, and 5.0.03.0530	Windows XP SP2

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"/>
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"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<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"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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

Certification Checklist: Web SSL VPN

Date Tested: December 29, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2000 SP4
Cisco ASA 5500	7.0(1)	IOS

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 type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
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 type="checkbox"/> N/A
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 Automation			
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
RSA SecurID 800Token Automation			
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"/>

SWA

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

Certification Checklist: Firewall

Date Tested: December 29, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2000 SP4
Cisco ASA 5500	7.0(1)	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 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
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800Token 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
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



Known Issues

1. **Firewall authentication:** New-PIN and Next-Tokencode does not work via FTP or HTTP. Virtual telnet needs to be configured to enable this functionality. See the Cisco documentation on how to enable this feature.
2. **IPSEC VPN Authentication:** After a user creates a PIN they are asked to re-authenticate using that new PIN. This authentication will fail but the next authentication a user performs will work. The end user will not notice this issue as they most likely will think that they entered the wrong code and try again which will succeed if they enter the correct information. The Authentication Manger Administrator will see an "Access Denied, name lock required" error in the log file. Cisco has been made aware of this issue and should be contacted if more information is needed.
3. **SSL VPN Authentication:** New-PIN and Next-Tokencode are not supported when using RADIUS as the authentication method.
4. **Name Lock Error:** Users will generate name locking errors in the RSA Authentication Manager logs when in NEW PIN mode and name locking is enabled.



Appendix

See the Cisco Secure VPN Client implementation guide for information on how to configure the Cisco VPN Client to work with the Cisco ASA 5500 and RSA SecurID authentication.