Cyberoam Technologies Pvt Ltd
Cyberoam

RSA SecurID Ready Implementation Guide

Last Modified: September 26, 2013

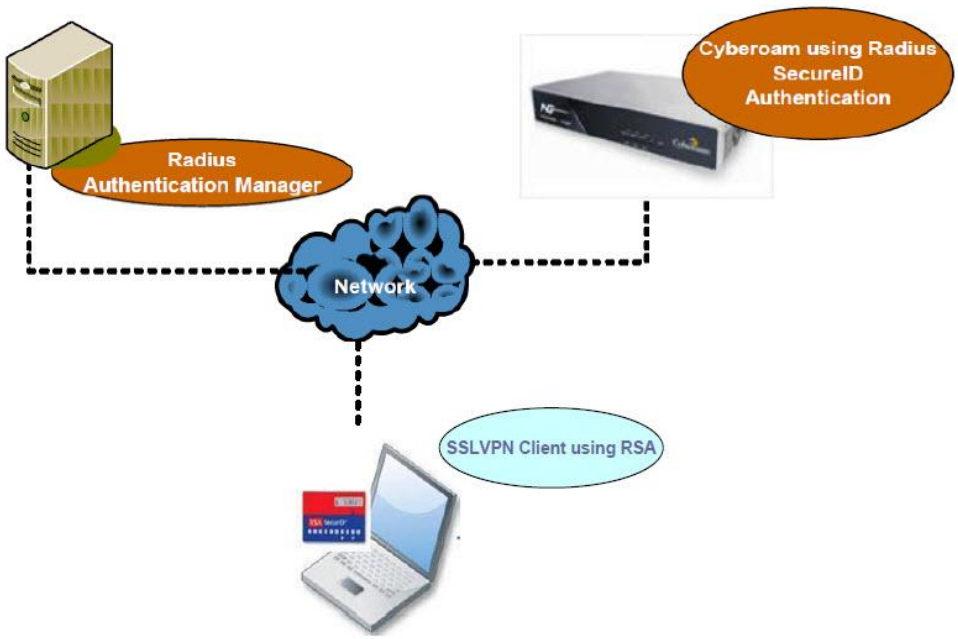
Partner Information

Product Information	
Partner Name	Cyberoam Technologies Pvt Ltd
Web Site	www.cyberoam.com
Product Name	Cyberoam
Version & Platform	10.04.4
Product Description	Cyberoam UTM delivers enterprise-class network security with stateful inspection firewall, VPN and IPS, offering the Human Layer 8 identity-based controls and Layer 7 application controls. It ensures high levels of network security, network connectivity, continuous availability and secure remote access with controlled network access to road warriors, telecommuters, partners, customers. With granular controls and advanced networking features, Cyberoam UTM appliances offer enterprise-class security and high flexibility with protection against blended threats, malware, Trojans, DoS, DDoS, IP spoofing attacks, spam, intrusions and data leakage.

Solution Summary

Cyberoam units can be configured to communicate with RSA Authentication Manager through the RADIUS protocol. This integration enables strong two factor authentication for users accessing protected.

RSA SecurID supported features	
Partner Product Cyberoam and 10.04.4	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes



RSA Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Cyberoam will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Cyberoam to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

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 documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Cyberoam with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

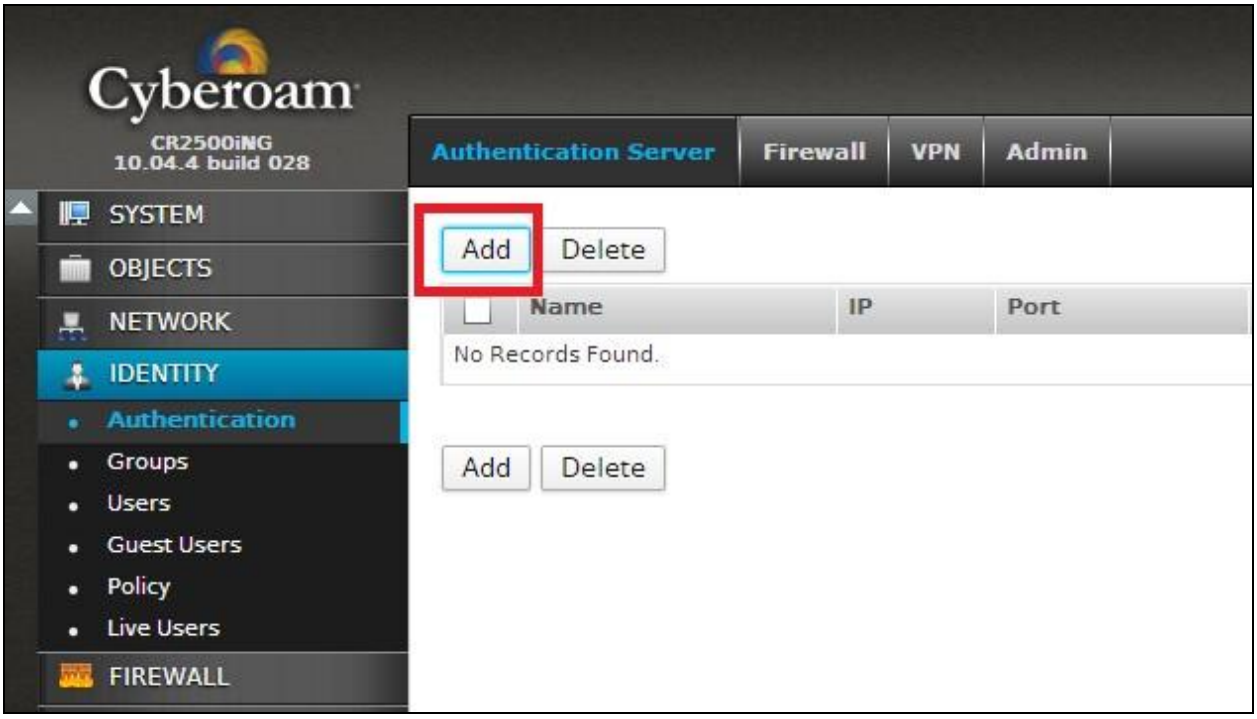
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

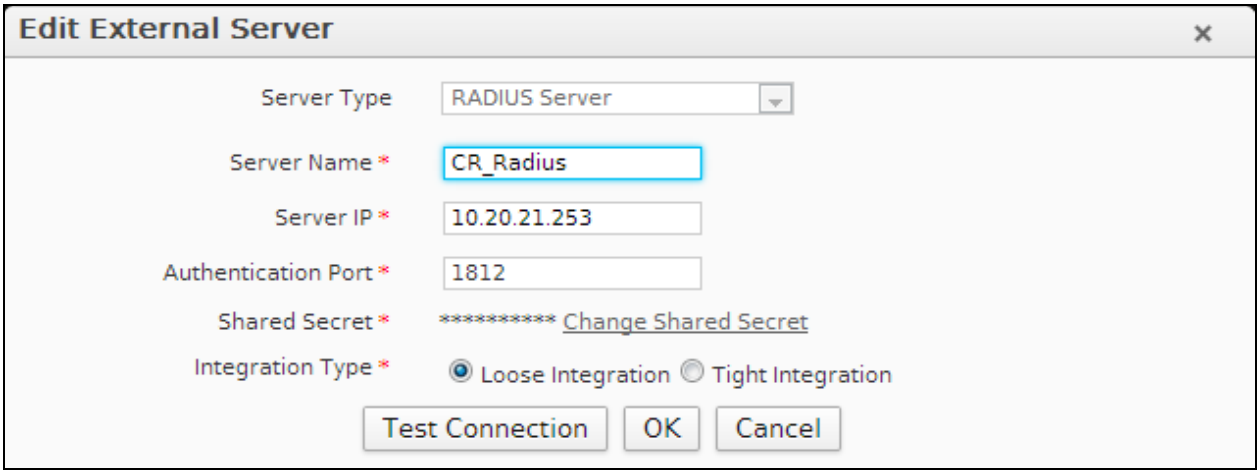
Configure Cyberoam for RADIUS

1. Login to the Cyberoam configuration GUI.
   http://<IPAddress of Cyberoam>/

2. Go to **Identity > Authentication > Authentication Server** and click **Add.**



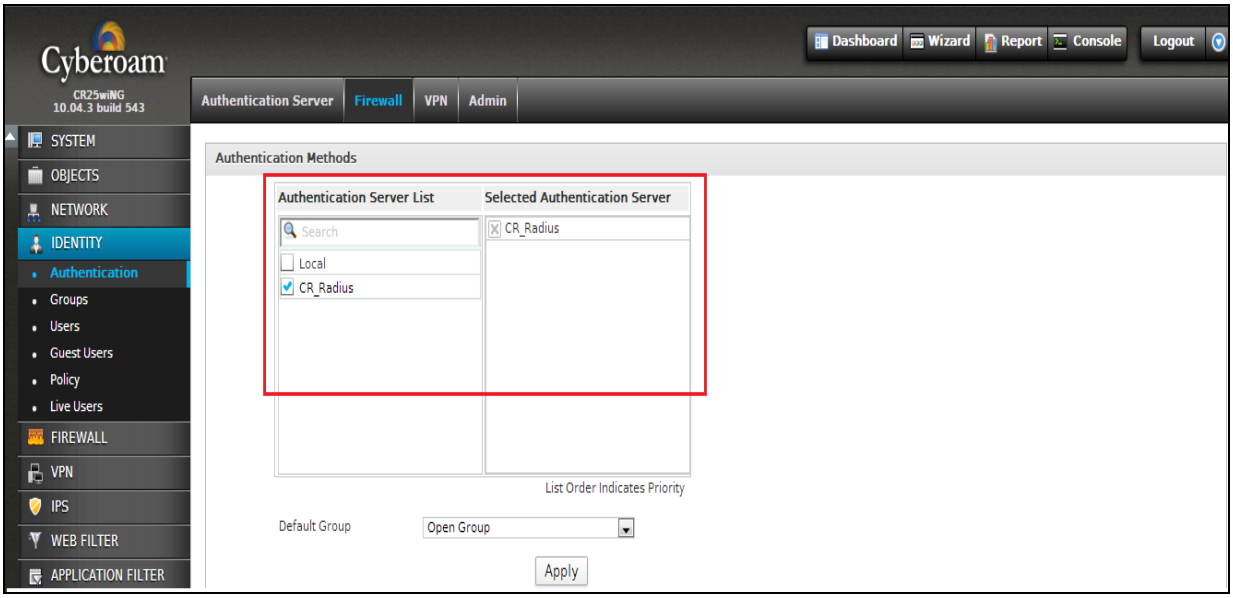
3. Select the Server Type **RADIUS Server** from the pull down list.
4. Enter the **Server Name**, **Server IP**, **Authentication Port**, and **Shared Secret**.
5. Choose the Integration Type **Loose Integration.**



6. Click **OK** to save the configuration.

Enable RADIUS on Firewall

1. Go to **Identity > Authentication.**
2. Click the **Firewall** tab and select **CR_RADIUS** as preferred authentication server.

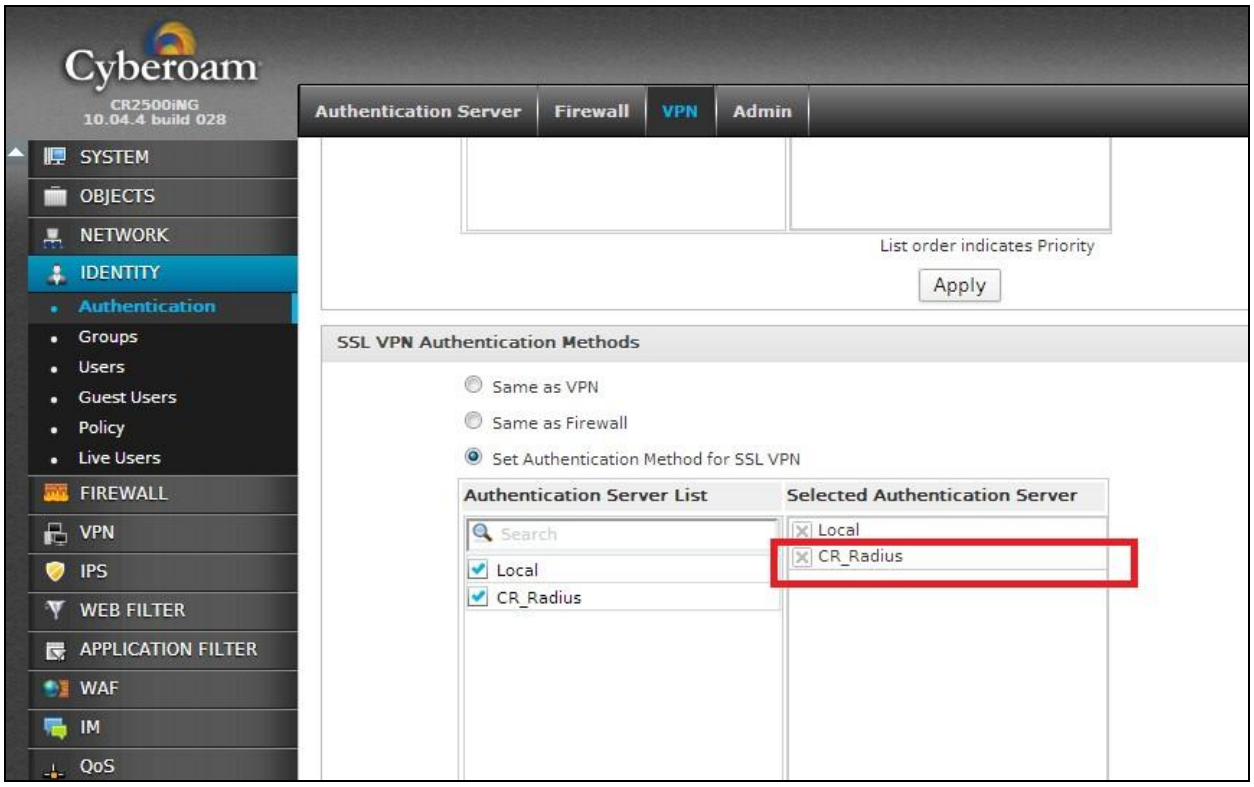


Note: In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication Server List.

3. Click **Apply**.
4. The Captive Portal at **http://<ipaddress of cyberoam>:8090** is now protected by SecurID via RADIUS.

Enable RADIUS on VPN

1. Go to **Identity > Authentication.**
2. Click the **VPN** tab **.**
3. Under **SSL VPN Authentication Methods** select **CR_RADIUS** as preferred authentication server.

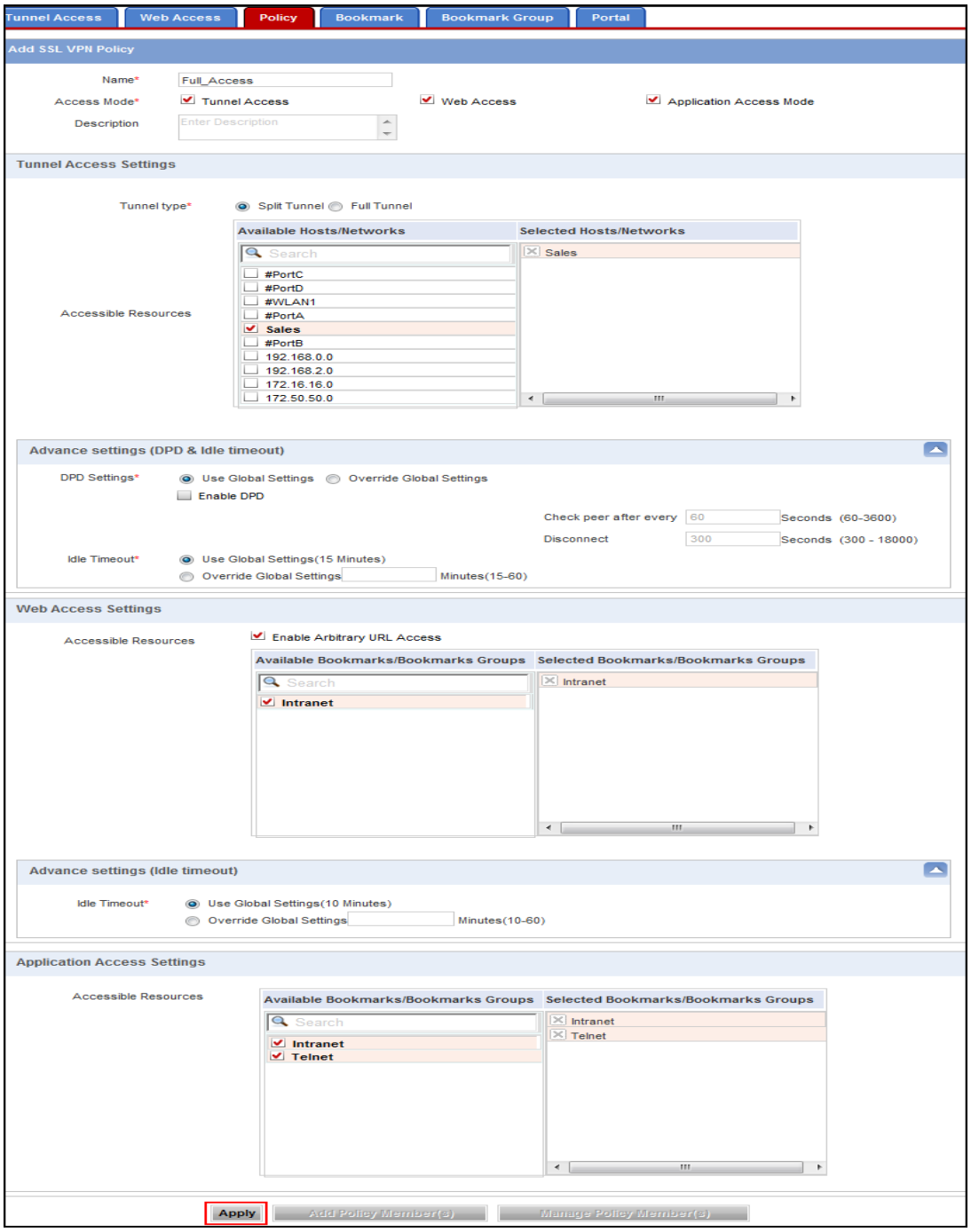


Note: In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication Server List.

4. Click **Apply**.

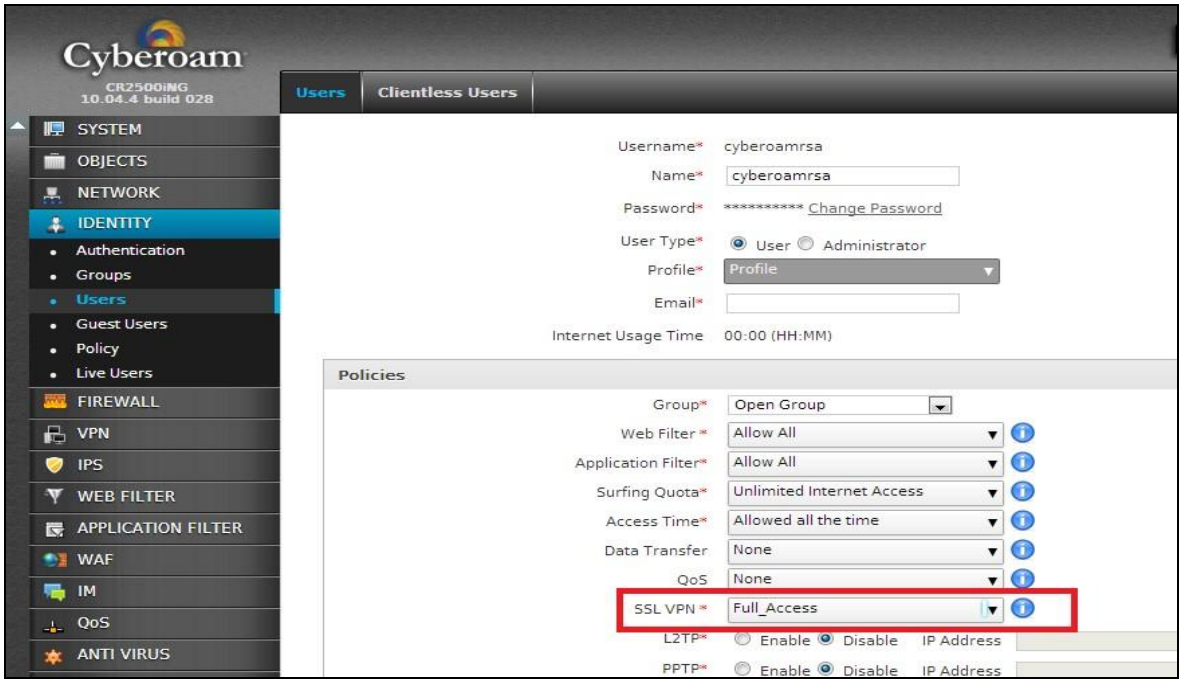
Configure SSL VPN Policy

1. Go to **VPN > SSL** and click the **Policy** tab.
2. Click **Add** and complete the required fields.
3. Click **Apply**.

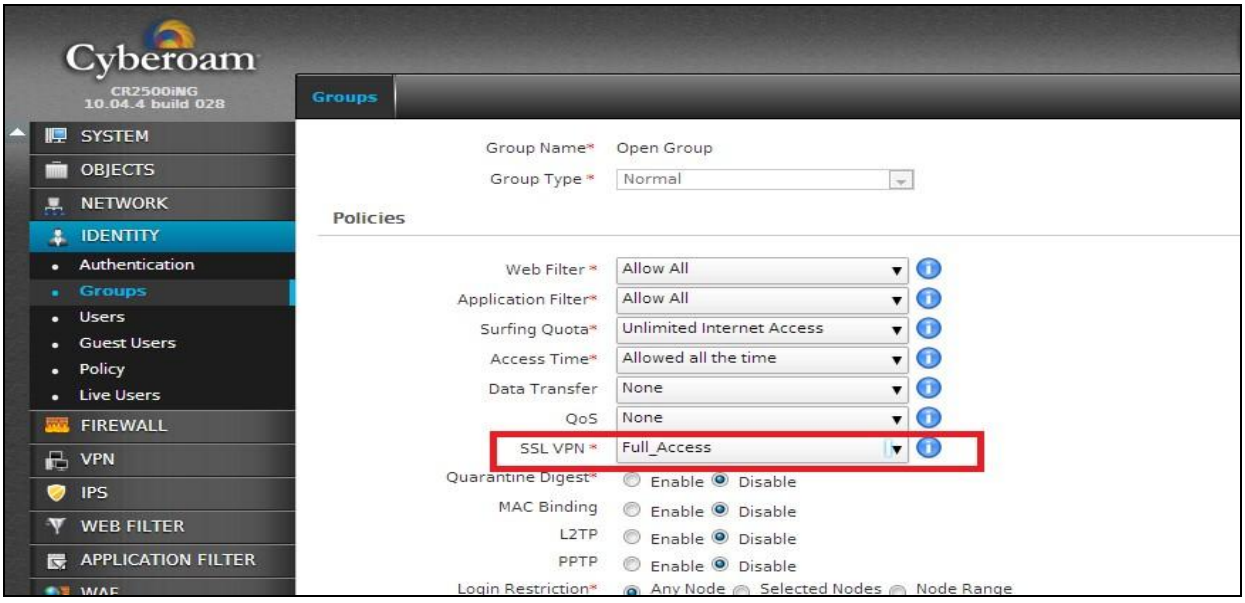


Apply SSL VPN Policy on User & Group

1. Go to **Identity > Users** and click the **Users** tab.
2. Select the user to which the policy is to be applied.
3. Select the policy for the user from the pull down list in the **SSL VPN** field.



4. Go to **Identity > Groups** and click the **Groups** tab.
5. Select the group to which the policy is to be applied.
6. Select the policy for the group from the pull down list in the **SSL VPN** field.



RSA SecurID Login Screens

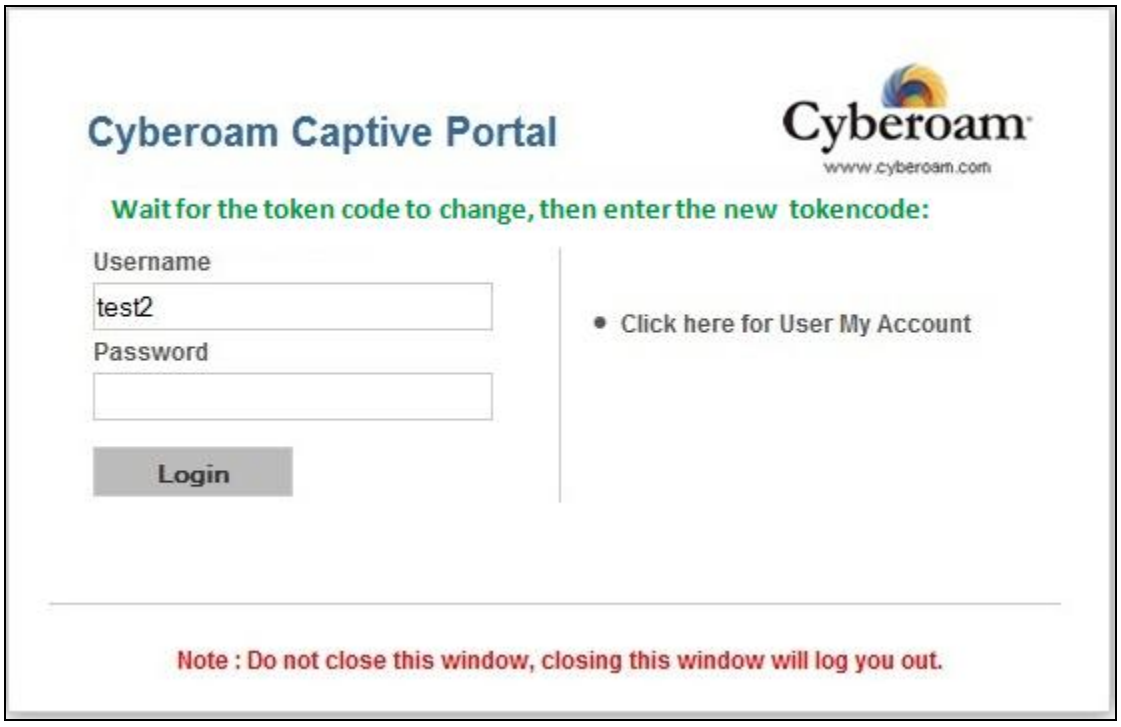
Cyberoam Captive Portal

Login screen:

User-defined New PIN:

System-generated New PIN:

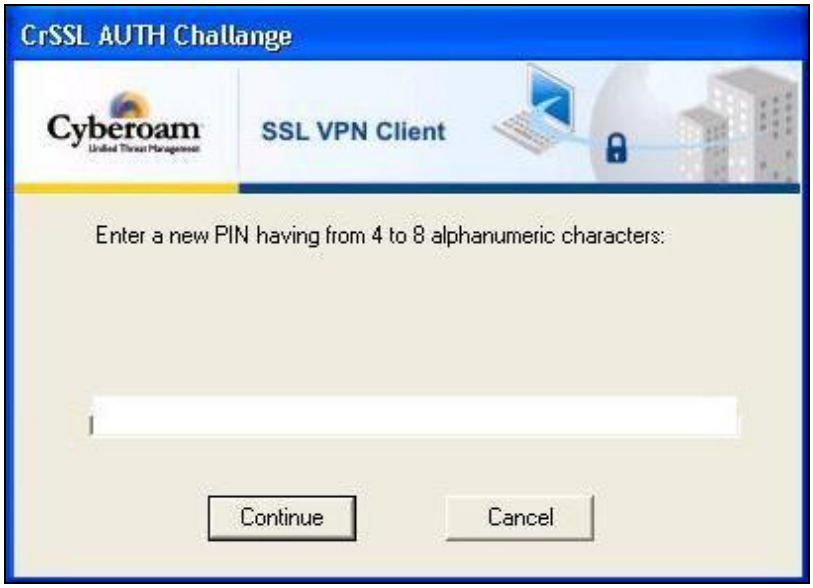
Next Tokencode:



Cyberoam SSL VPN

Login screen:

User-defined New PIN:



System-generated New PIN:

Next Tokencode:

Certification Checklist for RSA Authentication Manager

Date Tested: September 26, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cyberoam	10.04.3	UTM Appliance
Cyberoam SSL VPN Client	1.3.0	Windows

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	✓
Deny PIN Reuse	N/A	Deny 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	✓
On-Demand Authentication			
On-Demand Authentication	N/A	On-Demand Authentication	✓
On-Demand New PIN	N/A	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

GLS / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix: Provisioning of Tight-integration

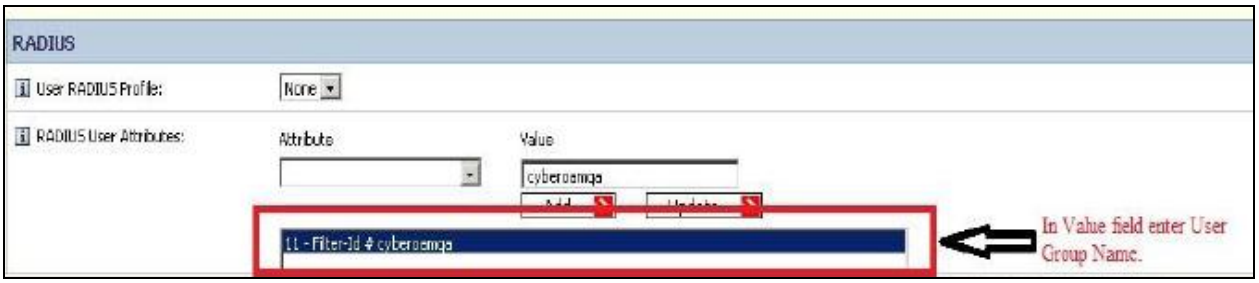
RSA Configuration

RSA Authentication Manager RADIUS file

1. Open **C:\Programfiles\RSA security\Radius\radius.ini**.
2. Edit the file and under [Configuration] add attribute **AunthenticateOnly = 0**.
3. Save the changes and Restart the Radius service.

RSA Authentication Manager Users

1. Open RSA Security Console.
2. Go to **Identity > Users > Manage Exiting**.
3. Click on **Search** and select **User > Authentication Setting**.
4. Edit the User account, under the RADIUS section add Radius Attribute “Filter-id”.
5. Set the Filter-id value to “Group Name”.
6. Click **Save**.



Note Please refer to the appropriate RSA documentation for additional information.

Cyberoam Configuration

Cyberoam RADIUS Configuration