How to Configure RSA-ACE SecurID Authentication

https://campus.barracuda.com/doc/96026628/

RSA-ACE is a commonly used two-factor authentication method for the authentication of network and VPN users. When authenticating with an RSA-ACE server, users can sign in with the username and password, consisting of PIN and RSA SecurID provided by a token.

Before You Begin

RSA-ACE does not provide group information. To create groups, follow the instructions given in How to Configure Explicit Groups.

For authentication against the Barracuda CloudGen Firewall using an RSA-ACE authentication server, verify that the **Clear Node Secret** is properly set:
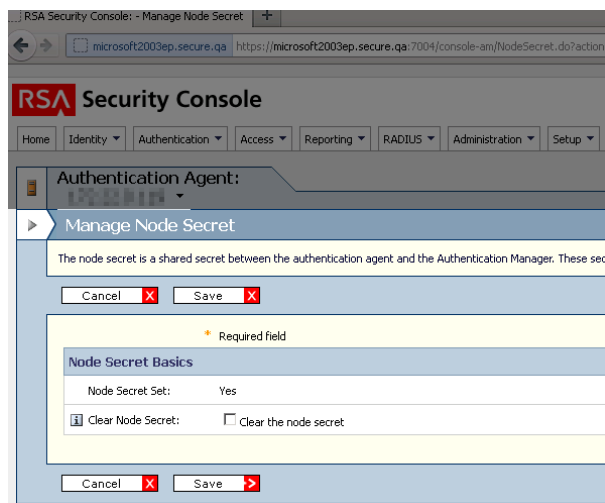
Step 1. Configure the RSA-ACE Server

Before configuring RSA-ACE authentication, you must prepare the RSA-ACE server:

1. Create an **Agent Host** and add the users who want to authenticate over the Barracuda CloudGen Firewall.
   The hostname must be DNS resolvable (Box IP address of the Barracuda CloudGen Firewall and ACE-Server IP address). Time on the Barracuda CloudGen Firewall must be the same as on the ACE server.
   ○ **Encryption** = DES
   ○ **Type** = Unix Agent
2. **Assign Acting Server**.
3. Export the configuration to insert it in the **RSA-ACE Authentication** configuration as explained

in Step 2.

Users who want to authenticate over proxy must be authenticated for the first time not over the Barracuda CloudGen Firewall because the PIN number validation is not supported.

If you want to use RSA-ACE authentification in a High Availability cluster, you have to configure both CloudGen Firewalls as separate nodes on the RSA-ACE server.

Step 2. Configure RSA-ACE Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **RSA-ACE Authentication**.
3. Click **Lock**.
4. Enable RSA-ACE as external directory service.
5. In the **RSA Configuration File** section, import the configuration file that is provided by the RSA SecurID server (sdconf.rec).
6. Enter the IP address of the RSA server.
7. In the **DNS Resolved IP** field, enter the IP address that is used to connect to the RSA server. This IP address must match the configured client IP address that the server has; otherwise, the connection is refused.
8. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list.
9. Click **Send Changes** and **Activate**.

RSA-ACE SecurID Authentication Through the Remote Management Tunnel

To allow remote CloudGen Firewalls to connect to the authentication server through the remote management tunnel, you must activate the outbound **BOX-AUTH-MGMT-NAT** Host Firewall rule. By default, this rule is disabled.

Figures

1. rsa-ace.png