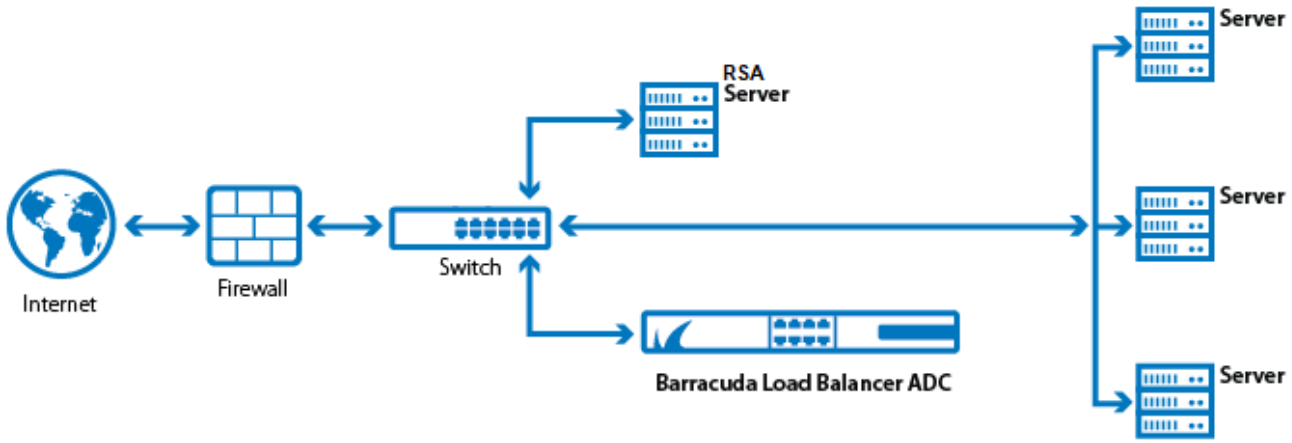
How to Configure the RSA Authentication Service on the Barracuda Load Balancer ADC

You can integrate an RSA Authentication Manager/RSA SecurID server with a Barracuda Load Balancer ADC as shown in Figure 1. An RSA Server can be used to authenticate clients attempting to access the web servers load balanced by the Barracuda Load Balancer ADC. RSA provides a high degree of authentication security, helping to ensure that only valid clients can access the protected servers.

Figure 1. RSA Server integrated with the Load Balancer ADC in a one-armed topology.



Before you complete this procedure, you should first configure the RSA Authentication Manager. See How to Configure the RSA Authentication Manager.

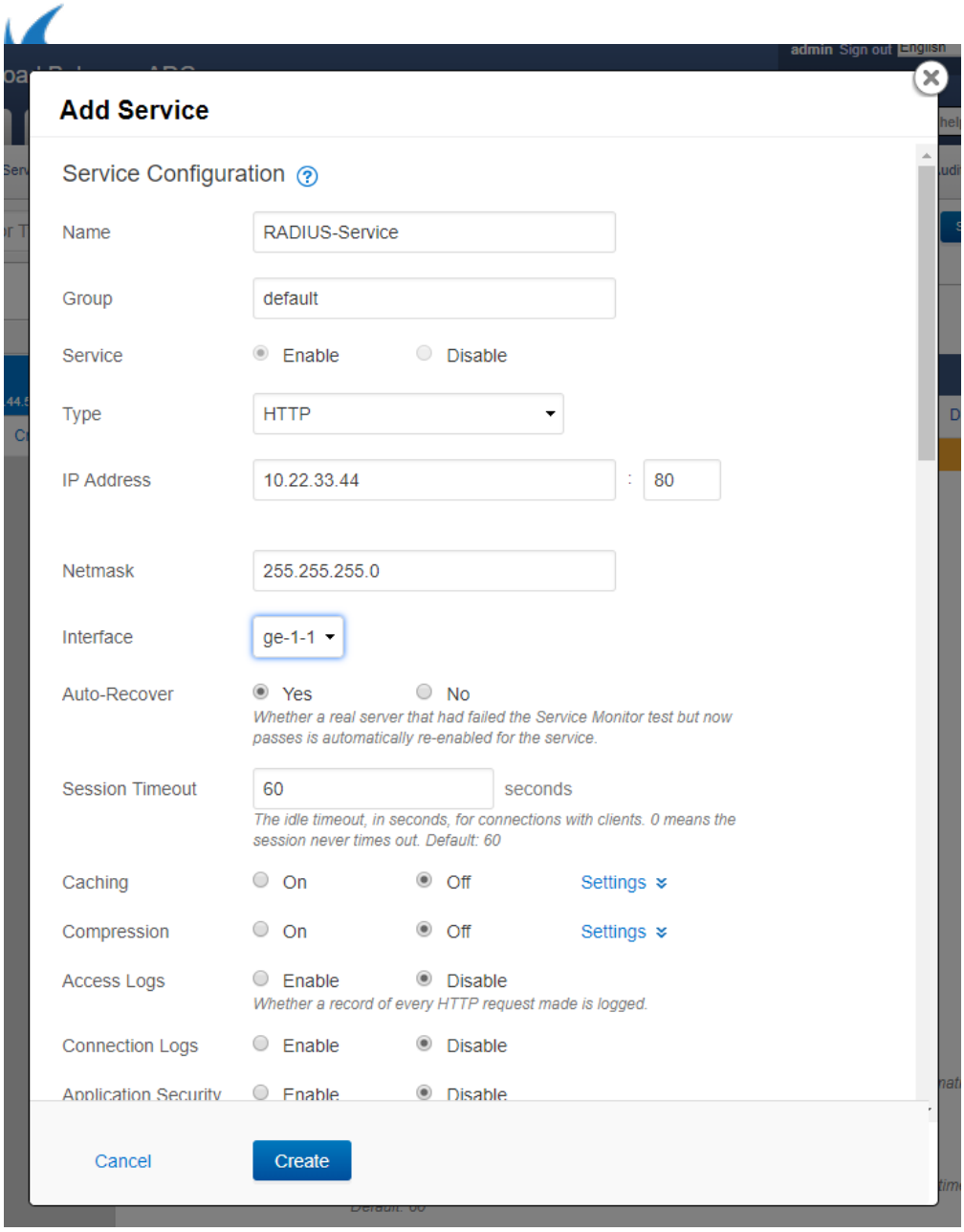
Configuring the Barracuda Load Balancer ADC for SecurID Authentication

The following configuration steps enable the Barracuda Load Balancer ADC to communicate using the RADIUS protocol with the RSA Authentication Manager to authenticate users:

Step 1: Create an HTTP Service on the Barracuda Load Balancer ADC

1. Log into the Barracuda Load Balancer ADC using a supported web browser.
2. Go to **BASIC > Services** and click **Add Service.**
3. In the **Add Service** user interface, select *HTTP* from the **Type** list and specify the service as required. Click the **Help** icon for an explanation of the other settings.
4. Click **Create**.

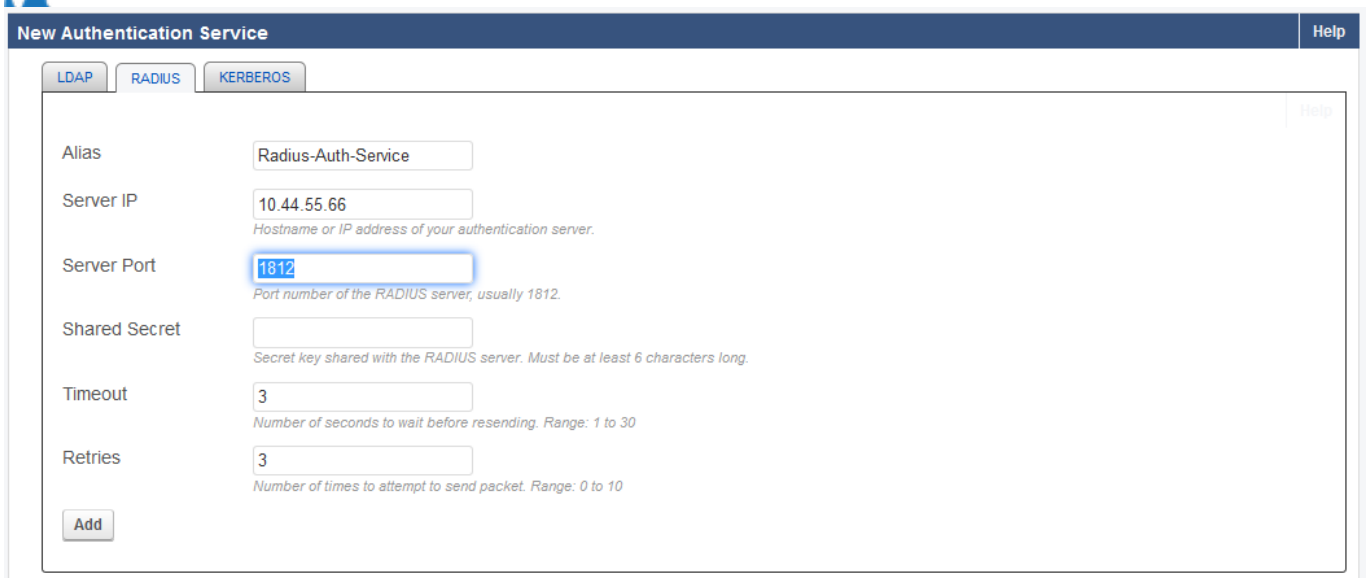
Figure 2. Create a New HTTP Service



Step 2: Add the RSA SecurID Server as an Authentication Service on the Barracuda Load Balancer ADC

1. Go to **ACCESS CONTROL > Authentication Services** and click the **RADIUS** tab (see Figure 3).
2. For the **Server IP**, specify the IP address of the RSA RADIUS server used for authenticating users.
3. The **Server Port** should be the port number of the RSA RADIUS server. The standard port numbers used by RADIUS are 1812 or 1645.
4. Specify the appropriate values for other parameters and click **Add**. For more information about the other configuration options, click **Help**.

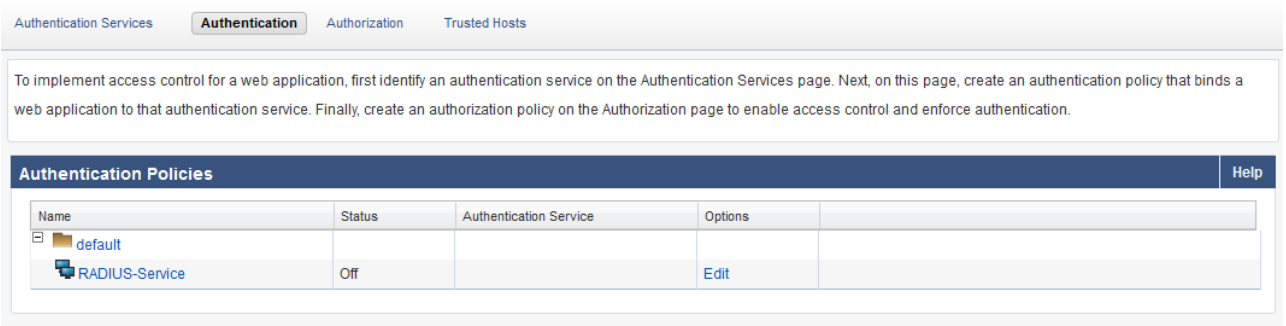
Figure 3. Configure RADIUS Authentication Service



Step 3: Associate the RADIUS Authentication Service with a Service on the Barracuda Load Balancer ADC

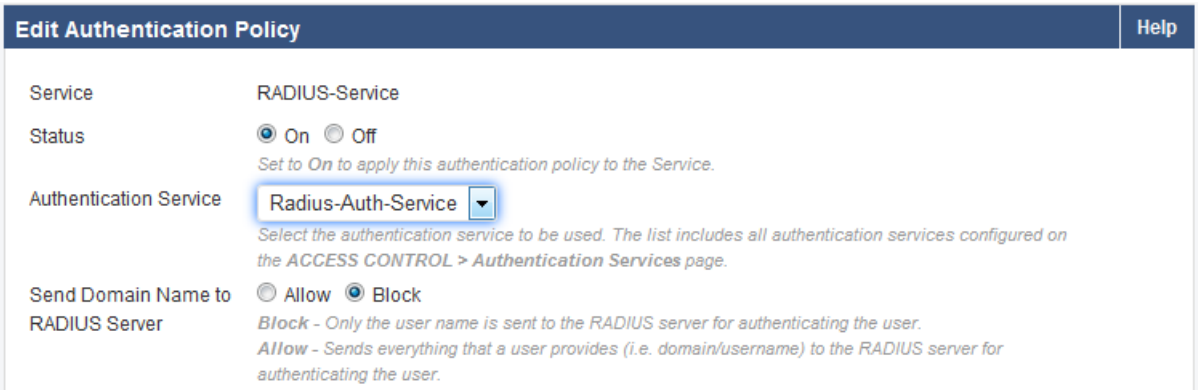
1. From the **ACCESS CONTROL** tab, select the **Authentication** page.
2. Under the **Authentication Policies** section, click **Edit** next to the Service requiring RSA SecurID authentication as shown in Figure 4.

Figure 4. Authentication



3. On the **Edit Authentication Policy** window:
    1. Set **Status** to *On* to enable authentication for the Service.
    2. From the **Authentication Service** list, select the RSA authentication service created in Step 2: Add the RSA SecurID Server as an Authentication Service on the Barracuda Load Balancer ADC as shown in Figure 5.

Figure 5. Configuring Authentication Policy



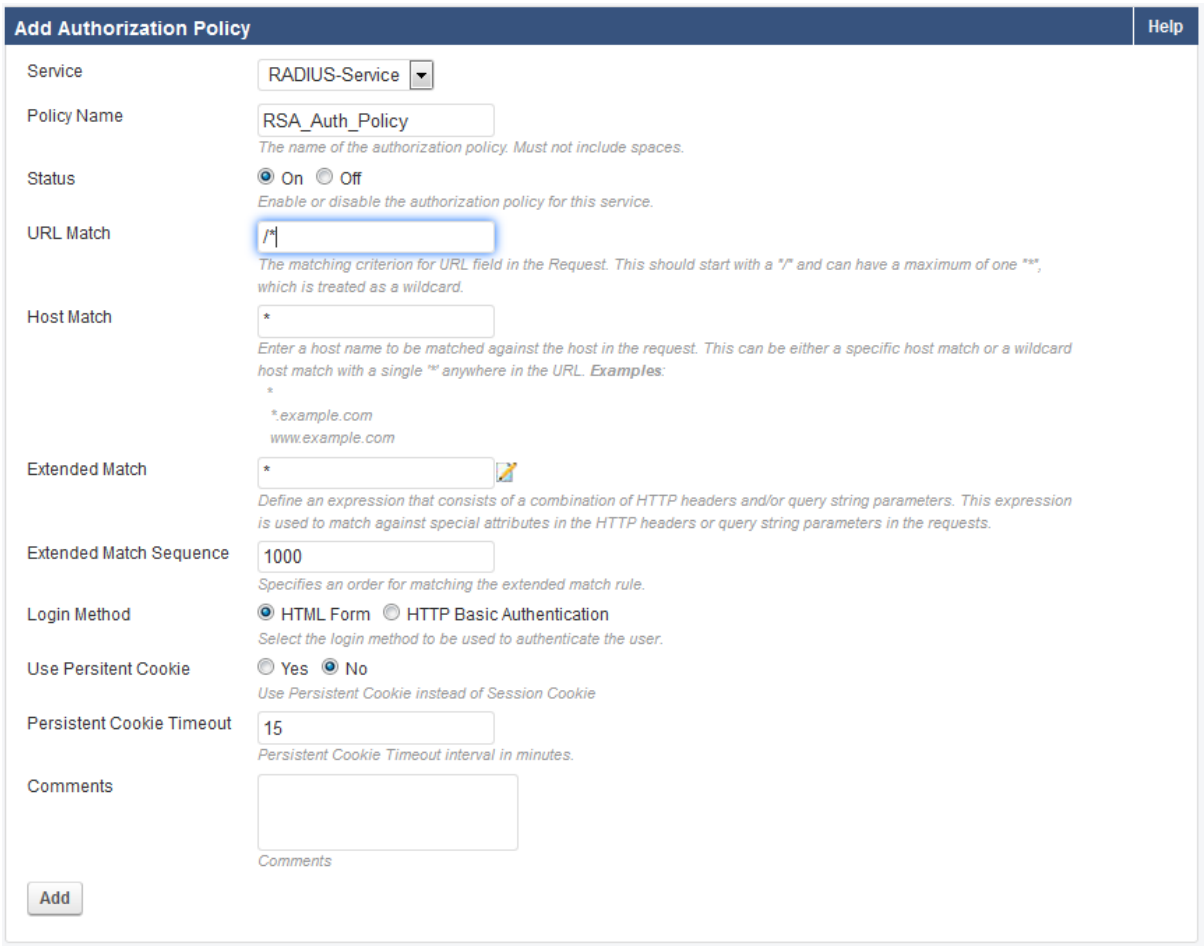
    3. Specify values for other parameters as needed and click **Save**. For more information on how to

configure authentication policies, click **Help**.

Step 4: Configure the Authorization Policy for the Service

1. Go to **ACCESS CONTROL > Authorization**.
2. In the **Add Authorization Policy** section, specify the following (see Figure 6):
   - Select the **Service** specified in Step 1: Create an HTTP Service on the Barracuda Load Balancer ADC.
   - **Policy Name** – Enter a name for the authorization policy.
   - Set **Status** to *On*.
   - Configure the other parameter(s) as needed and click **Add**. For more information on how to configure authorization policies, click **Help**.

Figure 6. Configuring Authorization Policy



When there is an attempt to access a protected resource, the Barracuda Load Balancer ADC presents a login page to authenticate the user. If **URL Match** is configured as /*, a login page displays for any request sent to the Service.

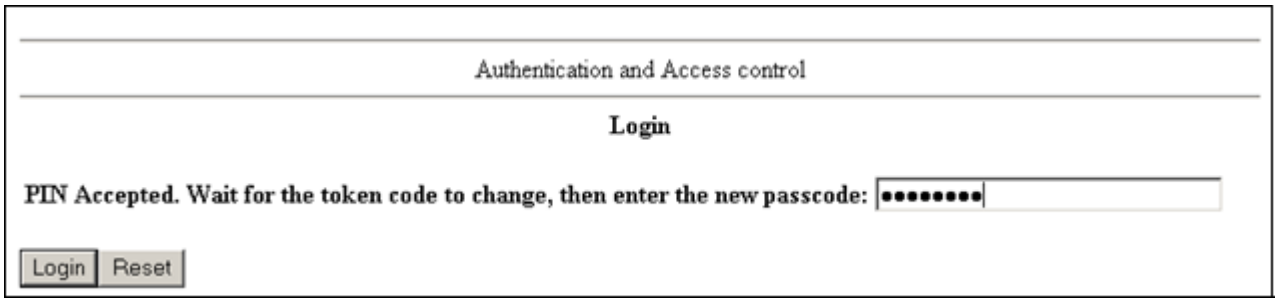
Verifying the End-User Login Procedure

Using a supported web browser, navigate to the URL for the services managed by the Barracuda Load Balancer ADC. To receive authorization to view the protected resource, a user must authenticate using RSA SecurID. To begin the authentication process, the user must enter a User Name and Password on the *Login* form.

The user is then presented with a New PIN challenge.

The user is challenged again to confirm the PIN.

When the new PIN is accepted, after entering the new passcode, the user is successfully authenticated and forwarded to the requested URL.



Figures