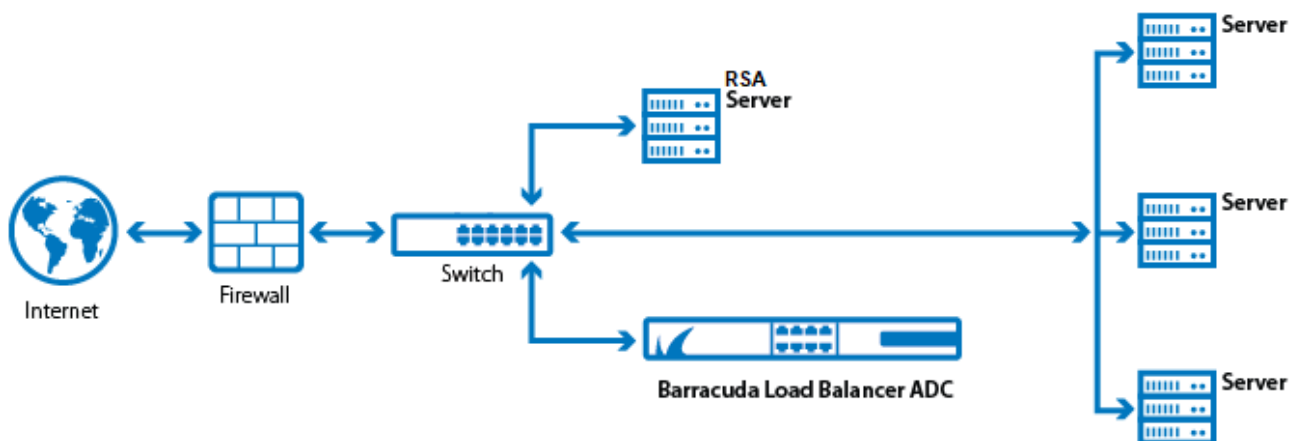


How to Configure the RSA Authentication Service on the Barracuda Load Balancer ADC

<https://campus.barracuda.com/doc/74548626/>

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

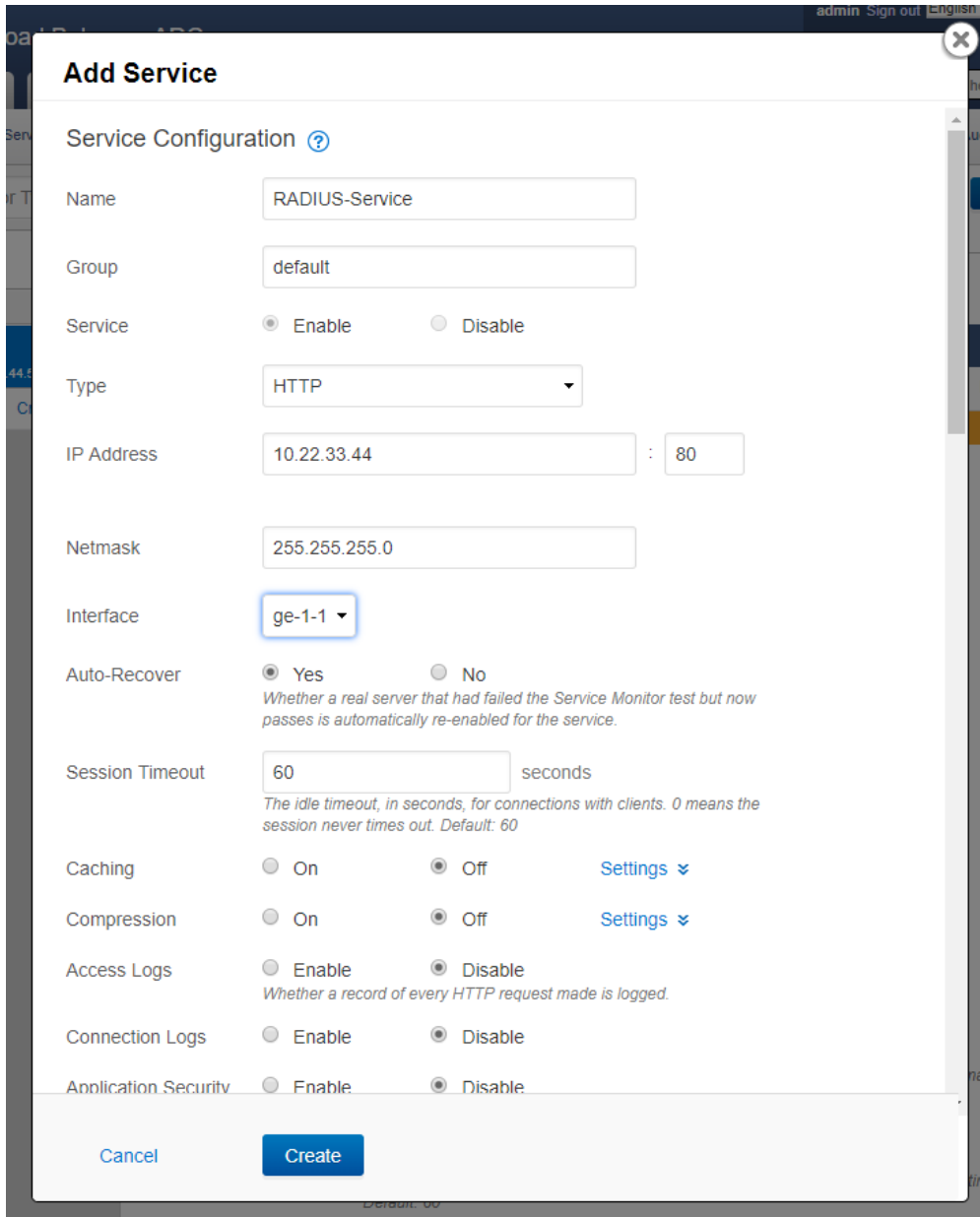
The following configuration steps enable the Barracuda Load Balancer ADC to communicate using the RADIUS protocol with the RSA Authentication Manager to authenticate users:

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



Add Service

Service Configuration ?

Name: RADIUS-Service

Group: default

Service: ☒ Enable ☐ Disable

Type: HTTP

IP Address: 10.22.33.44 : 80

Netmask: 255.255.255.0

Interface: ge-1-1

Auto-Recover: ☒ Yes ☐ No
Whether a real server that had failed the Service Monitor test but now passes is automatically re-enabled for the service.

Session Timeout: 60 seconds
The idle timeout, in seconds, for connections with clients. 0 means the session never times out. Default: 60

Caching: ☐ On ☒ Off [Settings](#)

Compression: ☐ On ☒ Off [Settings](#)

Access Logs: ☐ Enable ☒ Disable
Whether a record of every HTTP request made is logged.

Connection Logs: ☐ Enable ☒ Disable

Application Security: ☐ Enable ☒ Disable

[Cancel](#) [Create](#)

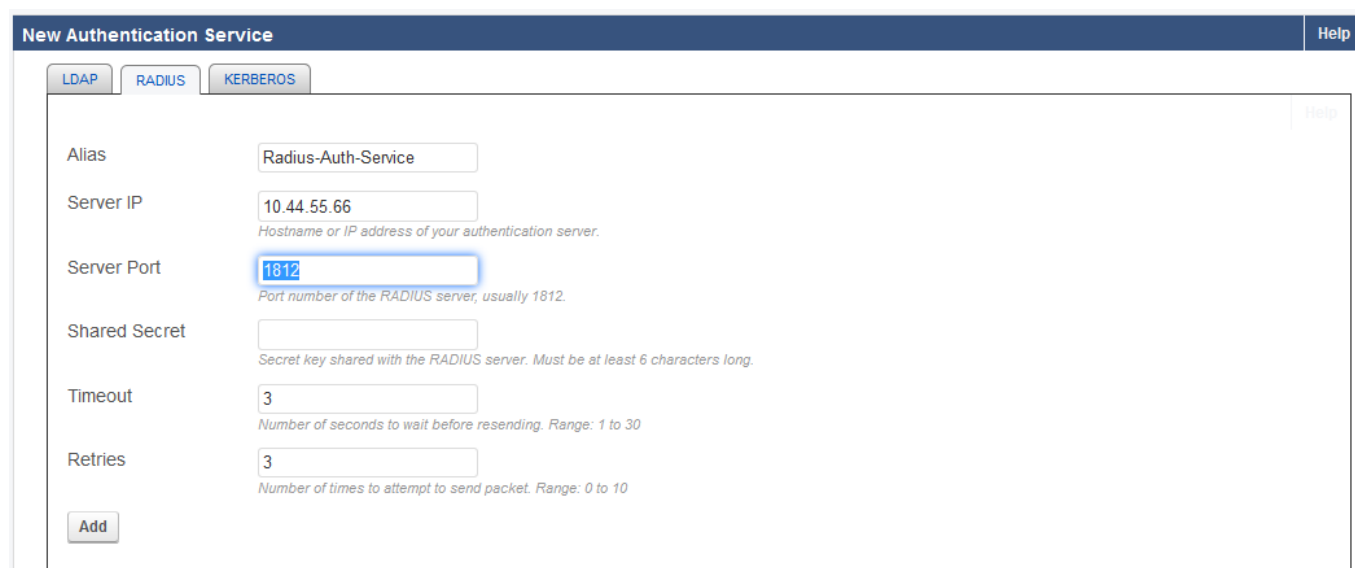
Step 2: Add the RSA SecurID Server as an Authentication Service on the Barracuda Load Balancer ADC

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



New Authentication Service Help

LDAP **RADIUS** **KERBEROS**

Alias: Radius-Auth-Service

Server IP: 10.44.55.66
Hostname or IP address of your authentication server.

Server Port: 1812
Port number of the RADIUS server, usually 1812.

Shared Secret:
Secret key shared with the RADIUS server. Must be at least 6 characters long.

Timeout: 3
Number of seconds to wait before resending. Range: 1 to 30

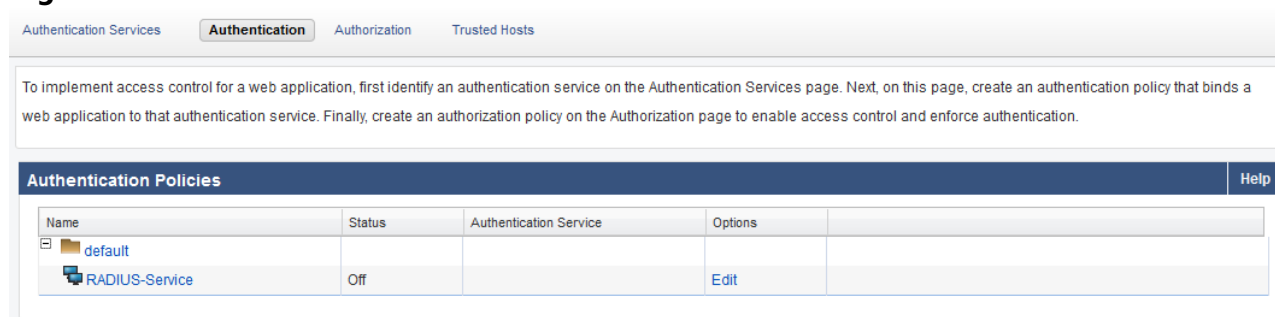
Retries: 3
Number of times to attempt to send packet. Range: 0 to 10

Add

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



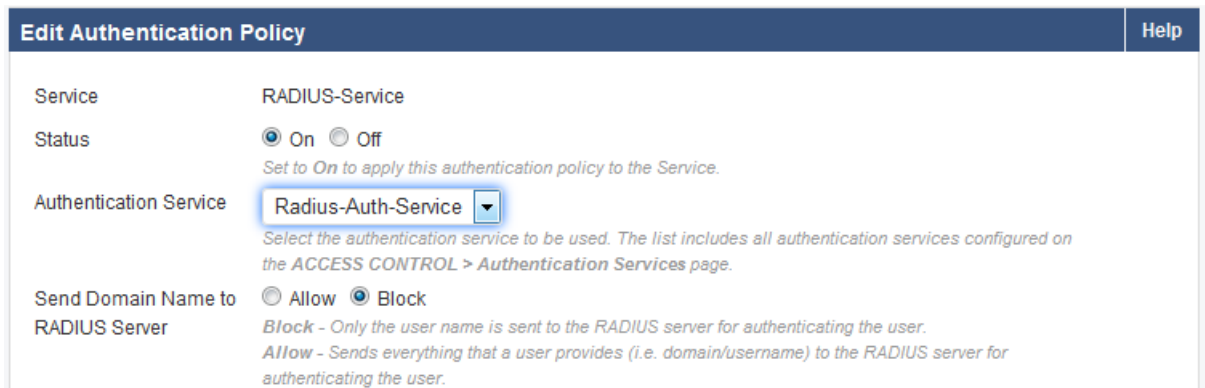
Authentication Services **Authentication** **Authorization** **Trusted Hosts**

To implement access control for a web application, first identify an authentication service on the Authentication Services page. Next, on this page, create an authentication policy that binds a web application to that authentication service. Finally, create an authorization policy on the Authorization page to enable access control and enforce authentication.

Name	Status	Authentication Service	Options	
default				
RADIUS-Service	Off		Edit	

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



Service	RADIUS-Service
Status	<input checked="" type="radio"/> On <input type="radio"/> Off <i>Set to On to apply this authentication policy to the Service.</i>
Authentication Service	Radius-Auth-Service <i>Select the authentication service to be used. The list includes all authentication services configured on the ACCESS CONTROL > Authentication Services page.</i>
Send Domain Name to RADIUS Server	<input type="radio"/> Allow <input checked="" type="radio"/> Block <i>Block - Only the user name is sent to the RADIUS server for authenticating the user. Allow - Sends everything that a user provides (i.e. domain/username) to the RADIUS server for authenticating the user.</i>

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

Add Authorization Policy Help

Service	<div>RADIUS-Service</div>
Policy Name	<div>RSA_Auth_Policy</div> <div>The name of the authorization policy. Must not include spaces.</div>
Status	<div><input checked="" type="radio"/> On <input type="radio"/> Off</div> <div>Enable or disable the authorization policy for this service.</div>
URL Match	<div><div>/</div></div> <div>The matching criterion for URL field in the Request. This should start with a "/" and can have a maximum of one "**", which is treated as a wildcard.</div>
Host Match	<div><div>*</div></div> <div>Enter a host name to be matched against the host in the request. This can be either a specific host match or a wildcard host match with a single "*" anywhere in the URL. Examples: * *.example.com www.example.com</div>
Extended Match	<div><div>*</div></div> <div>Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests.</div>
Extended Match Sequence	<div><div>1000</div></div> <div>Specifies an order for matching the extended match rule.</div>
Login Method	<div><input checked="" type="radio"/> HTML Form <input type="radio"/> HTTP Basic Authentication</div> <div>Select the login method to be used to authenticate the user.</div>
Use Persistent Cookie	<div><input type="radio"/> Yes <input checked="" type="radio"/> No</div> <div>Use Persistent Cookie instead of Session Cookie</div>
Persistent Cookie Timeout	<div><div>15</div></div> <div>Persistent Cookie Timeout interval in minutes.</div>
Comments	<div></div> <div>Comments</div>

Add

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.

Authentication and Access control

Login

Please provide your username and password to access restricted applications.

User Name:

Password:

Login Reset

The user is then presented with a New PIN challenge.

Authentication and Access control

Login

Please re-enter new PIN:

Login Reset

The user is challenged again to confirm the PIN.

Authentication and Access control

Login

Please re-enter new PIN:

Login Reset

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

Authentication and Access control

Login

PIN Accepted. Wait for the token code to change, then enter the new passcode:

Login Reset

Figures

1. rsa_server_topology.png
2. radius-service-add.png
3. RADIUS_Authentication_Service.png
4. RADIUS_Authentication_Policy.png
5. Edit_Authentication_Policy.png
6. add_auth_policy.png
7. RSA_User_Name.png
8. RSA_PIN.png
9. RSA_PIN.png
10. RSA_PIN_Accepted.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.