RSA SecurID Implementation

https://campus.barracuda.com/doc/4259850/

Partner Information

Product Information	
Partner Name	Barracuda Networks
Website	*www.barracuda.com*
Product Name	Barracuda Web Application Firewall
Version & Platform	x60 Series
Product Description	The Barracuda Web Application Firewall protects web applications and web services from malicious attacks, and can also increase the performance and scalability of these applications. The Barracuda Web Application Firewall offers every capability needed to deliver, secure, and manage enterprise web applications from a single appliance through an intuitive, real-time user interface.
Product Category	Network Firewalls

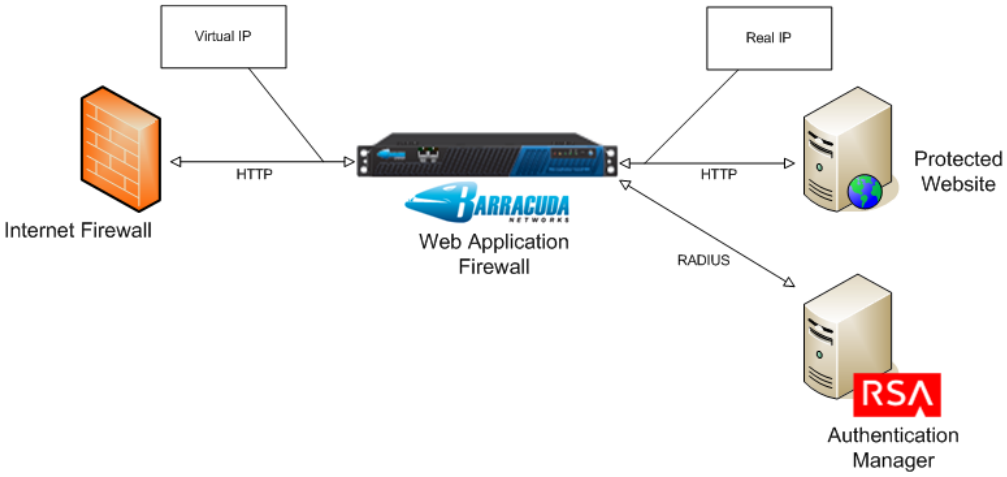
Solution Summary

The Barracuda Web Application Firewall protects your website from attackers leveraging protocol or application vulnerabilities to instigate unauthorized access, data theft, denial of service (DoS), or defacement of your website.

The Barracuda Web Application Firewall provides complete protection of web applications and enforces policies for both internal and external data security standards, such as the Payment Card Industry Data Security Standard (PCI DSS). In addition, the Barracuda Web Application Firewall features a number of traffic management capabilities to improve the performance, scalability, and manageability of the most modern and demanding data center infrastructures.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
RSA SecurID API Version	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes (1)
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users

RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No



Authentication Agent Configuration

All **Authentication Agent** types for 7.1 should be set to *Standard Agent*.

To facilitate communication between the Barracuda Web Application Firewall and the RSA Authentication Manager / RSA SecurID Appliance, an Authentication Agent Host record must be added to the RSA Authentication Manager database. The Authentication Agent Host record identifies the Barracuda Web Application Firewall within the RSA Authentication Manager database and contains information about communication and encryption. You will also need to configure a RADIUS client.

To create the Agent Host record, you will need the following information:

- Hostname
- IP addresses for all network interfaces

When adding the Agent Host Record, you should configure the Barracuda Web Application Firewall as *Standard Agent*. RSA Authentication Manager uses this setting to determine how to communicate with the Barracuda Web Application Firewall.

To create the RADIUS client record, you will need the following information:

- Hostname
- IP addresses for all network interfaces
- RADIUS secret

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 and RADIUS client records.

RSA SecurID Files

RSA SecurID Authentication Files
Files
aceclnt.dll
sdmsg.dll
sdconf.rec
Node Secret (securid)
sdstatus.12
sdopts.rec

Partner Product Configuration

Before You Begin

This section provides instructions for integrating partner products with RSA SecurID Authentication. This document does not necessarily suggest optimum installations or configurations.

You should have a working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should rely on product documentation for all relevant products to properly install the required components.

You should verify all vendor products/components are installed and working before proceeding.

Configuring the Barracuda Web Application Firewall for SecurID Authentication

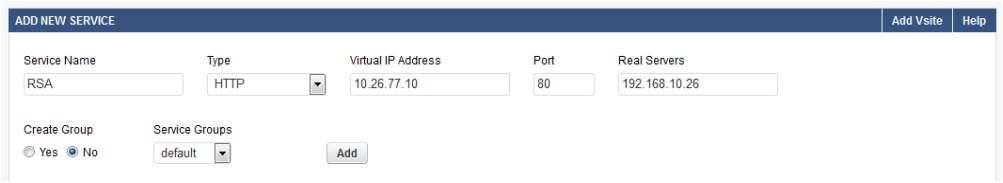
The following configuration steps enable the Barracuda Web Application Firewall to communicate via RADIUS protocol with the RSA Authentication Manager to authenticate users:

Step 1: Create an HTTP Service on the Barracuda Web Application Firewall

1. Log into the Barracuda Web Application Firewall using a supported web browser by navigating

to the web interface on port 443 (HTTPS).
2. From the **BASIC** tab, select the **Services** page.
3. In the **Add New Service** section, select *HTTP* from the **Type** list, and fill in other required information. Click **Help** on the **BASIC > Services** page for an explanation of other settings on this page.
4. Click **Add**.

Figure 1. Creating a New Service

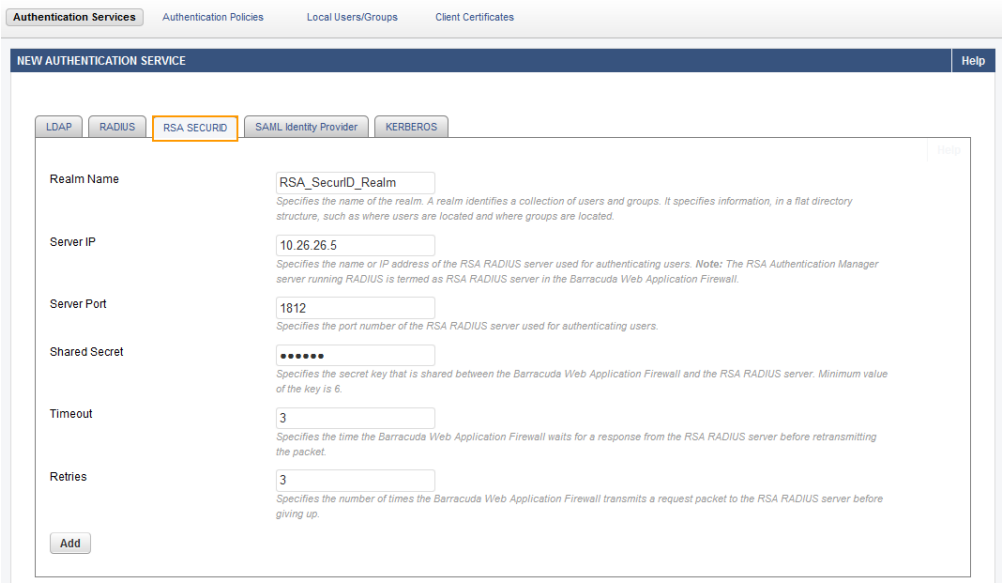


Step 2: Add the RSA SecurID Server as an Authentication Service on the Barracuda Web Application Firewall

The RSA Authentication Manager server running RADIUS is called an RSA RADIUS server in the Barracuda Web Application Firewall web interface

1. From the **ACCESS CONTROL** tab, select the **Authentication Services** page.
2. Select **RSA SecurID** under the **New Authentication Service** section. See Figure 2.
3. For the **Server IP**, specify the IP address of the RSA RADIUS server used for authenticating users.
4. The **Server Port** should be the port number of the RSA RADIUS server. The standard port number used for RADIUS is 1812 or 1645.
5. Specify appropriate values for other parameters and click **Add**. For more information, click **Help**.

Figure 2. Configure the RSA SECURID Authentication Service



Step 3: Associate the RSA SecurID Authentication Service with a Service on the Barracuda Web Application Firewall

1. From the **ACCESS CONTROL** tab, select the **Authentication Policies** page.
2. Under the **Authentication Policies** section, click **Edit Authentication** next to the Service requiring RSA SecurID 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 Web Application Firewall.
    3. Specify values for other parameter(s) as required, and click **Save**. For more information on how to configure an authentication policy, click the **Help** button. See Figure 4.

Figure 3. Authentication Page

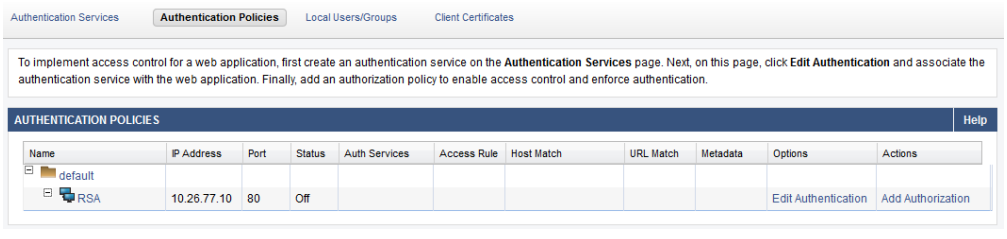
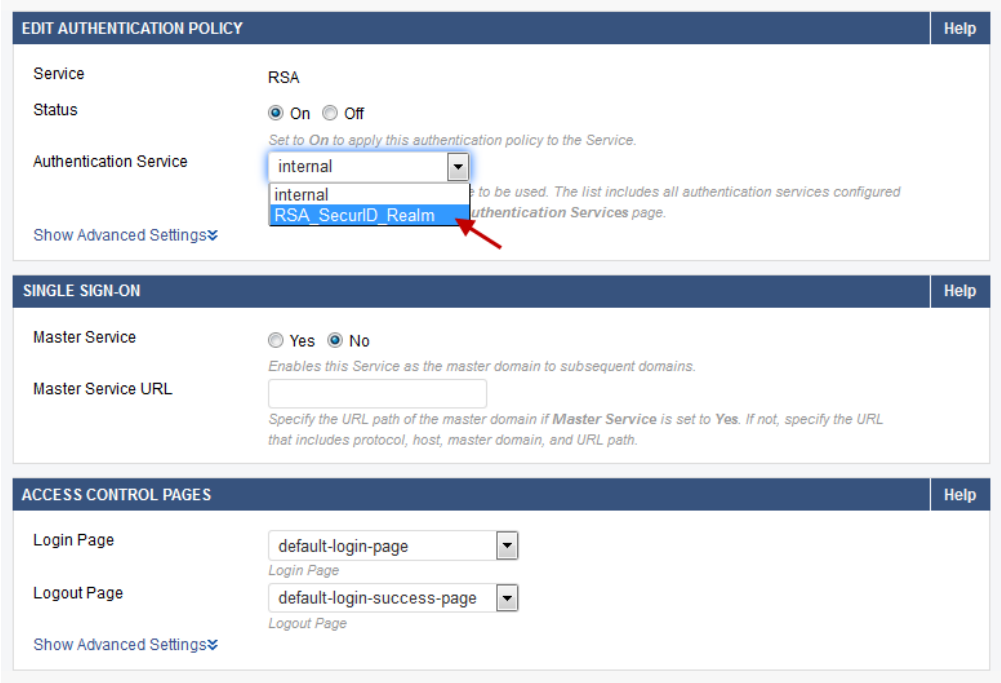


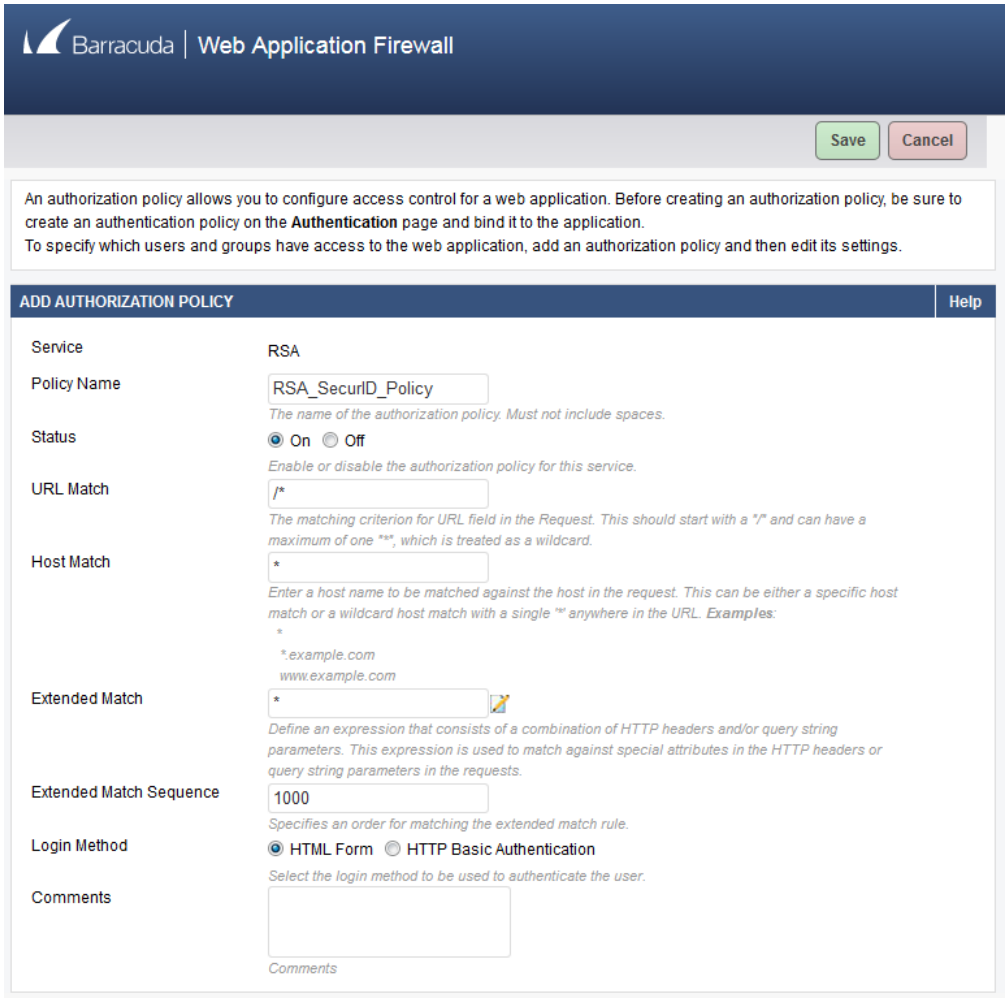
Figure 4. Configuring Authentication Policy



Step 4: Configure the Authorization Policy for the Service

1. From the **ACCESS CONTROL** tab, select the **Authorization Policies** page.
2. Under **Authentication Policies** section, click **Add Authorization** next to the service.
3. On the **Add Authorization Policy** window:
    1. **Policy Name** – Enter a name for the authorization policy.
    2. Set **Status** to *On*.
    3. Specify values for other parameter(s) as required, and click **Save**. For more information on how to configure an authorization policy, click the **Help** button.

Figure 5. Configuring Authorization Policy

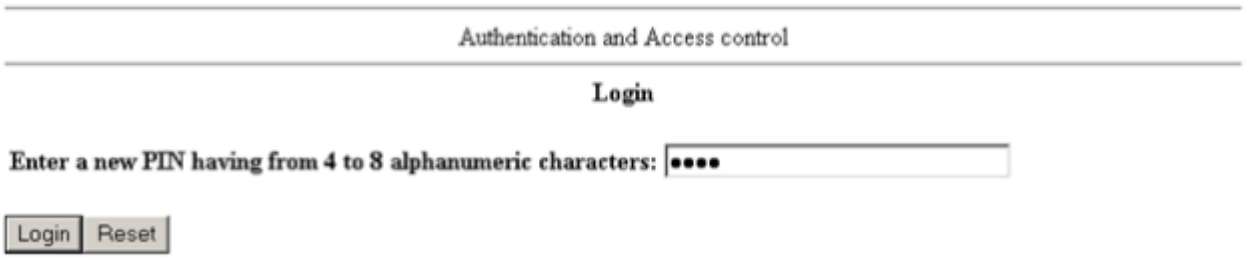


When there is an attempt to access a protected resource, the Barracuda Web Application Firewall presents a login page to authenticate the user. If **URL Match** is configured as /*, a login page displays for any request sent to the Service.

End-User Experience

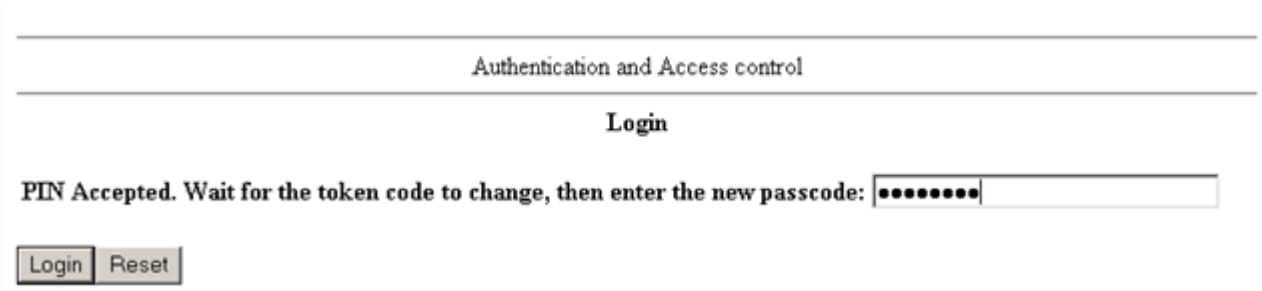
Using a supported web browser, navigate to the configured URL for the Barracuda Web Application Firewall. To receive authorization to view the protected resource, a user must authenticate using RSA SecurID. To begin the authentication process, the user must enter a username and password on the Login 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 password, the user is successfully authenticated and forwarded along to the configured URL. For more information on how to configure RSA Authentication Manager and to verify the setup, see **How to Integrate RSA SecurID with the Barracuda Web Application Firewall** .



Certification Checklist for RSA Authentication Manager 7.x

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP2	Windows 2003 Server
Web Application Firewall	7.4.0.r97235	Proprietary OS

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	√
PIN Reuse	N/A	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	√
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	√
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
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 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
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

BSD

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

Figures