



RSA SecurID Ready Implementation Guide

Last Modified: November 27, 2013

Partner Information

Product Information	
Partner Name	Barracuda Networks
Web Site	www.barracuda.com
Product Name	Web Application Firewall
Version & Platform	7.8.1, Model V660
Product Description	The Barracuda Web Application Firewall offers the capability to secure, deliver, and manage enterprise Web applications from a single appliance through an intuitive, real-time user interface.

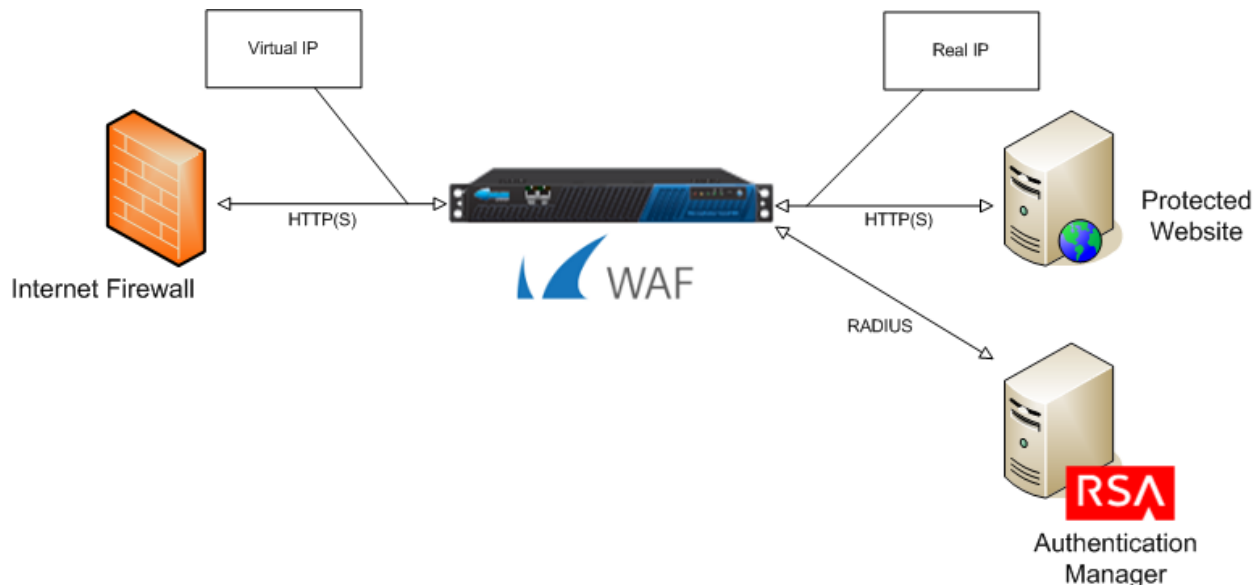


Solution Summary

The Barracuda Web Application Firewall (WAF) protects websites from attackers leveraging protocol or application vulnerabilities including data theft, denial of service (DoS), unauthorized access and website defacement.

The Barracuda Web Application Firewall provides advanced protection via RSA two factor authentication. The Barracuda WAF is designed to enforce policies for both internal and external data security standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

RSA Authentication Manager supported features	
Web Application Firewall 7.8.1	
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
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



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 the Web Application Firewall will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Web Application Firewall 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 Web Application Firewall 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 the Web Application Firewall components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Barracuda Web Application Firewall for SecurID Authentication

Create a New Service on the Barracuda Web Application Firewall

1. Log on to the Barracuda Web Application Firewall by using a supported Web browser.
2. From the **BASIC** tab, select the **Services** page.
3. In the **Add New Service** section, specify values for the following fields:
 - **Service Name:** Enter the name to identify this service on the Barracuda Web Application Firewall.
 - **Type:** Select HTTP from the drop-down list.
 - **Virtual IP:** Enter the IP address of the service. If the IP address is specified for the first time, a new Virtual IP is created and a Netmask will be automatically assigned based on the class of the IP address specified. If the Netmask is inappropriate, you need to create the Virtual IP first (where you can specify the Netmask) and then use that IP address in the service creation. The Virtual IPs can be added or managed on the **ADVANCED > Advanced IP Config** page.
 - **Port:** Enter the port number for the service. Port 80 is the default port for the HTTP Service.
 - **Real Server:** Enter the IP address of the server that hosts the service.
4. Click **Add** to add the service.

The screenshot shows the 'Add New Service' configuration page in the Barracuda WAF interface. The page has a navigation bar with tabs for 'BASIC', 'SECURITY POLICIES', 'WEBSITES', 'ACCESS CONTROL', and 'ADVANCED'. The 'BASIC' tab is selected. Below the navigation bar is a menu with options: 'Status', 'Services', 'Default Security', 'Certificates', 'IP Configuration', and 'Administration'. The 'Services' menu item is highlighted, and its sub-menu items are 'Web Firewall Logs', 'Access Logs', 'Audit Logs', 'Reports', and 'Online Help Search'. The main content area is titled 'Add New Service' and contains the following fields:

Service Name	Type	Virtual IP Address	Port	Real Servers
lomegaPE	HTTP	10.100.55.14	80	10.100.51.14

Below the table, there are two sections:

- Create Group:** Radio buttons for 'Yes' and 'No'. 'No' is selected.
- Service Groups:** A dropdown menu with 'default' selected.

An 'Add' button is located at the bottom right of the form.

Configure the Authentication Service on the Barracuda

1. From the **ACCESS CONTROL** tab, select the **Authentication Services** page.
2. Select **RSA SecurID** under the **New Authentication Service** section.

WEB APPLICATION FIREWALL 660 Vx | BASIC | SECURITY POLICIES | WEBSITES | ACCESS CONTROL | ADVANCED

Authentication Services: Authentication | Authorization | Local Users/Groups | Client Certificates

New Authentication Service

LDAP | RADIUS | SITEMINDER | **RSA SECURID** | KERBEROS

Realm Name	<input type="text" value="RSA"/>	Specifies the name of the realm. A realm identifies a collection of users and groups. It specifies information, in a flat directory structure, such as where users are located and where groups are located.
Server IP	<input type="text" value="10.100.50.29"/>	Specifies the name or IP address of the RSA RADIUS server used for authenticating users. Note: The RSA Authentication Manager server running RADIUS is termed as RSA RADIUS server in the Barracuda Web Application Firewall.
Server Port	<input type="text" value="1812"/>	Specifies the port number of the RSA RADIUS server used for authenticating users.
Shared Secret	<input type="password" value="••••••••"/>	Specifies the secret key that is shared between the Barracuda Web Application Firewall and the RSA RADIUS server. Minimum value of the key is 6.
Timeout	<input type="text" value="3"/>	Specifies the time the Barracuda Web Application Firewall waits for a response from the RSA RADIUS server before retransmitting the packet.
Retries	<input type="text" value="3"/>	Specifies the number of times the Barracuda Web Application Firewall transmits a request packet to the RSA RADIUS server before giving up.

3. Enter values for all the fields.
4. Click **Add**.
5. The Authentication Services will appear in the Existing Authentication Services table, click **Add** under **Options** to add a secondary RADIUS server to this service.

Existing Authentication Services Help				
Alias	Type	Service	Server IP	Options
RSA	RSA SECURID		10.100.50.29	Add Edit Delete
internal	LOCAL		127.0.0.1	

Bind the New Service with the Authentication Service

1. From the **ACCESS CONTROL** tab, select the **Authentication** page.
2. Under the **Authentication Policies** section, click **Edit** against the service for which you want to configure RSA SecurID authentication.

Authentication Policies bind a Web Site to an Authentication Service. For authentication, users are presented with either an HTML form with user ID and password fields, or a basic authentication login dialog box. Before enabling an Authentication Policy, Authentication Services must be configured via the Authentication Services screen.

Note: Authentication is enforced only when access control is enabled via the Authorization screen, which determines the set of users/groups which have access to particular sections of the Web Site. On successful authentication, login sessions are valid for the entire domain, though access control to different sections of the domain is determined by the Authorization Policies.

Name	Status	Authentication Service	Options
default			
lomegaPE	Off		Edit

3. The **Edit Authentication Policy** window appears. Specify values for the following fields:
 - Set the **Status 'On'** to enable authentication for this service.
 - Select the RSA Authentication Service you created on the **ACCESS CONTROL > Authentication Services > RSA SecurID** page from the **Authentication Service** drop-down list.
 - Specify value for other parameter(s). Click the help button to get more information about how to configure an authentication policy.

Edit Authentication Policy [Save Changes] [Cancel] [Help]

Service: lomegaPE
 Status: On Off
 Authentication Service: RSA (dropdown)
 Auth Success URL:
 Auth Logout Success URL:
 Auth Challenge URL:
 Challenge User Field: challenge_user
 Challenge Prompt Field: challenge_prompt
 Auth Failure URL:
 Trusted Hosts Action: Allow Default

Set to **On** to apply this authentication policy to the Service.

Select the authentication service to be used from the drop-down list. The list includes all authentication services configured on the **ACCESS CONTROL > Authentication Services** page.

Specify the URL to be used to redirect the user after successful authentication.

Specify the URL to be used to redirect the user after successful logout.

Specifies the URL to which a user is redirected, if the authentication service requires additional credentials.

The name of the query string field that will pass the challenged user's username to the challenge URL.

The name of the query string field that will pass the prompt string received in a RADIUS challenge message to the challenge URL.

Specify the URL to be used to redirect the user when authentication fails.

Select an action (**Allow** or **Default**) to be applied to the selected **Trusted Hosts Group**.

4. Click **Save Changes**.

Configure the Authorization Policy for the Service

1. From the **ACCESS CONTROL** tab, select the **Authorization** page.
2. In the **Add Authorization Policy** window, enter a **Policy Name**.
3. Change the **Status** to **On**.
4. Enter a **URL Match** value.

Add Authorization Policy Help

Service: IomegaPE
Policy Name: RSA_SecurID
Status: On Off
URL Match: /*
Host Match: *
Extended Match: *
Extended Match Sequence: 1000
Login Method: HTML Form HTTP Basic Authentication
Comments: [Text Area]

The name of the Authorization Policy.
Set this parameter to On to apply the authorization policy for this service.
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.
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
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.
Specifies an order for matching the extended match rule.
Select the login method to be used to authenticate the user.
Comments

Add

5. Click **Add** to add the Authorization policy configuration.

When a user attempts to access a protected resource, the Barracuda Web Application Firewall displays the login page to authenticate a user. If the URL Match is configured as "/*", it will display the login page for any request sent to the service.

RSA SecurID Login Screens

Login screen:

Authentication and Access control
Login
Please provide your username and password to access restricted applications.
User Name: <input type="text"/>
Password: <input type="password"/>
<input type="button" value="Login"/> <input type="button" value="Reset"/>

User-defined New PIN:

Authentication and Access control
Login
Enter a new PIN having from 4 to 8 alphanumeric characters: <input type="text"/>
<input type="button" value="Login"/> <input type="button" value="Reset"/>

System-generated New PIN:

Authentication and Access control	
Login	
Are you satisfied with system generated PIN AkfzAg ? (y/n): <input type="text"/>	
<input type="button" value="Login"/>	<input type="button" value="Reset"/>

Next Tokencode:

Authentication and Access control	
Login	
PIN Accepted. Wait for the token code to change, then enter the new passcode: <input type="text"/>	
<input type="button" value="Login"/>	<input type="button" value="Reset"/>

Certification Checklist for RSA Authentication Manager

Date Tested: November 27, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.0	Virtual Appliance
Web Application Firewall	7.8.1	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 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

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