



RSA Secured Implementation Guide For Portal Servers and Web-Based Applications

Last Modified: June 17, 2008

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	http://www.juniper.com
Product Name	Juniper Networks NetScreen-SA
Version & Platform	6.0R3.1 (build 12507)
Product Description	The NetScreen Instant Virtual Extranet enables you to give employees, partners, and customers, secure and controlled access to your corporate file servers, Web servers, native messaging and email clients, hosted servers and more from any Web browser, anywhere. The IVE eliminates the need to deploy extranet toolkits in a traditional DMZ or provision a remote access VPN for employees. The appliance intermediates data between external connections, from which it receives secure requests, and internal resources, to which it makes requests, on behalf of authenticated users.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)





Solution Summary

To achieve Single-Sign-On (SSO) with RSA Access Manager, the Juniper Networks NetScreen-SA IVE leverages a centralized LDAP Directory server that is shared by both products. The Juniper IVE transparently submits the user's Access Manager credentials to the RSA Access Manager login form for SSO to any internal applications protected by RSA Access Manager.

Partner Integration Overview	
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	N/A
API-level Authorization Support (RuntimeAPI)	No
User Management (AdminAPI)	Via Shared User Repository (LDAP)

Product Requirements

Partner Product Requirements: NetScreen-SA	
Platform	Required Patches
NetScreen-SA	6.0R3.1 (build 12507)



Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA Access Manager. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the NetScreen-SA

The following are the steps required for configuring the Juniper IVE to perform Single Sign-On (SSO) with internal web applications that are protected by RSA Access Manager.

1. Use or Create an Authentication Server that uses the same authentication credentials as RSA Access Manager. This is best achieved by sharing an LDAP Directory server (Active Directory e.g.) that is supported by both products. Consult the Juniper IVE Administration Guide for more information on how to do this.

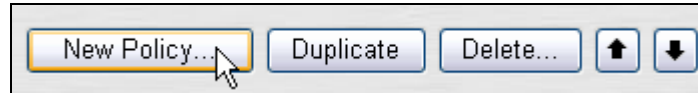
! Important: This guide assumes you are using a centralized LDAP Directory server that is shared by both RSA Access Manager and the Juniper IVE. If this is not the case, you will need to ensure that user accounts and passwords are synchronized between the two systems.

2. Use or Create a new Realm with this Authentication Server. Consult the Juniper IVE Administration Guide for more information on how to do this.
3. In the IVE Web console, choose **Resource Policies > Web > SSO FORM POST**





4. On the **Web Policies** page, click **New Policy**



5. On the **SSO Form POST Policy** page, enter:

- A **name** to label this policy.
- A **description** of the policy. (optional)

* Name:	<input type="text" value="RSA Access Manager Policy"/>
Description:	<input type="text" value="This policy is for FORM POST to the RSA Access Manager Web Agent Form."/>

6. In the **Resource** section, specify the resources to which this policy applies. In this case, the policy should be applied to the directory containing the RSA Access Manager authentication forms (/cleartrust/*). By defining the policy in this fashion, the FORM POST policy will be invoked whenever the RSA Access Manager authentication forms are invoked by the RSA Access Manager Web Agent.

Resource	
Specify the resource for which this policy applies.	
* Resource:	<input type="text" value="http://ps069.pe.rsa.net:80/cleartrust/*"/>



7. In the **Roles** section, specify:

- Policy applies to **ALL** roles

To apply this policy to all users.

- Policy applies to **SELECTED** roles

To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

- Policy applies to all roles **OTHER THAN** those selected below

To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles: Selected roles:

Cert Users	<input type="button" value="Add ->"/>	(none)
	<input type="button" value="Remove"/>	

8. In the **Action** section, specify **Perform the POST defined below**:

Action

Perform the POST defined below
 Do NOT perform the POST defined below
 Use Detailed Rules (see [Detailed Rules](#) page)




9. In the **POST details** section, specify the Header names and values as outlined below:

POST details


* POST to URL: Required:

Deny direct login for this resource

<input type="checkbox"/>	User label	Name	Value	User modifiable?	
<input type="checkbox"/>				Not modifiable	<input type="button" value="Add"/>
<input type="checkbox"/>	y	y	0	Not modifiable	
<input type="checkbox"/>	x	x	0	Not modifiable	
<input type="checkbox"/>	orig_url	orig_url		Not modifiable	
<input type="checkbox"/>	auth_mode	auth_mode	BASIC	Not modifiable	
<input type="checkbox"/>	Username	user	<USER>	User CAN change value	
<input type="checkbox"/>	Password	password	<PASSWORD>	User CAN change value	


 **Note:** In the example above, “user” and “password” are both set to “User CAN change value”. It is also valid and may be appropriate to set this to “Not modifiable.” Consult the Juniper IVE Administration Guide for more information on the use and configuration of this parameter.

This allows the IVE to seamlessly POST the RSA Access Manager username and password into the RSA Access Manager authentication form (http://<Access Manager Agent Host>/cleartrust/ct_logon.asp). The Juniper IVE then stores the resulting RSA Access Manager CTSESSION cookie on behalf of the user and replays it to any other RSA Access Manager Web Agents for Single Sign-On (SSO).

 **Note:** If your RSA ClearTrust resources are protected by an RSA Access Manager Web Agent using SecurID authentication, this will require custom UI work on the IVE. Please contact Juniper for assistance on Custom UI configuration if this is needed.



The resulting end-user experience is such that users do not see the RSA Access Manager logon process (which happens automatically in the background) and they are presented with the RSA Access Manager-protected page without having to re-enter user credentials.

 **Note:** Single Sign-On (SSO) with RSA Access Manager is also available via SAML. This requires the use of the RSA Federated Identity Manager and its out of the box SSO integration with RSA Access Manager. For more information on this solution, consult the RSA Federated Identity Manager Implementation Guide for the Juniper IVE available at <http://www.rsasecured.com>.

Certification Checklist Portal Servers and Web-Based Apps

Date Tested: June 17, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Access Manager	6.0.3	Microsoft Windows 2003 Server R2
RSA Access Manager Agent	4.7	Microsoft Windows 2003 Server R2
Juniper Networks NetScreen-SA	6.0R3.1 (build 12507)	Proprietary


Test Case	Result
Product Characteristics for SSO Support	
Application/Portal is web-based, and supports access by a standard HTTP-based browser	✓
Application/Portal runs on Web Server Platform supported by RSA Access Manager	N/A
Application/Portal login interface can be modified or replaced	N/A
Application/Portal can extract user information from RSA Access Manager session cookie	✓
Application/Portal can extract user information from HTTP Headers	✓
Application/Portal can extract authentication type from RSA Access Manager session cookie	N/A
Application/Portal can extract authentication type from HTTP Headers	N/A
Application/Portal can perform SSO with other RSA Access Manager-supported Web Server	✓
Login - General	
HTTP basic authentication	N/A
Forms based	✓
Forms based w/ URI retention	✓
Login – Basic Authentication	
Access Denied for unauthorized user	✓
Successful login for authorized user	✓
Successful recognition of identity/personalization in 3 rd Party Product	✓
Successful recognition of identity/personalization after SSO with other RSA Access Manager-supported Web Server	✓
Login –Graded Authentication	
Access Denied for unauthorized user	N/A
Successful login for authorized user	N/A
Successful recognition of identity/personalization in 3 rd Party Product	N/A
Successful recognition of identity/personalization after SSO with other RSA Access Manager-supported Web Server	N/A


BSD


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



Notes

 **Note:** If your RSA ClearTrust resources are protected by an RSA ClearTrust Web Agent using SecurID authentication, this will require custom UI work on the IVE. Please contact Juniper for assistance on Custom UI configuration if this is needed.

 **Note:** Single Sign-On (SSO) with RSA ClearTrust is also available via SAML. This requires the use of the RSA Federated Identity Manager and its out of the box SSO integration with RSA ClearTrust. For more information on this solution, consult the RSA Federated Identity Manager Implementation Guide for the Juniper IVE available at <http://www.rsasecured.com>.

 **Important:** This guide assumes you are using a centralized LDAP Directory server that is shared by both RSA ClearTrust and the Juniper IVE. If this is not the case, you will need to ensure that user accounts and passwords are synchronized between the two systems.

Known Issues

There are no known issues.