



# RSA Secured Implementation Guide for VPN Products

Last Modified August 27, 2004

## 1. Partner Information

Partner Name	Juniper Networks
Web Site	<a href="http://www.juniper.com/">http://www.juniper.com/</a>
Product Name	Juniper Networks NetScreen-SA 3000
Version & Platform	4.1
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)



## 2. Contact Information

	Sales Contact	Support Contact	
		<b>Juniper Networks</b>	<b>RSA Security</b>
Phone	(866) 298-6428	(800) 638-8296	(800) 995-5095
Web	<a href="https://www.juniper.net/solutions/">https://www.juniper.net/solutions/</a>	<a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a>	<a href="http://knowledge.rsasecurity.com">http://knowledge.rsasecurity.com</a>

### 3. Solution Summary

Feature	Details
VPN product acts as SAML Asserting Party (AP) for RSA FIM	Yes
VPN product provides Web Single Sign-On (SSO) to ClearTrust-protected resources via SAML	Yes
Common SAML version(s) supported	1.1
Web SSO Profile(s) supported	BAP, BPP

### Integration Overview

Juniper Networks NetScreen-SA IVE version 4.1 can provide Single-Sign-On (SSO) to RSA ClearTrust via the RSA Federated Identity Manager (FIM) version 2.5. Juniper IVE can act as a SAML Asserting Party (AP) for the RSA FIM by passing SAML authentication assertions to the RSA FIM for processing. Users are then automatically provided with a ClearTrust Single Sign-On session cookie via the FIM's RSA ClearTrust ticket plug-in. This prevents the need to perform additional authentication(s) to ClearTrust-protected resources once a user has successfully authenticated to the SSL VPN.

Juniper Networks NetScreen-SA 3000 version 4.1 supports SAML 1.1 and the BAP and BPP Web SSO profiles.

### 4. Product Requirements

#### Hardware and Software Requirements

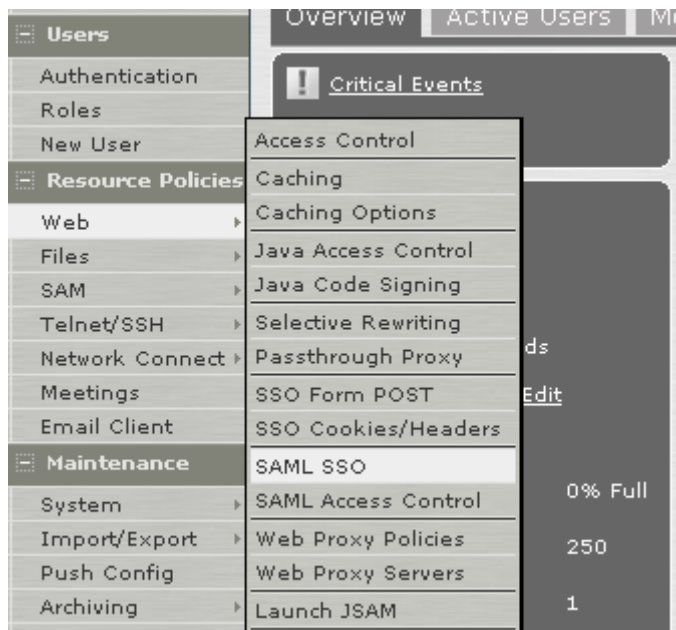
Component Name: Juniper Networks NetScreen-SA 3000	
Operating System	Version (Patch-level)
Juniper Networks NetScreen-SA 3000	4.1-(build 6641)

## 5. Product Configuration

### Configuring SAML Support on the Juniper Networks NetScreen-SA 3000

To write a SAML SSO artifact profile resource policy:

1. In the Web console, choose Resource Policies > Web > SAML > SSO



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

3. On the SAML SSO Policy page, enter:
  - A name to label this policy.
  - A description of the policy. (optional)

\* Name: FIM Policy

Description: FIM-Protected resources

4. In the **Resources** section, specify the resources to which this policy applies. See the *IVE Administration Guide* for more information.

Specify the resources for which this policy applies, one per line.

\* Resources: `http://ps075.securitydynamics.com:80/google/ *`

Examples:  
`http://*.domain.com/public/*`  
`https://www.domain.com:443/*`  
`10.10.10.10/255.255.255.0:80,443/public/*`  
`10.10.10.10/24:8000-9000/*`

5. 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 -&gt;"/> <input type="button" value="Remove"/>	(none)
---------------	---	--------

6. In the Action section, specify:
- Use the SAML SSO defined below

**Action**

Use the SAML SSO defined below  
 Do not use SAML  
 Use Detailed Rules (see [Detailed Rules](#) page)

The IVE performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. The IVE makes the SSO request when a user tries to access to a SAML resource specified in the Resources list.

- Do NOT use SAML  
The IVE does not perform a SSO request.
- Use Detailed Rules  
To specify one or more detailed rules for this policy. See *IVE Administration Guide* for more information.

7. In the SAML SSO Details section, specify:
- SAML Assertion Consumer Service URL

### SAML SSO Details

SAML  
Assertion  
Consumer  Example: http://hostname/acs  
Service  
URL:

Enter the URL that the IVE should use to contact the assertion consumer service (that is, the access management server). For example: https://hostname/acs. (Note that the IVE also uses this field to determine the SAML recipient for its assertions.)

**!> Important:** If you enter a URL that begins with HTTPS, you must install the assertion consumer service's root CA on the IVE (as explained in the "Certificates" section of the *IVE Administration Guide*).

- Profile

Select **POST** to indicate that the IVE should "push" information to the assertion consumer service during SSO transactions. You must also select the certificate you will be using to sign assertions, as this is required in the Browser POST Profile.

Profile:  Artifact  POST  
Issuer:  Hostname of the IVE  
Signing Certificate:  Select certificate used to sign the assertion.

Select **Artifact** to indicate that the assertion consumer service should "pull" information from the IVE during SSO transactions.

Profile:  Artifact  POST  
Source ID:  20-byte IVE identifier that maps to the URL https://<IVEhostname>/dana-  
ws/saml on the assertion consumer service  
Issuer:  Hostname of the IVE

- Source ID

Enter the **Source ID** for the IVE. If you enter a:

- Plain text string—The IVE converts, pads, or truncates it to a 20-byte string.
- Base-64 encoded string—The IVE unencodes it and ensures that it is 20 bytes.

If your access management system requires base-64 encoded source IDs, you can create a 20 byte string and then use a tool such as OpenSSL to base-64 encode it.

**!> Important:** The IVE identifier (that is, the source ID) must map to the following URL on the assertion consumer service (as explained in "Trusted application URLs" on page 3):

https://<IVEhostname>/dana-ws/saml.ws

- Issuer

Enter a unique string that the IVE can use to identify itself when it generates assertions (typically its hostname).

**! Important:** You must configure the assertion consumer service to recognize the IVE's unique string.

8. In the User Identity section, specify how the IVE and the assertion consumer service should identify the user:
  - Subject Name Type
    - DN—Send the username in the format of a DN (distinguished name) attribute.
    - Email Address—Send the username in the format of an email address.
    - Windows—Send the username in the format of a Windows domain qualified username.
    - Other—Send the username in another format agreed upon by the IVE and the assertion consumer service.
  - Subject Name

Use the variables described in the *IVE Administration Guide* to specify the username that the IVE should pass to the assertion consumer service. Or, enter static text.

**User Identity**

Subject Name Type:  ▼

Subject Name:  Example: <userAttr.distinguishedName>

**! Important:** You must send a username or attribute that the assertion consumer service will recognize (as explained in “User Identity” in the *IVE Administration Guide*). For a default ClearTrust installation, the name format would be **uid=<USER>**. If you are using a different Name Format for ClearTrust/FIM mapping, you must enter the appropriate value.

9. In the Web Service Authentication section, specify the authentication method that the IVE should use to authenticate the assertion consumer service:
  - None

Do not authenticate the assertion consumer service.
  - Username

Authenticate the assertion consumer service using a username and password. Enter the username and password that the assertion consumer service must send the IVE.

**Web Service Authentication**

Authentication Type:  None  
 Username/Password

Username:

Password:

Confirm Password:

Certificate

- Certificate Attribute

Authenticate the assertion consumer service using certificate attributes. Enter the attributes that the assertion consumer service must send the IVE (one attribute per line). For example, cn=sales. You must use values that match the values contained in the assertion consumer service's certificate.

**! Important:** If you select this option, you must install the assertion consumer service's root CA on the IVE (as explained in "Certificates" in the *IVE Administration Guide*).

10. Cookie Domain—Enter a comma-separated list of domains to which we send the SSO cookie.

Cookie Domain(s):  Comma-separated list of domains to which the SSO cookie is sent. For example, company.com.

11. Click **Save Changes**.
12. On the SAML SSO Policies page, order the policies according to how you want the IVE to evaluate them. Keep in mind that once the IVE matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

For an example Web resource policy, see the figures in the *IVE Administration Guide*.

- **Note:** The session timeouts on the IVE and your access management system may not coordinate with one another. If a user's RSA ClearTrust session cookie times out before his IVE cookie (DSI Dcookie) times out, then single sign-on between the two systems is lost. The user is forced to sign in again when he times out of the access management system.

## Configuring RSA FIM Asserting Party Settings for Juniper IVE

**Note:** The example screenshots provided below are for demonstration purposes only. Your environment may or may not vary from this example. All parameters are determined by your deployment environment unless specified otherwise.

To set up the Juniper IVE as a Trusted Asserting Party for the RSA FIM, perform the following steps:

1. Configure the Asserting Party Settings:

Asserting Party Settings > Edit	
<b>i</b> Trusted Asserting Party Name:	ph091
Description:	None
<b>i</b> Issuer ID:	ph091.securitydynamics.com
<b>i</b> SOAP Binding Service URL:	https://ph091.securitydynamics.com/dana-ws/saml.ws
<b>i</b> SOAP Connection Type:	N/A
<b>i</b> Source ID (Base 64):	a2uw+b9WDR9kiMpSPFeuBuoRM60=
<b>i</b> Source ID (Hex):	6b6bb0f9bf560d1f6488ca523c57ae06ea1133ad

Note the **SOAP Binding Service URL** and **SourceID** obtained from the IVE.

2. Configure settings for Web SSO

Web SSO > Edit	
<b>i</b> Profile Type:	Browser Post Profile
<b>i</b> Require Subject Namespace:	MUST NOT contain a subject namespace
<b>i</b> Subject Plug-In:	RSA_ClearTrust_X.509_Subject_Plug-in_RP
<b>i</b> Require IP Address:	MAY include the browser's IP address
<b>i</b> Require DNS Address:	MAY include the browser's DNS address
<b>i</b> Send Attributes:	Web SSO assertions MUST NOT contain an attribute statement

The example here is configured for **Browser Post Profile** (BPP).

**!** **Important:** It is **required** that you select **MUST NOT contain a subject namespace** in this section. Then select the **RSA\_ClearTrust\_X.509\_Subject\_Plug-in** from the drop-down box.

The IVE will also send the IP Address and DNS address if available, so set these two parameters to **MAY**.

3. Configure settings for Digital Signatures:

Digital Signatures > Edit	
<b>i</b> Sign Requests:	No
<b>i</b> Request Signature Keystore:	N/A
<b>i</b> Trusted Asserting Party Responses:	MUST be signed
<b>i</b> Response Signature Keystore:	ph091
<b>i</b> Trusted Asserting Party Assertions:	MUST NOT be signed
<b>i</b> Assertion Signature Keystore:	N/A
<b>i</b> Verification Method:	Local Verification
<b>i</b> Verificaton Interval:	3 Days
<b>i</b> Next Verification:	10:06:54 PM Jun 06, 2004

Note that for BPP the IVE only signs SAML responses, not the assertions themselves, so if signatures are required, set the responses to **MUST be signed** and the assertions **MUST NOT be signed**.

Note also that for BAP, the IVE does not sign responses. Signing of responses is only supported with BPP.

## 6. Certification Checklist for VPN Products

Date Tested: 05/18/04




Product	Tested Version
RSA Federated Identity Manager (FIM)	2.5
RSA ClearTrust	5.5.2
Juniper Networks NetScreen-SA 3000	4.1-(build 6641)

Test Case	Result	
<p><b>Note:</b> All VPN test cases assume that Partner Product is configured as the <b>Asserting Party (AP)</b> and the RSA Federated Identity Manager (FIM) is configured as the <b>Relying Party (RP)</b>.</p>		
<p><b>SAML Asserting Party (AP)</b></p>		
Partner Product <b>produces</b> valid authentication assertion in response to valid authentication query from FIM	SAML 1.0	SAML 1.1
RSA FIM <b>consumes</b> valid authentication assertion, requested in valid authentication query to Partner Product		P
Partner Product <b>produces</b> valid attribute assertion in valid response to attribute query from FIM		P
RSA FIM <b>consumes</b> valid attribute assertion, requested in valid attribute query to Partner Product		N/A
Partner Product <b>produces</b> valid assertions in valid response to AssertionIDReference request from FIM		N/A
RSA FIM <b>consumes</b> valid assertions, requested in valid AssertionIDReference request to Partner Product		N/A
<p><b>Web Browser SSO Profiles</b></p>		
<p><b>Browser/Artifact Profile (BAP)</b></p>		
Valid assertions produced in response to AssertionArtifact request		P
Valid assertions request corresponding to artifacts sent in HTTP message		
HTTP BASIC Authentication		P
Anonymous SSL		P
Mutual Auth SSL		P
Valid signed response sent to and validated by FIM (RP)		N/A
Valid signed assertion sent to and validated by FIM (RP)		N/A
Successful validation of signed requests from FIM (RP)		N/A
Valid RSA ClearTrust token generated via RSA ClearTrust ticket plug-in		P
<p><b>Browser/POST Profile (BPP)</b></p>		
Valid Assertions Received in Valid HTTP POST		P
Valid Assertions Sent in Valid HTTP POST		P
Valid RSA ClearTrust token generated via RSA ClearTrust ticket plug-in		P
Valid signed assertion sent to and validated by FIM (RP)		P
Successful validation of signed requests from FIM (RP)		P

JEC

\*P=Pass or Yes F=Fail N/A=Non-available function

## 7. Notes

-  The session timeouts on the IVE and your access management system may not coordinate with one another. If a user's RSA ClearTrust session cookie times out before his IVE cookie (DSI Dcookie) times out, then single sign-on between the two systems is lost. The user is forced to sign in again when he times out of the access management system.
-  The IVE does not support **attribute statements**, which declare specific details about the user (such as "John Smith is a member of the gold group").
-  The IVE can consume and enforce an **authorization decision statement** however; these types of SAML statements are not currently supported by RSA FIM.

## 8. Known Issues

-  **Important:** The IVE has been tested and does not work with FIM 2.0.