



RSA Secured Implementation Guide 3rd Party PKI Applications

Last Modified: February 15, 2005

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	Netscreen SSL VPNs
Version & Platform	4.1.1
Product Description	Juniper Networks Netscreen SSL VPNs are based on the Instant Virtual Extranet (IVE) platform, which uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for client software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper Networks SSL VPN appliances combine the overall category benefit of a lower total cost of ownership compared to traditional solutions, with unique end-to-end security features. Dynamic access privilege management adds granular access control for each user and for each resource.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)



Solution Summary

Juniper Networks NetScreen-RA/SA Series of SSL VPNs uses RSA Keon digital certificates to establish credentials and secure IVE session transactions. When validating users with CA certificates, the SSL VPN checks that the certificate is not expired or corrupt and that the certificate is signed by a CA that is recognized by the SSL VPN. If the CA certificate is chained the SSL VPN also follows the chain of issuers until it reaches the root CA, checking the validity of each issuer as it goes. The SSL VPN can also be configured to use Certificate Revocation lists to validate certificates.

Product Requirements

Partner Product Requirements: Juniper Networks SSL VPN	
Firmware Version	4.1.1

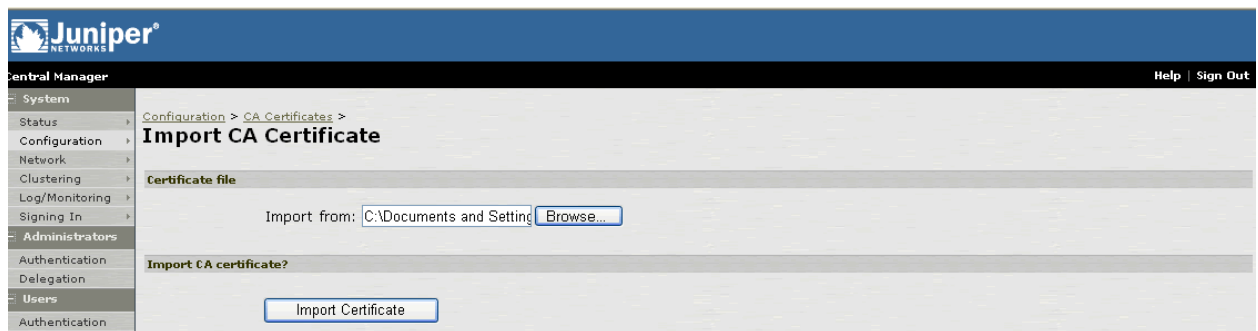
Product Configuration

A. Import a root certificate

1. Retrieve the root certificate from the RSA Keon Certificate Authority and save it the PC that you are managing the Juniper Networks SSL VPN from.
2. From the Administrator console, navigate to **System > Configuration > Certificates > CA Certificate tab**.



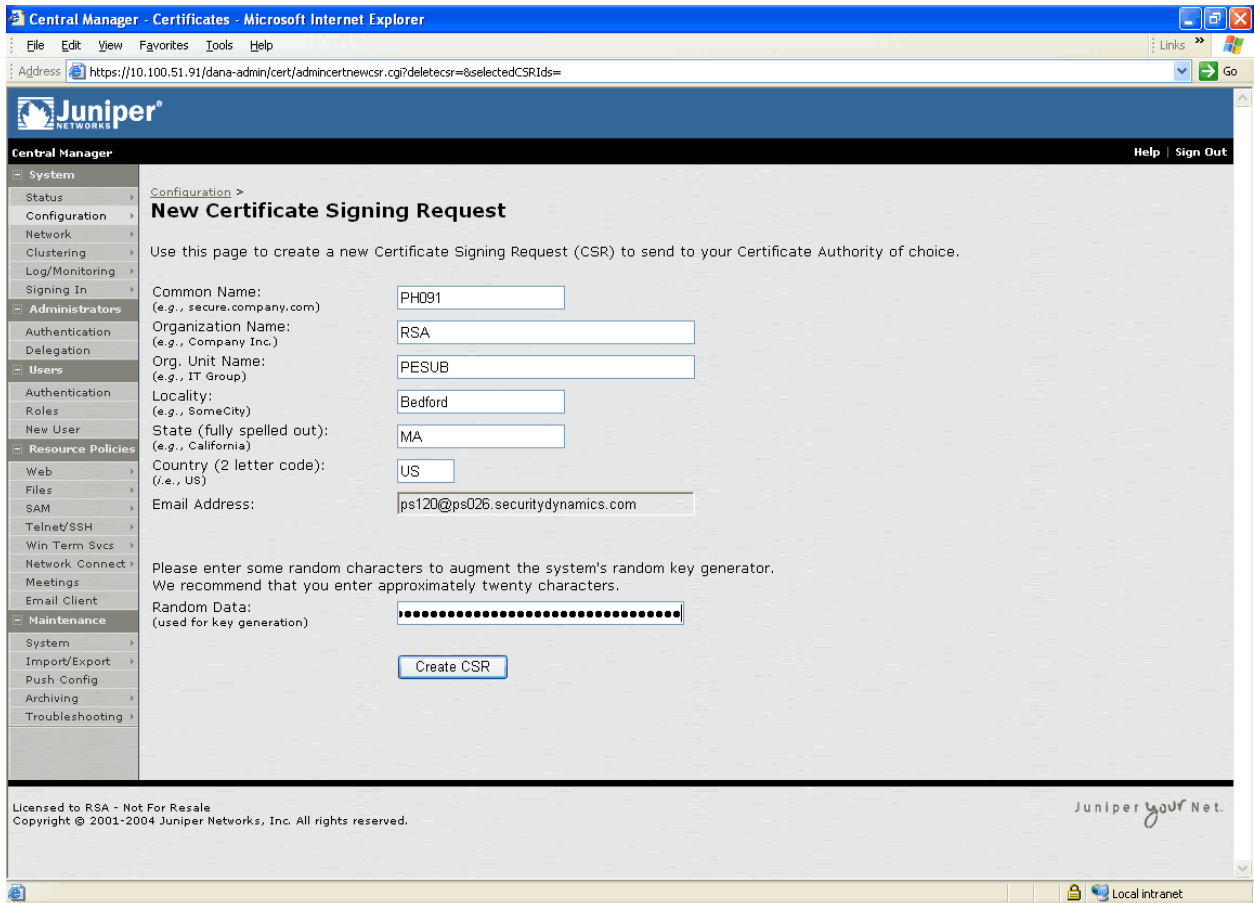
3. Click on the **Import CA Certificate** button.



4. Browse to the location where the Root CA Certificate was saved in step 1 above and click **Import Certificate**.
5. You should receive confirmation that the CA Certificate has been successfully imported.

B. Request a server certificate

1. To request a new certificate, from the menu in the left hand pane of the Administrator console, navigate to **System > Configuration > Certificates > Server Certificates**.
2. Click the button for New CSR. This will open a **New Certificate Signing Request**.
3. Enter the appropriate information for your device (Common Name, etc).
4. As requested, enter random data to augment the system's random key generator.



The screenshot shows the Juniper Central Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `https://110.100.51.91/dana-admin/cert/admincertnewcsr.cgi?deletecsr=&selectedCSRIDs=`. The page title is "Central Manager - Certificates - Microsoft Internet Explorer".

The main content area is titled "New Certificate Signing Request" and includes the following fields and instructions:

- Common Name:
- Organization Name:
- Org. Unit Name:
- Locality:
- State (fully spelled out):
- Country (2 letter code):
- Email Address:

Below the fields, there is a text box for random data with the instruction: "Please enter some random characters to augment the system's random key generator. We recommend that you enter approximately twenty characters." The text box contains 20 dots: `.....`.

A "Create CSR" button is located at the bottom of the form.

The footer of the page contains the text: "Licensed to RSA - Not For Resale. Copyright © 2001-2004 Juniper Networks, Inc. All rights reserved." and the Juniper logo.

5. Click the **Create CSR** button. You should now see your Certificate Signing Request.

The screenshot shows the Juniper Central Manager web interface. A notification at the top states "CSR created successfully". Below this, a yellow box contains instructions: "Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority. The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process." The main content area is titled "Pending Certificate Signing Request" and includes "CSR Details" with the following information:

- Common Name: PH091
- Created: 2/4/2005 10:45:53
- Org. Name: RSA
- Locality: Bedford
- Org. Unit Name: PESUB
- State: MA
- Email Address: ps120@ps026.securitydynamics.com
- Country: US
- Key Size: 1024 bits

Below the details is a link "Back to Server Certificates" and a section titled "Step 1. Send CSR to Certificate Authority for signing". This section explains that the user needs to copy the encoded text below and submit it to the CA. It provides three instructions:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

A note states: "Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR." The encoded CSR text is displayed in a text area:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAqYsxCzAJBgNVBAYTA1VTMQswCQYDVQQIEWJNQTQMA4GA1UE
BxMHQmVhZm9yZDEOMAwGA1UECzMFUEVTVUIxDDAKBgNVBAoTA1JQTQTEOMAwGA1UE
AxMFUEgwoTEXLzAtBgkqhkiG9w0BCQEWIHBzMTIwQHBzMDI2LnN1Y3VyaXR5S2H1u
YW1pY3MuY29tIGIEMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDP/dmZfweoPVbQ
```

6. Copy the encoded text, including the BEGIN and END lines and use it to make a PKCS#10 Certificate Request to the RSA Keon Certificate Authority.
7. When you receive your certificate, copy the certificate, being careful to include the Begin Certificate and End Certificate delimiters, and paste it into a text editor such as Notepad. Save the file as <certificatename>.cer (where certificatename is the Common Name of your SSL VPN).
8. From the Administrator Console, navigate to **System > Configuration > Certificates > Server Certificates** and click on the link to the Pending CRS request you made under Certificate Signing Requests.

Certificate Signing Requests	
	Created
<input type="checkbox"/> Pending_CSR for PH091	2/4/2005 10:45:53

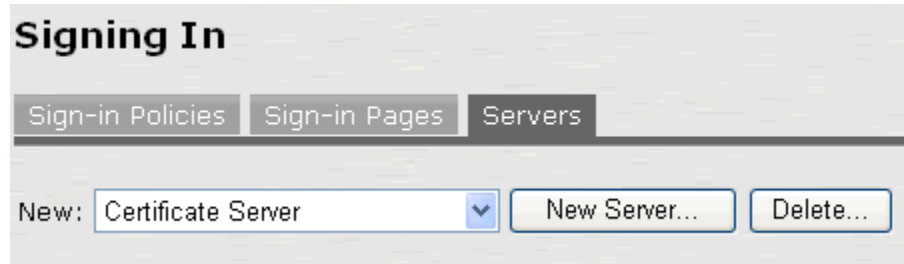
9. Click the **Browse** button under Import signed certificate and select the file for the server certificate you created in step 7.

10. Click **Import**.

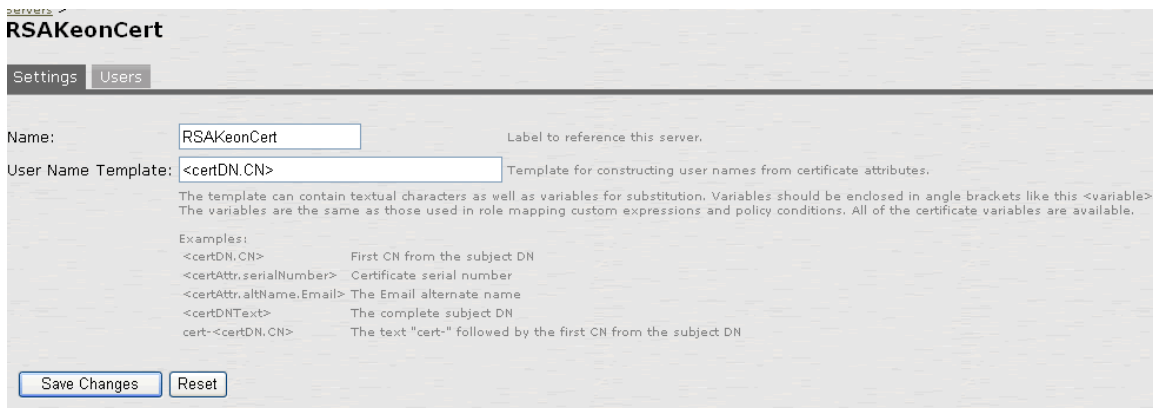


C. Require client machines to possess a valid certificate

1. From the Administrator Console, navigate to **Signing In > Authentication/Authorization Servers**.

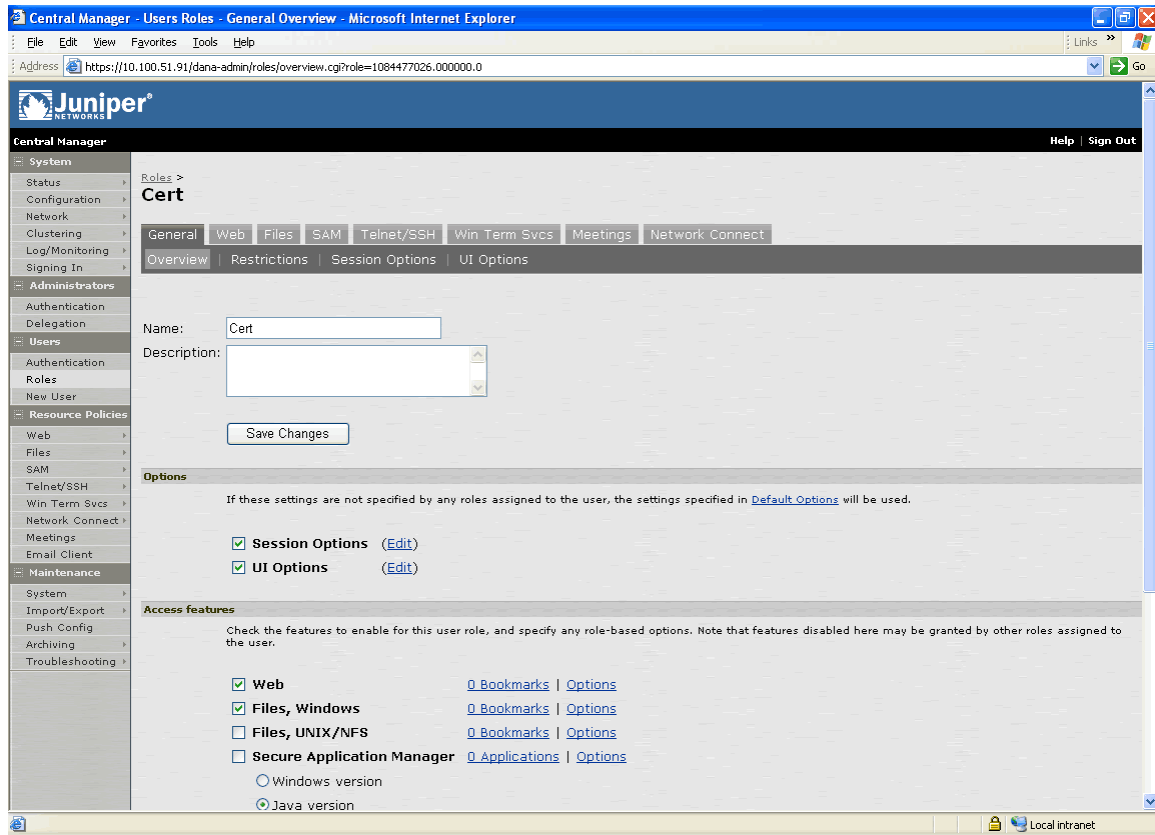


2. In the New: pull-down menu select **Certificate Server** and click the **New Server** button.



3. Enter a Name and select an appropriate User Name Template. Click Save Changes.

- From the Administrator Console, navigate to **Users – Roles** and create a role for the users that will use certificates. Select the appropriate information for your users.



- Click the Save Changes button to save the role.
- From the Administrator Console, navigate to **Users > Authentication**.

- Click the **New** button to create a new Realm.
- Enter a name for the new Realm and select the Certificate Server you created in step 2 for the Authentication server.

New Authentication Realm

Name: Label to reference this realm

Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication server: Specify the server to use for authenticating users.

Directory/Attribute server: Specify the server to use for authorization.

Save changes?

- Click the **Save Changes** button.
- You will now be on the Role Mapping tab. Click the **New Rule** button and create a rule for the user role you created in step 4 above.
- Click **Save Changes** to complete the process.

User Authentication Realms >

KeonCert Needed

General | Authentication Policy | **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. username is "***"	→ Cert		

When more than one role is assigned to a user:

Merge settings for all assigned roles

User must select from among assigned roles

User must select the sets of merged roles assigned by each rule

- The SSL VPN has now been configured to require client-side certificates.

D. Enable CRL Checking.

1. From the Administrator Console, navigate to **System > Configuration > Certificates > CA Certificates**.
2. Click on the CA certificate that you want to active CRL checking for.
3. Click the **CRL Checking Options** button.
4. Select the appropriate options for your CRL checking policy.

The following configuration was used for testing.

Use: **Manually Configure CDP**

CDP URL: **ldap://10.100.50.21/OU=PESUB,O=RSA,C=US**

Admin DN: **cn=Directory Manager**

Password=**"Password for Directory Manager"**

The screenshot shows the Juniper Central Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `https://10.100.51.91/dana-admin/cert/admincacertcrloption.cgi?certid=xCACert_6`. The page title is "Central Manager - Certificates - Microsoft Internet Explorer". The main content area is titled "CRL Checking Options" and is part of the "Configuration > CA Certificates > PESubCA >" navigation path. The page instructs the user to "Specify the CRL distribution point(s) from which to download the CRL, as well as how often to download." The "CRL Distribution Points (CDP)" section includes a dropdown menu for "Use:" set to "Manually configured CDP". Below this, there are fields for "Primary CDP" and "Backup CDP". The Primary CDP fields are: "CDP URL:" with the value "ldap://10.100.50.21/OU=PESUB,O=RSA,C=US", "Admin DN:" with the value "cn=Directory Manager", and "Password:" with a masked password. The Backup CDP fields are: "CDP URL:", "Admin DN:", and "Password:", all of which are empty. At the bottom, there is an "Options" section with "CRL Download Frequency:" set to "24 hours (1-9999)". A note states: "Note that CRLs can also specify a time to be updated. CRLs are downloaded based on that time or the frequency specified here...whichever comes first." A "Save changes?" button is located at the bottom of the form.

5. Click **Save Changes**.

6. You should now see that the CRL has been downloaded to the SSL VPN.

CRL checking for client certificates

Certificate revocation lists (CRL) are used to verify the ongoing validity of client-side certificates, and are obtained from CRL distribution points (CDP). To enable CRL checking, click CRL Checking Options, and specify the options.

Enable CRL distribution points	Status	Last Updated	Next Update
<input checked="" type="checkbox"/> ldap://10.100.50.21/OU=PESUB,O=RSA,C=US Success, new CRL	OK: 1KB, 1 revocations	2005/02/04 16:48:49 [Save CRL...]	2005/02/04 20:39:51

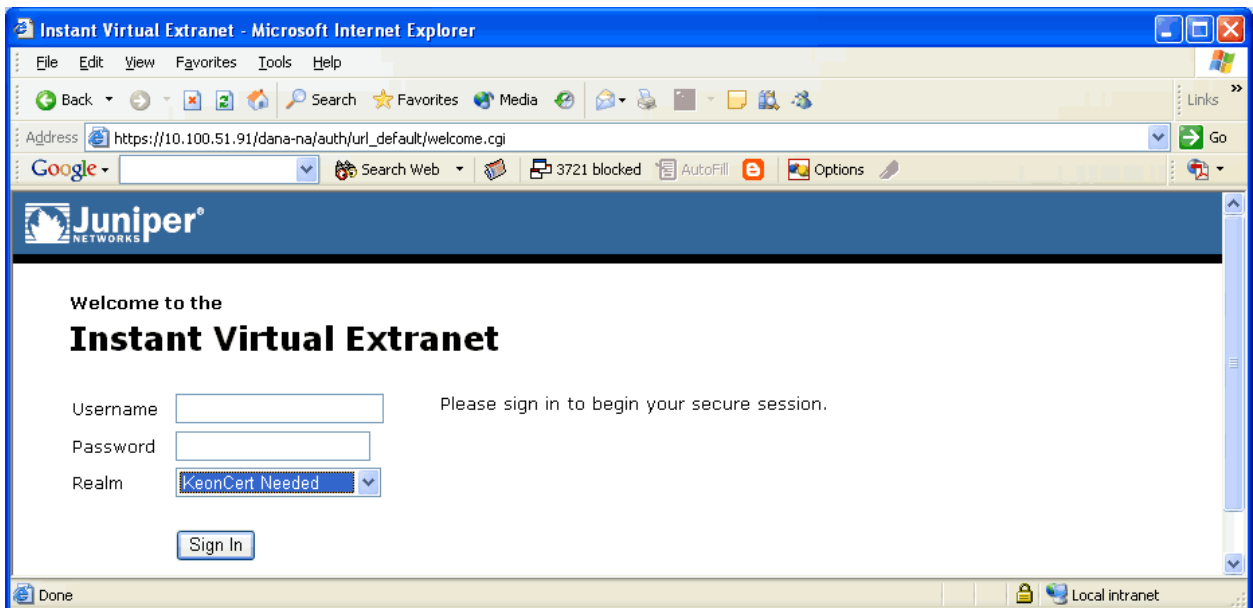
E. User certificate

1. Have the users enroll to the RSA Keon Certificate Authority using the SSL Client certificate profile with any additional attributes that are required.

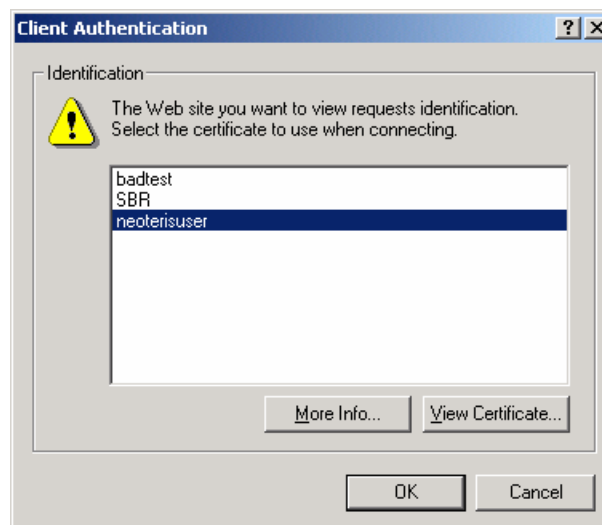
Product Operation

Partner gateway's operational elements

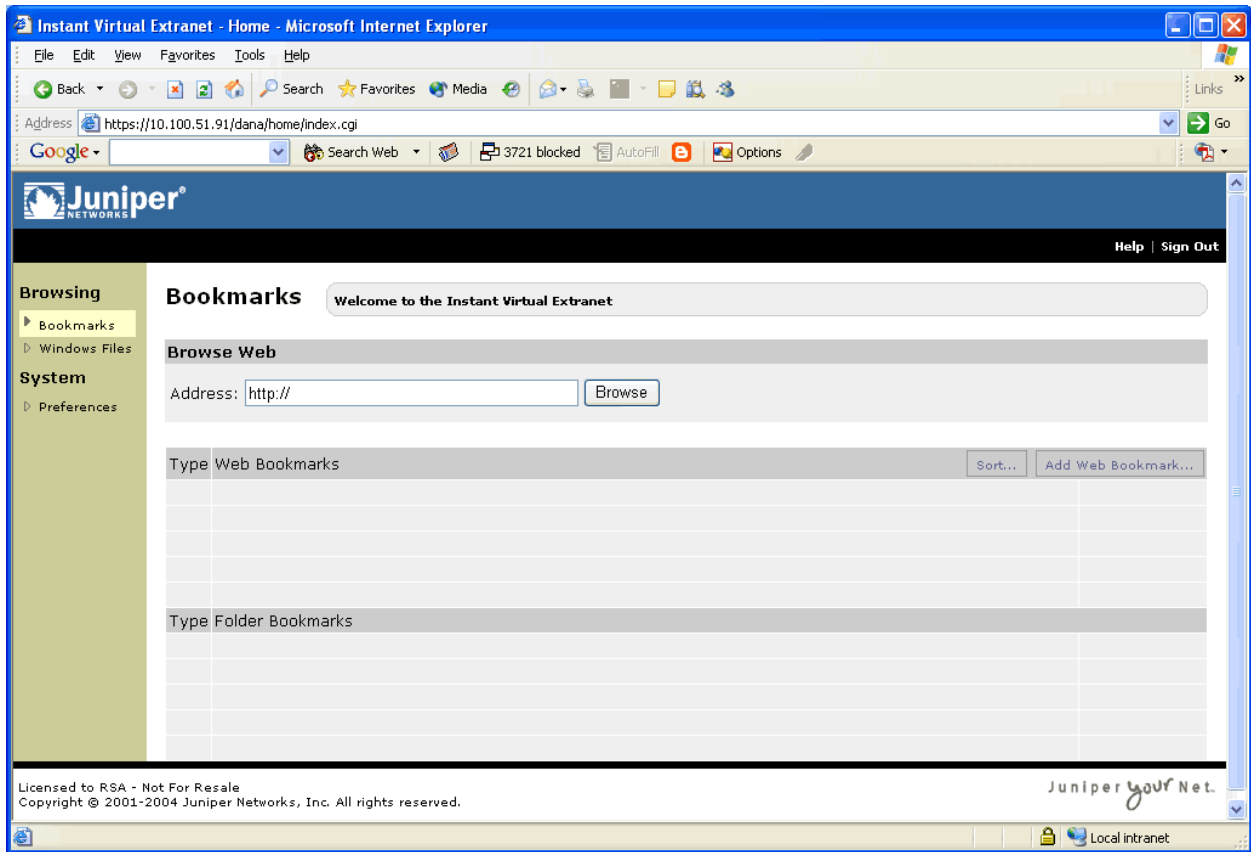
1. When a user connects to the Juniper SSL VPN via an Internet browser, have them select the Realm specified to require certificates.



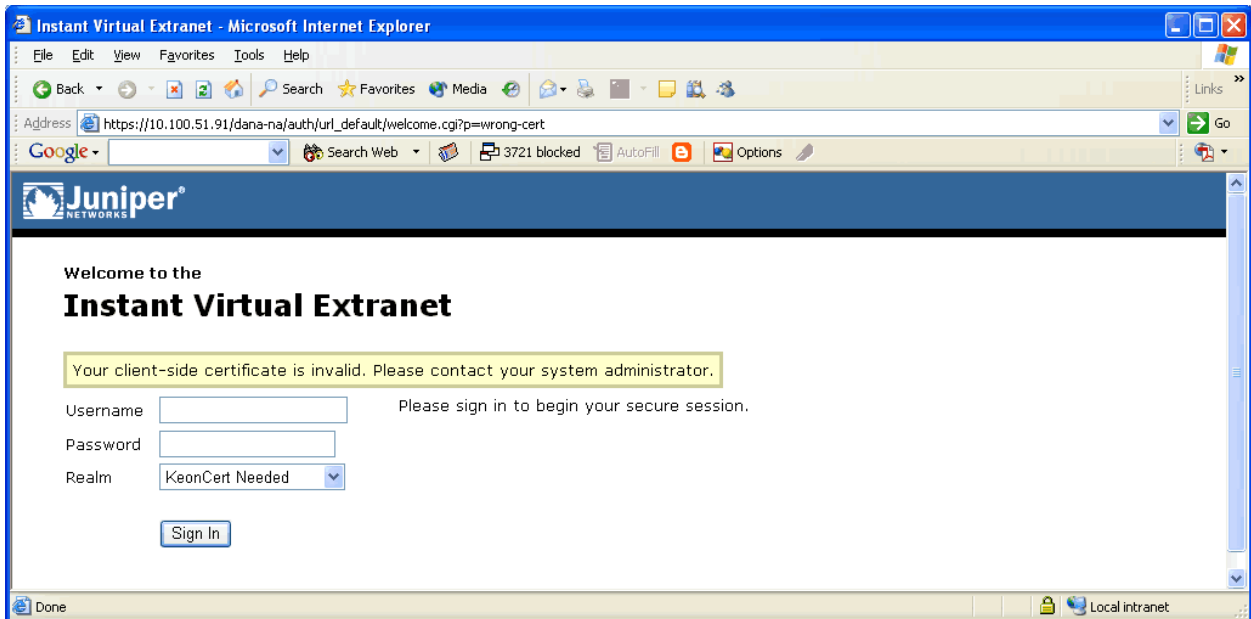
2. Then click **Sign In** and they will be asked to select a certificate. Select the appropriate certificate and click OK.



3. If it is a successful authentication the user will be connect to the SSL VPN.



4. If it is an unsuccessful authentication the user will be denied.



Certification Checklist for 3rd Party Applications

Date Tested: February 4, 2005

Product	Operating System	Tested Version
RSA Keon Certificate Authority	Windows	6.5.1
Juniper Networks SSL VPN	Netscreen-SA-3020	4.1.1

Test Case	Results		
Certificate Enrollment			
P10 Certificate Request			✓
P7 Response installed correctly			✓
CMP Certificate Request			N/A
CMP Response installed correctly			N/A
SCEP Certificate Request			N/A
SCEP Response installed correctly			N/A
Import Certificate			
Import PKCS#12 envelope			N/A
Import via cut & paste			N/A
Install Root Certificate via cut/paste			✓
Install SubCA Certificate via cut/paste			✓
Install Root Certificate via SCEP			N/A
Install SubCA Certificate via SCEP			N/A
Verify Certificate chain is installed			✓
Certificate Usage			
	Sign	Encrypt	SSL
S/MIME	N/A	N/A	
Document and Files	N/A	N/A	
SSL Client Authentication			✓
LDAP Support			
			Results
Name lookup			N/A
Certificate retrieval			N/A
Status Check of Certificate			
	OCSP	CRL	Other
Success with a valid certificate	N/A	✓	N/A
Fails with a revoked certificate	N/A	✓	N/A
Fails with a suspended certificate	N/A	✓	N/A
Pass with a re-instated certificate	N/A	✓	N/A
RSA Keon Web Passport / RSA Sign-On Manager			
Access certificates via MS CAPI (Internet Explorer)		KWP	SOM
		N/A	N/A

SWA

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