Pulse Secure

Java – Secure Application Manager

How-to Guide

Published Date July 2015

Contents

Note: This document applies to IVE OS 6.0 and above.

Introduction:

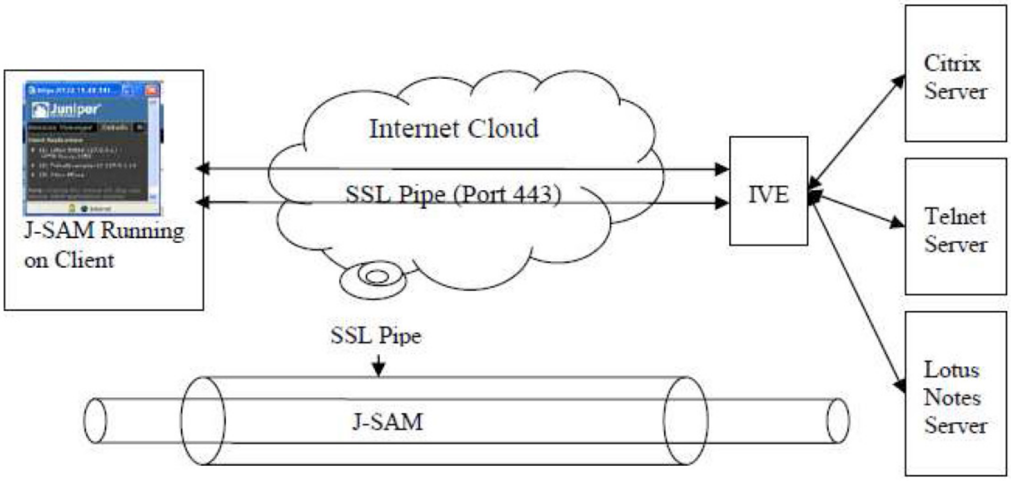
The Java version of the Secure Application Manager provides support for static TCP port client/server applications including enhanced support for Microsoft MAPI, Lotus Notes, and Citrix NFuse. J-SAM also provides NetBIOS support, which enables users to map drives to specified resources. J-SAM works well in many network configurations but does not support dynamic port TCP-based client/server applications, server-initiated connections, or UDP traffic. J-SAM allocates 20-30 MB of RAM when running (the exact amount of memory depends on the Java Virtual Machine (JVM) used), and if caching is enabled, may leave a .jar file on the client machine.

Overview:

The Java version of the Secure Application Manager (J-SAM) provides secure port forwarding for applications running on a remote machine. J-SAM works by directing client application traffic to the J-SAM applet running on a client machine. The IVE assigns a unique IP loopback address to each application server that you specify for a given TCP port. For example, if you specify: app1.mycompany.com, app2.mycompany.com, and app3.mycompany.com for a single port, the IVE assigns a unique IP loopback address to each application: 127.0.1.10, 127.0.1.11, and 127.0.1.12 respectively.

Operation:

When the IVE installs J-SAM on a user's machine, J-SAM listens on the loopback addresses (on the corresponding client port specified for the application server) for clientrequests to network application servers. J-SAM encapsulates the requested data and forwards the encrypted data to the IVE as SSL traffic. The IVE un-encapsulates the data and forwards it to the specified server port on the network application server. The application server returns its response to the IVE, which re-encapsulates and forwards the data to J-SAM. J-SAM then un-encapsulates the server's response and forwards the data to the client application. To the client application running on the local machine, J-SAM appears as the application server. To the application server in your network, the IVE appears as the client application.The following block diagram shows the operation of J-SAM.



Standard Applications are predefined applications that are available on the IVE for easy configuration. As stated earlier, these are Citrix NFuse, Microsoft Outlook/Exchange, Lotus Notes, and NetBIOS file browsing.

Custom applications can be configured to support applications that listen on various TCP ports. Some examples are PC Anywhere, Telnet, Custom Web Application that the administrator does not want to be rewritten by the IVE (this is discussed later under the section: Configuring Web Applications to Run Through J-SAM) and many other applications.

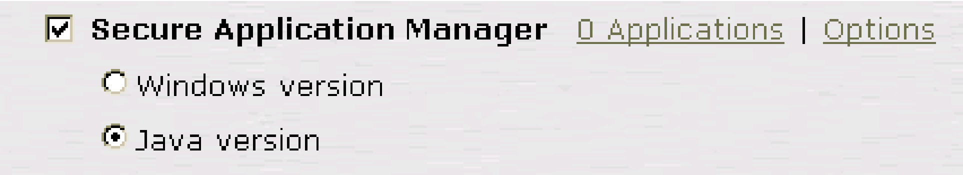
Example configuration:

The following step sequence explains how to configure a telnet (custom) application:

STEP-1: Enable Java SAM in the role.

Users>Roles ><RoleName>>General>Overview

Check Secure Application Manager and select Java Version and save changes.



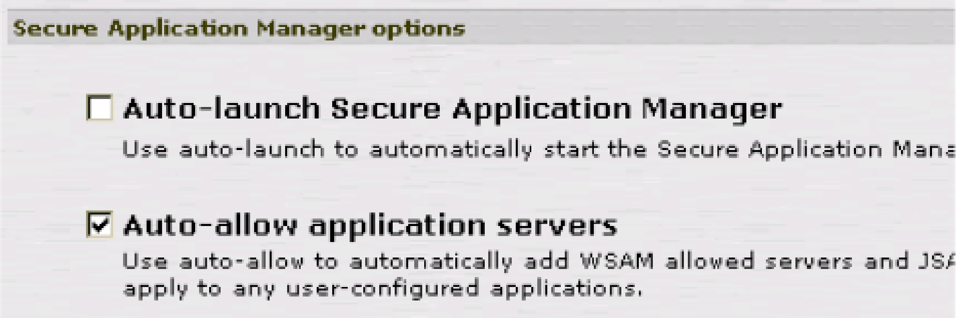
☑ **Secure Application Manager** 0 Applications | Options

○ Windows version

● Java version

STEP-II: Configure SAM Options:

Users>Roles><RoleName>>SAM>Options



Secure Application Manager options

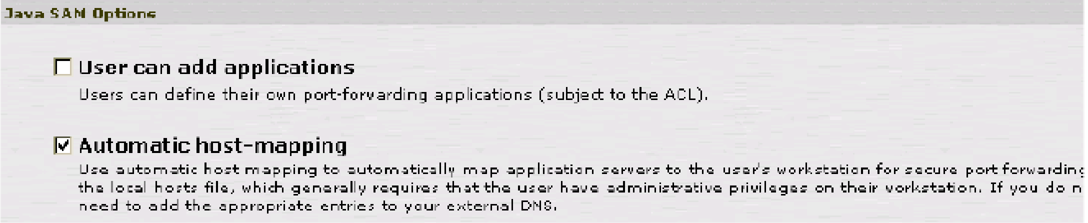
□ **Auto-launch Secure Application Manager**
Use auto-launch to automatically start the Secure Application Mana

☑ **Auto-allow application servers**
Use auto-allow to automatically add WSAM allowed servers and JS/
apply to any user-configured applications.

If user is not desired to start JSAM and JSAM needs to be launched as soon as user logs then enable **"Auto-launchSecure Application Manager".**

If automatic ACL's are to be created for JSAM application servers that will be created by IVE admin then enable "Autoallow application servers". If this option is disabled then IVE admin has to manually add ACL's for application servers under

Resource policies>SAM>Access control.



Java SAM Options

☐ User can add applications

Users can define their own port-forwarding applications (subject to the ACL).

☑ Automatic host-mapping

Use automatic host mapping to automatically map application servers to the user's workstation for secure port forwarding
the local hosts file, which generally requires that the user have administrative privileges on their workstation. If you do n
need to add the appropriate entries to your external DNS.

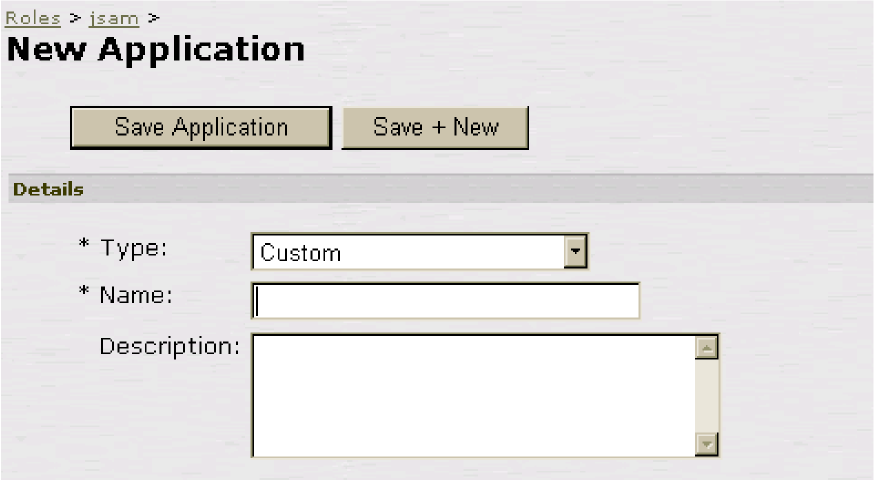
If IVE administrator wants users to add applications after they login then enable option “Users can add applications”

Since JSAM applies to accessing resource via server name, client computers should have a mechanism to resolve JSAM server names either using their host file or DNS server resolving methods.

To make client experience seamless with user minimal user intervention enable option “Automatic host-mapping”. This will edit the client computer host file with entries for JSAM server host names with appropriate loopback addresses. Save changes.

STEP-III: Add Applications:

Users>Roles><RoleName>>SAM>Applications

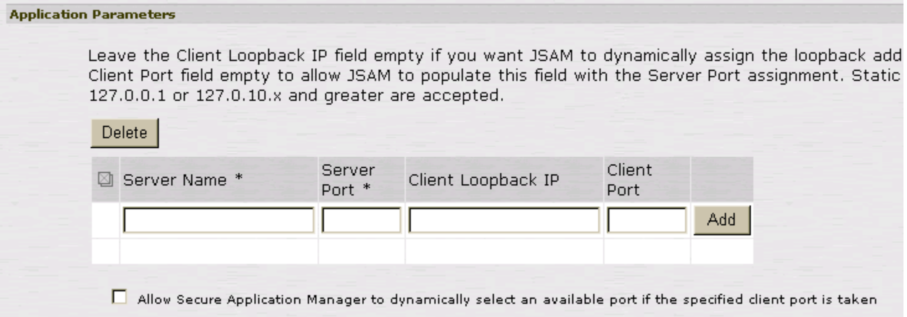


New Application

Details

* Type:	Custom
* Name:	
Description:	

- *Type: For applications which are other than the pre-defined applications use the Type as “Custom”.
- *Name: Any name to identify application / server



Application Parameters

Leave the Client Loopback IP field empty if you want JSAM to dynamically assign the loopback add
Client Port field empty to allow JSAM to populate this field with the Server Port assignment. Static
127.0.0.1 or 127.0.10.x and greater are accepted.

☒	Server Name *	Server Port *	Client Loopback IP	Client Port	
					Add

☐ Allow Secure Application Manager to dynamically select an available port if the specified client port is taken

- *Server Name: Add the server's host name or Fully qualified domain name that needs to be accessed via JSAM. (IVE should be able to resolve the name when resource is accessed).
- *Server Port: Port on which application is currently running / listening.

Client Loopback IP: Will be automatically configured by IVE. It will be in range of 127.0.1.10, 127.0.1.11, 127.0.1.12 etc.

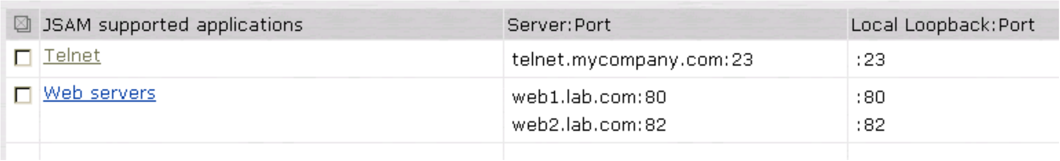
Client Port: Will be automatically configured by IVE.

- Enable "Allow Secure Application Manager to dynamically select an available port ..." checkbox if J-SAM is listening for multiple hosts on the same port and you want J-SAM to select an available port when the client port you specify is taken. The client application must allow you to specify the port number for the connection inorder to use this option.
- Click Add application.

Note: You may define all your custom application servers in this same page or you may create a separate custom application ("New Application") for each application.

- When finished adding custom applications, click "Save Application" to save the configuration.

Following shows examples of few customer configured applications with J-SAM:



□ JSAM supported applications	Server:Port	Local Loopback:Port
□ Telnet	telnet.mycompany.com:23	:23
□ Web servers	web1.lab.com:80 web2.lab.com:82	:80 :82

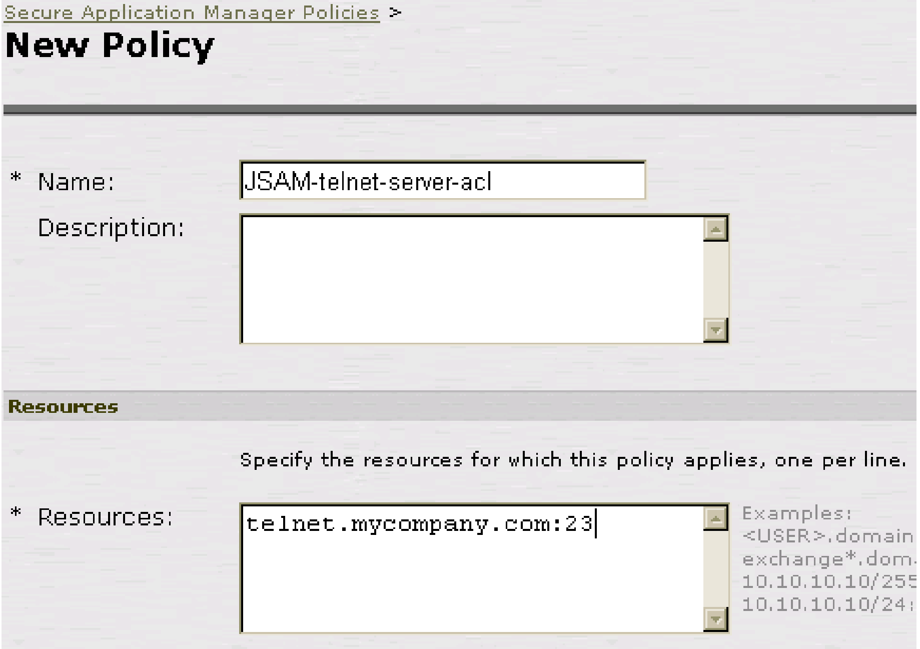
STEP–IV: Configure SAM Resource Policies:

Resource policies> SAM>Access control.

After applications are added to the SAM configuration under the Role, configure access policies to allow connection(s) to the backend server(s). Restrict the traffic to intended server(s) only. Avoid open access to any backend server (*:*).

Click on New Policy.

Add a policy name, under resources add the server name or IP address of the server that is to be accessed via JSAM along with port number.



Secure Application Manager Policies >

New Policy

* Name: JSAM-telnet-server-acl

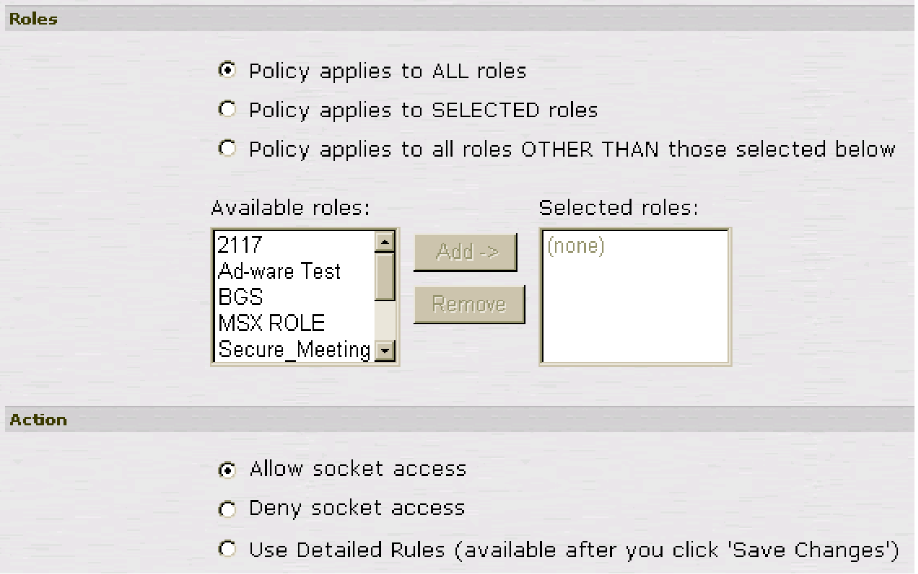
Description:

Resources

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

* Resources: telnet.mycompany.com:23

Select the role to which this policy applies and allow / deny socket access.



Roles

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

Available roles:
2117
Ad-ware Test
BGS
MSX ROLE
Secure_Meeting

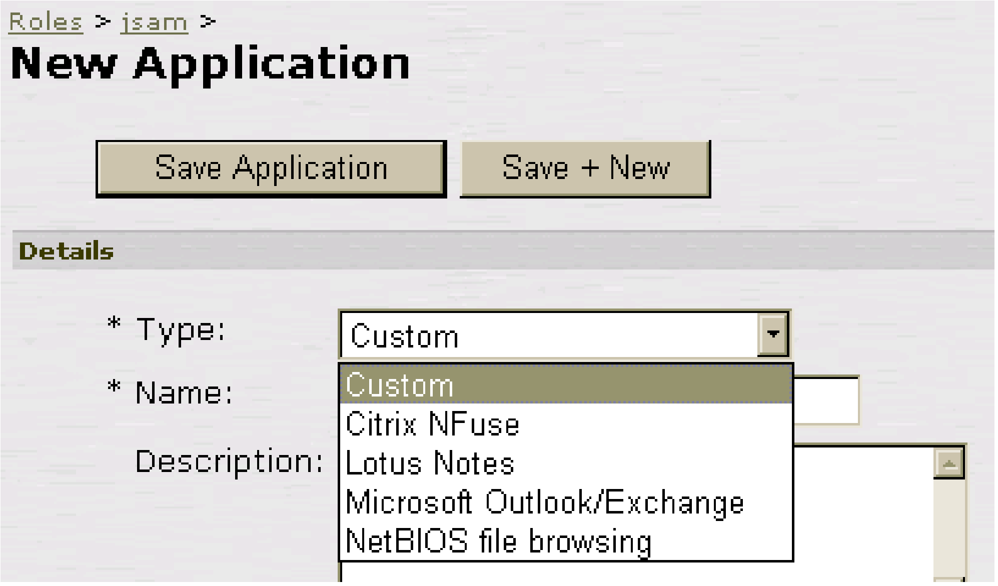
Selected roles:
(none)

Action

● Allow socket access
○ Deny socket access
○ Use Detailed Rules (available after you click 'Save Changes')

Save changes.

JSAM – Standard application support:



* Type: Custom

a. **Citrix Web Interface for MetaFrame (NFuse Classic)**

Remote users can use the Citrix Web Interface for MetaFrame server to access a variety of applications via the IVE. This process does not require any alterations to the user permissions on the client.

After a user browses to a Citrix Web Interface for MetaFrame server and selects an application, the server sends an ICA file to the client. When the IVE rewrites the ICA file, it replaces host names and IP addresses with pre-provisioned loopback IP addresses. The ICA client then sends application requests to one of the loopback IP addresses. The Secure Application Manager encapsulates the data and sends it to the IVE. The IVE un-encapsulates the data and sends it to the appropriate MetaFrame server using port 1494 or 2598 (depending on the client).

b. **Lotus Notes**

Remote users can use the Lotus Notes client on their PCs to access email, their calendars, and other features through the IVE. This ability does not require a network layer connection, such as a VPN. In order for this feature to work for remote users, they need to configure the Lotus Notes client to use "localhost" as their location setting (that is, their Home Location, Remote Location, or Travel Location setting). The Secure Application Manager then picks up connections requested by the Lotus Notes client. The following procedure describes the interactions between the Lotus Notes client and a Lotus Notes Server via the IVE.

1. The user starts the Lotus Notes client with the location setting. The client uses the HTTP Tunnel proxy setting for its location setting. Note that you must set the HTTP Tunnel proxy setting to use localhost (or 127.0.0.1) as the proxy address and 1352 as the proxy port.

2. The Lotus Notes client connects to the Secure Application Manager and starts sending requests for email.

3. The Secure Application Manager encapsulates and forwards requests from the Lotus Notes client to IVE over SSL.

4. The IVE un-encapsulates the client data and looks in the Lotus Notes request to find the target Lotus Notes Server. The request is then forwarded to the target server.

c. **MS Outlook**

Remote users can use the Microsoft Outlook client on their PCs to access email, their calendars, and other Outlook features through the IVE. Versions of MS Outlook currently supported are MS Outlook 2000 and MS Outlook 2002. This ability does not require changes to the Outlook client and does not require a network layer connection, such as VPN. In order for this feature to work for remote users, the network settings of the user's PC must resolve the name of the Exchange Servers embedded in the Outlook client to the local PC (127.0.0.1, the default localhost IP address). We recommend that you configure the IVE to automatically resolve Exchange server host names to the localhost by temporarily updating the hosts file on a client computer through the automatic host-mapping option.

1. The user starts the MS Outlook client. Outlook tries to contact the Exchange Server exchange1.yourcompany.com. The IVE resolves the Exchange Server host name to 127.0.0.1 (localhost) through temporary changes to the hosts file.

2. Outlook connects to the Secure Application Manager running on the user's PC and then starts sending requests for email.

3. The Secure Application Manager encapsulates and forwards all the requests from the Outlook client to the IVE over SSL.

4. IVE un-encapsulates the client data and looks in the MAPI request to find the target Exchange Server. The request is then forwarded to the target server.

5. Each request in the MAPI protocol encodes the target server for the request. When MAPI requests arrive from the Secure Application Manager, the IVE server looks in each of them and dispatches them to the appropriate target server. This process works transparently even if there are multiple Exchange Servers.

6. The Exchange Server responds to the IVE with email data.

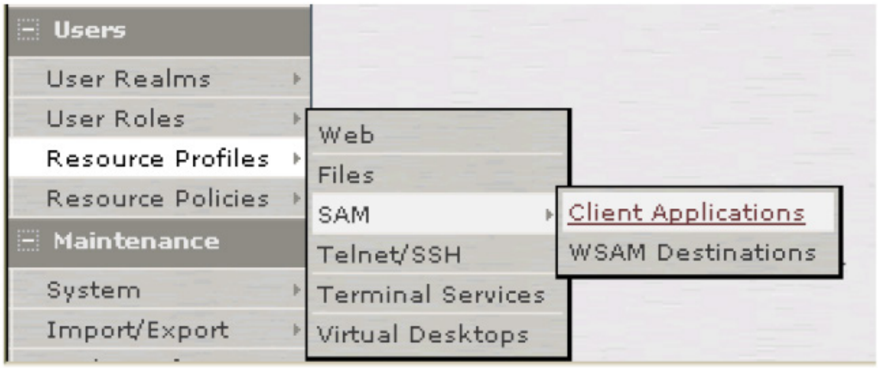
d. **NETBIOS file browsing:**

Select this option to tunnel NetBIOS traffic through JSAM

Enter the fully-qualified host name for your application servers in the Servers field.

JSAM resource profiles

JSAM resource profiles configure JSAM to secure traffic to a client/server application. When you create a JSAM application resource profile, the JSAM client tunnels network traffic generated by the specified client applications to servers in your internal network.



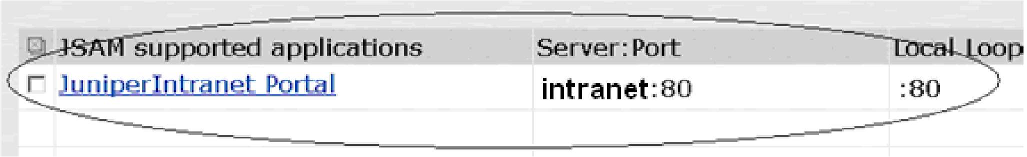
JSAM profiles support Custom and pre-defined applications as mentioned in above sections.

Configuring Web Applications to Run Through J-SAM

The following steps show how a web application can bypass the IVE web rewriter so that the traffic goes through J-SAM.

Users > Roles > <RoleName> > SAM > Applications >

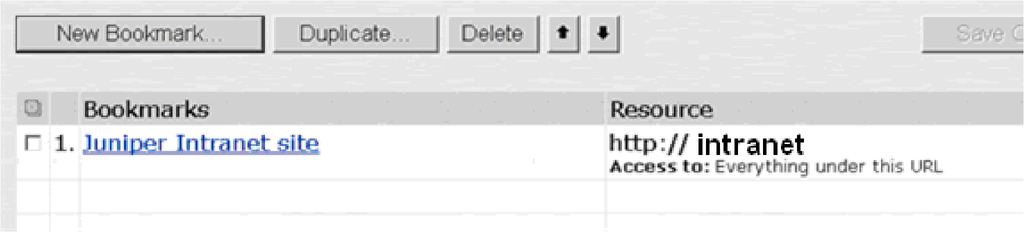
- **Configure the application under J-SAM.**



□ JSAM supported applications	Server:Port	Local Loop
□ JuniperIntranet Portal	intranet:80	:80

Users > Roles > <RoleName> > Web > Bookmarks >

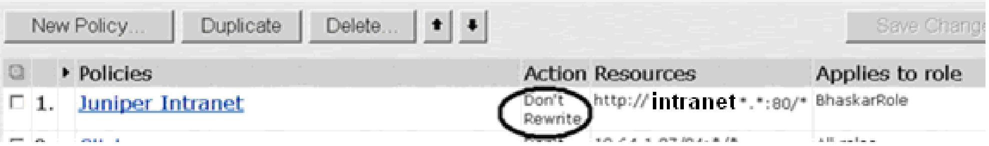
- **Add a Web bookmark**



□	Bookmarks	Resource
□	1. Juniper Intranet site	http:// intranet Access to: Everything under this URL

Resource Policies > Web > Selective Rewriting >

- **Add a rewrite rule**



		Policies	Action	Resources	Applies to role
□	1.	Juniper Intranet	Don't Rewrite	http://intranet*.*:80/*	BhaskarRole

Remember to move this “don’t rewrite” policy before the policy (top of list) that rewrites all (*:* policy) and then save the changes.

Note: In general selective rewriting policies are configurable for only web based applications. This means, those applications which are accessible using a web browser like Internet Explorer. Port used could be any thing. One more thing, this rewriting rule is necessary, only if the user would like to add a bookmark under IVE bookmarks page. If the end user accesses the backend web portal directly i.e. by opening a new browser windowand types the URL then this rewrite rule is not necessary.

J-SAM Troubleshooting:

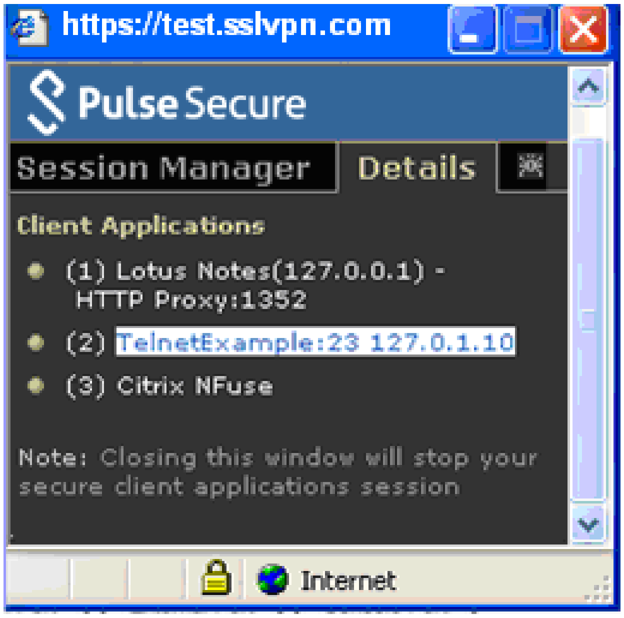
1. The first step to troubelshoot JSAM is to check if the entries in the hosts file on the client machineare created and loopback addresses are assigned.

   To see whether application servers configured in J-SAM are assigned loopback addresses, use DNS query (nslookup) and/or ping.

Example:

```
C:\>ping telnet.server.company

Pinging telnet.server.company [127.0.1.10] with 32 bytes of

data:

Reply from 127.0.1.10: bytes=32 time<10ms TTL=128

Reply from 127.0.1.10: bytes=32 time<10ms TTL=128

Reply from 127.0.1.10: bytes=32 time<10ms TTL=128

Reply from 127.0.1.10: bytes=32 time<10ms TTL=128

Ping statistics for 127.0.1.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. After J-SAM launches on the client system we can look at the following:



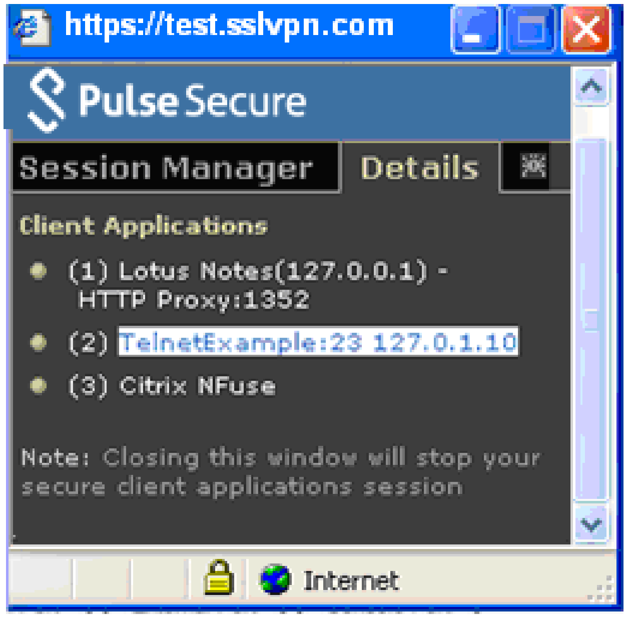
Client Applications

- (1) Lotus Notes(127.0.0.1) - HTTP Proxy:1352
- (2) TelnetExample:23 127.0.1.10
- (3) Citrix NFuse

Note: Closing this window will stop your secure client applications session

Is Status OK? Are Sent/Received bytes incrementing?

Details: list

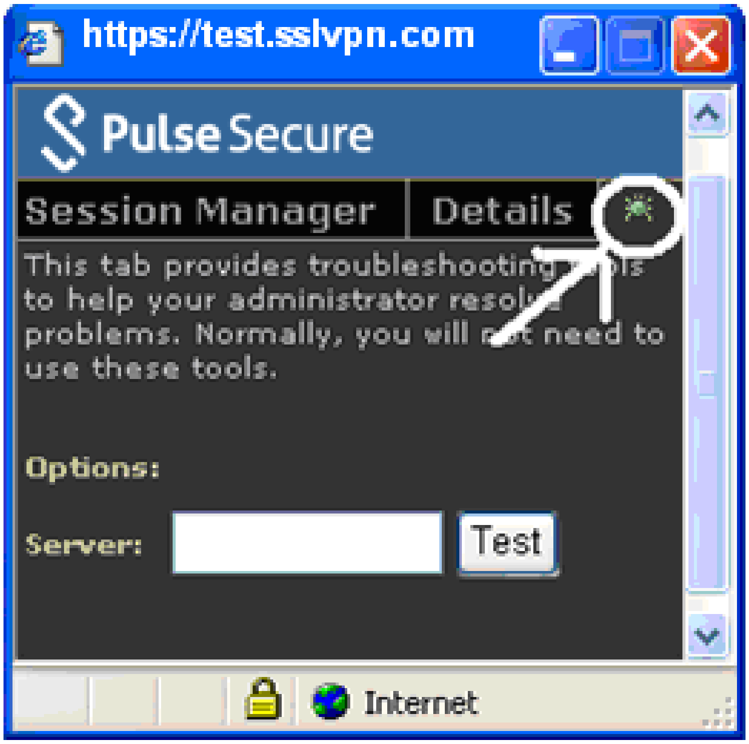


Client Applications

- (1) Lotus Notes(127.0.0.1) - HTTP Proxy:1352
- (2) TelnetExample:23 127.0.1.10
- (3) Citrix NFuse

Note: Closing this window will stop your secure client applications session

Details: list of applications configured



This tab provides troubleshooting tools to help your administrator resolve problems. Normally, you will not need to use these tools.

Options:

Server: [Test]

We can also check for the loopback address assigned for a server configured in J-SAM by entering the server name in the above window and clicking test.

Note: To check access related issues, Java Console log on the client shows any rejections of web requests from client. Also it shows any exceptions errors.

Below are the items to capture for further troubleshooting of J-SAM:

1. IVE Software Version and Build
2. Client Operating System, Browser, Service Pack, and JVM used.
3. TCPdump taken on the IVE's internal port while the problem is happening.
4. TCPdump taken on the client going straight to the server when it's working.
5. Screen Shots of pertinent J-SAM configurations as discussed in this document.
6. Policy trace for "Launch JSAM" and "SAM Policies"

7. Pertinent (Sun or Microsoft) Java Console
8. You can enable or disable client-side logs by clicking System > Log/Monitoring > Client Logs > Settings in the Web console.
    - For Windows 2000/XP, when you enable logging, JSAM adds C:\Documents and Settings\username\Application Data\Pulse Secure\Java Secure ApplicationManager\dsJSAM_win0.log and dsJSAM_win1.log
    - For Windows Vista, when you enable logging, JSAM adds C:\Users\username \AppData\Local\Temp\Low\Pulse Secure\Java Secure Application Manager\jsamtool.log and dsJSAM_win1.log.

Supported Platforms list as of IVE OS 6.5R2:

The below table lists the supported client OS and browser version details. This table is extracted from IVE OS 6.5R2's supported platform document. The list may vary depending on what version of IVE OS you are running. Please refer to the corresponding supported platforms document on our support site.

Qualified platforms:

Platform	Operating System : list of browsers and Java Environment
Windows	• XP Professional SP3 32 bit: Internet Explorer 7.0, 8.0 and Firefox 3.0.Sun JRE 6 • Vista Enterprise SP1 32 bit: Internet Explorer 7.0, 8.0 and Firefox 3.0.Sun JRE 6
Mac	• Mac OS X 10.5.0, 32 bit and 64 bit: Safari 3.2 Sun JRE 6 • Mac OS X 10.4.3, 32 bit only: Safari 2.0. Sun JRE 5
Linux	• OpenSuse 11, 32 bit only: Firefox 3.0.Sun JRE 6 • Ubuntu 8.10, 32 bit only: Firefox 3.0.Sun JRE 6

Compatible platforms:

Platform		Operating System : list of browsers and Java Environment
Windows	Vista Enterprise/Ultimate/Business/Home Basic/Home Premium with Service Pack 1 or 2 on 32 bit or 64 bit platforms XP Professional with SP2 or SP3 on 32 bit or 64 bit 2000 Professional SP4 XP Home Edition SP2 XP Media Center 2005 Windows 2003 server SP2, 32bit and 64 bit	Internet Explorer 8.0 * Internet Explorer 7.0 * Internet Explorer 6.0 * Firefox 3.5 Firefox 3.0 Firefox 2.0 Sun JRE 5/1.5.07 and above Microsoft JVM – for Windows 2000 (* Wherever-applicable)

Platform		Operating System : list of browsers and Java Environment
Mac	Mac OS X 10.6, 32 bit and 64 bit Mac OS X 10.5.x, 32 bit and 64 bit Mac OS X 10.4.x, 32 bit only Mac OS X 10.3.x, 32 bit only	Safari 1.0 and above Sun JRE 5/1.5.07 and above
Linux	OpenSuse 10.x, 32 bit only Ubuntu 7.10, 32 bit only Red Hat Enterprise Linux 5, 32 bit only	Firefox 2.0 and above
Solaris	Solaris 10 ,32 bit only	Mozilla 2.0 and above

Note: For Mac, Linux, and Solaris implementations:

1. Automatic editing of hosts file is only available for root users
2. Ports less than 1024 are only available for root users