

Java – Secure Application Manager

Abstract:

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.

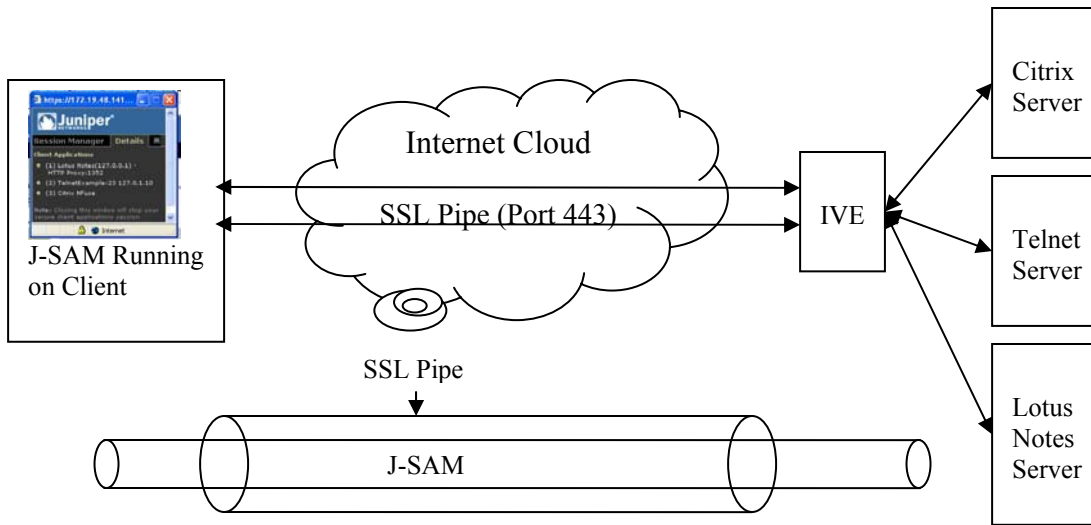
Overview:

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 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 client requests 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 preconfigured applications available on the IVE for easy configuration. As stated earlier, these are Citrix, Exchange, Notes, and NetBIOS (for drive mapping).

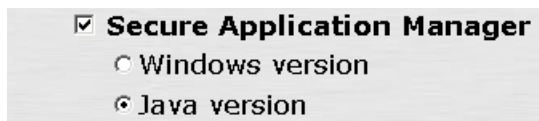
Custom applications can be configured to support applications that listen on various TCP ports. Some examples are PC Anywhere, Telnet, Custom Web Application that the administrator does not want to be rewritten by the IVE (this is discussed later under the section: **Configuring Web Applications to Run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

Example configuration:

The following step sequence explains how to configure a telnet application
 STEP-1: Enable Java SAM in the role.

Users → Roles → <RoleName> → General → Overview →

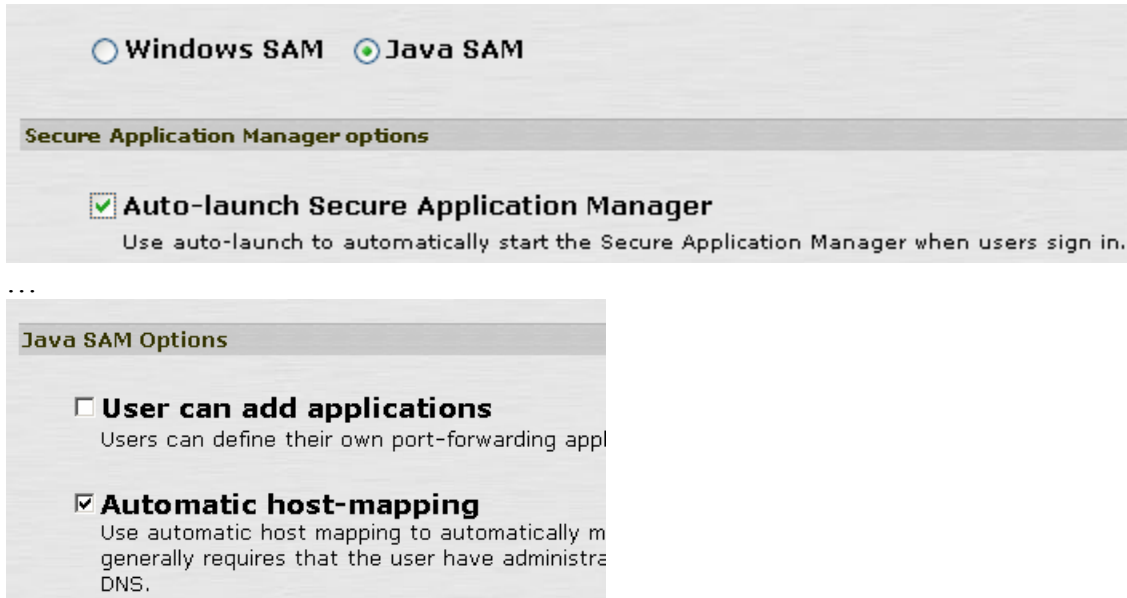
Check Secure Application Manager and select Java Version and save changes.



STEP-II: Configure SAM Options:

Users → Roles → <RoleName> → SAM → Options

Most of the options are self explanatory. Out of these options, Auto Launch Secure Application Manager and Automatic host-mapping are typically enabled. Some users do not know how to trigger J-SAM from the end-user login and may face some difficulty. If automatic host-mapping is disabled, users will need to edit their hosts file manually.



STEP-III: Add Applications:

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

Click on Add Application and fill in the following fields:

Name: Arbitrary name to identify the application.

Server Name: Use hostname or Fully Qualified Domain Name (FQDN).

Note: The IVE has to be able to resolve via DNS and reach the Server Name.

Server Port: Port on which the application is currently running (listening).

Client Loopback IP: can be left blank or defined.

Select the **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 in order to use this option.

Roles > bhaskar >
New Application

Save Application Save + New

Details

* Name:

Description:

Application Type

Standard application Custom application

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

Delete

* Server Name	* Server Port	Client Loopback IP	Client Port	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add

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

Click Add to add this application. When finished adding custom applications, click “Save Application” to save the configuration.

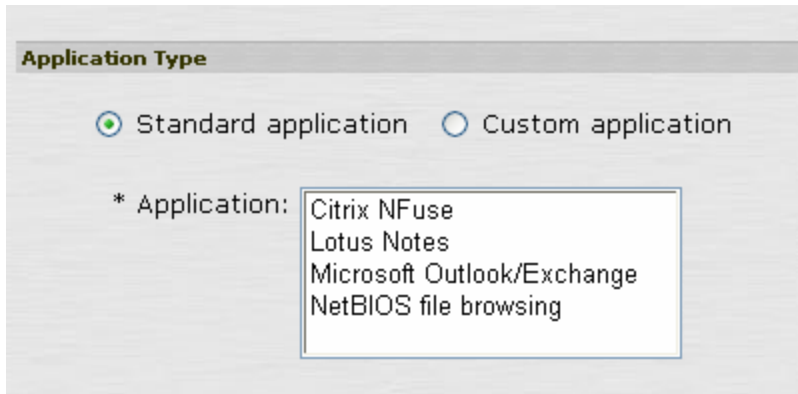
Note: You may define all your custom application servers in this same page or you may create a separate custom application (“New Application”) for each application.

The following shows few applications configured with J-SAM.

<input type="checkbox"/> JSAM supported applications	Server:Port	Local Loopback:Port
<input type="checkbox"/> Telnet	telnet.server.company:23	:23
<input type="checkbox"/> Citrix	*:1494,2598	127.0.2.1-5:1494,2598
<input type="checkbox"/> Lotus	*:1352	*:1352
<input type="checkbox"/> FileBrowsing	File-server1 File-server2 File-server3	*:139

JSAM – Standard application support:

You will also see a list of standard applications when you click on Standard Application button under “Role → <RoleName> → SAM → Applications → Add Application”



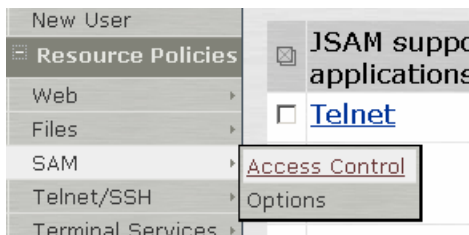
Currently we support four standard applications as shown above. Among them, Outlook/Exchange support is limited to Outlook 2000/Exchange 2000 only. WSAM is recommended for supporting Outlook 2003/Exchange 2003.

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 (*.*).

Select Access Control as show in the screenshot:



Click on New Policy

* **Name:** **Required:** Label to reference this policy.

Defining resources to allow access:

Resources

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

* Resources: Examples:
 <USER>,domain.com:22,23
 exchange*,domain.com;*
 10.10.10.10/255.255.255.0:80,443,8080
 10.10.10.10/24:8000-9000

Applying this rule to a selective role or to all roles:

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:

Add -> Remove

Action:

Action

Allow socket access

Save changes.

The above configuration allows users to access the backend Citrix server farm with an IP address range: 172.27.32.0 to 172.27.32.32 with specific ports: 1494 and 2598.

Configuring Web Applications to Run Through J-SAM

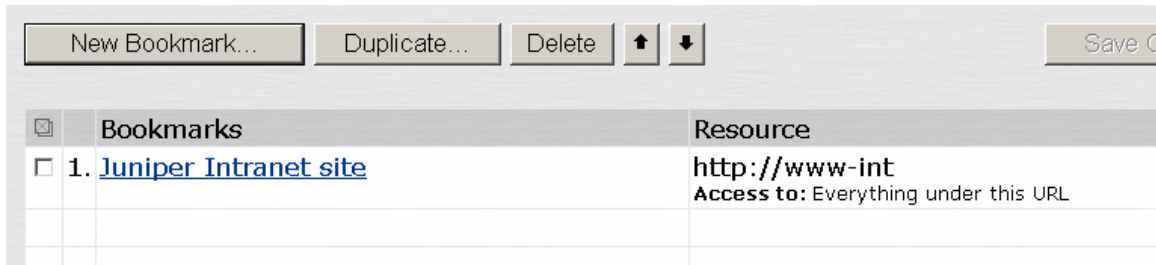
The following steps show how a web application can bypass the IVE web rewriter so that the traffic goes through J-SAM.

- Users → Roles → <RoleName> → SAM → Applications →
- Configure the application under J-SAM.

<input checked="" type="checkbox"/> JSAM supported applications	Server:Port	Local Loop
<input type="checkbox"/> JuniperIntranet Portal	www-int:80	:80

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

- Add a Web bookmark



Resource Policies → Web → Selective Rewriting →

- Add a rewrite rule



Remember to move this “don’t rewrite” policy before the policy that rewrites all and then save the changes.

NOTE: *In general selective rewriting policies are configurable for only backend web 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 we would like to add a bookmark under IVE bookmarks page. If the end user triggers the backend web portal directly opening a new IE and types the URL to send traffic directly through JSAM, this rewrite rule is not necessary.*

J-SAM Troubleshooting:

To ensure smooth operation of J-SAM, check that the entries in the hosts file on the client were written properly and loopback addresses were assigned.

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

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

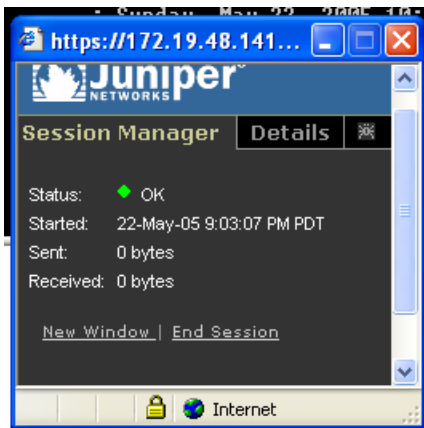
```
Pinging telnet.server.company [127.0.1.10] with 32 bytes of data:
```

```
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
```

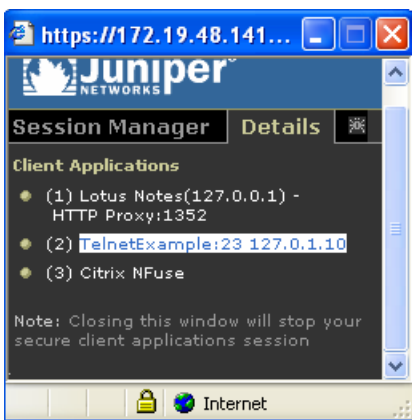
Ping statistics for 127.0.1.10:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

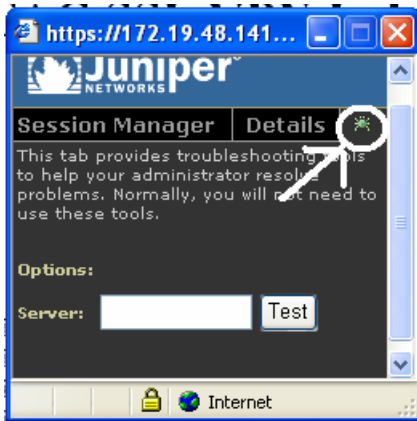
After J-SAM launches on the client system we can look at the following:



Is Status OK? Are Sent/Received bytes incrementing?



Details: list of applications configured



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.

Here 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

IMPORTANT:

On clients using Windows XP SP2 without Microsoft HotFix KB884020, J-SAM will not function for more than one application. Due to a bug in Microsoft security policies, we are unable to use multiple loopback entries on the client machine. This restricts us to use only one IP address.

Microsoft hotfix can be downloaded from the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=17D997D2-5034-4BBB-B74D-AD8430A1F7C8&displaylang=en>

Once this hotfix is installed we can use multiple loopback IP addresses on the client system and J-SAM functions properly.

Client side requirements:

Supported Platforms:

- Windows XP: Internet Explorer 6.0 running Microsoft JVM or Sun JVM 1.4.2_04
- Windows XP SP2*: Internet Explorer 6.0 running Microsoft JVM or Sun JVM 1.4.2_04
- Windows 2000: Internet Explorer 5.5 SP2 and Internet Explorer 6.0 running Microsoft JVM or Sun JVM 1.4.2_04
- Macintosh OS 10.3.3: Safari 1.2 running Sun JVM 1.4.2_04
- Mac OS 10.2.8: Safari 1.0 running Sun JVM 1.4.1_01
- Red Hat Linux 9.0: Mozilla 1.6 running Sun JVM 1.4.2_04

Note:

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

Compatible platforms:

- Windows 98 SE: Internet Explorer 6.0 running Microsoft JVM and Sun JVM 1.4.2_04
 - Note: Drive mapping is not supported
- Red Hat Linux 9.0: Netscape 7.1 running Sun JVM 1.4.2_04
 - Note: Automatic editing of hosts file is available for root user