How to run PINsafe on non-default ports

Contents

Overview

Some networks allow only traffic on certain ports, and therefore it may be necessary to make requests to Swivel over ports that are accessible, such as 80 or 443. This can be done by the following methods:

- Using Port Address Translation (PAT) on the organisations firewall.
- Using Port Address Translation (PAT) on the Swivel hardware or virtual appliance.
- Changing the port on which Swivel runs (not recommended on Swivel virtual or hardware appliances).

For software installations and ports above 1024 then the port which Tomcat runs can be changed. If it is a Swivel virtual or hardware appliance or Linux install where the required port is less than 1024 then for security reasons, the section on Port Address Translation should be followed.

Where the port is changed then references to that port would need to be changed in the integrations, such as login pages.

Port Address Translation: Running Swivel on port 443

There may be times when it is required for Swivel to respond on port 443, the default port for https. It is not recommended to do this by editing the server.xml file as this has other implications. An alternative approach is to use the Appliance firewall to re-route inbound traffic on port 8443 to port 443. Once the port is changed all Swivel references using 8443 must be updated.
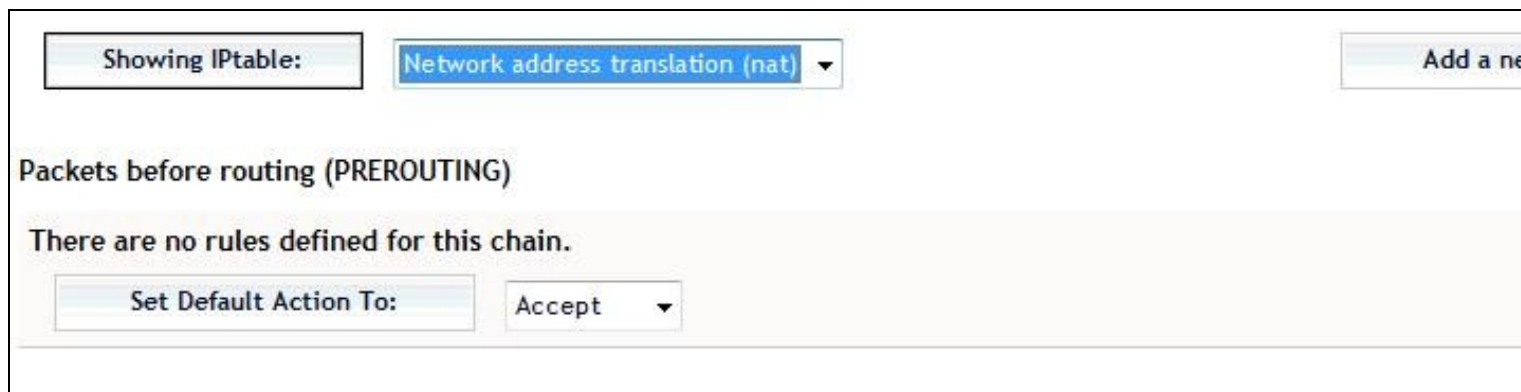
The options for this are:

- Use Port Address Translation (PAT) on the firewall device

- Use Port Address Translation (PAT) on the Swivel Appliance, as detailed below for access to the webmin see Webmin How To Guide

These are the steps required to achieve this.

Log onto the Swivel WEBMIN interface on https://<IPADDRESS>:10000

Select the Networking->Firewall option

Selecting NAT option

Then select the NAT option (as shown) and click Showing IPTable

Under the PREROUTING (top) section select **Add Rule**

Firewall Rule required to reroute from 443 to 8443
The rule has the following elements:

A comment or name, eg 443 to reroute to 8443

Specify that it is a re-direct action required.

Target port, the port TO which traffic is to be directed, in this case 8443.

Network protocol for which the rule applies, in this case TCP

Destination port equals 443 in this case.

Once this is in place select **Create Rule**, then **Apply Configuration**

This rule means that any traffic inbound on port 443 will be redirected to port 8443 before being forwarded to Swivel.

You can test this by first retrieving a TURing image from https://<ip address>:8443/proxy/SCImage?username=test and then trying https://<ip address>:8443/proxy/SCImage?username=test, without the 8443. Both urls should produce the same result.

Remember to update authentication devices that reference the image port.

Restart networking or the firewall with

```
service iptables restart
```

The above steps create a firewall rule in the file /etc/sysconfig/iptables with the following entry:

```
# 443 to 8443
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
COMMIT
# Completed
```

If this is not present, ensure that the Apply Configuration button was pushed.

Swivel Firewall rules with PAT

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1311 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 61616 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
# Generated by webmin
*nat
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# Port Address Translation 443 to 8443
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
COMMIT
# Completed
```

Swivel Firewall rules with 443 and 80 PAT

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1311 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 61616 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
# Generated by webmin
*nat
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# Port Address Translation 443 to 8443
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
```

```
#80 to 8080
-A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
COMMIT
# Completed
```

Troubleshooting

PAT not started at boot time

Ensure that the **Apply Configuration** button has been pressed.

Known Issues

Some versions of the appliance up to 2.0.13 failed to save the firewall changes, so changes would disappear after the firewall was rebooted. To see if an appliance is affected, reboot the appliance after making configuration changes.

To overcome this issue, Ensure this fix is added then make changes to the firewall:

Edit the file /etc/webmin/firewall/config

Add the following line as in the image below. For information on how to edit files use WinSCP How To Guide or the PuTTY How To Guide

save_file=/etc/sysconfig/iptables

When changes are made to the webmin and applied they will be written to the file /etc/sysconfig/iptables. Once the changes are made, Webmin will recognise the new path and so no services require a restart.

Changing the Port on which Swivel Runs

There may be times where you wish to change the ports on which Swivel listens, for example if this clashes with another application or if particular ports are blocked by firewall policies.

Note This approach should not be used to run Swivel on Ports lower than 1024. eg port 443, as this has security implications, for example this would mean that Tomcat would have to be run as root on a linux system. The next section detailing Port Address Translation and firewall rewriting, provides a way of achieving the same result in a different way. For ports above 1024 the below method can be used.

To change the ports used by Swivel you need to edit the apache-tomcat/conf/server.xml file

In this file there will be definitions of connectors which specify the port to be used

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />
```

Therefore to change Swivel to run on port 8181, this would be changed to

```
<Connector port="8181" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />
```

Tomcat would then need to be restarted.

A Swivel appliance will have three connectors defined.

```
  <Connector address="localhost" port="8181" />
  <Connector address="0.0.0.0" port="8080" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="/home/swivel/.key
  <Engine name="Catalina" defaultHost="localhost">
    <Host name="localhost" appBase="webapps" />
  </Engine>
 </Service>

 <Service name="Catalina-proxy">
   <Connector address="0.0.0.0" port="8443" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="/home/swivel/.key
```

There is no need to change port 8181 as this is only used internally Port 8080 serves the admin console and port 8443 is used to the external interface, eg to supply the TURing image.