Introduce websockify_can_connect_all boolean for non-VNC connections

On a fresh all-in-one installation of foreman with foreman-installer --scenario katello on Centos 7 I can't get the noVNC console to work.

When trying to connect to the console I get the following in audit.log

type=AVC msg=audit(1516297409.070:335): avc: denied { name_connect } for pid=1728 comm="websockify.py" dest=39124 scontext=system_u:system_r:websockify_t:s0 tcontext=system_u:object_r:ephemeral_port_t:s0 tclass=tcp_socket
type=SYSCALL msg=audit(1516297409.070:335): arch=c000003e syscall=42 success=no exit=-13 a0=7 a1=7 ff006407d0 a2=10 a3=1 items=0 ppid=1720 pid=1728 uid=993 gid=990 euid=993 egid=993 fsuid=993 fsgid=990 tty=(none) ses=4294967295 comm="websockify.py" exe="/usr/bin/python2.7" subj=system_u:system_r:websockify_t:s0 key=(null)

I have successfully installed the server certificate and disabling SELinux (setenforce 0) will make the console work. However I can't get it to work with SELinux enabled, even with foreman-selinux and katello-selinux packages installed.

Server is Centos 7.4
Foreman 1.16.0
Katello 3.5.0
Foreman-selinux 1.16.0
Katello-selinux 3.0.2

Associated revisions
Revision 3efbd524 - 05/30/2018 08:49 AM - Lukas Zapletal
Fixes #22317 - introduced websockify_can_connect_all

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Lukas Zapletal</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>1.18.0</td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Pull request</td>
<td><a href="https://github.com/theforeman/foreman-selinux/pull/77">https://github.com/theforeman/foreman-selinux/pull/77</a></td>
</tr>
<tr>
<td>Triaged</td>
<td></td>
</tr>
<tr>
<td>Bugzilla link</td>
<td></td>
</tr>
</tbody>
</table>

## Description

On a fresh all-in-one installation of foreman with foreman-installer --scenario katello on Centos 7 I can't get the noVNC console to work.

When trying to connect to the console I get the following in audit.log

I have successfully installed the server certificate and disabling SELinux (setenforce 0) will make the console work. However I can't get it to work with SELinux enabled, even with foreman-selinux and katello-selinux packages installed.

Server is Centos 7.4
Foreman 1.16.0
Katello 3.5.0
Foreman-selinux 1.16.0
Katello-selinux 3.0.2

## Associated revisions

Revision 3efbd524 - 05/30/2018 08:49 AM - Lukas Zapletal
Fixes #22317 - introduced websockify_can_connect_all

## History

- Subject changed from SELinux denies websockify on Centos 7 to Introduce websockify_can_connect_all boolean for non-VNC connections
- Tracker changed from Bug to Feature

Hello there, our policy only allows connecting to VNC ports to websockify:

https://github.com/theforeman/foreman-selinux/blob/develop/foreman.te#L394

You are trying to connect to some weird port identified as ephemeral_port_t, you need to tune the policy for that. Allow that or put websockify to permissive. Or modify firewall so you connect to what is considered a VNC port by SELinux.

I am turning this into work item of adding boolean websockify_can_connect_all that will do the job.
Thanks for your response.

I'm not sure why it's using a weird port as I haven't made any changes to the system or settings after the initial installation (at least not intentionally).

In any case, setting it to permissive as you suggest is working fine

```
[root@foreman ~]# semanage permissive -a websockify_t
[root@foreman ~]# semanage permissive -l
```

Customized Permissive Types

```
websockify_t
```

---

Thanks, I will do the boolean in a minute so you can turn it on in future releases. Out of curiosity, what virtualization are you connecting to?

I'm connecting to a newly installed XenServer 7.3 pool.

---

- Legacy Backlogs Release (now unused) set to 330
- Target version deleted (1.18.0)

Applied in changeset 3efbd5248acdf1e4e1793cb69709f5d3078dc28f.