TUSK Firewall Defaults

TUSK Firewall Defaults

TUSK servers only need a few services exposed to the local network, or the network at large. They are:

- SSH port 22/tcp - This provides shell access for system management. Access should be restricted to only internal hosts or networks: TUSK servers that are exposed to the Internet should not leave SSH exposed to anything but local administrative accounts and servers, to protect them.
- HTTP port 80/tcp - Basic web service port. This is typically accessible to the entire local network or to the Internet at large for public sites.
- HTTPS port 443/tcp - Encrypted web service port. This handles secured web traffic, and should be exposed to the same entire local network or the Internet at large.
- MySQL port 3306/tcp - Database access for TUSK. This should allow access only to the TUSK web servers and to designated MySQL slaves for backup or failover access.
    - DO NOT DIRECTLY EXPOSE MYSQL TO THE INTERNET AT LARGE.
- NFS - TUSK servers may be NFS clients of a NAS or storage server, to allow the TUSK hosts to share uploaded data. This storage should be only accessible from the TUSK servers.
    - DO NOT DIRECTLY EXPOSE NFS TO THE INTERNET AT LARGE.

No other ports are required. Optional ports that may be useful for monitoring include:

- SNMP port 161/udp - Local monitoring tools like MRTG or rrdtool may need this, but the service should be restricted to password protected access only from local hosts or local VLANS.
- NRPE port 5666/tcp - Nagios or Icinga can use NRPE for running local Nagios checks or shell commands. Configure with caution: the "nrpe.cfg" file can also be used to restrict NRPE access.

Custom MySQL IPtables Firewall

1. Create a customized, root-owned /etc/sysconfig/iptables.mysql file with something like this content:

```
-A INPUT -i eth0 -p tcp -s 10.250.159.0/25 --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -p tcp -s 130.64.0.0/16 --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT
```

    a. The 10.250.159.0/25 rule restricts access to the front end ports of the Summer St. VLAN 168.
    b. The 130.64.0.0/16 rule restricts access to the internal Tufts VLAN's, without limit.
    c. Seriously consider refining these rules to allow only designated hosts for production environments.
2. Run the "system-config" tool to add this rule.
    a. The tool is "system-config-securitylevel" on RHEL or CentOS 5.
    b. The tool is "system-config-firewall-tui" on RHEL or CentOS 6.
    c. Select to customize the firewall.
        i. Keep passing through the screens until asked to "Use custom rules"
        ii. Add a new rule, if necessary.
            1. The "Protocol Type" is **"tcp"**.
            2. The "Firewall Table" is **"filter".**
            3. The "File" is **"/etc/sysconfig/iptables.mysql"**.
3. Make sure that a way to log directly into the console exists, firewall mistakes can interrupt services.
4. Restart iptables.

```
/sbin/chkconfig --list iptables
/sbin/service iptables restart
```

5. Test the rules.