IPTable - Configuration Examples

Purpose

Here are some additional `iptables` config files:

Examples

Restrict SSH Access to Campus Network

This file is similar to the `iptables.base` example, but set up to only allow SSH connections from the Campus Network

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [14039465:18394491353]
# Keep Current connections alive
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
# Allow the UCSB Campus to ping the machine
-A INPUT -s 128.111.0.0/16 -p icmp -j ACCEPT
# Allow SSH Connections from Campus
-A INPUT -s 128.111.0.0/16 -p tcp --state NEW -m tcp --dport 22 -j ACCEPT
# Allow the computer to talk to itself for its applications
-A INPUT -i lo -j ACCEPT
# Otherwise, drop the connection
-A INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

In order to access it from the Campus Wireless or off Campus (not including ResNet), you will need to use the Campus VPN.

Restrict a port to only your lab subnet

This is an example of how to restrict a port to a subnet

```
```
In this example, `-A INPUT -s 128.111.43.0/24 -p tcp -m tcp --dport 8475 -j ACCEPT` line says to do the following:

Append this rule to the `INPUT` chain, where `Source` is from `128.111.43.0/24` (Basically any computer coming from an IP address starting `128.111.43.*`) trying to connect to `TCP` port `8475`, allow the connection.

This example only puts in one port allowance, but multiple lines can be put in to allow others.

The important part here is limiting the access to the port in question to the subnet the lab is in, as most projects don't need to have the port fully open to the world if possible.

This, however, should not exclude the fact that any service running should not have some form of authentication with this up.

Having the Firewall restricting access to the port will mitigate other vulnerabilities some services may have even with authentication in place.

**Related articles**

- IPTable - Configuration Examples
- IPTables - Basics
- General Recommendations for Mail Clients for UCSB Connect
- Securing Linux Computer
- How do I keep my computer from getting infected?