3.6.2 Ensure default deny firewall policy (Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:

```
# iptables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Notes

Changing firewall settings while connected over network can result in being locked out of the system. Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.