

4.4 Configure iptables

If Uncomplicated Firewall (UFW) or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting IPtables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

Note:

- Configuration of a live system's firewall directly over a remote connection will often result in being locked out.
- **iptables** is being phased out, and support for **iptables** will be reduced over time. It is recommended to transition towards either **nftables** or **ufw** as the default firewall management tool.

4.4.1 Configure iptables software

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

Note: Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If Uncomplicated Firewall (UFW) or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

4.4.1.1 Ensure iptables packages are installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; **iptables** applies to IPv4, **ip6tables** to IPv6, **arptables** to ARP, and **ebtables** to Ethernet frames.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Audit:

Run the following command to verify that **iptables** is installed:

```
# dpkg-query -s iptables &>/dev/null && echo "iptables is installed"
iptables is installed
```

Run the following command to verify that **iptables-persistent** is installed:

```
# dpkg-query -s iptables-persistent &>/dev/null && echo "iptables-persistent
is installed"
iptables-persistent is installed
```

Remediation:










Run the following command to install **iptables** and **iptables-persistent**

```
# apt install iptables iptables-persistent
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.1.2 Ensure *nftables* is not in use with *iptables* (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to *iptables*.

Rationale:

Running both **iptables** and **nftables** may lead to conflict.

Audit:

Run the following command to verify that **nftables** is not installed:

```
# dpkg-query -s nftables &>/dev/null && echo "nftables is installed"
```

Nothing should be returned

- OR -

Run the following command to verify **nftables.service** is not enabled:

```
# systemctl is-enabled nftables.service 2>/dev/null | grep '^enabled'
```

Nothing should be returned

Run the following command to verify **nftables.service** is not active:

```
# systemctl is-active nftables.service 2>/dev/null | grep '^active'
```

Nothing should be returned

Remediation:

Run the following command to remove **nftables**:

```
# apt purge nftables
```

- OR -










Run the following commands to stop and mask **nftables.service**:

```
# systemctl stop nftables.service
# systemctl mask nftables.service
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	

4.4.1.3 Ensure ufw is not in use with iptables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration

Rationale:

Running `iptables.persistent` with `ufw` enabled may lead to conflict and unexpected results.

Audit:

Run the following commands to verify that `ufw` is **either** not installed or disabled. **Only one of the following needs to pass.**

Run the following command to verify that `ufw` is not installed:

```
# dpkg-query -s ufw &>/dev/null && echo "ufw is installed"
```

Nothing should be returned.

- OR -

Run the following command to verify `ufw` is disabled:

```
# ufw status  
  
Status: inactive
```

Run the following commands to verify that the `ufw.service` is not enabled:

```
# systemctl is-enabled ufw 2>/dev/null | grep '^enabled'
```

Nothing should be returned

Run the following command to verify `ufw.service` is not active:

```
# systemctl is-active ufw.service 2>/dev/null | grep '^active'
```

Nothing should be returned

Remediation:

Run the following command to remove **ufw**:

```
# apt purge ufw
```

- OR -

Run the following commands to disable ufw, and stop and mask **ufw.service**:










```
# ufw disable
# systemctl stop ufw.service
# systemctl mask ufw.service
```

Note: **ufw disable** needs to be run before **systemctl mask ufw.service** in order to correctly disable **UFW**

References:

1. NIST SP 800-53 Rev. 5: CA-9, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	

4.4.2 Configure IPv4 iptables

iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note: This section broadly assumes starting with an empty **iptables** firewall ruleset (established by flushing the rules with **iptables -F**). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/bin/bash

# Flush IPtables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

4.4.2.1 Ensure iptables default deny firewall policy (Automated)

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.

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

Rationale:

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

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.2.2 Ensure iptables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Note:

- 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

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to the operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (**pkts** and **bytes** counts may differ, **prot** may be **all** or **0**):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source
destination
    0    0 ACCEPT      all  --  lo      *       0.0.0.0/0      0.0.0.0/0
    0    0 DROP        all  --  *       *       127.0.0.0/8    0.0.0.0/0

# iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source
destination
    0    0 ACCEPT      all  --  *       lo      0.0.0.0/0      0.0.0.0/0
```

Remediation:










Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.2.3 Ensure iptables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established connections.

Note:

- 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

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:










Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.2.4 Ensure iptables firewall rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

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
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# ss -4tuln
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer
udp	UNCONN	0	0	*:68	
:					
udp	UNCONN	0	0	*:123	
:					
tcp	LISTEN	0	128	*:22	
:					

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n
```

Chain INPUT (policy DROP 0 packets, 0 bytes)									
	pkts	bytes	target	prot	opt	in	out	source	destination
	0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0
	0	0	DROP	all	--	*	*	127.0.0.0/8	0.0.0.0/0
	0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0

```
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule. The last line identified by the **tcp dpt:22 state NEW** identifies it as a firewall rule for new connections on tcp port 22.

Remediation:










For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.3 Configure IPv6 ip6tables

ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

If IPv6 is enabled on the system, the ip6tables should be configured.

Note: This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with `ip6tables -F`). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/bin/bash

# Flush ip6tables rules
ip6tables -F

# Ensure default deny firewall policy
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Ensure loopback traffic is configured
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT
ip6tables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured
ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
ip6tables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

4.4.3.1 Ensure iptables default deny firewall policy (Automated)

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.

Note:

- 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

Rationale:

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

Audit:

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

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

- OR -

Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is enabled on the system.

```
#!/usr/bin/env bash

{
    l_ipv6_enabled="is"
    ! grep -Pqs -- '^\\h*0\\b' /sys/module/ipv6/parameters/disable &&
    l_ipv6_enabled="is not"
    if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
    "\\h*net\\.ipv6\\.conf\\.all\\.disable_ipv6\\h*=\\h*1\\b" && \
        sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
    "\\h*net\\.ipv6\\.conf\\.default\\.disable_ipv6\\h*=\\h*1\\b"; then
        l_ipv6_enabled="is not"
    fi
    echo -e " - IPv6 $l_ipv6_enabled enabled on the system"
}
```

Remediation:

- IF - IPv6 is enabled on your system:










Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.3.2 Ensure ip6tables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Note:

- 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

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# ip6tables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source
destination
    0     0 ACCEPT      all  --  lo      *       ::/0
    0     0 DROP        all  --  *       *       :::1

# ip6tables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source
destination
    0     0 ACCEPT      all  --  *       lo      ::/0
```

- OR -

Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is enabled on the system.

```
#!/usr/bin/env bash

{
    l_ipv6_enabled="is"
    ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
    l_ipv6_enabled="is not"
    if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
    '^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b' && \
    sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
    '^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b'; then
        l_ipv6_enabled="is not"
    fi
    echo -e " - IPv6 $l_ipv6_enabled enabled on the system"
}
```

Remediation:










Run the following commands to implement the loopback rules:

```
# ip6tables -A INPUT -i lo -j ACCEPT
# ip6tables -A OUTPUT -o lo -j ACCEPT
# ip6tables -A INPUT -s :::1 -j DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.3.3 Ensure iptables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Note:

- 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

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# ip6tables -L -v -n
```

- OR -

Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is enabled on the system.

```
#!/usr/bin/env bash

{
    l_ipv6_enabled="is"
    ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
    l_ipv6_enabled="is not"
    if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
    "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
        sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
    "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
        l_ipv6_enabled="is not"
    fi
    echo -e " - IPv6 $l_ipv6_enabled enabled on the system"
}
```

Remediation:










Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

4.4.3.4 Ensure iptables firewall rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

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
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# ss -6tuln
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer
udp	UNCONN	0	0	:::1:123	
:::*					
udp	UNCONN	0	0	:::123	
:::*					
tcp	LISTEN	0	128	:::22	
:::*					
tcp	LISTEN	0	20	:::1:25	
:::*					

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n
```

Chain INPUT (policy DROP 0 packets, 0 bytes)							
pkts	bytes	target	prot	opt	in	out	source
destination							
0	0	ACCEPT	all		lo	*	::/0
0	0	DROP	all		*	*	:::1
0	0	ACCEPT	tcp		*	*	::/0
tcp dpt:22 state NEW							

Verify all open ports listening on non-localhost addresses have at least one firewall rule. The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

- **OR** - verify IPv6 is not enabled:

Run the following script. Output will confirm if IPv6 is enabled on the system:

```
#!/usr/bin/env bash

{
    l_ipv6_enabled="is"
    ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
    l_ipv6_enabled="is not"
    if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
    '^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b' && \
        sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
    '^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b'; then
        l_ipv6_enabled="is not"
    fi
    echo -e " - IPv6 $l_ipv6_enabled enabled on the system"
}
```

Remediation:










For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037