Reglas de firewall para el servidor de correo virtual

Esta página es complementaria al artículo principal: Creando un servidor de correo virtual con Postfix, Dovecot y MySQL

Un firewall es simplemente un conjunto de reglas de enrutamiento del kernel, reglas de iptables, que bloquean o permiten selectivamente el tráfico de red dentro y fuera de su máquina. ¡Un servidor de correo electrónico orientado a la web debe estar protegido por un conjunto adecuado de reglas de firewall o se verá abrumado y comprometido rápidamente!

Si ya tiene instalado un firewall para otros servicios, deberá agregar las reglas necesarias para admitir el tráfico del servidor de correo. Si no tiene un servidor de seguridad actualmente instalado, entonces puede usar el siguiente ejemplo como un buen punto de partida.

Cargando *solo* las reglas a continuación, ya que su firewall cerrará otros accesos que pueden ser importantes para usted, como http y ssh! Primero debe usar iptables -L para verificar las reglas preexistentes y trabajar las siguientes a continuación en su cortafuegos existente. Si no tiene un firewall y/o necesita permitir http y ssh, elimine el comentario de las líneas –policy y las de http y ssh según sea necesario para cumplir con sus requisitos.

A continuación se incluye un **mínimo** conjunto de reglas de iptables para proporcionar un servidor de seguridad para su servidor de correo electrónico. Mientras

```
#--policy INPUT DROP
#--policy FORWARD DROP
#--policy OUTPUT ACCEPT

-A INPUT -m state --state INVALID -j DROP
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Postfix SMTP, SMTPS, SUBMISSION
-A INPUT -p tcp --dport 25 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 465 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 587 -m state --state NEW -j ACCEPT

# Imap and ImapS
#-A INPUT -p tcp --dport 143 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 993 -m state --state NEW -j ACCEPT

# Pop3 and Pop3S
#-A INPUT -p tcp --dport 110 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 995 -m state --state NEW -j ACCEPT

#  Allow HTTP and HTTPS connections from anywhere on normal ports
#-A INPUT -p tcp --dport 80 -j ACCEPT
```

```
#-A INPUT -p tcp --dport 443 -j ACCEPT

#  Allow SSH connections on normal port 22
#-A INPUT -p tcp -m state --state NEW --dport 22 -j ACCEPT

#  Respond to ping requests
#-A INPUT -p icmp --icmp-type echo-request -j ACCEPT

#  Drop all other inbound
-A INPUT -j DROP
```

El puerto 25, SMTP, debe estar habilitado para aceptar el correo electrónico entrante para enviarlo a sus buzones de correo virtual.

El puerto 465, SMTPS, debe estar habilitado para conexiones SMTP seguras.

El Puerto 587, SUBMISIÓN, es utilizado por los Agentes de Usuarios de Correo (MUA), como Thunderbird, para permitir el envío de correos electrónicos salientes de sus usuarios virtuales.

Los puertos 143 y 110 proporcionan conexiones Imap y POP3 de texto sin formato, respectivamente. Probablemente sea mejor no usar estos y forzar todas las conexiones Imap y Pop3 para que sean seguras, como lo haremos en este artículo. Si no se usa, es mejor comentarlos fuera de sus reglas de iptables como se muestra aquí.

Los puertos 993 y 995 proporcionan Imap y Pop3 seguros, respectivamente. Estos deben estar abiertos para que sus usuarios virtuales puedan enviar y recibir correos electrónicos.

Para instalar estas reglas como su firewall, guárdelas en un archivo de texto usando

```
 iptables-save> /etc/firewall.rules
```

y luego cargue ese archivo usando iptables-restore como se muestra a continuación. Esto reemplazará cualquier regla actual de iptables con aquellas en el archivo.

Hay muchas preferencias para guardar y cargar scripts de firewall. Generalmente uso /etc/firewall.rules para mis propios sistemas y usaré eso para este ejemplo.

```
iptables-restore </etc/firewall.rules
```

To see all currently active rules:

```
iptables -L
```

To flush all current rules:

```
iptables -F
```

Para cargar sus reglas de firewall en cada inicio, deberá crear un script de inicio y guardarlo en /etc/rc.d/rc.firewall y hacerlo ejecutable. Este archivo será iniciado por /etc/rc.d/rc.inet2 cuando se

inicie el sistema, antes de que se inicien los dispositivos de red.

Puede elegir crear un script más completo con opciones de inicio y detención, pero el siguiente script simple es suficiente para cargar sus reglas de firewall en el inicio.

```
vi /etc/rc.d/rc.firewall

# add the following lines #
if [ -e /etc/firewall.rules ]; then
        iptables-restore </etc/firewall.rules
fi
```

Make sure rc.firewall is executable...

```
chmod +x /etc/rc.d/rc.firewall
```

Cargue las reglas de su firewall y asegúrese de que sean como espera que sean antes de continuar. Además, ¡asegúrese de que su firewall se cargue en el arranque para evitar que se ejecute accidentalmente sin él!

```
iptables-restore </etc/firewall.rules
iptables -L
```

Volver a la página principal del artículo

Fuentes

- Escrito originalmente por astrogeek
- Traducido por: Victor 2019/02/14 12:52

howtos, email, postfix, dovecot, firewall