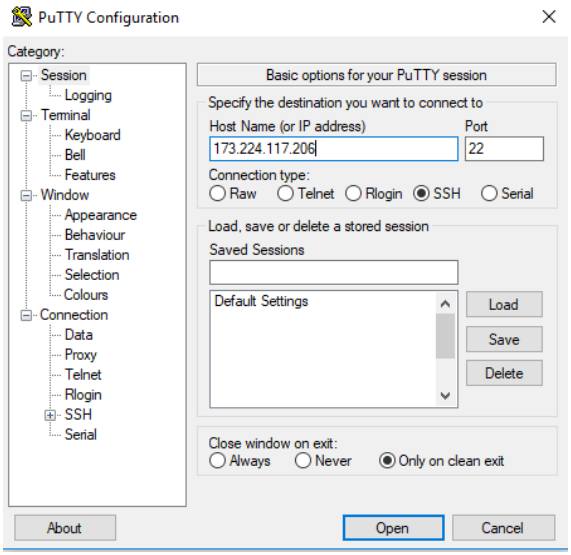
Procedimiento para habilitar IPs en Firewall Linux

El siguiente procedimiento explica los parámetros de configuración para habilitar direcciones IP dentro del Firewall (iptables) de Linux:

Paso 1: Acceder vía consola SSH al servidor Linux

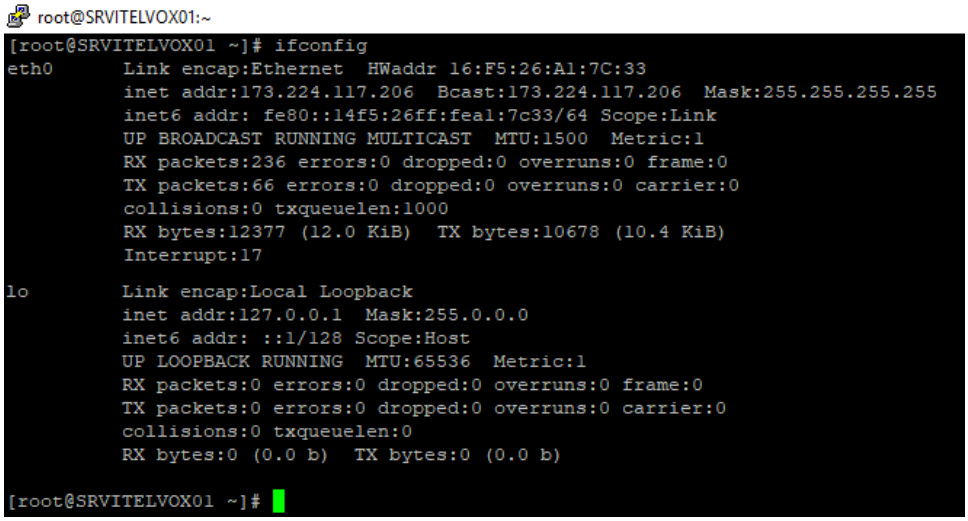
Para el acceso vía SSH utilizaremos la aplicación Putty



Necesitaremos la dirección IP y puerto del servicio. Para nuestro ejemplo usaremos la IP 173.224.117.206 con el puerto 22.

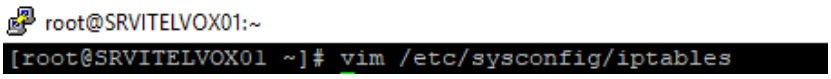
Paso 2: Consola SSH

En la consola SSH podremos modificar configuraciones del servidor, para este caso el servicio que vamos a configurar es el IPTABLES. Primero validaremos la dirección IP del servidor.



Paso 3: Configuración de IPTABLES

El archivo que configura las reglas del Firewall se encuentra en la siguiente ruta /etc/sysconfig/iptables al cual ingresaremos para ver los parámetros y configurar.



Al ingresar al archivo presionamos la tecla i para modo edición y veremos lo siguiente:

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -s 185.32.76.134 -j ACCEPT
-A RH-Firewall-1-INPUT -s 185.32.76.176/28 -j ACCEPT
-A RH-Firewall-1-INPUT -s 45.126.210.18 -j ACCEPT
-A RH-Firewall-1-INPUT -s 172.93.110.50 -j ACCEPT
-A RH-Firewall-1-INPUT -s 172.96.143.25 -j ACCEPT
-A RH-Firewall-1-INPUT -s 45.232.150.0/29 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p tcp -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p tcp -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p tcp -m tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p udp -m udp --dport 5060 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -m udp -p udp --dport 10000:65000 -j ACCEPT
-A RH-Firewall-1-INPUT -s 8.8.8.8 -p udp -m udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -s 8.8.4.4 -p udp -m udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -j DROP
COMMIT
```

1) Son las configuraciones por defecto.

2) Son los rangos y direcciones IPs utilizados por ITELVOX. Esas direcciones no deben de modificarse.

3) Configuración de rangos de red o direcciones IP. Para este ejemplo solo se habilito la red 200.0.0.0/8 para los siguientes servicios:

Protocolo/Puerto	Detalle
ICMP	Ping para ver conectividad
22	Acceso por SSH
80	Acceso web
443	Acceso web seguro
5060	Señalización SIP
10000:65000	Puerto de RTP (Audio)

En este punto verán que en la configuración solo hemos dejado habilitado un rango de red como ejemplo, pero en los servidores podrán encontrar más rango o direcciones IPs que el cliente haya solicitado.

En caso se requiera habilitar una dirección IP o rango de red podremos realizarlo de la siguiente manera:

Para habilitar acceso total a una IP
-A RH-Firewall-1-INPUT -s 161.132.210.25 -j ACCEPT

Para habilitar acceso total a un rango de red
-A RH-Firewall-1-INPUT -s 201.0.0.0/8 -j ACCEPT

Para habilitar un rango de red o IP únicamente a puertos específicos
-A RH-Firewall-1-INPUT -s [Rango de red o IP] -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -s [Rango de red o IP] -p tcp -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -s [Rango de red o IP] -p tcp -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -s [Rango de red o IP] -p tcp -m tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -s [Rango de red o IP] -p udp -m udp --dport 5060 -j ACCEPT
-A RH-Firewall-1-INPUT -s [Rango de red o IP] -p udp -m udp –dport 10000:65000 -j ACCEPT

Al momento de agregar dentro la configuración mantener el orden correspondiente.

4) Son las direcciones IPs de los DNS. Esas direcciones no deben de modificarse.

5) Bloqueamos el resto y finaliza el archivo.

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -s 185.32.76.134 -j ACCEPT
-A RH-Firewall-1-INPUT -s 185.32.76.176/28 -j ACCEPT
-A RH-Firewall-1-INPUT -s 45.126.210.18 -j ACCEPT
-A RH-Firewall-1-INPUT -s 172.93.110.50 -j ACCEPT
-A RH-Firewall-1-INPUT -s 172.96.143.25 -j ACCEPT
-A RH-Firewall-1-INPUT -s 45.232.150.0/29 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p tcp -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p tcp -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p tcp -m tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -p udp -m udp --dport 5060 -j ACCEPT
-A RH-Firewall-1-INPUT -s 200.0.0.0/8 -m udp -p udp --dport 10000:65000 -j ACCEPT
-A RH-Firewall-1-INPUT -s 8.8.8.8 -p udp -m udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -s 8.8.4.4 -p udp -m udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -j DROP
COMMIT
~
:x
```

Guardarnos la configuración presionando las teclas “ESC + :” luego de ello colocamos x y posteriormente Enter para grabar y salir del archivo.

Paso 4: Reiniciar servicio de IPTABLES

Luego de haber editado el archivo procedemos a reiniciar el servicio:

root@SRVITELVOX01:~

```
[root@SRVITELVOX01 ~]# service iptables restart
iptables: Poniendo las cadenas de la política ACCEPT: filte[  OK  ]
iptables: Guardando las reglas del cortafuegos:            [  OK  ]
iptables: Descargando módulos:                             [  OK  ]
iptables: Aplicando reglas del cortafuegos:                [  OK  ]
[root@SRVITELVOX01 ~]#
```

Paso 5: Validar las IPs habilitadas

Verificamos las direcciones habilitadas en el servidor:

```
[root@ ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  185.32.76.134        0.0.0.0/0
ACCEPT     all  --  185.32.76.176/28     0.0.0.0/0
ACCEPT     all  --  45.126.210.18        0.0.0.0/0
ACCEPT     all  --  172.93.110.50        0.0.0.0/0
ACCEPT     all  --  172.96.143.25        0.0.0.0/0
ACCEPT     all  --  45.232.150.0/29      0.0.0.0/0
ACCEPT     icmp --  200.0.0.0/8          0.0.0.0/0           icmp type 255
ACCEPT     tcp  --  200.0.0.0/8          0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  200.0.0.0/8          0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  200.0.0.0/8          0.0.0.0/0           tcp dpt:443
ACCEPT     udp  --  200.0.0.0/8          0.0.0.0/0           udp dpt:5060
ACCEPT     udp  --  200.0.0.0/8          0.0.0.0/0           udp dpts:10000:65000
ACCEPT     udp  --  8.8.8.8              0.0.0.0/0           udp dpt:53
ACCEPT     udp  --  8.8.4.4              0.0.0.0/0           udp dpt:53
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
DROP       all  --  0.0.0.0/0            0.0.0.0/0
```