Fundamentos de UFW: Reglas y Comandos de Firewall más Comunes.

Actualizado el 24 Octubre 2017. Posteado en Tutoriales/VideoTutoriales. Visitado 8610 veces.



INTRODUCCIÓN

**Fundamentos de UFW: Reglas y Comandos de Firewall más Comunes.** UFW es una herramienta de configuración de Firewall para iptables que se incluye con Fundamentos de UFW: Reglas y Comandos de Firewall más Comunes en Ubuntu de forma predeterminada. Este tutorial te muestra el estilo de hoja de trucos que proporciona una referencia rápida a los comandos de UFW que crearán reglas de Firewall de iptables que son útiles en escenarios cotidianos comunes. Esto incluye ejemplos UFW de permitir y bloquear varios servicios por puerto, interfaz de red y dirección IP de origen.

INSTRUCTIVOS

* Si está empezando a usar UFW para configurar su firewall, consulte nuestra [introducción a UFW](https://fututel.com/es/tutoriales-guias-manuales-videotutoriales/2631-como-configurar-un-firewall-con-ufw-en-ubuntu-14-04)
* La mayoría de las reglas que se describen aquí presuponen que está utilizando el conjunto de reglas UFW predeterminado. Es decir, está configurado para permitir el tráfico saliente y denegado entrante, a través de las políticas predeterminadas, por lo que debe permitir el tráfico de forma selectiva.
* Use las secciones siguientes que sean aplicables a lo que está tratando de lograr. La mayoría de las secciones no se basan en ninguna otra, por lo que puede usar los ejemplos a continuación de forma independiente
* Utilice el menú de Contenido en el lado derecho de esta página (en anchos de página amplios) o la función de búsqueda de su navegador para localizar las secciones que necesita
* Copie y pegue los ejemplos de la línea de comandos dados, sustituyendo los valores en rojo con sus propios valores

Recuerde que puede verificar su actual conjunto de reglas UFW con sudo ufw status o sudo ufw status verbose .

BLOQUEAR UNA DIRECCIÓN IP

Para bloquear todas las conexiones de red que se originan desde una dirección IP específica, 15.15.15.51 por ejemplo, ejecute este comando:

sudo ufw deny from 15.15.15.51

En este ejemplo, from 15.15.15.51 especifica una dirección IP **de origen** de "15.15.15.51". Si lo desea, en su 15.15.15.0/24 se puede especificar una subred, como 15.15.15.0/24 . La dirección IP de origen se puede especificar en cualquier regla de cortafuegos, incluyendo una regla de **permiso.**

BLOQUEAR CONEXIONES A UNA INTERFAZ DE RED

Para bloquear conexiones de una dirección IP específica, por ejemplo 15.15.15.51 , a una interfaz de red específica, por ejemplo, eth0 , use este comando:

sudo ufw deny in on eth0 from 15.15.15.51

Este es el mismo que en el ejemplo anterior, con la adición de in on eth0 . La interfaz de red se puede especificar en cualquier regla de firewall y es una gran manera de limitar la regla a una red en particular.

SERVICIO: SSH

Si está utilizando un servidor en la nube, probablemente quiera permitir las conexiones SSH entrantes (puerto 22) para que pueda conectarse y administrar su servidor. Esta sección cubre cómo configurar su firewall con varias reglas relacionadas con SSH.

PERMITIR SSH

Para permitir todas las conexiones SSH entrantes, ejecute este comando:

sudo ufw allow ssh

Una sintaxis alternativa es especificar el número de puerto del servicio SSH:

sudo ufw allow 22

PERMITIR SSH ENTRANTE DESDE UNA DIRECCIÓN IP ESPECÍFICA O SUBRED

Para permitir las conexiones SSH entrantes desde una subred o una dirección IP específica, especifique la fuente. Por ejemplo, si desea permitir toda la subred 15.15.15.0/24 , ejecute este comando:

sudo ufw allow from 15.15.15.0/24 to any port 22

PERMITIR RSYNC ENTRANTE DESDE UNA DIRECCIÓN IP ESPECÍFICA O SUBRED

Rsync, que se ejecuta en el puerto 873, se puede usar para transferir archivos de una computadora a otra.

Para permitir las conexiones rsync entrantes desde una subred o una dirección IP específica, especifique la dirección IP de origen y el puerto de destino. Por ejemplo, si desea permitir que toda la subred 15.15.15.0/24 pueda 15.15.15.0/24 rsync a su servidor, ejecute este comando:

sudo ufw allow from 15.15.15.0/24 to any port 873

SERVICIO: SERVIDOR WEB

Los servidores web, como Apache y Nginx, normalmente escuchan las solicitudes en los puertos 80 y 443 para las conexiones HTTP y HTTPS, respectivamente. Si su política predeterminada para el tráfico entrante está configurada para cancelar o rechazar, querrá crear reglas que le permitan a su servidor responder a esas solicitudes.

PERMITIR TODO EL HTTP ENTRANTE

Para permitir todas las conexiones HTTP entrantes (puerto 80), ejecute este comando:

sudo ufw allow http

Una sintaxis alternativa es especificar el número de puerto del servicio HTTP:

sudo ufw allow 80

PERMITIR TODO EL HTTPS ENTRANTE

Para permitir que todas las conexiones entrantes de HTTPS (puerto 443) ejecuten este comando:

sudo ufw allow https

Una sintaxis alternativa es especificar el número de puerto del servicio HTTPS:

sudo ufw allow 443

PERMITIR TODO EL HTTP ENTRANTE Y HTTPS

Si desea permitir el tráfico HTTP y HTTPS, puede crear una sola regla que permita ambos puertos. Para permitir todas las conexiones entrantes HTTP y HTTPS (puerto 443), ejecute este comando:

sudo ufw allow proto tcp from any to any port 80,443

Tenga en cuenta que debe especificar el protocolo, con proto tcp , al especificar múltiples puertos.

SERVICIO: MYSQL

MySQL escucha las conexiones de los clientes en el puerto 3306. Si su servidor de base de datos MySQL está siendo utilizado por un cliente en un servidor remoto, debe asegurarse de permitir ese tráfico.

PERMITIR MYSQL DESDE UNA DIRECCIÓN IP ESPECÍFICA O SUBRED

Para permitir las conexiones entrantes de MySQL desde una subred o una dirección IP específica, especifique la fuente. Por ejemplo, si desea permitir toda la subred 15.15.15.0/24 , ejecute este comando:

sudo ufw allow from 15.15.15.0/24 to any port 3306

PERMITIR MYSQL A LA UNTERFAZ DE RED ESPECÍFICA

Para permitir las conexiones de MySQL a una interfaz de red específica, digamos que tiene una interfaz de red privada eth1 , por ejemplo, use este comando:

sudo ufw allow in on eth1 to any port 3306

SERVICIO: POSTGRESQL

PostgreSQL escucha las conexiones de los clientes en el puerto 5432. Si su servidor de base de datos PostgreSQL está siendo utilizado por un cliente en un servidor remoto, debe asegurarse de permitir ese tráfico.

POSTGRESQL DESDE UNA DIRECCIÓN IP ESPECÍFICA O SUBRED

Para permitir conexiones PostgreSQL entrantes desde una subred o una dirección IP específica, especifique la fuente. Por ejemplo, si desea permitir toda la subred 15.15.15.0/24 , ejecute este comando:

sudo ufw allow from 15.15.15.0/24 to any port 5432

El segundo comando, que permite el tráfico saliente de conexiones PostgreSQL **establecidas** , solo es necesario si la política OUTPUT no está configurada para ACCEPT .

PERMITIR POSTGRESQL A LA INTERFAZ DE RED ESPECÍFICA

Para permitir conexiones de PostgreSQL a una interfaz de red específica, digamos que tiene una interfaz de red privada eth1 , por ejemplo, use este comando:

sudo ufw allow in on eth1 to any port 5432

El segundo comando, que permite el tráfico saliente de conexiones PostgreSQL **establecidas** , solo es necesario si la política OUTPUT no está configurada para ACCEPT .

SERVICIO: CORREO

Los servidores de correo, como Sendmail y Postfix, escuchan en una variedad de puertos dependiendo de los protocolos que se utilizan para la entrega de correo. Si está ejecutando un servidor de correo, determine qué protocolos está utilizando y permita los tipos de tráfico apropiados. También le mostraremos cómo crear una regla para bloquear el correo SMTP saliente.

BLOQUEAR EL CORREO SMTP SALIENTE

Si su servidor no debe enviar correo saliente, es posible que desee bloquear ese tipo de tráfico. Para bloquear el correo SMTP saliente, que usa el puerto 25, ejecute este comando:

sudo ufw deny out 25

Esto configura su Firewall para **eliminar** todo el tráfico saliente en el puerto 25. Si necesita rechazar un servicio diferente por su número de puerto, en lugar del puerto 25, simplemente reemplácelo.

PERMITIR TODO SMTP ENTRANTE

Para permitir que su servidor responda a las conexiones SMTP, puerto 25, ejecute este comando:

sudo ufw allow 25

**Nota:** Es común que los servidores SMTP usen el puerto 587 para correo saliente.

PERMITIR TODO IMAP ENTRANTE

Para permitir que su servidor responda a las conexiones IMAP, puerto 143, ejecute este comando:

sudo ufw allow 143

PERMITIR TODOS LOS IMAPS ENTRANTES

Para permitir que su servidor responda a las conexiones IMAPS, puerto 993, ejecute este comando:

sudo ufw allow 993

PERMITIR TODO POP3 ENTRANTE

Para permitir que su servidor responda a las conexiones POP3, puerto 110, ejecute este comando:

sudo ufw allow 110

PERMITIR TODO EL POP3S ENTRANTE

Para permitir que su servidor responda a las conexiones POP3S, puerto 995, ejecute este comando:

sudo ufw allow 995

CONCLUSIÓN

Eso debería cubrir muchos de los comandos que se usan comúnmente cuando se usa UFW para configurar un firewall. Por supuesto, UFW es una herramienta muy flexible, así que siéntete libre de mezclar y combinar los comandos con diferentes opciones para que coincidan con tus necesidades específicas si no están cubiertos aquí.

***Fuente.****Artículo traducido y con muy ligeras modificaciones de: https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-debian*