Tanıtım

UFW veya Komplike Olmayan Güvenlik Duvarı, iptablesbir güvenlik duvarı yapılandırma sürecini basitleştirmeye yönelik bir arabirimdir . iptablesSağlam ve esnek bir araç olmasına rağmen , yeni başlayanlar için bir güvenlik duvarını düzgün bir şekilde yapılandırmak için onu nasıl kullanacaklarını öğrenmek zor olabilir. Ağınızın güvenliğini sağlamaya başlamak istiyorsanız ve hangi aracı kullanacağınızdan emin değilseniz, UFW sizin için doğru seçim olabilir.

Bu eğitim size Ubuntu 18.04'te UFW ile bir güvenlik duvarının nasıl kurulacağını gösterecektir.

Önkoşullar

Bu öğreticiyi takip etmek için ihtiyacınız olacak:

* [Ubuntu 18.04 öğretici ile İlk Sunucu Kurulumu'ndaki](https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-18-04)sudo Adım 1–3'ü izleyerek kurabileceğiniz, root kullanıcısı olmayan bir Ubuntu 18.04 sunucusu .

UFW, Ubuntu'da varsayılan olarak kuruludur. Herhangi bir nedenle kaldırılmışsa, ile yükleyebilirsiniz sudo apt install ufw.

Adım 1 — IPv6'nın Etkin Olduğundan Emin Olmak

Ubuntu'nun son sürümlerinde IPv6 varsayılan olarak etkindir. Pratikte bu, sunucuya eklenen çoğu güvenlik duvarı kuralının hem IPv4 hem de IPv6 sürümünü içereceği anlamına gelir, ikincisi v6UFW'nin durum komutunun çıktısında tanımlanır . IPv6'nın etkinleştirildiğinden emin olmak için adresinden UFW yapılandırma dosyanızı kontrol edebilirsiniz /etc/default/ufw. Bu dosyayı nanoveya favori komut satırı düzenleyicinizi kullanarak açın :

* sudo nano /etc/default/ufw

kopyala

Ardından, değerinin IPV6olarak ayarlandığından emin olun yes. Şöyle görünmelidir:

/etc/default/ufw alıntısı

IPV6=yes

kopyala

Dosyayı kaydedin ve kapatın. kullanıyorsanız nano, bunu CTRL+X, ardından Yve ENTERonaylamak için yazarak yapabilirsiniz .

UFW, bu kılavuzun sonraki bir adımında etkinleştirildiğinde, hem IPv4 hem de IPv6 güvenlik duvarı kurallarını yazacak şekilde yapılandırılacaktır.

Adım 2 — Varsayılan İlkeleri Ayarlama

UFW'ye yeni başlıyorsanız, varsayılan güvenlik duvarı politikalarınızı kontrol etmek iyi bir ilk adımdır. Bu kurallar, diğer kurallarla açıkça eşleşmeyen trafiğin nasıl işleneceğini denetler.

Varsayılan olarak, UFW tüm gelen bağlantıları reddedecek ve tüm giden bağlantılara izin verecek şekilde ayarlanmıştır. Bu, sunucunuza ulaşmaya çalışan herhangi birinin bağlanamayacağı, sunucu içindeki herhangi bir uygulamanın dış dünyaya ulaşabileceği anlamına gelir. Belirli hizmetlere ve bağlantı noktalarına izin vermek için ek kurallar, bu genel ilkenin istisnaları olarak dahil edilmiştir.

Bu öğreticinin geri kalanıyla birlikte takip edebileceğinizden emin olmak için, şimdi gelen ve giden trafik için UFW varsayılan politikalarınızı ayarlayacaksınız.

Varsayılan UFW gelen politikasını olarak ayarlamak için şunu denyçalıştırın:

* sudo ufw default deny incoming

kopyala

Output

Default incoming policy changed to 'deny'

(be sure to update your rules accordingly)

Varsayılan UFW giden politikasını olarak ayarlamak için şunu allowçalıştırın:

* sudo ufw default allow outgoing

kopyala

Output

Default outgoing policy changed to 'allow'

(be sure to update your rules accordingly)

Bu komutlar, varsayılanları gelenleri reddetmek ve giden bağlantılara izin vermek için ayarlar. Bu güvenlik duvarı varsayılanları tek başına bir kişisel bilgisayar için yeterli olabilir, ancak sunucuların genellikle dış kullanıcılardan gelen isteklere yanıt vermesi gerekir. Bunu daha sonra inceleyeceğiz.

Adım 3 — SSH Bağlantılarına İzin Verme

UFW güvenlik duvarınızı şimdi etkinleştirirseniz, gelen tüm bağlantıları reddeder. Bu, sunucunuzun bu tür isteklere yanıt vermesini istiyorsanız, örneğin SSH veya HTTP bağlantıları gibi meşru gelen bağlantılara açıkça izin veren kurallar oluşturmanız gerektiği anlamına gelir. Bir bulut sunucusu kullanıyorsanız, sunucunuza bağlanabilmeniz ve sunucunuzu yönetebilmeniz için muhtemelen gelen SSH bağlantılarına izin vermek isteyeceksiniz.

OpenSSH UFW Uygulama Profiline İzin Verme

Kurulumun ardından, ağ bağlantılarına dayanan çoğu uygulama, kullanıcıların bir hizmete hızlı bir şekilde harici erişime izin vermesini veya reddetmesini sağlayan UFW içinde bir uygulama profili kaydeder. Şu anda UFW'de hangi profillerin kayıtlı olduğunu aşağıdakilerle kontrol edebilirsiniz:

* sudo ufw app list

kopyala

Output

Available applications:

OpenSSH

OpenSSH uygulama profilini etkinleştirmek için şunu çalıştırın:

* sudo ufw allow OpenSSH

kopyala

Output

Rule added

Rule added (v6)

Bu 22, SSH arka plan programının varsayılan olarak dinlediği bağlantı noktası olan bağlantı noktasındaki tüm bağlantılara izin vermek için güvenlik duvarı kuralları oluşturacaktır .

Hizmet Adına Göre SSH'ye İzin Verme

UFW'yi gelen SSH bağlantılarına izin verecek şekilde yapılandırmanın başka bir yolu da hizmet adına başvurmaktır: ssh.

* sudo ufw allow ssh

kopyala

Output

Rule added

Rule added (v6)

UFW, /etc/servicesdosyaya bağlı olarak bir hizmetin hangi bağlantı noktalarını ve protokolleri kullandığını bilir .

Bağlantı Noktası Numarasına Göre SSH'ye İzin Verme

Alternatif olarak, uygulama profili veya hizmet adı yerine bağlantı noktasını belirterek eşdeğer kuralı yazabilirsiniz. Örneğin, bu komut önceki örneklerle aynı şekilde çalışır:

* sudo ufw allow 22

kopyala

Output

Rule added

Rule added (v6)

SSH arka plan programınızı farklı bir bağlantı noktası kullanacak şekilde yapılandırdıysanız, uygun bağlantı noktasını belirtmeniz gerekir. Örneğin, SSH sunucunuz bağlantı noktasını dinliyorsa 2222, o bağlantı noktasındaki bağlantılara izin vermek için bu komutu kullanabilirsiniz:

* sudo ufw allow 2222

kopyala

Output

Rule added

Rule added (v6)

Artık güvenlik duvarınız gelen SSH bağlantılarına izin verecek şekilde yapılandırıldığına göre, onu etkinleştirebilirsiniz.

Adım 4 — UFW'yi Etkinleştirme

Güvenlik duvarınız şimdi SSH bağlantılarına izin verecek şekilde yapılandırılmalıdır. Şu ana kadar hangi kuralların eklendiğini doğrulamak için güvenlik duvarı hala devre dışı olsa bile şunları kullanabilirsiniz:

* sudo ufw show added

kopyala

Output

Added user rules (see 'ufw status' for running firewall):

ufw allow OpenSSH

Gelen SSH bağlantılarına izin vermek için bir kuralınız olduğunu onayladıktan sonra, güvenlik duvarını aşağıdakilerle etkinleştirebilirsiniz:

* sudo ufw enable

kopyala

Output

Command may disrupt existing ssh connections. Proceed with operation (y|n)? y

Firewall is active and enabled on system startup

Komutun mevcut SSH bağlantılarını bozabileceğini söyleyen bir uyarı alacaksınız. Zaten SSH bağlantılarına izin veren bir güvenlik duvarı kuralı ayarladınız, bu nedenle devam etmenizde fayda var. Komut istemine ile yanıt verin yve tuşuna basın ENTER.

Güvenlik duvarı artık etkindir. sudo ufw status verboseBelirlenen kuralları görmek için komutu çalıştırın . Bu öğreticinin geri kalanı, farklı bağlantı türlerine izin vermek veya reddetmek gibi UFW'nin nasıl daha ayrıntılı kullanılacağını kapsar.

Adım 5 — Diğer Bağlantılara İzin Verme

Bu noktada, sunucunuzun yanıt vermesi gereken diğer tüm bağlantılara izin vermelisiniz. İzin vermeniz gereken bağlantılar, özel ihtiyaçlarınıza bağlıdır. Uygulama profiline, hizmet adına veya bağlantı noktasına dayalı bağlantılara izin veren kuralların nasıl yazılacağını zaten biliyorsunuz; bunu zaten port üzerinde SSH için yaptınız 22. Bunu aşağıdakiler için de yapabilirsiniz:

* 80 numaralı bağlantı noktasındaki HTTP, şifrelenmemiş web sunucularının kullandığı sudo ufw allow httpveyasudo ufw allow 80
* Şifreli web sunucularının kullandığı 443 numaralı bağlantı noktasındaki HTTPS, sudo ufw allow httpsveyasudo ufw allow 443
* Apache, hem HTTP hem de HTTPS ile sudo ufw allow ‘Apache Full’
* Hem HTTP hem de HTTPS ile Nginx, kullanarak sudo ufw allow ‘Nginx Full’

ile sunucunuz için hangi uygulama profillerinin mevcut olduğunu kontrol etmeyi unutmayın sudo ufw app list.

Bağlantı noktası veya bilinen hizmet adı belirtmenin yanı sıra bağlantılara izin vermenin başka yolları da vardır. Bunlardan bazılarını ileride göreceğiz.

Belirli Bağlantı Noktası Aralıkları

UFW ile port aralıklarını belirtebilirsiniz. Bazı uygulamalar, tek bir bağlantı noktası yerine birden çok bağlantı noktası kullanır.

Örneğin, bağlantı noktalarını kullanan X11 bağlantıları, izin vermek için 6000- 6007:, bu komutları

* sudo ufw allow 6000:6007/tcp
* sudo ufw allow 6000:6007/udp

kopyala

UFW ile bağlantı noktası aralıklarını belirtirken , kuralların uygulanacağı protokolü ( tcpveya udp) belirtmelisiniz . Bundan daha önce bahsetmedik çünkü protokolün otomatik olarak belirtilmemesi çoğu durumda her iki protokole de izin verir.

Belirli IP Adresleri

UFW ile çalışırken, kurallarınızda IP adreslerini de belirtebilirsiniz. Örneğin, iş veya ev IP adresi gibi belirli bir IP adresinden gelen bağlantılara izin vermek istiyorsanız, izin vermek istediğiniz IP adresini sağlayarak parametreyi 203.0.113.4kullanmanız gerekir from:

* sudo ufw allow from 203.0.113.4

kopyala

Output

Rule added

Ayrıca, IP adresinin bağlanmasına izin verilen bir bağlantı noktası, to any portardından bağlantı noktası numarası ekleyerek de belirtebilirsiniz . Örneğin, 203.0.113.4bağlantı noktasına 22(SSH) bağlanmaya izin vermek istiyorsanız , şu komutu kullanın:

* sudo ufw allow from 203.0.113.4 to any port 22

kopyala

Output

Rule added

alt ağlar

IP adreslerinin bir alt ağına izin vermek istiyorsanız, bunu bir ağ maskesi belirtmek için [CIDR gösterimini](https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing#:%7E:text=CIDR%20notation%20is%20a%20compact,bits%20in%20the%20network%20mask.) kullanarak yapabilirsiniz . Örneğin, ile arasında değişen tüm IP adreslerine izin 203.0.113.1vermek 203.0.113.254istiyorsanız bu komutu kullanabilirsiniz:

* sudo ufw allow from 203.0.113.0/24

kopyala

Output

Rule added

Aynı şekilde, alt ağın 203.0.113.0/24bağlanmasına izin verilen hedef bağlantı noktasını da belirtebilirsiniz . Yine, 22örnek olarak bağlantı noktasını (SSH) kullanacağız :

* sudo ufw allow from 203.0.113.0/24 to any port 22

kopyala

Output

Rule added

Belirli Bir Ağ Arayüzüne Bağlantılar

Yalnızca belirli bir ağ arabirimi için geçerli olan bir güvenlik duvarı kuralı oluşturmak istiyorsanız, bunu ağ arabiriminin adının ardından "izin ver" seçeneğini belirleyerek yapabilirsiniz.

Devam etmeden önce ağ arayüzlerinize bakmak isteyebilirsiniz. Bunu yapmak için şu komutu kullanın:

* ip addr

kopyala

Output Excerpt

2: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state

. . .

3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default

. . .

Vurgulanan çıktı, ağ arabirimi adlarını gösterir. Genellikle eth0veya gibi bir adla adlandırılırlar enp3s2.

Bu nedenle, sunucunuzun adında bir genel ağ arabirimi varsa, bu komutla eth0HTTP trafiğine (port 80) izin verebilirsiniz :

* sudo ufw allow in on eth0 to any port 80

kopyala

Output

Rule added

Rule added (v6)

Bunu yapmak, sunucunuzun genel internetten HTTP istekleri almasına izin verir.

Veya MySQL veritabanı sunucunuzun (port 3306) özel ağ arayüzündeki bağlantıları dinlemesini eth1istiyorsanız, örneğin şu komutu kullanabilirsiniz:

* sudo ufw allow in on eth1 to any port 3306

kopyala

Output

Rule added

Rule added (v6)

Bu, özel ağınızdaki diğer sunucuların MySQL veritabanınıza bağlanmasına izin verir.

Adım 6 — Bağlantıları Reddetme

Gelen bağlantılar için varsayılan ilkeyi değiştirmediyseniz, UFW tüm gelen bağlantıları reddedecek şekilde yapılandırılır. Genel olarak bu, belirli bağlantı noktalarına ve IP adreslerine açıkça izin veren kurallar oluşturmanızı gerektirerek güvenli bir güvenlik duvarı ilkesi oluşturma sürecini basitleştirir.

Ancak, bazen sunucunuzun saldırıya uğradığını bildiğiniz için kaynak IP adresine veya alt ağa dayalı olarak belirli bağlantıları reddetmek isteyeceksiniz. Ayrıca, varsayılan gelen politikanızı **izin verecek** şekilde değiştirmek istiyorsanız (ki bu önerilmez), bağlantılara izin vermek istemediğiniz tüm hizmetler veya IP adresleri için **reddetme** kuralları oluşturmanız gerekir .

Yazmak için **inkar** kuralları değiştirmekte, daha önce açıklanan komutları kullanabilirsiniz **izin** ile **inkar** .

Örneğin, HTTP bağlantılarını reddetmek için şu komutu kullanabilirsiniz:

* sudo ufw deny http

kopyala

Output

Rule added

Rule added (v6)

Veya tüm bağlantıları reddetmek 203.0.113.4istiyorsanız bu komutu kullanabilirsiniz:

* sudo ufw deny from 203.0.113.4

kopyala

Output

Rule added

Bazı durumlarda, sunucudan giden bağlantıları da engellemek isteyebilirsiniz. Tüm kullanıcıların 25SMTP trafiği için bağlantı noktası gibi sunucudaki bir bağlantı noktasını kullanmasını engellemek için, deny outardından bağlantı noktası numarasını kullanabilirsiniz:

* sudo ufw deny out 25

kopyala

Output

Rule added

Rule added (v6)

Bu, sunucudaki tüm giden SMTP trafiğini engeller.

Adım 7 — Kuralları Silme

Güvenlik duvarı kurallarının nasıl silineceğini bilmek, onları nasıl oluşturacağınızı bilmek kadar önemlidir. Hangi kuralların silineceğini belirtmenin iki farklı yolu vardır: kural numarasına veya insan tarafından okunabilir değerine göre (kuralların oluşturulduklarında nasıl belirtildiğine benzer şekilde).

Numaraya Göre Bir UFW Kuralını Silme

Bir UFW kuralını numarasına göre silmek için önce tüm güvenlik duvarı kurallarınızın numaralı bir listesini almak isteyeceksiniz. UFW durum komutu, burada gösterildiği gibi, her kuralın yanında sayıları görüntüleme seçeneğine sahiptir:

* sudo ufw status numbered

kopyala

Numbered Output:

Status: active

To Action From

-- ------ ----

[ 1] 22 ALLOW IN 15.15.15.0/24

[ 2] 80 ALLOW IN Anywhere

Bağlantı noktası 80 (HTTP) bağlantılarına izin veren kural numarası **2'yi** silmek istediğinize karar verirseniz , bunu aşağıdaki gibi bir UFW silme komutunda belirtebilirsiniz:

* sudo ufw delete 2

kopyala

Output

Deleting:

allow 80

Proceed with operation (y|n)? y

Rule deleted

Bu, bir onay ister ve ardından HTTP bağlantılarına izin veren kural 2'yi siler. IPv6'yı etkinleştirdiyseniz, ilgili IPv6 kuralını da silmek isteyeceğinizi unutmayın.

Ada Göre Bir UFW Kuralını Silme

Kural numaralarını kullanmak yerine, kuralın türüne (tipik olarak allowveya deny) ve bu kuralın hedefi olan hizmet adına veya bağlantı noktası numarasına veya uygulama profiline dayanan insan tarafından okunabilir değeriyle de bir kurala başvurabilirsiniz. kullanılmış olması durumunda isim. Örneğin, daha önce etkinleştirilen allowbir uygulama profili adlı bir kuralı silmek isterseniz Apache Full, şunları kullanabilirsiniz:

* sudo ufw delete allow "Apache Full"

kopyala

Output

Rule deleted

Rule deleted (v6)

deleteKomut adını veya liman ile bir hizmeti başvuran oluşturulan edildi kuralları için aynı şekilde çalışır. Örneğin, daha önce ile HTTP bağlantılarına izin vermek için bir kural ayarladıysanız sudo ufw allow http, söz konusu kuralı şu şekilde silebilirsiniz:

* sudo ufw delete allow http

kopyala

Output

Rule deleted

Rule deleted (v6)

Hizmet adları, kurallar belirtilirken bağlantı noktası numaralarıyla değiştirilebildiğinden allow 80, aşağıdakiler yerine aynı kurala da başvurabilirsiniz allow http:

* sudo ufw delete allow 80

kopyala

Output

Rule deleted

Rule deleted (v6)

UFW kurallarını ada göre silerken, varsa hem IPv4 hem de IPv6 kuralları silinir.

Adım 8 — UFW Durumunu ve Kurallarını Kontrol Etme

UFW'nin durumunu istediğiniz zaman şu komutla kontrol edebilirsiniz:

* sudo ufw status verbose

kopyala

UFW, varsayılan olarak devre dışıysa, şöyle bir şey görürsünüz:

Output

Status: inactive

UFW etkinse, ki bu 3. Adımı izlediyseniz olmalıdır, çıktı etkin olduğunu söyleyecek ve ayarlanmış tüm kuralları listeleyecektir. Örneğin, güvenlik duvarı 22herhangi bir yerden SSH (bağlantı noktası ) bağlantılarına izin verecek şekilde ayarlanmışsa , çıktı şöyle görünebilir:

Output

Status: active

Logging: on (low)

Default: deny (incoming), allow (outgoing), disabled (routed)

New profiles: skip

To Action From

-- ------ ----

22/tcp ALLOW IN Anywhere

statusUFW'nin güvenlik duvarını nasıl yapılandırdığını kontrol etmek istiyorsanız komutu kullanın .

Adım 9 — UFW'yi Devre Dışı Bırakma veya Sıfırlama (isteğe bağlı)

UFW kullanmak istemediğinize karar verirseniz, şu komutla devre dışı bırakabilirsiniz:

* sudo ufw disable

kopyala

Output

Firewall stopped and disabled on system startup

UFW ile oluşturduğunuz hiçbir kural artık etkin olmayacaktır. Daha sudo ufw enablesonra etkinleştirmeniz gerekirse , her zaman çalıştırabilirsiniz .

Zaten yapılandırılmış UFW kurallarınız varsa ancak baştan başlamak istediğinize karar verdiyseniz, sıfırlama komutunu kullanabilirsiniz:

* sudo ufw reset

kopyala

Output

Resetting all rules to installed defaults. This may disrupt existing ssh

connections. Proceed with operation (y|n)? y

Backing up 'user.rules' to '/etc/ufw/user.rules.20210729\_170353'

Backing up 'before.rules' to '/etc/ufw/before.rules.20210729\_170353'

Backing up 'after.rules' to '/etc/ufw/after.rules.20210729\_170353'

Backing up 'user6.rules' to '/etc/ufw/user6.rules.20210729\_170353'

Backing up 'before6.rules' to '/etc/ufw/before6.rules.20210729\_170353'

Backing up 'after6.rules' to '/etc/ufw/after6.rules.20210729\_170353'

Bu, UFW'yi devre dışı bırakacak ve önceden tanımlanmış tüm kuralları silecektir. Bu size UFW ile yeni bir başlangıç ​​sağlayacaktır. Herhangi bir noktada değiştirdiyseniz, varsayılan ilkelerin orijinal ayarlarına değişmeyeceğini unutmayın.

Çözüm

Güvenlik duvarınız artık (en azından) SSH bağlantılarına izin verecek şekilde yapılandırılmıştır. Gereksiz bağlantıları sınırlandırırken sunucunuzun ihtiyaç duyduğu diğer gelen bağlantılara izin verdiğinizden emin olun, böylece sunucunuz işlevsel ve güvenli olacaktır.

Daha yaygın UFW yapılandırmaları hakkında bilgi edinmek için [UFW Essentials: Ortak Güvenlik Duvarı Kuralları ve Komutları](https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands) öğreticisine bakın.