LİNUX İŞLETİM SİSTEMİNİN KÖPRÜ MODUNDA ÇALIŞTIRILMASI VE GÜVENLİK DUVARI İŞLEMLERİ

Belge Hakkında

Bu belge ”GNU Free Documentation Licence” ı ile kaynak gösterilmek ve önceden yazarından izin alınmak kaydıyla yeniden yayınlanabilir. Belge içerisinde “Linux, iptables, ebtables ” gibi tescilli markaların isimlerinden söz edilmektedir.

Belgedeki eksik, yanlış ya da geliştirilmesi gerektiğini düşündüğünüz yerleri lütfen yazarına e-posta ile bildiriniz.

Bu belgenin en güncel haline,

http://www.enderunix.org/docs/linuxbridgemode.pdf

adresinden ulaşabilirsiniz.

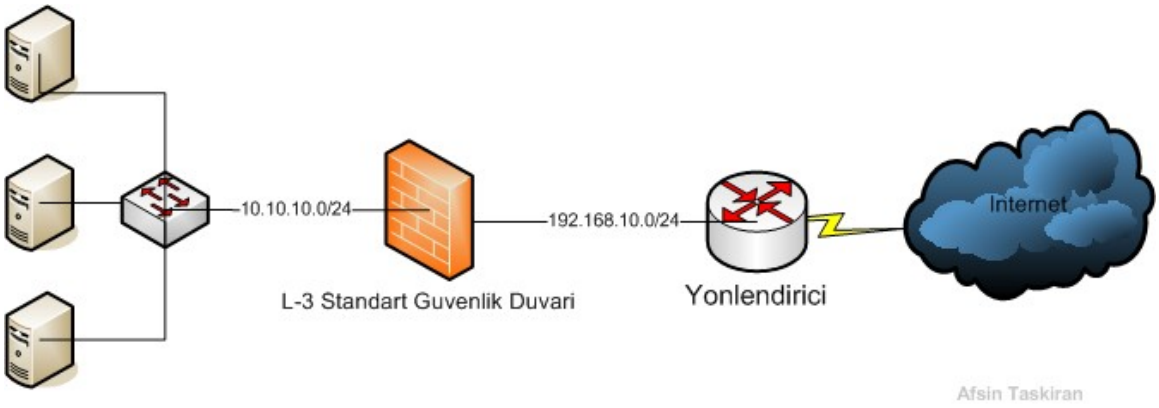
Sürüm numarası:	1.0
Belgenin İlk Oluşturulma Tarihi:	06.02.2007
Belgenin Son Güncellenme Tarihi:	12.02.2007

Tüm hakları Afşin Taşkıran’a aittir.

YAZAR HAKKINDA

Afşin TAŞKIRAN
EnderUnix Yazılım Geliştirme Takımı ~ Türkiye
Çekirdek Takım Üyesi
afsin ~ enderunix.org
http://www.enderunix.org/afsin

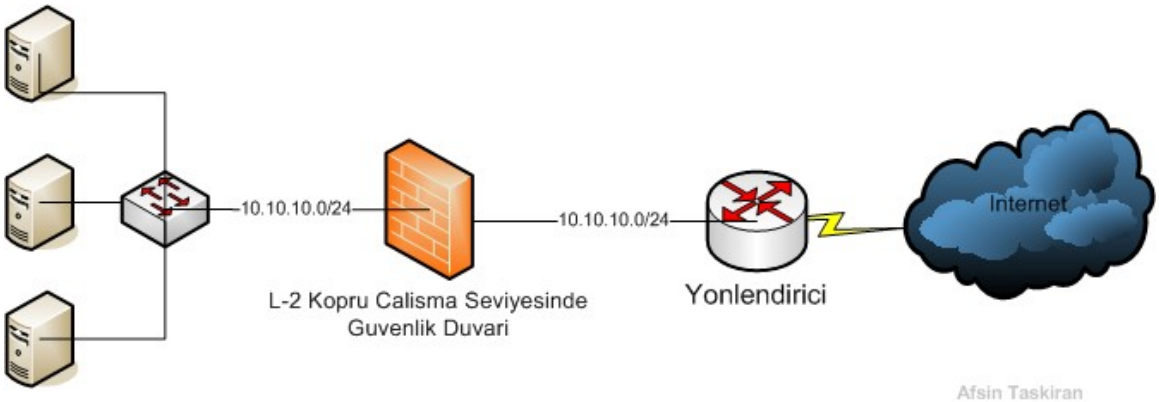
Güvenlik duvarlarının çıkış amacı gelen ve giden paketleri kontrol altında tutabilmek ve dolayısıyla paket filtreleme yapmaktı. Ancak gelişen ihtiyaçlar ile birlikte güvenlik duvarları birden fazla ağ katmanı arasında yönlendirici cihazlar gibi konumlandırılmaya başlandı. Böylece güvenlik duvarına gelen ve güvenlik duvarından giden paketlerin kontrolünün dışında hedefi farklı ağ katmanlarındaki sistemler olan paketler üzerinde kontrol yapılmaya başlandı. Günümüzde çalışan bir çok güvenlik duvarı da bu mantığa göre çalışmaktadır.



Şekil: Standart Güvenlik Duvarı Yapısı

Ağ geçidi olarak çalışan güvenlik duvarlarının farklı ağ katmanlarında IP adresi olması gerektiğinden ağ geçidinin gizliliği soz konusu olamaz. Varolan bir ağ yapısına güvenlik duvarı konumlandırılmak istendiğinde ağ katmanlarının ayrılması ve en az iki ağ katmanı oluşturulması gerekir. Adres yönlendirme gerekmeyen ağlarda güvenlik duvarının ilgili ağ arayüzünde IP adresi olmadan çalıştırılabilmesi, bu gibi güvenlik ve yapılandırma problemlerine çözüm getirmektedir. Güvenlik duvarının bu şekilde çalıştırılmasına köprü modu da (bridge mode) denmektedir.Ayrıca köprü modunda çalıştırılırken kullanıcılara hissettirmeden trafik kontrolu yapılabilmektedir. Layer 7 paket filtreleme ve IDS/IPS sistemler için ideal yapıdır.

Güvenlik duvarının köprü modunda çalışabilmesi için mac adresleri kullanılmaktadır. Bundan dolayı çalışma seviyesi Layer-2 dir.



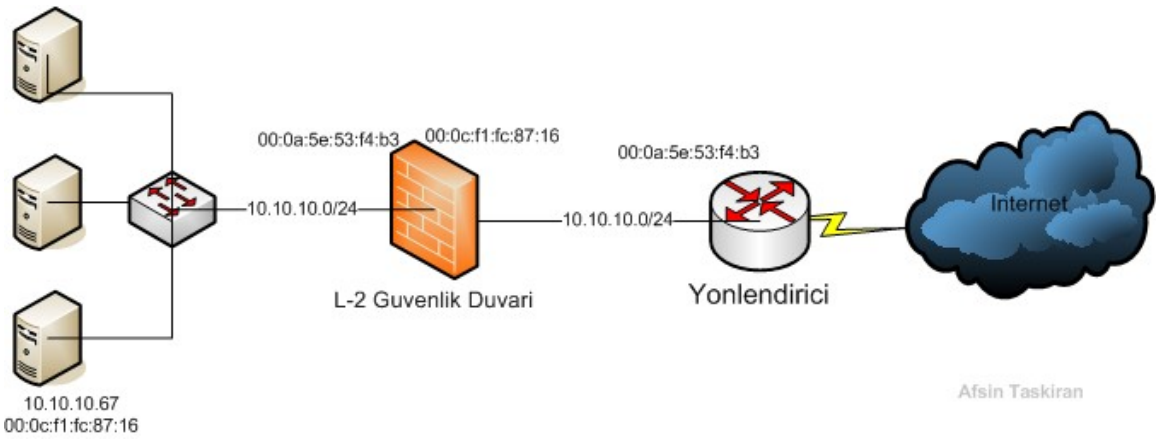
Şekil: Köprü modunda çalışan güvenlik duvarı

Linux sistemin köprü modunda çalıştırılabilmesi için bridge (bridge.sf.net) projesi kullanılmaktadır. Standart linux çekirdeğinde bridge desteği bulunmadığından çekirdeğe bu desteğin verilmesi gerekir.

Köprü Modunda Çalışırken MAC Adresleri

Ethernet çalışan yapılar ağ içerisinde haberleşme yaparken mac adreslerini kullanmaktadır. Yukarıdaki yapıda güvenlik duvarı L-2 modunda çalıştığından normal şartlarda ağ arayüzleri arasında mac adreslerinin geçişi söz konusu olmaz. Bu durumda Sunuculardan biri yönlendiri cihaza ulaşmak istediğinde mac adresi bilinemediğinden ulaşamayacaktır.

Güvenlik duvarında bu gibi problemleri engelleme amacıyla arp proxy denen yapılar kullanılmaktadır. Arp proxy sayesinde ağ arayüzleri birbirlerine gelen arp adreslerini karşılıklı olarak anons ederler.



Şekil: Köprü modunda çalışan güvenlik duvarında proxy arp

Yukarıdaki örneğimizden de görüldüğü gibi yönlendirici cihaz 10.10.10.67 IP li sunucuya erişmek istediğinde mac adresini soracak güvenlik duvarından dönüş olacaktır. Aynı şekilde sunucu sistem de yönlendirici cihaza erişmek istediğinde güvenlik duvarı tarafından mac adresi duyurulacaktır. Her iki durumda da paketlerin güvenlik duvarına gelmesi sağlanır.

Linux'un Köprü Modunda Çalıştırılması

Linux çekirdeğininizin bulunduğu dizine uygun bridge yamasını http://ebtables.sourceforge.net/ adresinden indirin.

```
EnderFW # cd /usr/src/linux
EnderFW # wget bridge_brnf.tar.gz
EnderFW # patch -p1 < bridge_surumnumarasi.patch
```

```
EnderFW # make menuconfig
```

Çekirdek konfigurasyonunuzda BRIDGE_NETFILTER ve IP_NF_ARPTABLES (modül olarak eklenebilir) parametreleri aktif hale getirilmelidir.

Daha sonra standart çekirdek derleme işlemleri yapılmalı ve derlediğiniz bridge desteği verilmiş çekirdek ile sistem açılmalıdır.

Linux çekirdeğine bridge desteği verdikten sonra bridge-utils isimli köprü modunda kullanacağımız yazılımlar kurulmalıdır.

```
EnderFW # cd /usr/local/src
EnderFW # wget http://.../bridge-utils-1.2.tar.gz
EnderFW # tar –zxvf bridge-utils-1.2.tar.gz
EnderFW # cd bridge-utils-1.2
EnderFW # make
EnderFW # make install
```

Bu aşamaya kadar sorunsuz kurulumları gerçekleştirdiyseniz herşey hazır demektir.

```
EnderFW # brctl
```

Öncelikle L2 seviyesinde sistemimizi çalıştıracağımızdan Linux sistemde proxy arp'ın aktif olmaı gerekir.

```
EnderFW # echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy_arp
EnderFW # echo 1 > /proc/sys/net/ipv4/conf/eth2/proxy_arp
```

eth1 ve eth2 köprü modunda çalışacak olan ağ arayüzleridir.

IP yönlendirmeyi de aktif hale getirmelisiniz.

```
EnderFW # sysctl -w net.ipv4.ip_forward=1
```

Güvenlik duvarınızı köprü modunda çalıştırmak için asıl yapılandırmanızı bridge yazılımı ile yapabilirsiniz.

Köprüde kullanacağınız ağ arayüzlerinin IP adresleri olmamalıdır.

```
EnderFW # ifconfig eth1 0.0.0.0
EnderFW # ifconfig eth2 0.0.0.0
```

Köprü modunda bir ağ arayüzü oluşturmak için;

```
EnderFW # brctl addbr br0
```

Bu komut ile br0 isimli bir köprü oluşturulmuştur.

Fiziksel ağ arayüzlerinizi bu köprüye dahil etmeniz gerekir.

```
EnderFW # brctl addif br0 eth1
EnderFW # brctl addif br0 eth2
```

br0 köprüsünü çalışır duruma getirmek için aşağıdaki komutu kullanabilirsiniz.

```
EnderFW # ifconfig br0 up
```

Sisteminizi köprü moduna geçirdikten sonra IPTables ve ebtables ile detaylı paket filtreleme işlemleri yapabilrsiniz.

Ebtables Kullanımı

ebtables, üst seviye filtreleme işlemlerinin yapılabildiği bir yazılımdır. 2. katmanda (Layer 2) filtreleme yapar. Temel IP filtrelemeyi ve iptables ile birlikte köprü (bridge) modda tam filtrelemeyi sağlar.

Ana Özellikleri:

- Ethernet filtreleme
- MAC adres filtreleme
- Basit IP başlığı filtreleme
- ARP Başlığı filtreleme
- 802.1Q VLAN filtreleme
- Giriş çıkış bazında arayüz filtreleme

Ebtables'in Kurulumu:

http://ebtables.sourceforge.net adresinden ebtables'in son sürümünü bilgisayarınıza indirin. Daha sonra;

```
EnderFW # tar –zxvf ebtables-v2.0.8-rc3.tar.gz
EnderFW # cd ebtables-v2.0.8-rc3
EnderFW # make
EnderFW # make install
```

Eğer init betiklerinizin yeri /etc/rc.d/init.d değilse ebtables'i kurulum aşamasında INITDIR parametresiyle birlikte derlemelisiniz. Örneğin init dizininiz /etc/init.d ise;

```
EnderFW # make install INITDIR=/etc/init.d/
```

olmalıdır.

Konsolda `ebtables –V` komutunu verdiğinizde sürüm bilgilerini ekrana yazıyorsa ebtables başarıyla kuruldu demektir.

ebtables Örnekleri

ebtables ile çok kullanışlı kurallar oluşturabilirsiniz.

Aşağıdaki örnekte özel bir mac adresi için sadece IPV4 sınıfı IP kullanımına izin verilmiş, diğer türler yasaklanmıştır.

```
ebtables -A FORWARD -s 00:11:22:33:44:55 -p IPV4 -j ACCEPT
```

```
ebtables -A FORWARD -s 00:11:22:33:44:55 -j DROP
```

ebtables ile mac adres NAT işlemleri yapabileceğimizi belirtmiştik.Hedefi 00:11:22:33:44:55 olan paketlerin hedef adresini 54:44:33:22:11:00 olarak değiştirmek için aşağıdaki örneği kullanabilirsiniz.

```
ebtables -t nat -A PREROUTING -d 00:11:22:33:44:55 -i eth0 \
        -j dnat --to-destination 54:44:33:22:11:00
```

Kaynaklar:

[1] http://www.faqs.org/docs/Linux-HOWTO/BRIDGE-STP-HOWTO.html
[2] http://www.spenneberg.com/talks/linux-kongress2002/ralf-spenneberg.bridgewall.pdf
[3] http://lists.netfilter.org
[4] http://linux-net.osdl.org/index.php/Bridge
[5] http://ebtables.sourceforge.net