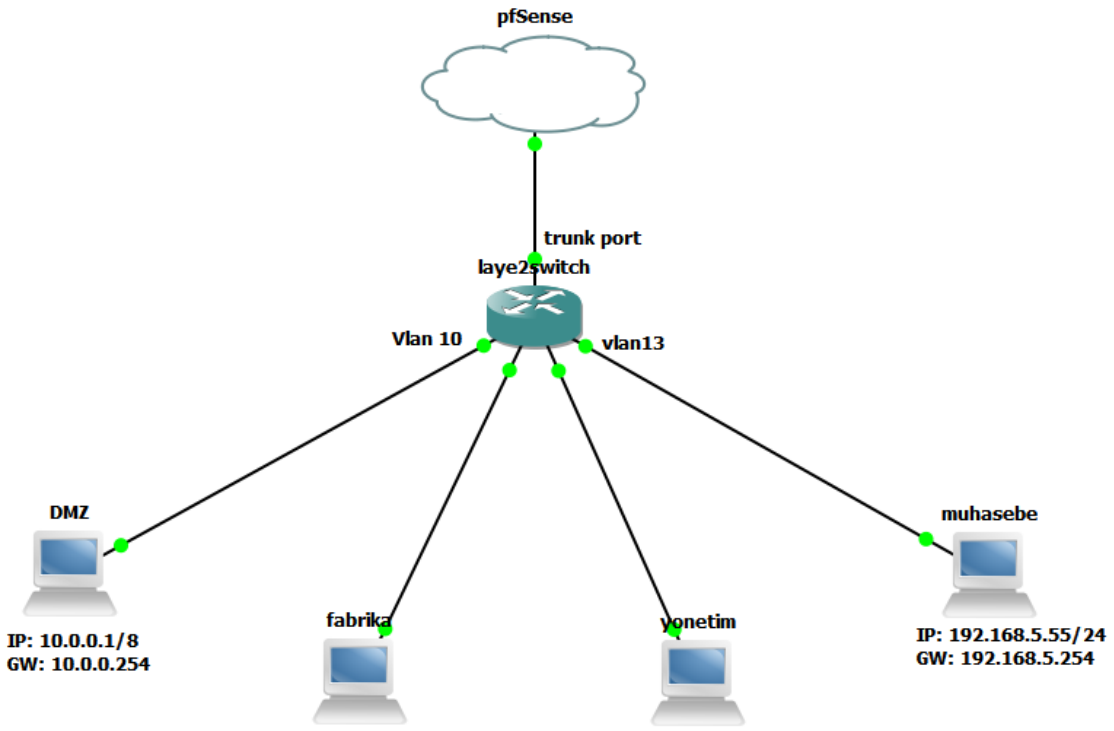
pfSense Firewall & Router ile Vlan Yönetimi

Orta ölçekli ve kurumsal bir çok firma network al yapısında vlan'lar uygulamaktadır. Vlan'lar ile ayrılan networkler bir birleri ile haberleşemez ve vlan'lar arası routing yaparken maksimum koruma sağlanabilir.

Bu yazıda, fabrikam.com ağında Layer 2 bir switch üzerinde vlan'lar oluşturarak ağları bölmek ve trunk porta bağlı pfSense ile bu vlan'ları yönetmek anlatılmışır. Bu uygulama labaratuar ortamında kurulmuş ve test edilmiştir.Yazılanları bire bir kendi yapınızda uygulamanız durumunda, ciddi sorunlar yaşayabilirsiniz.

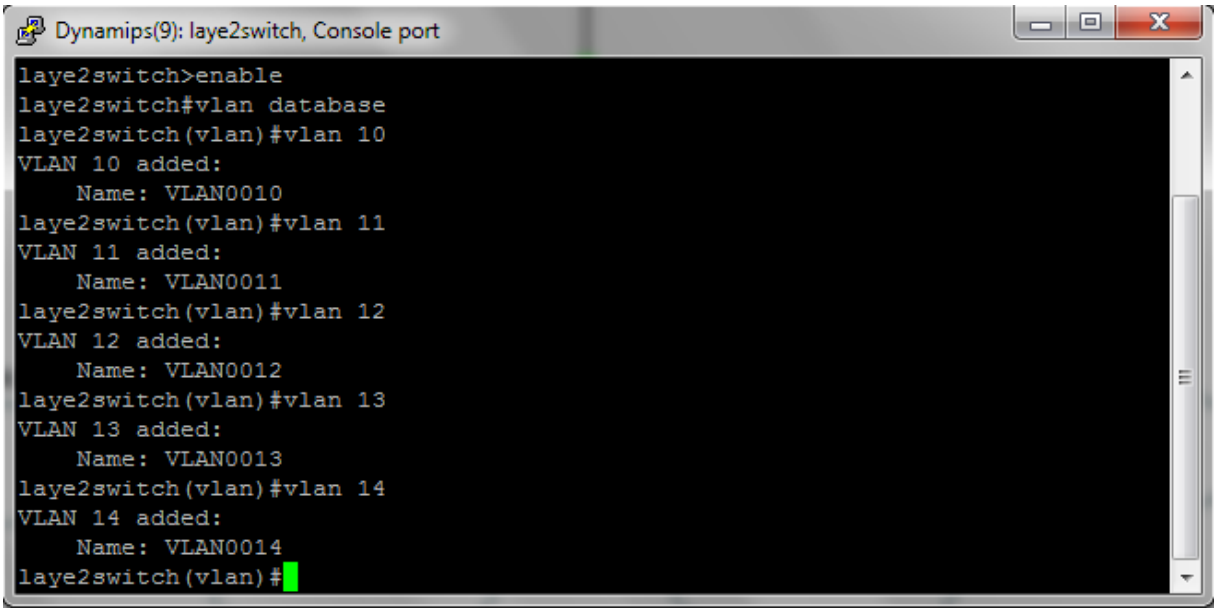
Dikkat: Bu yazıda layer2 switch nasıl çalışır, vlan nedir, trunk port nedir ve nasıl yapılır gibi teorik network bilgileri bulunmuyor. Eğer bu terimlerin ne olduğunu bilmiyorsanız detaylarını **19-20 Mayıs 2011 tarihlerindeki Uygulamalı pfSense** eğitiminde bulabilirsiniz ☺

fabrikam.com Network Yapısı



Adım 1:

Layer2 switch'de vlan database oluşturulur. Bu dökümanda uygulanan vlan id'leri, vlan10-vlan14 arasındadır.



Görüntüleyelim oluşturulan vlan'ları,

```
Dynamips(9): laye2switch, Console port
laye2switch#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
10   VLAN0010                         active    Fa1/0
11   VLAN0011                         active    Fa1/1
12   VLAN0012                         active    Fa1/2
13   VLAN0013                         active    Fa1/3
14   VLAN0014                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
12   enet  100012     1500  -      -      -        -    -        0      0
13   enet  100013     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
14   enet  100014     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
laye2switch#
```

FastEthernet'leri vlan üyesi yapalım ;

```
laye2switch#configure terminal
laye2switch(config)#interface FastEthernet 1/0
laye2switch(config-if)#switchport access vlan 10
laye2switch(config-if)#no shutdown
laye2switch(config-if)#
*Mar  1 00:09:13.095: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar  1 00:09:14.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up
```

Diğer FastEthernetlerde aynı komutlar ile istenilen vlanların üyesi yapılmalıdır.

Aynı vlan'da bulunan istemciler bir birleri ile haberleşebilecektir. Farklı vlan'lar ise haberleşemeyecektir. Trunk port oluşturup, pfSense ile farklı vlan'lar arası rouing ve vlan'ların internete çıkma gereksinimlerini yapalım.

Trunk port ayarı,

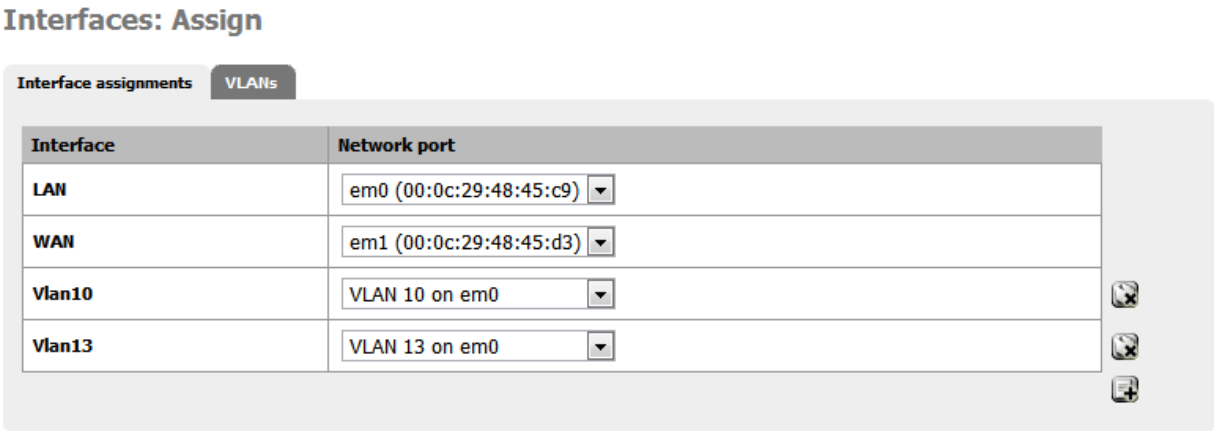
```
laye2switch(config-if)#switchport mode trunk
laye2switch(config-if)#switchport trunk encapsulation dot1q
laye2switch(config-if)#no shutdown
*Mar  1 00:14:34.359: %DTP-5-TRUNKPORTON: Port Fa1/10 has become dot1q trunk
```

Bakalım trunk portumuza

```
laye2switch#show interfaces fastEthernet 1/10 switchport
Name: Fa1/10
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
......
```

pfSense Vlan Yapılandırması,

İstemcilerden trunk porta gelen trafik dot1q olarak pfSense e ulaşmaktadır. Bu paketi okuyup geri yanı dönebilmek için pfSense'de vlan gruplarını oluşturmamız gerekiyor.



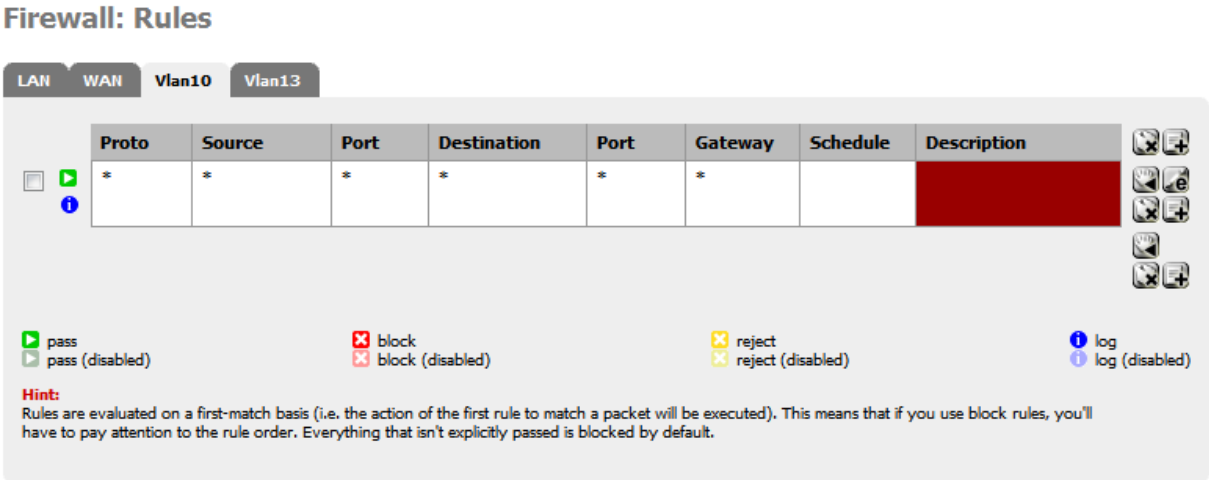
Oluşturulan Vlan’lar artık birer subinterface. Network yapımıza göre vlan’lara ip verip iletişim kurmaya başlayabiliriz.

Vlan10 interface (vlan1)	
Status	up
MAC address	00:0c:29:48:45:c9
IP address	10.0.0.254
Subnet mask	255.0.0.0
Media	1000baseTX <full-duplex>
In/out packets	203/69 (17 KB/11 KB)
In/out errors	0/0
Collisions	0

Vlan13 interface (vlan4)	
Status	up
MAC address	00:0c:29:48:45:c9
IP address	192.168.5.254
Subnet mask	255.255.255.0
Media	1000baseTX <full-duplex>
In/out packets	30/11 (3 KB/849 bytes)
In/out errors	0/0
Collisions	0

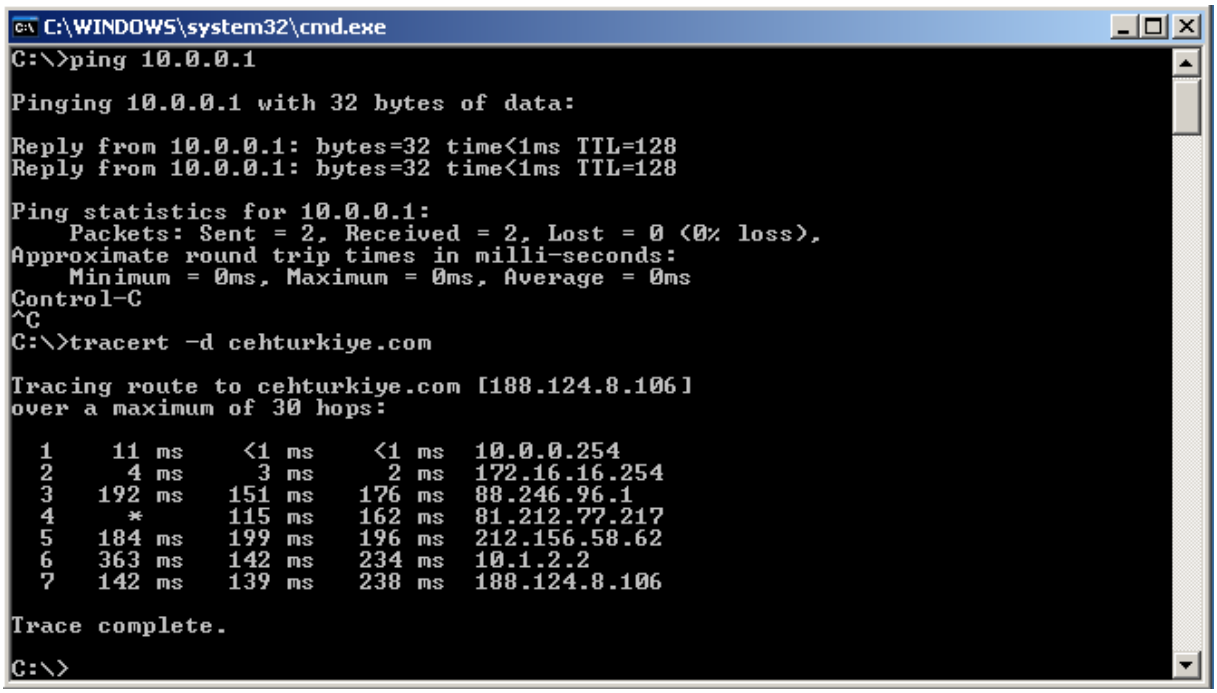
Vlanlar arası rouing yaparken ve vlan'dan gelen-giden paketleri filtreleme için firewall'dan gerekli kuralları yazmamız gerekiyor.

Vlan10'dan gelen istemciler, Vlan13 deki istemcilere ping atabilsin, dosya sistemine bağlabilsin vb. Not:Lab. Ortamında tüm trafiğe izin verilmiştir.



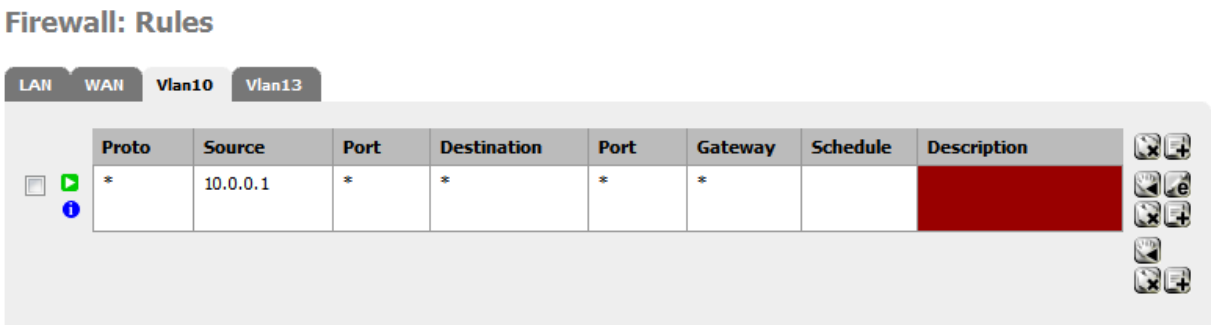
Şimdi test aşamasına geçebiliriz,

Vlan10 da bulunan 10.0.0.1 bilgisayarından pfSense ile haberleşebiliyor muyum ? İnernet'e çıkabiliyormuyum ?



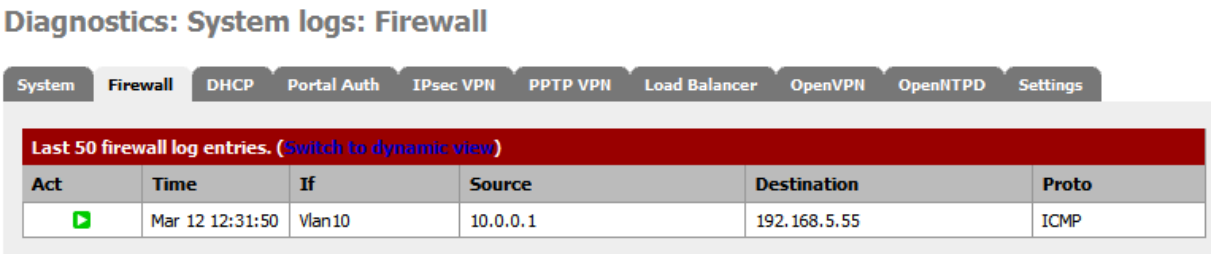
```
C:\WINDOWS\system32\cmd.exe
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>tracert -d cehturkiye.com

Tracing route to cehturkiye.com [188.124.8.106]
over a maximum of 30 hops:

  1    11 ms    <1 ms    <1 ms  10.0.0.254
  2     4 ms     3 ms     2 ms  172.16.16.254
  3   192 ms   151 ms   176 ms  88.246.96.1
  4     *      115 ms   162 ms  81.212.77.217
  5   184 ms   199 ms   196 ms  212.156.58.62
  6   363 ms   142 ms   234 ms  10.1.2.2
  7   142 ms   139 ms   238 ms  188.124.8.106

Trace complete.

C:\>
```

Vlan10'da bulunan 10.0.0.1 ip adresinin dışında, kimse vlan13 deki ağa erişemesin istiyorum.Bunun için firewall'dan kural oluşturup, diğer ip adreslerinin erişimlerini engelleyelim.



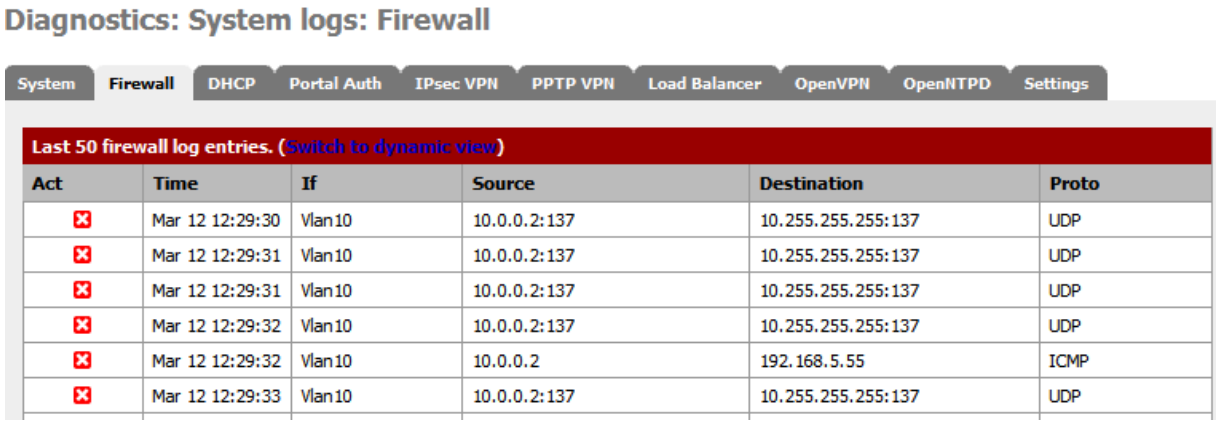
Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	10.0.0.1	*	*	*	*		

10.0.0.1 ip adresi vlan13 deki bir bilgisayara erişebilir durumda,



Act	Time	If	Source	Destination	Proto
	Mar 12 12:31:50	Vlan10	10.0.0.1	192.168.5.55	ICMP

10.0.0.2 ip adresi vlan13 e erişmek istediğinde trafik engellendi.



Act	Time	If	Source	Destination	Proto
	Mar 12 12:29:30	Vlan10	10.0.0.2:137	10.255.255.255:137	UDP
	Mar 12 12:29:31	Vlan10	10.0.0.2:137	10.255.255.255:137	UDP
	Mar 12 12:29:31	Vlan10	10.0.0.2:137	10.255.255.255:137	UDP
	Mar 12 12:29:32	Vlan10	10.0.0.2:137	10.255.255.255:137	UDP
	Mar 12 12:29:32	Vlan10	10.0.0.2	192.168.5.55	ICMP
	Mar 12 12:29:33	Vlan10	10.0.0.2:137	10.255.255.255:137	UDP

Yazar:
Ozan UÇAR
mail@ozanucar.com
www.cehturkiye.com