

ACL'yi Farklı Eylemlerle Kullanma

ACL (Access Control List) network erişimini sınırlar ve ağınıza bir security katmanı ekler. VigorSwitch ile network trafiğini MAC adreslerine, IPv4 adreslerine veya IPv6 adreslerine göre filtreleyebilirsiniz. Bu makalede, farklı ACL türleri ve eylemlerinin nasıl kullanılacağı tanıtılmaktadır.

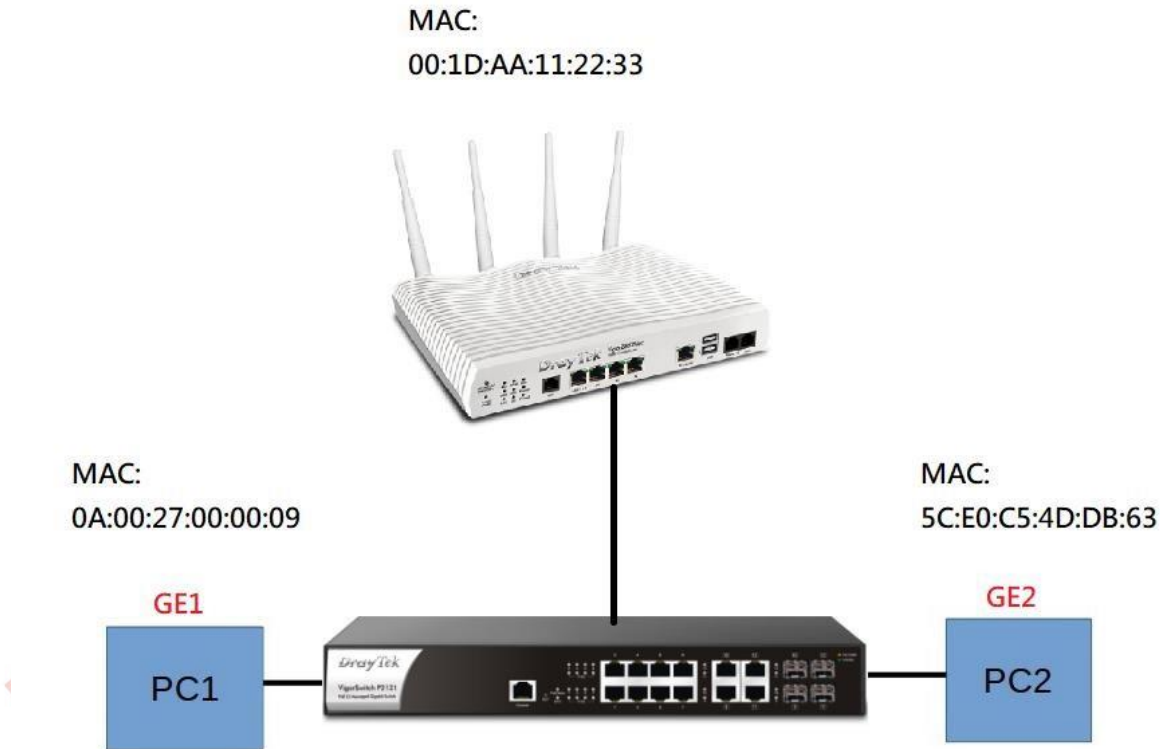
Permit: Sadece eşleşen kriterleri geç, diğerlerini filtrele.

Deny: Ölçütlere uyan trafiği filtreleyin, diğerlerini kabul edin.

Shutdown: Kriterlere uyan trafiği filtreleyin ve portu kapatın.

Permit olan MAC adresine göre filtrele

İlk senaryoda, Network Administrator PC1'in Router'e erişmesine ve PC2'yi engellemesine izin vermek istiyor.



1. ACL > Create ACL seçeneğine gidin, MAC sekmesine tıklayın ve bir profil adı ekleyin.

ACL > Create ACL > MAC

MAC IPv4 IPv6

ACL Profile Name:

No.	MAC ACL Name	Action
1	mac test	<input type="button" value="Edit"/>

2. ACL > Create ACL > MAC'e git.

1. adımda oluşturduğunuz profili seçin.
- Profil sırasını koyun.
- Action'u seç, buraya izin verdik.
- PC1 MAC adresini girin.
- Router MAC adresini girin

ACL > Create ACE > MAC

MAC IPv4 IPv6

ACL Profile Name: a mac test

Sequence: b 1 (1 - 2147483647)

Action: c Permit

Source MAC: Any

d 0A:00:27:00:00:09 / FF:FF:FF:FF:FF:FF

Destination MAC: Any

e 5C:E0:C5:4D:DB:63 / FF:FF:FF:FF:FF:FF

Ethertype: Any (0x600-0xFFFF)

VLAN: Any (1-4094)

802.1p: Any 0-7 / 0-7

Add

3. ACL> ACL Binding'e gidin, GE1 GE2 portunu seçin ve uygulanacak ACL profilini seçin.

ACL Binding

Ports: GE1, GE2

MAC ACL: mac test

IPv4 ACL: Select IPv4 ACL

IPv6 ACL: Select IPv6 ACL

Apply

4. Yukarıdaki konfigürasyonla, PC1, GE2'ye bağlandığı halde Router'a erişebilecek, PC2 Router'e erişemeyecektir..

- Deny eylemiyle IP adresine göre filtreleme
- Bu senaryoda, Network Administrator misafir ağının web sunucusuna erişmesini engellemek istiyor.



1. ACL > Create ACL > IPv4 'e gidin. Bir ACL Profile Name oluřturun.

Dashboard

ACL > Create ACL > IPv4

MAC IPv4 IPv6

ACL Profile Name:

No.	IPv4 ACL Name	Action
1	Test1	<input type="button" value="Deny"/>

2. ACL > Create ACE > IPv4'e gidin.
3. 1. adımda oluřturduėunuz profili seėin
4. Action'u seė, buraya Deny'i yerleřtir.
5. Protokolü koy
6. Guest networkü Source IP'ye yerleřtirin
7. Web sunucusunu Destination IP'ye yerleřtirin

ACL Profile Name: a Test1

Sequence: 1 (1 - 2147483647)

Action: b Deny

Protocol: c Any

Source IP: Any

d 192.168.2.1 / 255.255.255.0

Destination IP: Any

e 192.168..188.15 / 255.255.255.255

Service: Any

Source Port: Any

Destination Port: Any

ICMP Type: Any

ICMP code: Any

0-255

Add

3. ACL > ACL Binding'e gidin, portları seçin, IPv4 ACL profili

Ports: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8, GE9, GE10, GE11, GE12

MAC ACL: Select MAC ACL

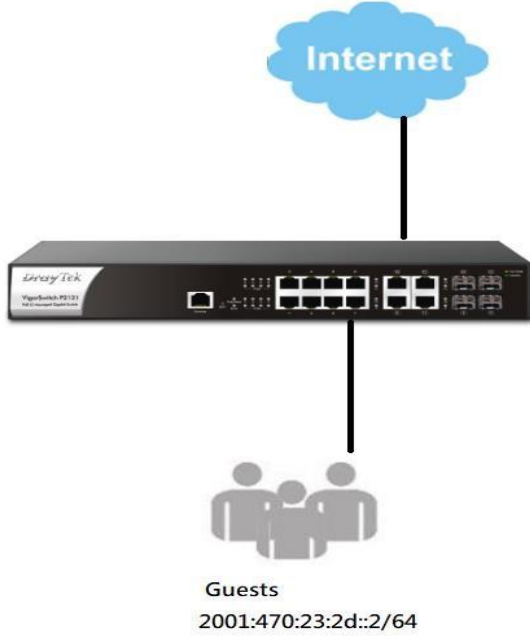
IPv4 ACL: Test1

IPv6 ACL: Select IPv6 ACL

Apply

4. Yukarıdaki konfigürasyonla, sadece guest network (192.168.2.x) web sunucusuna erişemez (192.168.188.15) Shutdown eylemiyle birlikte IPv6 adresine göre filtreleme Kapat

Bu senaryoda, network administrator misafirlerin IPv6 hizmetini kullanmasını engellemek ve IPv6 paketlerinin geçtiği portu kapatmak istiyor.



1. ACL > Create ACL > IPv6 'ya gidin. Bir ACL Profile Name oluşturun.

MAC IPv4 IPv6

ACL Profile Name:

No.	IPv6 ACL Name	Action
1	IPv6_test	<input type="radio"/>

2. ACL > Create ACE > IPv4'e git.
3. 1. adımda oluşturduğunuz profili seçin
4. Seçtiğimiz Action'a Shutdown'ı koyarız.
5. Guest networkü Source IP'ye yerleştirin.
6. Destination IP'ye Any ekleyin.

ACL > Create ACE > IPv6

MAC IPv4 IPv6

ACL Profile Name:	a	IPv6_test
Sequence:	1	(1 - 2147483647)
Action:	b	Shutdown
Protocol:		Any
Source IP:	<input type="checkbox"/> Any	
Destination IP:	c	2001:470:23:2d::2 / 64
Service:	d	<input checked="" type="checkbox"/> Any / 0-128
Source Port:		Any
Destination Port:		Any
ICMP Type:		Any
ICMP code:	<input checked="" type="checkbox"/> Any	0-255

[Add](#)

3. ACL > ACL Binding'e gidin, portları seçin, IPv6 ACL profili.

ACL > ACL Binding > ACL Binding

ACL Binding

Ports:	GE1, GE2, GE3, GE4
MAC ACL:	Select MAC ACL
IPv4 ACL:	Select IPv4 ACL
IPv6 ACL:	IPv6_test

[Apply](#)

4. Yukarıdaki konfigürasyonda, misafir IPv6 kullanırsa, belirli port kapatılacaktır.