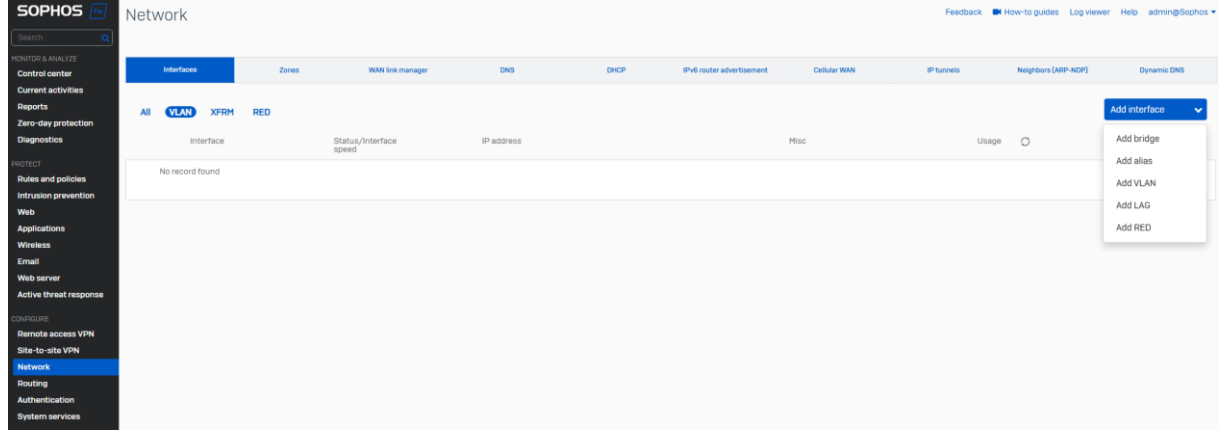


## InterVLAN Comm And DHCP

### InterVLAN Communication

Sophos FW üzerinde InterVLAN haberleşmesi için ilk olarak VLAN tanımlarının oluşturulması gerekiyor. VLAN tanımlarını oluşturmak için “Network -> Interfaces -> VLAN -> Add Interfaces -> Add VLAN” yolu takip edilmelidir.



Burada oluşturulmak istenen VLAN araüzü için “Name” kısmına VLAN ismi, “Interface” kısmında bağlanacağı/bağdaştırılacağı sanal/fiziksel port (burada LAG arayüzü de seçilebilir), “Zone” kısmı çalışacağı Zone, “VLAN ID” kısmında 802.1q protokolüyle eklenecek başlık bilgisinde VLAN ID kısmına eklenecek ID değeri tanımlanmalıdır. Son olarak ilgili VLAN tanımında kullanılan ip bloğunun Gateway olarak belirlenen ip adresi tanımlanmalıdır. Bu tanımlar yapıldıktan sonra ayarların kaydedilmesi yeterli olacaktır.

### VLAN interface

Interfaces	Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement
------------	-------	------------------	-----	------	---------------------------

#### Add VLAN

Name *	Client_VLAN
Hardware	PortB.100
Interface	PortB
Zone	LAN
VLAN ID *	100 [1-4094]
<input checked="" type="checkbox"/> IPv4 configuration	
IP assignment	<input checked="" type="radio"/> Static <input type="radio"/> PPPoE <input type="radio"/> DHCP
IPv4/netmask *	192.168.100.1 /24 [255.255.255.0]
Gateway detail	
Gateway name	
Gateway IP	
<input type="checkbox"/> IPv6 configuration	

VLAN tanımı oluşturulduktan sonra bu VLAN’a bağlı istemcilerin DHCP’den ip alması isteniyorsa “Network - DHCP” yolu takip edilmelidir. Burada FW üzerinde DCP sunucusu ayağa kaldırılabilir. FW üzerinde DHCP sunucusu ayağa kaldırmak için “Server -> Add -> IPv4” yolu, Relay tanımı yapmak için “Relay -> Add -> IPv4” yolu takip edilmelidir.

The screenshot shows the Sophos Firewall Network configuration page. The left sidebar contains navigation options: Monitor & Analyze, Control center, Current activities, Reports, Zero-day protection, Diagnostics, Protect, Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Active threat response, Configure, Remote access VPN, Site-to-site VPN, Network (selected), Routing, Authentication, System services, and System, Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware, and Certificates. The main content area is titled 'Network' and has tabs for Interfaces, Zones, WAN link manager, DNS, DHCP (selected), IPv6 router advertisement, Cellular WAN, IP tunnels, Neighbors (ARP-NDP), and Dynamic DNS. The DHCP section shows a table for DHCP servers with columns: Name, Interface, Lease detail, Static, IP version, Status, and Manage. One server is listed: 'GuestAccess\_DHCP' on interface 'GuestAP - 10.255.0.1' with a dynamic lease detail and IP version 'IPv4'. The status is 'On'. Below this, there are sections for DHCP Relay and IPv4/IPv6 leases, all showing 'No records found'.

DHCP sunucusu tanımı için;

- “Name” kısmına DHCP hizmetini tanımlamak üzere isim belirlenmelidir.
- “Interface” kısmında DHCP tanımının hizmet vereceği arayüz seçilmelidir.
- “Dynamic Ip Address” kısmında DHCP Ip Pool içerisinde kullanılacak ip adrs aralıkları belirtilmelidir. Burada dâhil edilecek ip aralıkları girilirken ip sırasına dikkat edilmelidir.
  - o Tanımın en üst kısmında ip bloğunun sonlarından bir aralık verilir, bu tanım altında ip bloğunun başından ip aralıkları tanımlandığı takdirde istemcilere ip bloğunun başından tanımlanan ip aralıklarından ip verilemeyebilir.
- “Static IP MAC Binding” kısmı için IP Pool tanımında belirtilen aralıklardan belirli istemcilerin bağlandığında aynı ip adresini alması istendiği durumda IP-MAC adresleri Bind edilerek/bağlanarak istemci her bağlandığında DHCP sunucusundan aynı ip adresini alması sağlanabilir.
  - o Policy’lerde cihaz bazlı tanımlar yapılmak istendiğinde Policy tanımı öncesinde cihazların IP adreslerinin burada sabitlenmesi gerekiyor.
- “Subnet Mask” kısmıyla verilecek ip adreslerini hangi Subnete sahip olduğu belirtiliyor.
- “Gateway” kısmında cihazlara Gateway ip adresi olarak hangi ip adresinin verileceği belirleniyor. Gateway adresi olarak DHCP sunucusunun bağlanacağı porta verilen ip adresi otomatik olarak verilebileceği gibi harici bir ip adresi de tanımlanabiliyor.
- “Lease Time” ve “Max Lease Time” kısımlarında istemcilere ip adreslerinin ne kadarlık zaman dilimi için ip adresi kiralanacağı belirtilmelidir.
- “Conflict” kısmıyla Ip Pool için belirlenen aralıkta tanımlı ip adreslerinden bir istemciye ip bilgisi önermeden önce birisinin önerilecek ip adresini farklı bir cihazda kullanılıp kullanılmadığını kontrol etmek için kullanılan özelliktir (ARP sorusuyla kontrol ediyor diye hatırlıyorum)

## Network

Interfaces	Zones	WAN link manager	DNS	<b>DHCP</b>	IPv6 router advertisement
------------	-------	------------------	-----	-------------	---------------------------

### General settings

Name *	<input type="text" value="CLNT VLAN DHCP SRV"/>		
Interface	<input type="text" value="Client_VLAN - 192.168.100.1"/>		
	<input type="checkbox"/> Accept client request via relay		
Dynamic IP lease			
	Start IP	End IP	<input type="button" value="+"/>
	<input type="text" value="192.168.100.50"/>	<input type="text" value="192.168.100.100"/>	<input type="button" value="-"/>
	<input type="text" value="192.168.100.150"/>	<input type="text" value="192.168.100.250"/>	<input type="button" value="-"/>
	* Press Tab to add a new row		
Static IP MAC mapping			
	Hostname	MAC address	IP address <input type="button" value="+"/>
	<input type="text" value="BOSS"/>	<input type="text" value="aa:bb:cc:dd-ee:ff"/>	<input type="text" value="192.168.100.52"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>
	* Press Tab to add a new row		
Subnet mask *	<input type="text" value="/24 (255.255.255.0)"/>		
Domain name	<input type="text"/>		
Gateway *	<input checked="" type="checkbox"/> Use interface IP as gateway		
	<input type="text" value="192.168.100.1"/>		
Default lease time *	<input type="text" value="1440"/>	1-43200 minutes (30 days)	
Max lease time *	<input type="text" value="2880"/>	1-43200 minutes (30 days)	
Conflict detection	<input checked="" type="checkbox"/> Enable		

- “DNS Server” kısmıyla istemcilere verilecek DNS bilgisinin tanımlandığı kısımdır. İsteğe bağlı olarak Sophos FW üzerindeki DNS bilgisiyle aynı dağıtılması da sağlanabilir.
- “Wins Server” kısmıyla istemcilerin bilgisayar adlarının üzerinden ip adreslerinin bulunabilmesi için kullanılan NETBIOS hizmetinin çalıştığı bir sunucu mevcut ise kullanıcının DHCP sunucusundan ip bilgileri aldıktan sonra kendisini buraya kaydetmesi sağlanabilir. Bu sayede istemcinin/bilgisayarın adı ile DHCP den aldığı ip adresi eşleştirilir ve bilgisayar adı üzerinden bilgisayarların ip adresi çözümlenebilir.
- “Boot Options” kısmıyla cihazların DHCP sunucusundan ip bilgileri alırken aynı zamanda işletim sistemini çekeceği bir FTP/TFTP sunucu ip adresi ve bu sunucu üzerinde hangi dizinde olduğunu tanımlamak gerektiğinde kullanılan alandır.
  - o Bu bilgisayarlar network üzerinden başlatılmak istendiğinde (PXE Boot olarak biliniyor) veya ip telefonların işletim sistemini santralden çekerek başlatması gerektiğinde kullanılabilir.
- “DHCP Options” bu kısımda DHCP üzerinden istemcilere farklı kaynakların ip bilgileri de öğretmek istendiğinde kullanılan alandır. Bilindik Option Code’ların dışında özel bir Code da kullanılabilir (Bilindik /yaygın kullanılan Option Code’lar i.in <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>).
  - o Eğer ki Option Code ile belirtilen kaynağın adresi farklı bir FW üzerindeyse buradaki tanım dışında ayrıca Static Route ve Policy tanımlarının yapılması da gerekecektir

## Network

Interfaces	Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement
------------	-------	------------------	-----	------	---------------------------

### DNS server

☐ Use device's DNS settings

Primary DNS

Secondary DNS

### WINS server

Primary WINS server

Secondary WINS server

### Boot options

Enter the next-server and boot file details to provision thin clients and diskless workstations. Alternatively, specify the corresponding options under DHCP options.

Next-server

Boot file

### DHCP options

Specify the DHCP options and their values to configure DHCP clients with your network settings, such as TFTP server addresses for IP phones and NTP settings.

Options	Code	Type	Value
Time_Servers(4)	4	Array of IP addresses	192.168.200.1

Save

Cancel

DHCP Sunucusu ayağa kaldırmak yerine istemcilere harici bir kaynaktan ip aldırılmak isteniyorsa DHCP Relay konfigürasyonu için bir Relay tanımı oluşturup burada paketin hangi arayüzden geleceği (burada arayüz fiziksel bir port olabileceği gibi VLAN veya LAG gibi sanal bir arayüz de olabilir) ve gönderileceği DHCP sunucusunun ip adresi tanımlanmalıdır.

- Eğer ki DHCP sunucusu farklı bir FW üzerindeyse buradaki tanım dışında ayrıca Static Route ve Policy tanımlarının yapılması da gerekecektir.

### Add DHCP relay configuration

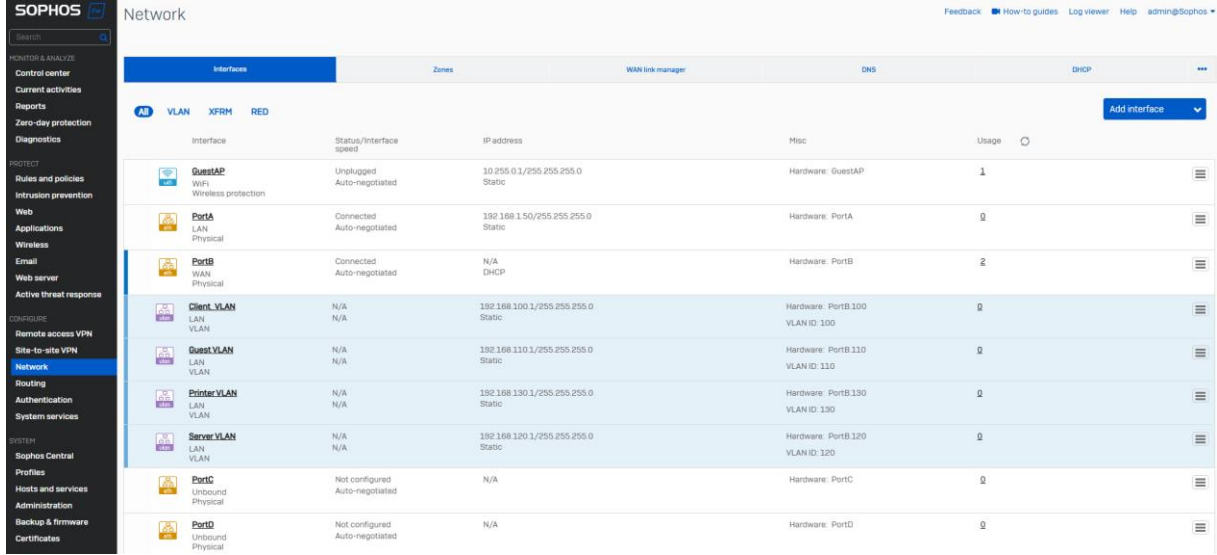
[Feedback](#) [How-to guides](#) [Log viewer](#) [Help](#) [admin@Sophos](#)

Interfaces	Zones	WAN link manager	DNS	DHCP	...
<div><div>Name *</div><div>IP version *</div><div>Interface *</div><div>DHCP server IP *</div><div>Relay through IPsec</div></div> <div><div>Guest VLAN DHCP Relay</div><div><input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6</div><div>Guest VLAN - 192.168.110.1</div><div>192.168.200.200</div><div>Search / Add</div><div><input type="checkbox"/> Enable</div></div>					

Aşağıda da görüldüğü üzere DHCP konfigürasyonu, diğer VLAN tanımları yapıldıktan sonra switch üzerinde de port tanımları yapıldıktan sonra istemcilere ip bilgilerini aldırıp FW'a erişimleri test edilmelidir (DHCP açık olmayan VLAN'lara Static olarak verilmelidir). İstemcilerin FW'a erişimleri sağlandıktan sonra artık InterVLAN Communication işlemi için Policy tanımlanmaya başlanabilir.

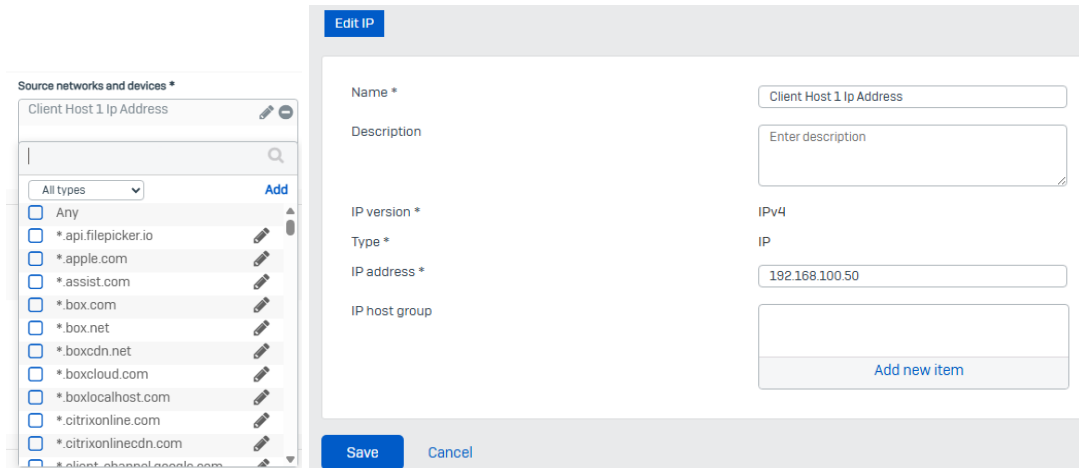


- “Log Firewall Traffic” kısmıyla bu politikayla eşleşen trafiklerin kayıt altına alınıp alınmayacağı belirleniyor.
- “Source Zone” kısmıyla trafiğin geleceği Zone tanımı yapılıyor.
  - o Bu kısım VLAN arayüzlerini oluştururken belirlenmişti. Diğer arayüzler için de “Network -> all” kısmından ilgili arayüzün içerisine bakılarak görülebilir.



Interface	Status/Interface speed	IP address	Misc	Usage
GuestAP: WiFi	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	Hardware: GuestAP	1
PortA: LAN Physical	Connected Auto-negotiated	192.168.1.50/255.255.255.0 Static	Hardware: PortA	0
PortB: WAN Physical	Connected Auto-negotiated	N/A DHCP	Hardware: PortB	2
Client VLAN: LAN VLAN	N/A N/A	192.168.100.1/255.255.255.0 Static	Hardware: PortB.100 VLAN ID: 100	0
Guest VLAN: LAN VLAN	N/A N/A	192.168.110.1/255.255.255.0 Static	Hardware: PortB.110 VLAN ID: 110	0
Printer VLAN: LAN VLAN	N/A N/A	192.168.130.1/255.255.255.0 Static	Hardware: PortB.130 VLAN ID: 130	0
Server VLAN: LAN VLAN	N/A N/A	192.168.120.1/255.255.255.0 Static	Hardware: PortB.120 VLAN ID: 120	0
PortC: Unbound Physical	Not configured Auto-negotiated	N/A	Hardware: PortC	0
PortD: Unbound Physical	Not configured Auto-negotiated	N/A	Hardware: PortD	0

- “Source Network and Devices” kısmıyla verilecek kaynak ip/network/FQDN (formatı değişebilir) adresinin belirlenmesi gerekiyor. Burada tanım bulunmuyorsa “add” kısmıyla tanım yapılabilir.
  - o Politika tanımlarında olabildiğince en sınırlı şekilde tanımlar yapılır. Burada doğrudan VLAN networkünün tamamını da haberleştirebiliriz ama bu VLAN’lar arasında sadece iki istemcinin haberleşmesi gerekiyorsa bu durumda sadece iki istemcinin erişimi için tanım yapılmalıdır.



**Edit IP**

Name \* Client Host 1 Ip Address

Description Enter description

IP version \* IPv4

Type \* IP

IP address \* 192.168.100.50

IP host group

[Add new item](#)

[Save](#) [Cancel](#)

**Source networks and devices \***

Client Host 1 Ip Address

All types

- ☐ Any
- ☐ \*.api.filepicker.io
- ☐ \*.apple.com
- ☐ \*.assist.com
- ☐ \*.box.com
- ☐ \*.box.net
- ☐ \*.boxcdn.net
- ☐ \*.boxcloud.com
- ☐ \*.boxlocalhost.com
- ☐ \*.citrixonline.com
- ☐ \*.citrixonlinecdn.com
- ☐ \*.client-channel.apple.com

- “During Schulade Time” kısmıyla politikanın hangi zaman aralıklarında devreye alınacağı belirlenebiliyor.
- “Destination Zone” kısmıyla paketlerin gönderileceği Zone tanımı yapılmalıdır.
  - o Biz VLAN arayüzlerine LAN Zone’a dâhil ettiğimiz için kaynak Zone olarak da hedef Zone olarak da LAN seçildi.
- “Destination Networks” kısmıyla paketlerin gönderileceği hedef ip/network/FQDN (formatı değişebilir) tanımlanmalıdır.

- “Services” kısmıyla kaynak ve hedef cihazların arasında hangi protokolleri kullanacağı belirtilmelidir.
  - o Bu kısım çok önemlidir. Eğer ki bilindik olmayan portlar kullanılıyorsa “add” kısmında ilgili portlar için Servis tanımları yapılarak politikaya uygulanmalıdır.
  - o Biz uygulamada sadece ping atacağımız için ayrıca servis tanımları yapılmadı.

Politika sadece trafiği başlatacak taraf için yazılmalıdır. Gönderilen pakete dönüşler için tanıma gerek yoktur ama eğer ki hedef cihaz da kaynak cihaza doğru trafik oluşturmak isterse bu durumda bu politikanın tersinin de ayrıca tanımlanması gerekecekti.

