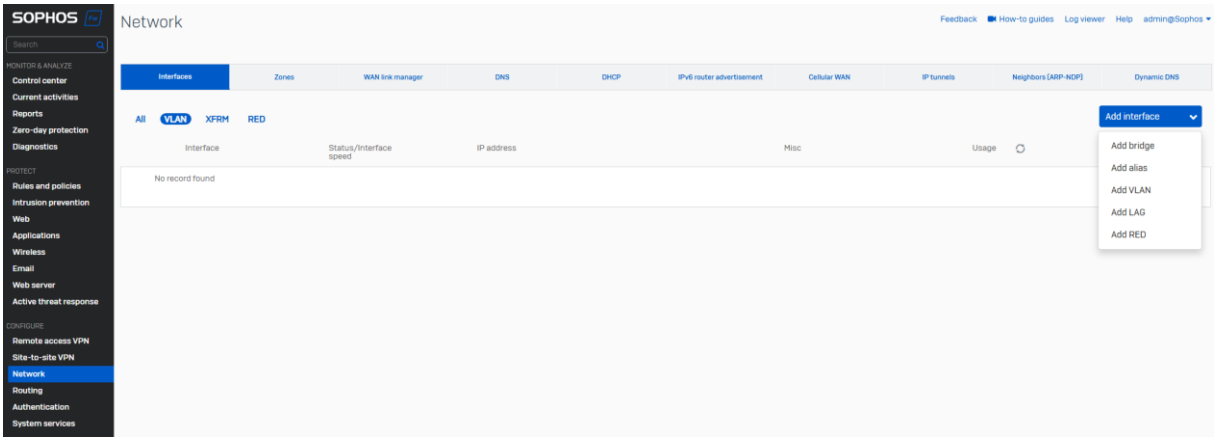
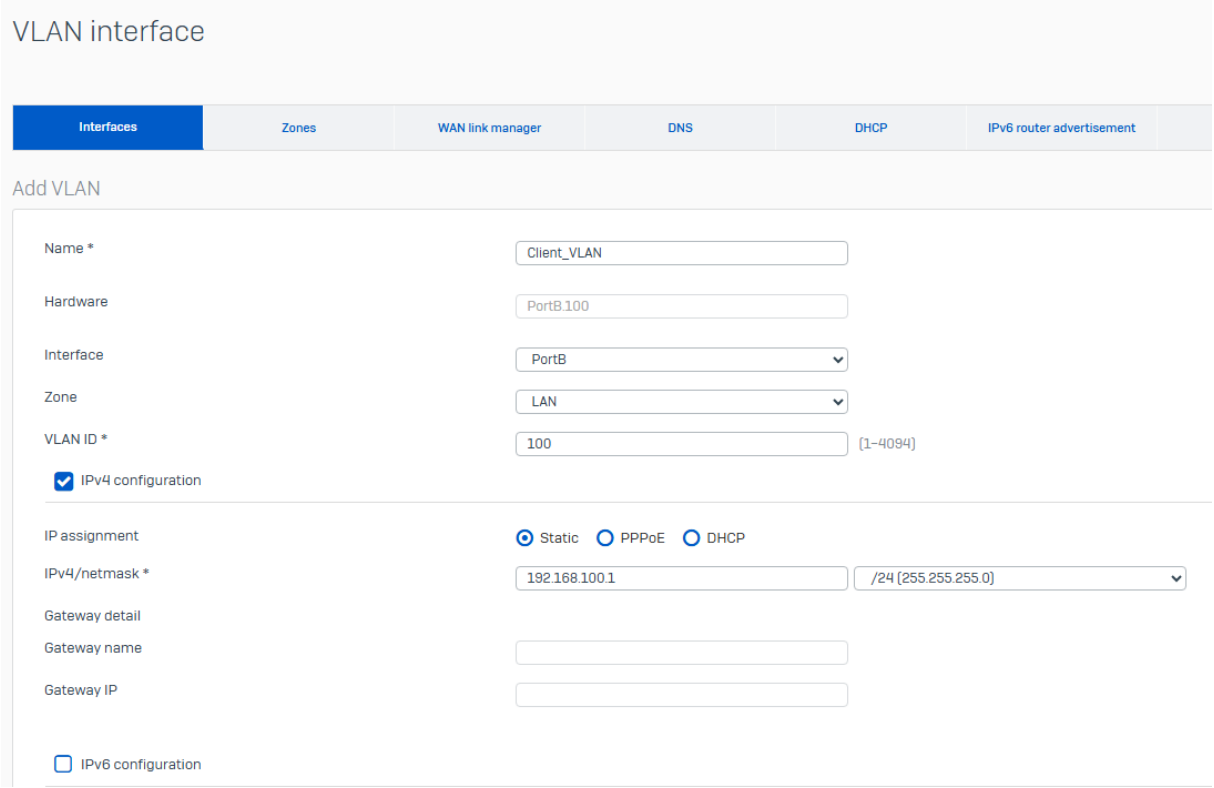
InterVLAN Comm And DHCP

InterVLAN Communication

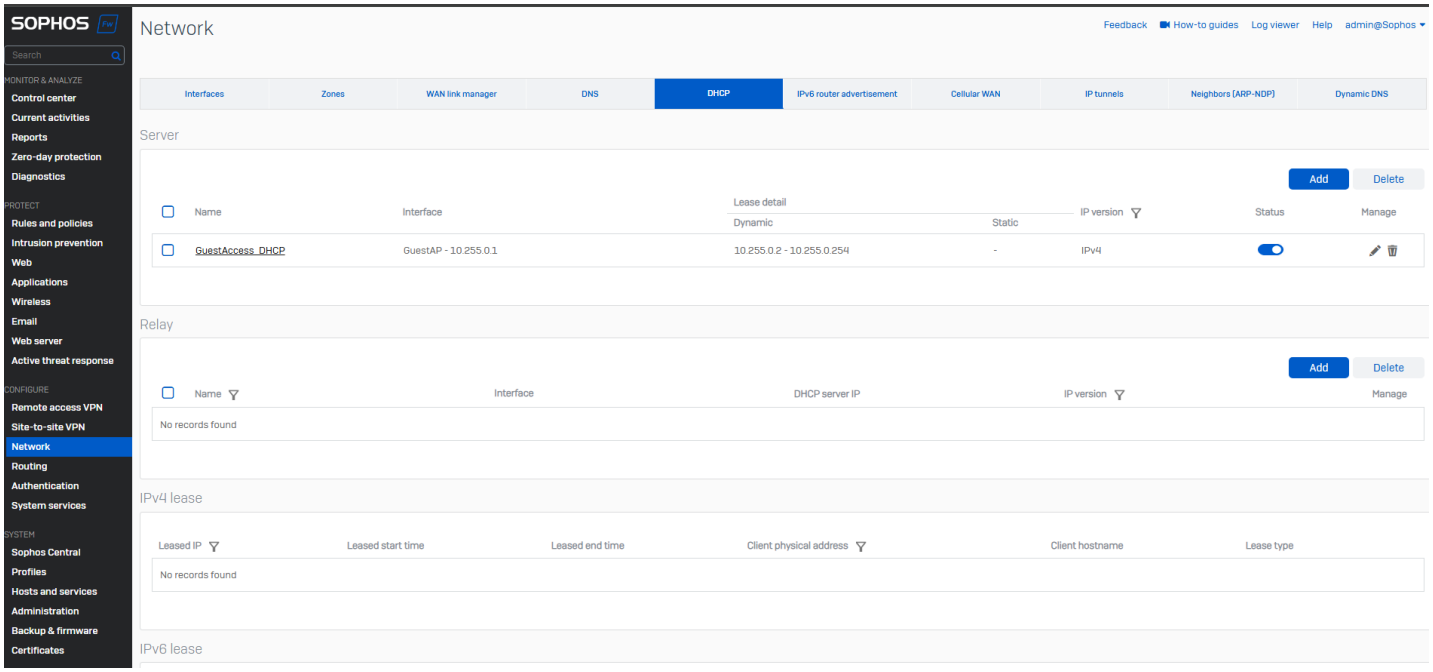
Sophos FW üzerinde InterVLAN haberleşmesi için ilk olarak VLAN tanımlarının oluşturulması gerekiyor. VLAN tanımlarını oluşturmak için “Network -> Interfaces -> VLAN -> Add Interfaces -> Add VLAN” yolu takip edilmelidir.



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 değri tanımlanmalıdır. Son olarak ilgili VLAN tanımında kullanılan ip bloğunun Gateway olarak belirlenen ip adresi tanımlanmalıdır. Bu tanımlar yapıldıktan sonra ayarların kaydedilmesi yeterli olacaktır.

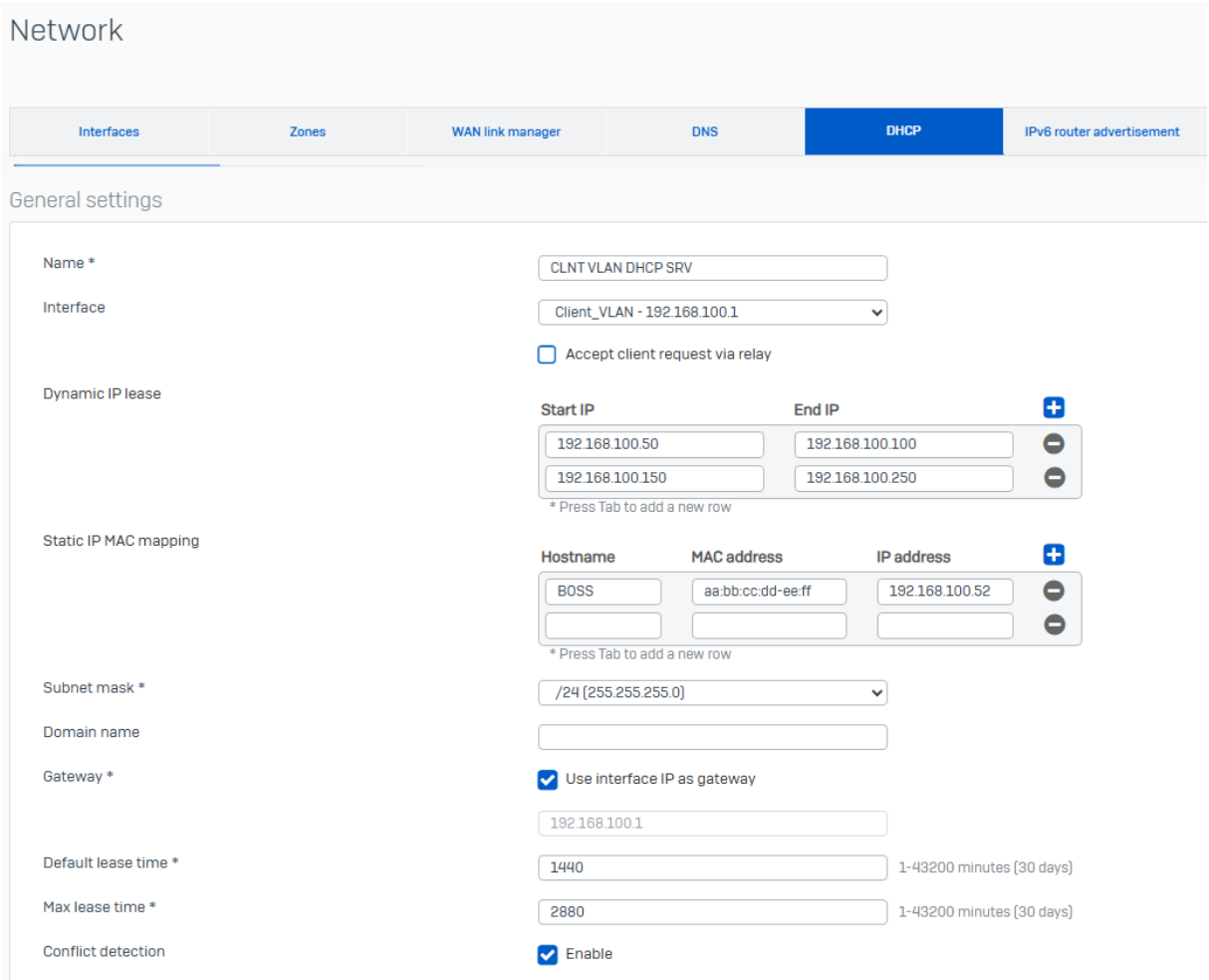


VLAN tanımı oluşturulduktan sonra bu VLAN'a bağlı istemcilerin DHCP'den ip alması isteniyorsa "Network - DHCP" yolu takip edilmelidir. Burada FW üzerinde DCP sunucusu ayağa kaldırılabileceği gibi Relay tanımı yapılarak harici bir DHCP sunucusundan ip bilgileri alınması sağlanabilir. FW üzerinde DHCP sunucusu ayağa kaldırmak için "Server -> Add -> IPv4" yolu, Relay tanımı yapmak için "Relay -> Add -> IPv4" yolu takip edilmelidir.

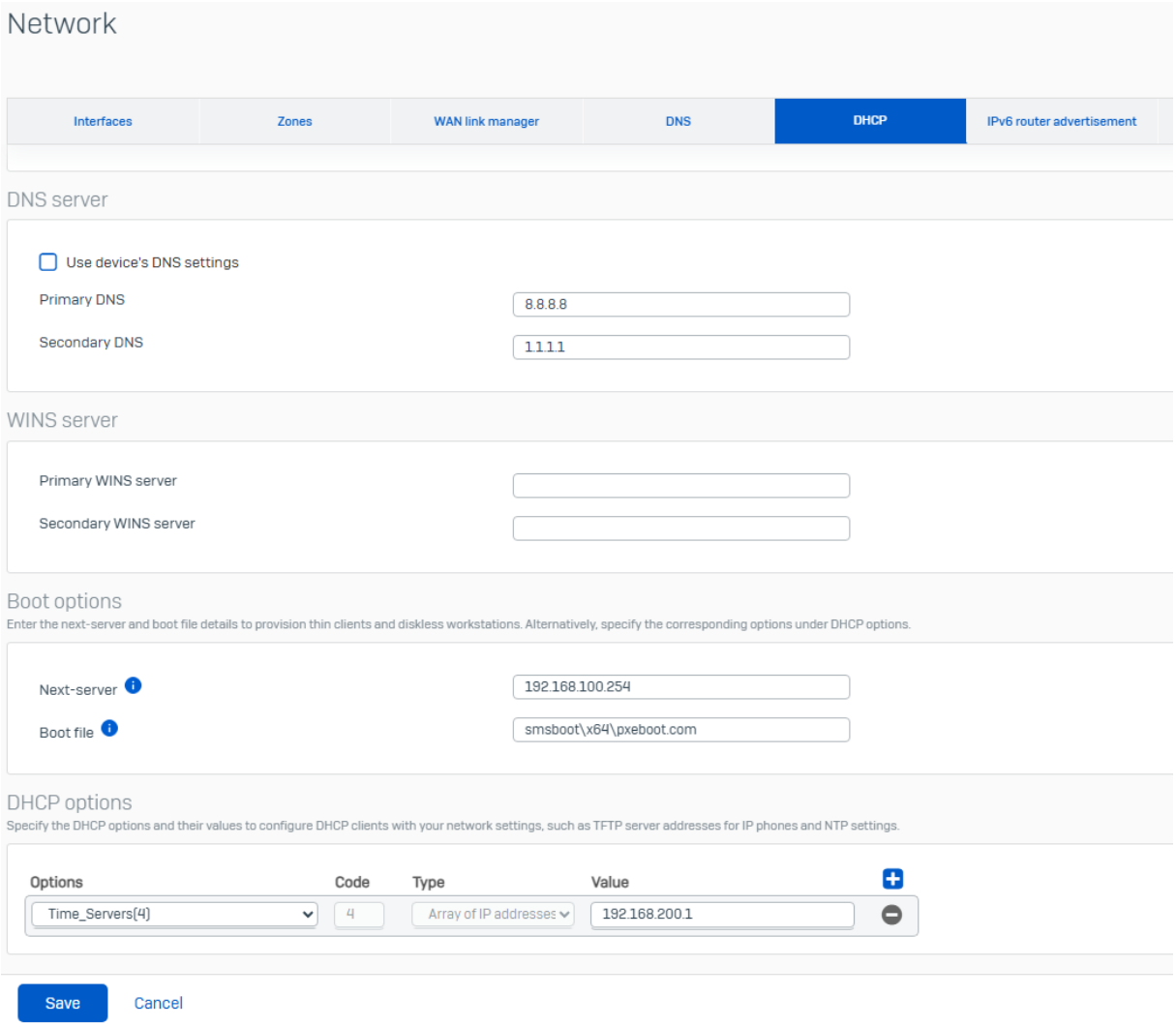


DHCP sunucusu tanımı için;

- "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.
    - Tanımın en üst kısmında ip bloğunun sonlarından bir aralık verilip, 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.
    - 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)

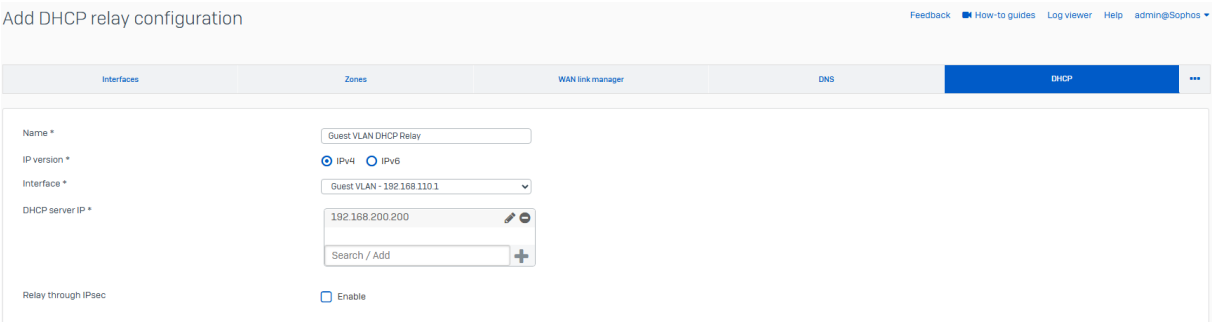


- “DNS Server” kısmıyla istemcilere verilecek DNS bilgisinin tanımlandığı kısımdır. İsteğe bağlı olarak Sophos FW üzerindeki DNS bilgisiyle aynı dağıtılması da sağlanabilir.
- “Wins Server” kısmıyla istemcilerin bilgisayar adlarının üzerinden ip adreslerinin bulunabilmesi için kullanılan NETBIOS hizmetinin 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.
    - Bu bilgisayarlar network üzerinden başlatılmak istendiğinde (PXE Boot olarak biliniyor) veya ip telefonların işletim sistemini santralden çekerek başlatması gerektiğinde kullanılabiliyor.
- “DHCP Options” bu kısımda DHCP üzzerinden istemcilere farklı kaynakların ip bilgileri de öğretilmek 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).
    - Eğer ki Option Code ile belirtilen kaynağın adresi farklı bir FW üzerindeyse buradaki tanım dışında ayrıca Static Route ve Policy tanımlarının yapılması da gerekecektir

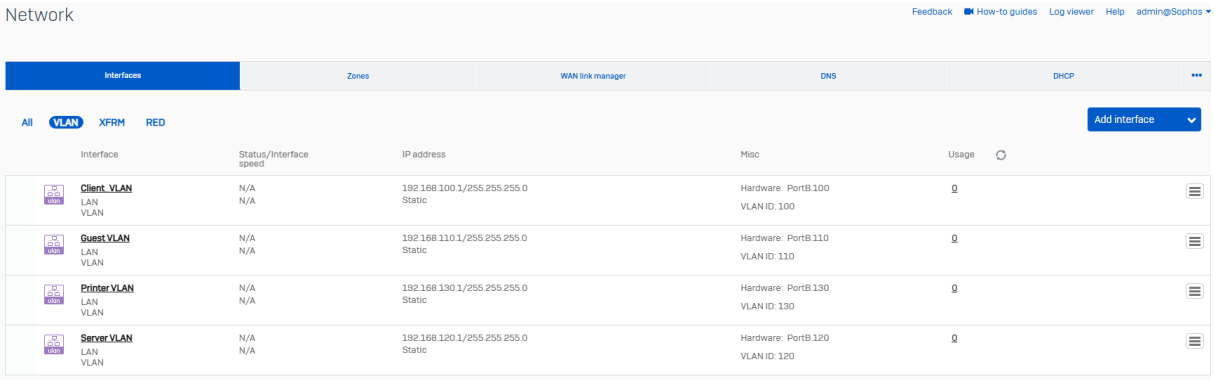


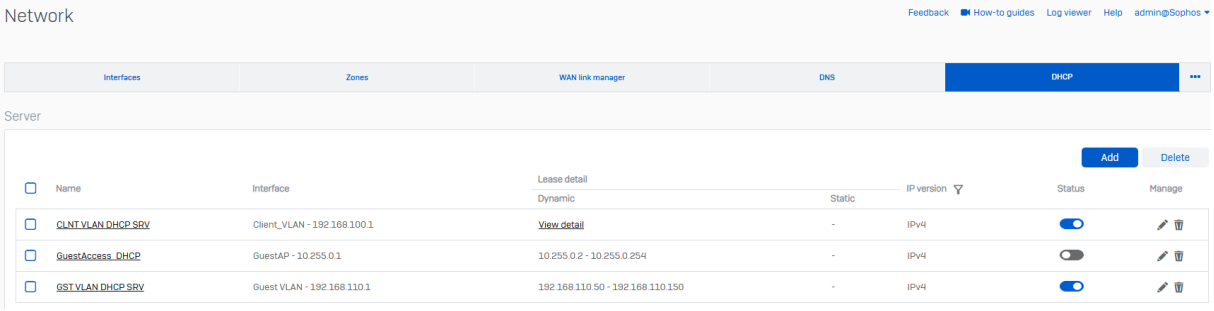
DHCP Sunucusu ayağa kaldırmak yerine istemcilere harici bir kaynaktan ip aldırılmak isteniyorsa DHCP Relay konfigürasyonu için bir Relaay tanımı oluşturup burada paketin hangi arayüzden geleceği (burada arayüz fiziksel bir port olabileceği gibi VLAN veya LAG gibi sanal bir arayüz de olabilir) ve gönderileceği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

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

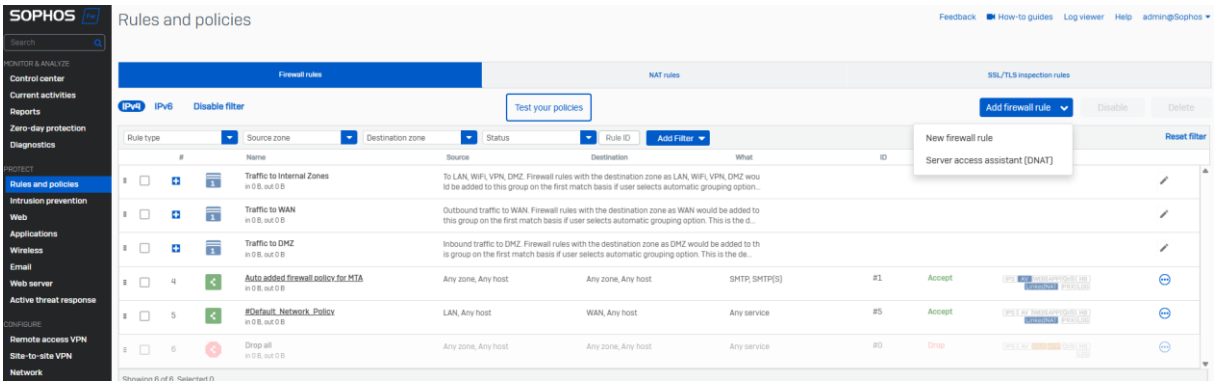


Aşağıda da görüldüğü üzere DHCP konfigürasyonu, diğer VLAN tanımları yapıldıktan sonra switch üzerinde de port tanımları yapıldıktan sonra istemcilere ip bilgilerini aldırıp FW'a erişimleri test edilmelidir (DHCP açık olmayan VLAN'lara Static olarak verilmelidir). İstemcilerin FW'a erişimleri sağlandıktan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





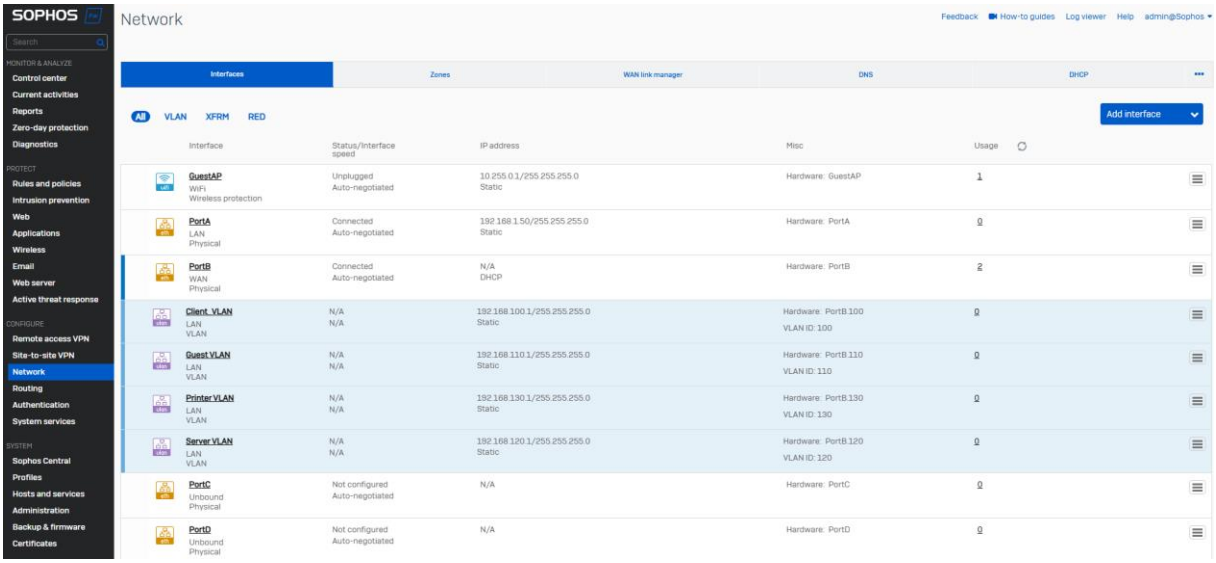
Policy tanımı için “Rules and Policies -> Firewall Rule -> IPv4 -> Add Firewall Rule -> New Firewall Rule” yolu takip edilmelidir.



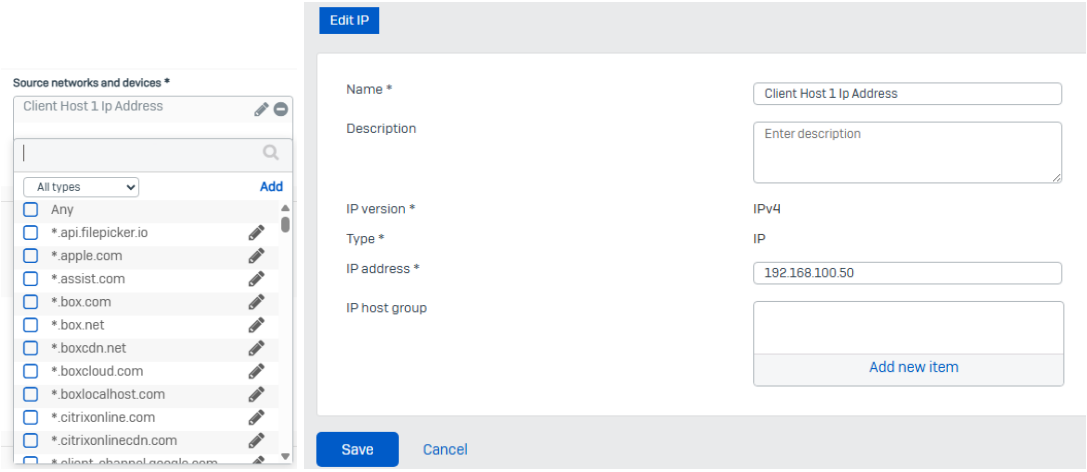
Burada herhangi bir özellik uygulamadan sadece erişim için kural yazacak olursak;

- “Rule Name” kısmıyla oluşturulacak Policy’e bir isim verilmelidir.
- “Description” kısmıyla açıklama eklenebilir. Büyük topolojilerde burasını doldurmak önemlidir. FW’a bir başkası baktığı zaman bu politikanın neden tanımlandığını anlamasında faydası olacaktır.
- “Rule Position” kısmıyla oluşturulacak politikanın diğer kurallara kıyasla en alt kısımda mı oluşturulması istendiği yoksa en yukarıda mı oluşturulmak istendiği belirlenmektedir.
    - Burada kuralın diğer kurallara kıyasla daha genel mi yoksa daha özel mi kaldığına göre karar verilmelidir. FW üzerinde trafikler politikaları yukarıdan aşağıya doğru kontrol eder ve eşleştiği ilk politikayı uygular.
    - Kural oluşturulduktan sonra politika sürüklenerek farklı konumlara taşınabiliyor.
- “Action ” kısmıyla oluşturulan kurallara uygulanacak aksiyon belirleniyor (izin ver, blokla gibi).
- “Rule Group” kısmıyla oluşturulan politikalar daha düzenli görünmesi adına gruplar oluşturulup gruplandırılabiliyor.
    - Gruplandırılan politikaların önceliği toplu olarak belirlenmiş oluyor.

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

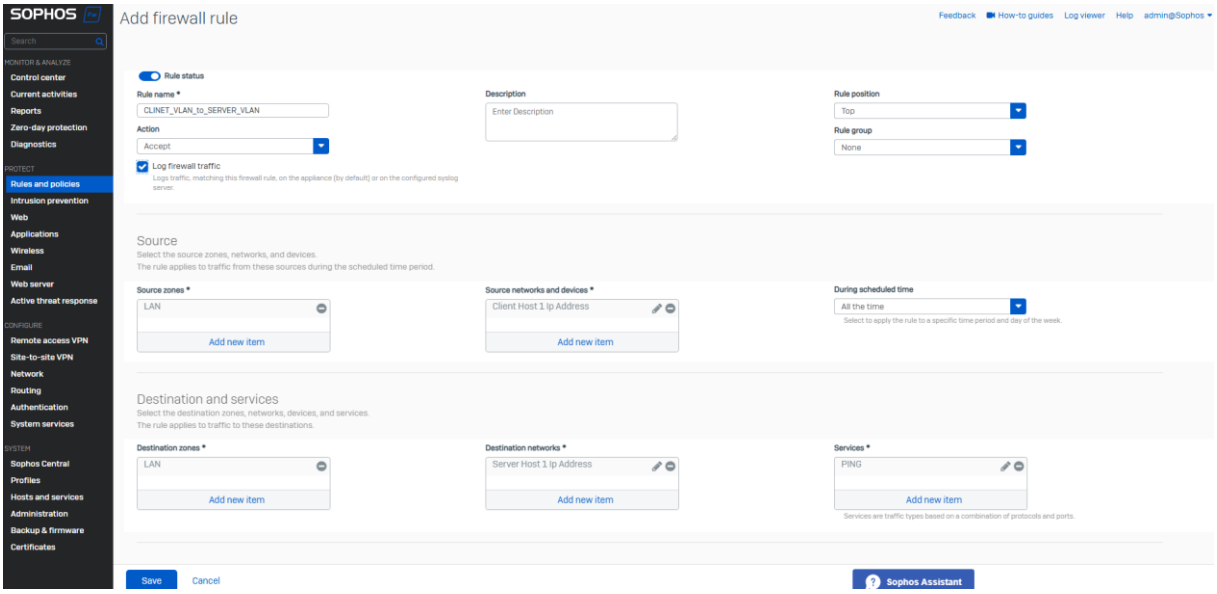
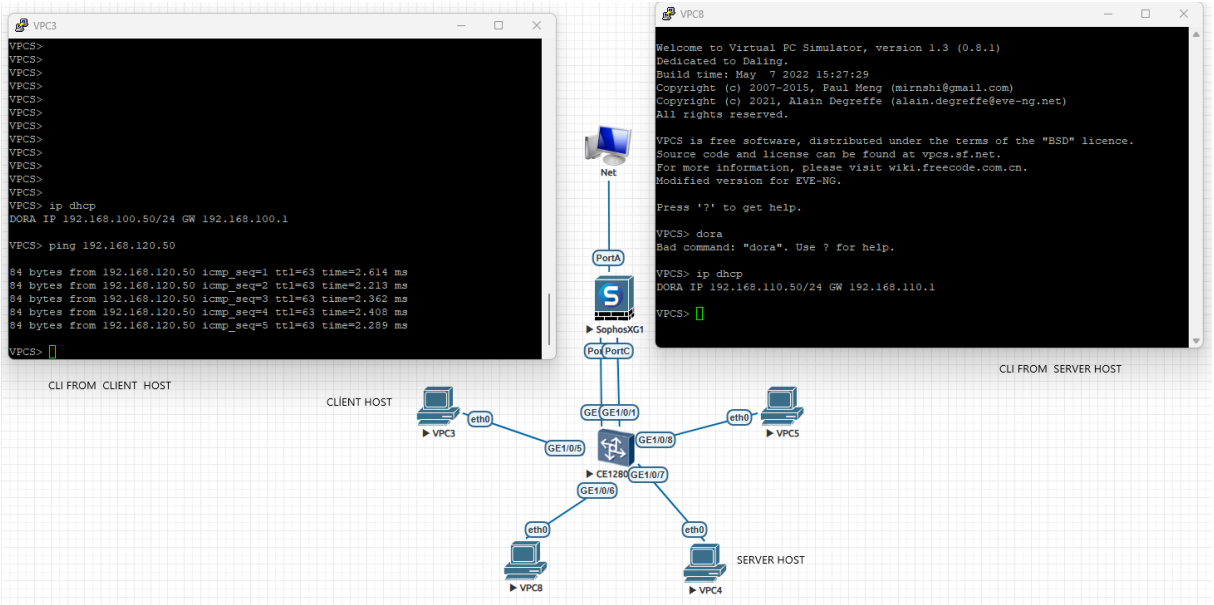


- “Source Network and Devices” kısmıyla verilecek kaynak ip/network/FQDN (formatı değişebilir) adresinin belirlenmesi gerekiyor. Burada tanım bulunmuyorsa “add” kısmıyla tanım yapılabilir.
    - Politika tanımlarında olabildiğince en sınırlı şekilde tanımlar yapılır. Burada doğrudan VLAN networkünün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



- “During Schulade Time” kısmıyla politikanın hangi zaman aralıklarında devreye alınacağı belirlenebiliyor.
- “Destination Zone” kısmıyla paketlerin gönderileceği Zone tanımı yapılmalıdır.
    - Biz VLANaraüzlerine 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.
    - Bu kısım çok önemlidir. Eğer ki bilindik olmayan portlar kullanılıyorsa “add” kısmında ilgili portlar için Servis tanımı yapılarak politikaya uygulanmalıdır.
    - Biz uygulamada sadece ping atacağımız için ayrıca servis tanımı yapılmadı.



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