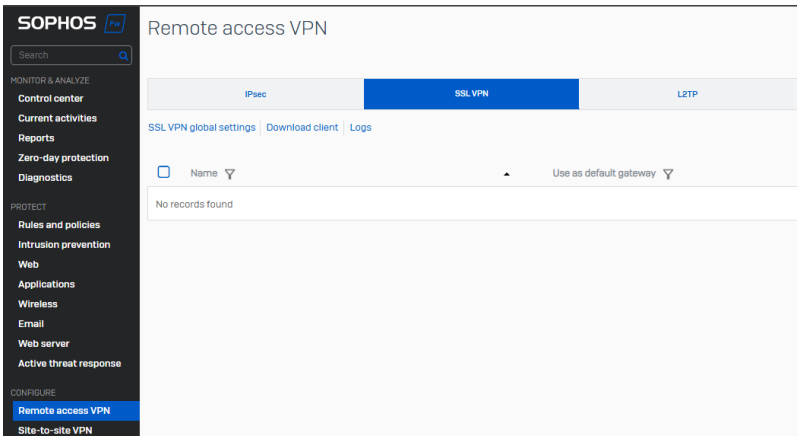
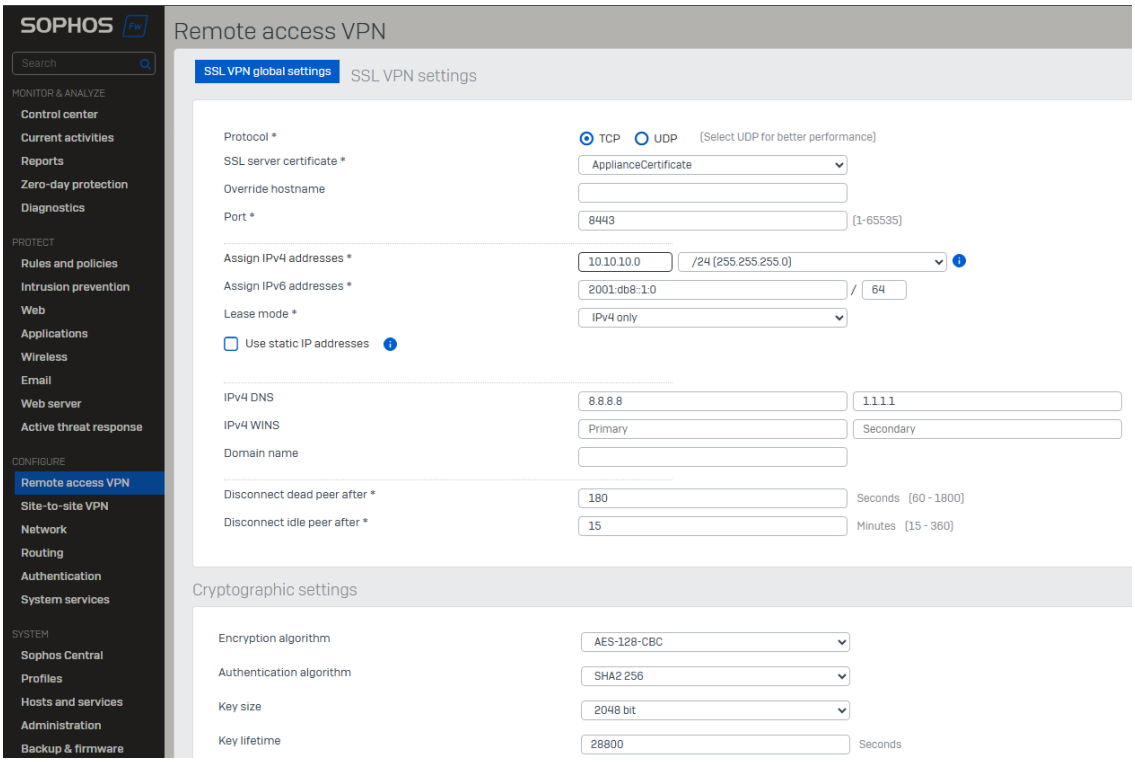
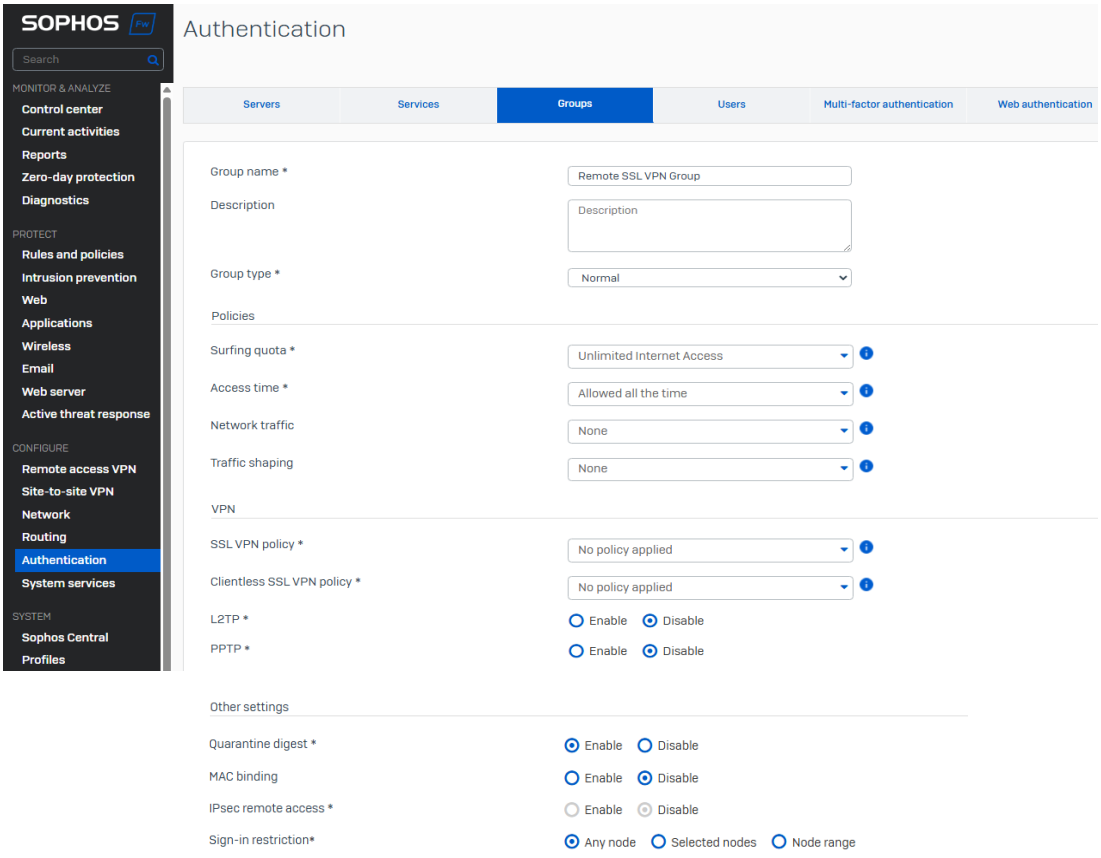
Sophos FW SSL VPN Configuration

1- Buradaki FW'a SSL VPN ile bağlanmak isteyen bütün kullanıcıların SSL olduklarında kullanacakları/alacakları ip adres aralığı/subneti "Rmote Access VPN -> SSL VPN -> SSL VPN Global Settings" kısmındaki ayarlarla belirleniyor. Bu nedenle burada verilen ip aralığını geniş tutmakta fayda var (SSL VPN üzerinden bağlanan kullanıcıların ayrımının nasıl belirlendiği yazı sonunda ayrıca açıklanmıştır). Benzer şekilde VPN olduğunda alması istenen DNS bilgisi varsa burada tanımlanıyor.

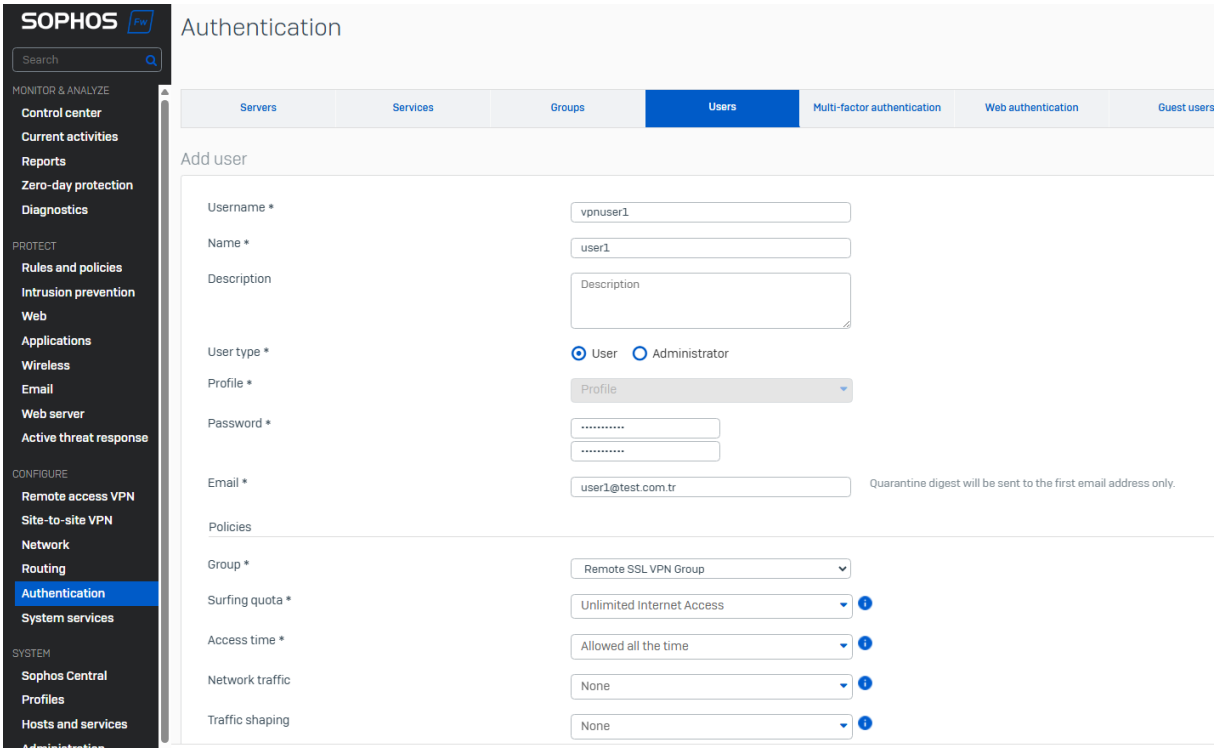




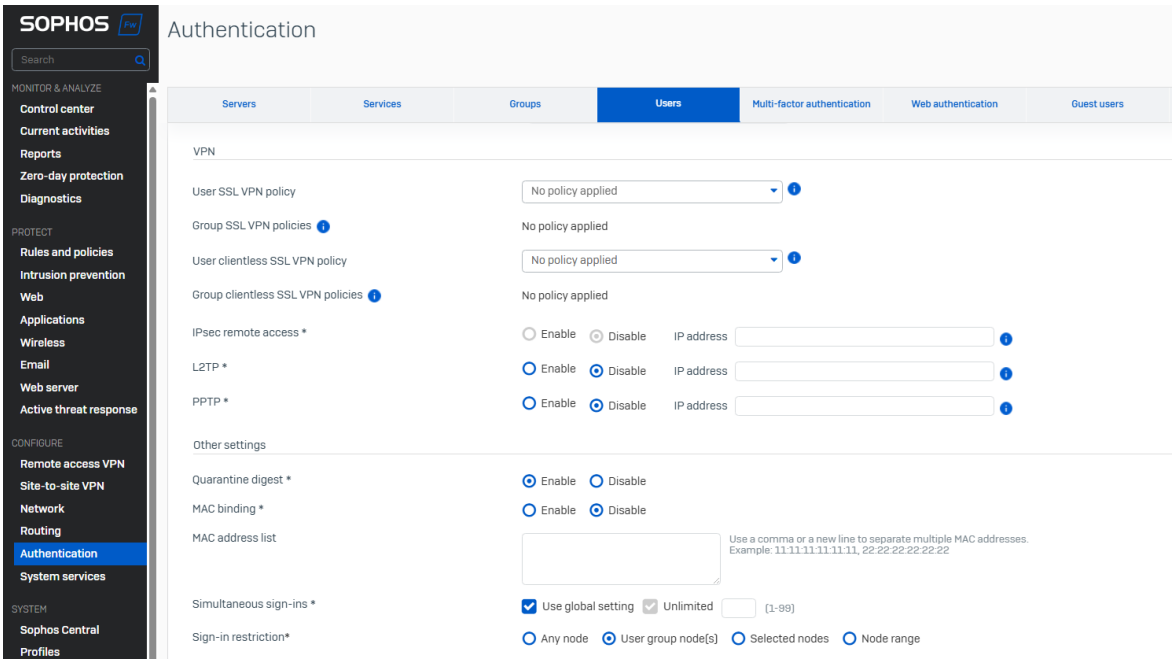
2- SSL VPN ayarları yapıldıktan sonra bir kullanıcı grubu ve bu gruba eklenmek üzere kullanıcıların oluşturulması gerekiyor. Burada Grup oluşturulmak zorunda değilsin. Bağlanacak kullanıcıları doğrudan SSL VPN için kullanılan tanımlara eklenebiliyor.
   a. İsteğe bağlı olarak gruba eklenen kullanıcılara bant genişliğinin kısıtlanması, belirli zaman dilimlerinde kullanabilmesi, Traffic Shaping gibi çeşitli politikalar uygulanabiliyor.



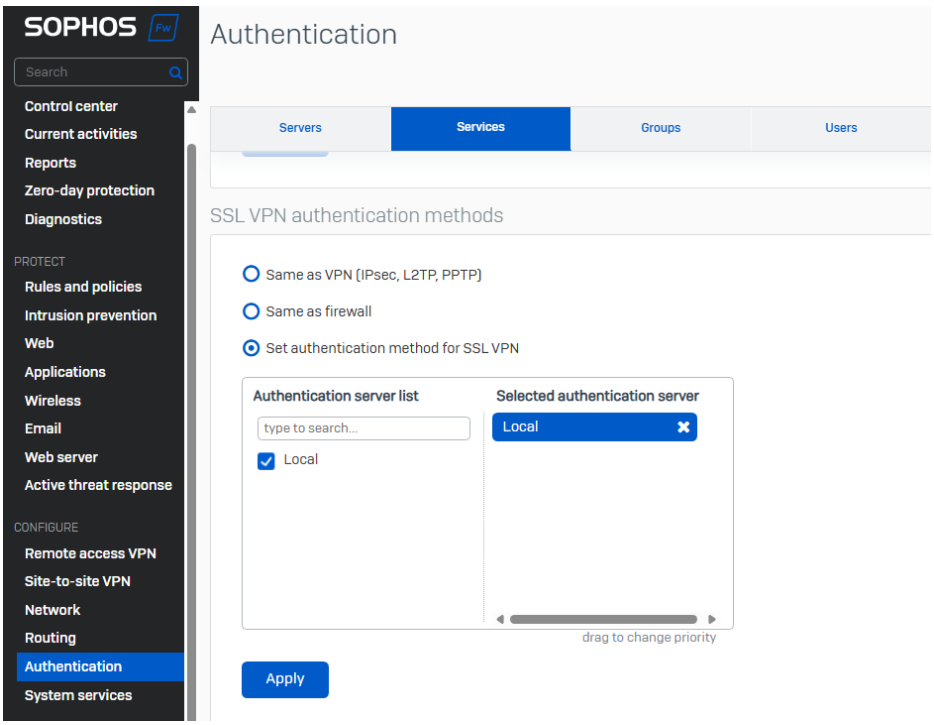
b. Kullanıcı oluştururken “Group” kısmında oluşturduğumuz SSL VPN grubunun seçtiğimizde SSL VPN grubu için tanımlı politikalar otomatik olarak kullanıcılara uygulanıyor. Bunlar dışında tanım için kullanıcı adı ve parola bilgileri yeterli olacaktır.



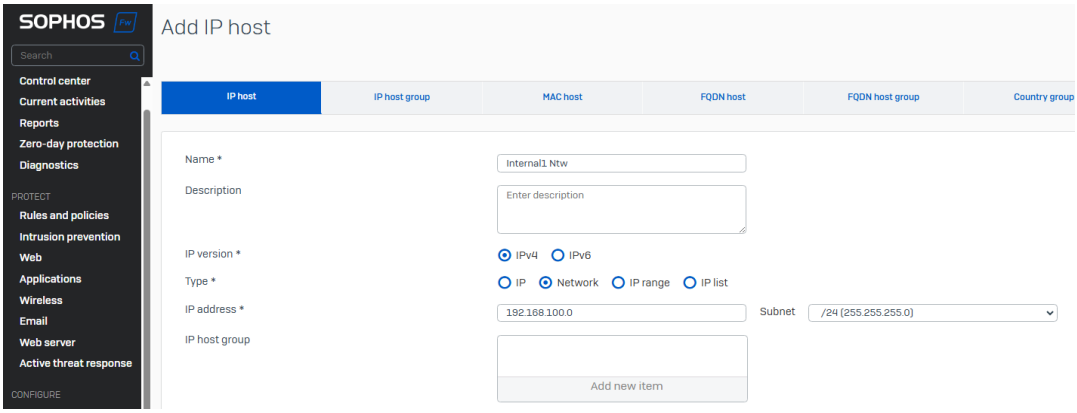
c. “Remote Access” kısmını bu kısma kadar henüz oluşturmadığımız için henüz burada seçemiyoruz ama oluşturduğumuzda buraya otomatik olarak eklenecektir. İsteğe bağlı olarak burada MAC Address List kısmıyla Trusted Host gibi sadece belirli MAC adreslerinden gelen kullanıcıların burada tanımlı kullanıcı bilgileriyle SSL VPN olması sağlanabiliyor. Benzer şekilde kullanıcı SSL olduğunda belirli ip adresini alması gerekiyorsa ip adresinin MAC adresine bağlanması sağlanabiliyor.



3- SSL VPN olacak kullanıcının kimlik denetiminin hangi kaynaktan yapılacağını tanımlamak için “Authentication -> Servers -> SSL VPN Authentication Methods” kısmında hangi kimlik denetimi kaynaklarından (LDAP,Radius, TACACS …) kullanıcıların doğrulanacağının belirlenmesi gerekiyor. Burada Sophos üzerinde tanımlı kullanıcıyla SSL VPN bağlantısı kurulması isteniyorsa burada varsayılanda gelen ”local” seçeneğinin ekli olması yeterlidir.

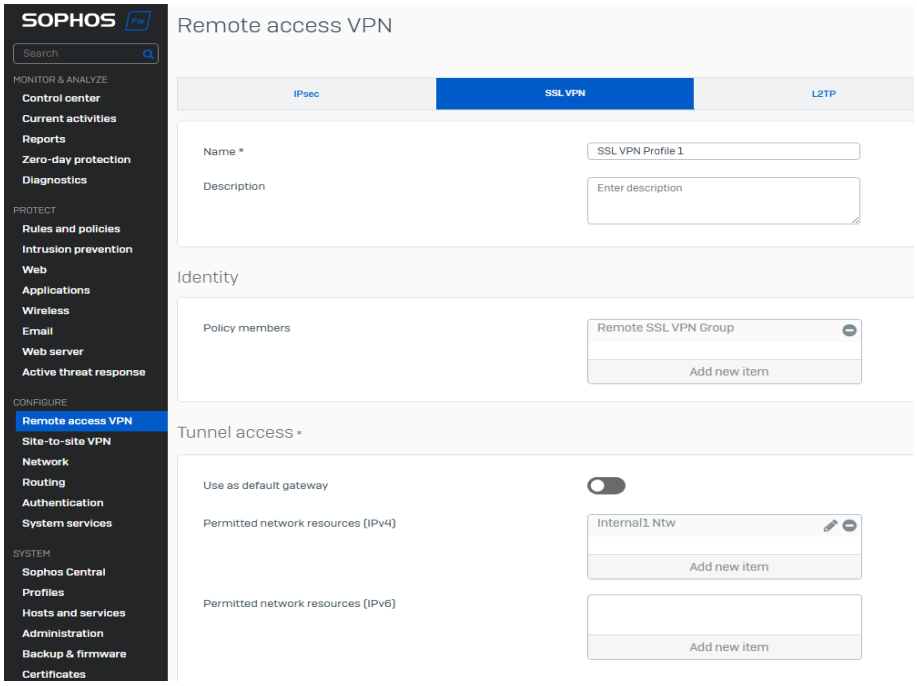


4- SSL VPN olan kullanıcıların kullanacağı ve SSL kullanıcılarının yönlendirileceği/ulaşması gereken hedef networkün “Host and Services -> IP Host” kısmında ip/subnet adres kısmında tanımlarının Politika tanımında kullanılmak üzere oluşturulması gerekiyor (Adres/subnet aralığı ilk adımda SSL VPN tanımında kullanılan ip adres aralığıyla ayı olduğuna dikkat et).

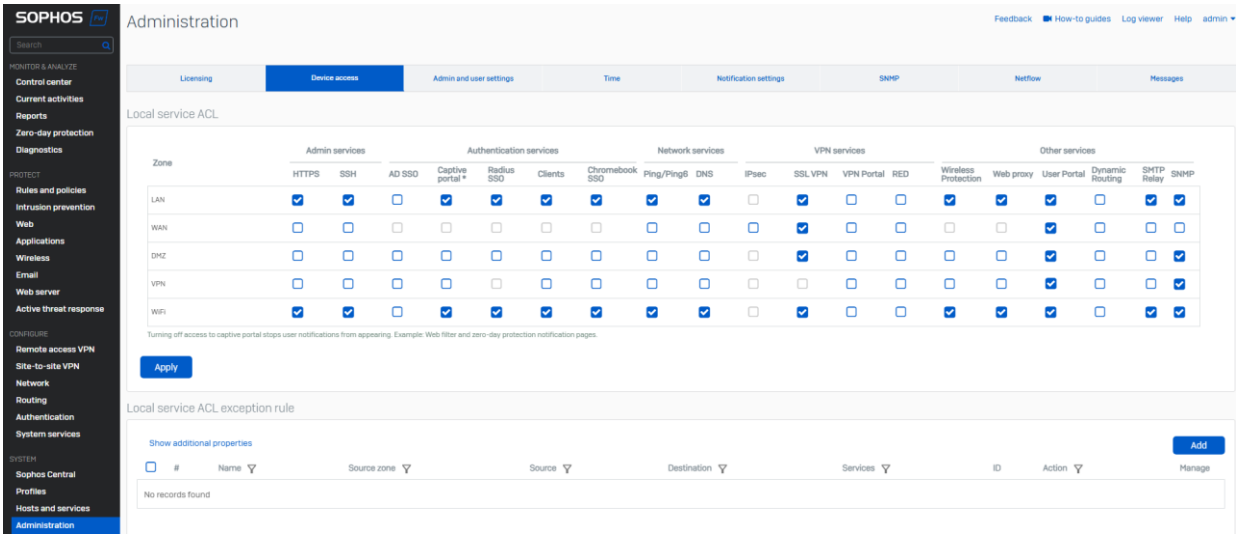


5- “Remote Access VPN -> SSL VPN” kısmından Remote SSL VPN Profile tanımının oluşturulması gerekiyor. Burada tanım yapıldığında 2. Adımda kullanıcı grubu oluşturulurken boş bırakılan “SSL VPN Policy” kısmı da otomatik olarak dolduruluyor.

   a. “Identity” kısmında oluşturulan kullanıcı grubunun eklenmesi gerekiyor. Burada doğrudan kullanıcı da eklenebiliyor.
   b. “Permited Network“ kısmı için kullanıcıların SSL olduğunda hangi networklere/ip/subnet erişeceğini belirlemek için kullanılıyor.
   c. “idle timeous” kısmında kullanıcı belirli bir süre boyunca aksiyon göstermezse ne olacağının belirlenmesi sağlanıyor.

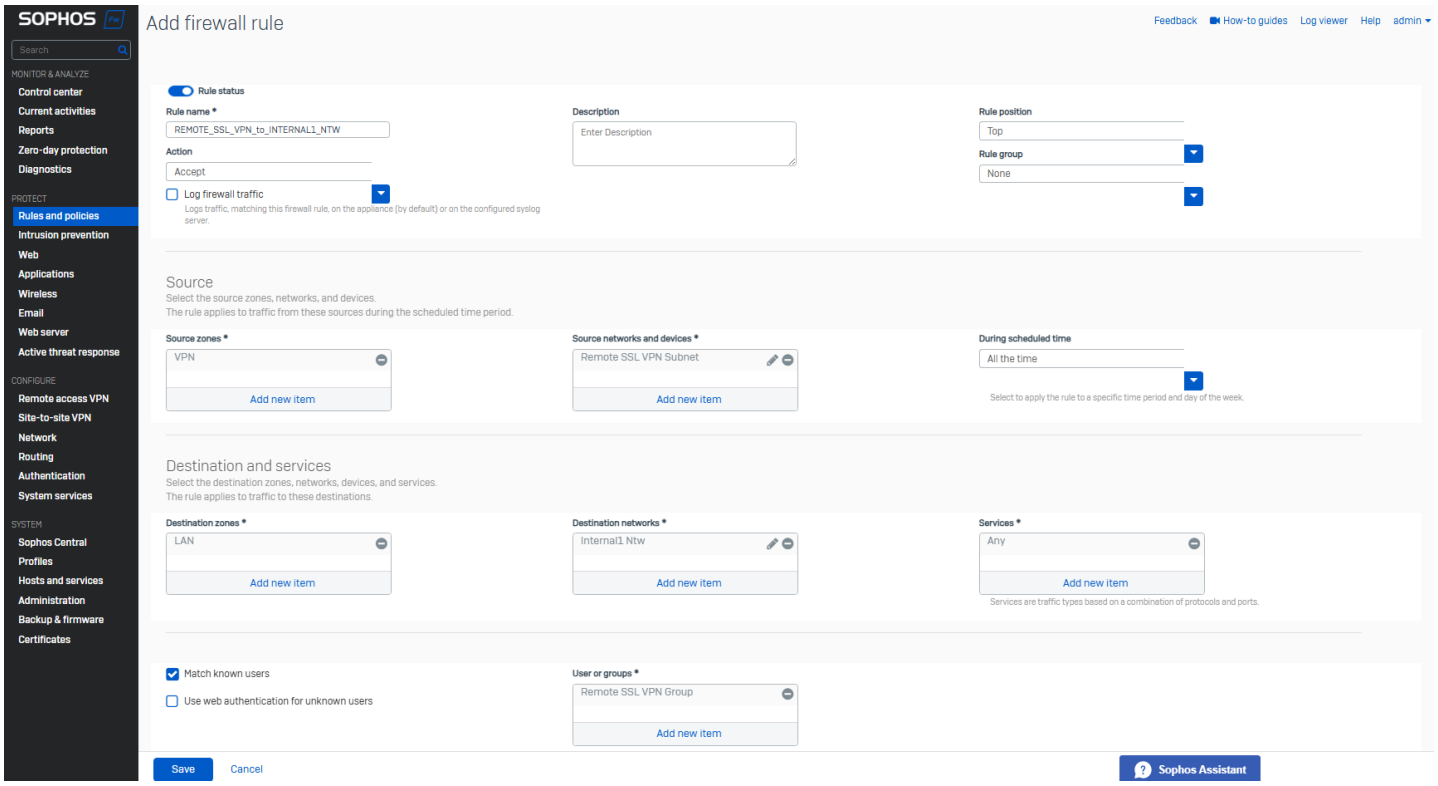


6- Bu tanımlar sonrasında “Administrators -> Device Access” kısmında cihaz üzerinde LAN, WAN ve VPN Zone’larda “SSL VPN” ve “User Portal” servislerine açık olup olmadığı kontrol edilmelidir. Bu sayede bu Zone’larda kullanıcılar hem Sophos’un SSL için oluşturacağı konfigürasyon dosyasını indireceği web arayüzüne erişim sağlayabilecek, hem de SSL VPN bağlantısını gerçekleştirebilecektir.

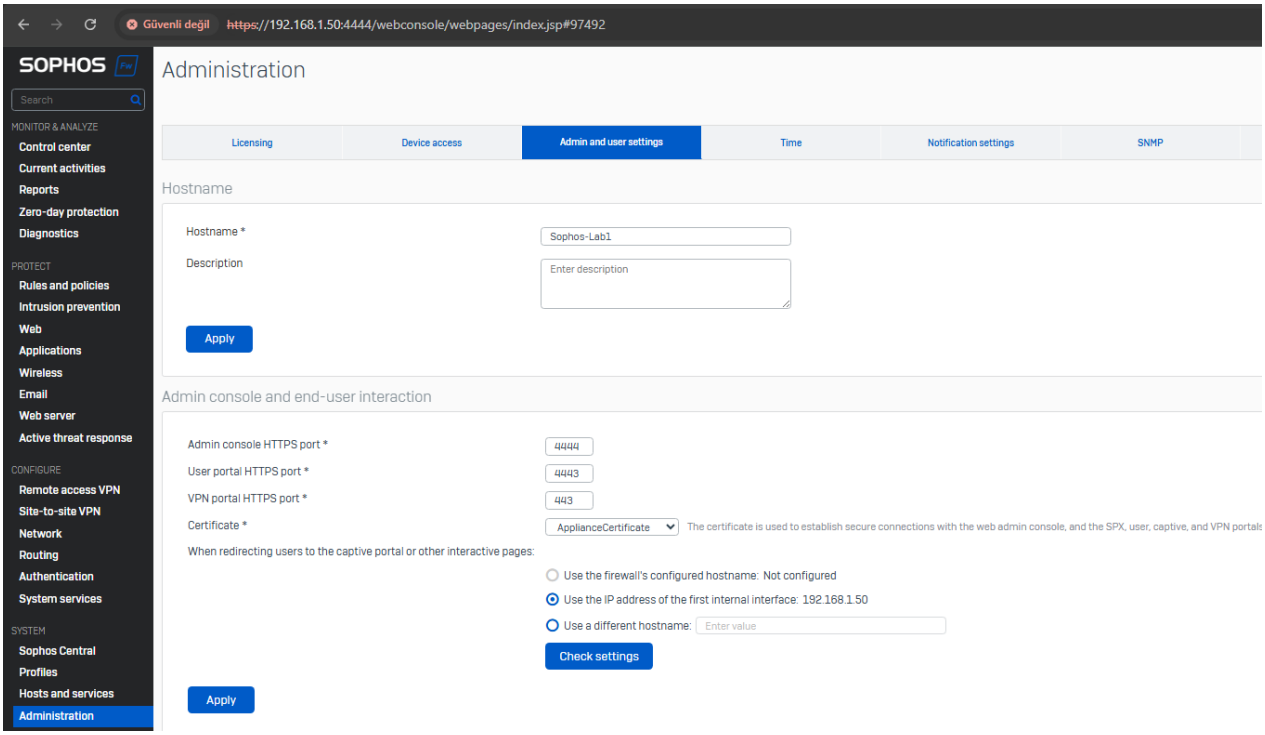


7- Servislere erişimlerin olduğu kontrol edildikten sonra “Rules and Policies -> Add” kısmında SSL kullanıcılarının bağlandıktan sonra erişmesi gereken kaynaklara bağlanabilmeleri için politika yazılması gerekiyor.

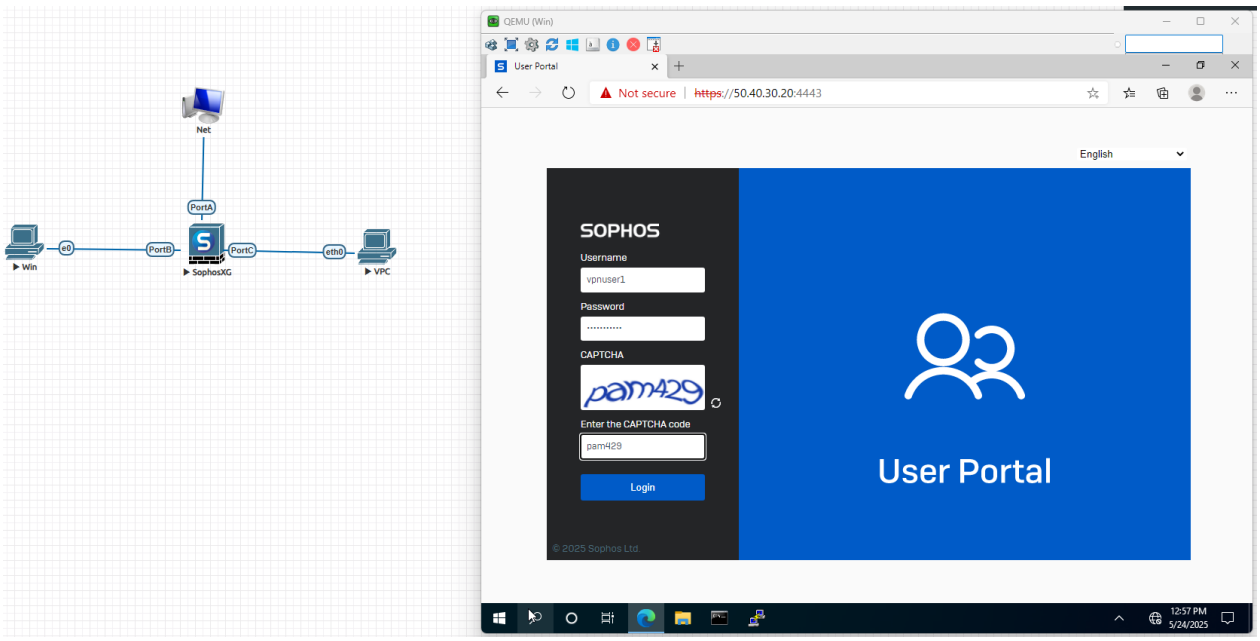
a. Source Zone : VPN
b. Source Network and Devices : <SSL VPN Kullanıcıları için oluşturulan adres tanımı eklenmeli>
c. Destination Zone : LAN <Trafiğin gönderileceği/hedef Interface/Zone seçilmelidir>
d. Destination Networks : SSL kullanıcılarının yönlendirileceği ip/subnet adresi tanımlanmalıdır.
e. Ek olarak aşağıdaki “Match Known Users” seçeneği devreye alınarak SSL VPN ile bağlanacak kullanıcılar için oluşturulan grubun eklenmesi gerekiyor (Fortigate FW’da kaynak adres kısmına doğrudan kullanıcı grubu ekleniyordu ama burada bu seçenek aracılığıyla ekleniyor).

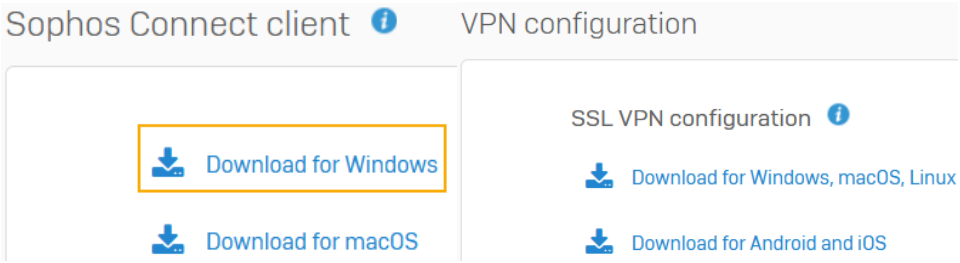


8- SSL VPN tanımları yapıldıktan sonra artık kullanıcının SSL VPN bağlantısını yapacağı Client uygulamasını indirmesini sağlayacağız. Kullanıcıların User Portal'a erişebilmesi için "Administration -> Amin Settings -> Admin Console and End User Interaction" kısmından "User PortalHTTPS port" portunu öğrenmek/gerekiyorsa değiştirmek gerekiyor. Web arayüzüne bağlanan ip adresiyle User Port bilgisi girildikten sonra kullanıcı portalı açılacaktır

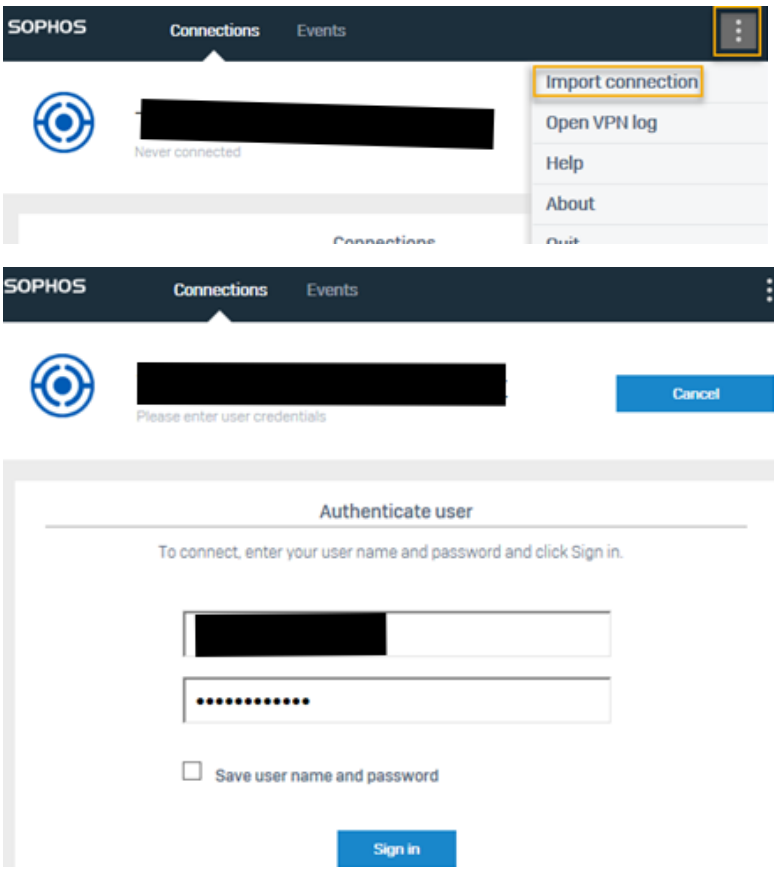


9- Kullanıcılar burada kendileri için oluşturulan kullanıcı adı ve parola bilgileriyle giriş yaptıktan sonra kullandığı cihaz türüne göre Sophos'un client uygulamasının indirilip kurulması gerekiyor. Ek olarak burada SSL VPN konfigürasyon dosyası da indirilmelidir.

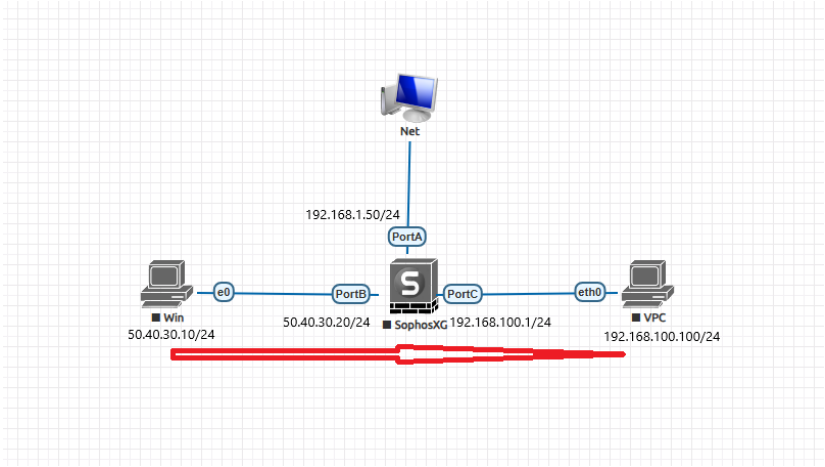




Sophos'ın Client uygulaması kurulduktan sonra açılan pencerenin sol üst köşesinde "import connection" kısmına indirilen SSL VPN konfigürasyon dosyası yüklenmelidir. Yükleme sonrasında kullanıcı adı ve parola bilgileriyle SSL VPN bağlantısı gerekleştirilebilir.



Kullanıcıların VPN olduğunu Sophos FW'un arayüzünde "Current Activites -> Lives Users" sekmesinden görüntüleyebilirsin. Topoloji kabaca aşağıdaki gibidir.



NOT:1: Eğer ki hedef network farklı bir FW üzerinde ise (Doğrudan bağlı veya VPN aracılığıyla bağlı) Static Route tanımı yapılması gerekir.

NOT:2: Anladığım kadarıyla 1. Adımda belirlediğimiz ip aralığı bütün SSL kullanıcılarının kullanımı için belirleniyor (yani Fortigate FW'da olduğu gibi her bir SSL VPN Profile tanımı için ayrı bir kaynak ip aralığının tanımlanması gerekmiyor. Bu nedenle bu aralığı geçiş tutmakta fayda var). SSL olan kullanıcılar arasında erişmeleri gereken hedef adreslerin ayrımı hem kullanıcı grubuna uygulanan SSL VPN Policy kısmıyla hem de Rules and Policies kısmında yazılan politika kısmında belirleniyor. Yani özetle bir kullanıcı X1 (192.168.10.0/24, 172.16.5.0/24 gibi birkaç subnet ve ip grubu olarak düşünelim) adreslerine erişmek istiyorsa;

- X1 adreslerini tanımlamak üzere 5. Adımda uygulanan "Remote Access VPN -> SSL VPN" sekmesinde bir tane Profile tanımı oluşturulması gerekiyor ve burada X1 adreslerini kullanacak kullanıcı grubu da ekleniyor.
- X1 adresleri için Rules and Policies sekmesinde bir politika yazıp burada da X1 adreslerini kullanacak kullanıcı grubu ekleniyor.

Kaynaklar:

- https[:]//www.youtube.com/watch?v=me0zd4TI_4E
- https[:]//docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/VPN/RemoteAccessVPN/VPNRemoteAccessSSLVPNSophosConnectClient/index.html#install-and-configure-sophos-connect-client-on-endpoints