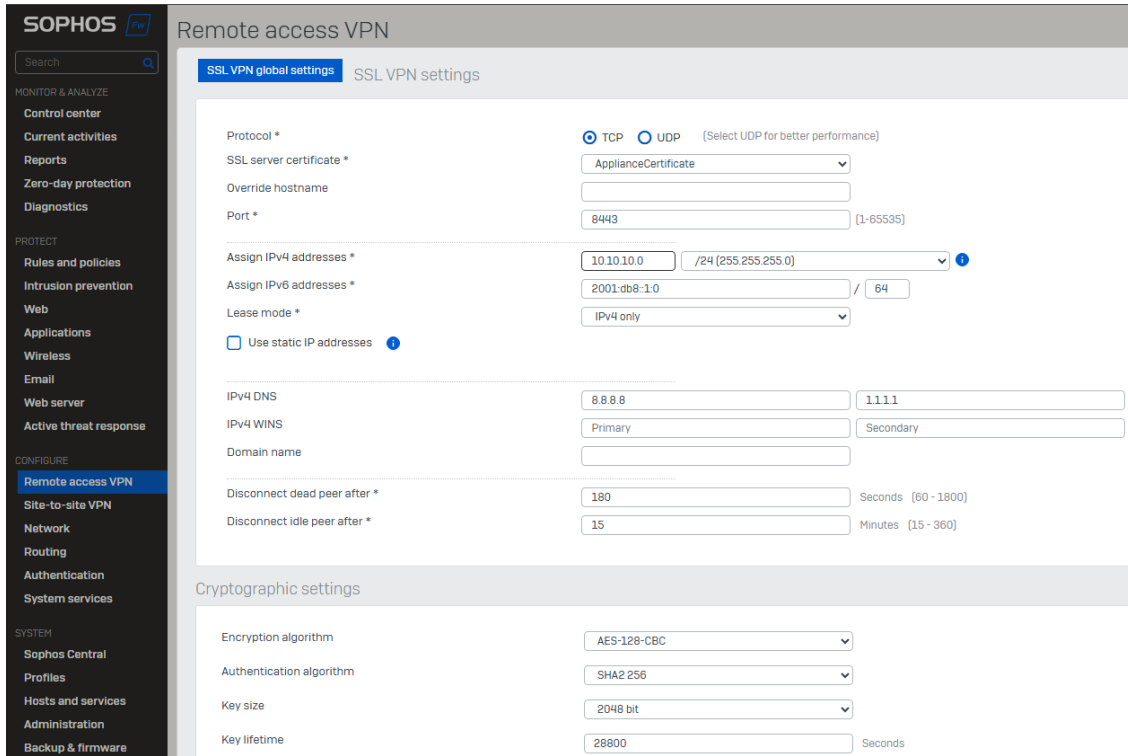
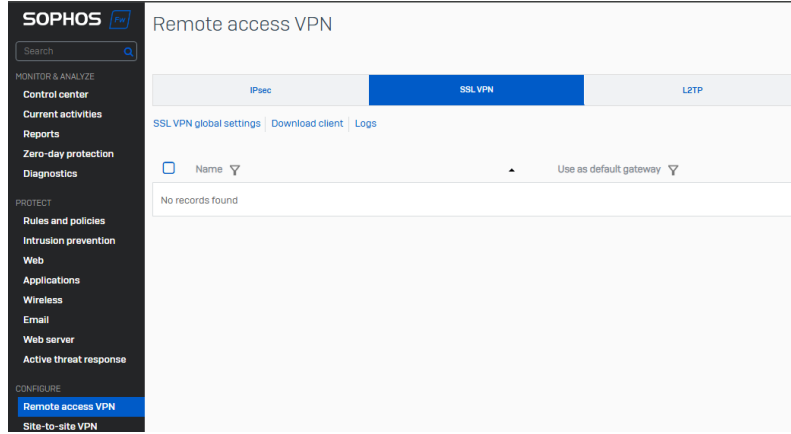


Sophos FW SSL VPN Configuration

- 1- Buradaki FW'ya SSL VPN ile bağlanmak isteyen bütün kullanıcıların SSL olduklarında kullanacakları/alacakları ip adres aralığı/subneti "Remote 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.

SOPHOS

Search

Q

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

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Authentication

Servers

Services

Groups

Users

Multi-factor authentication

Web authentication

Guest users

Add user

Username *

vpnuser1

Name *

user1

Description

Description

User type *

User

Administrator

Profile *

Profile

Password *

Email *

user1@test.com.tr

Quarantine digest will be sent to the first email address only.

Policies

Group *

Remote SSL VPN Group

Surfing quota *

Unlimited Internet Access

Access time *

Allowed all the time

Network traffic

None

Traffic shaping

None

- 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.

The screenshot shows the Sophos Firewall web interface, specifically the Authentication page under the Users tab. The left sidebar contains navigation menus for Monitor & Analyze, Protect, Configure, and System. The main content area is titled 'Authentication' and has tabs for Servers, Services, Groups, Users, Multi-factor authentication, Web authentication, and Guest users. The Users tab is active, showing a list of users with columns for Name, Status, and Actions. Below the list, there are sections for 'VPN' and 'Other settings'. The 'VPN' section includes settings for User SSL VPN policy, Group SSL VPN policies, User clientless SSL VPN policy, Group clientless SSL VPN policies, IPsec remote access, L2TP, and PPTP. The 'Other settings' section includes Quarantine digest, MAC binding, MAC address list, Simultaneous sign-ins, and Sign-in restriction.

- 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 doğrulanacağını belirlenmesi gerekiyor. Burada Sophos üzerinde tanımlı kullanıcıyla SSL VPN bağlantısı kurulması isteniyorsa burada varsayılanda gelen “local” seçeneğinin ekli olması yeterlidir.

The screenshot shows the Sophos Firewall web interface, specifically the Authentication page under the Services tab. The left sidebar is the same as the previous screenshot. The main content area is titled 'Authentication' and has tabs for Servers, Services, Groups, and Users. The Services tab is active, showing a list of services with columns for Name, Status, and Actions. Below the list, there is a section for 'SSL VPN authentication methods'. This section has three radio buttons: 'Same as VPN (IPsec, L2TP, PPTP)', 'Same as firewall', and 'Set authentication method for SSL VPN'. The 'Set authentication method for SSL VPN' option is selected. Below this, there is a section for 'Authentication server list' and 'Selected authentication server'. The 'Authentication server list' shows a search bar and a list of servers, with 'Local' selected. The 'Selected authentication server' shows 'Local' as the selected server. There is an 'Apply' button at the bottom.

- 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 aynı olduğuna dikkat et).

The screenshot shows the 'Add IP host' configuration page in the Sophos Firewall interface. The left sidebar contains navigation options like 'Control center', 'Current activities', 'Reports', 'Zero-day protection', 'Diagnostics', 'PROTECT', 'Rules and policies', 'Intrusion prevention', 'Web', 'Applications', 'Wireless', 'Email', 'Web server', 'Active threat response', and 'CONFIGURE'. The main area has tabs for 'IP host', 'IP host group', 'MAC host', 'FQDN host', 'FQDN host group', and 'Country group'. The 'IP host' tab is active. Fields include: Name (Internal1 Ntw), Description (Enter description), IP version (IPv4 selected, IPv6 unselected), Type (IP unselected, Network selected, IP range unselected, IP list unselected), IP address (192.168.100.0), Subnet (/24 (255.255.255.0)), and IP host group (Add new item button).

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

The screenshot shows the 'Remote access VPN' configuration page in the Sophos Firewall interface. The left sidebar is the same as the previous screenshot. The main area has tabs for 'IPsec', 'SSL VPN', and 'L2TP'. The 'SSL VPN' tab is active. Fields include: Name (SSL VPN Profile 1), Description (Enter description), Identity (Policy members: Remote SSL VPN Group), Tunnel access (Use as default gateway: off), Permitted network resources (IPv4: Internal1 Ntw), and Permitted network resources (IPv6: Add new item button).

- 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.

SOPHOS Administration

Feedback How-to guides Log viewer Help admin

Search

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

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Administration

Licensing Device access Admin and user settings Time Notification settings SNMP Netflow Messages

Local service ACL

Zone	Admin services		Authentication services			Network services			VPN services			Other services							
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Clients	Chromebook SSO	Ping/Ping6	DNS	IPsec	SSL VPN	VPN Portal	RED	Wireless Protection	Web proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WFI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Turning off access to captive portal stops user notifications from appearing. Example: Web filter and zero-day protection notification pages.

Apply

Local service ACL exception rule

Show additional properties

#	Name	Source zone	Source	Destination	Services	ID	Action	Manage
No records found								

Add

- 7- Servislere erişimlerin olduğu kontrol edildikten sonra “Rules and Policies -> Add” kısmında SSL kullanıcılarının bağlandıktan sonra erişmesi gereken kaynaklara bağlanabilmeleri için politika yazılması gerekiyor.
- Source Zone : VPN
 - Source Network and Devices : <SSL VPN Kullanıcıları için oluşturulan adres tanımı eklenmeli>
 - Destination Zone : LAN <Trafiğin gönderileceği/hedef Interface/Zone seçilmelidir>
 - Destination Networks : SSL kullanıcılarının yönlendirileceği ip/subnet adresi tanımlanmalıdır.
 - 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).

SOPHOS Add firewall rule

Feedback How-to guides Log viewer Help admin

Search

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

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Add firewall rule

Rule status

Rule name * REMOTE_SSL_VPN_to_INTERNAL1_NTW

Action Accept

Log firewall traffic

Description Enter Description

Rule position Top

Rule group None

Source

Select the source zones, networks, and devices. The rule applies to traffic from these sources during the scheduled time period.

Source zones * VPN

Source networks and devices * Remote SSL VPN Subnet

During scheduled time All the time

Destination and services

Select the destination zones, networks, devices, and services. The rule applies to traffic to these destinations.

Destination zones * LAN

Destination networks * Internal1 Ntw

Services * Any

Match known users

User or groups * Remote SSL VPN Group

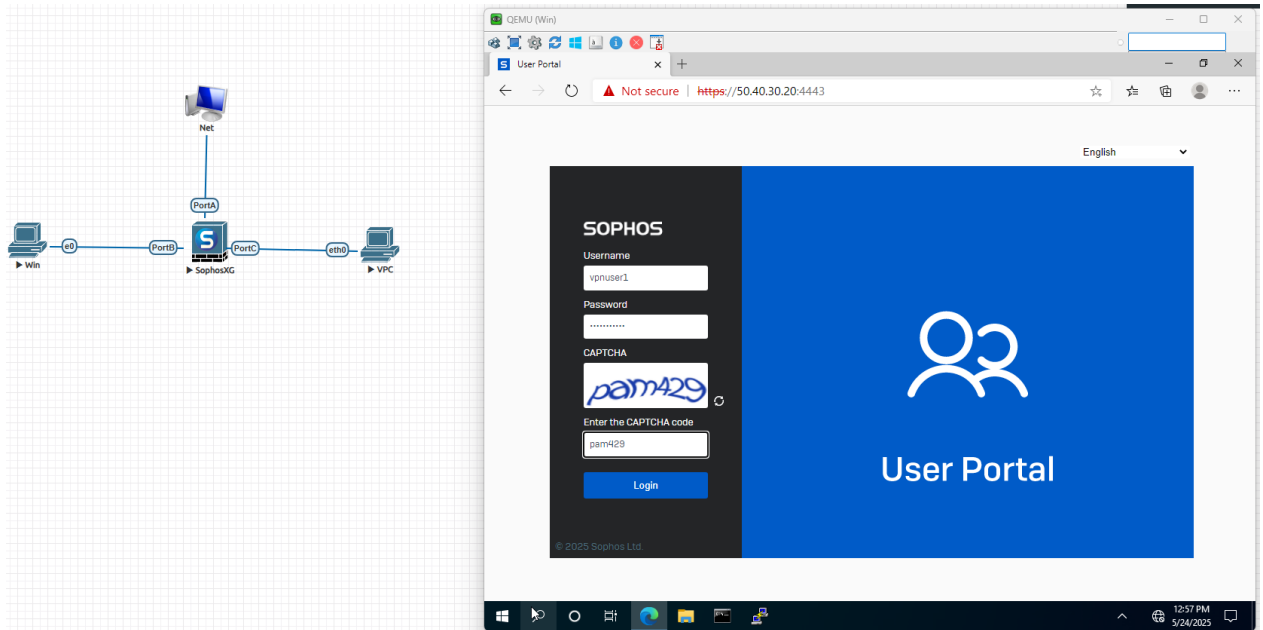
Save Cancel

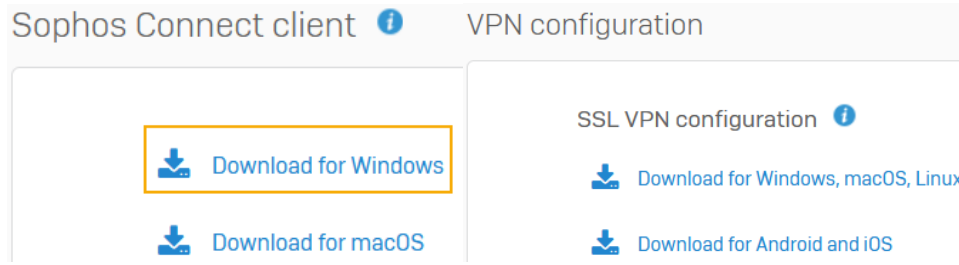
Sophos Assistant

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

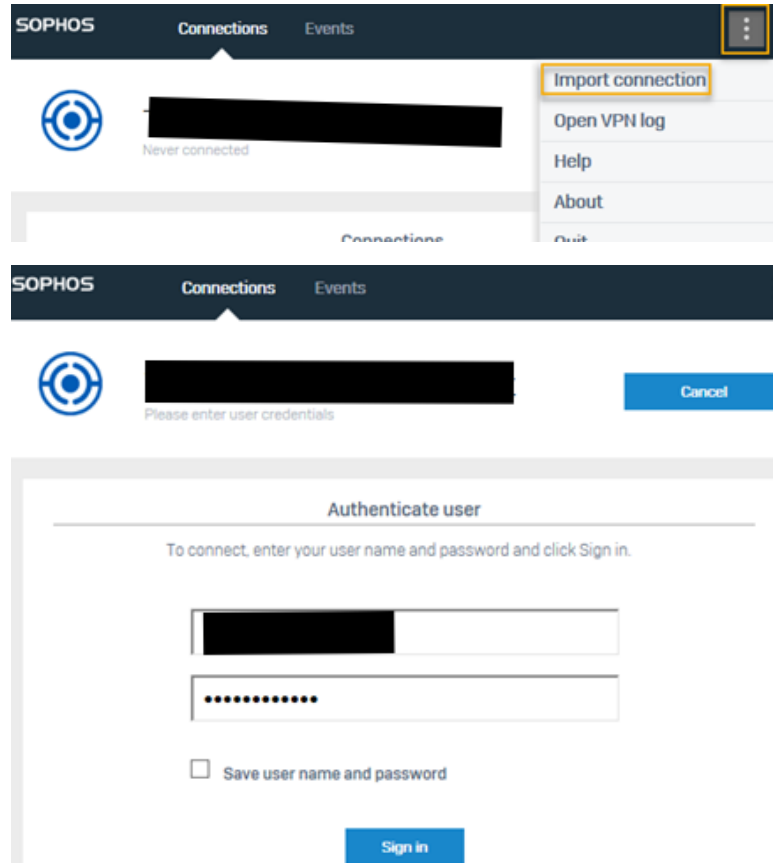
The screenshot shows the Sophos Administration web console. The left sidebar contains navigation options under 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area is titled 'Administration' and has tabs for 'Licensing', 'Device access', 'Admin and user settings' (selected), 'Time', 'Notification settings', and 'SNMP'. Under 'Admin and user settings', the 'Admin console and end-user interaction' section is expanded. It shows fields for 'Admin console HTTPS port *' (4444), 'User portal HTTPS port *' (4443), and 'VPN portal HTTPS port *' (443). A dropdown menu for 'Certificate *' is set to 'ApplianceCertificate'. Below these, there are radio buttons for 'When redirecting users to the captive portal or other interactive pages': 'Use the firewall's configured hostname: Not configured' (selected), 'Use the IP address of the first internal interface: 192.168.1.50', and 'Use a different hostname: Enter value'. An 'Apply' button is at the bottom left, and a 'Check settings' button is at the bottom right.

- 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.

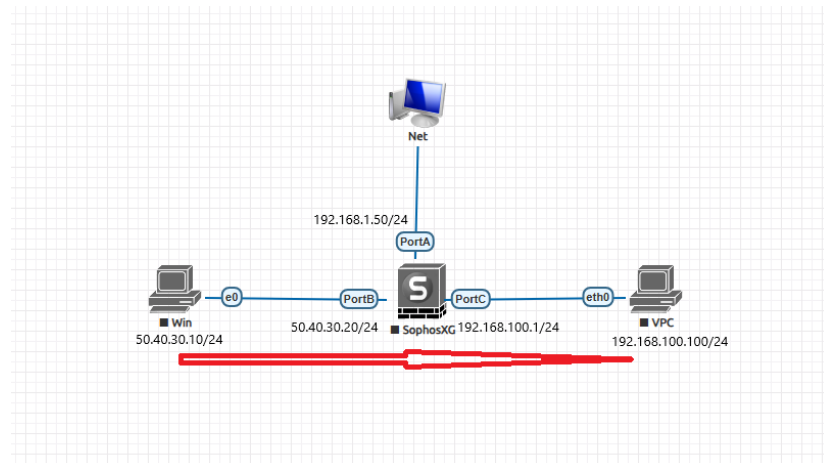




Sophos'ın Client uygulaması kurulduktan sonra açılan pencerenin sol üst köşesinde “import connection” kısmına indirilen SSL VPN konfigürasyon dosyası yüklenmelidir. Yükleme sonrasında kullanıcı adı ve parola bilgileriyle SSL VPN bağlantısı gerçekleştirilebilir.



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 erişimleri 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>