



İSTANBUL AYVANSARAY ÜNİVERSİTESİ
PLATO MESLEK YÜKSEKOKULU
İNTERNET VE AĞ TEKNOLOJİLERİ BÖLÜMÜ
2. ÖĞRETİM PROGRAMI

BERQNET FIREWALL KURULUMU

ÖĞRENCİNİN ADI-SOYADI

ŞENER ÖZBAĞÇE

İSTANBUL, 2020



İSTANBUL AYVANSARAY ÜNİVERSİTESİ
PLATO MESLEK YÜKSEKOKULU
İNTERNET VE AĞ TEKNOLOJİLERİ
2.ÖĞRETİM PROGRAMI

BERQNET FIREWALL KURULUMU

ÖĞRENCİNİN ADI-SOYADI

ŞENER ÖZBAĞÇE

PROJE DANIŞMANI

ÖĞR. GÖR. ERDAL CAN YALÇIN

İSTANBUL, 2020

BEYAN FORMU

Beyan Formu

Bitirme Projesi olarak sunduđum “BERQNET FIREWALL KURULUMU” bařlıklı alıřmanın kendi alıřmam olduđunu, arařtırma tasarımı ve yazım srelerinde etik dıřı davranıřta bulunmadıđımı, projedeki btn bilgileri akademik ve etik kurallar iinde elde ettiđimi, proje alıřmasıyla elde edilmeyen btn bilgi ve yorumlara kaynak gsterdiđimi ve bu kaynakları kaynaklar listesine aldıđımı, proje alıřması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranıřımın olmadıđını beyan ederim.

Tarih

İmza

řener ZBAĐE

BİTİRME PROJESİ SINAV FORMU

Bölüm ve Program adı: İnternet ve Ağ teknolojileri

Öğrencinin Numarası ve Adı-SOYADI: 18010504012 Şener ÖZBAĞÇE

Birimi: PLATO Meslek Yüksekokulu

Bitirme Projesinin Konusu: Berqnet Firewall Kurulumu

Bitirme Projesi Değerlendirme ve Puanlama Esasları

Sıra No	Değerlendirme Kriteri	Jüri Puanlaması				
1	Şekil kurallarına uygunluk					
2	Etik kurallara uygunluk					
3	Proje danışmanı ile takip sürecini işletme durumu					
4	Proje sunumunda konuya hakimiyeti					
5	Bitirme Projesi hakkında sorulan soruları cevaplama becerisi					
6	Projenin zamanında teslim edilme durumu					
7	Diğer					
Nihai Başarı Puanı		<table><tr><td>Rakamla</td><td>100</td></tr><tr><td>Yazıyla</td><td>Yüz</td></tr></table>	Rakamla	100	Yazıyla	Yüz
Rakamla	100					
Yazıyla	Yüz					

BİTİRME PROJESİ SAVUNMA SINAVI JÜRİSİ

Jüri Üyesi
Unvan-Adı-SOYAD-İmza
ÖĞRETİM GÖREVLİSİ ERDAL CAN YALÇIN



İSTANBUL
AYVANSARAY
ÜNİVERSİTESİ

BİTİRME PROJESİ ONAY FORMU

Kurum	İstanbul Ayvansaray Üniversitesi Plato Meslek Yüksekokulu
Program	İnternet ve Ağ Teknolojileri
Proje Sahib(i)/leri	Şener ÖZBAĞÇE
Proje Başlığı	Berqnet Firewall Kurulumu
Sınav Yeri	Plato Meslek Yüksekokulu
Sınav Tarihi	26.08.2020
Bitirme projesi jüri üyeleri tarafından usul ve esaslar bakımından değerlendirilmiş olup, kapsam ve ilgili alana katkısı bakımından ön lisans bitirme projesi olarak kabul edilmiştir.	

Jüri Üyesi
Unvan-Adı-SOYAD-İmza
ÖĞRETİM GÖREVLİSİ ERDAL CAN YALÇIN

TEŞEKKÜR METNİ

Başta, bize üniversite bölüm tanıtımından başlayıp, üniversite bitimine kadar olan derslerde sabırla eğitim verip, emeği geçen Sn. Erdal Can YALÇIN hocam başta olmak üzere yine eğitim ve gelişme sürecimde yardımcı olan genel müdürüm Sn. Serdar KUZUYAKA Bey'e emekleri ve çabaları için ayrı ayrı teşekkürlerimi sunarım. Yine bana destekleri için sevgili aileme teşekkürlerimi iletirim.

İmza

Şener ÖZBAĞÇE

senerozbagce.com.tr

TABLÖLAR

Tablo 4.7.1 Berqnet Firewall Özellikleri	13
---	----

senerozbagce.com.tr

ŞEKİL LİSTESİ

Şekil 5.1 1 Firewall Cihazının Şekilsel Olarak Konumu.....	14
Şekil 5.1 2 Firewall Portları	14
Şekil 5.1.2 1 Zyxel Marka Modemin Arayüzü	15
Şekil 5.1.3 1 Bridge Mode Kurulum Ekranı 1	16
Şekil 5.1.3 2 Bridge Mode Kurulum Ekranı 2	16
Şekil 5.1.3 3 Bridge Mode Kurulum Ekranı 3	16
Şekil 5.2 1 Berqnet Arayüzü	17
Şekil 5.2.2 Berqnet Karşılama Ekranı	17
Şekil 5.3.1.1 Wan Kurulumu 1.....	18
Şekil 5.3.1.2 Wan Kurulumu 2.....	18
Şekil 5.3.2.1 Lan ayarları kurulumu	19
Şekil 5.4.1 DNS Ayar Ekranı.....	20
Şekil 5.4.2 DNS Kurulum Ekranı.....	20
Şekil 5.4.3 DNS Sunucu Kurulum Ekranı	21
Şekil 5.5.1 Berqnet Lisans Ekranı Girişi	21
Şekil 5.5.2 Son kullanıcı ve Bayi bilgileri	22
Şekil 5.5.3 Lisans Anahtarı Giriş	22
Şekil 5.6.1 Yöneticiler Ayarları	23
Şekil 5.6.2 Web Yönetici Ayar Ekranı	23
Şekil 5.6.3 Web Kullanıcı Ekleme	24
Şekil 5.6.4 Web Kullanıcı Düzenleme	24
Şekil 5.6.5 Web Kullanıcı Düzenleme Mevcut Şifre Ekranı	25
Şekil 5.6.6 Web Kullanıcı Düzenleme Ekranı	25
Şekil 5.6.7 Mobil Yönetici Ekranı.....	26
Şekil 5.6.8 Mobil Kullanıcı Ekleme Ekranı.....	26
Şekil 5.7.1 Mobil Uygulama İndirme Ekranı.....	27
Şekil 5.7.2 Mobil Uygulama Hesap Ekleme	27
Şekil 5.7.3 Mobil Uygulama Grafik Ekranı.....	28
Şekil 5.7.4 Mobil Uygulama Menü Ekranı.....	29
Şekil 5.8.1 Bilgilendirme Servis Ekranı	29
Şekil 5.8.2 Bilgilendirme E-posta Ayarları Ekranı	30
Şekil 5.8.3 Bilgilendirme Kullanıcı Ekranı	30
Şekil 5.8.4 Bilgilendirme Kullanıcı Düzenleme Ekranı	31
Şekil 5.9.1 5651 Kayıt Aktarım Ekranı	31
Şekil 5.9.2 5651 Kayıt Aktarım Saat Ayarı Ekranı	32
Şekil 5.9.3 5651 Kayıt Aktarım Paylaşım Ekranı	32
Şekil 5.9.4 5651 Kayıt Aktarım Kayıtlar Ekranı.....	33
Şekil 5.9.5 5651 Kayıt Aktarım Uzak Sunucu Ekranı.....	33
Şekil 5.9.6 5651 Kayıt Aktarım Damga Ekranı	34
Şekil 5.9.7 Kayıt Aktarım Damga Ekranı 2	34
Şekil 5.9.8 5651 Kayıt Aktarım Uygula Ekranı.....	35
Şekil 5.10.1 Güncelleme Ekranı.....	35
Şekil 5.10.2 BerqOS Güncelleme Ekranı	35
Şekil 5.11.1 VOIP Ayar Ekranı.....	36
Şekil 5.11.2 Uygula Butonu.....	36
Şekil 5.12.1 Hotspot Ayar Ekranı	37

Şekil 5.12.2 Hotspot Ayar Ekranı 2	37
Şekil 5.12.3 Hotspot Port Seçim Ekranı	37
Şekil 5.12.4 Hotspot Durum Ekranı	38
Şekil 5.12.5 Hotspot Yöntem Ekranı.....	38
Şekil 5.12.6 Hotspot Arayüz Yönetici Oluşturma Ekranı	39
Şekil 5.12.7 Hotspot Oturum Ekranı	39
Şekil 5.12.8 Hotspot Arayüz Düzenleme Ekranı 1	40
Şekil 5.12.9 Hotspot Arayüz Düzenleme Ekranı 2	40
Şekil 5.12.10 Hotspot Arayüz Düzenleme Ekranı 3	40
Şekil 5.12.10 Hotspot Uygulama Ekranı	41
Şekil 5.13.1 Firewall Ayarlar Girişi	42
Şekil 5.13.2 Firewall Ayarlar Ekranı.....	42
Şekil 5.13.3 Firewall Ayarı Ana Ekranı 1	42
Şekil 5.13.4 Firewall Ayarı Ana Ekranı 2	43
Şekil 5.13.5 Ağ Nesnesi Ekranı	43
Şekil 5.13.6 Ağ Nesnesi Ekranı	44
Şekil 5.13.7 Ağ Nesnesi Ekleme Ekranı.....	44
Şekil 5.13.8 Limit Nesnesi Ekranı.....	44
Şekil 5.13.9 Bant Genişliği Nesnesi Ekranı.....	45
Şekil 5.13.10 Zaman Nenesi Ekranı	45
Şekil 5.13.11 Firewall Kuralı.....	45
Şekil 5.14.1 Port Yönlendirme Ekranı.....	46
Şekil 5.14.2 Ağ Nesnesi Ekranı	46
Şekil 5.14.3 Ağ Servisleri Ekranı.....	47
Şekil 5.14.4 Port Ekleme Ekranı	47
Şekil 5.14.5 Port Ekleme Ekranı	47
Şekil 5.14.6 Port Ekleme Ekranı	48
Şekil 5.14.7 Port Grubu Oluşturma	48
Şekil 5.14.8 Port Yönlendirme Kuralı	49
Şekil 5.15.1 Ayarlar Ekranı	49
Şekil 5.15.2 Web Filtreleme Ayarları Ekranı	50
Şekil 5.15.3 Web Filtre Kural Ekranı	50
Şekil 5.15.4 Medya Formatları Ekranı	51
Şekil 5.15.5 URL Kategorileri Ekranı	51
Şekil 5.15.6 Web Nesneleri Ekranı	52
Şekil 5.15.7 Web Nesnesi Ekranı 1	52
Şekil 5.15.8 Web Nesnesi Ekranı 2	52
Şekil 5.15.9 Web Nesnesi Ekranı 3	53
Şekil 5.15.10 Kelime Ekleme Ekranı	53
Şekil 5.15.11 Web Filtre Kuralı	53
Şekil 5.16.1 VPN Ekranı	54
Şekil 5.16.2 VPN Düzenleme Ekranı	54
Şekil 5.16.3 VPN Ağ Nesnesi Ekranı 1	54
Şekil 5.16.4 VPN Ağ Nesnesi Ekranı 2	55
Şekil 5.16.5 VPN Ağ Nesnesi Ekranı 3	55
Şekil 5.16.6 VPN Kural Ekranı.....	55
Şekil 5.16.7 VPN Karşılıklı Ayar Ekranı 1	56

Şekil 5.16.8 VPN Karşılıklı Ayar Ekranı 2	56
Şekil 5.16.9 VPN Karşılıklı Ayar Ekranı 3	57
Şekil 5.16.10 Bağlantı Ekranı	57
Şekil 5.17.1 SSL VPN Kuralı	57
Şekil 5.17.2 Ağ Nesnesi Ekleme	58
Şekil 5.17.3 VPN Ağı Nesnesi Ekleme	58
Şekil 5.17.4 VPN Kural Ekranı	58
Şekil 5.17.5 VPN Kullanıcı Ayarları	59
Şekil 5.17.6 Ekle Düzenleme Tuşları	59
Şekil 5.17.7 SSL VPN Kullanıcı Ekleme Ekranı	60
Şekil 5.17.8 İstemci Ayarlarını İndirme 1	60
Şekil 5.17.9 İstemci Ayarlarını İndirme 2	61
Şekil 5.17.10 İstemci Ayarlarını İndirme 3	61
Şekil 5.17.11 İstemci Ayarlarını İndirme 4	62
Şekil 5.17.12 İstemci Ayarlarını İndirme 5	62
Şekil 5.17.13 Open VPN İndirme	62
Şekil 5.17.14 Open VPN Kurulum 1	63
Şekil 5.17.15 Open VPN Kurulum 2	63
Şekil 5.17.16 Open VPN Kurulum 3	64
Şekil 5.17.17 Open VPN Kurulum 4	64
Şekil 5.17.18 Open VPN Programı Kurulum Ekranı 1	65
Şekil 5.17.19 Open VPN Programı Kurulum Ekranı 2	65
Şekil 5.17.20 Open VPN Programı Kurulum Ekranı 3	66
Şekil 5.17.21 Open VPN Programı 1	66
Şekil 5.17.22 Open VPN Programı 2	66
Şekil 5.17.23 Open VPN Programı 3	67
Şekil 5.18.1 IPS Ayarları	68
Şekil 5.18.2 IPS Kategori Listesi Ekranı 1	68
Şekil 5.18.3 Kategori Listesi Ekranı 2	69
Şekil 5.18.4 İmza Ekranı	69
Şekil 5.18.5 Uygula Butonu	69
Şekil 5.19.1 Kayıtlar Ayarı	70
Şekil 5.19.2 Kayıtlar Grafik Ekran	70
Şekil 5.19.3 Firewall Kayıtları	70

KISALTMALAR

IOT= Internet of Things

DNS= Domain Name System

Wi-Fi= Wireless Fidelity

VPN= Virtual Privet Network

PPTP= Point to Point Tunnel Protocol

L2TP= Layer Two Tunneling Protocol

IPSEC= Internet Protocol Security

SSL= Secure Sockets Layer

TLS= Transport Layer Security

VOIP= Voice Over Internet Protocol

IPS= Intrusion Prevention Systems

IDS= Intrusion Detection Systems

IP= Internet Protocol Address

ISS= Integrated Service Solutions

WAN= Wide Area Network

LAN= Local Area Network

DHCP= Dynamic Host Configuration Protocol

KVKK= Kişisel Verilerin Korunma Kanunu

USOM= Ulusal Siber Olaylara Müdahale Merkezi

SOME= Siber Olaylara Müdahale Ekipleri

BTK= Bilgi Teknolojileri ve İletişim Kurumu

ÖZET

Berqnet Firewall cihazı kurulu olan işletmelerde güvenli interneti sağlayacağım. Berqnet'in bq25 model Firewall cihazının kurulumlarını göstereceğim. Berqnet'i olan işletmeler güvenli hızlı ve yedekli internetin tadını doyasıya çıkaracak. Çalışanlarınız denetim altında olup izlenebilir şekilde onların log kayıtlarının nasıl izleneceğini göstereceğim. KVKK kanununu için gerekli ayarları ve bu konunun getirdiği yükümlülükleri yerine getireceğim.

senerozbagce.com.tr

İÇİNDEKİLER

BEYAN FORMU	i
BİTİRME PROJESİ SINAV FORMU	ii
BİTİRME PROJESİ ONAY FORMU	iii
Teşekkür Metni	iv
TABLolar	v
ŞEKİL LİSTESİ	vi
ÖZET	x
1. GİRİŞ	1
2. AĞ	2
2.1 Ağ Nedir?	2
2.1.1 Ağlar Neden Genişletilir?	2
2.2 DNS Nedir?	2
2.2.1 DNS Kullanım Amacı Nedir?	2
2.3 Hotspot Nedir?	3
2.3.1 Mobil Hotspot Nedir?	3
2.4 VPN Nedir?	3
2.4.1 VPN Nasıl Çalışır?	3
2.5 VPN Türleri Nedir?	4
2.5.1 PPTP Vpn	4
2.5.2 Site to Site Vpn	4
2.5.3 L2TP Vpn	4
2.5.4 IPSEC Vpn	5
2.5.5 SSL ve TLS Vpn	5
2.6 Virüs Nedir?	5
2.7 VOIP Nedir?	6
3. AĞ KANUNLARI	7
3.1 5651 Sayılı Kanun Nedir? Yükümlülükleri Nelerdir?	7
3.1.2 5651 Sayılı Kanuna Aykırı Hareketin Sonucu	8
3.2 KVKK Kanunu Nedir?	8
3.3 Zaman Damgası Nedir?	9
3.4 Zaman Damgası Başvurusu	9
3.4.1 Özel Firma Başvuruları	9
3.4.2 Bireysel Başvurular (Şahıs Başvuruları)	9

4	AĞ GÜVENLİĞİ	10
4.1	Ağ Güvenliği Nedir?	10
4.2	USOM Nedir?	10
4.2.1	USOM'un Görevleri Nelerdir?	10
4.3	Active Directory Nedir?	11
4.4	Antivirüs Nedir?	11
4.5	Firewall Nedir?	12
4.6	Berqnet Nedir?	12
4.7	Berqnet Genel Özellikleri?	12
5	BERQNET UYGULAMALARI	14
5.1	Modem Ayarları	14
5.1.2	Modem Arayüze Giriş	15
5.2	Berqnet Arayüz Girişi	17
5.3	Berqnet Network Ayarları	18
5.3.1	Wan Ayarları	18
5.3.2	Lan Ayarları	19
5.4	DNS Ayarları	20
5.5	Berqnet Lisans İşlemleri	21
5.6	Yönetici Ayarları	23
5.7	Berqnet Mobil Uygulama Kurulumu	27
5.8	Bilgilendirme Servisi	29
5.9	5651 Kayıt Aktarım Servisi	31
5.10	Berqnet ve Servis Güncellemeleri	35
5.11	VOIP Ayarları	36
5.12	Hotspot Ayarı	37
5.13	Firewall Ayarları	42
5.14	Port Yönlendirme	46
5.15	Web Filtre Ayarları	49
5.16	Ipsec Vpn Kurulumu	53
5.18	Ips Kategorileri	68
	KAYNAKÇA	71

1. GİRİŞ

Firewall cihazları olmayan birçok küçük, orta ve büyük işletmeler çok büyük bir tehdit altındalar. Firewall cihazları olmayan şirketler çok büyük zarara uğrayabilirler. Siber saldırılar günümüzde pek çok işletmeyi hedef almış ve maddi zararlara, iş kayıplarına neden olmuştur. Tam da bu sebeple firewall cihazları siber suçlulara karşı etkin ve kilit rol alırlar. Firewall cihazları olan işletmeler daha güvenli bir ağa sahip olurlar. Bunun ile birlikte daha güçlü ve daha güvenli iş imkanına sahiptirler. Firewall cihazları ile evden, tatilden hatta internetin bulunduğu her ortamda sizi güvenli şekilde şirket ağına bağlar ve işlerinizi sanki oradaymışsınız gibi sürdürmenize olanak sağlar. Bu projemizde Berqnet firewall cihazımızı kurulumunu ve ayarlarını nasıl yapacağınızı göstereceğim.

senerozbagce.com.tr

2. AĞ

2.1 Ağ Nedir?

Birden çok bilgisayarın ve IOT cihazlarının aynı ortamda birbirlerine kablolu veya kablosuz şekilde bağlanarak, bilgi alışverişinde bulundukları ortama özel ağ denir. Özel ağlarda örnek olarak şirket içinde bulunan cihazlarla iletişime geçebilirsiniz. Kendi bilgisayarınızdan aynı ağda olan bir yazıcıdan çıktı alabilir, aynı ağda bulunan arkadaşlarınıza paylaşım klasör açabilirsiniz. Tabi ki bu ağlar genişletilebilir.

2.1.1 Ağlar Neden Genişletilir?

Dış dünya ile iletişime geçmek istediğinizde özel ağdan çıkıp internete girmiş olmanız gerekmektedir. Modern teknolojiadaki gelişmeler bilgisayar kullanımını mümkün kılmıştır. Bugün birçok bankacılık işlemlerinizi gerçekleştirebilir internet üzerinden alışveriş yapabilirsiniz, hatta dışarda bulunduğunuz esnada cep telefonunuz veya bilgisayarınız ile evinizde bulunan kombi, aydınlatma sistemi gibi tüm IOT cihazlarını kontrol edebilirsiniz. Bu ve bunlar gibi pek çok işlemleri internet ağı kullanarak yaparız.

2.2 DNS Nedir?

DNS, Domain Name System'in kısaltılmış şeklidir. Türkçe karşılığı ise Alan İsimlendirme Sistemi olarak bilinir. Yani internetin telefon rehberidir. Kolay hatırlanan isimleri (senerozbagce.com.tr) IP adreslerine çevirir (5.180.186.163).

2.2.1 DNS Kullanım Amacı Nedir?

DNS'in kullanım amacı son derece basittir, kolay anlaşılabilir ve kullanılabilir makine ve alan isimleri ile makine IP adresleri arasında çift taraflı dönüşümü sağlar. IP adreslerinin gündelik hayatta kullanımı ve hatırlanması pek pratik olmadığı için domain isimlendirme sistemi kullanılır. (hosting.com.tr)

2.3 Hotspot Nedir?

Hotspot, belirli bir lokasyon içerisinde kablosuz erişim protokolleri yardımıyla sunulan internet bağlantısıdır. Türkçe karşılığı “Sıcak Nokta” olarak çevrilebilir. Ancak “Sıcak nokta” muhtemelen birçok kişiye yabancı gelecektir. Hotspot kelimesini Türkçeye çevirmeden birebir kullanımı daha yaygındır. Genel olarak “açık Wi-Fi noktası” şeklinde de kullanılabilir. Hotspot terimi ilk defa 1993 yılında NetWorld+Intercoop konferansında Brett Stewart tarafından kullanılmıştır. Bazı tahminlere göre bugün itibari ile dünya çapında yaklaşık 200 milyon Hotspot noktası olduğu söylenmektedir.

2.3.1 Mobil Hotspot Nedir?

Mobil Hotspot: Tamamen taşınabilir hotspot ağlarıdır. Normal bir hotspot ağı fiziki olarak bir lokasyona bağlı bulunurken, mobil hotspot ağları hareketlidir ve fiziki bir bağlantısı yoktur. Mobil hotspotlara en basit örnek, akıllı telefonlarınızdan oluşturduğunuz “internet paylaşımı” ağlarıdır. Bu ağlar taşınabilmir ve “tetheding” olarak adlandırılır. (berqnet.com)

2.4 VPN Nedir?

İngilizce olarak Virtual Private Network, Türkçesiyle Sanal Özel Ağ anlamına geliyor. VPN'in temel amacı, fiziksel olarak bulunmadığınız bir yerdeki ağa sizi uzaktan bağlamaktır. Aslında temel amaç daha güvenli bir iletişim yolu sağlayarak kurumsal çözümler sunmaktır.

2.4.1 VPN Nasıl Çalışır?

VPN, internete bağlandığınız cihazı sanal olarak farklı bir konumda gösterir. Bunun için karşıdaki ağa kriptolu bir tünel açar. Aktarılan bilgiler bu tünelden karşılıklı olarak paylaşılır. Yani örneğin Vikipedi'ye VPN üzerinden bağlanırsanız, cihazınız ve bağlandığını VPN ağı (Örneğin: Kanada) arasında veri akışı olur. Bu akış kriptolu olduğu için dışarıdan görüntülenemez. Böylece trafik Kanada üzerinden gerçekleşir, Kanada'nın ağ usüllerine göre internette dolaşırsınız.

2.5 VPN Türleri Nedir?

2.5.1 PPTP Vpn

PPTP VPN, Noktadan Noktaya Tünelleme Protokolünü kullanır. İsminin de belirttiği gibi, bir PPTP VPN bir tünel yaratır ve veriyi ele geçirir. Çok yaygın kullanılan bir VPN için biraz uzun bir isim. PPTP VPN'ler uzaktaki kullanıcılar tarafından mevcut internet bağlantıları aracılığıyla VPN ağına bağlanmaları için kullanılır. Bu, hem işletme hem de ev kullanıcıları için faydalı bir VPN'dir. VPN'e erişmek için kullanıcılar onaylı parolayı kullanarak VPN'e giriş yapar.

2.5.2 Site to Site Vpn

Siteden Siteye VPN aynı zamanda Yönlendiriciden Yönlendiriciye VPN olarak da isimlendirilir ve genellikle şirket tabanlı operasyonlarda kullanılır. Birçok şirketin ulusal ve uluslar arası lokasyonlarda ofisleri vardır, Siteden Siteye VPN ana ofis lokasyonunun diğer ofislerle bir ağ oluşturması için kullanılır. Bu, aynı zamanda İnternet tabanlı VPN olarak da bilinir.

2.5.3 L2TP Vpn

L2TP Katmandan Tünel Protokol kullanır ve Microsoft ve Cisco tarafından geliştirilmiştir. L2TP VPN'ler daha güvenli bir VPN bağlantısı oluşturmak için diğer VPN'lerin güvenlik protokolleri ile kombine olan bir VPN'dir. Bir L2TP VPN aynı IPSec protokolünün veri şifrelemesi gibi iki L2TP bağlantı noktası ve diğer bir VPN arasında bir tünel oluşturur ve tüneller arasında güvenli iletişim üzerine odaklanır.

2.5.4 IPSEC Vpn

IPSec Internet Protocol Security'nin kısaltmasıdır. IPSec bir IP ağı üzerinden internet bağlantısı sağlamak için kullanılan bir VPN protokolüdür. Uzak bir bölgede kurulan tünel sizin merkez bölgenize erişmenize izin verir. IPSec, her oturumu doğrulayarak ve her bir veri paketini bağlantı üzerinden şifreleyerek internet protokolü iletişimini korur. IPSec VPN'in çalıştığı iki mod bulunmaktadır; transport modu ve tünelleme modu. İki mod da veri transferini iki farklı ağda korur. Transport modu sırasında veri paketindeki mesajlar şifrelenir. Tünelleme modunda tüm veri paketi şifrelenir. IPSec VPN'i kullanmanın avantajı daha güçlü bir güvenlik sistemi sağlamak için diğer güvenlik protokolleriyle birlikte kullanılabilmesidir.

IPSec çok değerli bir VPN olsa da bu protokolü kullanmanın en büyük dezavantajı kullanımdan önce yüklemeniz gereken istemcilere çok fazla zaman harcanmasıdır.

2.5.5 SSL ve TLS Vpn

SSL Güvenli Soket Katmanı kullanır, TLS ise Transport Tabakası Güvenliği kullanır. İkisi de tek bir protokol olarak çalışır. İkisi de VPN bağlantısı oluşturmak için kullanılır. Bu, web tarayıcılarının istemci olarak hizmet verdiği bir VPN bağlantısıdır ve kullanıcılar tüm ağa değil yalnızca bazı spesifik uygulamalara erişimle kısıtlıdır. SSL ve TLS protokollerinden genellikle çevrimiçi alışveriş web siteleri ve servis sağlayıcıları yararlanır. Bir SSL ve TSL VPN, PC tarayıcınızdan uygulama sunucusuna güvenli bir oturum sağlar. Çünkü web tarayıcıları SSL'ye kolay bir şekilde kayar ve kullanıcının herhangi bir işlem yapmasına gerek kalmaz. Web tarayıcıları halihazırda SSL ve TSL ile entegre olarak gelir. SSL bağlantılarının URL başlangıcında http yerine https bulunur. (vpnmentor.com)

2.6 Virüs Nedir?

Bilgisayar virüsleri bir bilgisayardan diğer bilgisayara bulaşmak, bu bilgisayarların çalışmasını engellemek ve verileri çalmak için yazılmış küçük boyutlu zararlı yazılımlardır. Bilgisayar virüslerini engellemek için Antivirüs programları geliştirilmiştir. (datakey.com.tr)

2.7 VOIP Nedir?

VoIP İnternet üzerinden sesli görüşme yapmanıza olanak tanıyan IP tabanlı bir protokoldür. VoIP, Voice Over Internet Protocol kelimelerinin kısaltmasından oluşmaktadır. Genel olarak kurumlar bu teknolojiyi kullanarak iletişim kurmaktadırlar. VoIP teknolojisi Türkiye ve dünyada sıklıkla kullanılan son yılların en popüler iletişim teknolojilerinden biridir. Geleneksel bakır kablo ile santrallere bağlanılan telefon görüşmelerine göre çok daha avantajlı bir iletişim kanalı olarak tanımlanabilir. VoIP teknolojisi ile yapılan telefon görüşmelerinde ses sinyalleri önce dataya sonra elektrik sinyallerine çevrilerek İnternet veri hattı üzerinden taşınır ve geniş bir band aralığına sahiptir. Bu sayede sabit hatlarla veya mobil hatları ile ücretsiz veyahut çok daha düşük ücretlerle konuşma yapabilirsiniz. (VOIP berqnet.com)

senerozbagce.com.tr

3. AĞ KANUNLARI

3.1 5651 Sayılı Kanun Nedir? Yükümlülükleri Nelerdir?

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 23 Mayıs 2007 tarihinde 26530 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. 5651 Sayılı Kanun internet ortamında yapılan yayınların sistematik bir düzen ve kontrol altına alınması ve aynı zamanda yapılan bu yayınlar yoluyla işlenen suçlar ile mücadele edilmesi hakkındaki kanundur.

Bu kanunun yürürlüğe girdiği tarihten itibaren kablolu ya da kablosuz bağlantı ile kurum bünyesindeki internet hizmetini toplu olarak müşterilerinin ya da çalışanlarının kullanımına açan kurumların, yasal olarak yerine getirmekle yükümlü olduğu şartlar bulunmaktadır. Bu kanunun yönergelerine uymakla zorunlu olan kurumlar; oteller, alışveriş merkezleri, üniversiteler, kafeler, internet kafeler, KOBİ'ler, fabrikalar gibi interneti toplu kullanıma açan kurumlardır. Kanun kapsamına, işletmelerin müşterilerine sunduğu ücretsiz internet hizmeti ve firmaların çalışanlarına şirket içerisinde sundukları internet hizmeti de girmektedir. Günlük yaşamımızda sıkça uğradığımız kafelerde, yemek yediğimiz restoranlarda ya da çalıştığımız kurum içerisinde kullandığımız internet hizmeti, kanun kapsamında yer alıyor. İşletmeler ve kurumlar tarafından verilen bu tür internet hizmetinin kablosuz bağlantı noktaları büyük çoğunlukla şifreli olmaktadır. Şifresiz olarak sunulan bu tür hizmetler kesinlikle güvenli olmamakla birlikte kullanımı sonucunda kullanıcının özel bilgilerinin çalınması ya da virüs ve benzeri zararlı yazılımların bulaştırılması olarak soruna yol açabilir. Bu yüzden şifresiz bağlantılara kesinlikle güvenilmemelidir.

5651 Sayılı Kanun'a tam uygun olarak hareket edebilmek için en güvenli yöntem ağa bağlanacak kullanıcının cep telefonuna bir şifre gönderilerek gönderilen numaranın kayıt altına alınmasıdır. Bu sayede hat sahibinin TC Kimlik Numarası'na da gerekli durumlarda ulaşılabilir ve yasal takip yapılabilir. İşletmelerde bu şekilde SMS doğrulaması olmadığında ya da kullanıcıların kişisel bilgileri kayıt altına alınmadığında ağı kullanarak işlenecek suçlardan hizmeti sunan işletme ya da kurum sorumlu tutulacaktır. Bu yüzden işletmelerin bu tür bağlantıları şifre altına almaları ve kullanıcıların bilgilerini de kayıt altına almaları olası suç işleme durumunda şirketi ilave yükümlülükten kurtaracaktır.

3.1.2 5651 Sayılı Kanuna Aykırı Hareketin Sonucu

5651 Sayılı Kanunda açıkça belirtilen ve yasanın gerekliliklerini yerine getirmeyen işletme ve kuruluşlar için maddi ve idari para cezaları bulunmaktadır. Yasa gereği olarak işletmeler log tutma ve sundukları hizmetin kimler tarafından hangi zaman dilimlerinde kullanıldığını geçmişe dönük olarak belgeleyebilmek zorundadırlar, yasanın tümüne ya da bir kısmına uyulmadığı takdirde maddi ve idari çeşitli yaptırımlarla karşılaşılabilir. Verilebilecek ceza yapılan aykırılığın ya da kanunun içeriklerinden ne kadarının yerine getirilip ne kadarının kanuna uygun yapıldığına göre değişmekle birlikte verilebilecek para cezası kişilere 15.000, servis sağlayıcılara da 100.000 TL gibi bir tutara ulaşabilmektedir. Para cezasının yanı sıra hizmet durdurma ya da geçici süreyle iş yerinin faaliyetlerinin durdurulması şeklinde de olabilir. Bu yüzden yasalara uyumluluk konusunda kuruluşların azami ölçüde dikkatli olmaları gereklidir. (5651 berqnet.com)

3.2 KVKK Kanunu Nedir?

'6698 Sayılı Kişisel Verilerin Korunması Kanunu' 7 Nisan 2016 tarihinde yürürlüğe girmiştir. Kişisel verilerin korunması kanunu kişilerin özel hak ve özgürlüklerini korumak, oluşabilecek zararların önüne geçmeyi amaçlamaktadır.

3.2.1 KVKK Kanunu Amacı Nedir?

KVKK amacı, kişisel verilerin işleme şartlarını, kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunmasını ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemekle başladı. Veri güvenliğinin sağlanması, kişilerin haklarının ihlal edilmemesi için gerekli olan bu kanun, kişilerin bütün haklarını güvence altına alır. Kanun özel kurum veya kamu kurumu ayrımı yapmaksızın tüm kurumları kapsamaktadır. Kişisel veri sadece kişinin ad, soyad, doğum tarihi, doğum yeri değil, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, hobiler gibi kişiyi doğrudan veya dolaylı etkileyen her türlü bilgiler kişisel veri kapsamında yer alır. (haberler.com)

3.3 Zaman Damgası Nedir?

Zaman Damgaları belli bir verinin belirtilen bir tarihte var olduğunu kanıtlarlar. Zaman Damgası Sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar.

Bir sözleşmenin imzalandığı, paranın transfer edildiği, başvurunun yapıldığı vs. tarih ve saati kanıtlama ihtiyacı günümüz e-ticaret, e-devlet uygulamaları için hayati önem taşımaktadır. Bununla birlikte yeni bir çizim, tasarım, fotoğraf, düşünce, araştırma, formül, algoritma, kitap gibi fikri ve mülki kullanım hakkı elde edilmek istenen her türlü elektronik veri için zaman damgası alınabilir.

5070 sayılı Elektronik İmza Kanununa göre Zaman Damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı, ifade eder.

3.4 Zaman Damgası Başvurusu

3.4.1 Özel Firma Başvuruları

Zaman damgası portalinden zdportal.kamusm.gov.tr işlem tipi olarak kurumsal seçeneği işaretlenerek, talep edilen bilgiler doldurulur ve sipariş oluşturulur. Üyelik oluşturulduktan sonra işlemler menüsünden bilgi görüntüleme, güncelleme ve kontör ekleme işlemleri gerçekleştirilebilir.

3.4.2 Bireysel Başvurular (Şahıs Başvuruları)

Zaman damgası portalinden zdportal.kamusm.gov.tr işlem tipi olarak bireysel seçeneği işaretlenerek, talep edilen bilgiler doldurulur ve sipariş oluşturulur. Üyelik oluşturulduktan sonra işlemler menüsünden bilgi görüntüleme, güncelleme ve kontör ekleme işlemleri gerçekleştirilebilir. (kamusm.gov.tr)

4 AĞ GÜVENLİĞİ

4.1 Ağ Güvenliği Nedir?

Ağ güvenliği, ağ trafiğini de kapsayan dijital varlıkları korurken, izinsiz ağ saldırılarını izlemek, önlemek ve bunlara yanıt vermek için tasarlanmış araçları, taktikleri ve güvenlik politikalarını tanımlayan bir terimdir. Ağ güvenliği, donanım ve yazılım teknolojilerini (bilgili güvenlik analistleri, avcılar, olay yanıtlayıcıları vb. kaynaklar dahil) içerir ve ağını hedef alan tüm potansiyel tehditlere yanıt vermek üzere tasarlanmıştır.

4.2 USOM Nedir?

USOM, Ulusal Siber Olaylara Müdahale Merkezi kelimelerinin kısaltmasıdır. Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT), 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı ile yayınlanan “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı” 4. maddesi dahilinde Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulmuştur. Ulusal Siber Olaylara Müdahale Merkezi, ülkemizde siber güvenliğin sağlanmasına yardımcı olmada, ortaya çıkan tehditlerin belirlenmesinde, muhtemel saldırı ve siber güvenlik olaylarının etkilerinin azaltılması ve ortadan kaldırılmasına yönelik önlemlerin alınması ve belirlenen aktörlerle paylaşılması amacıyla kurulmuştur.

USOM, kendisine gelen ihbarları ilk aşamasından itibaren yöneten, özel ekipleri tarafından çözüm sürecine kadar takip eden ve değerlendiren resmi bir kurumdur. Aynı zamanda ulusal ve uluslararası siber güvenlik tatbikatları düzenlenerek kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalığının artırılmasına yardımcı olarak bilinçlendirme ve yönlendirme faaliyetleri sürdürmektedir.

4.2.1 USOM’un Görevleri Nelerdir?

USOM, yurtiçi ve yurtdışı kaynaklı siber suçları ve tehditleri tespit etme ile önleme faaliyetleri yürütmektedir. Ortaya çıkabilecek söz konusu siber güvenlik olaylarına ilişkin olarak yapılan çalışmalar çerçevesinde alarm, uyarı ve duyuru işlemlerini yapmakla ve kurumları bilgilendirmekle sorumludur. USOM görevleri kapsamında Kurumsal ve Sektörel Siber Olaylara Müdahale Merkezlerinin (SOME) kurulması süreçlerine de yer verilmiştir.

Bu kapsamda, kritik sektörlerle yapılacak saldırıların tespit edilerek önlenmesi, siber güvenlik olaylarının duyurulması ve ilgili kurumlarla paylaşılması, bu konuda ilgililerin uyarılması faaliyetlerini de gerçekleştirmektedir.

Aynı zamanda USOM bünyesinde SOME (Siber Olaylara Müdahale Ekipleri) isimli ekipler bulunmaktadır. Bu ekipler USOM altında Kurumsal SOME ve Sektörel SOME adlarıyla yer almaktadır. Kurumsal SOME bakanlıklar, müstakil kamu kurumları ile bilgi işleme sahip diğer kamu kurumları içerisinde koordinasyon sağlar. Sektörel SOME ise özel sektörler ve kritik seviyede iş yapan kurumlar için ayrılmıştır. Sektörel SOME'ler enerji, bankacılık ve finans sektörleri, ulaştırma, kritik kamu hizmetleri, su yönetimi ve elektronik haberleşme konusunda çalışan sektör ile koordinasyon içerisinde de bulunmaktadır.

Diğer bir yandan kritik alt yapı işletmecileri (kamu veya özel) için de gerektiğinde USOM ile koordinasyona geçebilmesi sağlanmıştır. Bu sayede USOM, kurum ve kuruluşların kendi SOME'lerini oluşturmaları konusunda yardımcı olma görevi üstlenmiştir. (USOM berqnet)

4.3 Active Directory Nedir?

Active Directory, Microsoft tarafından işletmelerin şirket ağlarının yönetimini sağlayan dizin hizmetidir. Şirket içerisinde bulunan sunucular, bilgisayarlar, yazıcılar, kullanıcılar, departmanlar gibi tüm bilgilerin saklandığı bir veritabanıdır. Bu hizmet ile yönetsel kısıtlamalar oluşturulabilir ve ihtiyaca göre şekillendirilebilir.

Active Directory yönetimi sağlamak için Domain Naming System (DNS)'i kullanır. Domain yapısında bulunan tüm sunucular ve bilgisayarlar DNS içerisinde saklanır. BT uzmanlarının domain içerisindeki kullanıcıları, bilgisayarları, programları ve ağ servislerini merkezi noktadan kolayca yönetmesini sağlar.

4.4 Antivirüs Nedir?

Antivirus bilgisayarın güvenliğini sağlamak için kullanılan yazılımlardır. Antivirüs tarama, temizleme, eş kurtarma ve koruma gibi işlevlere sahiptir. Antivirüs bilgisayarı zararlı programlardan korur. Antivirüs programı bilgisayara zararı olan programları bulup yedekler ve bazı zararlı programları bulup bu programları kullanıcısının bilgisine sunar. Her bilgisayarda yeni incelenmiş ve lisanslı bir antivirüs programı bulunması şarttır, çünkü bazı virüs programları telafisi mümkün olmayan kalıcı hasarlara neden olabilirler. (datakey.com.tr)

4.5 Firewall Nedir?

Türkçe kelime karşılığı “Güvenlik Duvarı” olan firewall, gelen ve giden ağ trafiklerini kontrol etmek için oluşturulmuş olan ve çeşitli kuralları olan bir ağ güvenlik sistemidir. Firewall hem donanım tabanlı hem de yazılım tabanlı olabilir. Firewall, güvenilir ağlar ile güvenilirmez ağlar arasında bir engel oluşturur. Firewall, pozitif bir kontrol modeli aracılığıyla ağ kaynaklarına olan erişimi denetler. Böylelikle firewall politikasına bağlı olarak bazı ağ trafiklerine izin verilir ve diğer tüm trafikler reddedilir. (firewall ostec.blog)

4.6 Berqnet Nedir?

Berqnet, dünyanın en kolay kurulabilen ve yönetilen firewall cihazıdır. Tamamı yerli ve alanında uzman AR-GE kadrosu tarafından her ölçekteki işletmenin siber güvenlik ihtiyaçlarına yönelik çözüm üretme amacıyla 2013 yılında AR-GE çalışmalarına başlayan Berqnet, 2015 yılında ilk ürün ailesini piyasaya sürmüştür.

Birinci kuruluş amacı işletmelerin veri ve sistem güvenliğinin, yüksek performans ve en doğru çözümlerle korunması olan Berqnet, bir LOGO Siber Güvenlik ve Ağ Teknolojileri A.Ş. markası olarak çalışmalarına devam etmektedir.

4.7 Berqnet Genel Özellikleri?

- Bütünleşik Güvenlik Hizmeti
- Basit, Anlaşılır ve Türkçe Kullanıcı Arayüzü
- Mobil Uygulama Aracılığıyla İstenilen Her Yerden Rapor Görüntüleme ve Cihaza Uzaktan Erişim İmkânı
- Hotspot Özelliği
- İleri Düzey Web ve Uygulama Filtreleme Özellikleri
- 5651 ve 6698 no’lu yasalara uygun tümleşik LOG tutma çözümü
- VPN Hizmetleri (IPSec, SSL)
- IPS (Saldırı Engelleme Sistemi)
- İleri seviye raporlama özellikleri
- Yerleşik Antivirüs Koruması
- WAN Balancing (İnternet Yük Dengeleme Sistemi)

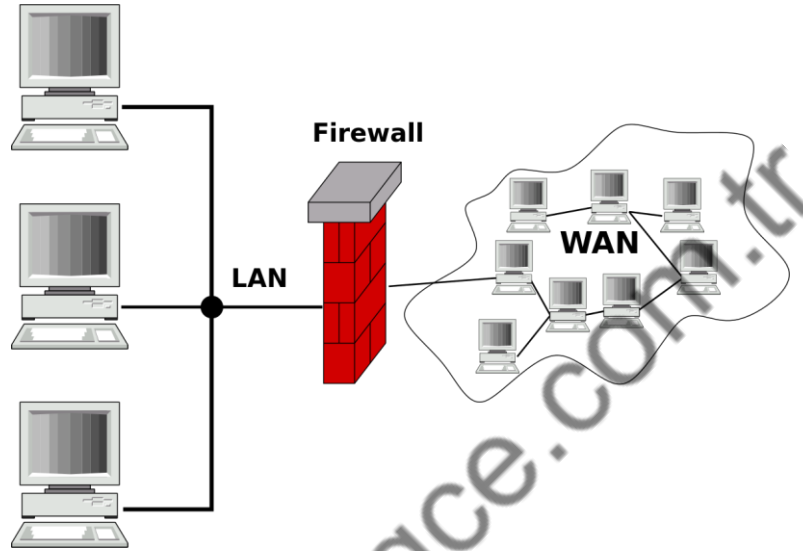
Tablo 4.7.1 Berqnet Firewall Özellikleri

MODEL	Mobil Raporlama	Sabit 10/100/1000 Ethernet Port	Maksimum 10/100/1000 Ethernet Port	USB Port	Harici Saklama Alanı (USB)	Dahili Saklama Alanı	Harici Saklama Alanı (Network)
BQ25S	VAR	4	4	2	1TB	8GB	SINIRSIZ
BQ60	VAR	6	6	2	1TB	8GB	SINIRSIZ
BQ100	VAR	8	8	2	1TB	16GB SSD	SINIRSIZ
BQ200	VAR	8	16	2	1TB	32GB SSD	SINIRSIZ
BQ300	VAR	8	16	2	1TB	64GB SSD	SINIRSIZ

5 BERQNET UYGULAMALARI

5.1 Modem Ayarları

Firewall kurulumu gerçekleştireceğimiz zaman internetimizi firewall da sonlandırmamız gerekir. Fiziki olarak firewallun konumu modemden sonra gelir. Şekil olarak ifade edersek Şekil 5.1 de görebiliriz.



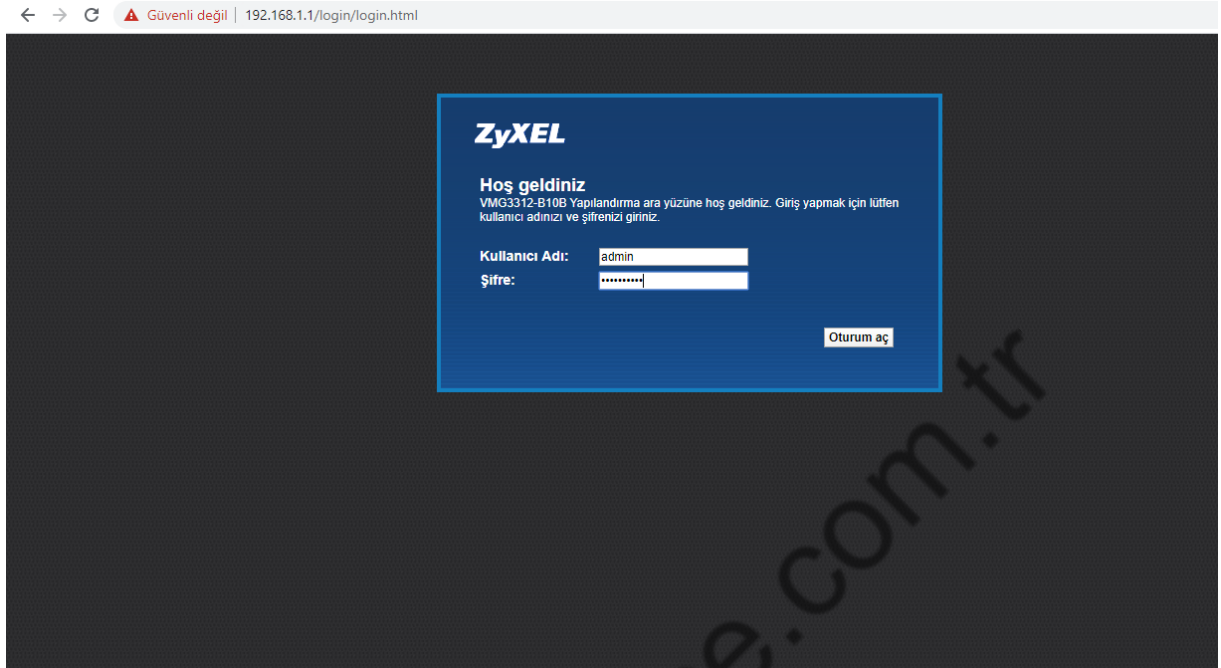
Şekil 5.1 1 Firewall Cihazının Şekilsel Olarak Konumu



Şekil 5.1 2 Firewall Portları

5.1.2 Modem Arayüze Giriş

Modemimizin arayüzüne giriş sağlıyoruz.



Şekil 5.1.2 1 Zyxel Marka Modemin Arayüzü

Modemlerimizin genel olarak default ip'leri 192.168.1.1 olmaktadır. Herhangi bir internet tarayıcısından modemimizin ip sini yazıp arayüze erişiyoruz. Kullanıcı adı şifreyi girdikten sonra ayarlarımıza devam ediyoruz.

Genel olarak modem kullanıcı adları “admin” olmaktadır.

Şifreleri ise genel olarak “admin” olmaktadır.

Kullanıcı adı şifreler marka ve modellere göre değişiklik gösterebilir

5.1.3 Modemi Bridge Moda Alma

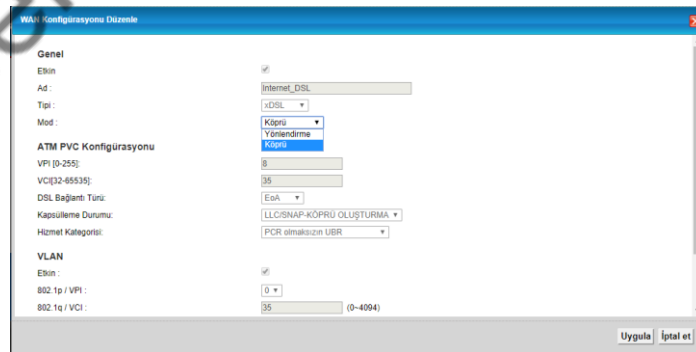
Modemimizi Bridge moda (Köprü) alıyoruz ki internete daha hızlı ve daha güvenli çıkış sağlayabilelim



Şekil 5.1.3 1 Bridge Mode Kurulum Ekranı 1



Şekil 5.1.3 2 Bridge Mode Kurulum Ekranı 2



Şekil 5.1.3 3 Bridge Mode Kurulum Ekranı 3

Uygula dedikten sonra modemimiz kendini bridge moda geçirir ve artık firewall tarafında kurulumu devam edebilir.

5.2 Berqnet Arayüz Girişi

Berqnetin varsayılan arayüz ip si 192.168.12.1 dir

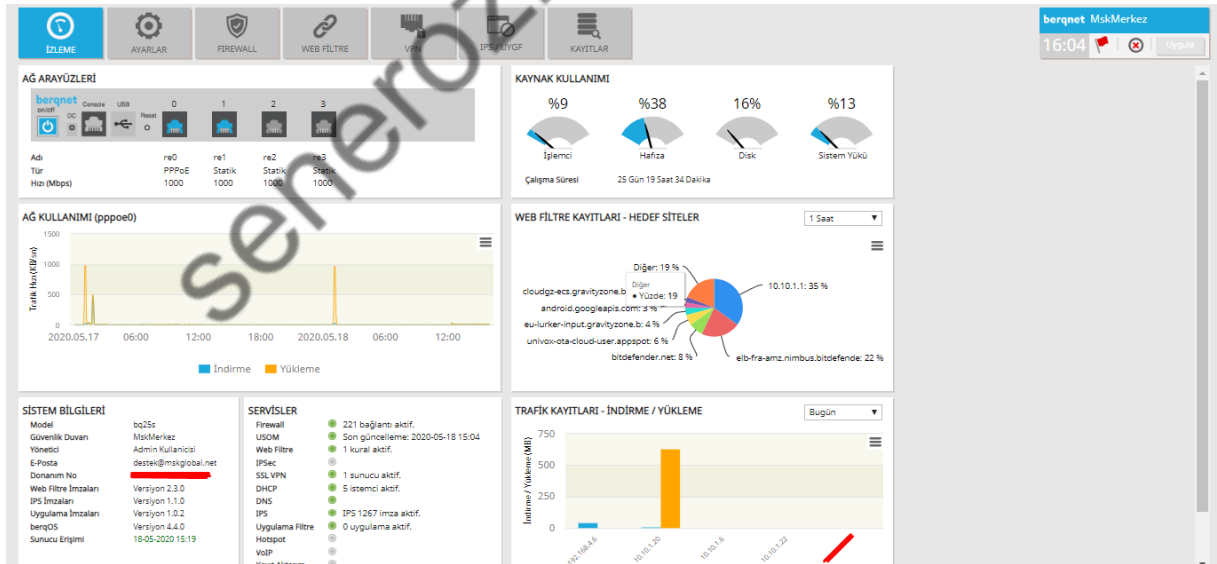
İnternet tarayıcısı üzerinden ip yi yazıp giriş yaptıktan sonra arayüz ekranı gelmektedir



Şekil 5.2 1 Berqnet Arayüzü

Berqnet kullanıcı adı “berqNET” şifre “berqNET” dir.

Giriş sekmesine basarak girişimizi sağlayabiliriz.



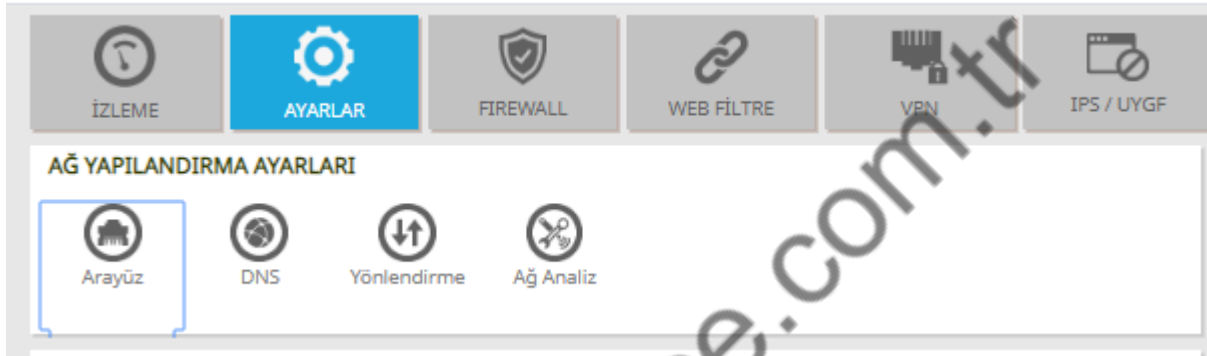
Şekil 5.2.2 Berqnet Karşılama Ekranı

5.3 Berqnet Network Ayarları

Local networkünüzdeki cihazların internete ulaşabilmesi için bu ayarları yapmamız gerekmektedir

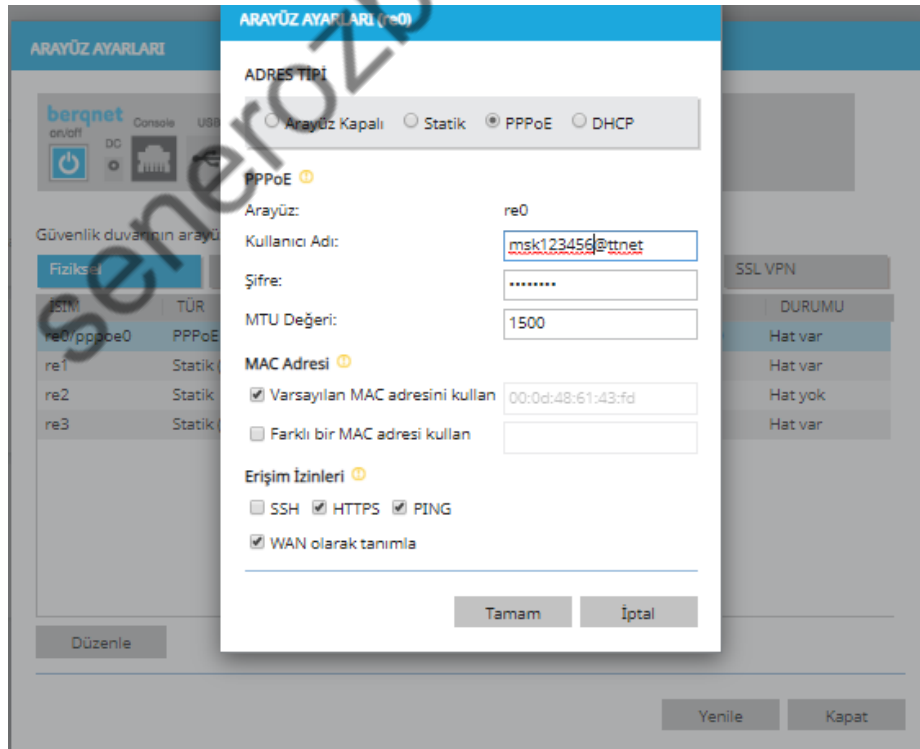
5.3.1 Wan Ayarları

Wan ayarında ISS sağlayıcımızın bize vermiş olduğu kullanıcı adı şifresini girmemiz gerekmekte, bu kullanıcı adı ve şifreyi ISS sağlayıcımızı arayarak ulaşabiliriz.



Şekil 5.3.1.1 Wan Kurulumu 1

Ayarlar Sekmesine tıklayıp Arayüz sekmesine tıklayarak



Şekil 5.3.1.2 Wan Kurulumu 2

ISS hizmeti aldığımız firmadan kullanıcı adı şifrenizi giriniz.

Erişim izinlerinizi Check Box'dan işaretleyin

Wan olarak tanımlayacağımız için bu portu “WAN olarak tanımla” Check boxına tıklayarak tamama basın.

5.3.2 Lan Ayarları

Lan ayarları için wandaki gibi arayüz ayarlarından em1 interfacesi ni seçip gerekli ayarları yapıyoruz

The image shows two screenshots of the MikroTik WinBox LAN configuration interface. The left screenshot shows the 'ADRES TİPİ' (Address Type) tab with 'Statik' (Static) selected. It displays fields for 'IP Adresi' (192.168.12.22) and 'Ağ Maskesi' (255.255.255.0). The 'Erişim İzinleri' (Access Permissions) section has checkboxes for SSH, HTTPS, and PING, all of which are checked. The 'WAN' section has a checkbox for 'WAN olarak tanımla' (Mark as WAN) which is unchecked. The 'Alias' section has a text box for 'Bu arayüz için birden fazla IP tanımlayabilirsiniz.' (You can define multiple IP addresses for this interface). The right screenshot shows the 'DHCP' tab selected. It displays fields for 'Ağ Aralığı' (IP Range) set to 192.168.12.2-192.168.12.254, 'Ağ Maskesi' (255.255.255.0), 'Alan Adı' (Domain Name), 'Ağ Geçidi' (Gateway) set to 192.168.12.1, 'DNS 1' (192.168.12.1), 'DNS 2', 'Yenileme Süresi' (720), and 'Ping kontrolü yapilsın.' (Ping control is performed) which is checked. Both screenshots have 'Tamam' (OK) and 'İptal' (Cancel) buttons at the bottom.

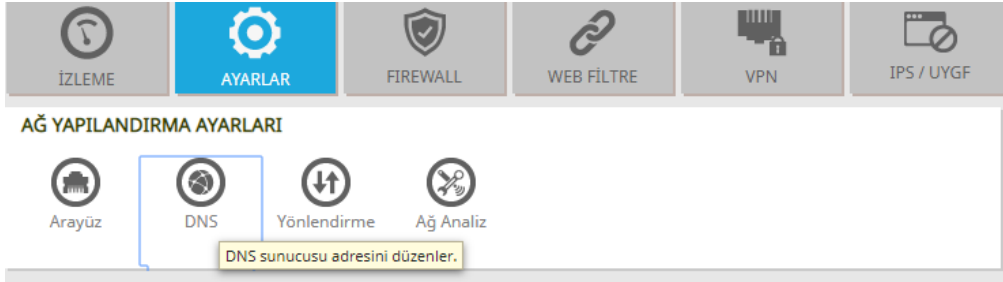
Şekil 5.3.2.1 Lan ayarları kurulumu

Burada ip adreslerini ağ geçitlerini ve erişim izinlerini yapıyoruz.

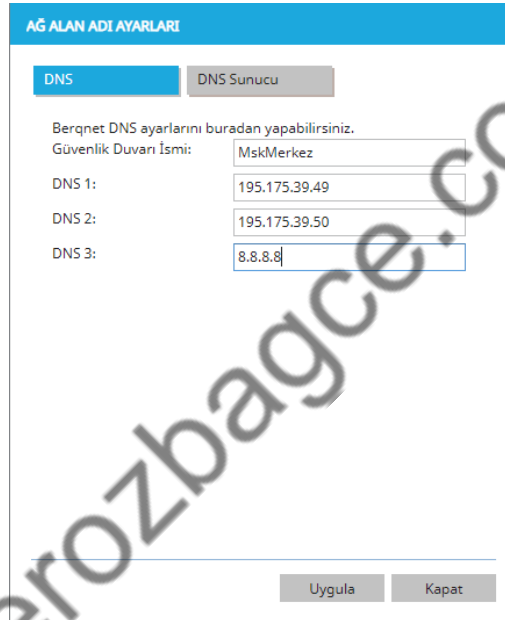
Sonra DHCP sekmesine basıp lan bacağımızda ip aralığımızı ağ maskemizi, ağ geçidimizi ve DNS ayarlarını yapıyoruz.

5.4 DNS Ayarları

DNS Ayarlarını yapmak için Ayarlar kısmından DNS i seçerek başlayabiliriz



Şekil 5.4.1 DNS Ayar Ekranı



Şekil 5.4.2 DNS Kurulum Ekranı

Berqnetin lisansı çekmesi için internete çıkması gerekli bu yüzden dns ayarlarını giriyoruz

Benburada türktelekom ve Google dns adreslerini girdim.

AĞ ALAN ADI AYARLARI

DNS DNS Sunucu

DNS Sunucu ayarlarını buradan yapabilirsiniz.

Aktif: ☒

DNS 1: 8.8.8.8

DNS 2: 8.8.4.4

DNS 3:

Statik DNS Kaydı:

HOST/DOMAIN İSMİ	IP
------------------	----

+ ✓ ✗

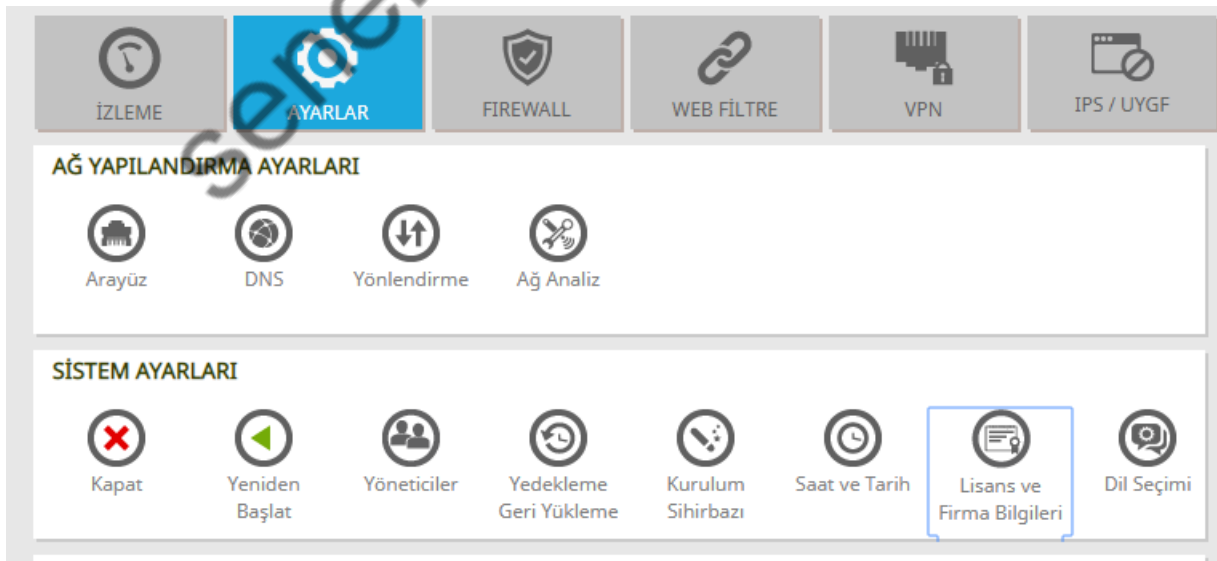
Uygula Kapat

Şekil 5.4.3 DNS Sunucu Kurulum Ekranı

Burada ise dhcp sunucumuzda dns adresine 192.168.12.1 olarak berqnetin kendisini göstermiştik bu dns adresinin yönlendirildiği yer. Ben burada 192.168.12.1 dns'ini Google a yönlendirdim.

5.5 Berqnet Lisans İşlemleri

Berqnet lisans işlemlerini bayiler temin etmektedir. Öncelikle hangi bayi üzerinden cihazı satın aldıysanız onlarla iletişime geçiyorsunuz, normalde cihazı aldığınızda bayi kurulum ekibi cihazı lisanslayıp teslim ediyor.



Şekil 5.5.1 Berqnet Lisans Ekranı Girişi

LİSANS VE FİRMA BİLGİLERİ

Firma Bilgileri Mevcut Lisanslar Lisans Anahtarı

Lütfen cihazınızın firma bilgilerinizi girerek kaydediniz.

İş Ortağı Bilgileri

Kullanıcı Adı: destek@mskglobal.net

Şifresi:

Ara Töptan Adı: ▼

Son Kullanıcı Bilgileri

Firma Adı: MSK GLOBAL

Yetkili Ad Soyadı: Şener ÖZBAĞÇE

Telefon: 902129890675

Eposta Adresi: info@mskglobal.net

İli: İstanbul ▼

İlçesi: Kağıthane

Kaydet Kapat

Şekil 5.5.2 Son kullanıcı ve Bayi bilgileri

Lisans ve Firma bilgileri sekmesine basıp burada son kullanıcının bilgilerini giriyoruz. İlk kurulumda lisansı çekmesi için cihazın, portal bilgilerinizi giriyoruz. Portal internet sitesi olan portal.berqnet.com ‘daki kullanıcı adı şifre bilgilerini giriyoruz. Eğer lisans yenilemesi olacaksa lisans anahtarı kısmından bayinin verdiği lisans anahtarını giriyoruz.

LİSANS VE FİRMA BİLGİLERİ

Firma Bilgileri Mevcut Lisanslar Lisans Anahtarı

Lisans Anahtarı: 9999 9999 9999 9999 9999 Anahtar Sorgula

Kapat

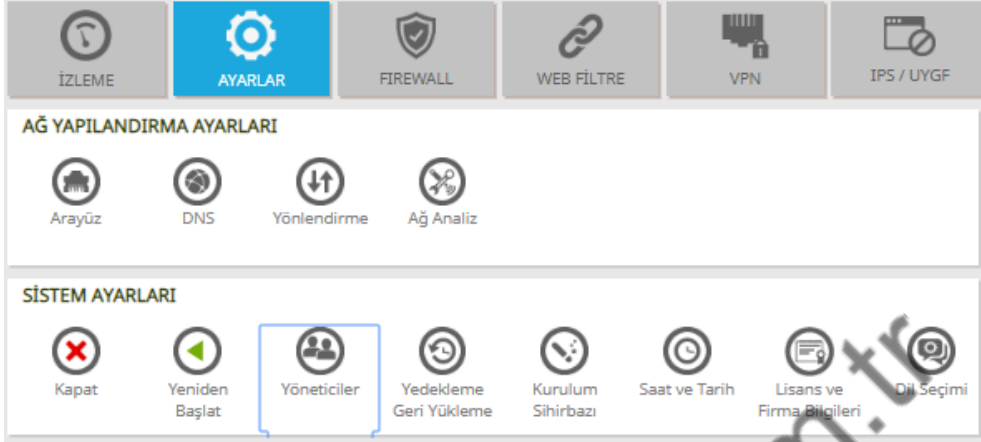
Şekil 5.5.3 Lisans Anahtarı Giriş

Lisans yenilemesi için lisans anahtarını buraya giriyoruz. “Anahtar Sorgula” butonuna basıp “Kapat” Butonuna basıyoruz.

Lisans ayarlarını yaptıktan sonra arayüzümüz yenilenir ve aktif olmayan butonlar aktifleşir.

5.6 Yönetici Ayarları

Yönetici ayarlarından kullanıcı adı şifrenizi değiştirebilir. Mobil raporlama uygulama bilgilerinizi ayarlayabilirsiniz.



Şekil 5.6.1 Yöneticiler Ayarları

Ayarlar > Yöneticiler butonundan girip



Şekil 5.6.2 Web Yönetici Ayar Ekranı

Ekle kısmından yeni kullanıcı ekleyebilir.

WEB ARAYÜZÜ KULLANICI DÜZENLEME

Kullanıcı Adı: sener

Tam Adı: Şener Özbağçe

E-Posta: sener@mskglobal.net

Şifre:

Şifre (Tekrar):

Açıklama: Teknik Destek Rapor Kullanıcısı

⚠ Yöneticilerin raporlama ayarlarını "Ayarlar->Bilgilendirme->Raporlama Ayarları" bölümünden yapabilirsiniz.

Tamam İptal

Şekil 5.6.3 Web Kullanıcı Ekleme

Düzenleme kısmından mevcut kullanıcıyı seçip mevcut şifrenizi girerek düzenleyebilir.

YÖNETİCİ AYARLARI

Web Mobil

KULLANICI ADI	ŞİFRE
beraNET	sener

+ ✓ ✗

Kapat

Şekil 5.6.4 Web Kullanıcı Düzenleme

WEB ARAYÜZÜ KULLANICI DÜZENLEME

berqNET isimli yöneticinizin bilgilerini düzenlemek için mevcut şifresini giriniz.

Mevcut Şifre:

Şekil 5.6.5 Web Kullanıcı Düzenleme Mevcut Şifre Ekranı

WEB ARAYÜZÜ KULLANICI DÜZENLEME

Kullanıcı Adı:

Tam Adı:

E-Posta:

Şifre:

Şifre (Tekrar):

Açıklama:

☐ Yöneticilerin raporlama ayarlarını "Ayarlar-> Bilgilendirme-> Raporlama Ayarları" bölümünden yapabilirsiniz.

Şekil 5.6.6 Web Kullanıcı Düzenleme Ekranı

İsterseniz mevcut kullanıcı adını değiştirebilir ve diğer bilgilerinizi düzenleyebilirsiniz.

Mobil kullanıcıları ise Mobil sekmesinden ayarlayabilirsiniz

YÖNETİCİ AYARLARI

Web Mobil

KULLANICI ADI

rapor

sener

Kapat

Şekil 5.6.7 Mobil Yönetici Ekranı

Yeni kullanıcı eklediğinizde akıllı cihazlarınızdan her anın mobil uygulamasına giriş yapabilirsiniz.

MOBİL KULLANICI DÜZENLEME

Kullanıcı Adı: rapor

Şifre: ****

Şifre (Tekrar): ****

Açıklama: Mobil rapor kullanıcısı

☐ Yönetici ☒ Normal

Tamam İptal

Şekil 5.6.8 Mobil Kullanıcı Ekleme Ekranı

Şekildeki gibi kullanıcı adı şifre bilgilerinizi giriyorsunuz açıklama kısmını doldurduktan sonra “Yönetici” veya “Normal” kullanıcı mı seçiyorsunuz.

Yönetici: Yönetici seçeneği uygulamada sadece cihazı yeniden başlatabilir özelliğini ekliyor uzaktan kullanıcı cihazı yeniden başlatabiliyor ve raporları görüntüleyebiliyor.

Normal: Normal kullanıcı ise sadece cihazı raporlayabiliyor.

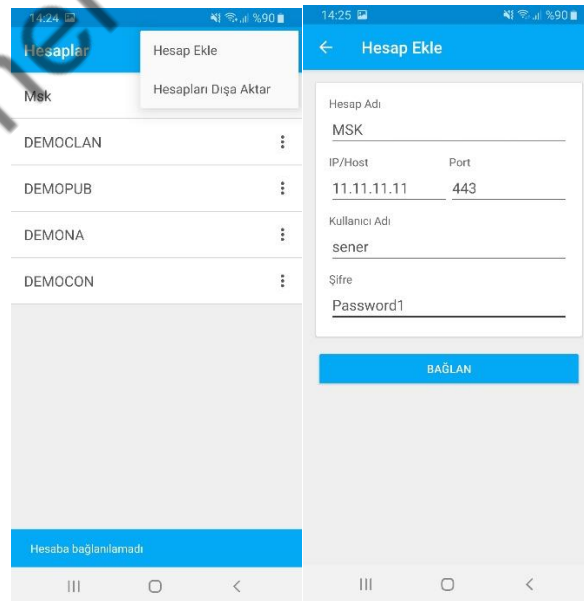
5.7 Berqnet Mobil Uygulama Kurulumu

Android ve IOS işletim sistemli akıllı cihazlarınızın uygulama indirme kısmından “Berqnet Rapor” uygulamasını indirebilirsiniz



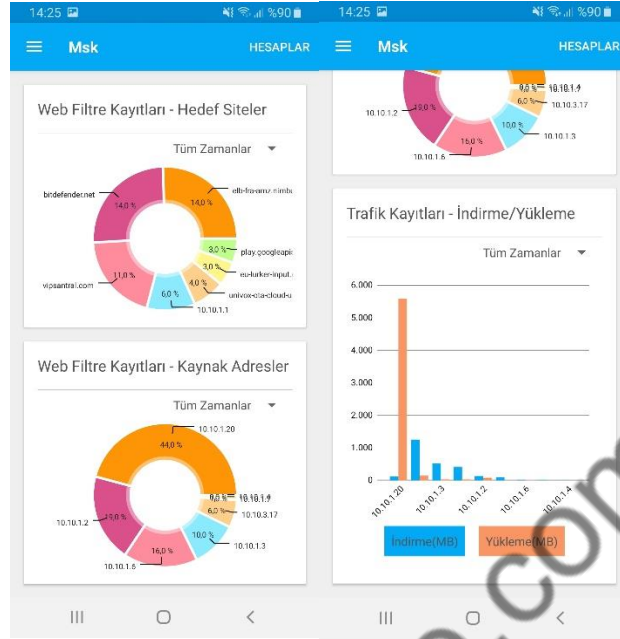
Şekil 5.7.1 Mobil Uygulama İndirme Ekranı

Uygulamayı indirdiğinizde uygulamayı açalım ve sağ taraftaki üç nokta kısmından Hesaap ekle diyelim.



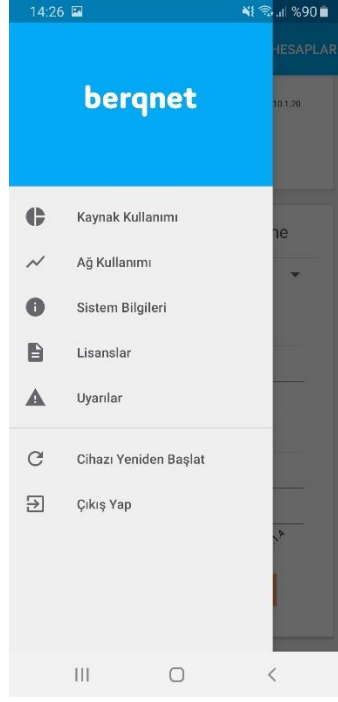
Şekil 5.7.2 Mobil Uygulama Hesap Ekleme

Cihaza bağlandığımızda ilk olarak grafik ekranları gelir, web filtre kayıtlarını ve kaynak adresleri buradan grafik şekillerle görebiliriz.



Şekil 5.7.3 Mobil Uygulama Grafik Ekranı

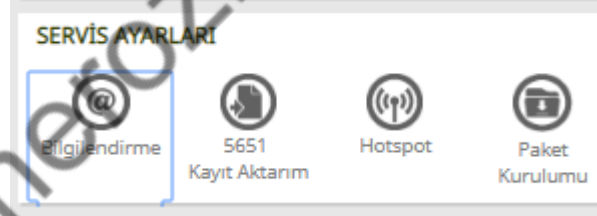
Cihaz isminin solundaki 3 çizgi işaretine basarak menüye ulaşabiliriz. Menü aşağıdaki gibidir.



Şekil 5.7.4 Mobil Uygulama Menü Ekranı

Bu menüde gösterilen tüm bilgilere tek tıkla kolay şekilde ulaşabilirsiniz.

5.8 Bilgilendirme Servisi



Şekil 5.8.1 Bilgilendirme Servis Ekranı

Bilgilendirme servisi ile berqnet cihazına mail attırabiliriz

BİLGİLENDİRME AYARLARI

E-Posta Ayarları Raporlama Ayarları

Bu bölümde e-postaları gönderen hesabın sunucu ayarlarını yapmaktasınız.
Güvenlik aşamaları içermeyen bir mail hesabı kullanınız.

Aktif: ☒

Gönderici Hesabı:

Şifre:

E-Posta Sunucu Adresi:

Port:

Bağlantı Türü: ☒ TLS ☐ SSL ☐ SMTP

☒ Uyarı mesajlarının, Logo Siber Güvenlik'e de gönderilmesini kabul ediyorum.

Şekil 5.8.2 Bilgilendirme E-posta Ayarları Ekranı

Gönderici hesabı şifrenizi ve gerekli diğer mail ayarlarını yaptıktan sonra raporlama ayarlarından hangi kullanıcılara rapor gitmesini ve hangi tür raporların gitmesini istiyorsanız onu seçin.

BİLGİLENDİRME AYARLARI

E-Posta Ayarları **Raporlama Ayarları**

KULLANICI ADI

admin

Şekil 5.8.3 Bilgilendirme Kullanıcı Ekranı

Kullanıcıyı seçip düzenle diyerek aşağıdaki ekrana gelip gerekli işaretlemeleri yapabilirsiniz.

KULLANICI DÜZENLEME

Kullanıcı Adı:

Tam Adı:

E-Posta:

Açıklama:

Rapor Türü:

- ☒ Sistem Uyarıları
- ☒ Web Filtre
- ☒ Uygulama Filtre
- ☒ Trafik Kayıtları
- ☒ Filtre Kayıtları
- ☒ Antivirüs
- ☒ IPS
- ☒ IDS

Raporlama Aralığı:

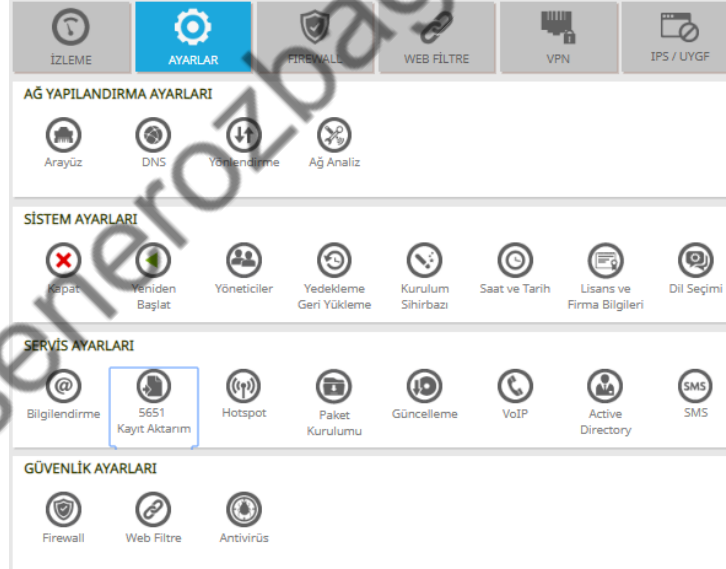
- ☐ Günlük
- ☒ Haftalık
- ☐ Aylık

Şimdi Gönder

Bu kullanıcının bilgilerini yöneticiler bölümünden değiştirebilirsiniz.
 Sistem Uyarıları raporlama aralığına bağlı olmadan çalışır.

Şekil 5.8.4 Bilgilendirme Kullanıcı Düzenleme Ekranı

5.9 5651 Kayıt Aktarım Servisi



Şekil 5.9.1 5651 Kayıt Aktarım Ekranı

Ayarlar>5651 Kayıt Aktarım seçeneğine tıklıyoruz. Burada paylaşıma açılmış bir dosyaya yada usb belleğe log kayıtlarının alınmasını, başka bir marka firewall dan log alımı veya başka bir syslog sunucuya log gönderimi ve damgalama ayarlarını yapıyoruz.

5651 VE KAYIT AKTARIM

5651 ve Kayıt Aktarım

Giriş
①

Aktarım
②

...

5651 ve Kayıt Aktarım

5651 ve Kayıt aktarım ayarlarını buradan gerçekleştirebilirsiniz.

Kayıt Aktarım Servisi: Pasif

Depolama Tipi: -

Zaman Damgası: Pasif

Kullanılan Kontör: 0

Kalan Kontör: 0

Şimdi Çalıştır

Devam etmek için lütfen İleri düğmesine tıklayınız.

Kayıt aktarım ayarını seçiniz.

☒ Açık
☐ Kapalı

Periyodik dışarı aktarım saatini seçiniz. ⌚

23 : 59

Geri

İleri

İptal

berqnet

Şekil 5.9.2 5651 Kayıt Aktarım Saat Ayarı Ekranı

5651 ve Kayıt Aktarım

Giriş
①

Aktarım
②

Paylaşım
③

Kayıtlar
④

Uzak Sunucu
⑤

Damga
⑥

Uygula
⑦

Kayıtların aktarılaacağı Windows bilgisayarınızın paylaşım alanına erişmek için aşağıdaki bilgileri giriniz.

Depolama Tipi: Paylaşım Alanı

IP Adresi: 192.168.1.10

Bilgisayar Adı: MYCOMPUTER

Paylaşım Adı: 5651

Kullanıcı Adı: SENER-PC

Şifre:

Bağlantı Testi

Depolama tipini seçiniz

berqnet

Geri

İleri

İptal

Şekil 5.9.3 5651 Kayıt Aktarım Paylaşım Ekranı

Burada Windows bir makinede paylaşıma açtığınız klasöre depolayabilir veya “Depolama Tipi” kısmında USB Belleği seçebiliriz.

Şekil 5.9.4 5651 Kayıt Aktarım Kayıtlar Ekranı

Şekil 5.9.5 5651 Kayıt Aktarım Uzak Sunucu Ekranı

Bu ekranda ise isterseniz başka bir firewall cihazından log alabilir isterseniz başka bir syslog sunucusuna logları gönderebilirsiniz.

Yöntem A: Log alımı için aşağıda ekle düğmesine basıp başka bir firewallın ipsini yazıp logları berqnet firewalla alabilirsiniz.

Yöntem B: Berqnet cihazınızdaki logları başka bir syslog sunucusuna gönderebilirsiniz.

5651 ve Kayıt Aktarım

Giriş ① Aktarım ② Paylaşım ③ Kayıtlar ④ Uzak Sunucu ⑤ **Damga ⑥** Uygula ⑦

Zaman Damgası için kullanıcı adı ve şifre bilgilerinizi giriniz.

Zaman Damgası:

Kullanıcı Adı:

Şifre:

☐ Kontör Sayacını Sıfırla

berqnet

Şekil 5.9.6 5651 Kayıt Aktarım Damga Ekranı

5651 ve Kayıt Aktarım

Giriş ① Aktarım ② Paylaşım ③ Kayıtlar ④ Uzak Sunucu ⑤ **Damga ⑥** Uygula ⑦

Zaman Damgası için kullanıcı adı ve şifre bilgilerinizi giriniz.

Zaman Damgası:

Kullanıcı Adı:

Şifre:

☐ Kontör Sayacını Sıfırla

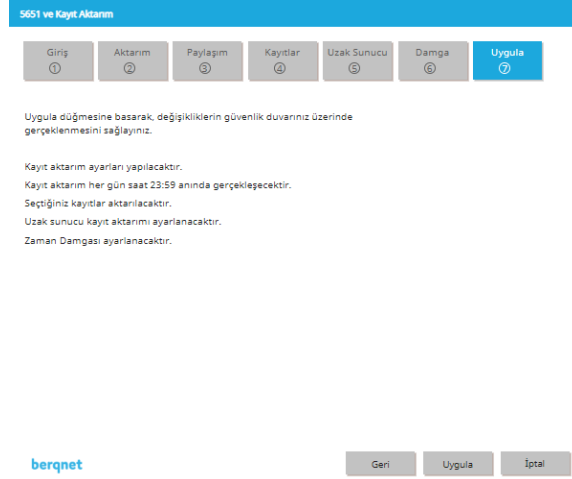
☐ Zaman Damgasının çalışabilmesi için "Ayarlar -> Sistem Ayarları -> Saat ve Tarih" ayarlarında otomatik zaman ayarlarının aktif olması gerekmektedir.

Zaman Damgası için şifre giriniz.

berqnet

Şekil 5.9.7 Kayıt Aktarım Damga Ekranı 2

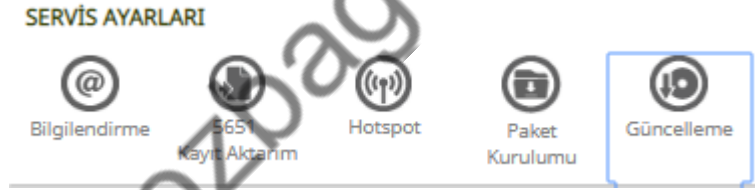
Burada zaman damgası için bilgileri giriyoruz. Burada daha önce Türktrast veya Tübitak'dan kontör almış olmanız gereklidir bunun için Tübitak veya Türktrast'ın sitelerini ziyaret edebilirsiniz.



Şekil 5.9.8 5651 Kayıt Aktarım Uygula Ekranı

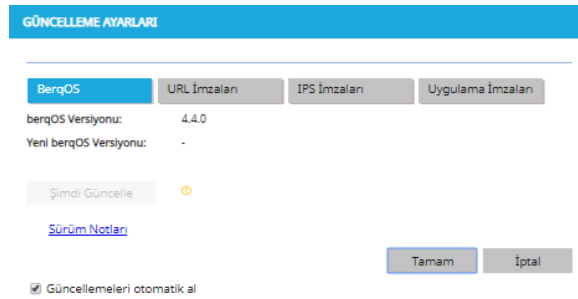
Son olarak uygula dediğimizde her gece 23.59 da logları damgalayıp dışarı almış olacaktır.

5.10 Berqnet ve Servis Güncellemeleri



Şekil 5.10.1 Güncelleme Ekranı

Ayarlar>Güncelleme kısmından girişimizi sağlıyoruz.



Şekil 5.10.2 BerqOS Güncelleme Ekranı

Burada yazılım ve diğer servislerin sürümlerini görebiliyoruz, “Güncellemeleri otomatik al” checkbox ile otomatik güncelleme alabilirsiniz.

5.11 VOIP Ayarları

Eğer mevcut sisteminizde voip hat kullanıyorsanız bu ayarları yapmanız gerekecektir.

Şekil 5.11.1 VOIP Ayar Ekranı

Yukarıdaki şekilde görüldüğü üzere RTP port aralığını, SIP portunu, iç ve dış bacaklarını seçip “VOIP bağlantısı için gerekli Firewall kurallarını oluştur” Checkboxuna tıklayıp ayarları kaydetmiş olursunuz.

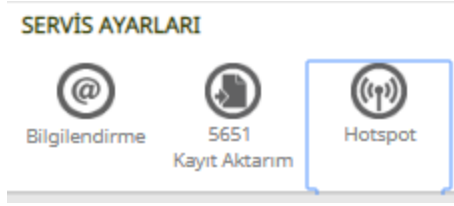


Şekil 5.11.2 Uygula Butonu

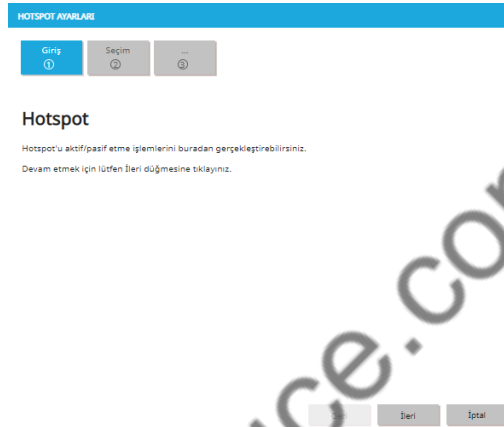
Yaptığınız her ayar sonrası aktifleşen “Uygula” Butonuna basmayı unutmayınız. Ayarların tamamen kaydedilmesi için bu tuşa basmanız gerekmektedir.

5.12 Hotspot Ayarı

Hotspot için Ayarlar>Hotspot kısmına gelmeniz lazım.

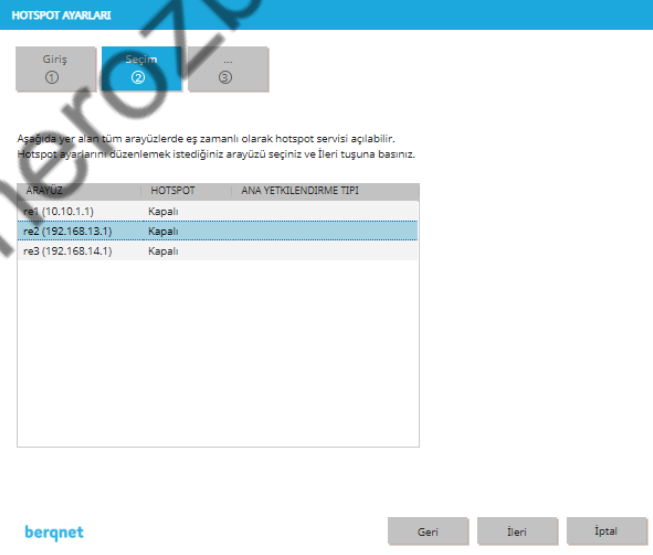


Şekil 5.12.1 Hotspot Ayar Ekranı



Şekil 5.12.2 Hotspot Ayar Ekranı 2

İçine girdikten sonra karşımıza çıkan ekran bu buradan “İleri” sekmesine basıyoruz.



Şekil 5.12.3 Hotspot Port Seçim Ekranı

Hangi portumuzu istiyorsak ona tıklıyoruz. Burada sadece o port hotspot için ayrılıyor bu yüzden birden çok accesspoint iniz var ise access pointlerinizi bir switch'e bağlayıp ayırdığımız portu switch'e takmanızı önerebilirim.

HOTSPOT AYARLARI (re3)

Giriş ① Seçim ② **Durum ③** ... ④

Bu ekranda hotspot servisini aktif/pasif hale getirebilir, hotspot servisinin hariç tutmak istediğiniz kullanıcıların MAC adreslerini girebilirsiniz.

Hotspot Aktif ☒

MAC Adresleri

İSM	HARİÇ TUTULAN MAC ADRESLERİ
-----	-----------------------------

berqnet

Geri İleri İptal

Şekil 5.12.4 Hotspot Durum Ekranı

İlerlediğimizde karşımıza yukarıda şekildeki gibi ekran gelmektedir. Burada “Aktif Et” Butonuna bastığımızda aktif ediyoruz ve hariç tutulacak MAC adreslerini buradan ekleyebilirsiniz.

HOTSPOT AYARLARI (re3)

Giriş ① Seçim ② Durum ③ **Yöntemler ④** ... ⑤

Kullanmak istediğiniz hotspot yetkilendirme yöntemlerini seçiniz. Yetki yöntemleri kullanıcı arayüzünde bu listede yer aldıkları sırayla gösterilecektir.

Okları kullanarak listedeki yerleri değiştirebilirsiniz. Aynı sırada yer alan yetkilendirmelerde çok doğrulamalı giriş yapılacaktır.

ANA YETKİLENDİRME		EK YETKİLENDİRMELER	
☐	Yabancı Kimlik	☐	Erişim Şifresi
☐	Otel	☐	Erişim Şifresi
☐	Manual	☐	Erişim Şifresi
☐	SMS	☐	Erişim Şifresi
☒	TC Kimlik	☐	Erişim Şifresi

berqnet

Geri İleri İptal

Şekil 5.12.5 Hotspot Yöntem Ekranı

Burada ise yetkilendirmeleri seçebiliriz. Manuel kullanıcı oluşturabilir, TC ve Yabancı Kimlik ile giriş sağlayabiliriz ek olarak kullanıcıların telefonuna sms ile kod gönderebiliriz. Bu ayarları ilgili checkbox ları işaretleyerek ayarlayabiliriz.

Şekil 5.12.6 Hotspot Arayüz Yönetici Oluşturma Ekranı

Bu kısımda ise hotspot kısmının arayüzü için kullanıcı oluşturuyoruz. Bu kısımda hotspot kullanıcılarını görebilir ve düzenleyebiliriz.

Şekil 5.12.7 Hotspot Oturum Ekranı

Bu kısımda sözleşme metnini, eş zamanlı oturum sayısını, internet erişim süresini gibi ayarları ayarlayabiliriz.

HOTSPOT AYARLARI (re3)

Seçim (2) Durum (3) Yöntemler (4) Yönetici (5) Oturum (6) **Kullanıcı (7)** Uygula (8)

Kullanıcı arayüzünde yapmak istediğiniz aşağıdaki değişiklikleri seçiniz.

ARKA PLAN MÜŞTERİ LOGOSU ARAYÜZ İÇERİK

Arka Plan: ☐ Varsayılan ☒ Özelleştirilmiş

Sayfa Rengi:

Başlık Rengi:

Başlık Metin Rengi:

Panel Rengi:

Panel Metin Rengi:

Buton Rengi:

Buton Metin Rengi:

berqnet

Geri İleri İptal

Şekil 5.12.8 Hotspot Arayüz Düzenleme Ekranı 1

Kullanıcının girdiği portalda görebileceği başlıkların renklerini vs. burada ayarlayabilir ve kendi şirketinizin logosunu koyabilir ve bu başlıkları ve alan kısımlarını arayüz kısmından dil seçeneklerinden ayarlayabilirsiniz.

Kullanıcı arayüzünde yapmak istediğiniz aşağıdaki değişiklikleri seçiniz.

ARKA PLAN **MÜŞTERİ LOGOSU** ARAYÜZ İÇERİK

Logo: ☒ Varsayılan ☐ Özelleştirilmiş

Logo Seçimi:

Şekil 5.12.9 Hotspot Arayüz Düzenleme Ekranı 2

Kullanıcı arayüzünde yapmak istediğiniz aşağıdaki değişiklikleri seçiniz.

ARKA PLAN MÜŞTERİ LOGOSU **ARAYÜZ İÇERİK**

Arayüz İçeriği: ☐ Varsayılan ☒ Özelleştirilmiş

DESTEKLENEN DİLLER

TÜRKÇE
ENGLISH
GERMAN
RUSSIAN

Düzenle Ekle Sil

SEÇİLEN DİLİ DÜZENLE

Dil Seçimi: TÜRKÇE

Alan Adı: Aktif Olmayan Kullanıcı Hatası

Özelleştirilmiş İçerik:

- Ayar Uygunsuzluğu Hatası Yazısı
- Başarılı Otel Kullanıcısı Oturum Açma Mesajı
- Başarılı Oturum Açma Bilgisi
- Başarılı Oturum Açma Mesajı
- Başarılı SMS Gönderme Mesajı
- Başarılı SMS Kullanıcısı Oturum Açma Mesajı
- Başarılı TC Kimlik Kullanıcısı Oturum Açma Mesajı
- Başarılı Yabancı Kimlik Kullanıcısı Oturum Açma Mesajı
- Başarısız Kullanıcı Oturum Açma Hatası
- Başarısız Manuel Kullanıcı Oturum Açma Hatası
- Başarısız Otel Kullanıcısı Oturum Açma Hatası
- Başarısız SMS Gönderme Hatası
- Başarısız SMS Kullanıcısı Oturum Açma Hatası
- Başarısız TC Kimlik Kullanıcısı Oturum Açma Hatası
- Başarısız Yabancı Kimlik Kullanıcısı Oturum Açma Hatası
- Bir IP hotspot kullanıcısı olarak daha önce giriş yapmış ise gösterilecek mesaj.
- Cep Telefonu Etiketli
- Cihaz Bulunamadı Yazısı
- Doğum Yılı Uyarı

Düzenle Ekle

Şekil 5.12.10 Hotspot Arayüz Düzenleme Ekranı 3

Arayüz içeriklerini, düzenle seçeneğine basıp alan adları kısmından teker teker gelecek olan mesajları düzenleyebilirsiniz. Bunu Türkçe hariç diğer diller için tek tek bölüm kısmından el ile yazmanız gerekmektedir. Cihazın içinde rusça, almanca ve diğer dil paketleri mevcut değildir el ile yazmanız gerekmektedir.

HOTSPOT AYARLARI(re3)

Seçim ② Durum ③ Yöntemler ④ Yönetici ⑤ Oturum ⑥ Kullanıcı ⑦ Uygula ⑧

Hotspot uygulama bilgisi

Hotspot arayüz seçimi yapılacaktır.
Hotspot seçilen arayüzde aktif edilecektir.
Seçilen hotspot kullanıcı yetkilendirme yöntemleri uygulanacaktır.
Yönetici arayüzü erişim bilgileri ayarlanacaktır.
Oturum ayarlarınız kaydedilecektir.
Kullanıcı arayüzü bilgileri ayarlanacaktır.

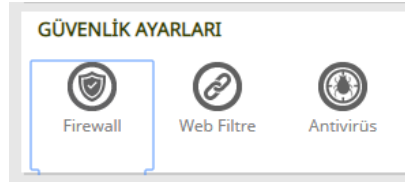
berqnet

Geri Uygula İptal

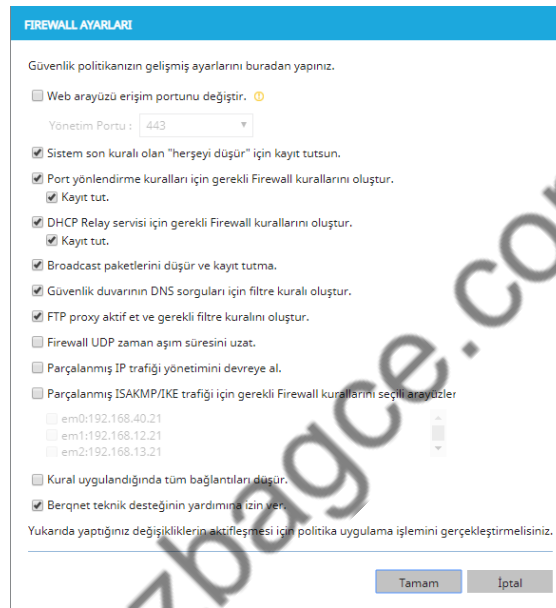
Şekil 5.12.10 Hotspot Uygulama Ekranı

Son olarak uygula dediğinizde ayarları uygulamış olacaksınız.

5.13 Firewall Ayarları

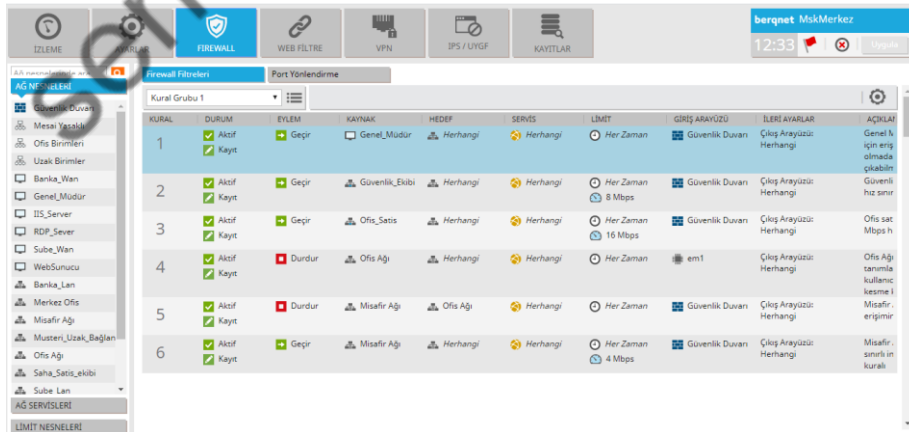


Şekil 5.13.1 Firewall Ayarlar Girişi



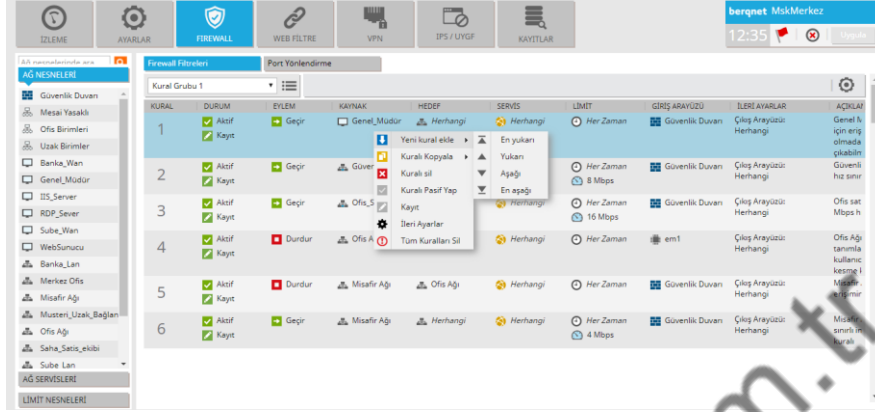
Şekil 5.13.2 Firewall Ayarlar Ekranı

Bu kısımdan istediğiniz ayarlar için checkboxu işaretlemeniz yeterlidir daha sonra,



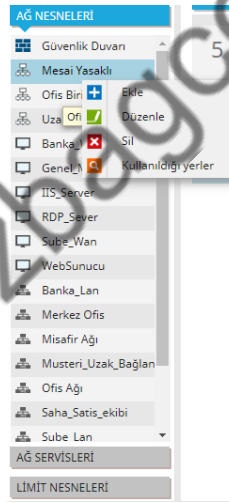
Şekil 5.13.3 Firewall Ayarı Ana Ekranı 1

Ayarların yanında firewall kısmına basarak yine ayarları sağlayabiliriz. Yukarıdaki şekilde daha önce yapılan kurallar mevcuttur. Bu kısımda isterseniz departmanlara ayırıp departmanlarınızı belirli saatler arasında internete çıkarıp belirli saatler arasında düşük hızlarda internete çıkmalarını sağlayabilirsiniz. Güvenmediğiniz ipleri de derseniz yine buradan yasaklayabilirsiniz.



Şekil 5.13.4 Firewall Ayarı Ana Ekranı 2

Yeni kural eklemek için mevcut bir kuralın üzerine sağ tıklayıp yeni kural oluşturabilirsiniz.



Şekil 5.13.5 Ağ Nesnesi Ekranı

Ağ nesneleri oluşturabilir düzenleyebilir ve silebilirsiniz.

Şekil 5.13.6 Ağ Nesnesi Ekranı

Eklemek istediğiniz türü seçebilirsiniz.

Şekil 5.13.7 Ağ Nesnesi Ekleme Ekranı

Örnek olarak bir nesne oluşturalım.

Şekil 5.13.8 Limit Nesnesi Ekranı

Oluşturduğumuz bu nesnede teknik servis çalışanlarımızın ip bloğunu nesne olarak ekledik

Limit nesnelerinden sağ tıklayıp zaman mı yoksa bant genişliğini eklemek istiyorsak onu seçiyoruz.

BANT GENİŞLİĞİ NESNESİ

İsim: 2 Mbps

Sınırlama: İndirme

Aktif: ☒

Maksimum: 250 KB/s

Garanti Edilen: 250 KB/s

Öncelik: Normal

Açıklama: Teknik Servis Hızı

Tamam İptal

Şekil 5.13.9 Bant Genişliği Nesnesi Ekranı

Bant genişliğini oluşturuyoruz. Ve artık sürükleyip bırak ile kuralımızı oluşturmaya başlıyoruz

ZAMAN NESNESİ

İsim: MESAI

Başlangıç Tarihi: 02.05.2020

Bitiş Tarihi: 05.09.2020

Periyot: Haftalık

☒ Pazartesi
☒ Salı
☒ Çarşamba
☒ Perşembe
☒ Cuma
☒ Cumartesi
☐ Pazar

Gün İçi Başlangıç Saati: Tümü

Gün İçi Bitiş Saati:

Açıklama:

Tamam İptal

Şekil 5.13.10 Zaman Nesnesi Ekranı

Zaman çizelgesi oluşturmak için ise yukardaki gibi nesne oluşturabiliriz.

4

Aktif Kayıt

Geçir

Teknik_LAN

Herhangi

Herhangi

MESAI

2 Mbps

Güvenlik Duvarı

Çıkış Arayüzü: Herhangi

Şekil 5.13.11 Firewall Kuralı

5.14 Port Yönlendirme

Bu kısımda port yönlendirmeyi göstereceğim.

Firewall Filtreleri		Port Yönlendirme					
Port yönlendirme kural grubu							
KURAL	DURUM	KAYNAK ADRES	GELEN SERVİS	GELİŞ ARAYÜZÜ	İLETİLEN SUNUCU	İLETİLEN SERVİS	AÇIKLAMA
1	☒ Aktif ☒ Kayıt	Herhangi	UDP5070	pppoe0	SANTRAL	UDP5070	Dış ağdan iç web sunucusuna yönlendirme
2	☒ Aktif ☒ Kayıt	Herhangi	60000-61000	pppoe0	SANTRAL	60000-61000	
3	☒ Aktif ☒ Kayıt	Herhangi	KAMERA	pppoe0	NVR	KAMERA	

Şekil 5.14.1 Port Yönlendirme Ekranı

Firewall ayarlarında port yönlendirmeyi seçiyoruz.

Örnek olarak bir uygulama göstereceğim.

AG NESNESİ

İsim:

NVR

Tür:

Uç birim

IP:

10.10.3.10

☐ Hariç (İçermeyen)

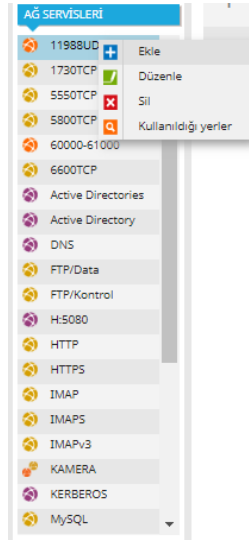
Açıklama:

Tamam

İptal

Şekil 5.14.2 Ağ Nesnesi Ekranı

Ağ nesnesi oluşturuyoruz, şirketimizde güvenlik kamerasını dışarda izlemek için ip sini ve ismini yazıyoruz daha sonra.



Şekil 5.14.3 Ağ Servisleri Ekranı

Ağ servislerinden portları oluşturmak için sağ klik yapıp ekle tuşuna basıyoruz.

Şekil 5.14.4 Port Ekleme Ekranı

Açılan sekmede port türünü seçiyoruz.

Şekil 5.14.5 Port Ekleme Ekranı

Kayıt cihazımızın tüm portlarını bu şekilde açtıktan sonra

SERVİS NESNESİ

İsim: Servis

Tür: TCP

☐ Kaynak Port:

☒ Hedef Port:

Açıklama:

Servis Grubu

Tamam İptal

Şekil 5.14.6 Port Ekleme Ekranı

Servis nesnelerinde tekrar ekle diyerek port grubu oluşturacağız. Yukarıda ki servis grubunu seçtikten sonra aşağıdaki şekildeki gibi ekran karşımıza çıkacak. Sol taraftaki pencerede portları seçip ortada bulunan yön tuşuyla sağ tarafa atabilir ve oluşturabiliriz.

SERVİS NESNESİ

İsim: KAMERA

Tür: Servis Grubu

Grup Dışı

- 60000-61000
- 6600TCP
- Active Directories
- Active Directory
- DNS
- FTP/Data
- FTP/Kontrol
- H:5080

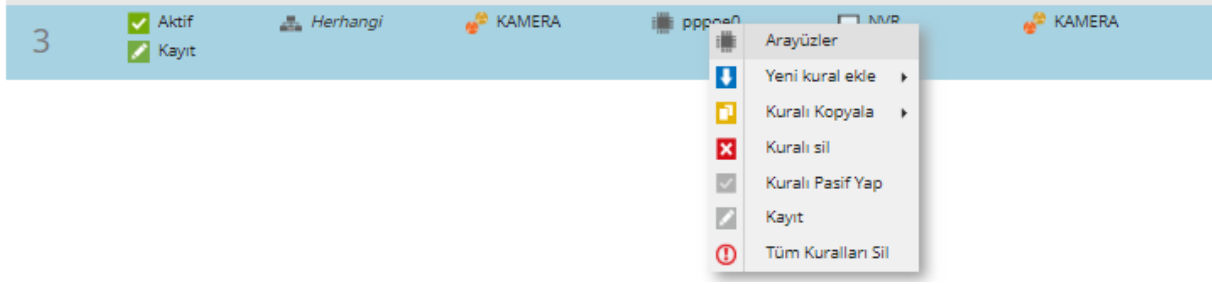
Grup Üyeleri

- 11988UDP
- 1730TCP
- 5550TCP
- 5800TCP
- HTTP

Açıklama:

Tamam İptal

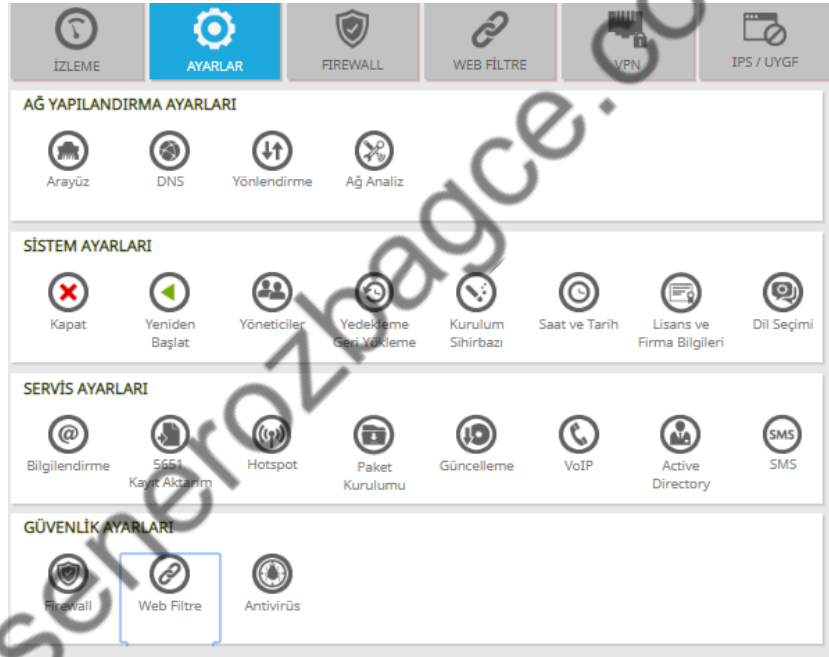
Şekil 5.14.7 Port Grubu Oluşturma



Şekil 5.14.8 Port Yönlendirme Kuralı

Yukarıda bulunan şekildeki gibi kuralımızı oluşturduğumuzda “Arayüzler” kısmında firewall cihazımızın wan bacağına yani pppoe bacağına seçip sağ en üstte bulunan uygula tuşuna basıyoruz.

5.15 Web Filtre Ayarları



Şekil 5.15.1 Ayarlar Ekranı

Ayarlar>Web Filtre kısmına giriyoruz öncelikle

WEB FİLTRELEME AYARLARI

Port Seçimi:

PORT LİSTESİ

80

+
✓
✗

☐ Web filtreden hariç tutmayı aktive etmek istiyorum.

HARIÇ DOMAIN/IP LİSTESİ

+
✓
✗

☒ USOM listesinde yer alan adresleri engelle 🔔

USOM Listesinden Hariç Tut

Engelleme Sayfası:

☒ Varsayılan engelleme sayfası
 ☐ Kişisel engelleme sayfası

```
<html>
<head>
<meta charset="utf-8">
<title>berqnet - Erişim engellendi</title>
<script>
```

☒ Web Filtreleme kayıtlarının tutulmasını istiyorum.

☐ Sadece engellenen sayfalar

☒ İçerik aramayı aktive etmek istiyorum.

☐ HTTPS taramayı aktive etmek istiyorum.

SSL Sertifikasını İndir

Tamam
İptal

Şekil 5.15.2 Web Filtreleme Ayarları Ekranı

Yukarıdaki gibi checkboxları işaretledikten sonra.

İZLEME	AYARLAR	FIREWALL	WEB FİLTRE	VPN	IPS / UYGF	KAYITLAR																																																	
Ağ nesnelerinde ara AĞ NESNELERİ - Güvenlik Duvarı - Mesaj Yasaklı - Ofis Birimleri - Uzak Birimler - Banka_Wan - Genel_Müdür - IIS_Server - RDP_Server - Sube_Wan - WebSunucu - Banka_Lan - Merkez Ofis - Misafir_Ağı - Musteri_Uzak_Bağla - Ofis_Ağı - Saha_Satis_ekibi - Sube_Lan - Uzak Ofis - Güvenlik_Ekibi ACTIVE DIRECTORY WEB NESNELERİ URL KATEGORİLERİ MEDYA FORMATLARI LİMİT NESNELERİ Web Filtreleme Kuralı Https Hariç Tutulanlar Antivirüs Hariç Tutulanlar <table border="1"> <thead> <tr> <th>KURAL</th><th>DURUM</th><th>KULLANICILAR</th><th>İZİN LİSTESİ</th><th>ENGELLEME LİSTESİ</th><th>LİMİT</th><th>AÇIKLAMA</th></tr> </thead> <tbody> <tr> <td>1</td><td>☒ Pasif</td><td>Genel_Müdür</td><td>Filtre Yok</td><td>Filtre Yok</td><td>Her Zaman</td><td>Genel Müdür kullanıcıları için full iznli internet erişim kuralı</td></tr> <tr> <td>2</td><td>☒ Pasif</td><td>Güvenlik_Ekibi</td><td>Filtre Yok</td><td>Filtre Yok</td><td>Öğle Arası</td><td>Güvenlik Ekibi için Öğle Arası Full iznli internet erişim kuralı</td></tr> <tr> <td>3</td><td>☒ Pasif</td><td>Güvenlik_Ekibi</td><td>Basın-Yayın www.whatsapp.com www.whatsapp.net</td><td>Tüm Siteler</td><td>Her Zaman</td><td>Güvenlik Ekibi için Sadece Whatsapp ve Haber sitelerine izin verilmesi kuralı</td></tr> <tr> <td>4</td><td>☒ Pasif</td><td>Ofis_Satis</td><td>Filtre Yok</td><td>Filtre Yok</td><td>Öğle Arası</td><td>Ofis Satis Ekibi için Öğle Arası Full iznli internet erişim kuralı</td></tr> <tr> <td>5</td><td>☒ Pasif</td><td>Ofis_Satis</td><td>Filtre Yok</td><td>Alışveriş Cinsel İçerik Engelleme Cinsellik Proxy</td><td>Her Zaman</td><td>Ofis Satis ekibi için Alışveriş Cinsellik ve Proxy kategorilerinin yasaklanması kuralı</td></tr> <tr> <td>6</td><td>☒ Pasif</td><td>Misafir_Ağı</td><td>Filtre Yok</td><td>Cinsel İçerik Engelleme Cinsellik Proxy</td><td>Her Zaman</td><td>Misafir Ağına Cinsellik ve Proxy kategorilerinin yasaklanması kuralı</td></tr> </tbody> </table>							KURAL	DURUM	KULLANICILAR	İZİN LİSTESİ	ENGELLEME LİSTESİ	LİMİT	AÇIKLAMA	1	☒ Pasif	Genel_Müdür	Filtre Yok	Filtre Yok	Her Zaman	Genel Müdür kullanıcıları için full iznli internet erişim kuralı	2	☒ Pasif	Güvenlik_Ekibi	Filtre Yok	Filtre Yok	Öğle Arası	Güvenlik Ekibi için Öğle Arası Full iznli internet erişim kuralı	3	☒ Pasif	Güvenlik_Ekibi	Basın-Yayın www.whatsapp.com www.whatsapp.net	Tüm Siteler	Her Zaman	Güvenlik Ekibi için Sadece Whatsapp ve Haber sitelerine izin verilmesi kuralı	4	☒ Pasif	Ofis_Satis	Filtre Yok	Filtre Yok	Öğle Arası	Ofis Satis Ekibi için Öğle Arası Full iznli internet erişim kuralı	5	☒ Pasif	Ofis_Satis	Filtre Yok	Alışveriş Cinsel İçerik Engelleme Cinsellik Proxy	Her Zaman	Ofis Satis ekibi için Alışveriş Cinsellik ve Proxy kategorilerinin yasaklanması kuralı	6	☒ Pasif	Misafir_Ağı	Filtre Yok	Cinsel İçerik Engelleme Cinsellik Proxy	Her Zaman	Misafir Ağına Cinsellik ve Proxy kategorilerinin yasaklanması kuralı
KURAL	DURUM	KULLANICILAR	İZİN LİSTESİ	ENGELLEME LİSTESİ	LİMİT	AÇIKLAMA																																																	
1	☒ Pasif	Genel_Müdür	Filtre Yok	Filtre Yok	Her Zaman	Genel Müdür kullanıcıları için full iznli internet erişim kuralı																																																	
2	☒ Pasif	Güvenlik_Ekibi	Filtre Yok	Filtre Yok	Öğle Arası	Güvenlik Ekibi için Öğle Arası Full iznli internet erişim kuralı																																																	
3	☒ Pasif	Güvenlik_Ekibi	Basın-Yayın www.whatsapp.com www.whatsapp.net	Tüm Siteler	Her Zaman	Güvenlik Ekibi için Sadece Whatsapp ve Haber sitelerine izin verilmesi kuralı																																																	
4	☒ Pasif	Ofis_Satis	Filtre Yok	Filtre Yok	Öğle Arası	Ofis Satis Ekibi için Öğle Arası Full iznli internet erişim kuralı																																																	
5	☒ Pasif	Ofis_Satis	Filtre Yok	Alışveriş Cinsel İçerik Engelleme Cinsellik Proxy	Her Zaman	Ofis Satis ekibi için Alışveriş Cinsellik ve Proxy kategorilerinin yasaklanması kuralı																																																	
6	☒ Pasif	Misafir_Ağı	Filtre Yok	Cinsel İçerik Engelleme Cinsellik Proxy	Her Zaman	Misafir Ağına Cinsellik ve Proxy kategorilerinin yasaklanması kuralı																																																	

Şekil 5.15.3 Web Filtre Kural Ekranı

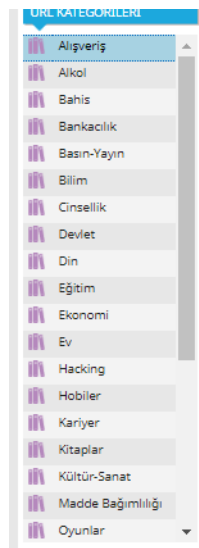
En üstte bulunan Web Filtre Kısımına basarak yukarıdaki şekildeki gibi ekran gelecek karşımıza.

Ağ nesneleri limit nesneleri firewall kurallarında olduğu gibi web filtre kurallarında da var ek olarak burada web nesneleri, URL kategorileri ve medya formatları var.

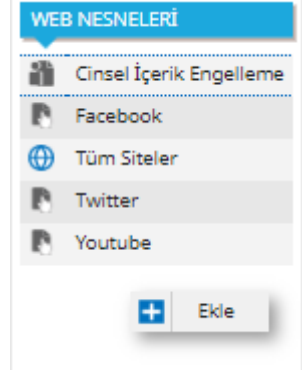


Şekil 5.15.4 Medya Formatları Ekranı

Medya formatlarında kullanıcıların kategorideki nesnelerin çalıştırıp çalıştıramayacağı nesneleri burada görüyoruz, sürükleyip bırak yöntemiyle kuralımıza ekleyebiliriz.



Şekil 5.15.5 URL Kategorileri Ekranı



Şekil 5.15.6 Web Nesneleri Ekranı

URL Kategorileri sayesinde hazırda bulunan URL listelerini kuralımıza ekleyebiliriz.

Şekil 5.15.7 Web Nesnesi Ekranı 1

Web nesnelerinde sağ klik>ekle diyerek yeni nesneler oluşturabiliriz.

Adres kısmından belirli bir adresi nesneleştiririz.

Şekil 5.15.8 Web Nesnesi Ekranı 2

Tür kısmından gruplar oluşturabilir, kelime kategorisi seçebilir, medya formatları ekleyebiliriz.

Şekil 5.15.9 Web Nesnesi Ekranı 3

Kelime kategorisinde engellemek istediğimiz kategorileri ekle tuşu ile ekleyebiliriz.

Şekil 5.15.10 Kelime Ekleme Ekranı

Kelime kategorilerini ekledikten sonra tamama basıp uygula diyerek kategorinizi kaydetmiş oluruz.

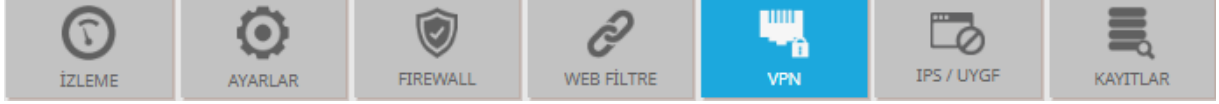
Web Filtreleme Kuralları		Https Hariç Tutulanlar		Antivirüs Hariç Tutulanlar		
Web Filtre Kural Grubu						
KURAL	DURUM	KULLANICILAR	İZİN LİSTESİ	ENGELLEME LİSTESİ	LİMİT	AÇIKLAMA
1	 Aktif	 LAN	 Filtre Yok	 Cinsel İçerik Engelleme  Cinsellik  Hacking  hack kelime engelleme  Sıkıştırma Dosyaları	 Her Zaman	Kullanıcılar, izin ve engelleme listelerine ilgili nesneler eklenerek Web Filtreleme kuralı oluşturulmuştur.

Şekil 5.15.11 Web Filtre Kuralı

Bu şekilde kuralınızı sürükleyip bırakarak oluşturabilirsiniz.

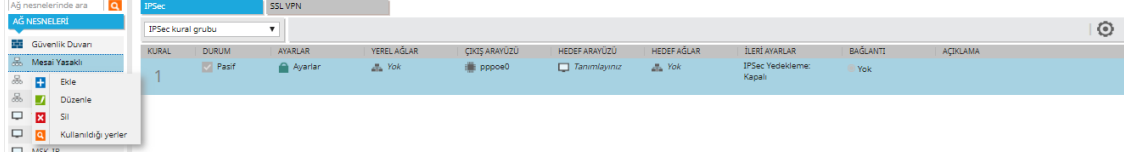
5.16 Ipsec Vpn Kurulumu

İki ofisi birbirine bağlamak için IPSEC VPN kullanırız bunun için aşağıdaki adımları uygulamamız gerekli.



Şekil 5.16.1 VPN Ekranı

Vpn ayarları sekmesine tıklıyoruz.



Şekil 5.16.2 VPN Düzenleme Ekranı

Öncelikle ağ nesneleri tabında güvenlik arayüzünü sürükleyip çıkış arayüzüne bırakıyoruz. Daha sonra sağ tıklayıp çıkış arayüzünü pppoe0 seçiyoruz. Ağ nesnelerinde kendi ağımızı oluşturup, ve karşı tarafın dış ip sini ekleyip yine ağ nesnelerinde uç birim ekleyerek bunu yapabilir, son olarak karşı tarafın networkunu yine ağ nesnelerinde ekleyerek ilgili yerlere sürükleyip bırakıyoruz. Aşağıdaki şekillerdeki gibi yapıyoruz.

Ağ Nesnesi

İsim: Sube_Msk

Tür: Uç birim

IP: 99.99.99.99

☐ Hariç (İçermeyen)

Açıklama: Karşı tarafın dış ipsini yazıyoruz

Tamam İptal

Şekil 5.16.3 VPN Ağ Nesnesi Ekranı 1

Ağ nesnelerinde sağ tıklayıp ekle dediğimizde uç birim olarak karşı tarafın ipsini giriyoruz ve tamama basıyoruz.

Şekil 5.16.4 VPN Ağ Nesnesi Ekranı 2

Yine ağ nesnelerinde ekle diyerek kendi ağıımızı ekleyebilir daha önce oluşturulmuşsa bu nesneyi ilgili yere sürükleyip bırak şeklinde yerine koyabilirsiniz.

Şekil 5.16.5 VPN Ağ Nesnesi Ekranı 3

Ağ nesneleri sekmesinde oluşturduğumuz karşı tarafın ip bilgilerini giriyoruz.

KURAL	DURUM	AYARLAR	YEREL AĞLAR	ÇIKIŞ ARAYÜZÜ	HEDEF ARAYÜZÜ	HEDEF AĞLAR	İLERİ AYARLAR	BAĞLANTI	AÇIKLAMA
1	☒ Pasif	Ayarlar	LAN	pppoe0	Sube_Msk	Sube_Lan	İLERİ AYARLAR IPSec Vedekleme: Kapalı	Yok	

Şekil 5.16.6 VPN Kural Ekranı

En son olarak gerekli yerlere ağ nesnelerini eklediğimizde yukardaki şekilde görüldüğü gibi oluyor.

Ayarlara çift tıklayıp karşı taraftaki güvenlik duvarı cihazınızda aynı ayarları ve şifreleri girilmiş olması gerekmektedir.

AYARLAR

Faz 1 Faz 2 Parametreler

Şifre Ayarları

Şifre:

Şifre (Tekrar):

IKE Ayarları

Bütünlük Algoritması: SHA1

Şifreleme algoritması: 3DES

DH Grubu (Anahtar Grubu): MODP1024 (2)

Tamam İptal

Şekil 5.16.7 VPN Karşılıklı Ayar Ekranı 1

Görüldüğü üzere şifre kısmında şifre girip IKE Ayarlarını şekildeki gibi yapıyoruz.

AYARLAR

Faz 1 Faz 2 Parametreler

ESP Ayarları

Bütünlük Algoritması:

- ☐ HMAC_MD5
- ☒ HMAC_SHA1
- ☐ HMAC_SHA256
- ☐ HMAC_SHA384
- ☐ HMAC_SHA512

Protokol:

- ☒ ESP
- ☐ AH

Şifreleme algoritması:

- ☐ DES
- ☒ 3DES
- ☐ AES 128
- ☐ AES 192
- ☐ AES 256

Tamam İptal

Şekil 5.16.8 VPN Karşılıklı Ayar Ekranı 2

Görüldüğü üzere aynı ayarları yapabilir veya farklı ayarları da seçip yapabilirsiniz önemli olan karşı taraftaki güvenlik cihazının da aynı ayarlara sahip olması.

AYARLAR

Faz 1 Faz 2 **Parametreler**

Zaman Aşımı/NAT Ayarları

IKE Zaman Aşımı: 28800

IPSec Zaman Aşımı: 3600

DPD Zaman Aşımı: 15

DPD Tekrar Sayısı: 5

☐ Kimlik Doğrulama Aktif

Yerel Kimlik (ID):

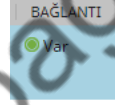
Hedef Kimlik (ID):

☐ NAT Traversal Aktif

Tamam İptal

Şekil 5.16.9 VPN Karşılıklı Ayar Ekranı 3

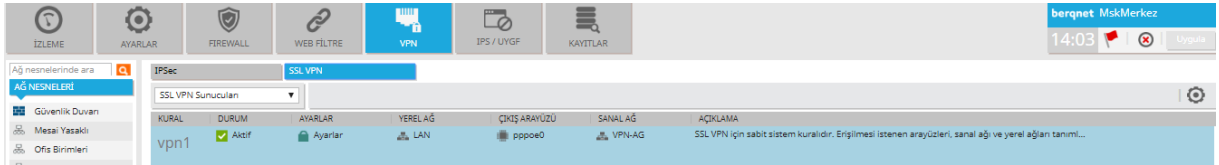
Gerekli ayarlamaları yaptıktan sonra tamam a basıp sağ üst tarafta bulunan uygula sekmesine basarak ayarları uygulayabilirsiniz. Aynı ayarları karşı taraftaki cihaz içinde yapmalısınız. Bağlantının sağlandığını



Şekil 5.16.10 Bağlantı Ekranı

5.17 Ssl Vpn Kurulumu

Kullanıcıların güvenli olarak bağlanması için ssl vpn kurmaktayız. Bu sayede evden çalışan arkadaşlarımız en güvenli şekilde evlerinden veya herhangi bir internet olan lokasyonda güvenli olarak sanki şirketteymiş gibi çalışabilir, ortak klasörlere vs. şeklinde ulaşabilirler. Bunun için aşağıdaki adımları takip etmelisiniz.



Şekil 5.17.1 SSL VPN Kuralı

Öncelikle VPN ayarlarına basıp SSL Vpn kısmına basmamız gerek. IPsec vpn de yaptığımız gibi ağ nesnelerinden iç ağıımızı ve sanal ağıımızı oluşturmamız gerekli. Sanal ağı vpn ile bağlanacak kullanıcılar için oluşturacağız.

AĞ NESNESİ

İsim: LAN

Tür: Ağ

IP: 192.168.9.0

Maske: 255.255.255.0

☐ Hariç (İçermeyen)

Açıklama: Kendi iç ip bilgilerini yazıyoruz.

Tamam İptal

Şekil 5.17.2 Ağ Nesnesi Ekleme

Ağ nesnelerinde sağ klik ekle diyerek kendi ağımızı oluşturuyoruz.

AĞ NESNESİ

İsim: VPN-AĞ

Tür: Ağ

IP: 192.168.4.0

Maske: 255.255.255.0

☐ Hariç (İçermeyen)

Açıklama:

Tamam İptal

Şekil 5.17.3 VPN Ağı Nesnesi Ekleme

Vpn kullanıcılarının alacağı sanal ipleri oluşturuyoruz.

KURAL	DURUM	AYARLAR	YEREL AĞ	ÇIKIŞ ARAYÜZÜ	SANAL AĞ	AÇIKLAMA
vpn1	Aktif	Ayarlar	LAN	pppoe0	VPN-AĞ	SSL VPN için sabit sistem kuralıdır. Erişilmesi istenen arayüzleri, sanal ağı ve yerel ağları tanımlı...

Şekil 5.17.4 VPN Kural Ekranı

Yukarıda bulunan şekildeki gibi ağ nesnelerini yerlerine yerleştiriyoruz. Şimdi ise kullanıcıları oluşturmak için Kilit işaretli ayarlar simgesine çift tıklıyoruz.

AYARLAR

Port: 1194 UDP

☐ Verileri gönderirken sıkıştır.

☒ Bütün trafiği VPN bağlantısı üzerinden gönder.

☐ DNS

DNS 1:

DNS 2:

Şifreleme algoritması: AES-128-CBC

Sertifika anahtar uzunluğu: 1024-bit

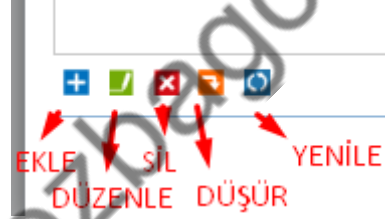
SSL VPN KULLANICILARI	KULLANICI TİPİ	SANAL IP	BAĞLANAN IP	YÜKLEME	İNDİRME	BAĞLANMA ZAMANI
► Serdar	Normal					
► Sener	Normal					
► Rumeysa	Normal	192.168.4.6		11.1 MB	39.7 MB	2020-05-09 00:24:57
► Atilla	Normal					
► Recep	Normal					
► tarik	Normal					

+ - ✕ ↺ ↻

Tamam İptal

Şekil 5.17.5 VPN Kullanıcı Ayarları

Şekilde görünen ayarlar kısmı örnek olarak verilmiştir. Cihazı ilk defa ayarlayacak olanlar boş ekran olarak göreceklerdir.



Şekil 5.17.6 Ekle Düzenleme Tuşları

Yukarıdaki şekilde tuşların ne işe yaradığını göstermek istedim buradan kullanıcı ekleyebilir kullanıcı siler ve bağlanan kullanıcıları vpn bağlantısından düşürebilirsiniz.

SSL VPN KULLANICISI DÜZENLE

Kullanıcı Tipi: Normal

Kullanıcı Adı:

Şifre:

Şifre (Tekrar):

☒ Otomatik IP

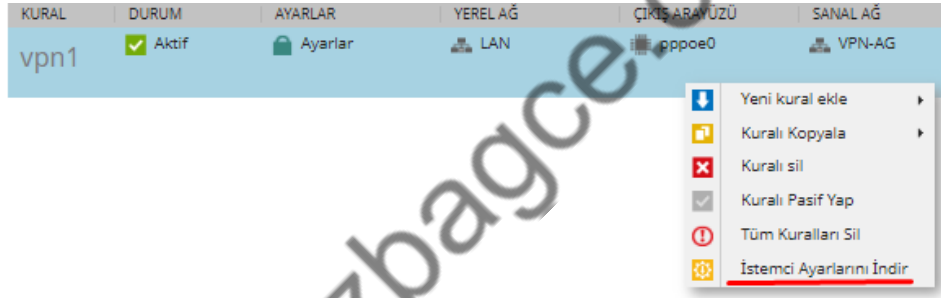
Statik IP: 192.168.4.6

Tamam İptal

Şekil 5.17.7 SSL VPN Kullanıcı Ekleme Ekranı

Kullanıcı eklemek istediğimizde ekle tuşuna bastıktan sonra karşımıza yukarıdaki şekildeki gibi ekran gelmektedir. Burada kullanıcı adı şifre bilgilerini girdikten sonra tamama basıyoruz.

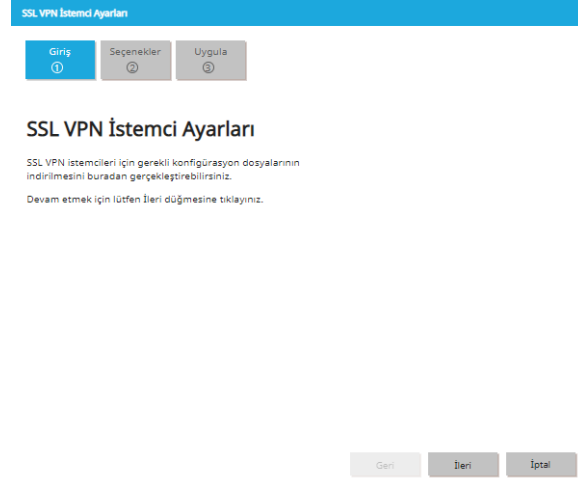
En son olarak uygula butonuna bastıktan sonra şekil 1.1.1. e geri dönüyoruz.



Şekil 5.17.8 İstemci Ayarlarını İndirme 1

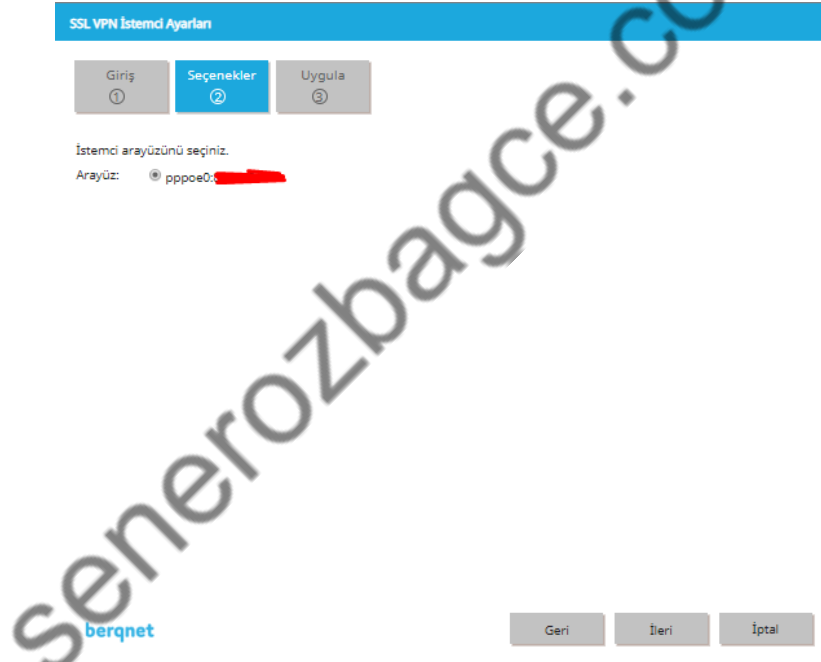
Burada kurala sağ tıklayıp istemci ayarlarını indiriyoruz ve daha sonra open vpn adlı programı bilgisayarımıza indiriyoruz.

Open vpn programını <https://openvpn.net/> adresinden indirebilirsiniz.



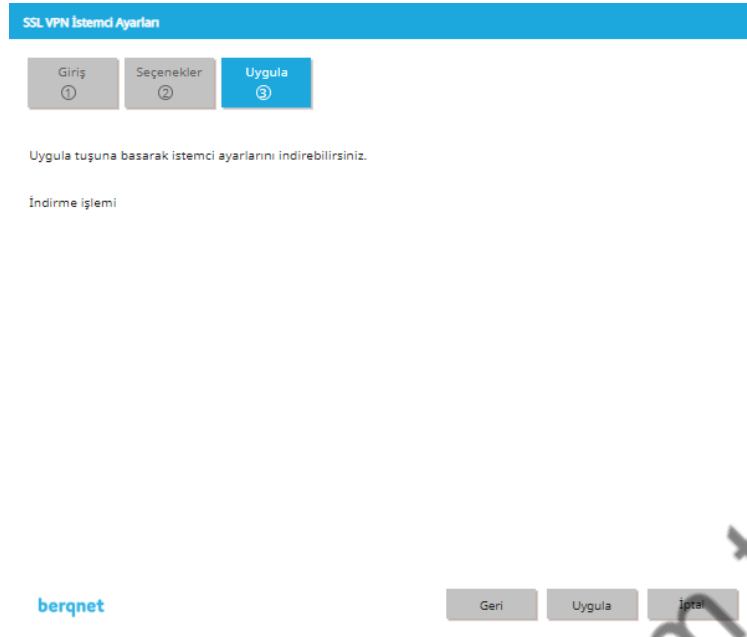
Şekil 5.17.9 İstemci Ayarlarını İndirme 2

İstemci ayarlarını indir sekmesine bastığınızda karşınıza yukarıdaki şekildeki gibi ekran gelmektedir. İleri diyerek



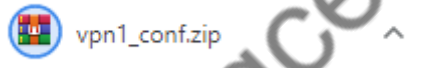
Şekil 5.17.10 İstemci Ayarlarını İndirme 3

Arayüzü seçip tekrar ileri diyerek



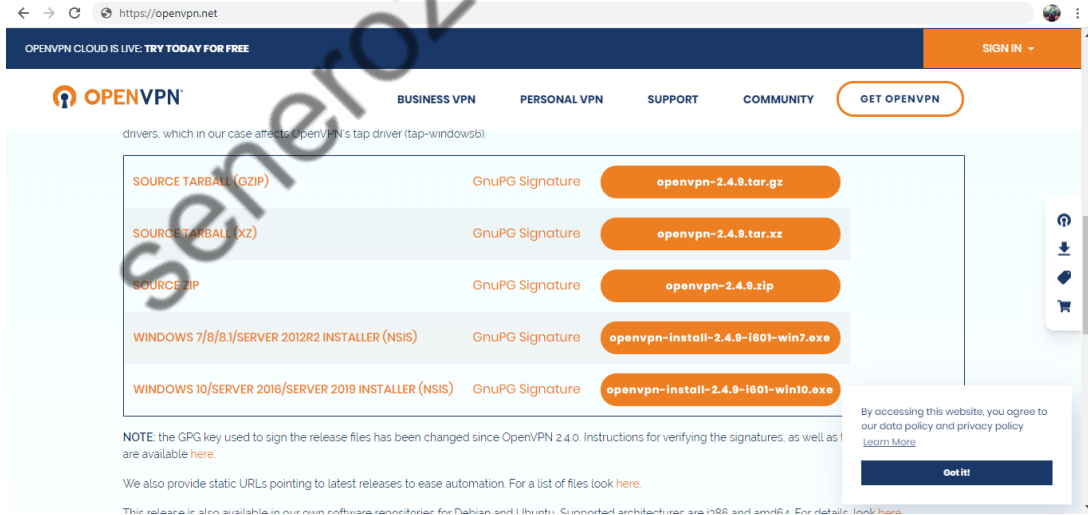
Şekil 5.17.11 İstemci Ayarlarını İndirme 4

Uygula ya basarak ayarları RAR dosyası şeklinde indirebilirsiniz.

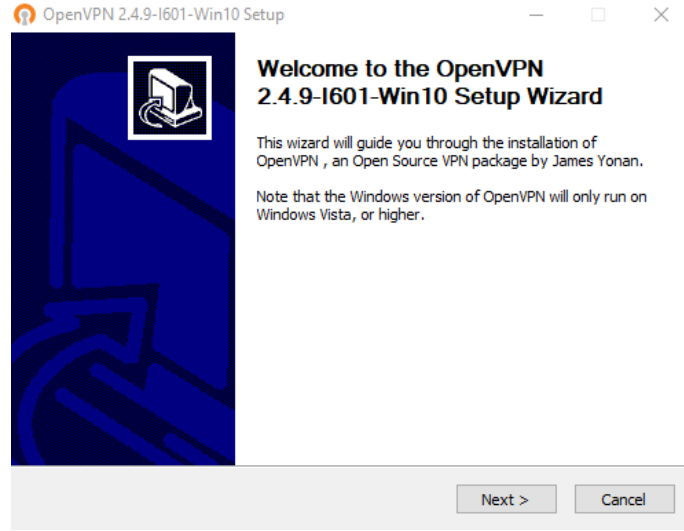


Şekil 5.17.12 İstemci Ayarlarını İndirme 5

Open vpn sayfasına girdiğinizde işletim sisteminize uygun programı indirebilirsiniz.

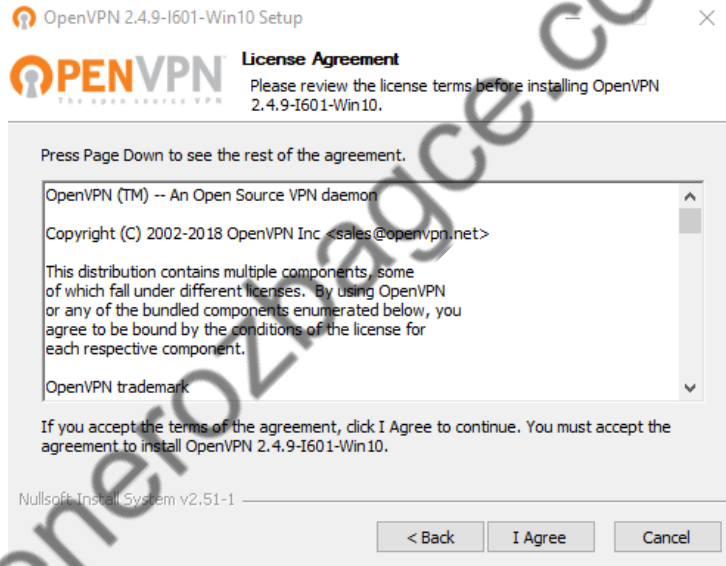


Şekil 5.17.13 Open VPN İndirme



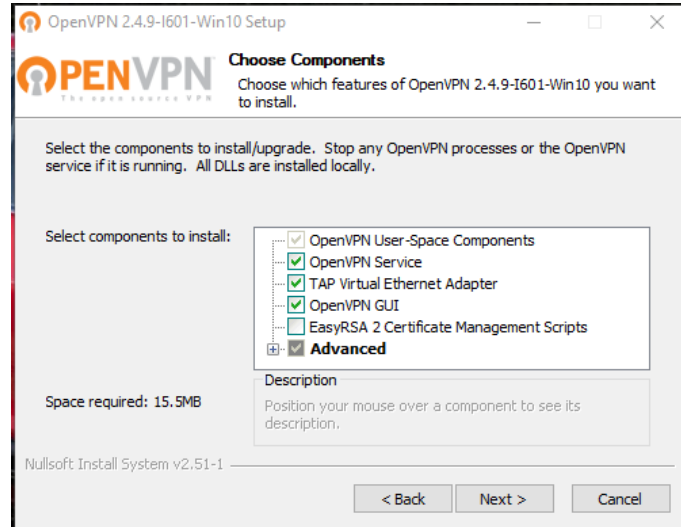
Şekil 5.17.14 Open VPN Kurulum 1

İndirdiğiniz programı next diyerek kurmaya başlayabilirsiniz.



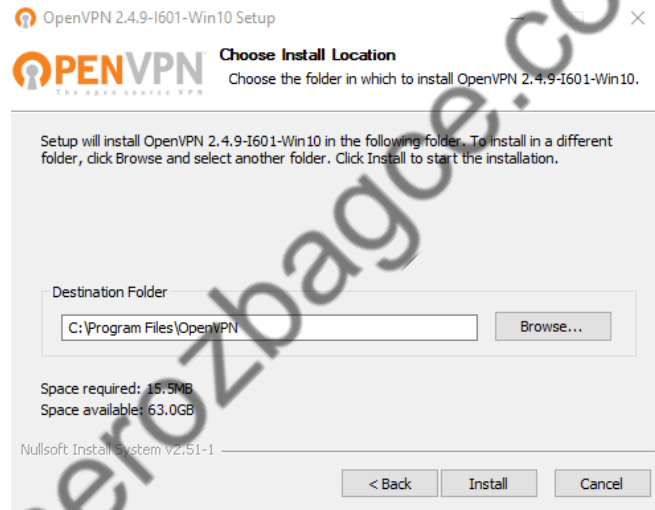
Şekil 5.17.15 Open VPN Kurulum 2

Koşulları kabul ettikten sonra (I Agree) Tuşuna basıp



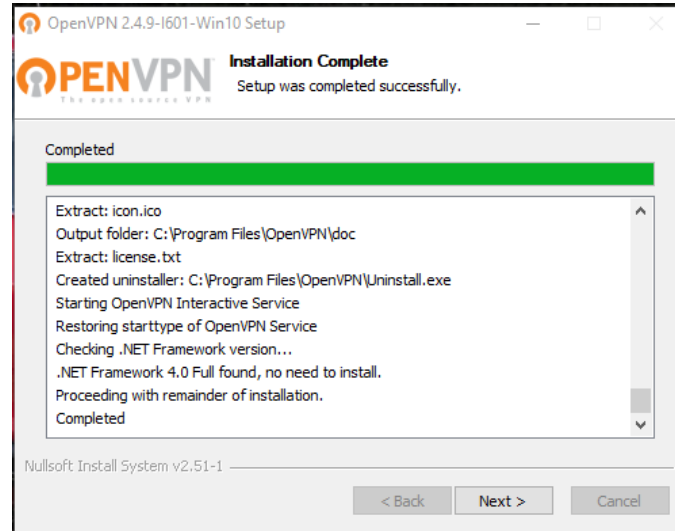
Şekil 5.17.16 Open VPN Kurulum 3

Tekrar next diyip.



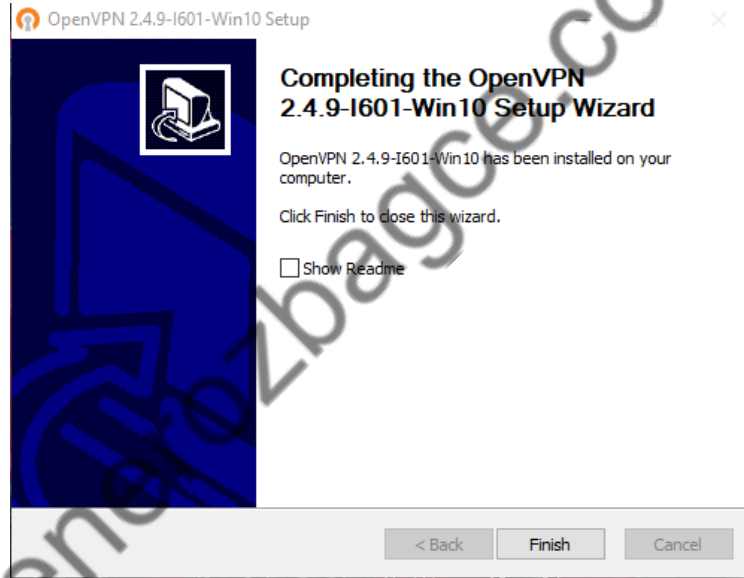
Şekil 5.17.17 Open VPN Kurulum 4

Programın kurulacağı dosya yolunu gösterip Install diyerek kurmaya başlayabilirsiniz.



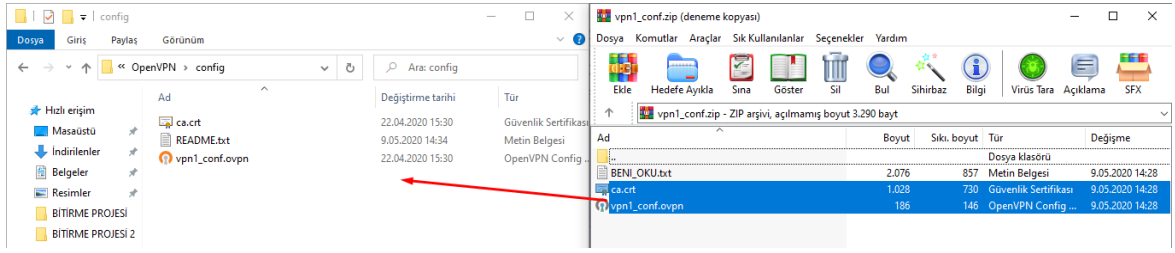
Şekil 5.17.18 Open VPN Programı Kurulum Ekranı 1

İndirme tamamlandıktan sonra next tuşuna basıp kurulumu bitirebilirsiniz.

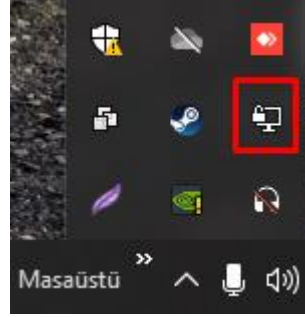


Şekil 5.17.19 Open VPN Programı Kurulum Ekranı 2

Daha sonra indirdiğiniz ayarları Open vpn programına atmanız gerekli bunun için Bilgisayarınızda C:\Program Files\OpenVPN\config konumuna gelip rardaki dosyaları config klasörünün içine kopyalamamız gerekli.

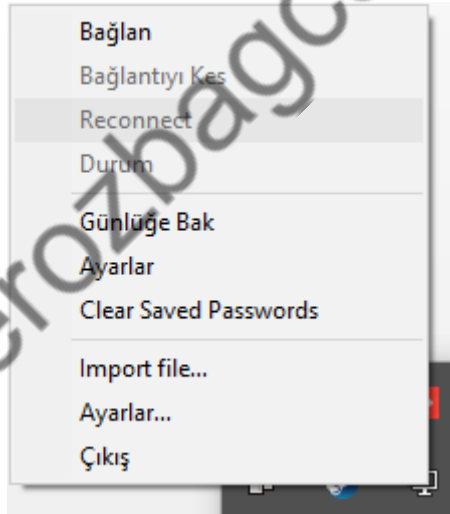


Şekil 5.17.20 Open VPN Programı Kurulum Ekranı 3



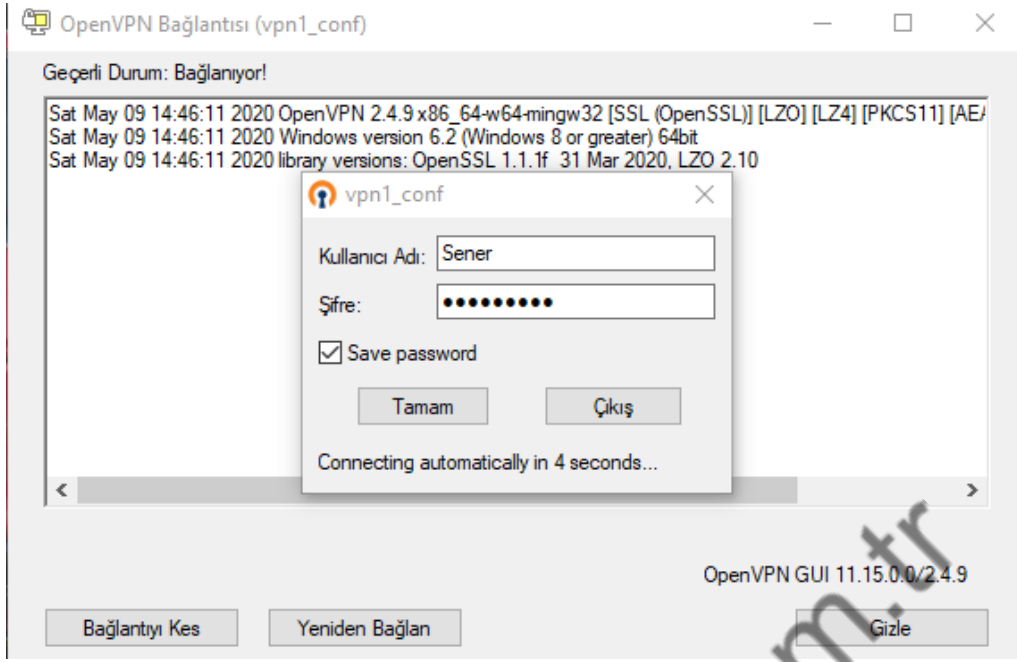
Şekil 5.17.21 Open VPN Programı 1

Araç çubuğunda gizli sekmelerde bulunan open vpn programını sağ tıklayarak



Şekil 5.17.22 Open VPN Programı 2

Bağlan butonuna tıkladığınızda

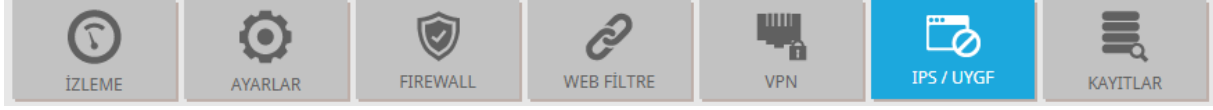


Şekil 5.17.23 Open VPN Programı 3

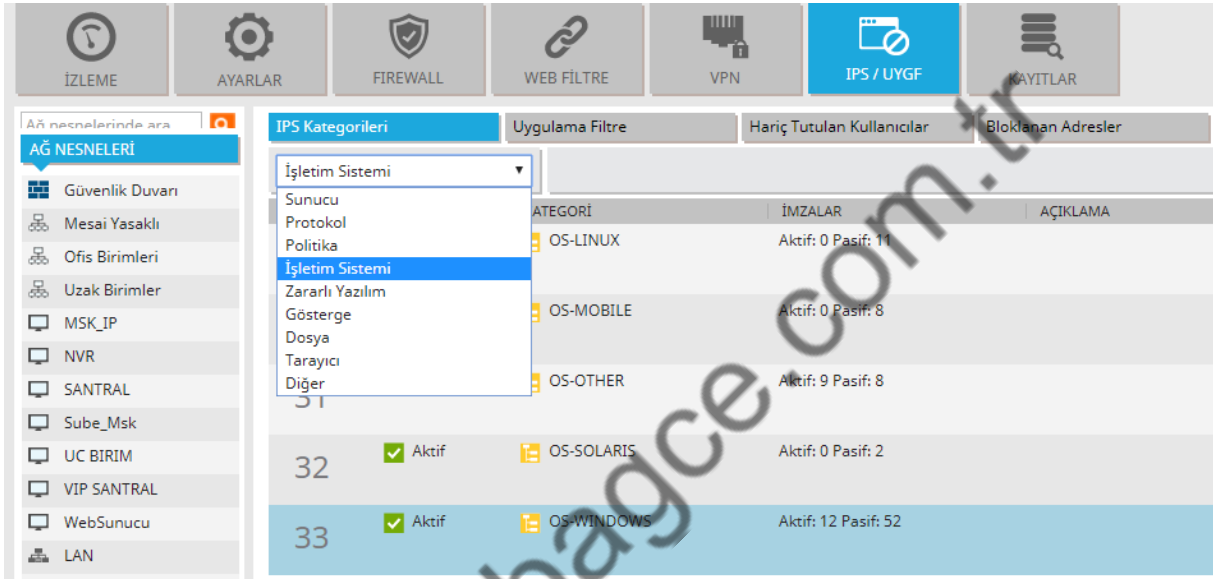
Karşınıza yukarıdaki şekildeki gibi kullanıcı adı şifrenizi soruyor tamam dedikten sonra vpn bağlantınıza bağlanabilirsiniz.

5.18 Ips Kategorileri

IPS Kategorilerinde işinize yarayacak hazır imzalar bulunmaktadır bunları seçip ister blok ister alarm verdirebilirsiniz. Bunun için aşağıdaki yönlendirmeleri gerçekleştirelim.



Şekil 5.18.1 IPS Ayarları



Şekil 5.18.2 IPS Kategori Listesi Ekranı 1

Kategorilere göre farklı imzalar bulunmaktadır. Biz şu an işletim sistemlerine gelebilecek dos saldırılarını önlemesini yapacağız.

İşletim Sistemi			
KURAL	DURUM	KATEGORİ	İMZALAR
29	✓ Aktif	OS-LINUX	Aktif: 0 Pasif: 11
30	✓ Aktif	OS-MOBILE	Aktif: 0 Pasif: 8
31	✓ Aktif	OS-OTHER	Aktif: 9 Pasif: 8
32	✓ Aktif	OS-SOLARIS	Aktif: 0 Pasif: 2
33	✓ Aktif	OS-WINDOWS	Aktif: 12 Pasif: 52

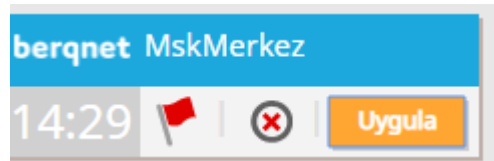
Şekil 5.18.3 Kategori Listesi Ekranı 2

Kural 33 içerisinde bulunan

İMZA AYARLARI (OS-WINDOWS)				
☐ Tüm imzaları aktif et ☒ Tüm imzaları blok moda al				
ID	AKTİF	İMZA	ÇALIŞMA MODU	REFERANS
272	✓	Microsoft Windows IGMP dos attack	Blok	ref1 ref2 ref3
530		NT NULL session	Blok	ref1 ref2
1079		Microsoft Windows WebDAV propfind access	Blok	ref1 ref2 ref3 ref4 ref5
1239		RFPalyze Attempt	Blok	ref1 ref2 ref3
1384		Microsoft Windows UPnP malformed advertisement	Blok	ref1 ref2 ref3 ref4 ref5
1388		Microsoft Windows UPnP Location overflow attempt	Blok	ref1 ref2 ref3 ref4 ref5
2101		attempt	Blok	ref1 ref2 ref3 ref4 ref5
2126		Microsoft Windows PPTP Start Control Request buffer overflow attempt	Blok	ref1 ref2 ref3 ref4
2176		Microsoft Windows SMB startup folder access	Blok	

Şekil 5.18.4 İmza Ekranı

Burada seçtiğimiz imzayı blok ve alarm durumuna alabiliyoruz. Blok koyduktan sonra güvenlik cihazımızın Windows işletim sistemlerine dos atacklarına karşı korumuş oluyoruz.



Şekil 5.18.5 Uygula Butonu

Ayarları yaptıktan sonra uygula butonuna basmayı unutmayınız.

KAYNAKÇA

- datakey.com.tr: <http://blog.datakey.com.tr/antivirus-nedir-virus-nedir/> adresinden alındı
- 5651 *berqnet.com*. <https://berqnet.com/blog/5651-sayili-yasa> adresinden alındı
- berqnet.com*. <https://berqnet.com/blog/hotspot-nedir> adresinden alındı
- firewall ostec.blog*. <https://ostec.blog/en/perimeter/firewall> adresinden alındı
- haberler.com*.<https://www.haberler.com/kvkk-kanunu-nedir-12987704-haberi/> adresinden alındı
- hosting.com.tr*. <https://www.hosting.com.tr/bilgi-bankasi/dns-nedir/> adresinden alındı
- kamusm.gov.tr*. http://www.kamusm.gov.tr/urunler/zaman_damgasi/ adresinden alındı
- ostec.blog*. <https://ostec.blog/seguranca-perimetro/firewall-stateful-stateless> adresinden alındı
- USOM berqnet*. <https://berqnet.com/blog/usom-nedir> adresinden alındı
- VOIP berqnet.com*. <https://berqnet.com/blog/voip-nedir> adresinden alındı
- vpnmentor.com*.<https://tr.vpnmentor.com/blog/farkli-vpn-tuerleri-hangi-vpn-tueruenue-ne-zaman-kullanmalisiniz/> adresinden alındı