SİBER UZAYDA GÜVENLİK ÖNLEMLERİ

abaküs

Udemy EĞİTİMİ HEDİYELİ

HERKES İÇİN SİBER GÜVENLİK

CEMAL TANER

- Ağ Temelleri
- Siber Güvenliğe Giriş
- Siber Saldırılar, Kavramlar ve Tehditler
- Verilerin, Ağların ve Cihazların Korunması
- Güvenlik Duvarları
- Güvenlik Duvarı Uygulamaları

Herkes için Siber Güvenlik

Cemal TANER

abaküs

abaküs 134
Herkes için Siber Güvenlik
Cemal TANER
1. Baskı: Temmuz 2019
ISBN: 978-605-2263-58-7

Kapak ve sayfa düzeni: Cem Demirezen
Satış: satis@abakuskitap.com

Baskı: Ezgi Matbaacılık San. Tic. Ltd. Şti.
Sanayi Cad. Altay Sok. No:14
Çobançeşme-Yenibosna/İSTANBUL
Tel: 0212 452 23 02
Matbaa Sertifika No: 12142

Selda Ustabaş Demiryakan
Abaküs Kitap Yayın Dağıtım Hizmetleri
Yayıncılık sertifika no: 43062
Hobyar Mah. Cemal Nadir Sok. No:24/178 Cağaloğlu-Fatih/İST.
Tel.: (0212) 514 68 61
www.abakuskitap.com - editor@abakuskitap.com

Cemal TANER

İzmir'de doğdu ve büyüdü. Gazi Üniversitesi mezunudur. Gopher protokolünü kullanacak kadar eski bir İnternet kullanıcısı ve BNC jak takacak kadar eski bir networkçüdür. 1996 yılından beri eğitimci, serbest yazar, formatçı vb. birçok işle meşgul oldu. Son yıllarda ağırlıkla Cisco CCNA eğitimleri vermektedir. MYK tarafından hazırlanan Bilgisayar Donanım Bakım Elemanı ve Ağ Teknolojiler Elemanı meslek standartlarının geliştirilmesi ve yeterliliklerinin hazırlanması kapsamında danışmanlık yaptı. 2011 yılında Orta ve Doğu Avrupa Bölgesinde en iyi Cisco Networking Academy eğitmenleri arasında seçilmiştir. Kendi ismini taşıyan blog sayfasında ve Youtube kanalında içerik üretmeye devam etmektedir.

ÖNSÖZ

Günümüzde ağa bağlanan cihaz sayısı ve çeşidi hızla artıyor. Daha düne kadar sadece birkaç bilgisayar, yazıcı ve sunucudan oluşan ağlar yerine, Nesnelerin İnternet'i (IoT) kavramı ile birlikte kombiden kahve makinesine, arabadan ayakkabıya kadar her nesnenin, her şeyin ağa bağlandığı ağ yapıları ile karşılaşmaya başladık.

Ağa bağlanan cihazların sayısının ve çeşidinin artması ile birlikte bu cihazların güvenliğini sağlamak en önemli konu haline gelmiştir. Bireylerden kurumlara kadar herkes bilgi işlem cihazlarının güvenliğini sağlamak zorunda. Bu yapılmadığında paradan zamana, itibardan değişik kaynaklara kadar birçok kayıp yaşanmakta. Hepimizin elindeki cep telefonları, bilinçli kullanılmadığında bir mağduriyet aletine dönüşebiliyor. Kurumlar verilerini koruyamadıklarında mevcut kanunlara göre büyük para cezaları ile karşılaşabiliyor.

Bilgi işlem cihazlarımızı korumaktan verilerimizi korumaya kadar gerekli önlemleri alma işlemlerine **siber güvenlik** diyoruz. Siber güvenlik bireylerden kurumlara oradan devletlere kadar herkesin önem vermesi gereken konuların başında geliyor.

Bu kitapta 7'den 77'ye herkes için gerekli olan siber güvenlik konularını öğrenmenin yanında, ülkemizin yerli ve milli ürünü Berqnet Tümleşik Güvenlik Sisteminin kurulum ve yapılandırma ayarlarını da göreceksiniz.

Siber uzayda her zaman güvende kalmanız dileğiyle...

Cemal Taner
www.cemaltaner.com.tr
cemaltaner@gmail.com

TEŞEKKÜR

Berqnet, siber güvenlik alanında yerli ürünler geliştirmekte ve bu misyonunu yerli bir siber güvenlik ekosistemi oluşturma doğrultusunda da genişletmektedir. Yerli ekosistem ise yerli ürünlerin yanısıra nitelikli insan gücü ve Türkçe yazılmış siber güvenlik kaynaklarını da barındırmalıdır.

Siber Güvenlik, birçok teknoloji ve sosyal alanı ilgilendirmekle beraber temel alanlarından biri ise ağ teknolojileridir. Bu nedenle birçok alanda Türkçe kaynağa ihtiyaç duyulmakla beraber bu kitapta ağ teknolojilerine öncelik verilmiştir. *Herkes İçin Siber Güvenlik* kitabı bu doğrultuda planlanarak, siber güvenlik alanında uzmanlaşmak isteyenlere sunulmuştur.

Bu kitabın siber güvenlikte kariyer inşa edeceklerin yoluna ışık tutmasını diliyoruz.

Kitabın oluşturulması sürecinde emeği geçen herkese teşekkürlerimizi sunarız.

DR. A. MURAT APOHAN
LOGO Siber Güvenlik Ve Ağ Teknolojileri – Genel Müdür

İÇİNDEKİLER

1

1. Ağ Temelleri

Bu bölümde günümüzde hemen hemen her şeyin (thing) parçası olduğu ağ (network) teriminin anlamını öğrenip, bir ağı oluşturan bileşenleri tanıyacağız. Sonrasında ağ protokollerini ayrıntılı bir şekilde tanıyıp bilgisayarlar arasında haberleşme nasıl gerçekleşiyor göreceğiz.

Bir ~~Aşk~~ Ağ Hikâyesi: Bilgisayarlar kendi başlarına özgürce takılırken muhasebe bölümündeki Zeynep Hanım bir rapor yazıyor. Bu raporu bir yazıcıdan yazdırması lazım ama tabi o zamanlarda yazıcılar çok pahalı ve sadece bölüm amirinin odasındaki bilgisayara bağlı bir nokta vuruşlu yazıcı var. Zeynep Hanım PW programı ile hazırladığı raporu aşağıda gördüğünüz diskete kaydediyor ve bölüm amirinin odasına gidiyor.

Daha sonra oradaki bilgisayarda disket sürücüye disketi takıp raporu açıp yazdırıyor ve masasına geri dönüyor. Ne kadar zahmetli değil mi? Günümüzde nasıl acaba hiç düşündünüz mü?

1.1. Ağ (Network) Nedir?

Bilgisayarların ilk üretilmeye başladığı yıllarda, bilgisayarlar tek başlarına çalışıyor ve başka bilgisayarlar ile iletişim kurma ihtiyacı hissetmiyorlardı. İnternet'in temelini de oluşturan ARPANET projesi, aslında farklı yerlerde bulunan bilgisayarlar arasında haberleşme sağlanması, kaynak ve dosyaların paylaşılması amacını taşıyordu. Daha sonraki yıllarda birçok faydasından ötürü bilgisayarların birbirleri ile bağlanarak ağ (network) oluşturulması tercih edilir olmuştur.

1.2. Neden Ağlara İhtiyacımız Var?

Ağ kurmaktaki temel amaç paylaşımdır (sharing). Bu şekilde maddi olarak tasarruf yapılırken, zamandan da kazanılmaktadır. Örneğin 15 kullanıcılı bir mali müşavirlik bürosunda her bilgisayara yazıcı bağlamak yerine bir ağ yazıcısı ağa bağlanarak maddi açıdan tasarruf edilir.

Program Paylaşımı: Merkezi bir sunucuya kurulmuş programa tüm kullanıcılar erişebilir böylece her bilgisayara ayrıca programın kurulmasına gerek kalmaz ve ortak çalışma aynı dosyalar üzerinde değişiklik yapma imkânı doğar.

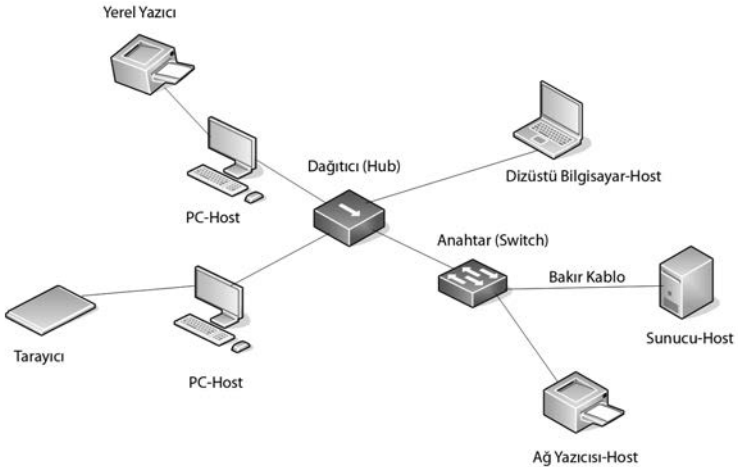
Dosya Paylaşımı: Ağ üzerinde tüm kullanıcıların ortak kullanabileceği ya da sadece kendilerinin ulaşabileceği alanlarda dosyalar, programlar paylaşılabilir.

Yazıcı Paylaşımı: Her bilgisayara yazıcı kurmak yerine bir bilgisayara bağlı bir yazıcıyı paylaşıma açarak veya bir ağ yazıcısını ağda paylaşıma açarak, donanım maliyetinden büyük tasarruf yapılır.

Güvenlik: Kullanıcılar parola ile ağa bağlandıkları takdirde yetkisiz kişilerin ağ kaynaklarına, dosyalara erişmesi engellenmiş olur.

Merkezi Yönetim: Bir ağ yöneticisi ağdaki tüm bilgisayarları tek bir merkezden yöneterek güvenlik sağlar ve program kurma güncelleme gibi işlemleri daha kolay gerçekleştirir.

1.3. Bir Ağı Oluşturan Bileşenler



Şekilde görüldüğü gibi bir ağı oluşturan birçok bileşen vardır. Kişisel bilgisayarlar (PC), sunucular, yazıcılar, anahtarlar, kablolar gibi. Bu bileşenler dört ana kategoriye ayrılabilir:

Uç Cihazlar (Host): Ağ üzerinde bir IP adresine sahip, kişisel bilgisayar, ağ yazıcısı ve sunucu gibi son kullanıcı cihazıdır.

Paylaşılan çevresel aygıtlar: Ağ üzerinde bir IP adresine sahip değillerdir. Bağlı oldukları cihaz üzerinden ağdaki diğer cihazlarla iletişim kurarlar. Tarayıcı, yazıcı, web kamerası gibi.

Ağ iletişim cihazları: Hostları birbirine bağlayan veri trafiğinin üzerlerinden aktığı dağıtıcı (hub), anahtar (switch) yönlendirici (router) gibi cihazlardır.

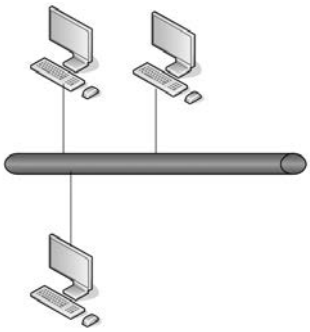
Ağ iletişim ortamı (Medya): Hostları ve ağ cihazlarını birbirine bağlayan bakır, fiber optik veya kablosuz bağlantı ortamlarıdır.

1.4. Ağ Topolojileri

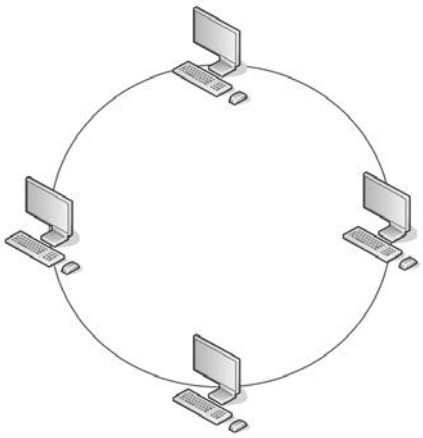
Hostların ağa bağlanma şekline göre çeşitli modeller oluşturulmuştur. Bu modellere topoloji denir. Bus topoloji, ring topoloji, star topoloji ve mesh topoloji önde gelen topoloji tipleridir.

Bus Toploji: Bu topoloji tipinde şekilde de görüleceği üzere tüm bilgisayarlar aynı ana hat kablosu üzerinden hub veya switch gibi bir ağ cihazı kullanmadan birbirine

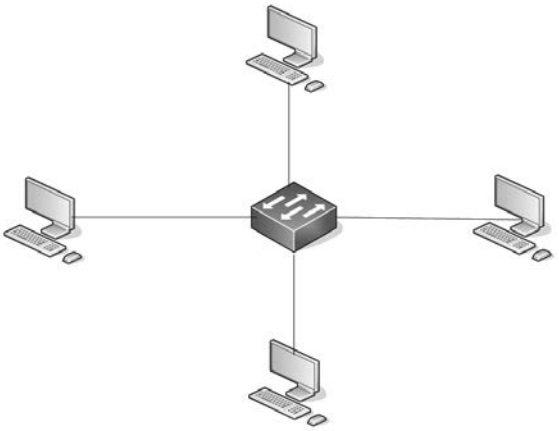
bağlanmıştır. Bu topolojinin birçok dezavantajı vardır. Aynı anda sadece bir bilgisayar veri gönderebilir. Başka bir bilgisayar da göndermeye çalışırsa çarpışma meydana gelir. Ayrıca ana hat kablosunda bir kopukluk meydana gelirse devamındaki tüm hostlar ağ bağlantısını kaybeder. Günümüzde artık kullanılmamaktadır.



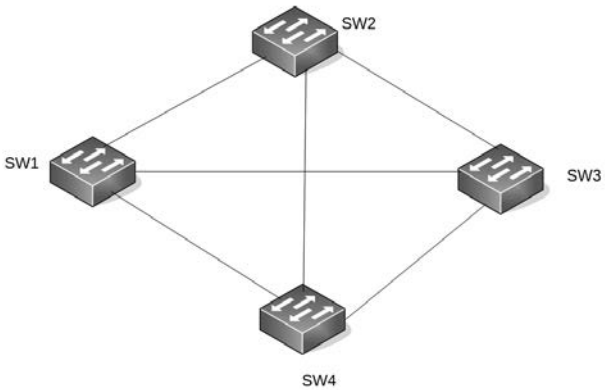
Ring Topoloji: Bu topolojide de bus topolojisinde olduğu gibi hub veya switch gibi bir ağ cihazı kullanmadan bilgisayarlar aynı kablo üzerinden birbirlerine bağlanmıştır. Bu kabloda meydana gelecek bir arıza tüm hostların ağ bağlantısını kaybetmesine neden olur. Günümüzde artık kullanılmamaktadır.



Star Topoloji: Hub veya switch gibi bir ağ cihazının merkezde bulunduğu ve hostların ağ cihazına ağ medyası aracılığıyla bağlandığı, günümüzde sıklıkla kullanılan topolojidir. Herhangi bir kablo veya port arızasında sadece ilgili bilgisayar arızadan etkilenir. Modern switchler üzerinde bulunan ledler ile arıza tespiti kolaylıkla yapılır.

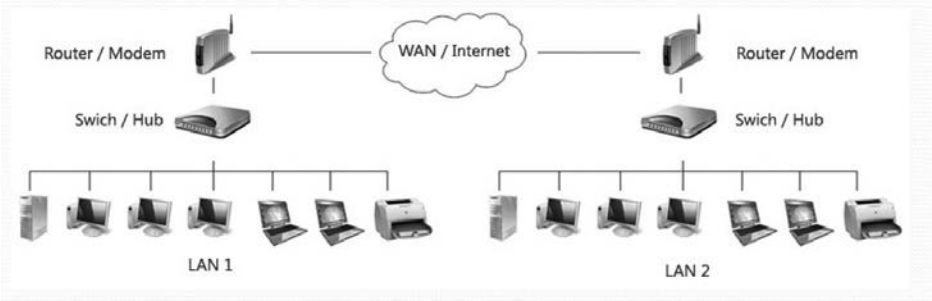


Mesh Topoloji: Hostların veya ağ cihazlarının birbirine birden fazla ağ medyası ile bağlanması ile oluşturulan topolojidir. Bu şekilde yüksek seviyede yedeklilik sağlanarak ağ kesintilerinin önlenmesi hedeflenmiştir. Daha fazla ağ cihazı ve ağ medyası kullanıldığından maliyeti fazladır.



1.5. Ağ Tipleri

Ağlar fiziksel büyüklüklerine göre LAN (Local Area Network - Yerel Alan Ağı) ve WAN (Wide Area Network - Geniş Alan Ağı) olmak üzere ikiye ayrılır.



LAN (Local Area Network): LAN, sınırlı bir alandaki; yani küçük bir coğrafi alandaki kullanıcılara hizmet sunan ve hostların ağa erişmesine imkan veren ağ yapısıdır. Bugün en çok karşılaştığımız SOHO (Small Office Home Office-Küçük Ofis ve Ev Ofis) ağları en yaygın LAN örneğidir. SOHO ağında bilgisayar, yazıcı gibi host cihazlar ethernet kabloları aracılığı ile bir switch üzerinden birbirleriyle haberleşir, ayrıca bir router aracılığıyla da İnternet'e çıkabilirler.

WAN (Wide Area Network): Farklı yerlerdeki LAN'ları birbirine bağlayan ağ yapısıdır. Bugün WAN bağlantısı dediğimizde aklımıza genellikle İnternet gelir. İnternet ağlar arası ağ anlamına gelir ve dünya çapında bütün bilgisayarları birbirine bağlar.

1.6. OSI Modeli

Ağlar ilk ortaya çıktığında her üretici sadece kendi ürettiği cihazların birbiri ile haberleşebildiği bir yapı oluşturmuştu. Örneğin IBM, Systems Network Architecture (SNA) ismini verdiği ve 1974 yılında yayınladığı modele göre sadece IBM marka cihazlar bu ağa bağlanabiliyordu. Diğer üreticiler de kendi ağ modellerini oluşturdular. Bu karmaşıklığı önlemek ve standart bir model oluşturmak için ISO (International Organization for Standardization) tarafından 7 katmandan oluşan OSI (Open Systems Interconnection) modeli açıklandı. Bu model şekilde görüldüğü üzere 7 katmandan oluşmaktadır ve her bir katman birbirinden bağımsız çalışmakta ve ayrı bir görevi ifa etmektedir.

Layer 7	Application	Uygulama
Layer 6	Presentation	Sunum
Layer 5	Session	Oturum
Layer 4	Transport	Taşıma
Layer 3	Network	Ağ
Layer 2	Data Link	Veri Bağlantısı
Layer 1	Physical	Fiziksel

Yukarıdan aşağıya doğru her bir katmanın ne işe yaradığını görelim:

Uygulama Katmanı: Kullanıcıya bir arayüz sunan katmandır. Kullanıcı ile uygulama arasında yer alır. HTTP, FTP, SMTP, TFTP, DNS protokolleri gibi birçok protokol bu katmanda çalışır.

Sunum Katmanı: Verilerin belirli bir formata sokulduğu katmandır. Örneğin bir resim dosyasının jpeg formatına sokulması bir örnektir.

Oturum Katmanı: Veriyi gönderen ve alan iki bilgisayardaki uygulama arasındaki bağlantının kurulması, kullanılması ve sonlandırılması işlemleri bu katmanda yapılır.

Taşıma Katmanı: Verinin parçalara ayrılması, sıralanması ve alan bilgisayarda tekrar birleştirilmesi işlemleri bu katmanda gerçekleşir. Bu katmanda üst katmanlardan gelen veriye kaynak ve hedef port bilgisi eklenir.

Ağ Katmanı: Verinin ilgili ağa yönlendirilmesi ve veriye mantıksal adres atanması bu katmanda gerçekleşir. Bu katmanda üst katmanlardan gelen veriye kaynak ve hedef IP adresi bilgisi eklenir.

Veri Bağlantısı Katmanı: Verinin bitlere dönüştürülerek alt katmana gönderilmesi bu katmanda gerçekleşir. Bu katmanda üst katmanlardan gelen veriye kaynak ve hedef MAC adresi bilgisi eklenir.

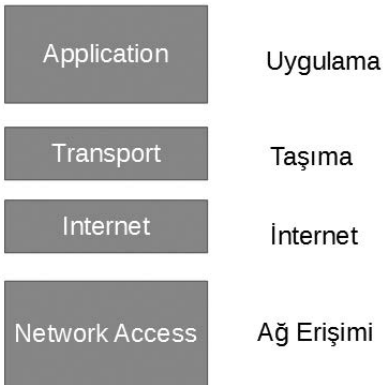
Fiziksel Katman: Verinin elektrik sinyali olarak bakır kablo üzerinden, ışık sinyali olarak fiber optik kablo üzerinden, radyo frekans sinyali olarak kablosuz olarak iletildiği katmandır.

Bunu Biliyor musunuz?
ARPANET (Advanced Research Projects Agency Network, Amerikan Gelişmiş Savunma Araştırmaları Dairesi Ağı), yeni adıyla DARPA (Defence Advanced Research Projects Agency, ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı için soğuk savaş sırasında geliştirilmiş dünyanın ilk çalışan paket anahtarlama ağı olmasının yanı sıra İnternetin de atasıdır. Araştırma ve araştırmacıları birbirine bağlamak amacıyla geliştirilen ARPANET, daha sonraları Internet'in gelişmesine yol açan TCP/IP protokolünün ortaya çıkmasını sağlamıştır. Kaynak: wikipedia

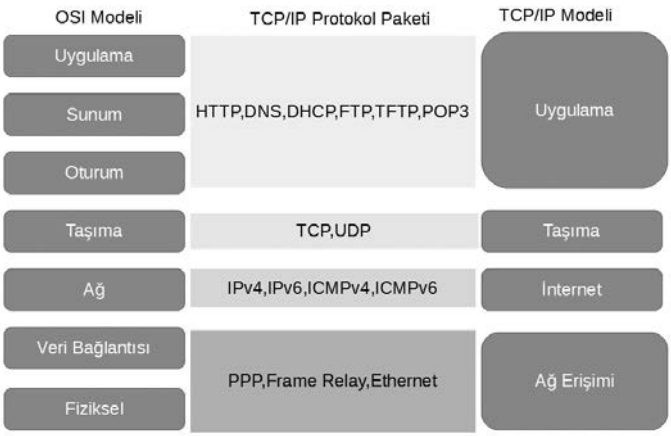
1.7. TCP/IP Protokol Yığını

Her ne kadar OSI standart bir model olarak ortaya konsa da İnternet'in temelini oluşturan protokoller kümesi olması ve daha önce geliştirilmeye başlanması nedeniyle 1990'lı yıllarda TCP/IP protokol yığını öne çıkmıştır.

TCP/IP Protokol yığını şekilde de görüldüğü üzere 4 katmandan oluşur ve her bir katmanın görevi OSI modelindekiyle benzerdir.



Aşağıdaki şekilde de OSI modeli ve TCP/IP Protokol kümesi karşılaştırılmıştır. OSI'deki Uygulama, Sunum ve Oturum katmanları TCP/IP'de karşımıza tek bir Uygulama katmanı olarak çıkmaktadır. Yine OSI'deki Veri Bağlantısı ve Fiziksel katman TCP/IP'de Ağ Erişimi olarak isimlendirilmektedir.



1.8. Ağ Cihazları

Ring ve Bus topolojilerinde gördüğümüz gibi ilk başlarda bilgisayarları birbirine bağlamak için herhangi bir ağ cihazı kullanılmıyordu. Sonraki yıllarda ağların büyümesi ile aynı yerel ağ üzerindeki cihazları haberleştirmek için hub (dağıtıcı) ve switch (anahtar), farklı ağlardaki cihazları haberleştirmek için de router (yönlendirici) kullanılmaya başlandı.

1.8.1. Dağıtıcı (Hub)

Star (Yıldız) topolojide merkezde bulunan ağ cihazıdır. 4-8-16-24-48 vb. port olarak üretilir. Hublar bir portuna gelen sinyali gelen port hariç diğer tüm portlarına ilet-

tiği için ağ tıkanıklıklara ve çakışmalara neden olur. Her ne kadar bunları önlemek için half duplex (tek yönde iletişim) ve CSMA/CD gibi mekanizmalar geliştirilse de switchlerin üretilmesiyle artık pek kullanılmamaktadır.

1.8.2. Anahtar (Switch)

Star topolojide ağın merkezinde bulunan cihazdır. Genellikle 8-24 ve 48 port olarak üretilir. Yönetilebilen ve yönetilemeyen tipleri vardır. Hangi portunda hangi MAC adresine sahip hostun olduğu bilgisini içeren bir MAC tablosu oluşturarak gönderen bilgisayardan gelen verinin sadece alıcı bilgisayara gitmesini sağlar. Bu nedenle full duplex (iki yönlü) çalışabilir ve hublardaki gibi çakışma meydana gelmez. Günümüzde 100 Mbit- 1 Gbit- 10 Gbit ve 40 GBit hıza sahip portları olan switchler üretilmiş ve artık LAN'ların en temel ağ bileşeni haline gelmiştir.

1.8.3. Yönlendirici (Router)

Farklı yerel alan ağlarını (LAN) birbirine bağlayan ağ cihazlarına router denir. İnternet olarak isimlendirdiğimiz geniş alan ağı (WAN) binlerce router'dan oluşan bir ağdır. Yukarıdaki şekilde genellikle yanlış olarak modem diye isimlendirilen bir kablosuz erişim noktası özelliği de olan ADSL router görülmektedir. Bu router evimizdeki bilgisayarları İnternet'e yönlendirir.

1.8.4. Güvenlik Duvarı (Firewall-UTM)

Türkçe kelime karşılığı olarak ateş duvarı anlamına gelse de ağımızı siber tehditlere karşı koruduğu için güvenlik duvarı olarak isimlendirilir. Güvenlik duvarı özelliği dışında antivirüs gateway, web filtreleme, hotspot vb. birçok özelliği ile artık UTM (Unified Threat Management-Tümleşik Güvenlik Sistemi) olarak anılmaya başlanmıştır. Kitabımızın ilerleyen bölümlerinde firewallar ve yerli firewall UTM Berqnet hakkında daha ayrıntılı bilgi vereceğiz.

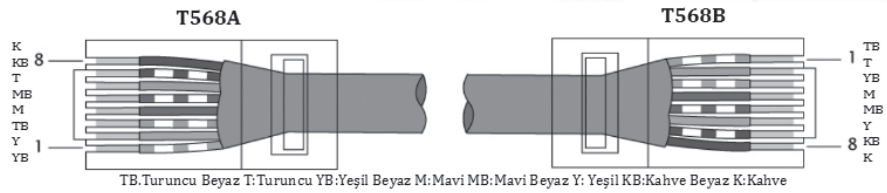
1.9. Ağ Medyaları

Ağ cihazları ile bilgisayarları birbirine bağlamak için ağ medyası ismi verilen bağlantı elemanları kullanılır. Çoğunlukla yerel alan ağlarında (LAN) ağ medyası olarak bakır kablo, fiber optik kablo ve kablosuz (wireless) bağlantı kullanılır.

1.9.1. Bakır Kablo

Bakır kablolar genellikle UTP (Unshielded Twisted Pair-Korumasız Büklümlü Kablo) olarak çeşitli kategorilerde (Cat5, Cat5e, Cat6, Cat 6A, Cat 7 ve Cat7A) üretilir. UTP kabloların manyetik alan ve radyo frekans girişimine karşı hassasiyetini arttırmak için her iki tel birbiri ile toplam 8 telde beraber sarmal haline getirilerek bükülmüştür. Belirli bir mesafedeki büklüm sayısı arttıkça kategori ve hız artmaktadır. Manyetik alan ve radyo frekans girişiminin çok yoğun olduğu yerlerde STP (Shielded Twisted Pair-Korumalı Büklümlü Kablo) kullanılır. STP kablolar ekranlı olarak üretilir ve uçtan uca topraklanır. STP kablolar UTP kablolardan daha pahalı ve işlemesi zordur. Piyasada çoğunlukla UTP kablo kullanılır. UTP kablolar ortalama 100 metre mesafeyi destekler. Aşağıdaki tabloda UTP kablo kategorileri ve desteklediklerı hız gösterilmiştir.

UTP kablolar RJ-45 bağlayıcılar ile sonlandırılır. Sonlandırma sırasında T568A veya T568B standartları kullanılır. Kablonun her iki ucu da 568A veya 568B şeklinde sonlandırılırsa düz kablo, bir ucu 568A diğer ucu 568B olarak sonlandırılırsa çapraz kablo elde edilir.



TB.Turuncu Beyaz T:Turuncu YB:Yeşil Beyaz M:Mavi MB:Mavi Beyaz Y: Yeşil KB:Kahve Beyaz K:Kahve

1.9.2. Fiber Optik Kablo

Elektrik sinyallerinin ışık şeklinde iletildiği, saç telinden ince cam veya plastikten yapılmış kablodur. UTP bakır kabloların manyetik alandan ve radyo frekansından dolayı girişime uğraması gibi sorunlar fiber optik kabloda yaşanmaz. Bu nedenle daha uzak mesafelere (ortalama 2000 metre) kayıpsız ve hızlı olarak verinin iletilmesi mümkündür. Günümüzde dünyamızı örümcek ağı gibi örmüş fiber optik kablolar İnternet'in altyapısını oluşturmaktadır. Dünyayı saran ve denizlerin altına döşenmiş fiber optik kablo hatlarını görmek için https://www.submarinecablemap.com/ adresindeki web sitesini ziyaret edebilirsiniz.

1.9.3. Kablosuz Bağlantı

Günümüzde bilgisayar, laptop, cep telefonu gibi cihazların çoğunlukla kablosuz olarak ağa bağlandığını görüyoruz. Wireless LAN dediğimiz ve IEEE 802.11 standartları ile tanımlanan kablosuz ağ teknolojileri gün geçtikçe hızlanmakta ve kapsama alanını genişletmektedir. Wifi olarak da adlandırdığımız Wireless LAN'larda veri radyo dalgaları şeklinde iletilir. Kablosuz bağlantı özelliği olan routerlara wireless access point yani kablosuz erişim noktası denir. Kablosuz erişim noktaları çalışma mantığı bakımından hublara benzer. Bu nedenle kablosuz bağlantıdan kablolu bağlantıdaki verimi alamayız. Kalın ve yoğun demir içeren duvarların kablosuz sinyalleri emmesi ve diğer kablosuz erişim noktalarının girişim yapması nedeniyle hız azalmaları ve bağlantı kopmaları yaşanabilir. Kablosuz erişim noktalarının kullandığı IEEE standartları aşağıdaki tabloda gösterilmiştir.

Son yıllarda üretilen kablosuz ağ cihazları 802.11 ac standartı ile gelmektedir. Bu standart, 5GHz'de çalışır ve teorik olarak Gbit hızında iletişim sağlar.

1.10. MAC Adresi Nedir?

Bir bilgisayar ağa bağlanmak için bir NIC'e (Network Interface Card) ihtiyaç duyar. Bu ağ arayüz kartı kablolu olabileceği gibi kablosuz da olabilir. Şekilde masaüstü bilgisayarlarda kullanılan harici bir ağ arayüz kartı görülmektedir.

Günümüzde bu kablolu ağ arayüz kartları ana kart üzerinde tümleşik olarak gelmektedir. İşte bu kablolu veya kablosuz ağ arayüz kartlarının hepsinde 48 bitten oluşan ve heksadesimal sayı sistemi (16'lı sayı sistemi) ile gösterilen ve benzersiz MAC (Media Access Control) adresi bulunur. Aynı zamanda bir yönlendiricinin Default Gateway (Varsayılan Ağ Geçidi) olarak yapılandırılan arayüzünün de bir MAC adresi vardır. OSI modelinde bahsettiğimiz gibi 2. katmanda veriye kaynak ve hedef MAC adresi bilgisi eklenir. Windows'ta komut satırındayken (CMD) **ipconfig/all** komutu ile ağ arayüz kartımızın MAC adresini öğrenebiliriz. MAC adresi Hardware adres ve Physical adres olarak da isimlendirilir.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 94-E9-79-AC-D6-07
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fd18:d276:a855:6700:8495:616c:c551:3868(Preferred)
   Temporary IPv6 Address. . . . . . : fd18:d276:a855:6700:a99c:aff:99c2:18a0(Preferred)
   Link-local IPv6 Address . . . . . : fe80::8495:616c:c551:3868%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 11 Nisan 2018 Çarşamba 10:46:34
   Lease Expires . . . . . . . . . . : 12 Nisan 2018 Perşembe 21:29:41
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 143976825
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-5C-81-17-C8-D3-FF-EE-D4-EB
   DNS Servers . . . . . . . . . . . : fe80::1%4
                                       192.168.1.1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

1.11. IP Protokolü

İster yerel ağda isterse de İnternet'te olsun ağa bağlanan tüm cihazlar benzersiz bir mantıksal (logical) adrese sahip olmalıdır. Bu adres IP adresi (IP: Internet Protocol) olarak adlandırılır. TCP/IP protokol yığının IP tarafı bu adreslemeden sorumludur. IP adresleri IPv4 ve IPv6 olarak iki çeşittir. Burada IPv4 ayrıntılı olarak anlatılacaktır.

IPv4 adresleri 32 bitten oluşmaktadır. Aslında 32 tane sıfır ve birden (0-1) oluşan bu adresler kullanım kolaylığı bakımından desimal (onlu) sayı sistemine göre yazılır. Örneğin desimal olarak gösterilen 192.168.1.5 IP adresi aslında binary (ikili) 11000 000.10101000.00000001.00000101 olarak açılabilir.

32 bitlik IPv4 adresler 4 tane sekizli grup halinde aralarına nokta konularak yazılır ve bu her sekizli gruba oktet (sekizli) denir. Yani IPv4 adresler 4 oktetten oluşur.

1.12. IP Adresleri ve Sınıfları

IPv4 adresleri ilk oktetlerinin ilk bitlerine göre A, B, C, D ve E olmak üzere 5 sınıfa ayrılır. A sınıfı adreslerin ilk oktetindeki ilk bit sıfır, B sınıfı adreslerin ilk oktetindeki ilk bit bir, C sınıfı adreslerin ilk oktetindeki ilk iki bit bir, D sınıfı adreslerin ilk oktetindeki ilk üç bit bir, E sınıfı adreslerin ilk oktetindeki ilk dört bit bir olmaktadır. Aşağıdaki tabloda IP adres sınıfları ve aralıkları gösterilmiştir.

Adres Sınıfı	İlk Oktet Bitleri	Adres Aralığı	Adresin Network ve Host Bölümü	Varsayılan Alt Ağ Maskesi	Farklı Ağ ve Host Sayısı
A	00000000	1-127*	N.H.H.H	255.0.0.0 /8	2^7=128 Ağ 2^{24}-2=16777214 Host
B	10000000	128-191	N.N.H.H	255.255.0.0 /16	2^{14}=16384 Ağ 2^{16}-2=65534 Host
C	11000000	192-223	N.N.N.H	255.255.255.0 /24	2^{21}=2097150 Ağ 2^8-2=254 Host
D	11100000	224-239			
E	11110000	240-255			

* 127'li IP adresleri geri döngü (loopback) adresi olarak kullanılmaktadır.

IP adresleri genel (public) ve özel (private) olarak ikiye ayrılır. Özel IP adresleri LAN'de kullanılır ve İnternet'e yönlendirilmez, genel IP adresleri ise WAN yani İnternet'te kullanılır. LAN'de kullanılan birden çok bilgisayarın IP adresi İnternet'e çıkarken NAT (Network Address Translation) dediğimiz işleme tabi tutulur. Çoğu yönlendirici ve güvenlik duvarı NAT işlemini otomatik gerçekleştirir.

Aşağıda sınıflarına göre genel IP adresleri görülmektedir.

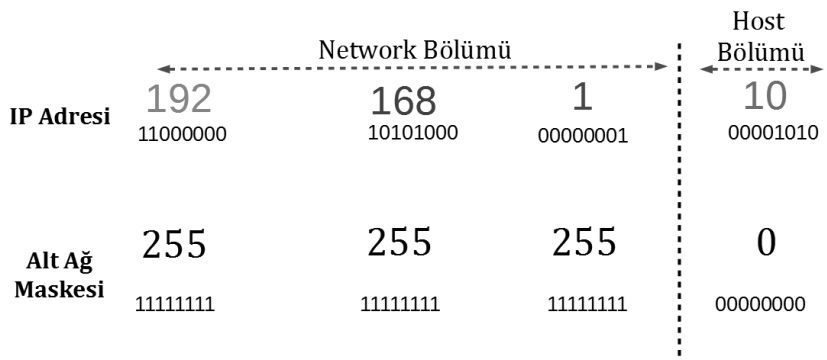
A Sınıfı: 1.0.0.0-126.255.255.255
B Sınıfı: 128.0.0.0-191.255.255.255
C Sınıfı: 192.0.0.0-223.255.255.255

Aşağıda sınıflarına göre genel IP adresleri görülmektedir.

A Sınıfı: 1.0.0.0-126.255.255.255
B Sınıfı: 128.0.0.0-191.255.255.255
C Sınıfı: 192.0.0.0-223.255.255.255

1.13. Alt Ağ Maskesi Ne İşe Yarar?

Subnet Mask yani alt ağ maskesi bir IP adresinin hangi kısmının network hangi kısmının host kısmı olduğunu gösterir. Bir oktetteki birler network kısmını gösterirken sıfırlar host kısmını gösterir. A sınıfı IP adresleri için 255.0.0.0, B sınıfı IP adresleri için 255.255.0.0, C sınıfı IP adresleri için 255.255.255.0 alt ağ maskesi kullanılır. Örneğin 192.168.1.10 IP adresi için varsayılan alt ağ maskesi 255.255.255.0'dır. Böylece 192.168.1. network kısmını gösterirken 10 host kısmını göstermektedir. Yani bu ağdaki tüm bilgisayarların IP adresleri 192.168.1 ile başlar ve 1,2,3,4,..... 255'e kadar devam eder.



1.14. DNS Nedir?

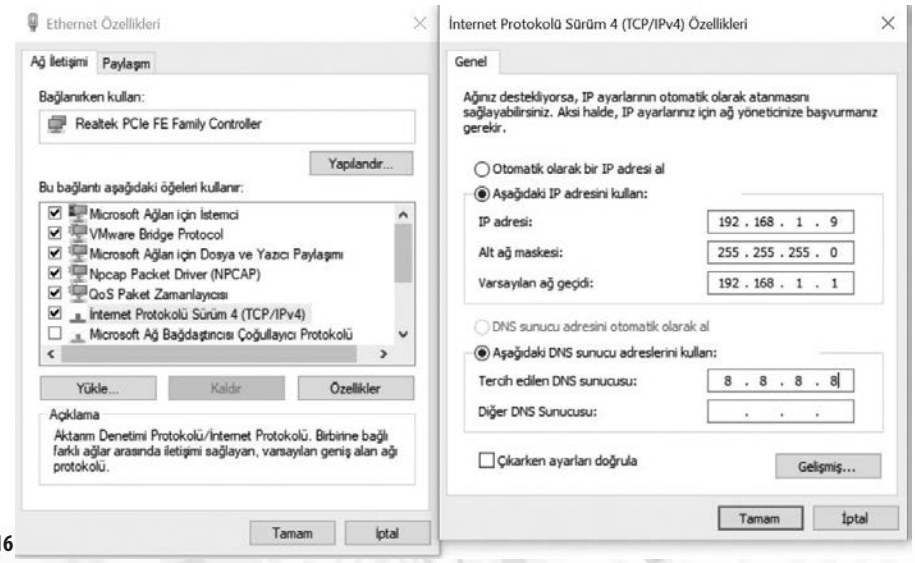
İnternet'te bir siteyi ziyaret ederken tarayıcımızın adres satırına www.site.com şeklinde bir adres yazarız. Buna domain name yani alan adı denir. Sonuçta bu domain name karşılığında bir IP adresi vardır. Fakat IP adreslerini hatırlamak zor olacağı için IP adresleri ile alan adlarını eşleştiren ve DNS (Domain Name System) denilen sistem geliştirilmiştir.

Örneğin www.google.com.tr adresini ziyaret etmek istediğinizde OSI modelinde bahsettiğimiz gibi Network katmanında hedef IP adresini yazmak gerekeceğinden öncelikle bu adresin öğrenilmesi gerekir. Bilgisayarda IP adresi yapılandırılırken DNS sunucu adresi de yazılır. İşte bu DNS sunucuya www.google.com.tr'nin IP adresi nedir diye sorulur ve gelen cevapta öğrenilen IP adresi hedef IP adresi olarak yazılır.

Tabi direkt DNS sunucuya sormadan önce Windows işletim sisteminde host dosyasına bakılır. Sonrasında ipconfig /displaydns komutu ile görüntüleyebileceğiniz DNS önbelleğine bakılır. Buralarda bulunamazsa DNS sunucuya sorulur. Eğer farklı bir ayar yapmadıysanız genellikle İnternet servis sağlayıcısının size sunduğu DNS sunucu adresini kullanırsınız.

1.15. DHCP İşimizi Kolaylaştırıyor mu?

Ağa bağlanan her cihazın benzersiz bir IP adresine ihtiyacı olduğunu söylemiştik. IP adresi ile birlikte alt ağ maskesi, varsayılan ağ geçidi ve DNS sunucu bilgilerinin de bir hosta atanması gerekir. İstersek bunu şekilde de görebileceğiniz gibi statik olarak yaparız.



Fakat yapılacak bir yazım hatası yapılandırmanın doğru olarak çalışmamasına neden olacak ayrıca çok büyük bir ağda tek tek her hosta IP yapılandırması gerçekleştirmek zor olacaktır. DHCP (Dynamic Host Configuration Protocol) ile IP yapılandırmasının otomatik olarak gerçekleşmesini sağlarız. **Otomatik olarak bir IP adresi al** seçeneği işaretlenerek bir hostun ağımızdaki bir DHCP sunucudan IP yapılandırmasını almasını sağlarız.

1.16. Yerel Ağdaki İletişim Çeşitleri

Yerel ağda bulunan bilgisayarlar arasındaki iletişim unicast (tekil yayın), broadcast (genel yayın) ve multicast (çoklu yayın) şeklinde gerçekleşir.

Unicast: Bir bilgisayardan çıkan mesajın sadece bir bilgisayara gitmesidir.

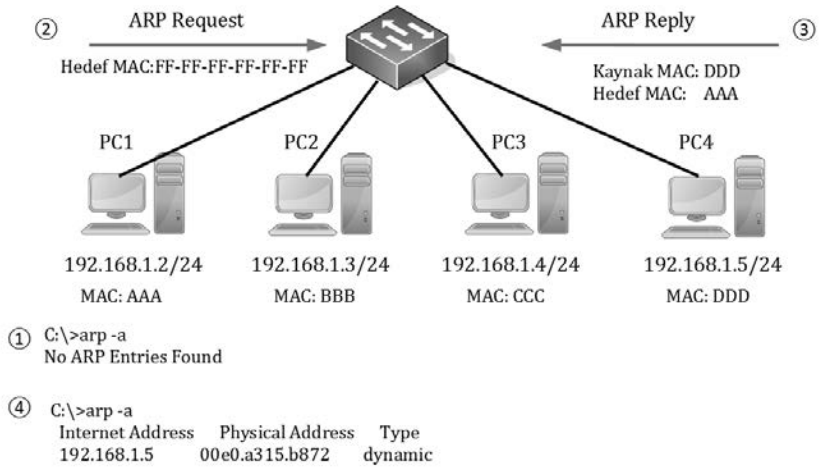
Broadcast: Bir bilgisayardan çıkan mesajın o ağdaki tüm bilgisayarlara gitmesidir.

Multicast: Bir bilgisayardan çıkan mesajın bir grup bilgisayara gitmesidir. Aşağıdaki şekilde unicast, broadcast ve multicast iletişim görülmektedir.

Resim:iletisim.png

1.17. ARP Protokolü?

Bir ağda bilgisayarlar şu şekilde haberleşir. Aşağıdaki şekle göre PC1 PC4 ile iletişim kurmak istesin. Veriye OSI'nin 2. katmanında (Veri Bağlantısı) hedef MAC adresinin eklendiğini söylemiştik. İşte PC1 önce arp tablosuna bakarak 192.168.1.5 IP adresine sahip PC4'ün MAC adresini arar. Komut satırında (CMD) **arp -a** ile ARP tablosu görüntülenebilir. Eğer yoksa ağdaki tüm bilgisayarlara hedef MAC adresi FF-FF-FF-FF-FF-FF olan bir broadcast mesaj gönderir. Bu mesaja ARP request (ARP isteği) denir. Mesajın anlamı şudur: Ben 192.168.1.2 IP adresine AAA MAC adresine sahip bilgisayar ağımdaki 192.168.1.5 ile haberleşmek istiyorum ama MAC adresini bilmiyorum ve öğrenmek istiyorum. Mesajı ağdaki tüm bilgisayarlar alır, PC4 hariç diğer hepsi açmadan çöpe atar. PC4 içinde MAC adresinin olduğu ARP Reply (ARP cevabı) mesajı gönderir. ARP Reply alan PC1 artık PC4'ün MAC adresini öğrenmiştir ve 2. Katmanda hedef MAC adresi olarak yazabilir. İşte IP adresi bilinen bilgisayarın MAC adresini öğrenmek için yapılan bu işleme ARP (Address Resolution Protocol-Adres Çözümleme Protokolü) denir.



Yerel ağımızda ARP benzeri broadcast mesaj üreten birçok protokol vardır. Her ne kadar sonuçta bir işlem gerçekleştirilse de bir yerel ağda aşırı broadcast trafiği ağda tıkanıklık ve yavaşlıklara yol açar. Piyasada çok sayıda bilgisayarın olduğu yerel ağlarda broadcast trafiğini minimize etmek için VLAN (Virtual LAN) çözümü kullanılır.

1.18. Sorun Giderme Komutları

Bir bilgisayarın ağa veya İnternet'e bağlanmasında sorun yaşandığında komut satırında (CMD) kullanılan bazı komutlar aracılığı ile sorunun nedenini araştırıp gidermeye çalışabiliriz. Komut satırında sıklıkla kullanılan sorun giderme komutları ping, ipconfig, nslookup ve tracert komutlarıdır.

1.18.1. Ping Komutu

ping komutu uçtan uca bağlantıyı test etmeye yarayan Mike Muus tarafından yazılmış bir programdır. Windows komut satırında 4 adet 32 byte'lık ICMP Echo Request (Yankı İsteği) paketi göndererek ICMP Echo Reply (Yankı Cevabı) bekler. 4 paket kayıpsız bir şekilde gidip gelirse iki bilgisayar arasında bağlantı doğrulanmış olur. Aşağıdaki örnekte www.google.com.tr adresine ping atılmıştır.

```
C:\>ping www.google.com.tr
Pinging www.google.com.tr [172.217.16.67] with 32 bytes of data:
Reply from 172.217.16.67: bytes=32 time=61ms TTL=51
Reply from 172.217.16.67: bytes=32 time=59ms TTL=51
Reply from 172.217.16.67: bytes=32 time=58ms TTL=51
Reply from 172.217.16.67: bytes=32 time=58ms TTL=51
```

Ping statistics for 172.217.16.67:
  Packets: Sent = 4, Received = 4, **Lost = 0 (0% loss),**
Approximate round trip times in milli-seconds:
  Minimum = 58ms, Maximum = 61ms, **Average = 59ms**

Yukarıdaki sonuçlara göre google.com.tr ile aramda bir bağlantı problemi yoktur. Çünkü kayıp paket sıfırdır. Gönderilen ping paketleri ortalama 59 mili saniyede gidip gelmiştir.

1.18.2. ipconfig Komutu

Bilgisayarımızın IP yapılandırmasını görüntülemek için **ipconfig** komutu kullanılır. Tüm yapılandırmayı görmek için (MAC adresleri vb.) ise **ipconfig/all** komutunu kullanırız. Aşağıdaki örnekte benim bilgisayarımın kablosuz ağ kartının IP yapılandırmasını görüyorsunuz.

C:\>ipconfig/all

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . : home
  Description . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
  Physical Address. . . . . : 94-E9-79-AC-D6-07
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  IPv6 Address. . . . . : fd18:d276:a855:6700:8495:616c:c551:3868(Preferred)
  Temporary IPv6 Address. . . . . : fd18:d276:a855:6700:c4de:18a1:e0d3:d032(Pref
erred)
  Link-local IPv6 Address . . . . . : fe80::8495:616c:c551:3868%4(Preferred)
  IPv4 Address. . . . . : **192.168.1.4(Preferred)**
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : 13 Nisan 2018 Cuma 11:58:24
  Lease Expires . . . . . : 14 Nisan 2018 Cumartesi 12:26:45
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 143976825
  DHCPv6 Client DUID. . . . . : 00-01-00-01-20-5C-81-17-C8-D3-FF-EE-D4-EB
  DNS Servers . . . . . : fe80::1%4
                          192.168.1.1
                          192.168.1.1
  NetBIOS over Tcpip. . . . . : Enabled

Yukarıdaki çıktıya göre bilgisayarımın kablosuz ağ kartı ADSL router'dan 192.168.1.4 IP adresini almıştır. Kablosuz ağ kartının MAC adresi 94-E9-79-AC-D6-07'dir. Varsayılan ağ geçidi IP adresi ise 192.168.1.1'dir.

1.18.3. Nslookup Komutu

Nslookup komutu ile bilgisayarımızın kullandığı DNS sunucuyu görüntüler, ardından girdiğimiz alan adlarının çözümlenmesini sağlarız. Aşağıdaki örnekte bilgisayarımın kullandığı DNS sunucu ve google.com.tr alan adının IP adresi çözümlemesini görüyorsunuz.

```
C:\>nslookup
Default Server: UnKnown
Address:  fe80::1
> www.google.com.tr
Server:  UnKnown
Address:  fe80::1
Non-authoritative answer:
Name:    www.google.com.tr
Addresses:  2a00:1450:4005:800::2003
          172.217.16.67
```

Yukarıdaki çıktıya göre bilgisayarımın varsayılan DNS sunucu adresi 192.168.1.1'dir. Yine google.com.tr IP adresi ise 172.217.16.67'dir.

1.18.4. Tracert Komutu

Tracert programı da ping gibi ICMP mesajlarını kullanır. Hedef bilgisayara giden paketlerin takibini yaparak problemin ve gecikmelerin nerede olduğunu görebiliriz. Aşağıdaki örnekte bilgisayarımdan çıkan paketler google.com.tr adresine gidene kadar hangi router'lardan geçmiş, ne kadar sürede geçmiş ve bu router'ların IP adreslerini görebiliriz.

```
C:\>tracert www.google.com.tr
Tracing route to www.google.com.tr [172.217.19.67]
over a maximum of 30 hops:
  1    2 ms    9 ms    2 ms  192.168.1.1
  2  152 ms    9 ms    8 ms  192.168.20.8
  3  150 ms   12 ms   11 ms  31.155.48.21
  4   76 ms   13 ms   15 ms  46.234.6.237
  5   11 ms   10 ms   11 ms  46.234.28.98
  6  119 ms   10 ms   13 ms  ae25-0.ist-001-score-2-re1.interoute.net [84.233.147.189]
```

```
 7   32 ms    32 ms    34 ms  ae5-0.bud-001-score-1-re0.interoute.net [195.81.54.37]
 8   45 ms    47 ms    57 ms  74.125.50.125
 9   88 ms    98 ms    47 ms  209.85.243.119
10   49 ms    54 ms    50 ms  108.170.236.247
11  275 ms   175 ms    58 ms  72.14.233.246
12   97 ms   101 ms    98 ms  66.249.95.149
13  169 ms   305 ms    66 ms  209.85.249.26
14  100 ms    98 ms   102 ms  216.239.49.191
15   61 ms    58 ms    58 ms  mil02s05-in-f67.1e100.net [172.217.19.67]
Trace complete.
```

Yukarıdaki çıktıya göre bilgisayarımdan çıkan paket öncelikle 192.168.1.1'den yani varsayılan ağ geçidinden çıkıp 31.155.48.21 IP adresine yani servis sağlayıcının yönlendiricisine gidiyor. Oradan da 46.234.6.237 IP adresine yönlendiriliyor. 15 sıçrama (hop) sonunda 172.217.19.67 IP adresine yani google.com.tr'ye ulaşıyoruz.

2

2. Siber Güvenliğe Giriş

Bu bölümde siber güvenliğin ne olduğunu öğrenip, siber güvenlik uzmanlarına ve siber güvenlik ürünlerine talebin artış nedenlerini göreceğiz. Kişisel verilerimizi korumanın öneminden kurumsal verinin gizliliğine dair tehditleri ve siber korsanların neden büyük bir tehdit olduğunu anlamış olacağız. Ayrıca artık savaşların silahla değil siber uzayda yapıldığına dair örneklere şahit olacağız.

2.1. Siber Güvenlik Nedir?

Finanstan eğitime, sağlıktan üretime kadar hemen hemen her sektörde ağa bağlanan cihaz sayısının hızla arttığı günümüzde bu cihazların güvenliğinin sağlanması en önemli konu haline gelmiştir. Cihazların güvenliğinin sağlanması demek aslında verilerimizin güvenliğinin sağlanması anlamına gelmektedir. Verilerinin güvenliğini sağlayamayan bir kurum her zaman para, itibar, zaman ve kaynak kaybetme tehlikesi ile yüz yüzedir.

Siber güvenlik, ağa bağlı sistemlerin ve verilerin yetkisiz kişilerin erişip zarar vermesini veya ele geçirmesini önlemeye yönelik çalışmaların bütünüdür. Siber güvenlik önlemlerini almak hem kişisel hem kurumsal hem de devletlerin en önemli görevi haline gelmiştir.

Her geçen gün İnternet'e bağlanıp daha fazla zaman geçirmeye başladık. Kendimizle, ailemizle, arkadaşlarımızla, işimizle ile ilgili birçok bilgiyi de İnternet'te paylaşmaya başladık. Aslında bu çevrimiçi kimliğimiz hakkında ayrıntılı bilgi vermek kendimizi

siber uzayda tehlikeye atmak demektir. Siber uzayda çevrimiçi kimliğimizi oluştururken ve korurken çok dikkatli olmalıyız.

İnternet'te paylaştığımız resimlerden kişisel bilgilerimize kadar her bilgi bizi tanımlayan özel alanlardır. Bununla beraber sağlık bilgilerimiz, finans bilgilerimiz de önemle korunması gereken verilerin başında gelmektedir. İşte bu verilerin gizliliğini sağlamak artık hayati bir önem arz etmektedir. Sizin kendi elinizle paylaştığınız verilerin gizliliğinden siz sorumlu olsanız da finans bilgilerinizi veya sağlık bilgilerinizi elinde tutan kurumlar da bu bilgilerin gizliliğinden sorumludur. Bu verilerin yetkili olmayan kişilerin eline geçmesi istenmeyen ve tehlikeli bir durumdur. Örneğin finans verilerinizi ele geçiren dolandırıcılar size çeşitli yollarla ulaşarak sizden para elde edip dolandırabilirler. Ya da resimlerinizi İnternet'te paylaştığınızda bu resimleri gören herkes alıp depolayabilir ve sizin aleyhinize kullanabilir.

Verileriniz sizin tarafınızdan saklanıyorsa sorumluluk size aittir. Ya başka kurumlar tarafından saklanan ve size ait olan verilerin güvenliği? Sağlık kayıtlarınız doktorunuzun ofisindeki bilgisayarda kayıtlıdır ya da şirketiniz varsa finansal bilgileriniz mali müşavirinizin bilgisayarındadır.

Sadece bilgisayarınıza kaydettiğiniz resim, doküman gibi bilgiler mi tehlikede? Bir web sitesinden alışveriş yaparken kredi kartı bilgilerinizi girerken bir bilgisayar korsanı kredi kartı bilgilerinizi çalabilir. Uzun sözün kısası siber uzay tehlikelerle dolu.

2.2. Siber Korsanlar Ne İstiyor?

Tabii ki paranızı. Siber saldırganlar yukarıda verdiğimiz örnekte olduğu gibi kredi kartı bilgilerinizi ya da İnternet bankacılığı bilgilerinizi ele geçirerek paranızı çalmak isteyebilir. Bunun dışında kişisel bilgilerinizi elde ederek bunları diğer siber korsanlara satabilir ya da kötü amaçlı kullanabilirler. Örneğin sizin hakkınızda ayrıntılı bilgi sahibi olan bir siber korsan profilinizi kopyalayarak bir sosyal medya hesabı açabilir ve akrabalarınızdan ve arkadaşlarınızdan sizin adınızı kullanarak para vb. maddi şeyler isteyebilir.

Siber korsanlar öncelikle paranızı çalmayı hedeflese de tek amaçları bu değildir. Kimlik bilgilerinizi çalan bir siber korsan adınıza şirket açarak sizi borçlandırabilir. Ya da sizin kimliğinizi kullanarak alış veriş yapar ve adınıza onlarca icra takibinin başlamasına neden olabilir.

Ne kadar dikkatli olmanız gerektiğinin farkında mısınız?

2.3. Veri Gizliliği, Bütünlüğü, Kullanılabilirliği

Kurumsal anlamda bakıldığında, personel bilgisinden bordro bilgilerine, şirketler arası teklif mektuplarından iş anlaşmalarına kadar birçok bilgi çok iyi saklanması gereken bilgi kapsamındadır. Nesnelerin İnternet'i (IoT) kavramıyla birlikte verinin çok büyüdüğü (Big Data) işlenmesinin özellikle de saklanmasının zor olduğu bir döneme girmiş bulunuyoruz.

Bu dönemde verinin **gizliliği, bütünlüğü ve kullanılabilirliği** daha önemli hale gelmiş bulunuyor. Gizlilik; kimlik doğrulama ve şifreleme yoluyla erişimi kısıtlayarak verilerin gizliliğini sağlar. Bütünlük; bilgilerin doğru ve güvenilir olduğunu garanti eder. Kullanılabilirlik, bilginin yetkili kişiler tarafından erişilebilir olmasını sağlar.

Gizlilik yerine mahremiyet terimini de kullanabiliriz. Şirket politikaları, bilgiye erişimi yetkili personelle sınırlamalı ve bu verileri yalnızca yetkili kişilerin görmesini sağlamalıdır. Veriler, bilgilerin güvenlik veya hassasiyet düzeyine göre bölümlere ayrılabilir. Örneğin, bir Java program geliştiricisi, tüm çalışanların kişisel bilgilerine erişmek zorunda kalmamalıdır. Ayrıca, çalışanlar kendilerini ve şirketi saldırılardan korumak için hassas bilgilerin korunmasında en iyi uygulamaları anlamak için eğitim almalıdırlar. Gizliliği sağlama yöntemleri arasında veri şifreleme, kullanıcı adı kimliği ve parola, iki faktörlü kimlik doğrulama gibi yöntemler kullanılabilir.

Bütünlük; tüm yaşam döngüsü boyunca verilerin doğruluğu, tutarlılığı ve güvenilirliğidir. Veriler taşıma sırasında yetkisiz kişilerce değiştirilmemelidir. Dosya izinleri ve kullanıcı erişim kontrolü yetkisiz erişimi engelleyebilir. Sürüm kontrolü yetkili kullanıcıların yanlışlıkla değiştirilmesini önlemek için kullanılabilir. Bozuk verilerin geri yüklenmesi için yedeklemeler mevcut olmalı ve aktarım sırasında verilerin bütünlüğünü doğrulamak için sağlama toplamı (hash) kullanılmalıdır.

Bir sağlama toplamı, yerel ağınızda veya Internet'te bir aygıttan diğerine aktarıldıktan sonra dosyaların veya karakter dizilerinin bütünlüğünü doğrulamak için kullanılır. Bir dosya indirildikten sonra, hash değerlerini kaynak dosyanın hash değeri ile karşılaştırmalısınız. Karma değerleri karşılaştırarak, dosyanın aktarım sırasında değiştirilmediğinden veya bozulmadığından emin olabilirsiniz. Siber korsanlar orijinal program dosyalarının içine backdoor denilen arka kapılar yerleştirerek bilgisayarınıza sızabilir. İşte hash değerini kontrol etmek bu tehlikeden sizi uzak tutar.

Kullanılabilirlik, ekipmanların bakımı, donanım onarımlarının yapılması, işletim sistemlerinin ve yazılımların güncel tutulması ve yedeklerin oluşturulması, ağın ve verilerin yetkili kullanıcılara sunulmasını sağlar. Doğal ya da insan kaynaklı felaketlerden hızla kurtulmak için planlar uygulanmalıdır. Güvenlik duvarları hizmet reddi (DoS) gibi saldırılardan kaynaklanan arıza sürelerine karşı koruma sağlar. Hizmet

reddi, bir saldırganın kaynakları boğma girişiminde bulunduğunda, hizmetlerin kullanıcılar tarafından kullanılamaması durumunda gerçekleşir.

2.4. Örnek Olaylarla Bir Siber Saldırının Sonuçları

Bir kurumu siber saldırılardan yüzde yüz oranında korumak hiçbir zaman mümkün değildir. Güvenliği kurmak ve sürdürmek her zaman önem verilmesi gereken bir konudur. Fakat her şeye rağmen iyi planlanmış ve zamanlanmış bir siber saldırı başarılı olacaktır. Siber saldırganlar şirket sunucularına erişerek kritik dosyalarınızı şifreleyerek sizden fidye talep edebilir. Ya da web sitenizde doğru olmayan bilgiler yayınlayarak şirketinizin itibarını küçük düşürebilir. Ya da şirket web sitesine erişimi tamamen engelleyerek maddi kayıplara yol açabilir.

Bir güvenlik ihlalinin parasal maliyeti, herhangi bir kayıp veya çalınan cihazın değiştirilmesi, mevcut güvenliğe yatırım yapılması ve binanın fiziksel güvenliğini güçlendirmekten çok daha yüksektir. Şirket, etkilenen tüm müşterilerin ihlale ilişkin olarak iletişim kurmasından sorumlu olabilir ve davaya hazırlıklı olmak zorunda kalabilir. Bütün bu kargaşanın sonucunda çalışanlar şirketi terk etmeyi seçebilir.

Şimdi yaşanmış birkaç olayla işin vahametini anlamaya çalışalım. Ortalama 12 çalışanı olan bir mali müşavirlik bürosunda, çalışanlardan birinin e-posta ekinde gelen ve telefon faturası şeklinde görünen zararlı yazılım içeren pdf belgesini açması sonucunda muhasebe yazılımının kurulu olduğu sunucudaki tüm bilgiler şifrelenmiş ve yedeklerinin olmaması nedeniyle bilgileri kurtarmak için siber korsanlara istedikleri fidye ödenmek zorunda kalınmıştır.

Yine geçtiğimiz yaz aylarında yedek almadan çalışan bir otelde, yönetim yazılımının bulunduğu sunucudaki bilgiler şifrelenmiş, otele misafir giriş çıkışı yapılamaz hale gelmiştir.

Şimdi de global bir örneğe bakalım. Dünya çapında milyonlarca müşterisi olan Equifax isimli kredi derecelendirme kuruluşu Eylül 2017'de siber saldırıya maruz kalmış ve müşterilerinin (yaklaşık 150 milyon) bilgilerini çaldırmıştır. Bu bilgiler içerisinde tüketicilerin isimleri, sosyal güvenlik numaraları, doğum tarihleri, adresleri ve diğer kişisel bilgiler bulunmaktadır. Olayın tek nedeni Equifax sistem yöneticilerinin veri tabanı yazılımında güncelleme yapmamasıydı. Bu olayın ortaya çıkması ile şirketin borsadaki değeri bir anda %20 azaldı ve ortalama 4 milyar dolar para kaybedildi. Siber korsanlar şirketten elde ettikleri bu bilgileri deep webte 2.5 milyon dolara satmaya çalıştılar.

2.5. Siber Saldırgan Tipleri

Siber saldırganların kimi ün yapmak, kimi para kazanmak kimi de belirli motivasyonlarla saldırı gerçekleştirse de büyük çoğunluğu maddi amaçlarla bu işi yaparlar. Şimdi bakalım siber saldırganlar kaç türe ayrılıyor ve her birinin özellikleri neler.

Amatörler: Script Kiddies de denen bu grup genelde İnternet'den buldukları hazır araçlar ile saldırı düzenlemeye çalışır. Network, kodlama, işletim sistemi gibi konularda ya az ya da hiç bilgi sahibi değillerdir. Birçoğu meraktan bu işi yaparken bir kısmı da web sitelerine izinsiz giriş yapıp ana sayfalarına takma adlarını (nick name) yazarak ün yapmak derdindedir. Her ne kadar hazır araçları kullansalar da yaptıkları zarar verici sonuçlar doğurabilir.

Hacker'lar: Çeşitli motivasyonlarla bilgisayar sistemlerine sızmaya çalışan beyaz, gri ve siyah şapkalı olarak adlandırılan, benim genelde siber korsan olarak adlandırdığım gruptur. Network, kodlama, işletim sistemleri vb. birçok konuda yeterli bilgiye sahip ve bu bilgilerini eğer iyi niyetle ve sistemlerin zafiyetlerini tespit etmek amaçlı kullanıyorlarsa beyaz şapkalı, bilgilerini kötü niyetle kullanıp bir çıkar amaçlıyorlarsa siyah şapkalı, bu ikisinin ortasında bir yerde iseler örneğin Mr.Robot dizisindeki Eliot ya da Matrix filmindeki Neo gibi gündüz iş yerinde beyaz şapka eve gidince siyah şapka takan tiplere ise gri şapkalı hacker denmektedir. Gri şapkalı hacker'lar sistemlerde buldukları açıkları sisteme hiçbir zarar vermeden ve bilgilerini çalmadan sistem yöneticilerine haber vererek bu iyi niyetleri karşılığında çeşitli maddi ödüller kazanabilirler.

Organize Gruplar: Bu grupta siber suçlular, hacktivistler, teröristler ve devlet destekli bilgisayar korsanları bulunur. Siber suçlular genellikle kontrol, güç ve zenginlik odaklı profesyonel suçlu gruplarıdır. Suçlular son derece sofistike ve organize olmuşlar ve siber suçları diğer suçlulara da hizmet olarak sunabilirler. Hacktivistler, kendileri için önemli olan konularda farkındalık yaratmak için politik açıklamalar yaparlar. Devlet destekli saldırganlar hükümeti adına istihbarat toplar ya da sabotaj yaparlar. Bu saldırganlar genellikle yüksek eğitimlidir ve iyi finanse edilirler ve saldırıları hükümetlerine faydalı olan belirli hedeflere odaklanır.

2.6. İç ve Dış Tehditler

Siber saldırılar sadece dışarıdan gelmez. Genel olarak siber tehditler iç ve dış tehditler olarak ikiye ayrılır.

İç tehditler, dış tehditlerden daha fazla zarar verme potansiyeline sahiptir, çünkü içerideki kullanıcılar binaya ve altyapı cihazlarına doğrudan erişime sahiptir. Çalışan-

lar ayrıca kurumsal ağ kaynakları ve gizli veriler ile farklı düzeylerde kullanıcı veya yönetici ayrıcalıkları hakkında bilgi sahibidir. İşinden ve yöneticilerinden memnun olmayan bir çalışan veya işten çıkarılan bir ağ yöneticisi sisteme çok büyük zararlar verebilir. Bazen de şirket içindeki önemli bilgiler içerideki çalışanlar aracılığı ile şirket dışına çıkarılabilir.

Amatörlerden veya yetenekli saldırganlardan gelen dış tehditler, ağ veya bilgi işlem cihazlarındaki güvenlik açıklarından yararlanabilir veya erişim kazanmak için sosyal mühendisliği kullanabilir.

İç ve dış tehditlere karşı alınacak önlemler birbirinden farklıdır ve yeri geldikçe değinilecektir.

2.7. Siber Savaş Başladı

Günümüzde savaşlar siber uzayda yaşanmaya başladı. Artık uçaklar, gemiler, bombalar ile değil de siber saldırılar ile ülkeler birbirlerine zarar verme ve üstünlük kurma çabasındalar.

Bir ülkenin desteklediği siber saldırganlar rakip ülkenin enerji sistemleri, ulaşım sistemleri veya bankacılık sistemlerine saldırı düzenleyerek, bu sistemlere zarar vermek ve rakip ülkede kaos çıkarmayı amaçlamaktadırlar.

Devlet destekli bir saldırının örneği olarak İran'ın nükleer zenginleştirme tesisine zarar verecek şekilde tasarlanmış Stuxnet kötü amaçlı yazılımı gösterilebilir. Stuxnet zararlısı, bilgi çalmak için hedef bilgisayarlara giriş yapmadı. Amacı bilgisayarlar tarafından kontrol edilen fiziksel ekipmana zarar vermekti. Kötü amaçlı yazılım içinde belirli bir görevi yerine getirmek üzere programlanmış modüler kodlamayı kullandı. Çalınan dijital sertifikaları kullandı ve sonunda yazılış amacını gerçekleştirerek İran'ın uranyum zenginleştirme tesisinin çalışmamasını sağladı.

Yine Rus hacker'lar 2007 yılında Estonya'ya siber saldırılar düzenleyerek özellikle de DDoS saldırıları ile kamu kuruluşlarının ve bankaların İnternet üzerinden verdikleri bütün hizmetlerin yaklaşık bir ay boyunca aksamasına neden oldular.

2.8. Yerel Kanunlar ve Mevzuatlar: 5651 ve 6698 Sayılı Kanunlar Ne İstiyor?

Şimdiye kadar tehlikenin ne kadar büyük olduğunu gördük ama durun daha bitmedi. Ülkemizde geçerli olan regülasyonlara (kanuni düzenlemeler) uymak zorunda olduğumuzu, bu kanunlara uygun tedbirleri almamız gerektiğini, almadığımızda da başımıza neler gelebileceğini görelim.

10-15 kullanıcılı bir mali müşavirlik bürosundan müşterilerine kablosuz İnternet kullanımı sağlayan bir kafeye kadar İnternet'in toplu olarak kullanıldığı her yerde bu İnternet kullanımının kayıt altına alınması gerekir. Kullanıcılardan birinin İnternet ortamında bir suç işlemesi durumunda eğer ilgili kayıtlar sunulamazsa ilgili işletmenin sahibi suçlu bulunacaktır.

5651 sayılı kanunun 7. maddesine göre ticari ya da ticari olmayan amaçla kullanıcılara İnternet erişimi sağlayan işletmeler toplu kullanım sağlayıcılar olarak tanımlanmış ve belirli yükümlülükler getirilmiştir. Buna göre 7. madde 2. bendine göre toplu kullanım sağlayıcılar kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür. Bu yükümlülüğü almayan işletmeler çeşitli cezalarla karşılaşabilmektedir. İşletmenizdeki İnternet kullanımını kayıt altına almak için bir **Tümleşik Güvenlik Sistemi** kullanmanız yeterlidir.

Yine aynı örnek üzerinden gidersek bir mali müşavirlik bürosu müşterilerinin bilgilerini her zaman en iyi şekilde saklamak zorundadır. Yukarıda örneklerini verdiğimiz bilgi sızıntıları gerçekleştiğinde 6698 Sayılı Kişisel Verilerin Korunması Kanununa göre sorumlu duruma düşmektedir. İlgili kanunun 8. maddesine göre kişilerin rızası olmadan verileri başka bir kuruma aktarılamaz. Yine 12. maddeye göre kişisel verilere erişilmesini engellemek ve muhafaza etmek ilgili kurumun sorumluluğundadır. Müşterilerinizin verileri şirketinizin içinde tutuluyorsa şirketinizin ağ güvenliğini çok iyi bir şekilde sağlamalısınız. Aksi halde şirket ağınıza sızan siber korsanlar müşteri bilgilerinizi çalarak satabilir sizi de zor durumda bırakabilir ve 15.000 Türk lirasından 1.000.000 Türk lirasına kadar ceza ödemenize neden olabilir. Bu konuda önlem almak için bir **Tümleşik Güvenlik Sistemi** kullanmanız yeterlidir.

3

3. Siber Saldırılar, Kavramlar ve Tehditler

Bu bölümde siber saldırılar hakkında bilgi sahibi olacak, saldırganların sistemlerine sızmasına neden olan güvenlik açıkları ve türlerini göreceğiz. Birçoğumuzun virüs diye bildiği malware (kötü amaçlı yazılım) ve türlerini tanıyacağız. Yine gerçekte çok güvenli sistemlerin insan zafiyeti istismar edilerek sosyal mühendislik ile nasıl ele geçirilebileceğini örneklerle göreceğiz. Son olarak en yaygın siber saldırılardan biri olan DoS (Denial of Service attack-Hizmet Engelleme) saldırıları hakkında bilgi sahibi olacağız.

3.1. Güvenlik Açıkları

Güvenlik açıkları, her türlü yazılım veya donanımda bulunan hatalardır. Bir güvenlik açığından haberdar olduktan sonra, kötü niyetli kullanıcılar bunu kullanmaya çalışır. İstismar (exploit), bilinen bir güvenlik açığından yararlanmak için yazılmış bir programı açıklamak için kullanılan terimdir. Güvenlik açığına karşı bir istismar kullanma eylemi saldırı olarak adlandırılır. Saldırının amacı, bir sisteme, barındırdığı verilere veya belirli bir kaynağa erişim sağlamaktır.

Yazılım güvenlik açıkları

Yazılım zafiyetleri genellikle işletim sistemi veya uygulama kodundaki hatalar tarafından ortaya çıkar. Üretici şirketlerin yazılım zafiyetlerini bulmak ve yamalamak için çaba sarf etmelerine rağmen, yeni zafiyetlerin yüzeye çıkması yaygındır.

Microsoft, Apple ve diğer işletim sistemi üreticileri neredeyse her gün yamalar ve güncellemeler yayınlıyor. Uygulama güncellemeleri de yaygındır. Web tarayıcıları, mobil uygulamalar ve web sunucuları gibi uygulamalar genellikle üretici şirketler veya kuruluşlar tarafından güncellenir. 2017 yılı Mayıs ayında dünya genelinde yüz binlerce bilgisayara bulaşan ve bulaştığı bilgisayardaki dosyaları şifreleyerek şifreleri açacak anahtar karşılığında fidye talep eden WannaCry isimli zararlı bir yazılım ortaya çıktı. Bu zararlı yazılım Microsoft işletim sistemine sahip cihazlara bulaşıyordu. Microsoft 2 ay önce bu açık için yama yayınlamış olmasına rağmen yama yapılmamış bilgisayarlar bu saldırıdan zarar gördüler.

Zero day yani sıfır gün ismi ile anılan saldırılar en tehlikeli olan saldırı tiplerindendir. Yazılımda açık bulan bir siber saldırgan bunu kullandığında ortaya çıkmasına bu isim verilir. Bundan sonra ilgili yazılım üreticisi bir yama yayınlayana kadar bu zafiyet istismar edilmeye devam eder.

Yazılım güncellemelerinin amacı güncel kalmak ve güvenlik açıklarını kapatmaktır. Bazı şirketler, yazılım açıklarını daha ortaya çıkmadan önce bulmaya adanan sızma testi ekiplerine sahipken, üçüncü taraf güvenlik araştırmacıları da yazılımlarda güvenlik açıklarını bulma konusunda uzmanlaşmıştır.

Google'ın Proje Sıfırı (Project Zero), bu tür uygulamalara mükemmel bir örnektir. Son kullanıcılar tarafından kullanılan çeşitli yazılımlarda birkaç güvenlik açığını keşfettikten sonra, Google yazılım açıklarını bulma konusunda kararlı bir ekip kurdu. Google gibi firmalar kendi güvenlik ekiplerini kurmanın yanında ürünlerinde zafiyet bulanları ödüllendirdikleri bug bounty denen programlar ilan etmiştir. Google yanında Yandex; Microsoft, Apple, Uber vb. birçok firmanın buna benzer programları vardır. Bug bounty yani ödül avcılığı ile bir yazılımda veya web sitesinde zafiyet bulup bunu uygun şekilde raporladığınızda binlerce dolara varan ödüller kazanmanız mümkündür. Bug bounty programları hakkında https://hackerone.com adresinden bilgi alabilirsiniz.

Donanım zayıflıkları

Donanım zayıflıkları genellikle donanım tasarımı kusurları olarak adlandırılır. Örneğin bir RAM bellekte birbirlerine çok yakın monte edilmiş kapasitörlerin yakınlık nedeniyle, komşu kapasitörleri etkileyebileceği keşfedilmiştir. Bu tasarım kusuruna dayanarak, Rowhammer adlı bir istismar oluşturuldu. Aynı adreslerdeki bellekleri tekrar tekrar yazarak, Rowhammer'ın yaptığı hücreler korunsa bile verilerin yakındaki adres bellek hücrelerinden alınmasına izin verir.

Donanım güvenlik açıkları, cihaz modellerine özeldir ve genellikle rastgele girişimlerle istismar edilmez. Son derece hedefli saldırılarda donanımsal istismarlar daha

yaygın olsa da, geleneksel kötü amaçlı yazılım koruması ve fiziksel güvenlik, günlük kullanıcı için yeterli korumadır.

3.2. Güvenlik Açığı Kategorileri

Çoğu yazılım güvenliği güvenlik açığı aşağıdaki kategorilerden birine girmektedir:

Arabellek taşması (Buffer overflow): Bu güvenlik açığı, bir arabelleğe sınırlarının ötesinde veri yazıldığı zaman ortaya çıkar. Tamponlar, bir uygulamaya tahsis edilen hafıza alanlarıdır. Bir arabelleğin sınırlarının ötesindeki verileri değiştirerek, uygulama diğer işlemlere ayrılan belleğe erişir. Bu, bir sistem çökmesine veya saldırganın ayrıcalıklarının artmasına neden olabilir.

Onaylanmamış giriş: Programlar genellikle veri girişi ile çalışır. Zararlı bir program, programın istenmeyen bir şekilde davranmasını zorlamak için tasarlanmış kötü amaçlı içeriğe sahip olabilir. Görüntü işleme için kullanılan bir programda kötü niyetli bir kullanıcı, geçersiz resim boyutlarına sahip bir resim dosyası oluşturabilir. Kötü amaçlarla hazırlanmış boyutlar, programı hatalı ve beklenmeyen boyutlarda arabellekleri ayırmaya zorlayabilir.

Yarış koşulları: Bu güvenlik açığı, bir olayın çıkışının sıralı veya zamanlanmış çıktılara bağlı olduğu zamandır. Bir yarış koşulu, gereken sıralı veya zamanlanmış olaylar doğru sırada veya doğru zamanlamada meydana gelmediğinde bir güvenlik açığı haline gelir.

Güvenlik uygulamalarındaki zayıflıklar: Sistemler ve hassas veriler, kimlik doğrulama, yetkilendirme ve şifreleme gibi tekniklerle korunabilir. Geliştiriciler, güvenlik açıkları oluşturacağı için kendi güvenlik algoritmalarını oluşturmaya çalışmamalıdır. Geliştiricilerin önceden oluşturulmuş, test edilmiş ve doğrulanmış güvenlik kitaplıklarını kullanmaları şiddetle tavsiye edilir.

Erişim denetimi sorunları: Erişim denetimi, kimin, bir dosya veya fiziksel kaynağa eriştiğini yönetmek ve kimin ne gibi şeyler yaptığını denetleme işlemidir. Örneğin, bir dosyaya erişimi olan ve okuma ve yazma hakkı olan biri erişim kontrollerinin uygunsuz kullanımıyla birçok güvenlik açığı oluşturabilir.

Neredeyse tüm erişim kontrolleri ve güvenlik uygulamaları, saldırganın hedef ekipmana fiziksel erişimi olduğunda aşılabilir. Örneğin, bir dosyanın izinlerinin nasıl ayarlandığına bakılmaksızın, cihaza fiziksel olarak erişen birisine karşı işletim sistemi, verileri doğrudan diskten okumasını engelleyemez. Makineyi ve içerdiği verileri korumak için, fiziksel erişim kısıtlanmalı ve verilerin çalınması veya bozulmasını önlemek için şifreleme teknikleri kullanılmalıdır.

3.3. Malware Türleri

Kötü Amaçlı Yazılımlar (Malware) için kısaca veri çalmak, erişim kontrollerini atlamak veya bir sisteme zarar vermek için kullanılabilecek herhangi bir koddur denilebilir. Aşağıda birkaç yaygın kötü amaçlı yazılım türü vardır:

Casus Yazılım (Spyware): Bu kötü amaçlı yazılım, kullanıcıyı izlemek ve casusluk yapmak için tasarlanmıştır. Casus yazılımlar genellikle etkinlik izleyicileri, tuş vuruşu toplama (key logger) ve veri yakalama içerir. Güvenlik önlemlerinin üstesinden gelmek için, casus yazılımlar genellikle güvenlik ayarlarını değiştirir. Casus yazılımlar genellikle meşru yazılımlarla veya Truva atları ile hedef sisteme bulaşır.

Reklam destekli yazılım (Adware): Reklamları otomatik olarak sunmak için tasarlanmıştır. Adware genellikle yazılımın bazı sürümleriyle yüklenir. Bazı reklam yazılımları yalnızca reklam yayınlamak için tasarlanmıştır, ancak reklam yazılımlarının casus yazılımlarla gelmesi de yaygındır.

Bot: Bir bot, genellikle çevrimiçi olarak harekete geçmek için tasarlanmış kötü amaçlı bir yazılımdır. Çoğu bot zararsız olsa da, kötü amaçlı botların artan kullanımı botnetlerdir. Botnetler (bot ağı) saldırgan tarafından sağlanan komutları sessizce beklemek üzere programlanan botlarla (zararlı yazılım bulaşmış bilgisayar) doludur. Genellikle lisanslı yazılımları kırmak için kullanılan yazılımlar ayrıca bilgisayarınızı bir botnetin parçası haline de getirir. Botnet ağındaki bilgisayarlar DDoS saldırısı amacıyla kullanılabilir. Yani siz farkında olmadan bir suç ağının parçası olursunuz.

Fidye yazılımı (Ransomware): Bu kötü amaçlı yazılım, bir bilgisayar sistemini veya içindeki dosyaları bir ödeme yapılıncaya kadar esir ettiği için bu ismi almıştır. Fidye yazılımı genellikle bilgisayardaki verileri kullanıcı tarafından bilinmeyen bir anahtarla şifreleyerek çalışır. Ransomware'in diğer bazı sürümleri, sistemi kilitlemek için belirli sistem güvenlik açıklarından yararlanabilir. Fidye yazılımı, indirilen bir dosya veya bazı yazılım güvenlik açığı tarafından yayılır.

Scareware: Bu kullanıcıyı korku temelli belirli bir eylemi yapmaya ikna etmek için tasarlanmış bir tür kötü amaçlı yazılım türüdür. Scareware, işletim sistemi diyalog pencerelerini andıran açılır pencereler açar. Bu pencereler, sistemin risk altında olduğunu bildiren veya normal çalışmaya dönmek için belirli bir programın yürütülmesini gerektiren sahte mesajlar iletir. Gerçekte, hiçbir sorun tespit edilmemiştir ve aksine kullanıcı söz konusu programı yürütmeyi üzere kabul ederse ve temizlerse, sisteme kötü amaçlı yazılım bulaşacaktır.

Rootkit: Bu kötü amaçlı yazılım, bir arka kapı oluşturmak için işletim sistemini değiştirmek üzere tasarlanmıştır. Saldırganlar daha sonra bilgisayara erişmek için bu arka kapıyı kullanırlar. Çoğu rootkit, ayrıcalık yükseltme gerçekleştirmek ve sistem dosyalarını değiştirmek için yazılım güvenlik açıklarından yararlanır. Ayrıca, rootkit'lerin sistem adli tıp ve izleme araçlarını modifiye etmeleri ve bunların tespit etmelerini zor hale getirmeleri de yaygındır. Genellikle, rootkit bulaşmış bir bilgisayar formatlanmalı ve işletim sistemi yeniden yüklenmelidir.

Virüs: Bir virüs, genellikle meşru programlara ekli olan kötü amaçlı yürütülebilir bir koddur. Çoğu virüs, son kullanıcı aktivasyonunu gerektirir ve belirli bir zamanda veya tarihte etkinleştirilebilir. Virüsler zararsız olabilir ve basitçe bir resim gösterebilir veya verileri değiştiren veya silenler gibi yıkıcı olabilirler. Virüsler ayrıca algılamayı önlemek için mutasyona uğrayacak şekilde programlanabilir. Çoğu virüs artık USB sürücüler, optik diskler, ağ paylaşımları veya e-posta ile yayılmaktadır.

Truva atı (Trojan): Truva atı, istenen operasyonun kılığına girerek kötü amaçlı operasyonlar yapan kötü amaçlı yazılımdır. Bu kötü amaçlı kod, onu çalıştıran kullanıcının ayrıcalıklarını kullanır. Çoğu zaman, Truva atları görüntü dosyalarında, ses dosyalarında veya oyunlarda bulunur. Bir Truva atı, bir virüsten farklıdır çünkü kendisini yürütülebilir olmayan dosyalara bağlar.

Solucanlar (Worm): Solucanlar, ağlardaki güvenlik açıklarını bağımsız olarak istismar ederek kendilerini kopyalayan zararlı kodlardır. Solucanlar genellikle ağları yavaşlatır. Bir virüs çalıştırmak için bir ana bilgisayar programı gerektirirken, solucanlar kendi başlarına çalışabilirler. İlk enfeksiyondan başka, artık kullanıcı katılımını gerektirmez. Bir bilgisayara enfekte olduktan sonra, solucan ağ üzerinden çok hızlı bir şekilde yayılabilir. Solucanlar benzer desenleri paylaşırlar.

Solucanlar, internetteki en yıkıcı saldırılardan sorumludur. 2001 yılında Kod Kırmızı solucanı 658 sunucuyu etkilemiştir. 19 saat içinde, solucan 300.000'den fazla sunucuya bulaşmıştı.

Ortadaki Adam (Man-In-The-Middle (MitM)): MitM, saldırganın kullanıcının bilgisi olmadan bir cihaz üzerinde kontrol sahibi olmasını sağlar. Bu erişim seviyesiyle, saldırgan, kullanıcının hedeflediği yere ulaşmadan önce kullanıcı bilgilerini yakalayabilir ve değiştirebilir. MitM saldırıları finansal bilgileri çalmak için yaygın olarak kullanılmaktadır. Saldırganlara MitM yetenekleri sağlamak için birçok kötü amaçlı yazılım ve teknik vardır.

Man-In-The-Mobile (MitMo): Ortadaki adam saldırısının bir varyasyonu olan MitMo, bir mobil cihaz üzerinde kontrolü ele geçirmek için kullanılan bir saldırı türüdür. Enfekte olduğunda mobil cihaza, kullanıcı açısından hassas bilgileri saldır-

ganlara göndermek için talimat verilebilir. MitMo yeteneklerine sahip bir istismar örneği olan ZeuS, saldırganların kullanıcılara gönderilen 2 adımlı doğrulama SMS mesajlarını sessizce yakalamasına izin veriyor.

3.4. Malware Belirtileri

Kötü amaçlı yazılım belirtileri: Bir sisteme bulaşmış olan kötü amaçlı yazılım türünden bağımsız olarak aşağıdaki belirtileri sonuç verebilir;

- CPU kullanımında bir artış var.
- Bilgisayar hızında bir düşüş var.
- Bilgisayar sık sık donuyor veya çöküyor.
- Web tarama hızında bir azalma var.
- Ağ bağlantılarında açıklanamayan sorunlar var.
- Dosyalar değiştirildi.
- Dosyalar silindi.
- Bilinmeyen dosyalar, programlar veya masaüstü simgeleri var.
- Bilinmeyen süreçler çalışıyor.
- Programlar kendiliğinden kapanıyor ya da yeniden yapılandırılıyor.
- E-posta kullanıcının bilgisi veya izni olmadan gönderilmektedir.

3.5. Sosyal Mühendislik

Sosyal mühendislik, bireyleri eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönlendirmeye çalışan bir erişim saldırısıdır. Sosyal mühendisler genellikle insanların yararlı olma isteklerine güvenir aynı zamanda insanların zayıf yönlerini de avlarlar. Örneğin, bir saldırgan yetkili bir çalışanı acil ağ erişimi gerektiren bir sorunla arayabilir. Saldırgan, çalışanın egosuna hitap edebilir, yetkili kişilerin isimlerini kullanarak otoriteye başvurabilir ya da çalışanın bilgisizliğini kullanabilir.

Bazı sosyal mühendislik saldırıları şunlardır:

Bağlama: Saldırgan bir kişiyi aradığında ve ayrıcalıklı verilere erişme girişimi sırasında onlara yalan söylediğinde ortaya çıkar. Örnek olarak alıcının kimliğini doğrulamak için kişisel veya finansal verilere ihtiyaç duyduğunu iddia eden bir saldırganı verebiliriz.

Yakından takip (Tailgating): Bu, bir saldırganın yetkili bir kişiyi güvenli bir yere hızlı bir şekilde takip etmesidir.

Taviz: Bir saldırganın ücretsiz hediye gibi bir şey karşılığında birinden kişisel bilgi talep etmesidir.

3.6. Wi-Fi Parolanız Kırılmasın

Wi-Fi şifre kırma, kablosuz ağı korumak için kullanılan şifreyi bulma işlemidir. Aşağıdakiler şifre kırmada kullanılan bazı tekniklerdir:

Sosyal mühendislik: Saldırgan, şifreyi bilen bir kişiyi manipüle ederek elde eder.

Kaba kuvvet saldırıları (Brute force): Saldırgan, şifreyi tahmin etme girişimi sırasında çeşitli olası şifreleri dener. Şifre 4 basamaklı bir sayıysa, örneğin, saldırgan 10000 kombinasyonun her birini denemek zorunda kalacaktır. Kaba kuvvet saldırıları genellikle bir kelime listesi dosyası içerir. Bu, bir sözlükten alınan sözcüklerin bir listesini içeren bir metin dosyasıdır. Bir program daha sonra her kelimeyi ve ortak kombinasyonları dener. Kaba kuvvet saldırıları zaman aldığı için, karmaşık şifrelerin tahmin edilmesi daha uzun sürer.

Ağ Dinleme (sniffing): Ağa gönderilen paketleri dinleyerek ve yakalayarak, şifrelenmemiş olarak gönderilen (düz metin halinde) şifreyi bulabilir. Eğer şifrelenmişse, saldırgan bir şifre kırma aracı kullanarak bunu açığa çıkarabilir.

3.7. Kimlik Avı

Kimlik avı (phishing), kötü amaçlı biri tarafından, meşru ve güvenilir bir kaynaktan gelen gizli bir e-posta gönderilmesidir. Mesajın amacı, alıcının cihazlarına kötü amaçlı yazılım yüklemek veya kişisel veya finansal bilgileri paylaşmak için kandırmaktır. Kimlik avının bir örneği, bir perakende satış mağazası tarafından gönderilmiş gibi görünen ve kullanıcıya bir ödül talep etmek için bir bağlantıyı tıklamasını isteyen bir e-postadır. Bağlantı, kişisel bilgi isteyen sahte bir siteye gidebilir veya bir virüs kurabilir.

Hedefe yönelik kimlik avı (Spear phishing): Hedefli bir phishing saldırısıdır. Bu saldırı türünde e-postalar belirli bir kişiye özel olarak düzenlenir. Saldırgan, e-postayı göndermeden önce hedefin ilgi alanlarını araştırır. Örneğin, bir saldırgan hedefin arabalarla ilgilendiğini öğrenir ve belirli bir araç modelini satın almak için uğraşır. Saldırgan, hedefin üye olduğu aynı araba tartışma forumuna katılır, bir araba satış teklifi verir ve hedefe e-posta gönderir. E-posta arabanın resimleri için bir bağlantı içerir. Hedef, bağlantıya tıkladığında, hedef bilgisayarın bilgisayarına kötü amaçlı yazılım yüklenir.

3.8. Güvenlik Açıklarının Sömürülmesi

Güvenlik açıklarından yararlanmak, yaygın olarak kullanılan bir sızma yöntemidir. Saldırganlar, bilgisayarları hakkında bilgi edinmek için ağı tarar. Aşağıda güvenlik açıklarından yararlanmak için yaygın bir yöntem vardır:

1) Hedef sistem hakkında bilgi toplayın. Bu bir port tarayıcı veya sosyal mühendislik gibi birçok farklı şekilde yapılabilir. Amaç, hedef bilgisayar hakkında olabildiğince fazla bilgi edinmektir.

2) 1. adımda öğrenilen ilgili bilgilerin bir parçası işletim sistemi, sürümü ve üzerinde çalışan hizmetlerin bir listesi olabilir.

3) Hedefin işletim sistemi ve sürümü biliniyorsa, saldırgan OS'in veya diğer işletim sisteminin bu sürümüne özgü bilinen güvenlik açıklarını arar.

4) Bir güvenlik açığı bulunduğunda, saldırgan kullanmak için önceden yazılmış bir kodu arar. Hiçbir istismar yazılmamışsa, saldırgan bir istismar yazmayı düşünebilir.

Gelişmiş Kalıcı Tehditler

Sızma işleminin gerçekleştirilmesinin bir yolu, gelişmiş kalıcı tehditlerdir (APT'ler). Belirli bir hedefe karşı çok aşamalı, uzun vadeli, gizli ve gelişmiş bir operasyondan oluşurlar. Gereken karmaşıklığı ve beceri seviyesi nedeniyle, bir APT genellikle iyi finanse edilir. Bir APT, kurumları veya ülkeleri ticari ya da politik nedenlerle hedefler.

Genellikle ağ tabanlı casusluk ile ilgili olarak, APT'nin amacı, hedeflenen sistemlerin bir veya daha fazlasına özelleştirilmiş kötü amaçlı yazılım dağıtmak ve fark edilmeden kalmaktır. Birden fazla işlem evresi ve farklı aygıtları etkileyen ve belirli işlevleri gerçekleştiren çeşitli özelleştirilmiş kötü amaçlı yazılım türleriyle, bireysel bir saldırgan, APT'leri gerçekleştirmek için beceri kümesine, kaynaklara veya kalıcılığa sahip değildir.

3.9. Hizmet Engelleme (DoS/DDoS) Saldırıları

Hizmet Reddi (DoS) saldırıları bir tür ağ saldırısıdır. Bir DoS saldırısı, ağ hizmetinin kullanıcılara, cihazlara veya uygulamalara bir çeşit kesintisi ile sonuçlanır. İki büyük DoS saldırısı türü vardır:

Ezici Trafik Miktarı: Bir ağ, sunucu veya uygulama, işleyemediği bir hızda çok büyük miktarda veri gönderildiğinde gerçekleşir. Bu, iletim veya yanıtta bir yavaşlamaya veya bir aygıtın veya hizmetin çökmesine neden olur.

Kötü Amaçlı Biçimlendirilmiş Paketler: Kötü amaçlı olarak biçimlendirilmiş bir paket, bir ana bilgisayara veya uygulamaya gönderildiğinde ve alıcı bunu gerçekleştiremediğinde ortaya çıkar. Örneğin, bir saldırgan, uygulama tarafından tanımlanamayan veya hatalı biçimlendirilmiş paketleri iletir. Bu, alıcı aygıtın çok yavaş çalışmasına veya çökmesine neden olur.

DoS saldırıları büyük bir risk olarak kabul edilir, çünkü iletişimi kolayca kesebilir ve önemli ölçüde zaman ve para kaybına neden olabilirler. Bu saldırıların vasıfsız bir saldırgan tarafından bile yürütülmesi nispeten kolaydır.

DDoS

Dağıtılmış DoS Saldırısı (DDoS) bir DoS saldırısına benzer, ancak birden çok koordineli kaynaktan kaynaklanır. Örnek olarak, bir DDoS saldırısı aşağıdaki gibi oluşabilir:

Bir saldırgan, botnet adı verilen virüslü ana bilgisayarlardan oluşan bir ağ oluşturur. Enfekte bilgisayarlara zombiler denir. Zombiler işleyici sistemleri tarafından kontrol edilir.

Zombi bilgisayarlar sürekli olarak daha fazla ana bilgisayarı tarayarak daha fazla zombiye yol açar. Hazır olduklarında bilgisayar korsanı, zombilerin botnetini DDoS saldırısı yapmak için işleyici sistemlere talimat verir.

3.10. SEO Zehirlenmesi

Google gibi arama motorları, sayfaları sıralayarak ve kullanıcıların arama sorgularını temel alarak alakalı sonuçlar sunarak çalışır. Web sitesi içeriğinin alaka düzeyine bağlı olarak, arama sonucu listesinde daha yüksek veya daha düşük görünebilir. Arama Motoru Optimizasyonu (SEO), bir web sitesinin bir arama motorundaki sıralamasını iyileştirmek için kullanılan bir tekniktir. Birçok şirket, web sitelerini daha iyi konumlandırmak için optimize etmede uzmanlaşırken, kötü niyetli bir kullanıcı kötü niyetli bir web sitesinin arama sonuçlarında daha yüksek görünmesini sağlamak için SEO kullanabilir. Bu teknik SEO zehirlenmesi olarak adlandırılır.

SEO zehirlenmesinin en yaygın amacı, kötü amaçlı yazılım barındırabilecek veya sosyal mühendislik gerçekleştirebilecek kötü amaçlı sitelere trafiği artırmaktır. Kötü amaçlı bir siteyi arama sonuçlarında daha üst sıralara zorlamak için saldırganlar popüler arama terimlerinden yararlanır.

4

4. Verilerin, Ağların ve Cihazların Korunması

Bu bölümde kişisel cihazlarınıza ve kişisel verilerinize odaklanacağız. Cihazlarınızı korumak, güçlü şifreler oluşturmak ve kablosuz ağları güvenli hale getirmek için ipuçları vereceğiz. Ayrıca verilerinizi nasıl güvenli bir şekilde koruyacağınızı öğreneceksiniz.

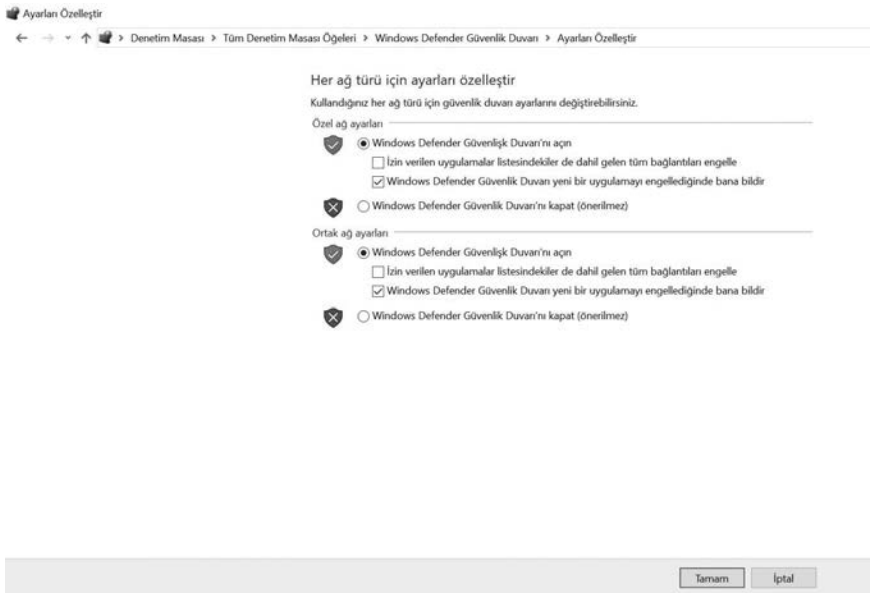
Çevrimiçi verileriniz siber korsanların ilk hedefidir. Bu bölümde, verilerinizi güvenli bir şekilde muhafaza etmenize yardımcı olacak kimlik doğrulama tekniklerine kısaca değineceğiz. Ayrıca, çevrimiçi verilerinizin güvenliğini sağlarken neleri de yapmamanız gerektiğiyle ilgili ipuçları vereceğiz.

4.1. Bilgisayarların Korunması

Bilgi işlem cihazlarınız verilerinizi saklar ve çevrimiçi hayatınızın merkezidir. Aşağıda, bilgi işlem cihazlarınızı izinsiz girişlerden korumak için atabileceğiniz adımların kısa bir listesi bulunmaktadır:

Güvenlik Duvarını Açık Tutun: Bir yazılım güvenlik duvarı veya bir yönlendirici üzerindeki bir donanım güvenlik duvarı olsun, bilgisayar korsanlarının kişisel veya şirket verilerinize erişmesini önlemek için güvenlik duvarı açılmalı ve güncellenmelidir. Windows›un güncel sürümlerinde örneğin Windows 7, 8 ve 10'da yazılımsal bir güvenlik duvarı vardır ve varsayılan olarak açık gelmektedir. Hiçbir

şekilde bunu kapatmanız tavsiye edilmez. Aşağıdaki şekilde Windows 10 güvenlik duvarı ayarları görünmektedir.



Antivirüs ve Antispyware kullanın: Bilgisayarınıza ve verilerinize erişim elde etmek için bilgi işlem cihazlarınıza virüs, Truva atı, solucan, fidye ve casus yazılım gibi kötü amaçlı yazılımlar izinsiz olarak yüklenir. Virüsler verilerinizi yok edebilir, bilgisayarınızı yavaşlatabilir veya bilgisayarınızı ele geçirebilir. Virüslerin bilgisayarınızı ele geçirmesinin bir yolu, spam göndericilerin hesabınızı kullanarak e-posta yayınlamasına izin vermektir. Casus yazılımlar çevrimiçi aktivitelerinizi izleyebilir, kişisel bilgilerinizi toplayabilir veya çevrimiçi olduğunuzda web tarayıcınızda istenmeyen pop-up reklamlar gösterebilir. İlk etapta casus yazılımlardan kaçınmak için yalnızca güvenilir web sitelerinden yazılım indirmeniz tavsiye edilir. Virüsten koruma yazılımı, bilgisayarınızı ve gelen e-postaları virüs taraması yapmak ve bunları silmek için tasarlanmıştır. Bazı antivirüs yazılımları antispyware içerir.

İşletim Sisteminizi ve Tarayıcınızı Yönetin: Bilgisayar korsanları, işletim sisteminizdeki ve web tarayıcınızdaki güvenlik açıklarından yararlanmaya çalışır. Bilgisayarınızı ve verilerinizi korumak için, bilgisayarınızdaki ve tarayıcınızdaki güvenlik ayarlarını orta veya daha yüksek bir değere ayarlayın. Bilgisayarınızın işletim sistemini web tarayıcılarınız da dahil olmak üzere güncelleyin ve üreticilerden en son yazılım yamaları ve güvenlik güncellemelerini düzenli olarak indirin ve yükleyin.

Tüm Aygıtlarınızı Koruyun: Masaüstü bilgisayarlarınız, dizüstü bilgisayarlarınız, tabletleriniz veya akıllı telefonlarınız, yetkisiz erişimi önlemek için parola korumalı olmalıdır. Saklanan bilgiler özellikle hassas veya gizli ise şifrelenmelidir. Mobil

cihazlar için çalınması veya kaybolması durumunda gerekli bilgileri başka bir yere yedekleyin. Mobil cihazlarınızdan herhangi birinin çalınması durumunda, hırsızların, iCloud veya Google Drive gibi bulut depolama servis sağlayıcınız aracılığıyla tüm verilerinize erişimi olabilir.

IoT cihazları diğer bilgi işlem cihazlarınızdan daha büyük bir risk oluşturur. Masaüstü, dizüstü bilgisayar ve mobil platformlar sık sık yazılım güncellemeleri alırken, IoT cihazlarının çoğu hâlâ orijinal donanımlarına sahiptir. Aygıt yazılımında güvenlik açıkları bulunursa, IoT aygıtı savunmasız kalabilir. IoT cihazları genellikle İnternet erişimi gerektirecek şekilde tasarlanmıştır. İnternete ulaşmak için, çoğu IoT cihaz üreticisi, müşterinin yerel ağına güvenir. Sonuç olarak, IoT cihazlarının açık oluşturması çok muhtemeldir ve bunun sonucunda müşterinin yerel ağına ve verilerine erişime izin verirler. Bu senaryodan kendinizi korumanın en iyi yolu, yalnızca başka bir IoT cihazıyla paylaşarak, yalıtılmış bir ağ kullanan IoT cihazlara sahip olmaktır.

4.2. Kablosuz Ağların Korunması

Kablosuz ağlar, dizüstü bilgisayarlar ve tabletler gibi Wi-Fi özellikli cihazların, SSID (Service Set Identifier-Servis Kümesi Tanımlayıcısı) olarak bilinen ağ tanımlayıcısı aracılığıyla ağa bağlanmasına izin verir. Davetsiz misafirlerin evinizin kablosuz ağına girmesini önlemek için, tarayıcı tabanlı yönetim arabirimi için önceden ayarlanmış SSID ve varsayılan şifre değiştirilmelidir. Bilgisayar korsanları, bu tür varsayılan erişim bilgilerini çok kolay bir şekilde tespit edebilir. İsteğe bağlı olarak, kablosuz yönlendirici, ağı keşfetmek için ek bir engel oluşturan SSID'yi yayınlamayacak şekilde de yapılandırılabilir. Bununla birlikte, bu bir kablosuz ağ için yeterli güvenlik olarak düşünülmemelidir. Ayrıca, kablosuz yönlendiricideki kablosuz güvenliği WPA2 şifreleme özelliğini etkinleştirerek şifrelemelisiniz. WPA2 şifrelemesi etkin olsa bile, kablosuz ağ hala savunmasız olabilir. 2017'de, WPA2 protokolünde bir güvenlik hatası tespit edildi. Bu kusur, bir davetsiz misafirin kablosuz yönlendirici ile kablosuz istemci arasındaki şifrelemeyi kırmasına ve izinsiz giriş yapan kişinin ağ trafiğine erişmesine ve işlemesine izin verir. Bu açık tüm modern korumalı Wi-Fi ağlarını etkiler. Bir saldırganın etkilerini azaltmak için, tüm ürünleri güncelleştirmek gerekir. Güvenlik güncelleştirmeleri kullanıma sunulduğunda kablosuz yönlendiriciler, dizüstü bilgisayarlar ve mobil aygıtlar gibi kablosuz özellikli aygıtlar bunu hemen gerçekleştirmelidir. Kablolu NIC olan dizüstü bilgisayarlar veya diğer cihazlar için, kablolu bir bağlantı bu güvenlik açığını azaltabilir. Ayrıca, kablosuz ağı kullanırken verilerinize yetkisiz erişimi önlemek için güvenilir bir VPN hizmetini de kullanabilirsiniz.

Evden uzakta olduğunuzda, herkese açık bir Wi-Fi noktası (örneğin bir kafede veya restorandaki), çevrimiçi bilgilerinize erişmenizi ve İnternet'te gezinmenizi sağlar.

Ancak, herhangi bir hassas kişisel bilginin (kredi kartı, Facebook şifresi vb.) halka açık bir kablosuz ağ üzerinden erişilmemesi veya gönderilmemesi en iyisidir. Bilgisayarınızın dosya ve medya paylaşımı ile yapılandırılmış olup olmadığını ve şifreleme ile kullanıcı kimlik doğrulaması gerektirdiğini doğrulayın. Herkese açık bir kablosuz ağ kullanırken bilgilerinizi ("gizlice dinleme" olarak bilinir) yakalamalarını engellemek için, şifreli VPN tünellerini ve hizmetlerini kullanın. VPN hizmeti, bilgisayarınız ve VPN servis sağlayıcınızın VPN sunucusu arasında şifreli bir bağlantı ile İnternet'e güvenli erişim sağlar. Şifrelenmiş bir VPN tüneli sayesinde, verileriniz ele geçirilse bile bu veriler çözülebilir değildir.

Akıllı telefonlar ve tabletler gibi birçok mobil cihaz, Bluetooth aracılığıyla kablosuz iletişim kurabilir. Bu özellik, Bluetooth özellikli cihazların birbirine bağlanmasına ve bilgi paylaşmasına olanak tanır. Ne yazık ki, Bluetooth bazı cihazlarda siber korsanların uzaktan erişim kontrolleri kurmak, kötü amaçlı yazılım dağıtmak gibi kötü amaçlı kullanımlarına neden olabilir. Bu sorunları önlemek için kullanmadığınız zamanlarda Bluetooth'u kapalı tutun.

4.3. Parolaların Korunması

Her çevrimiçi hesap için benzersiz parolalar kullanın. Muhtemelen e-posta, sosyal medya, vb. gibi birden fazla çevrimiçi hesabınız var. Her hesabın benzersiz bir parolası olmalıdır. Yani e-posta parolanız ile Facebook parolanız aynı olmamalıdır. Diyebilirsiniz ki hatırlanması gereken birçok şifre var. Ancak, güçlü ve benzersiz şifreler kullanmamak sizi ve verilerinizi siber korsanlara karşı savunmasız bırakır. Tüm çevrimiçi hesaplarınız için aynı şifreyi kullanmak, tüm kilitli kapılarınız için aynı anahtarı kullanmak gibidir, eğer bir saldırgan sizin anahtarınızı almak isterse, sahip olduğunuz her şeye erişme yetisine sahip olacaktır. Suçlular parolanızı örneğin oltalama (phishing) yoluyla alırsa, diğer çevrimiçi hesaplarınıza girmeye çalışırlar. Tüm hesaplar için yalnızca bir parola kullanırsanız, tüm hesaplarınıza girebilir, tüm verilerinizi çalabilir veya silebilir veya kimliğinize bürünebilir. Her hesap için aynı parolayı kullanmanın tehlikesini geçtiğimiz yıllarda Facebook kurucusu Mark Zukerberg yaşadı. 2016 yılında Linkedin veri tabanını ele geçiren siber korsanlar "dadada" gibi basit bir parolayı kullandığını hatta bunu Twitter hesabı için de geçerli parola yaptığını gördüler. Twitter parolasını da ele geçiren korsanlar Mark Zukerberg adına twit'ler attılar.

2018 yılında İngiltere'de yapılan bir araştırmaya göre kullanıcıların en az %50'sinden fazlası birden fazla çevrimiçi hesap için aynı parolayı kullanıyor. Üstelik bu kişilerin büyük çoğunluğunun parolaları sosyal medya hesaplarından kolaylıkla öğrenilebilecek çocuklarının ya da hayvanlarının isimlerinden oluşuyor. Aman sakın siz böyle yapmayın!

Hatırlanması gereken çok fazla parolaya ihtiyaç duyan çok sayıda çevrimiçi hesap kullanıyoruz. Parolaları yeniden veya zayıf parola kullanmaktan kaçınmak için bir çözüm, bir parola yöneticisi kullanmaktır. Bir parola yöneticisi, tüm farklı ve karmaşık parolalarınızı depolar ve şifreler. Yönetici daha sonra çevrimiçi hesaplarınıza otomatik olarak giriş yapmanıza yardımcı olabilir. Parola yöneticisine erişmek ve tüm hesaplarınızı yönetmek için ana parolayı hatırlamanız yeterlidir. Google'da "password manager" şeklinde bir arama yaparak ücretli ücretsiz birçok programa ulaşabilirsiniz.

İyi bir parola seçmek için ipuçları :

- Ahmet, Michael gibi herhangi bir dildeki isimleri kullanmayın.
- Sözlükteki kelimelerin yaygın yanlış yazımlarını kullanmayın.
- Bilgisayar isimlerini veya hesap isimlerini kullanmayın.
- Mümkünse, özel karakterleri kullanın! @ # $% ^ & * ()
- On veya daha fazla karakter içeren bir parola kullanın.

Parolanızı daha güvenli hale getirmek için anlamlı cümlelerden bir parola oluşturabilirsiniz. Örneğin Fatih İstanbul'u 1453'te fethetti cümlesindeki sesli harfleri atarak ve aralarına nokta koyarak güvenlik bir parola oluşturabilirsiniz. Fth.stnbl.1453.fthtt

https://howsecureismypassword.net sitesinde görebileceğiniz üzere bu şekildeki bir parola 117 Kentilyon yılda kırılabilir.

4.4. Verileri Şifreleme

Verileriniz her zaman şifrelenmelidir. Hiçbir sırrınız olmadığını ve saklanacak hiçbir şey olmadığını düşünebilirsiniz, o zaman neden şifreleme kullanıyorsunuz? Belki hiç kimsenin verilerinizi istemediğini düşünürsünüz. Büyük olasılıkla, bu muhtemelen doğru değildir.

Tüm fotoğraflarınızı ve belgelerinizi yabancılara göstermeye hazır mısınız? Bilgisayarınızda depolanan finansal bilgileri arkadaşlarınızla paylaşmaya hazır mısınız? E-postalarınızı ve hesap şifrelerinizi herkese vermek ister misiniz?

Kötü amaçlı bir uygulama bilgisayarınızı veya mobil cihazınızı etkiliyorsa ve hesap numaraları, parolalar ve diğer resmi belgeler gibi potansiyel olarak değerli bilgileri çalıyorsa, bu durum daha da zahmetli olabilir. Bu tür bilgiler kimlik hırsızlığı, dolandırıcılık veya fidye istemeye yol açabilir. Suçlular verilerinizi kolayca şifrelemeye ve fidyeyi ödeyene kadar kullanılamaz hale getirmeye karar verebilir.

Şifreleme nedir? Şifreleme, bilgiyi yetkisiz bir tarafın okuyamayacağı bir forma dönüştürme işlemidir. Gizli anahtar veya şifreye sahip yalnızca güvenilir, yetkili bir kişi verileri şifresini çözebilir ve orijinal biçiminde erişebilir. Şifrelemenin kendisi, birisinin verileri yakalamasını engellemez. Şifreleme, yetkisiz kişilerin yalnızca içeriği görüntülemesine veya bunlara erişmesine engel olabilir.

EFS (Encrypting File System-Şifreleme Dosya Sistemi), verileri şifreleyebilen bir Windows özelliğidir. EFS doğrudan belirli bir kullanıcı hesabıyla bağlantılıdır. Sadece verileri şifreleyen kullanıcı, EFS kullanılarak şifrelenmiş olduktan sonra ona erişebilir. Tüm Windows sürümlerinde verileri EFS kullanarak şifrelemek için şu adımları izleyin:

Bir dosyaya veya klasöre sağ tıklayın (ya da basılı tutun) ve Özellikler›i seçin. Gelişmiş düğmesini ve Verileri korumak için içeriği şifrele onay kutusunu seçin. Tamam›ı seçerek Gelişmiş Öznitelikler penceresini kapatın, Uygula›yı ve ardından Tamam›ı seçin. EFS ile şifrelenmiş dosyalar ve klasörler, yeşil renkte görüntülenir. Fakat bu özellik Windows 10 Home sürümünde kullanılamaz.

4.5. Verileri Yedekleme

Sabit sürücünüz bozulabilir. Dizüstü bilgisayarınız kaybolabilir. Akıllı telefonunuz çalınabilir. Belki de önemli bir belgenin orijinal versiyonunu silebilirsiniz. Yedekleme yapmak, aile fotoğrafları gibi yeri doldurulamaz verilerin kaybını önleyebilir. Verileri düzgün bir şekilde yedeklemek için ek bir depolama alanına ihtiyacınız olacak ve verileri o konuma düzenli ve otomatik olarak kopyalamanız gerecektir.

Yedeklenen dosyalarınızın yeri, ev ağınızda, sabit diskin ikinci bölümünde veya bulutta olabilir. Tüm verilerinizi ağa bağlı bir depolama aygıtına (NAS), basit bir harici sabit sürücüye kopyalamaya veya DVD'ye yedekleme yapabilirsiniz. Bu senaryoda depolama cihazı ekipmanının maliyetinden ve bakımından tamamen siz sorumlusunuz. Bir bulut depolama hizmetine abone olursanız, maliyet, gerekli depolama alanı miktarına bağlıdır. Amazon Web Services (AWS), Google Drive veya Microsoft OneDrive gibi bir bulut depolama hizmetiyle, hesabınıza erişiminiz olduğu sürece yedek verilerinize erişebilirsiniz. Çevrimiçi depolama hizmetlerine abone olduğunuzda, Depolama maliyeti ve sürekli çevrimiçi veri aktarımları nedeniyle yedeklenen

veriler hakkında daha seçici olmanız gerekebilir. Yedeklemenin alternatif bir yerde depolanmasının faydalarından biri de, yangın, hırsızlık veya depolama aygıtı arızası dışındaki diğer felaketler durumunda güvenli olmasıdır. Windows 10 kullanıyorsanız işletim sistemi ile gelen 5GB'lık bir OneDrive alanınız olur. İsterseniz Google Drive kullanarak 15GB'lık bir depolama alanına sahip olabilirsiniz. Google Drive'ı etkin bir şekilde kullanmak için uygulamasını bilgisayarınıza indirip kurmanız gerekir.

4.6. Verileri Güvenli Şekilde Silme

Bir dosyayı geri dönüşüm kutusuna veya çöp kutusuna taşıdığınızda ve kalıcı olarak sildiğinizde, dosyaya yalnızca işletim sisteminden erişilemez. Doğru adli araçlara sahip olan herkes, sabit sürücüde bırakılan manyetik iz nedeniyle dosyayı kurtarabilir.

Verileri daha sonra kurtarılamayacak şekilde silmek için, verilerin üzerine bir kereden fazla olmak üzere veri yazılması gerekir. Silinen dosyaların kurtarılmasını önlemek için, sadece bunu yapmak için özel olarak tasarlanmış araçları kullanmanız gerekebilir. Microsoft sitesinden indirebileceğiniz SDelete (Vista ve üstü için) ile hassas dosyaları tamamen kaldırabilirsiniz.

Veri veya dosyaların kurtarılamayacağından emin olmanın tek yolu, sabit sürücüyü veya depolama aygıtını fiziksel olarak imha etmektir.

4.7. İki Faktörlü Kimlik Doğrulama

Google, Facebook, Twitter, LinkedIn, Apple ve Microsoft gibi popüler çevrimiçi hizmetler, hesap girişleri için ekstra bir güvenlik katmanı eklemek için iki faktörlü kimlik doğrulaması kullanır. Kullanıcı adı ve şifre veya kişisel kimlik numarası (PIN) veya desen dışında, iki faktörlü kimlik doğrulaması, aşağıdaki gibi bir ikinci belirteci gerektirir:

Fiziksel nesne, kredi kartı, ATM kartı, telefon.

Biyometrik tarama, parmak izi, avuç içi baskısı yanı sıra yüz veya ses tanıma.

İki faktörlü kimlik doğrulama ile bile, bilgisayar korsanları, phishing saldırıları, kötü amaçlı yazılımlar ve sosyal mühendislik gibi saldırılar yoluyla çevrimiçi hesaplarınıza erişmeye devam edebilir.

Ziyaret ettiğiniz web sitelerinin iki faktörlü kimlik doğrulaması kullanıp kullanmadığını öğrenmek için bu siteden bilgi alabilirsiniz**: https://twofactorauth.org/**

4.8. Sosyal Medyada Çok Fazla Paylaşmayın

Sosyal medyada gizliliğinizi sağlamak istiyorsanız, mümkün olduğunca az bilgi paylaşın. Doğum tarihiniz, e-posta adresiniz veya telefon numaranız gibi bilgileri profilinizde paylaşmamalısınız. Kişisel bilgilerinizi bilmesi gereken insanlar muhtemelen zaten biliyordur. Sosyal medya profilinizi tamamen doldurmayın, sadece gereken minimum bilgiyi sağlayın. Ayrıca, sosyal medya ayarlarınızı yalnızca tanıdığınız kişilerin etkinliklerinizi görmesine veya görüşmelerinize katılmasına izin vermek için kontrol edin.

Çevrimiçi bir hesap için kullanıcı adı ve şifrenizi hiç unuttunuz mu? "Annenizin kızlık soyadı nedir?" veya "Hangi şehirde doğdunuz?" gibi güvenlik soruları, hesabınızı davetsiz misafirlere karşı güvende tutmanıza yardımcı olacak. Ancak, hesaplarınıza erişmek isteyen herkes, İnternet›teki muhtemel yanıtları arayabilir. Yanlış cevapları hatırlayabildiğiniz sürece bu soruları yanlış bilgi ile cevaplayabilirsiniz. Onları hatırlamakta sorun yaşıyorsanız, bunları yönetmek için parola yöneticisini kullanabilirsiniz.

4.9. E-posta ve Web Tarayıcısı Gizliliği

Her gün, diğer insanlarla iletişim kurmak ve iş yapmak için milyonlarca e-posta mesajı kullanılır. E-posta, insanların birbirleriyle hızlı bir şekilde iletişim kurması için uygun bir yoldur. Bir e-posta göndermek, bir kartpostal kullanarak bir mesaj göndermeye benzer. Kartpostal mesajı, erişimi olan herkesin göremediği bir yerde iletilir ve e-posta mesajı düz metin olarak iletilir ve erişimi olan herkes tarafından okunabilir. Bu iletişim, hedefe giden rotada farklı sunucular arasından geçirilir. E-posta mesajlarınızı sildiğinizde bile, mesajlar bir süre posta sunucularında arşivlenebilir.

Bilgisayarınıza veya yönlendiricinize fiziksel erişimi olan herkes, web tarayıcı geçmişi, önbellek ve muhtemelen günlük dosyaları kullanarak ziyaret ettiğiniz web sitelerini görüntüleyebilir. Bu sorun, web tarayıcısında özel tarama modunu etkinleştirerek en aza indirgenebilir. Popüler web tarayıcılarının çoğunun özel tarayıcı modu için kendi adı vardır:

Microsoft Edge : InPrivate
Google Chrome : Gizli pencere
Mozilla Firefox : Gizli pencere
Opera: Gizli pencere

Özel mod etkinken, çerezler devre dışı bırakılır ve pencere veya program kapatıldıktan sonra geçici İnternet dosyaları ve tarama geçmişi kaldırılır.

İnternet tarama geçmişinizi gizli tutmak, başkalarının çevrimiçi etkinlikleriniz hakkında bilgi toplamasını ve sizi hedefli reklamlar ile bir şeyler satın almanızı teşvik etmesini engelleyebilir. Özel göz atma özelliğine ve çerezlerin devre dışı bırakılmasına rağmen, şirketler bilgi toplamak ve kullanıcı davranışlarını izlemek için farklı yollar geliştirmektedir. Örneğin, yönlendiriciler gibi aracı cihazlar, kullanıcının İnternet sörfü geçmişi hakkında bilgi sahibi olabilir.

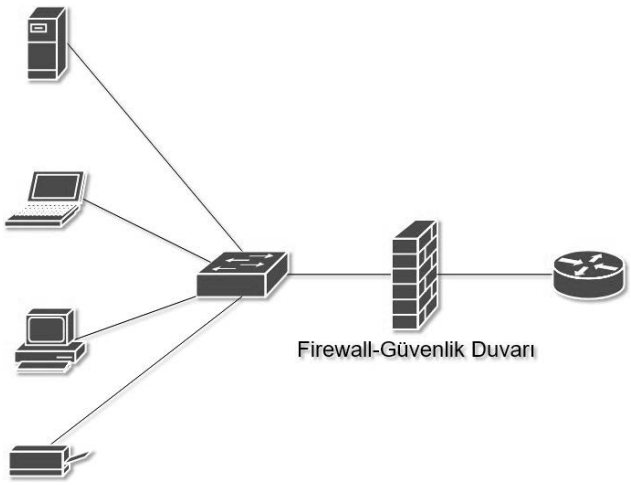
5

5. Güvenlik Duvarları

Bu bölüm, bir kurumun ağını, ekipmanını ve verilerini korurken siber güvenlik uzmanları tarafından kullanılan bazı teknoloji ve süreçleri anlatmaktadır. İlk olarak, en iyi uygulamalar dahil olmak üzere şu anda kullanılan birçok güvenlik duvarı, güvenlik cihazı ve yazılım türünü göreceğiz. Daha sonra, botnet'leri, davranış tabanlı güvenliği ve bir ağı izlemek için NetFlow'un nasıl kullanıldığını inceleyeceğiz.

5.1. Güvenlik Duvarı Türleri

Bir ateş (güvenlik) duvarı (firewall), yangının bir binanın bir kısmından diğerine yayılmasını önlemek için tasarlanmış bir duvar veya bölümdür. Bilgisayar ağında ise bir güvenlik duvarı, şekilde görüldüğü gibi, bir cihaza veya ağa izin verilen trafiği geçiren, izin verilmeyen trafiği engelleyen bir ağ cihazıdır.



Bir güvenlik duvarı, bir bilgisayarı (ana bilgisayar tabanlı güvenlik duvarı) korumak amacıyla tek bir bilgisayara kurulabilir. Bunlara en güzel örnek Windows ile tümleşik gelen güvenlik duvarı özelliğidir veya tüm ağ bilgisayarlarını ve bu ağdaki tüm ana bilgisayar aygıtlarını koruyan bağımsız bir ağ aygıtı olabilir. (Ağ tabanlı güvenlik duvarı).

Bilgisayar ve ağ saldırıları daha karmaşık hale geldikçe, bir ağın korunmasında farklı amaçlara hizmet eden yeni güvenlik duvarı türleri geliştirildi. Ortak güvenlik duvarı türlerinin listesi aşağıdadır:

Ağ Katmanı Güvenlik Duvarı: Kaynak ve hedef IP adreslerine göre filtrelemesi.

Aktarım Katmanı Güvenlik Duvarı: Kaynak ve hedef veri bağlantı noktalarına (port) göre filtreleme.

Uygulama Katmanı Güvenlik Duvarı: Uygulama, program veya servis bazında filtreleme.

Bağlam Bilinçli Uygulama Güvenlik Duvarı: Kullanıcı, cihaz, rol, uygulama türü ve tehdit profiline göre filtreleme.

Proxy Server: URL, alan adı, medya vb. gibi web içeriği isteklerinin filtrelenmesi.

Ters Proxy Sunucusu: Web sunucularının önüne yerleştirilir, ters proxy sunucuları web sunucularına erişimi korur ve gizler.

Ağ Adresi Çevirisi (NAT) Güvenlik Duvarı: Ağ ana bilgisayarlarının özel adreslerini gizler.

Ana Bilgisayar Tabanlı Güvenlik Duvarı: Bağlantı noktalarının filtrelenmesi ve sistem hizmeti tek bir bilgisayar işletim sisteminde çalışır. Örnek: Windows güvenlik duvarı.

5.2. Port Taraması

Port-tarama; bir bilgisayar, sunucu veya ağ cihazlarındaki açık portları sorgulama işlemidir. Ağda, bir cihazda çalışan her bir uygulamaya port numarası olarak adlandırılan bir tanımlayıcı atanır. Bu port numarası, iletimin her iki ucunda kullanılır, böylece doğru veriler doğru uygulamaya iletilir. Port tarama, bir bilgisayar veya ana bilgisayarda çalışan işletim sistemini ve hizmetleri tanımlamak için bir keşif aracı olarak kötü amaçlı olarak kullanılabilir veya ağdaki ağ güvenlik ilkelerini doğrulamak için ağ yöneticisi tarafından zararsız olarak kullanılabilir.

Kendi bilgisayar ağınızın güvenlik duvarını ve bağlantı noktası güvenliğini değerlendirmek amacıyla, ağınızdaki tüm açık bağlantı noktalarını bulmak için Nmap gibi bir bağlantı noktası tarama aracı kullanabilirsiniz. Port-tarama, bir ağ saldırısının habercisi olarak görülebilir ve bu nedenle İnternet üzerindeki halka açık sunucularda veya izinsiz bir şirket ağında yapılmamalıdır.

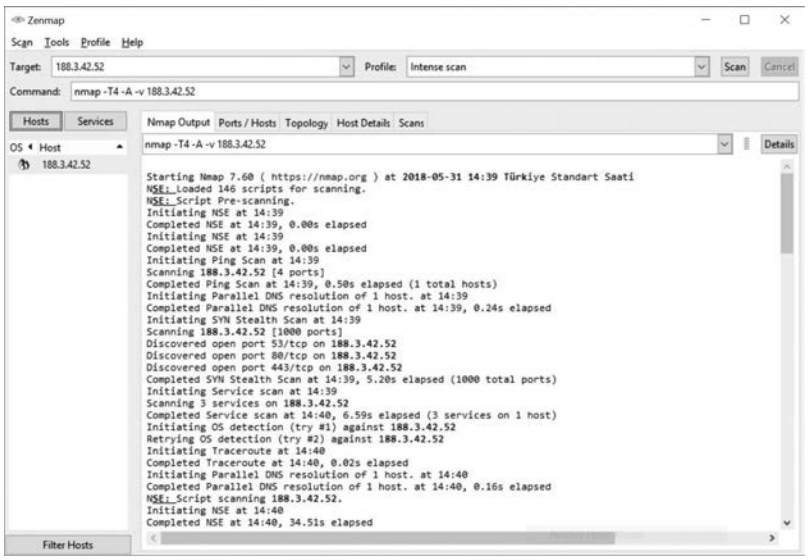
Yerel ev ağınızdaki bir bilgisayarda bir Nmap port taraması yapmak için, Zenmap gibi bir programı indirin (https://nmap.org) ve başlatın, taramak istediğiniz bilgisayarın hedef IP adresini girin, bir varsayılan tarama profili seçin ve taramayı başlatın. Nmap taraması, çalışan tüm hizmetleri (Web servisleri, posta hizmetleri vb.) ve bağlantı noktası numaralarını bildirecektir. Bir portun taranması genellikle üç yanıttan biriyle sonuçlanır:

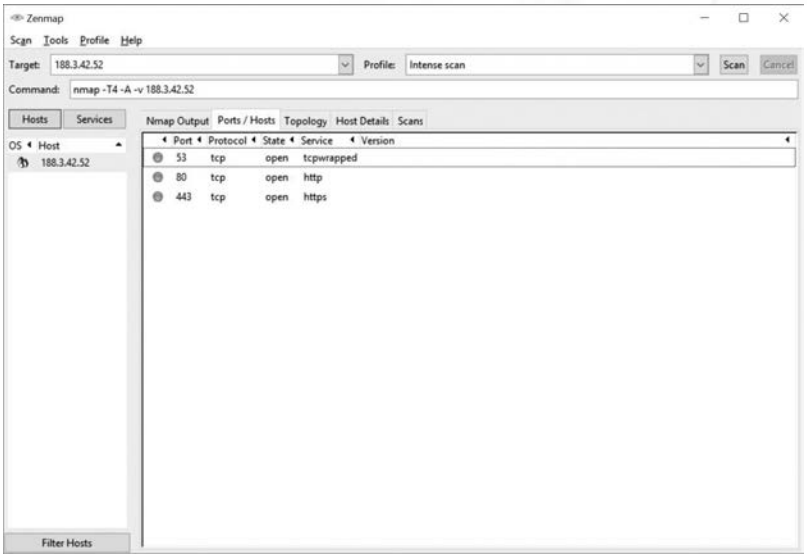
Açık veya Kabul (Open or Accepted): Bir servisin bağlantı noktasını dinlediğini belirten ana makine yanıtı.

Kapalı, Reddedildi veya Dinlenmiyor (Closed, Denied, or Not Listening): Ana bilgisayar bağlantıların reddedileceğini belirterek yanıt verdi.

Filtrelenmiş, Düştü veya Engellendi (Filtered, Dropped, or Blocked): Sunucudan yanıt gelmedi.

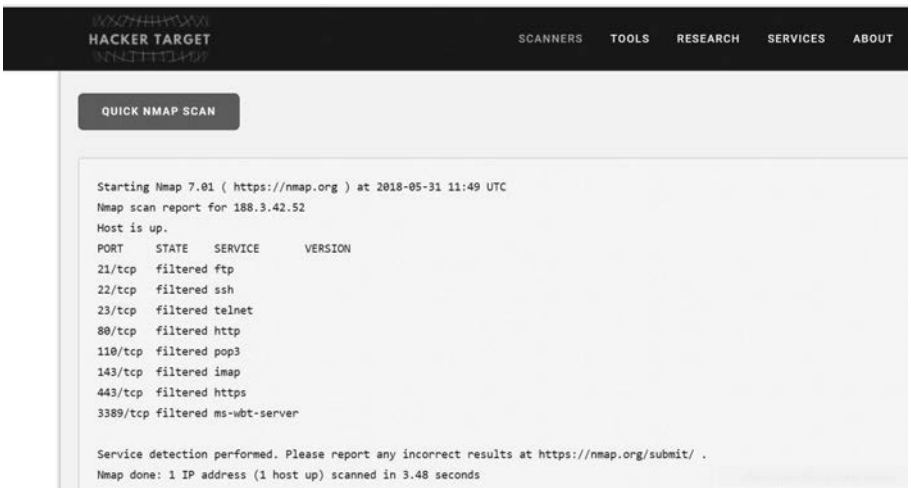
Ağınızın dışından bir port taraması yapmak için, taramayı ağın dışından başlatmanız gerekir. Bu, güvenlik duvarınıza veya yönlendiricinizin genel IP adresine karşı bir Nmap port taraması yapılması anlamına gelir. Genel IP adresinizi bulmak için Google gibi bir arama motorunu "ip adresim nedir?" sorgusuyla kullanın. Arama motoru genel IP adresinizi gösterecektir. Aşağıdaki şekilde Zenmap ile ADSL modemimin IP adresine yaptığım taramanın sonuçları görülmektedir.





Yukarıdaki şekilde görebileceğiniz üzere 53, 80 ve 443 numaralı portlar açık durumda.

Ana yönlendiricinize veya güvenlik duvarınıza karşı ortak kullanılan portları içeren bir bağlantı noktası taraması yapmak için, https://hackertarget.com/nmap-online-port-scanner/ adresindeki Nmap Çevrimiçi Bağlantı Noktası Tarayıcısına gidin ve genel IP adresinizi girin ve Quick Nmap Scan - Hızlı Nmap Taraması'na basın. 21, 22, 25, 80, 443 veya 3389 bağlantı noktalarından herhangi biri açıksa bunu görebilirsiniz. Fakat büyük olasılıkla, yönlendirici veya güvenlik duvarınızda bağlantı noktası yönlendirmesi etkinleştirildi ve portlar filtrelenmemiş olarak karşımıza geldi. Aşağıdaki şekilde tarama sonucunu görebilirsiniz.



5.3. Güvenlik Cihazları

Bugün, tüm ağ güvenliği ihtiyaçlarını çözecek tek bir güvenlik cihazı veya teknoloji yoktur. Uygulanması gereken çeşitli güvenlik aletleri ve araçları olduğundan, hepsinin birlikte çalışması önemlidir. Güvenlik cihazları, bir sistemin parçası olduklarında çok etkilidir.

Güvenlik aygıtları, bir yönlendirici veya güvenlik duvarı, ağ aygıtına takılabilen bir kart veya kendi işlemcisine ve önbelleğe alınmış belleğe sahip bir modül gibi bağımsız aygıtlar olabilir. Güvenlik cihazları ayrıca bir ağ cihazında çalışan yazılım araçları da olabilir. Güvenlik cihazları şu genel kategorilere ayrılırlar:

Yönlendiriciler: Birçok markanın ürettiği orta seviye yönlendiricilerde, trafik filtreleme, güvenli şifrelenmiş tünelleme, bir İzinsiz Girişi Önleme Sistemi (IPS), ve VPN gibi özellikleri bulabilirsiniz.

Güvenlik Duvarları: Her ne kadar yukarıda bahsettiğimiz gibi bazı yönlendiriciler ile güvenlik çözümleri sunulsa da sadece bu iş için üretilmiş güvenlik duvarı çözümleri bulunmaktadır.

Kötü Amaçlı Yazılımlar / Virüsten Koruma: Ağınıza gelen giden trafik içinde zararlı yazılım bulunup bulunmadığını kontrol eden ve bulunduğunda temizleyen güvenlik çözümleri ayrıca büyük şirket ağlarında karşımıza çıkmaktadır.

Web Uygulama Güvenlik Duvarı: Web sunucularına gelen trafiği ayrıntılı olarak inceleyen ve denetleyen güvenlik cihazlarıdır.

5.4. Tümleşik Güvenlik Sistemleri UTM'ler

Günümüzde ağ tehditlerinin çeşitlerinin artmasıyla beraber güvenlik duvarları da yenilikçi yaklaşımlarla UTM denen (Unified Threat Management) Tümleşik Güvenlik Sistemleri olarak karşımıza çıkmaya başlamıştır.

UTM'lerle birlikte sadece giden gelen trafiği denetlemenin dışında yerleşik anivirüs, IPS (Saldırı Engelleme Sistemi), Web filtreleme, uygulama filtreleme, hotspot, vpn, 5651 loglama gibi birçok çözüm tek bir kutuda sunulmaya başlanmıştır.

Böylece birçok çözüm için tek bir kutu alarak hem maliyetler düşürüldü hem de yönetim ve yapılandırma merkezi hale geldi ve kolaylaştı.

Bir UTM ile Neler Yapabilirsiniz?

Öncelikle bir UTM'nin temel görevlerinden biri firewall olarak çalışmasıdır. Bu sayede gelen ve giden ağ trafiğini denetleyerek istenmeyen durumları engelleyebilirsiniz. IPS (Intrusion Prevention System) yani saldırı önleme sistemi olarak çalışır ve engeller. Web filtreleme yaparak İnternet bağlantınızı verimli kullanma adına belirli kısıtlamalar getirebilir. Örneğin mesai saatleri içinde Youtube ve Facebook gibi siteler yasaklanabilir ama öğlen arasında serbest olur. VPN ile uzaktan şirket ağına bağlanan kullanıcıların güvenli bir şekilde erişimi sağlanır. Antivirüs özelliği ile zararlı yazılımların şirket ağına girmesini engeller. Uygulama filtresi ile örneğin çalışanların cep telefonlarından şirket kablosuz ağına bağlanarak Whatsapp kullanması engellenebilir. En önemlisi de bugün birçok AVM'de bulunan kafe ve restoranlarda wi-fi şifresi paylaşılmaktadır. Bunun getirdiği tehlike ise müşterinin İnternet ortamında işlenen bir suça karıştığında kimliğinin tespit edilememesini ve sonuçta sorumluluğun işletme sahibine yüklenmesidir. Birçok UTM'deki Hotspot ve 5651 loglama ile bu sorunun önüne geçilebilir.

5.5. Gerçek Zamanda Saldırıların Tespiti

Yazılımlar hiçbir zaman mükemmel değildir. Bir bilgisayar korsanı, üretici bunu düzeltmeden önce bir yazılım parçasında bir kusurdan yararlanırsa, sıfır gün saldırısı olarak bilinir. Günümüzde sıfır gün saldırılarının karmaşıklığı ve büyüklüğü nedeniyle, ağ saldırılarının başarılı olacağı ve bir ağın bir saldırıya ne kadar hızlı yanıt verebileceği konusunda başarılı bir savunma yapıldığı giderek yaygınlaşmaktadır. Saldırıları gerçek zamanlı olarak algılayabilme, saldırıları derhal durdurma veya birkaç dakika içinde gerçekleştirme yeteneği ideal hedeftir. Ne yazık ki, günümüzde birçok şirket ve kuruluş, saldırıların meydana gelmesinden günler hatta aylar sonra tespit edebilmektedir.

Uçtan Uç Noktaya Gerçek Zamanlı Tarama: Gerçek zamanlı saldırıların algılanabilmesi, güvenlik duvarı ve IDS / IPS ağ cihazlarını kullanarak saldırıları etkin bir şekilde tespit etmenizi gerektirir. Çevrimiçi küresel tehdit merkezlerine bağlantı ile yeni nesil istemci / sunucu kötü amaçlı yazılım tespiti de kullanılmalıdır. Günümüzde, etkin tarama aygıtları ve yazılımları, içerik tabanlı analiz ve davranış algılama kullanarak ağ anormalliklerini tespit etmelidir.

DDoS Saldırıları ve Gerçek Zamanlı Yanıt: DDoS, gerçek zamanlı yanıt ve algılama gerektiren en büyük saldırı tehditlerinden biridir. DDoS saldırılarına karşı savunmak son derece zordur çünkü saldırılar yüzlerce veya binlerce zombi bilgisayardan kaynaklanır. Birçok şirket ve kuruluş için düzenli olarak DDoS saldırıları İnternet sunucularını ve ağ kullanılabilirliğini engeller. DDoS saldırılarını gerçek zamanlı olarak algılama ve yanıtlama yeteneği çok önemlidir

5.6. Güvenlik için En İyi Uygulamalar

Birçok güvenlik kuruluşu, en iyi güvenlik uygulamaları listesini yayınlamıştır. Bazı en iyi uygulamaların listesi aşağıdadır:

Risk Değerlendirmesi Yapın: Koruduğunuz şeyin değerini bilmek, güvenlik harcamalarını haklı çıkarmaya yardımcı olur. Yani güvenlik duvarı için yapılacak bir harcama israf olarak görülmez.

Bir Güvenlik Politikası Oluşturun: Şirket kurallarını, iş sorumluluklarını ve beklentileri açıkça belirten bir politika oluşturun ve tüm kullanıcılara bildirin.

Fiziksel Güvenlik Önlemleri: Ağ bağlantılarına, sunucu konumlarına ve yangın söndürme sistemlerine erişimi kısıtlayın.

İnsan Kaynakları Güvenlik Önlemleri: Çalışanlar, arka plan kontrolleri ile uygun şekilde araştırılmalıdır.

Yedeklemeleri Gerçekleştirin ve Test Edin: Düzenli yedeklemeler yapın ve yedeklemelerden veri kurtarma işlemini test edin.

Güvenlik Yamalarını ve Güncellemelerini Koruyun: Sunucu, istemci ve ağ aygıtı işletim sistemlerini ve programlarını düzenli olarak güncelleyin.

Erişim Denetimleri Kullanın: Kullanıcı rollerini ve ayrıcalık düzeylerini ve güçlü kullanıcı kimlik doğrulamasını yapılandırın.

Olay Yanıtını Düzenli Olarak Test Etme: Bir olay müdahale ekibi oluşturun ve acil durum müdahale senaryolarını test edin.

Bir Ağ İzleme, Analitik ve Yönetim Aracı Uygulayın: Diğer teknolojilerle bütünleşen bir güvenlik izleme çözümü seçin.

Ağ Güvenlik Cihazlarını Uygulayın: Yeni nesil yönlendiriciler, güvenlik duvarları ve diğer güvenlik cihazlarını kullanın.

Kapsamlı bir Endpoint Güvenlik Çözümü Uygulayın: Kurumsal düzeyde antimalware ve antivirüs yazılımı kullanın.

Kullanıcıları Eğitmek: Kullanıcıları ve çalışanları güvenlik konularında eğitin.

Verileri şifreleyin: E-posta dahil olmak üzere tüm hassas şirket verilerini şifreleyin.

5.7. Botnet

Bir botnet, İnternet'e bağlı, kötü niyetli bir birey veya grup tarafından kontrol edilebilen bir grup bottur. Bir bot bilgisayarı genellikle bir web sitesini ziyaret ederek, bir e-posta eki açarak veya virüslü bir medya dosyasını açarak bulaşır ve botnet'e dahil olur.

Bir botnet, on binlerce hatta yüzbinlerce bot içerebilir. Bu botlar, kötü amaçlı yazılım dağıtmak, DDoS saldırılarını başlatmak, istenmeyen e-postaları dağıtmak veya kaba kuvvet şifre saldırıları gerçekleştirmek için etkinleştirilebilir. Botnet'ler tipik olarak bir komut ve kontrol sunucusu aracılığıyla kontrol edilir.

Siber suçlular genellikle bir ücret karşılığında, üçüncü taraflara kötü amaçlar için Botnet'leri kiralayabilir.

5.8. Bir Siber Saldırının Aşamaları

Siber güvenlikte, Kill Zinciri bir bilgi sistemleri saldırısının aşamalarıdır. Lockheed Martin tarafından olay tespiti ve müdahale için bir güvenlik çerçevesi olarak geliştirilen Cyber Kill Chain, aşağıdaki aşamalardan oluşur:

Aşama 1.
Keşif : Saldırgan hedef hakkında bilgi toplar.

Aşama 2.
Silahlanma : Saldırgan, hedefe göndermek için istismar ve kötü amaçlı bir yazılım oluşturur.

Aşama 3.
Teslimat: Saldırgan, e-posta veya başka bir yöntemle hedefe istismar ve kötü amaçlı yazılım yükler.

Aşama 4.
Sömürü: Zararlı yazılım çalıştırılır ve zafiyetler istismar edilir.

Aşama 5:
Kurulum: Malware ve arka kapılar hedefe kurulur.

Aşama 6.
Komut ve Kontrol: Hedefin uzaktan kontrolü, bir komut ve kontrol kanalı veya sunucusu aracılığıyla kazanılır.

Aşama 7.
Eylem: Saldırgan, bilgi hırsızlığı gibi kötü amaçlı eylemler gerçekleştirir veya Öldürme Zinciri aşamalarında tekrar çalışarak ağ içindeki diğer aygıtlara ek saldırılar gerçekleştirir.

Öldürme Zincirine karşı savunmak için, ağ güvenliği savunmaları Kill Zincirinin aşamaları etrafında tasarlanmıştır. Bunlar Siber Öldürme Zincirine dayanan bir şirketin güvenlik savunmasıyla ilgili bazı sorulardır:

- Kill Zincirinin her aşamasında atak göstergeleri nelerdir?
- Aşamaların her birinde saldırı göstergelerini tespit etmek için hangi güvenlik araçlarına ihtiyaç vardır?
- Şirketin saldırı tespit etme yeteneğinde boşluklar var mı?

Lockheed Martin'e göre, Kill Chain'in aşamalarını anlamak saldırıyı yavaşlatmasına veya engellemesine ve sonuçta veri kaybını önlemesine neden olur.

5.9. Davranış Tabanlı Güvenlik

Davranış tabanlı güvenlik, bilinen kötü amaçlı imzalara güvenmeyen bir tehdit algılama şeklidir, bunun yerine ağdaki anormallikleri algılamak için bilgi içeriği kullanır. Davranış tabanlı algılama, yerel ağdaki bir kullanıcı ile yerel veya uzak bir hedef arasındaki iletişim akışının yakalanmasını ve analiz edilmesini içerir. Bu iletişim, ele geçirildiğinde ve analiz edildiğinde, anormallikleri tespit etmek için kullanılabilecek bağlam ve davranış kalıplarını ortaya çıkarır. Davranış tabanlı algılama, normal davranışın değişmesiyle bir saldırının varlığını keşfedebilir.

Honeypots – Honeypot (bal küpü), saldırganın tahmin edilen kötü niyetli davranış modeline hitap ederek ilk önce davranışı tetikleyen davranış tabanlı bir tespit aracıdır ve bal küpü içinde olduğunda, ağ yöneticisi saldırganın davranışını yakalayabilir, günlüğe kaydedebilir ve analiz edebilir. Bu, bir yöneticinin daha fazla bilgi kazanmasına ve daha iyi bir savunma yapmasına olanak tanır.

NetFlow, verilerin ağ üzerinden nasıl taşındığı ile ilgili birçok farklı özellikten yararlanarak bilgi toplayabilir. Ağ veri akışları hakkında bilgi toplayarak NetFlow, 90'dan fazla farklı öznitelikte temel davranış oluşturabilir.

5.10. CSIRT (SOME)

Birçok büyük kuruluşun, bilgisayar güvenliği olay raporlarını almak, incelemek ve yanıtlamak için bir Bilgisayar Güvenliği Olayı Yanıt Ekibi- Siber Olaylara Müdahale Ekibi (CSIRT) vardır. CSIRT'in birincil misyonu, şirket, sistem ve veri korumasının gerçekleştirilmesini sağlamaya yardımcı olmaktır. Bilgisayar güvenliği olaylarına dair kapsamlı araştırmalar, güvenlik olaylarını önlemek için proaktif tehdit değerlendirmesi, tehdit azaltma planlaması, olay trend analizi ve güvenlik mimarisi incelemesi sağlar.

Ülkemizde de BTK'ya bağlı olarak çalışan Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) 2014 yılında kurulmuştur. https://www.usom.gov.tr adresinden ayrıntılı bilgi alabilirsiniz.

5.11. Güvenlik için Dikkat Edilecekler

Teknoloji sürekli değişiyor. Bu siber saldırıların da geliştiği anlamına geliyor. Yeni güvenlik açıkları ve saldırı yöntemleri sürekli olarak keşfedilmektedir. Güvenlik, ortaya çıkan itibar ve güvenlik ihlallerinden kaynaklanan mali etkiler nedeniyle önemli bir ticari sorun haline geliyor. Saldırılar kritik ağları ve hassas verileri hedefliyor. Organizasyonların bir ihlale hazırlık, anlama ve telafi etme planları olmalıdır.

Güvenlik ihlali için hazırlanmanın en iyi yollarından biri hazırlık ve planlamadır. Sistemler, varlıklar, veriler ve yeteneklere karşı siber güvenlik riskini tanımlamak, sistemi koruma ve personel eğitimi ile korumak ve siber güvenlik olayını mümkün olan en kısa sürede tespit etmek için rehberlik sağlanmalıdır. Bir güvenlik ihlali tespit edildiğinde, etkisini ve hasarını en aza indirmek için uygun önlemler alınmalıdır. İhlal planı, ihlal sırasında çoklu eylem seçenekleriyle esnek olmalıdır. İhlaller sonrasında tehlikeye atılan sistemler ve hizmetler geri yüklendikten sonra, güvenlik önlemleri ve süreçleri, ihlal sırasında öğrenilen dersleri içerecek şekilde güncellenmelidir.

Bütün bu bilgiler bir güvenlik izleme kitabına derlenmelidir. Güvenlik izleme kitabı, olay tespitine ve yanıtlamasına neden olan güvenlik olay veri kaynaklarına karşı tekrarlanabilir sorguların (raporların) bir araya getirilmesidir. İdeal olarak güvenlik oyun kitabı aşağıdaki eylemleri gerçekleştirmelidir:

- Kötü amaçlı yazılım bulaşmış makineleri tespit edin.
- Şüpheli ağ etkinliğini algıla.
- Düzensiz kimlik doğrulama girişimlerini tespit edin.
- Gelen ve giden trafiği tanımlayın ve anlayın.

- Trendler, istatistikler ve sayımlar dahil özet bilgiler sağlayın.
- İstatistiklere ve metriklere kullanılabilir ve hızlı erişim sağlayın.
- İlgili tüm veri kaynaklarındaki etkinlikleri ilişkilendirin.

5.12. Olay Önleme Araçları

Bunlar, güvenlik olaylarını tespit etmek ve önlemek için kullanılan araçlardan bazılarıdır:

SIEM: Güvenlik Bilgisi ve Olay Yönetimi Sistemi, güvenlik uyarılarını, günlüklerini ve diğer gerçek zamanlı verileri ağdaki güvenlik aygıtlarından toplayan ve analiz eden bir yazılımdır.

DLP: Veri Kaybını Önleme Yazılımı, hassas verilerin bir ağdan çalınmasını veya bir ağdan kaçmasını önlemek için tasarlanmış bir yazılım veya donanım sistemidir. Bir DLP sistemi dosya erişim yetkilendirmesine, veri alışverişine, veri kopyalama, kullanıcı etkinliği izleme ve daha fazlasına odaklanabilir. DLP sistemleri, verileri üç farklı durumda izleyecek ve koruyacak şekilde tasarlanmıştır: Veri kullanımı, veri hareketsizliği ve hareket halindeki veriler. Kullanımdaki veriler, istemciye odaklanır, veri içinde hareket, veriyi ağ üzerinden geçerken ifade eder ve geri kalan veriler, veri deposuna başvurur.

5.13. IDS/IPS

Saldırı Tespit Sistemi (IDS), ya özel bir ağ aygıtıdır ya da bir sunucu ya da güvenlik duvarındaki verileri, kurallar ya da saldırı imzaları veritabanına karşı tarar ve kötü amaçlı trafik arar. Bir eşleşme algılanırsa, IDS algılamayı günlüğe kaydeder ve bir ağ yöneticisi için bir uyarı oluşturur. Saldırı Tespit Sistemi, bir eşleşme tespit edildiğinde harekete geçmez, böylece saldırıların gerçekleşmesini engellemez. IDS'nin işi sadece tespit, kayıt ve rapor etmektir.

IDS tarafından gerçekleştirilen tarama, ağı yavaşlatır. Ağ gecikmesine karşı korunmak için, normal ağ trafiğinden ayrı olarak bir IDS genellikle çevrimdışı olarak yerleştirilir. Veriler bir anahtar tarafından kopyalanır veya yansıtılır ve daha sonra çevrimdışı algılama için IDS'ye iletilir. Linux veya Windows gibi bir ana bilgisayar işletim sisteminin üstüne kurulabilen IDS araçları da vardır.

Bir İzinsiz Giriş Önleme Sistemi (IPS), pozitif kural veya imza eşleşmesine dayalı olarak trafiği engelleme yeteneğine sahiptir. En iyi bilinen IPS / IDS sistemlerinden biri Snort'tur. Snort'un ticari versiyonu gerçek zamanlı trafik ve port analizi, kayıt,

içerik arama ve eşleme gerçekleştirme yeteneğine sahiptir ve prob'ları, saldırıları ve port taramalarını algılayabilir. Raporlama, performans ve günlük analizi için diğer üçüncü taraf araçlarla da entegre edilebilir.

6

6. Berqnet ile Siber Güvenlik

6.1. Berqnet'i Tanıyalım

Berqnet, alanında uzman AR-GE kadrosu tarafından her ölçekteki işletmenin siber güvenlik ihtiyaçlarına yönelik çözüm üretme amacıyla 2013 yılında çalışmalarına başlamış ve tamamen Türkiye'de geliştirilmiş, dünyanın en kolay kurulabilen ve yönetilen firewall cihazıdır.

Türkiye'nin en büyük ve yerli Teknoloji firmalarından Logo Yazılım'ın (BIST: LOGO) 35 yıllık bilgi ve tecrübelerini arkasına alarak yoluna devam eden ve Logo Yazılım'ın da içinde bulunduğu Logo Teknoloji ve Yatırım A.Ş.'nin bir parçası olan Berqnet Firewall (Logo Siber Güvenlik ve Ağ Teknoloji A.Ş'nin tescilli markasıdır), geliştirdiği ve satışa sunduğu tüm ürünlerde global kalitedeki ar-ge metotları ve iş süreçleri kullanılarak geliştirilmiş ve bu vizyonla AR-GE çalışmalarına devam etmektedir. Geliştirilen her Berqnet ürünü, satışa sunulmadan derinlemesine test süreçleriyle sınanmakta ve yüksek performans yakalanana kadar bu süreçler devam ettirilmektedir. Bu hassas süreçlere özellikle dikkat edilerek geliştirilen Berqnet Firewall; Türk Elektronik Sanayicileri Derneği (TESİD) tarafından KOBİ Dalında Yenilikçi Ürün Ödülünü kazanmış ve aynı zamanda BTVizyon tarafından da yılın en iyi yerli güvenlik yazılımı unvanıyla ödüllendirilerek bu alandaki iddiasını ve kalitesini kanıtlamıştır.

Berqnet, bağımsız güvenlik analizi firmaları tarafından yapılan internet üzerinden tarama, whitebox, graybox, blackbox derin tarama yöntemleri ile test edilmiş ve tüm

güvenlik analizlerinden başarıyla geçerek güvenlik alanında doğru bir tercih olduğunu tescillemiştir.

Peki Neden Berqnet?

Berqnet ürün ailesi, Türkiye'deki işletmelerin siber güvenlik ihtiyaçlarını başta veri ve sistem güvenliğinin, yüksek performans ve en doğru çözümlerle karşılamak için geliştirilmesine rağmen her ölçekteki işletmeye benzersiz özellikleri de tek kutuda sunmak için geliştirilmiştir. Ülkemizin cari açığının azaltılmasına katkıda bulunmak ve döviz kaybının önüne geçmek için tamamen milli bir duruşla tüm fiyatlandırma süreçlerini Türk Lirası fiyatları üzerinden satış ve Türk Lirası üzerinden yenileme politikasıyla oluşturan Berqnet, ülkemizde geçerliliği olan tüm aktif yerel yasalara da tamamen uyumlu bir şekilde geliştirilmiştir. Berqnet cihazlarıyla 5651 sayılı yasanın istediği kayıtları tutabilir ve saklayabilir, işletmenizdeki web filtreleme süreçlerini başarıyla yönetebilir yani işletme verimliliğinizi gözle görülür bir şekilde artırabilir; çalışanlarınız ya da şubeleriniz arasında VPN kurulumları yapabilir ve tüm bunlar için ekstra bir ücret ödemezsiniz.

Berqnet, tek kutuda tümleşik bir çözüm sunmak için tasarlanmış, bu alanda dünyanın en kolay kurulabilen ve yönetilebilen firewall'u olma iddiasıyla çalışmalarına devam etmektedir. Berqnet Firewall cihazlarını dakikalar içinde kurabilir ve ileri seviye uzmanlık gerektirmeden, kullanıcı dostu arayüzü ve benzersiz kullanım özellikleri sayesinde rahatlıkla yönetebilirsiniz.

Yukarıda sayılan benzersiz özellikleriyle rakiplerinden sıyrılan Berqnet'in hizmet verdiği alanda bir benzeri daha bulunmamaktadır.

Berqnet'i kimler kullanabilir?

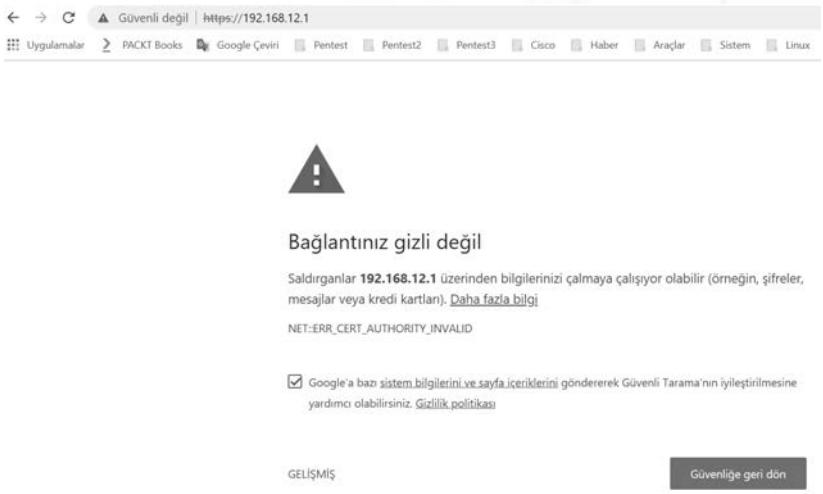
Tüm işletmelerin siber güvenlik ihtiyaçlarına benzersiz bir çözüm üretebilmek için tasarlanan Berqnet Firewall cihazlarını; restoran ve kafelerden öğrenci yurtlarına, otellerden belediye kurumlarına, üretim tesislerinden enerji santrallerine, devlet kurumlarından özel işletmelere, küçük bir avukatlık bürosundan orta boyutlu bir müşavirlik firmasına kadar büyüyen, büyümek isteyen ve iş süreçleri içinde internet bulunan herkes rahatlıkla kullanabilir.

6.2. Berqnet İlk Kurulum

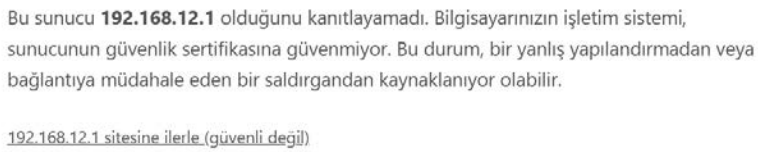
Berqnet'i kutusundan çıkarıp bir yere konumlandırdıktan sonra aşağıdaki şekilde gördüğünüz gibi güç ve ağ bağlantılarını gerçekleştiriniz. (Kitap boyunca Berqnet bq25 modeli kullanılmıştır.)

Diğer modellerde port isimlendirmeleri farklı olabilir fakat ilk portu (igb 0 veya em 0) modemin LAN portuna, ikinci portu (igb 1 veya em 1) anahtara (switch) bağlamanız gerekiyor. Örnek bir topolojiyi aşağıda görebilirsiniz.

Sonrasında switch'e bağlı bir bilgisayarda Chrome veya benzeri bir tarayıcıyı açıp adres satırına https://192.168.12.1 yazıp enter tuşuna basıyoruz. (https mutlaka yazılmalıdır.)



Yukarıdaki şekilde gördüğünüz üzere bağlantınız gizli değil uyarısı alırsınız. Sol altta bulunan Gelişmiş linkine tıklayın ve ardından 192.168.12.1 sitesine ilerle (güvenli değil) linkine tıklayın.

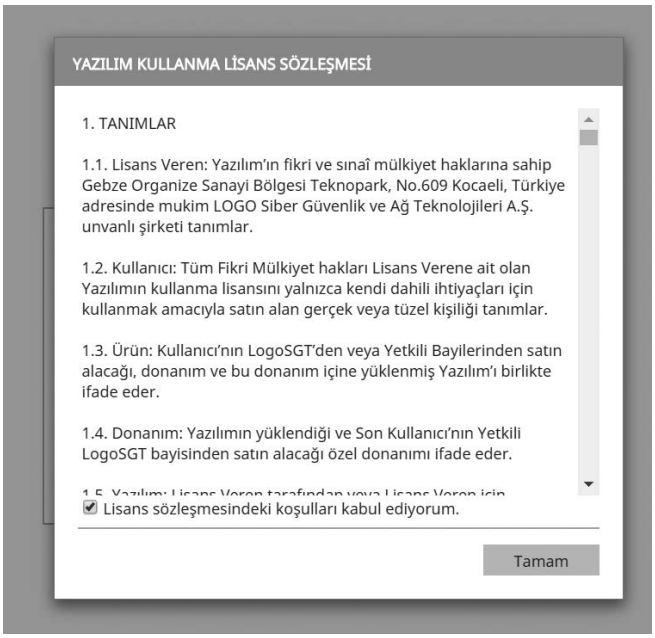


Artık Berqnet giriş sayfası karşınızda. Giriş yapabilmek için;

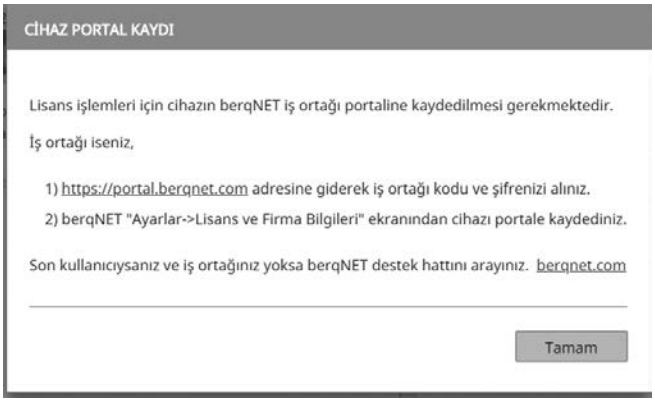
Kullanıcı adı : **berqNET**

Şifre: **berqNET** yazın ve Giriş düğmesine tıklayın.

Sonrasında sizi bir lisans sözleşmesi penceresi karşılayacak. Burada Lisans sözleşmesindeki koşulları kabul ediyorum seçeneğine onay koyup Tamam düğmesine tıklayın.



Şimdi de cihazınızın Berqnet portalına kaydedilmesinin gerekli olduğunu söyleyen bir uyarı penceresi karşınıza geldi. Buna da Tamam deyip geçin, ileride portal kayıt işlemlerini göreceğiz.

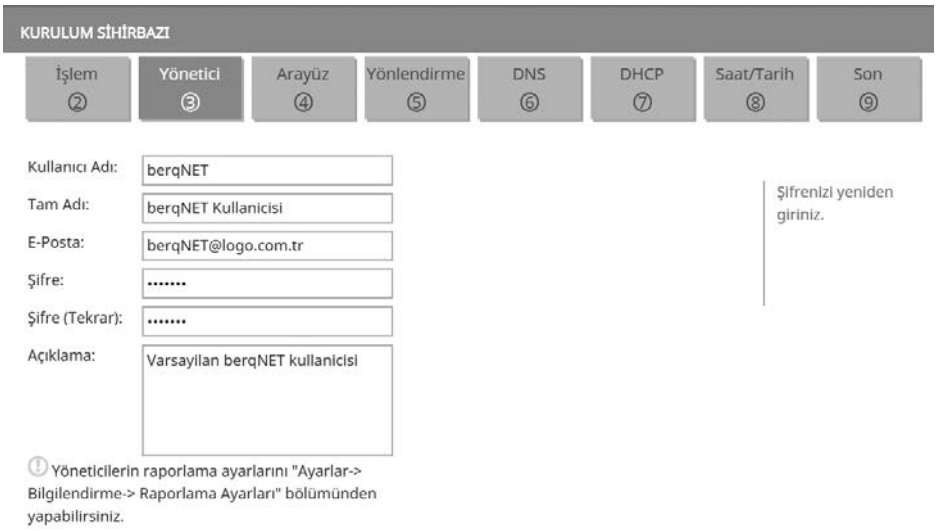


Ana sayfadaki düğmeler ve menülerin ne işe yaradığını biraz sonra göreceğiz. Şimdi Berqnet cihazımızın 30 saniyede kurulumunu gerçekleştiren sihirbazı çalıştıralım.

Ana sayfada Ayarlar düğmesine tıklayın, ardından açılan sayfada Sistem Ayarları bölümündeki Kurulum sihirbazı düğmesine tıklayın.

Açılan pencerede ileri düğmesine tıklayın, Yeni kurulum seçeneği seçili iken ileri düğmesine tıklayın.

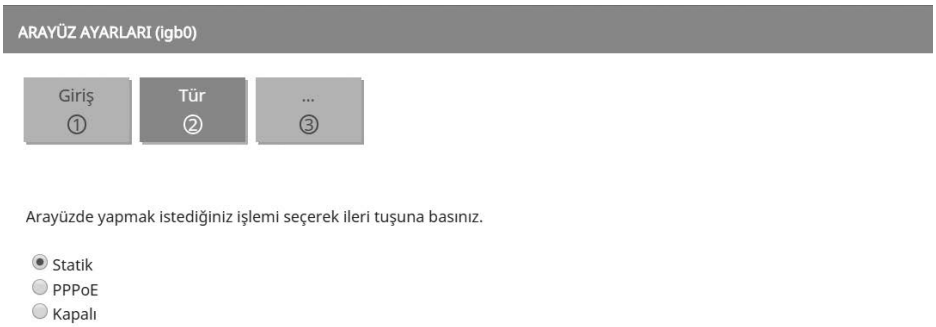
Yeni gelen pencerede cihaza giriş yaparken kullanacağınız kullanıcı adı ve şifre bilgilerini değiştirebilirsiniz. Değiştirmek istemiyorsanız şifre kısmına **berqNET** yazıp ileri düğmesine tıklayın.



Bu arada istediğiniz adımı Atla düğmesine basarak geçebilirsiniz. Şimdi sıra geldi arayüzleri yapılandırmaya.

Hatırlarsanız ig 0 arayüzünü modeme ig 1 arayüzünü switch'e takmıştık. Öncelikle igb 0 arayüzünü seçip düzenle düğmesine tıklayın. Yeni açılan arayüz ayarları penceresinde ileri düğmesine tıklayın.

Burada karşımıza birkaç seçenek çıkıyor. Statik seçeneği ile modemin olduğu ağın IP adresinden bir adresi atayabiliriz ya da PPPoE seçeneğini seçerek ve modemi bridge moda alarak İnternet sonlandırmasını Berqnet'te yapabiliriz. Benim modemim bridge moda alınmadığı için statik seçeneğini seçip ileri düğmesine tıkladım.

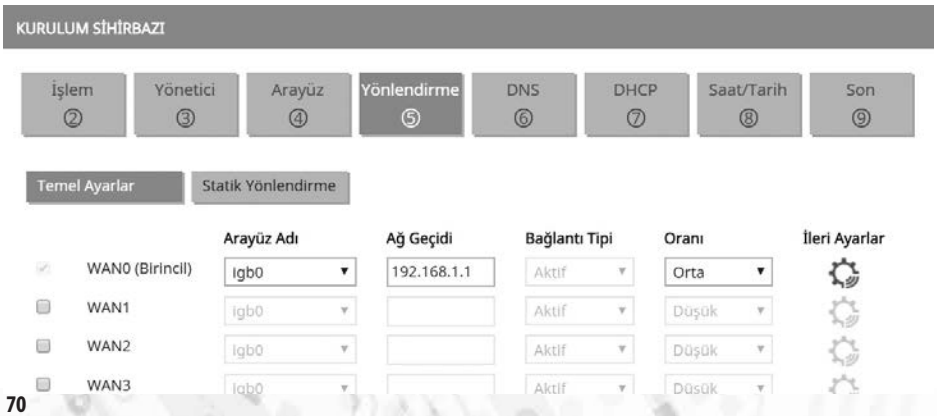


Burada modemin olduğu network olan 192.168.1.0 bloğundan bir IP adresi seçiyorum. Ben 192.168.1.35 adresini seçtim. Alt ağ maskesi olarak 255.255.255.0 yazıyorum. Bu arayüz modeme bağlı olduğu için WAN olarak tanımla kutucuğunu seçiyorum. Sonra da modemin IP adresi olan 192.168.1.1 adresini ağ geçidi olarak belirliyorum ve ileri düğmesine tıklıyorum.

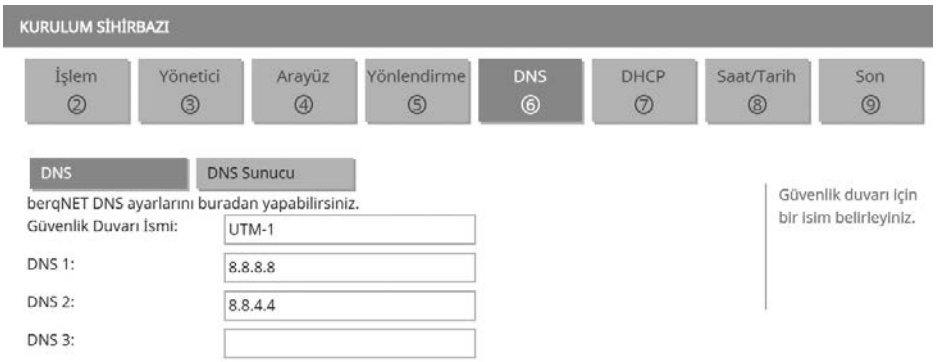
Bir sonraki pencerede bu arayüze birden fazla IP adresi atayabileceğimi belirten uyarı geliyor. İleri düğmesine tıklayıp geçebilirsiniz. Son olarak uygula düğmesine basıyoruz ve açılan pencerede yapılacak değişiklikleri görüyoruz. Burada son düğmesine basarak işlemi tamamlayalım.

Şimdi igb 0 arayüzünde hat var uyarısını almamız gerekiyor. Yoksa ağ geçidi adresini yanlış yazmış veya ağda kullanılan bir IP adresini arayüze atamış olabilirsiniz ya da alt ağ maskesini yanlış yazmış olabilirsiniz.

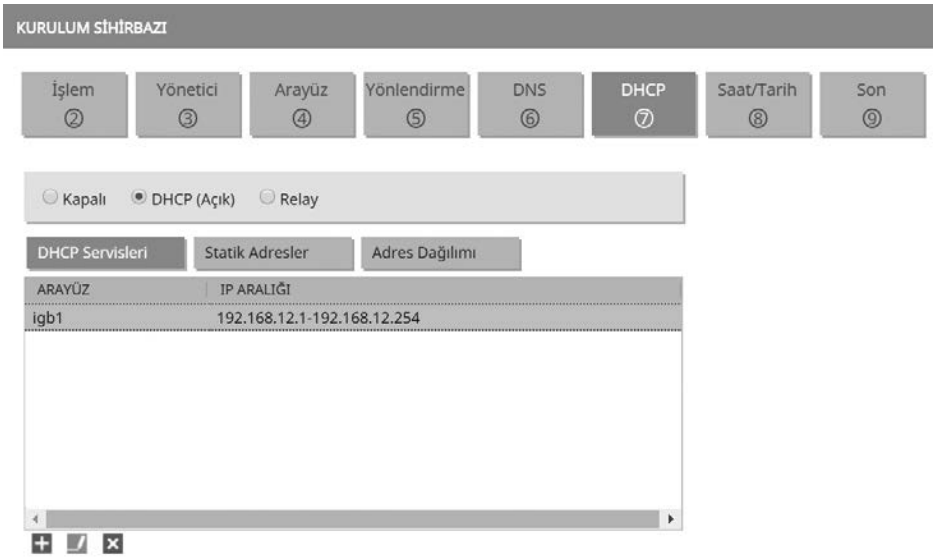
İleri düğmesine basıp sihirbaza devam edin. Burada birden fazla İnternet bağlantınız varsa yapılandırabileceğiniz pencere karşımıza gelir. Bir tane bağlantımız olduğunu varsayıp geçelim. İleride burayı ayrıntılı göreceğiz.



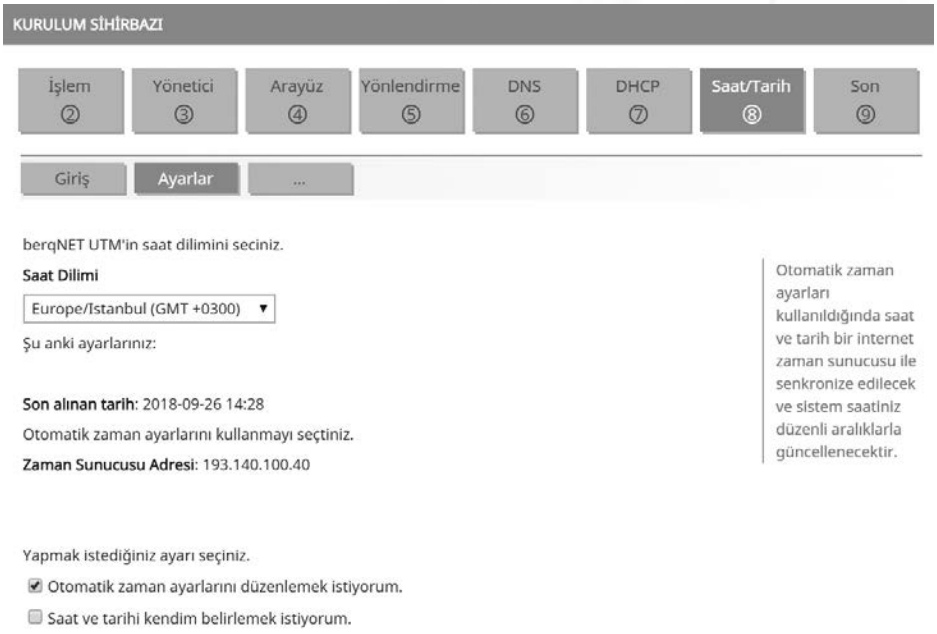
Şimdiki pencerede de güvenlik duvarı isim ve DNS ayarlarını yapıyoruz. Varsayılan olarak Google DNS sunucu adres bilgileri geliyor, istersek değiştirebilir istersek de ileri düğmesine tıklayabiliriz.



İgb 1 arayüzünü switch'e bağlamıştık. Bu switch'e bağlı hostlara bu arayüzden otomatik olarak IP adresi atamak için gerekli DHCP ayarlarına geldi sıra. Yine değişiklik yapmadan ileri düğmesine tıklayabilirsiniz.



Bir sonraki pencerede saat ve tarih ayarlarını değiştirebiliriz. Eğer bir hata yoksa atla düğmesine tıklayıp geçebilirsiniz.



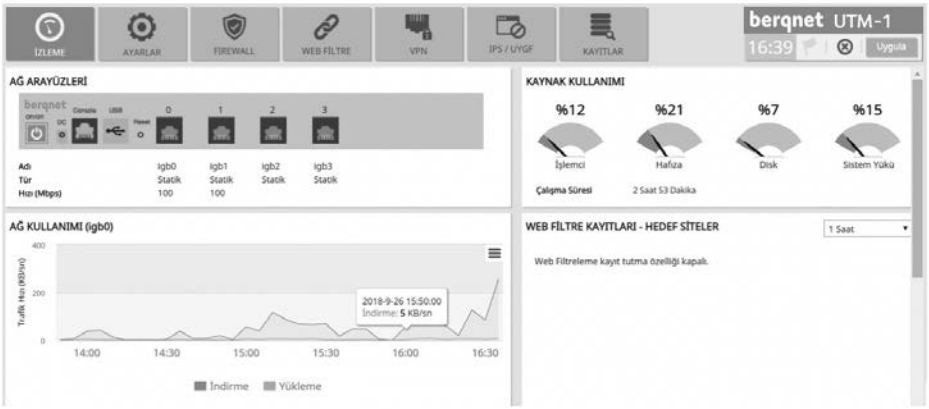
Bütün kurulum adımlarını tamamladık. Artık son düğmesine basarak ana ekrana dönebiliriz.

Ana ekranda sağ üst köşedeki Uygula düğmesine tıklayarak tüm değişikliklerin uygulanmasını sağlayalım.

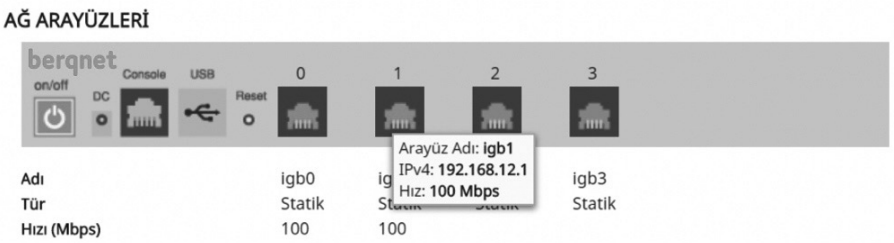
İşte Berqnet kurulumu bu kadar kolay ve hızlı.

6.3. İzleme Ekranı

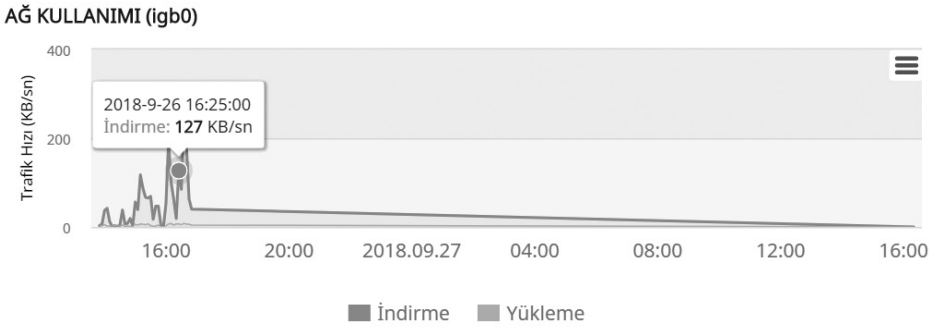
Berqnet'e giriş yaptığınızda sizi karşılayan ekrana izleme ekranı denir. Şimdi burada yer alan bölümleri görelim.



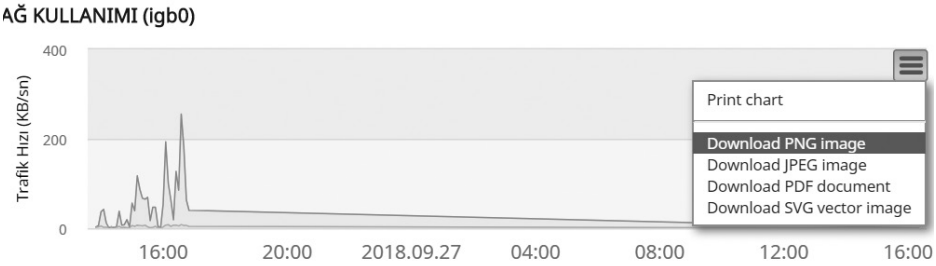
Öncelikle ekranın sol üst köşesinde Ağ arayüzleri bölümünü görüyoruz. Burada aktif olan (hat var) portlar mavi olarak belirtilmiş. WAN olarak belirlediğimiz igb 0 ve LAN olarak belirlediğimiz igb 1 portları şu an aktif durumda. İleride diğer portları da örnek topolojilerle devreye alıyor olacağız. Burada ayrıca portların üzerine fare imlecini getirdiğinizde portun arayüz adını, IP adresini ve hızını görebilirsiniz.



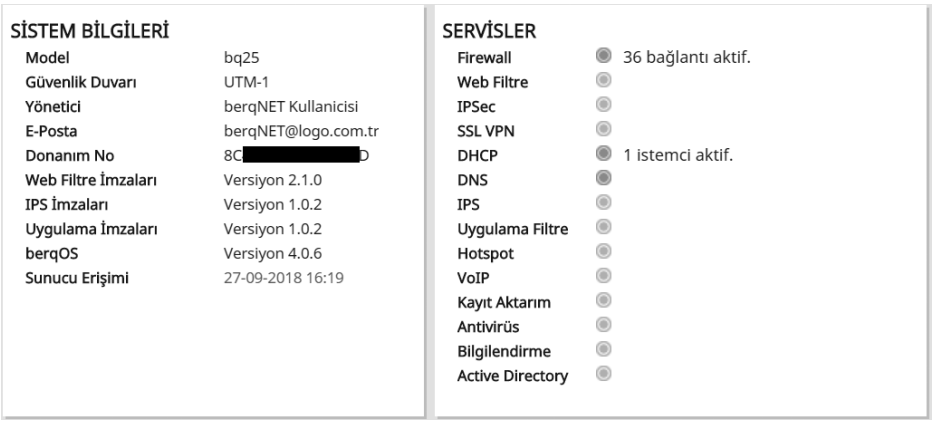
Solda ağ arayüzleri bölümün altında ağ kullanımı bölümünde grafik halinde Kb/sn cinsinden igb0 arayüzünün hızını ve zaman bilgisini görebilirsiniz. Burada indirmeler mavi, yüklemeler turuncu olarak renklendirilmiştir.



Ağ kullanımını grafik halinde değişik formatlarda indirmek isterseniz sağ üstteki menüye tıklayıp istediğiniz formatı seçebilirsiniz.



Ağ kullanımı bölümünün altında da sistem bilgileri ve servisler bölümünü görebilirsiniz.

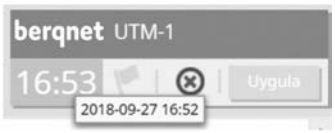


Yukarıdaki şekle göre cihazımın sistem bilgileri şöyle :

Modeli; Berqnet 25. Güvenlik duvarı ismi: UTM1. Cihaza giriş yaparken kullandığım yönetici adı: berqNET. Donanım numarası: 8Cxxxxxxxxx. Web filtre, IPS ve uygulama imza sürümleri. İşletim sistemi sürümü: 4.0.6. ve sunucuya erişim tarihi.

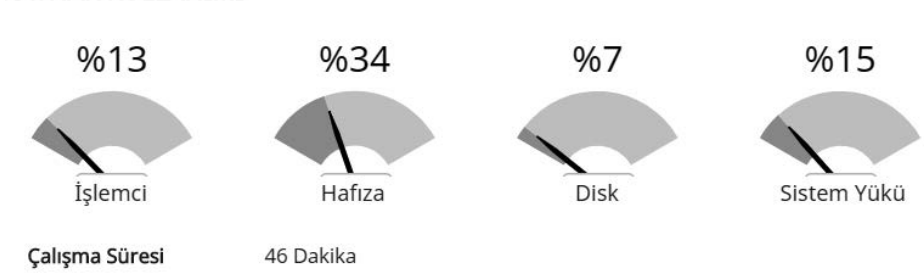
Yine yukarıdaki şekle göre çalışan servisleri yeşil olarak görüyoruz. Şimdilik sadece Firewall, DHCP ve DNS servisleri çalışıyor. Diğer servisleri de devreye aldıkça yeşil olarak belirtildiğini göreceğiz.

İzleme ekranının sağ üst köşesinde cihazın ismi, zaman bilgisi, uyarılar, çıkış ve uygula düğmesinin olduğu bir bölüm bulunuyor.



Cihazın ismini DNS ayarlarından değiştirebiliyorduk. Zaman bilgisi otomatik olarak İnternetteki zaman sunucularından alınıyor. Bayrak şeklindeki uyarılar simgesi ile mevcut uyarılar gösterilmekte ki şu an bir uyarı bulunmuyor. Kırmızı çarpı şeklindeki çıkış düğmesine tıkladığımızda cihazdan çıkış yapıyoruz. Uygula düğmesi ile de yaptığımız değişikliklerin örneğin web filtre ayarlarının uygulanmasını sağlıyoruz.

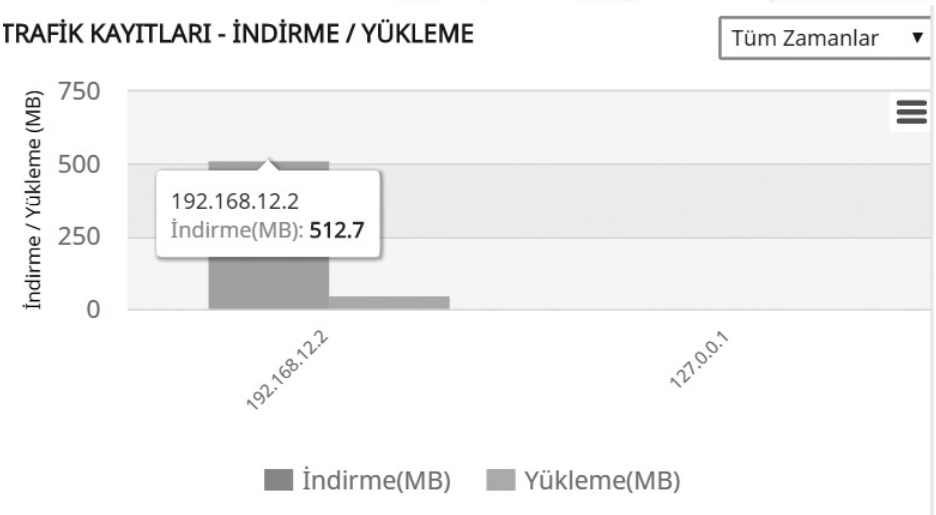
Sağ üstteki bölümlerden biri de cihazın donanım kullanımını gösteren kaynak kullanımı bölümü.



Yukarıdaki şekle göre cihaz 46 dakikadır çalışıyor. İşlemcinin %13'ü, belleğin %34'ü ve diskin %7'si aktif olarak kullanılmakta. Genel sistem yükü ise %15.

Sağdaki başka bir bölüm de Web filtre kayıtları. Burada web filtreleme şu an aktif olmadığı için bir şey göremiyoruz.

Son olarak trafik kayıtları bölümünde host başına indirilen ve gönderilen veri miktarını görebiliyoruz.



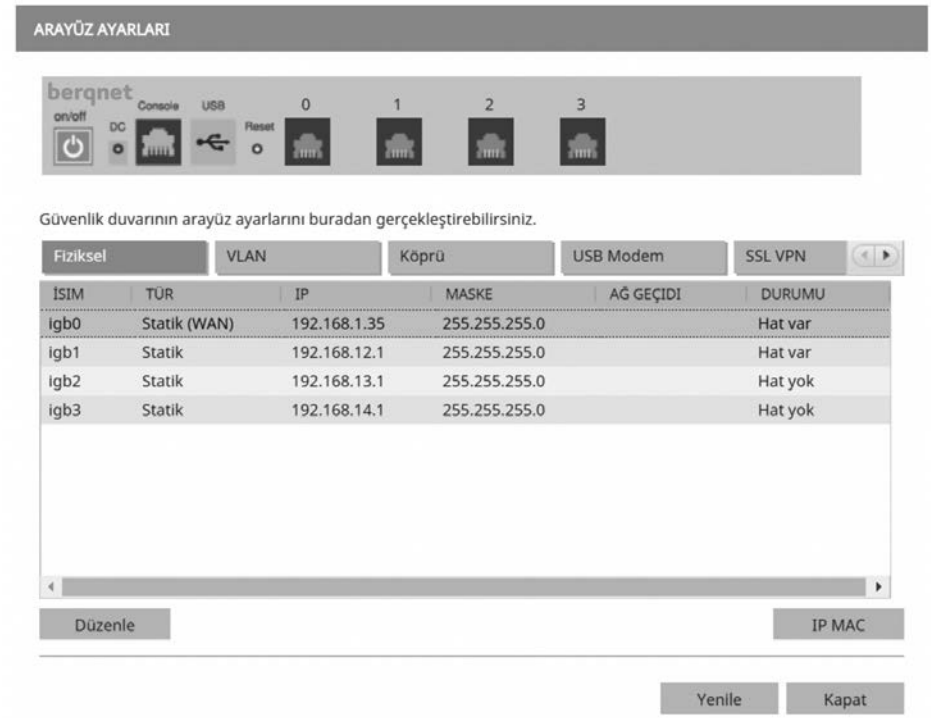
Örneğin burada 192.168.12.2 IP adresine sahip bilgisayar 512 MB veri indirmiş. Yine ağ kullanımında olduğu gibi bu grafikleri de değişik formatlarda bilgisayarınıza aynı yöntemle indirmeniz mümkün. Bu bölümle ağınızda İnterneti en çok kullanan kişileri görebilirsiniz.

6.4. Ayarlar Ekranı

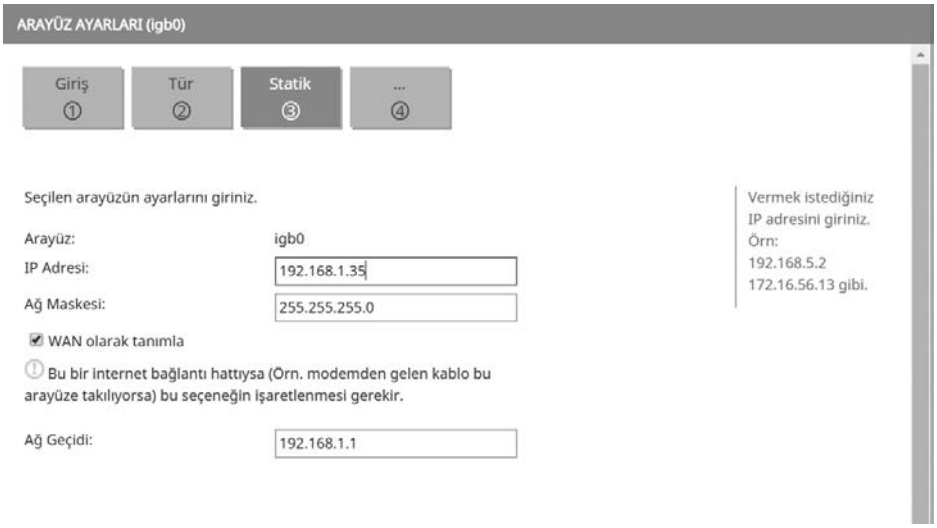
Ana sayfada Ayarlar sekmesine tıkladığımızda Berqnet'in ayarlarını yapabileceğimiz sayfaya ulaşırız.

Burada öncelikle ağ yapılandırma ayarlarına bakalım. Her ne kadar öncesinde kurulum sihirbazı ile hızlı bir kurulum gerçekleştirmiş olsak da arayüz ayarlarından başlayalım.

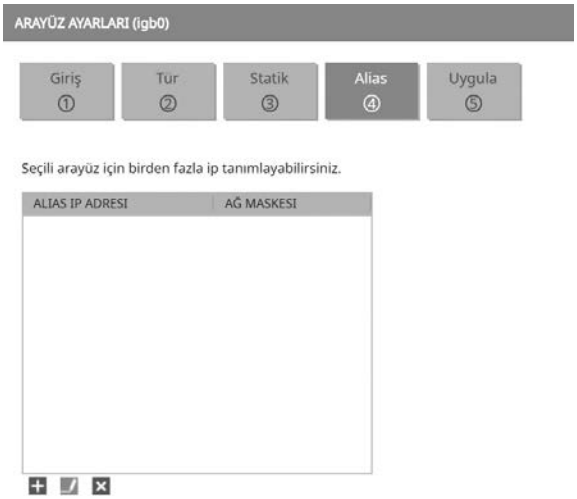
Arayüz ayarları simgesine tıkladığımızda arayüz ayarları penceresi açılır.



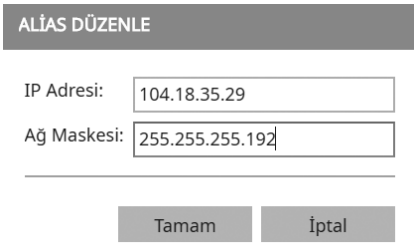
Berqnet'in modeline göre arayüz sayısı değişir. 25 modelinde 4 tane arayüz bulunmaktadır. Hatırlarsanız modemden gelen ağ kablosunu igb0 arayüzüne takmıştık. Şimdi bu arayüzü WAN arayüzü olarak nasıl yapılandırabiliriz görelim. İgb0 arayüzü seçili iken sol altta bulunan düzenle düğmesine tıklayın. Arayüz ayarları (igb0) penceresi açılacaktır. Burada ileri düğmesine tıklayarak devam edin. "Arayüzde yapmak istediğiniz işlemi seçerek ileri tuşuna basınız" seçeneğinin altında statik, PPPoE ve kapalı seçenekleri vardır. Statik seçeneği ile WAN arayüzüne modem ile aynı ağdan (subnet) bir IP adresi atarız. PPPoE seçeneği ile modemi bridge moda alarak İnternet'i Berqnet'te sonlandırırız. Kapalı seçeneği ile de arayüzü kapatırız. Şimdi statik seçeneği seçili iken ileri düğmesine tıklayalım. Açılan pencerede statik olarak modemin bulunduğu ağdan bir IP adresi atıyoruz. Benim modemimin DHCP sunucusu 192.168.1.0 ağından IP adresi dağıttığı için ben kullanılmayan 192.168.1.35 adresini bu arayüze 255.255.255.0 alt ağ maskesini kullanarak atadım. WAN olarak tanımla onay kutusunu seçtim ve varsayılan ağ geçidi olarak da modemin IP adresi 192.168.1.1'i yazdım.



Daha sonra ileri düğmesine tıklıyorum. Buradaki pencerede eğer gerekli ise bu arayüze (igb0) birden fazla IP adresi (ALIAS IP) atayabiliriz. Özellikle Metro Ethernet hatlarında birden fazla WAN IP'ye sahipsek bu bölüme ilgili IP'leri tanımlayarak daha sonra ilgili IP'lerin yönlendirmelerini gerçekleştirebiliriz.



Burada açılan pencerede sol alttaki mavi artı tuşuna basarak yeni açılan pencerede diğer WAN IP adreslerini yazıyoruz.



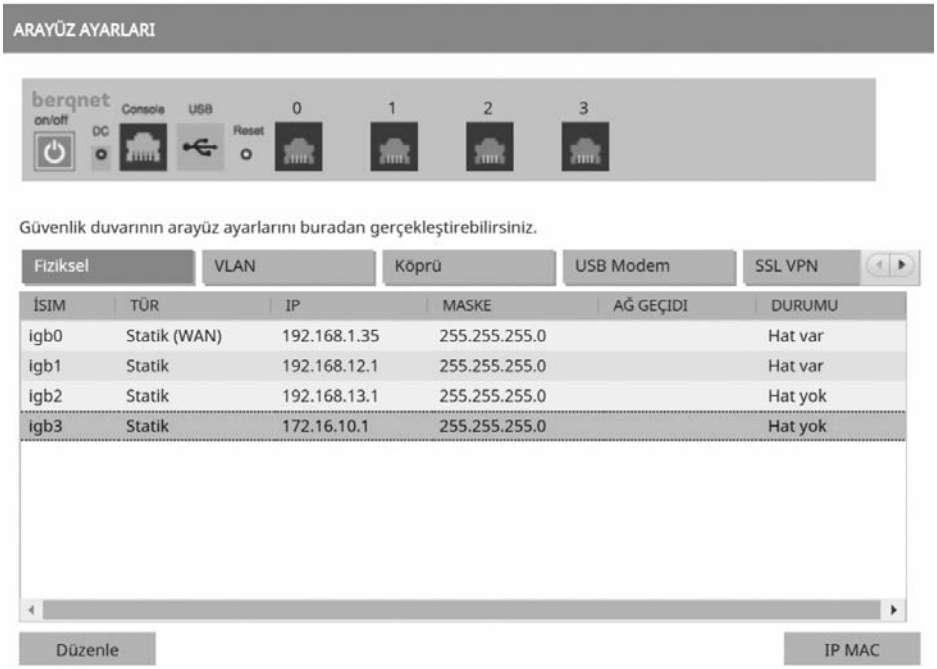
Son olarak uygula düğmesine basarak yaptığımız değişikliklerin uygulanmasını sağlıyoruz. Son düğmesine tıklayarak pencereyi kapatıyoruz. Bu arada arayüz ve DNS servisi tekrar başlatıldığı için varsa İnternet bağlantınızda kesinti yaşayabilirsiniz.

Şimdi de PPPoE yani İnternet'i Berqnet'te sonlandırmayı görelim. Bunun için arayüz ayarlarından igb0 arayüzü seçili iken düzenle düğmesine tıklayın. Açılan pencerede ileri düğmesine tıklayıp yeni gelen pencerede PPPoE seçeneğini seçip ileri düğmesine tıklayın ve servis sağlayıcının (ISP) size verdiği kullanıcı adı ve parola bilgilerini yazıp ileri düğmesine tıklayın.

Uygula ve son düğmelerine tıklayarak işlemi tamamlayabilirsiniz. PPPoE ayarını yapmadan önce modeminizi bridge (köprü) moduna almanız gerektiğini unutmayın.

Berqnet'in diğer arayüzlerine varsayılanda 192.168.12.1, 192.168.13.1, 192.168.14.1 IP adresleri atanmış olarak gelir. İsterseniz bu IP adreslerini kendi topolojinize göre değiştirebilirsiniz. Örneğin bir DMZ alanı oluşturmak ve bazı sunucularımızı burada barındırmak istiyoruz. DMZ alanını Berqnet'in igb3 arayüzünde gerçekleştirelim ve 172.16.10.1/24 IP adresini atayalım. İgb3 arayüzü seçili iken düzenle düğmesine tıklayın. Sonrasında ileri düğmesine tıklayın. Yeni açılan pencerede statik seçili iken ileri düğmesine tıklayın ve mevcut adresleri aşağıdaki resimdeki gibi değiştirin.

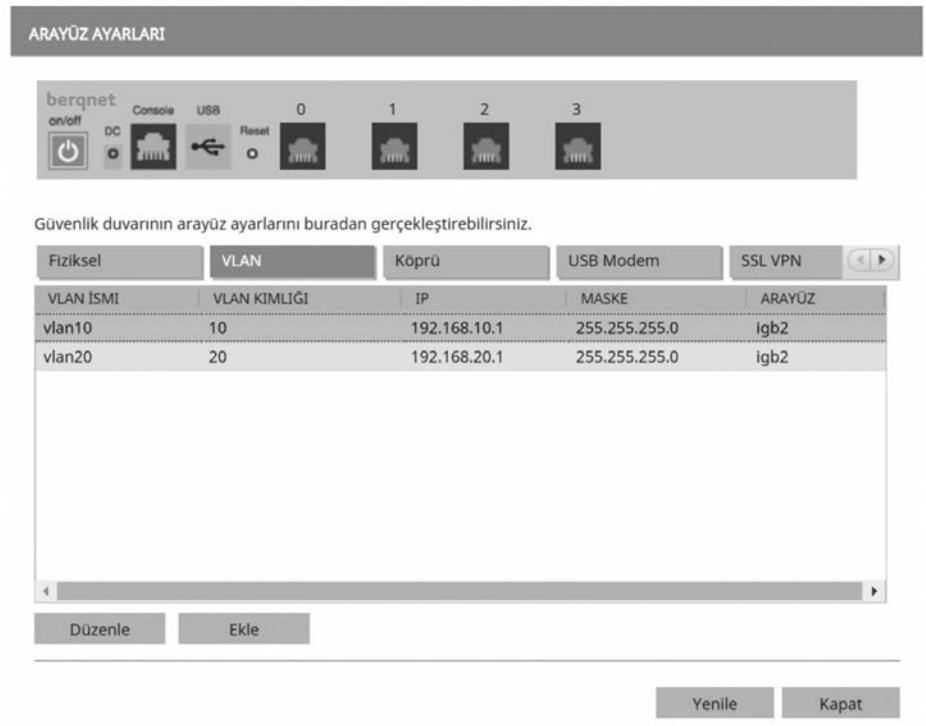
İleri düğmesine iki defa tıklayın ve uygula düğmesine tıklayarak değişikliklerin uygulanmasını sağlayın. Son düğmesine tıklayarak pencereyi kapatın. Artık igb3 arayüzünün yeni bir IP adresi var.



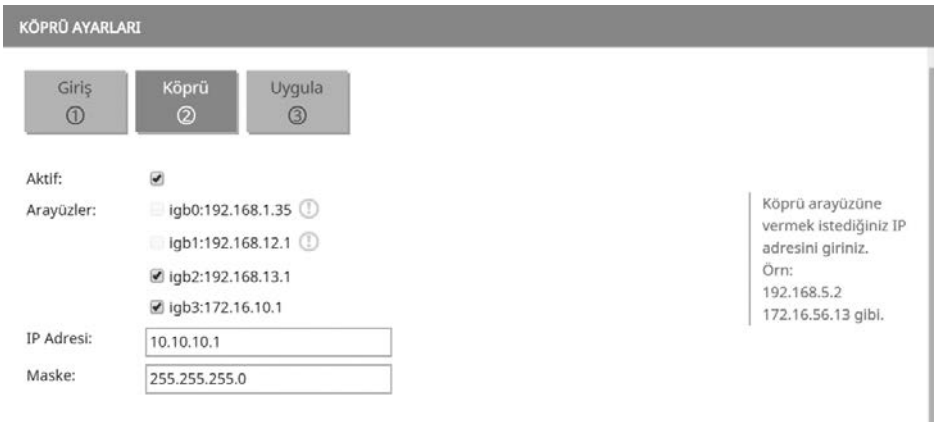
Arayüz ayarlarında fiziksel sekmesi altında arayüzlerin IP adresi ayarlamalarını gerçekleştirdik. Bir yandaki sekme olan VLAN sekmesinde de eğer yapımızda VLAN'ler varsa bunların sonlandırmasını Berqnet üzerinde gerçekleştirebiliriz. VLAN sekmesine tıklayalım. Burada ekle düğmesine tıklayın. Sonrasında ileri düğmesine tıklayarak VLAN ekleme penceresine gelin. Önce Aktif onay kutusunu seçin. Ve ardından VLAN bilgilerini girin.

İleri ve ardından uygula düğmesine tıklayarak işlemi tamamlayın. Son düğmesine tıklayarak pencereyi kapatın.

Aynı arayüze başka VLAN'ler eklemek istiyorsak ekle düğmesine tıklayarak aynı işlemleri gerçekleştirip yeni VLAN'ler ekleyebiliriz.

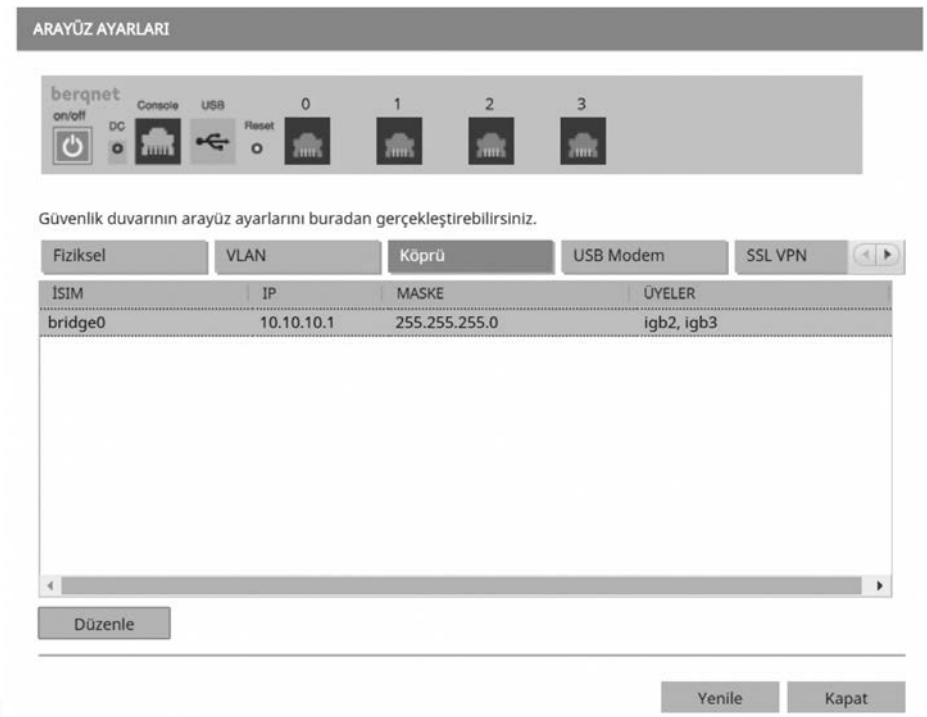


Arayüz ayarlarını görmeye devam edelim. Vlan ayarlarının hemen yanında bulunan köprü ayarları ile birden fazla arayüzü birleştirerek tek bir arayüz haline getirebilirsiniz. Cisco'daki etherchannel yapılandırmasına benzetebiliriz. Şekilde gördüğünüz üzere igb2 ve igb3 arayüzlerini birleştirdik ve yeni oluşan köprü arayüzüne 10.10.10.1/24 IP adresini atadık.



Uygula ve ardından son düğmelerine tıklayarak yapılandırmayı tamamlayabilirsiniz.

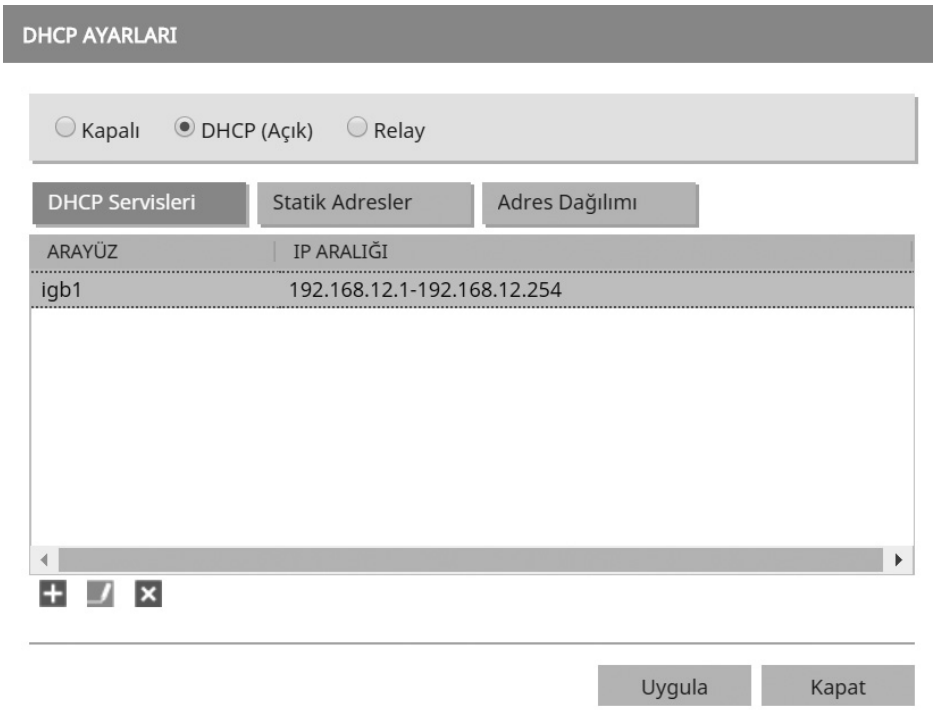
Artık igb2 ve igb3 arayüzlerinin birleşiminden oluşan bridge0 isimli 10.10.10.1 IP adresine sahip bir köprü arayüzümüz var.



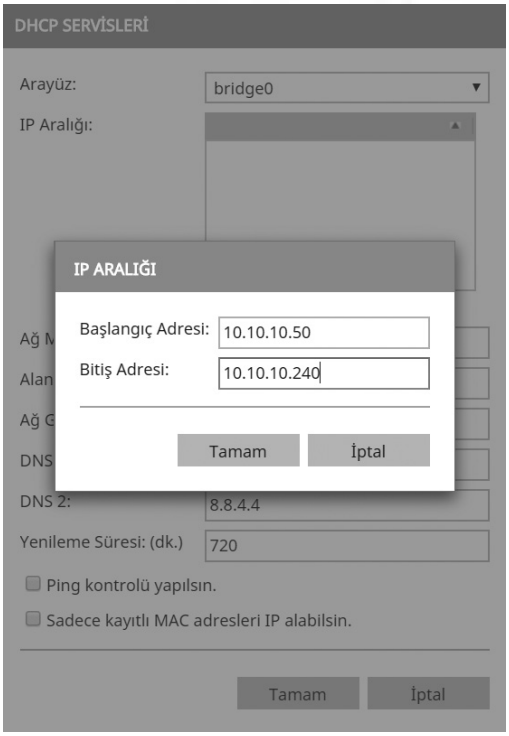
Arayüz ayarlarının USB Modem sekmesinde eğer Berqnet'in USB portlarından birine 3G veya 4G USB modem takmışsanız burada görüntüleyebilirsiniz.

Arayüz ayarlarının SSL VPN sekmesinde yalnızca izleme yapabilirsiniz, ayarlamak için ileride VPN sayfasını kullanacağız.

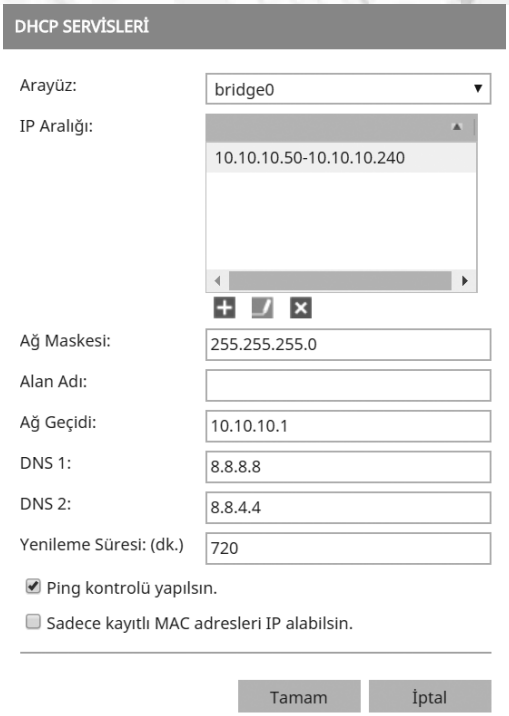
Ağ yapılandırma bölümünde DHCP ayarlarına bakalım. DHCP simgesine tıkladığınızda DHCP ayarları penceresi açılır.



Şekilde igb1 arayüzünde mevcut bir DHCP yapılandırması olduğunu görüyoruz. Bu yapılandırmayı düzenlemek istersek penceresinin sol alt köşesindeki yeşil kalem simgesine, silmek istersek kırmızı çarpı simgesine, başka bir arayüzde DHCP yapılandırmak için mavi artı simgesine tıklayın. Şimdi mavi artı simgesine tıklayarak daha önce oluşturduğumuz köprü arayüzünde (bridge0) DHCP yapılandırması gerçekleştirelim. En üstteki arayüz kısmından bridge0 seçin. IP aralığı için mavi artı simgesine tıklayın. Başlangıç ve bitiş adreslerini yazın.

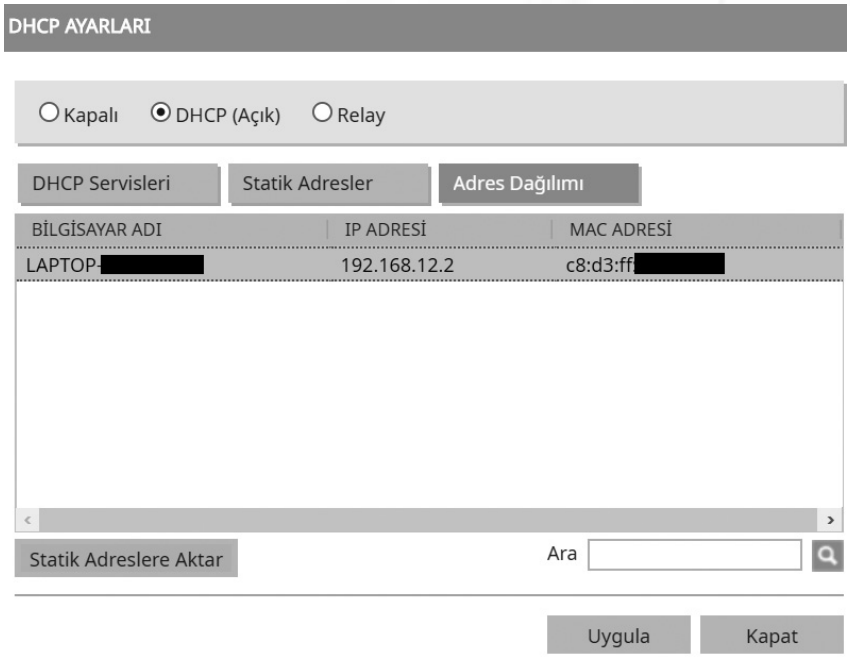


Şekildeki yapılandırmaya göre DHCP havuzundan 10.10.10.50 ile 10.10.10.240 arasında IP adresi dağıtılmasını sağlayacağız. Bunun dışında kalan örneğin 10.10.10.35 gibi bir IP adresini statik olarak bir ağ cihazına verebiliriz. Ayarların devamında alt ağ maskesini, ağ geçidini, DNS adreslerini ve yenileme (kira-lease) süresini belirleyebilir ya da eğer uygunsa varsayılan değerlerde bırakabiliriz.

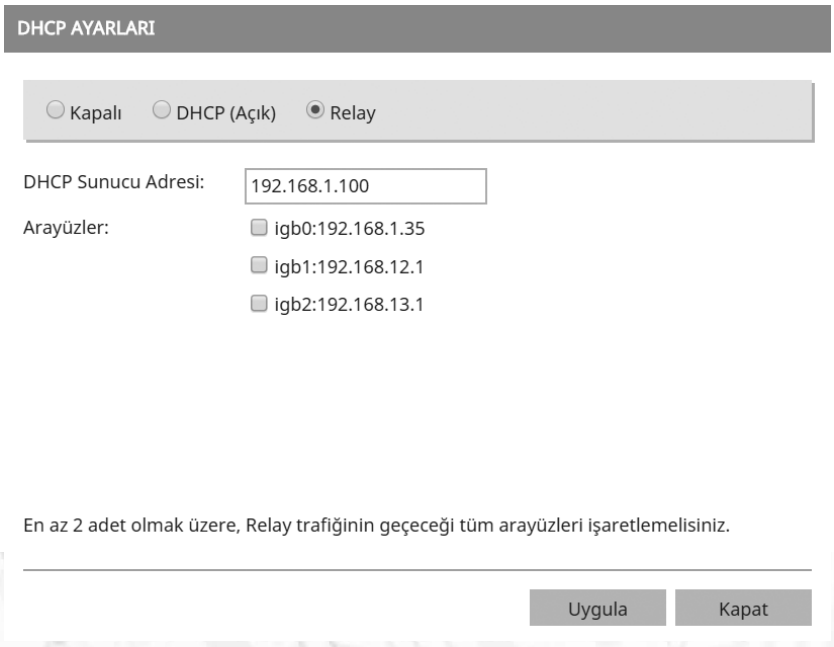


Yenileme süresi varsayılan ayarlarda 720 dakika yani 12 saattir. İsterseniz bunu artırıp azaltabilirsiniz. Özellikle misafir (guest) ağlarında bu değerin 2-3 saat olması tavsiye edilir. Pencerenin alt tarafındaki ping kontrolü yapılsın seçeneğine onay koyarak IP adresi DHCP tarafından atanmadan önce ping kontrolü yapılarak atamak istediği bir adresin yanlışlıkla veya statik bir host'a atanıp atanmadığını dolayısıyla IP çakışmasını önleyebilirsiniz. Yine sadece kayıtlı MAC adresleri IP alabilsin seçeneğine onay koyarak sadece tanımlı MAC adreslerine sahip host'lara IP adresi ataması yapılmasını sağlayabilirsiniz.

DHCP ayarlarının yapıldığı bölümde statik adresler sekmesinde statik olarak atanacak IP adresleri belirlenebilir. Adres dağılımı sekmesinde de DHCP sunucu tarafından atanmış mevcut adresler görülebilir. Burada atanan IP adreslerinin MAC adresleri ile eşlenmesi sağlanarak aynı bilgisayara her zaman aynı IP adresinin atanması sağlanabilir. Bunun için ilgili sekmede sol alttaki statik adreslere aktar düğmesine tıklamanız yeterlidir.



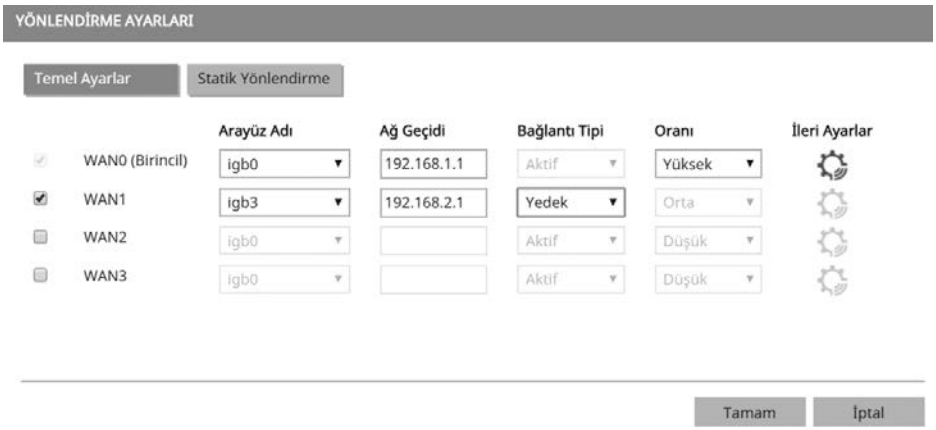
Relay sekmesinde DHCP Relay agent yapılandırması gerçekleştirilir. DHCP Discover mesajları broadcast olduğundan ve broadcast mesajlar ağ dışına çıkmadığından, ağın dışında bulunan bir DHCP sunucuya erişmek için bu yapılandırma gereklidir. Örneğimizde 192.168.1.100 IP adresine sahip DHCP sunucumuz olsun ve Berqnet değil bu sunucu IP adresi dağıtsın. Sunucuda her Berqnet arayüzü için ayrı scop'lar tanımladığımızı varsayarsak ilgili DHCP relay agent yapılandırması şekilde görüldüğü gibi yapılır.



Şimdi sıra geldi DNS ayarlarına. Ağ yapılandırma ayarlarında DNS simgesine tıklayın. Açılan pencerede Berqnet'in kullandığı varsayılan DNS ayarlarını göreceksiniz. Mevcut ayarlarda Google DNS'leri olan 8.8.8.8 ve 8.8.4.4 kullanılıyor. Eğer farklı DNS servisi kullanmak isterseniz buraya ilgili servisin IP adreslerini yazıp uygula düğmesine tıklayın.

DNS Sunucu sekmesinde ise igb1 DHCP ayarlarında DNS sunucu olarak 192.168.12.1 adresini girerek Berqnet'in bu arayüzüne DNS sorgusu gönderilir. Burada yine bir önceki DNS ayarları kullanılarak DNS sorgusu çözümleme işlemleri gerçekleştirilir.

Yönlendirme ayarları bölümünde WAN arayüzleri ve öncelik seviyelerini belirleyebiliyorsunuz. Berqnet bq25 modelinde 4 adet port bulunmaktadır. Bu portlardan istediğinizi WAN arayüzü olarak ayarlayabilirsiniz. Örneğin iki tane İnternet bağlantımız olsun birini igb0 arayüzüne bağlarken diğerini de igb3 arayüzüne bağlayabiliriz. Tabii öncelikle igb3 için daha önce arayüz ayarlarının yapılmış olması gerekiyor. Şekle göre igb3 arayüzüne bağladığım 2. İnternet bağlantısını yedek olarak tanımladım. Birinci bağlantım kesilirse hemen yedek bağlantım devreye girecektir.

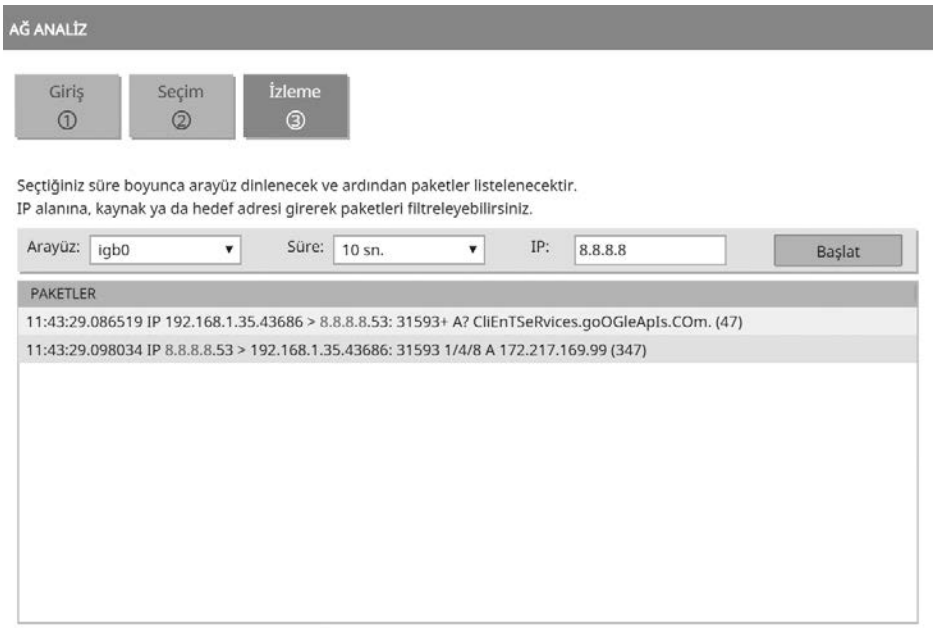


Bunun dışında ikinci bağlantıyı aktif olarak belirleyip daha düşük bir oran belirleyerek de yedek kullanabiliriz. Statik yönlendirme sekmesinde de statik routing veya varsayılan routing ayarları yapılabilir.

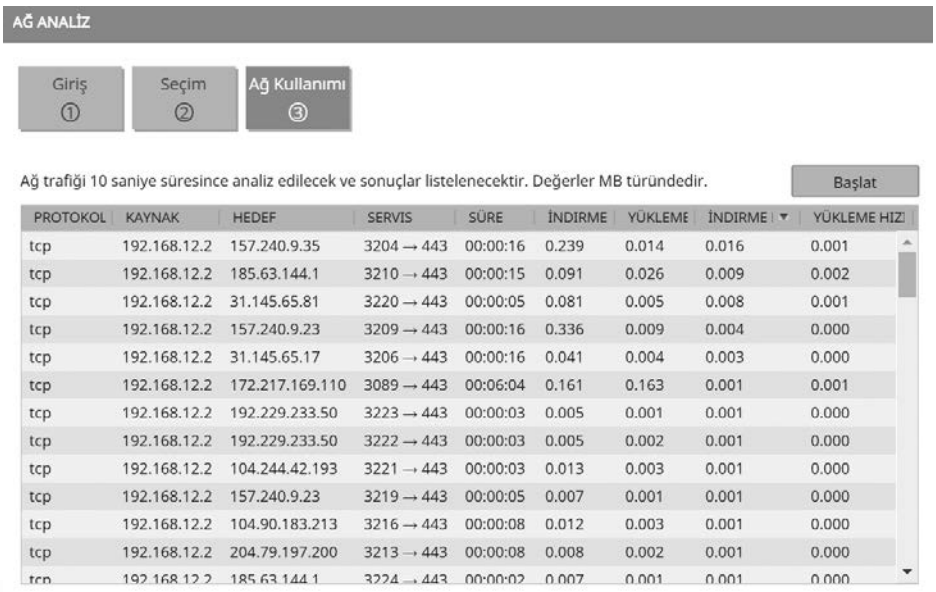
Ağ analiz bölümünde ise resimdeki kontrol servislerini kullanarak ağda sorun giderme ve performans ölçümlemesini gerçekleştirebiliriz.

İlk seçenek olan ping kontrol ile istediğimiz bir web sitesine ping atabiliriz. Varsayılan olarak www.ulakbim.gov.tr adresi gelmektedir. Bu adresi değiştirip ping düğmesine tıklayıp sonuçları alttaki sonuçlar bölümünde görebilirsiniz. Şekilde Ulakbim web sitesine ping işleminin sonucunu görebilirsiniz.

İkinci olarak paket izleme seçeneği ile seçtiğiniz süre boyunca belirlediğiniz arayüz dinlenecek ve ardından paketler listelenecektir. Şekilde igb0 arayüzünden 8.8.8.8 Ip adresine giden trafik listelenmiştir.



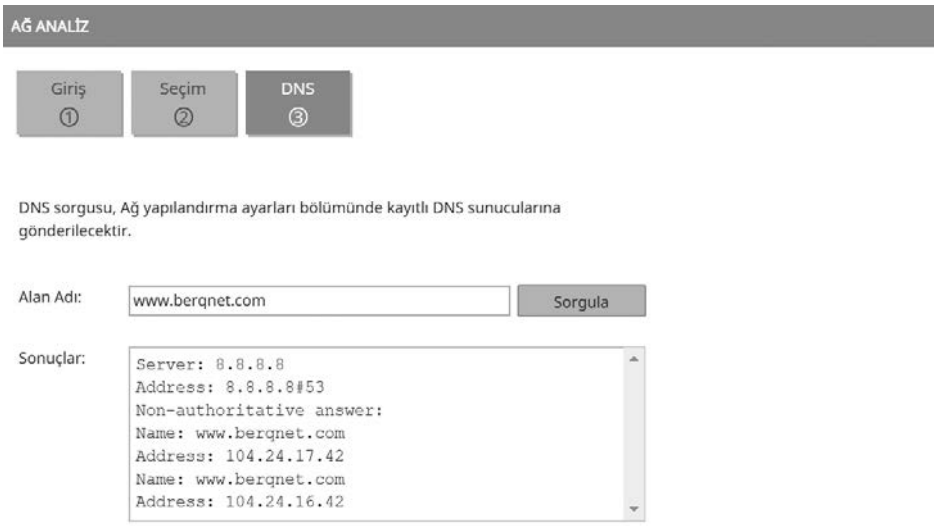
Üçüncü olarak anlık ağ kullanımı seçeneği ile ağ trafiği 10 saniye süresince analiz edilecek ve sonuçlar listelenecektir. Değerler MB türündedir. Şekilde 10 saniye boyunca yakalanan trafik görüntülenmiştir.



PROTOKOL	KAYNAK	HEDEF	SERVIS	SÜRE	İNDIRME	YÜKLEME	İNDIRME	YÜKLEME HIZ
tcp	192.168.12.2	157.240.9.35	3204 → 443	00:00:16	0.239	0.014	0.016	0.001
tcp	192.168.12.2	185.63.144.1	3210 → 443	00:00:15	0.091	0.026	0.009	0.002
tcp	192.168.12.2	31.145.65.81	3220 → 443	00:00:05	0.081	0.005	0.008	0.001
tcp	192.168.12.2	157.240.9.23	3209 → 443	00:00:16	0.336	0.009	0.004	0.000
tcp	192.168.12.2	31.145.65.17	3206 → 443	00:00:16	0.041	0.004	0.003	0.000
tcp	192.168.12.2	172.217.169.110	3089 → 443	00:06:04	0.161	0.163	0.001	0.001
tcp	192.168.12.2	192.229.233.50	3223 → 443	00:00:03	0.005	0.001	0.001	0.000
tcp	192.168.12.2	192.229.233.50	3222 → 443	00:00:03	0.005	0.002	0.001	0.000
tcp	192.168.12.2	104.244.42.193	3221 → 443	00:00:03	0.013	0.003	0.001	0.000
tcp	192.168.12.2	157.240.9.23	3219 → 443	00:00:05	0.007	0.001	0.001	0.000
tcp	192.168.12.2	104.90.183.213	3216 → 443	00:00:08	0.012	0.003	0.001	0.000
tcp	192.168.12.2	204.79.197.200	3213 → 443	00:00:08	0.008	0.002	0.001	0.000
tcp	192.168.12.2	185.63.144.1	3224 → 443	00:00:02	0.007	0.001	0.001	0.000

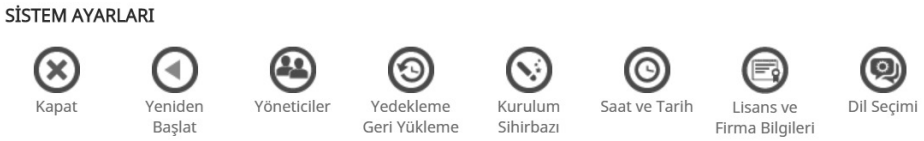
Dördüncü seçenekte traceroute ile bir paketin izini takip edebilirsiniz. Şekilde Berqnet web sitesine giden trafiğin hangi yönlendiricilerden geçtiğini görebilirsiniz.

Son seçenek olan DNS sorgulama ile de belirttiğiniz bir web adresi hakkındaki sorgu ağ yapılandırma ayarları bölümünde kayıtlı DNS sunucularına gönderilecektir. Şekilde berqnet.com alan adının DNS sorgusu sonuçlarını görebilirsiniz.



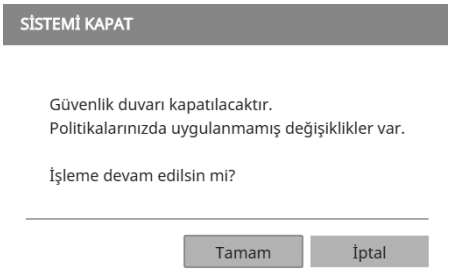
6.5. Sistem Ayarları

Bu bölümde ayarlar bölümündeki sistem ayarları ile ilgili seçenekleri göreceğiz. Soldan sağa tek tek bakalım şimdi bu seçeneklere.



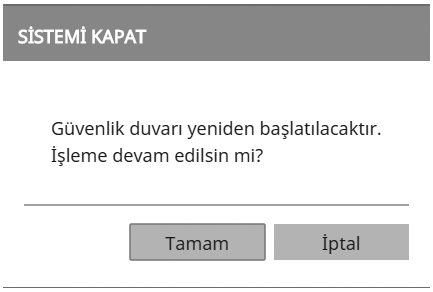
6.5.1. Kapat

Kapat düğmesine tıkladığımızda Berqnet kapatılacaktır. Eğer yaptığınız ve uygulamadığınız yapılandırmalar varsa bunu yapmanız için bir uyarı görebilirsiniz.



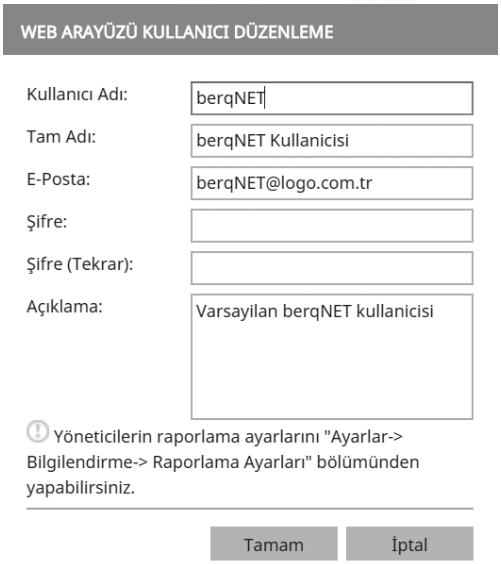
6.5.2. Yeniden Başlat

Yeniden başlat düğmesine tıkladığınızda da cihaz kapatılıp tekrar başlatılır.

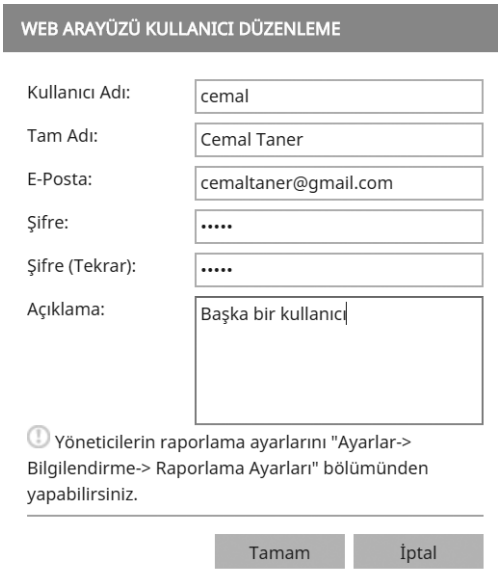


6.5.3. Yöneticiler

Yöneticiler düğmesine tıklayarak cihaza web arayüzünden erişip yönetebilecek hesapları görebilir ve yeni kullanıcılar ekleyebilirsiniz. Varsayılanda berqNET kullanıcı adı ve berqNET parolası ile bir hesap bulunmaktadır. İsterseniz kalem simgesine tıklayarak mevcut hesapta değişiklikler yapabilirsiniz.



Ya da + simgesine tıklayarak yeni bir kullanıcı ekleyebilirsiniz. Şekilde cemal kullanıcı adlı yeni hesap oluşturma işlemini görebilirsiniz.



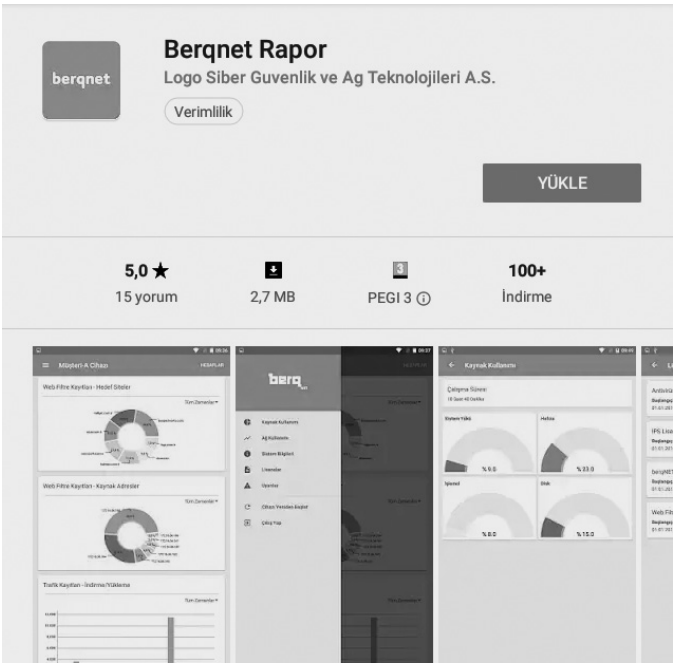
Yönetici ayarları penceresinin sağ alt kısmında çarpı (X) simgesine tıklayarak da seçili kullanıcıyı silebilirsiniz. Bu işlemi gerçekleştirmek için ilgili hesabın şifresini girmeniz gerekmektedir. Yeni kullanıcı ile oturum açtığınızda İzleme ekranının sistem bilgileri bölümünde kullanıcı bilgilerini görebilirsiniz.

SİSTEM BİLGİLERİ

Model	bq25
Güvenlik Duvarı	UTM-Berq
Yönetici	Cemal Taner
E-Posta	cemaltaner@gmail.com
Donanım No	8C490D004884ABCD
Web Filtre İmzaları	Versiyon 2.1.0
IPS İmzaları	Versiyon 1.0.2
Uygulama İmzaları	Versiyon 1.0.2
berqOS	Versiyon 4.0.6
Sunucu Erişimi	15-11-2018 14:31

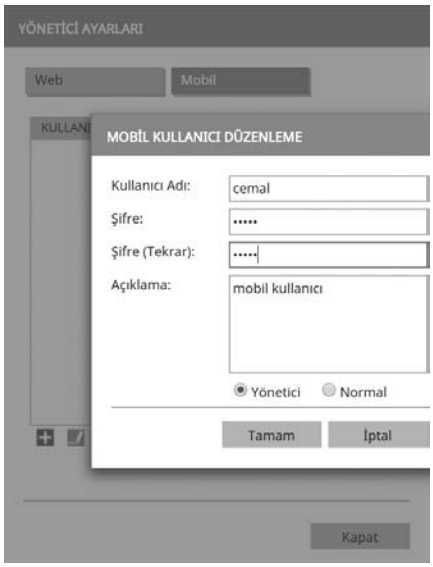
6.5.3.1. Mobil Raporlama Uygulamasına Genel Bakış

Berqnet'in üstün özelliklerinden biri de mobil raporlama uygulamasıdır. Bu uygulamayı cep telefonunuza yükleyerek birden fazla Berqnet cihazı uygulamaya ekleyebilir, cihazlarınıza uzaktan erişebilir, kapatıp açabilir, izleme ekranında gördüğünüz bilgileri (sistem bilgileri, lisans bilgiler vb.) mobil raporlama uygulamasından takip edebilirsiniz. Berqnet mobil rapor uygulaması Apple App Store ve Google Play Store üzerinden "Berqnet Rapor" ismiyle bulunarak indirilebilir. Uygulama, mobil cihazın diline göre Türkçe ve İngilizce olarak kullanılmaktadır.



Uygulamayı yükledikten sonra Berqnet üzerinde yapmamız gereken ayarlar bulunmaktadır. Bunun için önce sistem ayarları bölümünde yöneticiler simgesine tıklayın.

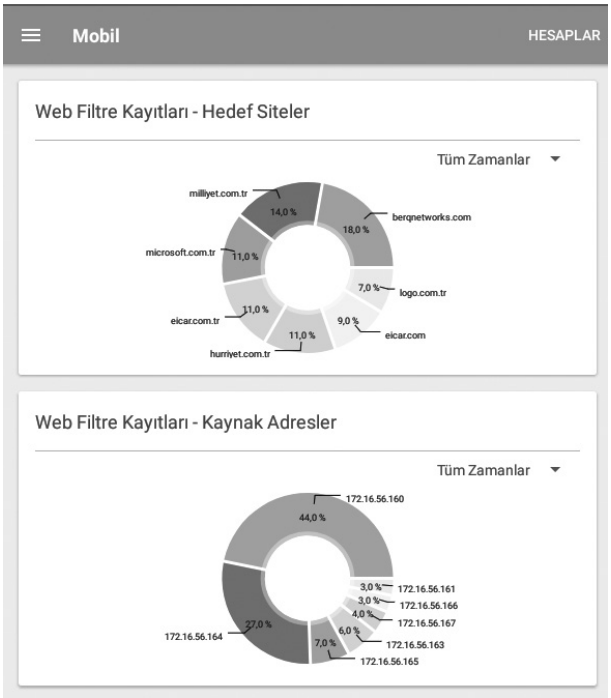
Sonrasında açılan pencerede mobil sekmesine geçiş yapın. Burada + simgesine tıklayarak yeni bir kullanıcı için bilgileri girin. Yönetici ve normal olarak iki farklı yetkide kullanıcı oluşturulabilmektedir. Yönetici yetkisiyle uygulama üzerinden cihazın temel web filtre ve trafik raporları, kaynak kullanımı, ağ kullanımı, sistem bilgileri, lisansları, uyarıları görülebilir ve cihaz yeniden başlatılabilir. Normal yetkiyle uygulama üzerinden sadece temel web filtre ve trafik raporları görülebilir. Şekilde yönetici haklarına ve **cemal** kullanıcı adına sahip bir mobil kullanıcı oluşturulmuştur.



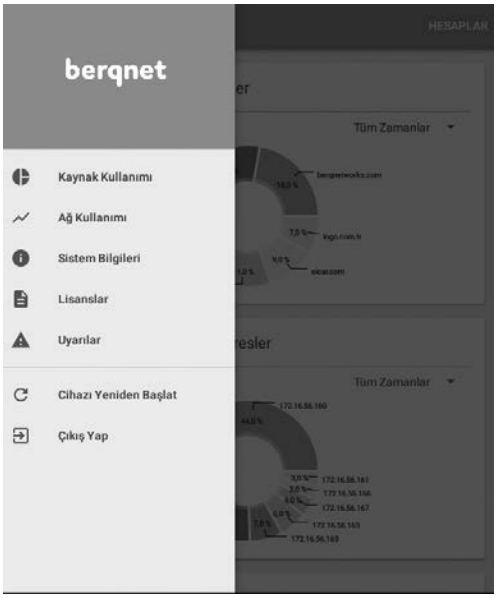
Şimdi mobil uygulamayı açalım ve az önce oluşturduğunuz hesabı tanımlayalım (Öncesinde kullanım sözleşmesini kabul etmeniz gerekmektedir.) Program açıldıktan sonra sağ üstteki üç noktaya tıklayın, ardından hesap ekle seçeneğine tıklayın.

Açılan sayfada gerekli bilgileri giriniz. Hesap adı olarak herhangi bir isim belirleyebilirsiniz. IP/Host olarak cihazın WAN Ip adresini ve port numarasını girin. Ardından oluşturduğumuz kullanıcı adı (örneğimizde "cemal") ve şifre bilgisini girerek bağlan düğmesine tıklayın.

Cihaza bağlandığınızda izleme ekranı görüntülenir. Burada web filtre kayıtlarını (hedef siteler ve kaynak adreslere göre) ve trafik kayıtlarının ayrıntısını görebilirsiniz.



Sol üstteki menüye tıklayarak diğer seçeneklere ulaşabilirsiniz.

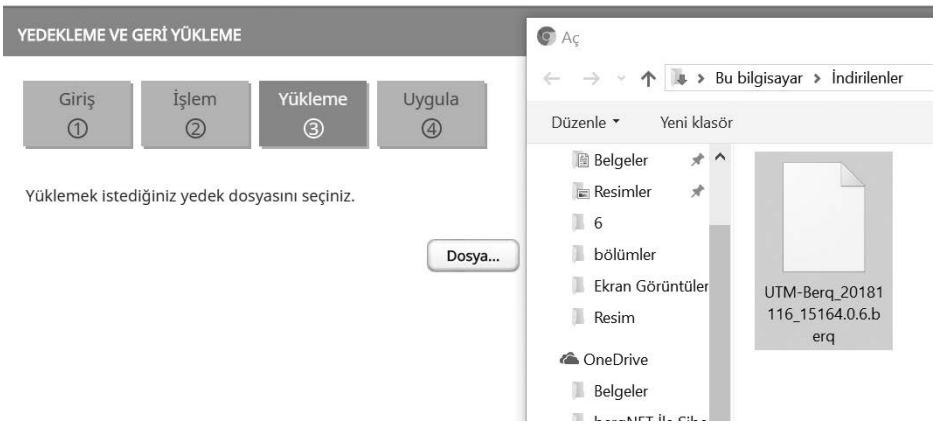


Mobil rapor uygulamasına istenen sayıda cihaz eklenebilmektedir. Çok sayıda cihaz eklendiğinde, sonradan mobil cihazın değiştirilmesi durumunda veya hesapların başka bir çalışana aktarımını kolaylaştırmak için, hesapların dışarıya aktarılması/içeriye alınması özelliği eklenmiştir.

6.5.4. Yedekleme ve Geri Yükleme

Sistem ayarlarındaki yedekleme ve geri yükleme seçeneği ile cihazın yapılandırmalarının yedeğini alma, yedeği yükleme ve yapılandırmaları sıfırlama işlemlerini gerçekleştirebilirsiniz.

Yedekleme seçeneği seçiliyken ileri, ardından uygula butonuna tıklayarak yedekleme dosyasını bilgisayarınızın indirilenler klasörüne indirebilirsiniz. İleride yapılandırmalarda bir sorun yaşarsanız veya cihazınızı değiştirmek zorunda kalırsanız tekrar yapılandırma ile uğraşmadan sistem geri yükleme seçeneği seçiliyken ileri düğmesine tıklayın. Ardından açılan sayfada yüklemek istediğiniz yedek dosyasını seçiniz. Bunun için dosya simgesine tıklayın ve açılan pencerede yedek dosyanızın bulunduğu dizine giderek seçin ve açın.



Sonrasında ileri ve uygula düğmelerine tıklayarak işlemi tamamlayın. Yedek dosyanın yüklenmesi yaklaşık 1 dakika sürecektir.

Bu bölümde son olarak yapılandırmaları (konfigürasyon) sıfırlayıp cihazı ilk aldığınız güne döndürebilirsiniz. Bunun için konfigürasyonları sıfırla seçeneği seçili iken ileri düğmesine tıklayın, ardından uygula tuşuna basın. Birkaç dakika sonra cihazdaki bütün yapılandırmalar silinecek ve cihaz yeniden başlatılacaktır.

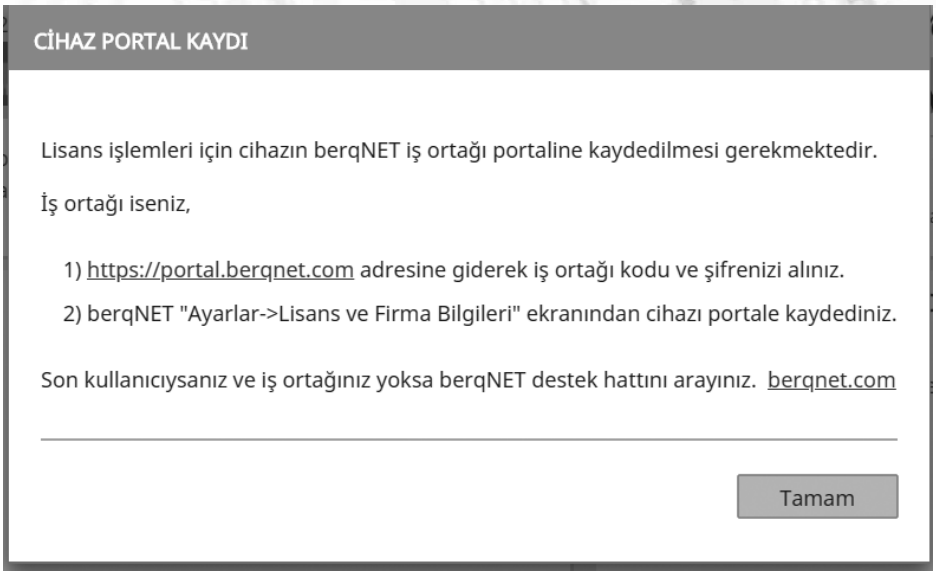
6.5.5. Saat ve Tarih

Bu bölümde cihazın saat ve tarih ayarlarını yapabilirsiniz. Bunun için saat ve tarih düğmesine tıklayın. Açılan pencerede ileri düğmesine tıklayarak devam edin. Açılan yeni pencerede saat dilimi seçimi yapabilirsiniz. Varsayılanda saat ve tarih bilgisi NTP (Network Time Protocol) aracılığıyla bir zaman sunucusundan otomatik olarak alınmaktadır. İsterseniz "Saat ve tarihi kendim belirlemek istiyorum" seçeneğine tıklayarak mevcut ayarları değiştirebilirsiniz. Zaman sunucusunu kullanmanız her zaman tavsiye edilen uygulamadır. İleri düğmesine tıklayarak mevcut zaman sunucusu adresini görebilir, isterseniz değiştirebilirsiniz.

Varsayılan ayarlarda (193.140.100.40) UlakNet NTP sunucusu kullanılmaktadır. 0.tr.pool.ntp.org veya time.google.com gibi başka bir NTP sunucusundan saat ve tarih bilgisini almak için yapılandırmayı değiştirebilirsiniz.

6.5.6. Lisans ve Firma Bilgileri

Bu bölümde cihazın lisans bilgilerini görüntüleyebilir ve cihazın iş ortağı portalına kaydını gerçekleştirebilirsiniz. Bu kaydı gerçekleştirmezseniz cihaza her giriş yaptığınızda aşağıdaki uyarıyı göreceksiniz.

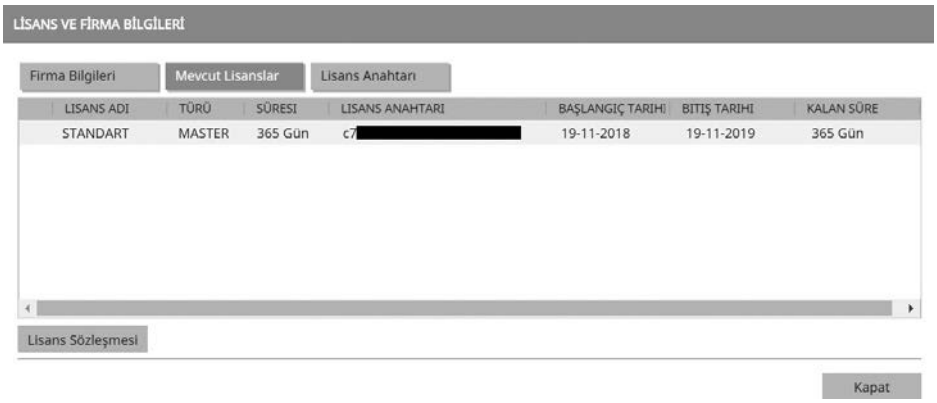


Öncelikle https://portal.berqnet.com adresine giderek firmanızın portala kaydını gerçekleştirin. Bu işlem öncesinde Berqnet iş ortağı olmalısınız. Bu kayıt sonucunda verdiğiniz e-mail adresine kayıt işlemi Berqnet tarafından onaylandıktan sonra iki tane şifre gönderilecektir. Birincisi portala giriş yaparken kullanacağınız şifre ikincisi de cihazı kayıt ederken kullanacağınız şifre.

Şimdi cihazın kayıt işlemini gerçekleştirelim. Bunun için firma bilgileri bölümündeki tüm bilgileri doldurup kaydet düğmesine tıklayınız.

Cihazınıza ait firma bilgileri başarı ile kaydedilmiştir şeklinde bir mesaj aldıysanız işlem tamamdır.

Şimdi mevcut lisanslar sekmesine tıklayarak cihazınızda geçerli lisansı görüntüleyebilirsiniz.



6.5.7. Dil Seçimi

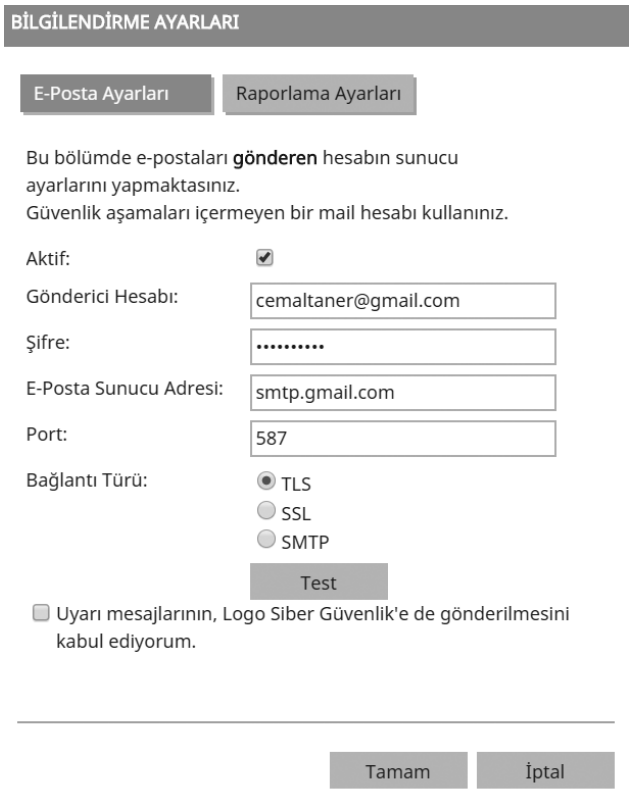
Bu bölümde cihazın arayüzünün dilini seçebilirsiniz. Varsayılan olarak Türkçedir. İsterseniz İngilizceye çevirebilirsiniz.

6.6. Servis Ayarları

Bu bölümde Berqnet'in sunduğu servislerin ayarlarının nasıl yapıldığını göreceğiz.

6.6.1. Bilgilendirme Ayarları

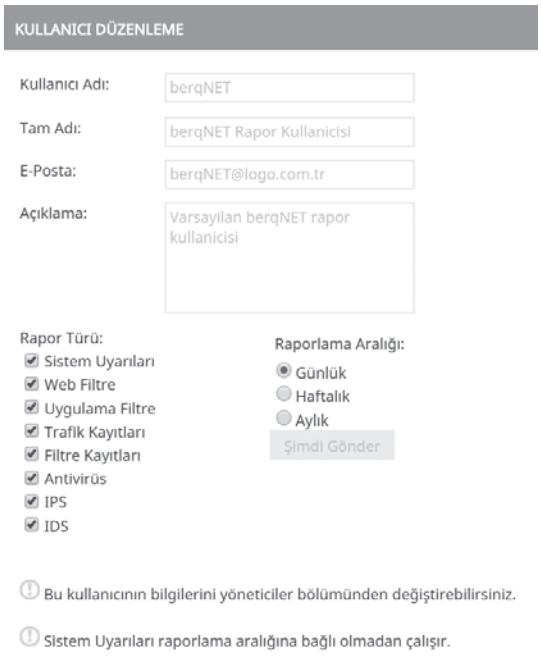
Burada cihaz tarafından üretilen rapor ve alarmların e-posta aracılığıyla gönderilmesini sağlayan ayarları gerçekleştiriyoruz. Bunun için bilgilendirme düğmesine tıkladıktan sonra açılan pencerede gönderen e-posta sunucu ayarlarını doğru bir şekilde girmemiz gerekiyor. Gerekli bilgileri girip tamam düğmesine tıklayınız. Uyarı mesajlarının, Logo Siber Güvenlik'e de gönderilmesini kabul ediyorum varsayılanda seçilidir, kabul etmiyorsanız onay kutusundaki seçimi iptal ediniz.



Eğer Gmail kullanıyorsanız cihazdaki ayarlardan sonra Gmail hesabınızda da yapmanız gereken ayarlar vardır. Bunun için;

1. Bilgisayarınızda Gmail'i açın.
2. Sağ üstteki Ayarlar simgesini tıklayın.
3. Ayarlar'ı tıklayın.
4. Yönlendirme ve POP/IMAP sekmesini tıklayın.
5. "POP İndirme" bölümünde, Tüm postalar için POP'u etkinleştir veya Şu andan itibaren gelen postalar için POP'u etkinleştir'i seçin.
6. Sayfanın alt tarafındaki Değişiklikleri Kaydet'i tıklayın.

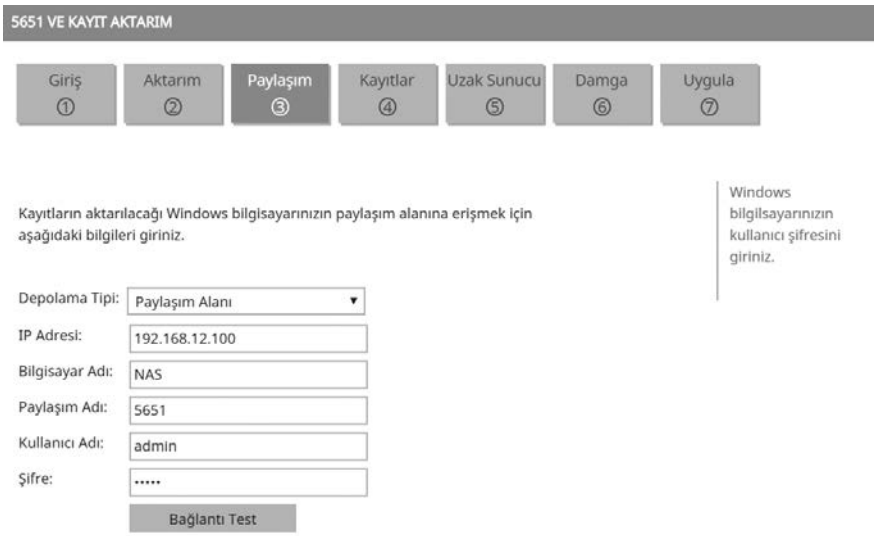
Raporlama ayarları sekmesinde ilgili kullanıcılar için raporlama ayarlarını gerçekleştirebilirsiniz. Bunun için kullanıcı seçili iken kalem simgesine tıklayın ve açılan pencerede rapor türlerini ve rapor aralığını belirleyerek kaydet düğmesine tıklayınız.



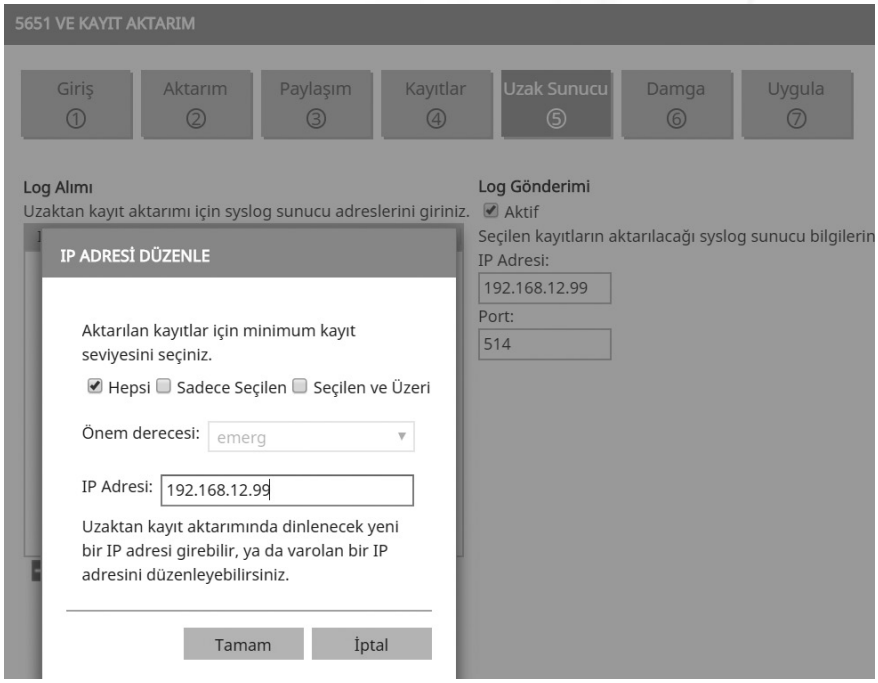
6.6.2. 5651 Kayıt Aktarım Ayarları

Berqnet'in üstünlüklerinden biri de 5651 sayılı kanuna uygun bir şekilde log tutabilmesidir. Birçok markada bu özellik bulunmazken Berqnet ile gelen varsayılan özelliklerden biridir. İşte tutulan bu log'ların nerede saklanacağı 5651 Kayıt aktarım ayarları bölümünden yapılır. Bunun için 5651 Kayıt aktarım ayarları düğmesine tıklayın. Açılan pencerede ileri düğmesine tıklayarak devam edin. Kayıt aktarım ayarını seçin seçeneğini açık duruma getirip ileri düğmesine tıklayın. Burada kayıtların

nerede saklanacağını belirleyeceksiniz. Depolama tipi olarak paylaşım alanı veya USB bellek seçebilirsiniz. Kayıtları ağınızda bulunan bir sunucu veya NAS cihazında saklamak için şekilde gördüğünüz gibi bir ayar yapmalısınız.



İleri düğmesine tıklamadan önce bağlantı test düğmesine tıklayarak sunucu veya NAS cihazına bağlanıp bağlanamadığınızı kontrol edin. Bir sonraki ekranda aktarılmasını istediğiniz kayıtları seçiniz. İleri düğmesine tıklayarak devam ediniz ve yeni gelen pencerede log alımı penceresinde ilgili ayarları yaparak log tutan ama bunu 5651'e uygun şekilde damgalayamayan bir sunucudan logları Berqnet'e aktarıp damgalayabilirsiniz. Yine log gönderimi kutucuğunu seçerek alınıp ve sonrasında damgalanan bu logları tekrar aynı sunucuya veya bir başka sunucuya gönderebilirsiniz.



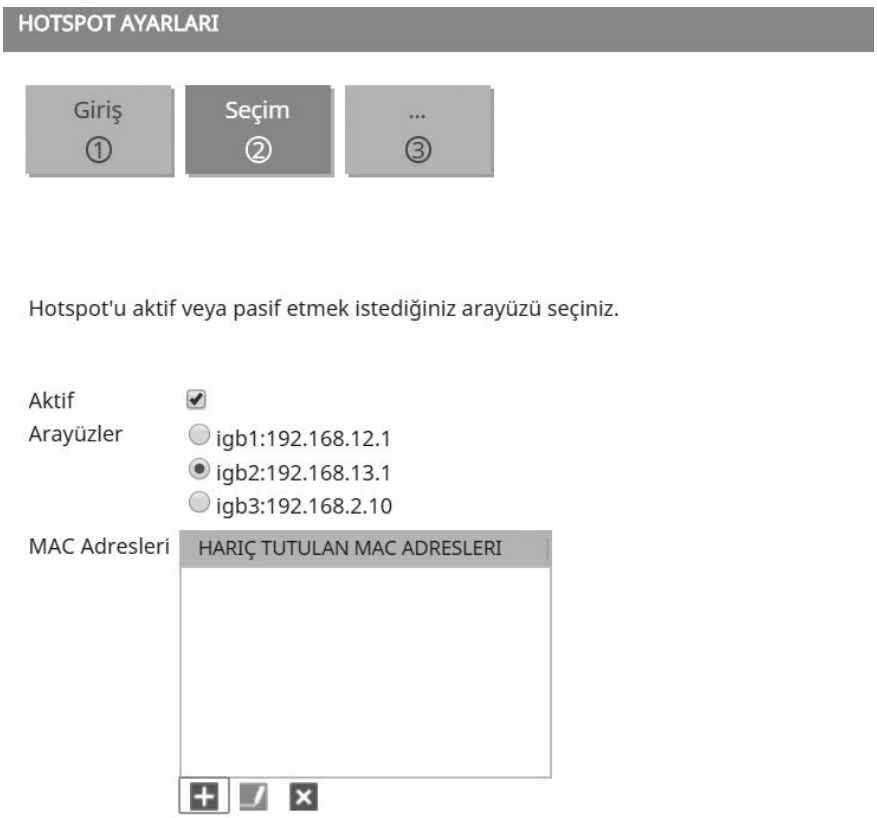
Bir sonraki ekranda ise zaman damgası için kullanılacak kullanıcı adı ve şifre bilgilerini giriniz. Zaman damgası hizmetini Tübitak (http://www.kamusm.gov.tr/urunler/zaman_damgasi) veya Türktrust gibi kurumlardan alabilirsiniz.

Son olarak Uygula düğmesine basarak, değişikliklerin güvenlik duvarınız üzerinde gerçekleşmesini sağlayınız. Böylece; Kayıt aktarım ayarları yapılacaktır, kayıt aktarımı her gece 23:59'de gerçekleşecektir, seçtiğiniz kayıtlar aktarılacaktır, uzak sunucu kayıt aktarımı ayarlanacaktır, zaman damgası ayarlanacaktır.

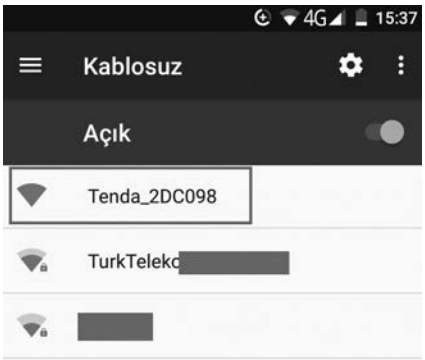
6.6.3. Hotspot Ayarları

Günümüzde kablosuz (wireless) olarak İnternet'e bağlanmak çok yaygın hale geldi. Özellikle otel, restoran, kafe gibi müşterilerine kablosuz internet hizmeti vermek isteyen yerler bunu güvenli bir şekilde yapmak ayrıca 5651 sayılı kanuna da uygun olarak bu hizmeti sunmak istiyorlarsa Berqnet, az önce gördüğümüz 5651 kayıt özelliğinin yanında hotspot özelliği ile de öne çıkıyor.

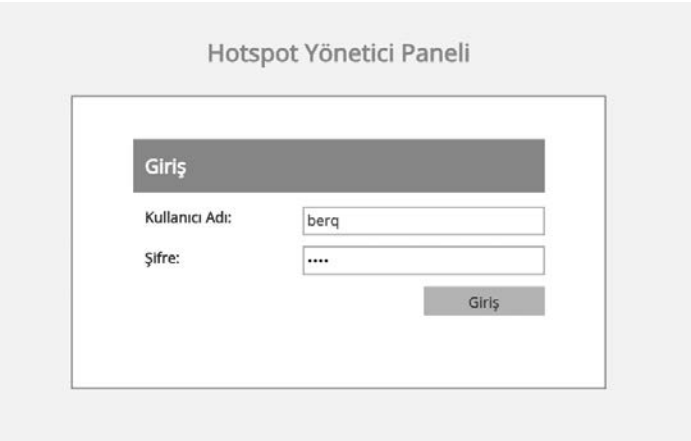
Hotspot ayarları için servis ayarları bölümündeki hotspot düğmesine tıklayın. İleri düğmesine tıklayın ve açılan pencerede hotspot özelliğini aktifleştirin. Burada ayrıca kablosuz erişim noktalarının (AP) hangi ağda olacağını ilgili arayüzü seçerek belirleyin.



Bu arayüzde daha önceden DHCP ayarlarını yapmış olmalısınız. Yine kullandığınız kablosuz erişim noktalarının (AP) DHCP sunucularını ve kablosuz ağ güvenliğini kapatmayı unutmayınız. Kullanıcılar ayarladığınız kablosuz ağı cep telefonlarında şekildeki gibi göreceklerdir. (Tenda_2DC098)

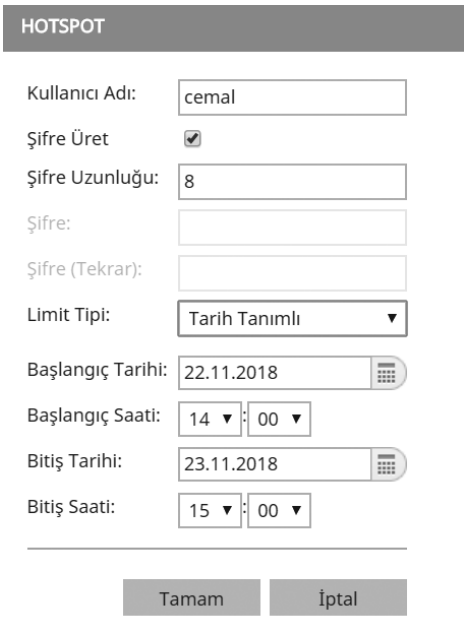


Sonrasında ileri düğmesine tıklayın. Açılan pencerede kullanıcıların hangi yöntemle kimliklerini doğrulayarak kablosuz ağınıza bağlanacağını seçebilirsiniz. İlk seçenek manuel yetkilendirmedir. Bu seçeneği seçtiğinizde kullanıcılar, sizin vereceğiniz kullanıcı adı ve parola ile kablosuz ağa bağlanacaktır. Bu seçenek restoran, kafe vb. yerlerde çok tavsiye edilmezken, kablosuz ağ kullanıcı sayısının az olduğu ve 5651 sayılı kanunun gereklilikleri yerine getirilmek istenirken tavsiye edilir. Kullanıcı oluşturma işlemini Hotspot yönetim paneli aracılığı ile gerçekleştiriyoruz. Panele Berqnet cihazına bağlanırken kullandığınız IP adresinin sonuna /hotspot yazarak ulaşabilirsiniz. Örneğin https://192.168.12.1/hotspot

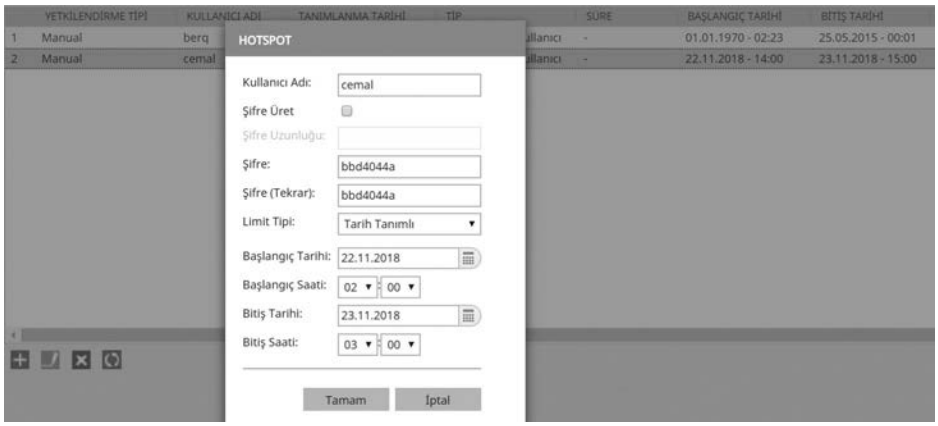


Panele giriş için varsayılan kullanıcı adı ve parola "berq"dir. İsterseniz ileri düğmesine tıklayarak yeni açılan pencerede panele giriş yapmak için kullanılacak varsayılan kullanıcı adı ve şifre bilgisini değiştirebilirsiniz.

https://192.168.12.1/hotspot adresinden panele giriş yaptıktan sonra manuel kullanıcılar sekmesine tıklayalım ve burada sol alttaki + simgesine tıklayarak yeni kullanıcı oluşturalım. Kullanıcı adı kısmına vermek istediğimiz kullanıcı adını yazıyoruz. Şifre üret ve şifre uzunluğu seçeneği ile belirttiğimiz uzunlukta otomatik şifre üretilmesini sağlayabiliriz. Şifre üret seçeneğini seçmez iseniz şifreyi sizin belirlemeniz gerekir. Limit tipi olarak tarih tanımlı veya süre tanımlı seçenekleri karşımıza çıkıyor. Tarih tanımlı ile kullanıcının kablosuz ağa bağlanabileceği başlangıç ve bitiş tarih ve saatlerini belirliyoruz. Süre tanımlı ile de kullanıcının kablosuz ağa bağlanabileceği tarihten bağımsız saat ve dakika bazında bir süre belirleyebiliyoruz.



Tamam düğmesine tıklayarak işlemi sonlandırın. Kullanıcıya otomatik olarak verilen şifreyi görmek için panel ana sayfasında oluşturduğunuz kullanıcıyı seçerek sol alttaki kalem simgesine tıklayın.



Şekilde cemal isimli kullanıcıya "bbd4044a" şifresinin verildiğini görüyoruz. Bundan sonra kullanıcı kablosuz ağa bağlanmak istediğinde karşısına çıkan şekildeki ekranda bu kullanıcı adı ve şifre ile bağlantı sağlayacaktır.

Kullanıcı adı ve şifreyi girince şekilde görüldüğü gibi başarıyla giriş yaptığını belirten bir ekran görüntülenecektir.

Hotspot panelinde ayrıca sms ile yetkilendirme, otel veri tabanı ile yetkilendirme veya TC kimlik no ile yetkilendirme yöntemleri ile bağlantı sağlamış kullanıcıları görüntüleyebilir, sol alttaki kırmızı çarpı (X) simgesine tıklayarak kullanıcıları silebiliriz.

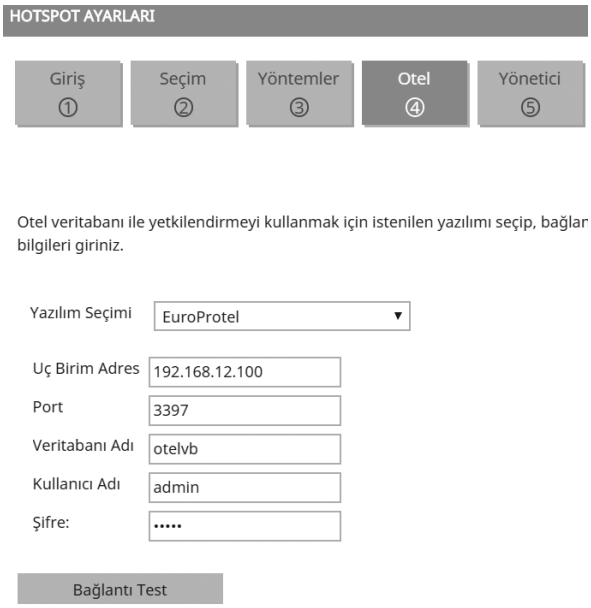
İkinci yetkilendirme yöntemi olan sms ile yetkilendirme seçeneğini seçip ileri düğmesine tıklarsanız sms sağlayıcı bilgilerini gireceğiniz ekran karşınıza gelir. Bu hizmet için iki firmadan ücret karşılığında sms satın alabilirsiniz. Örneğin Posta Güvercini (www.postaguvercini.com) firmasından hizmet aldınız. Firma tarafından size verilen kullanıcı adı ve şifre bilgilerini yazınız. Kullanıcılara gönderilecek şifrenin kaç karakter uzunluğunda olmasını istiyorsanız belirleyiniz. Bunun için 4-12 arasında bir değer girebilirsiniz. Örneğimizde 8 girdik yani sms ile gönderilecek şifre 8 rakamdan oluşacak.

Kullanıcılar kablosuz ağa bağlanmak istediklerinde aşağıdaki şekildeki gibi bir ekran gelecek ve burada cep numaralarını yazıp sms gönder düğmesine tıkladıklarında cep telefonlarına bir sms gelecektir.

Şekilde örnek bir sms görülmektedir. Kullanıcı adı olarak cep telefonu numarası, şifre olarak 8 rakamdan oluşan bir şifre gönderilmiştir.

SMS ile gelen bu bilgiler bir önceki ekrandaki kullanıcı adı şifre kısmına girilip giriş düğmesine tıklandığında yine başarıyla oturum açıldığı bildirilir.

Eğer hotspot uygulamasını bir otelde gerçekleştiriyorsanız otel veri tabanından kullanıcı bilgilerini alıp yetkilendirme yapabilirsiniz. Bunun için otel veri tabanı ile yetkilendirme seçeneğini seçip ileri düğmesine tıkladığınızda gelen ekranda kullanılan otel yönetim yazılımını seçin. Her yazılım için gelen seçenekler farklı olabilir. İlgili bilgileri doldurduktan sonra bağlantıyı test etmeyi unutmayın.



TC kimlik no ile yetkilendirmeyi seçerseniz, kullanıcılar kablosuz ağa bağlantı sağlamak için şekildeki hotspot kullanıcı panelinde ad, soyad, TC no ve yıl olarak doğum tarihi bilgilerini girerek kimlik doğrulama yapabilirler.

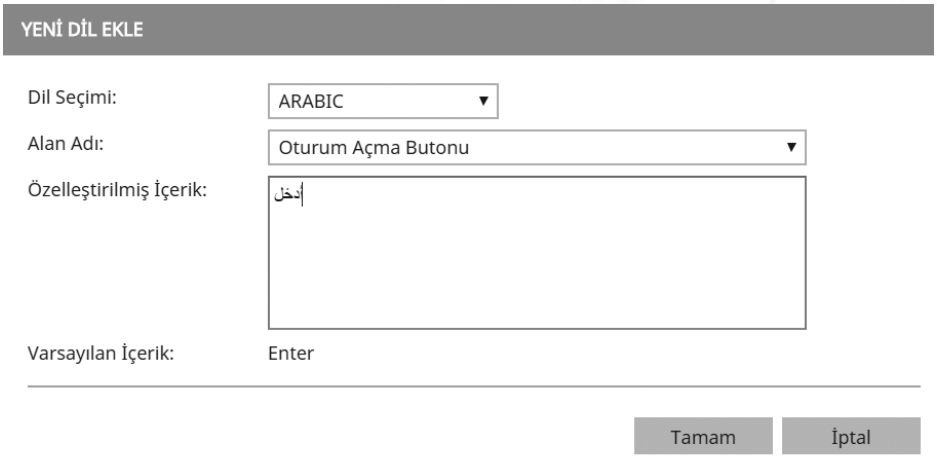
Şimdi kimlik doğrulama seçeneklerinden sonra ileri butonuna tıkladığımızda yapabileceğimiz hotspot ayarlarına bakalım. Daha önce de bahsetmiştik, öncelikle karşımıza hotspot yönetim paneline girişte kullanacağımız kullanıcı adı şifre belirleme akranı gelir. Burada varsayılan değerler "berq" ve "berq" idi. İleri düğmesine tıklayın. Burada oturum ayarlarını gerçekleştirebiliyoruz. İlk seçeneği seçip limit belirlerseniz aynı kullanıcı adı ile aynı anda açılabilecek oturum sayısını sınırlayabiliriz. 1 tavsiye edilen değerdir. Bir sonraki seçenekte bağlantının sona ereceği süreyi belirleyebilirsiniz. Varsayılanda bu değer iki saattir. Yani kullanıcı kablosuz ağa hotspot üzerinden bağlandıktan 2 saat sonra bağlantısı kesilir. Tekrar kimlik doğrulama yapması gerekir. İsterseniz bu süreyi arttırabilirsiniz. Bir sonraki seçenekte kullanıcının kendi isteğiyle bağlantıyı sonlandırmasına izin verebilirsiniz. Son olarak bağlantı başarılı olunca kullanıcıyı şirket sayfanıza yönlendirebilirsiniz.

Bir sonraki ekranda hotspot kullanıcı panelinde özelleştirmeler yapabiliriz.

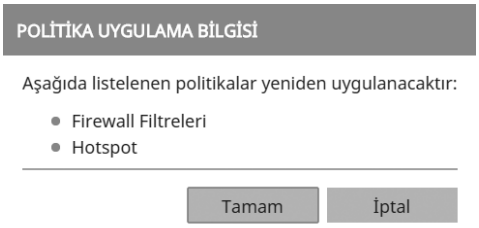
Burada arka plan sekmesine gelip Özelleştirilmiş seçeneğini seçip, sayfa rengi, başlık rengi, iç Panel rengi ve dış panel renklerinde istediğiniz değişiklikleri yapabilirsiniz.

Müşteri logosu sekmesindeki özelleştirme ile ücretsiz kablosuz internet hizmeti sunan firmanın logosunun panel ana sayfasında görünmesini sağlayabiliriz.

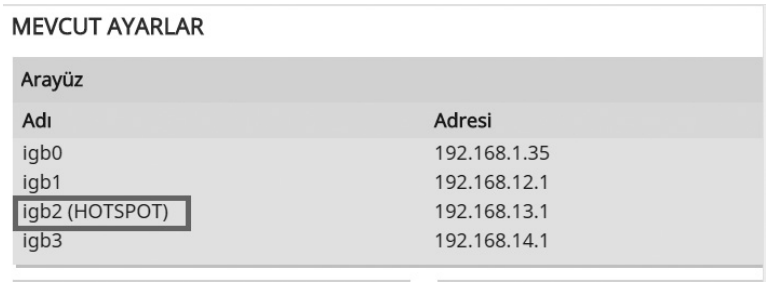
Arayüz içerik sekmesinde ise panelde desteklenen mevcut dillere (Türkçe, İngilizce, Almanca, Rusça) yeni diller ekleyebilirsiniz. Bunun için paneldeki her menü ve açıklamanın o dildeki karşılığını girmeniz gerekir. Bunun için önce özelleştirilmiş seçeneğini seçip sonra ekle düğmesine tıklayın ve açılan pencerede eklemek istediğiniz dili seçerek her bir alan adı için varsayılan içeriğin o dildeki karşılığını girin.



Bu düzenlemeler bittikten sonra ileri düğmesine tıklayın, ardından uygula düğmesine tıklayarak hostpot ayarlarının gerçekleşmesini sağlayın. Son düğmesine tıklayarak ilgili pencereyi kapatın. Son olarak en üst sağdaki uygula düğmesine tıklamayı unutmayın. Bu düğmeye tıklayınca şekildekine benzer bir uyarı alacaksanız.

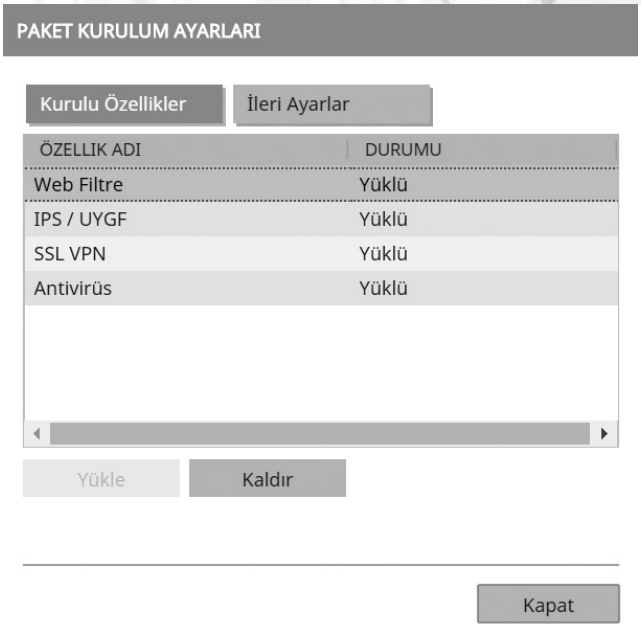


Tamam düğmesine tıklayın. "Politikanız başarıyla uygulandı" mesajını **mutlaka** görmelisiniz. Artık ayarlar ekranın sağ üstünde bulunan mevcut ayarlar bölümünde hotspot arayüzünü görebilirsiniz.



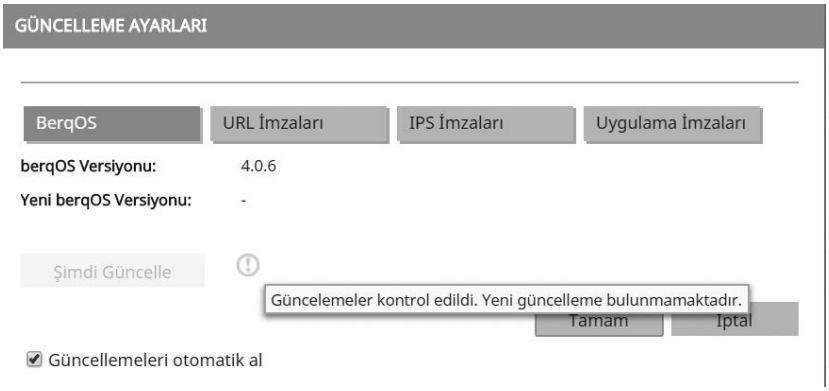
6.6.4. Paket Kurulumu

Bu bölümde Berqnet cihazında yüklü paketleri görebilir, yeni paketler ekleyebilir ya da mevcut paketlerden istediğinizi kaldırabilirsiniz.



6.6.5. Güncelleme

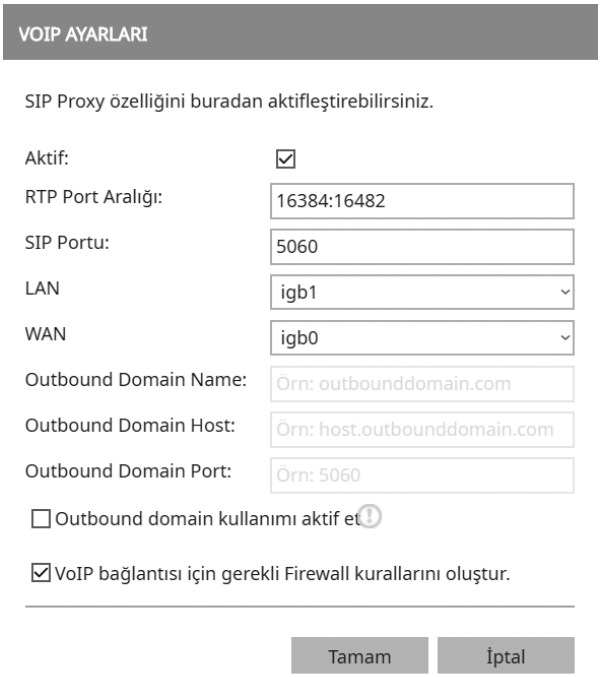
Bu bölümde cihazın işletim sisteminin (BerqOS), URL imzaları, IPS imzaları ve uygulama imzalarının güncellenmesi gerçekleştirilir. Eğer güncellemeleri otomatik al seçeneği seçilmiş ise güncellemeler otomatik olarak indirilip uygulanır.



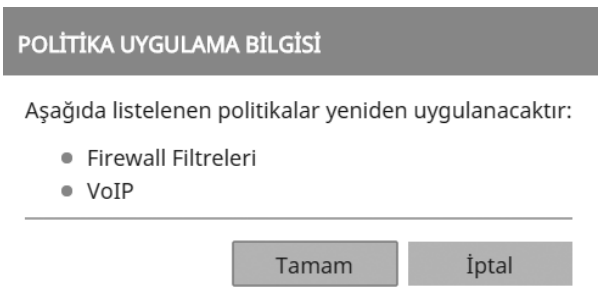
Güncellemeleri otomatik al seçeneği seçili değilse şimdi güncelle düğmesine tıklayarak güncellemeleri indirip uygulayabilirsiniz. Topolojinin büyüklüğü ve ihtiyaçlara göre hangisinin seçileceğine ağ yöneticisi karar vermelidir.

6.6.6. VoIP

Eğer işletmenizde bir IP telefon yapısı varsa gerekli SIP Proxy yapılandırmaları bu bölümde gerçekleştirilir.



Öncelikle aktif seçeneğini seçin, ardından kullanılan RTP port aralığını tanımlayın. Kullandığınız SIP portunu yazarak LAN ve WAN arayüzlerini seçin. (Varsayılanda WAN portu bellidir, IP telefonların bulunduğu ağ hangi arayüze bağlı ise LAN olarak bu arayüzü seçi.) Son olarak VoIP bağlantısı için gerekli firewall kurallarını oluştur seçeneğini seçerek tamam düğmesine tıklayın. Sağ üstteki uygula düğmesine tıklamayı sakın unutmayın.

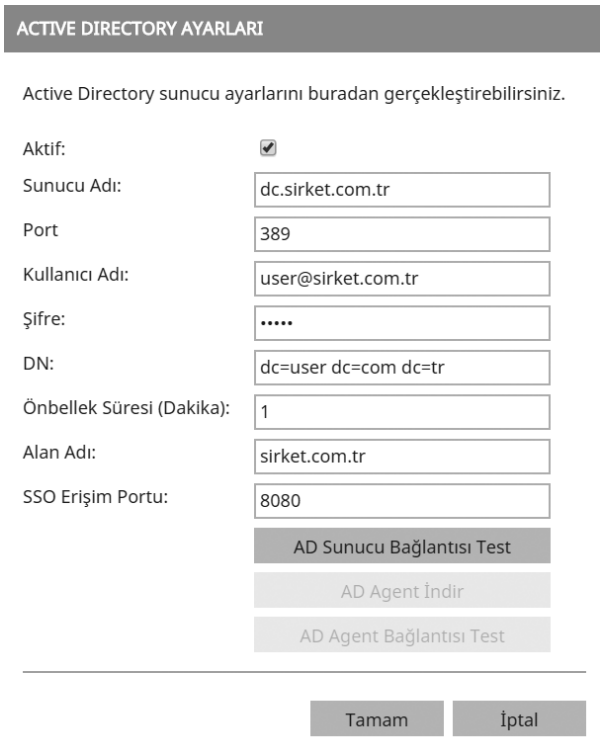


Politikanız başarıyla uygulandı mesajını alıyor olmalısınız.

6.6.7. Active Directory Ayarları

Bu bölümde active directory ayarlarını yaparak ileride göreceğimiz Web filtre vb. ayarlarını active directory aracılığı ile çekeceğimiz kullanıcılara rahatlıkla uygulayabileceğiz.

Bunun için Active Directory ayarları düğmesine tıklayın ve açılan pencerede AD sunucunuzun bilgilerini girin.



AD Sunucu Bağlantısı Test düğmesine tıklayarak ayarları doğrulayın. Bağlantı başarılı olunca AD Agent İndir düğmesine tıklayarak indirdiğiniz agent'i AD sunucunuza kurun. Son olarak AD Agent Bağlantısı test düğmesine tıklayarak agent bağlantısını doğrulayın. Tamam düğmesine tıklayarak pencereyi kapatabilirsiniz.

6.7. Güvenlik Ayarları

6.7.1. Firewall Ayarları

Berqnet'in en temel özelliklerinden biri firewall yani güvenlik duvarı olarak çalışmasıdır. Firewall özelliği varsayılanda etkin olarak gelir. Yine varsayılan kural olarak herhangi bir kaynaktan gelip herhangi bir hedefe giden bütün trafiğe izin verilmiştir. Yani içeriden dışarıya veya dışarıdan içeriye tüm trafik geçer. Ayrıca kayıtlar ekranında ilgili kayıtları görebilmemiz için kayıt seçeneği de varsayılanda aktiftir.

Fakat firewall sekmesindeki ayarlara gelmeden önce güvenlik ayarları bölümündeki firewall ayarlarına bakalım.

Web arayüz portunu değiştir seçeneği ile cihaza IP adresi ile uzaktan erişirken kullandığımız portu değiştirebiliriz. Varsayılanda 443 numaralı port kullanılmaktadır. İsterseniz 777 veya 999 numaralı portları kullanabilirsiniz. Örneğin 777 yapar iseniz bundan sonra cihaza https://192.168.12.1:777 adresinden ulaşacaksınız.

SSH portunu değiştir seçeneği ile SSH bağlantısı için kullanılan varsayılan 22 numaralı portu değiştirebilirsiniz.

Sistem son kuralı olan "her şeyi düşür" için kayıt tutsun seçeneği ile firewalldaki herhangi bir kurala takılmayan yani eşleşmeyen (match) trafiğin bu son kural ile düşürülmesini sağlıyoruz. Bu ayarı bu şekilde bırakmanız tavsiye edilir.

Engelleyen kural olsa da web arayüzüne erişime izin ver seçeneği ile belirttiğiniz bir IP adresinden veya subnetten gelen trafiği engelleyen bir firewall kural olmasına rağmen web arayüzüne erişime izin vermek istiyorsanız seçili olmalıdır.

Port yönlendirme kuralları için gerekli Firewall kurallarını oluştur seçeneği ile port yönlendirme (NAT-PAT) yapılandırması gerçekleştirdiğimizde ilgili kurallar için gerekli firewall kurallarının oluşturulmasını sağlıyoruz.

DHCP Relay servisi için gerekli Firewall kurallarını oluştur seçeneği ile eğer DHCP Relay agent yapılandırması yapmışsanız bu yapılandırma için firewall kurallarının oluşturulmasını sağlarsınız.

Broadcast paketlerini düşür ve kayıt tutma seçeneği ile broadcast paketler düşürülür. Bildiğiniz üzere normalde bir broadcast trafik router veya firewall tarafından diğer ağlara iletilmez.

Güvenlik duvarının DNS sorguları için filtre kuralı oluştur seçeneği ile DNS sorguları için firewall kuralları otomatik oluşturulur.

FTP proxy aktif et ve gerekli filtre kuralını oluştur seçeneği ile FTP Proxy aktif edilir ve gerekli filtre kuralı firewall ayarlarında otomatik oluşturulmuş olur.

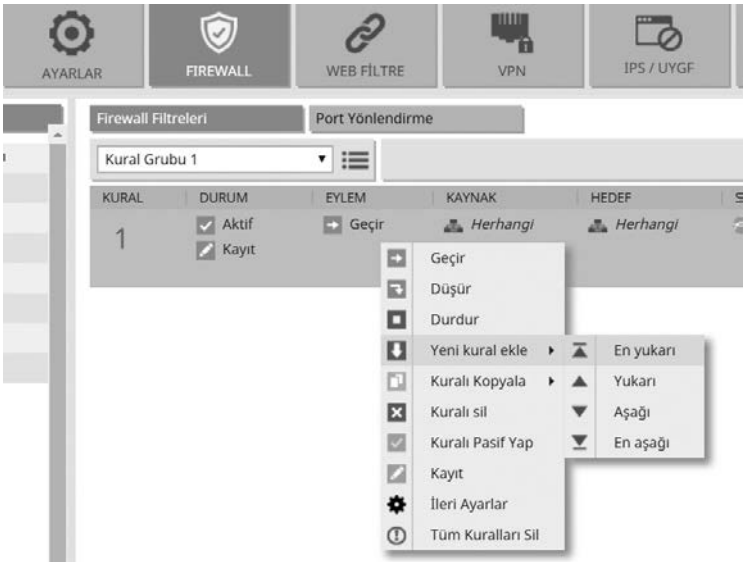
Parçalanmış ISAKMP/IKE trafiği için gerekli Firewall kurallarını oluştur seçeneği varsayılanda etkin değildir, gerekliyse etkinleştirebilirsiniz.

Hotspot ağlarından Web arayüzüne erişime izin ver seçeneği ile hotspot üzerinden bağlanan kullanıcıların web arayüzüne bağlanmasına izin verebilirsiniz.

Berqnet teknik desteğinin yardımına izin ver seçeneği ile Berqnet teknik desteğinin uzaktan cihazınıza bağlanıp sorunları gidermesini sağlayabilirsiniz.

Şimdi Firewall sekmesine geri dönelim ve örnek bazı senaryolar ile firewall yapılandırmasını öğrenelim. Bu yapılandırmaları Firewall filtreleri sekmesinde yapmanız gerektiğini unutmayın.

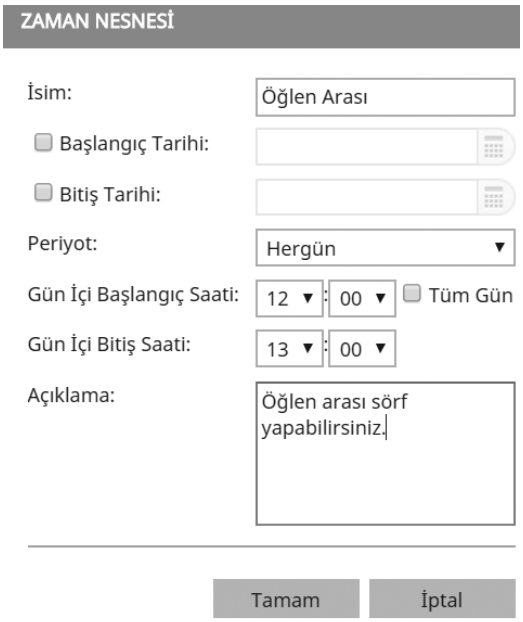
Daha önce de bahsetmiştik varsayılan olarak herhangi bir kaynaktan gelip herhangi bir hedefe giden bütün trafiğe izin verilmiştir. Şimdi mevcut kuralın üstünde sağ tıklayarak yeni kural ekle/en yukarı seçeneğini seçiyoruz.



Aynı şekilde bir kural daha ekliyoruz. Çünkü eklediğimiz kuralın iki durumu olacak. Kuralları ekledikten sonra kayıt tutmasını da aktif hale getirmek için kayıt seçeneğine çift tıklayıp yeşil yapıyoruz. Daha sonra eklediğimiz 1. Kuralın eylem kısmına gelip sağ tıklayıp geçir seçeneğini seçiyoruz. 2. Kuralın eylem seçeneği düşür olarak kalsın.

Senaryomuz şöyle olacak; belirli bir saatte, belirli bir IP aralığına veya belirli bir IP adresindeki host'a tüm servisleri kullanma iznini sadece bazı saatlerde vereceğiz. Örneğin sadece öğlen arasında İnternet bağlantısı olacak ve onun dışındaki saatlerde cihaz çevrimdışı çalışacak, çalışanın mesai saatlerinde kullandığı yazılımların hiçbir şekilde İnternet bağlantısına ihtiyaç yok. Öğlen arasında da biraz İnternette sörf yapsın.

Öncelikle limit nesneleri kısmına gelip sağ tıklayın ve yeni bir zaman nesnesi oluşturun. Zaman nesnesine bir isim verin, gün içi başlangıç ve bitiş saatlerini girin ve tamam düğmesine tıklayın.



Daha sonra ağ nesneleri kısmına gelip bir ağ nesnesi oluşturun. Sağ tıklayıp ekleyi seçin, açılan pencerede ağ nesnesine bir isim verin. Tür olarak uç birimi seçin. Uç birim (host) IP adresini girin ve tamam düğmesine tıklayın.

Şimdi oluşturduğumuz Cevimdisi_User isimli ağ nesnesini sürükle bırak (drag&drop) yöntemiyle 1. ve 2. Kuralın kaynak kısmına bırakıyoruz. Daha sonra öğlen arası ismini verdiğimiz zaman nesnesini de sürükleyip 1. Kuralın limit kısmına bırakıyoruz.

KURAL	DURUM	EYLEM	KAYNAK	HEDEF	SERVİS	LİMİT	GİRİŞ ARAYÜZÜ	İLERİ AYARLAR
1	Aktif Kayıt	Geçir	Cevrimdisi_User	*Herhangi*	*Herhangi*	Öğlen Arası	Güvenlik Duvarı	Ağ Geçidi: Herhangi
2	Aktif Kayıt	Düşür	Cevrimdisi_User	*Herhangi*	*Herhangi*	*Her Zaman*	Güvenlik Duvarı	Ağ Geçidi: Herhangi
3	Aktif Kayıt	Geçir	*Herhangi*	*Herhangi*	*Herhangi*	*Her Zaman*	Güvenlik Duvarı	Ağ Geçidi: Herhangi

Firewall'larda kurallar yukarıdan aşağıya satır satır çalışır. Yani burada düşür eylemini içeren kuralı yukarıya koysaydık 192.168.12.46 IP adresinden gelen trafik ilk satırla eşleşeceği ve 2. kurala bakılmayacağı için her zaman düşürülecekti. Şimdi kuralın çalışmasına bakalım; Saat 10.30'da İnternete bağlanmak isteyen bu kullanıcıdan yani 192.168.12.46'dan Berqnet'e gelen trafik için 1. Kurala bakılacak; eylem geçir ama ne zaman öğlen arasında, o zaman 1. Kural ile eşleşme olmadığı için ikinci satıra geçilecek, 2. Kurala bakınca her zaman trafiği düşür dediği için trafik düşürülecek. Kullanıcı saat 12:10'da İnternete bağlanmak istesin. 192.168.12.46'dan Berqnet'e gelen trafik için yine 1. Kurala başvurulacak, zaman limiti olarak 12-13 arası ve eylem olarak geçir dendiği için trafiğin geçmesine izin verilecek ve alttaki satırlara bakılmayacak bile. Herhangi bir host'tan herhangi bir zamanda gelen trafik 1. ve 2. Kural ile eşleşmeyecek ve 3. satıra bakacak. 3. Kural herhangi bir kaynaktan herhangi bir hedefe giden (any any) trafiğe her zaman izin ver olduğu için trafik geçecek.

Kuralları oluşturma işiniz bitince en üst sağdaki uygula düğmesine tıklamayı ve politikanız başarıyla uygulandı mesajını görmeyi unutmayınız.

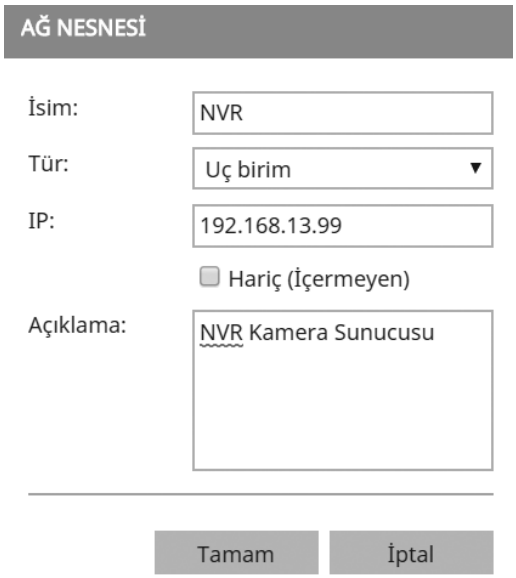
6.7.1.1. Port Yönlendirme

Eğer ağımızın içinde sunucu, kamera kayıt cihazı (DVR-NVR) vb. gibi ağın dışından erişilmesi gereken cihazlar varsa bu bölümden port yönlendirme ayarlarını yapmamız gerekir. Örneğimizde TCP 9000 port'undan ulaşılan ve IP adresi 192.168.13.99 olan bir DVR cihazı olsun. Bunun için öncelikle Firewall ayarlarında port yönlendirme sekmesine geçin.

Öncelikle mevcut kural üstünde sağ tıklayarak yeni kural ekle/aşağı seçeneğini seçin. Böylelikle 2. Kural eklenmiş oldu.

KURAL	DURUM	KAYNAK ADRES	GELEN SERVİS	GELİŞ ARAYÜZÜ	İLETİLEN SUNUCU	İLETİLEN SERVİS	AÇIKLAMA
1	Pasif Kayıt	*Herhangi*	HTTP	igb0	WebSunucu	HTTP	Dış ağdan iç web sunucusuna yönlendi
2	Aktif Kayıt	*Herhangi*	*Herhangi*	Güvenlik Duvarı	*Tanımlayınız*	*Herhangi*	

Sonra Ağ nesneleri kısmına gelip sağ tıklayın ve ardından ekle seçeneğine tıklayarak ağ nesnesi penceresini açın. İsim bölümüne NVR yazın ve tür olarak uç birim (host) seçin. IP adresi olarak 192.168.13.99 yazın. Açıklama kısmına istediğiniz bir açıklamayı yazıp tamam düğmesine tıklayın.



Daha sonra ağ servisleri kısmına gelin. Sağ tıklayıp ekle seçeneğini seçin. İsim olarak NVR Port yazın. Tür TCP seçiliyken hedef port kısmına 9000 yazın. İsterseniz bir açıklama ekleyin ve tamam düğmesine tıklayarak pencereyi kapatın.

Şimdi oluşturduğunuz NVR Port isimli servis nesnesini sürükleyip hem gelen servis hem de giden servis alanlarına bırakın. Oluşturduğunuz NVR isimli ağ nesnesini de sürükleyip iletilen sunucu alanına bırakın. Geliş arayüzü kısmındaki güvenlik duvarı simgesine çift tıklayarak açın ve geliş arayüzünü seçin.

Eğer etkin değilse durum kısmını çift tıklayarak aktif etmeyi ve kayıt tutulmasını istiyorsanız yine çift tıklayarak etkinleştirmeyi unutmayın. Açıklama kısmına çift tıklayarak kural hakkında bir açıklama yazabilirsiniz.

Her zaman olduğu gibi işiniz bitince en üst sağdaki uygula düğmesine tıklamayı ve politikanız başarıyla uygulandı mesajını görmeyi unutmayınız.

Yalnız şöyle bir uyarıda bulunmak istiyoruz, siber saldırıların çok fazla yaşandığı günümüzde port yönlendirme güvenlik zaafiyetlerine sebep olduğu için tavsiye edilmemektedir. Bunun yerine ileride anlatacağımız VPN ile güvenli bir şekilde uzak ağa bağlanıp yerel ağ içinde bir host gibi istediğimiz sunucuya ulaşmayı tercih etmelisiniz.

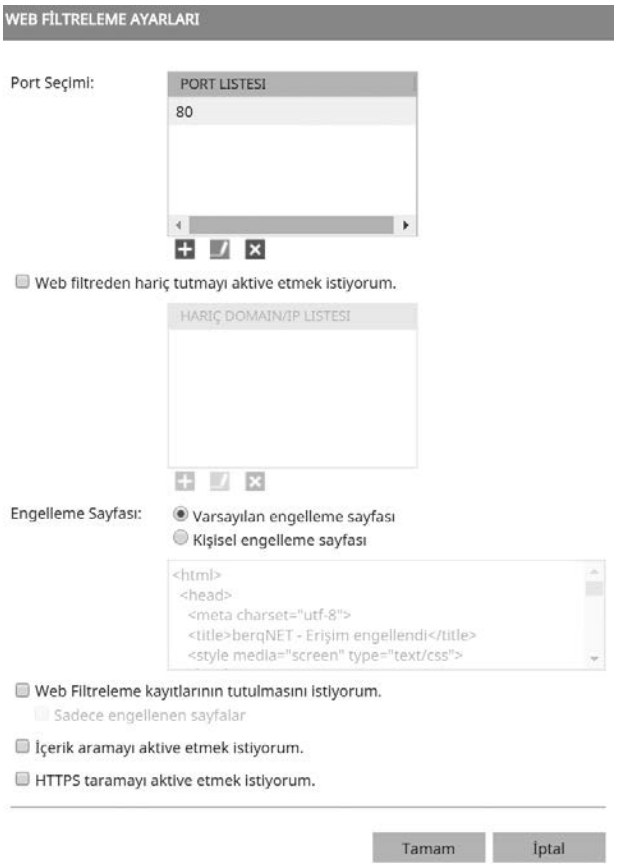
6.7.2. Web Filtre Ayarları

Çalışan Hayatı Araştırması'na göre, Türkiye'de çalışanların %54'ü sosyal medyaya mesai saatleri içinde 30 dakikadan fazla zaman ayırıyor. Yani 10 kişilik bir ekibiniz varsa her gün 5 saat sosyal medyada geçiyor demektir. İşte işletmenizin verimliliğini arttırmak için Berqnet'in web filtreleme özelliği harika bir seçenek.

Tabii tamamen yasaklamak mutsuz çalışanlar oluşturabileceği için Berqnet'in gelişmiş web filtreleme özellikleri bize birçok seçenek sunuyor. Örnek senaryomuzda çalışanların tümünün sosyal medya sitelerine Youtube dahil olmak üzere girmeleri-

ni yasaklamak, sadece öğlen aralarında bu yasağı kaldırmak istiyoruz. Firewall kurallarında olduğu gibi burada da kural sıralamasının önemli olduğunu unutmayın. Yani bir kullanıcıya 1. Kuralla izin verip 2. Kuralda da o kullanıcının olduğu grubu yasakladığınızda kullanıcı yasağa tâbi olmayacaktır. Ya da senaryomuza göre 1. Kuralda yasakladıktan sonra 2. Kuralda öğlen arası izin vermek bir işe yaramaz. Çünkü trafik hep 1. Kurala takılacağı için 2. Kurala geçmez bile.

Öncelikle ayarlar/güvenlik ayarları/web filtre ayarlarına gelin. Burada varsayılan değerlerde gerekli değişiklikleri yapabilirsiniz.



Varsayılan olarak 80 numaralı web port'u dinlenmektedir. Mavi artı (+) simgesine tıklayarak yeni port numaraları ekleyebilirsiniz. Bazı web sitelerini filtreden hariç tutmak isterseniz Web filtreden hariç tutmayı aktive etmek istiyorum seçeneğine onay koyup görünür hale gelen hariç/domain IP listesi ekranında mavi artı (+) simgesine tıklayarak alan adlarını veya IP adreslerini yazabilirsiniz. Filtreye takılan bir adrese giden kullanıcılara gösterilecek web sayfasında değişiklik yapmak isterseniz kişisel engelleme sayfasını seçip gerekli değişiklikleri yapın. Web filtreleme kayıt-

larının tutulmasını ve ana sayfadaki izleme ekranında kayıtların görünmesini istiyorsanız Web Filtreleme kayıtlarının tutulmasını istiyorum seçeneğini işaretleyin. İçerik aramayı aktive etmek istiyorum seçeneği ile yasaklamak istediğiniz kelime veya kelimeler o web sitesinde geçiyorsa filtreye takılsın diyebilirsiniz.

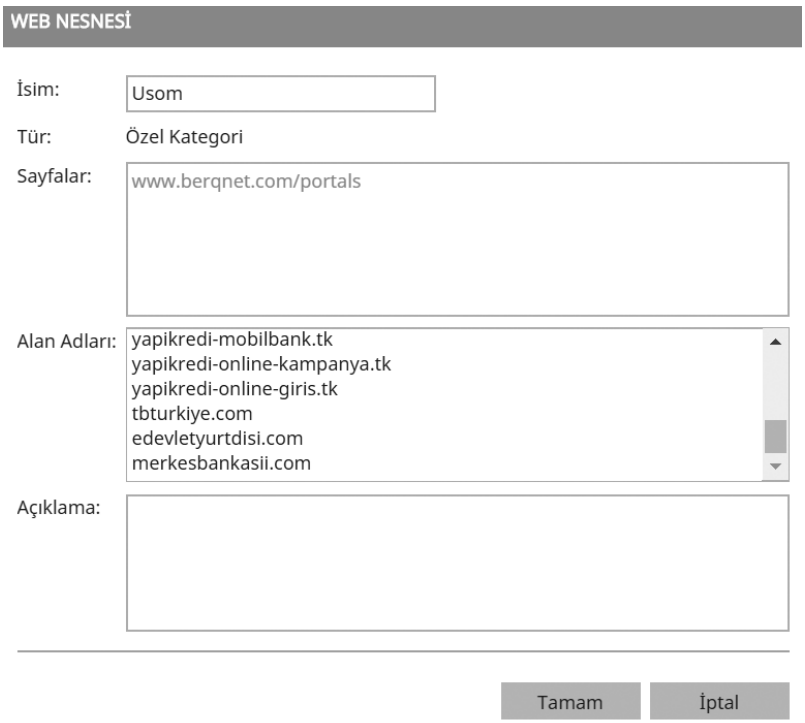
HTTPS taramayı aktive etmek istiyorum seçeneğini işaretleyerek yasaklanan sitenin kelime bazlı engelleme kurallarının ve medya formatlarının engellenmesi sağlanabilir. HTTPS Taramayı aktif etmek istiyorum seçeneği pasif olsa da https sitelerin alan adı şeklinde engellenebilmesi ve https loglaması mümkündür.

Şimdi senaryomuza gelelim. Öncelikle ana sayfada web filtre sekmesine geçin. Web filtreleme özelliği varsayılan olarak pasiftir. Aktifleştirmek için pasif simgesine çift tıklayın ve aktif durumuna çevirin. Sonra sağ tıklayın ve en aşağı kural ekle seçeneğini seçin. Kural 2'nin eklenmiş olduğunu görmelisiniz. Öncelikle öğlen izin kuralını oluşturalım. Limit nesneleri bölümüne gelin ve sağ tıklayın. Burada zaman seçeneğini seçin ve yeni bir nesne oluşturun. Nesne ismi olarak öğlen arası verin. Başlangıç ve bitiş saatlerini işletmenin öğlen arası saatlerine göre belirleyin ve tamam düğmesine tıklayın.

Öğlen arası seçeneğini sürükleyip 1. Kuralın limit kısmına bırakın. Sonra URL kategorileri kısmına gelip sosyal medya nesnesini sürükleyip 2. Kuralın engelleme listesi kısmına bırakın. Ardından web nesneleri kısmından Youtube nesnesini sürükleyip 2. Kuralın engelleme listesi kısmında sosyal medya nesnesi altına bırakın.

Her zaman olduğu gibi işiniz bitince en üst sağdaki uygula düğmesine tıklamayı ve politikanız başarıyla uygulandı mesajını görmeyi unutmayınız.

Bugün en çok yapılan siber saldırıların başında phishing saldırısı gelmektedir. Çalışanların bu siteleri ziyaret etmesini USOM (https://www.usom.gov.tr/url-list.txt) tarafından yayınlanan zararlı bağlantılar listesindeki siteleri oluşturacağınız bir web nesnesi ile sağlayabilirsiniz. Web nesneleri kısmında sağ tıklayın ekle seçeneğine tıklayın yeni açılan pencerede nesneye isim verin ve tür olarak özel kategori seçeneğini seçin. USOM sitesinden kopyaladığınız web adreslerini alan adları kısmına yapıştırın ve tamam düğmesine tıklayın.



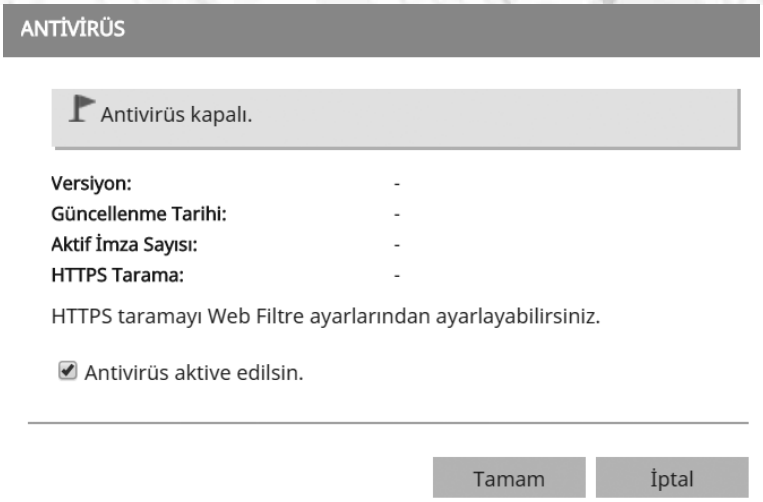
Şimdi bu nesneyi 1. ve 2. Kuraldaki engelleme listesi kısmına sürükleyip bırakın.

Bir kullanıcı bu sahtecilik sitelerinden birini ziyaret etmek istediğinde engellenecektir.

6.7.3. Antivirüs Ayarları

Berqnet'in özelliklerinden biri de antivirüs gateway olarak çalışmasıdır. Yani ağınıza giren bütün trafik tümleşik antivirüs tarafından denetlenir. Yalnız yapılandırmaya geçmeden önce gateway antivirüs ile endpoint antivirüs arasındaki farklara değinelim. Berqnet üzerindeki antivirüs motoru gateway antivirüse örnektir. Her ne kadar geçen tüm trafik denetlenecek olsa da şifrelenmiş ve VPN üzerinden gelen trafik tam olarak denetlenemeyebilir. Bu nedenle ağınızdaki tüm bilgisayar ve sunuculara endpoint antivirüs denen bir antivirüs yazılımı kurmanız tavsiye edilir. Antivirüs yazılımı olarak Windows 10 ile gelen Windows Defender'i kullanabileceğiniz gibi, Eset, Kaspersky, Trend Micro veya Bitdefender gibi markalardan birini de tercih edebilirsiniz.

Gateway antivirüs özelliğini etkinleştirmek için ayarlar sekmesinde güvenlik ayarlarından antivirüs simgesine tıklayın. Antivirüs aktive edilsin seçeneğine onay koyun ve tamam düğmesine tıklayın.



Sonrasında "*Antivirüs ayarlarınız uygulanmıştır. Antivirüs servislerinin başlaması imza veritabanınızın yüklenmesine bağlı olarak 5-10 dakika alabilir. Güvenlik politikanızı yeniden uygulayınız*" şeklinde bir uyarı almalısınız. Bunun için her zaman olduğu gibi sağ üstteki uygula düğmesine tıklamayı unutmayınız.

6.8. VPN Ayarları

Günümüzde işletmeler ve organizasyonlar, Internet veya extranet gibi üçüncü taraf ağlar üzerinden uçtan uca özel ağ bağlantısı oluşturmak için VPN (Virtual Private Network-Sanal Özel Ağ) kullanırlar. Tünel, mesafe engelini ortadan kaldırır ve uzak kullanıcıların merkezi site ağ kaynaklarına erişmesini sağlar. VPN, genellikle internet gibi genel bir ağ üzerinden tünel yoluyla oluşturulan özel bir ağdır. Günümüzde sanal özel ağ (Virtual Private Network) ile kastedilen, IPSec VPN'ler gibi VPN ile şifrelemenin uygulanmasıdır. VPN uygulamak için, bir VPN ağ geçidi gereklidir. Burada Berqnet bir VPN ağ geçidi olarak kullanılacaktır.

İki tür VPN ağı vardır:

- Site-to-site (Siteden-siteye)
- Remote access (Uzaktan erişim)

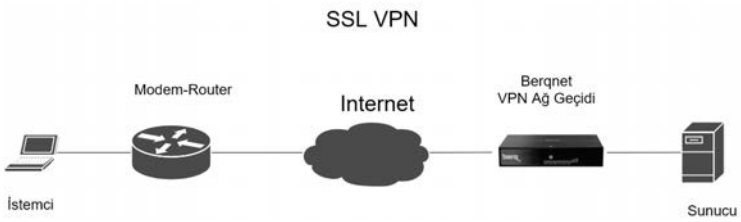
Site-to-Site VPN

VPN bağlantısının her iki tarafındaki cihaz da önceden yapılandırılmıştır. VPN statik olarak kalır ve içerideki host'lar VPN'in var olduğundan habersizdirler. Site-to-site VPN'de bulunan uç host'lar, normal TCP/IP trafiklerini VPN "ağ geçidi" aracı-

lığıyla gönderir ve alırlar. VPN ağ geçidi, belirli bir siteye giden dışarı yönlü trafiği kapsüllemekten ve şifrelemekten sorumludur. VPN ağ geçidi daha sonra hedef sitedeki eş VPN ağ geçidine internet üzerinden VPN tüneli aracılığı ile gönderir. Eş VPN ağ geçidi aldıktan sonra, başlıkları açar, içeriği çözer ve kendi özel ağı içindeki hedef host'a doğru paketi gönderir. Site-to-Site VPN yapılandırmasında IPsec protokolü kullanılır.

Remote-access (Uzaktan erişim) VPN

Uzaktan erişim VPN'ler, internet üzerinden güvenli bir şekilde kurumsal ağa erişmesi gereken bireysel host'ları bağlamak için kullanılır. Uzaktan erişim VPN evden çalışanların, mobil kullanıcıların ve extranet trafiğinin ihtiyaçlarını destekler. VPN bilgisi statik olarak ayarlanmadığında ve bunun yerine dinamik bilgi değişimi için izin verildiğinde bir uzaktan erişim VPN oluşturulur ve etkinleştirilebilip, kapatılabilir. Uzaktan erişim VPN'ler, bir VPN istemcisinin (uzak host) kurumsal ağın sınırındaki bir VPN sunucusuna güvenli erişim sağladığı istemci/sunucu mimarisini destekler. VPN istemci yazılımının mobil kullanıcının uç cihazınızda yüklü olması gerekebilir; Örneğin, her host'ta Open VPN gibi bir yazılım yüklemek gerekir.



Uzaktan erişim VPN uygulaması için iki temel yöntem vardır:

- Güvenli Soket Katmanı (Secure Sockets Layer - SSL)
- IP güvenliği (IPsec)

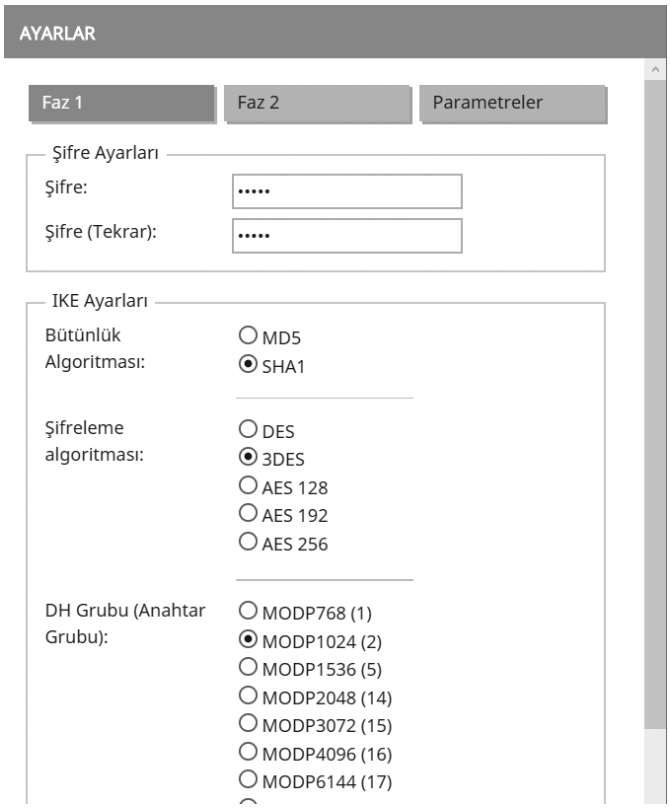
Uygulanan VPN yönteminin türü, kullanıcıların erişim gereksinimlerine ve şirketin BT süreçlerine dayanmaktadır. Hem IPsec hem de SSL VPN teknolojileri neredeyse tüm ağ uygulamalarına veya kaynağına erişim sunar. SSL VPN'ler, şirket tarafından yönetilmeyen masaüstülerden kolay bağlantı, az veya hiç masaüstü yazılım bakımı ve girişten sonra kullanıcıya özel web portalları gibi özellikler sunar. Berqnet uzaktan erişim için SSL VPN yapılandırmasını destekler.

6.8.1. IPsec VPN Ayarları

IPsec ile site-to-site VPN ayarları için her iki tarafta da bir VPN gateway olmalıdır. Birinci tarafta bulunan Berqnet'teki ayarları yapalım.

Ana sayfadaki üstteki menüden VPN simgesine tıklıyoruz. Burada IPSec ve SSL VPN sekmelerini göreceksiniz.

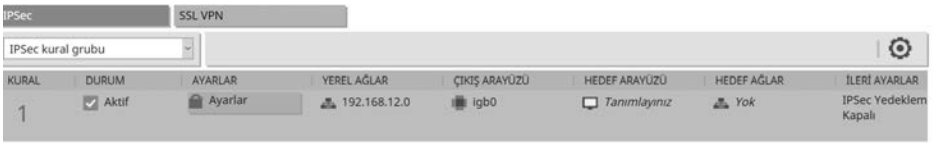
Burada durum seçeneğine çift tıklayarak pasiften aktife dönüştürüyoruz. Daha sonra ayarlar simgesine çift tıklayarak ayarlar penceresini açıyoruz.



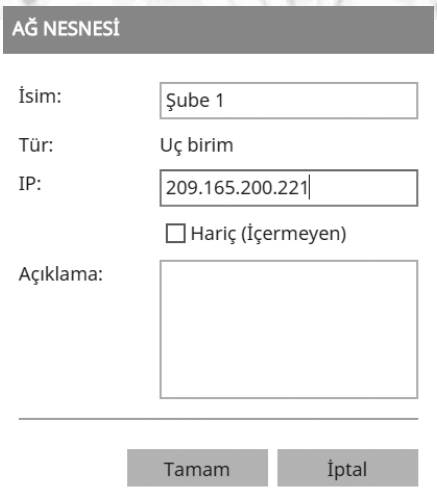
Ayarlar penceresinde şifre ayarları kısmında gördüğünüz şifre, diğer cihazlarda pre shared key olarak adlandırılır ve karşı tarafta başka marka bir firewall kullanıyorsanız her iki cihazda da aynı olmalıdır. IPsec kurulabilmesi için ayarlar kısmındaki diğer seçeneklerin de karşı taraftaki cihazla uyumlu olması gerekir.

Yerel ağlar kısmında karşı taraftan gelen kullanıcıların erişmesini istediğimiz bizim taraftaki yerel bir ağı belirliyoruz. Öncelikle sol tarafta sağ tıklayıp ekle diyerek yeni bir ağ nesnesi oluşturuyorum.

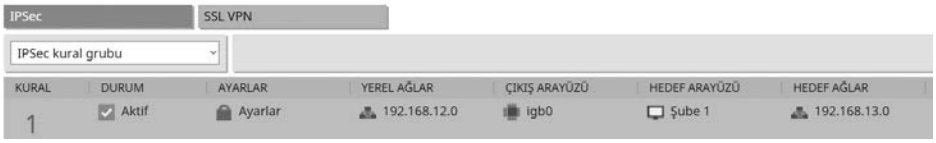
Bu ağ nesnesi igb1 arayüzüne bağlı bir yerel ağ. Bir ağ belirleyebildiğiniz gibi bir uç birim (host) veya adres grubu da belirleyebilirsiniz. Sonra bu ağ nesnesini sürükleyip yerel ağlar kısmına bırakıyoruz.



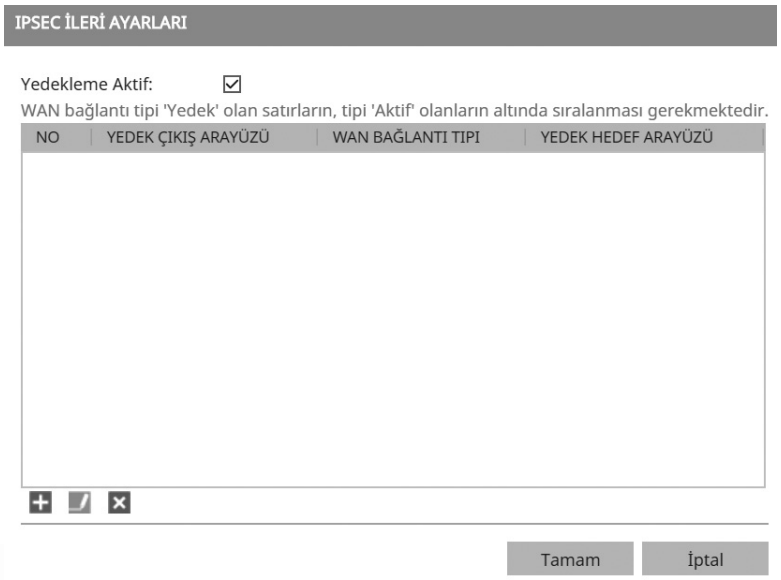
Çıkış arayüzü bölümünde cihazın dış IP adresi alan arayüzünü seçiyoruz. Burada zaten igb0 olduğu için değiştirmiyorum. Hedef arayüz kısmına da karşı tarafın dış IP adresini yazıyoruz. Bunun için hedef arayüz kısmına çift tıklayalım ve açılan pencerede karşı tarafın dış (public) adresini bir isim vererek girelim.



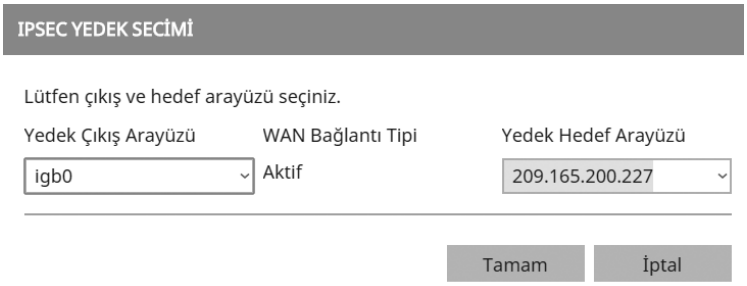
Hedef ağlar kısmına da karşı tarafta erişilmesine izin verilen yerel ağı tanımlıyoruz. Karşı tarafta da yerel ağ olarak 192.168.13.0 tanımlanmış. İlgili ağ nesnesini öncelikle oluşturup sonra sol taraftan alıp sürükleyip hedef ağlar kısmına bırakıyoruz.



IPsec yedekleme seçeneği ile iki taraf arasında IPsec VPN kurarken birden fazla İnternet bağlantınız varsa ve bunlardan biri kesilirse IPsec VPN bağlantısının kesintiye uğramasını engelliyoruz. Bunun için IPsec yedekleme kısmına çift tıklayalım ve açılan pencerede yedeklemeyi etkinleştirelim.

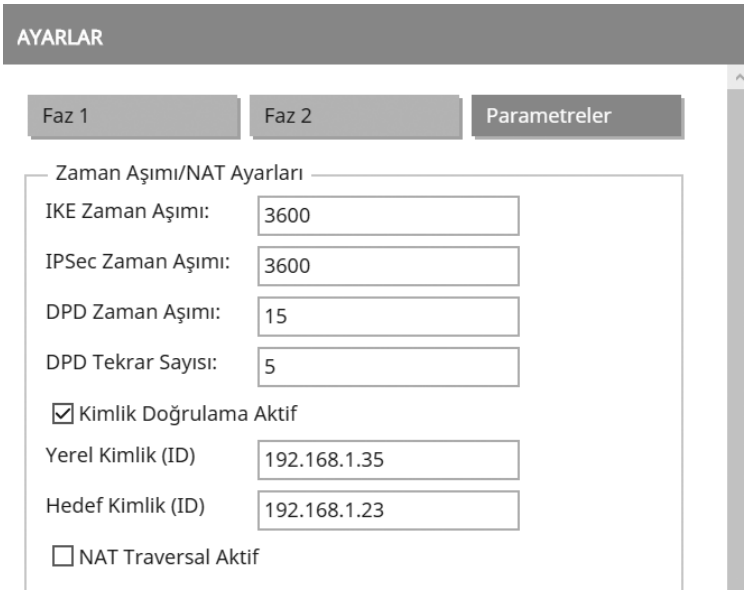


Sonra sol altta bulunan mavi artı düğmesine tıklayarak açılan pencerede yedek çıkış arayüzü kısmında birden fazla WAN bağlantımız varsa yedeklemek istediğimiz bağlantıyı seçiyoruz. Yedek hedef arayüzü kısmına da karşı taraftaki yedek İnternet bağlantısının IP adresini yazıyoruz. Karşı taraf IP adresi için öncelikle bir ağ nesnesi oluşturmuş olmalısınız.



Bu şekilde ne kadar yedek dış-WAN IP adresimiz varsa hepsi arasında yedekleme yapabiliriz.

Buraya kadar yaptığımız Ipsec ayarları İnterneti Berqnet üzerinde sonlandırdığımız (PPoE) yapılar için geçerliydi. Bazı yapılar da Berqnet modem arkasında çalışıyor olabilir. Bu durumda IPsec kurulabilmesi için ayarlar kısmında parametreler sekmesine geliyoruz. Kimlik doğrulama aktif kısmına onay koyup her iki tarafın dış arayüz (WAN) IP adreslerini yazıyoruz.



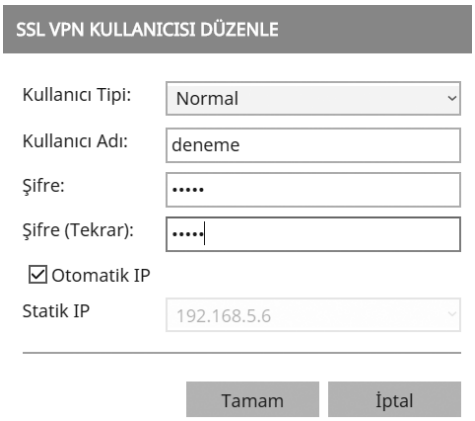
Son olarak uygula düğmesine tıklayarak yaptığımız değişikliklerin uygulanmasını sağlayalım.

6.8.2. SSL VPN Ayarları

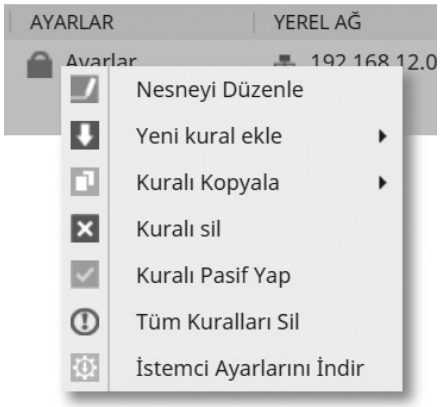
SSL VPN ayarları, VPN ayarları kısmında SSL VPN sekmesinde yapılandırılır. Öncelikle durum kısmında çift tıklayarak aktif yapalım. Yerel ağ kısmına sol taraftaki ağ nesneleri kısmından yerel ağımızı tanımlayan nesneyi sürükleyip bırakıyoruz (192.168.12.0). Çıkış arayüzü olarak WAN arayüzü seçili değilse seçiyoruz. Sanal ağ kısmında uzaktan SSL VPN ile bağlanan kullanıcıların almasını istediği IP ağını tanımlıyoruz. Yerel ağımızda kullanmadığımız 192.168.5.0 ağı olabilir. Bunun için sanal ağ kısmına çift tıklayarak düzenliyoruz.

Daha sonra ayarlar kısmına çift tıklayarak ayarlar penceresini açıyoruz.

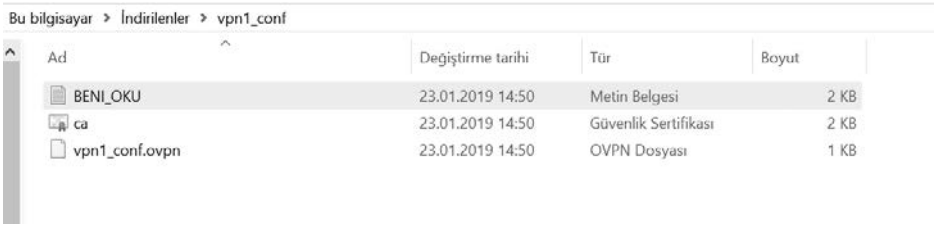
Burada sol alttaki mavi artı simgesine tıklayarak kullanıcı ekleyebiliriz. Kullanıcı adı "deneme" şifre "12345" olan yeni bir kullanıcı ekliyorum. Gerçek uygulamalarda bu kadar basit şifreler belirlemeyin uyarısını yaparak devam edelim.



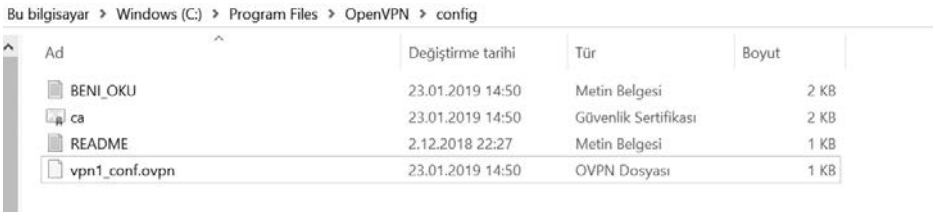
Tamam düğmesine tıklayarak pencereyi kapatalım. Sağ üstteki uygula düğmesine tıklayarak SSL VPN yapılandırmasını uygulayalım. Son olarak ayarlar kısmına sağ tıklayalım ve açılan menüden istemci ayarlarını indir seçeneğine tıklayalım.



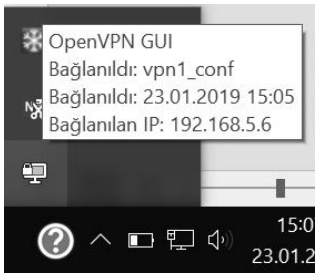
Açılan pencerede ileri, ileri, uygula ve son düğmelerine tıklayarak ayarları indiriyoruz. İndirilen sıkıştırılmış dosyayı klasöre çıkaralım. İçerisinde 3 tane dosya göreceğiz.



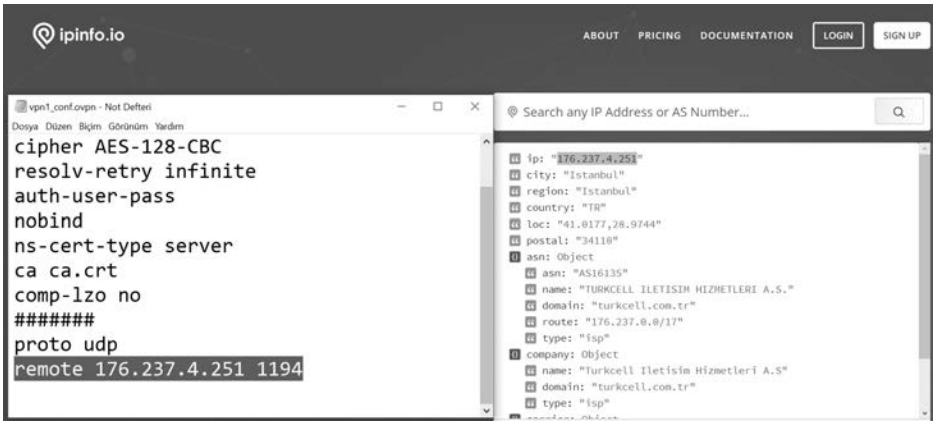
BENI_OKU isimli metin dosyasında yapmamız gerekenler adım adım anlatılmıştır. Ca ve vpn1_conf dosyalarını Open VPN programını kurduktan sonra ilgili klasörlere kopyalayıp yapıştıralım.



Şimdi Open VPN programını çalıştıralım. Open VPN simgesine sağ tıklayalım, ardından bağlan seçeneğine tıklayalım. Kullanıcı adı olarak "deneme" şifre olarak "12345" girelim ve tamam düğmesine tıklayalım. Bağlantı sorunsuz bir şekilde sağlanınca Open VPN simgesi yeşil olur ve üzerine geldiğinizde yerel ağdan aldığımız IP adresi (192.168.5.6) görüntülenir.

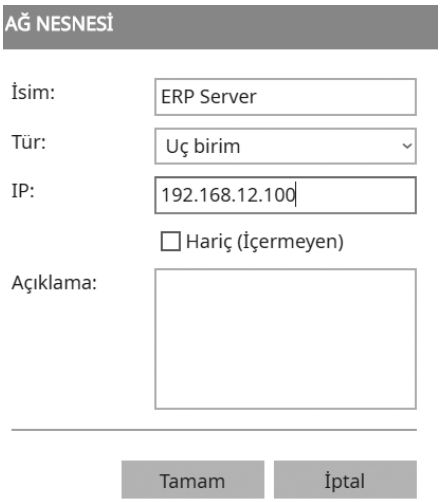


SSL VPN ayarlarını eğer statik kurulum yani İnterneti Berqnet'te sonlandırmadığımız durumlarda yapmak için indirdiğimiz vpn1_conf.ovpn dosyasını Not defteri (notepad) ile açıyoruz ve IP adresini modemin ISP'den aldığı IP adresi ile değiştiriyoruz.



Ardından modemde port yönlendirmesi yaparak 1194 numaralı porta gelen istekleri 192.168.1.35 (Berqnet'in WAN arayüz IP adresi) IP adresine yönlendiriyoruz.

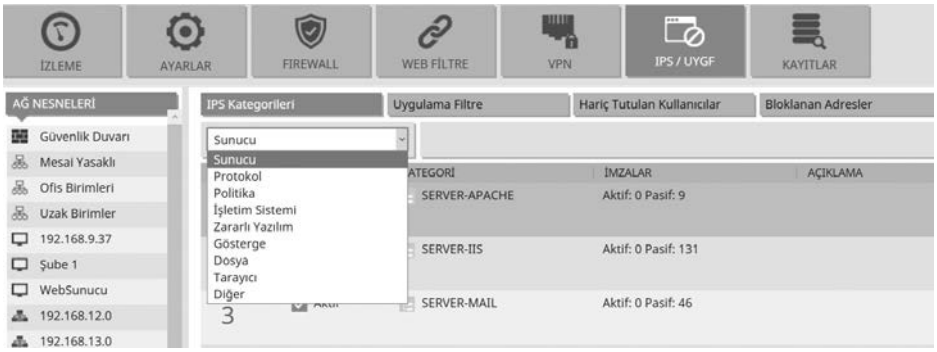
SSL VPN'de yerel ağ nesnesi bölümüne ağda hangi cihaza veya cihazlara erişmek isteniliyorsa o nesne ilgili bölüme atılabilir. Örneğin SSL VPN ile sadece 192.168.12.100 IP'sindeki ERP Server'a erişmek isteniliyorsa ilgili IP'yi uç birim olarak yerel ağ nesnesi bölümünde oluşturup sadece sunucuya erişim izni verilebilir veya birden fazla uç birim atanarak tek tek erişilmesi istenilen cihazlar kurala dahil edilebilir.



6.9. IPS ve Uygulama Filtresi Ayarları

6.9.1. IPS Ayarları

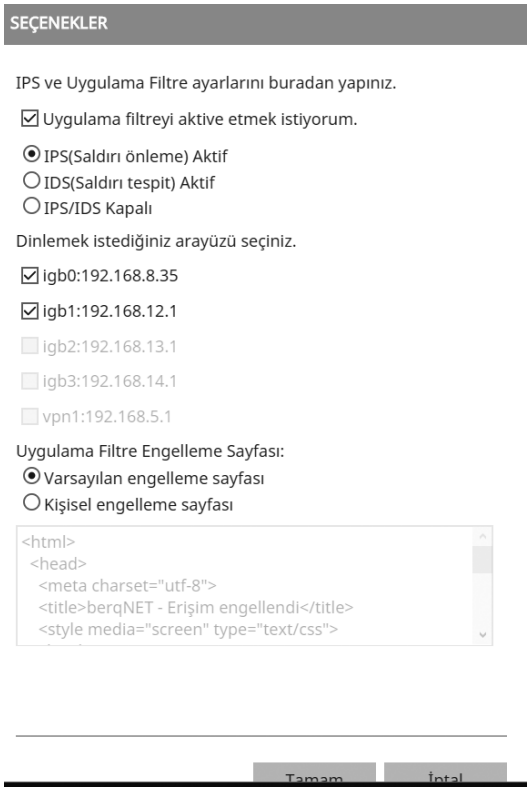
IPS (Intrusion Prevention System) Saldırı engelleme sistemi anlamına gelmektedir. Berqnet'in IPS özelliği ile ağınıza giren veya ağ dışına çıkan kötü niyetli trafiği ve bağlantılarını engellemiş olursunuz. İmza tabanlı çalışır ve Berqnet ile hazır gelen birçok imza kategorisi vardır. Bu kategorileri ana sayfada IPS/UYGF düğmesine tıkladıktan sonra karşınıza gelen sayfada IPS kategorileri sekmesinde açılan menüden görebilirsiniz.



Cihazınızı, güncelleme ayarları bölümünden güncellediğinizde veya otomatik güncelleştirmeyi açtığınızda bu imza dosyaları da güncellenir ve yeni saldırı tiplerine karşı korunmuş olursunuz.

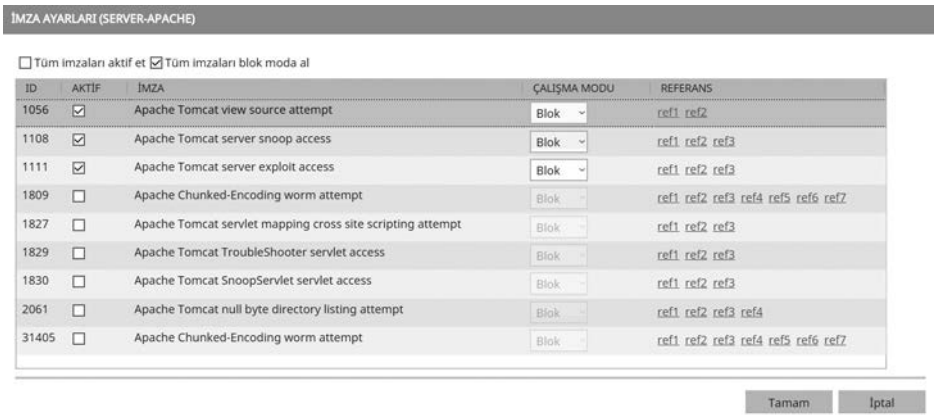
Şimdi IPS özelliğini etkinleştirelim. Bunun için sayfanın sağındaki genel ayarlar (dişli çark simgesi) simgesine tıklıyoruz.

Açılan pencerede uygulama filtreyi aktif etmek istiyorum seçeneğine onay koyarak şimdiden bu özelliği de aktif edebilirsiniz. IPS (saldırı engelleme) aktif seçeneğine tıklayarak IPS özelliğini etkinleştiriyoruz. Dinlemek istediğiniz arayüzü seçin kısmından incelenecek trafiğin geçeceği arayüzleri belirleyebiliriz. Uygulama filtresi engelleme sayfası için varsayılan sayfayı kullanabilir, isterseniz kişisel engelleme sayfası seçeneğine tıklayarak özelleştirebilirsiniz. İlgili ayarları yaptıktan sonra Tamam düğmesine tıklayarak pencereyi kapatıyoruz.



IPS servisini aktif hale getirdikten sonra saldırı tespit ve engelleme sistemi varsayılan politika ve imzalar ile aktif hale gelecektir. Özelleştirilmiş politika ve imza ayarlarınız için ise aşağıdaki resimde görüleceği gibi kategoriler seçeneği ile ayarlamalarınızı yapabilirsiniz.

Öncelikle IPS kategorileri sekmesine dönüyoruz ve burada etkinleştirmek istediğimiz imzaları seçiyoruz. Çalışma modu olarak blok veya alarm seçebilirsiniz. Blok seçerseniz imzaya uyan istenmeyen trafik algılandığında bloklanır, alarm seçerseniz alarm üretilir.



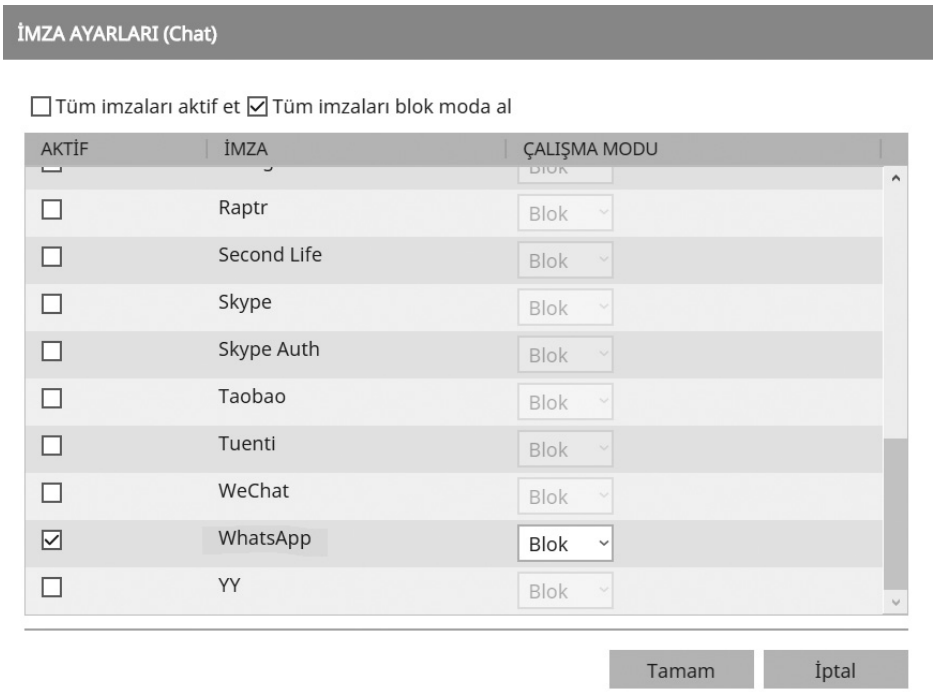
Diğer kategorilerdeki imzaları etkinleştirmek için ilgili kategoriyi açılır menüden önce seçiyoruz, sonra da istediğimiz imzaları, imzalar kısmına çift tıklayarak açtığımız pencereden etkinleştiriyoruz.

Hariç tutulan kullanıcılar sekmesinde IPS Servisindeki ayarlardan belirli kullanıcı veya kullanıcı gruplarını hariç tutmak isterseniz kullanıcı veya kullanıcı gruplarınızı Kullanıcı bölümüne sürükleyip bırakmanız yeterli olacaktır.

6.9.2. Uygulama Filtresi Ayarları

Berqnet'in uygulama filtresi ile kullanıcıların erişmesini ve kullanmasını istemediğiniz uygulamaları engelleyebilirsiniz. Örneğin şirket ağı üzerinden WhatsApp kullanmasını engellemek istiyoruz. Öncelikle IPS ayarlarını yaparken uygulama filtresini aktif hale getirdiğimizi hatırlayalım. Uygulama filtre sekmesine gelip, açılan menüden eğlence kategorisini seçiyoruz.

Burada önce durum kısmına çift tıklayarak aktif hale getiriyoruz sonra da Chat uygulamasına çift tıklıyoruz ve açılan pencerede WhatsApp uygulamasını seçip Tamam düğmesine tıklıyoruz.

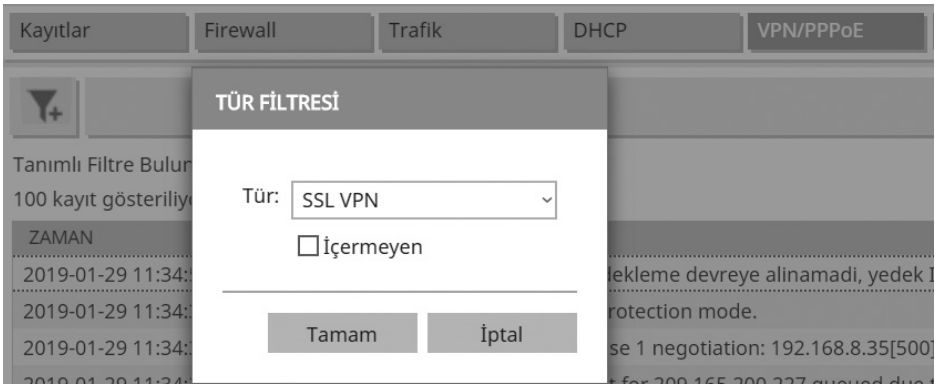


Bu şekilde diğer kategorilerde bulunan onlarca uygulamayı engelleyebilirsiniz.

6.10. Kayıtlar

Bu bölümde Berqnet'in oluşturduğu log kayıtlarını görüntüleyebiliriz. Bu sayede ağımızda yaşanan sorunları görüntüleyebilir, kimlerin ne kadar trafik kullandığını tespit edebilir, uyguladığımız web filtre kurallarının sonuçlarını izleyebiliriz. Bu kayıtlar anlaşılabilir pasta veya sütun grafik şeklinde ilk sekmede özetlenmiştir. Diğer sekmelere geçerek ayrıntılı biçimde görüntüleyebilirsiniz.

Kayıtlar bölümünde firewall, trafik, DHCP, VPN, Antivirüs, web filtre, IPS, Uygulama filtresi, hotspot ve sistem ile ilgili kayıtları görüntüleyebilirsiniz. Bu sekmelerde bulunan kayıtlarda çeşitli filtreler uygulayarak istediğiniz kayıtları bulabilirsiniz. Örneğin VPN kayıtlarında SSL VPN kayıtlarını filtreleyelim. VPN/PPoE sekmesine geliyoruz. Burada sol taraftaki huni artı simgesine tıklayıp açılan pencerede tür olarak SSL VPN seçiyoruz ve tamam düğmesine tıklıyoruz.



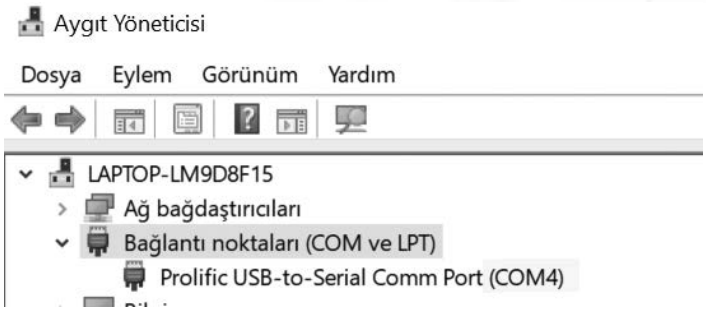
Özellikle ağınızda bağlantı sorunları yaşadığınızda veya İnternetinizin yavaşlaması söz konusu olduğunda kullanıcıların kullandığı trafik miktarını görüntüleyerek hız veya download limiti koymamış iseniz yoğun download yapan bir kullanıcının İnternet bağlantınızı yavaşlatabileceğini görebilirsiniz. Bunun için trafik sekmesine geliyoruz, burada filtreleme simgesine tıklayıp, İndirme(MB) seçeneğini seçip bir değer giriyoruz. Tamam düğmesine tıkladığımızda belirttiğimiz değere eşit veya daha fazla indirme yapan kullanıcı IP adreslerini görüntüleyebiliriz.

İleride anlatacağımız senaryolar ile bu kullanıcıların download hızlarını sınırlayabileceksiniz.

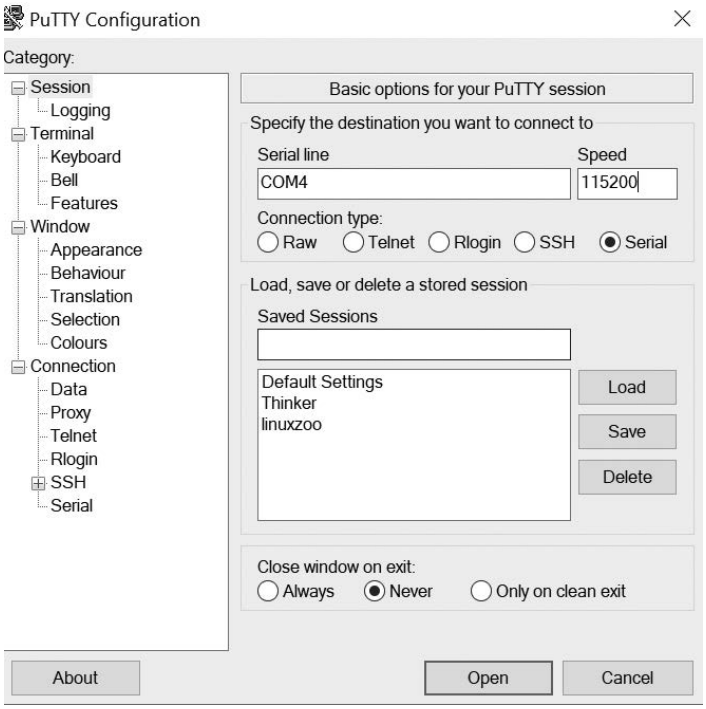
6.11. Şifre Sıfırlama ve Fabrika Ayarlarına Dönme

Cihazımızda herhangi bir sorun yaşarsak fabrika ayarlarına döndürebiliriz. Bunun yanında varsayılan Berqnet kullanıcı adı ve parolası dışında bir parola belirlediysek ve bunu unutursak yine aynı şekilde şifreyi sıfırlayabiliriz. Bu işlemler için Berqnet kutusundan çıkan konsol kablosunu cihazın konsol girişine diğer ucunu da bir seri-usb çevirici aracılığıyla bilgisayarımızın USB girişine bağlıyoruz.

Bilgisayarımızın Aygıt yöneticisi kısmına gelip (Bu bilgisayar sağ tık özellikler/aygıt yöneticisi) usb girişe taktığımız çeviricinin oluşturduğu COM port'u tespit ediyoruz. Benim bilgisayarımda COM4.



Daha sonra bir terminal programı aracılığıyla konsol bağlantısını gerçekleştiriyoruz. Ben en sık kullanılan Putty aracılığı ile bu işlemi gerçekleştireceğim. Programı çalıştırıyorum. Serial seçeneğine tıklayıp serial line kısmına COM4 yazıyorum. Speed olarak 115200 yazmayı unutmayın. Varsayılan değer olan 9600 ile bağlanırsanız anlamsız karakterler ile karşılaşabilirsiniz.



Cihaza enerji verip Putty'de open düğmesine tıkladığımızda konsol bağlantısı gerçekleşir, cihaz açılır (boot) ve şu ekranı görürüz.

```
Starting background file system checks in 60 seconds.

Tue Jan 29 12:16:19 +03 2019
BERQ
************************************************************
* berqNET Guvenlik Duvari Konsol Uygulamasina Hosgeldiniz *
************************************************************
Konsol menusu
 1- Sifre sifirla
 2- Firewall kurallarini sifirla
 3- Yonlendirme tablosunu sifirla
 4- Konfigurasyonlari sifirla
 5- Fabrika ayalarina geri don
 6- Tani araclari
Lutfen yapmak istediginiz islemi giriniz:
```

Lütfen yapmak istediğiniz işlemi giriniz kısmına yukarıdaki menüden ilgili numaraları yazarak işlemi gerçekleştirebilirsiniz. Örneğin şifre sıfırlama için 1, fabrika ayarlarına geri dönmek için 5 gibi.

1 tuşuna ardından enter tuşuna basıyorum ve gelen uyarıda E tuşuna basarak devam ediyorum. İşlem sonunda "şifre başarı ile sifirlandı" uyarısını görüyorum. Böylelikle cihaza tekrardan Berqnet ile giriş yapabilirim.

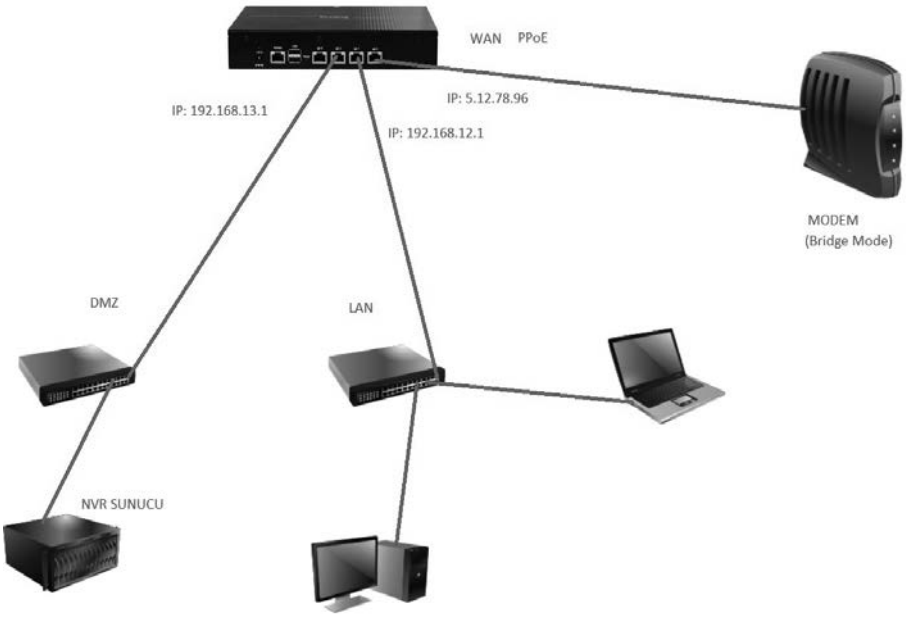
```
************************************************************
* berqNET Guvenlik Duvari Konsol Uygulamasina Hosgeldiniz *
************************************************************
Konsol menusu
 1- Sifre sifirla
 2- Firewall kurallarini sifirla
 3- Yonlendirme tablosunu sifirla
 4- Konfigurasyonlari sifirla
 5- Fabrika ayalarina geri don
 6- Tani araclari
Lutfen yapmak istediginiz islemi giriniz:1

Kullanicilar yeniden yapilandirilacaktir.
Devam etmek istiyor musunuz?[E]vet/[H]ayir/[I]ptal:e
<<---Sifre basari ile sifirlandi.--->>
```

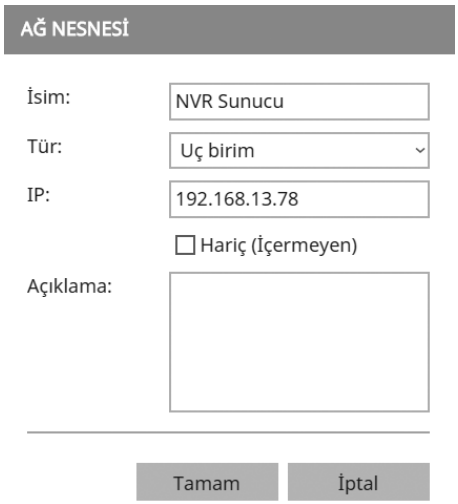
Cihazınızı fabrika ayarlarına döndürecekseniz daha önceden bütün yapılandırmaların yedeğini aldığınıza emin olun. Yoksa bütün konfigürasyonları tekrar yapmak zorunda kalırsınız.

6.12. Firewall Uygulama Senaryoları

Önceki bölümlerde firewall ayarlarından bahsetmiştik, burada bazı örnek senaryolar ile konuyu daha ayrıntılı inceleyelim. Aşağıdaki topolojiye göre cihazımızın arayüzlerinin ve gerekli yapılandırmaları gerçekleştirdiğimizi varsayalım.



Burada ilk yapmak istediğimiz; DMZ tarafında bulunan NVR sunucusuna ağımızın dışından erişebilmek ve güvenlik kamerası kayıtlarını izleyebilmek. Bunun için Firewall ayarlarında Port yönlendirme sekmesine geliyoruz. Soldaki ağ nesneleri kısmında sağ tıklayıp ekle diyerek NVR Sunucu için bir ağ nesnesi oluşturuyoruz.



Yine sol tarafta bulunan servis nesneleri kısmında sağ tıkla ekle diyerek NVR sunucunun yönlendireceğimiz port'u için bir nesne oluşturuyoruz.

Sonra port yönlendirme kurallar alanında sağ tıklayarak yeni bir kural ekleyelim. Kayıt tutulmasını istiyorsak kayıt kısmına çift tıklıyoruz. Daha sonra az önce oluşturduğumuz ağ nesnesini iletilen sunucu kısmına, servis nesnesini de gelen ve iletilen servis kısmına sürükleyip bırakıyoruz. Geliş arayüzü kısmına çift tıklayarak WAN arayüzünü seçiyoruz.

Sağ üstteki uygula düğmesine tıklamayı unutmayın. Daha önce de hatırlattığımız gibi siber güvenlik zafiyetlerinden dolayı port yönlendirme ile yerel ağınızdaki bir sunucuya erişmek yerine VPN ile ulaşmayı tercih ediniz. Artık ağınızın dışındaki bir kullanıcı İnternet tarayıcısında adres satırına http://5.12.78.96 yazdığında sunucuya erişip kamera görüntülerini izleyebilir.

Başka bir senaryoda cihazımıza https üzerinden dışarıdan erişimi yasaklayacağız. Nmap gibi por tarama programları ile İnterneti tarayan siber korsanlar açık buldukları servisler üzerinden ağlara sızabilmektedir. Hele ki varsayılan kullanıcı adı ve parola değiştirilmemiş cihazlar veya kaba kuvvet ve sözlük listesi saldırıları ile sistemlere sızmak mümkündür. İşte https servisini dışarıya kapatarak bu tehlikenin önüne geçeceğiz.

Firewall ayarları kısmında yeni bir kural ekleyebilir ya da mevcut 1. Kuralda değişiklik yapabiliriz. Öncelikle eylem kısmına çift tıklayarak düşür yapalım. Sonra sol taraftaki ağ servisleri kısmından https servisini sürükleyip servis kısmına bırakıyoruz.

Daha sonra giriş arayüzü kısmına çift tıklayarak WAN arayüzünü seçiyoruz. Diğer arayüzleri seçmeyin, yoksa yerel ağ üzerinden siz de erişemezsiniz.

Son olarak sağdaki çark simgesine tıklayıp Firewall ayarları penceresini açıyoruz ve Engelleyen kural olsa da web arayüzüne erişime izin ver seçeneğindeki onayı kaldırıyoruz.

FIREWALL AYARLARI

Güvenlik politikanızın gelişmiş ayarlarını buradan yapınız.

☐ Web arayüzü erişim portunu değiştir.

Yönetim Portu : 443

☑ Sistem son kuralı olan "herşeyi düşür" için kayıt tutsun.

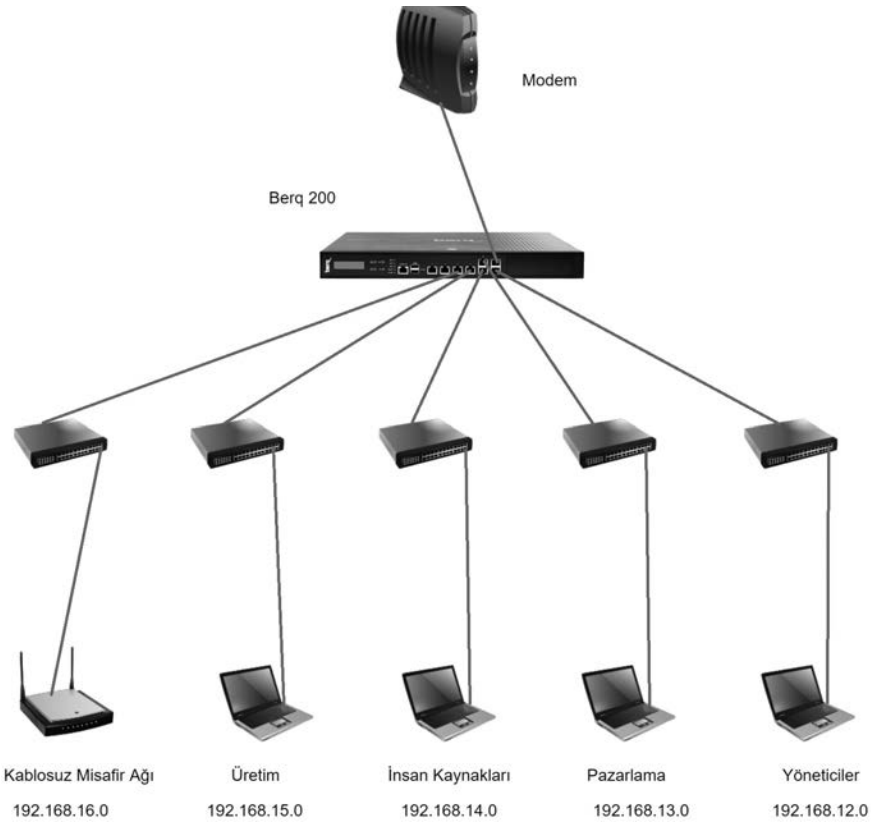
☐ Engelleyen kural olsa da web arayüzüne erişime izin ver.

☑ Kayıt tut.

Tamam düğmesine tıklayarak pencereyi kapatıyoruz. Her zaman olduğu gibi sağ üstteki uygula düğmesine tıklamayı unutmayınız.

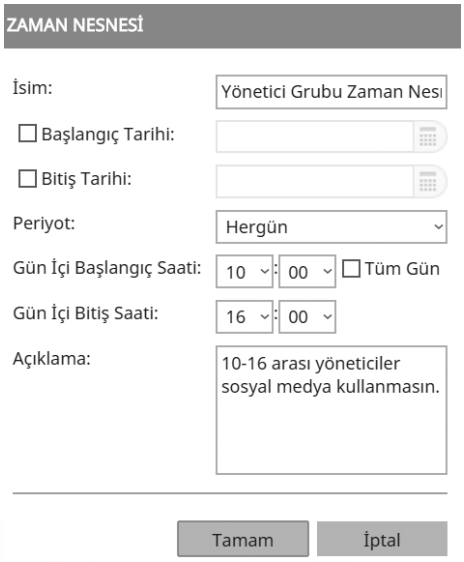
6.13. Web Filtre Örnek Senaryoları

Bu bölümde şekildeki topolojiye göre bazı web filtre senaryoları oluşturacağız.



Şekilde kullanıcı grupları ve grupların IP adresleri gösterilmiştir. Öncelikle yönetici grubundaki kullanıcılar sadece belirli zaman dilimlerinde sosyal medya sitelerini kullanmaları engelleyelim. Web filtre bölümüne gelelim. Soldaki ağ nesneleri bölümünde sağ tık ekle diyerek yönetici grubu için bir ağ nesnesi oluşturalım.

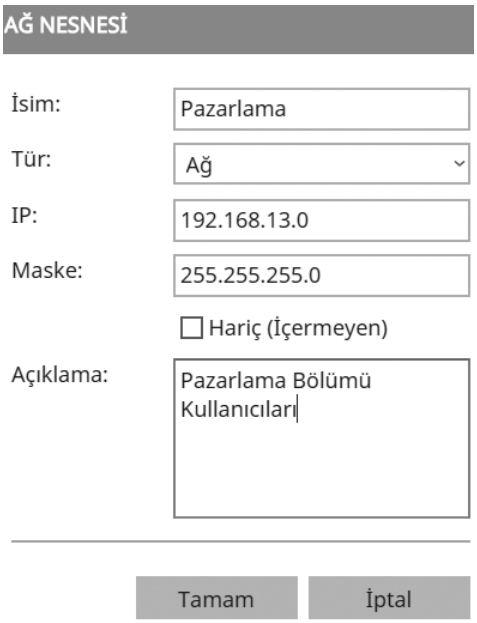
Sonra bu nesneyi sürükleyip kullanıcılar kısmına bırakalım. Soldaki URL kategorileri kısmına gelip sosyal medya kategorisini engelleme listesi kısmına sürükleyip bırakın. Son olarak yasaklamak istediğimiz zaman dilimi için limit nesneleri kısmına gelip sağ tıkla zaman diyerek yeni bir zaman nesnesi oluşturalım.



Oluşturduğumuz zaman nesnesi sürükleyip limit kısmına bırakalım.

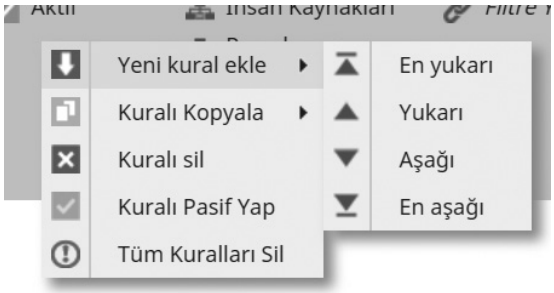
Bu kural ile yönetici grubundaki kullanıcıların saat 10-16 arasında sosyal medya sitelerini kullanmalarını engellemiş olduk. Bu zaman dilimleri dışında ise sosyal medya sitelerini kullanabilecekler.

Şimdi de pazarlama, insan kaynakları ve üretim bölümlerindeki kullanıcılar için bazı kurallar oluşturalım. Kurala göre bu gruplardaki kullanıcıların sosyal medya, bahis, cinsellik, alış veriş siteleri vb. sitelere girişi yasaklanacak, fakat öğlen tatilinde sosyal medya sitelerine girişlerine izin verilecek. Bunun için önce, az önce yaptığımız gibi ağ nesneleri kısmında bu gruplar için ağ nesneleri oluşturun şekilde pazarlama bölümü için ağ nesnesi oluşturulmuştur. Diğerlerini de aynı şekilde yapabilirsiniz.



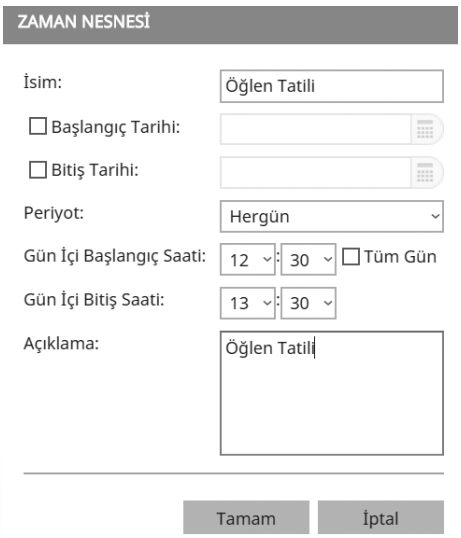
Önce filtre kuralları kısmında sağ tıklayıp en aşağı kural ekleyi seçelim. Sonra da oluşturduğumuz bu ağ nesnelerini kullanıcılar kısmına sürükleyip bırakalım. Engelleme listesi kısmına da URL kategorileri kısmından engellemek istediğimiz kategorileri sürükleyip bırakalım.

Şimdi de bu kullanıcı grubuna öğlen arasında sosyal medya kullanımına izin verecek kuralı oluşturalım. 2 numaralı kuralın üzerinde sağ tıklayalım, açılan menüden yeni kural ekle/yukarı seçeneği ile 2 numaralı kuralın üstüne yeni bir kural ekleyelim.



Şimdi 2 numaralı kural 3 numara oldu ve 2 numaralı boş bir kural eklendi.

2 numaralı kuralın kullanıcılar kısmına yine bu gruplar için daha önce oluşturduğumuz ağ nesnelerini sürükleyip bırakıyoruz. İzin listesi kısmına url kategorileri kısmından sosyal medya kategorisini sürükleyip bırakıyoruz. Daha sonra limit nesneleri kısmına gelip sağ tıkla zaman diyerek kurumun öğle tatilini belirleyen saatleri yazıp bir zaman nesnesi oluşturuyoruz.



Sonra bu zaman nesnesini sürükleyip limit kısmına bırakıyoruz.

Şöyle sorabilirsiniz: Bu kuralı neden üst ekledik? Firewall kuralları yukarıdan aşağıya çalışır ve bir eşleşme (match) olduğu zaman kural işler. Eğer yasak yazdığımız 2. Kural üstte, izin verdiğimiz kural altta olsaydı öğlen tatilinde bile bu kullanıcılardan gelen trafik 2. Kurala takılıp engelleneceği için aşağıdaki kurala hiç ulaşamayacaktı bile. Bunu engellemek için izin verdiğimiz kuralı üste yazdık. Sadece öğlen tatilinde sosyal medya izinli oldu. Bunun dışında aşağıdaki kurala göre öğlen tatili dışında yasakladığımız kategorilere giden ziyaret istekleri engellenmiş oldu.

Şimdi de kablosuz misafir ağı için bant genişliği limiti olan bir kural oluşturalım. Böylelikle hotspot ile ağımıza bağlanan misafirler herhangi bir yasağa tâbi olmasın ama İnternetimizi yavaşlatmasınlar diye bir hız sınırına tâbi olsunlar.

Kural kısmında sağ tıkla yeni kural ekle/aşağı diyerek yeni bir kural ekleyelim. Kablosuz misafir ağı için bir ağ nesnesi oluşturup kullanıcılar kısmına sürükleyip bırakalım. Sonra limit nesneleri kısmına gelip sağ tıkla bant genişliği diyerek resimde görüldüğü şekilde bir bant genişliği nesnesi oluşturalım.

Oluşturduğumuz bu bant genişliği nesnesini limit kısmına sürükleyip bırakıyoruz.

Oluşturduğumuz bu kural ile kablosuz misafir ağından bağlanan kullanıcıların bağlantı hızını 1 Mbit/sn ile sınırlandırmış olduk.

İşletmenizin
Emniyet Kemeri: Berqnet

Her gün onlarca işletme siber saldırılara maruz kalıyor. Bu saldırılar sonucunda yaşanan veri kayıpları ciddi **maddi zararları** da beraberinde getiriyor. Türkiye'nin Yeni Nesil Firewall'u Berqnet olarak **%100 yerli AR-GE** ile geliştirdiğimiz çözümlerle sizi hem siber saldırılara karşı korurken hem de **yasalara uygun internet kayıtlarınızı** tutmanızı sağlıyoruz.

Türk Lirası fiyatlarıyla bütçenizi üzmeyen Berqnet, iş ortaklarına sunduğu **ücretsiz ve sınırsız teknik destek hizmetiyle** de alanında bir ilki gerçekleştiriyor. Bu ülkenin mühendisleri tarafından her ölçekteki işletmenin siber güvenlik ihtiyaçlarını bütüncül bir anlayışla çözmek için geliştirilen Berqnet Firewall'la tanışmak için bizi hemen arayın, işletmenizin siber güvenliğini şansa bırakmayın!

Berqnet – Siber Güvenliğiniz Bize Emanet!

berqnet

www.berqnet.com

0850 577 23 77

linkedin/berqnet

Logo TEKNOLOJİ ve YATIRIM

TEK KUTUDA, TAM ÇÖZÜM.

AR-GE çalışmalarının tamamı alanında uzman Türk yazılım mühendisleri tarafından geliştirilen Türkiye'nin Yeni Nesil Firewall'u Berqnet, sunduğu çözümlerle büyümeye devam ediyor!

Kullanıcı dostu arayüzü ve mobil raporlama uygulamasıyla ezber bozan Berqnet ürünleri, 5651 sayılı yasaya uygun kayıt tutma, gelişmiş web filtreleme becerileri, güvenli internet paylaşımı modülü, VPN ve antivirüs gibi daha birçok çözümü tek kutuda kullanıcılarının hizmetine sunuyor. Üstelik ekstra ve sürpriz lisans ücretlerine yer bırakmadan!

Detaylı bilgi almak için 0850 577 23 77 'i hemen arayın, tanışma kampanyasını kaçırmayın!

Online demo için: www.berqnet.com

berqnet

www.berqnet.com

0850 577 23 77 linkedin/berqnet

Logo TEKNOLOJİ ve YATIRIM

Tebrikler!
Değerli okurumuz,
Siber güvenliğe ilgi duyan herkese ufak bir fayda sağlamak ve içinde bulunduğumuz ekosisteme katkıda bulunmak için hazırlanmış bu kitaba sahip olarak, online eğitim platformu Udemy'de kayıt rekoru kıran Detaylı Berqnet Firewall Eğitimi'ni de ücretsiz almaya hak kazandınız. Online olarak verilen bu eğitim sayesinde bir firewall'un tüm yapılandırma detaylarını öğrenebilir, eğitim bitiminde alacağınız bitirme sertifikası ile bu alanda bir adım öne geçebilirsiniz.

Eğitime ücretsiz olarak sahip olmak için info@berqnet.com adresine "HERKES İÇİN SİBER GÜVENLİK" kitabının bir adet fotoğrafının olduğu bir e-posta göndermeniz yeterli olacaktır. Berqnet ekibi tarafından eğitimi ücretsiz alabileceğiniz indirim kuponu size en kısa sürede iletilecektir.

Saygılarımızla,
Berqnet Firewall

Berqnet Nedir?

- Berqnet, internet erişimi olan işletmeleri siber saldırılardan koruyan yeni nesil Firewall'lar (UTM Cihazları) geliştirmekte ve üretmektedir.
- İşletmelerin, çalışanlarının internette iş verimini düşürecek şekilde işletme politikalarına aykırı internet kullanımlarını yönetebilmelerini sağlayan ileri seviye web ve uygulama filtreleme özelliklerini de bünyesinde barındır. Aynı zamanda bu işletmelerde bulunan kişilerin internete erişimlerinde kimlik bilgilerini alarak, o işletmenin içinden herhangi bir siber suç işlenmesi durumunda bu kullanıcının tespitini kolaylaştırıp işletmeyi yasal yaptırımlara karşı korur ve yasal yükümlülüklere (5651 sayılı kanun) uygun şekilde logların tutulmasını sağlar. Eğer internet kullanan bir kamu veya özel sektör işletmesiyseniz bir Berqnet Firewall cihazına ihtiyacınız var demektir.
- Berqnet Firewall ürünlerinin kurulumu ve yönetimi ileri seviye uzmanlık gerektirmez. Dünyanın en kolay kurulabilen ve yönetilebilen firewall'u olma vizyonuyla geliştirilen Berqnet ürünlerini, dakikalar içinde kurabilir ve yönetebilirsiniz. Bu da işletmelere, IT operasyon süreçlerinin yönetiminde önemli bir zaman tasarrufu sağlar.
- Berqnet, Türkiye'nin borsaya açık en büyük yazılım şirketi olan LOGO Yazılım'ın 35 yıllık tecrübesiyle çalışmalarına devam etmektedir. Tüm Türkiye›de 500›den fazla iş ortağı ağıyla birlikte binlerce firmada Berqnet ürünleri kullanılmaktadır.
- %100 Yerli AR-GE'siyle bu ülkenin mühendisleri tarafından geliştirilen Berqnet Firewall ürünleri, Türkiye'den dünya açılan bir global siber güvenlik markası olma vizyonuyla çalışmalarına devam etmektedir.

Berqnet Firewall'u Kimler Kullanır?

Kamu ya da özel sektör ayrımı olmaksızın tüm işletmelerin siber güvenliğini sağlamak için tasarlanan Berqnet Firewall ürünlerini; restoran ve kafelerden her türlü konaklama işletmesine, her ölçekteki kamu kurumundan çeşitli sektörlerdeki sanayi ve üretim tesislerine kadar iş süreçlerinde internet kullanımı bulunan her firma rahatlıkla kullanabilir.

Detaylı Bilgi İçin: **www.berqnet.com**

HERKES İÇİN SİBER GÜVENLİK

Günümüzde ağa bağlanan cihaz sayısı ve çeşidi hızla artıyor. Daha düne kadar sadece birkaç bilgisayar, yazıcı ve sunucudan oluşan ağlar yerine, Nesnelerin İnternet'i (IoT) kavramı ile birlikte kombiden kahve makinesine, arabadan ayakkabıya kadar her nesnenin, her şeyin ağa bağlandığı ağ yapıları ile karşılaşmaya başladık.

Ağa bağlanan cihazların sayısının ve çeşidinin artması ile birlikte bu cihazların güvenliğini sağlamak en önemli konu haline gelmiştir. Bireylerden kurumlara kadar herkes bilgi işlem cihazlarının güvenliğini sağlamak zorunda. Bu yapılmadığında paradan zamana, itibardan değişik kaynaklara kadar birçok kayıp yaşanmakta. Hepimizin elindeki cep telefonları, bilinçli kullanılmadığında bir mağduriyet aletine dönüşebiliyor. Kurumlar verilerini koruyamadıklarında mevcut kanunlara göre büyük para cezaları ile karşılaşabiliyor.

Bilgi işlem cihazlarımızı korumaktan verilerimizi korumaya kadar gerekli önlemleri alma işlemlerine siber güvenlik diyoruz. Siber güvenlik bireylerden kurumlara oradan devletlere kadar herkesin önem vermesi gereken konuların başında geliyor.

Bu kitapta 7'den 77'ye herkes için gerekli olan siber güvenlik konularını öğrenmenin yanında, ülkemizin yerli ve milli ürünü Berqnet Bütünleşik Güvenlik Sisteminin kurulum ve yapılandırma ayarlarını da göreceksiniz.

Siber uzayda her zaman güvende kalmanız dileğiyle...

Eğitime Bir Katkı da Biz Yapalım Diye, Berqnet Firewall Udemy Eğitimi Herkese Hediye!

Cemal Taner tarafından hazırlanan bu eşsiz online eğitimde, bir firewall / utm cihazının kurulum, yapılandırma ve yönetimini online olarak istediğiniz zaman istediğiniz yerden izleyebilir ve öğrenebilirsiniz. Udemy'de rekor öğrenci seviyesine ulaşan ücretli Udemy eğitimimiz bu kitaba sahip olan herkese hediye olarak verilmektedir.*

*** Ayrıntılı bilgiye kitabımızın 156. sayfasından ulaşabilirsiniz.**

abaküs Türkiye'nin Bilişim Kaynağı www.abakuskitap.com

info@abakuskitap.com
facebook.com/abakuskitap
twitter.com/abakuskitap

ISBN 978-605-226-358-7
9 786052 263587