AÇIK KAYNAK KODLU YAZILIMLARLA AĞ GÜVENLİĞİNİN SAĞLANMASI AFYON KOCATEPE ÜNİVERSİTESİ ÖRNEĞİ

YÜKSEK LİSANS

Ahmet ERTUĞRUL

DANIŞMAN

Yrd.Doç.Dr. Uçman ERGÜN

BİLGİSAYAR ANABİLİM DALI

Nisan, 2013

Bu tez çalışması 12.FENBİL.24 numaralı proje ile BAPK tarafından desteklenmiştir.

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS

AÇIK KAYNAK KODLU YAZILIMLARLA AĞ GÜVENLİĞİNİN SAĞLANMASI AFYON KOCATEPE ÜNİVERSİTESİ ÖRNEĞİ

Ahmet ERTUĞRUL

DANIŞMAN
Yrd.Doç.Dr. Uçman ERGÜN

BİLGİSAYAR ANABİLİM DALI

Nisan, 2013

TEZ ONAY SAYFASI

Ahmet ERTUĞRUL tarafından hazırlanan "Açık Kaynak Kodlu Yazılımlarla Ağ Güvenliğinin Sağlanması Afyon Kocatepe Üniversitesi Örneği" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 09/04/2013 tarihinde aşağıdaki jüri tarafından oy birliği ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar **Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman **:** (Yrd.Doç.Dr, Uçman ERGÜN)

İkinci Danışmanı **:** (Unvanı, Adı ve Soyadı) (Varsa Yazılacak)

Başkan	**:** Doç.Dr, Ahmet GAYRETLİ : Teknoloji Fakültesi,	İmza
Üye	**:** Yrd.Doç.Dr, Uçman ERGÜN : Mühendislik Fakültesi,	İmza
Üye	**:** Yrd.Doç.Dr, Uğur FİDAN : Mühendislik Fakültesi,	İmza

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve

……. sayılı kararıyla onaylanmıştır.

…….

Prof. Dr. Mevlüt DOĞAN

Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

08/05/2013

Ahmet ERTUĞRUL

ÖZET

Yüksek Lisans Tezi

AÇIK KAYNAK KODLU YAZILIMLARLA AĞ GÜVENLİĞİNİN SAĞLANMASI AFYON KOCATEPE ÜNİVERSİTESİ ÖRNEĞİ

Ahmet ERTUĞRUL

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Ana Bilim Dalı

Danışman: Yrd.Doç.Dr. Uçman ERGÜN

T.C 5651 sayılı kanun gereği toplu internet kullanım sağlayıcı konumundaki kurum ve kuruluşların internet erişim kayıtlarını zaman damgalı olarak tutması gerekmektedir. Bu kapsamda; Afyon Kocatepe Üniversitesi internet erişim kayıtları incelendiğinde mevcut sistem üzerinde sadece güvenlik duvarı kayıtlarının bulunduğu ve bu kayıtların da söz konusu yasada belirtilen özellikleri sağlamadığı gözlemlenmiştir. Ayrıca kampüs ağında çalışmakta olan cihazların yapılandırılma eksikliklerinden kaynaklanan sorunların bulunduğu ve ağ güvenliğinin tam olarak sağlanamadığı tespit edilmiştir. Bu çalışmada; açık kaynak kodlu yazılımlar kullanılarak kablolu veya kablosuz internete erişen bütün kullanıcıların kayıtlarının doğru bir şekilde ve zaman damgalı olarak kayıtlanması sağlanmıştır. Bu işlemi gerçekleştirebilmek için; kampüs içerisinde bulunan ağ cihazlarının yapılandırılmaları değiştirilmiş, laboratuvarlarda ve yönetilebilir cihazların olmadığı noktalarda captive portal uygulanmıştır. Yönetilebilir cihazların olduğu noktalarda ise 802.1X protokolü kullanılmıştır. Bu şekilde; ağdan kaynaklanan bağlantı problemleri giderilmiştir. Kullanıcıların internet erişim kayıtları yasada belirtildiği şekilde tutulmaya başlanmıştır.

2013, xii+ 97 sayfa

Anahtar Kelimeler: 5651 Sayılı Kanun, Zaman Damgası, Açık Kaynak Kod, 802.1x, Captive Portal, Ağ Cihazları, Güvenlik Duvarı

ABSTRACT
M.Sc Thesis

PROVIDING NETWORK SECURITY ON CAMPUS NETWORKS WITH OPEN SOURCE CODE SOFTWARE : A SAMPLE OF AFYON KOCATEPE UNIVERSTY

Ahmet ERTUĞRUL

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Computer

Supervisor: Assist. Prof. Dr. Uçman ERGÜN

According to law T.C 5651, public and private institutions acting as internet service provider should keep internet access log records with time-stamps. In this context, the current internet access log records of Afyon Kocatepe University were analyzed. Currently only firewall log records are held on system, but these records don't meet the requirements of the law. In addition, there are some network security issues and further problems caused by the misconfigured devices running on the campus network. The goal of this study is providing methods to save all users access records, regardless of using wired or wireless network, time-stamped and correctly with the help of open source software. For this purpose, the campus network devices are reconfigured, the captive portal technique is used for the laboratories and locations without managed devices. For other places with only managed devices, the 802.1X protocol is used. In this way, the network connection problems are solved, and internet access log records of all users are kept in the manner prescribed by the law.

2013, xii + 97 pages

Key Words: Law No. 5651, time stamp, open source code, 802.1x, captive portal, network devices, firewall

TEŞEKKÜR

Bu çalışmanın ortaya çıkmasında her zaman yakın ilgi ve desteğini gördüğüm, çalışmanın başlangıcından sonuna kadar aynı ilgiyi devam ettiren danışmanım Yrd.Doç.Dr. Uçman ERGÜN'e, düşünceleri ile bu çalışmanın gerçekleşmesinde desteklerini esirgemeyen Bilgi İşlem Daire Başkanlığındaki değerli mesai arkadaşlarıma ve aileme teşekkürü bir borç bilirim.

Ahmet ERTUĞRUL
AFYONKARAHİSAR, 2013

İÇİNDEKİLER **Sayfa**

SİMGELER ve KISALTMALAR DİZİNİ

1. Simgeler

2. Kısaltmalar

AV	Antivirüs
AIX	Advanced Interactive eXecutive
ARP	Address Resolution Protocol
CARP	Common Address Redundancy Protocol
CCPD	Hücresel Dijital Paket Verisi
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EM	Elektromanyetik Sinyal
FSF	Free Software Foundation
GPL	General Public License – Genel Kamu Lisansı
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
IPX	Internetwork Packet eXchange
IR	Infrared – Kızıl Ötesi
ISP	Internet Service Provider - İnternet Servis Sağlayıcısı
ISS	İnternet Servis Sağlayıcı
L3	Layer 3 (OSI 3. Katman)
L7	Layer 7 (OSI 7. Katman)
LAN	Local Area Network – Yerel Alan Ağı
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAN	Kentsel Alan Ağları
NAT	Network Address Table
NIDS	Network Intrusion Detecetion System - Saldırı Tespit Sistemi
NIPS	Network Intrusion Prevention System - Saldırı Engelleme Sistemi

OSI	Open Systems Interconnection
P2P	Peer to Peer
PEAP	Protected Extensible Authentication Protocol
RAS	Remote Access Server
RF	Radyo Frekansı
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol / Internet Protocol
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator.
UTM	Unified Threat Management
VLAN	Virtual Private Network – Sanal Özel Ağ
VPN	Sanal Özel Ağ
WAN	Geniş Alan Ağları
WWAN	Kablosuz Geniş Alan Ağları
WPAN	Kablosuz Kişisel Alan Ağları

ŞEKİLLER

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Günümüzde internet kullanımı, gerek kişisel gerekse iş ilişkileri arasındaki bilgi akışını sağlayan, dünyanın en büyük iletişim aracı hâline gelmiştir.

İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte bilişim sistemlerindeki güvenlik olayları da artmaya başlamıştır. Bilişim sistemlerindeki gizlilik, bütünlük ve sürekliliğin sağlanması için birçok ürün geliştirilmektedir.

Geliştirilen bu ürünler, son kullanıcıya çözüm odaklı bir ürün olarak sunulurken diğer taraftan geliştirilmeye müsait, açık kaynak kodlu olarak verilmektedir. Açık kaynak kodlu yazılımlar GPL (Genel Kamu Lisansı) lisansıyla sunulmaktadır. Herhangi bir telif hakkı istenmemektedir. Burada bir durum yanlış anlaşılmaktadır. Açık kaynak kodlu yazılımlar her zaman ücretsiz bir yazılım olarak düşünülmemelidir. Çünkü bazı kullanıcılar yazılımdan ziyade hizmet satın alma yolunu tercih edebilmektedirler.

Açık kaynak kodlu yazılımlar ilk aşamada çözülmesi zor gibi görünse de asıl sorun kullanılacak yazılımın bilinmemesidir. Yazılımların işleyişi hakkında yeteri kadar bilgi sahibi olunduğunda açık kaynak kodlu sistemler, donanım güvenlik cihazlarına göre daha esnek olduğu ve lisanslama bedeli olmadığı gözlemlenmektedir. Burada akla ilk gelen ise kurulum aşamasında ve sistemin devam ettirilmesinde uzman personele ihtiyaç duyulmaktadır.

Dünya üzerinde saldırı yapan ülke listesine bakıldığı zaman Türkiye'nin ilk on ülke arasında olduğu gözlenmektedir. Bu sebeple bilişim suçlarının artmasıyla birlikte Başbakanlıkça 01.11.2007 tarihli 5651 sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun" çıkartılmıştır.

Bu çalışmanın birinci bölümünde literatürde ağ, ağ güvenliği ve ağ cihazlarının üzerinde durulmuş, donanımsal ve yazılımsal saldırı tespit ve engelleme sistemlerine değinilmiştir.

Çalışma esnasında kullanılan anahtarlama cihazları, sunucular (freeradius, rsyslog ve open ldap), UTM ve yazılım tabanlı güvenli duvarları hakkında bilgi verilmiştir.
Metot kısmında ise 5651 sayılı yasa kapsamında istemcilerin kayıtlarının doğru bir şekilde toplanabilmesi için sistem kurulumları, sunucuların yapılandırılması ve anahtarlama cihazlarının ayarları tanımlanmaktadır.

Bulgular kısmında ise yapılan çalışma neticesinde sunucular ve ağ cihazları üzerinde hangi tür neticeler elde edilmiş bu konular hakkında bilgi verilmiştir.

Sonuç kısmında ise mevcut sistem üzerinde kullanılmakta olan iptables güvenlik duvarının konsol arabiriminden yönetimi yapılabildiği için bir takım kurallar veya ayar işlemlerinin tekrarı yapılmaktadır. Pfsense, untagle ve endian gibi web arabiriminden yönetilebilen yazılım tabanlı güvenlik duvarlarının kurulumu ve yapılandırılması tamamlanmıştır. Güvenlik duvarlarının performans ve işlevsellikleri test edilmiştir. Sistem üzerinde kullanılabilecek alternatif güvenlik duvarı çözümleri geliştirilmiştir.

2. LİTERATÜR BİLGİLERİ

2.1 Ağ Güvenliği

Sistemlerin büyümesi ve sistemi içerisindeki birimlerin farklı özelliklere sahip olması durumunda konak bazında güvenlik yaklaşımının kullanılması çok zor olacaktır. Bu da sistemlerin ağ güvenliği yaklaşımına dönmelerine sebep olmuştur. Bu yaklaşım, ağa ulaşmaların tamamı, ağ içerisinde yer alan farklı makinelere ve bunların sunduğu hizmetlere taleplerin bütünü kontrol altında tutar. Her bir makineyle ayrı ayrı ilgilenilmez. Bu yaklaşımda kullanılan ürünler; bir kuruluşa ait ağı, tüm ağdan ayıran güvenlik duvarları, mümkün olduğu kadar güçlendirilmiş kullanıcı belirleme mekanizmaları ve özel gizliliğe sahip olup da dış ağ üzerinden iletilmesi gereken bilgilerin başkaları tarafından ele geçirilip kullanılmasını engelleyecek olan şifreleme olarak sıralanabilir (Şahin 2005).

2.1.1 Ağ (Network) Nedir ?

Bilgisayar ağı, sahip olunan sayısal kaynakların paylaşılması için önemli bir araçtır; iki bilgisayar ve basit bir hub cihazıyla ağ oluşturabildiği gibi milyonlarca bilgisayarı kapsayan internet de bir bilgisayar ağıdır (Çölkesen 2012).

Ağ protokolleri; verilerin nasıl paketleneceğini, kullanılacağını ve ağdan iletileceğini belirten anlaşmalardır. Satıcılar ve endüstriyel komiteler, bu anlaşmaları geliştirirler ve firmalar bunlara uygun yazılımlar üretmeye çalışırlar. Bu tip yazılımların ilk denemelerinde bazı firmalar daha başarılıdır, fakat birkaç ay içerisinde deneme yanılma yöntemiyle yazılımlar doğru şekillerini alırlar (Derfler 2000).

OSI Modeli, herhangi bir donanım ya da network tipine özel değildir. OSI'nin amacı; network mimarilerinin ve protokollerinin, bir network ürünü bileşeni gibi kullanılmasını sağlamaktır (Mahler, 1999).

Bilgisayarlar arasındaki bağlantı, bakır tel üzerinden olabileceği gibi, fiber optik kablolar, radyo link sistemleri, haberleşme uyduları ve kısa mesafeler için kızılötesi iletişim sistemleri ya da radyo dalgaları ile haberleşen iletişim sistemleri üzerinden de sağlanabilir. Bilgisayar ağları fiziksel boyutlarına göre aşağıdaki türlere ayrılırlar:

- **Yerel Alan Ağları :** LAN'lar oda, bina ve kampus çapında ağlardır.
- **Kentsel Alan Ağları :** MAN'lar şehir çapında ağlardır.
- **Geniş Alan Ağları :** WAN'lar ülke ya da kıta çapında ağlardır.
- **Ağlararası İletişim :** Birden çok ağın bağlantısıyla oluşan internet gibi gezegen çapında ağlardır (Öner 2010).

2.1.2 Ağ Güvenliği Nedir ?

Büyük ağların güvenliği BT yöneticileri ve güvenlik analistleri için daima sorunludur. Büyük ağların ve üniversite ağlarının güvenliğini koruma işlemleri arasında büyük benzerlikler vardır fakat her ağın kendine göre sorunları ve zorlukları bulunmaktadır. Günümüzde eğitim-öğretim sektörü öğrencilerin eğitimini geliştirmek amacıyla bilişim teknolojilerine daha fazla önem vermektedir (Cuihong 2010).

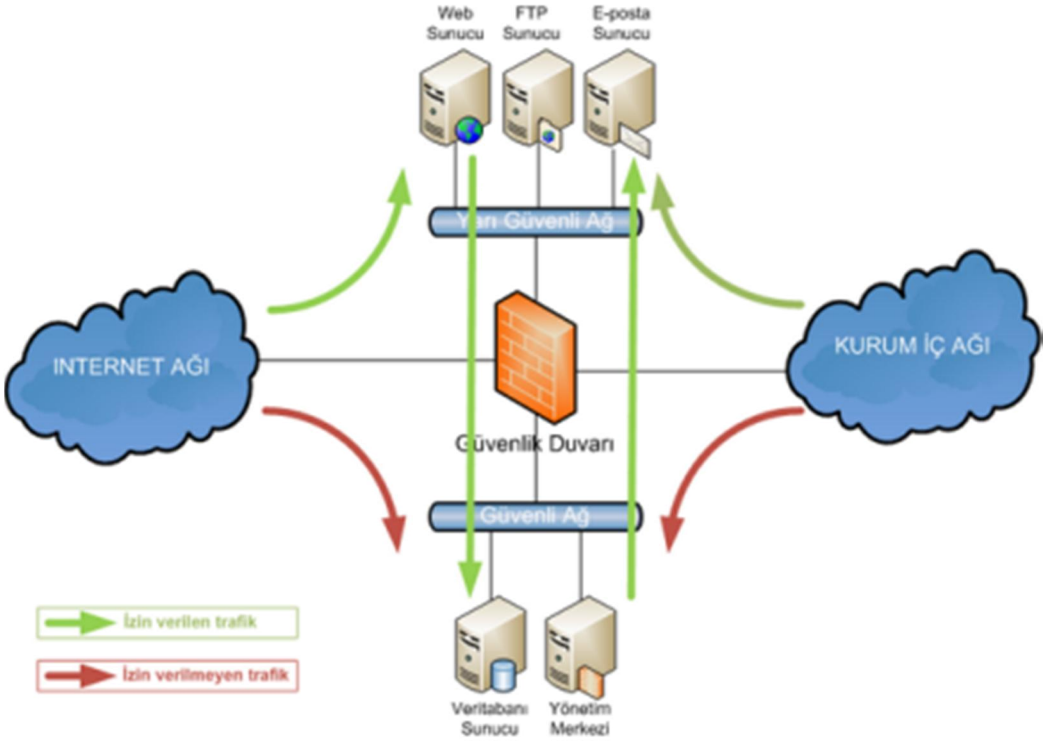
Ağ ortamlarının temelinde yatan paylaşım ve uzaktan erişim imkânlarının kullanılması sonucunda yeni güvenlik açıkları meydana gelmiştir. Bu açıklar, kötü niyetli veya meraklı kişiler tarafından kullanıldığında; bilgilere yetkisiz erişim, sistemler ve servislerin kullanılamaz olması, bilgilerin değiştirilmesi veya açığa çıkması gibi güvenlik ihlâlleri oluşmaktadır. Bilgisayar ağlarının yaygınlaşmasıyla güvenlik ihlâlleri artmış, bilgi güvenliği için alınması gereken önlemler fazlalaşmıştır (Gümüş 2010).

Güvenlik sisteminin tam ve etkili olması, genel katılımı gerektirir. Katılım; isteyerek ya da kural gereği olabilir. Kullanıcılar; güvenlik konusunda eğitilerek, katılımın isteyerek olması sağlanmalıdır. Sistem yöneticisi ya da güvenlikten sorumlu kişi her şeyi kontrol edemez. Kullanıcıların da karşılaştıkları farklı durumları sistem yöneticisine bildirmesi gerekir. Ayrıca kullanıcılar şifre seçiminde titiz davranmalı ve şifrelerini periyodik olarak değiştirmelidirler.

Kurumlar; ihtiyaç duydukları güvenlik düzeyine ve mali güçlerine göre çeşitli güvenlik stratejilerinden bir ya da birkaçını seçerler. Fakat, bu stratejilerden her biri ağ güvenliği için çok önemlidir. Bunlardan yalnız bir ya da ikisine bağlı kalmak yerine her birinin belirli düzeyde gerçekleştirilmesi gerekir. Özetle, titiz bir çalışma gerektiren ağ güvenliğinde yetkiler uygun bir biçimde dağıtılmalı, ağa giriş ve çıkış noktasında trafik denetlenmeli, sistemin yalınlığına dikkat edilmeli, sistemdeki açıklar kontrol edilerek önlemler alınmalı, kullanıcılar eğitilmeli ve çeşitli düzeylerde kullanılacak yazılım ve donanım nitelikli kaynaklarla ağın güvenliği sağlanmaya çalışılmalıdır (Çakar 2005).

Metro Ethernet VLAN yapısı üzerine kurulu bir teknolojidir. VLAN fiziksel olarak aynı ortamı paylaşan veya aynı kablo üzerinden iletişim yapan yerel ağa bağlı kullanıcıları sanki farklı noktalardaymış gibi yapılandıran yönteme verilen isimdir. VLAN sayesinde kullanıcılar fiziksel bölgesinden bağımsız olarak gruplanabilir ve farklı ağlarda çalışıyormuş gibi bir yapılandırma yapılabilir. Bir LAN (Local Area Network) ağını, farklı VLAN'lar olarak ayırmak ve yapılandırmak tek başına bir güvenlik önlemi sayılmamakla beraber, güvenlik çalışmalarında yapılması gereken önemli bir adımı teşkil etmektedir. VLAN'lar tamamen yazılımsal bir işlemdir ve genellikle switch cihazlar üzerinde yapılandırılırlar ve bunun neticesinde daha esnek ve kullanışlı bir yapı sunulmaktadır (Dennis 2004).

Bu durum karşısında sistem yöneticileri Şekil 2.1'de de sunulduğu üzere ağ cihazlarını çok iyi konumlandırıp, uçtan uca güvenlik sistemlerinin uygulanması sağlanmalıdır.



Şekil 2.1 Ağ Topolojisi (İnt.Kyn.1)

2.1.3 Kablosuz Ağ (Network)

Kablosuz ağlar; Şekil 2.2'de görüldüğü üzere kablosuz cihazlar arasında ve kablosuz cihazlar ile geleneksel kablolu ağlar (kurumsal ağlar ve internet) arasında taşıma mekanizması olarak hizmet vermektedir. Kablosuz teknolojiler radyo frekansı ve IR frekansı arasında değişen dalga boylarına sahiptirler. Kablosuz ağlar çok çeşitlidir ancak kapsama alanına göre 3 gruba ayrılmaktadır. WWAN, WLAN ve WPAN'dır. WWAN 2G hücresel teknolojisi, CCPD, GSM ve Mobitex gibi geniş kapsama alanına sahip teknolojileri de içermektedir.

WLAN, 802.11, HiperLAN ve benzeri teknolojileri içeren kablosuz yerel alan ağlarını içermektedir. WPAN, Bluetooth, kızılötesi gibi kablosuz kişisel ağ teknolojilerini temsil etmektedir. Tüm bu teknolojiler elektromanyetik sinyalleri alır ve gönderir (Karygiannis, Owens 2002).

Şekil 2.2 Kablosuz ağlar (İnt.Kyn.2)

2.1.4 Ağ Cihazları

Yerel ağ cihazları ve OSI referans modelinin hangi katmanlarında çalıştıklarına dair bir özet. Çizelge 2.1 de görülmektedir.

Çizelge 2.1 Yerel Ağ (LAN) Cihazları (Aysal 2007)

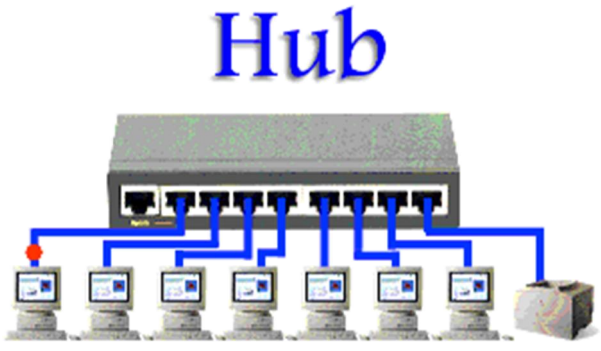
Cihaz	**OSI Referans Modeli**
Tekrarlayıcı	1. Katman (fiziksel)
Hub	1. Katman (fiziksel)
Köprü	2. Katman (veri iletim)
Anahtar	2. Katman (ver iletim) veya 3. Katman (ağ)
Yönlendirici	3. Katman (ağ)

2.1.4.1 Tekrarlayıcı (Repeater)

Bir verici (Transmilter) cihazı sinyalleri göndermek, alıcı (receiver) cihazı sinyalleri almak ve tekrarlayıcı (repeater) ise alıcı ve verici arasında yol alan sinyalleri kopyalamak veya güçlendirmek için kullanılan ağ cihazlarıdır.
Ayrıca Ethernet ağında kullanılabilecek mesafeyi arttırmak, ağa bağlı bilgisayar adedini arttırmak ve farklı kablo tipleri kullanan ağlan birleştirmek tekrarlayıcıların kullanım amaçlarıdır. Tekrarlayıcılar OSI referans modelinin fiziksel katmanında yer almaktadır. (Aysal 2007).

2.1.4.2 Hub

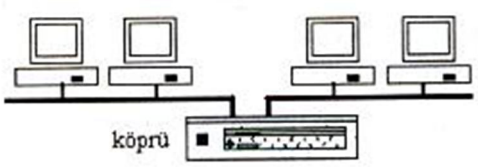
Hub, bilgisayarların ağda iletişim kurmasını sağlar. Şekil 2.3'de görüldüğü üzere her bilgisayar bir Ethernet kablosuyla hub'a bağlanır ve bir bilgisayardan diğerine gönderilen bilgiler hub üzerinden geçer. Hub kaynağı veya aldığı bilgilerin gönderilmesinin istendiği hedefi belirleyemez, bu nedenle bilgileri, bilgiyi gönderen bilgisayarı da içerecek şekilde kendisine bağlı tüm bilgisayarlara gönderir. Hub bilgi gönderebilir ve alabilir, ancak iki işlemi aynı anda yapamaz. Bu da, hub'ların anahtarlama cihazlarına göre daha yavaş olmasına neden olmaktadır. Hublar, ağ cihazları arasında en az karmaşık ve en az maliyetli olanıdır (İnt.Kyn.3).



Şekil 2.3 Hub (İnt.Kyn.4)

2.1.4.3 Köprü (Bridge)

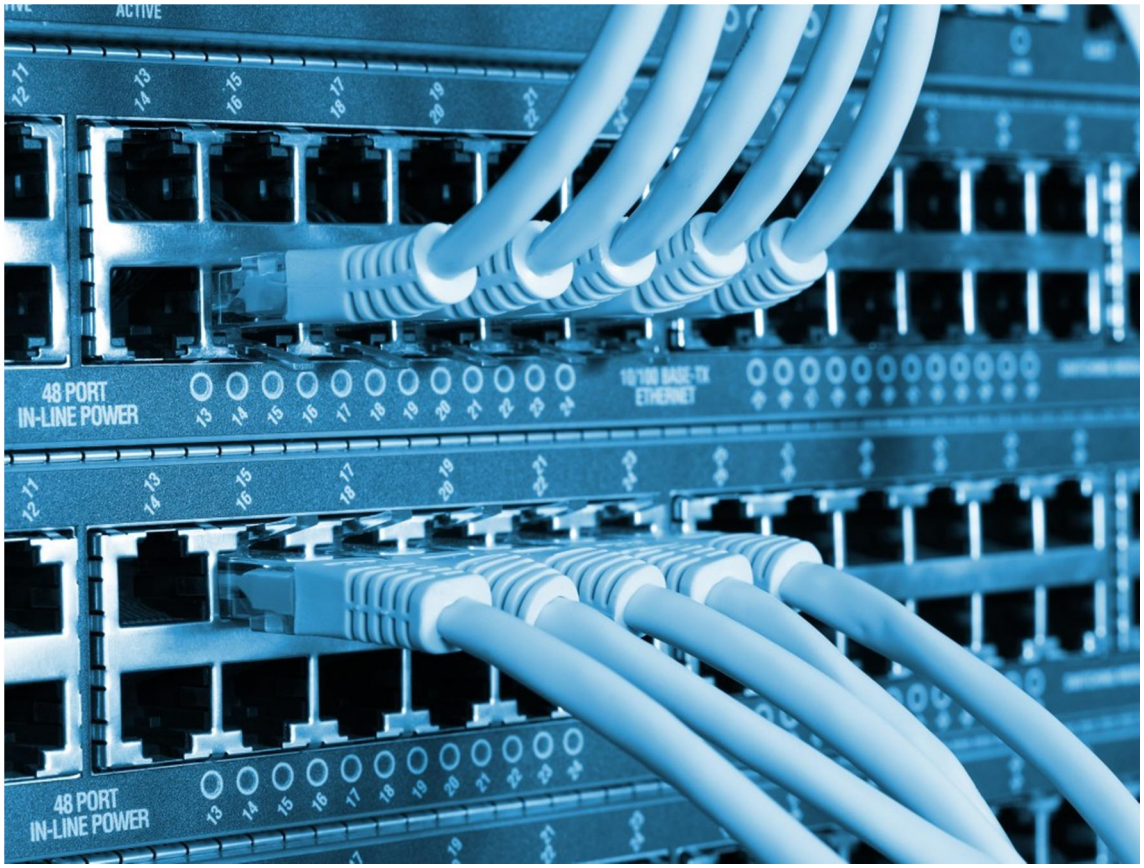
Köprüler, Şekil 2.4'de sunulduğu üzere iki benzer ağ bölümünü birbirine bağlamak için kullanılırlar. Köprüler, veri paketlerini fiziksel adresleri vasıtasıyla süzer ve iletir. Köprü cihazı bağlı olduğu ağın tüm bölümlerini dinler ve hangi fiziksel adresin hangi bölümde olduğunu gösteren bir tablo hazırlar. Bir bölümden bir veri iletilmek istendiğinde, köprü cihazı hedef adresin tablosunda yer alıp almadığını kontrol eder. Eğer hedef adresi tablosunda yoksa veriyi gönderildiği bölüm hariç tüm bölümlere iletir. Köprüler OSI modelinin veri iletim katmanında çalışırlar (Aysal 2007).



Şekil 2.4 Köprü (Bridge) (İnt.Kyn.5)

2.1.4.4 Anahtarlama (Switch)

OSI başvuru modelinin 2. Katmanında çalışan aktif (güç beslemeleri olan) aygıtlardır. Bu aygıtlar için anahtarlamalı bağlantı kutusu anlamına gelen "*Switching hub*" ya da çalıştığı OSI katmanını belirtmek için "2. Katman anahtarı *(layer-2 switch)"* adları da kullanılır. Anahtarlara bağlı bilgisayarlar farklı hızlarda çalışabilirler ve aynı anda birden fazla bilgisayarın çerçeve göndermesi durumunda çarpışma olmaz. Anahtara bağlı bilgisayarların tümü aynı anda ve anahtarın çalışma hızında (örneğin, 10 Mbps) veri gönderebilirler. Şekil 2.5 da görüldüğü gibi sadece anahtarlama cihazı üzerinden iletişim yapılan bir ağda bilgisayarlar ile anahtar arasında gönderme ve alma için ayrı iletim hatları kullanılır. Böylece, tüm bilgisayarlar aynı anda gönderme ve alma yapabilirler (Öner 2010).

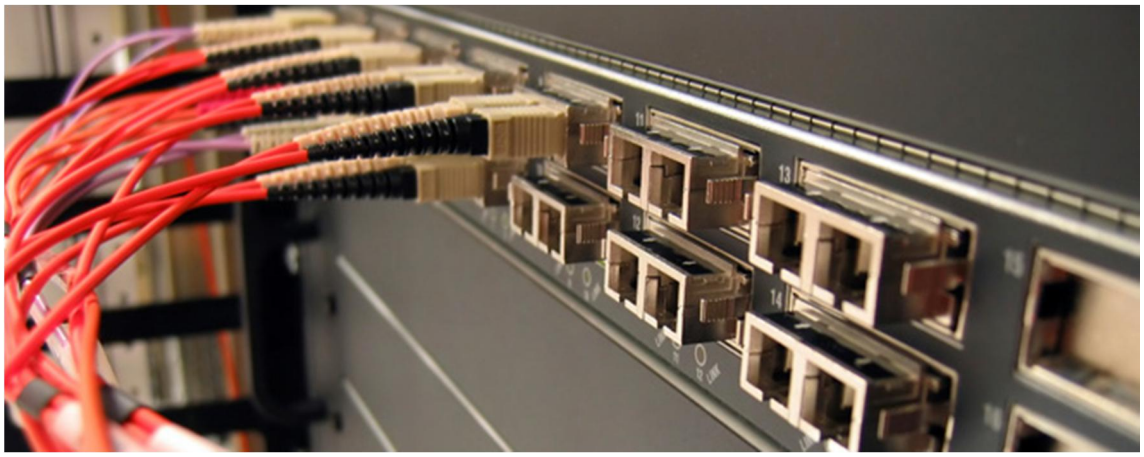


Şekil 2.5 Anahtarlama Cihazı (İnt.Kyn.6)

ACL (Access List) cihaz üzerine gelen paketleri yönlendirmek ya da silmek üzere inceleyen yazılımsal bir yapıdır. ACL karar mekanizması; kaynak IP adresi, hedef IP adresi, 3. Katman protokolü (ICMP ya da IP) ve üst katman port numaralarından oluşur. ACL oluşturulurken her bir kural satır şeklinde sırayla listeye tanımlanır. Bir koşul sağlandığında duruma göre pakete izin verilir ya da geri çevrilir (permit, deny). Tanımlama yaparken; her bir protokol için, her bir yön için (in, out) ve her bir uç için ayrı komut satırları uygulanır. Ağ sisteminin VLAN yapısından oluşması farklı portların ve farklı gurupların oluşturulabilmesine imkân tanır. Guruplar arası güvenlik yönetimi ve veri iletişim yapılandırmaları en verimli ACL kullanımı ile sağlanmaktadır (Ido 2007).

2.1.4.5 Omurga Anahtarlama (Backbone)

Yönlendirici (*router*); genel olarak LAN-WAN, LAN-LAN bağlantılarında veya vLAN'lar arası bağlantılarda kullanılır. Üzerinde LAN ve WAN bağlantıları için ayrı ayrı portlar bulunur. Örneğin, Şekil 2.6'da gösterildiği üzere bir router üzerinde bir adet LAN, en az bir adet WAN port modülleri takılır. ISP'lerde, çoğunlukla şaseli yönlendiriciler kullanılır. Böylece kolayca genişleme yapılabilmektedir.
Yönlendiricilerde çalışan ROS önemlidir. Hem kendi işlevini yerine getirmeli hem de ağda kullanılan protokol kümesini destekliyor olması gerekir. Bu amaçla TCP/IP ağlarda kullanılacak yönlendiricide IP protokolü, NetWare ağlarda kullanılacak yönlendiricide de IPX protokolü yüklü olmalıdır (Çölkesen 2012).



Şekil 2.6 Omurga Anahtarlama (İnt.Kyn.7)

2.2 Güvenlik Duvarları

Güvenlik duvarı, özel bir bilgisayar ağı ile internetin geri kalanı için bir noktada konumlandırılmış paket filtresidir. Güvenlik duvarı özel ağ ile internet arasında değiş tokuş edilen her paketi karşılamaktadır. Paket üstbilgisi alanlarını inceleyerek karar vermektedir. Ya paketin geçmesini sağlamaktadır. Ya da paketleri durdurmaktadırlar. (Acharya, Gouda 2011).

Güvenlik duvarı, bir sistemin özel bölümlerini halka açık bölümlerden ayıran, kullanıcıların ancak kendilerine tanınan haklar düzeyinde sistemden yararlanmasını

sağlayan çözümlerdir. Güvenlik duvarı belirli bir makinayı denetlemek için o makina üzerine (host-based) kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir.

Güvenlik duvarı, içeride birbirlerine güvenen, az korumalı makinaların olduğu bir kurum ağı ile dış ağlar (Internet) arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır. Güvenlik duvarları sadece dış saldırılara karşı sistemi korumakla kalmaz, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılmaktadır. Güvenlik duvarları, yazılımsal veya donanımsal güvenlik duvarları şeklinde olabilmektedir (İnt.Kyn.8).

2.2.1 Donanım Tabanlı Güvenlik Duvarları

Bilgisayar güvenliği, günümüz bilişim dünyasının en önemli sorunu haline gelmiştir. Virüsler, trojanlar, spamlar, saldırılar hızla artmaktadır. İnternetin yaygınlaşması ile bu zararlı uygulamalar ve ağın iş dışında başka amaçlarla kullanılması çok yaygınlaşmıştır. Bu nedenle antivirus ağ geçidi teknolojisi tüm büyük ağlar için zorunlu hale gelmiştir. Aksi takdirde bu zararlı uygulamaların verdiği zarar, sistemlerin kapalı olması, şifrelerin ve bilgilerin çalınması ve zaman kaybı gibi sorunlara yol açmaktadır.

Ayrıca yine büyük networkler için dışarıdan gelen saldırıları engelleyebilmek için saldırı tespit ve engelleme sistemleri gerekli hale gelmiştir.

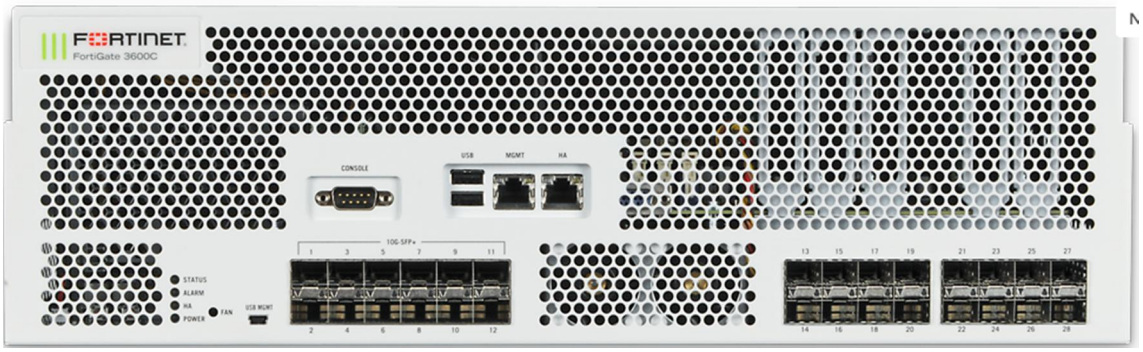
Kullanıcıların iş dışında başka şeylerle uğraşmalarını engellemek ve zararlı web sayfalarını önlemek için web filtreleme sistemlerine ihtiyaç vardır. Ağ trafiğini ve kullanıcıların zamanını oldukça alan bir diğer sorun spam maillerdir. Bunları da engelleyen anti spam teknolojileri hızla gelişmektedir.

Günümüzde çeşit çeşit marka ve teknolojide çözümler bulunmaktadır. Ancak sektör, genel olarak tüm tehditleri engelleyen bütünleşik cihazlara yönelmektedir. Bütünleşik Güvenlik Cihazları, güvenlik duvarı cihazı piyasasında gelişen bir eğilimdir. Bu amaçla birçok marka tüm tehditleri tek cihazda engelleyebilen "Bütünleşik Güvenlik Sistemleri" ürünler çıkartmaya başlamıştır. Bu sayede hem merkezi ve kolay kontrol

sağlanmakta hem de lisans maliyetleri farklı teknolojileri parça parça almaya kıyasla daha ucuz olmaktadır. UTM, sadece saldırılara karşı koruyan geleneksel güvenlik duvarları ve VPN hizmetini değil, aynı zamanda çoklu sistemler tarafından kullanılan içerik filtreleme, spam mail filtreleme, saldırı tespit sistemi, casus yazılım engelleme ve ağ geçitinde anti virüs görevlerini de yürüten gelişmiş cihazlardır. Bu gibi görevler daha önce çoklu sistemler tarafından yerine getiriliyorlardı. UTM cihazları aynı zamanda tümleşik yönetim, kontrol, log tutabilme servislerini sağlarlar.

Ağ güvenliğini sağlayan güvenlik duvarlarının donanım yapısında bulunmayan özellikleri eklemek zorunlu olmaktadır. Böylece güvenlik duvarları "güvenlik duvarı cihazları" oldular. Bu noktada bütünleşik güvenlik cihazları devreye giriyor. Anti-virüs, içerik filtreleme, saldırı tespit sistemi ve spam filtrelemede kullanılan çoklu sistemler yerine, kurumlar yukarıda sayılan tüm özellikleri barındıran tek bir ağ cihazını UTM güvenlik cihazı olarak alabilirler.

UTM güvenlik cihazları, çoklu tehditlere karşı kapsamlı güvenlik sağlamaktadır. UTM tümleşik paketinde tipik olarak bir güvenlik duvarı, antivirüs yazılımı, içerik filtreleme ve spam filtreleme özellikleri bulunur. Ek olarak ağ geçidi, saldırı tespit ve engelleme sistemini de tek bir platformda toplar. UTM cihazı, karmaşıklığı indirgeyerek kullanıcıları karışık tehditlerden korumak için tasarlanmıştır.



Şekil 2.7 UTM Forinet Firewall (İnt.Kyn.9)

Bütünleşik güvenlik cihazı ilk defa uluslararası veri şirketi tarafından güvenlik özelliklerini tek bir cihazda birleştiren güvenlik cihazları kategorisini tanımlamak için

kullanılmıştır. UTM sağlayıcıları Şekil 2.7'de görüldüğü gibi Fortinet, Sonicwall, Palo Alto ve Juniper olarak sıralanabilir.

UTM'in temel avantajları kullanım basitliği, hızlı kurulum ve kullanımı ayrıca tüm güvenlik uygulamalarının eş zamanlı güncellenebilmesi yetenekleridir.

UTM ürünleri, internet tehditlerinin yapısı gereği karmaşık şekilde gerçekleşen gelişimine ve büyümesine ayak uydurabilir. Bu ise sistem yöneticilerinin çoklu güvenlik programları kullanımı ihtiyacını ortadan kaldırır.

Virüsler yaygınlaştıkça, kurumlar anti-virüs ağ geçidini takiben web içerik filtreleme ve daha sonra spam filtreleme yöntemlerini kullanmaktadırlar. Bu durum yöneticilere yüksek maliyetli, kurulumu ve kullanımı karmaşık sistemler getirmektedir.

Anti-virüs, Anti Spam, Web Filtreleme, IPS gibi güncelleme gerektiren bu tür sistemleri satın alırken dikkat edilmesi gereken en önemli noktalardan birisi yıllık güncelleme ücretidir. Her bir ürün ayrı ayrı güncellendiğinde güncelleme ücreti çok fazla olmaktadır. Ürün tek merkezden birçok sıkıntıyı engelleyerek network performansının artmasını, network personelinin başka işlere vakit ayırabilmesini, personelinin iş dışında başka şeylerle uğraşmasının engellenmesini sağlayacağından ödenen ücretlerin kat kat fazlasını kısa sürede çıkartabilmektedirler.

- Bir UTM cihazı kullanmanın avantajları nelerdir?

Birçok harika yazılım tabanlı güvenlik uygulamaları piyasada çoktan varken neden insanlar tehdit yönetimi güvenliği cihazlarını satın alıyorlar?
Tehdit yönetim güvenliği cihazları piyasası büyük oranda şunlardan dolayı büyüyor:

- **Daha az karmaşıklık:** Hepsi bir arada yaklaşımı ürün seçimini, ürün entegrasyonunu ve sürekli desteği kolaylaştırıyor.
- **Kolay kurulum:** Müşteriler veya daha çok bayii ve sertifikalı kişiler ürünleri kolayca kurabilir ve kullanabilirler. Bu süreç artan bir şekilde uzaktan yapılmaktadır.
- **Sorun giderme kolaylığı:** Bir kutu hata verdiğinde sorun gidermektense yedekli kullanım ile bu sorun aşılabilir. Bu süreç sistemi daha hızlı şekilde çalışır

duruma geçirir ve teknik personel olmayan bir kişi de bu işlemi gerçekleştirebilir. Bu özellik özellikle teknik elemanları olmayan uzak ofisler için önemlidir.

Ayrıca önerilen bu cihazların aşağıdaki ek avantajları bulunmaktadır:

- **VPN :** Dışarıdan, örneğin evden internete bağlanarak iç ağa şifreli bir network kanalı ile ulaşılabilir.

- **IM FILTERING :** Messenger gibi mesajlaşma uygulamaları belli kullanıcılara izin verilebilir veya yasaklanabilir.

- **P2P FILTERING :** Kullanıcılar arası veri alışverişini sağlayan, trafiği boğan ve zararlı içeriklerin de yayılmasına neden olan P2P uygulamalarını (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb.) kişi bazlı kısıtlayabilir veya komple engelleyebilir.
- **TRAFFIC SHAPING :** İşle ilgili uygulamalara ağda öncelik verilerek, Messenger gibi çok gerekli olmayan uygulamalara düşük bant genişliği ayrılabilir.

Bir UTM cihazını değerlendirirken göz önünde bulundurulması gerekenler nelerdir?

- Güvenlik kurulumunuzda bir açık olmadığından emin olun. Bir UTM cihazı internet tabanlı tehditlere karşı geniş kapsamlı güvenlik koruması sağlamaktadır.
- Bütünleşik Güvenlik Cihazı'nı tam olarak sağlayabilmek için cihazın güvenlik duvarı, anti-virüs filtresi, anti-spam filtresi, URL filtresi ve saldırı tespit sisteminin olması gerekmektedir.
- UTM cihazı kusursuz olmalıdır; anti-virüs filtresi veritabanı gibi bileşenler güncel ve kullanımı kolay olmalıdır.
- Bir UTM cihazı yılda 7 gün 24 saat çalışıyor halde olmalıdır. Ağınız için şeffaf koruma ve istikrarlı olmalıdır.
- Fiyatının karşılanabilir olması ve ürünün kapsamlı olması gerekmektedir (İnt.Kyn.10).

2.2.2 Yazılım Tabanlı Güvenlik Duvarları

Bu tip güvenlik duvarları, genellikle kişisel ve sunucu bilgisayarları üzerine kurulabilen ve işletim sistemi ile bütünleşik olarak çalışan yazılımlardır. Bu yüzden bu tür güvenlik duvarları işletim sistemine bağımlıdır. Bir işletim sisteminde çalışan bir güvenlik duvarı diğerinde çalışmayacaktır.

Bu tip güvenlik duvarlarına örnek olarak birçok kişisel ve kurumsal güvenlik duvarı verilebilir. Kişisel ve ev kullanıcısı için güvenlik duvarı örnekleri olarak Symantec Norton Personal Firewall, Conseal PC Firewall, ZoneLabs Zone Alarm, Sygate Personal Firewall verilebilir. Hem kişisel hem de kurumsal olarak kullanılan birkaç güvenlik duvarı daha ayrıntılı olarak incelenecektir.

Bu tür güvenlik duvarları açık kaynak kodlu veya kapalı kaynak kodlu olabilir. Açık kaynak kodlu olanlar tamamen ücretsiz olup GPL (Genel Kamu Lisansı) lisansıyla dağıtılırlar. Kısaca, GPL, FSF tarafından geliştirilen ve kamunun kullanımına sunulan bir bilgisayar lisansıdır. GPL pek çok özgür yazılım tarafından kullanılmaktadır. GPL'in en fazla kullanıldığı platformlardan birisi Linux işletim sistemidir.

Bir yazılımı GPL altında yayınlamak, yazara telif hakkı güvencesi altında, yazılımının başkaları tarafından özgür yazılım felsefesine aykırı olarak dağıtılamayacağı güvencesini verir. Kapalı kaynak kodlu ürünlerin tüm telif hakkı ise üretici firmaya ait olmakla beraber kullanmak isteyen kişi ve kuruluşun ilgili firmadan belirli bir ücret karşılığında ürünün lisansını alması gerekir. Alınan ürün hiçbir şekilde başka bir kişiye verilemez, üzerinde değişiklik yapılamaz ve sadece lisans sözleşmesinde yazan şekilde kullanılabilmektedir (Karatabak 2006).

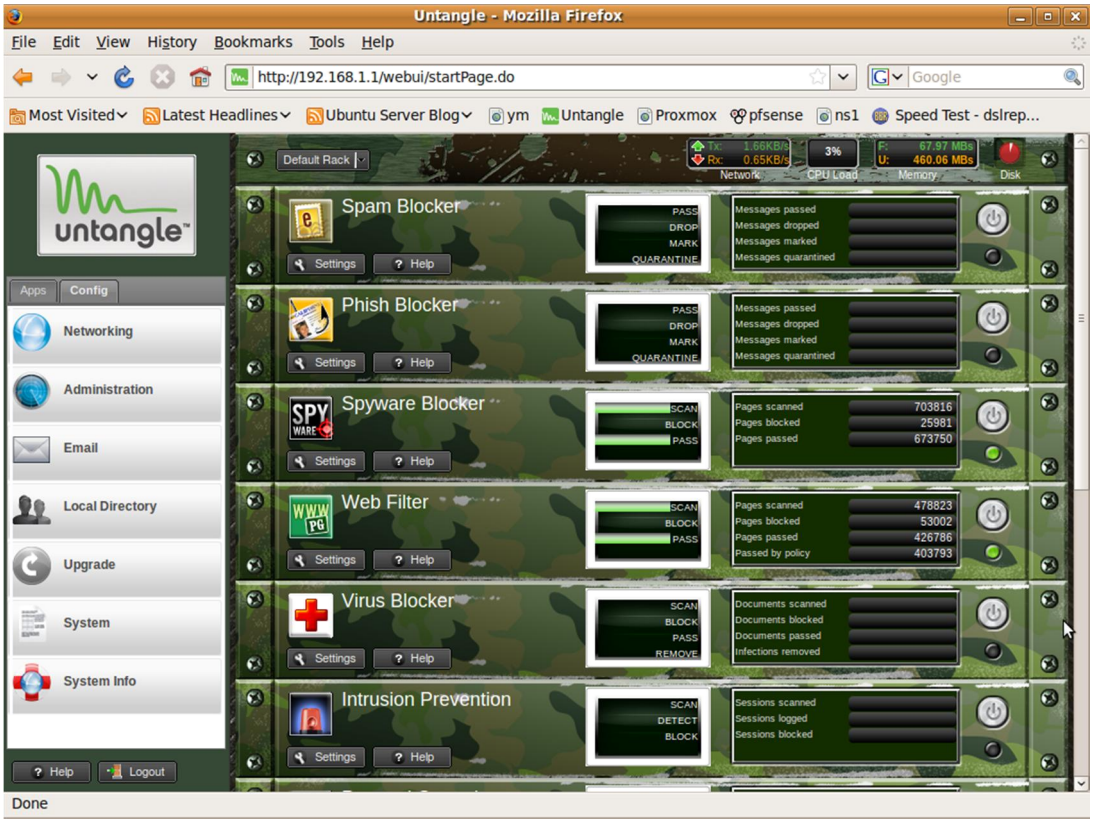
Her ne kadar ticari ürünler kadar başarılı imzaları olmadığı söylense de açık kaynak kodlu yazılımlarla ciddi anlamda ağ trafiğini düzenleyebilmek mümkündür. Açık kaynak kodlu yazılımların önemi imza üreticisinin olmaması, kendi imzalarınızı yazabilir ve maliyetlerin ortadan kaldırılması olarak belirtilebilir. Ayrıca ticari ürünlerin bazı ciddi olumsuzlukları da bulunmaktadır. Yanlış yüklenen bir imzanın ağınızda ciddi sıkıntılar ortaya çıkarması olası yaşanacak

senaryolardandır. Bu gibi durumlarda kapalı kutunun üretici firmasının sorunun neden kaynaklandığını bulup uygun çözüm üretmesi beklenmektedir (İnt.Kyn.11).

2.2.2.1 Untangle Güvenlik Duvarı

Untangle ürünü, Untangle adlı firma tarafından kendi ürettiği açık kaynak kodlu güvenlik yazılımı olarak ücretsiz sunulmaktadır. Untangle ürünü önce ticari olarak piyasaya sunulmuştur. Satış amacı güden bir ürün olarak piyasada bulunması sebebiyle, Untangle özellik ve satabilite açısından, birçok açık kaynak kodlu güvenlik duvarı yazılımlarına oranla daha güvenilirdir.

2007 yılında Untangle firmasının CEO'su Bob Walters, firmanın bu yazılımı satmaktan vazgeçtiğini artık sadece sattığı yazılıma destek vereceklerini açıkladı ve böylece Untangle, açık kaynak kod ürünlerinin içine dahil olmuştur. Untangle, Şekil 2.8'de gösterildiği gibi Premium Package, Standard Package, Education Premium, Education Standard ve Lite Package paketleriyle kullanıma sunulmuş durumdadır. Lite Package, ücretsiz kullanılan pakettir. Bu pakette küçük-orta ölçekli (50-150 kullanıcı) bir firmanın temel firewall ihtiyaçlarını rahatlıkla karşılayabilmektedir (İnt.Kyn.12).



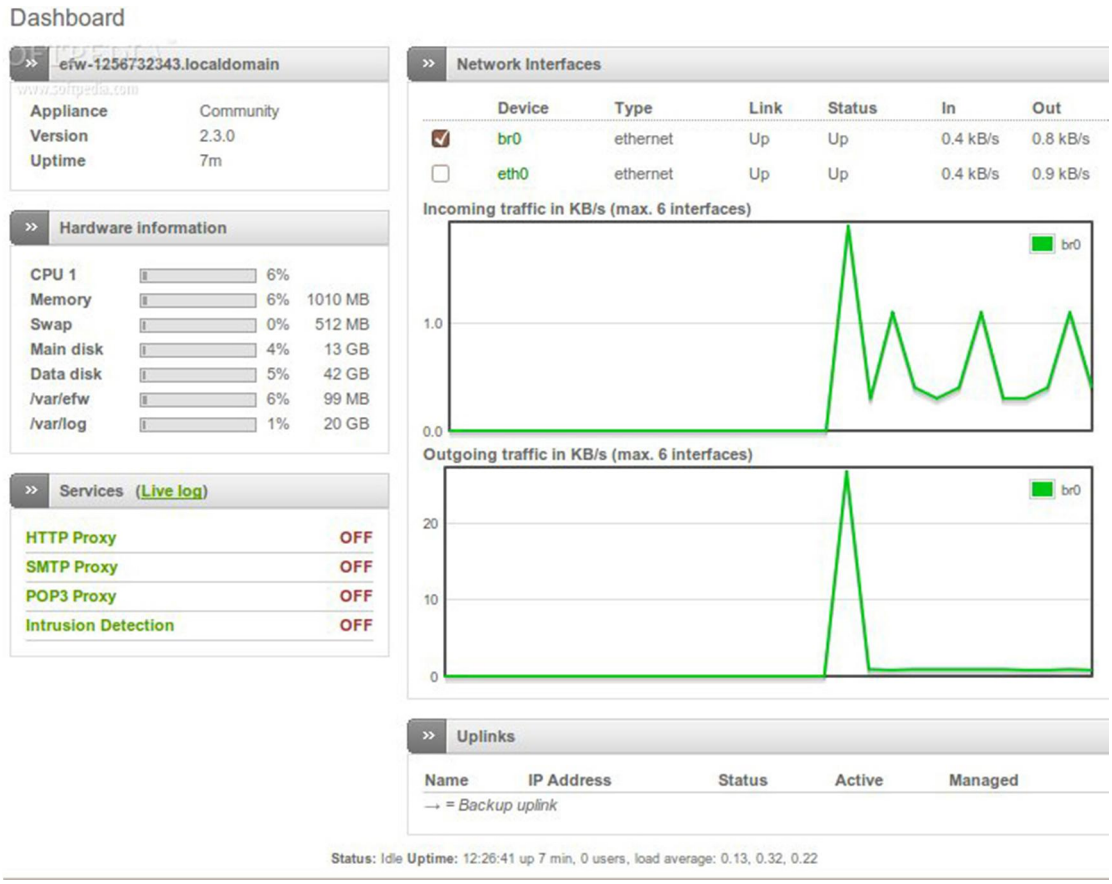
Şekil 2.8 Untagle Güvenlik Yazılımı (İnt.Kyn.13)

2.2.2.2 Endian Güvenlik Duvarı

Endian açık kaynak kodlu güvenlik yazılımı, Linux tabanlı bir dağıtım olarak, oldukça gelişmiş ve yetenekli bir güvenlik duvarı dağıtımıdır.

Endian öncelik olarak firewall ve içerik filtreleme olmak üzere pek çok amaca hizmet verebilecek bir yapıya sahiptir. AntiSpam, Vpn, Paket Filter gibi bir çok özelliği vardır. Şekil 2.9'da gösterildiği gibi endian oldukça sade bir web yönetim paneline sahiptir. Kullanışlı ve kolay bir yapıya sahiptir. Türkçe desteği bulunmaktadır (İnt.Kyn.14).

Ancak endian da, untangle gibi ücretli versiyonlarında tam sürümü kullanılabilmektedir.



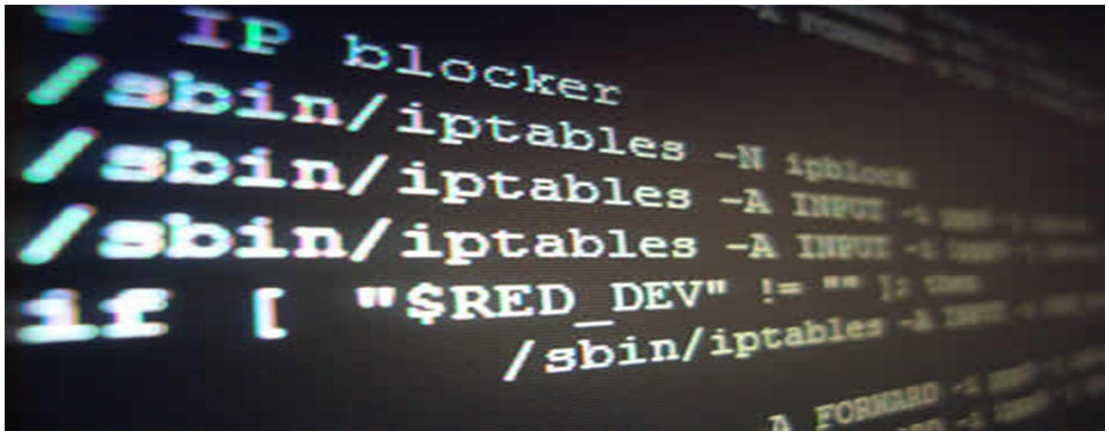
Şekil 2.9 Endian Güvenlik Yazılımı (İnt.Kyn.15)

2.2.2.3 İptables Güvenlik Duvarı

IP paketlerinin filtrelenmesi çekirdek düzeyinde gerçekleşir. Filtreleme belirli katmanlardan oluşur, bu katmanlara zincir denir. Ön tanımlı olarak üç tane zincir vardır: INPUT, OUTPUT ve FORWARD. Her zincir içerisinde kurallar vardır. Bu kurallar tanımlanma sırasına göre işletilir. Gelen paketler ilk olarak INPUT zincirindeki kurallara tabii tutulur. Buradan geçmesine izin verilenler FORWARD zincirindeki yönlendirme kurallarından süzülür. Eğer bir yönlendirme yapılacaksa paket burada değişikliğe uğratılır. Son olarak OUTPUT zincirindeki kurallara göre filtreleme yapılır. Bu üç zincir içerisinden elenmeyen paketlerin çıkışı sağlanmış olur. Çekirdekteki bu ön tanımlı zincirler silinemezler. Yeni zincirler eklenebilir, ancak çoğunlukla bunlar yeterlidir.

İnternet'ten gelenler ve gidenlerde ilk INPUT, son olarak OUTPUT zincirinde irdelenir. INPUT ve OUTPUT Internet'ten giriş veya çıkış olarak algılanmamalıdır.
Paketler bir zincire geldiğinde buradaki kurallar onun üzerine uygulanır. Bu kurallar ile ya paketin yoluna devam etmesine (ACCEPT) ya da durdurulmasına (DROP) karar verilir. Bu kararlara politika denmektedir.

İptables, Şekil 2.10'da sunulduğu üzere kullanıcı düzeyinde oluşturulan kuralların ya da yeni zincirlerin çekirdeğe gönderilmesi için kullanılan bir programdır. Oldukça geniş ve kapsamlı bir kullanıma sahiptir (Başer 2004).



Şekil 2.10 İptables Güvenlik Duvarı (İnt.Kyn.16)

2.3 Saldırı Tespit ve Engelleme Sistemi

Saldırı tespit sistemlerinin temel amacı ağa yapılan saldırıları tespit edip kayıt altına almak ve sistem yöneticisine gerekli uyarılarda bulunarak saldırıya karşı zamanında gerekli önlemlerin alınmasını sağlamaktadır. İlk saldırı tespit ve engelleme sistemleri, saldırıları ancak log kayıtlarını inceleyerek tespit edebilecek kapasitedeydi.

Günümüzde; yeterli işlem hızları nedeniyle saldırı log paketlerinin incelenmesi sadece saldırı sonrasında değil gerçek zamanlı ve saldırı tespit edildiğinde uyarı verecek şekilde yapılabilmektedir (Fuchsberger, 2005). Bu uyarma mekanizması olay kayıtları tutma, e-posta gönderme, çağrı bırakma, belli programları çalıştırma veya diğer şekillerde olabilir.

Saldırı engelleme sistemi ise saldırıları tespit etme yanında bu saldırıların durdurulmasını da sağlayarak saldırının ağ sistemini etkilemesini engellemektedir. Saldırı tespit/engelleme sistemleri hem yazılım hem de donanım tabanlı olabilmektedir (Tübitak Uekae 2009).

2.3.1 Donanımsal Tespit ve Engelleme Sistemi

Bir ağ tabanlı ihlal tespit sistemi genellikle ağın iç tarafına yerleştirilir ve oluşabilecek saldırılara karşı ağ paketlerini analiz eder. Bir NIDS ağın belirli bir bölümünden port mirroring gibi yöntemlerle tüm paketleri alır. Şüpheli davranış örneklerine göre trafiği analiz eder ve elde edilen bulgulardan dikkatlice sonuç çıkarır. Birçok NIDS faaliyetlerinin kayıtlarını tutma, rapor verme ve alarm üretme özellikleri ile donatılmışlardır. Şekil 2.11'de gösterildiği gibi üzerinde çok sayıda sfp ve bakır uca sahiptir. Ayrıca birçok yüksek performanslı yönlendiriciler de NIDS kabiliyetine sahip olabilmektedirler (Aysal 2007).

Şekil 2.11 IPS/IDS TippingPoint (İnt.Kyn.17)

2.3.2 Yazılım Tabanlı Saldırı Tespit ve Engelleme Sistemi

Bilgi güvenliği, toplumumuzda önemli bir problem haline gelmiştir. Özellikle bilgisayar ağları güvenliği ağ kapsamına yetkisiz sızmaların önlenmesi ile ilgilidir. Saldırı tespit

sistemleri, (IDS) zararlı ve zararlı olmayan trafiği ayrıştırmak amacıyla kullanıcı aktivitelerinin ve ağ trafiğinin izlenebileceği bir araçtır. SNORT lisans gerektirmeksizin kullanılabilen örüntü tanıma prensibine göre çalışabilen bir IDS aracıdır (Gómez, Gil, Padilla, Banos, Jimenez 2009).

Snort, 1998 yılında Martin Roesch tarafından geliştirilmiş bir ağ sızma tespit/engelleme sistemidir. GNU lisansı ile dağıtılan, açık kaynak kodlu ve ücretsiz bir yazılım olan Snort, şu anda Martin Roesch'un kurduğu Source fire firması tarafından geliştirilmektedir. Yazılım, çeşitli Linux dağıtımları, Windows ve MAC gibi pek çok işletim sistemi üzerinde çalıştırılabilmektedir. Snort yazılımını temel alarak grafik arayüz desteği ile çalışacak şekilde geliştirilen bağımsız şirket yazılımları da mevcuttur. Bu yazılımlar yönetim, raporlama, günlükleme gibi işlevleri yerine getirmektedir.

Snort'un mimarisi performans, basitlik ve esnekliğe dayalıdır. Snort IP ağları üzerinde gerçek zamanlı trafik analizi ve paket loglaması yapabilen bir yazılımdır. Yazılım protokol analizi, içerik tarama/eşleme yapabildiği gibi, arabellek taşması, port taraması, CGI saldırısı, işletim sistemi parmak izi denemesi gibi pek çok saldırı ve zararlı/şüpheli yazılım çeşidini tespit edebilmektedir. Snort üzerinden geçen tüm trafiği tanımlamak için kullanıcı tarafından da tanımlanabilen esnek kural dilini kullanır; bunun yanı sıra modüler takma-program mimarisini kullanan tespit motoru da bulunmaktadır. Snort'un gerçek zamanlı alarm mekanizması vardır. Bu mekanizma Windows istemcilerine WinPopup pencereleri çıkarabilir, Linux türevlerinde alarm mekanizmalarını syslog'a dahil edebilir, ya da özelleştirilmiş günlük dosyasında alarmları biriktirebilir.

Snort mimarisinin 3 temel bileşeni vardır: paket çözücü, tespit motoru ve günlükleme/alarm alt sistemi. Snort temel olarak uygulama seviyesine kadar tüm katmanlardaki veriye bakar ve bu veri içerisinden belirli trafiği toplar; kullanıcı ya da geliştirici tarafından tanımlanabilen kural setlerini uygulayarak bulduklarını değerlendirir.

Snort temelde 3 ayrı modda çalışabilecek şekilde yapılandırılabilir:

- **Paket İzleyici modu** (packet sniffer): Bu mod tcpdump paket izleyici programı gibi basit bir şekilde ağdan paketleri okuyup sürekli bir şekilde konsola akıttığı moddur. Konut satırında

./snort -v

şeklinde çalıştırılabilir; bu şekilde sadece TCP paket başlık bilgilerini ekrana yazmaktadır.

- **Paket Günlükleme modu** (packet logger): paketleri diske yazar. Komut satırında

./snort -dev -l ./log

komutu ile çalıştırılabilir. Burada TCP paket başlık ile birlikte paket bilgilerini de kaydeder ve /log dizinine günlükler.

- **Ağ Sızma Tespit/Engelleme Sistemi modu** (NIDS/NIPS): Snort'un en karmaşık ve yapılandırılabilir modudur. Snort bu modda temel olarak trafiği analiz edip kullanıcı tarafından tanımlanabilen bir kural seti ile gördüklerine karşı çeşitli eylemler gerçekleştirebilir. Örneğin komut satırında

./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf

ile çalıştırıldığında snort temel bir NIDS olarak çalışır ve snort.conf dosyasındaki kural seti uyarınca işlem yapar. Eğer snort "inline" modda çalıştırılırsa (./snort -Q) snort IPS olarak davranır ve drop paket düşürme (drop) kurallarını da devreye alır.

Kural Yazması:

Snort kuralları basit bir şekilde yazılabilmesine rağmen zararlı/şüpheli trafiği tespit etmede oldukça başarılıdır.

Snort kuralları mantıksal olarak iki kısma ayrılmaktadır:

kural başlığı ve **kural opsiyonları**.

Kural başlığı; kural eylemini, protokolü, kaynak IP adresi, hedef IP adresi, alt ağ maskeleri ile kaynak ve hedef port bilgilerini içerir.

Kural opsiyonu; kural eylemi takınılacaksa paketin hangi kısımlarının inceleneceğini belirler. Kural eylemi 8 şekilde olabilir:

- **Pass (Geçir):** Paketi basit bir şekilde geçirilir.
- **Log (Günlükle):** Günlükleme rutini kullanıcı tarafından ne tanımlandı ise tam paket olarak kaydedilir.

- **Alert (Alarm):** Kullanıcı tarafından belirlenen metotla bir olay bildirisi yaratır ve tüm paketi günlükler.
- **Activate (Etkinleştir):** Alarm ver ve ardından başka bir dinamik kuralı etkinleştirir.
- **Dynamic (Dinamik):** Bir kuralı etkinleştirinceye kadar boşta kalır, sonra günlükle beraber olarak çalışır.
- **Drop (Düşür):** Paketi düşür ve günlükler.
- **Reject (Reddet):** Paketi engeller, günlükler, protokol TCP ise *TCP yeniden başlat (TCP reset)* ya da*ICMP port erişilemez* mesajı yollar.
- **Sdrop (Günlüklemeden Düşür):** Paketi düşürür ve günlüklemez.

Kural setleri Şekil 2.12'de gösterildiği gibi periyodik olarak Snort geliştirici grup tarafından Snort resmi web sitesinden yayınlandığı gibi, kurallar kullanıcılar tarafından da oluşturulabilmektedir (İnt.Kyn.18).

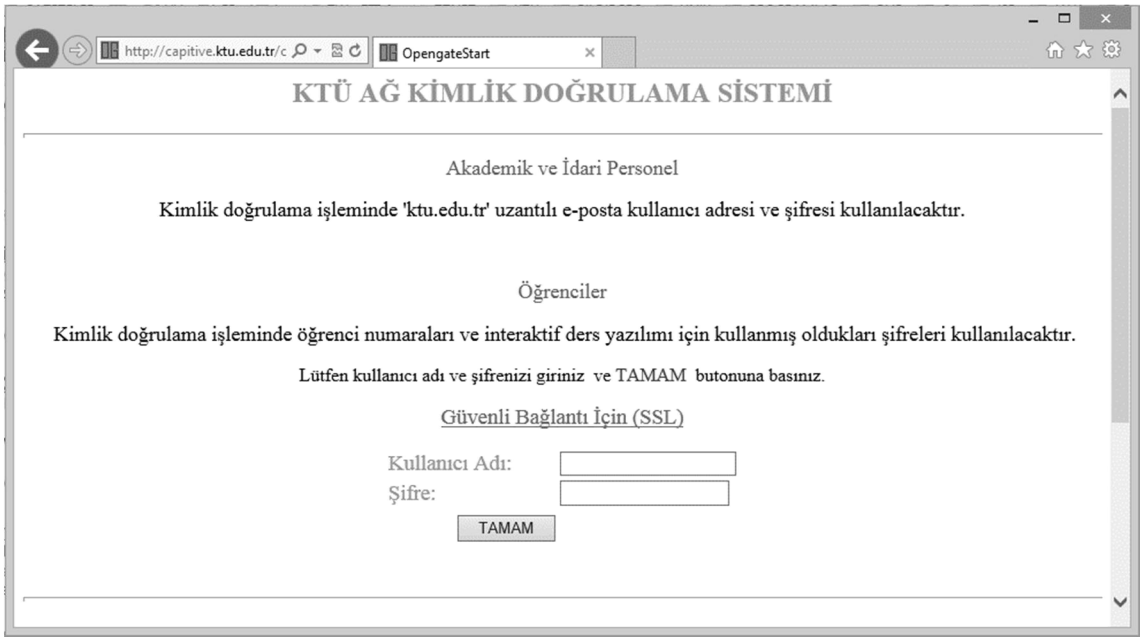
SID	Proto	Source	Port	Destination	Port	Message
549	tcp	$HOME_NET	any	$EXTERNAL_NET	8888	P2P napster login
550	tcp	$HOME_NET	any	$EXTERNAL_NET	8888	P2P napster new user login
551	tcp	$EXTERNAL_NET	any	$HOME_NET	8888	P2P napster download attempt
552	tcp	$EXTERNAL_NET	8888	$HOME_NET	any	P2P napster upload request
1432	tcp	$HOME_NET	any	$EXTERNAL_NET	any	P2P GNUTella client request
556	tcp	$HOME_NET	any	$EXTERNAL_NET	any	P2P Outbound GNUTella client request
557	tcp	$HOME_NET	any	$EXTERNAL_NET	any	P2P GNUTella client request
561	tcp	$HOME_NET	any	$EXTERNAL_NET	6699	P2P Napster Client Data
562	tcp	$HOME_NET	any	$EXTERNAL_NET	7777	P2P Napster Client Data
563	tcp	$HOME_NET	any	$EXTERNAL_NET	6666	P2P Napster Client Data
564	tcp	$HOME_NET	any	$EXTERNAL_NET	5555	P2P Napster Client Data
565	tcp	$HOME_NET	any	$EXTERNAL_NET	8875	P2P Napster Server Login
1383	tcp	$EXTERNAL_NET	any	$HOME_NET	1214	P2P Fastrack kazaa/morpheus GET request
1699	tcp	$HOME_NET	any	$EXTERNAL_NET	any	P2P Fastrack kazaa/morpheus traffic
2180	tcp	$HOME_NET	any	$EXTERNAL_NET	any	P2P BitTorrent announce request
2181	tcp	$HOME_NET	any	$EXTERNAL_NET	any	P2P BitTorrent transfer
2587	tcp	$HOME_NET	4711	$EXTERNAL_NET	any	P2P eDonkey server response

Şekil 2.12 Pfsense Snort Uygulaması (İnt.Kyn.19)

2.4 Literartürde Yapılmış Bazı Çalışmalar

F. Cali, M. Conti ve E. Gregori tarafından yapılan "IEEE 802.11 WLAN: Kapasite analizi ve protokol genişlemesi" adlı çalışmada IEEE 802.11 WLAN standardının verimliğini araştırmışlardır. Protokol kapasitesi için analitik bir formül geliştirmişlerdir. Çalışmanın sonucu olarak IEEE 802.11 standardının en üst seviyedeki teorik kapasitesini bularak, bu kapasitenin ağ konfigürasyonuna bağlı olarak teorik sınırlardan çok farklı sınır değerlerde çalışabildiğini, uygun geri dönüş algoritması ile performansın teorik sınır değerlere yaklaştırılabileceğini ortaya koymuşlardır (Cali, Conti, Gregori 1998)

Ticari veya açık kaynak kodlu Captive Portal isimli yazılımlar ile ağ üzerinden Şekil 2.13'de gösterildiği gibi bir web tarayıcısı ile birlikte kimlik doğrulama işlemini gerçekleştirilebilmektedir. Ramazan Özgür DOĞAN ve Hayati TÜRE'nin geliştirmiş oldukları yazılımla açık kaynak kodlu Captive Portal sistemlerinin kullanıcılara getirmiş olduğu rutin işlemleri kolaylaştıran, web sayfasına giriş yapmadan makinalarına kurulu bir yazılım üzerinden kimlik kontrolünü gerçekleştirilebilmektedir (İnt.Kyn.20).



Şekil 2.13 Karadeniz Teknik Üniversitesi Captive Portal Uygulaması (İnt.Kyn.20)

Üniversiteler gibi büyük kurumsal ağlarda; çok sayıda kullanıcı farklı ihtiyaçları ile aynı anda internet hizmetini kullanmayı talep etmektedir. Kurumsal kullanıcı politikalarının kısıtlı olmaması veya uygulanamaması nedeniyle, bazı kullanıcılar tarafından aşırı band genişliği tüketimi gerçekleşmekte ve band genişliği yeterince etkin kullanılamamaktadır. Bu sebeple; peer to peer, Video Streaming, oyun vb. programların bağlantı/transferini, portlara bakmaksızın engelleyebilecek sistemlere ihtiyaç duyulmaktadır. Kurum ağına girip çıkan paketler üzerinde daha etkin yaptırımlar uygulayabilmek ve ağ kullanımının etkinliğini arttırabilmek için OSI uygulama katmanı (L7) seviyesinde güvenlik duvarı kullanımı önemli bir hal almıştır. Bu kapsamda bu tür bir çözüm için önerilen açık kaynak kodlu PFSENSE yazılımı kullanılabilmektedir (İnt.Kyn.21).

Ağ güvenliği yaklaşımı, güvenlik konusunda farklı olanaklar sunabilmektedir. Bir güvenlik duvarı kullanmak suretiyle yüzlerce, binlerce ve hatta on binlerce bilgisayarın bulunduğu bir sistemi, bilgisayarlardaki konak güvenliği seviyelerini dikkate almaya gerek kalmadan dış dünyadan korumak mümkün olabilmektedir. Bu çalışmada güvenlik duvarı kullanılarak istemcilere belirli kurallar kapsamında internet hizmeti verilmiştir (Deregözü 1999).

Bu çalışmada ise ağ güvenliğini ilgilendiren her türlü bileşen incelenmiş ve son zamanlarda dünya çapında hızla yaygınlık kazanan güvenlik duvarı ile VPN ve NAT uygulamaları ele alınmış, İstenilen hedefe ulaşabilmek için genel işaretleşme kavramları, modülasyon teknikleri ve iletim ortamları üzerinde durulmuş sonra yerel alan ağlarında TCP/IP ve katman güvenliği incelenmiştir (Yüksel 2007).

Diğer bir çalışmada ise 802.11g ağların performansı birden çok istemci ve bir erişim noktası ile kurulan bir ağ üzerinde inceleyen deneysel çalışmalar yapılmış, ağ trafiği ve belirlenen güvenlik katmanlarının uygulaması yapılmıştır. Bu deneysel çalışmanın sonucu ile doğrulama ve şifreleme sistemlerini barındıran bu katmanlı yapının performans üzerindeki etkisi izlenmiştir (Gürkaş 2005).

Gün geçtikçe daha fazla cihaz üzerinden internete giriş yapılmakta ve bu sayı hızlı bir şekilde artış göstermektedir. Bu durum karşısında kötü amaçlı kimseler tarafından sunuculara yetkisiz giriş denemeleri yapılmakta, bu kimselere karşı yapılabilecek ilk önlem güvenlik duvarlarındaki paket filter özelliğini kullanarak yetkilendirme yapılmalıdır (İnt.Kyn.22).

3. MATERYAL VE METOT

3.1 Materyaller

Yapılan tez çalışmasında aşağıdaki materyaller kullanılmıştır.

- Anahtarlama Cihazları
- Pfsense 2.0.2 Güvenlik Yazılımı
- Freeradius ve Rsyslog Sunucu
- PHP Programlama Dili
- OpenLdap Veritabanı

Bu çalışmayı HP BL460C ve HP DL380 G4 sunucuları üzerinde pfsense 2.0.2 güvenlik duvarı yazılımını ve Linux dağıtımı centos 5.8 işletim sisteminin kurulumu gerçekleştirilmiştir. Kullanıcıların kayıt olabilecekleri ve bilgilerini düzenleme yapabilecekleri form tasarımı php programlama dili kullanılarak tasarlanmıştır. İstemcilerin kullanıcı bilgileri openldap üzerinde tutulmaktadır. İstemcilerin sistem üzerinden kimlik doğrulaması için portal üzerinden Radius sunucu seçilmiştir. Radius sunucu için açık kaynak kod yazılım olan freeradius sunucu tercih edilmiştir. Sistem üzerinde oluşan istemci kayıtlarının tutulabileceği merkezi bir syslog sunucu tasarlanmış oluşan kayıtların imzalanıp saklanması gerçekleştirilmiştir.

3.1.1 Anahtarlama Cihazları

Yapılan bu çalışmada iki farklı anahtarlama cihazından faydalanılmıştır.

3.1.1.1 3Com S7900E:

Şekil 3.1'de gösterildiği gibi omurga anahtarlama cihazının üzerindeki yuvalara modül ilavesi ile cihaz daha kapsamlı çalışabilmektedir. Kampüs ağında ihtiyaç duyulan bütün vlan id'ler 7900E üzerinde oluşturulmuştur. istemcilerin uçtan uca birbiriyle haberleşebileceği fiber uçlar 7900E üzerinde sonlandırılmış, kenar noktalarda hangi vlan id'ler kullanılacak ise o vlan id'ler trunk olarak gönderilmiştir. 7900E, üzerinden geçen trafiği hedef adresine göre yönlendirmeler yapmaktadır. Ayrıca dhcp sunucunun

ip adresi 7900E üzerinde tanımlanmış, istemciler hangi vlan id'ye üye iseler o tanımlanan subnet aralığından bir ip alabilmektedir.

Şekil 3.1 3com 7900E Omurga Anahtarlama (İnt.Kyn.23)

3.1.1.2 H3c 5120 SI:

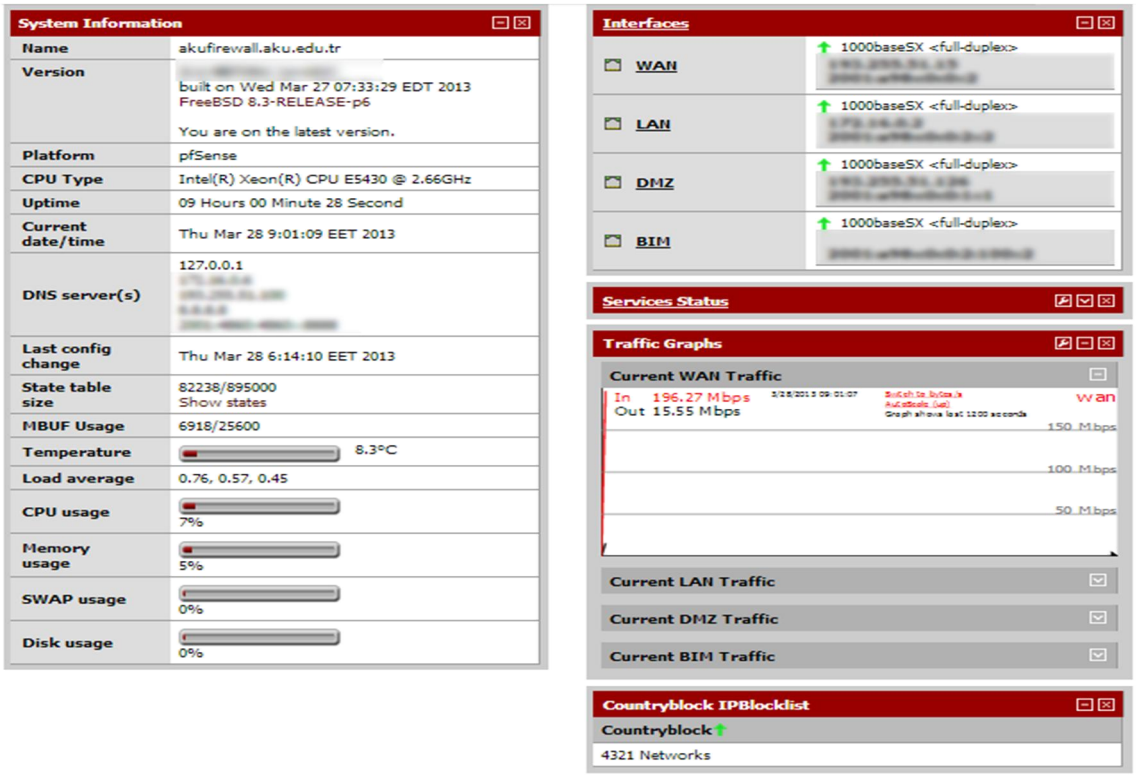
Uç noktalarda kullanılan anahtarlama cihazları olarak Şekil 3.2'de sunulan HP A5120 SI konumlandırılmıştır. Bu cihazlar L3 seviyesinde yönlendirme yapabilen, port bazlı ayar yapılmasını destekleyen yönetilebilir anahtarlama cihazlarıdır.

Şekil 3.2 HP 5120-SI Anahtarlama (İnt.Kyn.24)

3.1.2 Pfsense Güvenlik Duvarı

Yazılım tabanlı güvenlik duvarı olan pfsense'in, freebsd tabanlı özel geliştirilmiş bir güvenlik duvarı olması, web ara biriminden bütün ayarlarının yapılabiliyor olması, sistem üzerinde servislerin tamamının kurulumunun yapılabilmesi, daha da önemlisi GPL lisansıyla dağıtılabiliyor olması en önemli tercih sebebidir.

FreeBSD; açık kaynak kod güvenlik yazımları içerisinde en bilinen, ticari işletim sistemleri de olmak üzere diğer işletim sistemlerinde halen bulunmayan ağ yapılandırma, performans, güvenlik ve uyumluluk özelliklerini bir arada sunar. Donanım kaynaklarını etkin ve verimli kullanarak aynı anda binlerce kullanıcı prosesi için tepki zamanlarını en iyi seviyede tutar, çok ağır yükler altında dahi güçlü ağ servisleri sunmaya devam etmektedir. Yapılan karşılaştırmalı değerlendirmelerde Linux 2.6.22 veya 2.6.24 çekirdeklerine göre %15 daha fazla performansa sahip olduğu ortaya konulmuştur.



Şekil 3.3 PfSense Güvenlik Duvarı (Dashboard)

FreeBSD' nin Avantajları:

• Lisans gerektirmemesi

• Kullanıcı ve bağlantı bazlı lisans sınırlamasının olmaması

• Donanım kapasitesi ihtiyacı ve maliyetinin düşük olması

• Farklı işletim sistemlerine ve benzerlerine göre çok daha durağan, performanslı ve güvenli olması

• Uyumluluk probleminin bulunmaması

• İleri düzey yük paylaşım desteği

L7 seviyesinde güvenlik duvarı olarak çalışan birkaç dağıtım daha vardır. Bunları sayacak olursak Endian, Untangle, IPCop, OpenBSD PF, ebtables ve Bandwidth Arbitary gibi yazılımlar listelenebilir. Pfsense dağıtımı bu dağıtımlar arasından ön plana çıkaran temel özellikleri şu şekilde sıralanabilmektedir:

- L7 filtrelemede application pattern girebilir ve bu sayede dağıtımın desteklemediği patternler için paket filtreleme özelliğini kullanılmaktadır.
- Grafik arayüzünün basitliği sayesinde kullanıcı isterse ekstra modüller kurabilmektedir.
- Kurulabilecek modüller arasında IDS, Antivirus Gateway, Squid Proxy, ntop, trafik şekillendirme ve Vpn gibi yazılımlar sayılabilir.
- Modülleri web arayüzden aktive edebilir yada deaktive edebilmektedir.
- Yüksek boyutlu disklere kurulumu sırasında diski görmeme gibi sorunlar yaşanmamaktadır.
- Diğer Linux dağıtımlarındaki gibi kurulum sırasında grafik kartının tanınmaması gibi bir sorun ile uğraşmak zorunda kalınmamaktadır.
- Vlan desteği vardır.
- Birden fazla Wan ve Lan arayüzünü desteklemektedir.
- NAT, CARP, Load Balance, Packet Capture ve Bogon networkleri tanıma özellikleri ayrıca bulunmaktadır.

Pfsense özelleştirilmiş bir FreeBsd dağıtımıdır. Esas olarak güvenlik duvarı ve router olarak çalışmak üzere tasarlanmıştır. Şekil 3.3'de görüldüğü üzere pfsense, yüksek throughput senaryoları düşünülerek (500 Mbps) tasarlanmış bir dağıtımdır. Bu hızlarda çalışabilmesi için kullanacağınız yüksek kapasiteli bir donanım mimarisi kullanmanız gerekmektedir (İnt.Kyn.25).

3.1.3 Linux İşletim Sistemi

Sistemde kullanılan freeradius, ldap ve syslog gibi sunucular için centos işletim sistemi tercih edilmiştir.
Centos redhat firmasının ürettiği ücretsiz özgür kaynak yazılımıdır. Centos RHEL tabanlı sistem üzerine kurulmuş ve geliştirilmiştir. En fazla sunucu amaçlı kullanılmakla beraber Monolitic çekirdeğini kullanmaktadır. Centos ev amaçlı değil sunucu amaçlı kullanılması önerilmektedir.

- Sunucu için Centos ?

Şuan linux sunucuların büyük oranı centos dan oluşmaktadır. Linux tabanlı yazılan panellerin bir çoğu yine centos desteklidir. cpanel , plesk , kloxo gibi kontrol panelleri centos ile %100 uyumlu aktif olarak çalışabilmektedir (İnt.Kyn.26).

3.1.4 Kimlik Doğrulama

Kullanıcıların kimlik denetimini için Radius sunucu kullanılmıştır. Radius sunucu üzerine birden fazla ldap sunucu tanımlanabilmektedir. Böylece sistem güvenliği ve sistem yönetimi kolayca sağlanabilmektedir.

Radius; uzaktan başka ağlara erişim sağlayan kullanıcıların AAA (authentication, authorization, accounting) yani kimlik denetimi, yetkilendirme ve hesap verilerinin yönetimlerini yapmak üzere oluşturulmuş bir protokoldür. Bu protokol ilk olarak 1991 senesinde Livingston firması tarafından sunucu kimlik denetimi ve muhasebesi için geliştirilmiş, daha sonra IETF tarafından standartlaştırılmıştır. Gelişmiş destek ve yaygın kullanım ile ISS ve kurumlar tarafından İnternet, İntranet, kablosuz ağ ve bütünleşik e-posta servisleri erişimini yönetmek için kullanılmaktadır.

Radius, uygulama seviyesinde iletim için UDP kullanan bir sunucu/istemci protokolüdür. Ağ erişiminde kullanılan RAS, VPN sunucu gibi ağ geçitlerinde yoğunlukla kullanılır. Temel olarak üç işlevi vardır:

Kullanıcıların ağa erişimi sağlamadan önce kimlik denetimi bu kullanıcıların ya da cihazların ağda belirli servislere yetkilendirmesi bu servislerin kullanımının verilerinin hesabının tutulması FreeRADIUS: FreeRADIUS ise yukarıda bahsedilen RADIUS protokolünün, modüler, özellik açısından zengin ve yüksek performansla çalışan örneklerinden biridir. Açık kaynak kodlu bir yazılım olan FreeRADIUS, çeşitli işletim sistemlerinde çalışabilmektedir (AIX, Cygwin, FreeBSD, HP-UX, Linux, MAC OS-X, NetBSD, OpenBSD, Solaris gibi). Çoklu AAA sunucuları ile milyonlarca kullanıcıya hizmet veren geniş ölçekli uygulamaları da mevcuttur. Sunucu LDAP, SQL ve diğer veritabanlarını desteklemekte, 2001 yılından beri EAP, 2003'den beri de PEAP, EAP-TTLS desteği ile çalışmaktadır. FreeRADIUS şu anda bütün kimlik yetkilendirme protokollerini ve veritabanlarını desteklemektedir (İnt.Kyn.27).

Syslog; güvenlik duvarı üzerinden geçen trafiğin veya sistem üzerinde çalışan sunuculardan oluşan kayıtların merkezi bir log sunucu üzerinde toplanmasını ve openssl ile kayıtların imzalanıp saklaması yapılabilmektedir. Kurulumla ilgili bilgiler daha sonraki konularımızda verilecektir.

3.1.5 PHP Programlama Dili

Portal üzerinden çıkış yapacak istemcilerin tc kimlik no ile kimlik doğrulaması yapılarak sisteme kayıt yapabilecekleri bir sistem geliştirilmiştir.

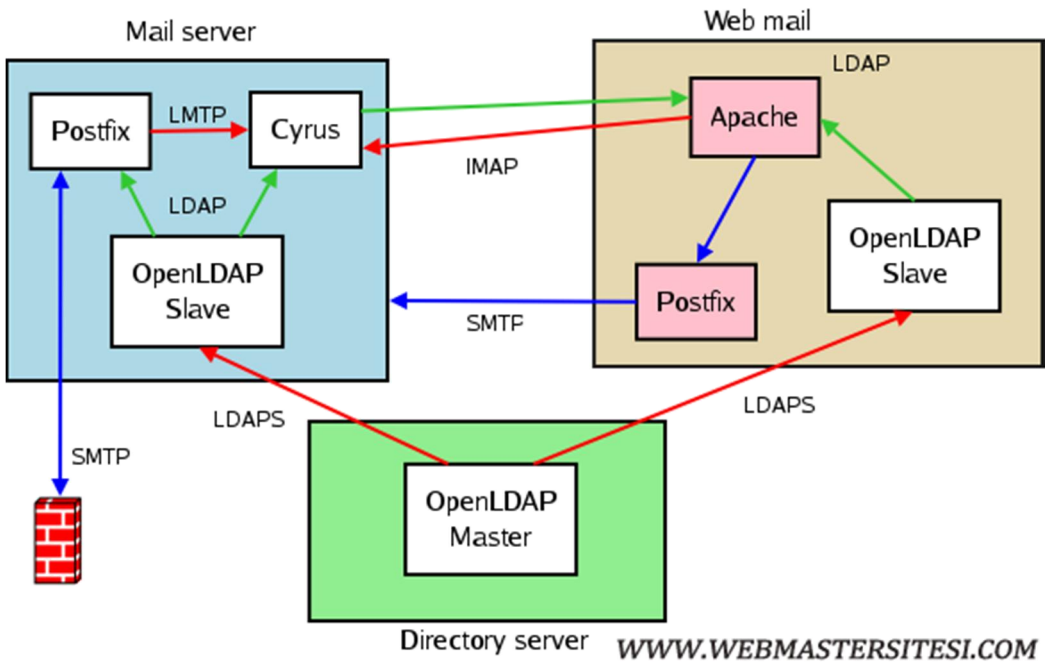
- Rasmus Lerdorf, 1994 yılında bir işbaşvurusu yaptığında kendisi ile ilgili bilgileri sergileyebileceği web ortamında bir personal homepage yapma amacıyla yola çıkarak PHP dilinin ilk versiyonunu ortaya çıkarmıştır.
- Başlangıçta büyük bir kısmı Perl dilinden alınmış olan bu dile daha sonraları bir form yoluyla ziyaretçiden gelen bilgileri işlemeyi sağlayan ekleri yazdı ve programın adı PHP/FI (Form Interpreter/ Form Yorumlayıcı) olmuştur.
- Rasmus Lerdorf, 1995'in ortalarında, Zeev Suraski, Stig Bakken, Shane Caraveo ve Jim Winstead ile bir grup kurdu ve PHP'yi Perl'den ödünç alma rutinlerle iş yapan bir paket olmaktan çıkartıp, Nesne-Yönelimli bir programlama dili haline getirilmiş.

- PHP ve açık kaynak olarak geliştirilmeye başlanan MySQL'in birlikte kullanıldıklarında yakaladıkları etkinlik binlerce dolar verilerek alınan veritabanı ve uygulama dilleriyle yarışmanın ötesinde farklılıklara sahip olmuştur (İnt.Kyn.28).

3.1.6 Kullanıcı Bilgileri

Sisteme giriş yapacak kişilerin giriş bilgilerinin tutulabileceği bir veritabanına ihtiyaç duyulmaktadır. Burada tercihen ldap veritabanı kullanılmış, personel kurum mailini kullanırken, öğrenci veya misafirlerin kullanıcı bilgileri ldap sunucu üzerinde tutulmaktadır.

OpenLDAP, LDAP'ın OpenLDAP Project tarafından geliştirilmiş bir uygulamasıdır. OpenLDAP Kamu Lisansı olarak bilinen BSD-türevi bir lisans kullanmaktadır. Platform bağımsız bir protokoldür. Kullanımda olan bir çok Linux dağıtımı, LDAP desteği için OpenLDAP yazılımını barındırır. OpenLDAP (Şekil 3.4), BSD dışında , AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows ve z/OS gibi sistemlerde de çalışabilir (İnt.Kyn.29).



Şekil 3.4 Open Ldap Sunucu (İnt.Kyn.29)

3.2 Metot

3.2.1 Ağ Cihazları Üzerinde Alınabilecek Güvenlik Önlemleri

3.2.1.1 Kimlik Denetimi (802.1X)

Kampüs ağında yönetilebilir anahtarlama cihazların bulunduğu noktalarda kablosuz bağlantı gibi kablolu bağlantılarda (Şekil 3.5) da 802.1x güvenlik protokolleri kullanılmaktadır. İstemciler Radius sunucu üzerinden kimlik doğrulması yapabilmeleri için anahtarlama cihazlarının güvenlik ayarları aşağıdaki şekilde tanımlanmıştır.

```
#
 dot1x
 dot1x authentication-method eap
#
#
radius scheme aku
 primary authentication [redacted]
 primary accounting [redacted]
 key authentication cipher $c$3$F4tkZ85PwAV5/9NED9KsxgbkgOp08pbMIBs=
 key accounting cipher $c$3$lNkvR8QxIYQAqdTqDdoewEINu11wRhGFtrU=
 user-name-format without-domain
#
domain aku.edu.tr
 authentication lan-access radius-scheme aku local
 authorization lan-access radius-scheme aku local
 authentication portal local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
#
interface GigabitEthernet1/0/1
 port access vlan 100
 broadcast-suppression pps 1000
 stp edged-port enable
 dot1x max-user 3
 dot1x guest-vlan 160
 undo dot1x handshake
 dot1x port-method portbased
 dot1x
 arp rate-limit rate 99 drop
#
```

Şekil 3.5 Hp A5120 SI 802.1X Uygulaması

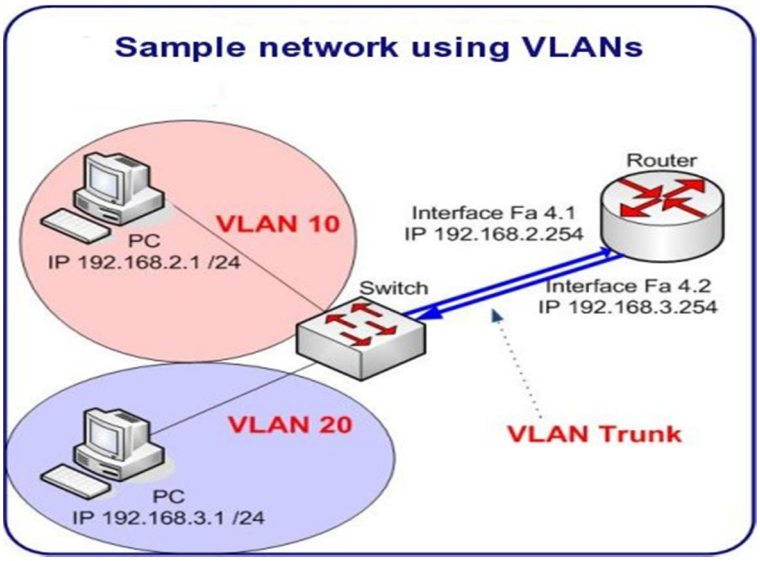
3.2.1.2 Kimlik Denetimi (Mac Authentication)

Kişilerin ağa bağlanabilmeleri için mac (fiziksel) adresleri sistem üzerinde bir veritabanı sunucusunda kayıtlı olmaları gerekmektedir. Anahtarlama cihazlarını aşağıdaki Çizelge 3.1'de gösterildiği gibi yapılandırarak mac authentication protokolü kullanılmaktadır.

Çizelge 3.1 Mac Kimlik Doğrulama

```
domain default enable system
#
mac-authentication
mac-authentication user-name-format mac-address with-hyphen uppercase
#
radius scheme aku
 server-type extended
 primary authentication 10.2.0.4
 primary accounting 10.2.0.4
 key authentication secret
 key accounting secret
 user-name-format without-domain
#
#
domain aku.edu.tr
 authentication default radius-scheme aku
 authorization default radius-scheme aku
 accounting default radius-scheme aku
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
mac-authentication
#
```

3.2.1.3 Vlan Yapılandırılması



Şekil 3.6 Örnek bir vlan şeması (İnt.Kyn.30)

Birden fazla anahtarlama cihazının bulunduğu yapılarda broadcast paketlerinin tüm ağ üzerinde dolaşması kaçınılmazdır. İpv4 protokolünde Broadcast paketleri olmazsa olmaz bir özellik olmakla beraber bir güvenlik unsuru olarak ta düşünülebilir. Sisteme dışardan gelen bir kullanıcı internet erişimi için ağa dahil olduğunda arp spoffing gibi programlarla ağda arp zehirlemesi yapabilir ve tüm ağa sızma şansı yakalayabilmektedir.

Böyle durumlarda VLAN'lar (Şekil 3.6), sayesinde ağı birbirinden bağımsız bölümlere ayırarak, riskleri önleme, karmaşıklığı ortadan kaldırma ve problem çözme konusunda büyük ölçüde fayda sağlamaktadır.

Anahtarlama cihazlarında vlan oluşturarak hostlar tarafından gönderilen broadcast paketleri sadece aynı vlana dahil olan portlara gönderilir. Bu nedenle her VLAN kendi içerisinde bir broadcast domainidir. Yani bu özellik sayesinde kaynağı bilinmeyen unicast paketlerde sınırlanmış olmaktadır.

Layer3 bir anahtarlama cihaz üzerinde farklı VLAN'ların haberleşebilmesi için kesinlikle VLAN routing işlemi yapılması gerekmektedir. Ayrı VLAN'lar haberleşiyor

olsalar bile broadcast paketleri sadece aynı VLAN'a dahil olan portlarda gerçekleşecektir. Per-Vlan Spanning Tree sayesinde Loop önlemiş olunmaktadır. Tabi her VLAN bu denetimi kendi içerisinde yaptığı için LOOP felaketinden hem tüm switch etkilenmiyor hem de LOOP'un oluştuğu kaynağın tespiti daha çabuk yapılmaktadır (İnt.Kyn.31).

Kenar switchlerde oluşturulan vlanlar Şekil 3.7'de görülmektedir.

```
ip default-gateway [redacted]
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged 49-50
   ip address [redacted]
   no untagged 1-48
   exit
vlan 100
   name "bim"
   untagged 1-35,37-48
   tagged 49-50
   exit
vlan 901
   name "kablosuz"
   tagged 49-50
   exit
vlan 50
   name "misafir"
   tagged 49-50
   exit
vlan 160
   name "Kablosuz"
   tagged 49-50
   exit
vlan 66
   name "**KAMERA**"
   untagged 36
   tagged 49-50
   exit
```

Şekil 3.7 Hp Procurver 2650 Vlan Örneği

3.2.1.4 Sahte Dhcp Sunucu

DHCP, son kullanıcı cihazların; IP adresi, alt ağ maskesi, varsayılan ağ geçidi ve DNS adresi gibi bilgileri otomatik olarak edinmesini sağlayan bir protokoldür. Getirdiği bu

faydanın yanında, birtakım güvenlik tehditlerine açık kapı bırakması ağlarda gerekli önlemlerin alınmasını zorunlu kılmaktadır. Ağda sahte DHCP sunucusu kuran ve çalıştıran bir kişi, aynı ağda DHCP isteğinde bulunan son kullanıcı cihazlara varsayılan ağ geçidi adresi kendisine ait olan bir DHCP cevabı dönebilir. Son kullanıcı bu cevabı aldığı andan itibaren ağ geçidi adresi olarak bu sahte adresi kullanmaya başlar ve yerel ağın dışında bir adresi hedefleyen paketler ilk olarak atak yapan kişinin makinesine yönlenir. Atakçı bu paketleri gitmeleri gereken doğru adreslere kendi üzerinden gönderirken tüm paketleri izleme olanağına sahip olur. Bu, son kullanıcı güvenliğini ve gizliliğini açıkça tehdit eden bir durumdur. Man-in the-middle ataklarının bir türü olan DHCP Snooping atakları tam olarak bu şekilde gerçekleşir.

Ciddi bir tehdit unsuru olan bu atağı engellemek için anahtarlayıcı cihazlarda DHCP Snooping özelliği kullanılmaktadır. DHCP Snooping özelliği bir cihazda etkinleştirilerek portlar trusted ve untrusted olarak kategorize edilebilir ve böylece gerçek DHCP sunucularının hangi portlar üzerinden yayın yapacağı cihaza öğretilmiş olur. Untrusted portlardan gelen DHCP istekleri anahtarlayıcı tarafından incelenir. Untrusted portlardan gelen cevaplar ise cihaz tarafından çöpe atılır ve atağa maruz kalan port kapatılır.

DHCP Snooping özelliği ek olarak son kullanıcıları aldıkları otomatik ayarların kaydını tutar. Kayıtta, hangi IP adresinin hangi MAC adresine ne kadarlık bir süre için atandığının bilgisi tutulur.

DHCP Snooping(Çizelge 3.2) özelliğini etkinleştirmek için global konfigürasyon modunda şu komut işletilmelidir:

Çizelge 3.2 Dhcp snooping komut satırı

[BIM-2]dhcp-snooping

Varsayılan olarak bütün yönetilebilir anahtarlayıcı portları untrusted modundadır ve DHCP cevaplarını engeller. Bu yüzden gerçek DHCP sunucuların bulunduğu portlar cihaza öğretilmelidir.
Bunun için Şekil 3.8'daki komut dizisi işletilmelidir:

```
[BIM-2-GigabitEthernet1/0/25]display this
#
interface GigabitEthernet1/0/25
 port link-type trunk
 port trunk permit vlan 1 66 98 100 160 901
 dhcp-snooping trust
 arp detection trust
#
return
```

Şekil 3.8 Dhcp-snooping trust örnek-1

DHCP Snooping konfigüre edildikten sonra bununla ilgili durumu Şekil 3.9'daki komutları işleterek görüntüleyebilmektedir:

```
[BIM-2-GigabitEthernet1/0/25]display dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static , R--Recovering
 Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
 ==== ============== ============== ============ ==== ===== ================
 D    172.16.101.148  d485-64b2-a775 45037        100  N/A   GE1/0/4
 D    172.16.101.214  d485-649e-5bc3 84052        100  N/A   GE1/0/7
 D    172.16.98.209   c4ca-d9e7-7140 60257        98   N/A   GE1/0/23
---   3 dhcp-snooping item(s) found   ---
```

Şekil 3.9 Dhcp-snooping örnek-2

Komuta [binding] seçeneğinin eklenmesiyle, anahtarlayıcının veri tabanında tuttuğu hangi IP adreslerinin hangi MAC adreslerine atandığı bilgisine ulaşılabilir (İnt.Kyn.32).

3.2.1.5 Arp Detection Protokolü

Lokal ağlarda gerçekleştirilmesi hiç de zor olmayan saldırılardan birisi de ARP sahtekarlığı saldırılarıdır. ARP sahtekarlığı saldırılarının anlaşılabilmesi için ARP

kavramının çok iyi bilinmesi gerekmektedir. ARP kavramının iyi bilinmemesi, ARP saldırılarının anlaşılmasına ve bu saldırıların önlenmesine engel olacaktır.

ARP sahtekarlığı saldırısı lokal ağlarda gerçekleştirilebilen bir saldırıdır. Bu saldırı, üç şekilde gerçekleştirilmektedir:

1. Hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamak.
2. Hedef bilgisayarın göndereceği tüm paketlerin, saldırganın bilgisayarı üzerinden geçmesini sağlamak (Man in the Middle).
3. Hedef bilgisayarın, paketlerini bir başka bilgisayara göndermesini sağlayarak bu bilgisayara servis dışı bırakma (Denial of Service) saldırısı yapmak şeklindedir.

Lokal ağlarda çok fazla önlem alınmayan ve saldırı tespit sistemleriyle de tespit edilmeleri mümkün olmayan ikinci katman saldırılarına karşı önlemlerin alınması lokal ağların güvenliği için oldukça önemlidir (İnt.Kyn.33).

3.2.2 Kimlik Doğrulama Sunucusu Oluşturma

Gün geçtikçe kullandığımız sistem sayısı artmakta ancak bu kadar farklı sistemi kullanırken her biri için kullanıcı ve şifre oluşturmak yönetimi ve takibi imkânsız bir hal almaktadır. Bu durum karşısında sistemlere erişimde tek kullanıcı adı ve şifre kullanmak kaçınılmaz olmaktadır. Bu denli farklı cihaz ve sistemlerin kimlik doğrulaması yaptıkları bazı protokoller mevcuttur. Güvenlik sistemleri kimlik denetimi için Aktif dizin, ldap veya Radius sunucu desteği koymaktadırlar.

Ldap veritabanı ile doğrudan kimlik denetimi yaptırmak üç sebepten dolayı tavsiye edilmemektedir.

- Kimlik denetimi yapılacak sistemlere Ldap kullanıcı bilgilerini ayrı ayrı tanımlanarak, Ldap sunucusuna yetkisiz kimselerin de giriş yapması kolaylaşmaktadır.
- Ldap sunucusunun kullanıcı bilgilerindeki değişiklik karşısında tüm ağ cihazlarında ve güvenlik sistemlerinde ayrı ayrı yeni bilgileri tanımlamak gerekmektedir.

- Sisteminizde birden fazla ldap sunucu mevcut ise onların ayrı ayrı tanımlanması her zaman mümkün olmamaktadır.

Sistemde kimlik denetimi için freeradius'u kullanılmıştır. Radius sunucuyu Centos işletim sisteminde kurulumunu tamamlandıktan sonra sunucunun ayarları aşağıdaki gibi yapılabilmektedir.

Sunucuya centos işletim sisteminin 5.8 versiyonunun kurulumu tamamlandıktan sonra mevcut güncelleştirmeleri ve gerekli paket yükleme işlemleri Çizelge 3.3'teki gibi yapılmaktadır.

Çizelge 3.3 Centos sunucu paket güncelleme

yum update yum upgrade yum install gcc

Güncelleme işlemini ve gerekli paket yüklemelerinin tamamlanmasıyla freeradius sunucunun kurulumuna devam etmektedir. Şekil 3.10'deki belirtilen komut satırıyla freeradius ile ilgili kurulum paketleri görüntülenebilmektedir.

```
[root@syslog ~]# yum search freeradius
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: repo.boun.edu.tr
 * epel: repo.boun.edu.tr
 * extras: repo.boun.edu.tr
 * updates: repo.boun.edu.tr
============================================================== Matched: freeradius
freeradius.i386 : High-performance and highly configurable free RADIUS server.
freeradius-mysql.i386 : MySQL bindings for freeradius
freeradius-postgresql.i386 : postgresql bindings for freeradius
freeradius-unixODBC.i386 : unixODBC bindings for freeradius
freeradius2.i386 : High-performance and highly configurable free RADIUS server
freeradius2-krb5.i386 : Kerberos 5 support for freeradius
freeradius2-ldap.i386 : LDAP support for freeradius
freeradius2-mysql.i386 : MySQL support for freeradius
freeradius2-perl.i386 : Perl support for freeradius
freeradius2-postgresql.i386 : Postgresql support for freeradius
freeradius2-python.i386 : Python support for freeradius
freeradius2-unixODBC.i386 : Unix ODBC support for freeradius
freeradius2-utils.i386 : FreeRADIUS utilities
pam_radius.i386 : PAM Module for RADIUS Authentication
```

Şekil 3.10 Freeradius kurulum paketleri

Bu listeden sadece Şekil 3.11'de seçilen komutlar çalıştırılarak freeradius sunucu ve ldap eklentileri kurulmuş olmaktadır.

```
[root@syslog ~]# yum install freeradius freeradius2-ldap freeradius2-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: repo.boun.edu.tr
 * epel: repo.boun.edu.tr
 * extras: repo.boun.edu.tr
 * updates: repo.boun.edu.tr
Setting up Install Process
```

Şekil 3.11 Freeradius kurulum paketleri

Centos işletim sisteminde /etc/raddb klasörünün altında Radius sunucunun dosyaları bulunmaktadır bu dosyalardan bazıları üzerinde düzenlenme yapılması gerekmektedir. Yapılan değişiklikler sırasıyla şöyle tanımlanmalıdır.

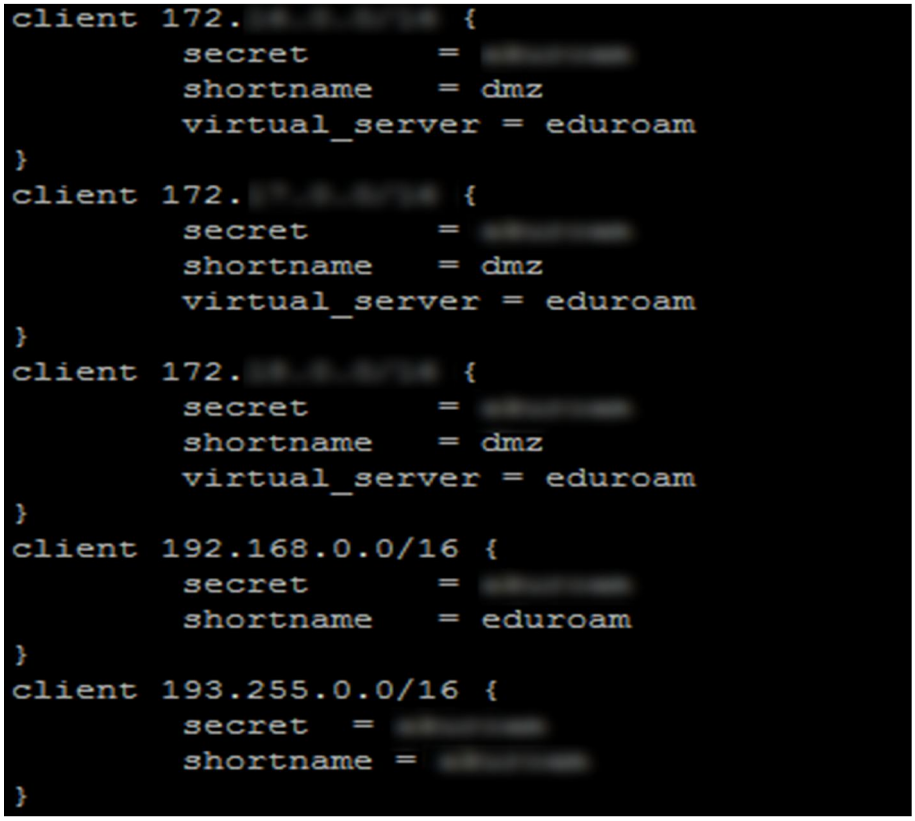
3.2.2.1 Clients.conf yapılandırılması

Radius sunucunun hangi ip bloklarından gelen istekleri kabul edeceğini client.conf dosyasında tanımlanmalıdır.
Sistemde kullanılacak Radius sunucu secret'i (şifresi) ve sunucunun ip adresi Şekil 3.12'de görüldüğü üzere burada tanımlanmaktadır.

```
client 127.0.0.1 {
        #
        #  The shared secret use to "encrypt" and "sign" packets between
        #  the NAS and FreeRADIUS.  You MUST change this secret from the
        #  default, otherwise it's not a secret any more!
        #
        #  The secret can be any string, up to 31 characters in length.
        #
        secret          = [redacted]

        #
        #  The short name is used as an alias for the fully qualified
        #  domain name, or the IP address.
        #
        shortname       = localhost
```

Şekil 3.12 Client ayarları Örnek 1

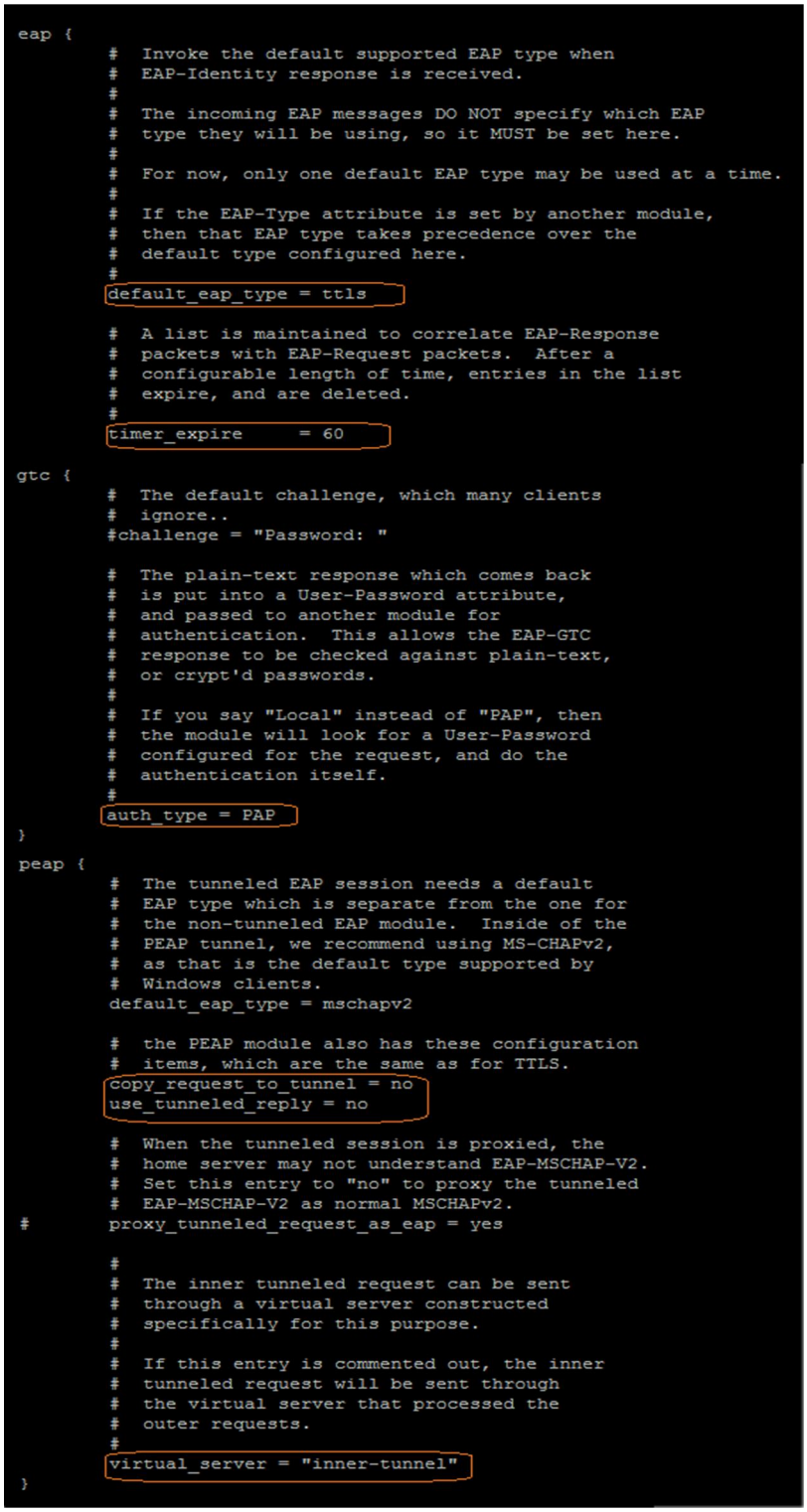
Radius sunucuya erişim sağlanacak ip bloklarının Şekil 3.13'de gösterildiği gibi tanımlanması gerekmektedir.



Şekil 3.13 Client ayarları Örnek 2

3.2.2.2 Eap.conf yapılandırılması

Eap.conf dosyasında şifreleme sisteminde kullanılacak parametreler Şekil 3.14'te gösterildiği gibi tanımlanmaktadır.



Şekil 3.14 Eap ayarları

3.2.2.3 Radius.conf yapılandırılması

Radius sunucu ile ldap veritabanını ilişkilendirmek için Şekil 3.15'da sunulduğu üzere ayarlar yapılandırılmalıdır.

```
listen {
        #  Type of packets to listen for.
        #  Allowed values are:
        #       auth    listen for authentication packets
        #       acct    listen for accounting packets
        #       proxy   IP to use for sending proxied packets
        #       detail  Read from the detail file.  For examples, see
        #               raddb/sites-available/copy-acct-to-home-server
        #       status  listen for Status-Server packets.  For examples,
        #               see raddb/sites-available/status
        #       coa     listen for CoA-Request and Disconnect-Request
        #               packets.  For examples, see the file
        #               raddb/sites-available/coa-server
        #
        type = auth
```

Şekil 3.15 Radius ayarları Örnek 1

Radius sunucu birden çok veritabanları ile entegre çalışabildiği gibi Şekil 3.16'de belirtildiği gibi aynı anda birden fazla ldap sunucu tanımlamaları yapılabilmektedir.

```
authorize {
        ldap1
        ldap2
}
authenticate {
        ldap1
        ldap2
}

listen {
        ipaddr = *
#       ipv6addr = ::
        port = 0
        type = acct
#       interface = eth0
#       clients = per_socket_clients
}
```

Şekil 3.16 Radius ayarları Örnek 2

Sistem üzerinde oluşan Radius kayıtlarının sunucu üzerinde hangi dizin altında tutulacağı Şekil 3.17'de gibi tanımlanmaktadır.

```
log {
        #
        #  Destination for log messages.  This can be one of:
        #
        #       files - log to "file", as defined below.
        #       syslog - to syslog (see also the "syslog_facility", below.
        #       stdout - standard output
        #       stderr - standard error.
        #
        #  The command-line option "-X" over-rides this option, and forces
        #  logging to go to stdout.
        #
        destination = files

        #
        #  The logging messages for the server are appended to the
        #  tail of this file if destination == "files"
        #
        #  If the server is running in debugging mode, this file is
        #  NOT used.
        #
        file = ${logdir}/radius.log
```

Şekil 3.17 Radius log ayarları Örnek 1

```
syslog_facility = daemon

#  Log the full User-Name attribute, as it was found in the request.
#
# allowed values: {no, yes}
#
stripped_names = yes

#  Log authentication requests to the log file.
#
#  allowed values: {no, yes}
#
auth = yes

#  Log passwords with the authentication requests.
#  auth_badpass  - logs password if it's rejected
#  auth_goodpass - logs password if it's correct
#
#  allowed values: {no, yes}
#
auth_badpass = no
auth_goodpass = no
```

Şekil 3.18 Radius log ayarları Örnek 2

3.2.2.4 Eduroam yapılandırılması

İstemcilerin bağlantı noktası olarak varsayılan ayarlar seçilebileceği gibi burada da görüldüğü üzere yök çatısı altındaki üniversitelerin ortak bağlantı noktası olarak belirledikleri Eduroam bağlantı ayarları Şekil 3.19'de gösterildiği gibi tanımlanmaktadır.

```
server eduroam {

authorize {
#         preprocess
#         chap
#         mschap
          suffix
          eap {
                  ok = return
          }
#         unix
#         files
          ldap1
          ldap2
#         expiration
#         logintime
          pap
}
```

Şekil 3.19 Eduroam bağlantı ayarları – 1

Yukarıda da belirtildiği üzere birden çok ldap sunucu sisteme eklenebilmektedir. Bu ekranda da eduroam bağlantısı için yetkin ldap sunucular Şekil 3.20'de gösterildiği gibi tanımlanmıştır.

```
authenticate {
          Auth-Type PAP {
                  pap
          }
#         Auth-Type CHAP {
#                 chap
#         }
#         Auth-Type MS-CHAP {
#                 mschap
#         }
#         unix
#
#         Auth-Type LDAP {
#                 ldap1
#         }
          eap
          ldap1
          ldap2
}
```

Şekil 3.20 Eduroam bağlantı ayarları – 2

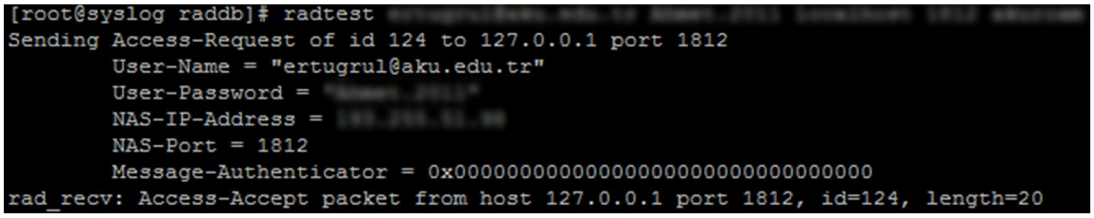
3.2.2.5 Ldap yapılandırılması

Ldap dosyasında, sistemde kullanılacak ldap veribanlarının erişim bilgileri tanımlanmaktadır. Şekil 3.21'de sadece ldap1 veritabanı erişim bilgileri sisteme tanımlanmıştır.

```
ldap ldap1 {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = '[redacted]'
        identity = '[redacted]'
        password = [redacted]
        basedn = "dc=aku,dc=edu,dc=tr"
        #server = "localhost"
        #identity = "cn=admin,dc=adu,dc=edu,dc=tr "
        #password = secret
        #basedn = "dc=adu,dc=edu,dc=tr"
        filter = "(mail=%{Stripped-User-Name:-%{User-Name}})"
        #filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        #base_filter = "(objectclass=radiusprofile)"

        #  How many connections to keep open to the LDAP server.
        #  This saves time over opening a new LDAP socket for
        #  every authentication request.
        ldap_connections_number = 5

        # seconds to wait for LDAP query to finish. default: 20
        timeout = 4

        #  seconds LDAP server has to process the query (server-side
        #  time limit). default: 20
        #
        #  LDAP_OPT_TIMELIMIT is set to this value.
        timelimit = 3

        #
        #  seconds to wait for response of the server. (network
        #   failures) default: 10
        #
        #  LDAP_OPT_NETWORK_TIMEOUT is set to this value.
        net_timeout = 1
```

Şekil 3.21 Radius ldap ayarları

Kurulum tamamladıktan sonra Radius sunucunun çalıştığını test için Şekil 3.22'te gösterilen komut çalıştırılmalıdır.



Şekil 3.22 Radius bağlantı testi

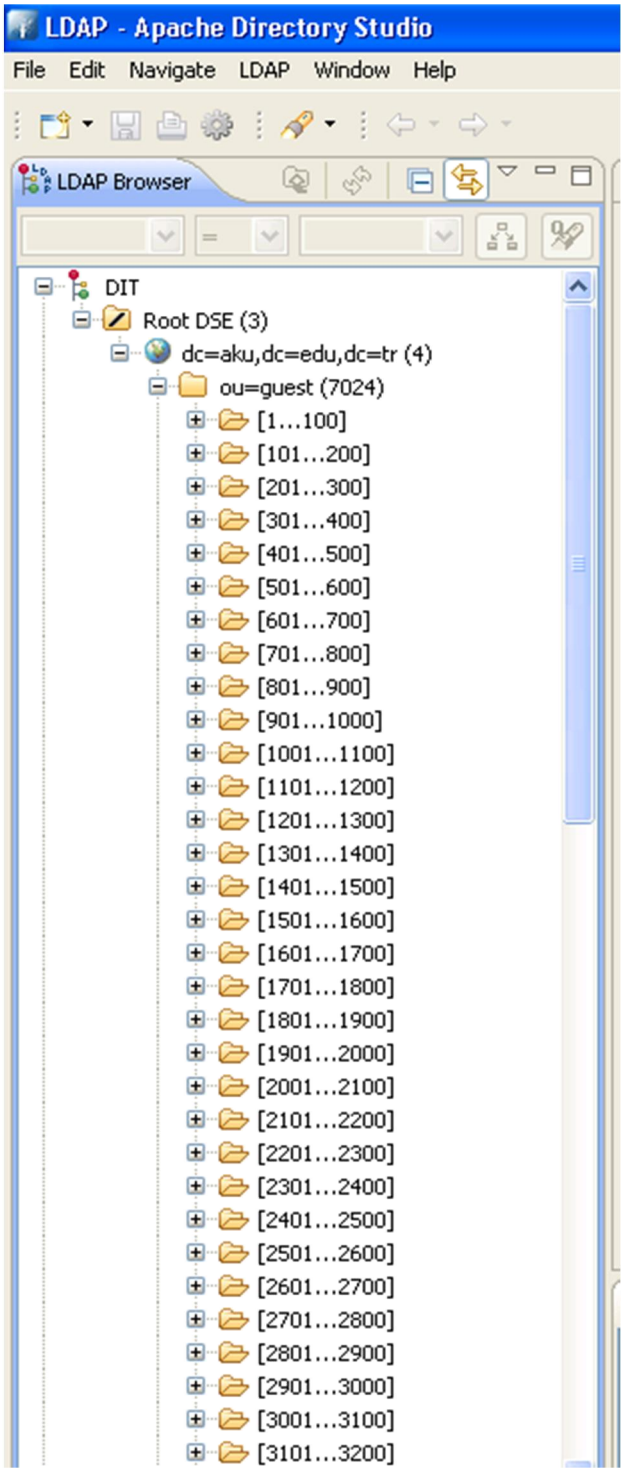
Radius sunucuyu debug modda çalıştırmak istersek Çizelge 3.4 üzerinde gösterilen komutu çalıştırıp çıktısı görüntülenebilir.

Çizelge 3.4 Radius sunucuyu debug modda çalıştırma

radiusd –X

3.2.3 Ldap Veritabanı

LDAP'ın diğer veritabanlarına göre okuma hızı daha fazladır. Sistem üzerinde 35-40 bin civarında kayıtın tutulmasına rağmen performans kaybı yaşanmamaktadır. Ldap'ın ağaç yapısını aşağıdaki Şekil 3.23'te daha net gösterilmektedir.



Şekil 3.23 Open ldap kullanıcı listesi

3.2.4 Log Sunucu (Rsyslog)

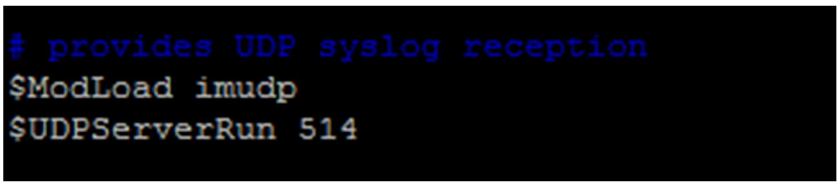
Başbakanlığın yayınlamış olduğu 01.11.2007 tarihli ve 26687 sayılı Resmi Gazete'de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik'in 5 inci maddesi birinci fıkrasının (e) bendine istinaden, (d) bendi gereğince, internet toplu kullanım sağlayıcılarının elektronik ortamda sistemlerine kaydettikleri ip dağıtımlarının kayıtları ile erişim kayıtlarını "Zaman Damgası" ile imzalı tutulması istenmektedir. Bu kayıtların enaz 6 ay ile 2 yıl arasında olması öngörülmektedir (İnt.Kyn.34).
Yukarıda da belirtildiği üzere internet hizmeti veren bir kurum olarak sistem üzerinde oluşan kayıtların zaman damgası ile imzalanıp saklanabilmesi için merkezi bir log sunucu kurulmuş. Bu sunucunun kurulum aşamalarını aşağıdaki Çizelge 3.5'de yapılmıştır.

- Log sunucu için Ubuntu 12.04 sürümü tercih edilmiştir.

Çizelge 3.5 Syslog sunucu yapılandırılması

vi /etc/rsyslog.conf

Şekil 3.24'daki gibi belirtilen satırları bulup başlarındaki "#" işareti kaldırılmalıdır.



Şekil 3.24 Syslog ayarları - 1

değişiklikler kaydedildikten sonra servis Şekil 3.25 gösterildiği üzere tekrar başlatılmalıdır.

```
root@syslog:/etc# /etc/init.d/rsyslog restart
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service rsyslog restart

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the stop(8) and then start(8) utilities,
e.g. stop rsyslog ; start rsyslog. The restart(8) utility is also available.
rsyslog stop/waiting
rsyslog start/running, process 27388
```

Şekil 3.25 Syslog ayarları – 2

Burada önemli bir nokta, sunucuya log kayıtları gelmiyorsa sunucu üzerinde güvenlik duvarı aktiftir onun Şekil 3.26'deki gibi pasifleştirilmesi gerekmektedir.

```
root@syslog:/etc# ufw disable
Firewall stopped and disabled on system startup
```

Şekil 3.26 Syslog ayarları – 3

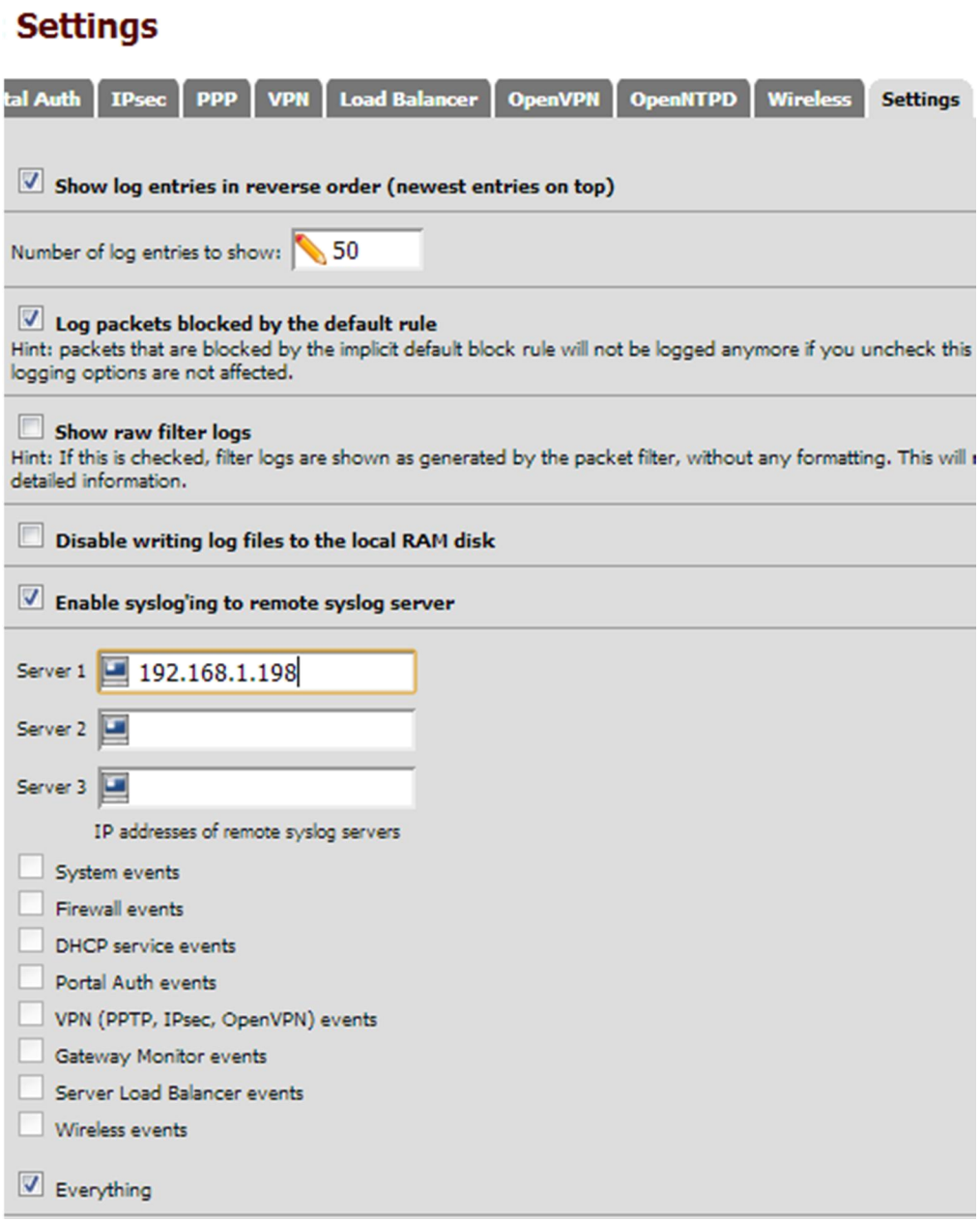
Böylece merkezi bir log sunucu kurulumu tamamlandı. Şekil 3.27'da da görüldüğü üzere güvenlik duvarı üzerinde oluşan kayıtlar gösterilmektedir.

Last 100 firewall log entries.Max(100)

Act	Time	If	Source	Destination	Proto
▶	Apr 1 05:46:32	LAN	172.16.180.73:49255	193.140.100.231:443	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.180.73:49254	193.140.100.231:443	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.48.18:21951	54.243.51.171:80	TCP:S
▶	Apr 1 05:46:32	DMZ	193.255.51.66:39616	75.116.63.158:53	UDP
▶	Apr 1 05:46:32	LAN	172.16.81.211:1384	78.40.226.91:443	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.0.6:32869	184.173.144.32:53	UDP
▶	Apr 1 05:46:32	LAN	172.16.0.6:32869	174.129.251.146:53	UDP
▶	Apr 1 05:46:32	DMZ	193.255.51.66:51726	67.214.64.7:53	UDP
✖	Apr 1 05:46:32	BIM	172.16.100.67:137	172.16.101.255:137	UDP
▶	Apr 1 05:46:32	LAN	172.16.77.130:50222	2.21.99.235:80	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.77.130:50221	2.21.99.235:80	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.158.241:2208	173.194.70.120:443	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.152.189:1187	188.132.199.45:80	TCP:S
▶	Apr 1 05:46:32	LAN	172.16.81.211:1383	78.40.226.91:443	TCP:S

Şekil 3.27 İnternete çıkış kayıtları

Sistem üzerinde oluşan kayıtların bir log sunucuda tutulabilmesi için güvenlik duvarı üzerinde Şekil 3.28'da belirtildiği üzere işlemler yapılmalıdır.



Şekil 3.28 Kayıtları log sunucusuna gönderme

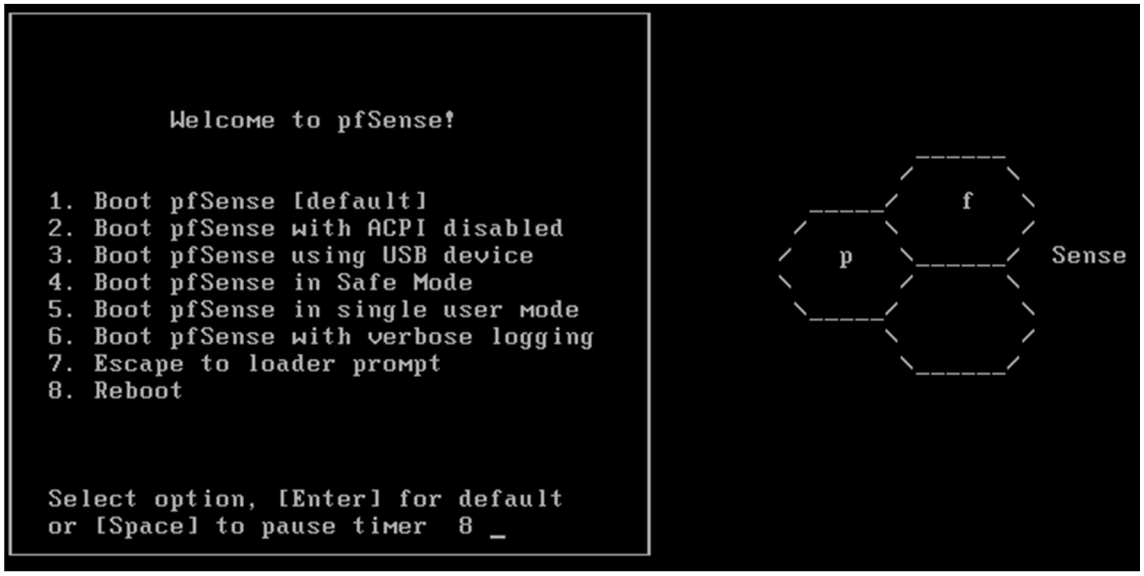
3.2.5 Güvenlik Duvarının Kurulumu ve Yapılandırılması

3.2.5.1 Pfsense'in Kurulumu

Açık kaynak kodlu bir dağıtım olan pfsense'sin kurulumu adım adım yapılmıştır.

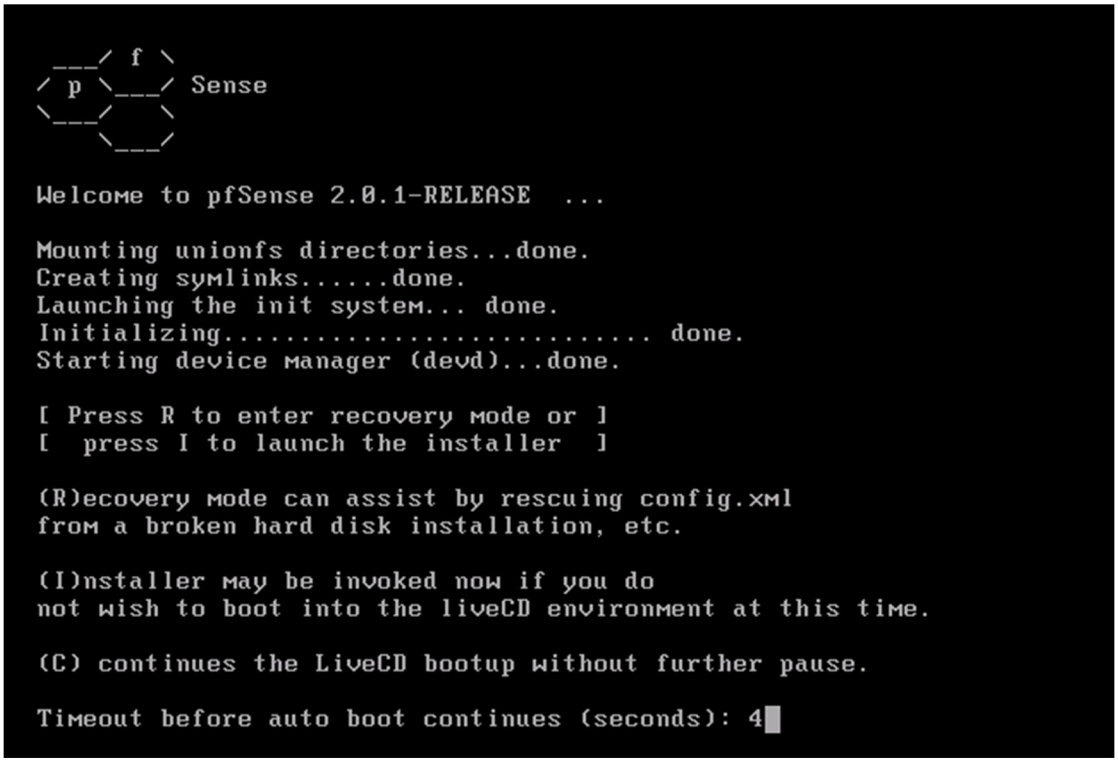
- Gerekli iso dağıtımını web sayfasından indirdikten sonra cd-rom'dan başlatılmalıdır.

Standart kurulum (Şekil 3.29) için sistem dosyalarının yüklenmesi gerekmektedir.



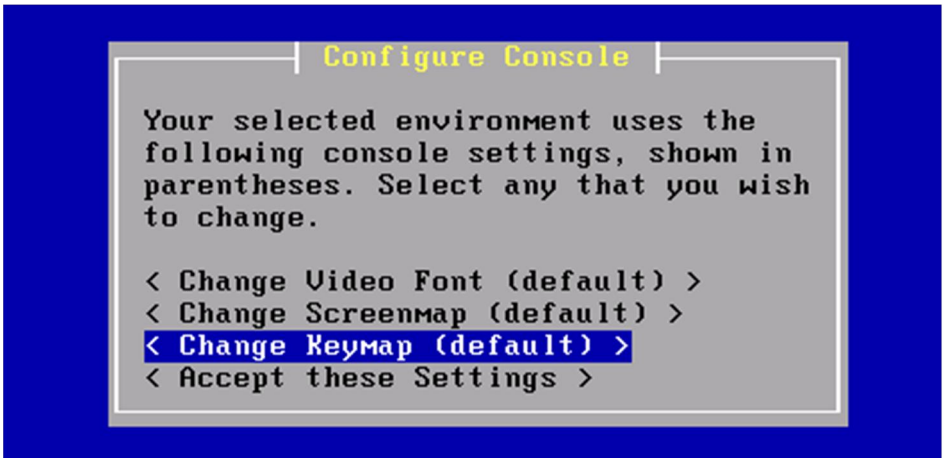
Şekil 3.29 Pfsense kurulum - 1

Sistemin diske kurulumu için Şekil 3.30'deki gibi büyük "I" tuşuna basılmalıdır.



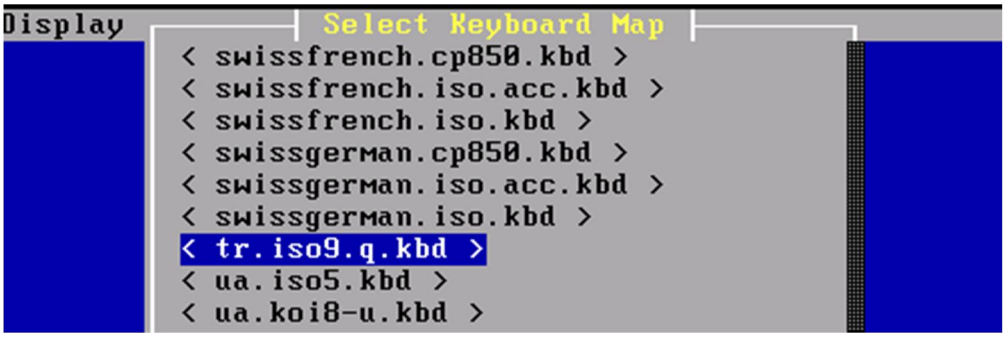
Şekil 3.30 Pfsense kurulum - 2

Şekil 3.31'de sunulduğu üzere "Change Keymap" menüsünden klavye dili seçeneklerine girilmelidir.



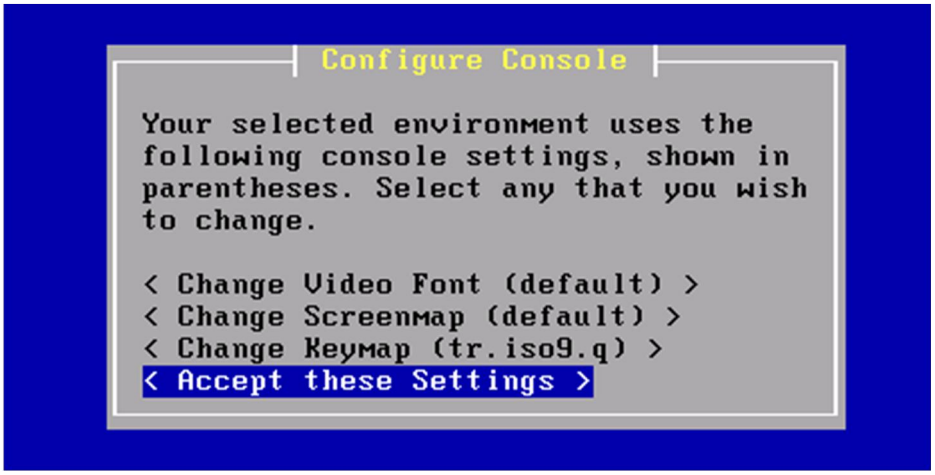
Şekil 3.31 Pfsense kurulum - 3

Dil seçeneği Şekil 3.32'de belirtildiği gibi türkçe q klavye olarak belirlenmelidir.



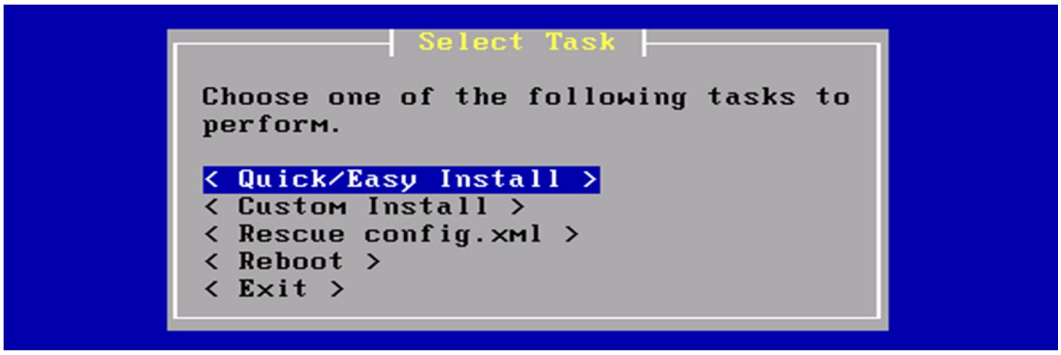
Şekil 3.32 Pfsense kurulum - 4

Şekil 3.33'de seçilen ayarları kaydederek bir sonraki ekrana geçilmelidir.



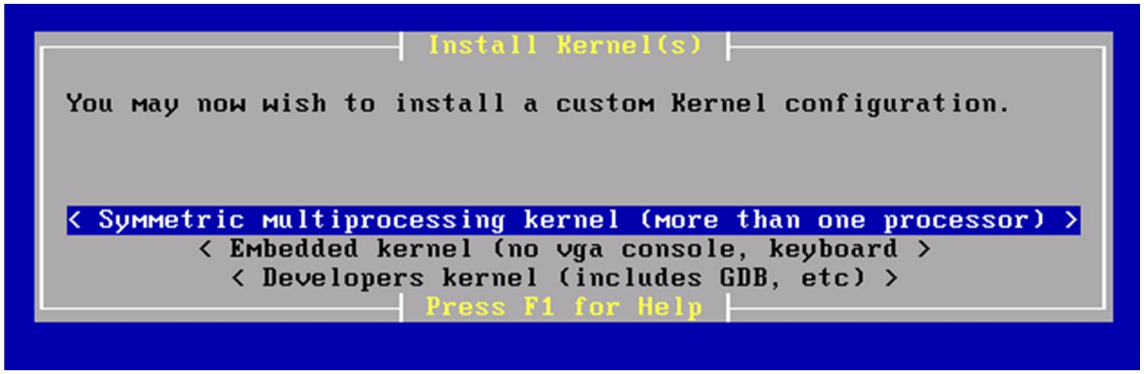
Şekil 3.33 Pfsense kurulum - 5

Sistem için gerekli paketlerin standart yüklenebilmesi için Şekil 3.34'da sunulduğu gibi birinci seçenek seçilmelidir.



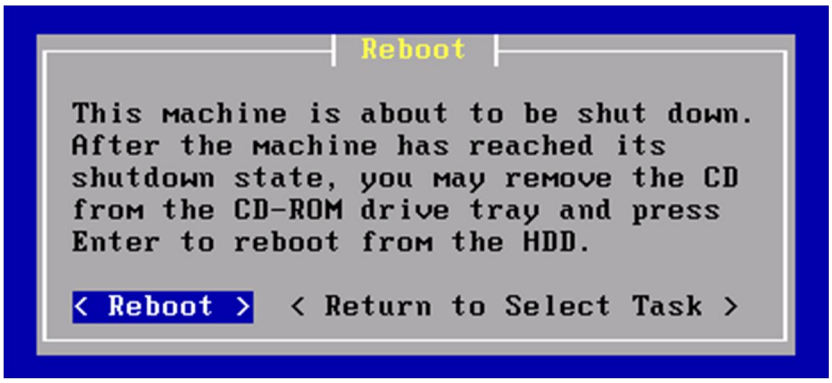
Şekil 3.34 Pfsense kurulum - 6

Pfsense güvenlik duvarının standart kurulumu için Şekil 3.35'de görüldüğü üzere ilk seçenek seçilmelidir.



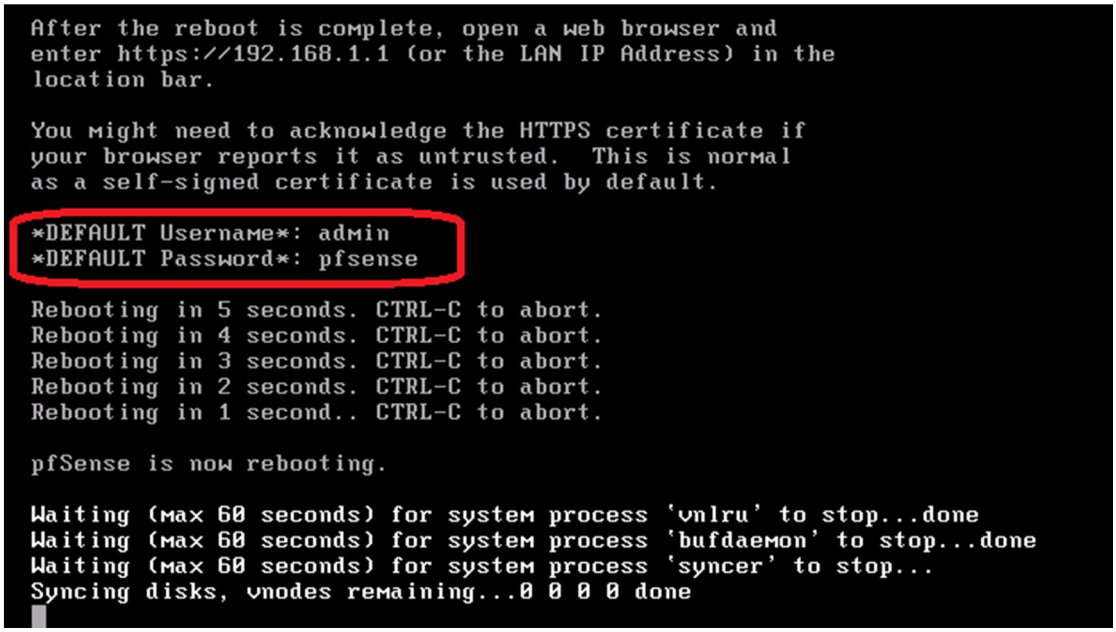
Şekil 3.35 Pfsense kurulum - 7

Kurulum tamamlanmıştır artık sunucu Şekil 3.36'deki gibi yeniden başlatılmalıdır.



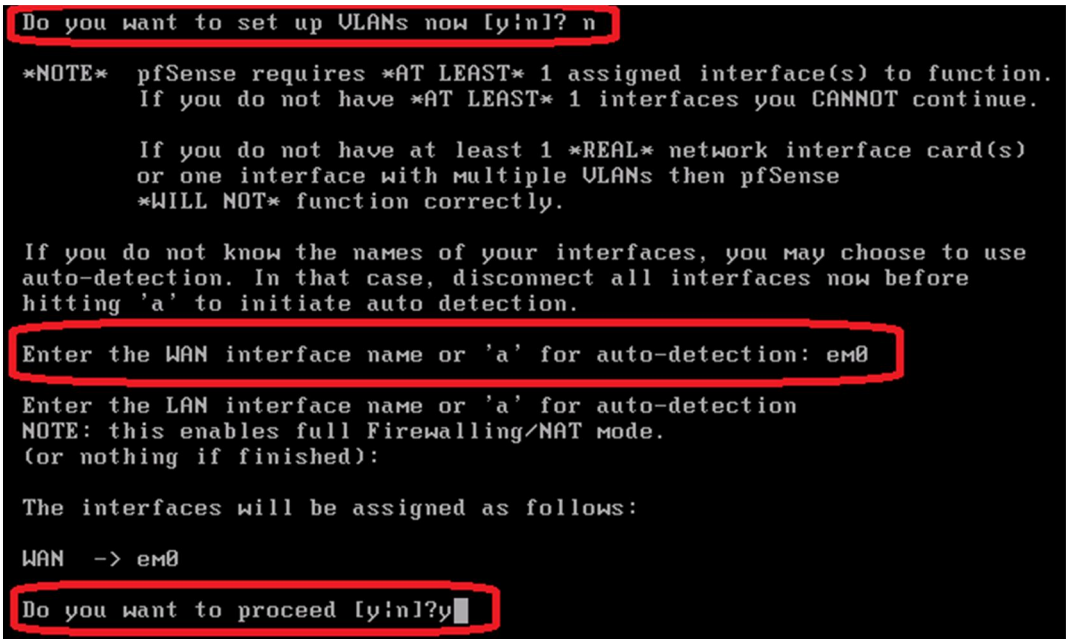
Şekil 3.36 Pfsense kurulum - 8

Pfsense'in standart kullanıcı bilgileri Şekil 3.37'da gösterilmektedir.



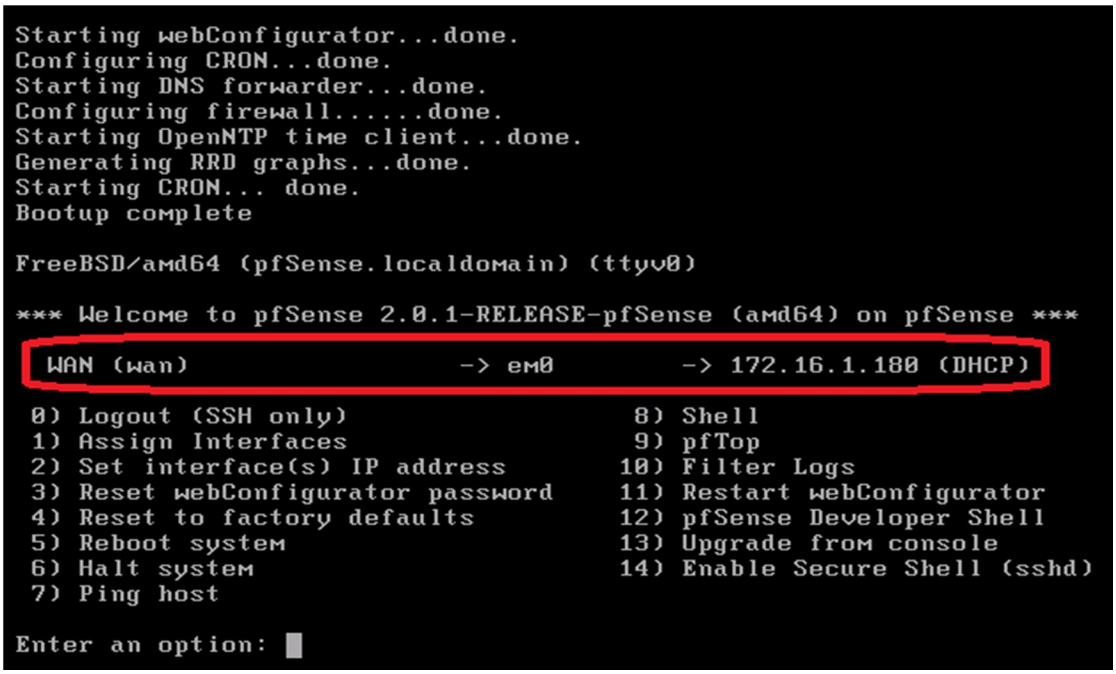
Şekil 3.37 Pfsense yapılandırma - 1

Vlan yapılandırılması web arayüzünden yapılacaktır. O yüzden Şekil 3.38 belirtildiği üzere "n" diyerek bu adım atlanılmıştır. Şuan sunucuda tek interface olduğu için onu wan interface olarak belirlenmiştir. Artık seçilen ayarların geçerli olabilmesi için işlem onaylanmalıdır.



Şekil 3.38 Pfsense yapılandırma - 2

Pfsense'in temel bazı ayarları için consol ekranı kullanılabilir ancak sistem için gerekli hemen hemen bütün ayarları web arayüzünden yapılmaktadır. Pfsense ile ilgili ayarları Şekil 3.39'de gösterilen ip adresinden yapılabilmektedir.

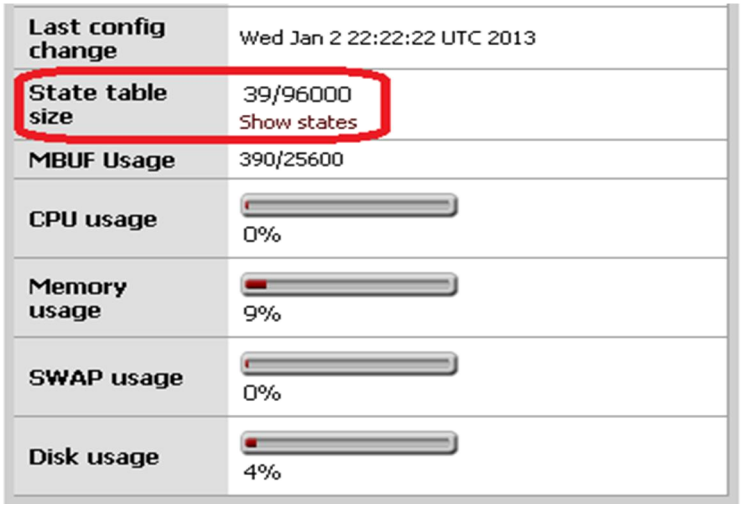


Şekil 3.39 Pfsense yapılandırma – 3

Sunucunun ekranı üzerinden yapılması gereken ayarlar şimdilik bu kadar artık herhangi bir browser ile Şekil 3.42'de sunulduğu üzere web üzerinden ip adresine erişim sağlanabilmektedir.

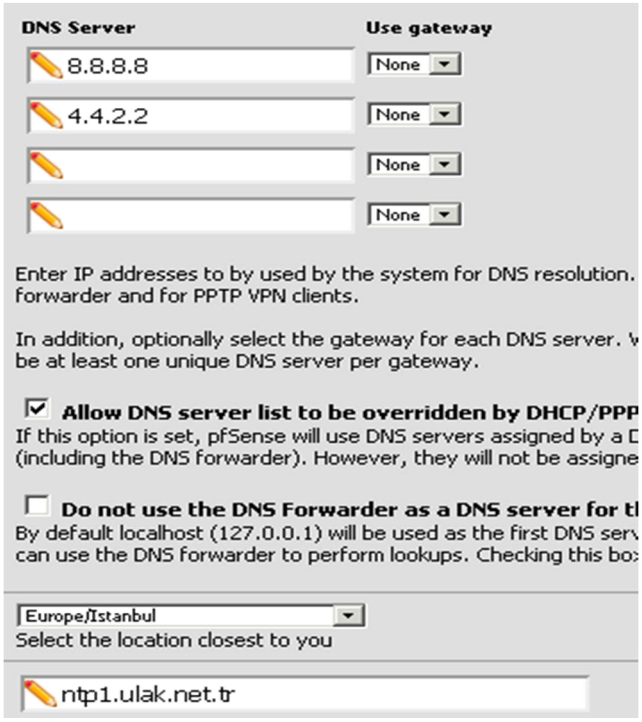
Şekil 3.40 Pfsense yapılandırma - 4

Açılan dashboard sayfasında sunucu üzerindeki aygıtların kullanım bilgileri verilmektedir. Burada küçük bir detay vermek gerekirse pfsense üzerinden geçecek paketlerin belirli bir sayıya ulaştıktan sonra paket kayıpları gözlenmektedir(Şekil 3.41). Bu durum karşısında System/Advanced bölümünden "State table size" değeri arttırılabilir.



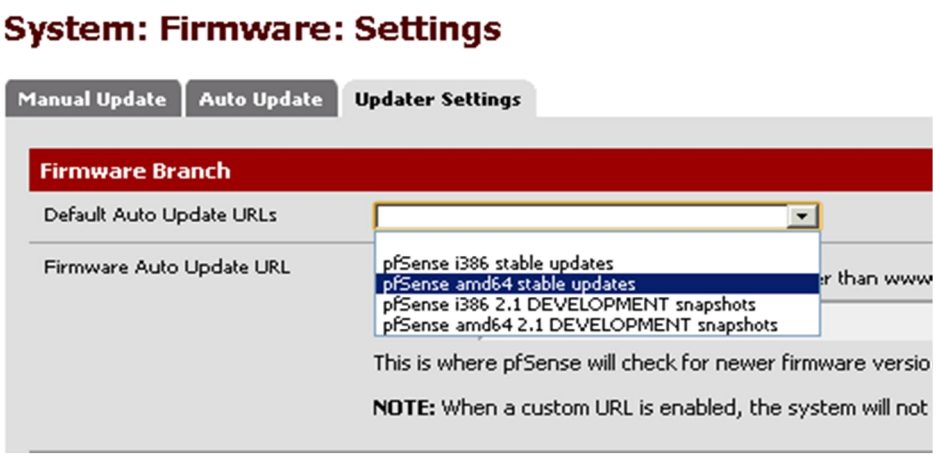
Şekil 3.41 Pfsense yapılandırma - 5

Pfsense güncellemelerini veya yeni versiyonlarını internet üzerinden indirebilmek için Dns bilgilerini ve güvenlik duvarı üzerinde oluşan kayıtların doğru saklanabilmesi için bölgesel saat ayarları Şekil 3.42'te belirtildiği gibi "System/General Setup" sayfasında tanımlanmaktadır.



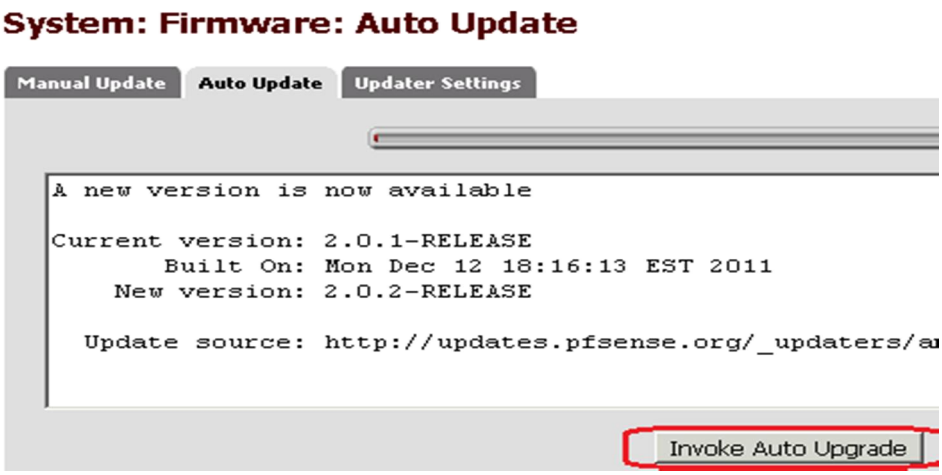
Şekil 3.42 Pfsense yapılandırma - 6

Güvenlik duvarının yeni güncellemelerini yüklemek için Şekil 3.43'de gösterilen "Advanced/Firmware" sayfasında "Updater Settings" sekmesinde mevcut sunucunun versiyonu seçilir.



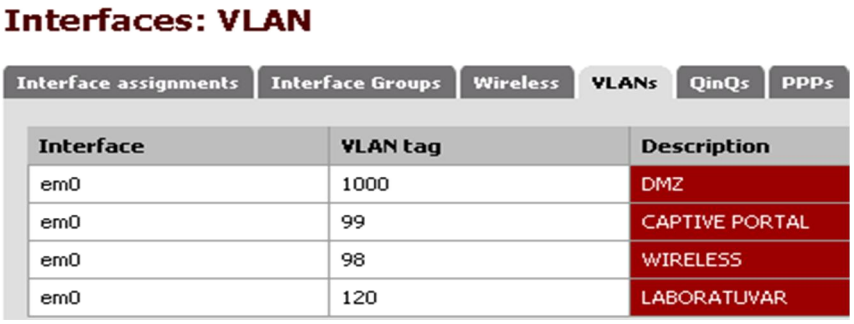
Şekil 3.43 Pfsense yapılandırma - 7

Şekil 3.44'da gösterilen "Auto Update" sekmesinden güncelleme başlatılabilmektedir.



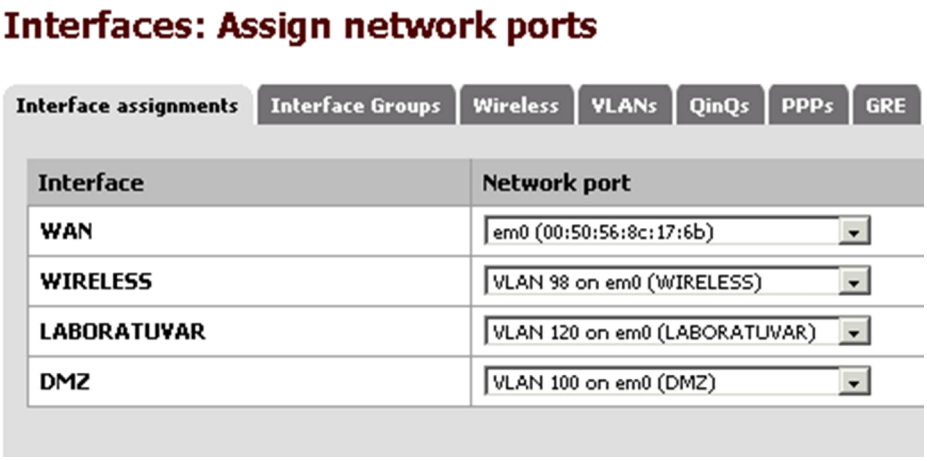
Şekil 3.44 Pfsense yapılandırma - 8

Güncellemeler tamamlandıktan sonra sistem üzerinde kullanılacak ip blokları (Subnet) Şekil 3.45'deki gibi arabirim üzerinde tanımlanmalıdır. Sunucuda yeterli sayıda arabirim olmadığı takdirde içeride vlan tanımlayarak sanal arabirim oluşturulabilmektedir.



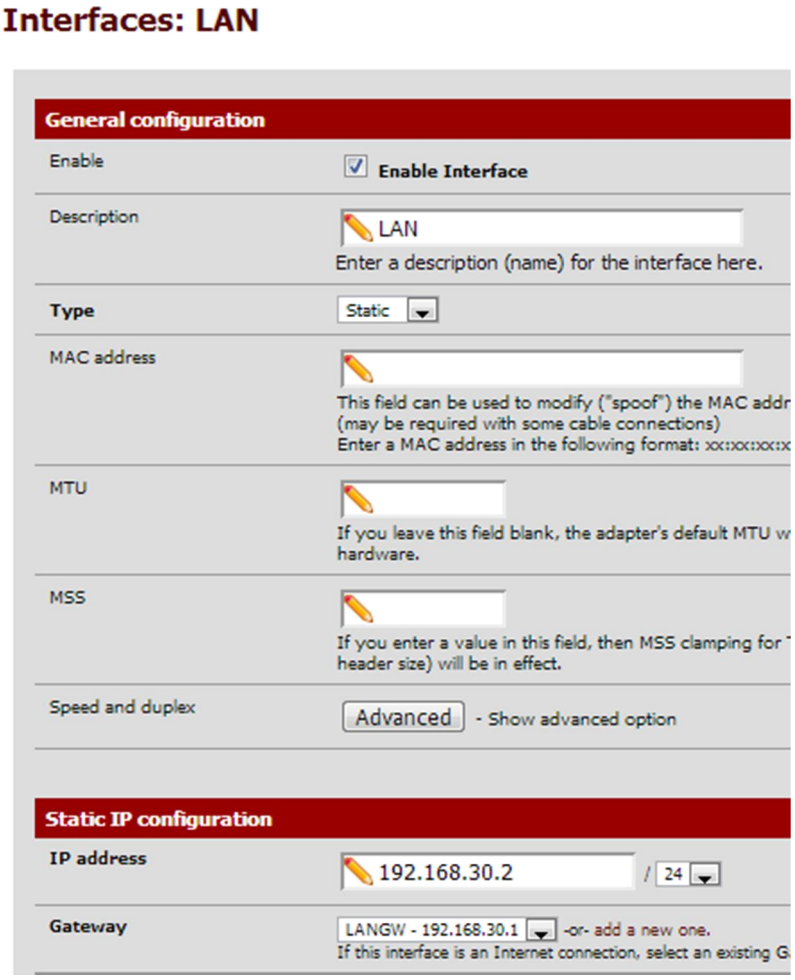
Şekil 3.45 Pfsense yapılandırma - 9

Sistem üzerinde kullanılacak arabirim ile vlan tagları Şekil 3.46'de gösterildiği üzere eşleştirilir.



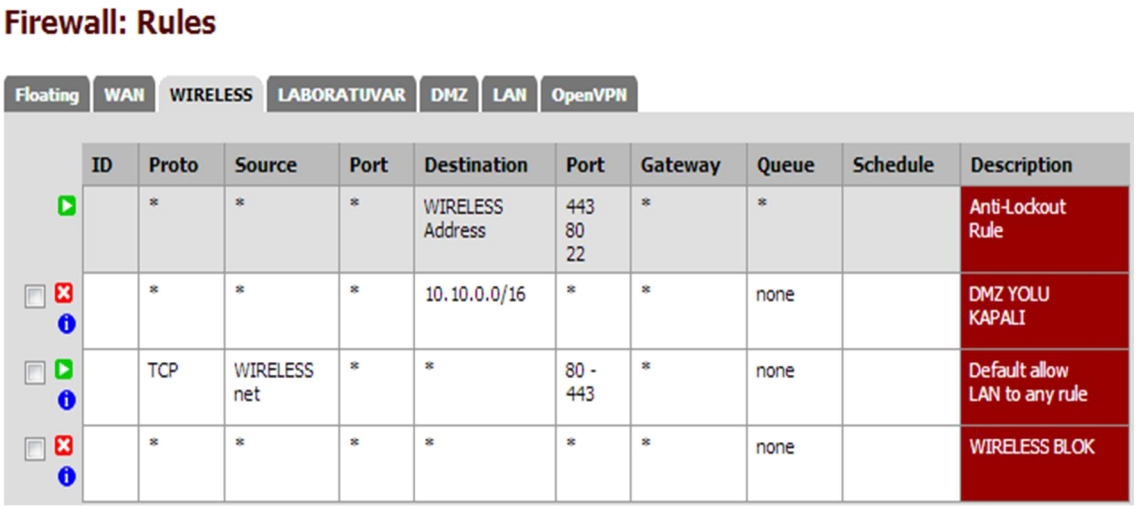
Şekil 3.46 Pfsense yapılandırma - 10

Oluşturulan arabirimlere ip tanımları Şekil 3.47'daki gibi yapılmaktadır.



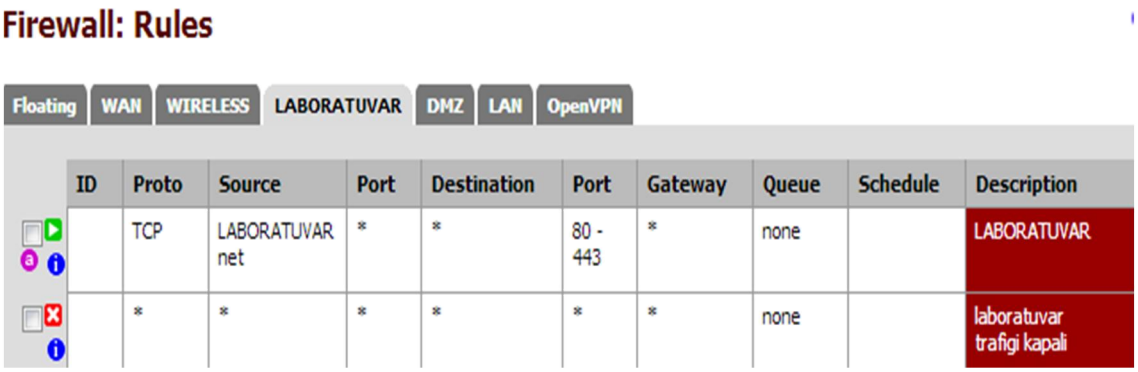
Şekil 3.47 Pfsense yapılandırma - 11

örneğin oluşturulan wireless subnetini internete çıkartırken kurallar dahilinde izin verilecektir. Kablosuz ağa bağlı bir istemciye sunuculara erişim hakkı tanınmamaktadır. Bu kullanıcı sadece web üzerinden Şekil 3.48'deki gibi http ve https (80,443) portlarına erişebilmelidir. Böylece kablosuz ağlardan kaynaklanan tehlikelerin önüne geçilmektedir.



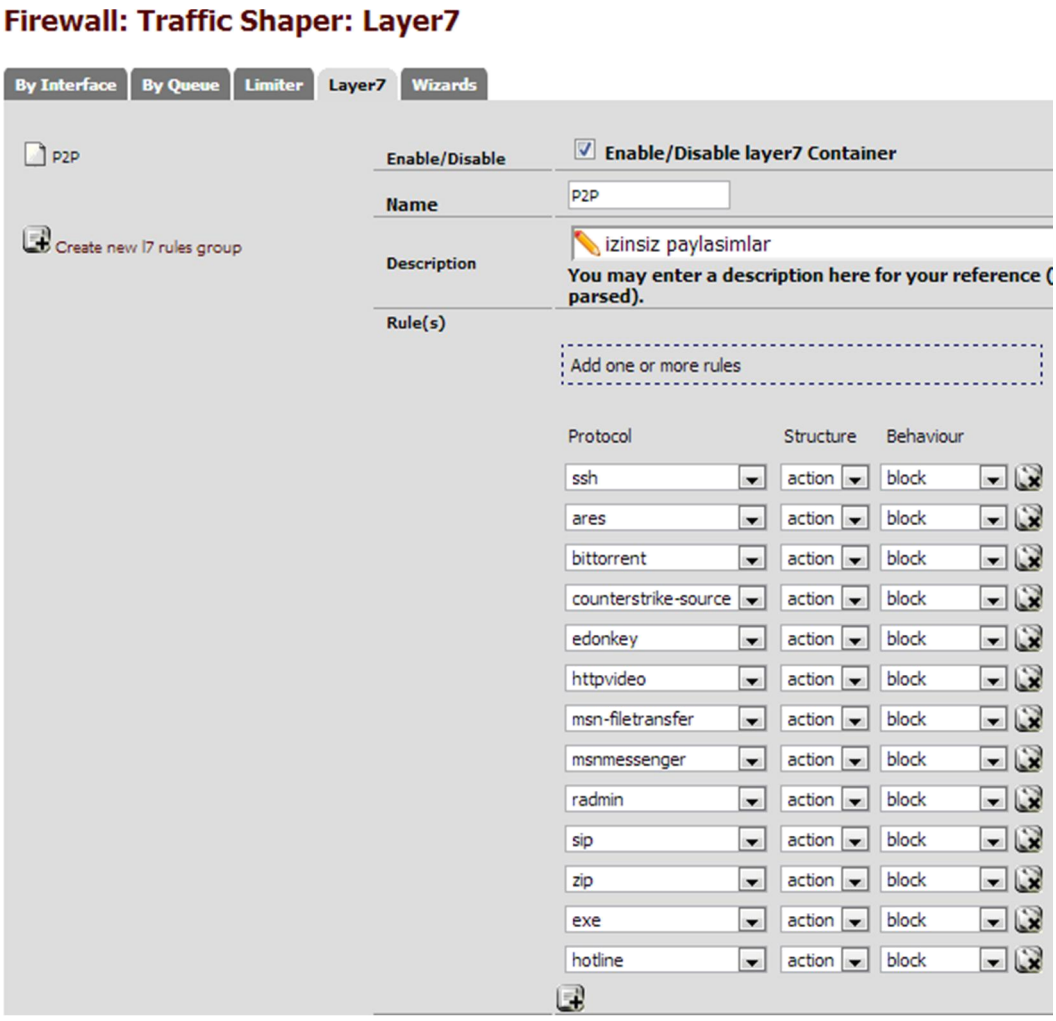
Şekil 3.48 Pfsense yapılandırma - 12

Laboratuvar gibi ortak alanlar için kurallar girilerek istemci trafiği Şekil 3.49'de gösterildiği gibi tanımlanabilmektedir. Böylece bu ağdaki kullanıcılar sistemde sadece verilen izinler çerçevesinde internet hizmetinden faydalanabilmektedir.



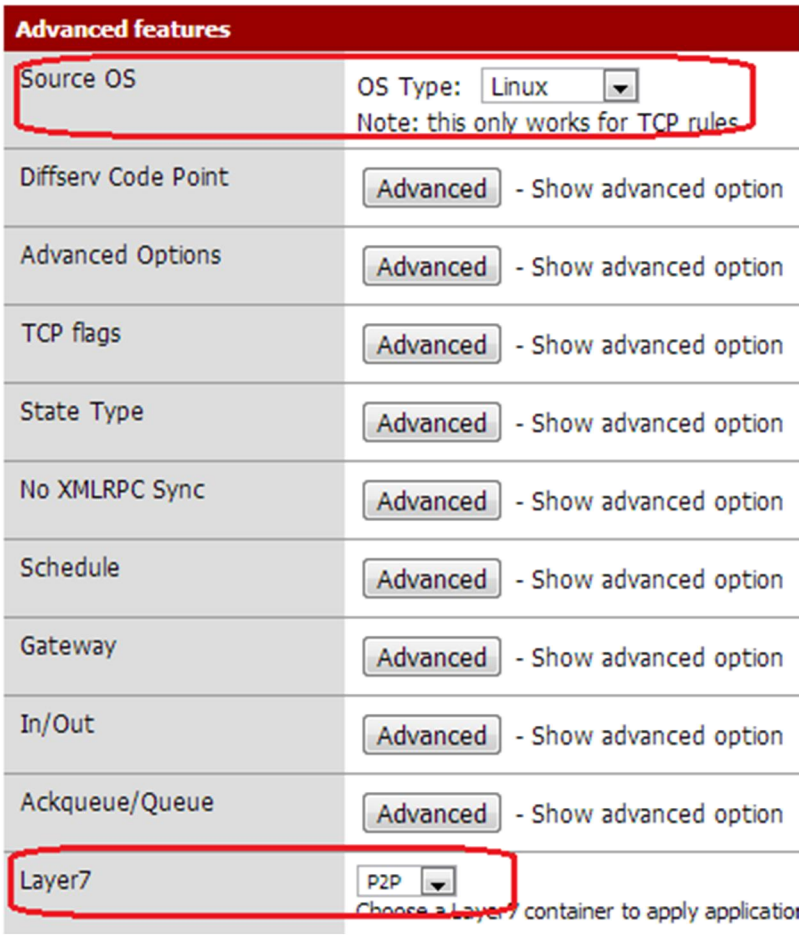
Şekil 3.49 Pfsense yapılandırma - 13

Laboratuvarlar için ayrıca layer7 katmanında bir önlem alınabilmektedir. Şekil 3.50'de de görüldüğü gibi bazı protokollerin erişimi engellenmiştir.



Şekil 3.50 Pfsense yapılandırma - 14

Ayrıca daha farklı kurallarda tanımlanabilmektedir. Şekil 3.51'de olduğu gibi Linux işletim sistemi hariç diğerlerinin internet çıkışı ve P2P uygulamaları yasaklanmıştır.

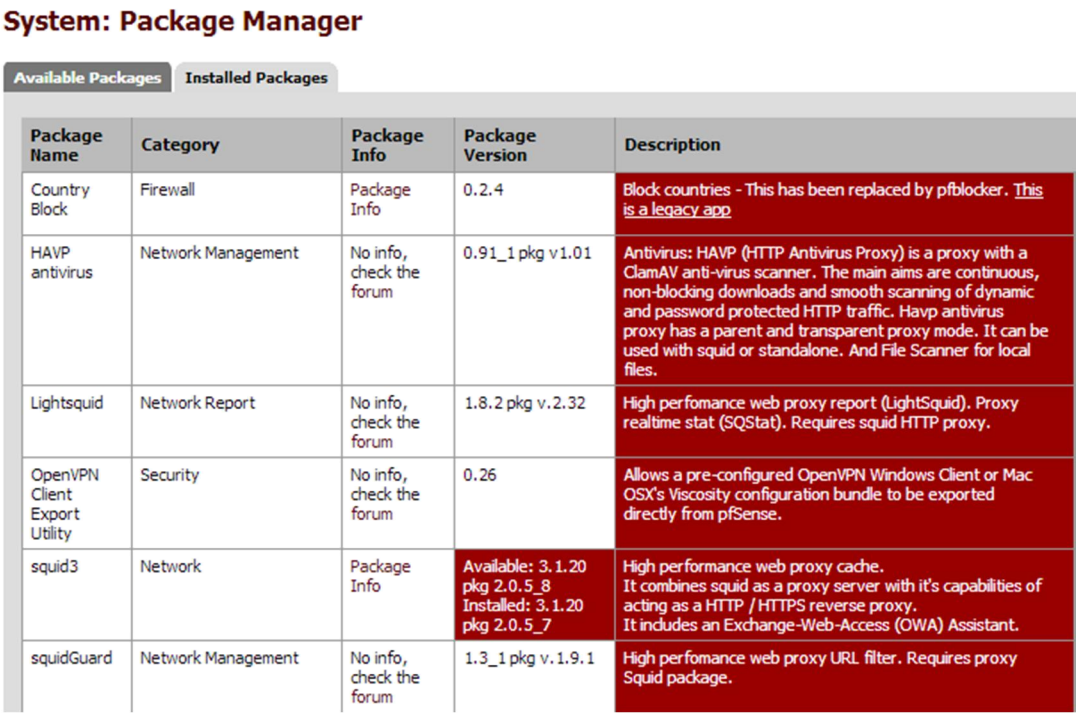


Şekil 3.51 Pfsense yapılandırma - 15

Eğer sistem üzerinde farklı ip blokları kullanılacaksa bu durumda trafiğin güvenlik duvarı üzerinden geçebilmesi için Şekil 3.52'teki gibi yönlendirmeler tanımlanmalıdır.

Şekil 3.52 Pfsense yapılandırma - 16

Güvenlik duvarı üzerinde kullanılacak servisleri Şekil 3.53'te sunulan "System/Packages" sayfasında "Available Packages" sekmesinden yüklenebilmekte aşağıdaki şekilde de yüklü servisler görülmektedir.

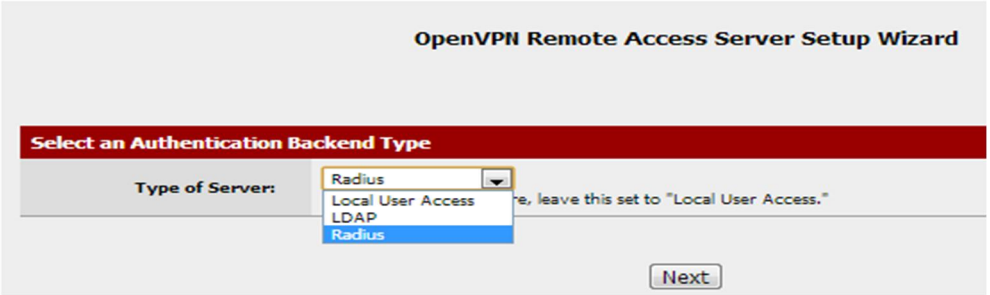


Şekil 3.53 Pfsense yapılandırma - 17

3.2.5.2 Openvpn Yapılandırma

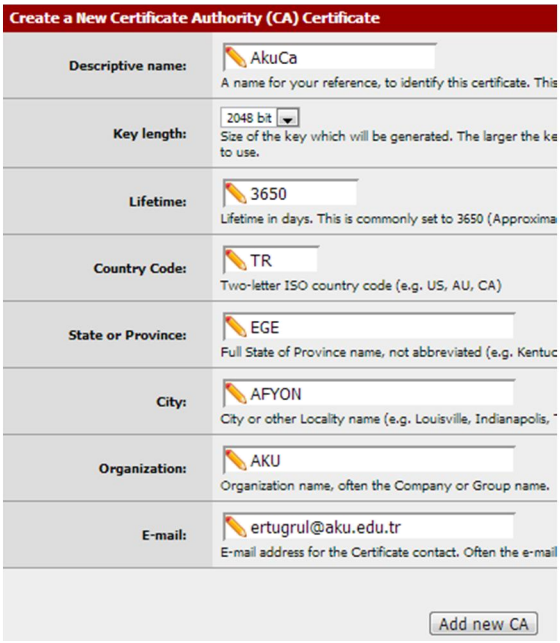
Gerektiğinde uzak noktalardan intranete güvenli erişim yapabilmek için uçtan uca bütün paketlerin bir tünel içinden, dış ortamdan izole edilerek gerçekleştirilen bağlantı türüne vpn diyoruz. Sistem üzerinde kullanılmakta olan sunuculara ya da anahtarlama cihazlarına erişimi güvenli yapabilmek için Openvpn kullanılmaktadır. Openvpn açık kaynak kod üzerine geliştirilmiş bir vpn programıdır. Güvenlik duvarı üzerinde openvpn programının ayarları şu şekilde yapılabilmektedir.

İntranet ağına uzaktan erişim sağlayacak kullanıcıların hangi protokoller üzerinden kimlik doğrulamasının yapılacağını öncelikli olarak belirtilmesi gerekmektedir. Kimlik doğrulama sunucusu olarak Şekil 3.54'da radius sunucu tercih edilmiştir.



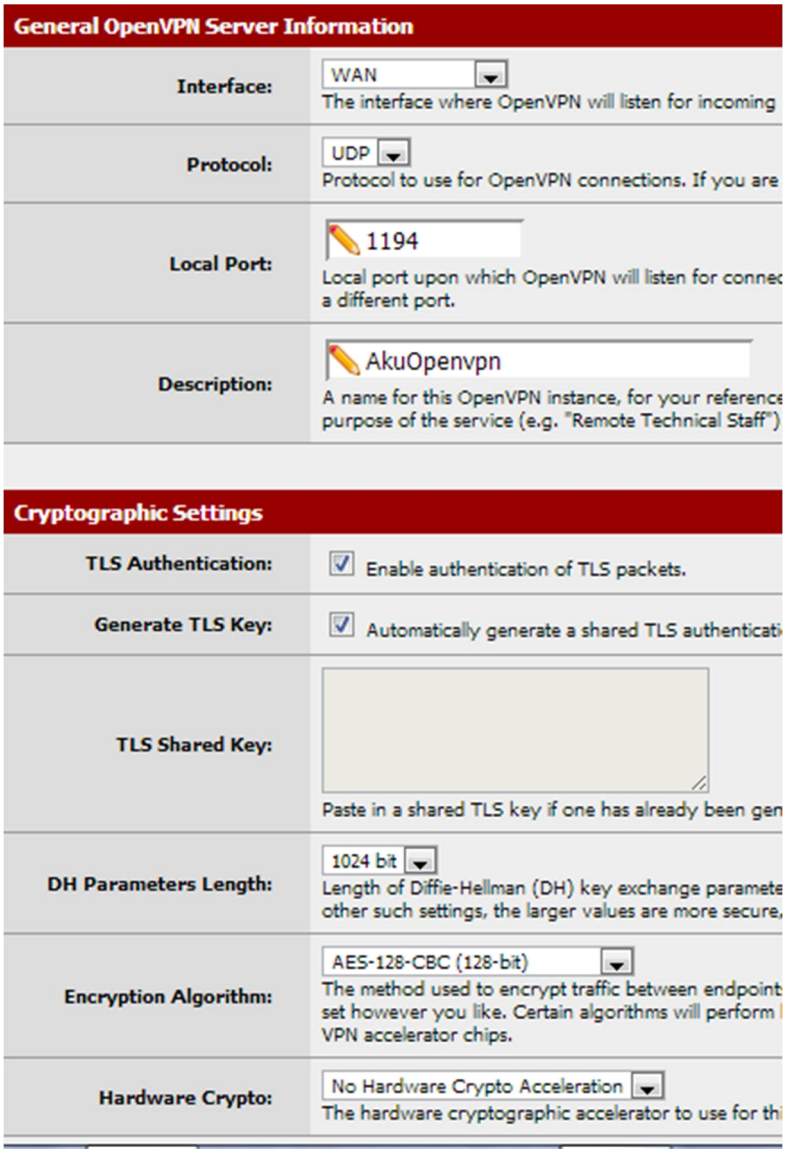
Şekil 3.54 Open vpn Örnek – 1

Bağlantıların şifrelenerek iletilebilmesi için sunucu üzerinde aşağıdaki Şekil 3.55'deki gibi sertifika oluşturularak bir sonraki adıma geçilir.



Şekil 3.55 Open vpn Örnek – 2

Şekil 3.56'da görüldüğü üzere bu alanda vpn bağlantısı oluştururken bağlantının hangi arayüz üzerinden gerçekleştirileceği, kullanılacak protokol ve port ayarları, bağlantı için kullanılacak algoritma şifrelemeleri, hangi ip bloğundan ip alacağı ve erişim sağlanacak ip blokları belirtilmektedir.



Şekil 3.56 Open vpn Örnek -3

Son olarak güvenlik duvarı kurullarını Şekil 3.57'deki gibi etkinleştirerek bağlantı ayarları tamamlanmış olmaktadır.

Şekil 3.57 Open vpn Örnek - 4

3.2.5.3 Captive Portal

Captive Portal tekniği http istemcisini İnterneti normal olarak kullanmadan önce ağ üzerinde özel bir Web sayfasını görmeye zorlar. Captive Portal web tarayıcısını kimlik denetleme cihazına çevirir. Bu işlem, kullanıcı bir tarayıcı açıp internete erişmeye çalışana kadar porttan veya adresten bağımsız olarak bütün paketleri engelleyerek gerçekleştirilir. Bu sırada browser kimlik denetleme ya da basitçe uygun kullanım poliçesini görüntüleyip kullanıcının onaylamasını sağlayacak web sayfasına yönlendirilir. Captive Portal uygulamaları en çok Wi-Fi erişim noktalarında kullanılır. Ayrıca kablolu kullanımı kontrol etmek için de kullanılabilir. (Otel odaları, iş merkezleri, vs.)

Yapılandırma;

Şekil 3.58'da sunulduğu üzere pfsense kurulu olan makinenin LAN arayüzüne atanmış olan IP adresi browser'a yazılarak pfsense yönetim sayfasına bağlanılır. "Ana sayfadan Services -> Captive portal" yoluyla pfsense captive portal yönetim sayfası açılmış olur.

Interface: Bu kısımda kısıtlama portalı'nın çalışacağı arayüz seçilir. (LAN vs.)

Maximum concurrent connections: Bu seçenek aynı anda kaç kişinin portal sayfasını açabileceğini belirler.

Idle timeout: Belirtilen süre kadar eylemsizlik sonunda istemcilerin bağlantısı kesilir. Gerekirse anında tekrar bağlanabilirler.

Hard timeout: Belirtilen süre sonunda faaliyetten bağımsız olarak istemcilerin bağlantısı kesilir. Gerekirse anında tekrar bağlanabilirler. (idle timeout belirlenmemişse kullanımı tavsiye edilmez.)

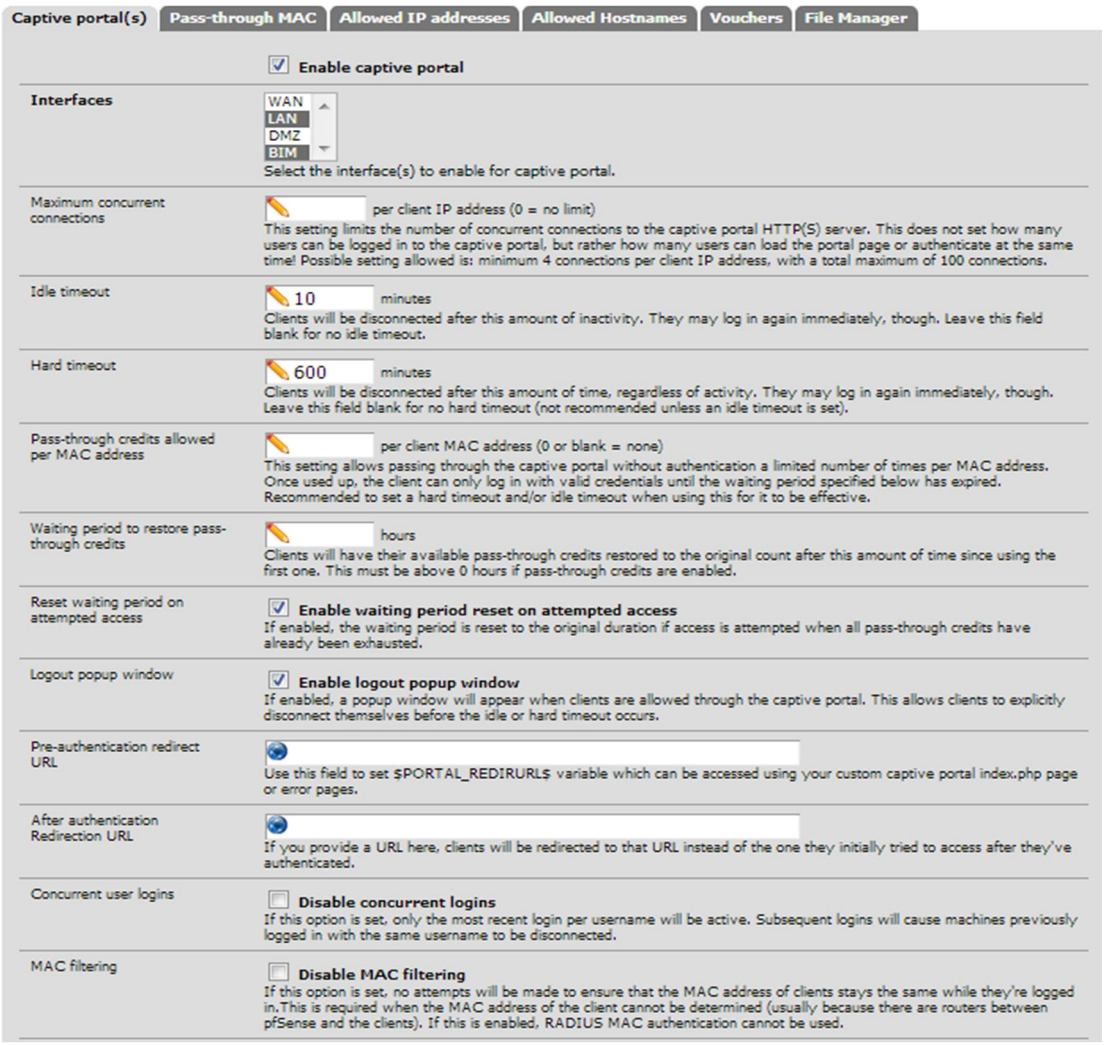
Logout popup window: Etkinleştirildiğinde ve kullanıcılara Captive portal üzerinden izin verildiğinde açılır pencere gözükür.

Redirection URL: Eğer bu kutucuğa bir URL girilirse, istemciler doğrulandıktan sonra ulaşmaya çalıştıkları yerine buna yönlenirler.

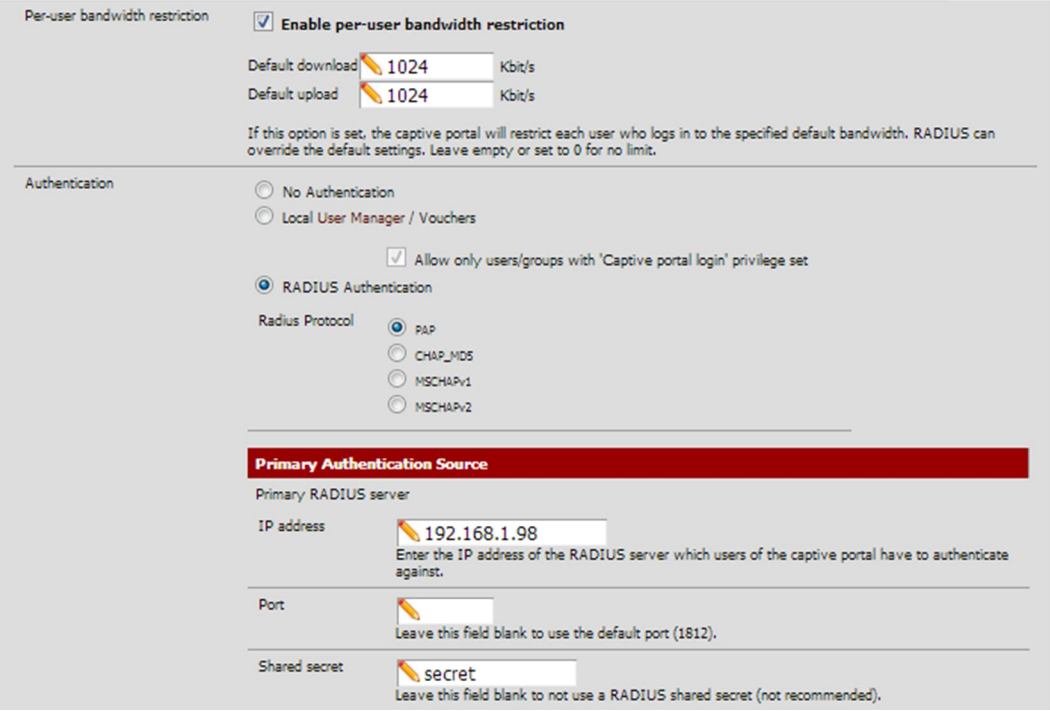
Concurrent user logins: Koyu yazılmış yazının yanındaki kutucuk işaretlenirse bir kullanıcının birden fazla bilgisayardan giriş yapması engellenmiş olur. Girilen son bilgisayar dışındaki bilgisayarlar sistemden atılır.

MAC filtering: Bu seçenek seçilirse kullanıcının MAC adresiinin sabit kaldığını kontrol etmek için bir girişimde bulunulmaz. Bu seçenek istemcinin MAC adresinin saptanamadığı durumlarda gereklidir. Etkinleştirildiğinde "RADIUS MAC authentication" seçeneği kullanılamaz.

Per-user bandwith restriction(Şekil 3.59)**:** Bu kısımdaki download ve upload kutucuklarına istenilen değerler girilerek belirtilen kısıtlama sağlanmış olur.



Şekil 3.58 Captive portal ayarları -1



Şekil 3.59 Captive portal ayarları -2

HTTPS login: Enable HTTPS login (HTTPS girişini etkinleştir) kutucuğu işaretlenirse kullanıcı adı ve şifre takipçilerden korumak için HTTPS bağlantısı üzerinden aktarılır.

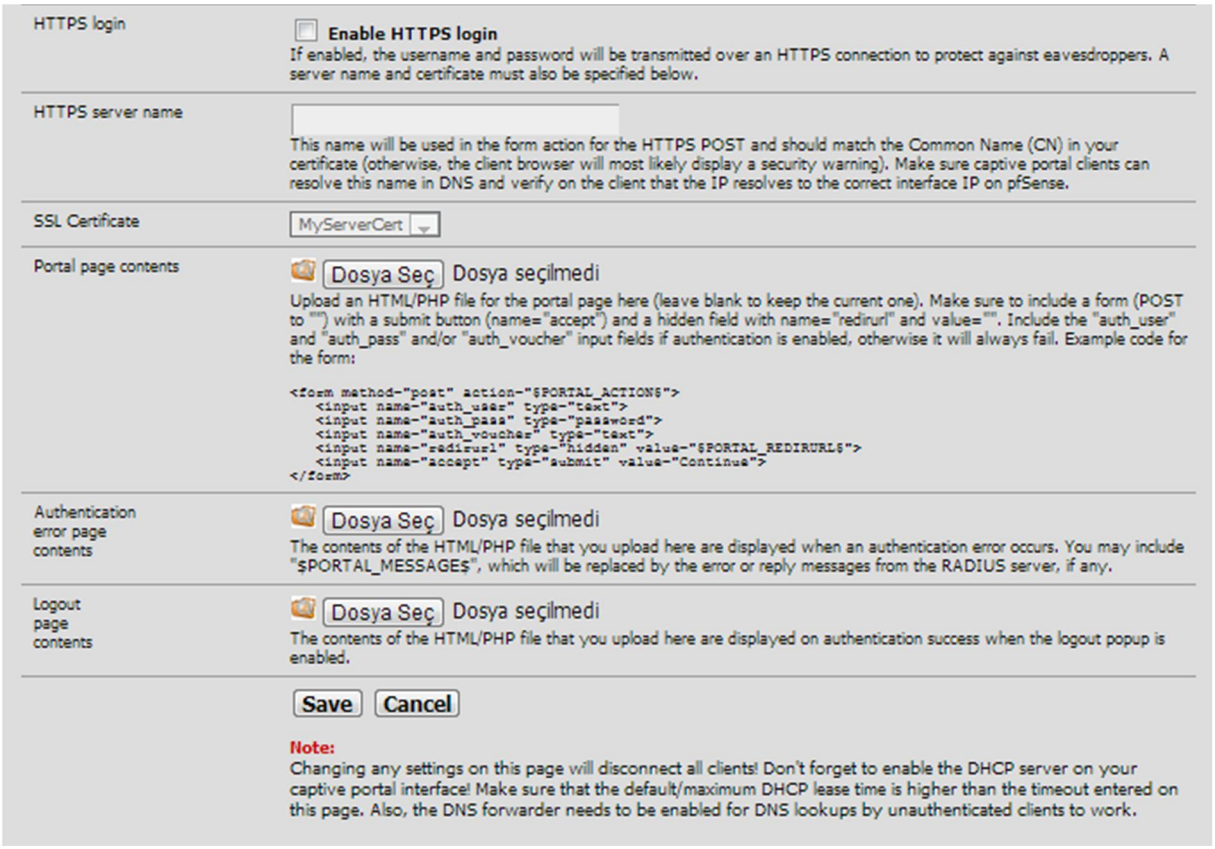
HTTPS server name: Buraya yazılan sunucu adı sertifikadaki Common Name (Ortak İsim) ile uyuşmalıdır.

HTTPS certificate: Bu alana X.509 PEM biçimindeki onaylı sertifika yapıştırılır.

HTTPS private key: Bu alana RSA özel anahtarı PEM biçimince yapıştırılır.

Portal page contents: Bu alana portal sayfası için HTML dosyası yüklenir (Mevcut olanı korumak için boş bırakılır). Gönder tuşu ve name="redirurl" ve value="$PORTAL_REDIRURL$" içeren gizli kısım bulunan form içerdiğinden emin olunmalıdır.

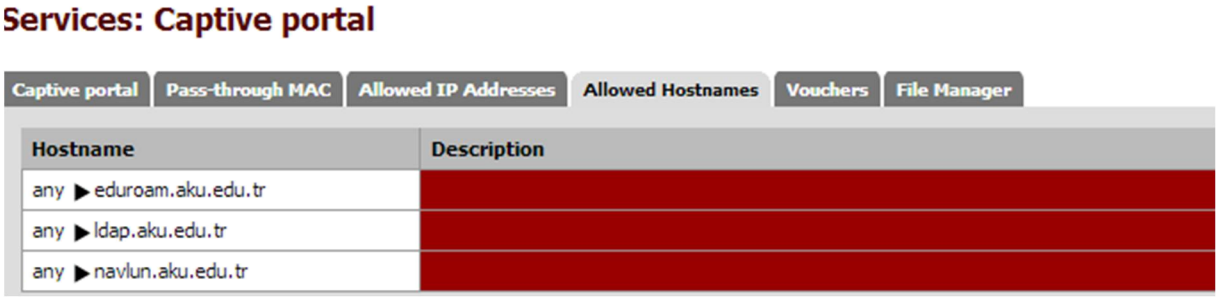
Authentication error page contents: Kimlik doğrulama hatası alındığında bu alana yüklenen HTML dosyasının içeriği görüntülenir.



Şekil 3.60 Captive portal ayarları -3

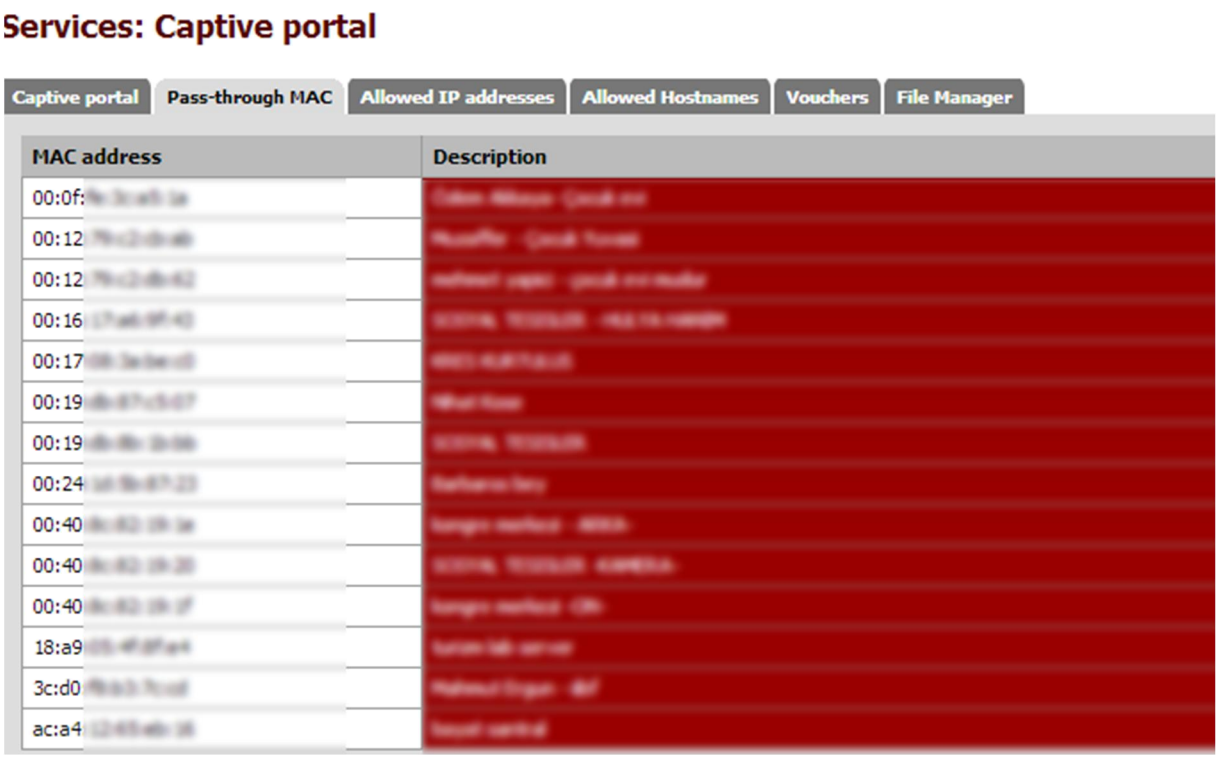
Şekil 3.60'de istenilen kısımlar doldurulduktan sonra sayfa sonunda yer alan Save tuşuna basılarak yapılandırma tamamlanmış olmaktadır.

Diğer taraftan kimlik doğrulaması yapılmadan bazı sunuculara Şekil 3.61'deki gibi erişim hakkı da verilebilmektedir.

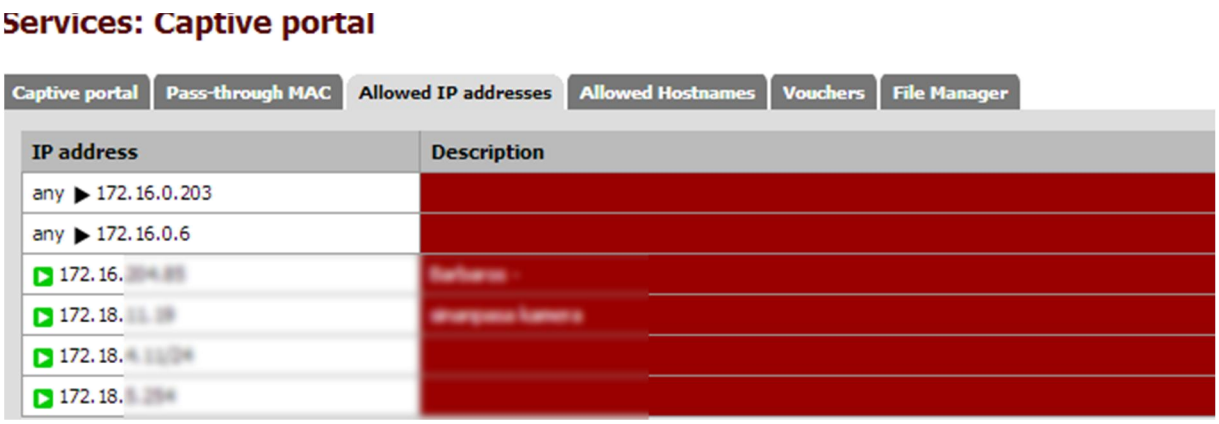


Şekil 3.61 Captive portal izinli hostlar

Ayrıca istenildiği takdirde istemcilerin mac-adresleri (Şekil 3.62) veya ip adresleri (Şekil 3.63) gösterildiği gibi sisteme tanımlanarak internete doğrudan erişim sağlayabilmektedir.



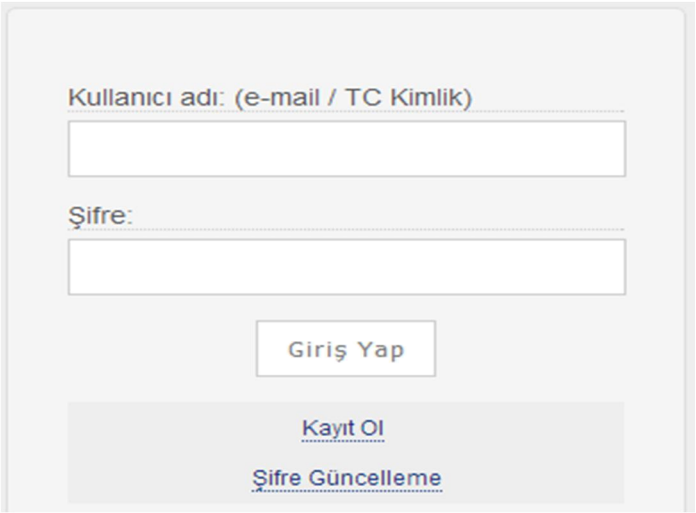
Şekil 3.62 Captive portal izinli mac adresleri



Şekil 3.63 Captive portal izinli ip adresleri

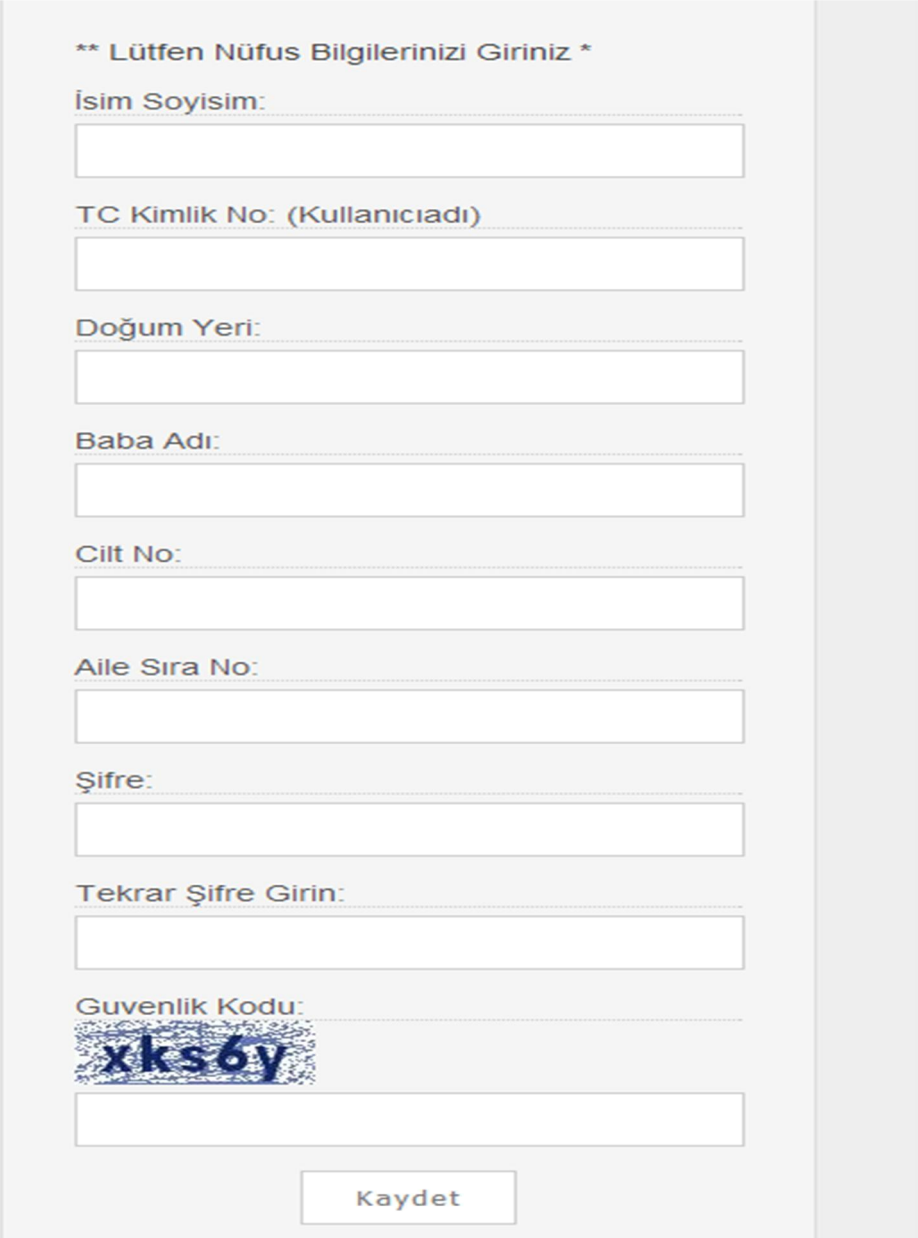
Böylece captive portalla ilgili yapılması gereken ayarlar tamamlanmaktadır.

İstemci web tarayıcısı üzerinden internete giriş isteminde bulunduğu an sistem giriş bilgilerini girebileceği ekrana (Şekil 3.64) yönlendirmektedir.



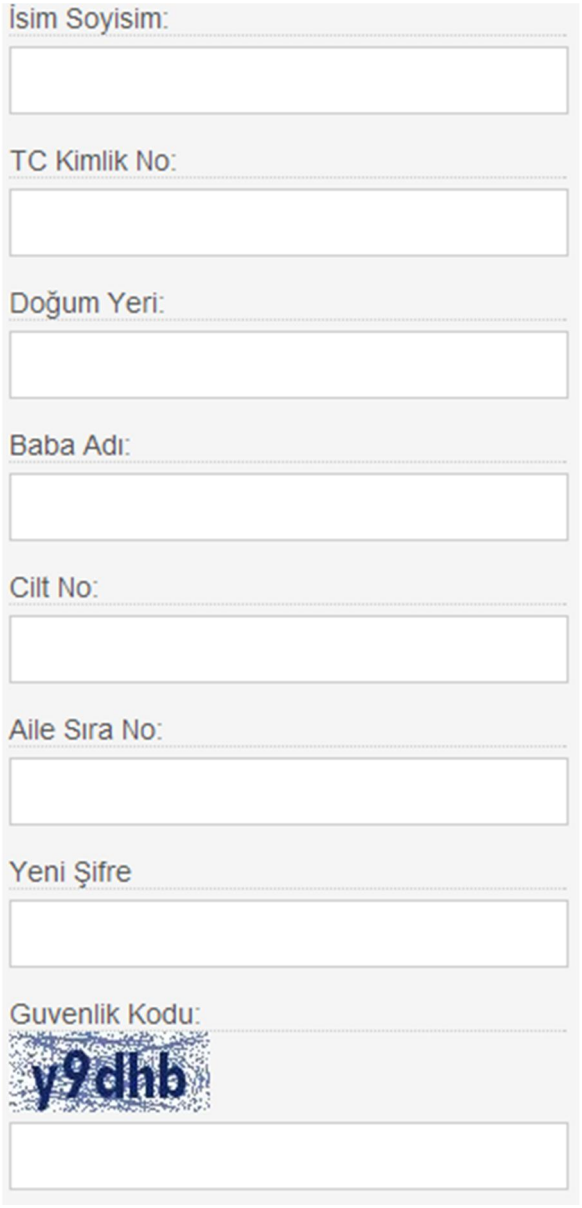
Şekil 3.64 Kullanıcı giriş ekranı

Giriş isteminde bulunan kişi kurum personeli ise kurum e-mail kullanıcı bilgilerini kullanarak sisteme giriş yaparken öğrenci veya misafirlerin ise sistem üzerinden kayıt olmaları gerekmektedir. Şekil 3.65'de gösterildiği üzere kayıt ekranında istenilen bilgiler http://www.nvi.gov.tr adresinden kontrol ettirilerek kullanıcıların bilgileri nüfus idaresinden doğrulanmaktadır.



Şekil 3.65 Kullanıcı kayıt ekranı

Kayıt işlemini gerçekleştirmiş kullanıcılar daha sonraki günler içerisinde kullanıcı bilgilerini unuturlarsa sistem üzerinden doğrulama yapmak kaydıyla şifrelerini değiştirebilmektedirler (Şekil 3.66).



Şekil 3.66 Kullanıcı şifre değiştirme ekranı

Captive portal sistemine giriş yapan kullanıcı listesi Şekil 3.67'de görüntülenebilmektedir. Böylece anlık sistem üzerinde ne kadar kullanıcı bağlı, ip adresleri, mac adresleri ve kullanıcı bilgileri ve hangi saatte sisteme bağlandı bilgileri tutulmaktadır.

Status: Captive portal (56)

IP address	MAC address	Username	Session start
172.18.	00:0f:		01/04/2013 07:41:29
172.18.	00:24		01/04/2013 08:41:54
172.18.	00:24		01/04/2013 08:43:34
172.18.	2c:41:		01/04/2013 08:43:49
172.18.	00:15		01/04/2013 08:44:00
172.18.	00:24		01/04/2013 08:48:02
172.18.	d4:85		01/04/2013 08:49:24
172.18.	f4:6d:		01/04/2013 08:51:14
172.18.	d4:85		01/04/2013 08:53:29
172.18.	00:1d		01/04/2013 08:55:45
172.18.	d4:85		01/04/2013 09:04:04
172.18.	00:15		01/04/2013 09:07:57
172.18.	f4:6d:		01/04/2013 09:09:49
172.18.	60:eb		01/04/2013 09:11:06
172.18.	00:1d		01/04/2013 09:17:38
172.18.	00:1c:		01/04/2013 09:20:51
172.18.	00:22		01/04/2013 09:22:26
172.18.	00:08		01/04/2013 09:24:31
172.18.	00:1c:		01/04/2013 09:31:34
172.18.	d4:85		01/04/2013 09:34:46
172.18.	00:22		01/04/2013 09:37:02
172.18.	00:0f:		01/04/2013 09:40:33
172.18.	d4:85		01/04/2013 09:43:25
172.18.	d4:85		01/04/2013 09:57:38
172.18.	00:1c:		01/04/2013 09:57:55
172.18.	00:22		01/04/2013 09:58:12

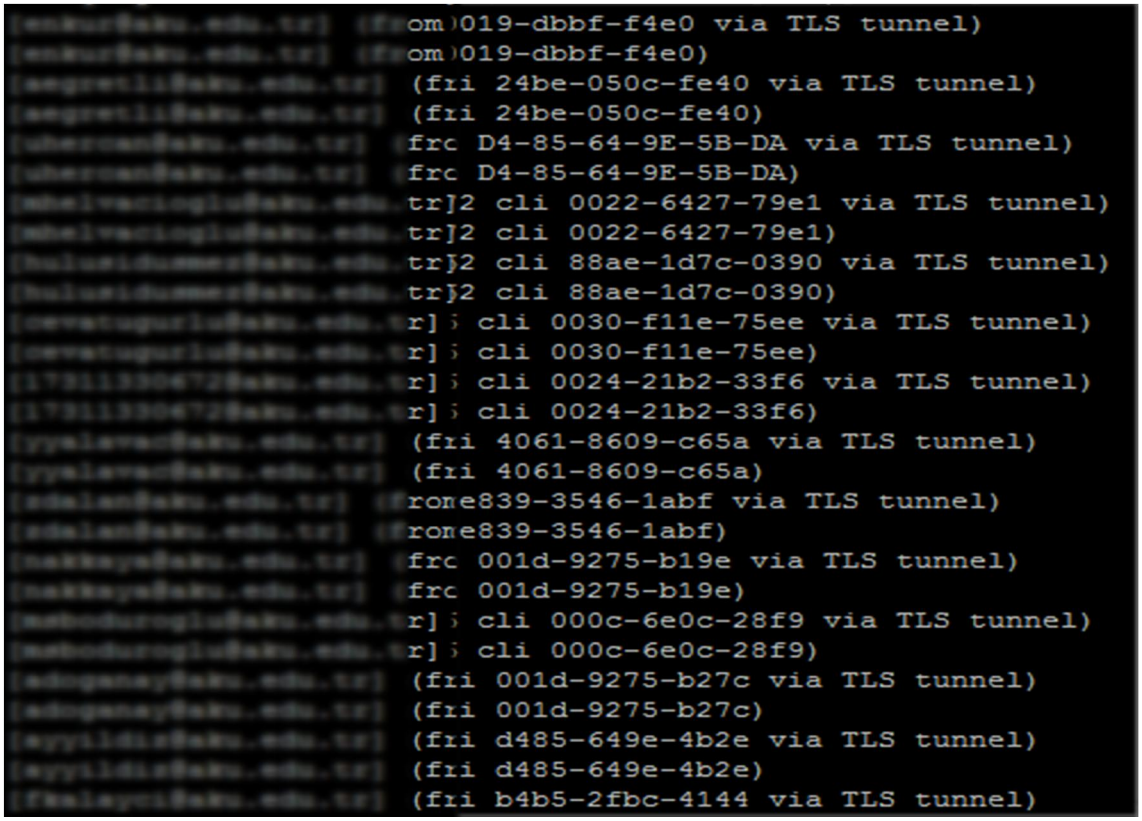
Şekil 3.67 Captiveportal kullanıcı listesi

4. BULGULAR

Üniversite kampüs ağları da internet toplu kullanım sağlayıcılar rolü üstlenmektedir. Bu nedenle Başbakanlık tarafından resmi olarak 01.11.2007 tarihinde yayımlanmış 5651 sayılı kanun kapsamında internet istemci kayıtlarını tutmak ve zaman damgalı bir biçimde 6 aydan 2 yıla kadar saklamak zorunluluğu bulunmaktadır. Bu kapsamda istemcilerin farklı sistemlerde oluşan kayıtları merkezi kayıt sunucusuna aktarılmış, oluşan kayıtlar dijital olarak imzalanarak arşivlenmektedir.

4.1 Radius Sunucu Kayıtları

İstemciler kablolu veya kablosuz olarak bağlantı kurabilmeleri için ilk önce kimlik doğrulama protokolünden geçmek zorunlulukları bulunmaktadır. Radius sunucu farklı veritabanları ile beraber çalışabilmektedir. Bu çalışmada ise radius sunucu open ldap veritabanı ile beraber çalıştırılmış, istemcilerin sistem üzerinde ilk kayıtları kimlik doğrulama protokolü olarak kullanılan radius kayıtlarında saklanmaktadır.



Şekil 4.1 Radius sunucu kayıtları

Şekil 4.1 de görüleceği üzere Radius protokol gereği sadece kullanıcı bilgilerini ve mac adreslerini tutabilmektedir. Bu nedenle Radius kayıtları tek başına bir anlam ifade etmemektedir.

4.2 DHCP Sunucu Kayıtları

Kimlik doğrulamasını başarıyla tamamlayan istemcilere sistem üzerinden otomatik ip adresi atanmaktadır. Çünkü istemciler web sayfalarıyla veya ağa bağlı diğer cihazlarla iletişimlerini tcp/ip protokolü üzerinden gerçekleştirebilmektedirler. Dhcp kayıtlarının bir örneği şekil 4.2'de belirtilmiştir.

IP address	MAC address	IP address	MAC address
172.17.33.144	2c:41:38:28:00:07	172.17.31.223	9c:20:7b:13:99:ce
172.17.32.125	2c:41:38:29:b2:90	172.17.31.234	c8:6f:1d:82:ac:22
172.17.26.186	00:1c:a8:fd:35:22	172.17.31.222	00:1c:b3:c5:21:65
172.17.25.103	2c:41:38:29:92:30	172.17.31.199	e4:ce:8f:c1:a2:82
172.17.24.156	2c:41:38:29:82:40	172.17.31.105	88:53:95:8d:b0:76
172.17.26.242	00:1d:b3:3e:17:b6	172.17.31.250	0c:74:c2:9c:f1:6b
172.17.31.89	ec:85:2f:0d:0a:4a	172.17.31.174	a0:75:91:fa:82:f9
172.17.31.223	9c:20:7b:13:99:ce	172.17.31.143	18:e7:f4:f3:c2:12

Şekil 4.2 DHCP Sunucu Kayıtları

Dhcp sunucu istemcilerin ip adresini ve mac-adresini kayıt altına almaktadır. Dhcp sunucular ağa bağlı bütün cihazlara ip dağıtabildikleri gibi sadece sistemde mac adresi kayıtlı olan istemcilere ip dağıtabilme özelliği de bulunmaktadır.

4.3 Güvenlik Duvarı Kayıtları

Bir sistemde güvenlik cihazlarının önemli bir özelliği de gerçek ip sayılarının yetersiz olmasından dolayı intranet tarafındaki sanal ip alan istemcileri gerçek ip üzerinden çıkış yapmalarını sağlamaktır. Ancak intranet tarafındaki yüzlerce veya binlerce kişi tek

gerçek ip adresi üzerinden çıkış yapabilmektedir. Bu durumda işlenecek herhangi bir adli suç durumunda intranet tarafındaki kişileri tespit etmek oldukça güç olmaktadır.

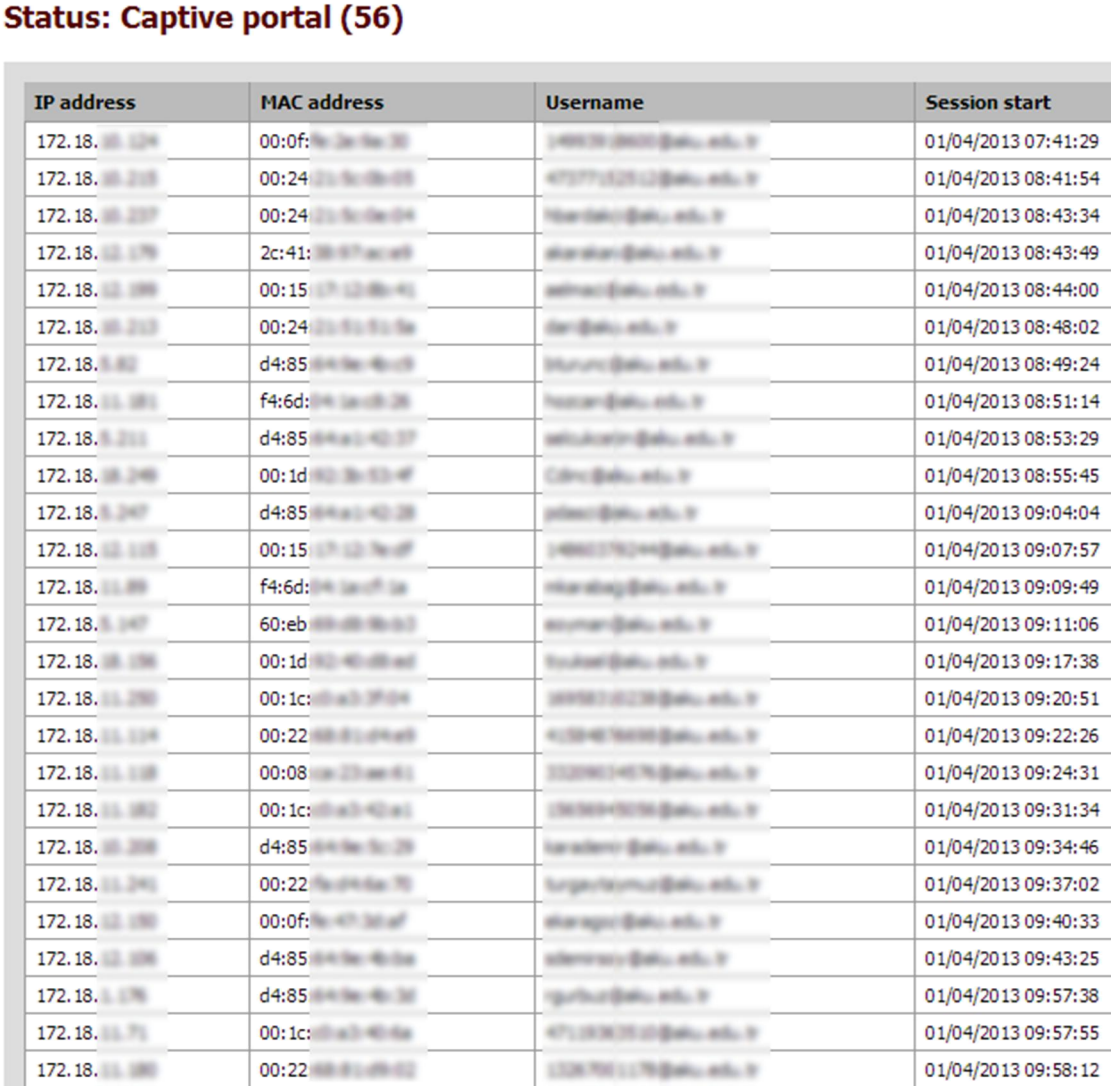
Source	Destination
172.16.0.6:32869	94.198.57.34:53
172.16.0.6:32869	194.146.107.6:53
172.16.48.12:62708	111.221.77.160:40016
172.16.181.254:54098	157.56.135.157:443
172.16.48.18:61439	188.165.224.115:80
172.16.0.6:32869	204.13.251.5:53
172.16.181.254:54097	78.46.69.237:80
172.16.0.6:32869	188.138.96.213:53
172.16.48.18:29044	188.165.224.115:80
172.16.48.20:15757	69.31.16.16:3478
172.16.48.15:4372	95.158.130.204:80
172.16.162.46:53580	193.255.51.103:80
172.16.0.6:32869	93.174.88.78:53
172.16.48.18:34320	188.165.224.115:80
172.16.48.12:29398	64.4.23.150:40003

Şekil 4.3 Güvenlik duvarı kayıtları

Güvenlik duvarları üzerinden geçen trafiğin kayıtlarını tutarken istemcilerle ilgili olarak sadece kaynak ip adresi ve hedef ip adresi bilgilerini şekil 4.3'de gösterildiği gibi tutmaktadır.

4.4 Captive Portal Kayıtları

Sistem üzerinde en anlamlı kayıtlar captive portal üzerinde oluşmaktadır. Çünkü portal üzerinde kimlik doğrulaması yapan istemcilerin ip adresleri, mac adresleri ve kullanıcı bilgileri şekil 4.4'de sunulduğu üzere tutulmaktadır.



Status: Captive portal (56)

IP address	MAC address	Username	Session start
172.18.	00:0f:		01/04/2013 07:41:29
172.18.	00:24		01/04/2013 08:41:54
172.18.	00:24		01/04/2013 08:43:34
172.18.	2c:41:		01/04/2013 08:43:49
172.18.	00:15		01/04/2013 08:44:00
172.18.	00:24		01/04/2013 08:48:02
172.18.	d4:85		01/04/2013 08:49:24
172.18.	f4:6d:		01/04/2013 08:51:14
172.18.	d4:85		01/04/2013 08:53:29
172.18.	00:1d		01/04/2013 08:55:45
172.18.	d4:85		01/04/2013 09:04:04
172.18.	00:15		01/04/2013 09:07:57
172.18.	f4:6d:		01/04/2013 09:09:49
172.18.	60:eb		01/04/2013 09:11:06
172.18.	00:1d		01/04/2013 09:17:38
172.18.	00:1c:		01/04/2013 09:20:51
172.18.	00:22		01/04/2013 09:22:26
172.18.	00:08		01/04/2013 09:24:31
172.18.	00:1c:		01/04/2013 09:31:34
172.18.	d4:85		01/04/2013 09:34:46
172.18.	00:22		01/04/2013 09:37:02
172.18.	00:0f:		01/04/2013 09:40:33
172.18.	d4:85		01/04/2013 09:43:25
172.18.	d4:85		01/04/2013 09:57:38
172.18.	00:1c:		01/04/2013 09:57:55
172.18.	00:22		01/04/2013 09:58:12

Şekil 4.4 Captive Portal kayıt bilgisi

Şekilde de görüldüğü üzere portala bağlı istemciler görüntülenmektedir.

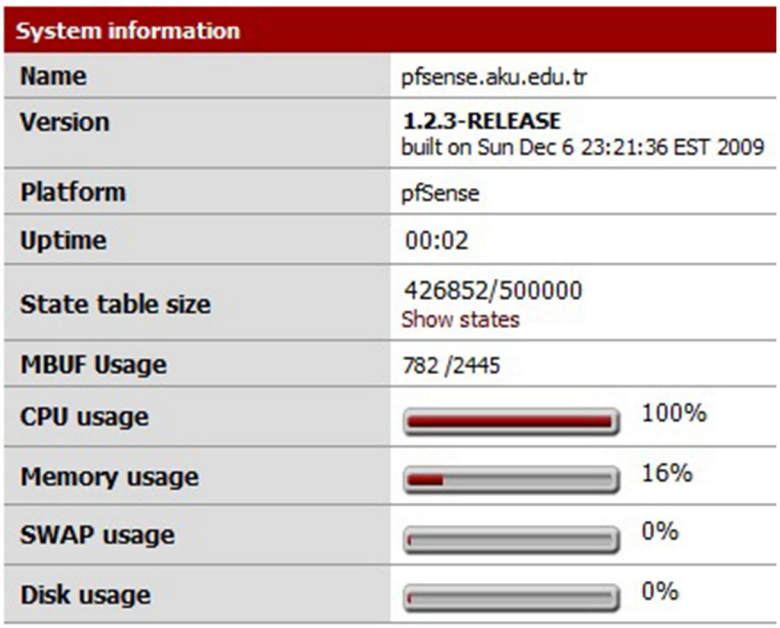
4.5 Kayıt Saklama Sunucusu

Sistem üzerindeki sunucu ve güvenlik duvarı kayıtlarını merkezi kayıt saklama sunucusunda tutulmasını sağlayarak kayıtların tek bir noktada birleştirmesi sağlanmıştır. burada dikkat edilmesi gereken diğer bir durum ise hem kayıt gönderen hem da gelen kayıtları saklayan sunucuların sistem saat bilgileri cihazların kendi saatlerinden değil merkezi bir ntp sunucudan almalıdır. Çünkü oluşan bütün kayıtlarda ortak nokta zaman kriterinin aynı olmasıdır. Böylece sunucuda toplanan tüm kayıtlar zaman damgası ile

imzalanarak saklanmaktadır. Adli bir soruşturma açılması durumunda tutulan kayıtların doğru ve güvenilir olması sağlanmıştır.

4.6 Güvenlik Duvarı Performanslarının Değerlendirilmesi

Yapılan bu çalışmada göz ardı edilemeyecek diğer bir durum ise internet erişim trafiğinin ve güvenlik duvarı sunucusunun kararlı çalışmasıdır. Bu çalışma öncesinde alınan sistem hata kayıtları ile sonrasında alınan hata kayıtları arasında gözle görünür bir düzelme kaydedilmiştir.



Şekil 4.5 Güvenlik duvarı uyarı mesajı

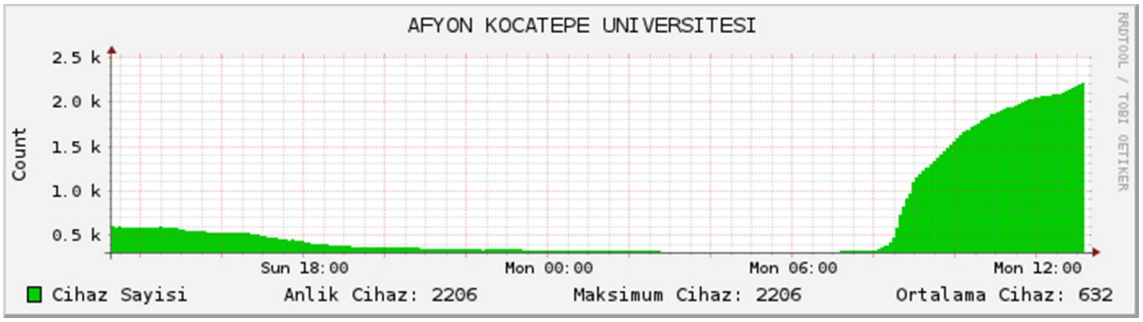
Şekil 4.5'de de görüldüğü üzere güvenlik duvarının cpu değerleri %100 leri bulmaktadır. Ağ cihazlarının yapılandırılması sonucu yüksek cpu kullanım oranları Şekil 4.6'da %10 lar seviyesine gerilemiştir.

Last config change	Thu Mar 28 6:14:10 EET 2013
State table size	82238/895000 Show states
MBUF Usage	6918/25600
Temperature	8.3°C
Load average	0.76, 0.57, 0.45
CPU usage	7%
Memory usage	5%
SWAP usage	0%
Disk usage	0%

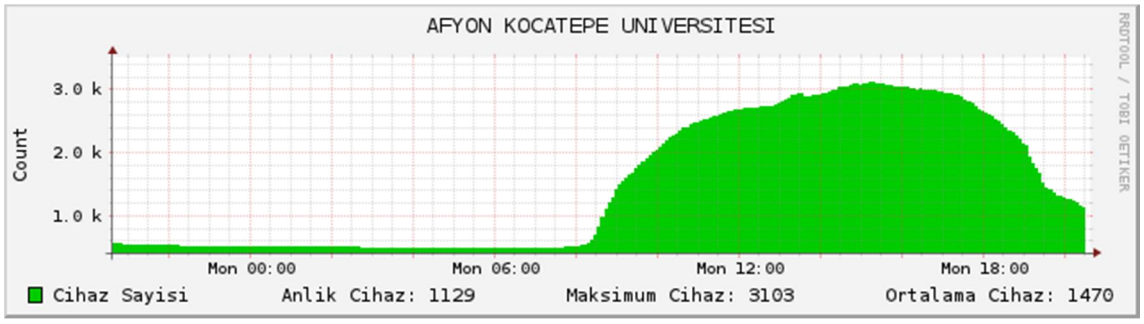
Şekil 4.6 Güvenlik duvarı sunucu performans değerleri

4.7 Ağ İstatistikleri

Çalışma öncesi internet kullanımı ile çalışma tamamlandıktan sonraki internet kullanımı arasında Şekil 4.7 ve Şekil 4.8'de görüldüğü üzere internet kullanımı % 40 oranında artış sağlamıştır. Ancak bu çalışmayla internet kullanımı kararlı bir hale getirilerek hat arttırımına gidilmemiştir.

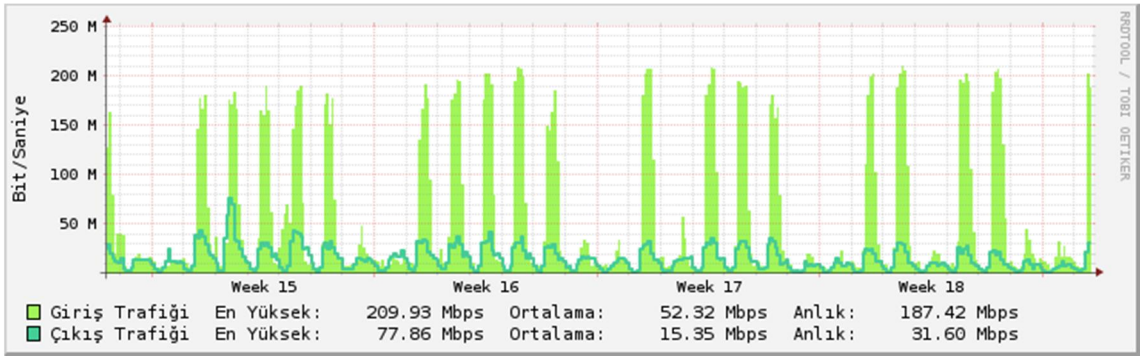


Şekil 4.7 Çalışma öncesi cihaz sayısı



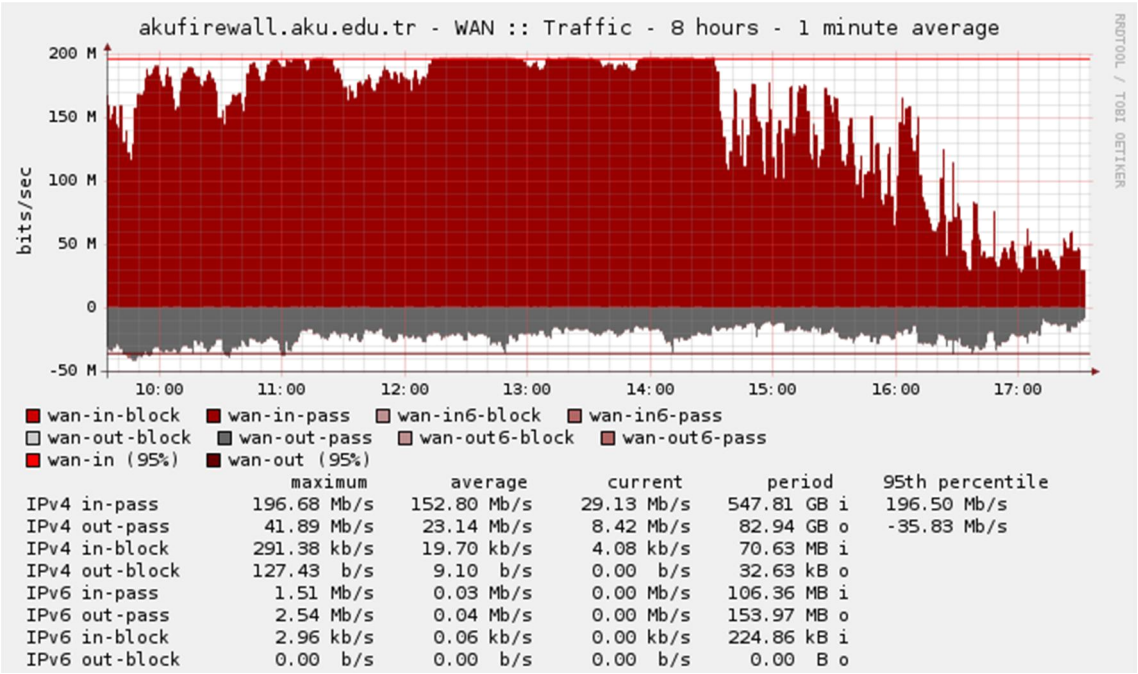
Şekil 4.8 Çalışma sonrası cihaz sayısı

İnternet erişim cihazlarının bu kadar artmasında en önemli sebep ise bilgisayar laboratuvarları ve kablosuz erişim cihaz sayılarının artması olarak gözlemlenmiştir. Yıl içerisinde internet ağ kullanım oranının değişimini Şekil 4.9'da görülebilmektedir.



Şekil 4.9 Yıl içinde internet kullanım oranı

Pfsense güvenlik yazılımıyla birer dakikalık arayla oluşan sekiz saatlik internet kullanım grafiği Şekil 4.10'da gösterilmektedir. Grafik üzerinde kullanılan maksimum band genişliğini, maksimum dosya yükleme oranları görülmektedir. Bunun yanında güvenlik duvarından geçen izinli internet erişim kayıtları ile yasaklanmış internet kayıtları grafikte gösterilmektedir.



Şekil 4.10 Pfsense güvenlik duvarının internet ağ kullanım grafiği

Ulakbim'den alınan raporlarda Çizelge 4.1 ve Çizelge 4.2'de de görüldüğü üzere 2012 yılında internetten aylık ne kadar veri kullanıldığı görülebildiği gibi yıllık olarak da toplam 145 TB bir verinin işlendiği gözlemlenmektedir.

Çizelge 4.1 2012 Yılı dosya aktarım istatistikleri (Birim/Tb)

	Ocak	Şubat	Mart	Nisan	Mayıs	Haz.	Tem.	Ağu.	Eylül	Ekim	Kasım	Aralık	Top
In	12.57	10.93	14.03	11.48	14.9	11.66	9.5	8.19	9.39	11.29	14.32	16.75	145
Out	11.38	4.57	3.57	3.39	5.43	5.95	3.62	2.2	3.18	3.43	4.57	4.15	55.4
Max	12.57	10.93	14.03	11.48	14.9	11.66	9.5	8.19	9.39	11.29	14.32	16.75	145
Sum	23.94	15.51	17.6	14.86	20.33	17.61	13.12	10.39	12.57	14.72	18.89	20.9	200

Çizelge 4.2 2013 Yılı dosya aktarım istatistikleri (Birim/Tb)

	Ocak	Şubat	Mart	Nisan	Mayıs	Haz.	Tem.	Ağu.	Eylül	Ekim	Kasım	Aralık	Top
In	15.55	14.55	19.48	17.33	2.1	0	0	0	0	0	0	0	69.01
Out	4.96	3.9	4.42	5	499 G	0	0	0	0	0	0	0	18.77
Max	15.55	14.55	19.48	17.33	2.1	0	0	0	0	0	0	0	69.01
Sum	20.52	18.45	23.9	22.33	2.58	0	0	0	0	0	0	0	87.78

Ayrıca 55.45 TB'lık veri de internet ortamına yüklenmiştir. 2013 yılında ise aylık bazda bir artış gözlemlendiği gibi toplam 69.01 TB veri indirilmiş, 18.77 TB'lık veri internet ortamına yüklenmiştir. Şekillerin ilk 4 aylık veri aktarım oranlarına bakıldığında 2013 yılında daha fazla veri aktarımının yapıldığı gözlemlenmektedir. Bu kadar hızla büyümekte olan kampüs ağını yönetebilmek için kullanımı esnek olan aynı zamanda internet erişimi ile ilgili farklı raporların alınabildiği yönetiminin web arabiriminden kolaylıkla yapılabildiği, kullanıcı dostu bir güvenlik duvarı tercih edilmelidir.

5. TARTIŞMA ve SONUÇ

Kampüs ağlarında sistem güvenliği kenar noktalardan merkeze kadar yaygınlaştırılmıştır. Çünkü merkezi bir sistem güvenliği yeterli olamamaktadır. Sadece merkezi alınan güvenlik önemlerinin performansı son derece düşürdüğü gözlenmiştir. Bu nedenle güvenlik sistemini farklı sistemlere dağıtarak yük dengelenmesi sağlanmıştır.

Yapılan bu çalışmada son kullanıcıların yerel sunuculara veya internet erişim sağlayıcılara erişim aşamaları ele alınmıştır.

Ağ tabanlı güvenlik;

Son kullanıcıların kablolu veya kablosuz internet erişimi sağlayabilmeleri için kimlik doğrulaması 802.1x protokolü sağlanmıştır. Böylece sisteme yetkisiz kimselerin erişimi engellenmiştir.

Port bazlı broadcast ve arp trafiği sınırlandırılmıştır. Böylece ağ üzerinde istemcilerden kaynaklanan sorunların %70'lerden %15'lere kadar düşmesi sağlanmıştır.

Ağda sahte dhcp sunucuların ip dağıtımı engellenmiştir. Böylece sahte dhcp sunucuların sistemde oluşturabilecekleri sorunlar engellenmiştir.

Kullanıcıların elle ip vermesi engellenerek bütün istemcilerin otomatik ip alması sağlanmıştır. Böylece hem kullanıcıların kimlik tespiti yapılırken gerekli olan ip ve mac adresleri dhcp sunucuda saklanmıştır. Hem de sahte ağ geçidini ele geçirmeye çalışan virüs veya saldırganlara karşı önlem alınmıştır.

Bir uçtan aynı anda bir istemcinin sisteme erişimine izin verilmiştir. İstemcilerin ağda sahte mac adresleri üreterek dhcp sunucuya yönelik saldırıları önlenmiştir.

Sistem kontrolsüz ağ cihazlarının erişimine kapatılmıştır. Sistem yöneticilerinden izinsiz cihazların ağa bağlanmaları engellenmiştir. Ağ trafiğini kilitleyebilecek, istemcilerin bağlantısını düşürebilecek girişimler önlenmiştir.

Anahtarlama cihazları üzerinde alınan bu güvenlik önlemleri neticesinde son kullanıcılardan merkeze gelebilecek kontrolsüz trafiğin önüne geçilmeye çalışılmıştır.

Sistem tabanlı güvenlik;

Bu çalışmada captive portal kimlik doğrulama uygulaması kullanılmıştır. Bu sistemin tercih edilmesinin en önemli nedeni kenar anahtarlama cihazlarının yönetilememesi, herhangi bir kural tanımlanmasına izin verilememesinden dolayı bu uygulama tercih edilmiştir. Bütün trafiğin güvenlik duvarı üzerinden geçmesi ağ performansını ciddi bir şekilde etkilemiştir. Bu sebeple güvenlik duvarından en iyi performansı alabilmek için sunucunun donanım özelliklerine dikkat edilmiştir.

İstemcilerin sistem üzerinden kullanıcı adı ve şifrelerini oluşturabilmeleri için captive portal üzerinde yazılım geliştirilmiştir. Bütün istemcilerden kayıt yapabilmeleri sağlanmıştır. Kimlik bilgileri http://nvi.gov.tr adresinden kontrol ettirilmiştir. Girilen bilgiler eşleştiğinde kayıt işlemi başarılı olarak gerçekleşmiştir.

Bu çalışmanın devamında; kimlik doğrulama sistemi olarak windows aktif dizin veya vekil sunucuların kurulumu yapılabilir. Bu sunucuların sistem üzerindeki performansları değerlendirilebilir. İstemcilerin kullanıcı adı ve şifre bilgilerinin cep telefonuna gelebilmesi için mevcut uygulama üzerinde geliştirme yapılabilir.

6. KAYNAKLAR

Acharya , H., & Gouda, M. (2011). Firewall verification and redundancy checking are equivalent. . INFOCOM 2011. 30th IEEE International Conference on Computer Communications, 2123-2128.

Aysal, H. (Ocak 2007). Güvenlik ve İnternet Erişim Politikaları Oluşturulması: İstanbul Üniversitesi'nde Uygulama Süreci. Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Başer, M. (2004). Ağ ve Sistem Yöneticileri için Linux Ağ Servisleri. İstanbul.

Cali, F., Conti, M., & Gregori, E. (1998). IEEE 802.11 Wireless Lan: CapacityAnalysis . *IEEE INFOCOM 1998 - The Conference on* , **1**: 142 – 149.

Cuihong, W. (2010). The problems in campus network information security and its solutions. in Industrial and Information Systems (IIS). 2nd International Conference on. 2010.

Çakar, H. (2005). Bilgisayar ağ güvenliği ve güvenlik duvarları. Yüksekl Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

Çölkesen, R. (2012). İnternet Omurgasının Altyapısı NETWORK TCP/IP UNIX. Papatya Yayıncılık, İstanbul.

Dennis, M., Keith, R., & Louis, D. (2007). *Security and interconnection of medical.* USA: Department of Veterans Affairs, Veterans Health Administration.

Deregözü, R. (1999). Bilgisayar ağlarında güvenlik sorunu "Firewall" kullanarak ağgüvenliğini sağlama. Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Dertler, F. (2000). Network Sistemleri. Sistem Yayıncılık, İstanbul.

Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion. Information Security Technical Report.

Gömez, J., Gil, C., Padilla, N., Banos, R., & Jimenez, C. (2009). Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living. *Lecture Notes in Computer Science*, 515-522.

Gülmüş, M. (2010). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Gürkaş, G. (2005). Kablosuz Güvenlik Protokollerinin Karşılaştırmalı Analizi. Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Ido, D. (2007). How to Cheat at Securing Your Network. *Topologies and IDS*, 281-315.

Karatabak, G. (2006). Açık Sistemdeki Güvenlik Duvarı Kullanarak Ağdaki Paketlerin Kontrolü. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

Karygiannis, T., & Owens, L. (November 2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices.* Gaithersburg, MD 20899-8930.

Mahler, K. (1999). Cisco Certified Network Associate. *Cisco Press*, 507.

Öner, D. (2010). Bilgisayar Ağları. Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Şahin, Y. L. (2005). İnternette Güvenlik ve Saldırı Sezme Sistemleri. Yüksek LisansTezi, Anadolu Üniversitesi, Fen Bilimleri Enstitüsü, Eskişehir.

Tübitak, U. (2009). Sınır Güvenliği Eğitimi. Kocaeli.

Yüksel, Z. (2007). Ağ Güvenliği ve Güvenlik Duvarında Vpn ve Nat Uygulamaları. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

İNTERNET KAYNAKLARI

1. http://www.bilgiguvenligi.gov.tr/guvenlik-testleri/bt-varliklarinin-guvenlik-testi-adimlari-3.html
   Erişim Tarihi : 10.01.2013
2. http://www.11820.com.tr/?p=379
   Erişim Tarihi : 08.04.2013
3. http://www.adslmerkezi.com/hub-nedir-nasil-calisir/
   Erişim Tarihi : 15.01.2013
4. http://www.bilgius.com/switch-ile-hub-arasindaki-farklar/hublar/
   Erişim Tarihi : 15.01.2013
5. http://www.mtuncel.com/bilgisayaraglari.htm
   Erişim Tarihi : 22.03.2013
6. http://manageditsystems.com/?attachment_id=47
   Erişim Tarihi : 18.01.2013
7. http://www.techniquenet.co.uk/technique-network-services/fibre-optic-network
   Erişim Tarihi : 20.03.2013
8. http://csirt.ulakbim.gov.tr/dokumanlar/GuvenlikDuvariCozumuOlusturmaSureci.pdf
   Erişim Tarihi : 04.04.2013
9. http://www.fortinet.com/products/fortigate/3600C.html
   Erişim Tarihi : 02.03.2013
10. http://www.beyaz.net/tr/guvenlik/dokumanlar/utm-nedir.html
    Erişim Tarihi : 03.03.2013
11. http://www.secretflow.com/icerik.asp?tur=1&aid=90&agac=,35,90
    Erişim Tarihi : 31.12.2012
12. http://www.utmfirewall.net/untangle/untangle-hakkinda/
    Erişim Tarihi 05.03.2013
13. http://mouweb.com/?p=1397
    Erişim Tarihi : 01.04.2013
14. http://www.enderunix.org/docs/efw.pdf
    Erişim Tarihi : 01.09.2013

15. http://www.ticnologia.pt/noticias/seguranca-informatica/endian-firewall-community-25-e-disponibilizada.html
Erişim Tarihi : 14.01.2013
16. http://www.placona.co.uk/172/linux/iptables-opening-server-ports-to-specific-ip-addresses/
Erişim Tarihi : 15.01.2013
17. http://www.hp.com/hpinfo/newsroom/press_kits/2011/InteropLasVegas2011/images/HP_S6100N_16Gbps_IPS_Bundle.jpg
Erişim Tarihi : 20.01.2013
18. http://cisn.metu.edu.tr/snort.php
Erişim Tarihi : 06.04.2013
19. http://www.hwturk.com/wp-content/uploads/2009/07/pfsense-snort-kurulum-08.jpg
Erişim Tarihi : 31.03.2013
20. http://ab.org.tr/ab13/bildiri/121.docx
Erişim Tarihi : 20.02.2013
21. http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43
Erişim Tarihi : 25.02.2013
22. http://www.interpeak.com/files/firewall.pdf
Erişim Tarihi : 03.04.2013
23. http://www.uit.co.th/
Erişim Tarihi : 02.02.2013
24. http://www.misco.co.uk/Product/164910/HP-5120-24G-SI-24-Port-Gigabit-Switch
Erişim Tarihi : 11.03.2013
25. http://www.cisn.odtu.edu.tr/2009-17/freeradius.php
Erişim Tarihi : 15.03.2013
26. http://ozkulablog.com/centos-vs-ubuntu-karsilastirmasi.html
Erişim Tarihi : 12.03.2013
27. http://www.cisn.odtu.edu.tr/2009-17/freeradius.php
Erişim Tarihi : 07.04.2013

28. http://members.comu.edu.tr/iturkyilmaz/BM216Dersler/ders5.pdf
Erişim Tarihi : 15.03.2013
29. http://www.webmastersitesi.com/network-internet/749913-openldap-nedir.htm
Erişim Tarihi : 16.03.2013
30. http://searchnetworking.techtarget.com/Configuring-VLANs
Erişim Tarihi : 20.03.2013
31. http://www.cozumpark.com/blogs/cisco_system/archive/2009/01/17/vlan-temel-konfigurasyonu.aspx
Erişim Tarihi : 25.03.2013
32. http://www.agciyiz.net/wp-content/uploads/2009/12/DHCP-Snooping-Ataklar%C4%B1.pdf
Erişim Tarihi : 30.03.2013
33. http://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katman-saldirilari-5-3.html
Erişim Tarihi : 30.03.2013
34. http://www.tib.gov.tr/tr/tr-menu-55-ip_log_imzalayici_programi.html
Erişim Tarihi : 31.03.2013

ÖZGEÇMİŞ

Adı Soyadı	: Ahmet ERTUĞRUL
Doğum Yeri ve Tarihi	: Kızılyurt – 16.02.1982
Yabancı Dili	: İngilizce
İletişim (Telefon/e-posta)	: ertugrul@aku.edu.tr
Eğitim Durumu (Kurum ve Yıl) :	
Lise	: Muğla İmam Hatip Lisesi 2000
Önlisans	: Yüzüncü Yıl Üniversitesi 2003
Lisans	: Anadolu Üniversitesi 2009
Yüksek Lisans	:
Çalıştığı Kurum/Kurumlar ve Yıl :	
Afyon Kocatepe Üniversitesi 2004 -	