T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ

GÜVENLİ AĞ ERİŞİMİ VE KİMLİK DOĞRULAMA

Yüksek Lisans Tezi

İlker ÖZKAN

İstanbul, 2011

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü
Bilgi Teknolojileri Yüksek Lisans Programı

GÜVENLİ AĞ ERİŞİMİ VE KİMLİK DOĞRULAMA

Yüksek Lisans Tezi

İlker ÖZKAN

Tez Danışmanı: Yrd.Doç.Dr.Yalçın ÇEKİÇ

İstanbul, 2011

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü
Bilgi Teknolojileri Yüksek Lisans Programı

Tezin başlığı : Güvenli Ağ Erişimi ve Kimlik Doğrulama
Öğrencinin Adı Soyadı : İlker Özkan
Tez Savunma Tarihi : 9 Eylül 2011

Bu yüksek lisans tezi Fen Bilimleri Enstitüsü tarafından onaylanmıştır.

Doç.Dr. F. Tunç BOZBURA
Enstitü Müdür V.

Bu tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans Tezi olarak yeterli görülmüş ve kabul edilmiştir.

Tez Sınav Jürisi Üyeleri :

Yrd. Doç. Dr. Yalçın ÇEKİÇ (Tez Danışmanı) :

Yrd. Doç. Dr. Mehmet Alper TUNGA :

Yrd. Doç. Dr. Orhan GÖKÇÖL :

ÖZET

GÜVENLİ AĞ ERİŞİMİ VE KİMLİK DOĞRULAMA

Özkan, İlker

Bilgi Teknolojileri Yüksek Lisans Programı

Tez Danışmanı: Yrd.Doç.Dr.Yalçın Çekiç

Eylül 2011, 52 Sayfa

Günümüzde bilgisayar ağlarının güvenliğini sağlamak için birçok yöntem mevcuttur ve her geçen gün geliştirilmektedir. Kullanılan bu yöntemlerden bazıları güvenlik açığına sahip olup, bazıları da yaşanan zorluklar nedeniyle tam anlamıyla uygulanamamaktadır.

Bu çalışmada, yaygın olarak kullanılan kablolu ve kablosuz ağ yapıları ve ağ standartları anlatılmış, ağ erişim ve kimlik yönetim metotları incelenmiş ve ağları daha güvenli hale getirecek önlemler anlatılmıştır. Son bölümde güvenli olan ve kimlik yönetimine imkan veren captive portal yöntemi uygulamalı olarak anlatılmıştır. Uygulamada, logların 5651 sayılı kanuna göre formatlı hale getirilmesi ve değişmemesinin garanti edilmesi için zaman damgası ile damgalanması yapılmıştır.

Anahtar Kelimeler: Ağ güvenliği, 802.1x, Kimlik doğrulama, Captive portal, Kablosuz ağlar

ABSTRACT

SECURE NETWORK ACCESSS AND AUTHENTICATION

Özkan, İlker

Information Technologies of Science Program

Supervisor: Asst.Prof.Dr.Yalçın Çekiç

September 2011, 52 Pages

Nowadays, many methods are available to ensure the security of computer networks and these methods are being developed every day. Some of these methods in use has a security vulnerability, due to difficulties in some of them can not be applied.

In this study, commonly used in wired and wireless networks and network standarts are described, the network access and identity management methods were examined and discussed measures to make networks more secure. The last section, allowing for secure and identity management captive portal method is described as practical. In practise, the log files according to the law of 5651, making the format and were stamped with the time stamp to prove not change.

Keywords : Network security, 802.1x, Authentication, Captive portal, Wireless networks

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

KISALTMALAR

Gelişmiş şifreleme standardı(Advanced Encryption Standard)	:	AES
Erişim noktası (Access Point)	:	AP
Genişletilebilir doğrulama protokolü (Extensible Authentication Protocol)	:	EAP
Mesaj özü (Message Digest Five)	:	EAP-MD5
EAP kaplamalı yerel ağ (EAP over lan)	:	EAPOL
Taşıma katmanı güvenliği (Transport Layer Security)	:	EAP-TLS
Dinamik istemci konfigürasyon protokolü (Dynamik Host Control Protocol)	:	DHCP
Grup geçis anahtarı (Group Transient Key)	:	GTK
Üstmetin aktarım protokolü (Hypertext Transfer Protocol)	:	HTTP
Bagımsız temel hizmet seti (Independed Basic Service Set)	:	IBSS
Elektrik elektronik mühendisleri enstitüsü (Institute of Electrical and Electronics Engineers)	:	IEEE
İnternet Tahsisli Sayılar Otoritesi (Internet Assigned Numbers Authority)	:	IANA
İnternet Protokolü (Internet Protocol)	:	IP
Uluslararası standartlar organizasyonu (International Standarts Organization)	:	ISO
ISP (Internet Service Provider) : Internet servis sağlayıcı		
Anahtar doğrulama anahtarı (Key Confirmation Key)	:	KCK
Anahtar şifreleme anahtarı (Key Encryption Key)	:	KEK
Yerel alan ağları (Local Area Networks)	:	LAN
Sadeleştirilmis genişletilebilir yetkilendirme protokolü (Lightweight Extensible Authentication Protocol)	:	LEAP
Sadeleştirilmiş dizin erişim protokolü (Lightweight Directory Access Protocol)	:	LDAP
Ana anahtar (Master Key)	:	MK
Network politika sunucusu (Network Policy Server)	:	NPS
Açık sistem bağlantı modeli (Open Systems Interconnection)	:	OSI
Kişisel dijital yardımcı (Personal Digital Assistant)	:	PDA
Korunmuş EAP (Protected EAP)	:	PEAP
Çiftli ana anahtar (Pairwise Master Key)	:	PMK
Çiftli geçis anahtarı (Pairwise Transient Key)	:	PTK
Uzaktan aramalı kullanıcı kimlik dogrulama servisi (Remote Authentication Dial-In User Service)	:	RADIUS
Çok güvenli ağ (Robust Security Network)	:	RSN
Servis seti tanımlayıcı (Service Set Identifier)	:	SSID
İletim kontrol protokolü (Transmission Control Protocol)	:	TCP
İletim kontrol protokolü/internet protokolü (Transmission Control Protocol/Internet Protocol)	:	TCP/IP
Geçici anahtar (Temporal Key)	:	TK
Geçici anahtar bütünlügü protokolü (Temporal Key Integrity Protocol)	:	TKIP

Ömür süresi (Time to Live)	:	TTL
Geniş alan ağı (Wide Area Network)	:	WAN
Kabloluya eşdeger gizlilik (Wired Equivalent Privacy)	:	WEP
Kablosuz sadakat birliği (Wireless Fidelity Alliance)	:	Wi-fi
Kablosuz yerel alan ağları (Wireless Local Area Network)	:	WLAN
Wi-Fi korumalı erişim (Wi-fi Protected Access)	:	WPA
Wi-Fi korumalı erişim ikinci sürüm (Wi-fi Protected Access 2)	:	WPA2

1. GİRİŞ

En az iki bilgisayarın birbirlerine bağlanıp, bilgi alış-verişinde bulunmasına bilgisayar ağı denir. Bilgisayar ağları, kullanıcılara bilgisayarlar arası bilgi paylaşımı yapabilecekleri bir ortam sağlar. Bilgisayar ağına bağlı kullanıcıların, ağın kaynaklarına ulaşması ve diğer kullanıcılarla iletişimde bulunması ağ kullanımının temel amacıdır. Bu da zaman ve para tasarrufu sağlar.

Günümüzde kullanılan sistemler büyük oranda internete bağlanabilmektedir. Finans kuruluşları, kamu kuruluşları, küçük ve büyük ölçekli işletmeler, üniversiteler hem bilgi paylaşımı, hem de iletişim için internete bağlıdır. Bu ağların internete bağlı olmasından dolayı birtakım riskler oluşmaktadır. Bu riskleri önlemek üzere ağ güvenliği teknolojileri kullanılır. Finansal hırsızlığa, bilgi hırsızlığına ve dolayısıyla gizli iş bilgilerinin kötüye kullanılmasına, internet'ten gelen virüs ve solucanların kötü amaçlı saldırılarına karşı koruma sağlar. Uygun ağ güvenliği unsurları tesis edilmediği zaman ağa yetkisiz sızma, ağın kapanması, hizmet kesintisi, yönetmeliklerle uyumsuzluk ve hatta yasal işlem riskleriyle karşı karşıya kalmak söz konusu olabilir.

Ağ güvenliğini sağlamak tek bir yönteme dayanmamaktadır. Genellikle, ağı farklı yöntemlerle savunmak için bir dizi engel kullanılır. Bir yöntemin başarısız ya da etkisiz olduğu durumlarda , diğer yöntem ya da yöntemler ağı ve verileri çeşitli ağ saldırılarına karşı korur. Ağ güvenliğini katmanlar haline getirmek, kurum ya da kişilerin işi yürütmek için kullandığı değerli bilgilerin yalnızca yetkili kişilerce kullanımına açık olması açık olması ve tehditlere karşı korunması anlamına gelir. Özellikle ağ güvenliği:

- İç ve dış ağ tehditlerine karşı koruma sağlamak: Tehditler, ağın bulunduğu yerde lokal sistemler içinden veya dışından gelebilir. Etkili bir güvenlik sisteminden beklenen, tüm ağ etkinliğini izleyerek dahili ve harici tehditleri, olağandışı davranışı belirlemesi ve uygun önlemlerin alınmasıdır.
- İletişimin gizliliğini sağlamak: Bilgiye erişmesi gereken yetkili kullanıcılar bilgi ağlarına yerel ağ üzerinden ya da kurum dışından sabit veya mobil sistemler ile iletişimlerinin gizli ve koruma altında olduğu güvencesiyle erişebilir.

- Yetkilendirme ve denetim : İşletmeler bilgi ağlarına kullanıcıların erişimi ve denetimi ile ilgili olarak kendi kurallarını oluşturabilir. Erişimin reddedilmesi veya onaylanması kullanıcıların veya sistemlerin kimliklerine, yapılacak işin işlevine veya diğer işle ilgili özel ölçütlere dayanabilir.

- Kurumu itibarının korunması, güvenilirliğin arttırılması: Kurumların bilgi ağlarının bilinen saldırılar ve yetkisiz erişimler karşı korunduğu ve yeni tehditlere göre güvenlik tedbirlerinin alındığı bir ortamda çalışanlar, müşteriler ve iş ortakları, bilgilerinin güvenli olduğundan emin olurlar.

Bu tez çalışmasında, yukarıda belirtilen "kullanıcı ve sistemleri doğru bir şekilde tanımlayarak bilgilere erişimini denetlemek" hedefi ele alınarak kablolu ve kablosuz ağ erişimlerinde kullanılabilecek tarayıcı temelli kimlik doğrulama sistemi uygulaması yapılmıştır.

Tez çalışması dört bölümden oluşmaktadır. İkinci bölümde günümüzde kablosuz ağlarda yaygın olarak kullanılan, kablolu ağlarda da kullanılmaya başlanan IEEE 802.1X port tabanlı ağ erişim kontrol standardı incelenmiştir. Üçüncü bölümde alternatif olarak açık alan ağlarda özellikle kablosuz erişimde kullanımı görülen captive portal uygulaması ele alınmıştır. Dördüncü bölümde açık kaynak kodlu örnek bir captive portal uygulaması yapılmış ve uygulama sonuçları değerlendirilmiştir.

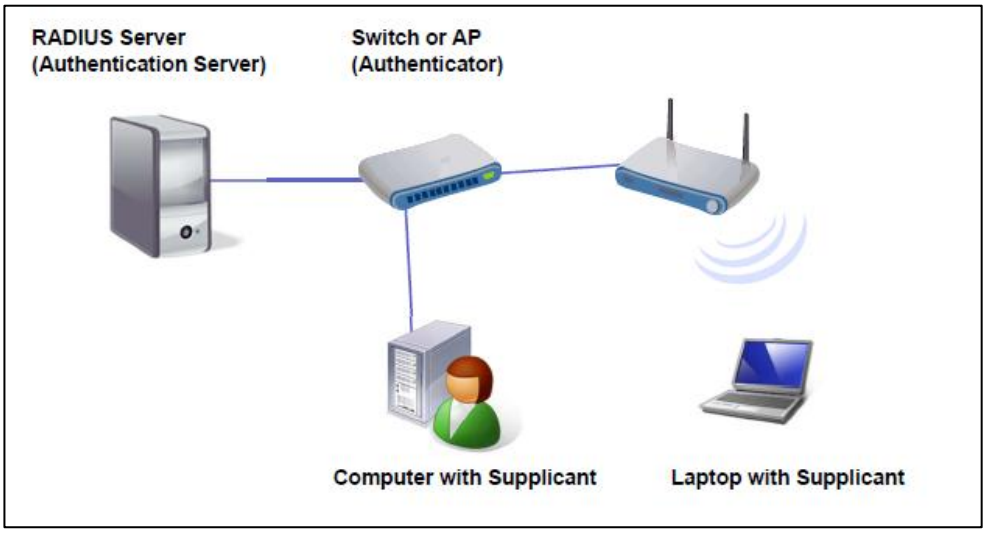
2. GENEL BİLGİLER

Kablolu ve kablosuz ağların güvenli hale getirilmesi için birtakım güvenlik standartları oluşturulmuştur. Bu bölümde, yaygın olarak kullanılan IEEE 802.1x standardının prensipleri ve nasıl çalıştığı açıklanmaktadır.

2.1 802.1X STANDARDI

802.1X standardı ağa bağlanan cihazların kimlik doğrulama ve yetkilendirilmesine olanak sağlayan port tabanlı ağ erişim denetimidir. Ağa yapılan bağlantı isteklerinde port tabanlı kullanıcı ya da sistemleri doğrulayabilmek, herhangi bir kullanıcıya, gruba ya da sisteme ağ erişim politikaları uygulamaya imkan tanır. Kimlik doğrulama ve yetkilendirme başarılı olmazsa bağlanmak istenen port erişime kapatılır ve bu sayede yerel ağ altyapısı korunmuş olur. Kullanıcı ya da sistem doğrulama; ağa bağlanmak isteyen sistemin fiziksel ağ adresi (MAC Adresi), bağlantıyı sağlayacak olan anahtar (switch) ya da erişim noktasının (AP) portu ya da harici bir yetkilendirme politikası ile sağlanır. Ağa kimin hangi hakla gireceğinin belirlenmesi, denetlenmesi ve yetkilendirmesi; kullanıcı odaklı, ağ tabanlı erişim kontrolü olan NAC tarafından belirlenir. (Kaynak: IEEE, 2004)

802.1X için ağ topolojisi örneği aşağıda şekil 2.1 ‘de gösterilmiştir.



Şekil 2.1: 802.1x Kablolu ve Kablosuz ağ bağlantı topolojisi

2.2 802.1X ÇALIŞMA PRENSİBİ

802.1x ‘in çalışmasında sertifika kullanımı gerekiyorsa PEAP eğer gerekmiyorsa EAP erişim protokolleri kullanılmaktadır. Her iki protokolünde temel çalışma prensibi hemen hemen aynıdır. İletişimin kurulması esnasında özetle aşağıdaki adımlar gerçekleşir:

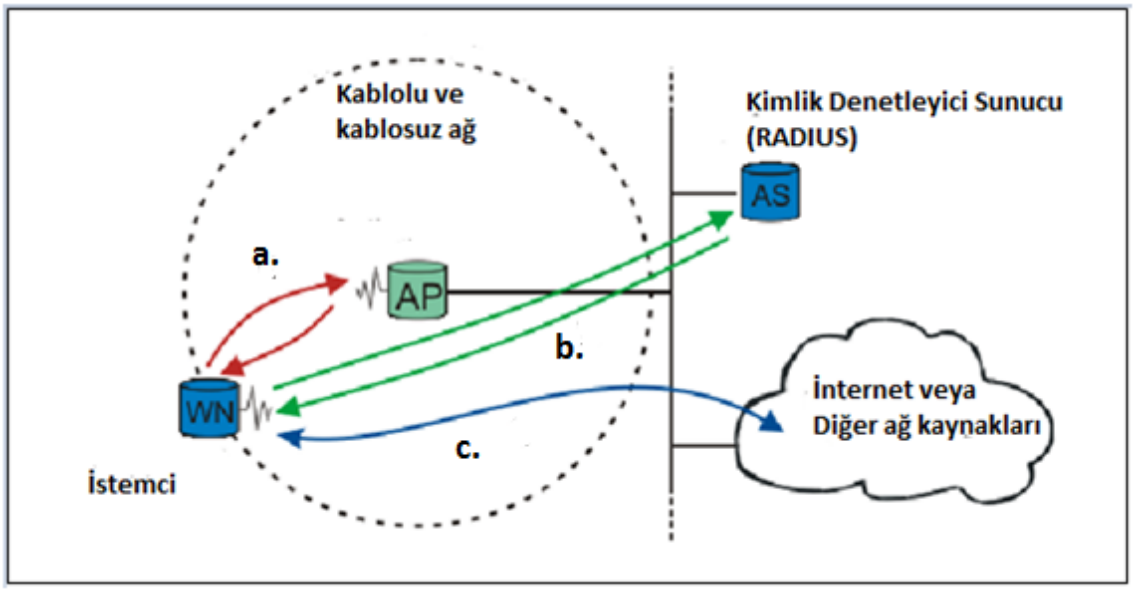
i. İstemci cihaz ya da kimlik doğrulaması yapmak isteyen kullanıcı ile kimlik denetiminin yapıldığı sunucu (Authentication Server) arasında bulunan denetleyici cihaz (authenticator), bağlantı durumunda bulunan istemciye EAP-Request/Identity paketi göndererek kendisini tanıtmasını ister.

ii. İstemci cihaz ya da kullanıcı, kimliğini tanıtan EAP-Response/Identity paketi ile cevap verir, bu cevap paketlenerek (encapsulation) sunucuya gönderilir.

iii. Erişim denetleyen sunucu, denetleyici cihaza şifreli token sistemi gibi bir davetiye atar. Denetleyici cihaz bu paketi açıp EAPOL (LAN üzerinden EAP) içerisinde istemciye gönderir. İstemci cihaz bu davetiyeye denetleyici üzerinden cevap gönderir.

iv. Eğer istemci cihaz veya kullanıcı gerekli kullanıcı ya da sistem tanımına ve haklarına sahipse, sunucunun gönderdiği doğrulayıcı mesaj sonunda denetleyici cihaz, istemci cihaza erişim izni vererek süreci tamamlar.

Aşağıdaki şekil 2.2 ‘de 802.1x doğrulama aşamaları gösterilmiştir.



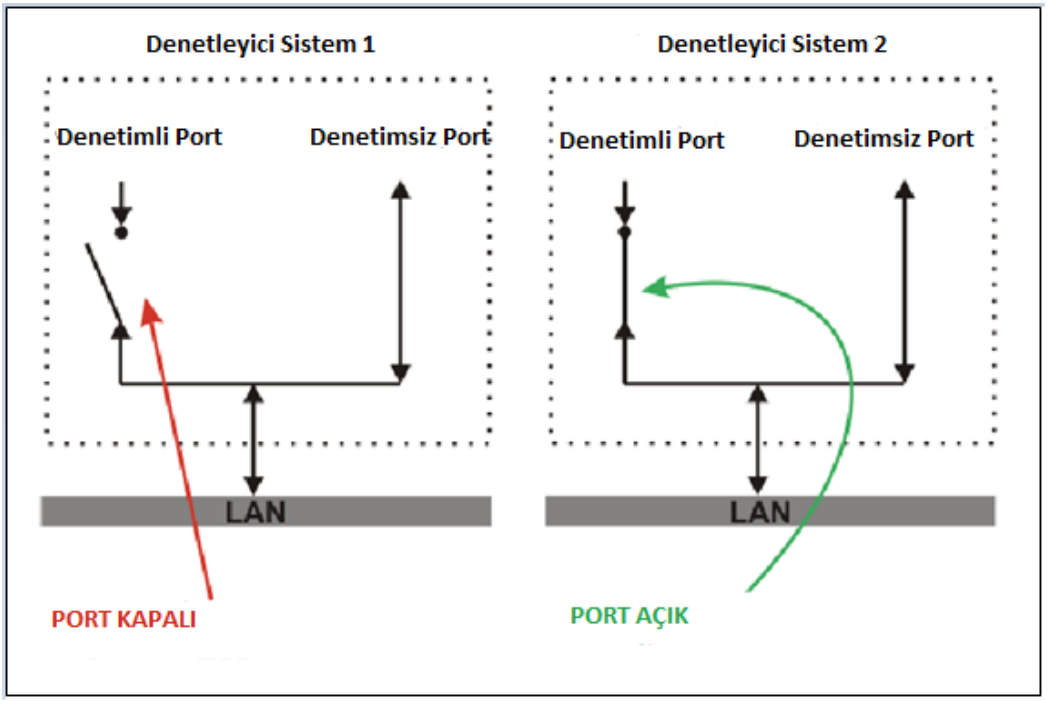
Şekil 2.2 : 802.1x kimlik doğrulama aşamaları

a. Yeni bir istemci (supplicant) cihaz ya da kullanıcı bir yerel ağ kaynağına erişmek isterse, denetleyici cihaz (authenticator) , istemci cihazın ya da kullanıcının kimliğini ister. Cihazın ya da kullanıcının kimliği doğrulanmadan EAP'den başka hiçbir akışa izin verilmez, bu durumda port kapalıdır. İstemcide kimlik olarak kullanıcı adı ile birlikte PAP veya CHAP tarafından doğrulaması yapılacak kullanıcı parolası kullanılır. Kimlik şifrelenmeden açık bir şekilde gönderildiği için kötü niyetli bir dinleyici kullanıcının kimliğini öğrenebilir. O zaman "Kimlik saklama" (EN - Identity hiding) kullanılır; şifrelenmiş TLS tüneli kurulmadan gerçek kimlik gönderilmez.

b. İstemci tarafından kimlik gönderildikten sonra kimlik kanıtlama sureci başlar. İstemci ve denetleyici cihaz arasında kullanılan protokol EAP olup, EAP kaplamalı yerel ağdır (EAPOL). Denetleyici cihaz EAP iletilerini RADIUS biçimine yeniden dönüştürür ve kimlik denetleyici sunucuya aktarır. Kimlik kanıtlama süresince, denetleyici cihaz, sadece istemci cihaz ile kimlik kanıtlama Sunucusu arasında paketleri nakleder. Kimlik kanıtlama süreci tamamlandığında kimlik kanıtlama sunucusu başarı (veya doğrulama başarısız olursa, başarısızlık) iletisi gönderir ve denetleyici cihaz, istemci cihazın bağlı bulunduğu portu istemci erişimi için açar.

c. Başarılı bir kimlik kanıtlamadan sonra istemci cihaz yetkisi bulunan diğer yerel ağ kaynaklarına ya da internete erişmeye hak kazanır.

Bu güvenli bağlantı yöntemine port tabanlı kimlik kanıtlama denilmektedir. Çünkü, Kimlik Kanıtlayıcı cihaz hem denetimli hem de denetimsiz portlarla uğraşır. Denetimli port ve denetimsiz port mantıksal varlıklardır (sanal portlar); ama yerel ağa aynı fiziksel bağlantıyı kullanırlar. Bu yapı aşağıda Şekil 2.3 'te gösterilmiştir.



Şekil 2.3: 802.1X denetimli/denetimsiz port

Kimlik kanıtlama yapılmadan önce sadece denetimsiz port "açıktır". Bu port üzerinden sadece EAPOL trafiğinin geçişine izin verilir (şekil 2.2.' de Denetleyici Sistem 1). İstemci kimliği kanıtlandıktan sonra, denetimli port açılır ve diğer yerel ağ kaynaklarına erişim hakkı verilir (şekil 2.3.2'de Denetleyici Sistem 2).

802.1X, yeni IEEE telsiz standardı 802.11i'de önemli bir rol oynamaktadır.

2.3 802.11i NEDİR?

2.3.1 WEP

WEP, adında belirtildiği gibi kabloluya eşdeğer gizlilik (Wired Equivalent Privacy) 802.11 standardının parçası olarak güvenilirliği sağlamak üzere tasarlanmıştır. Maalesef WEP güçsüz tasarlanmıştır ve kolayca kırılabilmektedir. Kimlik kanıtlama mekanizması olmayıp, erişim denetimi için sadece zayıf bir yöntem olan paylaşımlı anahtar altyapısı vardır.

WEP'in kolay kırılabilmesi sonrasında, IEEE 802.11i olarak isimlendirilen yeni bir telsiz güvenlik standardı ile gelmiştir. 802.1X bu yeni standartta önemli bir rol oynamaktadır.

2.3.2 802.11i

IEEE tarafından Haziran 2004'te onaylanmış olan bu güvenlik standardı 802.11i, tüm WEP zayıflıklarını onarmıştır. Bir sonraki bölümde anlatılan genişletilmiş bir anahtar türetme/yönetim işlevine sahiptir. 802.11i üç ana kategoriye ayrılmıştır:

i. Geçici Anahtar Tümleşikliği Protokolü (Temporary Key Integrity Protocol TKIP): Bu protokol tüm WEP zayıflıklarını onaran kısa vadeli bir çözümdür. TKIP eski 802.11 destekleyen denetim cihazlarıyla, sürücü aygıt yazılımı güncellemesinden sonra kullanılabilir ve tümleşiklik ile güvenilirlik sağlar hale getirildi.

ii. CBC–MAC ile Sayaç Modu Protokolü (Counter Mode with CBC–MAC Protocol CCMP): Bu protokol tamamen yeni bir protokoldur. Şifreleme algoritması olarak AES kullanılır ve daha yoğun işlemci kullandığından WEP ve TKIP'te kullanılandan yeni 802.11 denetleyici cihaz donanımına ihtiyaç duyulabilir. Bazı sürücüler yazılımda CCMP'yi uygulayabilirler. CCMP tümleşiklik ve güvenilirlik sağlar.

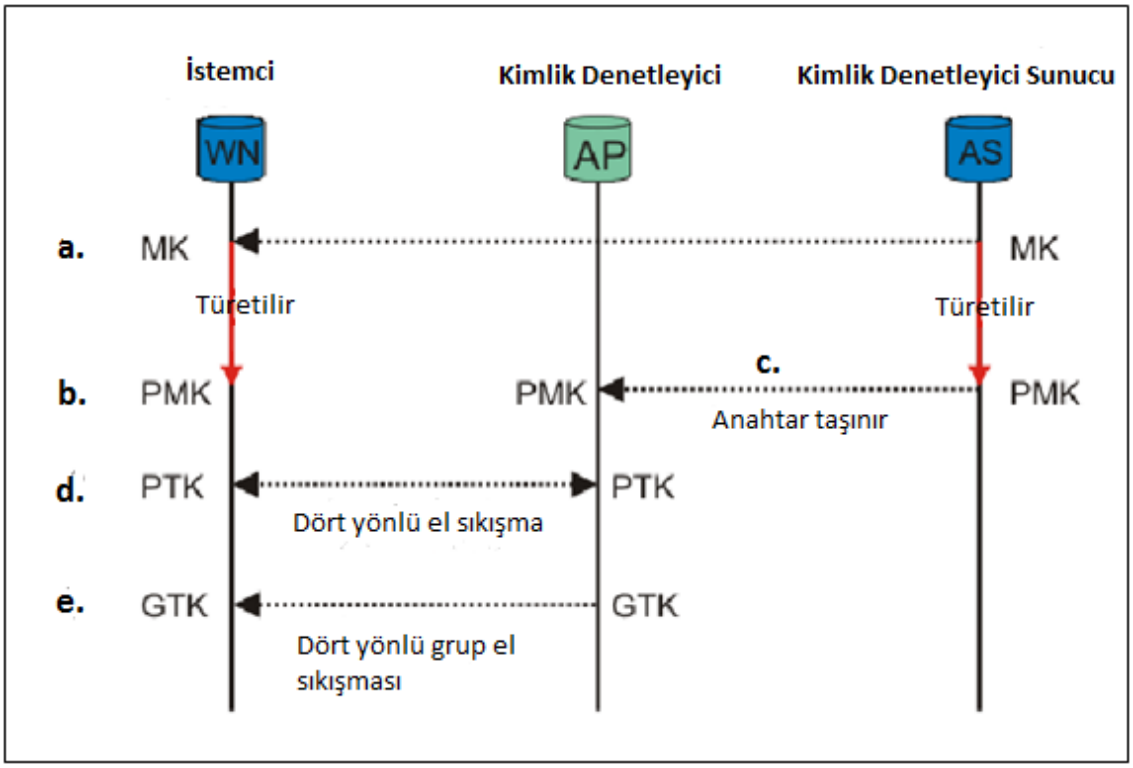
iii. 802.1X Port Tabanlı Ağ Erişim Denetimi: TKIP veya CCMP kullanılırken kimlik kanıtlama için 802.1X kullanılır. Burada ek olarak, seçimlik bir şifreleme yöntemi olan "Wireless Robust Authentication Protocol" (WRAP) CCMP'nin yerine kullanılabilir. WRAP için destek seçime bağlıdır, ama 802.11i'de CCMP desteği zorunludur.

2.3.3 Anahtar Yönetimi

2.3.3.1 Dinamik anahtar değişimi ve yönetimi

Güvenlik kuralları bütünü oluşturmak için şifreleme ve tümleşiklik algoritmaları kullanarak oluşturulan anahtarlar kullanılmalıdır. Bu anlamda 802.11i kapsamlı bir anahtar türetme/yönetim gücünü içermektedir. Aşağıdaki şekil 2.4'te Dinamik anahtar

değişimi ve yönetimi gösterilmektedir.



Şekil 2.4 : Dinamik anahtar değişimi ve yönetimi

a. İstemci cihaz ve Kimlik Kanıtlama Sunucusu (Authenticator Server) aralarında kimlik doğrulama işlemini yaparken, Kimlik Kanıtlama Sunucusu'ndan gönderilen doğrulamanın başarılı olduğunu belirten son iletilerden biri bir Ana Anahtar'dır (MK- Master Key). Gönderildikten sonra Ana Anahtar sadece istemci ve Kimlik Kanıtlama Sunucusu tarafından bilinir. Ana Anahtar, istemci ve Kimlik Doğrulama Sunucusu arasındaki bu oturuma bağlı olarak oluşturulur.

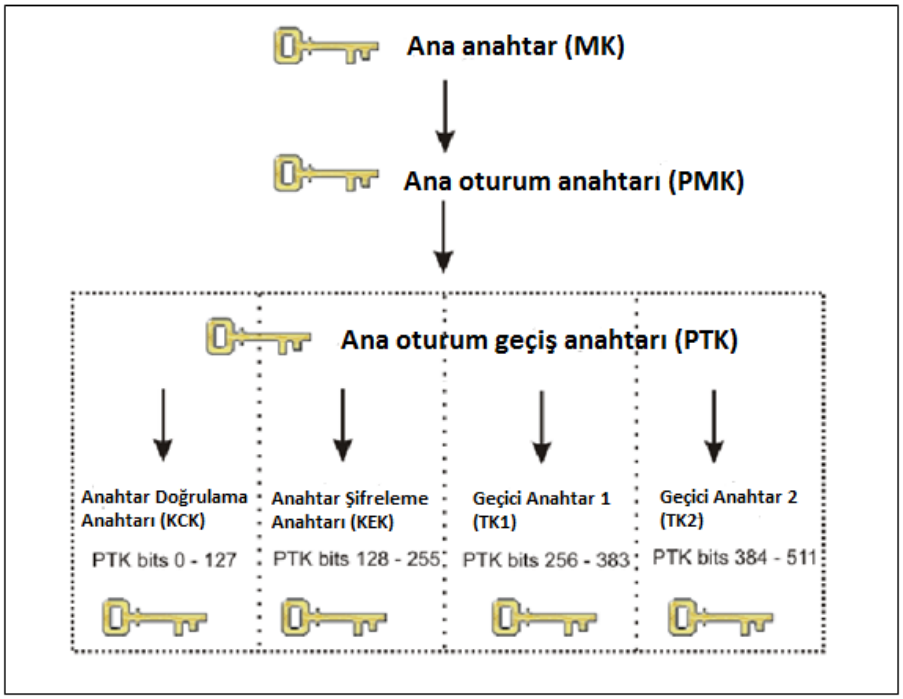
b. Hem istemci cihaz hem Kimlik Doğrulama Sunucusu, Ana Anahtar'dan bir Ana Oturum Anahtarı (PMK – Pairwise Master Key) üretir.

c. Bu noktada Ana Oturum Anahtarı, Kimlik Kanıtlama Sunucusu'ndan (AS) Kimlik denetleyici cihaza taşınır. Ana Oturum Anahtarını sadece istemci ve Kimlik Doğrulama Sunucusu türetebilir, bunun yanında Kimlik denetleyici, Kimlik Doğrulama Sunucusu yerine erişim–denetim kararları verebilir. Ana Oturum Anahtarı, istemci ve Kimlik Kanıtlayıcı arasındaki bu oturuma bağlı yepyeni bir simetrik anahtardır.

d. Ana Oturum Anahtarını türetmek, bağlamak ve doğrulamak için istemci ve Kimlik Kanıtlayıcı arasında Ana Oturum Anahtarı ve dört yönlü el sıkışma kullanılır. PTK ise işletimsel anahtarlar topluluğudur:
   - **Anahtar Doğrulama Anahtarı** (KCK – Key Confirmation Key), Ana Oturum Anahtarına (PMK) sahipliği kanıtlamak ve Ana Oturum Anahtarını (PMK) Kimlik denetleyiciye bağlamak için kullanılmaktadır.
   - **Anahtar Şifreleme Anahtarı** (KEK – Key Encryption Key), Grup Geçiş Anahtarı (GTK – Group Transient Key) dağıtımı için kullanılır. Aşağıda tanımlanmıştır.
   - **Geçici Anahtar 1 ve 2** (TK1/TK2 – Temporal Key 1 & 2) , şifreleme için kullanılır. TK1 ve TK2'nin şifreleme türüne özel olarak kullanılmaktadır.

e. Anahtar Şifreleme Anahtarı (KEK) ve dört yönlü grup el sıkışması Kimlik Doğrulama Sunucusu'ndan (AS) istemciye Grup Geçiş Anahtarını (GTK) göndermek için kullanılır. GTK aynı Kimlik denetleyiciye bağlı tüm istemciler arasında paylaşılan bir anahtardır ve çoğa gönderimli iletişim akışını güvenli hale getirmek için kullanılmaktadır.

Aşağıdaki şekil 2.5 'te ana oturum anahtarı düzeni gösterilmektedir.



Şekil 2.5 : Ana oturum anahtarı (PMK) düzeni

2.3.3.2 Ön paylaşımlı anahtar

Birkaç sistemden oluşan küçük ağlarda amaca yönelik küçük ağlarda ve ev kullanımı için Ön paylaşımlı Anahtar (PSK – Pre–Shared Key) kullanılabilmektedir. Ön paylaşımlı anahtar kullanırken kimlik kanıtlama sürecinde EAP ve kimlik kanıtlama sunucusu (RADIUS) kullanılmaz. EAP ve kimlik kanıtlama sunucusu (RADIUS) kullanan WPA'ya "Kurumsal WPA" veya sadece "WPA" dendiği gibi ön paylaşımlı anahtar kullanan yapıya da "Kişisel WPA" (WPA–PSK) denilmektedir. Verilen bir paroladan 256 bitlik ön paylaşımlı anahtar üretilir ve bu anahtar önceki bölümde anlatılan anahtar yönetim usulünde tanımlandığı gibi Ana Anahtar (MK) olarak kullanılır. Tüm ağ için tek bir ön paylaşımlı anahtar veya her istemci için ayrı bir ön paylaşımlı anahtar oluşturulabilir. İkisinin farkı ortak kullanılan tek bir ön paylaşımlı anahtarın daha az emniyetli oluşu, her istemci için ayrı oluşturulan ön paylaşımlı anahtarın daha güvenli oluşudur.

2.3.4 TSN (WPA) / RSN (WPA2)

WEP sorunlarının ortaya çıkması sonrasında sektörün 802.11i standardının tamamlanmasını bekleyecek kadar vakti yoktu. WEP sorunlarının hemen onarılmasını istediler. Wi–Fi Alliance baskıyı hissederek, standardın (3. taslağa dayanan) "bir anlık görüntüsünü" alarak ona Wi–Fi Korumalı Erişim (WPA–Wi–Fi Protected Access) dedi. Mevcut 802.11 ekipmanı WPA ile kullanılabilmesi dolayısıyla WPA temelde TKIP + 802.1X'tir. WPA uzun vadeli çözüm değildir. Çok Güvenli Ağ (RSN – Robust Secure Network) elde etmek için donanım AES (Advanced Encryption Standart – Gelişmiş Şifreleme Standardı), Counter Mode-CBC (Cipher Block Chaining-Zincirleme Blok Şifreleme) ve MAC (Message Authentication Code-Mesaj Doğrulama Kodu) desteklemeli ve kullanmalıdır.

2.4 EAP NEDİR?

Genişletilebilir Kimlik Kanıtlama Protokolü (EAP - Extensible Authentication Protocol) RFC 3748 ile tanımlanan bir kimlik kanıtlama iletim protokolüdür. Tek başına bir kimlik kanıtlama yöntemi olmayıp kimlik kanıtlama sürecinde, kimlik kanıtlama sunucusu ile istemci arasında geçen ve tarafların hangi kimlik kanıtlama yöntemini

kullanacaklarını belirler. EAP kimlik kanıtlama yöntemi olarak MD5, TLS, TTLS, PEAP, LEAP kullanır.

2.5 EAP KİMLİK KANITLAMA YÖNTEMLERİ

En çok kullanılan EAP kimlik kanıtlama mekanizmalarından bazıları aşağıda listelenmiştir. Kayıtlı EAP kimlik kanıtlama türlerinin tam bir listesi IANA sitesinde http://www.iana.org/assignments/eap-numbers/eap-numbers.xml bulunmaktadır.

2.5.1 EAP–MD5

MD5'li Kimlik Kanıtlaması kullanıcı adı/parolaya gereksinim duyar ve PPP CHAP protokolünün eşdeğeridir. Bu yöntem sözlük saldırısı direnci, karşılıklı kimlik kanıtlama veya anahtar türetimi içermez ve telsiz kimlik kanıtlama ortamında az kullanılır.

2.5.2 Hafif EAP (LEAP)

Kimlik kanıtlama için Kimlik Kanıtlama Sunucusuna (RADIUS) bir kullanıcı adı/parola çifti gönderilir. Leap, Cisco tarafından geliştirilmiş müseccel bir protokoldur ve güvenli olduğu düşünülmez.

2.5.3 EAP–TLS

EAP ile İstemci ve Kimlik Kanıtlama Sunucusu arasında bir TLS oturumu oluşturur. Hem sunucu hem istemci(ler) geçerli bir sertifikaya (x509) ve bununla birlikte bir PKI'ya ihtiyaç duyar. Bu yöntem her iki yönde kimlik kanıtlama sağlar.

2.5.4 EAP–TTLS:

Kimlik kanıtlama verisinin emniyetli iletimi için şifreli bir TLS tuneli kurar. TLS tünelinden diğer (herhangi) kimlik kanıtlama yöntemleri faydalanır. Funk Software ve Meetinghouse tarafından geliştirilmiştir.

2.5.5 Korumalı EAP (PEAP):

EAP–TTLS gibi şifreli bir TLS tüneli kullanır. Hem EAP–TTLS hem EAP–PEAP için istemci sertifikaları seçimliktir, ama sunucu sertifikaları gereklidir. Microsoft, Cisco ve RSA Security tarafından geliştirilmiştir.

2.5.6 EAP–MSCHAPv2:

Kullanıcı adı/parolaya ihtiyaç duyar ve temel olarak MS–CHAP–v2'nin EAP kaplamalı olanıdır. Genellikle PEAP , şifreli tünelde kullanılır. Microsoft tarafından geliştirilmiştir.

2.6 RADIUS NEDİR?

Uzaktan Aramalı Kullanıcı Kimlik Kanıtlama Servisi (RADIUS – Remote Authentication Dial–In User Service) RFC2865'te tanımlanmıştır ve ilk olarak, kullanıcılar, ISS'nin ağını kullanmak için yetkilendirilmeden önce kullanıcı adı ve parola doğrulaması yapacak olan ISS'ler tarafından kullanılmıştır.

802.1X ne çeşit bir arka–uç kimlik kanıtlama sunucusu olması gerektiğini belirtmez, ama RADIUS, 802.1X'te kullanılan fiili arka–uç kimlik kanıtlama sunucusudur.

Mevcut birçok AAA (Authentication, Authorization, Accounting) protokolü yoktur, ama RADIUS tam AAA desteği sağlar. AAA, Authentication (Kimlik Kanıtlama), Authorization (Yetkilendirme) ve Accounting (Hesap Yönetimi) kelimelerinin baş harflerinden oluşur

3. CAPTIVE PORTAL (TUTSAK KAPISI)

3.1 TANIM

Captive Portal, en kısa tanımıyla kullandığımız internet tarayıcıyı bir kimlik doğrulama sistemine çeviren bir kavramdır. Kütüphane, kampüs, internet kafe gibi ortak internet kullanım alanlarında kullanıcıların erişimlerinin kayıt altına alınması gerektiği her türlü internet çıkış noktasında kullanılabilmektedir.

3.2 KULLANIM AMAÇLARI

İnternet kullanıcılarının erişimde kullandıkları taşınabilir uç cihazlar teknolojik olarak epey gelişmiş ve çeşitlilik göstermiştir. Bu cihazlar üzerinden kablolu ya da kablosuz olarak ağa bağlanma ihtiyacı duyulduğunda, internet tarayıcılar üzerinden, ek istemci, yazılım, konfigürasyon gerektirmeden kimlik doğrulama yapılması amacıyla ortaya çıkmıştır.

3.3 KULLANIM ALANLARI

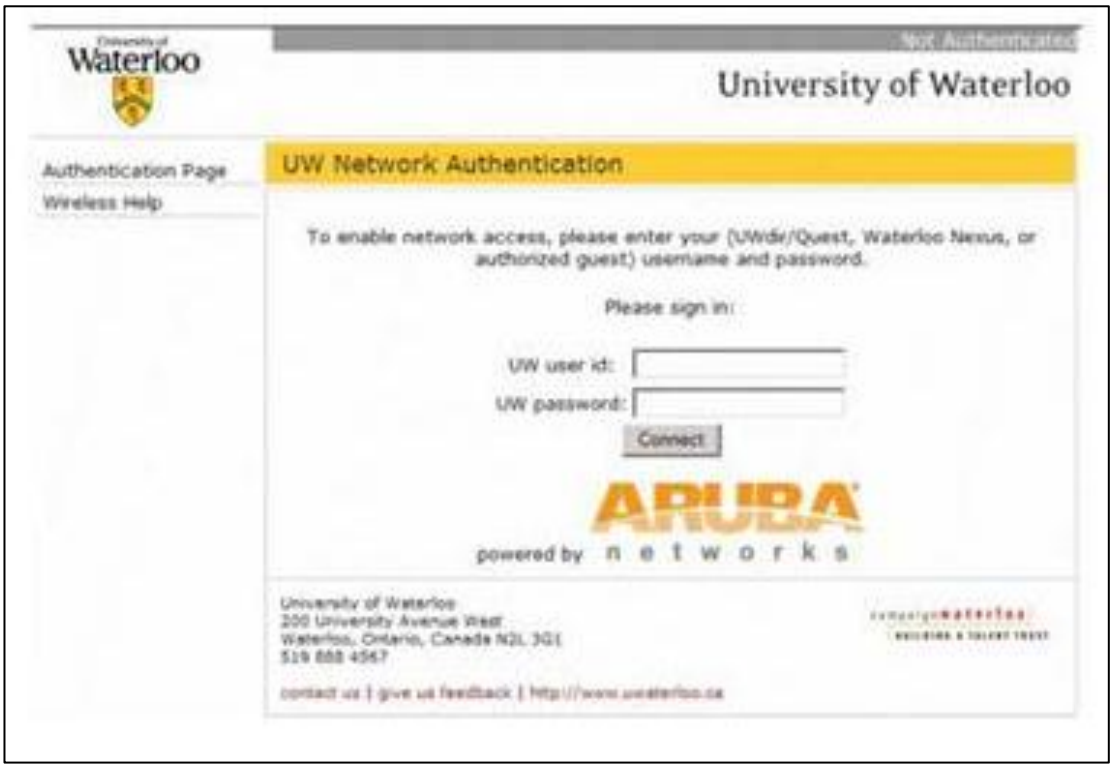
İlk başlarda kablosuz internete erişimde kimlik doğrulama aracı olarak çıkmış olmasına rağmen kablolu ağ erişimlerinde kullanımı yaygınlaşmaya başlamıştır.

- Ağda kullanılan aktif cihazların 802.1x desteğinin olmadığı ya da sorunlu olduğu noktalarda,
- Ağa bağlantıda kullanılan uç cihazların 802.1x kullanamadığı ya da istemci yazılım problemi yaşanan yerlerde,
- Sadece kullanıcı adı ve parolası olan kullanıcıların bağlantılarına izin vermek için,
- Bağlı olan kullanıcıların hesap (accounting) bilgilerini saklamak için,
- Çok kısa sürede ihtiyaç üzerine bir internet erişimi ihtiyacını güvenli bir şekilde sağlamak için,

Açık ve kapalı kaynak kodlu birçok güvenlik duvarı ve hotspot uygulamalarında dünyanın dört bir tarafında kullanılmaktadır.

Aşağıda şekil 3.1 ve 3.2 de, kampüslerinde captive portal kullanan iki üniversitenin erişim sayfaları görülebilmektedir.

Şekil 3.1 : Manchester Üniversitesi kablosuz ağ erişim portali
Kaynak: Manchester Üniversitesi ağ erişim prosedürü - http://www.south.manchester.ac.uk/itservices/



Şekil 3.2 : Waterloo üniversitesi kablosuz ağ erişim portali
Kaynak: http://wireless.anu.edu.au/anuaccess.php

3.4 ÇALIŞMA YÖNTEMLERİ

Piyasada bulunan Captive portal uygulamalarında çeşitli çalışma yöntemleri görülmüştür.

3.4.1 HTTP İle Yönlendirme

Eğer, kimliği doğrulanmamış bir istemci, web sitesi erişiminde bulunursa tarayıcı tarafından sitenin IP adresi DNS'e sorgulanır. Tarayıcı DNS'ten aldığı IP adresine HTTP isteği gönderir. Ancak bu istek güvenlik duvarı tarafından kesilerek yönlendirici sunucuya iletilir. Bu yönlendirme sunucusu captive portal yönlendirmesi için HTTP durum kodu 302 içeren normal bir HTTP yanıt ile yanıtlar. İstemci için bu süreç tamamen şeffaftır. İstemci web sitesi aslında ilk isteğe yanıt ve yönlendirme gönderildi varsayar.

3.4.2 IP Yönlendirme

İstemci trafiği OSI katmanı 3. seviyede IP yönlendirme kullanılarak yeniden yönlendirilebilir. Bunun dezavantajı, istemciye sağlanan içerik URL ile herzaman eşleşmeyebilir.

3.4.3. DNS Tarafından Yönlendirme

İstemci bir web sitesi erişim talebinde bulunduğunda tarayıcı tarafından DNS sorgulanır. Güvenlik duvarı, kimliği doğrulanmamış istemciler için sadece DHCP tarafından sağlanan DNS sunucusunun kullanılabilir olmasını sağlar. Bu DNS sunucu tüm DNS sorguları sonucunda Captive Portal sayfasının IP adresini döndürecektir.

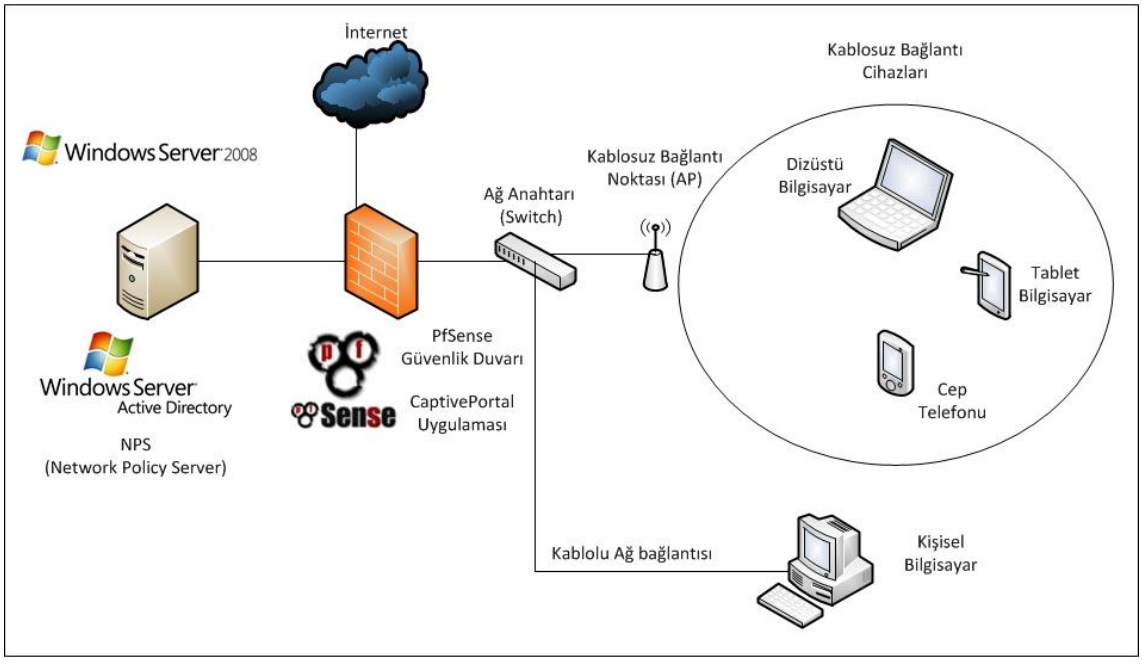
Burada DNS zehirleme tekniği (DNS Poisoning) kullanılmaktadır.

4. ÖRNEK CAPTIVE PORTAL UYGULAMASI

Bu bölümde, açık kaynak kodlu bir güvenlik duvarı kullanarak kablolu ve kablosuz internet erişimi için örnek bir Captive Portal (Esir Kapısı) uygulaması yapılmıştır.

4.1 KURULUM BİLEŞENLERİ

Bu uygulama çalışmasında açık kaynak kodlu PFSENSE güvenlik duvarı, Windows 2008 sunucu işletim sistemi üzerinde Active Directory servisi, RADIUS hizmeti sağlamak üzere NPS (Network Policy Server) servisleri kurularak aşağıdaki ağ topolojisi oluşturulmuştur.



Şekil 4.1 : Uygulama Ağ topolojisi

Uygulamada kullanılan bileşenlerin dökümü aşağıdaki gibidir:

i. RADIUS Sunucu: Bu sunucu Windows Server 2008 sunucu işletim sistemi üzerinde çalışan NPS (Network Policy Server) ile RADIUS hizmeti vermek üzere kurulmuştur. Ağ IP adresi 192.168.5.20 olarak tanımlanmıştır.

ii. Güvenlik Duvarı: Açık kaynak kodlu PfSense güvenlik duvarı kurulmuştur. İç ağ IP adresi 192.168.5.10 olarak tanımlanmıştır.

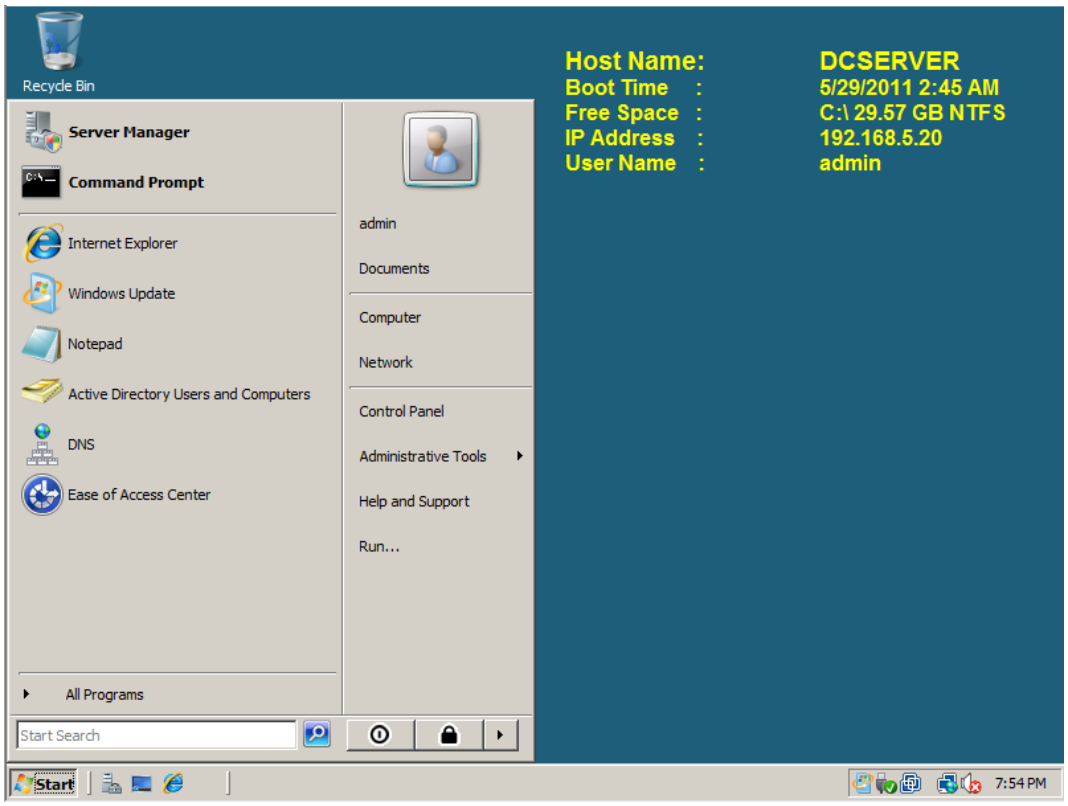
iii. Kablosuz Erişim noktası (AP) : D-Link marka, DWL-2000 model kablosuz erişim noktası kurulmuştur.

vi. Kablolu ve Kablosuz bağlantı cihazları : İnternete erişimde kullanılmak üzere Windows 7 işletim sistemi yüklü dizüstü bilgisayar, Iphone ve Blackberry cep telefonu ve Ipad tablet bilgisayar kullanılmıştır.

4.1.1 RADIUS Sunucu

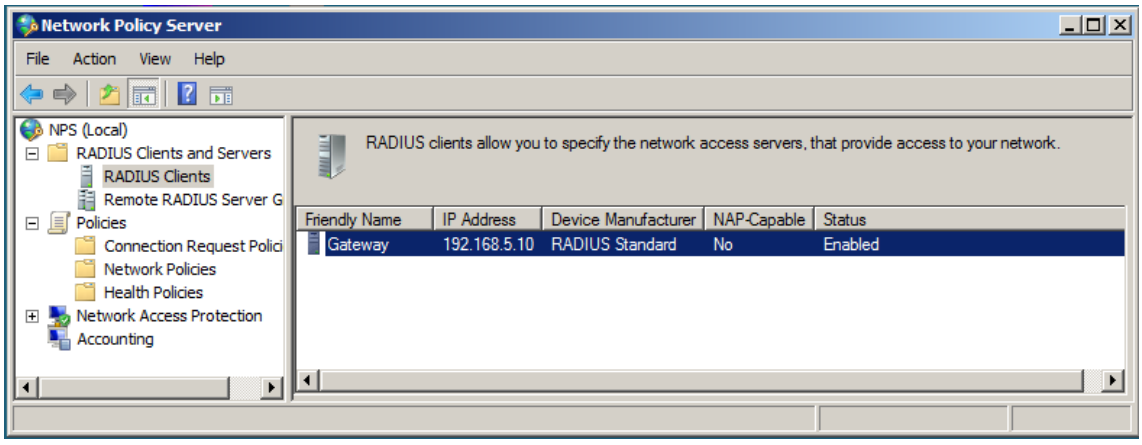
Bu örnek çalışmada kullanılan RADIUS sunucu, yaygın olarak kullanıldığı için ve yapılacak örnekte windows temelli bir dizin hizmeti ele alındığı için NPS (Network Policy Server) seçilmiştir. Linux temelli dizin hizmeti kullanılacağı durumda Free RADIUS gibi farklı kimlik denetleyici sunucular kullanabilmek mümkündür.

Standart bir kişisel bilgisayara Windows Server 2008 işletim sistemi kurulumu sonrasında dizin hizmeti sağlanması için Active Directory servisi kurulmuştur. Sonrasında NPS (Network Policy Server) kurularak RADIUS hizmeti verilmesi sağlanmıştır. Sunucunun ekran görüntüsü aşağıda şekil 4.2'de görüldüğü gibidir.



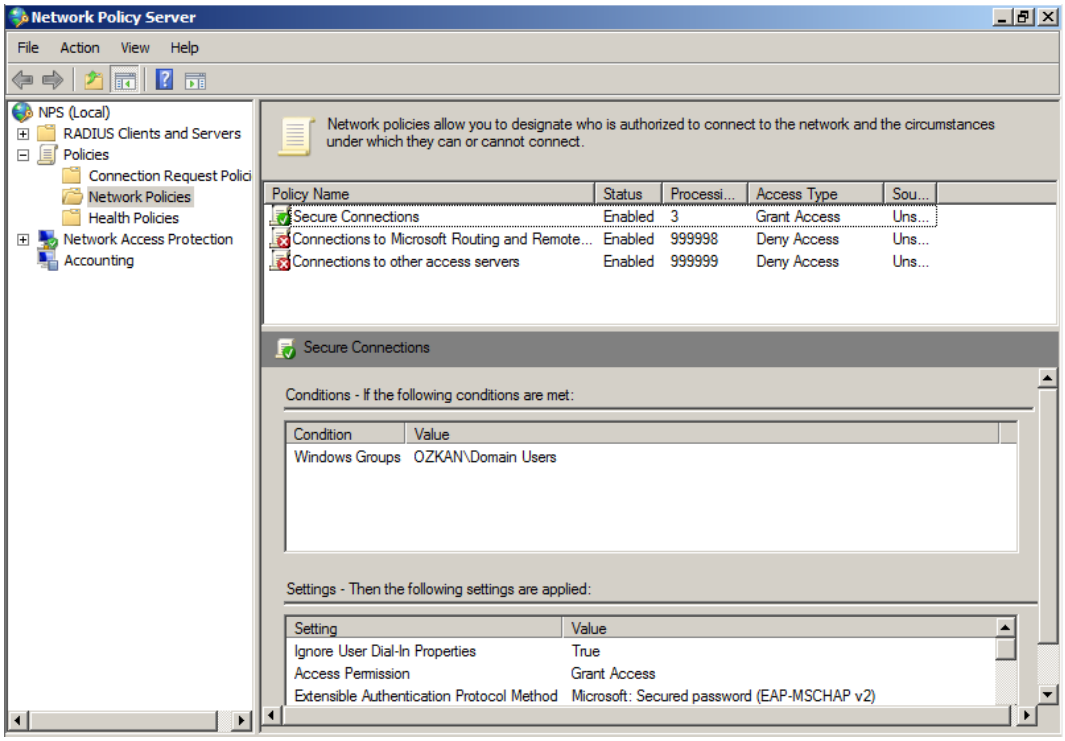
Şekil 4.2 : Windows Server 2008 ekran görüntüsü

Güvenlik duvarının bu NPS sunucuya erişerek RADIUS iletişimi kurabilmesi için NPS sunucuda RADIUS istemcileri bölümünden güvenlik duvarı ip adresi eklenmiştir. Ayrıca iletişimi başlatmak üzere kurulacak oturumda istemciyi doğrulamak için oturum şifresi (Shared Secret) tanımlanmıştır. RADIUS istemci ayarları ekranı şekil 4.3'te görüldüğü gibidir.



Şekil 4.3 : RADIUS İstemci ekran görüntüsü

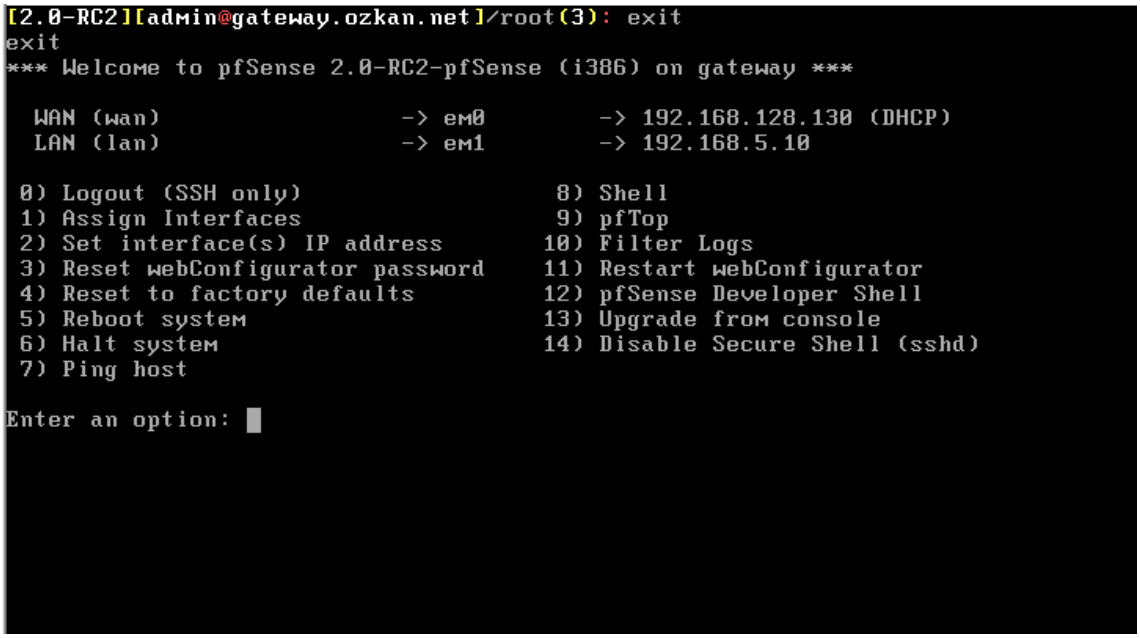
NPS (Network Policy Server) üzerinde ağ politikaları (Network Policies) bölümünden Secure Connections isimli bir politika oluşturularak etki alanında bulunan kullanıcılara (Domain Users) erişim hakkı verilmiştir. NPS politikaları ekranı Şekil 4.4'te görüldüğü gibidir.



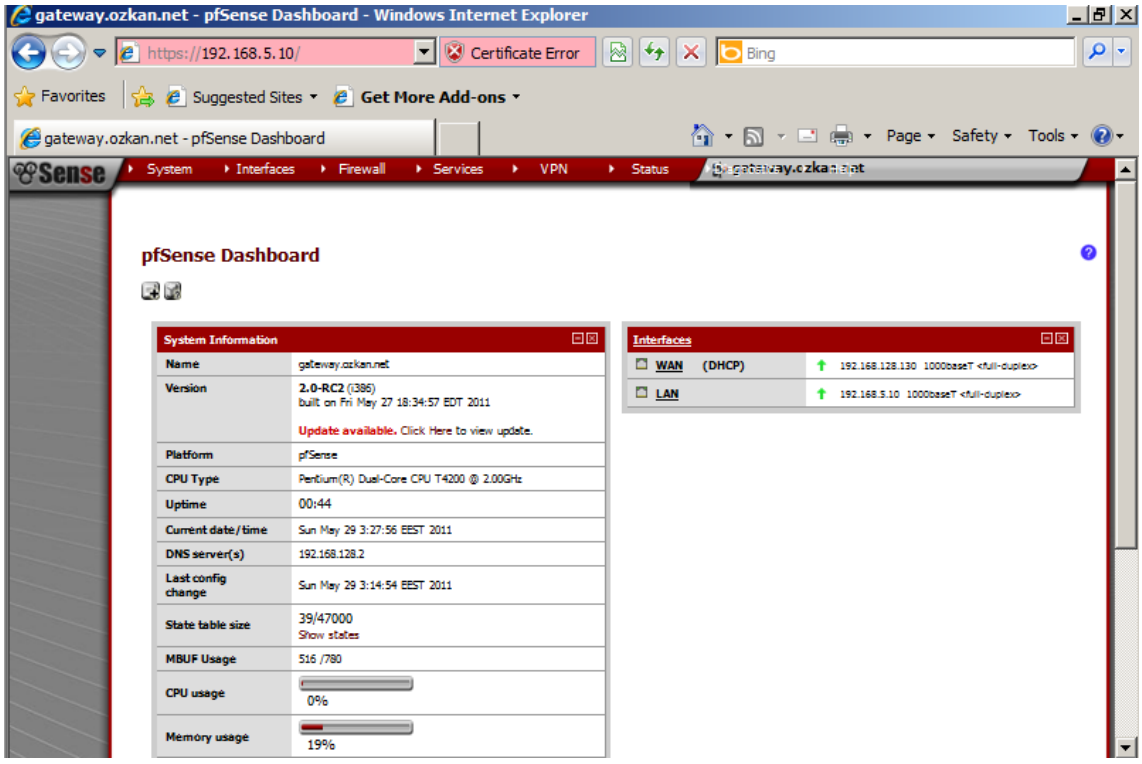
Şekil 4.4 : NPS politikaları ekran görüntüsü

4.1.2 Güvenlik Duvarı:

Standart bir kişisel bilgisayarda açık kaynak kodlu PfSense güvenlik duvarının kurulumu yapılmıştır. WAN ve LAN Ağ kartlarının IP adreslerinin ayarlaması şekil 4.5'te görülen konsol ekranından yapılmış, daha sonrasında aynı ağ segmentinde bulunan bir bilgisayarda şekil 4.6'da gösterilen web arayüzünden erişim sağlanmıştır.

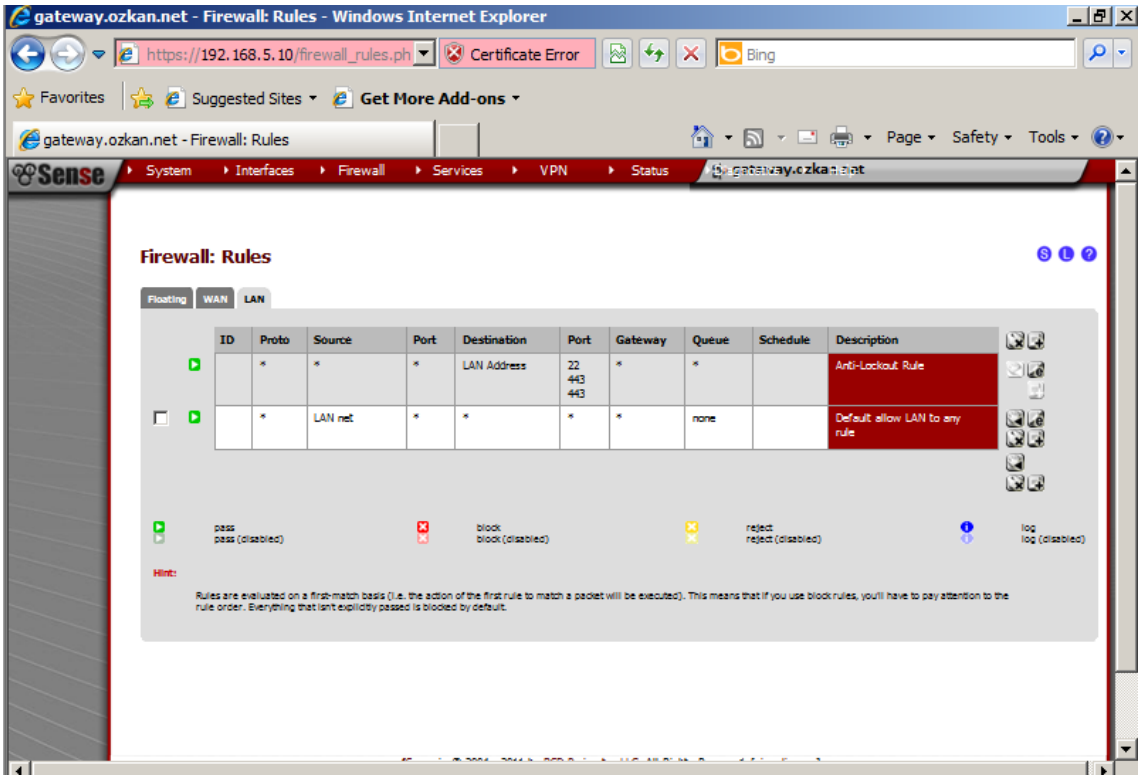


Şekil 4.5 : Güvenlik Duvarı konsol ekranı



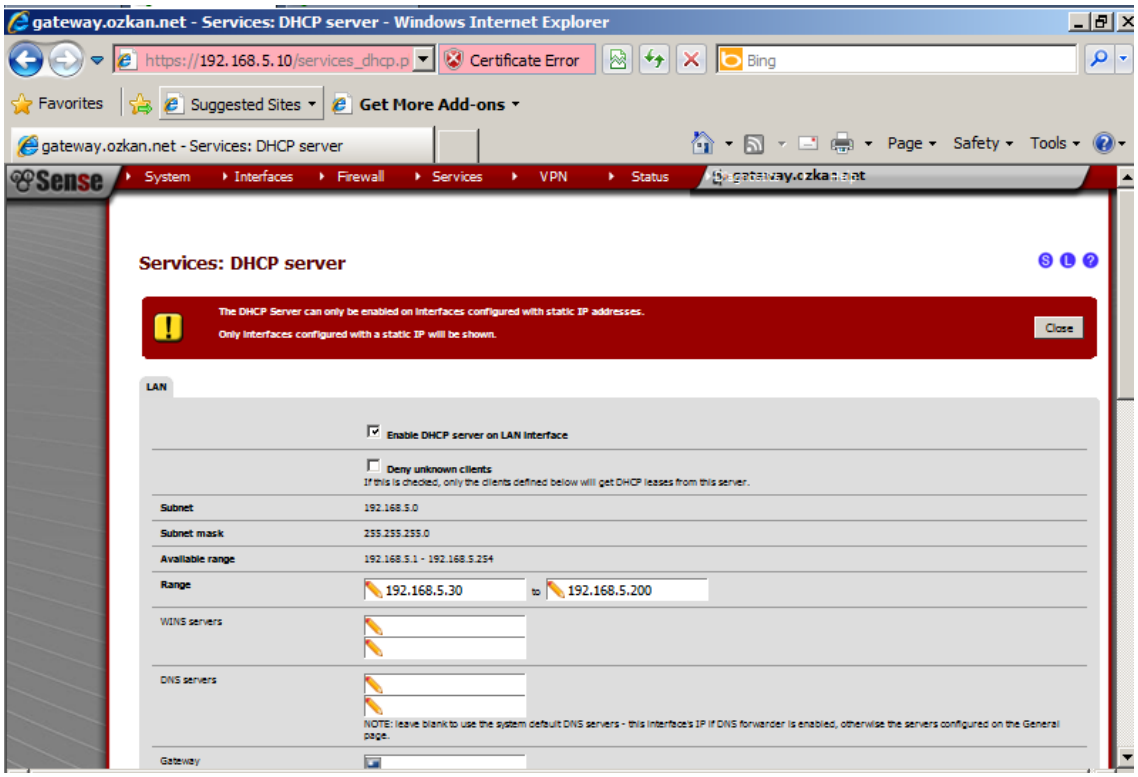
Şekil 4.6 : Güvenlik Duvarı web arayüzü

Web arayüzü aracılığıyla LAN'dan gelen kullanıcıların internete erişim kuralları tanımlanmıştır. Burada tanımlama yapılırken kullanıcıların, tüm portlardan internette istediklere yerlere ulaşması sağlanmıştır. Aşağıdaki Şekil 4.7'de Güvenlik Duvarı erişim kuralları gösterilmiştir.



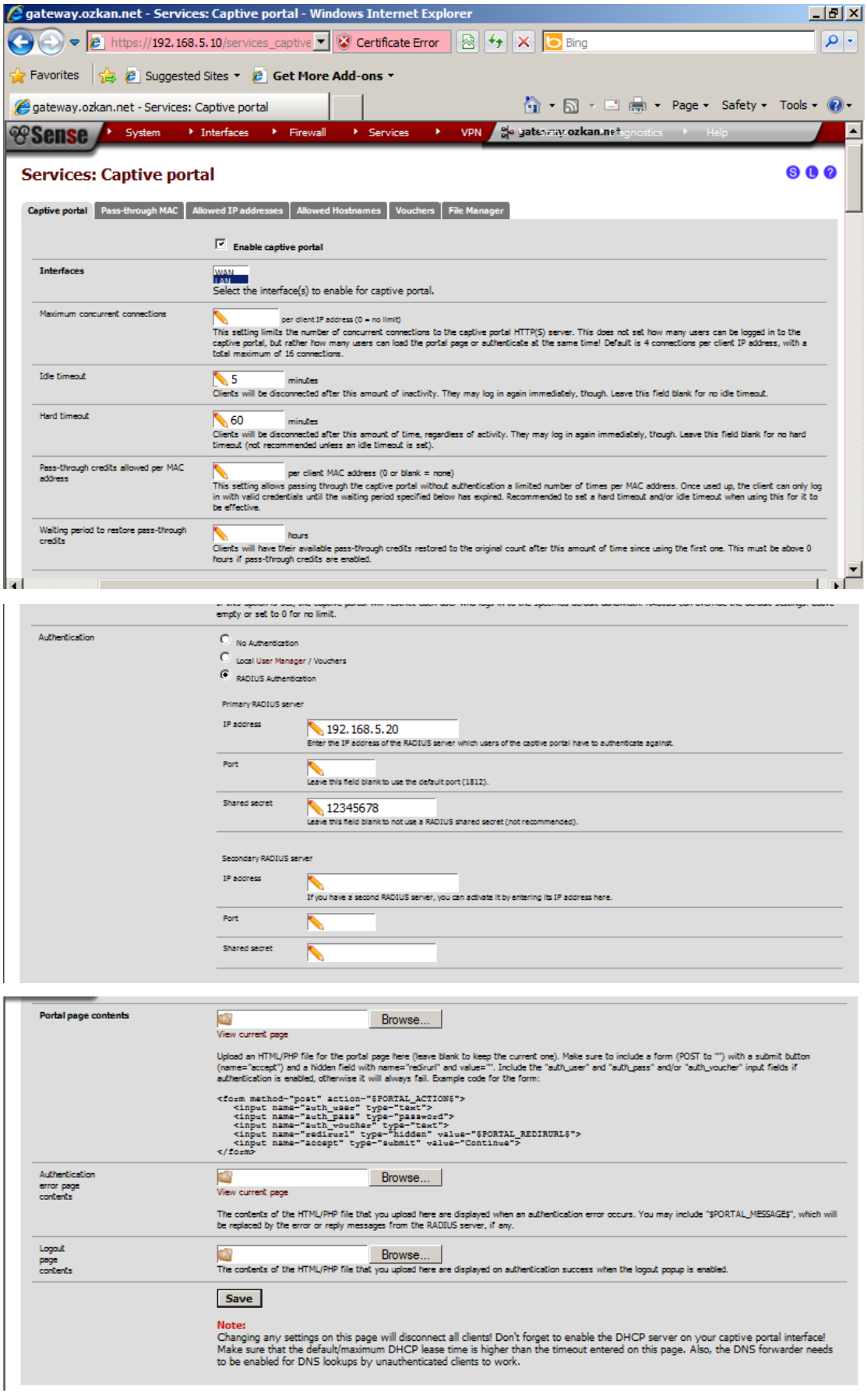
Şekil 4.7 : Güvenlik duvarı erişim kuralları ekran görüntüsü

Kullanıcıların ağa bağlandıklarında otomatik olarak IP adresi alması için DHCP ayarları yapılmıştır. Kullanıcılar bu sayede ağa bağlandıklarında 192.168.5.30 ile 192.168.5.200 arasında bir IP adresi, ayrıca DNS sunucu ve ağ geçidi olarak 192.168.5.10 yani güvenlik duvarının IP adresini alırlar.



Şekil 4.8 : DHCP ayarları ekran görüntüsü

Kullanıcıların ağa bağlandıklarında web arayüzü üzerinden kimlik doğrulaması yapması için Services altında Captive Portal bölümü etkileştirilmiş ve RADIUS sunucu ayarları yapılmıştır. Captive Portal ayarları aşağıdaki şekil 4.9'da gösterilmiştir.



Şekil 4.9 : Captive Portal ayarları ekran görüntüsü

Bu ekranda ;

Interface – Captive Portal'in hangi ağ kartı üzerinden gelen kullanıcılar için etkin olacağı,

Idle Timeout – Kullanıcıların oturumlarının hiçbir işlem yapmaması durumunda zaman aşımına uğrayacağı,

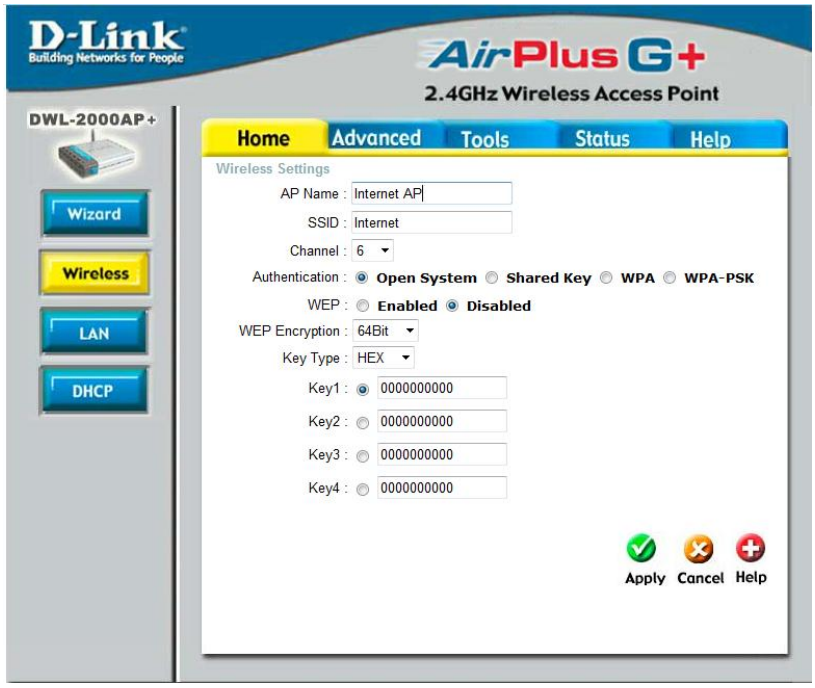
Hard Timeout – Kullanıcıların oturumlarının aktivite olmasına rağmen kaç dakika sonra zaman aşımına uğrayacağı,

Authentication – Kullanıcıların oturum açarken hangi yöntemle kimlik doğrulamasının yapılacağı (burada RADIUS sunucu ile kimlik doğrulama yapılacağı için RADIUS sunucu IP adresi ve paylaşım şifresi girilmiştir) belirlenir.

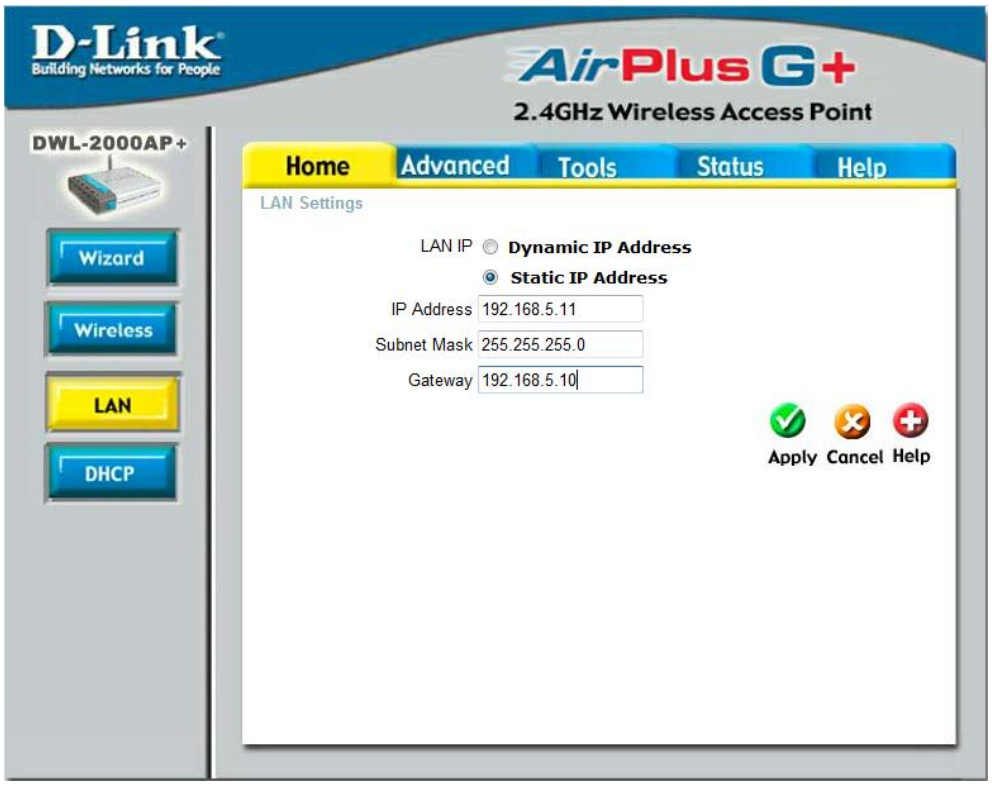
Portal Page, authentication error, logout page contents – Kullanıcıların oturum açarken, kimlik doğrulamada, oturum kapatırken kullanılan web arayüzü içerikleri geliştirilerek buradan yüklenmiştir.

4.1.3 Kablosuz Erişim Noktası:

Kablosuz ağ cihazlarına internet erişimi sağlayacak olan Kablosuz erişim noktası görünen SSID ismi Internet olacak şekilde ayarlanmış (Şekil 4.10) ve 192.168.5.11 IP adresi atanmıştır (Şekil 4.11).



Şekil 4.10 : Kablosuz erişim noktası (AP) SSID ayarları ekran görüntüsü



Şekil 4.11 : Kablosuz erişim noktası (AP) IP ayarları ekran görüntüsü

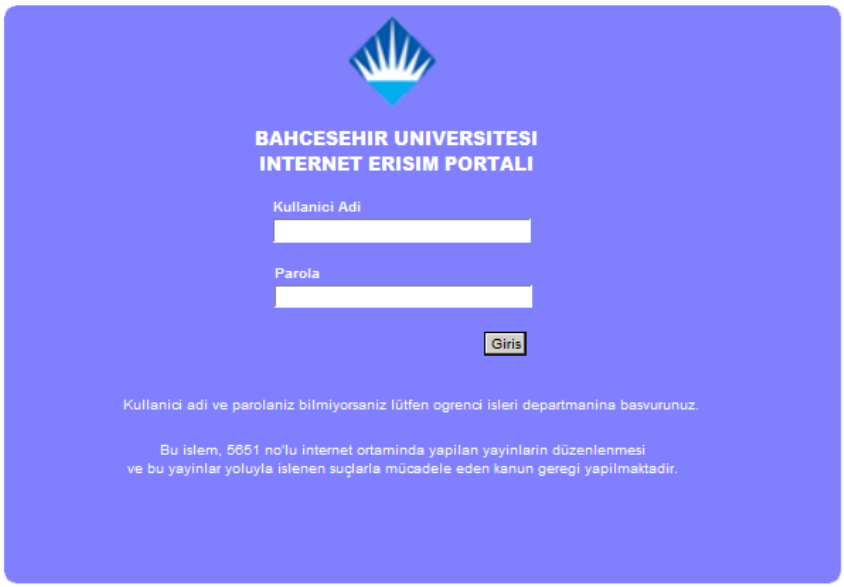
4.2 YAPILAN GELİŞTİRMELER

Kurulum bileşenleri üzerinde yapılan temel konfigürasyonlar sonrasında sistemin genelinde birtakım geliştirme ve özelleştirmeler yapılmıştır. Bu geliştirme ve özelleştirmeler aşağıdaki gibidir.

4.2.1 Captive Portal Ekranları

Pfsense güvenlik duvarı sistem kurulumu ile beraber gelen standart Captive Portal ekranları yerine Bahçeşehir Üniversitesi için özelleştirilmiş ekranlar tasarlanmıştır.

Captive Portal giriş ekranı için Captiveportal.html tasarlanmış olup ekran görüntüsü aşağıda şekil 4.12'de ve bu ekrana ait kodlar tablo 4.1'de gösterilmiştir.



Şekil 4.12 : Captiveportal.html ekran görüntüsü

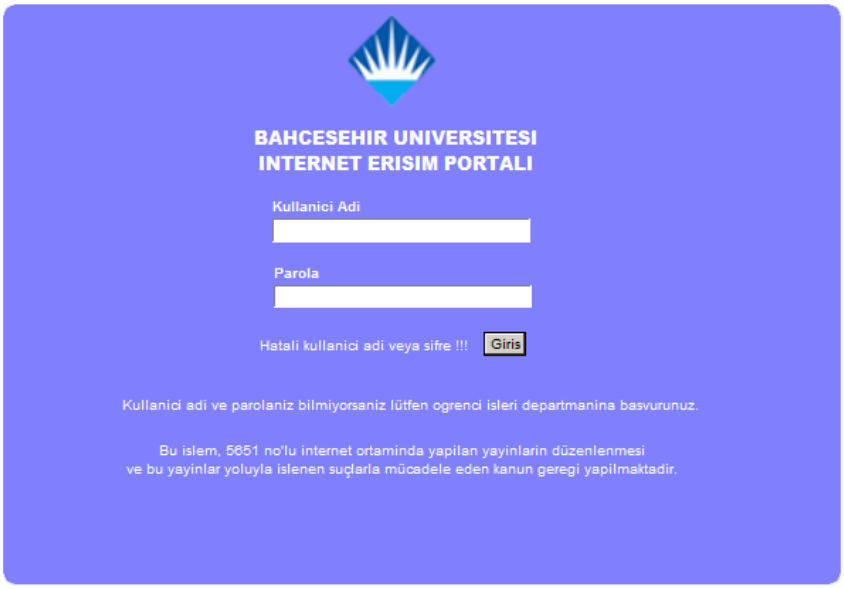
Tablo 4.1 : Captiveportal.html kodları

```
<html>
<head>
<title>Bahcesehir Universitesi Internet Erisim Portali</title>
<meta http-equiv="content-type" content="text/html; charset=windows-1254">
<meta http-equiv="Content-Language" content="tr">
<style type="text/css">
/*----------Text Styles----------*/
.ws6 {font-size: 8px;}
.ws7 {font-size: 9.3px;}
.ws8 {font-size: 11px;}
.ws9 {font-size: 12px;}
.ws10 {font-size: 13px;}
.ws11 {font-size: 15px;}
.ws12 {font-size: 16px;}
.ws14 {font-size: 19px;}
.ws16 {font-size: 21px;}
.ws18 {font-size: 24px;}
.ws20 {font-size: 27px;}
.ws22 {font-size: 29px;}
.ws24 {font-size: 32px;}
.ws26 {font-size: 35px;}
.ws28 {font-size: 37px;}
.ws36 {font-size: 48px;}
.ws48 {font-size: 64px;}
.ws72 {font-size: 96px;}
.wpmd {font-size: 13px;font-family: Arial,Helvetica,Sans-Serif;font-style: normal;font-weight: normal;}
/*----------Para Styles----------*/
DIV,UL,OL /* Left */
{
 margin-top: 0px;
 margin-bottom: 0px;
}
</style>
</head>
```

Tablo 4.1 : Captiveportal.html kodları (devam)

```
<body Text="#FFFFFF">
<div id="roundrect1" style="position:absolute; overflow:hidden; left:134px; top:23px; width:701px; height:485px; z-index:0"><img border=0 width="100%" height="100%" alt="" src="captiveportal-roundrect21843556.gif"></div>
<div id="text1" style="position:absolute; overflow:hidden; left:359px; top:184px; width:99px; height:25px; z-index:1">
<div class="wpmd">
<div><font face="Franklin Gothic Book"><B>Kullanici Adi</B></font></div>
</div></div>
<div id="text2" style="position:absolute; overflow:hidden; left:360px; top:239px; width:99px; height:26px; z-index:3">
<div class="wpmd">
<div><B>Parola</B></div>
</div></div>
<form method="post" action="#PORTAL_ACTION#">
<input name="auth_user" type="text" style="position:absolute;width:216px;left:359px;top:202px;z-index:2">
<input name="auth_pass" type="password" style="position:absolute;width:216px;left:360px;top:257px;z-index:4">
<input name="accept" type="submit" value="Giris" style="position:absolute;left:536px;top:296px;z-index:5">
<input name="redirurl" type="hidden" value="#PORTAL_REDIRURL#">
</form>
<div id="image1" style="position:absolute; overflow:hidden; left:419px; top:31px; width:80px; height:80px; z-index:8"><img src="captiveportal-bahcesehir_min_logo.png" alt="" title="" border=0 width=80 height=80></div>
<div id="text3" style="position:absolute; overflow:hidden; left:335px; top:123px; width:254px; height:80px; z-index:9">
<div class="wpmd">
<div align=center><font face="Arial Black" class="ws12">BAHCESEHIR UNIVERSITESI</font></div>
<div align=center><font face="Arial Black" class="ws12">INTERNET ERISIM PORTALI</font></div>
</div></div>
<div id="text4" style="position:absolute; overflow:hidden; left:192px; top:388px; width:550px; height:65px; z-index:10">
<div class="wpmd">
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book">Bu islem, 5651 no'lu internet ortaminda yapilan yayinlarin düzenlenmesi</font></div>
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book"> ve bu yayinlar yoluyla islenen suçlarla mücadele eden kanun geregi yapilmaktadir.</font></div>
</div></div>
<div id="text6" style="position:absolute; overflow:hidden; left:189px; top:350px; width:571px; height:20px; z-index:11">
<div class="wpmd">
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book">Kullanici adi ve parolaniz bilmiyorsaniz lütfen ogrenci isleri departmanina basvurunuz.</font></div>
</div></div>
</body>
</html>
```

Captive Portal giriş ekranında kullanıcı adı ve şifrenin yanlış girilmesi sonucunda gelen ekran için Captiveportal-error.html tasarlanmış olup ekran görüntüsü aşağıda şekil 4.13'te ve bu ekrana ait kodlar tablo 4.2'de gösterilmiştir.



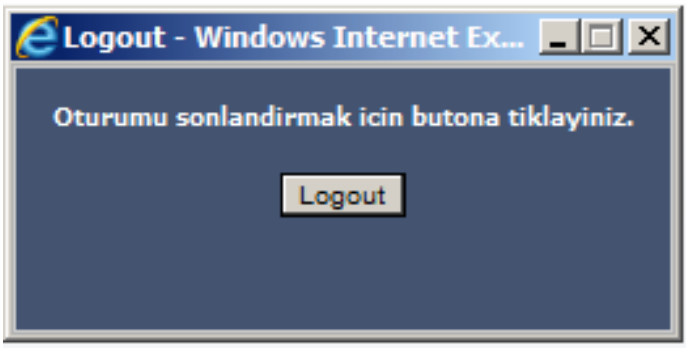
Şekil 4.13 : Captiveportal-error.html ekran görüntüsü

Tablo 4.2 : Captiveportal-error.html kodları

```
<html>
<head>
<title>Bahcesehir Universitesi Internet Erisim Portali</title>
<meta http-equiv="content-type" content="text/html; charset=windows-1254">
<meta http-equiv="Content-Language" content="tr">
<style type="text/css">
/*----------Text Styles----------*/
.ws6 {font-size: 8px;}
.ws7 {font-size: 9.3px;}
.ws8 {font-size: 11px;}
.ws9 {font-size: 12px;}
.ws10 {font-size: 13px;}
.ws11 {font-size: 15px;}
.ws12 {font-size: 16px;}
.ws14 {font-size: 19px;}
.ws16 {font-size: 21px;}
.ws18 {font-size: 24px;}
.ws26 {font-size: 35px;}
.ws28 {font-size: 37px;}
.ws36 {font-size: 48px;}
.ws48 {font-size: 64px;}
.ws72 {font-size: 96px;}
.wpmd {font-size: 13px;font-family: Arial,Helvetica,Sans-Serif;font-style: normal;font-weight: normal;}
/*----------Para Styles----------*/
DIV,UL,OL /* Left */
{
margin-top: 0px;
```

Tablo 4.2 : Captiveportal-error.html kodları (devam)

```
margin-bottom: 0px;
}
</style>
</head>
<body Text="#FFFFFF">
<div id="roundrect1" style="position:absolute; overflow:hidden; left:134px; top:23px; width:701px;
height:485px; z-index:0"><img border=0 width="100%" height="100%" alt="" src="captiveportal-
roundrect21843556.gif"></div>
<div id="text1" style="position:absolute; overflow:hidden; left:359px; top:184px; width:99px;
height:25px; z-index:1">
<div class="wpmd">
<div><font face="Franklin Gothic Book"><B>Kullanici Adi</B></font></div>
</div></div>
<div id="text2" style="position:absolute; overflow:hidden; left:360px; top:239px; width:99px;
height:26px; z-index:3">
<div class="wpmd">
<div><B>Parola</B></div></div></div>
<form method="post" action="#PORTAL_ACTION#">
<input name="auth_user" type="text" style="position:absolute;width:216px;left:359px;top:202px;z-
index:2">
<input name="auth_pass" type="password"
style="position:absolute;width:216px;left:360px;top:257px;z-index:4">
<input name="accept" type="submit" value="Giris" style="position:absolute;left:536px;top:296px;z-
index:5">
<input name="redirurl" type="hidden" value="#PORTAL_REDIRURL#"></form>
<div id="image1" style="position:absolute; overflow:hidden; left:419px; top:31px; width:80px;
height:80px; z-index:8"><img src="captiveportal-bahcesehir_min_logo.png" alt="" title="" border=0
width=80 height=80></div>
<div id="text3" style="position:absolute; overflow:hidden; left:335px; top:123px; width:254px;
height:80px; z-index:9">
<div class="wpmd">
<div align=center><font face="Arial Black" class="ws12">BAHCESEHIR
UNIVERSITESI</font></div>
<div align=center><font face="Arial Black" class="ws12">INTERNET ERISIM
PORTALI</font></div>
</div></div>
<div id="text4" style="position:absolute; overflow:hidden; left:192px; top:388px; width:550px;
height:65px; z-index:10">
<div class="wpmd">
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book">Bu islem, 5651 no'lu internet
ortaminda yapilan yayinlarin düzenlenmesi</font></div>
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book"> ve bu yayinlar yoluyla
islenen suçlarla mücadele eden kanun geregi yapilmaktadir.</font></div>
</div></div>
<div id="text5" style="position:absolute; overflow:hidden; left:150px; top:300px; width:571px;
height:20px; z-index:11">
<div class="wpmd">
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book">Hatali kullanici adi veya sifre
!!! </font></div></div></div>
<div id="text6" style="position:absolute; overflow:hidden; left:189px; top:350px; width:571px;
height:20px; z-index:11">
<div class="wpmd">
<div align=center><font color="#FFFFFF" face="Franklin Gothic Book">Kullanici adi ve parolaniz
bilmiyorsaniz lütfen ogrenci isleri departmanina basvurunuz.</font></div>
</div></div>
</body>
</html>
```



Şekil 4.14 : Captiveportal-logout.html ekran görüntüsü

Tablo 4.3 : Captiveportal-logout.html kodları

```
<HTML>
<HEAD><TITLE>Yönlendiriliyor...</TITLE></HEAD>
<BODY>
<SPAN STYLE="font-family: Tahoma, Verdana, Arial, Helvetica, sans-serif; font-size: 11px;">
<B>Redirecting to <A HREF="<?=$my_redirurl;?>"><?=$my_redirurl;?></A>...</B>
</SPAN>
<SCRIPT LANGUAGE="JavaScript">
<!--
LogoutWin = window.open('', 'Logout',
'toolbar=0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=256,height=64');
if (LogoutWin) {
        LogoutWin.document.write('<HTML>');
        LogoutWin.document.write('<HEAD><TITLE>Logout</TITLE></HEAD>') ;
        LogoutWin.document.write('<BODY BGCOLOR="#435370">');
        LogoutWin.document.write('<DIV ALIGN="center" STYLE="color: #ffffff; font-family:
Tahoma, Verdana, Arial, Helvetica, sans-serif; font-size: 11px;">') ;
        LogoutWin.document.write('<B>Baglantiyi sonlandirmak icin butona tiklayiniz. </B><P>');
        LogoutWin.document.write('<FORM METHOD="POST" ACTION="<?=$logouturl;?>">');
        LogoutWin.document.write('<INPUT NAME="logout_id" TYPE="hidden"
VALUE="<?=$sessionid;?>">');
        LogoutWin.document.write('<INPUT NAME="logout" TYPE="submit" VALUE="Logout">');
        LogoutWin.document.write('</FORM>');
        LogoutWin.document.write('</DIV></BODY>');
        LogoutWin.document.write('</HTML>');
        LogoutWin.document.close();
}

document.location.href="<?=$my_redirurl;?>";
-->
</SCRIPT>
</BODY>
</HTML>
```

4.2.2 Güvenlik Duvarı Log Ayarları

Güvenlik duvarı üzerinde yapılan geliştirme ile oluşan DHCP loglarının Telekomünikasyon İletişim Başkanlığı'nın (TİB) belirlediği ve 5651 sayılı kanun (5651 sayılı kanunun tam metni bu tezin ekinde Ek.1 olarak verilmiştir) tarafından

istenen şekilde formatlanması ve istenilen bir FTP sunucusuna aktarılması sağlanmıştır. TİB tarafından istenen DHCP iç dağıtım listelerinin örnek formatı aşağıdaki gibidir.

Tablo 4.4 : Örnek iç dağıtım listesi formatı

IP adresi	Kullanım Başlama Tarih-Saati	Kullanım Bitiş Tarih-Saati	MAC Adresi
192.168.1.2	10.07.2008-09:00:00	10.07.2008-21:00:00	00-1A-92-AD-ED-F3
192.168.1.3	10.07.2008-09:00:00	10.07.2008-21:00:00	00-1A-92-ED-AD-AA
192.168.1.5	10.07.2008-09:00:00	10.07.2008-21:00:00	00-1A-92-1D-CC-20
192.168.1.10	10.07.2008-09:00:00	10.07.2008-21:00:00	00-1A-EE-11-22-33

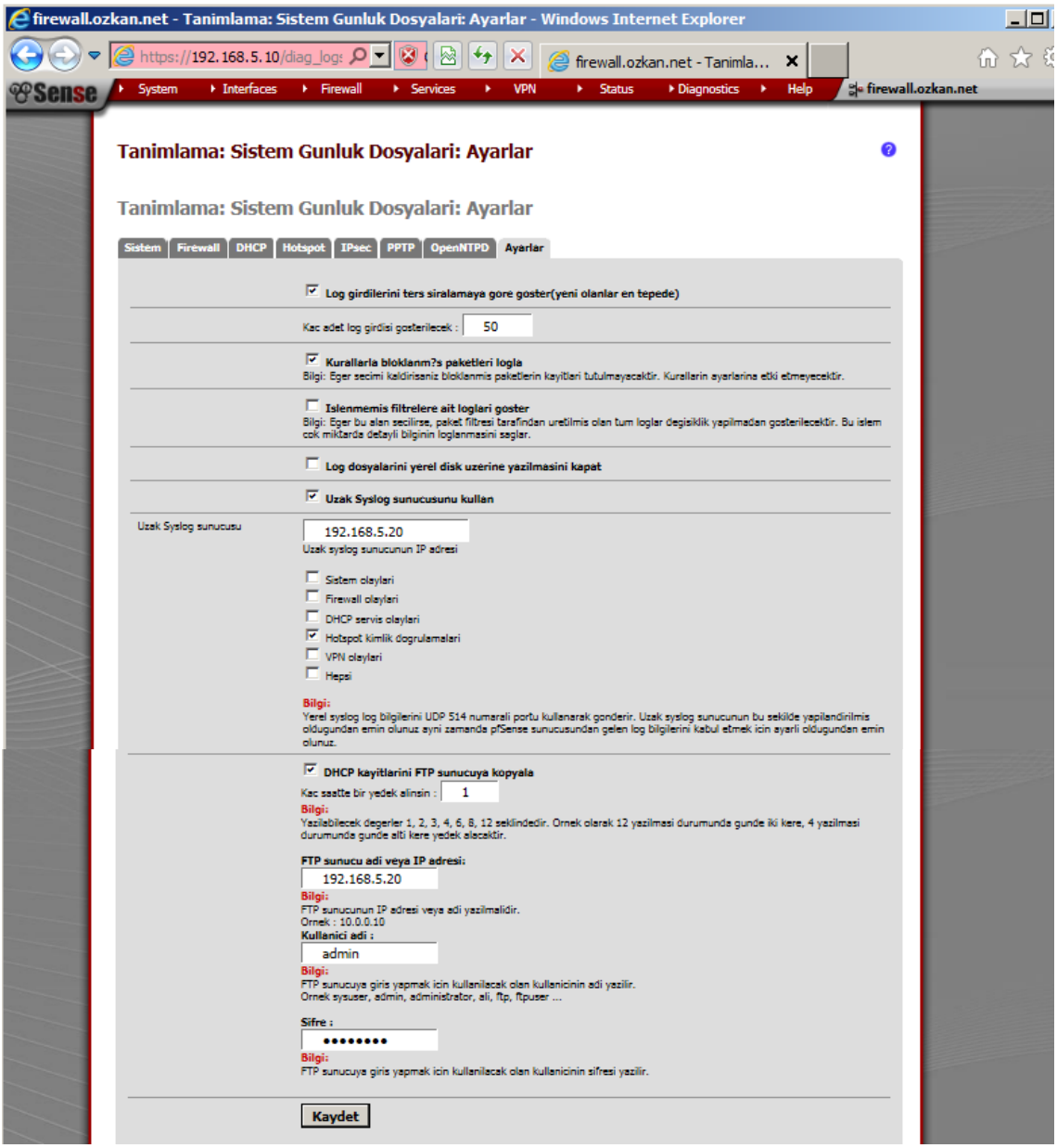
Kaynak : Türkiye İletişim Başkanlığı web sitesi (http://www.tib.gov.tr)

Yukarıdaki log formatına göre DHCP loglarının normalizasyonu için güvenlik duvarına geliştirilmiş olan dhcptibduzenle.sh programı eklenmiştir. Dhcptibdüzenle.sh programının kodları aşağıda tablo 4.5'te gösterilmiştir.

Tablo 4.5 : Dhcptibduzenle.sh program kodları

```
# dhcp.awk
# awk -f dhcp.awk  < /var/dhcpd/var/db/dhcpd.leases
/lease\ [0-9]*\.[0-9]*\.[0-9]*\.[0-9]*\ {/ {
        printf("%s\t\t", $2);
}
/starts\ [^;]*;/ {
        sub(";", "", $4);
        printf("%s-%s\t\t", $3, $4);
}
/ends\ [^;]*;/ {
        sub(";", "", $4);
        printf("%s-%s\t\t", $3, $4);
}
/hardware\ ethernet\ [^;]*;/ {
        sub(";", "", $3);
        printf("%s\r\n", $3);
}
```

Yukarıdaki dhcptibduzenle.sh programının belirtilen zamanlarda çalıştırılması ve tablo 4.4'te belirtilen formatta oluşturulan logların bir FTP sunucusuna aktarılması için güvenlik duvarında bulunan diag_logs_settings.php dosyası düzenlenerek eklemeler yapılmıştır. Düzenleme sonucunda güvenlik duvarı log ayarları web arayüzü şekil 4.15'te görüldüğü gibidir.



Şekil 4.15 : Güvenlik duvarı log ayarları ekran görüntüsü

Güvenlik duvarı log ayarları web arayüzünün eklenen kodlar aşağıda tablo 4.6 diag_log_settings.php kodları tablosunda verilmiştir.

Tablo 4.6 : Diag_log_settings.php dosyasına eklenen kodlar

```
#!/bin/sh
tarih=`date "+%Y%m%d-%H%M%S"`
HOST='{$config['system']['hostname']}.{$config['system']['domain']}'
USER='{$_POST['ftptibyedekkullanici']}'
PASSWD='{$_POST['ftptibyedeksifre']}'
SERVER='{$_POST['ftptibyedekip']}'
mkdir /var/mountftp
cd /var/mountftp
awk -f /sbin/dhcptibduzenle.sh < /var/dhcpd/var/db/dhcpd.leases > ./dhcplog\$HOST-\$tarih.txt
logger `ftp -n -v \$SERVER << EOT
ascii
user \$USER \$PASSWD
prompt
put dhcplog\$HOST-\$tarih.txt
bye
EOT`
cd ..
rm -rf /var/mountftp
EOF;
                        file_put_contents("/sbin/dhcplistcronftp.sh", $fstab);
                        exec("chmod 755 /sbin/dhcplistcronftp.sh");
                }//eger ftptibyedek false ise
                else{
                        if (empty($_POST['ftptibyedek'])) {
                        /* test whether a cron item exists and unset() it if necessary */
                        $itemhash = getFTPCRONSettings();
                        $item = $itemhash['ITEM'];
                        if (isset($item)) { unset($config['cron']['item'][$itemhash['ID']]); }
                        }
                }
                /* crontab yeniden baslat */
                configure_cron();
                sigkillbypid("{$g['varrun_path']}/cron.pid", "HUP");
                write_config();
                $retval = 0;
                config_lock();
                $retval = system_syslogd_start();
                if ($oldnologdefaultblock !== isset($config['syslog']['nologdefaultblock']))
                        $retval |= filter_configure();
                config_unlock();
                $savemsg = get_std_save_message($retval);
        }
}
                                                <tr>
                <td width="22%" valign="top" class="vtable"> </td>
                <td width="78%" class="vtable">
                  <input name="ftptibyedek" type="checkbox" id="ftptibyedek" value="yes" <?php if
($pconfig['ftptibyedek']) echo "checked"; ?>>
                  <strong> DHCP kayitlarini FTP sunucuya kopyala</strong>
                                                        <br>
                                                        Kac saatte bir yedek alinsin :
                                                        <input name="ftptibyedeksaat"
id="ftptibyedeksaat" type="text"
                                                        class="formfld" size="2"
value="<?=htmlspecialchars($pconfig['ftptibyedeksaat']);?>">
                                                                <br>
```

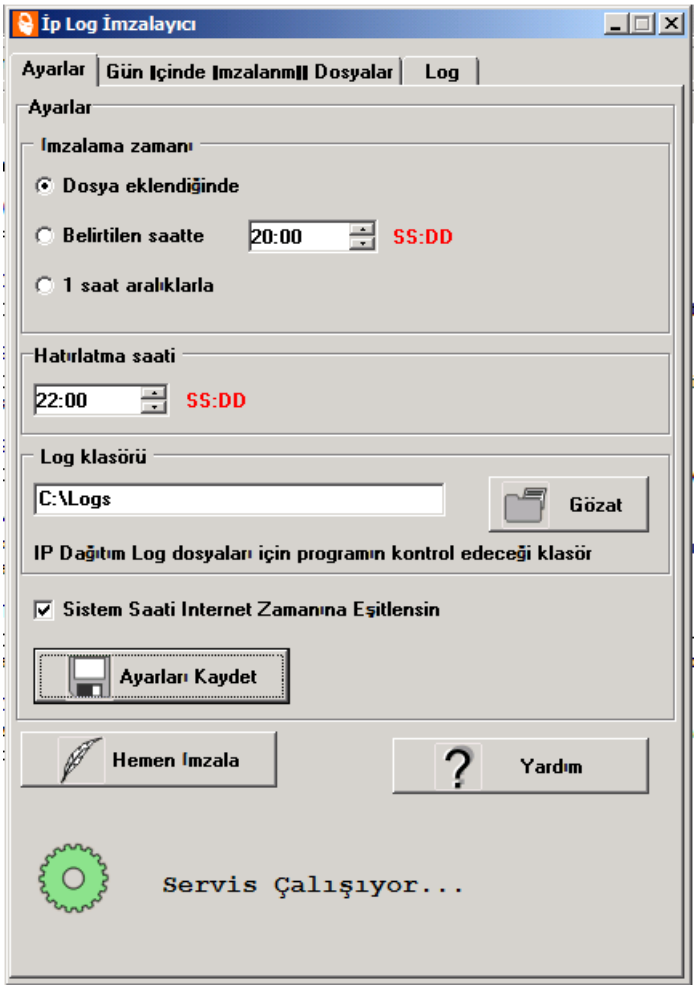
Tablo 4.6 : Diag_log_settings.php dosyasına eklenen kodlar (devam)

```
                                                    <strong><span
class="red">Bilgi:</span></strong>
                                                    <br>
                                                    Yazilabilecek degerler 1, 2, 3, 4, 6, 8, 12
seklindedir. Ornek olarak 12 yazilmasi
                                                    durumunda gunde iki kere, 4 yazilmasi
durumunda gunde alti kere yedek alacaktir.
                                                    <br>
                                                    <br>
                                                    <strong>FTP sunucu adi veya IP adresi:
</strong><br>
                                                    <input name="ftptibyedekip" id="ftptibyedekip"
type="text"
                                                    class="formfld" size="15"
value="<?=htmlspecialchars($pconfig['ftptibyedekip']);?>">
                                                    <br>
                                                    <strong><span
class="red">Bilgi:</span></strong>
                                                    <br>
                                                    FTP sunucunun IP adresi veya adi
yazilmalidir.<br>
                                                    Ornek : 10.0.0.10
                                                    <br>
                                                    <strong>Kullanici adi :</strong><br>
                                                    <input name="ftptibyedekkullanici"
id="ftptibyedekkullanici" type="text"
                                                    class="formfld" size="15"
value="<?=htmlspecialchars($pconfig['ftptibyedekkullanici']);?>">
                                                    <br>
                                                    <strong><span
class="red">Bilgi:</span></strong>
                                                    <br>

                                                    FTP sunucuya giris yapmak icin kullanilacak olan
kullanicinin adi yazilir. <br>
                                                    Ornek sysuser, admin, administrator, ali, ftp,
ftpuser ...
                                                    <br>
                                                    <br>
                                                    <strong>Sifre : </strong><br>
                                                    <input name="ftptibyedeksifre"
id="ftptibyedeksifre" type="password"
                                                    class="formfld" size="15"
value="<?=htmlspecialchars($pconfig['ftptibyedeksifre']);?>">
                                                    <br>
                                                    <strong><span
class="red">Bilgi:</span></strong>
                                                    <br>

                                                    FTP sunucuya giris yapmak icin kullanilacak olan
kullanicinin sifresi yazilir. <br>
                                                    <br>
                                                    </td>
                </tr>
```

4.2.3 DHCP Loglarının İmzalanması

Güvenlik duvarı tarafından oluşturulan ve FTP sunucuya aktarılan DHCP logları 5651 sayılı kanun gereğince değiştirilmediklerinin kanıtlanması için nitelikli ya da niteliksiz zaman damgasıyla imzalanmalıdır. Zaman damgası sertifikası dağıtımına yetkili otoritelerden sağlanan zaman damgası nitelikli zaman damgası, yetkili olmayan otoritelerden ya da sistemin kendi iç yapısında kurulu otorite tarafından sağlanan zaman damgası niteliksiz zaman damgası olarak tanımlanmaktadır. (Kaynak : Telekomünikasyon İletişim Başkanlığı – TİB http://www.tib.gov.tr)

Bu tez çalışmasında Telekomünikasyon İletişim Başkanlığı tarafından sağlanan imzalama programının logların bulunduğu FTP sunucuya kurularak logların imzalanması sağlanmıştır. Programın ayarları ekran görüntüsü aşağıda şekil 4.16'da gösterildiği gibidir.

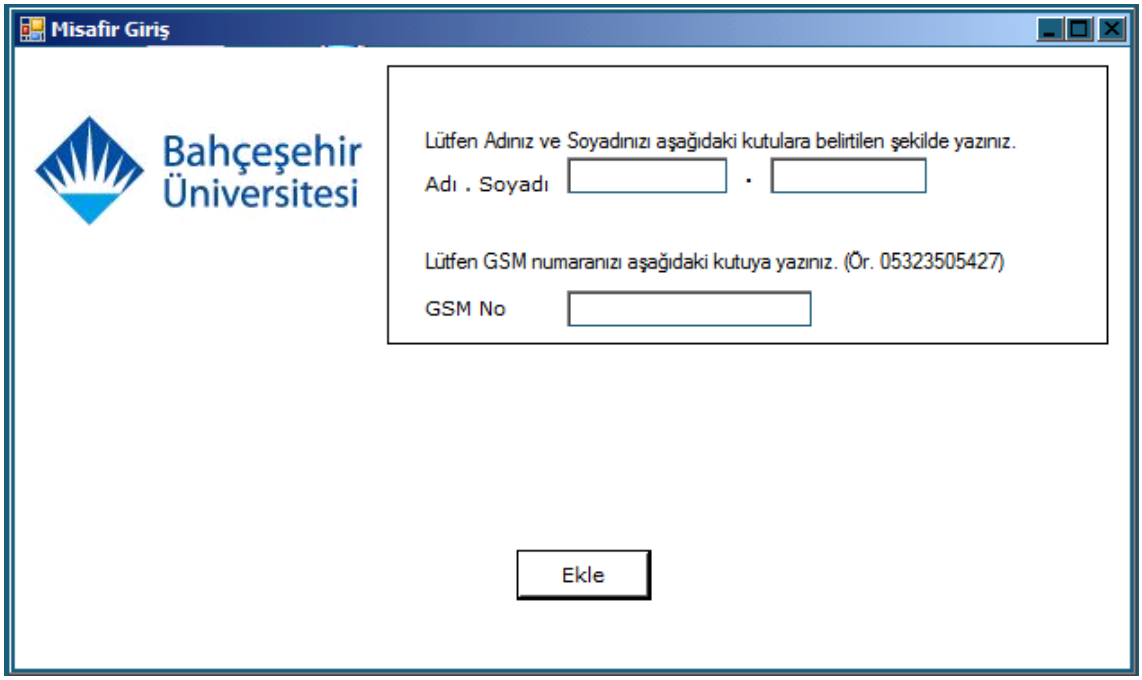


Şekil 4.16 : Log imzalama programı ekran görüntüsü

FTP sunucu üzerine kurulan bu program aracılığıyla sistem saatinin internet üzerinden zaman sunucusu ile saat ve tarih bilgisinin eşitlenmesi ve belirtilen klasöre eklenen her log dosyasının imzalanması sağlanmaktadır.

4.2.4 Sisteme Kullanıcı Ekleme Programı

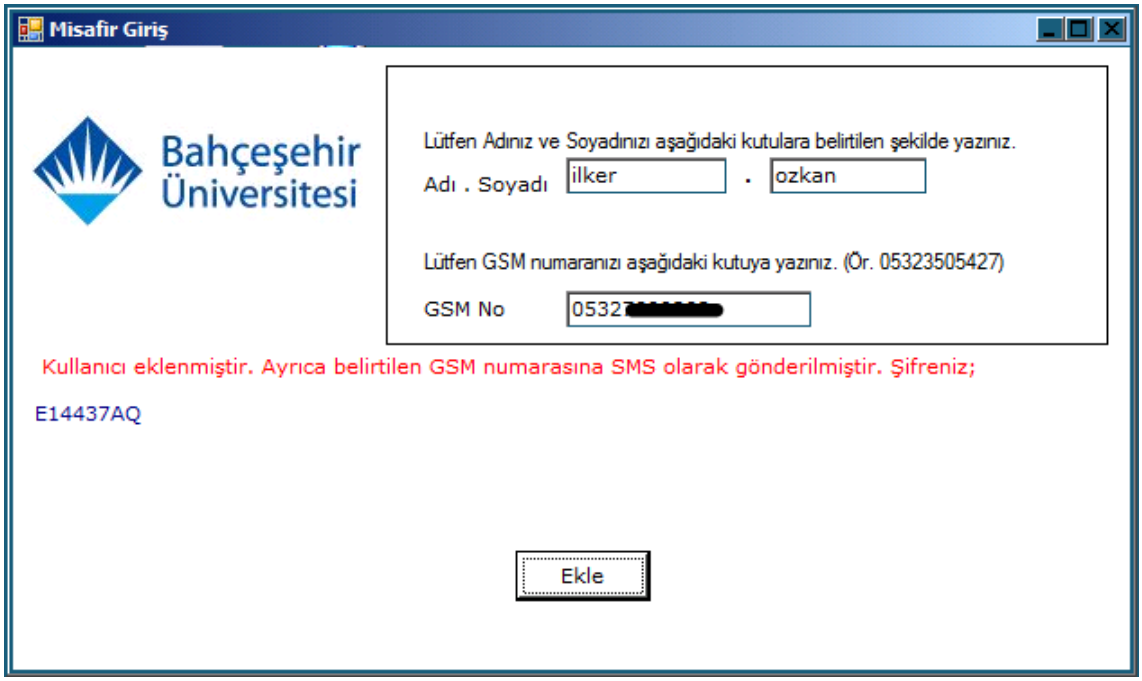
Captive portal sistemi, Güvenlik Duvarı üzerinde tanımlanan RADIUS sunucu ile iletişimde bulunarak kullanıcıların kimlik doğrulamasının yapılmasını sağlamakta, RADIUS sunucu ise bu hizmeti bağlı bulunduğu Active Directory dizin hizmeti sunucusu üzerindeki kullanıcı bilgilerinin doğruluğunu denetleyerek iletmektedir. Kimlik bilgilerinin tutulduğu ortam RADIUS değil, dizin hizmetleri sunucusudur. Bu sunucuya yeni kullanıcıların eklenmesi, dizin sunucusu üzerinde ya da aynı etki alanında bulunan bir sistem üzerinde çalışan dizin hizmeti konsolu aracılığıyla yapılmaktadır. Bu kullanıcı ekleme işlemi sırasında kullanıcıya ait şifre işlemi yapan personel tarafından belirlenir. Yeni bir kullanıcının eklenmesi işinin daha basit hale getirilmesi, bu iş için kullanılan operatör için yetkinliğe ihtiyaç duyulmaması ya da kullanıcı ekleme işleminin tamamen self servis hale getirilmesi için aşağıda şekil 4.17 ile ekran görüntüsü verilen program geliştirilmiştir.



Şekil 4.17 : Kullanıcı ekleme programı ekran görüntüsü

C# ortamında geliştirilen bu programda, eklenmek istenen kullanıcının adı ve soyadı ve cep telefonu numarası uygun şekilde giriş kutularına eklenir. Ekle butonuna tıklandığında program kullanıcının adı, soyadı ve cep telefonu bilgisini Active Directory sunucusu üzerinde program içinde belirlenmiş format ile ekler. Eklenen kullanıcının kullanıcı adı adı.soyadı şeklindedir. Kullanıcının sisteme eklenmesi sırasında aynı zamanda sekiz karakterden oluşan ve güvenli olması açısından içerisinde hem numaralar hem de harfler bulunan bir şifre oluşturur. Bu kullanıcı adı ve şifre sisteme eklenmiş ve kullanılmaya hazırdır. Son adımda kullanıcı adı ve şifre, programa girilmiş olan cep telefonu numarasına kısa mesaj yoluyla iletilir.

Kullanıcı ekleme işlemi sonucu aşağıda şekil 4.18 ile gösterildiği gibidir.



Şekil 4.18 : Kullanıcı ekleme işlemi sonucu

Program kodları aşağıda tablo 4.7'de verilmiştir.

Tablo 4.7 : Kullanıcı Ekleme Programı Kodları

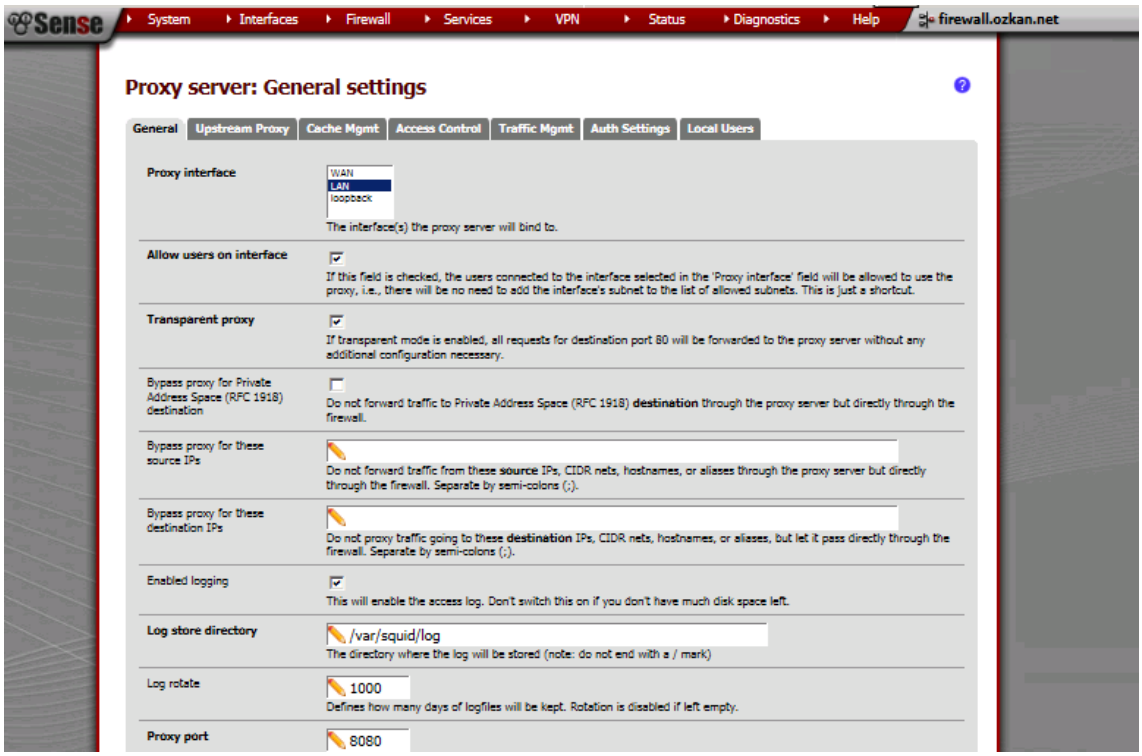
```
Using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.DirectoryServices;
using System.Diagnostics;
using System.Net.Mail;
using System.Net.Mime;
using System.Net;
using System.IO;

namespace ActiveDirectoryTest
{
   public partial class FormAddUser : Form
   {
      public FormAddUser()
      {
         InitializeComponent();
      }

      private void button1_Click(object sender, EventArgs e)
      {
         String pass = createRandomNumber();
         labelPass.Text = "";
         labelStatus.Text = "";
         labelStatus.Text = LaunchCommandLineApp(textBoxUser1.Text, textBoxUser2.Text,
textBoxGSM.Text, pass);
         labelPass.Text = pass;
       }
      static string LaunchCommandLineApp(string name, string Surname, string GSM, string password)
      {
         // Use ProcessStartInfo class
         ProcessStartInfo startInfo = new ProcessStartInfo();
         String username = name + "." + Surname;
         startInfo.CreateNoWindow = true;
         startInfo.UseShellExecute = false;
         startInfo.FileName = " dsadd.exe";
         startInfo.WindowStyle = ProcessWindowStyle.Hidden;
         startInfo.Arguments = "user cn=" + username + ",ou=misafir,dc=ozkan,dc=net -memberof
cn=Misafir_grubu,ou=misafir,dc=ozkan,dc=net -fn " + username + " -ln " + username + " -upn " +
username + "@ozkan.net -pwd " + password + " -acctexpires 1 -mobile " + GSM + " -samid " +
username + " -desc \"Misafir kullanıcı\" -office \"Kampus\" -disabled no";

         try
         {
            using (Process exeProcess = Process.Start(startInfo))
            {
               exeProcess.WaitForExit();
            }
         }
         catch (Exception E)
```

Tablo 4.7 : Kullanıcı Ekleme Programı Kodları (devam)

```
        {
            return E.Message.ToString();
        }
        return "Kullanıcı eklenmiştir. Ayrıca belirtilen GSM numarasına SMS olarak gönderilmiştir.
Şifreniz; ";
    }

    private static string createRandomNumber()
    {
        string deger=""; //boş değer tanımlıyoruz
        Random rnd=new Random(); // rastgele değeri tanımlıyouz
        for (int i = 0; i < 8; i++) //8 haneli rakam-harf üretmek için döngü sağlıyoruz
        {
            int karar=rnd.Next(0,2); // 0 veya 1
            if (karar == 0) // rastgele üretilen sayı 0 ise sayı üret
            {
                int sayi = rnd.Next(1, 10);
                deger += sayi.ToString();
            }
            else // değilse harf üret (65 ile 91 arası ascii kodlar olduğu için rakam değerleri girilmiştir)
            {
                int x = rnd.Next(65, 91);
                char harf = Convert.ToChar(x); //ascii kod olarak üretilen sayıyı harfe çevrilir
                deger += harf; //değere atanır
            }
        }
        return deger;
        }
    private string GonderOku(String Telno, String mesaj)
    {
        string donecek = "";
        WebClient client = new WebClient();
        client.Headers.Add("user-agent", "Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.2; .NET
CLR 1.0.3705;)");
        client.QueryString.Add("id", "GL9FTSPB");
        client.QueryString.Add("sifre", "SFZ21ANT");
        client.QueryString.Add("gonderen", "Bahcesehir Unv");
        client.QueryString.Add("telefon", Telno );
        client.QueryString.Add("mesaj", mesaj);
        string url = "http://www.mutlusms.com/api/gonder.do";
        Stream data = client.OpenRead(url);
        StreamReader reader = new StreamReader(data);

        donecek = reader.ReadToEnd();
        data.Close();
        reader.Close();

        return donecek;
    }
```

4.2.5 Vekil Sunucu Kurulum ve ayarlama

5651 sayılı kanun gereğince yapılan erişimlerde internet üzerinde gidilen sayfalara ilişkin GET ve PUT bilgilerinin loglanması beklenmektedir. Bu gereksinimi karşılamak üzere Güvenlik Duvarı üzerinde squid vekil sunucu (Proxy Server) kurulumu yapılarak loglamanın yapılması sağlanmıştır. Oluşan log dosyaların Güvenlik Duvarı üzerinde /var/squid/log dizininde saklanmaktadır. Squid ayarları ekran görüntüsü aşağıda şekil 4.19'da gösterilmektedir.

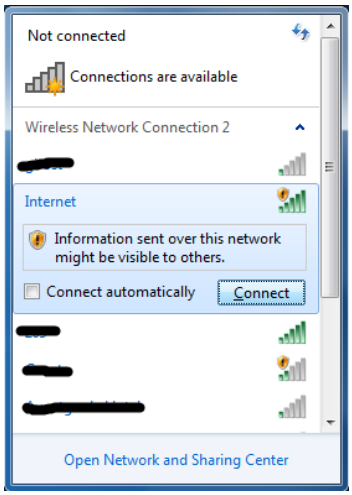


Şekil 4.19 : Squid Vekil Sunucu ayarları ekran görüntüsü

4.3 ERİŞİM TESTLERİ

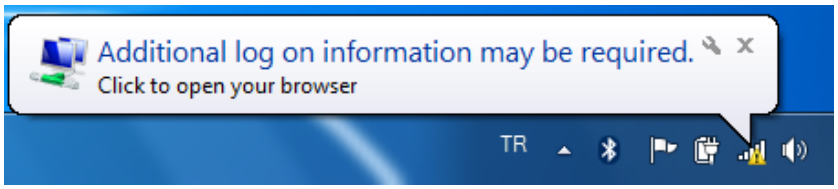
Ortam kurulumu tamamlandıktan sonra kablolu ve kablosuz erişim cihazları ile bağlantı sağlanmış ve internet erişim test edilmiştir.

Dizüstü bilgisayar ile kablosuz ağ bağlantısı yapılırken, kablosuz ağlar listesinde bulunan "İnternet" ağı seçilerek bağlantı sağlanmıştır.



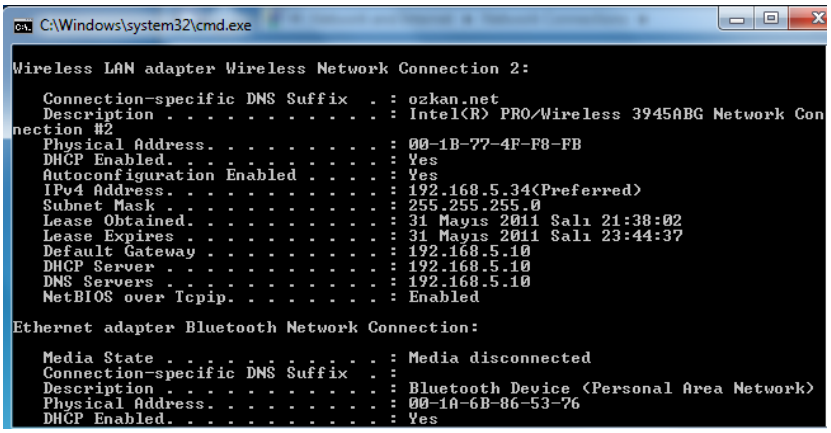
Şekil 4.20 : Kablosuz ağ bağlantısı ekran görüntüsü

Bağlantı sağlandıktan sonra işletim sisteminde ağ bağlantı ikonunun bulunduğu sağ alt köşede "Ek olarak giriş bilgileri gerekebilir. Tarayıcınızı açmak için tıklayın uyarısı" görüntülenmiştir.



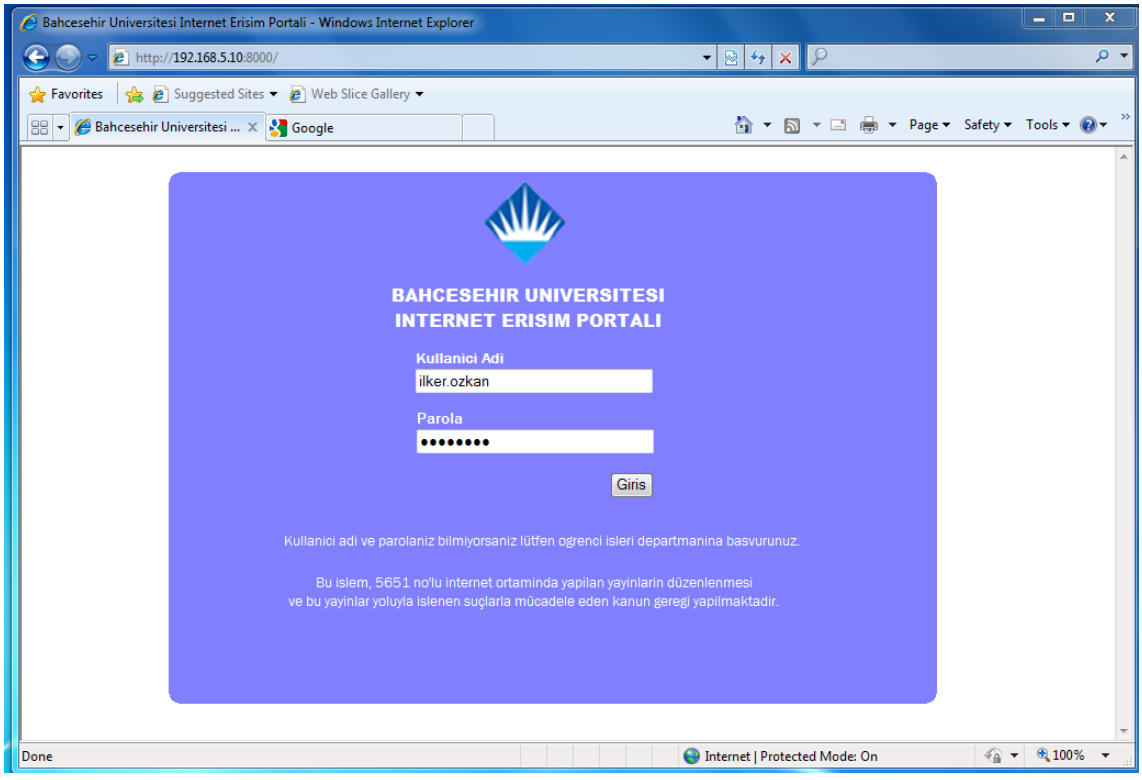
Şekil 4.21 : Kimlik denetimi uyarısı

Bu noktada kablosuz ağ kartı güvenlik duvarı üzerinden şekil 4.21'de görüldüğü gibi IP adresi, alt ağ maskesi ve DNS IP adresini almıştır . Fakat henüz kimlik doğrulaması yapılmamış olduğundan internet üzerinde herhangi bir yere erişemez.



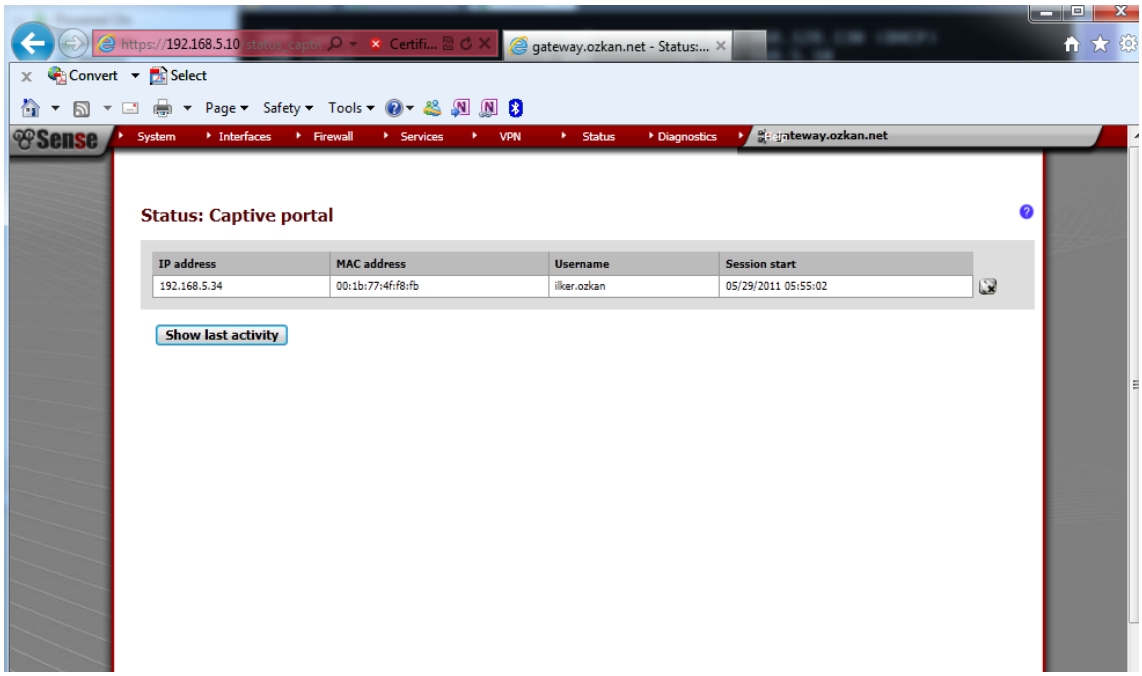
Şekil 4.22 : İstemci IP adresi ekran görüntüsü

Bu uyarıya tıklandığında ya da tarayıcı açılıp herhangi bir internet sayfasına girilmeye çalışıldığında güvenlik duvarında ayarlanmış olan kimlik doğrulama ekranı görüntülenir. Active directory dizin hizmetleri sunucusunda tanımlanmış kullanıcı adı ve parola ile giriş yapıldığında, güvenlik duvarı bu bilgileri RADIUS sunucu üzerinden sorgulayarak doğruluğunu denetler. Kimlik doğrulama başarılı olmuşsa internet erişimi güvenlik duvarında belirtilen kurallar çerçevesinde başlatılmış olur. Başarısız olursa hata uyarısı verir. Bu noktada, dizin hizmetleri sunucusunda oluşturulmuş kullanıcı hesapları için politika tanımlayarak, arka arkaya yapılmış oturum girişimlerinin olması durumunda, kullanıcı hesabının belirli bir süreliğine ya da sistem yöneticisi tarafından kilit kaldırılmadığı sürece sürekli olarak erişime kapalı olması sağlanabilir. Bu şekilde ayarlanmış bir sistemde hesap ele geçirme ataklarına karşı güvenlik önlemi alınmış olur.



Şekil 4.23 : İnternet Erişim Portali

Aşağıda şekil 4.24'te görüldüğü gibi Güvenlik duvarında, status bölümünde kullanıcının başarılı şekilde kimlik doğrulaması yaptığı ve oturumun başladığı görülmektedir.



Şekil 4.24 : Kullanıcı aktiviteleri durumu ekran görüntüsü

5. SONUÇ

Günümüzde internet işimizin ve sosyal yaşamımızın önemli bir parçası haline gelmiştir. Taşınabilir cihazların yeteneklerini arttırması ile birlikte bilgiye her yerden ulaşabilmek insanların vazgeçilmezi olmuştur. Bilgi akışının böylesine hızlı geliştiği günümüzde internet, firmaların iş yapış şekillerini değiştirerek daha hızlı ve rekabetçi olmalarını sağlamaktadır.

Her yerden bilgiye erişimin kolaylaşması beraberinde bir takım güvenlik risklerini içermektedir. Ayrıca internet erişimi hizmetini ücretli ya da ücretsiz olarak sunan tüm firma ve kuruluşların bilgi sistemleri yöneticileri güvenlik şartlarını sağlamanın yansıra yasal birtakım mevzuatlar nedeniyle erişimin denetlenmesi, içeriğin filtrelenmesi, yapılan erişimlerin kayıt altına alınması gibi bir takım sorunlarla uğraşmak zorunda kalmışlardır.

Ülkemizde 2007 yılında kanunlaşmış ve bu tezin ekinde de verilen, 5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanun erişim denetimini kesin olarak ifade etmektedir.

Kurumsal ağlarda merkezi politikalar ile hem kablolu hem de kablosuz ağ bağlantıları için 802.1x erişim denetimi yapmak, kimlik doğrulamada en sağlıklı çözümdür. Fakat Her ne kadar 802.1x ile erişim kimlik denetimi güvenli bir yol olarak kabul edilse de internete her yerden erişim talebinin karşılanması için hızlı ve kolay erişim metotları kullanılmak zorundadır. Kurumlar ağ yapılarını fiziksel ya da VLAN gibi teknolojilerle segmente ederek riskleri azaltmalıdırlar. Misafir ya da çalışanların kendi cihazlarıyla erişim yapılan yerlerde yerel ağdan yalıtılmış ağ segmentleri oluşturmak ve bunların kimlik denetimini tarayıcı üzerinden gerçekleştirmek, kurum internet erişiminde kabul edilebilir kullanım politikasını (Acceptable usage policy) hakkında kullanıcıya bilgi iletmek noktasında önemli olmaktadır.

KAYNAKÇA

1. GEIER, Jim, 2008, e-kitap, *Implementing 802.1x Security Solutions for Wired and Wireless Networks*

2. Hewlet-Packard Company, 2008, e-kitap, *How to configure 802.1X authentication on ProCurve Switches*

3. IEEE Standarts Association, 2004, http://standards.ieee.org/getieee802 [ziyaret Tarihi: Nisan 2011]

4. Cisco Systems Documentation, Internetworking technology handbook, http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook [ziyaret Tarihi: Aralık 2010]

5. ULAKBIM, II.ULAKNET Çalıştay ve Eğitimi, 2008, Çalışma grubu raporları http://www.ulakbim.gov.tr/ulaknet/calistay/08/ [ziyaret tarihi: Ocak 2011]

6. Manchester Universitesi kablosuz ağ erişim prosedürü, http://www.south.manchester.ac.uk/itservices/wireless.asp [ziyaret tarihi: Aralık 2010]

7. Australian National University kablosuz erişim prosedürü http://wireless.anu.edu.au/anuaccess.php [ziyaret tarihi: Şubat 2011]

8. Wikipedia, http://en.wikipedia.org/wiki/Captive_portal [ziyaret tarihi: Mart 2011]

9. WiFi Alliance http://www.wi-fi.org/ [ziyaret tarihi: Aralık 2010]

10. RFC2865, Radius, http://www.ietf.org/rfc/rfc2865.txt [ziyaret tarihi: Aralık 2010]

11. PfSense dökümantasyon, http://www.pfsense.org/index.php?option=com_content&task=view&id=50&Itemid=78 [ziyaret tarihi: Aralık 2010]

12. Telekomünikasyon İletişim Başkanlığı – TİB, http://www.tib.gov.tr [ziyaret tarihi: Kasım 2010]

EKLER

EK 1.

İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUN

Kanun No. 5651 **Kabul Tarihi : 4/5/2007**

Amaç ve kapsam

MADDE 1- (1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.

Tanımlar

MADDE 2- (1) Bu Kanunun uygulamasında;

a) Bakanlık: Ulaştırma Bakanlığını,

b) Başkanlık: Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığını,

c) Başkan: Telekomünikasyon İletişim Başkanını,

ç) Bilgi: Verilerin anlam kazanmış biçimini,

d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

g) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

ğ) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

h) İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

ı) Kurum: Telekomünikasyon Kurumunu,

i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

j) Trafik bilgisi: İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri,

k) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

l) Yayın: İnternet ortamında yapılan yayını,

m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,

ifade eder.

Bilgilendirme yükümlülüğü

MADDE 3- (1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

(2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından ikibin Yeni Türk Lirasından onbin Yeni Türk Lirasına kadar idarî para cezası verilir.

İçerik sağlayıcının sorumluluğu

MADDE 4- (1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

(2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

Yer sağlayıcının yükümlülükleri

MADDE 5- (1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi halinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür.

Erişim sağlayıcının yükümlülükleri

MADDE 6- (1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle,

yükümlüdür.

(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

(3) Birinci fıkranın (b) ve (c) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir.

Toplu kullanım sağlayıcıların yükümlülükleri

MADDE 7- (1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.

(2) Ticarî amaçla olup olmadığına bakılmaksızın bütün toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlüdür.

(3) Birinci fıkrada belirtilen yükümlülüğe aykırı hareket eden kişiye mahallî mülkî amir tarafından üçbin Yeni Türk Lirasından onbeşbin Yeni Türk Lirasına kadar idarî para cezası verilir.

Erişimin engellenmesi kararı ve yerine getirilmesi

MADDE 8- (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir.

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.

(5) Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir.

(6) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneğini Başkanlığa gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneği Başkanlığa gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(11) İdarî tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

İçeriğin yayından çıkarılması ve cevap hakkı

MADDE 9- (1) İçerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabı bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. İçerik veya yer sağlayıcı kendisine ulaştığı tarihten itibaren iki gün içinde, talebi yerine getirir. Bu süre zarfında talep yerine getirilmediği takdirde reddedilmiş sayılır.

(2) Talebin reddedilmiş sayılması halinde, kişi onbeş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir. Sulh ceza hâkimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hâkiminin kararına karşı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(3) Sulh ceza hâkiminin kesinleşen kararının, birinci fıkraya göre yapılan başvuruyu yerine getirmeyen içerik veya yer sağlayıcısına tebliğinden itibaren iki gün içinde içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına başlanır.

(4) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, bu fıkra hükmü yayın sorumlusu hakkında uygulanır.

İdarî yapı ve görevler

MADDE 10- (1) Kanunla verilen görevler, Kurum bünyesinde bulunan Başkanlıkça yerine getirilir.

(2) Bu Kanunla ekli listedeki kadrolar ihdas edilerek Başkanlığın hizmetlerinde kullanılmak üzere 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununa ekli (II) sayılı listeye eklenmiştir. Başkanlık bünyesindeki iletişim uzmanlarına, Kurumda çalışan Telekomünikasyon Uzmanlarına uygulanan malî, sosyal hak ve yardımlara ilişkin hükümler uygulanır. İletişim Uzmanı olarak Başkanlığa atanan personelin hakları saklı kalmak kaydıyla, kariyer sistemi, Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde çıkarılacak yönetmelikle düzenlenir.

(3) Başkanlığa Kanunla verilen görevlere ilişkin olarak yapılacak her türlü mal veya hizmet alımları, ceza ve ihalelerden yasaklama işleri hariç, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu ile 5/1/2002 tarihli ve 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(4) Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Başkanlığın bu Kanun kapsamındaki görev ve yetkileri şunlardır:

a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dahilinde Kurumca karşılanacak çalıma kurulları oluşturmak.

b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen gerekli tedbirleri almak.

c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.

ç) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek.

d) İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.

e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek.

f) Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.

g) Bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

(5) Başkanlık; Bakanlık tarafından 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanunun ek 1 inci maddesi uyarınca, Adalet Bakanlığı, İçişleri Bakanlığı, çocuk, kadın ve aileden sorumlu Devlet Bakanlığı ile Kurum ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile internet servis sağlayıcıları ve ilgili sivil toplum kuruluşları arasından seçilecek bir temsilcinin katılımı suretiyle teşkil edilecek İnternet Kurulu ile gerekli işbirliği ve koordinasyonu sağlar; bu Kurulca izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır.

Yönetmelikler

MADDE 11- (1) Bu Kanunun uygulanmasına ilişkin esas ve usûller, Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşleri alınarak Başbakanlık tarafından çıkarılacak yönetmeliklerle düzenlenir. Bu yönetmelikler, Kanunun yürürlüğe girdiği tarihten itibaren

dört ay içinde çıkarılır.

(2) Yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine ilişkin esas ve usûller, Kurum tarafından çıkarılacak yönetmelikle düzenlenir. Bu yönetmelik, Kanunun yürürlüğe girdiği tarihten itibaren beş ay içinde çıkarılır.

İlgili kanunlarda yapılan değişiklikler

MADDE 12- (1) 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanununun 2 nci maddesinin (f) bendine aşağıdaki cümle eklenmiştir.

"Bu idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir."

(2) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7 nci maddesinin onuncu fıkrasının birinci cümlesinde yer alan "belirtilen" ibaresinden sonra gelmek üzere "telekomünikasyon yoluyla yapılan iletişime ilişkin" ibaresi eklenmiş, ikinci cümlesi "Oluşturulan bu Başkanlık bir başkan ile daire başkanlıklarından oluşur." şeklinde değiştirilmiştir.

(3) 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununun 5 inci maddesine aşağıdaki fıkra eklenmiştir.

"Kurulca belirlenecek esas ve usûller çerçevesinde, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanununun 22 nci maddesinde belirtilen doğrudan temin usûlüyle serbest avukatlar veya avukatlık ortaklıklarıyla avukat sözleşmeleri akdedilebilir."

(4) 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesinin ikinci fıkrasının son cümlesi "4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesinin altıncı fıkrasının (a) bendinin (14) numaralı alt bendi kapsamında yapılacak dinlemeler de bu merkez üzerinden yapılır." şeklinde değiştirilmiş; dördüncü fıkrasında yer alan "Ancak" ibaresinden sonra gelmek üzere "casusluk faaliyetlerinin tespiti ve" ibaresi eklenmiş; altıncı fıkrasının üçüncü cümlesinde geçen "Bu madde" ibaresi "Bu fıkra" olarak değiştirilmiştir.

GEÇİCİ MADDE 1- (1) Başkanlığın kuruluştaki hizmet binasının yapımı, ceza ve ihalelerden yasaklama işleri hariç, Kamu İhale Kanunu ve Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(2) Halen faaliyet icra eden ticarî amaçla toplu kullanım sağlayıcılar, bu Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde 7 nci maddeye göre alınması gereken izin belgesini temin etmekle yükümlüdürler.

(3) Halen yer veya erişim sağlayıcı olarak faaliyet icra eden kişilere, Kurum tarafından, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla bir yetkilendirme belgesi düzenlenir.

Yürürlük

MADDE 13- (1) Bu Kanunun;

a) 3 üncü ve 8 inci maddeleri, yayımı tarihinden altı ay sonra,

b) Diğer maddeleri yayımı tarihinde,

yürürlüğe girer.

Yürütme

MADDE 14- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

ÖZGEÇMİŞ

20 Temmuz 1977 Hatay - İskenderun doğumludur. İlk, Orta ve Teknik Lise Bilgisayar bölümü eğitimlerini Gaziantep'te tamamlamıştır. 1997-1999 yılları arasında Marmara Üniversitesi Bilgisayar Programcılığı Bölümü okumuş, sonrasında Anadolu Üniversitesi İşletme Fakültesini bitirmiştir. 2002 tarihinden beri bankacılık sektöründe Bilgi Teknolojileri Bölümü Ağ ve Sistem Uzmanı olarak çalışmaktadır.