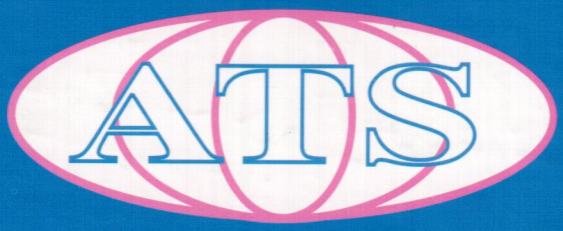
4. ULUSLARARASI İLERİ TEKNOLOJİLER SEMPOZYUMU



4th INTERNATIONAL ADVANCED TECHNOLOGIES SYMPOSIUM

Eylül/ September 28-30, 2005

SELÇUK ÜNİVERSİTESİ

KONYA / TÜRKİYE

TÜBİTAK TÜBİTAK'ın katkılarıyla hazırlanmıştır.

4th International Advanced Technologies Symposium
September 28–30, 2005 Konya / Türkiye

KAMPÜS AĞLARINDA İSTENMEYEN TRAFİĞİN ÖNLENMESİ VE SİSTEM PERFORMANSININ ARTTIRILMASI

Meriç ÇETİN [1] Süleyman ALTAN [2] Murat AYDOS [3]

[1)] Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü, Kampüs-Denizli TR mcetin@pamukkale.edu.tr

[2)] Samur Bilgisayar San. Tic. Ltd. Şti., Denizli TR saltan@samur.net

[3)] Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü, Kampüs-Denizli TR maydos@pamukkale.edu.tr

ÖZET

Günümüzde ağların mevcut yapılarındaki büyümelerden dolayı ekipman yönetimi ve kontrolü güçleşmektedir. Bununla birlikte, genişleyen ağlardaki performans, bilgilere ulaşılabilirlik gibi kriterlerin yanında mevcut ağ üzerinde çalıştırılan uygulamaların güvenlik politikaları da önem kazanmaktadır. Güvenlik politikaları sayesinde daha sağlıklı hale gelen bağlantılar; sunuculara erişimin yetkilendirilmesi ve yerel ağların internetten soyutlanması nedeniyle karşılaşılacak problemler ile virüs, solucan, truva atı gibi birçok etkenin sebep olduğu istenmeyen trafiğe maruz kalıp kesintiye uğrayabilir. Bu yüzden, güvenlik politikaları oluşturulurken sadece dış ağlardan gelecek saldırılar değil, sunucuların dış ağlara karşı güvenliği ile yerel ağ kullanıcılarına karşı güvenliği de düşünülmeli ve ağ trafiğinin kontrollü olması amacı gözetilmelidir. Bu çalışmada; küçük ya da orta ölçekli olarak düşünülebilecek bir ağ üzerindeki güvenlik duvarı ardında kalan kullanıcıların oluşturduğu bir yerel ağ ve kullanıcılardan farklı olarak silahsızlandırılmış bölge tarafına kurulmuş sunucuların bulunduğu varsayılan bir yapı üzerindeki istenmeyen trafiği engellemek adına oluşturulabilecek sistem konfigürasyonları ele alınmıştır. Uygulama açısından uzak noktalarda da birimlerinin olduğu daha geniş bir ağ yapısı düşünülmüş, geniş ağlarda, uzak erişimlerdeki ağ performansının istenilen düzeyde olabilmesi için güvenlik duvarı üzerindeki erişim listelerinde belirtilen kuralların kısmen uzak noktalara doğru kaydırılabileceği görülmüştür. Çalışma sonucunda; güvenlik duvarında belirtilen kurallarla belli noktalardaki trafikler gözlenerek ağ trafiğinin kontrolü, istenmeyen trafiğin önlenmesi, sunucu güvenliği ve ağ performansı açısından elde edilen verilerin analizi neticesinde oluşturulan yapılandırmalarla sistem performansı arttırılmıştır.

Anahtar Kelimeler: Kampüs Ağları, İstenmeyen Trafik, Erişim Listeleri, Sistem Performansının Arttırılması, Güvenlik Politikaları

GİRİŞ

Bilgisayar ağları; ağ üzerinde bulunan kullanıcıların bilgiye kolay ulaşmasını, dolayısıyla bu kullanıcıların çalışmalarındaki verimin artmasını ve zaman tasarrufunu sağlayan sistemlerdir. Ağ üzerindeki bilgilere kolay ulaşım için sunulan hizmetler, aynı zamanda ağa zarar verebilme riskini de taşımaktadır. Bilgisayar ağlarının sunduğu imkanlardan faydalanırken maruz kalınabilecek tehlikeleri en aza indirmek için bir takım tedbirler almak gerekir. Güvenliği ön plana çıkaran bu tedbirlerin avantajlarının yanında, sistem hızını aynı oranda azaltmak gibi dezavantajları da vardır.

Internetin doğuşu ve gelişimi arasında çok kısa bir zaman aralığı vardır. Özellikle büyük yatırımlar yapılarak geliştirilen internet teknolojisi, 1985 yılından sonra hızla yaygınlaşmıştır. Bu hızlı gelişim sürecinde birtakım konular için standartların tam oluşturulmadan kullanıma geçirilmesinden dolayı güvenlik problemleri gibi bazı sorunlar ortaya çıkmıştır. Güvenlik, her bilgisayar ağında olduğu gibi internet ortamında da öncelikli olarak düşünülmesi gereken bir konudur. Birçok ticari firma ya da kuruluş, ürünlerini ve hizmetlerini internet ortamına aktarmak suretiyle kullanıcılarına ulaşmak istemektedir. Ancak bu işlemler birtakım riskleri de beraberinde getirmektedir. Değişik güvenlik mekanizmalarının bir arada kullanılmasıyla, bu riski azaltmak mümkündür [1].

Bu güvenlik mekanizmalarını anlatmadan önce güvenlik konusunun neden gerekli olduğunun anlaşılması, sistem üzerinde güvenliği artırmak için yapılacak çalışmaların önemini anlamakda faydalı olacaktır.

GÜVENLİK BİLİNCİ

İnternet üzerinde bir noktadan başka bir noktaya ilerleyen hiçbir verinin ya da internete bağlı bir ağın, gerekli önlemler alınmadığı takdirde güvenli olduğu söylenemez. Ağ güvenliği konusunda kurumların yerel ya da geniş alan ağ topolojileri incelenerek sistem üzerindeki zayıflıkları ve güvenlik delikleri tespit edilebilir ve en üst düzeyde güvenliğin sağlanması için ağ topolojisi tekrar yapılandırılabilir.

Güvenlik yönetiminin amacı; ağ kaynaklarına erişimi kontrol etmek, ağa içeriden veya dışarıdan yapılması

muhtemel saldırıları engellemek ve önemli bilgilere yalnızca izin verildiği ölçüde, izin verilen kullanıcıların erişimini sağlamaktır.

Birçok kuruluş tarafından sağlanan birtakım hizmetlerin internet üzerinden kullanıcılarına ulaştırılması ve bu kullanılan teknolojilerin getirdiği yenilikler son derece önemlidir. Ancak açık ve güvensiz bir ağ olan internete bağlantı, bazı güvenlik sorunlarını da beraberinde getirmektedir. Bunlar; ağ dışındaki ortamlardan ağ içine yapılabilecek saldırılar, yerel ağda bulunan yetkisiz kişilerin dışarıya bilgi göndermesi, internet üzerindeki virüs, solucan, truva atı gibi programların kendi ağ ortamımıza bulaşması, yetkisiz kullanıcıların internet ortamında gezinmesi gibi birçok problem kampüs ağları ve yerel ağlar için birer tehlike unsuru oluşturmakta ve kullanıcıya istenmeyen trafikler olarak yansımaktadır [2], [3].

Tüm bu sebepler sistemdeki güvenlik açıklarını oluşturmaktadır. Bu güvenlik açıklarını kullanarak sisteme saldırmak isteyen kişi, normal ağ trafiğinde ağın en zayıf noktalarından saldırıyı gerçekleştirir. Bu saldırı veya hatalardan korunmak için, mevcut ağ üzerinde çalıştırılan uygulamalarda birtakım güvenlik politikaları oluşturulmalıdır.

GÜVENLİK POLİTİKALARI VE SALDIRI KAVRAMI

Mevcut veriler ve Internet ile birlikte kurumların hayatına giren farklı iş modellerinde oluşturulan bilgilerin güvenliğinin sağlanması, kurumlar açısından üzerinde ciddi şekilde düşünülmesi gereken bir konu haline dönüşmüştür. Güvenlik politikaları, farklı tiplerdeki bilgilere erişim için kişilere yetkiler vermenin yanısıra kuralların farklı ve yanlış anlaşılmasını önlemek, ilgilileri eğitmek, muhtemel sorunları önceden tespit etmek, kriz durumlarında hızlı hareket edebilmek gibi konularda da faydalar sağlar. Ayrıca, güvenlik zorunluluğu ölçütlerine bakarak da kuralları ve standartları belirler. Sağlıklı ve yaşayan bir güvenlik politikası, muhtemel saldırıların önceden belirlenmesi ve gerçekleşen saldırılara karşı, etkin önlem alınması konusunda yol gösterici bir hareket planı olarak kullanılabilir. Bu ihtiyaçlar doğrultusunda kurumlar, güvenlik politikalarını oluştururken sadece dış ağlardan gelecek saldırıları değil, mevcut çalışan içerideki ağ politikalarını da doğru konumlandırmak zorundadırlar. Yönetilen bu güvenlik politikaları ile kurumlar sadece internet üzerinden gelecek tehlikelere karşı değil, firma içinde oluşacak güvenlik tehditlerine karşı da kendilerini koruma altına almış olurlar [4].

Güvenlik politikalarının izlenebilir olması sayesinde, kurum genelindeki tüm kullanıcılar, dış ağlardan iç ağlara yapılan erişimler ve saldırılar sürekli izlenerek kurumun sahip olduğu teknoloji ve bilgi değerlerinin nasıl en iyi şekilde kullanılması gerektiği belirlenir. Güvenlik politikalarında tanımlanan iletişim kuralları ile ağa ve kaynaklara erişim, tüm giriş-çıkış noktalarında kontrol edilerek saldırılardan korunma sağlanır. Yönlendirici (router), anahtar (switch) veya yalnızca bu amaç için tasarlanmış güvenlik duvarı (firewall) çözümleri sadece izin verilen kullanıcıların ağı kullanmasını ve sadece izin verilen veri trafiğinin ağ üzerinden geçmesini sağlar.

Güvenlik duvarı; iki ağ arasında erişim kontrolü politikasını uygulayan, ağları izinsiz erişim ve saldırılardan korumak için onlara erişim seviyeleri sağlayan sistem veya sistemler grubuna verilen addır. Güvenlik duvarı, ağ erişim politikasının oluşturulmasını ve güçlendirilmesini sağlar. Kullanıcılara ve servislere erişim kontrolü imkanı verilmesiyle, güvenliğin sadece kullanıcılara bağlı olması yerine güvenlik duvarı ile güçlendirilmiş bir ağ erişim politikasının belirlenmesi de sağlanır. Sistem yöneticisi (administrator) tarafından belirlenen güvenlik politikası tabanında güvenlik duvarından geçişler ya yasaklanır ya da serbest bırakılır. Güvenlik duvarı bütün iletişim girişimlerindeki kimlik bilgilerini denetler ve var olan geçerli politika ile karşılaştırır. İletiyi kabul etme ya da reddetme kararı sistem yöneticisi tarafından belirlenmiş erişim listelerindeki (access lists) kurallar doğrultusunda işleme alınır ve daha sonra incelenmek üzere saklanır. [5]

Yönetimsel ihtiyaçlar, performans izlenmesi, süreklilik ve band genişliğinin en iyi şekilde kullanılması gibi konular kampüs ve geniş alan ağ cihazlarının doğru yönetiminde servis kalitesini sağlamak ve devam ettirmek için çok önemli bir duruma gelmiştir. Bu ihtiyaçlar doğrultusunda kurumlar güvenlik politikalarını oluştururken yazılımsal veya donanımsal güvenlik duvarlarına ihtiyaç duymaktadırlar. Ancak, bu problemlerin çözümünde bir tek güvenlik duvarı kullanmak veya internete bağlanmak için ağ geçidi sayısını arttırmak mevcut sistemin güvenliğini yeterli düzeyde sağlayamamaktadır. Bu durumda karmaşık kampüs ağları ve yerel alan ağlarında ek yazılım ve ekipmanları içeren yönetimsel araçlara gereksinim duyulmaktadır [6].

İnternet bağlantısı, dışardan gelecek saldırılar için bir kanal oluşturduğundan dolayı çok iyi korunmalıdır. Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, maddi/manevi kazanç sağlamak amacıyla onlara zarar vermek için bilişim sistemleri kullanılarak yapılan her türlü hareket, bilgisayar ağlarında saldırı olarak tanımlanabilir. İnternet bağlantı noktalarından geçen trafiğin düzenli olarak izlenmesi, saldırıların belirlenmesini ve onlara karşı önlem alınmasını kolaylaştırır [7].

Saldırganlar sisteme ağ üzerinden ulaşabilecekleri için, ağa bağlı cihazlar her zaman saldırıya maruz kalırlar. Burada saldırganın amacı; hedef makineye ulaşmak, yazılım ve donanıma zarar vermek şeklinde olabilir. Kuruma ait veritabanına ulaşıp verilere erişebilir, onları değiştirebilir ya da silebilirler. Verilen hizmetleri servis dışı bırakabilirler veya sadece internet bağlantısına zarar verebilirler. Truva Atı türünde programları bir şekilde hedef makineye yükleyerek kullanıcıyı takip edebilir ve girdiği sistemi tüm dünyaya açabilirler. Bir sistemdeki açık ve kullanılan portları tarayarak bu portlardan hizmetlere yönelik saldırılar gerçekleştirebilirler. Uzaktan erişim protokolünün açıklarından faydalanarak uzak erişim servislerine yönelik saldırılar yapabilirler. IP adres yanıltmasını kullanarak

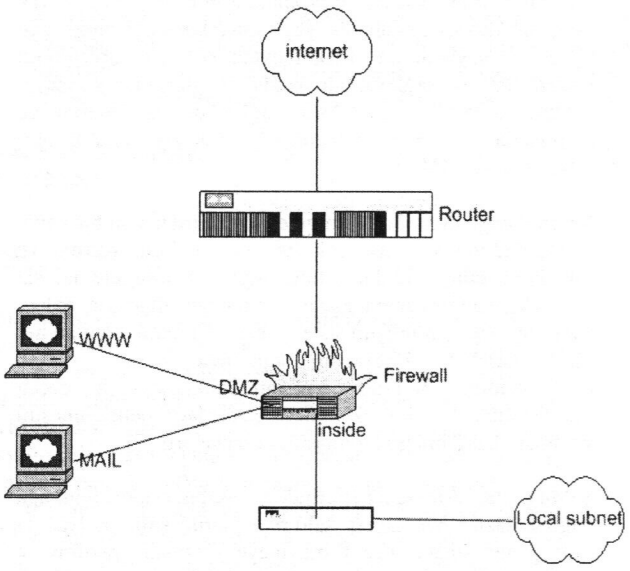
sistemdeki bir kullanıcının erişim haklarına sahip olabilirler.

YAPILAN ÇALIŞMA

Saldırı kavramı ve güvenlik politikaları anlatılırken internet ortamının güvensizliğinden, ağ dışından veya ağ içinden kaynaklanabilecek saldırılardan, güvenli olmayan servislerden ve bunların sisteme getirdiği olumsuz etkilerden bahsedilmiştir. Tüm bu sebeplerin oluşturduğu istenmeyen trafikler, bağlantılarda kesintilere sebep olmakta ve sistemin işleyişini aksatmaktadır.

Bahsedilen problemlerin çözümlerine yönelik olarak yapılan ilk uygulamada; öncelikle küçük ya da orta ölçekli olarak düşünebilecek bir ağdaki güvenlik duvarının ardında kalan, kullanıcıların oluşturduğu bir yerel ağda (inside) ve farklı olarak DMZ (**De**M**i**litarized **Z**one- silahsızlandırılmış bölge) tarafına kurulmuş sunucuların bulunduğu varsayılan bir yapı üzerindeki istenmeyen trafiği engellemek adına oluşturulabilecek sistem konfigürasyonları ele alınmıştır.

Uygulamalarda kullanılan güvenlik duvarı cihazı Cisco PIX serisi bir cihaz olduğu için uygulama örneği olarak komutlarda, tamamen bu cihaza özgü komutların kullanıldığı göz önüne alınmalıdır.



Şekil 1. Sadece yerel alan ağı içeren yapı

Şekil 1'de gösterilen ilk uygulamada, local subnet olarak ifade edilen tek bir yerel ağdan oluşan küçük bir yapı görülmektedir. Bu yerel ağda bulunan 25 bilgisayar için IP adreslerinin yapılandırması aşağıda ifade edildiği gibidir:

Yerel ağda bulunan 25 PC için IP yapılandırması:

Network : 192.168.1.0 / 26
Subnet ID : 192.168.1.0
Broadcast : 192.168.1.63
Kullanılacak IP aralığı: 192.168.1.1-192.168.1.62

Uygulamada güvenlik duvarı üzerinde iki farklı bölge oluşturulmuştur. Birinci bölgede; kullanıcılar yani yerel ağ (192.168.1.0/26) yer almakta, diğer bölgede ise; DMZ sunucular (10.1.1.0/29) yani web ve mail sunucuları yer almaktadır. DMZ tarafındaki ağın ve sunucuların IP yapılandırması aşağıda ifade edildiği gibidir:

DMZ tarafındaki sunucular için IP yapılandırması:

Network : 10.1.1.0 / 29
Subnet ID : 10.1.1.0
Broadcast : 10.1.1.7
Kullanılacak IP aralığı : 10.1.1.1-10.1.1.6

Stratejik önem taşıyan sunucuların mutlaka DMZ bölümüne aktarılması ve güvenlik duvarı üzerinden yerel ağ ve internet ile iletişimi gerekli olanların dışındakilerin iletişimlerinin kesilmesi gerekir. Mail ve web sunucularının DMZ bölgesi içinde olmasının avantajları vardır. Mail sunucusunun bu bölgede yer alması, kurum çalışanların e-maillerini mail sunucusu aracılığıyla almasına, tüm e-maillerin kontrol edilebilmesine, virüs taramasından geçirilebilmesine olanak tanır ve böylece yalıtılmış bir ortam sağlanmış olur. Web sunucusunun bu bölgede yer alması ise, HTTP ve FTP isteklerinin filtrelenmesine, ağ üzerindeki kullanıcıların sadece o sistemden sayfaları çağırabilmelerine ve dış ortama sadece o sistemin çıkabilmesine olanak sağlar. Böylece HTTP ve FTP isteklerinin tek bir sistemde toplanması ve o sisteme sadece içeriden dışarıya çıkış izni verilmesiyle birçok saldırı engellenmiş olur.

Güvenlik politikası oluşturulurken dikkat edilmesi gereken temel noktalardan birisi de, hangi DMZ bölgesine sadece hangi protokol ve port bağlantı geçişi izninin verileceğidir. Başta güvenlik duvarları olmak üzere ilgili cihazlar üzerinde uygun konfigürasyonlar, bunun paralelinde yapılır.

Aşağıdaki komut satırlarında yerel ağ üzerindeki bilgisayarların dışarıya doğru erişim trafiği için güvenlik duvarı üzerinde yapılacak düzenlemeler görülmektedir. Sunuculara erişimlerin yanısıra, yerel ağ kullanıcılarının internete ve DMZ'ye doğru gerçekleştireceği ağ trafiklerinin hangi uygulamalar olabileceğini belirleyecek ve buna göre gönderilen paketleri geçirecek ya da kısıtlayacak olan tanımlamaların yapılması da gerekmektedir.

Bu çalışmada gerçekleştirilen örnek konfigürasyonlardaki 80 numaralı port web, 21 numaralı port ftp, 25 numaralı port mail, 110 numaralı port POP3 ve 143 numaralı port IMAP uygulamalarının port numaralarını göstermektedir.

outbound 1 deny 0.0.0.0 0.0.0.0 0 ip
outbound 1 permit 192.168.1.0 255.255.255.224 80 tcp
outbound 1 permit 192.168.1.0 255.255.255.224 21 tcp
outbound 1 permit 192.168.1.0 255.255.255.224 25 tcp
outbound 1 permit 192.168.1.0 255.255.255.224 110 tcp
outbound 1 permit 192.168.1.0 255.255.255.224 143 tcp

Yukarıdaki konfigürasyon satırlarında belirlenen kurallara göre yerel ağ grubundaki tüm kullanıcılara ilk adımda tüm erişimler yasaklanır, ardından sırasıyla her satırda belirtilen port ve protokoller bazında erişim yetkileri verilir. Böylece yerel ağdan internete ve DMZ'ye doğru ilerleyen trafik tamamen kontrol altına alınmış olur ve sadece belirlenen uygulamaları çalıştırabilecek şekilde trafik akışı gerçekleştirilir. Kullanıcılar bu kısıtlamalar veya kurallar doğrultusunda internet üzerinde ve sunucular üzerinde uygulama çalıştırabilirler.

Güvenlik duvarı üzerinde yapılan düzenlemelerde amaç; hem internet üzerinden gelen paketlere karşı sunucuların ve yerel ağ kullanıcılarının güvenliğini sağlamak hem de yerel ağ kullanıcılarına karşı sunucuların güvenliğini sağlamaktır. Aynı zamanda güvenlik duvarı üzerinde, erişim listelerinde belirlenen kurallarla, kullanıcıların gerek internete doğru gerekse sunuculara doğru giden trafiğinin ve sunuculardan internete doğru olan trafiğin kontrol altında tutulması sağlanır.

DMZ bölgesinde bulunan web ve mail sunucuları için dışarıdan erişim yetkilendirmeleri amacıyla güvenlik duvarı üzerinde aşağıdaki konfigürasyon komut satırları yazılmıştır.

Mail ve web sunucusu için güvenlik duvarı üzerinde yapılan düzenlemeler:

1. *static (DMZ, outside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0* (mail sunucusu için)

2. *static (DMZ, outside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0* (web sunucusu için)

Yukarıdaki konfigürasyon satırlarında, sanal IP adreslerine sahip DMZ tarafındaki web ve mail sunucularının dışarıdan erişime açık olabilmeleri için Cisco PIX serisi güvenlik duvarında kullanılan "*static*" ifadesi ile NAT (Network Address Translation) tanımları yapılmıştır. Adres çevrimi anlamına gelen NAT işlemi; birden fazla IP adresinin, bir IP adresi arkasına saklanarak tüm makinelerin internete çıkarılması için kullanılan mekanizmaya verilen isimdir. Bu sayede sahip olunan tek bir IP adresi ile yerel alanda bulunan çok sayıda bilgisayar internete çıkarılabilir. Bu konfigürasyonda mail ve web sunucularına ayrı ayrı gerçek IP adresleri tanımlanmıştır.

Sistemde yer alan farklı bölümler farklı ağları temsil ettiğinden, ağlar arasındaki iletişim, verilen yetkiler oranında gerçekleşmelidir. Bu ağlar güvenlik duvarı tarafından kontrol edilerek aralarında tam bir yalıtım sağlamalıdır. Böylece yetkisiz erişimlerden korunulmuş olunur. Sunucular üzerinde çalıştırılması gereken uygulamalara göre güvenlik duvarı üzerinde erişim yetkileri tanımlanmalıdır. IP adresi ve uygulama portu bazında yapılacak tanımlamalar ile hangi sunuculara, hangi IP adreslerinin, hangi uygulama portlarından erişim yetkilerine sahip olacağı belirlenecektir.

Yetkilendirme tanımları:

1. *conduit permit tcp host 240.18.186.2 eq 25 any*

(Bu komut satırı ile 240.18.186.2 gerçek IP adresi ile eşleşen mail sunucusu SMTP, tüm mail sunucularından gelen mailleri kabul edebilir hale gelir)

2. *conduit permit tcp host 240.18.186.2 eq 143 192.168.1.0 255.255.255.224*

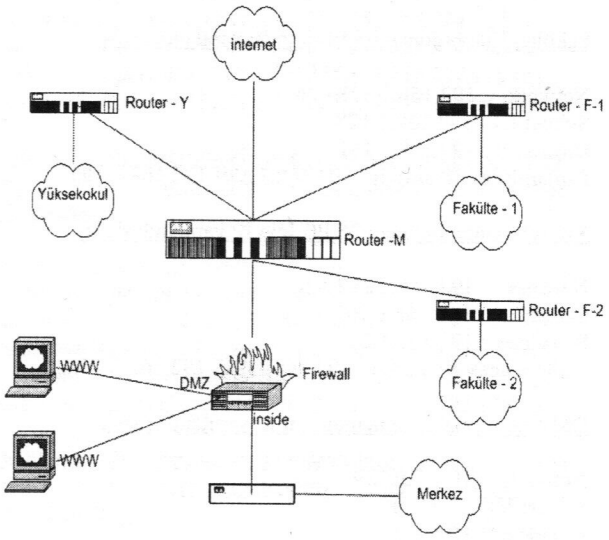
(IMAP protokolü mail sunucularına mail istemci programlarıyla erişebilmeyi sağlayan bir protokoldür. Bu komut satırı; sadece yerel ağ kullanıcılarının, mail sunucusuna bir mail programı ile bağlantı sağladığı durumlarda IMAP protokolünü kullanabilme yetkilerini veren komut satırıdır)

3. *conduit permit tcp host 240.18.186.2 eq 110 192.168.1.0 255.255.255.224*

(Bu komut satırı; sadece yerel ağ kullanıcılarının, mail istemci programlarının mail sunucusuna bağlanabilmesini, mail alıp gönderebilmesini sağlayan POP3 protokolünü kullanarak mail sunucusuna erişebilmelerini sağlayan komut satırıdır.)

4. *conduit permit tcp host 240.18.186.3 eq http any*

(Bu komut satırı ise; web sitesine herhangi bir istemciden ulaşılabilmesi kuralını belirleyen komut satırıdır.)



Şekil 2. Kampus ağı olarak düşünülebilecek, uzak alan ağlarını da içeren yapı

Güvenlik politikaları planlamasında, uygulamanın yapılacağı ağ genişledikçe güvenlik politikalarında da bir takım değişiklikler olmaktadır. Yapılan bu çalışmanın ikinci

kısmında; uygulama açısından uzak noktalarda da birimlerinin olduğu daha geniş bir ağ yapısı düşünülmüş ve bu noktalara olan bağlantının çeşitli bant genişliklerinde olduğu varsayılmıştır (şekil 2.). Bu uygulamadaki kuralları belirlemenin ve uygulamanın daha karmaşık bir hal almasının yanında, ilk uygulamada kullanılan kuralların bir kısmı bu yapı için de geçerliliğini korumuştur. Ancak geniş ağlarda, uzak erişimlerdeki ağ performansının istenilen düzeyde olabilmesi için bu kuralların kısmen uzak noktalara doğru kaydırılmasının gerekliliği ortaya çıkmıştır.

Yapılan ilk uygulamadan farklı olarak, merkezi yönlendiricinin üzerinde yapılandırılan kurallara geçmeden önce, bu uygulamadaki trafiklerin gözleneceği belirli noktaları içeren geniş alan ağının IP yapılandırmasının gerçekleştirilmesi gerekir. Şekil 2'de gösterilen ikinci uygulamada, sadece yerel ağ kullanıcıları değil, uzak alan ağları da bulunmaktadır. Öncelikle uygulamadaki geniş alan ağ sisteminde yer alan Merkez yerel ağı ile Fakülte-1, Fakülte-2 ve Yüksekokul uzak alan ağlarında bulunan 25'er adet bilgisayar ile DMZ tarafı sunucularının (web ve mail) IP yapılandırması gerçekleştirilir.

Merkez'de bulunan 25 PC için IP yapılandırması:

Network : 192.168.2.0 / 26
Subnet ID : 192.168.2.0
Broadcast : 192.168.2.63
Kullanılacak IP aralığı : 192.168.2.1-192.168.2.62

Fakülte-1'de bulunan 25 PC için IP yapılandırması:

Network : 192.168.1.64 / 26
Subnet ID : 192.168.1.64
Broadcast : 192.168.1.127
Kullanılacak IP aralığı : 192.168.1.65-192.168.1.126

Fakülte-2'de bulunan 25 PC için IP yapılandırması:

Network : 192.168.1.128 / 26
Subnet ID : 192.168.1.128
Broadcast : 192.168.1.191
Kullanılacak IP aralığı : 192.168.1.129-192.168.1.190

Yüksekokulda bulunan 25 PC için IP yapılandırması:

Network : 192.168.1.192 / 26
Subnet ID : 192.168.1.192
Broadcast : 192.168.1.255
Kullanılacak IP aralığı : 192.168.1.193-192.168.1.254

DMZ tarafındaki sunucular için IP yapılandırması:

Network : 10.1.1.0 / 29
Subnet ID : 10.1.1.0
Broadcast : 10.1.1.7
Kullanılacak IP aralığı : 10.1.1.1-10.1.1.6

Güvenlik duvarı üzerindeki IP yapılandırması:

outside: 240.18.186.2 /24
(Merkez yönlendiricinin ethernet0 portu ile bağlantı sağlayacak portun IP adresi)

inside : 192.168.2.1 /26
(Yerel ağ kullanıcılarının bağlanacağı portun IP adresi)

DMZ1: 10.1.1.1 /29
(Sunucuların bağlanacağı portun IP adresi)

DMZ2: 192.168.1.1 /24
(Merkez yönlendiricinin ethernet1 portuna bağlanacak portun IP adresi)

Bu uygulamada, yerel ağ kullanıcıları ile uzak alan ağ kullanıcılarının IP adres yapılandırmaları farklılaştırılmıştır. Çünkü uzak alan ağlardan gelecek olan veri paketleri, merkez yönlendiricinin ikinci ethernet portu üzerinden güvenlik duvarının DMZ2 ethernet portuna erişecek ve bu aradaki yapı tamamen VPN (Virtual Private Network-Özel Sanal Ağ) olacaktır. Dolayısıyla uzak alan ağ kullanıcıları, sanki güvenlik duvarının DMZ2 kısmında yer alıyormuş gibi davranacaklardır.

Geniş alan ağı içerisinde yer alan yerel ve uzak alan ağlarının IP yapılandırma işlemi tamamlandıktan sonra, bu ağların tamamının merkezdeki tek bir güvenlik duvarı üzerinde belirlenen kurallarla yetkilendirilmesi gerekmektedir. Bunun için yapının öncelikle yönlendiriciler üzerinde yazılan konfigürasyonlarla merkezileştirilmesi gerekir. Merkezdeki yönlendirici üzerinde tanımlanan aşağıdaki konfigürasyon satırları ile yapının tamamı merkeze VPN aracılığıyla bağlanır ve tüm yapı merkezdeki güvenlik duvarı ardında kalan herhangi bir ağ konumunda olur.

```
!
ip vrf A
rd 100:1
!
```
(MPLS aktif hale getirilir.)
```
!
interface FastEthernet0/0
ip vrf forwarding A
ip address 192.168.1.2 255.255.255.0
!
```
(Merkez yönlendirici ile güvenlik duvarı arasında, uzak alan ağlardan gelen paketler için tünelleme işlemi yapılır.)
```
!
interface FastEthernet0/1
 ip address 240.18.186.1 255.255.255.0
!
```
(Güvenlik duvarı ile bağlantı sağlayacak olan ethernet portu)
```
!
interface ATM1/0.1 point-to-point
description Internet_baglantisi
ip address 172.16.0.1 255.255.255.252
 pvc 0/1
protocol ip 172.16.0.2 broadcast
 encapsulation aal5snap
!
```

(Merkez yönlendirici ile internet servis sağlayıcısında bulunan yönlendirici arasındaki DLCI numarası 1 olan Frame Relay bağlantısını gösteren konfigürasyon satırıdır.)

```
!
interface ATM1/0.2 point-to-point
description fakulte1_baglantisi
 ip address 172.16.0.5 255.255.255.252
 pvc 0/2
 protocol ip 172.16.0.6 broadcast
 encapsulation aal5snap
!
```

(Merkez yönlendirici ile Fakülte-1'de bulunan yönlendirici arasındaki DLCI numarası 2 olan Frame Relay bağlantısını gösteren konfigürasyon satırıdır.)

```
!
interface ATM1/0.3 point-to-point
 description fakulte2_baglantisi
 ip address 172.16.0.9 255.255.255.252
 pvc 0/3
 protocol ip 172.16.0.10 broadcast
 encapsulation aal5snap
!
```

(Merkez yönlendirici ile Fakülte-2'de bulunan yönlendirici arasındaki DLCI numarası 3 olan Frame Relay bağlantısını gösteren konfigürasyon satırıdır.)

```
!
interface ATM1/0.4 point-to-point
 description yuksekokul_baglantisi
 ip address 172.16.0.13 255.255.255.252
 pvc 0/4
 protocol ip 172.16.0.14 broadcast
 encapsulation aal5snap
!
```

(Merkez yönlendirici ile Yüksekokulda bulunan yönlendirici arasındaki DLCI numarası 4 olan Frame Relay bağlantısını gösteren konfigürasyon satırıdır.)

Yukarıdaki konfigürasyon satırları tamamen merkez yönlendirici ile kenar yönlendiriciler arasındaki bağlantıları gösteren tanımlamalardır. Bu işlemlerin devamında gerçekleştirilen merkez yönlendirici üzerinde tüm trafiğin yönlendirilmesini sağlayan tanımlamalar da aşağıda verilmiştir.

```
ip route 0.0.0.0 0.0.0.0 ATM1/0.1
```

(Tüm internet çıkışı trafiğinin internet servis sağlayıcısında bulunan yönlendiriciye yönlendirilmesini sağlayan komut satırıdır.)

```
ip route vrf A 0.0.0.0 0.0.0.0 192.168.1.1
```

(Uzak alan ağlarındaki yönlendiricilerden gelen paketlerin tünelleme işlemi dahilinde güvenlik duvarının DMZ2 portuna yönlendirilmesini sağlayan komut satırıdır.)

```
ip route vrf A 192.168.1.64 255.255.255.192 ATM1/0.2
```

(Fakülte-1 ağı için yönlendirme tanımlamasını gösteren komut satırıdır.)

```
ip route vrf A 192.168.1.128 255.255.255.192 ATM1/0.3
```

(Fakülte-2 ağı için yönlendirme tanımlamasını gösteren komut satırıdır.)

```
ip route vrf A 192.168.1.192 255.255.255.192 ATM1/0.4
```

(Yüksekokul ağı için yönlendirme tanımlamasını gösteren komut satırıdır.)

Bu konfigürasyon satırları ile uzak alanlardaki tüm ağların, merkezdeki yönlendiricinin ikinci ethernet portu üzerinden güvenlik duvarı ardına bir tünelle bağlanması sağlanır. Böylelikle tüm ağlar, güvenlik duvarı ardında yerel bir ağ gibi davranacak ve güvenlik duvarı ile yönlendirici arasındaki bağlantı üzerinden tekrar yönlendirilerek internet bağlantılarını sağlayacaklardır. Bu durumda da güvenlik duvarı üzerinde erişim listeleri ile belirlenen tüm kurallar uzak alan ağları için de geçerli olacaktır.

Merkezdeki güvenlik duvarı üzerinde belirlenen kuralların konfigürasyon anlamında farkı yoktur. Sadece IP grupları olarak önceki uygulamada yerel ağ kullanıcılarına verilen yetkiler, bu uygulama için hem yerel ağ hem de uzak alan ağ kullanıcılarına verilecektir. Çünkü buradaki tüm yapı, güvenlik duvarı açısından tek bir yerel ağ olarak değerlendirilir.

İlk uygulamaya göre farklılık içeren bu kısmın yapılandırılmasından sonra yetkilendirme ve erişim yapılandırmalarına geçilir.

Yerel ağ üzerindeki bilgisayarların dışarıya doğru erişim trafiği için güvenlik duvarı üzerinde yapılan düzenlemeler

```
outbound  1 deny 0.0.0.0 0.0.0.0 0 ip
outbound  1 permit 192.168.2.0 255.255.255.224  80 tcp
outbound  1 permit 192.168.2.0 255.255.255.224  21 tcp
outbound  1 permit 192.168.2.0 255.255.255.224  25 tcp
outbound  1 permit 192.168.2.0 255.255.255.224 110 tcp
outbound  1 permit 192.168.2.0 255.255.255.224 143 tcp
```

Fakülte-1 ağı üzerindeki bilgisayarların dışarıya doğru erişim trafiği için yönlendirici üzerinde yapılacak düzenlemeler:

```
outbound  2 deny 0.0.0.0 0.0.0.0 0 ip
outbound  2 permit 192.168.1.64 255.255.255.192  80 tcp
outbound  2 permit 192.168.1.64 255.255.255.192  21 tcp
outbound  2 permit 192.168.1.64 255.255.255.192  25 tcp
outbound  2 permit 192.168.1.64 255.255.255.192 110 tcp
outbound  2 permit 192.168.1.64 255.255.255.192 143 tcp
```

Fakülte-2 ağı üzerindeki bilgisayarların dışarıya doğru erişim trafiği için yönlendirici üzerinde yapılacak düzenlemeler:

```
outbound 3 deny 0.0.0.0 0.0.0.0 0 ip
outbound 3 permit 192.168.1.128 255.255.255.192  80 tcp
outbound 3 permit 192.168.1.128 255.255.255.192  21 tcp
outbound 3 permit 192.168.1.128 255.255.255.192  25 tcp
outbound 3 permit 192.168.1.128 255.255.255.192 110 tcp
outbound 3 permit 192.168.1.128 255.255.255.192 143 tcp
```

Yüksekokul ağı üzerindeki bilgisayarların dışarıya doğru erişim trafiği için yönlendirici üzerinde yapılacak düzenlemeler:

outbound 4 deny 0.0.0.0 0.0.0.0 0 ip
outbound 4 permit 192.168.1.192 255.255.255.192 80 tcp
outbound 4 permit 192.168.1.192 255.255.255.192 21 tcp
outbound 4 permit 192.168.1.192 255.255.255.192 25 tcp
outbound 4 permit 192.168.1.192 255.255.255.192 110 tcp
outbound 4 permit 192.168.1.192 255.255.255.192 143 tcp

Mail ve web sunucusu için güvenlik duvarı üzerinde yapılan düzenlemeler:

1. *static (DMZ,outside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0* (mail sunucusu için)
2. *static (DMZ,outside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0* (web sunucusu)

Yetkilendirme tanımları:

1. *conduit permit tcp host 240.18.186.2 eq 143 any 192.168.1.0 255.255.254.0* (mail sunucusu imap)
2. *conduit permit tcp host 240.18.186.2 eq 25 any* (mail sunucusu smtp)
3. *conduit permit tcp host 240.18.186.2 eq 110 192.168.1.0 255.255.254.0* (mail sunucusu pop3)
4. *conduit permit tcp host 240.18.186.3 eq http any* (web sunucusu)

SONUÇ ve ÖNERİLER

Yapılan her iki uygulamada da öncelikle amaçlanan; güvenlik duvarı cihazının doğru yapılandırılması, sadece dışardan içeriye doğru gelen trafik için kurallar yazmak yerine her iki yönde ilerleyen ağ trafiği için kuralların yazılması, her iki yöndeki trafiğin denetlenmesi, kontrol altına alınması ve herhangi bir yönde ilerleyen trafik için hangi uygulamaların yetkilendirilmiş olduğunun tanımlanmasıdır.

Güvenlik duvarı, sadece internete karşı yerel ağların güvenlik altına alınmasını sağlamak için kullanılırsa fonksiyonları tam olarak kullanılıyor sayılamaz. Kuralları doğru tanımlamak, yön seçeneği yapmaksızın, güvenlik duvarı cihazının kısıtlama ve kontrol etme mekanizmasını harekete geçirir. Güvenlik duvarının yeteneklerinin kullanılmasıyla istenmeyen trafiği en az seviyeye indirgemek, sunucuların gerek internet trafiğine karşı, gerekse yerel ağ kullanıcılarına karşı güvenliğini sağlar.

Bu çalışmada; öncelikle küçük ya da orta ölçekli olarak düşünülebilecek bir ağ üzerindeki istenmeyen trafiği engellemek adına oluşturulabilecek sistem konfigürasyonları ele alınmıştır. Erişim listelerinde belirtilen kurallar vasıtasıyla inside-DMZ arası, inside-internet arası ve internet-DMZ arası trafikler incelenmiştir.

Uygulama açısından uzak noktalarda da birimleri olan, yerel ve uzak alan ağlarını içeren bir kampüs ağ yapısı kullanılmıştır. Bu yapı üzerindeki ağ erişimlerinin ağ performanslarını istenilen düzeye çıkarmak için, güvenlik duvarı üzerinde yazılan kuralların kısmen uzak noktalara doğru kaydırılmasıyla, %30 ile %60 arasında ağ trafiğinin kontrolüne, istenmeyen trafiğin önlenmesine, sunucu güvenliği ve ağ performansına, olumlu etkisi gözlenmiştir. Yapılan ilk uygulamadaki konfigürasyonlarda da ikinci uygulamada olduğu gibi sistem performansı ve ağların internete erişim hızlarında %30 ile %60 arasında bir artış gözlenmiştir. Buradaki değişkenlik, virüs, solucan, truva atı gibi yerel ağda istenmeyen trafiği oluşturan etkenlerden kaynaklanmaktadır.

Çözüm önerileri olarak; sistemde bir anti-virüs politikası oluşturulmalı; kullanılan işletim sistemleri, ofis uygulamaları, antivirüs yazılım güncellemeleri sürekli takip edilmeli, tüm kullanıcı ve sunucular için belirlenen politikalar geçerli olmalı ve gerekli olan tüm trafiğin izlenmesi sağlanmalıdır. Ayrıca çok çabuk yayılan ve ağa büyük ölçüde zarar verebilen truva atı, virüs, solucan gibi sistemi kötü yönde etkileyen zararlı programlar için de tebirler alınmalıdır.

Sistem yapısı içerisinde yer alan ağlardan, DMZ ile ağlar arasındaki trafiklerden ve uzaktaki kullanıcılardan gelebilecek olası tehlikelere karşı erişim hakları gereklilikler ölçütüne göre kısıtlanmalıdır. Güvenlik duvarı tüm bu iletişimi kaldırabilecek oranda güçlü olmalıdır.

Sonuç olarak sistemde yer alan ağların performansının ve güvenliğinin yüksek olması için politikaların, kurtarma planlarının ve tasarımın mükemmele yakın olması gerekmektedir.

KAYNAKLAR

[1] Stallings W., "Cryptography and Network Security", P.Hall 1999, ISBN0-0-13-869017-0.

[2] Kaplan Y., "Veri Haberleşmesi Kavramları", Papatya Yayınevi, 2000, 205 s.

[3] http://www.bilisimrehber.com.tr/tr_white.phtml

[4] Stallings W., "Network Security Essentials" P.Hall 2000, ISBN0-13016-093-8.

[5] http://www.bilgisayardershanesi.com/aglardaguvenlik1.htm#top

[6] http://www.datamarket.com.tr/int_guvenlik_coz.html

[7] http://www.bnt.com.tr/wan.php