YÜKSEK LİSANS TEZİ ONAY FORMU

Süleyman ALTAN tarafından Yrd. Doç. Dr. Murat AYDOS yönetiminde hazırlanan "**Kampüs Ağlarında Sistem Performansının Optimizasyonu**" başlıklı tez tarafımızdan okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans Tezi olarak kabul edilmiştir.

Yrd. Doç. Dr. Murat AYDOS

(Yönetici)

Yrd. Doç. Dr. Ahmet ÖZEK

(Jüri Üyesi)

Yrd. Doç. Dr. Sezai TOKAT

(Jüri Üyesi)

Pamukkale Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun
21./12./2005 Tarih ve 27/4. Sayılı kararıyla onaylanmıştır.

Prof. Dr. Mehmet Ali SARIGÖL

Müdür

Bu tezin tasarımı, hazırlanması, yürütülmesi, araştırılmalarının yapılması ve bulgularının analizlerinde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini; bu çalışmanın doğrudan birincil ürünü olmayan bulguların, verilerin ve materyallerin bilimsel etiğe uygun olarak kaynak gösterildiğini ve alıntı yapılan çalışmalara atfedildiğini beyan ederim.

İmza :

Öğrenci Adı Soyadı : Süleyman ALTAN

TEŞEKKÜR

Pamukkale Üniversitesi Bilgi İşlem Daire Başkanlığında çalıştığım süre içerisinde Yüksek Lisans Eğitimime başlamakta ve devam etmekte bana destek veren Bilgi İşlem Dai. Bşk. V. Doç. Dr. Mehmet MEDER'e; bu tezin hazırlanmasında akademik anlamda beni oldukça aydınlatan ve çalışmalarımı titizlikle inceleyerek daha iyi olma konusunda beni yönlendiren, Tez Danışmanım Yrd. Doç. Dr. Murat Aydos'a; materyal bulma ve araştırmalarda bana zaman ayıran Arş. Gör. Meriç Çetin'e; tez konusundaki uygulamaları beyin fırtınası yaparak hayata geçirmekte bana destek veren Uzm. İlker ULAŞ'a teşekkür ederim.

Süleyman ALTAN

ÖZET

Altan, Süleyman
Yüksek Lisans Tezi, Elektrik - Elektronik Mühendisliği ABD
Tez Yöneticisi: Yrd. Doç. Dr. Murat AYDOS

Eylül 2005, 40 Sayfa

Günümüzde bilgisayar ağlarının mevcut yapılarındaki büyümelerden dolayı 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. Ayrıca uygulama açısından uzak noktalarda da birimlerinin olduğu daha geniş bir ağ yapısı düşünüldüğünde, geniş ağlarda, uzak erişimlerdeki ağ performansının istenilen düzeyde olabilmesi için bu 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, istenmeyen ağ trafiği, erişim listeleri, ağ performansının optimize edilmesi, güvenlik politikaları

Yrd. Doç. Dr. Murat AYDOS
Yrd. Doç. Dr. Ahmet ÖZEK
Yrd. Doç. Dr. Sezai TOKAT

ABSTRACT

Altan, Suleyman
M. Sc. Thesis in Electrics – Electronics Engineering
Supervisor: Asst. Prof. Dr. Murat AYDOS

September 2005, 40 pages

OPTIMIZING TO NETWORK PERFORMANCE IN CAMPUS NETWORKS

With the increasing number of computers, and the amaount of tasks performed by these networks, it has become very important to manage and control the networks. In addition, while considering the performance on these networks, it has also become important the access to data and the security of applications running on these networks. Although the computer communications and connections have become more healthier with the presentation of security policies, it is still important to consider other security threaths, such as virus, trojan horse, isolotion of local networks from internet, and undesired traffics. Therefore, it is important to consider the security of servers against exterior networks, the security threats that may come from interior local users. It is also important to provide a monitored and controlled network traffic.

In this thesis, a small (or can be considered medium) size local area network, which is located behind a firewall, is considered. On this network, ther servers are located on a isolated area that is considered to be secure. The main goal here is to prevent the undesired and unnecessary traffic that might be occur on this local network. Several network architecture models are considered and simulated. It has been observed that when there are end points located in a long distance from each other on this network, the applied rules and policies can be shifted around and applied to this enlarged network architecture. In this work, with the use of rules defined on the firewall, it is possible to prevent or limit the undesired traffic on the network, it is possible to increase the server security and the network performance.

Keywords: Campus networks, unwanted network traffic, access lists, optimizing network performance, security policies

Asst. Prof. Dr. Ahmet ÖZEK
Asst. Prof. Dr. Sezai TOKAT
Asst. Prof. Dr. Murat AYDOS

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

1. 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.

Internet'in 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 (Stallings 1999).

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

1.1 Problem Tanımı

Bu çalışmada; bir kampüs ağında kontrol edilmeyen ve istenilmeyen ağ trafiğinden doğan performans azalması üzerinde durulmuştur. Ağ altyapısı genişledikçe oluşan trafiğin tamamen kontrol altında olması ve gereksiz paketlerin ağ üzerindeki dolaşımının ağ performansına etkisi incelenmiştir. Aktif cihazlar çalışma prensipleri doğrultusunda gerektiği şekilde konfigüre edilmemesi durumunda gerçek kapasitesi ile çalışamamakta, ağ üzerinde de ideal performans elde edilememektedir. Broadcast,

yetkilendirilmemiş paketler ve istekler, özellikle büyüyen ağ altyapılarında ağ performansını olumsuz derecede ve ciddi boyutta etkilemektedir.

1.2 Amaç ve Yöntem

Yapılan çalışmada kampüs ağlarında gereksiz trafiğin önlenmesi, ağ üzerindeki tüm trafiğin belirli kurallar çerçevesine alınması ve sistem performansının optimize edilmesi amaçlanmıştır. Bunun için kampüs ağları üzerinde bir model tasarlanmış, bu model üzerinden ağa bağlı aktif cihazlar üzerinde konfigürasyonlar geliştirilmiştir.

Kampüs ağlarında yapının genişlemesinden dolayı farklı noktalarda farklı aktif cihazlar bulunmakta, ağ üzerindeki istenmeyen trafiğin ve performansı olumsuz derecede etkileyen paketlerin kaynaklarına ve geçiş noktalarına göre aktif cihazlar üzerine de farklı görevler tanımlanmaktadır.

Bu çalışma ile, Yerel Alan Ağları ve Uzak Alan Ağları ayrı ayrı ele alınmış, güvenlik duvarı ve yönlendiriciler üzerinde geliştirilen konfigürasyonlar ile ağ performansının optimum düzeyde olması sağlanmıştır. Bu aynı zamanda ağ üzerinde dolaşan gereksiz ağ paketlerinin de önlenmiş olmasını sağlamaktadır.

1.3 Tezin Önemi ve Literatüre Katkısı

Yapılan literatür çalışmasında sürekli gelişen ağ teknolojilerinin kullanılmasıyla genişleyen kampüs ağlarında oluşan gereksiz ağ trafiğinin önlenmesi amacıyla konfigürasyon modeli geliştirilmiş, farklı kategorideki aktif cihazların farklı modellerdeki kampüs ağı yapıları üzerinde performans optimizasyonu için bir örnek oluşmuştur. Yapılan tez çalışması aynı zamanda bir üniversitenin ağ altyapısında uygulamaya alınmış ve bu çalışma temel alınarak kampüs ağında performans optimizasyonu anlamında yapılan çalışmalara ışık tutmuştur. Farklı uygulamaların yoğun bir şekilde kullanıldığı kampüs ağlarında ağ performansı optimizasyonuna ihtiyaç duymasından dolayı bunu sağlamakta geliştirilen çalışma önemlidir.

1.4 Tezin Organizasyonu

Tez çalışmasınını ilk bölümünde kampüs ağlarında sistem performansının optimizasyonu hakkında genel bilgi verilmiş, amaçlananlar anlatılmışve kullanılan yöntemlerden bahsedilmiştir. İkinci bölümde kurumsal bilgiler ve literatür taraması anlatılmış, güvenlik politikalarından ve saldırı kavramından bahsedilmiş ve tez çalışmasındak,i materyal ve metotlar anlatılmıştır. Üçüncü bölümde ise yerel alan ağlarında güvenlik politikalarının uygulanmasının yanısıra performans değerlerinin de artışı için yapılan çalışmadan bahsedilmiştir. Aynı zamanda uzak alan ağları içeren bir kampüs ağında bu kriterlerin daha farklı şekilde nasıl uygulandığı anlatılmıştır. Her bir aktif cihaz üzerinde geliştirilen konfigürasyonlar ayrı ayrı tanımlanmış ve devamında açıklanmıştır.

Bu çalışmada konfigürasyon tanımlanan konfigürasyonlar, Cisco aktif cihazlarının komutsal arayüzünde kullanılan tanımlamalarla gösterilmiştir.

Son bölümde ise bu tez çalışmasıyle elde edilen sonuçlar ortaya konmuş ve konuyla ilgili önerilerden bahsedilmiştir.

2. KURAMSAL BİLGİLER VE LİTERATÜR TARAMASI

2.1 Güvenlik Bilinci

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 (Kaplan 2000, WEB_1 2003).

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.

2.2 Güvenlik Politikaları ve Saldırı Kavramı

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 (Stallings 2000).

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 List) kurallar doğrultusunda işleme alınır ve daha sonra incelenmek üzere saklanır (WEB_2 2005).

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 (WEB_3 2005).

Internet 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. Internet bağlantı noktalarından geçen trafiğin düzenli olarak izlenmesi, saldırıların belirlenmesini ve onlara karşı önlem alınmasını kolaylaştırır (WEB_4 2005).

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.

3. MATERYAL VE METOT

Yapılan çalışmada tüm deney ve uygulamalar Pamukkale Üniversitesi Kampüs Ağı üzerinde uygulanmıştır. Pamukkale Üniversitesi Kampüs Ağı içerisinde kullanılan tüm yönlendiriciler, anahtarlar, güvenlik duvarı cihazları Cisco markası olduğu için, metinlerde yer alan cihaz konfigürasyonları tamamen Cisco üretici firmasının cihazlarına özgün olan konfigürasyon komutlarıdır. Güvenlik duvarı olarak Pix Serisinin 525 modeli, Merkez yönlendirici 3600 serisi 3662 modeli yönlendirici, diğer yönlendiriciler ise 1700 serisi 1760 modeli yönlendiriciler kullanılmıştır. Üniversitenin ağ altyapısında ve sunucu sistemlerinde kullanılan ve belirli bir bölümü internet üzerinden erişilebilen IP adresleri yerine, sanal olarak IP adresleri atanmış ve metne bunlar aktarılmıştır. Bu işlemde üniversite ağının ve sunucularının güvenliği gözönünde bulundurulmuştur.

Üniversitenin kampüs ağındaki performansı etkileyen faktörlerin tesbitinden yola çıkılarak yapılan çalışmada, öncelikli olarak düşünülen ağ sisteminin performansının optimize edilmesidir. Bunun için yapıda kullanılan cihazların standart konfigürasyonları yeterli olmadığı için, özellikle uzak alan ağlarında bant genişliği daha düşük olduğu için, gereksiz ağ trafiği oluşturan etkenlerin ortadan kaldırılması ya da belirli noktalarda kıstılanması yöntemi uygulanmıştır. Istenmeyen trafiği oluşturan etkenlerin tüm ağ üzerindeki aktif cihazlar, kullanıcı bilgisayarları ve sunucular üzerinden tam olarak ortadan kaldırılması işlemi için daha kapsamlı ve daha farklı bir çalışma yapılması gerekmektedir. Bu çalışmada ise üzerinde durulan kısım, sadece ağı oluşturan aktif cihazlar (yönlendiriciler ve güvenlik duvarları) üzerinde uygulanmıştır.

Yapı olarak iki farklı model düşünülmüştür. Öncelikle kampüs merkezinde bulunan ağ altyapısı (Yerel Alan Ağı) üzerinde çalışma yapılmış ve buradaki çalışma daha sonra genişletilerek 2 fakülte, 1 Yüksekokul ve merkez olmak üzere (Uzak Alan Ağları) uygulamaya alınmıştır.

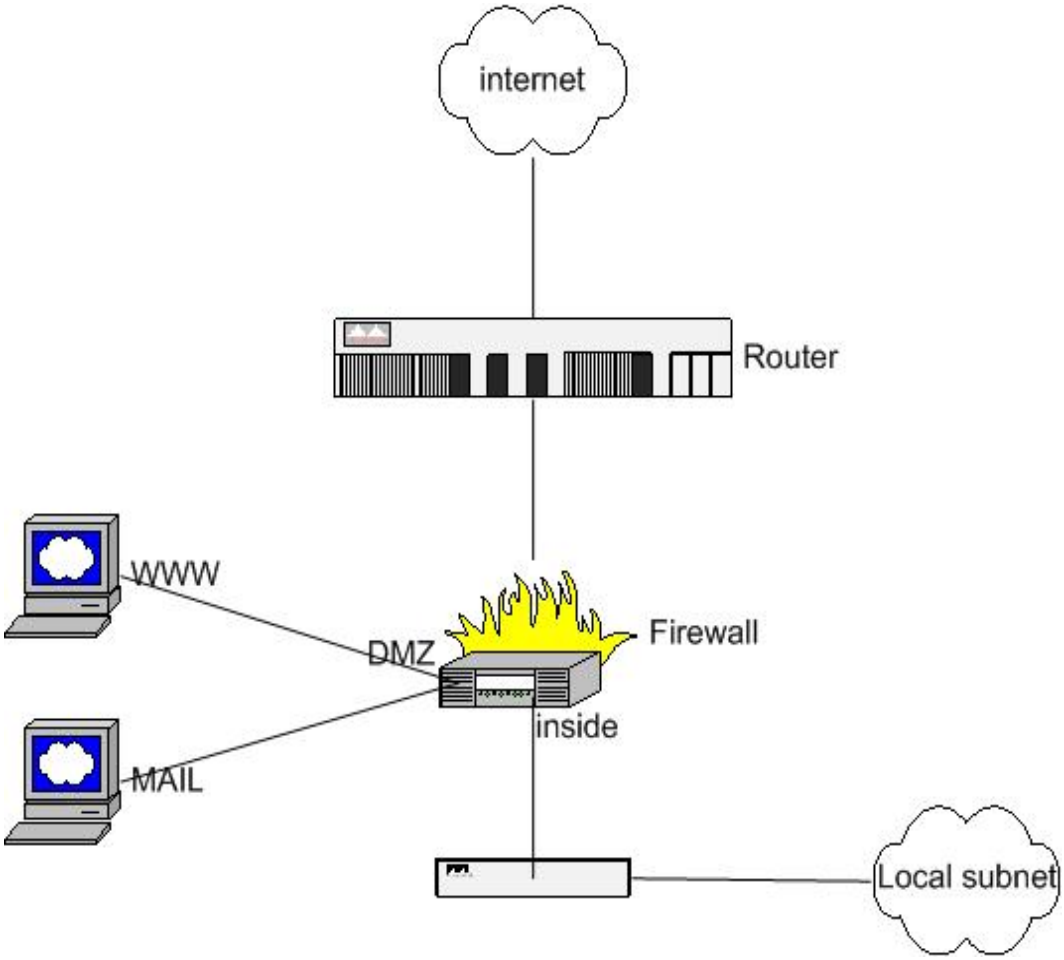
Güvenlik duvarı cihazı üzerinde izinler belirtilirken izlenebilecek iki yöntem vardır. Birincisi; önce tüm izinlerin kaldırılması, sonra gerekli izinlerin gerekli adreslere

yetkilendirilmesidir. İkincisi; tüm izinlerin varsayılan konfigürasyonda açık olması, sonrasında gerekli olmayan izinlerin kaldırılmasıdır.

Yapılan çalışmada birinci yöntem izlenmiştir. Bunun sebebi, sistem performansını olumsuz olarak etkileyen faktörlerin sayısı oldukça fazla olması ve bunların tek tek tanımlanmasının da sistem üzerinde çalışan aktif cihazlara ayrı bir yük getirebileceği olasılığının göz önünde bulundurulmasıdır.

4. YEREL ALAN AĞI ÜZERİNDE SİSTEM PERFORMANSININ OPTİMİZASYONU

Şekil 4.1'de gösterilen ilk uygulamada, local subnet olarak ifade edilen tek bir yerel ağdan oluşan küçük bir yapı görülmektedir. Bu yerel ağda bulunan 40 bilgisayar için IP adreslerinin yapılandırması aşağıda ifade edildiği gibidir:



Şekil 4.1 Sadece yerel alan ağından oluşan yapı

Yerel ağda bulunan 40 PC için IP adreslemesi;

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 posta sunucuları yer almaktadır. DMZ tarafındaki ağın ve sunucuların IP yapılandırması aşağıda ifade edildiği gibidir:

DMZ tarafındaki sunucular için IP adreslemesi;

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. Posta ve web sunucularının DMZ bölgesi içinde olmasının avantajları vardır. Posta sunucusunun bu bölgede yer alması; kurum çalışanların e-postalarını posta sunucusu aracılığıyla almasına, tüm e-postaların 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, hangi iletişim protokolü ve hangi uygulama portu bağlantısı geçişine izin 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'e 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 uygulama portu http (web), 21 numaralı uygulama portu ftp (file transfer protocol), 25 numaralı uygulama portu e-posta, 110 numaralı uygulama portu POP3 ve 143 numaralı uygulama portu IMAP uygulamalarının port numaralarını göstermektedir.

Outbound komutu, Pix cihazı üzerinde yerel ağda (inside) bulunan tüm kullanıcıların bulundukları ağın dışında herhangi bir ağa erişirken görecekleri kısıtlamaları tanımlayan komuttur.

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 240.18.186.3 netmask 255.255.255.255
outbound 1 permit 192.168.1.0 255.255.255.224 25 tcp 240.18.186.2 netmask 255.255.255.255
outbound 1 permit 192.168.1.0 255.255.255.224 110 tcp 240.18.186.2 netmask 255.255.255.255
outbound 1 permit 192.168.1.0 255.255.255.224 143 tcp 240.18.186.2 netmask 255.255.255.255

Yukarıdaki konfigürasyon satırlarında belirlenen kurallara göre; birinci satırda yerel ağ grubundaki tüm kullanıcılara tüm erişimler yasaklanır, ardındaki satırlada ise sırasıyla her satırda belirtilen uygulama portu ve iletişim protokolleri bazında erişim yetkileri verilir. Böylece yerel ağdan Internete ve DMZ'e 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 yerel sunucular üzerinde sadece belirtilen uygulamaları çalıştırabilirler.

Özel durum ise; ikinci satırdaki konfigürasyona göre kullanıcıların herhangi bir web sitesine erişim izni olmasına karşın, üçüncü satırdaki konfigürasyonda görüldüğü gibi sadece yerel web sunucusuna dosya transferi erişimi izni vardır. Aynı şekilde son üç satırda görülen konfigürasyon örneğinde olduğu gibi kullanıcıların sadece yerel e-posta sunucusu üzerinden e-posta gönderme ve alma izinleri vardır.

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. Güvenlik duvarı cihazlarının sadece internet ortamıyla yerel ağ ortamının birbirinden soyutlanması amacıyla konfigüre edilmesi eksik olur.

DMZ bölgesinde bulunan sunuculara sadece yerel ağ üzerinden değil internet ortamından da erişimin sağlanabilmesi düşünülmüştür. Dolayısıyla DMZ bölgesinde bulunan web ve e-posta sunucuları için dışarıdan erişim yetkilendirmeleri amacıyla güvenlik duvarı üzerinde aşağıdaki konfigürasyon komut satırları yazılmıştır.

Posta ve web sunucusu için güvenlik duvarı üzerinde yapılan düzenlemeler;

static (DMZ,outside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
static (DMZ,inside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
(e-posta sunucusu için yapılan NAT tanımlamaları)

static (DMZ,outside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
static (DMZ,inside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
(web sunucusu için yapılan NAT tanımlamaları)

Yukarıdaki konfigürasyon satırlarında, sanal IP adreslerine sahip DMZ tarafındaki web ve posta 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; bir veya birden fazla sanal IP adresinin, bir veya birden fazla gerçek IP adresi arkasına saklanarak tüm sunucu ve bilgisayarların Internete çıkarılması için kullanılan mekanizmaya verilen isimdir. Bu sayede sahip olunan tek bir IP adresi ile yerel alanda bulunan çok sayıda bilgisayar Interente çıkarılabilir. Pix serisi güvenlik duvarının *"static"* komutu tam olarak bu işemi yapmak için kullanılan komuttur. Bu konfigürasyonda e-posta sunucusuna hem internet ortamından hem de yerel ağ ortamından erişim için

240.18.186.2 gerçek IP adresi tanımlanmıştır. Web sunucusu için ise *240.18.186.3* gerçek IP adresi tanımlanmıştır. Sunucuların üzerinde tanımlanan IP adresleri ise sanal IP adresleridir.

Pix serisi güvenlik duvarı cihazı üzerinde alternatif olarak yapılabilecek bir konfigürasyon örneğinde yerel ağ ortamındaki kullanıcı bilgisayarlarının sunuculara erişimi için gerçek IP adresine dönüşün tanımlaması yapılmaz. Ancak sistem üzerindeki performans optimizasyonu düşünülürken bunun güvenlik kavramıyla da ilgili olmasından dolayı farklı bir yöntem izlenmiştir. Izlenen yöntemde kullanıcıların sunuculara erişim için zorunlu olarak gerçek IP adresleriyle erişmesi sağlanmış ve böylece e-posta ve web sunucularının gerçek IP adreslerine yönelik uygulanan tüm kurallar hem yerel ağ ortamındaki kullanıcıları hem de internet ortamındaki kullanıcıları etkilemektedir.

Sistemde yer alan farklı bölümler farklı ağları temsil ettiğinden dolayı, 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;

conduit permit tcp host 240.18.186.2 eq 25 any

(Bu komut satırı ile 240.18.186.2 gerçek IP adresi ile eşleşen e-posta sunucusu, tüm posta sunucularından gelen e-postaları kabul edebilir hale gelir.)

conduit permit tcp host 240.18.186.2 eq 143 192.168.1.0 255.255.255.224

(IMAP protokolü posta sunucularına posta istemci programlarıyla erişebilmeyi sağlayan bir protokoldür. Bu komut satırı; sadece yerel ağ kullanıcılarının, yerel e-posta

sunucusuna bir e-posta istemcisi programı ile bağlantı sağladığı durumlarda IMAP protokolünü kullanabilme yetkilerini veren komut satırıdır)

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, e-posta istemci programlarının e-posta sunucusuna bağlanabilmesini, posta alıp gönderebilmesini sağlayan POP3 protokolünü kullanarak posta sunucusuna erişebilmelerini sağlayan komut satırıdır.)

conduit permit tcp host 240.18.186.3 eq http any

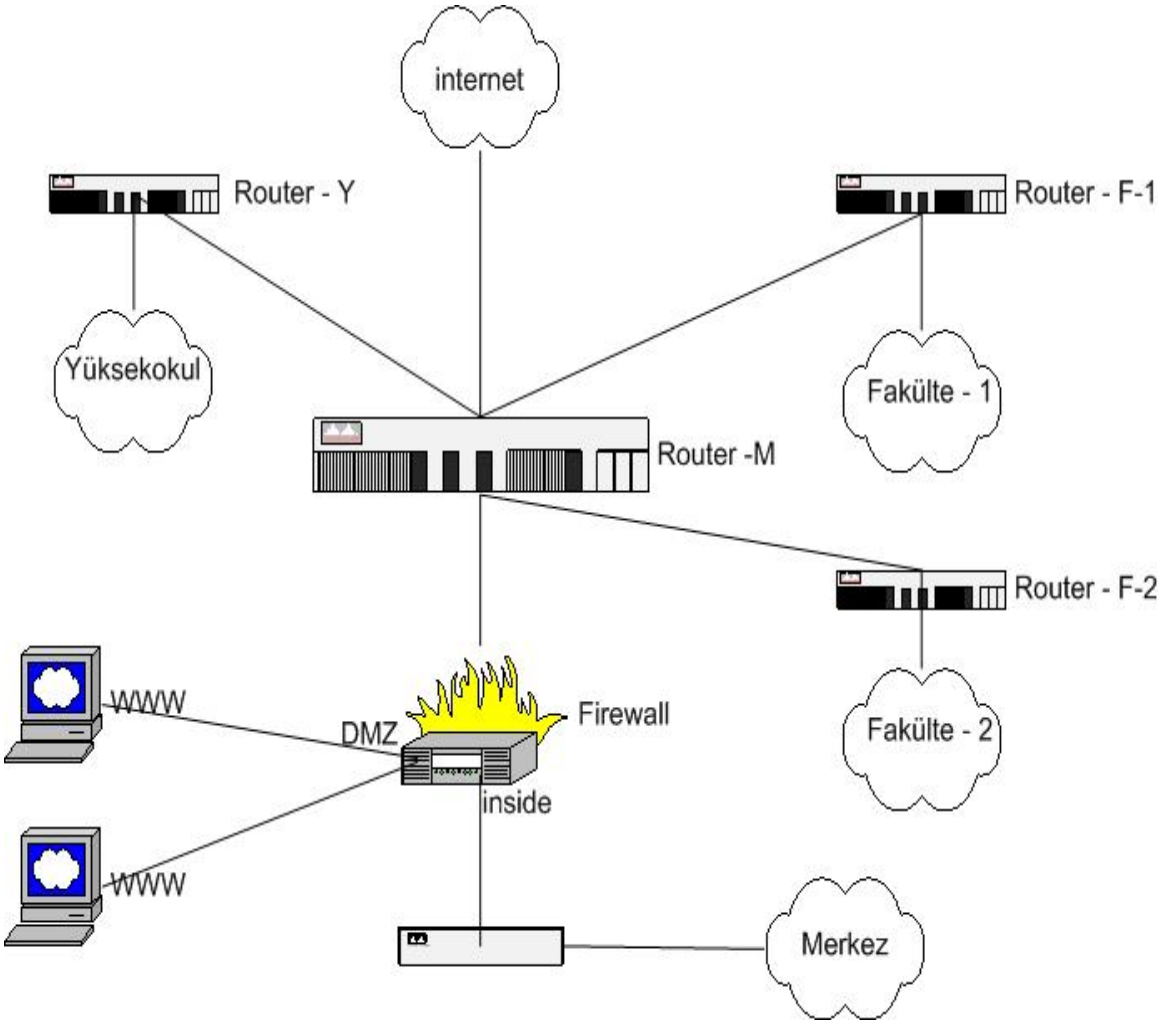
(Bu komut satırı; yerel web sunucusunda barındırılan web sitelerine herhangi bir istemciden ulaşılabilmesi kuralını belirleyen komut satırıdır.)

conduit permit tcp host 240.18.186.3 eq ftp 192.168.1.0 255.255.255.224
(Bu komut satırı ise; yerel web sunucusunda barındırılan web sitelerine dosya transferi yapabilme hakkının (ftp) sadece yerel ağ ortamında bulunan istemcilerde olduğu kuralını belirleyen komut satırıdır.)

5. UZAK ALAN AĞLARI İÇEREN YAPI ÜZERİNDE SİSTEM PERFORMANSININ OPTİMİZASYONU

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 ve bu bant genişliklerinin yerel alan ağlarındaki bant genişliklerinden oldukça düşük düzeyde olduğu varsayılmıştır (Şekil 4.1). 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. Uzak alan ağlarından diğer ağlara ve özellikle merkezde bulunan sunuculara erişimin belirlenen kurallar düzeyinde olması için sadece merkezde bulunan güvenlik duvarı veya yönlendirici cihaz üzerinde tanımlama yapılması, aradaki bant genişlikleri için herhangi bir performans optimizasyonu anlamına gelmez. Dolayısıyla uzak alan ağlarının bulunduğu noktada da ağ trafiğinin optimizasyonu için tanımlama yapılması gerekmektedir.

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 4.1'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 posta) IP yapılandırması gerçekleştirilir.



Şekil 5.1 Kampüs ağı olarak düşünülebilecek, uzak alan ağlarını da içeren yapı

Merkez'de bulunan 25 PC için IP adreslemesi;

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 adreslemesi;

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 adreslemesi;

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 adreslemesi;

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 adreslemesi;

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 adreslemesi;

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. Pix serisi güvenlik duvarı cihazlarının tamamı bu işlem için uygun değildir. Aynı zamanda merkez yönlendirici olarak tüm yönlendiriciler de bu uygulamada kullanılamaz. Yapılan çalışmada kullanılan 525 modeli üzerinde birden fazla DMZ bölgesi oluşturulabildiği için ve 3600 serisi yönlendirici üzerinde birden fazla ethernet bağlantısı yapılabildiği için bu uygulama tercih edilmiştir.

Çalışmanın gerek güvenlik duvarı cihazı kısmında gerekse merkez yönlendirici cihaz kısmında sadece bir noktadan bağlantı sağlanarak yapılsaydı, tüm trafik tek bir noktadan ilerleyecekti. Bu da bant genişliğinin yarı yarıya düşmesi anlamında gelirdi. Uzak alan ağları ile merkez arasında yapılan VPN bağlantısı için ayrı bir yol tercih edilmesi sistem performansına olumlu derecede katkı sağlamıştır.

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.

Uzak alan ağlarının merkez yönlendirici üzerinden VPN erişimi için Türk Telekom tarafından tahsis edilen data hatlarından noktadan noktaya frame-relay bağlantı sistemi kullanılmıştır. Buna göre her bir bağlantı için bir bağlantı numarası kullanılmalıdır. Bu numaraların tamamı, konfigürasyon satırlarında sırasıyla hangi bağlantılara ait olduğu açıklanmıştır. Aynı zamanda tüm bağlantılar için merkez yönlendirici cihaz üzerinde farklı sanal devreler oluşturulmalıdır. Bunlar da konfigürasyon satırlarında geçen *"pvc"* tanımlamaları ile belirtilmiştir.

Merkez yönlendirici konfigürasyonu;

```
version 12.2
service config
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname "router"
!
enable secret 5 $1$2go1$y4NO34/TSxntNno/HQlS.1
enable password 7 070C285F4D064A5341400202102F392A2D27
!
ip subnet-zero
ip cef
!
!
ip name-server 193.255.52.2
!
ip vrf A
 rd 100:1
!
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
 ip vrf forwarding A
ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1
```

```
 ip address 240.18.186.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 no cdp enable
!
interface ATM1/0
 no ip address
 no ip mroute-cache
 atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 description Internet_Baglantisi
 !
 ip address 172.16.0.1 255.255.255.252
 no ip redirects
 pvc 0/1
  protocol ip 172.16.0.2 broadcast
  encapsulation aal5snap
 !
!
interface ATM1/0.2 point-to-point
 description Fakulte-1
 ip vrf forwarding A
 ip address 172.16.0.5 255.255.255.252
 no ip redirects
 pvc 0/2
  protocol ip 172.16.0.6 broadcast
  encapsulation aal5snap
 !
!
interface ATM1/0.3 point-to-point
 description Fakult-2
 ip address 172.16.0.9 255.255.255.252
```

```
 no ip redirects
 no ip mroute-cache
 pvc 0/3
  protocol ip 172.16.0.10 broadcast
  encapsulation aal5snap
 !
!
interface ATM1/0.4 point-to-point
 description Yuksek_Okul
 ip vrf forwarding A
 ip address 172.16.0.13 255.255.255.252
 no ip redirects
 pvc 0/4
  protocol ip 172.16.0.14 broadcast
  encapsulation aal5snap
 !
!
!
interface Serial2/0
 no ip address
 encapsulation frame-relay
 no ip mroute-cache
 shutdown
 clockrate 2000000
 frame-relay lmi-type ansi
!
interface Serial2/1
 no ip address
 no ip mroute-cache
 shutdown
 clockrate 2000000
 no cdp enable
!
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 ATM1/0.1
ip route 240.18.186.1 255.255.255.0 Null0
ip route vrf A 0.0.0.0 0.0.0.0 192.168.1.1
ip route vrf A 192.168.1.64 255.255.255.192 ATM1/0.2
ip route vrf A 192.168.1.128 255.255.255.192 ATM1/0.3
ip route vrf A 192.168.1.192 255.255.255.192 ATM1/0.4
ip http server
ip pim bidir-enable
!
no cdp run
!
snmp-server community public RO
snmp-server community private RW
snmp-server ifindex persist
no snmp-server enable traps tty
!
no call rsvp-sync
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
 password 7 00071A150754585059734540 1D1C1719171F
 login
line aux 0
line vty 0 4
 exec-timeout 30 0
 password 7 094F471A1A0A44445D5E0D243F213A3D3036
```

login
!
end

Merkez yönlendirici üzerindeki konfigürasyon satırlarından sistem performansının optimizasyonu için yapılan düzenlemeler, konfigürasyon satırları ve açıklamalarıyla birlikte aşağıda verilmiştir.

ip vrf A
rd 100:1
!
(Merkez yönlendirici üzerinde 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 merkez yönlendiricinin 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 tanımlamalara göre her bir uzak alan ağı, merkeze ayrı ayrı VPN tanımlaması ile erişmektedir.

Bu işlemlerin devamında gerçekleştirilen merkez yönlendirici üzerinde tüm trafiğin yönlendirilmesini sağlayan yönlendirme tanımlamaları 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. Buna göre internet ortamına gitmesi gereken tüm trafik İnternet Servis Sağlayıcısına yönlendirilir.)

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. Buna göre uzak alnlardan gelen trafik internet ortamına erişmek istediğinde standart konfigürasyonlara göre merkez yönlendiriciden doğrudan İnternet Servis Sağlayıcısına yönlendirilmesi gerekirken, öncelikle güvenlik duvarı cihazı ardına yönlendirilmektedir. Bu işlem aynı zamanda bu trafiğin geri dönüşünü de aynı şekilde sağlar.)

ip route vrf A 192.168.1.64 255.255.255.192 ATM1/0.2

(Fakülte-1 ağı için yönlendirme tanımlamasını gösteren komut satırıdır. Fakülte-1 ağından gelen isteklerin cevabı olan veya diğer ağlardan Fakülte-1 ağına gitmesi gereken trafiğin yönlendirilmesini sağlar.)

ip route vrf A 192.168.1.128 255.255.255.192 ATM1/0.3

(Fakülte-2 ağı için yönlendirme tanımlamasını gösteren komut satırıdır. Fakülte-2 ağından gelen isteklerin cevabı olan veya diğer ağlardan Fakülte-2 ağına gitmesi gereken trafiğin yönlendirilmesini sağlar.)

ip route vrf A 192.168.1.192 255.255.255.192 ATM1/0.4

(Yüksekokul ağı için yönlendirme tanımlamasını gösteren komut satırıdır. Yüksekokul ağından gelen isteklerin cevabı olan veya diğer ağlardan Yüksekokul ağına gitmesi gereken trafiğin yönlendirilmesini sağlar.)

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. Birinci çalışmada güvenlik duvarının yerel ağ (inside) kullanıcıları pozisyonu ne ise bu örnekte de hem yerel ağ (inside) hem de DMZ2 kullanıcılarının pozisyonu aynıdır.

Kenar Yönlendiricilerin konfigürasyonu;

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Fakulte-1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$GN52$z/PULYSXsxwZCSPA0cAG70
enable password 7 045802150C2E
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
```

```
!
ip dhcp excluded-address 192.168.1.1-192.168.1.5
!
ip dhcp pool Fakulte-1
  network 192.168.1.0 255.255.255.224
  default-router 192.168.1.1
  dns-server 193.255.52.2
  lease 0 2
!
no ftp-server write-enable
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.224
 speed auto
 full-duplex
!
interface Serial1/0
 no ip address
 ip access-group optimization  in
 ip access-group optimization out
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
interface Serial1/0.1 point-to-point
 ip address 172.16.0.2 255.255.255.252
ip access-group optimization out
 no cdp enable
 frame-relay interface-dlci 2
!
ip default-gateway 240.18.186.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0.1
ip http server
```

```
!
ip access-list extended optimization
deny ip  any any
permit tcp 192.168.1.0 255.255.255.224 eq 80
permit tcp 192.168.1.0 255.255.255.224 eq 110
permit tcp 192.168.1.0 255.255.255.224 eq 143
permit tcp 192.168.1.0 255.255.255.224 eq 25 240.18.186.2
permit icmp any any
!
!
line con 0
line aux 0
line vty 0 4
 password 7 01100F1758045758771C47070D00051C0E18
 login
!
!
end
```

Kenar Yönlendiriciler üzerindeki tanımlanan konfigürasyon satırlarında, merkez yönlendirici ile yapılan bağlantı sisteminin bantgenişliği düzeyi yerel ağlar bantgenişliği düzeyine göre oldukça düşük olması sebebiyle optimizasyon yapılmıştır. Konfigürasyon satırları ve açıklamaları aşağıda belirtilmiştir.

```
ip access-list extended optimization
deny ip  any any
permit tcp 192.168.1.0 255.255.255.224 eq 80
permit tcp 192.168.1.0 255.255.255.224 eq 110
permit tcp 192.168.1.0 255.255.255.224 eq 143
permit tcp 192.168.1.0 255.255.255.224 eq 25 240.18.186.2
permit icmp any any
```

Yukarıdaki konfigürasyon satırlarında bu yönlendiricinin ardında kalan ağ için bir erişim listesi oluşturulmuştur. Bu erişim listesine göre bu ağ üzerindeki kullanıcılar sadece belirtilen uygulamalara erişebilirler.

ip access-group optimization out

Yukarıdaki konfigürasyon satırı da, merkez yönlendirici ile kenar yönlendirici arasındaki bağlantının sağlandığı konfigürasyon satırlarında yazılır. Bu komut belirlenen erişim listelerinin belirlenen bağlantı üzerinde aktif hale getirilmesini sağlar.

Diğer Fakülte ve Yüksekokul ağında bulunan kenar yönlendiricilerin de konfigürasyonları hemen hemen aynıdır. Sadece ardında bulunan ağ için gerekli olan IP adresleri farklılaşmaktadır.

Merkezdeki güvenlik duvarı üzerinde belirlenen kuralların konfigürasyon anlamında çok 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.

Güvenlik Duvarı cihazının konfigürasyonu;

PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface gb-ethernet0 1000auto
interface gb-ethernet1 1000auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside2 security80
nameif gb-ethernet0 dmz-s security90
nameif gb-ethernet1 inside1 security70
nameif ethernet2 inside3 security60
enable password zWM3AzoXjG1ktMmu encrypted
passwd nV7n6Ub69cHM1O8j encrypted
hostname PIX
domain-name ciscopix.com

clock timezone EEST 2

clock summer-time EEDT recurring last Sun Mar 3:00 last Sun Oct 4:00

fixup protocol dns maximum-length 512

fixup protocol ftp 21

fixup protocol h323 h225 1720

fixup protocol h323 ras 1718-1719

fixup protocol http 80

fixup protocol rsh 514

fixup protocol rtsp 554

fixup protocol sip 5060

fixup protocol sip udp 5060

fixup protocol skinny 2000

fixup protocol smtp 25

fixup protocol sqlnet 1521

fixup protocol tftp 69

names

mtu outside 1500

mtu dmz 1500

mtu dmz2 1500

mtu inside 1500

ip address outside 240.18.186.2 255.255.255.0

ip address inside 192.168.1.2 255.255.255.0

ip address dmz 10.1.1.4 255.255.255.248

ip address dmz2 192.168.1.2 255.255.255.0

ip audit name ATTACKPOLICY attack action drop

ip audit interface outside ATTACKPOLICY

ip audit interface inside ATTACKPOLICY

ip audit interface dmz ATTACKPOLICY

ip audit interface dmz2 ATTACKPOLICY

ip audit info action alarm

ip audit attack action alarm

no failover

failover timeout 0:00:00

failover poll 15

no failover ip address outside
no failover ip address inside
no failover ip address dmz
no failover ip address dmz2
pdm history enable
arp timeout 14400
global (outside) 1 240.18.186.250-240.18.186.254 netmask 255.255.255.248
global (outside) 1 240.18.186.249 netmask 255.255.255.248
global (inside) 1 192.168.2.251 netmask 255.255.255.192
global (dmz) 1 10.1.1.5-10.1.1.6 netmask 255.255.255.248
global (dmz2) 1 192.168.1.251 netmask 255.255.255.0
nat (inside) 1 192.168.2.0 255.255.255.248 0 0
nat (dmz) 1 10.1.1.0 255.255.255.248 0 0
nat (dmz2) 1 192.168.1.0 255.255.255.0 0 0
static (DMZ,outside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
static (DMZ,inside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
static (DMZ,DMZ2) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
static (DMZ,outside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
static (DMZ,inside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
static (DMZ,DMZ2) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
conduit permit tcp host 240.18.186.2 eq 25 any
conduit permit tcp host 240.18.186.2 eq 143 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq 143 192.168.2.0 255.255.255.224
conduit permit tcp host 240.18.186.2 eq 110 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq 110 192.168.2.0 255.255.255.224
conduit permit tcp host 240.18.186.3 eq http any
conduit permit tcp host 240.18.186.3 eq ftp 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq ftp 192.168.2.0 255.255.255.224
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 240.18.186.3 netmask 255.255.255.255
outbound 1 permit 192.168.2.0 255.255.255.224 25 tcp 240.18.186.2 netmask 255.255.255.255
outbound 1 permit 192.168.2.0 255.255.255.224 110 tcp 240.18.186.2 netmask 255.255.255.255
outbound 1 permit 192.168.2.0 255.255.255.224 143 tcp 240.18.186.2 netmask 255.255.255.255

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 240.18.186.3 netmask 255.255.255.255

outbound 2 permit 192.168.1.64 255.255.255.192 25 tcp 240.18.186.2 netmask 255.255.255.255

outbound 2 permit 192.168.1.64 255.255.255.192 110 tcp 240.18.186.2 netmask 255.255.255.255

outbound 2 permit 192.168.1.64 255.255.255.192 143 tcp 240.18.186.2 netmask 255.255.255.255

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 240.18.186.3 netmask 255.255.255.255

outbound 3 permit 192.168.1.128 255.255.255.192 25 tcp 240.18.186.2 netmask 255.255.255.255

outbound 3 permit 192.168.1.128 255.255.255.192 110 tcp 240.18.186.2 netmask 255.255.255.255

outbound 3 permit 192.168.1.128 255.255.255.192 143 tcp 240.18.186.2 netmask 255.255.255.255

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 240.18.186.3 netmask 255.255.255.255

outbound 4 permit 192.168.1.192 255.255.255.192 25 tcp 240.18.186.2 netmask 255.255.255.255

outbound 4 permit 192.168.1.192 255.255.255.192 110 tcp 240.18.186.2 netmask 255.255.255.255

outbound 4 permit 192.168.1.192 255.255.255.192 143 tcp 240.18.186.2 netmask 255.255.255.255

conduit permit tcp host 240.18.186.2 eq 143 any 192.168.1.0 255.255.254.0

conduit permit tcp host 240.18.186.2 eq 25 any

conduit permit tcp host 240.18.186.2 eq 110 192.168.1.0 255.255.254.0

conduit permit tcp host 240.18.186.3 eq http any

apply (inside) 1 outgoing_src

apply (dmz2) 2 outgoing_src

apply (dmz2) 3 outgoing_src

apply (dmz2) 4 outgoing_src

route outside 0.0.0.0 0.0.0.0 240.18.186.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80

Güvenlik Duvarı üzerindeki konfigürasyon satırlarında sistem performansının optimizasyonu için yapılan tanımlamalar ve açıklamaları aşağıda belirtilmiştir.

Posta ve web sunucusu için güvenlik duvarı üzerinde yapılan düzenlemeler;

static (DMZ,outside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
static (DMZ,inside) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
static (DMZ,DMZ2) 240.18.186.2 10.1.1.2 netmask 255.255.255.255 0 0
(e-posta sunucusu için yapılan NAT tanımlamaları)

static (DMZ,outside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
static (DMZ,inside) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
static (DMZ,DMZ2) 240.18.186.3 10.1.1.3 netmask 255.255.255.255 0 0
(web sunucusu için yapılan NAT tanımlamaları)

Bu konfigürasyonda e-posta sunucusuna hem internet ortamından hem de yerel ağ ortamından erişim için *240.18.186.2* gerçek IP adresi tanımlanmıştır. Web sunucusu için ise *240.18.186.3* gerçek IP adresi tanımlanmıştır

Yetkilendirme tanımları;

conduit permit tcp host 240.18.186.2 eq 25 any

(Bu komut satırı ile 240.18.186.2 gerçek IP adresi ile eşleşen e-posta sunucusu, tüm posta sunucularından gelen e-postaları kabul edebilir hale gelir. Birinci örnek ile aynıdır.)

conduit permit tcp host 240.18.186.2 eq 143 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq 143 192.168.2.0 255.255.255.224

(Bu komut satırı; sadece yerel ağ kullanıcılarının ve uzak alan ağları kullanıcılarının, yerel e-posta sunucusuna bir e-posta istemcisi programı ile bağlantı sağladığı durumlarda IMAP protokolünü kullanabilme yetkilerini veren komut satırıdır)

conduit permit tcp host 240.18.186.2 eq 110 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq 110 192.168.2.0 255.255.255.224

(Bu komut satırı; sadece yerel ağ kullanıcılarının ve uzak alan ağları kullanıcılarının, e-posta istemci programlarının e-posta sunucusuna bağlanabilmesini, posta alıp gönderebilmesini sağlayan POP3 protokolünü kullanarak posta sunucusuna erişebilmelerini sağlayan komut satırıdır.)

conduit permit tcp host 240.18.186.3 eq http any

(Bu komut satırı; yerel web sunucusunda barındırılan web sitelerine herhangi bir istemciden ulaşılabilmesi kuralını belirleyen komut satırıdır.)

conduit permit tcp host 240.18.186.3 eq ftp 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq ftp 192.168.2.0 255.255.255.224

(Bu komut satırı ise; yerel web sunucusunda barındırılan web sitelerine dosya transferi yapabilme hakkının (ftp) sadece yerel ağ ortamında ve uzak alan ağları ortamında bulunan istemcilerde olduğu kuralını belirleyen komut satırıdır.)

Uygulamada yine Pix serisi güvenlik duvarı cihazının yerel ağ kullanıcıları için kural tanımlaması sağlayan *"outbound"* komutu kullanılmıştır.

Güvenlik Duvarı üzerinde yapılan düzenlemeler;

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 240.18.186.3 netmask 255.255.255.255
outbound 1 permit 192.168.2.0 255.255.255.224 25 tcp 240.18.186.2 netmask 255.255.255.255
outbound 1 permit 192.168.2.0 255.255.255.224 110 tcp 240.18.186.2 netmask 255.255.255.255
outbound 1 permit 192.168.2.0 255.255.255.224 143 tcp 240.18.186.2 netmask 255.255.255.255

Yukarıdaki konfigürasyon satırlarında yerel ağda bulunan kullanıcıların diğer ağlara ve internet ortamına doğru oluşturacakları trafiği sınırlarını belirleyen satırlardır. Buna göre yerel ağ kullanıcıları istedikleri herhangi bir web sitesini ziyaret edebilir, sadece yerel web sunucusuna dosya transferi (ftp) sağlayabilir ve sadece yerel e-posta sunucusu üzerinden e-posta gönderebilir ve alabilirler. Aynı kurallar aşağıda, uzak alan ağlarında bulunan kullanıclar için yapılan tanımlamarda da geçerlidir. Dolayısıyla güvenlik duvarı cihazı üzerinde tanımlanan kurallar uzak alan ağlarındaki kullanıcılar için de geçerlidir.

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 240.18.186.3 netmask 255.255.255.255
outbound 2 permit 192.168.1.64 255.255.255.192 25 tcp 240.18.186.2 netmask 255.255.255.255
outbound 2 permit 192.168.1.64 255.255.255.192 110 tcp 240.18.186.2 netmask 255.255.255.255

outbound 2 permit 192.168.1.64 255.255.255.192 143 tcp 240.18.186.2 netmask 255.255.255.255

Yukarıdaki konfigürasyon satırlarına göre Fakülte-1 ağında bulunan kullanıcıların diğer ağlara ve internet ortamına doğru oluşturacakları trafiği sınırlarını belirleyen satırlardır. Buna göre Fakülte-1 ağında bulunan kullanıcılar istedikleri herhangi bir web sitesini ziyaret edebilir, sadece yerel web sunucusuna dosya transferi (ftp) sağlayabilir ve sadece yerel e-posta sunucusu üzerinden e-posta gönderebilir ve alabilirler. Yerel Ağ kullanıcıları için uygulanan kurallar aynen Fakülte-1 ağında bulunan kullanıcılar için de geçerlidir.

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 240.18.186.3 netmask 255.255.255.255
outbound 3 permit 192.168.1.128 255.255.255.192 25 tcp 240.18.186.2 netmask 255.255.255.255
outbound 3 permit 192.168.1.128 255.255.255.192 110 tcp 240.18.186.2 netmask 255.255.255.255
outbound 3 permit 192.168.1.128 255.255.255.192 143 tcp 240.18.186.2 netmask 255.255.255.255

Fakülte-2 ağında bulunan kullanıcılar için, aynı kurallar yukarıdaki konfigürasyon satırlarında belirtilmiştir.

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 240.18.186.3 netmask 255.255.255.255
outbound 4 permit 192.168.1.192 255.255.255.192 25 tcp 240.18.186.2 netmask 255.255.255.255

outbound 4 permit 192.168.1.192 255.255.255.192 110 tcp 240.18.186.2 netmask 255.255.255.255
outbound 4 permit 192.168.1.192 255.255.255.192 143 tcp 240.18.186.2 netmask 255.255.255.255

Yüksekokul ağında bulunan kullanıcılar için, aynı kurallar yukarıdaki konfigürasyon satırlarında belirtilmiştir.

Yetkilendirme tanımları;

conduit permit tcp host 240.18.186.2 eq 143 any 192.168.1.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq 143 any 192.168.2.0 255.255.255.224

Yukarıdaki konfigürasyon satırında 240.18.186.2 IP adresine sahip e-posta sunucusuna e-posta istemci programı kullanarak 192.168.1.0/24 ağındaki kullanıcılar yani uzak alan ağlarında bulunan kullanıcılar IMAP protokolü ile erişim sağlayabilirler. Aynı zamanda 192.168.2.0/29 ağında bulunan yani merkez yerel ağ ortamında bulunan kullanıclar da erişim sağlayabilirler.

conduit permit tcp host 240.18.186.2 eq 25 any

Yukarıdaki konfigürasyon satırında e-posta sunucusuna herhangi bir e-posta sunucusundan gelen e-postaların alınabilmesi için gerekli tanımlama yapılmıştır. E-posta sunucusu diğer tüm sunuculardan gelen e-postaları alabilmelidir.

conduit permit tcp host 240.18.186.2 eq 110 192.168.2.0 255.255.255.0
conduit permit tcp host 240.18.186.2 eq 110 192.168.1.0 255.255.255.224

Yukarıdaki iki konfigürasyon satırında da e-posta sunucusuna hem yerel ağdaki hem de uzak alan ağlarındaki kullanıcıların POP3 ayarlaması kullanarak e-posta istemci programıyla e-posta sunucusuna erişebilmelerine izin veren tanımlama yapılmıştır.

conduit permit tcp host 240.18.186.3 eq http any

Yukarıdaki konfigürasyon satırında da yerel web sunucusuna herhangi bir kaynaktan her hangi bir istemcinin erişim sağlayabilmesine izin veren tanımlama yazılmıştır.

6. 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 hangi yönde ilerleyen trafik için hangi uygulamaların yetkilendirilmiş olduğunun tanımlanmasıdır.

Güvenlik duvarı, sadece Internete karşı yerel ağların güvenlik altına alınmasını sağlamak için kullanılırsa fonksiyonlarını tam olarak kullanıyor 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 güvenliği 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 yazılımları güncellemeleri sürekli takip

edilmeli, tüm kullanıcı ve sunucular için belirlenen politikalar geçerli olmalı ve gerekli olan tüm trafiğin izlemesi sağlanmalıdır. Ayrıca çok çabuk yayılan ve ağa büyük ölçüde zarar verebilen truva atı, virüs, solucan gibi sistemi kötü yönde etkileyen zararlı programlar için de büyük 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 performanslı ve güvenli olması için politikaların, kurtarma planlarının ve tasarımın mükemmele yakın olması gerekmektedir.

KAYNAKLAR

Kaplan, Y. (2000) Network Veri Haberleşmesi Uygulamaları, **Papatya Yayıncılık**, İstanbul, 376s.

Stallings, W. (1999) Cryptography and Network Security, **Prentice Hall**, New Jersey, 681s.

Stallings, W. (2000) Network Security Essentials, **Prentice Hall**, New Jersey, 409s.

WEB_1. (2003). Bilişim Rehberi. http://www.bilisimrehber.com.tr/tr_white.phtml (10.08.2005).

WEB_2. (2005). Bilgisayar Dershanesi. http://www.bilgisayardershanesi.com/aglardaguvenlik1.htm#top (10.08.2005).

WEB_3. (2005). Datamarket. http://www.datamarket.com.tr/int_guvenlik_coz.html (10.08.2005).

WEB_4. (2005). BNT: Bussiness Network Technologies. http://www.bnt.com.tr/wan.php (10.08.2005).

ÖZGEÇMİŞ

Adi, Soyadı : Süleyman ALTAN

Ana Adı : Firdevs

Baba Adı : Celal

Doğum Yeri ve Tarihi : Denizli, 1979

Lisans Eğitimi ve mezuniyet tarihi : Pamukkale Üniversitesi Elektrik ve Elektronik Mühendisliği, 2000

Çalıştığı Yer : Samur Bilişim Ürünleri Ltd. Şti

Yabancı Dil bilgisi : İngilizce

Mesleki Etkinlikleri :

- S. Altan. Güvenlik Semineri, Bilgi Teknolojileri Kongresi, Mayıs 2003
- S. Altan. Kampüs Ağları ve İstenmeyen Trafik, İnternet Haftası Etkinlikleri, Nisan 2004
- S. Altan. Pamukkale Üniversitesi Kampüs Ağı Altyapısı ve Gelişimi Semineri, Bilgi Teknolojileri Kongresi,Mayıs 2004
- S. Altan. Temel Network Eğitimleri, PAÜSEM, 2002-2005