Yerleşke Ağ Güvenliği ve Yönetimi

Hüsnü Demir
hdemir at metu.edu.tr
Ağ Destek Grubu
ODTÜ

Özet

Günümüzde kampüs ağları hızla gelişmektedir. Aynı hız ne yazıkki kampüs güvenliği konusunda sağlanamamaktadır. Kampüslerin üniversitelerin merkezleri olmasından ötürü özgürlükçü br yapıda olması güvenlik anlayışında da bazı zorunluluklar getirmektedir. Bunlardan en önemlisi 'herşeye izin ver, gereksizleri kapat' anlayışıdır. Ne yazıkki bu anlayışın getirdiği pekçok güvenlik açığı kampüslerimizi kötü etkilemektedir.

Kampüs içerisinde alınabilecek bazı önlemler mevcuttur. Belki bu önlemlerin en önemlisi kalifiye eleman ihtiyacının karşılanmasıdır. Bundan sonra gerekli dökümantasyonun sağlanması ve trafik izlerinin takip edilebilir olmasıdır.

Kampüs dış bağlantılarının kontrol altına alınması bir başlangıç noktası olmalıdır. Dışarıdan gelen saldırılara karşı bir duvar oluşturulmalıdır.

Kampüs içerisinde ise kampüsün büyüklüğüne göre bir yapı tasarlanmalıdır. Dağıtık kampüslerde her bir kampüs bış bağlantı gibi düşünülebilir. Kampüs katmanlar şeklinde yapılandırılmalıdır.

Kampüs trafiğinin şekli belirlenmeli ve izlenmelidir. Kampüs içerisinde oluşan gereksiz trafik engellenmelidir.

Kampüs içerisine bir adet blackhole sistemi kurulmalıdır. Güvenlik ihlalelerini önceden tespit için HoneyNet uygulaması kullanılmalıdır.

Kampüs içerisinde kullanılan güvenlik birimlerinin/elemanlarının koordinasyonu sağlanmalıdır. Ağ güvenliği sistem güvenliğinden başlamalıdır. P2P yazılımlar sistemlerde kısıtlanmalıdır. Benzer şekilde ICMP trafiği de kısıtlanlamı ve hatta dışarıdan erişim engellenmelidir.

QoS, yani Ağ İletişimi Hizmet Kalitesi, sağlanmalıdır. Bu konuda çalışmalar yapılmalı ve özellikle sınır yönlendiricilerde uygulanmalıdır.

Giriş

Amacımız kampüs ağlarının güvenlğini sağlamak için yapılabilecek bazı çalışmaları sıralamak ve mümkün olduğunca örnek vermeye çalışmaktır. Ayrıca kampüs içerisinde uygulanan bazı standartlardan bahsedilecektir. Bunların çoğu genel nitelikte olmakla beraber, altyapısı için uygun çalışmaların tamamlanmış olması gereklidir.

Kampüs Güvenliği

Politika metni olmayan ağların yönetilmesi düşünülemez. Bu konuda daha önce AB'de yapılan sunumlara başvurmanızı öneririm. Kısaca, yönetilemeyen ağların güvenliğinin sağlanması düşünülemez. Bu yüzden alacağınız tüm güvenlik tedbirleri ve uygulamaları havada kalacaktır. Yapılması gereken ilk iş güvenlik politikasını da içeren bir ağ kullanım politikası oluşturmak ve ilgili çalışmaları yapmaktır.

Kampüs güvenliği sınırda başlar. Bunu ülke güvenliğine de benzetebiliriz. Sınırlarımızdan gelebilecek tüm saldırılara karşı hazırlıklı olmak durumundayız. Peki sınırlarımızı çizmek ülke sınırları gibi zor mudur? Evet. Kampüs sınırları birkaç noktadan oluşmaktadır.

Kampüs sınırları tek başına dış bağlantılardan oluşmaz. Buna uzak bağlantılar ve modem, RAS ve son olarak Wi-Fi bağlantılarını da eklemek yerinde olacaktır. Bu bağlantılar ne yazıkki kampüsü saldırı kaynağı ve/veya hedefi yapmaktadır.

Tüm bu bahsedilen bağlantılar ayrı ayrı ele alınmalı ve incelenmelidir. Esasen sınır yönlendiricide uygulamış olduğunuz politikaların burada da geçerli olduğunu unutmamak gereklidir. Ayrıca bu politikalara bazı eklemeler yapmak gerekecektir.

Ne yazikki son günlerde artan taşınabilir cihazlar nedeniyle güvenlik tehditlerinin yönü değişmiştir. Bundan dolayı tüm taşınabilir cihazlar da sınır içi değil sınır dışı tabir edilmeli ve buna göre uygun politikalar geliştirilmelidir.

Sistem güvenliği ağ güvenliğinin ayrılmaz bir parçasını olmuşturmaktadır. Son zamanlarda pek çok güvenlik firması PC tabanlı çözümler üretmeye başlamıştır. Aynı zamanda windows sistemleri de artık güvenlik duvarı özelliği ile beraber gelmeye başlamıştır. Bu tür sistemler için bir güvenlik duvarı ve virüs aracı edinme koşulu konulmalıdır. Nitekim bazı üreticiler bunu ağ bağlantısını sağlamak için zorunlu kılan yazılımlar üretmektedirler.

ICMP (Internet Control Message Protocol) kısıtlanmalıdır. Bu kısıtlama herşeyi kapsamamalı, bazı önemli ICMP (Echo Reply, Destination Unreachable, Echo Request gibi.) mesaj tiplerine izin verilmelidir. QoS parametreleri ile ICMP şekillendirilmelidir.

Ipv4 dışındaki tüm kullanılmayan protokoller engellenmelidir. Özellikle yeni çıkan Ipv6 protokolü engellenmelidir. Bu protokol pekçok güvenlik açığına neden olabilmektedir. Aynı şekilde her türlü *multicast* (çoğa gönderim) trafiği engellenmeli veya kontrol altında tutulmalıdır. Multicast trafiği pekçok şekilde (bkz http://en.wikipedia.org/wiki/Multicast) olmakla beraber en çok bilineni IP Multicast olarak adlandırılanıdır.

Genelde yapılan bazı saldırıları şöyle sıralıyabiliriz:

Uygulama tabanlı saldırılar; e-posta uygulamaları buna bir örnek teşkil edebilir. Bu uygulamalar trojan ve virüs tehlikeleri içermektedir.

Servis engelleme (Denial of Service, DoS) saldırıları; saldırganın sahte isteklerle saldırmasına denir. Eğer saldırı birden çok saldırgan tarafından geliyorsa dağıtık servis engelleme saldırısı (Distributed DoS) olarak adlandırılır. Bu saldırılar esnasında sunucu cevap veremeyecek derecede yoğun olur ve servis kesintisi yaşanır.

IP Spoofing; IP adreslerinin paketlerde değiştirerek saldırının geldiği IP adresini gizlemekte kullanılır. Bu şekilde sadece 3. Seviye IP adresine göre yapılan güvenlik önlemlerinin aşılması sağlanır.

Şifre saldırısı; bu saldırılar ağ erişimini sağlamak için kullanılan şifreleri ele geçirmek için düzenlenir. Bu saldırı metodundan biri sözlük kullanımı ile gerçekleştirilir.

Güvenlik nedeni ile erşim sınırlandırılması sağlanan tüm kullanıcılar (IP adresler, kullanıcı kodu veya MAC adresi bazında) bilgilendirilmelidir. Bu bilgilendirme web sayfası aracılığı ile olabileceği gibi telefon, e-posta gibi araçlarla da olabilir.

Son olarak alınan tüm güvenlik önlemleri ağ hizmetlerinin kullanımını engellememelidir. Yani kullanılabilir bir ağ olmalıdır. Kimsenin kullanmadığı çok güvenli bir ağ kurmanının bir anlamı olmayacaktır. Dolayısı ile ağ kullanımı ile güvenlik arasında bir orantı oluşturulmalıdır.

Yönetim Sistemi

Yönetim sistemini syslog, kullanıcı onaylama, tek seferlik şifre, ayarların tutulması, sistem yetkilendirme, saldırı tespit ve önleme sistemleri gibi parçalar oluşturmaktadır.

Tüm cihazların yönetiminin tek elden yapılması önem arz etmektedir. Mümkünse bu cihazlara ulaşım için ayrı bir ağ oluşturulması iyi olur. Aynı zamanda bu cihazların ve üzerindeki servislerin çalıştığını takip etmek gerekmektedir. Bunun için bedava yazılımlar (snips, nagios, vb.) olduğu gibi ticari yazılımlarda mevcuttur.

Gelen bilgiler bir ağ yönetim cihazında (NMS) toplanmalı ve gözden geçirilmelidir. Merkezi günlük tutma işi sağlıklı bir şekilde yürütülmelidir. Günlüklerin düzgün tutulması sağlanmalı gerekiyorsa devamlı kontrol edilmelidir. Günlük takibi için bazı betikler hazırlanabilir. Böylece sorun anında müdahale hızlanmış olur. Mesela; sözlük saldırısı uygulayan bir saldırganın denemeleri bu günlük işleme mekanizmaları ile bize bildirilebilir ve biz buna uygun tedbiri zamanında alabiliriz. Syslog bu işlevi (günlük tutma işlevini) rahatlıkla yerine getirmekle beraber syslog-ng uygulaması bu işler için daha kullanışlıdır. Bu uygulama UNIX tabanlı olmasına karşın Windows içinde mevcuttur. Günlük izleme işlemleri için ise logwatcher, swatch gibi uygulamalar kullanışlı olmaktadır.

Özellikle sınır yönlendiricilerden gelen izlerin toplanması ve işlenmesi önem arz etmektedir. Bu iş için genelde flow-tools kullanılmakta ve Cisco'nun geliştirdiği Netflow verileri ile yapılmaktadır. Flow-tools bu iş için kullanışlı bir araçtır.

Sınır Yönlendirici

Sınır yönlendiricilerin akıllı cihazlar olması doğaldır. Bunların Ipv4 yönlendirme yapıyor olaması kaçınılmazdır. Bu cihazlar üzerinde filtreleme yapılabilir olmalıdır. Bu filtreleme 2. seviyeden 7. seviyeye kadar çıkabilir. Tabii istenen nokta 7. seviye filtreleme yapabilmesidir.

Bu noktada düşünülmesi gereken nasıl bir cihaz olacağıdır ki en başta söylediğimiz politika metnine bağımlıdır. Eğer politika metni kişileri (kullanıcıları) yeterince bağlıyorsa konuşlandırılacak cihaz daha sade olacaktır. Eğer yaptırımlar yeterli değil ise bu cihazın güçlü olması, hatta bazı ağlar için çok güçlü olması gerekmektedir.

Üniversitelerin kamu kurumu olmasından dolayı maliyet analizleri yapılmamakta veya çok az yapılmaktadır. Esasen bu analizler ciddi bir şekilde yerine getirilmelidir. Mesela, kaç üniversite harcamış olduğu elektrik masrafını cihaz maliyetlerine yansıtmaktadır?

Kaldığımız yerden devam edersek, sınır yönlendiricilerin en az 4. seviye filtreleme yapması uygundur. Birden fazla dış bağlantıya sahip kampüsler için BGPv4 gereklidir. Tabii yapıya bağlı olarak, böyle kampüsler için yük paylaşımı da gerekli olacaktır. Bunlarda işini bilen teknik elemanlar aracılığı ile kolaylıkla icra edilebilir.

Bazı üreticiler her işi sınır yönlendiriciler üzerinden yapmaktadır. Bu ne yazıkki yukarıda bahsettiğim kampüs ağlarına uymamaktadır. Daha çok 'herşeyi engelle, gerekli olanlara izin ver' mantığına uymaktadır. İlk çerçevede çalışan ağların 'INLINE' olarak çalıştırılması performansı düşürmekte veya çok büyük maliyetler çıkarmaktadır.

Sınır yönlendirici üzerinde güvenlik duvarı bulunması genede istenen bir özelliktir ve çoğunukla da başarılı sonuçlar vermektedir. Özellikle bağlantı izlemeli sistemler (connection tracking) performans sorunu çıkarsalarda güzel sonuçlar vermektedir.

Sınır yönlendirici üzerinde içerden dışarıya ulaşılmasını izin vermek ama eğer içeriden bir istek yok ise dışarıdan içeriye bağlantı kurulmasına izin vermemek çok önemli güvenlik sorunlarını engellemektedir.

Blackhole

Bu sistem kampüs içerisinde dolaşan başıboş paketleri bulmanızı ve tedbir almanızı sağlar. Pek çok ağ virüsü aktif Ipleri öğrenmek için tarama yapar ve bu tarama esnasında kampüs içerisinde yönlendirmesi olmayan Iplere de ulaşmaya çalışır. Böylece blackhole IP yönlendirme işlemi yapılabilir.

Uygun donanımlara sahip bir IDS cihazı blackhole makinesi olarak kullanılabilir. Bu cihazın güvenliğinin sıkı tutulması yararlı olur. Cihaza gelen tüm günlük bilgileri incelenmeli ve ilgili tedbirler alınmalı veya alacak betikler çalıştırılmalıdır. Burada önemli olan diğer bir nokta cihaza ulaşımı aynı arayüzden yapmamaktır.

Bu sistemin kullanılabilir olması için varsayılan yönlendirmenin (default routing) kullanılmaması gerekmektedir. Çünkü varsayılan Varsayılan yönlendirme ayarları yapılan sistemler için ise öneri olarak kullanılmayan IP bloklarını blackhole IP'sine yönlendirmesi önerilebilir. Mesela; tüm ayrılmış olarak tanımlı ağlar (bkz http://www.iana.org/assignments/ipv4-address-space Reserved Networks) bu işlem için kullanılabilir. Aynı zamanda kendi IP bloğunuzda kullanmadığınız IP bloklarını da yönlendirebilirsiniz. Son olarak da genelde virüs kaynağı olan ve Microsoft tarafından kullanılan portları da bu IP'ye yönlendirebilirsiniz.

Benzer bir yöntem son zamanlarda DNS için uygulanmaya başlamıştır. Bu yöntem http://www.bleedingsnort.com/blackhole-dns/ adresinde ayrıntılı olarak anlatılmaktadır.

Kablosuz Ağlar

Kablosuz ağların güvenliği gerçekten büyük bir sorun olarak çıkmaktadır. Bu ağlarda işleyen pekçok cihazın taşınabilir olması güvenlik sorunlarının da başka yerlerden fiziksel olarak taşınmasını sağlamaktadır. Her ne kadar kampüs ağının her girişini kapatıyor olsanızda taşınabilir bilgisayarlarla

gelen tehlikeler ne yazikki içeriden sizi vurabilmektedir. Bunun en çok yaşandığı nokta kablosuz ağ bağlantı noktalarıdır.

Bu bağlantı noktalarının erişimleri iyi bir şekilde düzenlenmeli (mümkünse 802.1X kullanılmalı) ve bu ağlardan gelen paketlerin kampüs dışı gibi güvenlik taramasından geçmesi sağlanmalıdır.

802.1X

Ağa yetkilendirmeli erişimi sağlayan bir yöntemdir. Port tabanlı ağ erşim kontrolü sağlayan bir IEEE standardıdır. Ağa erişmeye çalışan kullanıcıların 2. seviyede kontrollerini yaparak erişimleri yönetir. Bu işlem esnasında RADIUS, LDAP gibi uygulamalar kullanılabilir. Yetkilendirme işlemi EAP-TLS, PEAP gibi yöntemler ile yapılabilmektedir.

Bu yöntemin kullanılabilmesi için fiziksel korumanın da aktif olması önemlidir. Cihazlar üzerindeki port güvenliği ile beraber iyi bir güvenlik sağlayabilen bir yöntemdir. Fakat tüm cihazların bu standardı desteklemesi gerekmektedir. Bu ise maliyeti arttıran bir etken olarak ağ yöneticisinin karşısına çıkmaktadır.

P2P

Peer2Peer olarak adlandırılan ve ağ kaynaklarını yoğun bir şekilde meşgul etmesi ile gündeme gelen bir paylaşım yöntemidir. Bittorrent, emule, edonkey gibi uygulamalar ile hayata geçen paylaşım yöntemlerinin kullanılması özellikle son zamanlarda yoğunlaşmıştır.

Bu uygulamalar pekçok yasal olmayan uygulama, film, müzik, kitap, vb. materyallerin dağıtımında kullanılmaktadır. Genelde bu konu ile gündeme gelen bu uygulamalar son zamanlarda oyun güncellemeleri, linux, bsd gibi işletim sistemlerinin dağıtımında sıklıkla kullanılmaya başlanmıştır. Bu ise bu tür uygulamaların engellenmesinde sıkıntı çıkarmaktadır.

İşin görülmeyen bir yüzü de güvenliktir. Bu tür uygulamalar Internet ortamına bağlı pekçok bilgisayarı saldırılara karşı açık duruma getirmekle kalmıyor, indirilen uygulamaların denenmesi ile ortaya çıkan virüs, worm gibi pekçok güvenlik sıkıntılarına neden olmaktadır. Kısaca bu tür uygulamalar doğal birer truva atı niteliğinde çalışmakta ve pekçok sistemin kolaylıkla ele geçirilmesini sağlamaktadır.

Bu nedenlerden ötürü bu tür uyulamalara sıcak bakmak bir güvenlik elemanı için çok hoş olmamaktadır. Diğer yandan pekçok iyi niyetli girişimleri de gözden kaçırmamak ve buna uygun yöntemlerden yararlanmaya çalışmak gereklidir. Mesela; bunlardan biri kullanıcıların çekmey isteyebileceği OS dağıtım sürümlerinin yansılarını önceden hazır etmek gibi.

İzin vermeminin getirdiği maddi zorlukları aşmak için QoS parametreleri kullanılabilir. Örnek vermek gerekirse; snort üzerinde yakalanan IP'lerin ağa erişimleri sınırlandırılabilir. Bunun için QoS tanımları yapılabilen bir cihaz yardımı ile oluşturulan bant genişliği kullanılabilir. Burada kısıtlama yapılamamasının iki önemli nedeni var. İlki akademik dünyada olduğumuzdan kullanıcılarımızı yeni yöntemler geliştirmeye sevk etmemektir. Diğeri ise ağa erşimin esas olmasıdır. Kullanılmayan ağ çok bir işe yaramayacaktır.

Honeypots (Bal küpleri) ve Honeynets

Günümüzde saldırılar pekçok yerden gelmektedir. Kullanıcılarımız yukarıda da anlattığımız gibi sistemlerinde nelerin çalıştığının farkında olmayabiliyor. Bu durum da dışarıdan da içeriden de pekçok

saldırının gelmesine neden olabiliyor. Bu saldırıların önüne geçmek için bunlardan haberdar olmamız gerekmektedir. IDS sistemleri bu işler için ideal yapılardır.

Bu sistemler yalancı bilgiler kullanarak saldırganları üzerine çekmekte ve saldırganlardan pekçok bilgi toplamaktadır. Böylece bu saldırıları engelleyecek yöntemler kurulmasını sağlarlar. Elde edilen bilgiler hızlıca güvenlik duvarında etkin hale getirilebilir.

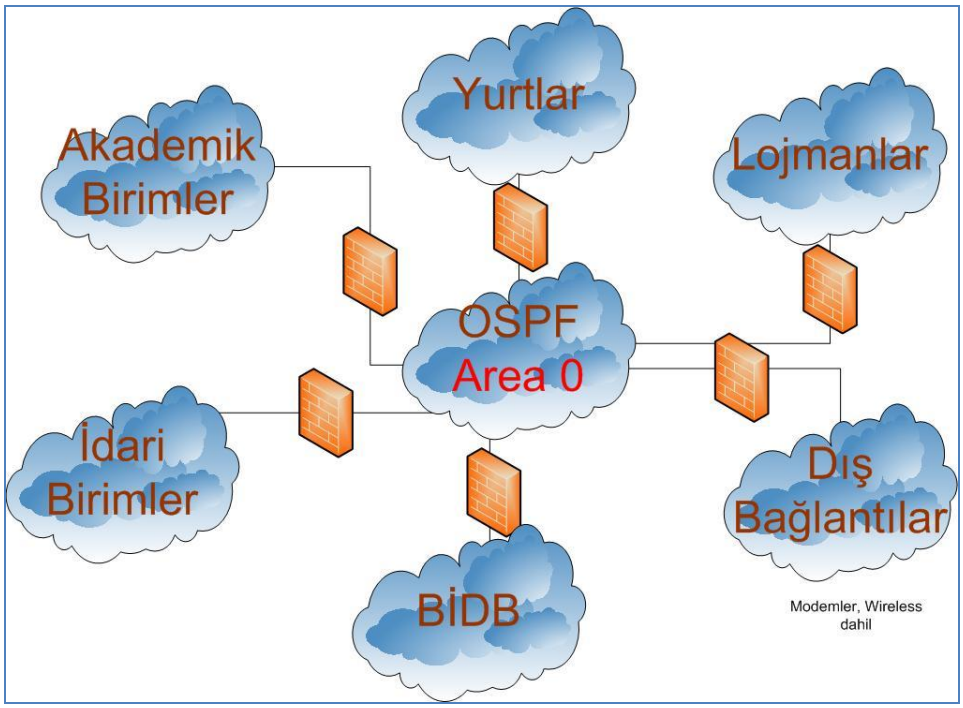
Sistemin ele geçirilmesi pek çok soruna neden olabilir. Bu yüzden gerekli tedbirlerin alınması önemlidir. Genelde gerçek sistemler üzerine kurulan honeypotlar böyle durumlarda daha tehlikeli olabilir.

Örnek vermek gerekirse; sınır yönlendiricinin yakınlarına kurulmuş bir honeypot kendisine gelen tüm bağlantıları saldırı olarak kaydedip gerekli tedbirleri alır. Tarpit (http://labrea.sourceforge.net/) sistemi honeypot için iyi bir örnektir. KFsensor (http://www.keyfocus.net/kfsensor/) ise windows tabanlı bir IDS/honeypot sistemidir. Son olarak da honeyd (http://www.honeyd.org/) örnek verilebilir.

Honeynet ise honeypotların oluşturduğu bir ağa verilen bir isimdir. Bu ağ sayesinde tüm veri kontrolü, veri toplama ve IDS işleri tek elden yapılmaktadır. Bu ayrıca honeypotlardan biri ele geçerse hızlı bir şekilde bulunmasına da yardımcı olur. Honeynetler 2. seviye veya 3. seviyede çalışacak şekilde kurulabilir. İlki diğerine göre daha güvenli bir sistem kurulmasını sağlar.

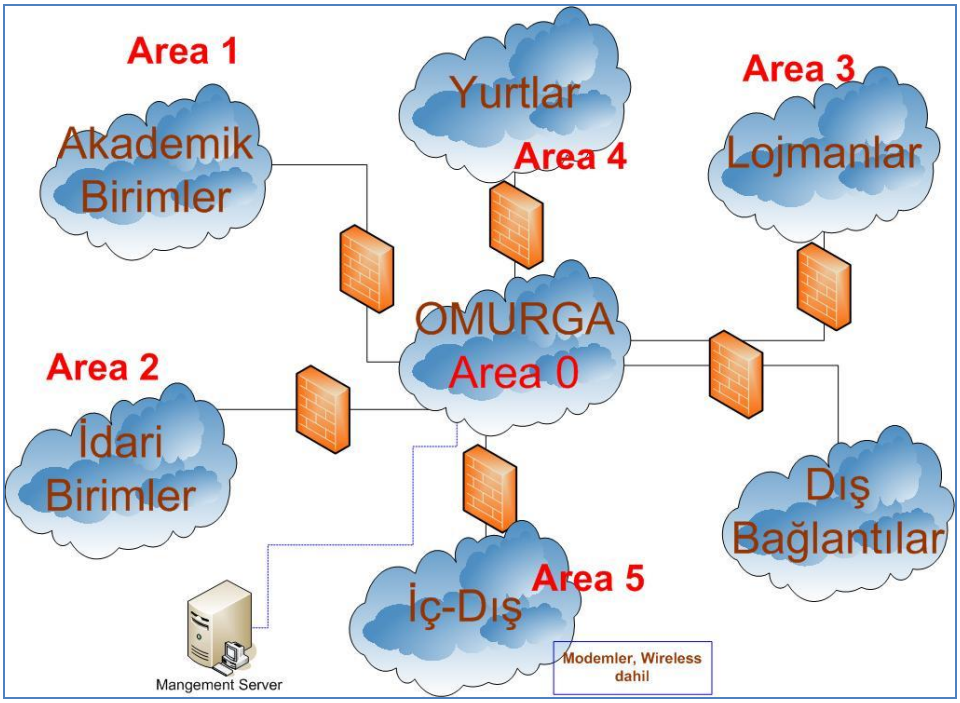
Örnek

Aşağıda olası bir ağ çizimi mevcuttur. Burada OSPF ile 3. seviye merkezi (backbone) ağ kurulmuş ve birimlerin merkezi ağa bağlantıları güvenlik duvarı üzerinden erişmeleri sağlanmıştır.



Çizim 1. Genel şematik kampüs çizimi.

2. çizimde ise her alt bölge ayrıca 3. seviye çalışabilir hale getirilmiştir. Burada yönetim cihazı merkezde bulunmaktadır. Güvenlik duvarları aynı zamanda IPS, IDS olarak da konuşlandırılabilir.



Çizim 2. Genel şematik kampüs çizimi.

Sonuç

Herşeye izin ver mantığı ile çalışan kampüs ağlarının güvenliğinin sağlanması gerçekten zordur. Etkileşimli metodlar ile güvenlik sağlama yöntemleri trafiği çok olan kampüsler için zor olmakta ve maddi açından külfet getirmektedir. Bu tür sistemlerde izle ve tepki ver yöntemi daha yararlı olmaktadır. Bu yöntem içerisinde IDS, honeynet ve sistem yönetimi önemli bir yer tutmaktadır. Devamlı takip altında tutulan bir ağda çıkabilecek sorunlara ve saldırılara karşı gerekli müdahaleler yapılarak sistem güvenli ve sağlıklı çalışır vaziyette tutulabilmektedir. Tabii böyle bir sistemi kurmak ve işletmek için iyi yetişmiş işgücüne ihtiyaç vardır.