

Süleyman Demirel Üniversitesi



Sertaç Selim SARICA

PC Yönlendirici ve Güvenlik Merkezi
Çalışma Grubu

Neden ihtiyaç duyduk?

Ana nedenler:

- Ağ güvenliği
- Kullanıcı denetimi

Diğer nedenler:

- Kullanıcı sayısı/Yetersiz IP adresi
- Dağınık kampüs yapısı
- Maliyet



Neler yapmamız gerekiyordu :

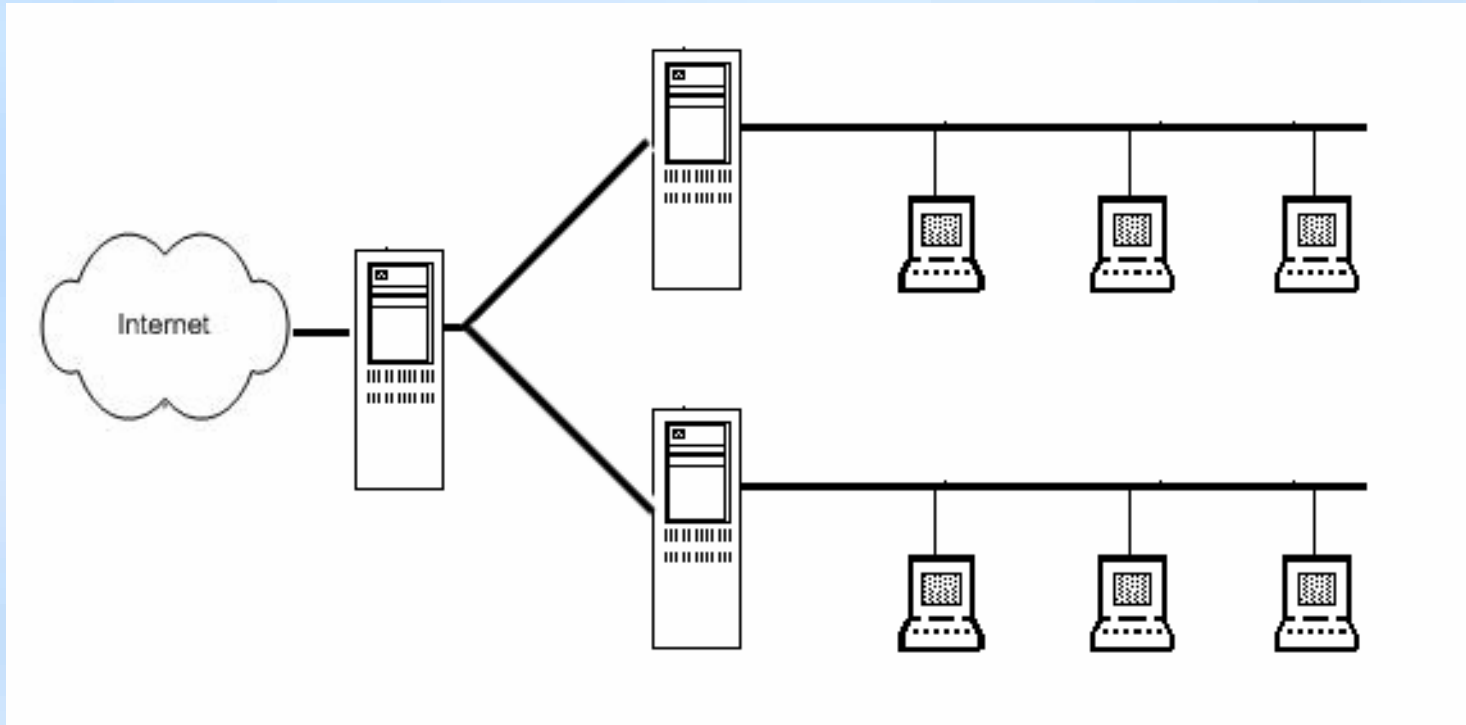
- Kullanıcı denetimini sağlamak
- Kullanıcıları dışarıdan gelen saldırılara karşı korumak
- IP ihtiyacını karşılamak
- Gereksiz ağ trafiğini engellemek



Elimizde neler vardı?

- Bol miktarda PC
- Linux / FreeBSD
- 2,3 adet ethernet kartı
- Bol miktarda kullanıcılar

Ne Planladık?





Kurulum yerlerimiz ?

- Kampüs çıkışı
- Fakülteler
- Öğrenci laboratuvarları
- MYO – Kampüs bağlantısı



Kampüs çıkışı

- Güvenlik Duvarı
- İnternet hızını arttırabilmek için yönlendirmeler. (Transparent Proxy sunucusuna)
- Bant genişliğini ayarlamak
- Kısıtlamalar yapabilecek



Fakülteler

- IP dağıtımı (DHCP)
- Güvenlik Duvarı (iptables)
- Gereksiz ağ trafiğini önlemek (squid – iptable)
- Ağ trafik analizi



Öğrenci laboratuvarları

- IP dağıtımı (DHCP)
- Güvenlik Duvarı (iptables)
- Gereksiz ağ trafiğini önlemek (squid – iptable)
- İstemeyerekte olsa kısıtlamalar
- Ağ trafik analizi



MYO-Kampüs Bağlantısı

- MYO ile Kampüs arasında Frame Relay bağlantısı yapılması gerekiyordu. Bu iş için üzerine E1 kart taktığımız bir Linux PC kullandık.

Neler kullandık?

İşletim Sistemi tercihleri :

- Fakültelerin bir kısmı ve MYO-Kampüs bağlantısında Linux;
- Fakültelerin kalan kısmı ve Öğrenci Labaratuvarlarında yönetim kolaylığı nedeniyle PfSense;
- Kampüs çıkışında; Linux

Neler kullandık?

Kullanılan sunucular :

- Fakülte, öğrenci laboratuvarları ve MYO-Kampüs bağlantısında standart masa üstü PC'ler;
 - * 4,3 Gb ve üstü Harddisk
 - * 2 adet 10/100 ethernet
 - * 64 MB ve üstü RAM
 - * Celeron 300A – P4 2.4 arası değişen işlemciler



Neler kullandık?

- MYO – Kampüs bağlantısını sağlayan PC üzerine ek olarak E1 kart takılarak bağlantı sağlandı.
- Kampüs çıkışında kullanılan PC'de 3 adet ethernet kartı kullanıldı (Proxy-Internet giriş – Internet çıkış)

Sonuç

- P2P uygulamalarının büyük çoğunluğunu denetleyebiliyoruz.
- Sürekli ağ trafiğini denetleyerek gereksiz trafik oluşturan noktalara hızlı müdahale edebiliyoruz.
- Maliyetleri düşürdük
- Ağımız küçük parçalara ayırarak worm botnet vb. trafiği dar alanlara hapsederek tüm kampüse yayılmasını engelliyoruz.

Sonuç

- SNMP-Mrtg ve netstat-nat gibi programlar yardımı ile sorunlu bölgeleri tespit edebiliyoruz. (netstat-nat programının loglarını kaydederek Ağ sorumlusuna e-posta atmasını sağlıyoruz)

