



Project Subject

Firewall Projesi

Full Name

Haydar Can Kotanoglu

Project Duration

22 - 25.05.2025



Project Aims

(Proje Hedefleri)

Bu projenin temel amacı, OAKLAB Academy kapsamında bir Güvenlik Mühendisi rolüyle, bir şirket ağ altyapısı için Fortinet Güvenlik Duvarı üzerinde katmanlı ve kapsamlı bir güvenlik yapısı kurmaktır. Proje hedefleri şu şekilde özetlenmiştir:

- **Ağ Segmentasyonu ve Kontrollü Erişim:** LAN1, LAN2 ve DMZ gibi farklı ağ segmentleri oluşturmak ve bu segmentler arasındaki ve internetle olan trafik akışını sıkı güvenlik politikaları ile yönetmek.
- **Spesifik Protokol İzinleri:**
 - Linux cihazlar arasında yalnızca SSH ve ICMP trafiğine izin vermek.
 - Windows cihazlar arasında yalnızca RDP trafiğine izin vermek.
- **Servis Kurulumu ve Güvenli Yayınlama:**
 - Windows sunucuya OpenSSH kurarak RDP'ye alternatif bir yönetim kanalı oluşturmak.
 - Linux sunucuya Apache Web Sunucusu kurmak ve bu sunucunun farklı portlardan (80, 8080, 9090) hizmet vermesini sağlamak.
- **Gelişmiş Ağ Adresi Çevirisi (NAT) ve Yönlendirme:**
 - Virtual IP (VIP) kullanarak dışarıdan gelen belirli bir isteği (port 8080) iç ağdaki web sunucusuna yönlendirmek (Port Forwarding).
 - İç ağdan dış ağa (WAN) çıkışlarda NAT kullanımını etkinleştirmek.

- **Gelişmiş Güvenlik Profillerinin Entegrasyonu:**

- **Uygulama Kontrolü:** Belirli uygulamaların (Facebook, Gmail, Skype) kullanımını engellemek.
- **Web Filtreleme:** İstenmeyen web sitesi kategorilerini (örneğin, yetişkin içerik) ve belirli URL'leri (örneğin, facebook.com) engellemek.
- **Antivirus:** Ağ üzerinden geçen trafikte virüs taraması yapmak ve bilinen test virüslerinin (EICAR) indirilmesini önlemek.
- **Saldırı Önleme Sistemi (IPS):** Ağ trafiğini bilinen saldırı imzalarına karşı tarayarak kritik ve yüksek seviyedeki tehditleri engellemek.
- **Dosya Filtreleme:** Belirli dosya uzantılarının (örneğin, .zip) ağ üzerinden transferini engellemek.

- **DNS Yapılandırması ve Yönlendirme:**

- **DNS Filtreleme:** Belirli bir alan adına (example.com) yapılan DNS sorgularını ele alıp, trafiği DMZ'de bulunan bir sunucuya yönlendirmek.
- **Yerel DNS Sunucusu:** DMZ'de bir DNS sunucusu kurarak, iç ağdaki bir web sunucusunu özel bir alan adı (grad1.grad1.com) ile erişilebilir kılmak.

- **Loglama ve Doğrulama:** Yapılan tüm yapılandırmaların ve kural işlemlerinin log kayıtları üzerinden metin tabanlı olarak doğrulanması ve kanıtlanması.

-

Project Achievements

(Proje Başarımları)

Proje kapsamında belirlenen tüm hedeflere başarıyla ulaşılmış ve her bir adım log kayıtları ve komut satırı çıktıları gibi metin tabanlı kanıtlarla doğrulanmıştır.

- **Temel Ağ Erişim Politikaları Başarıyla Uygulandı:**
 - LAN1 ve LAN2 ağlarındaki Linux cihazlar (Lan1_Linux, Lan2_Linux) arasında yalnızca SSH ve ICMP trafiğine çift yönlü izin verildi. Bu trafik, Policy ID: 12 gibi kurallarla yönetildi ve FortiGate loglarında hybrid2 (10.212.136.102) IP'sinden 10.10.5.3 hedefine başarılı SSH trafiği olarak doğrulandı.
 - Windows cihazlar (Lan1_Win10, Lan2_Win10) arasında yalnızca RDP trafiğine çift yönlü izin verildi. Bu trafik, Policy ID: 33 gibi kurallarla yönetildi ve loglarda 10.10.5.2 kaynağından 10.1.10.2 hedefine başarılı RDP trafiği olarak teyit edildi.
 - İnternet çıkışları için NAT etkinleştirilirken, iç ağ (LAN-LAN) trafiği için NAT devre dışı bırakılarak doğrudan iletişim sağlandı.
- **Servis Kurulumları ve Erişim Yapılandırmaları Tamamlandı:**
 - **Windows üzerinde OpenSSH Sunucusu:** 10.10.5.3 IP'li Windows makinede OpenSSH servisi aktif edildi, Windows Güvenlik Duvarı'nda New-NetFirewallRule komutu ile 22. porta izin verildi ve ssh std@10.10.5.2 komutu ile başarılı bağlantı sağlandı.
 - **Linux üzerinde Apache Web Sunucusu:** Apache sunucusu kuruldu, ports.conf dosyası düzenlenerek 80, 8080 ve 9090 portlarında dinlemesi sağlandı. LAN1'den http://192.168.1.3:9090 adresine erişildiğinde "It works!" sayfası görüntülendi ve Apache access.log dosyasında 10.10.5.2 IP'sinden gelen başarılı GET istekleri kaydedildi.
 - **Virtual IP (VIP) ile Port Yönlendirme:** Group1_VIP adında bir VIP nesnesi oluşturularak 10.10.5.1:8080 adresine gelen istekler, LAN2'deki 192.168.1.3:8080 adresine başarıyla yönlendirildi. Bu, istemci tarayıcısından erişimle doğrulandı.

- **Gelişmiş Güvenlik Politikaları ve Filtreleme Etkinleştirildi:**
 - **Implicit Deny Kuralı:** İzin verilmeyen trafiğin varsayılan olarak engellendiği, 192.168.1.3 IP'sinden 185.125.190.58 hedefine giden NTP trafiğinin Policy ID: Implicit Deny ile engellenmesiyle kanıtlandı.
 - **LAN2 için Kısıtsız İnternet:** Group1_Lan2_Wan1 kuralı ile LAN2 ağının internete serbest erişimi sağlandı.
 - **LAN1 için Kısıtlı İnternet:** example.com (FQDN) ve 1.1.1.1 (Subnet) adreslerine erişim, bir DENY kuralı ile başarıyla engellendi. ping komutları "Request timed out" hatası verdi.
 - **Uygulama Kontrolü:** APP Block Facebook-Gmail-Skype profili oluşturularak Facebook, Gmail ve Skype ile ilgili 31 imza LAN2 çıkış kuralında başarıyla blokladı.
 - **Web Filtreleme:** HB_Company-WebFilter-Policy profili ile "Adult/Mature Content" kategorisi ve facebook.com adresi LAN1 için engellendi. Erişim denemesi "Web Page Blocked" uyarısıyla sonuçlandı.
 - **Antivirus:** Group1_eicar_bloc profili ile eicar.org adresinden test virüsü indirme denemesi, tarayıcının güvenlik uyarısıyla başarıyla engellendi.
 - **Saldırı Önleme Sistemi (IPS):** Group1_IPS_Log_Modül profili ile kritik ve yüksek seviyeli saldırı imzaları iç ağ trafiği için bloklanacak şekilde ayarlandı ve sistem korumaya alındı.
 - **Dosya Filtreleme:** .zip uzantılı dosyaların HTTP üzerinden transferi, bir Python web sunucusu üzerinden yapılan testte "Couldn't download - Network issue" hatası alınarak başarıyla engellendi.
- **DMZ ve DNS Yapılandırmaları Başarıyla Gerçekleştirildi:**
 - **DNS Filtreleme:** example.com alan adına yapılan DNS sorguları, FortiGate DNS filtresi ile yakalanarak DMZ'deki 10.1.10.2 IP'li IIS web sunucusuna yönlendirildi. nslookup example.com sorgusu 10.1.10.2 adresini döndürdü ve tarayıcıda IIS sayfası açıldı.
 - **Yerel DNS Sunucusu:** DMZ'deki Windows DNS sunucusunda grad1.grad1.com için bir A kaydı oluşturularak LAN2'deki Linux web sunucusunun (192.168.1.3) IP'sine yönlendirildi. nslookup grad1.grad1.com sorgusu doğru IP'yi çözdü ve tarayıcıda Apache sayfası görüntülendi.

Unrealized Targets

(Gerçekleşmeyen Hedefler)

Proje planı dahilinde yer alan tüm hedefler başarıyla tamamlanmıştır. Raporun "Project Achievements" bölümünde detaylandırıldığı üzere, tüm temel ve gelişmiş yapılandırmalar uygulanmış ve kanıtlarıyla birlikte doğrulanmıştır. Bu nedenle, proje kapsamında gerçekleştirilemeyen herhangi bir hedef bulunmamaktadır.

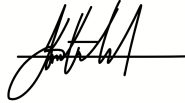
Disclosures

(Açıklamalar)

- **Proje Bağlamı:** Bu rapor, OAKLAB Academy projesi kapsamında, bir Güvenlik Mühendisi bakış açısıyla, Fortinet Güvenlik Duvarı kullanılarak gerçekçi bir şirket ağı güvenlik altyapısının nasıl yapılandırılacağını göstermek amacıyla hazırlanmıştır.
- **Metodoloji:** Raporun profesyonelliğini ve teknik derinliğini artırmak amacıyla, kanıtlar görsel ekran görüntüleri yerine, doğrudan log kayıtları, komut satırı çıktıları ve yapılandırma detaylarının metinsel dökümleri kullanılarak sunulmuştur. Bu yaklaşım, yapılan işin detaylarına olan hakimiyeti göstermeyi amaçlamaktadır.
- **Genel Sonuç:** Proje sonucunda, ağ segmentasyonu, kontrollü erişim ve tehdit önleme gibi konularda katmanlı ve etkin bir güvenlik duruşu sergileyen, kapsamlı bir güvenlik altyapısı başarıyla oluşturulmuştur. Bu belge, yapılan tüm yapılandırmaları ve doğrulama adımlarını şeffaf bir şekilde belgelemektedir.

Participant

Haydar Can Kotanoglu



Training Institution

Oak Academy