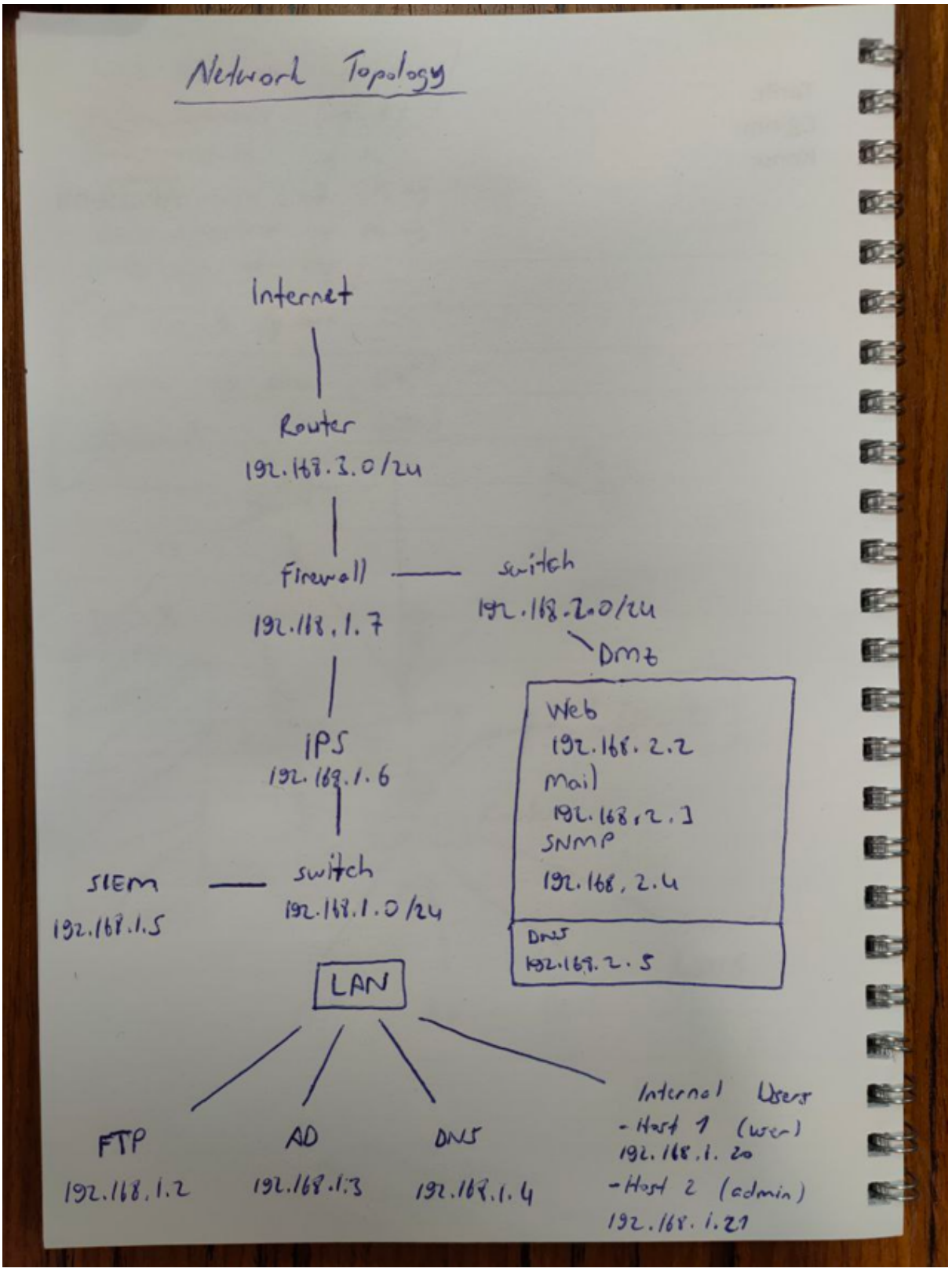
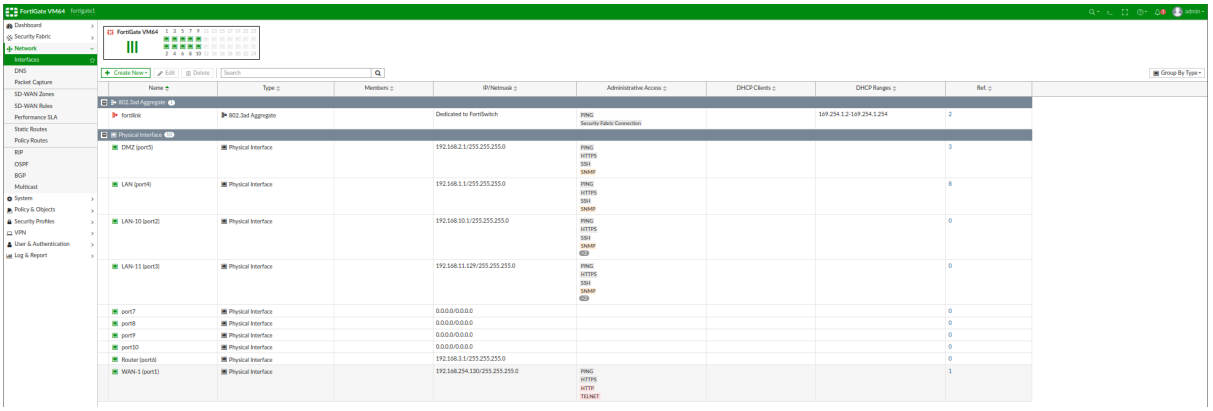
Firewall Uygulama Projesi (Fortigate)

Ağ Topolojisi

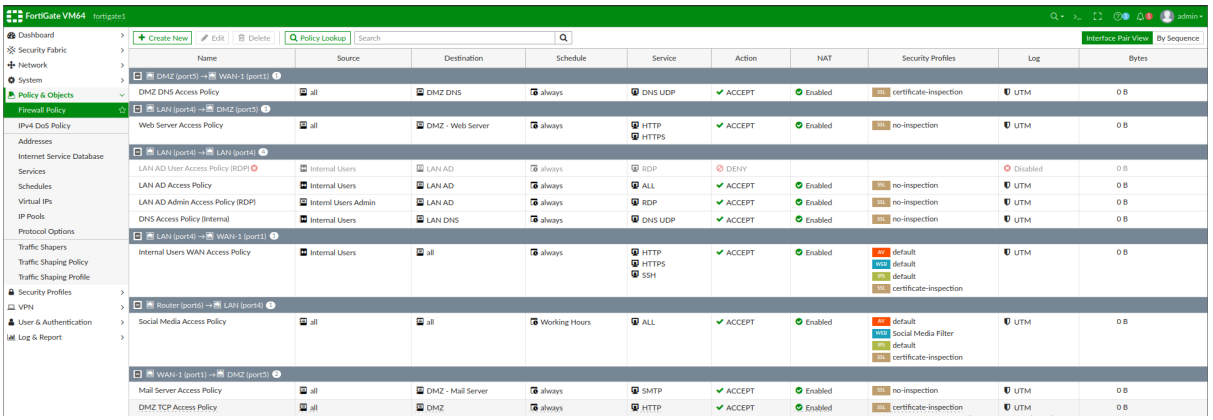


Network Interfaces (Ağ Arayüzleri)

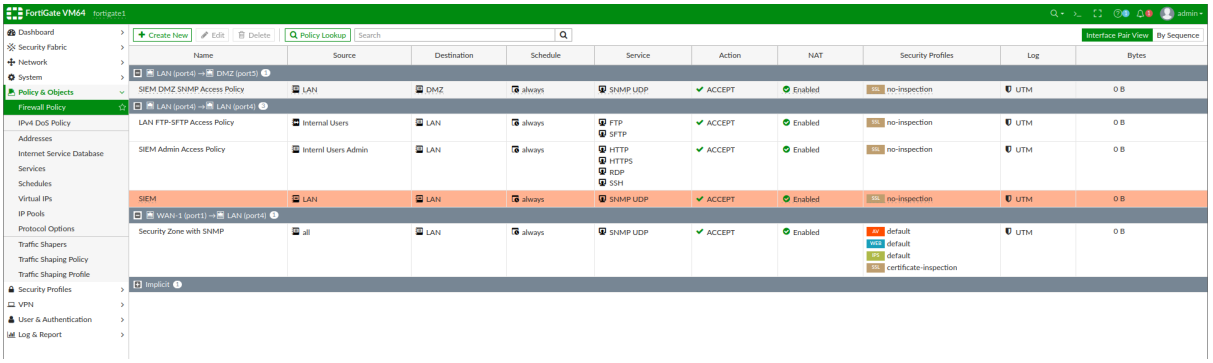


FW Erişim Politikaları

1) Sosyal medyaya erişim kısıtlıdır, sadece öğlen arası veya mesai saatleri dışında girilebilir.
2) herhangi bir yerden web sunucunun web portlarına (80,443) erişilebilir
3) her yerden mail sunucunun smtp portuna erişilebilir
4) iç ağdaki AD sunucuna iç ağdaki kullanıcılar erişebilecektir.
5) iç ağdaki AD suncunun yönetim portalrına (RDP) sadece admin kullanıcıları erişebilir.
6) iç ağdaki DNS sunucuna sadece iç ağdaki kullanıcılar erişebilecektir.
7) DMZ ağındaki dış DNS sunucusuna dns (udp/53) ile dışarıdan erişilebilecektir.
8) DMZ ağındaki streaming sunuculara , 80/tcp portu ile her yerden erişilebilecektir.
9) iç ağdaki kullanıcılar dışarıya http,https,ssh servislerine bağlanabilecektir.
10) iç ağdaki kullanıcılar dışarıya çıkarken antivirüs, içerik filtreleme, IPS ile kontrol edilecektir.
11) Güvenlik bölgesindeki SIEM sunucusuna iç ağdaki admin kullanıcıları (RDP, http,https,SSH) portlar üzerinden erişebilir
12) Güvenlik bölgesindeki SIEM sunucusuna DMZ bölgesindeki WEB, Mail, DNS sunucuları SNMP (udp/161) ile erişebilir
13) Güvenlik bölgesindeki SIEM sunucusuna iç ağdaki AD,FTP,iç DNS sunucusu SNMP (udp/161) ile erişebilir
14) Güvenlik bölgesindeki SIEM sunucusuna güvenlik duvarı SNMP(udp/161) ile erişebilir.
15) iç ağdaki FTP sunucusuna sadece iç ağdaki kullanıcılar ftp,Sftp servisleri ile bağlanabilir



10 kuraldan fazlasını kabul etmediği için hepsini silip kalan kısmı ekledim.



Faruk Ulutaş