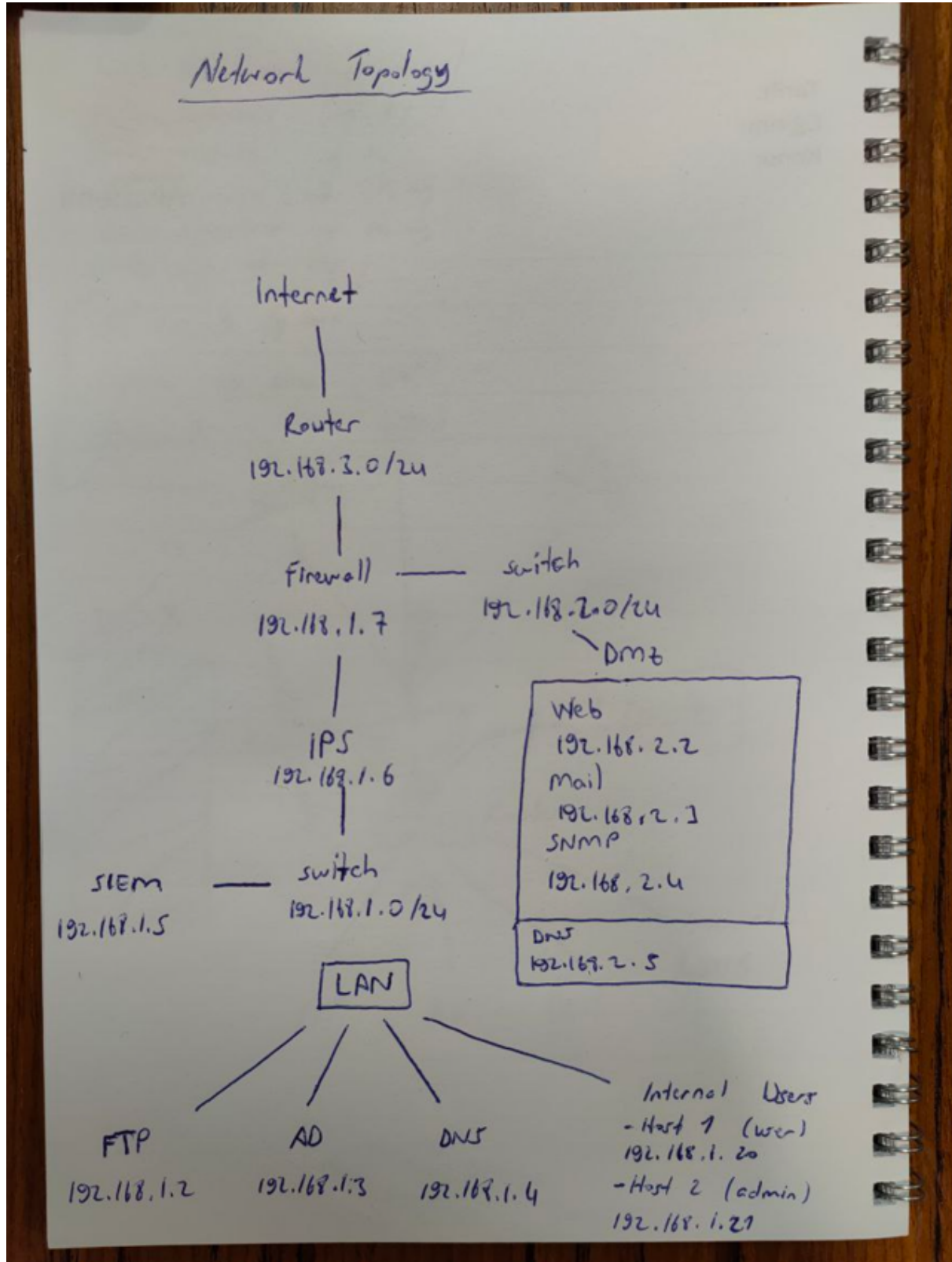


Firewall Uygulama Projesi (Fortigate)

Ağ Topolojisi



Network Interfaces (Ağ Arayüzleri)

Name	Type	Members	IP/Network	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Port0 (port0)	Physical Interface		192.168.1.1/255.255.255.0	FWG Security Profiles Connected		192.254.1.2-192.254.1.254	2
Port1 (port1)	Physical Interface		192.168.1.1/255.255.255.0	FWG HTTP SSH SNMP			3
Port2 (port2)	Physical Interface		192.168.1.1/255.255.255.0	FWG HTTP SSH SNMP			6
Port3 (port3)	Physical Interface		192.168.1.1/255.255.255.0	FWG HTTP SSH SNMP			0
Port4 (port4)	Physical Interface		192.168.1.1/255.255.255.0	FWG HTTP SSH SNMP			0
Port5 (port5)	Physical Interface		0.0.0.0/0.0.0.0				0
Port6 (port6)	Physical Interface		0.0.0.0/0.0.0.0				0
Port7 (port7)	Physical Interface		0.0.0.0/0.0.0.0				0
Port8 (port8)	Physical Interface		0.0.0.0/0.0.0.0				0
Port9 (port9)	Physical Interface		192.168.1.1/255.255.255.0	FWG HTTP SSH SNMP			0
Port10 (port10)	Physical Interface		192.168.254.120/255.255.255.0	FWG HTTP HTTP TELNET			1

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 sunucunun yönetim portalına (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

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
DMZ DNS Access Policy	all	DMZ DNS	always	DNS UDP	ACCEPT	Enabled	certificate-inspection	UTM	0 B
Web Server Access Policy	all	DMZ - Web Server	always	HTTP HTTPS	ACCEPT	Enabled	no-inspection	UTM	0 B
LAN AD User Access Policy (RDP)	Internal Users	LAN AD	always	RDP	DENY			Disabled	0 B
LAN AD Admin Access Policy (RDP)	Internal Users	LAN AD	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
LAN AD Admin Access Policy (RDP)	Internal Users	LAN AD	always	RDP	ACCEPT	Enabled	no-inspection	UTM	0 B
DNS Access Policy (Internal)	Internal Users	LAN DNS	always	DNS UDP	ACCEPT	Enabled	no-inspection	UTM	0 B
Internal Users WAN Access Policy	Internal Users	all	always	HTTP HTTPS SSH	ACCEPT	Enabled	default no-inspection default certificate-inspection	UTM	0 B
Social Media Access Policy	all	all	Working Hours	ALL	ACCEPT	Enabled	default Social Media Filter default certificate-inspection	UTM	0 B
Mail Server Access Policy	all	DMZ - Mail Server	always	SMTP	ACCEPT	Enabled	no-inspection	UTM	0 B
DMZ TCP Access Policy	all	DMZ	always	HTTP	ACCEPT	Enabled	certificate-inspection	UTM	0 B

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

FortiGate VM64 - FortiOS 6.4.0										
Create New Edit Delete Policy Lookup Search Interface Pair View By Sequence										
Name Source Destination Schedule Service Action NAT Security Profiles Log Bytes										
Policy & Objects	LAN (port4) → DMZ (port2)	LAN	DMZ	always	SNMP UDP	ACCEPT	Enabled	no-inspection	UTM	0 B
	SIEM DMZ-SNMP Access Policy	LAN	DMZ	always	SNMP UDP	ACCEPT	Enabled	no-inspection	UTM	0 B
	LAN (port4) → LAN (port4)	LAN	LAN	always	FTP SFTP	ACCEPT	Enabled	no-inspection	UTM	0 B
	LAN FTP-SFTP Access Policy	Internal Users	LAN	always	FTP SFTP	ACCEPT	Enabled	no-inspection	UTM	0 B
	SIEM Admin Access Policy	Internal Users Admin	LAN	always	HTTP HTTPS SSH	ACCEPT	Enabled	no-inspection	UTM	0 B
Firewall Policy	LAN (port4) → LAN (port4)	LAN	LAN	always	SNMP UDP	ACCEPT	Enabled	no-inspection	UTM	0 B
	SIEM	LAN	LAN	always	SNMP UDP	ACCEPT	Enabled	no-inspection	UTM	0 B
IPv4 DoS Policy	WAN-1 (port1) → LAN (port4)	all	LAN	always	SNMP UDP	ACCEPT	Enabled	default	UTM	0 B
	Security Zone with SNMP	all	LAN	always	SNMP UDP	ACCEPT	Enabled	default	UTM	0 B
Implicit										
Security Profiles										
VPM										
User & Authentication										
Log & Report										

Faruk Ulutaş