Overview

The following document outlines the results of a comprehensive audit of our network topology. Each table below details the necessary inbound and outbound network services required for each host to perform its designated business function. This list will serve as the foundation for building our perimeter and internal firewall security policies based on the principle of least privilege.

Please note that for direction, it will be listed as either “I”, “O”, or “I/O” which indicates the direction of traffic as inbound, outbound, or both onto that device through the specified service/port.

Palo Alto Segment

Palo Alto Firewall

Direction	Service/Application	Destination / Source	Network Scope	Notes / Justification
I	HTTPS/SSH (Management)	Admin Workstations	Internal	For authorized administrator access.
O	DNS	AD/DNS Server	Internal	To resolve hostnames for updates and threat intelligence feeds.
O	NTP	Internet	External	To ensure accurate time for logs and certificates.
O	Palo Alto Updates	Internet	External	To receive the latest software, threat, and application signatures.

Ecom (Ubuntu 24)

Direction	Service/Application	Destination / Source	Network Scope	Notes / Justification

I	web-browsing, ssl	External & Internal Clients	External & Internal	To serve the e-commerce website to customers and internal users.
O	DNS	AD/DNS Server	Internal	To resolve internal and external hostnames.
O	ms-ds-non-rpc (AD Auth)	AD/DNS Server	Internal	For user authentication against Active Directory.
O	splunk-forwarding	Splunk Server	Internal	To send application and system logs to the SIEM.

Webmail (Fedora 42)

Direction	**Service/Application**	**Destination / Source**	**Network Scope**	**Notes / Justification**
I	ssl (Webmail)	External & Internal Clients	External & Internal	To provide secure webmail access.
O	DNS	AD/DNS Server	Internal	To resolve internal and external hostnames.
O	ldap, kerberos	AD/DNS Server	Internal	For user authentication against Active Directory.
O	Syslog/SPLUNK FORWARDING	Splunk Server	Internal	To forward system logs to the Splunk SIEM.

Splunk (Oracle 9)

Dire	**Service/Application**	**Destination / Source**	**Network Scope**	**Notes / Justification**

cti on				
I	splunk-web (TCP 8000)	Admin Workstations	Internal	For administrator access to the Splunk management interface.
I	splunk-forwarding, syslog	All Internal Servers	Internal	To receive logs from all devices on the network.
O	DNS	AD/DNS Server	Internal	To resolve hostnames for updates.

Wkst (Ubuntu 24)

Direction	Service/Application	Destination / Source	Network Scope	Notes / Justification
O	DNS	AD/DNS Server	Internal	To resolve hostnames for browsing and updates.
Outbound	web-browsing, ssl	Internal Servers & Internet	Internal & External	To access internal web services and the general internet.
O	splunk-forwarding	Splunk Server	Internal	To forward endpoint logs to the SIEM.

Cisco FTD Segment

Cisco FTD Firewall

Direction	Service/Application	Destination / Source	Network Scope	Notes / Justification

I	HTTPS/SSH (Management)	Admin Workstations	Internal	For authorized administrator access.
O	DNS	AD/DNS Server	Internal	To resolve hostnames for updates and threat intelligence feeds.
O	NTP	Internet	External	To ensure accurate time for logs and certificates.
O	Cisco Updates	Internet	External	To receive the latest software, threat, and application signatures.

AD / DNS (Server 2019)

Direction	**Service/Application**	**Destination / Source**	**Network Scope**	**Notes / Justification**
I	dns, ldap, kerberos	All Internal Hosts	Internal	Primary function as a domain controller and DNS server.
O	DNS (Forwarding)	Internet (Root Hints)	External	To resolve external domains for internal clients.
O	syslog	Splunk Server	Internal	To forward security and system event logs to the SIEM.

Web (Server 2019)

Direction	**Service/Application**	**Destination / Source**	**Network Scope**	**Notes / Justification**
I	web-browsing, ssl	External & Internal Clients	External & Internal	To serve the primary company website.
O	DNS	AD/DNS Server	Internal	To resolve internal and external hostnames.

O	ms-ds-non-rpc	AD/DNS Server	Internal	For domain membership and authentication.
O	syslog	Splunk Server	Internal	To forward IIS and system logs to the SIEM.

FTP (Server 2022)

Direction	Service/Application	Destination / Source	Network Scope	Notes / Justification
I	ftp	Internal Clients	Internal	To allow internal users to upload/download files.
O	DNS	AD/DNS Server	Internal	To resolve internal hostnames.
O	ms-ds-non-rpc	AD/DNS Server	Internal	For domain membership and user authentication.
O	syslog	Splunk Server	Internal	To forward FTP and system logs to the SIEM.

Wkst (Windows 11)

Direction	Service/Application	Destination / Source	Network Scope	Notes / Justification
O	DNS	AD/DNS Server	Internal	To resolve hostnames for browsing and updates.
O	ms-ds-non-rpc	AD/DNS Server	Internal	For domain membership and user authentication.
O	web-browsing, ssl	Internal Servers & Internet	Internal & External	To access internal web services and the general internet.