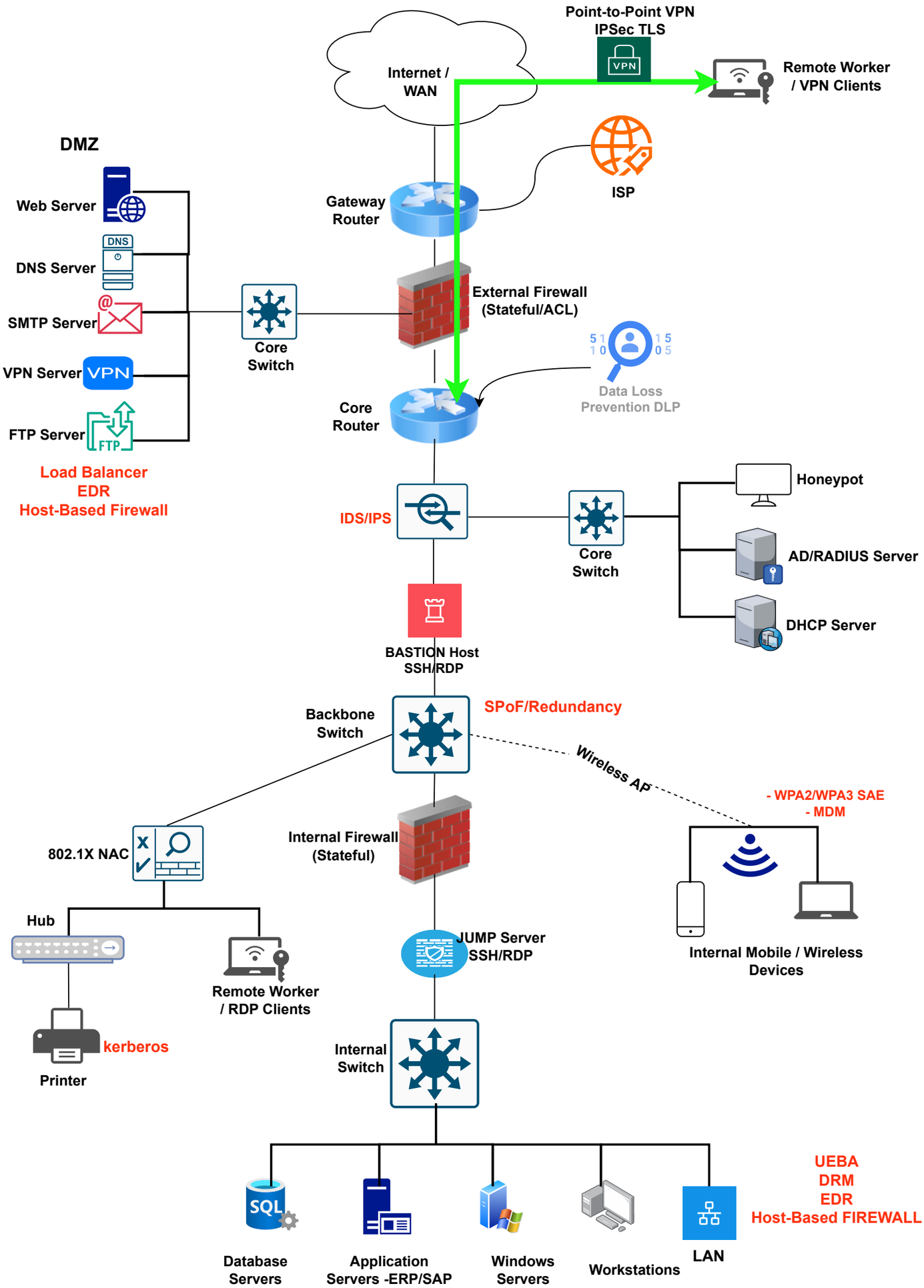
Point-to-Point VPN
IPSec TLS
VPN
Internet /
WAN
Remote Worker
/ VPN Clients
ISP
DMZ
Web Server
DNS Server
SMTP Server
VPN Server
FTP Server
Load Balancer
EDR
Host-Based Firewall
Gateway
Router
External Firewall
(Stateful/ACL)
Core
Switch
Data Loss
Prevention DLP
Core
Router
IDS/IPS
Core
Switch
Honeypot
AD/RADIUS Server
DHCP Server
BASTION Host
SSH/RDP
Backbone
Switch
SPoF/Redundancy
Wireless AP
- WPA2/WPA3 SAE
- MDM
802.1X NAC
Internal Firewall
(Stateful)
Hub
Printer
kerberos
Remote Worker
/ RDP Clients
JUMP Server
SSH/RDP
Internal Mobile / Wireless
Devices
Internal
Switch
Database
Servers
Application
Servers -ERP/SAP
Windows
Servers
Workstations
LAN
UEBA
DRM
EDR
Host-Based FIREWALL

Best Practices

- The DMZ - hosts the Web server, DNS, VPN server, SMTP/Email server, FTP server for both internal as well as for outside access and is directly connected to the firewall using a high speed cable.
- The VPN server can also be run on a router, then it would be a VPN gateway.
- Implement 2 core switches, interconnected with HIGH SPEED fiber optic cables - to provide redundancy, and to avoid single point of failure (SPOF).
- Stateful Firewall is used to filter traffic based on session state (eg. spoofed IPS), connection state (eg. SYN attack) and traffic anomalies (eg. DDoS), that is coming toward the inside network. This is achieved using access control list (ACL) configured inside the firewall.
- Gateway router is used to forward/route the traffic to other directly connected ISPs or branch offices through the leased lines (Assuming branch offices are connected to the main site through the leased lines). Can also be used as a IPSec VPN gateway tunnel.
- Core router is used to route traffic within inside the building (between VLANs) and to route traffic outside of the building (To Internet and branch offices).
- Implement 2 core routers, interconnected with HIGH SPEED fiber optic cables - to provide redundancy, and to avoid single point of failure (SPOF).
- AD /RADIUS (Active Directory / Remote Authentication Dial-In User Service) server is used to provide centralized authentication, authorization and accounting (AAA) service for users for different services across the network.
- DNS server for DNS-Lookup services (to translate domain name into IP address)
- DHCP server which dynamically assign IP address to hosts in different VLANs in the network (thus reduces difficulty in managing and configuring IPs).
- FTP server is used for file transfer within the network to include data that can be transferred or shared in bulk efficiently.
- SMTP servers are more reliable when sending mails to clients. They deliver mail to recipients quickly, they offer reliability in sending email messages (SMTP server will always try to re-send the same email until the transmission becomes successful), spam messages can be controlled in the central location and mailbox capacity is limited to hardware capacity.
- VPN – Virtual private network is used for the communication between main site and the remote worker. VPN is using an encrypted tunnel for the data transfer over the existing Internet infrastructure. Thus, provide secure and cheap communication for data transfer.
- Deploy a Honeypot - an air-gapped workstation or a network segment of PCs (honeynets) solely to serve as a decoy (false target) to attract and trap potential attackers so as to observe and analyze their tactics, techniques, and procedures (TTPs) aka attack vectors. The benefit is to divert attention, increase burnout time and use the TTPs to potentially hinder attacks on legitimate systems.
- IDS/IPS - how do you defend against what's already inside or originated from inside the network? Insider Threats? - Intrusion Detection/Protection System - to detect and protect malicious threats inside within the internal network - both egress and ingress monitoring.
- NAC- Network Access Control - Controls which devices can access the network, verifies device compliance before granting access.
- DLP - Data Loss Prevention - Prevents unauthorized access and exfiltration of sensitive data by blocking file transfers out of network. Data Breaches.
- DRM - Digital Rights Management - Installed as agents on endpoints to controls access to files - protecting intellectual property and copyrighted files.
- EDR - End Point Detection and Response - Advanced tool used to monitor endpoint behavior to detect and respond to malwares, ransomware, malicious files, APTs, etc
- UEBA - User Entity Behavior Analytics - To detect anomalies in malicious activity in both USERS and endpoints. It detects user account compromises, privilege abuse and unusual activities.
- Implement Mobile Device Management MDM - to control Bring Your Own Device BYOD of workers. For remote wiping of BYODs when device is lost or stolen, to grant access to network or resources based on context aware attributes such as location, time, type of device...for authentication
- Host-based Firewall - installed on individual devices/servers to control network traffic to/from a single device based on rules.
- BASTION Host - A special type of Hardened Server, directly exposed to the internet, outside the sec zone, to serve as a single point of entry/gateway for external access to internal protected network. Used by Service Accounts and Admin Accounts from outside the organization into the organization private internal network. Can also be placed in the DMZ. Allow sonly SSH/RDP connections.
- JUMP Server - A special type of Hardened Server, not directly exposed to the internet, inside the sec zone, to serve as a single point of entry/gateway for administrative access to internal protected network. Used by Service Accounts and Admin Accounts from inside the organization into other private networks within the organization. Allow sonly SSH/RDP connections.
- Implement SYSLOG integrated to SIEM and if possible integrated to SOAR - to normalize logs from multiple sources and possibly automate incidence response suing workflows.
- Keep it simple (KISS) -- Segment, microsegment and segregate networks and functions to reduce the attack surface
- Limit unnecessary lateral communications.
- Harden network devices - remove unnecessary services, disable unneeded ports, patch
- Principle of Least Privilege and Need to know - To secure access to infrastructure devices by only authorized persons
- Implement Zero Trust Architecture
- Validate integrity of hardware and software
- Implement Defense in Depth DiD
- Implement Separation of Duties SoD
- Implement Fail Sage and Fail Secure principles
- Implement Threat Modeling
- Implement Privacy by Design when designing software