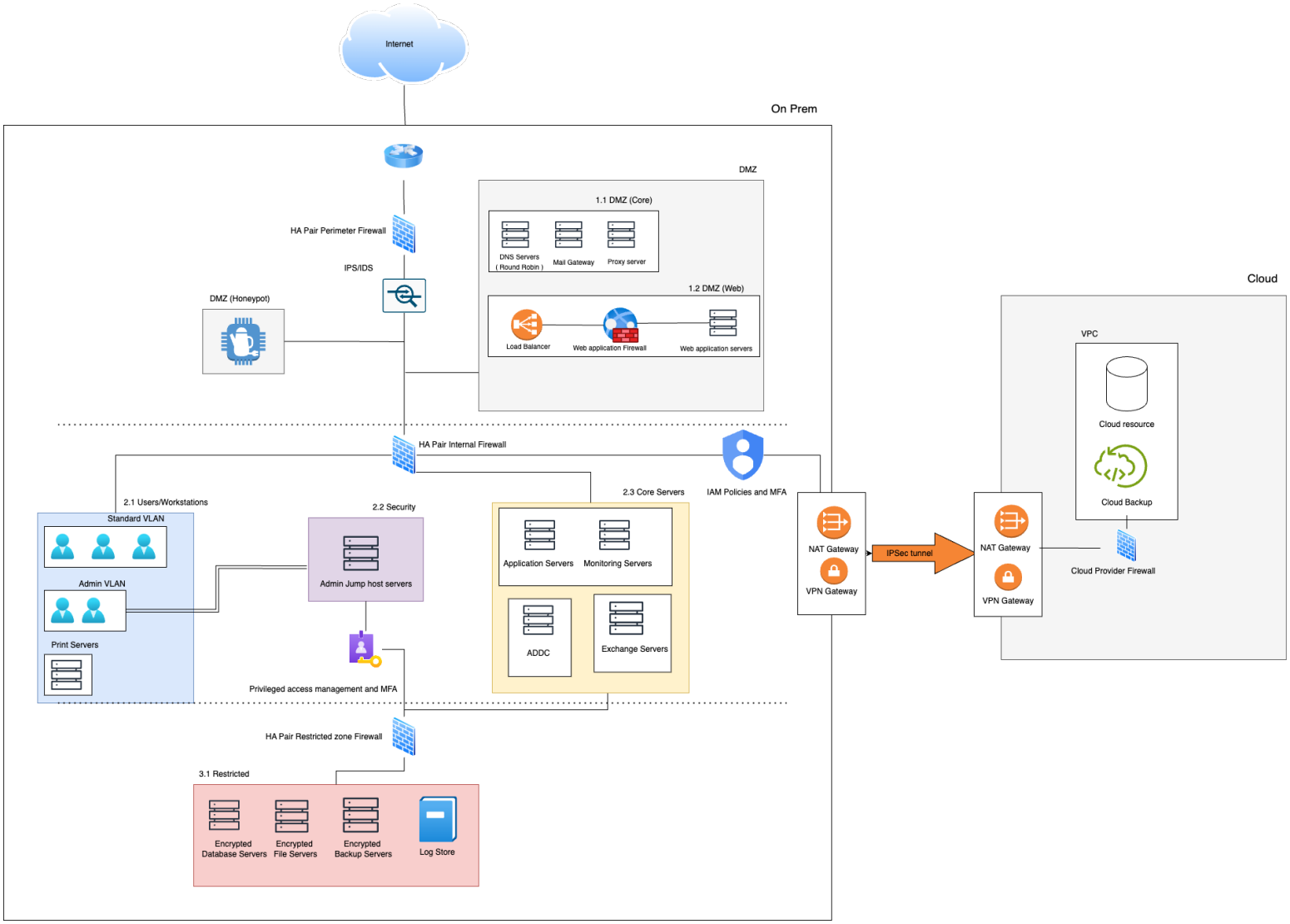
Startup Network Architecture Diagram


Internet
On Prem
DMZ
1.1 DMZ (Core)
DNS Servers
(Round Robin)
Mail Gateway
Proxy server
HA Pair Perimeter Firewall
IPS/IDS
DMZ (Honeypot)
1.2 DMZ (Web)
Load Balancer
Web application Firewall
Web application servers
HA Pair Internal Firewall
IAM Policies and MFA
2.1 Users/Workstations
Standard VLAN
Admin VLAN
Print Servers
2.2 Security
Admin Jump host servers
2.3 Core Servers
Application Servers
Monitoring Servers
ADDC
Exchange Servers
Privileged access management and MFA
HA Pair Restricted zone Firewall
3.1 Restricted
Encrypted
Database Servers
Encrypted
File Servers
Encrypted
Backup Servers
Log Store
NAT Gateway
VPN Gateway
IPSec tunnel
Cloud
NAT Gateway
VPN Gateway
VPC
Cloud resource
Cloud Backup
Cloud Provider Firewall

Details

1. Perimeter and Internal Firewalls (HA Pair)

- **High Availability (HA) Firewalls**: These firewalls are deployed in pairs for redundancy, ensuring continuous operation even if one fails. This setup protects against external threats, providing a defense against unauthorized access from the internet.
- **Intrusion Prevention/Detection System (IPS/IDS)**: Monitors incoming and outgoing network traffic for suspicious activities or potential threats. This system provides early detection of attacks or anomalies, allowing prompt responses.

Rationale: The perimeter firewall blocks unauthorized external access, while internal firewalls segment the network internally to limit the lateral movement of threats. IPS/IDS adds a proactive layer of monitoring.

2. DMZ (Demilitarized Zone)

2.1 DMZ (Core)

- **DNS Servers**: These servers handle the translation of domain names to IP addresses. By placing DNS in the DMZ, it allows external users to resolve internal services without compromising internal systems.Additional DNS security measures will be implemented such as DNSSEC , DNS filtering and DDOS protection
- **Mail Gateway**: Protects email servers from external threats like spam, phishing, and malware.
- **Proxy Server**: Controls internet access, manages bandwidth, and adds another layer of security by anonymizing outgoing traffic.

2.1 DMZ (Web)

- **Web Application Firewall (WAF)**: Protects web applications from common exploits like SQL injection, cross-site scripting (XSS), and other web-based attacks.
- **Load Balancer**: Distributes incoming traffic to multiple application servers, improving availability and reliability.
- **DMZ Honeypot (Optional) :** A honeypot is a decoy server designed to lure attackers, collecting information about attack methods while diverting them from critical assets.

Rationale: The DMZ acts as a buffer zone between the internal network and the external internet. By placing publicly accessible servers (DNS, proxy, and application servers) here, the architecture mitigates the risk of external attacks penetrating the internal network.

3. Internal Network Level

This level contains the organization's internal resources and employees' systems. It is segmented to isolate different functions, users, and critical services.

3.1 Users/Workstations (2.1)

This segment handles standard users, administrative users, and services like printing, all on separate VLANs to isolate different types of traffic and prevent unauthorised access. All workstations and servers will be secured by an **EDR/AV solution.**

- **Standard VLAN**: For regular users' workstations and everyday network operations.

- **Admin VLAN**: A separate VLAN for administrators to reduce the attack surface for privileged accounts. Only Administrator will have access to the restricted zone via a jump host and PAM.

- **Print Servers**: A dedicated VLAN for network-connected printing services.

Rationale: Segmentation limits the risk of lateral movement in case a workstation is compromised. The admin VLAN ensures that sensitive administrative tasks are segregated from normal user traffic.

3.2 Security (2.2)

This level focuses on secure management and access to administrative systems.

- **Admin Jump Host Servers**: These are secure servers that admins must use to access critical systems. Access to these jump servers is controlled with **Privileged Access Management (PAM)** and **Multi-Factor Authentication (MFA)** for additional security.

Rationale: Admin jump hosts enforce strict security controls for privileged users, ensuring that sensitive resources are only accessible by authorized personnel using strong authentication.

3.3 Core Servers (2.3)

This segment contains the core IT services required for business operations.

- **Application Servers**: Handles various internal applications.

- **Monitoring Servers**: Continuously monitor the network and services for performance issues or security anomalies.

- **Active Directory Domain Controllers (ADDC)**: Manage network authentication and directory services.

- **Exchange Servers**: Manage email and communication services for the organization.

Rationale: Segmenting these critical services from other parts of the network protects them from attacks originating from user VLANs or DMZs. This is essential to safeguard the integrity of the organization's core operations.

4. Restricted Zone

This level contains highly sensitive data and services. It is isolated with an additional firewall and provides maximum security for data storage and logging.

- **Encrypted Database Servers**: Store sensitive information, with encryption ensuring data is protected both at rest and transit.
- **Encrypted File Servers**: Secure storage for sensitive files and documents.
- **Encrypted Backup Servers**: Handle backups of critical data, also encrypted to protect against breaches or unauthorized access.
- **Log Store**: Centralized storage for all system and security logs, enabling secure logging for forensic and compliance purposes.
- **Rationale**: This zone is highly restricted and insulated from other parts of the network, with all data encrypted. It serves as the last line of defense, protecting high-value assets and sensitive information.

5. Cloud Integration Level

This level shows how the on-premises network connects to a cloud environment for backup and additional resources.

- **IPSec Tunnel**: Provides a secure, encrypted communication channel between the on-premises network and cloud resources.
- **NAT Gateway & VPN Gateway**: Enable secure access to and from the cloud, managing address translation and virtual private network (VPN) connections.
- **Cloud Backup**: Provides a remote backup of critical data, ensuring that data is recoverable even in the event of a local disaster.
- **Cloud Provider Firewall**: Protects the cloud environment from external threats.
- **Cloud Native Security Controls:** IAM policies , authentication and MFA

Note*: Depending on the cloud service requirement , an alternative way of accessing cloud services is to Cloud Access Security Broker (CASB) instead of a VPN. This would provide Visibility, Compliance, Data Security and Threat Protection.*

Rationale: Cloud integration ensures business continuity through off-site backups and access to cloud resources. The secure tunnel ensures data integrity and confidentiality during transfers.

Rationale for the Architecture

- **Defense-in-Depth**: Multiple layers of security (firewalls, IPS/IDS, WAF, segmentation) are employed to reduce the risk of breaches.
- **High Availability**: Redundant systems (HA firewalls) ensure availability, minimizing downtime and ensuring continuous protection.
- **Segmentation**: Logical separation of network segments limits the attack surface and controls the flow of traffic between less secure and more secure areas.
- **Security of Data in Transit and at Rest**: Use of encryption (IPSec tunnels, encrypted databases) ensures data confidentiality and integrity.
- **Visibility and Monitoring**: Logging, monitoring servers, and honeypots improve situational awareness and incident detection capabilities.

The design under the assumption that the startup has limited budget. Additional security controls such as SIEM , vulnerability management and DLP can be implemented once the company scales up.