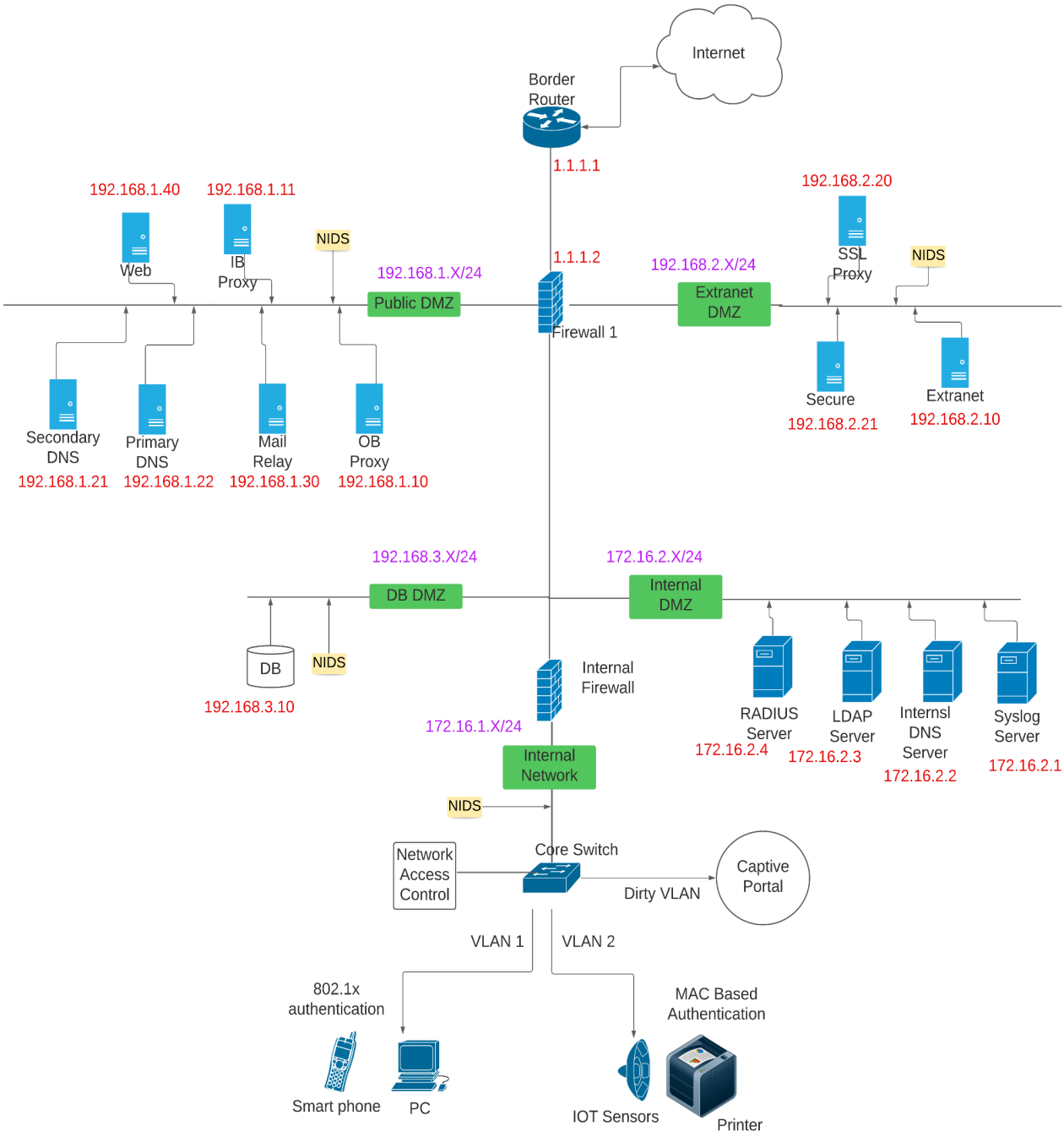
Secure Network Diagram

The following diagram depicts the design for a secure perimeter at a HQ site. The following architecture encompasses concepts related to Micro- Segmentation, Defense-In-Depth and Zero Trust Architecture (ZTA).



Architecture Components and Roles:

Border Router:

- One interface will connect to the ISP through the point-of-presence, and the others will connect to the perimeter architecture.
- Ingress filtering for known malicious traffic and egress filtering for internal addresses but no packet inspection.
- First filter for SYN FLood Defense, LEak of Internal addresses to internet and prevention of propagation of spoofed source addresses
- Filtering routers serve as the initial screen for the Internet connection. Since a router's job is to efficiently route traffic, it should not be overburdened with packet inspection
- Prime targets for attack - poisoning of routing tables, arp caches etc.
- Hardent the router, disable unneeded services, allow ssh instead of telnet, interactions with foreign systems such as BGP to the ISP routers are secure and authenticated.

Firewall:

- Systems in the DMZ will have their addresses translated to public Internet addresses through **Network Address Translation (NAT)** at the firewall. This will allow the purchase of only a limited number of public Internet addresses. **PAT (Port Address Translation)** to effectively mask the real number of internal systems in the DMZ.
- Access control to the company network, choke point for all traffic through the Internet connection.
- VPN connectivity for remote offices
- Block all inbound and outbound traffic not specifically authorized (**Zero Trust Mechanism).** Outbound control will prevent some worms and Trojans from contacting their masters out on the internet. It will prohibit all traffic not specifically allowed to the DMZ systems.
- **Dynamic port allocation (Zero Trust Mechanism)** so that a large range of ports are not open to accommodate dynamic protocols (FTP, HTTP etc.) and add dynamic rules to detected threats.
- Segregates extranet web server and database server from other zones (DMZ, Internet and Internal). Prevents direct access of databases from internal networks (insider threat).
- The firewall blocks all traffic from the internal network, except for that which originates from the proxy server.

Firewall VPN Function

- Allow remote access to the network only by authorized entities.
- Encrypt traffic between offices/ teleworkers and network to protect from sniffing.

Network- based Intrusion Detection (IDS) Sensors

- Monitor overall traffic for suspicious events on a network-wide basis. While the firewall may also accomplish this function, we do not want the firewall to become bogged down in analyzing traffic more than it needs to in determining access for that traffic.
- This will monitor traffic that makes it through the firewall as well as insider attacks.
- Must be tuned over a significant amount of time to eliminate false positives.
- Can only detect attacks which it knows how to recognize (signatures)
- Listens Passively, This ensures the IDS sensor is not detectable and cannot be compromised and used to bridge the DMZ to the internal network.

Host- based IDS/ IPS Sensors

- While NIDS looks at traffic as a whole for the network segment, the HIDS looks at traffic specifically for its host, and is more apt to catch anomalies that use proper protocols and interactions, but may have malicious payloads. In addition, certain Intrusion Protection System (IPS) agents monitor system processes for anomalies and react to behaviors and not signatures.
- Protection against Buffer Overflow attacks, Malicious mobile code protection, spyware/adware protection, OS integrity assurance, prevent rogue processes from executing, monitor files for unauthorized modification (detect installation of rootkits)

Extranet Server

- Firewall restricts connections to the Extranet Server to only certain semi-trusted source IP ranges.
- Presents web front-end for partner and customer applications
- Prevents direct access to the database server by partners, prevents unauthorized queries to the database.

Proxy Servers

- Proxies serve as an intermediary in the network traffic path that can serve as both an access control and a malicious traffic detection/prevention function.
- Can be used for access control (require authentication for connections to pass). Can be used to defeat unauthorized transmissions over authorized ports.
- When dealing with malicious traffic, the proxy captures the traffic, reconstructing any fragmented packets or streams, and then recreates the traffic and sends it to the intended host through a separate connection. This reconstruction as a separate connection effectively corrects the errors that form the attack, filtering them out of the traffic.
- Some protocol- or payload-based attacks on a web server will not be processed as web commands and will not compromise the proxy, but can be detected and filtered out instead.
- The proxy must be set for authentication so that it will forward only allow traffic through that comes from authenticated sources. This setup will require all outbound traffic to be authenticated through a username and password.

- Traffic logging and accounting function, keeps all records of authentication in addition to the usual IP address that the firewall tracks.
- Here, we only proxy inbound traffic to the Public Web Server and Secure Server, and not the Extranet Server.
- Inbound Proxy
    - Caching of web pages for quicker access, reduction of load for public web server
    - Proxies all connections from the Internet to the public DMZ systems
    - Mitigates fragmentation, protocol-, and OS-based attacks on the web server.
- Outbound Proxy
    - Proxies all connections from the internal network to the Internet.
    - Prevents unauthorized connections over authorized ports from reaching the Internet.

Mail Relay

- To avoid exposing the company mail server to the Internet, use a mail relay device to pass email traffic from the Internet to the mail server. This mail relay will not only proxy the connection from foreign mail servers (with the benefits detailed above for the proxy servers) but will also inspect the mail traffic for viruses and dangerous traffic, both inbound and outbound.

DNS Servers

- **Split DNS** Methodology -separating the tables of addresses and hostnames of the publicly addressable systems from the internal systems. By splitting the DNS records up between servers, an attacker cannot harvest information on the internal systems by attacking the external DNS server.
- The DMZ DNS systems will be authoritative for all publicly accessible systems and will not share this information with other DNS systems (internal or external).
- Only UDP DNS traffic for query resolution will be allowed through the firewall. Zone transfers (TCP traffic) cannot occur even if the internal or DMZ DNS is set to perform them.

Syslog Server

- Export log data from the firewall and IDS Sensors (NIDS and HIDS) to a central syslog server on the internal network.
- This serves two functions: 1) aggregating log data so that it may be correlated and immediately available; and 2) compromise of a single device in a DMZ will not compromise the log data since an attacker will need to penetrate the internal network and the syslog data to erase their tracks or otherwise alter the log data.

Defense-In-Depth Approach

- “resulting in a layered approach to security where the failure of one security system is not likely to lead to the compromise of the rest of the network.”
- External Router:
    - Initially screens traffic coming into the network perimeter.

    - Bad source addresses (Reserved addresses, internal addresses, spoofed source addresses) put in filtering rules
    - Filter Denial of Service attacks
- Primary Firewall:
    - The firewall only allows connections to the Inbound Proxy (80/TCP), DMZ DNS (53/UDP), and Mail Relay (25/TCP) on the Public DMZ. It also allows connections to the SSL Proxy (443/TCP), and Extranet Server (22/TCP, 443/TCP) on the Extranet DMZ.
    - The firewall will only allow access from the internal network to the Outbound Proxy, DMZ DNS servers (from the internal DNS only), mail relay (from the internal mail server only), and the Database Server (from the Intranet server only).
    - Connections only to specific ports and systems allowed. All other traffic dropped. Attacker will get no feedback of what happened.
- Inbound and SSL proxies
    - Public web traffic will be allowed to the Inbound Proxy, which will capture and retransmit the connection to the Public Web Server. This way, attacks cannot be mounted directly against the web server, and protocol-based attacks (such as fragmentation attacks) cannot be used as the proxy will simply detect that traffic is not correctly formed and will drop it.
    - Web Catching
    - The SSL proxy will then make another SSL connection to the Secure Server so that the payment information is protected even inside the Extranet DMZ. The Secure Server cannot be contacted directly from the Internet.
- Extranet Web Server
    - The risk is minimal since the firewall only allows connections from known partner and supplier addresses and not the general Internet. Also, the data is stored on the Database server, not the Extranet Server.
    - Only encrypted traffic (HTTPS and SSH/ STFP) is allowed past the firewall, so information is protected as it transits the Internet.
- Database Segregation
    - The database server, which is in a different access controlled network zone from the Public, Extranet, and Internal Network zone, The firewall only allows SQL connections between the Extranet, Secure, and Intranet servers, and the Database Server – all other connections are denied.
- Network Access Control
    - Network Access Control or NAC refers to technology that restricts network access to devices that meet certain policy controls (e.g. anti-virus software, patch level, host firewall), provide sufficient user credentials or Multi-Factor Authentication , or match a certain physical (MAC) address.
    - 802.1x Port-Based Network Access control allows clients to authenticate using credentials such as passwords or certificates to gain network access. The client sends an authentication request to the switch using the Extensible Authentication Protocol over LAN (EAPOL).

- The switch acts as a proxy and takes the encapsulated EAP request and converts it into a RADIUS request, sending it on to the authentication server. The responses returning from the authentication server are then converted back into EAPOL for the client.
- MAC Authentication Bypass - authentication method that grants network access to specific MAC address for 802.1x incompatible devices.