Network Interface Documentation

Document: Overview of network segmentation, firewall architecture, DMZs, and key network interfaces

- **Purpose:** To describe the World Bank's network architecture with a specific focus on security zoning, segmentation strategies, firewall deployments, the use of Demilitarized Zones (DMZs), and the documentation of key network interfaces. This document aims to provide a clear understanding of how network traffic is controlled and segregated to protect WDB's information assets.
- **Network Security Philosophy:** The World Bank's network security philosophy is founded on the principle of **defense-in-depth**, complemented by an evolving adoption of **Zero Trust** concepts where applicable. This means that security is not reliant on a single perimeter defense but is implemented through multiple layers of controls throughout the network. Network segmentation is a cornerstone of this philosophy, designed to limit the lateral movement of attackers in the event of a breach and to contain the impact of security incidents.

Network Zones

Key Network Zones and Segmentation: The WDB network is divided into multiple security zones, each with a specific purpose and trust level. Traffic between zones is strictly controlled by firewalls or other network security devices. Key zones include :

- **External/Untrusted Zone:** Represents the public internet and any networks not under WDB's direct control.
- **Demilitarized Zones (DMZs):**
    1. **Public DMZ:** Hosts public-facing services such as the WDB corporate website, client login portals, and publicly accessible API endpoints. These services are typically protected by Web Application Firewalls (WAFs).
    2. **Partner DMZ (Extranet):** Provides controlled access for trusted third-party partners, such as correspondent banks or critical data providers, to specific WDB services.
    3. **DMZ Outgoing:** A segment for internal systems that need to initiate connections to the internet (e.g., for updates, accessing external APIs) but should not be directly accessible from the internet.

- **Internal User Zone (Corporate Network):** Contains workstations, laptops, and other devices used by WDB employees for daily operations. This zone may be further segmented by department or user role.
- **Application Zone(s):** Hosts internal application servers. This zone is often further sub-segmented into:
    1. **Frontend Application Tier:** Servers handling initial user interaction or presentation logic.
    2. **Middleware/Business Logic Tier:** Servers processing application logic and orchestrating data access.
    3. **Backend Application Tier:** Servers directly interacting with databases or other core services.
- **Database Zone:** A highly restricted zone housing critical WDB databases. Access to this zone is severely limited and strictly controlled from the Application Zone.
- **Management Zone (OOB - Out-of-Band Network):** A dedicated and isolated network for the administration and management of network devices, servers, and security appliances. Access to this zone is highly privileged.
- **Cloud Zones (VPCs/VNETs):** Virtual Private Clouds (VPCs) in AWS, Virtual Networks (VNETs) in Azure, or similar constructs in other cloud providers. These are segmented based on workload sensitivity, environment (production, development, test), and compliance requirements, using cloud-native security groups and network ACLs.
- **Development and Test Zone:** Isolated environments for software development, quality assurance, and testing activities, segregated from production networks.
- **Critical Infrastructure Zone:** May exist for highly sensitive systems like payment processing engines or cryptographic key management, with extreme access controls.

Firewall

Firewall Architecture: WDB employs a multi-layered firewall architecture:

- **Perimeter Firewalls:** Next-generation firewalls (NGFWs) are deployed at the internet edge, between the External Zone and DMZs, and between DMZs and internal network zones. These provide threat prevention, intrusion detection/prevention (IDS/IPS), and application control.
- **Internal Segmentation Firewalls (ISFWs):** Deployed between key internal zones (e.g., between User Zone and Application Zone, Application Zone and Database Zone) to enforce segmentation policies and inspect east-west traffic.

- **Web Application Firewalls (WAFs):** Protect web applications hosted in the DMZs and potentially internal web applications from common web-based attacks (e.g., SQL injection, XSS).
- **Cloud-Native Firewalls:** Utilize security groups, network ACLs, Azure Firewall, AWS Network Firewall, and other cloud provider security services to control traffic within and between cloud environments.
- **Host-Based Firewalls:** Implemented on critical servers to provide an additional layer of protection.

Network Interface

Network Interface Documentation: While a full inventory of all network interfaces is part of the Asset Inventory (B.1), this section focuses on documenting the purpose and security policy for *critical* network interfaces, particularly those on firewalls, core routers, and servers hosting critical services. For each such interface, documentation includes:

- Device Name and Interface ID
- Connected Network Zone(s)
- IP Address / Subnet
- VLAN ID(s)
- Purpose of the Interface (e.g., "Uplink to ISP A," "Connection to Database Zone Firewall," "DMZ Web Server Interface")
- Key Security Policies Applied (e.g., specific firewall rule sets, ACLs enforced)
- Expected Traffic Types and Protocols

#	Device Name	Interface ID	Connected Network Zone(s)	IP Address / Subnet	VLAN ID(s)	Purpose
1	FW-Core1	eth0	Internet Edge / DMZ	203.0.113.1/30	10	Uplink to ISP A
2	FW-Core1	eth1	Internal Core	10.10.0.1/24	20	Internal segmentation
3	Router-Gateway1	gi0/1	Branch Office Network	10.20.0.1/24	30	WAN link to branch
4	DB-SERVER01	ens192	Database Zone	10.50.0.10/24	50	Database listener interface
5	WEB-APP01	eth0	DMZ	192.0.2.10/24	60	Public Web Interface
6	LB-Front01	eth1	DMZ to Web Servers	192.0.2.20/24	60	Load balancer to DMZ web servers
7	SIEM-Collector1	ens160	Monitoring VLAN	10.100.0.10/24	70	SIEM log collection interface
8	AD-DC01	nic1	Internal Auth Zone	10.30.0.1/24	80	Active Directory Domain Controller
9	NMS01	eth1	Management VLAN	10.200.0.10/24	90	Network management system
10	Proxy-Server01	eth0	Internal to Internet Proxy	10.60.0.1/24	100	Outbound internet access control

Traffic Flow

Traffic Flow Policies: General rules governing allowed and denied traffic between zones are formally documented and implemented in firewall configurations. Examples:

- Internet users can only access services in the Public DMZ on designated ports (e.g., TCP/80, TCP/443).
- No direct traffic is allowed from the External Zone to any Internal Zone.
- Application Zone servers can query Database Zone servers only on specific database ports (e.g., TCP/1521 for Oracle, TCP/1433 for SQL Server) and only from authorized source IPs.
- The Management Zone is only accessible from specific, hardened administrator workstations via secure protocols (e.g., SSH, HTTPS).
- Default-deny policies are enforced on all firewalls.

#	Source Zone	Destination Zone	Allowed Protocol(s)/Ports	Policy Description	Enforcement Notes
1	Internet	Public DMZ	TCP/80, TCP/443	Allow public web access to DMZ services	Only to Web Servers in DMZ, with Geo-IP filtering
2	Internet	Internal	*None*	Deny all traffic from Internet to Internal zones	Enforced by edge firewall (default deny)
3	Application Zone	Database Zone	TCP/1433, TCP/1521	Allow app servers to query databases on required ports only	Restricted to app server IPs only
4	External	Management Zone	*None*	Deny all external access to management interfaces	Management zone isolated with separate routing domain
5	Admin Workstations	Management Zone	SSH, HTTPS, RDP (TCP/22, 443, 3389)	Allow secure remote admin access from hardened endpoints only	Requires MFA + jump server
6	Internal Users	Internet	TCP/80, TCP/443, DNS	Allow standard outbound access to internet	Filtered through proxy and DNS inspection
7	Internal	Internal	Varies (internal app ports)	Allow inter-department communications only where justified	Based on business need; monitored via flow analysis
8	Backup Zone	Storage Zone	TCP/2049, TCP/445	Allow backup systems to write to storage over NFS/SMB	Nighttime backup windows only
9	Monitoring Zone	All Zones	SNMPv3, Syslog, HTTPS	Monitoring systems allowed to collect logs and metrics	Read-only access; SNMPv3 only; encrypted syslog
10	All Zones	Any	*None (default)*	Enforce default-deny policy unless explicitly allowed	All firewalls and routers must log denies

Intrusion Detection/Prevention Systems (IDS/IPS): IDS/IPS sensors are strategically placed at network ingress/egress points, in DMZs, and between critical internal zones to monitor for and block malicious activity. Alerts from these systems are fed into the SIEM.

Network Diagrams

Network Diagrams: This section includes high-level logical network diagrams illustrating:

- The major security zones and their relationships.
- The placement of key firewalls (perimeter, internal, WAFs).
- Major traffic flow paths for critical services.
- Connections to cloud environments. These diagrams are essential for visualizing the network topology and understanding how segmentation is enforced.