AWS Multi-Account Architecture Design

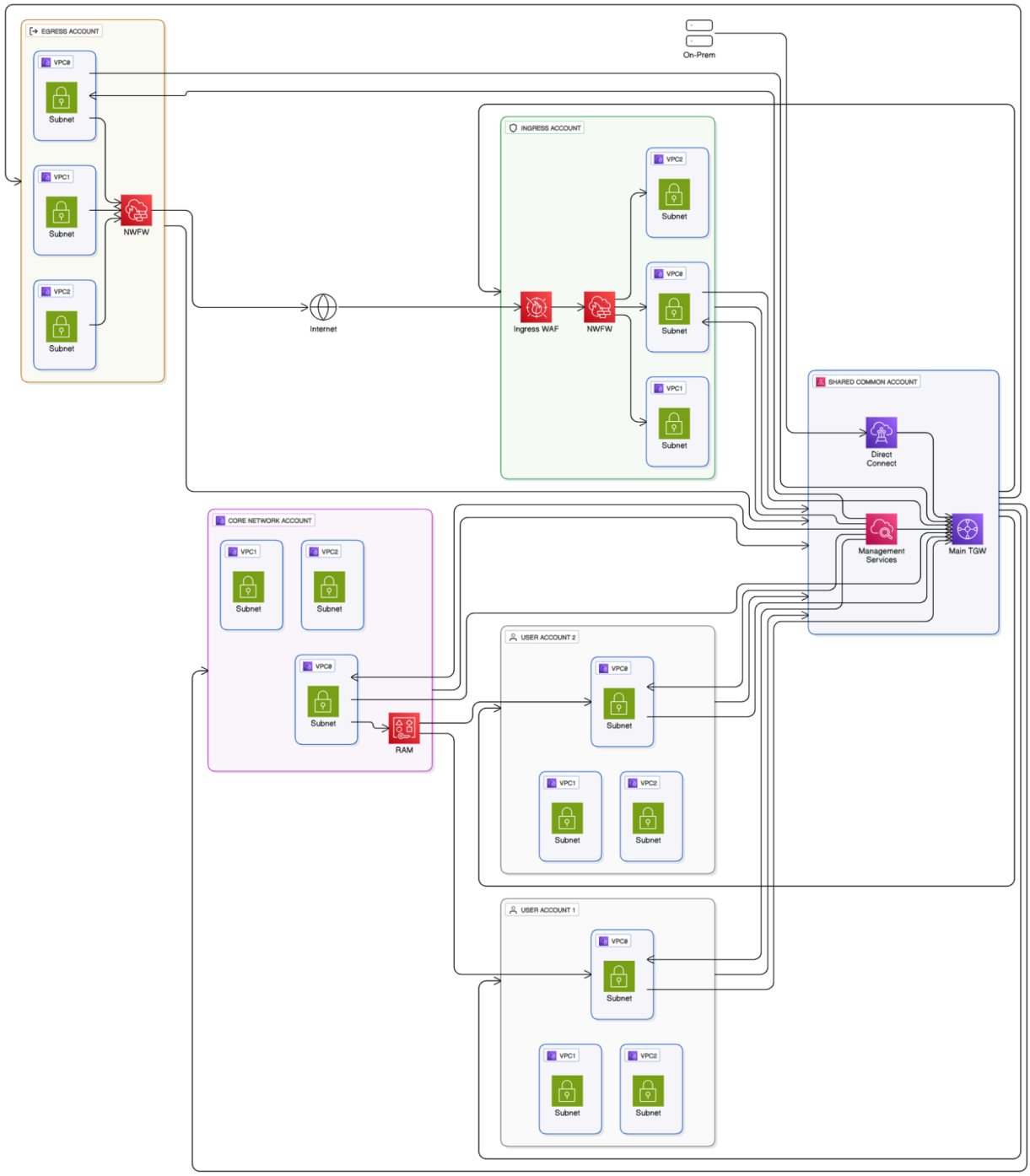
Purpose This document describes a multi-account AWS architecture captured in the provided diagram. It explains the purpose and functionality of each account, VPC, and network/security service shown, and includes tables summarizing VPC inventory and how VPCs are connected (Transit Gateway attachments, Direct Connect, Internet, and firewall paths). Use this as a reference for operations, security reviews, and network planning.

High-level overview

The architecture separates concerns across multiple AWS accounts to improve isolation, security, operational boundaries, and compliance. Key building blocks shown in the diagram are:

- **Ingress Account**: centralizes internet ingress controls (WAF, Network Firewall) and inbound traffic inspection.
- **Shared Common Account**: houses shared networking services such as the Main Transit Gateway (TGW), Direct Connect, and management services used across accounts.
- **Core Network Account**: owns VPCs for centralized services and shares them where appropriate (via RAM or TGW attachments).
- **Egress Account**: centralizes outbound internet egress and inspection.
- **User Accounts (1, 2, ...)**: tenant/application accounts where application VPCs reside. These attach to the shared network (TGW) for connectivity.
- **On-Prem / Direct Connect**: connectivity to on-premises networks via Direct Connect which peers into the shared account and connects to the TGW.

Traffic flows are intentionally centralized through WAF and network firewall appliances for consistent inspection, monitoring, logging, and enforcement of network-level policies.


EGRESS ACCOUNT
VPC3
Subnet
VPC1
Subnet
VPC2
Subnet
NWFW
On-Prem
INGRESS ACCOUNT
VPC2
Subnet
VPC3
Subnet
VPC1
Subnet
Internet
Ingress WAF
NWFW
SHARED COMMON ACCOUNT
Direct Connect
Management Services
Main TGW
CORE NETWORK ACCOUNT
VPC1
Subnet
VPC2
Subnet
VPC3
Subnet
RAM
USER ACCOUNT 2
VPC3
Subnet
VPC1
Subnet
VPC2
Subnet
USER ACCOUNT 1
VPC3
Subnet
VPC1
Subnet
VPC2
Subnet

Components and their responsibilities

Below are the services and icons visible in the diagram, with detailed responsibilities for each.

Ingress WAF

- **Service**: Web Application Firewall (managed or cloud WAF)
- **Role**: L7 (HTTP/HTTPS) inspection and protection for public-facing applications. Blocks common web attacks (SQLi, XSS, rate-limiting) before requests reach internal networks.
- **Placement**: Deployed in the Ingress Account in front of the inbound network firewall. All internet-originated HTTP/HTTPS traffic is routed through this component.

Network Firewall (NWFW) — Ingress & Egress

- **Service**: AWS Network Firewall (or virtual network firewall appliances)
- **Role**: Stateful L3–L7 traffic inspection, filtering, intrusion prevention, and enforced allow/deny policies for east-west and north-south traffic.
- **Placement**: Two logical placements appear: one in the Ingress account (protecting inbound traffic) and another in the Egress account (protecting outbound traffic). The NWFWs are in-line with gateway paths to inspect and control traffic.

Transit Gateway (Main TGW)

- **Service**: AWS Transit Gateway
- **Role**: Central hub for routing between multiple VPCs, accounts, and on-prem networks. Encapsulates complex peering into a single hub: spoke model.
- **Placement**: Located in the Shared Common Account. User and core account VPCs attach to the TGW to enable inter-account connectivity.

Management Services

- **Service**: Shared management network tools (could be monitoring, SIEM, NAT, management bastions, SSM endpoints)
- **Role**: Provide centralized operational tooling and connectivity needed by other accounts. May include log aggregation and network management functions.
- **Placement**: Shared Common Account and connected to TGW.

Direct Connect

- **Service**: AWS Direct Connect
- **Role**: Private, high-bandwidth, low-latency link between on-premises datacenter and AWS. Termination is shown in Shared Common Account and connected into the TGW for routing to VPCs.

Resource Access Manager (RAM)

- **Service**: AWS RAM
- **Role**: Share central resources (for example TGW route tables, subnets, or other network resources) across accounts. In the diagram RAM is used by the Core Network Account to share a VPC/subnet or managed resource with other accounts.

VPCs & Subnets

- **Service**: Amazon VPC — each account contains one or more VPCs. Each VPC includes subnets representing different tiers (public, private, management). The diagram shows multiple VPCs per account to allow segmentation and least privilege.

On-Prem

- **Role**: Customer datacenter(s) connected to AWS via Direct Connect and optionally via the internet. On-prem networks appear routed into the TGW through Direct Connect.

Account-by-account breakdown

Shared Common Account

Primary contents:

- Main Transit Gateway (TGW)
- Direct Connect termination and virtual interfaces
- Management Services (monitoring, logging, shared tooling)

Responsibilities:

- Central routing & cross-account connectivity via TGW
- Integration point for Direct Connect and on-prem circuits
- Central logging and management endpoints for visibility and operations

Ingress Account

Primary contents:

- Ingress WAF (edge L7)
- Ingress Network Firewall (NWFW)
- One or more VPCs hosting public-facing endpoints and routing to TGW

Responsibilities:

- Protect web applications at the edge
- Perform inbound traffic inspection and route approved traffic to TGW for delivery to application VPCs in user accounts

Egress Account

Primary contents:

- Egress Network Firewall
- VPC(s) and subnets for NAT / outbound proxying

Responsibilities:

- Centralized Internet egress inspection and logging
- Enforce outbound allow-lists and data exfiltration protections

Core Network Account

Primary contents:

- Central VPCs for shared services (e.g., DNS, authentication, shared databases)
- Uses RAM to share selected resources or allow cross-account access

Responsibilities:

- Host services that must be centrally managed or accessed by multiple user accounts
- Provide resources that can be attached to TGW or shared via RAM

User Accounts (1, 2, ...)

Primary contents:

- Multiple VPCs per account representing application tiers
- Each VPC connects to the Main TGW for intra-cloud and on-prem connectivity

Responsibilities:

- Run application workloads with network flows mediated by TGW and subject to central NWFW and WAF policies
- Leverage shared management services for SSM/patching and logging

---

VPC inventory and connections

Below is a table describing the VPCs visible in the diagram, their owner account, and how they are connected.

Legend: TGW = Transit Gateway; NWFW = Network Firewall; DC = Direct Connect; IGW = Internet Gateway; RAM = Resource Access Manager

VPC Name (diagram)	Owner Account	Subnets (logical)	Connectivity (attachments & routes)	Purpose
Ingress VPC (VPC2)	Ingress Account	Public subnets with WAF/NWFW	IGW -> WAF -> Ingress NWFW -> TGW	Entrypoint for internet traffic, WAF + NWFW enforcement
Ingress App VPCs (VPC1, VPC3 shown)	Ingress Account	Private & public subnets	TGW attachment to Shared TGW; route through NWFW for inspection	Host edge services and route traffic into core/user VPCs
Egress VPC(s)	Egress Account	Private subnets for NAT & firewall	TGW attachment to Shared TGW; Egress NWFW -> IGW	Centralized outbound proxy/NAT and filtering
Core VPC1, VPC2, VPC3	Core Network Account	Private subnets	TGW attachment; uses RAM to share select resources	Shared services (DNS, Active Directory, central services)
User Account VPCs (VPC1, VPC2, VPC3 per account)	Each User Account	Private app/DB/management subnets	TGW attachment to Main TGW (Shared Common Account)	Application workloads run here; use central network services
Shared Common: Management Services VPC	Shared Common Account	Private/management subnets	TGW attachment; connected to Direct Connect	Hosts management, logging, monitoring, and connectivity endpoints
On-Prem	Customer On-Prem	N/A	Direct Connect -> Shared Common -> TGW -> VPCs	On-prem systems access cloud

resources
securely

Routing & traffic flow (typical scenarios)

1) Internet → Public Web App (Inbound)

1. Client request from Internet reaches the architecture's public endpoint (Internet).
2. Traffic enters the **Ingress Account** and hits the **Ingress WAF** (L7 filtering).
3. If allowed, traffic flows into the **Ingress Network Firewall** for deeper inspection and stateful rules.
4. After firewall approval, traffic is routed onto the **Main TGW** (Shared Common Account) and forwarded to the destination VPC in a User Account or Core Account.
5. Responses return the same path in reverse, optionally inspected again by egress controls.

2) App → Internet (Outbound)

1. Application instances in a User Account send traffic destined to the internet.
2. Traffic is routed to the **Main TGW** and forwarded to the **Egress Account** attachment.
3. **Egress NWFW** inspects and enforces outbound policies (DLP, domain allow-list, logging).
4. Traffic exits the Egress VPC via an IGW (or proxy) to the Internet.

3) On-Prem → Cloud

1. On-prem systems connect over **Direct Connect** terminating in the **Shared Common Account**.
2. Traffic is routed via the TGW to the appropriate VPC in the Core or User accounts.
3. This path is subject to TGW route tables and firewall policies; in some designs, traffic may transit through a NWFW for additional control.

Security and operational considerations

- **Centralized inspection**: Inbound and outbound traffic funnels through WAF and Network Firewall appliances to ensure consistent policy enforcement and centralized logging.
- **Least privilege & segmentation**: Accounts and VPCs are used as trust boundaries. Application teams operate in user accounts while central controls remain in shared accounts.

- **Transit Gateway routing policies**: Use per-attachment route tables on the TGW to enforce segmentation (e.g., deny direct user account to user account traffic unless explicitly allowed).
- **Cross-account resource sharing**: Use AWS RAM carefully; prefer TGW attachments and route controls for network connectivity where possible to reduce complexity.
- **Logging & monitoring**: Send WAF logs, NWFW logs, VPC Flow Logs, and CloudTrail to the Management Services / Logging VPC for centralized observability.
- **High availability**: Deploy NWFW, WAF endpoints, TGW attachments, and Direct Connect in multiple AZs and redundant connections where required.
- **Bastion/Jump hosts**: Place management access in a dedicated management VPC with strict ingress rules and session recording.