Epic

Title: NJDC Architecture Optimization and Simplification

Description:

Migration of all services from the Juniper stack (EOS/EOL) to the Fortinet switch stack.

Optimize compliance, performance, and security by upgrading infrastructure, improving routing performance, and introducing enhanced security mechanisms like zone-level segregation.

Objective:

Ensure all services are transitioned to a modern, secure, and high-performing network architecture.

Decommission EOS/EOL devices and mitigate associated vulnerabilities.

---

User Stories

User Story 1: NAS Migration

As a network administrator,

I want to migrate the NAS service from the Juniper stack to the Fortinet switch stack,

So that it operates securely on an up-to-date network platform.

Acceptance Criteria:

NAS service successfully migrated with no downtime.

Configuration verified and tested for stability and security.

User Story 2: NetScaler Load Balancer Migration

As a network engineer,

I want to migrate the NetScaler LB from the Juniper distribution switch to the Fortinet stack,

So that the load balancer benefits from improved performance and security.

Acceptance Criteria:

NetScaler LB fully operational on Fortinet stack.

Load balancing configurations reviewed for optimal performance.

User Story 3: Email Exchange Migration

As a network administrator,

I want to move the email services from Juniper to the Fortinet infrastructure,

So that mail services continue to operate securely without interruptions.

Acceptance Criteria:

Email Exchange services migrated and tested.

Security and performance verified post-migration.

User Story 4: Azure Express Route Migration

As a cloud engineer,

I want to migrate the Azure Express Route connection to the Fortinet switch stack,

So that the network can securely access cloud resources via a reliable, modern infrastructure.

Acceptance Criteria:

Express Route fully operational on Fortinet switches.

Connectivity to Azure verified.

User Story 5: Compliance Optimization

As a network security team,

I want to remove the EOL/EOS Fortinet distribution switch from the LAN and migrate all services to the core switch,

So that the network remains compliant with operational standards.

Acceptance Criteria:

Distribution switch decommissioned.

All services successfully running on the core switch.

User Story 6: Inter-VLAN Routing Optimization

As a network engineer,

I want to move inter-VLAN routing from the firewall (INSID) to the new Fortinet core switch,

So that performance and security are improved for both core and perimeter firewalls.

Acceptance Criteria:

Inter-VLAN routing configured on the core switch.

Firewall offloaded from inter-VLAN routing responsibilities.

User Story 7: Security Enhancement with Zone Segregation

As a network security architect,

I want to introduce zone-level segregation at the firewall level,

So that the network has better isolation and improved security controls.

Acceptance Criteria:

Zone-level policies implemented and tested on the firewall.

No impact on existing services during policy introduction.

---

Sprint Plan

Sprint 1: Foundation & Initial Migration

Timeline: 2 Weeks

Scope:

Setup Fortinet switch stack for new services.

Migrate NAS and NetScaler LB to the Fortinet switch stack.

Validate performance and address issues.

---

Sprint 2: Email & Azure Migration

Timeline: 2 Weeks

Scope:

Migrate Email Exchange services to Fortinet.

Transition Azure Express Route to Fortinet switch stack.

Perform extensive testing for cloud connectivity and mail operations.

---

Sprint 3: Compliance Optimization

Timeline: 2 Weeks

Scope:

Decommission the EOL/EOS Fortinet distribution switch.

Move all services from distribution switch to the core switch.

---

Sprint 4: Routing and Performance Optimization

Timeline: 2 Weeks

Scope:

Transition inter-VLAN routing to the Fortinet core switch.

Monitor network performance improvements and address anomalies.

---

Sprint 5: Security Enhancements

Timeline: 2 Weeks

Scope:

Implement zone-level segregation on the firewall.

Test and validate security policies.

Finalize documentation and training for operations teams.