CYBERSECURITY TRANSFORMATION CASE STUDY

DC/DR Firewall Modernization for a Leading Banking Enterprise

NGFW modernization with DC/DR high availability and managed security operations.

Executive Summary
COMnet transformed the bank's perimeter defense posture by replacing legacy Cisco firewall infrastructure with Palo Alto Networks NGFW across DC and DR locations, enabling centralized policy governance, cloud-delivered security services and a tiered managed support model.

5+ Years	DC + DR	NGFW	24x7 L2	Onsite L1
Strategic IT partner	HA perimeter refresh	Palo Alto platform	Remote support	Local operations

IMPACT

Business and Cybersecurity Impact

- Modernized legacy Cisco firewall estate to Palo Alto Networks NGFW across Data Center and Disaster Recovery environments.
- Reduced end-of-life / end-of-support exposure and restored missing next-generation security capabilities.
- Delivered a controlled migration within the committed timeline, with no operational disruption reported.

Operational Impact

- Established centralized policy governance through Panorama and improved visibility across the perimeter.
- Enabled 24x7 L2 remote support and onsite L1 coverage for stable post-cutover operations.

MAJOR ISSUES

EOL/EOS Exposure

- Legacy perimeter devices had reached end-of-life / end-of-support, increasing cyber and operational risk.

Missing Security Features

- Security feature gaps limited malware prevention, URL control, secure access, and threat visibility.

HA & DR Dependency

- DC and DR firewall modernization required high availability, validated failover and continuity for critical banking services.

Migration Complexity

- Firewall migration carried policy, NAT, VPN, routing and application dependency risk.

Post-Cutover Ownership

- Post-cutover operations needed accountable L1 / L2 ownership, escalation, vendor coordination and governance.

HIGHLIGHTS

COMnet delivered a structured modernization program that combined security architecture, platform migration, cloud-delivered controls, managed operations and cyber-readiness support.

Platform Modernization

- Migration from Cisco Firewall to Palo Alto Networks NGFW for DC and DR locations in high-availability mode.
- Deployment of higher-end data center firewall models managed centrally through Panorama.

Security Controls Enabled

- Enablement of cloud-delivered security services: WildFire, Threat Prevention, GlobalProtect and URL Filtering.
- 24x7 remote L2 support for monitoring, policy administration, troubleshooting and escalation.

Operational Assurance

- Dedicated onsite L1 engineer for local coordination, operational continuity and change support.
- Security consulting support including incident response and digital forensics advisory.

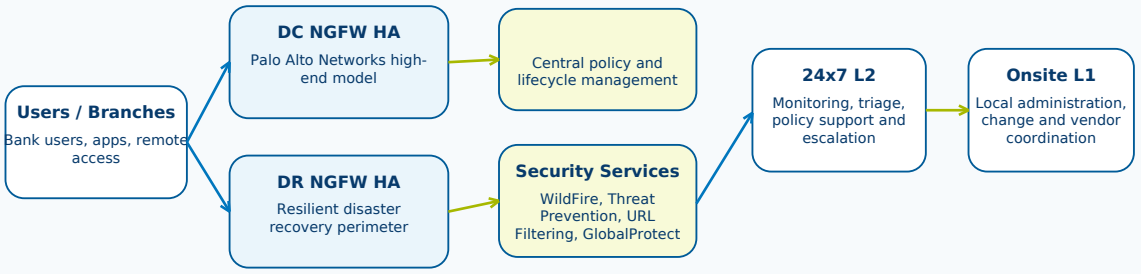
Use Cases Addressed

- NGFW migration for mission-critical DC and DR perimeter environments.
- High-availability firewall modernization with controlled policy cutover.
- Secure access, web control and threat prevention using cloud-delivered services.
- Post-migration managed operations using onsite L1 and remote L2 support.

Technical Controls and Services

- Palo Alto Networks NGFW, Panorama, WildFire and Threat Prevention.
- URL Filtering, GlobalProtect, policy validation and logging readiness.
- Incident response and digital forensics advisory for cyber resilience.
- Runbooks, escalation workflow and stakeholder service cadence.

ARCHITECTURE AND DEPLOYMENT SCOPE



Design principles: No-disruption migration | HA-first | Centralized policy | Defense-in-depth controls | Tiered support

Scope Area	Technical Scope	Expected Outcome
Perimeter Platform	Cisco firewall estate migrated to Palo Alto Networks NGFW across DC and DR.	Reduced technology risk and strengthened enterprise perimeter controls.
HA Architecture	HA pairs, traffic path checks, DR readiness and failover validation.	Improved availability and minimized interruption risk.
Central Management	Panorama policies, templates, device groups and lifecycle management.	Consistent governance, visibility and audit readiness.
Security Services	WildFire, Threat Prevention, URL Filtering and GlobalProtect.	Layered prevention, secure access and risk-based web control.
Managed Operations	24x7 remote L2 support with onsite L1 engineer for local operations.	Stable run-state, faster escalation and accountable support ownership.

KEY STRATEGIES

The program was positioned as a risk-reduction and cyber-resilience initiative - not only a firewall replacement. The following strategies make the engagement repeatable for enterprise decision makers and technical security teams.

Risk-Led Modernization

- Prioritize EOL/EOS exposure, missing control capabilities and business-critical traffic paths before technology refresh.

Zero-Disruption Migration

- Use phased design, rulebase conversion, staged validation, rollback planning and controlled cutover windows.

HA-First Architecture

- Deploy DC and DR firewalls in high availability with failover validation and service-continuity checks.

Centralized Governance

- Use Panorama for policy templates, device groups, rule lifecycle, audit traceability and reporting readiness.

Layered Defense

- Activate WildFire, Threat Prevention, URL Filtering and GlobalProtect to shift from perimeter enforcement to threat-aware prevention.

Managed Ops Continuity

- Combine 24x7 remote L2 support with onsite L1 execution for incident, change, vendor and stakeholder coordination.

Operational Handover

- Document policies, dependencies, runbooks, escalation paths and post-cutover tuning actions.

Continuous Optimization

- Conduct policy hygiene, performance review, threat-profile tuning and periodic service governance reviews.

IMPLEMENTATION AND GOVERNANCE CHECKLIST

Phase	Control Activities	Decision / Security Output
1. Discovery	Inventory firewall policies, NAT, VPNs, routing, HA state, dependent applications and business-critical flows.	Migration risk register, dependency map and validated target architecture.
2. Design	Define DC/DR NGFW architecture, Panorama hierarchy, security profiles, logging, escalation and cutover windows.	Approved HLD/LLD, runbook, rollback plan and stakeholder communication plan.
3. Migration	Convert policies and objects, validate application paths, enable security profiles and conduct controlled cutover.	Zero-disruption execution, verified policy behavior and validated HA/failover.
4. Run State	Activate L1/L2 support, SLA cadence, incident escalation, documentation and periodic optimization.	Operational readiness, measurable governance and continuous improvement loop.

Executive Takeaway
COMnet delivered a controlled, banking-grade security modernization that reduced obsolete infrastructure risk, improved defense-in-depth controls, and established a stable managed operations model across DC and DR perimeter environments.