

Core Infrastructure & IT/OT Security Transformation



Core switch modernization, IT/OT segregation, DMZ fiber upgrade, ECMP redundancy and secure management access

EXECUTIVE CONTEXT

COMnet delivered a core infrastructure and security transformation program for a critical industrial environment. The engagement retired end-of-life Juniper core switches, introduced high-performance Cisco SE switching, segregated IT and OT traffic using a dedicated OT firewall, upgraded DMZ connectivity from copper to fiber, enabled ECMP on the PMS link, and created a secure management VLAN behind the MPLS firewall. The program was planned for high availability and executed with zero business disruption.

0
Downtime

IT/OT
Segregated

Cisco
SE core



IMPACT

- Eliminated end-of-life Juniper core switch risk and replaced unsupported infrastructure with modern Cisco SE switching architecture.
- Reduced industrial cyber risk by physically and logically separating IT and OT traffic through a dedicated OT firewall layer.
- Completed core routing and security migration activities with zero reported downtime and no interruption to business operations.
- Improved throughput and reliability by upgrading DMZ interfaces from copper to fiber for higher-capacity connectivity.
- Strengthened resilience by implementing ECMP on the PMS link, enabling better load sharing and path redundancy.
- Improved secure administration by creating a dedicated management VLAN behind the MPLS firewall for controlled network gear access.

MAJOR ISSUES

- Core switching infrastructure was running on end-of-life Juniper hardware, increasing operational risk and limiting vendor support options.
- The existing IT and OT network design was logically flat, allowing OT traffic to remain dependent on IT firewall controls.
- Flat segmentation increased the risk that an IT-side compromise could pivot into operational technology environments.
- Core migration carried routing, LACP, cabling, firewall dependency, and traffic-path risks that required meticulous pre-validation.
- DMZ copper interfaces limited throughput and reliability for critical perimeter traffic flows.
- Secure management access was required to reduce administrative exposure and improve operational control.

Core Infrastructure & IT/OT Security Transformation

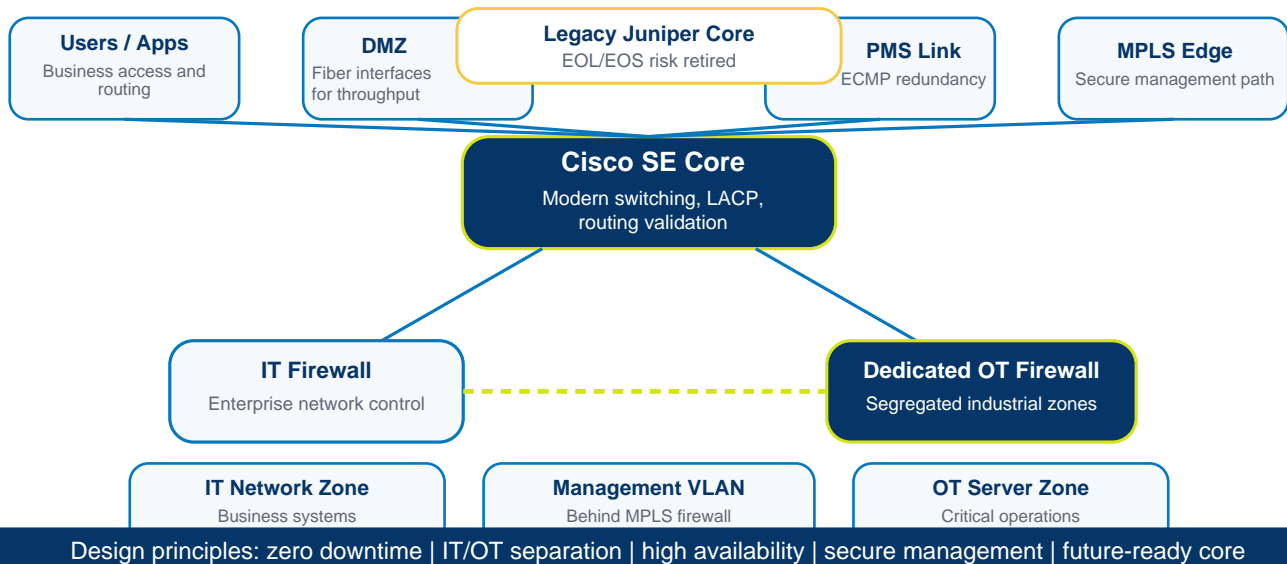


Core switch modernization, IT/OT segregation, DMZ fiber upgrade, ECMP redundancy and secure management access

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

REFERENCE ARCHITECTURE - CORE MODERNIZATION AND IT/OT SEGREGATION



Engagement Highlights

- Decommissioned the legacy Juniper core switching layer and migrated to high-performance Cisco SE switches.
- Executed a pre-activity validation phase covering route verification, LACP checks, physical cabling, and cutover readiness.
- Introduced a dedicated OT firewall to segregate critical server zones and core OT traffic from the IT security perimeter.
- Upgraded DMZ interfaces from copper to fiber to improve bandwidth, reliability, and perimeter connectivity resiliency.
- Implemented ECMP on the PMS link to support load balancing, path optimization, and redundant traffic forwarding.
- Created a dedicated management VLAN behind the MPLS firewall to support secure out-of-band-style administration.

Technical Deployment Scope

- Core Switching Layer: Cisco SE switches replaced legacy Juniper core infrastructure, with validated route tables, LACP state, and physical cabling before cutover.
- IT Security Zone: IT traffic continued through enterprise firewall controls, with clear separation from OT-bound pathways.
- OT Security Zone: A dedicated OT firewall isolated industrial server zones and critical OT traffic from the IT perimeter.
- DMZ Connectivity Layer: DMZ interfaces were migrated from copper to fiber to improve throughput and link reliability.
- PMS Resilience Layer: ECMP was enabled on the PMS link to provide path redundancy, better load distribution, and failover readiness.
- Management Access Layer: A dedicated management VLAN behind the MPLS firewall improved secure administrative access to network devices.
- Migration Control Scope: Pre-checks, cutover plans, rollback readiness, route validation, and post-cutover verification governed the migration lifecycle.

Core Infrastructure & IT/OT Security Transformation



Core switch modernization, IT/OT segregation, DMZ fiber upgrade, ECMP redundancy and secure management access

KEY STRATEGIES

Operations Assurance Model

Pre-validation, secure cutover, segmentation, post-migration verification and support readiness



- Risk-Led Modernization: The program prioritized unsupported core switching, flat segmentation, and OT exposure as business-critical risk areas.
- Zero Business Impact Execution: Migration windows, dependency mapping, pre-validation, and controlled cutovers were designed to avoid service interruption.
- Segmentation by Design: IT and OT flows were separated using a dedicated OT firewall to reduce lateral movement risk and protect industrial operations.
- High-Availability Planning: Routing, LACP, cabling, ECMP, and failover paths were validated before production migration activities.
- Perimeter Throughput Optimization: DMZ copper-to-fiber upgrades improved performance and reliability for critical perimeter interfaces.
- Secure Administration Model: A dedicated management VLAN behind the MPLS firewall strengthened administrative isolation and access governance.
- Future-Ready Infrastructure: Cisco SE core switching created a more supportable, scalable, and standards-aligned network foundation.
- Compliance-Aligned Governance: IT/OT segregation and controlled access support industry expectations for critical infrastructure security.

EXECUTIVE TAKEAWAY

COMnet transformed an obsolete and flat network architecture into a secure, segmented, and future-ready infrastructure foundation. By combining Cisco core modernization, IT/OT segregation, DMZ fiber upgrades, ECMP redundancy, and secure management access, the program reduced operational risk while preserving business continuity throughout the migration.

OUTCOME SNAPSHOT

- Zero downtime migration across core routing, switching, firewall, and network optimization activities.
- Reduced cyber risk through IT/OT segregation and dedicated firewall control for operational technology zones.
- Higher infrastructure capacity, supportability, and resilience through Cisco SE switching, fiber interfaces, and ECMP.

TRANSFORMATION SUMMARY

Cisco SE core modernization | IT/OT segregation | OT firewall | DMZ fiber | ECMP | secure management VLAN | zero downtime