Secure Connectivity Modernization for Power Sector Operations

Power Sector Connectivity Modernization with SD-WAN, Zero Trust Network Access (ZTNA), Cloud WAF, and 24x7 Managed Support

EXECUTIVE CONTEXT

COMnet partnered with a leading power-sector enterprise to modernize secure connectivity across distributed plant locations. The engagement focused on enabling uninterrupted VC access, preserving a consistent user experience inside and outside the office, and improving website security. The solution combined SD-WAN across 19 plants, zero-touch rollout through a central manager, industry-aligned Zero Trust Network Access (ZTNA), and a cloud-based Web Application Firewall (WAF) protecting 10 web properties supported by a 24 X 7 managed services

19
Plants on SD Wan

ZTNA
Posture based access

10
URLs on WAF

IMPACT

- Improved connectivity resilience across 19 plant locations through SD-WAN-based branch modernization and controlled failover behavior.
- Enabled a consistent access experience for users working both inside and outside the enterprise network, reducing productivity friction.
- Strengthened access security by applying ZTNA controls and user/device posture checks before granting application access.
- Enhanced public-facing web protection through a cloud-based WAF deployed for 10 URLs, reducing exposure to web-layer threats.
- Established an operational support construct with 24x7 remote handling for S2/S3 incidents and onsite engineering for S1 severity cases.

MAJOR ISSUES

- The client needed to deliver VC and collaboration access without disruption across a geographically distributed power-sector footprint.
- User access patterns inside and outside the office required a more uniform and secure connectivity model than traditional perimeter approaches.
- Distributed plants demanded centralized rollout and policy control to avoid inconsistent deployments and operational overhead.
- Website exposure created a need for stronger web application protection against internet-facing attacks and availability risks.
- The organization required controlled failover, posture-based access control, and an operating model capable of supporting critical operations continuously.

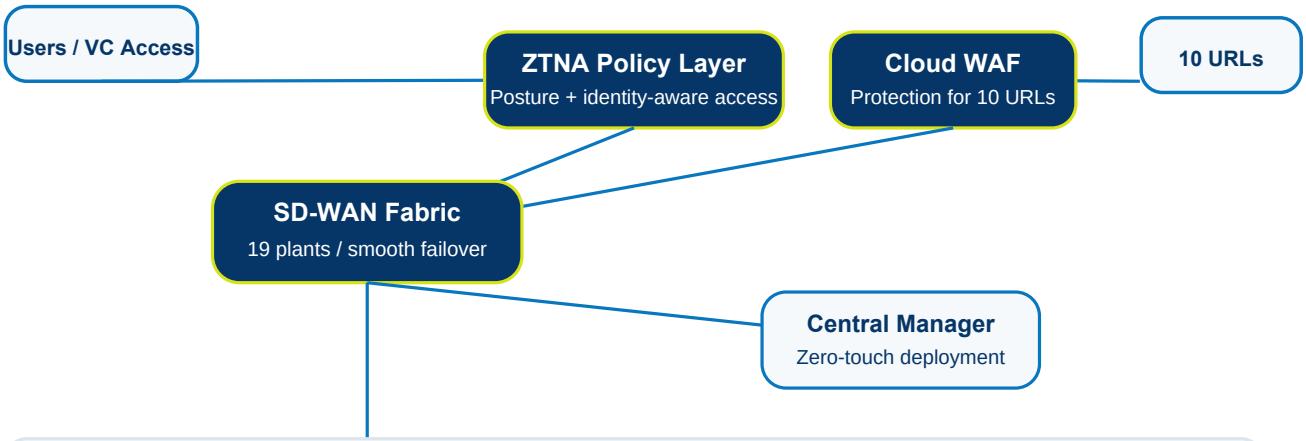
Secure Connectivity Modernization for Power Sector Operations

Power Sector Connectivity Modernization with SD-WAN, Zero Trust Network Access (ZTNA), Cloud WAF, and 24x7 Managed Support

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

REFERENCE SECURITY ARCHITECTURE



- Configured 19 plants with SD-WAN to modernize branch and site connectivity.
- Implemented zero-touch deployment through a central manager to accelerate rollout and simplify remote provisioning.
- Configured ZTNA controls in line with industry-standard secure-access principles.
- Deployed a cloud-based WAF to protect 10 URLs and improve web security posture.
- Enabled remote support for S2 and S3 incidents with onsite engineer support for S1 severity situations.
- Delivered posture checks for all users and preserved user experience both in-office and remote, with smooth failover behavior.

- Secure Access Layer: ZTNA enforced identity-aware and posture-based access for users connecting from internal and external environments.
- Network Modernization Layer: SD-WAN was deployed across 19 plants to deliver optimized routing, centralized policy, and improved failover behavior.
- Centralized Control Plane: A central manager enabled zero-touch provisioning, policy orchestration, and remote lifecycle management for the plant estate.
- Web Protection Layer: A cloud-based WAF secured 10 internet-facing URLs against common web-application attack vectors and exposure risks.
- User Experience Scope: The design preserved a consistent access experience for collaboration and business applications regardless of user location.
- Support and Operations: 24x7 remote support handled S2 and S3 incidents, while onsite engineering support addressed S1 severity events.

Secure Connectivity Modernization for Power Sector Operations

Power Sector Connectivity Modernization with SD-WAN, Zero Trust Network Access (ZTNA), Cloud WAF, and 24x7 Managed Support

KEY STRATEGIES

- Connectivity Without Disruption: The transformation prioritized uninterrupted VC and application access so operational teams could transition without business impact.
- Zero-Trust Access Modernization: ZTNA replaced implicit trust with identity, device posture, and policy-based access decisions suited to distributed work patterns.
- Centralized Rollout at Scale: Zero-touch deployment via a central manager reduced deployment time, minimized manual effort, and improved consistency across 19 plants.
- Resilience by Design: SD-WAN routing, failover policy, and centralized orchestration were designed to maintain continuity under network path changes or outages.
- Web-Risk Reduction: Cloud WAF controls were introduced to protect public-facing applications and improve internet-facing security posture.
- Operational Severity Model: A tiered support framework balanced 24x7 remote service continuity with onsite escalation support for critical incidents.
- User-Centric Security: Security controls were implemented to improve protection while maintaining a familiar user experience for in-office and remote access.

EXECUTIVE TAKEAWAY

COMnet transformed a distributed connectivity challenge into a secure-access and network-modernization program built on SD-WAN, ZTNA, cloud WAF, and centralized rollout governance. The result was a more resilient user-access model, improved website protection, and a supportable architecture aligned to the operational demands of the power sector.

OUTCOME SNAPSHOT

- Stronger secure connectivity across distributed power-sector sites.
- Higher confidence in user posture validation, web protection, and failover readiness.
- A scalable, centrally managed foundation for future access and network modernization.

TRANSFORMATION SUMMARY

19-plant SD-WAN | ZTNA posture checks | cloud WAF for 10 URLs | zero-touch deployment | 24x7 managed support