Modernization of Mission-Critical Networks

February 6, 2026

The continuous, resilient operation of defense critical infrastructure is fundamental to preserving national security, maintaining operational readiness, and executing mission objectives. Technology is now the decisive force multiplier in modern warfare, and reliable network connectivity and security form the absolute foundation that enables it all.

As our reliance on network-centric operations grows, we place ever-greater demands on the network infrastructure—from tactical edge communications to strategic command centers. We expect our mission-critical networks to be ultra-reliable, high-speed, and impenetrable, because failure is not an option in defense of the nation.

Organizations responsible for maintaining these vital capabilities and strategic assets face an unprecedented convergence of dynamic threats and operational complexity, driven by the key factors including:

Existential risk of Quantum Day and harvest now, decrypt later attacks

A new, invisible risk is emerging, Quantum Day (Q-Day), the moment a cryptographically relevant quantum computer becomes operational. At that point, current public-key encryption standards could be decisively broken, threatening the long-term confidentiality of sensitive data. Adversaries are not waiting for Q-Day. They are already leveraging "harvest now, decrypt later (HNDL)" tactics—stealing encrypted data today in the hope that future quantum computing capabilities will eventually decrypt it and compromise current or future missions.

Failure of the traditional network perimeter

Relying solely on a single, hardened edge is no longer viable against sophisticated nation-state threats. The challenge is the need for a multi-layered, Zero Trust defense strategy that includes next-generation perimeter control (inbuilt firewall capabilities) and mandates the establishment of a physically or logically air-gapped trust boundary to strictly isolate mission-critical functions from non-critical networks and shared domains.

Hardware and software tampering risk

Critical military networks face the specific risk of sophisticated supply chain attacks, where compromised hardware or software components are introduced during manufacturing or deployment. This requires defense against tampered components and demands end-to-end integrity verification (attestation) throughout the lifecycle to maintain the Trusted Supply Chain and ensure mission assurance.

Complexity of multi-domain transport networks

Critical infrastructure often relies on a mix of diverse media (ground-based fiber, satellite, cellular, and so on) and in some cases non-trusted network providers. The challenge is integrating these different links into a single, cohesive, and agile overlay and underlay transport fabric that allows for intelligent, mission-based routing and traffic steering across the entire domain.

Mandate for operational continuity and resilience

For mission-critical systems, even brief outages can have immediate, real-world consequences. Maintaining these services requires more than basic uptime; it demands five-nines high availability and intrinsic resilience. Strategies must go beyond patching known vulnerabilities—they must actively defend against advanced attacks, including those exploiting zero-day threats. By proactively mitigating such risks, military organizations can help ensure operational continuity and mission success.

Manual configuration risks and the need for intelligent automation

The speed and tempo of military operations demand the ability to rapidly build, deploy, and tear down network segments (for example, Forward Operating Bases or temporary command centers). The challenge is that current manual, box-by-box configuration processes are intrinsically slow, non-repeatable, and prone to catastrophic outages due to human error. This reliance on manual effort makes it virtually impossible to guarantee that every device in the domain is running a validated, security-hardened configuration. The operational mandate is the urgent need to transition to intelligent automation, moving away from individual device configuration toward adopting a single, secure Golden Configuration baseline to configure multiple devices at the same time.

Observability and monitoring

Defense and military networks operate across multiple domains—land, air, sea, cyber, and space—and demand high levels of security, resilience, and interoperability among coalition partners. To meet these requirements, observability is essential for enabling proactive monitoring, rapid issue detection and resolution, as well as advanced security and threat detection capabilities. This ensures mission-critical network performance and robust defense against evolving threats.

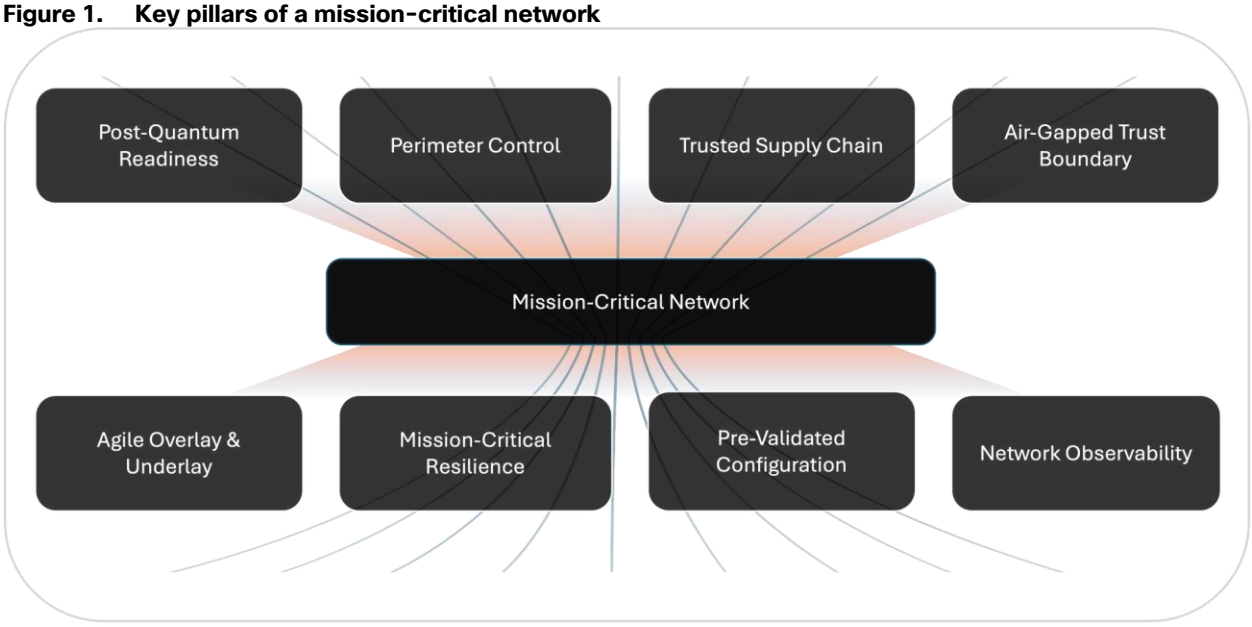
Given this escalating landscape of existential threats and the imperative for operational resilience, immediate and decisive action is necessary. The Cisco mission-critical network solution is engineered to address these challenges, delivering the requisite continuous connectivity and security framework to ensure mission success.

Cisco’s mission-critical network solution

Cisco’s mission-critical network solution delivers a next-generation routing and security architecture specifically designed to secure and modernize the networks that underpin national infrastructure. This solution ensures continuous connectivity and uncompromising security across all network layers, guaranteeing the integrity and availability of data.

The core architectural framework is built upon foundational principles to deliver a highly available, stable, and resilient network, ensuring the system can adapt to evolving demands while maintaining always-on service.

Figure 1. Key pillars of a mission-critical network



Post-quantum readiness

To ensure the long-term confidentiality and sovereignty of nationally sensitive data, the solution integrates a crypto-agile architecture ready for the emerging threat enabled by quantum computing. This is achieved through the implementation of Post-Quantum Cryptography (PQC) mechanisms across the entire security stack to protect against future decryption threats. The architecture is fully NIST-compliant, ensuring it is ready to swiftly deploy certified PQC standards, thereby protecting critical data from future quantum decryption risks.

Perimeter control

The solution leverages next-generation security architecture to establish a security perimeter. This includes the router's inbuilt firewall capabilities, which perform stateful inspection and packet filtering. These mechanisms act as the network's first gatekeeper, controlling inbound and outbound traffic to proactively prevent unauthorized access and cyber threats from penetrating the critical network boundary.

Trusted supply chain

The solution security strategy incorporates end-to-end hardware and software integrity verification to ensure all components are genuine and untampered, protecting the network against sophisticated supply chain attacks.

Air-gapped trust boundary

The solution mandates the establishment of a logically air-gapped environment for control and management plane functions. This boundary is defined to strictly isolate the mission-critical network from the public Internet and other non-critical enterprise services, creating a fully isolated operational domain. This ensures that a security event in a non-critical network cannot laterally affect the core national infrastructure services.

Agile overlay and underlay transport

The architecture natively supports modern network designs and a diverse set of transports, including ground-based (wired) and satellite (wireless) links, and several overlay and underlay technologies.

Mission-critical resilience

Stability and resilience are guaranteed by implementing device high availability and redundancy at every network layer. This is achieved by deploying purpose-built routing platforms engineered to meet the performance and uptime demands for edge and core network segment requirements.

Prevalidated configuration

The solution eliminates slow, error-prone manual configurations by mandating a shift to intelligent, zero-touch provisioning. This capability leverages prevalidated golden configurations, to guarantee a consistent and repeatable policy posture across multi-domain architectures. Orchestration is managed by trusted, on-premises systems to ensure security and reliability. The system incorporates configuration versioning and automated rollback functionality, enabling an immediate recovery to a known working state if a change causes issues, maximizing mission uptime.

Network observability

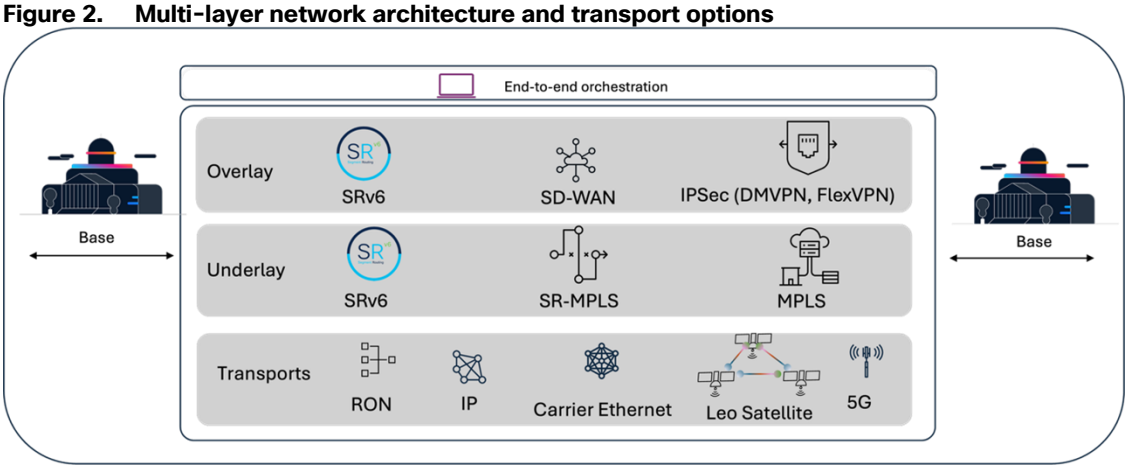
Observability in mission-critical network solutions eradicates blind spots by delivering continuous, comprehensive visibility into network, security, and operational telemetry. This capability is enhanced through integration with Splunk, which provides unified full-stack observability across on-premises, hybrid, and multi-cloud environments. Tailored for demanding environments such as defense networks, this integrated observability framework ensures proactive monitoring, and enables rapid troubleshooting, thereby maximizing resilience and operational continuity in defense network infrastructures.

High-level design and architecture

The next-generation Cisco mission-critical network architecture is built upon the critical separation of physical transport mechanisms from the logical service delivery layer, ensuring maximum resilience, policy enforcement, and agility.

This architecture illustrates the key components that form a highly available, secure, and resilient network infrastructure. We'll explore a layered approach, from physical transport to intelligent orchestration, that ensures connectivity and service delivery.

Figure 2. Multi-layer network architecture and transport options



End-to-end orchestration

At the top, we have end-to-end orchestration. This represents the intelligence layer that automates, manages, and provisions services across the entire network stack. It's vital for simplifying operations, ensuring consistent policy enforcement, and rapidly deploying new services, moving towards a truly programmable network.

Overlay networks and key technologies

The overlay is a policy-driven, logical network constructed on top of the physical infrastructure. It provides virtualized network services, logical connectivity, network segmentation, and application-level security—operating transparently regardless of the underlying physical transport. Overlays are essential for enforcing zero-trust principles, maintaining strict control over data flows, and delivering application services with necessary encryption and segmentation. Key overlay technologies include Software-Defined Wide Area Networking (SD-WAN), large-scale IPsec tunneling (such as DMVPN), or a modern SRv6 service layer. These technologies enable organizations to deploy overlays that meet modern security, scalability, and operational requirements.

Underlay network and key technologies

The underlay network forms the foundational, physical transport layer responsible for the efficient and reliable forwarding of packets between network devices across diverse locations. In a mission-critical network, the underlay is strictly controlled and prioritized, typically utilizing high-performance private infrastructure such as dedicated fiber, MPLS, Segment Routing MPLS (SR-MPLS), or native SRv6. This foundation is engineered to deliver extreme availability, deterministic performance, and low-latency—meeting the rigorous demands of mission-critical operational services.

For remote or tactical deployments, the architecture supports the use of third-party or shared transport (such as the Internet, LTE, or Satellite) as the underlay. In these scenarios, all data is secured end-to-end

through ubiquitous IPsec or MACsec encryption, ensuring confidentiality and integrity regardless of the underlying transport.

Note: SRv6 can be used to build both underlay and overlay networks, offering a unified IPv6-based approach for both physical infrastructure and logical services.

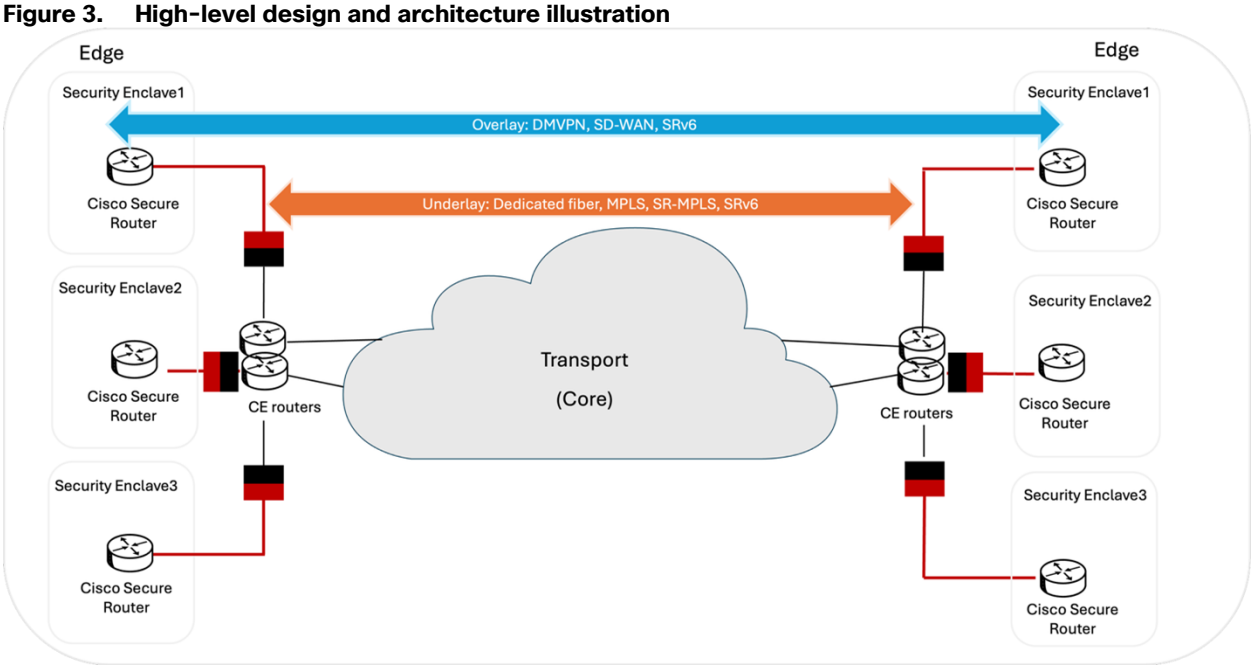
Transport layer

The transport layer represents the physical connectivity options that underpin the entire network. Some of the different transport types include MPLS, Internet broadband, LTE/5G, LEO satellite, leased line/dedicated fiber.

This layered architecture, from diverse transports to flexible underlay, overlay, and intelligent end-to-end orchestration, is designed to create a network that is inherently highly available, secure, and resilient. Cisco's solutions leverage these technologies to build future-ready networks capable of supporting demanding applications and services.

Here's a pictorial representation of the high-level design and architecture for the defense vertical.

Figure 3. High-level design and architecture illustration



The figure illustrates how multiple PQC-ready Cisco Secure Routers deployed at various locations establish secure, logical connections (Overlay Transport) over a shared, underlying infrastructure (Underlay Transport).

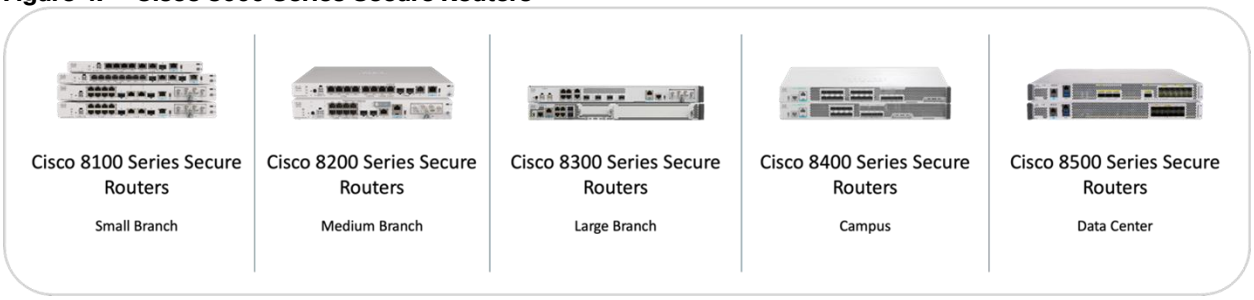
In this design, the security function is handled by IPsec VPN devices (IVDs), which are positioned to encrypt the data traffic before it is transmitted across the wide area network (WAN) transport.

This architecture directly relates to the capabilities of next-generation hardware. Let's explore the features and performance of the Cisco 8000 Series Secure Routers, which are ideally suited to implement this high-security, high-performance transport model.

The Cisco 8ooo Series Secure Router: the secure foundation for a mission-critical network

The new Cisco 8000 Series Secure Routers support a wide variety of connectivity options to operate their most critical network infrastructure. This platform brings together essential functions—security, routing, network orchestration and assurance—into a single, cohesive, and resilient solution, vital for maintaining operational continuity and integrity in mission-critical network environments.

Figure 4. Cisco 8000 Series Secure Routers



It serves as a single platform with core capabilities and differentiators for a mission-critical network.

Post-quantum cryptography ready

Cisco 8000 Series Secure Routers achieve quantum readiness by supporting post-quantum cryptographic algorithms, integrating with quantum key distribution hardware and employing quantum-resistant session key services to ensure secure networking in a quantum-threatened future.

For more details regarding Post-Quantum Cryptography (PQC) readiness in Cisco 8000 Series Secure Routers, see the white paper posted on the Cisco community, Quantum Era - PQC Unlocked: Securing Data in the Quantum Era.

Embedded security and secure boot

We discussed the necessity of perimeter security, as well as the integrity of hardware and software within defense and tactical networks. The Cisco 8000 Series Secure Routers include embedded security features such as Zone-Based Firewall (ZBFW) as part of their comprehensive security solutions. Additionally, they incorporate a Trust Anchor module (TAm), which is a tamper-resistant chip that provides several security features, including secure boot and image signing, run-time defenses, and supply chain security. This ensures the cryptographic integrity of the device firmware from the start.

Air-gapped and on-premises management

The Cisco 8000 Series Secure Routers provide both air-gapped and on-premises management options specifically designed for environments with stringent mission assurance and threat resilience. These options enable complete control over network management without reliance on external cloud connectivity, network Isolation through physical and logical separation from public or external networks to prevent unauthorized access and data sovereignty by ensuring that sensitive data remains within the controlled environment, complying with regulatory and security requirements.

Mission critical service-availability

Uninterrupted access to critical applications and services is vital in mission-critical environments, where five-nines (99.999%) service availability is the standard. This high level of reliability is achieved through N+1 redundancy for all network elements—including routers, security appliances, and WAN transports like

fiber, cellular, and satellite. Seamless failover is maintained using VRRP, while ECMP ensures both load-sharing and active path redundancy. High-availability firewall clusters provide continuous security enforcement, and NAT redundancy preserves session continuity during device failures. Designed to meet these rigorous demands, Cisco 8000 Series Secure Routers natively integrate these features, delivering resilient, always-on connectivity even during unexpected network events or component failures.

Predefined validated configurations

Cisco 8000 Series Secure Routers deployed in mission-critical networks benefit from predefined, validated configurations hosted in configuration catalogs on the Catalyst SD-WAN Manager (formerly Cisco vManage). These catalogs contain industry best-practice configuration groups and policies that have been rigorously tested and validated by Cisco to ensure reliability and security. Using these catalogs, network administrators can quickly power routers and apply base configurations automatically, significantly reducing deployment time and minimizing configuration errors.

Enhanced observability for critical networks

Cisco 8000 Series Secure Routers provide robust observability for mission-critical networks by delivering real-time telemetry, such as device status, traffic patterns, and performance metrics, integrated security features like threat detection, firewalling, and secure access controls, and automation capabilities such as the use of software-driven processes to automatically configure, manage, and respond to network events. This combination enables deep visibility into network performance and security, allowing for proactive monitoring, rapid issue detection, and efficient operations. Additionally, integration with Splunk enhances analytics and threat detection, offering a comprehensive observability solution tailored for demanding environments like defense networks.

Conclusion

The modernization of mission-critical networks is essential to ensure continuous, secure, and resilient operations that underpin national security and vital services. Cisco's mission-critical network addresses the evolving threat landscape. This future-proof architecture includes post-quantum cryptography and principles of Software-Defined Networking (SDN). The Cisco 8000 Series Secure Router platform further consolidates security, routing, and network assurance into a unified, scalable solution designed for the most demanding critical infrastructure environments. Together, these innovations enable mission-critical networks to adapt, survive, and thrive in an increasingly complex digital world.