Zero-Fail Connectivity for Air-Gapped Networks

May 5, 2026

Introduction: Delivering modern air-gap strategy

In an environment where ‘trust but verify’ is the operational standard, the choice of a technology partner is as critical as the network architecture itself. For defense teams and critical infrastructure operators, the mandate for total isolation has moved beyond simply ‘pulling the plug.’ Modern missions require a network that is completely self-reliant—where data, technology, and operations remain exclusively on-premises.

Cisco is uniquely positioned to lead this shift as we maintain a transparent chain of control across every layer of the network stack. We engineer our hardware, specifically the Cisco 8000 series secure routers, which form the critical WAN edge for defense networks anchored by the Secure Network Processor (SNP) and silicon-based Trust Anchor module (TAm). By combining specialized silicon with integrated software, Cisco delivers a resilient, reliable, and secure foundation that ensures you maintain exclusive control over your encryption keys and data jurisdiction.

The true value of this Cisco-led architecture is that it removes the penalty of being offline. Traditionally, air-gapping meant sacrificing modern tools like automated orchestration and AI-driven insights. Cisco eliminates this compromise by delivering a fully air-gapped installation of Cisco IQ. This localized, completely isolated deployment ensures that mission-critical teams can operate with the same speed and diagnostic intelligence as cloud-connected enterprises—without ever creating a path through their secure perimeter.

This paper outlines a unified strategy for building high-performance, air-gapped networks. By combining Cisco 8000 Series Secure Routers with SRv6/SD-WAN overlays, offline licensing (PLR/SLR), and localized AI, we provide the blueprint for a network that is both intelligent and entirely under your jurisdiction.

Building a self-reliant mission-critical network

For defense teams and critical infrastructure, moving to a fully on-premises, air-gapped design isn't just a security choice—it is ensuring that the network can function perfectly without any outside interference. This approach protects vital systems from international disruptions, hidden supply chain risks, and foreign legal claims.

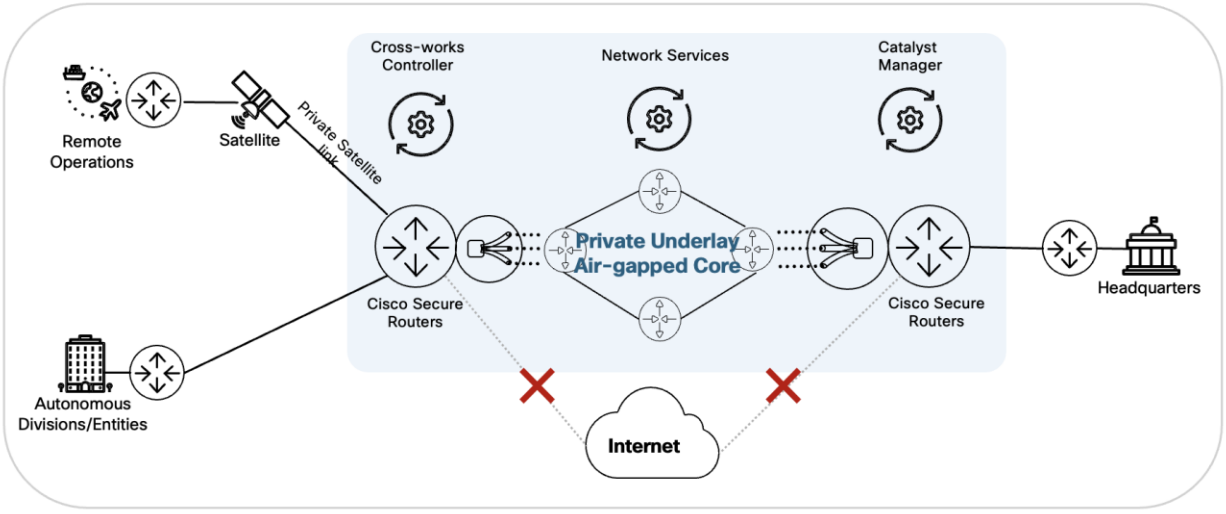
To achieve this level of self-sufficiency, we focus on three core areas of on-premises control:

- Technical Control: Eliminates dependence on hidden or untrusted supply chains. A key part of this is cryptographic control, where you hold exclusive ownership of your encryption keys.
- Data Control: Ensures all data is collected, stored, and processed strictly within your own physical jurisdiction, creating a shield against foreign "call-home" requirements.
- Operational Control: Guarantees the network remains active without ever reaching out to external servers. In this model, all licensing, updates, and management stay within the air-gap.

The following sections explain the specific steps and technologies used to reach these goals.

Architecting for mission resilience

Modern mission requirements do not necessitate sacrificing technical agility for the sake of a secure boundary. Organizations can operate a high-performance Private WAN that remains both logically and physically distinct from public infrastructure.



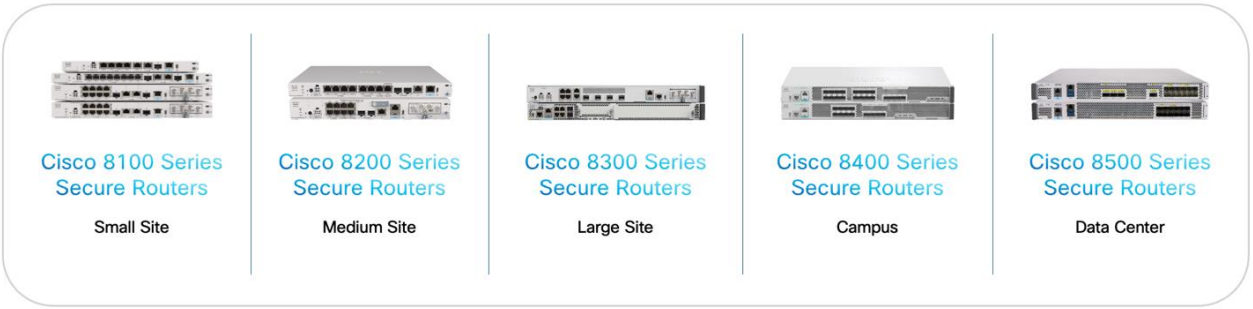
1. Isolation at the Operational Edge

   The architecture's security begins at the boundaries of the isolated environment. Whether it is 'Remote Operations' or fixed 'Autonomous Divisions', we establish total isolation using segmentation right at the network edge.

   One of the ways of achieving this is by using Virtual Routing and Forwarding (VRFs), we create discrete virtual networks on the same hardware. This logical separation is maintained across the entire journey. VRF tags are preserved, ensuring that mission-critical data never "leaks" into routine administrative paths.

2. Role of Edge Routers and Offline Licensing

   For a private WAN to be truly autonomous and segmented, security and intelligence must be integrated directly into the hardware at the network boundary. Cisco 8000 Series Secure Routers act as cryptographic boundaries for the architecture.



   Traffic moves across the segmented foundation using software-defined overlays such as SRv6 and SD-WAN, mapped to specific mission needs. While SRv6 and SD-WAN represent the modern standard, full

support for reliable, traditional IPsec solutions such as DMVPN and FlexVPN is maintained to ensure backward compatibility with existing encrypted tunnels.

Using the Secure Network Processor (SNP) and silicon-based Trust Anchor Module (TAm), these routers perform a verified boot process to ensure hardware integrity and tamper resistance. True autonomy also requires that the software operates in total isolation.

Most modern hardware requires phone-home check-ins to validate licenses. To close this vulnerability and ensure the air-gap remains intact, two completely offline activation methods are utilized:

- Specific License Reservation (SLR): This functions as a node-locked license for secure zones. It enables the activation of specific software features without requiring ongoing external communication. The process involves a one-time manual exchange with the Cisco Smart Software Manager (CSSM) to authorize selected licenses, which are typically valid for a three-year term.
- Permanent License Reservation (PLR): Designed for environments where any external contact is restricted, PLR provides a universal license product identifier (PID) that activates all product functionalities for the life of the hardware. This method eliminates the need for periodic renewals or future connectivity.

Unlike systems that rely on vendor policy alone, this portfolio is engineered so that Cisco cannot remotely access or influence deployed systems. Once these licenses are authorized, the network operates in total isolation.

To learn more about these licensing models, you can refer to the technical documentation on Cisco Smart Licensing.

3. The Private Underlay and Air-Gapped Core

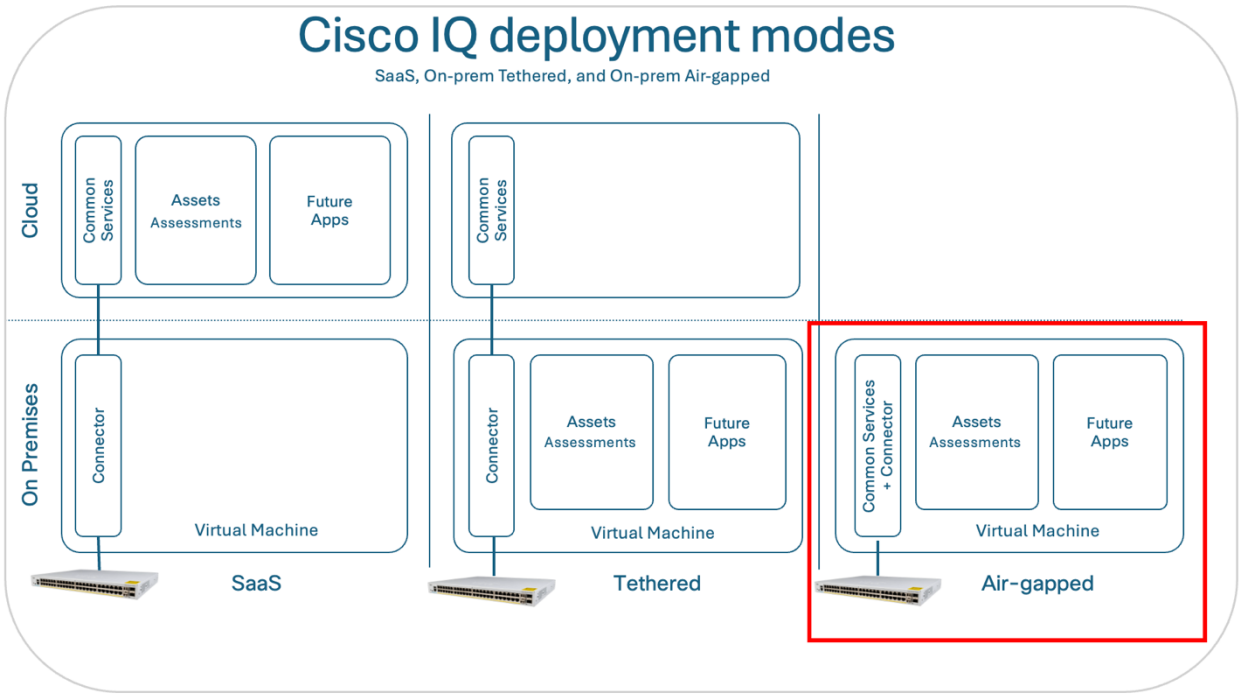
Once traffic is secured and licensed at the edge, it moves into the Air-Gapped Core. To maximize efficiency, organizations can implement SRv6 as the primary underlay. SRv6 simplifies the network by embedding forwarding instructions directly into packet headers, enabling Network Slicing to partition critical data from routine traffic. While SRv6 is the modern standard, the core is transport-agnostic and can be built using SR-MPLS, traditional MPLS, or any dedicated private IP core.

If external data is required, the architecture employs a data diode or proxy—a physical "one-way valve" enforcing unidirectional traffic flow, allowing data only into the secure network and preventing leaks.

Localized management and intelligence

Since these networks cannot rely on external cloud reachability, the entire management stack is hosted internally. This is achieved by deploying all foundational protocols—including DHCP, DNS, NTP, and Zero Touch Provisioning (ZTP)—directly on-site. By using systems like the Crossworks Network Controller and Catalyst Manager, operators gain powerful, API-driven oversight and automation across the entire fabric, ensuring that every configuration change is executed effectively.

To complement this automated management, we integrate Cisco IQ as the specialized intelligence layer of the local stack. While the controllers manage and automate the network's daily operations, Cisco IQ provides the deep, historical reasoning and diagnostic expertise that typically resides in a global cloud. Cisco offers this intelligence through three distinct deployment models to meet varying security needs: a standard SaaS model, a Tethered option where customer data remains private and the only external connection is for software updates, and a fully Air-gapped installation.



For the mission-critical networks described in this paper, the Air-gapped model is the primary standard. In this mode, all customer data is completely private, and the system operates in total isolation within a localized virtual machine. This ensures that mission-critical teams have the advanced reasoning required to solve complex issues with the same speed as cloud-connected enterprises, while maintaining absolute data sovereignty. Operating within the air-gap, this localized AI provides three critical outcomes:

- Proactive Asset Insights: Consolidates purchase contracts, telemetry, and support history into a single interface, tracking hardware lifecycles and identifying relevant Field Notices or Security Advisories without external connection.
- Adaptive Infrastructure Assessments: Uses AI to evaluate operational health and security hardening against best-practice guides, producing structured findings and prioritized recommendations.
- AI-Powered Troubleshooting: Employs agentic AI with hypothesis- and evidence-driven methods to identify root causes, leveraging digitized internal knowledge and anonymized historical data to resolve cases locally, mirroring senior engineer methodologies.

To learn more about Cisco IQ, Refer to the Cisco Services page.

Conclusion

By integrating the Cisco 8000 Series Secure Routers offline PLR/SLR licensing, and Cisco IQ, this architecture provides a stable foundation for mission-critical operations. It ensures that data, technology, and operations remain exclusively under your jurisdiction, providing a powerful defense against evolving global threats while maintaining the agility of a modern network.