Cisco Security Service Edge (SSE) and the NATO Cloud Directive

In today's digital landscape, organizations face complex security challenges across diverse devices, users, and locations. As they embrace hybrid work models and cloud computing, ensuring secure access to applications and data is important. The NATO Cloud Directive emphasizes strong security and compliance standards, crucial for protecting sensitive information.

This Solution Brief explores how the Cisco® Secure Access solution addresses these requirements, offering seamless connectivity and comprehensive protection. By integrating key network security technologies into a unified Security Service Edge (SSE) platform, Cisco enhances cybersecurity while reducing complexity and risk.

We will examine the NATO Cloud Directive's requirements, explore the features and benefits of the Cisco Security Service Edge (SSE) solution—Secure Access—and provide a detailed analysis of how the solution supports compliance with NATO's security standards.

Overview of the NATO Cloud Directive

The Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information systems (AC/322-D (2021) 0032), also known as the NATO Cloud Directive, is a strategic framework designed to secure and modernize the handling of NATO information within cloud-based environments. It aims to enable seamless communication, interoperability, and data-centric operations across the alliance's 32 member states.

Key aspects of the NATO Cloud Directive include:

- **Data Protection:** Ensures robust encryption for data at rest and in transit, compliance with NATO security standards, and adherence to national sovereignty laws.
- **Federated Cloud Model:** Promotes a "cloud-first" approach, integrating Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) into a unified digital backbone.
- **Interoperability:** Facilitates collaboration across multi-domain operations (land, air, maritime, cyber, and space) through standardized frameworks and shared resources.
- **Scalability and Resilience:** Supports dynamic resource allocation and distributed data centers to enhance agility and survivability in crisis scenarios.
- **Governance:** Establishes compliance mechanisms to harmonize policies across member nations while maintaining high security standards.

Understanding Security Service Edge

What is Security Service Edge?

Security Service Edge (SSE) is an approach that helps organizations embrace the rapidly changing digital environment. By improving overall security posture while reducing complexity for both the IT team and end users, SSE protects users and resources and simplifies deployment by consolidating multiple security capabilities—including Secure Web Gateway, Cloud Access Security Broker, and Zero Trust Network Access—and delivering them from the cloud. This consolidation provides secure, seamless, and direct connectivity to the web, cloud services, and private applications.

Cisco Secure Access includes all these elements and more to provide secure connectivity for hybrid workforces, while protecting resources from cyberattacks and data loss. It unifies multiple security functions into a cloud service to protect users and infrastructure from threats.

Cisco Secure Access overview

Cisco Secure Access offers seamless connectivity for both private and public applications, using the most secure connectivity—zero trust access or fallback catchall VPN as a Service (VPNaaS) – as defined by the centralized access policy. The solution leverages capabilities from Cisco's security and networking portfolio, including embedded internet and cloud visibility from Cisco ThousandEyes.

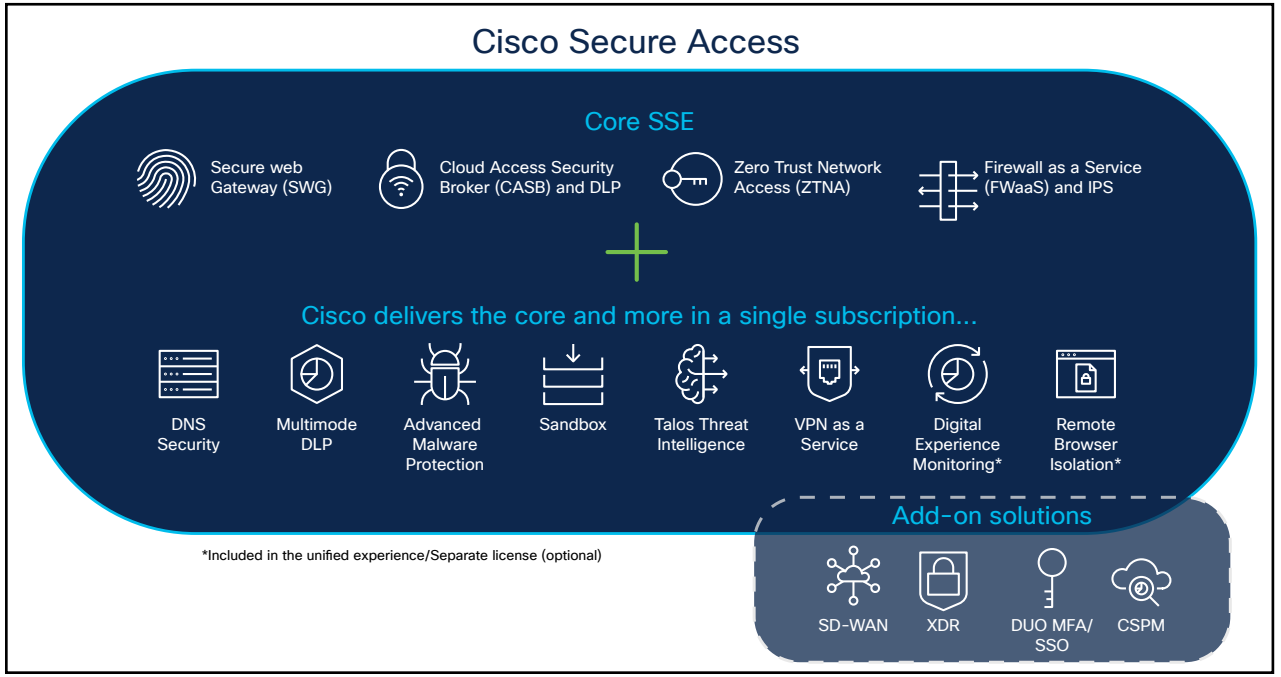

Figure 1. Cisco Secure Access Security Functions

Key benefits

Secure Access consolidates and innovates Cisco's deep portfolio of technologies to provide secure, identity-based access for all users and private applications in the cloud or on premises. It offers several key benefits:

- **Consolidates Security Functions:** Enhance protection through a comprehensive cloud security service that integrates Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), cloud firewall, DNS-layer security, Data Loss Prevention (DLP), and Remote Browser Isolation (RBI).
- **Simplifies the User Experience:** Enable users and devices, even unmanaged ones, to connect securely and effortlessly to the internet and mission-critical applications with confidence.
- **Delivers Security for a Hybrid World:** Continuously enforce granular access controls and security policies, ensuring robust threat protection and stringent compliance across diverse environments.
- **Streamlines IT Operations:** Utilize a single, cloud-managed console for simplified deployment, management, and optimization of your hyper-distributed environment, enhancing operational efficiency.

The solution contains a broad set of capabilities including:

- **Secure Web Gateway (SWG):** Protects web traffic with URL filtering, malware scanning, and Secure Socket Layer (SSL) decryption.
- **Cloud Access Security Broker (CASB):** Manages cloud app usage, detects shadow IT, and enforces security policies.
- **Zero Trust Network Access (ZTNA)/Virtual Private Network as a Service (VPNaaS):** Provides secure access to apps with zero trust principles and VPN for non-web traffic.
- **Firewall as a service (FWaaS):** Offers comprehensive security controls for internet and private traffic.
- **Digital Experience Monitoring (DEM):** Monitors endpoint and network performance to optimize user productivity.
- **DNS security:** Blocks malicious domains at the DNS layer to prevent threats before they reach the network.
- **Remote Browser Isolation (RBI):** Protects against web threats by isolating browsing activity in the cloud.
- **Data Loss Prevention (DLP):** Prevents sensitive data from leaving the organization with inline and API-based controls.
- **Sandboxing/Advanced Malware Protection:** Analyzes unknown files to detect and block malware.
- **Talos® Threat Intelligence:** Provides insight into cyber threats with AI and machine learning models.
- **AI Assistant:** Uses GenAI to help IT admins create security policies and troubleshoot issues.

In addition, the Cisco portfolio includes networking and operations functionality such as:

- **Digital Experience Assurance:** Beyond the DEM capability included in Secure Access, customers with ThousandEyes licenses can get extended visibility across networks and the internet.
- **SD-WAN:** Catalyst® and Meraki™ are available for a single vendor Secure Access Service Edge (SASE) environment with advanced networking capabilities to optimize reliability, performance, and cost.

This converged solution boosts efficiency with a single agent, management console, and unified policy system. Part of the Cisco Security Cloud, it offers a comprehensive cloud-native platform with enhanced threat protection and streamlined management. Consolidated licensing lowers costs, reduces staffing needs, and minimizes hardware requirements.

Supporting NATO Cloud Directive compliance

Cisco Secure Access supports compliance with NATO's Cloud Directive through the following features:

- **Enhanced Security Controls:** By integrating zero trust access and comprehensive security functions like CASB and DLP, Secure Access aligns with NATO's requirements for safeguarding sensitive data in the cloud.
- **Centralized Management:** The unified management console simplifies policy enforcement and compliance monitoring, ensuring consistent adherence to NATO's security standards across all environments.
- **Integrated Threat Intelligence:** Talos threat intelligence provides advanced threat detection and response capabilities, helping meet NATO's proactive cybersecurity objectives.
- **Scalability and Flexibility:** The cloud-based architecture supports NATO's need for scalable, flexible solutions that can adapt to evolving security landscapes and operational requirements.
- **Cost Efficiency:** Consolidated licensing and reduced hardware dependencies help align with NATO's focus on efficient resource utilization while maintaining robust security.

Mapping Cisco Secure Access to NATO Cloud Directive requirements

The NATO Cloud Directive outlines specific security requirements for cloud environments. These requirements are grouped into distinct categories, each focusing on different aspects of security and compliance. Cisco Secure Access aligns with these categories to ensure robust protection of sensitive data and operations within NATO's cloud framework. The Secure Access and NATO Cloud Directive mapping illustrates how Cisco's solutions address each security requirement, supporting NATO's mission-critical cloud operations.

Table 1. Mapping Cisco Secure Access to the NATO Cloud Directive

Control ID and Title	Description	NATO Cloud Directive Mapping to Cisco SSE (Secure Access)
Change Control and Configuration Management (CD4)	Establishes processes for managing changes to systems, documenting configurations, and maintaining system integrity through controlled implementation of modifications.	SM-CCC-04
Cryptography, Encryption, and Key Management (CD5)	Addresses requirements for data protection through encryption, secure key management practices, and cryptographic controls for data at rest and in transit.	SM-CEK-03
Data Center Security (CD6)	Focuses on physical and environmental security measures for cloud infrastructure facilities, including access controls, environmental protections, and facility security.	CM-DCS-08

Get started

Cisco Secure Access offers a comprehensive approach to meeting the stringent security requirements of the NATO Cloud Directive. By aligning with the Directive's distinct security categories, Secure Access ensures robust protection and compliance for NATO's cloud operations. The detailed mapping provided illustrates how Cisco's solutions effectively address each requirement, reinforcing NATO's mission to maintain secure and resilient cloud environments. As cloud technologies continue to evolve, Cisco remains committed to supporting NATO's cybersecurity objectives with innovative and adaptable solutions.

Resources

- IDC Spotlight: Flexibility in Convergence – Delivering on the Promise of Security Service Edge
- Cisco Secure Access At-a-Glance
- Modernizing Government Cybersecurity

Control ID and Title	Description	NATO Cloud Directive Mapping to Cisco SSE (Secure Access)
Data Security and Privacy Lifecycle Management (CD7)	Covers protection of data throughout its lifecycle, including classification, handling, storage, transmission, and secure disposal to maintain confidentiality and privacy.	SM-DSP-07, SM-DSP-09, SM-DSP-10, SM-DSP-11, SM-DSP-17, SM-DSP-20
Identity and Access Management (CD10)	Covers user authentication, authorization, privilege management, and access control to ensure only authorized individuals can access resources.	SM-IAM-01, SM-IAM-02, SM-IAM-03, SM-IAM-04, SM-IAM-05, SM-IAM-06, SM-IAM-07, SM-IAM-08, SM-IAM-09, SM-IAM-10, SM-IAM-11, SM-IAM-12, SM-IAM-13, SM-IAM-14, SM-IAM-15, SM-IAM-16, SM-IAM-17, SM-IAM-18, SM-IAM-19
Logging and Monitoring (CD13)	Covers requirements for event logging, security monitoring, threat detection, and maintaining audit trails to identify and respond to security events.	SM-LOG-02, SM-LOG-03, SM-LOG-03, SM-LOG-04, SM-LOG-05, SM-LOG-06, SM-LOG-08, SM-LOG-09, SM-LOG-14
Security Incident Management, E-Discovery, and Cloud Forensics (CD14)	Addresses incident detection, response, investigation capabilities, and forensic procedures specific to cloud environments.	SM-SEF-09

Learn more

Take the first step towards NATO Cloud Directive compliance.

- Explore Security Service Edge (SSE)
- Explore Cisco Secure Access

C22-5130092-00 05/25