Framework Mapping:

From SIG to S(A)SE: How Cisco maps against the Australian Government Gateway Security Standard

As the Australian Government updates its requirements to modernise Secure Internet Gateways (SIGs), this document explores how to move from traditional SIGs to a modern S(A)SE architecture with Cisco Secure Access and email security.

Background

The Australian Government Gateway Security Standard (Gateway Standard) is a framework designed to ensure compliance with Australian regulatory and security requirements for network gateways and related infrastructure. It is part of a broader set of geo-led compliance requirements that address national security concerns, cybersecurity threats, and data sovereignty, which are increasingly important due to rising geopolitical tensions and the explosion of data generation globally.

This standard aligns with Australia's information security manual (ISM) and Information (ISM) Security Registered Assessors Program (IRAP), a program run by the Australian Cyber Security Centre (ACSC), which is an assessment for cloud and network services, ensuring that products and services meet stringent security controls tailored to Australian government and industry needs. The Australian Government Gateway Standard involves controls for data residency, access management, encryption, and continuous monitoring to protect sensitive information and maintain compliance with local laws.

Cisco's Cloud Controls Framework (CCF) highlights its commitment to global security standards, supporting stringent requirements like Cisco's FedRAMP, ISO 27001, and the Australian ISM. The CCF streamlines compliance, ensuring Cisco SaaS solutions meet Australian regulations with region-specific controls.

The Australian Government Gateway Standard is a pivotal benchmark that bridges legacy policy frameworks with today’s advanced security architectures. By aligning with it, organisations can adopt modern approaches like Secure Service Edge (SSE) and Secure Access Service Edge (SASE), ensuring compliance and fostering innovation.

Understanding Cisco Secure Access

Cisco Secure Access is a converged, cloud-delivered Security Service Edge (SSE) solution designed to provide seamless, secure access for users connecting from any device to any resource, anywhere. It is a foundational component of Cisco's Secure Access Service Edge (SASE) architecture, which integrates multiple security functions into a unified platform to simplify IT operations and enhance security posture.

Key Features and Capabilities

- **Zero Trust Network Access (ZTNA):** Enforces least-privilege access by dynamically authenticating users and evaluating device posture, ensuring secure access to private applications from both managed and unmanaged devices.
- **Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Firewall as a Service (FWaaS):** These core SSE components provide comprehensive protection for internet and cloud access, including content filtering, malware detection, and cloud app visibility.
- **AI-Driven Security:** Cisco Talos threat intelligence powers advanced threat detection and blocking, while AI-assisted policy creation and management simplify administration and speed incident response.
- **Data Loss Prevention (DLP) and Generative AI Controls:** Protect sensitive data and manage the use of AI applications with machine learning guardrails, prompt filtering, and blocking controls.
- **Unified Management:** A single cloud-managed console and client provide centralised policy creation, aggregated reporting, and digital experience monitoring to streamline IT operations and improve user experience.
- **Flexible Deployment:** Supports client-based and clientless access methods, integrates with various identity providers (e.g., AD, Azure AD, Okta), and interoperates with other Cisco and third-party security products.
- **Cisco SASE:** Cisco SD-WAN integration enables a comprehensive SASE architecture. This integration supports direct internet access (DIA) from branches, enhancing performance and lowering costs with Intelligent traffic steering, application-aware routing, and load balancing to optimize application access.
- **Adaptive Identity Policy:** Cisco Secure Access Service Edge (SSE) integrates Cisco IDP (Cisco Duo) and Cisco Identity Intelligence (CII) to strengthen identity security by correlating user data, with role-based access, and enabling real-time threat detection through behaviour analysis, while centralised management simplifies policy enforcement, enhancing zero trust access within SSE.
- **Fine Grained Policy:** Fine-grained policy in SSE enables precise, attribute-based access control by setting detailed rules based on user behaviour, device posture, applications, and context. It enforces specific permissions at a granular level, supports zero trust by dynamically adjusting access, and continuously improves security through ongoing evaluation.
- **Sandboxing:** Cisco Secure Malware Analytics is a unified malware analysis and threat intelligence solution that enables organisations to perform

advanced malware analysis and gain context-rich threat intelligence either on-premises or via cloud subscription. It integrates with existing Cisco security products and third-party technologies to provide detailed malware behaviour analysis, rapid threat prioritization, and automated detection and response capabilities, helping security teams identify and mitigate advanced malware attacks efficiently.

Additional gateway services

- **Email Security Services:** Cisco Email Security (Secure Email Gateway) provides advanced threat protection by detecting, blocking, and remediating email threats such as spam, malware, ransomware, and phishing, while also securing sensitive information with data loss prevention and encryption. Cisco Secure Email Threat Defense enhances Microsoft 365 security by offering comprehensive visibility into inbound, outbound, and internal emails, using AI-powered threat detection and fast remediation to protect against sophisticated attacks like business email compromise and account takeover.

Benefits

- **Accelerated Compliance and High Assurance:** Cisco Secure Access has achieved the following Certifications: SOC2 Type 2, ISO 27001, ISO 27018, CSA STAR, Germany's C5, Spain's ENS High, Japan's ISMAP, HIPAA, PCI-DSS.
- **Seamless and Secure Access:** Users can securely connect to any app or resource using any protocol or port, from any location.
- **Simplified IT Operations:** Centralised management reduces complexity and administrative overhead.
- **Enhanced Security Posture:** Zero trust principles, granular policies, and real-time threat intelligence reduce risk and protect against sophisticated cyber threats such as phishing, ransomware, and data exfiltration.
- **Visibility and Control:** Provides insights into cloud application usage, shadow IT, and network traffic, enabling proactive security and compliance.
- **Support for Hybrid Work:** Designed to protect a distributed workforce accessing resources across on-premises, cloud, and SaaS environments.

Cisco Secure Access is available in multiple tiers—Essentials, Advantage, and DNS Defense—allowing organisations to select the appropriate level of security and functionality based on their needs. It also includes VPN-as-a-Service (VPNaaS) capabilities and supports advanced features like digital experience monitoring and reserved IP addresses.

Cisco Secure Access delivers a comprehensive, cloud-native security platform that enables organisations to protect users, data, and applications in today’s hybrid and cloud-centric work environments, while simplifying security management and improving operational efficiency.

Mapping the Framework

The security controls and operational processes that enabled Cisco Secure Access provide a strong foundation for meeting the stringent requirements of the Australian Government Gateway Standard. The following tables offer a clear alignment between Secure Access' features and the foundational technical components of the Australian Government Gateway Security Standard, illustrating how this architecture's capabilities enhance overall security and compliance.

Gateway Hosting

The Australian Gateway Standard defines Gateway Hosting as the responsibility of gateway solutions to implement comprehensive security measures to protect sensitive and classified information. Gateways, especially monolithic ones, act as critical points for data transit between security domains and are therefore at risk of compromise. The hosting location of gateways can significantly impact network performance, particularly for organisations with geographically dispersed offices or remote workforces.

Specifically, the standard requires that on-premises gateway infrastructure must be physically hosted within the appropriate Security Zone corresponding to the highest security domain it manages, in line with PSPF Requirement 0094 and PSPF Release 2025 guidance. For cloud-hosted or outsourced gateways, hosting must be within data centers or cloud providers certified under the Hosting Certification Framework (HCF), except for internationally hosted infrastructure.

Table 1. Cisco Secure Access Mapping to Australian Gateway Standard Requirement: Gateway Hosting

Requirement: Gateway Hosting	How Cisco Meets/Supports Compliance
Security of On-Premises Gateways	Cisco supports by providing flexibility for providing on-premises solutions like email, web proxy, sandboxing, firewall for those organisations. We work with our managed service providers and departments to meet on-premises gateway requirements. Additionally, Cisco Secure Access supports on-premises networks by enabling secure connectivity through IPsec tunnels from on-prem network devices such as Cisco Catalyst SD-WAN devices, Cisco ISR, Cisco ASA, and Cisco Secure Firewall.
Security of Cloud Hosted or Outsourced Gateways	Cisco Secure Access demonstrates a proven ability to exceed stringent government certification requirements. This ensures cloud-hosted gateways meet standards like the Hosting Certification Framework (HCF) and supports managed service provider environments with documented shared responsibility models for key management and security controls. Australian Secure Access Policy Enforcement Points (PEP) are hosted in HCF-certified facilities.
International Gateway Infrastructure	Cisco Secure Access supports international points of presence with risk-based assessments and controls. its global infrastructure and threat intelligence capabilities enable secure handling of data at network edges while maintaining compliance with risk management requirements.

This framework ensures that gateway hosting environments maintain the necessary physical and operational security controls to protect data integrity and confidentiality while balancing performance considerations for distributed environments.

Gateway Operations and Monitoring

The Australian Gateway Standard emphasizes the critical importance of Gateway Operations and Monitoring to ensure effective protection and management of data transiting between security domains. It mandates that gateway solutions provide Australian Government entities with sufficient visibility over both incoming and outgoing traffic to implement necessary security measures and manage risks effectively. This includes generating comprehensive logs and telemetry from multiple ingress and egress points, which are essential for detecting and investigating cybersecurity incidents. Entities are required to feed relevant gateway logs into centralised logging solutions and can refer to the Information Security Manual (ISM) Guidelines for System Monitoring and the Gateway Security Guidance Package for best practices on event logging and threat detection.

Traffic inspection is essential, with entities needing to ensure they can decrypt or inspect network traffic to enforce gateway policies, including content filtering and Data Loss Prevention (DLP). Where inspection is not possible, traffic should be blocked or quarantined. Deep Packet Inspection (DPI) is recommended as a risk-based approach to detect malicious payloads within packets.

Table 2. Cisco Secure Access Mapping to Australian Gateway Standard Requirement: Gateway Operations & Monitoring

Requirement: Gateway Operations & Monitoring	How Cisco Meets/Supports Compliance
Log Collection	Cisco Secure Access generates comprehensive logs and telemetry across multiple ingress and egress points. It integrates with centralised logging and SIEM solutions, supporting incident detection and response aligned with ISM guidelines and Gateway Security Guidance Packages.
Traffic Inspection	Cisco Secure Access provides deep traffic inspection capabilities, including decryption and inspection of encrypted traffic, enabling enforcement of content filtering and Data Loss Prevention (DLP) policies. It supports host-based measures and risk-based blocking or quarantining of uninspectable traffic.
Deep Packet Inspection (DPI)	Cisco Secure Access includes DPI features that inspect packet payloads and headers to detect malicious code and threats, applying risk-based approaches to balance security and privacy.
Cyber Threat Intelligence (CTI)	Cisco Secure Access leverages Cisco Talos threat intelligence to provide threat blocking and rapid investigation capabilities, enhancing security by applying zero trust principles and enforcing granular policies. Additionally, Splunk has a plug-in that integrates Splunk Enterprise Security with ASD's Cyber Threat Intelligence Sharing (CTIS) platform.
BGP Route Security	Cisco routers and platforms that handle BGP routing support full RPKI-based validation to verify that IP address announcements come from authorised sources.

Gateway solutions also play a vital role in Cyber Threat Intelligence (CTI) by observing adversarial behaviour and sharing intelligence via the ASD's Cyber Threat Intelligence Sharing (CTIS) platform, enhancing threat visibility and response.

Additionally, the standard requires robust Border Gateway Protocol (BGP) route security measures, including the use of Resource Public Key Infrastructure (RPKI) and Route Origin Authorization (ROA) records to prevent route hijacks and ensure the integrity of public IP address routing.

Overall, Gateway Operations and Monitoring under the Australian Government Gateway Standard ensure that entities maintain comprehensive oversight, logging, inspection, threat intelligence sharing, and routing security to protect sensitive government data and infrastructure.

Gateway Services

The Australian Gateway Standard secures and manages data traffic between security domains through key services such as:

- **Domain Name System (DNS):** Responsible for translating domain names to IP addresses and supporting resource record queries. Protective DNS (PDNS) services are mandated to block connections to known malicious endpoints, enhancing security by preventing access to harmful domains. DNS Security Extensions (DNSSEC) verify the integrity of DNS records, while DNS encryption methods (such as DNS over TLS, HTTPS, or QUIC) are recommended where visibility can be maintained to protect confidentiality without compromising security policy enforcement

- **Mail Relays:** These email gateways enforce security policies on email traffic entering and leaving security domains. They ensure email encryption using protocols like Opportunistic TLS with ASD Approved Cryptographic Algorithms, implement email authentication protocols (SPF, DKIM, DMARC) to prevent spoofing, and enforce protective markings on emails. Additionally, mail relays perform content filtering to detect and quarantine malicious email content.

- **Web Proxies:** Positioned between users and the internet, web proxies enforce web security policies through content filtering, malware scanning, and logging. They restrict access to unauthorised cloud services, block access to uncategorised or malicious websites, and support malware detection using various techniques including sandboxing and threat intelligence. Web proxies also support identity awareness for user authentication and access control.

- **Reverse Web Proxies:** These sit between public websites/web applications and the internet, providing security capabilities such as traffic forwarding only to approved destinations, restricting unauthorised cloud service access, malware detection, TLS termination for inspection, deny listing, HTTP header inspection and manipulation, and Denial of Service (DoS) protection.

- **Remote Access:** The standard requires active risk management of remote access solutions, enforcing multi-factor authentication with phishing-resistant factors, secure VPN configurations using approved cryptographic algorithms, and controls on remote endpoints including health validation and machine authentication.

Key Management: Entities must document and manage cryptographic keys with a Key Management Plan covering generation, storage, exchange, rollover, and revocation. Providers hosting gateways must have compatible key management plans with clear shared responsibilities.

Table 3. Cisco Mapping to Australian Gateway Standard Requirement: Gateway Services

Requirement: Gateway Services	How Cisco Meets/Supports Compliance
Domain Name System (DNS)	Cisco Umbrella, part of Cisco Secure Access, provides Protective DNS (PDNS) services that block connections to malicious domains, supports DNS Security Extensions (DNSSEC), and offers DNS encryption options while maintaining visibility for policy enforcement.
Mail Relays	Cisco Secure Email Security solutions offer comprehensive email security including encryption (STARTTLS with ASD Approved Cryptographic Algorithms), authentication protocols (SPF, DKIM, DMARC), content filtering, malware detection, and compliance with email protective marking standards. It supports GovLINK for secure government email exchange.
Web Proxies	Cisco Secure Access includes secure web gateway (SWG) capabilities with web security policy enforcement, content filtering, malware detections (heuristics, sandboxing, threat intelligence), TLS decryption, deny listing, and identity awareness for user authentication and access control.
Reverse Web Proxies	Cisco Secure Access supports reverse proxy functions with traffic forwarding controls, malware detection, TLS termination and re-encryption, HTTP header inspection and manipulation, deny listing, and Denial of Service (DoS) protection mechanisms.
Remote Access	Cisco Secure Access VPN provides secure remote access with multi-factor authentication (MFA), like Cisco Duo capabilities, including phishing-resistant factors, supports secure VPN connections using ASD Approved Cryptographic Algorithms, and enforces endpoint health validation and policy enforcement for remote endpoints.
Key Management	Cisco Secure Access uses key management to securely handle cryptographic keys that protect data and communications. Customers can use a certificate signed by their own Certificate Authority (CA) to enable secure connections between user devices in their organisation and Cisco Secure Access.

Conclusion

By leveraging its comprehensive security framework and proven compliance posture demonstrated through its many certifications, Cisco Secure Access offers a highly robust and efficient pathway to meeting the stringent requirements of the Australian Government Gateway Security Standard. This global approach ensures consistent, high-level security, reduces redundant efforts, and accelerates time-to-compliance for critical government and public sector deployments in Australia.

For a tailored discussion or technical deep dive around modernising your SIG environment, please reach out to your Cisco representative.

Resources

For more information, please refer to the following:

- Cisco Secure Access At-a-Glance
- Cisco Secure Access Data Sheet
- Cisco Secure Access Ebook
- Cisco Secure Access Home Page
- Cisco Secure Email Data Sheet
- Australian Government Gateway Security Standard