Request for Proposal: Secure Access Service Edge (SASE) Platform

Table of Contents

1. Introduction and Background

[Company Name] is seeking proposals for a comprehensive Secure Access Service Edge (SASE) platform to modernize our network and security infrastructure. This RFP outlines our requirements for a cloud-native solution that converges network connectivity and security services to support our distributed workforce and cloud-first initiatives.

Organization Background

- [Describe your company/organization]
- [Industry and regulatory requirements]
- [Size of organization and IT infrastructure]

Current Environment

- [Current network and security architecture]

-
- [Number of users and locations]

Project Goals

- Implementation of a unified, cloud-native SASE architecture
- Enhancement of security posture through integrated services
- Optimization of network performance and user experience
- Streamlined management and operations

2. Project Objectives

1. Deploy a comprehensive SASE platform that integrates:
    - Software-Defined Wide Area Networking (SD-WAN)
    - Security Service Edge (SSE) components
    - Zero Trust Network Access (ZTNA)
    - Cloud security services
2. Achieve the following outcomes:
    - Unified security and networking infrastructure
    - Enhanced visibility and control
    - Improved operational efficiency
    - Reduced total cost of ownership
    - Scalable cloud-native architecture

3. Scope of Work

Required Components

1. SD-WAN Capabilities
    - Network optimization
    - Application-aware routing

- WAN link management
- QoS controls

2. Security Service Edge (SSE)
    - Secure Web Gateway (SWG)
    - Cloud Access Security Broker (CASB)
    - Zero Trust Network Access (ZTNA)
    - Firewall as a Service (FWaaS)
3. Advanced Security Features
    - Data Loss Prevention (DLP)
    - Advanced Threat Protection
    - User and Entity Behavior Analytics
    - Integrated threat intelligence
4. Management and Analytics
    - Unified management console
    - Real-time monitoring
    - Advanced analytics
    - Automated incident response

Implementation Phases

1. Planning and Design
    - Architecture assessment
    - Migration strategy development
    - Policy framework design
    - Assessment of current network and security infrastructure
    - Training and change management planning for IT staff and end-users

2. Pilot Deployment
    - Initial implementation
    - Testing and validation
    - Performance baseline establishment
    - Proof of Concept (PoC) execution, including:
        - Clear objectives and success criteria
        - Key use cases testing
        - Performance benchmarks and security scenarios
        - Required integrations testing
        - Evaluation metrics and reporting requirements
3. Full Deployment
    - Phased rollout
    - User migration
    - Integration with existing systems
4. Optimization
    - Performance tuning
    - Policy refinement
    - User experience optimization

4. Technical Requirements

Network Capabilities

1. SD-WAN Features
    - Application-aware routing
    - Dynamic path selection
    - QoS and bandwidth management

- Link aggregation and failover
- Traffic shaping and prioritization

5. Functional Requirements

A. Core Functional Requirements

5.1 Cloud-Native Architecture

Tip: A cloud-native architecture is fundamental to a successful SASE implementation. Look for solutions that demonstrate true cloud-first design principles, with microservices-based architecture that enables scalability, flexibility, and resilient operations. Consider how the architecture supports distributed deployment and maintains consistent performance across different cloud environments.

Requirement	Sub-Requirement	Y/N	Notes
Cloud-Native Architecture	Cloud-first design with microservices architecture		
	Container-based deployment capabilities		
	Auto-scaling and elastic resource management		
	Multi-tenant architecture support		
	Native cloud service provider integration		

5.2 Integrated SD-WAN Capabilities

Tip: Effective SD-WAN integration is crucial for optimizing network performance and ensuring reliable connectivity across distributed locations. Focus on solutions that offer comprehensive WAN optimization features and intelligent traffic routing capabilities while maintaining consistent application performance.

Requirement	Sub-Requirement	Y/N	Notes
SD-WAN Integration	Application-aware routing capabilities		
	Dynamic path selection and optimization		

	WAN link load balancing and aggregation		
	Quality of Service (QoS) controls		
	Bandwidth management and optimization		

5.3 Comprehensive Security Services

Tip: Security services form the backbone of SASE architecture. Evaluate solutions based on their ability to provide integrated, cloud-delivered security controls that protect all edges of the network while maintaining simplicity in management and deployment.

Requirement	Sub-Requirement	Y/N	Notes
Security Services	Next-generation firewall functionality		
	Advanced threat prevention capabilities		
	Data loss prevention (DLP) features		
	Zero-trust network access implementation		
	Secure web gateway services		

5.4 Unified Management Interface

Tip: A centralized management interface is essential for efficient SASE operations. Look for solutions offering intuitive, comprehensive control through a single pane of glass that enables unified policy management, monitoring, and reporting while accommodating different administrative roles and access levels.

Requirement	Sub-Requirement	Y/N	Notes
Management Interface	Single console for all SASE functions		
	Role-based access control management		
	Customizable dashboards and reporting		
	Integrated policy management		

	Real-time configuration capabilities		

5.5 Policy Enforcement

Tip: Consistent policy enforcement across all network edges and security functions is critical for maintaining security posture. Evaluate solutions based on their ability to implement granular policies uniformly while supporting dynamic adjustments based on context and risk.

Requirement	Sub-Requirement	Y/N	Notes
Policy Enforcement	Granular policy creation and control		
	User and group-based policy management		
	Location-aware policy implementation		
	Application-specific rule enforcement		
	Automated policy deployment		

5.6 Traffic Optimization

Tip: Traffic optimization capabilities directly impact user experience and application performance. Focus on solutions that provide comprehensive optimization features while maintaining security and visibility across all traffic flows.

Requirement	Sub-Requirement	Y/N	Notes
Traffic Optimization	WAN traffic optimization		
	Application performance acceleration		
	Bandwidth allocation controls		
	Traffic prioritization mechanisms		
	QoS implementation capabilities		

5.7 Scalability

Tip: Scalability ensures your SASE solution can grow with your organization. Consider both horizontal and vertical scaling capabilities, along with the ability to maintain performance as the deployment expands.

Requirement	Sub-Requirement	Y/N	Notes
Scalability	Horizontal scaling support		
	Elastic resource management		
	Performance optimization at scale		
	Automated capacity planning		
	Dynamic load balancing		

5.8 Integration Capabilities

Tip: Integration capabilities determine how well the SASE solution works with your existing infrastructure. Evaluate the breadth and depth of integration options, focusing on APIs and pre-built connectors for common enterprise systems.

Requirement	Sub-Requirement	Y/N	Notes
Integration	API availability and documentation		
	SIEM system integration		
	Identity provider connectivity		
	Third-party security tool integration		
	Custom integration capabilities		

5.9 Advanced Threat Protection

Tip: Advanced threat protection is crucial in today's evolving threat landscape. Look for solutions that combine multiple detection methods with automated response capabilities to provide comprehensive protection against sophisticated attacks.

Requirement	Sub-Requirement	Y/N	Notes

Threat Protection	Zero-day threat prevention		
	Advanced sandboxing capabilities		
	Threat intelligence integration		
	Behavioral analysis features		
	Automated threat response		

5.10 Identity and Access Management

Tip: Identity-based access control is fundamental to zero-trust security. Evaluate solutions based on their ability to integrate with existing identity systems while providing robust authentication and authorization capabilities.

Requirement	Sub-Requirement	Y/N	Notes
IAM	Multi-factor authentication support		
	Single sign-on capabilities		
	Directory service integration		
	Privileged access management		
	Identity verification mechanisms		

5.11 Real-time Monitoring and Analytics

Tip: Effective monitoring and analytics provide visibility into security and performance. Focus on solutions that offer comprehensive real-time monitoring capabilities with actionable insights and customizable reporting.

Requirement	Sub-Requirement	Y/N	Notes
Monitoring & Analytics	Real-time performance monitoring		
	Security event analytics		
	User experience tracking		