The Top Questions to Ask in Your SASE RFP

Moving to a cloud-delivered architecture can be daunting. It is essential to find a SASE provider who can meet you where you are on your journey. But how do you make sure you find the right provider to fit your needs? Start by asking direct questions about your requirements and how the provider can accommodate them.

Operations Team Impact

Security tools typically come equipped with their own individual management system, each of which has its own configuration and interoperability challenges. No matter where security functions exist, they should be configurable through a single management console, improving IT and security teams and end-users' overall experience.

1. How does the solution sync between on-premises management, cloud-based management, individual firewalls, and sites?

2. How does the solution integrate with existing security management systems? Does it provide seamless visibility?

3. How does the solution convert on-premises security policies to cloud-based security policies?

Unified Policy Management

Unified policy management must be your first step towards SASE to ensure a seamless migration of services that doesn't create a heavy operational burden for your team. Consistent security policy and visibility is essential for safeguarding users, applications, and infrastructure across every point of connection on the network.

1. How does the solution manage and enforce consistent security policy across on-premises and cloud environments? How similar are the policy constructs?

2. Describe how policies follow the user, device, and application without copying over or recreating rule sets?

3. How do security policies ensure the security of users, devices, and applications? Can they follow the user "on" and "off" the network? How do you ensure that rule sets can be copied over or recreated across environments?

Fast and Effective Protection Against Advanced Threats

Every organization requires effective protection against known and unknown threats, even if they are encrypted. Organizations must reduce the risk of attack and have granular control of applications, devices, and traffic content through identity-based policies, segmentation, and validated threat protection.

1. Describe how the solution helps administrators set policies and block suspicious behaviors on the endpoint? How frequently are new threat signatures added?

2. What processes are in place to avoid introducing false positive alerts from automated signature updates?

3. How does the solution uncover zero-day threats and malicious connections, including botnets and C2 servers hiding in encrypted traffic? How is this threat intelligence shared to other parts of the network?

4. If TLS 1.3 is used, how are policies applied and how is session privacy respected? Does the solution downgrade to TLS 1.2?

5. How does the solution defend against lateral threat propagation? Does this require a separate endpoint agent?

Resilience and Scalability

Every organization requires easily and effective scalability for physical, virtual, and cloud-based security environments. The solution must offer operational simplicity and security at scale that is invisible to end users, never negatively impacts experience, and maintains business continuity and access to services, wherever users are located.

1. How does the solution help ensure regulatory and administrative compliance requirements?

2. Does the solution provide a detailed analysis of application volume and usage throughout the network based on bytes, packets, and sessions? How are these details reported?

3. Does the solution integrate reporting and dashboards with other SASE components, such as FWaaS?

4. Does the solution track usage and risk metrics and analyze traffic patterns? How does the solution improve overall network management and visibility?

Single Stack Architecture with a Single Policy Framework

Leverage existing investments as an on-ramp to business-critical cloud security services that offer low-latency and scale regardless of traffic volume. Create policies once and apply them anywhere and everywhere with unified policy management, including user- and application-based access, IPS, anti-malware, and secure web access within a single policy.

1. How does the solution accommodate for both VPN and ZTNA deployment?

2. How does the solution provide Web traffic categorizations that can be incorporated into application and security policy? How often are these categories updated?

Consistent Security for your Distributed Workforce

Support the remote workforce whether they are in the office, at home, or on the road with fast and secure user access to the applications and resources people need to do their jobs effectively. Security policies should be based on identity and follow the user wherever they go.

1. How is secure access extended to users?

2. How does the solution verify a user's identity and risk posture? Is it an all-in-one process?

3. Does the solution log locally and sync when the system is reconnected to the corporate network?

Environmental Extensibility

Whether an organization's infrastructure is on-premises, IaaS, or in-cloud services, or a combination, their SASE provider must support them all.

1. Is the solution scalable? How easily does it scale? How does it provide management capabilities for physical, virtual, and cloud-based security deployments?

2. How flexible is the policy model and ability to set groups? Is it possible to dynamically apply policies based on application or operational profiles? Please describe.

Identity Broker Flexibility

Every SASE provider should integrate with any identity service provider, to define policies and application usage based on individual users or user groups. It must provide visibility into application usage at the user level rather than IP address and provide powerful insights into application traffic traversing the network.

1. Does the solution integrate with any identity service provider, such as Azure AD and Okta?

2. How does the solution verify a user's identity and risk posture? Is it in all one process/engine?

3. How does the solution authenticate and authorize users and devices? How is resource access controlled?

Dynamic User Segmentation

Every SASE provider must have dynamic user segmentation based on zero trust principles that maintain the security of data around identity- and risk-driven policies. Security policies should be based on the user, device, and network context that automatically adapt based on new risks and attack vectors and follow the user wherever they go.

1. How does the solution provide visibility into user and device activity on the network? How are user risk profiles monitored and controlled?

2. Describe how the solution helps administrators set policies and block suspicious behaviors on the endpoint?

3. How is user web-behavior managed to assist with avoidance of malicious sites or applets? How is user privacy preserved without introducing risk?

Validated Security Efficacy

It is important to have validated protection from attacks that makes an impact. Organizations must look for SASE providers that are more than 99% effective against client- and server-side exploits, malware and C2 traffic, regardless of where the users and applications are located, ensuring consistent security enforcement.

1. What objective test results can be provided to validate the solutions effectiveness?

2. Has the solution's security efficacy been validated by a reputable third-party within the past year, and what was its efficacy score? Can a methodology for the testing and use cases be provided?

3. Does the solution provide 100% resistance to different types of network evasions?

Transition Seamlessly to Cloud-delivered Security at Your Own Pace

Not every organization is going to move to a cloud-delivered architecture overnight. A SASE provider must meet every organization where they are on their journey and enable them to transition seamlessly and securely to a SASE architecture at a pace that works best for the organization's business.

1. Am I able to leverage my existing security appliance investments?

2. Can you describe which technologies are able to be leveraged and how they would be utilized so I'm not forced to accelerate a depreciation schedule or replace out of cycle?

3. What about my SD-WAN technology, can I use what I have?

Security Assurance

Whether for a traditional firewall policy or policy delivered as a service, it's important that rules are placed in proper order. They can quickly add up, and are prone to being outdated, shadowed, and ineffective. Duplicate rules require hours dedicated to rule sorting before confidently make changes. Your IT team must quickly make changes, ensuring that policy changes are effective for users.

1. Describe how multiple operators can make rule edits without introducing conflicts. How is a policy conflict identified and resolved?

2. Does the solution help with policy hygiene and assist in the reduction of aged or unnecessary rules? Describe please.

3. How is rule precedence determined?

It is important to find a SASE provider who can meet you where you are on your SASE journey by managing physical, virtual, and cloud-based network security requirements without imposing the limitations of their approach on your organization and shifting operational overhead to your teams. Identify a SASE provider who can enable a seamless and secure transition to a SASE architecture by accommodating both a traditional network security architecture and a SASE architecture simultaneously.

When you commit to SASE, you're committing to a secure future. The promise of a SASE architecture is incredible, but every organization must transition at its own pace. For some organizations, that means rapid adoption, and for others, a more methodical and steady transformation.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701