CATO
NETWORKS

SASE RFP Template

Introduction

This RFP template was created to help IT professionals organize the set of business and functional requirements needed to address their network and security transformation journey.

This is a modular template, it covers multiple SASE requirements including SD-WAN, security, cloud, mobility, and global requirements. Some may not apply to your current project, but in our experience, they all become the “next project” at some point. The SASE architecture is built to enable smooth extension into these emerging projects.

Since we focus on the functional requirements, we didn’t include generic RFP sections, like getting the details of your vendor companies.

The RFP template is divided into four sections:

Business and IT Overview

The aim of this section is to have vendors understand your environment well enough to tailor their answers to your needs and point out how their solution is specifically valuable in your context. This section covers your business, your goals from the project, what geographies you operate in, and what network resources are covered. We also included a more detailed overview of your network topology, current networking and security stack, and how you connect and secure the different network connected entities.

Solution Architecture

The aim of the section is to understand the vendor architecture. While many SASE offerings include similar capabilities, the way these capabilities are delivered affects cost, complexity, and the overall success of the project. In this section we want to understand the architectural elements -- what they are, what they do, where they are placed (branch, device, cloud), how do they scale, how do they address failures and deliver resiliency, and more.

Solution Capabilities

The aim of this section is to understand the functionality provided by the solution across multiple areas. You can choose the requirements relevant to your network.

Support and Services

The aim of this section is to understand the support structure and available managed services. For global organizations, follow-the-sun support models are essential. And, if you are coming from a telco contract and used to a fully managed service, this project can create an opportunity to move towards a self-service or co-managed model.

Best of luck with your upcoming project and your new network.

SECTION 1

Business and IT Overview

In this section, you'll describe your business and IT overview. Be as thorough as possible. The more context you and your team provide vendors, the better they'll be able to help you.

1. Company

Please describe your business, the project goals and the parts of the business and infrastructure covered by that project.

1.1. Business overview

1.2. Primary business and technical goals

1.3. Strategic related IT projects

1.4. Project scope

1.4.1. Covered resources: datacenters, branches, mobile users, cloud applications and datacenters

1.4.2. Covered geographies

2. IT systems and architecture

Please describe your IT network topology, network and security technology stack, and other pertinent technical information that can enable the vendor to understand the context it needs to be inserted into.

2.1. Current network architecture and key technologies

2.2. Primary applications (function, location)

2.3. Datacenters and regional hubs

2.4. Cloud providers and applications

2.5. Branch topology and connectivity

2.6. You may have multiple classes of branches, classified by number of employees, and the technology stack deployed in each class. Please list all classes.

2.7. Enterprise security capabilities and footprint

2.8. Mobile workforce, technologies and use cases

SECTION 2

Architecture

SASE is a convergence of networking and security for branch, datacenter, cloud, and mobile at a global scale. This section will discuss the architecture of the proposed solution.

3. Architecture

3.1. Describe the architecture of your solution and how it provides the capabilities below. Please indicate when **third-party components** need to be used and the supported form factors: physical appliance, virtual appliance, cloud services, device-resident clients.

3.2. Describe the functional elements of your solution. How do you provide:

- 3.2.1. SD-WAN at the branch, datacenter, and cloud edges
- 3.2.2. Secure access to the Internet at the branch
- 3.2.3. Optimization of cloud access (SaaS and IaaS)
- 3.2.4. Mobile user access to physical and cloud datacenters, and cloud applications
- 3.2.5. Predictable global connectivity between remote locations, users, and the cloud

3.3. Architectural attributes

- 3.3.1. What is your approach to consolidating multiple capabilities into a single solution and what are the advantages it provides (uCPE, service chaining, VNFs, Cloud Service, etc.)?
- 3.3.2. How does your architecture provide high availability and resiliency for continuous service across all solution elements (discussed above)?
- 3.3.3. How does your architecture scale to add: more capacity per site, more sites? What is the limit to number of sites in a single deployment?
- 3.3.4. How does your architecture guarantee SASE capabilities are available globally close to our business locations and users?
- 3.3.5. How do you provide management, reporting and configuration for all components?
- 3.3.6. How do you maintain the software of all components? Are updates automated? Can update schedule be controlled by the customer?
- 3.3.7. Please explain how your architecture uniquely simplifies network management, increases agility, and improves security.

3.3.8. Please attach an architectural diagram of your solution.

SECTION 3

Capabilities

In this section we explore the capabilities of the proposed solution across multiple functional areas. Pick and choose the ones that are relevant to your business.

4. SD-WAN

4.1. Link Management

4.1.1. How many concurrent WAN links and what types (MPLS, xDSL, Fiber, 4G/LTE, etc.) does your solution support?

4.1.2. Please describe how Active/Active and Active/Passive link aggregation works in your solution.

4.1.3. How do you detect link degradation (blackouts and brownouts)? What metrics do you use?

4.1.4. What are the automated actions your solution can take to recover from various failure scenarios (link failure, link degradation, link congestion)?

4.2. Traffic routing and Quality of Service

4.2.1. What attributes can you use in configuring traffic routing/steering policies? IP, Host, Application, User/Group, other?

4.2.2. How many applications are recognized out of the box?

4.2.3. Can a customer create a rule to identify a private/custom application?

4.2.4. How do you prioritize traffic (applications, users, groups)? How many levels of priority are available?

4.2.5. How do you ensure bandwidth is always available/reserved to the most critical applications?

4.3. Voice and latency-sensitive traffic

4.3.1. How does your quality of service (QoS) mechanism support voice applications (VoIP and UCaaS) and other latency sensitive traffic, such as virtual desktops?

4.3.2. What capabilities do you have to support/enhance voice quality?

4.3.3. When link degradation is detected, how do you ensure voice calls are kept “alive”?

4.4. Throughput and edge devices

4.4.1. What throughputs are supported and how do you size your solution to meet them?

4.4.2. Please explain the different devices and models needed to deliver the various supported throughputs.

4.4.3. Please attach any sizing documentation used to determine real throughput based on customer requirements (size of mesh, decryption, routing, security inspection).

4.5. Monitoring and reporting

4.5.1. What network entities does your solution monitor (locations, links, applications, users, hosts, etc.)?

4.5.2. What metrics are tracked for each entity? Do you have both real time and historical views?

4.5.3. Detail the process by which you investigate a network incident to determine root cause?

4.5.4. Please include screen shots that demonstrate how you visualize the full network, a single site, multiple links, and a single host in both historical and real-time views.

4.6. Site provisioning

4.6.1. Please describe the process of provisioning a new site within your solution.

4.6.2. Please describe the process of configuring a site with high availability (across two edge devices)

4.6.3. How do you provision a site belonging to a third-party(partner/supplier)? Do you have an option to connect such a site without any edge solution?

4.7. Gradual deployment / Co-existence with legacy networks (MPLS)

4.7.1. Please describe your gradual roll out strategy.

4.7.2. Detail how you support MPLS with your SD-WAN (hybrid WAN) at a location and support for MPLS-connected sites not on your SD-WAN?

5. Security

5.1. Traffic Encryption

5.1.1. How do you provide end-to-end encryption of all traffic?

5.1.2. What impact will end-to-end encryption have on your solution's stated supported throughput?

5.2. Threat Prevention

5.2.1. What threat prevention capabilities are offered by your solution? Specifically indicate if you provide: URL filtering, anti-malware, Next gen anti-malware (non-signature based), or IPS.

5.2.2. Please include a short description of each security capability, and how its policy is configured and what customizations are available.

5.2.3. Which components are built into your solution and which require "service chaining" of multiple products?

5.2.4. If service chaining is required for multiple products please explain how you implement it (edge device, cloud service, combination). Please explain how each component is managed.

5.2.5. How does your solution perform deep packet inspection (DPI) to stop threats such as malware?

5.2.6. Assuming 100% of the traffic to be inspected is encrypted, what is the impact on your above stated supported throughput?

5.3. Threat Detection

5.3.1. What capabilities you provide to detect malware infected endpoints?

5.3.2. What is required to deliver these capabilities in the network and on endpoints?

5.3.3. How do you communicate incident information to customers? Please share an example of such report.

5.3.4. What assistance do you provide with remediation?

5.4. Branch Security

5.4.1. What security services do you provide (such as URL Filtering, Anti-malware, IPS) to secure direct Internet traffic at the branch?

5.4.2. What physical or virtual appliances must be deployed to secure direct Internet traffic at the branch?

5.4.3. What cloud services must be purchased/subscribed to, to secure direct Internet traffic at the branch?

5.4.4. How do you manage security policies? Is it integrated with network management or does it require a separate management interface?

5.4.5. What threat prevention and detection capabilities are offered for branch traffic?

5.5. Cloud Security

5.5.1. How do you secure traffic to and from cloud datacenters? Public cloud applications?

5.5.2. What solution components are required to provide cloud access security?

5.5.3. How do you manage your cloud security solution? Is it integrated with your network management?

5.6. Mobile Security

5.6.1. How do you secure traffic from mobile users to cloud applications or on-premise applications?

5.6.2. What solution components are required to provide mobile security?

5.6.3. How do you manage your mobile security solution? Is it integrated with your network management?

5.7. Identity and User Awareness

5.7.1. How do you associate identity with network flows across mobile users, office users, applications, and devices?

5.7.2. Can you include identity (users, groups) in network and security policies?

5.7.3. How do you maintain synchronization of current user and group entities? What federated ID management systems (like Azure AD) do you support?

5.8. Policy management and enforcement

5.8.1. How do you enforce a security policy on a branch, group of branches, a user, a group of users, the entire network?

5.8.2. What default policies are available out of the box?

5.9. Security management analytics and reporting

5.9.1. How do you control access to the security management console?

5.9.2. What default security policies and capabilities are available out of the box?

5.9.3. What types of events are generated by your solution?

5.9.4. What data is available for the events, and what tools can be used to investigate an event?

5.9.5. What reporting, alerting, and exporting capabilities are available for the events?

5.9.6. Does your security management and reporting integrate with your network management and reporting?

5.9.7. Please provide screen shots of networking and security events list and detailed event record.

6. Cloud

6.1. Describe the components and process needed to connect a cloud datacenter into the network?

6.2. Is cloud-integration (both cloud datacenter and cloud application) included in the quoted price?

6.3. What cloud datacenter providers do you integrate with?

6.4. How do you optimize traffic from a location or mobile users to a cloud datacenter?

6.5. How do you optimize traffic from a location or mobile users to a specific cloud application (UCaaS, cloud storage, CRM, ERP, O365)?

7. Mobile (SDP/ZTNA)

7.1. How does your solution connect a mobile user into the network?

7.2. What are the available mobile solutions for connecting mobile users to the WAN and the cloud (Client, Clientless)?

7.3. How do you optimize traffic from mobile users to a physical datacenter application, a cloud datacenter application, or a public cloud application (i.e. Office 365)?

7.4. What are the unique capabilities you offer over legacy VPN and zero trust network access solutions?

8. Global

8.1. How does your solution optimize traffic globally?

8.2. What SLAs do you provide for *global* latency, packet loss, jitter?

8.3. What third-party components are required to ensure optimal global WAN traffic?

8.4. What third-party components are required to ensure optimal global cloud/Internet traffic?

8.5. What capabilities do you offer for optimal traffic from Asia Pacific, Latin America, and China to out of region datacenters and cloud applications?

8.6. How do you deliver optimal network experience to mobile users?

SECTION 4

Support and Services

In this section we discuss the support and managed services offered by the vendor.

9. Support and Professional Services

9.1. Do you offer follow the sun support?

9.2. What geographic locations do you provide support from?

9.3. Is support available 7x24x365?

9.4. What are your support SLAs?

9.5. Are professional services provided by the vendor or through partners? Detail for which areas -- planning, design, deployment, implementation, or training?

10. Managed services

10.1. Please describe your managed services in the following areas:

10.1.1. Last-mile monitoring

10.1.2. Managed Detection and Response (MDR)

10.1.3. Fully managed network service to configure networking and security policies

10.2. Are these services provided as a complete package or a-la-carte?

10.3. Can we choose a self-service, co-managed, or fully managed service?

10.4. Is your self-service or co-managed service limited to monitoring or can we also change our network and security configuration?

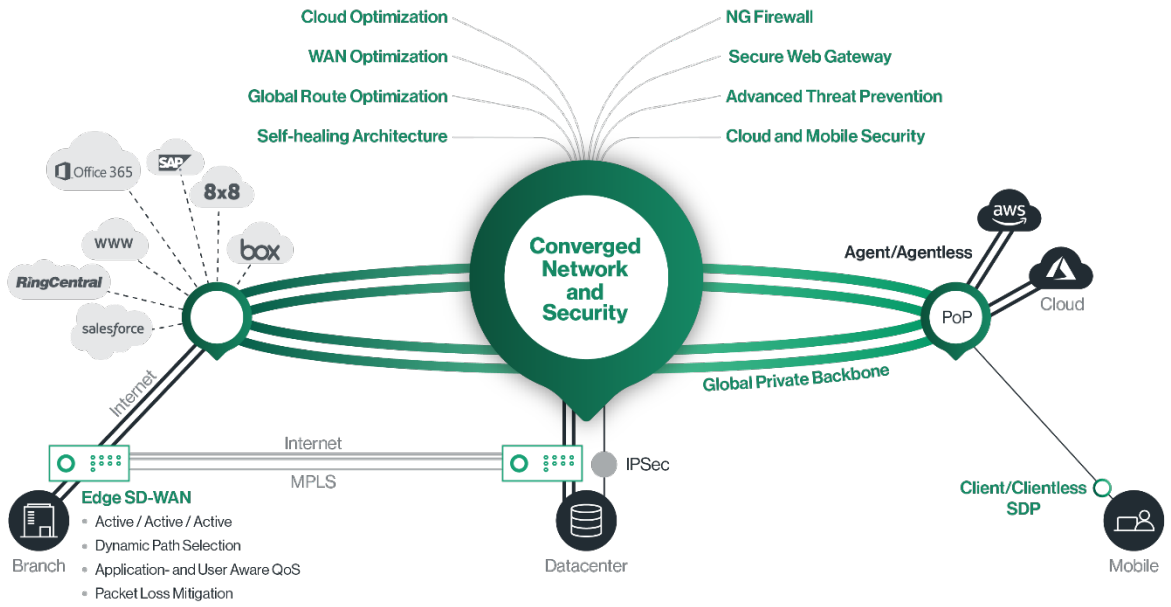
10.5. Does your managed service prevent customers from making self-service changes to the network?

10.6. What visibility is provided to networking and security under the fully managed service options?

About Cato

Cato provides a converged SD-WAN and network security as a global cloud service. Aligned with Gartner's Secure Access Service Edge (SASE) framework, Cato Cloud connects all data centers, branches, mobile users, and cloud resources into an agile and secure global network.

Our service empowers you to connect, secure, and run the network yourself, and supports you with expert managed services if you need them. Cato's cloud-native architecture delivers a future-proof network that evolves at the pace of your business. With Cato, your network, and your business, are ready for whatever comes next.



Cato. The Network for Whatever's Next.

Cato Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Mobile Access Optimization
- Cato Management Application

Managed Services

- Managed Threat Detection and Response (MDR)
- Intelligent Last-Mile Management
- Hands-Free Management
- Site Deployment