JUNIPER NETWORKS | Engineering Simplicity

White Paper

ENABLING SASE WITH JUNIPER SESSION SMART SD-WAN

Securing Today's Cloud Era Networks

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Gartner defines Secure Access Service Edge (SASE) as a transformational technology that combines elements of software-defined wide area networking (SD-WAN) and network security into a single cloud-managed package. For SASE to be truly successful, the network must be able to dynamically detect where services are located to be able to deliver valid sessions to those services.

Recognizing that security must be fully integrated into the network, the Juniper® Session Smart™ SD-WAN solution has built-in security capabilities that are an inherent part of the architecture. In addition, service-based routing ensures that sessions are delivered based on identity and context to relevant parties following real-time policies. This ensures that a modern cloud-centric digital business can provide secure access to users and devices anywhere—a key requirement of SASE.

Introduction

With businesses embracing the cloud, Internet of Things (IoT) becoming prevalent, users going mobile, and applications requiring increasing levels of responsiveness, it is not possible to provide security with traditional models where security is bolted onto the network at certain points.

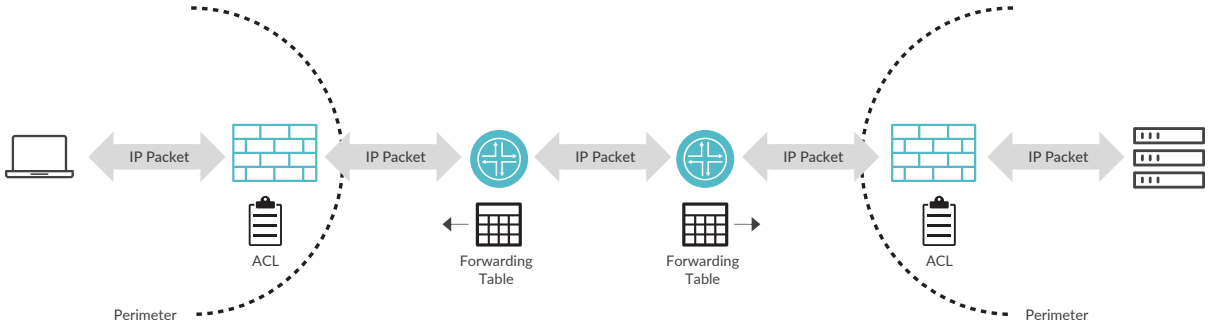


Figure 1: Traditional security model

Standalone Distributed Firewalls

The traditional model to protect users and data was to have firewalls at the perimeter. This led to having firewalls deployed everywhere, including the cloud, the data center, and on the desktop. As BYOD and cloud became prevalent, however, the perimeter became blurry with user data residing in Software as a Service (SaaS) applications, mobile phones, laptops, and tablets. These devices are mobile, which makes it impossible to define the perimeter. The standalone firewall everywhere is a deterrent to support cloud and does not work anymore. Service chaining firewall virtualized network functions (VNFs) at different locations removes the need for having a separate device but suffers from the same issues.

Centralized Firewalls

Another method which became popular when users started getting mobile was to backhaul all the traffic from the devices over VPNs back to the data center. Here the traffic could be scrubbed by a large centralized firewall before being sent to its destination. This requires large costly equipment at the data center to manage all the traffic. It increases latency resulting in poor user experience, and it defeats the cloud and SaaS model.

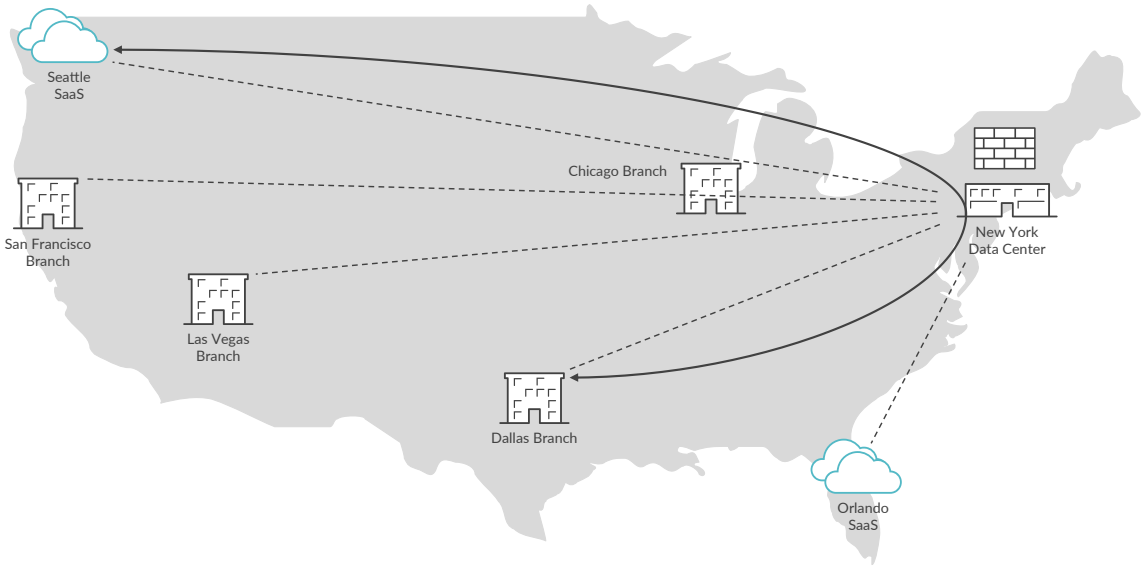


Figure 2: Backhauling traffic over VPNs to the data center degrades the user experience

Cloud-Based Firewalls

One popular method to offer network security is to send all the traffic from the devices to a firewall hosted by a cloud-based network security provider. This allows users to send data from their devices to the closest hosting location of the cloud provider rather than to a central data center. It improves latency in regions where the hosting facilities are close to where the user travels, but it requires costly payments to the cloud provider for all data that is being scrubbed by them. Also, the policies are not dynamic, as any change in user or devices requires coordination with the cloud provider.

Gartner states in their Future of Network Security in the Cloud report that "Instead of forcing (via "tromboning") various entities' traffic to inspection engines entombed in boxes in the data center, we need to invert our thinking to bring the inspection engines and algorithms closest to where the entities are located."

In addition to the problems posed by traditional security models, attackers have become more sophisticated and data is increasingly encrypted, making it difficult to scrub. Tunnels bypass security [RFC 6169] and users are demanding better responsiveness. Expedient patches, protocol extensions, tweaks, and workarounds have resulted in complex and convoluted systems, causing numerous outages and significant costs to the enterprise [IETF 102].

Delivering SASE

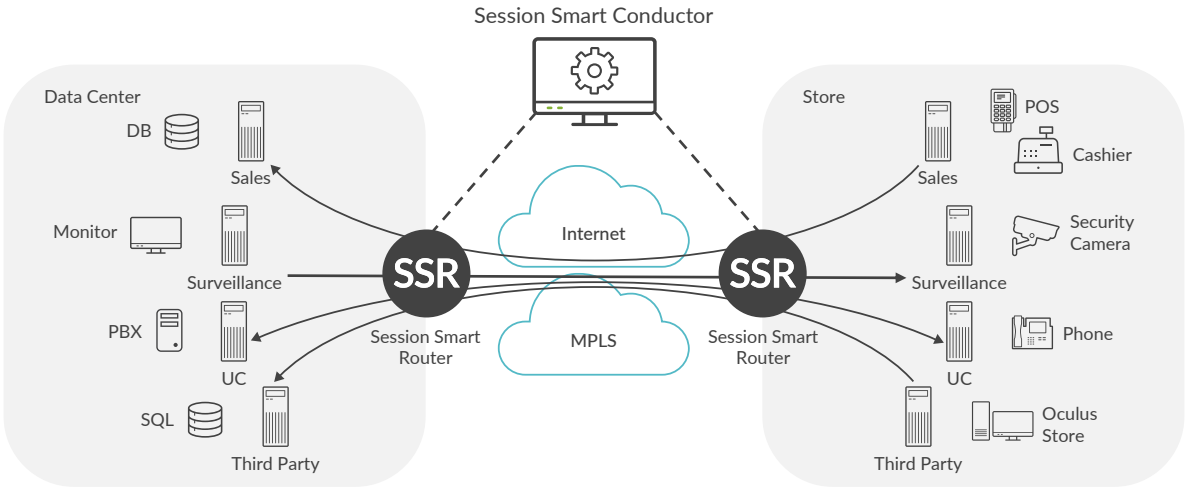
True SASE requires that network devices closest to users and their devices are able to dynamically provide security services by discovering endpoints, their privileges, and securing the traffic. The Juniper Session Smart SD-WAN solution has built-in capabilities to provide these security services at every router in the network.

Session-Based Routing

The Juniper Session Smart Router is session-based, meaning it operates on sessions rather than individual packets just like firewalls. Inherent directionality is built in, which allows the router to understand who is allowed to initiate sessions and in which direction. An administrator can specify which sessions to allow based on any given authentication criteria. Once the router confirms that the source is valid, the session is placed in a tenant that allows it access to certain destinations based on privileges. Any policies associated with the session related to security, encryption, authentication, quality of service (QoS), loads, or other criteria are also individually decided per session. This allows for fine-grained hypersegmentation. And this ensures secure access, as any unauthorized session will be dropped as soon as it traverses the first router in the network. The Session Smart Router can also identify sessions automatically and place them in different categories or tenants, giving them different treatment as desired by the administrator.

Service-Centric Routing

The Session Smart SD-WAN solution is designed around modeling the applications that users consume. Service-centric networking is a top-down approach to configuring routing infrastructure. Rather than using interior gateway protocols (IGPs) to exchange routes and access control lists (ACLs) to restrict access, administrators describe the services within the network and the group(s) within the network allowed to access each one. This enables the network to route sessions towards services rather than towards IP addresses. Once the routers know that the sessions are valid, they can then direct them towards services that they are meant to consume. This ensures that only valid sessions are sent towards services that can consume them depending on loads and traffic conditions. Without knowledge of services, a router is simply forwarding packets without understanding the identity of the user or device and connecting them to a destination IP address.



No Overlays | Hyper-Segmentation | Zero-Trust Security

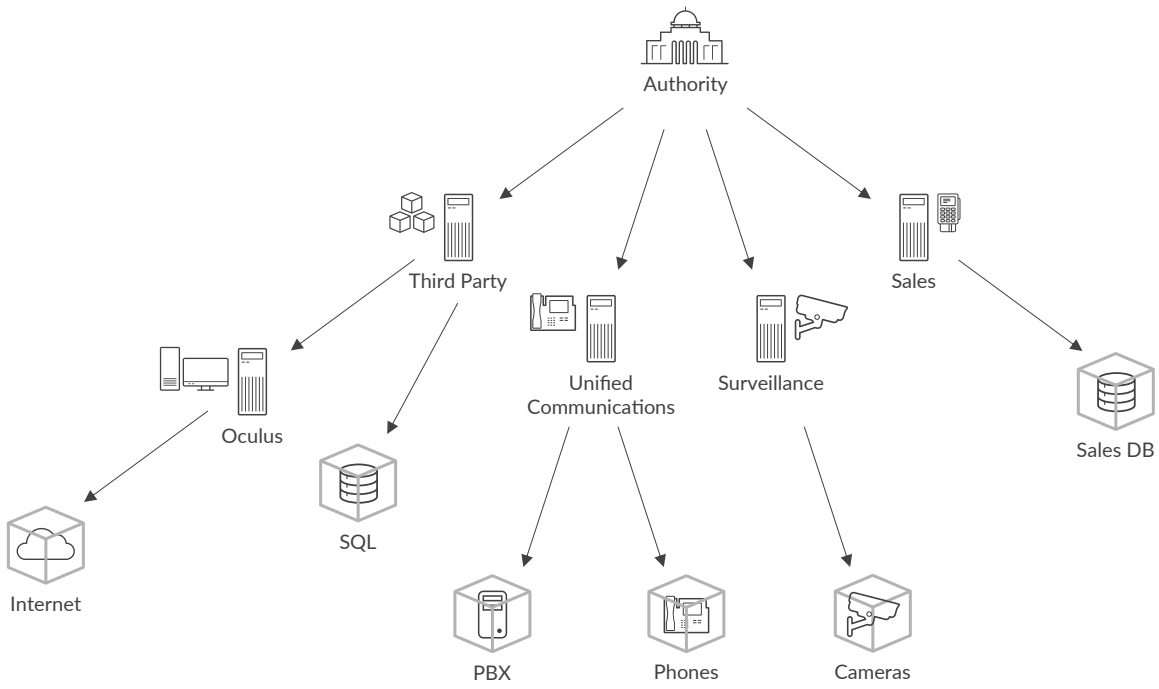


Figure 3: Juniper Session Smart SD-WAN Service centric routing

Dynamic Global Discovery

For SASE to be truly successful, the network must be able to dynamically detect where services are located to be able to deliver valid sessions to those services. Service and Topology Exchange Protocol (STEP) enables the Session Smart Router to exchange service and connection information to those services, using a service-oriented session-based paradigm. Network administrators define services to represent capabilities that the network is designed to deliver to consumers. STEP enables the exchange of this service capability to all routers along with reachability and other parameters to connect to these services. This enables network administrators to deliver an application-oriented intent-based SD-WAN solution that follows business logic and uses real-time information to enable routers to decide how to connect applications. Dynamic service discovery enables enterprises to spin up and down new locations for existing services based on loads, add new services, and remove or modify existing services. This reduces time to market and supports elastic growth.

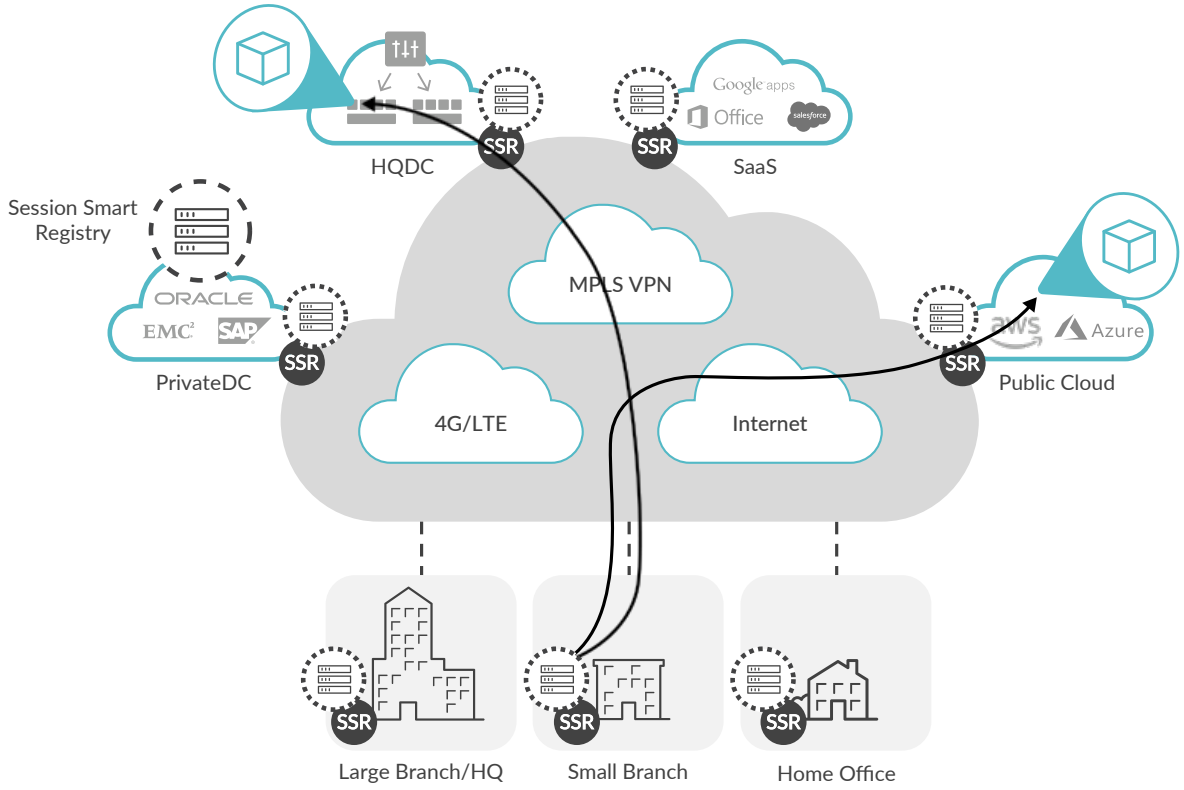


Figure 4: Session Smart Router enables dynamic service discovery

STEP performs dynamic service discovery in a unique way that cannot be achieved with any other protocol. Services can be defined with the granularity of prefixes, protocols, and ports. This means that in today's virtual or containerized world, each application on a compute instance can have its own service discovery. If the application is not reachable, the service will be withdrawn from the STEP report and other routers will stop sending packets to that server.

Routers in today's networks implicitly trust neighbors and information received from them. There is no way for a network to isolate a malicious user or to remove trust. STEP establishes trust through blockchains to share keys and validate ownership.

Be the Firewall

The way firewalls were deployed might be obsolete; however, their functions are not. Every Session Smart Router is an ICSA Certified Network Firewall along with additional capabilities to enable SASE.

These routers can encrypt/decrypt and authenticate any packet flowing through them. They support adaptive encryption to dynamically detect encrypted sessions and prevent double encryption. They are FIPS-140-2 certified. They follow a deny-by-default model just like firewalls so if there is no policy associated with a session, it will be dropped. This forces administrators to explicitly define policies for valid sessions.

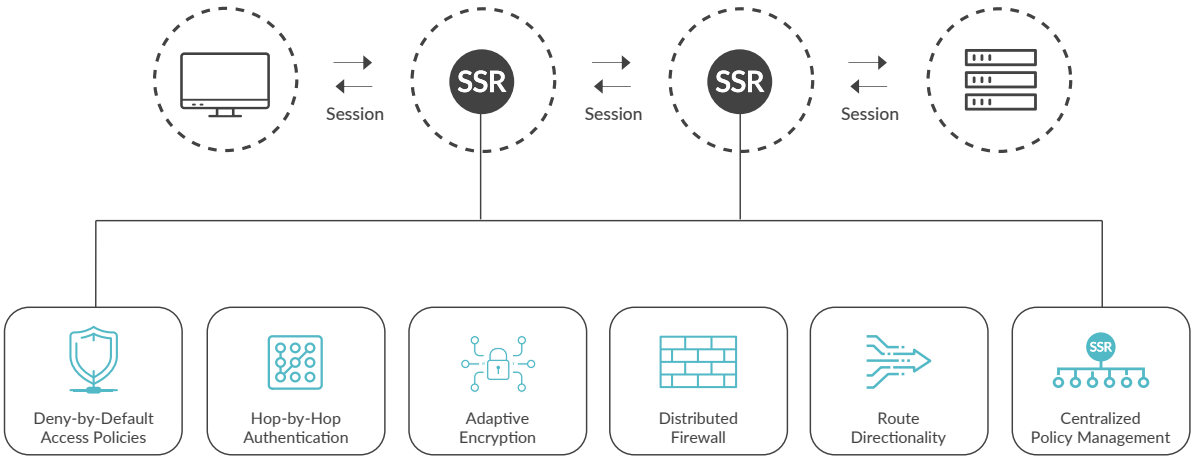


Figure 5: Session Smart SD-WAN capabilities

Conclusion

For SASE to be truly successful, the network has to dynamically detect where services are located in order to deliver valid sessions to those services. True SASE requires that every device in the network is aware of access policies, can discover changes in identities, encrypt and authenticate sessions, resist attacks, and enable security.

A router with no knowledge of services is simply forwarding packets without understanding the identity of the user or device and connecting them to a destination IP address. The STEP-enabled Session Smart Router lets network administrators deliver an application-oriented, intent-based networking solution that follows business logic and uses real-time information to enable routers to decide how to connect applications. Dynamic service discovery enables enterprises to confidently spin up and down new locations for existing services based on loads, add new services, and remove or modify existing services to reduce time to market and support elastic growth.

The Juniper Session Smart SD-WAN solution creates a SASE network with deny-by-default routing, policy-based forwarding, policing, and built-in corporate network firewall functions. The Juniper Session Smart Router is service-centric and session-based with inherent directionality built in. The Session Smart SD-WAN solution enables end-to-end segmentation and zero trust security, allowing enterprises to segregate and provide differentiated security and services to every traffic flow, in order to bring the vision of SASE to life.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

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

JUNIPER NETWORKS | Engineering Simplicity