Juniper Networks | Engineering Simplicity

White Paper

JUNIPER SESSION SMART SD-WAN FOR ZERO TRUST ARCHITECTURES (ZTA)

Ensure built-In NIST Zero Trust Security for U.S. Government Agencies, Cloud-Centric Organizations, Remote Sites, and Mobile Users

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As government agencies migrate IT infrastructure and applications to the cloud, they find that conventional perimeter-based security models, designed to control access to trusted enterprise networks, are not well suited for the digital era. In order to take advantage of the cloud's many benefits, they need a software-defined wide area network (SD-WAN) that will ensure security while allowing them to streamline operations, increase mobility, and reduce expenses. Juniper® Session Smart™ SD-WAN is just that kind of solution. With its built-in zero trust security model, it acts as a policy enforcement point in a zero trust architecture (ZTA), tightly controlling access to enterprise resources close to users and endpoints, independent of enterprise network borders. This ensures location-independent, zero trust security for cloud applications, remote workers, contractors, and guests, who can be authenticated, authorized, and secured in real time, upon session establishment, independent of network location.

Introduction

U.S. federal government agencies are adopting cloud-based applications and services to simplify operations, to accelerate the pace of innovation, and to support Cloud Smart and other modernization initiatives. But traditional perimeter-based security models, designed to control access to trusted enterprise networks, fall short in today's digital world. Malicious insiders or external threat actors can breach the perimeter, gain access to the trusted enterprise network, and move laterally to steal data or mount attacks.

Of equal importance is the fact that IT infrastructure often resides outside the confines of the enterprise data center. And users access enterprise resources from any place, at any time. To that end, the National Institute of Standards and Technology (NIST) Special Publication 800-207 defines a new ZTA for the world of on-the-go employees and on-demand services. In a zero trust security model, users are authenticated, authorized, and secured in real time upon session establishment, independent of location. The zero trust model is intended to shrink trust zones, reduce attack surfaces, and restrict lateral movement if a resource is compromised. It assumes that all users are inherently untrusted, wherever and whenever they try to access enterprise resources.

Built-In Zero-Trust Security for Cloud-Centric Organizations

The Juniper Session Smart SD-WAN solution has been built from the ground up with cloud workloads, mobile users, and zero trust security in mind. This advanced, service-centric solution is ideal for ZTA deployments, and it takes software-defined networking to a whole new level. In today's mobile and cloud-centric world, Session Smart SD-WAN enables fast, agile, and secure connectivity with unmatched cost savings and simplicity.

Perfect for all NIST 800-207 use cases, the Session Smart SD-WAN solution eliminates the inherent cost inefficiencies and performance limitations of traditional routing and security solutions, controlling access to enterprise resources close to users and endpoints, independent of enterprise network borders, as part of a Secure Access Service Edge (SASE). Unlike alternative networking solutions that encapsulate all data flows into a single overlay tunnel, the Juniper solution features a tunnel-free architecture that eliminates protocol overhead and avoids backhauling for optimal service quality and economics.

The complete Session Smart SD-WAN solution includes four key components: the Juniper Session Smart Router and Session Smart Conductor.

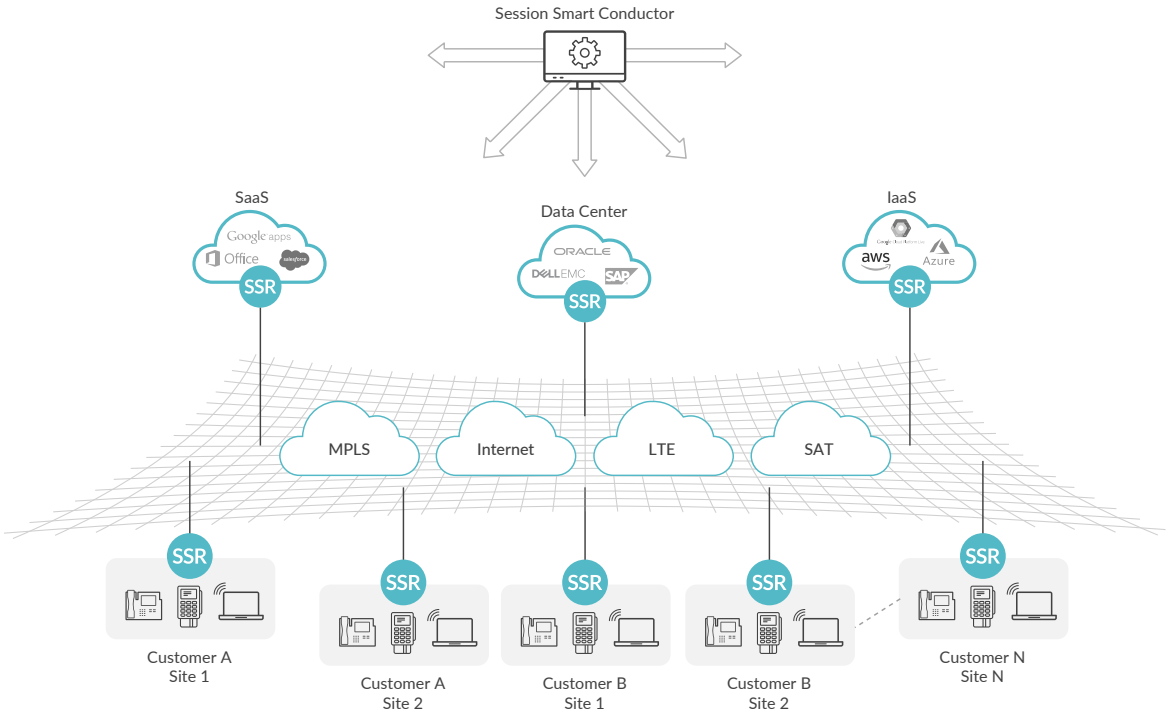

Figure 1: Juniper Session Smart SD-WAN architecture

Session Smart Router

The Juniper Session Smart Router is a 100% software-based, distributed routing solution featuring a service-centric control plane and a session-aware data plane. Government agencies can use the Session Smart Router to establish FIPS-140-2 certified secure connections to and from branch offices, private clouds, and public clouds over a variety of WAN interfaces, including MPLS, broadband, 4G/LTE, satellite, and microwave links.

The Session Smart Router provides a variety of network and security functions, including zero trust, deny-by-default routing; policy-based forwarding and policing; and integral enterprise network firewall functionality. It also enables end-to-end segmentation, allowing organizations to segregate traffic and provide differentiated security and services for every traffic flow. The Session Smart Router automatically forwards traffic over the right path, for the right application, at the right time based on policy and real-time network conditions for ultimate service quality and economics. This allows today's digital enterprises to provide secure access to users and devices, independent of location.

Session Smart Conductor

The Juniper Session Smart Conductor is a software-based management platform that enables centralized operations, administration, and maintenance for the geographically distributed Session Smart Router. It includes a unified policy engine and provides an intuitive user interface as well as northbound Network Configuration Protocol (NETCONF) and Representational State Transfer (REST) APIs for integration with third-party network and system management applications, and service orchestration solutions.

Using the Session Smart Conductor, central administrators can install and provision routers and perform software upgrades and maintenance functions without onsite assistance. The Session Smart Conductor provides single-pane-of-glass management, giving administrators full visibility into individual traffic flows, so they can efficiently monitor sessions, evaluate service quality, and troubleshoot problems on an end-to-end basis. Based on a multitenant architecture, it can easily be partitioned to support multiple organizations and administrative tiers.

Service-Centric Data Model Provides Granular, End-To-End Security

The Session Smart Router uses an innovative data model that lets network architects describe how the network will be used in an entirely new way. It starts with the applications and services that any network supports—things such as CRM systems, ERP systems, mail, voice, and Web resources. Access to these services is granted based on tenancy. The network can then be partitioned to support distinct, isolated tenants with unique resources and unique end-to-end security, routing, and service quality attributes. Each tenant in the data model represents a collection of users and their devices that share common policies (access policies, security policies, and so on). Unlike other networking solutions that employ zone-based schemes, tenancy is applied and enforced at every router instance, network-wide. In other words, tenant policies "stretch" across an extended network.

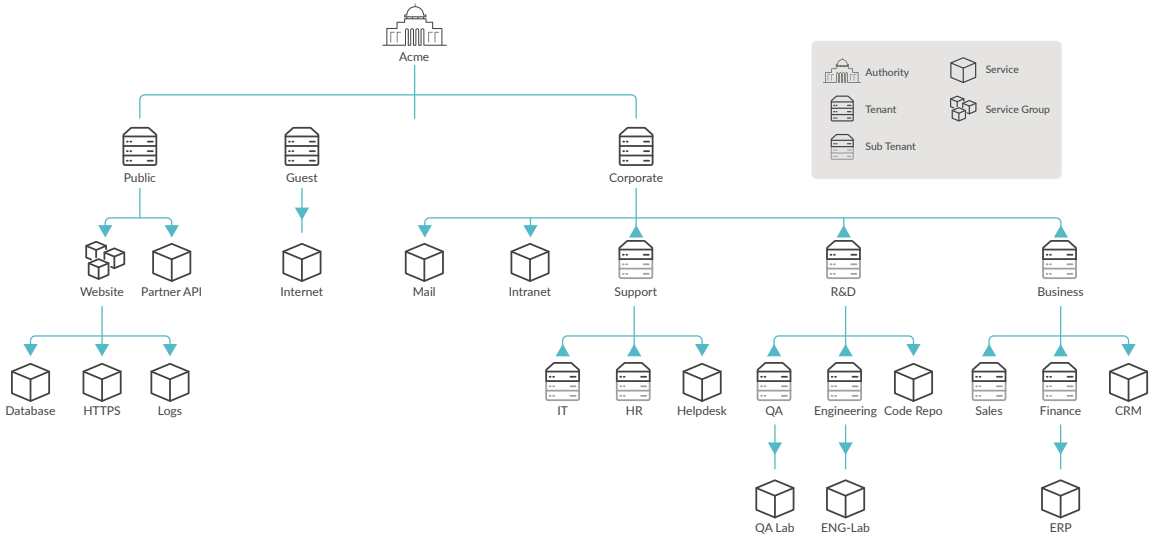

Figure 2: Access to network services is based on tenancy

Administrators define the tenants (user populations) that use the network and the services offered by the network. Using an intuitive, text-based language, administrators grant or deny access to those services for members of the various tenants on the network. Those tenants and services, along with security properties such as authentication and encryption keys, include each Session Smart Router within an administrative domain (what we call an authority).

This approach ensures that network resources are offered only to authorized users. Internally, these tenant and service definitions are used to construct a routing information base (RIB) and forwarding information base (FIB) for each Session Smart Router.

Zero Trust Model

As sessions are processed through the Session Smart SD-WAN solution, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other capabilities.

Unlike traditional routers, which implicitly trust all traffic by default, the Session Smart Router follows the SP 800-207 principle of assuming no implicit trust, denying all traffic by default. It establishes trust by examining tenancy and service attributes using a zero trust model.

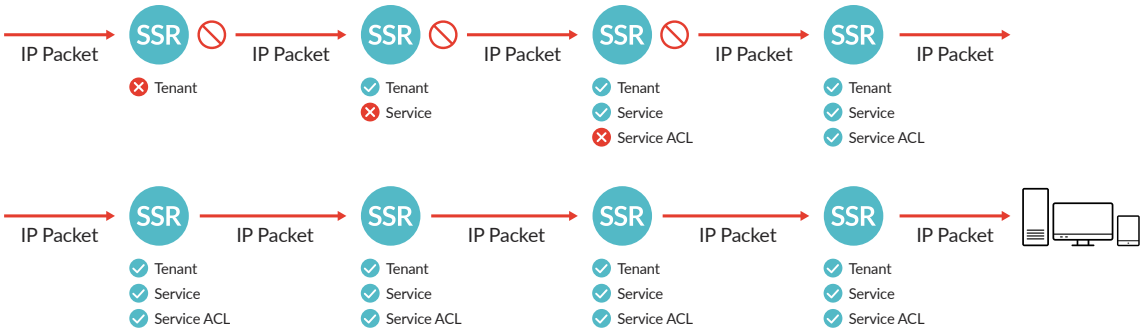

Figure 3: Deny by default access policy.

How It Works

When a packet hits the Session Smart Router, it first checks to see if the packet belongs to a tenant. If the packet does not belong to a tenant, the traffic is deemed untrusted, and the packet is dropped. If the packet belongs to a tenant, the router checks to see if the packet is destined to a service defined within the tenant. If the destination of the packet does not correspond to any service within the tenant, the traffic is deemed untrusted and the packet is dropped. If the destination of the packet belongs to a service, the Session Smart Router will look at the context-specific ACL defined within the service to see whether the source of the packet has permission to access the service. If the source does not have permission to access the service, the packet is dropped. If the packet passes all the above checks, the traffic is deemed trusted, and the packet is forwarded to the next hop towards its destination. It is important to note that each Session Smart Router performs all of these checks, on every packet, without impacting performance.

With a deny-by-default approach, unless an enterprise explicitly enables a session to traverse through the network, the Session Smart Router drops all the packets belonging to that session. This tight control of the packet flow within the network prevents lateral movement and can eliminate network attacks.

As sessions are processed through the Session Smart SD-WAN solution, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other functions.

Centralized Administration and Management

The Session Smart Conductor provides centralized administration and management for all routers running in the enterprise network. With traditional network firewall devices, policy management complexity for things such as configuring ACLs grows exponentially as the network grows. The Session Smart SD-WAN solution dramatically simplifies administration by describing policies in terms of services rather than networking constructs, making policies contextual. In addition, unlike with traditional network firewalls where ACLs are defined individually for every appliance, policies are defined and enforced globally for all routers associated with an authority.

Versatile Solution Supports All ZTA Use Cases

The Session Smart SD-WAN solution acts as a policy enforcement point (PEP) in an NIST SP 800-207 ZTA, securing and controlling traffic at the edge. The solution adheres to the key tenets of zero trust laid out in the NIST publication and supports a range of NIST SP 800-207 deployment scenarios. Figure 6 shows how Session Smart SD-WAN components can be deployed in an SP 800-207 zero trust architecture.

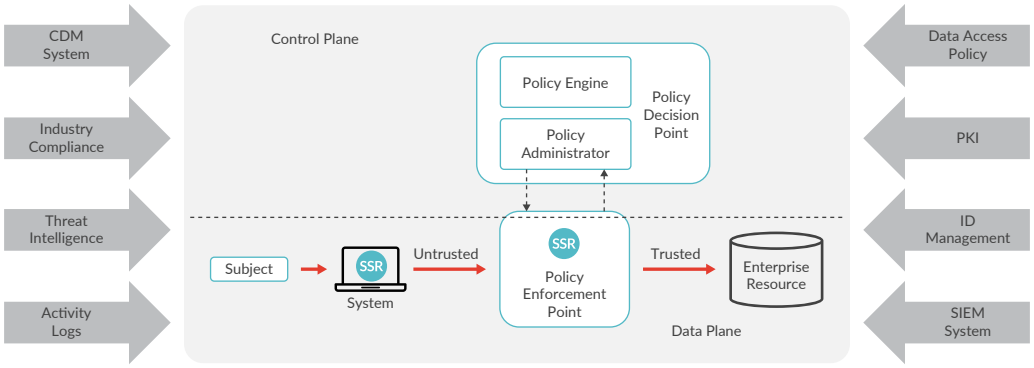

Figure 4: Session Smart SD-WAN deployed in an SP 800-207 zero trust architecture

The Session Smart SD-WAN solution supports the four primary ZTA use cases called out in NIST SP 800-207, namely Enterprise with Satellite Facilities, Multicloud/Cloud-to-Cloud Enterprise, Enterprise with Contracted Services and/or Nonemployee Access, and Collaboration Across Enterprise Boundaries.

Enterprise with Satellite Facilities

The first NIST SP 800-207 use case is intended to provide secure and cost-effective cloud connectivity for teleworkers and small remote offices. Session Smart SD-WAN satisfies this deployment scenario using the Session Smart Router and Session Smart Connect software.

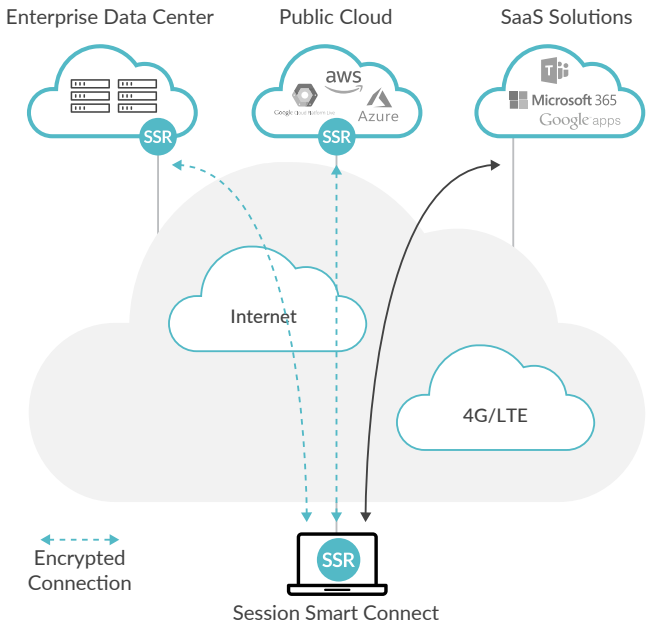

Figure 5: NIST SP 800-207 enterprise with satellite facilities use case

Session Smart Connect, which utilizes a third-party plugin, extends the benefits of Session Smart SD-WAN to the endpoint. Session Smart Connect works with the Session Smart Router, intelligently managing and securing traffic at the edge, based on administratively defined policies. The solution provides FIPS 140-2 certified, end-to-end encryption for cloud workloads and direct Internet connectivity (local Internet breakout) for Software as a Service (SaaS) applications.

Multicloud/Cloud-to-Cloud Enterprise

The second use case described in NIST SP 800-207 is intended to provide secure, efficient, and reliable WAN connectivity and cross-cloud communications for multicloud implementations.

The Session Smart SD-WAN solution is well suited for this use case, as it intelligently controls and routes traffic at the edge to avoid tunneling and backhauling cost and latency as guided by NIST SP 800-207.

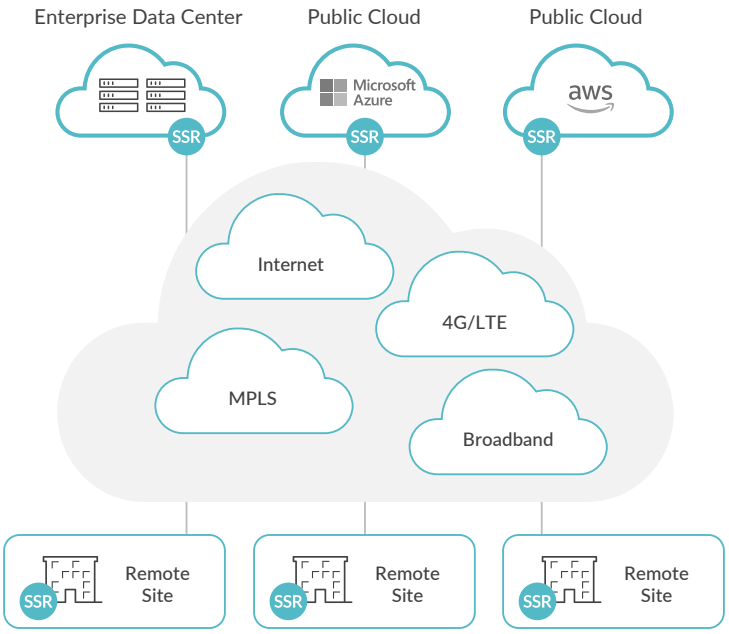

Figure 6: NIST SP 800-207 multicloud/cloud-to-cloud use case

The Session Smart Router automatically forwards traffic over the right path, for the right application, at the right time based on policy and real-time network conditions to optimize service quality, availability and costs. The solution distributes traffic across clouds to balance performance. And in the event of a link failure or network outage, the Session Smart Router seamlessly redirects traffic to a backup connection or alternative network path without disrupting sessions or impairing application performance. Session Smart SD-WAN leverages a unique tunnel-free architecture that eliminates protocol overhead, reduces WAN bandwidth consumption and data cloud transfer/egress fees by up to 50%, and provides granular visibility and control.

Enterprise with Contracted Services and/or Nonemployee Access

The third use case is intended to provide granular network access controls for onsite contractors and visitors. Based on the principle of hypersegmentation, the Session Smart Router easily satisfies this use case.

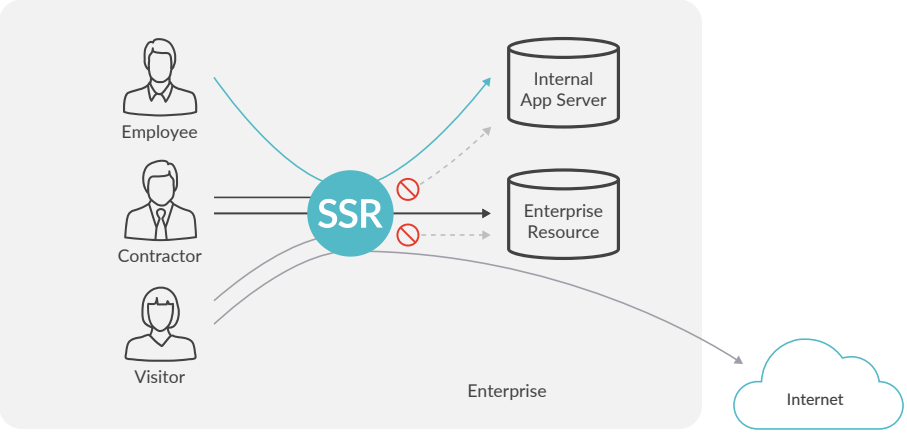

Figure 7: NIST SP 800-207 contracted services and/or nonemployee access use case

Juniper's zero trust, deny-by-default security model makes it easy to grant explicit access to specific enterprise resources on a per-session basis. Enterprise IT administrators can decide the exact enterprise resources each user is allowed to access. In this example, a full-time employee is granted full access to all enterprise resources; an onsite contractor is granted access to a project database, but not an internal application server; and a visitor is granted Internet access only.

Collaboration Across Enterprise Boundaries

The final use case is intended for organizations that share enterprise resources with external organizations for collaborative activities.

For example, a government agency (Enterprise A) may need to share select enterprise resources with certain employees working for an external contractor (Enterprise B) as part of a joint R&D program. The Session Smart Router tightly controls access based on user identities and administratively defined policies, making it ideal for this deployment scenario. In this example, an onsite employee is granted full access to all enterprise resources; an employee of Partner B is granted access to database 2; and an employee of Partner C is granted access to database 1 and database 2.

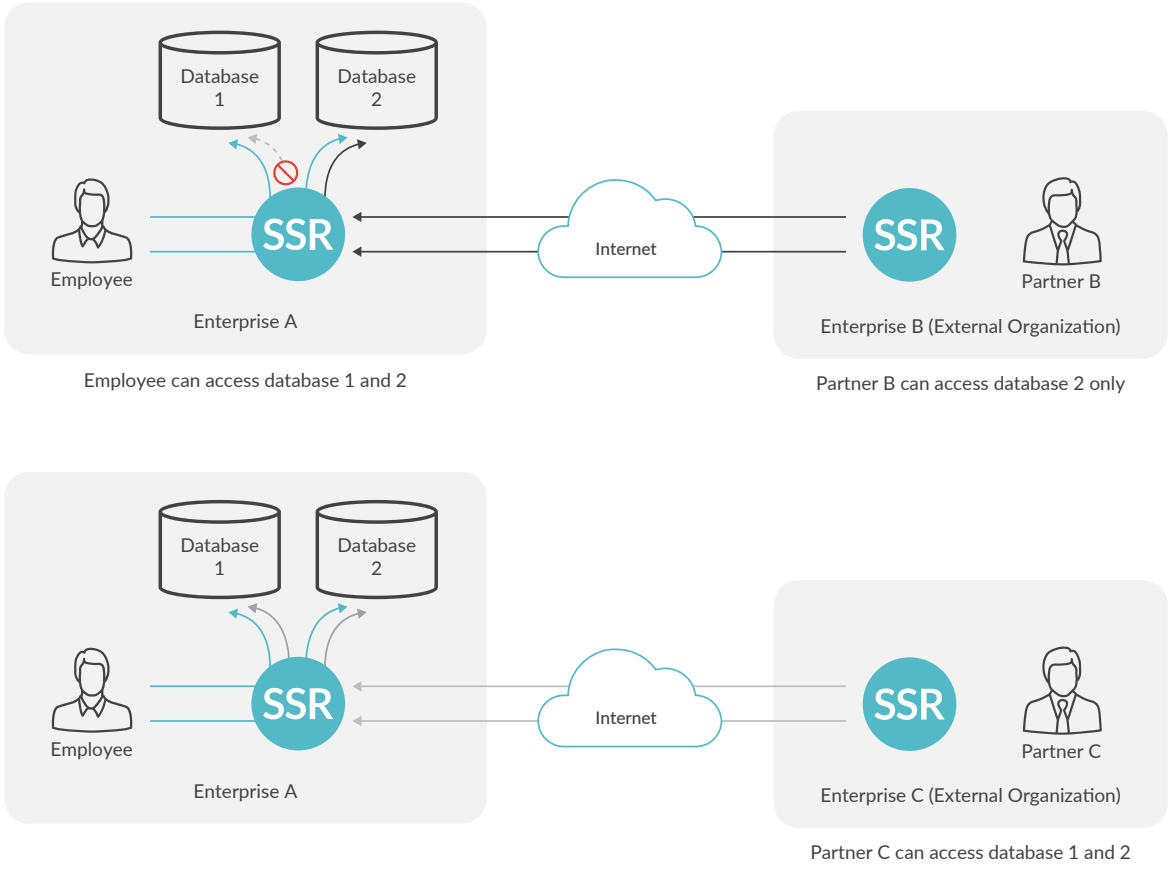

Figure 8: NIST SP 800-207 collaboration across enterprise boundaries use case

Conclusion

Government agencies and other enterprises are migrating IT infrastructure and applications to the cloud to streamline operations, increase mobility, and reduce expenses. But conventional perimeter-based security models, designed to control access to trusted enterprise networks, are not well suited for this new digital world. NIST SP 800-207 defines a new zero trust architecture for today's cloud-centric organizations using a model in which users are authenticated, authorized, and secured in real time, upon session establishment, independent of network location.

The Juniper Session Smart SD-WAN solution was conceived with zero trust principles in mind and can be deployed as a policy enforcement point in a variety of SP 800-207 use cases. The Session Smart Router automatically forwards traffic over the right path, for the right application, at the right time based on policy and real-time network conditions for ultimate service quality and economics. This allows today's digital enterprises to provide secure access to users and devices, independent of location.

The solution helps government agencies support their Cloud Smart programs and other modernization initiatives, while avoiding the inherent performance and cost constraints of traditional networking solutions and the inherent vulnerabilities of traditional enterprise security architectures. Session Smart SD-WAN helps agencies accelerate digital transformation initiatives, and make the most of their cloud investments, while mitigating risk.

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