TRANSITIONING ENTERPRISE CUSTOMERS TO THE CLOUD WITH JUNOS PULSE

Junos Pulse Secure Access Service Enables Service Providers to Deliver Scalable and On-Demand, Cloud-Based Deployments with Simplicity and Agility
Table of Contents
Executive Summary ........................................................................................................... 3
Introduction ..................................................................................................................... 3
Secure Cloud Access Service ........................................................................................... 5
  Junos Pulse Client ....................................................................................................... 5
  Junos Pulse Secure Access Service ............................................................................ 6
  The SAML-Based Federated Identity ........................................................................... 6
Use Cases in the Service Environment ................................................................................ 7
  Use Case 1: Delivering Enhanced Cloud Service with Secure Access ....................... 7
  Use Case 2: Offering Service Provider Managed Secure Access Service ................. 8
  Use Case 3: Offering a Virtual Data Center for SMBs .............................................. 9
Use Case Summary .................................................................................................... 10
Conclusion .................................................................................................................... 10
About Juniper Networks ................................................................................................ 10

List of Figures
Figure 1: Discrete cloud access and suboptimal cloud integration scenarios .................. 4
Figure 2: Secure cloud access service with Junos Pulse ............................................... 5
Figure 3: SAML model overview ................................................................................. 7
Figure 4: Use Case 1: Delivering cloud service with secure access ............................. 8
Figure 5: Use Case 2: Offering service provider managed secure access service .......... 9
Figure 6: Use Case 3: Offering a virtual data center for SMBs ................................... 9
Executive Summary

The emergence of cloud computing has placed a microscope over the data center and has resulted in innovative fabric technology that can unleash the potential for virtualized environments and the multi-tenancy of services. To capitalize on these new cloud-ready data centers, end user-oriented service delivery models are required to address not only the security needs of the enterprise but also deploy best-in-class security across hybrid private and public cloud environments while still maintaining the highest levels of user experience.

The rise of the “prosumer”—an individual who is both professional and consumer—drives the need for superior quality of experience and secure access to both personal and business applications from the same, often privately owned device—the so-called Bring Your Own Device (BYOD) trend. However, the need to protect and leverage incumbent investments, combined with the growing trend of mobile and unmanaged devices, leads to a number of security and integration challenges not previously experienced by the enterprise or service provider.

Juniper Networks® Junos® Pulse product portfolio enables service providers to provide a secure cloud access service. By providing this access “as-a-service,” providers become brokers who can offer the enterprise consistent, secure, and quick access to private, hosted, and third-party cloud services, thus enabling a more rapid cloud adoption. This paper provides an overview of the Junos Pulse Secure Access Service for service providers, highlighting ways that they can extend and enhance their cloud service capabilities and support the proliferation of mobile access.

Introduction

According to IDC, the Software as a Service (SaaS) market achieved worldwide revenues of $16.6 billion in 2010 and is expected to grow to $53.6 billion by 2015 at a compound annual growth rate of 26.4 percent. This high growth market gives service providers a unique opportunity to play a broker role with an end user-oriented service delivery model that alleviates integration and user experience challenges on behalf of their customers.

The service delivery model includes the following service characteristics:

- Provides trust-based federated identity within the cloud service environment to remove integration and access security barriers between cloud providers and consumers, driving a more rapid cloud adoption
- Provides various types of remote access, from Web application access to network Layer 3 private connection, differentiating the service provider’s cloud service from commodity-based cloud services
- Secures mobile devices with BYOD policy that allows end users to use privately owned devices to access cloud services and business applications without compromising security, thereby empowering enterprise customers’ mobile workforce
Figure 1 illustrates the customer challenges in a nonfederated cloud environment.

In flow 1 (Figure 1), the cloud access from an end user perspective is discrete. The user must establish a dedicated authenticated session with each cloud service. When the user accesses an increasing number of cloud services, the resulting multitude of authentication processes force the user to memorize an excessive number of user names and credentials, resulting in password fatigue. Password fatigue not only reduces the user’s productivity but also leads to increased security risks to the enterprise, as users can inappropriately handle the credentials by recording them on Post-It notes, for example.

In flow 2, the cloud service integration is suboptimal. The user first establishes a remote access connection to his or her enterprise network in order to ensure that the enterprise security policies are enforced. The session is terminated within the enterprise domain. To access a cloud-hosted service, the user traffic is directed over a private link to the cloud service as an extension of the enterprise network (flow 2a). Such an approach does not integrate effectively with third-party cloud services. Access to cloud services is limited to the cloud service providers to which the enterprise has a pre-established, permanent connection. Traffic is forced to traverse the enterprise premises before it reaches the service, degrading user experience as well as increasing OpEx.

The ideal scenario is to combine the policy control and enforcement of flow 2/2a with the direct access of flow 1.
Secure Cloud Access Service
Based on Juniper technology and open standards, secure cloud access service offers several compelling service benefits to customers:

- Extends incumbent enterprise security policies to cloud-based services, thereby allowing enterprises to implement a consistent, secure, and uniform access policy while still retaining control in the hybrid cloud environment.
- Uses these policies to enforce industry-leading levels of security and compliance to ensure uncompromised data protection in transit and mobile device protection.
- Enhances the user experience by simplifying the process of accessing business applications across multiple domains through seamless SSO.

The service is an end user-oriented service delivery model that consists of the following four key functions:

- Integrates the remote access security policies used in the cloud with those enforced within the enterprise, and reinforces the BYOD policy.
- Offers both Web application access and comprehensive remote access, which includes network Layer 3 tunneling and integrated access to Virtual Desktop Infrastructure (VDI).
- Federates identities among enterprises, cloud service providers and service providers.
- Supports operations support systems (OSS) and business support systems (BSS) as a delivery model.

As shown in Figure 2, secure cloud access service relies on the following two major components and one underlying technology to provide this delivery model in “as-a-service” fashion:

- Junos Pulse client running on mobile devices and desktops.
- Junos Pulse Secure Access Service running on virtual appliances to enable an easy-to-use, secure, authenticated, and protected connectivity service to remote applications.
- Security Assertion Markup Language (SAML)-based identity federation overlaid on the remote access services, to allow end users to seamlessly access multiple services with a global single sign-on (G-SSO), all under the control of a single (enterprise owned) access policy.

Figure 2: Secure cloud access service with Junos Pulse

Junos Pulse Client
In conjunction with Junos Pulse Secure Access Service, Junos Pulse client secures mobile access and reinforces security policies in real time by:

- Supporting various types of remote access, which range from access to web-based applications to a network Layer 3 tunneling for access to the corporate network.
- Optimizing the SSO experience when accessing the cloud service, while allowing the user to establish a network Layer 3 tunneling to the corporate network. This feature becomes increasingly critical as enterprises adopt more cloud services.
- Reinforcing security policies in real time to embrace enterprise BYOD policy. For instance, Host Checker can verify device-level identity to determine if the device is a corporate asset. Also, operators can use Host Checker to ensure that the device is compliant and current with the enterprise policies before allowing access to third-party cloud services.
Junos Pulse client protects mobile devices. The Junos Pulse approach of provisioning mobile security policy aligns with
a service provider's operation model:
• Provides a rich set of security functions such as antispam, antivirus, firewall, and loss and theft protection
• Supports a broad range of mobile operating system platforms, including Google Android, Apple iOS, Nokia Symbian,
  Microsoft Windows Mobile, and RIM blackberry
• Allows a service provider to dynamically provision device configuration to a larger customer base through Junos Pulse
  Mobile Security Suite
In fact, the loss and theft protection features in the Junos Pulse client significantly reduce the risk of credentials
getting lost or stolen from the mobile device, a significant security concern that exists in any federated identity or SSO
implementation.

Junos Pulse Secure Access Service
As shown in Figure 2, Junos Pulse Secure Access Service (in the premise of a service provider’s data center) offers the
following major secure access functions and supports SAML-based federated identity:
• Ubiquitous end user access from any Internet connected device
• Centralized device and user-level compliance checking and security policy enforcement, using the Host Checker function
• Granular role-based access control through integration with the enterprise's existing authentication servers
• Web-based access to applications with complex JavaScript and XML
• Web-based access to Flash applications and Java applets that require a network socket connection
• Remote access to collaboration tools such as standards-based e-mail, SharePoint, Windows, and UNIX file share
• Remote access to system management such as Telnet/SSH and terminal emulation
• Remote connection access with network Layer 3 tunneling
• Native support for two different SAML 1.1 and SAML 2.0 specifications
Junos Pulse Secure Access Service in a virtual appliance format is suitable for service providers to deliver scalable and on-
demand, cloud-based deployments with simplicity and agility. Junos Pulse Secure Access Service provides and supports:
• Policy separation to create a multi-tenancy operation model
• A single, self-contained service and automatic provisioning to each customer, with reduced deployment time for new
  customers
• A maximum of 5,000 concurrent users per virtual machine, with on-demand service that allows automated, real-time
  changes using a unique administration interface
• Billing integration with an existing service provider’s OSS and BSS to deliver a single bill to customers for various services
  and solutions

The SAML-Based Federated Identity
SAML is an open standard framework created by OASIS (www.oasis-open.org) for communicating user
authentication, entitlement, and attribute information between security domains. SAML solves cross-domain SSO
challenges by decoupling the identity and access management process with two independent but trustworthy parties:
• SAML Identity Provider (SAML IdP)
• SAML Service Provider (SAML SP)
Figure 3: SAML model overview

Figure 3 shows SAML access flows in a typical SAML model:

- The user enrolls using at least one SAML IdP that manages credentials, for example, the idp.example.org domain. Flow 1 in Figure 3 shows that the SAML IdP verifies a user’s credentials as part of the login process.
- The user is entitled to access different websites, which are typically in different security domains from the SAML IdP. The SAML SP defines and manages a website’s access control. Flow 2 shows that the SAML SP receives an access request to the service.example.com domain from an unauthenticated user.
- Flow 3 and 4 shows that both identity-federated parties have securely exchanged their SAML assertion through an end user’s browser. It is important to know that both flows are transparent to the end user.
- Flow 5 shows that the SAML SP makes access control decisions based on the assertion provided by the SAML IdP.

SAML-based federated identity is a de facto standard in the cloud service environment:

- Cloud service providers typically play the role of a SAML SP. Many leading cloud service providers such as Google Apps, Salesforce.com, and IBM lotuslive.com offer SAML SP features.
- Enterprise customers typically play the role of a SAML IdP.
- Cloud service providers and enterprise customers exchange the SAML assertions through the end user’s browser without requiring a site-to-site VPN, resulting in cost saving benefits to both parties.
- Service providers can play the role of either a SAML SP or a SAML IdP, depending on customer requirements. Because Junos Pulse Secure Access Service supports multiple SAML instances, service provider operators can configure each SAML instance as either a SAML IdP or a SAML SP to meet their customers’ needs.

Use Cases in the Service Environment

The following use cases demonstrate that service providers can offer different secure cloud access services based on a common deployment of Junos Pulse client and Junos Pulse Secure Access Service.

Use Case 1: Delivering Enhanced Cloud Service with Secure Access

This use case allows a service provider to offer a value-added secure access feature to enhance its cloud service. As indicated in Figure 4, for each cloud service instance, the service provider allocates an instance of secure cloud access service that accepts Web application access and acts as a SAML SP. The service provider also provides a high-performance network connection between these two instances so that the access request is forwarded to and is processed in the cloud service instance.

The cloud service, combined with SAML-based federated identity, makes the cloud integration process simple. The enterprise customer first enables the SAML IdP function in the remote access device, such as one of Juniper Networks SA Series SSL VPN Appliances, and then configures SAML identity federation with the cloud services.

This use case improves user experience and security. The Junos Pulse client secures a user’s mobile device or desktop. Once the user establishes a remote access connection with Junos Pulse, the Junos Pulse client can automatically provision SSO between the established connection and the cloud access sessions, as indicated in Figure 4, flow 1.
This use case allows users to directly access cloud services without channeling unnecessary access flow into the corporate network, thereby eliminating traffic trombone symptoms and improving enterprise infrastructure agility. While this use case optimizes direct access between the mobile device and the cloud service, the enterprise still retains control over access security policy and enforcement to meet enterprise security policy needs, industry best practices, and compliance requirements.

![INTEGRATED AND SECURED CLOUD ACCESS](image)

Figure 4: Use Case 1: Delivering cloud service with secure access

**Use Case 2: Offering Service Provider Managed Secure Access Service**

The service provider allocates and manages instances of the Junos Pulse Secure Access Service for the enterprise customer that relies on such service for both corporate remote access and cloud service integration.

Each service instance allows a remote access connection and also acts as a SAML IdP. In addition, the service instance directly connects to the customer’s data center whereby the customer directly manages the identities of its workforce for better security compliance.

Once the user (now a part of the customer’s mobile workforce) signs on to the secure access service, the user automatically receives a remote access portal page that centralizes corporate internal application access links and links to the federated cloud services. The user can either access various cloud services or establish a remote access connection to the corporate network—even from a mobile device. However, before the device can access the corporate network, Junos Pulse client can reinforce security by checking to ensure that the mobile device meets corporate compliance requirements, for example, whether the device’s operating system is patched to a certain version.
Flow 1 in Figure 5 shows how the service improves enterprise infrastructure agility by optimizing cloud integration and by preventing unnecessary access flow to traverse the corporate network.

**Figure 5: Use Case 2: Offering service provider managed secure access service**

**Use Case 3: Offering a Virtual Data Center for SMBs**

The service provider can offer small and mid-sized businesses (SMBs) a preconfigured virtual data center that emulates a typical small-scale IT infrastructure to support both business applications and remote access. As indicated in Figure 6, the virtual data center includes a number of virtual machines and deploys various business applications such as back office tools and VDI. It manages the user’s identity and provides remote access, which includes web-based access to various business applications, remote access to system management, and network Layer 3 tunneling to the virtual data center.

**Figure 6: Use Case 3: Offering a virtual data center for SMBs**
By configuring SAML IdP in the service, the virtual data center can integrate cloud services through federated identity, and it can efficiently manage these integrated cloud services by centralizing the links to these services and by providing role-based access control through the service portal offered by Junos Pulse Secure Access Service.

Flow 1 in Figure 6 shows that the remote access connection to the virtual data center is well integrated with the direct access of cloud services.

**Use Case Summary**

All three of these use cases show that service providers can deploy Junos Pulse and Junos Pulse Secure Access Service as an end user-oriented service delivery model to bridge the existing gap between the conventional remote access approach and a desired secure cloud access in the cloud service environment. This approach enables new offerings that help transition enterprise customers and SMBs to the cloud service environment.

**Conclusion**

The ability to overlay federated identity over remote access service further enables the integration of public and private cloud services for the mutual benefit of service providers and the enterprise. By providing this access as a service, service providers can become brokers, offering the enterprise consistent, secure, and quick access to private, hosted, and third-party cloud services, thus enabling a more rapid cloud adoption.

Juniper Networks Junos Pulse, a market-leading solution, offers service providers the perfect opportunity to extend and enhance their cloud service capabilities. With Junos Pulse and Secure Access Service, service providers can differentiate their cloud services, capitalize on their assets, and generate significant new revenue streams.

**About Juniper Networks**

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.