

Juniper Networks

Securely Federating Identities



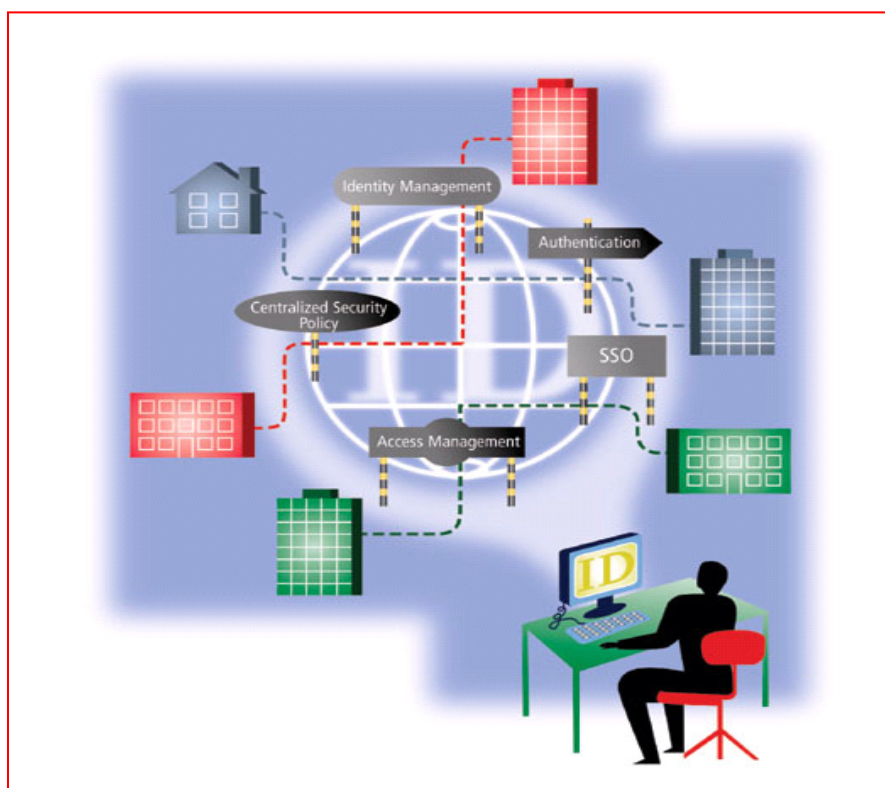
ABOUT JUNIPER NETWORKS, INC.

Juniper Networks transforms the business of networking by creating competitive advantage for our customers with superior networking and security solutions. Juniper Networks is dedicated to customers who derive strategic value from their networks, including global network operators, enterprises, government agencies and research and educational institutions. Juniper Networks' portfolio of networking and security solutions supports the complex scale, security and performance requirements of the world's most demanding mission critical networks. Additional information can be found at www.juniper.net.

BUSINESS CHALLENGE

In the networked economy, strategic partnerships are an important way to reduce product development and marketing costs, increase sales and seize new business opportunities. However, to capitalize on such opportunities, companies must be able to trust the electronic identities that access their web sites from external entities. At the same time, users need the convenience of being able to easily move from application to application across domains.

Federated identity enables organizations to share trusted identities across the boundaries of the corporate network—with business partners, autonomous business units and remote offices. A comprehensive solution, designed to be fully standards-based and compatible with other systems, is needed to allow you to unlock the true potential of your business relationships, while maintaining consistent and centralized control over the policies associated with your users and applications.



SOLUTION DESCRIPTION

Juniper Networks Netscreen SSL VPNs can provide single sign-on (SSO) to RSA Security web access management solutions via the RSA® Federated Identity Manager (FIM). Joint customers can cost-effectively provide security enforcement and extend access to critical resources without the need for incremental server hardening, resource replication and ongoing administration/patch maintenance.

Juniper Networks Netscreen SSL VPNs have been certified to interoperate with the RSA FIM. The RSA Secured® certification checklist consists of a number of SAML interoperability tests designed to ensure SAML compatibility between the RSA FIM and the Juniper SSL VPN.

Juniper SSL VPNs can act as a SAML asserting party for the RSA FIM by passing SAML authentication assertions to the RSA FIM for processing. Users are then automatically provided with an access management SSO session cookie. This prevents the need to perform additional authentication(s) to RSA ClearTrust® protected resources once a user has successfully authenticated to the SSL VPN.

A SAML profile is a set of rules that describes how to use SAML assertions within a framework or protocol to solve a particular problem. An OASIS SAML specification defines two profiles that solve the problem known as web SSO. The profiles are: Browser/Artifact Profile (BAP) and Browser/POST Profile (BPP).

Although both profiles use a SAML web SSO assertion to exchange users' security data between two web sites, each profile uses a different means to send the assertions. BPP sends assertions to the relying party by way of the user's browser. The use must always use XML digital signatures on the SAML messages to ensure their integrity.

The BAP, on the other hand, permits response messages to be signed, but signing is not required if the SOAP Binding Service communications are properly secured (for example, using SSL). The BPP is a simpler way of exchanging assertions between two sites, since no SOAP Binding Service is required. However, when using BPP, you must consider the additional complexity of configuring and managing the security environment to support XML digital signatures.

ABOUT RSA SECURITY INC.

RSA Security Inc. helps organizations protect private information and manage the identities of people and applications accessing and exchanging that information. RSA Security's portfolio of solutions—including identity & access management, secure mobile & remote access, secure enterprise access, secure transactions and consumer identity protection—are all designed to provide the most seamless e-security experience in the market. Our strong reputation is built on our history of ingenuity, leadership, proven technologies and our more than 17,000 customers around the globe. Together with more than 1,000 technology and integration partners, RSA Security inspires confidence in everyone to experience the power and promise of the Internet. For more information, please visit www.rsasecurity.com.

KEY FEATURES & SOLUTION BENEFITS**REDUCE COSTS**

- Eliminates logins and help desk calls
- Reduces administrative overhead and redundancies in managing user identity information
- Reduces deployment costs and public infrastructure maintenance

IMPROVE CUSTOMER SATISFACTION

- Provides more seamless user experience by eliminating multiple logins
- Enables personalization
- Makes navigation easier
- Allows effective web-based self-service

GENERATE REVENUE

- Makes buying and selling easier by delivering transparent access to applications
- Enables service providers to enhance their offerings, create new revenue streams and build competitive advantage

MINIMIZE SECURITY RISKS

- Increases an organization's control over its users' identity information
- Decreases the chance of identity theft since less identity information is managed by others
- Reduces information access points to minimize the risk of unauthorized access
- Reduces the number of passwords to minimize the risk of password compromise
- Stringent security with combination of RSA Security policies and Juniper End Point Defense

ADDRESS REGULATORY COMPLIANCE ISSUES

- Facilitates enforcement of security policies across multiple partners
- Allows tailoring of identity information shared across business boundaries so that organizations supply only what is absolutely necessary
- Enables design and enforcement of policies to protect user privacy
- Facilitates logging of user access events for auditing purposes

PLUG INTO EXISTING INFRASTRUCTURE

- Leverages existing user databases and user profiles
- Integrates with standards-based identity and access management solutions

PROTECT INFRASTRUCTURE INVESTMENTS

- Standards-based connections leverage investments across all partner systems and accelerate time-to-market for adding new partners
- Standards-based approach avoids vendor lock-in