

THE BUSINESS CASE FOR BUILDING AN EXTRANET PORTAL

Exploring the Virtues of an Extranet Portal and Highlighting SSL VPN Technology as the Ideal Approach for Creating It

Table of Contents

Executive Summary	1
Introduction	1
Defining the Extranet Portal	1
Traditional Extranet Implementations	4
Ongoing Costs	5
Conclusion	5
About Juniper Networks.....	6

Executive Summary

This paper will examine the benefits for using access privilege management functionality to deploy an extranet portal, as well as the specific attributes that should be taken into account as such a deployment is considered. We will then look at the use of SSL-based technology to provide a cost-effective, easy-to-manage extranet portal. This paper is ideally suited for IT administrators who are considering deploying an extranet portal. After reading this paper, IT administrators will have a better grasp on how to enable secure access for partners with an extranet portal while having the ability to control their access to specific resources.

Introduction

Enterprise IT departments have had to balance two seemingly mutually exclusive mandates—open access to corporate applications and resources, and increase access control and security. The need for access to information continues to grow exponentially as the audience that requires it has moved beyond the enterprise's walls, and the broad availability of Internet access has continued to expand. The power of SSL-based solutions meets the need for scalable remote access deployments, with the ability to provide access to all applications and access to the complete network for client/server applications, as well as clientless connectivity to telnet/SSH hosted servers, complex Web applications, files, and more. SSL VPNs provide a valid means to deliver "whole enterprise access," regardless of where the user is coming from and whether or not they have a dedicated laptop, because they provide connectivity via Secure Sockets Layer, which is part of all standard Web browsers.

As the enterprise has continued to evolve and the ubiquity of Internet use has grown, IT departments are now being forced to increase access to information for employees (intranets) as well as partners and customers (extranet portals) to maintain competitive advantage. These and other pressures are driving enterprise IT departments to re-evaluate their security, and information architectures to accommodate the increasingly dynamic and transparent ways in which a growing number of parties wish to interact. "Resource externalization" continues to grow where companies are finding the need to make at least one type of resource (files, data or applications) available to outsiders. The enterprise must find a solution that makes commonly-needed information accessible to the authorized external audience that requires it.

Extranet portals have become a part of today's mechanism for delivering information. Today's extranet portals range from partner portals, customer portals, knowledge management portals, project portals, to employee portals. Knowledge management portals have become mainstream for product support as a repository for answering the most common questions. Extranet portals have enabled many companies to be cost effective, while increasing customer service levels and enhancing relationships for future business. Increased productivity gains can be significant with the ability to quickly exchange information and/or update applications between partnering companies or people collaborating on a project using a partner or project portal.

Defining the Extranet Portal

As enterprises face the business demand for extranet portal development, IT departments must be able answer these questions for each user, based on the principle of least access:

- Who are you?
- What are you allowed to do?
- Where are you allowed to go?

While the goal is simple, the implementation can be very involved. For example, attempting to provide authentication and access controls within an application server deployed in a demilitarized zone (DMZ) using native OS, server or application controls is unwieldy. Having such vital controls in multiple places and formats creates unsustainable administrative issues and insecure deployments. It is also costly to replicate applications/servers in the DMZ, so that they are externally accessible. Ongoing patch maintenance and distributed software updates for each server permutation would have to be implemented. In addition, every new application brings with it a new database to store attributes and access rights, often incompatible with the existing infrastructure. Additionally, such a deployment can require custom development with application programming interfaces (APIs) for non-Web content, which adds costs.

Other identity and access management technologies have proven to be very expensive in terms of capital and operational costs. In fact, they have been so prohibitive that only the very largest enterprises have deployed them. Reverse proxies, as another approach, can save duplication and hardening of resources in the DMZ, but have several drawbacks. They add administrative burden and operational costs with manually managing rewriting rules and application development restrictions. Like custom portals, development is required for non-Web access.

Extranet portals represent a fundamental shift from the typical goal of network security. Instead of focusing solely on keeping potential intruders out, an effective extranet portal must focus on letting a host of users in—but in a highly controlled and selective way. Granular access management gives an organization a business-driven framework for security. The solution to secure an extranet portal must provide a single, unified framework that enables an organization to manage external users according to the principles of least access, ensuring that only legitimate users gain access, and providing fine-grained control of what each individual is given access to.

Products must include the following attributes to secure extranet portals:

Accessibility—Accessibility must be ubiquitous so that anyone can access the resources they need from any Web browser, with no client software downloads. This includes any time, anywhere secure access from a variety of Web browsers and end user devices/operating systems, including mobile and handheld PDA support.

Juniper Networks® SA Series SSL VPN Appliances use the Secure Socket Layer (SSL) as a method of secure transport. Since SSL is available as part of all standard Web browsers, there is no client software to install, configure or deploy, and the SA Series SSL VPN can provide access from anywhere and any device. Juniper Networks SA Series also supports the broadest range of operating systems/platforms and devices.

Authentication Services—The solution must accommodate a variety of different authentication methods which can be applied on a flexible per-role or per-resource basis. It should be able to check the security posture of the device before allowing authentication.

Juniper Networks SA Series SSL VPN Appliances are compatible with leading authentication stores and schemes, including Lightweight Directory Access Protocol (LDAP), RADIUS, Windows NT Domain, Active Directory, UNIX NIS, dual-factor authentication, and X.509 client-side digital certificates. SA Series appliances feature dynamic lookup to authentication stores, so that when a user logs in, the appliance sends a request to the authentication server. Once the user is authenticated, he or she is assigned a role which determines the type or types of access available for the session.

Access Privilege Management—Enterprises must be able to enforce granular controls for all applications including Web, files and client/server applications, and must take into account network trust level as well as device and session variables. Policy management and enforcement must be dynamic, to accommodate changing user environments and changing business rules. And the structure must be flexible, so that the enterprise can enable policy management using the model that best fits their needs.

The SA Series provides the ability to define rich authentication and authorization policies with flexible and expressive parameters, including endpoint device state, to allow for dynamic access provisioning. With the SA Series, enterprises can provision access by need/purpose to comply with enterprise security policies. Access Privilege Management comprises three functional areas:

- Dynamic authentication policies
- Role definition and mapping rules
- Resource authorization policies

Dynamic authentication policies specify the security requirements that need to be met before the SA Series appliance will authenticate a user. Role definition and mapping rules are rules by which the administrator can specify that any of the following variables must be present before matching a user to a role. If the user meets the requirements specified either by a role mapping rule or a role's restrictions, then the SA Series gateway maps the user to that appropriate role. Resource authorization policies include resource policies, which are a set of resource names, such as URLs, hostnames and IP address/netmask combinations, to which access is either granted or denied, or given other resource-specific actions such as rewriting and caching. A resource policy serves as the third level of resource access control. While a role may grant access to certain types of features and resources (such as bookmarks and applications), whether or not a user can access a specific resource such as Siebel, Outlook Web Access (OWA) or a given file, is controlled by resource policies.

Secure—The solution itself must be bulletproof, providing hardware, OS, and application hardening against the growing spread of Internet-launched worms and viruses. To be cost-effective, the extranet portal access solution must also provide security and system hardening without excessive manual software patching and administration. Security should be extended to ensure that the endpoint, the network and the user are secure and free from viruses or malware, from the beginning of their session and continuously throughout the entire session. Continuous security checks of the endpoint, network and user protect against malicious attacks, both intentional and unintentional.

Juniper Networks SA Series SSL VPN Appliances are built on the Instant Virtual Extranet (IVE) platform, which is our hardened, purpose-built operating system. The appliance is not designed to run any other services. There are no backdoors to exploit or hack. There is no interface, or interactive shell, or protocol to run on the machine. The IVE platform has been audited and certified by several third-party security experts.

The SA Series Host Checker can be configured to assess the security posture of the end device to confirm that the user meets certain predefined security criteria, especially if the connection is from an untrusted network. Integrated malware protection provides endpoint containment capabilities that protect users and devices from key-loggers, trojans, remote control applications and monitoring applications. Coordinated threat control technology enables the SA Series and Juniper Networks IDP Series intrusion Detection and Prevention Appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP Series to effectively identify, stop and remediate both network and application-level threats within remote access traffic.

Streamlined User Experience—Ease of use is imperative to serve any user. Single sign-on capabilities are essential, both for user convenience and to limit help desk calls generated by the user having to remember a myriad of different passwords. Customizable user interface (UI) capabilities allow companies to provide a consistent user experience and flow.

Juniper Networks SA Series SSL VPN Appliances offer extensive functionality designed to improve the end user experience including UI customization, session behavior customization, adaptive delivery, single sign-on capabilities, policy-based remediation, integrated password management, and more. Session behavior customization provides administrators with extensive capabilities to customize a user's session experience. Policy-based remediation provides administrators with the ability to customize remediation messages when end users or endpoint do not meet administrator-defined security policies, improving the end-user experience and reducing security related support issues. Password Management Integration enables users to change their passwords dynamically without needing to contact a help desk. This is particularly helpful for a partner who might not know who to contact at the hosting company.

Seamless Integration with Business Applications—The solution must interact with important business applications, without requiring major custom implementations, on a per application/server basis.

SA Series appliances provide broad support for both packaged and custom applications—all Web, thin client and client/server applications. Patent pending content intermediation engines can handle applications with advanced content types such as Extensible Markup Language (XML) and Javascript. Juniper has developed customized functionality for common user applications such as Outlook Web Access, iNotes, SharePoint, Citrix Presentation Server and Windows Terminal Server to make it easy to configure advanced settings (caching, single sign-on, and others). For example, the SA Series can prevent the download or upload of email attachments in OWA or iNotes based on the user's identity and endpoint, or the ability to connect to local printers or disks in Citrix or Windows Terminal Services Juniper's true core clientless access supports all Web-based applications.

Juniper Networks also has extensive directory and security infrastructure integration. Standards-based APIs can be used to deliver third-party endpoint products to unmanaged PCs and to integrate with installed clients.

Administration—To be effective, an extranet portal must be easy to manage. This includes management from a central point, as well as the ability to delegate administration tasks like system, resource and authorization policies to the local administrators who know them best. Adding incremental applications and users must be streamlined, and should eliminate the need to harden additional servers and deploy them in the DMZ.

The SA Series provides a variety of features for ease of administration. For example, using Juniper Networks NSM Central Manager, administrators can configure all units in a cluster from a single user interface. Wizard-based resource profiles, task guides, configuration templates, push configuration capabilities, role-based delegation, and the ability for zero downtime upgrades all make SA Series SSL VPN Appliances easy to administer.

Audit and Monitoring Services—As diverse users (partners, suppliers, customers) are allowed access to different resources, it is key to be able to audit their access and ensure that it complies with security policies. An effective extranet portal access solution must be able to show events by user and by resource, particularly if deployments need to conform to security regulations such as Health Insurance Portability and Accountability Act (HIPAA), or need to monitor critical infrastructure services for High Availability (HA).

SA Series appliances provide extensive granular logging and auditing. The appliances capture and sort logs by event, user and administrator access. Logs can be filtered and exported in a variety of formats, including WELF and W3C as well as custom formats, to leverage existing investments in reporting packages. SA Series appliances support RADIUS accounting. Juniper Networks provides virtualization capabilities that allow multiple companies to be hosted on the same appliance, each with separate auditing and logging. In addition, the SA Series dashboard gives an “at-a-glance” view of system performance and application usage, both for a single device or throughout a cluster, to aid in performance monitoring and capacity planning.

Performance—Extranet portal access solutions must scale. This necessity is due in part to the fact that the audience requiring access to resources can vary unpredictably. The solution must be able to handle an increase in audience as well as the addition of new applications or resources in a cost-effective, easy-to-manage fashion—even accounting for unplanned extreme peaks in demand, like heightened demand that might occur from a pandemic or disastrous event that suddenly triggers a substantial wave of users. In addition, the solution must be able to scale to be administered across a distributed global environment to serve users and access resources around the world. Scalability, with the ability to virtualize separate portals from a single appliance to provide even easier management and administrative capabilities like virtual LAN (VLAN) tagging and traffic separation, should be a part of that plan.

The SA Series has multiple appliances to meet the needs of medium, large, and worldwide SSL VPN enterprise and service provider deployments. SA Series mid-range and high-end appliance portfolios include hardware-based SSL acceleration for RC4, the 3DES Data Encryption Standard, and Advanced Encryption Standard (AES) encryption. Juniper Networks SA Series SSL VPN Appliances include software-based compression for all traffic (HTTP, file, client/server application) enabling rapid response times even at very high concurrent user loads. Juniper Networks SA Series Appliances with the ICE (In Case of Emergency) license option provides limited time licenses for a large number of additional users on an SA Series SSL VPN Appliance to handle a sudden short-term peak in demand. SA Series virtualization capabilities enable administrators to provision multiple logical independent SSL VPN gateways within a single appliance/cluster. Each virtual SSL VPN gateway represents a customer of a group within an enterprise providing complete segregation of traffic belonging to those customers/groups.

High Availability—The inability to access an extranet portal, particularly if it is designed to serve customers or business partners, can influence more than just user goodwill; it can impact the enterprise’s overall revenue and cost of doing business. Solutions must feature seamless failover, with no change to or interruption of user sessions.

SA Series SSL VPN Appliances can cluster units both within the LAN and across the WAN for performance, scalability and redundancy. SA Series units that are part of a cluster communicate user session information among themselves for stateful failover. Stateful synchronization is done for configuration, policy, profile and session. Note that this is true even if the cluster units are in different locations. SA Series high-end appliances include field upgradeable, dual redundant hot-swappable power supplies, hard discs with real-time data mirroring, and hot-swappable fans ensuring HA and reliability and operational convenience in the rare event of a component failure.

Traditional Extranet Implementations

Many access management software vendors have tailored their offerings around very complex e-commerce applications, with a narrow range of applications and a huge number of users. The business need in these deployments typically justifies the time required for custom development, as well as the ongoing support required to scale such a solution for more applications or a larger audience. Mid-sized to large enterprises or even departments within larger enterprises, however, cannot typically justify the cost and time needed to build such an infrastructure. A basic Authentication, Authorization and Accounting (AAA) custom extranet might include some Web servers (which must be hardened) along with accompanying agent software and a policy server for AAA and single sign-on. Portal content software can also add to the complexity.

Ongoing Costs

While the hardware and software capital expense required by traditional extranet portals can be sizable, it is the cost of deploying and maintaining them that truly puts this solution out of reach for many enterprises.

Regardless of what type of extranet the enterprise has chosen, the fact remains—traditional software-based extranet portals are not bought, they are built. Even simple deployments based on native resource access control lists (ACLs) require all of the following steps:

- Content replication from internal servers to servers in the DMZ
- Hardening of DMZ public-facing Web servers
- Enabling SSL on each server
- Deploying a digital certificate on each server
- Doing custom development with APIs to handle non-Web content such as files or client/server applications
- Enabling and administering authentication and authorization policies, potentially in multiple servers
- Ongoing patch maintenance of DMZ servers

It is important to note that these costs are not confined to the deployment of the extranet portal, but rather continue throughout the life of the deployment. Incremental applications require most of the same steps as the initial deployment itself. Security patches must be maintained continually. If the user audience grows, the deployment frequently requires the deployment of still more servers. The use of native resource ACLs across multiple different applications can quickly grow overwhelmingly complex.

Alternative options exist to deploy a software-based extranet portal solution, but in many cases the initial cost of deployment is prohibitively high. And such deployments are not without their own ongoing, incremental costs, including:

- Deployment of policy server software agents
- Design and deployment of a custom portal
- DMZ server deployment and maintenance issues as described above

Conclusion

The enterprise IT market has clearly reached a turning point as it pertains to extranet portal access. A solution is needed to keep pace with the accelerating need to provide often unknown users such as suppliers, partners and customers, who are coming from an unknown network and using unmanaged devices, a way to access resources and applications. With the advent of advanced SSL-based access solutions, customers now have an option to cost-effectively meet their extranet portal access needs. Many customers have validated the use of SSL VPNs for extranet portals. However, it is imperative to remember that a truly viable portal access solution must feature purpose-built capabilities to address the unique challenges of such a deployment. These include access privilege management capabilities and end-to-end security components that are dynamic enough to encompass changing user, device and network variables. Some SSL VPN solutions can offer convenience at the cost of these features, which are imperative for extranet portal access. Only by considering the technological capabilities of an SSL VPN offering in light of the relevant security imperatives and business needs can the enterprise find the solution that meets the entire extranet portal access challenge—securely and cost-effectively, both at implementation and into the future.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate And Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER
(888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
TaiKoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin,
Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. "Engineered for the network ahead" and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

