

Juniper Networks Increases Productivity and Protects Enterprise Resources with an Access Control Strategy



Industry: Technology

Company:

Juniper Networks

Challenges:

- Provide employees, contractors, auditors and guests with anywhere, anytime access to the specific business applications and resources they need
- Protect sensitive company information and resources
- Grant access to resources based on users' different roles and identities
- Protect network from downtime incurred from viruses and other threats
- Enforce devices accessing Juniper network resources to comply with corporate access policies such as operating system, application patch levels and current antivirus protection
- Collect user access logs to meet internal IT governance and security policies

Network Solution:

- Juniper Networks Secure Access 6000 (SA 6000) SSL VPN platform
- Juniper Networks firewall/IPSec VPN
- Juniper Networks unified access control (UAC) network access control (NAC) solution

Results:

- Secure access is provided for more than 6,200 Juniper Networks employees and 150 outside partners and contractors around the world.
- Increased productivity for employees and outside parties exists because of access to appropriate resources.
- Greater productivity is gained by short configuration time for new partners and users.
- Reduced IT support costs from using clientless SSL VPN eliminates remote access IT support calls for desktop connectivity software and access issues.

“Every user’s access is customized, but setting up new user profiles takes less than an hour because it’s so simple.”

Tony Tran,
Network Engineer,
Juniper Networks

Juniper Networks competes in a very fast-moving and innovative industry. This requires the company’s employees to collaborate with many partners, consultants and contractors, and creates a dynamic, fast-changing global workforce. The difference of succeeding or failing in any given quarter is predicated on increasing sales and development productivity through secure, reliable and high-performance network access.

Like many other companies, Juniper Networks must balance the need to allow users with the proper authority anywhere and anytime access to key resources with ensuring that business resources and applications remain secure and protected. Employees, whether they work in the office, telecommute or work from the road, need access to applications and resources. Contractors, outsourcing partners, auditors and guests need access to key Juniper resources—whether they are working from Juniper locations, their own offices or any location in between.

Challenges

Juniper's IT organization must provide the network access that facilitates everyday business while protecting the company's resources against threats. In today's highly mobile and dynamic business environment, no IT organization can take for granted that employees' or guests' devices are secure and clean. An infected laptop of an employee, guest or contractor can cause network performance issues and/or place company assets at risk.

Solution

Providing the right type of network access means not only knowing users' identities but also being confident in the integrity of the users' computers, taking comfort that the location and/or network from which they are trying to access a company's protected network is safe and secure, and that the users and their computers meet at least a minimum set of enterprise security policies.

Access controls are just one layer of protection in Juniper's multi-layered security defenses. Juniper uses SA 6000 SSL VPN and UAC NAC solutions to allow individuals both inside and outside of Juniper's offices to access the information and applications they need. The Juniper firewall/IPSec VPN is used to create secure encrypted connections to large partners.

More than 150 partner, vendor and contractor organizations access key business applications and resources on the Juniper network from anywhere in the world using only their Web browser to connect through the SA 6000 SSL VPN platform. The access for each user can be tailored on a project-by-project basis, ensuring security for resources based on users' specific profiles. Juniper's 6,200 employees use SSL VPN when they work from home or on the road. Employees in the office may use SSL VPN or UAC when connecting wirelessly on campus. As an additional layer of protection, employees use RSA SecurID tokens for two-factor authentication.

The SA 6000 SSL VPN is designed for medium to large enterprises and features best-in-class performance, scalability and redundancy. Using SSL to provide access eliminates the need for client-side software deployment, changes to internal servers and costly ongoing maintenance and desktop support. This has enabled Juniper IT to keep up with the company's rapid growth of employees and business partners.

Juniper IT ensures that endpoints meet the company's standards for antivirus and other threat protections before allowing network access. During remote access, the SA 6000 performs the endpoint assessment and provides integrated malware protection, which protects users' devices from threats such as trojans, key loggers, remote controls and monitoring applications. For LAN and branch-office coverage, UAC performs endpoint assessment. UAC combines user identity and device security state information with network location information, to create a unique access control policy for each user.

Select partners, such as offshore developers and support partners, connect through point-to-point VPN tunnels using the Juniper firewall/IPSec VPN appliances. To enhance the protection of Juniper intellectual property, offshore VPN connections are isolated through the use of "blacknets" or security zones. These zones limit these offshore developers' access to the appropriate and required resources they need to accomplish their jobs, but isolate them from the rest of Juniper's network.

Results

Easy remote access has been an important facilitator of Juniper's expansion of offshore software development. Development partners in India, China and Eastern Europe have access to the same resources as developers in the California headquarters. Juniper's education partners around the world also rely heavily on SSL VPN to get access to Juniper's Educational Services training organization. Juniper's IT support and consulting partners use SSL VPN to access the applications they support and their Microsoft® SharePoint® portal.

With the SA 6000's rich access privilege functionality, IT can ensure that different employee and visitor populations can work productively while enterprise security policies are enforced. "With the Juniper SSL VPN, a user never has direct access to our internal network and servers, which protects us from internal threats," says Tony Tran, network engineer at Juniper Networks. "We have granular control over which users have access to which resources. When they log in, they are mapped to a specific role. They can access very specific applications and file folders based on that role."

“Every user’s access is customized, but setting up new user profiles takes less than an hour because it’s so simple,” says Tran. “Role-based security and an intuitive interface makes security policies easy to manage.”

Juniper SA SSL VPN appliance has a service offering called Secure Meeting, which allows for planned or impromptu collaborative desktop and application sharing. Both Juniper’s JTAC service organization and IT service desk use Secure Meeting to diagnose customer and employee computer problems. No longer do technicians have to ask callers to take actions on their PCs and to describe the results. Callers simply accept a secure meeting from the technicians and sit back while they watch the necessary steps being taken to identify and correct their issue. The ability to remotely control users’ devices for diagnostics and repairs cuts case time down significantly.

Network access control is necessary because employees’ computers may be compromised while outside the enterprise walls. The computers may be unknowingly infected while employees surf the Internet or work remotely, and then connect their infected devices onto the network and spread malware inside the company. Guest users who may only need access to an Internet connection can come into the network with their own devices and unknowingly (or intentionally) expose the network to malware.

“Once upon a time, you could walk into a building at Juniper and plug your computer into any Ethernet jack and get network access,” says Tran. “That kind of access is becoming history.” Today, Juniper has deployed UAC in key locations and continues to roll out this NAC solution to other high-risk locations and groups. With UAC, a user must authenticate and go through a client integrity check to verify that the device is running antivirus software with the latest definition files as well as other checks—before network access is granted. Once the computer is validated to be compliant with Juniper’s security policies, it is granted network access. Checks continue even after network admission. This way, if users disable a security feature such as antivirus, they will be removed from the production network until they return to compliance.

Juniper IT also controls access inside the network through “blacknets.” Key development and IT support partners connect to the Juniper network through point-to-point IPSec VPN tunnels. “Giving contractor or vendor access into the network is a touchy topic for every organization,” says Neil Overmon, manager of advanced technology and deployment at Juniper Networks. “We needed to find a way to control their access without adding risk.”

To provide this protection, IT set up blacknets or multiple virtual firewalls using the virtualization feature of the Juniper Networks firewall. In each of these zones, traffic is isolated from other zones and from the internal Juniper network. “We called them ‘blacknets’ because we used black cables,” says Overmon. “No matter where you land in one of these network cul-de-sacs, traffic stays contained in that area.”

With blacknets, Juniper IT can prevent someone from taking inappropriate advantage of necessary resources. “For example, the outsourced IT team that supports PeopleSoft needs remote console access. Without the blacknets, there’s a risk that someone could inadvertently or intentionally control an unauthorized machine,” Overmon notes. Departments, such as human resources, development and product marketing, also have blacknets to further protect themselves and the company from threats.

Lessons Learned

As a fast-growing company, Juniper IT must provide many different user constituents with access to business applications and resources they need to do their jobs. But at the same time, the company must protect its sensitive information and intellectual property from increasingly sophisticated Internet attacks and inadvertent network security breaches. For Juniper IT, providing that comprehensive protection means a layered defense that marries proven security solutions, such as firewalls and SSL VPNs, with new solutions, such as NAC. By using the right tools for the right job, Juniper IT gains an environment that is simpler to administer while still being easily accessible for users.

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA
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
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

Copyright 2007 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

For More Information

To find out more about Juniper Networks products and solutions, visit <http://www.juniper.net>.

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.

