

Juniper Networks Increases Productivity and Protects Enterprise Resources with Access Control Solutions



Industry: Technology

Company:

Juniper Networks, Inc.

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 6500 (SA 6500) appliance
- 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 the employees of 150 outside partner and contractor vendor companies from around the world.
- Increased productivity for employees and outside parties by enabling access to job-role related resources.
- Reduced network risk and minimal IT burden and less support calls thanks to easy deployment, maintenance, and resulting increased user compliance to corporate policy.

“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 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 their 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 Control Solutions are just one layer of protection in Juniper's multi-layered security defenses. Juniper uses the SA 6500 appliance and UAC Access Control Solutions to allow individuals both inside and outside of Juniper's offices to securely access the information and applications they need. While IPsec VPN tunnels using Juniper Networks firewall/IPsec VPN devices are used to create always connected 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 6500 appliance. 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. To assure that only employees or partners with permission to access the Juniper network are allowed access they are challenged with two-factor authentication with their RSA SecureID tokens. In addition, all wireless communication is encrypted. This strong authentication and encryption is critical for both the protection of critical resources and to meet the requirements of multiple compliance programs that Juniper must adhere to.

Juniper IT ensures that endpoints like laptops meet the company's standards for current and active antivirus and other client based threat protections before allowing network access. During remote or LAN access attempts, endpoint assessment assures that users' devices meet Juniper's security requirements. A cluster of Juniper Networks Secure Access appliances is used for providing secure remote access. For LAN access at corporate HQ and select branch offices UAC is used to gain network access. Using SSL and UAC with clientless provisioning eliminated the need for client-side software management and costly ongoing maintenance and desktop support was greatly reduced. This has enabled Juniper IT to keep up with the company's rapid growth of employees and business partners without burdening the IT staff.

Select partners, such as offshore developers and support partners, connect through point-to-point VPN tunnels using the Juniper Firewall/IPsec VPN appliances or through the Secure Access appliance. The policy control capabilities of the Secure Access appliance allows Juniper IT to provide granular role-based access to each partner or vendor so they can only gain access to resources they require to accomplish their role. This greatly reduces the risk of data leakage and the compromise of intellectual property. To further enhance the protection of Juniper intellectual property on development systems, offshore VPN connections are isolated through the use of "blacknets" or secured sandboxes using the Juniper Networks firewalls. These secured sandboxes limit these offshore developers' access to the appropriate job-related 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 6500 and UAC solution'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 Networks SSL VPN appliance, partners and contractors, in most cases, do not have direct access to our internal network and servers, which protects us from unnecessary 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."

In addition to enabling a secure network environment, Secure Access appliances also enable a collaboration environment. The Secure Access family 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. In addition employees can quickly set up a Secure Meeting at anytime so that they can share and work on documents collaboratively. This is done in house, with no new hardware, and without having to pay any recurring service costs.

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. End-point assessment assuring that corporate client security policies are being followed by managed and unmanaged devices significantly reduces the risk of the spread of malware.

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.

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
www.juniper.net

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
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2008 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. JUNOSe is a trademark 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.

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 VPN, with new solutions, such as Access Control. 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.

For More Information

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

For more information on Access Control Solutions, visit <http://www.juniper.net/access>.

For more information on the Secure Access SSL VPN product family, visit http://www.juniper.net/products_and_services/ssl_vpn_secure_access/index.html.

For more information on the Unified Access Control solution, visit <http://www.juniper.net/uac>.

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.

