10 EASY STEPS TO SECURE TELEWORKING

Juniper Networks Enables Government Telework Programs

Table of Contents

Table of Figures

Executive Summary

The convergence of new technologies and business trends, along with employee preferences to work from home, is driving a rapid growth in telework. Additionally, the growth of web-enabled applications, collaboration tools and Virtual Private Network (VPN) technology has helped government departments and agencies of all sizes to allow their employees to work off-site, at least part of the time.

In addition to improved technology, which has enabled the move toward employee mobility, other drivers include greater employee retention, potentially lower real estate costs due to workers spending less time in the office, and greater productivity because employees can use travel time or waiting time to complete work-related tasks.

This paper will help business and IT managers at all levels of central and local government gain a better understanding of some drivers and benefits of teleworking and how simple it is to set up a secure teleworking environment. Using Juniper Networks® secure, high-performance networking solutions, you will be able to design and implement a cost-effective environment for remote employees in ten simple steps.

Introduction

The terms teleworking and telework for government employees refer to two scenarios enabled by remote access networking technology: working from home (also called telecommuting); and working "mobile," such as in a field-based role or working temporarily at a remote location. Together with extranet access (remote access provided to partners or vendors outside of the organization), these make up the "government extended enterprise"—a set of concepts and technologies for extending remote access into internal information and application resources in federal, state and local governments.

Market Accelerators

The adoption of telework across many government agencies continues to grow. There are many market accelerators that will continue to influence this growth of teleworking worldwide:

- The increasing availability of high-bandwidth access to homes in the more developed industrial nations continues to drive the spread of new teleworking programs and the extension of current teleworking programs, as a result of faster access options to a wider range of applications.
- National and regional legislation are placing pressure for businesses to expand flexible working options.
- Employees today expect flexible working options to improve their effectiveness and work-life balance. Many companies are implementing programs that allow working from home one or two days a week.
- Increasing environmental pressure, both globally and nationally, for companies to become good "green" citizens by reducing congestion and pollution caused by mass commutes, coupled with the inability of transportation infrastructure to keep pace with the urban population.

Initiatives

Telework programs and initiatives are justifiably gaining momentum in all levels of government. Extending the government enterprise, by extending remote access of centrally located applications and information resources to agencies, employees and partners, offers numerous benefits. Realizing that these benefits are available, government organizations are undertaking numerous initiatives to promote and facilitate telework programs for employees—even to the point of legislative mandate.[1] A recent bulletin from the General Services Administration (GSA) establishes guidelines for implementing and operating alternative workplace arrangements (AWA).[2]

[1] Rep. Frank Wolf, chairman of the appropriations sub-committee overseeing the Departments of Justice, Commerce, and State, legislated a requirement for these agencies to offer a teleworking option to eligible employees in 2005 else face a $5 million dollar budget withholding. Rep. Tom Davis, chairman of the House Government Reform Committee, is considering drafting a proposal to extend that provision government-wide.

[2] FMR Bulletin 2006-B3, dated March 13, 2006, establishes guidelines for implementing and operating AWA. These policies are designed to assist agencies in the design and operation of AWA programs as well as to resolve AWA issues commonly faced by agencies.

Benefits of Teleworking

Teleworking offers significant benefits to government employers, employees, and contractors, and it benefits the local economy as well. Interestingly, it also presents opportunities for wider social and economic benefits. A few of the key benefits are summarized below:

Benefits for Employers

- Cost savings—in facilities costs, office overheads and labor.
- Increased productivity—by avoiding travel time and the interruptions of an office environment.
- Improved motivation—through employee response to the signal of trust and confidence indicated by the employer.
- Skills retention—by keeping employees who might otherwise leave.
- Organizational flexibility—in the event of restructuring and reorganization, people can continue to work without disruption to their personal lives.
- Flexible staffing—by enabling staff to work limited hours to match peak workloads, without being concerned about travel time for those limited hours.
- Resilience—in the face of external disruptions like transport strikes, severe weather, natural disasters or terrorist action.
- Enhanced customer care—by extending customer services beyond the working day or the working week without the costs of overtime payments.

Benefits for Employees

- Reduced travel time and costs on gasoline —a primary motivation for many teleworkers.
- Improved work opportunities—by giving access to jobs outside a reasonable commuting distance.
- Less disruption to family life—reducing the need for relocation to take up “career moves” or other job changes.
- Better balance of work and family life—even with more hours of effective work, employees can still expect to see more of the family and can easily participate in home responsibilities.
- Participation in local community—by being “on the spot” to participate in community activities at a time when commuters are still en route.
- Flexible hours—by allowing each individual to adapt to their daily “rhythm.”

Social and Economic Benefits

- Reduced traffic congestion—during peak times.
- Reduced total travel and associated pollution/environmental impact—by generating a net reduction in total car travel by teleworkers.
- Wide employment/work opportunities—by allowing people access to work opportunities that arise outside of their immediate area.
- Access to work for people with specific difficulties—factors that make it difficult to travel to work or to do a normal nine-to-five working day.

In summary, the benefits of telework include increased productivity, improved balance of employee work and family-life responsibilities, reduced traffic congestion, less energy usage and resultant pollution, and reduced time spent commuting to and from the office. Having a percentage of employees at home even one day per week saves on facility costs for a current and growing workforce. These benefits are realized immediately, and have an impact every day. Government departments and agencies also benefit from a telework-enabled government workforce through an improved emergency preparedness and continuity of operations posture. Telework programs allow government agencies to remain responsive and online, supporting the needs of the American public in times of emergency or disaster.

> *“Telework also has numerous benefits that complement our transportation systems, conserve resources, and improve the quality of life. It also is a powerful way of assisting those with disabilities to participate fully in the Federal workforce by the means of advanced technology.”*
>
> —Kay Coles James, former Director, United States Office of Personnel Management (OPM)

Current Implementation Issues

Although the benefits of teleworking are clear, government has experienced problems like end user frustration, high costs of deployment and ongoing support when providing remote access solutions typically based on IPsec technology. The security concern has proven particularly vexing given the increasing sophistication and frequency of cyber-attacks against information systems. These issues have contributed to a status quo regarding remote access in government that is now beginning to change in earnest.

> *"Telework (also called telecommuting) is the ability to do your work at a location other than your official duty station. With portable computers, high speed telecommunications links, and ever-present pocket communications devices, many employees today can work almost anywhere at least some of the time. Using the flexibility to work in a home office or telework center when it is effective to do so is clearly the wave of the future, and for many of us the future is already here."*
>
> —From the Web site www.telework.gov, the joint GSA and OPM interagency Web site
> to promote federal telework adoption

Part of the problem across the all governments in general is many users and network managers are struggling to decide which technology should be deployed and where. Where do IPsec VPNs and SSL VPNs fit into their network policies, and which problems can each technology best address? These questions can best be answered by looking at the usage scenarios themselves (see Figure 1). The fact is that IPsec and SSL are not mutually exclusive technologies. They can—and in fact, often are—deployed in the same enterprise.

IPsec VPN

Administrators who need to achieve site-to-site connectivity will be well served by IPsec VPN offerings; they were created to meet the challenge of providing employees around the world with secure "always on" connectivity that enables them to access all of the corporate resources they need to achieve optimal productivity.

SSL VPN

Administrators who need to allow teleworkers, mobile employees, contractors, offshore employees, business partners or customers access to certain corporate resources will be well served by SSL VPNs. SSL VPNs are designed to address the needs of diverse audiences that need secure access to administrator-specified corporate resources from any location, and to change both the access methods and resources allowed as the user's circumstances change. SSL VPNs can also be configured to check endpoint security compliance and to either provision resources accordingly or to provide the end user with the means to remediate.

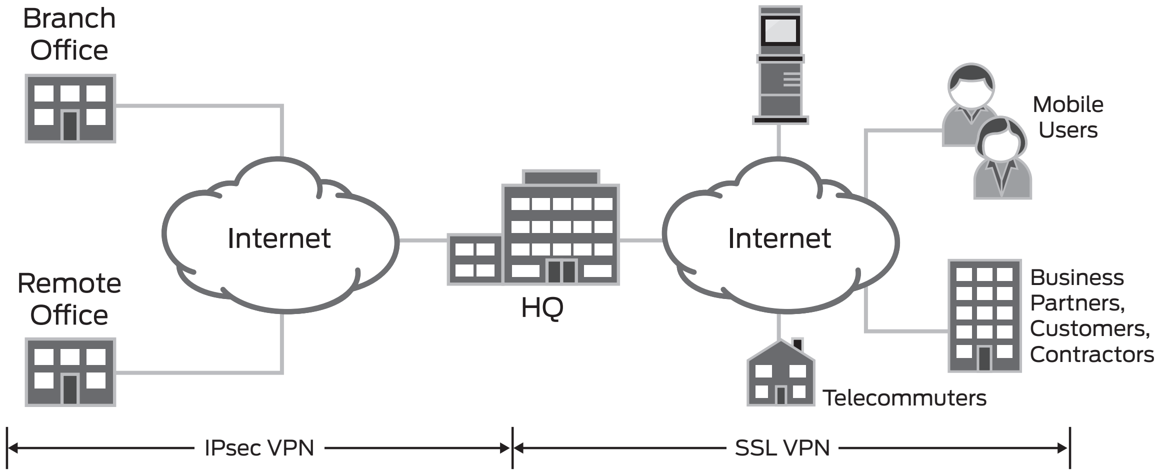

Figure 1: Applications for IPsec VPN and SSL VPN

Without this basic understanding, many of the government agencies that have already implemented client-based IPsec VPN technology for teleworkers are experiencing a multitude of problems with their current solution:

- Inflexible Access—Client-based IPsec VPN cannot reliably extend access to a variety of remote workers such as teleworkers, mobile employees, contractors and vendors/partners.
- Inadequate Security—Client-based IPsec VPN cannot provide a highly secure environment to a variety of endpoint devices, both managed (i.e., corporate smartphone) and unmanaged (i.e., home PC).
- High Cost—Client-based IPsec VPNs cannot provide this connectivity with cost-effective installation, setup, maintenance and support costs.

The Juniper Networks Teleworking Solution

As the remote access connection becomes more critical to the business of government, unparalleled security and optimization will ensure continued quality of the user experience. High-performance solutions and technologies can provide overall security and application response, thus increasing productivity while reducing cost and complexity in the data center by effectively extending the capacity of existing application servers.

Juniper Networks offers a broad portfolio of secure, high-performance networking solutions to meet the full spectrum of government agency needs. Central among these for remote and extranet access are the secure, easy to use and cost-effective Juniper Networks SA Series SSL VPN Appliances with both Common Criteria EAL2 certification and the availability of Federal Information Processing Standards (FIPS) appliances (see Figure 2).

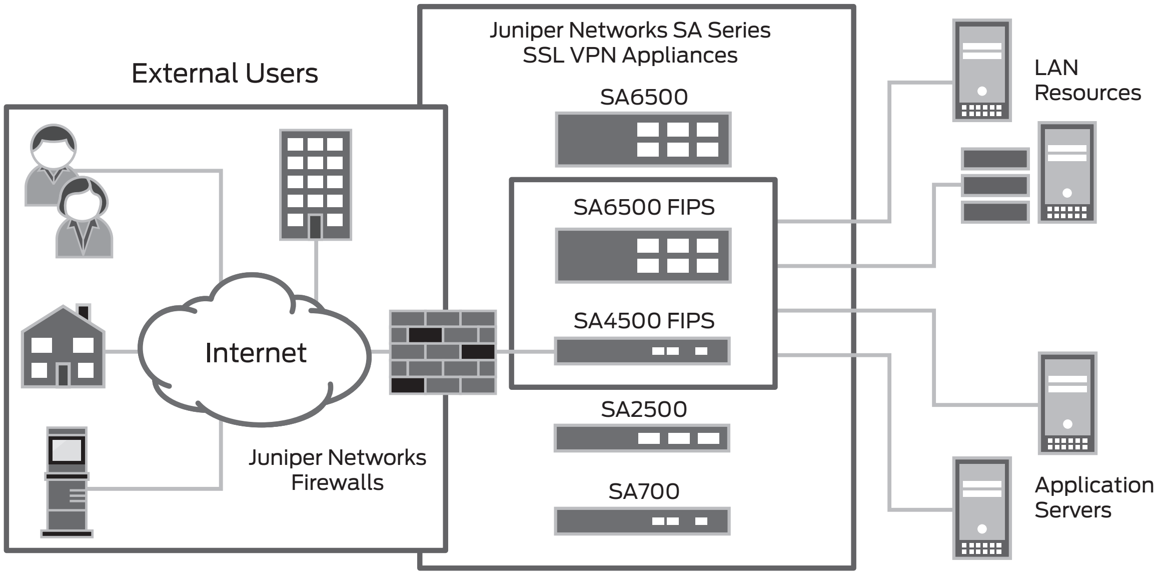

Figure 2: Juniper Networks SSL VPN solution

In fact, with Juniper Networks solutions, a secure telework program can be deployed on time and on budget in just 10 easy steps.

10 Easy Steps to Secure Teleworking

To overcome all of the issues discussed earlier, Juniper Networks can help government agencies with their existing and new telework implementations with 10 Easy Steps (as outlined in Figure 3 and discussed in further detail in the following sections).

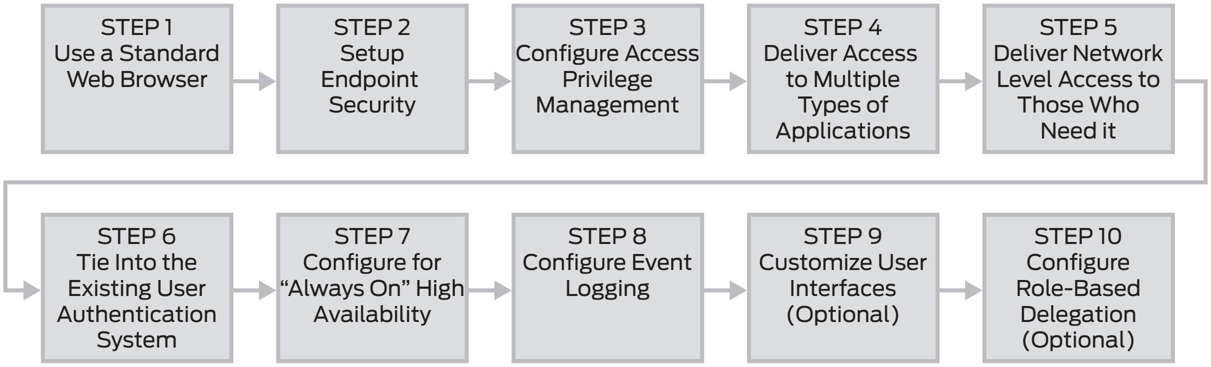
STEP 1
Use a Standard Web Browser
STEP 2
Setup Endpoint Security
STEP 3
Configure Access Privilege Management
STEP 4
Deliver Access to Multiple Types of Applications
STEP 5
Deliver Network Level Access to Those Who Need it
STEP 6
Tie Into the Existing User Authentication System
STEP 7
Configure for "Always On" High Availability
STEP 8
Configure Event Logging
STEP 9
Customize User Interfaces (Optional)
STEP 10
Configure Role-Based Delegation (Optional)

Figure 3: 10 easy steps to secure teleworking

Step 1

Step 1: Use a Standard Web Browser

Step 1 is significant in that it is a "non-step." Administrators do not need to install a VPN client application on each and every device used by end users for remote access. Unlike IPsec where a full software client must be loaded on each device, SSL VPN remote access is clientless and uses SSL (Secure Sockets Layer), the security protocol found in all standard Web browsers, providing significant savings in cost and aggravation for both IT staff members and end users. Where a thin client is needed for more sophisticated access, it is dynamically and automatically downloaded for the session. Best of all, this process is fully automatic and transparent to end users.

Step 2

Step 2: Setup Endpoint Security

The SA Series SSL VPN Appliances automatically performs a pre-authentication assessment of the network and system attributes of the end user device initiating the connection. This is done before the authentication process to ensure a secure environment before user credentials are exchanged. The Host Checker consists of specific checks selected by the administrator to ascertain the security posture of the end user device. Endpoint checks include ensuring devices have the required installed/running security appliances (antivirus, firewall, etc.) searches for specific files and running processes with Message Digest 5 (MD5) hash check validation, as well as a check of registry settings on the system. Checks can also require or restrict specific network ports, verify the source IP address, and validate the presence of digital certificates. Host Checker is supported on Windows, MAC and Linux platforms.

Also provided with the Host Checker functionality is an open application programming interface (API) allowing easy integration with leading third-party desktop security software vendors like Sygate, McAfee and Microsoft. The Host Checker API verifies the presence of these host-based antivirus and personal firewall programs, and determines whether the latest update version is running. The Enhanced Endpoint Security license provides a full-featured, dynamically deployable antispyware/antimalware module that is an OEM of Webroot's industry-leading Spy Sweeper product. With this new capability, organizations can ensure that unmanaged and managed Microsoft Windows endpoint devices conform to corporate security policies before they are allowed access to the network, applications, and resources. For example, potentially harmful keyloggers can be found and removed from an endpoint device before users enter sensitive information such as their user credentials.

Host checking substantially increases the overall system security by ensuring an acceptable endpoint security posture of both managed and unmanaged devices including the growing use of mobile devices. The endpoint security posture is one of the factors used to determine the level of access that will be permitted under the "provision by purpose" methodology (refer to steps 3 and 4).

Step 3

Step 3: Configure Access Privilege Management

Define which users can have access to which applications and information resources as granularly as required. Dynamic access privilege management is determined for each session and is based on user identity, the type of device connecting, administrator-defined Host Checker security controls, and network trust level. The result is mapped to a granular resource access control policy that specifically includes the URL, server, and application or file. This level of control over application access is not only strong security, but also supports regulatory compliance measures such as Sarbanes-Oxley and creates logs for auditing.

Step 4

Step 4: Deliver Access to Multiple Types of Applications

With SA Series SSL VPN Appliances, you are not limited to accessing only Web-enabled applications. Users can also have remote access to non Web-enabled applications and information. In addition to providing secure remote access to Web-based applications, the SA Series supports access to traditional client/server applications like Microsoft Outlook, IBM Lotus Notes, terminal services applications such as Microsoft Windows Terminal Services (MSTS) and Citrix, using just a standard Web browser. This access method used to access these applications is called the Secure Application Manager (SAM) and includes the following characteristics:

- Minimal requirements: Standard Web browser, Internet connection, and compatible Java VM or MS Windows OS
- Automatic and transparent provisioning of application connections to messaging servers, files servers, legacy servers and other client/server resources
- No administrative changes required for enabling access to either the network, the network addressing scheme or the applications being accessed

Provision by purpose is the functionality that allows for three methods of remote access to internal resources based on the user, device and network information on a per-session basis. All of this is controlled by the administrative policy configured into the SA appliance and is transparent to the end user. The three access methods are:

- **Clientless Core Web Access**: Access to Web-based applications, including complex JavaScript and Java applets, as well as standards-based email like Outlook Web Access (OWA), Windows and UNIX file shares telnet/SSH hosted-applications, Terminal Emulation, Sharepoint, virtual desktops, and others. This is the most basic access method.
- **Secure Application Manager (SAM)**: Described above.
- **Network Connect:** Complete network layer access via an automatically provisioned download for Windows, MAC or Linux platforms, using just a Web browser.

Step 5

Step 5: Deliver Network Level Access to Those Who Need It

The third connection method is called Network Connect. Network Connect basically provides the same level of access as traditional IPsec VPN remote access connections but without the heavy IPsec client maintenance and without the potential network snags of IPsec like Network Address Translation (NAT) issues. With Network Connect, a dynamic lightweight client applet (Java or ActiveX) is automatically downloaded after login to the remote machine. The applet runs during the session without any user involvement or even awareness, and is supported on Windows, MAC and Linux platforms.

Network connect is an appropriate connection method for certain user types such as IT staff, or when access to legacy protocol-based applications is required. The advantage is that now this IPsec-like full network layer access is provided with the additional security framework of the SA Series with Host Checker. With this method, application layer threat removal can be provided through Juniper Networks IDP Series Intrusion Detection and Protection Appliances. Best of all, both types of remote access are fully supported in the single SA Series appliance.

Step 6

Step 6: Tie Into the Existing User Authentication System

The SA Series can tie into the existing user authentication and public key infrastructure (PKI) systems already deployed. Whether you are using Lightweight Directory Access Protocol (LDAP), RADIUS, NT Domains, ACE, Unix NIS or a local user database, the SA Series can utilize your existing systems for user authentication and authorization. The SA Series also supports single sign-on functionality. SSO allows users to access applications or resources such as virtual desktops protected by another access management system without needing to re-enter their login credentials. This helps users by not having to maintain multiple sets of login names and passwords.

Step 7

Step 7: Configure for "Always On" High Availability (HA)

In addition to robust high performance being important to assuring the remote access experience, two high availability (HA) options keep the connections up and running, offering seamless failover with minimal downtime. HA helps keep government "always-on," and is especially important as reliance on the remote access connection grows. First, stateful peering operates in an active-standby mode, where the backup unit has fully synchronized the remote access sessions and can immediately take over without the client reinitiating a connection. If an application accelerator device from any vendor is included in the configuration and configured as a load balancer, it is possible to set up an active-active mode, where all the units are active and processing requests. Second, the "cluster" option provides the same degree of seamless failover and also easily handles connection bursts and intensive application support. In either case, the failover is transparent to end users. Additionally, ensuring HA and resilience in the firewall and router are also important considerations.

Step 8

Step 8: Configure Event Logging

Configure event logging to support business and security objectives. Events, user access and administrator activity all generate highly granular logs that are stored locally and can be sent out in system log format. User connections including actions are fully logged, and provide both access and usage logging for security, system provisioning and compliance auditing.

The Juniper Networks NSM Central Manager application can be used to compile the log data into standard reporting formats including W3C and WELF, or can be customized for inputting into proprietary reporting packages.

Step 9

Step 9: Customize User Interfaces (Optional)

Based on the specific user group or role, customizable sign-on Web pages provide an individualized look and feel. Also, specific features and functions can also be made available or kept hidden from the user on the individualized page. With this functionality, the single investment in the SA Series can be leveraged across various departments and uses. The customized user interface capability is especially useful for extranet applications.

Step 10

Step 10: Configure Role-Based Delegation (Optional)

The main administrator can delegate system control of specific user communities and their associated access policy configurations and settings to the appropriate personnel, giving direct ownership where it makes sense for the overall organization.

For organizations that have various groups each in charge of their own user communities, the SA Series can be configured to support this administrative separation virtually all within the single device. Role-based delegation supports the leveraging of a single device across various groups, and is also especially useful for extranet applications—offering flexibility and enhancing cost-effectiveness.

In summary, by following these 10 steps, any government agency can be well on its way to providing remote and extranet access that is secure, easy and cost effective.

Additional Steps for a Market-Leading Solution

Once a government agency has followed these 10 easy steps and implemented a secure telework environment, it should then take the additional steps towards ensuring a coordinated threat control posture around critical assets. It should also determine how best to optimize the WAN connections used (see figure 4).

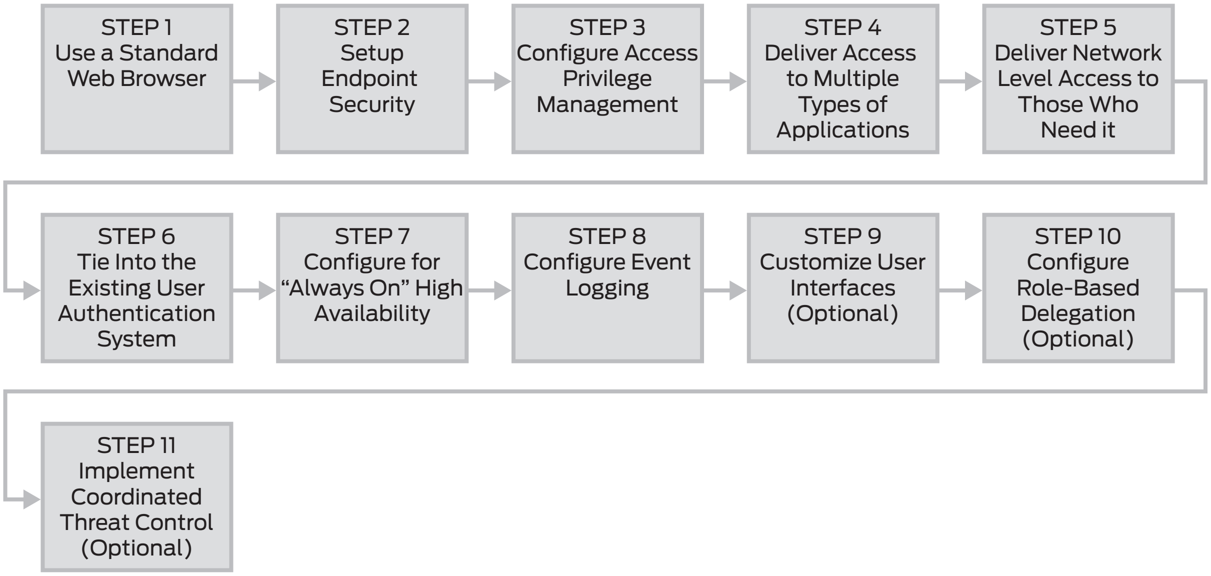
STEP 1 Use a Standard Web Browser
STEP 2 Setup Endpoint Security
STEP 3 Configure Access Privilege Management
STEP 4 Deliver Access to Multiple Types of Applications
STEP 5 Deliver Network Level Access to Those Who Need it
STEP 6 Tie Into the Existing User Authentication System
STEP 7 Configure for “Always On” High Availability
STEP 8 Configure Event Logging
STEP 9 Customize User Interfaces (Optional)
STEP 10 Configure Role-Based Delegation (Optional)
STEP 11 Implement Coordinated Threat Control (Optional)

Figure 4: Easy steps to secure teleworking

The increased need for remote access for the extended enterprise of employees, partners and customers must be balanced with steps to ensure that valuable resources and assets are protected from intentional or unintentional attacks like viruses, trojans, worms and spyware. A common way of adding security to a remote access deployment is to utilize an Intrusion Prevention System (IPS), however just deploying IPS behind an SSL VPN can be limiting. When malicious traffic is detected, it can be difficult to correlate the malicious tunneled traffic to a specific user and sometimes impossible to identify a user with inter-mediated traffic.

Step 11

Step 11: Implement Coordinated Threat Control (Optional)

Juniper’s coordinated threat control provides a solution for overcoming the challenge of balancing extranet access by remote employees and partners to critical applications, while maintaining a strong security posture around the enterprise’s critical assets (see Figure 5).

Unlike many of the existing solutions in the market today, this coordinated threat control technology enables Juniper Networks SA Series SSL VPN Appliances and IDP Series Intrusion Detection and Prevention Appliances to tie the session identity of the SSL VPN with the threat detection capabilities of the IDP Series to effectively identify, stop and remediate both network and application-level threats within remote access traffic.

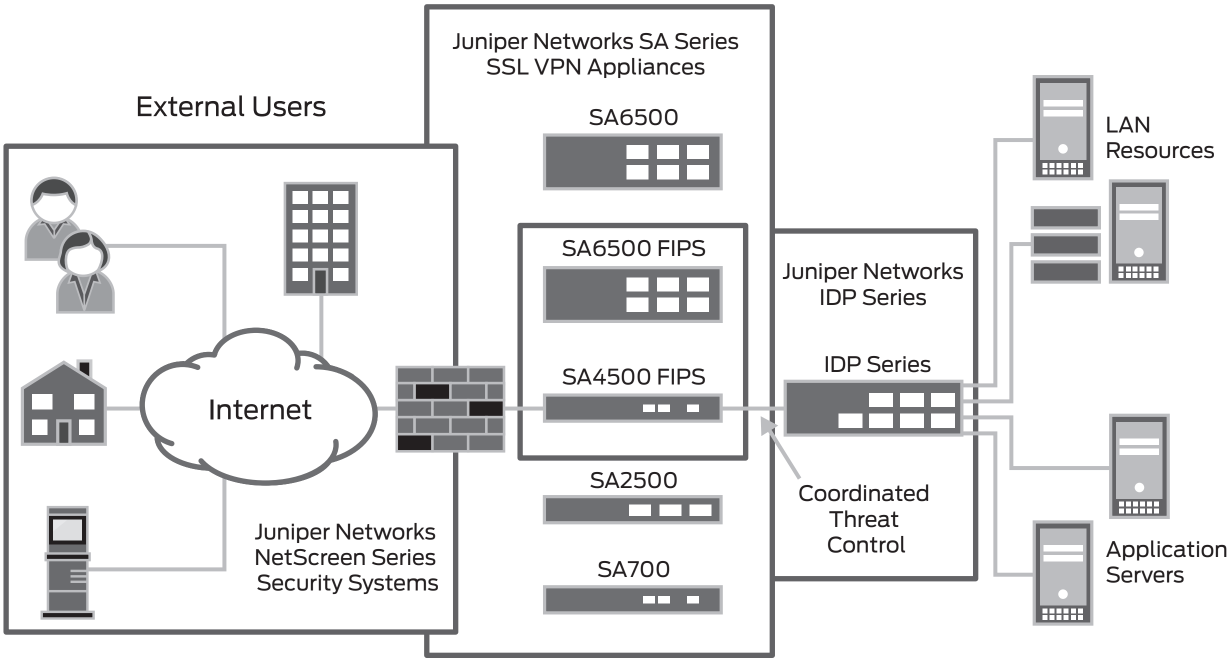

Figure 5: Juniper Networks coordinated threat control

With this technology, when the IDP Series detects a threat or any traffic that breaks an administrator-configured rule, it signals the SA Series appliance. The SA Series uses the information from the IDP Series to identify the user session that is the source of undesired traffic. Utilizing this information, the SA Series is able to take actions on the endpoint that include terminating the user session, disabling the user's account or mapping the user into a quarantine role.

With this functionality, the combined SA Series and IDP Series solution allows administrators to take action by not only blocking attacks before they reach their targets, but also by taking coordinated action against the endpoint that is the source of the attack. An added benefit of implementing the IDP Series component is its ability to secure the entire local area network.

Conclusion

Juniper Networks enables government departments and agencies to implement secure teleworking in 10 easy steps by providing Common Criteria and FIPS certified secure and cost-effective remote access along with a broad portfolio of high-performance networking solutions. Leading the charge out of the status quo with over 31 percent SSL VPN market share, Juniper Networks is the market leader in networking solutions that reduce capital expenditures for extranets and the operating costs associated with remote access.

With the addition of a Juniper Networks IDP Series appliance for a coordinated threat control solution works to provide secure access. With this solution, government agencies can continue to service the ever-expanding need for anywhere, any time access to information with the confidence that their security posture remains uncompromised, while also boosting application usability and acceptance.

Together with our partners, Juniper Networks provides tested, high-performance networking solutions implemented on any infrastructure to improve productivity and efficiency in an "always on" e-government environment.

For more information about Juniper Networks security solutions for government, visit: **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**.

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
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

2000145-002-EN Dec 2009

♲ Printed on recycled paper