

ENSURING BUSINESS CONTINUITY IN GOVERNMENT

Juniper Networks Remote Access and
Survivable Field Office Solutions

Table of Contents

Executive Summary	3
Introduction	3
Continuity Planning in Government	3
What is Continuity Planning?	3
Examples of Recent Disasters and Alerts	3
Pandemic	3
Natural Disasters	4
Other	4
Continuity Planning—Proactively Being Prepared	5
Business Continuity Challenges	5
Secure Remote Access	6
Current Remote Access Issues	6
SSL VPN	6
Remote Access and SSL VPN	7
SA Series with ICE License	8
Maintaining Productivity	8
Sustaining Partnerships	9
Meeting Federal and Government Mandates	9
Providing Online Collaboration	9
Balancing Risk and Scalability	10
Survivable Remote Field Offices	10
Additional Juniper Networks Solution Components	11
Coordinated Threat Control	11
Juniper Network Services	12
Conclusion	12
About Juniper Networks	12

Table of Figures

Figure 1: Remote access and SSL VPN	7
Figure 2: SA Series product family	8
Figure 3: Wireless 3G connectivity can be configured as primary or backup WAN connection	10
Figure 4: Juniper's coordinated threat control	11

Executive Summary

The concept of business continuity is based on the identification of all business functions within an organization, and the assignment of a level of importance to each business function. Business continuity planning ensures that all personnel in an organization understand which business functions are the most important to the business. These activities may include many daily chores such as project management, system backups, change control, and help desk. However, business continuity is not something implemented at the time of a disaster; business continuity requires planning and should include all activities that need to be performed daily to maintain service, consistency, and recoverability.

To help government IT managers gain a better understanding of and appreciation for continuity planning, this document explains the importance of having a secure and reliable remote access component and survivable field offices as part of your continuity plan, and describes how best to take a proactive approach using Juniper Networks® SA Series SSL VPN Appliances and SRX Series Services Gateways to support remote access and ensure field offices remain operational during emergency situations.

Introduction

Today more than ever, government agencies and enterprise businesses of all sizes are dependent on a variety of applications and resources to access, store, and process critical information for their business functions. Despite the importance of business continuity, business continuity planning has not often been deemed a high priority. Instead, an alarmingly large number of companies have been “assuming” that their existing systems will be adequate for emergency situations. This lack of preparedness is unwise for all, and it is definitely not an option for government departments and agencies.

Continuity Planning in Government

What is Continuity Planning?

Fundamentally, continuity planning is a government organization’s need to ensure that essential functions can continue during and after a disaster. This includes the prevention of mission critical service interruptions, and the ability to reestablish full functionality as quickly as possible.

Examples of Recent Disasters and Alerts

While the recent focus on government agency preparedness for a potential pandemic influenza has received much attention in the press, there are still a wide variety of other emergency situations prompting continuity planning throughout federal, state, and local governments. Emergency situations such as hurricanes, earthquakes, blizzards, and other natural disasters have the potential for causing a widespread impact on an organization or agency that supports the public, due to an “immediate” loss of physical facility assets, application servers, network infrastructures and more.

Pandemic

A pandemic is an infection that causes a global outbreak of serious illness that rapidly spreads from person to person. This type of outbreak normally occurs when a new virus emerges for which people have little or no immunity, and for which there is no vaccine available. Some examples of flu outbreaks that have had a global impact include the 1918 Spanish Flu, the 1957 Asian Flu, the 1968 Hong Kong Flu, and the 2009 H1N1 virus (swine flu) pandemic.

2009 H1N1 Flu (sometimes called “swine flu”) is a new influenza virus causing illness in people. This new virus was first detected in the United States in April 2009, and is spreading from person to person worldwide, probably in much the same way as regular seasonal influenza viruses spread. On June 11, 2009, the World Health Organization (WHO) signaled that a pandemic of 2009 H1N1 flu was underway. As of November 1, 2009, more than 199 countries and overseas territories/communities have reported laboratory confirmed cases of pandemic influenza H1N1 2009.

Avian Influenza is an infection caused by avian (bird) influenza (flu) viruses. While these influenza viruses occur naturally among wild birds with no effect, they are very contagious and can make domesticated birds like chickens, ducks, and turkeys very sick, even kill them. Although the term Avian influenza virus usually refers to Influenza A viruses found chiefly in birds, infections with these viruses can also occur in humans. Normally these viruses do not infect

humans, but Influenza A viruses are constantly changing, and there are cases where Avian Influenza A (H5N1) has affected humans in parts of Asia and Africa. Currently, there is no direct evidence that the H5N1 strain has mutated to a form that is easily transmissible between humans; however, once that occurs, it is anticipated that spread of the disease will be rapid with the high potential of creating a global pandemic.

Severe Acute Respiratory Syndrome (SARS) is a viral respiratory illness caused by a coronavirus, called SARS-associated coronavirus (SARS-CoV). SARS was first reported in Asia in February 2003 and over the next few months, the illness spread to more than two dozen countries in North America, South America, Europe, and Asia, before the SARS global outbreak was contained. SARS seems to spread mainly with close person-to-person contact. In May 2005, the disease itself was declared “eradicated” by the World Health Organization (WHO), becoming the second disease in mankind to receive this label (the other was smallpox).

Natural Disasters

Another type of emergency situation that can have a catastrophic impact on normal business operations is a natural disaster. These extreme displays of nature can occur quickly and without warning. As such, the best path of preparation for such natural occurrences is proactive continuity planning.

Italy Earthquake (April 2009): A powerful earthquake struck central Italy on the morning of April 6, 2009, killing 294 people and making tens of thousands homeless. Some 65,000 people were displaced by the 6.3 magnitude quake, which hit the mountainous Abruzzo region in the early hours, catching residents in their sleep.

Hurricane Katrina (August 2005): Hurricane Katrina was one of the strongest storms to impact the coast of the United States during the last 100 years. With sustained winds during landfall of 125 mph, Katrina caused widespread devastation along the central Gulf Coast. Cities like New Orleans, Louisiana, Mobile, Alabama, and Gulfport, Mississippi bore the brunt of Katrina’s force and are still undergoing recovery efforts to return to normalcy.

North American Blizzard of 1978 (February 5-8, 1978): The blizzard of 1978 was a severe Nor’easter that affected the New England area of the United States, and to a lesser but still significant extent the New York metropolitan area. Connecticut, Rhode Island, and Massachusetts were particularly hard hit by this storm with up to 55 inches of snow falling in some areas. With the snowfall starting primarily during the morning of the 6th, many people were stranded in their cars along roads and highways throughout the New England region. Over 3,500 cars were found abandoned and buried in the middle of the roads during the cleanup effort. While many people had been caught in the storm while driving, most others were trapped in their homes or offices with snow drifts of up to 15 feet. It took almost a week to clear the main roads as buried cars and trucks needed to be removed before the roads could be cleared, and many side streets were not cleared until the snow melted months later.

Other

The final category of emergency situations can occur when extremist groups or organized unions perform acts unexpectedly that have far reaching effects on a government organization’s or agency’s ability to continue its daily functions.

Terrorist Attacks: At 8:46 a.m. on the morning of September 11, 2001, an event occurred that changed America forever. Four airliners carrying thousands of gallons of jet fuel plowed into the Twin Towers of the World Trade Center in Lower Manhattan, into the western face of the Pentagon, and crashed in a field in southern Pennsylvania. More than 2,600 people died at the World Trade Center, 125 died at the Pentagon, and 256 died on the four planes. The death toll surpassed that at Pearl Harbor in December 1941.

MTA Strike in NYC (December 2005): The 2005 New York City transit strike was a strike called by Transport Workers Union Local 100 (TWU). When the strike started at 3:00 a.m. EST on December 20, 2005, most of the New York City Transit Authority personnel participated in the strike, halting all service on subways and buses. Over 8.1 million city residents and nearly one million suburban commuters were affected. The strike finally ended at 2:35 p.m. EST on December 22, 2005. Estimated losses to the local economy were around \$400 million per day, in addition to a loss of \$22 million a day in tax revenue and overtime police expenditures.

All of the disasters and alerts discussed previously present unique challenges and implications for business continuity planning. In addition to impacts on buildings and infrastructure, the loss of a large and random element of the workforce can be expected for a sustained period of time. This physical isolation of personnel can be attributed to either a pandemic outbreak or to mobility impacts such as local transportation restrictions, airline travel restrictions, and in some cases a government imposed restriction. A remote access plan becomes a critical component of the overall business continuity plan for supporting employees who have to work remotely, and the applications to which they may need access.

Continuity Planning—Proactively Being Prepared

A key component for helping government agencies plan for potential emergencies is taking continuity planning seriously and adopting a proactive approach. Planning for a range of scenarios ahead of time with clear processes and responsibilities is essential to ensuring that the needs of citizens will be met. Once disaster strikes, an organization's ability to respond quickly and effectively may be critical in protecting its staff, citizens, and reputation. While many businesses have business continuity plans to deal with disruptions, in today's world it is imperative that these plans be expanded for local, regional, or global situations. It becomes a cross-organizational planning effort to develop a plan that protects the health and safety of employees and the public, and ensures that critical business functions remain operational. The following stages outline a simple yet comprehensive approach for building a successful continuity plan.

Steering Committee—Continuity planning begins with the establishment of a steering committee. The role of this committee is critical, as its members are responsible for identifying the key functions and activities that will have the highest priority, both during and after a disaster. They are also responsible for setting up an order of succession and delegation of authority to ensure that there will not be a breakdown in continuity of business critical activities.

Planning Stage—The planning component of a continuity plan involves the evaluation, selection, and installation of (1) an emergency communications system that can handle the needs of remote “emergency” workers, and (2) an alternate facility for critical servers and systems. This component also includes setting up a plan for protection and availability of vital records during any disaster.

Execution Stage—The next part of a continuity plan is formation of an execution team that will test the emergency communications systems and the cutover from a primary to an alternate facility.

Ongoing Testing, Training, and Review—Following all of these steps, it is important to have ongoing testing, training, and review of the continuity plan to insure that the plan works, all personnel stay trained in proper procedures, and the plan keeps up with new directives and technology advances.

Business Continuity Challenges

Planning for a disruption to business services from typical network outages and server crashes is a full-time job by itself. When preparing contingency plans for a major disaster or emergency, the planning effort is magnified tenfold, and network managers are presented with unique challenges.

- 1. Maintaining Productivity by Enabling Access to Applications and Information from Anywhere at Any Time and on Any Device.** Security threats from today's global Internet community are constantly challenging companies and organizations. Added to these challenges are environmental threats of pandemic or catastrophic events that can bring a business to a halt. Business continuity relies on a company having the ability to maintain its productivity, services, and partnerships in the event of a disaster or pandemic. Pandemics, like the H1N1 virus, can impact a business by requiring a company to limit social interaction between employees, partners, and customers to isolate further spread of the virus. This makes a compelling case for the wider adoption of remote access, as employees are quarantined or required to work from home for an extended period of time.
- 2. Sustaining Partnerships with Real-Time Access to Applications and Services While Knowing that Your Resources Are Secured and Protected.** In the early 1990s, there were only limited options to extend the availability of the enterprise network beyond the boundaries of the corporate central site. These options consisted mainly of extremely costly and inflexible private networks and leased lines. However, as the Internet grew, it spawned the concept of VPNs as an alternative. Most of these VPN solutions leveraged free/public long-haul IP transport services and the IPsec protocol. VPNs effectively addressed the requirements for cost-effective, fixed, site-to-site network connectivity; however, they were, in many ways, still too expensive for mobile users, while for business partners

or customers, they were extremely difficult to deploy. It is in this environment that SSL VPNs were introduced, providing remote/mobile users, business partners, and customers an easy, secure way of accessing corporate resources through the Internet without the need to pre-install a client.

3. **Continuing to Deliver Exceptional Service to Customers and Partners with Online Collaboration.** If a pandemic disaster forces social distance between people, multiple means of conferencing will be required to help facilitate collaboration. Employees and partners will be looking for real-time applications that will help them function as if they were sitting in their offices. In addition, help desk staff and customer service representatives will need to provide remote assistance to users and customers by remotely controlling their PCs without requiring the user to install any software.
4. **Meeting Government Mandates for Contingencies and COOP Compliance.** In preparation and response to the threat of H1N1 and influenza pandemics, the U.S. federal government has prepared an implementation plan for the National Strategy for Pandemic Influenza. The Implementation Plan provides clear direction to federal departments and agencies, state and local governments, communities and the private sector on the actions that must be taken to prepare for a possible pandemic, including contingencies and Continuity of Operations (COOP) planning. Each agency is responsible for ensuring, in the context of contingencies and COOP situations, the continued availability of its mission essential and national security/emergency preparedness telecommunications services.
5. **Balancing Risk and Scalability with Cost and Ease of Deployment.** Network managers of government agencies and departments are constantly balancing between ease of deployment and high levels of security with their remote access solutions. These network managers are also faced with the challenge of preparing for possible disasters or epidemics, and the attendant remote users, with a cost-effective and scalable solution.

Secure Remote Access

As discussed earlier, remote access is a critical component of any business continuity plan. Remote or isolated emergency workers will need to continue their critical roles during times of emergency, and have secure and reliable access to an organization's key information databases and application servers.

Current Remote Access Issues

Although the benefits and importance of remote access are clear, government departments and agencies have experienced problems with providing remote access solutions that, until now, have typically been based on IPsec technology. IPsec solutions have resulted in end user frustration from only being able to access resources from a device with client software, and the high deployment and support costs associated with maintaining that software. 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 the government that is now beginning to change in earnest. 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.
- **Incomplete Security**—Client-based IPsec VPN cannot provide a widespread and 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.

SSL VPN

The term SSL VPN is used to refer to a new and fast-growing product category comprising a variety of technologies. Working backwards, the term "VPN" or virtual private network is the practice of using a public network like the Internet to transmit private data. Prior to 2001, most VPNs were based on some type of network layer transport such as IP Security (IPsec), or other methods like Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).

SSL VPNs use a different methodology to transport private data across the public Internet. Rather than forcing the end user to install and configure a complicated client on his or her system, SSL VPN uses SSL/HTTPS—available without additional software deployment on all standard Web browsers—as a secure transport mechanism. Rather than using the older IPsec network layer “tunnel” technology, SSL VPN connections happen via a Web connection at the application layer.

SSL VPN technology continues to advance with enhancements that allow a variety of access types for client/server applications and network layer connections that are still enabled via SSL. Another feature in SSL VPNs is the provisioning of additional endpoint security, where dynamic endpoint security checks can be done before a session is actually initiated as a means of ensuring that each endpoint is in compliance with corporate security policies.

Remote Access and SSL VPN

Part of the remote access problem across government agencies in general is the fact that many users and network managers are struggling to decide which technology should be deployed where. Where do IPsec VPNs and the newer SSL VPNs fit into network policies, and which problems can each technology best address? This question can be answered by looking at the usage scenarios themselves, as summarized in 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.

On the left side of Figure 1, we see a typical IPsec VPN, where administrators who need to achieve site-to-site connectivity for field and remote offices will be well served by IPsec VPN offerings. This technology was created to meet the challenge of how to provide employees around the world with secure “always on” connectivity that will enable them to access all of the corporate resources they need to achieve optimal productivity.

On the right side of Figure 1, we see a typical SSL VPN. Here, 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. SSL VPNs also allow administrators to change both the access methods and resources allowed as user circumstances change. SSL VPNs can also be configured to check endpoint security compliance to either provision resources accordingly or to provide the end user with the means to remediate.

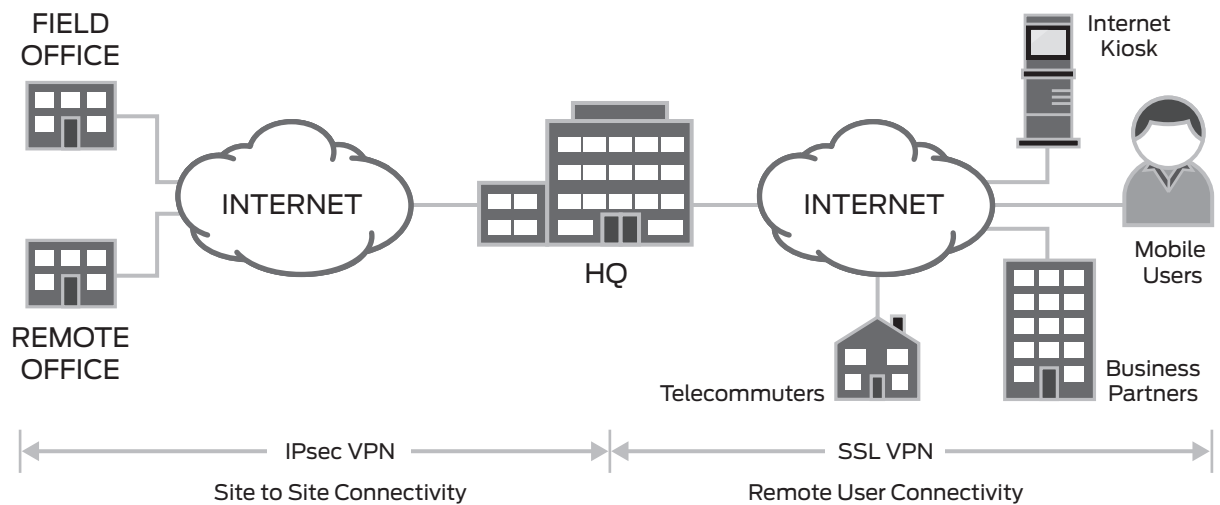


Figure 1: Remote access and SSL VPN

SA Series with ICE License

Juniper Networks SA Series SSL VPN Appliances lead the market with solutions that meet the needs of government organizations of every size. The world's IT leaders choose SA Series devices more than all other vendor solutions combined, thanks to the full featured flexibility that Juniper's systems provide. The SA Series appliances shown in Figure 2 include models sized to meet the needs of small departments with limited IT experience all the way up to high capacity systems for large government agencies requiring the utmost authentication, authorization, and accounting (AAA) capabilities.

The SA Series with In Case of Emergency (ICE) license helps government users and managers address the unique business continuity challenges covered earlier with a comprehensive and integrated solution.

Maintaining Productivity

To maintain productivity, the innovative technologies of SA Series appliances enable government workers to remain connected even in emergency situations, and they enable users to work from anywhere at any time using any device (unmanaged PCs, mobile phones, PDAs). The need for remote access capabilities in the event of a disaster can put a sudden strain on remote connectivity requirements, as more employees suddenly create a burst of demand. The ICE license delivers on that sudden peak in demand by providing the ability for a company to expand remote access connectivity within minutes and cost effectively (versus buying more user licenses).





Options/upgrades <ul style="list-style-type: none"> • 10-25 conc. users • Core Clientless Access • Network and Security Manager 	Options/upgrades <ul style="list-style-type: none"> • 25-100 conc. users • Secure Meeting • Cluster pairs • Enhanced Endpoint Security (EES) • NSM 	Options/upgrades <ul style="list-style-type: none"> • 50-1000 conc. users • Secure Meeting • Instant Virtual System • SSL acceleration • Cluster pairs • EES • NSM 	Options/upgrades <ul style="list-style-type: none"> • Up to 30K conc. users • Secure Meeting • IVS • 4-port SFP card • Second power supply or DC power supply • Multiunit clusters • EES • NSM
<p>SA700</p> 	<p>SA2500</p> 	<p>SA4500</p> 	<p>SA6500</p> 
Designed for: <ul style="list-style-type: none"> • SMEs • Secure remote access Includes: <ul style="list-style-type: none"> • Network Connect 	Designed for: <ul style="list-style-type: none"> • Medium enterprise • Secure remote, intranet and extranet access Includes: <ul style="list-style-type: none"> • Core Clientless Access • Secure Application Manager and Network Connect (SAMNC) 	Designed for: <ul style="list-style-type: none"> • Medium to large enterprise • Secure remote, intranet and extranet access Includes: <ul style="list-style-type: none"> • Core Clientless Access • SAMNC 	Designed for: <ul style="list-style-type: none"> • Large enterprises and service providers • Secure remote, intranet and extranet access Includes: <ul style="list-style-type: none"> • Core Clientless Access • SAMNC • SSL acceleration • Hot-swappable drives, fans

Figure 2: SA Series product family

Government employees can stay productive from anywhere, knowing that their corporate devices will make their connection to applications and resources seamless, as if they were physically in the office. The use of Secure Sockets Layer (SSL) protocol eliminates the need for client-side software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. With the best-in-class endpoint security features of the SA Series, IT organizations have peace of mind knowing that corporate resources will not be compromised. This is especially beneficial when users connect from locations like the home or public access terminals that are more vulnerable to network threats than the controlled, managed office LAN environment.

A key interesting technology beginning to get implemented is Virtual Desktop Infrastructure (VDI). VDI enables users to run personal computer instances (including applications, file access, and data) on a remote central server instead of on the hard drives of local PCs. Many organizations are beginning to consider VDI, because it will help them lower their administrative, support, and hardware costs associated with individual PCs. As VDI deployment begins to grow, organizations will need a solid, secure, remote access solution like SSL VPN that will allow seamless access for remote users to their virtual desktops. SSL VPN will enable employees to access their virtual desktops from any location and ultimately, keep them productive during normal times and during an emergency situation.

Sustaining Partnerships

SSL VPN technology is now seen as the best means to connect remote users, in addition to partners and customers. SA Series SSL VPN Appliances with ICE license provide the scalability and security required to ensure continued accessibility to partners in the event of a disaster, so that your agency can remain productive while sustaining important relationships.

The original design of the IPsec VPN protocol was to connect one private network to another, with the assumption that both networks were secure with the same security policies. However, network viruses and worms can propagate rapidly and widely through a geographically extended VPN. This is especially true when users are partners connecting from their office PCs and remote devices which are not a part of a company's controlled network.

SSL VPNs have more sophisticated controls for protecting the network. Unlike IPsec VPNs, SSL VPNs offer control at the user, application, and network level, with awareness of the security health status of connecting end nodes. For example, a connecting computer can be scanned to ensure that it meets corporate security requirements. Based on the knowledge of who the user is and which computer he or she is using, the SSL VPN can grant appropriate access rights and auditing at a granular level, showing the precise resources being accessed.

Meeting Federal and Government Mandates

The SA Series with ICE license aids all federal agencies, state and local governments, communities and enterprises in meeting the guidelines of various business continuity and COOP plans. The National Strategy for Pandemic Influenza plan includes establishing policies for preventing influenza spread at the workplace. And the plan specifically encourages enhancing communications and information technology infrastructure, as needed, to support employee telecommuting and remote customer access.

Certifications like Common Criteria and Federal Information Processing Standard (FIPS) 140-2 are required by many government customers worldwide. Juniper Networks' security certifications can give customers the assurance that their networking security products meet a standard set of security requirements. By meeting FIPS 140-2 and Common Criteria conformance, SA Series products are uniquely positioned to satisfy the most stringent certification requirements of government customers.

Providing Online Collaboration

The SA Series SSL VPN Appliances also provide online Web conferencing with the Secure Meeting capability. Web conferencing may be the only means for collaboration if a pandemic strikes, forcing social distance between people. Secure Meeting, which is included in the ICE license, provides secure anytime, anywhere, cost-effective online Web conferencing and remote control. It goes beyond the traditional communication methods of phone calls with real-time application sharing for employees, partners, and consultants using just a standard Web browser. Authorized employees and partners can easily schedule online meetings or activate instant meetings through an intuitive Web interface that requires no training or special deployments. This can prove to be extremely beneficial in the midst of a crisis or pandemic event. Help desk staff or customer service representatives can continue to provide remote assistance to all users and customers by remotely controlling their PCs without requiring the user to install any software. Customer service demands are sure to peak for any company during a catastrophic event, and those that are able to continue to provide exceptional service will be long remembered by their customers and the communities they serve

Balancing Risk and Scalability

SSL VPN is an easy to deploy and highly secure solution that has been purpose-built for secure remote access, and it should be at the top of the list for companies drawing up their “in case of emergency” IT plans. However, not all network managers can draw from their shrinking IT budget to purchase a large quantity of licenses for users who may never need emergency remote access. Juniper Networks SA Series SSL VPN Alliances with ICE licensing acts as a cost-effective insurance policy ready to provide immediate response during disasters. This licensing option provides a justifiable and scalable solution at a fraction of the cost of implementing a permanent solution which might not otherwise be used, providing a proactive and cost-effective defense against potential disaster or epidemic.

Survivable Remote Field Offices

Remote field offices are particularly susceptible to natural disasters and acts of terrorism. These sites typically have terrestrial fiber or copper WAN access connectivity. When redundant WAN access is provided to the remote field, this backup access is typically provided over terrestrial copper or fiber access as well. Frequently, the primary and backup WAN cabling travel a common path and enter the building at the same point of entry. This configuration makes both the primary and backup access susceptible to a common threat.

After Hurricane Katrina, traditional cable access was wet and useless for days if not months. It was cellular towers and wireless communications that were relied upon by first responders, and for some time thereafter, as a primary means of both voice and data communications. In examples of natural and man-made disasters, wireless communications have proven to be more resilient and heavily relied upon. Given that wireless communications do not follow a common path into remote field offices the way terrestrial WANs do, wireless can offer a very viable option to traditional WAN backup connectivity.

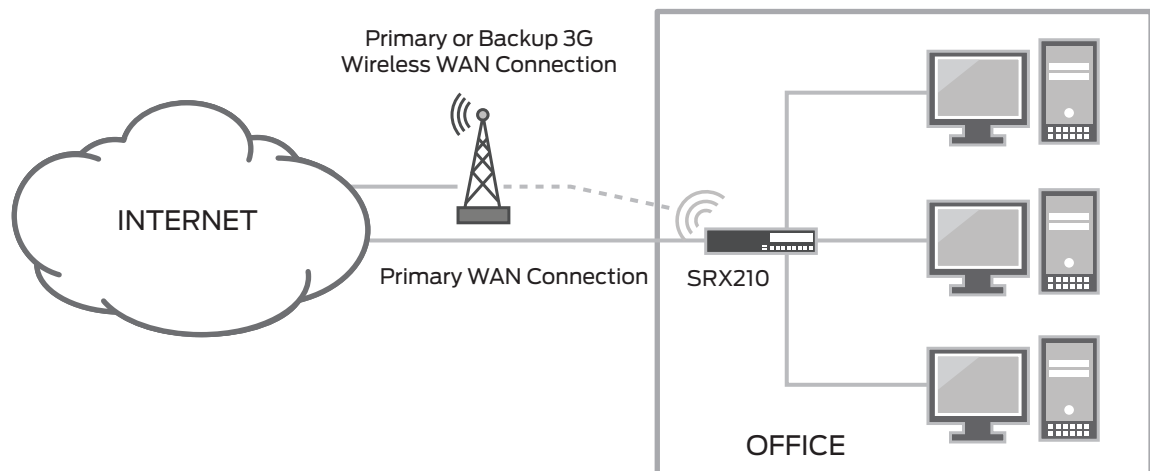


Figure 3: Wireless 3G connectivity can be configured as primary or backup WAN connection

Given the need and the opportunity to enable redundant and highly reliable WAN connectivity to the remote field office, Juniper has introduced a wireless third-generation (3G) connectivity option for its Juniper Networks SRX Series Services Gateways for the field. 3G data access can be configured as the primary WAN access or as a viable redundant backup option to primary terrestrial WAN access. Switching from primary to backup, terrestrial to wireless WAN access can be automated based upon the detection of a failure on the primary WAN access. Field SRX Series Services Gateways combine wireless 3G WAN connectivity with high-performance routing, stateful firewall, unified threat management (UTM) security capabilities, and switching.

When remote field office locations need to maintain connectivity in the event of a natural or man-made disaster, Juniper recommends that organizations consider WAN backup connectivity that includes options that are not susceptible to a single point of failure. Frequently, wireless is a very viable and cost-effective option for providing redundant WAN access. As a platform with integrated copper, and optical WAN connectivity with wireless 3G data WAN access, the SRX Series for the field is an ideal platform for this situation.

Additional Juniper Networks Solution Components

Once a government agency has implemented a secure remote access environment, it should then take the additional steps towards ensuring a coordinated threat control posture around its critical assets. 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 it is sometimes impossible to identify a user with intermediated traffic.

Coordinated Threat Control

Juniper's coordinated threat control provides a solution for overcoming the challenge of balancing extranet access that grants remote employees and partners full access to critical applications with a strong security posture around the enterprise's critical assets. Unlike many of the existing solutions in the market today, this 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 the IDP Series. This helps effectively identify, stop, and remediate both network and application-level threats within remote access traffic.

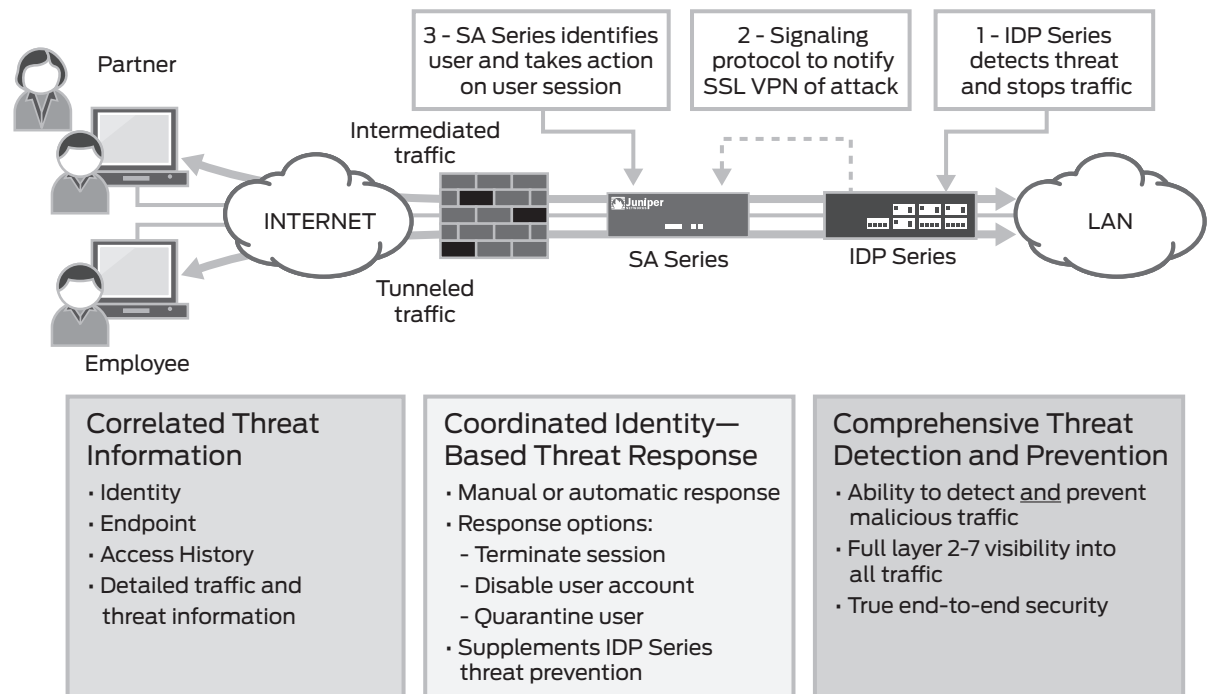


Figure 4: Juniper's coordinated threat control

With this technology, when the IDP Series appliance detects a threat or any traffic that breaks a rule that has been configured by an administrator, it signals the SA Series appliance. The SA Series appliance uses the information from the IDP Series to identify the user session that is the source of undesired traffic. Using 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 new functionality, the combined SA Series and IDP Series appliances allow 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 IDP Series technology is the ability to secure the entire local area network.

Juniper Networks Services

Juniper Networks Professional Services consultants and the experts of authorized Juniper Networks partners are recognized throughout the industry as highly knowledgeable networking specialists. They are uniquely qualified to assist you in planning and implementing a secure network. The Customer Support Center provides responsive assistance and software upgrades, security updates, and online knowledge tools to ensure the maximum reliability of Juniper Networks products. Professional instructors in Juniper Networks Education Services help customers keep pace with rapidly evolving technologies by sharing the company's expertise on operating stable, secure networks.

Conclusion

Government businesses can be prepared for emergency situations by taking a proactive approach to their business continuity planning. A comprehensive plan can provide a range of scenarios ahead of time, with clear processes and responsibilities defined in detail. A critical component of the overall business continuity plan is a secure remote access plan to ensure that remote or isolated workers can continue their work during and after a disaster strikes.

Juniper Networks SA Series SSL VPN Appliances and SRX Series Services Gateways for the field help to keep government agencies and departments functional by connecting people even during the most unpredictable circumstances—hurricanes, terrorist attacks, transportation strikes, pandemics, or virus outbreaks. With the right balance of risk and cost, the SA Series with the ICE license delivers a timely solution for addressing a dramatic peak in demand for remote access to ensure emergency services and business continuity, whenever an emergency strikes.

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.

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. 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.