Ensuring Business Continuity in Government
Juniper Networks Secure Access SSL/VPN Solution

Don Root
Solutions Marketing Manager
Tabel of Contents

Introduction.......................................................................................................................... 3
Continuity Planning............................................................................................................. 3
    What is Continuity Planning?......................................................................................... 3
    Examples of Recent Disasters and Alerts................................................................. 3
        Pandemic................................................................................................................... 3
        Natural Disasters..................................................................................................... 4
        Other......................................................................................................................... 5
    Continuity Planning – Proactively Being Prepared.................................................. 5
    Business Continuity Challenges.............................................................................. 6
Secure Remote Access..................................................................................................... 7
    Current Remote Access Issues.................................................................................. 7
    SSL VPN....................................................................................................................... 7
    Remote Access and SSL VPN..................................................................................... 8
The Juniper SSL/VPN ICE Solution............................................................................... 9
    Maintaining Productivity............................................................................................ 9
    Sustaining Partnerships............................................................................................. 10
    Meeting Federal and Government Mandates.......................................................... 10
    Providing Online Collaboration.............................................................................. 10
    Balancing Risk and Scalability............................................................................... 11
Additional Juniper Networks Solution Components..................................................... 11
    Coordinated Threat Control...................................................................................... 11
    Application Acceleration............................................................................................ 12
    Juniper Networks Services....................................................................................... 12
Conclusion.......................................................................................................................... 13
### Introduction

Today, more than ever, all sizes of government agencies and enterprise businesses are becoming dependent on a variety of applications and resources being used to access, store, and process critical information for business functions. Despite the importance of business continuity, business continuity planning was not a high priority at four of ten companies surveyed. An alarmingly larger number of companies were “assuming” their existing systems will be adequate for emergency situations. This lack of preparedness is not an option for government departments and agencies. This document will help you gain a better understanding and appreciation for continuity planning, the importance of ensuring you have a secure and reliable remote access component as part of that plan, and how to take a proactive approach using Juniper Networks Secure Access SSL VPN technology.

### Continuity Planning

#### 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, including the prevention of interruption to mission-critical services, 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 for continuity planning throughout the federal, state and local governments. The occurrence of these emergency situations, like hurricanes, earthquakes, blizzards and others, has the potential for causing a widespread impact to an organization or agency to support 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 which people have little or no immunity to, and where there is no vaccine available. Some examples of flu’s that had a global impact include the 1918 Spanish Flu, the 1957 Asian flu, and the more recent 1968 Hong Kong Flu.

**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 among birds and can make some domesticated birds, including chickens, ducks, and turkeys, very sick and kill them. Usually, the term avian influenza virus refers to Influenza A viruses found chiefly in birds, but infections with these viruses can 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 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 a high potential of creating a global pandemic. There is a National Strategy for Pandemic Influenza that provides a framework for future U.S. Government planning efforts that is consistent with The National Security Strategy and National Strategy for Homeland Security.

---

1. AT&T 5th Business Continuity Study – National Summary of Results, January – August 2005.
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. The main way SARS seemed to spread was by close person-to-person contact. The virus that causes SARS is thought to be transmitted most readily by respiratory droplets produced when an infected person coughs or sneezes. The virus can also be spread when a person touches a surface or object contaminated with the infectious droplets and then touches their mouth, nose, or eye(s). In May 2005 the disease itself was declared “eradicated” by the World Health Organization and it became the second disease in mankind to receive this label (the other was smallpox).

Natural Disasters
Another type of emergency situation that can cause 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.

Hurricane Katrina (August 05) – 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 (110 kts) (a strong category 3 hurricane on the Saffir-Simpson scale) and minimum central pressure the third lowest on record at landfall (920 mb), Katrina caused widespread devastation along the central Gulf Coast states of the US. Cities such as New Orleans, LA, Mobile, AL, and Gulfport, MS bore the brunt of Katrina’s force and are still undergoing recovery efforts to restore normality.

Pakistan Earthquake (October 05) – The Kashmir earthquake (also known as the South Asia earthquake or Pakistan earthquake) of 2005 was a major earthquake whose epicenter was the Pakistan-administered disputed region of Kashmir. The earthquake occurred at 08:50:38 Pakistan Standard Time (03:50:38 UTC, 09:20:38 Indian Standard Time) on October 8, 2005. It registered a minimum magnitude of 7.6 on the moment magnitude scale making it a major earthquake similar in intensity to the 1935 Quetta earthquake, the 2001 Gujarat Earthquake, and the 1906 San Francisco earthquake. As of 8 November, the Pakistani government’s official death toll was 73,276, while officials say nearly 1,400 people died in Indian-administered Kashmir and two people in Afghanistan. Some estimate that the death toll could reach over 100,000.

Hurricane Stan – SA (October 05) - Stan was only the second “s” storm to develop in history, the other being Sebastien during the 1995 Hurricane Season. Stan was a weak hurricane on the Saffir-Simpson Hurricane Scale, but nonetheless caused catastrophic damage and many deaths throughout Central America. Officially, Stan is responsible for 80 deaths in the Mexican states of Oaxaca, Veracruz, and Chiapas, however, Stan was embedded in a larger-scale surface circulation which dumped huge amounts of rainfall on portions of Central America. This caused massive flooding and catastrophic landslides that likely killed as many as 2000 individuals.

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 clean-up 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 or agencies ability to continue their daily functions.

Terrorist Attacks – At 8:46am on the morning of September 11, 2001, an event occurred that changed the outlook of all Americans in the United States 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 dies on the four planes. The death toll surpassed that at Pearl Harbor in December 1941\(^5\).

MTA Strike in NYC (December 05) – The 2005 New York City transit strike was a strike in New York City called by the 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 the subway and buses. Over 8.1 million city residents and nearly one million suburban commuters were affected. The strike finally ended at 2:35 pm EST on December 22, 2005. Estimated losses to the local economy were around $400 million per day as well as 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 to buildings and infrastructure, the loss of a large and random element of the work force 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 these remote employees and the applications to which they may need access.

### Continuity Planning – Proactively Being Prepared

A key component for helping government 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 critical in ensuring the needs of citizens are met. Once disaster strikes, an organizations 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 word it is imperative 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 with government agencies, 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** – The start of continuity planning begins with the establishment of a steering committee. The role of this committee is critical as they 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 insure there will not be a breakdown of continuity activities.

---

Planning Stage – The planning component of a continuity plan involves evaluating, selecting, 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 a turn-over 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 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, Anytime, and Any Device – Security threats from the global internet community of today are consistently challenging companies and organizations. Added to those 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 their productivity, services and partnerships in the event of a disaster or pandemic. Pandemics, like the Avian flu, can impact a business by requiring a company to limit social interaction between employees, partners and customers to isolate further spread of the virus, while making a compelling reason for the wider adoption of remote access, as employees are quarantined or recommended to work from home for an extended period of time.

2. Sustaining Partnerships with Real-Time Access to Applications and Services While Knowing Your Resources are Secured and Protected – In the early 1990s, there were only limited options to extend the availability of the enterprise’s network beyond the boundaries of the corporate central site, comprised mainly of extremely costly and inflexible private networks and leased lines. However, as the Internet grew, it spawned the concept of virtual private networks (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, for mobile users, they were, in many ways, still too expensive, 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 manner to access corporate resources through the internet and 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 or customer service representatives will need to provide remote assistance to any user or customer by remotely controlling their PC 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 Avian 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 which includes 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 highly secure solutions with their remote access solutions. Another large challenge for these network managers is preparing for the risk of a disaster or epidemic and the resulting thousands of remote users with a cost effective and scalable solution.

Secure Remote Access

As discussed earlier, a remote access plan is a critical component of an overall 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 into 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 resulting in end-user frustration and high deployment and support costs. 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 end point devices – both managed and unmanaged.
- **Expensive** – 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 Protocol (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 their system, SSL VPN uses SSL/HTTPS, which is 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 to allow a variety of access types for client/server applications and network-layer connections, which are still enabled via SSL. Another new feature in SSL VPNs includes 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 minimum corporate security policies.

**Remote Access and SSL VPN**

Part of the remote access problem across the government in general, is 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 their network policies, and which problems can each technology best address? This question can be best answered by looking at the usage scenarios themselves 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 – Administrators that need to achieve site-to-site connectivity for branch 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 that 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 anywhere and to change both the access methods and resources allowed as the users’ circumstances change. SSL VPNs can also be configured to check end-point security compliance and to either provision resources accordingly or to provide the end user with the means to remediate.

The use of SSL VPN is ideal for remote users because:

- SSL VPNs do not require a client download onto the device being used to access corporate resources
- SSL VPNs do not need to be configured by the end user
- SSL VPN is available wherever there is a standard Web browser, so users don’t need a company laptop
The Juniper SSL/VPN ICE Solution

Juniper Networks SSL VPN appliances lead the market with solutions that meet the needs of government organizations of every size. The world’s IT leaders choose Juniper Networks SSL VPN systems more than all other vendors combined thanks to the affordable, full-featured flexibility these solutions provide. The product family shown in Figure 2 - Juniper SSL VPN Product Family, includes 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 auditing (AAA) capabilities.

The Juniper Networks Secure Access SSL VPN ICE portfolio helps government users and managers to address the unique business continuity challenges covered earlier with a comprehensive and integrated solution.

Maintaining Productivity

To maintain productivity, the innovative technologies of Juniper Networks Secure Access SSL VPN products enable government workers to still remain connected and enable many to work from anywhere at anytime and with any device, including unmanaged PCs, mobile phones and 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. ICE delivers on that sudden peak in demand by providing the ability for a company to expand remote access connectivity in a cost effective manner.

Options/upgrades
- 10-25 conc. users
- Core Clientless Access

Options/upgrades
- 25-100 conc. users
- SAMNC
- Secure Meeting
- Advanced w/CM
- Cluster Pairs

Options/upgrades
- 50-1000 conc. users
- SAMNC
- Secure Meeting
- Advanced w/CM
- Instant Virtual System
- SSL Acceleration
- Cluster Pairs

Options/upgrades
- 100-2500 conc. users
- SAMNC
- Secure Meeting
- Advanced w/CM
- Instant Virtual System
- GBIC
- SSL Acceleration
- Multi-Unit Pairs

Figure 2 - Juniper SSL VPN 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 right in the office. The use of SSL eliminates the need for client-side software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. IT organizations have the peace of mind knowing that corporate resources will not be compromised with the best in class end point security features of Juniper Networks Secure Access SSL VPN. This is especially pertinent when users connect from locations such as the home or public access terminals which are more vulnerable to network threats than the controlled office LAN environment.
Sustaining Partnerships

SSL VPN technology is now seen as the best means to connect remote users, in addition to partners and customers. Junipers Secure Access SSL VPN ICE provides the scalability and continued security required to provide 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 both networks are secure with the same security policies. However, network viruses and worms can propagate rapidly and widely through a geographically extended VPN. This is especially pertinent 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 it meets corporate security requirements. Based on the knowledge of who the user is and which computer he/she is using, the SSL VPN can grant appropriate access rights and audit at a granular level, showing the precise resources accessed.

Meeting Federal and Government Mandates

Juniper Networks Secure Access ICE will aid all federal agencies, state and local governments, communities, and enterprises in meeting the guidelines of various business continuity plans and continuity of operations plans. The National Strategy for Pandemic Influenza plan includes establishing policies for preventing influenza spread at the workplace. And the plan specifically states enhancing communications and information technology infrastructure as needed to support employee telecommuting and remote customer access.

Certifications like Common Criteria and 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 obtaining FIPS 140-2 and Common Criteria conformance, Juniper Networks Secure Access SSL VPN products are uniquely positioned to satisfy the most stringent certification requirements of government customers.

Providing Online Collaboration

Juniper Networks Secure Access SSL VPN has the added capabilities to provide online Web conferencing with Secure Meeting. Web conferencing may be the only means for collaboration if a pandemic strikes forcing social distance between people. The Secure Meeting Option 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 with 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, which can prove to be extremely critical in the midst of a crisis or pandemic event. Help desk staff or customer service representatives can continue to provide remote assistance to any user or customer by remotely controlling their PC 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 purposely built for secure remote access and should be top of mind for companies drawing up their IT plans “in case of emergency”. However, not every network manager can draw from their shrinking IT budget to purchase a large quantity of licenses for remote users that may not even be used. Juniper Networks special Secure Access SSL VPN ICE licensing provides a cost-effective insurance policy for 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, in a proactive way against a potential disaster or epidemic.

Additional Juniper Networks Solution Components

Once a government agency has implemented a secure remote access environment, they should then take the additional steps towards insuring a coordinated threat control posture around their critical assets and how to best optimize the WAN connections used. The increased need for remote access for the extended enterprise of employees, partners, and customers must be balanced with steps to insure 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 Intrusion Prevention and Detection technologies, however just deploying IPS behind a 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 intermediated traffic.

Coordinated Threat Control

Juniper’s Coordinated Threat Control provides a solution for overcoming the challenge of balancing extranet access – for full access to remote employees and partners – to critical applications while maintaining 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 Juniper’s Secure Access SSL VPN and IDP Intrusion Detection Prevention appliances to tie the session identity of the SSL VPN with the threat detection capabilities of the IDP to effectively identify, stop, and remediate both network and application-level threats within remote access traffic.

---

**Correlated Threat Information**
- Identity
- Endpoint
- Access History
- Detailed traffic & threat information

**Coordinated Identity – Base Threat Response**
- Manual or automatic response
- Multiresponse options: Terminate, disable, or quarantine user
- Supplements IDP’s threat prevention

---

**Figure 3 – Juniper’s Coordinated Threat Control**
With this technology, when IDP detects a threat or any traffic that breaks an administrator-configured rule, it signals the Secure Access SSL VPN appliance. Secure Access uses the information from IDP to identify the user session that is the source of undesired traffic. Utilizing this information, Secure Access is able to take actions on the endpoint including: terminating the user session, disabling the user’s account or mapping the user into a quarantine role. With this new functionality, the combined Secure Access and IDP 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 by implementing the IDP component is its ability to secure the entire local area network.

**Application Acceleration**

Juniper Networks DX application acceleration platforms can reduce the time to access applications, dramatically boosting web application usability and acceptance – especially for remote and branch office users using the Secure Access SSL VPN products. The DX platforms optimize and compress all outgoing Web data in real time, without adding latency. DX application accelerators reduce bandwidth and offload processing from servers, yielding up to a 10x increase in server/application capacity. Internal firewall functionality delivers security, and full Layer 4-7 server load balancing is included. As in all Juniper Networks solutions, configurations for high availability and scalability are offered.

**Juniper Networks Services**

Juniper Network Professional Services consultants and the experts of authorized Juniper Networks partners are recognized throughout the industry as 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 maximum reliability of Juniper Networks products. Professional instructors of Juniper Networks Educational 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 will 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 remote or isolated emergency workers can continue their roles during and after a disaster strikes.

Juniper Networks Secure Access SSL VPN solutions 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 new Juniper Networks Secure Access ICE solution delivers a timely solution for addressing a dramatic peak in demand for remote access to ensure business continuity whenever an emergency strikes.