Datasheet

Juniper Networks SSL VPN Solution for Enabling Business Continuity with "In Case of Emergency" (ICE) Remote Access

Juniper Networks Secure Access SSL VPN ICE solution provides companies with a quick resolution when the unexpected happens, delivering the ability to handle extreme peak demands and to support the overall success of the business. ICE enables a company to continue business operations when disaster strikes, maintaining productivity, sustaining partnerships and delivering continued services to customers. ICE enables federal departments and agencies, state and local governments to meet compliance objectives for ensuring continuity of operations in the event of a disaster or pandemic event. Juniper Networks Secure Access ICE offers flexibility and scalability to help organizations effectively balance the costs and the risks inherent in preparing for and coping with "cases of emergency."

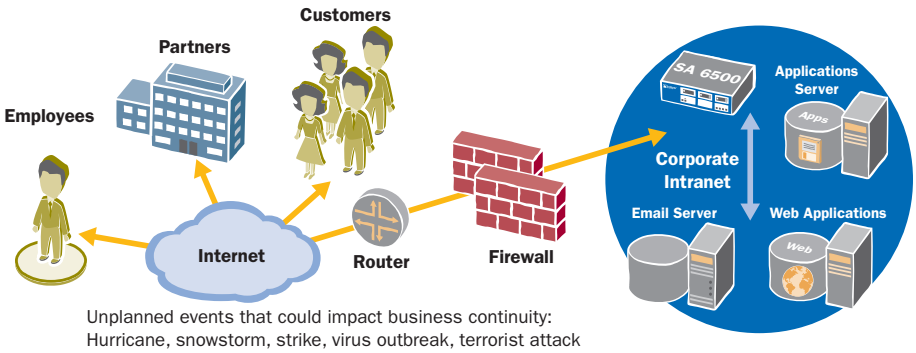
Product Description

SSL VPNs can help keep organizations and businesses functional by connecting people—even during the most unpredictable circumstances. When hurricanes, terrorist attacks, transportation strikes, pandemics, virus outbreaks or other potentially catastrophic events occur, they can result in the quarantine or isolation of entire regions or groups of people for an extended period of time. Effectively balancing risk and cost, the new Juniper Networks Secure Access ICE solution ensures business continuity by helping organizations instantly address a dramatic peak in demand for remote access in cases of emergency by using ICE licenses for a large number of additional users on a Secure Access SSL VPN appliance. ICE can be employed for a limited time to:

- Maintain productivity by rapidly enabling ubiquitous access to applications and information for employees from anywhere, at any time, and on any device
- Sustain partnerships with around-the-clock real-time access to applications and services while securing and protecting resources
- Continue to deliver exceptional service to customers and partners with online collaboration
- Meet federal and government mandates for contingencies and continuity of operations (COOP) compliance

Architecture and Key Components

As shown in the diagram below, the ICE license option enables companies to instantly accommodate spikes in remote access demand for various audiences during unplanned events. For example, employees who would typically come to the office can work from home or from any location, and they don't need to worry if they've left their laptops in the office. They can use any Web-enabled device such as their home PCs to access the network and stay productive. This minimizes downtime and also assures employees' safety by not requiring them to work at the office during emergencies. In addition, during these events, additional partners and customers can be granted access to ensure that business continues unimpeded.



Unplanned events that could impact business continuity:
Hurricane, snowstorm, strike, virus outbreak, terrorist attack

Figure 1. Business Continuity with ICE

Features and Benefits

Productivity with Ubiquitous, Any Time Access

Security threats from the global Internet community of today are continuously 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 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. This provides 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.

To maintain productivity, innovative technologies like SSL VPN help us to still remain connected and enable many to work from anywhere, at any time 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 whenever it is needed and in a cost-effective manner.

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 SSL eliminates the need for client-side software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. IT organizations have peace of mind knowing that corporate resources will not be compromised with the best-in-class endpoint 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.

Sustained Partnerships with Around-the-Clock Real-Time Access to Applications and Services

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. These mainly consisted 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, in many ways they were still too expensive for mobile users and 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 easy, secure access to corporate resources through the Internet—without the need to pre-install a client.

The original design of the IPSec VPN protocol was to connect one private network to another with the assumption that both networks were secure using 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 make sure that it meets corporate security requirements. Based on knowledge about 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. With all of these benefits, SSL VPN technology is being seen as the best means to connect remote users, in addition to partners and customers.

ICE provides the scalability and continued security required to provide continued accessibility to partners in the event of a disaster, so that your company can remain productive while sustaining important relationships.

Federal and Government Compliance for Contingencies and Continuity of Operations (COOP)

In preparation for 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. This 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.

The 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. Juniper Networks Secure Access ICE will aid all federal agencies, state and local governments, communities and enterprises in meeting the guidelines of this plan.

Exceptional Service to Customers and Partners with 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 and forces social distance between people. The Secure Meeting Option provides secure any time, 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 through the use of 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, and this 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.

Balanced Risk and Scalability with Cost and Ease of Deployment

As an easy to deploy and highly secure solution that is purpose-built for secure remote access, SSL VPN should be on the top of the list for companies drawing up their IT "in case of emergency" plans. ICE provides a cost-effective and scalable approach for mitigating the risk of a disaster or epidemic at a fraction of the cost of implementing a permanent solution which might not otherwise be used.

From a best practices perspective, Juniper Networks Secure Access ICE has all of the necessary features to enable testing before an unpredictable event occurs. For example, ICE can be activated and deactivated to test an SA appliance during emergency recovery drills. ICE also provides a seamless approach to automatically scaling a system should requirements change for deploying an increased number of remote users permanently, thereby providing investment protection.

Ordering Information

The ICE license for the SA4000, SA4000 FIPS, SA4500, SA6000, SA6000SP, SA6000 FIPS and SA6500 appliances include all of the following features:

- Baseline
- Secure Meeting

ICE provides licenses for a large number of additional users on a Secure Access SSL VPN appliance for four weeks, with an additional buffer of four weeks (for a total of up to eight weeks) for periodic testing and transitioning to permanent licenses, if necessary.

ICE licenses can be purchased for new SSL VPN appliances designated for business continuity requirements. Existing SSL VPN customers can also upgrade their SSL VPN appliances with ICE licenses.

ICE Part Number	Permanent License Equivalent
SA4500-ICE	SA4500-ADD-1000U SA4500-MTG
SA4500-ICE-CL	SA4500-CL-1000U
SA6500-ICE	SA6500-ADD-10000U and more (actual number depends on deployment) SA6500-MTG
SA6500-ICE-CL	SA6500-CL-10000U and more (actual number depends on deployment)

Note: Existing SA 4000, SA 4000 FIPS, SA 6000, SA 6000SP and SA 6000 FIPS customers must upgrade to version 6.1 software or higher before ordering the ICE SKUs above

Juniper Your 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.

Juniper® NETWORKS

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS FOR
NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

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

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

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

100171-004 June 2008

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