

Juniper Networks **Secure Access ICE**

The SSL VPN solution for enabling business continuity with remote access “In Case of Emergency” (ICE)

SSL VPNs can help to keep organizations and businesses functional by connecting people even during the most unpredictable circumstances – hurricanes, terrorist attacks, transportation strikes, pandemics or virus outbreaks. The result of which could result in the quarantine or isolation of entire regions or groups of people for an extended period of time. 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 a disastrous event strikes. ICE provides licenses for a large number of additional users on a Secure Access SSL VPN appliance for a limited time.

- Maintain productivity by enabling ubiquitous access to applications and information for employees from anywhere, anytime, and any device
- Sustain partnerships with around the clock real-time access to applications and services while knowing your resources are secured and protected
- 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
- Balance risk and scalability with cost and ease of deployment

Maintain productivity by enabling ubiquitous access to applications and information for employees 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.

To maintain productivity, the innovative technologies of today like SSL VPN enable us 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.

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.

Sustain 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, 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.

The original design of the IPSec VPN protocol was to connect one private network to another with the assumption of 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. With all 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.

Meet federal and government mandates for contingencies and continuity of operations (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.

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 the plan.

Continue to deliver 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 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.

Balance risk and scalability with cost and ease of deployment

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”. ICE provides a justifiable solution at a fraction of the cost of implementing a permanent solution which might not otherwise be used. The ICE solution provides a cost effective and scalable approach for balancing the risk of a disaster or epidemic.

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 the product during emergency recovery drills. ICE provides a seamless approach to also automatically scale a system should requirements change for deploying the increased number of remote users permanently, providing investment protection.

Summary

Juniper Networks Secure Access SSL VPN ICE provides companies with a quick resolution when the unexpected happens, with the ability to deliver on extreme peak demands and to support the overall success of the business. It enables a company to continue business operations by 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 event of a disaster or pandemic event. Juniper Networks Secure Access ICE offers the best in flexibility with a balance between risk and cost.

Ordering Information

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

- Baseline
- Advanced
- Secure Application Manager and Network Connect
- Secure Meeting
- SSL Acceleration

ICE provides licenses for a large number of additional users on a Secure Access SSL VPN appliance for 4 weeks, with an additional buffer of 4 weeks (for a total of up to 8 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
SA4000-ICE	SA4000-ADD-1000U
	SA4000-ADV
	SA4000-SAMNC
	SA4000-MTG
	SA4000-SSL
SA4000-ICE-CL	SA4000-CL-1000U
SA6000-ICE	SA6000-ADD-2500U and more (actual number depends on deployment)
	SA6000-ADV
	SA6000-SAMNC
	SA6000-MTG
SA6000-ICE-CL	SA6000-CL-2500U and more (actual number depends on deployment)



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

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.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)1372-385500
Fax: 44(0)1372-385501

Copyright 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.