

Meet federal and other governmental mandates for contingencies and continuity of operations (COOP) compliance

In preparation and response to the threat of Avian and other influenza pandemics, the U.S. federal government has prepared an implementation plan -- 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 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 the continued availability of its mission essential and national security/emergency preparedness telecommunications services. The plan includes establishing policies for preventing the spread of influenza at the workplace. And the plan specifically states the need for enhancing communications and information technology infrastructure to support employee telecommuting and remote customer access. Juniper Networks Secure Access ICE will significantly help agencies at all levels of government in meeting the guidelines of the plan.

Sustain vital communications with online meeting and collaboration capabilities

Juniper Networks Secure Access SSL VPN has added capabilities to provide online Web conferencing with Secure Meeting. Web conferencing may be the only means for collaboration if a pandemic strikes, preventing face-to-face contact between staff and citizens. The Secure Meeting option provides a cost effective and secure online Web conferencing tool that can be accessed and controlled remotely. It goes far beyond the communication methods of phone calls and emails by providing real-time application sharing to participants using a standard Web browser. Authorized employees can easily schedule online meetings or activate instant meetings through an intuitive Web interface that requires no training or special deployments. This resource could prove extremely critical in the midst of a crisis. Help desk staff or government service representatives could continue to provide 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 organization during a catastrophic event and those that are able to continue to communicate and provide exceptional service to their citizens will be maintain the confidence of the communities they serve.

Deploy an affordable continuance of operations solution

SSL VPN is easy to deploy and provides a highly secure solution for remote access. It should top the priority list as IT organizations make their "in case of emergency" plans. ICE provides the means to continue vital operations in the wake of an emergency. Importantly, it can be implemented at a fraction of the cost of 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 the product during emergency recovery drills. ICE also offers the ability to automatically scale a system should the number of remote users change.

Summary

Juniper Networks Secure Access SSL VPN ICE provides governments with a quick and cost effective resolution to ensure continuity of operations and services in the event of an emergency. It gives public agencies the ability to communicate with their citizens, thereby ensuring the safety of citizens and preserving the confidence of the community. It enables agencies to meet compliance mandates for ensuring continuity of operations in the event of a disaster. Overall, the Juniper Networks Secure Access ICE offers the most comprehensive solution for providing secure remote access.

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.