



VeriSign, Inc. (Nasdaq: VRSN) delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable, and secure. VeriSign is considered to be the leading provider of Managed Security Services (MSS) to Fortune 1000 companies.

Overview

Situation

As companies continue to enlist the Internet to expedite business processes, the incurred security risk grows in accordance. VeriSign provides a complete security program that includes around-the-clock management and monitoring, real-time security intelligence, global infrastructure, a staff of 24x7 security experts, and access to in-depth consulting expertise to keep pace with today's increasingly complex network security threats.

Solution

VeriSign provides the industry's leading Managed Security Service (MSS) based on Juniper's best in class FW/VPN and IDP solutions. VeriSign's security expertise enables Juniper's customers to deploy their security devices expeditiously.

Solution

VeriSign provides the industry's leading Managed Security Service (MSS) based on Juniper Network's FW/VPN and Intrusion Detection and Prevention (IDP) solutions. VeriSign's staff of security experts has been trained to monitor and manage Juniper's suite of world class security devices.

VeriSign's Managed Firewall Services (MFS) protect an organization's key information assets across networks, hosts, applications and databases. VeriSign's highly trained security experts become an extension of each customer's in-house IT staff, providing analysis, configuration, setup, alerts and 24x7 system management. The customized firewall services harness industry's best practices to ensure a high level of network access and information availability, integrity and privacy. Around-the-clock firewall monitoring generates immediate alerts and responses for service outages and security alerts associated with critical Internet access points.

VeriSign has the expertise to design and implement a corporate security architecture that includes proactive intrusion detection and prevention architecture ensuring the security of an organization's critical assets. While many organizations deploy firewalls as central gatekeepers to prevent unauthorized access, a firewall by itself is insufficient for complete protection of networks and servers. A layered defense provides the best result.

By intelligently placing intrusion detection and prevention sensors on a network, VeriSign's team of security experts can manage a customer's devices around-the-clock, monitoring for security violations or misuse that originates from inside or outside the network. VeriSign's Managed Intrusion Detection and Prevention Service (IDS) (IPS) enhances an organization's firewall protection. To prevent costly downtime and potential loss of revenue, IDS and IPS provide a comprehensive, real-time warning system that proactively identifies, isolates, and, in the case of IPS, blocks real security attacks.

VeriSign's Managed IDS offers 24x7 monitoring of all network traffic. The service acts as an alarm for an organization's network, setting off necessary alerts when a potential attack is recognized. These alerts, based on the specific customer requirements, are actively monitored and managed by VeriSign certified security engineers at the company's Security Operations Centers (SOC) and real security events are quickly identified and acted upon. All intrusion attempts, regardless of severity, are logged and well-defined customer notification and resolution procedures are executed for all security events.

VeriSign's Managed IPS offers 24x7 management and monitoring all network traffic. Creating and maintaining effective policies is the most challenging aspect of managing intrusion prevention technology. Given our extensive security experience and unmatched security intelligence, VeriSign is in a unique position to create a policy that is appropriate for the Customer's environment. During the initial tuning period, VeriSign will run policies in simulation mode and work closely with the Customer to determine which traffic should be blocked. After extensive tuning and customer approval, the active blocking mode is enabled. These policies are augmented as vendors release updates and new threats emerge. All intrusion attempts and device health status are logged and reported on VeriSign's customer information portal. Customers are notified of major security and health issues via phone, email or pager. In addition, VeriSign patches and upgrades all technology under management.

Key Features/Benefits

- Lower Total Cost
- 24X7 Management, Monitoring and Support
- Trained and Dedicated Professionals
- Powerful Event Correlation with TeraGuard™

Contact VeriSign
www.verisign.com

www.juniper.net



CORPORATE HEADQUARTERS
AND SERVICE 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
Technical Support: 408-745-9500

ASIA PACIFIC REGIONAL
SERVICE HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suites 2507-11, 25/F
Asia Pacific Finance Tower,
Citibank Plaza
Central, Hong Kong
Phone: +852-2332-3636
Fax: +852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SERVICE
HEADQUARTERS
Juniper Networks B.V.
Beech Avenue 3
1119 RA Schiphol Rijk
Amsterdam, The Netherlands
Phone: 31-20-712-5700
Fax: 31-20-712-5901

ADDITIONAL SERVICE
LOCATIONS
Herndon, VA, USA
Ogden, UT, USA
Westford, MA, USA
Beijing, China
Sydney, Australia

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-IL ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

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.

Part Number: 354004-001 Sept 2004