

# Juniper Networks NetScreen-SM 3000 Series



## Raise productivity with instant, secure meetings

- Provision real-time meetings on the fly
- Users need only a standard Web browser and Internet connection
- Intuitive user interface has no learning curve

## Eliminate security risks

- SSL/HTTPS transport security
- Proven network security via a hardened, purpose-built appliance
- Strong, group- and role-based authentication authorization policies

- Detailed, event-driven auditing
- System security based on the award-winning Instant Virtual Extranet platform

## Greatly reduce the total cost of cross-enterprise meetings

- Reduce the need for travel
- Eliminate recurring costs of hosted meeting services
- Infrastructure pricing without collaboration extranet deployments
- Demonstrable ROI in 3 months vs. traditional methods

### Enable instant, secure online meetings

As the extended enterprise becomes a reality, the need for cross-enterprise communication becomes increasingly essential. The Juniper Networks NetScreen-SM 3000 Series offers the industry's first secure meeting appliance, enabling enterprises to instantly and securely provision online meetings and user-to-user collaboration across enterprises without the security tradeoffs and costs of either hosted services or collaboration software. Built on the award-winning, field-proven Instant Virtual Extranet (IVE) platform, the NetScreen-SM 3000 Series appliances require no software installation or maintenance, no changes to internal servers, and virtually no ongoing maintenance. The NetScreen-SM 3000 Series supports cross-platform agents, and is directory and messaging-vendor independent. It leverages the existing network infrastructure for a solution that is truly plug-and-play. Most companies will see a return on investment in only three months versus traditional meeting solutions.

### Enterprise-class security

The traditional vendors or applications for providing online collaboration have defined security very narrowly to mean transport security. The NetScreen-SM 3000 Series ensures the transport security of data exchanged during meetings with SSL, but there are many other aspects of security that must be considered. Service-based solutions involve a third-party. Traditional Web conferencing and peer-to-peer (P2P) applications can create "dark networks" within the enterprise. Dark networks result from traditional conferencing services that encrypt application sessions apart from the corporate security infrastructure, leaving the IT administrator without visibility into application sharing events. By applying an infrastructure approach to user-to-user sessions, the Secure Meeting appliance enables enterprises to take greater control over authentication, authorization, and auditing (AAA) and prevents confidential information from leaving the network undetected or infected files from entering via P2P file sharing. Unauthorized disclosures and file transfers and the emerging threat of P2P worms make broad deployment of desktop collaboration clients and the use of hosted services for meetings a risky proposition. In addition, while hosted services offer travel cost savings, over face-to-face meetings, they still prove expensive due to the monthly recurring fee structure. Until now the only alternative to hosted services was

software-based collaboration extranet deployments, which were complex, costly, and can increase the enterprises public-facing risk because they often require custom integration for security features and increase the number of public-facing services that must be hardened against attack.

The NetScreen-SM 3000 Series eliminates these problems. The products are purpose-built, hardened security appliances, which also leverage enterprises' existing investments in a robust AAA infrastructure, including integration with leading enterprise authentication stores. Each collaboration event can be authorized against enterprise security policies. And, unlike service-based solutions and most custom deployments, the NetScreen-SM 3000 Series enables network security professionals to take control of online meetings and enforce group or role-based AAA policies. Network administrators can ensure strong authentication, implement access control to shared resources, provide logs for each collaboration event, or even monitor them in real-time, to guard against any suspicious activity.

### Cost-effective, cross-enterprise meetings

As the extended enterprise grows, face-to-face meetings are becoming increasingly impractical. Even when participants are within the same company, employees must often conduct meetings from remote locations. Hosted Web-conferencing services are cost-effective when compared to physical travel but are still exorbitantly expensive, particularly considering the recurring costs. The other extreme, deploying and supporting a dedicated Web-conferencing server farm or collaboration extranet, entails sizable deployment costs as well as ongoing maintenance.

Juniper changes this paradigm with the NetScreen-SM 3000 Series appliances. The hardened security appliances can be deployed in a public-facing DMZ in a matter of hours and facilitates secure, instant cross-enterprise meetings, including:

- Real-time collaborative team meetings
- Online briefings to press and analysts
- Virtual sales calls
- Technical support sessions
- Informal training for small groups

Because all online meetings are facilitated through a standard Web browser, the NetScreen-SM 3000 Series makes online meetings easier for meeting conductors and attendees, as well as for network administrators. And using NetScreen-SM 3000 Series management features such as event-based logging, the costs of meetings can be billed back to the internal departments, instead of relying on third-party service providers.

**Easy to deploy - and to use**

The more difficult, risky, and expensive it is for people to conduct cross-enterprise meetings, the less apt they are to collaborate. End-users don't need to be concerned with technical details such as what messaging system attendees use, how the attendee corporate network is configured, and what desktop software each attendee has installed, not to mention questions about directory stores and authentication methods. The NetScreen-SM 3000 Series requires no technical knowledge on the part of the meeting conductors and attendees and needs only a standard Web browser and Internet connection. The user interface is simple and intuitive. And the device itself is literally plug-and-play, with an average installation time of about an hour.

**Highly available, redundant architecture**

Enterprises demand increasing redundancy as they grow the volume of business transactions online. The NetScreen-SM 3000 Series is designed to support the enterprise need for high availability with cluster pairs. The cluster pairs can be deployed in an Active/Passive

configuration for protection in the unlikely event of a failure or in an Active/Active configuration to double aggregate throughput to meet abnormal usage patterns, such as burst traffic, and to provide seamless failover. The cluster pairs feature stateful peering, which synchronizes system-state, user profile-state, and session-state data, so there is no user downtime or loss of productivity.

**The complete solution**

NetScreen-SM 3000 Series appliances can be combined with NetScreen Secure Access appliances to secure Web-based or client-server project collaboration and document management applications. When deployed with Access Series products, Meeting Series appliances can secure online meetings as well as provide instant access to project portals and Web-based document management systems, providing a complete solution for real-time access and meetings in a single environment. The NetScreen-SM 3000 Series are built on the Instant Virtual Extranet platform. Appliances using IVE technology are currently installed in a variety of industries, including Fortune 1000, healthcare, finance, government, education, high technology and more, with one million users worldwide. The platform has been certified by leading third-party security authorities, including TruSecure. The Meeting Series combines the ubiquity and cost-effectiveness of SSL transport with enterprise AAA methodologies for a solution that provides unsurpassed, easily audited security.

**Specifications**

**Upgrade Options**

- Secure Application Manager Upgrade Option
- Network Connect Upgrade Option
- High Availability Clustering Options
- Secure Meeting Upgrade Option

**Technical Specifications**

**Chassis SA 3000 Series**

- Dimensions: 17.72"W x 1.74"H x 19"D (45.00cmW x 4.41cmH x 48.26cmD)
- Weight: 18.5lb 8.3916(kg) typical (unboxed)
- Material: 18 gauge (.048") cold-rolled steel
- Fans: 4 ball-bearing exhaust fans, plus 1 CPU blower

**Ports**

**Network**

- Two RJ-45 Ethernet
- 10/100 full or half-duplex (auto-negotiation)
- IEEE 802.3 compliant

**Console**

- One 9-pin serial console port

**Safety and Emissions Certification**

- Safety: CB to IEC 60950: 1999, 3rd edition; TUV GS mark to EN60950: 2000; TUV C-US to UL60950: 2000; CAN/CSA-C22.2 No 60950: 2000
- Emissions: FCC Class B, VCCI Class B, CE class B



**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 2004, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The following are trademarks of Juniper Networks, Inc.: ERX, ESP E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, JProtect, Jseries, JWeb, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M71, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-SGT, NetScreen-SXP, NetScreen-SXT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. 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.