

Juniper Networks

Secure Wireless Networks for Distributed Remote Sites

Introducing the Juniper Networks NetScreen-5GT Wireless

Ray Zeisz, Field Marketing Manager
Matt Keil, Product Marketing Manager
Jae Lee, Technical Marketing Manager



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200102-001 Mar 2005

Contents

Contents	2
Overview	3
Why Wireless?	3
Wireless Security Challenges	4
NetScreen-5GT Wireless	4
Wireless Security	5
Wireless Authentication	5
Wireless Data Privacy	6
Wireless Security Zones	6
Deployment Examples	7
Small Enterprise	7
Distributed Enterprise Remote Office	8
Wireless Radio Features	10
More about the NetScreen-5GT	10
Device Management	11
Web GUI and CLI	11
Centralized Policy Management	11
Conclusion	11

Overview

Wireless networking adoption is exploding. A January 2005 Infonetics survey of Wireless LAN Users¹ found that more than 60% of enterprises believe employees increase productivity when enabled with mobile computing. Wireless LAN mobility allows employees to carry their net-connected laptops to conference rooms and peers' offices, resulting in decisions being made quicker and based on more accurate data. Furthermore, with the increasing number of PDAs and mobile phones incorporating WiFi technology, demand for a wireless infrastructure will continue to increase. However, wireless networking deployment can be a challenge when faced with the realities of security. A wireless network with weak security can compromise an entire organization's security posture and create more problems than it solves.

The Juniper Networks NetScreen-5GT Wireless addresses this growing demand for secure wireless access, especially in small or remote offices where IT security staffing may be limited. Juniper Networks has listened to customers and partners, developing a product that meets their wireless LAN access and security needs while drawing on years of industry leadership in the network security market.

This paper examines the business drivers behind wireless LAN infrastructure deployments, the security concerns with wireless, and finally the specific features Juniper Networks NetScreen-5GT Wireless provides to solve these problems. The NetScreen-5GT Wireless is the latest integrated FW/VPN appliance targeted at the distributed remote office or small to medium business where integrated features and functionality are critical requirements due to limited budgets and IT staff.

Why Wireless?

The removal of wires from the communications and network access equation has obvious benefits. The most common reason for deploying a wireless network in the enterprise is increased employee productivity. In addition to information sharing, numerous new applications are enabled with wireless networks, such as on-line mobile patient/customer records, real-time inventory management, and public internet hotspots.

For employees who travel regularly, wireless access is a tool that represents significant productivity enhancement. The ability to access network resources easily at a hotel, a coffee shop, an airport lounge or the local office means less idle time while waiting to dial in or search out a broadband connection.

Secure wireless LAN access can also generate significant operational cost savings by greatly reducing or eliminating the IT administrative burden associated with employee Moves/Adds/Changes. It is widely accepted that the cost of deploying a LAN at a new office, for example, can be greatly reduced with WiFi technology compared to the cost of a purely Ethernet infrastructure. In environments where floor plans may change frequently, such as retail stores, the savings are even greater. Wireless LANs ease network deployment at new facilities since cables do not need to be run, a costly and time consuming task.

¹ Infonetics User Plans for Wireless LANS, October, 2004

Wireless Security Challenges

The same Infonetics survey that found increased productivity from wireless networks also found that more than half of enterprises felt that security was a barrier to implementation. However, that study also reported that enterprises believe the security barriers can be overcome with recent advances in available technology.

Authentication, or the prevention of unauthorized users from accessing the wireless network and ultimately the wired network to which it is connected, is equally as important as protecting data as it travels through the air. It has become a pastime for hackers to roam cities, war-driving, or looking for wireless access points that are vulnerable, either as a means of accessing a network for malicious activity or sadly just for the thrill. Authenticating users is just as important as protecting the privacy of the wirelessly delivered data.

Data privacy is the most common concern with any wireless technology. While there is clearly a need to protect data from unauthorized interception over the air, that is just one of many security concerns when deploying a wireless LAN.

Some employees feel that wireless is so valuable they may take matters into their own hands and purchase very inexpensive wireless access points and install them in their offices themselves. These *rogue access points* can severely reduce an organization's information security posture as well as create opportunity for network configuration problems which cause broadcast storms or other errors on the wired infrastructure. A much better solution is to offer company-supported wireless access which is secure and well-managed. The prices of WiFi adapters have dropped in recent years to the point that most new laptops are equipped with WiFi at time of manufacture. Giving an employee half of the wireless puzzle is a recipe for disaster.

Until now, there has not been an enterprise-class WLAN security solution for the remote site. To provide users with wireless access while reigning in rogue access point deployments, enterprises of all sizes are deploying SOHO-class wireless access points, in conjunction with existing security solutions, and attempting to manage them centrally. This is a daunting task that simply does not scale. While the wireless networking industry has made great strides in developing and implementing enterprise-grade wireless security, the majority of these technologies have been implemented in products built for the large or central office, as that has been where most enterprises have conducted early-stage WLAN trials. These central site WLAN devices have delivered wireless-specific security features without any traditional security mechanisms such as IPSec data encryption or even a trusted stateful firewall, thereby making a remote secure WLAN almost impossible to implement, and at best, very costly.

NetScreen-5GT Wireless

Juniper Networks has combined years of industry leadership in network security with state-of-the-art WiFi technologies to develop the Juniper Networks NetScreen-5GT Wireless, an integrated security appliance offering all the functionality of a traditional integrated firewall/VPN appliance with a secure wireless access point delivered in a compact form factor.



The NetScreen-5GT Wireless melds proven enterprise-grade security with 802.11b/g wireless access to provide a best-in-class wireless security solution for distributed remote sites. Unlike other solutions that merely slap an access point onto an existing firewall, the NetScreen-5GT Wireless includes several wireless-specific features that will provide customers with greater security and flexibility:

- Wireless Zones: these offer the ability to segment groups of wireless users and provision appropriate levels of network resource access.
- Broad set of wireless security: a wide range of wireless specific privacy and authentication mechanisms ensure WLAN access is protected, and maintain consistency and interoperability with other WLAN solutions.

Drawing upon the industry proven ScreenOS operating system, the NetScreen-5GT Wireless provides an exhaustive list of security features and protocols including a 75 Mbps Stateful firewall and 20 Mbps IPSec VPN, along with support for NAT, RIP, OSPF and BGP4. To help protect against network level attacks, application level attacks and viruses, the NetScreen-5GT Wireless includes integrated Stateful and Deep Inspection Firewall and Antivirus capabilities.

The NetScreen-5GT Wireless is also available with an integrated ADSL modem for applications where an ADSL broadband connection is used as the WAN access method. All models of the NetScreen-5GT also include a serial interface for connection to a modem for dial backup, in case of a WAN or broadband network disruption.

Wireless Security

The need for robust and comprehensive authentication is great with wireless networks. Since it is impractical to physically secure a wireless network, as can easily be done with a wired network, authentication plays a critical role in the security of WiFi networks. The deployment of IEEE 802.11 technology was hampered by security flaws in the original standard. Recently, significant work was completed to standardize new security mechanisms in the IEEE 802.11 standard. These new standards offer significant security, worthy of use in the enterprise and revenue generating networks.

Wireless Authentication

Authentication is critical to wireless LAN deployment since an unsecured wireless access point will expose not only enterprise wireless users, but also the wired infrastructure. An enterprise can be confident that users on the wireless network have been properly authorized to access specified resources by using newer, secured authentication techniques. In addition to the authorization mechanism already supported by ScreenOS such as Radius, RSA, SecureID, LDAP, and local, the NetScreen-5GT Wireless includes support for the following wireless-specific authentication mechanisms:

- Pre-Shared Key (PSK)
- MAC Address Access Control List
- EAP-PEAP
- EAP-TLS
- EAP-TTLS over 802.1X

Many corporations have already deployed limited WLAN capabilities at their headquarters or large sites. These limited deployments are currently using methods of authentication and privacy that, while older or less secure than the newer algorithms, still need to be supported. By offering a wide range of authentication and privacy options, Juniper Networks ensures enterprise-wide consistency in the WLAN security policies without making obsolete the existing investment in wireless infrastructure.

For larger enterprises, with multiple locations and employees that travel between locations, the NetScreen-5GT Wireless provides user-level authentication via support for the IEEE 802.1X-enabled RADIUS server at the enterprise headquarters. This provides central control of wireless network access, or as we will show in an example below, access to a particular segment of the network.

For smaller offices and in applications where the users do not roam between office locations, a local database may be maintained on the NetScreen-5GT Wireless. This enables the smaller enterprise to have a high level of security without additional investment in a RADIUS infrastructure.

Wireless Data Privacy

For data privacy, encryption is used to protect messages from unauthorized viewing in case they are intercepted in the air. The NetScreen-5GT Wireless supports the following wireless confidentiality mechanisms:

- WEP
- WPA (AES or TKIP)
- IPSec (3DES or AES)

As with the older authentication protocols, some of the older encryption, or more precisely key exchange methods, are vulnerable to attack. Juniper Networks has included these older encryption methods for compatibility with previously installed wireless solutions.

Depending on specific needs, stages of implementation, and deployment scenarios, administrators may choose between minimal security of WEP-PSK, or maximize protection using a variant of WPA-TKIP or WPA-AES with IEEE 802.1X and both client side and server side certificates, where feasible. By supporting older security mechanisms the device allows older clients to be upgraded to these new protocols via a flexible migration. The NetScreen-5GT Wireless meets the WPA-Enterprise requirements as set by the Wi-Fi Alliance.

Wireless Security Zones

The NetScreen-5GT Wireless is built upon a **zone based architecture** that allows the physical interfaces, including the wireless access point, to be used in various configurations to build a security policy that fits the needs of any small office. In short, security zones allow the network administrator to separate users by physical or logical port. When traffic is required to cross a zone boundary, a security policy is enforced. Traffic within a zone may also have a security policy applied. Each zone-to-zone boundary may have a unique policy, meaning that a single NetScreen firewall can support numerous policies.

Wireless Security Zones (patent pending) on the NetScreen-5GT Wireless enable four Service Set Identifiers (SSIDs) to be simultaneously broadcast from a single device.² This powerful feature coupled with the security functions and management capabilities already developed for the existing NetScreen firewall product line sets the Juniper Networks NetScreen-5GT Wireless apart from every other remote site security appliance vendor's offering.

² In total, the device supports configuration data for up to 8 SSIDs in the local database.

With the NetScreen-5GT Wireless, each of the SSIDs available in the device is associated with a zone which correlates to a level of trust. SSIDs can be assigned different security levels by selecting mapping them to the various fixed port modes available in the device. For example, one wireless zone may require no authentication and would be associated with the “Wireless1” zone. While a second wireless zone could require the strong authentication of EAP-TTLS over 802.1X, and would be associated with the “Wireless2 or the trust zone”. This same concept can be applied to the data privacy method used on a per wireless zone basis too. In fact over 50 different security features can be individually enabled on a per wireless zone basis. These features include Antivirus, Deep Inspection, Denial of Service attack prevention, web filtering and more.

By segmenting wireless users in these zones, a security policy may be built for wirelessly attached users attempting to access resources within the office, while another policy can be used for users attempting to access resources on the Internet. By providing multiple SSIDs, each with varying levels of trust associated with them, complex security policies can be created which enable untrusted wireless users a restricted level of access to resources, while authenticated (thus more trusted) users may access more resources. No other remote site secure access point product provides this level of flexibility and security.

Deployment Examples

Let's examine some applications of how an enterprise can leverage the proven security of ScreenOS and Wireless Security Zones secure wireless technology to improve business operations.

Small Enterprise

In this example, a small office has a limited number of employees that work on a wired network. The office will occasionally be visited by a user with a wireless laptop or PDA. This configuration allows the enterprise to support clients with access back to their company's resources, without having to open their network to those users.



Figure 1. A simple “open” wireless office configuration.

This configuration would provide a single “open” wireless interface to anyone wishing to access the Internet. No external authentication servers are required and the SSID could be broadcast for easy configuration of laptops. A feature called **Client Isolation** can be enabled which prevents client-to-client communication through the firewall, thus protecting wireless devices from each other. Additionally, the local authentication mechanism (WebAuth), inherent in all ScreenOS-based products, could be enabled to prohibit unconstrained use of the Internet by requiring authentication prior to granting access. Using ScreenOS's NAT function, all clients share a common public IP address.

Distributed Enterprise Remote Office

This example expands on the previous; here we add the scale afforded by ScreenOS's proven manageability. A typical large enterprise may have hundreds or even thousands of offices. Examples might include retail stores, insurance agencies, coffee shops and even restaurants. These enterprises could benefit by supporting one or more of the following wireless deployment scenarios:

- Real-time mobile inventory tracking
- Offering public hotspots
- Gaming (for example trivia games at bars)
- At-table credit card processing
- In-store employee mobility with access to data
- Segmentation of users with varied levels of network access

This example shows how wireless networking could be supported at main site as well as remote site and that a consistent security policy can be maintained across the enterprise, even at the enterprises' remote sites. This can be done without sacrificing any existing security investments in time or equipment, while enabling a centrally managed, unified policy for the entire enterprise. In this example we will use four zones and four wireless interfaces or SSIDs. In turn, these SSIDs map to different trust levels and thus different zones. The requirements for this type of enterprise deployment include:

- Varied levels of user authentication; wired vs. wireless, employee vs. visitor
- Prevention of wired network access from outside users
- Administrator controlled policy for wireless-to-wireless user communication
- Management from headquarters
- Support all major wireless standards, including WPA with AES
- Include integrated firewall and IPSec VPN capability
- Providing mobility at remote sites without sacrificing existing security investments

Juniper Networks enables the enterprise to use policies to control access between zones, for varied authentication/privacy requirements, and to interoperate with existing client wireless solutions which may be in use at headquarters or other locations. By assigning different **trust levels** to each zone and associating wireless users to various zones, multiple levels of access or permission can be easily achieved.

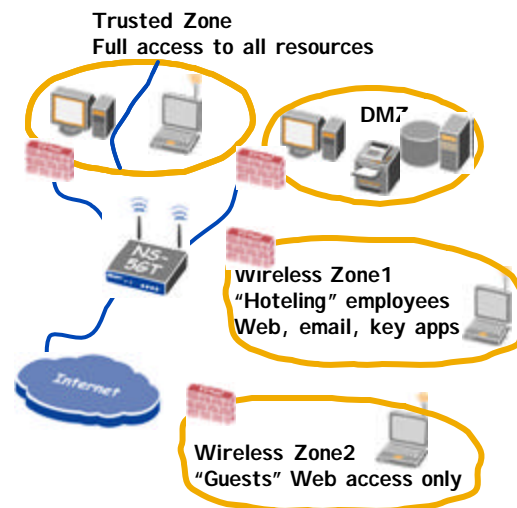


Figure 2. Wireless security for the distributed enterprise.

The trusted zone contains the Ethernet-attached computers as well as possibly point-of-sale terminals or stationary payment processing systems. One of the SSIDs maps to this trusted zone also, used for local employees using mobile devices. For a wireless user to gain access to this zone, they must use WPA with IEEE 802.1X authentication. In other words, they must authenticate securely, have a user ID and password on the system and use strong encryption for the data they send over the air.

A second zone, DMZ, contains a publicly accessible printer, server and desktop PC. A flexible security policy can be designed such that the DMZ is accessible from only select wireless SSIDs. This prevents attacks on the DMZ from the "open" wireless interface.

A third zone, Wireless1, might be used by visiting employees and vendors to access limited resources at the local facility, such as inventory data. This zone requires users to utilize WPA-PSK and affords them access to the DMZ and untrust or internet zone.

Finally, a fourth zone, Wireless2, is used for visitors or customers that have no reason to access any internal resources. These users might be using this wireless zone as a public internet hotspot for example. From this zone, which requires no authentication, users may only access the untrust zone.

For added protection the SSIDs are not broadcast for the trust, DMZ and Wireless1 zones; however, for Wireless2, the SSID is announced so that anyone may easily gain access to the Internet. Additionally, a second instance of a DHCP server could be configured for the Wireless1 zone, ensuring that Wireless1 and Wireless2 zones do not share any IP address similarities, further thwarting attack.

The availability of multiple zones and SSIDs, and specific security policies for inter-zone communication, provide numerous highly flexible security options for the security administrator. For example, the policy could be configured to enable Deep Inspection firewall on the Wireless1 zone, but not Wireless2. Other examples of how this technology can be applied include:

- Enabling the traveling employee access to corporate headquarters, but not to specific resources at a remote office. Email and other key corporate applications

are accessible to the wireless remote employee just as if they were in the headquarters.

- Protecting wireless hotspot users from each other. The ability to limit communication between wireless users means that hackers will not use your public hotspot to attack your customers.

These are just some of the ways in which our customers are using the power of wireless security zones to enhance productivity in a secure manner.

Wireless Radio Features

The NetScreen-5GT Wireless includes an industry-proven IEEE 802.11 b/g radio which operates in the unlicensed 2.4GHz frequency. The radio has its own processor, so wireless functionality, such as beacon control and AES encryption are accelerated, and do not impact the operation of the wired portion of the network in any way. Juniper Networks offers three antenna options with the NetScreen-5GT Wireless including:

- Standard antenna providing good coverage with smooth lobes
- External omni-directional antenna providing coverage at longer distances
- External Directional antenna which can be used to limit signal from straying from the premises and ensure excellent signal coverage in a limited area

The device also includes simple site survey information in the web-based user interface to ensure proper use of the RF spectrum.

More about the NetScreen-5GT

Introduced in 2003, the NetScreen-5GT is Juniper's most integrated security device and represents the right mix of integration for customers who need the benefits of layered protection in an optimal form factor. The NetScreen-5GT Wireless is an extension of the NetScreen-5GT Series which includes an Ethernet version and an ADSL version. It is a complete WLAN security solution ideal for distributed remote applications. With the NetScreen-5GT Wireless, a single device can provide all of these features:

- Encrypted wireless access with 802.1X authentication
- Deep Inspection Firewall
- Network Address Translation
- Full routing protocol support including RIP, OSPF, BGP4
- Embedded Antivirus
- Web Filtering with support for WebSense and/or SurfControl³
- Dial backup in case of WAN link failure
- Integrated ADSL modem (optional)

The Juniper Networks Deep Inspection firewall capabilities enable application layer protection for the most common internet protocols, in particular web, email, ftp, DNS, peer-to-peer, instant messaging and more. The Deep Inspection firewall capabilities are particularly useful in preventing the proliferation of network worms. Web filtering enables the security administrator to set policy to prevent employee access to objectionable, productivity-reducing or potentially malicious web sites. Integrated Antivirus ensures that remote computers are protected from email-based or web-based viruses, for example.

This level of integration extends security policy consistency across the distributed enterprise, while protecting existing investments in network infrastructure. This best-in-class all-in-one solution is ideal for the small business or the large distributed enterprise.

³ SurfControl support to be supported in an upcoming release.

No other vendor comes close to this level of integration, performance and time-tested and **proven** security.

Device Management

The NetScreen-5GT Wireless can be managed in a one of three different ways: Web GUI, Command Line Interface or centrally, via NetScreen-Security Manager.

Web GUI and CLI

The NetScreen-5GT Wireless is equipped with an intuitive and easy to use web interface as well as a flexible command line interface (CLI). Using either management mechanism, an administrator can control or monitor every aspect of the NetScreen-5GT Wireless, including security, routing, wireless LAN authentication and privacy, wireless radio and device status. Unlike solutions from other vendors which require multiple configuration utilities, Juniper Network's simplified management helps reduce the administrative burden and chances of incorrect configuration.

Centralized Policy Management⁴

For the large enterprise with numerous locations, the ability to centrally manage the remote locations is a key criterion. The NetScreen-5GT Wireless provides the same central management interface that all NetScreen firewalls have provided for years. NetScreen-Security Manger is a comprehensive and unified management platform, allowing administrators to manage all aspects of the product including security policy, network configuration and device status.

NetScreen-Security Manger also enables tasks to be limited to specific users, based on their roles. For example, the security officer may be given access to only the security policy while the network administrator may be given access to all configuration settings except security policy.

NetScreen-Security Manager and the NetScreen-5GT Wireless also support a rapid deployment capability where by the product may be installed by a typical employee, and no IT staff is required to be on-site for deployment.

Conclusion

Wireless networking, when deployed securely, is a valuable productivity enhancement at the remote office. The NetScreen-5GT Wireless enables employee mobility within the remote site, as well as between remote sites and headquarters, maintaining a consistent security policy throughout without increasing vulnerability.

Juniper Networks has significant experience securing the distributed enterprise, including large retailers. Now, that level of proven security is extended to the wireless realm. The unique solutions from Juniper Networks solve not only the wireless challenges, but the broader firewall VPN and virus issues seen at remote sites.

⁴ The NetScreen-5GT Wireless will be supported by NetScreen-Security Manager in an upcoming release.

In its January 2005 Firewall Magic Quadrant, the Gartner Group named Juniper Networks the industry leader in firewalls. The addition of secure wireless to the product line, coupled with unified and easy-to-understand central management, make the NetScreen-5GT Wireless the ideal choice for small offices, retail locations and distributed enterprise remote offices. Retail sites that are currently using IPSec VPNs, connected to a central office, can utilize this single device to provide all of the security functionality required at a store.

With the proliferation of wireless technology and the increasingly distributed nature of business with partners, vendors and extranets, security has never been more crucial to the success of a business. Many analysts believe that within a few years, all computers will include wireless technology at the factory.

Juniper Networks has moved wireless networking from a liability to an asset. Intelligently integrating the current and most stringent WLAN access technologies, Juniper Networks brings secure and assured wireless networking to the distributed enterprise remote sites and small offices with the NetScreen-5GT Wireless. Security should always be a concern, but it is no longer a barrier.

Copyright © 2005, 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, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, 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.