

End-to-End Security in Wireless LANs

Juniper Networks® and Trapeze Networks Deliver Secure Identity-Based Networking from Endpoint Devices to the Core of the Network

Challenge

To provide access to 802.11 clients and wired clients across your enterprise while ensuring their devices meet your company's security policies and are not introducing viruses and malware onto your network. Enforcement has to be seamless and secure.

Solution

A Trapeze Networks Smart Mobile wireless LAN integrated with a Juniper Networks Infranet Controller, UAC agents, and UAC Enforcement Points deliver a comprehensive identity-based, end-to-end secure wireless network. Companies can maintain the security and integrity of their entire network by using Juniper Networks Steel-belted RADIUS to provide authentication and authorization and using UAC to ensure endpoint integrity.

Benefits

Companies can simplify their security administration and enforcement by using one platform across wired and wireless networks. Unlike other wireless platforms that use third party components, like firewalls, the combined Juniper Networks UAC solution and Trapeze Networks Smart Mobile wireless LAN provide comprehensive, standards-based security.

In today's enterprises and institutions, wireless networks are transitioning from a network of convenience to becoming the network of choice. Historically, wireless users have been given limited access to a few corporate resources and Internet access. But as notebooks have become more powerful and wireless local area network (WLAN) performance has improved, users have required wireless access to more network resources and corporate applications. With the advent of the 802.11n standard for wireless networking, WLANs can provide up to 300 Mbps access for client devices. With the increase in available bandwidth and the ubiquitous availability of wireless devices, demand for access to corporate resources will only continue to grow. And as WLAN deployments increase network security and access control capabilities will need to keep pace. Trapeze Networks™ provides a broad array of security capabilities incorporated into its WLAN offering. Trapeze Networks' WLAN offerings leverage the capabilities of Juniper Networks Steel Belted Radius® family (SBR) and Juniper Networks Unified Access Control (UAC), extending best-in-class security solutions through the WLAN.

The Challenge

Many companies have been reluctant to adopt wireless networks because they believe that they are not secure enough to meet the security policies of their organization. Initially WLAN providers focused on securing access to the network by treating the wireless LAN like just another form of remote access. They implemented VPNs and provided encrypted communications between the client and the corporate network. But organizations quickly realized that once a device was on their wireless network, there was a greater risk that it could gain access to their core network. The industry responded to this challenge by introducing stronger authentication requirements restricting access to their WLANs. At the same time, IT administrators realized even though a client device had permission to access the network, that didn't necessarily mean that it didn't have viruses, Trojans, or other malware that could infect their network. It was becoming increasingly common for employees, contractors and guests to access the organization's network and unwittingly introduce malware to the network. IT and security administrators clearly needed a solution that could authenticate users and their devices, check both trusted and unknown endpoint devices for compliance to the organization's security policies, and isolate and prohibit unchecked systems from accessing the network, controlling access whether the user and/or device connected to the network through a wired port or over the WLAN.

The Juniper Networks UAC and Trapeze Smart Mobile Wireless LAN Solution

Trapeze Networks is a leading provider of enterprise wireless LAN equipment and management software. Trapeze solutions are optimized for industries whose companies require mobility and high bandwidth such as healthcare, education and hospitality. Trapeze delivers Smart Mobile™—providing scalable WLANs for applications such as Voice over Wi-Fi, location services and indoor/outdoor connectivity. Trapeze Networks Smart Mobile Wireless LANs provide comprehensive and robust identity-based security to ensure that only people with permission have access to your wireless network. Trapeze supports secure authentication and encryption to protect against misuse and eavesdropping, and to isolate traffic between multiple private groups. Distributed cryptography implemented in Trapeze Mobility Point access points ensures the scalability of security policies and network performance.

Trapeze Networks security ensures the integrity of the wireless LAN and allows only approved clients to access the LAN. But what happens once users are on the network? How do you prevent their clients from infecting your network applications and resources? Trapeze, through its support of Juniper Networks UAC, prevents misconfigured or infected devices from accessing the network by checking for the latest security patches and service packs, firewalls, antivirus software and anti-spyware. Trapeze Networks can ensure that each endpoint device which accesses the wireless LAN has been authenticated and inspected before being granted access to the network. If a client device is authenticated to the network but upon inspection is found to be a security risk, it is granted limited access to a quarantined segment of the corporate network to allow for automatic remediation, or to enable the network or IT administrator to correct the suspicious client device, to or deny it access.

Features and Benefits

Smart Mobile: The Only Traffic-Optimized WLAN Architecture

Smart Mobile from Trapeze Networks overcomes the limitations of current-generation WLANs with a breakthrough technology called “intelligent switching.” Smart Mobile’s intelligent switching combines both centralized and distributed data forwarding based on the requirements of the underlying application. This results in optimized traffic flow, radically reduced latency, and ultra high performance—all without the high cost of upgrading network controller infrastructure.

By supporting industry standards for encryption and authentication, the Trapeze Networks wireless LAN can be securely integrated into your existing networking infrastructure to provide:

- 802.1X based authentication—the most secure enterprise-level authentication protocol
- AES-CCMP encryption—the most robust encryption algorithm in the industry
- Wi-Fi Protected Access™ (WPA/WPA2)—the highest level of Wi-Fi security certification
- SmartPass™—the industry’s most robust and secure guest access control

RingMaster® software is a richly-featured, innovative, easy-to-use, full-lifecycle enterprise WLAN management suite that provides industry-leading Wi-Fi network management capabilities. RingMaster enables network managers to perform all critical functions necessary for planning, configuring, deploying, monitoring and optimizing their business Wi-Fi networks. RingMaster, unlike other planning tools, supports three-dimensional environments and incorporates indoor and outdoor management through one console.

Juniper Networks Unified Access Control delivers a comprehensive endpoint integrity and network access control that:

- Combines user identity, device security state and location information for session-specific access policy by user
- Leverages the existing network, including existing AAA infrastructure, any 802.1X-enabled switches, including Juniper Networks EX-series switches, and/or any Juniper firewalls
- Is based on industry standards - such as 802.1X, Extensible Authentication Protocols (EAP), RADIUS, IPSec, open standards and architectures - such as the Trusted Computing Group’s (TCG) Trusted Network Connect (TNC), and field-tested components - such as Juniper Networks Secure Access SSL VPN, Odyssey® Access Client (OAC), and Steel-Belted Radius®, which are used today in thousands of deployments worldwide

With UAC, policy enforcement can be enabled at Layer 2 using the 802.1X standards via any 802.1X-enabled access point or switch, such as the Trapeze Networks’ WLAN solutions or Juniper Networks EX-series Ethernet switches; or at Layer 3 using an overlay deployment with any Juniper Networks firewall platform. It can also be provisioned in mixed mode using 802.1X for network admission control and Layer 3 for resource access control. UAC also leverages the capabilities of Juniper Networks Intrusion Detection and Prevention (IDP) platforms to deliver broad application traffic visibility, isolating threats to the user or device level and employing an applicable policy action – via the Trapeze Networks’ WLAN solutions – against the offending user or device. It also correlates user identity and role information to network and application access, which better

addresses regulatory compliance. UAC extends access control to network traffic by implementing policy enforcement deeper into the network's core and outward to its edge, which mitigates risks and protects sensitive corporate assets. UAC reduces network threat exposure, delivers comprehensive control, visibility, and monitoring to surpass regulatory compliance, and decreases access control deployment cost and complexity, while delivering flexibility for phased deployments.

Solution Components

The Infranet Controller

The Juniper Networks Infranet Controller is the centralized security policy engine optimized for wireless and wired LAN access control. The Infranet Controller can push an agent down to the endpoint device, collect information about the device and its state from the agent, and act as an interface with existing enterprise AAA infrastructure. Once user credentials are validated and the device security state established, the Infranet Controller implements the appropriate access policy for each user/session, and pushes that policy to enforcement points throughout the network, including the Trapeze Networks' Mobile WLAN Solution. The Infranet Controller also features integrated RADIUS functionality from Juniper Networks SBR, the de facto standard in RADIUS servers and appliances. This enables the Infranet Controller to support an 802.1X transaction when an endpoint device enters the network, and provides a second method of user authentication and policy enforcement.

EX-Series Ethernet Switches

The EX-series Ethernet switches, running Juniper Networks powerful JUNOS™ software, deliver the operational simplicity, carrier-class reliability and integrated security that helps high-performance businesses accelerate the deployment of business-enabling applications and services across the extended enterprise. By leveraging JUNOS software, EX-series switches offer carrier-class continuous systems availability, automated network operations and a platform for open innovation that enables customers to quickly align the network with changing business requirements.

The UAC Agent

The UAC Agent is a dynamically downloaded agent that can be pre-installed and configured on endpoint devices, provisioned in real time by the Infranet Controller, installed using Juniper's Installer Service or deployed by other means. The UAC Agent collects user credentials and assesses the security state of the endpoint device. The UAC Agent can access the network at Layer 2 with 802.1X via integrated functionality from Juniper Networks Odyssey® Access Client (OAC), as well as at Layer 3. The UAC Agent includes an integrated personal firewall for dynamic client-side enforcement of policies, as well as specific functionality for Windows devices that includes IPSec VPN (to enable encryption from the endpoint to the firewall) and Single SignOn to Active Directory. The UAC Agent also includes Host Checker functionality, familiar from tens of thousands of Juniper Networks Secure Access SSL VPN deployments, which scans endpoint devices for a variety of security applications/states including, but not limited to, antivirus, malware and personal firewalls. UAC also enables custom checks of elements, such as registry and port status, and can do an MD5 checksum to verify application validity. Deployment is simplified by predefined Host Checker policies, as well as automatic monitoring of AV signature files for the latest definition files for posture assessment.

Access can also be provisioned in agent-less mode for circumstances where downloads of any software are impractical as in guest deployments. Access through agent-less mode still includes Host Checker endpoint device checks, guaranteeing the security state of all network users.

UAC Enforcement Points

Juniper has created an access control solution that is as functional with enforcement at Layer 2 as it is at Layers 3-7. For Layer 2 enforcement, UAC can work with any vendor's standards-compliant 802.1X-enabled wired switch - including Juniper Networks EX-series switches; or wireless switching infrastructure, such as Trapeze Networks' Mobile WLAN Solution. With UAC, Layer 3-7 enforcement is provided via any Juniper Networks firewall/VPN platform, including the Integrated Security

Gateways (ISG) with Intrusion Detection and Prevention (IDP) and the Secure Services Gateway (SSG) secure routing platforms. Juniper's wide range of firewalls as UAC enforcement points offers throughput ranging from 75Mbps to 30Gbps, while some firewalls also support unified threat management (UTM) capabilities, including network-based antivirus, anti-spam and URL filtering. All of these capabilities can be dynamically leveraged as part of the UAC solution, allowing not only the enforcement of access control policies but also the application of security policies such as deep packet inspection, antivirus and URL filtering on a per user/session basis. This enables the enterprise to unify the application of access and security policies for comprehensive network access and threat control.

Trapeze Networks Mobility Exchange Wireless LAN Controllers

The Trapeze Networks Mobility Exchange™ controllers, powered by Smart Mobile intelligent switching technology, enable seamless integration of scalable and secure wireless LANs with existing wired infrastructure. They support the IEEE 802.11i security specification and wireless intrusion detection and prevention application-aware switching, location tracking, voice and seamless indoor/outdoor mobility. Trapeze offers a broad range of MX controllers to meet the needs of any sized WLAN and to address the broadest range of deployments, from branch offices to corporate data centers.

Trapeze Networks Mobility Point Access Points

The Trapeze Mobility Point™ (MP™) family of multi-function 802.11 a/b/g/n access points provides access point, bridging, mesh access point, mesh portal, point-to-point and point-to-multipoint wireless services for Trapeze Smart Mobile™ wireless networks.

Smart Mobile is the only WLAN architecture with intelligent switching that combines both centralized and distributed data forwarding based on the requirements of the underlying application. Configured and controlled by Trapeze Mobility Exchange controllers, MPs perform encryption and can also enforce policy and forward data, depending on the application's needs. The result is optimized traffic flow, radically reduced latency and massive scalability.

RingMaster® Software

Trapeze Networks' award-winning WLAN management suite, enables full lifecycle management of Trapeze Smart Mobile wireless networks. RingMaster provides comprehensive 3D RF planning for indoor and outdoor coverage. RingMaster also provides best-in-class configuration, management and monitoring capabilities to deliver complete control of your wireless LAN

Summary—Trapeze and Juniper Deliver a Comprehensive Secure Wireless Network Solution

Security administrators recognize that it's not enough to control access to the network. You also have to ensure that those devices that are accessing the network are not introducing new problems. This challenge is exacerbated when your users' client PCs or guest PCs are used outside of work and are used to connect to other systems and networks, increasing the potential to introduce malware dramatically. Fortunately, Trapeze and Juniper address this problem. Your Trapeze wireless LAN with its support for the latest industry standards for security, coupled with your Juniper suite of enforcement and endpoint integrity solutions, will deliver comprehensive security solution for your corporate network.

Next Steps

For more information about the ways your company can benefit from Juniper Networks products, please visit http://www.juniper.net/products_and_services/unified_access_control/index.html. To learn more about Trapeze Networks solutions please visit www.trapezenetworks.com

About Trapeze Networks

Trapeze Networks delivers Smart Mobile—a ground-breaking approach to wireless networking, enabling organizations to deploy massively scalable mobile applications that leverage their existing infrastructure. Smart Mobile achieves this breakthrough by introducing intelligent switching, the first and only WLAN architecture that optimizes network traffic based on the underlying application. With Smart Mobile intelligent switching, organizations can support the most demanding next-generation wireless applications such as toll-quality voice over WLAN for thousands of users, seamless indoor/outdoor mobility, and high-speed networks based on 802.11n—all without requiring expensive forklift upgrades. Trapeze Networks is well capitalized, with strategic investments from networking industry leaders including Juniper Networks, Motorola and Nortel Networks. Founded in March 2002, Trapeze is headquartered in Pleasanton, California, with operations in Europe, Japan and Asia-Pacific. For more information, please visit www.trapezenetworks.com.

CORPORATE AND SALES HEADQUARTERS

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

APAC HEADQUARTERS

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA HEADQUARTERS

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. 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.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.



To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.