Creating Secure, Cost-Effective WLANs for the Enterprise

A White Paper

Vernier Networks, Inc.
465 National Avenue
Mountain View, California 94043
www.vernier.net

Introduction

WLANs offer enterprises great benefits, such as worker mobility and increased productivity, but they pose great risks, as well. Enterprises cannot afford to have their internal networks and daily operations jeopardized by the well-known shortcomings of WLAN security. Nor can they afford to tie up their network administrators with repetitive manual procedures, configuring and managing WLAN devices. Enterprises need a way to make WLANs secure and cost-effective at all stages of WLAN development: from the department-level pilot project to the enterprise-wide deployment across divisions and offices.

A Classic IT Dilemma: Centralization vs. Distribution

This problem of creating a secure, cost-effective WLAN raises a question familiar to every network architect: Which features should be centralized, and which should be distributed?

Deploying technology at the center of the network makes it accessible for administrators, but this convenience comes at the expense of fine-grained control at the network edge. For example, using VPNs to secure WLANs ensures that only authenticated users will access the network and that traffic will be encrypted with hacker-proof technology. But because users are tunneling straight from their computers to VPN terminators at the network core, there's no way for edge devices, such as access points, to offer any local services or enforce any local controls. Local controls might include allowing only members of a department to log in on the department's WLAN. Local services might include support for users roaming across subnets without having to continually log in and log out when crossing subnet boundaries. By over-centralizing WLAN security and management, VPNs force security policies to be general, rather than specific, and mobile services to be rudimentary.

On the other hand, putting security and management features at the edge of the network can make WLAN technology expensive to deploy and maintain and unwieldy to manage. Intelligent access points, for example, can enforce location-specific access policies; some even provide virus-filtering and other security features for wireless users. But this specialization comes at a price. Intelligent access points are more expensive than traditional access points, which are now available at commodity prices. Intelligent access points are often not compatible with generic network interface cards, which can limit the computing devices end users can use and force enterprises to deploy networking gear from a single vendor. With WLAN technology evolving so quickly, it's inevitable that enterprises will want to upgrade their networks

repeatedly in the coming years. But the prospect of upgrading tens or hundreds of intelligent access points is unappealing to both IT managers and financial managers, alike.

To resolve this dilemma, it's helpful to ask: **What data and technology is most likely to change frequently and require the intervention of administrators?**

User accounts, for example, change continually. The pool of employees at any organization is continually shifting as employees join or leave the organization or change roles. Partners and contractors may also require user accounts, which are likely to have limited privileges or special configurations. In any large organization, moves, adds, and changes have become a daily chore for system administrators.

Security is another thing that changes continually. As vendors and security experts respond to threats, they produce a seemingly never-ending stream of technology updates and security patches.

To reduce costs and to ensure that security updates are applied promptly, it's best to centralize network functions, such as authentication controls and security policies, that change continually.

What technology should be distributed, then? Technology that provides services for end users. These services should be based on centrally defined policies, but they should be flexible enough to account for local network conditions that may be changing in real time.

Monitoring and traffic management features belong at the network edge, so edge devices can support mobility and location-specific services and enforce location-specific controls.

Enterprises can adopt this guideline when deploying WLANs: **Put control at the center of the network, and intelligence at the network edge.**

VPNs centralize too much intelligence. They rob the network of fine-grained management functions where users are connecting to the network. Conversely, intelligent access points distribute too much control. They turn administrators into traveling technicians, forever moving from one device to another to ensure that access point and client device has the latest account information and security patch.

Enterprises need a third approach, an approach that combines centralization and distribution to create a secure, cost-effective solution for WLANs.

The Advantages of WLAN Gateways

A WLAN Gateway is a security and management device that is deployed at the wireless edge, just behind the access point. When deployed in a tiered configuration with a central control server, **WLAN Gateways provide the combination of centralization and distribution that enterprises need.**

The WLAN Gateway's central control server acts as an administration console for all the WLANs in the enterprise. The server integrates with central authentication systems, such as LDAP directories and RADIUS servers, so that all the WLANs in an enterprise can enforce the latest access rights for users and groups. The server also includes a policy engine, which enables administrators to refine WLAN access rights to take into account factors such as location and time. For example, an access policy might limit which users can access a particular subnet after 5 P.M. and on weekends.

Deployed in a distributed fashion across the network, WLAN Gateways enforce the user access rights and security policies stored in the control server. Each WLAN Gateway is deployed behind a collection of access points, as the next upstream networking device. The Gateway monitors and manages the traffic flowing through its access points, enforcing access rights on each of its network connections and performing network edge security functions such as packet-filtering.

Deployed between the network core and the network edge, WLAN Gateways can work together to increase network security and to improve network services. For example, if a hacker attempts to spoof an active address and login, WLAN Gateways can detect the duplication and thwart the attempt. They can also provide the intelligent coordination required to support mobile services, tunneling network connections from one Gateway to another as users move across subnets. Putting these features in WLAN Gateways enables enterprises to deploy inexpensive access points, which are available from a variety of vendors.

WLAN Gateways offer these benefits to enterprises:

- They enable enterprises to leverage their existing investments in authentication systems, switches, network cards, and access points. Enterprises do not have to duplicate or replace existing systems simply to support secure wireless networking.
- They lower operational costs by centralizing control of the WLAN. Policies can be defined and updated at a central console, rather than at hundreds of devices at remote locations.
- They make WLANs more secure, compensating for the security shortcomings of the 802.11 standard.
- They support advanced mobile services, such as roaming across subnets. By increasing user connectivity, WLAN Gateways increase user productivity and accelerate WLAN ROI.

Conclusion

Using just the right combination of centralized administration and distributed services, WLAN Gateways enable enterprises to create secure, cost-effective WLANs that are easy to deploy, easy to manage, and easy to scale.

About Vernier Networks

Founded in March 2001, Vernier Networks develops innovative systems and software to protect, manage, and enhance wireless networks. Vernier's intelligent, networking technology allows network managers to centralize wireless LAN usage policies, secure wireless network access at the edge, and deploy scalable wireless mobility across the enterprise. Vernier Networks has been honored with a 2003 Product of the Year Award from Network Magazine, Network Computing Editors' Choice Award, and Best of Show award at NetWorld+Interop. A privately held company, Vernier Networks is the first spinout company of Packet Design, LLC; a technology development company founded by entrepreneurs Judy Estrin and Bill Carrico. For more information, visit the Vernier Networks web site at: www.vernier.net or contact a Vernier representative at info@vernier.net