CONSENTRY NETWORKS

APPLICATION BRIEF

How ConSentry Augments Wireless LAN Security

Whether deploying a wireless LAN (WLAN) for the first time or expanding an existing one, IT faces a series of challenges. The promise of wireless is that employees, guests, and contractors will have network service no matter where they roam within an enterprise building or campus. But IT must ensure that security measures are met, and securing wireless connections should not require a different process than securing the rest of the LAN.

ConSentry Networks can greatly simplify IT's job in ensuring that wireless links into the corporate LAN are secure. ConSentry's LANShield platforms provide a set of services and management capabilities that address security concerns, allow for consistent access policies across both the wireless and wired infrastructures, and simplify the task of separating traffic by user group.

With ConSentry's robust solution, enterprises can use whatever wireless architecture fits their mobility needs and be assured of a high degree of security and traffic separation.

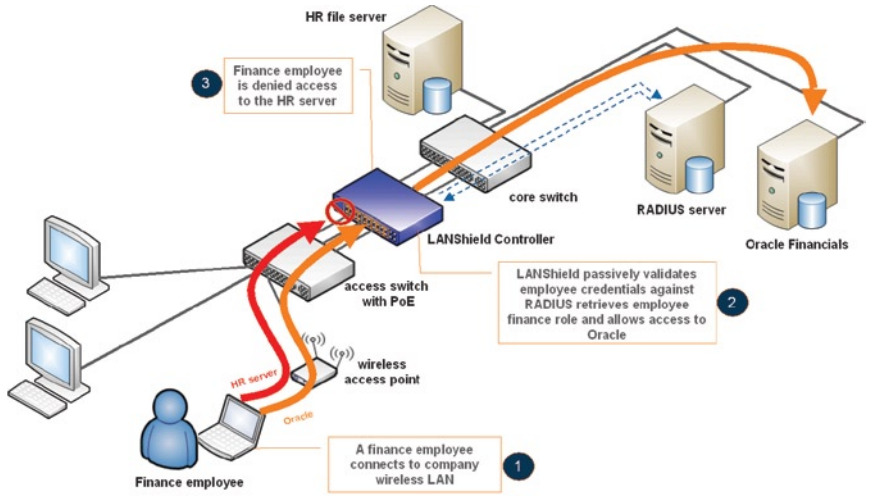
- One policy spans wired and wireless
- Authentication without the need for 802.1X
- User separation without relying on SSIDs or VLANs

Securing Who Gets on the Wireless LAN

IT must secure the WLAN, ensuring only authenticated users have access to corporate resources and, at a minimum, segmenting employee traffic from non-employee traffic. Many WLAN systems support 802.1X, providing user authentication. ConSentry's LANShield devices augment this authentication with traffic separation and access controls.

Specifically, the LANShield system passively observes authentication requests and responses between client machines and back-end identity stores, such as RADIUS. LANShield can also provide passive authentication by snooping a user's Active Directory login process. Only if the authentication or domain login is successful is a client given network access beyond essential services, such as access to DNS, DHCP, and authentication servers.

Secure Wired and Wireless Access



ConSentry enables role/user separation without relying on SSIDs or VLANs and authentication without the need for 802.1X.

The LANShield platforms also support active authentication, where the ConSentry device actively challenges a user for authentication information via a browser-based captive portal. This technique provides an easy authentication means that's not dependent on 802.1X, so enterprises can use simple access points (APs) with no 802.1X support and still enable authentication through the ConSentry platform.

Separating Users' Traffic — In the Air and on the Wire

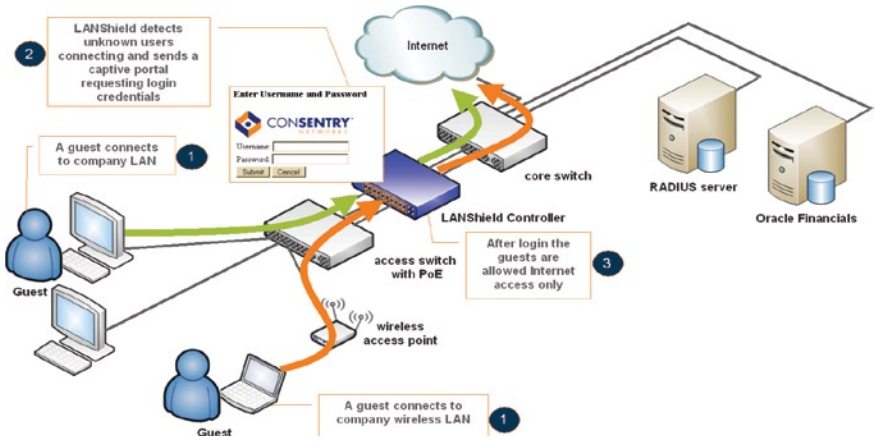
Many WLAN systems rely on service set identifiers (SSIDs) and virtual LANs (VLANs) to separate traffic. IT can choose from several combinations of these technologies to keep traffic from different users separate. One option is to define multiple SSIDs, each associated with a VLAN. For example, one SSID/VLAN would be established for guests and a second one for employees. IT could further subdivide employee traffic by configuring additional SSID/VLAN pairs.

Another option is to configure a single SSID and multiple VLANs, with users placed into a VLAN based on their authentication status. Guests, for example, wouldn't authenticate successfully, and so would be placed in the guest VLAN. Employees would be placed into VLANs based on a vendor-specific attribute (VSA) relayed as part of the authentication process.

Alternately, IT could establish a single SSID/VLAN for all users that allows for Internet access only. This architecture does not separate user traffic on the WLAN; rather, it requires employees to access corporate resources by launching a virtual private network (VPN) from the Internet back into the company.

In contrast, ConSentry makes it easy to keep user traffic separate – on both wireless and wired LANs. During authentication, the LANShield platforms learn each user's username, authentication status, and role by observing authentication traffic. Once the ConSentry device learns who the user is, it can tie all network activity back to specific users. This role-based provisioning allows IT to define policies that effectively separate user traffic, regardless of connection type.

Universal Guest Access Solution



ConSentry enables one security policy to span both wired and wireless.

ConSentry eliminates the need to use SSID/VLAN-based separation schemes, enabling IT to use just one system to implement traffic segmentation centrally, based on user roles — for both wired and wireless traffic. More importantly, it avoids the very cumbersome process of defining VLANs according to user role vs. retaining the geography-based VLANs as they typically exist in enterprises.

Unifying and Improving Security

In addition to simplifying segmentation, relying on the ConSentry platforms to separate users provides for a uniform security policy that spans wired and wireless connections. In many cases, IT endures a duplication of effort to configure security and other parameters on both the wired and wireless infrastructures. ConSentry eliminates that duplication.

ConSentry's LANShield platforms provide a comprehensive set of services, from network admission control and granular traffic visibility to user access control and threat control. Using ConSentry's InSight command center, IT can easily create, distribute, and administer role-based policies and perform incident response and other troubleshooting. And because the LANShield platform ties all WLAN and LAN activity to users, access controls are applied regardless of how they connect to the network. By delivering a robust set of centrally managed LAN services, ConSentry makes it possible for enterprises to augment the security of their wireless LANs. In addition, by serving both the wired and wireless infrastructures, ConSentry reduces operational overhead, improves overall LAN security, and ensures separation of users with a uniform, simple process.

CONSENTRY NETWORKS

Corporate Headquarters
ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035
Phone 408.956.2100 **Fax** 408.956.2199
Toll-Free 866.841.9100
www.consentry.com

Germany
ConSentry Networks
Lyoner Strasse 6 D-605 8
Frankfurt Germany
Phone +49 69 677 33 4
Fax +49 69 677 33 00

United Kingdom
ConSentry Networks
Lakeside House 1, Furzeground Way
Stockley Park, Heathrow, UB11 1BD
Phone +44 (0) 2086 22 3020
Fax +44 (0) 2086 22 3200

Japan
ConSentry Networks
Hibiya Central Bldg. 14F
1-2-9, Nishi Shinbashi, Minato-ku
Tokyo 105-0003 Japan
Phone +813-5532-7630
Fax +813-5532-7373