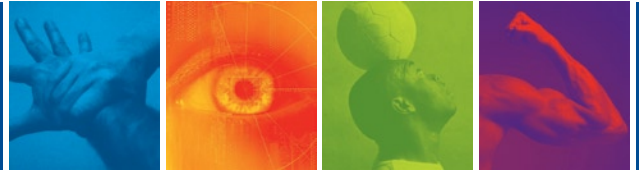


Securing Guest/Contractor Network Access



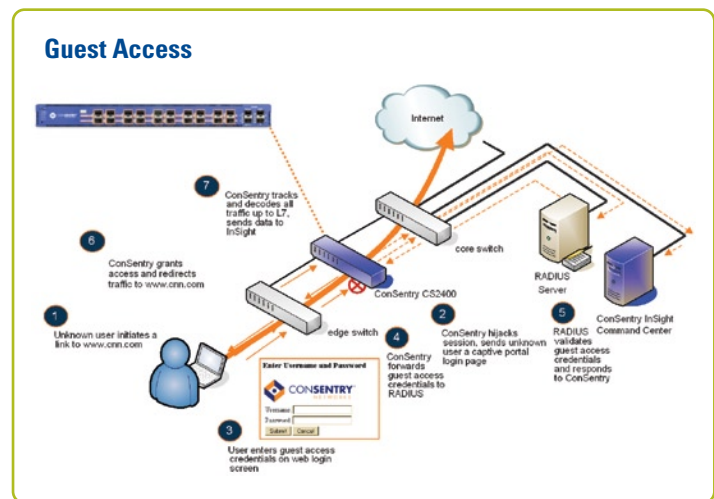
Whether visiting or working at a corporate site, guests and contractors want – and often need – access to an enterprise’s network. Wireless networks and open jacks in locations such as conference rooms make it easy for guests and contractors to physically access the LAN in the same way that employees do. Such free-range access poses security risks, however, prompting IT to look for ways to limit which “outside” users can get onto the LAN, where they can access it, and what resources and applications they can use.

To limit guests to Internet access while supporting appropriate privileges for contractors, IT needs an access solution that lets them easily create and distribute policies based on a user’s role. And such a solution must operate ubiquitously, regardless of where the user connects to the network. (For more on ConSentry’s policies and role-based provisioning, see “User Access Control: How ConSentry Networks Delivers Role-Based Provisioning.”)

How ConSentry Delivers Secure Guest/Contractor Access

An effective guest/contractor access solution must meet a range of requirements. ConSentry Networks delivers secure guest/contractor access as part of a set of LAN security services supported by its LANShield product family. The LANShield Controller deploys transparently upstream of LAN switches, and the LANShield Switch sits in the access layer directly hosting users and wireless access points. Both LANShield platforms observe all traffic and learn each user’s identity and role during authentication.

This comprehensive visibility is the basis for control and enforcement actions, which IT can easily define using the ConSentry InSight command center. InSight’s GUI and policy templates give IT the flexibility to limit where guests and contractors go on the network and what applications they can run, automatically restricting access for unauthenticated users. LANShield’s sophisticated combination of hardware and software addresses the spectrum of requirements for secure guest/contractor access, including:



- **Traffic separation and control.** An access solution must be able to identify and separate guest, contractor, and employee traffic on the LAN and appropriately limit what resources each category of user can reach. Once the LANShield platform has identified a user, it will limit that user to the network destination(s) and/or zone(s) that IT has specified as allowed for that user type. By controlling a user’s reach using Layer 3 addresses, ConSentry eliminates the need for IT to employ virtual LANs (VLANs) and access control lists to restrict user access, greatly simplifying guest/contractor access control and making it independent of the L2 infrastructure.
- **Control over application use.** An access solution must have the ability to limit which applications each category of user can use. With LANShield’s deep-packet inspection and policy-based controls, ConSentry enables IT to easily restrict which applications guests and contractors can use. For example, guests might be restricted to IPsec and HTTP or HTTPS, while all other applications (including risky applications such as peer-to-peer and IM) are denied.
- **Threat control.** An access solution must be able to identify and contain known as well as unknown threats, including zero-day attacks. ConSentry has developed application-specific anomaly detection algorithms that distinguish normal behavior from abnormal behavior for individual applications. With this capability, the LANShield platform can recognize both known and unknown threats and stop traffic on a per-user or per-application basis if malware is detected.
- **Universal access.** An access solution must apply the same set of controls to each user, regardless of how he or she accesses the network. The LANShield platform ties all LAN activity to users, so access controls are applied regardless of whether users access the LAN via a wired or wireless connection and whether they’re attached locally or remotely via a VPN.

- **Scans of unmanaged computers.** Since guest and contractor computers are not under an enterprise's control, an access solution must be capable of scanning unmanaged computers for malware and other requirements, such as OS version. ConSentry has teamed with Check Point Software Technologies to incorporate endpoint posture check into the LANShield platform, enabling it to issue a dissolvable agent to all end user machines as part of the admission process. A dissolvable agent can easily be applied to computers brought in by guests and contractors, enabling companies to prevent infected or non-compliant machines from accessing the LAN.

While guests generally require Internet access only, contractors need access to specific corporate resources. In addition, an enterprise may be employing contractors from multiple firms, necessitating more granular controls than guests. To accommodate these contractor-specific requirements, a guest/contractor access solution must also be able to:

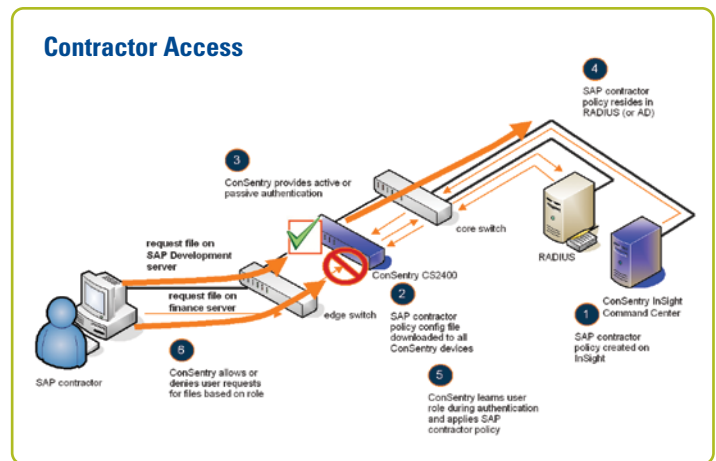
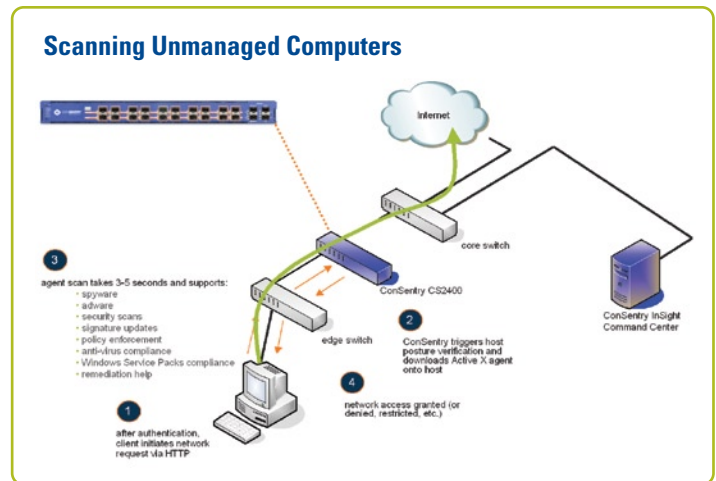
- **Identify a contractor.** Access controls must be tied to the user; being able to identify a user as a contractor is fundamental to applying appropriate access controls. Enterprises typically support contractor access in one of two ways: IT either

adds the individual contractor to the corporate identity store, such as an Active Directory or RADIUS server, or creates a common user name that all contractors from a given company share. The LANShield platform learns the user's identity during authentication, either passively by "snooping" the login to Active Directory or RADIUS or actively via captive portal (whereby the platform challenges a user for authentication information via a browser).

- **Automatically assign a user to a role.** An access solution must be able to automatically derive a user's role information from an enterprise's identity store(s). Knowing a user's role is key to creating and enforcing role-based policies. The LANShield platform automatically learns a user's role during the authentication process, avoiding any manual effort. For example, the platform can query Active Directory for a user's role information or can learn it by parsing RADIUS packets.

- **Restrict user reach based on role.** Defining access controls on a per-user or per-machine basis creates a tremendous burden for IT. Therefore, an access solution must support restrictions based on the user's role. ConSentry's LANShield platform allows IT to easily define policies that limit where a contractor can go on the network and what resources can be accessed. IT can restrict contractors to specific network destination(s) and/or zone(s), such as a collection of servers; to specific applications; and even by content at Layer 7 and above. For example, a contractor may be allowed access to select file shares or folders only and allowed read-only access.

In today's business environment, guests and contractors are among the users who regularly access enterprise networks. ConSentry Networks' LANShield product family provides a comprehensive yet simple solution to the guest/contractor access problem.



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