CONSENTRY NETWORKS

APPLICATION BRIEF

LAN Segmentation Alternatives

IT relies on LAN segmentation to separate traffic from different classes of users, such as guests, contractors, and employees, and to control what resources users can reach. IT often uses LAN segmentation to block traffic between users as well as to restrict resource access and application use for sub-groups of employees; for example, separating production vs. development personnel or employees in the engineering vs. finance departments.

Several methods for implementing LAN segmentation have emerged over the years, each with trade-offs among complexity, cost, and security effectiveness. In evaluating LAN segmentation alternatives, IT should look for a solution that meets the following requirements:

- leverages the existing infrastructure;
- leverages existing identity stores;
- is easy to implement;
- is easy to change;
- maintains LAN-speed throughput;
- provides user-based controls;
- supports application-based controls; and
- delivers effective security that can't be circumvented.

LAN Segmentation Options

1. Physical segmentation
2. VLAN-based segmentation
3. Firewall-based segmentation
4. 802.1X-based segmentation
5. DHCP-based segmentation
6. Identity-based segmentation

Current Options

To date, LAN segmentation solutions have fallen into four broad categories. We examine each relative to the requirements for an effective solution.

1) Physical segmentation

Used in high-security environments such as defense contractors and government agencies such as the Department of Defense, physical segmentation involves dedicating a LAN to a specific set of users. Sometimes, the segmentation extends to complete physical separation, where contractors work in one building and employees in another. For example, contractors may be restricted to a LAN that provides access to only the select applications and resources they need for their work, while employees are serviced by a separate LAN or set of LANs. Common areas, such as conference rooms, may be served by yet a different LAN.

This approach is limited to sites that have the most extreme need for traffic separation. It's expensive, inefficient, and inflexible since the user groups share no common infrastructure. Simple changes, such as to a user's role or physical location, are difficult to accommodate. Access to applications and resources is gated by whether the user has physical access to the LAN. If users can be denied physical access to unauthorized buildings or areas of a building, for example, physical segmentation can provide effective access controls. However, if an unauthorized user gains entry to a restricted area, security is ineffective as this approach has no inherent user- or application-based access controls.

2) VLAN-based segmentation

Switch-based virtual LANs represent one of the most commonly used LAN segmentation approaches. VLANs are created by grouping ports on LAN switches, so the user's reach on the network is gated by which VLAN that user's PC is plugged into. Traffic on each VLAN is logically separated and can pass from one VLAN to another only via a router. Virtually all LAN switches support VLANs, which means IT can leverage existing LAN infrastructure to implement this segmentation.

However, VLANs must be set up manually, and IT must define access control lists (ACLs) on routers to control where user traffic can go on the LAN. Both these steps make the VLAN/ACL approach time consuming and complex to implement as well as cumbersome to change. The administrative overhead of VLANs makes them costly and difficult to scale.

VLANs have no inherent application access controls; routers have varying levels of application visibility but ACLs operate at or below Layer 4. For example, ACLs cannot be defined for applications that use dynamic ports, such as voice over IP (VoIP) and Windows file sharing. User-based controls are predicated

on users connecting to the network from authorized locations. Users can circumvent this control simply by plugging their PC/laptop into a port connected to a VLAN they're not authorized to access.

3) Firewall-based segmentation

Firewalls can be deployed internally to segment LAN traffic. IT has the option to install a single, high-capacity firewall in a centralized location or smaller firewalls on uplinks or individual LAN segments. Separation via firewalls leverages existing network infrastructure and provides application-based controls up through Layer 4, including applications that use dynamic ports.

However, this approach is very expensive, both in equipment costs and operational overhead. Firewalls are complex to configure and administer, requiring knowledge of both protocols and security. As a result, their effectiveness depends on staff expertise. In addition, firewalls perform at the limited speeds needed at the LAN-WAN boundary – their primary application –so they typically slow LAN throughput. Because they lack any notion of users, they cannot provide user-based controls or leverage an enterprise's identity stores. Likewise, their application controls are coarse since they provide only limited visibility into Layer 7, the application layer.

4) 802.1X-based segmentation

Designed to provide port-based access control, 802.1X restricts network access to authenticated users. It leverages existing RADIUS servers to authenticate users , but it is not designed to provide post-admission control. For those kinds of user-based controls, IT must further architect the 802.1X deployment to extract and apply VLANs. As a result, 802.1X segmentation suffers from the same complexity as the VLAN/ACL combination previously described. Organizations that have upgraded their LAN switches in the past four years are likely to have 802.1X-capable hardware. However, organizations with older infrastructure, or those who have only partially upgraded their LANs, need to fully upgrade to 802.1X-compliant switches to use this segmentation scheme.

As with VLAN-based segmentation, the 802.1X approach lacks application-based controls, reducing its security effectiveness. In addition to needing 802.1X-compliant switches, this method also requires 802.1X supplicant software on all clients. Installing or simply configuring software already built into the desktop systems creates an administrative burden. Adding to the complexity, 802.1X relies on RADIUS for user authentication and VLAN assignment; since so many organizations run Active Directory as their identity store, those enterprises must take the extra step of having AD interface to a RADIUS database to support 802.1X.

5) DHCP-based segmentation

This approach to segmenting the LAN relies on an identity-based DHCP server. The server assigns IP addresses based on a user's status. Before a user or device authenticates, the server assigns a temporary source address for use during authentication. For users unable to authenticate to the LAN, such as guests, the server assigns a new IP address associated with a quarantined subnet. For users who successfully authenticate and pass their endpoint compliance check, the DHCP server assigns a new IP address associated with the production network. The DHCP database links the IP address assigned with the device MAC address. Once authorized, a user can access any network segment or individual resource permitted by the ACLs on the network's routers and firewalls.

IT must take measures to ensure that only traffic from devices using IP addresses issued by a known good DHCP server is allowed on the LAN, to prevent the use of static IP addresses or IP addresses issued by a rogue DHCP server, such as a DSL router.

But regardless of IT's ability to ensure the validity of the IP addresses in use, DHCP-based segmentation has other more fundamental shortcomings. First, the segmentation is very coarse – IT has no ability, for example, to apply multiple sets of controls based on user having multiple roles in the organization. Also, access control relies on ACLs and subnets, complicating setup and making changes difficult to implement. This approach lacks any post-admission visibility or application-based information, and users must authenticate twice – once to the DHCP server and a second time to the identity stores.

6) Identity-based segmentation

ConSentry Networks provides identity-based LAN segmentation as part of the security services supported by its LANShield product family.

Specifically designed for LANs, the LANShield platforms are cost effective, allowing for pervasive deployment. These high-performance platforms can be easily added to the existing LAN infrastructure, with the LANShield Controller deployed transparently upstream of LAN switches and the LANShield Switch deployed in the access layer hosting users and wireless access points. In addition, the LANShield devices leverage existing identity stores, such as Active Directory and RADIUS, to automatically learn each user's identity and role during authentication.

Knowledge of users and application-level visibility translate to flexible user- and application-based access controls. Through deep packet inspection encompassing Layers 2-7, the LANShield platforms provide visibility into and control over LAN traffic on a per-user, per-application, per-flow basis, enabling IT to securely separate traffic. Using ConSentry's InSight command center, IT can easily define access controls for individual users as well as by group or role. Those controls extend to application-level and even transaction-level controls. For instance, LANShield's complete traffic visibility enables IT to apply controls to application details within Layer 7, such as the destination URL in an HTTP session or the file name in an FTP download. InSight's graphical interface and pre-defined templates make it easy to set up access controls initially as well as make changes, and InSight enables IT to implement LAN segmentation centrally.

ConSentry provides a simple means for IT to separate traffic. The ability to deploy transparently, and have user access control policies apply ubiquitously throughout the enterprise, simplifies enforcement for IT. ConSentry gives IT an effective, affordable alterative to other LAN segmentation approaches.

	leverage existing infrastructure	leverage identity store	ease of implementation	ease of changes	user-based control	app-based control	overall effectiveness of security
physical	○	○	○	○	◑	○	◑
VLAN	●	○	◑	○	◑	○	○
firewall	◑	○	○	◑	○	◑	◑
802.1X	○	◑	○	◑	●	○	◑
DHCP	●	◑	●	◑	◑	○	◑
identity	●	●	●	●	●	●	●

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