

Deploying Access Controls without Rearchitecting Your LAN

The Impact of VLAN-based Architectures

Contents

Introduction	2
The Trouble with VLANs	2
Loss of Geographic Context	3
Instantiating VLANs Everywhere	3
Limited Control	3
The ConSentry Advantage	4
About ConSentry Networks	5

Introduction

Increasingly, organizations are looking to deploy access controls as a key weapon in their LAN security arsenal. Compliance demands, such as Payment Card Industry Data Security Standard (PCI-DSS) for example, mandate embedded controls over who can reach what data. And enterprises looking to provide guest or contractor access, without letting those users onto the entire corporate LAN, need these access controls.

Network admission control (NAC) solutions are a primary alternative IT shops are evaluating today for gaining this network-level access control. In addition to the admission control features of user authentication and host posture check, some NAC offerings also support post-admission controls such as role-based access.

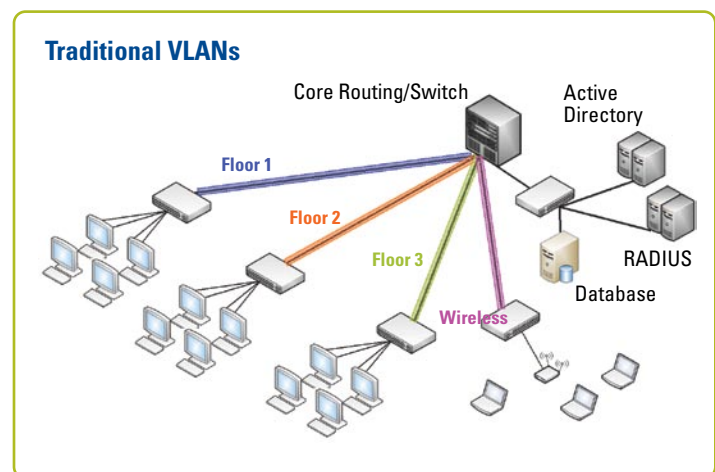
Role-based access control can be a powerful tool, providing enterprises the means to granularly control user access to network resources based on their role in the organization. Employees in human resources, sales, engineering, and marketing would have access only to those resources needed to do their jobs. Likewise, guests and contractors could be appropriately constrained. With granular user-based access controls, IT could even distinguish between the access needs of senior managers vs. middle managers vs. staff.

Some NAC solutions rely on virtual LANs (VLANs) to provide this user-based control. However, implementing this capability via VLANs requires organizations to rearchitect their LANs, making substantial changes to their VLANs and Access Control Lists (ACLs). This daunting task requires extensive implementation and ongoing work, negates some key operational uses that VLANs provide, and leaves IT with very limited post-admission control. This paper will explore these VLAN challenges and contrast them with the simplicity of ConSentry Networks' system for deploying flexible role-based access controls independent of VLANs.

The Trouble with VLANs

VLANs are a common method for segmenting LAN traffic and breaking up the LAN into smaller broadcast domains. Although vendor tools have greatly simplified the instantiation of VLANs on LAN switches, the real work in deploying VLANs is in defining the logic of the VLAN structure itself and in creating the ACLs that control which traffic can pass between VLANs.

Most organizations take a geographical approach to VLAN structure. That is, each VLAN represents a physical location on a campus and within a building. So VLAN 1 might correspond to floor one in building one, for example. VLAN information often gets incorporated into an organization's IP scheme; devices in VLAN 1 may have that "1" built into their addressing, for example. This link between VLANs and IP addresses greatly simplifies the job of locating network equipment for troubleshooting purposes.



Traditionally, IT has constructed VLANs based on building geography

In addition to defining the VLANs themselves and mapping DHCP servers and static IP addresses to match that VLAN informa-

tion, IT must also define ACLs on routers. Traffic on each VLAN is logically separated and can pass from one VLAN to another only via a router. ACLs either allow or block traffic from passing between VLANs. Defining ACLs on routers is a cumbersome and time-consuming process, and they must change any time a VLAN changes, adding to the overall complexity of setting up VLANs.

VLANs have no inherent understanding of users or their roles. NAC solutions that rely on VLANs for role-based access controls require organizations to rearchitect their VLANs, establishing a VLAN per role. Given the administrative overhead of setting up VLANs in the first place, rearchitecting them places a clear burden on IT, who must change the VLAN structure, re-instantiate VLANs in switches, change ACLs, and perhaps change IP addresses.

Loss of Geographic Context

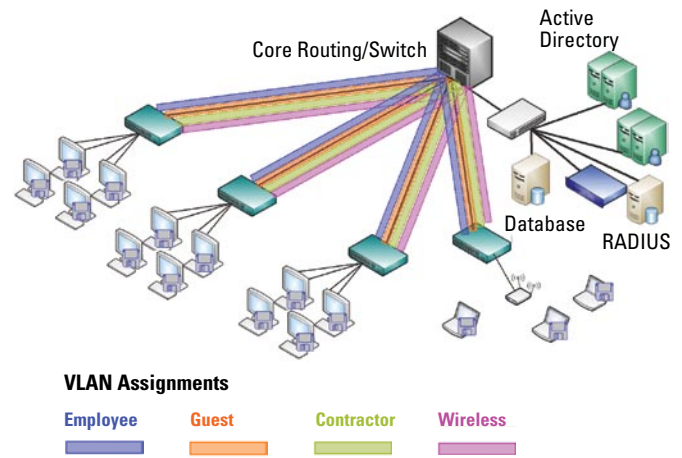
In addition to the extra work, IT loses geographical information when rearchitecting VLANs to support role-based access controls. IT has come to rely on the geographic orientation of VLANs when troubleshooting. When a user is experiencing connection problems, for example, IT can readily resolve that user's IP or MAC address to a VLAN, so IT then knows the geographic location of that user and the switch and other equipment connecting that user into the LAN.

With VLAN-based NAC products, VLANs are changed to be associated with a user's role. For example, all guests would be placed in VLAN 1, contractors in VLAN 2, and employees in a series of additional VLANs according to the roles IT defines for them. As a result, all geographical associations are lost, so IT operations and helpdesk personnel, as well as other IT groups heavily dependent on geography-based VLANs for troubleshooting, would have to be retrained on the new structure.

Instantiating VLANs Everywhere

For role-based VLANs to work effectively and not constrain where users might access the network, IT must distribute VLANs throughout the campus. Users must be able to log into the LAN from any location and be put into the appropriate VLAN, so either IT must instantiate every role-based VLAN in every switch where users connect, or the NAC solution must have a means to dynamically instantiate VLANs in switches.

VLANs add Complexity to Access Control



With VLAN-based access control, IT must change VLANs from geography to role, distribute the VLANs throughout the enterprise, and update ACLs to control access.

For example, the contractor role/VLAN must be distributed to every switch where contractors might connect; likewise for guests. Employees may connect from anywhere in the organization, especially if wireless is in use, so each VLAN for each user role must be distributed everywhere in the campus.

Limited Control

NAC solutions that rely on VLANs for access control provide very limited post-admission controls. First, VLAN-based architectures lack the ability to support multiple roles per user; each role corresponds to a single VLAN with its associated resources. This limitation creates serious challenges, as many users wear several hats. For example, the head of human resources needs access to both HR and select executive resources. Similarly, a CIO needs access to IT resources as well as key executive resources.

In theory, IT could create "super-set" roles and associated VLANs that provide access to a particular set of cross-role resources. However, this approach would rapidly evolve into an explosion of VLANs, with many containing only a single user.

Second, NAC solutions that use VLANs for access control provide no post-admission monitoring, limiting the controls they can apply. These solutions include an out-of-band appliance that is able to monitor a user's initial connection to the LAN and tells the wiring closet switches the VLAN in which to place the user.

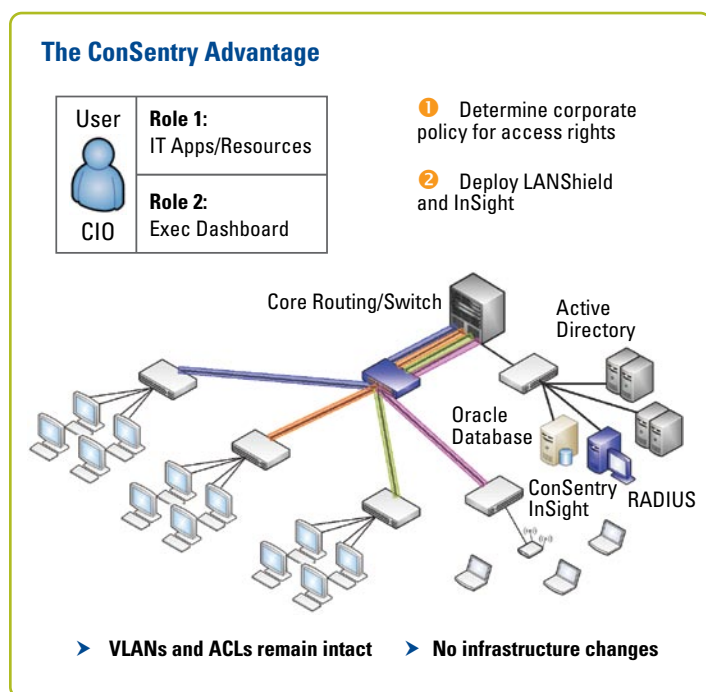
Out-of-band NAC appliances, though, are not in the path of traffic and so have no sense of what users are attempting to do on the

LAN. Traffic that violates policy is simply dropped by the ACLs, but IT has no notion of which user attempted the inappropriate access or which policy was violated. Also, IT cannot tell whether the dropped traffic was the result of an ACL the NAC appliance created or an ACL directly applied to the switch. This lack of insight greatly complicates troubleshooting in cases where the traffic should not have been dropped, and IT has no ability to discern inappropriate user behavior.

The inability to see traffic after a user has been admitted to the LAN also means out-of-band NAC appliances have no ability to detect or block malware. Some out-of-band appliances can be deployed inline in limited deployments, such as on a wireless segment or behind a VPN, but these devices do not have the horsepower needed to be pervasively deployed inline throughout an enterprise to provide malware containment.

The ConSentry Advantage

ConSentry Networks delivers access control as part of a comprehensive set of LAN security services supported by its LANShield product family. ConSentry access controls are based on a user's identity and role and are therefore completely independent of an organization's VLAN architecture. As Layer 2-7 aware devices that perform deep packet inspection of all LAN traffic, the LANShield platforms have complete visibility into and control over network activity on a per-user, per-flow basis.



ConSentry's approach requires no changes to switches, VLANs, identity store, endpoint software, and enables multiples roles per user.

ConSentry leverages an organization's existing AAA servers and identity stores to automatically learn a user's identity and role. The LANShield platforms bind an IP and MAC address to a user name, allowing all LAN activity to be tied back to individual users, including application flows, files opened and closed, and use of resources such as printers and IP phones.

This ability to granularly track LAN traffic allows for flexible access controls based on a user's role in an organization. Using the InSight command center's graphical user interface and policy templates, IT can easily create role-based and location-specific policies. These centrally-defined policies are distributed by InSight to LANShield devices, which enforce them on the fly. No changes to the existing network are required.

In contrast to NAC solutions that employ VLAN-based access controls, ConSentry access controls operate independently of VLANs, eliminating the need to rearchitect VLANs and ensuring that VLANs retain their geographical context and other benefits. In addition, ConSentry can apply multiple policies to users and so can easily support users who have multiple roles.

Because the LANShield platform ties all LAN activity to users, access control is applied regardless of where – or how – users connect to the network. Whether sitting at a desktop computer or accessing the network in a conference room via a wireless laptop, the same access controls apply to each user. The system is also flexible enough to support geographically dependent policies, so that an enterprise can allow one set of access rights to employees connecting locally and a different, perhaps more limited, set when those employees connect over the VPN.

Regardless of policy, with the ConSentry solution, IT never has to instantiate specific controls – let alone VLANs or ACLs – everywhere in the network or make any other architectural changes or device upgrades. Instead, IT simply sets policy in InSight, and those policies are then distributed to the LANShield platforms throughout the enterprise which then directly enforce access controls with no infrastructure dependency.

User- or role-based access controls are a boon to organizations needing to beef up their LAN security. ConSentry gives organizations sophisticated, easy to deploy access controls that operate across the enterprise with no impact on the existing network infrastructure.

About ConSentry Networks

ConSentry Networks delivers comprehensive LAN security, enabling businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry enables this pervasive security while lowering IT's cost of operations through its flexible, high-performance platform powered by ground-breaking custom silicon and revolutionary LAN security software. Backed by blue-chip venture capital firms that include Accel Partners, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California. For more information, visit the company's web site at www.consentry.com.

Corporate Headquarters

ConSentry Networks

1690 McCandless Drive
Milpitas CA 95035

Tel: 408-956-2100

Toll-Free: 866-841-9100

Fax: 408-956-2199

Email: sales@consentry.com

Germany Office

ConSentry Networks

Lyoner Strasse 26 D-60528
Frankfurt Germany

Tel: +49 69 677 33 422

Fax: +49 69 677 33 200

United Kingdom Office

ConSentry Networks

Lakeside House 1, Furzeground Way
Stockley Park, Heathrow, UB11 1BD

Tel: +44 (0) 2086 22 3020

Fax: +44 (0) 2086 22 3200

Japan Office

ConSentry Networks

Hibiya Central Bldg. 14F
1-2-9, Nishi Shinbashi, Minato-ku
Tokyo 105-0003 Japan

Tel: +813-5532-7630

Fax: +813-5532-7373