TECHNOLOGY WHITE PAPER

# Evolving Network Security with the Alcatel-Lucent Access Guardian

Enterprise network customers encounter a wide variety of difficulties and complexities when designing and implementing a security infrastructure. The solution must be comprehensive, flexible, and able to grow and evolve in tandem with the network and the threats it faces. Alcatel-Lucent has a large portfolio of tools and solutions to help the enterprise network customer. One such solution is the Alcatel-Lucent Access Guardian, which integrates authentication, device compliance and access control functions directly into the network infrastructure at the switch level. The following paper outlines several common customer security challenges and how the Access Guardian can be used to meet them.

# Table of contents

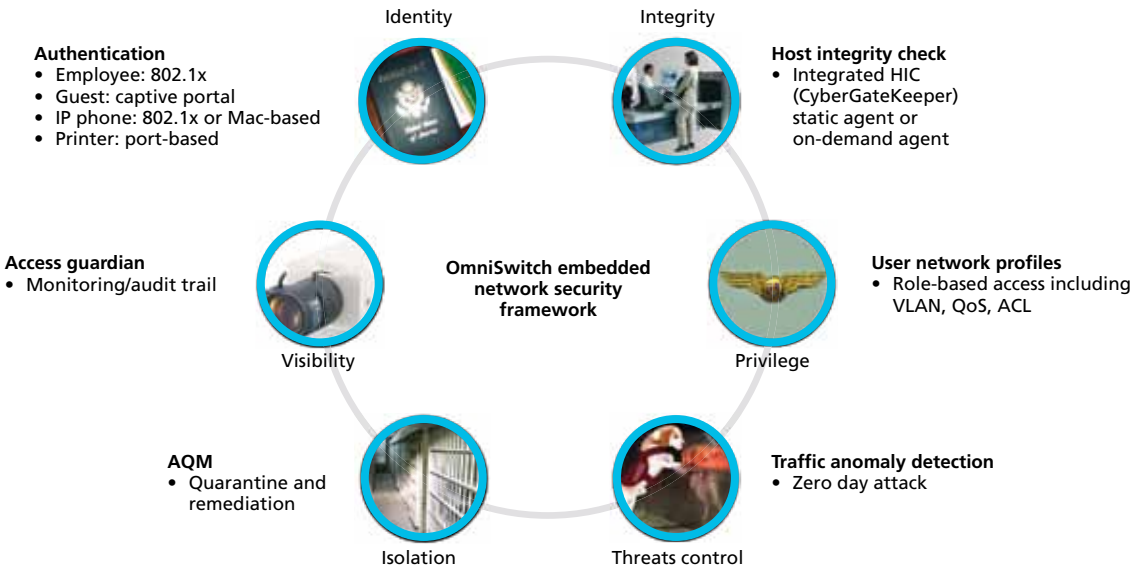
## Introduction

Every enterprise network has individual security requirements. Alcatel-Lucent has several tools and solutions to fully customize network security based on a customers needs.

The following examples outline common customer security requirements and their possible solutions.

*"Only the right people should have access to my network"*

**Figure 1. Alcatel-Lucent Embedded Network Security Framework**




## Network authentication with Access Guardian

Although network authentication technologies have been around for many years, deployment has been limited in most enterprise networks. The recent introduction of the wireless LAN (WLAN) infrastructure has changed the perception regarding network security. This heightened security awareness in conjunction with the prevalence of mobile devices and the integration of authentication methods into the wireless encryption process (WPA, WPA2) has propelled network authentication back into the forefront of network security technologies.

Even as authentication has gained widespread adoption in WLAN infrastructures, deploying it on the wired LAN is a continuous struggle. Legacy devices, lack of driver support and other compatibility issues limit how users and devices access network resources. The Alcatel-Lucent Access Guardian solves the wired LAN problem by combining several authentication technologies into one customizable and flexible framework within the edge switch to evolve current authentication systems from manual to dynamic.

### Employee access

Possibly the biggest challenge in implementing authentication is determining the identity of authorized devices. Not all devices may have actual end users entering credentials (printers, copiers, vending machines, cameras, some IP phones, etc.), so alternative processes must be established to recognize them, which places an extra burden on network administrators.

To grant network access to devices that do not have built-in capabilities such as challenge-based authentication (802.1X or web-based authentication), media access control (MAC) authentication can be implemented using a RADIUS server and an appropriate database (SQL, etc.) The database contains all the MAC addresses and optionally the appropriate "role" to be returned to the switch.

Gathering and managing all the MAC addresses is daunting, but several tools are available to make it easier. The Alcatel-Lucent OmniVista™ 2500 Network Management System includes the Locator application, which polls and stores information on all MAC addresses in the network. By cross-referencing a vendor's IEEE organizationally unique identifier (OUI) with the OmniVista 2500 NMS database an administrator can quickly recognize various device classes, such as printers or IP phones.

Recognizing guests on the network is the result of a process of elimination. Once employees and other known devices have been recognized by 802.1X, MAC-based or web-based authentication, all other devices are considered new and/or guest devices. The administrator is then able to decide whether to grant access or not. If access is granted, the web-based authentication method could be used, and separate roles returned to grant the guest different access rights and VLANs.

An effective method of control is to provide guest credentials using a sign-in process at a front desk or visitor desk. A temporary login/password is assigned to each visitor, and these credentials are used to gain wired and/or wireless access to the network infrastructure.

### Enabling access for guests in public areas

Access Guardian authentication policies are defined on a per-port basis. Which means different devices may be connected to a port using different VLANs or access controls, but the configuration of the authentication policy is defined per port. To allow access to the network from public and semi-public areas such as lobbies, conference rooms, etc., physical ports in those areas could be configured to require web-based authentication. This change does not require a wide-scale implementation of other authentication methods, but can be pinpointed to specific areas without the introduction of a new security infrastructure.

*"I want to control what parts of my network users can access"*

## Access control with Access Guardian

The Access Guardian framework allows administrators to implement dynamic access controls through the network infrastructure. User network profiles (UNP) enforced at the edge switch provides a means of correlating a user group to a specific set of access control policies.

Access controls can be based on user identity through authentication or physical location based on the port. Control based on physical location is achieved by assigning the appropriate UNP to a specific set of ports, which is then linked to access control lists (ACLs) in the edge switch hardware. Because there is no limit to the number of endpoints that can be associated to an internal list, the design is scalable to any size of network. UNPs can also be determined by any form of authentica-

tion implemented on the edge switch (802.1X, MAC-based and web-based authentication). By associating a list of ACLs to a UNP, groups of users are given specific access rights. Note that this association does not take the VLAN or source IP address into consideration. ACLs are implemented based on the MAC address of the station and not its membership in a particular VLAN or subnet.

It is possible for a customer to implement the same UNP names across their entire infrastructure, as the VLAN association is kept locally on each switch. For example, a UNP named 'Engineering' is deployed in one building with VLAN 10, while the same UNP in another building is VLAN 20. In each building, the same ACLs are enforced, simplifying the authentication and access attributes that RADIUS provides to the edge switches.

The current generation of Alcatel-Lucent edge switches supports eight different ACL lists that have the ability to be shared by many different UNPs. For example, a customer wants to implement two access control mechanisms in a remote office, but does not want to burn multiple subnets. All that has to be done is to configure two UNPs for the same VLAN, but with different ACL lists, thereby separating the access for each user group.

Determining the appropriate access rights is a complex undertaking. To determine what IP addresses are accessed by a user, a combination of multiple tools is necessary. Starting with the internal connection list of the host is a good start (using the "netstat" command in Windows or Linux). However, monitoring network devices using a network analyzer is highly recommended, as most analyzers will build a connectivity table that translates into the appropriate ACLs for that group. Also, it is possible during the initial implementation phase to create ACLs to log network traffic. By capturing network activity instead of dropping it, the administrator obtains a log for future analysis.

*"I want to make sure endpoints on my network are safe"*

## Endpoint compliance with Access Guardian

Access Guardian has the ability to perform endpoint compliance independent of authentication and access controls directly from the edge switch. This feature does not require additional hardware or changes in the network architecture.

To enable endpoint compliance, configure the switch to interact with the centralized host integrity check (HIC) server, also known as the InfoExpress CyberGatekeeper server. Next, specify a UNP role for the devices to be verified as well as the allowed resources, such as specific servers or subnets. The UNP can be derived from the source port, a source MAC address range, source IP addresses or through authentication.

A device is quarantined when it has not been verified or if it has failed the check. The edge switch will still allow access to a predefined set of resources while restricting all other access. In this way the administrator can still have access to quarantined users with SMS or a remote session in order to fix and update the machines. Alternatively, the administrator is able to allow access to certain areas of the network and restrict access to other parts until the user's device has been checked. Limiting network access is achieved by widening the scope of "remediation servers" to include the accessible subnets. At this point four distinct entries are available, each with its own IP range and mask.

## Conclusion

Access Guardian enhances the functions of the Alcatel-Lucent edge switch families by integrating authentication, device compliance and access control functions directly into the hardware. Switch-based security functions allow an administrator to configure, manage and maintain their entire security infrastructure more efficiently and without additional equipment. Host integrity checking and user profiles simplify the network while automatically managing the security fitness of end points and limiting the access of unauthorized users and devices. By creating a flexible customizable security infrastructure at the switch-level, Alcatel-Lucent distributes security functions to all corners of the network leaving no backdoor for intruders.

## Abbreviations

| | |
|---|---|
| 802.1X | IEEE Standard for port-based network access control |
| ACL | access control list |
| HIC | host integrity check |
| IEEE | Institute of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| LAN | local area network |
| MAC | media access control |
| OUI | organizationally unique identifier |
| RADIUS | remote authentication dial in user service |
| SMS | short message service |
| SQL | structured query language |
| UNP | user network profile |
| VLAN | virtual local area network |
| WLAN | wireless local area network |
| WPA, WPA2 | Wi-Fi protected access |

## Contacts

**Vincent Vermeulen** (vincent.vermeulen@alcatel-lucent.com)
Enterprise Solutions Division
Alcatel-Lucent

**Sarveshwar Rao** (sarveshwar.rao@alcatel-lucent.com)
Enterprise Solutions Division
Alcatel-Lucent

## References

User-centric Security: **http://www.alcatel-lucent.com/enterprise/security**

Network Security: **http://www.alcatel-lucent.com/enterprise/networksecurity**


EPG3310090520 (06)

Alcatel·Lucent