

Access Control for Enterprise Networks

Protecting information privacy
and availability using Alcatel
Access Guardian



Table of Contents

Dynamic communications demand privacy and availability for enterprise information . . .	3
Secure, dynamic mobility	3
The enterprise network	3
Secure access to your network	4
Alcatel Access Guardian implementation overview	4
Operation of Access Guardian	4
Authenticating all the users and devices on your network	5
Employees with PCs	5
Guests with Notebook Computers	5
IP phones	6
Simple to implement	6
Summary	6
Specifications & Availability	7

Dynamic communications demand privacy and availability for enterprise information



Secure, dynamic mobility

Your business communications today are dynamic and mobile from the widespread use of PDAs, phones, and PCs over your LANs, wireless LANs, and public networks. Keeping this information secure as it passes between and over these devices remains a primary concern for you and your business.

The enterprise network

Your network can play a unique role in protecting the availability and privacy of information. It can prevent security problems by providing identity-based access, by protecting PCs from viruses and malware, and by detecting and controlling intrusions.

Is your network part of the identity management solution and does it protect your PCs? For most organizations the answer is still no. Yesterday's LAN switch does not provide the depth of feature support necessary for an efficient, effective network-based solution.

With the convergence of voice and data onto a single IP network, it's common to connect both an IP phone and a PC to the same LAN switch port. However, yesterday's LAN switches do not provide the tools to authenticate multiple clients on a single port. Today's switches need to be able to authenticate multiple clients on a single LAN switch port to eliminate this barrier.

By deploying auto-sense authentication found in modern LAN switches, an administrator will save costly operations staff time by eliminating the need to partition ports based on the authentication method supported by the device and user that will use the port. Today's switch can support multiple methods of authentication on a single port without involving an administrator.

Access Guardian eliminates the barriers and reduces the cost of deploying identity-based network access controls and allows your network to help protect PCs from viruses and malware.

Alcatel's Access Guardian is a component of the Alcatel CrystalSec security framework. CrystalSec offers proactive and reactive security solutions composed of comprehensive switch-based security capabilities, and integration with security appliance industry leaders.



Mobility demands improved IT security. Your network is part of the solution. Identity-based mobility ensures security, privacy and availability.

Secure access to your network

Access Guardian, designed by Alcatel, is a proactive network security solution that provides intelligent interworking between standards-based devices. Alcatel Access Guardian provides identity based network access to enable enforcement of device and network security policies, resulting in increased privacy and availability of communications.

Access Guardian authenticates the network users including employees, contractors and guests, confirms their PC's conformance to security policies, and then provides access rights based on the user's role. With Alcatel's Access Guardian, the network is able to prevent virus and worm attacks, ensure performance, protect IP telephony devices regardless of vendor, and provide network services to all authorized users. All while protecting the privacy and availability of your business' communications.

Alcatel Access Guardian implementation overview

Alcatel's Access Guardian combines LAN switch and wireless LAN controller authentication and access control features with standards based directory services.

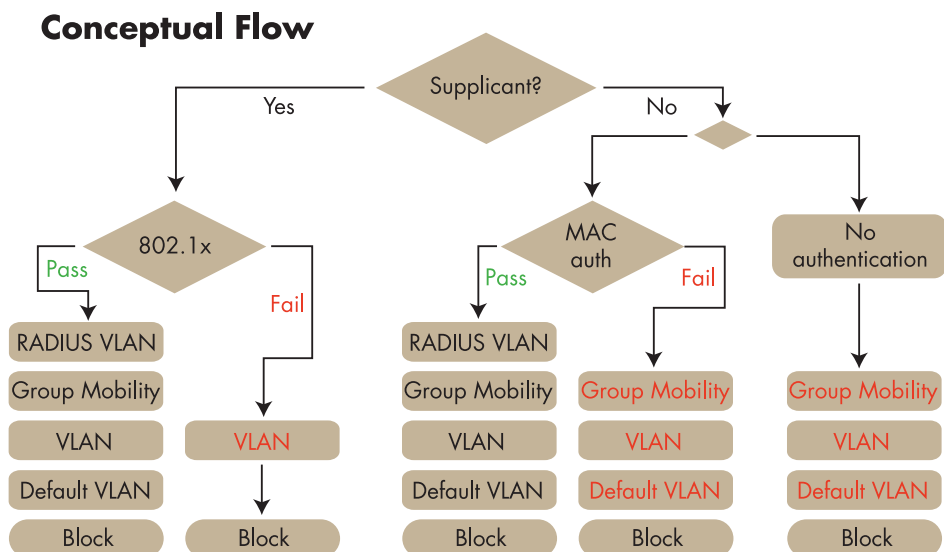
The LAN switch or wireless LAN controller provides 802.1x authentication and additional authentication options for devices not supporting 802.1x. This means that all devices on the network can be authenticated, not just the newest PCs. In addition to 802.1x authentication, the LAN/WLAN switches also provide auto-sensing authentication policies, access controls after authentication and the option of policy conformance verification.

Access Guardian works with directory servers supporting RADIUS as well as RADIUS implementations from Microsoft, Juniper, Bradford, Lucent and others.

Operation of Access Guardian

1. Authenticate the user or device
2. Verify the device meets security policies (optional)
3. Authorize network access rights based on role and policy conformance

Another component of the Alcatel CrystalSec security framework is the Alcatel OmniVista 2770 Quarantine Manager application, which defends against attacks at the network and application levels by isolating misbehaving users and providing a means for user remediation.



Converged and mobile networks need to support multiple methods of authentication. Access Guardian provides MAC-based authentication to support non-802.1x devices including non-802.x IP phones.

Authenticating all the users and devices on your network

The following examples illustrate how privacy and availability of services is ensured for different types of users on the network. The three scenarios are: an enterprise employee using a PC, a company visitor, and an IP phone.

Employees with PCs

For the employee using a PC, when they connect their PC to the network they must prove their identity with 802.1x. Once the identity is known, the PC's configuration is confirmed using a host integrity check and then provides employee network access rights. If the employee's identity or device does not conform to security policies, network access is limited to a self-service web portal for additional assistance.

Guests with Notebook Computers

For the network guest that requires only Internet access but should be prevented from accessing business information, authentication is provided using a captive portal. Once authenticated, the guest is provided limited network access. Additional guest authentication options are also supported.



You can protect and control your network when you know who or what is using it. Access controls are an important part of the network security solution and must be easy to implement and support all devices across the entire network.

IP phones

IP phones illustrate the need for the network to support multiple methods of authentication. Alcatel's IPTouch phones support 802.1x authentication. Once authenticated using 802.1x, an IPTouch phone is assigned network access rights. It's recommended that the IP phone be placed into an IP Telephony (VoIP) VLAN where ACLs and IP Telephony aware firewalls control access to the VLAN.

Since most non-Alcatel IP phones do not support 802.1x authentication, an alternate method is required. Access Guardian provides MAC-based authentication to support non-802.1x devices including non-802.x IP phones.

With MAC-based authentication the switch uses the IP phone's MAC address as the user ID and password for RADIUS authentication. This allows a single directory to authenticate both PC users and IP phones. Non-Alcatel IP phones should be placed into a VoIP VLAN where ACLs and IP Telephony aware firewalls control access to the VLAN.

If the IP phone and PC are being supported on a single LAN switch port, authentication must support multiple clients using multiple authentication methods. This is a common objective in VoIP deployments and fully supported by the Access Guardian solution.

Simple to implement

Most networks have a mixture of users and device types similar to these examples and likely even broader. Printer, LAN based Video cameras, XBox, PlayStation, wireless LAN APs and other non-PC devices make up half of the devices on the network. If the network does not support auto-sense authentication of non-802.1x devices, then implementing 802.1x for some devices requires changing the configuration of the network port as devices are moved or added.

Alcatel Access Guardian removes this problem by auto-sense application of multiple methods of accurate authentication. All types of devices can be authenticated without any network configuration changes. This means identity-based access is possible, affordable and accurate.

Summary

Communications have become dynamic and information security has become more demanding. The enterprise network plays a unique role in ensuring the privacy and availability of information. Identity based network access controls are a foundation for enhanced information security.

Alcatel's Access Guardian protects your information, enforces PC configuration policies and provides identity based resource controls. These services are provided with an open architecture and support all types of devices and users on the network. The network access controls are open, universal and effective.

Specifications

Alcatel OmniSwitch and OmniAccess support for Access Guardian

Availability

Alcatel LAN switches using the Alcatel Operating System (AOS) software support the authentication and access control features required by Access Guardian.

- OmniSwitch 6600, 7700/7800 and 8800 support the Access Guardian feature set beginning in software release 5.4.1. These features are available now.
- OmniSwitch 6850 and 6800 support the Access Guardian feature set beginning in software release 6.1.2R03. These features are available now.
- OmniSwitch 9000 will support the Access Guardian feature set beginning in software release 6.1.3. These features will be available in Q4 2006.

OmniSwitch features supporting Access Guardian

Access Guardian uses the OmniSwitch 802.1x feature set to provide flexible authentication for 802.1x supplicants and non-supplicants. These features include:

- 802.1x
- 802.1x multi-client support
- 802.1x VLAN assignment policies
- 802.1x non-supplicant support
- 802.1x MAC authentication for non-supplicants
- 802.1x Device Classification Policies
- Group mobility for 802.1x supplicant and non-supplicants
- Concurrent, autosense authentication

PC Security Policy Conformance

Access Guardian supports multiple methods to confirm the user's PC conforms to security policies. The combination of multiple methods allows (optionally) confirmation of employee, contractor and guest configurations before they are authorized network access.

- Application on the PC: Host Integrity Check interworking with 802.1x,
 - Sygate/Symantec
 - InfoExpress
- Windows operating system on the PC: Host integrity check interworking with 802.1x
 - Microsoft NAP
- Clientless Host Integrity Check: Interworks with 802.1x on the LAN switch
 - OmniAccess 4300/600 Client Integrity Module
 - InfoExpress clientless host integrity check
 - Third party appliances that rely on standard DHCP and 802.1x capabilities

Alcatel
26801 West Agoura Road
Calabasas, CA 91301 USA
Contact Center
(800) 995-2612 US/Canada
(818) 880-3500 Outside US
www.alcatel.com/enterprise

Product specifications contained in this document are subject to change without notice. Contact your local Alcatel representative for the most current information. Copyright © 2006 Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the expressed written permission of Alcatel Internetworking, Inc. Alcatel® and the Alcatel logo are registered trademarks of Alcatel. All other trademarks are the property of their respective owners.

P/N 031888-00 Rev. A 7/06