Alcatel-Lucent OmniAccess Policy Enforcement Firewall Module

WIRELESS LAN SOFTWARE

Alcatel-Lucent® OmniAccess™ Wireless Policy Enforcement Firewall (PEF) module provides identity-based security, quality of service (QoS) control and traffic management capabilities to a user-centric network. Identity-based security is essential since mobile users can enter a network at any point, wired or wireless. The OmniAccess Wireless stateful firewall enables user classification on the basis of user identity, device type, location, and time of day and provides differentiated access for different classes of users.

FEATURES	BENEFITS
• Identity-based stateful firewalls	• Firewall rules are aware of the user, not just IP addresses, leading to greater visibility and more complete control
• Policy-based access control	• Permits translation of corporate security policy into action. Compliance with corporate security policy becomes mandatory and enforced rather than simply monitored
• Quality of service control	• Stateful flow classification enables identification of application flows for special treatment, such as providing enhanced QoS for voice
• Role-based access control	• Permits templates to be applied based on group membership, simplifying administration
• High-performance security	• Hardware-accelerated encryption/ decryption and firewall rule processing to eliminate bottlenecks • Separation of control and data plane for scalability

Since the physical layer of security is missing in mobile networks, mobile users need to be treated with greater security than traditional fixed users. Firewalls are a mandatory part of an enterprise's layered security strategy for the mobile network, and the OmniAccess Wireless solution's unique identity-based stateful firewall technology enables enterprises to define access controls for any user or group of users on the network.

Identity-based stateful firewalls

The Alcatel-Lucent OmniAccess WLAN switches provide a single point of encryption/ decryption, authentication, and firewall enforcement. Since the switches are identity-aware and also terminate encryption, they are immune from spoofing attacks that plague traditional network-based firewalls that filter on IP address rather than user identity.

Complete policy-based access control

All organizations have written IT security policies. Policies dictate the network access, protocols and applications that are permitted or denied, and levels of services that are provided. In most enterprises, policy compliance is monitored to varying degrees, but violations are discovered and dealt with after the fact. The Alcatel-Lucent OmniAccess Wireless solution permits policies to be actively enforced, even in a mobile environment, with policies following the users as they roam across the wireless infrastructure.

Figure 1: Easy to use GUI for firewall policy configuration: Firewall Settings

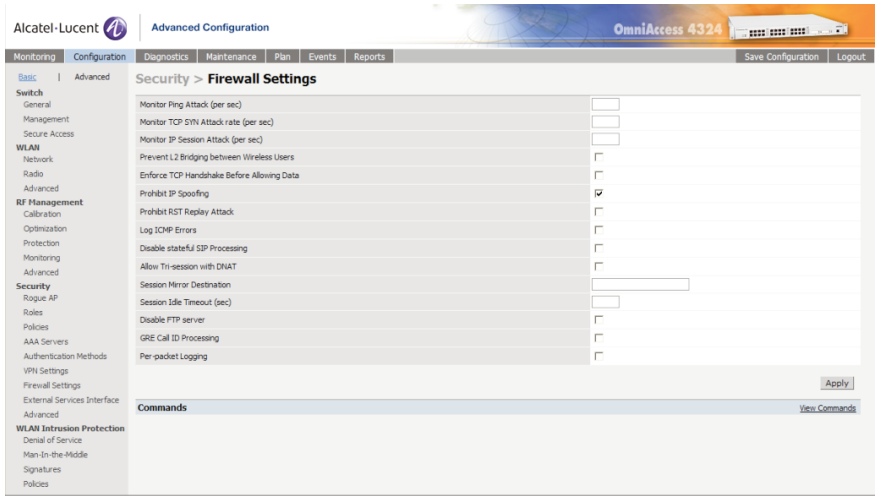

Figure 2: Global Settings

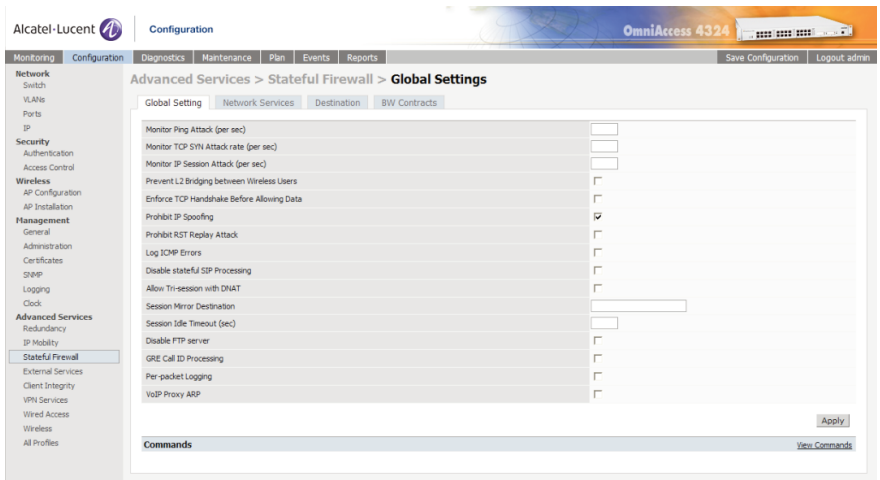

Figure 3: Firewall Policies

Quality of service control

Once application flows have been identified by the firewall, standard firewall actions such as permit, drop, log, or reject can be applied. However, the OmniAccess Wireless stateful firewall capability enables more than just robust security. Rule actions can also tag packets with an 802.1p or DSCP marking, prioritize the traffic into multiple queues, or even redirect specific protocols to different destinations. Flow classification is stateful for many popular protocols, such as SIP and Alcatel-Lucent New Office Environment (NOE) voice protocol, permitting appropriate QoS to be applied to both the control protocol and the call sessions.

Role-based access control

The OmniAccess Wireless Stateful Policy Enforcement Firewall enables access to network resources based on the role of the user. This role is assigned or derived through a variety of different mechanisms such as external authentication databases, ESSID, or physical location. Once the role has been assigned to a user, differentiated policies can be applied.

High-performance Wireless Security

Until now, enterprises have been forced to quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet. While this mechanism works from a security standpoint, the performance offered to the wireless user is severely impacted due to limitations with DMZ-based VPN gateways and firewalls. The OmniAccess Wireless solution allows corporate users to be authenticated, encrypted and firewalled within the corporate intranet with the highest degree of security and performance, providing the connecting point between mobile users and the wired network.

TECHNICAL SPECIFICATIONS

Role determination criteria
- Authentication – Default or RADIUS-derived
- Physical location

Wired and wireless QoS
- Flow classification
- Priority queues
- Bandwidth contracts
- 802.1p and DSCP tagging

Network address translation
- Source and destination

Stateful application-level gateway
- FTP
- SIP
- RTP/RTSP
- Alcatel-Lucent New Office Environment (NOE)
- Skinny Call Control Protocol (SCCP)

To learn more, contact your dedicated Alcatel-Lucent representative, authorized reseller, or sales agent. You can also visit our Web site at www.alcatel-lucent.com.

This document is provided for planning purposes only and does not create, modify, or supplement any warranties, which may be made by Alcatel-Lucent relating to the products and/or services described herein. The publication of information contained in this document does not imply freedom from patent or other protective rights of Alcatel-Lucent or other third parties.

www.alcatel-lucent.com

Alcatel·Lucent