# Identity-Based Security

Aruba's identity-based security solution dramatically improves network security by eliminating excess privilege on the network while also providing identity-based auditing of activity. Traditional fixed networks can only apply access rights to ports or VLANs. Mobile users and devices, by definition, do not connect to the network through a fixed port. The network must therefore identify every user and device that joins the network. Once this identity is known, custom security policies may be applied to the network so that only access appropriate to the business needs of the user or device is provided.
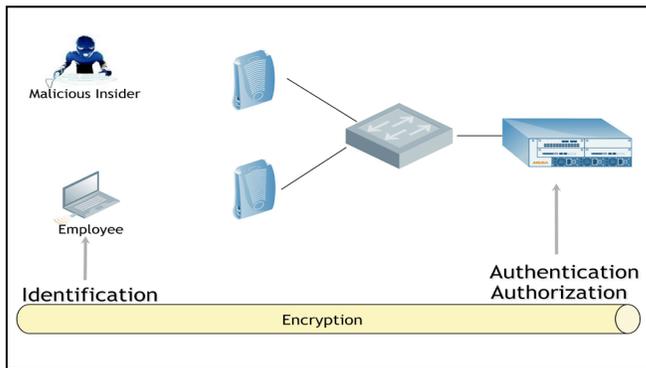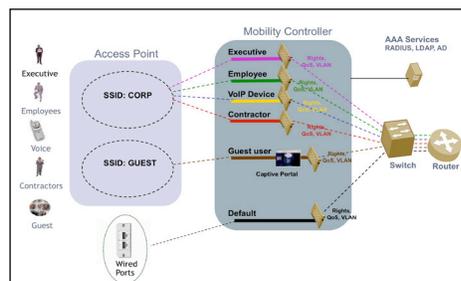

Single Point of Security Control

prevents against address spoofing attacks by combining the point of encryption, authentication, and access control into a single unit. Without a single point of security control, one device normally does encryption, another device does authentication, and an external firewall does access control. This makes the firewall vulnerable to IP address spoofing, since the firewall is not identity-aware. In an Aruba system, firewall policies are applied to users, not to IP addresses. An address spoofing attack in an Aruba system will not result in the bypassing of any firewall policies.

Role-Based Access Control

Identifies who the user or device is, based on an authentication method such as 802.1x, VPN, or captive portal. During the authentication

process, the Aruba mobility controller learns the group, or role, of a user or device. This information comes from an authentication server such as Active Directory, RADIUS, or LDAP. Once the role of the user or device is learned, appropriate access rights and policies can be applied to that session. This practice allows multiple classes of users to share the same network infrastructure, and eliminates excess privilege normally granted by "one size fits all" fixed networks.

Highlights:

- Identifies users or devices and separates them into roles

- Provides role-based access control based on group membership

- ICSA-certified stateful firewall enforces per-user access rights

Benefits:

- Allows different classes of users to share the same network infrastructure

- Eliminates excess network privilege normally granted by "one size fits all" fixed networks

- Locks down the network against unauthorized disclosure or alternation of information

- Provides accountability through auditing of network access and activity

- Protects client devices from attack by other client devices

- Blocks spreading of viruses, worms, and other malware

Stateful Firewalls

Provide the industry-standard level of protection required at the edge of the network. Unlike simple Access Control Lists (ACLs), a stateful firewall tracks upper-layer flows and ensures that unauthorized traffic cannot bypass access control. For example, a packet claiming to be part of an established Telnet session would be blocked unless there was an actual established session. Aruba's internally-developed firewall has been certified by ICSA Labs under the Corporate Version 4.0 criteria. ICSA's rigorous certification program for firewalls is the recognized benchmark by which all network firewalls are judged.

High-Speed Encryption

Encryption is a critical component of wireless networks, and can greatly enhance security on wired networks as well. Aruba supports a broad array of encryption types, including AES, TKIP, and WEP for wireless; AES-CBC, Triple-DES, and MPPE for VPN; AES-CBC-256 through the xSec protocol for wired or wireless encryption, and SSL forsystem management and captive portal.

Hardware-based Processing

Assures the highest possible level of performance. Aruba mobility controllers have separate control, data, and encryption processors to provide scalability and performance. Firewall rules are processed by special-purpose packet processing hardware in each mobility controller, resulting in no loss of throughput even when complex rule sets are in use.

Automatic Client Blacklisting

Permits the administrator to automatically blacklist – or block from all network access – any client that violates specific firewall rules even a single time. This is particularly useful when single-purpose devices such as voice over IP handsets are used. If the Aruba mobility controller detects a voice handset attempting to conduct database queries or file server browsing, it is likely that the device credentials have been compromised by an intruder. The mobility controller, using automatic client blacklisting, will immediately disconnect the device from the network and generate alert messages to the administrator.

Flexible Policy Creation

Permits firewall policies to be constructed based on identity, source and destination of traffic, service type, time of day, physical location, and even device state when using client integrity software. Policy actions can include permit, deny, redirect to external devices or tunnels, logging, or QoS actions such as setting 802.1p or DiffServ bits and placing traffic into high or low queues.

Control Processor **Packet Processor** **Encryption Processor**

L2/L3 Switch Core
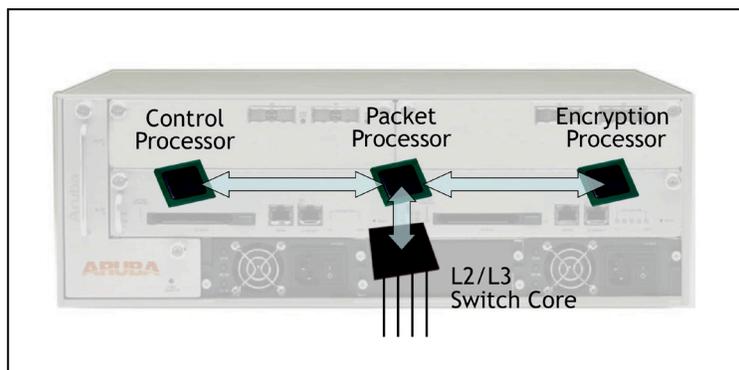
Hardware Architecture

WWW.ARUBANETWORKS.COM

1344 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550