Aerohive NETWORKS

solution brief

Delivering Secure Guest Access and Mobile Internet Device (MID) Management with HiveOS 4.0

Table of Contents

Introduction

Mobile Internet Devices (MIDs) are easily the most exciting development in computing devices in the post-laptop era. By combining portability near to that of a phone with a larger screen, it is possible to interact with much larger data sets and to perform previously inaccessible computing tasks.

Tablets began as tools for wireless network users in traditional vertical markets, especially in health care. From that initial point, they have become much more widely adopted for general enterprise use. The combination of a Smartphone plus a tablet can replace a general-purpose computer for many devices, lowering support costs. Retailers are using MIDs for kiosks to eliminate the need for custom hardened computing devices.

In addition to business use, end users are bringing devices to the office and attaching them to the corporate network. Although many tablets have 3G capabilities, carriers have changed data plan pricing to encourage use of Wi-Fi networks. Many companies are setting up a network for employee-owned devices with limited access as a result.

Together, the strong end-user demand for personal MIDs usage, combined with the business benefits of supporting such devices, has combined to make the product category a runaway success. New devices are eagerly anticipated, and Apple's iPad in particular has been a spectacular success, with 15 million devices sold in the first nine months of availability.

The key considerations for using MIDs on a network are the same as for any other device on a wireless LAN. Security remains a paramount consideration. If network administrators cannot ensure the security of both network communications and data storage with new devices, adoption will be limited. Several tools are available to provide granular access control for MIDs without dramatically increasing the cost and complexity of the configuration process.

Enhancing Network Connectivity for Users on the Move

MIDs boost productivity by making information more accessible to those who need it. For most users, security requirements for MID access will continue to be a high priority. The AES-driven cryptographic core of WPA2 continues to play a central role in protecting data "in flight" across the wireless LAN link. Aerohive has certified the HiveOS WPA2 implementation to ensure compatibility with any other Wi-Fi CERTIFIED device.

Not all devices must be connected with WPA2-Enterprise level security. Aerohive's Private PSK (PPSK) feature provides the security of WPA2 without the complexity of network authentication using RADIUS with certificates. This hybrid between security and configuration is especially important for networks in which guest traffic must be encrypted because the PPSK prevents guests from capturing and analyzing the traffic of other users on the network.

Without local storage, many MIDs depend on consistent and reliable network service. Advanced tablet devices such as Apple's iPad are dual-band 11n devices with the capability to use any available radio channel to obtain network access. Aerohive has built band-steering and high-density capabilities to ensure that network administrators can steer 11na-capable devices like the iPad to the less crowded and higher capacity 5 GHz band, leaving the 2.4 GHz band for low-power devices such as VoIP phones or earlier devices that may not be capable of 5 GHz operation.

Copyright ©2011, Aerohive Networks, Inc.

Service quality is also determined in part by airtime allocation. Aerohive's Dynamic Airtime Scheduling improves application response time for 11n devices like the iPad by prioritizing short bursts of high-speed 802.11n traffic.

User-based access control adds a second layer of security. In the Aerohive system, users are assigned network access privileges that may include VLAN assignment, guest tunneling, or stateful firewall rule sets, along with other parameters. Network administrators can use these features to attach devices to any convenient logical network location.

User access may be subject to modification. Although the user identity provides a baseline level of network access rights, administrators may wish to modify those rights based on the type of device in use. One common method of restricting data leakage on the local storage of laptops is to use virtual desktops, potentially in combination with display-only devices such as tablets. A second defense against data leakage is to prevent personally-owned devices from attaching to corporate resources.

Aerohive's OS detection capabilities allow administrators to modify user access rights based on the type of device in use. Corporate-owned devices that are registered as computers in an Active Directory domain may be given full access to the network and all available resources. Personal devices access the network with the same user credentials as corporate devices, but may be directed to a guest network offering only Internet access. Many MIDs are designed around the assumption of consistent Internet connectivity, and recent changes to data tariffs are motivating users to seek out cheaper Wi-Fi connectivity instead of using relatively expensive wireless WAN connections.

To interact with an Active Directory installation, Aerohive offers a variety of features beyond simple LDAP integration. HiveAPs join the domain and can access the full user information, including a complete list of group memberships. No RADIUS installation or user database replication is required, and there is no dependence on the Microsoft Network Policy Service (formerly known as Internet Authentication Service). HiveManager and HiveOS 4.0 integrated a directory browser that enables a network administrator to walk through the Active Directory looking for particular groups and users.

Usage Scenarios

Configuring an Aerohive network to support a large MID deployment does not require installing software on the devices themselves, obtaining any feature licenses for the Aerohive network, or installing additional network components such as a guest management system or an additional RADIUS server. All features, including device-specific policy enforcement, are included with all Aerohive devices.

Secure Guest Access

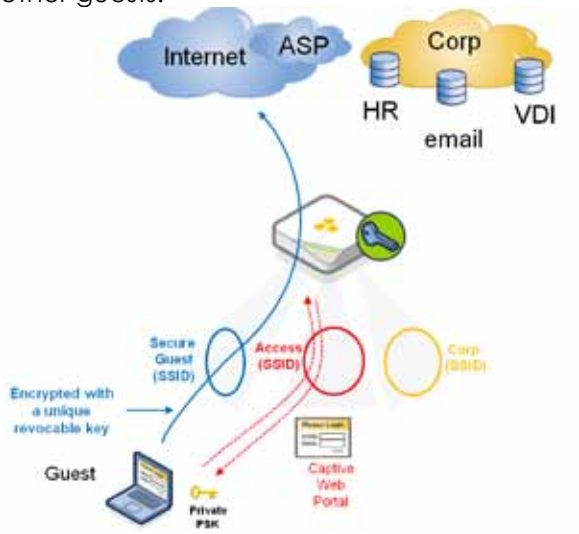
Guest access on Wi-Fi networks has traditionally been controlled through captive web portals. Web-based enforcement of network access does not require new client-side software or extensive user training because it depends on familiar metaphors. It does not, however, protect data flowing over the wireless link, which may leave guest users vulnerable to tools such as Firesheep. Without cryptographic security on the wireless link, accountability is significantly weaker as well. Minimally technical observers can "hijack" a web-based session simply by observing the MAC addresses in use.

Copyright ©2011, Aerohive Networks, Inc.

Aerohive developed Private PSK (PPSK) to make encrypted access easier to deploy and manage. With PPSK, each user receives a unique pre-shared key for network access. Most home networks use WPA-Personal security, making users familiar with entering a pre-shared key.

PPSKs can be generated by the network administrator, or generated on demand through a self-registration page. Instead of asking an administrator or other staff member for network access as a guest, users connect to a setup network and see the following splash page.

As part of the self-registration process, the network supplies a pre-shared key that is tied to a particular user. PPSKs can be changed or revoked for a single user without affecting other guests.



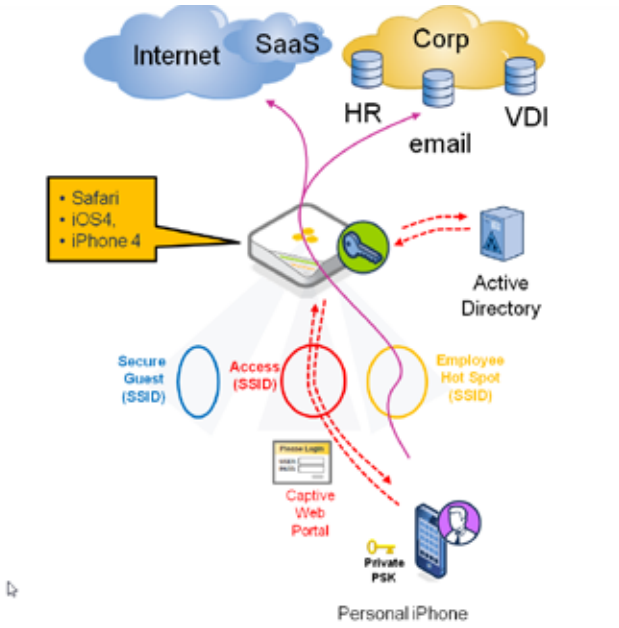
Network administrators can configure access roles based on the building blocks of Aerohive's policy enforcement engine, which go beyond simple VLAN assignment and

Copyright ©2011, Aerohive Networks, Inc.

tunneling to include stateful firewall rules, QoS policies, and configuration Aerohive's award-winning Service Level Agreement (SLA) monitoring of connection quality.

Employee hot-spots

Employees use MIDs to enhance productivity by access corporate resources while on the go, whether within the office or on the road. Many MIDs are multi-mode devices with both a Wi-Fi interface for local access and a WAN interface to provide connectivity over longer distances. The flood of user-generated data from these devices has overwhelmed service providers and resulted in tariffs and data packages that penalize users for excessive use of mobile data and encourage the use of Wi-Fi. Employers have responded by making the office wireless LAN available to "offload" the 3G/4G/LTE network, either for employee satisfaction or out of a desire to directly reduce wide-area data charges they pay directly.



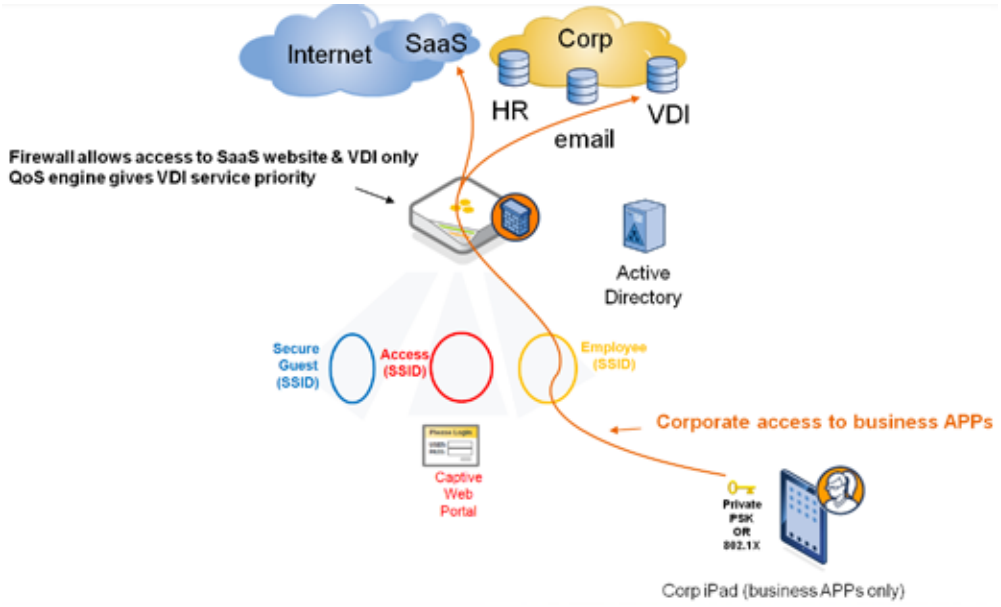
The PPSK self-registration portal described in the previous section can be used in an alternative manner. Instead of registering guests, it can be connected to an authoritative user store to create PPSKs for employees to use on personal devices. Unlike the PPSKs assigned to guest users, employee PPSKs can be configured for access to both the Internet and internal resources.

Network administrators can assign access rights based in part on device type, enabling a single set of corporate credentials to be used for both restricted access on a MID and unrestricted access for a corporate-owned laptop.

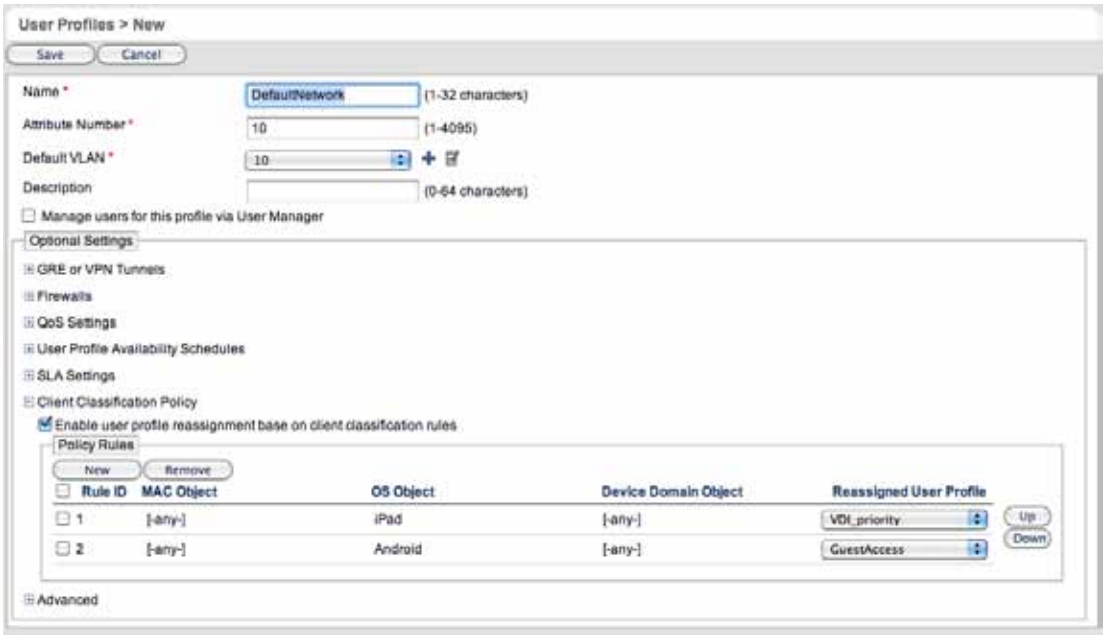
Corporate MID configuration

Corporate-owned devices go through a similar process of registration as personally-owned devices. Typically, the access rights given to corporate devices will be optimized for and restricted to approved applications.

Copyright ©2011, Aerohive Networks, Inc.



As a deployment example, tablet devices are often used with virtual desktop infrastructure (VDI). Data requiring special treatment is securely stored in a data center, and tablets are used as a window into that data. At connection time, the Aerohive network is used to restrict access to only the VDI servers with a firewall rule, and VDI network traffic is given a higher level of access to the wireless medium than data traffic.



Conclusion

From the user perspective, one set of credentials is used on all devices, including MIDs. However, only corporate-owned devices have access to the corporate network. Personal devices can be restricted to only Internet access, or can be given access only to a restricted set of resources such as a virtual desktop infrastructure.

Copyright ©2011, Aerohive Networks, Inc.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901

SB1102006