Meru AirShield Security Suite: A Framework for Assured Mobile Application Delivery

Meru Networks AirShield™ Security Suite Wireless Security Framework

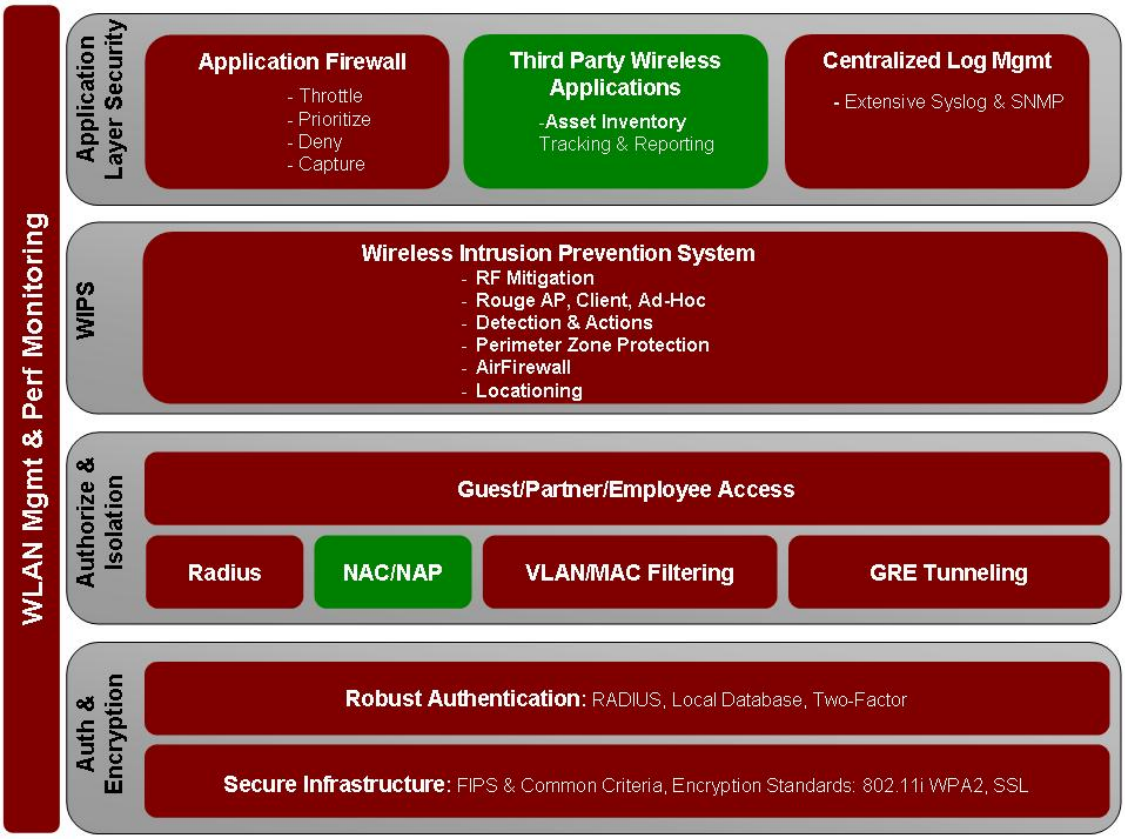
Wireless web access is pervasive. It is rapidly becoming an integral part of everyday life. Expectations are that organizations will provide wireless LAN access and extend it to their business partners for access to key business applications. Fortunately, the wireless LAN is rapidly coming of age, especially so in education and healthcare applications, and it is becoming a viable replacement for the wired LAN. Recognized by Gartner in their 2006 Magic Quadrant Survey as the industry's most visionary vendor, Meru Networks offers the only fourth generation wireless LAN solution to enable the assured delivery of mobile Enterprise applications.

As wireless becomes more prevalent in enterprises, however, legitimate concerns about security and reliable service must be addressed. Today more than ever, it is crucial that key mobile business applications are delivered securely and scaleably to employees and business partners. As a result, for the wireless, as well as for the wired LAN, IT administrators need to establish and implement security and application availability policies that facilitate these productivity-enhancing networks.

Meru AirShield Security Suite is the first wireless LAN (WLAN) security solution providing application-based security for ALL classes of applications—traditional, end-to-end, encrypted, and new peer-to-peer in converged voice and data networks. This patent-pending, innovative security technology allows network administrators to assign and enforce firewall policies for encrypted traffic and peer-peer applications, an industry first. Additionally, Meru AirShield Security Suite provides comprehensive security capabilities based on application, user and location data to control access to corporate assets and confidential information.

Meru AirShield Security Suite enables enterprises to implement wireless security policies while simultaneously ensuring the reliable delivery of all types of applications in a pervasive mobile workplace over a Meru wireless LAN infrastructure. AirShield recognizes that security is not the end-goal in-and-of itself, but rather that it is the key building block in providing the assured mobile application delivery to your business partners and employees. AirShield makes it a reality by weaving WLAN management and performance monitoring into the wireless security and application availability framework to deliver a layered security solution. It allows close monitoring of the potential impact of various security outbreaks such as Denial of Service floods, viruses and worms on wireless application availability. Additionally, the AirShield security framework enhances and extends the best practices of wireless security, authentication and encryption, authorization and isolation, and Wireless Intrusion Prevention Systems (WIPS), by providing a unique application security layer. In doing so, AirShield is the industry's first and only solution that empowers organizations to plan and implement a strong and extensive wireless security posture as a part of an overall mobile application strategy which includes business-critical applications like wireless voice over IP (VoIP).

Figure 1. Wireless Security Best Practices Framework



Red color is used to indicate Meru developed solutions and green the interoperable third party solutions.

Authentication and Encryption

Legacy approaches to protecting the wireless network meant slapping IPSec VPNs on the top of insecure wireless networks. This is unnecessary and inefficient nowadays with the advent of WPA2 for encryption and 802.1x for authentication, which taken together offer a more appropriate fit for securing wireless networks. Customers are increasingly embracing this paradigm and the need for deploying IPSec VPNs for this purpose is becoming a thing of the past. Additionally, most enterprises have already chosen to deploy IPSec solutions by selecting the solution from a specialized vendor. Meru endorses this approach, rather than requiring customers to invest in additional wireless IPSec VPN solution since it reduces the inefficiencies and administrative burden of installing and maintaining two disjointed solutions.

Meru's AirShield offers a variety of the authentication and encryption methods spanning from convenient and easy to deploy local database authentication, to robust two-factor authentication. This layer offers a high level of security and provides the foundation for the other wireless security layers.

Authorization and Isolation

The enterprise is challenged to open up the network to the high number of employees, partners and guests. AirShield's Authorization and Isolation security layer allows organizations to achieve this in a secure and controlled manner. The components of this layer work together to seamlessly provide controlled and separated access for guests, partners, and employees. For example, guests or partners can access the network through the captive portal, which provides role-based traffic separation through Generic routing-encapsulation (GRE) tunneling and Web-based authentication method (SSL).

When a guest user tries to associate with an access point, he is redirected to the captive portal authentication page where his credentials are checked and the privileges determined. During authentication and authorization all traffic, with the exception of the subset needed for authentication, is dropped, user's privileges are verified, and the security state of his wireless access device assessed. Based on that information, the user is authorized onto the appropriate VLAN partition. During the session, AirShield records the activity of guest users while connected to the enterprise network.

Assuring security on the wireless endpoints is also a major concern. To achieve endpoint security and assure that only the devices passing the corporate health check can access the network, the corporate-issued wireless devices need to be checked on a regular basis. Non-conforming devices may need to be quarantined and brought into policy compliance before these wireless clients can gain access to internal networks. Meru assures that customer benefit from the best-of-breed Network Access Control (NAC)/network Access Point (NAP) solutions by partnering with the leading vendors and jointly developing and testing the solutions.

Wireless Intrusion Prevention System (WIPS)

AirShield's WIPS module secures the network from the Denial of Service (DoS) and the common wireless security exploits attacks through a unique tiered solution. It also monitors their impact on overall network performance. Wireless IPS is not a complete replacement for the wired IPS but rather augmentation to it. Established wired IPS solutions can't always detect attacks originating from the wireless network nor can they mitigate against such attacks. In many cases wireless exploits, while related to the wired exploits, are not identical. Some exploits are specific to the wireless domain and can be best identified and prevented as such.

AirShield's WIPS offers a tiered approach to wireless security and timely response to intrusions in a distributed office environment. Meru's Wireless IPS protection starts at the network perimeter through its AirFirewall™ component, which protects through over-the-air countermeasures. AirFirewall three main building blocks are: RF-Mitigation, Micro-scanning and Location hiding. RF Mitigation prevents hackers & rogue APs by scrambling signals of unauthorized devices. Micro-scanning offers 100% concurrent service and scanning for Rogue APs. Additionally, Location Hiding hides the enterprise assets and devices from hackers.

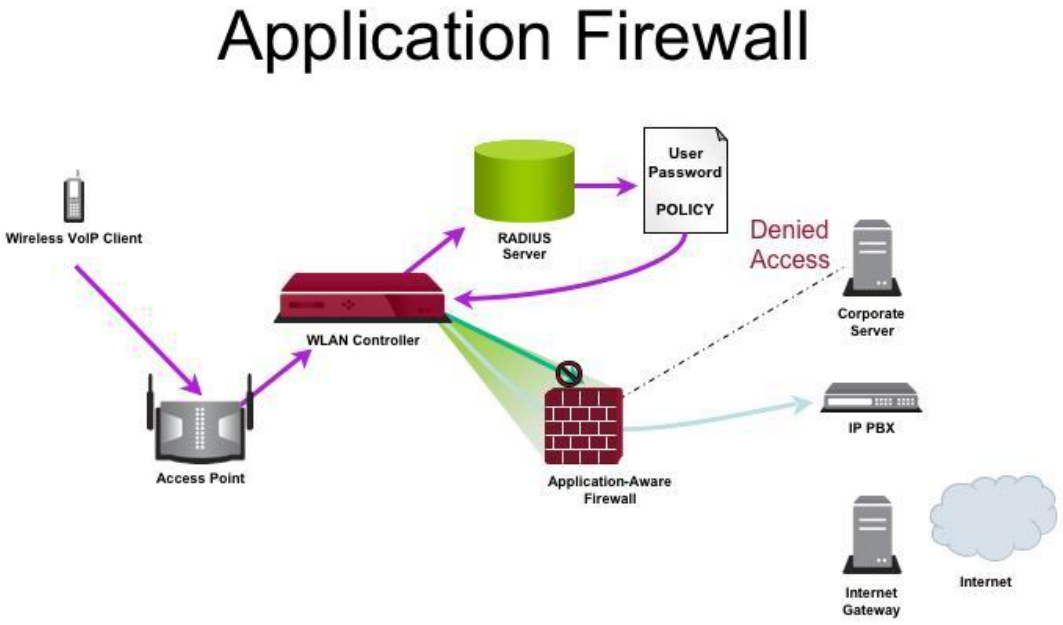
AirFirewall effectively denies unauthorized traffic and management frame DoS attacks from even accessing the network. Also it is able to simultaneously scan, analyze, and act on the security threats it detects. Besides DoS protection, the rogue detection and mitigation is built into every Meru network. Access Points are continuously scanning while attending the voice and data traffic to detect anomalous or harmful clients and behavior. They quarantine the compromised clients while preserving WLAN performance and bandwidth. Meru wireless IPS solution is very efficient and never adds incremental RF traffic just to mitigate rogues.

AirShield's Wireless IPS interoperates with the external monitoring third party tools such as Security Event Monitoring (SEM) and wired IPS. Organizations benefit by centralizing the security monitoring for both wired and wireless networks and receiving an extensive set of the compliance reports for SOX, PCI and GLBA.

Application Layer Security

AirShield application layer security provides a critical line of application layer defense against malicious Denial of Service (DoS) wireless network attacks as well as against the misuse of wireless bandwidth by non-business critical applications such as BitTorrent™ and YouTube™. This layer is composed of the three main components: AirShield application firewall, centralized log management, and wireless security applications.

Figure 2. VoIP Unauthorized Application Server Access



The application aware firewall offers a unique application traffic flow classification mechanism. It can distinguish applications by their unique flow characteristics, based on the packet length range and inter-packet arrival times. Once the traffic-flow is auto-classified, the encrypted and proprietary applications can be isolated and blocked. This comes in handy if you need to protect your corporate network resources from potentially harmful and bandwidth hungry peer-to-peer applications. Instead of allowing the wireless bandwidth to be eaten up by non-business critical applications or hijacked by hackers, you can free up the wireless bandwidth for legitimate business applications delivery. AirShield can do this very efficiently as the core engine is built around traffic classification for both voice and data traffic and shared with the wireless Quality Of Service (QoS) engine. The application traffic flow is classified and tagged with QoS parameters and priority parameters and the users' role privileges are applied. As a result, the traffic is denied, rate limited, quarantined or prioritized based on device, user and corporate usage policies for a given application freeing up the network pipe for business critical applications. Application Firewall further strengthens security, without compromising application performance, and provides strong application and user-aware policy-based security for large enterprises.

Extensive logging and centralized log management assures that key information on who did what and when is logged and available to feed into applications that monitor system security and as input into the third-party reporting products such as security intelligence and event monitoring (SIEM) applications.

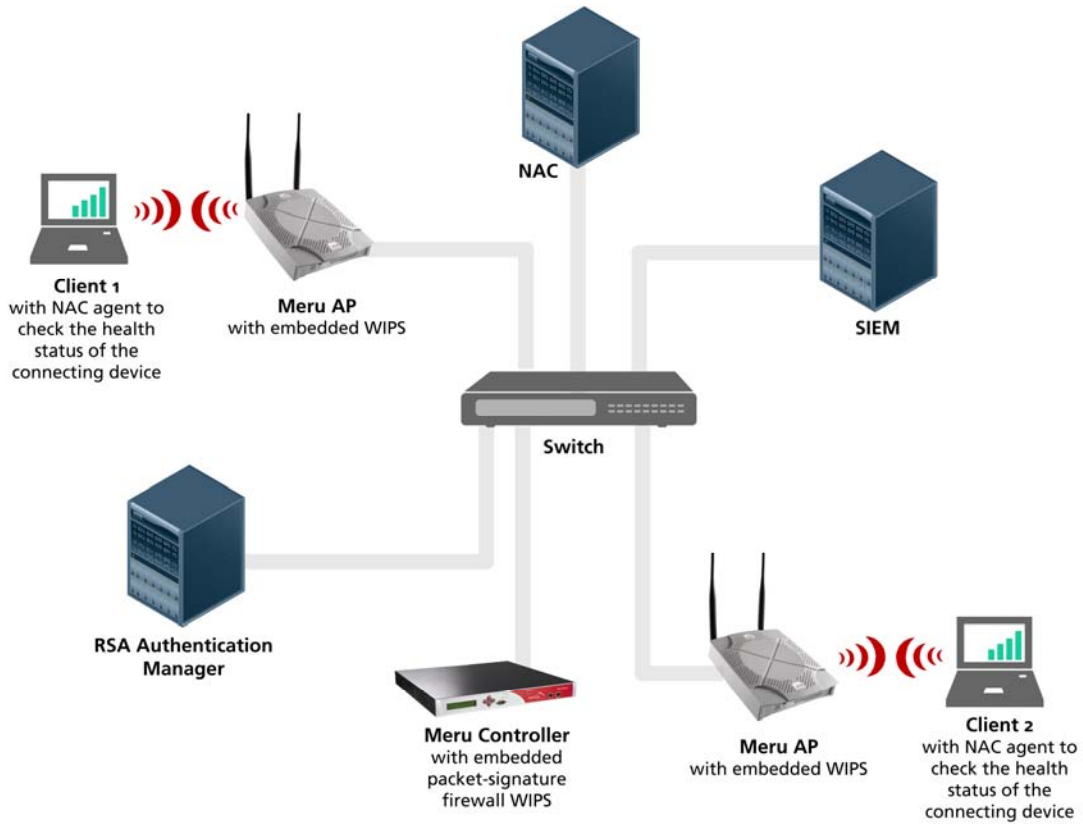
The main focus of the wireless security applications is providing the asset tracking. Assets need to be inventoried and kept closely monitored. Wireless devices such as PDAs are expensive and the cost of the shrinking asset pool can quickly add up even for smaller organizations. Having an accurate inventory of wireless assets also allows organizations to quickly distinguish friendly client wireless device from foe.

In summary the advanced features of the application Layer solution include:

- Packet signature-based inspection provides accurate detection of traffic based on packet length and inter-packet arrival times
- Packet signature-based policy enforcement for rate limiting and providing specific QoS for the flow and dropping undesirable traffic
- Packet signature-based firewall for classifying, isolating and blocking encrypted and proprietary applications

Meru AirShield reduces the total cost of ownership by reducing the operational and capital costs associated with a converged network for voice, data, and location. This product allows network managers to maintain better control over the airwaves, a constrained resource, in the face of peer-to-peer applications. By efficiently reserving bandwidth for business critical applications, this product reduces the number of redundant networks needed to serve clients and frees IT staff to focus on more critical needs. Additionally, the per-user, per-application, per-location level of security provided by this product enables more sensitive applications to be accessed via the wireless network, allowing for greater user mobility and improved productivity, customer responsiveness and delivery of services. Finally, Meru's unique multi-layer approach requires few access points, saving the customer capital equipment costs and deployment costs.

Figure 3. Overview of Meru Secure Wireless Solution



Summary

With the pervasiveness of wireless technologies, organizations are seeking a comprehensive and robust WLAN solution that allows them to provide assured application delivery for business-critical voice and data applications. Meru's wireless LAN solution, coupled with its AirShield offering does that while integrating multi-layer wireless security. AirShield delivers an industry leading and innovative solution for securing wireless LANs and covering the critical areas of Authentication and Encryption, Authorization and Isolation, Wireless Intrusion Prevention System (WIPS) and Application Security.

Summary of AirShield Benefits

- Meru AirShield Provides Best-In-Class, Layered Security:
  - Authentication and Encryption
  - Authorization and Isolation
  - Wireless IPS
  - Application Layer Security
- Unique ability to ensure voice quality when security scanning
- Scalability—Smart Access Points eliminate bottlenecks by distributing crypto processing
- Cost-Effectiveness—Provides wired security services while integrating WLAN-unique security features and leveraging existing investments in Firewall and VPN solutions
- Traffic Signature-based Firewall—Provides security, without compromising application performance
- Controlled guest user access—Provides policy enforcement and auditing services