SECURITY & COMPLIANCE

SECURITY & COMPLIANCE

The Meru solution features a wide range of security measures to protect your confidential data and aid in compliance. Extensive security features are built in to Meru products, with additional security functions available as add-on options.

SECURITY AND COMPLIANCE OVERVIEW

Enterprise security is among the top priorities for IT departments today. To give you control over your security posture, a broad range of security features is built in to the Meru architecture. Meru provides secure connectivity with full support for WPA2 Enterprise and IEEE 802.1X. Your data is protected with enterprise-class authentication, authorization control, and encryption. A per-user firewall provides granular control over policy settings, with applications recognized through flow signatures as well as deep packet inspection. Meru supports industry standards TACACS+ and RADIUS for WLAN access control, enhancing security and scalability. The System Director operating system detects and mitigates rogue access points, and access points continuously scan for intruders. The AP110 Virtual Office Access Point includes integrated TLS-VPN encryption to ensure secure wireless and wired access for home office and small branch office environments.

For further assurance, Meru provides the option to add additional security and compliance functions:

- Meru Identity Manager is an identity-based software platform for provisioning and managing secure access for guests and for employee- and corporate-owned devices
- Meru Wireless Intrusion Prevention System (WIPS) Module is fully customizable and comes with a base set of signatures corresponding to common wireless attacks
- PCI Compliance Manager Module audits and verifies a network's security posture to ensure PCI compliance

Benefits

- Puts you in control of your security posture
- Protects your network and confidential data
- Delivers secure access for guests, employees, and their mobile devices
- Prevents attacks on the WLAN
- Aids in achieving compliance

Meru Security and Compliance Features

A broad range of built-in and optional measures secures your Meru wireless LAN, protects your confidential data, and aids in compliance.

Secure Connectivity	Authorization	Intrusion Prevention	User, Device, and Application Security
• WPA2, WPA • 802.1X, PEAP, LEAP • VPN from remote offices	• RADIUS • MAC-based • Captive portal	• Rogue AP detection and mitigation • Wireless IPS/IDS	• Per-user and application-aware security policies • Policy-based control of devices • Guest lifecycle management • 802.1X provisioning for client devices • PCI compliance

SECURITY & COMPLIANCE TECHNICAL SPECIFICATIONS

STANDARD SECURITY FEATURES

Authentication
Combination of 802.1X and open authentication
802.1X with EAP-Transport Layer Security (EAP-TLS), Tunneled TLS (EAP-TTLS), Protected EAP (PEAP), MS-CHAPv2, Smartcard/Certificate, Lightweight EAP (LEAP), EAP-FAST, and EAP-MD5, with mutual authentication and dynamic per-user, per-session unicast and broadcast keys
Secure HTTPS with customizable captive portal utilizing RADIUS

Encryption Support
WPA2 Enterprise Certified
802.11n: Full support of 802.11i with dynamic AES keys
802.11/a/b/g: Static and dynamic 40-bit and 128-bit WEP keys, TKIP with MIC

Security Policy
Access control entries supported based on user identity, location, group membership, application, or SSID
Multiple ESSID/BSSID, each with its own security policy
Granular management of multiple security policies

Dual Radios
Centralized, continuous rogue access point detection and suppression/permit for 802.11a/b/g/n

Firewall
Deep packet inspection for application-aware policies
Per-user firewall

MERU COMPLIANCE

Auditing and Analysis
Automatic discovery and inventory of wireless assets and configurations
Historical and on-demand reporting based on Payment Card Industry (PCI) Data Security Standard (DSS) v1.2
Comprehensive analysis of failures in PCI compliance

Policy Verification
Strong encryption of data transmitted over the air
Firewall set to default deny posture
Passwords changed from vendor defaults
Discover and remediate security vulnerabilities
Restrict access to cardholder data by business need to know
Restrict physical access to cardholder data

Tracking and Monitoring
All actions taken by users with root or administrative privileges
Access to all audit trails
Invalid login attempts
Use of identification and authentication mechanisms
Initialization of audit logs
Creation and deletion of system level objects

WIRELESS INTRUSION PREVENTION

Configuration
Action taken upon detection of each threat fully customizable
Support for custom signatures to deal with new threats as well as any threats unique to a given enterprise
Intuitive web GUI or powerful CLI

Reporting
Dashboard shows trends based on threat severity, time, and location
Alerts when security issues are detected
Automatically generated reports of security posture and attempted malicious activity or potential threats on demand or according to regular schedule

Included Signatures
Adhoc Network
Antistumbler
Association Flood
Authentication Flood
Channel Hogger
De-authentication Flood
Disassociation Flood
EAP Handshake Failure
EAPoL Logoff Flood
EAPoL Start Flood
Fake AP
Fragmentation and Re-Assembly
Large Duration ID
MAC Spoof
Null Probe Response
Overutilized AP
PRGA
Rogue AP
Too Big SSID
Unregulated Channel
Ability to disable unused radios via software to lower power consumption

ADDITIONAL HARDWARE AND SOFTWARE REQUIREMENTS FOR OPTIONAL MODULES

Identity Manager
Hardware Appliance: SA200 or SA2000 Services Appliance
Virtual Appliance minimum specifications: 1 GB memory, 20 GB disk space, 2.0 GHz CPU, VMware ESX/ESXi 3.5

PCI Compliance Module
SA2000 Services Appliance (also requires E(z)RF™ Network Manager software license)

Wireless Intrusion Prevention System (WIPS) Module
SA2000 Services Appliance (also requires E(z)RF™ Network Manager software license)

Meru delivers an all-wireless network that fully supports the enterprise, delivering a consistent, interactive experience for all users. No matter what applications they are running. No matter how many other users are on the network.

For information about Meru Security, visit | www.merunetworks.com | Or email your questions to: info@merunetworks.com

Meru NETWORKS®
Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089
T +1 (408) 215-5300
F +1 (408) 215-5301
E info@merunetworks.com