POLICY ENFORCEMENT

POLICY ENFORCEMENT MODULE

Enforce Firewall and Quality of Service Policies on a Per-application, Per-group, and Per-user Basis.

PRODUCT OVERVIEW

Security policies require managing and restricting access to network resources based upon users' roles in the organization. Organizations also have bandwidth and quality of service (QoS) policies for managing capacity usage. These policies enable them to optimize available bandwidth while providing QoS that meets or exceeds business requirements. The Meru Policy Enforcement Module for the System Director operating system gives you the power to efficiently apply these policies to govern your wireless LAN. It extends your control and lets you deliver required service levels to end users while restricting access to network resources to appropriate levels.

PER-USER POLICIES AND ROLE-BASED ACCESS CONTROL

The Policy Enforcement Module enables you to quickly and easily firewall users and applications. A network user within the marketing organization can be restricted from accessing resources within the finance organization, while an IT administrator can be granted full access to all resources.

Any use of wireless resources for non-essential data transfer is airtime stolen from business-critical operations. WLAN administrators must limit spectrum usage while ensuring that no users or applications are starved for bandwidth. Using System Director's bandwidth management and throttling capabilities, the Policy Enforcement Module enforces policies designed for each user as determined by existing corporate authentication infrastructure such as RADIUS or Microsoft Active Directory. This way, users access the network based on predefined policies appropriate to their role and/or their physical location.

With Meru's application-aware QoS and over-the-air optimization, every application can be dynamically assigned different QoS levels using predefined role-based policies. This helps to ensure that required service levels are provided for each application, which is critical in environments where many users and devices are competing for the same network resources.

Features	Benefits
• Quality of service and network access policy enforcement • Define policies on a per-user, per-group, or per-application basis • Generic Routing Encapsulation (GRE) tunneling • Web authentication pass-through • Integrates with authentication infrastructure tools such as RADIUS and Active Directory	• Prioritizes wireless traffic to optimize available bandwidth • Delivers granular control over access to network resources • Segregates guest traffic from corporate traffic • Ensures security and flexibility of the wireless LAN • Supports existing infrastructure investments

POLICY ENFORCEMENT

WEB AUTHENTICATION PASS-THROUGH

Web authentication is the most expedient means to enforce authentication on a WLAN network, especially when devices connecting to the network are unknown or not provided by the IT organization. If the user has valid credentials, they can enter their username and password on a special web page known as a captive portal and gain immediate access to the network. If users are using other, stronger forms of encryption and authentication such as VPN and do not need more authentication, captive portal can allow them to pass through. When network resources like servers need to be accessed across the WLAN and through the captive portal, web authentication pass-through prevents additional administrative burden while avoiding disruption for pre-configured users and applications.

GENERIC ROUTING ENCAPSULATION (GRE) TUNNELING

While it has become critical for enterprises to provide network connectivity to guests and visitors, it may not be in the best interests of the enterprise's security policy to allow outsiders to share the corporate WLAN. In this case, GRE tunneling capability enables you to provide Internet access without allowing access to corporate data. The controller forms a GRE tunnel with a remote end point that can be an Internet router or a firewall. Using the GRE tunnel, guest traffic is tunneled directly to the Internet without sharing the corporate network. Using GRE, a widely supported secure tunneling protocol, you can rest assured that the security policies of your organization are being enforced and that corporate data is secure.

Module Part Numbers

MC1500-PEF
Policy Enforcement Module License for Meru MC1500 Controller. License enables features for all access points on the controller.

MC3200-PEF
Policy Enforcement Module License for Meru MC3200 Controller. License enables features for all access points on the controller.

MC4200-PEF
Policy Enforcement Module License for Meru MC4200 Controller. License enables features for all access points on the controller.

MC5000-PEF
Policy Enforcement Module License for Meru MC5000 Controller blades. One license required per controller blade. Up to 5 licenses per chassis.

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 more information about the Meru Policy Enforcement Module 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