

# The Mako System

## Small-site and branch office networking solution

The Mako System offers a centrally managed, turnkey solution to create broadband networks for small sites. With anytime, anywhere access, the Mako System offers real-time management, reporting and proactive security in one solution.

The Mako System is a combination of two parts: a network appliance and hosted Central Management System (CMS). These components work together to provide a complete network connectivity and management service, enabling you to connect, protect and control your network(s). It's not just another router and firewall.

### Mako Appliances

Mako appliances offer the choice of WAN interfaces including 3G, Ethernet and ADSL2+. There is a Mako appliance to suit any small site's requirements, and Mako Virtual Private Network (VPN) concentrators can link them back to a central or corporate network (see separate hardware appliance specifications for specific details). Mako appliances ship with proprietary software incorporating a default configuration, which enables them to connect to the Internet, communicate with the CMS and retrieve their customer-specific configuration. Once online, Mako appliances connect directly to the Internet and communicate regularly with the CMS using a patented communication method.

### The Unique Mako Central Management System

The Mako CMS is accessed via a secure website that users log into to manage their network(s). A user's login gives them access to all their Mako appliances around the world, providing a central place from which to manage their complete network.

With Mako Networks' CMS, you or your designated IT Professional have 24-hour secure remote control over your connection(s) to the Internet or connections between sites. Via Mako Networks' website, you can modify firewall rules, connect sites via VPNs, check usage patterns and even change your network's IP addressing.

### Benefits of Hosted Central Management

- No hosting or management hassles
- Support can be provided by multiple parties
- No requirement for technical personnel on-site
- Remote configuration and deployment
- Easy to understand graphical interface
- Automatic security, software and features updates
- Real-time reporting and control of Mako appliances
- Diagnostic suite ensures quick, remote resolution of issues, and reduces helpdesk calls
- Remotely manage multiple sites easily

### Firewall

Paramount to the security of your network(s) is the type of firewall you use. Mako appliances utilise an ICSA-certified stateful inspection firewall that examines packets of information, and makes decisions based upon information derived from all communication layers and other applications. Online inbound and outbound security controls let you choose what traffic enters and leaves your network(s).



### VPNs

Virtual Private Networks (VPNs) allow you to connect remote sites over the Internet. Offices can be securely linked together using Mako Networks' CMS in seconds with just three mouse-clicks. This can be extended to specific users to allow them to remotely access your network(s) with the Remote VPN feature. VPNs eliminate the need for expensive leased lines, reduce telephone charges and lower support costs.

### Patented Communication Method

The Mako communication method makes it possible to have a hosted, Internet-based management system that receives traffic information from individual Mako appliances and then analyses, interprets and reacts to that information. The communication method eliminates the need for on-site configuration, with authenticated users accessing the CMS via the Internet to interact with their Mako appliances.

Unlike traditional management platforms, communication with the management system is initiated by the endpoint, thus negating the need for static IP addresses and individually pre-configured appliances. Every two minutes, each Mako appliance checks with the management system if there is a need for configuration changes or firmware updates. The Mako appliances also transmit raw traffic logs to the CMS for automatic interpretation and analysis.

### Proactive Alerts

The Mako CMS automatically provides proactive alerts for extraordinary usage, unit offline, worm detection and hardware triggers such as fan speed and CPU temperature. The CMS also sends monthly reports on usage, intrusion attempts and easy-to-read companywide summaries for end-users with multiple sites.

### Automatic Updates

Mako automated software and firmware upgrades mean that new services and increased functionality are added to the platform on an ongoing basis. Mako appliance software is proactively patched and updated immediately upon authentication and availability, providing unparalleled reliability and security without manual intervention.

### Diagnostics

Mako Diagnostics give support personnel the ability to remotely resolve network and connectivity issues without the need for onsite visits or technically literate users. Mako Diagnostics reduce support costs by allowing the helpdesk to very quickly identify and resolve problems all the way to the Mako appliance level.



### PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) rules have been designed to protect banks, merchants and cardholders from falling victim to credit card fraud. PCI DSS outlines how a merchant should protect their point of sale network and ensures security is maintained on an ongoing basis. Mako Networks is the world's first PCI DSS-certified Network Management Service.

The Mako System lowers the cost and complexity of PCI DSS compliance by automating network security and nearly every other process of a merchant's PCI DSS compliance.



With proactive alerts, merchants using the Mako System cannot mistakenly put themselves at risk of non-compliance. Any attempt to inappropriately modify the network configuration will generate a warning and require the user to confirm the modification by entering an authorising password.

A merchant can force a non-compliant change if they so wish. Authorising this type of change will generate an alert to their acquiring bank. Email alerts of non-compliance can be sent to any appropriate party including bank, merchant, IT provider and/or Qualified Security Assessor (QSA). This eliminates the guesswork on what a merchant can change within a PCI DSS controlled environment.

Mako Networks provides a QSA-designed website which can deal with almost all remaining aspects of merchant PCI DSS (documentation, policy and process), leaving the merchant only having to take care of physical security.

Mako Networks is the solution for card-present merchants transacting over IP, providing peace of mind to cardholders, merchants and their banks. The Mako System enables a merchant to more easily comply with all of their PCI DSS obligations. Many merchants lack the technical knowledge required to correctly implement the PCI DSS requirements and buying in that experience is expensive using traditional solutions.

### Key Benefits of Choosing The Mako System

- Rapid deployment of new offices or sites
- Easy management of multiple sites
- Access to your network 24/7 remotely and securely from any internet connection
- Summarised easy to understand monthly reports emailed to you
- Detailed reporting available online, anytime/anywhere
- Complete control and visibility of your networks
- Enterprise level security protecting against worms, spam, viruses and malware
- No manual security or feature updates – it's all automatic
- Lower cost of network management and maintenance and increased network uptime with comprehensive diagnostic and management tools
- IP Transitioning in a PCI DSS compliant manner