Mako Networks/Fortinet Comparison

Mako Networks offerings overlap with some of Fortinet's but Mako has a much more focused solution for the distributed enterprise. The Mako hosted CMS makes for easier deployments and enables large deployments to be spread across multiple service providers.

Mako Networks solutions are targeted at distributed enterprises with features and functions designed specifically to deliver benefits across multi-thousand site estates including those that are supported by MNSPs and/or franchised and thus complicated in structure.

Fortinet has a wide range of products spanning the enterprise through to small business. Their product set aimed at the distributed enterprise has traditionally been sold through MNSPs. This document compares the Mako System with Fortinet products aimed at the distributed enterprise.

Both Mako and Fortinet have their own hardware devices that are cloud managed. The Mako Central Management System (CMS) is designed to be fully utilized by distributed retail enterprises and franchise groups where different levels of access to retailer LANs and WANs are required. The CMS simplifies deploying and managing large numbers of customer sites consistently and securely, with features including Enterprise Templates (ETs) and cascading security profiles, which allow for role-based, nested security access across multiple entities. Mako also offers PCI-certified templates, reviewed by a QSA to assist merchants in meeting PCI obligations in a streamlined and highly effective way.

The FortiManager product enables cloud management of Fortinet firewalls, switches and access points. FortiManager is NOT hosted by Fortinet. Fortinet also have FortiCloud which offers a subset of the FortiManager functionality in a hosted environment. Anyone wanting full cloud management of Fortinet devices must host **and secure** their own instance(s) of FortiManager burdening the client with additional costs for hardware and software support and maintenance. Fortinet's FortiManager is designed to be used by core IT personnel and offers less flexibility in access levels and template-based security.

Mako technology was designed from inception around network security across any available broadband, (including cellular) and was created to support thousands of remote locations for thousands of unique customers. Fortinet technology was built primarily to deploy to SMB locations and is more recently focusing on the mid-market.

Fortinet is a public company with extensive distribution and gains access to many opportunities a smaller independent business like Mako does not. However, Mako is highly agile and development cycles can be dynamic, even to the point of being reactive to specific customer and partner requirements.

Mako devices have specific variants designed for the market being served, whether that be for US or other global markets. For example, xDSL using customer-supplied equipment is prevalent in the UK and Europe but not the US. Fortinet delivers a single US-centric solution internationally. Mako is headquartered in the US but was founded in New Zealand and has significant international experience.

FEATURE/FUNCTION	MAKO	FORTINET
Target Market	Distributed enterprise with a strong focus on the distributed retail enterprise. Mako's DNA is distributed networking security.	SMB and mid-market with a strong focus on MNSPs. Fortinet's DNA is enabling MNSPs to deliver network security to SMBs.
Role-Aware Cloud Management	Yes. Mako CMS is designed to be accessed by users throughout the distributed enterprise and incorporates role-based user control to ensure users only get access to the Mako devices and functionality they need.	No. FortiManager is an all-or-nothing service which usually means only a limited number of IT personnel have access – typically an MNSP. This model limits the value proposition of cloud management in larger organizations.
No Localized Management	Yes. Mako devices may only be configured via the Mako CMS. This architecture is a key reason why the Mako System carries a PCI DSS certification. Mako devices do not have default usernames or passwords.	No. Fortinet devices can be configured locally as well as via the cloud. This capability requires additional physical security to be implemented to ensure devices cannot be manipulated by bad actors. This also provides a local attack vector for exploitation.
No Reset Button	Yes. Mako Security Gateways do not have a reset button. This enhances physical security and ensures configuration cannot be removed should a bad actor have physical access to the device. Mako devices are "reset" via the CMS which requires an appropriate level of MFA-controlled access.	No. Fortinet devices have a local reset button requiring additional physical security to be implemented to ensure devices cannot be manipulated by bad actors.
PCI DSS Certification	Yes. The entire Mako System carries a PCI DSS Service Provider certification. This certification makes it easier for a distributed enterprise to meet many of their PCI obligations (and for a Mako partner to deliver such services).	No. Fortinet does not have a PCI DSS certification. Like many networking solutions, Fortinet technology can be made PCI compliant by configuring (and maintaining) devices appropriately, placing significant burden of risk on Fortinet partners and end clients. Fortinet is not subject to external security assessment.
Enterprise Configuration Templating	Yes. Mako functionality includes the ability to create layered configuration and security templates to enable fast and consistent configuration across large deployments. Mako ETs may be used to restrict CMS configuration access to the templated content from users below the template owner (e.g., a retail brand may use a Mako ET to ensure their branded retail locations' POS environments cannot be overridden by their dealers).	Yes. Although Fortinet has limited templating capability suitable to the distributed enterprise compared to Mako. Fortinet's architecture does not support role-based access throughout a distributed organization to the same extent that Mako's does.

FEATURE/FUNCTION	MAKO	FORTINET
Extensive Diagnostic Toolset	Yes. Mako CMS delivers a wide range of diagnostic tools to assist help desk and technical personnel troubleshoot all aspects of Mako devices and WAN connectivity. Users cannot remotely access a Mako device. Diagnostics are run via the CMS which reaches out to a Mako devices and presents the diagnostic result to the user in their web browser.	Yes. Fortinet diagnostics are not as extensive as Mako and proper troubleshooting usually requires SSH access to the device. This type of access reduces the security of the device and makes troubleshooting more difficult and cumbersome.
Cloud Management	Yes, with complete control over all aspects of a Mako device.	Yes, but care must be taken to keep local changes and cloud changes in sync. FortiManager must be hosted, managed and secured by the end user or MNSP. FortiCloud is hosted by Fortigate but is not PCI DSS compliant and does not offer the full functionality of FortiManager.
Integrated Cellular	Yes, most Mako Security Gateways feature built-in commercial grade cellular modules with extensive diagnostics.	Yes, but only a small number of Fortinet devices incorporate built in cellular. Fortinet has a separate device called a FortiExtender or a third-party cellular router are more commonly used.
Hardware Devices Supported	Security Gateways, Managed Switches, APs, VPN Concentrators	Security Gateways, Managed Switches, APs, VPN Concentrators, Anti-virus, Email Protection
SD-WAN/VPN	VPN Cloud delivers multiple levels of redundancy and resiliency including geographic, device and circuit. Mako supports zero-packet loss VPNs for uninterruptable data streams, e.g. VoIP calls.	Traditional VPN options with routing protocol support.
Licensing	Simple, delivers most functions as standard. Pricing is in the medium range for the target market.	Complex and difficult to understand. Pricing is in the high range for the target market.
Security	Next-generation stateful-inspection firewall with IDS/IPS capability. Mako's approach of no local configuration and no reset button adds significant physical security.	Next-generation stateful-inspection firewall with IDS/IPS capability.
Deployment	Tools for large scale deployment included. Multi-thousand site deployments common.	FortiManager has tools to simplify deployments. No specific toolset for very large deployments.