

McAfee UTM Firewall Control Center

Single-Point Security Management for Large, Distributed Enterprises



The McAfee UTM Firewall Control Center gives network administrators and managed service providers a browser-based solution for remotely configuring, monitoring, and maintaining hundreds or even thousands of McAfee UTM Firewall appliances.

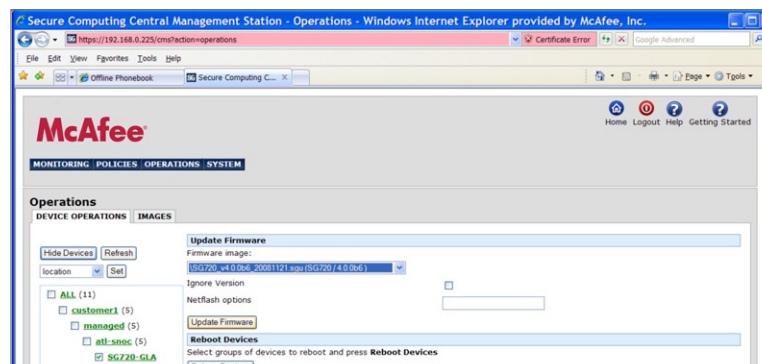
McAfee UTM Firewall is the perfect security choice for organizations that operate distributed environments, such as retail point-of-sale locations, franchises, and branch or small/home offices with remote access requirements. These appliances offer highly flexible and affordable options for delivering unified threat management, firewall, and VPN functions to any site.

As the number of distributed security devices increases, maintaining a consistent security policy becomes more difficult and time-consuming. As you attempt to coordinate protection across all appliances, manage firmware updates and diagnose network faults, the risk of overlooking potential security gaps increases. McAfee UTM Firewall Control Center is designed to meet these challenges and put you in charge, no matter how far away or how widely distributed your McAfee UTM Firewall appliances may be.

With McAfee UTM Firewall Control Center, you control them all with a single, virtual appliance that operates securely over the web using HTTP/HTTPS and TLS/SSL.

Software Updates and Firmware Repository

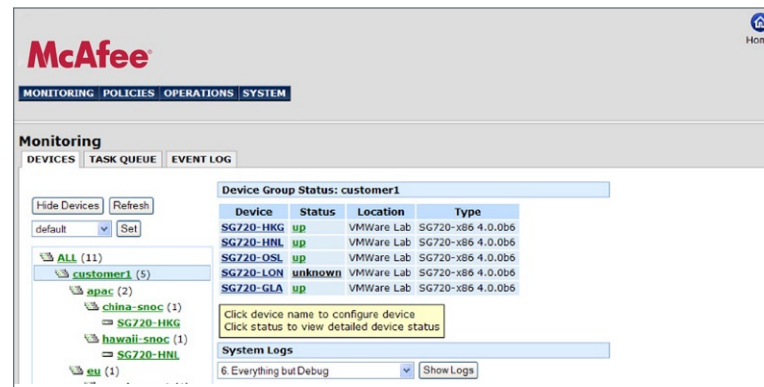
Manually updating each security appliance in your organization, one-by-one, is a time consuming and potentially dangerous task. With McAfee UTM Firewall Control Center, you have a simple solution for managing firmware images and controlling how and when new images are pushed out to managed devices. Ensuring that all configuration settings are completed—and, more importantly, completed correctly—can be as easy as the click of your mouse. A top-tier IT analyst firm recently stated that “60 to 70 percent of all firewalls are misconfigured, rendering them worse than useless.” An effective mechanism for configuration management is critical to securing your business.



McAfee UTM Firewall Control Center allow administrators to choose which appliances to update with new firmware images and to push the builds out.

Device Monitoring with Flexible Views and Error Log Drilldown

When monitoring a significant number of appliances within one interface, you need the ability to organize the views of your infrastructure for the easiest understanding and control. McAfee UTM Firewall Control Center allows you to customize your view, placing appliances in a hierarchy that makes navigation to different endpoints seamless and intuitive for your administrators. You can also sort and group appliances to easily map the policies you need to put in place. McAfee UTM Firewall Control Center displays the status of each device status and provides a task queue detailing the tasks completed and failed tasks waiting to be retried. And you can access all event log data securely from a web browser for the ultimate in management convenience.



Here's an example of a custom hierarchical structure, displaying the status of all devices listed under "customer1."

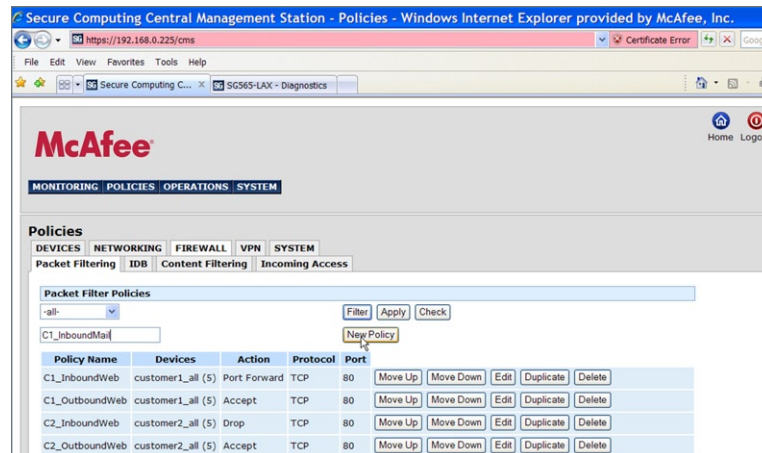
Scalable VPN Configurations with Pre-Shared Key or RSA Digital Signature Key Management

VPN hub-and-spoke architectures are becoming commonplace. Requiring remote offices, franchises, or even remote employees to go through anti-malware and web filtering gateways at a main office is an effective way to ensure consistent security policies are being followed. However, this architecture requires a secure connection back to that corporate office. The VPN tunnel technology built into all McAfee UTM Firewall appliances provides a cost-effective method for achieving this—however, the initial setup of VPN technology can be time-consuming, especially if you need to set up hundreds or thousands of them. With McAfee UTM Firewall Control Center, you have a simple way to perform the setup and push it out to all devices, eliminating the pain and gaining time for other tasks.

Packet Filtering Rules with Integrated NAT or Port Forwarding Rules

When policies change or attacks emerge, you can simply update the affected objects and let McAfee UTM Firewall Control Center instantly apply the changes to all appliances across your environment. You can even compare policy configurations on all of your managed devices to ensure consistency across your network. Robust configuration management features let you centrally track, trace, and validate all policy changes.

Solution Brief McAfee UTM Firewall Control Center: Single-Point Security Management for Large, Distributed Enterprises



McAfee UTM Firewall Control Center allows you to develop packet filter policies to be pushed out to all appropriate devices.

Enforcing Best Practices with Role-Based Administration

Some configuration changes are routine; others profound and far-reaching. Role-based administration of McAfee UTM Firewall appliances allows you to determine which management functions can be viewed or changed based on each user's network responsibilities.

For example, one administrator may be allowed only to change DNS entries, another to view event logs, and a third to create rules associated with a specific network service or protected server. Role-based administration ensures the appropriate division of management responsibility and maximum flexibility. McAfee UTM Firewall Control Center allows for the distribution of both monitoring and management of the devices under its control.

Key Benefits

- Lowers costs by promoting centralization of key security personnel and consistent policy implementation throughout the network
- Reduces complexity of security device administration while maintaining the flexibility to address each organization's diverse needs and individual appliance configurations
- Helps meet regulatory requirements, restricting auditing and other critical functions to specific individuals within the organization to improve security and reduce legal exposure

Additional Features

- Scalable user, password, and access control management for appliance groups
- Least-privilege and separation-of-duties schema for administrators, supporting compliance with
- PCI-DSS and other high-security implementations
- Quality of Service rules for global bandwidth management
- Scalable WLAN implementations with Pre-Shared Key Rotation in TKIP (WPA) or AES (WPA2) formats
- Role-based administration to allow for separation of monitoring and management responsibilities

Solution Brief McAfee UTM Firewall Control Center: Single-Point Security Management for Large, Distributed Enterprise

Policy Definitions

- Networking: DNS proxy, traffic shaping, and wireless
- Firewall: Packet filtering rules, content filtering, incoming access control
- VPN: PPTP client/server, L2TP client/server, IPSec managed/unmanaged endpoints, tunnel settings, and tunnel mapping
- System: User authorization, NTP

Specifications

- Supported devices: McAfee UTM Firewall appliances with firmware version 3.2.1 or higher.
- Installation: The McAfee UTM Firewall Control Center virtual machine can be installed on any system running VMware Workstation, Server, or ESX
- The minimum VMware resource requirements for McAfee UTM Firewall Control Center are:
 - » CPU – Pentium 4 (2.8 GHz or higher)
 - » Disk Space – 10GB or higher
 - » RAM – 2GB or higher

