



## McAfee Firewall Enterprise Virtual Appliance ("FV")

FV.x

### Quickstart Scope Definition Guidelines

McAfee's enterprise security strategy represents the next generation of protection. Adapting to meet the security challenges brought about by the ever-changing face of the Internet, our solutions provide unbeatable security protections, bi-directional application intelligence, built-in compliance mechanisms, best-of-breed processing efficiency, and real-time visibility for making on-the-spot security-related decisions to detect and dismantle even unidentified dangers before they can cause harm. Next generation firewalls provide total protection for high value targets, ensuring the availability and security of critical networks, applications, assets, and data and virtually eliminating all exposure to unknown attacks and attackers. Get the appropriate service type below to ensure it is implemented and configured fast, cost-effectively and securely.

#### **New Installation: 2 X MD-QS-SMB-4HR\***

A McAfee Subject Matter Expert ("SME") will create an initial set of configuration and baseline of policies to support a basic configuration based of McAfee's Best Practices.

##### **Session 1**

- Initial Configuration and Baseline
  - Add FV to the network
  - Perform the initial setup wizard to configure base settings
  - Ensure License is applied
  - Perform required update(s) to FV if available
  - Configure DNS, Interfaces, and Zones
  - Configure VPN's and Static Routes
  - Configure High Availability if needed

##### **Session 2**

- Advanced Configuration, Policy Tuning & Deployment
  - Configure Administrator accounts
  - Configure Rule Elements
    - Applications (up to 10)\*
    - Network Objects (up to 10)\*
    - Authenticators (up to 3)\*
    - Time Periods (up to 3)\*
  - Configure Access Control Rules (up to 10)\*
  - Configure IPS Settings
  - Configure Network Defenses
  - Configure Application Defenses
  - Work with you to outline how to switch the appliance into production

#### **Upgrading: 2 X MD-QS-SMB-4HR**

McAfee's SME will perform the following tasks:

- Initial Configuration and Baseline
  - Backup current configuration
  - Flash the internal memory on the device with the upgraded image
  - Restore the recently saved configuration

- Perform the initial setup wizard to configure base settings
- Verify configuration for email domain(s) for routing to internal server(s)

#### **Optimization: 1 X MD-QS-SMB-4HR**

McAfee's SME will perform the following tasks:

Review Applications

- Create Rule Elements
  - Applications
  - Network Objects
  - Authenticators
  - Time Periods
- Configure Access Control Rules
  - Order for Specificity
  - Remove conflicting or duplicate rules
- Configure Automated Updates
- Configure Automated Backup

#### **Knowledge Transfer: 1 X MD-QS-SMB-4HR**

McAfee's SME will perform the following tasks:

- Explain Rule Elements and how to create them
  - Applications
  - Network Objects
  - Authenticators
  - Time Periods
- Explain Access Control Rules
  - Order for Specificity
  - Remove conflicting or duplicate rules
- Explain Automated Updates
- Explain Automated Backup

#### **Session Requirements - before getting started: Client's responsibility...**

- Validated that **server(s)** meet McAfee's minimum hardware requirements (See Product Guide)
- Establish and verify virtual environment and ensure connectivity to virtual appliance.
- Configured the Appliance (IP, host name, DNS server, etc...) and out of band access to all systems for console access
- Validate the latest applicable ISO and required software have been downloaded via Client's valid grant number
- Perform necessary backups
- Indicate if there are any outstanding Service Requests/Trouble Tickets opened with McAfee Technical Support

**\* Configurations and deployments exceeding these numbers will require additional sessions. Each remote session lasts up to 4.0 hours**