

**McAfee Web Security Gateway Virtual Appliance (“WSG”)****WSG.x****Quickstart Scope Definition Guidelines**

Organizations can do more over the web today than ever before. Today’s web offers a dynamic, real-time user experience. Static information has given way to social networking sites, blogs, wikis, RSS feeds, interactive applications, and user-generated content. Enterprises are taking advantage of these innovative capabilities to do business in more efficient, collaborative ways. This is the reason it is more important than ever to ensure that your organization is protected from the ever-increasing cyber-attacks on confidential information with McAfee Web Security Gateway – edition software (“WSG”). Get the appropriate service type below to ensure it is implemented and configured fast, cost-effectively and securely.

New Installation: 3 X MD-QS-SMB-4HR*

McAfee Subject matter Experts (“SME”) will assist you in creating an initial configuration and baseline of policies for the MWG based on McAfee’s Best Practices.

Session 1

- Initial Configuration and Baseline
 - Add WSG to the network
 - Perform the initial setup wizard to configure base settings
 - Perform required update(s) to WSG if available
 - Configure routing to use the WSG for filtering

Session 2

- Intermediate Configuration and Initial Policy Tuning
 - Configure Network Modes (Proxy or Transparent)
 - Configure Rule Set and Rule Configuration (up to 5)*
 - Configure Monitoring - WSG, Dashboard, logging, error handling

Session 3

- Advanced Configuration and Policy Tuning
 - Configure Multiple Domains (if required)
 - Test and tune all policies
 - Outline how to switch the appliance into production

Upgrading: 1 X MD-QS-SMB-4HR

McAfee’s SME will perform the following tasks:

- Upgrade 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:

- Configure Network Modes
 - Explicit Proxy
 - Transparent Bridge
 - Transparent Router
- Configure Authentication
 - NTLM/ NTLM Agent
 - LDAP, eDirectory, Kerberos
- Configure Filtering
 - URL
 - media type
 - virus
 - malware Filtering
- Review current WSG policies to ensure compliance with McAfee Best Practices (up to 5)*
- Configure associated dashboards

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

McAfee’s SME will perform the following tasks:

- Explain Network Modes
 - Explicit Proxy
 - Transparent Bridge
 - Transparent Router
- Explain Authentication
 - NTLM/ NTLM Agent
 - LDAP, eDirectory, Kerberos
- Explain Filtering
 - URL
 - media type
 - virus
 - malware Filtering
- Explain current MWG policies to ensure compliance with McAfee Best Practices (up to 5)*
- Explain associated dashboard

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
- Validated that 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**