6.0 SECURITY SERVICES

6.1 MANAGED FIREWALL SERVICE (L.34.1.6)

Qwest's Managed Firewall Service is a proven global managed security service that provides an effective front line of defense for Agencies' internal networks and systems from a wide variety of Internet-borne threats.

The Qwest Team's Managed Firewall Service (MFS) provides a comprehensive management service delivering three levels of tiered service, a multitude of value-added features, and a robust offering of Service Enabling Devices (SEDs) to meet the requirements of General Services Administration (GSA) and the Agencies. The three tiers of service offered are as follows:

- Tier 1 - providing firewall support for up to 10Mbps and up to 100 Internet Protocol (IP) addresses
- Tier 2 - providing firewall support for up to 100Mbps and up to 1,000 IP addresses
- Tier 3 - providing firewall support for up to 1Gbps and unlimited IP addresses

Qwest is providing industry leading firewall SEDs to address the Agencies' requirements across all three tiers.

[redacted] Qwest's MFS provides the technology, processes, and trained security engineering team necessary to implement, monitor, and manage an Agency's defined firewall security polices from a 24x7x365 Security Operations Center (SOC). The SOC currently supports numerous Government and commercial customers around the globe. [redacted]

[redacted]

This section describes the MFS features, functions, and capabilities and shows how they meet the requirements for service delivery, performance, and service specifications. MFS is an integral component of the Qwest Team's defense-in-depth strategy of Managed Tiered Security Services (MTSS). An Agency may choose MFS alone or in combination with other services.

Qwest MFS is security vendor agnostic, so we can support Agencies with varying technical firewall requirements and analyze and recommend a product(s) that meets their needs. [redacted] The technical strengths and flexibility of our solutions make Qwest MFS an excellent choice for General Services Administration (GSA) and the Agencies it serves.

6.1.1 Technical Approach to Managed Firewall Service Delivery (L.34.1.6.1)

MFS safeguards internal networks and systems from unauthorized accesses and hostile activity, protecting critical data from compromise and tampering. MFS serves as the first line of defense between an Agency's trusted internal networking environments, Demilitarized Zones (DMZs), and external and public networks. MFS inspects traffic according to a set of Agency defined security policies, blocking all traffic not meeting the Agency's

criteria. Qwest's MFS technical solution incorporates robust functionality, proactive monitoring and management, potent event correlation, ease of administration, sophisticated reporting, and experienced technical support, with a single interface to coordinate technical service and trouble ticketing. This model fits well with the Networx requirements. Qwest's MFS allows an Agency to acquire service for either firewalls that they currently have deployed (subject to determination of technological compatibility) or for new implementations of firewall technology from the SEDs list.

6.1.1.1 Approach to Managed Firewall Service Delivery (L.34.1.6.1(a))

Qwest MFS meets all the service delivery requirements and can be customized to meet the specific firewall technology deployed or selected by the Agency. Our approach is to use proven processes and a skilled security engineering team that has experience and knowledge of Transmission Control Protocol/IP, Internet services, firewall methodologies, Virtual Private Networks (VPNs), and encryption, combined with the technical knowledge of the specific firewall technology under management. Qwest's MFS provides Agencies with a value-added managed service that is secure, reliable, flexible, scalable, and extremely cost efficient.

Qwest's MFS takes a security lifecycle approach to managed firewall services. MFS provides for firewall and supporting system software and hardware component design, implementation, remote monitoring, and management of SEDs or Network-Based Equipment to secure the network and its perimeter. We customize our services based on each Agency's needs regarding selected technologies, tiers of service, logical placement, and configuration of the security devices. Support is provided for firewall solutions of varying size, performance, and capabilities.

[redacted]

6.1.1.2 Benefits of Managed Firewall Services Technical Approach (L.34.1.6.1(b))

[redacted]

[redacted]

Figure 6.1.1-3. Benefits of Qwest's MFS Offering

Feature	Benefit	[redacted]
Team of Certified Security Professionals	Specialized security knowledge and best practice application to ensure the Agencies' data protection policies are upheld.	[redacted]
Early Warning System through Access to Open Source Intelligence	Agencies are provided an early warning system that is integrated into MFS.	[redacted]
Smart Management Consoles that Enable Fast Service Changes	Agency requested MFS updates, policy changes, and threat mitigation are managed through a sophisticated management console in order to make changes near real-time, and error free.	[redacted]

Qwest's MFS addresses the Federal Enterprise Architecture (FEA) as shown in ***Figure 6.1.1-4***.

Figure 6.1.1-4. Qwest's MFS meets Federal Enterprise Architecture requirements

FEA Requirement	[redacted]
Improve Government Efficiency and Effectiveness	[redacted]
Improve Service Delivery to Customer Agencies	[redacted]

FEA Requirement	[redacted]
Enhance Cost Savings and Cost Avoidances	[redacted]
Improve Utilization of Government Information Resources	[redacted]

6.1.1.3 Solutions to Managed Firewall Services Problems (L.34.1.6.1(c))

[redacted]

Figure 6.1.1-5. Qwest MFS Anticipated Problems and Solutions

Problem	[redacted]
Firewall policy updates, by default, will deny traffic that is not explicitly permitted, which can impact the use of new protocols or applications.	[redacted]
Hardware failures	[redacted]
"Zero-day" viral activity leaves organizations vulnerable	[redacted]

[redacted]

[redacted]

6.1.2 Satisfaction of Qwest MFS Performance Requirements (L.34.1.6.2)

6.1.2.1 Managed Firewall Services Quality of Service (L.34.1.6.2(a))

Qwest's MFS offering is designed to enable sustainable results at an operational level through a performance measurement system based on the use of Key Performance Indicators (KPIs) that meet Government Acceptable Quality Levels (AQLs). Performance measurement of quantifiable indicators is measured, collected, monitored, and reported to determine the success or failure of the KPIs for Qwest's MFS. Active monitoring ensures that performance is achieved, and Qwest will provide performance data to Agencies [redacted] Qwest's MFS offering is fully compliant with GSA requirements, as shown in ***Figure 6.1.2-1***.

Figure 6.1.2-1, Qwest's MFS Performance Standards and AQLs

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[redacted]
Availability	Routine	99.5%	≥ 99.5%	[redacted]
Event Notification	Routine	Next business day for a Low category event	≤ Next business day	[redacted]
		Within 4 hours of a Medium category event	≤ 4 hours	[redacted]
		Within 30 minutes of a High category event	≤ 30 minutes	[redacted]
Grade of Service (Configuration/ Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	[redacted]
		Within 2 hours for an Urgent priority change	≤ 2 hours	[redacted]
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	[redacted]
	With Dispatch	8 hours	≤ 8 hour	[redacted]

Availability: Qwest MFS is delivered through industry-leading security appliances [redacted]

Event Notification (EN): Qwest's proactive network monitoring capabilities correlates network performance statistics and trigger performance thresholds, which automatically create notification trouble [redacted]

Grade of Service (Configuration/ Change): Configuration Changes can be requested by the Agency [redacted]

Time to Restore (TTR): All troubles are recorded [redacted]

6.1.2.2 Approach for Monitoring and Measuring Managed Firewall Services (L.34.1.6.2(b))

To ensure AQLs are met and that critical issues are immediately addressed, thresholds are set depending on the nature of the event, in accordance with Federal Information Processing Standards 199 and the NIST 800 series. The events are tracked via individual tickets that are prioritized based on classification and response time AQLs. [redacted]

[redacted]

The ticket is subsequently tracked and updated for technical and AQL performance throughout the escalation process until successful closure.

Qwest recognizes that it is the Government's intent that KPI monitoring of services is included in the scope of work to be performed. Depending on network topology and policies, additional systems may be required for different security zones to ensure that all critical systems are closely monitored. The SOC lead engineer assigned to the Agency is responsible for monitoring and oversight of the performance of the SLAs. Qwest's delivery experience, combined with our knowledge that each Agency will have unique requirements, especially around Grade of Service, allows the definition of appropriate change control processes and commitment levels by task order AQLs.

[redacted]

[redacted]

Once an order has been accepted by the Qwest Team and the SEDs and services are provisioned and commissioned, the required KPI monitoring is included without additional action by the Government.

6.1.2.3 Verification of Managed Firewall Services (L.34.1.6.2(c))

[redacted]

6.1.2.4 Managed Firewall Services Performance Improvements (L.34.1.6.2(d))

[redacted]

6.1.2.5 Additional Managed Firewall Services Performance Metrics (L.34.1.6.2(e))

[redacted]

6.1.3 Satisfaction of Managed Firewall Service Specifications (L.34.1.6.3)

6.1.3.1 Satisfaction of Managed Firewall Service Requirements (L.34.1.6.3 (a))

The Qwest MFS is fully compliant with the mandatory technical capabilities required in the Request for Proposal (RFP). Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for MFS. The following ***Figure 6.1.3-1, Figure 6.1.3-2,*** and Section 6.1.3.1.3 summarize Qwest's response to the MFS capabilities listed in RFP C.2.10.1.1.4, features of RFP C.2.10.1.2, and interfaces of RFP C.2.10.1.3. These subsections are intended to provide the technical description required per L.34.1.6.3(a) and do not limit or caveat Qwest's compliance in any way.

6.1.3.1.1 Satisfaction of MFS Capability Requirements (L.34.1.4.2(a); C.2.10.1.1.4)

Figure 6.1.3-1 provides a discussion of our approach to satisfying MFS capabilities.

Figure 6.1.3-1 Qwest's approach to satisfying MFS Capabilities

MFS Capabilities	[redacted]
1. The contractor shall provide firewall software and hardware components, including log servers, as applicable. The service shall include the following, as required by the Agency: a. Premises-based firewalls b. Network-based firewalls c. Application/proxy-based firewalls	[redacted]
2. The contractor shall support remote monitoring capabilities and proactively monitor the firewall, including hardware/software components, on a 24x7x365 basis.	[redacted]
3. The contractor shall monitor the overall performance of the firewall, including monitoring the adequacy of the firewall as the network expands.	[redacted]
4. The contractor shall ensure that firewall statistics and logs are sent to the contractor's operation center via secure means.	[redacted]
5. The contractor shall implement firewall security policies according to the Agency's needs.	[redacted]
6. The contractor shall detect suspicious activity and policy violations.	[redacted]
7. The contractor shall employ various protection techniques including but not limited to:	[redacted]
a. Stateful Packet Inspection by which the firewall goes beyond just examining a packet's source and destination, but	[redacted]

MFS Capabilities	[redacted]
also verifies its legitimacy. The firewall confirms requests made and matches open connections to valid packets prior to allowing them through the network.	
b. Network Address Translation (NAT) and Port Address Translation (PAT) in order to disguise internal IP addresses, shielding systems from the outside world, especially from malicious activity.	[redacted]
8. The contractor shall guard the Agency's networks from attacks, including but not limited to:	[redacted]
a. Denial of Service (DOS) assaults that flood the network with false requests, overwhelming servers and eventually causing them to crash.	[redacted]
b. Ping of Death or Long Internet Control Message Protocol attacks in which packets larger than 65,536 bytes are sent deliberately in an attempt to crash the system.	[redacted]
c. IP Spoofing attacks in which packets' IP addresses are disguised. These packets appear to have originated from a trusted source with appropriate authorization or privileges.	[redacted]
d. Synchronize Flood attacks, which clog connections and prevent legitimate session requests from being established.	[redacted]
e. Tear Drop attacks in which packet fragments are deliberately designed to	[redacted]

MFS Capabilities	[redacted]
disrupt proper packet reassembly at the receiving end.	[redacted]
9. The contractor shall block hostile Java applets, JavaScript, and ActiveX controls to guard against potentially unsafe code, as required. The contractor shall also block cookies and Web bugs, as required.	[redacted]
10. The contractor shall maintain a problem detection system for the diagnosis of alerts and violations.	[redacted]
11. The contractor shall notify the Agency of events via email, pager, fax, or telephone, as directed by the Agency.	[redacted]
12. The contractor shall provide the Agency with secure Web access to the service in order to request/perform security policy updates, report troubles, track status of reported problems, obtain firewall logs and reports, and administer user databases, as needed. The information shall contain but not be limited to the following information, as applicable: a. Active Surfers b. Authentication Reports c. Change Requests d. Configuration Modifications e. Connections/Attempts Accepted/Rejected f. Events g. Firewall Statistics h. Firewall Utilization i. File Transfer Protocol (FTP) Connections Counts j. HyperText Transfer Protocol (HTTP) Destinations Counts k. IP Addresses l. Mail Statistics m. Originating and Terminating Addresses n. Outages o. Port Activity	[redacted] [redacted] [redacted]

MFS Capabilities	[redacted]
p. Protocol Data for HTTP, HTTP Secure (HTTPS), FTP, Simple Mail Transfer Protocol (SMTP), and Telnet q. Rule Violations r. Tickets s. Uniform Resource Locator (URL) and Visited Websites Reports t. Web Hits per Specified Period	
13. The contractor shall maintain the latest configuration information for restoration purposes.	[redacted]
14. The contractor shall maintain the firewall, performing the necessary hardware/software upgrades, updates, and necessary replacements.	[redacted]
15. The contractor shall test and deploy the latest patches and bug fixes as soon as they become available and are approved by the Agency, in order to ensure optimal performance of the firewall service.	[redacted]
16. The contractor shall perform Configuration and Change Management, including modifying the following attributes, as applicable and as requested by the Agency: a. Filtering and Blocking Requirements b. Firewall Policies and Rules c. VPN Characteristics d. IP Hosts such as Web and Mail Servers Impacted by the Firewall e. Protocols f. User/groups	[redacted]
17. The contractor shall perform firewall security scans capable of detecting open port vulnerabilities in order to ensure that the firewall is secure.	[redacted]

MFS Capabilities	[redacted]
18. The contractor shall provide Domain Name Server (DNS) and SMTP configuration support to ensure the firewall is appropriately set up to handle DNS queries and mail traffic, as required.	[redacted]
19. The contractor shall support firewalls of varying complexity, in terms of size, performance, and capabilities.	[redacted]

6.1.3.1.2 Satisfaction of MFS Feature Requirements (L.34.1.4.2(a); C.2.10.1.2)

Figure 6.1.3-2 provides a discussion of our compliance to all required MFS features.

Figure 6.1.3-2 Qwest compliance to MFS required features

ID #	Name of Feature	Description	[redacted]
1	Demilitarized Zones (DMZs) Support	The contractor shall support connections to DMZs, which serve as buffers between the Agency's private networks and outside public networks. DMZs can apply to Web (HTTP), FTP, Email (SMTP), and DNS servers.	[redacted]
2	Email Security	The contractor shall support email security measures that can conceal, limit, or change information about the Agency's networks or domains, reducing visibility to outsiders. The contractor shall also have the capability to block email attachments that are above a specified size.	[redacted]

ID #	Name of Feature	Description	[redacted]
3	Extranet Support	The contractor shall support connections to extranets that can facilitate inter-Agency interactions or enable the Agency to interface with various trusted stakeholders, such as contractors or vendors.	[redacted]
4	Fast Ethernet Connection	The contractor shall support fast Ethernet connections (100BaseT/1000BaseT), which provide greater data flows from the firewall to the Agency's internal networks.	[redacted]
5	Firewall Load Balancing	The contractor shall implement a hardware or software load balancing capability, as required by the Agency. The service shall distribute traffic across multiple firewalls, in order to minimize potential downtime caused by any single point of failure. This provides firewall scalability, ensures availability, and adds further safeguards against hardware and software problems.	[redacted]
6	Firewall Redundancy	The contractor shall provide a firewall redundancy solution based on a dual firewall systems approach, in a primary/secondary setup. The system, comprised of hardware and software as applicable, will enable automatic transfers from one system to the next in case of severe hardware/ software failures in order to maintain availability of the firewall.	[redacted]
7	Firewall-to-Firewall VPNs	The contractor shall support firewall-to-firewall VPNs that establish secure tunnels between Agency firewalls and also between firewalls and the contractor's operation center.	[redacted]

ID #	Name of Feature	Description	[redacted]
			[redacted]
8	Personal Firewalls (Optional)	The contractor shall provide personal firewalls or personal firewall appliances in order to secure remote personal computers or small remote networks (i.e., home offices), as required by the Agency.	[redacted]
9	Remote Client VPNs	The contractor shall provide remote Agency users with secure access to the network, employing VPN encryption technology.	[redacted]
10	URL Filtering	The contractor shall support URL blocking, as required. URLs may fall in categories such as: 1. Advertisements (such as banner ads) 2. Computer Hacking 3. Criminal Skills 4. Drugs, Alcohol, and Tobacco 5. Extremists 6. Gambling 7. Hate Promotion 8. Illegal or Questionable Sites 9. Online Gaming (non-gambling) 10. Satanism and Cults 11. Search Engines 12. Sexually Explicit/Adult Material 13. Sports and Leisure 14. Violence or Profanity	[redacted]
11	User Authenticatio n Integration	The contractor shall support the integration of the firewall service with the Agency's own authentication services, as specified by the Agency. The Agency may employ several user authentication tools such as, but not limited to: 1. Lightweight Directory Access Protocol 2. Microsoft Active Directory 3. Microsoft Windows NT 4. Operating System Passwords 5. Remote Authentication Dial-In User Service 6. Rural Service Area Secure ID 7. Terminal Access Controller	[redacted]

ID #	Name of Feature	Description	[redacted]
		Access Control System (TACACS) or Extended TACACS (XTACACS)	

6.1.3.1.3 Satisfaction of MFS Interface Requirements (L.34.1.4.2(a); C.2.10.1.3)

Qwest provides all required interfaces based upon the capabilities of our proposed services as defined in: Frame Relay Service (RFP Section C.2.3.1), Asynchronous Transfer Mode Service (RFP Section C.2.3.2), Internet Protocol Service (RFP Section C.2.4.1), Premises-based IP VPN Services (RFP Section C.2.7.2), and Network Based Internet Protocol VPN Services (RFP Section C.2.7.3).

6.1.3.2 Proposed Enhancements for Managed Firewall Services (L.34.1.6.3(b))

To enhance an Agency's ability to recognize and respond to network security events, if multiple managed security services are ordered during the course of this contract, [redacted]

6.1.3.3 Network Modifications Required for Managed Firewall Services Delivery (L.34.1.6.3(c))

Qwest requires no network modifications to deploy MFS to Agencies. Qwest will conduct operational reviews to identify any specific Agency network modifications needed for MFS deployment.

6.1.3.4 Experience with Managed Firewall Service Delivery (L.34.1.6.3(d))

[redacted]

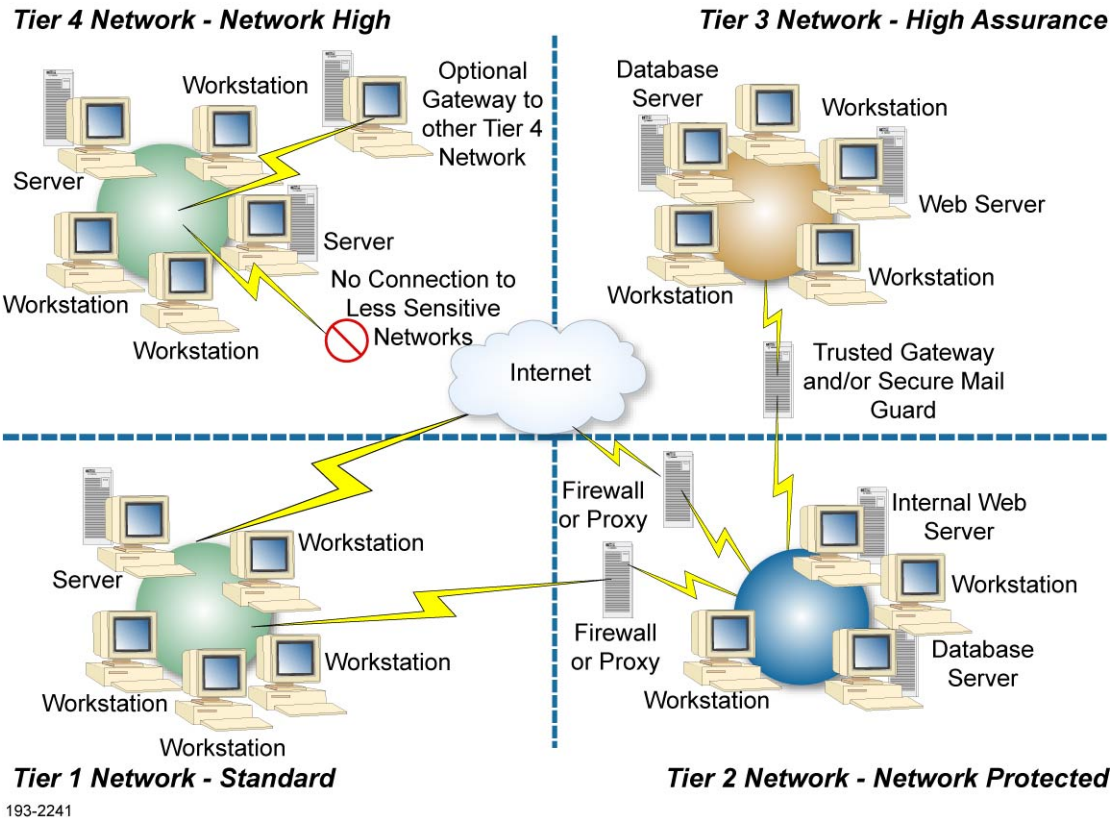
[redacted]

6.1.3.5 Managed Tiered Security Service (MTSS) Approach (L.34.1.6.3(e))

MFS is part of the Qwest MTSS technical solution. Design, implementation, and delivery according to GSA's Multi-Tier Security Profile (MTSP), ***Figure 6.1.3-3***, will be addressed to meet an Agency's requirements based on security service levels identified as described in Section 6.8. A defense-in-depth strategy and technical solution that includes MFS will be engineered as described in Section 6.8.3.1.1 to account for specific differences in each tier.

MTSP Tier 2 - Protected Service shall provide security enhancements to the subscribing Agency with additional protection from unauthorized activities and the proliferation of malicious code. Protected service shall also mitigate the potential for DOS attacks. Security enhancements include a

Figure 6.1.3-3. MTSP Notional Architecture



combination of firewall, premises-based VPN (encrypted tunnels), filtering router, proxy server, and boundary anti-virus detection technologies configurable to the subscribing Agency's security policy(s) and specifications.

Tier 2 is tailored to Sensitive But Unclassified mission functions and information. It employs both technical and network management components appropriate to the respective mission and/or information sensitivity.

[redacted]