LUMEN®

Lumen Service Guide

Managed Firewall Services

Version: February 25, 2021

This Lumen Service Guide ("SG") sets forth a description of the Managed Firewall Services ("Service") offered by Lumen and its suppliers, including technical details and additional requirements or terms. "Lumen" is defined as CenturyLink Communications, LLC d/b/a Lumen Technologies Group and its affiliated entities. This SG is subject to and incorporated into the Agreement and the Hybrid Technologies Service Exhibit (formerly the CenturyLink TS Service Exhibit) and the Security Schedule. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order.

Service offerings in this SG include:

- Managed Firewall 1
- Managed Firewall IDC
- Managed Firewall 2.0 IDC
- Managed Firewall 3.0 IDC
- Managed Firewall CPE
- Managed Firewall 3.0 CPE
- Managed Cisco Firewall – Non-Customer Premises version 1.0
- Managed Cisco Firewall – Customer Premises version 1.0
- Managed Palo Alto Firewall IDC
- Managed Palo Alto Firewall CPE

Service Description

1. Standard Service Description: Managed Firewall services are Security services available in a CenturyLink provided or managed environment and this may also be referred to as Managed Firewall – IDC or Non-Customer Premises; and/or at a Customer's premises and this may also be referred to as Managed Firewall - CPE or Customer Premises (collectively, the "Service(s)"). Firewalls may also be referred to in this SG as equipment, device, appliance, hardware or platform. Lumen provides the design/installation, configuration, administration, monitoring, testing, maintenance and support for the components as detailed in this SG. Differences between supported activities based on location of firewalls, whether in Lumen provided environments or on Customer premises will be noted where applicable.

Customer acknowledges that Lumen's responsibility is related to enabling policies and configurations designed to protect Customer network through this firewall service and information that traverses that network and such responsibility does not extend to any information, data or content that the Customer may send, transmit and/or store. Lumen does not represent or warrant that the Lumen provided equipment or the Service (i) will be uninterrupted or error-free; (ii) will detect or generate an alert for every security event that may be recorded in customer logs; (iii)will be effective for blocking or filtering technologies; or; (iv) that others will be unable to gain access to Customer's computer(s), data or information. Lumen has no responsibility and assumes no liability for any suchacts or occurrences. Customer's exclusive remedies are as provided in the Service Level Agreement (SLA) located in Appendix A of this SG.

In addition, when purchasing either of the Managed Palo Alto Firewall Services service offerings, Customers must also separately purchase Lumen's Security Log Monitoring 2.0 Services at an additional cost as a dependency and this requires additional contractual documents to be signed.

2. Service Components for all Managed Firewall Services:

2.1. Dedicated Firewall: Includes hardware and any software required for the firewall, which may be provided and/or licensed from third parties. Customer may choose to purchase certain available service options as further detailed in Optional Features Section below. Not all options and features are available on all vendor platforms. Please refer to Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls.

2.2. Virtual Machine Firewalls: A Virtual Machine Firewall is a virtualized form factor of the dedicated firewalls consisting of virtual machine (VM) models. Virtual Machine Firewalls are only available with Lumen Edge Private Cloud on VMware Cloud Foundation, which must be contracted separately and Palo Alto Firewalls must include the purchase of Security Log Monitoring 2.0.

2.2.1. VM firewalls do not support the Logical Firewall option described below in section 3.4.

2.3. Connectivity: Installation of the Service within a Lumen managed environment will include (2) two VLANs, (2) two high-speed connections to each firewall, and assignment of a private IP address for management. External access and upgrades to these capabilities are available at an additional fee and may require additional contractual documents to be signed.

2.4. Design/Installation: Lumen will provide the design/installation tasks marked with an "X" in the Lumen column in Table 1.0 Standard Roles and Responsibilities for Dedicated, Logical, and Virtual Machine Firewalls. Lumen's baseline design utilizes a template with default recommended policies when installing a new firewall.

2.5 Configuration: Lumen will provide the configuration tasks marked with an "X" in the Lumen column in Table 1.0 Standard Roles and Responsibilities for Dedicated, Logical, and Virtual Machine Firewalls.

2.6 Rule Set Changes: A Lumen network engineer will perform ongoing firewall configuration upon receipt of rule request changes from Customer during onboarding, install and ongoing per Lumen's standard change request process. Lumen reserves the right to refuse rule-set and configuration changes it deems unnecessary in its reasonable discretion.

2.6.1 Backup and Storage: Lumen will backup and store off-site the most recent firewall policies or configuration details for the time period in which the Customer maintains the Service with Lumen. Any time a change to the firewall policy or configuration is implemented, a new backup is generated in accordance with the procedures identified by the applicable vendor.

2.6.2 Lumen is obligated to log backup and storage only during a Customer's committed Service Term, including renewal terms. If the retention period selected extends beyond the Customer's Service Term or if Customer or Lumen terminate the Services prior to the end of the retention period selected, Customer acknowledges that Lumen has no further obligation to back up and store any Customer metrics or log related data after Agreement expiration or termination and Lumen will automatically delete all logs. Customer acknowledges and consents that it is solely Customer's responsibility to make copies of or obtain the logs obtained from the firewall services prior to expiration or termination.

2.6.3 If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, Lumen will contact Customer, if necessary, to schedule the activity (typically during normal Maintenance Windows) and Customer agrees to cooperate with Lumen to schedule such activity. If Lumen determines that an emergency security change is required, Lumen will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

2.7 Administration: Lumen will provide the administration tasks marked with an "X" in the Lumen column in Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls.

2.7.1 System Administration: For configuration consistency and accountability, all system administration and firewall passwords will be managed by Lumen. Customer will not have access to firewall passwords or be able to make direct changes to the firewall configurations. The Customer must request changes by first contacting the Security Operations Center. The Customer must provide complete authentication credentials to the Security Operations Center when requesting changes.

2.7.1 Reporting: Reporting will be as available for Customer to select in the applicable portal which will show the multiple time frequencies subject to log retention time frames. Dashboards, reports and query capabilities will vary between portals and the Services purchased.

2.7.2 Rate Limiting: Rate limiting of firewall log traffic (i.e. dropping log traffic), when on Lumen managed environments, will be implemented to mitigate the impact to the network from, as an example denial of service type attacks. Lumen offers limited assistance to facilitate rate limiting on Customer request for Customer premises.

2.7.3 System Security and Event Logs Retention: See Table 2.0 System Security and Event Logs Retention for a list of the security and event logs that will be retained and the length of time. Customers who purchase Managed Palo Alto Firewall Services must purchase Security Log Monitoring as a dependency.

2.8 Monitoring: Lumen will provide the monitoring tasks marked with an "X" in the Lumen column in Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls.

2.8.1 SNMP Statistics: Collects SNMP statistics on firewall performance and makes the information available in the applicable portal (only available with specific vendors and models).

2.8.1 Attack Notification: When the Customer notifies Lumen of an attack on a Customer's site, Lumen will modify the Customer's firewall policy to prevent attacks if the source IP can be readily determined by Lumen using commercially reasonable efforts.

2.9 Testing: Lumen will perform system testing as marked with an "X" in the Lumen column in Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls prior to moving device into steady state operations.

2.10 Maintenance and Support: Lumen will provide the maintenance and support tasks marked with an "X" in the Lumen column in Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls.

2.10.1 Updates: Lumen may periodically update the software, hardware, or other components of the Services, to maintain the latest vendor-supported versions in operation. If Lumen determines an update is necessary and has successfully completed requisite testing, Lumen will work with Customer to schedule a time to make necessary changes, typically during the scheduled Maintenance Windows as defined in this SG. Customer must acknowledge Lumen's request to make these changes within five (5) business days of receipt of the request from Lumen, or Customer will be ineligible to receive service credits in accordance with the SLA until Customer grants Lumen the access required to make such changes. This ineligibility of service credits may also apply to other related Services purchased by the Customer. If Lumen determines that an emergency security change is required, Lumen will make the change as quickly as possible. Lumen will make commercially reasonable attempts to contact the Customer's technical contact prior to making said change. Some updates, including migrations attributable to vendor service availability as more fully described below in Customer Responsibilities, and as determined by Lumen may require Customer to sign a new Service Order to implement the changes which could include changes to pricing.

2.10.2 Hardware Maintenance: For deployments on Customer premises, Lumen will maintain hardware as detailed in Table 1.0, Table 3.0, and as defined in the SLA (Service Level Agreement).

2.10.3 Hardware Repair: For deployments on Customer premises, Lumen is responsible for the replacement of hardware if a failure occurs, unless Customer is responsible for the damage as a result of unauthorized action or any other error or omission of Customer. Customer will have responsibility for the physical network installation of the replacement firewall appliance on Customer premises.

3. Optional Features: At Customer's option and depending on which Firewall Service a Customer purchases, the items below may be purchased in addition to the standard Service (described in Section 1) for an additional fee. Contact your sales representative for additional information.

3.1 Intrusion Protection Service (IPS): Customer can choose to have Lumen setup and configure IPS as applicable on supported models.

3.1.1 Roles and Responsibilities: In addition to the Tasks listed in Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls, Lumen will provide tasks marked with an "X" in the Lumen column in Table 3.0 Roles and Responsibilities for Additional/Optional IPS and NextGen Options. The IPS deny policy could impact legitimate Customer activity, and is the sole responsibility of the Customer to review prior to implementation.

3.1.2 IPS Signatures: Available IPS signatures and other NextGen content will be proactively applied to Customer devices on a regular basis. The applicable vendor may delay the release schedule for signature updates, thus impacting the Lumen ability to perform signature updates on the routine interval. Lumen will apply the signatures at the next available scheduled interval.

3.2 Client VPN Users: The Remote Client to LAN functionality connects Customer's end users to the Lumen managed firewall securely via an encrypted session over the Internet. A secure VPN tunnel is initiated from Customer's end users leveraging the VPN client software installed on the end user's computers. The Customer's end user VPN connection terminates into the Lumen managed firewall, at which point the Customer's end users can gain access to their network environment. Lumen provides this feature only on specific supported firewall models. Lumen will provide the VPN software and licensing for the requested number of Customer's Client VPN Users. Customer acknowledges they may be required to click to accept or otherwise agree to additional terms and conditions during installation of the VPN software, including any installation on a mobile device. VPN client software is currently supported for: Windows, Linux, Mac OS X, Android and Apple iOS. Support for specific OS and mobile versions may vary. See Table 5.0 Roles and Responsibilities VPN Users and Site-to-Site VPNs detailing Lumen and Customer responsibilities.

3.2.1 Lumen will provide VPN client software to Customer. Administration and support of Customer end points will be the sole responsibility of the Customer. Client VPN connections will not carry any quality of service SLAs.

3.2.2 Configuration: Includes configuration of Lumen managed firewall.

3.2.3 Client VPN User username and password authentication: If Customer is using Lumen's managed environment, Lumen will use Lumen Managed Microsoft Active Directory services within the Lumen provided environment. When on Customer premises, Customer's Microsoft Active Directory will be required for Lumen to configure.

3.2.4 Client VPN Users Password Policy: Password policy to set expiration at 90 days for customers using Managed Hosting services within a Lumen provided environment.

3.2.5 Client VPN Users Authentication: Requests not using Lumen's Managed Hosting services authentication will leverage Customer provided infrastructure.

3.2.6 Installation of the VPN software client is the responsibility of the Customer's end users. Lumen will provide an installation guide during service implementation.

3.3 Site-to-Site VPN Users: Site-to-Site functionality connects Customer's sites securely via the Internet. A secure IPsec tunnel is created from supported models of Lumen Managed Firewalls to up to two Customer or Lumen managed devices. See Table 5.0 Roles and Responsibilities VPN Users and Site-to-Site VPNs detailing Lumen and Customer responsibilities.

3.3.1 Lumen will use reasonable efforts to establish a tunnel between the VPN devices. Differences in software versions, configurations and conflicting applications may prevent the VPN from functioning. Customer managed VPN devices must be licensed by Customer to accommodate appropriate encryption standards compatible with the device. Administration of Customer managed end points will be the sole responsibility of the Customer. Meshed or hub and spoke VPN connectivity will not be supported. IPsec connections will not carry any quality of service SLAs.

3.3.2 Configuration: Lumen will provide configuration of the managed firewalls and associated authentication infrastructure for Customers using Managed Hosting services within a Lumen provided environment or firewalls managed by Lumen on the Customer premise. Administration of Customer managed devices will be the sole responsibility of the Customer.

3.3.3 Additional VPN Costs: Additional sites (to more than two Customer or Lumen Managed devices) may be added for an additional charge for the Site-to-Site VPN feature.

3.4 Logical Firewall Option: Customer can purchase additional licenses for Logical Firewalls as Lumen has available from its vendors. Lumen will support logical firewall setup and configuration as an option with the base firewall service. Vendor limitations may restrict the use of a logical firewall with IPsec VPN with specific code revisions. The quantity of logical firewalls supported by Lumen may be lower than the vendor's technical specifications.

3.5 Ethernet Upgrade: Contact your account rep to order expansion modules as applicable to various models.

3.6 Firewall Failover Solution: The Failover Solution is designed to deliver firewall high-availability by providing a dedicated hot standby. In the event the primary device fails, the secondary device detects the failure and begins operation. The primary and secondary devices are connected to the Customer's networks on the front-and back-ends of the device via switches or hubs. At the Customer's request, Lumen will work with the Customer to recommend a solution based on the Customer's requirements. The recommendation may require additional network equipment and network services. The cost of the hubs, switches and secondary network connections are not included with the Service price and must be purchased separately by the Customer.

3.7 NextGen Features: Various security features may be available for specific vendor devices commonly referred to as NextGen. Additional fees may apply where further software is required, and such software may require Customer to click to accept the vendor's terms and conditions. URL filtering is a current example. These features are rapidly evolving. Your Lumen sales representatives can provide up-to-date feature availability.

3.8 Customer Policy & Migration Support is an available option for an additional fee that provides additional support beyond the standard baseline service delivery design and configuration build with Managed Firewalls and it includes evaluation, replication of Customer pre-existing firewall policies for configuration on the new device that behaves in an equivalent manner, and Customer migration planning with coordinated cutover from a different managed security service provider or another firewall device. This does not modify nor provide evaluation for the validity of existing firewall policy, rules, and behavior. Standard baseline build includes design and configuration where Customer populates and confirms the firewall policies via input to a Lumen template with suggested default settings with minimal assistance for basic policy error checking. The firewall is implemented in a new Customer environment without accounting for existing Customer environment constraints. Both standard baseline and customer policy & migration support include GSOC installation tuning.

4. Customer Responsibilities: Customer is responsible for all tasks with an "X" in the Customer column in the applicable Tables herein. Customer acknowledges and agrees that its failure to perform its obligations set forth in any of the Tables may result in Lumen's inability to perform the Services and Lumen will not be liable for any failure to perform in the event of Customer's failure. Lumen will not be liable for any failure to perform in the event Customer does not fulfill Customer's responsibilities and requirements as detailed herein and in the event of Customer's errors or omissions in setting up the required environment. Lumen assumes no responsibility whatsoever for any damage to, loss, corruption or destruction of, or unauthorized disclosure of any of Customer's hardware, software, files, data, information or peripherals, including any damages or losses which may result from Customer's use of Service or Customer's errors or omissions as noted herein.

4.1 Network Topology Changes: The Customer must notify Lumen in advance of any network topology or system changes that may affect the Service or the effectiveness of the agreed policies. Failure to notify Lumen of system changes may result in the inability to monitor traffic or the generation of false alerts. Lumen will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, Lumen may modify the firewall configuration to reduce repetitive alarms caused by Customer actions that are not indicative of security incidents.

4.2 Equipment and Installation: For Services installed on Customer premises, Customer must ensure the following are in place prior to Lumen installing the appliance to enable the Service.

4.2.1 Required Infrastructure and Connectivity: Provide the necessary space, power, environmental conditions, connectivity, and security precautions at each Customer site for the appliance. See Table 4.0 Customer Premises Physical Site Requirements.

4.2.2 Installation: Customer will have responsibility for the physical network installation of the appliance. Customer to provide the necessary network connections and Internet access to connect the appliance.

4.3 IP Address: Customer must provide IP addresses for all network connections to the firewall, the number of which will be determined by Lumen.

4.4 Bandwidth: To avoid degradation of the Service, Customer must not have sustained bandwidth exceeding rated capacity of the appliance. Lumen will provide the appliance information as part of the installation process.

4.5 Access and Permissions: Customer will provide Lumen's approved personnel, immediate access to the firewall on Customer premises if there is a service outage and at reasonable times in all other situations. Should Lumen determine the need for Lumen personnel to physically access the firewall, Customer must allow Lumen personnel access to the Customer site. Customer will ensure that all permissions of any kind needed for the installation and operation of Lumen firewalls are in place at all times. If the Customer has an Access Control List (ACL) that interferes with management connections, the Customer must allow Lumen access for management and monitoring. Customer will be ineligible to receive service credits in accordance with the SLA until Customer grants Lumen the access required.

4.6 Repair Costs: When the Service is located on Customer's premises, Customer will have responsibility for the physical network installation of the replacement appliance on Customer premise. Customer will pay any costs for repairs or replacement of the appliance that are not covered by the underlying vendor maintenance agreement. Lumen can provide additional instructions on processing a appliance return.

4.7 Unauthorized Testing: Customer will not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any appliances used to deliver Lumen services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing, credentialed scans from firewalls, or external network scans on Lumen's network without the prior written consent of Lumen.

4.8 Provide Contact: Designate and maintain a Customer Contact during the service term and any applicable renewal term (including current contact information). "Customer Contact" means a technical point of contact with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable systems.

4.9 Provide Technical Support. Customer agrees to provide technical support during implementation and on-going support. Customer will ensure environments are provisioned with servers, local incremental and replica storage, network connectivity, CPU and memory resources, and other infrastructure components; and replication is operational.

4.10 Neither Customer nor its representatives will attempt in any way to circumvent or otherwise interfere with any security precautions or measures of Lumen relating to the Service or any other Lumen equipment.

4.11 Customer acknowledges and agrees that it is solely responsible for selecting and ensuring its software and systems are up to date and supportable.

4.12 Customer further acknowledges it is solely responsible for ensuring all Customer-owned devices, software and hardware are updated to meet vendor configurations.

If any configuration, version, or component of the Service is identified as either unsupported or no longer available by a vendor notifying Lumen, then Lumen will in turn notify Customer. Customer may be required to sign a new Service Order to ensure the affected Services are updated or migrated to a supportable version. The new Service Order may require a new Service Term and/or a change in pricing. If Customer remains with the unsupported or unavailable Services, Customer acknowledges the Services are subject to all of the following conditions and/or requirements: (i) a service level objective ("SLO") referring to Lumen's reasonable effort to provide support will apply in lieu of any other applicable SLA and will automatically apply from the time Lumen receives notice from the vendor of such unsupported service; (ii) Lumen, in its reasonable discretion may elect to charge the customer for any support or additional tasks/work incurred by Lumen resulting from Customer's continued use of unsupported configuration until Customer obtains the required and supported updates or extended support from the vendor. The requirement to purchase updates or extended support from vendor will apply at any time, regardless of any contract term, term commitments, or renewal periods. Customer's failure to do so may result in Lumen's inability to provide the Services and Lumen will have no liability therefrom.

4.13 Customer consents to Lumen's and its affiliates or subcontractors' use and transfer to the United States, or other countries, information (including Customer Contact information such as names, phone numbers, addresses and/or email addresses) of the Customer for the sole purpose of: (i) fulfilling its obligations under the Agreement; and (ii) providing information to Customer about Lumen's products and services. Customer represents that it will ensure that all information provided to Lumen is accurate at all times and that any business contact has consented to Lumen's processing of such information for the purposes identified herein.

4.14 Customer consents to Lumen collecting and compiling system and security event log data to determine trends and threat intelligence. Lumen may associate this security event log data with similar data of other Customers so long as such data is merged in a manner that will not in any way reveal the data as being attributable to any specific Customer.

4.15 Customer is responsible for returning all hardware, software and any related components to Lumen upon expiration or termination of the Service.

4.16 If a Customer requests any assistance to transition firewall Services either in-house or to a new service provider, Customer and Lumen must mutually agree on such assistance.

4.17 Customer agrees that Lumen's SLA only applies to currently supported configurations (including but not limited to related devices, software, and operating systems) at the time SLA support requests are triggered.

Tables and Appendices

Table 1.0 Standard Roles and Responsibilities for Dedicated and Logical Firewalls

Activity	Task	Lumen	Customer
Design / Installation	While based on the firewall policies, the firewall architecture is the vision and logical building blocks needed to feed into final firewall design, including the network diagram, based on the Customer organizations security policies.	X	
	Selection of the firewall appliances that meet the Customer's firewall policies and architecture requirements.	X	X
	The detailed design and technical features delivered within the service, required for the Customer firewalls supported by Lumen. Examples of design can include inclusion of logical firewalls and VPN.	X	X
	The creation of Customer rules that govern the device configuration policies.		X
	Verification that device configuration meets the Customer's security requirements.		X
	Perform an initial set-up consultation with the Customer.*	X	
	Provide all required information during initial consultation.		X
	As applicable in Lumen provided environments, installation of physical devices to Lumen standard, including racking and cabling.	X	
	As applicable on Customer premises, physical device shipped to Customer premises for Customer to install.		X
	Installation of operating system and applicable patches to Lumen standard.	X	
	Optional Customer Policy & Migration support in addition to base build configuration	X	
	Creation of Lumen base build configuration (including logging and alert configuration).	X	
Configuration	Configure alert policy and response procedures for Customer.	X	
	Deployment of the firewall policy.	X	
	Perform a one-time security review of the network configuration, firewall rule-set, make recommendations for security improvements.*	X	
	Provide configuration of firewall hardware and software to the Customer's rule-based Internet security policy.	X	
	Set device to steady state operational status based on customer acceptance.	X	
Administration	Adherence to industry standard security, privacy, and all other applicable compliance regulations.		X
	Request and gain approval of changes to the firewall policy rules via the Customer's change management process.		X
	Change firewall policy rules after appropriately approved via Lumen's change management process.	X	
	Provide policy review to enhance the performance of the firewall policy.*		X
	Oversee the continuous observation of firewall logs.		X
	Conduct periodic testing to verify that firewall rules are functioning as expected and to confirm that the firewall policy rules remain in compliance with security policy.		X
	Carry out the regular backup of firewall configuration and policies.	X	

Activity	Task	Lumen	Customer
	Provide the hit count against Customer firewall at Customer's request.	X	
	Provide an explanation of the firewall reports and statistics provided in the applicable portal, upon request.	X	
	Lumen will monitor firewall resource utilization and initiate support tickets to engage Customer and address issues.	X	X
	Lumen will collect SNMP statistics on firewall performance and make available in the applicable portal.	X	
	Conduct ICMP (e.g., ping) monitoring of the firewall to determine system availability (24/7). In the event that the firewall fails to respond, Lumen will notify Customer via phone and/or email and initiate corrective action.	X	
Testing	Verification of the rule set includes both reviewing the rule set manually and testing whether the rules work as expected.	X	X
	Test that all relevant network connections can be established and maintained through the firewall.	X	X
	Verification of the rule set includes both reviewing the rule set manually and testing whether the rules work as expected. Testing that network traffic that is specifically allowed by the configured firewall policies are permitted. Testing that all network traffic that is not allowed by the stated firewall policies are blocked.	X	
	Verification and testing that network communications between Customer specified application components, that traverse the firewall, perform as per the firewall policies.		X
	Testing and verification that Security Analysts can configure and manage the firewall effectively and securely from the appropriate networks.	X	
	Testing that firewall logging is performing in accordance with the Customer's logging requirements.	X	
	The testing that known firewall operating system vulnerabilities are identified and patched.	X	
	Customer to sign off on the firewall testing prior to Lumen support initiated.		X
Maintenance and Support	Patch devices as required or when the Customer requests for a specific patch that has been approved by Lumen.	X	
	24/7 support for firewall problem resolution and Customer inquiries.	X	
	Maintain vendor based maintenance / support contracts to enable code updates and patches.	X	
	As applicable to Lumen provided environment, provide hardware break-fix support for new equipment within guidelines of vendor support agreements.	X	
	Notify Customer via phone and/or email and initiate corrective action in the event that the device fails to respond.	X	

* Tasks listed in Installation and Configuration are performed one time only, and are not included in the ongoing Administration, Maintenance and Support of the Service. Additional services may be available for an additional fee and may require additional contract documents to be signed.

Table 2.0 System Security and Event Logs Retention

Data	Location	Event Log Retention
Check Point Raw firewall log files - denied traffic	In Lumen provided environment or Customer premise	30-day online (rolling)

Check Point IPS and NextGen events	In Lumen provided environment or Customer premise	90-days online (rolling)
Cisco Raw firewall log files - denied traffic	In Lumen provided environment or Customer premise	30-day online (rolling)
Cisco IPS and NextGen events	In Lumen provided environment or Customer premise	90-days online (rolling)
Palo Alto logs and events	In Lumen provided environment or Customer premise	90 days default with 1, 3, 5, and 7 year options

Table 3.0 Roles and Responsibilities for Additional/Optional IPS and NextGen Options

Activity	Task	Lumen	Customer
Design / Installation	Verification that device configuration adheres to the Customers organizational security policies.		X
	Perform an initial set-up consultation with the Customer.	X	
	Develop the Customer's alert policy, determine the appropriate response procedure, and answer Customer's questions regarding service or monitoring options.	X	
	Provide all required information as requested by Lumen during initial consultation.		X
	Installation of physical devices to Lumen standard, including racking, cabling within the Lumen provided environment.	X	
	Installation of physical devices per Lumen requirements, including vendor's recommendations. This includes racking, cabling on Customer premise.		X
	Physical device shipped to Customer premises for Customer to install.	X	
	Software Installation: Installation of software in accordance with the vendor's recommendations.	X	
	Patch devices as required or when the Customer requests for a specific patch that has been approved by Lumen.	X	
Configure	Configure alert policy and response procedures for Customer.	X	
	Deployment / configuration of baseline policies as mutually agreed in advance.	X	
	Validate that network connections can be established and maintained through the IPS module.	X	
	Implement proactive deny rules as part of IPS configuration.	X	
	Request additional IPS deny rules to meet Customer risk and security requirements.		X
	IPS is configured inline and Customer can request traffic not be blocked.	X	
	Review IPS deny policy to be covered within implementation meeting between Lumen security personnel and the designated Customer contact.		X
	Customer to request specific IPS rules and filters (if not captured via monitoring).		X
	Apply applicable signatures.	X	
	Customer provides specific IPS signatures.		X
	Creation of Lumen base build configuration (including logging and alert configuration).	X	
	Evaluate the alert traffic for false alarms and make appropriate recommendations for policy tuning.	X	
	Make required adjustments to the policy as necessary; set device to full monitored status.	X	
Administration	Advise Lumen of any compliance regulations.		X
	The creation of alerting and notification documentation to include alert policies and escalation procedures.	X	

Activity	Task	Lumen	Customer
	Maintain the network diagram showing the placement of the device within the network.	X	
	Request and gain approval of changes to the policy rules via the Customer's change management process.		X
	Change policy rules after approved via the Customer's change management process.	X	
	Provide policy review to enhance the performance of the policy.		X
	Up to twice a year tuning to verify that IPS rules are functioning as expected, when requested by the Customer.	X	
	The regular backup of policies and configurations	X	
	Provide the Customer with access to alert reports for the previous 90 days via a secure Web-based interface.	X	
	Explanation of the reports and statistics provided in the applicable portal(s).	X	
Monitoring	Oversee the continuous observation of health and availability alerts and or events that are reported from the device.	X	
	Oversee the continuous observation of IPS alerts and events.	X	
	Implement various health checks such as ICMP (e.g., ping) monitoring and pre-set test event triggering of the sensor to determine system availability (24/7) where practical.	X	
	Portal access to monitor events.		X
Testing	Verification of the rule set includes both reviewing the rule set manually and testing whether the rules work as expected. Testing that network traffic that is specifically allowed by the configured IPS and NextGen policies are permitted. Testing that all network traffic that is not allowed by the stated IPS policies are blocked.	X	
	The testing that known operating system vulnerabilities are identified and patched.	X	
	Verification and testing that network communications between Customer specified application components, that traverse the IPS, perform as per the IPS policies.		X
	Testing and verification that IPS administrators can configure and manage the IPS effectively and securely from the appropriate networks.	X	
	Testing that logging and alerting are performing in accordance with the Customer's logging and alerting requirements.	X	
	Customer to sign off on testing prior to Lumen support initiated.		X
Maintenance and Support	As applicable to Lumen provided environments, provide hardware break-fix support with a next business day response time for new equipment.	X	
	Patch devices as required or when the Customer requests for a specific patch that has been approved by Lumen.	X	
	Lumen will provide Customers at their request a bi-annual review of the Customer's IPS policy and log summary.	X	
	Initiate a request for a bi-annual review through SOC.		X
	24/7 support for firewall problem resolution and Customer inquiries.	X	
	Provide vendor based maintenance / support contracts to enable code updates and patches.	X	
	Notify Customer via phone and/or email and initiate corrective action in the event that the device fails to respond.	X	

Table 4.0 Customer Premises Physical Site Requirements

Item	Requirement
Physical Environment	Predefined and adequate rack shelf or space for installation, with unobstructed entry for Lumen and others working for Lumen.
Electrical Power	Electrical outlet.
	Extension wiring if distance to the electrical outlet is greater than (6) six feet.
	Power supply ready at installation location.
Support modem communication	Dedicated analog (dial-up) line for the support modem with inbound direct dial capability.
	Extension wiring if distance to the analog line termination is greater than (6) six feet.
	Customer will arrange and pay for a standard (POTS) telephone line (with direct inward dialing) for each Customer site to enable Lumen to perform remote network management functions on the Managed Firewall appliance. Customer may provide an alternative out of band access to the Managed Firewall appliance for Lumen and Customer authentication and ongoing management support. Lumen will not provide service level objectives or SLAs for any problems related to the delivery of the Managed Firewall Service on Customer Premises if this telephone line is not available, or if is not functioning properly when required.
Connectivity	Always-on Connection: If it is not already available, the Customer must purchase an always-on connection to the public Internet (DSL, T1, cable modem etc.) Dial-up connection is not sufficient. Customer is required to maintain Internet connectivity as Customer Premises installations, management and alert events are transmitted to the Lumen infrastructure utilizing a Customer-provided Internet connection.
	Ethernet LAN topology. Customer must provide IP addresses for all network connections to the firewall, the number of which will be determined by Lumen. To avoid degradation of the Service, Customer must not have sustained bandwidth exceeding rated capacity of the device.
	Customer provides capacity for two external interfaces and IP addresses for each firewall. This is for primary internet connection and network management.

Table 5.0 Roles and Responsibilities VPN Users and Site-to-Site VPNs

Activity	Task	Lumen	Customer
Configuration	Administration of Customer managed devices for Customers opting for site to site VPN option.		X
	Testing that the VPN Solution is working.		X
	Provide support for 24x7x365 end user administration requests by Lumen system administrators for Customers using Managed Hosting services within a Lumen data center for Customers opting for Client VPN user service option.	X	
	Configuration of Lumen managed firewall.	X	
	Authentication and configuration of username and password for VPN users using Lumen's managed Microsoft Active Directory services for Customers using Managed Hosting services within a Lumen provided environment and opting for the Client VPN user option.	X	

Activity	Task	Lumen	Customer
	Configure one VPN user group as part of this service for Customers opting for the Client VPN user option.	X	
	Enable split tunneling configuration.	X	
	Enable self-signed certificate for Client VPN connections on the firewall for Customers opting for the Client VPN user option.*	X	
	Provide IP address assignment for Client VPN users for Customers using Managed Hosting services within a Lumen provided environment and opting for the Client VPN user option.	X	
	Configuration of "A-End", Lumen end of VPN.	X	
	Configuration of "B-End", Customer end of VPN.		X

* Tasks listed in Installation and Configuration are performed one time only, and are not included in the ongoing Administration, Maintenance and Support of the Service. Additional services may be available for an additional fee.

Appendix A: Service Level Agreement

Response Times for Managed Firewall Service

Response descriptions for the Managed Firewall Service are referenced in the Incident Management and Request Management sections below that describe the priority levels.

- Fault reaction time to Service outage. Maps to Priority 1 (P1) (Urgent).
- Hardware fault resolution time to Service outage: If Lumen determines that the device must be swapped, Lumen will complete the swap by the next business day for most service locations from the date of problem detection.
- Configuration changes to firewall rule-set. Maps to Priority 3 (P3) (Medium)

Response descriptions for the Managed Firewall Service with IPS Option are referenced in the Incident Management and Request Management sections below that describe the priority levels.

- IPS Critical Alarm. Maps to Priority 2 (P2) (High)
- IPS Configuration and Policy Change Request. Maps to Priority 3 (P3) (Medium)
- IPS new Configuration request. Maps to P3 (Medium)

Response descriptions for the VPN options available with the Managed Firewall Service are referenced in the Incident Management and Request Management sections below that describe the priority levels.

- Fault reaction time to IP VPN Service outage. Maps to P2 (High)
- Configuration change requests associated with VPN users. Maps to P3 (Medium)

Response Time Priorities for Incident Management

Priority	Priority Definition	Reponse Time for Proactive Monitoring	Initial Response from the Client Response Centers to phone calls or Customer emails	Resolution Target based on resource availability	Initial triage to Customer escalations	Communications Methods
P1 Urgent	Business impacting or imminent impact; full site outage; A system or device is down; Customer cannot perform business critical functions.	Initial Response Time: Active Alert Owned/ Acknowledged within 10 minutes. Initial Notify Customer: Lumen will notify Customers within 15 minutes via email. Priority 1 and 2 Will be followed up with a phone call after investigation has	Call Response Time: Immediate. Average Speed of answer: <20 seconds Email Response Time: Within 6 hours	Work with Customer to implement as soon as possible. Target within 5 hours.	PRIORITY 1 INCIDENTS must be called into the relevant Client Response Center. USA: 888-638-6771 CANADA: 866-296-5335 EMEA: 011-44-118-322-6100 ASIA: 011-65-6768-8099	PRIMARY METHOD: Phone call while case status = Open-Solving SECONDARY METHOD: Method of receipt either call, email or portal to case contact. FREQUENCY: Every 1 hour or as agreed with Customer contact.
P2 High	Partial site outage/loss of redundancy; A system or component is			Target within 12 hours.	Response Time: 1 hour	PRIMARY METHOD: Phone call while case status = Open-Solving

	down; Customer may be experiencing degradation of service, or loss of resilience.	confirmed an incident exists.				SECONDARY METHOD: Method of receipt Either call, email or portal to case contact FREQUENCY: Every 1 hour or as agreed with Customer contact
P3 Medium	Incident/ Non-Business Impacting; A system is experiencing minor issues or an individual system component has failed, however is not causing degradation of service.			Target within 48 hours.	Response Time: 2 hours	PRIMARY METHOD: Phone call while case status = Open-Solving SECONDARY METHOD: Method of receipt Either call, email or portal to case contact FREQUENCY: Every 1 hour or as agreed with Customer contact
P4 Low	Incident/ Non-Business Impacting; No service issues but low level incident required to investigate minor issue.			Target within 60 hours.	Response Time: 4 hours	PRIMARY METHOD: Phone call while case status = Open-Solving SECONDARY METHOD: Method of receipt Either call, email or portal to case contact FREQUENCY: Every 1 hour or as agreed with Lumen and Customer contact

Response Time Priorities for Request Management

Request Category	Request Description	Scheduled Completion Target based on resource availability	Initial Response to Portal Requests (Preferred Method)	Triage to Request Emails (Secondary Method)	Communications Methods
P1 Urgent	Emergency request in order to avoid potential business impact. Example: Immediate Remote Hands for server down.	Work with Customer to implement as soon as possible.Target wit hin 8 hours.	PRIORITY 1 REQUESTS must be called into t he relevant Global Hosting Client Response Center. USA = 888-638-6771 CANADA = 866-296-5335 EMEA = 011-44-118-322-6100 ASIA = 011-65-6768-8099		PRIMARY METHOD: Phone call while case status = Open-Solving SECONDARY METHOD: Method of receipt either call, email or portal to case contact. FREQUENCY: Every 4 Hours or as agreed with Customer contact.
P2 High	Non-standard service request that the Customerre quires in order to complete da y-to-day business activity. Example: Ad-hoc backup to be completed by nextw orking day.	Target within 24 hours	Initial Response Time: 2 hours	Initial Response Time: 6 hours from receiptof email to Security Operations Center	PRIMARY METHOD: Phone call while case status = Open-Solving SECONDARY METHOD: Method of receipt either call, email or portal to case contact. FREQUENCY: Every 8 hours or as agreed with Customer contact.
P3 Medium	Standard service request. Example: Requestfor information, query or password reset etc.	Target within 48 hours	Initial Response Ti me: 4 hours		PRIMARY METHOD: Phone call while case status = Open-Solving SECONDARY METHOD: Method of receipt either call, email or portal to case contact FREQUENCY: Every 24 hours or as agreed with Customer contact
P4 Low	Minor service request with no urgency or to be scheduled to	Target within 60 hours	Initial Response Ti me: 6 hours		PRIMARY METHOD: Phone call while case status = Open-Solving

	work with the Customer such as (Remote Hands). Example: Remote H ands scheduled for dd/mm/yy @ hh:mm to coordinate patch cable moves.				SECONDARY METHOD: Method of receipt either call, email or portal to case contact. FREQUENCY: Update upon completion of the request or as agreed with Customer contact.

SLA Payout
In the event that Lumen fails to achieve the P1 Response Time outlined in the table above, and such failure is not the result of an Excluded Event, Customer will be entitled to a service credit in the amount of three percent (3%) of the affected service MRC. In no event will the credits accrued in any single month exceed, in the aggregate across all response time goals and incidents, thirty percent (30%) of the invoice amount for the affected service.

SLA Process
Customer must request any credit due under this SLA by submitting an e-mail to billing.department@Lumen.com within sixty (60) days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this sixty (60) day period. Credits will be issued once validated by Lumen and applied toward the invoice which Customer receives no later than two (2) months following Customer's credit request. All performance calculations and applicable service credits are based on Lumen records and data.

This SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies in this SLA will not apply and Customer will not be entitled to receive a credit in the case of an Excluded Event. "Excluded Event" means any event that adversely impacts the Service that is caused by:

a) the acts or omissions of Customer, its employees, customers, contractors or agents
b) the failure or malfunction of equipment, applications or systems not owned or controlled by Lumen
c) Force Majeure events
d) scheduled and/or emergency maintenance
e) any suspension of Service pursuant to the applicable Service Attachment or Agreement
f) the unavailability of required Customer personnel, including as a result of failure to provide Lumen with accurate, current contact information
g) Customer's inability to fulfill Customer's responsibilities as defined in the Agreement or Service Attachments including but not limited to providing Lumen's approved personnel immediate access, whether on Lumen or Customer premises, to Lumen-owned firewall if there is a service outage and at reasonable times in all other situations, ensuring any necessary permissions needed for installation and operation are in place, and ensuring accesses when the Customer has an Access Control List (ACL) that interferes with management connections.
h) Any problems caused by or associated with the Customer's failure to meet specified Customer Requirements or Customer Responsibilities.
i) Any Customer provided connectivity,network installation or underlying Internet access service.
j) Any security tests.

Definitions

Access Control Lists (ACL): An **access control list** (**ACL**) is a list of access control entries with permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

Intrusion Prevention Systems (IPS): An IPS is a network security appliance monitoring network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Logical Firewall: A separate logical firewall instance with its own routing and forwarding tables with independent policies and rules. These are only available on a dedicated physical firewall. Firewall vendors may reference logical firewall instances as "virtual context", "virtual systems", "virtual instance", or "virtual domains".

Maintenance Windows: Lumen will use commercially reasonable efforts to perform routine maintenance only during defined maintenance windows. See our published Maintenance Window schedule, or navigate to https://www.ctl.io/legal/managed-hosting/maintenance-windows/ from any Internet browser. Lumen has the right to perform scheduled maintenance (during the windows specified), which may limit or suspend the availability of the Services.

NextGen: The evolution of firewall appliances adds anti-virus, anti-spam, URL filtering and additional threat defense capabilities to the traditional firewall. Not all NextGen features will be supported on all vendor platforms.

Security Operations Center: The Lumen support center for resolving issues that is staffed 24/7/365 to respond in a timely manner to incidents and requests. This includes the GSOC or Global Security Operations Center, also often called SOC.

SNMP: Simple Network Management Protocol is a standard approach to obtaining network management statistics.