CenturyLink Technology Solutions Service Guide

Managed Firewall Care 3.0 IDC

This CenturyLink Service Guide (“SG”) sets forth a description of CenturyLink Managed Firewall Care 3.0 IDC (“Service”) offerings including technical details and additional requirements, if any. This SG is subject to and incorporated into the Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

Products Included:
Managed Firewall Care 3.0 IDC

Version	Previous	Section Modified	Date
SEC-20141003-SG-FirewallCareServices	SEC-20100420-External-SSG-GL-Firewall_Care_Services	All	October 3, 2014

Table of Contents

Service Description

Managed Firewall Care 3.0 IDC

1. **Service Descriptions:**
   Managed Firewall Care 3.0 IDC with IPS option: Managed Firewall Care 3.0 with IPS option is a CenturyLink provided service (the "Service"). The standard features of the Service consist of the installation, configuration, administration, monitoring, maintenance and support of the components in Table 1.0. The Service Level Agreement (SLA) associated with this Service is located in Appendix D. CenturyLink does not represent or warrant that the CenturyLink Equipment or the Service will be uninterrupted or error-free; will detect or generate an alert for every security event that may be recorded in Customer logs, or meets any particular data security standard.

   Managed Firewall Care 3.0 Service in IDC
   Service Description: Managed Firewall Care 3.0 Service in IDC is a CenturyLink provided service (the "Service"). The standard features of the Service consist of the installation, configuration, administration, monitoring, maintenance and support of the components in Table 2.0. The Service Level Agreement (SLA) associated with this Service is located in Appendix D. CenturyLink does not represent or warrant that the CenturyLink Equipment or the Service will be uninterrupted or error-free; will detect or generate an alert for every security event that may be recorded in Customer logs, or meets any particular data security standard.

1.1. **Service Components:**

1.1.1. **Dedicated Firewall Appliances:** Supported system configurations with and requirements are listed in Table 1.0 and Table 2.0 Supported Systems, Platforms and Requirements.

1.1.1.1. **Cisco ASA Firewall** (Customer – owned) residing in Customer's server-hosting facilities at CenturyLink. The Customer to provide ASA device / license(s) and associated support contracts needed to perform the Service.

1.1.1.2. **Check Point 4000 Series** (Customer-owned) within a CenturyLink IDC. The Customer to provide Check Point device / license(s) and associated support contracts needed to perform the Service.

1.2. **Design/Installation:** CenturyLink will provide installation tasks marked with an "X" in the CenturyLink column in Table 3.0 Standard Roles and Responsibilities.

1.2.1. **Billing Cycle:** The Service will be considered installed for billing following the initial five-day burn-in cycle. Following the burn-in period and any follow-up conversations with Customer to discuss alert traffic, required adjustments will be made to Customer's policy as necessary, and the device will be set to blocking status if approved by Customer.

1.2.2. CenturyLink will provide on-site installation of the firewall.

1.2.3. For Check Point service CenturyLink will provide the management license required to integrate Customer-owned device into the CenturyLink Check Point management infrastructure.

1.3. **Configuration:** CenturyLink will provide configuration tasks marked with an "X" in the CenturyLink column in Table 3.0 Standard Roles and Responsibilities.

1.3.1. **Rule Request Changes:** CenturyLink system administrators will perform ongoing firewall configuration upon receipt of rule request changes from Customer. CenturyLink reserves the right to refuse rule-set and configuration changes it deems unnecessary in its reasonable discretion.

1.3.2. **Backup and Storage:** CenturyLink will provide firewall configuration data backup and off-site storage of the current configuration for the time period in which the Customer maintains the Service with CenturyLink.

1.4. **Administration:** CenturyLink will provide administration tasks marked with an ”X” in the CenturyLink column in Table 3.0 Standard Roles and Responsibilities.

1.4.1. **System Administration:** CenturyLink will manage all system administration and passwords. Customer will not have access to passwords or be able to make direct changes to the configuration. Instead, Customer must request changes by contacting the CenturyLink Service Center. Customer must provide complete authentication credentials to the CenturyLink Service Center when requesting changes.

1.4.2. **Reporting:** Standard reporting available via the Customer portal can be found in Table 7.0 Standard Reporting. Rate limiting of firewall log traffic will be implemented to protect firewall from denial of service type attacks.

1.4.3. **Data Retention:** See Table 6.0 Data Retention Files for a list of the files that will be retained and the length of time.

1.5. **Monitoring:** CenturyLink will provide monitoring tasks marked with an ”X” in the CenturyLink column in Table 3.0 Standard Roles and Responsibilities.

1.5.1. **SNMP Statistics:** Conduct SNMP statistics on firewall performance and make available via CenturyLink Customer facing web portal. (Only available with Cisco ASA-based appliance).

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

1.6. **Maintenance and Support:** CenturyLink will provide maintenance and support tasks marked with an ”X” in the CenturyLink column in Table 3.0 Standard Roles and Responsibilities.

1.6.1. **Upgrades:** CenturyLink may periodically upgrade the security software to maintain the latest versions in operation. If CenturyLink determines an upgrade is necessary, CenturyLink will work with Customer to schedule a time to make necessary changes, preferably during the Scheduled Maintenance Windows. Customer must allow CenturyLink to make these changes within five (5) business days of receipt of the request from CenturyLink, or CenturyLink’s obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes. If CenturyLink determines that an emergency security change is required, CenturyLink will make the change as quickly as possible. CenturyLink will make commercially reasonable attempts to contact the Customer’s technical contact prior to making said change.

2. **Customer Responsibilities:** Customer is responsible for all tasks marked with an ”X” in the Customer column in Table 3.0 Standard Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 3.0 may result in CenturyLink’s inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer’s failure.

2.1. **Customer Installation Requirements in CenturyLink Data Center:**

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

2.1.2. **Permissions:** Ensure that all permissions of any kind needed for the installation and operation of CenturyLink-owned equipment are in place at all times

2.1.3. **Connection Management:** If the Customer has an Access Control List (ACL) that interferes with management connections, the Customer must allow CenturyLink access for management and monitoring.

2.1.4. **IP Address:** Customer must provide IP addresses for all network connections to the device and the secure management device, the number of which will be determined by CenturyLink.

2.1.5. **Bandwidth:** To avoid degradation of the Service, Customer must not have sustained bandwidth exceeding rated capacity of the device.

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

2.1.7. **Third Party Software:** If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

3. **Additional Services:** At Customer's option and expense Customer can choose to have CenturyLink complete one or more of the service options listed below. The items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work ("SOW") or Service Order. Contact a sales representative for additional information.

3.1. **IPS (Cisco ASA only):** Customer can choose to have CenturyLink setup and configure IPS. Customer must select an appliance that supports IPS from Table 1.0 Supported

3.1.1. **Roles and Responsibilities:** In addition to the Tasks listed in Table 4.0 Standard Roles and Responsibilities. CenturyLink will provide tasks marked with an "X" in the CenturyLink column in Table 4.0 IPS Roles and Responsibilities. The IPS deny policy could impact legitimate Customer activity, and is the sole responsibility of the Customer to review prior to implementation. The review of the IPS deny policy to be covered within the implementation meeting between CenturyLink security personnel and the designated Customer contact.

3.1.2. **Incident Response (IR):** Incident Response ("IR") is included in the Service if the Customer selects the IPS appliance. Incident Response as part of the IDS/IPS (intrusion detection and prevention) event investigation process will consist of the CenturyLink Service Center performing an analysis of the detected event. The IDS/IPS analysis may include the use of both internal and commercial tools in determining the event impact to a specific Customer environment. Review of system logs, system statistics and files from live systems may be used in the event analysis process, but only for CenturyLink managed security service devices.

3.1.3. **Vendor Supplied IDS/IPS Signatures:** Vendor supplied IDS / IPS signatures will be proactively applied to Customer devices on a weekly basis. The vendor may delay the release schedule for signature updates, thus impact the CenturyLink ability to perform signature updates on the weekly interval.

3.2. **VPN:** Customer can choose to add Remote Client or Client VPN Users. See Appendix A for additional information about the service and Table 5.0 VPN Roles and Responsibilities.

3.3. **ASA Virtual Firewall Option**: Customer can purchase virtual firewall in 5, 10, and 20 license increments. CenturyLink will support virtual firewall setup and configuration as an enhancement to the base firewall service. Vendor limitations may restrict the use of a virtual firewall with IPSec VPN with specific Cisco ASA code revisions. (See Appendix B).

3.4. **Spares:** On-site spare firewalls for Service in IDC are available at an additional cost to Customer and must be purchased in advance of expected use.

3.5. **Firewall Failover Solution:** The Failover Solution is designed to deliver firewall high-availability by providing a dedicated hot standby. In the event that the primary device fails, the secondary device detects the failure and begins operation.

3.6. **Ethernet Upgrade:** as with the main firewall appliance, the Customer will be responsible with procurement and support contracts associated with any upgrade cards. Upgrade cards to be supported under the Service. Network runs / connections to the firewall may incur additional costs.

3.6.1. **Check Point:** The Gigabit Ethernet upgrade for Check Point provides up to four (4) gigabit copper interfaces available for Customer use.

3.6.2. **ASA:** The Gigabit Ethernet upgrade for six (6) or 20-gigabit copper interfaces available for Customer use, depending on selected platform.

Tables and Appendices

Table 1.0 Supported Systems, Platforms and Requirements Integrated Firewall with IPS Care Service in IDC

Model	Additional Requirements
ASA5500-X	Supported with Customer provided IDS/IPS licensing
Software & Licenses	Description
OS	ASA – CenturyLink validated version
Cisco ASA	Unrestricted
	Customer provided security plus license for ASA5512-X required
Support Contract	Minimum support level includes:
The Customer must maintain a current Cisco support contract for ASA devices.	8 hours/day x 5 days/week next-business-day response time

Table 2.0 Supported Systems and Platforms Managed Firewall Care Service in IDC

System	Model	Additional Requirements
Checkpoint	4000 Series	Customer provided Firewall / VPN blade license
ASA	5500-X Series	Customer provided VPN licensing required if this service option is selected
Software & Licenses		Description
Cisco ASA / Checkpoint 4000 Series		CenturyLink will supply necessary management license. OS version is CenturyLink validated version of Vendor provided OS.
Support Contract		Minimum support level includes:
The Customer must maintain a current Cisco support contract for ASA or Check Point 4000 Series devices.		8 hours/day x 5 days/week; next-business-day response time

Table 3.0 Standard Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Design / Planning **Installation**	Firewall Architecture: 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	

Activity	Task	CenturyLink	Customer
	Firewall Selection: The owner of the final selection of the firewalls that meet the Customer organizations firewall policies and architecture.		X
	Firewall Design: The detailed design and technical features delivered within the service, required for the Customer firewalls supported by CenturyLink. Examples of design can include inclusion of virtual firewalls and VPN (if purchased by Customer)		X
	Establishment of Firewall Policy: The creation of Customer rules that govern the device configuration policies. Defined conforming to RFC spec for IPv4 or IPv6 addressing. IPv6 supported only on Cisco ASA based platform.		X
	Adherence to Security Policy: Verification that device configuration adhere to the Customers organizations security policies.		X
	Perform an initial set-up consultation with the Customer	X	
	Provide all required information during initial consultation		X
	Installation of physical devices to CenturyLink standard, including racking, cabling within the CenturyLink data centers.	X	
Configuration	Configure alert policy and response procedures for Customer	X	
	Firewall Policy Configuration: Deployment of the firewall policy	X	
	Perform a security review of the network configuration, firewall rule-set, make recommendations for security improvements	X	
	Provide customized configuration of firewall hardware and software to the Customer’s rule-based Internet security policy	X	
Administration	Provide adherence to industry standard 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 the Customer's	X	

Activity	Task	CenturyLink	Customer
	change management process.		
	Provide policy review to enhance the performance of the firewall policy.		X
	Oversee the continuous observation of firewall health and availability alerts and or events that are reported from the firewall.	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 firewall policy.		X
	Carry out the regular backup of firewall operating system, configuration, policies and rule sets.	X	
	Provide the hit count against Customer firewall at Customer's request	X	
Monitoring	Network Connectivity Testing: Testing that all relevant network connections can be established and maintained through the firewall.	X	
	Policy Connectivity Testing: Customer 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	
	Application Compatibility Testing: Verification and testing that network communications between Customer-specified application components, that traverse the firewall, perform as per the firewall policies.		X
	CenturyLink will monitor firewall infrastructure for performance load to include CPU and memory allocations to individual Customer virtual firewall instances.	X	
	CenturyLink will conduct SNMP statistics on firewall performance and make available via CenturyLink Customer facing web 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, CenturyLink will notify Customer via phone and/or email and initiate	X	

Activity	Task	CenturyLink	Customer
	corrective action.		
Testing	Rule Set 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 policies are permitted. Testing that all network traffic that is not allowed by the stated IPS policies are blocked.	X	
	Network Connectivity Testing: Testing that all relevant network connections can be established and maintained through the firewall.	X	
	Policy Connectivity Testing: Customer 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	
Maintenance and Support	Patch devices as required or when the Customer requests for a specific patch that has been approved by CenturyLink product team.	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
	Provide hardware break-fix support with a next business day response time for new equipment.		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 Roles and Responsibilities IPS Option

Activity	Task	CenturyLink	Customer
Planning/Design and Implementation	Develop the Customer's alert policy, determine the appropriate response procedure, and answer Customer's questions regarding service or IPS option	X	
	Software Installation: Installation of IPS software in accordance with the vendor's recommendations.	X	

Activity	Task	CenturyLink	Customer
	IPS Patch Installation: Patch devices as required or when the Customer requests for a specific patch that has been approved by CenturyLink product.	X	
	Evaluate the alert traffic for false alarms and make appropriate recommendations for policy tuning	X	
	IPS Policy Configuration: Deployment / Configuration of baseline policies.	X	
	Implement proactive deny rules as part of IPS configuration	X	
	Request additional IPS deny rules to meet Customer risk and security requirements		X
	Provide option to choose between three IPS configurations to meet Customer risk and security requirements	X	
	Review IPS deny policy to be covered within implementation meeting between CenturyLink security personnel and the designated Customer contact		X
	Provide portal view of daily summary report with detailed IPS denied events.	X	
	Custom IPS Rules and Filters: Customer specific IPS rules and filters (if not captured via monitoring).		X
	Vendor Signatures: Review and apply applicable signatures.	X	
	Custom Signatures: Customer specific IPS signatures		X
Configuration	CenturyLink will implement proactive deny rules as part of the IPS configuration.	X	
	Request additional IPS deny rules to meet their risk and security requirements.		X
	Review IPS deny policy and communicate needs between technical contact and provider		X
Administration	Provide adherence to industry standard compliance regulations.		X
	IPS Requirements Documentation: The creation of IPS alerting and notification documentation to include alert policies and escalation procedures.	X	

Activity	Task	CenturyLink	Customer
	IPS Design: The network diagram showing the placement of the IPS within the network	X	
	Request and gain approval of changes to the IPS policy rules via the Customer's change management process.		X
	Change IPS policy rules after appropriately approved via the Customer's change management process.	X	
	Provide policy review to enhance the performance of the IPS policy.		X
	Oversee the continuous observation of IPS health and availability alerts and or events that are reported from the IPS.	X	
	Oversee the continuous observation of IPS alerts and events.	X	
	IPS Policy Tuning: Twice a year tuning to verify that IPS rules are functioning as expected, when requested by the Customer.	X	
	Policy Backup: The regular backup of IPS policies and rule sets.	X	
	Web portal Self Service Setup: Initial setup of Self Service for IPS functionality.	X	
	Web portal Self Service Training: Explanation of the IPS reports and statistics provided.	X	
Monitoring	Receive and review alerts issued by the IPS device(s) according to the response time chart	X	
Maintenance and Support	CenturyLink Management Testing: Testing and verification that firewall administrators can configure and manage the firewall effectively and securely from the appropriate networks.	X	
	Web portal and Reporting: Access to the security web portal, where IDS / IPS events are available for appropriate organization personal review. IDS / IPS reporting to include: -Raw event detail for previous 90 days -Event summary graphs, with event break down into High / Med / Low severity. -Event Summary graphs, with detail on		X

Activity	Task	CenturyLink	Customer
	targeted and originating IP addresses. -Event Summary graphs to show IDS activity over the previous 90 days -Monthly IDS summary reports in PDF format		
	CenturyLink will provide Customers at their request a bi-annual review of the Customer's IPS/NIDS policy and log summary	X	
	Initiate a request for a bi-annual review through support center		X
	Provide the Customer with access to NIDS alert reports for the previous 90 days via a secure Web-based interface.	X	
	Firewall OS Vulnerability Testing: The testing that known firewall operating system vulnerabilities are identified and patched.	X	
	Testing of Logging and alerting: Testing that IPS logging and alerting are performing in accordance with the Customer's logging and alerting requirements.	X	
	Response to device issues, inclusive of coordination with vendor if necessary in accordance to IPS requirements documentation.	X	
	Implement various health checks such as ICMP (e.g., ping) monitoring and pre-set test event triggering of the NIDS sensor to determine system availability (24/7) where practical.	X	

Table 5.0 Roles and Responsibilities VPN Users

Activity	Task	CenturyLink	Customer
Configuration	Administration of Customer managed end points for Customers opting for site to site VPN option		X
	VPN Testing: Testing that the VPN Solution is working		X
	Provide support for 24x7x365 end user administration requests by CenturyLink system administrators for Customers using Managed Hosting services within a CenturyLink data center for Customers opting for Client VPN user service option	X	
	Configuration of CenturyLink ASA based managed firewall required to accept end	X	

Activity	Task	CenturyLink	Customer
	user’s Client VPN connections for Customers opting for the Client VPN user option		
	Authentication and configuration of username and password using CenturyLink’s managed Microsoft Active Directory services for Customers using Managed Hosting services within a CenturyLink data center and opting for the Client VPN user option	X	
	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 ASA appliance 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 CenturyLink data center and opting for the Client VPN user option.	X	
	VPN Configuration "A-End" (CenturyLink Side): Configuration of "A-End", CenturyLink end of VPN	X	
	VPN Configuration "B-End" (Customer Side): Configuration of "B-End", Customer end of VPN		X

Table 6.0 Data Files Retention

Data	Location	Retention Period
Raw firewall log files - denied traffic	In IDC	30-day online
NIDS/IPS events	In IDC	90-days

Table 7.0 Standard Reporting

Report Type	Frequency
Viewing of current rule-set on firewalls	12 hours, 24 hours, 48 hours, 1 day, 1 week,

Viewing of the firewall properties	1 month
Total of traffic on any physical port	
Total traffic dropped on any physical port	
Total traffic allowed on any physical port	
Breakdown of traffic type of any port (dropped, accepted, total)	
Per port traffic in – throughput	
Per port traffic out –throughput	

Appendix A: IP-VPN

Client VPN Users

Service Description:

The Remote Client to LAN functionality, offered at additional charge, connects Customer's end users to the CenturyLink managed ASA firewall securely via an encrypted session over the Internet. A secure VPN tunnel is initiated from Customer's end users leveraging the Cisco AnyConnect client software installed on the end user's computers. The Customer's end user VPN connection terminates into the CenturyLink Cisco based ASA managed firewall, at which point the Customer's end users can gain access to their network environment

Customer will provide the Cisco AnyConnect software and licensing for the requested number of Customer's Client VPN Users. Cisco AnyConnect will be supported for: Windows, Linux, MacOS X. Specific OS versions may vary. Please contact a Sales Representative for specifics.

CenturyLink will make commercially reasonable efforts to establish VPN communications link between the CenturyLink managed hardware endpoint and Customer's end user computers installed with AnyConnect client software. However, differences in software versions, configurations and conflicting applications may prevent the link from functioning. Administration of Customer computers will be the sole responsibility of the Customer. Client VPN connections will not carry any quality of service SLAs.

Configuration:

Includes configuration of CenturyLink ASA based managed firewall, required to accept end users' Client VPN connections.

- Client VPN User username and password authentication: will be configured using CenturyLink Managed Microsoft Active Directory services for Customers using Managed Hosting services within a CenturyLink data center.
- Client VPN Users Password Policy: Password policy to set expiration at 90 days for Customers using Managed Hosting services within a CenturyLink data center.

- Client VPN Users Authentication: Requests not using Managed Hosting services authentication will leverage Customer provided infrastructure

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

Additional Costs:

In many cases, an attack may require additional investigation to determine the source, impact, and to implement preventative measures. These additional services are not included with the Firewall Service, but are available from CenturyLink Security Services for an additional charge.

Additional VPN user groups will be considered additional instances of the Client VPN User Service. Additional sites (to more than two Customer or CenturyLink Managed end points) may be added for an additional charge for the Site-to-Site VPN Service.

Appendix B: Virtual Firewall

Virtual Firewall

The Customer may opt for Cisco ASA-based services, offered at an additional cost. Virtual firewall license will be provided by Customer in desired vendor increments. As part of the Virtual Firewall Service Option, CenturyLink will support virtual firewall setup and configuration as an enhancement to the base firewall service. Support of virtual firewall will be in 5, 10, and 20 license increments consistent with vendor licensing. Support of virtual firewall will require additional license(s) (one per firewall) to be purchased by Customer. Vendor limitations restrict the use of virtual firewall with IPSec VPN.

Customer should be aware that the implementation of Virtual firewall may negatively impact overall firewall performance.

Firewall Failover Solution

The Failover Solution is designed to deliver firewall high-availability by providing a dedicated hot standby. In the event that 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. CenturyLink 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.

Customer Installation Requirements

- In order for CenturyLink to ensure proper configuration and installation, Customer must provide CenturyLink with a topology of their existing network.
- For Customer Premises installations, management and alert events are transmitted to the CenturyLink infrastructure utilizing a Customer-provided Internet connection. Therefore, Customer is required to maintain Internet connectivity.
- Installation of the firewall service within a CenturyLink-managed environment will include 1U of rack space and power provided by CenturyLink. Installations not performed within the CenturyLink-managed environment will require Customer to provide 1U of rack space and necessary power for the firewall appliance.
- Installation of the firewall service within a CenturyLink-managed environment will include (2) VLANs, (2) 10/100 connections to each firewall appliance, and assignment of a public IP address for management. Installations not performed within the CenturyLink-managed environment will require Customer-provided

10/100 network connection(s) into Customer's switching infrastructure in addition to a Customer-provided public IP address for WAF management.

- Customer must provide IP addresses for all network connections to the firewall, the number of which will be determined by CenturyLink.
- The Customer will, using CenturyLink's standard procedures, notify CenturyLink of the initial and later changes to the firewall information to be configured by CenturyLink within the Managed Firewall appliance.
- If the VPN Site is located outside a CenturyLink IDC (not CenturyLink Managed Firewall appliances), then the following additional requirements apply:
    - The Customer must have a reliable and stable Internet connection.
    - Customer must have one IP address per hardware device.

Customer Responsibilities

Since the Service, as with all security systems, has potential vulnerabilities, the Customer should consider the Service as just one tool to be used as part of an overall security strategy, and not as a total solution.

- Customer must comply with all of its responsibilities under this CenturyLink Service Guide or CenturyLink's obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer does so.
- The Customer will not instruct or permit any other party to take any actions that would reduce the effectiveness of the managed integrated firewall appliance.
- Customer must provide dedicated analog (dial-up) line for the support modem with inbound direct dial capability.
- If the Customer's provider has an ACL on the Internet connections, the Customer must allow CenturyLink access for management and monitoring.
- Should CenturyLink determine the need for CenturyLink personnel to physically access the firewall or secure support modem, Customer must allow CenturyLink personnel access to their site.
- The Customer must maintain the vendor support contract as detailed in the "Supported Systems and Requirements" section above. Failure to maintain this contract may result in cancellation of CenturyLink's Firewall Care Service.
- For service deployments at customer premise sites, Customer will have responsibility for the physical network installation of the firewall appliance. Onsite installation services for deployments can be provided by CenturyLink, at an additional cost to Customer.

Fault reporting and service restoration

- Suspected faults on the Service should be reported to CenturyLink at the telephone number provided to the Customer for this purpose.
- To diagnose and resolve suspected faults, CenturyLink requires certain information when the problem is first reported. This may include:

Required Information
The CenturyLink references for the circuit(s) and/or any other part of a service thought to be affected
Symptoms of the problem
Details of any tests carried out in attempting to isolate the problem
Availability of access to the Customer site

Whether affected services can be taken out of service for testing, if necessary
The name and telephone number of the person reporting the fault

Appendix C: Site to Site VPN

Service Description:

Site-to-Site functionality connects Customer's sites securely via the Internet. A secure IPSec tunnel is created from the CenturyLink Managed Firewall to up to two Customer or CenturyLink managed end points.

CenturyLink will make commercially reasonable efforts to establish a VPN communications link between the endpoint connections; however, differences in software versions, configurations and conflicting applications may prevent the VPN from functioning. Customer endpoint devices must be licensed to accommodate DES, 3DES or AES encryption standards. 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.

Additional sites (to more than two Customer or CenturyLink Managed end points) may be added for an additional charge for the Site-to-Site VPN Service.

Non-CenturyLink Managed Firewall Appliances: If a VPN Site is located outside a CenturyLink IDC, and is not a CenturyLink Managed Firewall appliance, then the following additional Customer installation requirements apply:

- The Customer must have a reliable and stable Internet connection.
- Customer must have one IP address per hardware device.

Appendix D: Service Level Agreement

Managed Firewall Care 3.0 IDC with IPS option

Event	Response Time & Procedure
IDS Critical Alarm. Maps to SLO P2 (High)	**Reference Service desk SLO link off Savvisstation.com, Incident Management section.**
IDS / IPS Configuration and Policy Change Request. Maps to SLO P3 (Medium)	**Reference Service desk SLO link off Savvisstation.com, Request Management section.**
IDS / IPS new Configuration request. Maps to SLO P3 (Medium)	**Reference Service desk SLO link off Savvisstation.com, Request Management section.**

Managed Firewall Care 3.0 IDC

Response Description	Response Time & Procedure
Fault reaction time to Service outage. Maps to SLO P1 (Urgent).	**Reference Service desk SLO link off Savvisstation.com, Incident Management section.**
Hardware fault resolution time to	If CenturyLink determines that the firewall must be swapped, CenturyLink will

Service outage	complete the swap by the next business day from the date of problem detection.
Configuration changes to firewall rule-set. Maps to SLO P3 (Medium)	**Reference Service desk SLO link off Savvisstation.com, Request Management section.**

Response Times for VPN

Response Description	Response Time & Procedure
Fault reaction time to IP VPN Service outage. Maps to SLO P2 (High)	Reference Service desk SLO link off Savvisstation.com, Incident Management section.
	Requests related to troubleshooting Client VPN issues must first be directed to a central Customer contact for review, at which time the central Customer contact can open requests to Savvis.
Configuration change requests associated with VPN users. Maps to SLO P3 (Medium)	Reference Service desk SLO link off Savvisstation.com, Request Management section. Requests for VPN user changes must be submitted through a designated Customer contact.

Response Times SLA

In the event that CenturyLink is unable to provide service within the "Response Time" windows outlined above, the Customer's sole and exclusive remedy shall be a service credit in the amount of three percent (3%) of the affected service MRC for each response time failure. 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.

CenturyLink's obligation to meet stated Response Times will not apply to:

- any problems caused by or associated with the Customer's failure to meet specified Customer Requirements
- underlying Internet access service
- any security tests.

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this 30-day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer's credit request. All performance calculations and applicable service credits are based on CenturyLink records and data.

The applicable SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies hereunder 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 CenturyLink

c) Force Majeure events
d) scheduled maintenance
e) any suspension of Service pursuant to the Agreement
f) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information

General Service Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

Customer shall:

a) Provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.
b) Not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.
c) notify CenturyLink at least 5 business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes)
d) purchase and maintain a reliable, stable and always-on, high speed connection to the public Internet (i.e., DSL, T1, cable modem etc. -- a dial-up connection is not sufficient) and/or a standard (POTS) telephone line (with direct inward dialling) for each Customer Site to enable CenturyLink to perform remote network management functions.
e) Designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.
f) For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges. Provision of the Service is subject to Customer's compliance with this Section.

CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor able to make changes to the system configurations and must instead submit change requests to CenturyLink.

CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

Customer may incur additional charges if:

a) Customer impairs the Service;
b) CenturyLink dispatches a technician to a Customer Site and the technician is unable to complete the work because Customer was not available when the technician arrived.
c) Customer incurs three false alarms in a month; in which case, Customer will pay a $300 false alarm fee, plus an additional fee for each additional false alarm during that month (except where CenturyLink provides the Internet connection). Customer may request that CenturyLink discontinue Service monitoring in order to avoid false alarm fees; provided, however, CenturyLink shall have no further monitoring obligations whatsoever with regard to the affected Service. CenturyLink may require the purchase of Incident Response ("IR") Services, which consist of CenturyLink personnel responding to security events impacting Customer. IR services are limited to response and mitigation of incidents and do not include ongoing or long-term security consulting, which are subject to additional terms and charges.

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

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.

Adaptive Security Appliance (ASA): The core operating system for the Cisco ASA firewall class used for enterprise-class firewall capabilities for ASA devices such as- standalone appliances, blades, and virtual appliances -for any distributed network environment and also integrates with other critical security technologies.

CenturyLink Service Center: The primary organization for resolving infrastructure issues that is staffed 24/7/365 to respond in a timely manner to incidents and requests pertaining to Customer IT infrastructure.

Intrusion Detection System (IDS): An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

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.

Gigabit Ethernet: is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second).

Local Area Network (LAN): A local area network (LAN) is a computer network that interconnects computers within a limited area.

Maintenance Windows: A period of time designated in advance by CenturyLink, during which preventive maintenance that could cause disruption of service may be performed. Current Scheduled Maintenance windows are:

- Americas: Saturday 00:00AM to 5:00AM; Sunday 00:00AM to 5:00AM
- EMEA: Saturday 02:00AM to 6:00AM
- APAC (Except Japan): Saturday 21:00 (GMT) AM to Sunday 01(GMT)
- Japan: Sunday 04:00 (JST) to 8:00 (JST)

Network Intrusion Detection System (NIDS): A managed intrusion detection system with 24/7 monitoring and response to network security incidents that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity.

Reasonable Effort: A fair estimate of an activity, measured with reference to the particular circumstances, scheduling agreements and diligence as might be expected within the grounds of the Service. Just because something is possible and reasonable does not mean CenturyLink has to do it if it is not necessarily reasonable for the business.

Simple Network Management Protocol (SNMP)

Unified Threat Management (UTM)