SECURE GATEWAY SERVICES

1. GENERAL

1.1 **Service Definition.** Secure Gateway is a network-based service that securely connects Customer's private network to the public Internet through a logical, virtual port (Universal Port or Universal Port UBB or alternatively hosted Virtual Network Services – Routing service). Three versions of Secure Gateway are available:

- Retail and Remote Office (RRO), for users at fixed locations.
- Mobile User or Mobile Client, for mobile users.
- Firewall, a Verizon network-based solution that provides Customer with enhanced security when its end users are using Verizon Private IP Service to access the Internet. Firewall may be purchased in combination with RRO, Mobile User, or Mobile Client – or by itself.

1.1.1 **Platforms.** Except where explicitly stated otherwise, these terms apply to Optimized Service (denoted with a "+" and sometimes referred to as Rapid Delivery) and non-Optimized Service.

1.2 **Universal Port.** Customer selects either a Universal Port or a Universal Port UBB (Usage-Based Billing), depending on the desired version(s) of Secure Gateway and whether Customer wants charges to be based on its selected port bandwidth (for non-UBB) or its Usage Data Plan (for UBB). Mobile Client is only available with Universal Port UBB. Customers wanting Universal Port with UBB for RRO, Mobile User, or Mobile Client also will need the Virtual Router Service feature (described below).

Universal Port Type	Secure Gateway Versions Supported	Requires Virtual Router Service?	MRC Based On:
Usage-Based Billing	All – Optimized Service only	Yes	Usage Data Plan
Non-UBB	All except Mobile Client	No	Port Bandwidth

335984_7

1.3 **Standard Service Features – Virtual Router Service.** Virtual Router Service is a prerequisite for Customer's use of RRO or Mobile User/Mobile Client with Universal Port UBB. Virtual Router Service provides software-enabled virtual routers hosted on Verizon's network, each dedicated to Customer, thereby enabling better redundancy and offering a more scalable service to meet Customer's needs. Virtual Router Service enables Customer to connect a combination of RRO devices, as well as Mobile User and Mobile Client users, directly to the Universal Port UBB via encrypted tunnels, thus allowing remote devices and users to route traffic to Customer's Verizon-provided Private IP Service. The bandwidth of Virtual Router Service affects the number of concurrent tunnels supported.

1.4 **Optional Service Features**

1.4.1 **Partner DSL (Asia-Pac only) – Service Description.** Verizon provides Partner DSL Access (Partner DSL) to enable Customer to obtain access with Secure Gateway to Verizon's Private IP network via third-party-provided DSL circuits. Note that the transmission speeds available for selection are based on the maximum possible. If Partner DSL is interrupted or has other performance issues, Verizon will provide to Customer the information it has obtained from the third-party provider.

1.4.2 **Partner DSL – Customer Responsibilities.** Customer will:
- Ensure that its equipment and network are compatible with Partner DSL.
- Disconnect its equipment and network from the third party provider's network when the Service has ended.

2. **AVAILABLE VERSIONS**

2.1 **Retail and Remote Office**

2.1.1 **Service Definition.** With Retail and Remote Office (RRO), Verizon provides Customer with an end-to-end logical connection between Customer's corporate resources on Verizon's Private IP network and Customer's remote sites connected to the Internet or Verizon's IP network – via either a Universal Port, Universal Port UBB, or hosted Virtual Network Services – Routing service.

2.1.2 **Standard Service Features**

2.1.2.1 **Router Management.** For RRO, Verizon provides router management that includes configuration, set-up, administration, monitoring, support, and reporting (if applicable) for the RRO devices selected by Customer (each, a Managed Device) upon installation of such devices.

2.1.2.2 **RRO Site CPE Monitoring.** Verizon provides monitoring, alarm response, and email notification of the RRO CPE on a 24 x 7 x 365 basis.

2.1.2.3 **Reporting.** With RRO, Customer may also select WAN Analysis Reporting, which is available via a separate Service Attachment.

2.1.3 **Optional Service Features**

2.1.3.1 **Managed Device Feature – WAN Backup Service.** For RRO routers, Verizon will configure a Managed Device to support backup access (over separately-provided Verizon or third-party Internet service) in the event the primary circuit fails. Verizon will identify where WAN Backup is available outside the U.S. Mainland upon Customer's request.

2.1.3.2 **Backup Service Configuration Option.** With the Backup Service Configuration Option, Verizon will configure RRO at implementation to be used as a primary service for Customer's remote locations to connect to Verizon Private IP Service, or as a backup service to connect to its Verizon-provided Private IP network and Managed Devices under Verizon's Managed WAN Service.

2.1.3.3 **Quality of Service Support.** With Quality of Service (QoS) support on the RRO CPE routers, Verizon will route Customer traffic based on the priority assigned by Customer using different classes of service designations, which follow the Internet Engineering Task Force Differentiated Services or "Diff-Serv" model. If Customer does not set different classes, Verizon will route all Customer traffic using the BE class as the default priority designation.

2.1.3.4 **Network Engineering Service and Provisioning – Optional Change Management (OCM) (for Networks with 20+ Managed Devices under Full Management in the U.S.).** With Network Engineering, Verizon provides network design, planning, operating system vulnerability checks, network documentation change maintenance, and change-management support services for up to five Customer-requested OCM changes per week. Logical changes are provided on a one change-for-two Managed Devices basis; for example, a 50-device network permits support for up to 25 logical changes. Physical changes requested by Customer are not included within NE, nor is change management support for Managed Devices with more than a single routing table per device such as multi-VRF (virtual routing and forwarding)-configured routers. Verizon will inform Customer where Network Engineering is available outside the U.S. upon Customer's request.

2.1.3.5 **Optimized Service-Only Optional Features**
- **Managed Device Feature – Switching.** For Customers using Cisco-manufactured routers with added switch modules for additional ports and functionality, Verizon provides a switching feature to manage the LAN hardware module (but not the individual ports on the LAN module) that is a part of the Cisco routers.
- **Wireless LAN Controller Management.** With Wireless LAN Controller Management, Verizon will provide to RRO customers wireless LAN controller management capabilities for Customer network sites with access point CPE compatible with the controller.
- **Lightweight Access Point Management.** With Lightweight Access Point Management, Verizon will configure a supported CPE device embedded with access point functionality (e.g., a router configured with an antenna) such that it will interoperate with Verizon's Managed Wireless LAN Service.

2.1.3.6 **Embedded Wireless LTE.** For select Managed devices, an embedded LTE modem is available for use to provide wireless access as an access path, either as primary or backup to RRO.

2.1.4 **Customer Responsibilities**

2.1.4.1 **OOB Access.** Where available, OOB Access is an RRO service option that can be selected by Customer. Unless otherwise agreed, Customer will provide OOB Access to each Managed Device over a separate PSTN line (Analog OOB) or wireless connection (Wireless OOB). Direct console access connections are used to provide OOB Access to the Managed Devices. Console access works without an actual configuration on the Managed Device. Inline management requires a configured Managed Device. Where Verizon provides OOB Access, Customer will not interfere with it, or use it for any purpose other than enabling OOB management by Verizon. Unless otherwise agreed to by Verizon, disconnecting the OOB Service voids any SLAs provided by Verizon.

For Customer Sites with two or more circuits, Customer may utilize the alternate circuit or backup wireless options, where the backup access is used in lieu of either Analog OOB or Wireless OOB for

inline management access to the Managed Devices, by either connecting into two separate Managed Devices or into a single Managed Device.

Verizon also offers the No OOB option to Customers that do not have any OOB Access or backup access that can be used for management access.

2.1.4.2 **Alternative Internet Service Provider.** Customer may use RRO with Internet service from an alternative service provider (ASP) that offers appropriate Ethernet interface, speed, protocol, and remote access capabilities, the details of which are available from Verizon upon request. Where Customer chooses Internet service provided via an ASP, Customer is responsible for the installation and maintenance of all Customer-provided connections, including but not limited to the telephone line access circuit, to enable OOB management.

2.2 **Mobile User or Mobile Client.** With Mobile User or Mobile Client, Verizon provides Customer's mobile users secure access to Verizon's Private IP Network via a Verizon-provided or Customer-provided Internet service connection.
- Mobile User is a single-user service which utilizes software installed on a PC or other device to build an encrypted tunnel to Customer's Universal Port or Universal Port UBB.
- Mobile Client is a single-user service which utilizes software installed on a PC or other device to build an encrypted tunnel to Customer's Universal Port UBB only.
- Customer may have both Mobile User and Mobile Client services on the same Universal Port UBB service.

2.3 **Firewall.** Firewall provides perimeter security via a Verizon-network-based firewall. With Firewall, Verizon provides firewall configuration, administration, support, and the use of a firewall system consisting of firewall equipment and related software that is owned and supported by Verizon on its network. Verizon provides up to seven IP addresses with Firewall; additional IP addresses may be ordered.

3. **SUPPLEMENTAL TERMS**

3.1 **Availability.** Secure Gateway is not available for sale and deployment in India and Russia.

3.2 **Resale of Secure Gateway Services.** Secure Gateway is designed for use by Customer and its direct end users. If Customer wishes to resell Secure Gateway in its entirety to another person or entity, it will first work with Verizon to agree upon the terms and conditions appropriate for resale.

3.3 **Mobile User/Mobile Client.** Mobile User and Mobile Client each require the Mobile Workforce Manager Service, which is available from Verizon under separate Service Terms. Customer also will obtain all necessary licenses from the third-party provider of the Mobile Client for each end user that utilizes the Mobile Client service.

3.4 **Partner DSL.** If Partner DSL is no longer available from the third party provider for any reason, Verizon may terminate Partner DSL with reasonable notice to Customer. Where possible, Verizon will attempt to provide a replacement service.

3.5 **Acceptable Use Policy.** For purposes of Verizon's Acceptable Use Policy, Secure Gateway is deemed to be a Verizon Internet Service. If no policy exists for the country in which an Authorized User connects to the Verizon network, the U.S. Policy applies.

3.6 **Provisioning Entities in China.** In the event of regulatory changes in China affecting Verizon's ability to provide Secure Gateway, Verizon may terminate Secure Gateway without liability or where possible transition its provision of Secure Gateway to Customer via a different Third Party network supplier at a price to be agreed between the Parties.

4. **SERVICE LEVEL AGREEMENT.** The Secure Gateway Service Level Agreement (SLA) for Optimized Service is set forth at: www.verizonenterprise.com/external/service_guide/reg/cp_sgs_plus_sla.pdf. The Secure Gateway Service Level Agreement (SLA) for Non-Optimized Service is set forth at: www.verizonenterprise.com/external/service_guide/reg/cp_secure_gateway_services_sla.pdf.

5. **FINANCIAL TERMS**

5.1 **Optimized Service.** Customer will pay the charges for Optimized Secure Gateway + specified in the Agreement, including those below and at the following URL: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm. Charges below are in U.S. dollars and will be billed in the invoice currency for the associated service.

5.1.1 **Administrative Charges**

Administrative Charge	Charge Instance	NRC
Dispatch Charge (applies to both No Fault Found Dispatch Charge and re-dispatch if Customer not ready)	Dispatch/Re-dispatch	$300.00
Expedite Fee	Per managed device	$1,100.00
After Hours: Installation	Per site	$600.00

5.1.2 **Universal Port.** NRCs and MRCs are applicable to and are based on the selected bandwidth of the Universal Port. A secondary Universal Port (not available for load sharing) is configured as a back-up at no additional charge.

5.1.3 **Universal Port UBB (Usage-Based Billing).** Universal Port UBB usage charges will be based on the Usage Data Plan subscribed to by Customer. Customer usage is measured per month, and usage is reset to zero for the next month's measurement. Any usage in a given month above the selected Usage Data Plan will be billed on a per-Gigabyte (GB) basis. No credit is issued for Customer's usage below the selected Usage Data Plan. Customer may change its Usage Data Plan at any time. All Customer traffic routed through the Universal Port UBB will be measured by Verizon for inclusion in the monthly invoice, including Virtual Router Service and Firewall traffic.

5.1.4 **Virtual Router Service.** Virtual Router Service charges are determined based on the number of tunnels and maximum bandwidth required to support Customer's remote sites and end users.

5.1.5 **Retail & Remote Office.** Charges for router management are based on the size of the Managed Device.

5.1.6 **Mobile User/Mobile Client**
- For Universal Port, Mobile User supports up to 128 concurrent users with no additional charges for the Universal Port. Customer may order additional concurrent 128-user blocks for Mobile User for an additional MRC per block, fixed for Customer's Service Commitment.
- For Universal Port UBB the number of concurrent users supported for Mobile Client and Mobile User depends on the amount of bandwidth provided with the associated Virtual Router Service.

5.1.7 **Firewall and IP Addresses.** There are no charges for Firewall additional to the Universal Port or

Universal Port UBB charges set forth above. Customer will be charged an additional MRC, fixed for the Service Commitment, for IP addresses in excess of the first seven requested.

5.1.8 **Optional Change Management (OCM).** Customer can order remote change management support for Secure Gateway Services at the NRCs listed below:

Secure Gateway Optional Change Management Charges		
Change	**Change Instance (Charged per device unless noted)**	**NRC**
After Hours: Changes	Per request per site	$600.00
Implementation (Modify Existing)[1,3]	Change per device	$50.00
Design (Single Feature/Protocol)[2]	Change per device	$250.00
Design Plus (Multiple Feature/Protocol)[2]	Change per device	$400.00
1. Implementation is used to modify existing features or protocols including the following: dynamic host configuration protocol (DHCP), IP network address translation, network routed protocol, MNSO IP address/subnet mask change, permanent virtual circuit (PVC) Change, routing protocol changes, switch VLAN, dynamic port/CAR, and VPN Tunnel. 2. Design and Design Plus is used for requests to add single (Design) or multiple (Design Plus) new features, protocols or applications/policies that do not currently exist in the Customer Network, including the following: add DHCP, quality of service (QoS), NAT router configuration, traffic filter design, traffic shaping/queuing, application Aware routing, and SD WAN. 3. Customer may create a new design at one site by selecting Design/Design Plus to add the new feature(s) or protocol(s) and then replicate the design across other sites by selecting Implementation for the remaining sites.		

5.1.9 **Network Engineering (NE) Services Provisioning.** NE Service includes (i) annually up to one-half logical OCM change per Managed Device (e.g., a 50-device network permits support for up to twenty-five logical changes), and up to 0.25 full time equivalent (FTE) hours for every 75 Managed Devices (i.e., a total of two FTE hours per Business Day for every 75 Managed Devices). Additional changes can be supported for an additional OCM cost. NE charges cover only the required engineering services described. If Customer requests NE Services that exceed the standard FTE hours set forth above after being so advised by Verizon's Network Engineer, then Verizon reserves the right to charge, at Verizon's then current labor hourly rate, for the entirety of such NE service.

5.2 **Non-Optimized Service.** Customer will pay the charges for non-Optimized Secure Gateway specified in the Agreement. Online pricing for Services provided by a U.S. Verizon entity is at: www.verizonenterprise.com/external/service_guide/reg/cp_secure_gateway_services.htm.

6. **DEFINITIONS.** In addition to the definitions identified in the Master Terms, the following administrative charge definitions apply to Secure Gateway: www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm