

Secure Gateway Services  
Retail & Remote Office  
Mobile User  
Firewall

SERVICE LEVEL AGREEMENT FOR NON-OPTIMIZED SERVICE

1. Scope. This Service Level Agreement (“SLA”) applies to Secure Gateway Services Universal Port deployed on Cisco architecture. It covers two elements of Secure Gateway Services: (i) the Universal Port, which is used with each Secure Gateway Services-- Retail & Remote Office, Mobile User, and Firewall (standard and network-based); and (ii) the RRO CPE, which is deployed only on the Retail & Remote Office service. Further, this SLA applies to Retail & Remote Office only when the RRO CPE is Company -provided and under 24 x 7 maintenance coverage with a Next Business Day response time from Company or a Company - approved Alternative Internet Service Provider, as defined below.

This SLA is offered only to Secure Gateway Services that are provisioned on a Universal Port and does not apply to Secure Gateway Services provisioned on a different type of port.

The Service Availability SLA, as applicable to the Universal Port, covers the local loop and Internet service used to access the Universal Port only when they are ordered through or provided by Company pursuant to a U.S.-based contract. If Customer provides its own local loop and Internet service from a third party provider (Alternative Service Provider) such local loop or Internet service are not covered by this SLA. Moreover, when the cause of a Hard Outage (as defined below) is determined to result from Alternative Service Provider local loop or Internet service, no credit will be provided under this SLA.

Except as set forth in this SLA, Company makes no claims regarding the availability or performance of the Secure Gateway Services. This SLA sets forth Customer’s sole remedies for any claim relating to Secure Gateway Services, including any failure to meet any standard set forth in this SLA. Standard enhancements will become automatically applicable to Customer without notice as they are released. Company reserves the right to amend the SLA from time to time effective upon notice, as provided for in the Agreement, provided that in the event of any amendment resulting in a material reduction of the SLA’s service levels or credits, Customer may terminate the Secure Gateway Services without penalty by providing Company written notice of termination during the 30 days following notice of such amendment. Company may avoid such termination if, within 30 days of receipt of Customer’s written notice, it agrees to amend its Agreement for Secure Gateway Services to eliminate the applicability of the material reduction.

2. Service Availability.

- 2.1 Service Availability Standards. In the case of Retail & Remote Office, the standards for Service Availability vary by component and service method as shown below. For purposes of this SLA, “Broadband” service means services provided pursuant to Company’s Internet DSL and Cable services, or Company’s Internet Dedicated services (other than Internet Dedicated T1, which is identified separately in this SLA). The Service Availability SLA applies only to “Hard Outages”, i.e., an inability to exchange data between the Customer Edge and the Provider Edge in the case of Retail & Remote, and from the Company Internet backbone to the Provider Edge in the case of Mobile User and Firewall. Slow service or other service degradation is not considered a Hard Outage. Moreover, in those cases where Customer- provided local loop or Internet access is identified as the cause of the failure to meet the Service Availability SLA, then no credit will be provided under this SLA.

## Service Availability SLA

Component	Secure Gateway Service(s)	Service Method	Service Availability Standard
Universal Port	Retail & Remote Office, Mobile User and Firewall	N/A	100%
RRO CPE	Retail & Remote Office	Company local loop and Internet Dedicated T1 or T3	99.5%
RRO CPE	Retail & Remote Office	Company local loop, if required, and Broadband service	99.0%

- 2.2 Calculation. Service Availability is determined by adding (i) the total number of minutes during a calendar month that Secure Gateway Services was available to Customer to exchange data (i.e., not subject to a Hard Outage) between the Customer Edge and the Provider Edge, in the case of Retail & Remote Office, and between the Company Internet backbone and the Provider Edge, in the case of Mobile User and Firewall; plus (ii) any minutes during which the Secure Gateway Service was not available to exchange data due to events described in "Exclusions" and for the Service Installation SLA, "Service Installation Credit Process" below. Divide the sum by the total number of minutes in the billing month and multiply the quotient by 100.

The total number of minutes in a calendar month is as follows:

Month in Days	Total Minutes
31 Day Month	44,640
30 Day Month	43,200
29 Day Month	41,760
28 Day Month	40,320

- 2.3 Time to Repair ("TTR").

- 2.3.1 TTR Standards. The time-to-repair standards vary by component (RRO CPE or Universal Port) and service type. The TTR SLA applies only to "Hard Outages", i.e., an inability to exchange data between the Customer Edge and the Provider Edge in the case of Retail & Remote Office, and between the Company Internet backbone and the Provider Edge in the case of Mobile User and Firewall. Slow service or other service degradation is not considered a Hard Outage. Moreover, in those cases where Customer- provided local loop or Internet service is identified as the cause of the failure to meet the Service Availability SLA, then no credit will be provided under this TTR SLA.

## TTR SLA

Component	Secure Gateway Service(s)	Service Method	SLA
Universal Port	Retail & Remote Office, Mobile User and Firewall	N/A	4 hours or less
RRO CPE	Retail & Remote Office	Company local loop and Internet Dedicated T1 or T3	4 hours or less
RRO CPE	Retail & Remote Office	Company local loop, if	8 hours or

		required, and Broadband service	less
--	--	------------------------------------	------

2.3.2 Calculation. TTR is the time to correct a Hard Outage that Customer has reported as described in “Service Availability and TTR Credit Process” below. Customer’s TTR time starts when a Trouble Ticket is opened by Company for a Hard Outage and concludes with the restoration of Secure Gateway Service -- i.e., the time that the Hard Outage condition no longer exists. TTR for Universal Port includes the time needed to repair the Universal Port, its supporting elements and the backbone trunking to the Verizon Network Service. TTR for the RRO CPE at the Customer site includes time to repair the Company -provided local loop and Broadband service, the IPSec tunnel and the RRO CPE.

2.4 Service Installation – Installation Standards and Calculation. Service Installation time refers to the period of time to install the Universal Port and in the case of Retail & Remote Office, the RRO CPE at a site. The Installation SLA time period starts from the date all prerequisite steps forth in the table below have been taken and Company has received all required information to provide and bill the Secure Gateway Services and ends when the acceptance testing process has been completed.

Prerequisite Tasks Before Service Installation Period Begins

Component	Secure Gateway Service(s)	Service Method	Prerequisite Task (s)
Universal Port	Retail & Remote Office, Mobile User and Firewall	N/A	One active port on Company private network established; capacity check for Secure Gateway bandwidth above 43.000 Mbps
RRO CPE	Retail & Remote Office	Broadband service	One active port on Company private network established; one active Universal Port on Secure Gateway, and activation of Retail & Remote Office feature
RRO CPE	Retail & Remote Office	Alternative Service Provider local loop and Internet access	One active Port on Company private network established; Customer-provided local loop and access activation; one active Universal port on Secure Gateway, and activation of Retail & Remote Office feature

Service Installation SLA

Component	Secure Gateway Service(s)	Access Method	Installation Time Standard
Universal Port (and any other installable components ordered on Universal Port order)	Retail & Remote Office, Mobile User and Firewall	N/A	20 business days or fewer
RRO CPE	Retail & Remote Office	Company Internet Dedicated T1 or T3	45 business days or fewer that includes Company Internet Dedicated T1 or T3 activation
RRO CPE	Retail & Remote	Company local	20 business days or fewer

	Office	loop, if required, and Broadband service	
--	--------	--	--

2.5 Proactive Notification. Proactive Notification Standard and Calculation. The Proactive Notification SLA applies solely to the RRO CPE. Company will ping the RRO CPE at Customer's premises at regular intervals. If the RRO CPE router does not respond after two consecutive ping cycles, Company will send an email notice to Customer's designated point of contact within 15 minutes of opening the Trouble Ticket.

### 3. Credits.

3.1 General. Customer is eligible to receive credits if Company does not meet the SLA standards set above. To qualify for such credits, Customer must comply with the procedures set forth in this section. Credits are based on a stated percentage of the MRC for the service component (i.e., the RRO CPE and the Universal Port) in Customer's Agreement for which the SLA standard has not been met. Notwithstanding any other provision of this SLA, the maximum credit available to Customer under any combination of the Service Availability, Time to Repair; Service Installation, and Proactive Notification SLAs within a single calendar month is 15% of the total MRCs billed for Customer's Secure Gateway Services for that month. Company data and calculations will be used to determine if an SLA standard has been missed and a credit is due. Company will issue a credit due, net of discounts and taxes, within 90 days of its determination that an SLA standard was not met.

#### 3.2 Service Availability SLA Credit

Component	Secure Gateway Service(s)	Service Method	Credit Percentage of MRC
Universal Port	Retail & Remote Office, Mobile User and Firewall	N/A	20%
RRO CPE	Retail & Remote Office	Company local loop and Internet Dedicated T1 or T3	10%
RRO CPE	Retail & Remote Office	Company local loop, if required, and Broadband service	10%

#### 3.3 TTR SLA Credit

Component and Secure Gateway Service(s)	Universal Port	RRO CPE Broadband Service	RRO CPE T1 Service
	Retail & Remote Office, Mobile User and Firewall	Retail & Remote Office	Retail & Remote Office
Measured in one second Increments	Credit Percentage of MRC		
4:00:1 – 7:59:59	10%	0%	10%
8:00:00 or more	10%	10%	10%

#### 3.4 Service Installation Credit

Component	Secure Gateway Service(s)	Service Method	Credit Percentage of MRC
Universal Port	Retail & Remote Office, Mobile User and Firewall	n/a	20%
RRO CPE	Retail & Remote Office	Company local loop and Internet Dedicated T1 or T3	10%
RRO CPE	Retail & Remote Office	Company local loop, if required, and Broadband service	10%
RRO CPE	Retail & Remote Office	Customer-provided Internet service	10%

### 3.5 Proactive Notification Credit for Retail & Remote Office CPE

Secure Gateway Service(s)	Time From Opening of Trouble Ticket to Customer Notification	Credit Percentage Of MRC
Retail & Remote Office	> 15 minutes	10%

### 3.6 Service Availability and TTR Credit Process. Customer must perform the following to become eligible for credit under either the Service Availability or the TTR SLA:

- 3.6.1 Open a Trouble Ticket within four hours of first learning of a Hard Outage if Company has not already notified Customer that Company has opened the Trouble Ticket.
- 3.6.2 Submit in writing the following information no later than thirty (30) days from the end of the calendar month in which the Secure Gateway Services was restored:
  - All applicable Trouble Ticket numbers associated with each circuit affected by a Hard Outage;
  - The date and time the Trouble Ticket(s) were opened;
  - NASP ID; and
  - The circuit ID number for each circuit that experienced the Hard Outage.

Failure to comply with each of the preceding requirements may result in Company denying Customer's request for credit under either the Service Availability or TTR SLA.

A Trouble Ticket is a Company document used to record network service issues. Trouble Tickets are time stamped when opened and closed. The time stamps are used to calculate whether (i) the Service Availability and TTR standards under this SLA have been met, (ii) the issue reported is considered a Hard Outage; and (iii) the issue isn't excluded under "Exclusions", below.

### 3.7 Service Installation and Proactive Notification Credit Process.

- 3.7.1 To qualify for credit under the Service Installation or Proactive Notification SLA, Customer must make a written request for credit to Company within 15 business days of completed installation of the qualifying service or the Hard Outage for which Company did not meet the Proactive Notification standard.

When making credit request for the Service Installation SLA, Customer must provide its Company Account Team with the following information:

- Date the Service Installation period commenced;
- Date Service Installation was completed;
- Circuit ID number for each circuit that was not installed within the SLA; and
- Customer's order number.

When making a credit request for the Proactive Notification SLA, Customer must provide its Company Account Team with the following information:

- Date the circuit outage occurred;
- Time the circuit outage began and ended; and
- Circuit ID(s) for each circuit(s) that did not receive notification within the time frame.

3.7.2 Company will use its order activation system(s) as the basis to determine if the Service Installation SLA standard has been met. In addition to the exclusions described below, no credit is available under the Service Installation SLA for:

- A Customer-ordered installation date that is prior to the Secure Gateway Services installation interval;
- Installations outside of the continental United States;
- Delays resulting from inaccurate or incorrect order package information;
- Delays resulting from changes to a previously-accepted service order by customer, its agents or vendors;
- Internet circuits not provided by Company;
- Prerequisite tasks outlined in "Prerequisite Tasks" above, are not completed fully or successfully before Secure Gateway implementation begins.

### 3.8 Other.

3.8.1 If Company fails meet any particular SLA for three (3) consecutive months, Customer may elect to:

- Continue Secure Gateway Services subject to the limit (a) in "Credits", above and (b) that for any particular SLA, Customer may not receive credits for more than six (6) months during any 12-month period.
- Discontinue Secure Gateway Services without liability except for charges incurred prior to discontinuation of Secure Gateway Services, by submitting a written disconnect notice to its Company Account Team within 30 days following the end of either the third or subsequent consecutive month of Company's failure to meet the SLA standard.

3.8.2 Company –

- reserves the right to enhance or restrict these SLAs in whole or in part;
- after a failure of three consecutive months or more to meet any particular SLA standard, upon written notice to Customer, may terminate its performance obligations for that particular SLA standard.

Customer may, within thirty (30) days of being informed of any such restriction or termination of SLA obligations, terminate the affected Secure Gateway Services pursuant to the discontinuation terms of Section 3.8.1 above.

4. Exclusions. In addition to any exclusions specified above, SLA standard calculations will not count as unavailable or repair time any time that results from any one or more of the following:
- 4.1 The Secure Gateway Services have been installed for less than one full calendar month;
  - 4.2 Any act or omission on the part of Customer, its contractors, vendors, agents or any other entity over which Customer exercises control or has the right to exercise control, other than acts or omissions of Company or Company -approved third-party network or maintenance providers, including, but not limited to, the following:
    - Delays of any kind attributable to Customer;
    - Incorrect or incomplete information provided by Customer;
    - Company or the Company -approved maintenance provider is denied access to the RRO CPE or network components at the Customer location when such access is required;
    - Customer configuration and rule set changes to Firewall feature contribute to downtime or lack of availability of Secure Gateway Universal Port;
    - Customer fails or refuses to release the circuit for testing;
    - Customer is unavailable when needed to close a Trouble Ticket;
    - Customer (not Company) provides the local access loop; or
    - Incomplete or inaccurate orders.
  - 4.3 Interruptions not reported by Customer, or for which no Trouble Ticket was opened, if required under "Credits", above;
  - 4.4 Proper electrical power is not available;
  - 4.5 A force majeure event, including but not limited to, acts of God, government regulation, labor strikes, natural disasters, national emergency, acts of terrorism, or other such events that are not reasonably within Company's control;
  - 4.6 Scheduled maintenance by Customer or entities under Customer's direction or control;
  - 4.7 Scheduled or emergency maintenance by Company;
  - 4.8 Customer uses the Secure Gateway Services in an unauthorized or unlawful manner;
  - 4.9 Network degradation, such as slow data transmission;
  - 4.10 The Hard Outage that causes the SLA standard to be missed is due to Customer-provided Internet service;
  - 4.11 The Secure Gateway Services circuit does not have a static public IP address.
  - 4.12 Secure Gateway Services are not yet activated in the case of claims made pursuant to the Service Availability, Time to Repair or Proactive Notification SLA.