Table of Contents

LevelBlue Secure Network Gateway

Section Effective Date: 22-Nov-2013

LevelBlue Secure Network Gateway is a bundled offer of cloud-based security services that includes LevelBlue Network-Based Firewall Service, LevelBlue Secure E-Mail Gateway Service and LevelBlue Web Security Service.

The LevelBlue Secure Network Gateway Service Guide consists of the following parts:

- Service Description (SD)
- Service Level Agreements (SLA)
- Pricing (P)

In addition, the General Provisions are incorporated and apply as specified therein.

Service Description

SD-1. General

SD-1.1. LevelBlue Secure Network Gateway

Section Effective Date: 12-Dec-2016

LevelBlue Secure Network Gateway consolidates LevelBlue Network-Based Firewall, LevelBlue Secure E- Mail Gateway, LevelBlue DDoS Defense or LevelBlue Reactive DDoS Defense on a Secure Network Gateway Pricing Schedule and order. The bundled Services appear on one consolidated bill with pricing discounts for purchasing multiple services.

SD-1.1.1. Opt-Out Clause

Section Effective Date: 05-Apr-2019

The Opt-Out Clause applies to the Services provided under the Secure Network Gateway Pricing Schedule. The Opt-Out Clause applies to Customer's Initial Order ("Initial Order") placed at contract signing. Service or features added after Initial Order will be considered change orders and no Opt-Out applies.

Termination Charges for the thirty (30) day Opt-Out Period shall not apply if Customer terminates a Service under the Pricing Schedule Initial Order within thirty (30) days after the Service test and turn-up is completed by LevelBlue and Service has been made available for Customer ("Opt-out Period"). Customer will be required to remit payment for all charges incurred for the Service received.

SD-1.1.2. Termination Orders

SD-1.1.2.1. Customer Initiated

Section Effective Date: 17-May-2013

If Customer wishes to terminate a Service Component, the Customer must provide LevelBlue with at least thirty (30) days' prior written notice to that effect. Recurring monthly charges will continue to apply for a period of at least thirty (30) calendar days from the date when LevelBlue receives a termination notice or until the disconnect date specified in the disconnect order applicable to the affected Service Component(s), whichever is later.

SD-1.1.3. Customer Compliance Responsibilities SD-1.1.3.1. Monitoring of Communication

Section Effective Date: 04-Dec-2019

LevelBlue is providing these Services for a cybersecurity purpose as defined in and consistent with the Cybersecurity Information Sharing Act of 2015 (“CISA”). In the United States, Customer agrees to undertake any monitoring of its network, undertake defensive measures and share cyber threat indicators or defensive measures consistent with CISA. In the U.S and globally, Customer agrees that it is responsible for setting all security policies, including monitoring policies, and will implement any and all security policies pursuant to CISA or other applicable law. LevelBlue retains the right to reject any security policies Customer asks it to implement that in LevelBlue’s sole judgment are not for a cybersecurity purpose or as defined in or are inconsistent with CISA or other applicable law. Customer consents to the monitoring by the Services contemplated here. Customer is responsible for obtaining consent from and giving notice to its Users, employees and agents regarding Customer’s and LevelBlue’s collection and use of the User, employee or agent information in connection with a Service.

SD-1.1.4. Secure Network Gateway Services – General Capabilities

Section Effective Date: 28-Feb-2017

Service	Architecture Summary and Options	Key Features	Reporting
LevelBlue MFS- NB Private to Internet	LevelBlue specific security platform, including Firewall, Intrusion Detection and other security features.	-Firewall network-based -Centralized firewall policy for all locations on the network -Global availability -Port and Application level protection for LevelBlue AVPN, EVPN, PNT Customers -No Customer-premises equipment required -Customer WAN access points *Options available for this Service are Web Filtering, Intrusion Detection/Prevention -Data Loss Prevention, Application Control	Through LevelBlue BusinessDirect. For details see reporting section at the end of this Service Guide.

Service	Architecture Summary and Options	Key Features	Reporting
LevelBlue MFS- NB Private to Cloud Solution Provider (CSP)	LevelBlue network security platform, including Firewall, Intrusion Detection and other security features for use with LevelBlue AT&T NetBond®.	-Firewall (network-based) -Centralized firewall policy -Port and Application level protection for LevelBlue VPN, Enhanced VPN Services, MPLS- PNT Services -Customer-premises equipment not required -Customer WAN access points -Burstable bandwidth *Options available for this Service are Web Filtering, Intrusion Detection/Prevention, Malware Scanning -Data Loss Prevention, -Application Control	LevelBlue BusinessDirect®
LevelBlue Secure E- Mail Gateway	Email Security	-Customer Managed Administration -Anti-Virus Protection -Spam Filtering -Policy Enforcement -Quarantine -Disaster Recovery -Transport Layer Security -Administrative Reports	Through LevelBlue BusinessDirect. For details see reporting section at the end of this Service Guide.

Service	Architecture Summary and Options	Key Features	Reporting
LevelBlue Distributed Denial of Service (DDoS) Service LevelBlue DDoS Defense - Agnostic	DDoS Defense for LevelBlue Dedicated Internet (ADI) (formerly known as LevelBlue Managed Internet Service (MIS))ADI/ADI+/LevelBlue Dedicated Internet Global (ADIG) (formerly known as LevelBlue Global Managed Internet Service (GMIS)) customers and LevelBlue IDC Hosting customers with connectivity to the LevelBlue IP Backbone DDoS Defense for Agnostic (non-LevelBlue provided internet access) customer	-Volumetric attack detection and mitigation -Reporting portal -24X7 monitoring - No Customer-premises equipment required	Yes
LevelBlue Reactive Distributed Denial of Service	Reactive DDoS Defense for ADI customers	-Volumetric attack mitigation -Reporting portal -24x7 Customer Care -No Customer-premises equipment required	Yes

SD-1.2. Country Availability

Section Effective Date: 14-Apr-2022

LevelBlue Secure Network Gateway is available in select countries in the regions and countries detailed in the table below.

In addition, not all service features described in this document are available in all regions and countries. Please refer to the Country Specific Provisions section at the end of the Service Guide Section for additional details, if applicable.

Table of Regions

Region	**Countries within a Region**
Americas†	Argentina, Brazil, Canada, Chile, Colombia, Panama, Peru, Venezuela
Asia Pacific (AP)	Australia, Hong Kong, Japan, New Zealand, Singapore, Republic of Korea
EMEA	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, United Kingdom
Japan	Japan
United States*	United States

NOTE: †LevelBlue DDoS Defense is not available in the Americas.
*Managed Firewall Service for AT&T NetBond® is only available in the United States.
*LevelBlue Reactive DDoS Defense is only available in the United States.

SD-1.3. Managed Firewall Service – Network Based (MFS-NB) when included in LevelBlue Network Suite (ANS) – Contracts executed after December 15, 2014

SD-1.3.1. Overview

Section Effective Date: 20-Dec-2014

LevelBlue MFS-NB is designed to help enterprises implement and monitor Internet access for multiple sites. The Service will enable businesses to support and enforce sophisticated network Security Policies from US based LevelBlue Internet Data Centers where the Network Based Security platform resides, also referred to as the Security Data Center (SDC). Customers are able to more efficiently implement a consistent Security Policy for multiple sites.

In regard to designating configuration complexity, there are two levels available as a part of LevelBlue's MFS-NB service in the LevelBlue Network Suite:

- Primary
- Enhanced

Each complexity level supports both inbound and outbound traffic through the MFS-NB platform. Complexity categorization is determined by examining the required traffic types that would be passing through the gateway. LevelBlue completes the policy administration on the equipment but also allows the Customer to make changes to certain configuration settings. With Enhanced Complexity Level, add-on features, such as Web Filtering, Malware Scanning, Active IDS/IPS and User Authentication support are available.

MFS-NB enforces traffic separation among Customers by enabling Virtual Local Area Network (VLAN) tagging. For Customers who wish to make use of the LevelBlue MFS-NB Service, LevelBlue will establish a Permanent Virtual Circuit (PVC) from a Customer location to the service in order to filter the traffic coming in or going to the Internet.The type of PVC will vary based on Customer's WAN architecture. Traffic separation is designed to occur without tunneling or encryption. This is enabled through a combination of Border Gateway Protocol (BGP), MPLS, and IP address resolution as described below.

BGP is a routing information distribution protocol that is designed to define who can talk to whom using multi-protocol extensions and community attributes. VPN membership depends upon logical ports entering the VPN, where BGP assigns a unique route distinguisher. In an MPLS-enabled VPN, BGP distributes Forwarding Information Base (FIB) tables about VPNs to members of the same VPN. This is designed to permit users to participate on an Intranet and Extranet only if they reside on the correct physical or logical port and have the proper route distinguisher.

A packet received by the network backbone is associated with a particular VPN. A forwarding table associated with the particular VPN is used along the originating IP address, to determine a set of possible egress interfaces and the packet's IP destination address.

Overall security policy and the selection and use of security features provided by LevelBlue is a Customer and User responsibility. LevelBlue does not guarantee that use of the security features that LevelBlue provides will prevent unauthorized access to Customer systems or data.

SD-1.3.2. Features of the MSS NB Service

Section Effective Date: 08-Apr-2016

Based on traffic and application requirements, MFS-NB Customers select the Feature (complexity) Level for their service. This selection pre-determines the basic service offering, and what add-on features can be supported under the given complexity.

Primary Complexity: Common Customer Security Policy allowing both inbound and outbound traffic flow based on the configuration. The Primary Level Includes basic set of reports and certain self-administration capabilities via BusinessDirect®. With this service level, the customer is provided a PAT address as default, but since inbound services can be supported, up to 8 IP addresses could be assigned as part of the service if there is sufficient justification from the customer and confirmed by LevelBlue based on the design.

Enhanced Complexity: this service level provides the option to turn on add-on features in addition to the inbound and outbound traffic flow support. By default, a single PAT address is assigned, but up to 16 IP addresses including the PAT address can be supported on a standard basis with sufficient justification submitted by the customer and confirmed by LevelBlue during the design phase.

LevelBlue reserves the right to charge extra fees for any additional IP addresses requested above the supportable number defined above.

SD-1.3.3. Standard Components

Section Effective Date: 15-Dec-2014

- All levels of LevelBlue's MFS-NB Service provide:
- Security Monitoring:
  - 7x24 monitoring of traffic into the network Firewall. This keeps inbound attacks outside of the MFS-Network Based infrastructure at the high-throughput circuits, away from individual Customer components or services.
  - Stateful Inspection of allowed IP traffic via Firewall.
  - Open Systems Interconnection (OSI) Layer 2 isolation. All PVC traffic remains isolated through the MFS-MB Service infrastructure and the Security Policy.
- Network:
  - One network as primary defined by the ingress of a single VPN Multi-Protocol Label Switching (AVPN MPLS network) into a Security Data Center (SDC).
  - If AVPN is purchased, the MFS-NB Service provisions as part of the basic subscription an ePVC (or Logical Channel) and a backup ePVC (or Logical Channel) of the subscribed size into the Service.
  - A wide range of bandwidth options are available to support Customer requirements on AVPN. Restrictions may apply depending on the chosen transport type or the total bandwidth required to support a network segment that needs to be protected by the Service.
  - Transparent, Stateful Inspection (i.e., non-proxied) Internet access
  - Many-to-one outbound Network Address Translation (NAT) to the Internet, hiding Customer's address space.
- DNS
  - The below details about DNS apply to MFS-NB when the service is provided in conjunction with VPN Multi-Protocol Label Switching (MPLS network), AVPN network.
  - LevelBlue Primary DNS is provided by LevelBlue-Enhanced Network Services as part of the MFS-NB, or it can be provided by a Customers' own DNS authority. When the primary DNS is provided by LevelBlue, Managed Security Services Operations will be acting on behalf of Customer to provide administration support for changes affecting the DNS configuration.
  - DNS caching is provided by MSS-Network Based Service to provide Customers with resolution performance and protection services. All Customer queries will be to the MFS-NB DNS caching servers from the Customers' specified internal primary DNS servers.

  - MFS-NB expects that Customers have implemented some form of split DNS, where their internal address resolution resides on an internal corporate root DNS Server for their users' internal address resolution. These internal DNS servers are maintained and administered by the Customer, and will forward external queries to the MSS-Network Based caching DNS servers for resolution.
  - MFS-NB does not support internal Customer address resolution on its caching DNS servers. The Customer must provide this functionality for its internal network.
- Self-Administration Capability of NBFW configuration
  - MFS-NB provides a self-administration capability for Customers to administer certain aspects of the configuration of the MSS-NB solution.
  - For configuration changes unavailable through the self -administration interface, Customers are required to engage the MFS Operations team via the LevelBlue Business Direct Portal.
- Reporting
  - MFS-NB provides a standard set of reports via the Business Direct portal. Content and format of the reports are subject to change without notice. LevelBlue maintains a Customer accessible website where reports may be obtained.

SD-1.3.4. Offer Limitations

Section Effective Date: 28-Feb-2017

MFS-NB provides support for up to 10 total authorized Customer contacts (applies to all levels).

Six (6) MACD service requests per month are allowed with each service level. Additional requests are subject to additional charges.

- Only MFS-NB platforms located in the US can be supported with this offer.
- No SNMP traffic is allowed to traverse the firewall (applies to all service levels).
- Only Critical ICMP (ping) traffic is allowed (troubleshooting or periodic checks).
- Porting of currently assigned public address space including ADI, SBC and Bell South IA is not supported.
- Customer-owned public address space cannot be transferred to NBFW.
- Hosted cross-connect services is not supported at any Security Data Center (SDC).
- Customer cannot migrate to NBFW site by site since the NBFW default route affects all remote sites at the same time.
- Security policy for IPv6 is not supported.
- The following bandwidth tiers are supported by LevelBlue VPN, the underlying MPLS transport. The following are the bandwidth tier options Network Based Firewall can accept for initial orders or subsequent bandwidth upgrade requests. In the event a request is made for a bandwidth tier that is not on the list below, LevelBlue reserves the right to decline the request or to recommend an alternate tier. The pricing for alternate tiers will be set forth in the Customer's Pricing Schedule. AVPN supported bandwidth tiers: 1Mbps, 2Mbps, 3Mbps, 4Mbps, 5Mbps, 6Mbps, 7Mbps, , 8Mbps, 9Mbps, 10Mbps, 20Mbps, 30Mbps, 40Mbps, 50Mbps, 60Mbps, 70Mbps, 80Mbps, 90Mbps, 100Mbps, 150Mbps, 200Mbps, 250Mbps, 300Mbps, 400Mbps, 450Mbps, 500Mbps, 600Mbps, 700Mbps, 800Mbps, 900Mbps, 1000Mbps, 1500Mbps, 2000Mbps, 2500Mbps, 3000Mbps, 3500Mbps, 4000Mbps, 4500Mbps, 5000Mbps.

Customers are encouraged to aggregate their Rules' source and destination addresses into networks rather than to specific Hosts. Source and destination networks should be subnetted up to the largest/most inclusive range. For common services, such as HTTP, HTTPS or FTP, LevelBlue recommends that source or destination Rules apply to all users ("ANY").

If there is an explicit need for specific granular source addresses by Customer, and if there is proper justification submitted during the design, additional MFS-NB IP addresses may be assigned up to the limit supportable for each Service Level. LevelBlue reserves the right to charge extra fees for additional IP addresses requested over the number of IP addresses defined under each Service Level.

SD-1.3.5. Optional Features

Section Effective Date: 09-Dec-2015

The following table describes the optional features available as a part of this service, and the Levels that apply to each:

Optional Features		
Features	**Level**	**Description**
Web Filtering – Basic	Enhanced (no user count)	Allows internet traffic to be filtered based on website content. The Basic option has the following features available: Over 75 pre-defined URL categories (e.g., religion, sports, etc.) which are selected to be allowed or denied. The Whitelist/Blacklist function allows browsing to specific URLs to be permitted or denied. This function overrides any URL filtering options. Content Filtering URL blocking can also be done by IP address rather than URL name.
Web Filtering – Advanced	Enhanced (no user count)	Allows internet traffic to be filtered based on website content. This option is licensed on the number of total end Users. The Advanced option provides the features of Web Filtering – Basic plus: User Authentication support Logging of allows (permitted web browsing traffic) Application Control SafeSearch Anonymization of Log Data for International Privacy Regulations Data Loss Prevention

Optional Features		
Features	**Level**	**Description**
Malware Scanning – Basic	Enhanced (no user count)	Provides inline scanning HTTP and FTP content for common virus, spyware, and malware threats and vulnerabilities. Also provides the ability for inline scanning of Instant Messaging protocols (ICQ, MSN, Yahoo and AIM). Support for User Authentication is also available to provide User level reporting and User group specific configuration. Filtering based on file size and file type can also be enforced. Advanced option provides the features of Basic plus: • User Authentication support • Logging of allowed traffic • Application Control • Grayware • Anonymization of Log Data for International Privacy Regulations • Data Loss Prevention • Content Filtering/Control
Intrusion Detection System (IDS) Logging only – not turned on by default	Enhanced	MFS-NB has implemented a set of certain basic IDS features, which includes limited scanning of Customer traffic for a small number of exploits, attacks and other malicious activities. This capability will not be turned on by default but can be requested by Customer at no extra charge.
Active IDS/IPS-Basic	Enhanced	This feature is applied on a per Secnet basis. Service includes IDS/IPS initial technical consultation and applies LevelBlue's best practices policy. Also includes IDS policy customization and addition of a limited set of custom IDS signatures to the profile as well as proactive investigational analysis for critical events and enablement of a limited set of automated IPS capabilities.

Optional Features		
Features	**Level**	**Description**
Active IDS/IPS-Advanced	Enhanced	Provides a more customized service level and alert thresholds to meet more specific IDS requirements including a higher degree of profiling and tuning of IDS policy to strip out "noise" and provide notification on critical events. Additionally, LevelBlue Security Analyst provides live investigational analysis for all IDS events assisting with recommended mitigation actions, and making firewall policy changes to help eliminate a threat if warranted.
Additional Public IPv4 Addresses (blocks of 2)	Primary, Enhanced	If more than the allocated number of IPv4 addresses for the chosen Service Level are needed, extra IP addresses can be requested. Additional charges for extra IP addresses will apply. Justification for additional IP addresses will be required in all cases.
Additional Secure Networks (SecNets)	Enhanced	Based on Customer definition/design, configures MFS-NB policies for each network segment needing further protection, joining that to the network and injecting default or host routes.
Additional Site Egress/Ingress	Enhanced	Allows outbound/inbound access from more than one SDC. For each additional SDC, the pricing will be based on the bandwidth required for each connection (SecNet). The selected complexity level will be applied once per total customer solution. By default, each extra SDC will receive • a PAT address. The Enhanced Service Level can include up to 16 in total. Any additional IP addresses being requested require justification. • Two additional ePVCs for each extra SDC. • Policy setup and support for each SDC. • Special technical considerations and/or restrictions may apply when there are inbound requirements in conjunction with Additional Site Egress and Ingress.

Optional Features		
Features	**Level**	**Description**
Site Failover	Enhanced	This option allows the customer to have a single alternate SDC in the same geographical region to receive “failover traffic”. A 3rd ePVC is provisioned from the alternate site to the customer’s MPLS network. A duplicate security policy is maintained on the alternate SDC for a specified SecNet. If Customer has multiple SecNets, they must purchase Site Failover for the same number of SecNets if failover is a requirement for each. Special requirements apply for MFS-NB Failover which have to be followed for proper operations and which would be considered during the design phase.

SD-1.3.6. SafeSearch

Section Effective Date: 15-Dec-2014

For this capability, the Enhanced complexity level of MFS-NB in the LevelBlue Network Suite offer has to be selected. SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature. Three search sites are supported: Google, Yahoo and Bing.

SD-1.3.7. Anonymization of Log Date for International Privacy Regulations

Section Effective Date: 15-Dec-2014

MFS-NB in LevelBlue Network Suite is unavailable in Most of World (MOW).

SD-1.3.8. Malware Scanning

Section Effective Date: 15-Dec-2014

Antivirus scanning examines files for viruses, worms, Trojans and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

- Malware Scanning anti-virus scan engines will scan websites visited by users.
- Provides inline scanning of HTTP content for common virus, spyware, and malware threats and vulnerabilities.
    - Also provides the ability for inline scanning of Instant Messaging protocols (ICQ, MSN, Yahoo and AIM).
- If a web page or web page attachments are found to contain a virus or spyware, then access to that web page or attachments is denied and the Internet user will be displayed an automatic virus alert web page.
- All attachments can be blocked by file type or extension.
- Scanning of encrypted traffic and attachments are not supported at this time.
- If the enforcement of the Customer's User Authentication policy is required to support User Groups, the Malware Scanning – Advanced feature must be ordered.

If the logging of permitted HTTP, FTP, IM traffic is required (e.g. User Level detailed reporting is needed if available), the Enhanced complexity level of MFS-NB in the LevelBlue Network Suite offer must be ordered.

SD-1.3.9. Grayware

Section Effective Date: 15-Dec-2014

For this capability, the Enhanced complexity level of MFS-NB in the LevelBlue Network Suite offer must be ordered.

This category includes:

- Spyware – that tracks users activities
- Adware
- Dial
- Downloader
- Keylogger
- Hacker Tool
- Remote Access/Administration Tool

SD-1.3.10. Content Filtering

Section Effective Date: 15-Dec-2014

The Content Filtering set forth above, applies to MFS-NB in ANS.

Cross References

SD-2.1.4. Optional Features

SD-1.3.11. Application Control

Section Effective Date: 15-Dec-2014

This feature controls end user access to Web 2.0 applications, i.e. Video and Audio streaming, IM control, VOIP, Peer to Peer and Games. Abuse of these applications can lead to increased bandwidth demand and increased susceptibility to malware attacks.

Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

This feature is included when the Enhanced complexity level of MFS-NB in the LevelBlue Network Suite offer is ordered.

SD-1.3.12. Data Loss Prevention

Section Effective Date: 15-Dec-2014

For this capability the Enhanced complexity level of MFS-NB in the LevelBlue Network Suite offer must be ordered.

This feature allows the Customer to help prevent sensitive data from leaving the network, to help prevent unwanted data from entering the network and to archive some or all of the content. When the Customer defines sensitive data patterns, data matching these patterns will be blocked or logged and allowed.

The Customer creates individual filters in a DLP sensor and assigns the sensor to a security policy.

Examples include filters based on the file type (e.g.. all JPEG files), file name (e.g., find all files called secret.*), file size (e.g., files exceeding a specified size), a regular expression (match strings of text), an advanced rule (a single condition and the traffic in which the condition will appear), or a compound rule (a combination of advanced rules) .This feature helps prevent leakage of personal data and allows the definition of data flexibility to define rules based on HTTP, FTP and IM protocol. It is designed to provide analysis and blocking of outbound file types, preconfigured IDs (e.g., credit card numbers or social security numbers) and DFA-based regular expressions.

- Service also provides key word identification and blocking. For example, key word in document will block sending of document, e.g. “Proprietary”.

SD-1.3.13. User Authentication

Section Effective Date: 15-Dec-2014

If User Authentication is requested to be supported, Customers will be able to set policy controls over User level access to the Internet. After certain criteria is met (as determined by LevelBlue) and needed components are set up in the Customer network, the MFS-NB platform will interface with a Customer’s hosted and managed User Authentication service (RADIUS, LDAP or Active Directory) to authenticate User activity to the Internet. Note: MFS-NB will not provision, administer, support or troubleshoot the Customers User Authentication solution.   For User Authentication support, Customer must have the Enhanced complexity level of MFS-NB in the LevelBlue Network Suite offer.

SD-1.3.14. Customer Responsibilities

Section Effective Date: 15-Dec-2014

The Customer Responsibilities set forth above apply to the MFS-NB in ANS.

Cross References

SD-2.4. Customer Responsibilities

SD-1.3.15. Service Availability

Section Effective Date: 15-Dec-2014

The Service Availability set forth above, applies to MFS-NB in ANS.

Cross References

SD-2.5. Service Availability

SD-1.3.16. Support and Management

Section Effective Date: 15-Dec-2014

The Support Management set forth above, applies to MFS-NB in ANS.

Cross References

SD-2.6. Support and Management

SD-2. Managed Firewall Service — Network Based (MFS-NB)

SD-2.1. MFS-NB Service Overview

Section Effective Date: 09-Dec-2015

LevelBlue MFS-NB is designed to help enterprises implement and monitor Internet access for multiple sites. The Service will enable businesses to support and enforce sophisticated network Security Policies from one or more of the LevelBlue Internet Data Centers where the Network Based Security platform resides, also referred to as the Security Data Center (SDC). Customers are able to more efficiently implement a consistent Security Policy for multiple sites.

Designating configuration complexity, there are three feature levels available as a part of LevelBlue's MFS-NB service. These levels are:

- Low Complexity
- Medium Complexity
- High Complexity

All complexity levels support both inbound and outbound traffic through the MFS-NB platform. Complexity categorization is determined by examining the required traffic types that would be passing through the gateway. LevelBlue completes the policy administration on the equipment but also allows the Customer to make changes to certain configuration settings. Starting at Medium Complexity Level, advanced add-on features, such as Web Filtering, Advanced, Malware Scanning Advanced, Active IDS/IPS Advanced and User Authentication support are available.

MFS-NB enforces traffic separation among Customers by enabling Virtual Local Area Network (VLAN) tagging. For Customers who wish to make use of the LevelBlue MFS-NB Service, LevelBlue will establish a Permanent Virtual Circuit (PVC) from a Customer location to the service in order to filter the traffic coming in or going to the Internet. The type of PVC will vary based on the Customer's WAN architecture. Traffic separation is designed to occur without tunneling or encryption. This is enabled through a combination of Border Gateway Protocol (BGP), MPLS, and IP address resolution as described below.

BGP is a routing information distribution protocol that is designed to define who can talk to whom using multi-protocol extensions and community attributes. VPN membership depends upon logical ports entering the VPN, where BGP assigns a unique route distinguisher. In an MPLS-enabled VPN, BGP distributes Forwarding Information Base (FIB) tables about VPNs to members of the same VPN. This is designed to permit users to participate on an Intranet and Extranet only if they reside on the correct physical or logical port and have the proper route distinguisher.

A packet received by the network backbone is associated with a particular VPN. A forwarding table associated with the particular VPN is used, along the originating IP address, to determine a set of possible egress interfaces and the packet's IP destination address.

Overall security policy and the selection and use of security features provided by LevelBlue is a Customer and User responsibility. LevelBlue does not guarantee that use of the security features that LevelBlue provides will prevent unauthorized access to Customer systems or data.

SD-2.1.1. Features of the MSS-NB Service

Section Effective Date: 22-Apr-2022

Based on traffic and application requirements, MFS-NB Customers select the Feature Level for their service. This selection pre-determines the basic service offering, and what add-on features can be supported under the given complexity.

Low Complexity: Common Customer Security Policy allowing both inbound and outbound traffic flow based on the configuration. The Low Complexity Level Includes basic set of reports and certain self administration capabilities via BusinessDirect®. With this service level, the customer is provided a PAT address as default, but since inbound services can be supported, up to 8 IP addresses could be assigned as part of the service given there is justification from the customer based on the design.

Medium Complexity: this service level provides the option to upgrade to more add-on features in addition to the inbound and outbound traffic flow support. By default, a single PAT address is assigned, but up to 16 IP addresses including the PAT address can be supported on a standard basis if there is sufficient justification submitted by the customer and confirmed by LevelBlue during the design phase.

High Complexity: this service levels supports all the features listed under Low and Medium complexities as well as provides the capability to support more add-ons. By default, a single PAT address is assigned but up to 32 IP addresses including the PAT address can be supported on a standard basis with sufficient justification submitted by the Customer and confirmed by LevelBlue during the design phase.

LevelBlue reserves the right to charge extra fees for any additional IP addresses requested above the supportable number defined above.

SD-2.1.2. Standard Components

Section Effective Date: 22-Apr-2022

All levels of LevelBlue's MFS-NB Service Private to Internet provide:

- Security Monitoring:
    - 7x24 monitoring of traffic into the network Firewall. This keeps inbound attacks outside of the MFS-Network Based infrastructure at the high-throughput circuits, away from individual Customer components or services.
    - Stateful Inspection of allowed IP traffic via Firewall.
    - Open Systems Interconnection (OSI) Layer 2 isolation. All PVC traffic remains isolated through the MFS-MB Service infrastructure and the Security Policy.
- Network:
    - One network as primary defined by the ingress of a single VPN Multi Protocol Label Switching (MPLS network), or as ATM or Internet Protocol enabled Asynchronous Transfer Mode (IPeATM), AVPN or PNT network into a Security Data Center (SDC).
    - If IPeATM, AVPN or PNT are purchased, the MFS-NB Service provisions as part of the basic subscription an ePVC (or Logical Channel) and a backup ePVC (or Logical Channel) of the subscribed size into the Service. However, if the Customer is using direct PVC's, then it is their responsibility to provision a backup direct PVC. Note: Only one direct PVC is included in the basic pricing. Additional direct PVC's (primary or backup) are considered additional networks and are charged accordingly.
    - A wide range of bandwidth options are available to support Customer requirements on AVPN, EVPN or PNT. Restrictions may apply depending on the chosen transport type or the total bandwidth required to support a network segment that needs to be protected by the Service.
    - Transparent, Stateful Inspection (i.e., non-proxied) Internet access
    - Many-to-one outbound Network Address Translation (NAT) to the Internet, hiding Customer's address space.

- DNS - GRANDFATHERING NOTICE: As of April 30, 2022, the DNS feature of LevelBlue Network Based Firewall is grandfathered and no new customers for the feature will be accepted. Existing Customers can continue using the feature pursuant to the terms of their Service Agreement.
    - The below details about DNS apply to MFS-NB when the service is provided in conjunction with VPN Multi Protocol Label Switching (MPLS network), ATM or Internet Protocol enabled Asynchronous Transfer Mode (IPeATM), AVPN or PNT network.
    - LevelBlue Primary DNS is provided by LevelBlue-Enhanced Network Services as part of the MFS-NB, or it can be provided by a Customers' own DNS authority. When the primary DNS is provided by LevelBlue, Managed Security Services Operations will be acting on behalf of Customer to provide administration support for changes affecting the DNS configuration.
    - DNS caching is provided by MSS-Network Based Service to provide Customers with resolution performance and protection services. All Customer queries will be to the MFS-NB DNS caching servers from the Customers' specified internal primary DNS servers.
    - MFS-NB expects that Customers have implemented some form of split DNS, where their internal address resolution resides on an internal corporate root DNS Server for their users' internal address resolution. These internal DNS servers are maintained and administered by the Customer, and will forward external queries to the MSS-Network Based caching DNS servers for resolution.
    - MFS-NB does not support internal Customer address resolution on its caching DNS servers. The Customer must provide this functionality for its internal network.
- Self Administration Capability of NBFW configuration
    - MFS-NB provides a self administration capability for Customers to administer certain aspects of the configuration of the MSS-NB solution.
    - For configuration changes unavailable through the self administration interface, Customers are required to engage the MFS Operations team via the LevelBlue Business Direct Portal.
- Reporting
    - MFS-NB provides a standard set of reports via the Business Direct portal. Content and format of the reports are subject to change without notice. LevelBlue maintains a Customer accessible website where reports may be obtained.

SD-2.1.3. Offer Limitations

Section Effective Date: 14-Nov-2015

MFS-NB provides support for up to 10 total authorized Customer contacts (applies to all levels).

Six (6) MACD service requests per month are allowed with each service level. Additional requests are subject to additional charges.

- No SNMP traffic is allowed to traverse the firewall (applies to all service levels).
- Only Critical ICMP (ping) traffic is allowed (troubleshooting or periodic checks.

Customers are encouraged to aggregate their Rules' source and destination addresses into networks rather than to specific Hosts. Source and destination networks should be subnetted up to the largest/most inclusive range. For common services, such as HTTP, HTTPS or FTP, LevelBlue recommends that source or destination Rules apply to all users (“ANY”).

If there is an explicit need for specific granular source addresses by Customer and if there’s proper justification submitted during the design, additional MFS-NB IP addresses may be assigned up to the limit supportable for each Service Level. LevelBlue reserves the right to charge extra fees for additional IP addresses requested over the number of IP addresses defined under each Service Level.

SD-2.1.3.1. Geo Location Support

Section Effective Date: 09-Dec-2015

In some instances for Customers having locations connecting to the LevelBlue provided MPLS network in a country or region other than the location where the NBFW service with internet access is being provided, it may be possible that content providers on the internet may not present content in the desired language. If the design calls for such a deployment, the customer must initiate a change to the configuration or request support for this requirement during the provisioning process. If a customer is not satisfied with the language, it is the customer’s responsibility to contact the content providers and ask for an arrangement that will satisfy the customer’s requirements.

SD-2.1.3.2. Multi Egress Design

Section Effective Date: 09-Dec-2015

Generally, multi-egress designs may be used with Network Based Firewall to provide more than one gateway to the internet for a given LevelBlue provided MPLS VPN. However, under certain circumstances, unexpected routing conditions may occur once the customer is in maintenance. Some unexpected routing conditions may not be within the control of the Network Based Firewall Service.

SD-2.1.4. Optional Features

Section Effective Date: 22-Apr-2022

The following table describes the optional features available as a part of this service, and the Levels that apply to each:

Optional Features		
Features	**Level**	**Description**
Web Filtering – Basic # of Users	Low, Medium, High	Allows internet traffic to be filtered based on website content. This option is licensed on the total number of end Users. The Basic option has the following features available: • Over 75 pre-defined URL categories (e.g., religion, sports, etc.) which are selected to be allowed or denied. • The Whitelist/Blacklist function allows browsing to specific URLs to be permitted or denied. This function overrides any URL filtering options. • Content Filtering • URL blocking can also be done by IP address rather than URL name.

Optional Features		
Features	**Level**	**Description**
Web Filtering – Advanced # of Users	Medium, High	Allows internet traffic to be filtered based on website content. This option is licensed on the number of total end Users. The Advanced option provides the features of Web Filtering – Basic plus: • User Authentication support • Logging of allows (permitted web browsing traffic) • Application Control • SafeSearch • Anonymization of Log Data for International Privacy Regulations • Data Loss Prevention
Malware Scanning – Basic # of Users	Low, Medium, High	This option is licensed on the number of total end Users. Provides inline scanning of HTTP and FTP content for common virus, spyware, and malware threats and vulnerabilities. Also provides the ability for inline scanning of Instant Messaging protocols (ICQ, MSN, Yahoo and AIM). Filtering based on the file size and file type can also be enforced.

Optional Features		
Features	**Level**	**Description**
Malware Scanning – Advanced # of Users	Medium, High	This option is licensed on the number of total end Users. Provides inline scanning HTTP and FTP content for common virus, spyware, and malware threats and vulnerabilities. Also provides the ability for inline scanning of Instant Messaging protocols (ICQ, MSN, Yahoo and AIM). Support for User Authentication is also available to provide User level reporting and User group specific configuration. Filtering based on file size and file type can also be enforced. Advanced option provides the features of Basic plus: • User Authentication support • Logging of allowed traffic • Application Control • Grayware • Anonymization of Log Data for International Privacy Regulations • Data Loss Prevention • Content Filtering/Control
Intrusion Detection System (IDS) Logging only – not turned on by default	Low, Medium, High	MFS-NB has implemented a set of certain basic IDS features, which includes limited scanning of Customer traffic for a small number of exploits, attacks and other malicious activities. This capability will not be turned on by default but can be requested by Customer at no extra charge.

Optional Features		
Features	**Level**	**Description**
Additional Public IPv4 Addresses (blocks of 2)	Low, Medium, High	If more than the allocated number of IPv4 addresses for the chosen Service Level are needed, extra IP addresses can be requested. Additional charges for extra IP addresses will apply. Justification for additional IP addresses will be required in all cases.
Additional Secure Networks (SecNets)	Medium, High	Based on Customer definition/design, configures MFS-NB policies for each network segment that needing further protection, joining that to the network and injecting default or host routes. A DMZ or other isolated MPLS network is considered to be another Secure Network. Note that if another Secure Network is needed and it's in a different Secure Data Center, at a minimum, the medium service level is required. With the Medium Service Level, NBFW instances in 2 geographic regions or two SDC's in the same region are supported • Geographic regions are defined as Americas, AsiaPac, EMEA, Japan and the United States. With the High Service Level, NBFW instances in 3 or more geographic regions or 3 or more SDC's in the same region are supported.: • Geographic regions are defined as Americas, AsiaPac, EMEA, Japan and United States.

Optional Features		
Features	**Level**	**Description**
Additional Site Egress	Medium, High	Allows outbound access from more than one SDC. For each additional SDC, the pricing will be based on the bandwidth required for each connection (SECNet). The selected complexity level will be applied once per total customer solution. On the Medium Service Level: • NBFW instances in 2 geographic regions are supported. ○ Geographic regions are defined as Americas, AsiaPac, EMEA, Japan and United States. • Support for multi egress – up to 2 firewall locations. On the High Service Level: • NBFW instances in 3 or more geographic regions are supported. ○ Geographic regions are defined as Americas, AsiaPac, EMEA, Japan and United States. • Support for multi egress – 3 or more firewall locations. By default, each extra SDC will receive a PAT address. While the Medium Service Level can include up to 16 total (shared among all locations) and the High Service Level can include up to 32 IP addresses (also shared among all MFS-NB locations for this service), any additional IP addresses being requested require justification.

Optional Features		
Features	**Level**	**Description**
Additional Site Egress & Ingress	Medium, High	This option allows the Customer to have inbound and/or outbound access through more than one SDC. They can select multiple SDCs. For each additional SDC, the pricing will be based on the bandwidth required for each connection (SecNet). The selected complexity level will be applied once per total customer solution. On the Medium Service Level: • NBFW instances in 2 geographic regions are supported. o Geographic regions are defined as Americas, AsiaPac, EMEA, Japan and United States. • Support for multi egress – up to 2 firewall locations. On the High Service Level: • NBFW instances in 3 or more geographic regions are supported. o Geographic regions are defined as Americas, AsiaPac, EMEA, Japan and United States. • Support for multi egress – 3 or more firewall locations. For each additional SDC there will be the following elements: 1. By default each extra SDC will receive a PAT address. While the medium service level can include up to 16 total (shared among all locations) and the high service level can include up to 32 IP addresses (also shared among all MFS-NB locations for the Customer), any additional IP addresses being requested require justification by the Customer. This is due to the global shortage of IPv4 address space. 2. Two additional ePVCs for each extra SDC. 3. Policy setup and support for each SDC. 4. Special technical considerations and/or restrictions may apply when there are inbound requirements in conjunction with Additional Site Egress and Ingress.

Optional Features		
Features	**Level**	**Description**
Cross Connect - GRANDFATHERING NOTICE: As of April 30, 2022, the Cross-Connect feature of LevelBlue Network Based Firewall is grandfathered and no new customers for the feature will be accepted. Existing Customers can continue using the feature pursuant to the terms of their Service Agreement.	High	Provides connections between the NBFW instance in a Data Center location and the customer's cage in the same Internet Data Center. Cross Connect options supported are where the equipment in the cage is 1) Managed by MFS Operations, 2) The equipment is managed by the customer; or 3) the equipment is managed by Managed Hosting Operations.
Site Failover - GRANDFATHERING NOTICE: As of April 30, 2022, the Cross-Connect feature of LevelBlue Network Based Firewall is grandfathered and no new customers for the feature will be accepted. Existing Customers can continue using the feature pursuant to the terms of their Service Agreement.	High	This option allows the customer to have a single alternate SDC in the same geographical region to receive "failover traffic". A 3rd ePVC is provisioned from the alternate site to the customer's MPLS network. A duplicate security policy is maintained on the alternate SDC for a specified SecNet. If Customer has multiple SecNets, they must purchase Site Failover for the same number of SecNets if failover is a requirement for each. Special requirements apply for MFS-NB Failover which have to be followed for proper operations and which would be considered during the design phase.

SD-2.1.4.1. SafeSearch

Section Effective Date: 04-Nov-2015

For this capability, the Web Filtering – Advanced feature has to be ordered. SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature. Three search sites are supported: Google, Yahoo and Bing.

SD-2.1.4.2. Anonymization of Log Data for International Privacy Regulations

Section Effective Date: 13-Jun-2012

Privacy requirement in Most of World (MOW) for user data to be anonymized in reporting, which will anonymize the user ID in Network Based Firewall logs. The Customer will enable this feature using Self-Service.

SD-2.1.4.3. Malware Scanning

Section Effective Date: 09-Dec-2015

Antivirus scanning examines files for viruses, worms, Trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

- Malware Scanning anti-virus scan engines will scan websites visited by users.
- Provides inline scanning of HTTP content for common virus, spyware, and malware threats and vulnerabilities.
    - Also provides the ability for inline scanning of Instant Messaging protocols (ICQ, MSN, Yahoo and AIM).
- If a web page or web page attachments are found to contain a virus or spyware, then access to that web page or attachments is denied and the Internet user will be displayed an automatic virus alert web page.
- All attachments can be blocked by file type or extension.
- Encrypted traffic and attachments cannot be scanned.

If the enforcement of the Customer's User Authentication policy is required to support User Groups, the Malware Scanning – Advanced feature must be ordered.

If the logging of permitted HTTP, FTP, IM traffic is required (e.g. User Level detailed reporting is needed if available), the Malware Scanning – Advanced feature must be ordered.

SD-2.1.4.4. Grayware

Section Effective Date: 13-Jun-2012

For this capability, the Web Filtering – Advanced, or Malware Scanning – Advanced feature must be ordered.

This category includes:

- Spyware – that tracks users activities
- Adware
- Dial
- Downloader
- Keylogger
- Hacker Tool
- Remote Access/Administration Tool

SD-2.1.4.5. Content Filtering

Section Effective Date: 13-Jun-2012

The Customer can control web content by blocking access to web pages containing specific words, phrases, patterns or images. This helps to prevent access to pages with questionable material.

The web content filter feature scans the content of every web page. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases. If the sum is higher than the threshold set, the page is blocked.

SD-2.1.4.6. Application Control

Section Effective Date: 13-Jun-2012

This feature controls end user access to Web 2.0 applications, i.e. Video and Audio streaming, IM control, VOIP, Peer to Peer and Games. Abuse of these applications can lead to increased bandwidth demand and increased susceptibility to malware attacks.

Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

This feature is included when either or both the Web Filtering- Advanced or Malware Scanning – Advanced add-ons are ordered for the appropriate number of users.

SD-2.1.4.7. Data Loss Prevention

Section Effective Date: 13-Jun-2012

For this capability, either or both the Web Filtering – Advanced or Malware Scanning – Advanced feature must be ordered.

This feature allows the Customer to prevent sensitive data from leaving the network to prevent unwanted data from entering the network and to archive some or all of the content. When the Customer defines sensitive data patterns, data matching these patters will be blocked or logged and allowed.

The Customer creates individual filters based on the file type (e.g. all JPEG file), file name (e.g., find all files called secret.*), file size (e.g., files exceeding a specified size), a regular expression (match strings of text), an advanced rule (a single condition and the traffic in which the condition will appear), or a compound rule (a combination of advanced rules) in a DLP sensor and assign the sensor to a security policy.

- This feature prevents leakage of personal data and allows the definition of data flexibility to define rules based on HTTP, FTP, and IM protocol. Provides analysis and blocking of outbound file types, preconfigured IDs (e.g., credit card numbers or social security numbers) and DFA-based regular expressions.
- Service also provides key word identification and blocking. For example, key word in document will block sending of document, e.g., “Proprietary”.

SD-2.1.4.8. User Authentication

Section Effective Date: 27-Aug-2013

If User Authentication is requested to be supported, Customers will be able to set policy controls over User level access to the Internet. After certain criteria is met (as determined by LevelBlue) and needed components are set up in the Customer network, the MFS-NB platform will interface with a Customer's hosted and managed User Authentication service (RADIUS, LDAP or Active Directory) to authenticate User activity to the Internet. Note: MFS-NB will not provision, administer, support, or troubleshoot the Customers User Authentication solution. For User Authentication support, Customer must have either or both the Web Filtering – Advanced or Malware Scanning – Advanced feature.

SD-2.1.4.9. IP Sec Connection to Cloud Web Security (CWSS)

Section Effective Date: 02-Apr-2015

IPSEC Connection to Cloud Web Security Service (CWSS)

Customers who purchase MSS-NB and CWSS may opt to use a IPSEC tunnel to connect MSS- NB to the CWSS provider. This option allows Internet browsing access with minimal workstation configuration changes because there is no browser proxy configuration required. Using a policy-based feature on MSS-NB, traffic that is destined to an IP address of "any" (i.e., 0.0.0.0/32) that has a destination TCP port of 80 or 443 can be sent to CWSS through the IPSEC tunnel.

When using the IPSEC option with CWSS, Customer understands there is neither a) monitoring of the IPSEC tunnel by LevelBlue, or b) automated failover to a secondary CWSS location. If the CWSS location is unreachable, it is the Customer responsibility to submit an expedited MACD and to notify the GCSC to change the IP address to a different CWSS node. The following example illustrates one scenario:

CWSS Public Address	
Primary	198.135.124.164
Secondary	199.116.171.164

In this example, if the Primary CWSS center was unreachable and the Customer was unable to browse to the Internet through CWSS, the customer would initiate a MACD request and call the

GCSC operations center for an expedited change. The change would be a request to modify the destination of the IPSEC definition from 198.135.124.164 to 199.116.171.164. To make the request easier to implement, customer should maintain a list of primary, secondary, and tertiary IP addresses that can be used.

SD-2.2. MFS-NB Service Option 2

Section Effective Date: 08-Apr-2016

LevelBlue MFS-NB has announced a new simplified pricing model for new customers. There are two service levels available as a part of LevelBlue's MFS-NB service:

- Primary
- Enhanced

Each complexity level supports both inbound and outbound traffic through the MFS-NB platform. Complexity categorization is determined by examining the required traffic types that would be passing through the gateway. LevelBlue completes the policy administration on the equipment but also allows the Customer to make changes to certain configuration settings. With Enhanced Complexity Level, add-on features, such as Web Filtering, Malware Scanning, Active IDS/IPS and User Authentication support are available.

SD-2.3. MFS-NB service for AT&T NetBond®

Section Effective Date: 09-Dec-2015

LevelBlue MFS-NB service for AT&T NetBond® provides inline security between the customers Multi-Protocol Label Switching (MPLS) VPN and their cloud partners. MFS-NB for AT&T NetBond® creates two VPNs: a trusted enterprise VPN and an extranet Cloud Solution Provider (CSP) VPN. The MFS-NB service for AT&T NetBond® firewall provides traffic separation between the trusted corporate VPN and the extranet CSP VPN using a stateful firewall function and Unified Threat Management features. MFS-NB service for AT&T NetBond® supports two VLANs (primary and backup) with burstable bandwidth up to 5GB each from the firewall edge routers to the trusted VPN. LevelBlue MFS-NB service for AT&T NetBond® provides:

- Security Monitoring – 7x24 monitoring of traffic into the network Firewall.
- Stateful Inspection of allowed IP traffic via Firewall.
- Layer 2 isolation – VLAN traffic remains isolated through the MFS-MB Service infrastructure and the Security Policy.
- Self-Administration Capability of NBFW configuration
- Reporting – standard firewall reports via the Business Direct portal.
- Support – 24x7 helpdesk support for trouble ticket and Move/Add /Change requests

SD-2.3.1. Features of the MFS-NB Service for AT&T NetBond

Section Effective Date: 09-Dec-2015

Two service levels are available with MFS-NB/P-to-CSP:

- Primary
- Enhanced

SD-2.3.1.1. Primary Service Level

Section Effective Date: 09-Dec-2015

Primary Service Level supports burstable bandwidth up to 5GB and a common Customer Security Policy allowing both inbound and outbound traffic flow based on the configuration. The Primary Level includes basic reporting and self-administration capabilities via BusinessDirect®.

SD-2.3.1.2. Enhanced Service Level

Section Effective Date: 09-Dec-2015

The Enhanced Service level provides the Primary Service Level capabilities as well as:

- Basic or Advanced Web Filtering
- Basic or Advanced Malware Filtering
- IDS Logging or Active IDS/IPS

SD-2.4. Customer Responsibilities

Section Effective Date: 27-Aug-2013

Customer is responsible for:

- Designating a person who will be the technical focal point to work with LevelBlue to help promote a successful implementation.
- Providing a list of desired IP protocols to deploy during the implementation including source addresses, destination addresses, ports, TCP and/or UDP and a description of the Service to be implemented.
- Providing LevelBlue with user workstation counts and traffic estimates if URL Filtering features or options are selected.
- Providing the necessary network information to allow LevelBlue to provision ingress virtual circuits into the network firewall.
- Identifying a suitable test location during enablement and implementation to properly test desired Security Policies prior to deploying all sites on the MFS-NB Service.
- Utilizing internal Hosts and servers that are properly maintained to include the latest available security patches and are not infected with any worm, trojan or virus or similar security threat. LevelBlue is not responsible for patching or removing security threats on Customer maintained equipment.
- Ensuring that Customer systems and networks (including outsourced and educational environments) that connect with those belonging to MFS-NB, or that use common services network features, have appropriately implemented security controls. These controls should be designed to prevent loss, disclosure, unauthorized access, or service disruption, by restricting LevelBlue network access and use to authorized Customer personnel only. Use of the LevelBlue network and its facilities is intended for the contracting Customer only and not for those who may be interconnected with the Customer's systems. The administration of individual IP addresses on a Customer's LAN, including maintaining distinct, unique, and non-overlapping private IP address space.
- Customer needs to notify LevelBlue about any changes to a Customers configuration(s). If changes to security configurations are necessary at a given location based upon Customer notification, LevelBlue will review these new requirements and make recommendations as necessary.

SD-2.5. Service Availability

Section Effective Date: 30-May-2018

The MFS-Network Based Service is designed to provide single site redundancy and optional failover to other Security Data Centers in the event of catastrophic failure. Optional failover is not available with MFS-NB on ADI. LevelBlue incorporates many automatic redundancy and diversity features designed to quickly handle failures in network components. Additionally, equipment within the LevelBlue backbone network and LevelBlue packet services networks are generally connected to other equipment with multiple routes across the global backbone or packet services network infrastructures.

The LevelBlue MFS-NB Service is available 7 X 24, except for possible Outages during scheduled maintenance. LevelBlue utilizes the scheduled maintenance windows to upgrade equipment, software, and facilities which may add capacity, new features, resiliency and which may provide fixes to known problems to help ensure high network performance. The scheduled maintenance windows are typically used to maintain many sites, including the global backbone, packet services, LevelBlue enhanced network services IDC's and MFS-NB networks. Scheduled maintenance times are:

Scheduled Maintenance Table	
Region	**Times**
United States	Every Sunday - 3:15 a.m. until 4:45 a.m. Eastern Standard Time and Every 3rd Sunday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time Every Monday through Friday from 00:00 a.m. until 6:00 a.m. Eastern Standard Time Every 1st Wednesday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time
Canada	Every Sunday - 3:00 a.m. until 4:45 a.m. Eastern Standard Time and Every 3rd Sunday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time Every Monday through Friday from 00:00 a.m. until 6:00 a.m. Eastern Standard Time Every 1st Wednesday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time
Asia Pacific	Every Monday - 2:00 a.m. until 5:00 a.m. Japan Standard Time and Every 3rd Sunday*- 00:00 a.m. until 8:00 a.m. Japan Standard Time Every Monday through Friday from 00:00 a.m. until 6:00 a.m. Japan Standard Time Every 1st Wednesday* - 00:00 a.m. until 8:00 a.m. Japan Standard Time

Scheduled Maintenance Table	
Region	**Times**
Europe, Middle East, Africa (EMEA)	Every Sunday - 3:00 a.m. until 5:00 a.m. Central European Time and Every 3rd Sunday* - 00:00 a.m. until 8:00 a,m. Central European Time Every Monday through Friday from 00:00 a.m. until 6:00 a.m. Central European Time Every 1st Wednesday* - 00:00 a.m. until 8:00 a.m. Central European Time
Latin America	Every Sunday - 3:15 a.m. until 4:45 a.m. Eastern Standard Time and Every 3rd Sunday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time Every Monday through Friday from 00:00 a.m. until 6:00 a.m. Eastern Standard Time Every 1st Wednesday* - 00:00 a.m. until 8:00 a.m. Eastern Standard Time
*If the 3rd Sunday of the month or the 1st Wednesday of the month falls on a holiday or other special day, LevelBlue may reschedule the monthly maintenance window.	

In addition, LevelBlue may perform extended maintenance up to four times per year, and LevelBlue may need to schedule planned maintenance at other times due to, for example, government inspections or power maintenance. LevelBlue will use reasonable efforts to give Customers at least 30 days' notice of such scheduled or extended maintenance. However, LevelBlue reserves the right to perform maintenance at any time in order to maintain the service and/or network.

SD-2.6. Support and Management

Section Effective Date: 27-Aug-2013

LevelBlue provides the following support for MFS-NB:

SD-2.6.1. Initial Consultation for a Customer's Security Enablement

Section Effective Date: 27-Aug-2013

- Review of the inbound and outbound Security Policies provided to LevelBlue by Customer to recommend a proposed migration configuration of the MFS-NB Service.
- Review of the network topology to determine general access requirements.
- Recommendation of Security Policies to meet the current and forecasted needs specified by the Customer, consequent with LevelBlue's need to manage, maintain, operate and provide measurement reports based upon them.
- Recommendation of additional security management options to meet the specified Customer support needs.

SD-2.6.2. Assistance

Section Effective Date: 30-Apr-2012

- Communicating with the Customer's technical contact(s) for installations, moves, adds changes.
- Communicating with various LevelBlue work centers for packet services or Managed Router or other data or IP services.

SD-2.6.3. Installation Support

Section Effective Date: 27-Aug-2013

- Connection and test of MfS-NB access circuits(s) to the network access point.
- ePVC ordering, provisioning, configuration, and associated testing.
- Configuration of LevelBlue MFS-NB network infrastructure.
- Registration of Customer information and security configuration in LevelBlue's databases.

SD-2.6.4. Network Monitoring and Management

Section Effective Date: 27-Aug-2013

- Proactive 7x24 monitoring of the Customer’s MFS-NB connection (including access) from LevelBlue’s network management center of all the components supplied by LevelBlue.
- Help desk support for connection problems related to the MFS-NB service.
- Change management. If changes to security configurations are necessary at a given location based upon Customer notification, LevelBlue will review these new requirements and make recommendations as necessary. LevelBlue will also manage any resulting changes to the platform that LevelBlue deems necessary, which may result in a conversion charge for affected LevelBlue MFS-NB provided Services.
- Scheduled software and hardware maintenance upgrades to help ensure LevelBlue’s hardware and software are appropriately configured for transmission of traffic.
- Problem management; logging, tracking and escalation of reported problems based on LevelBlue specified severity levels.

SD-2.6.5. Service Activation Date

Section Effective Date: 27-Aug-2013

The Start Date when a new standard MFS-NB connection will be made available to the Customer will be agreed upon after receipt of a signed contract and/or order letter.

Installation is defined as complete once a Host or other device on a site has been PINGed, a Customer’s end-to-end connections have been verified and LevelBlue has implemented the initial deployment of the MFS-NB Service (initial Security Policy deployment).

Billing will begin after successful PING and verification tests are complete, and the initial Customer site(s) have been accepted into maintenance, except in the event that LevelBlue is unable to complete the installation because of Customer actions, including the unavailability of the Customer’s final Security Policies or configurations, in which case billing will commence on the original scheduled Start Date.

SD-2.6.6. Special Requests

Section Effective Date: 09-Dec-2015

Customers can request a change in bandwidth, optional features and/or functional support (such as service level support) of an installed MFS-NB Service agreement. Other than the possibility of a change in the billing amount, enablement time periods will vary depending on the type of change to the service.

Changes may result in an interruption of connectivity for a period of time depending on the complexity. For each change, LevelBlue will register, arrange for installation, and test the circuit as appropriate. If required, LevelBlue will configure and arrange for installation of a new network connection (and a backup connection). Additional MFS-NB connection charges may be applied, depending on the type of change to the service.

Change charges are due upon acceptance of an order and payable upon installation or cancellation of an order. Major Service changes or additions may require extended lead times, depending on the type of change. For example, if a Customer's subscription level is increased from 10Mbps to 50Mbps, LevelBlue may require network capacity and packet service resource adjustments.

MFS-NB new connections and migrations are scheduled on an individual basis. Lead times for installations and changes to existing connections may vary by geography. LevelBlue will endeavor to accommodate special Customer requests regarding installations and conversions such as expediting the scheduled installation date.

LevelBlue will invoice the Customer for engineering or enablement fees plus an administration charge as a result of special requests.

Billing will begin after successful PING and verification tests are complete, and the initial Customer site(s) have been accepted into maintenance, except in the event that LevelBlue is unable to complete the installation because of Customer actions, including the unavailability of the Customer's final Security Policies or configurations, in which case billing will commence on the original scheduled Start Date.

SD-2.6.7. Help Desk Support

Section Effective Date: 27-Aug-2013

All problems, questions or requests for assistance related to the MFS-NB Service should be made to the designated LevelBlue help desk support. Problems may be reported by telephone or electronically, where available. The time an incident starts is when a trouble is validated by LevelBlue and a trouble ticket is opened. The resolution time is the time at which the incident is resolved to the satisfaction of both the Customer and LevelBlue, and the trouble ticket is closed.

- US, EMEA and AP: Centralized Customer Help Centers provide 7x24 problem assistance.

SD-2.6.8. Problem Severity Code Definitions

Section Effective Date: 27-Aug-2013

The Customer defines the severity of a problem when the call is placed. The following definitions are provided as guidance to assist the Customer to appropriately assign the severity of a problem.

Problem Severity Codes and Definitions	
Severity	**Definition**
1	LevelBlue's highest level of severity, a severity 1 Trouble Ticket is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects a Firewall Outage. By way of illustration, without any limitation of the description, such incidents include a Firewall Service Component interface(s) being unavailable, any failures of Firewall Equipment and the inability of a Customer sanctioned IP protocol from working through the Firewall Equipment denotes a severity 1 ticket.
2	A severity 2 Trouble Ticket is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects an attack against a Customer's Firewall Equipment. The types of incidents which will generate Severity 2 incidents are: a) unexplained root logins or access attempts to the Firewall, b) unexplained Firewall server file transfers or c) failed or interrupted Firewall processes.
3	Severity 3 Trouble Tickets are defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects certain system health problems with the Firewall Equipment. The types of incidents which will generate Severity 3 alerts are: a) backup problems, such as backup failures or missing backup files, or b) an audit which reveals missing files; or c) Trouble Tickets generated when LevelBlue has specific and accurate information about a specific Customer Trouble.
4	Severity 4 Trouble Tickets are most often used for Moves, Adds and Changes, and Deletes (MACDs). Severity 4 tickets are also generated when LevelBlue needs additional specific information about a Customer Trouble.
5	Severity 5 Trouble Tickets are reserved for changes associated with out-of-band testing.

SD-2.6.9. Electronic Problem Reporting

Section Effective Date: 30-Apr-2012

The service hours for electronic problem reporting, available in selected countries, are 24 X 7 excluding the periods for maintenance. LevelBlue will use commercially reasonable efforts to notify Customers in advance of maintenance periods in addition to those listed below. LevelBlue reserves the right to perform emergency maintenance on the electronic Customer support system as may be required.

- United States
  - Saturday 04:00 am EST through Saturday 07:00 am EST
  - Sunday 03:00 am EST through Sunday 05:00 am EST

SD-3. LevelBlue Secure E-Mail Gateway Service (SEG) (grandfathered*)

SD-3.1. Advanced Level of Service

SD-3.1.1. Overview

Section Effective Date: 25-Jul-2015

The Secure E-Mail Gateway Advanced service helps protect customer networks from inbound messages containing spam, viruses, and malware. The Service provides features that enable customer to manage and enforce its security policy on outbound email content. The Service provides disaster recovery protection against lost email data in event of a customer email server Outage and provides end-user continuity functionality if the customer email server becomes unavailable. SEG is administered by the customer through a self-service web console and provides a suite of reports.

SEG requires that the Customer own and manage their Simple Mail Transfer Protocol (SMTP) email server or servers. The customer must also own and manage their Internet domain(s) in order to direct email to the Service for filtering.

*The LevelBlue Secure E-Mail Gateway Service (SEG) set forth in this Section SD-3, and SLA-1, are no longer available to order or renew for existing Customers as of July 24, 2015 and will be grandfathered as of September 1, 2015. This SEG Service will be replaced with the new SEG service as set forth in Section SD-4, below.

Cross References

SD-4. LevelBlue Secure E-Mail Gateway (SEG) Service

SD-3.1.2. Supported Features

Section Effective Date: 27-Aug-2013

- Customer Managed Administration
- Anti-Virus Protection
- Spam Filtering
- Policy Enforcement
- Quarantine
- Disaster Recovery Transport Layer Security
- Attachment Filtering
- Content Groups
- Web Hyperlink Filters (this feature will no longer be available as of October 1, 2013)
- Enforced Domain Keys Identified Mail (DKIM)
- Emil Authentication/Enforced SPF
- Message Audit
- Custom Regular Expressions
- Registered Documents
- Administrator Reports

SD-3.1.2.1. Summary of Supported Features

SD-3.1.2.1.1. Customer Managed Administrations

Section Effective Date: 30-Apr-2012

The primary interface to the SEG Advanced service is the Administration Center web console. This console is available 24 x 7 and allows Customer Administrators to define and manage settings and configurations for their domains, including spam treatment options, virus scanning selections, content filter settings, policy rules and user permissions.

SD-3.1.2.1.2. Anti-Virus Protection

Section Effective Date: 30-Apr-2012

Anti-Virus Protection provides an extensive and redundant anti-virus filtering process that is designed to detect, clean, and record virus infected e-mail messages before they enter the Customer’s network. Virus Protection can be configured to scan all inbound and outbound messages for viruses as recognized by industry standard virus scanning technologies. Virus definition libraries used by the Service are continuously updated with new virus signatures.

If the Service detects what it perceives to be a virus in an e-mail message, it will attempt to remove the virus. If it is not possible or feasible to remove the virus, then the anti -virus management service will delete the attachment and the message in its entirety. The Customer administrator may configure anti-virus notification options in the event that a virus-infected message is detected.

SD-3.1.2.1.3. Spam Filtering

Section Effective Date: 30-Apr-2012

Spam Filtering detects Spam e-mail messages before they enter the Customer’s network. Captured spam is routed to the spam quarantine and can be accessed by administrators or end users at any time through a web-based interface. The Customer administrator may configure spam quarantine notification options for messages that have that been quarantined.

SD-3.1.2.1.4. Policy Enforcement

Section Effective Date: 19-Jan-2013

Policy enforcement supports the ability to apply the Customer’s corporate messaging policies on unwanted and malicious content to e-mail messages entering and leaving the Customer’s e-mail system. Policy enforcement features are definable by domain or user level.

Policy actions that can be taken include:

None - The email is forwarded to the recipient email address.

- Quarantine the message – The email is sent to the recipient’s domain content quarantine area.
- Deny Delivery – The email is denied delivery.
- Allow – The email is sent to the recipient email address.
- Tag the message subject with “[SPAM]” – The phrase “[SPAM]” is added to the subject line of the email at the beginning of the subject text and the email is sent to the recipient email address.

The Customer can define text, referred to as an “outbound disclaimer” that will be appended to the email content.

The Customer administrator may configure policy enforcement notification options for emails have been identified by policy rules.

SD-3.1.2.1.5. Quarantine

Section Effective Date: 08-Feb-2014

The Service provides multiple quarantine areas with different security access requirements to store and support review of suspect email outside of your email network. Emails that violate configured policies and that have the quarantine action applied are sorted into multiple quarantines. Quarantined messages will be accessible for 14 calendar days.

- Spam Quarantined Messages – Accessible to all users, with users with role of User or Reports Manager allowed to access only their own personal spam quarantine.
- Virus Quarantined Messages – Accessible to only Administrators and Quarantine Managers.
- Attachment Quarantined Messages – Accessible to only Administrators and Quarantine Managers.
- Content Keyword Quarantined Messages – Accessible to only Administrators and Quarantine Managers.

SD-3.1.2.1.6. Disaster Recover provides:

Section Effective Date: 19-Jan-2013

Disaster Recovery provides added protection against lost emails in case the Customer’s inbound email server may be unavailable to receive email.

- Automatic email failover rolling storage for up to sixty (60) calendar days.
- Automatic monitoring of Customer’s e-mail server to establish return of service with attempt to deliver the e-mail every 20 minutes.
- Automatic forwarding of stored e-mail once Customer’s e-mail service is restored
- User access to read and send messages through a web-based interface while messages are in fail-over storage status. Messages can remain in fail-over storage for up to 60 calendar days.

SD-3.1.2.1.7. General Features

Section Effective Date: 31-Jul-2018

The Content Groups, Custom Regular Expressions and Registered Documents will no longer be available of October 10, 2014 with the SEG Advanced Level of Service, but will be available with SEG Premium Service.

Transport Layer Security

The SEG Advanced Service supports both forced and opportunistic Transport Layer Security (TLS) connections between the Customer's email server and the SEG network. TLS is designed to provide basic network level encryption through an encrypted tunnel for message transfer. The Service also supports Certificate Authority Validation whereby the certificate issued to the sending server (if Inbound) or recipient server (if Outbound) will be validated against the SEG Service's list of trusted certificate authorities.

Attachment Filtering

The Service supports filtering by file type, file name, file size and also the scanning of text content within outbound email attachments.

Web Hyperlink Filters

The Service provides the ability for a Customer to configure whether the Web hyperlinks in email are blocked or can be clicked and followed by the user. The customer can also designate an allow List of URL addresses that are excluded from the processing.

The Web Hyperlink Filters feature will no longer be available beginning October 1, 2013.

Enforced Domain Keys Identified (DKIM)

Administrators have the ability to apply policy to inbound email depending on a Domain Keys Identified Mail (DKIM) check. Customers can also use DKIM to sign outbound emails. DKIM allows email senders to 'sign' messages so that recipients can validate their origin and the integrity of the emails' content.

Email Authentication/Enforced SPF

Enforced SPF allows customers to enforce stronger protection against email spoofing. To implement SPF, domain owners must create special DNS entries conforming to the SLF standard which list the IP addresses that are authorized to send email from their domain. The Enforced SPF feature allows the customer to take actions based on whether or not inbound email was sent from an IP address authorized by the domain owner.

Message Audit

Message Audit provides a basic self-service message audit capability that allows you to research message disposition information. Message disposition data may lag the underlying message by 30 minutes and will be available for the following 13 calendar days.

Cross References

SD-3.3. Summary of Supported Features

SD-3.1.2.1.8. Administrator Reports

Section Effective Date: 09-Sep-2013

Included in the SEG Administration Center console is a suite of reports with which you can monitor your service activity. Data for Administrator Reports may lag several hours behind the current time. Data for Administrator Reports will be available for at least 30 calendar days from the date of the applicable underlying message.

The reports that are available on a domain or organization basis are:

Reports	
Report Name	**Description**
Traffic Overview	Information about all Inbound and Outbound email traffic and bandwidth for the designated domain(s) during the selected date or date range.
Traffic TLS	Information about all TLS Inbound and Outbound email traffic, percentages and bandwidth for the designated Domain(s) during the selected date or date range.
Threats: Overview	Information about email violations by policy type for the designated domain(s) during the selected date or date range.
Threats: Viruses	Information about all Inbound and Outbound emails that violated the virus policies for the designated domain(s) during the selected date or date range,
Threats: Spam	Information about emails that violated the spam policies for the designated domain(s) during the selected date or date range.
Threats: Content	Information about emails that violated the content keyword policies for the designated domain(s) during the selected date or date range.
Threats: Attachments	Information about emails that had attachments that violated the attachment policies for the designated Domain(s) during the selected date or date range.
Enforced TLS Details	Information about all Enforced TLS Inbound and Outbound email traffic, including the number of messages and bandwidth for the designated Domain(s) during a selected timeframe. The report also includes a count of Inbound and Outbound messages that were denied due to an Enforced TLS Policy violation.

Reports	
Report Name	**Description**
Enforced SPF	Displays all Enforced SPF inbound email traffic, including the information about number of messages and validations for the designated domains during a selected timeframe. The report also includes a percentage of incoming email messages that were denied, validated or unavailable due to an Enforced SPF Policy violation.
QuickProtect: Overview	Information about ClickProtect processing. ClickProtect processing tracks Web hyperlinks received in emails that can be clicked and followed by the user or that can be blocked depending on the ClickProtect policy configurations for the designated domain(s) during the selected date or date range. The QuickProtect: Overview report will no longer be available beginning October 1, 2013
ClickProtect: Click Log	Information about Web hyperlinks in emails that were clicked by the recipient for the designated domain(s) during the selected date or date range. The ClickProtect: Click Log report will no longer be available beginning October 1, 2013.
Quarantine Release: Overview	Information about emails that were quarantined and released from all quarantine areas within the Service for the designated domain(s) during the selected date or date range.
Quarantine Release Log	Information about emails that were released from all quarantine areas within the Service for the designated domain(s) during the selected date or date range.
User Activity	Information about all Inbound and Outbound email traffic and bandwidth for the designated domain(s) during the selected date or date range.
Event Log	Displays messages that have had actions performed based on the content, spam content, virus, or attachment policy definitions. Messages can be sorted per domain, and Inbound direction, Outbound direction or both. Messages that are identified as threats by the Email Defense Service are also included.
Audit Trail	Displays the audit log items for all actions performed by users at Report Manager, or higher level, roles within the Control Console for the designated domain(s) during the selected date or date range, including sign ins and configuration changes.
Inbound Server Connections	Displays information about the connections made to the Inbound email servers during processing.
Disaster Recovery: Overview	Information about emails that were spooled and unspooled by the disaster recovery service for the designated domain(s) during the selected date or date range.
Disaster Recovery: Event Log	Displays the event log items for actions performed within the disaster recovery service. Included are actions performed automatically by the Service and performed manually by the administrator.

SD-3.2. Premium Level of Service

SD-3.2.1. Overview

Section Effective Date: 19-Jan-2013

The SEG Premium Level of Service includes all features of the Secure E-Mail Gateway Advanced service and also includes the additional Premium features described in this section.

SEG Premium enables the customer to configure their content policies so that outbound messages meeting certain policy criteria are automatically encrypted.

Messages sent by the Customer's end-user scan be encrypted automatically through policy or through end-user self-initiated encryption. Encrypted messages are delivered for pick-up by an authenticated recipient and can be retrieved up to 30 days from the day they have been sent after which they are destroyed.

The SEG Premium Service requires Customer acknowledgement that it is the Customer's responsibility to store or process, in an unencrypted format, any and all messages or attachments which it desires to have unencrypted access after 30 days and/or post-expiration or termination of the Services.

SD-3.3. Summary of Supported Features

Section Effective Date: 10-Oct-2014

- Policy based Encryption
- End-User Initiated Encryption
- Delivery Notification
- Web-based delivery
- Direct delivery
- Mobile device support
- Branding
- Administrator Reports
- Content Groups
- Custom Regular Expressions
- Registered Documents

SD-3.3.1. Policy Based Encryption

Section Effective Date: 30-Apr-2012

The SEG Premium Service provides a policy-based encryption and decryption process. The process is designed to analyze messages leaving the Customer's network using the policy engine, match an outbound encrypt rule and enable the encryption. Outbound content policies are centrally created using the policy manager. One or more conditions (e.g. contains credit card number, message body contains keywords, email address of sender or recipient matches a domain name, message attachment is of a certain type, etc.) are defined by the Customer, and the policy is associated with the 'encrypt message' action. If a message matches one of the policies it is encrypted within the LevelBlue SEG network and sent to the recipient.

SD-3.3.2. End-User Initiated Encryption

Section Effective Date: 19-Jan-2013

SEG Premium enables End Users to send encrypted email messages from the gateway by pressing a "Send Encrypted" button installed on the mail client. End-User Initiated Encryption is supported through an email client plug-in that provides the "Send Encrypted button". The plug- in is available for versions of Microsoft Outlook.

SD-3.3.3. Delivery Notification

Section Effective Date: 16-Feb-2013

SEG Premium provides notification to senders when message recipients pickup and decrypt messages. Notification messages are customizable.

SD-3.3.2. End-User Initiated Encryption

Section Effective Date: 19-Jan-2013

SEG Premium enables End Users to send encrypted email messages from the gateway by pressing a "Send Encrypted" button installed on the mail client. End-User Initiated Encryption is supported through an email client plug-in that provides the "Send Encrypted button". The plug- in is available for versions of Microsoft Outlook.

SD-3.3.3. Delivery Notification

Section Effective Date: 16-Feb-2013

SEG Premium provides notification to senders when message recipients pickup and decrypt messages. Notification messages are customizable.

SD-3.3.4. Encryption Console Delivery

Section Effective Date: 19-Jan-2013

The Encrypted Message Console is a web-based Console for message pick-up. After an encrypted message is sent, the recipient is prompted through an email notification to collect their message at the Encrypted Message Console. First time users of the portal are required to create a password protected profile. Once a recipient has created a profile, they collect subsequent messages by clicking the link in the email notification and logging in to Encrypted Message Console with their email address and password. Messages stored within the Encrypted Message Console expire and are destroyed after 30 days Recipients have the option within the Encrypted Message Console to export a message as an .eml file enabling the user to store a message locally unenecrypted.

SD-3.3.5. Regular Mailbox Delivery

Section Effective Date: 19-Jan-2013

Recipients of encrypted email messages have the option of receiving their encrypted messages in their regular email client mailbox. For users who have chosen Regular Mailbox Delivery, the encrypted message is sent as an encrypted attachment to a notification email sent to the recipient’s regular mailbox. To read the encrypted message, the recipient is prompted to login to the Encrypted Message Console. Encrypted messages sent through regular mailbox delivery do not expire. Recipients have the option within the Encrypted Message Console to export a message as an .eml file enabling the user to store a message locally unencrypted.

SD-3.3.6. Mobile Device Support

Section Effective Date: 19-Jan-2013

SEG Premium supports mobile devices that can render HTML on a mobile browser. As an example, SEG supports Blackberry devices, Apple iPhone, Windows mobile devices, and more. All encrypted messages being decrypted on the web-based message portal can be read on any traditional mobile browser.

The user experience is optimized for each mobile browser because the SEG Premium service has the ability to recognize which mobile browser is being used by the recipient to read and decrypt messages and adjust accordingly.

SD-3.3.7. Branding

Section Effective Date: 16-Feb-2013

The SEG Premium Service supports use of one customer provided logo that can be displayed within Encrypted message sender/recipient notification messages and within the Encrypted Message Console.

SD-3.3.8. Content Groups

Section Effective Date: 10-Oct-2014

The Service provides both predefined and custom content group functionality. The following predefined content groups are available: Acceptable Use, Australia Policy, Austria Policy, Banking and Financial Sector, Brazil Policy, Canada Policy, China Policy, China National ID, Chinese Hong Kong Policy, Chinese Taiwan Policy, Competitive Edge, Employee Discontent,

Entertainment Industry IP, FERPA Compliance, FISMA Compliance, Financial and Security Compliance, France Policy, GLBA Compliance, German Policy, HIPAA Compliance, India Policy, Israel Policy, Korean Policy, Legal, Mexico Policy, Netherlands Policy, North America PII, Payment Card Industry, Poland Policy, Russia Policy, Sexual Content, SOX Compliance, Singapore Policy, Spain Policy, State Privacy Laws, Turkey Policy, UK Policy. The customer cannot edit predefined content groups but can designate whether or not they are used. Custom content groups can be defined by the Customer.

SD-3.3.9. Traffic: Encryption Report

Section Effective Date: 09-Sep-2013

The Traffic Encryption Report window displays information about all Outbound Email Traffic, percentages, and bandwidth for the designated Domain(s) during the selected date or date range sent out to be encrypted. Data for Traffic Encryption Report may lag several hours behind the current time. Data for Traffic Encryption Report will be available for at least 30 calendar days from the date of the applicable underlying message.

SD-3.3.10. Custom Regular Expressions

Section Effective Date: 10-Oct-2014

Enables Customer Administrators to define, test and implement custom content policies using regular expressions (regex). Regex that is deemed harmful will not be accepted by SEG system.

SD-3.3.11. Registered Documents

Section Effective Date: 10-Oct-2014

Registered Documents detects and blocks key documents, based on their content, from being emailed out of the organization.

Registered document scanning is performed on an outbound basis only. With Registered Documents, key documents can be uploaded by the Customer to the SEG network, where every word is scanned by a hashing algorithm, and a hashed version of the document is stored in the SEG system. The original document is not retained in the SEG system and therefore is not subject to data residency compliance. All outbound emails are then scanned and compared against the hashed document, and if a match is found, a policy action will be applied. (Encrypt, Allow, Tag, Quarantine, Deny or None).

Registered Documents supports a wide variety of file formats and languages, however, formats that don’t include any text content, including some zip, .ipg and .mov files, may not be compatible. Customers can maintain a library of 100 registered documents and each file can be up to 30 MB in size. Each Registered Document can be retained for one year, but the Customer Administrator can remove the document at any time.

SD-3.4. LevelBlue Secure E-Mail Gateway Service — Message Archiving Option

SD-3.4.1. Overview

Section Effective Date: 19-Jan-2013

The Message Archiving option of the Secure E-Mail Gateway Service provides capabilities that can assist the Customer in complying with company, industry, and government requirements for email retention. Message Archiving is designed to automatically archive all inbound, outbound and internal email message and associated meta data to a centralized location and provides search and export functionality. Message Archiving is administered through a customer managed web console and provides a suite of reports.

Message Archiving requires Customer the use of journaling on Customer managed Microsoft Exchange Servers. Supported Microsoft Exchange email versions are listed below; for all servers, the journal mailbox of the MS Exchange Server must be configured to support Message Archiving.

Supported Servers		
Email Server	**Edition**	**Additional Requirements**
Microsoft Exchange Server 2000	Standard/Enterprise	-Service Pack 3 or higher -Email Journaling Advanced Configuration tool (exejcfg.exe)
Microsoft Exchange Server 2003	Standard/Enterprise	- Service Pack 1 or higher -Email Journaling Advanced Configuration tool (exejcfg.exe)
Microsoft Small Business Server with Exchange Server 2003	Standard	- Service Pack 1 or higher - Email Journaling Advanced Configuration tool (exejcfg.exe)
Microsoft Exchange Server 2007	Standard/Enterprise	- Journaling agents configured on the appropriate Hub Transport servers - For premium journaling, the Exchange Enterprise Client Access License (CAL).
Microsoft Exchange Server 2010	Standard/Enterprise	-Journaling agents configured on the appropriate Hub Transport servers. -For premium journaling, the Exchange Enterprise Client Access License (CAL).

Attachment formats: Message Archiving supports over 300 different file attachment formats that can be archived (including attachments inside of .zip files) and searched based on content. Most common business file formats, such as .doc, .html, .ppt, .txt, .xls, are supported. All attachment names are searchable.

Archive data security: Messages are transported to Message Archiving via TLS or SSL and are stored using 256-bit encryption. A message stored by Message Archiving can be viewed only by the end-user who sent or received the message and the Customer Administrator.

SD-3.4.2. Summary of Supported Features

Section Effective Date: 19-Jan-2013

- Customer Managed Administration
- Retention Period
- Search and Export functionality
- Legal Hold
- Administrator Reports
- Historical Message Storage and Import Options
- Data export upon termination

SD-3.4.2.1. Customer Managed Administration

Section Effective Date: 30-Apr-2012

Message Archiving is configured by the Customer administrator through the Archiving control console. After the Message Archiving service is activated, the Customer can access to the Message Archiving Overview screen to see status of current communication status between Customer mail sources (mail servers) and the Message Archiving service and a summary of key Message Archiving configurations and activity.

Message Archiving supports up to 64 individual mail sources. Each mail source points to a Journal mailbox on your Exchange Server(s). Message Archiving continuously cycles through all customer mail sources to archive messages. A Customer initiated maintenance window can be setup through Customer assignment of a quiet period for each mail source, this suspends the automatic message import process for a defined period of time.

SD-3.4.2.2. Retention Period

Section Effective Date: 19-Jan-2013

Customers determine how long their e-mails need to be retained to meet business, compliance or legal requirements. Depending on the Customer contract, the Service will support a retention period from 30 days to a maximum of 10 years.. At the time an e-mail message is inserted into the archive, it is assigned a time-to-live (TTL) value, based on the length of the customer's defined retention period. Messages will be automatically purged from the system upon reaching the end of retention period.

SD-3.4.2.3. Search and Export Functionality

SD-3.4.2.3.1. Search

Section Effective Date: 19-Jan-2013

Customer Administrators can search for and view the archived messages for all users via one of three search methods – Simple, Advanced and Archive ID. Users, Reports Managers, Quarantine Managers, and Domain Administrators can only search for and view their own archived messages.

Messages that matched Customer search criteria are displayed in the search results pane. To enable efficient multi-tasking, the service allows administrators to view multiple search parameters and results on one screen. Search results can also be saved for later use.

- Simple Search capability: The Customer defines search criteria for one or more of the four main elements of archived messages:
  - Sender
  - Recipient
  - Date Range
  - Message Text
- Advanced Search capability: The Customer define search criteria for any of allowable archived message elements. Advanced search allows more precise search of message text because Customer can specify which part of the following message text to search:
  - Message header
  - Subject line
  - Message body
  - Attachment body

In addition, Customer can search metadata, or information about the messages that Message

- Archiving stores, for specific values. This information includes:
  - Names of attachments

  - Message sizes
- Archive ID searches capability: The Customer can search for a specific message archive ID. A message's archive ID I known by Customer after previously viewing the message or exporting it.

SD-3.4.2.3.2. Export

Section Effective Date: 19-Jan-2013

The Customer can export messages a local computer hard drive through export functionality. Export is limited to up to 1 GB of data found by a search at one time. The Export function of Message Archiving creates a .zip file that contains messages. After exporting, messages must be viewed using the Microsoft Outlook email client.

SD-3.4.2.4. Legal Hold

Section Effective Date: 19-Aug-2013

By selecting the Enable Global Legal Hold option or by applying a User Legal Hold to specific users, you can override the automatic deletion of a e-mail messages so they are preserved beyond their default expiration date. The Legal hold allows you to retain your messages, including expired messages, indefinitely.

With the Global Legal Hold option, all users will be subjected to the specific legal hold.

With the User Legal Hold option, Customer can create and maintain 16 separate legal hold sets. Each legal hold set can contain up to 128 user accounts.

SD-3.4.2.5. Administrator Reports

Section Effective Date: 09-Sep-2013

Reports provide detailed information on specific Customer Administrator activities. Data for Administrator Reports may lag several hours behind the current time. Data for Administrator Reports will be available for at least 30 calendar days from the date of the applicable underlying message.

Reports include:

Administrator Reports	
Report Name	**Report Description**
Administrator Exports	Message exports conducted by users with the Customer Administrator role.
Administrator Message Views	Message views conducted by users with the Customer Administrator role.
Administrator Searches	Message searches conducted by users with the Customer Administrator role.
Legal Hold	Changes in Legal Hold status by users with the Customer Administrator role.
Message Purges	Message purges conducted by users with the Compliance Officer role.
Storage Configuration	Changes in storage configurations by users with the Global, Support, Partner and Administrator role.

SD-3.4.2.6. Historical Message Import Option

Section Effective Date: 19-Jan-2013

In addition to archiving current email messages, customers can contract for a Service option that enables archiving of messages that were created prior to Service activation and stored by the Customer.

Historical messages, which can be up to 25 MB in size, are stored on a designated Historical mail source and are imported into the Email Archiving system along with current mail. Historical messages are never automatically purged by the system. The customer administrator assigned archive compliance officer must manually purge historical messages depending on the customer's retention policy.

SD-3.4.2.7. Managed Import Option (available in the United States only)

Section Effective Date: 19-Aug-2013

Customers with large stores of historical email – generally 50 GB or larger – can contract for an optional professional services engagement that supports offline Managed Import if email data.

SD-3.4.2.8. Data Export upon Termination (available in the United States only)

Section Effective Date: 19-Aug-2013

Should the customer choose to terminate Message Archiving, there are 2 methods for the Customer to obtain their data. Data is exported in .eml format.

Option 1: Self-service export: the Customer can export their data self -service through the Archiving administrative console. Data can be exported in increments of 1GB. There is no charge for customer self-service export of data.

Option 2: Managed export service: the Customer data will be exported onto a storage device by the service provider and shipped to the Customer. There is a one-time charge for the managed export service.

SD-3.4.2.9. 3.X Supported Browsers

Section Effective Date: 19-Jan-2013

The following browsers and related operation systems will be supported:

- Internet Explorer 9 (Windows 7, Windows Vista)
- Internet Explorer 8 (Windows 7, Windows Vista and Windows XP)
- Internet Explorer 7 (Windows Vista and Windows XP)
- Firefox 13 (OS X 10.6, OS X 10.7, Windows 7, Windows Vista, Windows XP)
- Chrome (OS X 10.6, OS X 10.7, Windows 7, Windows Vista, Windows XP)
- Safari* - (OS X 10.6, OS X 10.7) * SaaS Web Protection end users only

SD-3.4.2.10. Message Purge

Section Effective Date: 19-Aug-2013

Allows the Customer assigned Archive Compliance Officer to delete one or more messages from the archive, including Historical messages.

SD-3.5. Domain Name System Services

Section Effective Date: 30-Apr-2012

Customer may, from time to time, request LevelBlue to host Customer's IP addresses or domain names, in accordance with the terms and co nditions set forth herein and at the following web site, which site may be revised from time to time: https://mis- att.bus.att.com/mys/dns_res_terms.html.

Except for the actual domain names expressly registered in Customer's name, all IP addresses, LevelBlue-based domain names and telephone numbers shall remain, at all times, property of LevelBlue and shall be non-transferable and Customer shall have no right to use, and shall release to LevelBlue, such IP addresses upon termination or expiration of this Online Ordering Agreement.

Customer is responsible for registration of its domain names and payment of any domain name registration fees.

SD-3.6. Customer Responsibilities

Section Effective Date: 30-Apr-2012

Customer is responsible for the following with respect to the LevelBlue Secure E-Mail Gateway Service:

- Designating a person who will be the technical focal point to work with LevelBlue to help promote a successful implementation.
- Customer needs to notify LevelBlue about any changes to a Customers configuration(s). If changes to security configurations are necessary at a given location based upon Customer notification, LevelBlue will review these new requirements and make recommendations as necessary.
- Design and management of email filtering policies
- Managing customer internet access and DNS settings
- Managing customer owned email server
- Directory services that communicate with the SEG service
- Microsoft Exchange® Server "journaling" setup and maintenance for SEG Message Archiving

SD-3.7. Help Desk Support

Section Effective Date: 30-Apr-2012

All Inquiries with regard to problems, questions, or requests due to errors that cause SEG service interruption should be made to the designated LevelBlue help desk support. Problems must be reported by telephone. The time an incident starts is when a tro uble is validated by LevelBlue and a trouble ticket is opened. The resolution time is the time at which the incident is resolved to the satisfaction of both the Customer and LevelBlue, and the trouble ticket is closed.

SD-3.8. Problem Severity Code Definitions

Section Effective Date: 30-Apr-2012

Supported Servers		
Severity	**SEG Option and Severity Definition**	**SEG Option and Severity Definition**
1	SEG Advanced and SEG Premium --Errors that cause system wide* interruptions in the delivery of mail, anti spam or anti virus protection, SEG Control Console in accessibility at the Administrator access level or unavailability of quarantined mail outside of regularly scheduled maintenance windows.	SEG Message Archiving --Errors that cause system* wide interruptions in the message archiving service.
2	SEG Advanced and SEG Premium --Errors in which an optional feature of the service is unusable, reporting is unavailable, or a component of the service causes a limited loss of functionality (i.e., minor options or features of the service fail to function) for which there may or may not be a known workaround.	SEG Messaging Archiving --Errors in which an option feature of the message archiving service is unusable or is unavailable, or a component of the service causes a limited loss of functionality (i.e., minor options or features of the service fail to function) for which there may or may not be a known workaround.

Supported Servers		
Severity	**SEG Option and Severity Definition**	**SEG Option and Severity Definition**
3	SEG Advanced and SEG Premium --Errors that only have a minor effect on functionality, or a suggestion is made relating to the operation or is a feature request of a component of the service. Minor administrative user inconveniences.	SEG Message Archiving --Errors that only have a minor effect on functionality, or a suggestion is made relating to the operation or is a feature request of a component of the service. Minor administrative user inconveniences.
4	--General Service Questions --Configuration Questions --Feature Requests --Message Trace Inquiries --Delisting Request	--General Service Questions --Configuration Questions --Feature Requests --Message Trace Inquiries --Delisting Request
5	Awaiting Customer Response	Awaiting Customer Response
NOTE	Individual occurrences are classified as Level 2 errors.	

SD-3.9. LevelBlue Secure E-Mail Gateway Service Use Policy

SD-3.9.1. Summary

Section Effective Date: 16-Jun-2017

LevelBlue does not authorize anyone to send email or cause email to be sent through LevelBlue Secure E-Mail Gateway that violates the LevelBlue acceptable use policy (https://www.att.com) or Service Use Policy within this Service Guide

LevelBlue prohibits the use of LevelBlue Secure E-Mail Gateway to accept, transmit or distribute bulk or otherwise automated email. In addition, email sent, or caused to be sent, to or through LevelBlue Secure E-Mail Gateway that makes use of or contains invalid or forged headers, invalid or non-existent domain names or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit email to be sent to or through Secure E-Mail Gateway is unauthorized.

Email that is relayed from any third party's mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the email is unauthorized.

SD-3.9.2. Policy for Outbound Email Delivery

Section Effective Date: 18-Nov-2013

The following standards apply to the delivery of outbound email through LevelBlue Secure E-Mail Gateway and at LevelBlue's sole discretion we may enforce the following policies:

LevelBlue Secure E-Mail Gateway servers will deny connections from unsecured systems contained within the customer's environment including open relays, open proxies, open routers, or any other system that has been determined to be available for unauthorized use.

LevelBlue Secure E-Mail Gateway mail servers will not accept connections from systems that use dynamically assigned, not controlled within the customer dedicated IP space or residential IP addresses

LevelBlue Secure E-Mail Gateway will not deliver email that contains a hex-encoded Universal Resource Locator (URL). (Example: http://%6d%6e%3f/), where the URL references potential or known sites that are deemed fraudulent).

LevelBlue Secure E-Mail Gateway mail servers will reject messages with attachments that exceed 50MB in accordance with our mail filtering polices.

LevelBlue Secure E-Mail Gateway will deny connections from servers that consistently generate higher than a 10% invalid recipient rate (i.e. over 10% of a sender's mailing list is destined for users that do not exist).

SD-3.9.3. Service Use Policy Enforcement and Notice

Section Effective Date: 30-Apr-2012

Customer's failure to observe the guidelines set forth in this Service Use Policy may result in LevelBlue taking actions anywhere from a warning to a suspension or termination of Customer's IP Services. When feasible, LevelBlue may provide Customer with a notice of an SUP violation via e-mail or otherwise allowing the Customer to promptly correct such violation.

LevelBlue reserves the right, however, to act immediately and without notice to suspend or terminate affected IP Services in response to a court order or government notice that certain conduct must be stopped or when LevelBlue reasonably determines, that the conduct may: (1) expose LevelBlue to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of LevelBlue's network or networks with which LevelBlue is interconnected, (3) interfere with another LevelBlue Customer's use of IP Services or the Internet

(4) violate any applicable law, rule or regulation, or (5) otherwise present an imminent risk of harm to LevelBlue or LevelBlue Customers.

SD-3.10. SEG Conditions

Section Effective Date: 03-Oct-2012

One SEG Advanced/Premium “User” is defined as an individual person that sends or receives email that is processed by the SEG Advanced/Premium Service.

One SEG Archiving “User” is defined as an individual person or a system (including resource mailboxes, distribution group mailboxes, and shared mailboxes) that send or receive email that is archived using the SEG Archiving Service.

Customer will maintain the number of SEG seat licenses to cover all Customer end user/system email being filtered and or archived by the SEG Service and Customer will notify their LevelBlue account manager to process a SEG change order to add/remove SEG seat licenses when Customer end user/system count changes from the contracted amount.

Billing of the SEG Service begins when the Service is provisioned by LevelBlue and made available for Customer use, whether or not Customer has directed their email to the Service.

LevelBlue may terminate the SEG Pricing Schedule if Customer does not change its MX record(s) to direct email to SEG Service within thirty (30) calendar days after the Service is provisioned by LevelBlue and made available for Customer use.

A Customer initiated change order that reduces the user count for the SEG Service constitutes an early termination and is subject to termination fees

Customer with a mix of SEG Advanced and SEG Premium seats will create a separate group of SEG Premium email users with total count of users not to exceed SEG Premium licenses purchased and Customer will only create and apply outbound email filtering policies that use the encrypt action to the SEG Premium email user group.

Customer with a mix of SEG Advanced or SEG Premium and SEG Archiving seats will create a separate journalized mails tore within Microsoft Exchange for the SEG Archiving users with total count of users not to exceed SEG Archiving licenses purchased and Customer will only enable SEG Archiving for the SEG Archiving user mail store.

SD-4. LevelBlue Secure E-Mail Gateway (SEG) Service

SD-4.1. Enterprise E-Mail Security Service

Section Effective Date: 25-Jul-2015

Enterprise E-Mail Security Service consists of Enterprise Protection and Enterprise Privacy.

SD-4.1.1. E-Mail Security Service Overview

Section Effective Date: 25-Jul-2015

Enterprise Protection and Enterprise Privacy provide gateway-based filtering that is designed to protect organizations against external threats such as spam, virus, malware, and phishing attacks, and to help protect information that is leaving from the organization.

SD-4.1.1.1. Enterprise Protection

Section Effective Date: 25-Jul-2015

Enterprise Protection includes the following:

- Email Firewall – provides a first line of defense against threats by providing recipient verification, SPF and DKIM verification, as well as defining and enforcing acceptable -use policies for message content, message size, and attachment file types. The Email Firewall can be applied to both inbound and outbound message flow.
- Quarantine – multiple folders allow for different categories of messages (e.g., phishing, spam, adult and bulk (legitimate marketing messages) to be isolated independently and each can be put into different quarantine folders). Each folder can be configured by the administrator for different levels of end-user access, including no visibility, just visibility, and the ability the release messages.
- Transport Layer Security (TLS) - industry standard gateway-to-gateway encrypted communications. Policies can be configured to connect via TLS when available or enforce TLS for specific domains.
- Graphical Admin Interface – all management functions (administration, reporting, and monitoring) are performed through web-based, graphical interface.
- Spam Detection, the Spam Detection feature is designed to examine attributes in email in order to help block spam, image-based spam, and phishing attacks, while automatically adapting to emerging attacks as they appear.
- Virus Protection – signature based anti-virus scanning.
- Zero-Hour Anti-Virus – behavioral-based zero-hour virus detection technology to help protect against emerging viruses.
- Dynamic Reputation – designed to provide capability to accept, reject, or throttle incoming email connections. This service utilizes real-time database of IP reputation that combines both local data as well as globally observed reputation.
- Smart Search – designed to provide real-time email tracing with the ability to search across

multiple attributes including sender, recipient, subject, sending and host, attachment

SD-4.1.1.2. Enterprise Privacy

Section Effective Date: 25-Jul-2015

- Regulatory Compliance – provides a policy engine to help identify content related to various regulations, including HIPAA, GLBA, and other pre-configured dictionaries and Smart Identifiers to assist in defining policies. Policies can be configured to take specific actions based on sender, sender group, severity of violation and may include blocking, capturing for later review, and/or automatically encrypting.
- Digital Asset Security – provides a policy engine to identify unstructured data (i.e., documents) by "training" the system to identify documents. The Digital Asset Security engine can then be configured to identify exact document or partial document matches and specific actions can be taken based on sender, sender group, severity of violation and may include blocking, capturing for later review, and/or automatically encrypting.
- Encryption – offers email encryption. End-users can force encryption via keyword in Subject line or via an Outlook Plug-In. Administrators may also configure policies in Regulatory Compliance or Digital Asset Security to create policy-based encryption. A Premium Plug-In for Outlook is also available which provides end-to-end encryption from the Outlook client.

SD-4.1.1.3. Target Attack Protection (TAP)

Section Effective Date: 25-Jul-2015

TAP is composed of two primary modules: Attachment Defense and URL Defense.

TAP Attachment Defense - Attachment Defense is focused on helping to protect organizations against malicious weaponized files found in email attachments. Suspicious attachments are sent to the Dynamic Malware Analysis Service to be analyzed for detection of malicious content. All results are summarized in the Threat Insight Dashboard

TAP URL Defense - URL Defense is designed to address the threat of attacks utilizing URLs within emails that ultimately deliver malware to the end-user when a user clicks. Two additional features are provided by URL Defense:

- URL Rewriting - URLs are re-written by TAP as they pass the email gateway. This. By re-writing the URL, TAP also has the ability to help provide protection whether users are on- or off- the corporate network.
- Predictive Analysis - The Predictive Analysis engine is designed to provide a constant, real-time state of unique URLs as they are seen by TAP. This Predictive Analysis engine can then trigger a pre-emptive analysis of URLs without the need to wait for a user to click on a URL.

Both modules include:

- Dynamic Malware Analysis Service - designed to perform a combination of static and dynamic analysis of URLs and files to help identify indicators of malicious behavior. The Dynamic Malware Analysis Service also returns forensic information on the malicious behavior, which is presented within the Threat Insight Dashboard
- Threat Insight Dashboard - This summary threat dashboard provides visibility into when attacks are occurring, who is being attacked, and who may be exposed to malicious content that may require immediate response. The dashboard enables the customer to:
    - See how many and what types of threats are currently being received.
    - Analyze who has received which messages.
    - Check the status of emails containing malicious URLs or attachments and alert response teams to investigate users that may be infected or at risk of being infected.
    - Identify forensic details about the malicious payloads in each attack.

SD-4.1.1.4. Threat Response and Threat Response auto-pull packages

Section Effective Date: 15-Nov-2018

Threat Response is an available orchestration and response automation platform that helps customers with the incident response process.

Threat Response is available in 2 service levels:

- Threat Response auto-pull package

SD-4.1.1.5. Threat Response auto-pull package

Section Effective Date: 15-Nov-2018

- Threat Response auto-pull package (TRAP) provides the following:
- Support of one (1) playbook (i.e. use case) for automating delivered email threat quarantine from user mailbox.
- Support of ingestion of delivered email threat alerts from:
    - Targeted Attack Protection
    - FireEye® EX
    - Custom JSON Alert Source
- Support of grouping of alerts into incidents and enriching incoming alerts with contextual information about the targeted user:
    - Integration with Active Directory® to pull user context information including, but not limited to, department, location, and group membership.
    - Integration with emerging threats and nexus threat graph for enriching delivering email threats against email campaigns and malwares, including WHOIS information for context on IP and domains.
- Support of incident management capabilities such as creating and closing incidents
- Support of integration with exchange on-premises and Office 365
    - Exchange 2010, 2013, 2016
    - Office 365

SD-4.1.1.6. Remote Syslog Forwarding

Section Effective Date: 15-Nov-2018

Remote Syslog Forwarding offers highly secure, near real-time streaming of syslog email data from SEG to a customer provided Security Incident and Event Management (SIEM) service.

SD-4.2. Small and Medium Business Email Security Service

SD-4.2.1. Advanced Package

Section Effective Date: 25-Jul-2015

Service includes: inbound & outbound spam and virus filtering, content filtering, spooling, continuity (24hr storage of e-mails in the event of a planned or unplanned customer mail server outage), email logs and reports.

SD-4.2.2. Advanced Plus Package

Section Effective Date: 25-Jul-2015

Service includes: inbound & outbound spam and virus filtering, content filtering, spooling, continuity inbox (14 days emergency storage of e-mails in the event of an planned or unplanned customer mail server outage), email logs, reports, Instant Replay, URL Defense and Data Loss Prevention (DLP).

SD-4.2.3. Premium Package

Section Effective Date: 25-Jul-2015

Service includes: inbound & outbound spam and virus filtering, content filtering, spooling, continuity inbox (14 days emergency storage of e-mails in the event of a planned or unplanned customer mail server outage.), email logs, reports, Instant Replay, URL Defense, Data Loss Prevention (DLP), and email encryption.

SD-4.3. General Descriptions for Professional Services

Section Effective Date: 15-Nov-2018

Professional Services for Enterprise - For existing customer adding new products and custom engagements these services are purchased individually as set forth in the Pricing Schedule.

SD-4.3.1. Configuration – Enterprise Protection

Section Effective Date: 25-Jul-2015

Installation services for the Enterprise Protection Module. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of the Enterprise Protection Module ("Implementation"). The Implementation excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.3.2. Configuration – Enterprise Privacy

Section Effective Date: 25-Jul-2015

Installation services for the Enterprise Privacy Module. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of the Enterprise Privacy Module ("Implementation"). Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.3.3. SAAS Initiated for Targeted Attack Protection

Section Effective Date: 25-Jul-2015

Installation services for a single Service and the Targeted Attack Protection Module. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of their Service and Targeted Attack Protection Module. Excludes onsite engagements, off hours work, and week-end work and is limited to this particular service

SD-4.3.3.1. Configuration -Targeted Attack Protection

Section Effective Date: 25-Jul-2015

Installation services for the Targeted Attack Protection (TAP) Module. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of the Targeted Attack Protection (TAP) Module. Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.3.3.2. Weekend Cutover Support

Section Effective Date: 25-Jul-2015

The Professional Services team will assist the Customer outside business hours either after hours during the business day or during weekend hours with the cutover to their product. This engagement is charged by the hour with a four (4) hour minimum. Onsite engagements are excluded.

SD-4.3.3.3. System Health Check

Section Effective Date: 25-Jul-2015

System review services for Customer's installation. The Professional Services team will review Customer configuration during standard business hours and provide a written report of recommended best practices the customer should be employing with the configuration of their Service. The expected duration of the project is expected to be 1 week and the effort is expected to be approximately 8 hours. Excludes onsite engagements, off hours work, and week–end work and is limited this particular service and limited to one (1) Service.

SD-4.4. Packaged Professional Services for Enterprise

SD-4.4.1. SAAS Initiated & Configuration for Enterprise Protection

Section Effective Date: 25-Jul-2015

Installation services for a single Service and the Enterprise Protection Module. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of their Service and Enterprise Protection Module. Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.4.2. SAAS Initiated & Configuration for Enterprise Privacy

Section Effective Date: 25-Jul-2015

Installation services for a single Service and the Enterprise Privacy Module. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of their Service and Enterprise Privacy Module. Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.4.3. SAAS Initiated & Configuration for Enterprise Protection and Privacy

Section Effective Date: 25-Jul-2015

Installation services for a single Service and the Enterprise Protection and Privacy Modules. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of their Service and Enterprise Protection and Privacy Module. Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.4.4. SAAS Initiation & Configuration for Enterprise Protection and TAP

Section Effective Date: 25-Jul-2015

Installation services for a single Service and the Enterprise Protection and Targeted Attack Protection Modules. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of their Service and Enterprise Protection and Targeted Protection Modules. Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.4.5. SAAS Initiation & Configuration for Enterprise Protection, Privacy and TAP

Section Effective Date: 25-Jul-2015

Installation services for a single Service and the Enterprise Protection, Privacy and Targeted Attack Protection Modules. The Professional Services team will assist the Customer during standard business hours with planning, configuration, deployment, testing and cutover of their Service and Enterprise Protection, Privacy, and Targeted Attack Modules. Excludes onsite engagements, off hours work, and week-end work and is limited this particular service.

SD-4.5. Small and Medium Business Email Security Service Initiation

Section Effective Date: 25-Jul-2015

If purchased, Small and Medium Business Email Security Service Initiation includes implementation/training support (up to two (2) hours). Service includes: A one on one training appointment (up to two hours) with a Technical Account Manager (TAM). The TAM will provide an overview of the features and configuration options within the Small and Medium Business Email Security service, including a walk-through of the Administrator and End User interfaces, and provide any needed assistance for initial service configuration.

SD-4.6. Training

Section Effective Date: 25-Jul-2015

Virtual Training sessions are available for Enterprise protection and Enterprise privacy at the prices set forth in the Pricing Schedule.

SD-4.7. Domain Name System Services

Section Effective Date: 25-Jul-2015

Customer may, from time to time, request LevelBlue to host Customer's IP addresses or domain names, in accordance with the terms and conditions set forth herein and at the following web site, which site may be revised from time to time: https://mis- att.bus.att.com/mys/dns_res_terms.html.

Except for the actual domain names expressly registered in Customer's name, all IP addresses, LevelBlue-based domain names and telephone numbers shall remain, at all times, property of LevelBlue and shall be non-transferable and Customer shall have no right to use, and shall release to LevelBlue, such IP addresses upon termination or expiration of this Online Ordering Agreement.

Customer is responsible for registration of its domain names and payment of any domain name registration fees.

SD-4.8. Customer Responsibilities

Section Effective Date: 25-Jul-2015

Customer is responsible for the following with respect to the LevelBlue Secure E-Mail Gateway Service:

- Customer Configurations. The Service does not include Customer configurations, policies and procedures implemented and set by Customer available through the Service, including, without limitation, the selection of filtered categories and web application controls (collectively, "Customer Configurations"). Customer is solely responsible for selecting the Customer Configurations and assuring that the selection conforms to Customer's policies and procedures and complies with all applicable laws and regulations in jurisdictions in which Customer is accessing the Service.
- Designating a person who will be the technical focal point to work with LevelBlue to help promote a successful implementation.
- Managing customer internet access and DNS settings.

SD-4.9. Help Desk Support

Section Effective Date: 25-Jul-2015

All Inquiries with regard to problems, questions, or requests due to errors that cause SEG service interruption should be made to the designated LevelBlue help desk support. Problems must be reported by telephone. The time an incident starts is when a trouble is validated by LevelBlue and a trouble ticket is opened. The resolution time is the time at which the incident is resolved to the satisfaction of both the Customer and LevelBlue, and the trouble ticket is closed.

SD-4.10. LevelBlue Secure E-Mail Gateway Service Use Policy and Licenses

SD-4.10.1. Summary

Section Effective Date: 25-Jul-2015

LevelBlue does not authorize anyone to send email or cause email to be sent through LevelBlue Secure E-Mail Gateway that violates the LevelBlue acceptable use policy (http://www.corp.att.com/aup/) or Service Use Policy within this service guide

LevelBlue prohibits the use of LevelBlue Secure E-Mail Gateway to accept, transmit or distribute bulk or otherwise automated email. In addition, email sent, or caused to be sent, to or through LevelBlue Secure E-Mail Gateway that makes use of or contains invalid or forged headers, invalid or non-existent domain names or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit email to be sent to or through Secure E-Mail Gateway is unauthorized.

Email that is relayed from any third party's mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the email is unauthorized.

SD-4.10.2. Policy for Outbound Email Delivery

Section Effective Date: 25-Jul-2015

The following standards apply to the delivery of outbound email through LevelBlue Secure E-Mail Gateway, and at LevelBlue's sole discretion the following policies may be enforced:

LevelBlue Secure E-Mail Gateway servers will deny connections from unsecured systems contained within the customer's environment including open relays, open proxies, open routers, or any other system that has been determined to be available for unauthorized use.

LevelBlue Secure E-Mail Gateway mail servers will not accept connections from systems that use dynamically assigned, not controlled within the customer dedicated IP space or residential IP addresses

LevelBlue Secure E-Mail Gateway will not deliver email that contains a hex-encoded Universal Resource Locator (URL). (Example: http://%6d%6e%3f/), where the URL references potential or known sites that are deemed fraudulent).

LevelBlue Secure E-Mail Gateway mail servers will reject messages with attachments that exceed 50MB in accordance with our mail filtering polices.

LevelBlue Secure E-Mail Gateway will deny connections from servers that consistently generate higher than a 10% invalid recipient rate (i.e. over 10% of a sender's mailing list is destined for users that do not exist).

SD-4.10.3. Service Use Policy Enforcement and Notice

Section Effective Date: 25-Jul-2015

Customer's failure to observe the guidelines set forth in this Service Use Policy may result in LevelBlue taking actions which may include, but not be limited to, a warning, a suspension or the termination of Customer's IP Services. When feasible, LevelBlue may provide Customer with a notice of an SUP violation via e-mail or otherwise allowing the Customer to promptly correct such violation.

LevelBlue reserves the right, however, to act immediately and without notice to suspend or terminate affected IP Services in response to a court order or government notice that certain conduct must be stopped or when LevelBlue reasonably determines, that the conduct may: (1) expose LevelBlue to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of LevelBlue's network or networks with which LevelBlue is interconnected, (3) interfere with another LevelBlue Customer's use of IP Services or the Internet

(4) violate any applicable law, rule or regulation, or (5) otherwise present an imminent risk of harm to LevelBlue or LevelBlue Customers.

SD-4.10.4. License

Section Effective Date: 08-Aug-2015

Use of the Services is subject to the license terms below, and use of the Services indicates acceptance of the licensing terms.

- Customer is granted a limited term, non-sub licensable, non-transferable, and non-exclusive license/subscription to access the Services, for its intended purposes, solely for Customer’s internal business purposes and not for further use by or disclosure to third parties and solely in connection with the Services and in accordance with the LevelBlue Documentation and any applicable laws or regulations. “LevelBlue Documentation” means collectively, the operating instructions, user manuals, and help files, in written or electronic form, made available by LevelBlue to End Users in connection with the Service.

SD-4.10.5. Additional SEG Conditions and Restrictions

Section Effective Date: 08-Aug-2015

Customer will maintain the sufficient number of SEG seat licenses to cover all Customer end user/system email being filtered and or archived by the SEG Service, and Customer will notify their LevelBlue account manager to process a SEG change order to add/remove SEG seat licenses when Customer end user/system count changes from the contracted amount.

Billing of the SEG Service begins when the Service is provisioned by LevelBlue and made available for Customer use, whether or not Customer has directed their email to the Service.

LevelBlue may terminate the SEG Pricing Schedule if Customer does not change its Domain Name Service MX record(s) to direct email to SEG Service within thirty (30) calendar days after the Service is provisioned by LevelBlue and made available for Customer use.

A Customer initiated change order that reduces the user count for the SEG Service constitutes an early termination and is subject to termination fees.

Customer will not, and will not allow any third party to:

(a) sell, resell, license, sublicense, distribute, include any Services in a service bureau or outsourcing offering; or make any Services available to any third party other than Customer's end users;

(b) attempt to gain unauthorized access to, or disrupt the integrity or performance of, a Services or the data contained therein;

(c) use of Services to intentionally transmit any virus, worms, Trojan horses, or other programming routine intended to damage any system or data; or

(d) Copy any part, feature, and function or user interface of the Services. Services are for use with normal business messaging trafficking only and Customer shall not use the Services for the machine generated message delivery of bulk, unsolicited emails or in any other manner not prescribed by the applicable LevelBlue Documentation.

SD-5. LevelBlue Web Security – (grandfathered*)

SD-5.1. Overview

Section Effective Date: 09-Jan-2016

WSS is part of the Secure Network Gateway (SNG) platform which also includes Network- Based Firewall and Secure Email Gateway. WSS can be bundled with these security services, for additional discounts, or sold stand-alone.

WSS is available for any type of Internet connection, covering non-LevelBlue customers as well as LevelBlue customers who use MPLS and have a Network-Based Firewall. It is available in US, EMEA and AP.

*The LevelBlue Secure Network Gateway-Web Security Service (SNG-WSS) as a standalone service will no longer be available to order or renew for existing Customers as of June 29, 2015 and will be grandfathered as of June 29, 2016. The SNG-WSS Service may be replaced with the LevelBlue Cloud Web Security Service (Cloud WSS) located at http://serviceguidenew.att.com/sg_CustomPreviewer?attachmentId=00P1A00000mWo9MUAS

or such other LevelBlue designated location by contacting an LevelBlue sales representative. Note that this service discontinuance does not impact Network-Based Firewall customers who have purchased Network Based Firewall Web Filtering and/or Network Based Firewall Malware Scanning.

SD-5.2. Standard Features

Section Effective Date: 30-Apr-2012

WSS offers the following standard features:

SD-5.2.1. Web Filtering

Section Effective Date: 30-Apr-2012

- Allows internet traffic to be filtered based on web site content. This option has the following features available:
- Over 75 pre-defined URL categories (e.g. religion, sports, etc) which are selected to be allowed or denied.
- The Whitelist / Blacklist function allows browsing to specific URL's to be permitted or denied. This function overrides any URL filtering options. Customer can filter on URL, IP address or both.
- It is possible to block web searches based on keywords
- Web filtering can also be done by IP address as well as URL name.
  - The Web Filtering feature provides the ability for web pages to be filtered using URL categorization and content analysis. URL's are categorized by reference to a number of predefined categories as specified in Customer's portal. Customer will be able to configure the Web Filtering to create their own access restriction policies (based on categories and types of content) and deploy them to specific User groups.
  - Web Filtering will filter as much of the web page and its attachments as possible. Web Filtering may not filter certain web pages or attachments (for example, those that are password protected or encrypted). Customer may also configure specific exceptions for web sites that should not be filtered. Encrypted traffic (i.e. HTTPS/SSL) cannot be filtered and will be passed through unfiltered unless otherwise specified by Customer. Web Filtering will only filter pages based on the specific categories which Customer has chosen.
  - Customer has the option of performing individual and/or group administration and reporting capabilities.
  - If the User requests a web page or attachment where an access restriction policy applies, then access to that web page or attachment is denied and the User will be displayed an automatic alert web page.
  - WSS supports any language for URL filtering. The browser converts the user request into UTF format and the query against the URL database is also in UTF.

SD-5.3. SafeSearch

Section Effective Date: 30-Apr-2012

SafeSearch is a feature of popular search sites that prevents explicit websites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful User may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature. Three search sites are supported: Google, Yahoo and Bing.

SD-5.4. Malware Scanning and Content Filtering and Grayware

Section Effective Date: 04-May-2012

Antivirus scanning examines files for viruses, worms, trojans and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

- Malware Scanning anti-virus scan engines will scan as much of the web page and its attachments as possible (Content Filtering).
- •Provides in-line scanning of HTTP content for common virus and malware threats and vulnerabilities
- Also provides the ability for in-line scanning of Instant Messaging protocols (ICQ, MSN, Yahoo, and AIM).
- If a Web page or Web page attachments are found to contain a virus or spyware, then access to that web page or attachment is denied and the Internet user will be displayed an automatic virus alert web page.
- All attachments can be blocked by file type or extension.
- Encrypted traffic and attachments cannot be scanned (target 4Q2012 for Encrypted Traffic scanning).

WSS's gateway architecture takes advantage of specialized hardware architecture in LevelBlue's network to accurately and quickly detect malicious content without sacrificing the security or performance of the network.

WSS uses proxy inspection, which unpacks files prior to inspection. Files are subjected to multiple layers of content and protocol analysis, allowing the system to detect even the most sophisticated polymorphic malware.

The Web Security Service architecture is certified by ICSA (International Computer Security Association) labs to verify detection of all viruses in the WildList. The WildList is a database of the most active viruses on the internet. The list is updated continually and is maintained by www.wildlist.org. Monthly ICSA testing certifies our appliances contain the most up-to-date wild list database. In contrast, none of the current stream-based gateway methods have been certified or industry-proven to provide 100% WildList protection.

WSS provides real time and two-hour emergency signature updates. The database of viruses will include:

- Viruses currently spreading (as determined by our Security Team)
- Recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared
- “Zoo” viruses, which have not spread in a long time and are largely dormant. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.
- Signatures for polymorphic and packed-file viruses.

Files are scanned for the following

- File Size
- File pattern/type
- Virus Scan

SD-5.4.1. Grayware

Section Effective Date: 07-May-2012

This category includes:

- Spyware- that tracks users activities
- Adware
- Dial
- Downloader
- Keylogger
- Hacker tool
- Remote Access/Administration Tool

This feature is provided as optional in case customers determine it creates too many false positives.

SD-5.4.2. Content Filtering and Web Content Control

Section Effective Date: 30-Apr-2012

The customer can control web content by blocking access to web pages containing specific words, phrases, patterns or images. This helps to prevent access to pages with questionable material.

The web content filter feature scans the content of every web page. The system administrator can specify banned words and phrases and attach a numerical va lue, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases. If the sum is higher than the threshold set, the page is blocked.

Web Content Control allows customers to allow or block Java Script, Active X, and Cookies per user group. The customer needs to consider how to use this capability some since web sites may not work if these features are blocked.

SD-5.5. Roaming User Support

Section Effective Date: 30-Apr-2012

This feature provides the ability for customer's to set policy controls over group user level access to the internet. The WSS gateway interfaces with a customer hosted and managed User Authentication server (Active Directory with Secure LDAP or RADIUS) to provide this feature and to assist in authenticating user activity to the internet.

- In order for traveling users to have the same protection as corporate users regarding Web Filtering, Malware Scanning, Application Control and DLP and Keyword Blocking, the customer must download and install a client to each roaming user's laptop.
- Support is provided in US, EMEA and AP regions.

Customers can define multi-regional service which will allow roaming users to automatically connect to the closest data center.

SD-5.6. Application Control

Section Effective Date: 30-Apr-2012

Application filtering controls end user access to Web 2.0 applications, i.e., Video and Audio streaming, IM control, VOIP, Peer to Peer, Games. Abuse of these applications can lead to increased bandwidth demand and increased susceptibility to malware attacks.

Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

SD-5.7. Data Loss Prevention and Key Word Blocking

Section Effective Date: 04-May-2012

This feature allows the customer to prevent sensitive data from leaving the network, to prevent unwanted data from entering the network and to archive some or all of the content. When the customer defines sensitive data patterns, data matching these patterns will be blocked, or logged and allowed.

The customer creates individual filters based on file type (ex. all JPEG files), file name (ex. find files called secret.*), file size (ex., files exceeding a specified size), a regular expression (match strings of text), an advanced rule (a single condition and the traffic in which the condition will appear), or a compound rule (a combination of advanced rules), in a DLP senso r and assign the sensor to a security policy.

- This feature prevents leakage of personal data and allows the definition of data flexibility to define rules based on HTTP, FTP and IM protocol. Provides analysis and blocking of outbound file types, preconfigured IDs (e.g. credit card numbers or social security numbers) and DFA-based regular expressions.
- Service also provides key word identification and blocking. For example, key word in document will block sending of document, ex. “Proprietary.”

SD-5.8. Anonymization of Log Data for International Privacy Regulations

Section Effective Date: 30-Apr-2012

Privacy requirement in MOW for user data to be anonymized in reporting, which will anonymize the user ID in WSS logs. The customer will enable this feature using Security Self-Service.

SD-5.9. IPSEC Support

Section Effective Date: 30-Apr-2012

IPSEC tunnels transport traffic in an encrypted mode from the customer’s site or network to the Web Security Gateways. This allows users at the company site, and roaming users visiting the company site, to have a better secured connection to the Internet. Work stations on premise will not need configuration changes or additional software with this option. For roaming users visiting a customer site, the client will recognize the user is on the corporate network allowing the user to connect directly to the Internet without the use of the client.

SD-5.10. SSL Support for WSS Customer

Section Effective Date: 30-Apr-2012

Provides an encrypted session so hackers can't eavesdrop on the User's session.

SD-5.11. Security Self-Service

Section Effective Date: 30-Apr-2012

Security Self-Service is an LevelBlue web application that allows customer administrators of WSS to view their company's policies and manage features like Web Filtering, Malware Scanning and Application Control configuration from a browser.

Once the customer administrator makes and saves changes to their policies and selects the Deploy button, the change is pushed to the Web Security gateway, which is inspecting traffic.

Management of users (add/delete users and user groups) will take place on the customer's Active Directory.

The administrator can:

- Set web filtering policies (block and allow categories, white list/black list)
    - Block or allow predefined categories such as "Personal Relationships", "Internet Radio and TV", etc. which contain the most common URLs (facebook.com, myspace.com, pandora.com, etc.)
    - Block or allow predefined classifications such as "Image Search", "Video Search", etc.
    - Block or allow custom categories created by the customer administrator containing specific URLs defined by the customer administrator
    - Manage identity based user group policies- add, change, delete and move rules,
- Manage Malware Scanning policies to control virus attacks, spam and spyware.
    - Allow users to view, create, change and delete Malware scanning profiles and file filter profiles.
- Manage Application Control List Profiles for IM, Audio and Video Streaming, etc.
    - Allow users to view, create, change and delete Application Control profiles and file filter profiles.
- Manage Web Content Control policies to control Java applets, Active X and Cookies.
    - Allow users to view, create, change and delete Web Content Control profiles and file filter profiles.

- Audit logging capability includes the individual(s) who made the change, what was changed and when it was changed. Audit logs can be searched by specifying a time period, category or type of log and type of action taken.
- Customize alert pages via direct input or file upload- dynamically generated HTML pages displayed to the end User when they attempt to access prohibited web content. Customer can choose a standard Block Alert Page or their own customized content, which can be uploaded via the portal

Note: Customer will need to ensure changes to policies on one site or VDOM occurs in other VDOMs.

SD-5.12. Reporting

Section Effective Date: 30-Apr-2012

WSS reports are provided via the LevelBlue Business Direct Portal. The reports provide top 10 through top 50 details on events for day, week and month periods. A list of the reports is given below.

Automated reports are available on overall traffic, blocked URLs, spyware and web viruses stopped. Reports can be downloaded to PDF, Powerpoint, Excel or Snapshot.

- Bandwidth Usage Reports- permit customers to monitor bandwidth usage, by category and user, and to detect the abuse of certain applications that consume large amounts of bandwidth.
- Web Category Access Reports- permit customers to track business vs. non-business use of the Internet by users.
- Sites Accessed Reports- track how many users visit denied sites against company policy. For allowed sites, determine if users are visiting business-related sites..
- Browse Time Reports- permit customers to determine how long users browse to sites that may reduce productivity.
- Malware Scanning Reports- permit customers to monitor the frequency and types of threats attempting to enter their networks, and to monitor where these threats originated. The report also permits customers to determine which users receive more attacks than others, which indicates they may need training on surfing the Internet.
- Application Control reports- allow customers to determine what users attempted to access blocked applications by type and category and examine usage of allowed application categories.
- Data Leakage Prevention reports- allow customers to measure blocked leakage of sensitive personal data, ex. credit card numbers, Social Security Numbers, via web traffic.

SD-5.13. Responsibilities of the Parties

SD-5.13.1. Customer Responsibilities

Section Effective Date: 30-Apr-2012

- Customer will supply LevelBlue with all technical data and any additional information required in order for LevelBlue to activate the LevelBlue Web Security Services. The LevelBlue Web Security Services does not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection.
- Customer agrees to undertake all necessary steps to keep confidential and not reveal or disclose to any third party, without prior permission from LevelBlue, any username or password information provided to Customer by LevelBlue. If for any reason LevelBlue believes that there has been a security related breach, LevelBlue may take whatever action LevelBlue deems appropriate to remedy the situation.
- Customer will:
  - Install LevelBlue-provided software for communication between customer-owned authentication servers and the Web Security Service. The software will provide authentication for local, on-net users for Scenario 1 (NBFW with roaming users) and Scenario 3 (IP SEC authentication).
  - When required, install and maintain Network Policy Server in conjunction with Active Directory for RADIUS authentication.
  - Support RADIUS authentication if they enable the WSS Client for any of their users, roaming or non-roaming.
  - Customer will need to configure a VSA (Vendor Specific Attribute) on their premises RADIUS server for RADIUS authentication to be granular at the group level.
  - Manage installation of the WSS Client on all remote user laptops
  - Manage installation of the WSS Client on all non-roaming user laptops when customer is using Client Authentication for all users.
  - Provide Tier 1 Help Desk for all corporate users.
  - Provide and manage CPE (IP SEC termination for the WSS service) which may be required for customers who:
    - do not have MPLS service
    - who have stationed users at a particular site
    - who do not want to install the SSL client on each work station
  - Notify LevelBlue of any unauthorized use of Customer's account;

  - Implement recommended changes or service upgrades, as reasonably requested;
  - Designate a Single Point of Contact (SPOC) to provide Customer Tier 1 helpdesk to internal Customer users; and this SPOC shall adhere to the roles and responsibilities as designated in the Agreement;
  - Verify on a regular basis the portal which is permanently accessible, except when the Service is unavailable, to validate the functionalities activated by Customer for his customer policy(ies) in support of the Services and notify LevelBlue in writing, within 24 hours, in case Customer were to notice a discrepancy between the functionalities displayed on the portal and the ones Customer deems to have activated;
  - Create service policies for the features they have purchased, ex. URL Filtering, Malware Scanning, Application Control.
  - Customer will need to ensure changes to policies on one site or VDOM occurs in other provisioned sites or VDOMs

SD-5.13.2. Customer Premise Equipment Requirements for WSS

Section Effective Date: 30-Apr-2012

- IP SEC termination devices supported- Juniper, Cisco, Fortinet, Netgear, Checkpoint.
- Mac Notebooks are supported.
- Client Support
- Windows release versions supported for end user client are:
  - Windows 2000 on 32-bit, and both 32-bit and 64-bit versions of Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, and
  - Windows 7
  - Internet Explorer version 8 or higher is recommended for client rendering.

SD-5.14. LevelBlue Responsibilities

SD-5.14.1. LevelBlue will:

Section Effective Date: 30-Apr-2012

- Provide tier two and tier three level technical support to Customer's designated Single Point of Contact ("SPOC").
- Accept trouble report calls initiated by the customer designated SPOC

SD-5.15. Half Tunnel Responsibility (only for Scenario 3 Other-Carrier — IPSEC Authentication with/without Roaming Users)

SD-5.15.1. Responsibilities of the Parties

Section Effective Date: 30-Apr-2012

In order for the VPN Half-Tunnel to work, Customer must ensure that the Customer or third party firewall device runs IPSEC capable of supporting 3DES and/or AES encryption with a pre- shared key, and meets such other specifications as LevelBlue provides to Customer.

Half-Tunnel implementation requires the cooperation of the Customer or third party for proper configuration of the Customer or third party device and for successful test and turn up. It is a Customer responsibility to ensure that the third party is available and actively participates in the implementation to turn up the VPN Half-Tunnels. Customer understands and agrees that LevelBlue may not be successful in implementing the turn up. If the turn-up effort is unsuccessful after approximately one hour of work by LevelBlue, Customer shall review the configurations on the Soft MACD and re-submit a revised configuration.

Upon Customer's notification that there is a problem on a VPN Tunnel problem, LevelBlue will verify the configuration has not changed and is in accordance with Customer's original request and will then refer all troubles back to the Customer. LevelBlue will be responsible for troubleshooting only the LevelBlue-provided VPN Half-Tunnel and Customer will be responsible for troubleshooting the third party VPN Half-Tunnel. LevelBlue will not troubleshoot, or attend to, any problems or issues that arise with regard to the third party Firewall Device. Customer will be responsible for engaging and working with the third party in all such troubleshooting efforts. LevelBlue will not work directly with or have any obligations to the third party.

Customer must supply to LevelBlue any and all details required to enable LevelBlue to properly configure the Firewall Devices. Customer is responsible for requesting any configuration changes required on LevelBlue-provided Firewall Devices that may be needed in order to initiate, establish or maintain a VPN Tunnel.

LevelBlue is not responsible for any configuration, changes or any aspects of the third party Firewall Device.

Unless otherwise agreed to in writing by LevelBlue, LevelBlue shall provide no more than ten VPN Tunnels and/or VPN Half-Tunnels, in total.

SD-5.15.2. Customer Care/Technical Support

Section Effective Date: 27-Aug-2013

For issues regarding Web Security Service, client installation, connectivity or user authentication, customers can contact the GCSC. If the Security Self-Help portal does not support the creation or change of a Web Security feature policy (ex. Data Leak Prevention), customers can contact the GCSC Help Desk to request the change.

FAQs and help for customer questions on creating policies, how to apply them to particular groups and other questions on how to use Security Self-Help can be found on the Self-Help portal.

Hours of Operation:

- 24 hours per day X 7 days per week X 365 days per year coverage
- United States - Operations Help Desk:

The GCSC team access number is: 877 677 2881

You will then be prompted for your client PIN

Select prompt 3 - Secure Network Gateway

Then select prompt 4 – Web Security Service

Incident Management Escalation/Notification and Change Request Escalation Procedures are covered in the LevelBlue MSS Welcome Package distributed by the GCSC for all MSS customers.

SD-5.15.3. Problem Severity Code Descriptions

Section Effective Date: 30-Apr-2012

LevelBlue determines the severity of a trouble ticket when it is created or proactively identifies the cause of the incident. This occurs either when a Customer call is received or when the monitoring center identifies an incident. The following descriptions are provided as guidance to assist the Customer with appropriately understanding the priority and severity of a problem.

SD-5.15.3.1. Severity Description

Section Effective Date: 30-Apr-2012

LevelBlue’s highest level of severity, a severity 1 Trouble Ticket, is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects a problem with the performance of the WSS. By way of illustration, without any limitation of the description, such incidents include a Service Component interface(s) being unavailable, any failure of platform Equipment and the inability of a Customer sanctioned IP protocol from working through the platform Equipment denotes a severity 1 ticket.

A severity 2 Trouble Ticket is defined as a Trouble Ticket generated by LevelBlue in the event that LevelBlue detects an attack against a Customer's Firewall Equipment. The types of alarms which will generate Severity 2 incidents are: a) unexplained root logins or access attempts to the Firewall, b) unexplained Firewall Server file transfers or c) failed or interrupted Firewall processes.

Severity 3 Trouble Tickets are defined as Trouble Tickets generated by LevelBlue in the event that LevelBlue detects certain system health problems with the platform Equipment. The types of incidents which will generate Severity 3 alerts are: a) backup problems, such as backup failures or missing backup files, or b) an audit which reveals missing files; or c) Trouble Tickets generated when LevelBlue has specific and accurate information about a specific Customer Trouble.

Severity 4 Trouble Tickets are most often used for Moves, Adds and Changes, and Deletes (MACDs). Severity 4 tickets are also generated when LevelBlue needs additional specific information about a Customer trouble.

Severity 5 Trouble Tickets are reserved for changes associated with out-of-band testing.

SD-5.15.3.2. Usage of the Service

Section Effective Date: 30-Apr-2012

Customers will be audited throughout the year to determine if the number of seats on the service has grown above the number of contracted seats.

Number of seats is defined as the number of the customer's users and servers who can potentially send traffic through the service or the number of users and servers identified in the customer's Active Directory.

Number of seats is not concurrent (number of users on the service at the same time).

SD-5.16. LevelBlue Web Security Services Installation

Section Effective Date: 26-Apr-2013

WSS Installation is defined as complete once a Customer has confirmed that its web traffic is flowing through the Web Security Gateway.

Billing will begin once the WSS has been accepted into maintenance, except in the event that LevelBlue is unable to complete the WSS Installation because of Customer's actions or omissions, including Customer's failure to implement final Security Policies or configurations, in which case billing will commence on the ninetieth (90th) day following the date Customer and LevelBlue have signed the WSS Pricing Schedule.

SD-6. LevelBlue DDoS (Distributed Denial of Service) Defense

SD-6.1. Overview

Section Effective Date: 05-May-2018

The LevelBlue DDoS Defense Service ("DDoS Defense Service" or the "Service") can only be provided to ADI/ADI+/ADIG Customers and/or LevelBlue Internet Data Center ("IDC") Hosting customers with connectivity to the LevelBlue IP Backbone.

The Bandwidth Based, Proactive DDoS Defense service is available only to qualifying Government entities and Education customers.

The DDoS Defense – Data Center Model service is only available to qualifying resellers of LevelBlue for the protection of their own internet access links and not for purpose of further resale to their customers.

The DDoS Defense Service includes DDoS attack detection and mitigation that takes place within LevelBlue's backbone and provides protection against volumetric attack traffic before reaching the Customer site. It consists of a network detection device, which examines samples of Customer traffic flow data from the LevelBlue network for each address identified by Customer. Upon detection, or

Customer notification of a perceived DDoS Attack, LevelBlue can reroute traffic targeted at an attacked host through the LevelBlue IP Backbone to a shared Scrubbing device which then 'scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic. The DDoS Defense Service is designed to then pass valid traffic to the Customer access router. Once it is determined that the DDoS attack has subsided, Customer may request that LevelBlue continue proactive mitigation. Otherwise, LevelBlue will resume the normal routing of Customer traffic once LevelBlue determines the DDoS attack has subsided. The Customer will have access to reports on the attack and mitigation activity through a Customer-specific portal ("DDoS Defense Portal"). In addition, LevelBlue shall:

- During the first two (2) weeks following the Service Activation Date, examine samples of Customer traffic flow data and analyze patterns within such data in order to baseline Customer traffic patterns to assist in determining when a DDoS attack is occurring;
- When LevelBlue believes that conditions so warrant; (a) issue Alert(s) to Customer about IP Threat(s) which shall direct Customer to the DDoS Defense Portal for further information; (b) provide information via the DDoS Defense Service Portal to assist Customer in addressing and/or mitigating IP Threats;
- Notify Customer via email within fifteen (15) minutes, and where warranted, by telephone within twenty (20) minutes, when LevelBlue believes a DDoS attack is occurring;
- Provide Customer access to reports on specific attacks and mitigation activity through an LevelBlue specific website provided to Customer; and
- Make available to Customer the Traffic Anomaly Detection analysis and Traffic Anomaly Detection reports related to any DDoS Attacks on Customer during the period in which DDoS Defense Service is provided to Customer. All reports are LevelBlue Proprietary Information and are subject to the terms and provisions of the Agreement.

SD-6.2. Traffic Anomaly Detection

Section Effective Date: 01-Aug-2013

LevelBlue uses sampled traffic flow data from access routers within the LevelBlue network. This data is directed to the LevelBlue Anomaly Traffic Detection devices.

Traffic Anomaly Detection has two algorithms that run on a single detection portal. The first algorithm looks for "Misuse Anomalies" while the second algorithm looks for "Profiled Anomalies". Traffic Anomaly Detection, using both algorithms, is designed to detect anomalous traffic patterns that are considered malicious and to alert Customer that mitigation may be warranted.

SD-6.2.1. Detection Capabilities and Exclusions

Section Effective Date: 07-Dec-2016

The DDoS Defense Service is designed to detect and help protect against attacks that are volumetric in nature, regardless of attack size. For the purposes of this Service Guide, a volumetric attack is defined as an attack that sends high volumes of traffic designed to overutilize bandwidth and eventually deny access for legitimate users. Volumetric attacks include those attacks listed in the Volumetric Attack Types and Description table set forth below. Volumetric attacks do not include: (i) application layer attacks (those that primarily target applications); (ii) SSL attacks (those aimed at exploiting the CPU intensive nature of encrypting and decrypting packets); and (iii) "low and slow" attacks (those that consume a high number of connections and can exhaust server resources).

Volumetric Attack Types and Descriptions	
Attack Type	**Description**
Spoofed	Sending packets with a forged source address
Malformed	Sending packets with abnormal bits or flags set
Floods	Sending high rates of legitimately formed packets
Null	Sending packets with no content or illegitimate protocol
Fragmented	Sending packet fragments that will never be completed
Brute Force	Sending packets that exceed defined flow rates threshold

SD-6.2.2. DDoS Anomalies

Section Effective Date: 31-Jul-2013

Misuse Anomalies are traffic patterns that are of known DoS signatures including high rates of protocol fragments, ICMP, SYNs, RSTs and Nulls (No payload).

Profiled Anomalies are traffic patterns that have exceeded the learned baselines that have been generated by LevelBlue based on a sliding two week interval of Customer traffic flow. Profiled thresholds are set at certain levels of Packets Per Second ("PPS") or Bits Per Second ("BPS") in excess of the pre-determined baseline.

Both Misuse Anomalies and Profiled Anomalies have three severity levels: LOW, MEDIUM, and HIGH. Low level anomalies are generated when traffic exceeds a minimum threshold. Medium level anomalies occur when the traffic exceeds a higher threshold value. A High level anomaly occurs if the attack exceeds a higher threshold and is sustained for 300 seconds (5 minutes). An Alert is automatically generated in response to a High level anomaly. Low and Medium level anomalies can be viewed via the DDoS Defense Portal. Anomaly notifications will be deleted after thirty (30) days if Low level, sixty (60) days if Medium level and one year if High level.

SD-6.3. Mitigation

Section Effective Date: 29-Sep-2017

Network Packet Scrubbing facilities utilize centralized DDoS mitigation devices to mitigate known malicious packets destined to the Customer network. A predefined BGP speaker will instruct a facility to re-route Customer traffic to one or more Scrubbing facilities. The BGP speaker will advertise the specific /32 address that is being attacked. This will reroute only that traffic targeted for the specific IP address to one or more of the LevelBlue Scrubbing facilities. After the Scrubbing facilities mitigate the malicious content, traffic determined to be valid wi ll be forwarded back to the Customer through a path that includes an LevelBlue managed virtual private network ("VPN"). Customer is not required to purchase VPN services from LevelBlue for mitigation to take place.

Mitigation duration on the Bandwidth Based, Proactive DDoS Defense service will be eight (8) hours.

SD-6.3.1. Methods of Triggering

Section Effective Date: 18-Aug-2018

LevelBlue will activate the DDoS Defense Service mitigation via BGP speaker within the LevelBlue network. During service enablement, Customer may choose between pre-authorized mitigation and manual mitigation.

- Pre-Authorized Mitigation: When the LevelBlue detection device identifies a volumetric attack and provides an Alert to the S/NOC and the Customer, the work center will trigger the start of mitigation prior to notifying the Customer. With DDoS Defense – Agnostic service, special routing configurations required by LevelBlue may have to be implemented by Customer for this feature to function properly.
- Manual Mitigation: When the LevelBlue detection device identifies a volumetric attack and provides an Alert, the S/NOC will consult with the Customer before any mitigation is activated.

In addition, in the event Customer identifies a volumetric attack, the Customer can notify LevelBlue to request activation of mitigation.

With the DDoS Defense – Data Center Model service the pre-authorized mitigation triggering method is configured.

SD-6.3.2. Platform Initiated Mitigation (PIM)

Section Effective Date: 29-Sep-2017

Using the LevelBlue DDoS Defense service components, PIM detects and automatically initiates DDoS mitigation for active DDoS attacks when pre-defined traffic thresholds are exceeded. Pre-defined thresholds are configured during initial setup of the PIM feature. PIM is supported on the 215 hour or higher Hourly Rate DDoS Defense plans. Platform Initiated Mitigation is not available with DDoS Defense Carrier Agnostic service or on the Bandwidth Based, Proactive DDoS Defense service.

SD-6.3.3. Resumption to Normal Traffic Flow SD-6.3.3.1. Non-Agnostic Service

Section Effective Date: 14-Nov-2015

When LevelBlue determines, within its sole discretion, that traffic patterns have returned to normal, acceptable pre-attack levels and DDoS Defense mitigation has become unnecessary, LevelBlue will notify Customer, stop the scrubbing of traffic destined for the monitored IP address and will revert to standard, optimal routing. LevelBlue will continue the monitoring of registered IP address through the DDoS Defense service and will initiate mitigation steps as described in the “Methods of Triggering” section.

SD-6.3.3.2. Customer Responsibilities

Section Effective Date: 29-Sep-2017

Cooperate with LevelBlue when LevelBlue Help Desk personnel notify Customer that mitigation will stop as the DDoS attack subsided. LevelBlue reserves the right to stop DDoS Defense mitigation and revert to standard routing when traffic patterns return to normal, pre-attack levels.

SD-6.3.3.3. Agnostic Service – Customer Responsibilities

Section Effective Date: 29-Sep-2017

For customers with Agnostic service, Customer will cooperate with LevelBlue when LevelBlue Help Desk personnel notify Customer that mitigation will stop as the DDoS attack subsided. LevelBlue reserves the right to revert to standard routing when traffic patterns return to normal, pre-attack levels should Customer not agree to stop mitigation.

SD-6.4. Annual Tests

Section Effective Date: 29-Sep-2017

Customer can request one limited test of the DDoS Defense Service once every calendar year. A test must be coordinated with the LevelBlue Operations team and will consist of LevelBlue generating a volume of data traffic that will exceed Customer-defined thresholds as measured on network detection devices. During the test, up to five (5) addresses can be tested. A test is

designed to simulate attack and to assess the systems for alerting Customer. Additionally, a test can confirm successful traffic mitigation as well as validate that valid traffic can be returned to the Customer site.

SD-6.5. Service Activation

Section Effective Date: 25-Jun-2015

LevelBlue provides Service Activation for the DDoS Defense Service. Service Activation consists of the following elements:

- Provisioning LevelBlue equipment used for monitoring of Customer IP address blocks
- Identifying access routers on which Customer traffic is located
- Exporting Customer traffic flow data from access routers to a DDoS Defense Portal platform for analysis
- Activating Customer on the DDoS Defense Portal

The Service Activation will occur after the above steps are complete. Billing will begin upon Service Activation.

SD-6.6. DDoS Defense Portal

Section Effective Date: 29-Sep-2017

Reports of the DDoS Defense Service are available to the Customer via the DDoS Defense Portal. Access to the DDoS Defense Portal is provided through the LevelBlue Threat Manager Portal, which can be accessed through LevelBlue BusinessDirect® or LevelBlue Business Center. The Customer is responsible for maintaining LevelBlue BusinessDirect® and LevelBlue Business Center Login IDs and appropriate access for individual users requiring access to the DDoS Defense Portal.

SD-6.7. Third Party ISP

Section Effective Date: 01-Aug-2013

Service mitigation is only provided on the LevelBlue Common Backbone ("CBB"). Detection and mitigation can only be supported with traffic that terminates on an LevelBlue-provided Internet circuit.

In order for LevelBlue to provide mitigation for traffic on a third party ISP network, the attack traffic will need to be rerouted to the LevelBlue CBB. Customer is responsible for understanding and coordinating the withdrawal of route advertisements from third party ISPs.

SD-6.8. Changes

Section Effective Date: 25-Jun-2015

If Customer is currently an LevelBlue Enterprise Hosting Customer and needs to make a change, either adding circuits or disconnecting circuits, Customer must advise its LevelBlue Sales Representative of such change so as not to negatively impact the DDoS Defense Service that Customer receives. Service Level Agreements will not apply if Customer fails to notify LevelBlue of such change(s).

SD-6.9. DDoS Defense Welcome Kit

Section Effective Date: 01-Aug-2013

LevelBlue will provide Customer with an LevelBlue DDoS Defense Welcome Kit, which includes an overview of the provisioning of the Service, FAQ's and other documentation.

SD-6.10. Customer Responsibilities

Section Effective Date: 05-May-2018

Customer shall:

- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to providing LevelBlue with the name(s) of a point of contact for the Service.
- Assure that only it or its designated Users will access the Service and that Customer and all Users will not share User IDs or other methods for accessing the Service with individuals who are not the designated Users of the Service. Customer further agrees to notify LevelBlue of the designated User of each User ID provided with the Service. Customer shall promptly notify LevelBlue of any changes to any of the designated Users assigned to the User ID.
- Not disclose, copy, disseminate, redistribute or publish any portion of the Service to any other party. Reproduction of the Service in any form or by any means is forbidden without

LevelBlue's written permission, including but not limited to: (a) information storage and retrieval systems; (b) use in any timesharing, service bureau, bulletin board or similar arrangement or public display; (c) posting any portion of the Service to any other online service (including bulletin boards or the Internet); or (d) sublicensing, leasing, selling, offering for sale or assigning the Service(s) to another entity or User;

- Assure that its and Users' use of the Service(s) will comply with written and electronic instructions for use of the DDoS Defense Portal;
- Be solely responsible for determining the configuration of and how and where to use the DDoS Defense Portal views and reporting features. The portal views and reporting features of the Services are intended to provide Customer with information that is helpful in optimizing and otherwise managing its network and the Service purchased from LevelBlue;
- Be the owner and controller of any data collected via these portal views and reporting features. LevelBlue shall be acting only as a data processor as to such information;
- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to, providing LevelBlue information regarding any changes to the Customer network, in order to assist LevelBlue in its analysis and examination of the Customer traffic flow data;
- Provide LevelBlue with a list of Customer IP addresses connected to the LevelBlue IP Backbone that Customer wishes to have subject to the DDoS Defense Service, and immediately notify LevelBlue of any additions or deletions to such list while Customer is receiving DDoS Defense Service;
- Provide LevelBlue with the names of at least three (3), but no more than one hundred (100) Customer points of contact and related contact information;
- Immediately notify LevelBlue of events that Customer becomes aware of that wo uld cause significant traffic pattern changes in the Customer network that is being monitored under the DDoS Service;
- Customer is solely responsible for the accuracy of all information provided to LevelBlue relating to the IP addresses Customer owns or controls;
- Submission of IP addresses to LevelBlue is Customer verification of ownership or control of the IP addresses; and
- Immediately notify LevelBlue if Customer believes their resources are under a DDoS attack.
- When using multi ISP solution including LevelBlue link(s), Customer is responsible to:
  - Ensure that the LevelBlue link is sized to support any additional traffic during the attack
  - Withdraw the super block advertisement(s) from other ISPs

SD-6.11. DDoS Defense – Agnostic Option

SD-6.11.1. Overview

Section Effective Date: 05-May-2018

The LevelBlue DDoS Defense Service - Agnostic Option can be provided to customers who rely on alternate Internet providers, other than LevelBlue, for their Internet access. Geographic restrictions on service availability may apply.

The Bandwidth Based, Proactive DDoS Defense service is available to support DDoS Defense – Agnostic configurations and is only available to qualifying Government entities and Education customers.

The DDoS Defense – Data Center Model service is available to support DDoS Defense – Agnostic configurations and is only available to qualifying reseller of LevelBlue for the protection of their own internet access links and not for purpose of further resale to their customers.

There are two components to the DDoS Defense Agnostic Option, including DDoS detection and mitigation, both of which use Generic Routing Encapsulation (GRE) tunnel technology. The DDoS Defense Agnostic Option helps protect against volumetric attack traffic before reaching the Customer site. DDoS Defense utilizes a network detection device, which examines Customer traffic flow data from the Customer site that is being protected. Upon detection, or Customer notification of a perceived DDoS Attack, LevelBlue can reroute traffic targeted at either an attacked host or an IP Address Block to the LevelBlue IP Backbone. Once rerouted to the LevelBlue IP Backbone, the traffic is directed to a shared Scrubbing device which then 'scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic. The DDoS Agnostic Option is designed to then pass valid traffic to the Customer site via a GRE tunnel. LevelBlue and the Customer will resume the normal routing of Customer traffic once LevelBlue determines the DDoS attack has subsided. The Customer will have access to reports on the attack and mitigation activity through a Customer-specific portal ("DDoS Defense Portal"). In addition, LevelBlue shall:

- During the first two (2) weeks following the DDoS Defense Agnostic Option Activation Date, examine Customer traffic flow data and analyze patterns within such data in order to baseline Customer traffic patterns to assist in determining when a DDoS attack is occurring;
- When LevelBlue believes that conditions so warrant; (a) issue Alert(s) to Customer about IP Threat(s) which shall direct Customer to the DDoS Defense Portal for further information; and/or (b) provide information via the DDoS Defense Portal to assist Customer in addressing and/or mitigating IP Threats;
- When LevelBlue believes a DDoS attack is occurring, notify Customer via email within fifteen (15) minutes, and where warranted, by telephone within twenty (20) minutes.
- Provide Customer access to reports on specific attacks and mitigation activity through an LevelBlue specific website provided to Customer; and
- Make available to Customer the Traffic Anomaly Detection analysis and Traffic Anomaly

Detection reports related to any DDoS Attacks on Customer during the period in which DDoS Defense Carrier Agnostic Option is provided to Customer. All reports are LevelBlue Proprietary Information and are subject to the terms and provisions of the Service Agreement.

SD-6.11.2. Traffic Anomaly Detection

Section Effective Date: 24-Feb-2014

LevelBlue uses Customer traffic flow data to detect traffic anomalies. This flow data is sourced from a Customer premise router and is directed to LevelBlue Anomaly Traffic Detection devices through a GRE tunnel.

Traffic Anomaly Detection has algorithms that run on a single detection portal. The algorithms look for “Misuse Anomalies” and “Profiled Anomalies”. Traffic Anomaly Detection, using these algorithms, is designed to detect anomalous traffic patterns that are considered malicious and to alert Customer that mitigation may be warranted.

SD-6.11.3. Detection Capabilities and Exclusions

Section Effective Date: 24-Feb-2014

Cross References

SD-6.2.1. Detection Capabilities and Exclusions

SD-6.11.4. DDoS Anomalies

Section Effective Date: 24-Feb-2014

Refer to the DDoS Anomalies Section, above. Cross References

SD-6.2.2. DDoS Anomalies

SD-6.11.5. Mitigation

Section Effective Date: 24-Feb-2014

Network Packet Scrubbing facilities utilize centralized DDoS mitigation devices to mitigate known malicious packets destined to the Customer network. Customer may choose between two options to divert traffic to the Scrubbing facilities: 1) DNS A-record change or 2) LevelBlue Direct Route Advertisement of Customer IP address block, via Border Gateway Protocol (BGP) direct route advertisement. In order to select the direct route advertisement option, Customer must own a Provider Independent IP Address Block of at least a size Class "C" or larger. Both options will reroute only the traffic targeted for the specific IP address or IP address block to one or more of the LevelBlue Scrubbing facilities. After the Scrubbing facilities mitigate the malicious content, traffic determined to be valid will be forwarded to the Customer through a GRE tunnel.

When the LevelBlue detection device identifies a volumetric attack and provides an Alert, the S/NOC will consult with the Customer before any mitigation is activated.

Mitigation duration on the Bandwidth Based, Proactive DDoS Defense service will be eight (8) hours.

SD-6.11.6. DNS A-record Change

Section Effective Date: 25-Jun-2015

When the DNS A-record option is selected, a limitation of four concurrent mitigations is enforced by LevelBlue. It should be noted that the A-record Change option is most applicable to HTTP/HTTPS.

Customer will actively work with LevelBlue to initiate activation of the DDoS Defense Carrier Agnostic Option mitigation by requesting a DNS A-record change to their DNS provider. Using this method, the following sequence of events will occur when mitigation is activated:

- Customer requests DNS A-record change from original IP address(es) to LevelBlue-provided IP address(es).

- Customer will request to their provider to black hole the original IP address of the attacked host(s)
- Policy routing on customer premises router will be required to return traffic through the GRE tunnel back to LevelBlue.
- LevelBlue advertises the LevelBlue-provided IP address(es) that DNS A-record(s) were changed to
- LevelBlue will initiate the DDoS mitigation
- LevelBlue will perform a Network Address Translation (NAT) on the destination IP address to allow flow of packets to the Customer server under attack.
- Clean traffic is delivered through pre-defined GRE tunnel to the Customer premise
- Return traffic is delivered through a pre-defined GRE tunnel to the LevelBlue scrubbing facility
- LevelBlue will perform a NAT on the source IP address of the return traffic packets to the LevelBlue- provided address before the packets are sent back to the valid user.

SD-6.11.7. Direct Route Advertisement via Border Gateway Protocol (BGP)

Section Effective Date: 24-Feb-2014

If Customer chooses the direct route advertisement method to mitigate DDoS attacks, Customer will be required to perform specific tasks in order for mitigation to occur. The following events will occur in the direct route advertisement option:

- Customer withdraws route advertisement of minimum Class “C” network block
- LevelBlue will begin advertising the customer Class “C” vi a BGP
- LevelBlue will initiate the DDoS mitigation
- Clean traffic is delivered to customer site through a pre-defined GRE tunnel

SD-6.11.8. Resumption to Normal Traffic Flow

Section Effective Date: 05-May-2018

When the DDoS attack subsides, LevelBlue and Customer will establish an agreed upon time to resume normal traffic flow. In order to resume normal traffic flow at the agreed upon time, both LevelBlue and Customer will perform the necessary steps to achieve such result.

Where Customer has subscribed to the Bandwidth Based, Proactive DDoS Defense service on their third party internet access links, if LevelBlue determines after eight (8) hours of mitigation that the attack is subsided, LevelBlue may initiate the return to normal traffic flow.

SD-6.11.9. DDoS Defense Service Agnostic Option Service Activation

Section Effective Date: 05-May-2018

LevelBlue provides Service Activation for the DDoS Defense Agnostic Option. Service Activation consists of the following elements:

- If DNS A-record option is used, LevelBlue will provide Customer with four IP addresses that will be used during attack mitigation
- Provisioning of LevelBlue equipment from two LevelBlue sites to be used for GRE tunnel establishment and for monitoring of Customer IP address blocks
- Providing Customer with GRE termination IP addresses
- Activating GRE tunnels
- Activating Customer on the DDoS Defense Portal

The Service Activation will occur after the above steps are complete. Billing will begin upon Service Activation.

SD-6.11.10. DDoS Defense Portal

Section Effective Date: 24-Feb-2014

Refer to the DDoS Defense Portal Section, above. Cross References

SD-6.6. DDoS Defense Portal

SD-6.11.11. Changes

Section Effective Date: 24-Feb-2014

Refer to Changes in the DDoS Defense Section, above.

Cross References

SD-6.8. Changes

SD-6.11.12. DDoS Defense Welcome Kit

Section Effective Date: 24-Feb-2014

Refer to DDoS Defense Welcome Kit Section, above.

Cross References

SD-6.9. DDoS Defense Welcome Kit

SD-6.11.13. Customer Responsibilities

Section Effective Date: 05-May-2018

Customer shall:

- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to providing LevelBlue with the name(s) of a point of contact for the Service.
- Assure that only it or its designated Users will access the Service and that Customer and all Users will not share User IDs or other methods for accessing the Service with individuals who are not the designated Users of the Service. Customer further agrees to notify LevelBlue of the designated User of each User ID provided with the Service. Customer shall promptly notify LevelBlue of any changes to any of the designated Users assigned to the User ID, not disclose, copy, disseminate, redistribute or publish any portion of the Service to any other party. Reproduction of the Service in any form or by any means is forbidden without LevelBlue's written permission, including but not limited to: (a) information storage and retrieval systems;
  (b) recordings and re-transmittals over any network (including any local area network); (c) use in any timesharing, service bureau, bulletin board or similar arrangement or public display; (d) posting any portion of the Service to any other online service (including bulletin boards or the Internet); or (e) sublicensing, leasing, selling, offering for sale or assigning the Service(s) to another entity or User;

- Assure that its and Users' use of the Service(s) will comply with written and electronic instructions for use of the DDoS Defense Portal;
- Be solely responsible for determining the configuration of and how and where to use the DDoS Defense Portal views and reporting features. The portal views and reporting features of the Services are intended to provide Customer with information that is helpful in optimizing and otherwise managing its network and the Service purchased from LevelBlue;
- Be the owner and controller of any data collected via these portal views and reporting features. LevelBlue shall be acting only as a data processor as to such information;
- Be responsible either for (a) taking all relevant procedural steps to ensure that viewing and using the portal views and reports is in compliance with applicable local laws and (b) ensuring that the portal views and reports are not used in countries where this is not permitted;
- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to, providing LevelBlue information regarding any changes to the Customer network, in order to assist LevelBlue in its analysis and examination of the Customer traffic flow date;

  Provide LevelBlue with a list of Customer IP addresses connected to the LevelBlue IP Backbone that Customer wishes to have subject to the DDoS Defense – Agnostic Service, and immediately notify LevelBlue of any additions or deletions to such list while Customer is receiving DDoS Defense – Agnostic Service;
- Provide LevelBlue with the names of at least three (3), but no more than one hundred (100) Customer points of contact and related contact information;
- Immediately notify LevelBlue of events that Customer becomes aware of that would cause significant traffic pattern changes in the Customer network that is being monitored under the DDoS Defense Service; and
- Immediately notify LevelBlue if Customer believes that its resources are under a DDoS attack.
- If DNS A-record change method is chosen:
  - Understand how to initiate a DNS A-record change with their DNS provider
  - Implement a recommended TTL value of 5 minutes or lower with their DNS provider
- If direct route advertisement method is chosen, understand how to initiate route advertisement withdrawal from their ISP
- Ensure Customer side of the Internet circuit is terminated by a router or a layer 3 switch. Customer should have administrative access to the equipment.
- Provide CPE that supports GRE tunnels, static or policy routing, and Cisco Netflow or JFLOW configuration.
- Have access to site router in order to configure GRE tunnel, routing, and Customer Flow Data export

- Maintain GRE tunnel configuration including routing and Customer Flow Data export
- Use a different network block for GRE tunnel termination from the network block of the hosts that are being protected.

Customer acknowledges and understands that if Customer does not fulfill its obligations or provide the necessary information as provided herein, then the DDoS Defense - Agnostic Service may be degraded or LevelBlue may not be able to provide the DDoS Defense – Agnostic Service to Customer.

SD-6.12. LevelBlue Reactive Distributed Denial of Defense Service (Reactive DDoS)

SD-6.12.1. Overview

Section Effective Date: 28-Feb-2017

The LevelBlue Reactive DDoS Defense Service ("Reactive DDoS Defense Service" or the "Service") may only be provided to ADI customers. Third party internet access solutions are not supported with LevelBlue Reactive DDoS Service.

The LevelBlue Reactive DDoS Defense Service includes the provisioning activity for Service Readiness and DDoS attack Mitigation Service Activation upon specific customer request. Mitigation takes place within LevelBlue's backbone and provides protection against the adverse effects of volumetric attack traffic before reaching the Customer site. Upon Customer notification of a perceived DDoS Attack, LevelBlue can reroute traffic, targeting up to 10 (ten)

hosts (ten /32 IP addresses), through the LevelBlue IP Backbone to a shared scrubbing or mitigation device which then applies filtering to the rerouted traffic to drop the suspected offending DDoS attack data packets. The Reactive DDoS Defense Service is designed to pass traffic deemed valid to the Customer access router. Mitigation will be in effect for a predetermined interval of 8 hours. At the end of the mitigation time period, LevelBlue will resume the normal routing of Customer traffic. Customer may request that LevelBlue re-start mitigation should the attack continue beyond 8 hours. The Customer will have access to reports on the attack and mitigation activity through a Customer-specific portal ("DDoS Defense Portal"). In addition, LevelBlue shall:

Provide Customer access to reports on specific attacks and mitigation activity through an LevelBlue specific website provided to Customer.

SD-6.12.2. Definition of DDoS Attacks

Section Effective Date: 12-Dec-2016

The LevelBlue Reactive DDoS Defense Service is designed to help protect against attacks that are volumetric in nature, regardless of attack size. A volumetric attack is defined as an attack that sends high volumes of traffic designed to over-utilize access lines, exhaust available bandwidth and eventually deny access for legitimate traffic. Volumetric attacks include those attacks listed in the Volumetric Attack Types and Description table set forth below. Volumetric attacks do not include: (i) application layer attacks (those that primarily target applications); (ii) SSL attacks (those aimed at exploiting the CPU intensive nature of encrypting and decrypting packets); and (iii) “low and slow” attacks (those that consume a high number of connections and can exhaust server resources).

Volumetric Attack Types and Descriptions	
Attack Type	**Description**
Spoofed	Sending packets with a forged source address
Malformed	Sending packets with abnormal bits or flags set
Floods	Sending high rates of legitimately formed packets
Null	Sending packets with no content or illegitimate protocol
Fragmented	Sending packet fragments that will never be completed
Brute Force	Sending packets that exceed defined flow rates threshold

SD-6.12.3. Mitigation

Section Effective Date: 12-Dec-2016

Network Packet Scrubbing facilities utilize centralized DDoS mitigation devices to filter out known malicious packets which are destined through the Customer network to the public IP addresses registered with the LevelBlue Reactive DDoS Defense service. A predefined BGP speaker will instruct a facility to re-route Customer traffic to one or more Scrubbing facilities. The BGP speaker will advertise the specific /32 address or addresses that are being attacked. This will reroute only that traffic targeted for the specific IP addresses to one or more of the LevelBlue Scrubbing facilities. After the Scrubbing facilities filter out the malicious content, traffic determined to be valid will be forwarded back to the Customer through a path that includes an

LevelBlue Scrubbing facilities. After the Scrubbing facilities filter out the malicious content, traffic determined to be valid will be forwarded back to the Customer through a path that includes a

LevelBlue managed virtual private network (“VPN”). Customer is not required to purchase VPN services from LevelBlue for the LevelBlue Reactive DDoS Defense service mitigation to take place.

SD-6.12.3.1. Mitigation Triggering Method

Section Effective Date: 12-Dec-2016

LevelBlue will activate the LevelBlue Reactive DDoS Defense Service mitigation for an 8-hour period via BGP speaker within the LevelBlue network upon the Customer requesting the activation of the Service by notifying LevelBlue via the toll-free number provided in the Welcome Package or by sending an email to threat@att.com.

SD-6.12.3.2. Resumption to Normal Traffic Flow

Section Effective Date: 12-Dec-2016

Mitigation will automatically stop after the eight (8) hour period following the start of mitigation. LevelBlue will notify Customer by email approximately one hour before the stop that mitigation will be concluded and normal traffic flow will be restored shortly. Upon mitigation stop, LevelBlue will send another email confirming the stoppage. Should Customer determine that further mitigation is necessary, Customer may notify LevelBlue to continue or re-start mitigation. A new 8 hour mitigation process will be started and mitigation charges will apply per rates specified in the LevelBlue Reactive DDoS Defense Price Schedule in effect.

SD-6.12.3.3. Customer Responsibilities

Section Effective Date: 12-Dec-2016

Customer must notify LevelBlue to start the LevelBlue Reactive DDoS Defense mitigation process. Using the DDoS Defense portal, Customer is responsible for keeping the list of registered IP addresses as well as the list of Authorized Users updated. Customer is required to notify LevelBlue Account Representatives when Customer is adding IP addresses on any circuits not previously identified to LevelBlue. LevelBlue reserves the right to refuse to provide mitigation services on public IP addresses that are made available to the public by Customer via circuits not covered by the executed Pricing Schedule or appear to be in excess of the number of circuits listed on the Customer’s monthly service invoice.

Upon discovery of IP addresses being registered with the LevelBlue Reactive DDoS Defense Service that are advertised through more circuits than what is reflected on the monthly invoice, LevelBlue reserves the right to charge for such additional circuits in order to be consistent with the number of circuits being provided with the LevelBlue Reactive DDoS Defense Service.

SD-6.12.4. LevelBlue Reactive DDoS Defense Mitigation Tests

Section Effective Date: 12-Dec-2016

Customer can request a test of the LevelBlue Reactive DDoS Defense Service at their convenience. Standard mitigation charges will apply. A test may be performed by notifying the LevelBlue Operations team in advance and will consist of LevelBlue generating a volume of data traffic that will mimic a DDoS attack against up to 10 (ten) registered public IP addresses on Customer's network. A test may confirm successful traffic mitigation as well as validate that legitimate traffic can be returned to the Customer site.

SD-6.12.5. LevelBlue Reactive DDoS Defense Service Activation for Billing and Mitigation Service Activation

Section Effective Date: 12-Dec-2016

Customer's billing begins upon Service Activation. Service Activation begins upon service readiness. Service Readiness means the following:

- Based on information provided by Customer, LevelBlue has registered the list of public IP addresses, in the LevelBlue Reactive DDoS Defense support systems in order to allow LevelBlue to activate mitigation upon Customer notification.
- Based on information provided by Customer, LevelBlue has provisioned Customer's Authorized Users on the DDoS Defense Portal.

LevelBlue Reactive DDoS Defense Service Activation will begin upon order completion and notification to Customer by email that the steps above have been completed.

LevelBlue begins preparation for Mitigation Service Activation for the LevelBlue Reactive DDoS Defense Service upon specific Customer request when calling the LevelBlue Threat

Management team toll- free number or by sending an email to threat@att.com. Mitigation Service Activation consists of the following prerequisite steps by LevelBlue:

- Authenticating the caller as Authorized User to request mitigation services for the account
- Identifying LevelBlue access routers on which Customer traffic is located
- Verifying the presence of a DDoS attack

Mitigation Service Activation will occur upon Customer's express request for Mitigation Services and after the authentication, identification, and verification steps above are complete.

SD-6.12.6. DDoS Defense Portal

Section Effective Date: 29-Sep-2017

Reports of the LevelBlue Reactive DDoS Defense Service are available to Customer via the DDoS Defense Portal. Access to the DDoS Defense Portal is provided through the LevelBlue Threat Manager Portal, which can be accessed through LevelBlue BusinessDirect®. Customer is responsible for maintaining LevelBlue BusinessDirect® Login IDs and appropriate access for individual users requiring access to the DDoS Defense Portal.

SD-6.12.7. Third Party ISP

Section Effective Date: 05-May-2018

LevelBlue Reactive DDoS Defense Service is only available with LevelBlue Dedicated Internet (ADI) Service.

SD-6.12.8. Changes

Section Effective Date: 05-May-2018

If Customer is currently an LevelBlue Dedicated Internet Customer and needs to make a change, either adding circuits or disconnecting circuits, Customer must advise its LevelBlue Sales Representative of such change so as not to negatively impact the LevelBlue Reactive DDoS Defense Service. Any Service Level Agreements will not apply if Customer fails to notify LevelBlue of such change(s).

SD-6.12.9. Customer Responsibilities

Customer shall:

Section Effective Date: 12-Dec-2016

- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to providing LevelBlue with the name(s) of a point of contact for the Service.
- Assure that only it or its designated Users will access the Service. Customer and all Users will not share User IDs or other methods for accessing the Service with individuals who are not the designated Users of the Service. Customer further agrees to notify LevelBlue of the designated User of each User ID provided with the Service. Customer shall promptly notify LevelBlue of any changes to any of the designated Users assigned to the User ID.
- Not disclose, copy, disseminate, redistribute or publish any portion of the Service, inc luding but not limited to documentation or service publications, to any other party. Reproduction of the Service in any form or by any means is forbidden without LevelBlue’s written permission, including but not limited to: (a) information storage and retrieva l systems; (b) use in any timesharing, service bureau, bulletin board or similar arrangement or public display; (c) posting any portion of the Service to any other online service (including bulletin boards or the Internet); or (d) sublicensing, leasing, selling, offering for sale or assigning the Service(s) to another entity or User;
- Assure that its and Users’ use of the Service(s) will comply with written and electronic instructions for use of the DDoS Defense Portal;
- Be solely responsible for determining the configuration of and how and where to use the DDoS Defense Portal views and reporting features.
- Be the owner and controller of any data collected via these portal views and reporting features. LevelBlue shall be acting only as a data processor as to such information;
- Cooperate with LevelBlue in all aspects of the Service, including, but not limited to, providing LevelBlue information regarding any changes to the Customer network, in order to assist LevelBlue in its analysis and examination of the Customer traffic flow data;
- Provide LevelBlue with a list of Customer IP addresses connected to the LevelBlue IP Backbone that Customer wishes to have subject to the LevelBlue Reactive DDoS Defense Service, and immediately notify LevelBlue via the DDoS Defense portal of any additions or deletions to such list while Customer is receiving LevelBlue Reactive DDoS Defense Service;

- Provide to LevelBlue and maintain via the DDoS Defense portal the names of up to ten (10) Customer points of contact and related contact information.

SD-7. Glossary

Section Effective Date: 30-Mar-2021

Glossary	
Term	**Definition**
Alerts	Means notification via email of IP Traffic Anomalies or IP Threats that, in the opinion of LevelBlue, require immediate action by the customer to mitigate or to monitor for possible defensive action.
LevelBlue Help Desk	Means the single point of contact for Customer Tier 1 Help Desk(s) regarding the Services contained in this Service Guide. The LevelBlue Help Desk will provide the following functions: (i) Manage In-Scope Troubles to Resolution; (ii) Manage the dispatch of LevelBlue personnel to Resolve In- Scope Troubles (iii) perform Soft MACDs; and (iv) Manage the dispatch of LevelBlue personnel to perform Hard MACDs.
"LevelBlue Common Backbone ("CBB") or LevelBlue IP Backbone"	Means the LevelBlue owned and operated Internet Protocol (IP) infrastructure and consists of all LevelBlue Internet Service Points of Presence ("POPs"), the telecommunications hardware and facilities that interconnect all wiring within them, and the physical plant that surrounds them. The LevelBlue IP Backbone does not include Customer Premise Equipment or the dedicated access facility connecting Customer Premises to the LevelBlue IP Backbone.
"LevelBlue DDoS Defense Welcome Kit"	Means an informational document (which in no way amends of modifies this Amendment or the Services) which has been sent to Customer and contains information related to the Services, including: Service Provisioning Requirements; DDoS Defense Service Overview; Using the DDoS Defense Portal; and LevelBlue DDoS Defense Frequently Asked Questions (FAQs).
LevelBlue Observed Holidays	Means the holidays as defined in the General Provisions.
Attack Mitigation Equipment	Means the denial of service detection equipment and the data scrubbing equipment located on LevelBlue's premises and used in connection with the DDoS Defense Service provided to Customer by LevelBlue.

Glossary	
Term	**Definition**
"Attacked Host"	Means Customer's computer equipment, such as a server with a public IP address, residing inside Customer's network that is being targeted by a DDoS Attack.
"Automatic Mitigation"	Means that when LevelBlue's detection device identifies a Volumetric Attack and provides an Alert to the S/NOC and Customer, the work center will trigger the start of mitigation prior to notifying Customer.
Border Gateway Protocol (BGP)	Means the routing information distribution protocol that is designed to define who can talk to whom using multi-protocol extensions and community attributes.
Business Days	Monday through Friday.
Change Order Process	Means the process by which changes to the Service are requested by Customer and processed by LevelBlue.
Connectivity (Front-end and Back-end)	Is how Customer Servers, housed in an IDC, are connected to the Internet and to Customer Premises. Front-end connectivity is how access to the Internet is provided. Back-end Connectivity is Optional as the administrative functions may be performed across the front-end (Internet) connection.
Content	Means information made available, displayed or transmitted (including, without limitation, information made available by means of an HTML "hot link", a third party posting or similar means) in connection with a Service, including all trademarks, service marks and domain names contained therein, Customer and User data, and the contents of any bulletin boards or chat forums, and, all updates, upgrades, modifications and other versions of any of the foregoing.
Customer Signature	Means a signature created to meet a single Customer's requirement Normal Vendor releases signatures on a bi-weekly basis at least. Sensors will be updated in 3-5 business days at no additional charge to Customer.
Distributed Denial of Service Attacks or DDoS Attacks	Means a distributed denial of service attack, similar to those defined in DDoS Defense Service Level Agreements and Objectives Section of this Service Guide, directed toward Customer's IP addresses connected to the LevelBlue IP Backbone that, in LevelBlue's reasonable judgment, causes LevelBlue to believe that Customer's network may be compromised by being inundated with nefarious or bogus data traffic, thereby denying service to Customer's systems connected to LevelBlue's IP Backbone.

Glossary	
Term	**Definition**
"DDoS Defense Portal"	A portal that is accessed via the following link using Customer's existing BusinessDirect credentials: LevelBlue BusinessDirect Portal: http://www.businessdirect.att.com/ Click on the LevelBlue Security Center ICON located in the bottom left hand corner of your LevelBlue BusinessDirect Portal landing screen. Once in the LevelBlue Security Center the DDOS portal can be accessed as follows: 1) Select the My Services icon; and 2) Select the DDoS Defense icon.
"DDoS Defense Service", LevelBlue DDoS Defense Service – Carrier Agnostic Option, Reactive DDoS Defense Service or "Service"	Means the LevelBlue Distributed Denial of Defense Service, or LevelBlue Reactive DDoS Defense Service as described herein and as further elaborated in the Service Guide in the appropriate sections. In the event of a conflict, the provisions of this Amendment shall control as it pertains to the description of the DDoS Defense Service, LevelBlue DDoS Defense Service - Carrier Agnostic Option or the Reactive DDoS Defense Service.
DDoS Mitigation	DDoS mitigation occurs when one or more IP addresses are rerouted to one or more LevelBlue DDoS Defense Scrubbing facilities. A mitigation hour is defined as a sixty (60) minute period when DDoS mitigation is occurring. Mitigation hours within a billing cycle are calculated by aggregating the number of hours, or partial hours, of DDoS mitigation within a billing cycle.
Demilitarized Zone (DMZ)	Means the buffer space outside of both your own and your opponent's direct control. In modern data networks, a Demilitarized Zone is generally an Internet-accessible web, data, or application server that is outside your trusted internal network for use by business partners, Customers, etc. but is not part of the public Internet. DMZ's generally allow gated access through passwords or user registration.
Event Notification	Means the communications between LevelBlue and Customer that relate to identification, Management, and resolution of events, including Outages and any other event that may affect the Service.
Forwarding Information Base (FIB) tables	Means the tables that contain information on proper user identification data.
FTP	Means File Transfer Protocol.
GCSC	Means LevelBlue's Global Customer Support Center.
Host	Means a single IP Address
In Scope Troubles	Means problems or malfunctions that are LevelBlue's responsibility to resolve as described in this Service Guide.

Glossary	
Term	**Definition**
Install	Means to physically set up for use or service in an IDC, typically associated with HW and SW.
Internet Control Message Protocol (ICMP)	Means the TCP/IP protocol used to report network errors and to determine whether a computer is available on the network. The ping utility uses ICMP.
Internet Data Center (IDC)	Means is the specific LevelBlue facility where Customer Space, HW or Service is located or provided.
IP Threat	Refers to data traffic across the LevelBlue IP Backbone such as viruses, buffer overloads, DDoS attacks or other traffic that may potentially disable, interrupt or degrade single or multiple connection(s) to the LevelBlue IP Backbone.
IP Traffic Anomaly	Refers to data traffic across the LevelBlue IP Backbone that has a pattern or characteristic recognized by LevelBlue as warranting investigation.
Lightweight Directory Access Protocol (LDAP)	Means the emerging Internet standard for directory services. It is based on the earlier ISO X.500 Directory Access Protocol (DAP) standard, but simplifies that standard considerably, allowing LDAP to be more efficient, straightforward, and easier to implement.
Local Area Network (LAN)	Means a group of computers and associated devices that share a common communications line and typically share resources.
Location	Is each physical customer access location. For example protection of sites at a data center in New York with OC3 access and protection of sites at a data center in Kansas City with separate physical OC3 access would be two locations to be protected.
Mail Exchanger (MX)	Means the domain name server mail exchange record to enable the Secure E-Mail Gateway Service.
MACD (Move, Add, Change, Delete)	Means either Hard or Soft. A Hard MACD is a single HW move, add, change, delete, deactivate, decommission, de-install or disconnect performed by ATT on a single Component Managed by LevelBlue. A Soft MACD is a single logical move, add, change or delete to the on a Component Managed by LevelBlue.
LevelBlue Dedicated Internet (ADI)	Means the Internet service provided by and managed by LevelBlue.
Manual Mitigation	Means when the LevelBlue's detection device identifies a Volumetric Attack and provides an Alert, the S/NOC will consult with Customer before any mitigation is activated.

Glossary	
Term	**Definition**
Manual Mitigation	Means when the LevelBlue's detection device identifies a Volumetric Attack and provides an Alert, the S/NOC will consult with Customer before any mitigation is activated.
LevelBlue Dedicated Internet+ (ADI+)	Means the LevelBlue Dedicated Internet plus service.
Misuse Anomalies	Are traffic patterns that are of known denial of service signatures including high rates of protocol fragments, ICMP, SYNs, RSTs and Nulls (No payload).
Mitigation Service Activation	For the DDoS Defense Service it consists of the following tasks: • Provisioning Supplier Hardware used for monitoring of Customer's IP address blocks • Identifying access routers on which Customer's traffic is located • Exporting Customer's traffic flow data from access routers to a DDoS Defense Portal platform for analysis • Activating Customer on the DDoS Defense Portal For LevelBlue Reactive DDoS Defense, Mitigation Service Activation consists of the following prerequisite steps by LevelBlue: • Authenticating the caller as Authorized User to request mitigation services for the account • Identifying LevelBlue access routers on which Customer traffic is located • Verifying the presence of a DDoS attack • Mitigation Service Activation will occur upon Customer's express request for Mitigation Services and after the authentication, identification and verification steps above are complete.
MPLS	Means multi-protocol label switching.
Network Address Translation (NAT)	Means hiding of IP addresses in an internal network by presenting one IP address to the outside world. It performs the translation back and forth.
Network Detection Device	Means a hardware component of the LevelBlue owned and managed DDoS Defense platform that accepts incoming traffic samples and generates Alerts when it detects Misuse Anomalies or Profiled Anomalies.
Network Elements	Means the Components that make up Customer network and may include items such as Switches, FWs and routers to the Web Servers. They could vary from Client to Client.

Glossary	
Term	Definition
Outage	Means an interruption of the LevelBlue Secure Network Gateway Services, excluding planned maintenance schedules.
Permanent Virtual Circuit (PVC)	Is a virtual circuit established for repeated/continuous use between the same data terminal equipment (DTE). In a PVC, the long-term association is identical to the data transfer phase of a virtual call. Permanent virtual circuits eliminate the need for repeated call set-up and clearing.
Personal Data”	Means Data belonging to Customer and its Users which information when taken on its own or in conjunction with other data processed would enable to identify a person.
Pricing Schedule	Means the document that contains the services that Customers can order under the agreement as more fully described in this Service Guide and the prices Customer will pay for such Services.
Proactive Operations Support and Troubleshooting	Means LevelBlue will perform tasks that give LevelBlue the ability to take preventive measures to limit the frequency of service Interruptions.
Profiled Anomalies	Are traffic patterns that have exceeded the learned baselines that have been generated by Supplier based on a sliding two week interval of Customer traffic flow. Profiled thresholds are set at certain levels of Packets Per Second (“PPS”) or Bits Per Second (“BPS”) in excess of the pre-determined baseline.
Profiling	Means the analysis completed to determine what alarms are important for a specific Customer as it relates to the Active IDS/IPS – Advanced Optional Components. This profiling is based on Customer’s security policy and network infrastructure.
RADIUS	Means the type of server used to support the provision of LevelBlue’s Secure Network Gateway Service.
Redundancy	Means the provision of alternate paths to minimize the potential for failure or vulnerabilities.
Policy Rules	Means the Customer-defined parameters, thresholds, boundaries or limitations of a specific Customer’s security policy.
S/NOC	Is LevelBlue’s Security Network Operations Center.

Glossary	
Term	**Definition**
Sales Order	Means the document which details specific provisioning related information for an order, including applicable options and features. The initial Sales Order is typically completed by LevelBlue after the execution of this Agreement, in consultation with Customer. Subsequent Sales Orders are typically completed by the parties to effectuate additional Service Component orders. All Sales Orders shall be subject to the terms of this Online Ordering Agreement. Terms and conditions on any non-LevelBlue order form shall not apply.
Scrubbing	Means activity performed by equipment used by LevelBlue to isolate and mitigate a DDoS Attack.
Security Policy	Means the set of methods and procedures associated with a particular enterprise's security requirements.
Secure Network (SecNet)	Means the separate Security Policy setup for a unique VLAN or MPLS VPN.
Server	Means the computer program that provides services to Users and/or the computer that runs the Server program.
Service Activation Date	Means the date the Service becomes available for Customer use and when billing will begin.
Service Guide	Means the standard LevelBlue service descriptions and other provisions as revised by LevelBlue from time to time, relating to Service offered under this Attachment. The Service Guide is located at http://www.att.com/abs/serviceguide or at such other address as LevelBlue may specify by posting or email notice.
Service Level Agreement (SLA)	Means the agreement between Customer and LevelBlue to Manage processes, procedures and Equipment pertaining to Customer Service which will reflect a level of performance for LevelBlue to achieve.
Service Portal	Refers to the website where Customers and User(s) access the Internet Protect Service
Service Readiness – LevelBlue Reactive DDoS Defense	Based on information provided by Customer, LevelBlue has registered the list of public IP addresses, in the LevelBlue Reactive DDoS Defense support systems in order to allow LevelBlue to activate mitigation upon Customer notification. Based on information provided by Customer, LevelBlue has provisioned Customer's Authorized Users on the DDoS Defense Portal.
Shared Scrubbing Device	Means LevelBlue Hardware used to isolate and mitigate a DDoS Attack while providing Service to multiple LevelBlue customers.
SMTP	Means Simple Mail Transport Protocol.

Glossary	
Term	**Definition**
Switch	Means the device that opens or closes circuits, completes, or breaks an electrical path, or selects paths or circuits.
TCP/IP is a Transmission Control Protocol/Internet Protocol	Means the common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide inter-networks. TCP and IP are the two best-known protocols in the suite. TCP corresponds to Layer 4 (the transport layer) of the OSI reference model. It provides reliable transmission of data. IP corresponds to Layer 3 (the network layer) of the OSI reference model and provides connectionless datagram service.
Telnet	Means the command and program used to login from one Internet site to another. The telnet command/program gets you to the login: prompt of another host.
Tier I Help Desk	Means the function performed by Customer or a third party contracted to Customer to perform initial call receipt, fault validation, or fault isolation. Customer agrees to instruct End-Users to contact the Tier I Help Desk regarding all troubles or questions pertaining to LevelBlue's Secure Network Gateway Services. Customer support personnel will make reasonable efforts to Resolve Troubles before they are referred to LevelBlue for Resolution.
Tier II Help Desk	Means the function performed by LevelBlue to receive, Manage, and Resolve Trouble Tickets in accordance with this Service Guide.
Traffic Anomalies	Means anomalous traffic patterns that are considered malicious by LevelBlue and are used to alert Customer that mitigation may be warranted.
Traffic Anomaly Detection	Means LevelBlue's identification of Traffic Anomalies directed at a defined set of Customer IP addresses on the LevelBlue Backbone.
Trouble Ticket	Means the work order that LevelBlue uses to identify In-Scope and Out of Scope Troubles and to Manage the In-Scope Troubles through Resolution.
Tuning	Means the disabling or setting specific thresholds for signatures to eliminate alarms which have no value to Customer's security policy or infrastructure.
UDP is a User Datagram Protocol	Means one of the protocols for data transfer that is part of the eTCP/IP suite of protocols. UDP is a stateless protocol in that UDP makes no provision for acknowledgement of packets received.

Glossary	
Term	**Definition**
Volumetric Attack	Means an attack that sends high volumes of traffic designed to over utilize bandwidth and eventually deny access for legitimate users. Volumetric Attacks include those listed in the Volumetric Attack Types and Description table below. Volumetric Attacks do not include: (i) application layer attacks (those that primarily target applications); (ii) SSL attacks (those aimed at exploiting the CPU intensive nature of encrypting and decrypting packets); and (iii) "low and slow" attacks (those that consume a high number of connections and can exhaust server resources).
VPN Access	Means the access to the Staging Server via the Virtual Private Network (VPN), which is a connection with state-of-the-art security features over the Internet, and only Customer Authorized Users can access them.

Service Level Agreements (SLAs)

SLA-1. LevelBlue Secure E-Mail Gateway Service Level Agreement

SLA-1.1. Network Uptime SLA — 99.999%

Section Effective Date: 30-Apr-2012

Description: The percentage of time in a calendar month that the network is able to receive and process email messages.

- Includes emergency and planned maintenance

SLA Remedy		
Description	**% of Service Availability per Calendar Month**	**Service Credit**
SEG Network Uptime SLA	<99.999%	25%
	<99.0%	50%
	<98%	100%

SLA-1.2. Email Latency of 1 Minute or Less

Section Effective Date: 30-Apr-2012

Email delivery is defined as the elapsed time from when an email enters the SEG network to when the delivery attempt is first made.

Email delivery latency is the average of total email delivery time measured in minutes over a calendar month. Email delivery time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.

Email delivery latency applies only to legitimate business email (non-bulk email) delivered to valid email accounts.

This SLA shall not apply to:

- Delivery of email to quarantine or archive
- Email in deferral queues
- Denial of Service attacks (DoS)
- Email loops

SLA		
SLA	**Average Email Delivery Time**	**Service Credit**
SEG Latency SLA	Greater than 1 minute	25% of the Monthly Recurring Charges
	Greater than 4 minutes	50% of the Monthly Recurring Charges
	Greater than 10 minutes	100% of the Monthly Recurring Charges

SLA-2. LevelBlue Secure E-Mail Gateway Service Level Agreement

SLA-2.1. Definitions

Section Effective Date: 25-Jul-2015

- “Filter” means to detect and block or quarantine all email messages with Viruses that (i) match an available virus signature; (ii) are identifiable by industry standard anti-virus engine heuristics; or (iii) are propagated through registered attachment types.
- “Infection” means if an inbound email to a Customer Mailbox is delivered with a Virus, or if an outbound email from a Customer Mailbox is processed through the Security Services with a Virus without being quarantined.
- “Scheduled Maintenance Window" means the window during which weekly scheduled maintenance of the Products may be performed. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.
- "Emergency Maintenance" means any time outside of Scheduled Maintenance Window that Supplier is required to apply urgent patches or fixes, or undertake other urgent maintenance activities.
- "System Availability" means the percentage of total time during which a Service is available to Customer, excluding Scheduled Maintenance Window and Emergency Maintenance.
- “Service Credit” means the percentage of the monthly Subscription Fees paid or payable for the Products that is awarded to Customer for a validated claim associated with that portion of the Products related to breach of the applicable SLA during that month.
- “Virus” means a binary or executable code whose purpose is to gather information from the infected host (such as trojans), change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host’s system resources.

SLA-2.2. Service Credits

Section Effective Date: 25-Jul-2015

In any given month Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming Products.

SLA-2.3. SLA Claims

Section Effective Date: 25-Jul-2015

Customer must notify LevelBlue Support within thirty (30) business days from date of incident it first believes entitles it to receive a remedy under any one of the SLAs set forth below. If requested by LevelBlue, Customer will provide LevelBlue a live copy of the applicable email with the original Supplier headers (complete and untampered with) for analysis. Failure to comply with these reporting requirements may forfeit Customer right to receive a remedy in connection with an SLA.

For all claims subject to validation by LevelBlue, LevelBlue will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. LevelBlue shall make information used to validate a SLA claim available for auditing by Customer at Customer request.

In the event that more than one aspect of a Service is affected by the same root cause, the single SLA applicable to such Service product of LevelBlue's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

SLA-2.4. Exclusions

Section Effective Date: 25-Jul-2015

Customer may not have any remedies, or may only have a partial remedy, under any SLA to the extent any SLA claim is due to: (i) use of the Service product outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Supplier's data center and not under the direct control of Supplier; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; or (iv) a Force Majeure Event.

SLA-2.5. SEG Security Services SLAs

Section Effective Date: 25-Jul-2015

The following SLAs apply to the Security Services.

SLA-2.5.1. Filtering System Availability SLA

Section Effective Date: 25-Jul-2015

- LevelBlue warrants at least 99.999% System Availability for the filtering and delivery of email during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance.
- Remedy. If the email System Availability is less than 99.999%, and if Customer is in material compliance with its obligations under the Agreement and this SLA, LevelBlue will provide Customer with a Service Credit for the month in which the failure to meet the email System Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of Email System Availability per Calendar Month	Service Credit
< 99.999%	25%
< 99. 0%	50%
< 98.0%	100%

SLA-2.6. Email Delivery SLA

Section Effective Date: 25-Jul-2015

LevelBlue warrants that the average of Email Delivery (as defined below) times, as measured in minutes over a calendar month, will be one (1) minute or less.

For purposes of this SLA “Email Delivery” is defined as the elapsed time from when a business email enters the Security Services network to when it exits the Security Services network.

This SLA applies only to legitimate business email (i.e. not to any spam email as defined under applicable law for commercial messages including the CAN-SPAM Act) delivered to valid Mailbox accounts that are contracted for the Security Services.

Customer shall not have any remedies under this SLA to the extent any SLA claim hereunder is due to (i) delivery of email to quarantine; (ii) email in deferral queues; or (iii) email loops.

Remedy. If in any calendar month the Email Delivery SLA is not met and if Customer is in material compliance with its obligations under the Agreement and this SLA, LevelBlue will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

Average Email Delivery Time	Service Credit
> 1 minute	25%
> 5 minutes	50%
> 10 minutes	100%

SLA-2.7. Virus Filtering SLA

Section Effective Date: 25-Jul-2015

- LevelBlue warrants that the Security Services will Filter (as defined below) 100% of all Viruses (as defined below) contained in an inbound email to a Customer Mailbox for which a Security Services subscription has been purchased.
- LevelBlue warrants that the Security Services will Filter 100% of all Viruses contained in an outbound email from a Customer Mailbox for which a Security Services subscription has been purchased.
- For purposes of this SLA, the following definitions shall apply:
- This SLA does not apply to (i) text messages that use fraudulent claims to deceive the Customer and/or prompt the Customer to action (such as phishing); (ii) a binary or executable code installed or run by an end user that gathers information for sales and marketing purposes (such as spyware); (iii) a virus that has been detected and has been cleaned by other virus scanning products; (iv) an ineffective or inactive virus contained in a bounced email; (v) a Virus-infected email that is quarantined by the Service but is subsequently delivered to an end user or administrator by such end user or administrator;
- (vi) emails containing attachments that are password protected, encrypted or otherwise under an end user’s control; or (vii) any action by a LevelBlue end user or administrator that results in deliberate self-infection.
- Customer will not be eligible to receive a remedy under this SLA if Customer (i) is not subscribing to the corresponding anti-virus Security Services modules for Customer Mailboxes for which a Security Services subscription has been purchased; (ii) has not enabled full virus protection for all Customer Mailboxes for which a Security Services subscription has been purchased; and (iii) does not provide LevelBlue with conclusive

written evidence that the Virus was caused by an email that passed through the Security Services network.

- Remedy. If a validated Infection occurs in any calendar month, and if Customer is in material compliance with its obligations under the Agreement and this SLA, LevelBlue will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

Number of validated infections that occurred during a month	Service Credit
1 to 3 Validated Occurrences	25%
4 to 5 Validated Occurrences	50%
> 5 Validated Occurrences	100%

SLA-2.8. Spam Inbound Effectiveness SLA

Section Effective Date: 24-Oct-2015

- LevelBlue warrants that the Security Services will detect 99% of inbound spam in each calendar month.
- This SLA does not apply to false negatives to invalid Mailboxes.
- LevelBlue will make a good faith estimation of the spam capture rate based on the regular and prompt submission to the Security Services support center of all false negatives to report spam missed by Security Services.
- LevelBlue will estimate the percentage of spam detected by the Security Services by dividing the number of spam emails identified by the Security Services as recorded in the Security Services report logs by all spam emails sent to Customer. Supplier will estimate all spam emails sent to Customer by adding the number of spam messages (false negatives) missed by the Security Services and reported to the Security Services support team to the number of spam emails detected by the Security Services.

Remedy. If the Security Services detects less than 99% of inbound spam in any calendar month, and if Customer is in material compliance with its obligations under the Agreement and this SLA, LevelBlue will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

If monthly average spam capture rate is	Service Credit
< 99%	25%
< 98%	50%
< 95%	100%

SLA-2.9. Spam Outbound Effectiveness SLA

Section Effective Date: 24-Oct-2015

- LevelBlue warrants that the Security Services will detect 95% of outbound spam in each calendar month.
- LevelBlue will make a good faith estimation of the spam capture rate based on the regular and prompt submission to the Security Services support center of all false negatives to report spam missed by Security Services.
- LevelBlue will estimate the percentage of spam detected by the Security Services by dividing the number of outbound spam emails identified by the Security Services as recorded in the Security Services report logs by all outbound emails sent from the Customer through the Security Services. LevelBlue will calculate the total number of emails sent from the Customer through the Security Services in each calendar month.
- Remedy. If the Security Services detects less than 95% of outbound spam in any calendar month, and if Customer is in material compliance with its obligations under the Agreement and this SLA, LevelBlue will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

If monthly average spam capture rate is	Service Credit
< 95%	25%
< 93%	50%

< 90%	100%

- Exclusion. The Spam Outbound Effectiveness SLA does not apply to the Small and Medium Business Advanced, Advanced Plus, and Premium Services.

SLA-2.10. False Positive SLA

Section Effective Date: 24-Oct-2015

- LevelBlue warrants that the ratio of legitimate business email incorrectly identified as spam by the Security Services to all email processed by the Security Services for Customer in any calendar month will not be greater than 1:350,000.
- LevelBlue will make a good faith estimation of the false positive ratio based on evidence timely supplied by Customer.
- This SLA does not apply to (i) spam email (as defined as under applicable law for commercial messages including the CAN-SPAM Act under U.S. federal law), personal email from an individual end user of Customer outside of the scope of such individual end user's employment or independent contractor services for the benefit of Customer, pornographic email; or (ii) emails blocked by a policy rule, reputation filtering, or SMTP connection filtering.
- Remedy. If LevelBlue does not meet this SLA in any calendar month and if Customer is in material compliance with its obligations under the Agreement and this SLA, LevelBlue will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

False Positive Ratio in a Calendar Month	Service Credit
> 1:350,000	25%
> 1:50,000	50%
> 1:1,000	100%

SLA-3. Service Level Objectives

SLA-3.1. LevelBlue Managed Firewall Service — Network-Based Option 1 and Option 2 Service Level Objectives

Section Effective Date: 14-Nov-2015

LevelBlue will observe the following objectives when delivering MFS-NB:

- MACD turnaround time of 24 hours
- Service Availability – 99.99%

Service Level Objectives ("SLO") are indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

SLA-4. LevelBlue Web Security Service Level Objectives

SLA-4.1. SLO Availability

Section Effective Date: 01-Aug-2013

LevelBlue will observe the following Service Level Objectives when delivering WSS:

- Provisioning Intervals - MACD turnaround time of 24 hours
- MTTR is 4 hours for service to be turned up once ticket is submitted in AOTS
- MTTR for vendor call out is 8 hours.

Service Level Objectives ("SLO") are indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

SLA-4.2. SLA Availability

Section Effective Date: 30-Apr-2012

LevelBlue warrants that the LevelBlue Network will process and deliver web requests 99.999% of the total hours during every month LevelBlue's Customers use the Services when averaged across all available LevelBlue data centers. The Availability Warranty applies only to Downtime due in whole or in part to LevelBlue's inability to provide service to LevelBlue's Customers which are not attributable in whole or in part to the events described in Section SLA Limitations below.

Failure of the WSS to meet the SLA may entitle Customer to receive credits, as indicated below. Service Level Objectives ("SLO") are indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

LevelBlue reserves the right to change or modify the terms and conditions or discontinue this SLA program at any time without notice.

The SLA applies only to the LevelBlue Web Security Service specified in the applicable SLA description and to no other services or options.

SLA-4.3. SLA Claim Process

Section Effective Date: 30-Apr-2012

- The SLA will take effect upon the Service Activation Date of WSS.
- The monthly service charge that will be the subject of the credit for the WSS will be the monthly charge for the Service.

SLA-4.4. SLA Limitations

Section Effective Date: 30-Apr-2012

- LevelBlue will only be responsible for Availability during normal circumstances. The SLA does not apply and no credits will be issued in the event of fire, explosion, lightning, power surges or failures, strikes or labor disputes, water, acts of God, the elements, war, civil disturbances, acts of civil or military authorities, fuel or energy shortages, acts or omissions of suppliers or other causes beyond LevelBlue's control, whether or not similar to the foregoing, and acts outside LevelBlue's control as described in the LevelBlue Master Agreement; or
- Local or international regulatory laws or ethical (ethical meaning conforming to accepted professional standards of conduct) issues that limit or prevent the ability of LevelBlue or the Local Service Provider to offer or comply with these SLAs; or
- Customer's lack of availability to respond to incidents that require Customer's participation for resolution.
- Customer's failure to provide required site power for necessary equipment, including the IP SEC termination device (if this option was provisioned) or
- Any service failure which is due to Customer owned equipment residing on Customer's premises (unless such equipment was provided by LevelBlue or its authorized contractors), or failure or unavailability of any of the elements of the services provided by Customer or under Customer's responsibility including, but not limited to, power supply,

internal wiring, proper environmental conditions, or router connected telephone line for problem determination.

- Any service failure or interruption caused by a third party (including LevelBlue subcontractors, suppliers and Local Service Providers) not recognizing or delivering upon an LevelBlue request to reroute a customer's traffic to LevelBlue's designated facilities for the purpose of scrubbing the traffic
- Scheduled maintenance. LevelBlue will perform maintenance during the scheduled maintenance window of 1 a.m. U.S. Eastern Standard Time (06:00 UTC- Coordinated Universal Time) to 5 a.m. U.S. Eastern Standard Time (10:00 UTC). LevelBlue may perform maintenance outside of the scheduled maintenance window upon an advanced prior notice to the customer. LevelBlue reserves the right to provide emergency maintenance, or to repair services, at any time and when LevelBlue determines needed, and in such case LevelBlue will notify affected customers as soon as is. All claims are subject to review and verification by LevelBlue.

SLA-4.5. SLA Credits

Section Effective Date: 23-Aug-2013

Credit amounts are calculated based on billed charges, exclusive of any applicable taxes charged to the customer or collected by LevelBlue.

The SLA credits may not under any circumstances exceed (either alone or in combination with other credits issued to Customer) in any given month, one hundred (100) percent of the LevelBlue Web Security Service monthly charge.

The SLA is Customer's sole and exclusive remedy for any Outages, failures of the Service or LevelBlue otherwise not meeting the Service Level Agreements outlined herein.

SLA-4.5.1. Monthly Service Availability and Monthly Reimbursement Percentage

Section Effective Date: 30-Apr-2012

Monthly Service Availability and Percentage Reimbursement	
Monthly Service Availability	**Credit Percentage**
99.999-99.99%	10%
99.98-99.5%	20%
99.49-99.0%	30%
98.99-98.5%	40%

98.49-98.0%	50%
97.99-97.5%	60%
97.49-97.0%	70%
96.99-96.5%	80%
96.49-96.0%	90%
95.99-95.5%	100%

SLA-4.5.2. SLA Claim Process

Section Effective Date: 12-Aug-2015

1. Customer must proactively submit an SLA claim in writing and request the credit within 30 days of the incident in order for this SLA to take effect, or forfeit their right to the claim. All credit requests should be sent via an email addressed to pm075k@att.com or such other email address identified by LevelBlue.
2. Please include the Trouble Ticket number with your request. LevelBlue will attempt to acknowledge all requests for credit within ten (10) business days of receipt and inform customer via email or U.S. Postal Mail within thirty (30) days whether the request is approved or denied.
3. Trouble tickets, where Service Availability cannot be verified with LevelBlue's standard diagnostic procedures, do not count towards this SLA.

SLA-5. DDoS Defense or LevelBlue Reactive DDoS Defense Service Level Agreements and Objectives

SLA-5.1. Overview

Section Effective Date: 25-Jun-2015

Failure of the DDoS Defense Service to meet a Service Level Agreement (“SLA”) described below may entitle Customer to receive a credit, as indicated below.

A Service Level Objective (“SLO”) is indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

SLA-5.2. Service Level Agreement Rules, Regulations and Limitations

Section Effective Date: 06-Oct-2015

Customer must proactively submit an SLA claim in writing and request the credit within 30 days of the initiation of mitigation of the volumetric attack in question in order for this SLA to take effect or Customer will forfeit its right to the claim. All credit requests should be sent via email to threat@att.com with a copy to the LevelBlue Account Team. Customer shall include any Trouble Ticket number associated with its credit request. LevelBlue will attempt to acknowledge all requests for credit within ten (10) business days of receipt and inform Customer via email whether the request is approved or denied.

- Trouble tickets, where the Time to Mitigate cannot be verified with LevelBlue's standard diagnostic procedures, do not count towards these SLAs.
- The SLAs will take effect upon the Service Activation Date of the DDoS Defense Service.
- LevelBlue will only be responsible for a DDoS related attack in which the offending traffic can be routed to the LevelBlue access link with Customer. In the event that the Customer traffic (or any portion thereof) is not routed through LevelBlue, an SLA will not apply. Additionally, the SLAs do not apply and no credits will be issues in the event of:
  - Fire, explosion, lightning, power surges or failures, strikes or labor disputes, water, acts of God, the elements, war, civil disturbances, acts of civil or military authorities, fuel or energy shortages, acts or omissions of suppliers or other causes beyond LevelBlue's control, whether or not similar to the foregoing, and acts outside LevelBlue's control as described in the LevelBlue Master Agreement; or
  - Local or international regulatory laws or ethical (ethical meaning conforming to accepted professional standards of conduct) issues that limit or prevent the ability of LevelBlue or the Local Service Provider ("LSP") to offer or comply with these SLAs; or
  - Customer's lack of availability to respond to incidents that require Customer's participation for resolution.
  - Any service failure which is due to Customer owned equipment residing on Customer's premises (unless such equipment was provided by LevelBlue or its authorized contractors), or failure or unavailability of any of the elements of the services provided by Customer or under Customer's responsibility including, but not limited to, power supply, internal wiring, proper environmental conditions, or router connected telephone line for problem determination.
  - Any service failure or interruption caused by a third party (including LevelBlue subcontractors, suppliers and LSP) not recognizing or delivering upon an

LevelBlue request to reroute a customer's traffic to LevelBlue's designated facilities for the purpose of scrubbing the traffic.

  - Scheduled maintenance. LevelBlue maintains Scrubbing centers around the world. LevelBlue will periodically perform maintenance using local time of the Scrubbing center from 00:00-06:00. LevelBlue may perform maintenance outside of the scheduled maintenance window upon an advanced prior notice to the Customer. LevelBlue reserves the right to provide emergency maintenance, or to repair services, at any time and when LevelBlue determines needed, and in such case LevelBlue will notify affected customers as soon as is reasonably practicable. SLAs do not apply during any of the maintenance periods.

- All claims are subject to review and verification by LevelBlue.
- LevelBlue reserves the right to change or modify the terms and conditions or discontinue this SLA program at any time without notice.
- Credit amounts are calculated based on billed charges, exclusive of any applicable taxes charge to the Customer or collected by LevelBlue.
- The SLA credits may not under any circumstances exceed (either alone or in combination with other credits issued to Customer) in any given month, one hundred (100) percent of the monthly charges for the DDoS Defense Service. The SLAs are the sole and exclusive remedy for Customer for any outages, failures of the Service or LevelBlue otherwise not meeting the SLAs outlined herein.

SLA-5.3. Time To Mitigate Service Level Agreement SLA-5.3.1. Service Level Measure

Section Effective Date: 05-May-2018

As part of the DDoS Defense Service, Bandwidth Based Proactive DDoS Defense Service and DDoS Defense – Data Center Model Service, LevelBlue provides the following Service Level Agreements:

- With pre-authorized mitigation: mitigation begins within 30 minutes of a validated DDoS attack after receiving the Alert.
- With manual mitigation: mitigation begins within 30 minutes of Customer informing the S/NOC of a request to initiate mitigation.
- If Customer chooses Platform Initiated Mitigation: mitigation begins within 5 minutes of the relevant alert. After validation following the SLA claim process, SLA credits will only be granted in situations where the system did not trigger mitigation even though the

thresholds were properly set. Mitigation that did not trigger due to incorrectly defined customer requirements or thresholds unknown to LevelBlue will not qualify.

If in any calendar month LevelBlue fails to meet the service level measures set forth above in connection with one or more volumetric attacks, and subject to the limitations set forth in the Service Level Agreement Rules, Regulations and Limitations section of this Service Guide, Customer may be eligible for a credit equal to a percentage of the recurring charge for the month in question, based on the Time to Mitigate table below.

Time to Mitigate for Pre-Authorized Mitigation and Manual Mitigation	
Time to Mitigate (in minutes)	**Percentage of Monthly Charge Credit**
31-60	25%
61-120	50%
121+	100%

Time to Mitigate for Platform Initiated Mitigation	
Time to Mitigate (in minutes)	**Percentage of Monthly Charge Credit**
6-30	25%
31-60	50%
61+	100%

Alert generation will be determined by using the log or report information from the Attack Mitigation Equipment, or a trouble ticket or event logged with the S/NOC.

Customer request to the S/NOC to initiate mitigation will be determined based on the creation of a trouble ticket with the S/NOC.

The beginning of mitigation will be determined by using the log or report information from the Attack Mitigation Equipment.

SLA-5.3.2. Service Level Measure — LevelBlue Reactive DDoS Defense Service

Section Effective Date: 12-Dec-2016

As part of the LevelBlue Reactive DDoS Defense Service, LevelBlue provides the following Service Level Objective (SLO):

- After Customer calls in to request the activation of mitigation services LevelBlue will start mitigation within 30 minutes of verifying the presence of a DDoS attack against any of the Customer's registered public IP addresses.

SLA-5.4. Attack Notification Service Level Objective

Section Effective Date: 12-Dec-2016

It is LevelBlue's objective that Customer will receive an Alert of a volumetric DDoS attack by email within 15 minutes of attack identification.

This SLO does not apply to the LevelBlue Reactive DDoS Defense Service.

Pricing (P)

P-1. LevelBlue Secure Network Gateway Pricing

Section Effective Date: 30-Apr-2012

LevelBlue Secure Network Gateway rates and charges are as specified in Customer's Pricing Schedule.

In the Pricing Schedule, the terms "Activation" and "Activating Charge" are used synonymously with the terms "installation" and "installation charge" and the terms "non-recurring charge" and "one-time charge" are synonymous.

Charges for Secure Network Gateway features are billed at fixed monthly recurring charges based on the features ordered plus any installation charges.

P-1.1. Billing

Section Effective Date: 09-Dec-2015

Secure Network Gateway Services are billable as of the Service Activation Date and are billed in advance and/or arrears depending on the Service.

P-2. LevelBlue Distributed Denial of Service (DDoS) Defense – Pricing P-2.1. Usage Options

Section Effective Date: 05-May-2018

The DDoS Defense Service has Service levels that provide different numbers of included monthly mitigation hours set forth in Customer Service Agreement.

P-2.1.1. Monthly Rate Plan Hours

Section Effective Date: 19-Sep-2018

Pursuant to technical and administrative requirements, a separate Hourly Rate Plan is to be setup with each individual DDoS Defense instance allocated to the customer. Customers with multi-regional presence must have a DDoS Defense instance per region. A separate DDoS Defense instance is also required every time the Customer desires to apply a different mitigation method highlighted in Methods of Triggering Section of this Service Guide, or separate notification list for alerts generated by the DDoS Defense service monitoring different customer resources even if this is requested within the same geographical region.

Monthly Mitigation hours relate to the number of monthly mitigation hours set forth in the Customer Pricing Schedule. Monthly Mitigation hours are calculated as follows:

- If a customer has separate mitigation events occurring on multiple monitored IP addresses at separate times throughout a month, the separate mitigation hours will be aggregated on a calendar month basis.
- If Customer has mitigation events occurring simultaneously on multiple monitored IP addresses, the events will be considered as a singular event and will be recorded as such for billing purposes.
- In either situation above, hours exceeding the chosen mitigation hour tier will be billed on an hourly basis as Overage.

P-2.2. Mitigation Hours

Section Effective Date: 19-Sep-2018

DDoS mitigation occurs when one or more IP addresses are rerouted to one or more LevelBlue DDoS Defense scrubbing facilities. A mitigation hour is defined as a sixty (60) minute period when DDoS mitigation is occurring. Mitigation hours within a billing cycle are calculated by aggregating the number of hours, or partial hours, of DDoS mitigation within a billing cycle. The mitigation hours are based upon the time necessary to mitigate an attack. The maximum number of mitigation hours possible within a billing cycle are calculated by multiplying the number of days in the month by 24 hours per day.

P-2.3. Number of Monitored IP Addresses

Section Effective Date: 19-Sep-2018

Monitored IP addresses are individual IP addresses and blocks of IP addresses that are configured to be monitored by the DDoS Defense Service through detection algorithms. Some DDoS Defense Service Levels may have restrictions on the number of IP Addresses that can be monitored. Customer should consult the applicable Service Agreement for specific information about any such restrictions.

P-2.4. Upgrades to Adjust High Overage Charges under the LevelBlue DDoS Defense Service

Section Effective Date: 19-Sep-2018

If a Customer exceeds its contracted number of mitigation hours, as set forth in Customer's Pricing Schedule, within a billing cycle, overage charges will be applied. Overage charges will qualify for an adjustment for that billing cycle if Customer upgrades to the next higher Monthly Mitigation plan. To exercise the option to upgrade, Customer must notify LevelBlue seven (7) days prior to the last business day within the month of the received invoice which reflected the overage charge. If an upgrade is not selected as previously set forth herein, overage charges will be due and owing as set forth on Customer's received invoice. Once Customer reaches the highest Service Level, as specified in Customer's Pricing Schedule in effect for the Service, no further upgrades are available.

P-3. LevelBlue Reactive Distributed Denial of Service Defense (R-DDoS) — Pricing P-3.1. Usage Options for the LevelBlue Reactive DDoS Defense Service

Section Effective Date: 28-Feb-2017

The LevelBlue Reactive DDoS Defense Service has tiers of service components corresponding with Customer's ADI links for which it charges a monthly fee reflected in Customer's Pricing Schedule. The required amount of LevelBlue Reactive DDoS Defense service components from the proper tier have to be ordered by Customer so LevelBlue may provide support for the same number of ADI circuits and corresponding, up to ten (10) in total, public IP addresses on the customer's network. During a month, LevelBlue will charge the Mitigation Instance fee based on the number of requests it receives from Customer for Mitigation Service Activation. The duration of any mitigation instance is eight (8) hours during which LevelBlue may provide Mitigation Services for up to a total of ten (10) previously registered public IP addresses of Customer advertised through ADI circuits.

P-3.2. Mitigation Hours for the LevelBlue Reactive DDoS Defense Service

Section Effective Date: 12-Dec-2016

DDoS mitigation occurs when one or more IP addresses are rerouted to LevelBlue Reactive DDoS Defense scrubbing facilities as specifically requested by the Customer after calling LevelBlue Threat Management. As defined for the LevelBlue Reactive DDoS Defense service, a mitigation instance lasts eight (8) hours. A mitigation hour is defined as a sixty (60) minute period when DDoS mitigation is occurring. All mitigation instances starting before the end of the final day in the month will be reflected in the bill for that month.

P-3.3. Number of Registered IP Addresses for LevelBlue Reactive DDoS Defense Service

Section Effective Date: 12-Dec-2016

Registered IP addresses are individual (/32) host IP addresses that are stored in LevelBlue systems and are available for viewing and editing by Customer through the DDoS Defense portal. Under the LevelBlue Reactive DDoS Defense service, the maximum number of supported individual IP addresses (/32 addresses or host addresses) is ten (10).

P-3.4. Upgrades from for the LevelBlue Reactive DDoS Defense Service

Section Effective Date: 12-Dec-2016

While under contract for the LevelBlue Reactive DDoS Defense service should Customer requirements change warranting a higher level of service, LevelBlue will support a migration event to the DDoS Defense service. Customer is required to contact the supporting Account Team to initiate the migration through the means of executing a contract document containing the DDoS Defense service details.

P-4. Bandwidth Based Proactive DDoS Defense Service — Pricing

Section Effective Date: 05-May-2018

The Bandwidth Based Proactive DDoS Defense Service pricing is based on the number and size of the corresponding internet access links. It is charged monthly as set forth in the Customer's Service Agreement.

P-4.1. IP Address Monitoring

Section Effective Date: 05-May-2018

Refer to the Number of Monitored IP Addresses for LevelBlue DDoS Defense Service Section, above.

Cross References

SD-6.3.1. Methods of Triggering

P-4.2. Mitigation

Section Effective Date: 05-May-2018

DDoS mitigation begins when one or more IP addresses are rerouted to one or more LevelBlue DDoS Defense scrubbing facilities.

P-5. DDoS Defense — Data Center Model — Pricing

P-5.1. IP Address Monitoring

Section Effective Date: 05-May-2018

Customer will be charged for monitoring as set forth in Service Agreement.

P-5.2. Mitigation

Section Effective Date: 05-May-2018

DDoS mitigation begins when one or more IP addresses are rerouted to one or more LevelBlue DDoS Defense scrubbing facilities. A mitigation hour is defined as a sixty (60) minute period when DDoS mitigation is occurring. Mitigation hours within a billing cycle are calculated by aggregating the number of hours, or partial hours, of DDoS mitigation within a billing cycle. The mitigation hours are based upon the time necessary to mitigate an attack. The maximum number of mitigation hours possible within a billing cycle are calculated by multiplying the number of days in the month by 24 hours per day. If customer has several mitigations in-process, Customer will be billed for the total hours of each individual mitigation unless the Service Agreement states otherwise.

P-6. MFS-NB service for AT&T NetBond®

P-6.1. MFS-NB Service for AT&T NetBond — Billing

Section Effective Date: 08-Apr-2016

Billing for MFS-NB service for AT&T NetBond is separate and apart from billing for AT&T NetBond service which is subject to the AT&T NetBond Pricing Schedule.

The MFS-NB Service for AT&T NetBond is billed as monthly recurring charges for:

- Firewall service level (Primary or Enhanced)
- Firewall Minimum Bandwidth Commitment (MBC) per Virtual Network Connection (VNC)
- Firewall Overage usage (VNC Capacity Overage) for calculated usage over the

Minimum Bandwidth Commitment (MBC).

P-6.1.1. Virtual Network Connections — Calculation of Charges

Section Effective Date: 08-Apr-2016

At the beginning of each calendar month, LevelBlue will calculate monthly VNC firewall charges as described in the Pricing Schedule. After creation of a VNC, firewall charges apply until deletion of the VNC by the Customer. Proration applies for any VNC created after the first day of the calendar month. Monthly Recurring Charges and Overage Charges are billed in arrears.

P-6.1.2. Minimum Bandwidth Commitment

Section Effective Date: 08-Apr-2016

The applicable monthly recurring charge for the last firewall MBC selected for a VNC by the Customer prior to the end of the billing month is charged.

P-6.1.3. VNC Capacity Overage

Section Effective Date: 08-Apr-2016

A VNC Capacity Overage firewall charge is applied if measured firewall usage exceeds the MBC during the calendar month. Firewall usage is measured as follows:

Usage is measured in megabits per second (Mbps) for a VNC during a billing month as follows:

- The aggregate total of all bits transmitted across the VNC (for all VLANs on a VNC) is measured, separately for each direction (inbound and outbound), for each five minute period during the month.
- Each measured aggregate total of bits transmitted across the VNC during a five minute period is divided by 300 seconds to obtain a bandwidth measurement in bits per second.
- All 5 minute periods in the month are ranked in order and compared to determine the 95th percentile. Separate calculations are performed for inbound and outbound measurements, to determine the 95th percentile measurement for each category.
- The largest 95th percentile (inbound or outbound) is selected as the measured usage for the monthly billing period.
- The selected measurement is divided by 1,000,000 to obtain the measured usage, expressed in Mbps.

If the measured firewall usage (in Mbps) exceeds the selected MBC for the billing month, then the measured usage exceeding the MBC is multiplied by 1,000 to convert to Kbps and the VNC

Overage Charge for the selected MBC in the LevelBlue MSF-NB for AT&T NetBond Pricing Schedule Rate Table is applied.

Country-Specific Provisions

CSP-1. Indonesia

CSP-1.1. Billing and Payment Currency – Indonesia

Section Effective Date: 01-Jul-2015

Effective July 1, 2015, pursuant to Bank Indonesia issued Regulation No. 17/3/PBI/2015 on the Mandatory Use of Rupiah within the Territory of the Republic of Indonesia, all transactions conducted in Indonesia will be quoted, priced and invoiced in Indonesia Rupiah (IDR).

Charges for local Customers with existing Services in Indonesia with LevelBlue on July 1, 2015 who are currently billed in US Dollars (USD) will be billed in Indonesian Rupiah after July 1, 2015. The conversion rate upon which these billings will be calculated will be the spot exchange rate for USD/IDR published by Bloomberg L.P. - New York Composite – 5:30 PM US Eastern time on June 30, 2015.

CSP-2. Turkey

CSP-2.1. Billing – BusinessMail Web-based Invoicing – Turkey

Section Effective Date: 15-Mar-2016

Customer agrees that LevelBlue may deliver invoices to Customer through submission to the Turkey Ministry of Finance (MOF) Web-based Billing portal. Customers must register with the Ministry of Finance at https://mportal.kamusm.gov.tr/bp/mm.go prior to receiving and issuing electronic invoices (eInvoices). Customer will log onto the MOF portal to view their monthly LevelBlue eInvoice or can retrieve eInvoices using a Government MOF approved, Integrator application. Customer must provide LevelBlue with the local company name, company Tax Registration Number and Tax Office. Customer will be responsible for logging onto the MOF portal or using an integrator application to obtain the monthly invoice. Customer agrees that

Customer will be deemed to have received each invoice as of the date the invoice is made first available by LevelBlue and that Customer's failure to access any invoice shall not relieve, waive or delay Customer's obligation to remit payment to LevelBlue. Customer must provide LevelBlue with 45 days' prior written notice of any change affecting Customer's designated billing by e-mail at arcustomer@emea.att.com or telephone (caller paid) +44 20 34 505 751.