SERVICE DESCRIPTION

Managed Next Generation Firewall (NGFW)

Service Description Overview

- The Next Generation Firewall (NGFW) Service is a multifunction security offering, consolidated in a single appliance available as a hardware device or a virtual appliance on the customer premises, and remotely managed by Trustwave as a managed service. The Managed NGFW service provides perimeter security as part of an overall defense in depth strategy. The NGFW Device consolidates the following functionality:
- Firewall – Stateful firewall with NAT support.
- Intrusion Prevention System (NGFW) – Intrusion Prevention System (IPS) with a focused signature library. The IPS functionality is placed in detection mode by default and prevention signatures can be enabled by clients via the change request process.
- Gateway Anti-Virus– For web and email protection and Gateway Anti-Spam – For email protection.
- VPN & Network DMZ segments – support for one (1) site-to-site (S2S) VPN connection and configuration of one (1) local network DMZ segment.
- Web URL Whitelist/Blacklist support – restriction of or allowance to specific web sites by internal users based purely on a whitelist (allowed) or blacklist (disallowed). For more granular controls and functionality, consider optional web content filtering.

Base Features of Service

- The Managed NGFW service includes access to the TrustKeeper Client Portal to track provisioning progress; Access to the 24x7 Security Event and Security Alert reporting available in the security activity area; and access to Change and support requests creation and management.
- Initial baselining and tuning of the Managed NGFW Device(s), policies and rulesets based on review of Client's network and bandwidth requirements;
- 24x7 system management, 24x7 cloud log monitoring with Reporting and access to Log Data.
- Security Updates and Product Updates for Managed NGFW Device(s).

Provisioning and Implementation

Provisioning and Implementation

- The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with the Client to implement the Managed NGFW Service. Please

see the Trustwave Provisioning Guide for additional details on the service implementation.

- Configure the Managed NGFW Device(s) to ensure that normal day-to-day device operations are working properly and all supported capabilities are able to be managed by the SOC in a manner that allows Trustwave to meet service responsibilities and SLA's for the Managed NGFW service; and
- The Managed NGFW service is deemed to be delivered and operational when the SOC is able to view and has management control of the Managed NGFW Device(s) and
- The Client has access to the TrustKeeper Client Portal to view Log Data, Log Events, Alerts and reports.

Device and environment assessment

- Trustwave provisioning engineers work with the Client to help ensure optimal placement and configuration, including assessment of the completeness of the Client's responses to the Provisioning Questionnaire and Client provided information and Trustwave confirmation with the Client of the Client's NGFW system environment, policies and rulesets; and
- Assessment of the configuration of the Managed NGFW Device(s) to determine if current version and features are consistent with Trustwave supported device requirements.

Device configuration

- Trustwave provisioning will work with the Client to verify that the Managed NGFW Device(s) are integrated into the Trustwave Platform, in a "supported state", confirming any Product Updates required to the Managed NGFW Device(s) required to meet Trustwave's supported device requirements;
- That the Managed NGFW Device(s) communicate with Trustwave Platform for log data collection, device management and control;
- An active secure connection between the Trustwave Platform and the Managed NGFW Device(s);
- Client has completed a comprehensive test plan to review all impacted Client systems associated with the Managed NGFW Device(s) and/or Managed NGFW service.

Device tuning

- Provisioning will review and work with the Client to tune and update the configured security policies, in the Managed NGFW Device(s) to an approved state for Trustwave standard operations, in accordance with the following criteria:
- If the device is new to the Client environment, the device will be configured in accordance with the initial provisioning process and then monitored to ensure correct operation of the Managed NGFW Device(s). Fine-tuning of firewall and rulesets will continue until steady state operation has been achieved.
- If the Managed NGFW Device(s) is an existing Client device and already configured based on the Client's existing policy, that policy will be monitored and recommendations made for fine-tuning.
- Once the configuration is optimized, the baselining period ends and the Managed NGFW Device(s) are prepared for transition to Trustwave standard SOC operations, for monitoring and management.

TrustKeeper Client Portal

The TrustKeeper Client Portal allows the Client to view security data providing a current security posture of the Client's environment to the extent possible with services provided by Trustwave. The available features and functionality of the TrustKeeper Client Portal set out below may differ depending on the relevant Trustwave managed security service acquired by the Client. The Trustkeeper Portal allows clients to:

- Review current security events and alerts of Client's Trustwave-monitored network(s), as well as historical data;
- Create and track support tickets and status of Client change requests to equipment installed on Client's premises or within the Client's environment; and

- Provides a method for the client to securely communicate with the Trustwave MSS provisioning and SOC personnel and Access device configuration and status information;
- Allows for the Upload documentation and security policies;
- Track Progress of the service rollout.

Trustwave Responsibilities

- Navigate the Client through the provisioning process until the SOC has ongoing management control of the Managed NGFW Device(s).
- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to the Managed NGFW Device(s) and operating environment as necessary to complete the provisioning process.
- Supply and deliver the Managed NGFW Device(s) if applicable.
- Create a Client account in the TrustKeeper Client Portal and verify that client has access to portal.
- Assess, configure and baseline the Managed NGFW Device(s) based on information and instructions provided by Client.
- Provide applicable user guides, introduce and review the Client's usage and understanding of the TrustKeeper Client Portal and implement the applicable support process and procedures.
- Verify that the Managed NGFW Device(s) are functioning according to the service delivery design; and Managed NGFW Device(s) is generating Log Data, Log Events and Log Alerts and visible to the Trustwave Platform.

Client Responsibilities

- For virtual deployments, customer will provide the virtual deployment environment, including the hypervisor, OS of the hypervisor, and OS of the virtual machine for deployment and will provide all requisite version information to Trustwave provisioning engineers prior to provisioning.
- Accurately complete the Provisioning Questionnaire and respond to requests from the provisioning team when establishing contact and collecting the Provisioning Questionnaire.
- Make available an onsite resource capable of installation of the Managed NGFW Device(s) and troubleshooting and Client environment.
- Provide remote access to on premise infrastructure to accommodate configuration of any Managed NGFW Device(s).
- Provide appropriate credentialed access to Trustwave, to the Managed NGFW Device(s).
- Provide and maintain a secure connection between the Managed NGFW Device(s) and the Trustwave Platform, which is compatible with available Trustwave connection standards.
- Develop and complete a comprehensive test plan to review all impacted customer systems associated with the provisioned Managed NGFW Device(s) prior to commencement of the Managed NGFW Device(s) tuning activities referred to in this service description.
- Read and confirm the Client's understanding all provided user guides and documentation and Participate in and confirm the Client's understanding of the processes explained during the welcome call.
- Procure valid licenses and maintenance contracts for Managed Client owned NGFW Device(s) and all relevant NGFW configuration data.
- Review Security Event and Security Alert activity in the TrustKeeper Client Portal.
- Adhere to Trustwave's recommended security practices with respect to the NGFW Device and service.

    - Client acknowledges that:

- The Trustwave provisioning, management and threat analysis services are performed remotely. Any on-

site provisioning or support services required by the Client would be acquired separately as a Trustwave consulting service;

- Trustwave is not responsible for delays in provisioning due to delays or inaccurate Provisioning Questionnaire responses and Client provided information;
- The consolidated features and functionality of the NGFW Device(s) may not include all of the functionality and features of equivalent standalone appliance or services.
- Failure to implement and comply with Trustwave recommended security practices, may adversely impact the operation and functionality of the Managed NGFW Device(s) and the Managed NGFW Service.
- It has made its own enquiries as to the available features and functionality of the NGFW Device(s) and the suitability of the Managed NGFW service to meet the Client's requirements.
- Client will not have access to the Managed NGFW Device(s).

System Management

- The Managed NGFW service includes the ongoing configuration, health monitoring and provision of Product Updates and Security Updates to the Managed NGFW Device(s). These management features ensure that the Managed NGFW Device(s) are performing their function within the Client environment as designed.
- The Trustwave SOC manages the Managed NGFW Device(s) to ensure that the Managed NGFW Device(s) are active and tracks the version of firmware or software that is active on the Managed NGFW Device(s); and applies Product Updates and Security Updates to the Managed NGFW Device(s).

Health status monitoring

- The health status-monitoring feature of the Managed NGFW Service, monitors the network availability of the Managed NGFW Device(s) to ensure they are visible to the Trustwave Platform.
- Managed NGFW Device(s) are monitored to detect when these devices are no longer showing as active within the Trustwave Platform. This includes initial steps taken to assess the cause of the offline status of the relevant device and remediate the issue if possible.
- The SOC analysts will contact the Client's technical contact or other designated contact to notify the Client if remediation steps available to Trustwave are not successful.
- The notifications sent to the Client regarding the device status will be provided within the time requirements specified in the SLA.
- For Trustwave owned NGFW devices, the SOC analyst will act on behalf of the Client to contact the Managed NGFW System Device third party vendors to activate an RMA process and provide remote assistance, support and configuration, in respect of any repaired or replaced Managed NGFW Device(s).
- For client owned NGFW devices, the SOC analyst will notify the Client when a Client owned NGFW fails and needs to be replaced. Client is responsible to contact their third party vendor to activate an RMA process. Trustwave will provide remote assistance, support and configuration, in respect of any repaired or replaced Client owned Managed NGFW Device(s).

Product and Security Updates

- The Trustwave SOC will provide Product Updates and Security Updates and apply those updates to the Managed NGFW Device(s). The Trustwave SOC will also monitor the availability of third party vendor Product Updates and Security Updates and apply those updates to the Client owned Managed NGFW Device(s) being managed by Trustwave.
- Product Updates and Security Updates are assessed by the SOC to determine the priority of the update and the potential impact to the Managed NGFW Device(s) and the related functionality associated with the changes provided in the update.

- When a Product Update or Security Updates becomes available, a Ticket will be created and assigned to the Client by the Trustwave SOC;
- Product Updates and Security Updates available under the relevant valid Managed NGFW Device(s) application license or maintenance contract will be scheduled with the Client for implementation;
- The Trustwave SOC will give consideration to accommodate the Client's preferred maintenance window and apply threat protection features with the least disruption to the Managed NGFW Device(s), as possible. The Trustwave SOC will implement the relevant Product Updates and Security Updates within timeframe required depending on priority, to ensure that the Managed NGFW Device(s) are operating, and the Managed NGFW Service provided as designed.
- Security and Product Updates
    - All Security Updates and Product Updates for Managed NGFW Device(s) software will be completed during version upgrades;
    - Product Updates that include only bug fixes will be applied to the Managed NGFW Device(s) only when applicable to that device

Trustwave responsibilities

- Maintain management connection to the Managed NGFW Device(s) and Monitor the Managed NGFW Device(s) to ensure their active online status and that they are available.
- Notify Client within SLA timeframe if management connection is unavailable and cannot be restored by Trustwave
- For Trustwave owned NGFW devices, manage the vendor support and maintenance contracts applicable to the NGFW Device(s) to identify available Product Updates and provide remote assistance, support and configuration, in respect of any repaired or replaced Managed NGFW Device(s).
- Apply Security Updates and Product Updates as they are made available by the vendor and are applicable to Managed NGFW Device(s) and within timeframe required depending on the relevant update's priority.
- Create a Managed NGFW Service Ticket and schedule the Product Update, Security Update or rule update with the Client.
- Attempt to resolve any connectivity or system issues identified in order to return the device to a steady state of operation.

Client responsibilities

- Maintain and procure necessary renewals of valid vendor software licenses and maintenance contracts applicable to the Client owned Managed NGFW Device(s).
- For Client owned NGFW devices, provide Trustwave technicians access to 3rd party vendor portals to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of the Client for management, maintenance and Support purposes. Trustwave SOC will act as a verified Support Operations that is allowed to make support calls on the 3rd party NGFW. The ownership of the Client NGFW is not changed or affected.
- Inform Trustwave of all Client environment maintenance activity and changes that may impact on Trustwave's ability to provide the Managed NGFW Service, as designed.
- In the case where the management server is owned and hosted by the client, client will update any Bios, Firmware or apply operating systems patches as needed and as requested by Trustwave
- Access the TrustKeeper Client Portal, respond to Tickets and confirm scheduled implementation of Product Updates and Security Updates.
- When requested by Trustwave, provide onsite support, for the Managed NGFW Device(s), to resolve connectivity or support issues.

- For Client owned NGFW devices, notify Trustwave that an RMA Process has been initiated, and:
    - Notify Trustwave on delivery of an RMA Device
    - Perform the physical installation of an RMA Device; and
    - Contact the SOC to arrange for Trustwave remote support and configuration of an RMA Device.
- The Client acknowledges that:
    - The implementation of necessary Product Updates and Security Update is not an optional feature of the Managed NGFW service; and
    - Failure to implement a required Product Update and Security Update as required, may adversely impact the operation and functionality of the Managed NGFW Device(s).

Security and Compliance Monitoring

- The Security and Compliance Monitoring services enable the Client to submit Log Data from Managed Enterprise Firewall Device(s) to the Trustwave Platform for Log Data collection, correlation, storage and reporting.
- The Security and Compliance Monitoring service consists of Three monitoring, analysis and detection service options:
    - Cloud Log Monitoring – collection and automated correlation of Log Data.
    - Managed Compliance Monitoring – Cloud Log Monitoring plus periodic human analysis
    - Managed Threat Analysis – Cloud Log Monitoring plus real-time human monitoring, analysis and investigation.
- Reporting and exploration – access to predefined reports and an interactive search functionality via the TrustKeeper Client Portal.

Cloud Log Monitoring

The Cloud Log Monitoring option includes the following base service features:

- Automated notification through the TrustKeeper Client Portal;
- 24x7 access to reports and interactive search functionality through the TrustKeeper Client Portal;
- 1-year offline storage of Log Data
- Daily, Monthly and Quarterly Reports including Event Summary, Security Alert and Incident Summary.
- Collection, automated correlation and automated analysis of Log Data collected by the Managed Enterprise Firewall Device(s), based on an evolving set of automated analysis use cases for threat detection. An example of the use cases are set out below, however actual rules in production are subject to change:
    - account lockout events, failed administrator authentication events, filesystem full events, filesystem nearing full events, reboot events, shutdown events, audit trail cleared events, account privileges modification events, time sync error events, network traffic anomaly events, audit system error events, brute force authentication attempt events, configuration change events, security audit trail cleared events, escalation of high priority IDS/IPS events, multiple suspected attacks from same source, multiple suspected attacks to same target, failed login (same user) on many hosts, recurring operational errors, source-specific escalations by event ID, source or target is in Known Bad Actor watchlist

Managed Compliance Monitoring

- The Managed Compliance Monitoring option includes the following base service features:
- The Cloud Log Monitoring base service features as referred to above;
- A SOC analyst review of Log Data for compliance- and security-related activity on a periodic basis and at least once per day and notify Client in accordance with the agreed pre-defined escalation procedures identified in the Client Initiation Information.

- 24X7 access to email support;
- Daily, Monthly and Quarterly Reports including Event Summary, Security Alert and Incident Summary.

Managed Threat Analysis

- The Managed Threat Analysis option includes the following base service features:
- The Managed Compliance Monitoring base service features as referred to above;
- 24x7 telephone support;
- Daily, Monthly and Quarterly Reports including Event Summary, Security Alert and Incident Summary.

Security threat investigation and incident notification

The GTO team has established incident investigation processes that provide for a consistent methodology of investigation across the globally distributed GTO teams. This process includes the advice and guidance from Trustwave Spider Labs malware research, threat intelligence and incident response teams. The GTO team will evaluate the available information it has to the point of helping to identify a potential attack attempts or Security Incidents. Where the investigation identifies a Security Incident, the GTO team will notify the Client of the results. Where the investigation does not result in a Security Incident, the GTO team will record the investigation without Client notification. The Client may access the history of investigations performed by the GTO via the TrustKeeper Client Portal.

- Security Alerts are analyzed by the GTO team on a 24 / 7 / 365 basis
- GTO analysts leverage all available Client information and intelligence associated with the Security Alert to determine the severity of the Security Alert.
- Where warranted, and based on the GTO investigation, the analyst will escalate a Security Alert to a Security Incident.

Trustwave Responsibilities

- Collect and Monitor Log Data via the Trustwave Platform via automated processes;
- Review Security Events collected by the Collector(s) and help in identification compliance- and security-related activity;
- Maintain availability of Security Events and Security Alerts in the TrustKeeper Client Portal.
- Generate automatic notifications of Security Alerts via the TrustKeeper Client Portal.
- Generate and publish the relevant reports to the TrustKeeper Client Portal.
- Investigate and analyze Security Alerts, help identify false positives and notify Client in the case of a suspected actual or potential threat.
- Help identify and prioritize Security Incidents and notify designated Client personnel based on the priority of the incident and the appropriate response.
- If needed, escalate the Incident based on its priority and according to the service level agreement (“SLA”) referred to in the previous clause of this service description.
- Create an exception rule or turn off the relevant rule, for identified false positives;
- Maintain updated status of Security Incidents on the TrustKeeper Client Portal.
- Record all communications in the Ticketing system.

Client Responsibilities

- Review Security Event and Security Alert activity in the TrustKeeper Client Portal.
- Review reports published to the TrustKeeper Client Portal.
- Notify Trustwave if Events or relevant reports are not available in the TrustKeeper Client Portal, as expected.
- Validate the prioritization of a Security Incident according to its business impact and notify Trustwave of priority classification errors.
- Work with Trustwave to resolve each Security Incident by providing relevant personnel and ensuring support and engagement of third parties as required.

- Provide Trustwave with requested information and confirmations in a timely manner.
- Maintain access to the Client TrustKeeper Portal to confirm updated status of Security Incidents.
- Request changes in accordance with the Trustwave change management process, and use and access the TrustKeeper Client Portal to log tickets, receive notifications, view, download and track the status of and respond to, Security Alerts and Security Incidents.

Reporting

Security Events and Security Alerts are available as a report in the TrustKeeper Client Portal as follows:

- 7 days of Security Events in the security activity page of the TrustKeeper Client Portal and 110 days of Security Alerts in the security activity page of the TrustKeeper Client Portal;
- Upon Client request, provide Client with 12 months of Log Data in csv format, which can be accessed securely through the TrustKeeper Client Portal.
- Summary of Tickets raised

Change Management

- Trustwave maintains an overall change control and configuration management procedure for its support infrastructure and associated managed services. Changes that could affect the operation of Client systems are coordinated with appropriate Client IT staff. Trustwave establishes an email address for each Client contact that is used to support communication with the Client and its service contractors responsible for administration of its networks.
- The SOC will assesses and implement change requests submitted by the Client or SOC through the TrustKeeper Client Portal. All requests are evaluated to help ensure that they are aligned with the features included with the service and will not detrimentally impact the security of the Client environment. Typical change request for the Managed NGFW Service are:
- Configuration changes to the Managed NGFW Device(s) as requested by authorized Client contact or a Threat Analyst in response to a known threat if Threat Analyst services are part of contract.
- Change reversals as requested by an authorized Client contact.

Trustwave Responsibilities

- Allow authorized Client personnel to submit Security Incidents through the TrustKeeper Client Portal, as needed.
- Perform change management activities when requested and in compliance with Trustwave policies.
- Validate that the request was submitted by an authorized Client contact, and notify Client if validation is not successful.
- Determine whether the request is in-scope with the terms of the Service.
- Source additional information as necessary to support the implementation of the change request.
- Assess the potential risk that will result from implementation of the change request and advise Client of the outcome
- Confirm Client approval to implement the change request after reviewing risk assessment results with Client and Confirm Client acceptance of implemented changes.
- When authorized Client personnel request that Trustwave roll back or reverse a change request:
    - Confirm receipt of Client's request for a change reversal.
    - Confirm completion of the change rollback upon successful execution of change reversal activities.
    - Execute joint testing with Client to validate the rollback is aligned to Client's request, and gain Client confirmation of the same.
    - Update the change request with information on rollback changes.
- Notify Client a change request is outside the scope of the service and or if additional charges will apply to a change request.

Client Responsibilities

- Submit change requests using the TrustKeeper Client Portal.

- Where the Client does not agree with a Security Incident priority, submit a change management request to change the priority of the relevant Security Incident.
- Provide Trustwave with requested information in a reasonable timeframe.
- Provide resources to review the risk assessment relating to requested changes.
- Review, assess and notify Trustwave of approval or non-approval to a proposed change request.
- When required, authorized Client personnel may request that Trustwave roll back or reverse a change request.
    - Submit reversal requests using the TrustKeeper Client Portal, emailing or phoning the Trustwave support team.
    - Provide resources to execute joint testing and confirm the change reversal is aligned with the Client-submitted request.
    - Confirm completion of the change rollback request.
    - The Client acknowledges that change requests that exceed two (2) man days of effort is deemed a project and is subject to acceptance by the Client of separately quoted additional charges.

Optional Service Features

- Optional services are available based on vendor specific capabilities. Not all optional services may apply to devices supported as part of this service.

Out of Band Connectivity

- Providing for connectivity with the device when the management network is offline can be critical. Out of band (OOB) console devices are used to provide remote console access to client premise equipment. In situations where MSS loses internet connectivity directly to the device the OOB can be used to connect to the device and determine if there is a health problem that can be fixed remotely. Also during maintenance work it is sometimes necessary to have console access while upgrades are being performed on devices. OOB consoles are available with 110 & 220V options.

Customer responsibilities

- Maintain a dedicated PSTN POTS connection

High availability management

- Trustwave managed NGFW services offers the option to manage the Managed NGFW Device(s) in a High Availability (HA) configuration. This provides redundancy for Managed NGFW Devices by placing two devices instead of one that work as a redundant pair so that if one device fails, the second device can take over operation. The HA NGFW's are set up in an Active/Passive mode
- HA devices are monitored to ensure they are online and operating as designed. HA devices are monitored and updated with Product Updates and Security Updates.
- When the primary monitored device is offline and not able to be recovered the HA device will be enabled.

Trustwave responsibilities

- Notifying the Client when a high availability Secondary Managed NGFW Device is brought online as part of a support ticket associated with the offline Primary device.

Customer responsibilities

- When requested by Trustwave, provide onsite support to resolve connectivity or support issues, when a high availability Secondary Managed NGFW Device(s) is brought online as part of a support ticket associated with the offline Primary device.

Web Content Filtering

- Web Content Filtering is commonly used to help prevent computer users from viewing inappropriate web

sites or content, or as a pre-emptive security measure to help prevent access of known malware hosts based on the Customer notified filter preferences. Web Content Filtering helps to prevent inappropriate use of an organization's internet connection by using the following additional features:

- List of over 100 categories for filtering purposes with Individual user policies supported; Usage and filtering activity reporting in Trustwave's secure customer portal
- Access Lists managed by Trustwave operations center staff
- Active Directory authentication support via RADIUS or NTLM

Application Control

- Application control allows clients to decide which applications are able to be accessed in the client environment based on the Customer notified preferences provided at time of provisioning. User based rules and time based rules are currently not supported, application policy configurations are limited to application allow or deny.

NAC on NGFW

- Network Access Control (NAC)-based service that helps detect, alerts and optionally blocks unauthorized devices that connect to the network. NAC performs a discovery on assets attached to the network and assets can also be manually added. Assets connecting to the network can then be restricted from access. Assets and alerts can be viewed via the TrustKeeper Portal. NAC on NGFW is not available on other 3rd Party NGFW's provided by Trustwave.

Internal Vulnerability Scanner

- Internal Vulnerability Scanning (IVS) is a vulnerability scanning service. The IVS service helps identify network vulnerabilities on the Client's internal network segments. The IVS service features are set out in the IVS Service Description and in summary consists of:
- Discovery, which is the information gathering and discovery process to understand the Client's System Target(s) and the scope of the required scanning of those targets.
- Scanning, helps identify potential vulnerabilities or weak configurations of the Clients System Target(s).
- Reporting, is the provision of results of the Client Target System(s) scans, as a completed report available through the TrustKeeper Client Portal;
- IVS services can be delivered in multiple ways. As part of the NGFW software or remotely with Trustwave 3rd Party NGFW's

Trustwave Responsibilities

- Request and collect Client Setup Information
- Provide and maintain a vulnerability signature database used by the Trustwave Platform
- Perform change management activities when requested and in compliance with Trustwave policies

Customer Responsibilities

- Provide initial IP addresses and schedule for scan to run
- Scheduling, configuring and conducting the scanning on the Clients target system(s) through the TrustKeeper Client Portal
- Generating, reviewing, analyzing and interpreting the results of the relevant scans
- Submit change requests using the TrustKeeper Client Portal

Virtual Private Network (VPN)

- Configuration of encrypted communication links available based on Supported Device selected. Support provided for both Site-to-Site connections and Remote User VPN Clients. One site to site VPN is included as part of the baseline offering, with additional VPN's available for purchase.

Trustwave Responsibilities

- Configure VPN in accordance with client predefined criteria and Monitor condition of VPN in accordance with monitoring policy

Customer Responsibilities

- Provide initial VPN configuration information.

Network DMZ segments

- Configuration of additional network DMZ segments. One DMZ is included as part of the baseline offering. Providing additional DMZ segments and managing the policies associated with those DMZ segments is an additional charge. Additional DMZ segments can be requested via the TrustKeeper portal as a change request.

Trustwave Responsibilities

- Configure DMZ in accordance with client predefined criteria and
- Perform change management activities when requested and in compliance with Trustwave policies

Customer Responsibilities

- Request additional DMZ segments via TrustKeeper Portal
- Provide DMZ configuration information
- Submit change requests using the TrustKeeper Client Portal
- Assist Trustwave on site if necessary for troubleshooting

Cellular Backup – * Only Available in USA and Canada

- Cellular backup to primary uplink in case of failure. If this option is included, see the cellular backup service description for more details regarding the features included with this option.

Trustwave Responsibilities

- Manage the interaction with the cellular provider on behalf of the client and Perform change management activities when requested and in compliance with Trustwave policies.

Customer Responsibilities

- Submit change requests using the TrustKeeper Client Portal