BT Managed Firewall Service Schedule
Part B – Service Description

Section A The Service

1. STANDARD COMPONENTS OF THE SERVICE

BT will provide the Customer with the following Services in accordance with the details as set out in the Order:

1.1 Advise on Security Appliances. BT will recommend an appliance (or appliances) as part of the overall service design. The Service supports Security Appliances from the following vendors:

1.1.1 Fortinet Inc.;

1.1.2 Paolo Alto Networks Inc.;

1.1.3 Cisco Systems Inc.; and

1.1.4 Check Point Software Technologies Ltd.

The delivery and management of Security Appliances depends on the selected Service Option taken by the Customer as further described in paragraph 2.1.

1.2 Security Applications. An appropriate security application license (e.g. for firewall or URL filtering software) will be provided by BT as part of the Service.

1.4 BT Portal: Provides a secure mechanism for service requests and Incident management.

1.5 BT Support. BT will provide the Foundation Graded Service Tier as standard. The features of Foundation are as follows:

BT Support	Description - Foundation Features
Implementation Support	BT's project manager will coordinate the installation and commissioning of the Service, in accordance with the delivery model selected on the Order, liaising with the Customer, installers and equipment suppliers as appropriate, depending on whether BT Equipment or Customer Equipment is being used. All project management activity will be administered remotely and the named representative will not visit the Site(s).
BT Service Desk - 1st Line Reactive Incident Management	The BT Service Desk is responsible for managing Incidents raised via the BT Portal or by phone by the Customer. Initial triage of the issue is carried out by using structured questions to capture all of the relevant details. Where necessary, if the issue cannot be resolved by the Service Desk, an Incident will be raised with the BT Global Security Operations Centre ("**GSOC**"). The Customer can access the BT Portal for progress updates and to respond to any requests for information BT asks for in order to help resolve the issue. Once the Incident is resolved, an update will be posted on the BT Portal and the Incident closed following confirmation from the Customer.
BT Global Security Operations Centre support - 2nd Line Reactive Incident Management	The GSOC is responsible for managing Incidents raised by the BT Service Desk which can't be resolved at 1st Line. The GSOC will carry out in-depth analysis, which will include logging onto the BT Portal to troubleshoot, check for best practices, etc. Where necessary, if the GSOC cannot resolve the issue, an Incident ticket will be raised with the Supplier.
Configuration Management Simple Service Requests ("SSRs")	BT will implement reasonable Customer-requested changes to the CSP, and upgrade Security Applications according to recommended and tested vendor patches. In accordance with the Service Request Management Process set out in Paragraph 8.5, the Customer may request SSRs per Security Appliance which will be available via the catalogue on the BT Portal. The number of SSRs per Security Device per Year are as follows for Foundation: • 6 Standard SSR changes; and • 1 Urgent SSR change.

Reporting	The Customer will have access to near real-time or historic reports for key Service performance metrics, and for security-related Incidents. This may be either via the BT Portal, or a reporting application provided by BT and installed on a server owned by the Customer.

Further details of these BT support services are set in Paragraph 8 of this Part B.

2. SERVICE OPTIONS

BT will provide the Customer with any of the following chargeable options in accordance with the details as set out in the Order:

2.1 Security Appliances. The Customer may choose on the Order between the following Security Appliance options:

2.1.1 "BT Owned". Where the Customer has selected this option the Security Appliances will be provided as BT Equipment. During the term of this Service BT will provide, install and commission any Security Appliances as BT Equipment, including any hardware and Software, licensing and support agreements for the Security Appliances and will arrange for any on-Site support and remote service management. Upon termination of the Service, BT will retain ownership of the Security Appliances.

2.1.2 "Customer Owned – Purchased from BT". Where the Customer has selected this option the Security Appliances will be purchased from BT subject to separate terms for hardware resale. During the term of this Service BT will provide applicable licensing and support agreements and will renew those agreements when required. BT will install and commission the Security Appliances and will provide on-Site support and remote service management. If there is a fault in the Security Appliances, BT will raise the necessary support requests on the Customer's behalf. Upon termination of the Service, the Customer will retain ownership of the Security Appliances.

2.1.3 "Customer Owned – Take over by BT". Where the Customer has selected this option the Security Appliances will be the Customer's existing Security Appliances. Once BT has confirmed in writing that such Customer Equipment is suitable for use with the Service, BT will remotely manage existing Customer Equipment, arrange applicable licensing and support agreements and will renew those agreements when required. If there is a fault in the Customer Equipment, BT will raise the necessary support requests on the Customer's behalf. Upon termination of the Service, the Customer will retain ownership of the Security Appliances.

2.1.4 "Service Wrap Only". Where the Customer has selected this option the Security Appliances will be the Customer's existing Security Appliances whereby BT will only provide remote service management and notify the Customer of any failure in the Customer Equipment that BT detects and it will be the Customer responsibility to raise the necessary support requests to its vendor. Upon termination of the Service, the Customer will retain ownership of the Security Appliances.

2.2 Additional Equipment for High Availability. The Customer can order dual appliance solutions for increased resilience against failure. There are options for hot-standby and load-sharing configurations.

2.3 Optional BT Security Features. The Customer may select the following options independently of the ordered Graded Service Tier level:

Feature	Description
High Availability (dual appliance) solutions	BT will configure a pair of Security Appliances on a single Site to give increased resilience against failure. Each Security Appliance may be connected to a separate Internet circuit to provide further resilience as set out in the Order. This Service Option will require additional switches to be included as part of the solution which will be provided by BT or the Customer. If it is the Customer's responsibility to provide the additional switches, BT will advise the Customer of the number and type of switches required. Depending on the Security Appliances used and the CSP, BT may configure the Security Appliances as "**Active Active**" (both Security Appliances share the load under normal conditions) or "**Active**

	Passive" (one Security Appliance handles the load under normal conditions, with failover to a secondary Security Appliance in the event of the primary Security Appliance failing). For "**Active Active**" configurations, throughput performance may reduce under failure conditions.
VPNs	BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards: (i) remote access IP Sec/SSL VPNs, for remote Users to gain secure access to Customer's internal network. BT will implement rules to authenticate against Customer's authentication server. (ii) Site to Site IP Sec VPNs between two Security Appliances which are both owned by the Customer and managed by BT; and (iii) third party (extranet) IP Sec VPNs, for creating a site-to-site VPN between Customer's Security Appliance managed by BT, and a Security Appliance owned or managed by the Customer or a third party. BT will only deliver VPNs to Security Appliances managed by a third party after the Operational Service Date. Where a digital certificate is required for remote VPN set up, either BT will provide, or the Customer will provide to BT, as set out in the Order, an up-to-date digital certificate that will be installed on the Security Appliance. Where the Customer provides the digital certificate, BT will: (i) install it within seven days of receipt from the Customer; and (ii) notify the Customer of the date of expiry of the digital certificate three months prior to the date of expiry. The Customer will advise BT, in writing, within one month of the date of BT's notification whether or not the Customer wants to renew its digital certificate. If the Customer wants to renew its digital certificate, the Customer will provide the new digital certificate to BT at least seven days prior to the expiry of the original digital certificate. BT will not be liable for any losses suffered by the Customer caused by expired digital certificates if the Customer does not: (i) confirm to BT that the Customer does want to renew its digital certificate; or (ii) provide BT with an up-to-date digital certificate.
De Militarized Zones (DMZs)	BT will provide additional LAN segment interfaces on the Security Appliance, or on an adjacent network switch, according to the Customer's requirements. This is subject to there being sufficient physical ports available and additional Charges will apply if additional hardware is required to provide the interface.
Firewall Intrusion Detection and Prevention Service ("IPS")	BT will: (i) monitor traffic passing through Customer's Security Appliance for attacks, in accordance with the applicable intrusion signature files; (ii) implement this Service option with a default configuration setting, as defined by the Supplier Software used to deliver the IPS. BT will also maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the Supplier; and (iii) not be responsible for evaluating these signatures beforehand. BT will advise the Customer how the IPS that have been selected operates with regard to alerting or IPS specific reporting. If BT agrees a request from the Customer to alter the parameters for applying new signatures in "**block**" mode, to give a greater or lower sensitivity to attacks, BT will not be responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

Firewall URL Filtering and Application Control	BT will: (i) block access to those Internet sites that Customer asks BT to, in accordance with the CSP. Internet sites are arranged into groups which are regularly updated. The Customer may choose to block or restrict access to any or all groups; (ii) send an appropriate message to a User attempting to access a blocked or restricted site to advise either: i. that the User request has been blocked; or ii. that the User will first confirm acceptance of your acceptable use policy (or similar warning). Upon acceptance, the page will be delivered; (iii) implement the necessary alterations via the standard configuration management process in the event of any change in the CSP; and (iv)
Firewall Anti-Virus	BT will: (i) check web browser (http) traffic for known Malware; (ii) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and (iii) keep antivirus definition files up to date by regular downloads direct from the antivirus service. Provision of this Service Option is subject to a maximum file size and compressed archive limits, depending on the Security Appliance selected.
Firewall Anti-Bot Service	BT will check and block outbound traffic for communication with known "**command** and **control**" servers used by owners of malicious software.
Threat Emulation Service	BT will encrypt suspected malicious files and send them to the vendor's cloud-based infrastructure where they will be decrypted and analysed for Malware by reviewing its behaviour in a virtual environment (sandbox). Depending on the Security Appliance selected, the Customer may be able to choose whether to hold the file whilst it is being analysed (to provide increased security) or to release it and analyse it in the background (for improved User response). Background processing may lead to malicious files being permitted until signature updates are subsequently generated and applied to the Security Appliances. If a file has been deemed malicious, its characteristics will be added to the vendor's anti-virus signature list. BT will determine the country in which this inspection and analysis occurs. If the Customer requires the Service to protect against Malware contained within SMTP (email) attachments, the Customer will arrange for its DNS mail exchange records to be re-directed to the Security Appliance so that email is delivered to that Security Appliance. BT will configure the Security Appliance to deliver email to Customer's email server. BT will not be responsible if the Customer is submitting and processing the Customer's data via the Threat Emulation Service option.
Security Event Reporting	BT will: (i) provide reporting facilities, either on-line or on a server hosted on the Site, which allows analysis of security-related events; and (ii) not pro-actively view the reports and events for Security Incidents. If this Service Option is delivered via a shared reporting platform, BT will configure the platform such that the Customer is only provided with access to its reports. This may mean that some of the platform's functionality is restricted to preserve the confidentiality of all customers using that platform. The period over which data can be analysed is dependent on the capacity of the Security Appliances or the space allocated on the reporting platform.
SSL/TLS Inspection	If the SSL/TLS Inspection Service Option is selected, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided the CSP permits such scanning. BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in

	accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP). BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites e.g. some websites may not permit decryption.
Identity Awareness / User groups	BT will configure the features of the Security Appliance that support the Identity Awareness/User groups Service Option to apply certain rules of the CSP according to the authenticated identity of the User rather than just their IP Address. This may require client software to be installed within the Customer's network or on end-user Security Appliances, or ensuring BT has remote, read-only, access to the Customer's active directory authentication server. The Customer will maintain the authentication database of Users, groups and any access credentials the Customer requires.
Vulnerability Notification and Patching	BT will identify, test and implement patches for High and Critical CVSS scores in accordance with the Customer's authorisation. The Vulnerability Notification and Patching Service Option will only be available while the Security Appliance is supported by the vendor.
Complex Service Requests ("CSRs")	The Customer can request help from BT via the BT Portal for requests that are complex and require technical support to be provided. These are reviewed on an individual basis and the Customer will be informed of the applicable charges to carry out the specific CSR requested. The Charges and Service details will have to be agreed on an Order before any CSR is implemented.
Security Optimisation Manager ("SOM")	The SOM will provide security-specific technical support and will review and make any recommendations on optimizing the Service. This will ensure best practice.
Service Manager ("SM")	The SM can be selected if the Customer does not already have a service manager supporting for other BT services. The primary role of the SM is: • providing regular reporting on the Incident and service request management functions • updating the Customer Handbook; and • reviewing any service improvement initiatives.
Ad Hoc Professional Service	Ad hoc professional Services may consist of: - BT support in setting out the Customer security policy in the CSP; - Support in Customer's network design; or - Other consultancy services. The details and applicable Charges for any optional ordered ad hoc professional services will be set out in the Order.
CSP production	BT will provide the Customer support in the production and implementation of the CSP for a period of three Business Days. Any additional days needs to be ordered as "Ad Hoc Professional Services".
Co-Management	BT will provide the Customer with a Role Based Account Control Profile ("**RBAC Profile**") for up to a maximum of 5 authorised nominated Users on the BT Portal. Users of the RBAC Profile will have restricted access to implement SSR's. BT will provide the Customer with a separate user guide setting out details how to manage SSR's.

2.4 Optional BT Support Services. The Customer may select the Foundation Plus and Premium Graded Service Tiers. In addition to the standard Foundation features as set out in Paragraph 1.5, the features of Foundation Plus and the Premium Graded Service Tiers are as follows:

BT Support	Description
Implementation Support	In addition to the standard implementation support; with Premium the BT Project Manager will be available to visit the Site(s).
Simple Service Requests ("SSRs")	In accordance with the Service Request Management Process set out in Paragraph 8.5 of this Part B, the Customer may request SSRs per Security Appliance which will be available via the catalogue on the BT Portal. The number of SSRs per Security Device per year is as follows: For Foundation Plus:

	• 12 Standard SSR changes; and • 2 Urgent SSR changes For Premium: • 24 Standard SSR changes; and • 3 Urgent changes.
Reporting	BT will provide reports on the Portal with regards to Incident Management, SSRs and CSRs. For Foundation Plus: • quarterly For Premium • monthly there will be a review and report to the Customer as further detailed in Paragraph 8.4.2 of this Part B.
BT Eagle-i	BT Eagle-i is a tool providing enhanced Security Incident alerts, which contains additional detail on the reported Security Incident allowing BT to provide improved recommended mitigation or corrective action to the Customer. Depending on the Graded Service Tier selected, the BT Eagle-i Service option provides various management options as set out on the Order.

3. SERVICE MANAGEMENT BOUNDARY AND SERVICE LIMITATIONS.

3.1 BT's responsibility to provide and manage the Service up to and including the following service management boundary:

3.1.1 The standard Service elements as set out in Paragraph 1; including the BT Portal/s where access is managed by BT and the BT Portal;

3.1.2 Any optional Service elements ordered by the Customer as and forming part of a Graded Service Tier as set out in Paragraph 2.

3.2 Paragraph 3.1 constitutes the "**Service Management Boundary**."

3.3 BT will have no responsibility for the Service outside the Service Management Boundary.

3.4 BT does not make any representations, whether express or implied, about:

3.4.1 whether the Service will operate in combination with any Customer equipment or other equipment and software; and

3.4.2 the ability of the Service to detect and mitigate all Unknown Viruses, malicious threats or attacks from the Internet.

4. ENABLING SERVICE

4.1 The Customer will have the following services in place that are necessary for the Service to function:

4.1.1 Internet connectivity between the Customer Site and the BT Network;

4.1.2 A firewall policy to be provided to BT; e.g. deny all, least privilege, explicit allow, and stateful inspection. These rules govern how a firewall handles inbound and outbound network traffic, including traffic involving different subnets and IP addresses ; and

4.1.3 The connectivity to any Customer IT services through the firewall that are necessary to ensure the integrity of the data network and to allow for vulnerability scans by BT.

(the "**Enabling Service**")

5. COMMISSIONING OF THE SERVICE

5.1 Before the Operational Service Date, BT will:

5.1.1 deliver and configure the Service as set out in the Order;

5.1.2 conduct a series of standard tests on the Service to ensure that it is configured correctly;

5.1.3 connect the Service to each Enabling Service;

5.1.4 on the date that BT has completed the activities in this Paragraph 5.1, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

6. ACCEPTANCE TESTS

6.1 The Customer will carry out the Acceptance Tests for the Service within five (5) Business Days after receiving notice from BT ("**Acceptance Test Period**").

6.2 The Service is accepted by the Customer if the Customer confirms acceptance in writing during the Acceptance Test Period or is treated as being accepted by the Customer if the Customer does not provide BT with notice to the contrary by the end of the Acceptance Test Period.

6.3 Subject to Paragraph 6.4, the Operational Service Date will be the earlier of the following:

6.3.1 the date the Customer confirms or BT deems acceptance of the Service in writing in accordance with Paragraph 6.2;

6.3.2 the date of the first day following the Acceptance Test Period; or

6.3.3 the date the Customer starts to use the Service.

6.4 If, during the Acceptance Test Period, the Customer provides BT notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide the Customer notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Section B Supplier Terms

7. EULA

7.1 Depending on the selected Supplier Security Appliances; the applicable EULA will be:

7.1.1 Paolo Alto: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-end-user-license-agreement-eula.pdf

7.1.2 Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf

7.1.3 Cisco – General Terms: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/Cisco_General_Terms.pdf

7.1.4 Checkpoint: https://www.checkpoint.com/fr/support-services/software-license-agreement-limited-hardware-warranty/

Section C Service Management

8. SERVICE MANAGEMENT

8.1 Technical Incidents

8.1.1 Where the Customer or BT becomes aware of a Technical Incident:

(a) it will be reported to the BT Service Desk;

(b) BT use structured questions to record the details of the Technical Incident. The BT Service Desk will log the Technical Incident in BT's standard Incident management system and generate an Incident ticket;

(c) BT will inform the Customer when it believes the Technical Incident is cleared and will close the Incident Ticket when:

(i) the Customer confirms that the Technical Incident is cleared within 24 hours after having been informed; or

(ii) if BT is unable to reach the Customer to confirm Technical Incident resolution, BT will attempt to contact the Customer three times in total, at regular intervals, before automatically closing the Technical Incident ticket.

(d) If the Customer confirms that the Technical Incident is not cleared within 24 hours after having been informed, the ticket will remain open, and BT will continue to work to resolve the Technical Incident.

8.2 Security Incidents

8.2.1 When BT becomes aware of a Security Incident related to the Service, the GSOC will be assigned to work on the Security Incident and the BT Service Desk will provide updates to the Customer in line with the service targets associated with the priority. Updates will be communicated via the BT Portal and with any agreed Customer contacts associated with the Security Incident.

8.2.2 When the Customer reports a Security Incident to BT, BT will log the Security Incident and carry out an initial triage of the issue by using structured questions to capture all of the relevant details. Where necessary, if the BT Service Desk cannot resolve the issue the BT Service Desk will raise a Security Incident to the GSOC so they can address more complex cases.

8.2.3 The GSOC is responsible for managing Security Incidents raised by the BT Service Desk for more in-depth analysis to be carried out, which includes logging on to the BT Portal to troubleshoot, check for best practices, etc.

8.3 Technical and Security Incidents additional terms:

8.3.1 The Customer will ensure that any Incident notification includes all relevant and available information at the time of contacting BT.

8.3.2 The progress update times and restoration times are targets only and BT will have no liability for failure to meet them.

8.4 Reviews and reporting

8.4.1 Foundation

(a) Reporting is available to the Customer as part of self-service directly on the BT Portal.

(b) The Customer will be responsible for administering the Service in life. Incidents can be raised using the BT Portal and additional professional services can be purchased by the Customer if required.

8.4.2 Foundation Plus

(a) Where the Customer has selected this optional BT Support Service, the in-life Service Security Support personnel will carry out on a quarterly basis a review on the technical performance of the Service and send a report to the Customer or discuss at review meetings with the following actions:

(i) a review focusing on the performance of the Service; and

(ii) a review of the Customer's security policy(ies) focusing on the effectiveness of the rules applied to the Customer's security policy(ies) and the need to fine tune or amend the rules of the Customer's security policy(ies) or recommendations on the User experience set up.

8.4.3 Premium

(a) Where the Customer has selected this optional BT Support Service, the in-life Service Security Support personnel will carry out on a monthly basis a review on the technical performance

of the Service and send a report to the Customer or discuss at review meetings with the following actions:

(i) a review focusing on the performance of the Service; and

(ii) a review of the Customer's security policy(ies) focusing on the effectiveness of the rules applied to the Customer's security policy(ies) and the need to fine tune or amend the rules of the Customer's security policy(s); or recommendations on the user experience set up.

8.5 Service Request Management process

8.5.1 BT will implement changes to the Customer's security policy(ies) in response to Customer requests, subject to the following process:

(a) BT will provide secure access to the BT Portal to all pre-agreed and authorised Customer contacts to enable service requests to be submitted;

(b) SSRs are upgrades and modifications needed because of planned developments and security improvements. SSRs will be executed subject to the Customer's approval and when the Customer requests a SSR the Customer needs to inform BT is the request is urgent or not. The lead times for implementing a SSR are set out on the Order.

(c) The initial SSRs are set out on the Order which may be amended from time to time depending on changes by the Supplier subject to BT providing notice to the Customer and, where any changes may have a material impact on the Customer, the Customer's approval will be sought; and

(d) SSRs are limited to the quantity per month depending on the Graded Service Tier level ordered by the Customer. If the Customer requires additional SSRs a maximum of 15 per month can be ordered at an additional charge.

8.5.2 Where the Customer raises SSRs more frequently than the standard allowance, the Parties may either agree:

(a) to aggregate the Customer requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays;

(b) to review the Customer requirements and agree with the Customer an appropriate alternative implementation process and any associated charges via a new Order; or

(c) to charge such additional SSRs at the rate as set out in the Order.

8.5.3 BT will communicate the status of all service requests on the BT Portal for a period of six months.

8.5.4 The Customer will ensure that any authorised Customer contact with access to the BT Security Portal will not submit any unauthorised requests.

8.6 Co-Management

8.6.1 If the Customer orders Co-Management:

(a) BT will provide the Customer with a separate user guide setting out details how to manage SSRs; and

(b) if a SSSR implemented by any User using the RBAC Profile has resulted in an Incident as notified by the Customer, BT will provide assistance to resolve the Incident using the audit and logging capability on the BT Portal to support any root cause analysis undertaken to confirm this.

8.7 Service targets

8.7.1 Service Care target response times and follow-up

(a) The Foundation Graded Service Tier provides support as set out in the table below.

(b) The Customer must have a dedicated employee who is available by phone with the necessary access to assist in troubleshooting. If an employee is not available, the Customer will agree with BT on a timeframe for updates.

		Incident Stage			
Priority	**Description**	**Initial Response**	**Next Response**	**Further Responses**	**Target Restoration**
P1	one or more core Service components are completely unavailable or one or more core business functions are completely unable to be performed. This would typically be all Users for this Service	Customer will be informed that BT is dealing with their Incident within 15 minutes of receiving it (either via an alert or by the Customer advising us)	First update within 30 minutes from the Incident ticket being opened	Every 60 minutes	4 hours
P2	Material impact to the Service e.g., a partially interrupted or impaired Service which cannot be mitigated, or core business functions can be performed but in a reduced capacity	Customer will be informed that BT is dealing with their Incident within 30 minutes of receiving it (either via an alert or by the Customer advising us)	First update within 60 minutes from the Incident ticket being opened	Every 2 hours	8 hours
P3	Medium impact to the Service, e.g., an interruption or impairment. This might be an issue where a large percentage of the Service is functioning normally, such as the Service is suffering slow response, but Users are able to work, a small number of Users have total loss of service but the majority are functioning normally, or perhaps one element of Service is unavailable.	N/A	First update within 4 hours from the Incident ticket being opened	Every 4 hours	24 hours
P4	Very minor or no impact on Associated Services, such as a single User or very small number of Users having minor issues but core functions of the Service can be carried out as normal.	N/A	First update within 24 hours from the Incident ticket being opened	Every 24 hours	48 hours