

GTT *PRIVACY* *DATA SHEET*

FOR SECURE CONNECT FIREWALL SERVICE

SERVICE DESCRIPTION

This Privacy Sheet outlines how and why we process personal data in connection with GTT's Secure Connect (the "Service"). It provides details on where we store and transfer that personal data, how we maintain its security, and our compliance with relevant privacy laws and regulations. We will process personal data in accordance with this Privacy Data Sheet and with our [Privacy Policy](#).

Secure Connect Firewall Service - GTT provides the Service which involves procuring, configuring, deploying, testing, design, support and managing firewall components. The Service encompasses the set-up, maintenance, and modification of Firewall Policies as well as Firewall monitoring.

For a comprehensive understanding of the Service and its associated commitments, including Service Level Agreements (SLAs), please refer to the GTT Secure Connect Schedule, available upon request.

TYPES OF (CLIENT) END USER DATA

End User Personal Data may include:

For Secure Connect that incorporates Palo Alto Networks solution:

- Access time
- Usage data and configurations
- Threat prevention (including URL filtering and summaries)
- IPv4 and IPv6 addresses(source/destination)
- MAC addresses
- Device information
- Device interface information
- Device and User Attributes (URL, URL/page title, Filename, file path, file decryption, file open activity, source/destination, successful or failed logins (URLs, websites))
- File details of file blocked by security policy
- User names of login blocked by security policy
- UUID
- User ID



- Serial number
- Customer support portal ID
- Domain names
- Information contained in emails (Sender/recipient email addresses, subject line, personal data in email body and in attachments if any)
- IP/NAT address, credentials, URLs, cookies
- Host names
- Network Object names
- Operating Systems
- Group or names associated with accounts including Active Directory information
- URLs visited
- HTTP response data
- URL associated with unknown file
- Name of unknown file
- Geolocation data
- Port ID, protocols and packet sizes

For Secure Connect Firewall solutions that incorporate Fortinet technologies:

- Access time
- IPv4 and IPv6 addresses (source/destination)
- Product IP Address
- Product Serial Number
- Unrated URLs
- Antivirus, IPS and other Malware statistics
- Security Rating Results
- Chat interaction data
- Technical support tickets may contain technical data shared by clients to assist GTT and the vendor in troubleshooting product-related issues
- Credentials used to login to the support portal
- Logs and telemetry data from the product enabled by client
- Event and UTM logs (may contain device serial number, device interfaces, source/destination IP, and optionally application name and username)
- FortiGate configuration
- Web portal usage
- MAC addresses
- Device information
- Device interface information
- Domain names
- Host names
- Network Object names
- Customer support portal ID
- Operating System information
- Traffic data
- Information about activity on computing systems including but not limited to registry changes, running processes, network communication, application behavior, web traffic
- Meta data of files detected as malicious on endpoint
- Group or names associated with accounts including Active Directory information
- URLs visited



- URLs submitted for URL ratings
- Port ID, protocols and packet sizes

PURPOSE OF PROCESSING (PROCESSOR)

- Service Provision
- Client Support
- Service Management
- Reporting
- Technical Monitoring
- Investigation
- Threat analysis
- Troubleshooting, including log analysis, insight reports development.

DATA DELETION & RETENTION

The table below lists the applicable retention periods for each category of personal data processed by GTT in connection to the Service.

Categories of Personal Data	Retention Period
End User Personal Data	- Data retention and log storage shall apply for the duration of the Agreement and shall be subject to: (i) the Client's requirements, (ii) the retention period agreed between the Parties, and (iii) the Client's use of the log storage facility.

DATA LOCATION & STORAGE

Storage Location	Access Location
Fortinet - GTT locations once the data is sent to the analyser from the firewall, which is on the customer premises - the location is agreed with the client out of the following: UK (Slough), UK (London), US (Dallas), US (New York), US (Los Angeles), US (Chicago), US (Atlanta), Canada, the Netherlands, Sweden, Germany (Frankfurt), Germany (Berlin), Switzerland (Zurich), Switzerland (Geneva), France, Italy, Spain, Hong Kong, Japan, Singapore, Australia, South Africa, Brazil. For clients using Fortinet provided services please refer to the Fortinet Data Privacy Practices in the Sub-Processor's section.	GTT Personnel: Authorized personnel located in Bulgaria, India, and USA or other locations with authenticated access into the appropriate management platform. Client: Authorized Client employees, contractors, representatives and end-users depending on their country location.
Palo Alto GTT locations once the data is sent to the analyser from the firewall, which is on the customer premises - the location is agreed with the client out of the following: UK (Slough), UK (London), US (Dallas), US (New York), US (Los Angeles), US (Chicago), US (Atlanta), Canada, the Netherlands, Sweden, Germany (Frankfurt), Germany (Berlin), Switzerland (Zurich), Switzerland (Geneva), France, Italy, Spain, Hong Kong, Japan, Singapore, Australia, South Africa, Brazil. For clients using Palo Alto Networks provided services please refer to the Palo Alto Privacy Data Sheets in the Sub-Processor's section.	GTT Personnel: Authorized personnel located in Bulgaria, India, and USA or other locations with authenticated access into the appropriate management platform. Client: Authorized Client employees, contractors, representatives and end-users depending on their country location.

PERSONAL DATA TRANSFER

To ensure compliant data transfers across jurisdictions, GTT has established an Intra Group Data Transfer Agreement (IGDTA) between GTT's entities. This agreement utilizes the EU Standard Contractual Clauses and other applicable data transfer mechanisms as needed to maintain lawful and secure data processing practices.



ACCESS TO PERSONAL DATA

Users, Client, and GTT can access personal data in connection to the Service as described in the table below.

Parties with Access	Justification	Access Control
GTT personnel	Troubleshoot and support Service	Corporate Credentials and MFA
Client	Through appropriate management platform with access limited to only that Client's End User Personal Data	Client Credentials MFA (if available)
Fortinet	Customer support, forensic analysis, threat research and troubleshooting	Access privileges Credentials MFA
Palo Alto	Customer support, forensic analysis, threat research, product development and troubleshooting	Access privileges Credentials MFA



THIRD-PARTY SERVICE PROVIDERS (SUB-PROCESSORS)

Below is a list of third-party service providers that GTT may use to deliver the service, along with links to their respective privacy policies.

Third-Party Suppliers	Country	Supplier's Privacy Statement
Fortinet	Global	Fortinet Privacy Policy Data Privacy Practices
Palo Alto Networks	Global	Privacy Statement Telemetry Strata Logging Service Prisma Browser DLP Advanced Threat Prevention Advanced URL Filtering GlobalProtect Cloud Services WildFire Advanced DNS Security Panorama Centralised Management