# GTS Managed Security

Valid from November 1st 2011.

## 1 Content of the service

**GTS Managed Security or Comprehensive security in the form of a service**

There are countless different threats to data networks, files and identity today. Viruses, spyware, spam, malicious e-mails, online evil-doers, hackers, identity thieves and intruders to wireless networks, all that represents a threat to you and your company. Your provider offers an exceptional opportunity to easily provide for the required protection of your network on a very high level – using **GTS Managed Security.** GTS Managed Security has been designed as a value added service to GTS VPN, GTS internet, etc.

GTS Managed Security is a lease of state-of-the-art security device by Fortinet (Fortigate) providing for the services of firewall, intrusion prevention system (IPS), web content filtering, antivirus, anti-spam, antispyware, traffic monitoring and the management of IM/P2P preventing security breaches by combined attacks or unauthorised use. The solution is complemented by full outsourcing of all management services. GTS Managed Security can become an integral part of the services of interconnection of branches and Internet connection (VPN) and it can also appropriately complement your existing firewall that does not have application protection or integrated antivirus or antispyware protection.

**Comprehensive security as a service brings significant savings compared to a one-time investment in an entire solution, while it does not increase security risks.**

The basic principle of the service lies in provision of a top quality solution on the interface between the Internet connection and the subscriber's private network (LAN or VPN – depending on the characteristics of the services, the firewall may be located in the provider's data centre or in the subscriber premises). All of the subscriber's corporate communication goes through the provider's firewall that ensures protection of the subscriber's systems and compliance with the defined security policies. The equipment and the software are owned by the provider, including management and configuration. All updates of the operating system and the modules, security patches issued by the producer and other services are provided for by outsourcing via the provider's specialists who have rich experience in the area of security.

As regards the side of the customer, the only thing needed is to define security policies for the users and their user rights (Internet access and use of the application services), including the options of advanced authentication. Key benefits include high service availability, i.e. in case of an outage or a defect, the device will be replaced so that the limitation of the subscriber's operation is kept to the minimum. The device is replaced free of charge and supplied in the required configuration so that it is capable to immediately fulfil the subscriber's security requirements and avoid any threats.

In case the needs or requirements of the subscriber increase above the level of the supplied solution during the service provision, the requirements and the performance of the solution will be assessed and a new, better suited solution will be offered to the subscriber. Also included in the service is a regular evaluation and discussion of the performance of the equipment, which can be done in regular three-month intervals upon the subscriber's request.

## 2 Characteristics of the service

### 2.1 Standard variants of the service - Firewall + Intrusion prevention (IPS)

**UTM firewalls (Unified Threat Management )**

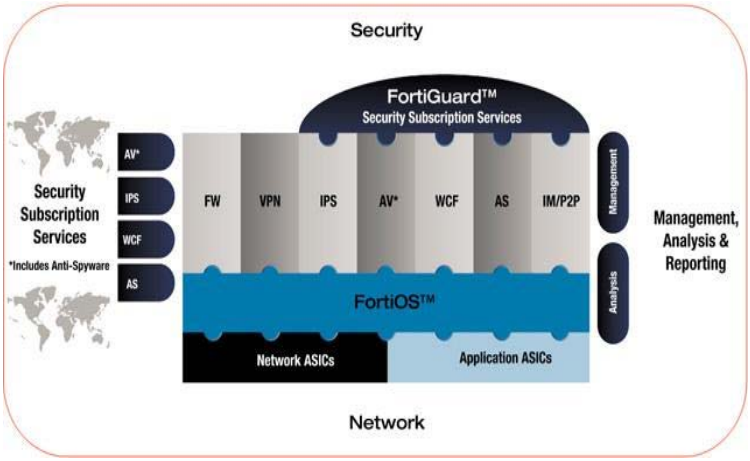
UTM firewalls offer unrivalled security and performance parameters in all of its products. In order to achieve high levels of security without negative impact on data throughput, Fortinet developed a high-performance ASIC processor for scanning the application layer of the TCP/IP protocol - FortiASIC. Also patented is the Content Pattern Recognition Language (CPRL) accelerating the repeated operations used for data content analysis. The technology is much more advanced than the packet in-depth scanning used by a lot of firewalls by competitors. Thanks to the advantage of information sharing between the security elements, it is possible to prevent attacks that are not signature based and are unknown.

#### Intrusion Detection and Prevention System

This provides for warning based on configurable database of more than 1,300 known intrusion codes. IPS stops attacks that avoid the common host-based antivirus systems, while quickly reacting to the quickly spreading intrusions in real-time. The worldwide network of these devices offers to the subscribers signatures of virus and intrusion codes in real time. The IPS modules uses a worldwide update network to stop most lethal intrusions on the network interface regardless of the network type – classic, wireless or a branch connected to the network. FortiASIC also supports learning based and heuristic methods, which expands the detection abilities compared to simple content comparison with the known codes.

## 2.2 Value added services

The service is based on Firewall + Intrusion prevention system (IPS); any of the additional sets of services may be added to the basis:




#### 2.2.1 Antivirus + Antispam[1]
#### Antivirus Gateway

This detects and removes viruses, worms and spyware in real time. It also scans attachments to incoming and outgoing email messages (SMTP, POP3, IMAP) and all traffic via FTP and HTTP, including web email, all that without reducing the performance. Antivirus gateways stop viruses and worms before they can penetrate the network. Antivirus personnel of those devices around the world offers to the subscribers continuous updates of antivirus signatures in real-time, using the worldwide updating network FDN (FortiGuard Distribution Network).

#### Antispam

Antispam keeps domain black lists white lists, lists of IP addresses and email addresses that may be maintained and updated as required by the company. Content filtering coordinates the activity with URL filtering of the FortiGuard service – this is a technique of impressions searching for specific URL or other objects like images included in messages, and compares them with impressions formerly identified as spam. This innovative method offers a highly efficient method of fight against image and pdf spam, while most antispam solutions have problem with this as they cannot read and subsequently process text in an image.

[1] The added set of Antivirus + Antispam (AV+AS) may not be used with the shared variant. If you prefer this additional module, you need to choose a dedicated firewall.

#### 2.2.2. Web Filtering

Webfiltering provides for testing of all web content for undesired URL's, blocking of unwanted content and dangerous Java applets, cookies, Active X scripts before they enter the network. Categorises more than 50 million domains and over two billion websites to protect the subscriber from unwanted sites. Website filtering dynamically cooperates with the systems providing for automatic updates of the categorised sites sorted in more than 70 categories based on their content. Services may also be configured by the user to enable the company network to add another URL to prevent access to other unwanted sites. Web content filtering guarantees improved productivity of work and to companies compliance with the regulations in educational institutions by disabling access to sites contradicting corporate ethics.

#### 2.2.3 Reporting

A comprehensive report in the form of charts and tables will be sent in regular intervals as an email with a PDF attachment; the report will describe use of the defined service parameters (virus frequency, top traffic, top users, top spam, etc.) for the monitored period. The individual properties of the reporting are also given by the structure of the ordered additional modules.

#### 2.2.4 DLP; Data-Leak Protection

DLP prevents sending of sensitive documents of the subscriber outside the company, thus preventing leakage of confidential information. This provides for control of incoming and outgoing documents that can be read in plain-text (*.txt, *.doc, *.rtf type documents, etc.) for prevents of the defined (banned) words. In case the document contains the defined words, DLP will prevent its sending. The controls may be done above the SMTP, FTP, HTTP protocols.

#### 2.2.5 Aplication control and P2P

Traffic profiling helps the subscriber to optimise and effectively manage the data flow for maximum usage of the transfer capacities, while maintaining the throughput guarantee, short waiting time and the necessary bandwidth for crucial corporate services. It provides for control (full blocking or definition of maximum bandwidth) of utilisation of networks for data sharing (like kazaa, gnutella, eDonkey, BitTorrent, WinNY, etc.). These protocols typically establish a massive number of connections thanks to which they may cause an overload of the Internet connection at the expense of protocols that are more important for the company and crucial corporate services. Moreover, these networks are also a great source of illegal content and malicious software. Application control – control o the data content transferred from the Internet sites, typically used for filtering of data transfer of different applications (streamed video, audio, data storage, game portals) from websites like rapidshare, youtube, online radios, etc.

#### 2.2.6 VPN concentrator (SSL)

The VPN concentrator provides users with remote access to the corporate network via the VPN technology. This is an alternative to VPN access using IPSec protocol, and it has much greater throughput in the filtered environment via different sources of Internet connectivity, where it may not be always possible to establish an IPSec tunnel. This is typically a connection via public hotspots, in hotels, Internet cafés and other networks using multiple transfer of addresses and potential restriction of ports and protocols. The service runs in the so-called portal mode, which means that unlike in the case of IPSec VPN, the connected PC does not become a remote service computer. This brings advantages as well as disadvantages – no infiltration of a remote network from a potentially dangerous computer out of the reach of network administrators, but it will not be possible to exchange data between the connected computer and other network devices – shared discs, printers.

### 2.2.7 Vulnerability scan

This provides for one-time checks of the systems connected to the data network in order to detect their weaknesses. This applies primarily to the operating systems (Windows, Linux and MacOS.), application and database servers, backdoor detection, operation of P2P networks, worms, DNS vulnerability, DOS vulnerability, etc. The output is in the form of a PDF document describing the identified vulnerabilities, their relevance, possible abuse, and information for the network administrator, how to avoid such vulnerabilities and prevent abuse of such vulnerabilities.

## 3 Key advantages of the service:

- Firewall is provided as a service and it is fully administered b the provider's specialists.
- Zero acquisition investments – monthly service fees are direct cost of operation, no cost of hardware, its maintenance and upgrade, no cost of software for administration of another system, saving of costs of solving communication outages and other effects of hacker intrusions, savings of operational costs of security (the price of the provided services is significantly lower than the price required for direct acquisition and management using an experienced specialist), no risk of poor or unfinished implementation.
- Full outsourcing enables the subscriber's IT team to fully concentrate on their own work, not having to deal with Internet threats, patching, licensing and service contracts.
- Software updates, software upgrades, monitoring of security issues, trained and experienced personnel.
- Easy deployment – the subscriber's network can be protected within just a few days.
- Guaranteed quality, complete security – firewall, IPS, antivirus + antispam + antispyware protection, web content filtering and remote access of "mobile" VPN clients.
- Common Criteria EAL4+ certification, 8 certifications of ICSA Labs.
- Protects your network and the entire VPN, also optimises the cost of connection capacity.
- Maximum reliability and availability of the provided services.
- Changes of the firewall configuration – as needed by the subscriber.
- High level of technical support – guaranteed replacement of equipment in case of an outage.
- Depending on the service characteristics, possibility of the firewall hosting in the premises of the data centre of the Provider compliant with the strictest quality limits for data centres

## 4 Key functions of the service:

- Securing the internal network of the subscriber on the level of application control of the communication (higher level of protection than common control provided by open source or commercial packet firewalls).
- Provides for secure remote access of mobile clients to the network.
- Protection of the internal mail server and DNS thanks to their proxy functions directly on the firewall.

- Antivirus, antispyware and antispam protection for http, smtp, pop3, IMAP, FTP...
- Control of outgoing web access with IM and P2P blocking.
- Detection of operational anomalies, IPS/IDS, DoS elimination, etc.
- Integration of effective web content filtering.

Connectivity services via IPv6 protocol (IPv4 as standard) may be ordered with GTS Managed Security. Connectivity services with IPv6 protocol are provided as value added services. They are not provided on all access technologies and they are not fully compatible with all services specified in this Service Description. The service may be provisioned upon positive outcome of the technical survey.

## 5 Service charges

The service is charged for as follows:

a) By Contract/Service specification
b) By Service pricelist of GTS manager security;
c) Potentially by pricelist of a supreme main connectivity service (GTS IP VPN, GTS Internet, GTS housing, etc.)

In case of discrepancies of specific provisions of the individual documents, the provisions of the documents shall prevail in the said order.

## 6 Service provisioning period

The standard period for service provisioning is usually **15** working days as of the date of signing of the contract (Service Specification) by the provider and the subscriber. This period shall not apply if another service by the provider is provisioned together with GTS Managed Security and provisioning of the two services is interrelated. Adherence to the agreed deadline of service provisioning is conditioned by provision of the necessary interaction by the subscriber as well as the existence (commissioning) of the connective services that GTS Managed Security is being provisioned for.

## 7 Minimum service utilisation period

The minimum period of utilisation of GTS Managed Security is determined for 12 or 24 months depending on the subscriber's request, unless another period is agreed upon in the contract/Service Specification is expressly agreed upon.

## 8 Provisioning and provision (operation) of the service

### 8.1 Service model

Two models are considered within the solution of GTS Managed Security: Dedicated GTS Managed Security firewalls for the individual users or shared GTS Managed Security firewalls used by multiple users. The optional set of Antivirus + Antispam (AV+AS) may not be used in case of the shared variant. If you prefer choosing that additional module, you should choose a dedicated firewall.
The shared model of the service may only be offered, if the firewall is located in the data centre of the provider – Nagano in Prague. If the Internet access is located at a different location, it is necessary to use the service variant located at the customer's (especially in case of GTS internet).

**Recommended parameters of the offered service variants:**

| Server type | Line throughput | Number of sessions | Number of VPN tunnels | Throughput of AV+AS | IPS throughput | VPN throughput |
|---|---|---|---|---|---|---|
| **Dedicated service** GTS Managed Security – Basic | 400 Mbps | 80 tis | 50 | 10 Mbps | 25 Mbps | 25 Mbps |
| **Dedicated service** GTS Managed Security – Normal | 125 Mpbs | 100 tis | 100 | 20 Mbps | 40 Mbps | 30 Mbps |
| **Dedicated service** GTS Managed Security – Profi | 200 Mbps | 400 tis | 800 | 30 Mbps | 80 Mbps | 40 Mbps |
| **Dedicated service** GTS Managed Security – Exclusive | 1,5 Gbps | 500 tis | 1500 | 40 Mbps | 200 Mbps | 1 Gbps |
| **Shared service** GTS Managed Security | 200 Mbps | 70 tis | 100 | N/A | 25 Mbps | 100 Mbps |

### 8.2 Provisioning and provision (operation) of GTS Managed Security

The equipment and the software are owned by the provider (or subcontractor). Provision of the service includes management and configuration of the respective equipment and software. All updates of the operating system and equipment modules, security patches issued by the producer and other services are done within full outsourcing of provider's specialists with rich experience in the area of security. The subscriber is only required to define the security policy, users and their user rights.

#### 8.2.1 Provisioning of the standard service includes Firewall +IDS:

Supply and connection of the equipment in the data centre of the provider or at the subscriber's premises, setting of the default configuration of the equipment according to the GTS Managed Security Service specification within the standard installation, commissioning, tests and handover.

1. Configuration of network interfaces
2. Configuration of routing (static/dynamic)
3. Configuration of DNS servers
4. Configuration of firewall rules
5. Creation of backup of the basic configuration
6. Announcement of service handover to the subscriber

Total scope of provisioning of the standard service is limited by the limit of 3 hours.

Provisioning of the standard service includes post-installation support which is understood as the technical support in the scope of 2 hours available to the subscriber for the first month of the operation for the purpose of fine-tuning of the configuration according to the specific needs.

Service provisioning does not include any work on local cabling and configuration of the subscriber's LAN. It is recommended that the network administrator is present during installation of the service. Service provisioning does not include an audit of the current security and definition of the security rules for the subscriber. Service provisioning does not include training of the subscriber or users, respectively.

**8.2.2 Monthly provision (operation) of the standard service includes Firewall + IDS:**

1. Supply and lease of all equipment (hardware), lease of software operation licences
2. Administration of the service and provision of permanent functionality according to the defined guaranteed parameters
3. Technical support and service configuration in the scope of 1 hour/calendar month (technical support is to be understood primarily as remote modification of service configuration according to the subscriber's requirements) – a greater volume of technical support and higher limits of guaranteed parameters can be purchased for a surcharge in the form of a higher class of guaranteed parameters (Premium, Nonstop).,
4. Emergency intervention in case of a defect of the equipment (depending on the selected technical support),
5. Upgrade of the firmware and software of the equipment, verification of the producer's licensing policy,
6. Evaluation of the system performance,
7. Creation and retention of backup of the last configuration change.

**8.2.3 Provisioning of each individual value added service includes:**

Setting of the default configuration of the equipment according to the Service Specification within the scope of standard provisioning of a value added service, commissioning, tests, service handover. The anticipated scope of work on establishment of a value added service within 2 hours/one individual value added service.

**8.2.4 Monthly provision (operation) of a value added service includes:**

1. operational, service and administrative cost of service (including software updates of the DB of antivirus, antispam, antispyware, etc., security patches and software upgrade, verification of the producer's licensing policy, etc. for the individual value added services)
2. backup of configuration of a value added service

**8.2.5 Monthly provision (operation) of a standard and value added service does not include:**

- Technical support requested b the subscriber which is in excess of the time frame included in the standard service (depending on the selected variant)
- Installation does not include any work on local distribution systems or configuration of the subscriber's LAN. Network administrator's presence is recommended during service installation.
- An emergency intervention, if the defect or non-functionality was caused by the subscriber, user, a third party, etc. – i.e. reasons that are not on the side of the provider.

**8.3 Service handover after provisioning (commissioning)**

The service is provisioned and handed over to the Subscriber for commissioning after setting of the default configuration of the equipment according to Service Specification, tests and provision of the Service Handover Protocol sent to the contact person of the subscriber.

Then the subscriber has two (2) complete working days (i.e. the period commences as of the first working day immediately following reception of a notification of commissioning of the service by the provider) for testing the functionality, configuration of settings parameters, comparison of the service compliance with the parameters provided in the respective Service Specification and confirmation of service acceptance according to the following.

The subscriber shall be obliged to confirm within the said period in writing (by e-mail) the acceptance of the service according to the respective Service Specification, or to raise comments or claim the functionality and parameters of the service, otherwise it is understood that the service is considered duly handed over in accordance with the respective Service Specification by expiry of the above deadline, e.g. two (2) complete working days. The service shall be considered duly provisioned to the subscriber by the provider according to the respective specification as of the moment of confirmation of service acceptance by the subscriber without comments and claims, or by expiration of the said deadline in vain. Post-installation support of 2 hours in the first month of service provision for the purpose of fine-tuning of the service configuration for the specific needs of the subscriber.

## 9 Variants of guaranteed service parameters and scope of technical support

Guaranteed parameters of the service are offered in 3 variants. Parameters of the Standard variant are included in the standard service, while Premium and Nonstop parameters are available upon subscriber's request for the surcharge specified in the valid Pricelist of GTS Managed Security, or expressly defined by the parties in the contract/Service specification.

**Variants of guaranteed service parameters**

The provider shall grant to the subscriber the following guaranteed service parameters (specific agreed variant of the guaranteed service parameters is agreed in the contract/service specification, and if not expressly agreed, it shall be understood that it is the Standard variant):

| Guaranteed service parameters | Standard | Premium | Nonstop |
|---|---|---|---|
| Reaction time regarding remedy of a service outage.<br>In the working hours (i.e. in working hours from 8:00 a.m. to 6:00 p.m.)/outside working hours (i.e. outside working days and on working days from 6:00 a.m. to8:00)* | up to 3h / max. do 6h* | up to 2h / up to 5h* | up to 1h / up to 4h* |
| Maximum time of remedy of a service defect – for equipment located in data centres of the provider in Prague | up to 18 h | up to 12 h | up to 9 h |
| Maximum time of remedy of a service outage – for equipment located anywhere in ČR | up to 24 h | up to 18 h | up to 12 h |
| Customer and technical support of the service on the spot | up to 24 h | up to 18 h | up to 12 h |

All the deadlines specified here commence as of the moment of reception of the respective request (for remedy of the service or customer and technical support of the service on the spot agreed) in the agreed form by the provider.

In case of a breach of any of the agreed guaranteed service parameters by the provider due to his fault, the subscriber shall be eligible to require the provider to pay the contractual sanction of CZK 200 per hour of default for each individual breached guaranteed parameter of the service. Summary of all contractual sanctions for all breaches of any guaranteed service parameters in a single billing period may not exceed the agreed recurring monthly fee for provision (operation) of the agreed service variant. The contractual sanction shall be provided to the subscriber in the form of a discount from the charged recurring monthly fee upon reception of the respective request by the provider. The subscriber shall be obliged to ask the provider for the contractual sanction

in writing within 2 months as of termination of the respective billing period for which the subscriber is eligible to receive the sanction, otherwise the right to the sanction shall cease to exist.

**Technical support of the service**

The provider offers the following variant of technical support of the service to the subscriber. The Standard variant is included in the standard service and also in the basic pricing proposal, while the Premium and Nonstop variants are available to the subscriber for the surcharge defined in the applied Pricelist of GTS Managed Security, or expressly defined by the parties in the contract/Service specification.

| Technical support | Standard | Premium | Nonstop |
|---|---|---|---|
| Remote customer and technical support | 24 x 7 | 24 x 7 | 24 x 7 |
| Scope of TP support/calendar month (modifications, settings, re-configuration, solution of user problems) | 1 hour | 2 hours | 4 hours |

## 10 Technical information about GTS Managed Security

GTS Managed Security may be an inseparable part of branch interconnection and Internet access (VPN) services and it may also suitably complement your existing firewall that doe not have application protections, or an integrated antivirus or antispyware protection for http or smtp.

Technical equipment for operation of the service:

### FortiGate-60C Features

Maximum Firewall Throughput 1 Gbps
Maximum IPSec VPN Throughput 70 Mbps
Maximum Antivirus Throughput 20 Mbps
Maximum Concurrent Sessions 80 000
Network Interfaces 5 1000Mbps switch, 1 DMZ 10/100Mbps, 2 WAN 10/100Mbps

### FortiGate-80C/CM Features

Maximum Firewall Throughput (1518 byte UDP packets) 700 Mbps
Maximum Firewall Throughput (512 byte UDP packets) 350 Mbps
Maximum Antivirus Throughput 50 Mbps
Maximum IPS Throughput 100 Mbps
Maximum Concurrent Sessions 100,000
Network Interfaces 2 10/100/1000 Base-T (WAN),7 10/100 Base-T (6 switch/LAN, 1 DMZ)
3G WAN Connectivity 1 ExpressCard slot Analog Modem Yes (FortiGate-80CM)

### FortiGate-110C Features

Maximum Firewall Throughput 500 Mbps
Maximum IPSec VPN Throughput 100 Mbps
Maximum Antivirus Throughput 65 Mbps
Maximum Concurrent Sessions 400K
Network Interfaces 2 Copper GigE 10/100/1000 Base-T, 8 10/100 Base-T

### FortiGate-200B Features

Firewall Throughput (Max, 512B/1518B UDP) 5 Gbps
Firewall Throughput (Max, 64B UDP) 4 Gbps
Antivirus Throughput (Max, 32KB HTTP) 95 Mbps
Maximum Concurrent Sessions 500,000
Network Interfaces 8 x 10/100/1000 (4 x FortiASIC Network Processor Accelerated) 8 x 10/100
FSM Expansion Bay 1

## 11 Changes in settings of parameters and configuration of the service

The subscriber may order a change of parameters or the configuration of the service from the provider via the respective service change specification, or via the Customer Care Department. Changes are implemented within the hours of the agreed technical support of the service. If the scope and elaborateness of the change of the required parameters is greater than the scope of the hours of technical support agreed within the service, the changes shall be charged for according to the applied Pricelist of GTS Managed Security. The requirement for change may be filed only by an authorised representative of the subscriber. No changes may be implemented in the period of 5 or less working days before the agreed term of service provisioning.

## 12 Changes of service variant

A change of the service variant (standard, non-standard, Normal, Profi, Exclusive) is considered a termination of the original service (termination of the original Service Specification) and provisioning of the new service according to the new Service Specification, or a change Service Specification.

## 13 Service claims, remedy of a service outage (defect)

"Customer Care Centre" is available 24 hours a day, 365 days a year and calls are processes continuously. In order to expedite remedy of a defect/service claim, the provider requires that the subscriber notifies the provider already when first symptoms of a defect appear. The subscriber shall be obliged to notify the "Customer Care Department" of the provider by telephone about the defect/service claim. The contact s specified in the contract.
The subscriber's information (report) about the defect/ service claim shall include especially the following information:

- Customer identification (name, identification number, customer number or the number of the contract between the provider and the subscriber);
- Identification of the defect location (address of the place of the end point of the service / subscriber location, or the location of the defect);
- Description of defect/claim;
- Date and time of defect origination;
- First and second name of the person acting on behalf of the subscriber and his/her telephone connection.

The "Customer Care Centre shall take the steps necessary to remedy the defect/claim. The subscriber shall be assigned a defect number to be used in the subsequent contacts so that it is possible to correctly monitor the progress of repair.
If a service defect cannot be remedied by a "remote" intervention using the subscriber's personnel, the authorised worksite of the provider shall organise a service intervention to repair the defect; such service defect will be repaired by a service group based on a work order. A technician's intervention in case of a defect caused by the subscriber shall be charged for according to the applied pricelist of GTS Managed Security. A defect caused by the subscriber shall also be understood as the technician's intervention in vain (the defect does not exist or the work necessary to remedy the defect is rendered impossible by the subscriber, non-provision of the respective interaction, or if the defect has demonstrably been caused by the subscriber).