

D. SLA Managed Firewall Service agreement MF999

D.1 Parties

A Company Manufacturing Everything, statutory established at
Companylane 12,
9999 XX ACITY, referred to as ACME,

and

TUNIX Internet Security & Opleidingen b.v., statutory established at
Wijchenseweg 111,
6538 SW NIJMEGEN, referred to as TUNIX,

both parties hereto, through their duly authorized representatives, have executed this Managed Firewall Service agreement.

This agreement with contract number MF999 applies to the machine known as ns.acme.nl



D.2 Managed firewall service

TUNIX delivers a managed and secure network connection to the Internet with:

- 1 Installation of a firewall as described in paragraph D.3.
- 2 The maintenance of this software as described in paragraph D.4.
- 3 The offering of a support desk standby service as described in paragraph D.5.
- 4 The administration and surveillance of the firewall as described in paragraph D.6.
- 5 The installation and maintenance of the firewall hardware as described in paragraph D.7.

D.3 Firewall implementation

- 1 TUNIX provides, configures and installs an operational **managed firewall** that follows the functional specifications as described in SS/RP/27574.
- 2 TUNIX delivers the **managed firewall** turnkey, assembled, tested and demonstrated at the following location:
ACME, Companylane 12, 9999 XX ACITY.
- 3 The initial purchase price of the **managed firewall** is incorporated into the monthly charge of this agreement.
The necessary **hardware** and **software** will be employed by TUNIX at the aforementioned location as part of this agreement for purpose of the *managed firewall service*, but will remain the property of TUNIX.
- 4 Unless explicitly stated, all calculations in our proposal are only intended as a base for the management-price mentioned in this agreement.



D.4 Software maintenance

- 1 Under the terms of this contract TUNIX will periodically provide the necessary security patches and bugfixes for the aforementioned firewall software. These activities are referred to as **updates**.
- 2 As part of this contract TUNIX will periodically provide the aforementioned firewall-software of new **software** which TUNIX develops and which typically comes with any new firewall. These activities are referred to as **upgrades**.
- 3 TUNIX will install available **updates** and **upgrades** on the aforementioned firewall and ensure integration into the existing environment. The **updates** and **upgrades** will at the latest be installed one month after these have been incorporated in the standard firewall **software**.
- 4 **Updates** and **upgrades** which are urgent on grounds of security will always be installed as quickly as possible.
- 5 By providing and installing **updates** and **upgrades** TUNIX will keep the firewall-**software** on the same functional level as the **software** of firewalls which is per default installed on new firewalls.
After installation and integration **updates** and/or **upgrades** are a part of the firewall but are not activated unless they replace an existing, active component. The existing functionality of the firewall remains. TUNIX will advise if, and if so, how the new functions may be used. New functions are only configured and activated when ACME so orders it.
- 6 The installation of **updates** and **upgrades** for standard modules (such as the installed virus scanner which scans SMTP traffic for viruses) is a part of this agreement.
- 7 If ACME wants to arrange specific **service windows** then these will be laid down in a separate appendix. Such arrangements are considered not made unless a separate **backups** appendix is attached to this agreement. If such an arrangement was not made then TUNIX may independently plan the **service windows**.
- 8 **Upgrades** procedure (in chronological order):
 - a TUNIX will announce **upgrades** at least two weeks up front. In this announcement is indicated which components of the **software** are affected by the changes/extensions and what implications this will have. Also, the starting date of the **upgrades** will be announced.
 - b Prior to the date of the planned **upgrades** ACME may contact **Tunix support** in order to arrange a different time for the upgrade (within office hours). If ACME does not contact **Tunix support** TUNIX will upgrade your firewall at a moment of their choosing.
 - c Directly prior to the **upgrades** TUNIX will contact one of the **contacts** of ACME and confirm the **upgrades**. When all **contacts** are unreachable TUNIX will begin the upgrade.



- d Prior to the **upgrades** TUNIX will make a local and an off-site backup of the configuration.
 - e Prior to the **upgrades** TUNIX will verify whether the configuration, as well as a possible mirror or any parallel systems, are in order. If in the opinion of TUNIX the configuration is not in order the **upgrades** will be carried out until one of the **contacts** has been notified.
 - f TUNIX carries out the **upgrades** and reports to one of the **contacts** of ACME that the activities have been completed.
 - g TUNIX will make a local and an off-site backup of the configuration.
 - h TUNIX verifies whether the configuration is functioning according to specifications after the **upgrades** are carried out.
 - i If the functionality has been altered or changed by the **upgrades** TUNIX will provide supplementary documentation such as manuals, release notes or configuration implications to ACME.
- 9 Should a malfunction occur which is possibly caused by the **upgrade/update** a **roll back** will be at all times possible. The response time for serious calamities as described in paragraph D.5 applies to carrying out the **roll back**.



D.5 Remote stand-by via the Tunix support help desk

- 1 TUNIX will assist the registered **contact** of ACME in case of security or firewall related questions, malfunctions to the managed-firewall or disruptions of the *managed firewall service*.
- 2 This agreement obliges TUNIX to support under the following conditions:
 - a Follow-up for assistance with urgent malfunctions (at least one of the active components of the system does in the opinion of ACME no longer function). This assistance has the highest priority, will be picked up post-haste and has the following maximum reaction time of 8 office hours, on weekdays between 09.00h and 17.00h (**coverage**)
 - b Follow-up for assistance during less severe malfunctions (system is still functioning but in a limited fashion) in mutual agreement.
 - c Follow-up for support with general questions, assistance with policy management and the like in mutual agreement. For these matters TUNIX will contact ACME via email within 2 weekdays after **notification**.
- 3 For assistance with problems that are caused by errors in the **hardware** and/or **software** that was provided by TUNIX, ACME will never be charged.
- 4 The first 2 hours spend to stand-by support as part of D.5 per calendar month are free.
- 5 The time TUNIX spends processing a **service-call** will be charged on subsequent calculation if it exceeds 2 hours in the same calendar month. For issues which are expected to take more than 8 office hours, TUNIX will first provide an estimate.
- 6 In case the 2 hours limit is exceeded, TUNIX will provide a detailed hourly report as an appendix of the invoice for the additional hours. These hours are charged for the standard rate for this type of activities.
- 7 To enable TUNIX to adequately administrate the system, ACME is required to notify TUNIX of any modifications in the configuration or topology which may influence the firewall.



D.6 Maintenance/Monitoring

- 1 TUNIX will monitor the **managed firewall**. **Monitoring** the firewall covers the following aspects:
 - a System-logging and alerting are guarded by TUNIX 7 days a week during office hours. Every morning the logging of the night before is processed. TUNIX will examine the logging for **hacking attempts**. When TUNIX detects a hacking attempt the following actions are taken:
 - If in the opinion of **Tunix support** it is necessary and possible actions are taken to minimize the effect of the hacking attempt.
 - TUNIX will contact one of the **contacts** of ACME and notifies him/her of the hacking attempt.
 - TUNIX has in the execution of its duties all the authorities of an administrator and may for security reasons decide to terminate firewall services. After any such action TUNIX will immediately try to contact the administrator to inform him/her. These actions automatically lead to escalation as described in D.17.
 - Detection of **hacking attempts** will be reported in the monthly reporting (see appendix D.19).
 - b TUNIX installs and maintains software and definition files for anti-virus scanning on the firewall. The safeguarding of the proper updating of the anti-virus software is monitored by TUNIX. In case of a **virus-incident** the following holds:
 - A **virus-incident** may announce itself in various ways. TUNIX is informed via AVP and various Internet sources.
 - When a **virus-incident** occurs TUNIX will react proactively by taking measure to minimize the effects and by activating the virus-scenario. ACME may arrange with TUNIX for additional actions which are carried out under these circumstances.
 - Via the link *Virus Alerts* on www.tunix.nl/news ACME will be kept abreast of any particular details of the **virus-incident**.
 - A **virus-incident** will be closed with an email message to all registered **contacts**.
 - A **virus-incident** will be reported in the monthly reporting (see appendix D.19).
 - c Monitoring of the availability of the firewall. The availability of the firewall is monitored 24/7. When problems arise, TUNIX will:



- contact one of the **contacts** of ACME by phone.
 - Should TUNIX establish that the problem is caused by a disturbance on the **local-loop** or on the Internet, TUNIX will apprise UUNET. In order to enable TUNIX to represent ACME towards the UUNET, ACME must report all contact information and any changes in the UUNET-contract that might affect the firewall to TUNIX. ACME must also enroll TUNIX as an authorised administrator.
- d TUNIX will manually inspect the **managed firewall** on a monthly basis, at a time chosen by **Tunix support**:
- This inspection is carried out remotely.
 - ACME is not required to make any backups prior to this inspection.
 - During this inspection active processes are examined on the system.
 - During this inspection the load of the system is examined. Should in the opinion of **Tunix support** the load approach the capacity of the firewall, TUNIX will notify ACME in the monthly standard reporting (see appendix D.19).
 - The system will be cleaned if necessary by compressing logging and removing any remaining backups.
- 2 TUNIX will plan maintenance activities that do not influence the availability of the *managed firewall service* on its own and carry these activities out on their own initiative.
 - 3 The time spend on **monitoring** will not be charged separately and will **not** be taken of the arranged 2 free support hours.
 - 4 Some maintenance duties (such as planned reboots) lead to a short interruption of connectivity. In case no service-window was arranged for such maintenance duties, a specific time during office hours will be announced one week prior to the event.
 - 5 ACME and TUNIX will determine at what times the system may be rebooted for maintenance, unless service-windows were arranged for this.



D.7 Hardware

- 1 TUNIX guarantees the **hardware** provided as part of the *managed firewall service* during the run of this agreement performs as firewall-platform if prior conditions such as bandwidth, the number of users and user profile do not change. Nevertheless should the **hardware** age prematurely TUNIX will provide a replacement at no charge.
- 2 Should the throughput of the firewall be no longer sufficient because of changes in the aforementioned prior conditions, TUNIX will offer a tender for extension of the contract.
- 3 ACME should install the hardware properly in a room suitable for operational computer equipment. The following conditions apply to such a room:
 - a The temperature of the environment lies within the limits set by the hardware vendor.
 - b The power supply is suitable for feeding computer equipment.
 - c The room is accessible only for authorised personnel.
- 4 When operating the hardware ACME should act according to the user manual of the vendor. The hardware may not be opened or modified by ACME.
- 5 A replacement service applies to the **hardware** during the run of this contract. The costs of a possible necessary (temporary) replacement or repairs by defects are a part of this contract.
- 6 If a hardware-malfunction is detected TUNIX will, if a mirror system is available, activate this system as quickly as possible, though no less than 2 office hours after the malfunction was detected. With this the "managed firewall service" is operational again.
- 7 If there is no mirror system present the *managed firewall service* can only be continued until after the **hardware** has been repaired. In the Netherlands, TUNIX will take care of the repairs and if necessary install a replacement firewall within 8 office hours. Firewalls abroad are serviced under a *Dell Bronze Next Business Day* contract.
- 8 In case of alleged hardware malfunctions, one of the **administrators** of ACME will on location assist TUNIX in the diagnose. The time that TUNIX has to wait for this assistance is not counted as downtime.
- 9 The firewall hardware will be replaced by TUNIX when this contract is extended. Prior to this replacement TUNIX will evaluate the required capacity.



D.8 Technical malfunctions

TUNIX distinguishes the following types of **malfunctions**:

- 1 **Hardware malfunctions** on the managed firewall@ will be solved in accordance with the conditions in paragraph D.7.
- 2 **Software malfunctions** will, if their cause is firewall based, solved in accordance with the conditions in paragraph D.5.
- 3 With **Software malfunctions** that are caused by **upgrades** a **roll back** will be performed within 8 office hours after the problem was detected. TUNIX will subsequently attempt to fix the malfunction after which the **upgrades** procedure will be started again.
- 4 For **external malfunctions** (for instance caused by routers or configuration errors on the internal network or system administration conducted by ACME) a response time applies of 4 uur.

D.9 Backups

- 1 During installation TUNIX will make a complete backup of the firewall **software** and its configuration files.
- 2 During the run of this agreement TUNIX will make a **secure off-site configuration backup** of the configuration files of the firewall to the backup server TUNIX has equipped for this on a **regular basis**.
- 3 By default, no backups are made of log files and/or mailboxes. Additional arrangements can be made should this be desired. Such arrangements are considered not to be made unless a separate **backups** appendix is attached to this agreement.



D.10 Registration contacts

Problems and requests for modification of the configuration may only be put forward to TUNIX Support by registered contacts of ACME. When this agreement is entered into ACME is required to fill in the following list:

Contact	Name	Phone	Function
Administrative contact			
Technical contact 1			
Technical contact 2			
Technical contact 3			
Technical contact 4			

A request for altering the contacts should be put forward in writing by the **Administrative contact**. The appropriate fax mutation-forms are available on our website www.tunix.nl.

At least one of these contacts is required to be available for TUNIX to contact during the coverage of this agreement.



D.11 Support requests

Registered contacts (see paragraph D.10) should report urgent malfunctions in two ways:

- a An email to `fwsupport@tunix.nl` with a short problem description and the contract number. Should email not function ACME is required to send a fax labelled clearly *URGENT* to number 024-3455013.
- b Also a confirmation by telephone to TUNIX on number 0900-FWSUPPORT expressly referring to the type of contract, the contract number (MF999), The category the problem falls into (see paragraph D.5, item 2a or 2b) and a short problem description.
- c Less urgent problems and assistance requests may optionally be sent by email only to `fwsupport@tunix.nl`.

Logging of the support calls occurs by establishing the time of the phone **notification** or fax or email transmission.

TUNIX cannot guarantee the **follow-up** within the agreed time frame should this procedure not be followed fully and correctly.

D.12 Remote access

- 1 TUNIX will provide and maintain a service (VPN) which enables her to carry out maintenance on the system remotely and in a secure manner.
- 2 ACME will use an Internet connection at UUNET which can be used by TUNIX for the stated service.
- 3 The Internet VPN connection may drop during calamities. TUNIX will therefore install a fallback modem in the firewall at no extra charge. ACME will, on her own account, install a dedicated PSTN-line (analog), suitable for data, that can be dialed into.
- 4 To communicate with your system (also with dialup access) TUNIX uses one-time passwords and encrypted sessions (VPN) using SSL certificates. The price of the certificate is a part of the contract.



D.13 Exclusions / Requirements

- 1 TUNIX carries out the daily maintenance of the **managed firewall** and reports if something is not functioning correctly. Within this agreement however only the aforementioned administrator's activities are carried out. Activities that therefore are not covered by this agreement are:
 - a The solving of problems that are caused for instance by internal systems, service-network systems and systems of providers.
 - b Postmaster activities due to incorrect addressing.
 - c The maintenance of authorisation data.
 - d The carrying out of modifications to the network.
- 2 TUNIX can only guarantee the provisions described in paragraph D.5 and paragraph D.15 when ACME has **qualified personnel available** for assistance. after **notification** of a problem and during **upgrades or updates**.
- 3 The environmental requirements for the correct functioning of the **hardware** are described in paragraph D.7.
- 4 Fall-back after fire or other calamities which make it necessary to move the **managed firewall** are expressly not part of this contract. ACME needs to take measures if such issues should be covered. In such cases TUNIX guarantees that at request, within 8 hours after **notification**, a functionally similar firewall will be delivered on any location within the Netherlands. Any further assistance that might be needed in such cases, will be charged at the standard hourly rate. ACME should realize that more factors play a role such as the availability of alternative Internet connections, configuration adjustments, etc.
- 5 Improperly maintenance activities of local **administrators** may lead to extensive amounts of alerts. Under such circumstances TUNIX is entitled to terminate the monitoring functions temporarily. TUNIX will immediately notify ACME of such an event. A 24 hour waiting period applies before this extreme measure is carried out.
- 6 As part of this agreement TUNIX provides and maintains among other things third party software. TUNIX is obliged to provide these software components for as long as possible. Should the third party decide to discontinue the product (under the same conditions or with the same quality) TUNIX may in consultation with ACME offer an alternative product that offers the same functionality, or remove this functionality. The price of this component will then be deducted.



D.14 Availability of the TFB helpdesk

The availability of TUNIX for reporting technical malfunctions is described in paragraph D.16. To this end a general availability of 99,8% per kwartaal during your **coverage** is guaranteed.

TUNIX has an alternative support location at her disposal. All its internal systems have a redundant setup in order to be able to always resume TUNIX services to ACME within 2 work hours.

D.15 General availability of the managed firewall service

TUNIX guarantees a general availability of the **managed firewall** of 99,8% per kwartaal excluding service windows and other predetermined service moments. This availability does **not** hold in case of malfunctions that are caused by external factors, such as power failures, deliberate intent or negligence, misappropriation and the like, or in cases of malfunctions that are caused by the actions of **administrators** of ACME.

To insure an uptime of the **managed firewall** that is as high as possible, TUNIX took the following measures:

- To minimize the downtime of the firewall in case of a malfunction the most vulnerable components (disks) are equipped as removables.
- The firewall is delivered with a duplicate so that in case of a malfunction of the master, the mirror can be configured to immediately take over its services.
- TUNIX guarantees in accordance with paragraph D.7 that a (temporary) firewall will be made available when repairs are not an option.



D.16 Contacting TUNIX

TUNIX can be reached through the following channels:

how	identification	availability
email	fwsupport@tunix.nl	24x7
phone	024-3455012 OR 0900-FWSUPPORT (is 0900-397877678)	coverage
fax	024-3455013	24x7
phone	0900-FWSUPPORT (is 0900-397877678)	24x7 for serious calamities

Only registered **contacts** of ACME who refer to the **contract number** may issue support requests.

D.17 Escalation

Should ACME be dissatisfied with the service or when ACME is of the opinion that a response time was not met, ACME may escalate to the escalation manager.

Escalation requests are only accepted when they are put forward by registered **contacts** of ACME who refer to the **ticket number** and the **contract number**.

Automatic escalation occurs when the response time is exceeded.

how	identification	availability
email	escalatie@tunix.nl	24x7
phone	024-3455012 OR 0900-FWSUPPORT (is 0900-397877678)	coverage
fax	024-3455013	24x7
phone	0900-FWSUPPORT (is 0900-397877678)	24x7 for serious calamities



D.18 Reliability

- 1 TUNIX employees are at all times able to identify themselves using a valid ID card. Furthermore, TUNIX employees have signed a non-disclosure agreement and an acceptable use policy (AUP). Also each TUNIX employee has submitted a *verklaring ontrent gedrag* (a certificate of moral conduct) from which no objections emerged for the execution of his/her duties.
- 2 Physical access to the offices of TUNIX is possible only for authorised personnel. The computer rooms and other security-sensitive spaces are electronically protected.
- 3 Storage of the **secure off-site configuration backup** occurs (as described in paragraph D.9) via encrypted connections. The stored configuration files are encrypted separately.

D.19 Reporting

Reporting on firewall usage is automated and will be distributed on a monthly basis no later than 10 weekdays after the month that is covered in the report. The report will be based on the log and export facilities of the firewall and will be emailed in a format decided by ACME (comma separated, dbf or welf).

For advice and maintenance with regard to this reporting ACME may call for assistance using the services as described in paragraph D.5. Included in the report are:

- 1 An overview from **upgrades** carried out.
- 2 An overview per **virus-incident**.
- 3 An overview of **hacking attempts**.
- 4 A report of the manual inspection of the **managed firewall** as described in paragraph D.6.
- 5 An overview of service calls, with response time, closing time and a brief description.
- 6 A List of system administration activities carried out by TUNIX.
- 7 Escalation report.



D.20 General Terms

Applying to all our services and deliveries are the General Conditions of the Federation of Dutch Branch Associations for Information Technology (FENIT) as deposit date December 8th, 1994 at the Registry of the District Court in The Hague under number 1994/189 (available on request free of charge).

D.21 English Language

The official language of this Agreement is Dutch. It is the express wish of ACME that this Agreement and any related documents be drawn up in English. Should the English text of this Agreement deviate from the Dutch version, the Dutch text shall always prevail.

D.22 Definitives

follow-up

The active processing of and working on a service-call by a specialist.

hardware

The equipment provided by TUNIX as part of the *Managed Firewall Service*.

local-loop

The connection between the firewall and the local connection point of the ISP. This connection may consist of dialup lines, routers, converters, multiplexers and other network equipment used by the ISP.

managed firewall

The TUNIX firewall that is covered by this contract.

roll back

To undo (the effects of) an **update**, **upgrade** or an other **software** modification in the **managed firewall** configuration.

service-call

A **service-call** is the follow-up on a call as part of D.5.

service windows

that are possible included in a separate appendix. The **agreed upon** times during which **upgrades/updates** or changes in the configuration may be carried out.



software

The system and proxy software installed by TUNIX as part of the *Managed Firewall Service* on the **hardware**.

updates

In general minor **software** modifications such as applying security patches, bugfixes and the renewing of the filter tables.

upgrades

In general major **software** modifications such as the **software** that is developed by TUNIX and which is standard included in a new firewall, as well as newer versions of existing packages.

virus-incident

New knowledge of a fast spreading new virus with a great technical impact.

D.23 Term, termination and costs of the agreement

This *managed firewall service* agreement is subsumed in 1 januari 2004. The agreement is valid for an initial period of 3 years. After that it is automatically extended for a new period of 3 years unless one of the parties cancels the agreement no later than three months before the end of the term of the agreement. Cancellation must always be done in writing and by recorded mail.

The costs for this agreement are EUR .**,- (excl. VAT) per month. Billing occurs every month in advance.

Should ACME be behind in payment TUNIX may suspend the *managed firewall service* without judicial intervention. ACME will in that case still owe TUNIX the costs of collections and the costs of the agreement.

In case of bankruptcy, suspension of payment or liquidation of TUNIX ACME is entitled to take over the equipment and the software for the residual value in order to take over the existing service.

In case of bankruptcy, suspension of payment or liquidation of ACME TUNIX is entitled to seize the equipment and the software, dissolve the agreement in part or in total or suspend the service, such at the discretion of TUNIX. In such cases every claim TUNIX charges ACME with is immediate and on call.



D.24 Signing

Signatories have examined the contents of this agreement, approve the contacts list (paragraph D.10) and as legally valid representative declare to have concluded this agreement.

(place)

(date)

TUNIX Internet Security & Opleidingen b.v.
On behalf of TUNIX,
Ronald L. Pikkert

A Company Manufacturing Everything, ACITY
On behalf of ACME (please include your name legibly),

