

## E. SLA Managed Firewall Service overeenkomst MF999

### E.1 Partijen

A Company Manufacturing Everything, statutair gevestigd te  
Companylane 12,  
9999 XX ACITY, verder te noemen ACME,

en

TUNIX Internet Security & Opleidingen b.v., statutair gevestigd te  
Wijchenseweg 111,  
6538 SW NIJMEGEN, verder te noemen TUNIX,

beide partijen in deze rechtsgeldig door ondergetekenden vertegenwoordigd, verklaren de volgende niet aan derden overdraagbare Managed Firewall Service overeenkomst te hebben afgesloten.

Deze overeenkomst met contractnummer MF999 is van toepassing op de machine die bekend staat als ns.acme.nl



## E.2 Managed firewall service

TUNIX levert een beheerde en beveiligde netwerkkoppeling met het Internet door:

- 1 Installatie van een firewall zoals beschreven in paragraaf E.3.
- 2 Het onderhouden van deze software zoals beschreven in paragraaf E.4.
- 3 Het bieden van een helpdesk standby voorziening zoals beschreven in paragraaf E.5.
- 4 Het beheren en bewaken van de firewall zoals beschreven in paragraaf E.6.
- 5 Het installeren en onderhouden van de firewall hardware zoals beschreven in paragraaf E.7.

## E.3 Firewall implementatie

- 1 TUNIX levert, configureert en installeert een operationele **managed firewall** die voldoet aan de functionele specificaties zoals beschreven in ons voorstel SS/RP/27573.
- 2 De **managed firewall** wordt door TUNIX turn-key afgeleverd, gemonteerd, getest en gedemonstreerd op de volgende locatie:  
ACME, Companylane 12, 9999 XX ACITY.
- 3 De initiële aanschafprijs van de **managed firewall** is verwerkt in de maandprijs van deze overeenkomst.  
De benodigde **hardware** en **software** wordt in het kader van deze overeenkomst door TUNIX op de genoemde locatie ingezet ten behoeve van de *managed firewall service*, maar blijft eigendom van TUNIX. Bij beëindiging van het gebruik zal ACME de beschikbaar gestelde **hardware** in goede staat aan TUNIX doen toekomen.
- 4 De in ons voorstel opgenomen calculaties zijn alleen bedoeld als grondslag voor de in deze overeenkomst genoemde management-prijs, tenzij expliciet anders vermeld.



#### E.4 Software onderhoud

- 1 In het kader van dit contract wordt de genoemde **firewall-software** door TUNIX periodiek voorzien van security patches, bugfixes e.d. Deze werkzaamheden worden aangeduid met de term: **updates**.
- 2 Met dit contract wordt de genoemde **firewall-software** periodiek voorzien van nieuwe **software** die TUNIX ontwikkelt en die standaard met een firewall uitgeleverd wordt. Deze werkzaamheden worden aangeduid met de term: **upgrades**.
- 3 TUNIX zal beschikbare **updates** en **upgrades** op de genoemde firewall installeren en zorgen voor integratie in de bestaande omgeving. De **updates** en **upgrades** zullen worden geïnstalleerd maximaal 1 maand nadat deze zijn opgenomen in de **standaard** firewall **software**.
- 4 **Updates** en **upgrades** die uit security overwegingen spoedeisend zijn, zullen altijd zo snel mogelijk worden geïnstalleerd.
- 5 Door het leveren en installeren van **updates** en **upgrades** houdt TUNIX de firewall-**software** op hetzelfde functionele niveau als de **software** van firewalls die zij op dat moment als *standaard* uitlevert.  
Na installatie en integratie maken **updates** cq. **upgrades** deel uit van de firewall maar zijn niet actief tenzij zij een bestaande, actieve component vervangen. De bestaande functionaliteit van de firewall blijft behouden. TUNIX zal een advies geven of, en zo ja, hoe de nieuwe functies gebruikt kunnen worden. Het activeren en configureren van nieuwe functies zal alleen na opdracht van ACME worden uitgevoerd.
- 6 Het installeren van **updates** en **upgrades** voor geleverde standaard modules (zoals de geïnstalleerde virus-scanner die SMTP verkeer op virussen scant) maakt onderdeel uit van deze overeenkomst. ACME mag het aantal van 1000 door de firewall beschermde mailboxen niet overschreiden.
- 7 Indien ACME vaste **service windows** wenst af te spreken zullen deze in een aparte bijlage worden vastgelegd. Indien geen aparte bijlage **service windows** aan deze overeenkomst is toegevoegd worden dergelijke afspraken geacht niet te zijn gemaakt en kan TUNIX zelfstandig **service windows** inplannen.
- 8 Werkwijze uitvoering **upgrades** (chronologisch):
  - a TUNIX kondigt **upgrades** ten minste twee weken van te voren aan. In deze aankondiging wordt aangegeven op welke onderdelen van de **software** de veranderingen/uitbreidingen betrekking hebben en welke implicaties dit heeft. Verder wordt aangegeven vanaf welke datum de installatie van de **upgrades** zal plaatsvinden.
  - b ACME kan vóór de datum van de geplande **upgrades** contact opnemen met **TFB** om een ander tijdstip af te spreken (binnen kantooruren). Wanneer ACME hierover geen contact opneemt, voert TUNIX de upgrade uit op een zelf gekozen moment.



- c Direct voorafgaand aan **upgrades** bevestigt TUNIX één van de **contactpersonen** van ACME dat de **upgrades** zullen worden uitgevoerd. Wanneer geen enkele **contactpersoon** bereikbaar is, zal TUNIX aanvangen met de upgrade.
  - d TUNIX maakt vooraf een lokale en een off-site backup van de configuratie.
  - e TUNIX verifieert vooraf of de configuratie, inclusief eventuele mirror of parallele systemen, in orde is. Indien de configuratie naar mening van TUNIX niet orde is, worden de **upgrades** niet uitgevoerd alvorens contact opgenomen te hebben met één van de **contactpersonen**.
  - f TUNIX voert de **upgrades** uit en meldt aan een **contactpersoon** van ACME dat de werkzaamheden zijn uitgevoerd.
  - g TUNIX maakt een lokale en een off-site backup van de configuratie.
  - h TUNIX verifieert of de configuratie werkt nadat de **upgrades** zijn uitgevoerd.
  - i TUNIX zal na **upgrades**, waarbij functionaliteit zodanig is gewijzigd of uitgebreid dat dit wenselijk is, aanvullende documentatie van de firewall (manuals, release notes, configuratie consequenties) ter beschikking stellen aan ACME.
- 9 Wanneer een storing optreedt die mogelijk het gevolg is van een **upgrade/update** is te allen tijde een **roll back** mogelijk. Voor het uitvoeren van de **roll back** geldt een responsetijd voor ernstige storingen, zoals omschreven in paragraaf E.5.

#### E.5 Remote stand-by door de TFB help-desk

- 1 TUNIX zal geregistreerde **contactpersonen** van ACME bijstaan in geval van security- of firewall gerelateerde vragen, storingen aan de managed-firewall, of onderbreking van de *managed firewall service*.
- 2 Dit contract verplicht TUNIX tot support onder de volgende condities:
  - a Follow-up voor assistentie bij urgente storingen (minimaal één van de productie genomen componenten van het systeem functioneert naar mening van ACME niet meer). Deze assistentie krijgt de hoogste prioriteit, wordt met de meeste spoed opgepakt en kent een maximale reactietijd van 8 werkuren, op werkdagen tussen 09.00 uur en 17.00 uur (**dekkingstijd**)
  - b Follow-up voor assistentie bij minder ernstige storingen (het systeem functioneert nog, maar met beperkingen) in wederzijds overleg.
  - c Follow-up voor ondersteuning bij algemene vragen, assistentie bij policy-management en dergelijke in wederzijds overleg. TUNIX zal voor deze zaken binnen maximaal 2 werkdagen na **aanmelding** (e-mail) contact met ACME opnemen.
- 3 Bij assistentie inzake problemen die worden veroorzaakt door fouten in de door TUNIX geleverde firewall **hardware** en **software** worden nooit kosten in rekening gebracht.
- 4 De eerste 2 uren besteed aan stand-by support in het kader van E.5 per kalendermaand zijn gratis.
- 5 De tijd die TUNIX aan de behandeling van een **service-call** besteedt, wordt, indien hiervoor in de betreffende kalendermaand meer dan 2 uur nodig zijn, op basis van nacalculatie verrekend. Voor zaken die naar het zich laat aanzien meer dan 8 werkuren vergen, zal TUNIX vooraf een raming afgeven.
- 6 Bij overschrijding zal TUNIX als bijlage bij de aanvullende factuur een gedetailleerde urenrapportage verstrekken. Deze uren worden doorbelast tegen het geldende standaard tarief voor configuratie-werkzaamheden.
- 7 Om TUNIX in staat te stellen het systeem adequaat te beheren dient ACME door haar zelf uitgevoerde **configuratie- en topologie-wijzigingen** die de firewall kunnen beïnvloeden aan TUNIX te melden.



## E.6 Beheer/bewaking

- 1 TUNIX zal de **bewaking** van de **managed firewall** op zich nemen. Onder deze **bewaking** vallen de volgende aspecten:
  - a Bewaking van systeem-logging en alerting worden door *TUNIX/heartbeat*, 7 dagen per week gedurende alle uren van de dag op continue basis uitgevoerd. Evaluatie en opvolging door **TFB** vindt 7 dagen per week gedurende kantooruren plaats. Elke morgen wordt de logging van de afgelopen nacht alsnog geanalyseerd. De firewall logging zal worden beoordeeld op **hackpogingen**. TUNIX zal bij de constatering van **hackpogingen**:
    - Indien dit naar het oordeel van **TFB** mogelijk en noodzakelijk is, actie ondernemen om de eventuele gevolgen van deze **hackpogingen** minimaliseren.
    - TUNIX neemt contact op met een van de **contactpersonen** van ACME en voorziet deze van informatie over de **hackpogingen**.
    - TUNIX heeft bij het uitvoeren van haar taken de normale bevoegdheden van een beheerder en mag om redenen van security bijvoorbeeld besluiten firewall diensten te stoppen. Na een dergelijke actie zal TUNIX meteen proberen de beheerder te informeren. Tevens leiden deze acties automatisch tot escalatie zoals beschreven in E.17.
    - Constatering van **hackpogingen** wordt vermeld in de maandelijkse rapportage (zie bijlage E.19).
  - b TUNIX installeert en onderhoudt de software en de definitie-bestanden van Kasperski Anti Virus voor anti-virus scanning op de firewall. De bewaking van het juist verlopen van **updates** van anti-virus software wordt door TUNIX bewaakt. Inzake een **virus-incident** geldt:
    - Een **virus-incident** kan op verschillende manieren bij TUNIX bekend worden. TUNIX informeert zich via KAV en diverse bronnen op het Internet.
    - Als zich een **virus-incident** voordat, zal TUNIX pro-actief reageren door maatregelen te nemen om de gevolgen zoveel mogelijk te beperken en het virus-draaiboek te activeren. ACME kan met TUNIX afspraken maken over aanvullende acties die onder deze omstandigheden door TUNIX moeten worden uitgevoerd.
    - Via de link *Virus Alerts* op [www.tunix.nl/news](http://www.tunix.nl/news) wordt ACME op de hoogte gehouden over bijzonderheden inzake het **virus-incident**.
    - Een **virus-incident** wordt afgesloten met een mailbericht naar alle geregistreerde **contactpersonen**.
    - Een **virus-incident** wordt vermeld in de maandelijkse rapportage (zie bijlage E.19).



- c Het controleren van de bereikbaarheid van de firewall. De bereikbaarheid wordt 24 uur per dag gemonitord. Bij problemen zal TUNIX:
- Telefonisch contact opnemen met een van de **contactpersonen** van ACME.
  - Indien TUNIX vaststelt dat het probleem wordt veroorzaakt door een storing op de **local-loop** of op het Internet, zal zij UUNET op de hoogte stellen. Om TUNIX in staat te stellen om richting UUNET als contactpersoon op te treden moet ACME contactinformatie en wijzigingen in het UUNET-contract, die de firewall kunnen beïnvloeden, aan TUNIX melden. Tevens dient ACME TUNIX aan te melden als geautoriseerd beheerder.
- d TUNIX verzorgt maandelijks, op een door **TFB** te verkiezen moment, een handmatige inspectie van de **managed firewall**:
- Deze inspectie wordt remote uitgevoerd.
  - ACME hoeft voorafgaande aan deze inspectie geen backup te maken.
  - Tijdens deze inspectie wordt gekeken naar de actieve processen op het systeem.
  - Tijdens deze inspectie wordt gekeken naar de belasting van het systeem. Indien de belasting naar de mening van **TFB** de capaciteit van de firewall nadert zal TUNIX ACME hierover via de standaard rapportage (bijlage E.19) informeren.
  - Indien nodig wordt het systeem opgeschoond door bijvoorbeeld logging te comprimeren en achtergebleven backups te verwijderen.
- 2 TUNIX zal beheer-werkzaamheden die de beschikbaarheid van de *managed firewall service* niet beïnvloeden zelfstandig inplannen en op eigen initiatief uitvoeren.
- 3 De tijd die aan de **bewaking** wordt besteed, wordt niet apart doorbelast en gaat **niet** ten koste van de afgesproken 2 gratis support-uren.
- 4 Sommige onderhoudstaken (zoals geplande reboots) leiden tot een korte stagnatie van de connectiviteit. Voor dergelijke onderhoudstaken zal, indien geen service-window is afgesproken, één week vooraf een tijdstip tijdens kantooruren worden aangekondigd.
- 5 In overleg tussen ACME en TUNIX wordt bepaald op welk moment het systeem voor onderhoud gereboot kan worden, tenzij hiervoor service-windows zijn afgesproken.



## E.7 Hardware

- 1 TUNIX garandeert dat de in het kader van de *managed firewall service* geleverde **hardware** gedurende de looptijd van deze overeenkomst als firewall-platform voldoet indien randvoorwaarden als bandbreedte, aantal gebruikers en gebruiksprofiel ten opzichte van de initiële situatie niet wijzigen. Mocht de **hardware** desondanks vroegtijdig verouderen dan zal TUNIX voor eigen rekening voor vervanging zorgdragen.
- 2 Indien de throughput van de firewall door wijzigingen van de genoemde randvoorwaarden niet langer toereikend is, dan zal TUNIX een voorstel tot uitbreiding van het contract aanbieden.
- 3 ACME moet voor haar eigen rekening TUNIX in staat stellen de apparatuur te monteren in een ruimte die geschikt is voor operationele computerapparatuur. Voor zo'n ruimte gelden de volgende condities:
  - a De omgevingstemperatuur ligt binnen de door de fabricant van de hardware opgegeven grenzen.
  - b De stroomvoorziening is geschikt voor het voeden van computerapparatuur.
  - c De ruimte is alleen toegankelijk voor geautoriseerde personen.
- 4 ACME moet bij het bedienen van de apparatuur handelen conform de gebruiksaanwijzing van de leverancier en moet deze als een goed huisvader beheren en verzorgen. De apparatuur mag door ACME niet worden geopend of gemodificeerd en merktekens of aanduidingen mogen niet worden verwijderd. Verplaatsing van de apparatuur is alleen met toestemming van TUNIX toegestaan.
- 5 Op de **hardware** is, gedurende de looptijd van dit contract, vervangingservice van toepassing. De kosten van eventuele noodzakelijke (tijdelijke) vervanging of reparatie bij **hardware storingen** zijn onderdeel van dit contract.
- 6 Indien een hardware-storing wordt geconstateerd zal TUNIX, indien een mirror-systeem beschikbaar is, dit systeem zo snel mogelijk toch uiterlijk binnen 2 kantooruren na de vaststelling van de storing activeren. Hiermee is de *managed firewall service* weer operationeel.
- 7 Indien geen mirror-systeem aanwezig is, kan de *managed firewall service* pas worden hersteld nadat de **hardware** is gerepareerd. TUNIX zal hiertoe binnen 8 kantooruren een monteur de reparatie laten uitvoeren en zo nodig een vervangende firewall laten installeren.
- 8 In geval van vermeende hardware-storingen zal een van de **beheerders** van ACME TUNIX op locatie bijstaan in de diagnose. De tijd die TUNIX op deze ondersteuning moet wachten geldt niet als downtime.
- 9 De firewall-hardware zal bij verlenging van dit contract door TUNIX worden vervangen. Voorafgaande aan deze vervanging zal TUNIX de benodigde capaciteit met ACME evalueren.



## E.8 Storingen

Bij storingen wordt onderscheid gemaakt tussen verschillende soorten **storingen**:

- 1 **Hardware storingen** op de **managed firewall** worden opgelost overeenkomstig de afspraken in paragraaf E.7.
- 2 **Software storingen** worden, wanneer zij op de firewall hun oorsprong vinden, opgelost overeenkomstig de afspraken in paragraaf E.5.
- 3 Bij **software storingen** die worden veroorzaakt door **upgrades** wordt binnen 8 kantooruren na constatering van het probleem een **roll back** uitgevoerd. Vervolgens zal TUNIX trachten zo snel mogelijk de storing te verhelpen, waarna de procedure voor het uitvoeren van de **upgrades** opnieuw wordt gestart.
- 4 Voor **externe storingen** (veroorzaakt door bijvoorbeeld routers of configuratiefouten op het interne netwerk of door ACME verricht beheer) geldt een responsetijdgarantie van 4 uur.

## E.9 Backups

- 1 Bij installatie wordt door TUNIX een volledige backup van de firewall-**software** en configuratie-bestanden gemaakt.
- 2 TUNIX zal gedurende de looptijd van deze overeenkomst op **regelmatige basis** een **secure off-site configuratie backup** van de configuratie bestanden van de firewall maken naar de backup-server die TUNIX hiervoor heeft ingericht.
- 3 Er worden standaard geen backups gemaakt van logfiles en/of mailboxen. Indien dit wenselijk is kunnen hierover aanvullende afspraken worden gemaakt. Indien hiertoe geen aparte bijlage **backups** aan deze overeenkomst is toegevoegd worden dergelijke afspraken geacht niet gemaakt te zijn.



### E.10 Registratie contactpersonen

Problemen en verzoeken tot wijziging van de configuratie kunnen alleen bij TUNIX Support worden aangemeld door geregistreerde contactpersonen van ACME. Bij het afsluiten van deze overeenkomst dient ACME in onderstaande lijst de contactpersonen in te vullen.

Contactpersoon	Naam	Telefoon	Functie
Administratief contactpersoon			
Technisch contactpersoon 1			
Technisch contactpersoon 2			
Technisch contactpersoon 3			
Technisch contactpersoon 4			

Een verzoek tot het wijzigen van contactpersonen dient schriftelijk te geschieden door de **administratief contactpersoon**. De hiervoor te gebruiken fax-mutatieformulieren zijn via onze website [www.tunix.nl](http://www.tunix.nl) op te vragen.

Gedurende de dekkingstijd van deze overeenkomst dient minimaal één van de contactpersonen voor TUNIX bereikbaar te zijn.



## E.11 Support verzoeken

Geregistreerde contactpersonen (zie paragraaf E.10) dienen urgente storingen aan te melden via twee wegen:

- a Een e-mail naar `fwsupport@tunix.nl` met een korte omschrijving én het contractnummer. Indien e-mail niet functioneert dient ACME een fax met de duidelijke kop *SPOED* te sturen naar nummer 024-3455013.
- b Bovendien een telefonische bevestiging naar TUNIX op nummer 0900-FWSUPPORT, onder nadrukkelijke vermelding van het type contract, het contractnummer (MF999), de categorie waarin het probleem valt (zie paragraaf E.5, punt 2a of 2b) en een korte beschrijving van het probleem.
- c Minder urgente problemen en assistentie verzoeken mogen eventueel via alléén e-mail naar `fwsupport@tunix.nl` worden aangemeld.

Logging van de support verzoeken vindt plaats door het tijdstip van de telefonische **aanmelding** of het tijdstip van de verzending van de fax of e-mail vast te leggen.

Indien de bovenstaande procedure niet volledig en correct wordt gevolgd, kan TUNIX niet garanderen dat de **follow-up** binnen de afgesproken tijd plaatsvindt.

## E.12 Remote access

- 1 TUNIX zal een voorziening (VPN) maken en in stand houden die het haar mogelijk maakt om het onderhoud op het systeem op een veilige manier op afstand uit te voeren.
- 2 ACME zal een Internet voorziening afnemen bij UUNET die door TUNIX voor voorgenoemde dienst kan worden gebruikt.
- 3 Bij calamiteiten kan de Internet VPN-verbinding uitvallen. Daarom zal naast de VPN-verbinding voor rekening van TUNIX een fall back modem aan de firewall worden gekoppeld. Hiervoor zal ACME voor haar eigen rekening een dedicated en extern aankiesbare PSTN-lijn (analoog) aanleggen, geschikt voor data.
- 4 De communicatie met uw systeem (ook bij dialup toegang) geschiedt op afstand met one-time passwords en encrypted sessies (VPN) met behulp van SSL certificaten. De prijs van het certificaat is onderdeel van het contract.



### E.13 Uitsluitingen / Vereisten

- 1 TUNIX zorgt voor de dagelijkse controle van de **managed firewall** en rapporteert indien er iets niet correct functioneert. Binnen deze overeenkomst worden echter alleen eerdergenoemde beheerwerkzaamheden uitgevoerd. Werkzaamheden die derhalve niet onder dit contract vallen zijn:
  - a Het oplossen van storingen die worden veroorzaakt door bijvoorbeeld interne systemen, service-netwerk systemen en systemen van providers.
  - b Postmaster werkzaamheden ten gevolge van onjuiste adressering.
  - c Het onderhouden van de autorisatie-gegevens.
  - d Het uitvoeren van wijzigingen aan het netwerk.
- 2 TUNIX kan de in paragraaf E.5 en paragraaf E.15 genoemde zaken aléén garanderen wanneer ACME, na **aanmelding** van een probleem en bij **upgrades** of **updates**, **gekwalificeerd personeel ter beschikking** heeft voor assistentie.
- 3 De omgevingseisen voor het correct functioneren van de **hardware** worden in paragraaf E.7 beschreven.
- 4 Uitwijk na brand of andere calamiteiten, die het noodzakelijk maken om de **managed firewall** te verplaatsen, zijn uitdrukkelijk niet geregeld. Hiervoor dient ACME zelf maatregelen te treffen. TUNIX garandeert in dat geval wel binnen 8 uur na **aanmelding** een functioneel gelijkwaardige firewall op elke lokatie in Nederland te kunnen leveren, alsmede assistentie ter plaatse door een consultant, tegen vergoeding op basis van nacalculatie tegen de hiervoor geldende tarieven. ACME dient zich te realiseren dat hierbij veel meer zaken een rol spelen, zoals de beschikbaarheid van alternatieve Internet-verbindingen, configuratie-instellingen etcetera.
- 5 Onjuist uitgevoerde activiteiten van de lokale **beheerders** kunnen leiden tot omvangrijke hoeveelheden alarmeringen. Indien dergelijke omstandigheden zich voordoen is TUNIX gerechtigd om de bewakingsfunctie tijdelijk te staken. TUNIX zal hiervan in voorkomende gevallen terstond melding maken. Voor het ten uitvoer brengen van deze extreme maatregel geldt een wachttijd van 24 uur na de bovengenoemde melding.
- 6 In het kader van deze overeenkomst levert en onderhoudt TUNIX ondermeer third party software. TUNIX verplicht zich deze software-componenten zolang mogelijk te blijven leveren. Indien de third party besluit om het product niet langer (onder dezelfde condities of met dezelfde kwaliteit) te leveren mag TUNIX in overleg met ACME een alternatief product leveren dat dezelfde functionaliteit biedt, of de betreffende functionaliteit schrappen. Een hiervoor in deze overeenkomst opgenomen meerprijs zal dan worden verrekend.



#### E.14 Beschikbaarheid van de TFB helpdesk

De bereikbaarheid van TUNIX voor het melden van storingen staat beschreven in paragraaf E.16. Hiervoor is gedurende de **dekkingstijd** een algemene beschikbaarheid van 99,8% per kwartaal gegarandeerd.

TUNIX beschikt over een uitwijkprocedure en een uitwijklocatie en heeft haar interne systemen redundant ingericht teneinde in het geval van ernstige calamiteiten haar dienstverlening aan ACME binnen 2 werkuren te kunnen voortzetten.

#### E.15 Algemene beschikbaarheid van de managed firewall service

TUNIX garandeert een algemene beschikbaarheid van de **managed firewall** van 99,8% per kwartaal, uitgezonderd service-windows en andere afgesproken service-momenten. Deze beschikbaarheid geldt **niet** in geval van storingen met een externe oorzaak, zoals stroomstoringen, opzet of grove nalatigheid, malversatie en dergelijke, of in geval van storingen, ontstaan door het handelen van **beheerders** van ACME.

TUNIX heeft de volgende maatregelen genomen om een zo hoog mogelijke uptime van de **managed firewall** te realiseren:

- De meest kwetsbare componenten (disken) worden removable uitgevoerd om in geval van een storing aan de firewall de downtijd zoveel mogelijk te reduceren.
- De firewall wordt volledig dubbel uitgevoerd zodat in geval van storing aan de master meteen kan worden overgeschakeld op de mirror.
- TUNIX garandeert overeenkomstig paragraaf E.7 dat zij (tijdelijk) een vervangende firewall beschikbaar stelt, als reparatie niet mogelijk is.



## E.16 Bereikbaarheid

TUNIX is via de volgende kanalen te bereiken:

hoe	identificatie	bereikbaarheid
email	fwsupport@tunix.nl	24x7
telefoon	024-3455012 OF 0900-FWSUPPORT (is 0900-397877678)	<b>dekkingstijd</b>
fax	024-3455013	24x7
telefonisch bij ernstige calamiteiten	0900-FWSUPPORT (is 0900-397877678)	24x7

Voor alle verzoeken om support geldt: alleen door geregistreerde **contactpersonen** van ACME en onder verwijzing naar het **contractnummer**.

## E.17 Escalatie

Indien ACME ontevreden is over de dienstverlening of wanneer ACME van mening is dat een responsetijd niet wordt gehaald, is er de mogelijkheid te escaleren naar de escalatiemanager.

Escalatieverzoeken worden alleen aangenomen van geregistreerde **contactpersonen** van ACME, onder verwijzing naar het **ticketnummer** en het **contractnummer**.

Er vindt automatisch escalatie plaats wanneer de responsetijd wordt overschreden.

hoe	identificatie	bereikbaarheid
email	escalatie@tunix.nl	24x7
telefoon	024-3455012 OF 0900-FWSUPPORT (is 0900-397877678)	<b>dekkingstijd</b>
fax	024-3455013	24x7
telefonisch bij ernstige calamiteiten	0900-FWSUPPORT (is 0900-397877678)	24x7



### E.18 Betrouwbaarheid

- 1 TUNIX personeel kan zich te allen tijde legitimeren met een identiteitsbewijs. Bovendien heeft TUNIX personeel een geheimhoudingsverklaring en een *acceptable use policy* (AUP) ondertekend, en heeft elke TUNIX medewerker een *verklaring omtrent gedrag* overlegd waaruit geen bezwaar is gebleken voor het uitoefenen van zijn of haar functie.
- 2 Fysieke toegang tot ruimtes van TUNIX is slechts mogelijk voor geautoriseerd personeel. De computerruimtes en andere security-gevoelige ruimtes zijn bovendien elektronisch beveiligd.
- 3 Opslag van de **secure off-site configuratie backup** gebeurt (zoals beschreven in paragraaf E.9) over versleutelde verbindingen en ook de opgeslagen bestanden worden separaat versleuteld.

### E.19 Rapportage

Rapportage over het gebruik van de firewall is geautomatiseerd en wordt maandelijks per e-mail beschikbaar gesteld in een door ACME te specificeren formaat (comma separated, dbf of welf) en op basis van de log- en exportfaciliteiten van de firewall, uiterlijk 10 werkdagen na de maand waarover gerapporteerd wordt.

Voor advies en onderhoud inzake deze rapportage kan een beroep worden gedaan op de in paragraaf E.5 beschreven dienstverlening.

In de rapportage zijn opgenomen:

- 1 Een overzicht van uitgevoerde **upgrades**.
- 2 Een overzicht per **virus-incident**.
- 3 Een overzicht van **hackpogingen**.
- 4 Een verslag van de handmatige inspectie van de **managed firewall** zoals beschreven in paragraaf E.6.
- 5 Overzicht van service-calls, met responsetijd, afsluittijd en een korte toelichting.
- 6 Lijst van door TUNIX ondernomen beheeractiviteiten.
- 7 Escalatie rapportage.



## E.20 Algemene Voorwaarden

Van toepassing zijn de Algemene Voorwaarden van de Federatie van Nederlandse Brancheverenigingen voor Informatietechnologie (FENIT) zoals gedeponereerd d.d. 8 december 1994 ter Griffie van de Arrondissementsrechtbank te Den Haag onder nummer 1994/189 (op aanvraag kosteloos verkrijgbaar).

## E.21 Definities

### aanmelding

Het kenbaar maken van een service-call aan TUNIX door **contactpersonen** van ACME via de onder E.16 vermelde wegen, onder vermelding van het **contractnummer**.

### administratief contactpersoon

- a De **administratief contactpersoon** ontvangt van TUNIX een aankondiging met voorinformatie en documentatie inzake voorgenomen of uitgevoerde **upgrades**.
- b Een **administratief contactpersoon** is gerechtigd om wijzigingen door te voeren in de lijst van **contactpersonen**.

### beheerder(s)

Personeel van ACME dat toegang heeft tot de **firewall**, of dat toegang heeft tot de lokatie van de **firewall**, of dat toegang heeft tot apparatuur die is aangesloten op de **firewall** (zoals bijvoorbeeld routers, **local-loop** of console) of de lokatie waar deze apparatuur zich bevindt.

### bewaking

Het lezen en interpreteren van de alertlogging door een getrainde TUNIX functionaris.

### configuratie- en topologie-wijzigingen

Aanpassingen aan- en uitbreidingen van netwerken of netwerkdiensten die gebruik maken van de firewall functionaliteit.

### contactpersonen, contactpersoon

De **beheerders** die door ACME bekend zijn gemaakt aan TUNIX door het invullen van de tabel in paragraaf E.10, of die later bekend zijn gemaakt via de op de TUNIX website gepubliceerde procedure.



**contactpersonen, contactpersoon**

De **beheerders** die door ACME bekend zijn gemaakt aan TUNIX door het invullen van de tabel in paragraaf E.10, of die later bekend zijn gemaakt via de op de TUNIX website gepubliceerde procedure.

**contractnummer**

Het nummer waaronder dit contract bekend is.

**dekkingstijd**

De in artikel E.5 beschreven tijd waarin aanspraak kan worden gemaakt op de overeengekomen responsetijd.

**externe storingen**

De **storingen** die niet niet gelocaliseerd zijn op de **managed firewall**.

**firewall-software**

Door TUNIX als onderdeel van de *Managed Firewall Service* op de **hardware** geïnstalleerde systeem- en proxy-programmatuur teneinde een firewall functionaliteit te creëren al dan niet voorzien van klantspecifieke packages.

**follow-up**

Het door een specialist actief werken aan een service-call.

**gekwalificeerd personeel**

Personeel van ACME dat verantwoordelijk is voor de **managed firewall** en/of assistentie moet verlenen, dient kennis te hebben van alle **hardware, software** en procedures die nodig zijn voor het juist functioneren van de **managed firewall**, zoals netwerkkapparatuur, bekabeling, Internet-verbindingen, toegang tot de computerruimte, etcetera. Personeel van ACME dat toegang moet hebben tot de **managed firewall** dient met goed gevolg de TUNIX-cursus **beheer S2** te hebben gevolgd.

**hackpoging**

Gerichte activiteiten die naar oordeel van **TFB** bedoeld zijn om het correct functioneren van de **managed firewall** te ondermijnen, of om toegang te verkrijgen tot de **managed firewall** of de achterliggende netwerken. **TOELICHTING: portscans, probes, netscans, httpsceenmeldingen** en **virusmeldigen** worden op zichzelf niet als **hackpogingen** beschouwd, maar combinaties van dit soort activiteiten waaruit zou kunnen blijken dat dit om meer gaat dan een automatische inventarisatie zijn dat wel.

**hardware**

Door TUNIX als onderdeel van de *Managed Firewall Service* geleverde apparatuur.

**hardware storingen**

Het zodanig niet of niet goed functioneren van **hardware** dat de reguliere firewall-diensten niet meer beschikbaar zijn. Hieronder valt niet schade door ongelukken, brand, vandalisme of abnormaal gebruik. Dergelijke schade dient onmiddellijk aan TUNIX te worden gemeld en komt voor rekening van ACME.

**kantooruren**

Maandag tot en met vrijdag van 9.00 tot 17.00 uur, uitgezonderd algemeen erkende Nederlandse feestdagen.



**local-loop**

Onder de **local-loop** wordt verstaan de verbinding tussen firewall en het aansluitpunt van de ISP. Deze verbinding kan bestaan uit huur- of dialup-lijnen, routers, convertors, multiplexors en andere door de ISP gebruikte netwerk-apparatuur.

**managed firewall**

De onder dit contract vallende TUNIX firewall.

**regelmatige basis**

Tenminste wekelijks, maar in overleg met ACME anders overeen te komen.

**roll back**

Het ongedaan maken van een **update**, **upgrade**, of enige andere **software**-aanpassing in de **managed firewall**-configuratie.

**secure off-site configuratie backup**

Alle informatie die op een **managed firewall** aanwezig is en die noodzakelijk is voor het configureren van een functioneel equivalente **managed firewall**.

**service-call**

Een **service-call** is follow-up op een call in het kader van E.5.

**service windows**

De eventueel in een aparte appendix vastgelegde tijden waarop na **overleg upgrades/updates** of veranderingen in de configuratie kunnen worden uitgevoerd.

**software**

Door TUNIX als onderdeel van de *Managed Firewall Service* op de **hardware** geïnstalleerde systeem- en proxie-programmatuur.

**standaard**

Bedoeld als standaard software: de software die TUNIX ontwikkelt teneinde een firewall functionaliteit te creëren al dan niet voorzien van klantspecifieke packages.

**storingen**

Niet of gedeeltelijk functioneren van de **managed firewall**, zoals beschreven in paragraaf E.8.

**beschikbaarheid, ter beschikking**

Een van de **contactpersonen** dient, gedurende de looptijd van de overeenkomst, telefonisch bereikbaar te zijn op een bij TUNIX bekend telefoonnummer.

De Managed Firewall Service is beschikbaar als de firewall functionaliteit via *TUNIX/Heartbeat* als zijnde beschikbaar wordt gedetecteerd.

**TFB TUNIX Firewall Beheer**

De afdeling *TUNIX Firewall Beheer*.

**ticketnummer**

De bij een **melding** van TUNIX ontvangen referentie die ACME bij vervolcontact of escalatie van een **storing** dient te vermelden.



**updates**

Over het algemeen kleine **software** aanpassingen zoals het uitvoeren van security patches, bugfixes en de vernieuwing van filtertabellen.

**upgrades**

Over het algemeen grotere **software** aanpassingen zoals nieuwe **software** die TUNIX ontwikkelt en die standaard met een firewall uitgeleverd wordt alsmede nieuwe versies van bestaande packages.

**virus-incident**

Het bekend worden van een zich snel verspreidend nieuw virus met een grote technische impact.

**E.22 Looptijd, beëindiging en kosten van de overeenkomst**

Deze *managed firewall service* overeenkomst gaat in op 1 januari 2004. De overeenkomst wordt afgesloten voor een initiële periode van 3 jaar. Daarna wordt ze automatisch verlengd voor een nieuwe periode van 3 jaar, tenzij een van de partijen de overeenkomst uiterlijk drie maanden voor het einde van de looptijd opzegt. Opzegging dient altijd schriftelijk en aangetekend te geschieden.

De kosten voor deze overeenkomst bedragen EUR .\*\*,- (excl. BTW) per maand. Facturering geschiedt maandelijks vooraf.

In geval er sprake van een betalingsachterstand is TUNIX zonder rechtelijke tussenkomst zelfstandig gerechtigd de *managed firewall service* op te schorten. Dit laat onverlet dat ACME aan TUNIX de kosten van de overeenkomst, alsmede de kosten van invordering verschuldigd blijft.

Indien TUNIX in staat van faillissement, surseance van betaling, stillegging of liquidatie komt te verkeren, is ACME gerechtigd de apparatuur en de software tegen de restwaarde over te nemen om op die manier de bestaande dienst zelf in te vullen.

Indien ACME in staat van faillissement, surseance van betaling, stillegging of liquidatie komt te verkeren, is TUNIX gerechtigd de apparatuur en de software in te nemen, de overeenkomst geheel of gedeeltelijk te ontbinden of de dienstverlening op te schorten, zulks ter keuze van TUNIX. In deze gevallen is elke vordering welke TUNIX ten laste van ACME heeft of krijgt, dadelijk en ineens opeisbaar.



### E.23 Ondertekening

Ondergetekenden hebben kennis genomen van de inhoud van deze overeenkomst, geven goedkeuring aan de contactpersonenlijst (paragraaf E.10) en hebben deze overeenkomst rechtsgeldig voor akkoord getekend.

(plaats) .....

(datum) .....

TUNIX Internet Security & Opleidingen b.v.  
Namens deze,  
Ronald L. Pikkert

A Company Manufacturing Everything, ACITY  
Namens deze (s.v.p. ook uw naam duidelijk leesbaar vermelden),

---

---

