

TUNIX Security Portfolio

Producten en Diensten

Whitepaper

**TUNIX keeps your
security up !**

Version: 2/1.21

Formatted: 15-08-2007

Copyright 2007 TUNIX Internet Security & Opleidingen



1. De TUNIX organisatie

TUNIX houdt zich primair bezig met het voor haar klanten beheren van netwerkbeveiligingsoplossingen en heeft daarin een goede naam opgebouwd. TUNIX bouwt, levert, evalueert, beheert en zorgt voor het onderhoud van beveiliging-systemen.

Firewalls worden door TUNIX turn-key en dus volledig operationeel opgeleverd. Tot onze taken rekenen we daarom opleiding, advies, ontwerp, implementatie, coördinatie, plaatsing van de hardware, oplevering, overdracht en beheer. In de praktijk nemen wij dit soort projecten meestal in z'n geheel voor onze verantwoording en wordt de geïnstalleerde firewall middels een *Managed Firewall Service* SLA door TUNIX beheerd.

Op het gebied van beveiligingsoplossingen biedt TUNIX een breed dienstenpakket. Dat pakket bestaat uit productonafhankelijke opleidingen op het gebied van netwerktechnologie, netwerkbeveiligingsadvies, firewall-implementaties, VPN-oplossingen, beheer van firewall-systemen en zowel standaard- als maatwerk ontwikkelingswerkzaamheden.

De TUNIX beveiligingsoplossingen zijn modulair opgebouwd, wat het mogelijk maakt dat wij voor klanten die dat wensen, 3rd party componenten naadloos kunnen integreren.

De optionele modules die wij aanbieden bevatten technologie van 3rd parties (onze Technology Partners) zoals Kaspersky Labs, Cisco, F5, V-one, Rainbow, Vordel, Emerging Technologies, Secure Computing en anderen.

Contactinformatie

TUNIX is gevestigd op de volgende locaties:

- Het technisch centrum en N.O.C. bevindt zich in Nijmegen. De contactgegevens voor deze locatie zijn:

TUNIX Internet Security & Opleidingen	
Wijchenseweg 111	
6538 SW Nijmegen	
Telefoon algemeen:	+31 (24)3455000
Fax algemeen:	+31 (24)3455001



- Ons cursus-, presentatie- en verkoop-centrum bevindt zich in Veenendaal. De contactgegevens voor deze locatie zijn:

TUNIX Internet Security & Opleidingen	
Plesmanstraat 36	
3905 KZ Veenendaal	
Telefoon verkoop:	+31 (318)546300
Fax verkoop:	+31 (318)546303

Routebeschrijvingen voor deze locaties vindt u op onze website www.tunix.nl.



2. Diensten en producten

Dit white paper geeft een overzicht van de diensten en producten die TUNIX levert voor netwerkbeveiligingsoplossingen. Voor consultancy, opleidingen en algemene firewall-achtergronden bestaan aanvullende white papers en brochures.

De netwerkbeveiligingsdiensten van TUNIX zijn vormgegeven in diverse contractsoorten met Service Level Agreements (SLA's). De diensten worden gerealiseerd met produkten van TUNIX en Technology Partners. Naast integratie van deze producten in onze diensten worden de producten ook separaat geleverd en ondersteund.

TUNIX levert de volgende security-diensten:

Managed Firewall Services Onderhoudscontracten en ondersteuning: Upgrade, TUNIX/Webchecker en Remote Standby overeenkomsten. Maatwerk en security consultancy
--

Tabel 1: Security-diensten

De volgende security-producten zitten in het portfolio:

TUNIX/Firewall	Cisco Routers en Cisco PIX
TUNIX/Mirror Firewall	F5 Firepass SSL portal/VPN gateway
TUNIX/Parallel Firewall Solution	Pointsec disk-encryptie
TUNIX/Satellite Firewall	Kaspersky Anti Spam
TUNIX/VPN Satellite Firewall	Kaspersky Anti Spam
TUNIX/WebGuard	Kaspersky Anti Virus
TUNIX/B2BGuard	Vordel Secure XML Firewall
TUNIX/NIDS	Secure Computing Safeword
TUNIX/Secure Server Platform	

Tabel 2: Security-producten



2.1 Managed Firewall Services

Beveiliging wordt steeds crucialer vanwege de toenemende externe bedreigingen enerzijds en de toenemende complexiteit van de interne systemen anderzijds. Door de alsmaar groeiende vraag naar meer functionaliteit en online transactie-mogelijkheden worden deze toepassingen steeds bedrijfskritischer en mogen deze systemen niet onderuit gaan door een aanval van hackers of virussen. Desondanks moeten bedrijven in het huidige economische klimaat kritische keuzes maken over investeringen in ICT en personeel om de interne ICT-infrastructuur te bewaken.

Beheer van de security-omgeving wordt dus ook steeds ingewikkelder en vereist specialistische kennis die 24 uur per dag aanwezig moet zijn om de systemen te bewaken. Indien u daarvoor de kennis of middelen ontbeert kan TUNIX u deze taak uit handen nemen doordat TUNIX beschikt over een aantal ervaren security-experts die 24x7 de systemen van u en andere klanten bewaken. Dit wordt Managed Firewall Service genoemd, die uiteraard door een SLA wordt ondersteund zodat u weet wat u van ons mag verwachten.

Een kort overzicht van de voordelen van de *Managed Firewall Service*:

- Er is *geen initiële investering*: de kosten van de hardware, de software en de installatie zijn ondergebracht in de service-prijs.
- TUNIX *beheert en bewaakt* de firewall en overige apparatuur 7 dagen per week, 24 uur per dag. Bij het constateren van onregelmatigheden (b.v. hackpogingen) neemt TUNIX actie om de gevolgen te minimaliseren en stelt de contactpersonen van uw organisatie hiervan op de hoogte.
- Op de hardware die wij in het kader van de overeenkomst beschikbaar stellen, bieden wij wereldwijd *onsite hardware support* aan (7x24 uur).
- In de TUNIX/Firewall is een modem ingebouwd met secure access, zodat remote-access bij calamiteiten mogelijk blijft, ook als het VPN niet meer functioneert.
- Op de beveiligingssystemen voeren wij *bereikbaarheids- en service-beschikbaarheids-monitoring* uit.
- TUNIX is voor de klant het aanspreekpunt voor 2e lijns support (beheer). Indien bij een support call blijkt dat het probleem veroorzaakt wordt door de ISP, zal TUNIX als intermediair optreden.
- Als de beveiligingssystemen niet binnen 8 kantooruren kunnen worden gerepareerd, stelt TUNIX kosteloos een *reserve systeem* ter beschikking.

In de SLA is vastgelegd waar u op kunt rekenen bij deze vorm van dienstverlening. Hieronder treft u enige kernpunten waaruit de SLA is opgebouwd:



- Upgrades worden gedurende de looptijd van het contract binnen een afgesproken tijd geïnstalleerd. Het van tevoren maken van backups en een roll-backprocedure behoort tot de standaard-procedure.
- Onderhoud kan indien gewenst plaatsvinden binnen van tevoren overeengekomen service-windows. Indien geen service-window is overeengekomen worden geplande onderhoudswerkzaamheden één week van tevoren aangekondigd.
- Afspraken rond Mean Time To React (MTTR), voor al of niet spoedeisende ondersteuning wordt in de SLA vastgelegd. Tevens wordt een lijst van contactpersonen overeengekomen die TUNIX met ondersteuningsvragen kunnen benaderen, evenals de escalatie-niveau's en daaraan gekoppelde personen.
- TUNIX monitort de performance van systemen, gerelateerd aan de beschikbare bandbreedte, aantallen gebruikers en gebruikersprofiel e.d. om vast te stellen of systemen nog aan de eisen voldoet. Mocht dit niet langer het geval zijn dan draagt TUNIX binnen de overeengekomen randvoorwaarden zorg voor vervanging van het systeem, zonder dat daar kosten voor de klant aan verbonden zijn.
- De SLA biedt garanties ten aanzien van beschikbaarheid van de Managed Firewall Service en de support-afdeling.
- TUNIX levert maandelijks een management-rapportage aan met daarin onder meer:
 - 1 uitgevoerde upgrades
 - 2 overzicht virus-incidenten
 - 3 overzicht hackpogingen
 - 4 verslag van maandelijks handmatige inspectie firewalls
 - 5 overzicht services-calls (incl. responsetijden, afsluittijd, toelichting)
 - 6 escalatierapportage

2.2 Maatwerk en security-consultancy

Bij maatwerk support worden de diverse contracten uitgebreid met klantspecifieke extensies: bijvoorbeeld uitgebreide backup-service op afstand, reservering van extra ontwikkel- en onderhoudsuren, enzovoorts.



Naast maatwerk wordt security-consultancy aangeboden op ad hoc en projectbasis. Tot de consultancy mogelijkheden behoren ondermeer audits, Outpost-24 analyses, e-crime incident begeleiding en reviewing van software- en netwerk-security design.



2.3 Overzicht TUNIX/Firewall producten

De TUNIX/Firewall is een state of the art modulaire layer 2, 3 en 4 firewall-appliance. De basisuitvoering van deze firewall heeft twee ethernet interfaces. De licentieprijs wordt bepaald door de capaciteit van de machine en het aantal ethernet interfaces. De TUNIX/Firewall is leverbaar in verschillende uitvoeringen.

Product	Paragraaf
TUNIX/Firewall	2.3
TUNIX/Mirror Firewall	2.3.1
TUNIX/Parallel Firewall Solution	2.3.2
TUNIX/Satellite Firewall	2.3.3
TUNIX/VPN Satellite Firewall	2.3.4
TUNIX/WebGuard	2.3.5
TUNIX/B2BGuard	2.3.6
TUNIX/NIDS	2.3.7
TUNIX/Secure Server Platform	2.3.8

Tabel 3: Overzicht TUNIX/Firewall producten

2.3.1 De TUNIX/Firewall Mirror

Als een firewall uitvalt kan de bedrijfsvoering in gevaar komen: voor veel organisaties is email business critical. Daarom is het wenselijk een firewall uit te voeren met kwaliteitshardware zodat hardware-problemen zeldzaam zijn en de downtime geminimaliseerd wordt. Toch kunnen componenten zoals het systeembord, voedingen en netwerkkaarten defect raken.

Om dergelijke storingen op te vangen biedt TUNIX de mogelijkheid om een *mirror* van de firewall op te zetten. Een mirror is een hardware-kopie van de firewall die regelmatig (zo vaak als wenselijk wordt geacht) software-matig wordt bijgewerkt vanuit de actieve firewall. Indien een storing optreedt in de firewall kan de beheerder met een eenvoudig commando de mirror als master-firewall activeren. Vervolgens kan het defecte systeem worden gerepareerd en worden geconfigureerd als mirror.

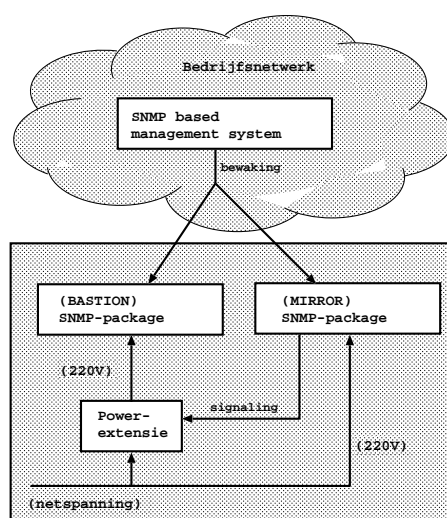
TUNIX biedt voor haar TUNIX/Firewall Mirror een uitbreiding om de overname van de master firewall door de mirror firewall automatisch te laten plaatsvinden. Deze oplossing, de TUNIX/Auto-mirror, gebruikt een standaard SNMP-interface, zodat de aansturing van TUNIX/Auto-mirror door een netwerkbeheersysteem naar keuze kan worden uitgevoerd.



In het geval van uitval van de master firewall zorgt TUNIX/Auto-mirror ervoor dat deze volledig wordt uitgeschakeld en de mirror firewall automatisch opstart als master firewall, waarmee de connectiviteit wordt hersteld, zonder dat een beheerder actie hoeft te ondernemen.

Vooraf buiten de reguliere kantooruren is dat een groot voordeel, met name als de Internetverbinding ook wordt gebruikt voor communicatie met vestigingen of andere bedrijven in een andere tijdzone, of de beschikbaarheid van de Internetverbinding een kritische factor is.

Schematisch ziet de TUNIX/Auto-mirror oplossing er als volgt uit:



Figuur 1: Topologie TUNIX/Auto-mirror oplossing

Meer in detail werkt TUNIX/Auto-mirror als volgt:

- Op de TUNIX/Firewall is een SNMP-optie actief, die op basis van standaard *Management Information Base* (MIB) waarden wordt geconfigureerd. Op uw verzoek kan TUNIX ook speciale traps en aanvullende MIB-waarden implementeren. Zowel de master - als de mirror firewall zijn hierdoor te monitoren.
- De master firewall wordt gevoed via een schakelbare powerextensie van de TUNIX/Auto-mirror.
- Een door de gebruiker beheerd netwerkmonitorsysteem verzorgt de bewaking en de aansturing van TUNIX/Auto-mirror. Zo'n netwerkmonitorsysteem is doorgaans al operationeel. Het netwerkmonitorsysteem dient te beschikken over SNMP-2 functionaliteit.
- Indien het netwerkmonitorsysteem op basis van de geconfigureerde regels constateert dat de mirror firewall de taak van de master firewall moet overnemen, zal deze een SNMP-trap naar de mirror firewall sturen.



- TUNIX/Auto-mirror zal de master firewall fysiek uitschakelen en ervoor zorgen dat de mirror firewall herstart in master mode. Dankzij TUNIX/Auto-mirror zal bij het uitvallen van de master firewall de connectiviteit in slechts enkele minuten weer hersteld zijn.
- Nadat de storing aan de master firewall is opgelost, kan de beheerder de originele configuratie weer herstellen.

2.3.2 TUNIX/Parallel Firewall Solution

De TUNIX/Parallel Firewall Solution levert dezelfde mogelijkheden als een TUNIX/Firewall. Met een TUNIX/Parallel Firewall Solution licentie kunnen TUNIX/Firewalls parallel worden geschakeld om meer performance te bieden. Bij een TUNIX/Parallel Firewall Solution zijn alle firewalls, in tegenstelling tot de TUNIX/Auto-mirror, tegelijk actief.

2.3.3 TUNIX/Satellite Firewall

Een veilige manier om netwerken van vestigingen met elkaar te koppelen is het gebruik van een *Virtual Private Network* (VPN).

TUNIX/Firewalls bieden standaard de mogelijkheid om een VPN op te bouwen, waarbij in de vestiging gebruik kan worden gemaakt van een TUNIX/Satellite Firewall. Het VPN kan bijvoorbeeld worden gebruikt voor datasharing, applicatiebeheer of *Voice Over IP* (VOIP).

Behalve de mogelijkheid om een VPN te creëren heeft een TUNIX/Satellite Firewall natuurlijk ook andere voordelen. Wij noemen er enkele:

- Een TUNIX/Satellite Firewall is een veilige oplossing om voor de vestiging(en) Internettoegang te realiseren.
- Tussen de netwerken van de vestigingen kunt u gebruik maken van een firewall-to-firewall VPN, zodat transparante (maar wel gecontroleerde) toegang tussen de netwerken mogelijk is.
- De opzet en werking van een TUNIX/Satellite Firewall is identiek aan die van de TUNIX/Firewall in de hoofdvestiging.
- Door het gebruik van gelijksoortige firewalls wordt het systeem- en policybeheer eenvoudiger.
- Een TUNIX/Satellite Firewall heeft twee interfaces: voor het interne netwerk en voor het Internet.



- De functionaliteit van een TUNIX/Satellite Firewall is een subset van die van de hoofd TUNIX/Firewall.
- Een TUNIX/Satellite Firewall wordt vanuit de hoofdvestiging beheerd en het policy-management wordt centraal geregeld.
- De verschillende locaties kunnen als fallback voor email fungeren.
- Een TUNIX/Satellite Firewall biedt dezelfde mogelijkheden als de hoofd TUNIX/Firewall, maar is qua licentie voordeliger.
- De TUNIX/Satellite Firewall wordt geleverd als een Managed Firewall Service.

2.3.4 TUNIX/VPN Satellite Firewall

Om te voldoen aan de grote vraag naar veilige koppelingen voor locaties die via ADSL aan het Internet kunnen worden gekoppeld, is door TUNIX de TUNIX/VPN Satellite Firewall ontwikkeld. De TUNIX/VPN Satellite Firewall is een minibox met ingebouwd ADSL-modem, router, firewall en IPsec feature, die uitstekend geschikt is voor thuiswerksituaties of vestigingen met maximaal 15 werkplekken.

De TUNIX/VPN Satellite Firewall biedt de volgende functionaliteit:

- Een transparant en gemanaged IP-level-VPN met de hoofd TUNIX/Firewall.
- Directe Internettoegang of uitsluitend toegang via de VPN-tunnel en de centrale TUNIX/Firewall.
- Heartbeat monitoring van de TUNIX/VPN Satellite Firewall.

In combinatie met een voordelig ADSL-abonnement kan met deze oplossing een werkplek of een vestiging worden ontsloten, zonder dat de centrale security policy geweld wordt aangedaan. Ook decentrale gebruikers profiteren zo van de functionaliteit en de bescherming van de centrale firewall.

Voor het gebruik van een TUNIX/VPN Satellite Firewall gelden de volgende voorwaarden:

- Een TUNIX/VPN Satellite Firewall kan alleen worden ingezet in combinatie met een full-license TUNIX/Firewall.
- Een TUNIX/VPN Satellite Firewall heeft maximaal twee interfaces en biedt directe Internettoegang of uitsluitend toegang via de centrale firewall.



- De access policy wordt vanuit de hoofdvestiging beheerd.
- De TUNIX/VPN Satellite Firewall wordt geleverd als een Managed Firewall Service.

2.3.5 TUNIX/WebGuard - webserver bescherming voor HTTP en HTTPS

Voor bedrijven die online diensten aanbieden via hun website is beveiliging van essentieel belang. De veiligheid en integriteit van webserver wordt steeds belangrijker, ook omdat steeds meer aanvallen gebruik maken van de data-inhoud die wordt verzonden via de HTTP-protocollen.

TUNIX biedt met de HTTP-screening appliance TUNIX/Webguard een optimale bescherming tegen dit soort aanvallen. De TUNIX/Webguard wordt als extra verdedigingslinie ingezet tussen het Internet en de webserver. Hierdoor is de TUNIX/Webguard in staat om aanvallen op webserver af te slaan. Aanvallers maken vaak gebruik van gemanipuleerde HTTP-verzoeken die zwakheden in webserversoftware, scripts of backoffice koppelingen uitbuiten. De TUNIX/Webguard fungeert als *schild* en inspecteert de binnenkomende requests op *malicious content*.

De voordelen op een rij:

- screening van HTTP-verkeer: inhoudelijke inspectie op mogelijke *malicious content*, biedt ook bescherming tegen nog niet bekende aanvallen;
- de screening faciliteiten zijn zeer nauwkeurig op de achterliggende websites aan te passen. Mogelijkheid om inkomende requests te *remappen*;
- schildfunctie die de webserver afschermt: er is geen direct verkeer mogelijk tussen de webserver en het Internet, dit wordt afgehandeld door de TUNIX/Webguard;
- de *window of vulnerability* voor het patchen van de webserver is kleiner want deze wordt afgeschermd door de TUNIX/Webguard;
- ondersteunt encryptie; de TUNIX/Webguard neemt desgewenst de SSL-functionaliteit voor zijn rekening zodat content-screening ook in geval van een versleutelde verbinding plaats kan vinden;
- 1U concept: ruimtebesparing in een 19"-rack, met name van belang als de website elders gehost wordt;
- de standaard meegeleverde *TUNIX/Webchecker* service controleert onder meer de bereikbaarheid en beschikbaarheid van de achterliggende websites, veranderde pagina's en het vereist zijn van wachtwoorden;



- maandelijkse management rapportages verschaffen inzicht in de status van uw webservices;
- modulair concept; diverse uitbreidingen leverbaar (HTTPS screening, PKI, hardware-encryptie accelerator etcetera);



Figuur 2: TUNIX/WebGuard

Uitbreidingsmogelijkheden en technische specificaties

- de TUNIX/WebGuard is leverbaar in uitvoeringen met een throughput van 4, 8, 16, 32, 64 en 100 Mbps;
- mogelijkheid voor 2.000 parallele connecties of meer;
- afhandeling van 200 HTTP requests per seconde of meer;
- hardware encryptie accelerator leverbaar in een uitvoering voor 200, 400, 600 en 1000 HTTPS-transakties per seconde;
- leverbaar in verschillende performance- en SLA klassen;
- mogelijkheid voor hardwarematige encryptie-versnelling om snel een groot aantal simultane HTTPS-sessies af te kunnen handelen;
- SecureBase™ operating system; een zwaar beveiligd systeem dat ook wordt gebruikt voor E-banking en andere high security omgevingen;
- onboard: 2 netwerkinterfaces 10/100Mb UTP voor koppeling Internet - webserversegment;



2.3.6 TUNIX/B2BGuard

Samen met onze technology partner Vordel levert TUNIX diverse oplossingen om business to business (B2B) en Consumer to Business (C2B) webservices veilig te maken. Zoals de TUNIX/WebGuard het HTTP verkeer bewaakt op gevaarlijke inhoud, zo bewaakt de TUNIX/B2BGuard XML-gebaseerde transacties. Er is ondermeer ondersteuning voor XML, SOAP, WSecurity en EbXML.

2.3.7 TUNIX/NIDS - Network Intrusion Detection System

De TUNIX/Firewall beschikt over een *Host Intrusion Detection System* (HIDS) dat vijandige activiteiten op - of gericht aan - de firewall detecteert. Deze beveiliging kan worden uitgebreid met een *Network Intrusion Detection System* (NIDS). TUNIX is GIAC gecertificeerd voor de NIDS-oplossing Snort.



Figuur 3: GIAC gecertificeerd

TUNIX/NIDS is een Network Intrusion Detection System dat real-time traffic-analyse en packet logging uitvoert. Het ondersteunt protocol analyse en content search en kan een variëteit aan aanvallen en probes onderscheiden, zoals buffer overflows, stealth port scans, CGI attacks, SMB probes, pogingen tot OS fingerprinting en nog veel meer.

TUNIX/NIDS gebruikt een flexibele rules programmeertaal om het verkeer te beschrijven dat het zou moeten oppakken of laten doorgaan en een detectie engine die een modulaire plug-in structuur ondersteunt. TUNIX/NIDS heeft ook een real-time alert functie met mechanismes voor syslog, een door de gebruiker gedefinieerde file, een UNIX socket of WinPopup boodschappen naar Windows clients door middel van Samba's smbclient.



TUNIX/NIDS wordt in principe op drie manieren gebruikt: als een gewone packet sniffer, als een packet logger (nuttig voor het debuggen van netwerkverkeer, etc.) of als een volledig netwerk intrusion detection systeem.

TUNIX/NIDS is als volgt opgezet:

- TUNIX/NIDS is op een dedicated systeem geïnstalleerd.
- Als platform is TUNIX/SecureBase gebruikt. Dit platform wordt gebruikt voor secure services (zie paragraaf 2.3.8) die in een te beschermen netwerk moeten functioneren.
- De *afluister interface* is fysiek *read-only* gemaakt. Hierdoor wordt voorkomen dat de meetopstelling kan worden opgemerkt of aangevallen. Indien TUNIX/NIDS op een geswitched netwerk staat moet de switch over een *span poort* of *tap interface* beschikken.
- Voor het beheer en de logging is een dedicated koppeling naar de firewall gemaakt.

Network Intrusion Detection is belastend voor de beheerder in verband met de vele *false alerts* die plaats hebben als de detectie-database niet voortdurend bijgesteld wordt. Daarom wordt de TUNIX/NIDS geleverd als Managed Service.

2.3.8 De TUNIX/Firewall als secure server platform

Het SecureBase platform waarop de TUNIX/Firewall functioneert kan dienen als basis voor bijvoorbeeld een secure web-server of *Network Intrusion Detection* systeem. Een dergelijke installatie is daarmee meteen voorzien van een complete security oplossing. Op zo'n server kan TUNIX allerlei additionele software leveren zoals het I-Pay betaalsysteem, PKI/SSL-certificaat programmatuur, CGI data-screeners (TUNIX/HttpScreen), load-schedulers en koppelingen met databases. Alle extra's worden geïntegreerd met de centrale loggingfaciliteit en met de system integrity checker.

Een bekende toepassing die op een TUNIX secure server platform draait is de DNS-server van de Nederlandse domeinregistratie, de *Stichting Internet Domeinregistratie Nederland* (www.domain-registry.nl).

