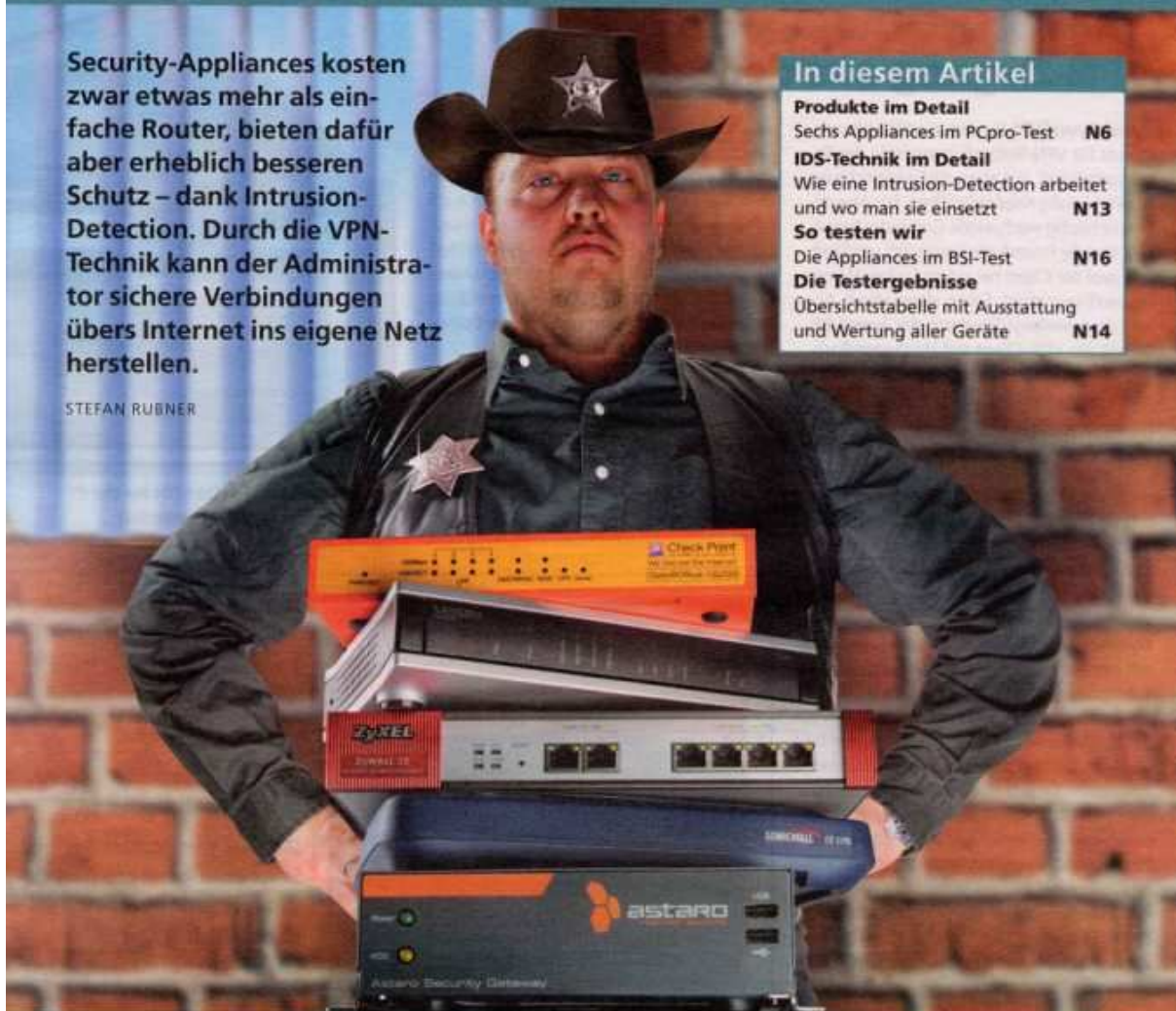


## NETZWERK Security-Appliances

Security-Appliances kosten zwar etwas mehr als einfache Router, bieten dafür aber erheblich besseren Schutz – dank Intrusion-Detection. Durch die VPN-Technik kann der Administrator sichere Verbindungen übers Internet ins eigene Netz herstellen.

STEFAN RUBNER



### In diesem Artikel

#### Produkte im Detail

Sechs Appliances im PCpro-Test **N6**

#### IDS-Technik im Detail

Wie eine Intrusion-Detection arbeitet und wo man sie einsetzt **N13**

#### So testen wir

Die Appliances im BSI-Test **N16**

#### Die Testergebnisse

Übersichtstabelle mit Ausstattung und Wertung aller Geräte **N14**

# Starke Sheriffs

Verglichen mit einem herkömmlichen Router bieten aktuelle Security-Appliances wesentlich mehr Funktionen. So ist die Erkennung von Angriffen über eine Intrusion-Detection (IDS) inzwischen schon bei Geräten unter 1000 Euro Standard. Zusätzlich finden sich Features wie Virens Scanner für E-Mail-Anhänge und aus dem Internet heruntergeladene Dateien sowie Spamfilter und Content-Überwachung. Diese Zusatzfunktionen verschlingen mehr Rechenleistung als die reine Routingfunktion. Im Sicherheits-Check mit der BSI-Suite (siehe Seite N16) schneiden alle Geräte gleich gut ab. Bei Performance und Benutzerfreundlichkeit gibt es aber große Unterschiede.

#### Kostenfalle: Folgekosten

Niedriger Grundpreis, aber Sonderausstattung kostet zusätzlich: Nach diesem Preismodell kalkulieren die meisten Anbieter im

Test. Die Grundpreise für die Geräte liegen mit 600 Euro für die Lancom 1711 VPN und 900 Euro für die Zywall 35 vergleichsweise niedrig. Dazu kommen bei allen Produkten außer bei der »Budget-Empfehlung« von Lancom aber noch diverse Lizenzgebühren. Diese Gebühren können je nach Hersteller ein empfindliches Loch ins IT-Budget reißen.

Updates, Contentfilter, Virens Scanner und IDS-Signaturen kosten oft schon beim Neukauf extra. In Summe erreichen die Einstiegskosten beim teuersten Gerät, der Safe@Office 225 von Checkpoint, somit erkleckliche 2000 Euro. Auch in den Jahren nach dem Kauf sind regelmäßige Gebühren fällig, wenn man das Gerät up to date halten will. Eine Höchstmarke setzt auch hier Checkpoint: Mit über 1200 Euro jährlich ist Safe@Office 225 fast doppelt so teuer im Unterhalt wie die Geräte von Aristo oder Zyxel und sogar fast dreimal so teuer wie die Sonicwall

TZ 170. Die günstigsten Folgekosten bieten die Cisco 871 mit 50 Euro jährlich sowie der »Budget-Sieger« Lancom 1711 VPN. Bei Lancom sind sogar die Updates kostenlos. Allerdings muss man dafür bei beiden Geräten auf Features wie Contentfilter oder Virens Scanner verzichten.

#### VPN-Support ist Standard

Zusätzlich zu den Schutzfunktionen unterstützen die getesteten Appliances ausnahmslos virtuelle private Netze (VPNs). Alle Geräte unterscheiden dabei zwischen Netzzu-Netz- und Netzzu-Client-Verbindungen, die oft auch gesondert zu lizenzieren sind. So ist im Preis der Sonicwall TZ 170 lediglich eine Client-Lizenz für den VPN-Zugriff eines Clients auf die Appliance enthalten, obwohl die Appliance bis zu 25 Client-Verbindungen annehmen kann. Für die Clients müssten also 24 Lizenzen nachgekauft wer-



## Astaro ASG 110

Als einzige Appliance im Test setzt Astaro auf PC-Hardware, im Labor belegt sie durchgängig Spitzenplätze in den Leistungsmessungen. Die Festplatte erlaubt das Puffern großer Dateien für den Virensan. Im PCpro-Test gibt sich die ASG 110 auch keine Blöße und wird so mit deutlichem Abstand zum restlichen Teilnehmerfeld verdient Testsieger.



## Lancom VPN 1711

Mit der VPN 1711 hat Lancom einen echten Preisbrecher im Angebot, über den Kaufpreis hinaus entstehen keine weiteren Kosten. Das ist einmalig im Testfeld. Die Appliance bietet weder E-Mail-Schutz noch Surf-Protection, ist davon abgesehen aber reichhaltig ausgestattet. Obwohl sie nur 600 Euro kostet, hat sie ausreichend Leistungsreserven für ADSL2.

## Die besten Security-Appliances

<b>1</b>	<b>ASG 110</b>	Astaro .....	<b>86,9</b>
<b>2</b>	<b>Zywall 35</b>	Zyxel .....	<b>80,7</b>
<b>3</b>	<b>TZ 170 Total Secure</b>	Sonicwall .....	<b>77,8</b>
<b>4</b>	<b>Safe@Office 225</b>	Checkpoint .....	<b>75,4</b>

Produkt Hersteller maximal 100 Punkte

den. Bei Checkpoint ist nur die Zusammenarbeit mit Clients möglich, die aus demselben Haus stammen. Das engt den Einsatzbereich der teuren Appliance künstlich ein. Ähnlich sieht es bei bei Cisco aus, während Lancom und Astaro durch ihre offene Architektur beliebige Clients unterstützen. Die VPN 1711 bietet ab Werk fünf parallele Verbindungen, die ASG 110 überzeugt mit bis zu 100 gleichzeitigen VPN-Tunneln.

## Parallele Tunnel fressen Bandbreite

Die nominellen Werte der maximal unterstützten VPN-Tunnel sind in der Praxis mit Vorsicht zu genießen. Wie die Messwerte zeigen, bricht bei einigen Produkten die Transferrate so weit ein, dass sich faktisch nicht mehr als zwei gleichzeitige VPN-Tunnel bei akzeptabler Geschwindigkeit einsetzen lassen. Besonders betroffen sind hier die Cisco 871 und die Sonicwall TZ 170. Allerdings ist auch bei den restlichen Probanden zu beachten, dass DSL-Verbindungen in der Regel dem Uplink deutlich weniger Bandbreite einräumen als dem Downlink. Für VPN-Verbindungen ist aber der Upstream entscheidend, denn auf diesem werden die Daten vom lokalen Netz zum VPN-Client gesendet. Auf herkömmlichen DSL-Leitungen mit 1024 MBit/s Downstream und nur 128 oder 256 MBit/s Upstream ist folglich maximal ein VPN-Tunnel mit befriedigenden Transferraten realisierbar.

## DSL, Kabelmodem, Standleitung

Allerdings sind die Appliances im Test nicht ausschließlich für den Einsatz am DSL-Netz konzipiert. Keines der Geräte besitzt ein integriertes DSL-Modem. Alle Produkte benötigen ein externes Bindeglied zum Internet wie beispielsweise ein DSL- oder Kabelmodem. Damit steht dann theoretisch auch der Weg zu schnelleren Verbindungen wie großvolumigen Standleitungen offen. In der Praxis setzen aber Faktoren wie Durchsatz der Firewall sowie gegebenenfalls die VPN-Engine dem Geschwindigkeitshunger enge Grenzen. So ist beispielsweise die Cisco 871 nominell nur für Leitungen mit bis zu 3 MBit/s ausgelegt, kommt also bereits

an schnelleren DSL-Zugängen ins Schwitzen. Immerhin 25 MBit/s kann die Lancom 1711 VPN verarbeiten. Damit ist sie schnell genug für den derzeit noch im Prototypenstadium befindlichen ADSL2-Standard.

Der Rest des Testfelds ließe sich mit nominellen Leistungswerten von 80 (Checkpoint), 90 (Sonicwall und Zyxel) und sogar 100 MBit/s (Astaro) theoretisch auch an einer Fast-Ethernet-Leitung betreiben. Das klappt aber nur, wenn IDS und sonstige Schutzfunktionen deaktiviert sind. IDS ist sehr rechenintensiv und drückt im Test drastisch auf die real erzielbaren Transferraten. Besonders betroffen sind bei HTTP-Übertragungen Checkpoint und Sonicwall. Der Testsieger Astaro erreicht durchgehend Spitzenwerte im Labor. Keine andere Appliance hat eine gleichwertige Performance vorzuweisen.

## Verwaltung übers Netzwerk

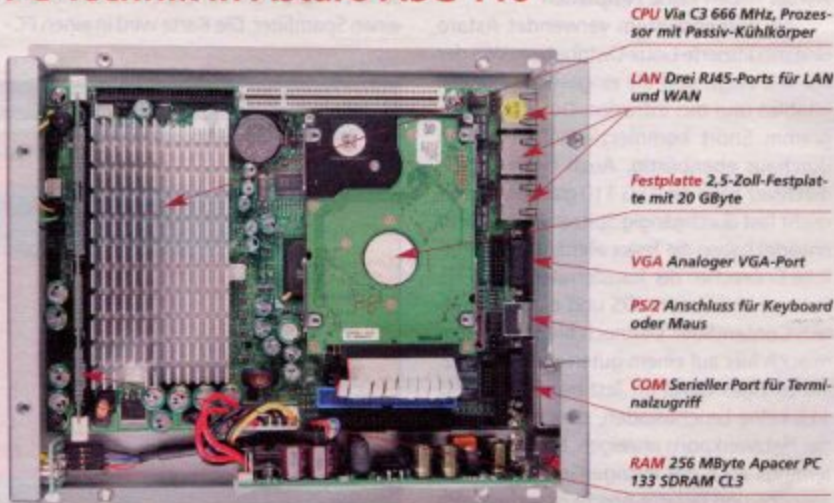
Als Standard zur Verwaltung der Geräte dient ein per Browser abrufbares Web-Interface. Zusätzlich bieten alle Produkte außer Sonicwall die Möglichkeit, direkt auf der Kommandozeile Änderungen an der Konfiguration vorzunehmen. Auch hier zeigt sich ein wesentlicher Unterschied zu reinen Routern, da alle Appliances von Haus aus das

verschlüsselte Protokoll Secure Shell (SSH) beherrschen. Das wegen fehlender Verschlüsselung unsichere Telnet bieten Cisco, Lancom und Zyxel optional.

Ist keine Netzwerkverbindung vorhanden, lassen sich alle Probanden auch via Terminalprogramm über die serielle Schnittstelle verwalten. Der Terminalzugriff ist praktisch, wenn sich der Administrator wegen eines Konfigurationsfehlers selbst vom Netzzugriff auf das Gerät ausgeschlossen hat. Eine Besonderheit ist die Appliance von Astaro. Sie lässt sich dank ihres PC-basierten Designs wie ein normaler Computer direkt an Monitor und Tastatur anschließen.

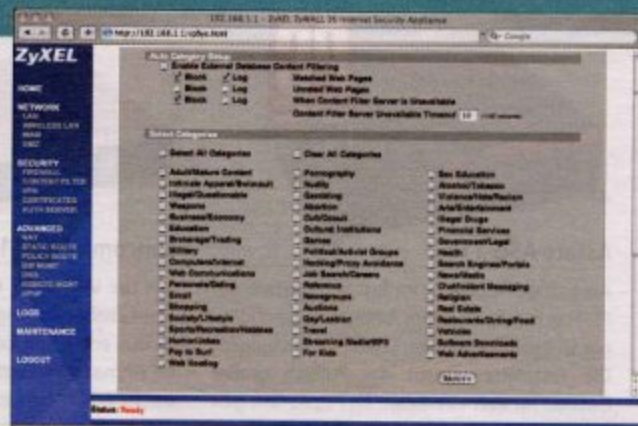
Eine stets abrufbare, kontextsensitive Online-Hilfe gehört bei allen Geräten ebenso zum Standard wie einfache Plausibilitätsprüfungen der Eingaben. Das verhindert grobe Fehlkonfigurationen. Temporäre Puffer bieten nur Cisco und Lancom. Hier werden Änderungen an den Einstellungen zwar vorübergehend übernommen, beim nächsten Neustart kommen jedoch wieder die alten Settings zum Einsatz. Erst durch explizite Anweisung des Administrators schreiben die Geräte Änderungen in den permanenten Speicher. Auf diese Weise lassen sich neue Konfigurationen gefahrlos testen. SST

## PC-Technik in Astaro ASG 110





Der interne Log-Viewer der ASG 100 von Astaro erlaubt dem Administrator, in Echtzeit Datenpakete nachzuverfolgen



ZyXel bietet im Contentfilter umfangreiche Optionen, um unerwünschte Web-Inhalte komfortabel auszufiltern

## Produkte im Detail

Die Appliances sind für kleinere Firmennetze mit 10 bis 25 Benutzern ausgelegt. Alle haben kompakte Außenmaße und eine Ausstattung mit mehreren Ports für LAN, WAN und DMZ. Unter der Haube enden aber die Gemeinsamkeiten.

### Astaro ASG 110

Die Astaro ASG 110 ist in mehrfacher Hinsicht eine Besonderheit im Testfeld. Sie ist die einzige PC-basierte Appliance im Test. Mit zwei LAN-Ports, einem WAN-Port sowie seriellen, PS/2 und USB-Schnittstellen ist sie gut ausgestattet. Als zentrales Rechenwerk dient ein VIA-C3-Prozessor, der mit 666 MHz mehr als genug Rechenleistung für IDS, Firewall und VPN bietet. Die integrierte Festplatte mit 20 GByte Kapazität erlaubt die Sicherung großer Protokollmengen. Zusätzlich dient sie als Zwischenspeicher für den zuschaltbaren Proxy-Server. Mit seiner Hilfe speichert die ASG 110 nicht nur aus dem Web heruntergeladene Inhalte, sondern ermöglicht gleichzeitig dem integrierten Virens scanner sowie dem Spamfilter, komplette Dateien zu untersuchen. Das ist besser, als sich mangels Speicherplatz auf die Analyse der Datenströme beschränken zu müssen. Diese Funktionen bietet nur Astaro, die Mitbewerber haben keine Festplatten.

Als Betriebssystem verwendet Astaro eine modifizierte Linux-Distribution. Wie der BSI-Test zeigt, sind die eingesetzte Firewall Iptables und das Intrusion-Detection-Programm Snort kommerziellen Produkten durchaus ebenbürtig. Auch beim Datendurchsatz kann die ASG 110 glänzen und erreicht fast durchgängig Spitzenwerte. Nicht erwartet haben die Tester allerdings das deutliche Einbrechen der Transferraten beim FTP-Test mit aktiviertem IDS und eingeschaltetem Contentfilter. Dennoch bleibt die Astaro auch hier auf einem guten zweiten Platz. Als einziges Gerät im Test besitzt die ASG 110 keine Leuchtdioden, die den Zustand der Netzwerkports anzeigen. Dafür ist sie allerdings auch das einzige Gerät, das über Monitor- und Tastatur-Anschluss verfügt, sich

also ohne externen Rechner warten lässt. Positiv fällt den Testern das übersichtlich gestaltete Web-Interface auf. Hier lassen sich Syslog- oder SNMP-Protokolle komfortabel in Echtzeit einsehen oder an entsprechende Server weiterleiten. Die Verwaltung von Zertifikaten und VPN-Sitzungen ist ebenfalls benutzerfreundlich gelöst.

Für insgesamt 1510 Euro bietet die Astaro ASG 110 dem Anwender ein leistungsfähiges Komplettpaket, das neben IDS und VPN auch Virens can für Dateien und Mail sowie einen Spamfilter bietet. Zusammen mit den überdurchschnittlichen Leistungen im Performance-Test bringt das der ASG 110 die »Empfehlung der Redaktion«.

**1 Note gut • 86,9 Punkte**

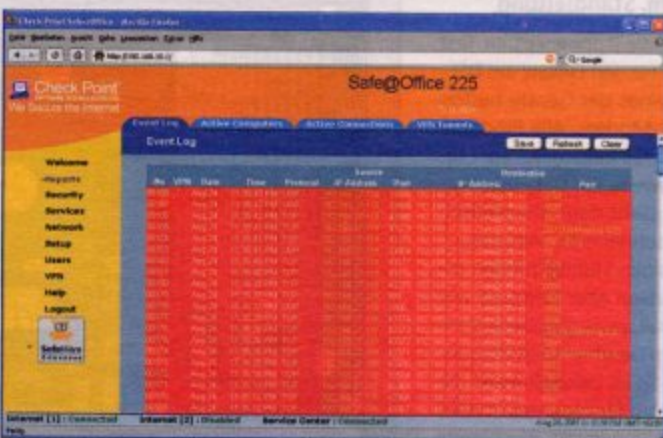
### ZyXel Zywall 35

Ein interessantes Konzept verfolgt ZyXel bei den Geräten der Zywall-Serie. In der Grundversion ist die Zywall 35 eine einfache Firewall. Erst der Zukauf einer Turbocard beschert ihr IDS-Funktionen, Virens scanner und einen Spamfilter. Die Karte wird in einen PC-

Card-Slot eingebaut. Dabei soll der auf der Turbocard enthaltene Crypto-ASIC die mit 400 MHz im Vergleichsfeld schon schnelle Intel-CPU der Appliance entlasten und Performance-Einbußen verhindern.

Dass dieses Konzept aufgeht, erfahren die Tester bei den Leistungsmessungen. Im Vergleich zum Durchsatz ohne IDS fallen die Werte bei aktivierter Angriffserkennung nur minimal ab und reichen auch für den Betrieb an schnellen Internet-Anbindungen mit 24 MBit/s völlig aus. Etwas gemischerter ist das Bild beim Test mit der BSI-Suite. Zwar lässt auch die Zywall 35 keine der Attacken durch, vermeldet Angriffsversuche aber ausschließlich im Firewall-Protokoll als gefilterte Pakete. So wird es für den Administrator schwierig, Angriffe überhaupt zu erkennen.

Positiv fällt den Testern das überarbeitete Verwaltungs-Interface auf. Im Vergleich zu bisher getesteten Produkten von ZyXel ist es aufgeräumter und übersichtlicher, so dass die verschiedenen Aufgaben schnell und problemlos zu erledigen sind. Das gilt für die Konfiguration von Firewall und IDS ebenso



Checkpoints Safe@Office 225 protokolliert den Port und teilweise auch die betroffene Applikation einer Attacke, nicht aber den Verursacher



**Aktuelle Appliances glänzen bei einem Grundpreis von unter 1000 Euro mit Funktionen, die lange viel teureren Geräten vorbehalten waren. Bei Preisvergleichen muss man aber Unterhaltskosten berücksichtigen.«**

SASCHA STEINHOFF, REDAKTEUR NETZWERK

wie für die Verwaltung von VPN-Verbindungen und Zertifikaten. Auch die Zywall 35 bietet eine Option, Backup-Verbindungen für die Internet-Anbindung zu definieren. So können mehrere Internet-Zugänge über die WAN-Ports parallel genutzt werden, wobei eine automatische Lastverteilung stattfindet.

Mit 1830 Euro Einstiegspreis für das Gesamtpaket mit IDS, E-Mail Schutz und Surf-Protection ist die Zywall 35 wirklich kein Billigheimer. Davon entfallen aber 500 Euro auf die Turbocard. Das ist eine einmalige Investition, die jährlichen Folgekosten sind dann überschaubar. Die Leistung von Zyxel ist durchweg überdurchschnittlich. Im Testfeld muss sie sich nur dem Testsieger ASG 110 von Astaro geschlagen geben.

**2 Note gut • 80,7 Punkte**

## Sonicwall TZ 170

Das Bundle Sonicwall TZ 170 Total Secure bringt neben der Appliance auch die nötigen Lizenzen für IDS, Contentfilter und Virens Scanner für ein Jahr mit und ist mit 751 Euro rund 300 Euro günstiger als die Summe der Einzelbestandteile. Das Upgrade auf die Betriebssystemvariante Sonic OS Enhanced kostet weitere 490 Euro. Nur dann werden Backup-Verbindungen, Load-Balancing, Spam-Schutz und Bandbreiten-Management unterstützt. Im Performance-Test fällt auf, dass die Werte ohne IDS und Contentfilter überzeugend sind, nach Aktivierung dieser Funktionen aber dramatisch absacken – Sonicwall fällt hier auf den letzten Platz. Bei eingeschaltetem IDS und aktivem Inhaltsfilter erreicht die TZ 170 die schlechtesten Werte des Testfelds, die gerade noch den Betrieb

an einer DSL-Leitung mit 6 MBit/s erlauben. Das an sich sauber aufgebaute Web-Interface zur Verwaltung hinterlässt bei den Testern einen zwiespältigen Eindruck. In der Fülle von Menüs und Untermenüs verirrt man sich schnell und vergeudet viel Zeit beim Suchen der benötigten Optionen. Wichtige Punkte wie die Verwaltung von VPN-Verbindungen und das Zertifikat-Management sind aber in der Oberfläche gut abgebildet.

Sehr positiv beurteilen die Tester das im Vergleich beste Verhalten beim Angriffstest mit der BSI-Suite. Hier leistet sich die TZ 170 nicht nur keine Schwäche, sie glänzt auch mit dem mit Abstand besten Reporting der Angriffe. Viele, wenngleich nicht alle Attacken werden korrekt und mit dem Namen des zugehörigen Schadprogramms oder der angegriffenen Schwachstelle im Protokoll aufgeführt. Das erleichtert sowohl die Einschätzung der eigenen Gefährdung als auch die Suche nach eventuell kompromittierten Rechnern im LAN erheblich.

Für einen Paketpreis von 750 Euro bietet die Sonicwall TZ 170 viele Funktionen und hervorragenden Schutz bei ausreichender Leistung. Zu berücksichtigen ist bei Preisvergleichen allerdings, dass die Kosten in den Folgejahren etwas ansteigen. Der Preisvorteil des Bundlings gilt nur für das erste Jahr, in den Folgejahren entfallen die Rabatte.

**3 Note befriedigend • 77,8 Punkte**

## Checkpoint Safe@Office 225

Trotz der kleinsten Bauform im Testfeld bietet die Checkpoint Safe@Office 225 eine überdurchschnittlich gute Ausstattung. Vier LAN-Ports, ein WAN-Anschluss, ein weiterer



**IDS, Virens Scanner und Spamfilter werden bei Zyxel über die Turbocard nachgerüstet**

Anschluss, den man zwischen WAN- und DMZ-Port umschalten kann, sowie eine serielle Schnittstelle zur Konfiguration per Terminal sind am Gerät vorhanden. An der Vorderseite signalisieren mehrere LEDs den Zustand der einzelnen Verbindungen. Die LEDs zeigen sogar Attacken an. Das grundsätzlich sinnvolle Feature wird von Checkpoint aber nur halbherzig umgesetzt. Die zuständige LED blinkt nur während des Angriffs rot, nachfolgend eintreffende Pakete mit unkritischem Inhalt setzen sie wieder auf Normalzustand zurück. Die optische Erkennung eines Angriffs, der beispielsweise in der Nacht stattgefunden hat, ist so nicht möglich.

Eigenwillig präsentiert sich auch das Web-Interface zur Verwaltung. Dieses ist dank vielfältiger Wizards zwar sehr komfortabel, schirmt jedoch professionelle Anwender zu stark von den Feineinstellungen ab. So kann man die Firewall lediglich mit einem Schieberegler auf niedrige, mittlere und hohe Sicherheit einstellen. Das Intrusion-Detection-System lässt sich überhaupt nicht beeinflussen. Der Leistungsfähigkeit der Schutzfunktionen tut dies allerdings keinen Abbruch, die Safe@Office 225 meistert den BSI-Test problemlos. Punkten kann die Appliance auch beim Datendurchsatz, wo sie fast in allen Punkten vordere Platzierungen erreicht. Lediglich die HTTP-Transferrate bei aktivem IDS und Contentfilter sinkt überproportional ab. Der Einbruch ist umso bemerkenswerter, als Checkpoint auf eine rechenintensive Filterung aktiver Inhalte wie ActiveX-Komponenten oder Javascript verzichtet.

Beim Anlegen von VPN-Verbindungen fällt den Testern auf, dass das Menü nur die Konfiguration von Gegenstellen zulässt, die mit der Checkpoint-eigenen VPN-Software arbeiten. Entsprechend knapp sind auch hier die Optionen, die Zusammenarbeit mit VPN-Clients anderer Hersteller ist faktisch unmöglich. Als zusätzliches Feature bietet die Safe@Office 225 einen Virens Scanner an, der

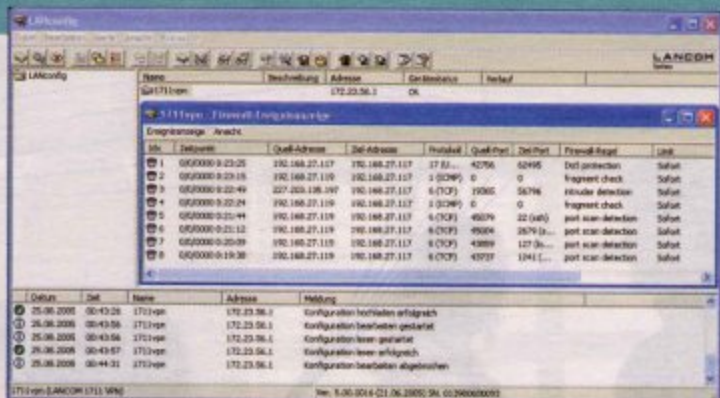
## VPN: Standard ohne Standard

Beim Virtual Private Network werden Datenpakete über ein Tunnelprotokoll verschlüsselt, um über das unsichere Internet eine abhörgeschützte Verbindung aufzubauen. Mit VPNs lassen sich Clients remote ans Firmennetz anbinden oder ganze Netzwerke koppeln. Sie sind bei Routern und Appliances inzwischen Standard. Die VPN-Technik ist aber nicht standardisiert. Aktuell kommen die Tunnelprotokolle IPsec und TLS/SSL zum Einsatz. Die veralteten Protokolle L2TP und PPTP sind ebenfalls noch weit verbreitet. VPN-

Clients sind in der Regel kostenpflichtig. Ihre Konfiguration kann gerade bei IPsec sehr komplex sein. Viele Hersteller gehen dazu über, die Clients eng auf ihre Appliance abzustimmen. Das vereinfacht die Einrichtung, schränkt aber die Kompatibilität zu anderen Herstellern ein. Vor dem Kauf einer Appliance sollte man daher prüfen, ob das Gerät alle erforderlichen Protokolle beherrscht und mit dem gewünschten Client kompatibel ist. Am einfachsten ist es, VPN-Client und Server vom selben Hersteller zu verwenden.



**Sonicwall berichtet dem Anwender auf der TZ 170 Zeitpunkt und Verursacher sowie den Zielports des Angriffs**



**Das per Windows-Utility unkompliziert abzurufende Protokoll der VPN 1711 von Lancom informiert über den registrierten Angriff**

allerdings nur Mails prüft. Ein echter Nachteil der Appliance ist ihr überzogener Preis. Zwar liegt der reine Gerätepreis mit 600 Euro am unteren Ende des Testfelds, für die Lizenzkosten gilt das Gegenteil. IDS, Content-Filter und Virens Scanner kosten 1220 Euro pro Jahr. Damit ist Checkpoint unterm Strich das teuerste Gerät im gesamten Testfeld.

**4 Note befriedigend • 75,4 Punkte**

**Lancom 1711 VPN**

Als einziges Gerät im Test setzt die Lancom 1711 VPN bei der Intrusion-Detection nicht auf Signaturen, sondern verwendet statisch in der Firmware hinterlegte Erkennungsmuster. Dass diese Architektur kein Nachteil sein muss, beweisen die Tests mit der BSI-Suite, bei der sich das Gerät keine Blöße gibt. Allerdings kann man wegen der Beschränkung auf Daten in der Firmware weder Virens Scanner noch Spamfilter für die 1711 VPN nachrüsten. Überraschend im Test ist zunächst der unterdurchschnittliche Datendurchsatz im Auslieferungszustand. Das Verhalten erklärt sich schnell, als das IDS für den zweiten Durchlauf aktiviert werden soll: Die 1711 VPN arbeitet immer mit aktivierter Intrusion-Detection, man kann sie nicht abschalten. Aktiviert man an den anderen Geräten im Test die Performance-hungrige IDS, erreicht Lancom immerhin die drittbesten Werte bei HTTP-Übertragungen und hat genug Reserven für den Betrieb an einer ADSL2-Leitung mit bis zu 24 MBit/s.

Jeder der vier im Gerät verbauten Netzwerkports lässt sich als WAN- oder DMZ-Port verwenden, womit inklusive des festen WAN-Ports bis zu vier Internet-Anbindungen zur Verfügung stehen. Diese lassen sich als kaskadierende Backup-Verbindungen konfigurieren. Darüber hat die 1711 VPN einen Load-Balancer-Modus, der mehrere Internet-Verbindungen parallel nutzt und so mehr Bandbreite zur Verfügung stellt.

Die hohe Flexibilität ist jedoch auch Schuld an einem Manko der Appliance. Den Testern fällt auf, dass die Programmierer des Web-Interfaces offensichtlich nicht mit der Fülle der Funktionen Schritt halten können. So fehlen dringend benötigte Funktionen zur komfortablen Einstellung der Firewall und

des IDS. Die mitgelieferte Windows-Applikation zur Konfiguration und Überwachung entschärft das Problem nicht.

VPN-Verbindungen lassen sich ebenso problemlos einrichten und verwalten wie Zertifikate. Die 1711 VPN ist das einzige Gerät im Test, das im Auslieferungszustand VPN-Verbindungen durch die Firewall zu einem zentralen VPN-Server im LAN gestattet.

Mit einem Anschaffungspreis von 600 Euro, der Firmware-Updates auf Lebenszeit enthält, ist die Lancom 1711 VPN das günstigste Gerät im Testfeld. Folgekosten entstehen keine. Anders als Astaro hat die VPN 1711 weder E-Mail- noch Surf-Protection. Das gute Abschneiden beim BSI-Test sowie die umfangreichen VPN-Funktionen bringen dem Produkt die »Budget-Empfehlung« ein.

**5 Note befriedigend • 66,6 Punkte**

**Cisco 871**

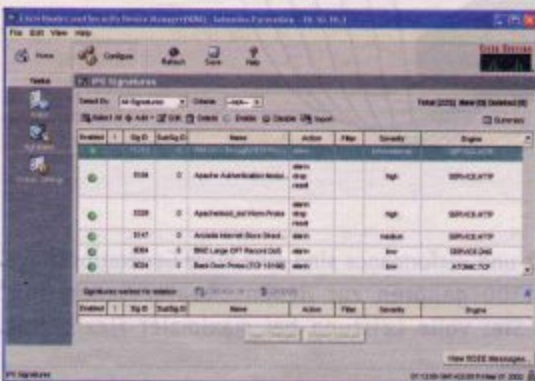
Die kleine Cisco hat Anschlüsse für vier LAN-Geräte, einen WAN-Zugang sowie eine serielle Konsole. Zusätzlich fallen den Testern die beiden USB-Ports auf, über die sich Krypto-USB-Sticks von Cisco anschließen lassen. Dank des im Vergleich extrem langen Stromkabels lässt sich die Cisco 871 deutlich flexibler platzieren als die Mitbewerber. Die zur Signalisierung des Zustands der einzelnen Verbindungen dienenden Leuchtdioden sind ungewohnt über die gesamte Frontblende verstreut, was ein schnelles Ablesen der Informationen erschwert.

Cisco setzt auf einen wenig performanten 266-MHz-Prozessor von Freescale. Die Appliance ist ausschließlich für den Betrieb

am DSL-Netz konzipiert, das belegen die Messwerte: Selbst ohne aktiviertes IDS reichen die Transferraten bei weitem nicht an die der Konkurrenz heran. Ist die Intrusion-Protection eingeschaltet, genügt der Datendurchsatz gerade noch den Anforderungen, wie sie der Betrieb an einer schnellen DSL-Leitung mit 6 MBit/s stellt. Keinen Anlass zur Kritik gibt die Funktion des IDS, die Alarmfunktionen sind aber verbesserungswürdig: Nur mit Mühe gelingt es den Testern, der Appliance Informationen über die Attacken der BSI-Suite zu entlocken. Cisco-Profis können das Gerät wie gewohnt über die Kommandozeile administrieren, für alle Normalsterblichen gibt es eine grafische Oberfläche. Das Management-Interface leitet den Benutzer komfortabel durch Setup und Feinkonfiguration. Dabei kommt eine Java-Applikation zum Einsatz, die im Speicher der Appliance abgelegt ist und so auf jedem angeschlossenen Client zur Verfügung steht. Mit ihrer Hilfe lassen sich VPN-Sitzungen komfortabel einrichten, und auch die Verwaltung von Zertifikaten geht flüssig von der Hand.

Mit einem Anschaffungspreis von 640 Euro und einer jährlichen Service-Pauschale von 50 Euro pro Jahr ist die 871 sehr günstig. Allerdings ist die Übertragungsleistung für aktuelle Verhältnisse auch nur ausreichend. Bei einem Wechsel auf zukünftige, schnellere Internet-Anbindungen dürfte die kleine Cisco schnell überfordert sein. Die preislich in der gleichen Klasse liegende Appliance von Lancom bietet erheblich mehr Leistung für noch weniger Geld.

**6 Note ausreichend • 63,2 Punkte**



**Die Signaturliste im Intrusion-Detection-System der Cisco 871 ist umfangreich und lässt sich komfortabel editieren**



**VPN 1711**

**Lancom**

www.lancom.de

600 Euro

ja

ja

nein

nein

600 Euro

**befriedigend**

**66,6**

befriedigend

66,7

ausreichend

58,3

ausreichend

62,5

gut

81,8

**871**

**Cisco**

www.cisco.de

640 Euro

50 Euro

ja

nein

nein

690 Euro

**ausreichend**

**63,2**

ausreichend

59,3

ausreichend

62,5

gut

81,3

ausreichend

59,1

Robuste Appliance mit Schwächen bei der Verwaltung. Konstant gute Durchsatzwerte und hohe Sicherheit trotz vergleichsweise einfachem IDS. Lebenslanger Update-Service inklusive. Load-Balancing über mehrere Internet-Verbindungen möglich.

Gute Abwehr von Attacken, aber Mängel bei der Benachrichtigung. Sehr komfortable Verwaltung über ein Web-Interface. Attraktiver Preis, aber vergleichsweise geringer Datendurchsatz. Nur für DSL-Anbindungen mit maximal 6 MBit/s geeignet.

5.00.0016

Intel 266 MHz

16 MByte/nein

4/2<sup>1)</sup>

nein<sup>2)</sup>/nein/1/nein

nein/ja/nein

ja/ja

ja/ja

ja/ja

ja/ja

ja/nein

12.8(T)

Freescall 266

128 MByte/nein

4/1

nein/1/nein/2

nein/ja/nein

ja/ja

ja/nein

ja/ja

nein/ja

ja/ja

ja/ja/ja

ja/ja/ja/ja

ja/ja

2048

25/17 MBit/s

ja/ja/ja

ja/ja/ja/ja

ja/ja

k. A.

k. A./k. A.

ja/nein

ja/nein

ja/nein

nein/nein

nein/nein

nein/nein

nein/nein

nein/nein

ja/nein

nein/nein

ja/nein

nein/nein

nein/nein

nein/nein

nein/nein

nein/nein

ja/ja

ja/ja

ja/nein

ja/ja

ja/ja

ja/ja

ja/nein

ja/nein

5/25

ja/ja/ja/ja/ja

ja/nein/ja/ja

20/20

ja/ja/ja/ja/ja

ja/ja/ja/ja

ja/ja/ja/ja

ja/ja/ja

ja/ja/ja

ja/ja/ja/ja

ja/ja/ja

ja/ja/nein

3,15 MByte/s

3,16 MByte/s

3,15 MByte/s

3,16 MByte/s

1,52 MByte/s

1,87 MByte/s

1,35 MByte/s

0,82 MByte/s

nein/ja/ja

(019 07) 641 00<sup>4)</sup>

3 Jahre

nein/ja/ja

(08 00) 101 67 93<sup>4)</sup>

2 Jahre



Produkt	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
Hersteller	Astaro	Zyxel	Sonicwall	Checkpoint
Internet	www.astaro.de	www.zyxel.de	www.sonicwall.de	www.checkpoint.de
Grundpreis Appliance	800 Euro	900 Euro	750 Euro	600 Euro
Standard-Support 1 Jahr	170 Euro	ja	ja	180 Euro
Intrusion-Detection (IDS)	ja	500 Euro	ja	1220 Euro
E-Mail-Schutz für 1 Jahr	230 Euro	180 Euro	ja	ja, in IDS
Surf-Protection für 1 Jahr	310 Euro	250 Euro	ja	ja, in IDS
Summe der Einzelpreise	1510 Euro	1830 Euro	750 Euro	2000 Euro
Gesamturteil (Note/Punkte)	gut 86,9	gut 80,7	befriedigend 77,8	befriedigend 75,4
Leistung (50 %)	sehr gut 96,3	befriedigend 77,8	befriedigend 74,1	gut 88,9
Ausstattung (20 %)	sehr gut 91,7	gut 87,5	befriedigend 66,7	ausreichend 62,5
Bedienung (15 %)	gut 81,3	sehr gut 93,8	gut 87,5	befriedigend 68,8
Service (15 %)	ausreichend 54,5	befriedigend 68,2	sehr gut 95,5	ausreichend 54,5

Fazit	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
	Einzig PC-basierte Lösung im Testfeld. Bester Datendurchsatz ohne IDS, sehr gute Transferaten mit IDS. Fehlerlose Abwehr aller Testattacken. Übersichtliches Management-Interface. Sehr gutes Preis-Leistungs-Verhältnis.	Konstant gute Leistungen mit und ohne IDS. Hohe Erkennungsrate von Angriffen, aber ungenaue Protokollierung. IDS und AV nur in Verbindung mit Turbocard erhältlich. Komfortables und übersichtliches Web-Interface.	Sehr gute Erkennung und Kennzeichnung von Angriffen. Bei aktivem IDS und Contentfilterung drastischer Einbruch der Transferate, für DSL aber ausreichend. Günstige jährliche Update-Preise.	Appliance mit gutem Datendurchsatz mit und ohne IDS. Sehr einfache Bedienung, für Profis aber zu wenig Einstellmöglichkeiten. Sehr gute Schutzfunktionen, jedoch hoher jährlicher Subskriptions-Preis.

Ausstattung	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
Firmware-Version	6002	3.64(WZ.4)	3.1.0.6-74s	5.0.90
Prozessor	VIA C3 666MHz	Intel 400 MHz	Sonicwall	Checkpoint
Arbeitsspeicher/Festplatte	256 MByte/20 GByte	64 MByte/nein	64 MByte/nein	64 MByte/nein
LAN-Ports/WAN-Ports	2/1	4/2	5/1	4/2
DMZ-Port/Konsolen-Ports/Seriell/USB	nein/nein/1/2	nein <sup>2)</sup> /1/1/nein	1/1/nein/nein	1/nein/1/nein
KVM-Anschluss/Reset-Taster/Sonstige Slots	ja/nein/nein	nein/ja/PC-Card	nein/ja/nein	nein/ja/nein

WAN-Verbindung	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
DSL-Modem (PPPoE)/Kabel-Modem	ja/ja	ja/ja	ja/ja	ja/ja
LAN-Verbindung/PPTP	ja/ja	ja/ja	ja/ja	ja/ja
Backup-Verbindung/Auto-Failover	ja/ja	ja/ja	nein <sup>3)</sup> /nein <sup>3)</sup>	ja/ja
Load-Balancing/Traffic Redirect	nein/nein	ja/ja	nein <sup>3)</sup> /nein <sup>3)</sup>	nein/ja
MAC-Cloning/High availability	ja/nein	ja/nein	ja/nein	ja/ja

Router	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
DNAT/SNAT/Externer Default-Gateway	ja/ja/ja	ja/ja/ja	ja/ja/ja	ja/ja/ja
Port-Weiterleitung/DMZ/Statisch/Dynamische Routen	ja/ja/ja/ja	ja/ja/ja/ja	ja/ja/ja/ja	ja/ja/ja/ja
Multiple Subnetze/virtuelle Interfaces	ja/ja	ja/ja	ja/ja	ja/ja
Sessions	60 000	10 000	6000	8000
Firewall-/VPN-Durchsatz	100/30 MBit/s	90/40 MBit/s	90/30 MBit/s	80/20 MBit/s

Firewall	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
Intrusion-Detection/Zertifikat-Blocker	ja/ja	ja/nein	ja/ja	ja/nein
E-Mail-/SMS-Notification	ja/nein	ja/nein	ja/nein	ja/nein
SNMP-Notification/Contentfilter	ja/ja	ja/ja	ja/ja	ja/ja
ActiveX-/Java-Blocker	ja/ja	ja/ja	ja/ja	nein/nein
Cookie-/Proxy-Blocker	ja/nein	ja/ja	ja/ja	nein/nein
Virens Scanner Mail/Webtraffic	ja/ja	ja/ja	ja/ja	ja/nein
Spam-Schutz/SIP-Support	ja/ja	ja/ja	nein <sup>3)</sup> /ja	nein/nein

Sonderfunktionen	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
DHCP-Server/Echter DNS-Server	ja/nein	ja/ja	ja/nein	ja/nein
DNS-Relay/DNS-Cache	ja/ja	ja/ja	nein/nein	ja/nein
DNS-Autoupdate/DynDNS-Support	nein/ja	nein/ja	nein/ja	nein/ja
Bandwidth-Management/Zeitserver	nein/nein	ja/nein	nein <sup>3)</sup> /nein	ja/nein

VPN	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
Sitzungen aktiv/konfigurierbar	100/unbegrenzt	35/40	25/50	10/10
AES/3DES/DES/SHA1/MD5	ja/ja/ja/ja/ja	ja/ja/ja/ja/ja	ja/ja/ja/ja/ja	ja/ja/ja/ja/ja
Preshared Key/RSAX.509-Zertifikat/RADIUS	ja/ja/ja/ja	ja/nein/ja/ja	ja/ja/ja/ja	ja/nein/ja/ja

Verwaltung	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
HTTP/HTTPS/SNMP/Config (save/load)	ja/ja/ja/ja	ja/ja/ja/ja	ja/ja/ja/ja	nein/ja/ja/ja
Telnet/SSH/Terminal (seriell)	nein/ja/ja	ja/ja/ja	nein/nein/ja	nein/ja/ja
Protokoll intern/extern (Syslog)/per Mail	ja/ja/nein	ja/ja/ja	ja/ja/ja	ja/ja/nein

Messwerte	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
Datendurchsatz FTP-Transfer ohne IDS	10,60 MByte/s	4,08 MByte/s	4,47 MByte/s	9,05 MByte/s
Datendurchsatz HTTP-Transfer ohne IDS	10,00 MByte/s	4,10 MByte/s	4,22 MByte/s	8,54 MByte/s
Datendurchsatz FTP-Transfer mit IDS	4,33 MByte/s	3,49 MByte/s	0,95 MByte/s	8,65 MByte/s
Datendurchsatz HTTP-Transfer mit IDS	6,54 MByte/s	3,52 MByte/s	0,74 MByte/s	1,51 MByte/s

Services	ASG 110	Zywall 35	TZ 170 Total Secure	Safe@Office 225
Handbuch gedruckt/PDF/Quickstart-Guide	ja/nein/ja	nein/ja/ja	nein/ja/ja	ja/ja/ja
Hotline	(08 00) 278 27 61 <sup>4)</sup>	(018 05) 21 32 47 <sup>5)</sup>	(08 00) 000 36 66 <sup>6)</sup>	(009 72) 36 11 51 00
Garantie	2 Jahre	2 Jahre	2 Jahre	2 Jahre

<sup>1)</sup> 1 x Fast Ethernet, 1 x ISDN <sup>2)</sup> alle LAN-Ports sind als DMZ-Ports definierbar <sup>3)</sup> nur mit Sonic Enhanced OS <sup>4)</sup> kostenfrei <sup>5)</sup> 12 Euro pro Minute <sup>6)</sup> 1,24 Euro/Min. bei Anrufen aus dem deutschen Festnetz

# Angriffe vorab erkennen

**Intrusion-Detection-Systeme (IDS) sind eine sinnvolle Ergänzung zur obligatorischen Firewall. Sie erkennen Angriffe auf das Netzwerk und blocken sie frühzeitig ab. Ihr Schutz ist eine Stufe tiefer im Übertragungsprotokoll angesiedelt als bei der Firewall. Eine wichtige Rolle spielt auch die Position des IDS im Netz.**

Eine einfache Firewall prüft eintreffende Datenpakete anhand der verwendeten Ports: Ist der Zugriff auf den adressierten Zielport vom Internet erlaubt, lässt sie die Pakete durch, ansonsten werden sie verworfen. Einen Schritt weiter gehen Firewalls mit Stateful-Packet-Inspection. Sie prüfen zusätzlich, ob das eingehende Datenpaket eine Antwort auf eine Anfrage aus dem LAN ist. Nur dann hat das Paket eine Beziehung zum lokalen Netz und darf passieren.

Leider genügt der Schutz durch eine Firewall nicht, alle Angriffe effektiv abzuwehren. Ursache dafür sind Anfälligkeiten in den eingesetzten Betriebssystemen und Anwendungen. Diese lassen sich durch mutwillig erzeugte, fehlerhafte Pakete aus dem Tritt bringen. Manipulierte Header oder überlange Datenpakete führen zu Buffer-Underruns oder -Overflows. Dadurch erhält der Angreifer im schlimmsten Fall die völlige Kontrolle über das attackierte System.

## Intrusion-Prevention ist Standard

Diese Lücke schließen Intrusion-Detection-Systeme, die von einigen Herstellern auch als Intrusion-Prevention-Systeme bezeichnet werden. In der Funktion gibt es zwischen den Systemen keinen Unterschied. Angriffe werden auf Paketebene nicht nur erkannt, sondern auch geblockt. Ähnlich einem Virens Scanner arbeiten sie meist mit einer Liste von Signaturen. Diese beschreiben jedoch nicht nur den Schadcode, sondern nennen auch den Zielport und die Art der am Datenpaket vorgenommenen Modifikation. Anhand der Liste untersucht das IDS die Datenpakete und entscheidet, ob es sich um einen Angriffsversuch oder zulässige Daten handelt. Nur zulässige Daten können das IDS passieren. Der Vorteil einer Signaturliste ist, dass mit ihrer Hilfe nicht nur die Erkennung optimiert, sondern auch der Anwender präziser über die Art des Angriffs informiert werden kann.

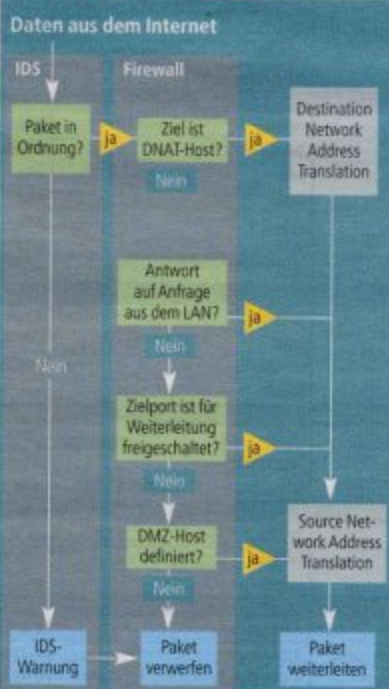
Zwingend erforderlich ist die Signaturliste nicht. Bei Lancom wird der Datenverkehr anhand der RFC-Spezifikationen geprüft. Dieses Verfahren hat den Nachteil, dass der Anwender nicht detailliert über die Art des Angriffs informiert werden kann. Beim Test der SMB-Appliances fällt allerdings auf, dass auch einige der Kandidaten mit Signaturliste die Testatta-

cken lediglich als illegale Datenpakete melden. Das liegt daran, dass bei diesen Produkten die IDS hinter der Firewall platziert ist. Weil die Firewall einen Teil der eingehenden Daten als nicht angefordert erkennt, verwirft sie die Pakete. Das dahinter liegende IDS bekommt sie nicht zu sehen. Angriffe auf das eigene Netz werden dann nicht als solche erkannt.

## Optimal: IDS vor der Firewall

Besser ist es, das IDS in der Verarbeitungsreihenfolge vor die Firewall zu setzen. Für die Hersteller bedeutet das jedoch, dass sie leistungsfähigere Hardware verbauen müssten, um weiterhin akzeptable Transferraten zu erreichen. Der Scan aller Pakete durch das IDS ist sehr rechenintensiv, bei schwachen CPUs bricht die Performance ein. Nur wenige Hersteller geben Informationen über die interne Arbeitsweise ihrer Produkte preis. Es empfiehlt sich daher, selbst mit der BSI-Suite zu testen. Die Rate der erkannten und benannten Attacken gibt einen Anhaltspunkt darüber, mit welcher Art von IDS man es zu tun hat. *Stefan Rubner/SST*

## IDS vor Firewall



**IDS filtert Daten schon vor der Firewall: Nur die Appliances von Astaro und Sonicwall verwenden diese Topologie**

## Wertungen

Gesamtwert 100 %



Leistung 50 %



Ausstattung 20 %



Bedienung 15 %



Service 15 %

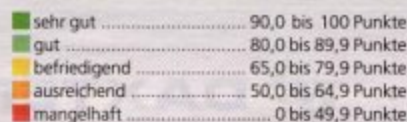


**Leistung (50 %)** Erkennungsrate der Angriffe und vorhandene Sicherheitslücken, Datendurchsatz mit und ohne aktivierte IDS-Funktion

**Ausstattung (20 %)** Umfang der Schutzfunktionen, Anzahl der Anschlüsse, verwendete CPU und installierter Hauptspeicher

**Bedienung (15 %)** Installation und Konfiguration, Bedienung der IDS-Funktionen, Zertifikatverwaltung, VPN-Management

**Service (15 %)** Garantiedauer, Hotline, Grundkosten, Servicekosten



# So testen wir

## Hohe Transferraten sind nicht alles, auch die Intrusion-Detection der Geräte wird im Labor intensiv geprüft.

Um die Leistungsfähigkeit der in den Appliances eingebauten Schutzfunktionen zu testen, verwenden die PCpro-Experten die BSI OSS Security Suite ([www.bsi.de](http://www.bsi.de)), mit deren Tools sie die Probanden intensiv unter Beschuss nehmen. Die BSI-Suite simuliert zum einen bekannte Angriffe auf Schwachstellen in Betriebssystemen und Netzwerkgeräten, die von den Appliances erkannt und gemeldet werden sollten. Zum anderen prüft sie, ob die Appliances selbst über Schwachstellen angreifbar sind.

Bei der Angriffsabwehr bestehen alle Kandidaten den Test mit Bravour: Die Laborexperten registrieren keine einzige erfolgreiche Attacke. Anders sieht das Bild jedoch bei der Benachrichtigung des Anwenders aus. Lediglich die Sonicwall TZ 170 meldet dem Administrator die meisten Angriffe auch als solche, während der Rest des Testfelds sie bereits in der Firewall abfängt und nur als unzulässige Pakete markiert. So verpuffen die Attacken zwar wirkungslos, allerdings bleibt auch dem Administrator der versuchte Einbruch ins Netz verborgen.

Ein Problem meldet der BSI-Scanner bei der Lancom 1711 VPN. Das Protokoll für den Schlüsselaustausch bei IPsec-Verbindungen sei eventuell fehlerhaft, im schlimmsten Fall eine DoS-Attacke auf die VPN-Verbindungen möglich. Hierbei handelt es sich aber um eine bekannte Eigenheit der Lancom-Appliances. Im Auslieferungszustand ist VPN-Passthrough aktiviert, um Anwendern den Zugriff auf einen hinter der Firewall arbeitenden VPN-Server zu gewähren. Dazu müssen eingehende VPN-Anfragen zunächst angenommen und geprüft werden. Das führt

zu der beschriebenen Fehlinterpretation durch den BSI-Scanner. Eine Sicherheitslücke ist dieses Verhalten nicht, außerdem lässt sich die Passthrough-Funktion abschalten.

## Einfluss auf den Datendurchsatz

In einem weiteren Test ermitteln die Prüfer die Auswirkung der Schutzmechanismen auf den erzielbaren Datendurchsatz. Dazu nehmen sie Dateitransfers mit den im Internet am häufigsten auftretenden Protokollen FTP und HTTP vor. Der erste Durchlauf erfolgt mit deaktivierten Filtern und Scannern. Hier fällt die Cisco 871 mit niedrigen Datenraten auf, die zeigen, dass das Produkt nicht für den Betrieb an schnellen Internet-Leitungen konzipiert ist.

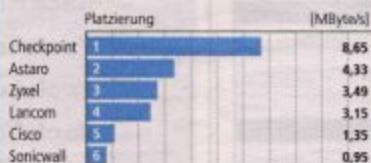
Im nächsten Testlauf sind Intrusion-Detection, Firewall und – sofern vorhanden – Contentfilter aktiv. Die Leistung der Sonicwall TZ 170 bricht dann schon bei den FTP-Transfers deutlich ein. Bei HTTP-Übertragungen zeigen neben Sonicwall auch die Checkpoint und die Cisco einen gravierenden Leistungsabfall. Die von diesen Geräten erzielten Werte genügen zwar den Anforderungen einer DSL-Anbindung mit 6 MBit/s, für ADSL2-Anschlüsse mit bis zu 24 MBit/s sind sie jedoch nicht mehr geeignet.

Die Verwaltung erfolgt bei den meisten Produkten im Testfeld bevorzugt mit Hilfe der integrierten Web-Oberfläche. Diese ist in der Regel sehr komfortabel und übersichtlich. Außerdem fließen in die Wertung Alarmfunktionen ein. Alarmmeldungen sollten sich per Mail an den Administrator oder per SNMP an ein zentrales Management-System übermitteln lassen.

Stefan Rubner/SST

## Messungen mit IDS

FTP-Transfer mit IDS



▶▶▶ besser

## Messungen ohne IDS

FTP-Transfer ohne IDS



▶▶▶ besser

HTTP-Transfer mit IDS



▶▶▶ besser

HTTP-Transfer ohne IDS



▶▶▶ besser