Sicher ohne Flaschenhals

Pilottest Intrusion-Prevention – Security-Appliances bieten heute mehr als nur Firewall und VPN. Was Intrusion-Prevention-Lösungen leisten, mussten fünf Exemplare dieser Gattung in den Real-World Labs unter Beweis stellen.

Würmer, Viren, Trojaner, Denial-of-Service-Attacken oder Applikationsangriffe sind moderne Gefahren, die schon viel Schaden angerichtet haben und die weiter in ihrem Bedrohungspotential anwachsen. Dabei nutzen gegen diese Angriffstechniken traditionelle Firewalls alleine nicht viel. Intrusion-Detection-Systeme, die seit ein paar Jahren auf dem Markt sind, stellen als digitale Alarmanlagen zwar Angriffe fest, alarmieren aber lediglich die IT-Verantwortlichen, die sich in Anbetracht der Geschwindigkeit moderner Angriffe dann bestenfalls um die Schadensbegrenzung kümmern können. Die Fähigkeit sich selbst zu verteidigen sollen dagegen Intrusion-Prevention-Systeme, kurz IPS, in Unternehmensnetze tragen.

Funktionsweise

IPS sollen vielfältige Gefahren und Angriffe innerhalb des Unternehmensnetzes erkennen und geeignete Gegenmaßnahmen treffen, um eventuelle Schäden zu vermeiden. Hierzu müssen sie den Datenverkehr mitlesen und auf vorgegebene Muster oder Signaturen prüfen, um bekannte Angriffe abwehren zu können. Darüber hinaus sollen eine intelligente Protokollanalyse und verhaltensbasierte Algorithmen auf Applikations-Level dem IPS ermöglichen, weitere Angriffsformen zu erkennen und abzuwehren. Dazu zählen insbesondere bisher nicht bekannte Angriffe. IPS arbeiten auf allen relevanten Ebenen des OSI-Modells ab Ebene 3 aufwärts und untersuchen möglichst viele Protokolle.

Zwei Arten von IPS sind zu unterscheiden, netzwerkbasierte und Host-basierte Lösungen. Während letztere auf den potentiell gefährdeten Systemen wie Servern oder Notebooks selbst als Software installiert laufen, werden netzwerkbasierte IPS als Appliance im Netzwerk integriert. Beide Typen ergänzen sich sinnvoll im Unternehmensnetz. Gegenstand unserer Tests waren aber ausschließlich netzwerkbasierte IPS.

Was solche Geräte denn nun genau an Funktionalität bieten müssen, ist nach dem Studium des üblichen Marketingmaterials eher unklar. Aufschlussreich ist bei der Klärung dieser Frage eine Studie von Gartner (G00123902, »Seven Key Selection Criteria for Network IPS«, Greg Young, 11/01 2004). Als Mindestfunktionsumfang einer Netzwerk-IPS definiert diese Studie Schutz gegen:

- Denial-of-Service- und Distributed-Denial-of-Service-Angriffe,
- Abweichungen vom erwarteten Protokoll-Verhalten,
- generelle Protokoll-Anomalien sowie
- Versuche, feindliche Signaturen über die Nutzlast vieler Pakete verteilt einzuschleusen.

Ein »echtes« Netzwerk-IPS ist nach Gartner ein System, das:

- als aktive Inline-Netzwerkkomponente mit Leitungsgeschwindigkeit arbeitet,
- dabei alle Datenpakete zusammensetzt und prüft,
- Regeln anwendet, die auf verschiedenen Methoden basierend die Paketströme mindestens auf Protokoll-Anomalien, feindliche Signaturen und ungewöhnliches Verhalten untersucht und
- alle Pakete verwirft, die zur erkannten feindlichen Session gehören, und nicht nur ein Reset verschickt.

IPS dürfen die vorhandenen Bandbreiten im Unternehmensnetz nicht einschränken, damit der Datenverkehr und alle Anwendungen innerhalb des Unternehmensnetzes ungebremst weiter laufen können. Daraus folgt, dass sie ebenso wie Switches mit Leitungsgeschwindigkeit arbeiten müssen, auch wenn die nominelle Bandbreite von beispielsweise 1 GBit/s zeitweise ausgeschöpft wird oder gerade Angriffe auf das Netzwerk erfolgen. Selten sind sich die Hersteller in der IT-Branche so einig wie im Fall der Anforderungen im Bereich IPS-Perfomance: Netzwerk-IPS sind Inline-Systeme, die genauso wie LAN-Switches in allen Fällen mit Leitungsgeschwindigkeit und ohne nennenswerte Latenzzeiten arbeiten müssen. Schaffen sie es nicht, den gesamten zulässigen Datenverkehr zu transportieren, dann drohen Datenverluste mit allen bekannten Konsequenzen.

TESTFELD

IPS-Appliances

- ISS Proventia G2000
- McAfee IntruShield 4010
- Sonicwall Pro 5060
- 3Com TippingPoint 2400
- Top Layer Attack Mitigator IPS5500

Internet Security Systems
Proventia G2000

Wie viel Performance und Sicherheit IPS heute bieten, haben wir in unseren Real-World Labs an der FH Stralsund untersucht. Das Testfeld bildeten »ISS Proventia G2000«, »McAfee IntruShield 4010«, »Sonicwall Pro 5060«, 3Coms »TippingPoint 2400« und »Top Layer Attack Mitigator IPS5500«. Im Verlauf unseres Tests haben wir die Geräte auf ihre Performance und auf die Sicherheit, die sie bieten, untersucht.

UDP-Performance bidirektional

Den UDP-Performance-Test haben wir mit unseren »Smartbits 6000C« von Spirent durchgeführt. Ermittelt haben wir hier das Datendurchsatzverhalten der Testgeräte in Abhängigkeit von den zu übertragenden Paketgrößen. Der Durchsatz ist dabei als der Wert definiert, bei dem keine Datenverluste auftreten. Die Messung haben wir mit UDP-Paketen von 1518 Byte, 1024 Byte, 512 Byte und 64 Byte durchgeführt. Es wurden zwei Datenströme mit je 1GBit/s aufgesetzt, so dass die Gesamtbelastung des Testgerätes bei maximal 2 GBit/s lag. Das Ergebnis ist in Prozent angegeben und bezieht sich auf die maximale Übertragungsleistung von 2 GBit/s.

Volle Leitungsgeschwindigkeit lieferten die Systeme von ISS, McAfee, Tipping Point und Top Layer bei dieser Messreihe. Bei der Sonicwall-Pro-5060 war die UDP-Performance-Messung dagegen nicht durchführbar, weil diese nicht im Transparent-, sondern nur im Router-Modus stabil gearbeitet hat. Im normalen Layer-2-Modus hat die Sonicwall-IPS als ARP-Proxy gearbeitet und dabei die originalen MAC-Adressen im Ethernet-Header mit denen der IPS ausgetauscht. In diesem Modus konnten aber unsere Smartbits und das Testtool Tomahawk nicht arbeiten, da sie die originalen MAC-Adressen im Netzverkehr erwarteten. Die IPS hatte über das GUI prinzipiell die Möglichkeit, diese ARP-Proxy-Funktionaliät auszuschalten. Allerdings hatte diese Funktion in unserem Test keine Auswirkungen auf das Verhalten der IPS, es arbeitete weiterhin im ARP-Proxy-Modus und änderte die MAC-Adressen weiterhin. Deshalb wurde die Sonicwall-IPS in den Layer-3-Modus konfiguriert. In diesem Modus konnten wir mit den Spirent-Geräten Smartbits und Avalanche/Reflector sowie Metasploit die Messungen durchführen. Die Messungen mit Tomahawk unten sind in diesem Modus ebenfalls nicht möglich, da Tomahawk ein Testtool für Layer-2-Systeme ist. Lediglich die Verwendung von 64-Byte-Paketen machte dem Testfeld Probleme. Bei dieser Messung ging der Datendurchsatz der ISS-Proventia-G2000 auf 36 Prozent zurück. Bei McAfees Intrushield-4010 waren noch Durchsätze von rund 54 Prozent möglich. Mit 64 Prozent schaffte Tipping Points 2400 den höchsten Durchsatz mit 64-Byte-Paketen. Top Layers Attack-Mitigator-IPS5500 kam hier dagegen nur auf 32 Prozent Datendurchsatz.

TESTERGEBNISSE INLINE-IPS-SYSTEME

	Internet Security Systems Proventia G2000	McAfee IntruShield IPS 4010	SonicWALL Pro 5060	3 Com TippingPoint 2400	Top Layer Networks Attack Mitigator IPS5500
Exploits					
T1 - linux-samba_trans2open	●	●	●	●	●
T2 - win32_apache_chunked (Port 80)	●	●	●	●	●
T3 - win32_apache_chunked (Port 8000)	●	●	●	●	●
T4 - win32_dcom (Port 135)	●	●	●	●	●
T5 - win32_lsass (Port 139)	●	●	●	●	●
T6 - win32_lsass (Port 445)	●	●	●	●	●
Exploits - fragmentiert					
T1 - linux-samba_trans2open	●	●	●	●	●
T2 - win32_apache_chunked (Port 80)	●	●	●	●	●
T3 - win32_apache_chunked (Port 8000)	●	●	●	●	●
T4 - win32_dcom (Port 135)	●	●	●	●	●
T5 - win32_lsass (Port 139)	●	●	●	●	●
T6 - win32_lsass (Port 445)	●	●	●	●	●
Browser-Check (http1.0 / http1.1)					
T1 - IE6.0: Read local Files via GetObject II	● / ●	● / ●	-	● / ●	● / ●
T2 - IE6.0: Read local Files via execScript	● / ●	● / ●	-	● / ●	● / ●
T3 - IE6.0: Execute any Program via showhelp	● / ●	● / ●	-	● / ●	● / ●
T4 - IE6.0: Execute any Program via Cache-Objects	● / ●	● / ●	-	● / ●	● / ●
T5 - IE6.0: Read local Files via Dialog-Function	● / ●	● / ●	-	● / ●	● / ●
T6 - IE6.0: Load and Execute any File via Object-Tag	● / ●	● / ●	-	● / ○	● / ●
T7 - IE6.0: Load and Execute any File via ADODB.Stream	● / ●	● / ●	-	● / ●	● / ●
T8 - IE6.0: Load and Execute any File via mhtml-Redirects	● / ●	● / ●	-	● / ●	● / ●
T9 - IE6.0: IE hangs after access to c:\aux	● / ●	● / ●	-	● / ●	● / ●
T10 - IE6.0: NIMDA-Virus	● / ●	● / ●	-	● / ●	● / ●

● = geblockt und protokolliert; ○ = geblockt; ● = nicht erkannt; – = Test nicht durchführbar

TCP-Performance

Den TCP-Performance-Test haben wir mit Avalanche/Reflector von Spirent durchgeführt. Die Messung der TCP-Übertragungsleistung basiert auf dem HTTP-Protokoll, wobei der Avalanche als Client spezielle HTTP-Requests sendet. Der Reflector agiert als HTTP-Server und beantwortet diese Anfragen je nach Messung mit 1518, 1024 und 512 Byte großen Paketen. Daraus resultiert ein asynchroner Netzverkehr zwischen Avalanche (Client) und Reflektor (Server). Als Messergebnis haben wir die unidirektionale TCP-Übertragungsleistung in MBit/s vom Reflektor (Server) zum Avalanche (Client) ermittelt.

Auch hier herrscht nahezu Gleichstand zwischen den einzelnen Systemen. Bis auf Sonicwall schafften alle Leitungsgeschwindigkeit oder lagen nur marginal darunter. Sonicwalls Pro-5060 erreichte dagegen lediglich Durchsätze von rund 200 MBit/s.

IPS-Check Netzverkehr

Den Netzverkehr-Test haben wir mit den HP-Servern DL380/2 und den Tomahawk-Tools durchgeführt. Bei diesem Test haben wir unterschiedlichen Netzverkehr mit anomalen Inhalten über die IPS gesendet. Als Messergebnis haben wir die Erkennungsrate, das Logging und das Blocken der verschiedenen Exploits ermittelt.

McAfee
IntruShield IPS 4010

Vier von sechs Anomalien hat Top Layers Attack-Mitigator-IPS5500 erkannt und geblockt. Drei von sechs Treffern schaffte McAfees Intrushield-4010 in dieser Disziplin. Tipping Points 2400 hat zwei von sechs Anomalien erkannt und geblockt. Die ISS-Proventia-G2000 hat dagegen alle Anomalien unbeachtet gelassen. Sofern die Systeme Anomalien erkannt haben,

TECHNISCHE DATEN INLINE-IPS-SYSTEME

	Internet Security Systems Proventia G2000	McAfee IntruShield IPS 4010	SonicWALL Pro 5060	3Com TippingPoint 2400	Top Layer Networks Attack Mitigator IPS5500
Anzahl Ports					
Fast-Ethernet	8	0	0	1	8
Gigabit-Ethernet	8	12	6	8	6
Seriell	1	2	1	1	1
USB 2.0	4	–	–	1	2
Hardware/Betriebssystem					
Prozessor (Typ), MHz	2 Intel Xeon 3,60GHz	k.A.	Intel Xeon, 2,4 GHz	Pentium 4, 3,4 GHz	prop. Netzwerk-prozessoren
Anzahl CPUs	2	k.A.	1	k.A.	7
Anzahl ASICS	–	k.A.	1	4	7
Anzahl FPGA	–	k.A.	–	2	2
Arbeitsspeicher in MByte	3072	k.A.	512 (RAM), 64 (Flash)	2048	k.A.
Betriebssystem Name/Version	Linux / –	k.A.	SonicOS / 3.1	customized VxWorks Real-time-OS	proprietär
IPv6-Unterstützung f. alle Funktionen	●	○	○	○	●
IPS-Funktionen / Schutz vor					
Würmern	●	●	●	●	●
Viren	●	●	●	●	●
Trojanern	●	●	●	●	●
Server-Site-Attacken	●	●	●	●	●
Phishing-Attacken	●	○	○	●	●
Spyware	●	●	●	●	●
Auf viele Pakete verteilte Signaturen	●	●	●	●	●
Erkennung von Signaturen in Archiven (zip etc.)	●	●	●	●	○
DoS	●	●	●	●	●
DDoS	●	●	●	●	●
Protokoll-Missbrauch / -Anomalien	●	●	●	●	●
Frei definierbare Filterregeln	●	●	●	●	●
Sicherheitsfunktionen					
Statefull-Inspection-Firewall	○	●	●	○	●
Application-Gateway-Proxies	○	●	○	○	○
Spam-Filter	○	●	●	○	○
AAA-Support	○	●	k.A.	●	●
DHCP	○	●	●	○	○
Verhalten bei Überlast					
Blockieren der Datenströme	●	●	●	opt.	keine neuen Verbindungen
Ungefilterte Passage der Datenströme	opt.	●	○	opt.	○
Hochverfügbarkeit					
Maximale Cluster-Größe	2	2	2	2	8
Cluster über 3rd-Party	●	k.A.	●	opt.	○
Cluster über externen Switch	●	k.A.	●	opt.	8
Cluster über Netzwerk-Link	●	k.A.	●	k.A.	2
Redundanter Netzanschluss 230 Volt	●	●	○	●	●
Erkennung des Geräteausfalls	●	●	●	●	●
Festplattenlaufwerk austauschbar	●	○	k.A.	k.A.	k.A.
Fail-over im passiven Modus	●	●	●	●	●
Monitoring					
CPU überwacht	●	●	●	●	●
Speicherauslastung gemessen	●	●	●	●	●
Port-Auslastung gemessen	○	●	●	●	●
Synchronisierung überwachen	●	●	●	●	●
Software überwacht	●	●	k.A.	●	●
Schwellenwerte für Auslastung mögl.	● (fixed)	○	●	●	●
Log-Verhalten bei Überlast					
Stopp des Loggings	●	○	○	●	○
Blockieren des Traffic	●	●	●	○	○
Logging immer gewährleistet	●	○	●	●	●
Alarm bei Überschreiten von Grenzwerten					
Per E-Mail	●	○	●	●	●
Per SMS	●	○	○	○	●
Management					
Telnet	○	○	●	●	●
Rollenbasierte Verwaltung	●	●	●, mit GMS	●	●
Auditing-fähig	●	●	○	●	●
SSH-Support	●	●	○	●	●
HTTP	○	○	●	●	●
HTTPS	●	●	●	●	●
Autom. Synchronisation im Cluster	●	●	●	●	●
Synchronisation über multiple Pfade	k.A.	●	●	○	k.A.
Out-Band-Management	k.A.	●	○	●	●
Häufigkeit der Signatur-Updates pro Woche	mind. 1	14-tägig	stündlich / nach Bedarf	2 x	nach Bedarf
Automatische Firmware-Updates	●	○	●	○	●
Outsourcing des Managements mögl.	●	●	●	●	●
Webadresse	www.iss.net	www.mcafee.com/de	www.sonicwall.com	www.tippingpoint.com	www.toplayer.com

● = ja; ○ = nein; k.A. = keine Angabe; opt. = optional

Quelle: Angaben der Hersteller

haben sie diese auch geblockt und den Vorgang protokolliert. Die vergleichsweise schlechte Erkennungsrate kann den IPS-Systemen allerdings nur bedingt angelastet werden, da diese Anomalien von Firewalls herausgefiltert werden sollten. Und diese klassischen Security-Systeme sollen ja nicht durch IPS ersetzt, sondern ergänzt werden. Bei der Sonicwall-Pro-5060 konnten wir diesen Test aus genannten Gründen nicht durchführen.

Exploits-Test

Der Exploits-Test wurde mit den HP-Servern DL380/2 und den Tools Tomahawk und Metasploit durchgeführt. Bei diesem Test haben wir verschiedene Exploits über die IPS gesendet, die auf Schwächen der Betriebssysteme oder angebotener Dienste abzielten. Die Expoits haben wir nicht-fragmentiert und fragmentiert gesendet. Als Messergebnis dient die Erkennung, das Logging und das Blocken der verschiedenen Exploits.

Ausnahmslos alle Expoits haben ISS-Proventia-G2000, McAfee-Intrushield-4010, Tippingpoint-2400 sowie Top Layers Attack-Mitigator-IPS5500 erkannt und ordnungsgemäß verarbeitet. Lediglich Sonicwalls Pro-5060 hatte Probleme mit einem nicht fragmentierten Expoit und konnte alle fragmentierten Exploits nicht erkennen. Diese Funktion ist bei der Sonicwall-IPS explizit einzustellen. Das Aktivieren der Funktion führte aber dazu, dass selbst das Zusammensetzen eines fragmentierten ICMP-Paketes zum Absturz der IPS führte.

Browser-Check-Test

Auch diesen Browser-Check-Test haben wir mit den HP-Servern DL380/2 und dem Tool Tomahawk durchgeführt. Bei diesem Test haben wir

SonicWALL Pro 5060

aufgezeichneten Netzverkehr über die IPS gesendet, der auf die Ausnutzung von Schwächen in Browsern abzielt. Den Test haben wir sowohl mit HTTP 1.0 als auch HTTP 1.1 durchgeführt. Im Fall von HTTP 1.0 sind dabei html-Dateien zu analysieren. Haben wir HTTP 1.1 verwendet, waren die Daten zusätzlich komprimiert. Als Messergebnis dient die Erkennung, das Logging und das Blocken der verschiedenen Exploits.

Mit Ausnahme von Top Layers Attack-Mitigator-IPS5500, die lediglich zwei von zehn kom-

3Com
TippingPoint 2400

primierten Attacken nicht erkannte, hatten alle IPS-Systeme im Testfeld hier deutliche Schwächen. Die Bewertung dieses Verhaltens ist schwierig, weil hier die Hersteller mehr oder weniger unterschiedliche Standpunkte haben. Die einen sagen, es wäre nicht Aufgabe der IPS, sondern Aufgabe entsprechender Tools auf den Hosts in Abhängigkeit von den verwendeten Betriebssystemen und Browsern.

Unabhängig davon betonten aber alle Hersteller, dass es durch die mögliche Vielfalt in den übertragenen HTTP-Daten ein sehr schwieriges Thema sei, an dem man aber arbeitet und Lösungen mit in die IPS integrieren möchte. Trotz Einsatz einer Netzwerk-IPS kommen IT-Verantwortliche derzeit noch nicht darum herum, auch auf den Endsystemen entsprechende Sicherheitsmaßnahmen durchzuführen und entsprechende Tools zu installieren.

File-Transfer

Den File-Transfer-Test haben wir mit zwei Standard-PCs und dem Tool Tomahawk durchgeführt. Wir haben ein rund 1,5 GByte großes ISO-Image zwischen den PCs übertragen. Als Übertragungsprotokolle kamen dabei NFS, FTP und HTTP zum Einsatz, wobei ein PC die Netzdienste bereitstellt und der zweite PC als entsprechender Client fungiert. Als Messergebnis dient die notwendige Übertragungszeit ohne und mit Exploit-Belastung des Testgerätes.

Ohne Belastung durch Exploits lagen alle gemessenen Übertragungszeiten zwischen rund 60 und 70 Sekunden. Die zusätzliche Belastung durch Exploits hat an den gemessenen Übertragungszeiten auch keine großen Abweichungen gegenüber der vorhergehenden Messung verursacht. Einzige Ausnahme bildet hier Tipping Points 2400. Die bei diesem System mit Exploit-Belastung gemessenen Übertragungszeiten lagen um den Faktor 2 über den Werten ohne Exploit-Belastung.

HTTP-Response-Time

Den HTTP-Response-Time-Test haben wir mit Avalanche/Reflector von Spirent und einem HP-Server DL380/2 mit dem Tool Tomahawk durchgeführt. Bei diesem Test wird der Einfluss von HTTP-Exploits auf die Übertragungleistung von regulärem HTTP-Verkehr gemessen. Als Messergebnis dient die HTTP-Response-Time des regulären HTTP-Verkehrs. Die HTTP-Response-Time wurde in keinem Fall signifikant durch die zusätzliche Belastung durch Exploits beeinflusst.

Exploit-Erkennung unter Netzlast

Den Test Exploit-Erkennung unter Netzlast haben wir mit Avalanche/Reflector von Spirent und einem HP-Server DL-380/2 mit dem Tool Tomahawk durchgeführt. Bei diesem Test wird der Einfluss der Netzlast auf die Erkennung von Exploits gemessen. Als Messergebnis dient die Exploit-Erkennungsrate. Und diese betrug in allen Fällen 100 Prozent.

Fazit

Die Kernfunktionalität eines IPS-Systems liegt im Erkennen und Blocken von Angriffen zu möglichst 100 Prozent. Zudem sollen die Systeme die geprüften Datenströme möglichst verzögerungsfrei und mit Leistungsgeschwindigkeit weiterleiten. Diese Aufgaben haben die Systeme von ISS, McAfee, Tipping Point und Top Layer in Anbetracht der Ergebnisse unseres vorhergehenden Firewall-Tests erstaunlich gut gemeistert. In diesem Feld deplaziert wirkt Sonicwalls Pro-5060, die einige Schwächen zeigte und wohl zum Testzeitpunkt noch kein ausgereiftes Produkt war. Nachtests sollten zeigen, ob der Hersteller inzwischen seine Hausaufgaben gemacht hat.

IT-Verantwortliche tun gut daran, bei der Auswahl eines IPS-Applliance genau zu prüfen, welche Funktionalität die in Frage kommenden Hersteller integriert haben. Nicht abgedeckte Risiken sollten sie durch weitere Sicherheitsmaßnahmen und -techniken versuchen auszuschließen. Denn auch ein Intrusion-Prevention-System kann nur ein Baustein im gesamten IT-Security-Konzept sein. Und wer wissen will, ob sein Netzwerk dann auch wirklich gegen alle denkbaren Risiken bestmöglich geschützt ist, der kommt um die Durchführung von Sicherheitstests nicht herum. Denn Vertrauen ist gut, aber Kontrolle ist besser.

Dipl.-Ing. Thomas Rottenau,
Prof. Dr. Bernhard G. Stütz,
dg@networkcomputing.de

Top Layer Networks
Attack Mitigator IPS5500

TESTVERFAHREN

HP Proliant DL 380

Als Lastgenerator/Analysator haben wir in unseren Real-World Labs den bekannten »Smartbits 6000C Traffic Generator/Analyser« von Spirent eingesetzt. Das in dieser Konfiguration gut 250 000 Euro teuere Gerät war mit der Software »Smartflow« ausgestattet und mit 24 Fast-Ethernet-Ports sowie vier Kupfer- und fünf Multimode-LWL-Gigabit-Ethernet-Ports bestückt. Alle Ports arbeiten im Full-Duplex-Modus und können somit gleichzeitig Last mit Wirespeed generieren und analysieren. Für die TCP-Messungen haben wir dann »Avalanche« und »Reflector« von Spirent verwendet. Bei allen Messungen handelt es sich um Zangenmessungen, bei denen entsprechende Datenströme generiert und analysiert werden.

Für die Überprüfung der Sicherheitsfunktionalität haben wir dann auf zwei HP-Server vom Typ »Proliant DL380/2« die entsprechenden Tools installiert und die verschiedenen Exploits über die IPS gesendet. Die HP-Server waren jeweils mit drei Gigabit-Ethernet-Adaptern bestückt. Zum Abspielen von aufgezeichnetem Netzverkehr haben wir Tomahawk v1.0 (http://tomahawk.sourceforge.net) eingesetzt. Als Exploits für verschiedene Betriebssysteme und Netzwerk-Dienste haben wir mit »Metasploit Framework 2.3« (www.metasploit.com) genutzt. Und für den Dateitransfer-Test haben wir auf Suse 9.2 mit Standard-HTTP-, FTP- und NFS-Servern und die entsprechenden Clients zurückgegriffen.

Um vergleichbare, gültige und aussagefähige Ergebnisse zu erzielen, haben wir vor den Tests die Einstellungen der Security-Appliances festgelegt und ein für alle Security-Tests verbindliches Standard-Rule-Set vorgegeben. Für die korrekte Konfiguration haben wir gemeinsam mit den Ingenieuren des jeweiligen Herstellers gesorgt, die ihr eigenes System im Test begleiten konnten.

Die einzelnen Netzsegmente haben wir über LAN-Switches vom Typ Extreme Networks Summit-1i und Summit-7i realisiert. Diese Systeme leisteten in den den einzelnen Tests vorhergehenden Kontrollmessungen volle Wirespeed und sind aus diesem Grund in Hinsicht auf das Datenrahmenverlustverhalten des Testaufbaus vollständig transparent. Mit Hilfe von drei Linux-Intel-PCs in den einzelnen Netzsegmenten haben wir die korrekte Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.