Marktübersicht: Freie und kommerzielle Analysewerkzeuge für Firewall-Logfiles

Waldarbeiter

Im Wald von zigtausend belanglosen Logfile-Einträgen die wertvollen Hölzer erkennen und einsammeln – das ist die schwere Pflicht des Firewall-Admin. Dazu braucht er passende Werkzeuge, die ihm einen Überblick geben und zudem die Details beschreiben. Dieser Artikel vergleicht zehn Tools. Kai-Oliver Detken, Andre Brandt

Firewalls kontrollieren und beschränken den Datenverkehr zwischen Netzen. Sie selbst sind aber auch zu überwachen – neben der korrekten Konfiguration ist das die wichtigste Aufgabe des Firewall-Administrators. Er untersucht dazu die Logdaten, schlimmstenfalls mit »less«. Die Logs sammeln wichtige Informationen, etwa Absender, Empfänger, Typ sowie diverse Statusinformationen zu auffälligen Datenpaketen. Leider unterscheiden sich Art und Aufbau dieser Informationen je nach Firewall und keine erzeugt übersichtliche Logs.

Ordnung und Übersicht in dieses Chaos bringen Analysewerkzeuge. Die besseren unter ihnen verstehen verschiedene Formate und lesen mehrere Quellen: Während einfache Firewalls nur einen Systemdienst zum Protokollieren nutzen, schreiben andere die Daten in eine externe Datenbank oder verwenden spezielle Logsysteme.

Bereits die schiere Menge an Informationen stellt Menschen vor Probleme, wenn sie gezielt Hinweise in den Datenbeständen suchen oder ausfiltern wollen. Im produktiven Einsatz landet pro Tag oft eine fünf- oder sechsstellige Anzahl an Meldungen im Log. Spätestens wenn der Wert die Millionengrenze überschreitet, geht ohne datenbankgestütztes Logging nichts mehr. Oft sind Angriffe oder Konfigurationsfehler erst erkennbar, wenn man viele Datensätze kombiniert auswertet – auch hier hilft eine Datenbank.

Große Auswahl

Die folgende Marktübersicht untersucht und vergleicht Applikationen, die sich zur Analyse von Firewall-Logs eignen. Sie berücksichtigt proprietäre kommerzielle Systeme ebenso wie Open-Source-Werkzeuge. Tabelle 1 fasst die Ergebnisse zusammen und sorgt für Überblick.

Das für diesen Artikel verwendete Testszenario in Abbildung 1 ist einem über die Zeit gewachsenen Firmennetz nachempfunden. Von außen erreichbare Server stehen in einer DMZ. Das interne LAN gliedert sich in zwei Bereiche: Während LAN 1 das interne Firmennetz darstellt, steht LAN 2 für eine besonders zu sichernde Umgebung innerhalb der Firma oder für eine VPN-Verbindung zu einem Geschäftspartner oder Kunden. Die Datensammlung geschieht in der Regel über einen Syslog-Daemon, der auf dem Logserver läuft.

Gut aufgestellt

Wo ein Logserver sinnvollerweise steht, hängt von den beteiligten Firewalls, der Logtechnik und den verwendeten Analyseprogrammen ab. Der Protokollsammler soll seine Arbeit optimal erfüllen, ohne neue Sicherheitslöcher ins Netz zu reißen. Idealerweise befindet er sich in einem geschützten Netz: Ein Angriff auf den Server könnte wichtige Logfiles vernichten oder interne Informationen verraten, daher ist er ein beliebtes Ziel für Sabotagen. Die DMZ eignet sich nicht als Aufstellungsort.

Ein zentraler Server im LAN könnte die Logfiles sämtlicher Firewalls einsammeln und verwerten. Bei Syslog-basierten Protokollen muss der Admin dafür allerdings einen UDP-Port von der DMZ ins interne LAN öffnen, um auch die Protokolle der externen Firewall einzusammeln. Der offene Port schwächt aber den Schutz des internen Netzes. Hier kann es sinnvoller sein, den Logserver gut abgesichert in der DMZ zu platzieren. Dann braucht nur die Analysesoftware Zugriff auf den Server in der DMZ.

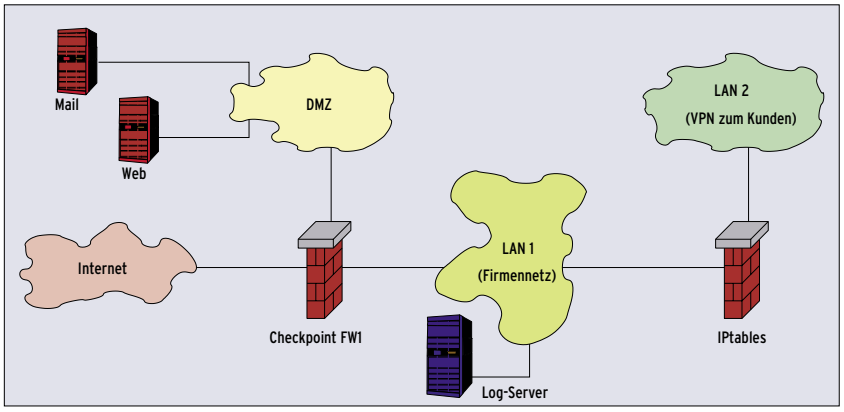
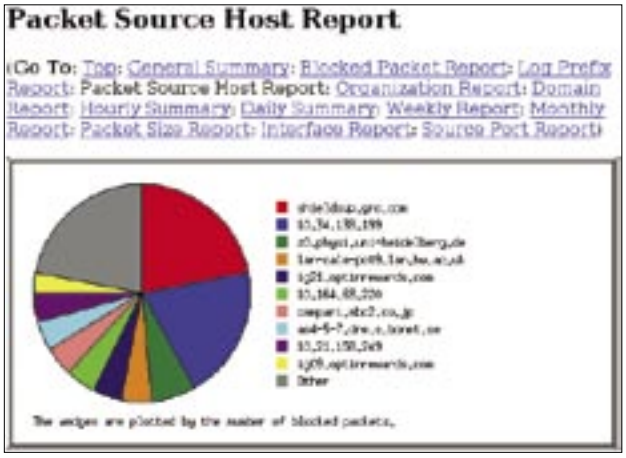


Abbildung 1: In dieser Testumgebung mussten sich die Log-Applikationen einem Praxistest unterziehen. So oder so ähnlich sind die Firewall-Infrastrukturen vieler kleinerer und mittlerer Firmen aufgebaut.

Analyse-Applikationen müssen dem Benutzer das Verständnis der Informationen erleichtern und ihn dabei unterstützen, die Informationen auszuwerten. Folgende Merkmale dienen als Maßstab:

- Quelle der Logdaten: Beispielsweise Logdateien des Unix-Syslog oder eine Datenbank.
- Format der Logdaten: Es gibt leider keinen einheitlichen Standard, jeder Hersteller verwendet eine eigene Formatierung. Eine Applikation sollte möglichst viele Formate kennen.
- Echtzeitmonitoring: Logdaten fortlaufend im Betrieb analysieren.
- Ansicht der Logdaten: Schon die unverarbeiteten Daten liefern wertvolle Informationen. Der Analysator sollte dem Admin auf Wunsch auch diese Rohdaten zeigen.
- Filter: Sie dienen dazu, aus den Rohdaten relevante Informationen zu gewinnen, also nach bestimmten Merkmalen zu filtern.
- Statistiken: Zur Analyse von Trends sind Statistiken unerlässlich. Entscheidend ist, wie aussagekräftig diese Informationen sind.
- Benutzerverwaltung: Nur vorher bestimmtes Personal darf Zugriff auf die Logdaten erhalten. Eine integrierte Benutzerverwaltung sollte unterschiedliche Sichtweisen auf die Daten ermöglichen.
- Benutzungseinschränkungen: Kommerzielle Lizenzen begrenzen manchmal die Benutzeranzahl oder die der zu überwachenden Geräte.
- Mehrsprachigkeit: Bestimmt, ob die Oberfläche für den internationalen Einsatz taugt.

Zwar gibt es keinen einheitlichen Standard für Logformate, viele Firewalls und Analysewerkzeuge verstehen sich aber per WELF. Das Webtrends Enhanced Log Format war ursprünglich für den Einsatz



▲ **Abbildung 2: FW-Analog benutzt den Web-Klassiker Analog, um Firewallprotokolle statistisch auszuwerten. Hier ermittelt das Tool, aus welchen Quellen die meisten geblockten Pakete stammen.**

▶ **Abbildung 3: Die Einstiegsseite des PHP-basierten Webfwlog listet die bereits definierten Filter, die je einen Report erzeugen. Der Edit-Link verzweigt zum mächtigen Filter-Editor.**

in Proxy-Servern und Intrusion-Detection-Systemen (IDS) gedacht, eignet sich aber auch für Firewalls.

WELF

Der Aufbau eines WELF-Eintrags ähnelt in einigen Punkten dem Logformat von IPtables, erreicht jedoch bei weitem nicht denselben Informationsgrad. Während IPtables sogar einzelne Header-Flags der Pakete enthält, stellt WELF nur Adressen und Protokolle zur Verfügung. Im Gegenzug führen die WELF-Einträge eine Priorität, die angibt, wie kritisch das Ereignis ist, das die Meldung ausgelöst hat. Beispiel eines WELF-Logeintrags:

```
WTsyslog[2005-05-01 15:05:46 ip=10.0.0.1 ➥
pri=6] id=firewall time="2005-05-01 14:10➥
:23" fw=firewall pri=5 msg="ICMP packet d➥
ropped" src=10.0.0.2 dst=10.0.0.3 rule=3
```

Die Meldung besteht aus mehreren Einträgen der Form *Name = Wert*. Enthält der Wert Leerstellen, steht er in Anführungszeichen. Manche Firewalls verteilen WELF-Protokolle per Syslog-Dienst, andere wiederum schreiben sie direkt in Textdateien.

Acht Open-Source-Tools sowie zwei aus dem kommerziellen Softwarebereich mussten nach den oben aufgestellten Kriterien zeigen, was sie aus den protokollierten Log-Informationen herausfiltern und wie gut sie den Administrator bei seiner Suche nach verdächtigen Spuren unterstützen.

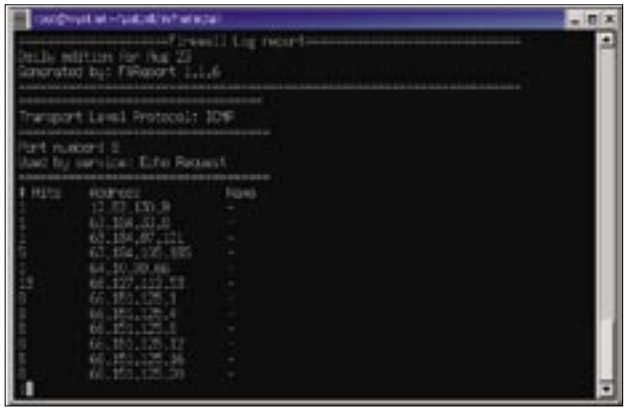


Abbildung 4: FW-Report arbeitet auf der Kommandozeile und erzeugt sehr einfache, aber übersichtliche Berichte. Bei ICMP zeigt das Tool nur die Quell-IP-Adresse, bei TCP und UDP zudem die Ziel-Portnummer an.

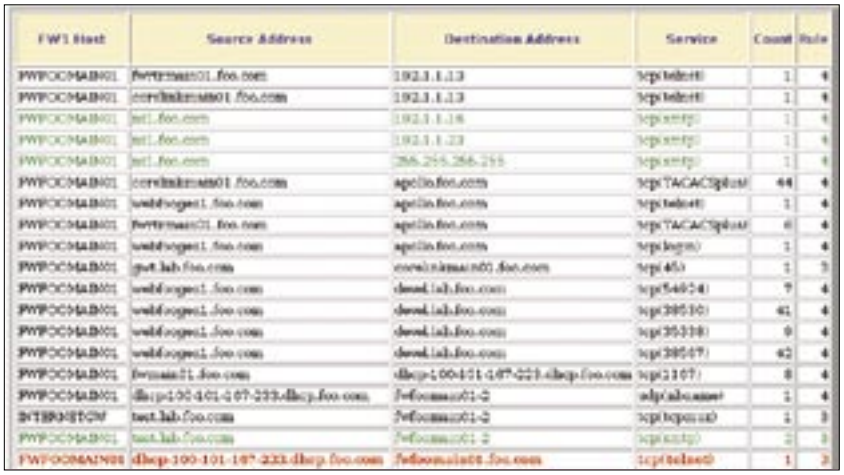
Den Reigen der Testkandidaten aus dem Open-Source-Lager eröffnet FW-Analog [1]. Dieses Shellskript des Ungarn Balázs Bárány übersetzt Firewallprotokolle in Webserver-Logfiles, die es anschließend an Analog [2] übergibt, das daraus Statistiken generiert. Die resultierenden HTML-Seiten zeigen Log-Infos in 13 Kategorien, unter anderem die Belegung der häufigsten Quell- und Zielports als Tortendiagramm (Abbildung 2). Zwar kennt das Programm viele Logformate, doch eignen sich die gewonnen Informationen nur dazu, Trends aufzuzeigen oder einen Überblick zu erhalten. Zu einzelnen Datenpaketen ist ein Zugriff auf exakte Log-Informationen nicht möglich.

Einfache Textausgabe

Das Perl-Skript Adcfw-log [3] hat Alessandro Dotti Contra für Linux-Plattformen entwickelt. Es liegt zurzeit in Version 0.9.1 vor, Alessandro treibt die

Tabelle 1: Analyse-Tools für Firewallsysteme

Applikation	Version	Logquellen	Logformate	Echtzeit-Monitoring
Adcfw-log [3]	0.9.1	Syslog-Dateien	IPtables (Kernel 2.4)	Nein
Firewall Analyzer [14]	3.3	Integrierter Syslog-Server, Checkpoint LEA Server, exportierte Logdateien der Firewalls	Checkpoint Firewall-1 (4.x, NG), Cisco PIX, Clavister Firewall, Symantec Enterprise Firewall, Raptor, Borderware Firewall Server, Watchguard, Stonegate, Nokia Firewall-1 (über Export), über WELF: Sonicwall, Netscreen, 3Com etc.	Nein
FW-Analog [1]	0.6.4	Syslog-Dateien	IPchains, IPtables, IPfilter, Cisco PIX, IPfw, Zyxel Router, Netgear Router, Watchguard Firebox, Checkpoint Firewall-1, Sonicwall	Nein
FW-Logsum [6]	5.0.2	Firewall-1-Logdateien	Checkpoint Firewall-1 (3.x, 4.x, NG), Konverter für Cisco PIX, Netscreen, IPtables/Netfilter, Windows-Firewall, Stonegate, WELF-Logfiles	Nein
FW-Logwatch [9]	1.0	Syslog-Dateien, Gzip	IPchains, IPtables, IPfilter, IPfw, Cisco IOS, PIX, Netscreen, Windows-FW, Elsa Lancom, Snort IDS	Nein
FW-Report [5]	1.1.8	Syslog-Dateien	IPtables (Kernel 2.4 und 2.6)	Nein
IPtables Log Analyzer [11]	CVS	Syslog-Dateien	IPtables (Kernel 2.4 und 2.6)	Ja
Sawmill Enterprise Edition [15]	7.1.7	Logdateien, die lokal oder auf Web-/FTP-Servern vorliegen	Checkpoint Firewall-1, Cisco PIX, Symantec Enterprise Firewall, Raptor, Borderware, Watchguard, Sonicwall, IPtables, IPchains, IPfw, WELF (mehr als 80 Firewall-Formate)	Nein
Webfwlog [4]	0.91	Ulogd, Syslog-Dateien, MySQL/ PostgreSQL	Netfilter, IPtables, IPfw, IPchains, Windows XP	Nein
WF-Logs [10]	0.9.8	Syslog-Dateien	IPchains, IPtables, IPfilter, Cisco IOS, PIX, Snort IDS, Logkonvertierung für IPchains, IPtables und IPfilter	Nein



FW1 Host	Source Address	Destination Address	Service	Count	Rule
FWFOOMAIN01	fwtermas01.foo.com	192.1.1.13	tcp/telnet	1	4
FWFOOMAIN01	corelinkmas01.foo.com	192.1.1.13	tcp/telnet	1	4
FWFOOMAIN01	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
FWFOOMAIN01	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
FWFOOMAIN01	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
FWFOOMAIN01	corelinkmas01.foo.com	apollo.foo.com	tcp/TACACS[illegible]	44	4
FWFOOMAIN01	webfwgw1.foo.com	apollo.foo.com	tcp/telnet	1	4
FWFOOMAIN01	fwtermas01.foo.com	apollo.foo.com	tcp/TACACS[illegible]	6	4
FWFOOMAIN01	webfwgw1.foo.com	apollo.foo.com	tcp/login	1	4
FWFOOMAIN01	gw.lab.foo.com	corelinkmas01.foo.com	tcp/49	1	3
FWFOOMAIN01	webfwgw1.foo.com	dmzd.lab.foo.com	tcp/54924	7	4
FWFOOMAIN01	webfwgw1.foo.com	dmzd.lab.foo.com	tcp/38510	41	4
FWFOOMAIN01	webfwgw1.foo.com	dmzd.lab.foo.com	tcp/35338	9	4
FWFOOMAIN01	webfwgw1.foo.com	dmzd.lab.foo.com	tcp/38567	42	4
FWFOOMAIN01	[illegible]	dhcp-100-101-107-223.dhcp.foo.com	tcp/2107	8	4
FWFOOMAIN01	dhcp-100-101-107-223.dhcp.foo.com	[illegible]	udp/domain	1	4
INTERNETCM	test.lab.foo.com	[illegible]	tcp/[illegible]	1	3
FWFOOMAIN01	test.lab.foo.com	[illegible]	tcp/ssh	2	3
FWFOOMAIN01	dhcp-100-101-107-223.dhcp.foo.com	[illegible]	tcp/telnet	1	2

Abbildung 5: Die HTML-Reports von FW-Logsum enthalten recht wenig Information. Das Tool liest Firewall-1-Logfiles und verweist immerhin in der letzten Spalte auf die Nummer der betreffenden Regel.

Entwicklung aber seit Mitte 2004 nicht weiter voran. Das Kommandozeilenwerkzeug verarbeitet ausschließlich IP-tables-Logs und bietet eingeschränkte Funktionen zum Filtern der Logdaten. Der Admin kann beispielsweise Interfaces, Ports und Protokolle benennen, nach denen das Programm die Daten filtern soll. Adcfw-log schreibt die Resultate als Text auf die Konsole, wer will, leitet sie per E-Mail weiter und setzt einen Cronjob auf, der für regelmäßig wiederkehrende Reports sorgt.

In PHP geschrieben ist das sehr umfangreiche Webfwlog [4]. Die Web-basierte Software läuft auf Unix-Plattformen sowie – mit Hilfe von Cygwin – unter Windows. Die vielfältigen Analysemöglichkeiten bestehen vor allem aus leistungsfähigen Filtern, die auf der Hauptseite der Anwendung als Einstiegspunkt zur weiteren Analyse bereitstehen (Report genannt, Abbildung 3). Webfwlog enthält dafür einen eigenen Editor bereit, der auch das Ex- und Importieren von Filtern erlaubt.

Wichtige Aufgabe: Informationen filtern

Bei den Webfwlog-Filtern kann der Admin jede im Logfile gespeicherte Information in die Analyse einbeziehen: Sowohl die üblichen Daten wie Quell- und Ziel-Adressen oder -Ports als auch Protokolle, Interfaces, Loghosts bis hin zu Datumsangaben, TCP-Optionen und ICMP-Types oder Codes. Jeder Filter kann zudem eine eigene Quelle erhalten, aus der er seine Daten bezieht. Die Hauptaufgabe der Filter ist, die Daten einer Quelle in kleinere, überschaubarere Untermengen aufzuteilen. So lassen sich im Gegensatz zu FW-Logwatch gezielt Logfiles nach Paketen eines bestimmten Protokolls durchsuchen, die von einem speziellen Rechner kommen.

Die gefilterten Daten stellt Webfwlog tabellarisch dar (Abbildung 3). Dabei fasst es gleiche Einträge zusammen und gibt ihre Anzahl an. Zwar kann der Admin

	Rohdaten-Anzeige	Filtern der Daten	Statistiken	User-Verwaltung	Benutzungseinschränkungen	Sprachen	Lizenz
	Teilweise (nicht alle Daten sind sichtbar)	Teilweise (nicht alle Daten können gefiltert werden)	Nein	Nein	Nein	Englisch	GNU GPL
	Nein	Nein	Ja	Ja	Ja, in Abhängigkeit von der Lizenz	Programm in Englisch; Berichte in Deutsch, Französisch, Spanisch	Firmeneigene, SOHO ab 500, sonst ab 900 US-Dollar
	Nein	Nein	Ja	Nein	Nein	Englisch	GNU GPL
	Ja (nur IP-Adresse, Ports und Protokolle)	Nein	Ja	Nein	Nein	Englisch	GNU GPL
	Teilweise (nicht alle Daten sind sichtbar)	Nein	Nein	Nein	Nein	Englisch, Deutsch, Portugiesisch, Schwedisch, Japanisch, Chinesisch	GNU GPL
	Nein	Nein	Ja	Nein	Nein	Englisch	GNU GPL
	Teilweise (nicht alle Daten sind sichtbar)	Nein	Nein	Nein	Nein	Englisch	GNU GPL
	Ja (teilweise, je nach Firewall)	Nein	Ja	Ja	Ja, in Abhängigkeit von der Lizenz	Englisch	Firmeneigene, ab 880 Euro
	Ja (komplette Rohdaten über Detailansicht)	Nein (Filtern durch Profil möglich)	Nein	Nein	Nein	Englisch	GNU GPL
	Ja	Einmalig beim Erstellen des Reports	Nein	Nein	Nein	Englisch	GNU GPL

die Tabellenansicht nach den einzelnen Kategorien sortieren, auf Basis eines dieser Reports weiter zu filtern ist aber nicht mehr möglich.

Chris Travers entwickelt sein Perl-Programm FW-Report [5] als Reportgenerator, der Tages- und Monatsberichte erstellt. Das Programm ist für Linux-Umgebungen gedacht und wertet nur Netfilter-Logdaten aus. Bedient wird die Applikation über die Kommandozeile (Abbildung 4) oder per Cronjob. Ihr Funktionsumfang ist eingeschränkt, die Reports enthalten lediglich die Quell-IP-Adresse und die Ziel-Portnummer. Dennoch kann ein Programm dieser Klasse Fehler in der Konfiguration aufdecken und Portscans anzeigen.

Ebenfalls zu den Reportgeneratoren gehört FW-Logsum [6], ein seit 1996 entwickeltes Perl-Programm zur Analyse von Firewall-1-Logfiles des Herstellers Checkpoint. Das Kommandozeilenprogramm erzeugt Reports im Text- und HTML-Format und läuft auf Linux/Unix- und auf Windows-Systemen. Um die Bedienung zu vereinfachen, stellt der Autor des Programms ein Webformular bereit [7], über das sich die Optionen bequem zusammenstellen lassen.

Schwachpunkt: Gezielte Spurensuche

Wie viele Reportgeneratoren ist auch FW-Logsum eher dazu gedacht, tägliche Übersichten zu generieren, als aktiv die Fehlersuche zu unterstützen. Um Fehler oder Angriffe deutlicher sichtbar zu machen, hebt es auf Wunsch immerhin bestimmte Dienste hervor. Daneben ist es möglich, Einträge auszufiltern, IP-Adressen aufzulösen und den Ports passende Servicenamen zuzuordnen.

Ein Schwachpunkt des Tools ist die geringe Menge der dargestellten Informationen (Abbildung 5): Es zeigt nur Protokolle, Quell- und Ziel-IP-Adressen sowie Ports, die Nummer der Firewallregel und die Anzahl der insgesamt zutreffenden Pakete. Besonders interessant ist allerdings die Fähigkeit, Logfiles fremder Hersteller über einen Konverter in Firewall-1-Logfiles zu übersetzen. Damit gelingt es pfiffigen Admins, jedes Programm, das Firewall-1-Logfiles versteht, auf fremde Formate anzusetzen (siehe Kasten „Formatwandler“).

Alte Bekannte

Drei weitere Open-Source-Tools hat das Linux-Magazin bereits in einer früheren Ausgabe [17] vorgestellt: FW-Logwatch [9], WF-Logs (Wallfire, [10]) und IPtables Log Analyzer [11]. FW-Logwatch wurde ursprünglich von Boris Wesslowski für das RUS-CERT (Computer Emergency Response Team der Ruhr-Universität Stuttgart) entwickelt. Das Programm ist für Linux, Solaris und BSD-Unix verfügbar. Mit Cygwin-Hilfe läuft es sogar unter Windows. Es liest Klartext- oder Gzip-komprimierte Logdateien sowie Files mit kombinierten Einträgen mehrerer Systeme. FW-Logwatch erstellt Reports als Text oder HTML und verteilt sie auf Wunsch per E-Mail.

Das von Hervé Eychenne entwickelte WF-Logs [10] analysiert Firewall-Logs statisch, es fehlt eine Funktionen, um aktiv in den Reports nach bestimmten Vorkommnissen zu suchen. Der Benutzer stößt die Analyse von Hand an oder setzt einen Cronjob auf. WF-Logs erzeugt HTML-Seiten, Textdateien oder XML-Dokumente. Das Programm versteht mehrere Logformate und – ähnlich wie das oben beschriebene FW-Logsum – konvertiert WF-Logs einiger Formate (siehe Kasten „Formatwandler“).

Ausschließlich auf die Verarbeitung von IPtables-Protokollen spezialisiert ist der IPtables Log Analyzer [11] von Gérald

Abbildung 6: Das Security Reporting Center wertet nicht nur Security-Vorfälle aus, es erzeugt auch Statistiken über die genutzte Bandbreite (im Bild ist ein Proxy zu sehen) oder Daten zu den angeschlossenen VPNs.

Security Reporting Center

Ende Juni 2005 hat die Firma Net IQ einen Teil ihrer Produkte an die Investitionsgesellschaft Francisco Partners verkauft und das neue Unternehmen Webtrends gegründet. Vor diesem Deal hatte Net IQ zwei Log-Analysetools im Angebot, die zwar seit dem 30. Mai nicht mehr verfügbar, aber mancherorts noch im Einsatz sind: das Security Reporting Center (SRC, [12]) und die kleinere Webtrends Firewall Suite (WFS, [13]). Das Web-basierte SRC läuft auf Windows- und Solaris-Plattformen. Standardmäßig unterstützt es Checkpoint, Symantec Enterprise, Borderware, Lucent und Cisco PIX sowie viele Firewalls, die ihre Protokolle im Webtrends-Enhanced-Logformat ausgeben. Die Logdaten sammelt das SRC wahlweise mit Syslog, Datei-Import oder speziellen Verfahren für Checkpoint- und Cisco-PIX-Firewalls.

Die integrierte Benutzerverwaltung unterscheidet normale User, Administratoren und Gruppen. Die Auswertung gliedert sich in 14 Kategorien und in mehrere zeitliche Abschnitte, sie umfasst neben internen und externen Adressen auch VPN-Verbindungen und Bandbreitennutzung (Abbildung 6). Ein Zugriff auf die Rohdaten ist aber nicht möglich. Der Funktionsumfang ist am ehesten mit dem ebenfalls getesteten Firewall Analyzer [14] zu vergleichen.

Die kleinere WFS läuft nur als Stand-alone-Programm auf Windows NT/2000/XP und verzichtete auf Auswertungsfunktionen für die Logs von Clavister und Netscreen und bereitet die Daten auch in weniger Kategorien auf.

Garcia. Das in PHP geschriebene, Web-basierte Programm ist in der Lage, die wichtigsten Informationen aus einem IPtables-Logfile tabellarisch darzustellen und lässt den Anwender einfache Filter setzen. Allerdings ist das Tool noch in einem recht frühen Entwicklungsstadium.

Firewall Analyzer

Neben den freien Open-Source-Programmen umfasst diese Übersicht auch einige kommerzielle proprietäre Tools. EIQ-Networks schickt den Firewall Analyzer [14] ins Rennen. Das nur für Windows verfügbare Analyseprogramm arbeitet Web-basiert. Die Oberfläche spricht nur Englisch, erzeugt aber Reports in Deutsch, Französisch, Spanisch und weiteren Sprachen. Die Übersetzungen scheinen allerdings teilweise automatisch generiert zu sein, sie fallen mitunter missverständlich aus.

Als Datenquellen kann der integrierte Syslog-Server dienen, ein lokales oder

Formatwandler

Als Teil ihres Programms FW-Logsum [6] stellt Ginini Technologies auf ihrer Webseite ein sehr interessantes Perl-Programm namens FW1 Log Converters zur Verfügung [8]. Mit Hilfe einiger Plugins wandelt es fremde Logformate in das Firewall-1-Format des Marktführers Checkpoint um.

Logs mit Hilfe eines Konverters auswerten

Da viele Programme Checkpoint-Logfiles verarbeiten, besteht so die Chance, sein eigenes System mit in die Auswertung einzubeziehen. Folgende Formate lassen sich umwandeln:

- Microsoft ICF (Internet Connection Firewall)
- Netfilter/IPtables
- Netscreen
- Cisco PIX
- Stonegate CSV Log
- WELF (Webtrends Extended Log Format)

Die Installation des Programms gestaltet sich einfach. Es setzt lediglich ein installiertes Perl voraus, der Anwender muss zudem den Pfad zum Verzeichnis mit den Plugins (Modulen) im Skript anpassen. Anschließend wandelt beispielsweise folgender Aufruf IPtables-Logfiles in das Checkpoint-Format:

```
./c2fw1.pl -i iptables.log.12 ➥
  -o checkpoint.log -c netfilter
```

Für Netfilter-Logs nachteilig ist der Aufwand: Wer im FW1-Logfile sinnvolle Nummern haben will, um die Meldungen ihren auslösenden Regeln zuzuordnen, muss das Konvertermodul von Hand darauf vorbereiten. In der Datei »netfilter.pm« ordnet die Hashtabelle »@action« jedem Logpräfix die passende Aktion und Regel aus dem Checkpoint-Sprachgebrauch zu.

Zweiter Wandler

Auch WF-Logs [9] beherrscht das Umwandeln von Logging-Formaten (WF steht für den Projektnamen Wallfire). Hier ist kein zusätzliches Tool nötig, es genügen passend gesetzte Kommandozeilen-Argumente. Als Eingaben versteht WF-Logs die Formate von Netfilter, IPchains, IPfilter, Cisco PIX, Cisco IOS und Snort. Als Ausgabeformate nennt die Manpage neben den Reports auch Netfilter, IPchains und IPfilter. Folgender Aufruf wandelt IPchains-Logfiles in das Netfilter-Format:

```
wflogs -i ipchains -o netfilter ➥
  ipchains.log > netfilter.log
```

per FTP abzuholendes File oder im Falle von Checkpoint ein externer LEA-Server (Logging and Event API), von dem der Firewall Analyzer die Logdaten abholt. Auch die Syslog-Server sind nicht an den Rechner gebunden, auf dem die Auswertung läuft. Per Default landen die gesammelten Daten in einer eigenen MySQL-Datenbank, auf Wunsch benutzt das Programm auch einen MS-SQL-Server oder eine Oracle-Datenbank.

Wer den Firewall Analyzer nur für kleine Firewalls der SOHO-Kategorie (Small Office, Home Office) verwendet, bezahlt für eine Lizenz 500 US-Dollar. Die gilt dann aber auch nur für ein einzelnes Gerät; handelt es sich um eine größere Firewall, dann schlägt die Einzellizenz bereits mit 900 Dollar zu Buche, ebenfalls für nur ein überwachtes Gerät. Support und Updates kosten dazu jährlich weitere 180 Dollar.

Und täglich grüßt der Firewall-Report

Seine Reports erzeugt das Programm auf manuellen Befehl oder zeitgesteuert über einen eigenen Scheduler, der stündlich, täglich, wöchentlich oder monatlich Berichte generiert. Die Reports liegen dann als HTML (Abbildung 7), PDF, MS Word, MS Excel oder Textdokument vor. Wahlweise verschickt das Tool die Berichte per E-Mail oder lädt sie auf einen FTP-Server. Die Reports sind ausführlich und in Kategorien unterteilt, die sich weiter in Unterkategorien gliedern und einzelne Ergebnisse als Tabelle und zusätzlich als Diagramm darstellen. Wie umfangreich die Berichte ausfallen, ist im Profil einstellbar.

Das Programm ist in der Lage, bekannte Angriffe wie beispielsweise Land oder Teardrop sowie gefälschte und ungültige IP-Adressen zu erkennen und hervorzuheben. Neben den üblichen Daten wie IP-Adressen und Ports enthalten die Berichte auf Wunsch auch Daten über ACLs, Content-Filter, Bandbreiten-, Web- und E-Mail-Nutzung sowie gefundene und gefilterte Viren. Ein direkter Zugriff auf die Logdaten oder das nachträgliche Ausblenden von Teilen der Ergebnisse ist allerdings nicht möglich.

Sawmill

Aus dem Hause Flowerfire kommt Sawmill [15]. Das Programm ist eigentlich für Webserver-Logfiles ausgelegt, es analysiert aber auch andere Logformate (bis zu 600 verschiedene). Recht ungewöhnlich für ein kommerzielles Programm ist, dass Sawmill viele Formate aus dem Open-Source-Lager unterstützt. Sawmill ist für alle wichtigen Plattformen verfügbar, von diversen Linux/Unix-Varianten über Solaris und Mac OS X bis hin zu Windows. Wer seine eigene Plattform vermisst, der kann den C++-Quellcode anfordern und Sawmill selbst portieren.

Für die Bedienung ist ausschließlich ein englischsprachiges Webinterface verfügbar. Sawmill bezieht seine Daten aus vier verschiedenen Quellen: lokale Protokolldateien, Files auf HTTP- und FTP-Servern oder die Ausgabe eines Kommandos. Ist die Quelle gewählt, versucht das Programm das Format des Logfile selbst zu ermitteln, was im Test erstaunlich gut funktionierte. Im Zweifelsfall wählt der Admin das Format aus einer umfangreichen Liste.

Eine einfache Lizenz für eine Installation und ein Logfile-Profil (also einen Protokolltyp) kostet 880 Euro, bei fünf Profilen verlangt der Distributor 1500 Euro [16]. Für Support sind jährlich zusätzlich 480 Euro fällig.

Mit eigener Datenbank

Die Daten speichert Sawmill entweder in einer eigenen Datenbank oder in einem externen MySQL-Server. Der Umfang der Auswertung hängt von der Firewall ab. Während Checkpoint nur wenige Daten liefert, fällt die IPtables-Analyse deutlich detaillierter aus. Für alle im Logfile enthaltenen Parameter gibt es Übersichten über die Häufigkeit des Auftretens (Abbildung 8) sowie eine Detailansicht, die alle mitgeloggten Einträge darstellt. Leider fehlen in der Detailansicht Filtermöglichkeiten. Die erstellten Berichte lassen sich als CSV-Datei exportieren, andere Formate wie PDF- oder Word-Dateien sind nicht vorgesehen.

Abbildung 7: Die Reports-Übersicht des Firewall Analyzer von EIQ-Networks fasst alle Ergebnisse zusammen. Das Tool erzeugt detailreiche Auswertungen, lässt aber nachträgliches Filtern oder den Zugriff auf einzelne Logeinträge vermissen.

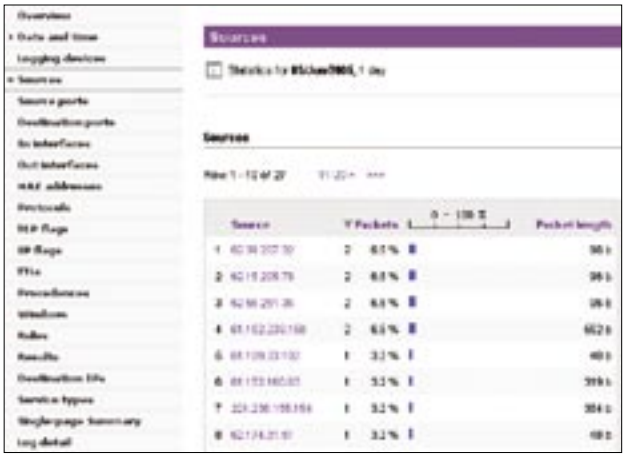


Abbildung 8: Der Reportgenerator Sawmill erzeugt recht umfangreiche Statistiken, zu sehen sind die Häufigkeit von IP-Quelladressen und die durchschnittliche Länge der Pakete aus dieser Quelle.

Das Programm verfügt über einen eigenen Scheduler. Er kümmert sich um wiederkehrende Aufgaben, beispielsweise automatisch Berichte generieren und sie per E-Mail versenden. Die eingebaute User-Verwaltung unterscheidet zwischen Admins und Benutzern. Während die Administratoren Zugriff auf alle Funktionen haben, sind die Benutzerrechte auf die Ansicht einzelner Reports beschränkt.

Übergewicht der Reportgeneratoren

Auffallend viele Firewall-Analyseprogramme sind dem Typ der Reportgeneratoren zuzurechnen. Besonders unter den kommerziellen Systemen gewährt keines der vorgestellten Programme tieferen Einblick in das Verhalten der Firewall. Zwar bringen alle Programme gute Voraussetzungen bezüglich Anzahl der möglichen Log-Formate und -Quellen mit, doch erzeugen sie aus den gewonnenen Daten nur Reports, die Trends aufzeigen und Zusammenfassungen liefern. Selbst wenn ein Tool Angriffe oder Fehlkonfigurationen erkennt, liefert es dem Admin keine wirklich detaillierten und aussagekräftigen Daten.

Ein weiterer Schwachpunkt ist die Lokalisierung. Zwar sind die Berichte meist in mehreren Sprachen verfügbar, nicht jedoch die Programme selbst. Außerdem sind die Übersetzungen teilweise missverständlich.

Unter den kommerziellen Produkten fällt Sawmill positiv auf. Als einziges analysiert es auch Open-Source-Firewalls. Da IPtables umfangreiche Daten ins Log schreibt, ist Sawmill zumindest dort in der Lage, umfangreichere Auswertungen zu betreiben. Dennoch fehlen selbst hier wichtige Funktionen, um die geloggten Daten umfassend zu untersuchen. Zu wünschen wäre es, einzelne Daten innerhalb der geloggten Informationen ausblenden zu können oder gezielt bestimmte Daten zu sichten, die etwa ein Flag im IP-Header gesetzt haben.

Die bei der kommerziellen Konkurrenz vermissten Funktionen sind bei einigen Open-Source-Programmen sehr wohl anzutreffen, etwa um Pakete auf bestimmte Daten zu untersuchen. Das große Manko in diesem Lager ist die Anzahl unterstützter Formate. Die meisten untersuchten Programme lesen zwar die Protokolle der wichtigsten Hersteller wie Cisco oder Checkpoint, aber bei weniger verbreiteten Firewalls scheitern sie.

In beiden Produktgruppen fällt auf, dass sich alle Programme nur eingeschränkt zur Echtzeitüberwachung eignen. Die Reportgeneratoren erzeugen ihre Berichte auf Wunsch zwar in festgelegten Intervallen und stellen sie per E-Mail zu, es bleibt aber ein Zeitfenster zwischen Angriff und Report. Echtzeitüberwachung reagiert dagegen sofort – und nur wenn sie wirklich einen Angriff feststellt.

Guter Mix

Wer sowohl umfassende Statistiken als auch einen tieferen Einblick in das Verhalten der Firewall benötigt, ist mit einem Mix von kommerziellen und Open-Source-Programmen am besten beraten. Besonders Webfwlog [4] und Sawmill [15] ergänzen sich hervorragend. Ein sinnvolles Szenario wäre es, mit Sawmill die Firewalls zu überwachen (durch Beobachten der Statistiken) und mit dem Tool auch erste Nachforschungen bei Unregelmäßigkeiten anzustellen.

Zur detaillierten Analyse schwenkt der Administrator dann um auf Webfwlog und grenzt damit die Probleme genauer ein. Dazu definiert er Filter, die gezielt uninteressante Pakete ausblenden, und konzentriert sich auf die relevanten Informationen. Erst das Gespann aus beiden Tools gibt dem Firewall-Admin die gewünschte Hilfe bei seiner anspruchsvollen Arbeit. *(fjl)*

Infos

[1] FW-Analog: [http://tud.at/programm/fwanalog/]
[2] Analog: [http://www.analog.cx]
[3] Adcfw-log: [http://adcfw-log.sf.net]
[4] Webfwlog: [http://www.webfwlog.net]
[5] FW-Report: [http://www.sf.net/projects/fwreport/]
[6] FW-Logsum: [http://www.ginini.com/software/fwlogsum/]
[7] FW-Logsum-Generator: [http://www.ginini.com/cgi-bin/fwlogsum.cgi]
[8] FW1 Log Converters: [http://www.ginini.com/software/fwlogsum/converters/]
[9] FW-Logwatch: [http://fwlogwatch.inside-security.de]
[10] WF-Logs: [http://www.wallfire.org/wflogs/]
[11] IPtables Log Analyzer: [http://iptablelog.sourceforge.net]
[12] Security Reporting Center: [http://www.netiq.com/support/src/]
[13] Webtrends Firewall Suite: [http://www.netiq.com/products/fwr/]
[14] Firewall Analyzer: [http://eiqnetworks.com/products/firewallanalyzer.shtml]
[15] Sawmill Enterprise Edition: [http://www.sawmill.net]
[16] Sawmill-Preisliste: [http://www.haage-partner.de/sawmill/order.html]
[17] Ralf Spenneberg, „Nur fürs Protokoll – Analysetools für Firewall-Logfiles“: Linux-Magazin 12/04, S. 44

Die Autoren

Dr. Kai-Oliver Detken ist Senior IT Consultant und Geschäftsführer der Decoit GmbH in Bremen. Er veröffentlicht zusätzlich regelmäßig Fachpublikationen bei verschiedenen Verlagen und ist Dozent an der Hochschule Bremen.

Andre Brandt arbeitet bei der Decoit GmbH im Bereich Systemmanagement und ist für Linux-Implementierung und -Entwicklung zuständig.