KAPITEL 5:

GRUNDLAGEN VON NGX

Für den Administrator, der das erste Mal eine Check Point VPN-1 installiert oder sich überlegt, mit dieser Software zu arbeiten, ist dieses Kapitel wichtig. Check Point NGX kann durchaus mit einem Auto verglichen werden, und der Administrator muß sich zunächst für das Modell und seine Ausstattung entscheiden.
Dieses Kapitel beschreibt die Grundlagen der Check Point NGX (*Next Generation X*[1]). Die Detailkonfiguration wird in den Nachfolgekapiteln ausführlich beschrieben. Sowohl die FireWall-1 als auch die VPN-1 sind lediglich ein Teil der NGX, die aus wesentlich mehr Modulen besteht, beispielsweise bei der Power-Version auch aus FloodGate-1 für das Bandbreitenmanagement.

5.1 Funktionsprinzip von NGX

Dieser Abschnitt geht kurz auf den Firewall-Mechanismus und weitere Grundlagen von NGX ein. Detailliert wird diese Lösung von Check Point in den nachfolgenden Kapiteln dargestellt.

5.1.1 Firewall-Mechanismus und Application Intelligence

Check Point setzt in seiner FireWall-1 bereits seit über zehn Jahren, also der ersten Version überhaupt, Stateful Inspection als Firewall-Mechanismus ein. Über die Jahre wurde sie stets weiter entwickelt, so daß sie auch heute einen wirklich ausgereiften Stand hat. Falls mit exotischen Protokollen Probleme auftreten sollten, sind diese Probleme nicht immer bei Check Point selbst zu suchen. NGX stellt an den Administrator hohe Anforderungen und es wird vorausgesetzt, daß er die mehrere tausend Seiten umfassende Dokumentation gut durchgearbeitet hat. Da dies meist schon aus Zeitgründen nicht möglich ist, passiert es immer wieder, daß auf Mailinglisten und Foren Fragen auftauchen, die eigentlich durch das Lesen der Dokumentation nicht auftreten sollten und mit den vier Buchstaben

[1] Und hier die Preisfrage: Für was steht das *X* in NGX?
Anregungen werden gerne unter *mleu@aerasec.de* entgegengenommen :-)

»RTFM« abgehandelt werden können. Die Stateful Inspection ist ausgereift und wird inzwischen von sehr vielen Herstellern ebenfalls verwendet. Auch Linux filtert anhand dieser Methode die Daten. NGX unterscheidet sich also diesbezüglich von den anderen Firewalls kaum – und nicht immer ist das Argument, daß dieser Mechanismus von Check Point entwickelt wurde, wirklich der Grund für den Erwerb von NGX. Mit frei verfügbaren Lösungen und ein wenig Bastelarbeit läßt sich eine Firewall aufbauen, die die Basis-Anforderungen an Sicherheit und Funktionalität ebenfalls erfüllt.
Genau das hat Check Point wohl im Jahre 2003 mit der Einführung seiner »Application Intelligence«, kurz AI, ebenfalls erkannt. Heute sind die meisten Unternehmen durch eine Firewall gegenüber Angriffen aus dem Internet geschützt. Der Zugriff auf interne Systeme von Unternehmen ist also durchaus beschränkt und Angreifer versuchen häufig schon gar nicht mehr, direkt mit beispielsweise Telnet oder FTP auf interne Server zuzugreifen. Aber so gut wie jede Firewall hat Löcher, durch die Server der Unternehmen anzusprechen sind. Das sind nicht potentielle Schwachstellen, sondern gewünschte Zugriffe für Außenstehende. Beispielsweise soll der Nameservice die Namen von Servern auflösen, E-Mail soll aus dem Internet entgegengenommen werden und schließlich auch der Zugriff auf den für Werbe- oder Verkaufszwecke betriebenen Webserver möglich sein.
Heute haben sich Angreifer damit abgefunden, daß nur noch bestimmte Ports der Server ansprechbar sind. Um auf einem Webserver möglicherweise erhöhte Rechte zu erlangen, erfolgt der Angriff gegen das System über die Applikationsebene, genau über den Port, der an der Firewall erlaubt ist. Oft handelt es sich aus Sicht der Firewall um eine normale Verbindung, obwohl gerade über diese Verbindung Daten übertragen werden, die nicht gut für den Webserver sind. Application Level Gateways untersuchen die weitergeleiteten Daten sehr genau, zeigen aber bei der Performance oft Nachteile. Auch ist die Untersuchung und Weiterleitung tatsächlich aller Protokolle nicht immer möglich beziehungsweise vorgesehen. Dies bietet aber die Stateful Inspection.
Um die Vorteile der Application Level Gateways mit denen der Stateful Inspection zu vereinen, führte Check Point die *Application Intelligence* (AI) und Web Intelligence ein. Hier werden die übertragenen Daten der Applikationsschicht im Kernel untersucht. Eine wirkliche Interpretation der Daten ist im Kernel zwar nicht möglich, wohl aber funktioniert eine Mustererkennung über viele Pakete hinweg, so daß bestimmte und bekannte Angriffsmuster erkannt und entsprechend gesperrt werden können. Da diese Untersuchungen im Kernel stattfinden, ist die Geschwindigkeitseinbuße im Vergleich zu den klassischen Proxies gering. Zusätzlich erfolgt eine Untersuchung, ob beispielsweise die an den Webserver übertragenen Daten den geltenden RFCs entsprechen. Demnach dürfen beispielsweise in dem URL keine Binärdaten enthalten sein und die HTTP-Header nur eine bestimmte Länge besitzen. Die AI ist also eine wichtige Erweiterung der Stateful Inspection, die durch andere Hersteller oder freien Lösungen nicht in diesem Maße umgesetzt wird. Zwar führen Firewalls anderer Hersteller eine genaue Untersuchung durch, aber durch die ständigen Aktualisierungen durch Check Point bietet NGX derzeit einen wirklich guten Schutz gegenüber Angriffen auf der Applikationsebene. Diese Aktualisierungen sind nicht kostenfrei, sondern setzen eine »SmartDefense Subscription«[1] voraus.

[1] Diese SmartDefense Subscription ist pro Gateway abzuschließen, obwohl bis einschließlich NGX R61 die in SmartDefense formulierten Vorgaben zentral für alle Firewalls gelten.

5.1.2 Security Server

Bereits seit vielen Versionen der FireWall-1 gibt es die Security Server, die einerseits für die Authentisierung von Benutzern, andererseits für die integrierte Inhaltskontrolle zuständig sind. Dabei kann beispielsweise JavaScript im übertragenen HTML-Code deaktiviert werden. Das sind direkte Änderungen der Daten auf der Applikationsebene. Die Security Server arbeiten so wie Application Level Gateways im Userspace. Sie funktionieren genau wie diese Firewalls und damit auch als Proxy, durch den eine separate Verbindung zum Zielsystem aufgebaut wird. Seit NG ist dieser Proxy scheinbar transparent. Das heißt, daß nicht mehr die externe IP-Adresse der Firewall, sondern die des anfragenden Clients beim Server sichtbar ist. Erreicht wird dieses durch das Austauschen der IP-Absenderadresse, wenn das Paket die Firewall verläßt.
Die Security Server haben also den Vorteil von Application Level Gateways und auch einen ihrer Nachteile: Die Performance kann leiden, weil sie zusätzlich als Applikation auf der Firewall arbeiten und die Untersuchung nicht im Kernel durchgeführt wird.

5.1.3 Zentrales Management

Moderne Firewalls sind nicht mehr nur Mechanismen, um den Datenverkehr zwischen Netzwerken unterschiedlicher Vertrauensstufen zu regeln. Vielmehr kommen heute weitere Anforderungen hinzu, unter anderem daß die Firewall gleichzeitig als Endpunkt für feste VPNs zwischen einzelnen Unternehmensteilen oder auch bei der Anbindung von Partnern arbeitet. Eigene Mitarbeiter müssen von Ihrem PC aus über das Internet auf interne Daten zugreifen und nutzen hierfür einen VPN-Client oder bauen die Verbindung über SSL auf. Zusätzlich sollen bestimmte Dienste priorisiert werden, besonders bei Internet-Telephonie (Voice over IP, VoIP) oder Videokonferenzen kann das wichtig sein. Viele weitere Funktionalitäten sind heute gefragt und werden auch von unterschiedlichen Herstellern ebenfalls angeboten, was zu Schwierigkeiten bei der Verwaltung all dieser Komponenten führen kann. Check Point hat bereits seit den ersten Versionen der FireWall-1 ein wirklich zentrales Management integriert, mit dem auch komplexe Installationen mit beispielsweise mehr als 25 Firewalls übersichtlich zu verwalten sind. Diese Übersicht ist neben einer guten Technologie essentiell, um die gewünschte Sicherheit tatsächlich und mit einem vertretbaren zeitlichen Aufwand erreichen zu können. Seit NGX R61 kann zusätzlich optional neben Firewalls auch Check Point InterSpect, Connectra und VPN-1 Edge X[1] direkt über ein zentrales GUI verwaltet werden. Das ist ein weiterer Schritt, daß der Administrator wirklich nur noch eine zentrale Stelle für die Verwaltung seiner die Firewalls betreffende Sicherheitsinfrastruktur benötigt.

[1] Diese Begriffe werden weiter unten näher erklärt.

5.2 Secure Virtual Networking und Secure Internal Communication

Bereits mit der Einführung von NG vereinheitlichte Check Point die gesamte interne Kommunikation der einzelnen Komponenten seiner Sicherheitslösung. Frühere Versionen der FireWall-1 besaßen proprietäre Protokolle zur internen Kommunikation, die größtenteils (proprietär) verschlüsselt abgewickelt wurde. Dafür mußte zwischen den einzelnen Komponenten die Vertrauensbeziehung explizit hergestellt werden. Dieser Punkt bereitete aber immer wieder Probleme, da der Administrator das gegenseitige Vertrauen immer manuell herstellen mußte. Besser wäre eine zentrale Instanz, die alle Komponenten der Check Point kennt und das Vertrauen durch die Ausgabe von Zertifikaten bekanntgibt. Genau das wurde durch die Einführung der *Secure Internal Communication* (SIC) im Rahmen des *Secure Virtual Networking* (SVN) erreicht. Damit ist die gegenseitige Authentisierung der Komponenten von NGX und auch die Verschlüsselung vereinheitlicht.

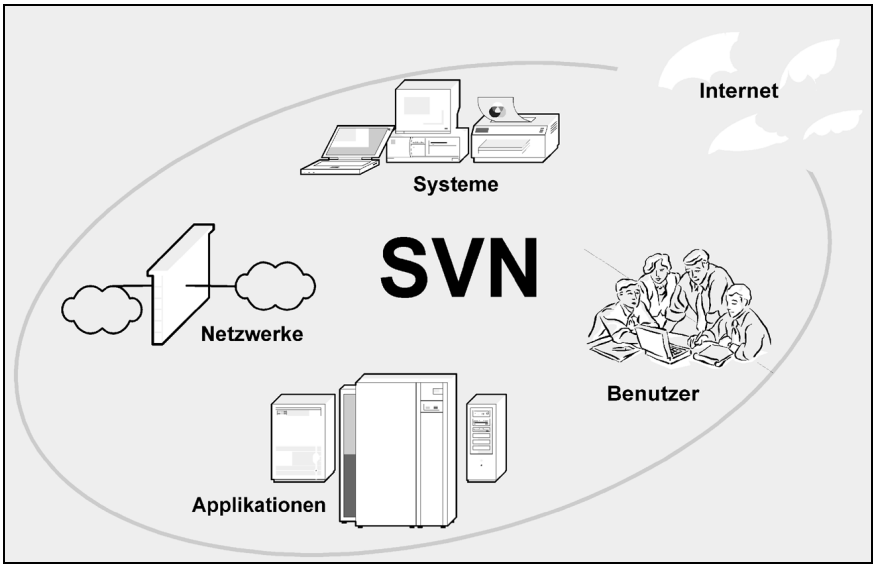

Abbildung 5.1: Prinzip von SIC und SVN

NGX nutzt für die Übertragung von Daten zwischen seinen einzelnen Komponenten, beispielsweise zwischen dem SmartCenter und der Firewall, grundsätzlich SSL[1]. Auch das birgt potentielle Risiken, beispielsweise muß die Identität der beteiligten Partner sichergestellt sein. Hier sorgt Check Point durch den obligatorischen Einsatz einer Internal Certificate Authority (ICA) dafür, daß die Authentisierung während des normalen Betriebes grundsätzlich über Zertifikate erfolgt. Lediglich für den ersten Verbindungsaufbau zwischen den Komponenten wird ein Einmal-Paßwort, hier *Activation Key* genannt, genutzt. Auch beim GUI, das sich zum SmartCenter verbindet, erfolgt der Aufbau der verschlüssel-

[1] SSL: Secure Socket Layer, ein ursprünglich von Netscape entwickelter Standard, der heute für eine sichere Datenübertragung im World Wide Web sorgt.

ten Strecke erst nach einer zertifikatsbasierten Authentisierung. Wenn das Zertifikat erstmals an den Client übertragen wurde, hat der Administrator die Aufgabe, den Fingerprint zu überprüfen. Ist er richtig und vom Administrator bestätigt, wird das Zertifikat gespeichert und für die weiteren Authentisierungen genutzt. Natürlich können diese Zertifikate wieder gelöscht werden.
Insgesamt betreibt Check Point mit NGX einen eher ganzheitlichen Ansatz, der eine frühere Einschränkung auf die Firewall an und für sich aufhebt. Durch SVN ist die Integration des Schutzes von Netzwerken, Servern sowie Applikationen vollzogen. Auch ist die Verwaltung von Benutzern, seien es interne oder Benutzer aus dem Internet, integriert. Somit besteht liegt auf der einen Seite eine einfach zu bedienende, integrierte Sicherheitslösung mit zentraler Verwaltung vor, die auf der anderen Seite aber sehr komplex ist. Daß so etwas nicht nur vorteilhaft ist, zeigte die Einführung der ersten Version von Next Generation. Die Administratoren, die damals eine der ersten Versionen installierten, hatten mit erheblich mehr Schwierigkeiten zu kämpfen als erwartet. Diese Probleme sind seit einiger Zeit allerdings gründlich behoben.
Durch Next Generation wurde insgesamt eine Trennung der Basis-Software für den Betrieb der Produkte von Check Point insgesamt und der FireWall-1/VPN-1 vollzogen. Die Basis ist die SIC mit der SVN Foundation. Befehle, die die SIC und damit die gesamte Installation betreffen, beginnen mit den Buchstaben »cp...«, während die kommandozeilenorientierte Steuerung des SmartCenter mit »fwm« beziehungsweise der Firewall mit »fw« geschieht. Diese beiden Anweisungen beziehen sich also speziell auf die FireWall-1/VPN-1.
Seit Next Generation besteht auch in den Verzeichnissen eine deutliche Trennung der Zuständigkeiten. Die Umgebungsvariable

```
$CPDIR
```

steht für den Pfad, in dem sich bei das Unterverzeichnis mit der SVN Foundation befindet, die für die Secure Internal Communication zuständig ist. Im Unterverzeichnis */bin* befinden sich unter anderem die Befehle *cpstart*, *cpstop*, *cprestart* und *cpconfig*. In dem dazu gehörenden Konfigurationsverzeichnis sind unter anderem beispielsweise die Lizenzen und Zertifikate hinterlegt. Auch befinden sich hier die Dateien, in denen die Check Point festhält, welche IP-Adressen als intern erkannt wurden – falls es sich um eine Version der VPN-1 handelt, die nicht für unbeschränkt viele IP-Adressen gültig ist. Während der Installation (auch bei Microsoft Windows) wird nicht gefragt, welches Verzeichnis hierfür genutzt werden soll. Unter Windows wird es unterhalb vom Programmverzeichnis automatisch angelegt. Die Umgebungsvariable

```
$FWDIR
```

beschreibt den Ort, an dem die FireWall-1/VPN-1 installiert ist. Hier befinden sich also die Programme und Dateien zur Konfiguration der Firewall beziehungsweise der VPNs. Bei

der Installation unter Microsoft Windows kann der Administrator das Verzeichnis bestimmen. Üblicherweise befindet es sich unterhalb vom Windows-Verzeichnis.
Falls FloodGate-1 zum Bandbreitenmanagement zum Einsatz kommt, wird hier eine weitere Umgebungsvariable wichtig: *$FGDIR*. Die einzelnen Komponenten sind bei NGX also sauber getrennt.
Diese mit NG eingeführte Unterscheidung bereitete Administratoren, die bereits länger mit Produkten von Check Point arbeiten, ab und zu Probleme. Sie ist aber dennoch sehr sinnvoll, da *$CPDIR* die Basis darstellt, auf der *$FWDIR* aufsetzt. Nur durch diese Trennung kann zwischen den einzelnen Produkten von Check Point eine Unterscheidung in den Verzeichnissen erfolgen.
Insgesamt nennt Check Point seit Einführung des Feature Pack 3 für Next Generation die gesamte Architektur *Secure Management ARchiTecture* (SMART). Als Folge haben die meisten Komponenten von Check Point seitdem zumindest diese Vorsilbe.
Die gesamte Installation wird durch einen WatchDog überwacht. Das heißt, wenn ein ursprünglich gestarteter Prozeß plötzlich nicht mehr vorhanden ist, erfolgt automatisch ein Neustart. Dies erhöht die Verfügbarkeit von NGX. Allerdings sollte sich jeder Administrator darüber im klaren sein, daß das einfache Abschießen eines Prozesses nicht wirklich hilft, denn der Watchdog startet ihn erneut. Besser ist in einem solchen Fall, NGX durch das Kommando *cpstop* komplett anzuhalten.

5.3 Die Basiskomponenten von NGX

Die Grundlage für alle Komponenten bildet die Check Point SVN Foundation, die bei allen Produkten installiert wird. Sie ist für die Nutzung der SIC zwingend notwendig. Ist SVN nicht installiert, können die Komponenten von Check Point NGX nicht sicher miteinander kommunizieren. Zusätzlich kann die weitere Kommunikation zu Servern, auf denen OPSEC[1]-kompatible Applikationen laufen, auch über SIC geregelt werden. Die Hersteller von beispielsweise Anti-Virus-Software haben diese Möglichkeiten oft implementiert. Erfolgt die Kommunikation zu diesen Servern über SIC, kann zusätzlich der Zustand der Server über den SmartView Monitor überwacht werden.
Bei NGX sind nicht grundsätzlich alle optionalen Features automatisch aktiviert. Dies hat zwar den möglichen Nachteil, daß der Administrator zu einem Zeitpunkt, ab dem weitere Möglichkeiten genutzt werden sollen, ein mit Kosten verbundenes Update der Lizenz vornehmen muß. Andererseits ist der Vorteil dieses Ansatzes, daß keine für den Administrator unnötigen Features lizenziert und damit letztendlich auch bezahlt werden müssen.
Check Point NGX ist mit ihren vielen Kombinationsmöglichkeiten im Bereich Lizenzen mit einem Auto vergleichbar. Der Kunde geht zu einem Autohändler und bestellt sein »maßgeschneidertes«, neues Fahrzeug. Wenn er nur ein »Auto« wünscht, kommt erst einmal die Frage des Verkäufers, was sich denn der Kunde in Bezug auf Modell und Ausstattung erwartet. Die gleichen Fragen sollten von einem guten Reseller kommen, wenn ein Unternehmen lediglich eine »Check Point NGX« bestellt. Die grundsätzliche, erste Unterscheidung war bis NGX R60 die Lizenzierung als »Express« oder »Enterprise«. Express heißt nicht, daß diese Version schneller arbeitetet, vielmehr handelte es sich um eine

[1] OPSEC: Open Platform for Secure Enterprise Computing, siehe auch http://www.opsec.com

bezüglich der geschützten Benutzer grundsätzlich beschränkte Versionen, während die Enterprise-Version keinerlei Beschränkungen für Benutzer oder verwalteten Firewalls hatte. Dieses spiegelte sich auch im Preis für die Enterprise-Version wieder. Seit NGX R61 sind nur noch zwei andere Versionen verfügbar. Bei VPN-1 UTM ist für mittlere Unternehmen gedacht, es ist optional eine Anti-Virus-Software integriert. Lizenzen gibt es ab 50 bis unlimitiert viele interne Benutzer. VPN-1 Power enthält zwar keinen Schutz gegen Schadcode, dafür aber den »Performance Pack«, der die Weiterleitung von Daten erheblich beschleunigt. Auch die Kombination von UTM und Power ist möglich. Näheres zu UTM und Power ist in Kapitel 6.9.1 zu finden. Daneben lassen sich weitere Optionen lizenzieren. Der Vergleich mit dem Auto geht so weit, daß die Ledersitze und das Navigationssystem nicht mit einem kleinen Motor (VPN-1 UTM) zu kombinieren sind.

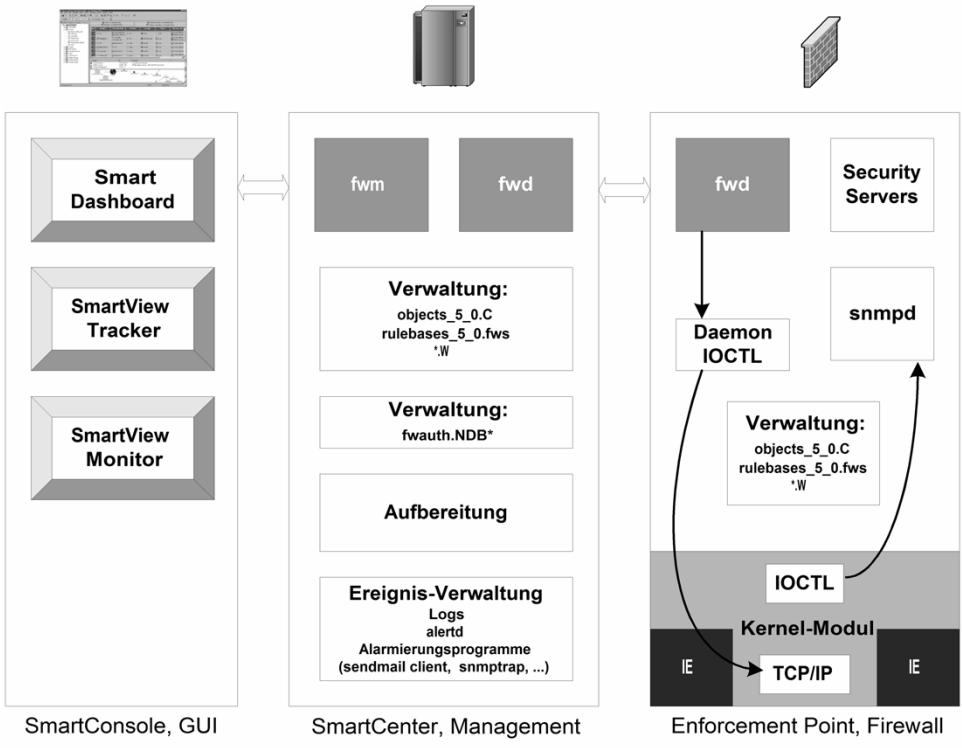

Abbildung 5.2: Zusammenhang der einzelnen Komponenten von NGX

Die FireWall-1 ist auch in der Version NGX neben der SVN grundsätzlich aus drei Grundkomponenten aufgebaut:

Enforcement Point: Umsetzung der Sicherheitsrichtlinien auf der technischen Ebene, also die Firewall an sich.

SmartCenter: Zentrale Verwaltungseinheit von NGX mit der Internal Certificate Authority.

SmartConsole: Verschiedene Programme mit grafischen Oberflächen für den Administrator.

Diese drei Teile sind neben der SVN für den Betrieb von Check Point NGX unabdingbar. Dazu gibt es inzwischen eine zusätzliche Möglichkeit, auf die Konfigurationsdaten von außen mit einem Browser verschlüsselt zuzugreifen (SmartPortal). Bei keiner Version von NGX müssen sich alle drei Komponenten zwingend auf einer einzigen Maschine befinden. Auch bei der kleinsten Lizenz für 50 interne Benutzer ist die Aufteilung auf drei Systeme möglich und oft auch sinnvoll.
Neben diesen Grundkomponenten gibt es verschiedenste Erweiterungsmöglichkeiten, wodurch Check Point NGX eine äußerst flexible und anpaßbare Lösung für sehr unterschiedliche Anforderungen ist.

5.3.1 Enforcement Point – die Firewall

Der Enforcement Point, oft auch einfach »Firewall« genannt, wird auf dem System installiert, das als Gateway zwischen zwei abzugrenzenden Netzwerken arbeitet. Es muß mindestens zwei Netzwerk-Interfaces besitzen, ansonsten ist der gewünschte Schutz nicht gewährleistet. Falls eine Firewall nur ein Netzwerk-Interface besitzen sollte, kann im schlimmsten Fall eine solche Firewall nur »zusehen«, was an Datenverkehr über die Grenze des Netzwerkes geht, aber nicht direkt eingreifen.

Bemerkung:

Von Check Point wird eine Version angeboten, die prinzipiell ähnlich wie eine normale Firewall arbeitet: der SecureServer. Dieses Modul ist für den Schutz von einer einzigen Maschine ohne Routing-Funktionalität gedacht. Diese Software regelt also nicht den Datenverkehr über ein Gateway, sondern lediglich Verbindungen von und zu diesem System. Angewendet wird dies beispielsweise zum Schutz eines Web-, SAP- oder Datenbankservers. Prinzipiell kann der Computer mit SecureServer zwar mehrere Netzwerk-Interfaces besitzen, darf beziehungsweise kann lizenztechnisch aber die Pakete nicht von einem Interface zum nächsten routen.

Die Firewall besteht aus verschiedenen Teilen. Die Inspect-Engine ist der Teil der FireWall-1, der die Regeln, die der Administrator zur Kontrolle des Datenverkehrs zwischen einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netzwerk eingegeben hat, auf der technischen Ebene umsetzt. Es befindet sich zwischen den ISO/OSI-Schichten 2 und 3 im Stack der Gateway-Maschine als ein an den Kernel gelinktes Modul. Die an einem Netzwerk-Interface ankommenden Daten werden kontrolliert und weitergeleitet beziehungsweise fallengelassen, je nach dem, was der Regelsatz fordert. Das Untersuchungsprinzip ist die Stateful Inspection, damit ist also im Prinzip eine Kontrolle bis zur Applikationsebene möglich. Die in Kapitel 4.3 genannten Vor- und Nachteile gelten hier.
Den entsprechenden Regelsatz bekommt die Inspect-Engine in kompilierter Form vom SmartCenter. Einerseits kann die Installation auf der lokalen Maschine erfolgen, das heißt, der SmartCenter und die Inspect-Engine befinden sich auf dem gleichen System. Andererseits erfolgt bei einer verteilten Installation die Kommunikation über das Netzwerk über SIC. Ist die FireWall-1 gut eingerichtet, muß diese Verbindung vom SmartCenter zur Firewall explizit gestattet sein; verwendet wird der im GUI bereits vordefinierte Service *CPD*[1] (18191/tcp).

[1] CPD: Check Point Daemon

Hinweis:

Der normale Betrieb von örtlich getrennten SmartCenter und Firewalls erfordert weitere Verbindungen, teilweise in der umgekehrten Richtung.

In der gleichen Richtung wie bei der Installation erfolgt immer dann ein Verbindungsaufbau vom SmartCenter zur Firewall, wenn der Administrator den Status der Firewall abruft beziehungsweise aktualisiert. Hier kommt der Service *CPD_amon* (18193/tcp) zum Einsatz. Außerdem muß für die Nutzung der in Kapitel 11.1.7 vorgestellten Block-Intruder-Funktionalität auch der Service *FW1_sam* (18183/tcp) vom SmartCenter zur Firewall gestattet sein.
In umgekehrter Richtung liefert die Firewall ihre Logdaten an das SmartCenter. Der hier notwendige Service ist *FW1_log* (257/tcp). Damit liegen später die Ereignisse, die nach dem Regelsatz einen Log-Eintrag erfordern, im Log auf dem SmartCenter vor. Kann die Firewall ihre Daten für das Logging einmal nicht an den SmartCenter »abliefern«, werden sie lokal auf der Maschine, auf der sich die Firewall befindet, zwischengespeichert. Wenn nach einer gewissen Zeit oder dem Neustart der Maschine die Verbindung zum SmartCenter wieder klappt, werden die Daten am Stück übertragen.
Neben der dieser Verbindung ist bei einer getrennten Installation von SmartCenter und Firewall wiederum der Service *CPD* (18191/tcp) beim Neustart der Firewall notwendig. Bei einem Neustart wird versucht, den zu installierenden Regelsatz vom SmartCenter herunterzuladen. Nur wenn das nicht gelingen sollte oder der lokale Regelsatz aktuell ist, wird die während der letzten Installation lokal angelegte Sicherungskopie des Regelsatzes installiert.
Für eine nähere Beschreibung der Trennung von SmartCenter und Firewall sowie der hier notwendigen Dienste siehe Kapitel 18.3.3.
Einige Firewalls bieten die Option, mehr als die für eine wirksame Firewall minimal notwendige Anzahl von zwei Netzwerk-Interfaces anzuschließen. Sind die Firewalls einiger Hersteller auf beispielsweise maximal drei Netzwerk-Interfaces beschränkt, gilt das für NGX nicht. Sind virtuelle Interfaces oder die Konfiguration von VLANs notwendig, lassen sie sich entsprechend konfigurieren, falls das vom Betriebssystem unterstützt wird. Die maximale Anzahl physikalischer beziehungsweise virtueller Interfaces ist heute so hoch, daß die hierdurch vorgegebenen Grenzen in der Praxis meist nicht erreicht werden. Zudem kann es vorkommen, daß beispielsweise die Hardware oder das Betriebssystem, unter dem diese Software läuft, die für die NGX maximal mögliche Anzahl von Interfaces nicht unterstützt.
Der Enforcement Point, also die Firewall, besteht genau genommen auch wieder aus unterschiedlichen Teilen. Neben der eben genannten Inspect-Engine, die im TCP/IP-Stack zwischen dem Netzwerktreiber und der Netzwerkschicht arbeitet, übernimmt ein Daemon-Prozeß (*cpd*) die meiste Kommunikation zwischen der Firewall und dem SmartCenter. Ein weiterer Prozeß, der *fwd*, steuert das Kernel-Modul über IOCTL() und ist für die Logs sowie das Auslesen der Kernel-Traps von */dev/fw0* zuständig. Außerdem befinden sich hier weitere Prozesse: die Security Server. Sie arbeiten unter anderem als Proxies, die stellvertretend für die anfragende Maschine eine Verbindung zum Ziel aufbauen. Für den Benutzer erscheinen sie, je nach Konfiguration, transparent. Sie nehmen beispielsweise ebenfalls die Authentisierung der einzelnen Benutzer vor, untersuchen übertragene Daten auf der Applikationsebene und können über verschiedene Protokolle auch mit anderen Servern wie beispielsweise einem Anti-Virus-Server kommunizieren. Bei der Konfigurati-

on solcher Kontrollmöglichkeiten sind grundsätzlich die Security Server der Firewall beteiligt. Eine nähere Untersuchung der Applikationsebene wird mit Hilfe von Ressourcen erreicht, die in Kapitel 8.4 vorgestellt werden. Sie setzen heute nicht mehr immer und zwingend die Security Server voraus. So gibt es beispielsweise die Möglichkeit, über eine URI-Ressource für HTTP nur ein sehr ausführliches Logging zu aktivieren. Zwischenzeitlich kann man auch Ressourcen für CIFS definieren, die für Datei- und Druckerfreigaben unter Microsoft Windows vorgesehen sind. Die Security Server kommen an dieser Stelle nicht zum Einsatz.

5.3.2 SmartCenter – das zentrale Management

Der SmartCenter von NGX ist die zentrale Verwaltungseinheit des gesamten Sicherheits-Systems. Hier sind alle für den Betrieb der NGX notwendigen Daten gespeichert. Die einzelnen Daten der FireWall-1, wie beispielsweise die Logdaten, die einzelnen Regelsätze, die Benutzerdatenbasis und vieles weiteres mehr werden hier gespeichert und verwaltet. Deshalb sollte der SmartCenter nur auf einer wirklich vertrauenswürdigen und möglichst gut geschützten Maschine laufen. Das kann einerseits die Firewall selbst sein, so daß beide Teile auf einem einzigen System arbeiten. Andererseits ziehen viele Administratoren eine getrennte Installation vor. Es sind keine speziellen Sicherheitslücken bekannt, die aus dem gleichzeitigen Betrieb des SmartCenter und der Firewall auf einer Maschine resultieren. Zu bedenken ist allerdings, daß die Last auf dem System erhöht wird oder auch die Verfügbarkeit bei einem Upgrade des SmartCenter nicht in dem Maße gegeben ist, wie bei einer getrennten Installation.
Der SmartCenter besteht genau genommen aus mehreren Prozessen, dem *cpd* (Check Point Daemon), *fwd* (Firewall-Daemon) und *fwm* (Firewall-Manager). Während der *cpd* für die Kommunikation mit der beziehungsweise den Firewalls und der *fwd* unter anderem für den Export von Logs zuständig ist, findet die zentrale Verwaltung über den *fwm* statt. Beide Prozesse greifen lesend und schreibend auf die internen Datenbanken zu. Aus diesen Daten werden unter anderem auch die in der Regelbasis konfigurierten Alarme generiert. Der Alarmierungsmechanismus kann auf dem SmartCenter auch andere Programme ansprechen, wodurch er sehr flexible Möglichkeiten bietet. Beispielsweise wird ein Alarm per E-Mail versandt oder ein vom Administrator selbst geschriebenes Programm auf dem SmartCenter ausgeführt.
Der *fwm* des SmartCenter hat als weitere Aufgabe die Kommunikation mit dem GUI zur Administration, heute SmartConsole genannt. Auch hier ist darauf zu achten, daß die entsprechenden Verbindungen zwischen dem GUI und dem SmartCenter gestattet sind. Der Service ist *CPMI* (18190/tcp), er muß zwischen dem Arbeitsplatz des Administrators und dem SmartCenter erlaubt sein. Wenn bei den *FireWall-1 Control Connections*[1] von der Grundeinstellung abgewichen wird, muß ein Zugriff vom PC auf Port 18190/tcp zur Firewall-Maschine explizit erlaubt sein, falls SmartCenter und Firewall auf einem System laufen. Außerdem muß am SmartCenter konfiguriert werden, daß von bestimmten IP-Absenderadressen der Zugriff auf den SmartCenter überhaupt gestattet ist.

[1] *VPN-1 & FireWall-1 Control Connections* sind Verbindungen, die unter anderem für die interne Kommunikation der einzelnen Module von NGX notwendig sind – bei einer Installation sind sie (vorerst) grundsätzlich gestattet.

5.3.3 SmartConsole – das GUI

In frühen Versionen der Check Point FireWall-1 hieß die Schnittstelle zum Administrator lediglich GUI. Inzwischen kamen aber so viele Möglichkeiten für die Konfiguration unterschiedlichster Software hinzu, daß Check Point den Ausdruck »SmartConsole« einführte. Der ehemalige Policy Editor heißt inzwischen SmartDashboard – überhaupt ist seit Check Point Next Generation Feature Pack 3 alles smart ;-)
Das GUI unterscheidet bei NGX mehrere Programme, die unterschiedlichen Zwecken dienen. Hierbei sind die wichtigsten das SmartDashboard zur Eingabe von Objekten und Regeln, der SmartView Tracker zur Kontrolle der Logs, SmartUpdate zur zentralen Verwaltung von Lizenzen und Produkten sowie der SmartView Monitor, der unter anderem den Status der Komponenten kontrolliert. Den bei den früheren Versionen vorhandenen SmartView Status gibt es nicht mehr, er ist seit NGX in den SmartView Monitor integriert.
Der Zugriff des Administrators auf den SmartCenter erfolgt normalerweise nur über die grafische Benutzeroberfläche. Sie kann auf dem gleichen Rechner installiert sein, auf der auch der SmartCenter unter Microsoft Windows oder SUN Solaris läuft, muß es aber nicht. Man kann grundsätzlich das GUI auf einer separaten Maschine installieren und den SmartCenter über das Netzwerk ansprechen. Es ist zu beachten, daß unter Umständen die Kommunikation zwischen dem Computer mit dem GUI und dem SmartCenter über den Service *CPMI* (18190/tcp) explizit gestattet sein muß.

Abbildung 3:
Authentisierung vor dem Zugriff auf das SmartDashboard

Da SmartConsole auf jeder beliebigen Maschine betrieben werden kann (auch auf PCs unter einem nicht aktuell gehaltenen Microsoft Windows), ist dem Arbeiten mit dem GUI ein Authentisierungsmechanismus vorgeschaltet. Der Administrator muß hier seinen Benutzernamen, sein Paßwort und den SmartCenter, mit dem er arbeiten möchte, angeben. Bereits seit Next Generation besteht die Möglichkeit, den Administrator am SmartCenter auch über ein paßwortgeschütztes Zertifikat zu authentifizieren. Wenn das Zertifi-

kat auf einem Token gespeichert ist, hängt die Frage nach dem Paßwort auch davon ab, wie das Token mit wiederholt eingegebenen Paßworten umgeht. Hier ist auch ein Single-Sign-on möglich, indem das Token das gerade vorher für die Authentisierung an einer Windows-Domain genutzte Paßwort oder PIN für diese Authentisierung übernimmt.
Für den Betrieb des GUI ist unter Microsoft Windows keine separate Lizenz notwendig, für das GUI unter Motif/Unix ist eine zu erwerben. Für Linux und die anderen Betriebssysteme für NGX ist derzeit kein GUI erhältlich. Wohl aber besteht die Möglichkeit, beispielsweise unter Linux mit Wine das GUI für Windows aufzurufen und damit zu arbeiten.
Das GUI für NGX besteht aus einer Anzahl unterschiedlicher Programme, die unter dem Namen SmartConsole zusammengefaßt sind. Die jeweilige Komponente der SmartConsole wird als normales Programm auf dem PC des Administrators aufgerufen. Zum Verbinden mit dem SmartCenter öffnet sich beispielsweise das in Abbildung 5.3 gezeigte Fenster. Nachdem der Administrator die notwendigen Daten angegeben hat, verbindet sich das Programm der SmartConsole mit dem SmartCenter. Hier erfolgt die eigentliche Authentifizierung.
Zunächst überprüft der SmartCenter, ob von der IP-Adresse, von der die Anfrage kommt, überhaupt ein Zugriff erfolgen darf. Die entsprechende Konfiguration wird zunächst direkt bei der Installation vorgenommen. Änderungen sind jederzeit durch den Befehl *cpconfig* oder auch durch das manuelle Editieren der Datei *$FWDIR/conf/gui-clients* möglich.

Abbildung 4: Meldung beim ersten Anmelden

Wenn sich der Administrator unter NGX das erste Mal an seinem SmartCenter anmeldet, wird ein Hinweis angezeigt. Er sollte an dieser Stelle kontrollieren, ob er wirklich mit dem richtigen SmartCenter verbunden ist. Es wird ein Fingerprint des öffentlichen Schlüssels angezeigt, mit dem die Überprüfung der Identität des SmartCenters möglich ist. Hier sollte der Administrator die Ausgabe mit dem Fingerprint vergleichen, die direkt am SmartCenter erfolgt. Dieses geschieht über den Aufruf des weiter unten beschriebenen Kommandos

```
cpconfig
```

am SmartCenter und der Auswahl von »Fingerprint«. Diese Daten lassen sich auch in einer Datei speichern und an die entsprechenden Administratoren verteilen.
Stimmt der ausgegebenen Fingerprint mit den bekannten Daten überein, kann der Administrator sicher sein, mit der richtigen Maschine verbunden zu sein. Durch die Bestätigung zwischen dem GUI und dem SmartCenter wurde eine verschlüsselte Vertrauensbeziehung aufgebaut (Secure Internal Communication). Falls das GUI lokal auf dem SmartCenter betrieben wird und der Administrator bei seiner Anmeldung die IP-Adresse 127.0.0.1 angegeben hat, braucht die beschriebene Überprüfung nicht stattzufinden.

Abbildung 5: Kontrolle des Fingerprint am SmartCenter (Windows)

Ist der Administrator erfolgreich authentisiert, werden dem Programm der SmartConsole vom SmartCenter die angeforderten Daten zur Verfügung gestellt. Außerdem erhält der Administrator seinem Profil entsprechend Rechte zugeordnet (vgl. auch 8.7). Hier kann nicht nur eine Unterscheidung zwischen einzelnen Administratoren getroffen werden, vielmehr kann jeder Administrator auch unterschiedliche Rechte bekommen. Diese Rech-

te müssen am SmartCenter für jeden Administrator eingetragen sein, wie es in Kapitel 8.6.3 beschrieben ist.
Im Gegensatz zu früheren Versionen kann seit NGX nur noch genau ein Administrator über das Programm *cpconfig* angelegt werden, weitere werden über den User-Manager angelegt, näheres dazu in Kapitel 8.6.3. Der mit *cpconfig* angelegte (einzige) Administrator besitzt alle Rechte. Damit hat er neben dem Schreib- und Lesezugriff auf die Daten des SmartCenter auch das Recht, über den User-Manager neue Administratoren anzulegen. Hier können auch andere Möglichkeiten als statische Paßworte[1] zur Authentisierung der Administratoren konfiguriert werden. Beispiele hierfür sind die Authentisierung über RSA SecurID oder Zertifikate. Zusätzlich kann bei zu vielen fehlgeschlagenen Versuchen ein Administrator-Account automatisch gesperrt werden.
Wichtig beim Zugriff vom GUI auf den SmartCenter ist, daß nur ein einziger Administrator mit Schreibrechten angemeldet sein darf. Der Schreib-/Lesezugriff mit dem SmartDashboard erfolgt schreibend, auch wenn lediglich die Benutzerdatenbank aktualisiert wird. Der Grund für diese vermeintliche Einschränkung ist, daß sich bei zwei schreibend angemeldeten Administratoren einer eigentlich durchsetzen muß. Das bedeutet eine Gefahr für die Sicherheit.
Arbeiten mehrere Administratoren am SmartCenter, kann sich ein Administrator, der eigentlich Schreib- und Leserechte hat, auch nur lesend anmelden. Nur lesende Zugriffe sind beliebig viele erlaubt und das Zurücksetzen der Rechte auf *Nur Lesen* geschieht bei der Anmeldung beim GUI (siehe auch Abbildung 5.3 links unten). Versucht sich ein Administrator aber trotzdem mit Schreibrechten anzumelden, erscheint die in Abbildung 5.6 gezeigte Meldung.

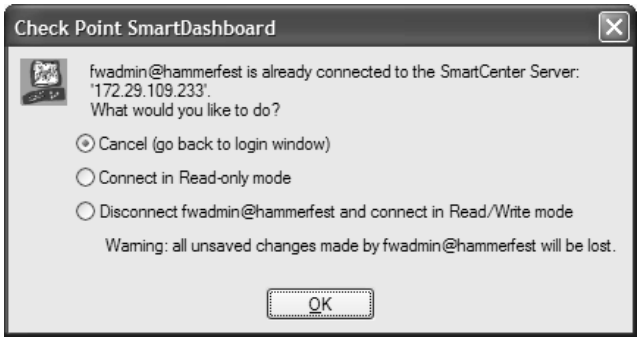

Abbildung 5.6: Meldung des GUI, daß bereits ein Administrator mit Schreibrechten am SmartCenter angemeldet ist

Unter Umständen kann es passieren, daß ein Administrator, der mit Schreibrechten am SmartCenter angemeldet war und seine Abmeldung wegen der plötzlichen Mittagspause vergißt und sich der auf Diät befindliche Administrator nicht mit Schreibrechten anmelden kann. Es kann aber auch passieren, daß ein mit Schreibrechten angemeldeter Administrator das GUI nicht sauber verläßt, weil beispielsweise die Verbindung unterbrochen ist.

[1] Mit dem Hotfix Accumulator 3 für Check Point NGX R60 kann in Kombination mit einem aktuellen SmartDashboard die Länge der Administratoren-Paßworte auf 50 Zeichen ausgedehnt werden. Die Beschränkung auf 8 Zeichen ist also zumindest in diesem Bereich aufgehoben.

Hier ist nicht immer die Schuld beim Administrator zu suchen, denn besonders einige frühe Versionen des GUI für Solaris stürzten auch manchmal ab. Zum Erlangen von Schreibrechten mußte damals entweder der SmartCenter durchgestartet oder die für diese Sperre verantwortliche Datei gelöscht werden. Bei NGX wurde eine Besonderheit des Provider-1 übernommen: Ein mit Schreibrechten angemeldeter Administrator kann von einem anderen Administrator, der die Schreibrechte benötigt, »hinausgeworfen« werden. So etwas sollte auf keinen Fall spaßeshalber gemacht werden, weil sämtliche noch nicht gespeicherten Änderungen damit verloren sind. Aber wenn beispielsweise das bisher schreibend verbundene SmartDashboard keine Verbindung mehr zum SmartCenter hat, ist diese Option von NGX durchaus sehr sinnvoll.
Noch ein kurzer Blick auf die Dateien: Für die Sperre ist die Datei *$FWDIR/tmp/manage.lock* zuständig. Sie kann, falls ein Konsolenzugriff auf den SmartCenter besteht und es sich um eine ältere Version handelt, in der die in Abbildung 5.6 gezeigte Möglichkeit noch nicht geboten ist, auch manuell gelöscht werden, was aber bitte nicht aus »Optimierungsgründen« geschehen sollte. Nach dem Löschen der Datei sollte der SmartCenter durchgestartet werden.
Die Abfrage nach einem Benutzernamen und Paßwort erfolgt sowohl beim Aufruf des SmartDashboard als auch beim Aufruf des SmartView Tracker, des SmartView Monitor oder anderen Programmen zur Bedienung von NGX über das GUI. Auf die drei genannten Anwendungen wird in den folgenden Abschnitten grob eingegangen. Eine detailliertere Beschreibung folgt ab Kapitel 7 sowie in Kapitel 11.

SmartDashboard

Das SmartDashboard, oft von Administratoren auch noch Regelbasiseditor beziehungsweise Policy Editor genannt, ist das zentrale Programm, über das der Administrator seine Firewalls administriert. Es kann unter Microsoft Windows im Gegensatz zu SUN Solaris ohne zusätzliche Lizenz genutzt werden. Einen Blick auf das SmartDashboard zeigt Abbildung 5.7.

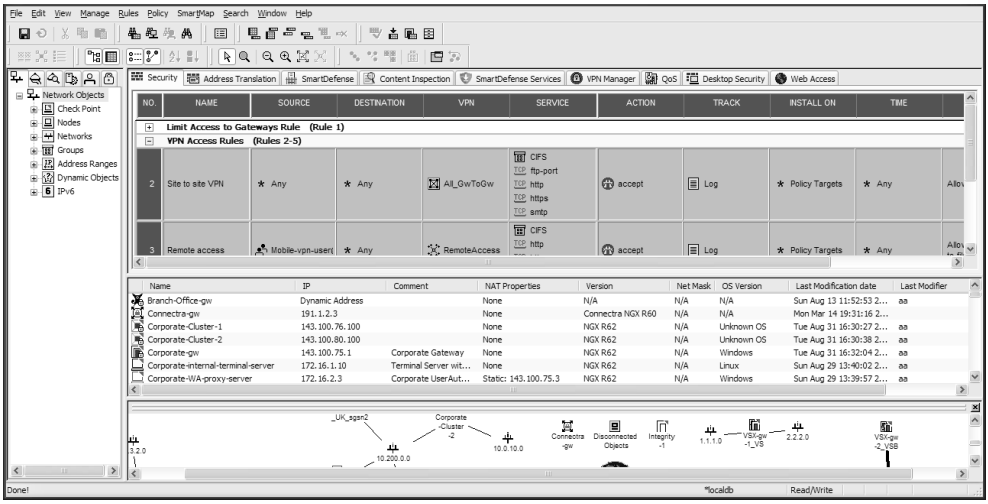

Abbildung 5.7: SmartDashboard

Bevor jedoch einzelne Regeln eingegeben werden können, müssen zunächst alle verwendeten Objekte deklariert werden. Nach der Installation von NGX ist zunächst nur der SmartCenter mit der ICA und sonst kaum etwas bekannt. Auch wird nicht zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken unterschieden. In diesem Status ist der meiste Datenverkehr zwischen den Netzwerk-Interfaces gesperrt, von Ausnahmen abgesehen. Diese sind zwar nicht unbedingt sicherheitskritisch, trotzdem sollte der Administrator sie möglichst frühzeitig kennen und dann entsprechende Anpassungen vornehmen. Sie werden in Kapitel 7.3 detailliert besprochen.
Das SmartDashboard setzt einige grundlegende Arbeiten voraus, damit überhaupt Regeln eingegeben werden können. Hierzu gehört neben dem Anpassen der Globalen Grundeinstellungen unter anderem auch die Definition einzelner Netzwerkobjekte wie beispielsweise Rechner, Netzwerke oder Router. Gegebenenfalls sind auch proprietäre Services oder Ressourcen sowie Benutzer anzulegen. Erst danach kann der Administrator mit dem Übertragen der Sicherheitspolitik auf die technische Ebene beginnen. Gewarnt sei an dieser Stelle, ohne Definition einer firmeninternen Sicherheitspolitik erst einmal »einfach so« mit dem Zusammenklicken einzelner Regeln zu beginnen. Das GUI verführt durch seine leichte und (vorerst) übersichtliche Art dazu; und dann besteht die große Gefahr, daß die Sicherheit aufgrund einer schlechten Konfiguration nicht gewährleistet ist.
Nachdem alle Regeln eingegeben sind, kann die Regelbasis abgespeichert und danach installiert werden. Wichtig ist, daß der Administrator nach der Installation überprüft, ob die Regeln entsprechend greifen beziehungsweise ob alles, was verboten sein soll, auch noch immer nicht funktioniert. Am besten erfolgt direkt nach der Installation der Regelbasis eine intensive Kontrolle der Logs. Insbesondere die unternehmenskritischen Applikationen sollten noch funktionieren.

SmartView Tracker

In dem Moment, in dem eine Regelbasis installiert wurde, sollte also kontrolliert werden, welcher Datenverkehr über die Firewall läuft beziehungsweise auch, welche Daten von der Firewall fallengelassen werden. Dazu dient die zweite Applikation der SmartConsole, der SmartView Tracker (vgl. Abbildung 5.8).
Die ausführliche Beschreibung der einzelnen Einträge bringt Kapitel 11.1. Hier gibt es grundsätzliche, beispielsweise die Installation einer Regelbasis. Andere werden vom Administrator in der Regelbasis gefordert. Hier kann er bestimmen, ob ein bestimmtes Ereignis einen Logeintrag zur Folge hat. Alarme werden automatisch geloggt.
Neben dem normalen Log kann man sich im SmartView Tracker alle derzeit aktiven Verbindungen anzeigen lassen. Optional können einzelne (eigentlich durch die Regeln gestattete) Verbindungen über das Feature »Block-Intruder« verboten werden, und zwar genau in dem Moment, in dem diese Verbindung aktiv, also in die State Tables von NGX eingetragen ist.
Beim Betrachten des Logs momentan aktiver Verbindungen (siehe hierzu auch Kapitel 11.1.6) könnte man sich wundern: Eigentlich schon abgebaute TCP-Verbindungen werden eine zeitlang noch als aktiv dargestellt, sie sind auch in den State Tables noch gespeichert. Daß aber auch UDP- und ICMP-basierter Datenaustausch als Verbindung gewertet wird, wobei diese Protokolle doch verbindungslos arbeiten, führt häufig zu Verwirrung. Nein, hier »täuscht« sich NGX oder einer ihrer Entwickler nicht, sondern die Stateful

Inspection sorgt dafür, daß beispielsweise UDP in einer Richtung erlaubt ist und die Antworten auf genau diese Pakete gestattet sind. Das führt dazu, daß auch UDP einen Eintrag in die State Tables zur Folge hat. Damit gilt also auch UDP oder ICMP als *virtuelle Verbindung*.

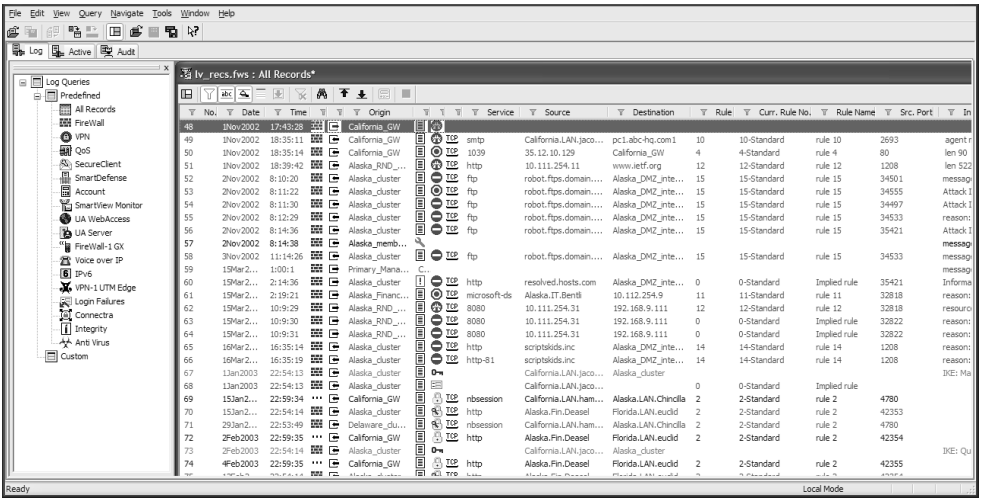

Abbildung 5.8: SmartView Tracker

Als drittes Fenster gibt es im SmartView Tracker das Audit-Log. Dort werden die einzelnen Tätigkeiten, die ein angemeldeter Administrator durchführt, festgehalten. Das ist schon aus Gründen der Revisionssicherheit sehr wichtig. Neben dem An- und Abmelden einzelner Administratoren ist in diesem Log auch das Anlegen oder Verändern von Objekten sowie das Verändern von Regeln oder Objekten nachzulesen.
Administratoren, die sich bereits mit früheren Versionen der Check Point FireWall-1 auskennen, werden das Accounting-Log vermissen. Diese Informationen wurden in das normale Log übernommen. Möglich machte das die Umstellung der gesamten Verwaltung der Logs auf eine Datenbank. Die Informationen zum Accounting sind also weiterhin im Log vorhanden, nur muß sie sich der Administrator explizit anzeigen lassen.
Insgesamt kann die Ausgabe der drei Logs unabhängig voneinander gefiltert werden, nicht immer müssen sämtliche Informationen sichtbar sein. Das Setzen von Filtern kann aber auch dazu führen, daß der SmartView Tracker scheinbar nicht richtig funktioniert – wenn der Administrator eben wissentlich oder unwissentlich Filter gesetzt hat.
Neben dem SmartView Tracker besteht durch SmartView Monitor eine weitere Möglichkeit, die FireWall-1 und andere Geräte, auf denen zur OPSEC kompatible Software installiert ist, zu überwachen.

SmartView Monitor

In den SmartView Monitor ist die bisherige Funktionalität des gegebenenfalls aus früheren Versionen bekannten SmartView Status integriert. Der Zustand einzelner Komponenten, zu denen die SIC aufgebaut ist, läßt sich so überwachen.

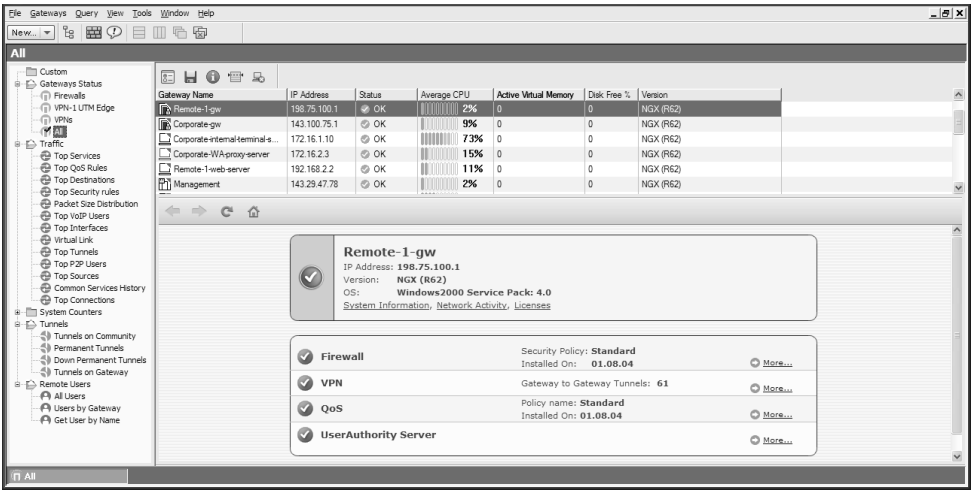

Abbildung 5.9: SmartView Monitor

Für die Nutzung der Basisfunktionen des SmartView Monitor ist keine separate Lizenz notwendig. Abbildung 5.9 ist ein Blick auf das GUI. Der Status aller Objekte wird gleich beim Öffnen angezeigt, wobei überall der grüne Kreis mit dem Haken dargestellt sein sollte, dann ist der Status *OK* und alles ist in Ordnung. Besonders bei größeren Installationen ist es sinnvoll, sich nicht alle Objekte anzeigen zu lassen. Daher kann man im linken Fenster unter dem Punkt *Gateways Status* Einschränkungen festlegen.
Die beiden auf der linken Seite unten dargestellten Menüpunkte sind sehr sinnvoll, falls VPN konfiguriert und produktiv in Betrieb sind. Über den Menüpunkt *Tunnels* kann man sich mit unterschiedlichen Auswahlkriterien den Status einzelner VPN darstellen lassen. So hat der Administrator zentral den Überblick, ob ein festes VPN ausgefallen ist. Einen zentralen Überblick zu Benutzern, die über ein VPN mit einem überwachten Gateway verbunden sind, gibt der unterste Menüpunkt *Users*.
Die Nutzung der Grundfunktionen des SmartView Monitors ist kostenfrei. Nun gibt es aber noch eine Komponente des SmartView Monitor, die auf einem Gateway installiert wird. Beides hat den gleichen Namen, weshalb eigentlich immer genau dazu gesagt werden muß, welcher Teil eigentlich gemeint ist. Die Komponente für ein Gateway ist separat zu lizenzieren. Dafür sind aber über den SmartView Monitor dann weitere Eigenschaften zu überwachen. Der Punkt *Traffic* liefert Statistiken in Echtzeit über beispielsweise die am häufigsten genutzten Regeln, Services oder auch IP-Adressen. Die Überwachung von WAN-Strecken ist ebenfalls möglich, indem Virtual Links konfiguriert und kontrolliert werden. Die *System Counters* liefern eher statistische Informationen über die häufigsten Angriffe, Systemauslastung oder Daten zu den VPN.
Insgesamt ist die Funktionalität des SmartView Monitor von *vor NGX* erhalten geblieben. Mit NGX ist der SmartView Status integriert. Die so zur Verfügung stehenden Informationen sind für die Administration von NGX sehr hilfreich und erheblich ausführlicher als früher.
Näher beschrieben wird der SmartView Monitor in Kapitel 11.2.

Weitere Programme der SmartConsole

Neben den bereits genannten Programmen enthält die SmartConsole einige weitere Programme, die Administratoren in speziellen Situationen durchaus gut weiterhelfen können. Einzelne Optionen dieser Software müssen gegebenenfalls separat lizenziert werden.

SmartUpdate

Soll mit diesem Programm nicht nur die Zuweisung von Lizenzen, sondern auch die Option zur zentralen Aktualisierung der Komponenten von NGX über das Netzwerk durchgeführt werden, muß eine separate Lizenz vorliegen. Sie ist bei der Lizenz für den SmartCenter Pro und damit auch der Version VPN-1 Power enthalten. Dann lassen sich über das Netzwerk Hotfixes einspielen oder auch eine neue Version wie beispielsweise NGX installieren. Besonders bei großen, komplexen Installationen ist es für einen Administrator nicht immer leicht, bei den Lizenzen und den tatsächlich installierten Produkten den Überblick zu behalten. Hier hilft neben der mit NG eingeführten zentralen Lizenzierung SmartUpdate als Werkzeug zur kostenfreien Verwaltung der Lizenzen über das Netzwerk.

Eventia

Die gründliche Auswertung von Logs wird heute noch von vielen Unternehmen vernachlässigt. In solchen Fällen weiß ein Administrator oft überhaupt nicht, ob und wie oft seine Firewall und Server angegriffen werden. Meist wird auch seltsamer Datenverkehr nicht erkannt. Eine Hilfe ist der Eventia Reporter, mit dem die Auswertung historischer Logs relativ einfach ist, da auch unterschiedlichste Kriterien für die Auswertung nutzbar sind. Eine Erweiterung ist der Eventia Analyzer, mit dem die Auswertung unterschiedlichster Logdaten fast in Echtzeit mit Hilfe eines Expertensystems geschieht und bei der ein Administrator auch eine sicherheitstechnische Bewertung der einzelnen Ereignisse erhält. Diese Option ist nicht nur separat zu lizenzieren, sondern auch teuer. Dafür sind aber als Datenquellen für den Eventia Analyzer nicht nur Geräte von Check Point, sondern auch von vielen Drittherstellern möglich.

SecureClient Packaging Tool

Der Rollout sehr vieler VPN-Clients stellt oft ein Problem dar. Der meist von Haus aus gut mit Arbeit versorgte Administrator müßte theoretisch diese VPN-Clients einzeln konfigurieren oder zumindest den Benutzern bei der Installation mit Rat und Tat beiseite stehen. Vereinfacht ist die Installation durch das SecureClient Packaging Tool, mit dem für den Benutzer fertige Pakete geschnürt werden können. Dieser muß im Prinzip dann nur noch die Installationsroutine aufrufen. Die Konfiguration ist in diesem Paket enthalten, so daß SecureClient nach einem Neustart im Prinzip gleich fertig konfiguriert ist. Dieses Werkzeug ist auch bei der Integration von SecureClient mit einem der Integrity-Clients von Bedeutung[1], da nur so hergestellte Pakete bei Integrity weiter bearbeitet und an den Benutzer ausgegeben werden können.

[1] Check Point Integrity ist ein Produkt zur zentralen Verwaltung von Clients, das unter anderem. ein- und ausgehende Verbindungen, laufende Prozesse und Programmaufrufe überwacht.

SmartLSM

Ein smarter und separat zu lizenzierenden Large Scale Manager, mit dessen Hilfe sich sehr viele ROBO[1]-Gateways verwalten lassen. Solche Gateways sind Appliances, wie beispielsweise die Nokia IP60 oder Geräte der Serie VPN-1 Edge. Die Konfiguration dieser Geräte wird in Profilen deklariert, was bei NGX inzwischen gegenüber den Vorgängerversionen stark vereinfacht ist. Außerdem lassen sich mit dem SmartLSM auch VPN-1 UTM und VPN-1 Power verwalten. SmartLSM unterstützt den Administrator hier bei der zentralen Verwaltung.
Teile der oben genannten Optionen sind separat zu lizenzieren, wobei sich durch diese zusätzlichen Lizenzen auch Vorteile ergeben. Besonders die Verwaltung der Geräte für kleine Außenstellen ist bei NGX gegenüber den Vorgängerversionen stark vereinfacht.

5.3.4 SmartPortal – das Webinterface

Seit der Einführung von NGX gibt es neben der SmartConsole eine weitere Möglichkeit, über das Netzwerk auf die Regelsätze, Objekte und Logs zuzugreifen. Wenn die entsprechende Lizenz vorliegt (CPMP-SMPO), kann bei der Installation des SmartCenter gleich das SmartPortal eingerichtet und in Betrieb genommen werden. Damit kann ein authentisierter Benutzer mit seinem Browser über HTTPS zu Port 4433/tcp eine verschlüsselte Verbindung zum SmartCenter aufbauen und sich authentisieren. Unter anderem werden die Objekte, Regeln und Benutzer dargestellt, aber auch ein Blick in das Log ist möglich. Derzeit ist lediglich der lesende Zugriff auf die Daten vorgesehen, wobei aber seit Version NGX R61 zumindest die auf dem SmartCenter angelegten Benutzer über SmartPortal verwaltet werden können.
Ein Vorteil dieser Lösung, die JavaScript im Browser voraussetzt, ist, daß für den Zugriff auf die Konfiguration der Firewall keinerlei separate Software vorausgesetzt wird. Damit ist einerseits prinzipiell der Zugriff aus dem Internet-Cafe möglich, falls dieser Port am PC ausgehend erlaubt ist und der Administrator tatsächlich mit den gegebenenen Risiken leben möchte. Andererseits besteht auch grundsätzlich die Möglichkeit, eine entsprechende Verbindung von PDAs aus aufzubauen und die Regeln beziehungsweise Logs zu kontrollieren. Für diese Verbindungen sollte allerdings UMTS genutzt werden, mit GPRS macht es nicht wirklich Spaß.
Zusätzlich kann SmartPortal sinnvoll sein, wenn die IT-Revision auf die Firewall zugreifen und den Ist- mit dem Soll-Zustand vergleichen möchte. Einerseits hat SmartPortal hier den Vorteil, daß keine zusätzliche Software notwendig ist. Für den Administrator hat es andererseits aber auch den Effekt, daß er sicher sein kann, daß die IT-Revision an der Konfiguration keinerlei Änderungen vornimmt beziehungsweise vornehmen kann.
Insgesamt stellt diese (kostenpflichtige) Möglichkeit zum Zugriff auf den SmartCenter mit einem Web-Browser insbesondere bei komplexeren Installationen eine sinnvolle Erweiterung dar, bei der Check Point zukünftig sicherlich noch die eine oder andere Verbesserung vornehmen wird. Beim Blick in die Kristallkugel könnte sogar diese Option vielleicht auch das GUI in einigen Jahren ablösen.

[1] ROBO: Remote Office, Branch Office – Lösungen für kleine und mittlere Standorte