Netzwerk-Sicherheit – Schutz eines Netzwerks durch ein Check Point Security Gateway

Stefan Schurtz

Check Point Software Technologies Ltd. ist weltweit für seine Firewall- und VPN-Produkte bekannt, und stellt mit seiner noch recht neuen Software Blades eine sehr flexible Security Architektur für Unternehmen bereit.

IN DIESEM ARTIKEL ERFAHREN SIE…

- Kenntnisse in der System- und Netzwerk-Sicherheit
- Kenntnisse in der TCP/IP Netzwerktechnik

WAS SIE VORHER WISSEN SOLLTEN…

- http://www.checkpoint.com – die offizielle Check Point Website
- http://downloads.checkpoint.com/dc/download.htm?ID=11550 – R75 Documentation Package
- http://www.checkpoint.com/campaigns/nss-next-gen-firewall/index.html# - NSS Labs Next Generation Firewall Test Report for Check Point

Einführung

Firewalls gelten als ein wichtiger Teil der IT-Infrastruktur und bilden den Übergang von einem unsicheren, nicht vertrauenswürdigen Netzwerk (z. b. dem Internet) in einen oder mehrere als sicher bzw. vertrauenswürdig geltenden Bereich eines (Firmen)-Netzwerkes.

Auch wenn die heutigen Firewall-Produkte immer sicherer zu werden scheinen, mit gehärteten Betriebs-

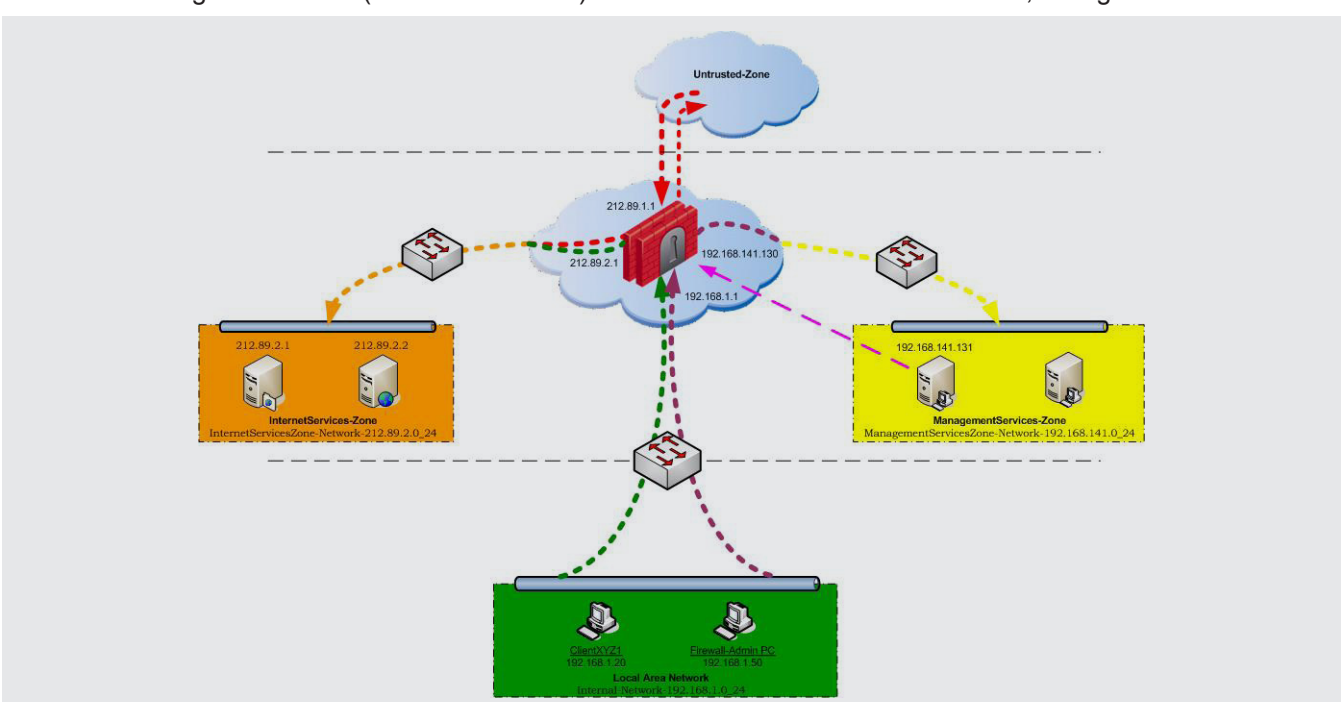


Abbildung 1. *xxxxxxxxx*

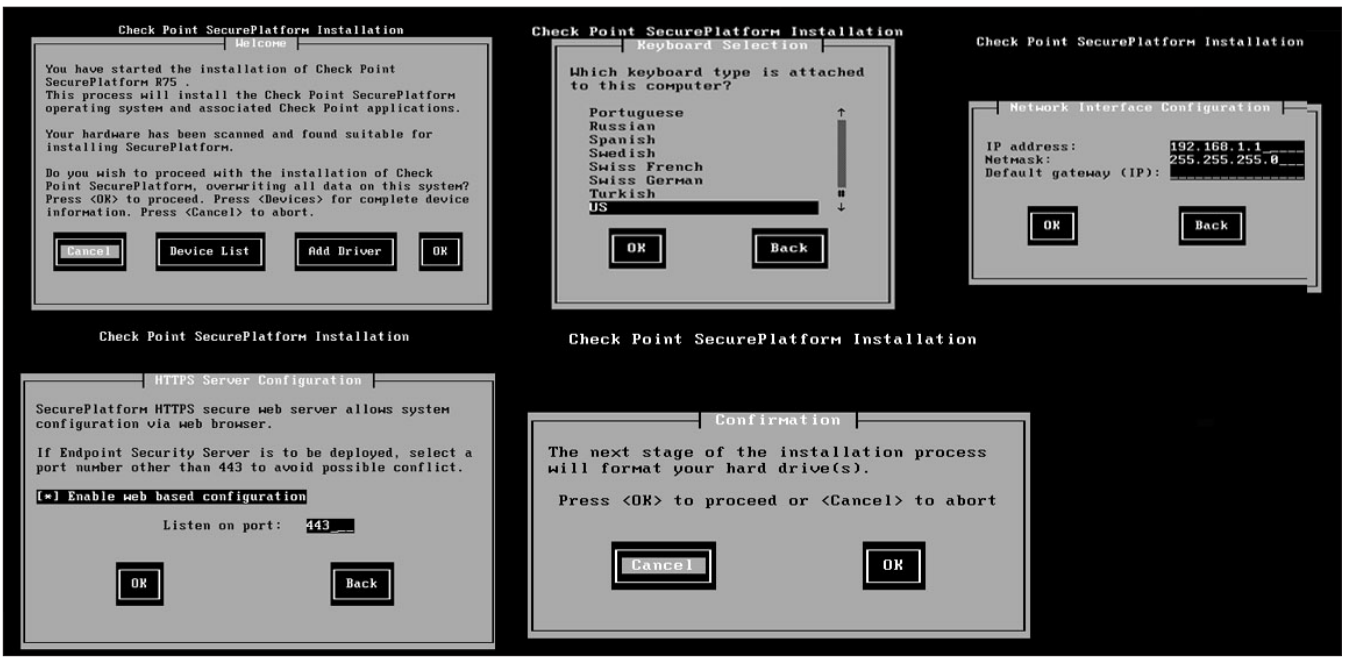


Abbildung 2. *xxxxxxxxx*

systemen daher kommen, steigt auf der einen Seite der Grad an Komplexität der zu schützenden Netzwerke und auf der anderen Seite, wachsen der Druck und Anforderungen an die Security-Administratoren. Schnell werden wichtige und nötige Dokumentationen und Standards „vergessen“ bzw. vernachlässigt und dann sind es gerade diese wichtigen Systeme die Fehlerkonfigurationen unterliegen, was wiederum dazu führen kann, dass selbst die beste und teuerste Firewall schnell ziem-

Abbildung 3. *xxxxxxxxx*

Abbildung 4. *xxxxxxxxx*

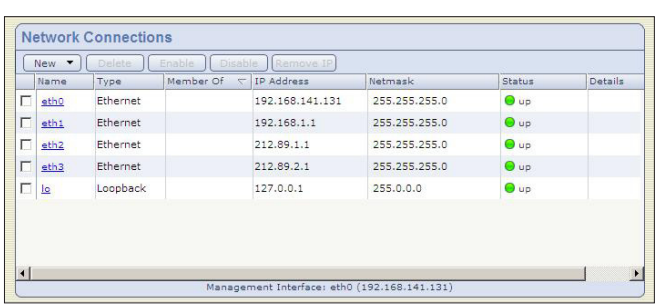


Abbildung 5. *xxxxxxxxx*

Abbildung 6. *xxxxxxxxx*

lich nutzlos wird und von findigen Angreifen schnell überwunden werden kann. Daher ist es für einen Security-Administrator ungemein wichtig den Überblick über das Regelwerk nicht zu verlieren, dieses so einfach wie nur möglich zu gestalten, sich eine strikte Vorgehensweise bzw. einen Standard für die Konfiguration von Objekten, Regeln und Zugriffsrechten zu überlegen, zu dokumentieren und einzuhalten. Ebenso sollte auch die Konfiguration der Firewall bzw. des Regelwerks selbst, den Administrator nicht vor eine zu große Herausforderung stellen und relativ „einfach“ durchzuführen sein und nicht durch eine komplizierte Syntax und/oder unübersichtliche Regel-Konfiguration unnötig erschwert werden.

Check Point

Check Point Software Technologies Ltd. ist weltweit für seine Firewall- und VPN-Produkte bekannt, und stellt mit seiner noch recht neuen Software Blades eine sehr flexible Security Architektur für Unternehmen bereit. Durch diese Architektur ist es möglich Gateway bzw. Management schnell um zusätzliche Security-Module (wie z. b. Application Control Software Blade, Identity Awareness Software Blade, DLP Software Blade, Mobile Access Software Blade) zu erweitern und neuen Anforderungen anzupassen und in einem zentralen Management zu administrieren. Vergessen sollte man hierbei allerdings nicht, dass bei Check Point dies meist mit zusätzlichen (teils nicht unerheblichen) Kosten verbunden ist.

Dennoch bietet Check Point seinem Security Management und den damit verbundenen Werkzeugen (SmartDashboard, SmartTracker, SmartMonitor …) eine gute Möglichkeit mit Hilfe von Objekten (Networks, Groups, Nodes, Interoperable Devices) einen entsprechenden Standard zu etablieren und zu pflegen. Durch die mögliche Unterteilung des Regelwerks in Sektionen, dem Hin-

Abbildung 7. *xxxxxxxxx*

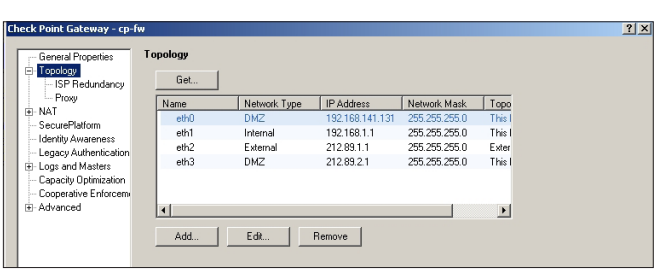


Abbildung 8. *xxxxxxxxx*

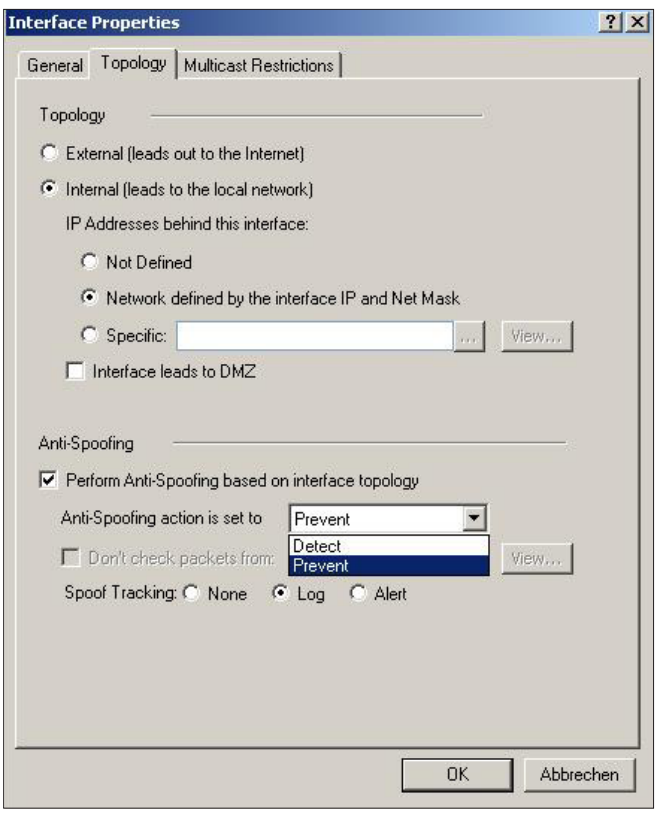


Abbildung 9. *xxxxxxxxx*

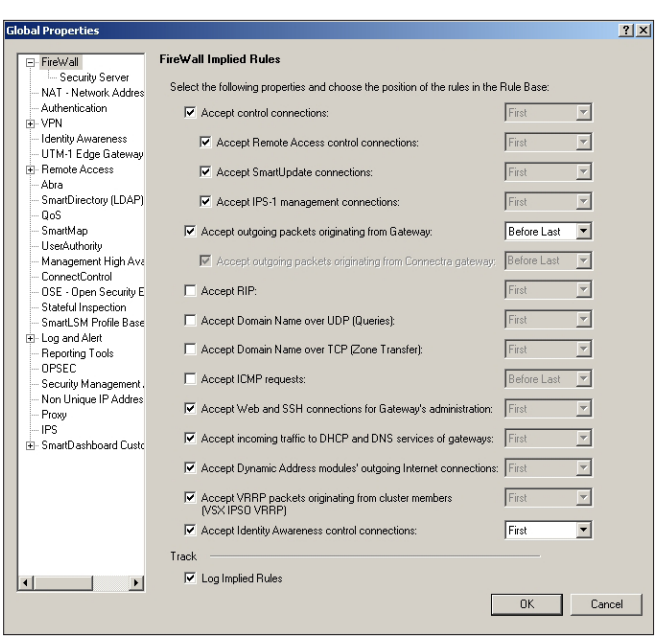


Abbildung 10. *xxxxxxxxx*

terlegen von unterschiedlichen Farben für Objekte, der Benennung von Regeln und dem Hinterlegen von Kommentaren, erhält der Security-Administrator gute Hilfsmittel an die Hand, die Ihm helfen können, den Überblick über das Firewall-Regelwerk nicht vollends zu verlieren.

Übersicht

Der nachfolgende Artikel geht auf die Konfiguration eines Check Point Security Gateway, mit zentralem Management, auf der aktuellen Version R75 ein. Es wird gezeigt wie mit Hilfe des SmartDashboard ein Regelwerk zum Schutz eines (kleinen) Netzwerkes vor unerlaubten Zugriffen, mit zwei DMZ-Bereichen und des LANs (Abbildung1) konfiguriert werden kann. Das Ziel ist es hierbei, dass die Regeln für den jeweiligen Bereich unter eigenen Sektionen zusammengefasst werden, sämtlicher Traffic der über die Firewall läuft, sei es nun ein- oder ausgehend, explizit freigeben werden muss, damit nur die wirklichen benötigen Dienste erreichbar sind und jeder sonstige Traffic durch die Firewall geblockt wird. Bei der aktuellen Konfiguration nicht berücksichtigt werden weitere Sicherheitsmechanismen, wie beispielsweise Proxy/Content Filter, VPN-Zugänge, Mail-Gateway, da es den Rahmen des Artikels sprengen würde.

Installation

Die Installation eines Security Management und eines Security Gateway unterscheiden sich, bis zu der Auswahl der zu installierenden Produkte nicht voneinander. Nach dem Download des entsprechenden Image von der Check Point Website, in dem vorliegenden Fall „*Check_Point_R75.Splat.iso*“, dem Brennen auf eine DVD, startet nach dem Bootvorgang die Grundinstallation des auf Secure Platform basierenden Systems. Diese beinhaltet neben dem Festlegen des Keyboard Layouts, die Konfiguration eines Netzwerkinterface und des https-Ports für den Zugriff auf die WebGUI (Abbildung2). Nach einer letzten Bestätigung, wird im nächsten Installationsschritt die Festplatte formatiert und das Grundsystem installiert. Nach erfolgreicher Installation und einem Reboot steht das Webinterface per https, mit der konfigurierten IP und dem angegebenen Port, zur Verfügung.

Nach dem ersten erfolgreichen Login mit den Anmeldedaten „*Benutzer: admin;Passwort: admin*“, muss aus Sicherheitsgründen zunächst das Default-Password neu gesetzt werden (Abbildung3). Bei den nun folgenden Konfigurationsschritten werden übliche Systemeinstellungen, wie z. b. NTP, DNS, weitere IP-Adressen, Routing usw. abgefragt. Letztlich steht unter dem Punkt „*First Time Configuration Wizard-Products*“ (Abbildung4) die Entscheidung an, welche Aufgabe das System in Zukunft übernehmen soll, Security Gateway oder Check Point Management-Server. Wählt man hier nun den Punkt Security Management, stehen vor der endgültigen Fertigstellung noch die Konfiguration der „*Security Management GUI Clients*“ und der „*Security Management Administrators*“ an. Die Konfiguration eines Security Gateway unterscheidet sich insofern, da man hier nicht GUI-Clients bzw. Administratoren, sondern einen Activation Key für die Secure Internal Communication (kurz SIC) angeben muss, welcher Voraussetzung für die Kommunikation zwischen Security Gateway und Security Management ist.

Bevor man endgültig mit der Konfiguration per SmartDashboard beginnt, sollten noch die restlichen IPs (falls nicht schon bei der Installation geschehen) auf dem Gateway, per „*WebGUI -> Network -> Connections*“ konfiguriert werden (Abbildung5). Sind nun alle diese Schritte erfolgreich durchgeführt worden, wird im nächsten Schritt das SmartDashboard installiert und das Security Gateway in das Management aufgenommen.

SmartDashboard

Um sich nun mit dem Management zu verbinden muss das SmartDashboard für die jeweilige Version des Manage-

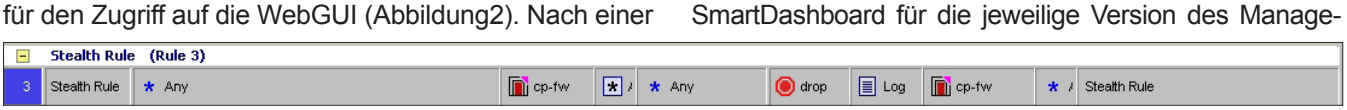


Abbildung 11. *xxxxxxxxx*

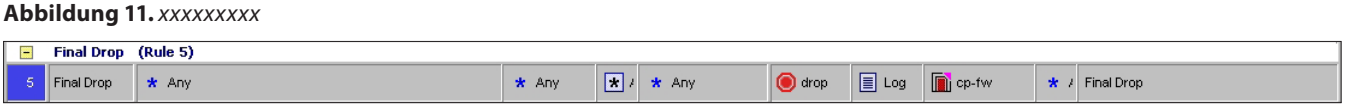


Abbildung 12. *xxxxxxxxx*

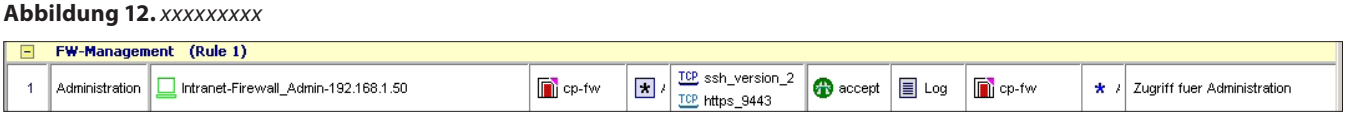


Abbildung 13. *xxxxxxxxx*

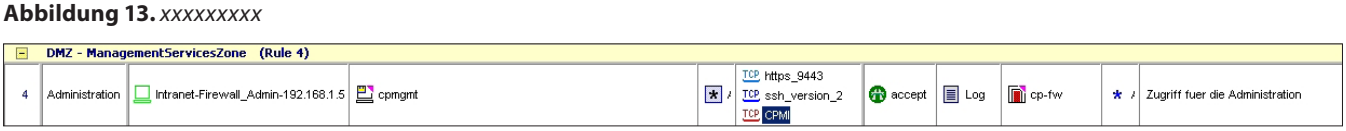


Abbildung 14. *xxxxxxxxx*

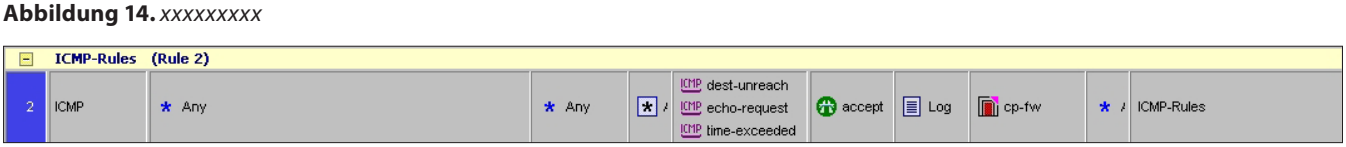


Abbildung 15. *xxxxxxxxx*

ment Server (hier R75) heruntergeladen und installiert werden. Dies kann entweder über die WebGUI *„Product Configuration -> Download SmartConsole Applications“* oder über die Check Point Website getan werden. Die Installation des SmartDashboard sollte niemanden vor eine allzu große Herausforderung stellen, daher wird hier nicht näher darauf eingegangen. Anzumerken wäre an dieser Stelle noch, dass es durchaus möglich ist mit einem Management-Server auf Version R75, ein Security Gateway in früherer Version (R71, R70, R65) zu administrieren, umgekehrt ist aber ein Security Gateway auf der Version R75 nicht von einem Management in einer älteren Version zu administrieren. Mit dem ersten Login per SmartDashboard wird ein Fingerprint (Abbildung6) abgefragt. Um die Korrektheit zu überprüfen, kann man den Fingerprint mit dem auf dem Management hinterlegten „*WebGUI -> Product Configuration -> Certificate Authority*“ vergleichen.

Einbinden in das Security-Management

Nach dem erfolgreichen Login per SmartDashboard fügt man auf der linken Seite über „*Network Objects -> Check Point -> Rechte Maustaste -> Security Gateway/Management*“ das Gateway ins Management ein. Dazu trägt man Namen und IP-Adresse des Gateway ein und unter dem Punkt „*Secure Internal Communication -> Communication (Certificate State steht zunächst auf: Uninitialized)“* den bei der Installation vergebenen Activation Key. Wenn hier alles funktioniert hat, steht der Certificate State nun auf „Trust established“ (Abbildung7) und es werden gleichzeitig die zuvor konfigurierten IPs in die Topology eingetragen (Abbildung8). In der Topology gelangt man per Doppelklick auf die einzelnen Interfaces in das sogenannte *Interface Properties*. Hier wird das Interface einem *Network Type* (Internal, External, DMZ) zugeordnet und das Anti-Spoofing konfiguriert (Abbildung9). Bei einem „Internal-Interface“ hat man die Möglichkeit zwischen *Network defined by the interface IP and Net Mask* oder *Specific* zu wählen. Wenn *Specific* ausgewählt wird, kann dort ein Netzwerk-Objekt oder gar ein Gruppen-Objekt hinterlegt werden, welches dann die Topology für das Interface bildet.

Regelwerk

Das Regelwerk auf einem Check Point Security Gateway wird von oben nach unten verarbeitet, d.h. genauer werden zuerst die sogenannten *Implied Rules* verarbeitet, welche man sich mit „*View -> Implied Rules“* im Re-

INTERNET (Rule 5)										
5	Internet	Internal-Network-192.168.1.0_24	Untrusted	*	TCP http TCP https TCP ftp TCP smtp TCP pop-3	accept	Log	cp-fw	*	Internet-Zugriff

Abbildung 16. *xxxxxxxxx*

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
General NAT Rules (Rule 1)								
1	Internal-Network-192.168.1.0_24	* Any	* Any	cp-fw (H)	= Original	= Original	cp-fw	Hide-Nat für Internet-Zugriff

Abbildung 17. *xxxxxxxxx*

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
General NAT Rules (Rules 1-2)								
1	Firewall-connectedNetworks	Firewall-connectedNetworks	* Any	= Original	= Original	= Original	cp-fw	Kein NAT zwischen den angeschlossenen Netzen
2	Internal-Network-192.168.1.0_24	* Any	* Any	cp-fw (H)	= Original	= Original	cp-fw	Hide-Nat für Internet-Zugriff

Abbildung 18. *xxxxxxxxx*

DMZ - InternetServicesZone (Rules 6-9)										
6	FTP-Server	UntrustedZoneNetworks	InternetServicesZone-ftp.example.com-212.89.2.1	*	TCP ftp	accept	Log	cp-fw	*	Zugriff auf FTP-Server
7	Webserver	UntrustedZoneNetworks	InternetServicesZone-webserver.example.com-212.89.2.2	*	TCP http TCP https	accept	Log	cp-fw	*	Zugriff auf Webserver

Abbildung 19. *xxxxxxxxx*

DMZ - InternetServicesZone (Rules 6-9)										
6	FTP-Server	UntrustedZoneNetworks	InternetServicesZone-ftp.example.com-212.89.2.1	*	TCP ftp	accept	Log	cp-fw	*	Zugriff auf FTP-Server
7	Webserver	UntrustedZoneNetworks	InternetServicesZone-webserver.example.com-212.89.2.2	*	TCP http TCP https	accept	Log	cp-fw	*	Zugriff auf Webserver
8	FTP-Server	Internal-Network-192.168.1.0_24	InternetServicesZone-ftp.example.com-212.89.2.1	*	TCP ftp	accept	Log	cp-fw	*	Zugriff auf FTP-Server
9	Webserver	Internal-Network-192.168.1.0_24	InternetServicesZone-webserver.example.com-212.89.2.2	*	TCP http TCP https	accept	Log	cp-fw	*	Zugriff auf Webserver

Abbildung 20. *xxxxxxxxx*

gelwerk anzeigen lassen kann. In den Implied Rules sind unter anderem *Control Connections für Remote Access, IPS-1* und *SmartUpdate* definiert, welche im Regelwerk nicht direkt zu bearbeiten sind. Unter dem Menüpunkt „*Policy -> Global Properties -> FireWall -> FireWall Implied Rules*“ (Abbildung10) können diese aktiviert, deaktiviert bzw. Logging und Reihenfolge eingestellt werden.

Für die Reihenfolge stehen folgende Möglichkeiten zur Auswahl: First, Before Last und Last. Wird eine Implied Rule als *First* definiert, kann diese nicht mehr von einer selbst erstellten Regel (Explicit Rule) überschrieben werden, da sie damit in der Verarbeitung des Regelwerks immer an erster Stelle steht. Bei der Definition *Before Last* wird die Regel, wie der Namen vermuten lässt, vor und mit der letzten Möglichkeit *Last* nach der letzten Regel (Implicit Drop Rule) verarbeitet, welche sämtliche Pakete verwirft und dazu führt, dass eine mit *Last* definierte Implied Rule keine Relevanz hat. Im Endeffekt bedeutet dies, wenn ein Paket bei der Verarbeitung auf eine Regel zutrifft, wird diese Regel angewandt, danach aber keine weitere, d.h. nur die erste zutreffende Regel wird auch tatsächlich ausgeführt.

Stealth Rule

Im ersten Schritt wird in dem Regelwerk unter dem Reiter „Firewall“ zunächst die Sektion “Stealth Rule“ über die Menüpunkte „*Rules -> Add Section Title -> Below/ Above*“ erstellt. Unter dieser folgt dann die erste selbst erstellte Firewall-Regel, welche sämtliche Anfragen an die Firewall selbst verbietet und dieser damit einen ge-

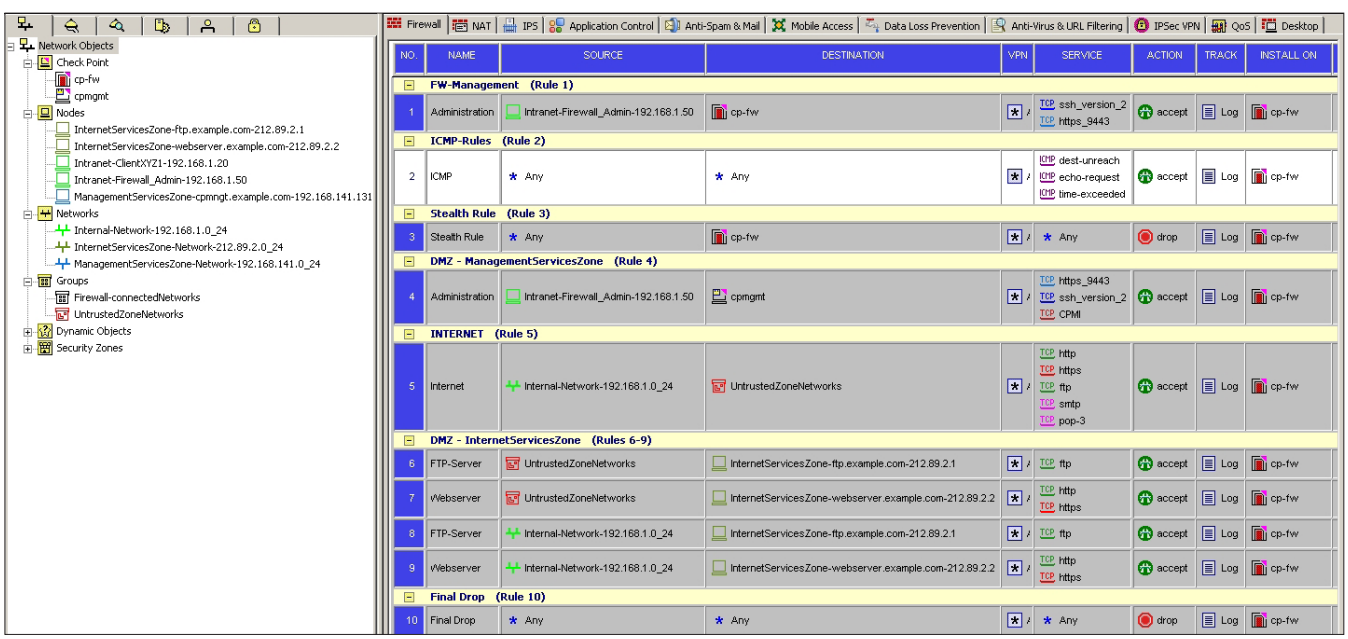


Abbildung 21. *xxxxxxxxx*

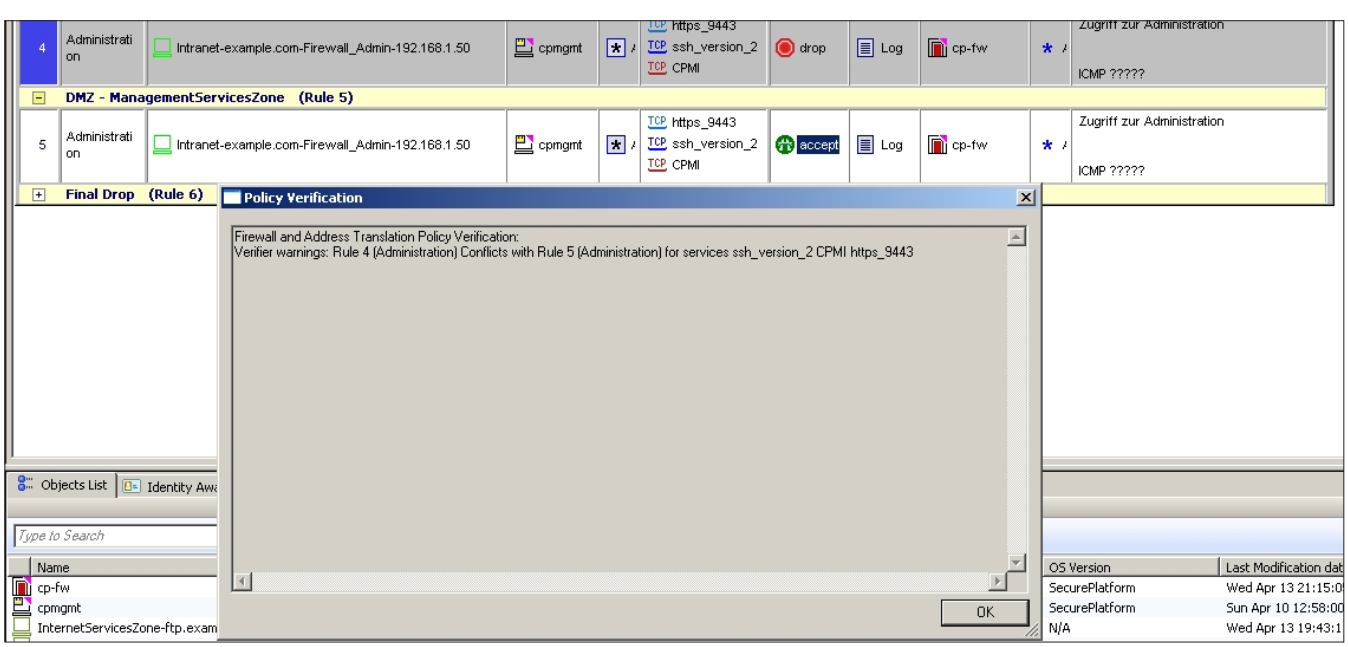


Abbildung 22. *xxxxxxxxx*

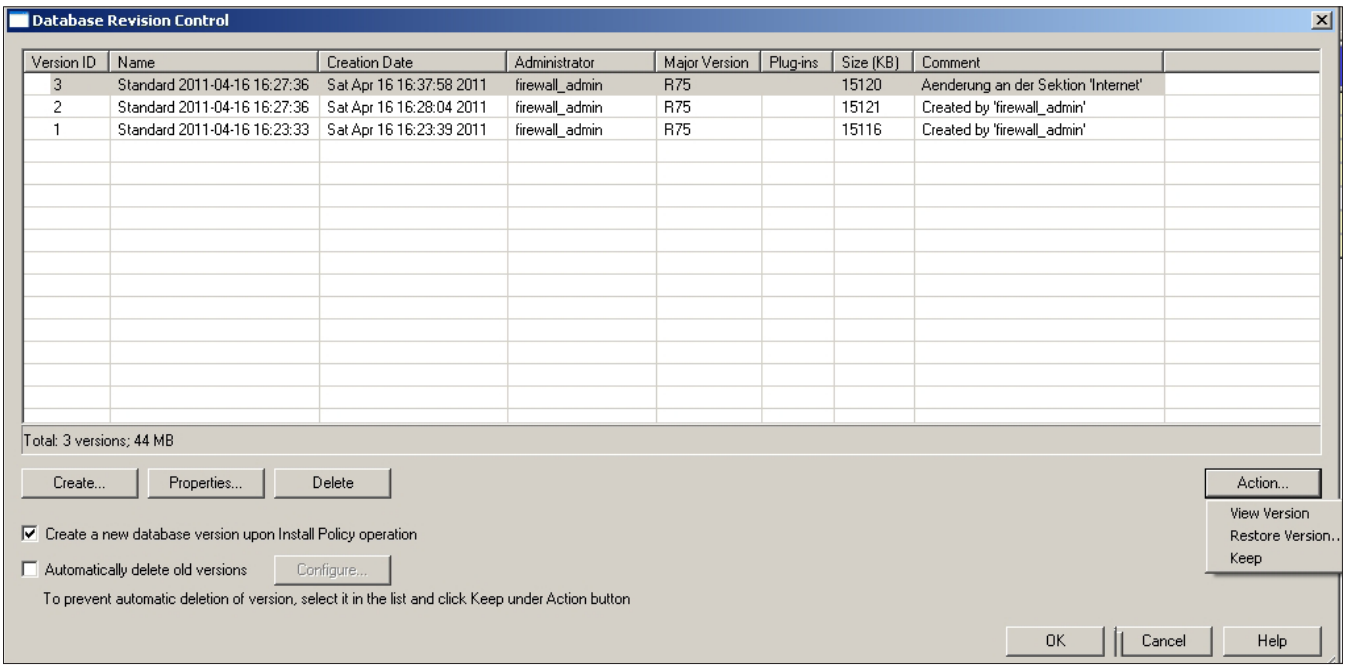


Abbildung 23. *xxxxxxxxx*

wissen Schutz bieten soll. *„Source->any, Destination->cp-fw, Service->any, Action->Drop"* (Abbildung11).

Final Drop

Die zweite Sektion bzw. Regel trägt den Namen „Final-Drop", und verwirft alle Pakete, die das Regelwerk komplett durchlaufen haben und für die es am Ende keine Übereinstimmung in dem Regelwerk gab. Diese Regel fügen wir am Ende (also aktuell als Nr. 2, hinter die „Stealth Rule) ein. *„Source->any, Destination->any, Service->any, Action->Drop"* (Abbildung12). Das Check Point Security Gateway besitzt zwar, durch die bereits erwähnten Implied Rules, eine derartige „Final-Drop"-Regel (Implicit Drop Rule), allerdings werden für diese **keine** Logeinträge erstellt, was aber für das Erkennen von möglichen Angriffen und/oder für das Debugging ungemein wichtig ist.

Security Management

Da durch die „Stealth Rule" sämtliche Anfragen an das Gateway selbst verworfen werden, muss als nächstes dafür gesorgt werden, dass die Möglichkeit der Administration per https_9443 und SSH besteht. Dazu wird die nächste Sektion „Firewall-Management" **über** der Sektion „Stealth-Rule" mit *„Rechte Maustaste auf die Sektion „Stealth Rule" -> Add Section Title -> Above*" erstellt. Unter dieser neuen Sektion wiederum wird eine Regel erstellt, die den Zugriff von der IP 192.168.1.50 für die Administration des Security Gateway erlaubt.*„Source->192.168.1.50, Destination->cp-fw, Service->https_9443/ssh_version2, Action->Accept"* (Abbildung13).

Zwingend notwendig für die Administration ist natürlich ebenfalls der Zugriff auf das zentrale Management, welches in einer eigenen DMZ steht. Um diesen Zugriff sicherzustellen, wird in die, unter der Stealth-Rule Sektion, liegenden Sektion mit der Bezeichnung „DMZ – ManagementServicesZone" eine Regel angelegt, welche den Zugriff von 192.168.1.51 auf das Management für die Ports https_9443, ssh_version2 und CPMI_18190 (Check Point Management Interface) erlaubt. *„Source->192.168.1.51, Destination->cpmgmt, Service->https_9443,ssh_version2,CPMI, Action->Accept*" (Abbildung14)

ICMP

Als nächstes wenden wir uns dem Thema ICMP zu. Da weder ein allgemeines Verbieten noch ein allgemeines Freigeben von ICMP sehr sinnvoll ist, wird die nächste Sektion „ICMP-Rules" **über** der Sektion „Stealth-Rule" erstellt. Hier wird nun eine Regel angelegt, welche „ICMP Destination Unreachable, ICMP Time Exceeded und ICMP Echo Request" für alle (any) freischaltet. *„Source->any, Destination->any, Service->dest-unreach/echo-request/time-exceeded, Action->Accept"* (Abbildung15).

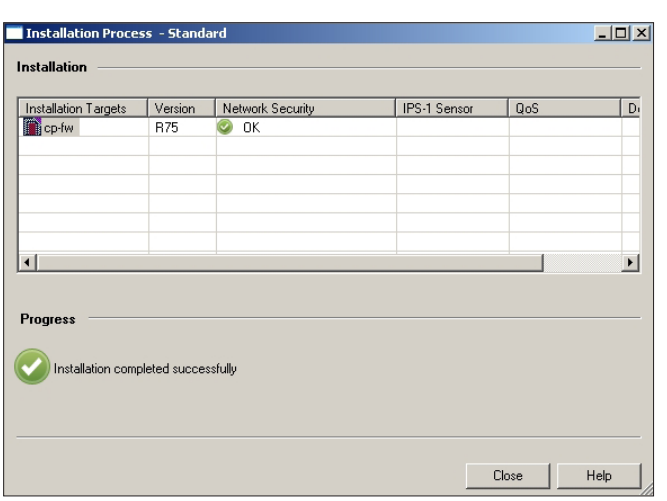
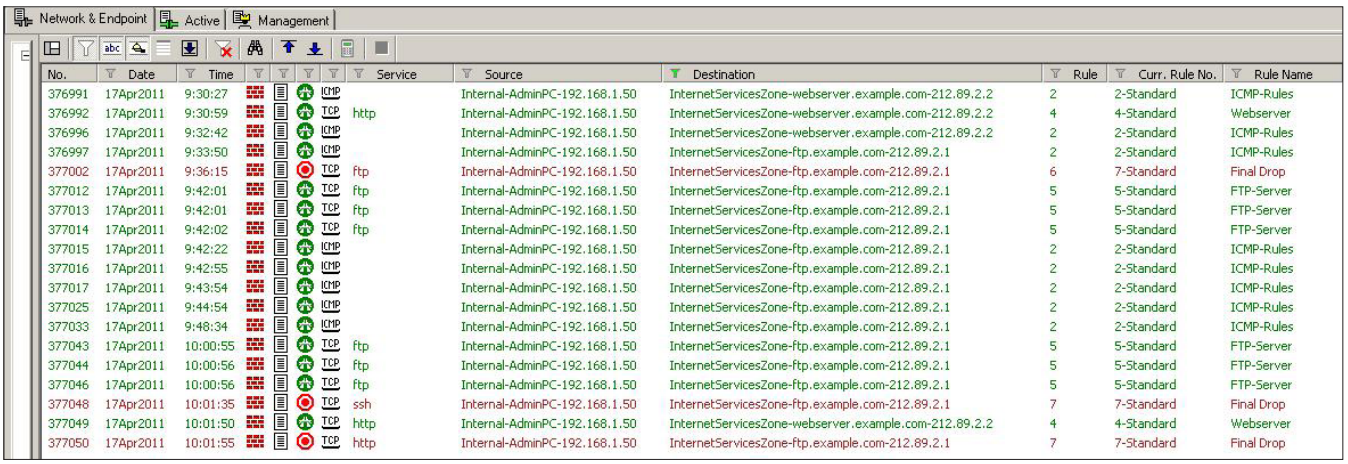


Abbildung 24. *xxxxxxxxx*



No.	Date	Time	Service	Source	Destination	Rule	Curr. Rule No.	Rule Name
376991	17Apr2011	9:30:27		Internal-AdminPC-192.168.1.50	InternetServicesZone-webserver.example.com-212.89.2.2	2	2-Standard	ICMP-Rules
376992	17Apr2011	9:30:59	http	Internal-AdminPC-192.168.1.50	InternetServicesZone-webserver.example.com-212.89.2.2	4	4-Standard	Webserver
376996	17Apr2011	9:32:42		Internal-AdminPC-192.168.1.50	InternetServicesZone-webserver.example.com-212.89.2.2	2	2-Standard	ICMP-Rules
376997	17Apr2011	9:33:50		Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	2	2-Standard	ICMP-Rules
377002	17Apr2011	9:36:15	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	6	7-Standard	Final Drop
377012	17Apr2011	9:42:01	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	5	5-Standard	FTP-Server
377013	17Apr2011	9:42:01	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	5	5-Standard	FTP-Server
377014	17Apr2011	9:42:02	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	5	5-Standard	FTP-Server
377015	17Apr2011	9:42:22		Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	2	2-Standard	ICMP-Rules
377016	17Apr2011	9:42:55		Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	2	2-Standard	ICMP-Rules
377017	17Apr2011	9:43:54		Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	2	2-Standard	ICMP-Rules
377025	17Apr2011	9:44:54		Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	2	2-Standard	ICMP-Rules
377033	17Apr2011	9:48:34		Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	2	2-Standard	ICMP-Rules
377043	17Apr2011	10:00:55	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	5	5-Standard	FTP-Server
377044	17Apr2011	10:00:56	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	5	5-Standard	FTP-Server
377046	17Apr2011	10:00:56	ftp	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	5	5-Standard	FTP-Server
377048	17Apr2011	10:01:35	ssh	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	7	7-Standard	Final Drop
377049	17Apr2011	10:01:50	http	Internal-AdminPC-192.168.1.50	InternetServicesZone-webserver.example.com-212.89.2.2	4	4-Standard	Webserver
377050	17Apr2011	10:01:55	http	Internal-AdminPC-192.168.1.50	InternetServicesZone-ftp.example.com-212.89.2.1	7	7-Standard	Final Drop

Abbildung 25. *xxxxxxxxx*

Internet-Zugriff

Erlaubt für den Zugriff vom internen Netz in das Internet werden nur die Dienste http, https, ftp, smtp und pop3. Für diesen Zugriff wird auch erstmals das Objekt „UntrustedZone“ verwendet. Dieses Gruppen-Objekt „enthält“ alle Netze (any) mit Ausnahme, der in dem Gruppen-Objekt „Firewall-connectedNetworks“ hinterlegten Netze, in dem vorliegenden Fall also 192.168.1.0/24, 192.168.141.0/24, 212.89.2.0/24. *„Source->Internal-Network-192.168.1.0_24, Destination->UntrustedZone, Service->http,https,ftp.smtp,pop3, Action->Accept“* (Abbildung16). Damit nun das interne Netz auf das Internet zugreifen kann muss für das Netz ebenfalls eine NAT eingerichtet werden. Auf dem Check Point Security Gateway wird hierzu ein „Hide-Nat“ (bei Hide-Nat wird eine Port Address Translation durchgeführt) konfiguriert. *„Original Packet (Source->192.168.1.0/24, Destination->any, Service->any)/Translated Packet (Source->cp-fw(H), Destination->Original, Service->Original)”* (Abbildung17). Durch die zuvor konfigurierten Regeln, ist somit der Zugriff per http, https, ftp, smtp und pop3 ins Internet erlaubt und alle weiteren Zugriffe werden von dem Security Gateway geblockt und ins Log geschrieben.

Zu beachten ist bei der NAT-Konfiguration aber noch, dass durch das Setzen von „Destination->any“ unter „Original Packet“, auch für den Zugriff in Richtung DMZ-Bereiche ein NAT gemacht wird, was allerdings nicht gewollt ist. Also muss **über** der Hide-Nat-Regel zusätzlich eine weitere Regel erstellt werden, die dafür sorgt, dass zwischen den direkt verbunden Netzen **kein** NAT durchgeführt wird. *„Original Packet (Source->Firewall-connectedNetworks, Destination->Firewall-connectedNetworks, Service->any)/Translated Packet (Source->Original, Destination->Original, Service->Original)* (Abbildung18)

Web- und FTP-Server

Die letzten Regeln betreffen die Zugriffe auf Web- und FTP-Server, einmal aus dem Internet und zum anderen aus dem LAN. Hierzu werden unter der Sektion „DMZ – InternetServicesZone“, zwei Regeln erstellt. In der ersten Regel wird das Objekt „UntrustedZone“, diesmal allerdings als Source eingetragen und als Ziel der FTP-Server. *„Source->UntrustedZone, Destination->212.89.2.1, Service->ftp, Action->Accept“. D*ie zweite Regel bekommt als Ziel den Webserver mit den entsprechenden Ports http und https. *„Source->UntrustedZone, Destination->212.89.2.2, Service->http/https, Action->Accept“* (Abbildung19). Mit diesen Regeln ist sichergestellt, dass Web- und FTP-Server aus dem Internet erreichbar sind. Zugriffe aus dem internen Netz werden allerdings nach wie vor von der Firewall in der „Final Drop“-Regel geblockt, da mit den ersten beiden Regeln nur der Zugriff von nicht direkt verbunden Netzen (UntrustedZone) erlaubt wurde. Um dies zu ändern, werden die eben erstellten Regeln einfach mit *„Rechte Maustaste -> Copy“* kopiert und unter die ersten beiden Regeln mit *„Rechte Maustaste -> Paste -> Below“* eingefügt. Zuletzt wird dann einfach die Source „UntrustedZone“ gegen „Internal-Network-192.168.1.0_24„ ausgetauscht (Abbildung20). Somit ist nun ebenfalls sichergestellt, dass aus dem internen Netz auf Web- und FTP-Server zugegriffen werden kann.

Damit sieht das gesamte Regelwerk inklusive der erstellen Objekte wie in Abbildung21 dargestellt aus.

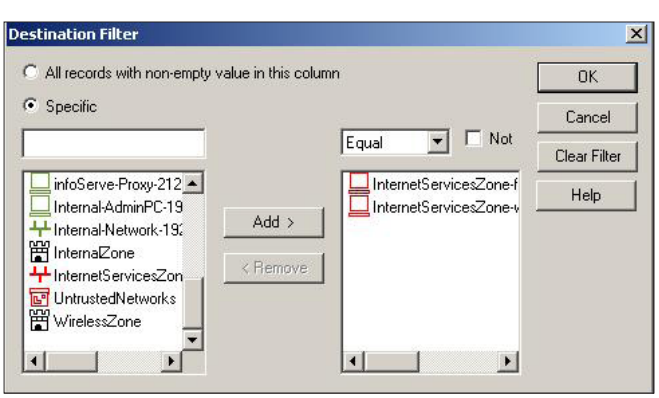


Abbildung 26. *xxxxxxxxx*

Policy

Alle oben, per SmartDashboard, angelegten Objekte und Regeln existieren bisher ausschließlich auf dem Management, d.h. tatsächlich kennt das Security Gateway diese Regeln und Objekte aktuell noch gar nicht und wendet diese damit natürlich auch noch nicht an. Um das erstellte Firewall-Regelwerk nun auch auf dem Security Gateway zu aktivieren, muss man diese vom Management auf das Gateway „pushen".

Policy Verify

Vor der eigentlichen Installation besteht noch die Möglichkeit der Überprüfung des Regelwerks per *„Policy -> Verify*". Wird hier z. b. eine Überschneidung in den Regeln festgestellt, gibt es eine Warnung, welche Regeln und Dienste von der möglichen Fehlkonfiguration betroffen sind (Abbildung22). In dem gezeigten Beispiel wurde die an für sich gleiche Regel zweimal konfiguriert, mit dem Unterschied, dass in Regel 4 der Zugriff geblockt und in Regel 5 erlaubt würde. Diese Warnung würde allerdings ebenfalls erscheinen wenn man direkt ein Install Policy ausgeführt hätte.

Revision Control

Des Weiteren kann vor dem pushen der Regeln eine Revisions-Kontrolle per „*File -> Database Revision Control*" durchgeführt werden. Hier besteht die Möglichkeit eine Kopie der aktuellen Regeln und Objekte auf dem Management zu speichern bzw. eine frühere Version des Regelwerks zu betrachten und gegebenenfalls auch wiederherzustellen (Abbildung22). Die Revision Control kann ebenfalls direkt vor dem pushen erstellt werden und muss nicht jedes Mal manuell ausgeführt werden.

Policy Install

Um das pushen der Regeln nun durchzuführen, wählt man im SmartDasboard „*Policy -> Install*" aus. In dem nun erscheinenden Fenster stehen gegebenenfalls eine oder mehrere Gateways, auf welche das aktuelle Regelwerk gepusht werden kann und die „Revision Control" zur Auswahl. Mit einem Klick auf OK, startet die Übertragung der Regeln auf das Security Gateway und wird mit der Meldung „*Installation completed successfully*" (Abbildung24) bei erfolgreicher Übertragung abgeschlossen.

Im Internet

- *http://www.checkpoint.com* – die offizielle Check Point Website
- *http://downloads.checkpoint.com/dc/download.htm?ID=11550* – R75 Documentation Package
- *http://www.checkpoint.com/campaigns/nss-next-gen-firewall/index.html#* - NSS Labs Next Generation Firewall Test Report for Check Point

SmartTracker

Um nun die in das Log geschriebenen Einträge nachvollziehen zu können, steht das Tool „SmartTracker" zur Verfügung. Hier kann man alle im Regelwerk mit „*Track->Log*" versehenen Regeln, egal ob Accept oder Drop, verfolgen (Abbildung25). Wir zu erkennen, sieht man zum einen die üblichen Informationen, wie Port, Ziel- und Quell-IP, aber auch welche Regel den Zugriff erlaubt bzw. geblockt hat. Des Weiteren besteht die Möglichkeit, in den angezeigten Reitern eigene Filter zu hinterlegen (Rechte Maustaste -> Edit Filter), so dass man nur die wirklich gewünschten Informationen aus dem Log ziehen kann. (Abbildung26)

Fazit

Firewalls werden natürlich auch in Zukunft einen wichtigen Platz in der Netzwerk-Infrastruktur einnehmen und trotz aller möglichen Vorteile oder Vereinfachungen eines Produktes, gibt es immer noch genügend Fallen in die ein Security-Administrator tappen kann. Beispielsweise kann in ein Gruppen-Objekt schnell der falsche Host oder das falsche Netzwerk eingetragen werden und damit ungewollte Zugriffe auf Systeme frei geschaltet werden.

Auch wird die Komplexität weiterhin steigen und bereits heute kann eine („reine") Firewall, viele Anforderungen an die „Sicherheit" gestellt werden nicht mehr alleine erfüllen, was unweigerlich dazu führt das weitere Security-Komponenten integriert werden müssen. Dies wiederum stellt die Administratoren vor die Aufgabe, sich mit unterschiedlichen Methoden und verschiedenen Konfigurationsansätzen zu beschäftigen. Auch in diesem Punkt schafft Check Point mit Hilfe seines (zentralen) Managements, in dem die Software-Blades administriert werden können, gute Abhilfe. Darüber hinaus bietet das Management noch eine Menge weiterer kleiner Hilfen, die einem Administrator das Leben durchaus erleichtern können, wie z. b. die Möglichkeit mit „Where Used ..." auf ein Objekt um zu sehen in welchen Regeln bzw. Policies dieses Objekt verwendet wird. Nicht vergessen sollte man aber auch, dass im Umfeld von Check Point, das meiste einen stolzen Preis hat und natürlich auch immer eine entsprechende Lizenz gekauft werden muss. Doch trotz aller Vor- und Nachteile von den jeweiligen Produkten, bleiben am Ende die (Security)-Administratoren die wohl wichtigste „Komponente" und werden weiterhin verstärkt in der Pflicht sein, sich Gewissenhaft an Vorgaben zu halten und über zu konfigurierende Zugriffe genau nachzudenken, um es am Ende einem Angreifer nicht allzu leicht zu machen.

STEFAN SCHURTZ

Der Autor arbeitet bei einem saarländischen ISP im Bereich Netzwerk-Sicherheit und beschäftigt sich auch privat mit dieser Thematik

Kontakt mit dem Autor: sschurtz@t-online.de