Check Point NGX – das ist neu

von Dr. Matthias Leu, Geschäftsführer der Aerasec GmbH und Autor der im C&L-Verlag erschienenen Bücher zur Check-Point-Firewall

Besonders in großen Unternehmen ist die bereits seit über zehn Jahren verfügbare FireWall-1 von Check Point weit verbreitet. Die Neuauflage NGX zeichnet sich durch viel Detailarbeit im GUI, aber auch unter der Motorhaube aus, wodurch sich die Ergonomie dieser Firewall zur zentralen Verwaltung von Schutzmechanismen weiter verbessert hat.

Schon seit langer Zeit ist die Check Point FireWall-1 dreigeteilt. Unterschieden wird zwischen der eigentlichen Firewall, die auf einem Gateway installiert ist, dem zentralen Management (SmartCenter) und der SmartConsole, das GUI als Schnittstelle zum Administrator.

Durch diesen Ansatz ist eine gute Skalierbarkeit gewährleistet. Vom SmartCenter aus lassen sich (zumindest bei der Enterprise-Version) beliebig viele Firewalls verwalten, die auch als Cluster für Hochverfügbarkeit beziehungsweise Load Sharing betrieben werden können. Speziell im Bereich Cluster wurde bei NGX die Verwaltung der jeweiligen Netzwerk-Interfaces deutlich verbessert.

Neben einem zentralen Logging und Überwachung des Zustands der einzelnen Komponenten erfolgt vom SmartCenter aus die Konfiguration und Installation der jeweiligen Regelsätze.

Wie bei der Vorgängerversion auch, ist die Sicherheit der internen Kommunikation durch den Einsatz einer Certificate Authority (CA) auf dem SmartCenter gesichert. Die Authentisierung erfolgt über von dieser CA ausgestellte Zertifikate und die Verschlüsselung selbst mit SSL. Als Nebeneffekt lassen sich dann auch Zertifikate ohne großen Aufwand für die Authentisierung innerhalb von VPN für Administratoren und Benutzer einsetzen.

Verbindungen erlauben und verbieten

Wie jede gängige Firewall arbeitet auch NGX als eine Art Pförtner, um vertrauenswürdige Netzwerke und Server gegenüber Angriffen zu schützen. Vorbei sind die Zeiten, in denen Angreifer lediglich versuchten, bestimmte Ports auf den potentiellen Zielen zu erreichen. Fast alle Unternehmen setzen inzwischen Firewalls ein, so daß ein unkontrollierter Zugriff aus dem Internet nicht mehr möglich ist.

Heutige Angriffe erfolgen nicht mehr, indem jemand mit Telnet versucht, in einen Server einzubrechen. Dieser Port ist sehr wahrscheinlich durch eine Firewall gesperrt. Vielmehr erfolgen Angriffe heute über die bekannten (und gewollten) Löcher in einer Firewall, denn der Webserver muß ebenso wie der Mailserver oder Nameserver aus dem Internet erreichbar sein. Insbesondere Webserver stellen oft ein gutes Ziel dar. Der Server ist öffentlich erreichbar und wenn beispielsweise die Indexseite ausgetauscht worden ist, sieht der

Angreifer auch gleich die Früchte seiner Arbeit. Insofern erfolgen heutige Angriffe über die Applikationsebene, also mit scheinbar normalen Verbindungen.
Nicht jeder Webserver ist heute gegenüber den gängigen Angriffen auf der Applikationsebene wie beispielsweise Directory Transversal, Cross Site Scripting oder SQL Injection immun. In NGX ist neben der bisher bekannten Application Intelligence auch die Web Intelligence enthalten. Hier erfolgt nicht nur eine genaue Kontrolle der Verbindung bezüglich ihrer Konformität zu den geltenden RFCs, sondern auch eine paketübergreifende Mustererkennung im Kernel, so daß bereits auf dieser Ebene viele Angriffe erkannt und verhindert werden. Damit sind einerseits die Vorteile der Stateful Inspection, andererseits in gewisser Weise auch die von Application Level Gateways gegeben.

Weitere zentral verwaltete Komponenten

Neben dem Einsatz einer Firewall sind weitere Komponenten zur Umsetzung eines Sicherheitskonzeptes notwendig. Daher unterstützt NGX unter anderem NAT, VPN und die zentrale Verwaltung weiterer Produkte von Check Point. Neben den bekannten Site-to-Site-VPN, die bei NGX auf eine sehr einfache Art und Weise konfiguriert werden, sind heutzutage Client-Server-VPNs wichtig. Neben dem bereits seit längerem verfügbaren VPN-Client SecureClient, der unter anderem eine zentral verwaltete Personal Firewall umfaßt, ist auch das Thema SSL-VPN jetzt in NGX integriert. Um auch andere Protokolle über HTTPS tunneln zu können, wird auf dem Client eine Software installiert. Der Benutzer verbindet sich dann optional mit der Check Point Connectra, einem Webportal, das ihm nach seiner Authentisierung seine Ressourcen anzeigt und zur Verfügung stellt. Daneben ist auch die Sicherheit im internen Netzwerk wichtig. Check Point InterSpect arbeitet als eine Art Intrusion-Prevention-System, das auch die Option bietet, verdächtige Clients in Quarantäne zu verbannen. Die Verwaltung, das Logging und Monitoring dieser Geräte erfolgt bei NGX jetzt zentral.

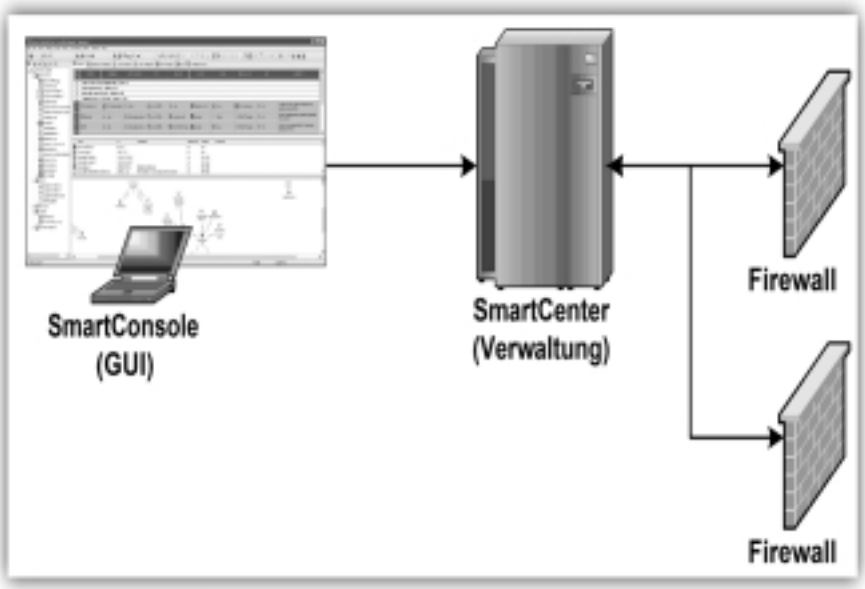

Bild 1: Die drei Teile von Check Point

Stark vereinfacht wurde mit NGX auch die Einbindung und zentrale Verwaltung der kleinen Appliances (VPN-1Edge), mit denen Außenstellen über VPN an die Zentrale angebunden und zentral Regeln für diese Systeme vorgegeben werden können.

Verwaltung der Systeme

Administratoren, die sich gut mit beispielsweise Sun Solaris oder Microsoft Windows Server auskennen, können NGX auf ihrem favorisierten Betriebssystem installieren. Die Tendenz geht aber immer mehr in Richtung Appliances – und da ist Nokia IPSO bereits ein Klassiker. Hier braucht der Administrator die Kommandozeile des BSD-basierten Unix überhaupt nicht mehr, sondern bedient das System komplett über seinen Browser. Ähnlich verhält es sich bei SecurePlatform, einer Linux-Distribution von Check Point, die speziell für den Einsatz derer Produkte entwickelt wurde und seit NGX auf Red Hat Enterprise Linux 3 basiert. Die mit NGX neu eingeführte Version SecurePlatform Pro unterstützt neben dynamischen Routing auch Route Based VPN. Hier wird das VPN nicht, wie bisher üblich, über Verschlüsselungsdomains, sondern über spezielle Einträge in das Routing konfiguriert. Zum Einsatz kommen dann VPN Tunnel Interfaces (VTI), die sich wie normale virtuelle Netzwerk-Interfaces verhalten. NGX bietet diese Art zur Konfiguration von VPN optional an, die Mischung mit den bisher bekannten Domain Based VPN ist möglich. Eine entsprechende Ausfallsicherheit für VPN ist in Kombination mit OSPF ebenfalls zu konfigurieren.

Fazit

Mit der Einführung von NGX hat Check Point einen weiteren Schritt zur zentralen Verwaltung unterschiedlichster Sicherheitskomponenten getan. Nur so lassen sich die heutigen komplexen Anforderungen überhaupt noch umsetzen und verwalten. Und nur wenn der Administrator den Durchblick hat, ist die Basis für eine sichere Infrastruktur und Kommunikation gelegt.
Als Nachteil muß der Administrator dann in Kauf nehmen, daß diese Sicherheitslösung Meilen vom eigentlich notwendigen KISS – keep it stupid simple – entfernt und eher sehr komplex ist. ◆