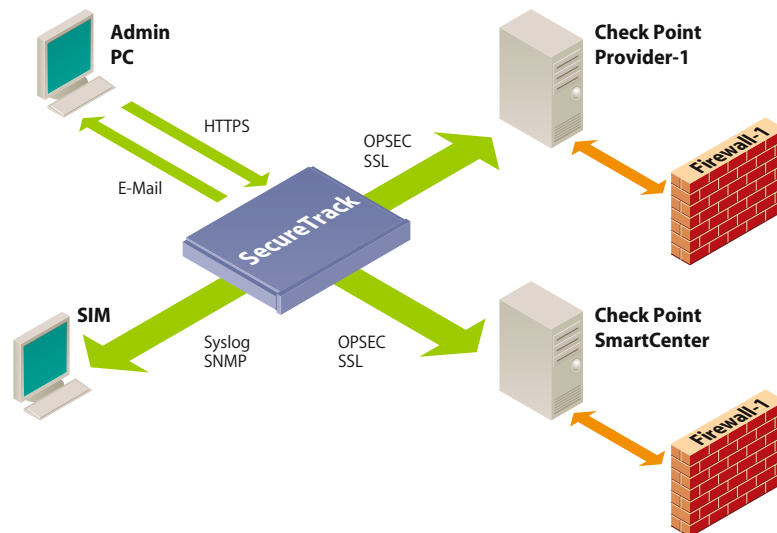


Check Point Firewalls nachvollziehbar betreiben

Die Rulebase jeder Firewall ist notorisch anfällig für Wildwuchs. Laufende Ergänzungen führen dazu, dass die definierten Regeln immer weiter anwachsen und der Überblick verloren geht. Sollen die Forderungen nach Performance, leichter Pflege und Compliance-Nachweisen erfüllt werden, ist Know-how gefragt. Bei Bacher Systems erfahren Sie, wie Sie die Einstellungen Ihrer Check Point Firewall sauber, schnell und nachvollziehbar halten.



Mit SecureTrack von Tufin wird es leichter, den Firewall-Betrieb zu optimieren und Compliance nachzuweisen.

Firewall-Regeln neigen zu unkontrolliertem Wachstum. Immer wieder kommen neue Regeln dazu, nicht

mehr benötigte Regeln werden dagegen nur selten entfernt. Die Folge ist ein Wildwuchs von Zugriffsberechtigungen, der auch bei genauerer Recherche meist nicht mehr zu durchblicken ist. Dem entgegen steht die starke Forderung, die aktuellen Einstellungen und erfolgte Änderungen an der Firewall nachvollziehen zu können. Diese Forderung hat zwei wesentliche Gründe:

- **Administration verlangt Nachvollziehbarkeit:**

Viele Firewall-Installationen werden von mehreren Administratoren betreut. Der Change Management Prozess ist zwar meistens innerhalb des Unternehmens definiert, jeder Administrator hat aber seine eigenen

bewährten Ansätze, wie und wo er Regeln einarbeitet. Dadurch wächst die Rulebase unnötig, wenn ähnliche Regeln nicht zusammengefasst, sondern einzeln eingetragen werden. Die Folge ist, dass die Performance beeinträchtigt wird und der Sicherheitslevel sinkt. Hier würde ein guter Überblick der Änderungen eine saubere Pflege möglich machen. Ein weiteres Beispiel bietet der klassische Hilferuf eines Users, dass ein Dienst plötzlich nicht mehr verfügbar ist – irgendeine Änderung in der Firewall hatte einen ungewollten Nebeneffekt. Auch in solchen Fällen ermöglicht eine gute Nachvollziehbarkeit der Änderungen eine rasche Problemlösung, ohne ungewollt neue Sicherheitslöcher zu reißen.

Einladung zum Bacher Systems Breakfast 30.9.2007

Wie Sie Ihre **Check Point Firewall-Einstellungen** nachvollziehbar machen, erfahren Sie auf dem nächsten Bacher Systems Breakfast am 13. September (9:30 bis 12:00) im Atelier Augarten. Die Teilnahme ist kostenlos, um rechtzeitige Anmeldung unter www.bacher.at/breakfast wird gebeten.



Newsletter 4/2007

Informationen für IT-Sicherheit und IT-Infrastruktur

● Compliance verlangt

Nachvollziehbarkeit:

Ein weit verbreitetes Beispiel für eine Compliance-Forderung ist der Nachweis, dass die aktuelle Firewall-Policy tatsächlich die Security-Policy des Unternehmens abbildet. Erst wenn eine gute Nachvollziehbarkeit der aktuellen Firewall-Einstellungen gegeben ist, kann dieser Nachweis leicht erbracht werden. Ähnliches gilt für gesetzliche Regulative und Industriestandards, deren Einhaltung belegt werden muss. SOX (Sarbanes-Oxley Act), Basel II (Basel Capital Accord) oder PCIDS (Payment Card Industry Data Security) sehen vor, dass bestimmte Abläufe und Prozesse aus der IT belegt werden. Ein weiterer Grund, auf gute Nachvollziehbarkeit der Firewall-Einstellungen zu achten.

Praktische Wege zur Nachvollziehbarkeit

Einstellungen und Änderungen in Check Point Firewalls lassen sich auf zwei Wegen nachvollziehbar machen. In etwas eingeschränkter Weise mit Firewall-eigenen Mitteln, wesentlich umfassender mit einem Add-On Produkt namens SecureTrack von Tufin.

● Mit Firewall-Mitteln:

Mit der so genannten Database Revision Control ist es möglich, zu jedem Zeitpunkt einen Snapshot der kompletten Database zu speichern. Geschieht dies sorgfältig nach jeder Änderung, können bei einer Fehlersuche verschiedene Versionen verg-

lichen werden. In der Rulebase selbst gibt es die Möglichkeit, jede einzelne Regel genauer zu beschreiben. Wird diese Funktion genutzt, so ist der Sinn einer Regel auch zu einem späteren Zeitpunkt noch zu verstehen. Schließlich bietet die Firewall noch die Möglichkeit, mit dem Smart-View Tracker auf das Audit Log zuzugreifen, in dem alle Änderungen an Objekten und Regeln dargestellt werden. Zusammenfassend könnte man sagen, dass die Firewall-eigenen Mittel nur bei sehr disziplinierter Administration ausreichen, um die Nachvollziehbarkeit auch langfristig sicherzustellen.

● Mit dem Add-On SecureTrack:

Mit diesem Zusatzprodukt steht eine Lösung zur Verfügung, die den operativen Betrieb von Check Point Firewalls unterstützt und damit auch die Nachvollziehbarkeit aller Einstellungen und Änderungen garantiert. Das Produkt überwacht Veränderungen, erstellt Berichte und bietet eine genaue Historiendokumentation – damit wird die Revisionsicherheit gewährleistet. Darüber hinaus ist es mit SecureTrack möglich, die Firewall-Rulebase zu optimieren und zu bereinigen. Nicht verwendete Firewall-Regeln werden entfernt und mögliche Sicherheitslücken eliminiert. Damit wird der so oft auftretende Wildwuchs in der Rulebase bereinigt, die Performance der Firewall wiederhergestellt und der Sicherheitslevel erhöht. Weitere Funktionen dienen speziell dazu, die Compliance der Firewall-Einstellungen mit

der Security-Policy und gesetzlichen Regulativen nachzuweisen.

Auf dem nächsten Bacher Systems Breakfast am 13. September erfahren Sie, wie Sie mit diesen Mitteln sowohl die Effektivität als auch die Compliance Ihrer Firewall herstellen und nachvollziehbar machen.

Trainings bei Bacher Systems

IT-Infrastruktur

Solaris 10 OE Systemadministration I

10.9. - 14.9.2007 / € 2.790,-

Solaris 10 OE Systemadministration II

17.9. - 21.9.2007 / € 2.790,-

Shell Programmierung für Systemadministratoren

10.9. - 14.9.2007 / € 2.270,-

Solaris 10 OE für erfahrene Systemadministratoren

24.9. - 28.9.2007 / € 2.790,-

Sun Cluster 3.2 Verwaltung

15.10. - 19.10.2007 / € 3.890,-

Solaris 10 ZFS Administration

22.9. - 23.9.2007 / € 1.170,-

Solaris 10 Containers

24.10. - 25.10.2007 / € 1.050,-

IT-Sicherheit

Check Point Security Administration NGX I Rev. 1.1

24.9. - 25.9.2007 / € 1.350,-

Check Point Security Administration NGX II Rev. 1.1

26.9. - 28.9.2007 / € 1.990,-

Check Point Security Administration NGX III

22.10. - 25.10.2007 / € 2.560,-

Alle Preise pro Person exkl. Mwst.

Firmenspezifische Kurse auf Anfrage.

Anmeldungen: training@bacher.at

Kursinfos: www.bacher.at/training

Package NGX I+II+III € 4.900,- statt € 5.900,-

Änderungen vorbehalten

Offenlegung gemäß § 25 Mediengesetz; Medieninhaber: Bacher Systems EDV GmbH, Clemens Holzmeister Straße 4, 1100 Wien Reg. zu FN 54202i, Handelsgericht Wien, GF: Manfred Köteles, Mehrheitsgesellschafter: Manfred Köteles, Martin Mörtinger Unternehmensgegenstand: Handel mit Computer-Soft- und Hardware IT-Beratung; Blattlinie: Verbreitung von Information für sichere IT-Infrastruktur

