Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 80 (2002)

Heft: 7-8

Artikel: Firewall Appliances als Konzept verstehen

Autor: Bilek, Bernd

DOI: https://doi.org/10.5169/seals-877219

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 07.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Plug and Protect

Firewall Appliances als Konzept verstehen

Der klassische Firewall-Begriff meint weniger ein Gerät als vielmehr ein Konzept. Innerhalb dieses Konzepts gibt es Geräte, die ebenfalls als Firewalls bezeichnet werden. Um diese Geräte geht es im Folgenden, wenn von Firewalls die Rede ist.

Firewalls bestehen häufig aus zwei oder mehr separat erworbenen Komponenten: Einem Rechner einschliesslich Betriebssystem und einer oder mehreren Software-Komponenten. Die Einrichtung eines Firewall-Rechners

BERND BILEK

beginnt mit dem Einbau mehrerer Netzwerkkarten, gefolgt von der Installation und Konfiguration des Betriebssystems, das den speziellen Erfordernissen dieser Aufgabe angepasst werden muss. So müssen alle Dienste, die zum Betrieb als Firewall nicht benötigt werden, entfernt oder deaktiviert werden. Dann kann die eigentliche Firewall-Software installiert und konfiguriert werden. Dabei müssen zuweilen Teile des Betriebssystems durch geeignetere, gehärtete Elemente ersetzt werden, zum Beispiel der Betriebssystemkern oder der IP-Stack, da das Betriebssystem Schwachstellen aufweist, die für einen Einsatz als Firewall-Rechner nicht hinnehmbar sind. Erst jetzt kann damit begonnen werden, die Filterregeln so zu definieren, dass die spezifischen Anforderungen im Unternehmen erfüllt werden. Bis hierhin sind bereits einige Arbeitsstunden vergangen. Seit einiger Zeit gibt es in vielen Bereichen der Netzwerktechnik speziell für eine bestimmte Aufgabe angepasste Geräte, die bereits alle erforderlichen Komponenten vorkonfiguriert enthalten. Sie werden als *Appliances* bezeichnet. Bei Internet-Providern weit verbreitet sind zum Beispiel Web-Server. Auch im IT-Sicherheitsbereich halten solche Geräte mittlerweile Einzug, man spricht hier von Firewall-Appliances.

Die Firewall-Appliance

Eine Appliance ist ein vergleichsweise hoch integriertes Gerät, das auf eine bestimmte Anwendung zugeschnitten ist. Sie enthält eine Platine mit allen benötigten Komponenten wie CPU, Speicher, Netzwerkschnittstellen. Sofern die konkrete Anwendung keine Dateidienste umfasst (wie etwa bei einem Web-Server), ist ein Gehäuselüfter meist das einzige bewegliche Bauteil – wenn überhaupt.
Betriebssystem und Anwendungssoftware sind oft in einem Flash-Baustein untergebracht und werden auch als *Firmware* bezeichnet. Das ermöglicht Updates, bietet jedoch Schutz vor Überschreiben. Auch werden Risiken wie der Ausfall einer Festplatte so vermieden.
Als Betriebssysteme kommen angepasste Versionen der auch sonst eingesetzten Systeme zum Einsatz, von Windows NT bis zu verschiedenen Unix-Derivaten wie OpenBSD oder Linux. Die eigentliche Firewall-Software ist meist eine Eigenentwicklung des jeweiligen Anbieters. Dieser bietet seine Appliances häufig in unterschiedlichen Konfektionen an, um verschiedene Szenarien abzudecken.
So unterscheiden sich die einzelnen Modellvarianten in der Art und Anzahl der Netzwerkschnittstellen, der CPU-Leistung und zusätzlichen Software-Komponenten.
Der wesentliche Vorteil einer Firewall-Appliance ist, dass ein solches Gerät einsatzbereit geliefert wird und alle enthaltenen Komponenten aufeinander abgestimmt und vorkonfiguriert sind. Man

Checkliste zur Auswahl einer Firewall-Lösung

- Wie viele Benutzer/Arbeitsplätze müssen insgesamt geschützt werden?
- Welche Art(en) externe(r) Verbindung(en) werden genutzt/sind geplant?
- Welche Bandbreite der externen Anbindung(en) wird benötigt/gewünscht?
- Welchen Anwendungen sollen über die externe Verbindung benutzt werden?
- Welche Zusatzfunktionalitäten (z. B. VPN) werden benötigt/gewünscht?
- Sind mehrere Standorte zu verbinden, wie viele?
- Welche Ausbaustufen sind in absehbarer Zeit vorgesehen/möglicherweise nötig?
- Welcher Kostenrahmen steht insgesamt zur Verfügung?
- Sind (genügend) interne Fachleute vorhanden?
- Kann der Anbieter Einrichtung und Wartung übernehmen?
- Wie hoch ist der Installations- und Wartungsaufwand insgesamt (inklusive flankierender Massnahmen)?
- Welche vorhandenen Komponenten/Geräte/Infrastrukturen können/müssen integriert werden?
- Welche verbleibende Lebensdauer haben bereits vorhandene Lösungen?
- Müssen vorhandene Lösungen ersetzt oder angepasst werden?

Bild 1. Symantec präsentiert die neuen Firewall-Systeme Symantec Firewall/VPN 100, 200 und 200R. Jedes der neuen Systeme integriert Firewall, VPN und die Vernetzung mit weiteren Fähigkeiten in einem kompakten Gerät, um speziell den Anforderungen von Telearbeitsplätzen, Unternehmensfilialen und kleinen Unternehmen gerecht zu werden.

erhält eine schlüsselfertige Lösung aus einer Hand wie beispielsweise die Symantec Veloci Raptor, eine integrierte Firewall/VPN-Lösung. Was zu tun bleibt, ist die Anpassung der Filterregeln an die spezifischen Erfordernisse des konkreten Einsatzbereichs. Hierdurch wird nicht nur eine erhebliche Menge an Arbeitszeit gespart, man verringert auch das Risiko, durch Fehler bei der Installation Sicherheitslücken zu schaffen, die im Nachhinein schwer zu schliessen sind. Stellt sich später heraus, dass eine Appliance eine Sicherheitslücke aufweist, kann diese durch Einspielen eines Firmware-Updates beseitigt werden. Hierbei ist man allerdings auf den Hersteller angewiesen, der ein solches Update bereitstellen muss.
Die herstellerseitige Anpassung auf ein bestimmtes Anwendungsszenario, dass zum Beispiel die Art der Internet-Anbindung (Wählverbindung, DSL, Standleitung) oder die Anzahl der Benutzer umfassen kann, bringt den Nachteil einer geringeren Flexibilität mit sich, wenn sich das Szenario wesentlich verändert. Genügt der Durchsatz nicht mehr den gestiegenen Anforderungen, weil sich die Anzahl der Benutzer deutlich erhöht hat und man diese Möglichkeit bei der Anschaffung nicht ausreichend berücksichtigt hat, kann man in vielen Fällen die Last auf eine oder mehrere weitere Appliances verteilen.
Ein weiterer Vorteil einer Appliance ist, dass mit einer solchen Lösung auch in solchen Unternehmen eine gesicherte Internet-Anbindung erreicht werden kann, die nicht über ausreichende und entsprechend qualifizierte Personalkapazitäten verfügen, wie sie für Einrichtung, Betrieb und Wartung einer klassischen Firewall notwendig wären.
Auch beim Einsatz einer oder mehrerer Firewall-Appliances ist qualifiziertes Fachpersonal erforderlich, jedoch nicht in demselben Masse. Ist kein oder nicht genügend qualifiziertes Fachpersonal vorhanden, ist es bei Einsatz von Appliances kostengünstiger und transparenter, externe Dienstleitungen in Anspruch zu nehmen.
Zusätzliche Funktionen wie Virtuelle Private Netze (VPN) zur Anbindung von entfernten Unternehmensstandorten an das interne Netz ermöglichen die Nutzung des Internets als Transportmedium über beliebige Distanzen, ohne die erheblichen Kosten von Stand- oder Wählleitungen zwischen den einzelnen Filialen und der Zentrale. Dabei werden alle Daten vor dem Übergang ins Internet verschlüsselt und am anderen Ende wieder entschlüsselt. Dadurch entsteht ein gesicherter *Tunnel*, der die Daten nicht nur vor neugierigen Blicken, sondern auch vor Manipulationen schützt. Quelle und Ziel der Daten sind definiert und nicht manipulierbar.

Fazit

Bei entsprechender Planung, die man in jedem Fall betreiben muss, bieten Firewall-Appliances gegenüber der klassischen Firewall-Lösung aus Hard- und Software verschiedener Hersteller einige Vorteile. Diese liegen vor allem auf der Kostenseite, denn Einrichtung, Betrieb und Wartung sind weniger aufwändig. Ausserdem verringert sich das Risiko, durch Fehler bei der Installation und Einrichtung Sicherheitslöcher zu erzeugen, die schwer zu finden und zu schliessen sind. Schliesslich bringen Zusatzfunktionen wie VPN weitere Kostenvorteile bei verteilten Standorten, die anders nur mit deutlich höherem Aufwand zu erzielen wären. Als Nachteil ist die Bindung an einen einzelnen Hersteller und eine geringere Flexibilität bei sich ändernden Anforderungen zu nennen. 4

Plus/Minus

Software-Firewall

(+) Hardware und Software können separat umgerüstet, erweitert und aktualisiert werden
(–) hoher Zeitaufwand für Installation und Wartung
(–) hohe Ansprüche an Fachkenntnisse des Personals

Firewall-Appliance

(+) Lösung aus einer Hand, Hard- und Software sind aufeinander abgestimmt
(+) geringerer Zeitaufwand für Installation und Wartung
(+) serienmässige Zusatzfunktionen wie VPN
(–) geringe Flexibilität bei Änderungen der Anforderungen
(–) Skalierbarkeit nur durch Kombination mehrerer Appliances

Grundtypen von Firewalls

- Paketfilter: Einfache Paketfilter prüfen IP-Paket nach Quelle und Ziel (IP-Adresse, Port) und entscheiden anhand von Filterregeln, ob sie durchgelassen oder abgewiesen/verworfen werden.
- Stateful-Inspection-Paketfilter: Die Header der IP-Pakete werden analysiert, der Verbindungsstatus wird in die Beurteilung einbezogen.
- Application Proxy/Gateway: Daten werden auf Anwendungsebene analysiert, dabei fallen beispielsweise «verbotene» Kommandos auf.
- Hybride: Kombinationen aus Application Proxy und Stateful Inspection Paketfilter, nicht notwendigerweise in einem Gerät.

Bernd Bilek, *Systems Engineer und Firewall-Experte bei Symantec (Deutschland) GmbH, Homepage: www.symantec.de*

Summary

Plug and Protect: Understanding the Concept of Firewall Appliances

The term firewall refers not so much to a terminal as to a concept. Within this concept there are terminals which are also called firewalls. In what follows, the term firewall refers to these terminals. They often consist of two or more separate components: a computer including operating system and one or more software components. Set-up of a firewall computer starts with the installation of several network cards, followed by the installation and configuration of the operating system, which must be adapted to meet the special requirements of this task. All services not required for firewall operation must be removed or deactivated so that installation and configuration of the actual firewall software can take place.

Über Symantec

Symantec ist weltweit marktführend auf dem Gebiet der Internet-Sicherheit. Die umfangreiche Palette an Lösungen in den Bereichen Content und Netzwerksicherheit für Privatanwender, Unternehmen und Internet-Dienstleister umfasst Virenschutz, Firewalls und Virtual Private Networks ebenso wie Schwachstellen Management, Intrusion Detection, Internet- und E-Mail-Filter sowie Technologien für die Fern-Verwaltung und Sicherheitsservices für Unternehmen und Internet-Dienstleister weltweit. Die Konsumermarke für Sicherheitsprodukte Norton ist weltweit marktführend im Einzelhandel und hat zahlreiche Auszeichnungen der Branche bekommen. Das Unternehmen ist in Cupertino, Kalifornien, beheimatet und vertreibt seine Produkte in 37 Ländern. Homepage: www.symantec.de

FORSCHUNG UND ENTWICKLUNG

Platznot führt weiter in die dritte Dimension

Ob PDA oder Mobiltelefon – tragbare Geräte leiden unter chronischer Platznot im Innern. Kein Wunder, dass man intensiv die dritte Dimension nutzen will, um Grundfläche zu sparen. Doch auch da herrscht qualvolle Enge, weil die Geräte flach bleiben sollen. Der schon länger verfolgte Ausweg führt zu den Multi Chip Packages (MCP), die immer mehr Chips aufnehmen können. Fujitsu (und auch andere Hersteller) zeigt, wie man heute viele Chips in ultraflache Gehäuse einbaut. In seinen neuen MCPs bringt das Unternehmen bis zu sechs Chips unter. Zuvor wird mit mechanischem Polieren die jeweilige Chipdicke auf nur noch 25 µm herunter geschliffen. Damit kommt man bei sechs Chips auf maximale Gehäusehöhen von 1,4 bis 1,6 mm, bei acht Chips auf 2 mm Höhe. Eine besondere Technologie für den Einbau in Smart Cards erlaubt drei Chips gestapelt in einem «Land Grid Array» (LGA): Da ist das gesamte Gehäuse nur 0,5 mm (!) hoch.

Fujitsu Limited
Marunouchi Center Building
6-1 Marunouchi 1-Chome
Chiyoda-ku
Tokyo 100
Japan
Tel. +81-3-3216-3211

Neue Erkenntnisse über das Internet

Man hat es schon immer geahnt, aber jetzt haben es Wissenschaftler des NEC Forschungsinstitutes in Princeton bewiesen: Das Internet ist zwar formal unorganisiert, verfügt aber über eine inhärente Form der Selbstorganisation. Die entsteht durch die «Links» auf den Websites, mit denen man durch einfaches Anklicken eines Stichworts zu weiteren ähnlichen Informationen auf anderen Websites kommt. Die NEC-Forscher ziehen daraus den Schluss, dass man viel bessere Suchmaschinen entwickeln könnte, wenn man diesen Links nachgeht. Sie stehen in viel engerem semantischen Zusammenhang untereinander als eine reine Stichwort-orientierte Suche. Auf dieser Erkenntnis haben die Wissenschaftler einen so genannten «Community-Algorithmus» entwickelt. Sie erwarten, dass nun verbesserte Webfilter und Suchmaschinen gebaut werden können. Die Ergebnisse ihrer Arbeit wurden im «IEEE Computer Magazine» veröffentlicht (3/2002).

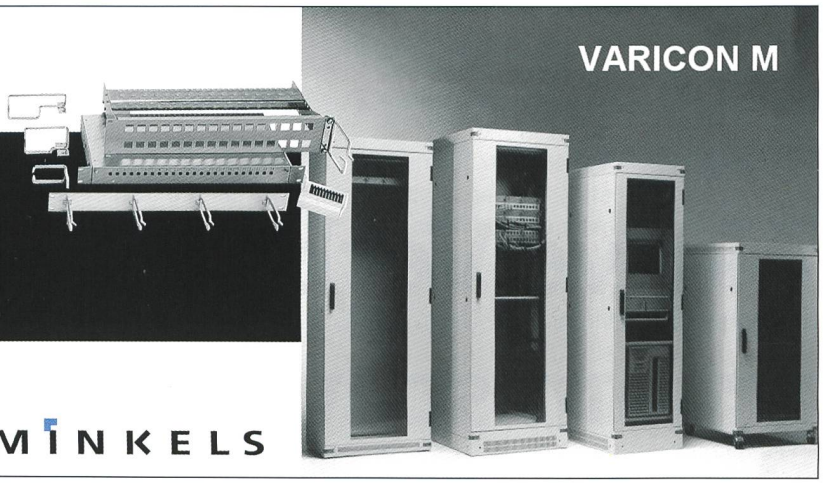
Homepage NEC Forschungsinstitut: www.neci.nj.nec.com, Homepage zum aktuellen Thema: www.nec.co.jp/press/en/0203/0501.html

Jetzt schon zwei Millionen ADSL-Nutzer

Der schnelle Internet-Anschluss wird zum Hit in Japan. Im letzten halben Jahr kamen jeden Monat rund eine Viertelmillion neuer Teilnehmer hinzu. Nach Angaben des MultiMedia Research Institutes wurde im März 2002 erstmals die Zahl von zwei Millionen ADSL-Teilnehmern überschritten.

Cabling-Zubehör?

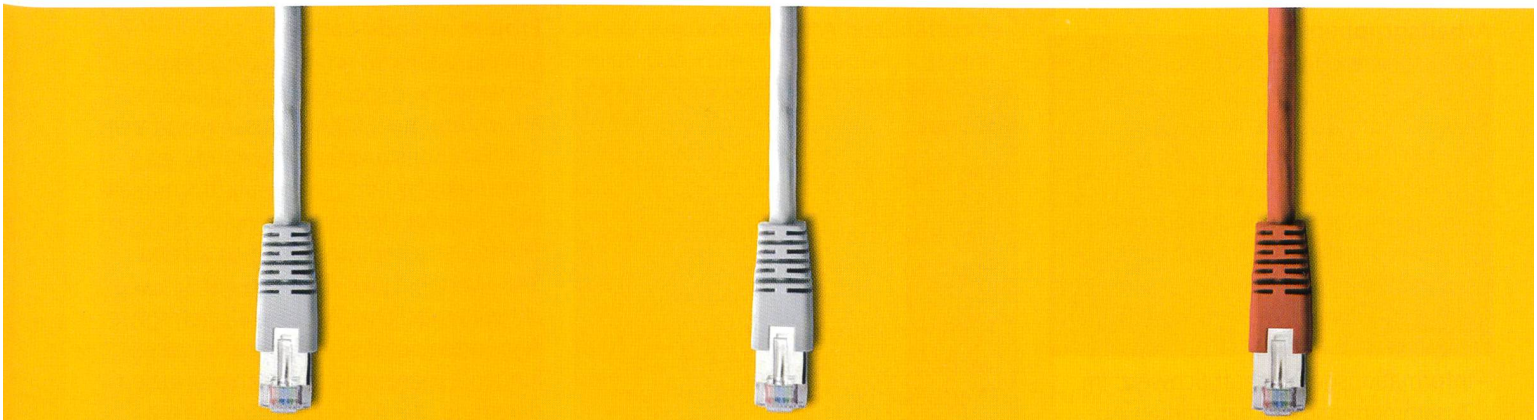
Netzwerkschränke und Gehäuse
Wandrack
Rangierfrontplatte
Blindplatte
Rangierringe und vieles mehr!



Minkels AG
Riedstrasse 3–5, CH-6330 Cham
Telefon +41 (0)41 748 40 60
Telefax +41 (0)41 748 40 79
verkauf@minkels.ch, www.minkels.ch

MINKELS

www.koe.ch
Branchenregister für Kommunikation und Produktion



drei für zwei

Faszinierende Beiträge über die Welt der Telekommunikationstechnik.

☐ **Ja, senden Sie mir die nächsten 3 Ausgaben für nur Fr. 16.–. Ich spare so Fr. 8.– oder 33 % gegenüber dem Einzelverkauf.**
☐ **Ja, senden Sie mir bitte das comtec im Jahresabo mit 11 Ausgaben für Fr. 80.–.**

Name | Vorname
Firma | Adresse
PLZ | Ort
Unterschrift

Coupon einsenden oder faxen an: Künzler-Bachmann Direct AG \ Frau Renate Meyer \ Zürcherstrasse 601
Postfach 345 \ CH-9015 St.Gallen \ Telefon 071 314 04 82 \ Telefax 071 314 04 45 \ r.meyer@kueba.ch \ www.kueba.ch
Preise inkl. MwSt. und Porto. Auslandpreise auf Anfrage.