Firewall - Lösungen

AvHG, Inf, My

Aufgabe 1:

Gebäude	**Firewall**
Eine Schutzmauer trennt die Gebäudeteile voneinander und schottet definierte Bereiche ab	Die Firewall trennt zwei Netze voneinander.
Ein Pförtner überwacht den Zugang zum Haus. Personen müssen sich bei ihm identifizieren.	Die Firewall bildet den einzig möglichen Zugang von einem Netz zum anderen. Die Paket-Adressen werden von der Firewall überprüft.
Besucher melden sich beim Pförtner und dieser meldet ihr Erscheinen an die betreffenden Personen im Haus.	Die Firewall lässt nur Pakete mit bestimmten IP-Adressen und Ports durch. Gegebenenfalls leitete sie alle Pakete explizit weiter (und ändert vielleicht sogar die Adresse).
Transportmittel und Gegenstände werden vom Pförtner überprüft.	Die Firewall überprüft gegebenenfalls den Inhalt von Datenpaketen.
Besondere Ereignisse werden vom Pförtner protokolliert.	Die Firewall kann Ereignisse in eine Log-Datei schreiben.

(a) Ein Proxy stellt stellvertretend für einen PC des Netzwerks (als Client) die HTML-Anfragen an das Internet. Wenn ihm die Anwort vertrauenswürdig erscheint spielt er für den PC den Server und gibt die Anworten weiter.

(b) extras / Internetoptionen.../Verbindungen / Button „Einstellungen...“

Aufgabe 3:

(a) Paket-Filter:

Überprüft nur die Adresse.

Application Gateway:

Überprüft auch die Inhalte.

(b) Paket-Filter:

Der Pförtner prüft, ob das Logo auf dem LKW bekannt ist und lässt den Lastwagen passieren.

Application Gateway:
Der Pförtner prüft Papiere und Inhalt. Er nimmt die Pakete entgegen und bestellt einen Fahrer der eigenen Firma, der die Pakete zum eigentlichen Empfänger bringt.

Aufgabe 4:

Personal Firewall:

Schützen nur einen Rechner (kein Netz) vor dem Internet. Beinhalten Paket-Filter und Content-Filter (auch Virenscanner möglich).

Kein Getrenntes Netz / Proxy / NAT möglich.

Aufgabe 5:

(a) Network Address Translation: Übersetzt IP Adresse (und eventuell auch Port Adresse): private ←> öffentliche.

(b) Aus welchen Gründen wird Network Address Translation durchgeführt?

- weil es nicht ausreichend freie Internet-Adressen gibt (Bsp: die IP unseres Servers gibt es noch mal in Amerika)
- aus Sicherheitsgründen

Aufgabe 6:

Kann eine Firewall zum Schutz vor den nachfolgend aufgelisteten Gefahren eingesetzt werden? Falls ja, was für ein Firewall-Typ wird benötigt?

(a) Angreifbare Programme auf Rechnersystemen im zu schützenden Netz (wie Sendmail) können **durch ein Application Gateway mit einem Proxy (Stellvertreter)** entkoppelt werden. Dadurch ist gegen aussen nur der Proxy sichtbar, welcher eine zweite Verbindung nach innen herstellt. Sendmail ist so nicht mehr direkt erreichbar und die geprüfte Minimalsoftware (Proxy) bietet idealerweise keine Angriffsmöglichkeit.

(b) Es können allerdings Pakete vom externen Interface (Input Filter) verworfen werden, welche als Source-Adresse eine Adresse des internen Netzwerkes besitzen. Dazu muss ein **Paketfilter** unterschieden können, von welcher Seite ein Paket stammt.

(c) Ein Ping erfolgt via ICMP als "Echo Request", der mit Type=8 verschickt wird (vgl. Abbildung: Format der ICMP Echo-Anforderung/Antwort). Entsprechende Pakete von aussen können mit einem **Paketfilter** verworfen werden. Hinweis: ICMP-Daten werden immer mit einem vollständigen IP-Header verschickt.

Aufgabe 7:

a)

- Reduzierte Angriffspunkte durch die Abschottung interner Systeme
- Effiziente Umsetzung der Sicherheitspolitik an zentraler Stelle
- Vollständige und einfache Protokolliermöglichkeit der gesamten Kommunikation

b) Application Gatewax, Proxy, (eventuell NAT) : volles Programm!

c)

- Eine Firewall kann zwar einen Netzübergang sichern, sie hat aber keinen Einfluß auf die Sicherheit der Kommunikation innerhalb dieser Netze.
- Es werden Protokolle überprüft, nicht die Inhalte. Eine Protokollprüfung bestätigt beispielsweise, daß eine E-Mail mit ordnungsgemäßen Befehlen zugestellt wurde, kann aber keine Aussagen zum eigentlichen Inhalt der E-Mail machen.
- Attacken, welche die Firewall umgehen (z.B. Diskette, via Modem, etc.).
- Die Filterung von aktiven Inhalten ist unter Umständen nur teilweise erfolgreich. z.B. Viren, wenn sie verschlüsselt eingeschleust werden.
- Angriffe und Fehler auf der Ebene der Anwendungssoftware.
- Menschliches Versagen, Social Engineering.
- Neue oder unbekannte Gefahren.
- Am sichersten ist gar keine Verbindung! Eine Netz mit extrem heikler Information soll nicht mit dem Internet verbunden werden.