Berufliche Schule der Landeshauptstadt Schwerin – Technik

LF7:Vernetzte IT-Systeme Datum:

Arbeitsblatt Firewall Tabelle:

Füllen Sie die Tabellen mit Hilfe des Lehrbuch Net-IT S 217 ff. aus.

Allgemeine Informationen zu Firewallsystemen:

Gründe für den Einsatzt einer Firewall Schutz gegen welche Bedrohungen?	vielfältige Bedrohungen • Address Spoofing1: Unter einer gefälschten Identität wird eine Kommunikationsverbindung aufgebaut. Hierbei erzeugt der Angreifer IP-Pakete mit gefälschter IP-Absenderadresse. • Denial-of-Service-Angriff 2: Ziel ist es, einen bestimmten Server „lahmzulegen“ und ihn so daran zu hindern, Antworten auf Anfragen zu erzeugen. Dies geschieht meist in der Form, dass die Ressourcen des Servers voll belegt werden und so für weitere Anfragen keine Ressourcen mehr zur Verfügung stehen. • Abhören fremder Zugangsdaten während des Netzverkehrs.
Aufgaben einer Firewall	Aufgaben einer Firewall: • Schutz vor unbefugten Netzzugriffen. • Zugangskontrolle: Steuerung, welche Nutzer in welcher Form auf welche Netzressourcen zugreifen dürfen. • Protokollierung der Netzwerkaktivitäten: Aufzeichnung des Netzverkehrs, um hieraus Rückschlüsse auf erfolgte Angriffe ziehen zu können. • Alarmierung bei sicherheitsrelevanten Ereignissen: Werden sicherheitsrelevante Aktionen von hierzu nicht befugten Nutzern durchgeführt, so wird durch die Firewall ein Alarm ausgelöst. • Verbergen der internen Netzstruktur: Um Angreifern mögliche Angriffspunkte des internen Netzwerks vorzuenthalten, verhindert die Firewall das Einsehen der Struktur dieses Netzwerks von außen. • Gewährleistung der Vertraulichkeit von Daten: Sicherstellung, dass der interne Netzverkehr nicht abgehört werden kann.

Beschreiben Sie die Leistungen verschiedener Firewallsysteme:

	Paketfilter	Proxy-Firewall	Applikationsfilter
OSI-Schicht:	3 & 4 Vermittlung/Transport	4 (Transport) -zwischen den beiden Netzwerken und vermittelt zwischen	7 (Anwender) Im Gegensatz zu den reinen auf der Transportschicht arbeitenden Proxies besitzen sie jedoch die Fähigkeit, die Inhalte der einzelnen Datenpakete entpacken und bzgl. des Inhalts untersuchen zu können. Ein Applikationsfilter für den FTP-Dienst kann so z. B. erkennen, welche FTP-Befehle (siehe Abschnitt 9.3.1: Protokolle des Anwendungssystems) übertragen werden, und behandelt diese dann gemäß der festgelegten Sicherheitsstrategie unterschiedlich.
Arbeitsweise:	. Sie überprüfen alle ankommenden Datenpakete auf bestimmte Eigenschaften, die den einzelnen Feldern der jeweiligen Protokollheader entnommen	Client und Server -> Zugriff auf das jeweilige andere Netz erfolgen, nicht direkt durch Client und Server vonstattengehen -> Stattdessen Proxy-Server ein entsprechender Dienst angeboten, beiden Rechner verwenden -> sicherstellen, dass die eigentliche Netzverbindung nur über die sichere Software des Proxy-Servers erfolgt (NAT -> Network Address Translation)	
Geschwindigkeit:	hoch	Mittel Direkte TCP-Verbindungen zwischen Client und Server werden verhindert.	Langsam (jede Inhalt wird kontrolliert)
Sicherheit:	kein umfassender Schutz • nur einfache Protokollierungsmöglichkeiten • Eine einzelne Komponente ist für den Schutz des gesamten	• Für viele Dienste einsetzbar wie z. B. für Mail-, Web- und PrintDienste. • Verbergen der Netzstruktur durch IPAdressumsetzung	Durchführung von Kontrollen in Abhängigkeit der versendeten Nachrichten. • Hohe Sicherheit
Kontrollmöglichkeit:	Protokollierung der Netzwerkaktivitäten	HTML-Verbindungen nur als Ganzes kontrollierbar	hohe Kontrollmöglichkeit (Protokollierung)

LF7:Vernetzte IT-Systeme Datum:

Firewalls werden in verschiedene Klassen eingeteilt:

- Paketfilter
- Proxy-Firewalls
- Applikationsfilter

Beschreiben Sie Vor- und Nachteile von Firewallsystemen:

	Vorteile	Nachteile
Paketfilter	• **Vorteile:** ▪ hohe Arbeitsgeschwindigkeit ▪ kostengünstig ▪ leichte Konfiguration und Wartung	• **Nachteile:** ▪ kein umfassender Schutz ▪ nur einfache Protokollierungsmöglichkeiten ▪ Eine einzelne Komponente ist für den Schutz des gesamten Netzwerks zuständig.
Proxy-Firewall	• **Vorteile:** ▪ Direkte TCP-Verbindungen zwischen Client und Server werden verhindert. ▪ Für viele Dienste einsetzbar wie z. B. für Mail-, Web- und Print-Dienste. ▪ Verbergen der Netzstruktur durch IP-Adressumsetzung.	• **Nachteile:** ▪ Aufgrund der Ansiedlung auf der Transportebene und nicht auf der Anwendungsebene des ISO/OSI-Referenzmodells, können nur allgemeine Vermittlungsdienste zur Verfügung gestellt werden. Besonderheiten einzelner Anwendungsprotokolle bleiben unberücksichtigt. So sind HTML-Verbindungen nur als Ganzes kontrollierbar. Eine unterschiedliche Behandlung der übermittelten Datenpakete in Abhängigkeit der konkreten Inhalte ist jedoch nicht möglich. ▪ Der Einsatz einer Proxy-Firewall erfordert in der Regel eine entsprechende Konfiguration der Software auf der Clientseite, da Aufrufe, die sich an einen bestimmten Server richten, auf den Proxy-Server umzuleiten sind.
Applikationsfilter	• **Vorteile:** ▪ Durchführung von Kontrollen in Abhängigkeit der versendeten Nachrichten. ▪ Hohe Sicherheit • **Nachteile:** ▪ Langsamer als Paketfilter und einfache, auf der Transportschicht arbeitende Proxy-Firewalls.	