Kontrollfragen

Firewalltypen

Paketfilter

Die vier Grundaktionen des Paketfilters

Ein Paketfilter repräsentiert das Urgestein der Firewallthematik. Er arbeitet mit so genannten Regelketten, welche sequentiell von oben nach unten abgearbeitet werden. Doch welche vier Aktionen stehen dem Administrator zur Verfügung?

Variante 1	*Variante 2*	*Variante 3*
ACCEPT DROP REJECT LOG □ Richtig	ACCECPT DELETE REJECT LOG □ Richtig	ACTION DROP REJECT LOG □ Richtig

Das Ende einer Prüfkette

Falls keine der definierten Prüfkriterien einen *MATCH* erzielt, was geschieht mit dem zu prüfenden Paket am Ende einer Kette?

- □ Das Paket wird verworfen
- □ Das Paket wird ggf. in eine zweite Kette weitergeleitet
- □ Die *Default*-Regel greift (sofern konfiguriert).
- □ Das Paket wird an den Start der aktuelle Kette geleitet.

Der statische Paketfilter

In der Thematik des Paketfilters kennen wir zwei Typen - den statischen und den dynamischen Paketfilter. Welche Aussagen treffen auf den statischen Paketfilter zu?

- □ Der statische Paketfilter arbeitet zustandslos
- □ Der statische Paketfilter prüft ganze Datenstörme, nicht nur einzelnen Pakete.
- □ Aufgrund der statischen Arbeitsweise, gilt der statische Paketfilter als Ressourcen-Fresser.
- □ Aufgrund der statischen Arbeitsweise, gilt der statische Paketfilter als performant.
- □ Der statische Paketfilter wird so genannt, da er ganze Datenströme statisch speichert und somit immer den Überblick über aktuelle Verbindungen hat.

Der dynamische Paketfilter

Welche Aussagen treffen auf den dynamischen Paketfilter zu?

- □ Der dynamische Paketfilter arbeitet zustandsorientiert.
- □ Der dynamische Paketfilter prüft ganze Datenstörme.
- □ Der dynamische Paketfilter, kann im Vergleich zum statischen Paketfilter, bis zum vierten Layer im ISO/OSI Modell filtern.
- □ Der dynamische Paketfilter kann nur einzelne Datenpakete prüfen - daher wird er auch als dynamisch betitelt (situative Prüfung).
- □ Der dynamische Paketfilter kann, sofern gewünscht, eine *Statefull Inspection* durchführen. Dadruch können ganze Datenströme geprüft werden.
- □ Im Vergleich zum statischen Paketfilter gilt der dynamische Paketfilter als Ressourcen-Fresser und schliesst in punkto Sicherheit deutlich schlechter ab.

Proxy Firewall

Begrifflichkeiten

Erst wenn wir verstehen, können wir begreifen... welche Aussagen stimmen?

- □ Proxy ist ein klassisches IT-Wort (keine weitere Verwendung im Alltag).
- □ Proxy ist ein alltägliches Wort aus dem englischen Sprachraum.
- □ Proxy steht nebst *Vollmacht, Stimmrechtsermächtigung und Prokura* für *Vertreter*.

Wie und wo wird geprüft

Die Proxy-Firewall kann viel aber nicht alles, welche Aussagen betreffend dieser Technologie umschreiben den Leistungsumfang einer Proxy-Firewall am besten?

- □ Die Proxy-Firewall benötigt für jedes zu prüfende Protokoll (HTTP, FTP, SMTP etc.) einen eigenen Proxy-Prozess. Zudem werden verschlüsselte Verbindungen mittels der *direct packet*-Funktion transparent durch die Proxy-Firewall geschleust.
- □ Da eine Proxy-Firewall für uns zum Beispiel einen HTTP-Request ins WWW absetzt, gilt sie als eine Netzwerkkomponente mit nicht transparenter Arbeitsweise.
- □ Falls mit einem unbekannten Protokoll kommuniziert wird, stuft sie sich direkt auf den Level eines Paketfilters runter, sodass der Verkehr trotzdem statt finden kann.
- □ Da eine Proxy-Firewall für uns stellvertretend ins Internet geht, gilt Ihre Arbeitsweise als transparent und sicher.

Paketfilter und Proxy-Firewall im Vergleich

	Paketfilter	*Proxy-Firewall*	*Bewertung*
Protokoll-konformität	Wird nicht geprüft	Sofern gewünscht, ist eine Überprüfung realisierbar	☐ Richtig ☐ Falsch
Arbeitsfokus	Filterung unerwünschter Pakete	Filterung unerwünschter Pakete	☐ Richtig ☐ Falsch
Arbeitsweise	Nicht transparent, da komplette Datenströme geprüft werden	Transparent, da Benutzer nichts merkt von der Proxy-Firewall	☐ Richtig ☐ Falsch
Arbeitslast	Die Arbeitslast ist vergleichsweise zur Proxy-Firewall sehr gering	Im Vergleich zum statischen und dynamischen Paketfilter eher hohe Arbeitslast	☐ Richtig ☐ Falsch

Application Level Firewall

Wo und wie prüft die ALF?

Welche Aussagen treffen für die Prüfarbeit der Application Level Firewall zu?

- ☐ Die Application Level Firewall gilt als High-Level-Protokoll-Prüfer - sie beherrscht alle sieben Layer des ISO/OSI Modells.
- ☐ Die Application Level Firewall gilt als High-Level-Protokoll-Prüfer - sie beherrscht die Layer 5 - 7 des ISO/OSI Referenzmodells.
- ☐ Die ALF unterscheidet sich in punkto Datenverkehrprüfung grundlegend von einem Paketfilter und hat nur wenig Ähnlichkeit mit der Proxy-Firewall
- ☐ Mit einer ALF können HTTP:GET gesperrt und HTTP:POST Befehle zugelassen werden.
- ☐ Die ALF arbeitet zustandsorientiert und kann somit ganze Datenströme scannen.

Proxy-Firewall und Application Level Firewall im Vergleich

	Proxy-Firewall	*ALF*	*Bewertung*
Protokoll-konformität	Wird nicht geprüft	Wird geprüft	☐ Richtig ☐ Falsch
Arbeitsfokus	Filterung von Paketen	Filterung von Paketen sowie Prüfung von Benutzern und Paket-inhalt	☐ Richtig ☐ Falsch
Arbeitsweise	Nicht transparent	Nicht transparent	☐ Richtig ☐ Falsch
Arbeitslast	Mittel - Hoch	Hoch, benötigt in der Regel eigene Appliance	☐ Richtig ☐ Falsch

Informationen zu den Firewalltypen

Welche Aussage würden Sie unterschreiben?

Aussage 1	*Aussage 2*
Aktuelle Hardware-Firewall-Produkte sind ein Mix aus den drei Firewalltypen (Paket-filter, Proxy-Firewall und Application Level Firewall). Man spricht bei diesen Firewalls auch von einer Hybrid-Technologie, welche die Vorteile von allen drei Firewalltypen gekonnt kombiniert. ☐ Richtig	Aktuelle Hardware-Firewall-Produkte fokusieren sich stark auf die Vorzüg einer Application Level Firewall. Sie kombinieren die Vorteile einer ALF mit denen des LINUX-Kernels, welcher seit der Version 2.6.24 (seit 2008) als sehr sicher, kostengünstig und skalierbar gilt. ☐ Richtig