20.18 Spezialtrainer – Firewall-Regeln und Sicherheitszonen

Dieser Spezialtrainer ist eine zusätzliche Übungsseite.

Der allgemeine Netzwerktechnik-Trainer ist bereits abgeschlossen. Diese Seite dient nur als vertiefender Trainer für Firewall-Regeln, Sicherheitszonen, DMZ, VLAN-Trennung und typische Prüfungsformulierungen.

Ziel ist, Firewall-Aufgaben sauber, vollständig und prüfungssicher zu beantworten.

Merksatz:

> Eine Firewall-Regel ohne Quelle,
> Ziel,
> Protokoll,
> Port,
> Aktion
> und Zweck ist unvollständig.

Lernziele

Nach dieser Seite solltest du sicher können:

- Firewall-Regeln vollständig formulieren
- Quelle,
  Ziel,
  Port
  und Protokoll unterscheiden
- Sicherheitszonen erklären
- DMZ-Regeln bewerten
- Any-to-Any-Regeln kritisch einordnen
- Default Deny erklären
- typische Fehlkonfigurationen erkennen
- sichere Alternativen zu breiten Freigaben nennen

Grundaufbau einer Firewall-Regel

Eine saubere Firewall-Regel enthält mindestens:

Bestandteil	Bedeutung
Quelle	Von wo kommt der Verkehr?
Ziel	Wohin geht der Verkehr?
Protokoll	TCP, UDP, ICMP oder anderes
Port	Welcher Dienst ist gemeint?
Richtung	Eingehend oder ausgehend
Aktion	Erlauben oder blockieren
Zweck	Warum gibt es diese Regel?

Merksatz:

> Quelle,
> Ziel,
> Protokoll,
> Port,
> Aktion,
> Zweck.

Typische Sicherheitszonen

Zone	Bedeutung
Internet	unsicheres externes Netz
DMZ	Zone für öffentlich erreichbare Dienste
internes Netz	interne Clients und Systeme
Servernetz	interne Server
Managementnetz	Administration von Systemen
Gastnetz	Netz für Gäste oder fremde Geräte
VPN-Netz	Netz für entfernte Benutzer
Backup-Netz	Netz für Sicherungen und Wiederherstellung

Merksatz:

> Zonen trennen Systeme nach Schutzbedarf.

Aufgabe 1

Was ist eine Firewall?

Antwort anzeigen

Eine Firewall ist ein System, das Netzwerkverkehr anhand von Regeln erlaubt oder blockiert.

Typische Kriterien:

```
Quelle

Ziel

Protokoll

Port

Richtung

Zone

Benutzer

Anwendung

Verbindungszustand
```

Merksatz:

```
Firewall = kontrollierter Netzwerkverkehr.
```

Aufgabe 2

Warum reicht die Regel „Port 443 erlauben“ nicht aus?

Antwort anzeigen

Die Regel ist unvollständig.

Es fehlen:

```
Quelle

Ziel

Protokoll

Richtung

Aktion

Zweck
```

Besser:

```
Quelle:
Internet

Ziel:
Webserver-DMZ

Protokoll:
TCP

Port:
443

Aktion:
erlauben

Zweck:
HTTPS-Zugriff auf Webserver
```

Merksatz:

```
Port allein ist keine vollständige Firewall-Regel.
```

Aufgabe 3

Warum ist „Port 53 erlauben“ ungenau?

Antwort anzeigen

Es fehlt das Transportprotokoll.

DNS nutzt:

```
UDP 53
```

und bei Bedarf:

```
TCP 53
```

Eine Regel für TCP 53 erlaubt nicht automatisch UDP 53.

Merksatz:

```
Portnummer immer mit TCP oder UDP nennen.
```

Aufgabe 4

Was bedeutet Default Deny?

Antwort anzeigen

Default Deny bedeutet:

```
Standardmäßig ist Verkehr blockiert.
```

Nur ausdrücklich erlaubter Verkehr wird zugelassen.

Vorteile:

kleinere Angriffsfläche

bessere Kontrolle

weniger unbeabsichtigte Freigaben

klare Sicherheitsstruktur

Merksatz:

Erst blockieren,
dann gezielt erlauben.

Aufgabe 5

Was ist eine Any-to-Any-Regel?

Antwort anzeigen

Any-to-Any bedeutet:

jede Quelle

zu

jedem Ziel

Meist zusätzlich:

alle Ports

alle Protokolle

erlauben

Das ist kritisch, weil sehr viel Verkehr ungeprüft zugelassen wird.

Merksatz:

```
Any-to-Any ist eine sehr breite Freigabe.
```

Aufgabe 6

Warum ist Any-to-Any kritisch?

Antwort anzeigen

Risiken:

```
große Angriffsfläche

schlechte Nachvollziehbarkeit

Sicherheitszonen werden umgangen

unnötige Freigaben

laterale Bewegung wird erleichtert

Fehler schwerer erkennbar
```

Besser:

```
gezielte Regeln mit Quelle,
Ziel,
Port,
Protokoll
und Zweck.
```

Merksatz:

Je breiter die Regel,
desto größer das Risiko.

Aufgabe 7

Welche Regel ist besser?

A:
Quelle: internes Netz
Ziel: any
Port: any
Aktion: erlauben

B:
Quelle: Clientnetz
Ziel: DNS-Server
Protokoll: UDP/TCP
Port: 53
Aktion: erlauben
Zweck: DNS-Auflösung

Antwort anzeigen

B ist besser.

Begründung:

Die Regel ist genauer.
Sie erlaubt nur den benötigten DNS-Verkehr
zum vorgesehenen DNS-Server.

Regel A ist zu breit, weil sie jeden Verkehr zu jedem Ziel erlaubt.

Merksatz:

Genau erlauben,
nicht pauschal freigeben.

Aufgabe 8

Ein Webserver in der DMZ soll öffentlich per HTTPS erreichbar sein.

Formuliere eine passende Regel.

Antwort anzeigen

Passende Regel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Internet	Webserver-DMZ	TCP	443	erlauben	HTTPS-Zugriff

Wichtig:

Keine pauschale Freigabe vom Internet ins interne Netz.

Merksatz:

Öffentlich nur den benötigten Dienst freigeben.

Aufgabe 9

Ein Webserver in der DMZ braucht Zugriff auf eine interne Datenbank.

Formuliere eine möglichst sichere Regel.

Antwort anzeigen

Beispielregel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck

Webserver-DMZ	interner Datenbankserver	TCP	5432	erlauben	Anwendung benötigt Datenbank

Wichtig:

Nur der konkrete Webserver darf auf den konkreten Datenbankserver zugreifen.

Nur der benötigte Datenbankport wird erlaubt.

Kein Any-to-Any zwischen DMZ und internem Netz.

Merksatz:

DMZ zu intern nur minimal und gezielt erlauben.

Aufgabe 10

Warum sollte eine Datenbank nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

Eine Datenbank enthält oft sensible Daten und ist ein attraktives Angriffsziel.

Risiken:

Brute Force

Exploits

Datenabfluss

Manipulation

DoS

Besser:

Zugriff nur vom Anwendungsserver

privates Netz

Firewall-Beschränkung

starke Authentifizierung

Logging

Merksatz:

Datenbankports gehören nicht offen ins Internet.

Aufgabe 11

Ein Gastnetz soll eingerichtet werden.

Welche Regeln sind sinnvoll?

Antwort anzeigen

Typische Regeln:

Quelle	Ziel	Aktion	Zweck
Gastnetz	Internet	erlauben	Internetzugriff für Gäste
Gastnetz	internes Netz	blockieren	interne Systeme schützen
Gastnetz	Servernetz	blockieren	Server schützen
Gastnetz	Managementnetz	blockieren	Administration schützen

Merksatz:

Gastnetz nur ins Internet,
nicht ins interne Netz.

Aufgabe 12

Ein Managementnetz soll geschützt werden.

Welche Regeln sind sinnvoll?

Antwort anzeigen

Sinnvolle Regeln:

```
Adminnetz zu Servern:
benötigte Adminports erlauben

Adminnetz zu Switches:
SSH oder HTTPS erlauben

Clientnetz zu Managementnetz:
blockieren

Gastnetz zu Managementnetz:
blockieren

Internet zu Managementnetz:
blockieren
```

Zusätzlich:

```
MFA

Logging

getrennte Admin-Konten

Least Privilege
```

Merksatz:

```
Managementzugänge besonders schützen.
```

Aufgabe 13

Ein Clientnetz soll nur DNS zum internen DNS-Server nutzen dürfen.

Formuliere die Regel.

Antwort anzeigen

Regel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Clientnetz	interner DNS-Server	UDP/TCP	53	erlauben	DNS-Auflösung

Optional zusätzlich:

> Clientnetz zu externen DNS-Servern blockieren,
> wenn DNS zentral kontrolliert werden soll.

Merksatz:

> DNS-Regeln brauchen UDP 53,
> TCP 53 mitdenken.

Aufgabe 14

Ein Clientnetz soll per HTTPS ins Internet.

Formuliere eine sinnvolle Regel.

Antwort anzeigen

Regel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Clientnetz	Internet	TCP	443	erlauben	HTTPS-Webzugriff

Je nach Umgebung zusätzlich:

HTTP TCP 80 erlauben oder blockieren

Proxy verwenden

Webfilter einsetzen

Logging aktivieren

Merksatz:

Webzugriff gezielt und protokolliert erlauben.

Aufgabe 15

Ein Clientnetz soll nicht direkt auf Server-Managementports zugreifen.

Welche Regel ist sinnvoll?

Antwort anzeigen

Sinnvolle Block-Regel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Clientnetz	Servernetz	TCP	22, 3389	blockieren	direkte Administration verhindern

Besser:

Administration nur aus Adminnetz erlauben.

Merksatz:

Normale Clients sollen keine Adminports erreichen.

Aufgabe 16

Warum sollte SSH nur aus dem Adminnetz erlaubt sein?

Antwort anzeigen

SSH ist ein Administrationszugang.

Wenn SSH aus allen Netzen erreichbar ist, steigt das Risiko für:

```
Brute Force

Missbrauch gestohlener Zugangsdaten

laterale Bewegung

unautorisierte Administration
```

Besser:

```
Quelle auf Adminnetz beschränken

MFA oder Schlüssel nutzen

Logging aktivieren
```

Merksatz:

```
Adminzugänge nur aus Adminnetzen erlauben.
```

Aufgabe 17

Warum sollte RDP nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

RDP ist ein häufiges Angriffsziel.

Risiken:

```
Brute Force

Credential Stuffing

Exploits

unberechtigter Zugriff
```

Sicherer:

```
VPN

RDP-Gateway

MFA

Zugriff nur von bekannten Quellnetzen

Logging
```

Merksatz:

```
RDP nicht offen ins Internet stellen.
```

Aufgabe 18

Warum sollte SMB nicht zwischen allen Netzen erlaubt sein?

Antwort anzeigen

SMB ermöglicht Datei- und Druckfreigaben.

Risiken bei breiter Freigabe:

```
Datenabfluss
```

Malware-Ausbreitung

laterale Bewegung

Zugriff auf interne Freigaben

Ausnutzung von Schwachstellen

Besser:

SMB nur gezielt zwischen benötigten Systemen erlauben.

Merksatz:

SMB breit freigeben ist riskant.

Aufgabe 19

Was bedeutet Regelreihenfolge bei Firewalls?

Antwort anzeigen

Viele Firewalls verarbeiten Regeln von oben nach unten.

Die erste passende Regel entscheidet.

Problem:

Eine breite Erlauben-Regel kann spätere Block-Regeln wirkungslos machen.

Oder:

Eine frühe Block-Regel kann spätere Erlauben-Regeln überdecken.

Merksatz:

Firewall-Regeln auch in der richtigen Reihenfolge prüfen.

Aufgabe 20

Eine Erlauben-Regel existiert, aber der Zugriff funktioniert nicht.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

Regelreihenfolge

Quelle korrekt?

Ziel korrekt?

Protokoll korrekt?

Port korrekt?

Richtung korrekt?

Zone korrekt?

NAT-Regel nötig?

Rückverkehr erlaubt oder stateful?

lokale Firewall auf Zielsystem

Dienst läuft?

Logs prüfen

Merksatz:

Eine Regel allein beweist noch nicht,
dass der Zugriff funktioniert.

Aufgabe 21

Was ist eine Stateful Firewall?

Antwort anzeigen

Eine Stateful Firewall merkt sich den Zustand von Verbindungen.

Wenn ein Client eine Verbindung nach außen startet, kann die Firewall passende Antwortpakete automatisch erlauben.

Vorteil:

Rückverkehr muss nicht immer manuell als eigene Regel definiert werden.

Merksatz:

Stateful Firewall kennt Verbindungszustände.

Aufgabe 22

Was ist eine Stateless Firewall?

Antwort anzeigen

Eine Stateless Firewall prüft Pakete einzeln.

Sie merkt sich keinen Verbindungszustand.

Folge:

Regeln für Hin-
und Rückrichtung müssen genauer berücksichtigt werden.

Merksatz:

```
Stateless Firewall kennt keine Verbindungshistorie.
```

Aufgabe 23

Was ist der Unterschied zwischen Firewall und ACL?

Antwort anzeigen

ACL steht für:

```
Access Control List
```

Eine ACL ist eine Liste von Regeln, die Zugriff erlaubt oder blockiert.

Eine Firewall kann ACL-ähnliche Regeln nutzen, bietet aber je nach System weitere Funktionen:

```
Zustandsprüfung

Logging

NAT

Anwendungskontrolle

Benutzerbezug

IDS/IPS-Funktionen
```

Merksatz:

```
ACL ist Regelliste.
Firewall ist oft umfassenderes Schutzsystem.
```

Aufgabe 24

Was ist eine Security Group in der Cloud?

Antwort anzeigen

Eine Security Group ist eine ressourcennahe Zugriffskontrolle in Cloud-Umgebungen.

Sie steuert typischerweise:

```
eingehenden Verkehr

ausgehenden Verkehr

Ports

Protokolle

Quellen

Ziele
```

Merksatz:

```
Security Group ist wie eine Cloud-nahe Firewall-Regelgruppe.
```

Aufgabe 25

Eine Cloud-VM ist nicht per SSH erreichbar.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

```
Security Group erlaubt TCP 22?

Quelle korrekt eingeschränkt?
```

VM hat richtige IP?

Route ins Subnetz korrekt?

Network ACL korrekt?

lokale Firewall der VM?

SSH-Dienst läuft?

SSH lauscht auf TCP 22?

Benutzer oder Schlüssel korrekt?

Merksatz:

Cloud-Zugriff braucht Security Group,
Route,
lokale Firewall
und Dienst.

Aufgabe 26

Eine Webanwendung in der Cloud soll öffentlich erreichbar sein, die Datenbank aber nicht.

Welche Grundidee ist richtig?

Antwort anzeigen

Richtig:

Webserver oder Load Balancer öffentlich erreichbar machen.

Datenbank in privatem Subnetz betreiben.

Zugriff auf Datenbank nur vom Anwendungsserver erlauben.

Security Group der Datenbank eng einschränken.

Merksatz:

Web nach außen,
Datenbank privat.

Aufgabe 27

Ein VPN-Benutzer soll nur einen Server erreichen dürfen.

Welche Regel ist sinnvoll?

Antwort anzeigen

Beispielregel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
VPN-Benutzergruppe Dienstleister	Zielserver	TCP	22	erlauben	Wartung durch Dienstleister

Zusätzlich blockieren:

VPN-Dienstleister zu restlichem internen Netz

Merksatz:

VPN-Zugriff nach Least Privilege begrenzen.

Aufgabe 28

Warum ist „VPN-Benutzer dürfen alles im internen Netz“ kritisch?

Antwort anzeigen

Risiken:

kompromittierte VPN-Zugangsdaten führen zu großem Schaden

laterale Bewegung im Netz möglich

Dienstleister sehen zu viele Systeme

Angriffe können sich leichter ausbreiten

Besser:

Zugriff nach Gruppen

nur benötigte Zielsysteme

nur benötigte Ports

Logging

MFA

Merksatz:

VPN ist ein Eingang ins Netz,
kein Freifahrtschein.

Aufgabe 29

Ein Backup-Server soll besonders geschützt werden.

Welche Regeln sind sinnvoll?

Antwort anzeigen

Sinnvolle Grundidee:

Nur Backup-Clients oder Backup-Agenten dürfen zum Backup-Server kommunizieren.

Normale Benutzer dürfen nicht direkt auf Backup-Speicher zugreifen.

Administration nur aus Adminnetz.

Löschrechte stark begrenzen.

Backup-Logs und Monitoring erlauben.

Beispiel:

Quelle	Ziel	Aktion	Zweck
Backup-Clients	Backup-Server	erlauben	Sicherung durchführen
Clientnetz	Backup-Speicher	blockieren	Schutz vor Manipulation
Adminnetz	Backup-Server	erlauben	Administration
Internet	Backup-Server	blockieren	Schutz vor Angriffen

Merksatz:

Backups brauchen besonders strenge Zugriffskontrolle.

Aufgabe 30

Warum ist eine Firewall-Regel ohne Zweck problematisch?

Antwort anzeigen

Ohne Zweck ist später unklar:

warum die Regel existiert

ob sie noch benötigt wird

wer verantwortlich ist

ob sie entfernt werden kann

welches Risiko sie abdeckt

Folge:

Regelwerke werden unübersichtlich
und unsichere Altregeln bleiben bestehen.

Merksatz:

Jede Firewall-Regel braucht eine Begründung.

Aufgabe 31

Was ist eine Regelwerksprüfung?

Antwort anzeigen

Eine Regelwerksprüfung kontrolliert bestehende Firewall-Regeln.

Geprüft wird:

Ist die Regel noch nötig?

Ist Quelle und Ziel genau genug?

Ist der Port korrekt?

Ist Any-to-Any vorhanden?

Gibt es doppelte Regeln?

Gibt es ungenutzte Regeln?

Ist der Zweck dokumentiert?

Gibt es Ablaufdaten für temporäre Regeln?

Merksatz:

Firewall-Regeln müssen regelmäßig aufgeräumt werden.

Aufgabe 32

Was ist eine temporäre Firewall-Regel?

Antwort anzeigen

Eine temporäre Regel ist nur für begrenzte Zeit gedacht.

Beispiele:

Wartung

Migration

Test

Fehleranalyse

Wichtig:

Ablaufdatum dokumentieren

Verantwortlichen nennen

nach Nutzung entfernen

Merksatz:

Temporäre Regeln dürfen nicht dauerhaft vergessen werden.

Aufgabe 33

Was ist Logging bei Firewall-Regeln?

Antwort anzeigen

Logging bedeutet:

```
Erlaubter oder blockierter Verkehr wird protokolliert.
```

Nutzen:

```
Fehlersuche

Sicherheitsanalyse

Nachvollziehbarkeit

Erkennen von Angriffen

Regelwerksprüfung
```

Merksatz:

```
Firewall-Logs zeigen,
was wirklich passiert.
```

Aufgabe 34

Ein Zugriff funktioniert nicht. Im Firewall-Log steht „Deny TCP 443“.

Was bedeutet das?

Antwort anzeigen

Bedeutung:

```
Verkehr zu TCP 443 wurde blockiert.
```

Prüfen:

```
Ist der Zugriff gewollt?

Quelle korrekt?

Ziel korrekt?

Regel fehlt?

Regelreihenfolge falsch?

falsche Zone?

falscher Port?
```

Merksatz:

```
Deny im Log ist ein konkreter Hinweis,
keine Vermutung.
```

Aufgabe 35

Ein Zugriff soll blockiert sein, aber er funktioniert trotzdem.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

```
Gibt es eine frühere Allow-Regel?

Regelreihenfolge korrekt?
```

falsche Quelle oder falsches Ziel?

falsche Zone?

anderer Port oder anderes Protokoll?

NAT verändert Ziel oder Quelle?

Verbindung bereits bestehend bei Stateful Firewall?

Logs prüfen

Merksatz:

Wenn Block nicht wirkt,
Regelreihenfolge und Matching prüfen.

Aufgabe 36

Welche Antwort ist besser?

Aufgabe:

Warum ist eine Any-to-Any-Regel unsicher?

Antwort A:

Weil sie zu offen ist.

Antwort B:

Eine Any-to-Any-Regel erlaubt Verkehr von jeder Quelle zu jedem Ziel.
Dadurch werden Sicherheitszonen umgangen,
die Angriffsfläche wird stark vergrößert
und laterale Bewegung im Netzwerk wird erleichtert.
Besser sind gezielte Regeln mit Quelle,

Ziel,
Protokoll,
Port
und Zweck.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt Risiko,
Wirkung
und bessere Maßnahme.

Merksatz:

Sicherheitsbewertung braucht Begründung.

Aufgabe 37

Welche Antwort ist besser?

Aufgabe:

Warum soll ein Gastnetz nicht auf interne Server zugreifen?

Antwort A:

Weil Gäste fremd sind.

Antwort B:

Geräte im Gastnetz sind nicht vertrauenswürdig.
Zugriff auf interne Server würde das Risiko für Datenabfluss,
Malware-Ausbreitung
und unberechtigten Zugriff erhöhen.

Deshalb sollte das Gastnetz nur ins Internet dürfen
und vom internen Netz getrennt werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt konkrete Risiken und eine passende Maßnahme.

Merksatz:

Risiko und Maßnahme verbinden.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

Eine Datenbank soll aus dem Internet erreichbar sein.
Bewerten Sie das.

Antwort A:

Datenbank ist wichtig,
also geht das.

Antwort B:

Das ist kritisch,
weil eine öffentlich erreichbare Datenbank direkt Angriffen wie Brute Force,
Exploits,
Datenabfluss
und Manipulation ausgesetzt ist.
Besser ist,

die Datenbank in einem privaten Netz zu betreiben
und nur Zugriff vom Anwendungsserver auf den benötigten Port zu erlauben.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort bewertet fachlich
und nennt eine sichere Alternative.

Merksatz:

Öffentlich erreichbare Datenbanken vermeiden.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Warum sollten Firewall-Regeln dokumentiert werden?

Antwort A:

Damit man mehr Unterlagen hat.

Antwort B:

Dokumentation macht nachvollziehbar,
warum eine Regel existiert,
wer verantwortlich ist,
welchen Zweck sie erfüllt
und ob sie noch benötigt wird.
Dadurch können unsichere oder veraltete Regeln später entfernt werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt den betrieblichen und sicherheitstechnischen Nutzen.

Merksatz:

Dokumentation hilft Sicherheit und Betrieb.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Ein Dienst funktioniert nicht.
Was prüfen Sie an der Firewall?

Antwort A:

Firewall an oder aus.

Antwort B:

Ich prüfe Quelle,
Ziel,
Protokoll,
Port,
Richtung,
Zone,
Regelreihenfolge
und Firewall-Logs.
Zusätzlich prüfe ich,
ob NAT oder eine lokale Firewall auf dem Zielsystem beteiligt ist.

Antwort anzeigen

B ist besser.

Begründung:

> Die Antwort nennt konkrete Prüfpunkte
> und ist damit prüfungssicher.

Merksatz:

> Firewall prüfen heißt:
> Regel-Matching konkret prüfen.

Mini-Prüfung: vollständige Regelangaben

Fehlende Angabe	Warum wichtig?
Quelle	bestimmt, wer senden darf
Ziel	bestimmt, wohin gesendet wird
Protokoll	TCP, UDP, ICMP unterscheiden
Port	Dienst genau bestimmen
Richtung	eingehend oder ausgehend
Aktion	erlauben oder blockieren
Zweck	spätere Nachvollziehbarkeit
Zone	Sicherheitsbereich erkennen

Mini-Prüfung: sichere Grundregeln

Situation	Sichere Grundidee
Webserver öffentlich	nur TCP 443 zur DMZ erlauben
Datenbank	nicht öffentlich, nur Appserver erlauben
Gastnetz	Internet erlauben, intern blockieren
Managementnetz	nur Adminnetz darf zugreifen
VPN-Dienstleister	nur benötigte Ziele und Ports
Backup-Server	kein normaler Benutzerzugriff

Situation	Sichere Grundidee
DNS	Clientnetz zu DNS-Server UDP/TCP 53
RDP	nicht direkt aus Internet
SMB	nicht breit zwischen allen Netzen
temporäre Regel	Ablaufdatum und Verantwortlichen dokumentieren

Mini-Prüfung: typische Fehlerbilder

Fehlerbild	Wahrscheinliches Thema
Zugriff trotz Block-Regel möglich	Regelreihenfolge, falsches Matching
Zugriff trotz Allow-Regel nicht möglich	Regelreihenfolge, Zone, Port, NAT, lokale Firewall
nur ein Port funktioniert nicht	Firewall-Regel oder Dienst
DMZ-Server erreicht internes Ziel nicht	DMZ-zu-intern-Regel fehlt
Gastnetz erreicht interne Server	Zonentrennung fehlerhaft
VPN-Benutzer sieht alles	Least Privilege fehlt
Datenbank aus Internet erreichbar	kritische Fehlkonfiguration
Backup-Speicher für Clients offen	Ransomware-Risiko
Firewall-Regel unbekannter Zweck	Dokumentationsproblem
Deny im Log	Firewall blockiert konkret

Typische Prüfungsfallen

Falle	Richtig denken
Portnummer ohne TCP/UDP	unvollständig
Quelle und Ziel vergessen	Regel nicht prüfungssicher
Any-to-Any als einfache Lösung	Sicherheitsrisiko
DMZ mit internem Netz gleichsetzen	falsch, DMZ ist getrennte Zone
VLAN ersetzt Firewall	falsch, VLAN trennt nur Layer 2
NAT ersetzt Firewall	falsch, NAT übersetzt
RDP direkt ins Internet	hohes Risiko
Datenbank öffentlich	hohes Risiko
Gastnetz darf intern zugreifen	falsch
temporäre Regel bleibt dauerhaft	Regelwerksrisiko

IHK-sichere Kurzformulierung

Eine Firewall filtert Netzwerkverkehr anhand von Regeln. Eine vollständige Regel enthält Quelle, Ziel, Protokoll, Port, Richtung, Aktion und Zweck. Nach dem Default-Deny-Prinzip wird Verkehr standardmäßig blockiert und nur gezielt erlaubt. Any-to-Any-Regeln sind kritisch, weil sie Verkehr von jeder Quelle zu jedem Ziel erlauben, Sicherheitszonen umgehen und die Angriffsfläche erhöhen. Öffentlich erreichbare Dienste sollten in einer DMZ betrieben werden. Zugriffe aus der DMZ ins interne Netz müssen minimal und zweckgebunden erlaubt werden. Management-, Gast-, VPN- und Backup-Netze benötigen besonders klare Zugriffsbeschränkungen. Firewall-Logs, Regelreihenfolge und Dokumentation sind wichtig für Fehlersuche und Sicherheit.

Merksätze

Firewall filtert Verkehr.

NAT übersetzt Adressen.

VLAN trennt Layer 2.

Firewall kontrolliert Verkehr zwischen Zonen.

Default Deny ist sicherer als Default Allow.

Erst blockieren,
dann gezielt erlauben.

Any-to-Any ist kritisch.

Jede Regel braucht Quelle.

Jede Regel braucht Ziel.

Jede Regel braucht Protokoll.

Jede Regel braucht Port.

Jede Regel braucht Aktion.

Jede Regel braucht Zweck.

Portnummer ohne TCP oder UDP ist unvollständig.

DMZ trennt öffentliche Dienste vom internen Netz.

DMZ zu intern nur minimal erlauben.

Gastnetz nicht ins interne Netz lassen.

Managementnetz besonders schützen.

VPN-Zugriff nach Least Privilege.

Backup-Systeme besonders schützen.

RDP nicht direkt ins Internet.

SMB nicht breit freigeben.

Datenbanken nicht öffentlich erreichbar machen.

Regelreihenfolge beachten.

Firewall-Logs auswerten.

Temporäre Regeln mit Ablaufdatum dokumentieren.

Unbenutzte Regeln entfernen.

Gute Firewall-Antwort:
Risiko,
Regel,
Wirkung.