11.5 Fehlersuche bei Firewalls, NAT und DMZ

Bei Problemen mit Firewalls, NAT und DMZ reicht es nicht, nur zu prüfen, ob ein Server grundsätzlich erreichbar ist.

Man muss die komplette Verbindungskette prüfen:

```
Client
DNS
Routing
Firewall-Regel
NAT-Regel
Zielsystem
Dienst
Rückweg
Logs
```

Merksatz:

```
Firewall-Fehlersuche bedeutet:
Quelle, Ziel, Port, Richtung, NAT und Logs prüfen.
```

Grundidee der Fehlersuche

Bei Firewall- und NAT-Problemen ist die wichtigste Frage:

```
Wo wird der Verkehr unterbrochen?
```

Dazu prüft man Schritt für Schritt:

```
Kommt die Anfrage beim richtigen Ziel an?
Wird sie erlaubt oder blockiert?
Wird sie richtig übersetzt?
Antwortet der Dienst?
Kommt die Antwort zurück?
```

Merksatz:

Nicht raten,
sondern den Weg der Verbindung nachvollziehen.

Die wichtigsten Angaben vor der Fehlersuche

Vor der Fehlersuche braucht man genaue Informationen.

Wichtige Fragen:

Wer ist die Quelle?
Was ist das Ziel?
Welcher Dienst wird genutzt?
Welcher Port wird genutzt?
TCP oder UDP?
In welche Richtung geht die Verbindung?
Intern oder extern?
Gibt es NAT?
Gibt es eine DMZ?
Gibt es einen Reverse Proxy?
Welche Fehlermeldung erscheint?

Merksatz:

Ohne Quelle,
Ziel,
Port
und Richtung ist Firewall-Fehlersuche ungenau.

Quelle bestimmen

Die Quelle ist das System, das die Verbindung startet.

Beispiele:

Client im LAN
externer Benutzer im Internet
Server in der DMZ
VPN-Client

Monitoring-Server
Admin-PC
Anwendungssystem

Wichtig:

Die tatsächliche Quell-IP kann durch NAT verändert werden.

Merksatz:

Quelle = wer startet die Verbindung?

Ziel bestimmen

Das Ziel ist das System oder der Dienst, der erreicht werden soll.

Beispiele:

Webserver
Datenbankserver
Reverse Proxy
Mailgateway
DNS-Server
SMB-Freigabe
VPN-Gateway
RDP-Server

Wichtig:

Bei DNS-Namen muss geprüft werden,
auf welche IP-Adresse der Name wirklich zeigt.

Merksatz:

Ziel = welches System soll erreicht werden?

Port und Protokoll bestimmen

Ein Port allein reicht nicht.

Man muss auch wissen:

> TCP oder UDP?

Beispiele:

Dienst	Protokoll
HTTPS	TCP 443
DNS	UDP/TCP 53
NTP	UDP 123
SMB	TCP 445
SSH	TCP 22
RDP	TCP 3389
SNMP	UDP 161
HTTP/3	UDP 443

Merksatz:

> TCP 443 und UDP 443 sind unterschiedliche Dinge.

Richtung bestimmen

Firewall-Regeln sind richtungsabhängig.

Beispiele:

> LAN → WAN
> WAN → DMZ
> DMZ → LAN
> VPN → Servernetz
> Managementnetz → DMZ
> Gastnetz → Internet

Ein häufiger Fehler ist, eine Regel in der falschen Richtung anzulegen.

Merksatz:

Regelrichtung nach dem Verbindungsaufbau bestimmen.

Zonen bestimmen

Viele Firewalls arbeiten mit Zonen.

Beispiele:

LAN
WAN
DMZ
VPN
Gastnetz
IoT-Netz
Servernetz
Managementnetz

Eine Regel muss zur richtigen Zone passen.

Beispiel:

WAN → DMZ ist nicht dasselbe wie DMZ → WAN.

Merksatz:

Firewall-Regeln gelten zwischen Zonen oder Interfaces.

DNS zuerst prüfen

Viele vermeintliche Firewall-Probleme sind eigentlich DNS-Probleme.

Beispiele:

Domain zeigt auf falsche öffentliche IP.
Interner DNS zeigt auf externe IP.
Split DNS ist falsch.
DNS-Cache enthält alten Eintrag.
AAAA-Record zeigt auf nicht erreichbare IPv6-Adresse.

CNAME zeigt auf falschen Namen.

Merksatz:

Falsche DNS-Auflösung führt zur falschen Zieladresse.

Routing prüfen

Firewall-Regeln helfen nicht, wenn kein gültiger Weg zum Ziel existiert.

Zu prüfen:

Gibt es eine Route zum Zielnetz?
Gibt es einen Rückweg?
Ist das richtige Gateway eingetragen?
Geht der Rückverkehr über dieselbe Firewall?
Gibt es asymmetrisches Routing?
Ist ein VPN-Routing beteiligt?

Merksatz:

Routing bestimmt den Weg,
Firewall erlaubt oder blockiert ihn.

NAT prüfen

Wenn NAT beteiligt ist, muss geprüft werden:

Wird die richtige Quelladresse übersetzt?
Wird die richtige Zieladresse übersetzt?
Stimmt der externe Port?
Stimmt der interne Port?
Stimmt TCP oder UDP?
Zeigt NAT auf das richtige interne Ziel?
Gibt es mehrere NAT-Regeln?
Greift eine alte Regel vorher?

Merksatz:

NAT-Fehler entstehen oft durch falsches Ziel,
falschen Port
oder falsche Reihenfolge.

Firewall-Regel prüfen

Bei der Firewall-Regel prüft man:

Quelle korrekt?
Ziel korrekt?
Dienst korrekt?
Protokoll korrekt?
Port korrekt?
Richtung korrekt?
Zone korrekt?
Regel aktiv?
Regel an richtiger Position?
Logging aktiv?
Wird die Regel überhaupt getroffen?

Merksatz:

Die tatsächlich getroffene Regel ist wichtiger als die gedachte Regel.

Regelreihenfolge prüfen

Viele Firewalls arbeiten von oben nach unten.

Die erste passende Regel entscheidet.

Problem:

Eine allgemeine Blockregel kann eine spätere Erlaubnisregel verdecken.

Beispiel:

Regel 1:
DMZ → LAN any blockieren

Regel 2:
DMZ-Webserver → DB-Server TCP 5432 erlauben

Wenn Regel 1 zuerst greift, funktioniert Regel 2 nicht.

Merksatz:

Spezifische Erlaubnis vor allgemeine Blockregel setzen.

Logs prüfen

Firewall-Logs sind bei der Fehlersuche besonders wichtig.

Sie zeigen:

Quelle
Ziel
Port
Protokoll
Aktion
Regelname
Zeit
Interface
Zone
NAT-Übersetzung

Typische Aktionen im Log:

allowed
denied
dropped
rejected

Merksatz:

Logs zeigen,
ob die Firewall erlaubt oder blockiert.

Keine Logs sichtbar

Wenn keine Logs sichtbar sind, kann das bedeuten:

```
Verkehr kommt gar nicht bei der Firewall an.
Falsche Firewall wird geprüft.
Falsches Interface wird geprüft.
Logging ist für Regel deaktiviert.
DNS zeigt auf anderes Ziel.
Routing geht anderen Weg.
Client sendet gar keine Anfrage.
Provider oder vorgeschaltetes Gerät blockiert.
```

Merksatz:

```
Kein Logeintrag heißt nicht automatisch:
Firewall ist nicht beteiligt.
```

Dienst auf Zielsystem prüfen

Wenn Firewall und NAT korrekt aussehen, muss der Dienst selbst geprüft werden.

Fragen:

```
Läuft der Dienst?
Lauscht der Dienst auf dem richtigen Port?
Lauscht der Dienst auf der richtigen IP-Adresse?
Blockiert die Host-Firewall?
Gibt es Anwendungslogs?
Antwortet der Dienst korrekt?
Ist das Zertifikat passend?
Ist die Anwendung richtig konfiguriert?
```

Merksatz:

```
Erlaubter Port heißt nicht,
dass der Dienst funktioniert.
```

Host-Firewall prüfen

Neben der zentralen Firewall kann auch das Zielsystem selbst blockieren.

Beispiele:

```
Windows Defender Firewall
Linux nftables
iptables
ufw
firewalld
lokale Sicherheitssoftware
Cloud Security Group
```

Typisches Fehlerbild:

```
Netzwerkfirewall erlaubt,
aber Zielsystem lehnt ab oder antwortet nicht.
```

Merksatz:

```
Auch die lokale Firewall des Zielsystems prüfen.
```

Rückweg prüfen

Eine Verbindung braucht Hinweg und Rückweg.

Wenn der Rückweg fehlt, funktioniert die Verbindung nicht.

Mögliche Ursachen:

```
falsches Gateway
falsche Route
asymmetrisches Routing
NAT-Zuordnung fehlt
Antwort geht an falsche Firewall
Zielsystem antwortet über anderes Interface
```

Merksatz:

Verbindung funktioniert nur,

wenn Anfrage und Antwort den passenden Weg haben.

Asymmetrisches Routing

Asymmetrisches Routing bedeutet:

Hinweg und Rückweg laufen über unterschiedliche Wege.

Bei Stateful Firewalls ist das problematisch, weil die Firewall den Verbindungszustand nur auf einem Weg sieht.

Folge:

Antwortpakete können als ungültig blockiert werden.

Merksatz:

Stateful Firewalls brauchen zusammenpassenden Hin- und Rückweg.

Typisches Szenario: Externer Webdienst nicht erreichbar

Beispiel:

Benutzer im Internet kann https://wiki.firma.de nicht öffnen.

Prüfreihenfolge:

1. DNS zeigt auf richtige öffentliche IP?
2. Öffentliche IP gehört wirklich zum Anschluss?
3. Kein CGNAT?
4. Portweiterleitung TCP 443 korrekt?
5. Firewall-Regel WAN → DMZ oder WAN → Reverse Proxy korrekt?
6. Reverse Proxy erreichbar?
7. Backend erreichbar?
8. Zertifikat gültig?
9. Webserver-Logs prüfen.

10. Firewall-Logs prüfen.

Merksatz:

Öffentlicher Webdienst braucht DNS,
NAT,
Firewall,
Proxy,
Backend
und Zertifikat.

Typisches Szenario: Intern funktioniert, extern nicht

Wenn ein Dienst intern funktioniert, aber extern nicht, liegen Ursachen oft bei:

externem DNS
öffentlicher IP
Portweiterleitung
Firewall-Regel WAN → DMZ
CGNAT
Providerblockade
Reverse Proxy
Zertifikat
Dienstbindung nur auf interne IP

Merksatz:

Intern funktioniert,
extern nicht:
externe Erreichbarkeit prüfen.

Typisches Szenario: Extern funktioniert, intern nicht

Wenn ein Dienst extern funktioniert, aber intern über denselben Namen nicht, liegen Ursachen oft bei:

```
Hairpin NAT fehlt
Split DNS fehlt
internes DNS zeigt falsch
interne Firewall blockiert
Zertifikat passt intern nicht
interner Client geht falschen Weg
```

Merksatz:

```
Extern funktioniert,
intern nicht:
Hairpin NAT oder Split DNS prüfen.
```

Typisches Szenario: Portweiterleitung funktioniert nicht

Mögliche Ursachen:

```
- falsche öffentliche IP
- CGNAT
- Double NAT
- NAT-Regel fehlt
- NAT-Regel zeigt auf falschen Host
- falscher externer Port
- falscher interner Port
- TCP/UDP verwechselt
- Firewall-Regel fehlt
- Host-Firewall blockiert
- Dienst läuft nicht
- DNS zeigt falsch
- Test aus internem Netz ohne Hairpin NAT
```

Merksatz:

```
Portweiterleitung braucht korrekte öffentliche IP,
NAT,
Firewall
und Dienst.
```

Typisches Szenario: 502 Bad Gateway

Ein 502-Fehler tritt häufig bei Reverse Proxys auf.

Mögliche Ursachen:

```
Backend läuft nicht.
Backend-Port falsch.
Backend-Protokoll falsch.
DNS-Name des Backends falsch.
Container oder Server nicht erreichbar.
Firewall blockiert Proxy → Backend.
Backend antwortet ungültig.
TLS zum Backend falsch konfiguriert.
```

Merksatz:

```
502 bedeutet oft:
Proxy erreicht Backend nicht korrekt.
```

Typisches Szenario: Zugriff auf Datenbank aus DMZ geht nicht

Beispiel:

```
Webserver in DMZ soll Datenbank im Servernetz erreichen.
```

Prüfen:

```
Quelle:
Webserver in DMZ

Ziel:
Datenbankserver im Servernetz

Dienst:
Datenbankport

Richtung:
DMZ → Servernetz
```

Zusätzlich:
Datenbankdienst läuft?
Datenbank lauscht auf richtiger IP?
Host-Firewall erlaubt?
Benutzerrechte in Datenbank korrekt?
Rückweg vorhanden?

Merksatz:

Datenbankzugriff aus DMZ braucht enge,
gezielte Regeln.

Typisches Szenario: VPN-Benutzer erreicht internen Server nicht

Mögliche Ursachen:

- VPN-Verbindung nicht korrekt aufgebaut
- VPN-Client bekommt falsche IP
- Route zum internen Netz fehlt
- Firewall-Regel VPN → Servernetz fehlt
- DNS für interne Namen fehlt
- Split Tunnel falsch
- Zielserver-Firewall blockiert
- Benutzergruppe nicht berechtigt
- NAT im VPN falsch

Merksatz:

VPN-Probleme mit Adresse,
Route,
DNS,
Firewall
und Berechtigung prüfen.

Typisches Szenario: Gastnetz erreicht LAN

Das ist ein Sicherheitsproblem.

Mögliche Ursachen:

- Firewall-Regel zu offen
- falsche Zonen-Zuordnung
- VLAN falsch konfiguriert
- Gastnetz und LAN im selben Netz
- Any-Any-Regel
- Routing ohne Filter
- alte Testregel vergessen

Merksatz:

Gastnetz darf nicht ins interne LAN führen.

Typisches Szenario: IoT-Geräte erreichen interne Server

Auch das kann ein Risiko sein.

Mögliche Ursachen:

- IoT-Netz nicht getrennt
- Firewall-Regel zu breit
- Geräte im falschen VLAN
- mDNS oder Broadcast-Freigaben unkontrolliert
- Any-Regel aktiv
- fehlende Segmentierung

Besser:

IoT → Internet nur nötig
IoT → LAN blockieren
Admin-Netz → IoT gezielt erlauben

Merksatz:

IoT-Geräte nur kontrolliert kommunizieren lassen.

Typisches Szenario: DNS funktioniert nicht

Mögliche Ursachen:

- UDP 53 blockiert
- TCP 53 blockiert
- falscher DNS-Server
- DNS-Server nicht erreichbar
- Firewall erlaubt nur externe DNS
- interne DNS-Zone fehlt
- Split DNS falsch
- DNS-Cache veraltet
- DHCP verteilt falschen DNS

Merksatz:

DNS braucht je nach Fall UDP und TCP 53.

Typisches Szenario: NTP funktioniert nicht

Mögliche Ursachen:

- UDP 123 blockiert
- falscher Zeitserver
- DNS zum Zeitserver fehlerhaft
- Zeitabweichung zu groß
- NTP-Dienst läuft nicht
- Firewall erlaubt nur TCP statt UDP
- VM-Zeitquelle widerspricht NTP

Folgeprobleme:

Zertifikatsfehler
Kerberos-Probleme
falsche Logs
Monitoringfehler

Merksatz:

NTP-Probleme können viele Folgefehler erzeugen.

Typisches Szenario: RDP funktioniert nicht

Mögliche Ursachen:

- TCP 3389 blockiert
- RDP am Zielsystem deaktiviert
- Benutzer nicht berechtigt
- Zielsystem ausgeschaltet
- VPN nicht verbunden
- Firewall-Regel fehlt
- Host-Firewall blockiert
- NLA-Problem
- DNS zeigt falsch

Sicherheit:

RDP nicht direkt aus dem Internet veröffentlichen.

Merksatz:

RDP besser über VPN oder Gateway nutzen.

Typisches Szenario: SSH funktioniert nicht

Mögliche Ursachen:

- TCP 22 blockiert
- SSH-Dienst läuft nicht
- SSH läuft auf anderem Port
- falscher Benutzer
- falscher Schlüssel
- Passwortlogin deaktiviert
- Host-Firewall blockiert
- Zugriff nur aus Managementnetz erlaubt
- Fail2ban blockiert Quelle

Merksatz:

```
SSH mit Port,
Dienst,
Benutzer,
Schlüssel
und Firewall prüfen.
```

Typisches Szenario: Mailserver empfängt keine Mails

Mögliche Ursachen:

```
- MX-Record falsch
- DNS zeigt falsch
- TCP 25 blockiert
- NAT-Regel fehlt
- Firewall-Regel fehlt
- Mailgateway down
- Spamfilter lehnt ab
- Zertifikat oder TLS-Problem
- Provider blockiert Port 25
- Mailserver nicht zuständig für Domain
```

Merksatz:

```
Mail-Empfang braucht MX,
DNS,
SMTP,
Firewall
und Mailserverkonfiguration.
```

Typisches Szenario: Anwendung funktioniert nur teilweise

Mögliche Ursachen:

```
- Hauptport erlaubt,
  Zusatzport fehlt

- API erreichbar,
```

Datenbank nicht erreichbar

- Weboberfläche erreichbar,
  WebSocket blockiert

- DNS erlaubt,
  NTP blockiert

- FTP-Login geht,
  Datenports fehlen

- Authentifizierung geht,
  LDAP-Gruppenabfrage blockiert

Merksatz:

> Manche Anwendungen brauchen mehr als nur einen Port.

TCP und UDP nicht verwechseln

Ein häufiger Fehler ist, nur den Port zu betrachten.

Beispiele:

> DNS kann UDP 53 und TCP 53 brauchen.
>
> NTP nutzt UDP 123,
> nicht TCP 123.
>
> SNMP nutzt UDP 161,
> nicht TCP 161.
>
> HTTP/3 nutzt UDP 443,
> während HTTPS klassisch TCP 443 nutzt.

Merksatz:

> Portnummer ohne Protokoll ist unvollständig.

ICMP bei Fehlersuche

ICMP wird oft für Diagnose genutzt.

Beispiele:

```
Ping
Traceroute
Ziel nicht erreichbar
Time Exceeded
Fragmentierung nötig
```

ICMP komplett zu blockieren, kann Fehlersuche erschweren und Netzwerkprobleme verdecken.

Merksatz:

```
ICMP ist mehr als Ping.
```

Ping reicht nicht aus

Ping zeigt nur, ob ICMP-Echo funktioniert.

Ping sagt nicht:

```
ob TCP 443 offen ist
ob HTTP funktioniert
ob Anmeldung klappt
ob DNS korrekt ist
ob Zertifikat passt
ob Anwendung gesund ist
```

Merksatz:

```
Ping ist nur ein erster Hinweis,
kein vollständiger Diensttest.
```

Porttest reicht nicht aus

Ein erfolgreicher Porttest zeigt:

Zielport ist erreichbar.

Er zeigt nicht automatisch:

Anwendung antwortet korrekt
Authentifizierung klappt
Datenformat stimmt
Zertifikat passt
Reverse Proxy leitet richtig weiter
Benutzer hat Rechte

Merksatz:

Offener Port heißt nicht:
Anwendung funktioniert.

Typische Testwerkzeuge

Werkzeug	Zweck
ping	einfache Erreichbarkeit prüfen
traceroute / tracert	Weg zum Ziel prüfen
nslookup	DNS prüfen
dig	DNS detaillierter prüfen
curl	HTTP/HTTPS/API testen
nc	TCP/UDP-Port testen
Test-NetConnection	Windows-Porttest
openssl s_client	TLS-Zertifikat prüfen
tcpdump	Paketmitschnitt
Wireshark	Paketmitschnitt analysieren
Firewall-Log	erlaubten oder blockierten Verkehr prüfen
Serverlog	Dienstfehler prüfen

Merksatz:

Werkzeug nach Fragestellung auswählen.

Paketmitschnitt

Ein Paketmitschnitt kann zeigen, ob Verkehr wirklich ankommt.

Man sieht zum Beispiel:

```
ARP
DNS
TCP-Handshake
TLS-Handshake
ICMP
DHCP
Wiederholungen
Timeouts
Reset-Pakete
```

Wichtig:

```
Bei TLS sieht man den Inhalt nicht einfach im Klartext.
```

Merksatz:

```
Paketmitschnitt zeigt den echten Verkehr.
```

TCP-Handshake prüfen

Bei TCP ist der Verbindungsaufbau wichtig.

Vereinfacht:

```
SYN
SYN-ACK
ACK
```

Fehlerbilder:

```
Nur SYN:
Ziel antwortet nicht oder Firewall blockiert.
```

SYN und RST:
Ziel lehnt aktiv ab oder Dienst nicht offen.

SYN, SYN-ACK, ACK:
TCP-Verbindung wurde aufgebaut.

Merksatz:

TCP-Handshake zeigt,
ob eine TCP-Verbindung entsteht.

Timeout

Timeout bedeutet:

Es kommt keine Antwort innerhalb der erwarteten Zeit.

Mögliche Ursachen:

- Firewall droppt Pakete
- Routingproblem
- Ziel nicht erreichbar
- Dienst antwortet nicht
- Rückweg fehlt
- Paket geht an falsches Ziel
- Provider blockiert

Merksatz:

Timeout bedeutet oft:
keine oder keine passende Antwort.

Connection Refused

Connection refused bedeutet:

```
Zielsystem ist erreichbar,
aber der Dienst nimmt auf dem Port keine Verbindung an.
```

Mögliche Ursachen:

```
- Dienst läuft nicht
- falscher Port
- Dienst lauscht nur lokal
- Host-Firewall lehnt aktiv ab
- Anwendung nicht gestartet
```

Merksatz:

```
Connection refused deutet auf Zielsystem oder Dienst hin.
```

Reset

Ein TCP Reset beendet oder verweigert eine Verbindung aktiv.

Mögliche Ursachen:

```
- Dienst lehnt Verbindung ab
- Firewall sendet Reset
- Anwendung beendet Verbindung
- falsches Protokoll auf Port
- Sicherheitsregel greift
```

Merksatz:

```
Reset ist eine aktive Ablehnung oder Beendigung.
```

Fehlersuche mit Logs kombinieren

Am besten kombiniert man:

```
Client-Fehler
DNS-Ergebnis
```

Porttest
Firewall-Log
NAT-Log
Serverlog
Anwendungstest

Beispiel:

Client meldet Timeout.
Firewall-Log zeigt Drop.
Ursache:
Firewall-Regel fehlt oder blockiert.

Oder:

Client meldet 502.
Firewall erlaubt.
Reverse-Proxy-Log zeigt Backend nicht erreichbar.
Ursache:
Backend oder interne Regel prüfen.

Merksatz:

Mehrere Hinweise zusammen ergeben die Ursache.

Fehler nach Änderung

Wenn ein Problem direkt nach einer Änderung auftritt, prüft man zuerst diese Änderung.

Beispiele:

neue Firewall-Regel
NAT geändert
DNS geändert
Zertifikat erneuert
Reverse Proxy angepasst
Dienst neu gestartet
Server-IP geändert

VLAN geändert
VPN-Gruppe geändert
Update installiert

Merksatz:

Nach Änderung zuerst Änderung prüfen.

Änderungen dokumentieren

Firewall- und NAT-Änderungen sollten dokumentiert werden.

Wichtige Angaben:

- Datum
- Zweck
- Quelle
- Ziel
- Port
- Protokoll
- Richtung
- NAT-Ziel
- Verantwortlicher
- Ticket
- Testergebnis
- Rollback-Möglichkeit

Merksatz:

Gute Dokumentation verkürzt spätere Fehlersuche.

Rollback

Rollback bedeutet:

Änderung zurücknehmen,
wenn sie Probleme verursacht.

Bei Firewall-Änderungen wichtig:

```
vorherigen Zustand kennen
Backup der Konfiguration haben
Wartungsfenster beachten
Zugriff auf Firewall nicht selbst aussperren
Notfallzugang sichern
```

Merksatz:

```
Vor kritischen Änderungen Rückweg planen.
```

Sich nicht selbst aussperren

Bei Firewall-Änderungen kann man sich selbst den Zugriff nehmen.

Beispiele:

```
Admin-Regel gelöscht.
Managementnetz blockiert.
VPN-Regel falsch gesetzt.
Weboberfläche der Firewall nicht mehr erreichbar.
```

Vorbeugung:

```
Konfiguration sichern.
lokalen Zugriff bereithalten.
Änderung mit Zeitplan oder Rollback absichern.
Managementzugriff nicht ungetestet ändern.
```

Merksatz:

```
Managementzugriff besonders vorsichtig ändern.
```

Checkliste: Firewall-Fehlersuche

1. Fehlerbild genau aufnehmen.
2. Quelle bestimmen.
3. Ziel bestimmen.
4. Port und Protokoll bestimmen.
5. Richtung und Zone bestimmen.
6. DNS prüfen.
7. Routing prüfen.
8. NAT prüfen.
9. Firewall-Regel prüfen.
10. Regelreihenfolge prüfen.
11. Firewall-Logs prüfen.
12. Zielsystem-Firewall prüfen.
13. Dienststatus prüfen.
14. Anwendung testen.
15. Rückweg prüfen.
16. letzte Änderungen prüfen.
17. Ergebnis dokumentieren.

Merksatz:

Firewall-Fehlersuche ist eine Kette,
kein einzelner Test.

Was man nicht vorschnell tun sollte

Nicht sofort:

Any-Any-Regel erstellen.
Firewall komplett deaktivieren.
alle Ports öffnen.
DMZ ins LAN freigeben.
Adminport ins Internet öffnen.
Logs ignorieren.
DNS ungeprüft lassen.
NAT und Firewall verwechseln.

Warum?

Solche Maßnahmen können Sicherheitslücken erzeugen
und die eigentliche Ursache verdecken.

Merksatz:

Nicht Sicherheit opfern,
nur um schnell einen Test zu machen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Wie geht man bei Firewall-Fehlersuche systematisch vor?
- Warum reichen Ping und Porttest nicht aus?
- Warum muss man Quelle, Ziel, Port und Richtung kennen?
- Warum ist DNS bei Firewallproblemen relevant?
- Warum muss NAT zusätzlich zur Firewall geprüft werden?
- Warum kann eine Portweiterleitung trotz NAT-Regel nicht funktionieren?
- Was bedeutet Timeout?
- Was bedeutet Connection Refused?
- Was ist asymmetrisches Routing?
- Warum sind Firewall-Logs wichtig?
- Warum können interne und externe Tests unterschiedliche Ergebnisse liefern?
- Warum sollte man nicht einfach Any-Any erlauben?
- Warum ist Dokumentation bei Firewall-Regeln wichtig?

Typische Prüfungsfallen

Ping prüft nicht den Dienst.

Porttest prüft nicht die Anwendung.

DNS kann wie ein Firewallproblem wirken.

NAT-Regel ist nicht Firewall-Regel.

Firewall-Regel ist nicht NAT-Regel.

TCP und UDP nicht verwechseln.

Regelrichtung beachten.

Zone beachten.

Regelreihenfolge beachten.

Rückweg beachten.

Stateful Firewalls brauchen Verbindungszustand.

Asymmetrisches Routing kann Verbindungen stören.

Timeout und Connection Refused bedeuten nicht dasselbe.

Host-Firewall zusätzlich prüfen.

Dienst muss wirklich laufen.

Logs sind zentrale Hinweise.

Keine Any-Any-Regel als Dauerlösung.

Änderungen dokumentieren.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Quelle	System, das Verbindung startet
Ziel	System, das erreicht werden soll
Richtung	Weg zwischen Zonen oder Interfaces
Zone	Sicherheitsbereich der Firewall
NAT	Adressübersetzung
PAT	Port- und Adressübersetzung
Portweiterleitung	externer Port wird intern weitergeleitet

Begriff	Kurze Erklärung
Rückweg	Antwortweg zurück zur Quelle
asymmetrisches Routing	Hin- und Rückweg sind unterschiedlich
Timeout	keine Antwort innerhalb der Zeit
Connection Refused	Ziel lehnt Verbindung aktiv ab
TCP Reset	aktive Verbindungsbeendigung
Firewall-Log	Protokoll erlaubter oder blockierter Verbindungen
Host-Firewall	Firewall auf dem Zielsystem
Hairpin NAT	interner Zugriff über öffentliche Adresse
Split DNS	intern und extern unterschiedliche DNS-Antwort
CGNAT	Provider-NAT, oft ohne eingehende Ports
Rollback	Änderung zurücknehmen
Any-Any	sehr breite Erlaubnisregel

IHK-sichere Kurzformulierung

Bei der Fehlersuche an Firewalls, NAT und DMZ müssen Quelle, Ziel, Port, Protokoll, Richtung und Zone genau bestimmt werden. Zusätzlich sind DNS, Routing, NAT-Regeln, Firewall-Regeln, Regelreihenfolge, Host-Firewall, Dienststatus, Rückweg und Logs zu prüfen. Eine NAT-Regel übersetzt Adressen oder Ports, ersetzt aber keine Firewall-Regel. Ein erfolgreicher Ping oder ein offener Port beweist nicht, dass der Anwendungdienst korrekt funktioniert. Typische Ursachen für Fehler sind falsche DNS-Einträge, fehlende Portweiterleitungen, blockierende Firewall-Regeln, falsche Richtung, TCP/UDP-Verwechslung, fehlender Rückweg, CGNAT, Double NAT oder ein nicht laufender Dienst.

Merksätze

Erst Quelle bestimmen.

Dann Ziel bestimmen.

Dann Port und Protokoll bestimmen.

Dann Richtung und Zone prüfen.

DNS zuerst nicht vergessen.

Routing findet den Weg.

Firewall erlaubt oder blockiert den Weg.

NAT übersetzt Adressen oder Ports.

NAT ersetzt keine Firewall-Regel.

Firewall-Regel ersetzt keine NAT-Regel.

TCP und UDP nicht verwechseln.

Regelreihenfolge beachten.

Spezifisch vor allgemein.

Logs zeigen,
welche Regel greift.

Kein Log kann bedeuten,
dass Verkehr gar nicht ankommt.

Host-Firewall zusätzlich prüfen.

Dienst muss wirklich laufen.

Rückweg muss stimmen.

Timeout bedeutet:
keine passende Antwort.

Connection Refused bedeutet:
Ziel lehnt aktiv ab.

Ping reicht nicht aus.

Porttest reicht nicht aus.

Offener Port heißt nicht:
Anwendung funktioniert.

Intern und extern getrennt testen.

Hairpin NAT oder Split DNS bei internen Tests beachten.

CGNAT kann Portweiterleitungen verhindern.

Any-Any nicht als schnelle Dauerlösung verwenden.

Änderungen dokumentieren.

Vor kritischen Änderungen Rollback planen.