3.1 Störungsumfang und Kommunikationsweg bestimmen*

Bevor einzelne Netzwerkprotokolle, Firewallregeln oder Server untersucht werden, muss der Umfang der Störung bestimmt werden. Dadurch lässt sich erkennen, ob die Ursache wahrscheinlich auf einem Endgerät, in einem Netzsegment, an einer zentralen Komponente oder am Zielsystem liegt.

Danach wird der erwartete Kommunikationsweg vom betroffenen Client bis zum Ziel dokumentiert.

> **Grundregel:** Erst bestimmen, wer betroffen ist und welchen Weg die Kommunikation nehmen soll. Danach Messungen an den beteiligten Komponenten durchführen.

---

1. Welche Informationen müssen zuerst aufgenommen werden?

Information	Beispiel
Betroffener Benutzer	Max Mustermann
Betroffenes Gerät	`CLIENT-023`
Standort	Berlin
Verbindungsart	LAN
Fehlerbeginn	`2026-07-31 09:42 CEST`
Letzter funktionierender Zeitpunkt	`2026-07-31 09:35 CEST`
Zielanwendung	interne Webanwendung
Zielname	`app.example.intern`
Ziel-IP-Adresse	`192.0.2.20`
Zielport	TCP 443
Exakte Fehlermeldung	Verbindung wegen Zeitüberschreitung fehlgeschlagen
Reproduzierbarkeit	bei jedem Aufruf
Betroffene Benutzer	nur ein Benutzer bekannt
Kürzliche Änderung	VPN-Client wurde aktualisiert

Ungeeignete Fehlerbeschreibung

„Das Internet funktioniert nicht.“

Geeignete Fehlerbeschreibung

CLIENT-023 kann seit 09:42 Uhr die interne Anwendung
https://app.example.intern nicht öffnen. Der Browser meldet nach ungefähr
30 Sekunden eine Zeitüberschreitung. Andere Internetseiten sind erreichbar.
CLIENT-024 kann die interne Anwendung weiterhin öffnen.

Diese Beschreibung grenzt den Fehler bereits auf einen Client beziehungsweise dessen Kommunikationsweg ein.

2. Welche Fragen sollten der meldenden Person gestellt werden?

1. Was wollten Sie genau durchführen?
2. Welche Anwendung oder Adresse haben Sie verwendet?
3. Welche Fehlermeldung wird vollständig angezeigt?
4. Seit wann tritt der Fehler auf?
5. Hat die Funktion vorher auf demselben Gerät funktioniert?
6. Tritt der Fehler bei jedem Versuch auf?
7. Sind weitere Benutzer betroffen?
8. Funktionieren andere interne Anwendungen?
9. Funktionieren externe Internetseiten?
10. Besteht die Verbindung über LAN, WLAN oder VPN?
11. Wurde der Arbeitsplatz oder Standort gewechselt?
12. Wurde kurz vorher etwas aktualisiert oder verändert?
13. Funktioniert der Zugriff von einem anderen Gerät?
14. Funktioniert der Zugriff mit einem anderen Benutzerkonto?
15. Welche Auswirkung hat die Störung auf die Arbeit?

Wichtig

Die Fragen sollten möglichst konkrete und überprüfbare Antworten erzeugen.

Ungenau:
„Ist das Netzwerk langsam?“

Besser:
„Wie lange dauert der Aufruf normalerweise und wie lange dauert er jetzt?“

3. Wie wird der Störungsumfang bestimmt?

Prüffrage	Wenn ja	Wenn nein
Ist nur ein Benutzer betroffen?	Benutzerkonto, Profil und Berechtigungen prüfen	Umfang auf Geräte oder Gruppen erweitern
Ist nur ein Endgerät betroffen?	lokale Konfiguration, Adapter und Host-Firewall prüfen	gemeinsame Infrastruktur untersuchen
Ist nur ein Switchport betroffen?	Kabel, Port, VLAN und Port-Security prüfen	Switch oder VLAN weiter untersuchen
Ist nur ein VLAN betroffen?	Gateway, DHCP, ACL und VLAN-Konfiguration prüfen	übergeordnete Komponenten untersuchen
Ist nur ein Standort betroffen?	Standortverbindung, Firewall und lokales DNS prüfen	zentrale oder externe Ursache möglich
Ist nur ein Zielsystem betroffen?	Zielserver, Dienst, Port und Firewall prüfen	gemeinsamer Netzwerkpfad möglich
Ist nur ein bestimmter Port betroffen?	Dienst, Firewall und Transportprotokoll prüfen	grundlegende Erreichbarkeit untersuchen
Sind alle externen Ziele betroffen?	Internetzugang, NAT, Proxy oder Provider prüfen	zielbezogene Störung möglich
Sind alle internen Ziele betroffen?	lokales Gateway, Routing oder zentrale Firewall prüfen	einzelner Dienst oder Pfad betroffen
Sind alle Systeme betroffen?	zentrale Infrastruktur oder großflächige Störung prüfen	Fehler weiter eingrenzen

Mögliche Umfangsebenen

```
Benutzer
  → Gerät
    → Switchport
      → Access Switch
        → VLAN
          → Standort
            → Unternehmensnetz
              → Dienst
                → externer Anbieter
```

Je höher die gemeinsame betroffene Ebene liegt, desto wahrscheinlicher ist eine gemeinsame technische Ursache.

4. Welche Vergleichstests sind besonders aussagekräftig?

Test	Gleichbleibender Faktor	Veränderter Faktor	Mögliche Aussage
anderer Benutzer am selben Client	Gerät und Netzwerkpfad	Benutzerkonto	Benutzer- oder Berechtigungsproblem
gleicher Benutzer an anderem Client	Benutzer und Ziel	Endgerät	gerätebezogenes Problem
anderer Client am selben Anschluss	Switchport und Pfad	Endgerät	Endgerät oder Kabel eingrenzen
gleicher Client an anderem Anschluss	Client	Port und möglicherweise VLAN	Switchport oder Verkabelung
LAN statt WLAN	Client und Ziel	Zugangsnetz	WLAN-spezifisches Problem
WLAN statt LAN	Client und Ziel	Zugangsnetz	LAN-Port, Kabel oder VLAN
IP-Adresse statt DNS-Name	Client und Zielsystem	Namensauflösung	DNS-Problem möglich
anderes Ziel im selben Netz	Client und lokaler Pfad	Zielsystem	zielbezogene Störung
gleiches Ziel über anderen Port	Client und Ziel	Dienst beziehungsweise Port	port- oder dienstbezogen
ohne VPN statt mit VPN	Client und Ziel	Tunnel, Routen und VPN-DNS	VPN-spezifisches Problem

> Bei einem Vergleichstest sollte möglichst nur ein relevanter Faktor verändert werden. Werden gleichzeitig Benutzer, Gerät, Netzwerk und Standort gewechselt, ist das Ergebnis kaum eindeutig zuzuordnen.

5. Wie wird bestimmt, was weiterhin funktioniert?

Die funktionierenden Bereiche sind für die Eingrenzung genauso wichtig wie der eigentliche Fehler.

Beispiel

```
Funktioniert:
- Anmeldung am Client
```

- Zugriff auf andere interne Webanwendungen
- Zugriff auf externe Internetseiten
- DNS-Auflösung des betroffenen Zielnamens
- Ping zum Standardgateway

Funktioniert nicht:
- TCP-Verbindung zu app.example.intern auf Port 443

Daraus kann zunächst abgeleitet werden:

- der Client ist grundsätzlich betriebsbereit,
- die Netzwerkschnittstelle funktioniert zumindest teilweise,
- eine gültige IP-Kommunikation ist vorhanden,
- DNS funktioniert für den geprüften Namen,
- der Fehler betrifft möglicherweise den Zielport, den Dienst oder den spezifischen Kommunikationspfad.

Negativtest und Positivtest

Testart	Beispiel
Negativtest	betroffene Anwendung funktioniert nicht
Positivtest	andere Anwendung im selben Zielnetz funktioniert
Referenztest	anderer Client erreicht dieselbe Anwendung

Eine belastbare Eingrenzung verwendet möglichst alle drei Testarten.

6. Wie wird das Quellsystem eindeutig identifiziert?

Die Bezeichnung „mein Computer“ reicht für eine technische Analyse nicht aus.

Zu erfassen sind:

- Hostname,
- Betriebssystem,
- Benutzerkonto,
- Netzwerkschnittstelle,
- IP-Adresse und Präfix,
- MAC-Adresse,
- Standardgateway,
- DNS-Server,
- Verbindungsart,

- gegebenenfalls VLAN, VPN oder Proxy.

Windows

```
[RO] hostname
```

```
[RO] Get-ComputerInfo |
    Select-Object CsName,
                  WindowsProductName,
                  WindowsVersion,
                  OsBuildNumber
```

```
[RO] Get-NetIPConfiguration
```

```
[RO] Get-NetAdapter |
    Select-Object Name,
                  InterfaceDescription,
                  Status,
                  LinkSpeed,
                  MacAddress,
                  ifIndex
```

Linux

```
[RO] hostnamectl
```

```
[RO] ip -brief address
```

```
[RO] ip route
```

```
[RO] ip -brief link
```

macOS

```
[RO] scutil --get ComputerName
```

```
[RO] sw_vers
```

```
[RO] ifconfig
```

```
[RO] netstat -rn
```

```
[RO] networksetup -listallhardwareports
```

Die erfasste IP-Adresse muss der tatsächlich für die Zielverbindung verwendeten Schnittstelle zugeordnet werden. Ein System kann gleichzeitig LAN, WLAN, VPN, virtuelle Adapter und Containerinterfaces besitzen.

7. Wie wird das Zielsystem eindeutig bestimmt?

Ein Dienstname oder eine URL muss in seine technischen Bestandteile zerlegt werden.

Beispiel-URL

```
https://app.example.intern:8443/login
```

Bestandteil	Wert
Schema beziehungsweise Protokoll	HTTPS
Hostname	`app.example.intern`
expliziter Port	TCP 8443
Pfad	`/login`
erwartetes Zielsystem	Reverse Proxy oder Webserver
möglicher Backenddienst	Anwendungsserver
mögliche weitere Abhängigkeit	Datenbank oder Identitätsanbieter

Zu erfassen sind:

- vollständige URL oder Freigabe,

- Hostname,
- aufgelöste IP-Adresse beziehungsweise Adressen,
- Transportprotokoll,
- Port,
- erwarteter Server oder Load Balancer,
- Anwendungspfad,
- möglicherweise verwendeter Proxy,
- mögliche Backendabhängigkeiten.

Windows

```
[RO] Resolve-DnsName app.example.intern
```

```
[TEST] Test-NetConnection app.example.intern -Port 443
```

Linux

```
[RO] getent ahosts app.example.intern
```

```
[TEST] nc -vz app.example.intern 443
```

macOS

```
[RO] dscacheutil -q host -a name app.example.intern
```

```
[TEST] nc -vz app.example.intern 443
```

Ein Hostname kann mehrere IPv4- und IPv6-Adressen zurückgeben. Es muss dokumentiert werden, welche Adresse der Client beim fehlerhaften Versuch tatsächlich verwendet.

8. Wie wird der erwartete Kommunikationsweg gezeichnet?

Direkter Zugriff im lokalen Netz

```
CLIENT-023
192.0.2.10/24
```

```
  │
  ├─ Access Switch SW-01
  │    VLAN 20
  │
  └─ SERVER-01
     192.0.2.20/24
     TCP 443
```

Da Quelle und Ziel im selben IPv4-Subnetz liegen, ist normalerweise kein Router für die direkte Kommunikation erforderlich.

Zugriff in ein anderes internes Netz

```
CLIENT-023
192.0.2.10/24
  │
  ├─ Access Switch SW-01
  │    VLAN 20
  │
  ├─ Standardgateway
  │    192.0.2.1
  │
  ├─ Core Router oder Firewall
  │
  ├─ Server-VLAN 40
  │
  └─ APP-01
     198.51.100.20/24
     TCP 443
```

Zugriff über Reverse Proxy

```
Browser
  → DNS-Auflösung
    → Reverse Proxy TCP 443
      → TLS-Verarbeitung
        → Backend TCP 8080
          → Anwendung
```

```
        → Datenbank
```

Zugriff über VPN

```
Client
  → lokales Gateway
    → Internet
      → VPN-Gateway
        → verschlüsselter Tunnel
          → interne Route
            → interne Firewall
              → Zielserver
```

Zu jeder Verbindung sollte bekannt sein:

- welche Komponente als Nächstes angesprochen wird,
- welche Adresse sie besitzt,
- welches Protokoll und welcher Port verwendet werden,
- ob Adressen übersetzt werden,
- ob Daten verschlüsselt oder getunnelt werden,
- welche Komponente den Rückweg bestimmt.

9. Wie wird geprüft, welchen Weg das Betriebssystem verwenden möchte?

Windows – Route zu einem Ziel untersuchen

```
[RO] Find-NetRoute -RemoteIPAddress 198.51.100.20
```

Routingtabelle anzeigen:

```
[RO] Get-NetRoute -AddressFamily IPv4 |
    Sort-Object DestinationPrefix, RouteMetric |
    Format-Table ifIndex,
                 DestinationPrefix,
                 NextHop,
                 RouteMetric,
                 InterfaceMetric
```

Pfad verfolgen:

```
[TEST] tracert -d 198.51.100.20
```

Linux – ausgewählte Route anzeigen

```
[RO] ip route get 198.51.100.20
```

Beispielausgabe:

```
198.51.100.20 via 192.0.2.1 dev eth0 src 192.0.2.10
```

Feld	Bedeutung
`via 192.0.2.1`	nächster Router
`dev eth0`	verwendete Schnittstelle
`src 192.0.2.10`	ausgewählte Quelladresse

Pfad verfolgen:

```
[TEST] traceroute -n 198.51.100.20
```

macOS – ausgewählte Route anzeigen

```
[RO] route -n get 198.51.100.20
```

Pfad verfolgen:

```
[TEST] traceroute -n 198.51.100.20
```

> Traceroute zeigt nur antwortende Zwischenstationen. Firewalls und Router können die verwendeten Diagnosepakete verwerfen oder nicht beantworten. Ein Sternchen beweist daher nicht, dass genau dieser Hop den eigentlichen Anwendungsverkehr blockiert.

10. Wie wird bei mehreren Netzwerkschnittstellen die verwendete Schnittstelle bestimmt?

Ein Client kann gleichzeitig besitzen:

- Ethernet,
- WLAN,
- VPN,
- Mobilfunk,
- virtuelle Hypervisoradapter,
- Containerbridges,
- Loopback,
- Tunnelinterfaces.

Das Betriebssystem wählt den Weg anhand der Routingtabelle, der Präfixlänge und der Metrik.

Windows

Ausgewählte Route:

```
[RO] Find-NetRoute -RemoteIPAddress 198.51.100.20
```

Schnittstellenmetriken:

```
[RO] Get-NetIPInterface |
    Sort-Object AddressFamily, InterfaceMetric |
    Select-Object ifIndex,
                  InterfaceAlias,
                  AddressFamily,
                  ConnectionState,
                  InterfaceMetric
```

Linux

```
[RO] ip route get 198.51.100.20
```

Richtlinienregeln anzeigen:

```
[RO] ip rule show
```

Alle wichtigen Routingtabellen anzeigen:

```
[RO] ip route show table all
```

macOS

```
[RO] route -n get 198.51.100.20
```

Netzwerkdienstreihenfolge grafisch prüfen:

```
Systemeinstellungen
→ Netzwerk
→ Aktionsmenü
→ Reihenfolge der Dienste festlegen
```

Die sichtbare Dienstreihenfolge allein ersetzt nicht die Prüfung der tatsächlich ausgewählten Route.

11. Wie werden lokale und entfernte Ziele unterschieden?

Das Endgerät entscheidet anhand von IP-Adresse und Präfix beziehungsweise Subnetzmaske, ob das Ziel lokal erreichbar sein sollte.

Lokales Ziel

```
Quelle: 192.0.2.10/24
Ziel:   192.0.2.20
```

Beide Adressen gehören zum Netz:

```
192.0.2.0/24
```

Der Client versucht normalerweise, die MAC-Adresse des Zielsystems direkt zu ermitteln.

Entferntes Ziel

```
Quelle: 192.0.2.10/24
Ziel:   198.51.100.20
```

Das Ziel liegt außerhalb des lokalen Netzes. Der Client sendet das Paket normalerweise an einen Router beziehungsweise das passende Next Hop.

Bedeutung für die Fehleranalyse

Zieltyp	Erste technische Untersuchung
lokal	VLAN, ARP beziehungsweise Neighbor Discovery, Switchport
entfernt	Standardgateway, Route, Firewall und Rückweg
unklar	lokale IP-Konfiguration und Präfix zuerst prüfen

Eine falsche Subnetzmaske kann dazu führen, dass ein Client ein entferntes Ziel fälschlich für lokal hält oder ein lokales Ziel unnötig an das Gateway sendet.

12. Wie wird bestimmt, ob IPv4 oder IPv6 verwendet wird?

Ein Hostname kann IPv4- und IPv6-Adressen besitzen.

Windows

```
[RO] Resolve-DnsName app.example.intern -Type A
```

```
[RO] Resolve-DnsName app.example.intern -Type AAAA
```

Bestehende TCP-Verbindung prüfen:

```
[RO] Get-NetTCPConnection |
    Where-Object RemotePort -eq 443 |
    Select-Object LocalAddress,
                  LocalPort,
                  RemoteAddress,
                  RemotePort,
                  State,
                  OwningProcess
```

Linux

```
[RO] getent ahosts app.example.intern
```

IPv4 gezielt testen:

```
[TEST] curl -4 -I https://app.example.intern/
```

IPv6 gezielt testen:

```
[TEST] curl -6 -I https://app.example.intern/
```

macOS

```
[RO] dscacheutil -q host -a name app.example.intern
```

```
[TEST] curl -4 -I https://app.example.intern/
```

```
[TEST] curl -6 -I https://app.example.intern/
```

Wenn IPv4 funktioniert und IPv6 nicht, bedeutet das nicht automatisch, dass IPv6 deaktiviert werden sollte. Stattdessen müssen IPv6-Adresse, Präfix, Router, DNS, Firewall und Rückweg untersucht werden.

13. Wie wird ein Dienst hinter Load Balancer oder Reverse Proxy berücksichtigt?

Der im DNS eingetragene Endpunkt ist möglicherweise nicht der eigentliche Anwendungsserver.

```
Client
  → DNS
    → virtuelle IP-Adresse
      → Load Balancer oder Reverse Proxy
        → Backend 1
        → Backend 2
```

```
    → Backend 3
```

Zu dokumentieren sind:

- DNS-Name,
- aufgelöste virtuelle IP-Adresse,
- Load-Balancer- beziehungsweise Proxyname,
- Frontend-Port,
- Backendpool,
- Backendadressen,
- Backendports,
- Health-Check,
- TLS-Terminierung,
- verwendete Host-Header,
- Sitzungsbindung,
- mögliche Quelladressübersetzung.

Mögliche Fehlerbilder

Beobachtung	Untersuchungsrichtung
jeder zweite Aufruf schlägt fehl	einzelnes Backend möglicherweise fehlerhaft
direkter Backendzugriff funktioniert	Proxy- oder Frontendkonfiguration prüfen
Proxy antwortet mit 502	Backendverbindung oder Antwort ungültig
Proxy antwortet mit 504	Backend antwortet nicht rechtzeitig
Zertifikat passt nicht	SNI, Hostname oder TLS-Terminierung prüfen
nur ein Benutzer betroffen	Sitzung, Cookie oder bestimmtes Backend prüfen
DNS liefert mehrere Adressen	jede Zieladresse getrennt testen

Ein erfolgreicher Test gegen ein einzelnes Backend beweist nicht, dass der vollständige produktive Weg über den Load Balancer funktioniert.

14. Wie wird ein Proxy im Kommunikationsweg erkannt?

Windows – WinHTTP-Proxy

```
[RO] netsh winhttp show proxy
```

Benutzerbezogene Windows-Proxyeinstellungen:

```
[RO] Get-ItemProperty `
    'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' |
    Select-Object ProxyEnable,
                  ProxyServer,
                  AutoConfigURL
```

Linux

```
[RO][SENS] env |
    grep -iE '^(http|https|all|no)_proxy='
```

macOS

```
[RO] scutil --proxy
```

Proxykonfiguration eines bestimmten Netzwerkdienstes:

```
[RO] networksetup -getwebproxy "Wi-Fi"
```

```
[RO] networksetup -getsecurewebproxy "Wi-Fi"
```

Zu beachten

- Anwendungen können eigene Proxyeinstellungen verwenden.
- Umgebungsvariablen können benutzer- oder prozessbezogen sein.
- PAC-Dateien können das Ziel dynamisch unterschiedlichen Proxys zuordnen.
- WinHTTP- und Benutzer-Proxyeinstellungen können voneinander abweichen.
- Ein Browser kann Richtlinien oder eigene Mechanismen verwenden.
- `NO_PROXY` beziehungsweise Bypasslisten beeinflussen den tatsächlichen Weg.

Ein Proxy muss daher als eigene Komponente in den Kommunikationsweg aufgenommen werden.

15. Wie wird eine Störungsmatrix erstellt?

Eine Störungsmatrix macht Muster sichtbar.

Test	CLIENT-023	CLIENT-024	CLIENT-025
Gateway erreichbar	Ja	Ja	Ja
DNS-Auflösung	Ja	Ja	Ja
Ziel-IP erreichbar	Ja	Ja	Ja
TCP 443 erreichbar	Nein	Ja	Ja
Anwendung funktioniert	Nein	Ja	Ja
Internetzugriff	Ja	Ja	Ja
VLAN	20	20	30
Betriebssystem	Windows	Windows	Linux

Erste Einordnung

Da nur `CLIENT-023` betroffen ist und andere Clients denselben Zielport erreichen, sind folgende Bereiche wahrscheinlicher:

- lokale Host-Firewall,
- Sicherheitssoftware,
- falsche lokale Route,
- VPN- oder Proxykonfiguration,
- clientbezogene Netzwerkzugriffsregel,
- fehlerhafte Quelladresszuordnung.

Eine allgemeine Störung des Zielservers ist anhand dieser Matrix weniger wahrscheinlich, aber noch nicht vollständig ausgeschlossen.

16. Wie wird eine Zeitlinie der Störung erstellt?

Zeitpunkt	Ereignis
09:30	VPN-Client-Update abgeschlossen
09:35	letzter erfolgreicher Anwendungszugriff
09:40	Client wurde neu gestartet
09:42	erster fehlgeschlagener Zugriff
09:45	Fehler im Ticket gemeldet
09:50	anderer Client erfolgreich getestet
09:55	DNS-Auflösung erfolgreich geprüft
10:00	TCP-Porttest schlägt fehl

Auswertung

Die zeitliche Nähe zwischen VPN-Update und Störung erzeugt eine prüfbare Hypothese. Sie beweist jedoch noch nicht, dass das Update die Ursache ist.

Zu prüfen wären beispielsweise:

- neue virtuelle Schnittstelle,
- geänderte Routingtabelle,
- geänderte DNS-Server,
- aktivierter Always-on-Tunnel,
- neue lokale Filterregeln,
- veränderte Proxykonfiguration.

17. Welche typischen Fehlschlüsse müssen vermieden werden?

Beobachtung	Unzulässiger Schluss	Richtige Einordnung
ein Benutzer meldet den Fehler	nur ein Benutzer ist betroffen	Umfang aktiv prüfen
Ping funktioniert	Anwendung funktioniert	nur ICMP-Erreichbarkeit bestätigt
Ping funktioniert nicht	Host ist offline	ICMP kann blockiert sein
DNS liefert eine Adresse	DNS ist vollständig korrekt	Adresse und verwendete Antwort prüfen
Port 443 ist erreichbar	Webanwendung ist fehlerfrei	nur TCP-Verbindungsaufbau bestätigt
Traceroute zeigt Sterne	dort liegt der Fehler	Hop antwortet möglicherweise nur nicht
anderer Client funktioniert	Zielserver ist fehlerfrei	clientspezifischer oder intermittierender Fehler möglich
direkter Backendtest funktioniert	gesamter Dienstpfad funktioniert	Proxy, Load Balancer und DNS fehlen im Test
Fehler trat nach Update auf	Update ist die Ursache	zeitlicher Zusammenhang ist nur ein Hinweis
nur WLAN betroffen	Access Point ist defekt	Funk, Authentifizierung, VLAN und Client prüfen
hohe Latenz an einem Hop	dieser Router verursacht Verzögerung	Antwortpriorisierung kann abweichen

18. Welche Informationen werden an die nächste Diagnosephase übergeben?

Nach der ersten Eingrenzung sollten folgende Ergebnisse vorliegen:

Störungsumfang:
Nur CLIENT-023 betroffen.

Quelle:
CLIENT-023
192.0.2.10/24
LAN
VLAN 20

Ziel:
app.example.intern
198.51.100.20
TCP 443

Erwarteter Weg:
CLIENT-023
→ SW-01
→ Gateway 192.0.2.1
→ FW-01
→ Reverse Proxy
→ APP-01

Funktioniert:
- Link vorhanden
- gültige IP-Adresse
- Gateway erreichbar
- DNS-Auflösung erfolgreich
- andere interne und externe Ziele erreichbar

Funktioniert nicht:
- TCP-Verbindung zum Zielport 443

Vergleich:
CLIENT-024 im selben VLAN erreicht das Ziel.

Änderung:

VPN-Client wurde kurz vorher aktualisiert.

Arbeitshypothese:
Lokale Route, VPN-Filter oder Host-Firewall auf CLIENT-023.

Nächste Diagnosephase:
Physische Schnittstelle, IP-Konfiguration und ausgewählte Route
des Clients vollständig prüfen.

Damit beginnt die nächste Seite:

3.2 Physische Verbindung und Netzwerkschnittstelle prüfen

19. Dokumentationsvorlage

Ticketnummer:
Bearbeitungsbeginn:
Bearbeitende Person:
Priorität:

Fehlerbeschreibung:
Exakte Fehlermeldung:
Fehlerbeginn:
Letzter funktionierender Zeitpunkt:
Zeitzone:
Reproduzierbar: Ja / Nein

BETROFFENER UMFANG

Benutzer:
Endgeräte:
Switchports:
VLANs:
Standorte:
Dienste:
Zielsysteme:

Nicht betroffen:

QUELLE

Hostname:
Betriebssystem:
Benutzer:
Verbindungsart:
Schnittstelle:
MAC-Adresse:
IPv4-Adresse und Präfix:
IPv6-Adresse und Präfix:
Standardgateway:
DNS-Server:
VLAN:
VPN:
Proxy:

ZIEL

Dienstname:
URL oder Freigabe:
Hostname:
IPv4-Adresse:
IPv6-Adresse:
Transportprotokoll:
Port:
Anwendungsprotokoll:
Load Balancer:
Reverse Proxy:
Backend:
Weitere Abhängigkeiten:

ERWARTETER KOMMUNIKATIONSWEG

1.
2.
3.
4.

5.

6.

VERGLEICHSTESTS

Gleicher Client, anderes Ziel:

Anderer Client, gleiches Ziel:

IP-Adresse statt Name:

LAN statt WLAN:

Ohne VPN:

Anderer Benutzer:

Referenzsystem:

FUNKTIONIERT WEITERHIN

-

-

-

FUNKTIONIERT NICHT

-

-

-

ZEITLINIE

Zeitpunkt:

Ereignis:

Zeitpunkt:

Ereignis:

Kürzliche Änderungen:

Arbeitshypothese:

Begründung:

Nächster Prüfschritt:

Eskalation erforderlich: Ja / Nein

20. Offizielle Quellen und weiterführende Dokumentation

Microsoft

- Get-NetIPConfiguration
- Get-NetAdapter
- Get-NetRoute
- Find-NetRoute
- Get-NetIPInterface
- Get-NetTCPConnection
- Resolve-DnsName
- Test-NetConnection
- netsh winhttp

Linux

- ip-address – Linux Manual Page
- ip-link – Linux Manual Page
- ip-route – Linux Manual Page
- ip-rule – Linux Manual Page
- getent – Linux Manual Page

Apple

- Lokale Befehlsreferenzen: `man ifconfig`, `man route`, `man netstat`, `man scutil` und `man networksetup`
- Apple Platform Deployment – Network Services

> Der erwartete Kommunikationsweg muss anhand der tatsächlich eingesetzten Netzwerkarchitektur dokumentiert werden. Beispieladressen und Komponentennamen dürfen nicht ungeprüft auf eine produktive Umgebung übertragen werden.