Teams-Telefonie über VPN: Split Tunneling richtig einrichten



WISSEN

Alles zur Teams-Telefonie: Direct Routing, SBC, Wählpläne, Routing, Notruf und Betrieb an einem Ort.

› **Teams-Telefonie**

BERATUNG

VPN, Proxy und Teams-Medien vertragen sich nicht? Wir planen mit dir die Ausnahmen, ohne dass die Security-Abteilung Schnappatmung bekommt.

› **Beratung zur Teams-Telefonie**

SCHULUNG

Für Admins, die Medienwege, Netzwerkstandorte und Notruf in Teams selbst sicher beurteilen wollen.

› **Schulung Teams-Telefonie**

Im Büro klingt alles wunderbar. Im Homeoffice klingt der Kollege aus dem Vertrieb wie ein Roboter mit Schluckauf, und zwar nur dann, wenn das VPN an ist. Das ist kein Zufall und auch kein Fluch des heimischen Routers. Es ist Physik mit Ansage: Sprache in Echtzeit mag keine Umwege, keine doppelte Verschlüsselung und schon gar keinen Proxy, der jedes Paket einmal umdreht, bevor er es weiterreicht. Genau das bekommt sie aber, wenn Teams-Telefonie über VPN im Forced Tunnel läuft.

Dieser Beitrag gehört zur Serie rund um die Teams-Telefonie und ist problemorientiert. Du erfährst, wie sich der Fehler zeigt, warum Medien im Tunnel leiden, wie du mit lesenden Befehlen nachweist, wo deine Sprachpakete wirklich langlaufen, wie du Split Tunneling nach Microsofts Empfehlung einrichtest und was das alles mit dem Notrufstandort zu tun hat. Letzteres ist der Teil, den die meisten vergessen, bis es zu spät ist.

FAKTEN · Das Beispiel in diesem Beitrag

Erfundener Tenant Contoso (contoso.com), Zentrale in Frankfurt, weitere Standorte in Köln, Berlin, Hamburg und München. Direct Routing über sbc1.contoso.com und sbc2.contoso.com, Rufnummern im Muster +49 69 555 0100. Der VPN-Konzentrator steht in Frankfurt und vergibt Adressen aus 10.99.0.0/16. Öffentliche Adressen stammen aus den Dokumentationsbereichen 198.51.100.0/24 und 203.0.113.0/24. Alles erfunden, jede Ähnlichkeit mit deinem Netz ist rein statistisch.

Das Symptom: Im Büro gut, im Homeoffice mit VPN schlecht

So klingt es im Helpdesk

VPN-Probleme bei Teams-Telefonie haben ein typisches Muster: Sie treten nur außerhalb des Büros auf, nur mit aktivem Tunnel und bevorzugt dann, wenn alle gleichzeitig im Homeoffice sind. Die Sätze, die du kennen wirst:

- **„Wenn ich das VPN trenne, ist alles gut."** Der ehrlichste Satz im ganzen Helpdesk. Er ist zugleich die Diagnose und die schlechteste Lösung.
- **„Montags um neun klingt jeder wie unter Wasser."** Dann sitzen alle gleichzeitig im Tunnel, der Konzentrator ist voll, und Jitter und Paketverlust steigen mit der Teilnehmerzahl.
- **„Ich höre den Kunden, er hört mich nur abgehackt."** Upload im Heimanschluss plus Tunnel-Overhead plus Umweg. Die Richtung, die ohnehin knapp ist, leidet zuerst.
- **„Seit dem neuen VPN-Client brechen Anrufe ab."** Ein Neuaufbau des Tunnels ist für den Teams-Client ein Netzwechsel. Laufende Medien müssen sich neu sortieren, und das klappt nicht immer.
- **„Bei mir steht als Notrufstandort die Zentrale, ich sitze aber in Köln."** Der leiseste und gefährlichste Satz. Er kommt selten, weil kaum jemand nachschaut.

So sieht es der Admin

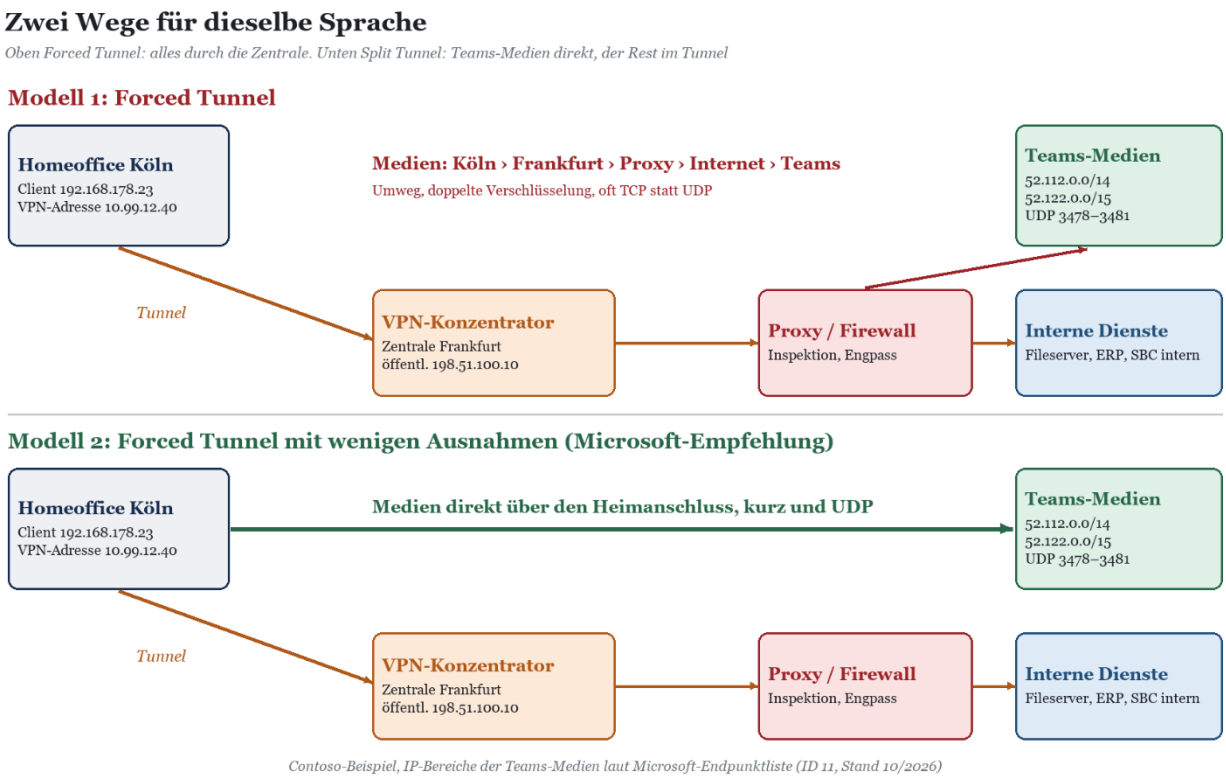
In der Anrufanalyse des Teams Admin Centers fallen betroffene Anrufe durch hohe Roundtrip-Zeiten, Jitter und Paketverlust auf, oft gepaart mit TCP als Transport statt UDP. Im Call Quality Dashboard (CQD) häufen sich schlechte Streams bei Endpunkten, deren Netzadapter sich als VPN meldet. Und wer Netzwerkstandorte gepflegt hat, findet Homeoffice-Benutzer plötzlich am Standort Frankfurt wieder, obwohl dort an diesem Tag niemand im Büro war. Wie du Jitter, Verlust und Roundtrip grundsätzlich liest, steht in Abgehackte Sprache in Teams: Jitter, Paketverlust und Roundtrip.

Wie der Fehler entsteht: Echtzeit-Medien im Tunnel

Der Weg der Sprachpakete

Ein Teams-Anruf besteht aus zwei Verkehrsarten. Die Signalisierung läuft über HTTPS, ist nicht besonders zeitkritisch und von Microsoft in der Kategorie „Allow" eingestuft. Die Medien, also Sprache und Video, laufen als SRTP bevorzugt über UDP zu den Medien-Relays von Microsoft und sind in der Kategorie „Optimize" einsortiert. Diese Kategorie umfasst laut Microsoft nur wenige Endpunkte, die aber rund 70 bis 80 Prozent des Datenvolumens zu Microsoft 365 ausmachen und besonders empfindlich auf Latenz reagieren.

Im Forced Tunnel nimmt ein Sprachpaket aus dem Homeoffice in Köln folgenden Weg: Client › VPN-Tunnel › Konzentrator in Frankfurt › Proxy oder Firewall › Internet-Ausgang der Zentrale › Microsoft-Netz › zurück zum Gesprächspartner. Ohne Tunnel wäre es: Client › Heimanschluss › Microsoft-Netz. Der Unterschied ist nicht nur die Strecke. Jedes Glied in der Kette kann puffern, Pakete verwerfen oder UDP gar nicht durchlassen, was den Client auf TCP zurückfallen lässt. Warum TCP für Sprache Gift ist, erklärt Teams-Telefonie über TCP statt UDP: warum das schlecht klingt.



Contoso-Beispiel, IP-Bereiche der Teams-Medien laut Microsoft-Endpunktliste (ID 11, Stand 10/2026)

Warum es erst unter Last richtig wehtut

Ein VPN-Konzentrator ist für Dateizugriffe und Fachanwendungen dimensioniert, nicht für einige hundert gleichzeitige Echtzeitströme. Solange zehn Leute im Homeoffice sind, merkt niemand etwas. Bei zweihundert wird aus „geht schon“ ein Montagmorgen-Phänomen. Microsoft beschreibt den Forced Tunnel ausdrücklich als Modell, das die VPN-Infrastruktur hoch belastet und die Leistung des gesamten Firmenverkehrs bremsen kann. Mit anderen Worten: Die Sprache leidet, und die Buchhaltung, die auf das ERP wartet, leidet gleich mit.

FAKTEN · Microsofts VPN-Modelle für Microsoft 365

Microsoft unterscheidet fünf Modelle: 1. Forced Tunnel (alles durch den Tunnel), 2. Forced Tunnel mit wenigen vertrauenswürdigen Ausnahmen, 3. Forced Tunnel mit breiten Ausnahmen, 4. Selective Tunnel (nur Firmennetz durch den Tunnel) und 5. kein klassisches VPN. Microsoft empfiehlt als schnellen und sicheren Schritt den Wechsel von Modell 1 auf Modell 2: Standardroute in den Tunnel, aber die Optimize-Endpunkte direkt über die lokale Internetverbindung.

Die Teams-Medien stehen in der Endpunktliste als ID 11 (Kategorie Optimize, erforderlich) mit den Bereichen 52.112.0.0/14, 52.122.0.0/15 und 2603:1063::/38 auf den UDP-Ports 3478, 3479, 3480 und 3481 (Stand der Liste: Oktober 2026).

Die Tabelle: VPN-Variante › Auswirkung

Die folgende Übersicht fasst zusammen, was die gängigen Varianten mit deiner Teams-Telefonie machen. Sie ist bewusst aus Sicht der Telefonie geschrieben, nicht aus Sicht der Security. Beide Sichten musst du am Ende zusammenbringen.

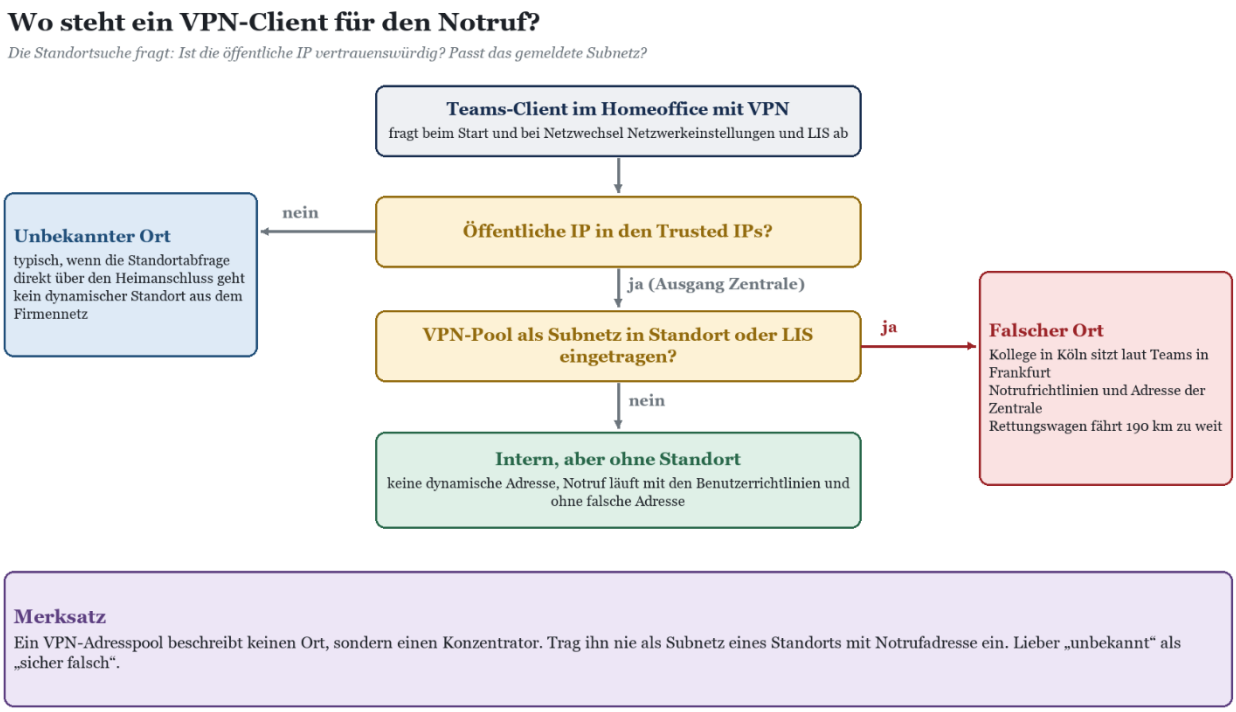
VPN-Variante	Weg der Teams-Medien	Sprachqualität	Notrufstandort	Last am Konzentrator
1 Forced Tunnel	Durch Tunnel, Konzentrator und	Schlecht bis instabil, unter Last deutlich schlechter,	Zentrale, falls VPN-Pool als Subnetz eingetragen; sonst	Hoch

	Proxy der Zentrale	oft TCP	unbekannt	
2 Forced Tunnel mit wenigen Ausnahmen	Optimize-Bereiche direkt, Rest im Tunnel	Wie ohne VPN, abhängig vom Heimanschluss	Hängt davon ab, über welchen Weg die Standortabfrage läuft	Deutlich geringer
3 Forced Tunnel mit breiten Ausnahmen	Microsoft 365 komplett direkt	Wie ohne VPN	Meist unbekannt (öffentliche IP des Heimanschlusses)	Gering
4 Selective Tunnel	Direkt, nur Firmennetze im Tunnel	Wie ohne VPN	Unbekannt, sofern die Heim-IP nicht vertrauenswürdig ist	Sehr gering
5 Kein klassisches VPN	Direkt	Wie ohne VPN	Unbekannt außerhalb des Firmennetzes	Entfällt
Sonderfall: Cloud-Proxy ändert Quell-IP	Über den Proxy-Dienst	Abhängig vom Dienst, oft zusätzliche Latenz	Nicht unterstützt: Microsoft schließt die Standortsuche hier aus	Entfällt

Und was hat das mit dem Notruf zu tun?

Mehr, als dir lieb ist. Der Teams-Client fragt beim Start, regelmäßig und bei jedem Netzwechsel die Netzwerkeinstellungen und den Location Information Service (LIS) ab. Teams prüft zuerst, ob die öffentliche Adresse, mit der der Client ankommt, in den vertrauenswürdigen IP-Adressen steht. Nur dann sucht es nach dem internen Subnetz und damit nach Netzwerkstandort und Notrufadresse. Steht die öffentliche Adresse nicht in der Liste, gilt der Client als „an unbekanntem Ort“.

Im Forced Tunnel kommt der Client mit der öffentlichen Adresse der Zentrale an, die natürlich vertrauenswürdig ist. Teams sucht dann nach dem internen Subnetz, und das ist der VPN-Pool. Hat irgendwer 10.99.0.0/16 aus Ordnungsliebe dem Standort Frankfurt zugeordnet oder im LIS mit der Adresse der Zentrale verknüpft, sitzt die Kollegin in Köln für Teams in Frankfurt. Dann bekommt sie die Notrufrichtlinien des Standorts Frankfurt und, wenn der LIS-Eintrag existiert, die Adresse der Zentrale. Die Leitstelle schickt den Rettungswagen zur Zentrale nach Frankfurt, während der Notfall in Köln-Ehrenfeld stattfindet. Schwarzer Humor hört an dieser Stelle auf.



Vereinfachte Logik nach Microsoft-Dokumentation zu Netzwerkeinstellungen und LIS, Contoso-Beispiel

Mit Split Tunneling ändert sich das Bild, aber nicht automatisch zum Guten. Welche öffentliche Adresse der Standortdienst sieht, hängt davon ab, über welchen Weg die Abfrage läuft. Die Signalisierung gehört zur Kategorie Allow und darf laut Microsoft durch den Tunnel. Läuft sie dort entlang, gilt das oben Gesagte weiter. Läuft sie direkt, kommt der Client mit der Heim-IP an und ist „unbekannt“. Beides kann richtig sein, solange der VPN-Pool keinem Ort zugeordnet ist. Die Grundlagen zu Standorten und Subnetzen findest du in Netzwerkstandorte und Subnetze in Teams richtig pflegen, die Notruf-Grundlagen in Notruf in Microsoft Teams konfigurieren.

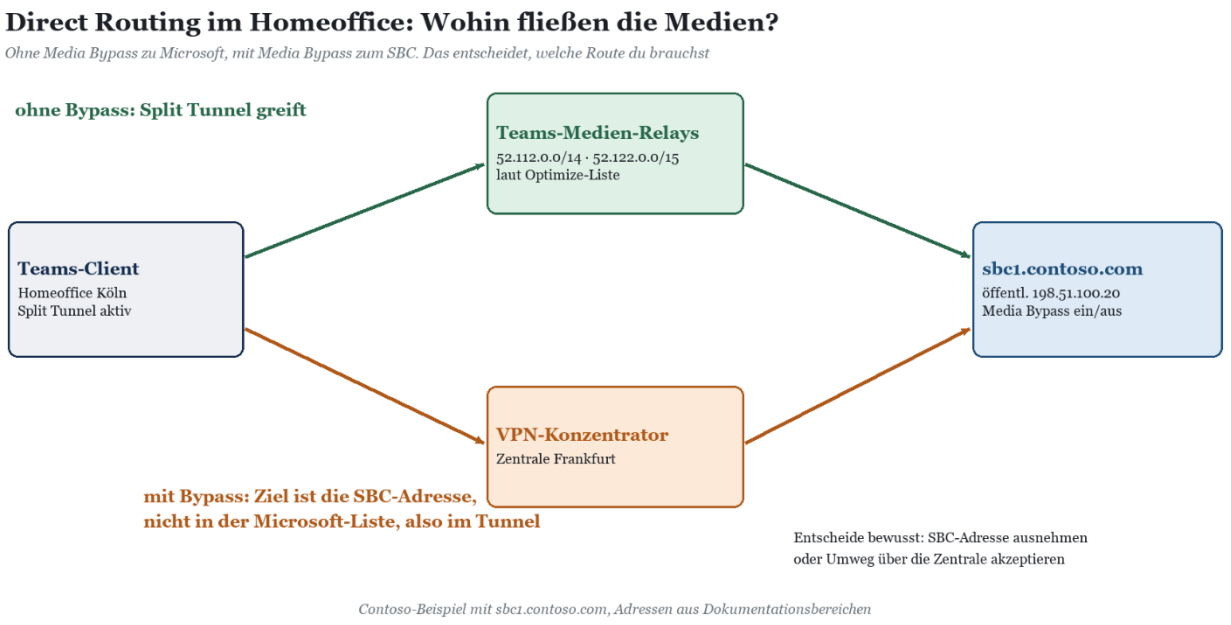
WARNUNG · Ein VPN-Pool ist kein Ort

Trag Adressbereiche deines VPN-Konzentrators nie als Subnetz eines Netzwerkstandorts mit Notrufrichtlinie und nie im LIS mit einer Notrufadresse ein. Ein Pool beschreibt, wo der Tunnel endet, nicht wo der Mensch sitzt. Für 110 und 112 gilt: lieber gar keine dynamische Adresse als eine falsche.

Microsoft beschreibt für die USA und Kanada zusätzlich eine Funktion, mit der Benutzer im Homeoffice ihre Adresse selbst bestätigen oder eintragen (External Location Lookup Mode in der Notrufrichtlinie). Die Dokumentation bezieht sich dabei auf die dortigen Notrufregeln. Plane für Deutschland nicht damit, ohne die Zustellung des Standorts mit deinem SBC und deinem Carrier geklärt zu haben. Was bei einem Notruf ohne Adresse passiert, steht in Notrufadresse fehlt in Teams: was bei 112 wirklich passiert.

Direct Routing: Der SBC ist nicht in der Microsoft-Liste

Bei Direct Routing gibt es eine Feinheit, die in Microsofts Split-Tunnel-Anleitung nicht im Vordergrund steht. Ohne Media Bypass laufen die Medien vom Client zu den Teams-Medien-Relays, also in die Optimize-Bereiche, und der Split Tunnel greift. Mit Media Bypass spricht der Client direkt mit dem SBC. Dessen öffentliche Adresse steht in keiner Microsoft-Liste und läuft damit über die Standardroute, also durch den Tunnel. Ein internes SBC-Bein erreicht der Client ohnehin nur über den Tunnel.



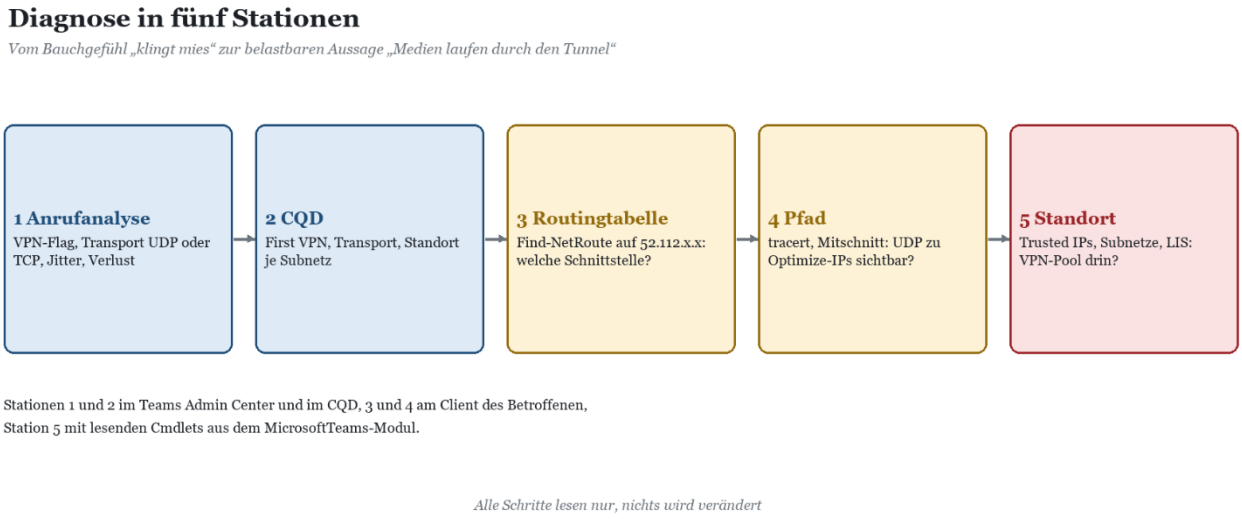
AUS DER PRAXIS · Aus Ulis eigenem Netz

Als ich an meinem eigenen anynode-SBC Media Bypass eingeschaltet habe, klang das Homeoffice-Telefonat plötzlich schlechter als vorher statt besser. Die Medien gingen nicht mehr zu Microsoft, sondern zur öffentlichen Adresse des SBC, und die stand nicht in der Ausnahmeliste des VPN-Profils. Ergebnis: Sprache durch den Tunnel ins Büro und von dort wieder hinaus zum SBC. Eine Zeile im VPN-Profil später war alles gut. Lehre: Wer Media Bypass einschaltet, muss den Medienweg neu denken.

Wie Media Bypass und Local Media Optimization im Detail funktionieren, erklärt Teams Media Bypass und Local Media Optimization. Für die Rolle des SBC insgesamt lohnt ein Blick in Teams SBC Grundlagen: der Session Border Controller.

Diagnose Schritt für Schritt

Die gute Nachricht: Für die Diagnose musst du nichts ändern. Alle Schritte lesen nur. Du brauchst einen betroffenen Benutzer, einen Anruf mit schlechter Qualität, Zugriff auf das Teams Admin Center und eine PowerShell mit dem MicrosoftTeams-Modul.



Schritt 1: Anrufanalyse im Teams Admin Center

Öffne im Teams Admin Center unter Benutzer den betroffenen Benutzer und dort den Anrufverlauf. Wähle einen schlechten Anruf und sieh dir in den erweiterten Details die Netzwerkangaben des Clients an: lokale und öffentliche IP-Adresse, Verbindungstyp, Transport (UDP oder TCP) sowie Jitter, Paketverlust und Roundtrip. Steht als öffentliche Adresse die Ausgangsadresse der Zentrale, in unserem Beispiel 198.51.100.10, obwohl der Benutzer zu Hause sitzt, laufen die Medien mit hoher Wahrscheinlichkeit durch den Tunnel.

Schritt 2: Call Quality Dashboard

Im CQD gibt es eigene Dimensionen für VPN. „First VPN“ und „Second VPN“ sind wahr, wenn der Netzadapter des Endpunkts sich als VPN meldet; Microsoft weist darauf hin, dass nicht alle VPN-Clients das korrekt tun. „First Network Mapped VPN“ wertet dagegen deine hochgeladenen Gebäudedaten aus und ist nur dann aussagekräftig, wenn du die VPN-Subnetze dort als VPN markiert hast. Kombiniere die VPN-Dimension mit „Transport“ und dem Anteil schlechter Streams. Wenn VPN-Streams deutlich schlechter sind als der Rest, hast du deinen Beweis für das nächste Gespräch mit der Security.

Schritt 3: Routingtabelle am Client

Jetzt wird es konkret. Am Rechner des Betroffenen, mit aktivem VPN, prüfst du, über welche Schnittstelle Windows ein Ziel in den Teams-Medienbereichen erreichen würde. Teams fragt das Betriebssystem nach der besten Route und nimmt die Schnittstelle, die es zurückbekommt.

```
# Netzadapter und Indizes anzeigen
Get-NetAdapter | Select-Object Name, InterfaceDescription, ifIndex, Status

# Welche Route würde Windows für ein Ziel im Teams-Medienbereich nehmen?
Find-NetRoute -RemoteIPAddress 52.112.0.10 |
    Select-Object InterfaceAlias, DestinationPrefix, NextHop, RouteMetric

# Gibt es eigene Routen für die Optimize-Bereiche?
Get-NetRoute -DestinationPrefix 52.112.0.0/14, 52.122.0.0/15 -ErrorAction SilentlyContinue

# Pfad prüfen (Beispiel aus der Microsoft-Dokumentation)
tracert worldaz.tr.teams.microsoft.com
```

Zeigt Find-NetRoute den VPN-Adapter, gehen die Medien in den Tunnel. Zeigt es den WLAN- oder Ethernet-Adapter mit dem Heimrouter als nächstem Hop, ist die Ausnahme aktiv. Der tracert sollte dann über den Internetanbieter des Heimanschlusses laufen und bei einer Adresse aus den Teams-Bereichen enden. Microsoft nennt als weiteren Test einen Netzwerkmitschnitt während eines Anrufs: Filterst du auf UDP und siehst Verkehr zu Adressen aus den Optimize-Bereichen auf der physischen Schnittstelle, ist alles richtig. Siehst du ihn dort nicht, steckt er im Tunnel.

> **TIPP · Ein Mitschnitt sagt mehr als tausend Tickets**
>
> Schneide auf der physischen Schnittstelle mit, nicht auf dem VPN-Adapter. Ist dort während eines Anrufs kein UDP-Verkehr zu 52.112.0.0/14 oder 52.122.0.0/15 zu sehen, laufen die Medien durch den Tunnel, egal was im VPN-Profil steht.

Schritt 4: Media Bypass am SBC prüfen

Bei Direct Routing klärst du, ob Media Bypass am Gateway aktiv ist. Dann ist die öffentliche Adresse des SBC ein Medienziel und gehört in deine Betrachtung.

```
Connect-MicrosoftTeams
```

```
Get-CsOnlinePSTNGateway |
    Select-Object Identity, Enabled, MediaBypass, BypassMode, PidfLoSupported
```

Steht MediaBypass für sbc1.contoso.com auf True, wiederhole Schritt 3 mit der öffentlichen Adresse des SBC als Ziel. PidfLoSupported zeigt dir nebenbei, ob der SBC Standortdaten im INVITE für Notrufe erwartet.

Schritt 5: Standortlogik prüfen

Zum Schluss prüfst du, ob dein VPN-Pool irgendwo als Ort auftaucht. Die Befehle lesen nur.

```
# Vertrauenswürdige öffentliche Adressen
Get-CsTenantTrustedIPAddress | Select-Object Identity, IPAddress, MaskBits, Description

# Ist der VPN-Pool einem Netzwerkstandort zugeordnet?
Get-CsTenantNetworkSubnet |
    Where-Object { $_.SubnetID -like '10.99.*' } |
    Select-Object SubnetID, MaskBits, NetworkSiteID, Description

# Hat der VPN-Pool eine Notrufadresse im LIS?
Get-CsOnlineLisSubnet | Where-Object { $_.Subnet -like '10.99.*' }

# Welche Richtlinien hängen am betroffenen Standort?
Get-CsTenantNetworkSite -Identity 'FRA' |
    Select-Object Identity, NetworkRegionID, EmergencyCallingPolicy, EmergencyCallRoutingPolicy
```

Liefert eine der beiden Subnetzabfragen einen Treffer für 10.99.0.0/16, hast du den gefährlichen Fall aus der Skizze oben. Kontrolliere zusätzlich im Teams-Client des Betroffenen, welcher Notrufstandort im Bereich Anrufe angezeigt wird. Beachte: Änderungen an den Netzwerkeinstellungen können laut Microsoft bis zu vier Stunden brauchen, bis sie bei den Clients ankommen.

WERKZEUG · So findet es der Teams-Telefonie Diagnostiker

Die Anrufqualität zeigt je Standort und Subnetz den Anteil schlechter Audiostreams und den Anteil der Medien, die über TCP statt UDP laufen, dazu Paketverlust, Jitter, Roundtrip und die öffentliche IP-Adresse. Ein VPN-Pool fällt dort als eigene Zeile oder unter „Nicht zugeordnet“ auf, meist mit auffällig hohem TCP-Anteil und der öffentlichen Adresse der Zentrale.

Der Benutzer-Steckbrief zeigt für einen einzelnen Benutzer den ermittelten Notrufstandort und das Netz am Standort. Die Befunde nennen jeweils einen Prüffall, mit dem du das Ergebnis selbst nachvollziehen kannst.

Mehr zum Werkzeug: Teams-Telefonie Diagnostiker. 15 Tage kostenlos testen.

Behebung: Split Tunneling für Teams-Medien einrichten

Schritt 1: Die richtigen Bereiche besorgen

Nimm die Adressbereiche ausschließlich aus Microsofts offizieller Endpunktliste Microsoft 365-URLs und -IP-Adressbereiche oder aus dem zugehörigen IP-Adress- und URL-Webdienst. Nicht aus einem Forum, nicht aus dem Gedächtnis und nicht aus der Konfiguration von 2020. Die Liste ändert sich: Microsoft aktualisiert sie in der Regel zum Monatsanfang und veröffentlicht neue Adressen 30 Tage bevor sie aktiv werden.

Endpunktsatz	Kategorie	Adressbereiche	Ports	Behandlung im

				VPN
ID 11 Teams-Medien	Optimize, erforderlich	52.112.0.0/14, 52.122.0.0/15, 2603:1063::/38	UDP 3478, 3479, 3480, 3481	Am Tunnel vorbei, direkt über den Heimanschluss
ID 12 Teams-Signalisierung und Dienste	Allow, erforderlich	u. a. *.teams.microsoft.com, *.lync.com sowie IP-Bereiche laut Liste	TCP 443, 80; UDP 443	Darf laut Microsoft im Tunnel bleiben
ID 1 Exchange Online, ID 31 SharePoint	Optimize, erforderlich	laut aktueller Liste	TCP 443, 80; UDP 443	Optional ebenfalls direkt, entlastet den Konzentrator

Wichtig ist der Hinweis, den Microsoft selbst gibt: Teams-Medien haben keine URL. Manche VPN-Clients können Ausnahmen nach Domänennamen definieren, das hilft hier nicht. Für Medien musst du mit IP-Bereichen arbeiten.

Schritt 2: Lokal testen, bevor du verteilst

Microsoft beschreibt einen Test, der die Ausnahme auf einem einzelnen Rechner über die Routingtabelle nachbildet. Das ist der ehrlichste Probelauf, den du machen kannst, und er lässt sich vollständig zurücknehmen. Ermittle den Index des Adapters mit Internetzugang und das Standardgateway des Heimrouters, dann:

```
$intIndex = 12               # ifIndex des Adapters mit Internetzugang
$gateway  = '192.168.178.1'  # Standardgateway dieses Adapters
$destPrefix = '52.112.0.0/14', '52.122.0.0/15'

foreach ($prefix in $destPrefix) {
    New-NetRoute -DestinationPrefix $prefix -InterfaceIndex $intIndex -NextHop $gateway
}
route print

# Rollback
foreach ($prefix in $destPrefix) {
    Remove-NetRoute -DestinationPrefix $prefix -InterfaceIndex $intIndex -NextHop $gateway -
Confirm:$false
}
```

Führ vorher und nachher einen Testanruf durch und vergleiche Roundtrip, Jitter und Transport in der Anrufanalyse. Für den IPv6-Bereich 2603:1063::/38 brauchst du ein IPv6-Gateway; teste ihn getrennt, falls dein Heimanschluss IPv6 nutzt. Manche VPN-Clients überschreiben manuell gesetzte Routen beim Neuaufbau des Tunnels. Dann ist der Test nur eine Momentaufnahme, aber eine aussagekräftige.

Schritt 3: Ausnahme im VPN-Profil hinterlegen

Die eigentliche Konfiguration gehört ins VPN-Profil, nicht in Skripte auf dem Client. Wie das geht, hängt vom Produkt ab. Microsoft verweist in Implementieren von VPN-Split-Tunneling für Microsoft 365 auf Anleitungen für verbreitete VPN-Lösungen und für den in Windows integrierten VPN-Client, der dafür Ausschlussrouten im Profil kennt. Die Logik ist überall gleich:

1. **Standardroute bleibt im Tunnel.** Du baust Modell 2, nicht Modell 4. Alles, was du nicht ausdrücklich ausnimmst, läuft weiter über die Zentrale.
2. **Optimize-Bereiche der Teams-Medien ausnehmen.** 52.112.0.0/14, 52.122.0.0/15 und, wenn IPv6 im Spiel ist, 2603:1063::/38.

3. **Bei Media Bypass die SBC-Adresse prüfen.** Entweder die öffentliche Adresse von sbc1.contoso.com ebenfalls ausnehmen oder den Umweg bewusst akzeptieren. Das ist eine Architekturentscheidung, keine Fußnote.
4. **Lokale Firewall-Regeln prüfen.** Microsoft nennt Fälle, in denen Medien trotz korrekter Routen im Tunnel landen. Dann hilft eine Regel, die den Teams-Bereichen oder -Ports den Weg über den VPN-Adapter versperrt.
5. **Webclient nicht vergessen.** Für Teams im Browser unterstützt Microsoft Edge ab Version 96 Split Tunneling für Peer-to-Peer-Verkehr; maßgeblich ist die Edge-Richtlinie WebRtcRespectOsRoutingTableEnabled.

WICHTIG · Das Security-Gespräch vorbereiten

Das häufigste Gegenargument lautet: Was nicht durch den Tunnel geht, ist nicht verschlüsselt. Für Teams-Medien stimmt das nicht. Sie sind mit SRTP verschlüsselt, der Sitzungsschlüssel wird über den TLS-gesicherten Signalisierungskanal ausgetauscht. Microsoft weist zudem darauf hin, dass die Medien auch im Forced Tunnel spätestens hinter der Zentrale ohnehin als SRTP ins Internet gehen. Die Ausnahme betrifft nur Microsoft-eigene, veröffentlichte Adressbereiche.

Schritt 4: VPN-Pool aus der Standortlogik nehmen

Hat deine Diagnose ergeben, dass 10.99.0.0/16 einem Netzwerkstandort oder einer LIS-Adresse zugeordnet ist, nimmst du den Pool dort heraus. Sichere vorher den Ist-Zustand:

```
# Ist-Zustand sichern
Get-CsTenantNetworkSubnet | Export-Csv .\subnets-vorher.csv -NoTypeInformation -Encoding UTF8
Get-CsOnlineLisSubnet     | Export-Csv .\lis-vorher.csv     -NoTypeInformation -Encoding UTF8

# Änderung
Remove-CsTenantNetworkSubnet -Identity '10.99.0.0'
Remove-CsOnlineLisSubnet -Subnet '10.99.0.0'
```

Rollback: Lege die Einträge mit den gesicherten Werten über New-CsTenantNetworkSubnet und Set-CsOnlineLisSubnet wieder an. Rechne auch beim Rollback mit bis zu vier Stunden, bis die Clients den neuen Stand kennen. Und teste anschließend mit einem echten Client im Homeoffice, welcher Notrufstandort angezeigt wird, ohne dafür die 112 zu wählen; wie man das macht, ohne die Leitstelle zu verärgern, steht in Notruf in Teams testen, ohne die Leitstelle zu verärgern.

Maßnahme	Wo	Rollback
Testrouten für Teams-Medien	Einzelner Client, PowerShell	Remove-NetRoute mit denselben Parametern oder Neustart
Ausnahme im VPN-Profil	VPN-Verwaltung	Profil auf die vorherige Version zurücksetzen und neu verteilen
SBC-Adresse ausnehmen	VPN-Profil	Eintrag entfernen; Medien laufen wieder über den Tunnel
Firewall-Regel gegen Medien im Tunnel	Client-Firewall, zentral verteilt	Regel deaktivieren
VPN-Pool aus Standort und LIS entfernen	Teams, PowerShell oder Admin Center	Einträge aus der CSV-Sicherung neu anlegen

Vorbeugung: damit der Tunnel nicht wieder zuschnappt

Split Tunneling ist kein Projekt, das man einmal macht und dann vergisst. Ein Maschinenbauer mit zwölf Standorten hatte die Ausnahmen sauber eingerichtet, und zwei Jahre später klangen die

Anrufe aus dem Homeoffice wieder nach Blechdose. Ursache: ein neues VPN-Produkt, ein frisch migriertes Profil, und die Ausnahmen waren im Migrationsprotokoll unter „Sonstiges“ verschwunden.

- **Liste automatisch abgleichen.** Abonniere die Änderungen der Microsoft-Endpunktliste oder frag den Webdienst per Skript ab und vergleiche die Optimize-Bereiche mit deinem VPN-Profil. Neue Adressen kündigt Microsoft 30 Tage vorher an.
- **VPN-Pools markieren.** Trag die VPN-Subnetze in den Gebäudedaten des CQD als VPN ein, damit die Auswertung sie sauber trennt, und nirgends als Standort mit Notrufadresse.
- **Monatlich auf VPN-Streams schauen.** Vergleiche im CQD die Qualität von VPN- und Nicht-VPN-Streams. Steigt die Kluft, ist eine Ausnahme verloren gegangen.
- **Media Bypass als Netzänderung behandeln.** Wer am SBC Media Bypass ein- oder ausschaltet, prüft die Medienwege im Homeoffice neu.
- **Change-Prozess koppeln.** VPN-Profiländerungen bekommen ein Pflichtfeld: Teams-Medien weiterhin ausgenommen, VPN-Pool weiterhin keinem Ort zugeordnet?

Diese Punkte gehören in die Betriebsdokumentation und in die Verantwortungsmatrix zwischen Netzwerk-, Security- und Teams-Team; einen Rahmen dafür beschreibt Microsoft Teams Telefonie-Governance. Wer regelmäßig prüfen will, ob sich die Konfiguration schleichend verändert, findet Ansätze in Konfigurationsdrift in der Teams-Telefonie erkennen. Und wenn die Diskussion zwischen Security und Telefonie festgefahren ist, hilft oft ein neutraler Blick von außen in der Beratung zur Teams-Telefonie.

WEITERLESEN · Passend zu diesem Thema

› Teams-Telefonie über TCP statt UDP: warum das schlecht klingt
› Abgehackte Sprache in Teams: Jitter, Paketverlust und Roundtrip
› Netzwerkstandorte und Subnetze in Teams richtig pflegen
› Teams Media Bypass und Local Media Optimization
› Notrufadresse fehlt in Teams: was bei 112 wirklich passiert
› Notruf in Teams testen, ohne die Leitstelle zu verärgern
› Teams-Anruf bricht nach einigen Minuten ab
› Sprachqualität in Teams: QoS, CQD und Troubleshooting
› Teams-Telefonie Probleme: die zehn häufigsten Ursachen

FAQ: Teams-Telefonie über VPN

Ist Split Tunneling für Teams nicht ein Sicherheitsrisiko?

Die Medien sind mit SRTP verschlüsselt, der Schlüssel kommt über den TLS-gesicherten Signalisierungskanal. Ausgenommen werden nur veröffentlichte, Microsoft-eigene Adressbereiche. Microsoft empfiehlt genau dieses Modell als ersten Schritt. Ob es zu deinen Sicherheitsvorgaben passt, entscheidest du mit deiner Security, aber das Verschlüsselungsargument trägt nicht.

Reicht es, *.teams.microsoft.com im VPN-Client auszunehmen?

Nein. Teams-Medien haben keine URL. Ausnahmen nach Domänennamen erfassen die Signalisierung, nicht die Sprache. Für Medien brauchst du die IP-Bereiche aus dem Endpunktsatz 11.

Muss die Signalisierung auch am Tunnel vorbei?

Nein. Microsoft stuft sie als Allow ein; sie darf durch den Tunnel. Bedenke aber, dass der Weg der Abfragen beeinflusst, mit welcher öffentlichen Adresse dein Client beim Standortdienst ankommt.

Warum stimmt der Notrufstandort im Homeoffice nicht?

Meist, weil der Client über den Tunnel mit der vertrauenswürdigen Adresse der Zentrale ankommt und der VPN-Pool einem Standort oder einer LIS-Adresse zugeordnet ist. Nimm den Pool dort heraus. Ein VPN-Pool beschreibt keinen Ort.

Was ist mit 110 und 112, wenn kein dynamischer Standort ermittelt wird?

Der Notruf wird trotzdem abgesetzt und läuft nach den Richtlinien, die dem Benutzer zugewiesen sind. Welche Standortinformation die Leitstelle dann bekommt, hängt von deiner Direct-Routing-Konfiguration, dem SBC und dem Carrier ab. Prüfe genau das vorher, nicht im Ernstfall.

Hilft QoS gegen schlechte Qualität im VPN?

Kaum. DSCP-Markierungen helfen in deinem eigenen Netz. Im Tunnel über das Internet und am Heimanschluss werden sie in der Regel nicht beachtet. Der kürzere Weg bringt mehr als jede Markierung. Mehr dazu in Sprachqualität in Teams: QoS, CQD und Troubleshooting.

Gilt das auch für Teams Rooms oder Teams-Telefone?

Diese Geräte stehen normalerweise im Firmennetz und nutzen kein Client-VPN. Das Thema betrifft vor allem Laptops im Homeoffice und unterwegs. Für Geräte im Firmennetz gelten die Regeln aus der Netzwerkstandort-Pflege.

Wie oft ändern sich die Teams-IP-Bereiche?

Microsoft aktualisiert die Endpunktliste in der Regel zum Monatsanfang und veröffentlicht neue Adressen 30 Tage vor ihrer Aktivierung. Bei Bedarf gibt es auch Änderungen im laufenden Monat. Ein automatischer Abgleich ist deshalb Pflicht.

Fazit: Sprache gehört nicht in den Tunnel

Teams-Telefonie über VPN im Forced Tunnel ist wie ein Telefonat mit einem Dolmetscher, der jedes Wort erst in die Zentrale faxt. Es funktioniert, irgendwie, solange nicht alle gleichzeitig reden. Die Lösung ist gut dokumentiert: Optimize-Bereiche der Teams-Medien aus der offiziellen Liste nehmen, im VPN-Profil am Tunnel vorbeiführen, mit Routingtabelle, tracert und Mitschnitt nachweisen, dass es wirkt, und die Liste automatisch aktuell halten.

Der zweite Teil ist der, der Leben betrifft: Ein VPN-Pool ist kein Ort. Prüf, dass er weder als Subnetz eines Netzwerkstandorts noch im LIS mit einer Notrufadresse auftaucht, und denk bei Direct Routing mit Media Bypass an die Adresse deines SBC. Wenn du das Ganze für alle Standorte und Arbeitsmodelle einmal grundsätzlich planen willst, ist das Festpreispaket Grobkonzept Teams-Telefonie ein guter Startpunkt.