



WIRESHARK

User Group Switzerland

Real-World Case Studies and Troubleshooting

It's not the network vs. It was the network



Vorstellung

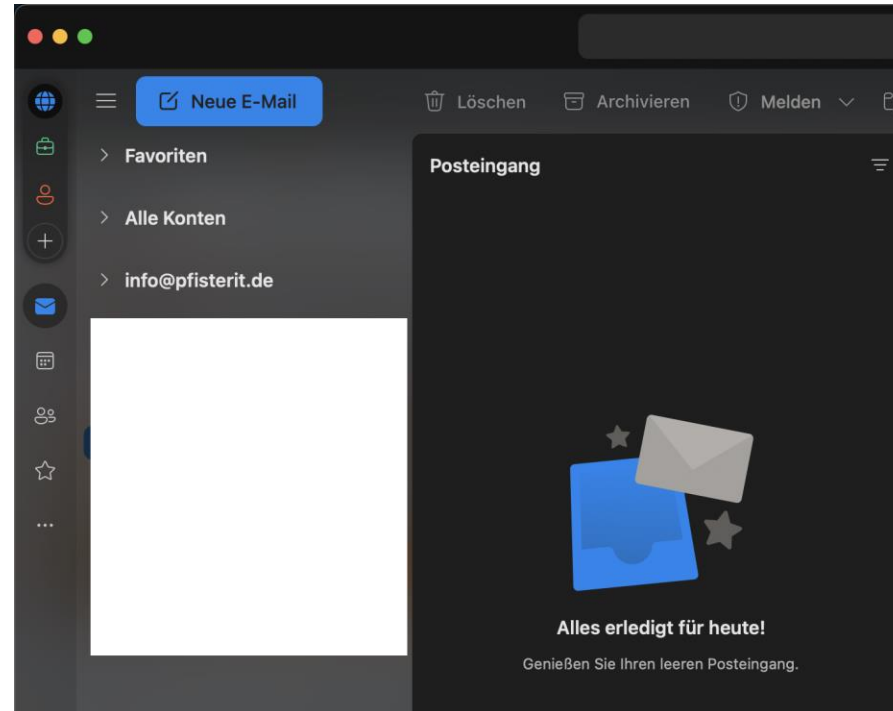
- Benjamin Pfister
- Leiter Netzwerk & Telekommunikation
- IT-Consultant
- Trainer
- Freier Autor



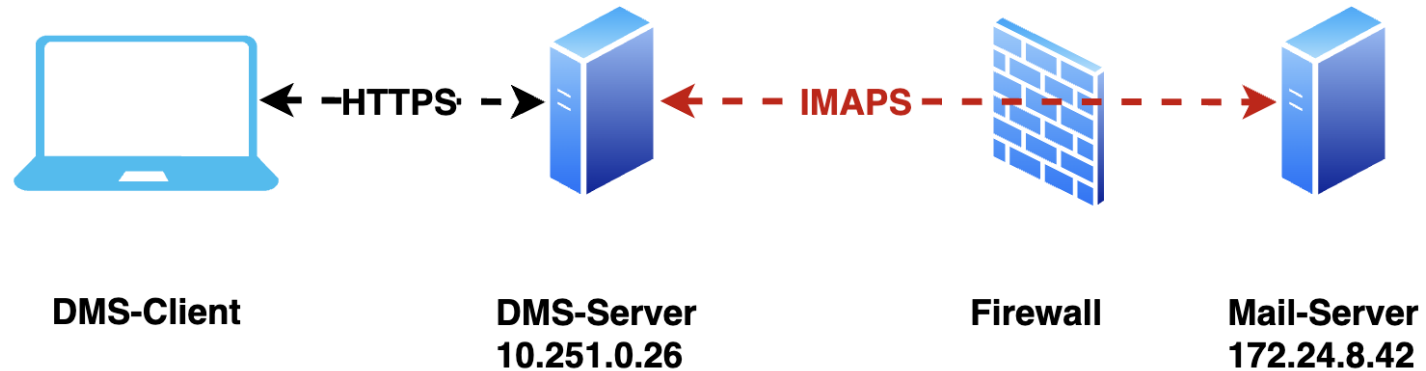
Case Studies

- Keine E-Mails im DMS
- Keine ausgehenden VoIP-Gespräche
- Falsche Stimmen auf Sprachbox
- Fehler Synchronisierung im Servercluster

Keine E-Mails im DMS



Keine E-Mails im DMS



Keine E-Mails im DMS

The image shows a Wireshark packet capture of a network session. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 571), and the bottom pane shows the packet bytes.

No.	Time	Source	Destination	Protocol	Length	Info
437	91.404000	192.168.4.24	192.168.4.1	NTP		90 NTP Version 3, client
438	91.404000	192.168.4.1	192.168.4.24	NTP		90 NTP Version 4, server
485	108.112000	192.168.4.1	192.168.4.1	DNS		75 Standard query 0xcabb A rps.yealink.com
486	108.128000	192.168.4.1	192.168.4.24	DNS		91 Standard query response 0xcabb A rps.yealink.com
534	111.516000	192.168.4.24	192.168.4.1	DNS		82 Standard query 0x4e6a A gw.intern.pfister.com
535	111.516000	192.168.4.1	192.168.4.24	DNS		98 Standard query response 0x4e6a A gw.intern.pfister.com
539	111.608000	192.168.4.24	192.168.4.1	TCP		66 12592 → 5061 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
540	111.608000	192.168.4.1	192.168.4.24	TCP		58 5061 → 12592 [SYN, ACK] Seq=0 Ack=1 Win=16384
541	111.608000	192.168.4.24	192.168.4.1	TCP		60 12592 → 5061 [ACK] Seq=1 Ack=1 Win=5840 Len=0
542	111.788000	192.168.4.24	192.168.4.1	TLSv1.2		182 Client Hello
543	111.788000	192.168.4.1	192.168.4.24	TCP		54 5061 → 12592 [ACK] Seq=1 Ack=129 Win=16384
544	111.792000	192.168.4.1	192.168.4.24	TLSv1.2		1078 Server Hello
545	111.792000	192.168.4.24	192.168.4.1	TCP		60 12592 → 5061 [ACK] Seq=129 Ack=1025 Win=7040
546	111.852000	192.168.4.1	192.168.4.24	TLSv1.2		539 Certificate, Server Hello Done
547	111.852000	192.168.4.24	192.168.4.1	TCP		60 12592 → 5061 [ACK] Seq=129 Ack=1510 Win=9216
552	112.620000	192.168.4.24	192.168.4.1	TLSv1.2		628 Client Key Exchange, Change Cipher Spec, Encrypted
553	112.620000	192.168.4.1	192.168.4.24	TCP		54 5061 → 12592 [ACK] Seq=1510 Ack=703 Win=16384
556	115.888000	192.168.4.1	192.168.4.24	TLSv1.2		280 New Session Ticket, Change Cipher Spec, Encrypted
557	115.888000	192.168.4.24	192.168.4.1	TCP		60 12592 → 5061 [ACK] Seq=703 Ack=1736 Win=9216
571	119.724000	192.168.4.24	192.168.4.1	TLSv1.2		658 Application Data
572	119.724000	192.168.4.1	192.168.4.24	TCP		54 5061 → 12592 [ACK] Seq=1736 Ack=1307 Win=16384

Details of packet 571 (Selected):

- Frame 571: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits)
- Ethernet II, Src: XiamenYe_c5:82:a3 (00:15:65:c5:82:a3), Dst: eImegt_7a:70:68 (08:00:27:7a:70:68)
- Internet Protocol Version 4, Src: 192.168.4.24, Dst: 192.168.4.1
- Transmission Control Protocol, Src Port: 12592, Dst Port: 5061, Seq: 703, Ack: 1736, Win: 9216, Len: 658
- Transport Layer Security
 - Record Layer: Application Data Protocol: sip.tcp
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 599
 - Encrypted Application Data: a7642d291c3150f33efd436fb84cc3504587c53de3443894
 - [Application Data Protocol: sip.tcp]

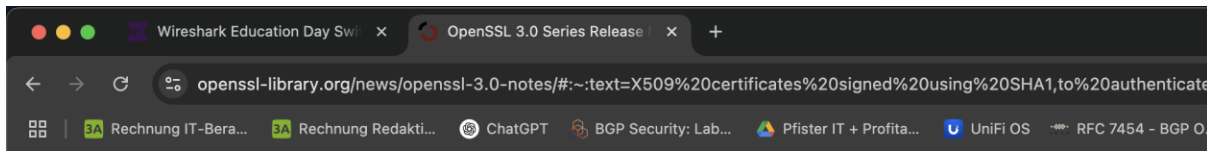
Packet bytes pane shows the Ethernet frame structure:

- Ethernet
 - Destination: 08:00:27:7a:70:68
 - Source: 00:15:65:c5:82:a3
 - Type: 0x0800
- Internet Protocol Version 4

Keine E-Mails im DMS

- Fehlgeschlagene Verbindung
- Alte funktionierende Verbindung

Keine E-Mails im DMS

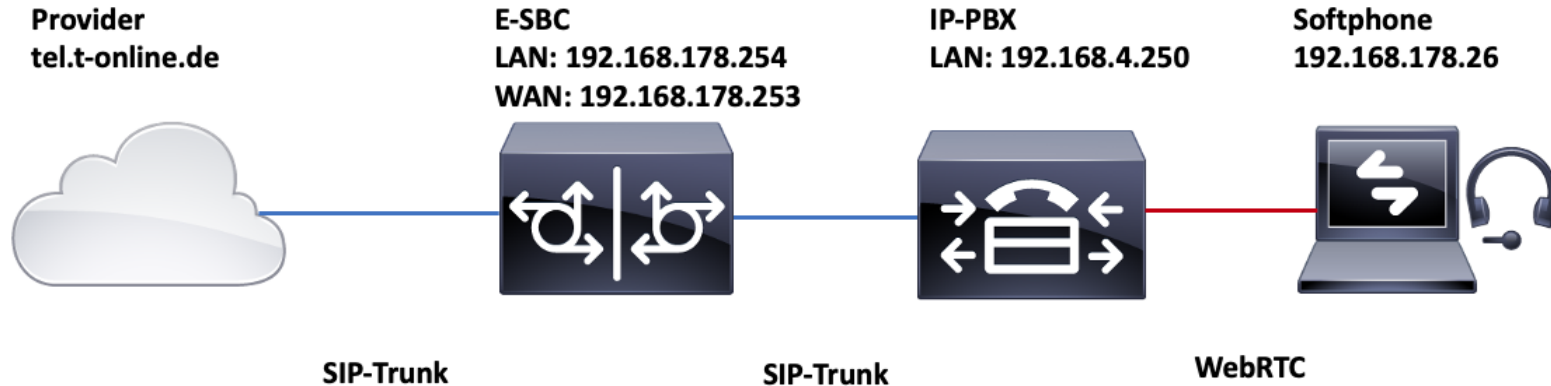


- Deprecated the `DSA` and `DSA\_METHOD` types and functions.
- Deprecated the `DH` and `DH\_METHOD` types and functions.
- Deprecated the `ERR\_load\_` functions.
- Remove the `RAND\_DRBG` API.
- Deprecated the `ENGINE` API.
- Added `OSSL\_LIB\_CTX`, a libcrypto library context.
- Added various `\_ex` functions to the OpenSSL API that support using a non-default `OSSL\_LIB\_CTX`.
- Interactive mode is removed from the `openssl` program.
- The X25519, X448, Ed25519, Ed448, SHAKE128 and SHAKE256 algorithms are included in the FIPS provider.
- X509 certificates signed using SHA1 are no longer allowed at security level 1 or higher. The default security level for TLS is 1, so certificates signed using SHA1 are by default no longer trusted to authenticate servers or clients.

Keine ausgehenden VoIP-Gespräche



Keine ausgehenden VoIP-Gespräche



Keine ausgehenden VoIP-Gespräche

Kein ausgehender Anruf

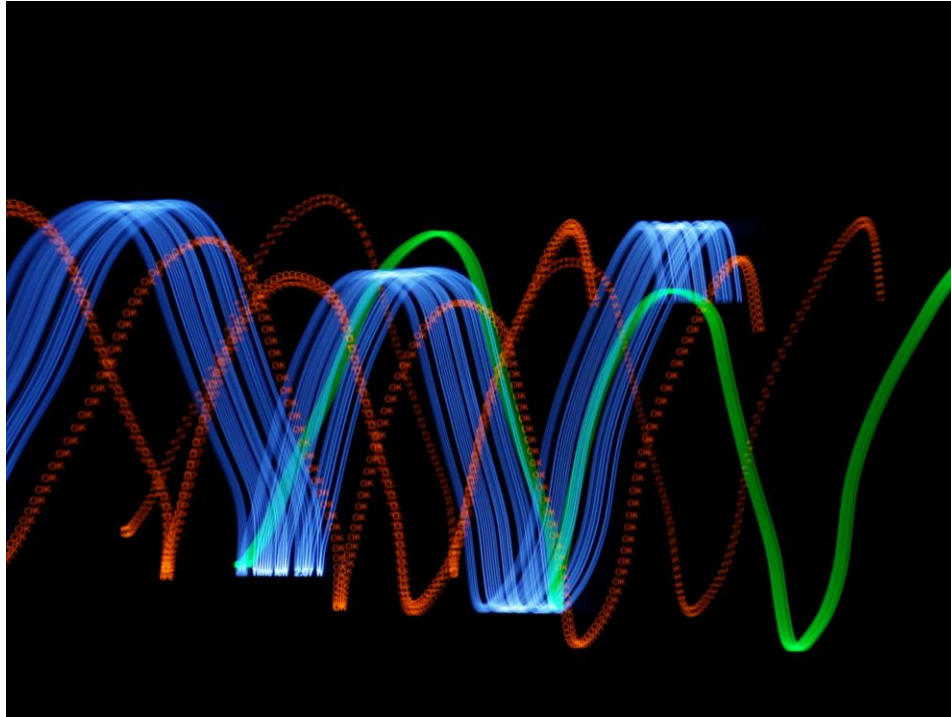
Keine ausgehenden VoIP-Gespräche

Root Cause

The SIP-PBX must reuse already existing TCP and TLS-connections to send and receive SIP-messages.

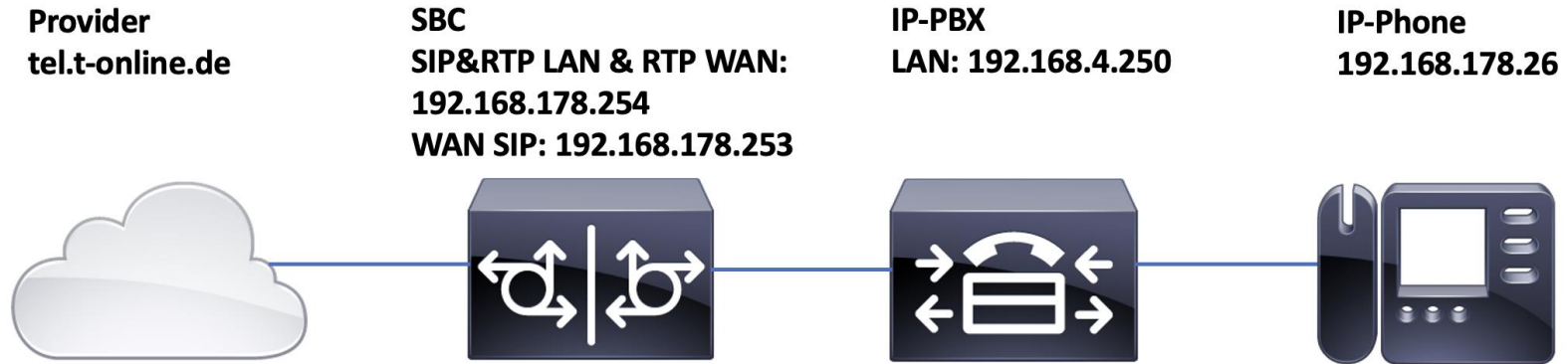
Quelle <https://www.telekom.de/hilfe/downloads/1tr118>

Vereinzelte falsche Gesprächsdaten auf Sprachbox



Vereinzelte falsche Gesprächsdaten auf Sprachbox

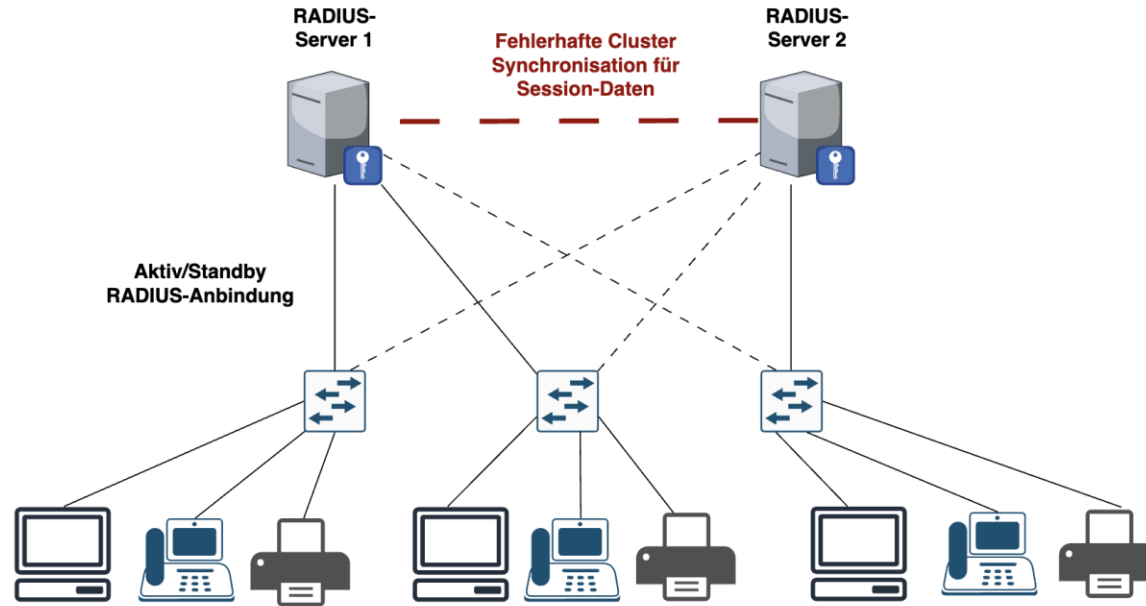
Topologie



Vereinzelt falsche Gesprächsdaten auf Sprachbox

Falsche Gesprächsdaten auf Sprachbox

Synchronisierung im Servercluster funktioniert nicht



Synchronisierung im Servercluster funktioniert nicht

Synchronisierungsfehler

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0
Replication and Synchronization	• HTTPS (SOAP): TCP/443 • Data Synchronization/ Replication (JGroups): TCP/12001 (Global) • ISE Messaging Service: SSL: TCP/8671 • ISE internal communication: TCP/15672 • Profiler Endpoint Ownership Synchronization/ Replication: TCP/6379

handshake_failure

Reception of a handshake_failure alert message indicates that the sender was unable to negotiate an acceptable set of security parameters given the options available. This is a fatal error.

Danke

linkedin.com/in/benjamin-pfister-90136b298



Sponsored by



&



emitec
datacom

