

Editorial

Liebe Leserin, lieber Leser,

dieses Sonderheft deckt wichtige aktuelle Netzwerkthemen ab. Es behandelt exemplarisch alle Ebenen der PC-Vernetzung, angefangen beim ersten Kabel, führt über Router-, Mesh- und Switch-Tests bis hin zur Konfiguration eines eigenen VPN.

Den Schwerpunkt bilden umfassende Beiträge zum beliebten Fritzbox-Router und zu seinem erneut stark verbesserten FritzOS. Zu den praktisch abgehandelten Themen gehören die vielseitige WireGuard-VPN-Vernetzung, ein schonungsloser Vergleich mit anderen IPv6-fähigen Routern und ausführliche Beiträge zur Fritzbox als Smart-Home-Zentrale mitsamt Konfigurationsbeispielen.

Das Heft erklärt Grundlagen und Hintergründe zur Mesh-Vernetzung mit dem aktuellen Wi-Fi 6 und hilft bei der Kaufentscheidung mit einem fundierten Test von Mesh-Kandidaten. Und es blickt mit dem ersten gründlichen Test auf das kommende Wi-Fi 7 voraus.

Falls Sie gerade ein neues Netzwerk aufsetzen, etwa vor einem Umzug, soll das Heft Ihnen als kompetenter Ratgeber zur Seite stehen, der durch die korrekte Installation leitet. Dabei hilft es mit einer Auswahl von günstigen Komponenten zur Verdrahtung, Einkaufslisten inklusive.

Aber egal, ob Sie Ihr eigenes kleines Netz als persönliches Bastelprojekt betreiben oder in Ihrem Betrieb das Netzwerk in Gang halten: Oft will man auf die Netzwerkgeräte auch von unterwegs per VPN zugreifen. Hier hat sich Entscheidendes getan, die modernsten VPNs ersparen Ihnen den zentralen Server. Was bedeutet: ein Flaschenhals weniger.

Viel Spaß beim Netzwerken wünscht



Dušan Živadinović

Inhalt

FRITZBOX EINRICHTEN UND TUNEN

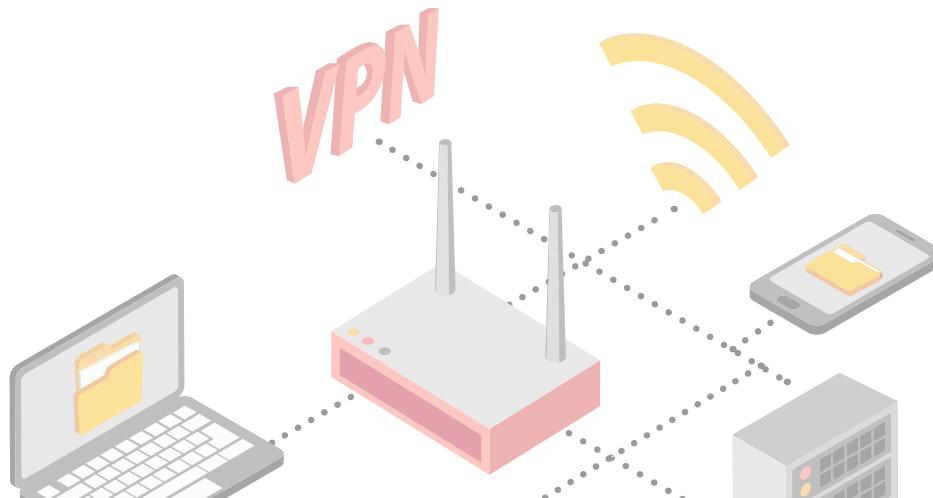
Fritzbox-Router bekommt man für alle üblichen Internetanschlüsse. Doch eine Fritzbox im Werkszustand ist wie das Internet ohne Webseiten – lesen Sie, wie Sie die Einstellungsvielfalt rund um WireGuard, MyFritz und Smart Home beherrschen.

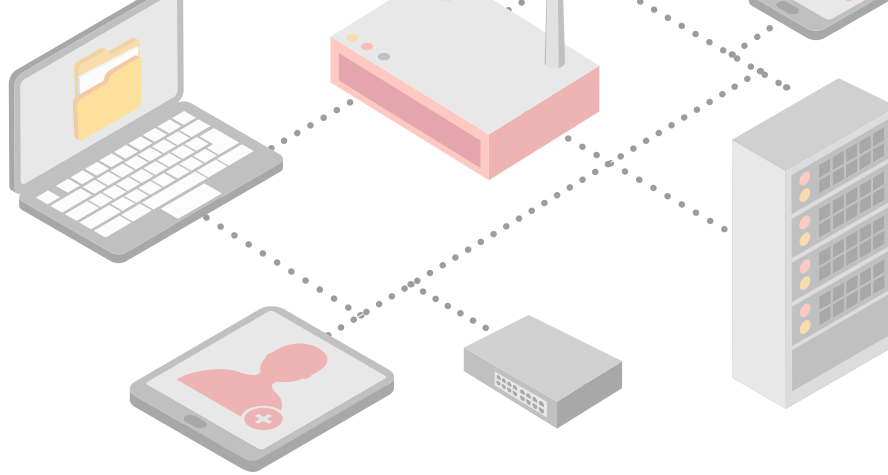
- 6 Zwei große Updates für Fritzboxen
- 12 Die richtige Fritzbox für jeden Zweck
- 16 25 Router auf IPv6 getestet
- 24 Abschied von der Fritzbox
- 30 Fritzbox als Smart-Home-Zentrale
- 34 Smart Home mit der Fritzbox einrichten
- 42 Fritzsmart-Gateway in der Praxis
- 48 Fritzbox per Bash-Script abfragen

SCHNELLES WLAN NUTZEN

Mesh-Systeme erleichtern die Abdeckung von Wohnungen zwar enorm, aber am Markt kämpfen teils sehr unterschiedliche Kandidaten um die Käufergunst. Wir ordnen den Stand der Technik ein und helfen mit gründlichen Tests bei der Kaufentscheidung.

- 56 Mesh-WLAN-Systeme richtig einsetzen
- 60 Sieben Mesh-Systeme mit Wi-Fi 6 getestet
- 68 „Revolutionärer WLAN-Booster“ entzaubert
- 72 Wi-Fi 7: Die nächste WLAN-Generation
- 76 Wi-Fi-6-Router RT6600ax getestet
- 78 Fritz-Repeater 3000 AX
- 79 Draußen-WLAN
- 80 Mesh-Kit TP-Link Deco XE75 untersucht
- 82 Orbi RBKE963: Mesh-Kit mit Wi-Fi 6E





NETZWERKE BAUEN

Egal, ob Sie Teile der Verkabelung modernisieren, das Netz erweitern oder gar völlig neu aufsetzen: Unser Ratgeber weist den Weg zu einem funktionalen, aber dennoch preisgünstigen Netzwerk und liefert Lösungen für viele aktuelle Netzwerkprobleme.

- 86 Netzwerkkabel günstig nachgerüstet
- 92 Koax-Switch
- 92 Koax-Express
- 93 Heimnetz per Telefondraht
- 94 Tipps & Tricks

VPN MODERNISIEREN

Die VPN-Technik entwickelt sich in unerwartete Richtungen. Peer-to-Peer-VPNs ersparen neuerdings den zentralen Server und locken mit stark vereinfachter Einrichtung. Und Google mischt ernsthaft mit und verhindert das Erstellen von Surf-Profilen.

- 100 VPN-Vernetzung mit Peer-to-Peer-Turbo
- 102 VPNs für PCs und Smartphones
- 108 Smartphoneschutz per PGPP
- 112 PCs und Heimnetze mit ZeroTier vernetzen
- 118 Google One VPN für PCs und Smartphones

ZUM HEFT

- 3 Editorial
- 75 Impressum
- 122 Vorschau: c't KI-Praxis

NETZWERKE

Heimnetze optimal einrichten

Schnelles WLAN nutzen

- 56, 60 Mesh & Repeater optimal auswählen
- 56, 60, 72 Das bringen Wi-Fi-6E und Wi-Fi-7

Netzwerke bauen

- 86 Preisgünstig verdrahten
- 94 Tipps & Tricks · schnelle Switches

VPN modernisieren

- 100 Peer-to-Peer statt VPN-Zentrale
- 108, 118 Mit speziellen VPNs die Privatsphäre schützen

Fritzbox einrichten und tunen

- 12 Kaufberatung: Die beste Fritzbox für jeden Anschluss
- 6 SmartHome: Zigbee- und DECT-Geräte kombinieren
- 30, 34, 42 Per WireGuard-VPN das Heimnetz unterwegs nutzen

€ 14,90
inkl. MwSt.
 zzgl. Versand

Zwei große Updates für Fritzboxen

Alle paar Jahre bekommen AVMs Router gratis ein großes Firmware-Update, das die vielseitigen Geräte noch nützlicher macht. AVM hat nun binnen Jahresfrist FritzOS 7.50 und 7.56 herausgebracht: Sie bringen unter anderem mehr Wumms ins VPN, machen das Telefonieren komfortabler und das Smart Home schlauer. Hier schildern wir, was FritzOS derzeit kann.

Von **Ernst Ahlers** und **Dušan Živadinović**

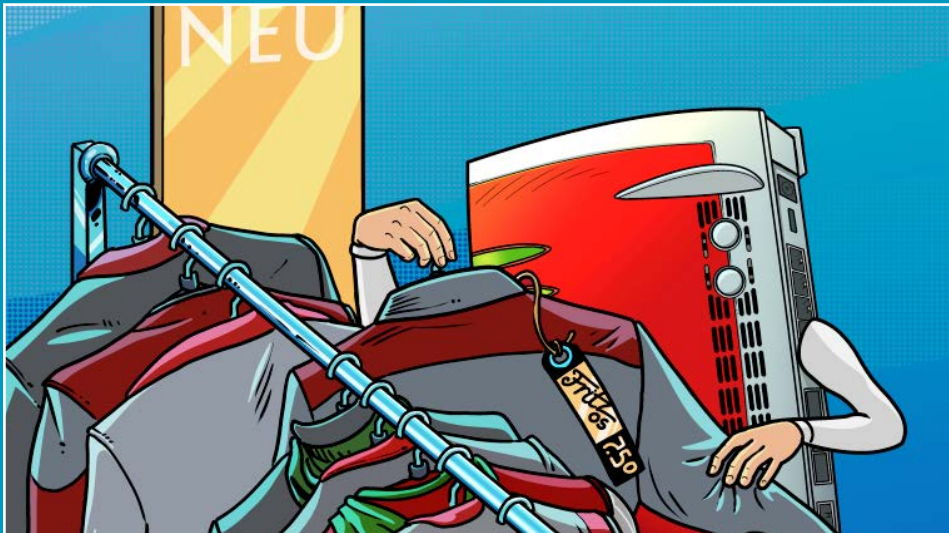


Bild: Michael Vogt

Zwei große Updates für Fritzboxen	6
Die richtige Fritzbox für jeden Zweck	12
25 Router auf IPv6 getestet	16
Abschied von der Fritzbox	24
Fritzbox als Smart-Home-Zentrale	30
Smart Home mit der Fritzbox einrichten	34
Fritzsmart-Gateway in der Praxis	42
Fritzbox per Bash-Script abfragen	48

AVM hat in diesem Jahr nach dem großen Update FritzOS 7.50 noch einige weitere Verbesserungen mit 7.56 herausgebracht. Vor allem 7.50, aber auch 7.56 enthalten viele nützliche Funktionen. Weil das große Update auf FritzOS 7.50 die meisten Neuigkeiten bringt, widmen wir uns diesem zuerst: Auf den ersten Blick unterscheidet es sich nur wenig vom Vorgänger, FritzOS 7.3x. AVM hat das Browsermenü dezent modernisiert, sodass es auf großen Bildschirmen besser lesbar ist. Falsche Klicks, durch die man bei älteren FritzOS-Versionen Änderungen ungewollt verworfen hat, kommen dank geschickter angeordneter „Übernehmen“- beziehungsweise „Verwerfen“-Knöpfen nicht mehr vor.

Mehr Neuerungen stecken unter der Haube: AVM hat mit FritzOS 7.50 weit über hundert Funktionen verbessert und Fehler behoben. Dazu kommen 17 neue Funktionen und 27 Änderungen. Das Update haben nicht nur alle zurzeit vertriebene Fritzboxen und WLAN-Repeater erhalten, sondern auch einzelne ältere Modelle wie die verbreitete 7490. Ist Ihr Router nicht darunter, liefern wir im nachfolgenden Artikel Tipps, wie Sie eine passende neue Fritzbox für Ihren Anschluss finden.

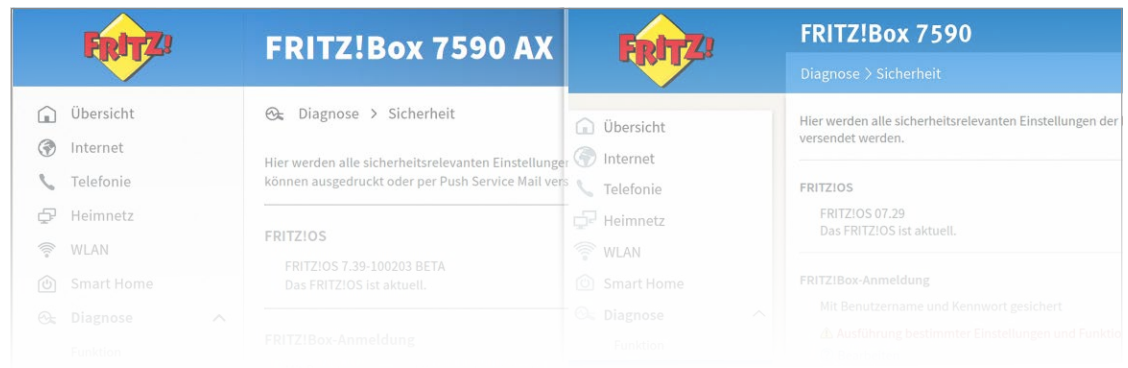
Mit einem virtuellen privaten Netz (VPN) kann man über eine verschlüsselte Verbindung beispiels-

weise aus der Ferne den Schwiegereltern Hilfeleistung geben. In Unternehmen verschaffen VPNs Heimarbeitern Zugriff auf Ressourcen im Firmennetz.

Das ist die größte Neuerung von FritzOS 7.50: WireGuard ist nun der moderne Kompagnon des alten IPsec-basierten Fritz-VPN. Der VPN-Neuling hat sich in den letzten Jahren rasant ausgebreitet und ist auch in den Linux-Kernel eingezogen, was auf Linux beschleunigte Verarbeitung gewährleistet.

Bei WLAN- Routern war die Deutsche Telekom der hiesige WireGuard-Pionier: Schon im Frühjahr 2020 erschien in Speedport-Geräten die erste Umsetzung für einen einzigen Zugang. Inzwischen lassen sich fünf definieren, aber nach wie vor können Speedports WireGuard erstens nur alternativ zu IPsec nutzen und zweitens VPN-Tunnel nur über IPv4 als Trägerprotokoll aufbauen [1].

Vielleicht hat das Telekom-Vorpreschen AVM dazu bewegt, WireGuard ebenfalls einzubauen. Das haben die Berliner dann gleich richtig angegangen, mit prinzipiell unbeschränkter Anzahl an Zugängen (genaueres dazu finden Sie im Artikel „Tipps & Tricks“ bei „Maximale Anzahl der Site-2-Site-Verbindungen“), parallelem Betrieb beider VPN-Typen und sowohl IPv4 als auch IPv6 als Trägerprotokolle. Schon die erste FritzOS-Laborversion auf der Fritzbox 7590 überraschte



Lesen Sie mehr in c't Netzwerke 2023

Mesh-WLAN-Systeme richtig einsetzen

Flottes Internet drahtlos im ganzen Haus, das versprechen Mesh-Systeme. Was ein Mesh ist und wie Sie es richtig installieren, erfahren Sie hier. Im folgenden Test haben wir sieben Kits mit dem aktuellen Wi-Fi-6-WLAN auf die Antennen gefühlt.

Von **Andrijan Möcker**



Bild: Andreas Martini

Mesh-WLAN-Systeme richtig einsetzen	56
Sieben Mesh-Systeme mit Wi-Fi 6 getestet	60
„Revolutionärer WLAN-Booster“ entzaubert	68
Wi-Fi 7: Die nächste WLAN-Generation	72
Wi-Fi-6-Router RT6600ax getestet	76
Fritz-Repeater 3000 AX	78
Draussen-WLAN	79
Mesh-Kit TP-Link Deco XE75 untersucht	80
Orbi RBKE963: Mesh-Kit mit Wi-Fi 6E	82

Vor 25 Jahren machte WLAN seine ersten Schritte, heute ist die allgegenwärtige Datenfunktechnik schnell, effizient und in allerhand Geräte integriert – vom Notebook über die Smartwatch bis hin zum Toaster. Die Naturgesetze kümmern dieser Fortschritt jedoch nicht: Wenn zwischen Router und Client dämpfende Hindernisse liegen, etwa eine Steinwand oder eine Stahlbetondecke, drosseln oder stoppen diese das Netz. Dann hilft nur, weitere WLAN-Zugangspunkte aufzustellen und so das Funknetz näher an seine Nutzer zu bringen.

Früher waren das Access Points und Repeater, heute dominieren Mesh-WLAN-Systeme den Markt für kleine Netze. Alle großen Netzwerkhersteller und viele Provider bieten Produkte an, um das Heim bestmöglich mit WLAN zu fluten. Derzeit sind Sets mit zwei bis vier Geräten und von 150 bis 2000 Euro erhältlich. Mancher mag nun glauben, „Mesh“ sei lediglich ein hipbes Wort für „Repeater“ und „Access-Point“. Doch es gibt einige Unterschiede, die Sie kennen sollten. Deshalb haben wir die Grundlagen aufgeschrieben und im nachfolgenden Artikel sieben Mesh-Systeme getestet.

Was ist Mesh?

Der klassische Repeater verbindet sich drahtlos mit dem WLAN-Router, der Access-Point nutzt spektrumschonend ein Kabel. Beide strahlen dasselbe Netz mit gleichem Funknetznamen (SSID), Verschlüsselungsmethode und Passwort aus. So können die Clients den signalstärksten Zugangspunkt herauspicken.

„Mesh“ ist im Privatkundenbereich primär ein Marketingbegriff und „WLAN-Systeme“ wäre treffender, dennoch machen die Geräte einiges besser als der erstbeste, billige Repeater aus irgendeinem Webshop: Die Zentrale jedes Mesh-Systems ist der Root-Node (Hauptknoten). Er stellt die Konfigurationsschnittstellen – Apps oder Browserseiten – des

einfach, indem man einen passenden Repeater dazu kauft und ihn mit dem Router koppelt – ein simpler Knopfdruck an beiden Geräten genügt und nach zwei Minuten funkt das Mesh.

Bei anderen Mesh-Kits agiert ein Gerät als Zentrale, der Root-Node (Hauptknoten). Er steckt per LAN-Kabel am Internet-Router oder Modem. Seine Kompagnons, die Repeater-Nodes, verteilt man über die abzudeckende Fläche. Sie arbeiten als Zugangspunkte für Endgeräte und leiten deren Daten weiter an den Root-Node.

Der Backbone (auch: Backhaul), also die Verbindung zwischen den Repeater-Nodes und dem Root-Node, läuft typischerweise wie bei klassischen Repeatern über Funk. Er bestimmt, wie viel Datenrate Clients erhalten, die sich mit den Mesh-Nodes verbinden. Viele Mesh-Systeme heben sich dabei durch Cross-Band-Repeating ab; sie entscheiden dynamisch, ob sie die Daten übers 2,4- oder 5-Gigahertz-WLAN-Band weiterleiten. Das verspricht mehr Durchsatz, weil die Datenpakete nicht zweimal auf demselben Funkband laufen müssen, sondern zwischen durch auf die „Parallelspur“ wechseln und deswegen die verfügbare Sendezeit (Airtime) besser nutzen.

Damit sich Clients nahtlos im abgedeckten Bereich bewegen können, gehören Roaminghelferfunktionen wie IEEE 802.11k (Radio Resource Management, Spektrumsmessung), 11v (BSS Transition, Basiswechsel) und 11r (Fast BSS Transition) mittlerweile zur Standardausstattung [1]. Außerdem können die Nodes schwächer werdende Clients gezielt „abwerfen“. So zwingen sie sie dazu, sich beim Wandern in der Wohnung mit einem signalstärkeren Kollegen zu verbinden.

Im Backbone spielt die Musik

Bei hochpreisigen Sets haben die Mesh-Nodes oft ein zusätzliches Funkmodul, mit dem sie auf einem separaten 5- oder 6-GHz-Kanal den Backbone aufbauen. Mit ihnen ist man flotter unterwegs als mit

Lesen Sie mehr in c't Netzwerke 2023

Netzwerkkabel günstig nachgerüstet

Stockende Videos und hakende Videokonferenzen aufgrund von lahmem WLAN und Powerline können den Geduldsfaden auf Spannung ziehen. Aber nur für wenige Jahre in der Mietwohnung teuer Netzwerkkabel in die Wand legen und renovieren? Muss nicht sein, so geht Gigabit-Ethernet günstig!

Von **Andrijan Möcker**



Netzwerkkabel günstig nachgerüstet	86
Koax-Switch	92
Koax-Express	92
Heimnetz per Telefondraht	93
Tipps & Tricks	94

Egal wohin man schaut: Überall gibt es kleine oder größere Netzwehwehchen; lahmes WLAN oder Powerline, schlechter Empfang und so weiter. Die Situation ist tatsächlich prekär, denn viele Menschen leben in Mietobjekten, wovon der Großteil seit Jahrzehnten nicht kernsaniert wurde. Selbst wenn, spart sich fast jeder Vermieter die Netzwerkinstallation; es gibt ja schließlich WLAN, so oft die Auffassung, und man muss ja nicht selbst drin wohnen.

Die alternativ aufgebaute kabellose Internetversorgung über WLAN-Mesh-Sets oder Powerline-Adapter (Ethernet übers Hausstromnetz) kommt jedoch vergleichsweise teuer und bleibt in puncto Geschwindigkeit oft hinter der Herstellerwerbung zurück; insbesondere, wenn massive Wände oder lange Stromleitungen die WLAN- beziehungsweise Powerline-Signale abschwächen. Groß ist die Enttäuschung, wenn von den 500 Mbit/s des neuen Glasfaseranschlusses drei Räume weiter nur 50 bis 100 Mbit/s übrig sind. Kurzum: Nur Twisted-Pair-Netzwerkkabel schaffen die Daten wirklich flott und günstig durchs Heim zum Router. Führen zusätzliche WLAN-Basen die Daten per Kabel statt durch die Luft zum Router, ist man auch an Mobilgeräten schneller unterwegs.

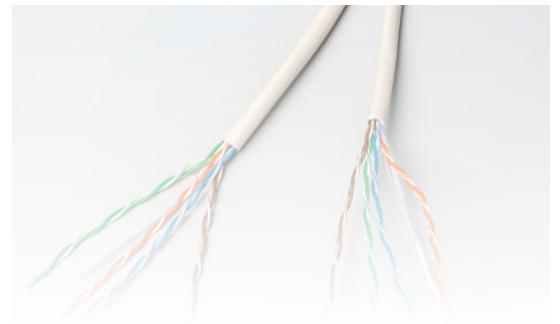
In einer Mietwohnung möchte man aber nicht tausende Euro für eine Netzwerkinstallation vom Elektriker und die dann erforderliche Renovierung ausgeben. Deshalb haben wir den Bauvorschlag fürs günstige Gigabit-Heimnetz zusammengestellt: Mit steckerlosem Netzwerkkabel, einfachen RJ45-Dosen, Plastik-Patchpaneln und Kabelkanal-Sockelleisten können Sie das Problem lösen. Dabei ist egal, ob Sie die ganze Wohnung verkabeln wollen oder nur zwei Anschlüsse benötigen. Die Installationskosten beginnen bei etwa 140 Euro für zwei Räume und vier Dosen.

Kern der Idee ist, Sockelleisten mit Kabeln zu versehen oder gegen solche mit Kabelkanal auszutauschen und so eine Netzwerkverteilung minimal-

entspricht nicht den aktuellen Standards für feste Installationen, er ist weder professionell noch Jahrzehnte zukunftstauglich. Er ist ein Kompromiss.

Falls Sie Wohneigentum besitzen, für das Sie zeitnah eine Renovierung planen, ist unser Vorschlag nichts für Sie. Investieren Sie in diesem Fall besser in eine professionelle Netzwerkverteilung mit Twisted-Pair-Installationskabel der Kategorie 8. Zwar kostet allein das Kabel rund einen Euro pro Meter, es eignet sich aber für 10 GBit/s und auf kürzeren Strecken sogar für 25 Gbit/s. Wir verwenden dieses Kabel in diesem Artikel nicht, weil es aufgrund von Dicke und Starrheit kaum für die engen Kabelkanäle geeignet ist und auch zu teuer für eine Interimslösung.

Die im Weiteren empfohlenen Cat-5e-Kabel liefern bis 90 Meter Länge mindestens Gigabit-Ethernet-Geschwindigkeit und auf Strecken unter 50 Metern je nach Signalgüte 2,5, 5 oder sogar 10 Gigabit pro Sekunde. Wir haben ein Vierer-Bündel aus ungeschirmtem Kategorie-5e-Patchkabel über 25 Meter getestet: Zwei 5-Gigabit- und zwei Gigabit-Verbindungen liefern anstandslos gleichzeitig, ohne sich gegenseitig zu stören. Verlassen Sie sich dennoch nicht darauf, denn äußere Störeinflüsse können einen Strich durch die Multigigabit-Rechnung machen.



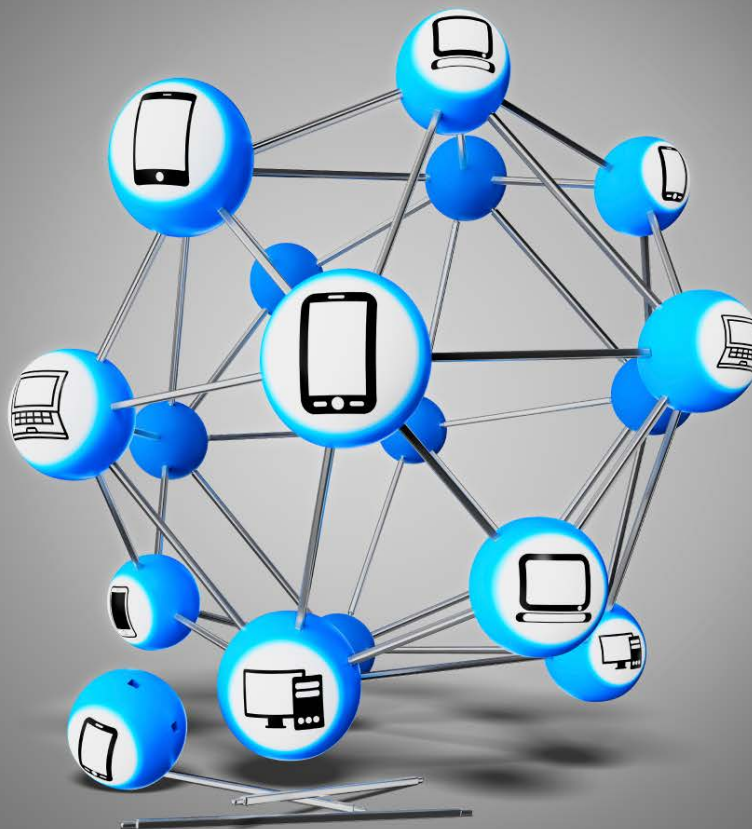
Lesen Sie mehr in c't Netzwerke 2023

VPN-Vernetzung mit Peer-to-Peer-Turbo

Bild: Andreas Martini

Fortgeschrittene VPN-Anwendungen koppeln Geräte mit Direktverbindungen, sprechen kleine Arbeitsgruppen an und nehmen dem Admin viel Arbeit ab. Außerdem stellen wir ein mächtiges Werkzeug zur digitalen Selbstverteidigung auf Smartphones vor, das ebenfalls auf VPN gründet.

Von **Dušan Živadinović**



VPN-Vernetzung mit Peer-to-Peer-Turbo	100
VPNs für PCs und Smartphones	102
Smartphoneschutz per PGPP	108
PCs und Heimnetze mit ZeroTier vernetzen	112
Google One VPN für PCs und Smartphones	118

Viele Anwendungen verwenden VPN-Techniken, aber teils für sehr unterschiedliche Zwecke. In der folgenden Artikelserie stellen wir sehr fortgeschrittene, aber zugleich sehr komfortable VPN-Anwendungen vor. An der Speerspitze der Entwicklung steht der Smartphone-Schutz Pretty Good Phone Privacy. Und wenn Sie entfernte Geräte miteinander koppeln wollen, sollten Sie Peer-to-Peer-VPNs kennen. Was sie leisten, stellen wir anhand von Nebula, Twingate, Tailscale und ZeroTier vor. Damit vernetzt man ferne Standorte und Geräte zum Beispiel für Freigaben und für die Fernwartung. Aber anders als bei herkömmlichen VPNs wie IPsec oder WireGuard steht dabei kein zentraler VPN-Server als Drehscheibe im Mittelpunkt. Dabei kommunizieren die Clients direkt miteinander, Peer-to-Peer.

Mit Pretty Good Phone Privacy zieht das US-Startup Invisio viel Aufmerksamkeit auf sich. Die Firma verspricht eine Tarnkappe für Smartphones, die sogar vor den Augen von Mobilfunknetzbetreibern schützt. Mehr dazu im Abschnitt „Spurlos funken“.

Die Peer-to-Peer-VPNs gehen auf gestiegene Schutzanforderungen und auf eine Modernisierung der Architektur zurück. In herkömmlichen VPNs bildet der Server den zentralen Umschlagpunkt und somit einen Engpass: Ein langsamer Internetanschluss des Servers bremst die Clients ebenso aus wie eine Serverüberlastung. Der Peer-to-Peer-Ansatz löst den Umschlagpunkt auf, Clients kommunizieren direkt miteinander. Zu dieser VPN-Klasse gehören etwa Tinc, yggdrasil und auch manche Selbstbauanleitung (siehe ct.de/wxw1).

Die Verteilung von kryptografischen Schlüsseln und Konfigurationen erledigt man per Browser in einem zentralen Dashboard per Mausklick.

Ein Beispiel ist ZeroTier, mit dem man Server, PCs, NAS-Geräte und Smartphones vernetzt. Das geht so schnell, dass man von Blitz-VPNs sprechen kann. Mehr dazu lesen Sie in den nachfolgenden Artikeln.

Büroverbesserung

man hinter der Firewall VPN-Server ein, zu denen ähnlich einer Zugbrücke ein gut geschützter Zugang führt. Das interne Netz gilt als sichere Umgebung für Unternehmensanwendungen.

Doch längst sind Fachleute überzeugt, dass auch das interne Netzwerk voller Gefahren steckt. Beispielsweise können Phishing-Mails zum Herunterladen von Schadsoftware verleiten.

Hinzu kommt, dass viele Mitarbeiter im Homeoffice bleiben und viele Applikationen vom abgeschotteten Firmenserver in die Cloud wandern. So sind immer mehr Mitarbeiter und Betriebsmittel übers Internet verstreut. Ein traditionelles VPN ist daher schwer zu verwalten.

Nach neueren Konzepten ist keinem Netzwerkgerät und keinem Nutzer zu trauen, jeglicher Zugriff auf Firmenressourcen muss authentifiziert, autorisiert und verschlüsselt werden (Zero Trust). Zusätzlich schränkt man den Zugriff auf die für die Arbeit erforderlichen Ressourcen und Applikationen ein (Least Privilege). So schrumpft die Angriffsfläche und es spielt keine Rolle, wo sich Mitarbeiter physisch aufhalten.

Zu dieser VPN-Klasse gehören Tailscale, Twingate und Nebula, die wir im nachfolgenden Artikel vorstellen. Tailscale gründet auf dem modernen WireGuard. Das gilt auch für das noch junge NetBird, an dem das Saarbrücker CISA Helmholtz Center für Informationssicherheit mitwirkt. Das c't-Magazin widmet NetBird einen separaten Beitrag in einer der kommenden Ausgaben.

Spurlos funken

VPNs können andererseits auch im Mobilfunk die Privatsphäre schützen. Kritiker sehen diese Privatsphäre längst ausgehöhlt und halten Smartphones mit GPS für digitale Plaudertaschen.

Eine durchgehende digitale Selbstverteidigung fällt da schwer. Selbst Apples Private Relay und Google One VPN schützen nur die Kommunikation

Lesen Sie mehr in c't Netzwerke 2023