TDT®

Your experts in **TELE COMMUNICATION**

Bundesamt für Sicherheit in der Informationstechnik

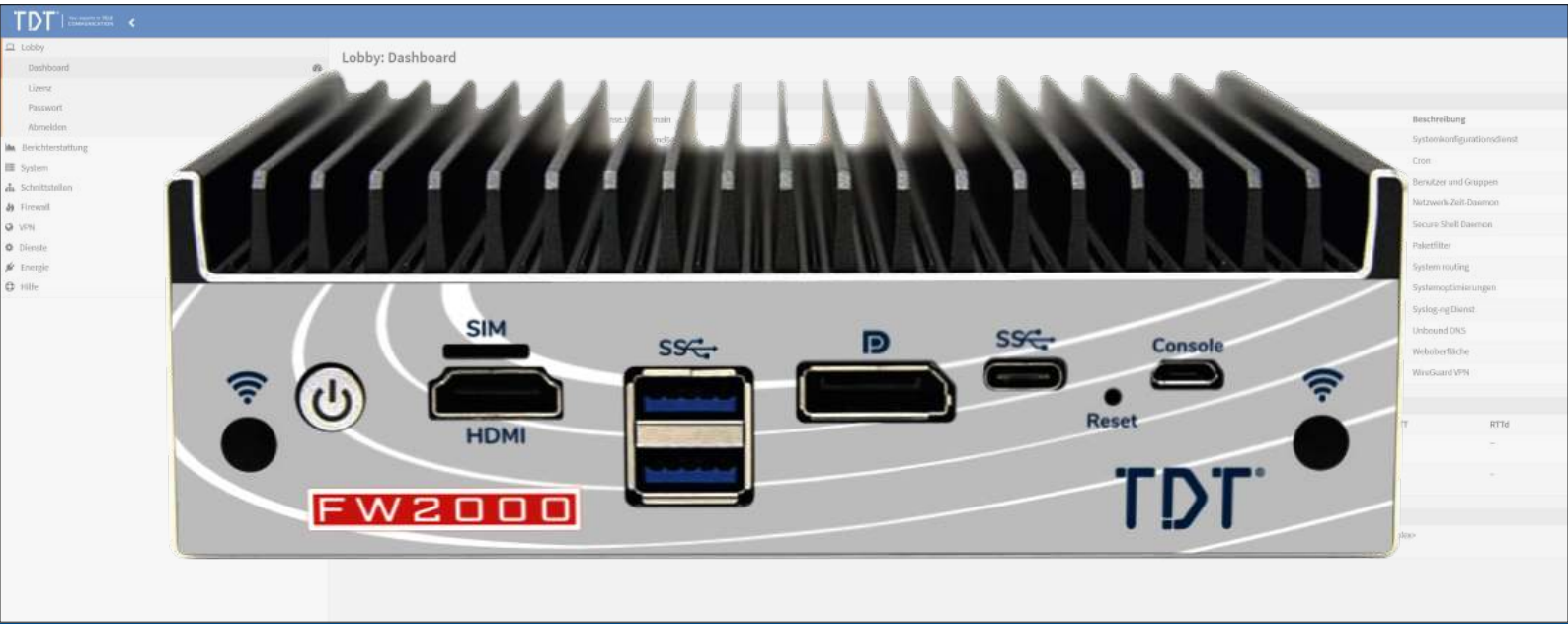
ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz

Zertifikat Nummer:
BSI-IGZ-0495-2022
Gültig bis 22.08.2025

DATENBLATT FW2000

SOHO FIREWALL

TDT AG – Ihr Experte für sichere und innovative Telekommunikation



SICHERHEIT

TDT AG – MADE IN GERMANY

Version 2.000.00
Stand 12.07.2024

FW2000

DIE SOHO FIREWALL VON TDT

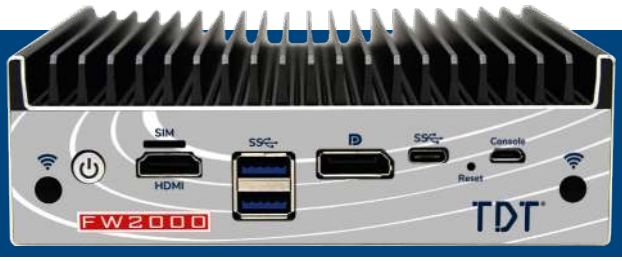
Maximale Sicherheit, Datenverfügbarkeit und Service

Perfekter Schutz für SOHO-Umgebungen (Small Office, Home Office) – sichern Sie Ihre Verbindungen und schützen Sie Ihr Netzwerk vor potenziellen Bedrohungen.

Die FW2000 Firewall bietet umfassende Sicherheitsfunktionen, darunter eine leistungsstarke Stateful Inspection Firewall und ein fortschrittliches Inline Intrusion Detection & Prevention System. Diese Kombination gewährleistet maximalen Schutz und hält Ihr Netzwerk sicher vor Angriffen und unbefugtem Zugriff. Sichern Sie den Zugriff auf Ihr Netzwerk mit OpenVPN, IPsec oder dem optional als Plugin installierbaren WireGuard.

Verbessern Sie die Netzwerkleistung mit dem Traffic Shaper, um z. B. Voice over IP gegenüber anderem Datenverkehr zu priorisieren. Blockieren Sie unerwünschten Datenverkehr mithilfe der kategorienbasierten Webfilterung. Die Firewall verfügt zudem über ein integriertes Captive Portal mit Voucher-Unterstützung, das sich einfach und schnell einrichten lässt.

Sie haben Fragen? Wir sind für Sie da
+49 8703 929-00 oder info@tdt.de



Die wichtigsten Features im Überblick

- Dashboard
- Statefull Firewall
- Aliase (GeoLite Country Database)
- TRAFFIC SHAPER
- 2FA
- Intrusion Detection & Prevention System
- High Availability (CARP)
- Netflow Analysator
- Captive Portal
- Caching Proxy
- Reporting & Monitoring
- Backup & Restore

Stateful Firewall

Eine Stateful Firewall ist eine Firewall, die den Status von Netzwerkverbindungen (wie TCP-Streams, UDP-Kommunikation), die über sie laufen, verfolgt. Das System bietet die Möglichkeit, Firewall-Regeln nach Kategorien zu gruppieren, eine optimale Funktion für anspruchsvollere Netzwerk-Setups.

Dashboard

Die moderne Benutzeroberfläche liefert eine eingängige Benutzererfahrung mit integrierter Hilfe und schneller Navigation mit dem Suchfeld.
Die FW4000 bietet eine Dashboard-Funktion, mit der Sie schnell den Status der Firewall überprüfen können, mit mehrspaltiger Drag-and-Drop-Unterstützung.

Captive Portal

Das Captive Portal ermöglicht es Ihnen, eine Authentifizierung zu erzwingen oder eine Weiterleitung zu einer Click-Through-Seite für den Netzwerkzugang. Dies wird häufig in Hotspot-Netzwerken verwendet, ist aber auch in Unternehmensnetzwerken weit verbreitet, um eine zusätzliche Sicherheitsebene für den drahtlosen Internetzugang zu schaffen. Das System bietet die meisten Unternehmensfunktionen, einschließlich Radius- und Voucher-Unterstützung.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung, auch bekannt als 2FA oder 2-Step Verification, ist eine Authentifizierungsmethode, die zwei Komponenten erfordert wie z.B. einen Pin/Passwort + ein Token. Die Firewall bietet volle Unterstützung für die Zwei-Faktor-Authentifizierung (2FA) im gesamten System unter Verwendung von TOTP wie z. B. dem Google Authenticator.

Traffic Shaper

Das Traffic Shaping der Firewall ist sehr flexibel und basiert auf Pipes, Warteschlangen und entsprechenden Regeln. Die Pipes definieren die erlaubte Bandbreite; die Queues können verwendet werden, um eine Gewichtung innerhalb der Pipe festzulegen und schließlich werden die Regeln verwendet, um das Shaping auf einen bestimmten Paketfluss anzuwenden. Die Shaping-Regeln werden unabhängig von den Firewall-Regeln und anderen Einstellungen gehandhabt.

Aliase & GeoLite Country Database

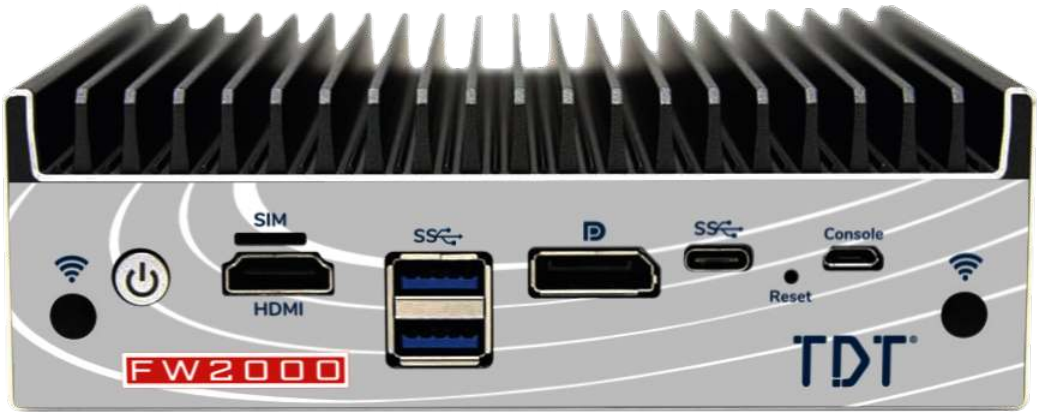
Die Verwaltung von Firewall-Regeln war noch nie so einfach. Durch die Verwendung von Aliasen können Sie mehrere IPs oder Hosts in einer Liste gruppieren, um sie in Firewall-Regeln zu verwenden. Zusätzlich können IP- oder Hostnamen von externen URLs abgerufen werden. Beispiele dafür sind DROP (Do Not Route Or Peer), der Ransomware-Tracker von Abuse.ch und die eingebaute Maxmind GeoLite2 Länderdatenbank.

High Availability / Hardware Failover

Die Firewall nutzt das Common Address Redundancy Protocol (CARP) für die Hardware-Ausfallsicherung. Zwei oder mehr Firewalls können als Failover-Gruppe konfiguriert werden. Wenn eine Schnittstelle der primären Firewall ausfällt oder die primäre Firewall komplett offline geht, wird die sekundäre Firewall aktiv. Durch die Nutzung dieser leistungsstarken Funktion entsteht eine vollständig redundante Firewall mit automatischem und nahtlosem Failover. Während der Umschaltung auf das Backup bleiben die Netzwerkverbindungen mit minimaler Unterbrechung für die Benutzer aktiv.

Caching Proxy

Der enthaltene Caching Proxy ist voll funktionsfähig und beinhaltet kategorienbasierte Webfilterung, umfangreiche Access Control Lists und kann im transparenten Modus laufen. Der Proxy kann mit dem Traffic Shaper kombiniert werden, um die Benutzerfreundlichkeit zu erhöhen. Die Integration mit den meisten professionellen Anti-Virus-Lösungen ist über die ICAP-Schnittstelle möglich.



SOFTWARE

Funktionen

Stateful Firewall
- Filter by
  - Source
  - Destination
  - Protocol
  - Port
  - OS (OSFP)
- Limit simultaneous connections on a per rule base
- Log matching traffic on a per rule bases
- Policy Based Routing
- Packet Normalisation
- Option to disable filter for pure router mode

Policy Organisation
- Alias Support
  - IP addresses
  - Port ranges
  - Domain names (FQDN)
- Interface Groups
  - Create security zones with equal rules
- Rule Category
  - Easy access rule sets

Granular Control State Table
- Adjustable state table size
- On a per rule bases
  - Limit simultaneous client connection
  - Limit states per host
  - Limit new connections per second
  - Define state timeout
  - Define state type
- State types
  - Keep
  - Sloppy
  - Modulate
  - Synproxy
  - None
- Optimisation options
  - Normal
  - High latency
  - Agressive
  - Conservative

Authentication
- External Servers
  - LDAP
  - Radius
- Integrated Servers
  - Local User Manager
  - Vouchers / Tickets
  - FreeRadius (Plugin)
- Authorisation
- User Interface
  - Local User Manager
- Accounting
- FreeRadius (Plugin & External)
- Vouchers / Tickets

2-Factor Authentication
- Supports TOTP
- Google Authenticator
- Support services:
  - Captive Portal
  - Proxy
  - VPN
  - GUI
  - SSH / Console

Certificates
- Certificate Authority
  - Create or Import CA's
  - Create or Import Certificates
- Let's Encrypt (Plugin)
  - Automated (Trusted) CA

802.1Q VLAN Support
- max 4096 VLAN's
- Link Aggregation & Failover
- Failover
- Load Balance
- Round Robin
- Cisco Ether Channel (FEC)
- 802.3ad LACP

Other Interface Types
- Bridged interfaces
- Generic Tunnel Interface (GIF)
- Generic Routing Encapsulation
- 802.1ad QinQ

Network Address Translation
- Port forwarding
- 1:1 of ip's & subnets
- Outbound NAT
- NAT Reflection

Traffic Shaping
- Limit bandwidth
- Share bandwidth
- Prioritise traffic
- Rule based matching
  - Protocol
  - Source
  - Destination
  - Port
  - Direction

IGMP Proxy
- For multicast routing

Universal Plug & Play
- Fully supported
- Dynamic DNS
- Selectable form a list
- Custom
- RFC 2136 support

DNS Forwarder
- Host Overrides
- Domain Overrides
- DNS Server
- Host Overrides
  - A records
  - MX records

Funktionen

- Access Lists

DNS Filter
- Supports OpenDNS

DHCP Server
- IPv4 & IPv6
- Relay Support
- BOOTP options

Multi WAN
- Load balancing
- Failover
- Aliases

Load Balancer
- Balance incoming traffic over multiple servers

Network Time Server
- Hardware devices
  - GPS
  - Pulse Per Second

Intrusion Detection & Prevention
- Inline Prevention
- Integrated rulesets
  - SSL Blacklists
  - Feodo Tracker
  - Geolite2 Country IP
  - Emerging Threats ETOpen
- SSL Fingerprinting
- Auto rule update using configurable cron

Captive Portal
- Typical Applications
  - Guest Network
  - Bring Your Own Device (BYOD)
  - Hotel & Camping Wifi Access
  - Template Management
  - Multiple Zones
- Authenticators
  - All available authenticators
  - None (Splash Screen Only)
- Voucher Manager
  - Multiple Voucher Databases
  - Export vouchers to CSV
- Timeouts & Welcome Back
- Bandwidth Management
  - Use Traffic Shaper
- Portal bypass
  - MAC and IP whitelisting
- Real Time Reporting
  - Live top IP bandwidth usage
  - Active Sessions
  - Time left
  - Rest API

Virtual Private Networks
- IPsec
  - Site to Site
  - Road Warrior
- OpenVPN
  - Site to Site
  - Road Warrior
  - Easy client configuration exporter
- Tinc (Plugin)
  - Full mesh routing
- ZeroTier (Plugin)
  - VPN, SDN & SD-WAN
- PPTP (Legacy)
- LT2P (Legacy)

High Availability
- Automatic hardware failover
- Synchronised state table
- Configuration synchronisation

Caching Proxy
- Multi interface
- Transparent Mode
- Support SSL Bump
- SSL Domain only (easy filtering)
- Access Control Lists
- Blacklists
- Category Based Web-filter
- Traffic Management
- Auto sync for remote blacklists
- ICAP (supports virus scan engine)

Virus Sanning
- External engine support (ICAP)
- ClamAV (Plugin / C-ICAP)

Reverse Proxy
- HAProxy - Load balancer (Plugin)

Online Identity Protection
- Tor - Anonymity online (Plugin)

Backup & Restore
- History & Diff support
- File Backup
- Cloud Backup

SNMP
- Monitor & Traps

Diagnostics
- Filter reload status
- Firewall Info (pfInfo)
- Top Users (pfTop)
- Firewall Tables
  - Aliases
  - Bogons
- Current Open Sockets
- Show All States
- State Reset
- State Summary
- Wake on LAN
- ARP Table
- DNS Lookup
- NDP Table
- Ping
- Packet Capture
- Test Port
- Trace route

Monitoring
- Zabbix Agent (Plugin)
- Monit (Plugin)
  - Proactive System Monitoring
- Checkmk (SNMP)

Enhanced Reporting
- Network Flow Analyser ‘Insight’
  - Fully Integrated
  - Detailed Aggregation
  - Graphical Representation
  - Clickable and Searchable
  - CVS Exporter
- System Health
  - Round Robin Data

Funktionen

- Selection & Zoom
- Exportable

⊙ Traffic Graph
- Live Traffic Monitoring

Network Monitoring

⊙ Netflow Exporter
- Version 5 & version 9
- Local for 'Insight'

Firmware

⊙ Support Virtual Installs
- VMware tools (Plugin)
- Xen Guest Utilities (Plugin)

⊙ Easy Upgrade
- Reboot warning for base upgrades

⊙ SSL Flavour selectable
- OpenSSL
- LibreSSL

⊙ Selectable Package Mirror

⊙ Reinstall Single Package

⊙ Lock Package (prevents upgrade)

⊙ Audit Feature
- Check installed packages for known security vulnerabilities

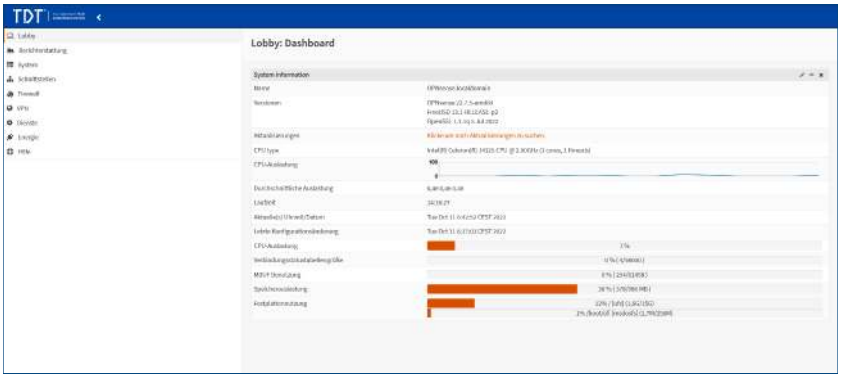
⊙ Plugin Support

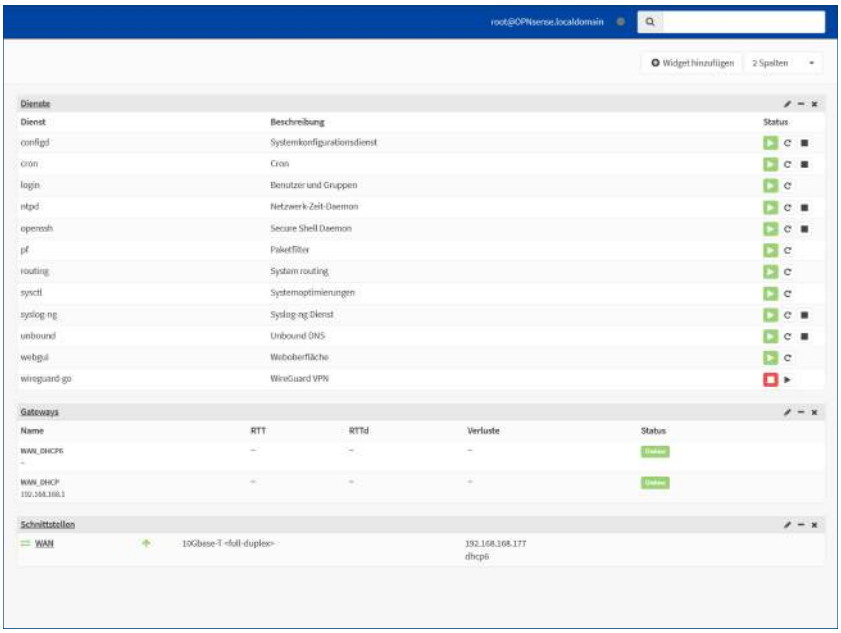
REST API

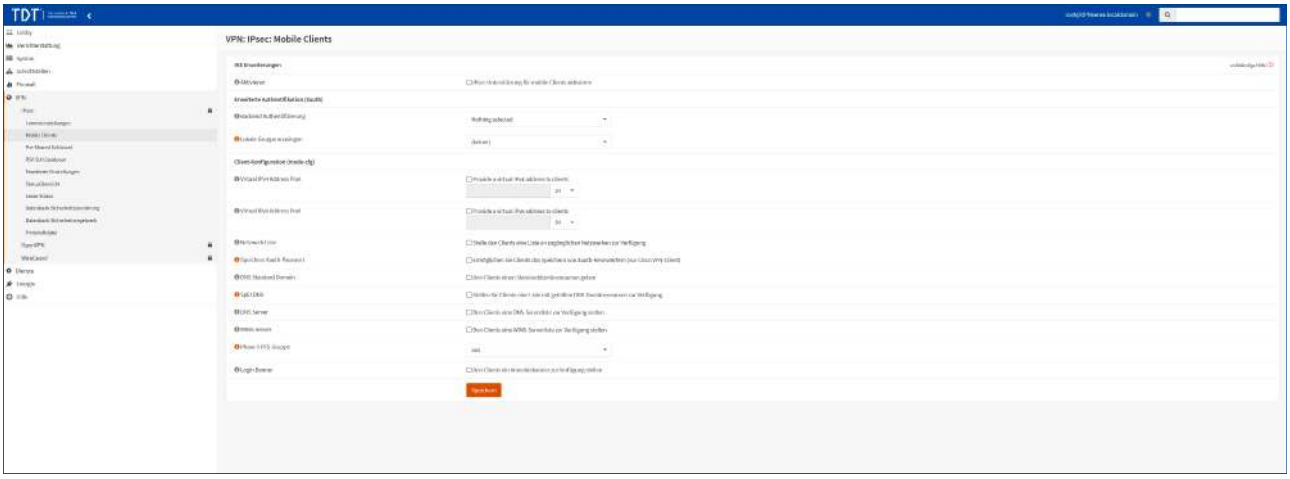
⊙ ACL support

Online Documentation

⊙ Free & Searchable







Hardware

Basissystem

Prozessor	Leistungsfähiger Quad-Core Prozessor mit bis zu 2.6 GHz
Arbeitsspeicher	8 GB DDR4-3200
Systemspeicher	120 GB M.2 SSD
Ethernet-Ports	4x 2.5G Ethernet, RJ45
LEDs	1x Power Button (blau), 1x Betriebsanzeige (grün), 1x LED-Festplattenaktivitätsanzeige (rot), 1x LED-Festplattenaktivitätsanzeige (gelb)
Video / Grafik	1x HDMI 1.4, 1x DP 1.4
USB Ports	2x USB 3.0 Typ A, 1x USB-C 3.2 Typ C
Konsole	1x USB Micro 2.0 (Serielle RS232-Kommunikation über UART)

Technische Daten

Robustes Metallgehäuse	Desktop, Lüfterlos
Abmessungen	50 mm (H), 146 mm (B), 127 mm (T)
Gewicht	Ca. 800 g
Betriebstemperatur	-10°C bis 50°C (Im laufenden Betrieb)
Luftfeuchtigkeit	0-95% (nicht kondensierend)
Maximale Leistungsaufnahme	max. 24W

Garantie

Herstellergarantie	2 / 3 Jahre Bring-In Garantie

Lieferumfang

	FW2000, Patchkabel, Netzteil, Quickstart-Anleitung

Durchsatz

Unverschlüsselt (Mbps) "#iPerf3 -c -P4 -f m"	~2330 Mbit/s
IPSec (OPNsense) 128 bit AES-GCM w/ 128 bit ICV/AES-XCBC/14 [2048 bits] DH/ AES128gcm16/No Hash/14 [2048 bits] PFS "#iPerf3 -c -P4 f m"	~1320 Mbit/s
WireGuard (OPNsense wireguard-go) 256-bit ChaCha20Poly1305 Avg (Mbps) "#iPerf3 -c -P4 -f m"	~1200 Mbit/s

Anmerkung
In diesem Beispiel werden Daten vom LAN-Netzwerk 192.168.50.0 über die WAN-Schnittstelle zum LAN-Netzwerk 192.168.60.0 „getunnelt“. In umgekehrter Richtung werden Daten vom LAN-Netzwerk 192.168.60.0 über die WAN-Schnittstelle zum LAN-Netzwerk 192.168.50.0 „getunnelt“. Der maximale Durchsatz, der über den IPsec-Tunnel für eine 1-Gbit/s-Ethernet-Schnittstelle getestet wurde, beträgt ~ 880 Mbit/s, was aufgrund des durch die IPsec-Konfiguration hinzugefügten Overheads zu erwarten ist.

Schlussfolgerungen zur OpenVPN- und IPSec-Leistung
OpenVPN ist ein wichtiger Satz von Protokollen, die für eine sichere Kommunikation über das Internet verwendet werden. Es gibt viele verschiedene Cipher Suites, die je nach den Anforderungen des Benutzers verwendet werden können. Die verwendete Konfiguration kann sich auf die Leistung und damit auf den Durchsatz der Geräte im Netzwerk auswirken.

Schlussfolgerungen zur WireGuard-Leistung
WireGuard ist ein moderner VPN-Tunnel, der für eine sichere Kommunikation über das Internet entwickelt wurde. Er zeichnet sich durch seine Einfachheit, Schnelligkeit und Effizienz aus. Dank der Verwendung modernster Kryptografie und einer minimalen Codebasis bietet WireGuard eine hervorragende Leistung. Die Konfiguration von WireGuard ist im Vergleich zu traditionellen VPN-Lösungen weniger komplex, was die Wahrscheinlichkeit von Konfigurationsfehlern verringert und die Benutzerfreundlichkeit erhöht. Die Wahl der Cipher Suites und die Anpassung der Netzwerkkonfiguration können die Leistung beeinflussen, aber generell zeigt WireGuard in den meisten Szenarien eine bemerkenswerte Durchsatzleistung und niedrige Latenzzeiten. Diese Merkmale machen WireGuard zu einer attraktiven Option für Nutzer, die eine leistungsfähige und sichere VPN-Lösung suchen.

Ansichten

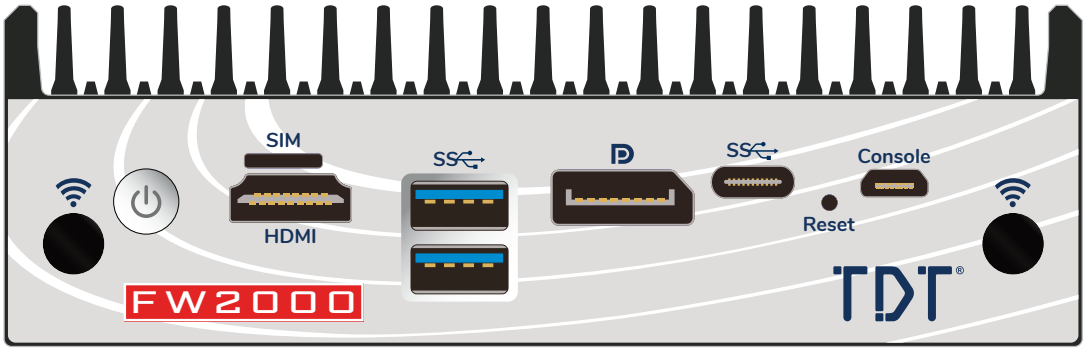


Abb. FW2000 Vorderseite

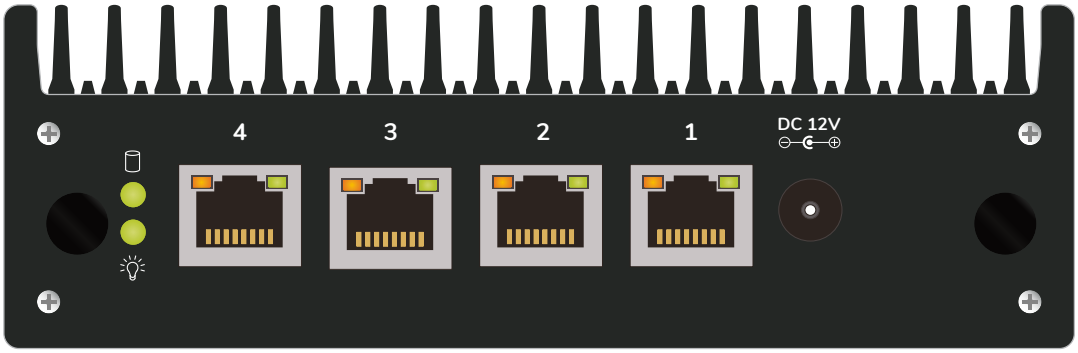


Abb. FW2000 Rückseite

Weitere Informationen

Weitere Informationen erhalten Sie unter der Rufnummer **+49 8703 929 00** oder per Mail an **info@tdt.de**.

EU-Konformitätserklärung

Hiermit erklärt TDT, dass der Telekommunikationsendeinrichtungstyp **FW2000** der Richtlinie **2014/35/EU** entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: **download.tdt.de**