Your experts in **TELE COMMUNICATION**

DATENBLATT FW5000

HIGH-END SECURITY FIREWALL

TDT AG – Ihr Experte für sichere und innovative Telekommunikation

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

SICHERHEIT

TDT AG – MADE IN GERMANY

Version 1.007.00
Stand 28.09.2023

Technische Änderungen und Irrtümer vorbehalten.

FW5000

DIE HIGH-END SECURITY FIREWALL VON TDT

Maximale Sicherheit, Datenverfügbarkeit und Service

Schützen Sie Ihr Unternehmensnetzwerk und sichern Sie Ihre Verbindungen mit OpenVPN, IPsec oder WireGuard (optional als Plugin installierbar), um eine sichere Netzwerkverbindung zu und von Ihren Außenstellen herzustellen. Von der Stateful Inspection Firewall bis zum Inline Intrusion Detection & Prevention System ist alles enthalten. Nutzen Sie den Traffic Shaper, um die Netzwerkleistung zu verbessern und priorisieren Sie Voice over IP vor anderem Datenverkehr.

Begrenzen Sie die verfügbare Bandbreite und teilen Sie sie gleichmäßig auf, nutzen Sie die kategorienbasierte Webfilterung, um unerwünschten Datenverkehr zu filtern. Die Firewall verfügt über ein eingebautes Captive Portal mit Voucher-Unterstützung und kann dieses einfach und schnell erstellen.

Genießen Sie die einfache Konfiguration und die durchsuchbare Online-Dokumentation mit einfachen Anleitungen, damit Sie schnell loslegen können.

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
- 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 FW5000 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

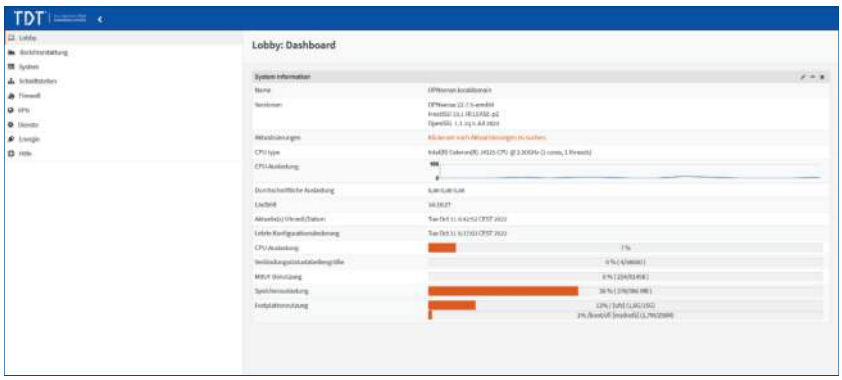
- Support Virtual Installs
  - VMware tools (Plugin)
  - Xen Guest Utilities (Plugin)
- Easy Upgrade
  - Reboot warning for base upgrades
- SSL Flavour selectable
  - OpenSSL
  - LibreSSL
- Selectable Package Mirror
- Reinstall Single Package
- Lock Package (prevents upgrade)
- Audit Feature
  - Check installed packages for known security vulnerabilities
- Plugin Support

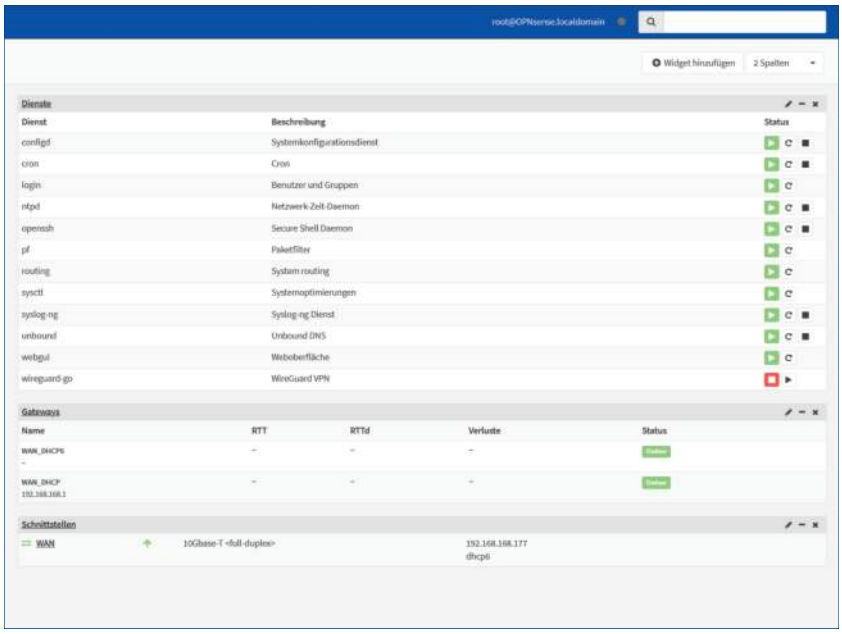
REST API

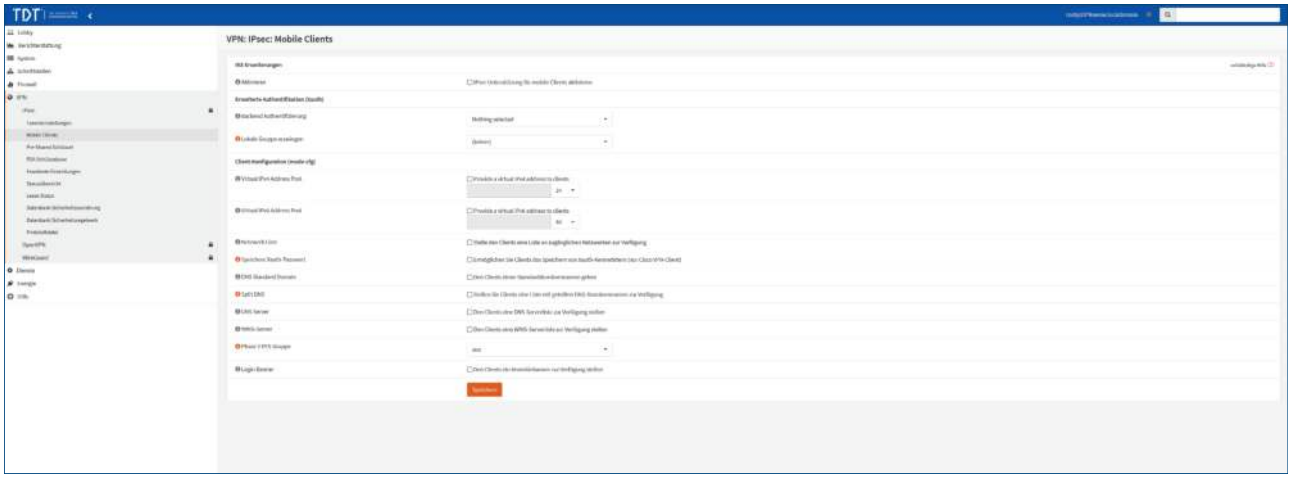
- ACL support

Online Documentation

- Free & Searchable







Hardware

Basissystem

Prozessor	Leistungsfähiger Hexa-Core Prozessor
Arbeitsspeicher	16 GB ECC DDR4 RAM
Systemspeicher	240 GB SSD (Solid State Disk)
Ethernet-Ports	8x 10/100/1000 Mbit/s
IPMI-Port	1x (dedizierte NIC, IPMI 2.0)
USB Ports	2x USB 3.1 Gen1, 2x USB 3.1 Gen2
Sonstige Anschlüsse	1x VGA
TPM2.0 (Trusted Platform Module)	Zum sicheren Speichern von geheimen Schlüsseln
Echtzeituhr (RTC)	CMOS Hardware-Uhr

Technische Daten

Robustes Metallgehäuse	19" 1HE
Abmessungen	43 mm (H), 437 mm (B), 503 mm (T)
Gewicht	Ca. 15 kg
Betriebstemperatur	20°C bis 22°C
Luftfeuchtigkeit	40% (nicht kondensierend)
Rackeinbauschienen	Enthalten, 65 - 84cm (Toolless)
Redundantes Netzteil	2x 400 Watt redundantes Hot Swap Netzteil (80plus Platinum, > 94%)
Maximale Leistungsaufnahme	≈ 112W

Garantie

Herstellergarantie	3 Jahre Bring-In Garantie

Lieferumfang

	FW5000, 2x Netzkabel, Patchkabel, abschließbare Frontblende, ausziehbare Montageschienen 65 - 84cm (Toolless), Kabelgelenkträger

Ansichten

Abb. FW5000 Vorderseite

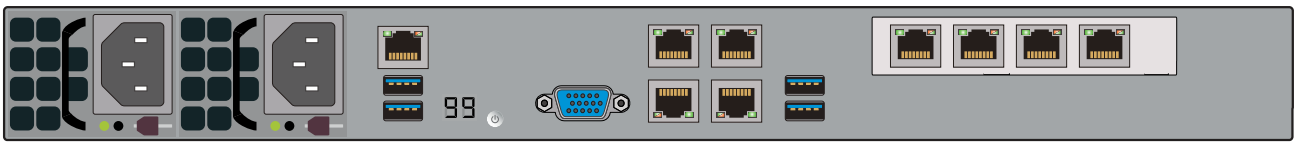


Abb. FW5000 Rückseite

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 **FW5000** der Richtlinie **2014/35/EU** entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: **download.tdt.de**

© 2023 by TDT AG