

fw300 Network Firewall - Secure your network infrastructure!

T3's FW300 Firewall provides the most advanced solution in its class, including stateful inspection firewall, Virtual Private Network (VPN), multi-wan load balancing with failover, captive portal and optional WiFi. The FW300 is designed to fulfill the demands of Small- and Medium-Businesses requiring an advanced LAN and WAN router solution that offers the highest level of protection, while allowing expansion of the network infrastructure without compromising it's security.

Load Balancing

Load balancing optimizes usages of internet resources. QoS can be setup to prioritize packets routing for VoIP and SIP applications.

Redundancy

"Seamless" Failover provides reliable and uninterrupted access to the Internet. High availability is setup through CARP Clustering.

VPN

VPN allows secure connections between branches, remote offices, or Data Centers. The Fw300 offers three options for VPN connectivity; IPsec, OpenVPN, and PPTP.

Features

Network Security

- Stateful Inspection
- Transparent layer 2
- Multiple Public Ips
- Traffic shaper
- QoS/VoIP/SIP support
- DoS and DDoS Protection
- Defense against SYN/ICMP Flood
- Anti-Spoofing

Firewall State table

- Adjustable state table size
- Per-Rule basis
- State types
- Various State Table optimization

Intrusion Prevention

- Network-Protection (Block attacks such as DoS, port scanning, IP/ICMP/TCP scanning etc)

Malware Protection (Optional)

- Anti-virus protection
- Anti-spyware blocks

Captive Portal (Optional)

- URL Redirection
- Authentication options: none, local or Radius

Load Balancing (Optional)

- Outbound and Inbound

Virtual Private Network (VPN)

- IPSec
- OpenVPN
- PPTP
- Encryption: 3DES, AES
- Authentication: preshared key, certification, local

Network Address Translation (NAT)

- Port forwarding
- 1:1 NAT
- Outbound NAT
- NAT reflection

Redundancy

- WAN failover Routing
- Static Routes
- RIP v1 and 2

Reporting and Monitoring

- RRD Graphs showing CPU Utilizations, Total Throughput, Firewall States, Individual throughput, Packets per seconds rates, WAN interface gateway, and traffic shaper queues.
- Realtime Data

Logging

- System (CPU, Memory, Services, etc)
- Firewall (Action, Time, Source, Destination, Port, Protocol)
- DHCP (IP address, MAC address, Interface)
- Portal Authentication Status
- VPN (VPN Status, IP Address, Port)
- Load Balancer information

Optional Wireless Access Point (WAP)

- Wireless N+ technology
- Remotely Managed WiFi
- Commercial Grade

The FW300 is a fully capable business class firewall at a fraction of the cost of it's nearest competitor. Nothing comes close to the performance or quality for a similar price!

Highlighted Features

Stateful Inspection Firewall

With default firewall policy, all traffic is denied, this prevents bypassing of security policy at network perimeter. The firewall also prevents unauthorized traffic, enforces security policies and resists malicious attacks.

Network Address Translation (NAT)

NAT protects and hides internal network information from the outside world.

Virtual Private Network (VPN)

VPN offers significant savings over leased connections between branches or remote offices.

Captive Portal

Captive Portal allows you to enforce authentication for secure wired or wireless internet access in public areas.

RRD Graphs

Graphs report detailed information about the state of the firewall as well as the networks it protects.

Monitor / Logging

Provides logging capacity for tracing realtime threats and malware activities as well as giving useful information for Internet traffic such as HTTP, HTTPS, SMTP, FTP, POP3, IMAP, Instant Messaging, etc.

