# MPT UTM: Comprehensive, Enterprise-Grade Network Security

A complete overview of the MPT Next-Generation Firewall platform.

**Installation, Design, Configuration, and Support proudly delivered by MPT Saudi Arabia.**

# An Innovative, User-Friendly, and Modular NGFW Platform

MPT UTM is an NGFW that combines the extensive features of commercial products with the usability and flexibility required for modern networks.

## Built on a Solid Foundation

Based on High End BSD for long-term support, with a core focus on security.

## Modular and Extendible

Through its modular design and MVC framework, the product is extendible with API functionality readily available.

## Reliable and Timely Updates

The robust update mechanism provides important security updates in a timely fashion.

A security-first mindset is built-in, with unique features like integrated one-time password authentication.

# A Unified Platform Built on Four Pillars of Excellence

**1. Core Security & Networking**

Foundational traffic control, routing, and network defence.

**2. Secure Connectivity**

Versatile and encrypted remote access for any scenario.

**3. Advanced Threat Protection**

Application-layer security for web and email.

**4. Operational Command**

Complete management, visibility, and automation.

*The MPT UTM is not just a collection of features; it is a comprehensive security platform. These four pillars work in concert to deliver a unified, enterprise-grade solution.*

# I. Core Security & Networking

Granular control over traffic flow and network architecture.

## Stateful Firewall & Routing

- Stateful Packet Inspection with Aliases (IP, GeoIP, BGP ASN)
- Time-based Rules, Port Forwarding (NAT), and Traffic Shaping
- Policy-Based Routing and Static Routing

## Advanced Network Defence

- Intrusion Detection & Prevention (Suricata)
- Anti-DDoS Protection (SYN cookies)
- GeoIP & Bogon Network Blocking **Enterprise Edition**

## Flexible Network Architecture

- Advanced VLAN support (802.1Q up to 4096, QinQ 802.1ad)
- Support for VXLAN, Bridging (RSTP), LAGG, Virtual IPs, and GIF/GRE Tunnels
- Advanced Dynamic Routing via FRR (BGP, OSPF, IS-IS, etc.) **Plugin**

# II. Secure Connectivity

Secure and high-performance VPN for site-to-site and remote access.

## Primary VPN Protocols

**OpenVPN:** SSL/TLS encryption with an easy-to-use client export feature.

**IPsec:** Robust support for secure site-to-site and remote connections.

**WireGuard:** Lightweight, high-performance protocol with easy QR code client configuration.

## Additional Tunneling Options

Support for Openconnect, Stunnel, Tinc, and ZeroTier (SD-WAN) **Plugin**

## Enhanced Security & Usability

- Multi-Factor Authentication (TOTP) for enhanced security.

- Customised Dynamic DNS integration for endpoints with dynamic IPs.

- Full support for 'Road Warrior' mobile client setups.

# III. Advanced Threat Protection

Secure your web applications, control content, and block modern threats.

## Web Application Firewall (WAF)

Protect web services against injection attacks and manage traffic encryption.

`Enterprise Edition`

## Web & Content Control

- Caching Web Proxy (Squid) with Transparent Mode `Plugin`
- URL Filtering with blacklists and categories `Plugin`
- SSL/TLS Inspection with SSL bumping capabilities `Plugin`

## Threat Prevention & Email Security

- Antivirus Integration (ClamAV) for web and email traffic `Plugin`
- DNS Filtering with DNS over TLS `Enterprise Edition`
- SMTP Proxy with Antispam (SpamAssassin) `Plugin`

## Certificate Management

Automated SSL/TLS certificate management with Let's Encrypt integration.

`Plugin` `Enterprise Edition`

# IV. Operational Command
Simplify management, gain deep insight, and ensure resilience.

## Unified Management & Access

- **Web-based dashboard** with customisable widgets.
- Full **console** access (Serial & SSH) with text-based menu.
- **Role-Based Administration** for multi-user management.

## Deep Visibility & Reporting

- Flexible **Netflow Analyser** (Insight) and NetFlow Exporter.
- **Live Traffic Monitoring** with Top Talkers overview.
- Graphical system health and performance monitoring.

## Automation & Integration

- **REST API** for automating configuration and management tasks.
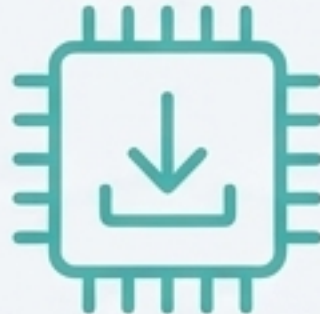- **Monit** for automated service and system resource monitoring.

## Resilience & Recovery

- Configuration **Backup/Restore** (local or cloud)
  `Plugin`
- Full system **Snapshots** for space-efficient recovery.

NotebookLM

# Operational Command: Central Management for Scaled Deployments

**All features on this slide are Enterprise Edition**

A flexible and powerful environment to manage multiple firewalls from a single pane of glass.

## Multi-Tenancy
Create isolated setups using host groups with user access controls.

## Centralised Backups
Automate configuration backups for all managed hosts.

## Remote Provisioning
Centrally push Users, Groups, Aliases, Firewall Rules, and NAT configurations.

## Fleet Firmware Control
View firmware status across all devices and trigger remote upgrades.

## Remote Service Control
Monitor and control (start/stop) services on remote hosts.

## Centralised Monitoring
View resource usage (CPU, Memory, State Table, Bandwidth) for all hosts.

## Seamless Access
Use configured trust to log in to remote host WebGUIs with a single click.

NotebookLM

# Operational Command: A Comprehensive Diagnostics & Troubleshooting Toolkit

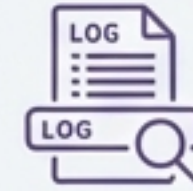Quickly identify and resolve network issues with a complete suite of built-in tools.

## Real-time Analysis

- Firewall Live View (colour-coded)
- Packet Capture (downloadable)
- System Activity (top)
- Traffic Graphs

## Connectivity & Routing Utilities

- Ping, Traceroute, DNS Lookup
- Test Port
- Routing Table Viewer
- Route Lookup Tool

## In-Depth Logging

Access comprehensive, searchable logs for all major services: System, Firewall, VPN, Unbound DNS, IDS Alerts, Proxy Server, and more.

## System Integrity

- Firmware Audit
- Configuration History
- Backup & Restore

## State & Table Inspection

- Live views of ARP/NDP Tables
- Firewall State Table (full & summary)
- DHCP/DHCPv6 Leases
- IPsec SAD/SPD

# Built for Resilience: High Availability & Load Balancing

Ensure continuous operation and optimal performance with robust failover and traffic distribution.

## Stateful Failover

- **CARP Failover**: Provides seamless hardware redundancy.
- **pfsync State Synchronisation**: Ensures active connections are maintained during failover.
- **High Availability Sync**: Automatically synchronises configuration between primary and secondary nodes.
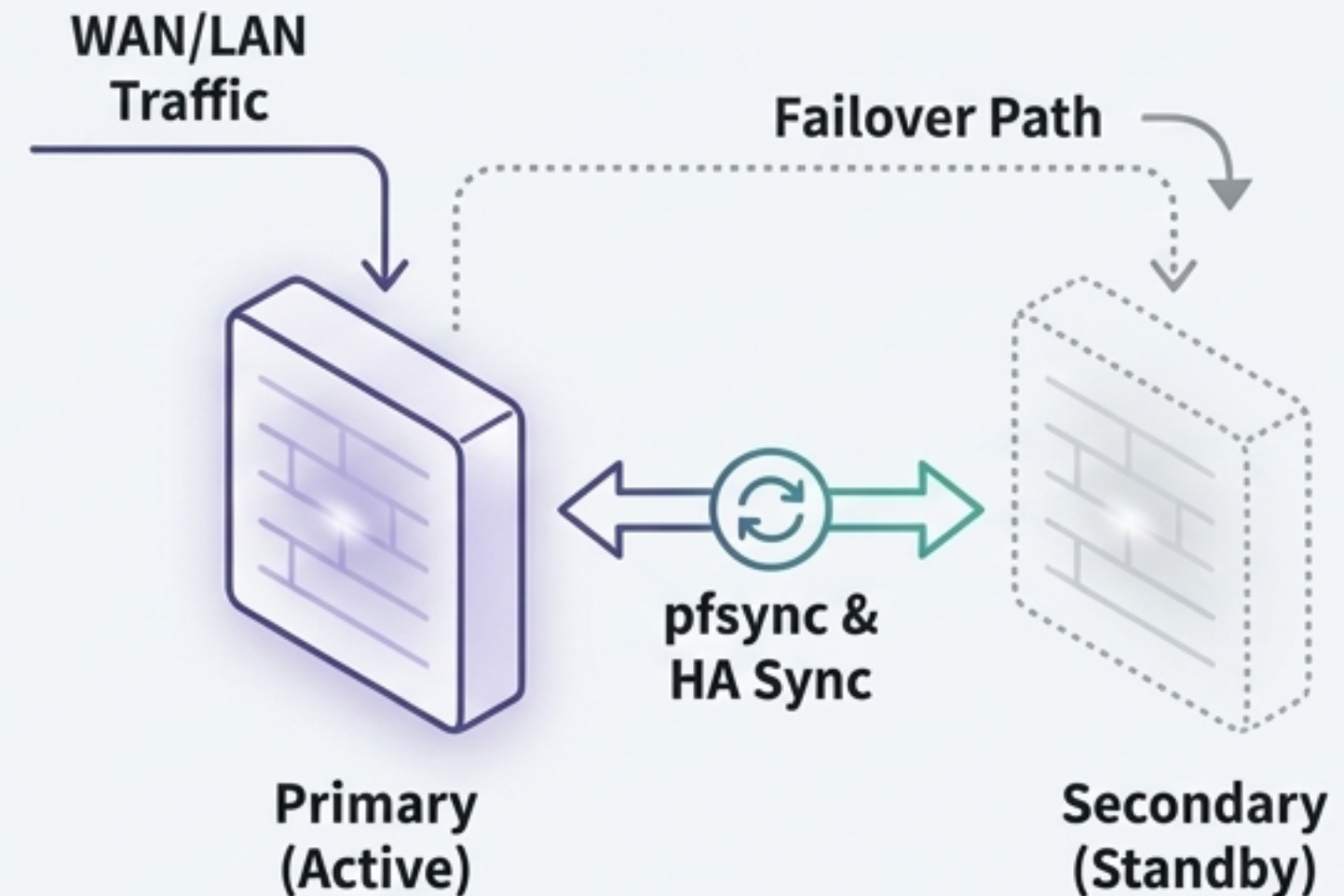
## Bandwidth Optimisation & Redundancy

- **Multi-WAN Load Balancing**: Distributes outbound traffic across multiple internet connections.
- **Link Aggregation (LAGG)**: Combines multiple interfaces for increased bandwidth and redundancy.
- **Gateway Quality Monitoring**: Proactively monitors WAN links for latency and packet loss.

## Traffic Distribution

- Inbound Load Balancing across multiple servers.
- (Options include relayd and WAF)  Business Edition

**WAN/LAN Traffic**

**Failover Path**

**pfsync & HA Sync**

**Primary (Active)**
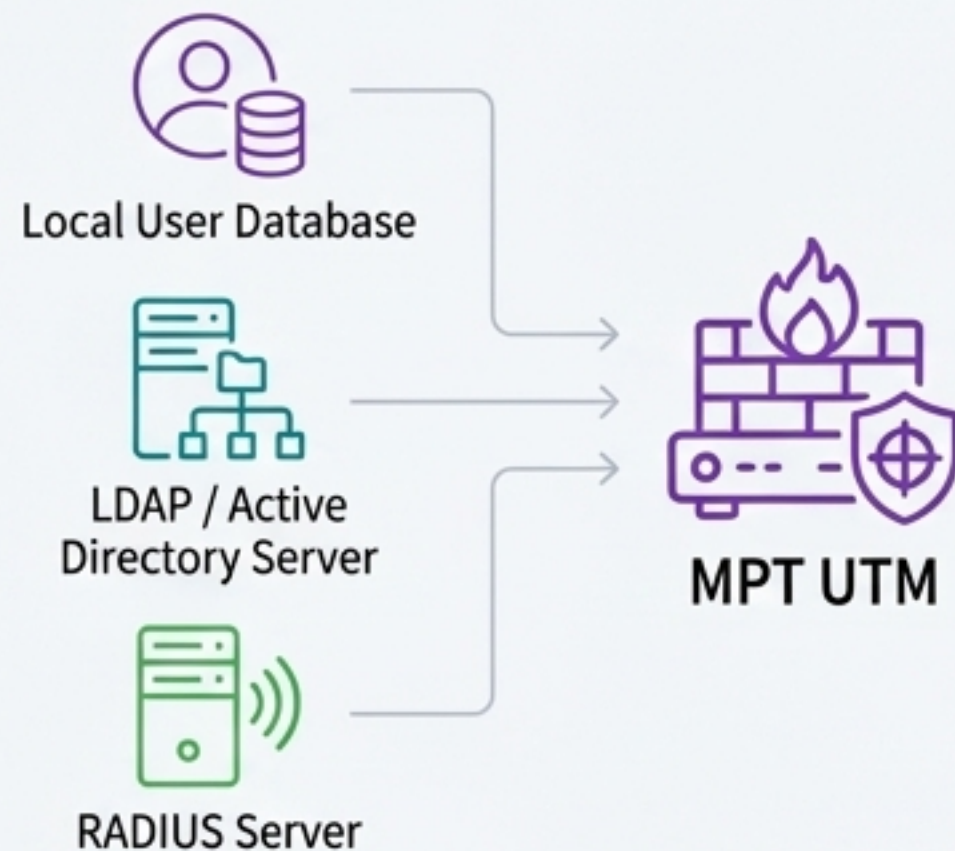
**Secondary (Standby)**

NotebookLM

# Secure & Controlled Access: Authentication & Identity Management

Integrate with existing directories and enforce granular access policies for users and devices.

## Flexible Authentication Sources

Local User Database

LDAP / Active Directory Server

RADIUS Server

MPT UTM

- Local User and Group Management.
- Integration with LDAP / Active Directory and RADIUS servers.

## Secure Access Methods

**Two-Factor Authentication (TOTP)** for administrative logins.

**Captive Portal** for user authentication before network access.

**802.1X Authentication** for wired and wireless network access control. **Plugin**

## Identity & Trust Management

- Full Certificate Management suite, including CAs and CRLs.
- Limited Single Sign-On (SSO) capabilities via directory integration.
- Comprehensive Authentication Logging for auditing and compliance.

# Deploy Anywhere: Cloud & Virtualisation Ready

MPT UTM runs seamlessly on your preferred virtualisation platform or public cloud provider.

## Broad Hypervisor Support

Runs on VMware, Hyper-V, Proxmox, and VirtualBox.

## Cloud Deployment

Ready for deployment on cloud platforms like AWS and Azure (Marketplace).

## Optimised for Virtual Environments & Simplified Provisioning

### Optimised for Virtual Environments

Includes guest utilities for deeper integration (open-vm-tools & Xen).

Plugin

### Simplified Provisioning

Available as an Open Virtual Appliance (OVA) for rapid deployment.

Business Edition

# A Complete Ecosystem: Documentation, Support, & Compliance

Empowering you with the resources and expertise needed for success.

## Support & Learning Resources

### Self-Service

Fully searchable online documentation and active online user forums.

### Professional Training

E-Book ("The complete Practical Firewall') and E-learning Hands-On Labs.

**Enterprise Edition**

### Commercial Support

Professional support for configuration and troubleshooting available.

**Enterprise Edition preferred**

### Compliance Validation

Highlight the availability of external, 3rd party LINCE compliance testing.

**Enterprise Edition**

# The MPT UTM Platform: Your Strategic Security Asset

## Comprehensive Security

An all-in-one NGFW platform, from stateful firewall and VPN to WAF and IDS/IPS, providing defence-in-depth.

## Modular & Extendible

A flexible core enhanced by a rich ecosystem of plugins and tiered editions to meet specific needs.

## Enterprise-Ready

Built for performance and reliability with high availability, scalable central management, and deep diagnostic tools.

## Unified & Manageable

An intuitive interface, powerful API, and deep visibility tools that simplify complex security operations.

# MPT Saudi Arabia: Local Expertise, Global Power

## Installation, Design, Configuration and Support is proudly delivered by MPT Saudi Arabia.