

Funkwerk UTM 1500

Funkwerk UTM 1500



Attacks and threats have become increasingly diverse over recent years. The times when firewalls and virus scanners were sufficient to build security solutions are now history. Thanks to Funkwerk UTM, however, comprehensive protection at the gateway does not need to be complex or involve numerous different systems. The new Funkwerk UTM technology is able to identify the various attacks and threats and specifically blocks them without impairing communication. Funkwerk UTM combines centralized remote administration with fine-tuned security components to boost security. It is easy to use and thereby dramatically reduces investment and running costs.

Specifications UTM 1500



25 / 50 / 75 User

	UTM 1500	UTM 1500	UTM 1500
Appliance Platform	UTM 1500	UTM 1500	UTM 1500
Model		Desktop	
Users	25	50	75
Processor		1,2 GHz	
RAM		512 MB	
Hard Disk		40 GB	
Interfaces 10/100 Mbit/s		4	

Firewall

Feature	Description
Stateful Firewall	Stateful Firewall or Stateful Inspection Firewall is an advanced security feature. The data connection is not only checked on packet filter level (source IP address, destination IP address and port) but also checks on the state of a connection to allow or to block a connection.
NAT	Network Address Translation is used to hide private IP addresses in the internal LAN behind the external official Internet IP address of the Funkwerk UTM gateway. In addition Funkwerk UTM can handle Basic NAT (also known as Static NAT) in which an internal IP can be substituted 1:1 with an external IP.
PAT	Port Address Translation is used to redirect TCP and UDP ports. Example: an external request is coming to a mail server on port 25. At the UTM gateway it can be redirected e.g. to the internal port 225.
Full Application Level Gateway	Beyond the checks of the connection state (Stateful Firewall) the Funkwerk UTM firewall has even more advanced protocol and integrity checks. The integrated application level gateway checks if the communication protocols are correctly spoken or if somebody tries to compromise a system using forbidden protocols. Application level checks are done on the following protocols: DNS, FTP, HTTP, SMTP, POP3

VPN

Feature	Description
VPN Protocols	Available VPN protocols are: IPSec, PPTP, L2TP over IPSec, SSL VPN
Unlimited dedicated tunnels	The amount of tunnels that a gateway will handle is not limited by the UTM license.
Encryption	Encryption standards that are supported are: DES, 3DES, AES, Blowfish, Twofish, Serpent
Data integrity	Supported hash algorithms for the VPN are SHA-1 and MD5
Certificate authentication	Pre-shared keys and support of X.509 certificates. Certificates can be imported or generated with the integrated certificate server.
IPSec NAT traversal	Available
Site to site VPN	Available
Client to site VPN	Available

Anti Virus

Feature	Description
Protocol scanning	Incoming and outgoing data is scanned by UTM for viruses <u>before</u> entering the LAN in real-time within the following protocols: - HTTP (surfing web pages using http) - FTP (downloading files using ftp) - SMTP (sending and receiving email using smtp) - POP3 (polling email from external mail servers using pop3)
Automatic Update	The virus signature database is updated automatically (up to hourly)

Intrusion Prevention

Feature	Description
High Quality Attack Database	The Funkwerk UTM advanced intrusion prevention engine detects and blocks a large variety of known attacks and threads inside the data stream. The advanced quality attack database contains at moment more than 6000 known attacks. This means maximum security and protection.
Auto-Prevention	Funkwerk UTM is equipped with a very unique feature called Auto-Prevention. This means that the Funkwerk UTM comes with predefined security policy levels which contain how to react automatically to the different attacks. Through the Auto-Prevention feature intrusion prevention gets usable and secure with a single click and without individual customization.
Advanced Attack Prevention	Advanced prevention and detection mechanisms against major threads and attacks like port scans, DoS (denial of service) attacks, buffer overflows, UDP attacks, application and protocol anomaly attacks, packet fragmentation attacks (= to hide attacks from regular Intrusion Prevention Systems, attacks are not send in one data packet but are split into several data packets. To prevent from attacks that are fragmented Funkwerk UTM not only looks at single packets but also reassembles complete data streams and does checks over the complete data stream)
Automatic Update	The attack signature database is updated automatically (up to hourly)
Stateful Intrusion Prevention	The Funkwerk UTM intrusion prevention also considers sessions. This maximizes the detection rate significantly.
RFC compliance checks	Communication protocols are checked for RFC compliance. This gives additional security against attacks. The following protocols are checked for their RFC compliance: http, ftp, pop3, smtp, dns, tcp, udp, rpc.

Anti Spam

Feature	Description
Black List / White List	Inside the spam detection engine the user can additionally define its own lists of either definitely wanted (White List) or definitely unwanted (Black List) mail addresses or mail domains. So regardless if the mail is classified as spam or not, the mail will be blocked (in case the sender address or domain is defined inside the Black List) or accepted (in case the sender address or domain is defined inside the White List).
Greylisting	The funkwerk UTM implements an additional method for combatting e-mail spam. This method, known as greylisting, will reject the initial e-mail from an unknown sender with a prompt to re-send the message later. Subsequent delivery attempts from the same source are then accepted immediately.
Mime Header Check	To identify spam mails the mime headers are also checked.
RBL, ORDB	For spam detection and classification UTM includes Realtime Blackhole Lists (RBL) and Open Relay Databases (ORDB) in its Spam rating. If e.g. an email is coming from a well known Spam server or an open relay server (server that was hacked and is misused from spammers) the Spam rating will go up.
<i>Optional:</i> CommTouch Spam detection engine	The spam detection engine can be optionally supplemented to the CommTouch scan engine. CommTouch is a market leader in Spam detection and well known for its very advanced scan technologies (fast) and its very good quality of detection (high detection rates with minimum false positives). More info on CommTouch and their advanced Spam detection technologies can be found at http://www.commtouch.com .
Automatic Update	The spam detection database is updated automatically in real-time
BATV	The SMTP proxy supports now Bounce Address Tag Validation. This allows you to reject bounce messages (notifications set from a mail server) that do not refer to a mail previously sent from the UTM.

Content Filter

Feature	Description
Regular expression based URL black lists und white lists	Access to specific web pages can be deliberately denied or granted.
User reliant or IP based filters	Content filters can be configured for individual users, user groups or IP addresses.
<i>Optional:</i> IBM Content Filter	Loss of productivity and legal consequences may arise if employees are given unrestricted access to web pages. With the optional Content Filter extension, funkwerk UTM provides the possibility to control web access using arbitrary combinations of over 60 content categories. Access can be granted to specific pages only, as well as applying individual criteria for distinct users throughout an organization. User management can either be performed on the funkwerk UTM itself or by accessing a remote repository, for example a Radius server or the Active Directory of a Windows Domain. More than 4.4 billion web pages and pictures are rated.

User Authentication

Feature	Description
Internal database	Funkwerk UTM allows to build up an internal user database. These users can be used for in-band, out-of-band and VPN authentication.
External Database	Funkwerk UTM can communicate with external user databases (LDAP and Radius). These users can be used for in-band, out-of-band and VPN authentication.

Out-of-band Authentication	Nearly all protocols can be authenticated using the out-of-band authentication. The user can logon at an authentication web interface with his login and password. After successful login the access will be temporarily granted to the allowed services for this user.
In-band Authentication	In-band user authentication for http using the authentication features of the protocols.
Client to site VPN	Client to site VPN can be authenticated using user and certificates.

Administration

Feature	Description
Automatic pattern update	All pattern and attack signatures are updated automatically on an e.g. hourly basis.
Automatic software update	If software updates are available the administrator will be notified and can download and install them automatically with a single click.
Web GUI	Funkwerk UTM comes with an intuitive and easy to use GUI. The management can be done from any web browser using http or https.
Console interface	Alternatively to the web based management the appliance can be administrated using a simple console cable and a standard console software.

Logging

Feature	Description
Logging to remote Syslog	Attacks, alerts, notifications and log files can be logged to an external Syslog Server.
Logging to remote SNMP	Attacks and alerts can be logged to an external SNMP Server using SNMP traps.
Logging to remote SMTP	Attacks and alerts can be sent to an email server using SMTP.
Local logging	Attacks and alerts can be logged internally on the system

More functions

Feature	Description
PPoE-Client	funkwerk UTM has a DSL functionality. The external interface can be used as PPPoE interface.
DHCP-Client	funkwerk UTM includes a DHCP client on every interface. It is therefore usable in environments where i.e. the existing internet router distributes IPs over its own DHCP server.
High Availability	Reliable Internet connectivity and perpetual access to vital data is of growing importance to businesses today. To achieve this goal, all equipment along the communication path as well as the end points have to be available at all times. As an internet gateway, funkwerk UTM is playing a critical role here. Using the High Availability feature of the funkwerk UTM, a standby system can be installed in parallel. In the unlikely case of failure or during maintenance of the main system, all tasks are transferred to the standby system until the main system is fully functional again.
Quality of Service	The Quality of Service feature allows allocating bandwidth for selected services or groups of services by specifying minimum and/or maximum bandwidths. This ensures that network applications like for instance "Voice over IP" are not affected by other applications using the same network connection. As an example, the throughput of FTP downloads can be throttled to make sure there is sufficient remaining bandwidth for speedy web surfing.

Firewall Nodes and Features

Stateful Inspection Firewall
NAT Network Address Translation
PAT Port Address Translation

Dynamic Intrusion Detection and Prevention

No. of Signatures > 6.000
Auto-Prevention
Automatic updates
Port scans
DoS
Buffer overflow
Packet fragmentation attacks
Application anomaly attacks

Anti Spam

By default integrated
Commtouch optional available
Black list / White list
Greylisting
MIME header check
RBL, ORDB
BATV

Anti Virus scanner

Scans HTTP, FTP, SMTP, POP3
Automatic Virus database update

Content filtering

URL / Black List / White List
IBM content filter optional available
More than 4.4 billion webpages

VPN

PPTP, L2TP, IPSec, SSL VPN
Unlimited VPN Tunnel
Encryption DES, 3DES, AES, Blowfish,
Twofish, Serpent
SHA-1 / MD5 Authentication
IKE certificate authentication
IPSec NAT traversal
Client to site VPN

User authentication

Internal database
External LDAP database support
External RADIUS database support
Out-of-Band authentication
In-Band-Authentication

Local Services

DNS
FTP
HTTP
SMTP
POP3
DHCP Server

System Features

Monitoring via SNMP
High Availability

Logging

Log to remote syslog server
Log to SNMP server
Log to SMTP
Local logging

Traffic Mangement

Application protocol analysis
RFC compliance checking
Stateful pattern matching
OSPF
Quality of service

Administration

Automatic real-time update
Console interface
WebGUI (HTTPS)