

funkwerk UTM 1100

funkwerk UTM 1100

Die Angriffe und Bedrohungen sind in den letzten Jahren vielfältiger geworden. Vorbei sind die Zeiten in denen Sicherheitslösungen mit Firewalls und Virens Scanner ausreichend waren.

Umfassende Absicherung am Gateway muss dank der Funkwerk UTM nicht kompliziert sein und aus vielen verschiedenen Systemen bestehen. Die neuartige UTM Technologie von Funkwerk erkennt die unterschiedlichen Angriffe und Bedrohungen und blockt diese gezielt ohne dabei die gewollte Kommunikation zu beeinträchtigen. Durch die zentrale Administration und die optimale Abstimmung der Sicherheitskomponenten steigert das Funkwerk UTM die Sicherheit, ist einfach zu handhaben und reduziert dadurch drastisch einmalige und laufende Kosten.



Spezifikation UTM 1100



10 User

Appliance Plattform	UTM 1100
Modell	Desktop
Empfohlener Einsatzbereich - Users	10
Prozessor	500 MHz lüfterlos
RAM	256 MB
Flashspeicher	512 MB
Interfaces 10/100 Mbit/s	4

Firewall

Feature	Beschreibung
Stateful Firewall	Eine Stateful Firewall oder Stateful Inspection Firewall ist ein Hauptbestandteil einer UTM Lösung. Die Datenverbindung wird dabei nicht nur auf Packetfilter Ebene geprüft (Source IP Address, Destination IP Address und Port), sondern es wird ebenfalls der Verbindungsstatus (state) geprüft, um letztendlich die Verbindung zu erlauben, oder zu blocken.
NAT	Die Network Address Translation wird zum Schutz der privaten IP Adressen im internen LAN hinter der externen, offiziellen Internet IP Adresse des UTM Gateway's eingesetzt. Zusätzlich kann das Funkwerk UTM System auch Basic NAT (auch bekannt als Static NAT), in welchem eine interne IP 1:1 durch eine externe IP ersetzt werden kann.
PAT	Die Port Address Translation wird zur Umadressierung von TCP und UDP Ports verwendet. Beispiel: Eine externe Anfrage wird an einen Mail Server auf Port 25 gestellt. Im UTM Gateway kann diese Anfrage nun beispielsweise auf den internen Port 225 umgeleitet werden.
Full Application Level Gateway	Über die Überprüfung des Verbindungsstatus hinaus (Stateful Firewall) verfügt die UTM Firewall über weitere wichtige Protokoll- und Integritätsprüfungen. Der integrierte Application Level Gateway prüft dabei die Kommunikationsprotokolle auf ihre Korrektheit und Zulässigkeit, oder ob jemand versucht mit nicht zulässigen Protokollen ein System zu kompromittieren. Application Level Prüfungen werden mit folgenden Protokollen durchgeführt: DNS, FTP, HTTP, SMTP, POP3

VPN

Feature	Beschreibung
VPN Protokolle	Verfügbare VPN Protokolle sind: IPSec, PPTP, L2TP over IPSec, SSL VPN
Anzahl an VPN Tunnels	Die Anzahl an Tunnels ist bei der Funkwerk UTM Lizenz unlimitiert.
Verschlüsselung	Folgende Verschlüsselungsstandards werden unterstützt: DES, 3DES, AES, Blowfish, Twofish, Serpent
Daten Integrität	Die unterstützten hash Algorithmen für den VPN sind: SHA-1 und MD5
Certificate Authentication	Pre-shared keys und Unterstützung von X.509 Zertifikaten. Zertifikate können im integrierten Zertifikatserver erzeugt oder importiert werden.
IPSec NAT traversal	Verfügbar
Site to site VPN	Verfügbar
Client to site VPN	Verfügbar

Anti Virus

Feature	Beschreibung
Protokoll Scanning	Ein- und ausgehende Daten werden von UTM mit folgenden Protokolle auf Virus in Echtzeit untersucht <u>bevor</u> sie das LAN erreichen: - HTTP (surfen auf Web-Seiten mittels http) - FTP (download von Dateien mittels ftp) - SMTP (senden und empfangen von eMails mittels smtp) - POP3 (Abruf von eMails von externen Mailservern mittels pop3)
Automatisches Update	Die Virus Signaturen Databasis wird automatisch aktualisiert (bis hin zu stündlich)

Intrusion Prevention

Feature	Beschreibung
High Quality Attack Database	Das UTM Intrusion Prevention System analysiert und blockt eine große Anzahl verschiedener, bekannter Angriffe und Bedrohungen im Datenstrom. Die Datenbank umfasst derzeit mehr als 6000 bekannte Angriffe. Dies steht für ein Maximum an Sicherheit und Schutz.
Auto-Prevention	Das Funkwerk UTM ist mit einer einmaligen Funktion der sogenannten Auto-Prevention ausgestattet. Dies bedeutet, dass das Funkwerk UTM mit vordefinierten Security Policy Levels ausgestattet ist, die beinhalten wie automatisiert auf die verschiedenen Angriffe reagiert werden soll. Durch die Auto-Prevention Funktion wird die Intrusion Prevention sehr leicht in ihrer Handhabung und sicher durch nur einen Click, ohne manuelle Anpassung.
Advanced Attack Prevention	Intrusion Prevention und Detection Mechanismen gegen Bedrohungen und Angriffe wie: port scans, DoS (denial of service) Angriffe, buffer overflows, UDP Angriffe, Application und Protokoll Anomalie Angriffe, Packet Fragmentation Angriffe (= um Angriffe vor Intrusion Prevention Systems zu verstecken werden die Angriffe nicht in einem Datenpaket gesendet, sondern aufgeteilt in mehrere Pakete. Um vor fragmentierten Angriffen zu schützen untersucht das Funkwerk UTM nicht nur auf einzelne Datenpakete hin, sondern reassembled und untersucht den kompletten Datenstrom).
Automatisches Update	Die Datenbank der Angriffssignaturen wird automatisch aktualisiert (bis hin zu stündlich)
Stateful Intrusion Prevention	Das Funkwerk UTM Intrusion Prevention beinhaltet ebenfalls "Sessions". Dies verbessert die Erkennungsrate extrem.
RFC compliance checks	Kommunikationsprotokolle werden auf ihre RFC compliance hin geprüft. Dies gewährt zusätzliche Sicherheit gegen Angriffe. Folgende Protokolle werden hinsichtlich ihrer RFC compliance geprüft: http, ftp, pop3, smtp, dns, tcp, udp, rpc.

Anti Spam

Feature	Beschreibung
Black List / White List	Innerhalb der Spam Detection Engine kann der Benutzer zusätzlich seine eigene Liste der gewollten (White List) und definitiv ungewollten Mail- und Domain-Adressen (Black List) anlegen. Ungeachtet ob die Nachricht als Spam klassifiziert ist oder nicht, wird sie geblockt (im Fall, die Domain ist in der Black List aufgeführt) oder akzeptiert (im Fall, die Domain ist in der White List aufgeführt).
Mime Header Check	Zur Identifikation von Spam Mails werden die "mime headers" ebenfalls geprüft.
RBL, ORDB	Zur Spam Erkennung und Klassifikation beinhaltet UTM so genannte Realtime Blackhole Lists (RBL) und Open Relay Databases (ORDB) für die Spam Bewertung. RBL beinhaltet bekannte Spam Server, Open Relay Server sind "gehackte" Server die von Spammern zum Versand missbraucht werden.
<i>Optional:</i> CommTouch Anti Spam	Die integrierte Spam Detection Engine kann optional mit dem CommTouch Anti-Spam System aufgerüstet werden. CommTouch ist einer der Marktführer in Sachen Spam Erkennung und weithin bekannt für seine innovative Scann-Technologie (schnell) und seine hohe Qualität der Erkennung (höchste Erkennungsrate bei einem Minimum an false positives). Mehr Informationen über CommTouch und ihrer innovativen Spam Erkennungstechnologie finden Sie unter http://www.commtouch.com .
Automatisches Update	Die Spam Datenbank wird automatisch in Echtzeit aktualisiert.

Content Filter

Feature	Beschreibung
Regular expression basierte URL black lists und white lists	Bestimmte Webseiten können bewusst gesperrt oder freigeschaltet werden.
Benutzerabhängige oder IP basierte Filter	Pro Benutzer, Benutzergruppe oder IP Adresse können Content Filter eingerichtet werden.
<i>Optional:</i> IBM Content Filter	Mit dem optional erhältlichen Content Filter verfügt die funkwerk UTM über eine Möglichkeit die zu erreichenden Webseiten mit Hilfe von über 60 Kategorien einzuschränken. Natürlich können für unterschiedliche Benutzer im Unternehmen unterschiedliche Einschränkungen konfiguriert werden oder man kann sie nur auf ganz bestimmte Seiten zugreifen lassen. Ob die Benutzer nun lokal auf der funkwerk UTM angelegt werden oder zum Beispiel aus dem Active Directory der Windows Domäne oder einem Radius Server ausgewählt werden, ist frei konfigurierbar. Es werden über 4,4 Milliarden Seiten berücksichtigt.

User Authentication

Feature	Beschreibung
Internal database	Funkwerk UTM erlaubt den Aufbau einer internen User Datenbank. Diese Datenbank wird sowohl für die In-band-, als auch für die Out-of-band- und VPN Authentication verwendet.
External Database	Das Funkwerk UTM kann mit externen Datenbanken via LDAP und RADIUS kommunizieren. Die Datenbank kann sowohl für die In-band-, die Out-of-band- und die VPN Authentication verwendet werden.
Out-of-band Authentication	Fast alle Protokolle können durch die Nutzung der Out-of-Band Authentication authentifiziert werden. Der User kann sich auf einem Authentication Web Interface mit seinem Login und Passwort anmelden. Nach erfolgreichem Login wird der Zugang temporär für die erlaubten Dienste freigegeben.
In-band Authentication	In-band User Authentication für http bei Nutzung der Authentication Merkmale der Protokolle.
Client to site VPN	Client to site VPN kann bei Nutzung der User und Zertifikate autorisiert werden.

Administration

Feature	Beschreibung
Automatic pattern update	Patterns und Angriffssignaturen werden automatisch auf z.B. stündlicher Basis aktualisiert.
Automatic software update	Sind Software Updates verfügbar, wird den Administrator informiert und kann die Updates mit nur einem Klick automatisch installieren.
Web GUI	Funkwerk UTM verfügt über eine intuitive und einfach zu handhabende GUI. Das Management erfolgt über einen beliebigen Web Browser mittels http oder https.
Console interface	Alternativ zum Web basierenden Management kann die Appliance mittels eines mitgelieferten Konsolenkabels und einer standardisierten Konsolensoftware administriert werden.

Logging

Feature	Beschreibung
Logging to remote Syslog	Angriffe, Alarme, Meldungen und Logfiles können durch einen Syslog Server erfasst werden.
Logging to remote SNMP	Angriffe und Alarme können durch einen externen SNMP Server, mittels SNMP traps erfasst werden.
Logging to remote SMTP	Angriffe und Alarme können mittel SMTP an einen eMail Server gesendet werden.
Local logging	Angriffe und Alarme können auf dem System, intern erfasst werden.

Weitere Funktionen

Feature	Beschreibung
PPoE-Client	Das funkwerk UTM ist selbstverständlich auch DSL-fähig. Das externe Interface kann als PPoE-Interface betrieben werden.
DHCP-Client	Das funkwerk UTM 1100 verfügt über DHCP Clients auf allen Ethernet-Interfaces. Es kann dadurch auch in Umgebungen eingesetzt werden, bei der die IP-Adresse durch einen vorhandenen Internet-Gateway per DHCP zugewiesen wird.
High Availability	Mit Hilfe des High Availability Feature der funkwerk UTM wird ein zweites System parallel geschaltet, welches im seltenen Falle eines Ausfalls des Hauptsystems sofort dessen sämtlichen Aufgaben übernimmt und das so lange, bis das Hauptsystem wieder voll funktionsfähig ist.
Quality of Service	Mit dem Quality of Service Features können einzelnen Diensten oder Gruppen von Diensten eine minimale Bandbreite oder ein Bandbreiten Limit zugewiesen werden. Dadurch wird gewährleistet, dass netzwerkbasierende Anwendungen, wie z.B. „Voice over IP“ unbeeinflusst von anderen Anwendungen im Netzwerk kommunizieren können. Der Durchsatz von Downloads via ftp kann beispielsweise eingeschränkt werden, um genügend Bandbreite für ein flüssiges Surfen im Web zu ermöglichen.

Firewall Features

Stateful Inspection Firewall
NAT Network Address Translation
PAT Port Address Translation

Dynamic Intrusion Detection und Prevention

Anzahl an Signaturen > 6.000
Auto-Prevention
Automatische Updates
Port scans
DoS
Buffer overflow
Packet fragmentation attacks
Application anomaly attacks

Anti Spam

Im Lieferumfang enthalten
Optional erhältlich Commtouch
Black list / White list
MIME header check
RBL, ORDB

Anti Virus scanner

Scans HTTP, FTP, SMTP, POP3
Automatisches Update der Virus Datenbank

Content filtering

URL / Black List / White List
Optional erhältlich IBM Content Filter
über 4,4 Milliarden Seiten

VPN

PPTP, L2TP, IPSec, SSL VPN
Unlimitierte Anzahl an VPN Tunnels
Encryption DES, 3DES, AES, Blowfish,
Twofish, Serpant
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 Management

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

Administration

Automatic real-time update
Console interface
WebGUI (HTTPS)