

Funkwerk UTM

Funkwerk UTM (Gestion unifiée des menaces)





Les attaques et les menaces sur le réseau se sont, ces dernières années, de plus en plus diversifiées. Le temps où les pare-feux et les systèmes de détection de virus étaient suffisants pour mettre en place des solutions de sécurité est désormais révolu. La nouvelle gamme Funkwerk UTM garantit, sur un seul dispositif, une gestion "tout en un" des diverses fonctions de sécurité. La technologie Funkwerk UTM est capable d'identifier et de bloquer les différentes attaques et menaces sans altérer la communication.



Cette appliance simple d'utilisation, allie une administration centrale à distance avec des composantes réglables avec précision pour définir et augmenter ces mécanismes de sécurité. Les UTM Funkwerk stoppent toutes tentatives d'intrusion indésirables et assurent également les fonctions de filtrage de contenu, d'antivirus, d'antispam et de détection d'intrusions. Cette nouvelle gamme de produits de sécurité Funkwerk fournit une surveillance efficace des différents types de communication réseau et réduit, ainsi, vos coûts d'investissements et de maintenance.

Spécifications UTM

Plate-forme de l'Appliance

				
Plate-forme de l'Appliance	UTM 1100*	UTM 1500	UTM 2100	UTM 2500*
Modèle			Poss. rack	Poss. rack
Utilisateur	10	25 50 75	100 150 200	250 illimité
Processeur	400 MHz	1,2 GHz	2,8 GHz	2,8 GHz
RAM	256	512 MB	512 MB	1 GB
Disque dur / Flash	256 MB	40 GB	40 GB	40 GB
Interfaces 10/100 Mbit/s	4	4	6	-
Interfaces 10/100/1000 Mbit/s	-	-	-	6

*Disponibilité des modèles UTM 1100 et 2500 : Q2/2007. Leurs caractéristiques peuvent être soumises à modification.

Firewall

Caractéristiques	Description
Stateful Firewall	Stateful Firewall ou Stateful Inspection Firewall est un dispositif de sécurité avancé. La connexion n'est pas seulement vérifiée sur le niveau « filtrage de paquet » (adresse IP source, adresse IP de destination et port) mais cette connexion est aussi vérifiée sur son état pour la bloquer ou l'autoriser.
NAT	Network Address Translation est utilisé pour cacher les adresses IP privées du LAN interne derrière une adresse IP externe Internet de la passerelle Funkwerk UTM. Le NAT Statique est également géré : l'ensemble des adresses internes est traduit dans un ensemble de même taille d'adresses externes.
PAT	Port Address Translation est utilisé pour rediriger les ports TCP et UDP. Exemple : Une requête externe arrive sur un serveur de messagerie sur le port 25. Sur la passerelle UTM, elle peut, par exemple, être redirigée sur le port interne 225.
Full Application Level Gateway	Au delà des vérifications de l'état de la connexion (Stateful Firewall), le Firewall UTM de Funkwerk contrôle l'intégrité des données et les protocoles. L'Application Level Gateway intégrée vérifie si les protocoles de communication sont corrects ou si quelqu'un essaie de compromettre un système en utilisant des protocoles interdits. Les contrôles sont effectués sur les protocoles suivants : DNS, FTP, HTTP, SMTP, POP3.

VPN

Caractéristiques	Description
Protocole VPN	Protocoles disponibles : IPSec, PPTP, L2TP sur IPSec.
Tunnels illimités	Pas d'achat de licence UTM.
Chiffrement	Chiffrements standards supportés : DES, 3DES, AES, Blowfish, Twofish, Serpent, Cast.
Intégrité des données	Algorithmes de contrôle supportés pour VPN : SHA-1 et MD5.
Authentification/Certificat	Clés pré-partagées et support de certificats X.509. Les certificats peuvent être importés ou générés à partir du serveur de certificats intégré.
IPSec NAT traversal	Disponible
Site vers site VPN	Disponible
Client vers site VPN	Disponible

Antivirus

Caractéristiques	Description
Examen des protocoles	Les données en entrée/sortie sont scannées, en tant réel, par l'UTM <u>avant</u> d'infiltrer le LAN, grâce aux protocoles suivants, afin de détecter et prévenir les intrusions : <ul style="list-style-type: none"> - HTTP (accès aux pages web via http), - FTP (téléchargement des fichiers via ftp), - SMTP (émission et réception de courriers électroniques via smtp), - POP3 (récupération de courriers électroniques sur un serveur de messagerie via pop3).
Mise à jour automatique	La base de données de signatures est mise à jour automatiquement (toutes les heures).
<i>Option :</i> Moteur Kaspersky	Le moteur de recherche de virus peut être amélioré en option par le moteur de recherche de Kaspersky. Kaspersky est leader sur le marché de la détection de virus et bien connu pour ses technologies de recherche de virus avancée (rapide) et sa très bonne qualité de signatures de virus (taux élevé de détection). Pour plus d'informations, consultez le site http://www.kaspersky.com .

Prévention d'intrusion

Caractéristiques	Description
Base de données des attaques de haute qualité	Le moteur de prévention d'intrusion UTM de Funkwerk détecte et bloque de nombreuses attaques et menaces. La base de données des attaques contient pour le moment plus de 6000 attaques connues, ce qui garantit une protection de réseau sécurisée.
Auto-Prévention	L'UTM de Funkwerk est équipé d'une fonction unique, l'Auto-Prévention. Elle lui permet, grâce aux divers niveaux de sécurité prédéfinis, de savoir comment réagir automatiquement face aux différentes attaques. Grâce à cette fonction, la prévention d'intrusion s'utilise, de manière sécurisée, par simple click sans adaptation personnalisée.
Prévention d'attaques avancées	L'UTM de Funkwerk comprend les mécanismes de prévention et de détection avancées contre les attaques et les menaces, comme les examens de ports, les attaques DoS (Denial of Service), les débordements de mémoire tampon, les attaques UDP, les attaques de type Packet Fragment (= pour cacher les attaques des Systèmes de Prévention d'Intrusion standard, les attaques ne sont pas émises dans un seul paquet mais réparties dans plusieurs). Afin de prévenir les attaques fragmentées, l'UTM de Funkwerk examine les paquets simples, mais aussi, ré-assemble complètement les flux de données et vérifie leur conformité.
Mise à jour automatique	La base de données de signatures est mise à jour automatiquement (toutes les heures).
Prévention d'intrusion Stateful	La prévention d'intrusion UTM de Funkwerk prend, également, en considération les sessions. Le taux de détection est ainsi maximisé de manière significative.
RFC	Les protocoles de communication sont conformes RFC, garantissant ainsi une haute sécurité. Protocoles concernés : http, ftp, pop3, smtp, dns, tcp, udp, rpc.

Antispam

Caractéristiques	Description
Liste noire / Liste blanche	Dans le moteur de détection antispam, l'utilisateur peut définir les listes d'adresses ou de domaines de messagerie qu'il souhaite (Liste blanche) ou qu'il rejette (Liste noire). Ainsi, sans savoir si le message est classé « spam » ou non, il sera bloqué (si l'adresse ou le domaine est défini dans la Liste noire) ou accepté (si l'adresse ou le domaine est défini dans la Liste blanche).
Vérification en-tête Mime	Pour identifier les messages « spam », les en-têtes mime sont également vérifiées.
RBL, ORDB	Pour la détection et la classification des « spams », l'UTM inclut les listes Realtime Blackhole Lists (RBL) et les bases Open Relay Databases (ORDB). Si, par exemple, un message arrive d'un serveur « spam » connu ou d'un serveur relai (serveur craqué et utilisé abusivement par des spammers) le pourcentage de « spam » va augmenter.
<i>Option :</i> Moteur de détection de « spams » CommTouch	Le moteur de détection de « spam » peut être complété par le moteur de détection de CommTouch. CommTouch est leader sur le marché de la détection de « spam » et bien connu pour ses technologies de recherche de « spam » avancée (rapide) et sa très bonne qualité de détection (taux de détection élevé de « faux positif ». Pour plus d'informations, consultez le site http://www.commtouch.com .
Mise à jour automatique	La base de données de détection de « spam » est mise à jour automatiquement en temps réel.

Authentification

Caractéristique	Description
Base de données interne	L'UTM de Funkwerk permet de construire une base de données utilisateurs interne. Ces utilisateurs peuvent être utilisés pour une authentification VPN, In-band, et Out-of-band.
Base de données externe	L'UTM de Funkwerk peut entrer en communication avec des bases de données utilisateurs externes (LDAP et Radius). Ces utilisateurs peuvent être utilisés pour une authentification VPN, In-band, et Out-of-band.
Authentification Out-of-band	Presque tous les protocoles peuvent être authentifiés en utilisant l'authentification Out-of-band. L'utilisateur peut ouvrir une session sur l'interface web avec son login et son mot de passe. Une fois la connexion établie, l'accès est temporairement accordé à l'utilisateur, en fonction des services qui lui sont autorisés.
Authentification In-band	Authentification utilisateur In-band pour http utilisant les caractéristiques d'authentification des protocoles.
Client pour site VPN	Le client pour le site VPN peut être authentifié en utilisant l'utilisateur et les certificats.





Administration

Caractéristiques	Description
Mise à jour automatique des modèles	Toutes les signatures d'attaques et de modèles sont mises à jour automatiquement (toutes les heures).
Mise à jour automatique du logiciel	Si les mises à jour du logiciel sont disponibles, l'administrateur est prévenu et peut les télécharger, puis les installer par simple clic.
Interface graphique Web	L'UTM de Funkwerk est livré avec une interface graphique (GUI) conviviale. La gestion peut être effectuée à partir de n'importe quel navigateur utilisant http ou https.
Interface Console	L'appliance est administrable via un simple câble console et un logiciel console standard.

Logging

Caractéristiques	Description
Logging pour Syslog distant	Attaques, alertes, notes et fichiers log peuvent être stockés sur un serveur Syslog externe.
Logging pour SNMP distant	Attaques et alertes peuvent être stockés sur un serveur SNMP externe utilisant SNMP traps.
Logging pour SMTP distant	Attaques et alertes peuvent être envoyées sur un serveur de messagerie utilisant SMTP.
Logging local	Attaques et alertes peuvent être stockés en interne sur le serveur.

Plate-forme de l'Appliance

				
Plate-forme de l'Appliance	UTM 1100*	UTM 1500	UTM 2100	UTM 2500*
Modèle			Poss. Rack	Poss. rack
Utilisateurs	10	25 50 75	100 150 200	250 illimité
Processeur	400 MHz	1,2 GHz	2,8 GHz	2,8 GHz
RAM	256	512 MB	512 MB	1 GB
Disque dur / Flash	256 MB	40 GB	40 GB	40 GB
Interfaces 10/100 Mbit/s	4	4	6	-
Interfaces 10/100/1000 Mbit/s	-	-	-	6

Performance du système		Jusqu'à	Jusqu'à	
Débit du Firewall (Mbps)	*	600	1900	*
Débit du Firewall + IDS (Mbps)	*	180	540	*
Débit du VPN (Mbps)	*	80	210	*
Débit du Proxy (Mbps)	*	130	450	*
Débit du Proxy + AV (Mbps)	*	40	100	*
Sessions simultanées	*	100.000	500.000	*

*Disponibilité des modèles UTM 1100 et 2500 : Q2/2007. Leurs caractéristiques peuvent être soumises à modification.

Firewall et caractéristiques

Stateful Inspection Firewall
Translation d'adresse réseau NAT
Translation d'adresse port PAT

Détection et prévention dynamique d'intrusion

Nb de signatures > 6000
Auto-Prévention
Mises à jour automatiques
Examen de port
DoS
Débordement de mémoire tampon
Fragmentation des paquets
Détection d'anomalie basée sur une application

Antispam

Intégré par défaut
Disponibilité Commtouch en option
Liste noire / Liste blanche
Vérification en-tête MIME
RBL, ORDB

Antivirus

Intégré par défaut
Disponibilité Kaspersky en option
Examen HTTP, FTP, SMTP, POP3
Mise à jour automatique de la base

Filtrage URL

URL / Liste noire / Liste blanche
URL / Filtrage avancé (Q3 2007)

VPN

PPTP, L2TP, IPSec
Nb de tunnels VPN illimité
Chiffrement DES, 3DES, AES, Blowfish, Twofish, Serpant, Cast
Authentification SHA-1 / MD5
Certificat d'authentification IKE
NAT traversal IPSec
Client pour site VPN

Authentification utilisateur

Base de données interne
Support de la base externe LDAP
Support de la base externe RADIUS
Authentification Out-of-Band
Authentification In-Band

Services

DNS
FTP
HTTP

Gestion du système

Surveillance via SNMP

Logging

Log pour serveur distant syslog
Log pour serveur SNMP
Log pour SMTP
Logging local

Gestion de trafic

Application analyse de protocole
Vérification conformité RFC
Modèles Stateful

Administration

Mise à jour automatique en temps réel
Interface console
WebGUI (HTTPS)