

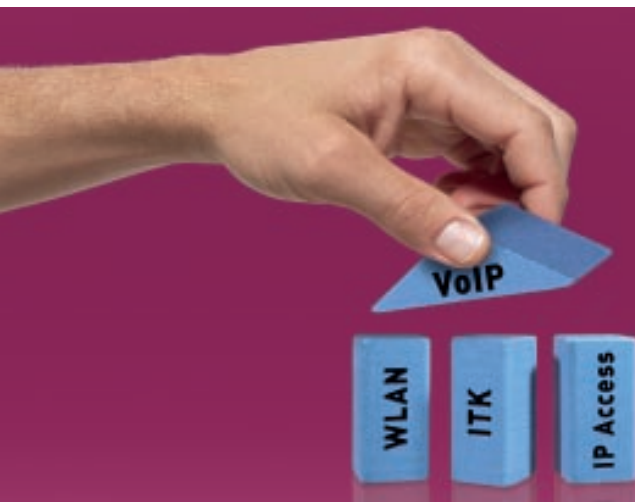


Simplicité et Sécurité pour des produits “tout en un”!

La protection de votre réseau passe par
les UTM : Gestion Unifiée des Menaces.

Systèmes funkwerk UTM





Flexibilité et Pérennité.

Funkwerk Enterprise Communications : Un seul fournisseur pour toutes vos solutions Voix-Données.

Funkwerk Enterprise Communications propose plusieurs gammes de produits pour les communications d'entreprise :

- ▶ des solutions réseaux IP via VPN, VoIP, VoVPN
- ▶ des solutions LAN sans fil (Wi-Fi, VoWIFI)
- ▶ des solutions PBX/Voix, VoIP et ToIP
- ▶ des solutions PTI (Protection du Travailleur Isolé)

Ces solutions utilisent les dernières technologies télécoms pour proposer des produits performants, flexibles et pérennes. Cette vaste palette de solutions permet à des PME/PMI, grands comptes, pouvoirs publics et opérateurs de connecter les entités distantes via VPN, d'intégrer les travailleurs externes, les bureaux délocalisés, les filiales et d'utiliser des liens sécurisés à haut débit ou des infrastructures LAN sans fil.

La sécurité de votre réseau reste la priorité. C'est dans cette optique que Funkwerk Enterprise Communications propose des technologies innovatrices de sécurité et de chiffrement, comme les systèmes IPS, IDS et UTM pour la protection de vos données en entreprise.

Réseaux Corporate : Une cible favorite pour les attaques

De nos jours, la plupart des tâches dans le milieu de l'entreprise ou de l'industrie sont gérées par des systèmes électroniques qui traitent les données. De ce fait, la disponibilité de l'infrastructure IT est indispensable, indépendamment du fait qu'il s'agisse de communication via messagerie ou de systèmes ETP. Un fonctionnement sans panne est un gage important de réussite.

Les attaques et les menaces sur les réseaux se sont, ces dernières années, diversifiées : vers, virus, chevaux de Troie, attaques DoS, spam d'e-mails, ou autres attaques dues à des pirates cherchant à exploiter les moindres failles pour dérober des informations sensibles. Aujourd'hui, les attaques qui réussissent, font des ravages s'élevant à des millions de dollars, diminuent la productivité, et violent des secrets d'entreprises, mettant en péril la vie de ces dernières.

Des risques de plus en plus intelligents et sophistiqués menacent votre réseau. Ne pas prendre de contre-mesures est négligent et risqué pour votre société. Ces dernières années, les attaques sur les réseaux corporate sont devenues plus nombreuses, plus variées et plus complexes. Le temps où les firewalls et détecteurs de virus étaient suffisants pour garantir une protection étendue est révolu. Il devient important de se protéger, quotidiennement, contre ces dangers multiformes afin d'éviter le piratage des ressources de l'entreprise.

La nouvelle gamme UTM de Funkwerk Enterprise Communications offre une protection intelligente de votre réseau, en temps réel, réduisant ainsi les risques décrits précédemment. Les systèmes UTM garantissent un RoI (Retour sur Investissement) rapide, dû à la diminution des coûts d'exploitation.

Les systèmes innovateurs funkwerk UTM sont capables de protéger votre réseau en identifiant et bloquant les différentes attaques et menaces sans altérer la communication. Une administration centralisée, une configuration optimale des composants de sécurité, ainsi qu'une gestion simple conduisent à une réduction drastique des coûts d'investissements et de fonctionnement.

funkwerk UTM : Protection de votre Réseau.

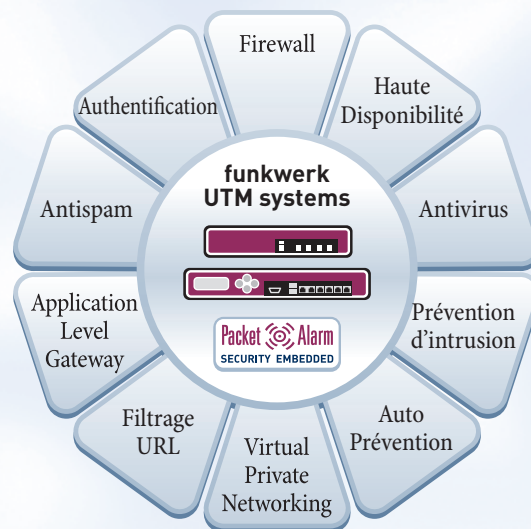


funkwerk UTM - Un système "tout en un"

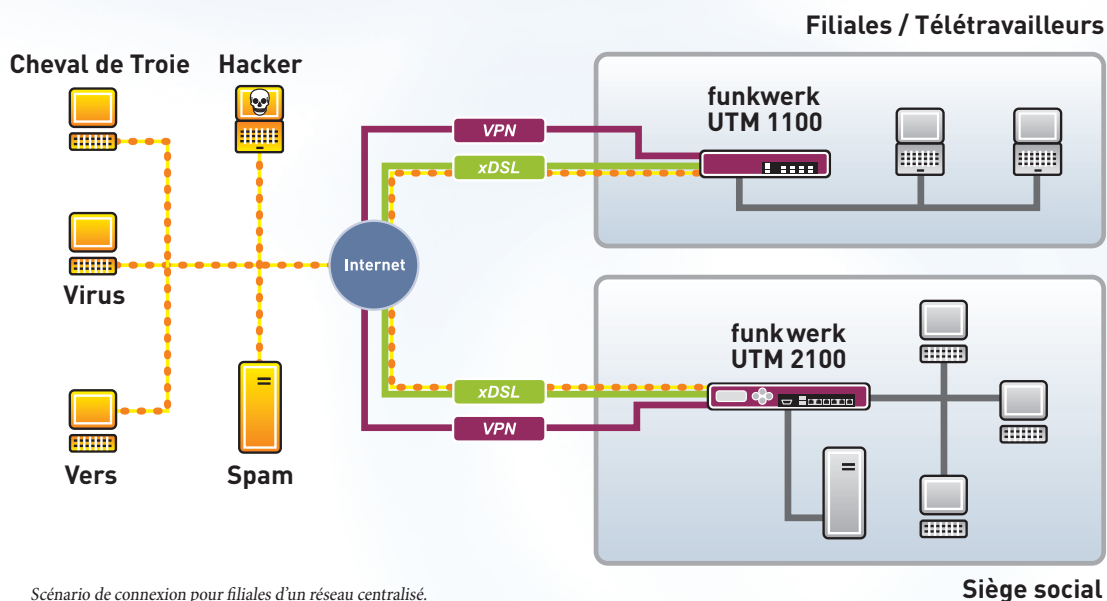
Les appliances funkwerk UTM (Unified Threat Management) combinent diverses fonctions de sécurité et assurent la protection du réseau en totalité, dans un dispositif "tout en un". Ces solutions répondent aux besoins de toutes les entreprises et fonctionnent grâce à une haute flexibilité des divers éléments de sécurité.

En règle générale, les systèmes UTM sont utilisés pour les passerelles Internet. Ils contrôlent le trafic des données entrantes et sortantes, en temps réel. Grâce à différents composants, réglés de manière optimale, les systèmes UTM détectent et contrent les virus, vers, chevaux de Troie, spam d'e-mail, violations des règles, attaques DoS et autres tentatives de piratage.

Cette gamme funkwerk UTM assure une protection complète pour la sécurité du réseau. Il n'est plus nécessaire d'installer un firewall additionnel, un système de protection antivirus, ou un filtre antispam. Cette solution réduit les coûts d'investissement et de maintenance.



De nombreuses options de sécurité dans un système "tout en un" : funkwerk UTM.



Scénario de connexion pour filiales d'un réseau centralisé.

Fonctions passerelles et Prévention d'intrusion

Firewall Multi Inspection et Application Level Gateway

Premier point de contrôle pour tout trafic de données

Le Firewall Multi Inspection des systèmes funkwerk UTM est le premier point de contrôle pour tout trafic de données. De la même manière qu'un portier, le firewall permet seulement de laisser passer les données que vous souhaitez réellement. Les règles du firewall peuvent être configurées facilement, comme toutes les autres fonctions des produits UTM. Le firewall est opérationnel quasiment en temps réel et peut ainsi assurer ses fonctions de surveillance. S'il y a lieu, des utilisateurs peuvent également être authentifiés au moyen de mots de passe locaux, via RADIUS ou LDAP, ou par authentification in-band et out-of-band.

Passerelle VPN

Connexions sécurisées pour données confidentielles

L'intégrité, l'authenticité, la confidentialité et la disponibilité des données doivent être, à tout prix, sauvegardées. Pour ce faire, il est judicieux de travailler via un VPN (Virtual Private Networking). Les appliances funkwerk UTM supportent les protocoles PPTP, IPsec, et L2TP. Les chiffrements DES, 3DES, AES, Blowfish, Twofish, Serpent, et Cast sont utilisés comme algorithmes de cryptage.

Le Firewall Multi Inspection, le détecteur de virus et de spam, ainsi que le système de Prévention d'intrusion peuvent être utilisés dans chaque tunnel. Les certificats peuvent être mis en place à des fins d'authentification.

Prévention d'intrusion

Identification d'attaques avant infiltration du réseau

Le système de Prévention d'intrusion utilise des milliers de règles et signatures afin d'identifier les attaques. Il intervient activement dans les attaques du trafic de données et les bloque avant que le réseau soit infiltré. Une fonction particulière d'Auto-Prévention simplifie la configuration et permet de ce fait que les règles et groupes de règles s'adaptent rapidement à la sécurité en fonction des différents besoins de protection.

Seuls les produits funkwerk UTM possèdent cette fonction d'Auto-Prévention, et cette mise à jour automatique de règles signifie que ces systèmes vont être protégés contre des attaques plus rapidement que d'autres systèmes.

Analyse et filtrage des données : Protection active

Filtrage d'URL

La confiance, c'est bien, le contrôle, c'est mieux.

Si les employés ont un accès libre à tous les sites Internet et qu'ils abusent de cette liberté, les effets risquent d'avoir des conséquences néfastes sur la productivité. Cependant, bien plus inquiétantes sont les violations légales potentielles pour lesquelles l'entreprise peut être tenue pour responsable.

Ce filtrage optionnel permet aux systèmes funkwerk UTM de restreindre de manière flexible l'accès aux sites Web et les services sur le LAN grâce à 60 catégories de filtres paramétrables. Les filtres et restrictions peuvent être librement programmés pour différents utilisateurs et groupes. Une liste positive, bloquant tous les accès en dehors des adresses et services identifiés, est également possible.

Tous les utilisateurs peuvent être configurés dans le système funkwerk UTM, mais peuvent également être sélectionnés à partir d'Active Directory de Windows ou d'un serveur Radius, par exemple. La gestion des utilisateurs s'adapte donc pour répondre de manière optimale à l'exigence de chacun.

Détecteur de virus

Recherche, analyse et détection de logiciels malveillants

La sécurité des réseaux est de plus en plus menacée par des virus dangereux. Les nouveaux virus se propagent avec une rapidité croissante et de plus en plus fréquemment. Les coûts et dommages provoqués au sein des entreprises, par ces virus, augmentent de jour en jour, jusqu'à mettre en péril la vie des entreprises.

La gamme funkwerk UTM filtre les fichiers infectés en provenance d'HTTP, FTP, SMTP, et POP3 et évite ainsi que les systèmes ciblés soient contaminés.



*Les virus et chevaux de Troie sont extrêmement ennuyeux
- des centaines de millions de spams sont envoyés par des ordinateurs contrôlés à distance.
Dans le pire des cas, le possesseur du micro-ordinateur peut même être tenu pour responsable.*

Filtres additionnels optionnels développés par des spécialistes

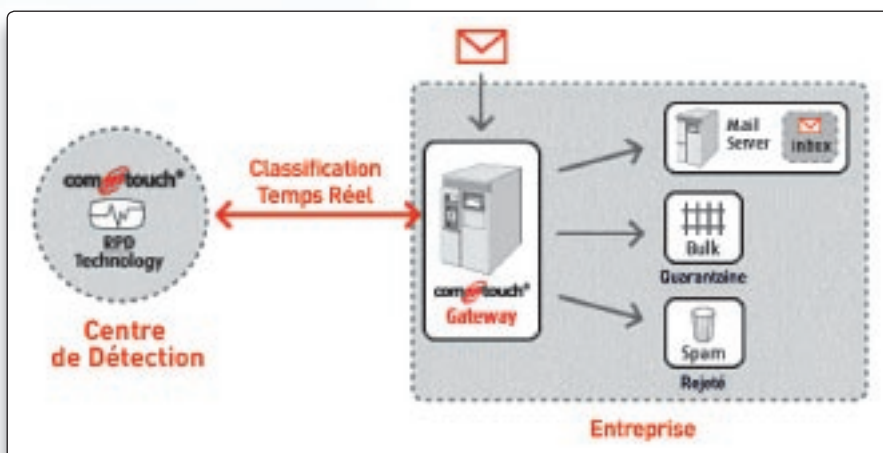
Kaspersky

Rien ne vaut un professionnel, hautement qualifié. C'est pour cette raison que Funkwerk propose une protection antivirus via le détecteur de virus Kaspersky, dont la renommée n'est plus à défendre. Ainsi, les systèmes funkwerk UTM offrent un niveau optimal de sécurité.



Filtres antispam

80 à 95% des courriers électroniques sont considérés comme des «spams». De nos jours, un filtre professionnel ne doit pas être simplement basé sur le contenu URL ou les méthodes heuristiques. Les filtres antispam intégrés dans les produits funkwerk UTM peuvent être complétés par une solution antispam, leader sur le marché, réputée pour sa vitesse de détection de « spams ». Ainsi, la sécurité est maximale.



Haute disponibilité et ergonomie

Setup Wizard

Configuration simple et transparente

Les appliances Unified Threat Management sont conçues avec de nombreux systèmes de sécurité et offrent une solution « tout en un ». Grâce au Wizard d'installation, ces produits funkwerk UTM peuvent être mis en place rapidement et tout système peut être synchronisé avec le reste des produits à la perfection. Son interface utilisateur intuitive facilite la configuration ainsi que l'administration.

Qualité de Service

Des opérations tout en douceur et réfléchies

Les services utilisés sur le réseau et via Internet requièrent différents traitements pour lesquels des autorisations individuelles (priorités) peuvent être nécessaires dès que la bande passante maximale est utilisée ou si des services différents doivent être utilisés en même temps. Pour un transfert de données via FTP, une brève interruption lors de la transmission ne pose pas de problème, alors qu'une conversation par téléphonie sur Internet (VoIP) ne doit en aucun cas être interrompue ou retardée.

Grâce à la Qualité de Service des systèmes funkwerk UTM, une bande passante maximale ou minimale peut être attribuée à des services individuels ou à des groupes de services. Ainsi, les applications en continu ou en temps réel, comme la téléphonie sur Internet, ne peuvent être perturbées par d'autres applications sur le réseau. L'installation et le paramétrage individuel de tous les services permettent une adaptation souple en fonction des besoins de l'utilisateur et une utilisation optimale des bandes passantes disponibles.

Haute Disponibilité

Disponibilité optimale grâce à la redondance

Avec la centralisation toujours croissante des systèmes de gestion de données et le besoin d'accès flexibles, également à partir de l'extérieur, la disponibilité permanente via Internet et la possibilité d'accéder en permanence aux données souhaitées sont de plus en plus importantes pour de nombreuses entreprises.

Grâce à ses mécanismes de sécurité avancés et ses redondances, les systèmes funkwerk UTM offrent une passerelle qui fournit une disponibilité optimale du réseau.

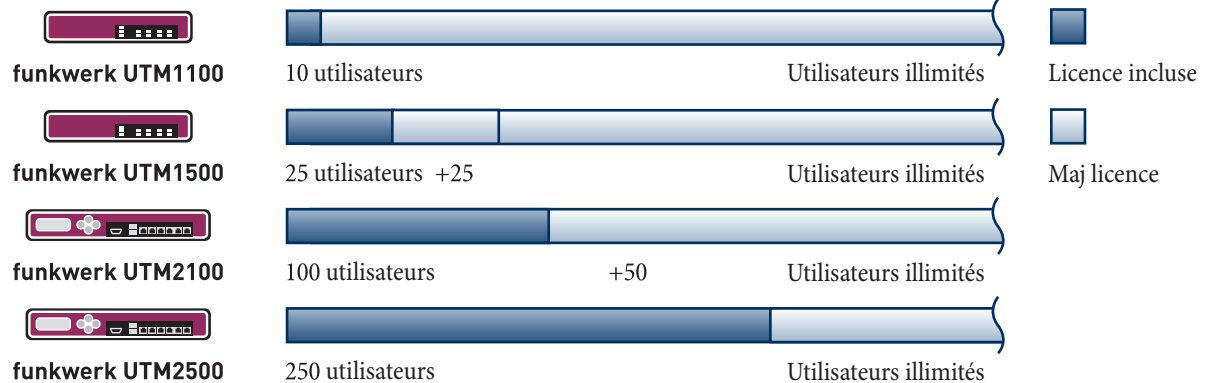
Un second système redondant, dit de secours, est disponible en cas de panne et prend en charge, automatiquement et sans interruption, les tâches du système principal jusqu'à ce que celui-ci soit réparé et remis en service.



POINTS FORTS

- ▶ Prévention d'intrusion avec fonction auto-prévention
- ▶ Des milliers de règles et signatures intégrées
- ▶ Authentification Out-of-Band
- ▶ Firewall et VPN
- ▶ Filtrage d'URL
- ▶ Qualité de Service (QoS)
- ▶ Antispam et antivirus inclus de base gratuitement
- ▶ Protection avancée via l'antivirus Kaspersky, l'antispam Commtouch et le filtrage URL Cobion
- ▶ Protection de type "Day zero"
- ▶ Configuration facile via Wizard
- ▶ Exploitation intuitive via l'interface utilisateur basée sur le Web
- ▶ Haute disponibilité

SYSTEMES UTM - LICENCES



Plus qu'un simple produit : un concept de sécurité sophistiqué.

SERVICE HARDWARE

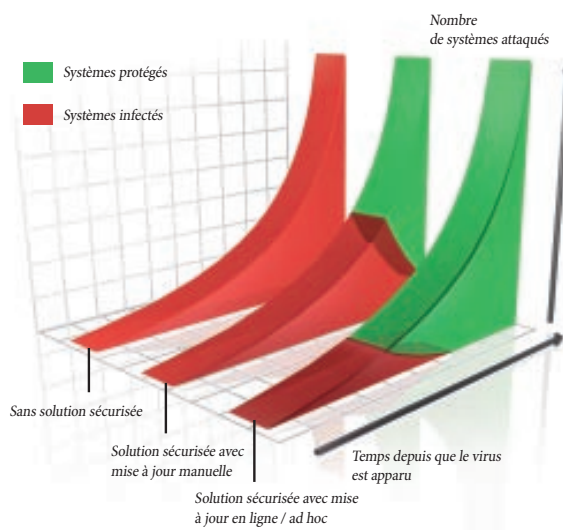
Un service hardware peut être souscrit pour une période de 12, 24 ou 36 mois pour tous les systèmes UTM.

Dans le cadre de ce contrat de service, Funkwerk Enterprise Communications garantit la livraison de pièces de rechange – y compris les extensions de garantie – sous 48 H.

SERVICE DE MISE À JOUR : SÉCURITÉ

Une application de sécurité, qui n'est pas à jour, ne peut pas protéger efficacement votre réseau. Les pirates informatiques développent très rapidement de nouvelles stratégies pour attaquer et endommager les réseaux.

C'est pourquoi Funkwerk Enterprise Communications offre un service de mise à jour pour les produits de sécurité des gammes IDS, IPS et UTM, et fournit automatiquement aux applications de sécurité les toutes dernières règles et signatures, protégeant ainsi votre réseau de manière optimale, à intervalle régulier et, en cas de danger imminent, en temps réel.

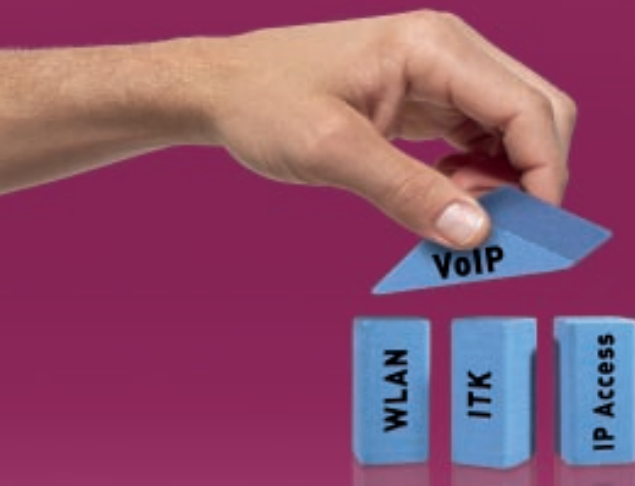


FORMATION UTM

Funkwerk Enterprise Communications propose à ses partenaires commerciaux, administrateurs et utilisateurs une formation complète sur deux jours portant sur l'installation, l'utilisation et l'administration des systèmes funkwerk UTM.

FONCTIONNALITES DES SYSTEMES FUNKWERK UTM

Gestion Unifiée des Menaces	funkwerk UTM1100	funkwerk UTM1500	funkwerk UTM2100	funkwerk UTM2500
Administration				
Mise à jour automatique	•	•	•	•
Interface Console	•	•	•	•
Web GUI (HTTPS)	•	•	•	•
Statistique en Temps réel	•	•	•	•
Antispam				
Moteur heuristique intégré	•	•	•	•
Quarantaine pour POP3	•	•	•	•
Quarantaine pour SMTP	Q3/08	Q3/08	Q3/08	Q3/08
Liste blanche / Liste noire	•	•	•	•
Vérification en-tête MIME	•	•	•	•
Protection optionnelle	Commtouch	Commtouch	Commtouch	Commtouch
RBL, ORDB	•	•	•	•
Antivirus				
Moteur AV intégré	•	•	•	•
Mise à jour automatique	•	•	•	•
Protection optionnelle	Kaspersky	Kaspersky	Kaspersky	Kaspersky
Examen HTTP, FTP, SMTP, POP3	•	•	•	•
Filtrage d'URL				
Filtrage basé sur l'utilisateur	•	•	•	•
Filtrage basé sur IP	•	•	•	•
Protection optionnelle	•	•	•	•
Filtrage par catégorie	•	•	•	•
Base de données en ligne (> 4,4 billions pages)	•	•	•	•
Détection et Prévention d'intrusion dynamique				
Nombre de signatures	> 6000*	> 6000*	> 6000*	> 6000*
Mise à jour automatique	•	•	•	•
Auto-Prévention	•	•	•	•
Analyse du protocole au niveau applicatif	•	•	•	•
Filtrage "stateful pattern" (trame)	•	•	•	•
Authentification Utilisateur				
Certificats (utilisateur et système)	•	•	•	•
Authentification FTP, HTTP, PPTP, L2TP	•	•	•	•
Base de données utilisateur locale	•	•	•	•
Authentification Out-of-band	•	•	•	•
Support des bases externes LDAP et Radius	•	•	•	•
Licences utilisateur				
Nombre maximum d'utilisateurs	10	25 / 50 / illimité	100 / 150 / illimité	250 / illimité
Détection des menaces				
Détection d'anomalie basée sur une application	•	•	•	•
Débordement de mémoire tampon	•	•	•	•
DoS	•	•	•	•
Fragmentation de paquets	•	•	•	•
Examen de ports	•	•	•	•
Virus, Trojans, Phishing, Vers, Attaques de pirates	•	•	•	•
Fonctions Firewall				
Suivi des connexions (FTP, SIP, PPTP, TFTP)	•	•	•	•
Firewall Multi Inspection	•	•	•	•
NAT (Translation d'adresse Réseau)	•	•	•	•
PAT (Translation d'adresse Port)	•	•	•	•
Gestion de Trafic				
Protocole de routage (OSPF)	•	•	•	•
Qualité de Service	•	•	•	•
Règle basée sur la classification	•	•	•	•
Priorisation des données	•	•	•	•
Réservation de la bande passante	•	•	•	•
Limitation de la bande passante	•	•	•	•
Routage étendu (Policy based routing)	•	•	•	•
VPN				
Client pour site VPN	•	•	•	•
Tunnels dédiés	illimité	illimité	illimité	illimité
Certificats IKE	•	•	•	•
Dead peer Detection	•	•	•	•
IPsec avec adresses dynamiques	•	•	•	•
IPsec NAT Traversal	•	•	•	•
PPTP, L2TP, IPsec	•	•	•	•
Authentification SHA1 / MD5	•	•	•	•
Chiffrement (DES, 3DES, AES, Blowfish, Twofish, Serpent)	•	•	•	•
Services Locaux				
Serveur DHCP	•	•	•	•
Serveur DNS	•	•	•	•
Client dynamique DNS	•	•	•	•
FTP, HTTP, SMTP et POP3 Proxy	•	•	•	•
Relais SMTP	•	•	•	•
Logging				
Log pour serveur distant syslog	•	•	•	•
Log pour serveur SNMP	•	•	•	•
Logging local	•	•	•	•
Notification Email	•	•	•	•
Configuration du système				
Ports Ethernet 10/100 Mbit/s	4	4	6	-
Ports Ethernet 10/100/1000 Mbit/s	-	-	-	6
Gestion du système				
Surveillance via SNMP	•	•	•	•
Disponibilité du système				
Configuration de secours automatique	•	•	•	•
Haute disponibilité	•	•	•	•



Flexibilité et Pérennité.

**Vous avez des questions ou vous souhaitez recevoir des informations plus détaillées ?
N'hésitez pas à nous contacter !**

Funkwerk Enterprise Communications France

6 Allée de la Grande Lande - CS 20102 - 33173 Gradignan Cedex - France

Tél : +33 (0)5 57 35 63 00 / Fax : +33 (0)5 56 89 14 05

e-mail : info.france@funkwerk-ec.com
www.funkwerk-ec.com