D-Link®

Firewall / Pare-feu

NETDEFEND

DFL-1100

PARE-FEU DE SECURITE RESEAU POUR ENTREPRISE

Le DFL-1100 est un pare-feu facile à déployer, d'une grande capacité conçu pour les grandes entreprises qui ont besoin d'une performance supérieure. Ce produit est une solution de sécurité puissante qui comprend tolérance de panne et haute disponibilité, fournissant un NAT (Network Address Translation) intégré, un pare-feu, le filtrage du contenu, la protection IDS, la gestion de la bande passante aussi bien que le VPN (Virtual Private Network). Le DFL-1100 inclut un lien WAN, un port LAN protégé, un port DMZ pour supporter les serveurs e-mails et Web locaux ainsi qu'un port de secours pour se connecter à un autre pare-feu.

Application de sécurité multifonction

Les fonctions du DFL-1100 sont celles des pare-feux pour entreprise, comme SPI (Stateful Packet Inspection), détection/abandon des paquets intrus, VPN incorporé, un port physique DMZ, de multiples IP mapping et serveurs virtuels. Le DFL-1100 connecte facilement votre bureau à un modem-routeur câble ou DSL via un port externe WAN 10/100Base-TX.

Fonctions pare-feux complètes

Le DFL-1100 offre des fonctions pare-feux complètes, incluant le mode NAT, le mode PAT (Port Address Translation), le mode Routage et SPI. Il supporte également des règles configurables adaptées au besoin du client ainsi qu'une configuration en serveur virtuel. Les administrateurs peuvent facilement administrer le réseau via les statistiques graphiques dans un système d'enregistrement et de surveillance.

VPN IPSec haute performance

Le DFL-1100 est équipé d'un support VPN incorporé vous permettant de créer de multiples tunnels IPSec pour les sites/clients distants. IPSec sur le DFL-1100 utilise un fort encryptage avec DES, 3DES, AES et Automated Key Management via IKE/ISAKMP. Un tunnel VPN peut être activé du DFL-1100 vers un site distant ou un utilisateur mobile afin d'avoir un flux de trafic sécurisé utilisant un triple encryptage DES. Cela offre aux utilisateurs un moyen d'accéder confidentiellement et de transférer des informations sensibles. Plusieurs tunnels VPN peuvent être facilement créés sans besoin de paramétrer des règles IKE (Internet Key Exchange).

Liste de contrôle d'accès (ACL)

Le blocage d'URL est une des caractéristiques de base offertes par le DFL-1100. Cette fonction offre le bénéfice d'un accès limité aux sites Internet indésirables. Le trafic Internet est enregistré en temps réel. Les alarmes sur les attaques Internet et la notification des activités de surf sur le Web sont enregistrées et peuvent être transmises par e-mail. Le DFL-1100 supporte une authentification Radius donc vous pouvez utiliser votre Serveur Radius existant et les droits d'accès utilisateurs associés.

Caractéristiques avançées pour une protection complète

Le DFL-1100 offre des caractéristiques avancées incluant le filtrage du contenu, l'IDS (Intrusion Detection System), la gestion de la bande passante pour une solution complète de protection des utilisateurs du réseau. Le filtrage du contenu vous permet de filtrer et protéger votre réseau avec des règles adaptées. La gestion de la bande passante garantit et/ou limite une bande passante pour les différents services.

Le DFL-1100 protège votre réseau des attaques. Il peut être configuré pour enregistrer toutes les attaques, localiser l'adresse IP source qui génère l'attaque, envoyer l'avis de rapport d'attaques à une adresse e-mail spécifiée et établir des règles pour limiter le trafic entrant d'adresses IP sources spécifiques. Les administrateurs réseaux peuvent configurer des adresses e-mails pour qu'elles reçoivent un message d'alerte de la part du DFL-1100. Lorsque les évènements d'instrusion sont détectés, le DFL-1100 les enregistrera et enverra un e-mail d'alerte. L'administrateur pourra alors contrôler le fichier enregistré sur le routeur afin de découvrir ce qui s'est produit.

Haute performance et tolérance de panne

Le DFL-1100 peut gérer jusqu'à 200 000 sessions concurrantes, procurant jusqu'à 1000 tunnels VPN pour jusqu'à 1000 utilisateurs mobiles qui ont besoin d'une connexion à distance sécurisée au réseau de la société. De plus, ce pare-feu fournit aussi la tolérance de panne en utilisant un autre pare-feu connecté sur le port de secours, fournissant ainsi une protection pare-feu continue pour des applications de mission critique.

1 port DMZ, 1 port LAN sécurisé et 1 port de secours

Le DFL-1100 inclut un port LAN qui permet la connexion sur le réseau interne de votre bureau, un port de secours qui permet la connexion à un pare-feu et un port physique DMZ (Demilitarized Zone) qui connecte vos serveurs Web, mail ou FTP pour y accéder via Internet. La fonction DMZ est utile car elle sépare le trafic encombré du serveur du réseau interne, pendant que vous protégez les autres ordinateurs de votre bureau des attaques Internet en les cachant derrière le pare-feu.

CARACTERISTIQUES PRINCIPALES

- *1 port LAN 10/100Base-TX, 1 port DMZ 10/100Base-TX, 1 port de secours 10/100BASE-TX*
- *1 port WAN 10/100Base-TX pour connecter un modem câble/DSL*
- *PPTP, L2TP, VPN IPSec tunneling supportés**
- *PPTP, L2TP, VPN IPSec pass-through supportés*
- *Mode agressif/client principal pour VPN*
- *Protection pare-feu SPI (Stateful Packet Inspection)*
- *Deni de Service (Dos) et blocage des attaques DDoS*
- *Network Address Translation (NAT)/Network address Port Translation (NAPT)*
- *NAT Application Level Gateway (ALG) supportée*
- *Serveur/client DHCP et contrôle parental*
- *PPPoE supporté*
- *Filtrage du contenu, blocage d'URL/de domaine et contrôle de mot clé*
- *Serveur virtuel supporté*
- *Configuration via le Web et enregistrement en temps réel*
- *Protocole SYSlog supporté*

**Les tunnels VPN PPTP et L2TP seront supportés dans une prochaine mise à jour firmware.*

DFL-1100

Spécifications techniques

Firewall / Pare-Feu

Matériel
- DRAM : SDRAM 256Mbytes
- Mémoire flash : 64Mbytes
- Accélérateur : accélérateur VPN pour une plus haute performance

Ports du produit
- WAN : port 10/100Base-TX
- LAN : port 10/100Base-TX
- DMZ : port 10/100Base-TX
- Secours : port 10/100Base-TX
- Port console : port série COM

Performance et Sortie
- Pare-feu : 250Mbps ou supérieur
- 3DES : 34Mbps ou supérieur
- AES : 84Mbps ou supérieur
- Sessions concourantes : 200 000 max.
- Tunnels VPN : 1000 max.
- Polices : 2000 max.
- Programmes : 256 max.
- Utilisateurs en ligne : 500 max.

Logiciel

Modes d'opération du pare-feu
- NAT (Network Address Translation)
- PAT (Port Address Translation)
- Mode Routage
- IP Virtuel
- Règles basées NAT

Sécurité VPN
- Serveur/Client IPSec, PPTP, L2TP*
- Pass through IPSec/PPTP/L2TP
- Authentification : MD5 et SHA-1
- Encryptage : Nul, DES, 3DES et AES
- Administration de la clé : manuelle et IKE
- Mode de vérouillage : clé pré-partagée
- Echange de clé : DH1, DH2 et DH5
- Mode de négociation : Rapide, Principal et Agressif
- Accès VPN à distance
- Règles de protection et protection de session
- Keep-Alives sur tunnels configurables
- Hub-n-Spoke

**Les fonctions Serveur/Client PPTP et Serveur/Client L2TP seront disponibles dans une prochaine mise à jour firmware.*

Sécurité du pare-feu
- NAT
- Stateful Packet Inspection (SPI)/Deni de Service (DoS)
- Filtre de paquet
- Filtrage du contenu (blocage d'URL par mot clé, Java/ ActiveX/Cookie/Blocage Proxy)
- Filtres de protocoles courants
- Filtre ICMP
- Microsoft Active Directory Integration (via MS IAS)

Administration
- Administrateurs multiples
- Niveaux super Administrateur, Administrateur et lecture seule
- Mises à niveau logicielles et changements de configuration
- Hôte sécurisé

Services Réseaux
- Serveur/Client DHCP
- Relais DHCP
- DHCP sur IPSec
- PPPoE pour DSL
- PPTP pour DSL
- Câble BigPond
- Niveau d'application passerelle H.323*, SIP*, FTP
- Résolution DNS de la passerelle distante

**Fonctions disponibles dans une prochaine mise à jour firmware.*

Système
- Enregistrement système
- Mise à jour firmware
- Alertes e-mail
- Filtrage de l'activité (enregistrement des requêtes de connexions internes et externes rejetées)
- Enregistrement des accès Web
- Monitoring des accès Internet
- Administration à distance par le WAN
- Simple Network Time Protocol (SNTP)
- Simple Network Management Protocol (SNMP)
- Service SDI qui utilise les solutions Internet d'Ericsson
- Http
- Contrôle de la consistence

Authentification de l'utilisateur du pare-feu et du VPN
- Base de données RADIUS (Externe)
- Base de données intégrée : limitée à 1500 utilisateurs

IDS
- Modèle NIDS
- DDoS et DoS détectés
- Adresse Mac liée avec IP
- Modèle de mise à jour en ligne
- Détection CodeRed
- Alarme attaque (via e-mail)
- Enregistrement et rapport

Administration de la bande passante
- Bande passante garantie
- Bande passante maximum
- Utilisation prioritaire de la bande passante
- DiffServ stamp
- Class-based policies
- Classification du trafic par applications spécifiques
- Règles de gestion du trafic
- Classification du trafic par subnets spécifiques

Haute disponibilité
- Protection de session pour pare-feu et VPN
- Active-Active cluster et balance de charge
- Détection des défaillances du produit
- Synchronisation des états
- Synchronisation VPN
- Méthode de synchronisation : Ethernet
- Temps moyen de rétablissement : <800ms
- Notification du réseau sur échec

Driver / Firmware supporté
Via le Web

Physique et Environnement

LEDs de diagnostic
- Alimentation
- Statut
- WAN
- LAN
- DMZ
- Backup

Alimentation électrique
Via une alimentation universelle interne

Dimensions et Poids (produit seulement)
- 295 x 440 x 44 mm
- 3,8 kg

Températures supportées
- A l'utilisation : 0° à 60°C
- En stockage : -20° à 70°C

Humidité
5% à 95% non condensé

Emission
- FCC Class A
- CE Class A
- C-Tick
- BSMI

Sécurité
- UL
- TUV/GS
- LVD (EN60950)

D-Link®