

NETASQ F50

IPS-Firewall



ANTIVIRUS INTÉGRÉ⁽²⁾, PRÉVENTION D'INTRUSION, FIREWALL, ANTISPAM, VPN ET FILTRAGE DE CONTENU

Les IPS-Firewalls NETASQ ont été spécialement conçus pour assurer une sécurité complète des réseaux en combinant Prévention d'Intrusion en Temps Réel, Firewall, Réseaux Privés virtuels avec IPSEC (RPV), Filtrage de contenu avancé, antispam et antivirus Kaspersky⁽²⁾. Basés sur l'ASQ, technologie propriétaire et révolutionnaire de prévention d'intrusion, tous les IPS-Firewalls NETASQ offrent le plus haut niveau de sécurité.

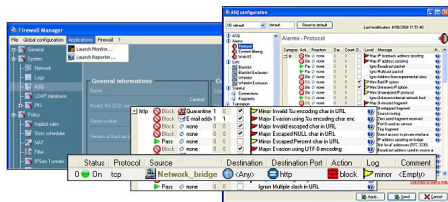


L'IPS-FIREWALL F50 DE NETASQ F50 est une solution de sécurité facile à déployer à destination des petites entreprises et/ou agences qui nécessitent un port DMZ, un antivirus encore plus intégré, ainsi que du management, du monitoring et du reporting granulaires. Le F50 s'adresse aux besoins des petites entreprises jusque 50 employés qui exigent une solution complète de filtrage de contenu ainsi que du VPN IPSEC.

PRÉVENTION D'INTRUSION A LA VOLÉE : ASQ, la prévention d'intrusion intégrée de NETASQ, multi couches et multi méthodes analyse le trafic en temps réel, le protégeant ainsi contre les attaques réseau, applicatives ainsi que les attaques combinées les plus sophistiquées. Grâce à son mode d'opération en ligne, il fournit une protection sur toutes les interfaces, sécurisant ainsi les serveurs locaux des activités malicieuses.

ANTISPAM PERFORMANT : identifie les e-mails non sollicités (spam) avant qu'ils n'atteignent la boîte aux lettres de l'utilisateur.

UTILISATEUR DISTANT ET VPN GATEWAY-GATEWAY : L'IPS-Firewall F50 de NETASQ supporte le VPN IPSEC pour les deux tunnels gateway-gateway et pour l'utilisateur distant. Alors que le trafic peut être crypté en AES 256-bit, il reste surveillé par la prévention d'intrusion intégrée de NETASQ et par l'antivirus KASPERSKY.



FILTRAGE D'URL AVANCE : La solution de Filtrage d'URL avancé de NETASQ est intégrée et repose sur une base de données dynamique répertoriant des sites web classés par catégorie.

SIGNATURES CONTEXTUELLES : Les Signatures Contextuelles ASQ intègrent les signatures de nouvelles applications, de nouvelles attaques et des adaptations aux signatures existantes. Les signatures ASQ supportent les protocoles applicatifs et les applications Peer-to-Peer telles que Kazaa et Emule, ou les outils de messagerie instantanée comme Yahoo!, AOL ou MSN Messenger.

Les IPS-Firewalls NETASQ ont été conçus autour d'une technologie unique de **prévention d'intrusion en temps réel** : l'**ASQ (Active Security Qualification)**. L'ASQ fournit une prévention d'intrusion **basée sur le contexte** en analysant le trafic de la couche réseau jusqu'à la couche applicative et en appliquant de **multiples méthodes** pour identifier et bloquer tout trafic malveillant. L'ASQ utilise des familles d'attaques lui garantissant une précision optimum afin de protéger le réseau contre les menaces les plus récentes tout en conservant plusieurs gigabits de débit. Ce concept unique, associé à des plates-formes matérielles spécifiquement développées pour offrir une nouvelle génération de prévention d'intrusion, permet aux IPS-Firewalls NETASQ de réaliser un traitement préventif en temps réel au niveau de la couche applicative **sans diminuer les performances du système**.

■ ■ ADMINISTRATION SUITE

Tous les IPS-Firewalls F50 de NETASQ sont livrés avec un package complet de fonctionnalités appelé Administration Suite. Celle-ci comprend le Firewall Manager, Monitor et Reporter. Tous ces outils comportent une interface graphique intuitive et conviviale sous plate-forme Windows, permettant une facilité d'installation et de configuration de votre IPS-Firewall ainsi que des fonctionnalités de monitoring et de reporting simplifiées.

GESTION CENTRALISÉE – NETASQ ADMINISTRATION GLOBALE

NETASQ Administration Globale permet aux entreprises, intégrateurs ou fournisseurs de services de gérer d'importants déploiements d'IPS-Firewalls NETASQ à partir d'un point central. Une interface graphique conviviale et simple d'utilisation vous permet de **mettre à jour, superviser et configurer** de manière centralisée les IPS-Firewalls NETASQ. La collecte et le stockage dans une base SQL de l'ensemble des logs des IPS-Firewalls installés permettent une analyse de l'activité des utilisateurs, des incidents et attaques ainsi que la **génération de rapports**.

Le F50 est livré, en standard, avec une version limitée à 5 appliances de l'Administration Globale. Cette version limitée n'intègre pas la collecte et le stockage des logs dans une base SQL. La version non limitée est disponible en option.

OPTIONS DE LICENCE :

■ ■ ANTIVIRUS KASPERSKY

L'antivirus KASPERSKY offre une protection supplémentaire contre les virus et vers qui se diffusent par E-mail.

Spécifications du F50⁽¹⁾

■ Performances IPS-Firewall (Incl. Prévention d'intrusion)	100 Mbits/s
■ Débit VPN AES (Incl. Prévention d'intrusion)	15 Mbits/s
■ Interfaces 100 Base-T (cuivre)	3
■ Nb maximum d'interfaces	3
■ Connexions simultanées	4 000
■ Politique de filtrage	550
■ Tunnels VPN Gateway-Gateway	100
■ Tunnels VPN Client-Gateway	Oui
■ Utilisateurs	10, 25, illimité

(1) Les performances système fournies sont les mesures maximum sous conditions idéales de test et peuvent varier selon les conditions d'exploitation et de déploiement.
(2) Requiert une licence Kaspersky



Fonctionnalités Réseau

- Mode routage, translation, bridge et hybride
- Routage par interface
- Support jusque 16 VLANs
- Routeur Dialup intégré (PPTP, PPPoE, PPP)
- Translation d'adresses (NAT, 1 to 1, PAT et Split)
- Gestion horaire
- Haute disponibilité xDSL et Load Balancing
- Support jusque 4 modems xDSL ou Dialup
- Gestion de la bande passante
- Gestion de plusieurs adresses IP par interface

Système de Prévention d'Intrusion (ASQ)

- Prévention d'Intrusion en temps réel ASQ
- Plug-ins ASQ (HTTP, FTP, DNS, RIP, H323, EMule, SSL, SSH, Telnet, SMTP, POP3, IMAP4, NNTP, Generic...)
- Prévention des attaques dans les tunnels VPN
- Analyse multi couches (couches protocolaires, connexion, session et applicative)
- Blocage des attaques connues et inconnues avec ou sans contexte
- Protection contre les attaques de saturation (ICMP, UDP et TCP)
- Protection contre l'évasion des données
- Chevaux de Troie/Backdoor et protection
- Protection contre la découverte d'OS
- Protection contre le détournement de session
- Signatures contextuelles
- Blacklisting dynamique
- Mise en quarantaine

Fonctionnalités VPN

- Protocoles VPN supportés : IPSec et PPTP
- Support jusque 16 clients VPN PPTP
- Chiffrement jusque 256 bits supportant les algorithmes DES, 3DES, AES, CAST 128 et Blowfish
- ESP
- Authentification SHA-1 et MD5
- Authentification des certificats IKE
- Clés pré partagées, certificats PKI, statique
- VPN Hub & Spoke
- Tunnels VPN Gateway - Gateway
- Tunnels VPN Client - Gateway
- VPN Keep-alive
- Détection Dead Peer
- NAT-Traversal (UDP 500 et 4500)

Antispam

- Blacklisting DNS

Authentification

- Support de l'authentification unique SSO
- Authentification LDAP (Interne et Externe)
- Authentification Windows (NT4 – NTLM et WIN2K Kerberos)
- Compatibilité PKI externe
- Radius

Services

- Proxy HTTP – Filtrage URL
- Support ICAP pour filtrage URL
- Proxy SMTP
- Proxy POP3
- DynDNS
- SNMP v1, v2 et v3
- Serveur DHCP Interne

Haute Disponibilité

- Active / Passive
- Gestion logicielle de la fonction
- Synchronisation de la configuration
- Réplication des sessions



Logging / Monitoring

- Notification E-mail
- SNMP v1, v2 et v3
- Moniteur en temps réel
- Syslogging
- Stockage interne des logs
- Rapports historiques
- Dump de paquets

Management

- Firewall Manager (Interface Windows)
- Firewall Monitor (Interface Windows)
- Firewall Reporter (Interface Windows)
- Syslog, SSHv2, Console

Options

- Antivirus Kaspersky
- Licence pour 25 / utilisateurs illimités

Fonctionnalités Antivirus ⁽²⁾

- Redirection Proxy HTTP
- Redirection Proxy SMTP
- Antivirus Kaspersky (SMTP, POP3)
- Taille maximum des fichiers analysés (non compressés ou après décompression) : 10 MB

Software Suite en option

- NETASQ Administration Globale

Performances

Performances IPS-Firewall (Incl. Prévention d'Intrusion)	100 Mbits/s
Débit VPN AES (Incl. Prévention d'Intrusion)	15 Mbits/s

Spécifications Hardware

Nb de ports Ethernet	3
Nb max d'interfaces	3
Processeur	400 Mhz
Stockage	Flash 128 Mo
Mémoire	128 Mo
Dimensions (mm)	213 x 195 x 44
	1U / 0,5 x 19"
Poids	1,5 Kg
Alimentation	30 W externe
Connexion de contrôle	Port Série RS-232C
	Emulation VT100

Environnement

De fonctionnement	5° à 35 °C
Hors fonctionnement	-30° à 65 °C

www.netasq.com

