

NETASQ V50, V100, V200 & V500

APPLIANCES VIRTUELLES POUR PME ET SEGMENTATION RÉSEAU

Les PME doivent garder à l'esprit que tous les réseaux présents dans leur infrastructure IT, qu'ils soient virtuels ou physiques exigent le même niveau de protection contre les menaces actuelles et émergentes.

Les avantages de la virtualisation sont évidents, en particulier pour les petites et moyennes entreprises : réduction des coûts, optimisation des ressources, gestion et déploiement des services simplifiés et récupération plus rapide des données. Toutefois, la virtualisation permet le regroupement d'une multitude de services, dont un grand nombre ayant des niveaux de confiance différents, qui peuvent s'exécuter sur la même plateforme physique.

Cette pratique requiert des solutions performantes afin de sécuriser la circulation des données entre les machines virtuelles. Parce qu'il est impossible d'installer un firewall traditionnel sur un réseau virtuel, la meilleure méthode pour surveiller la communication au sein d'un environnement de ce type consiste à déployer une appliance virtuelle de sécurité.

LES POINTS CLÉS

- Certifié VMware Ready et Citrix XenServer Ready
- Pas de coût initial
- Portabilité
- Prévention d'intrusion zero-day
- Mises à jour automatiques

LA SÉCURISATION DE VOTRE RÉSEAU VIRTUEL

Les machines virtuelles disposent des mêmes systèmes d'exploitation, logiciels CRM/ERP et applications essentielles de l'entreprise que les serveurs physiques. Les serveurs de messagerie et les serveurs Web traditionnellement installés sur la DMZ, peuvent par conséquent être hébergés dans le même environnement que les serveurs de production, rendant ce dernier potentiellement plus accessible.

Lorsque vous passez d'un environnement physique à un réseau virtuel, une appliance virtuelle de sécurité est nécessaire pour assurer la continuité de votre activité. Une solution proactive et tout-en-un (UTM) mature basée sur un IPS incluant une analyse complète et en temps réel vous permettra de profiter pleinement de tous les avantages de la virtualisation.

Le moteur de prévention d'intrusion NETASQ est au cœur de toutes les appliances virtuelles pour PME. Intégrées au système d'exploitation, elles délivrent également les fonctionnalités de firewall, d'antivirus et d'antispam. La protection de votre trafic VoIP est assurée ainsi que vos communications intersites, grâce aux tunnels VPN IPSec et SSL.

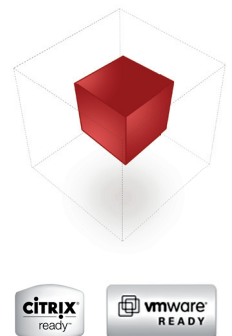
Le moteur de NETASQ analyse les applications et les protocoles réseaux afin de détecter et de bloquer les menaces. Il apporte une sécurité de haut niveau en réduisant considérablement le risque de fausses alertes à l'aide de l'analyse comportementale alliée à plusieurs bases de données de signatures contextuelles.

LA RÉDUCTION DES COÛTS

Pour rester compétitives, les PME doivent minimiser les coûts liés à leur infrastructure IT, ce qui conduit souvent à réaliser des compromis quant à la qualité des services IT déployés.

En tenant compte de ces contraintes, les appliances virtuelles NETASQ font bénéficier les PME d'une gamme complète de fonctions de sécurité sans coût initial, par un simple abonnement aux services, qui inclut les mises à jour du système et des différentes protections.

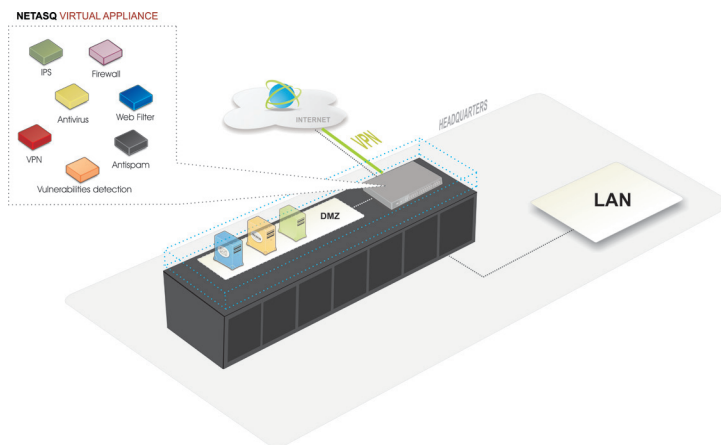
Les avantages de l'approche « à la demande » sont évidents : réduction significative des investissements pour la sécurité, contrôle total des coûts, retour sur investissement rapide et protection de pointe.



Cas d'usage

Les réseaux virtuels et physiques, un même niveau de protection requis.

Les appliances virtuelles NETASQ dédiées aux PME assurent que chaque réseau virtuel possède la même protection de pointe que leur équivalent physique. La série V de NETASQ protège le trafic entre machines virtuelles mais aussi tout le trafic des réseaux physiques et virtuels. La virtualisation permet de réduire les coûts de manière significative, Il n'y a donc plus besoin de compromettre la sécurité. Les appliances virtuelles et physiques NETASQ sont toutes les deux administrées depuis la même suite d'administration.



CARACTÉRISTIQUES PRINCIPALES	V50	V100	V200	V500
Adresses IP protégées	50	100	200	500
Connexions simultanées	100 000	200 000	400 000	600 000
VLANs 802.1Q (max)	32	128	128	128
Tunnels VPN IPSEC (max)	100	500	1 000	1 000
Clients VPN SSL simultanés	50	256	512	512

FIREWALL UTILISATEUR

Base de données interne (LDAP)

Authentification par un tiers - LDAP, Active Directory, Radius, NTLM

Authentification transparente - Microsoft SPNEGO - Certificat SSL

FIREWALL MULTIFONCTION - UTM

Proxies SMTP, POP3, HTTP, FTP

Antivirus, antispyware intégrés

Antispam par réputation (DNS RBL)

Antispam avec analyses heuristiques

VPN IPSEC

VPN SSL

IPS - FIREWALL APPLICATIF

Vérification en temps réel de la politique de sécurité

Programmation horaire de politiques

Quarantaine automatique en cas d'attaques

Protection contre les attaques de type flooding

Protection contre l'évasion de données

Gestion avancée de la fragmentation

Protection contre les SQL injections

Protection contre les Cross Site Scripting (XSS)

Détection de chevaux de Troie

Protection contre l'hijacking de sessions

Analyses applicatives dédiées (plugins) : IP, TCP, UDP, HTTP, FTP, SIP, RTP/RTCP, H323, DNS, SMTP, POP3, IMAP4, NNTP, SSL, MGCP, Edonkey, SSH, Telnet ...

SERVICES RÉSEAU

Client et serveur DHCP

Client NTP

Proxy cache DNS

RÉSEAU - ROUTAGE - QUALITÉ DE SERVICE

Mode transparent, routé et hybride

Translation d'adresses (NAT, PAT, split)

Routage statique - Routage par politique

Routage dynamique

Garantie et limitation de bande passante

Gestion de bande passante par priorité

MANAGEMENT

Administration par rôles

NETASQ UNIFIED MANAGER

NETASQ REAL-TIME MONITOR

NETASQ EVENT REPORTER

ssh v2

MONITORING - REPORTING

Serveurs syslog (max 3)

Alertes e-mail

Génération automatique de rapports

Agent SNMP v1, v2, v3 (DES, AES)

OPTION

Gestion des risques avec NETASQ

VULNERABILITY MANAGER

A propos de NETASQ

Avec plus de 75 000 firewalls UTM déployés dans des entreprises de toute taille, des institutions gouvernementales et des organismes de défense, NETASQ développe des solutions sans équivalent sur le marché en termes de performances, de protection et de contrôle. Leur certification au plus haut niveau européen (EU RESTRICTED, OTAN et EAL4+) les rend tout à fait uniques.

Plus d'informations : www.netasq.com

FRANCE Paris
+33 1 46 21 82 30
france@netasq.com

BENELUX & NORDICS
Breda
+31 76 8883022
benelux@netasq.com

IBERICA Madrid
+34 91 761 21 76
iberia@netasq.com

ITALIA Milano
+39 02 7253 7249
italia@netasq.com

UK London
+44 207 092 6682
uk@netasq.com

DACH München
+49 89 20 300 6320
dach@netasq.com

MIDDLE EAST & AFRICA
+971 50 5573 746

INTERNATIONAL
international@netasq.com