

Une passerelle de sécurité unique pour les PME : des performances sans compromis



Aujourd'hui, virus et malwares véhiculés par les pages web, attaques de phishing par e-mail, spam, e-mails contaminés par des virus font désormais partie des attaques mixtes variées et sophistiquées qui parviennent à contourner facilement les firewalls classiques. Les petites entreprises ont été les plus durement touchées, car à la différence des grandes organisations, elles n'ont bien souvent ni le temps ni les ressources nécessaires pour renforcer et sécuriser leur réseau face à ces menaces.

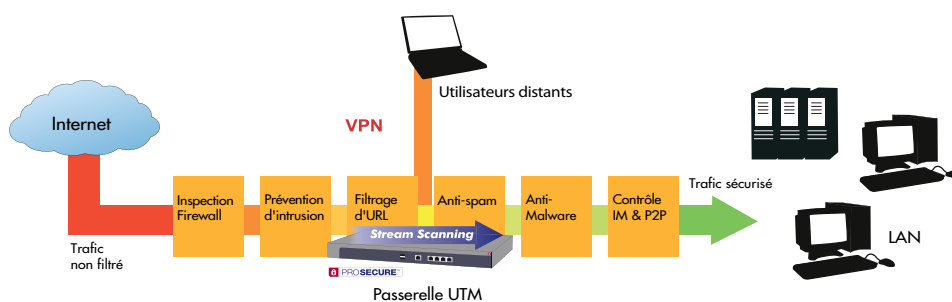
De plus, le profil des menaces a sensiblement évolué : Auparavant, les menaces qui touchaient les petites entreprises adoptaient principalement une approche de type " push " par laquelle les pirates visaient directement l'accès aux petites entreprises, une occurrence relativement rare, les moyennes et grandes entreprises constituant des cibles plus facilement identifiables et plus riches. Mais avec l'apparition des technologies Web 2.0 et le développement des services informatiques à distance, le paysage des menaces s'est modifié, désormais caractérisé largement par des attaques de type " pull ", les utilisateurs finaux " attirant " la menace à l'intérieur de leur organisation par le simple fait d'utiliser les technologies Web 2.0 et l'informatique à distance.

Les solutions de sécurité réseau complètes nécessitant une puissance de calcul très importante pour analyser le trafic réseau en temps réel, les solutions tout-en-un actuelles destinées aux PME ont bien souvent recours à des technologies de sécurité rudimentaires, qui privilégient la vitesse au détriment de la couverture de protection. Une véritable sécurité doit impérativement proposer des performances suffisantes à la fois en termes de couverture et de vitesse de traitement.

Sécurité réseau tout-en-un, sans compromis

Les passerelles NETGEAR ProSecure UTM (Unified Threat Management) assurent la gestion centralisée des menaces en combinant performances et exhaustivité de l'analyse. Grâce à la technologie brevetée Stream Scanning (scan à la volée), il est possible d'utiliser une base de données très complète de virus et de malware tout en maintenant les débits à un niveau satisfaisant et en minimisant les temps d'attente provoqués par l'analyse. L'architecture logicielle flexible et modulaire adoptée exploite au mieux **la technologie du Stream-Scanning, analysant les fichiers et les flux de données jusqu'à 5 fois plus vite que les méthodes classiques.**

En retour, cette architecture permet aux passerelles UTM d'utiliser les bases de données de virus et de malware de NETGEAR et Sophos™, qui **comportent des centaines de milliers de signatures** et qui sont ainsi jusqu'à 200 fois plus complètes que les plateformes UTM pour petites entreprises existant jusqu'alors. Cette architecture, associée au meilleur des filtres web hybrides in-the-cloud et des technologies antispam, qui bénéficie également du savoir-faire reconnu de NETGEAR en matière de firewall et de fonctionnalités VPN, met à la disposition des PME une solution de sécurité idéale, centralisée au niveau de la passerelle.



Une Plate-forme Stream-Scanning Révolutionnaire

Etant donné les performances élevées que nécessite l'analyse du trafic web, processus sensible aux temps d'attente, il n'a pas été facile d'intégrer la technologie des solutions de sécurité 'grandes entreprises' aux plateformes tout-en-un classiques pensées pour les PME. Les passerelles NETGEAR UTM s'appuient sur une technologie de stream-scanning brevetée, qui analyse les flux de données dès leur entrée sur le réseau. L'approche NETGEAR du stream-scanning autorise une exécution bien plus rapide que les méthodes classiques de batch-scanning, qui supposent la mise en tampon d'un fichier complet avant analyse.

Fonctionnalités et caractéristiques principales des appareils Netgear Prosecure UTM

Un moteur anti-malware à la pointe de la technologie

- Moteur d'analyse de malware de niveau professionnel
- Couverture jusqu'à 200 fois supérieure à celle des solutions PME tout-en-un existantes
- Détecte plus de 13 millions de menaces
- Mise à jour automatique des signatures, toutes les heures

La Technologie brevetée de Stream Scanning

- Les flux de données sont traités dès leur arrivée sur le réseau
- L'analyse du trafic web limite les temps d'attente

Technologie antispam par analyse répartie du spam

- Architecture hybride in-the-cloud
- Rassemble les données sur les menaces provenant de plus de 50 millions de sources dans le monde
- Chaque nouveau spam apparaissant est répertorié et détecté en quelques minutes
- Pas de période d'apprentissage, le boîtier est opérationnel immédiatement
- Taux de faux positif réduit au minimum
- Adaptabilité exceptionnelle à tous les types de spam

Filtrage d'URL par analyse répartie du trafic web

- Une technologie de pointe assurant un filtrage d'URL hybride in-the-cloud
- Des centaines de millions d'URL catégorisées
- Les nouveaux sites web sont catégorisés en temps réel
- 64 catégories
- Filtrage en fonction des utilisateurs et des groupes

Détection instantanée des menaces (" Zero Hour ")

- Détection de type heuristique
- Détecte les menaces inconnues dans l'instant
- Limite l'exposition du réseau aux nouvelles menaces non répertoriées

Système anti-intrusion NETGEAR

- Langage obéissant à des règles
- Les pirates sont maintenus à l'extérieur du périmètre du réseau

Contrôle d'applications messagerie instantanée et Peer-to-peer

- Bloque l'accès aux clients publics de messagerie instantanée (IM)
- Bloque les clients peer-to-peer

Accès distant par VPN SSL & IPSec

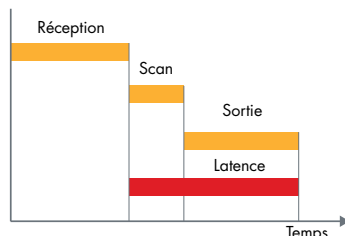
- VPN SSL : accès distant sans client, partout, à tout moment
- VPN IPSec : tunnels sécurisés de site à site et accès distant par client.
- Pas de licence supplémentaire à acquérir

VPN/Firewall intégré

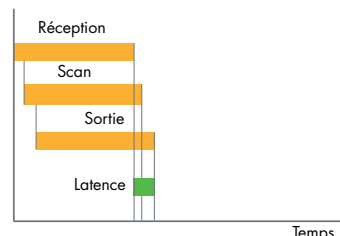
- Le Firewall* Gigabit Dual WAN assure équilibrage des charges et protection contre les défaillances
- Quatre ports LAN Gigabit, un port DMZ configurable
- Stateful packet inspection (SPI)
- Protection DoS (dénier de service)

Par son principe même, la méthode de batch-scanning classique impose une certaine latence sur le trafic réseau. Des temps d'attente acceptables pour le trafic e-mail, mais pas pour le trafic Web, car la navigation peut s'en trouver ralentie dans des proportions déraisonnables. Jusqu'à aujourd'hui, les solutions tout-en-un s'efforçaient d'en réduire l'impact en limitant le panel de signatures de malwares et en concentrant l'analyse sur quelques types de fichiers seulement, ou bien en faisant tout simplement l'impasse sur l'analyse du trafic web. Mais cette approche expose un pan entier du réseau aux attaques véhiculées par malware...

Batch Scanning



Stream Scanning (Scan à la volée)


Simple à paramétrer, facile à manager

La passerelle NETGEAR ProSecure UTM prendra sans problème la place de tout firewall ou routeur existant. Un assistant très simple en 10 étapes, vous guidera au cours de l'installation : votre boîtier UTM sera prêt à travailler en quelques minutes seulement. L'administration se fait à partir d'une plate-forme Web intuitive. Définissez des politiques et des alertes, passez en revue des statistiques résumées et générez des graphiques, récupérez des données au niveau de l'adresse IP, intégrez des journaux avec certains outils de management réseau standard utilisant le protocole SNMP. Les mises à jour des signatures de malware et IPS, des logiciels et firmwares sont gérées par le boîtier UTM, en ligne et automatiquement.

Pour bien des administrateurs et techniciens informatiques, le management des différentes licences est un véritable cauchemar. Acquérir une nouvelle licence chaque fois qu'on ajoute un ordinateur ou un utilisateur au réseau est un processus fastidieux et coûteux. La série des passerelles NETGEAR UTM propose des licences d'abonnement web et e-mail, sans restriction du nombre d'utilisateurs.

COMPARAISON

MODELES	UTM10	UTM25
CHOISIR LE BON BOÎTIER		
Type de client	Petit réseau	Petit réseau
Nombre d'utilisateurs en simultané	1-15	10-30
Débit AV	31 Mbps	45 Mbps
Débit du firewall SPI	133 Mbps	153 Mbps
Débit IPS	TBD	TBD
Débit du VPN	TBD	TBD
Sessions simultanées	8 000	20 000
VLANs	4 096	4 096
SECURITE DES CONTENUS		
Web (HTTP, HTTPS, FTP)	•	•
Email (SMTP, POP3, IMAP)	•	•
Stream Scanning (Scan à la volée)	•	•
Inspection du trafic entrant et sortant	•	•
Prévention et détection des intrusions	•	•
Protection instantanée sans signature	•	•
Signature des malwares	600 000	600 000
Mise à jour automatique des signatures	par heure	par heure
Véritable analyse et filtrage HTTPS	•	•
Filtrages des contenus web	Filtrage par : mots clés, extension de fichiers	

MODELES	UTM10	UTM25
Filtrage web	ActiveX, Java™, Flash, Javascript™, Proxy, Cookies	
Filtrage du contenu des Emails	Filtrage par : mots clés, pièces jointes protégées par mot de passe, extension de fichier, nom de fichier	
Analyse Répartie du Spam (DSA)	•	•
Liste noire antispam enrichie en temps réel		
Liste de messages spam bloqués/autorisés définie par l'utilisateur	Filtrage par : adresse Email de l'expéditeur, Adresse IP du domaine, adresse Email du destinataire, Domaine	
Analyse répartie du trafic web avec 64 catégories	•	•
Contrôle de messagerie instantanée	MSN Messenger, Yahoo Messenger, Skype, mIRC, Google Talk	
Contrôle Peer to Peer	BitTorrent, eDonkey, Gnutella	
Nombre d'utilisateurs Maximum	illimité	
FIREWALL		
SPI (stateful Packet Inspection)	Blocage de ports et services, Prévention des denial of service, Virus furtifs, blocage TCP, blocage UDP, Contrôle de la réponse au Ping WAN/LAN	
Modes WAN	NAT, Routage classique	
Affectation d'adresses IPS	DHCP, affectation d'adresses IP fixe, PPPoE, PPTP	
Mode NAT	1-1 NAT, PAT	
Routage	Statique, Dynamique, RIPv1, RIPv2	
VoIP	SIP ALG	
DDNS	DynDNS.org TZO.com, Oray.net	
Fonctions du Firewall	Port Forwarding et triggering, proxy DNS, Cloning/spoofing adresses MAC, Support NTP, outils de diagnostic (Ping, DNS, lookup, trace route et autres), Auto-Uplink sur les ports du switch, QoS niveau 3, LAN-to-WAN et WAN-to-LAN (ToS)	
DHCP	Serveur DHCP, relais DHCP	
Authentification utilisateur	Active directory, LDAP, Radius, Local User Database	
Compatibilité PCI support d'authentification à deux facteurs	•	•
VPN		
Tunnels site à site	10	25
Accès Distant VPN SSL	5	13
Algorithme de cryptage IPsec	DES, 3DES, AES (128, 192, 256 bit)	
Algorithme d'authentification IPsec	SHA-1, MD5	
Echange de clés	IKE, Clé manuelle, Clé partagée, PKI, X.500	
Traversée NAT IPsec	•	•
Support SSL	SSLv3, TLS1.0	
Support de cryptage SSL	DES, 3DES, ARC4, AES (128, 256 bit)	
Intégrité des messages SSL	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1	
Prise en charge des certificats SSL	RSA, Diffie-Hellman, Self	
Plateforme SSL VPN supportées	Windows 2000 / XP / Vista, Mac OS X 10.4 +	
MISE EN PLACE		
Support VLAN	•	•
Double WAN		•
Equilibrage intelligent de la charge de trafic par décompte des octets	•	•
Configuration	Setup, VPN IPsec, VPN SSL	
LOGGING ET REPORTING		
Management	HTTP/HTTPS, SNMP v2c	
Reporting	Statistiques résumées, rapports graphiques, alerte automatique en cas d'attaque, notification automatique de malware, alertes système	

MODELES	UTM10	UTM25
Logging	Trafic, Malware, Spam, Filtrage de contenu, Filtre Email, Système, Service, IPS, Port Scan, messageries instantanées, P2P, Firewall, VPN IPsec, VPN SSL	
Génération de journaux	Management requête GUI, Emails, Syslog	
SPECIFICATIONS MATERIEL		
Port WAN Gigabit RJ-45	1	2
Port LAN Gigabit RJ-45	4	4
Interface DMZ	1	1
Administration par Port console	RS232	RS232
Ports USB	1	1
Conformité aux principales réglementations applicables	FCC Class A, CE, WEEE, RoHS	
Température de stockage et fonctionnement	Température de fonctionnement : de 0 à 45° C Température de stockage : de -20 à 70° C	
Humidité	Fonctionnement : 90% hors condensation, Stockage : 95% hors condensation	
Spécifications électriques	100-240V, AC/50-60Hz, Entée universelle, 1.2A max	
Dimensions (W x H x D) cm	33 x 4.3 x 20.9	33 x 4.3 x 20.9
Dimensions (W x H x D) pouces	13 x 1.7 x 8.2	13 x 1.7 x 8.2
Poids (kg)	2.1	2.1
Poids (lb)	4.6	4.6
Contenu	Appliance Prosecure (UTM10 ou UTM25), Câble Ethernet, Câble d'alimentation, Patins anti-dérapants, Carte de garantie, Guide d'installation rapide, Carte de souscription (uniquement pour les bundles)	
Garantie	2 ans	
REFERENCE LOCALE		
Matériel (Fonctionnalités Firewall et VPN uniquement)		
Amérique du nord	Europe	Asie
UTM10-100NAS	UTM10-100EUS	UTM10-100AJS
UTM25-100NAS	UTM25-100EUS	UTM25-100AJS
Bundle (matériel incluant 1 an service web, 1 an service Email, 1 an logiciel de maintenance et mise à jour, Support 24 x 7 et remplacement avancé)		
Amérique du nord	Europe	Asie
UTM10EW-100NAS	UTM10EW-100EUS	UTM10EW-100AJS
UTM25EW-100NAS	UTM25EW-100EUS	UTM25EW-100AJS
1 an de souscription		
Gestion des menaces web	Gestion des menaces Emails	Logiciel de maintenance et de mise à jour, support 24 x 7, remplacement avancé
UTM10W-1000S	UTM10E-1000S	UTM10M-1000S
UTM25W-1000S	UTM25E-1000S	UTM25M-1000S
3 ans de souscription		
Gestion des menaces web	Gestion des menaces Emails	Logiciel de maintenance et de mise à jour, support 24 x 7, remplacement avancé
UTM10W3-1000S	UTM10E3-1000S	UTM10M3-1000S
UTM25W3-1000S	UTM25E3-1000S	UTM25M3-1000S

* disponible sur UTM25

NETGEAR®

2, rue de Marly
78150 LE CHESNAY
Tél : 01 39 23 98 50
Fax : 01 39 43 08 47
www.NETGEAR.fr

© 2009 NETGEAR, Inc. NETGEAR, the NETGEAR logo, Connect with Innovation, Everybody's connecting, the Gear Guy logo, IntelliFi, ProSafe, RangeMax and Smart Wizard are trademarks or registered trademarks of NETGEAR, Inc. in the United States and/or other countries. Microsoft, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.