

Les informations contenues dans ce document représentent la vision actuelle de Panda Software International sur les problématiques qui y sont évoquées à la date de publication. Ce document a un rôle purement informatif. En aucun cas Panda Software International ne saurait donner des garanties, expresses ou implicites, dans ce document. L'utilisateur a l'entière responsabilité du respect de toutes les lois applicables aux droits d'auteur.

Aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système d'archivage, ni transmise sous quelque forme que ce soit (électronique, mécanique, photocopie ou autre) pour une quelconque utilisation, sans l'accord exprès écrit de Panda Software International

Panda Software International est susceptible de détenir des brevets, des brevets logiciels, des marques déposées, des droits d'auteur ou d'autres droits sur la propriété intellectuelle, couvrant les sujets abordés dans ce document. En dehors de tout contrat de licence écrit de Panda Software International, la possession de ce document ne vous donne aucun droit sur ces brevets, marques déposées, droits d'auteur et autre propriété intellectuelle. © 2004 Panda Software International. Tous droits réservés. R20040804







Table des matières

PUBLIC CONCERNE	
STRATÉGIE DE PROTECTION PÉRIPHÉRIQUE POUR L'ENTREPRISE	
La problématique	
VECTEURS D'INFECTION ET DE PROPAGATION DES LOGICIELS MALVEILLANTS	
STRATÉGIE DE PROTECTION PAR NIVEAUX	
PANDA GATEDEFENDER	10
Présentation	10
PANDA GATEDEFENDER : PRINCIPALES FONCTIONNALITÉS	11
PROTECTION COMPLÈTE	11
PERFORMANCES ÉLEVÉES ET TRANSPARENTES POUR LES UTILISATEURS	
MISES À JOUR QUOTIDIENNES ET AUTOMATIQUES	
ADMINISTRATION EN TOUTE SIMPLICITÉ, DU TYPE " CONNECTÉ PUIS OUBLIÉ "	11
Antispam	
FILFRAGE DE CONTENU WEB	
FILTRAGE DE CONTENU	
FAIBLE COÛT DE POSSESSION	
HAUTE ÉVOLUTIVITÉ ET RÉPARTITION DE CHARGE	
RAPPORTS DÉTAILLÉS ET ALERTES PERSONNALISABLES	
PROTECTION DE L'ENTREPRISE PAR NIVEAUX	
INFORMATIONS TECHNIQUES	15
ANALYSE DES PROTOCOLES DE COMMUNICATION	15
SYSTÈME D'EXPLOITATION ET LOGICIEL D'INTERCEPTION	15
ANALYSES ET ACTIONS CONTRE LES VIRUS ET LES LOGICIELS MALVEILLANTS	15
ANALYSES ET ACTIONS CONTRE LE SPAM	15
FILTRAGE DE CONTENU WEB	
FILTRAGE DE CONTENU (CANULARS, NUMÉROTEURS, SPYWARES)	16
PROTECTION CONTRE LES VULNÉRABILITÉS	17
PROTECTION CONTRE LA VULNÉRABILITÉ DES EN-TÊTES MIME	17
PROTECTION CONTRE LES VULNÉRABILITÉS AFFECTANT LE COURRIER ÉLECTRONIQUE	
PROTECTION CONTRE LA VULNÉRABILITÉ IIS 5.0 WEBDAV	
PROTECTION CONTRE SQLSLAMMER ET LES VERS SIMILAIRES	
PROTECTION CONTRE LES FICHIERS À DOUBLE EXTENSION	
SYSTÈMES À TOLÉRANCE DE PANNES	19
WATCHDOG	19 19
MASTER BOOT MANAGER	19
RÉPARTITION DE CHARGE NATIVE	20
DÉTAILS TECHNIQUES DE LA RÉPARTITION DE CHARGE	20
ANALYSE DE LA VITESSE DE TRANSFERT	
ANNEXE A. PANDA SOFTWARE DANS LE MONDE : COORDONNÉES	23
ANNEXE B. GLOSSAIRE.	25
ANNEXE C. ABREVIATIONS ET ACRONYMES	27
AND THE TANK DAVIN OF DEGREE CONTRACT	
INDEX DES TABLEAUX ET DES SCHEMAS	
TABLEAU 1. MATRICE D'INFECTION ET DE PROPAGATION DE MALWARES DANS L'ENTREPRISE	
TABLEAU 2. SÉCURITÉ ANTIVIRUS PAR NIVEAUX	
TABLEAU 3. SOLUTIONS PANDA SOFTWARE POUR LES ENTREPRISES	
Tableau 4. Caractéristiques techniques	
TABLEAU 5. PRINCIPALES FONCTIONNALITÉS ET CARACTÉRISTIQUES	
Tableau 6. Comparatif entre Panda GateDefender et Panda EnterpriSecure Figure 1. protection par niveaux	
FIGURE 2. EXEMPLE DE RÉPARTITION DE CHARGE	



Public concerné

Ce document s'adresse aux personnes en charge de la sécurité informatique dans les petites, moyennes et grandes entreprises :

- Responsables de la sécurité informatique.
- Administrateurs système.
- Administrateurs de la sécurité.
- Directeurs techniques.
- Directeurs informatiques.
- Responsables de la sécurité.
- Responsables de la confidentialité.

Résumé

Des informations récentes révèlent qu'un e-mail sur 204 contient un virus, et que 99 pour cent des virus s'introduisent dans les entreprises via le courrier électronique SMTP ou la navigation Web HTTP.

Et les problèmes ne viennent pas uniquement des virus. En janvier 2003, le ver SQL Slammer a frappé des milliers de serveurs à travers le monde, en exploitant une vulnérabilité de débordement de tampon et en provoquant sur les serveurs SQL des Déni de service qui, selon Computer Economics, ont occasionné des pertes estimées à 705 millions d'euros.

Par ailleurs, la productivité des employés ne cesse de se dégrader, non seulement en raison du temps qu'ils consacrent au classement et à l'élimination des nombreux spams qui arrivent dans leur boîte aux lettres, mais aussi du fait du temps perdu à accéder à du contenu Web inapproprié ou non autorisé, qui pourrait, s'il était diffusé, ternir l'image de marque de l'entreprise.

En raison de la sophistication sans cesse croissante des menaces Internet, Panda Software propose une stratégie de protection par niveaux, dans laquelle la passerelle Internet joue un rôle crucial puisque c'est par ce point stratégique du réseau que transitent les courriers électroniques, tous les types de contenu et... 99 pour cent des virus.

Panda GateDefender est un appareil qui combine des éléments matériels et logiciels particulièrement performants afin d'assurer une protection optimale au niveau de la passerelle Internet. Il décuple et complète la protection contre les logiciels malveillants de votre entreprise tant sur les serveurs que sur les stations de travail, et il est capable d'arrêter les virus, le spam, le contenu indésirable et d'autres menaces Internet.

Stratégie de protection périphérique de l'entreprise

La problématique

Ces dernières années, les points d'entrée utilisés par les virus informatiques ont beaucoup évolué. Alors qu'auparavant, les disquettes et autres supports amovibles constituaient la principale source des infections, Internet est aujourd'hui un canal d'infection incomparable.

En outre, les virus qui arrivent par Internet sont statistiquement les plus rapides et les plus dangereux, et ils disposent souvent de plusieurs méthodes de propagation et d'infection, notamment les « menaces combinées ». Il est donc essentiel d'installer une protection sur les passerelles, car la plupart des virus arrivent via le courrier électronique ou les téléchargements Internet.

Il existe toutefois d'autres points d'entrée et vecteurs de propagation dans un environnement d'entreprise, comme les ordinateurs portables ou les connexions Internet par modem, la messagerie instantanée, le Webmail ou les comptes de messagerie externe POP3. Et à cause de cette multitude de menaces et de points d'entrée sans surveillance, les entreprises continuent à être attaquées, et elles sont maintenant nombreuses à considérer la sécurité des communications Internet comme une priorité stratégique.

Selon Computer Economics, 99% des entreprises interrogées disposent d'une certaine forme de protection antivirus. Pourtant, 76% d'entre elles admettent avoir été infectées par un virus il y a moins d'un an et plus de 50% révèlent avoir subi une attaque virale massive.

Il semblerait que la raison en soit simplement que les antivirus n'offrent pas une protection adéquate. La vérité est toutefois sensiblement différente. Même si 99% des entreprises disposent d'une forme de protection antivirus, elles se trouvent souvent dans au moins un des cas suivants :

- La protection antivirus ne couvre que certaines plates-formes. Les stations de travail et les serveurs sont la plupart du temps protégés, mais les entreprises ne disposent pas toutes d'une protection pour les serveurs de passerelle Internet et de courrier électronique.
- Les paramètres antivirus ne sont souvent pas adaptés aux dernières menaces Internet telles que la désactivation de la protection résidante sur les stations de travail, les versions d'antivirus obsolètes, la faiblesse de la stratégie de mise à jour du fichier des signatures ou encore l'absence de stratégie appropriée de filtrage de contenu sur les passerelles.
- Il existe dans de nombreuses entreprises des groupes d'utilisateurs auxquels aucune stratégie antivirus n'est appliquée, soit parce qu'il s'agit d'utilisateurs distants ou de groupes d'administrateurs, soit simplement parce qu'il n'y a pas de stratégie.

Vecteurs d'infection et de propagation des malwares

Le tableau qui suit montre les différents points d'entrée des virus et des malwares, leurs vecteurs de propagation et la manière dont ils affectent chaque niveau de l'entreprise.

		Matrice d'infection et de propagation de malwares dans l'entreprise							
		Couches réseaux							
Matrice d'infection et propagation		Connexions	Firewalls	Serveurs Web	Passerelles et relais SMTP	Groupware et serveurs de collaboration	Serveurs de fichiers et d'applications	Station	s de travail
		physiques						PC	Portables
Courrier électronique	Virus dans les mails SMTP	2	₽	®	® X	※		® X	®
	Virus dans les comptes POP3	®	⊗ X	*				8 %	©
	Vers de messagerie se répandant grâce au carnet d'adresses d'Outlook et Exchange	®	® X		© X	®		® X	S
	Contenus offensifs (choquants, illicites,)	*	® X	*	⊕ X			€» X	*
	Spam	\$	€> X		® X	※		® X	®
Vulnérabilités	Infections par le biais de failles de sécurité	S	€ ×X	*	⊛ X	*	® X	€> X	*
vuinerabilites	Protection antivirus désactivée ou obsolète	®	® X	©	® X	®	*	₩	©
	Codes malicieux cachés dans les pages Web (Java, Active X,)	*	® X	*				® X	*
Internet	Contenus offensifs (choquants, illicites,)	*	® X	*				® X	®
	Spywares	※	® X	*			• ×	® X	®
	Numéroteurs	\$	® X	®			• ×	® X	®
Ressources partagées	Virus, vers et chevaux de Troie par les ressources partagées du réseau	*	® X	®			® X	® X	S
	Backdoors et autres outils de piratage	*	® X	®	® X	®	* **	® X	®
Périphériques	Supports de stockage externes (disquettes, CD-ROM,)						®	*	®

Tableau 1 - Matrice d'infection et de propagation de malwares dans l'entreprise.

Stratégie de protection par niveaux

La sécurité totale n'existe pas. Toutefois Panda Software s'en approche aussi près que possible en favorisant une stratégie de protection contre les codes malveillants par niveaux.

En protégeant tous les niveaux de l'entreprise – connexion Internet entrante/sortante (routeur), navigation Web (serveur proxy, serveurs Web et de bases de données), passerelles d'e-mails (SMTP), stockage de données (serveurs de bases de données internes), messagerie interne (groupware et collaboration), serveurs de fichiers et utilisateurs (stations de travail et utilisateurs distants) - ainsi que tous les protocoles de communication et d'échange d'informations possibles dans tous les produits, il est possible de tendre vers une protection parfaite.

Ainsi, pour chaque niveau de l'entreprise, Panda propose un produit distinct, spécialement optimisé pour chaque environnement (Panda GateDefender pour la passerelle, ExchangeSecure pour les serveurs de courrier électronique, ClientShield pour les stations de travail, etc.). L'ajout de nouveaux niveaux de protection augmente l'efficacité de la protection antivirus et par conséquent optimise les investissements en sécurité.

Grâce à cette stratégie de sécurité par niveaux, il est extrêmement difficile pour un virus ou un autre code malveillant de pénétrer dans l'entreprise, ce qui réduit les risques d'infection et de propagation. Plus les différents niveaux d'une entreprise sont protégés, plus cette entreprise est proche d'une sécurité parfaite car l'efficacité antivirus y est maximale.



Figure 1. Protection par niveaux

Sécurité antivirus par niveaux					
Niveau antivirus	Action	Couches réseau de l'entreprise	Éléments protégés	Solutions Panda Software	
Trafic Internet entrant / sortant	Bloque les virus avant qu'ils ne pénètrent dans le réseau.	- Firewalls - Routeurs	TCP/IP (SMTP, HTTP, POP3, FTP,)	■ Panda GateDefender ■ Panda CVPSecure ■ Panda ISASecure	
Navigation Web	Bloque les virus dissimulés dans des pages Web.	- Serveurs Proxy http	Fichiers, Java Script, ActiveX	Panda GateDefender Panda ProxySecure Panda ISASecure	
Passerelles de courrier électronique	Empèche les virus dissimulés dans les e-mails de pénétrer dans le réseau par Internet.	- Passerelles et relais SMTP - Message Transfer Agents	SMTP	Panda SendmailSecure Panda OmailSecure Panda PostixSecure Panda ContinandlineSecure Panda ExchangeSecure Panda EmolinoSecure Panda DominoSecure Panda Antivirus Integration Kit (API)	
Serveurs Web et de bases de données	Bloque l'infection des serveurs Web et empêche les virus de se propager vers les utilisateurs et les clients.	- Windows IIS Server - MS SQL Server	SMTP	■ Panda FileSecure ■ Panda FileSecure avec les Technologies TruPrevent	
Messagerie interne	Empêche les virus de se propager dans le réseau interne, dissimulés dans des messages, des tâches, des dossiers publics, etc.	- Serveurs de messagerie - Serveurs Groupware	MAPI, IMAP, SMTP	■ Panda ExchangeSecure ■ Panda DominoSecure	
Serveurs de fichiers	Empêche les virus de se propager dans le réseau interne, dissimulés dans des documents, des fichiers, des programmes, etc.	- Serveurs de fichiers - Réseaux de stockage (SAN)	Fichiers et partages réseau, NetBIOS, SPX	Panda FileSecure Panda FileSecure avec les Technologies TruPrevent Panda Antivirus Integration Kit (API) Panda CommandlineSecure	
Protection des utilisateurs en réseau	Empêche les infections des utilisateurs de postes de travail en réseau.	- Postes de travail en réseau - Clients légers - Windows 9x,NT,XP,2000	Fichiers, protocoles, Webmail, POP3, MAP1, messagerie instantanée, CD & disquettes	Panda WebAdmin Antivirus Panda ClientShield Panda ClientShield avec les Technologies TruPrevent Panda Platinum Internet Security 2005 Panda ActiveScan Pro Panda ActiveScan	
Protection des utilisateurs distants	Empèche les infections à partir de l'extérieur et renforce la protection des autres couches réseau.	- Ordinateurs portables - PDA et mobiles - PC domestiques	Fichiers, protocoles, Webmail, POP3, IM, CD & disquettes	WebAdmin Antivirus Panda Platinum Internet Security 2005 Panda Titanium Antivirus 2005 Panda ActiveScan Pro Panda ActiveScan	

Tableau 2 - Sécurité antivirus par niveaux

La stratégie de protection par utilisateurs

Le tableau suivant montre les différentes solutions antivirus recommandées pour chaque niveau et chaque type d'utilisateur. Chaque solution possède les fonctionnalités spécifiques que doivent posséder les produits contre les virus et les codes malveillants pour protéger les protocoles de communication, les performances et les caractéristiques fonctionnelles de chaque niveau.

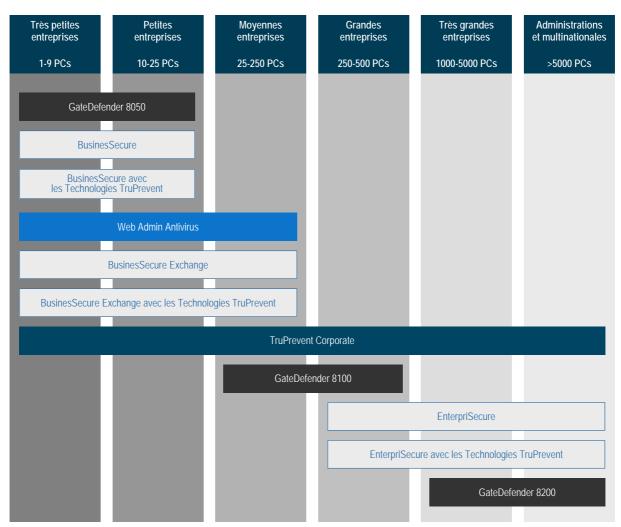


Tableau 3 - Solutions Panda Software pour les entreprises

Panda GateDefender

Présentation

Panda GateDefender est un appliance haute performance qui combine hardware et software pour fournir une protection maximale au niveau de votre passerelle Internet. Cette solution complète votre protection d'entreprise, en empêchant la plupart des menaces d'Internet (virus, vers, chevaux de Troie, spam et les contenus indésirables) de se répandre à travers votre réseau.

La combinaison de hardware et de software permet à cette solution, d'offrir des performances optimales. Comme il est installé à la périphérie du réseau, il protège la passerelle Internet, en réduisant considérablement les risques de sécurité et la charge de travail des ordinateurs.

Il offre une protection de la passerelle conçu pour s'intégrer simplement dans tous les réseaux d'entreprises, sans dégrader les performances et la productivité et sans affecter les autres systèmes critiques, tels que les firewalls, les applications, les serveurs Web, ...

Panda GateDefender est disponible en trois modèles, disposant d'une répartition de charge native et offrant une évolutivité maximale pour s'adapter aux besoins des entreprises de toutes tailles, jusqu'à 40.000 stations de travail.

	Panda GateDefender 8050	Panda GateDefender 8100	Panda GateDefender 8200	
Entreprises cibles	Jusqu'à 25 utilisateurs	De 25 à 500 utilisateurs	Plus de 500 utilisateurs	
Caractéristiques processeurs	Intel® Pentium™ IV Processor	Intel® Pentium™ IV Processor	Dual AMD® Opteron™ Processors AMD Opteron	
Répartition de charge native	Oui	Oui	Oui	
OS intégré	Linux	Linux	Linux	
E-mails analysés par heure	120,000	300,000	600,000	
Interface Ethernet	10/100	10/100/1000 Gibabit	10/100/1000 Gibabit	

Tableau 4 - Caractéristiques techniques

Les principaux avantages des nouveaux Panda GateDefender sont son efficacité, ses multiples fonctionnalités, sa facilité d'utilisation et d'installation (connecté puis oublié), ses hautes performances et sa répartition de charge.



Panda GateDefender: principales fonctionnalités

Protection complète

Panda GateDefender analyse les six protocoles les plus utilisés: HTTP, FTP, SMTP, POP3, IMAP4, et NNTP.

Performances élevées et transparentes pour les utilisateurs

Panda GateDefender réduit considérablement la charge de travail des antivirus traditionnels de votre réseau, à la fois sur les stations de travail et sur les serveurs, optimisant ainsi l'utilisation des ressources réseau.

Il garantit des performances remarquables et la capacité d'analyse la plus élevée de sa catégorie. Il peut analyser jusqu'à 600 000 messages par heure (trafic SMTP) et 30 Mo par seconde (trafic HTTP) d'une manière totalement transparente pour les utilisateurs d'un réseau d'entreprise.

Mises à jour quotidiennes et automatiques

Le fichier des signatures de virus et de spam est automatiquement mis à jour toutes les deux heures et le moteur d'analyse est mis à jour toutes les douze heures. Ainsi actualisé en permanence, Panda GateDefender constituera le fer de lance de la protection de votre réseau

Administration en toute simplicité, du type « Connecté puis oublié »

Cette solution est conçue pour s'intégrer en toute simplicité à n'importe quel réseau d'entreprise, sans nécessiter de reconfiguration du trafic réseau. GateDefender envoie des informations préventives aux administrateurs. Il est géré à distance d'une manière sécurisée, grâce à une console Web simple et intuitive.

Antispam

GateDefender contrôle tous les courriers électroniques reçus par l'entreprise, au moyen de son module antispam. Les messages sont analysés et classés comme spam ou non spam, ce qui permet de bloquer les messages non sollicités avant qu'ils n'atteignent les boîtes aux lettres des utilisateurs ou de modifier leur objet. Il en résulte une réduction considérable de la répercussion du spam sur la productivité.

Filtrage du contenu Web

Le module de filtrage du contenu Web permet aux administrateurs de restreindre l'accès à Internet. Les administrateurs peuvent définir des catégories de contenu indésirable et des listes de pages Web autorisées et proscrites. Ils sont ainsi en mesure de contrôler les ressources du réseau et d'empêcher l'entrée d'un contenu Web choquant, violent ou à caractère pornographique, ou encore d'un contenu tout simplement indésirable dans l'entreprise. Des listes d'utilisateurs auxquels ce contrôle ne s'appliquera pas peuvent être définies.

Filtrage de contenu

Son filtrage de contenu empêche les virus et les vers de pénétrer au sein du réseau de l'entreprise. Ce système réduit la consommation de la bande passante et permet une optimisation de l'utilisation des ressources en faisant face aux dangers potentiels avant qu'ils n'atteignent le réseau : les numéroteurs, les jokes, les spywares, etc.

Faible coût de possession

En évitant la saturation des ressources du réseau et la baisse de productivité, **Panda GateDefender** offre des capacités de gestion plus élevées. Tout ceci, ajouté à sa conception 'installez-le et oubliez-le', à son besoin minimum d'interventions de l'administrateur, fait que le coût de possession de **Panda GateDefender** est extrêmement faible.

Haute évolutivité et répartition de charge

Grâce à sa haute évolutivité, **Panda GateDefender** s'adapte parfaitement aux besoins des PME et des grandes entreprises, jusqu'à 40 000 postes de travail, en ajustant ses capacités d'analyse au volume global du trafic réseau.

Sa répartition de charge est native et complètement automatique, permettant ainsi le partage de la charge de travail entre différentes unités. Il en résulte une évolutivité augmentée et des performances antivirus améliorées pour une protection complète de la périphérie du réseau.

Rapports détaillés et alertes personnalisables

L'administrateur peut contrôler, en temps réel, le trafic du réseau et les statistiques d'activité de la protection antivirus. **Panda GateDefender** délivre des rapports complets sur les virus, le spam et le filtrage de contenu, ainsi que des alertes personnalisables et des notifications.

Comparatif entre les différents boîtiers

	Panda GateDefender 8050	Panda GateDefender 8100	Panda GateDefender 8200
ANTIVIRUS			
Protocoles scannés par l'antivirus	SMTP, HTTP (y	compris Java et Active X), POP3,	FTP, IMAP4 et NNTP.
ANTISPAM			
Protocoles scannés		SMTP, POP3 et IMAP4	
Type de filtre		Bayésien	
Whitelist et Blacklist	✓	✓	✓
Actions effectuées avec le spam		Blocage, redirection et marqua	ge
FILTRAGE DE CONTENU			
URL par catégories	✓	✓	✓
URL par Whitelist et Blacklist	✓	✓	✓
Exclusion d'utilisateurs du filtrage de contenu	√	✓	✓
Filtrage de contenu par extension	✓	✓	✓
Filtrage des vulnérabilités Outlook, IIS et SQL Slammer	✓	✓	✓
Filtrage des spywares, numéroteurs et plaisanteries	✓	✓	✓
CARACTERISTIQUES SYSTEME			
Passerelle transparente	✓	✓	✓
Répartition de charge native	✓	✓	✓
Système de tolérance de panne logicielle	✓	✓	✓
Système de tolérance de panne matérielle (WatchDog)	√	✓	✓
Performance (messages analysés par heure)	120,000	300,000	600,000
Aucune nécessité de rediriger le trafic réseau.	✓	✓	✓
Capacité d'analyse	5 Mbps	14 Mbps	30 Mbps
MISE A JOUR DU FICHIER DE SIGNATURES			
Mise à jour du fichier de signatures		Toutes les deux heures	
Mises à jour automatiques	✓ a	ucune intervention utilisateur n'est r	nécessaire
Monitoring en temps réel du processus	✓	✓	✓
ADMINISTRATION ET FONCTIONNALITES			
Console d'administration		Console Web HTTPS	
Affichage des rapports et des compteurs en temps réel	✓	✓	✓
ALERTES ET NOTIFICATIONS			
Virus détectés	✓	✓	✓
Disponibilité des mises à jour	✓	✓	✓
Erreurs de mise à jour	√	✓	✓
Mises à jour effectuées	✓	✓	✓
SUPPORT			
Support technique 24h/24 et 365j/an	✓	✓	✓
Support matériel et logiciel	✓	✓	1
CARACTERISTIQUES TECHNIQUES			
Connexion réseau	10/100 Ethernet, RJ45	Gigabit Ethernet, RJ45	Gigabit Ethernet, RJ4
Boîtier	SuperMicro Minibox	SuperMicro SC512L Medium 1U	SuperMicro SC812L-350C 1U
Dimensions (mm) L x H x P	184 x 80 x 263	425 x 44 x 355	425 x 44 x 652
Certifications		Certifié FCC et CE.	1

Tableau 5 - Principales fonctionnalités et caractéristiques des différents boîtiers

Protection de l'entreprise par niveaux

Panda GateDefender constitue le premier niveau de défense pour l'environnement d'entreprise, car il empêche les vers, virus et chevaux de Troie de s'infiltrer dans le réseau, complétant ainsi à la perfection les autres types de protection en place.

L'antivirus installé sur une station de travail empêche l'action d'un virus qui s'est infiltré dans le réseau de l'entreprise par le biais d'un ordinateur portable doté d'un modem, de supports de stockage externes, du Webmail, de comptes POP3 externes ou d'une messagerie instantanée.

Les solutions d'antivirus de passerelle protègent les flux des serveurs du réseau et empêchent les systèmes de détection de logiciels malveillants des stations de travail d'altérer la productivité de l'entreprise.

Panda GateDefender empêche l'entrée et la sortie des virus, du spam et du contenu indésirable via Internet, filtre le trafic des six protocoles les plus répandus et arrête les attaques telles que SQL Slammer ou les autres exploitations de vulnérabilités non détectées par les antivirus traditionnels. Ce faisant, il consolide la protection existante et libère les autres ordinateurs afin qu'ils puissent affecter pleinement leurs ressources aux fonctions qui sont les leurs. Comme il s'agit d'un système de protection intégré, les paramètres matériels et logiciels sont conçus pour des performances optimales, ce qui limite ainsi au maximum son incidence sur le réseau.

Toutefois, si la protection n'est pas installée sur les autres niveaux réseau et si un virus parvient à s'infiltrer, par exemple via un ordinateur portable, Panda GateDefender pourra seulement empêcher le virus de sortir du réseau. Il préviendra donc les conséquences désastreuses pour la réputation de l'entreprise d'une transmission du virus aux clients et fournisseurs, mais le réseau sera malgré tout infecté. Les stations de travail et les serveurs seront touchés et l'administrateur réseau devra consacrer beaucoup de temps et de ressources à la désinfection des ordinateurs, à la restauration des copies de sauvegarde, à la gestion des incidents, etc.

De même, une entreprise qui ne dispose que d'une protection antivirus sur les stations de travail et les serveurs de fichiers et de messagerie pourra toujours être exposée à des épidémies virales comme LoveLetter, Klez, Nimda et SQL Slammer, susceptibles de bloquer les serveurs, de provoquer des Déni de service ou simplement d'obliger les administrateurs à arrêter les systèmes pour empêcher une infection massive.

Panda GateDefender complète également l'antivirus de firewall, car il permet d'améliorer les performances et empêche les exploitations de vulnérabilités non détectables par les antivirus analysant les flux transitant par le firewall. Panda GateDefender est un serveur dédié optimisé pour les fonctions anti-logiciels malveillants, antispam et filtrage de contenu Web, alors qu'un firewall est un serveur dédié au contrôle d'accès. Cette séparation des rôles est fondamentale pour les principaux serveurs de l'entreprise.

Il est par conséquent réellement nécessaire de rechercher une sécurité parfaite avec une stratégie de protection par niveaux telle que celle fournie par Panda Software. Chaque ajout d'un niveau de protection augmente de façon exponentielle la valeur des solutions installées dans le réseau. La première génération de virus infecteurs de fichiers, de virus d'amorçage, etc., dont le seul moyen de propagation était les disguettes, est depuis longtemps révolue.

Depuis le premier virus de macro apparu en 1995 jusqu'aux premiers virus Internet datant de 1999, ces menaces prolifèrent de plus en plus et ne cessent de gagner en sophistication et en capacité à nuire. Ces dernières années ont marqué l'émergence de vers à propagation rapide qui ont une longueur d'avance sur la protection antivirus classique, car ils utilisent le spam pour se propager et se servent fréquemment du courrier électronique comme seul moyen de transmission. Par ailleurs, l'utilisation de nouvelles applications telles que les programmes de partage de fichiers de poste à poste du type KaZaA ou eMule ou encore les connexions sans fil constituent de nouveaux vecteurs de propagation pour les menaces.

Comparatif entre la protection au niveau de la passerelle et la protection au niveau du réseau		
Fonctionnalité ou caractéristique	Panda GateDefender	EnterpriSecure
Protection de la périphérie au niveau passerelle	✓	✓
Protège n'importe quelle plate-forme et topologie informatique (Unix, Solaris, etc.)	✓	
Sendmail, Qmail, Postfix, ISA, Proxy ou Firewall-1 avec Win32 ou Linux	✓	✓
Sendmail, Qmail, Postfix, ISA, Proxy ou Firewall-1 avec Unix, Solaris, HP-UX ou un autre Unix	✓	
Intégration du logiciel dans la passerelle		✓
Options antivirus avancées nécessaires		✓
Options avancées de filtrage de contenu nécessaires	✓	✓
Protection contre les vulnérabilités IIS, SQL et Outlook	✓	
Entreprise avec du personnel informatique expérimenté	✓	✓
Entreprise sans personnel informatique expérimenté	✓	

Tableau 6 - Comparatif entre Panda GateDefender et Panda EnterpriSecure

Informations techniques

Panda GateDefender est un équipement installé à la périphérie du réseau qui est chargé d'intercepter et d'analyser le trafic entrant et sortant, offrant ainsi une protection complète contre les logiciels malveillants.

Analyse des protocoles de communication

GateDefender intercepte et analyse le trafic HTTP, FTP, SMTP, POP3, IMAP4 et NNTP à la recherche de logiciels malveillants. L'administrateur peut activer ou désactiver l'analyse de chacun d'eux.

Afin d'intercepter et de filtrer le trafic propre à chaque protocole, le système utilisera par défaut les ports standard suivants :

- Accès Internet (HTTP) : 80
- Transfert de fichiers (FTP) : 21
- Courrier électronique (SMTP) : 25
- Courriers électroniques à télécharger (POP3) : 110
- Courriers électroniques à télécharger (IMAP4) : 143
- Accès aux news (NNTP) : 119

L'utilisateur peut modifier ces ports ou entrer des ports supplémentaires pour chaque protocole à partir de la console d'administration. Les ports utilisés seront à la fois les ports standard et les ports supplémentaires spécifiés par l'utilisateur.

Système d'exploitation et logiciel d'interception

Le logiciel incorporé dans GateDefender repose sur le système d'exploitation Linux, qui a été renforcé et optimisé afin d'offrir une sécurité maximale et des performances élevées. Le système d'exploitation GateDefender inclut uniquement les services et processus dont il a besoin pour fonctionner correctement.

Panda GateDefender agit comme un pont transparent entre Internet et le réseau de l'entreprise. Cela signifie que le trafic le traverse de manière transparente et que l'appareil intercepte les protocoles que sa configuration lui impose d'analyser.

Analyses et actions contre les virus et les logiciels malveillants

Les actions suivantes peuvent être entreprises en cas de détection d'un virus, d'un ver ou d'un cheval de Troie :

GateDefender nettoie tous les fichiers infectés pour tous les protocoles analysés.

Dans SMTP, POP3, IMAP4 et NNTP, la pièce jointe infectée est nettoyée. Si le fichier ne peut pas être désinfecté, il est supprimé. Il est possible de bloquer les messages contenant des pièces jointes infectées et non pas seulement le fichier joint, afin que le message ne parvienne pas au destinataire (pour les analyses SMTP).

Dans le cas des protocoles HTTP et FTP, le contenu est bloqué et ne parviendra donc pas au destinataire.

Dans le cadre de l'analyse du courrier électronique, GateDefender est également en mesure de détecter les virus envoyés en masse, capables de bloquer des serveurs de messagerie et de dégrader sensiblement les performances du réseau. Ce type de ver sera automatiquement supprimé, quelle que soit la manière dont GateDefender est paramétré.

Analyses et actions contre le spam

Panda GateDefender complète l'analyse contre les logiciels malveillants par une protection antispam contrôlant le courrier qui sort de l'entreprise, ce qui limite les répercussions du spam sur la productivité.

L'analyse antispam peut être activée pour les protocoles SMTP, POP3 et IMAP4. L'appareil appliquera cette analyse au courrier entrant par le biais de chacun de ces protocoles.

Pour déterminer si un message est un spam, il analyse le corps et les en-têtes du message en question, dans tous les formats (texte, html). Après cette action, le système détermine la probabilité que le message soit un spam et il le classe en tant que tel ou comme « Non spam ».

Les actions à entreprendre peuvent être configurées en fonction du classement en tant que spam ou non spam du message. L'utilisateur a le choix entre marquer l'objet au moyen d'un indicateur, rediriger le message vers une adresse e-mail ou bloquer le message. Afin d'affiner l'analyse, le module antispam comporte une fonction d'auto-apprentissage.

Des listes blanches et des listes noires d'adresses peuvent également être générées et servir à exclure un message de l'analyse ou à le classer en tant que spam en fonction de l'adresse de l'expéditeur.

Filtrage du contenu Web

Le module de filtrage du contenu Web permet aux administrateurs réseau de contrôler les ressources du réseau et d'empêcher l'entrée dans l'entreprise d'un contenu Web choquant, violent ou à caractère sexuel, susceptible d'une part de dégrader l'environnement de travail et la productivité, et d'autre part de compromettre l'image de marque de l'entreprise s'il est transmis ou reproduit par les employés.

Le module analyse les URL ayant fait l'objet d'un accès HTTP, bloque celles configurées comme non autorisées et informe en outre l'administrateur de tout contenu auquel les utilisateurs accèdent. Les critères de filtrage reposent sur des catégories de contenu prédéfinies ainsi que sur des listes blanches (autorisées) et des listes noires (proscrites) définies par l'administrateur. GateDefender autorise la création d'une liste d'utilisateurs « VIP » auxquels les critères de filtrage du contenu Web ne s'appliqueront pas.

Filtrage du contenu

Le module contre les logiciels malveillants inclus dans Panda GateDefender est en mesure de détecter et d'éliminer d'autres contenus malveillants ou indésirables. Ces contenus peuvent être classés comme suit :

Protection contre les canulars

La diffusion des canulars est relativement récente. Il s'agit d'applications qui s'installent automatiquement sur les ordinateurs à l'insu de l'utilisateur et affectent la productivité. Lorsque cette protection est activée, GateDefender analyse tous les protocoles activés dans la protection antivirus à la recherche de canulars. Tout canular détecté est supprimé, dans la mesure où une désinfection est impossible puisqu'il ne s'agit pas d'un virus infectant des fichiers. Qui plus est, lorsqu'un canular est détecté dans un courrier électronique, GateDefender insère une alerte.

Protection contre les numéroteurs

Tout comme les canulars, les numéroteurs s'installent sur les ordinateurs à l'insu de l'utilisateur, et ils sont souvent employés pour rediriger de façon malveillante les connexions Internet. Lorsque cette protection est activée, GateDefender analyse tous les protocoles activés dans la protection antivirus à la recherche de numéroteurs. Tout numéroteur détecté est supprimé, dans la mesure où une désinfection est impossible puisqu'il ne s'agit pas d'un virus infectant des fichiers. Qui plus est, lorsqu'un numéroteur est détecté dans un courrier électronique, GateDefender insère une alerte.

Protection contre les logiciels espions

Enfin, tous les protocoles activés dans la protection antivirus sont analysés à la recherche de logiciels espions (programmes qui s'installent automatiquement avec un autre programme et sont chargés de collecter des informations à caractère personnel). Lorsqu'un logiciel espion est détecté, il est supprimé ou bloqué dans la mesure où une désinfection est impossible puisqu'il s'agit de programmes et non de fichiers infectés. Comme pour les canulars, les numéroteurs et les logiciels espions, Panda GateDefender est capable de bloquer les tentatives d'exploitation des vulnérabilités susceptibles d'affecter différents composants de l'organisation.

Protection contre les vulnérabilités

Comme mentionné précédemment, Panda GateDefender empêche les virus d'entrer ou de sortir de l'entreprise. Panda GateDefender protège également contre toute tentative d'exploitation de plusieurs vulnérabilités affectant différents composants de l'entreprise.

Protection contre la vulnérabilité des en-têtes MIME

La vulnérabilité Incorrect MIME Header (En-tête MIME incorrect), qui affecte les versions 5.01 et 5.5 d'Outlook et d'Outlook Express, permet d'exécuter le contenu d'une pièce jointe simplement lorsque les utilisateurs lisent l'e-mail (même sans ouvrir la pièce jointe). Le contenu de ce fichier peut être un virus, un ver, un cheval de Troie, etc.

MIME est un protocole pour l'envoi et la réception de contenus complexes (programmes exécutables, fichiers sons, images, etc.). MIME classifie le contenu des messages selon leur type et ajoute deux balises : MIME-Version et Content-type. Cette dernière spécifie le groupe de classification pour le code contenu dans le message.

La modification de ces balises peut conduire Internet Explorer à croire qu'il a affaire à un fichier son ou un fichier image, alors qu'il s'agit en réalité d'un exécutable. Klez, Bugbear.B, Nimda, Badtrans ou Frethem sont quelques-uns des virus qui tentent d'exploiter cette vulnérabilité.

Panda GateDefender est capable de détecter si l'en-tête de l'e-mail a été altéré pour exploiter cette vulnérabilité, en détectant si le type MIME ne correspond pas à l'extension du fichier. De cette manière, même si le lecteur d'e-mails est sujet à la vulnérabilité, le fichier joint ne pourra pas être exécuté automatiquement.

Protection contre les vulnérabilités affectant le courrier électronique

Panda GateDefender protège également contre les autres vulnérabilités affectant le courrier électronique, susceptibles d'affecter les systèmes, comme :

- Vulnérabilité de pièce jointe VBS : cette vulnérabilité permet d'exécuter du code VBS dans l'e-mail lors de l'interprétation du code HTML. Grâce à ses fonctions de filtrage, Panda Antivirus GateDefender est capable de bloquer les fichiers potentiellement dangereux, y compris ceux d'extension VBS.
- Vulnérabilité d'extension CLSID: permet de masquer l'extension réelle d'un fichier joint. Panda Antivirus GateDefender bloque les fichiers d'extensions CLSID.
- Vulnérabilité d'extension de fichier mal formée : les en-têtes MIME fournissent des informations comme l'objet, la date ou le nom du fichier. Par le passé, Outlook Express s'est avéré être vulnérable aux débordements de tampons par l'intermédiaire des champs date et nom de fichier. En utilisant une chaîne spéciale trop longue, un pirate expert peut exécuter du code sur les machines attaquées. Ces vulnérabilités sont quelquefois exploitées pour pénétrer des réseaux distants ou introduire des virus ou des vers. Pour éviter les attaques exploitant ce type de vulnérabilité, Panda Antivirus GateDefender bloque les fichiers dont les noms se terminent par un point (.).

Protection contre la vulnérabilité IIS 5.0 WebDAV

WebDAV (World Wide Web Distributed Authoring and Versioning) est une extension du protocole HTTP version 1.1 qui fournit une norme de modification et d'administration des fichiers entre opérateurs au travers d'Internet. WebDAV est un composant par défaut d'Internet Information Server 5.0 qui permet d'effectuer sur les fichiers des actions comme l'écriture, la copie, la suppression, la modification, etc. au travers d'une connexion HTTP.

Une vulnérabilité a toutefois été découverte, due à l'absence de vérification d'un tampon, qui peut être exploitée à distance au moyen d'une attaque de type déni de service ou pour prendre le contrôle de tout un réseau.

Plus précisément, ce problème peut occasionner un débordement de tampon si des demandes sont envoyées à Internet Information Server avec des en-têtes HTTP incluant une URL de plus de 65 Ko (plus de 50 000 caractères).

Des études récentes ont montré que le composant WebDAV est activé sur environ trois serveurs Microsoft IIS 5.0 sur quatre, ce qui signifie qu'il existe plus de six millions de sites Web vulnérables.

Panda GateDefender effectue ses analyses au niveau TCP/IP en bloquant les fichiers suspects et en empêchant ainsi l'exploitation de cette vulnérabilité. La solution de périphérie de Panda Software a également été conçue pour bloquer les en-têtes HTTP de plus de 40 Ko.

Bien que Panda GateDefender protège les entreprises contre ce type de vulnérabilité, il est toujours conseillé d'installer le correctif publié par Microsoft pour résoudre le problème dans IIS 5.0.

Protection contre SQLSlammer et les vers similaires

En janvier 2003, le ver SQLSlammer a frappé des milliers de serveurs SQL à travers le monde en exploitant une vulnérabilité de débordement de tampon dans ces serveurs et en causant des pertes estimées par *Computer Economics* à 705 millions d'euros.

SQLSlammer a été conçu pour lancer des attaques de type déni de service contre les serveurs d'entreprise par un envoi en masse sur le port 1434 de paquets contenant ce ver. Sa fonctionnalité et ses caractéristiques sont similaires à celles de Code Red, un ver qui exploitait la vulnérabilité .ida des serveurs IIS et pouvait se propager rapidement sans laisser de trace sur les périphériques de stockage traditionnels.

Panda GateDefender effectue ses analyses au niveau TCP/IP, en bloquant les paquets qui tentent d'exploiter les vulnérabilités connues des serveurs SQL. Il empêche réellement d'exploiter deux vulnérabilités de débordement de tampon et une vulnérabilité de déni de service décrites par Microsoft dans ses bulletins de sécurité. Il peut ainsi bloquer toute attaque de type SQLSlammer.

Même si Panda GateDefender protège en temps réel et de façon transparente contre SQLSlammer, il est toujours conseillé d'installer le correctif fourni par Microsoft pour corriger cette vulnérabilité des serveurs SQL.

Protection contre les fichiers à double extension

De nombreux virus, vers ou chevaux de Troie (Klez.I, Bugbear.B, etc.) utilisent des extensions doubles pour traverser les lecteurs d'emails sans se faire remarquer et se propager car ces lecteurs ne présentent souvent au plus qu'une extension de pièces jointes.

Panda GateDefender protège les entreprises contre ce problème en bloquant automatiquement tous les fichiers à plusieurs extensions.

Même si cela offre une sécurité supplémentaire pour l'entreprise, l'option peut être désactivée en cochant 'Don't scan files with the following extensions' (Ne pas analyser les fichiers d'extensions suivantes) sur la console d'administration de Panda GateDefender.

Par exemple, si vous ne voulez pas que le fichier REPORT.V3.DOC.TXT soit analysé, vous pouvez exclure tous les fichiers TXT des analyses de Panda GateDefender.

Système à tolérance de panne

Panda GateDefender, conçu pour être simplement connecté puis oublié, dispose aussi d'une série d'outils de réparation automatique comme WatchDog ou Master Boot Manager, qui évitent les longues périodes d'indisponibilité des connexions réseau.

La tolérance de pannes consiste généralement à créer des 'sous-systèmes' en utilisant une capacité redondante qui peut être exploitée en parallèle. Dans ce contexte, la tolérance de pannes peut être définie comme la création d'un système de sauvegarde pour garantir la continuité du service.

Panda GateDefender dispose de plusieurs systèmes de tolérance de pannes pour garantir la disponibilité de l'antivirus de périphérie. Ces systèmes ont pour but de restaurer un fonctionnement correct en cas de défaillance d'un des composants suivants :

- Matériel : altération de l'enregistrement d'amorçage maître (Master Boot Record) ou du disque dur.
- Antivirus : défaut de service du moteur d'analyse antivirus.
- Interception de protocole : défaillance du service d'interception des paquets TCP/IP.
- Système d'exploitation : défaillance du système d'exploitation.

Les principaux systèmes de tolérance de pannes sont WatchDog et le Master Boot Manager.

WatchDog

Le système WatchDog est installé sur la carte mère de Panda Antivirus GateDefender. Il s'agit d'un circuit de surveillance de système.

Sa fonctionnalité est simple. WatchDog vérifie l'état des appareils Panda Antivirus GateDefender toutes les 10 secondes. S'il n'obtient pas de réponse, il réinitialise totalement le système à partir de la carte mère.

Grâce à son système de tolérance de pannes, Panda Antivirus GateDefender est capable de restaurer automatiquement un fonctionnement correct en cas de défauts de service dans les applications ou le système d'exploitation.

Master Boot Manager

Dans des circonstances extrêmes (chaleur excessive, etc.), il est possible que le matériel de Panda GateDefender subisse des dommages, comme des altérations du disque dur ou de l'enregistrement d'amorçage maître.

Pour empêcher les défaillances système dans ces situations et garantir la continuité des services antivirus de périphérie, Panda GateDefender inclut un Master Boot Manager avec un code assembleur destiné à permettre au système d'exploitation de se restaurer automatiquement.

Le système Master Boot Manager se trouve au début du disque dur. Différentes copies cachées de la partition principale sont également stockées physiquement après cette partition.

Au démarrage de Panda GateDefender, le système Master Boot Manager détecte la partition qu'il devra utiliser pour démarrer le système en fonction des résultats du démarrage précédent.

Si le Master Boot Manager détecte une défaillance quelconque de la partition principale, il utilisera l'une des copies existantes pour restaurer la partition endommagée et démarrer le système à partir d'une partition saine.

Le Master Boot Manager nettoiera en même temps les partitions endommagées pour garantir qu'elles fonctionneront correctement lors des démarrages ultérieurs.

REMARQUE: il existe d'autres solutions de périphérie qui offrent une disponibilité élevée au moyen de disques RAID SCSI. Panda Software estime que les disques RAID SCSI ne sont vraiment nécessaires que pour les serveurs de stockage qui doivent protéger des données et offrir une disponibilité élevée. Ils n'offrent par contre aucun avantage pour les appareils qui ne sont pas destinés à stocker des données, comme Panda GateDefender ou d'autres appareils du marché. Il s'agit en réalité d'un simple aspect marketing qui n'a pas d'autre effet que d'augmenter le coût pour l'utilisateur final, et Panda Software a préféré éliminer les coûts inutiles. Panda GateDefender offre une disponibilité élevée au moyen d'outils comme WatchDog et Master Boot Manager, ainsi que grâce à la répartition de charge.

Répartition de charge native

Un autre aspect important de la disponibilité élevée d'un appliance de sécurité périmètrique est l'évolutivité de son débit d'analyse.

Lors de la mise en oeuvre de systèmes ou de services à haute disponibilité, les entreprises ne doivent pas considérer l'utilisation moyenne de la bande passante mais les pics de trafic, car c'est pendant ces périodes critiques que les systèmes sont le plus exposés aux surcharges, aux défaillances et aux blocages.

Panda GateDefender a été conçu pour être évolutif en matière d'analyse de volumes de trafic importants car il dispose d'un système de répartition de charge natif.

De même, si l'un des appareils cesse de fonctionner, les autres prennent automatiquement le relais en quelques secondes.

Cette fonction de répartition de charge est importante pour l'écoulement du trafic réseau. Si le ralentissement des communications occasionné par Panda GateDefender est déjà minimal (autour de 3%), la répartition de charge de cette solution augmente la vitesse et le débit de l'analyse et des communications.

Détails techniques de la répartition de charge

La répartition de charge démarre automatiquement dès que plusieurs appareils Panda GateDefender sont installés dans un même segment du réseau. Les deux appareils doivent pouvoir 'se voir l'un l'autre', c'est-à-dire se trouver entre deux concentrateurs dans le même segment, comme illustré dans la diagramme suivant :

Lorsque plusieurs appareils d'un segment de réseau doivent effectuer une répartition de charge, l'un d'eux est identifié comme appareil maître. A partir de ce moment, même si tous les appareils peuvent voir le trafic qui traverse le segment du réseau, les appareils Panda GateDefender utilisent un algorithme de hachage pour déterminer quelles sessions utilisateur chaque appareil devra analyser. Cette décision est uniquement basée sur les adresses IP source et cible de chaque session.



Figure 2. Exemple de répartition de charge

REMAROUE: il est possible de répartir les charges entre plusieurs appareils Panda GateDefender situés entre deux commutateurs au lieu de deux concentrateurs. Les ports des commutateurs doivent alors être configurés pour permettre la communication en mode diffusion sur tous les ports auxquels chaque Panda GateDefender est connecté.

Les appareils de répartition de charge sont en communication constante les uns avec les autres et ils sont automatiquement informés du nombre d'appareils présents et du nombre d'appareils prêts à effectuer la répartition de charge. Si un appareil connaît une défaillance pour quelque raison que ce soit, les autres continueront à répartir le trafic entre eux. Les autres appareils mettent environ 22 secondes à prendre à leur charge le trafic affecté à l'appareil qui a subi une défaillance. Lorsque cet appareil redevient opérationnel, la nouvelle répartition de charge du trafic s'effectue au bout d'environ 12 secondes.

De la même manière, les appareils communiquent fréquemment pour vérifier qu'ils utilisent le même algorithme de hachage et que le trafic est par conséquent bien réparti.

Analyse de la vitesse de transfert

En supposant que les limites réelles des performances Ethernet, compte tenu des collisions, équivalent à peu près à 70% du total théorique, la capacité de transfert maximum de plusieurs appareils de répartition de charge Panda GateDefender entre 2 concentrateurs est de 70 Mbps dans un réseau à 100 Mbps.

La vitesse d'analyse dans un cluster de répartition de charge Panda GateDefender est définie par le calcul qu'effectue chaque nœud pour ignorer les paquets qu'il n'a pas à analyser. Cette limite est donc définie par le nombre de paquets et non par la bande passante de trafic réelle. Par exemple, avec un grand nombre de paquets de petite taille, la capacité d'analyse de Panda GateDefender peut atteindre ses limites, même si les transferts sont réduits et que l'utilisation de la bande passante est faible.

Il existe sur le marché d'autres solutions qui " partagent " les charges au lieu de les répartir. C'est le cas des WebShield e500 et e1000 de NAI. Pour disposer d'une installation évolutive en termes d'analyse de bande passante, un composant supplémentaire est nécessaire afin de répartir la charge entre les différents appareils. La capacité d'analyse de bande passante doit alors être divisée par deux, car le trafic à analyser doit aller et venir entre le composant de répartition de charge et l'appareil.

En termes de performances, Panda GateDefender 8100 est capable d'analyser 22 emails par seconde, en supposant qu'aucun de ces e-mails n'est infecté. Deux appareils Panda GateDefender sont capables d'analyser plus de 35 emails par seconde.

ANXEXES

Annexe A. Panda Software dans le monde

EU Headquarters

Ronda de Poniente 19 - Tres Cantos 28760 Madrid, Spain Tel: +34 91 806 37 00

E-mail: info@pandasoftware.com

Panda Software Argentina

Calle Roque Saenz Peña 1160, piso9b **Buenos Aires**

Tel: +00 5411 43823448

E-mail: argentina@pandasoftware.com

Panda Software Bulgaria

126, Tzar Boriss III Blvd. office 111 1612 – Sofía-Bulgaria Tel: +359 2 9556575

E-mail: bulgaria@pandasoftware.com

Panda Software China

Room 801, Chun Shen Jiang Mansion Shanghai 200001

Tel: +86 21 6351 9020

E-mail: china@pandasoftware.com

Panda Software Denmark

Ny Vestergardsvej 15 DK 3500 - Værløse Tel: +45 44 355 375

E-mail: denmark@pandasoftware.com

Panda Software Germany Dr.-Detlev-Karsten-Rohwedder-Str. 19 47228 Duisburg

Tel: +49 20 65 9 87 654

E-mail: germany@pandasoftware.com

Panda Software Hungary

Szugló utca 54 1145 Budapest Tel: +36 1 469 70 97

E-mail: hungary@pandasoftware.com

Panda Software Italy

Viale E. Marelli 165 20099 Sesto S. Giovanni (Mi) Tel: 02-24 20 22 08

E-mail: italy@pandasoftware.com

USA Headquarters

230 N. Maryland, Suite 303 P.O. Box 10578 Glendale, CA 91209, USA E- mail: usa@pandasoftware.com

Panda Software Belgium

Mechelsesteenweg 311 1800 Vilvoorde Tel: +32 2 756 08 80

E-mail: belgium@pandasoftware.com

Panda Software Canada

1117 Ste Catherine O. Suite 920 Montreal Quebec H3B 1H9 Tel: +1 514 842 2288

E-mail: canada@pandasoftware.com

Panda Software Colombia

Calle 45 FF Nº 77A-44 Medellín

Tel: + 57 4 412 63 53

E-mail: colombia@pandasoftware.com

Panda Software Finland

P.O. BOX 636

33101 Tampere Tel: +358 3 339 26 700

E-mail: finland@pandasoftware.com

Panda Software Greece

Botsari 12-14 18538 Pireaus Tel: +30 1 04531201

E-mail: greece@pandasoftware.com

Panda Software Iran

4th Floor, NO. 57, Khorramshahr P.O. Box: 14335-1353 Tehran Tel: +98 21-873 36 94 E-mail: iran@pandasoftware.com

Panda Software Japan

Nakameguro GT Tower 7F, 2-1-1 Meguro-ku, Tokyo 153-0051 Tel: +81-3-6412-6020

E-mail: japan@pandasoftware.com

Panda Software Bolivia

Calle Miguel de Cervantes Nro. 2725, Sopocachi, La Paz

Tel: +591 2 411823

E-mail: bolivia@pandasoftware.com

Panda Software Chile

Mosqueto 428, oficina 502 6500426, Santiago Tel: +56 2 639 7541

E-mail: chile@pandasoftware.com

Panda Software Costa Rica

Calle 25, Ave 6 y 8 #648 San José

Tel: 00 506 258 0100

E-mail: costarica@pandasoftware.com

Panda Software France

33 bis Boulevard Gambetta. 78300 Poissy

Tel: +33 1 30 06 15 15

E-mail: france@pandasoftware.com

Panda Software Guatemala

Avenida Reforma 8-60 Zona 9 Edificio Galería Reforma, Torre 1 Oficina

Tel: +502 385 6657

E-mail: guatemala@pandasoftware.com

Panda Software Israel

43 Hamelacha street, New Industrial Zone - 42504 Natanya Tel: +972 9 - 8859611

E-mail: israel@pandasoftware.com

Panda Software Latvia Merkela Street 1 1050 Riga

Tel: +371 7211636

E-mail: latvia@pandasoftware.com

Panda Software Lithuania

Žemaites g. 21 LT-2009 Vilnius -Lithuania Tel: +370 5 2397833

E-mail: lithuania@pandasoftware.com

Panda Software Mexico

Tuxpan #39, Despacho 503 06760 México, D.F. Tel: +52 5 2642127

E-mail: mexico@pandasoftware.com

Panda Software Norway

ViroSafe Norge AS - Midtbyen Park - Skolegt. 2 2315 HAMAR

Tel: 00 47 62 53 96 80

E-mail: norway@pandasoftware.com

Panda Software Poland

UI. Wiktorska 63 02-587 Warszawa –Poland Tel: +48 (22) 540 18 06

E-mail: poland@pandasoftware.com

Panda Software Russia

Tveritina 38/3 Ekaterinburg, 620026 Russia Tel: +7 3432 78-31-27

E-mail: russia@pandasoftware.com

Panda Software South Africa

Unit 11a, Midpark Business Village, Cnr Frans Conradie Drive, Parow Capetown

Tel: 00 27 21 595-2394

E-mail: south a frica@pandas of tware.com

Panda Software Thailand

192 Soi Laprao 107 Bangkapi, Bangkok 10240 Tel : 00 662 7311480

E-mail: thail and @pandas of tware.com

Panda Software Uruguay

Jose Enrique Godó 1955 11200 Montevideo Tel: +5982 4020673

E-mail: uruguay@pandasoftware.com

Panda Software Luxembourg

Mechelsesteenweg 311 1800 Vilvoorde Tel: +32 2 756 08 80

E-mail: luxembourg@pandasoftware.com

Panda Software Netherlands

Fellenoord 23 – Postbus 2020 5600 CA Eindhoven Tel: +31 40 233-3501

E-mail: netherlands@pandasoftware.com

Panda Software Paraguay

Eliseo Reclus 247 Calle Guido Spano, República del Paraguay - Asunción Tel: +00 595 21 607594

E-mail: paraguay@pandasoftware.com

Panda Software Portugal

Quinta da francelha - Edificio Sagres, 7B 2685-338 Prior Velho

Tel: + 351 219426800

E-mail: portugal@pandasoftware.com

Panda Software Singapore

10 Ubi Crescent, # 06-71, Ubi Techpark, Singapore 408564. Tel: +65 6749 6836

E-mail: singapore@pandasoftware.com

Panda Software Spain

Ronda de Poniente 19 - Tres Cantos

28760 Madrid

Tel: 902 365 505

E-mail: info@pandasoftware.es

Panda Software Turkey

Darulaceze Cad - Karatas Sok. SNS Plaza Nº 6 80270 OKMEYDANI - ISTANBUL Tel : 90 212 222 1520/90 212 210 2200

E-mail: turkey@pandasoftware.com

Panda Software Venezuela

Av. Libertador, C.C. Libertador, PH-7

Caracas

Tel: +5821 276188 60

E-mail : venezuela@pandasoftware.com

Panda Software Malaysia

6, Jln Pengacara U1/48, Temasya Ind. Park, Shah Alam, 40150 Selangor

Tel: +60 3 7620 6250

E-mail: malaysia@pandasoftware.com

Panda Software Nigeria

5th Floor Eleganza Plaza 15 B Joseph St, Off Broadway Street, Lagos

Tel: +234 1 - 264 7634

E-mail: nigeria@pandasoftware.com

Panda Software Peru

Calle Lord Cochrane 521 Miraflores – Lima 18 - Perú Tel : 00 51 1 221 6001/ 221 0159

E-mail: peru@pandasoftware.com

Panda Software Puerto Rico/Dominican

Av. Luis Muñoz Rivera 1058, Suite 1 Puerto Rico, 00920

Tel: +1 787 296 1139

E-mail: caribe@pandasoftware.com

Panda Software Slovak Republic

Lublanska 1 83102 Bratislava

Tel: +421 2 444 55 702

E-mail: slovakia@pandasoftware.com

Panda Software Sweden

P. O. Box 26026 100 41 Stockholm

Tel: +46 8-545 25030

E-mail: sweden@pandasoftware.com

Panda Software United Kingdom

5 Signet Court, Swanns Road Cambridge CB5 8LA Tel: +44 (0)870 444 5640 E-mail: uk@pandasoftware.com

Annexe B. Glossaire

Antivirus / programme antivirus : Il s'agit de programmes qui analysent la mémoire, les disques durs et d'autres parties d'un ordinateur à la recherche de virus.

Cheval de Troie: Au sens strict du terme, un cheval de Troie n'est pas un virus, bien qu'il soit souvent considéré comme tel. En fait, il s'agit de programmes qui pénètrent sur des ordinateurs en semblant inoffensifs, s'installent et exécutent des actions qui portent atteinte à la confidentialité des informations des utilisateurs. Leur nom provient du fameux cheval en bois dans lequel des Grecs se sont dissimulés pour pénétrer dans la cité de Troie sans être repérés.

Cheval de Troie de type backdoor : Programme qui s'introduit sur un ordinateur et crée une trappe par le biais de laquelle il est possible de contrôler le système affecté, à l'insu de l'utilisateur.

Correctif de sécurité : Ensemble de fichiers supplémentaires appliqués à un logiciel, des outils ou des applications informatiques d'origine afin de résoudre certains problèmes, vulnérabilités ou bogues.

Cryptage: Mécanisme de protection des informations consistant à faire varier le format des données en fonction de certains critères afin d'empêcher les accès non autorisés.

Débordement de tampon (Buffer Overflow) : Vulnérabilité fréquemment utilisée par les pirates informatiques pour attaquer un ordinateur. Cette attaque se sert d'une certaine partie de la mémoire de l'ordinateur pour insérer du code malveillant qui s'exécute et provoque des dommages.

Déni de service (DoS): Il s'agit d'un type d'attaque, parfois causé par des virus, qui empêche les utilisateurs d'accéder à certains services (au niveau du système d'exploitation, de serveurs Web, etc.).

Déni de service distribué (DdoS) : Il s'agit d'une attaque de type déni de service au cours de laquelle plusieurs ordinateurs attaquent simultanément un même serveur.

Exploitation de vulnérabilité : Technique ou programme tirant avantage d'une vulnérabilité ou d'une faille de sécurité au niveau d'un protocole de communication, d'un système d'exploitation ou d'autres utilitaires ou applications informatiques.

Firewall : Il s'agit d'une barrière servant à protéger les informations d'un système ou d'un réseau connecté à un autre réseau, par exemple Internet.

Hoax: Il ne s'agit pas d'un virus, mais d'un message leurre signalant un virus qui en fait n'existe pas.

Hôte: Tout ordinateur faisant office de source d'informations.

IIS (Internet Information Server) : Il s'agit d'un serveur Microsoft (Internet Information Server) conçu pour publier et gérer des pages et portails Web.

IP (Internet Protocol) / TCP/IP : Une adresse IP est un code qui identifie chaque ordinateur. Le protocole TCP/IP est le système utilisé sur Internet pour interconnecter les ordinateurs et empêcher les conflits d'adresses.

Journal : Fragment d'information enregistré lorsqu'un événement se produit. Les journaux sont généralement générés par les systèmes de détection en vue de leur consultation ultérieure.

Navigateur : Un navigateur est un programme qui permet aux utilisateurs de consulter des pages Internet. Les navigateurs les plus courants sont : Internet Explorer, Netscape Navigator, Opera, etc.

Noyau : Il s'agit du cœur (module central) d'un système d'exploitation.

Ordinateur de bureau / station de travail : Ordinateur utilisé par les employés d'une entreprise. Il s'agit généralement d'un ordinateur personnel (PC) connecté à un réseau.

Passerelle: Ordinateur qui permet la communication entre des plates-formes, réseaux, ordinateurs ou programmes de types différents. Pour ce faire, il convertit les différents protocoles de communication qu'il prend en charge.

Pirate informatique : Personne qui accède de manière illégale ou sans autorisation à un ordinateur.

Réseau local (LAN, Local Area Network): Réseau d'ordinateurs interconnectés, généralement circonscrit à une zone géographique relativement restreinte, (généralement dans la même ville, voire le même bâtiment).

Tampon : Il s'agit d'un espace mémoire intermédiaire servant à enregistrer temporairement des informations transférées entre deux unités ou périphériques (ou entre des composants du même système).

Macro: Une macro est une série d'instructions définies de telle sorte qu'un programme (par exemple, Word, Excel, PowerPoint ou Access) effectue certaines opérations. Comme il s'agit de programmes, les macros peuvent être affectées par des virus. Les virus qui utilisent des macros pour infecter un système sont connus sous le nom de virus de macros.

Logiciel malveillant : Programmes, documents ou messages susceptibles d'avoir des effets dommageables sur les systèmes informatiques.

Moyen d'infection : Caractéristique fondamentale d'un virus. Il s'agit de la méthode utilisée par le virus pour infecter un ordinateur.

Moyen de transmission : Caractéristique fondamentale d'un virus. Il s'agit de la méthode utilisée par un virus pour se propager d'un ordinateur à l'autre.

Point à point (P2P, Peer to peer) : Programme ou connexion réseau utilisé(e) pour proposer des services via Internet (généralement partage de fichiers) et que des virus ou d'autres types de menaces peuvent exploiter pour se propager. A titre d'exemple de ce type de programme, citons KaZaA, eMule, eDonkey, etc.

Polymorphe / polymorphisme : Technique employée par les virus leur permettant de crypter leur signature d'une manière différente à chaque fois, voire d'appliquer cette méthode aux instructions d'exécution du cryptage.

POP (Post Office Protocol): Protocole utilisé pour la réception et l'envoi de courriers électroniques.

Port / port de communication : Point par lequel un ordinateur transfère des informations (entrantes / sortantes) via TCP/IP.

Prévention : Aptitude à prévoir les événements, au moyen de toute technique permettant d'agir par anticipation en vue de traiter une difficulté escomptée.

Registre de Windows : Fichier qui stocke toutes les informations de configuration et d'installation concernant les programmes, notamment des informations sur le système d'exploitation Windows.

Signature : Il s'agit en quelque sorte du numéro de passeport du virus. Séquence de caractères (chiffres, lettres, etc.) qui identifie un virus.

Spam : Courrier électronique non sollicité contenant généralement de la publicité. Ces messages, habituellement envoyés en masse, peuvent être extrêmement importuns et entraîner une perte de temps et de ressources.

Ver : Un ver est similaire à un virus, mais en diffère par sa capacité à se dupliquer intégralement ou partiellement.

Virus : Les virus sont des programmes qui peuvent pénétrer sur les ordinateurs ou les systèmes informatiques de différentes façons et dont les effets vont de la simple gêne à la destruction irrémédiable du système.

Virus d'amorçage : Virus qui affecte spécifiquement le secteur d'amorçage des disques durs et des disquettes.

Virus de macro: Virus qui affecte les macros des documents Word, des feuilles de calcul Excel, des présentations PowerPoint, etc.

Virus de script : Le terme script fait référence aux fichiers ou sections de code écrits dans des langages de programmation tels que Visual Basic Script (VBScript), JavaScript, etc.

Vulnérabilité : Failles de sécurité dans un programme ou sur un système informatique, qui sont souvent exploitées par les virus comme moyen d'infection.

Annexe C. Abréviations

CPU: Central Processing Unit (processeur)

CSV: Comma Separated Values

CVP: Content Vectoring Protocol

DMZ: De-Militarized Zone (zone démilitarisée)

DPC: Data Processing Centers (centres de traitement informatique)

FTP: File Transfer Protocol

HTTP: HyperText Transfer Protocol

ICSA: International Computer Security Association

IP: Internet Protocol

ISP: Internet Service Provider (fournisseur d'accès à Internet - FAI)

IT : Information Technology (informatique)

LDAP: Lightweight Directory Access Protocol

MAPI: Messaging Application Programming Interface

MIME: Multipurpose Internet Mail Extensions

MSDE: Microsoft SQL Server Desktop Engine

MTBF: Medium Time Between Failure (temps moyen entre pannes)

POP: Post Office Protocol

SMS: Systems Management Server

SMTP : Simple Mail Transfer Protocol

SQL: Structured Query Language

TCO: Total Cost Ownership (coût total de possession)

TCP: Transmission Control Protocol

USB: Universal Serial Bus

XML: eXtended Markup Language

VPN: Virtual Private Network (réseau privé virtuel)

certifications Panda Software

















Software et le logo Panda Software sont des marques déposées de Panda Software. Tous les autres noms de produit peuvent être des marques déposées urs sociétés respectives. Microsoft, Windows et le logo Windows sont des marques ou des marques déposées de Microsoft Corporation aux USA et/ou dans es pays.

Panda Software France

33 bis, boulevard Gambetta

78300 POISSY

Téléphone: +33 1 30 06 15 15 E-mail : france@pandasoftware.com Web : www.pandasoftware.com/fr

Panda Software Headquarters USA

230 N. Maryland, Suite 303 P.O. Box 10578

Glendale, CA 91209

Phone: +1 (818) 553-0599
E-mail: info.usa@pandasoftware.com
Web: www.pandasoftware.com

Panda Software Headquarters Europe

Ronde de Poniente, 19 28760 Tres Cantos

Madrid - Spain
Phone : +34 91 806 37 00
E-mail : info@pandasoftware.com Web: www.pandas of tware.com

www.pandasoftware.com

