FORTINET

Rapport d'évaluation des cybermenaces

Statistiques essentielles

Ce document présente l'analyse récente de l'infrastructure. Il fournit une synthèse et des recommandations sur les actions de remédiation aux événements. L'analyse porte sur les données, sur la base de ces critères :

Informations entreprise

Nom entreprise: Functest

Localisation: city, BS

Secteur d'activité: Retail/Hospitality

Taille entreprise: 100-249 employees

Détails test

Date début test: Jan 1, 2015

Durée test: 671 jour(s)

Modèle FortiGate: FG-300D

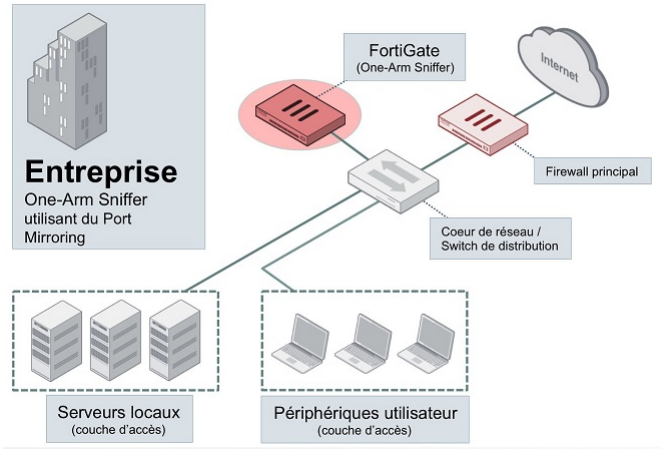
Version FortiOS: FortiOS 5.4.1

Réseau analysé: Network Segment

Fonctions activées: Firewall + Sandbox

Déploiement/méthodologie

Le réseau a été surveillé à l'aide d'une appliance FG-300D en mode One Arm Sniffer interceptant le trafic de façon non intrusive durant le transit sur le réseau.



Lors de l'évaluation, l'activité réseau au sein de l'infrastructure a été surveillée en temps réel. Les logs de trafic enregistrent la plupart des infos de session du réseau, mais FortiGate consigne les activités de prévention des intrusions, d'analyse antivirus, de filtrage URL et contrôle applicatif. S'appuyant sur les données télémétriques des logs, cette évaluation offre un aperçu de l'activité réseau. Avec FortiAnalyzer, FortiGate offre d'autres fonctions : gestion des événements (alertes), analyse FortiView (activité utilisateur), rapports, etc.

Synthèse

Attaques IPS: 12,453
Logiciels malveillants/botnets détectés: 17
Applications à haut risque utilisées: 17
Sites Web malveillants détectés: 125

L'an dernier, plus de 2 100 entreprises ont été victimes de brèches de sécurité en raison de mauvaises pratiques internes et de l'exploitation inadéquate des solutions de sécurité. Dans une entreprise, une brèche de sécurité coûte 3,5 mns de dollars et augmente de 15 % chaque année. Les intrusions, malwares/botnets et programmes malveillants présentent un risque majeur pour le réseau. Grâce à ces mécanismes, les cybercriminels accèdent aux infos critiques des fichiers et bases de données sensibles. FortiGuard Labs neutralise ces attaques grâce aux solutions de sécurité du contenu primées par des organismes comme NSS Labs, VB 100 et AV Comparatives.

Applications détectées: 330
Application la plus utilisée: Zoho
Principale catégorie d'applications: Network.Service
Sites Web visités: 567
Principal site Web: ca.archive.ubuntu.com
Principale catégorie Web: Information Technology

Les habitudes d'utilisation des applications et de navigation révèlent un usage inefficace des ressources, mais indiquent une mauvaise application des règles associées. L'utilisation des ressources à des fins personnelles est tolérée. Il existe cependant de nombreuses zones d'ombre à surveiller, en particulier les applications P2P, le contournement de proxy, les sites Web inappropriés ou de phishing, et les activités illégales. Tout cela engage la responsabilité de l'entreprise et représentent un risque. Avec plus de 5 800 règles de contrôle applicatif et 250 mns de sites Web catégorisés, FortiGuard Labs fournit à FortiOS toutes les données télémétriques nécessaires au bon fonctionnement de l'entreprise.

Bande passante totale: 42.06 GB
Hôte consommant le plus de bande passante: 192.168.1.119
Hôte enregistrant le plus de sessions: 172.18.58.121
Nombre moyen d'événements consignés par seconde: 12.60

Les performances sont sous-estimées. Les Firewalls peuvent prendre en charge les bandes passantes de switchs nouvelle génération. Selon Infonetics, 77 % des décideurs de grandes entreprises jugent devoir améliorer ces performances (débit cumulé > 100 Gbit/s) pour l'an prochain. Le processeur FortiASIC des appliances FortiGate, accélère les fonctions sollicitant fortement l'UC : la transmission de paquets et outils de pattern-matching, des performances 5 à 10 fois supérieures aux concurrents.

Données de référence du secteur

Secteur d'activité: Retail/Hospitality

Retail and hospitality industries are some of the biggest targets for financially motivated cybercrime as they commonly maintain payment processing information. Corporate web portals, Internet-connected point of sale devices, and backend payment databases are common targets for threat actors. High profile breaches within these verticals have led to long-term brand reputation damage for certain organizations, which can be nearly as damaging as the theft of individual records themselves. Smaller franchises and individually operated stores often deprioritize their network security and are underprepared for attackers who gravitate towards the easiest targets (and not necessarily the largest ones).

Dans les tableaux ci-après, le terme « entreprise » fait référence à votre organisation. Cette activité vous donne une idée de votre situation par rapport aux autres organisations de votre secteur spécifique. En prenant pour référence des organisations similaires, certaines entreprises novatrices optimisent continuellement leur réseau afin de mettre en place des pratiques de sécurité « supérieures à la moyenne du secteur ».

Attaques IPS par jour

#	Entité	Nombre
1	Entreprise	19
2	Secteur d'activité	9,097
3	Globalité	15,724

Applications dissimulées par jour

#	Entité	Nombre
1	Entreprise	0
2	Secteur d'activité	2
3	Globalité	3

Principal logiciel malveillant (entreprise)

#	Nom du logiciel malveillant	Type	L'application
1	EICAR_TEST_FILE	Virus	FTP
2	EICAR_TEST_FILE	Virus	HTTP
3	Asprox.Botnet	Botnet C&C	Asprox.Botnet
4	Adware/TEST_FILE	Adware	HTTP
5	ETDB_TEST_FILE	Virus	FTP

Principal logiciel malveillant (secteur d'activité)

#	Nom du logiciel malveillant	Type	L'application
1	Cidox.Botnet	Botnet C&C	Cidox.Botnet
2	Cerber.Botnet	Botnet C&C	Cerber.Botnet
3	Mariposa.Botnet	Botnet C&C	Mariposa.Botnet
4	Conficker.Botnet	Botnet C&C	Conficker.Botnet
5	Conficker	Botnet C&C	Conficker.Botnet

Utilisation des protocoles HTTPS/HTTP

#	Entité	Pourcentage
1	Entreprise	125.85%
2	Secteur d'activité	118%
3	Globalité	99%

Utilisation du cloud (applications IaaS + SaaS)

#	Entité	Nombre
1	Entreprise	83
2	Secteur d'activité	1,379
3	Globalité	35,318

Analyse via Sandbox

Les menaces d'aujourd'hui, de plus en plus sophistiquées, peuvent masquer leur dangerosité et contourner les solutions anti-malware traditionnelles. Ces engins anti-malware conventionnels sont souvent incapables, dans des temps acceptables et avec la certitude requise, de classer certains contenus comme étant bons ou mauvais; en fait, leur intention est inconnue. Le sandboxing aide à résoudre ce problème - il contraint ces fichiers inconnus à être exécutés dans un environnement protégé, observe les comportement inhérents et classe les risques sur la base ce comportement. Avec cette fonctionnalité activée pour votre évaluation, nous examinons de plus près les fichiers qui traversent votre réseau.

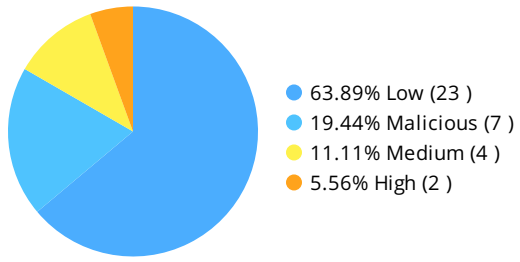
Résultats de l'analyse via Sandbox

Nombre de fichiers analysés (8,190)

Après une analyse anti-malware standard sur le FortiGate, les fichiers sélectionnés ont été envoyés au sandbox pour une inspection plus poussée. Le nombre ici représente le nombre total de fichiers exécutés dans un environnement protégé tout en observant certains comportements individuels (tels que des mises à jour de registres, suppressions de fichiers ou tentatives de communications avec des sites Web externes).

Les résultats de l'analyse comportementale sont généralement classés dans l'une des trois catégories suivantes: propre, suspect ou malveillant. Une désignation comme propre signifie qu'aucun comportement anormal n'a été observé et que le fichier peut être considéré comme sûr. Les activités suspectes sont potentiellement dangereuses et peuvent justifier une attention particulière - par exemple, un fichier hautement suspect peut essayer de se répliquer alors qu'un fichier à faible soupçon modifiera uniquement des registres de façon anormale. Une désignation malveillante devrait être considérée comme une menace légitime à votre réseau et nécessitera une attention immédiate. Le graphique présenté ici montre des fichiers malveillants et suspects (ne comprend pas de fichiers désignés comme propres).

Fichiers malveillants et suspects



Fichiers les plus fréquemment identifiés comme malveillants via sandbox

#	Nom de fichier	Service	Nombre
1	1D26B266.vXE	HTTP	1
2	1D28E4E7.vsc	HTTP	1
3	1D43634F.vsc	HTTP	1
4	1D45FCB7.vsc	HTTP	1
5	1D46A1FA.vsc	HTTP	1

Hôtes ciblés (par les fichiers malveillants identifiés via sandbox)

#	Source	Nombre
1	10.10.10.2	7

Actions recommandées

Attaques exploitant des vulnérabilités applicatives détectées (50)

Les vulnérabilités applicatives (attaques IPS) servent de points d'entrée aux cybercriminels pour contourner l'infrastructure de sécurité et pénétrer dans le réseau. Souvent, ces vulnérabilités sont exploitables en raison de la non-application d'une mise à jour ou l'absence de processus de gestion des correctifs. Pour se protéger contre ce type d'attaques, il faut identifier les hôtes auxquels aucun correctif n'a été appliqué.

Logiciels malveillants (16)

Les logiciels malveillants prennent différentes formes : virus, chevaux de Troie, logiciels espions/publicitaires, etc. Tout logiciel malveillant détecté qui se déplace latéralement sur le réseau peut annoncer un vecteur de menace venant de l'intérieur de l'entreprise, sans forcément venir d'un employé. En analysant les signatures et les comportements, il est possible d'empêcher les logiciels malveillants de s'exécuter et d'exposer le réseau à des activités malveillantes. L'ajout d'une technologie APT/Sandbox (telle que FortiSandbox) au réseau peut également éviter la propagation de logiciels malveillants inconnus (menaces de type « zero-day) au sein du réseau.

Infections de botnets (1)

Les bots servent à lancer des attaques par déni de service, à diffuser des spams et des logiciels espions/publicitaires, à propager du code malveillant et à s'emparer d'informations confidentielles, ce qui peut avoir de graves conséquences financières et juridiques. Les infections de botnets sont à prendre au sérieux et nécessitent une action immédiate. Identifiez les ordinateurs infectés par des botnets et nettoyez-les à l'aide d'un logiciel antivirus. Vous pouvez utiliser la solution FortiClient de Fortinet pour détecter les bots et les supprimer des ordinateurs infectés.

Sites Web malveillants (125)

Les sites Web malveillants hébergent des logiciels malveillants conçus pour collecter des informations, endommager l'ordinateur hôte ou manipuler la machine cible à l'insu de l'utilisateur. Leur consultation ouvre la voie à une infection et constitue la phase initiale de l'attaque. Le meilleur moyen de prévention consiste à bloquer les sites malveillants ou donner l'ordre aux employés de ne pas visiter de sites Web inconnus ou installer de logiciels associés.

Sites Web de phishing (1)

Comme sites Web malveillants, les sites de phishing reproduisent les pages de sites Web légitimes pour soutirer des infos confidentielles (identifiants, mots de passe, etc.) d'utilisateurs. Ces sites sont souvent des liens de courriers indésirables envoyés aux employés. Une approche sceptique à l'égard des e-mails demandant des informations et la vérification des liens avec le curseur peuvent empêcher la plupart des attaques.

Applications de proxy (5)

Ces applications sont utilisées (souvent intentionnellement) pour contourner les mesures de sécurité. Les utilisateurs peuvent déjouer le Firewall en camouflant ou chiffrant des communications externes. Souvent, cela est considéré comme un acte délibéré et une violation des règles d'usage de l'entreprise.

Applications d'accès à distance (5)

Les applications d'accès à distance sont utilisées pour accéder aux hôtes internes depuis l'extérieur, contournant le NAT ou offrant une voie d'accès secondaire (« porte dérobée ») à des hôtes internes. Au pire, l'accès à distance peut être exploité pour des d'extraction de données et d'espionnage industriel. Souvent, l'utilisation de l'accès à distance est libre, aussi des changements sont à apporter en internes.

Applications P2P et de partage de fichiers (5)

Ces applications sont utilisées pour contourner les contrôles de contenu existants, donnant lieu à des transferts non autorisés et violations des règles de données établies. Vous devez mettre en œuvre des règles d'utilisation appropriée.

Sécurité et prévention des menaces

Applications à haut risque

L'équipe de recherche FortiGuard attribue un niveau de risque allant de 1 à 5 à chaque application sur la base de ses caractéristiques comportementales. Les administrateurs peuvent ainsi identifier rapidement les applications à haut risque et mettre en place de meilleures règles de contrôle. Les applications répertoriées ci-dessous se sont vu attribuer un niveau de risque supérieur ou égal à 4.

Applications à haut risque

#	Risque	Nom de l'application	Catégorie	Technologie	L'utilisateur	Bande passante	Sessions
1	5	Proxy.HTTP	Proxy	Network-Protocol	11	9.46 MB	595
2	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
3	5	Psiphon3	Proxy	Client-Server	2	455.31 KB	15
4	5	Onavo.Protect	Proxy	Client-Server	1	2.51 KB	13
5	5	Hotspot.Shield	Proxy	Client-Server	2	207.76 KB	10
6	5	Skyfire	Proxy	Client-Server	3	40.33 KB	4
7	4	BitTorrent	P2P	Peer-to-Peer	8	2.14 MB	6,292
8	4	Telnet	Remote.Access	Client-Server	2	6.96 MB	632
9	4	Raysource	P2P	Peer-to-Peer	1	1.75 MB	147
10	4	RDP	Remote.Access	Client-Server	9	7.55 MB	39

Figure 1 : Applications à plus haut risque, classées par niveau de risque et par nombre de sessions

Exploitations des vulnérabilités applicatives

Les vulnérabilités applicatives peuvent être exploitées afin de compromettre la sécurité de votre réseau. L'équipe de recherche FortiGuard analyse ces vulnérabilités, puis élabore des signatures permettant de les détecter. À l'heure actuelle, FortiGuard tire parti d'une base de données répertoriant plus de 5 800 menaces applicatives connues afin d'identifier les attaques qui échappent aux systèmes de Firewall classiques. Pour en savoir plus sur les vulnérabilités applicatives, consultez le site FortiGuard à l'adresse suivante : http://www.fortiguard.com/intrusion.

Principales exploitations de vulnérabilités applicatives détectées

#	Gravité	Nom de la menace	Type	Victime	Source	Nombre
1	5	Adobe.Flash.Player.Authplay.DLL.SWF.Handling.Code.Execution	Other	1	1	2,035
2	5	IBM.Rational.ClearQuest.Username.Parameter.SQL.Injection	SQL Injection	30	1	195
3	5	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	3	2	19
4	5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	8	3	16
5	5	McAfee.Web.Reporter.EJBInvokerServlet.Object.Code.Execution	Code Injection	1	1	3
6	5	MS.IE.MSXML.Object.Handling.Code.Execution	Buffer Errors	1	1	2
7	4	LaVague.PrintBar.PHP.File.Inclusion	Code Injection	30	1	183
8	4	IISadmin.ISM.DLL.Access	Information Disclosure	29	1	169
9	4	GameSiteScript.Index.PHP.SQL.Injection	SQL Injection	30	1	169
10	4	OTE.Header.PHP.File.Inclusion	Code Injection	30	1	163

Figure 2 : Principales vulnérabilités identifiées, classées par niveau de gravité et par nombre

Logiciels malveillants, botnets et logiciels espions/publicitaires

Les cybercriminels diffusent leurs logiciels malveillants via une multitude de canaux. Les méthodes les plus courantes consistent à inciter les utilisateurs à ouvrir un fichier infecté joint à un e-mail, à télécharger un fichier infecté ou encore à cliquer sur un lien menant à un site malveillant. Lors de l'évaluation de sécurité, Fortinet a identifié un certain nombre d'événements liés à des logiciels malveillants et à des botnets. Ils correspondent à des téléchargements de fichiers malveillants ou à des connexions vers des botnets permettant la prise en main et le contrôle des ordinateurs infectés.

Principaux logiciels malveillants, botnets et logiciels espions/publicitaires détectés

#	Nom du logiciel malveillant	Type	L'application	Victime	Source	Nombre
1	EICAR_TEST_FILE	Virus	FTP	1	1	824
2	EICAR_TEST_FILE	Virus	HTTP	1	1	792
3	Asprox.Botnet	Botnet C&C	Asprox.Botnet	55	1	600
4	Adware/TEST_FILE	Adware	HTTP	1	1	411
5	ETDB_TEST_FILE	Virus	FTP	1	1	406
6	W32/NGVCK	Virus	HTTP	1	1	405
7	W32/ForeignRansom.583D!tr	Virus	HTTP	1	1	400
8	W32/ForeignRansom.583D!tr	Virus	FTP	1	1	395
9	W32/NGVCK	Virus	FTP	1	1	384
10	Adware/TEST_FILE	Adware	FTP	1	1	379

Figure 3 : Logiciels malveillants, botnets et logiciels espions/publicitaires courants détectés

Périphériques et hôtes à risque

Les types d'activités constatés pour un hôte nous permettent d'estimer le niveau de confiance de chaque client. La réputation du client repose sur des facteurs clés comme les sites Web consultés, les applications exécutées et les destinations entrantes/sortantes utilisées. En fin de compte, nous pouvons établir un niveau de menace global en considérant l'activité agrégée de chaque hôte.

Périphériques et hôtes les plus à risque

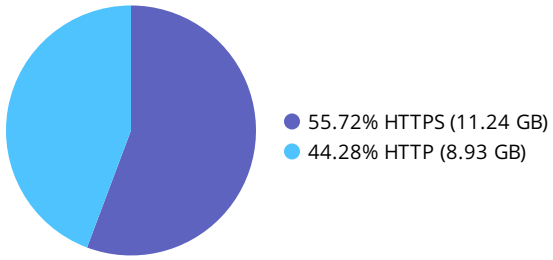
#	L'appareil	Niveau de menace
1	172.18.58.121	1,349,535
2	WX-UBUNTU-SERVER	506,760
3	172.18.3.250	237,790
4	172.18.27.205	220,595
5	172.18.27.207	199,275
6	dell-R200	181,795
7	172.18.27.254	179,225
8	172.18.52.165	177,740
9	172.18.32.158	130,835
10	StarrQian-FGT	119,700

Figure 4 : Il est nécessaire d'analyser ces périphériques pour vérifier leur vulnérabilité aux logiciels malveillants ou aux intrusions.

Trafic Web chiffré

Du point de vue de la sécurité, il est important de déterminer la part de trafic Web chiffré. Le trafic chiffré soulève des difficultés bien réelles pour les entreprises qui souhaitent s'assurer que les applications en question ne sont pas utilisées à des fins malveillantes, notamment pour extraire des données. Dans l'idéal, votre Firewall doit être capable d'inspecter le trafic chiffré à une vitesse élevée ; c'est pourquoi les performances et le déchargement matériel/ASIC sont des éléments essentiels à prendre en considération lors de l'évaluation d'un Firewall.

Part de trafic HTTPS/HTTP



Principaux pays d'origine

En examinant le trafic par adresse IP source, il est possible de déterminer le pays d'origine de n'importe quelle requête. Un certain nombre de botnets, de fonctions de commande et de contrôle, et même de sessions d'accès à distance peuvent utiliser beaucoup de bande passante et être révélateurs d'attaques ciblées ou de menaces persistantes en provenance de certains États-nations. Le tableau ci-après répertorie le trafic en fonction des différents pays ; l'activité provenant de pays spécifiques peut être anormale et justifier un examen plus poussé.

Principaux pays d'origine

#	Pays	Bande passante
1	United States	275.74 MB
2	Anonymous Proxy	11.01 MB
3	United Kingdom	5.11 MB
4	Belgium	2.02 MB
5	Netherlands	603.07 KB
6	Ireland	389.32 KB
7	Russian Federation	75.65 KB
8	Romania	47.75 KB
9	France	26.97 KB
10	China	6.23 KB

Figure 5 : Il est nécessaire d'analyser l'activité en provenance de ces pays pour vérifier la source du trafic

Productivité des utilisateurs

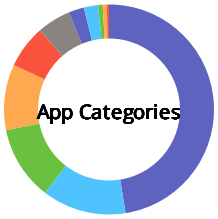
Utilisation des applications

L'équipe de recherche FortiGuard classe les applications en différentes catégories selon leurs caractéristiques comportementales, la technologie sous-jacente et le trafic associé. Ce classement permet d'optimiser le contrôle applicatif. FortiGuard gère des milliers de capteurs d'applications et peut même réaliser une inspection approfondie des applications. Par exemple, les responsables informatiques peuvent pour la première fois prendre connaissance du nom des fichiers envoyés ou du titre des vidéos lues en streaming.

Pour des informations détaillées sur les catégories d'applications, consultez le site suivant : http://www.fortiguard.com/encyclopedia/application

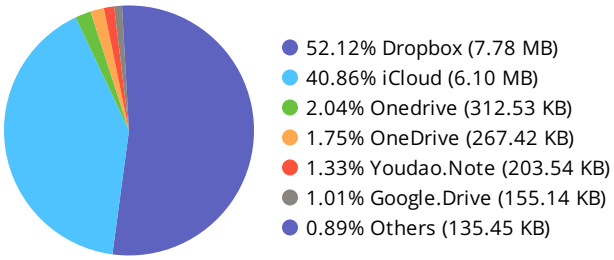
Catégories d'applications

Network.Service	47.47%
Web.Others	12.95%
Web.Client	11.40%
Video/Audio	10.13%
Unknown	6.61%
General.Interest	5.19%
Collaboration	2.39%
Update	2.18%
Email	0.70%
Social.Media	0.64%
Others	0.33%



Avec le développement rapide de l'informatique dans le cloud, les entreprises externalisent de plus en plus les différentes composantes de leur infrastructure. Malheureusement pour elles, la sécurité de leurs informations repose donc entièrement sur celle du fournisseur de services cloud. De plus, cela se traduit souvent par une redondance (si les services sont déjà disponibles en interne) et une augmentation des coûts (si la surveillance n'est pas effectuée correctement).

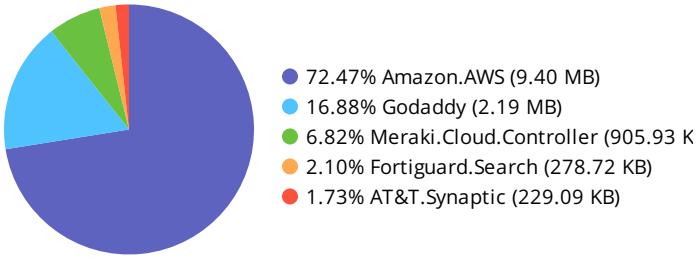
Utilisation du cloud (SaaS)



Les responsables informatiques ignorent souvent combien de services cloud sont déployés au sein de leur entreprise. Parfois, ces applications peuvent être utilisées pour contourner voire remplacer l'infrastructure en place dans un souci de confort d'utilisation. Malheureusement, cela peut avoir pour conséquence indésirable le transfert de vos informations sensibles dans le cloud. Par conséquent, vos données pourraient être exposées en cas de brèche dans l'infrastructure de sécurité du fournisseur de services cloud.

Les plateformes d'« infrastructure en tant que service » (Infrastructure-as-a-Service ou IaaS) connaissent un grand succès et s'avèrent précieuses lorsque les ressources informatiques sont limitées ou font l'objet d'exigences particulières. Cela dit, l'externalisation effective de votre infrastructure doit être bien réglementée afin d'empêcher toute utilisation inappropriée. Un audit ponctuel des applications IaaS peut être utile non seulement pour optimiser la sécurité, mais aussi pour minimiser les coûts organisationnels associés aux modèles de paiement à l'usage ou aux frais d'abonnement.

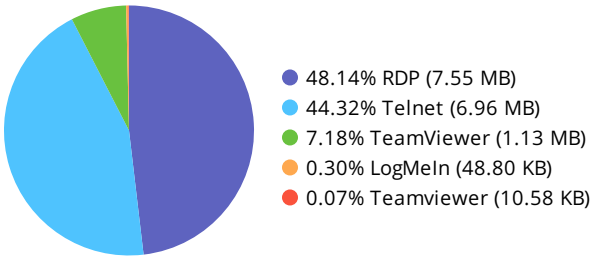
Utilisation du cloud (IaaS)



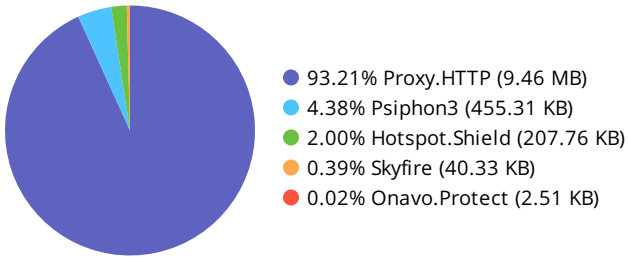
Décomposition des catégories d'applications

Une bonne compréhension des sous-catégories d'applications fournit un précieux éclairage sur l'efficacité du réseau de votre entreprise. Certains types d'applications, comme les applications Peer-to-Peer ou les jeux, n'ont pas nécessairement leur place dans un environnement professionnel. Il est possible de les bloquer ou de limiter leur portée. D'autres applications peuvent avoir un double usage, comme la diffusion audio/vidéo ou les réseaux sociaux, et pourront être gérées en conséquence. Les graphiques ci-après illustrent les catégories d'applications classées par quantité de bande passante consommée tout au long de la détection.

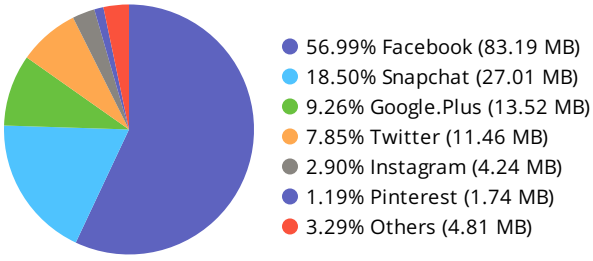
Applications d'accès à distance



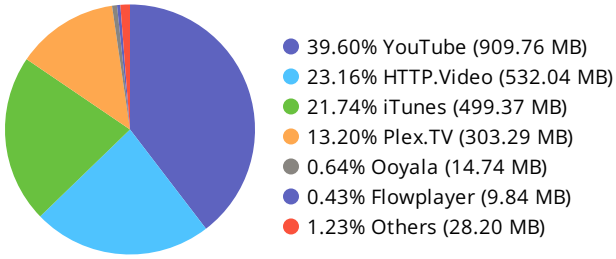
Applications de proxy



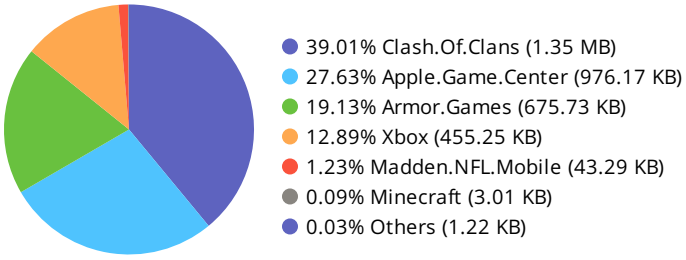
Principales applications de médias sociaux



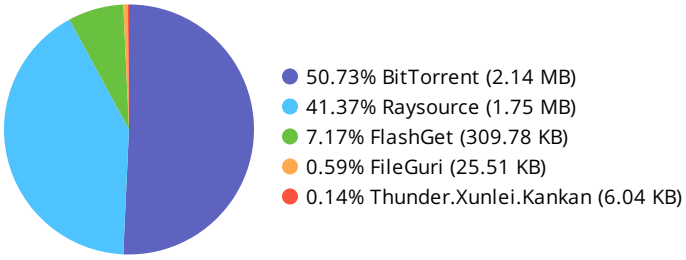
Principales applications de diffusion audio/vidéo



Principales applications de jeu



Principales applications Peer-to-Peer



Utilisation du Web

Les habitudes de navigation sur le Web peuvent non seulement être révélatrices d'un usage inefficace des ressources de l'entreprise, mais aussi pointer du doigt une mauvaise application des règles de filtrage Web. Elles peuvent également vous éclairer sur les habitudes de navigation Web de votre personnel et vous aider à définir des règles de conformité internes.

Principales catégories Web

#	Catégorie d'URL	L'utilisateur	Nombre	Bande passante
1	Unrated	3	1,359	2.06 MB
2	Information Technology	5	1,106	56.71 MB
3	Search Engines and Portals	5	757	40.05 MB
4	Advertising	4	558	4.82 MB
5	Web Hosting	3	447	2.68 MB
6	Instant Messaging	3	285	1.75 MB
7	File Sharing and Storage	3	257	1,018.61 KB
8	Business	4	245	3.97 MB
9	News and Media	3	212	7.78 MB
10	Content Servers	4	205	7.94 MB

Dans les environnements réseau actuels, de nombreuses applications, dont certaines auxquelles on ne s'attendrait pas, utilisent le protocole HTTP pour les communications. Son principal intérêt est qu'il est très répandu, universellement accepté et ouvert sur la majorité des Firewalls. Si le protocole HTTP facilite la communication pour la plupart des applications métier et celles sur liste blanche, certaines applications non professionnelles peuvent en revanche l'utiliser à des fins non productives, voire pour des raisons pernicieuses.

Principales applications Web

#	L'application	Sessions	Bande passante
1	SSL	146,699	6.47 GB
2	HTTP.BROWSER	250,146	4.99 GB
3	HTTPS	207,789	2.99 GB
4	YouTube	5,137	882.78 MB
5	HTTP	182,783	854.39 MB
6	HTTP.Audio	681	626.99 MB
7	HTTP.Video	400	531.03 MB
8	iTunes	217	499.37 MB
9	HTTPS.BROWSER	7,338	372.21 MB
10	Apple.Services	25	241.61 MB

Sites Web consultés

Les sites Web consultés en disent long sur la manière dont les employés utilisent les ressources de l'entreprise et dont les applications communiquent avec des sites Web spécifiques. L'analyse des domaines auxquels le personnel se connecte peut inciter l'entreprise à modifier son infrastructure en adoptant des techniques telles que le filtrage des sites Web, l'inspection approfondie des applications cloud et l'accélération Web.

Domaines Web les plus visités

#	Domaine	Catégorie	Visites
1	ca.archive.ubuntu.com	Reference	1,256
2	ads2.westca.com	Advertising	462
3	security.ubuntu.com	Information Technology	387
4	cdn.speedshiftmedia.com	Advertising	335
5	gs-loc.apple.com	Information Technology	194
6	caextshort.weixin.qq.com	Instant Messaging	157
7	mmsns.qpic.cn	Content Servers	156
8	173.194.33.86	Search Engines and Portals	133
9	23.209.27.138	Unrated	123
10	23.3.105.162	Unrated	122

Les durées de consultation estimées pour des sites Web individuels peuvent être utiles pour se faire une idée précise des sites les plus visités. Il s'agit généralement de ressources Web internes telles que des intranets, mais ils peuvent également être révélateurs d'une utilisation abusive. Les durées de consultation peuvent servir à justifier l'implémentation de technologies de mise en cache Web ou à élaborer les règles d'usage de l'entreprise.

Principaux sites Web par durée de consultation

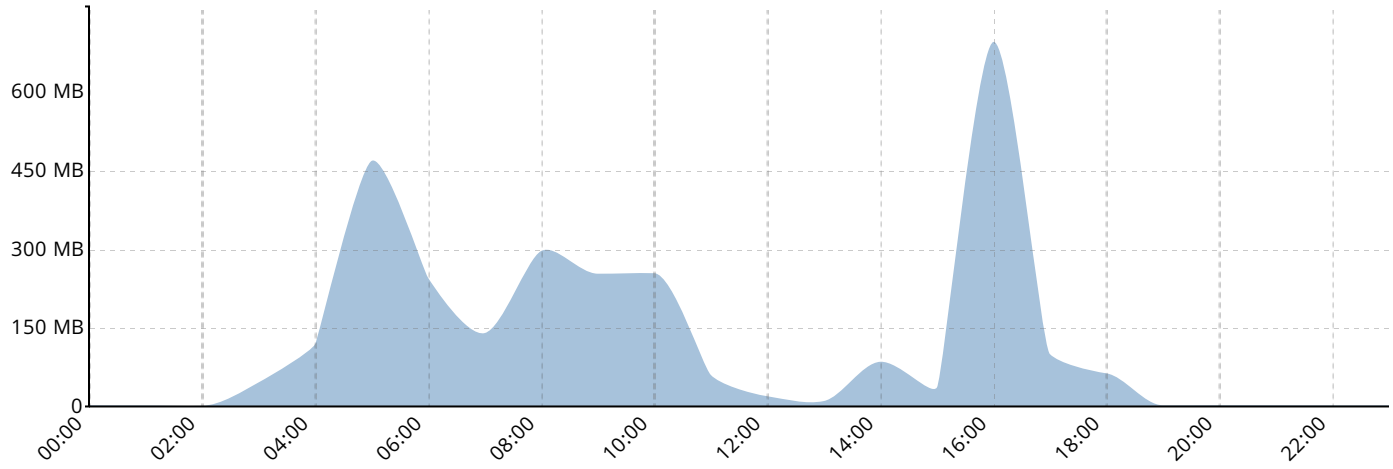
#	Sites	Catégorie	Durée de consultation (hh:mm:ss)
1	blu407-m.hotmail.com	Web-based Email	01:00:21
2	np.lexity.com	Information Technology	00:35:58
3	www.encyclopedia.com	Reference	00:31:34
4	www.google-analytics.com	Information Technology	00:27:30
5	ssw.live.com	Search Engines and Portals	00:26:59
6	clients1.google.com	Search Engines and Portals	00:24:23
7	www.google.com	Business, Search Engines and Portals, Web-based Applications	00:23:52
8	www.forever21.com	Shopping and Auction	00:21:56
9	ping.chartbeat.net	Information Technology	00:20:11
10	apple-finance.query.yahoo.com	Search Engines and Portals	00:17:27

Utilisation du réseau

Bande passante

En examinant l'utilisation de bande passante au cours d'un jour normal, les administrateurs peuvent mieux comprendre les besoins de leur entreprise en matière de débit d'interface et de connexion de FAI. Il est également possible d'optimiser la bande passante pour des applications particulières (à l'aide de la fonction de limitation), de donner la priorité à des utilisateurs spécifiques aux heures où le trafic est le plus important et de reprogrammer les mises à jour en dehors des heures de travail.

Bande passante moyenne par heure



L'une des façons les plus pertinentes d'analyser la bande passante consiste à examiner les destinations et les sources générant le plus de trafic. La consommation de bande passante des sites de destination courants (par exemple, les sites Web externes), tels que ceux utilisés pour les mises à jour d'OS ou de microprogramme, peut être limitée pour laisser la place au trafic prioritaire et stratégique. En interne, les hôtes générant un trafic élevé peuvent être optimisés via une mise en forme du trafic ou des règles d'usage.

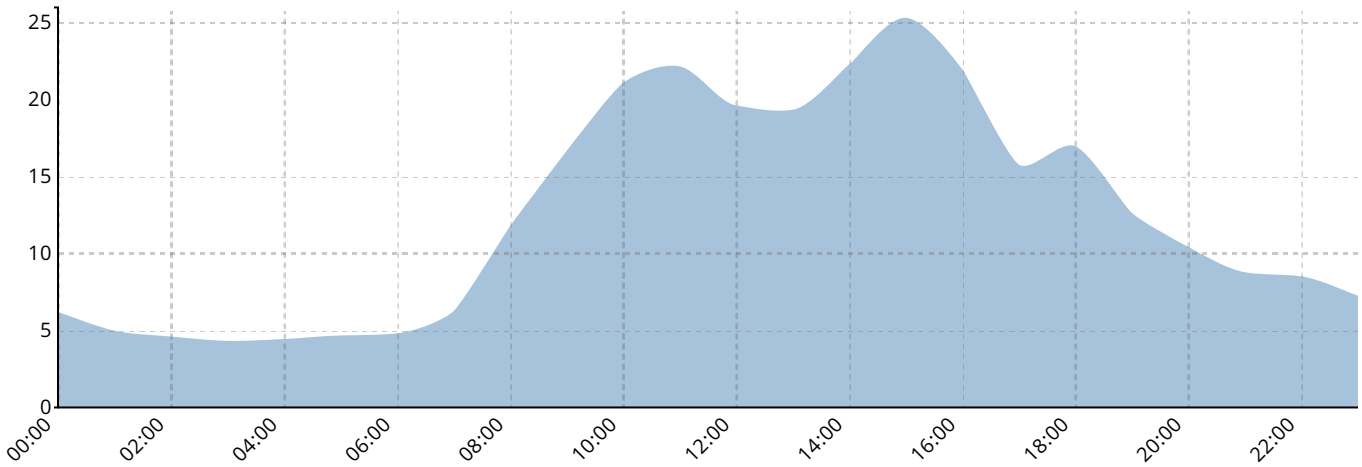
Sources/destinations consommant le plus de bande passante

#	Nom de l'hôte	Bande passante
1	ca.archive.ubuntu.com	89.99 MB
2	iosapps.itunes.apple.com	54.59 MB
3	www.forever21.com	48.13 MB
4	www.amazon.com	34.90 MB
5	tlu.dl.delivery.mp.microsoft.com	32.57 MB
6	appldnld.apple.com	29.17 MB
7	www.games.com	28.74 MB
8	security.ubuntu.com	20.91 MB
9	streamingaudio.itunes.apple.com	18.27 MB
10	hds.video-cdn.espn.com	14.82 MB

Informations de dimensionnement

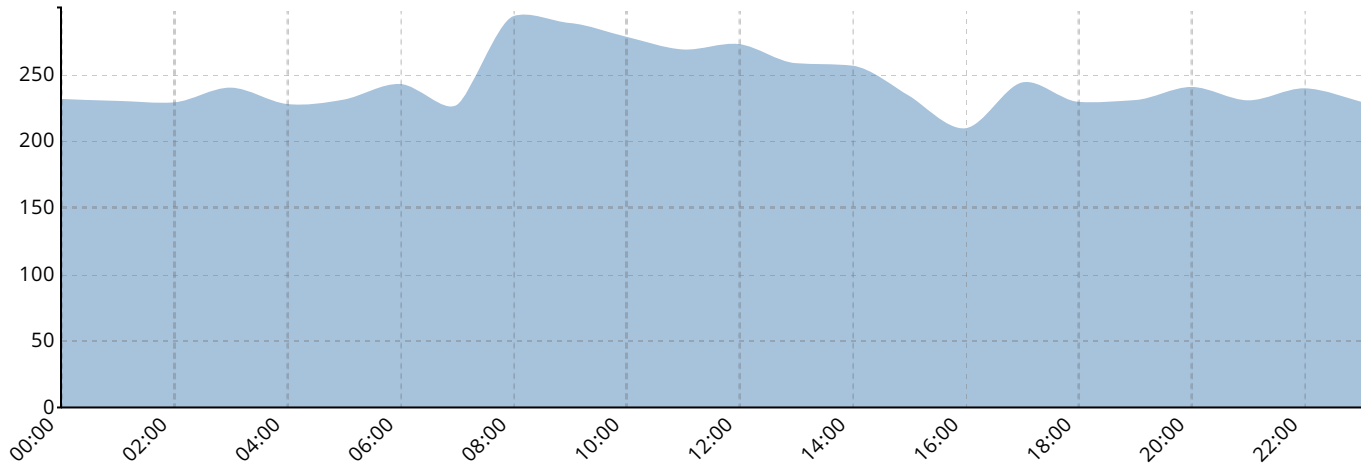
Du point de vue des performances, une bonne compréhension du nombre moyen d'événements consignés est extrêmement bénéfique pour le dimensionnement d'un environnement de sécurité. Un nombre d'événements consignés élevé à des heures spécifiques signale généralement un pic de trafic et d'utilisation de bande passante. Le calcul du nombre moyen d'événements consignés à l'échelle de l'entreprise peut également s'avérer utile pour le dimensionnement de dispositifs d'enregistrement de logs/d'analyse en amont tels que FortiAnalyzer. Notez que le nombre moyen d'événements consignés présenté ici a été obtenu avec l'ensemble des fonctionnalités de l'appliance FortiGate activées et inclut tous les types de logs (Firmware, antivirus, contrôle applicatif, IPS, filtrage d'URL et événements système).

Nombre moyen d'événements consignés par heure



Le nombre moyen de sessions appelées au cours d'une heure peut vous éclairer sur les besoins en matière de performances (pour FortiAnalyzer, mais aussi pour l'architecture finale de la solution FortiGate). En règle générale, il existe une corrélation entre la consommation de bande passante, le nombre d'événements consignés et le nombre de sessions. Le nombre de sessions constitue une autre donnée utilisable pour dimensionner le réseau actuel, mais il permet aussi de préparer le réseau à une augmentation ultérieure du trafic.

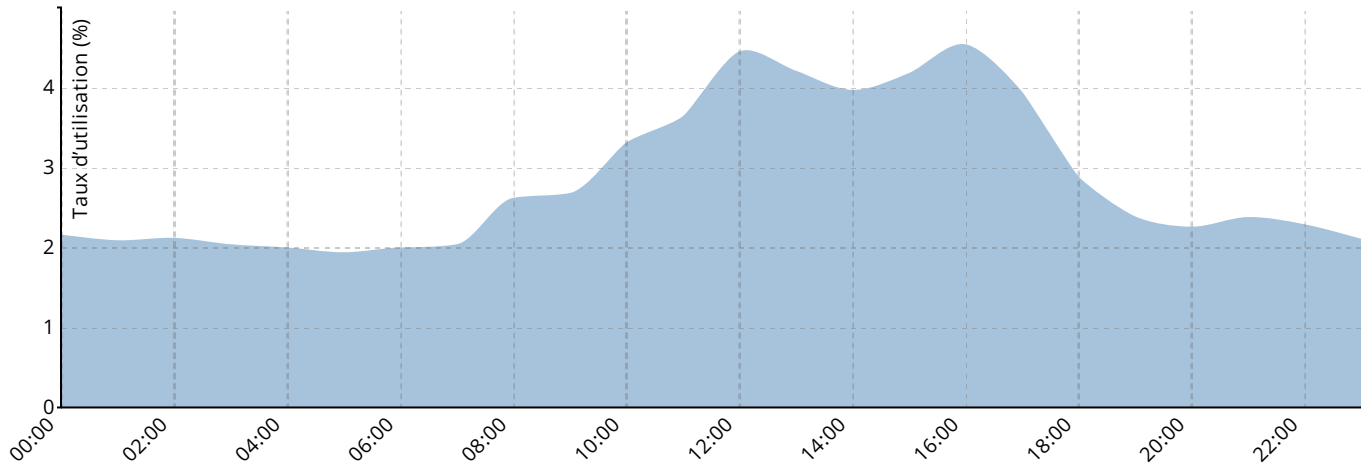
Nombre de sessions moyen par heure



Statistiques relatives au Firewall

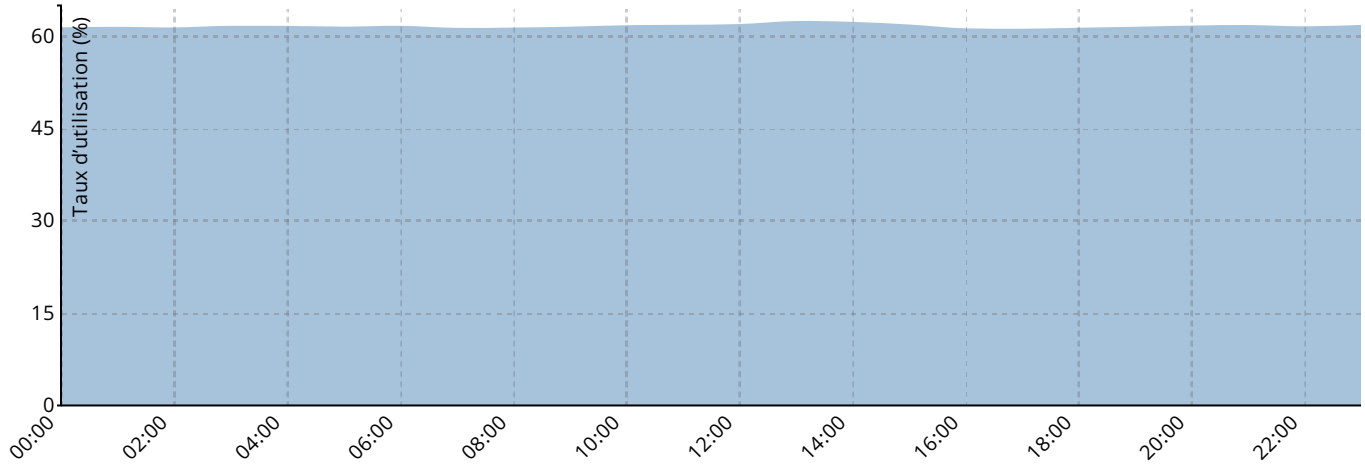
On se réfère souvent à l'UC utilisée par une appliance FortiGate pour dimensionner la solution finale. Un relevé horaire du taux d'utilisation de l'UC permet de se faire une bonne idée de la manière dont l'appliance FortiGate fonctionnera dans le réseau cible. Un débit élevé produit en général davantage de logs. Si le taux d'utilisation se maintient à 75 % ou plus sur une longue période, cela signifie qu'un nouveau modèle est requis ou que l'architecture doit être revue pour l'implémentation finale.

Taux d'utilisation horaire moyen de l'UC par l'appliance FortiGate



De la même manière, le taux d'utilisation de la mémoire dans le temps est un excellent indicateur de la viabilité de l'appliance FortiGate dans l'environnement réseau cible. Même si l'utilisation de la bande passante est faible, la consommation de la mémoire peut rester élevée en raison de l'enregistrement des logs (ou de la gestion de la file d'attente des logs).

Taux d'utilisation horaire moyen de la mémoire par l'appliance FortiGate



Sécurité et services FortiGuard

La connaissance du paysage des menaces et la capacité à réagir rapidement à plusieurs niveaux constituent le socle d'une sécurité efficace. Des centaines de chercheurs de FortiGuard Labs ratissent chaque jour le paysage informatique pour identifier les menaces émergentes et développer des contre-mesures visant à protéger les entreprises du monde entier. C'est grâce à eux que la solution FortiGuard est créditée de plus de 250 détections d'attaques de type « zero-day » et de vulnérabilités, et que les solutions de Fortinet sont si bien notées lors des tests d'efficacité de la sécurité en conditions opérationnelles menés par NSS Labs, Virus Bulletin, AV Comparatives et autres organismes tiers.

Contrôle applicatif et IPS nouvelle génération

Le contrôle applicatif et la prévention des intrusions (IPS) constituent des technologies de sécurité fondamentales d'un Firewall de nouvelle génération tel que l'appliance FortiGate. Les entreprises du monde entier s'appuient sur les fonctions de contrôle applicatif et IPS offertes par la plateforme FortiGate pour gérer leurs applications et empêcher les intrusions dans leur réseau (chaque jour, FortiGuard bloque environ 470 000 tentatives d'intrusion par minute). L'efficacité des appliances FortiGate avec ces fonctions activées est évaluée dans le cadre de tests comparatifs des solutions du secteur réalisés par NSS Labs, qui attribue systématiquement la mention « Recommandé » aux produits FortiGate.

Web Filtering

Chaque jour, FortiGuard Labs traite environ 43 mns de requêtes de catégorisation et bloque quelque 160 000 sites Web malveillants par minute. Le service Web Filtering examine plus de 250 mns de sites Web et fournit près de 1,5 mn de nouvelles évaluations d'URL chaque semaine. Seule solution de filtrage Web certifiée par VBWeb, FortiGuard a bloqué 97,7 % des téléchargements directs de logiciels malveillants lors des tests réalisés par l'organisme en 2016.

Antivirus et sécurité mobile

Chaque jour, FortiGuard Labs neutralise environ 95 000 programmes malveillants ciblant les plateformes traditionnelles, mobiles et IoT par minute. S'appuyant sur des technologies brevetées, FortiGuard Antivirus est capable d'identifier des milliers de variantes de logiciels malveillants actuelles et à venir à partir d'une seule signature, optimisant à la fois l'efficacité et les performances en matière de sécurité. Fortinet obtient systématiquement des résultats supérieurs dans le cadre des tests d'efficacité des solutions du secteur réalisés par Virus Bulletin et AV Comparatives.

AntiSpam

FortiGuard Labs bloque environ 21 000 spams par minute chaque jour et fournit quelque 46 mnsde règles antispam nouvelles et mises à jour. Les e-mails constituent le principal vecteur utilisé pour le lancement d'une attaque avancée contre une entreprise, c'est pourquoi un antispam ultra-efficace est un composant essentiel d'une stratégie de sécurité.

Advanced Threat Protection (FortiSandbox)

Des milliers d'entreprises du monde entier tirent parti de FortiSandbox pour identifier les menaces avancées. FortiSandbox se voit systématiquement attribuer la mention « Recommandé » dans le cadre des tests des systèmes de détection des brèches réalisés par NSS Labs et a obtenu un score de plus de 97 % lors de ces tests en 2015.

Réputation IP

Chaque jour, FortiGuard Labs bloque environ 32 000 tentatives de commande et de contrôle effectuées par des botnets par minute. La communication de la menace avec un serveur de commande et de contrôle, pour télécharger d'autres menaces ou extraire des données volées, constitue une phase essentielle du processus d'attaque contre une entreprise. La réputation de l'adresse du domaine et IP est utilisée pour bloquer cette communication et neutraliser ainsi les menaces.