La gestion des données personnelles avec un Firewall nouvelle génération

Forcepoint

Sommaire

Informations générales

Objectif du document

Ce document a pour but de fournir une transparence et des explications concernant la gestion des données personnelles par les produits et services suivants de Forcepoint : Next-Generation Firewall (NGFW), Security Management Center (SMC), Endpoint Context Agent (ECA), User ID Service et VPN Client. Ce document vise à fournir les informations nécessaires aux équipes chargées de l'application et de l'évaluation de la protection de la vie privée, pour qu'elles puissent prendre des décisions éclairées concernant les produits et services Forcepoint mentionnés précédemment.

Règlement général sur la protection des données (RGPD)

Le fonctionnement des produits et services de Forcepoint est conçu pour respecter les principes de confidentialité énoncés dans le Règlement général sur la protection des données (RGPD) (règlement (UE) 2016/679). Conformément aux principes du RGPD, les clients de Forcepoint sont considérés comme les seuls responsables du traitement des données. Forcepoint n'est ni le contrôleur de données, ni le responsable du traitement des données, en ce qui concerne les données des clients stockées dans les produits et services Forcepoint NGFW, SMC, ECA, User ID Service et VPN Client. De plus amples informations concernant le RGPD sont disponibles sur le site https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

Données personnelles

Le présent document applique la définition des données à caractère personnel figurant à l'article 4.1 du RGPD, qui définit les « données à caractère personnel » comme toute information concernant une personne physique identifiée ou identifiable (la « personne concernée ») ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, par référence à un identifiant tel que, sans s'y limiter, un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou d'autres facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Protéger les Données personnelles

Forcepoint utilise des techniques basées sur les normes de l'industrie pour protéger les données détenues dans les produits Forcepoint, y compris les données personnelles. Cette approche de la sécurité des données permet de garantir que les données à haut risque sont incompréhensibles pour toute personne qui n'est pas autorisée à y accéder. Retrouvez tous les détails sur la politique et les processus de confidentialité de Forcepoint à l'adresse suivante : https://www.forcepoint.com/forcepoint-privacy-hub.

Avertissement :

Ce document contient des informations concernant les produits et/ou services de Forcepoint. Ces informations sont la propriété de Forcepoint. Bien que tous les efforts aient été faits pour s'assurer que le contenu est à jour et exact, les informations sont fournies *telles quelles*, sans aucune représentation ou garantie, expresse ou implicite, et peuvent être modifiées sans préavis.

Toute référence à des versions ou fonctionnalités futures est une prévision et ne constitue pas un engagement. Forcepoint n'assume aucune responsabilité quant à l'utilisation de ces informations.

Identité et Politique

Ensemble de données	Quelles sont les données personnelles utilisées ?	Objectif	État des données	Quelles sont les données personnelles utilisées ?	Conservation
Comptes administrateur	Un compte super-utilisateur est créé lors de l'installation du SMC. Ce compte est utilisé pour créer des comptes administrateurs après l'installation. Si les clients choisissent d'utiliser l'authentification par certificat, un identifiant de sujet, comme une adresse courriel, est utilisé pour identifier les administrateurs.	Les administrateurs qui ont des niveaux d'accès différents peuvent effectuer des tâches dans le SMC en fonction des rôles d'administrateur qui leur sont attribués.	Les données ne sont pas pseudonymisées	Les noms d'utilisateur et les hashs SHA-512 des mots de passe de l'administrateur générés par le SMC sont stockés dans la base de données du serveur de gestion, que les clients hébergent soit sur leur réseau interne/sur site, soit dans leur propre espace/solution cloud hors de Forcepoint.	Le client peut supprimer les comptes administrateurs manuellement.
Base de données des utilisateurs LDAP interne	La base de données interne des utilisateurs LDAP du SMC contient les noms d'utilisateur et les hashs des mots de passe des utilisateurs. Si l'authentification par certificat est utilisée, un identifiant de sujet tel qu'une adresse courriel est utilisé pour identifier les utilisateurs.	Les comptes d'utilisateurs peuvent être utilisés pour l'authentification et le contrôle de l'accès au réseau.	Les données ne sont pas pseudonymisées	Les noms d'utilisateurs et les hashs AES des mots de passe des utilisateurs sont stockés dans la base de données des utilisateurs LDAP interne sur le serveur de gestion. Ils peuvent être répliqués vers les moteurs NGFW par le biais d'une connexion protégée TLS conforme aux normes industrielles. Le client peut accéder aux données en utilisant un compte qui permet l'accès au système d'exploitation.	Le client peut supprimer les comptes utilisateurs manuellement.

Comment gérer une Demande d'Accès d'un Sujet (DAS)

DAS – Droit d'accès	L'administrateur superutilisateur SMC assigné par le client peut accéder et gérer (ajouter/modifier/supprimer) les données des comptes administrateur et utilisateur dans la base de données des comptes utilisateur SMC, qui est stockée dans la configuration du serveur SMC. Le terme anglais correspondant à DAS est « SAR » (*Subject Access Request*).
DAS – Correction/Rectification	L'administrateur superutilisateur SMC peut accéder et gérer (ajouter/modifier/supprimer) les données des comptes administrateur et utilisateur dans la base de données des comptes utilisateur SMC, qui est stockée dans la configuration du serveur SMC.
DAS – Droit à l'oubli	L'administrateur superutilisateur peut supprimer les données des comptes administrateur et utilisateur dans la base de données des comptes utilisateur du SMC, qui est stockée dans la configuration du serveur SMC. Toutes les actions des administrateurs du SMC sont collectées et stockées dans des journaux d'audit qui ne peuvent pas être filtrés ou supprimés, selon un compte administrateur spécifique.
Stockage des données/Emplacement	Les données des comptes utilisateurs et administrateurs du NGFW et du SMC sont stockées sur des serveurs gérés par le client.

Enregistrement des activités

Ensemble de données	Quelles sont les données personnelles utilisées ?	Objectif	État des données	Quelles sont les données personnelles utilisées ?	Conservation

Stockage du serveur de journaux (Comprend les journaux d'accès, d'inspection et d'alerte, et les données du compteur)	Par défaut, aucune donnée personnelle n'est enregistrée dans les journaux d'accès. Cependant, les clients peuvent configurer les moteurs NGFW pour qu'ils journalisent les données d'accès qui peuvent inclure des informations sur les adresses IP, les URL, les noms d'utilisateur et les applications. Les données peuvent être utilisées à diverses fins, comme la collecte de statistiques. Pour plus de détails, voir le TABLEAU 1 : Attributs de données personnelles pour les journaux d'accès dans le SMC dans l'annexe A.	Pour surveiller le trafic réseau et créer des rapports	Les données ne sont pas pseudonymisées	Les journaux d'accès sont stockés sur les disques du serveur de journaux dans un format propriétaire. Les données sont reçues des moteurs NGFW par le biais d'une connexion protégée TLS conforme aux normes industrielles. Lorsque l'intégration avec ElasticSearch est configurée, le SMC peut déléguer l'indexation des journaux du SMC à une instance de base de données ElasticSearch locale gérée par le client. Le client peut ainsi bénéficier d'une consultation plus rapide des journaux et de rapports statistiques transparents via l'interface utilisateur du SMC. Le client peut accéder aux données en utilisant un compte qui permet l'accès au système d'exploitation NGFW.	Le client peut supprimer ou archiver les données du journal des activités de surveillance de l'accès, soit manuellement, soit automatiquement, en utilisant le SMC et/ou la fonctionnalité de tâche planifiée du SMC.
Journaux d'audits	Les journaux d'audit comprennent les noms des comptes d'administrateur et les adresses IP des postes de travail clients. Pour plus de détails, voir le TABLEAU 2 : Attributs de données personnelles pour les journaux d'audit dans le SMC dans l'annexe A.	Pour auditer les actions de l'administrateur	Les données ne sont pas pseudonymisées	Les journaux d'audit sont stockés sur les disques du serveur de gestion et du serveur de journalisation dans un format propriétaire. Les données sont reçues des moteurs NGFW via une connexion protégée par TLS. Le client peut accéder aux données en utilisant un compte qui permet l'accès au système d'exploitation.	Le client peut utiliser le SMC pour supprimer ou archiver les données des journaux d'audit, soit manuellement à l'aide du SMC, soit automatiquement grâce à la fonctionnalité de planification de tâche du SMC.
Rapports planifiés	Les rapports sont utilisés pour présenter des statistiques à partir des données du journal, qui peuvent inclure des données personnelles selon la configuration du journal du client.	Créer des rapports sur les événements liés au trafic réseau et/ou répondre aux besoins des clients en matière de rapports.	Les données ne sont pas pseudonymisées	Les rapports sont stockés sur les disques du serveur de gestion dans un format propriétaire. Le client peut accéder aux données en utilisant un compte qui permet d'accéder au système d'exploitation ou aux interfaces de gestion du SMC.	Le client peut définir le délai d'expiration du rapport dans les conceptions de rapport. Le délai d'expiration par défaut du rapport est de 10 jours.
Journaux de débogage ECA sur les terminaux Windows	Les données contenues dans les journaux de débogage ECA comprennent les utilisateurs actuellement connectés au terminal et leurs domaines, ainsi que certaines informations de base telles que le système d'exploitation, le type de CPU, la mémoire physique libre et totale, l'espace disque libre et total, et les applications installées.	Résoudre les problèmes techniques des clients.	Les données ne sont pas pseudonymisées	Les clients sont invités à sauvegarder les journaux de débogage dans le répertoire d'installation ECA.	Les données du journal de débogage sont stockées dans des fichiers de 2 Mo. La quantité maximale de données de journal pouvant être conservée étant de 10 Mo, le système peut conserver jusqu'à 5 fichiers de 2 Mo. Lorsque le nombre maximal de fichiers journaux est atteint, le système élimine les plus anciens pour laisser la place aux fichiers journaux les plus récents.

Comment gérer une Demande d'Accès d'un Sujet (DAS)

DAS – Droit d'accès	Les administrateurs du FWNG peuvent accéder aux données des journaux et des rapports du SMC et les gérer par le biais de l'API de gestion du SMC.
DAS – Correction/Rectification	Le NGFW et le SMC sont conçus pour empêcher toute modification (correction/rectification) des données du journal stockées à des fins de sécurité et d'audit.
DAS – Droit à l'oubli	L'administrateur super-utilisateur du NGFW et du SMC peut filtrer et supprimer les journaux sélectionnés en fonction de l'identité d'un utilisateur spécifique (par exemple, le nom d'utilisateur, l'identifiant du compte utilisateur). Toutes les actions des administrateurs du SMC sont collectées et stockées dans des journaux d'audit qui ne peuvent pas être filtrés ou supprimés, selon un compte administrateur spécifique.
Stockage des données/Emplacement	Le client NGFW choisit et gère l'emplacement de son installation NGFW et SMC et de ses serveurs de données.

Modules d’extension

Ensemble de données	Quelles sont les données personnelles utilisées ?	Objectif	État des données	Quelles sont les données personnelles utilisées ?	Conservation
Advanced Malware Detection (AMD)	La détection avancée des logiciels malveillants (*Advanced Malware Detection* ou AMD) reçoit du NGFW des fichiers qui doivent être analysés à la recherche de malware. À la réception du fichier, AMD procède à son analyse pour déterminer si le fichier contient un malware. Les fichiers téléchargés pour être analysés par AMD peuvent potentiellement contenir des données personnelles. L'administrateur du client est en mesure de configurer les types de fichiers à soumettre à AMD.	Pour comprendre si l'ensemble du fichier soumis présente un risque de malware.	Les résultats des fichiers sont rendus anonymes en générant un hash SHA-1 du fichier soumis et en associant le résultat de l'analyse avec le hash du fichier. Une fois l'analyse terminée, le fichier et son contenu sont immédiatement supprimés.	Advanced Malware Detection enregistre le résultat de l'analyse du malware qui est lié au hash du fichier généré par AMD. Le fichier soumis est immédiatement supprimé à la fin de l'analyse. L'analyse peut prendre entre 10 secondes et 5 minutes, selon la taille et le type du fichier analysé. Le fichier est soumis à AMD via un canal crypté TLS conforme aux normes industrielles. La capacité d'analyse d'AMD est externalisée. L'analyse se déroule dans deux centres de données, situés à Los Angeles (États-Unis) et à Amsterdam (Pays-Bas). Les clients choisissent le centre de données qu'ils utilisent, mais peuvent aussi sélectionner « Automatique ». Cela configurera le centre de données le plus proche géographiquement de l'adresse IP publique du NGFW qui fait la demande de résolveur DNS.	Advanced Malware Detection ne conserve pas le fichier soumis. AMD conserve indéfiniment les résultats d'analyse d'un fichier. En outre, si un code de malware est découvert au cours de l'analyse, ce code (artefact de malware) est conservé indéfiniment.
User ID Service (UID)	L'adresse IP et l'utilisateur correspondent. Pour plus de détails, voir le TABLEAU 3 : Attributs de données personnelles pour le service User ID de Forcepoint dans l'annexe A.	Résoudre les associations entre les adresses IP des utilisateurs et les groupes d'utilisateurs.	Les données ne sont pas pseudonymisées	Les données sont stockées en clair dans une base de données interne. Les clients ont la possibilité de crypter la base de données avec un cryptage de leur choix. La base de données contient un sous-ensemble d'attributs Active Directory spécifiques aux utilisateurs, tels que le nom d'utilisateur, l'adresse courriel, l'appartenance à un groupe et l'adresse IP actuelle. L'accès aux données nécessite un compte permettant l'accès au système d'exploitation. L'API du service UID permet des requêtes non authentifiées pour ces données à partir du réseau. Le firewall du système d'exploitation peut être utilisé pour contrôler l'accès réseau à l'API.	Les données relatives aux paires d'utilisateurs et d'adresses IP sont conservées pendant 6 heures. Pour supprimer les données, le client peut désinstaller le Forcepoint User ID Service.
VPN Client pour Windows	Les données du journal de VPN Client contiennent les adresses courriel des utilisateurs si un certificat qui contient les adresses courriel est utilisé comme méthode d'authentification dans les VPN.	Journalise l'utilisation du VPN des clients via le NGFW et peut également être utilisé pour résoudre les problèmes techniques des clients.	Les données ne sont pas pseudonymisées	Les données du journal de VPN Client sont stockées sous forme de fichiers texte dans le dossier de données de Client VPN (par défaut, C:\ProgramData\Forcepoint\Stonesoft VPN Client\log ou C:\ProgramData\Forcepoint\VPN Client\log).	Les données des fichiers journaux du Client VPN sont automatiquement écrasées lorsque de nouvelles données journaux sont créées. Pour supprimer les données, désinstallez VPN Client pour Windows, puis supprimez manuellement les fichiers du dossier de données du VPN Client.

Les produits suivants, qui peuvent être intégrés ou utilisés avec le Forcepoint NGFW, ne stockent pas de données personnelles localement :

- Forcepoint VPN Client pour Android
- Forcepoint VPN Client pour Mac

Comment gérer une Demande d'Accès d'un Sujet (DAS)

DAS – Droit d'accès	AMD : Les clients de NGFW peuvent accéder à leurs rapports de sandbox à partir du compte client du portail AMD et des liens “Rapports d'analyse” dans les journaux de filtrage de fichiers. Les documents de support des produits AMD de Forcepoint doivent être référencés pour fournir des détails supplémentaires sur la protection des données et les rapports spécifiques à AMD. Service User ID : Les données utilisateur qui se trouvent dans le service Forcepoint User ID (FUID) sont importées directement de l'annuaire Microsoft Active Directory (AD) qui a été configuré par le client utilisateur du NGFW. Les données utilisateur FUID sont accessibles et gérables (accès/modification/suppression) via le compte administrateur NGFW - FUID et les outils de gestion Microsoft AD du client.
DAS – Correction/Rectification	FUID contient les données des utilisateurs qui ont été importées directement du système Microsoft Active Directory (AD) du client, telles qu'elles apparaissent dans Microsoft AD. Les corrections des données des utilisateurs doivent être effectuées dans Microsoft AD et réimportées dans FUID.
DAS – Droit à l'oubli	La désinstallation des services FUID supprimera automatiquement toutes les données des utilisateurs.
Stockage des données/Emplacement	Les clients utilisant NGFW choisissent et gèrent l'emplacement de son installation FUID et de son serveur de données.

Annexe A :

Terminologie

Terme	Explication
Next-Generation Firewall (NGFW)	La solution Next-Generation Firewall comprend des moteurs Next-Generation Firewall, des éléments de serveur SMC et des éléments d'interface utilisateur SMC.
Centre de gestion de la sécurité (SMC)	Le SMC (*Security Management Center*) est l'élément de gestion de la solution Next-Generation Firewall. Le SMC gère et contrôle les autres éléments du système.
Serveur de gestion	Le serveur de gestion est l'élément central de l'administration du système.
Serveur de journaux	Les serveurs de journaux (*Log Servers*) stockent les journaux de trafic qui peuvent être gérés et compilés dans des rapports. Les serveurs de journaux mettent également en corrélation les événements, surveillent l'état des moteurs NGFW, affichent des statistiques en temps réel et transmettent les journaux à des appareils tiers.
Moteurs Next-Generation Firewall (Moteurs NGFW)	Les moteurs Next-Generation Firewall inspectent également le trafic. Ils sont utilisés pour configurer le contrôle d'accès aux ressources et pour surveiller les actions des utilisateurs et des administrateurs. Les moteurs du Next-Generation Firewall assignés à un rôle Firewall/VPN peuvent également être utilisés comme passerelles VPN.
Advanced Malware Detection (AMD)	Forcepoint AMD détecte les menaces avancées en analysant le comportement des fichiers. Les moteurs NGFW peuvent être configurés pour envoyer des fichiers vers AMD pour y être analysés.
Endpoint Context Agent (ECA)	ECA collecte des informations sur les utilisateurs et les applications par connexion pour les clients terminaux Windows. Vous pouvez intégrer ECA à Forcepoint NGFW pour recevoir des informations sur les utilisateurs et les applications des terminaux clients Windows qui se connectent via un moteur NGFW géré par le SMC. Vous pouvez utiliser ces informations comme critères pour le contrôle et la surveillance des accès et pour créer des rapports.
Forcepoint User ID Service (FUID)	Forcepoint User ID Service collecte des informations sur les utilisateurs, les groupes et les adresses IP à partir des serveurs Windows Active Directory (AD) et des serveurs Microsoft Exchange. Vous pouvez intégrer Forcepoint User ID Service avec Forcepoint NGFW et utiliser les informations que le Forcepoint User ID Service fournit pour surveiller les utilisateurs et configurer le contrôle d'accès.

Attributs des données personnelles

TABLE 1 : Attributs de données personnelles pour les journaux d'accès dans le SMC

Les données personnelles contenues dans cet ensemble de données ne peuvent pas être anonymisées, car cela contreviendrait aux meilleures pratiques en matière de sécurité en neutralisant les journaux d'audit qui notent les accès au réseau et les incidents d'inspection. La collecte de ces journaux est toutefois facultative.

Attribut	Exigence
Adresse IP	En option
Nom de connexion et domaine de l'utilisateur	En option

TABLEAU 2 : Attributs de données personnelles pour les journaux d'audit dans le SMC

Les données personnelles de cet ensemble de données ne peuvent pas être anonymisées, car cela empêcherait le bon fonctionnement de la politique de sécurité. Les journaux d'audit ne peuvent pas être désactivés, mais ils peuvent être supprimés via les tâches de gestion des journaux programmées par le SMC ou en supprimant les données des journaux d'audit du disque.

Attribut	Exigence
Nom de connexion de l'administrateur	Obligatoire
Adresse IP Client Administrateur	Obligatoire

TABLEAU 3 : Attributs de données personnelles pour User ID Service

Les données personnelles de cet ensemble de données sont mises en miroir à partir de l'environnement Microsoft Active Directory configuré. Elles sont automatiquement supprimées lorsqu'elles sont retirées de l'AD de Microsoft. Les données personnelles de cet ensemble de données ne peuvent pas être anonymisées, car cela contreviendrait aux meilleures pratiques en matière de sécurité en empêchant l'appariement des utilisateurs dans la politique d'accès au réseau. La désinstallation du serveur FUID supprimera également toutes les données mises en cache dans l'installation FUID.

Attribut
Nom de connexion et domaine de l'utilisateur
Membres du groupe AD de l'utilisateur
Adresse IP de l'utilisateur (telle que vue par le contrôleur de domaine AD)
Adresse courriel de l'utilisateur