
clavister
SECURITY BY
SWEDEN
CONNECTER
PROTÉGER
PRÉVENIR
SÉCURITÉ POUR LES ENTREPRISES -
GUIDE DES CAS D'UTILISATION

Un monde qui communique, fondé sur la confiance et la sécurité.

La vision de Clavister

ASSURER LA CONTINUITÉ D'AFFAIRES

Clavister sécurise et protège les réseaux d'entreprise et de fournisseurs de service, et assure la continuité d'affaires grâce à une suite de produits qui couvre une multitude de cas d'utilisation

La cybersécurité est désormais perçue comme l'une des menaces majeures pesant sur l'économie mondiale, et devrait représenter 6 mille milliards de dollars de coûts annuels d'ici 2021 (source : Cybersecurity ventures). Clavister fournit à des entreprises réparties des solutions qui protègent et connectent leurs affaires en toute sécurité. Nos produits sont conçus en Suède. Ils sont garantis sans « backdoors » et ne sont pas basés sur des systèmes d'exploitation standard.

Nos solutions tout incluses sont adaptées à de multiples cas d'utilisation qu'il s'agisse de fournir une connexion sécurisée, de protéger des différentes menaces ou de d'appliquer des mesures préventives afin de restreindre l'utilisation inappropriée d'un réseau. Elles sont fournies au sein d'équipements adaptés aux petits comme aux grands bureaux mais également de façon virtualisée. Les solutions Clavister peuvent être gérées en interne par un service informatique ou bien par des infogérants locaux spécialisés.

Avec son siège à Örnsköldsvik en Suède et des bureaux en Scandinavie, en Allemagne, au Japon et en Asie du Sud, Clavister compte à son actif plus de 200.000 installations et des clients dans 154 pays. Nos solutions sont vendues à travers des contrats équipementiers avec Nokia, D-Link et autres.

L'offre Clavister

Le pare-feu de dernière génération Clavister est fourni avec un système de licence extrêmement simple qui fait fi des licences utilisateur, par fonctionnalité et autres modularités.
C'est au contraire un modèle bipartite qui est proposé pour tous les cas de figure : fonctionnalités basiques ou avancées. Dans les deux cas, la gestion centralisée est fournie afin d'assurer une maintenance efficace et des options de configuration flexibles.

Cette offre permet de fournir à des entreprises de toutes tailles une solution extrêmement efficace de pare-feu de dernière génération clé en main comprenant dans un unique boîtier les classiques fonctionnalités de gestion unifiée des menaces. Avec Clavister vous déployez une solution de sécurité qui vous apporte à la fois sérénité et coûts réduits.

Écosystème

Clavister intègre des solutions de fournisseurs de technologie de pointe dans leur domaine. L'écosystème Clavister a pour but de fournir les meilleures des solutions possibles. Pour cela il inclut :

- **McAfee (Intel Security) pour le système de prévention des intrusions**
- **Bitdefender pour l'antivirus**
- **Webroot pour la réputation IP**
- **ContentKeeper pour le filtrage de contenus Web**
- **Qosmos par ENEA pour le contrôle applicatif et l'inspection des paquets en profondeur**
- **Bitdefender pour la protection des points d'accès**

McAfee WEBROOT ContentKeeper ENEA Bitdefender

Les deux formules de souscription sont les suivantes :

Souscription Produit Clavister — CPS
La souscription basique donnant droit au support technique 24h/24h 7j/7j et le remplacement matériel au jour suivant ouvré.
Les mises à jour sont incluses et les différents logiciels sont conçus pour répondre à la majorité des cas d'utilisation.

Souscription Sécurité Clavister — CSS
Inclus CPS plus l'accès aux fonctionnalités suivantes : protection contre les attaques réseau/serveur, protection avancée contre les cybermenaces, blocage de contenus Web et contrôle applicatif.

Les produits Clavister sont utilisés pour répondre à des problématiques de sécurité pour tout un ensemble de différents cas d'utilisation. Dans le présent livre, nous présentons quelques-uns des cas les plus plébiscités et décrivons leurs avantages.

CONNECTER

Interconnecter des sites d'entreprise avec un souci particulier pour la sécurité et la continuité d'affaires.

PROTÉGER

Inspecter le trafic et son comportement dans le but de détecter les menaces pesant sur vos actifs numériques.

PRÉVENIR

Mettre en place mesures préventives et règles afin de réduire le risque que des utilisateurs mettent involontairement en péril le périmètre numérique de votre entreprise.

« D'ici 2020, plus de 50% des remplacements d'infrastructure de réseaux étendus feront intervenir des SD-WAN plutôt que des routeurs traditionnels (la part actuelle représentant 2%) » - Gartner

Réseaux privés virtuels sécurisés et fiables

Connecter des succursales ou des emplacements distants de façon sûre et efficace

Le fonctionnement des entreprises repose sur l'interconnectivité de leurs différents sites. Elles ont donc besoin d'une solution à la fois robuste, fiable et sécurisée. Dans un environnement de bureaux distribués la communication en temps réel entre systèmes est la clé de l'intelligence d'affaires et des opportunités. Autrefois, les entreprises louaient des lignes privées ou optaient pour des solutions de commutation multiprotocole par étiquetage (MPLS).

Ces recours se sont avérés contraignants, coûteux et exigeaient souvent de n'employer qu'un seul fournisseur télécom. Les différents impératifs en matière de flexibilité et de réduction des coûts ont favorisé l'utilisation généralisée de réseaux privés virtuels plutôt que de connexions Internet classiques. Les progrès permis par les solutions cloud ont introduit des solutions clé en main dites de réseaux étendus à définition logicielle (SD-WAN).

La solution

La solution de SD-WAN sécurisée de Clavister allie la solution réseaux privés virtuels sécurisés et fiables à d'autres telles que la protection du périmètre et le routage, la redondance et la répartition de charge. Elle est fournie en version logicielle prête à être déployée sur le cloud ou toute une gamme d'équipements dédiés. Un réseau virtuel entre sites peut facilement être mis en place grâce à des outils de gestion permettant une communication sécurisée entre sites et cloud.

La plus petite des installations de Clavister relie tout juste deux sites. La plus importante en relie 3000 à l'aide de plus de 10000 tunnels VPN individuels. Cette solution qui emploie une gestion holiste et le routage par politique est à la fois simple, flexible et évolutive.

Le résultat

Les entreprises utilisant les solutions de réseau privé SD-WAN peuvent faire une économie significative en termes de coûts opérationnels par comparaison à l'emploi de lignes louées ou de solutions faisant intervenir le MPLS. Qui plus est, contrairement au MPLS, le fournisseur d'accès Internet peut être différent pour chacun des sites. Un large choix de modes de transport (câble, DSL, fibre et 4G) peuvent être employés ce qui offre un avantage supplémentaire en termes de flexibilité et de réduction des coûts.

Vous pouvez en lire davantage à propos de la solution SD-WAN de Clavister ici :

www.clavister.com/sd-wan

Routage, redondance et répartition de charge

Éviter les périodes d'indisponibilité et assurer la continuité d'affaires

L'efficacité opérationnelle des entreprises repose sur leur infrastructure de communication. La moindre période d'indisponibilité de connexion peut nuire à la productivité, voire rendre injoignable un site distant critique. Du fait de la dépendance croissante des affaires en termes de connectivité, c'est l'ensemble des effectifs qui risque d'être rendu improductif.

La fonctionnalité de routage de Clavister a été décrite comme à la fois simple et à la pointe du progrès dans toutes les enquêtes effectuées auprès de nos clients depuis 1997.

La solution

Avec l'infrastructure appropriée, les entreprises peuvent si nécessaire dédier des connexions secondaires de moindre coût (comme le câble, la LNA ou la 3G) comme solution de secours. Au sein d'installations plus importantes, le pare-feu peut agir comme routeur et effectuer des décisions complexes avec un effort de configuration minime.

Le résultat

Les fonctionnalités intégrées de routage et de répartition de charge assurent la continuité d'affaires par la voie la plus rentable. Ceci facilite les tâches de maintenance et de migration des techniciens informatiques et rend superflu le recours à des équipements tiers.

Vous pouvez en lire davantage à propos de la fonctionnalité de routage et de répartition de charge de Clavister ici :
www.clavister.com/routing

« Seules 3% des entreprises interrogées par Gartner disposent d'une protection anti logiciels malveillants pour les appareils Android et seulement 1% pour les appareils iOS - Gartner

Zones réseau sécurisées

Segmenter le réseau afin de protéger les actifs numériques des entreprises

Les employés souhaitent pouvoir apporter leurs appareils personnels au bureau et de pouvoir les connecter à l'infrastructure réseau. Toutefois, ces appareils sont rarement pris en charge par les administrateurs et ne bénéficient donc pas du même niveau de protection que ceux fournis par l'entreprise. Ceci constitue un risque pesant sur les systèmes internes, au sein même du périmètre sécurisé.

La solution

La solution est de segmenter votre réseau en plusieurs zones et de contrôler strictement le trafic qui est permis entre elles. De façon complémentaire, il est possible de mettre en place un périmètre sécurisé autour des applications les plus critiques telles que bases de données, serveurs de fichiers et collecticiels.

Le résultat

En protégeant l'ensemble de vos actifs numériques à l'aide d'un pare-feu virtuel dédié, vous obtenez un contrôle complet du trafic au sein même de votre réseau. Du fait de leur empreinte mémoire minime, les solutions virtualisées Clavister sont peu exigeantes en ressources ce qui les rend idéales dans le cadre d'infrastructures hyperviseur .

Vous pouvez en lire davantage à propos des zones réseau sécurisées Clavister ici :
www.clavister.com/zones

Répartition de la charge serveur

Simplifier l'évolutivité et permettre la maintenance préventive

Toute infrastructure informatique comprend des composants critiques qui justifient la mise en place de la haute disponibilité, c'est à dire d'une redondance. Cela a deux buts : de garantir une continuité de service lorsqu'un serveur est victime d'un problème mais également de permettre une maintenance simplifiée et proactive. La redondance peut être intégrée à la couche applicative ou mise en place à l'aide d'un DNS round-robin, mais ceci ajoute en complexité et ne permet pas toujours un contrôle effectif.

La solution

Utiliser un pare-feu qui intègre la fonctionnalité de répartition de charge serveur permet d'obtenir à la fois haute disponibilité et contrôle. Cette solution permet, sans avoir à recréer des paquets, de répartir la charge de trafics tels que HTTP(S), DNS et LDAP en fonction du taux de connexion ou de l'utilisation de ressources. Le pare-feu peut recevoir des informations via une API. La répartition de charge peut donc être rendue dynamique par le biais de processus tiers. Il peut s'agir de réduire l'impact de files d'attente de courriels, de l'espace disque, de l'utilisation du processeur, etc.

Le résultat

La fonctionnalité intégrée de répartition de charge serveur permet à l'administrateur de répondre au besoin de haute disponibilité sans avoir recours à des solutions spécialisées.
Cela facilite la possibilité de mettre en place une maintenance proactive sans temps mort pendant des heures normales et contribue à rendre l'infrastructure évolutive.

La solution de pare-feux Clavister permet de confirmer la disponibilité d'un serveur de plusieurs façons.
Un simple ping ICMP vérifie si le serveur répond. Le monitoring TCP est en charge de valider si des services donnés répondent sur leurs ports respectifs.
La supervision HTTP permet d'interroger une URL spécifique et ainsi de valider la réponse. Ceci, avec l'emploi de scripts exécutés depuis le serveur peut vérifier si une base de données en back-end fonctionne correctement et effectuer un éventuel basculement.

Vous pouvez en lire davantage à propos de la fonctionnalité de répartition de charge de Clavister ici :
www.clavister.com/slb

Accès distant flexible

Donner les moyens sécurisés de travailler à distance

Notre façon de travailler a changé drastiquement : nous sommes désormais mobiles et mondiaux, nous utilisons nos appareils personnels et accédons à nos ressources à travers des connexions non sécurisées telles que bornes Wi-Fi et autres points d'accès. Indépendamment d'où et comment, le fait de disposer d'une solution permettant d'administrer et de confirmer des accès distants sécurisés pour une variété de dispositifs est l'une des clés du succès et de la protection des données.

La solution

Une solution d'accès distant flexible se doit d'être compatible avec une gamme de technologies au nombres desquelles IPsec, SSL, L2TP/PPTP afin d'assurer une connectivité même au sein des environnements distants les plus restrictifs. La compatibilité avec les clients RPV fournis avec Windows, Mac et autres systèmes d'exploitation mobiles permet à tout appareil de pouvoir se connecter. Le client SSL VPN Clavister conçu à cet effet permet une simplicité d'utilisation à la fois pour l'utilisateur et pour l'administrateur.

Le résultat

Les solutions d'accès distant par RPV de Clavister sont rapides à mettre en place sur tous vos appareils sans nécessiter l'intervention du service informatique. Vous aurez l'assurance que toutes vos données sont partagées de façon confidentielle et sans risque d'injection de code malveillant pendant leur transit. La solution Clavister, virtuelle ou non, permet à votre réseau (et employés) de fonctionner à plein régime sans latence.

Vous pouvez en lire davantage à propos des solutions RPV de Clavister ici :

www.clavister.com/vpn

Protection du périmètre

Un pare-feu qui protège ressources informatiques et utilisateurs

Hackers, virus, logiciels rançonneurs, vol de données, espionnage industriel et même cyberattaques commanditées par des gouvernements... La liste des cybermenaces pouvant porter préjudice à votre entreprise n'en finit pas de s'allonger. Le forum économique mondial a estimé les cyberattaques comme étant le 3ème type d'incident le plus susceptible d'avoir lieu et le 6ème le plus dévastateur en termes économiques. Le défi n'est pas simplement de rendre le réseau plus sûr, mais également de le rendre à la fois efficace et productif.

La solution

La nécessité ici est de disposer d'un pare-feu qui surveille et contrôle le trafic entrant et sortant via un ensemble de règles de sécurité intelligentes. Pour une protection idéale, il est indispensable de spécifier très exactement quel type de trafic est autorisé à l'exception de tout le reste. Si la place la plus évidente pour un pare-feu est la bordure avec Internet, il est également vrai que son déploiement à l'intérieur du réseau d'entreprise peut accroître le niveau de sécurité de différents segments.

Le résultat

En version virtualisée ou matérielle, Clavister apporte la sérénité à tout l'ensemble de votre réseau. Toutes les versions professionnelles incluent une option de haute disponibilité afin de garantir la continuité d'affaires, même durant les périodes de maintenance.

Les pare-feux de dernière génération de Clavister sont « Made in Sweden : » et basés sur notre système d'exploitation propriétaire. Ils sont donc garantis sans backdoors et ne sont pas sujets aux vulnérabilités apparaissant continuellement sur des systèmes d'exploitation tels que Windows et Linux. Nos pare-feux comprennent un ensemble de services aux nombres desquels traduction d'adresses réseau, allocation dynamique d'adresses et authentification des utilisateurs intégrée à Microsoft Active Directory (« user awareness : »).

Vous pouvez en lire davantage à propos de la solution de protection du périmètre de Clavister ici :
www.clavister.com/firewall

Protection contre les attaques réseau/serveur

Un système de prévention et de détection des intrusions et une protection contre le déni de service

En utilisant l'un des nombreux outils dédiés disponibles, il est facile de mener une attaque contre des centaines, voire des milliers d'ordinateurs, et de submerger de trafic à peu près n'importe quel système ou pare-feu afin de le mettre hors ligne ou de l'obliger à fonctionner à vitesse réduite.
Ce ne sont pas seulement les sites de vente en ligne qui en sont victimes, mais également des entreprises dotées de systèmes de sécurité dits à grande échelle qui font l'objet de demandes de rançon. Dans la plupart des cas, l'entreprise finit par payer pour se débarrasser de la menace quel que soit le montant exigé. Loin d'être optimal cela est toujours moins coûteux que des jours entiers d'indisponibilité risquant de causer des dommages irréparables à une marque.

La solution

Clavister fournit une protection sur mesure, adaptée à vos activités. Nous créons un système de défense qui ne se contente pas de bloquer le trafic, mais s'avère également indétectable et flexible. Même lors d'une attaque DDoS massive qui met tout à l'arrêt, les pare-feux de dernière génération de Clavister font en sorte que votre réseau interne et les connexions Internet de secours restent opérationnels. Les attaques DoS dirigées contre des services protégés par un pare-feu peuvent être contrées avec la gestion de trafic et la limitation de débit.

Le résultat

Les pare-feux de dernière génération de Clavister font plus que proposer une multitude de stratégies pour contrer ou réduire l'impact d'une attaque DoS menée contre un serveur protégé par un pare-feu.
Cette solution permet d'assurer que le fonctionnement de votre entreprise ne soit pas affecté par ce type d'attaques et que vos employés puissent se concentrer sur la continuité.

Vous pouvez en lire davantage à propos de la fonctionnalité de protection contre le déni de service ici :
www.clavister.com/server-protection

« 4% des gens cliquent invariablement lors d'opérations d'hameçonnage. »

L'institut AV-TEST recense plus de 250000 nouveaux programmes malveillants par jour.

Protection avancée contre les cybermenaces

Système de prévention des intrusions intégré avec antivirus et détection de logiciels malveillants

L'un des buts de hackers animés de mauvaises intentions est de transmettre du code ou des liens à travers un pare-feu afin de faire en sorte que des utilisateurs créent un trou de sécurité depuis l'intérieur. Bien souvent, ceci leur permet de prendre le contrôle de tout ou partie de l'équipement de l'utilisateur ce qui leur fournit une plateforme depuis laquelle explorer librement les actifs numériques de votre entreprise.

Ces attaques sont souvent très bien préparées et même le plus prudent des utilisateurs peut finir, contre son gré, par aider le hacker.

La solution

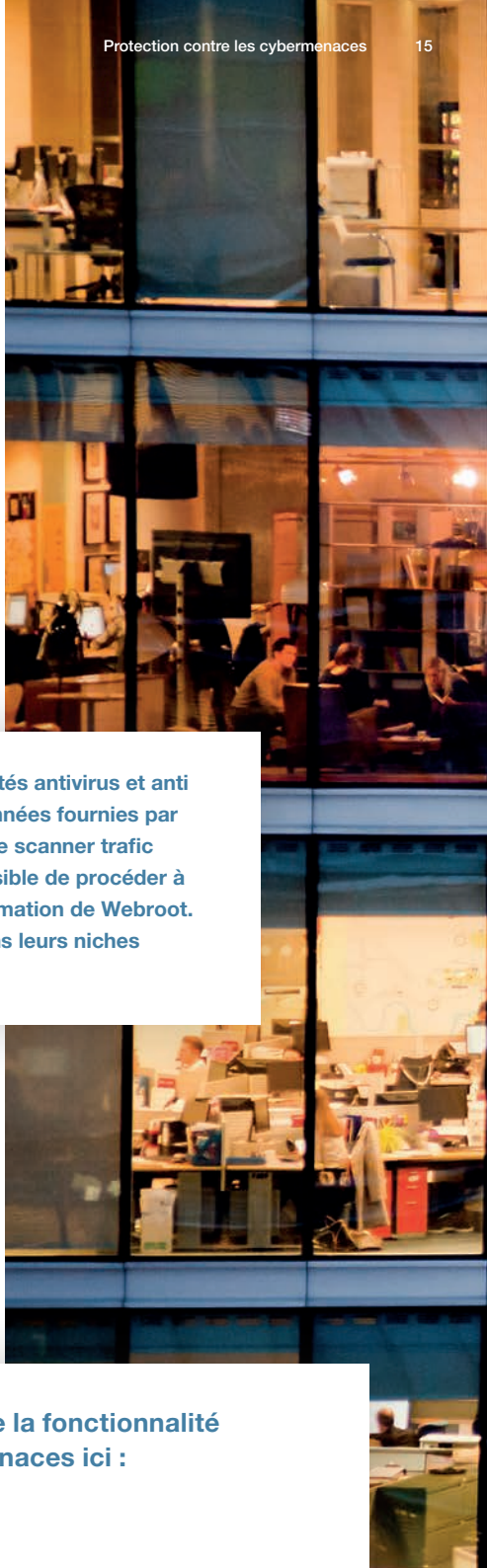
Les pare-feux de dernière génération fournissent une protection contre les menaces de plusieurs façons. Le trafic non sécurisé peut être analysé dans le but de détecter virus et logiciels malveillants par l'utilisation de bases de données de signatures, de l'intelligence artificielle et la détection de comportement. Le trafic impliqué par les courriels et l'usage du web en particulier font l'objet d'un tri rigoureux afin de repérer menaces connues ou comportements suspects. Par exemple, dans les courriels les pièces jointes doivent être analysées, leur provenance et la destination des liens vérifiée.

Toute adresse IPv4 publique est unique et une collecte de renseignements quant à leur réputation (en d'autres termes leur fiabilité) peut être organisée. En fonction de cette réputation le pare-feu peut bloquer le trafic relatif aux sites les moins recommendables ou effectuer une analyse supplémentaire du contenu de ces zones à risque.

Les pare-feux Clavister comprennent des fonctionnalités antivirus et anti logiciels malveillants s'appuyant sur des bases de données fournies par Kaspersky et McAfee / Intel Security qui permettent de scanner trafic web, FTP et courriel en temps réel. De plus, il est possible de procéder à la vérification de réputation IP grâce à l'apport d'information de Webroot. Tous nos fournisseurs sont des leaders mondiaux dans leurs niches respectives.

Le résultat

Avec un pare-feu de dernière génération Clavister en place, vous protégez votre réseau et vos utilisateurs des hackers et autres intrus. Le contenu malveillant est bloqué et le trafic depuis et vers des sites de réputation douteuse peut être évité. Les utilisateurs peuvent concentrer leurs efforts sur l'ajout de valeur plutôt que de d'avoir à se préoccuper de courriels et de contenus web malveillants.



Vous pouvez en lire davantage à propos de la fonctionnalité de protection avancée contre les cybermenaces ici :

www.clavister.com/threat-protection

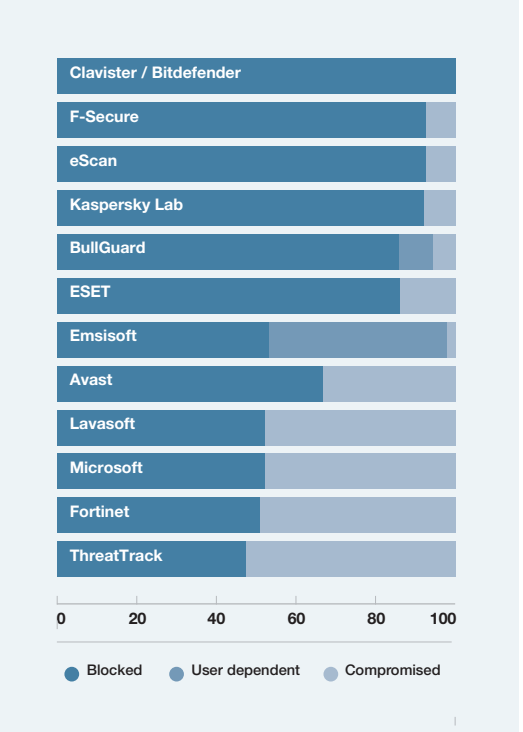
Protection des utilisateurs finaux

Bloquer les menaces et détecter la perte de données depuis les points d'accès

Les appareils mobiles étant amenés à sortir de votre périmètre sécurisé, il est très probable qu'ils se trouvent exposés lorsqu'ils sont connectés à d'autres réseaux.
Lors de leurs déplacements, ces appareils risquent d'être infectés, et dans le pire des cas cette infection n'est détectée qu'une fois que l'appareil est reconnecté au réseau d'entreprise. Le virus ou logiciel malveillant obtient alors un accès illimité à l'environnement interne, une situation à la fois indésirable et risquée.

La solution

La solution de défense des points d'accès de Clavister est fournie par le leader du domaine Bitdefender et repose sur l'intelligence artificielle, l'analyse de comportement et des bases de données de signatures pour la détection de virus et logiciels malveillants. Ce logiciel permet aussi un protection contre la fuite de données (DLP), assurant la conformité au RGPD et la préservation de données sensibles.
Administrée depuis le cloud et facile à déployer, cette solution a été établie année après année comme la meilleure solution sur le marché par les principaux laboratoires de test indépendants.



Source : AV-Comparatives, test de comportement/heuristique

Vous pouvez en lire davantage à propos de la solution pour la protection des points d'accès ici :
www.clavister.com/endpoint

Blocage de contenu web

Restreindre l'accès aux contenus inappropriés et se mettre en conformité avec la règlementation

Mise à disposition de réseaux publics, politiques d'entreprise ou conformité aux lois, les raisons de restreindre l'accès à certains types de sites sont nombreuses.

La solution

Les pare-feux Clavister comprennent un moteur de classification de contenu qui compare en temps réel URL et noms d'hôtes à une base de données de catégories, le flux de trafic est ensuite étiqueté en fonction de ce résultat. Les règles de pare-feu permettent ensuite d'adopter l'action appropriée ou de simplement enregistrer l'évènement dans le but de collecter des statistiques. Ainsi, les administrateurs peuvent facilement bloquer l'accès à du contenu classé XXX ou aux réseaux sociaux durant des horaires planifiables.

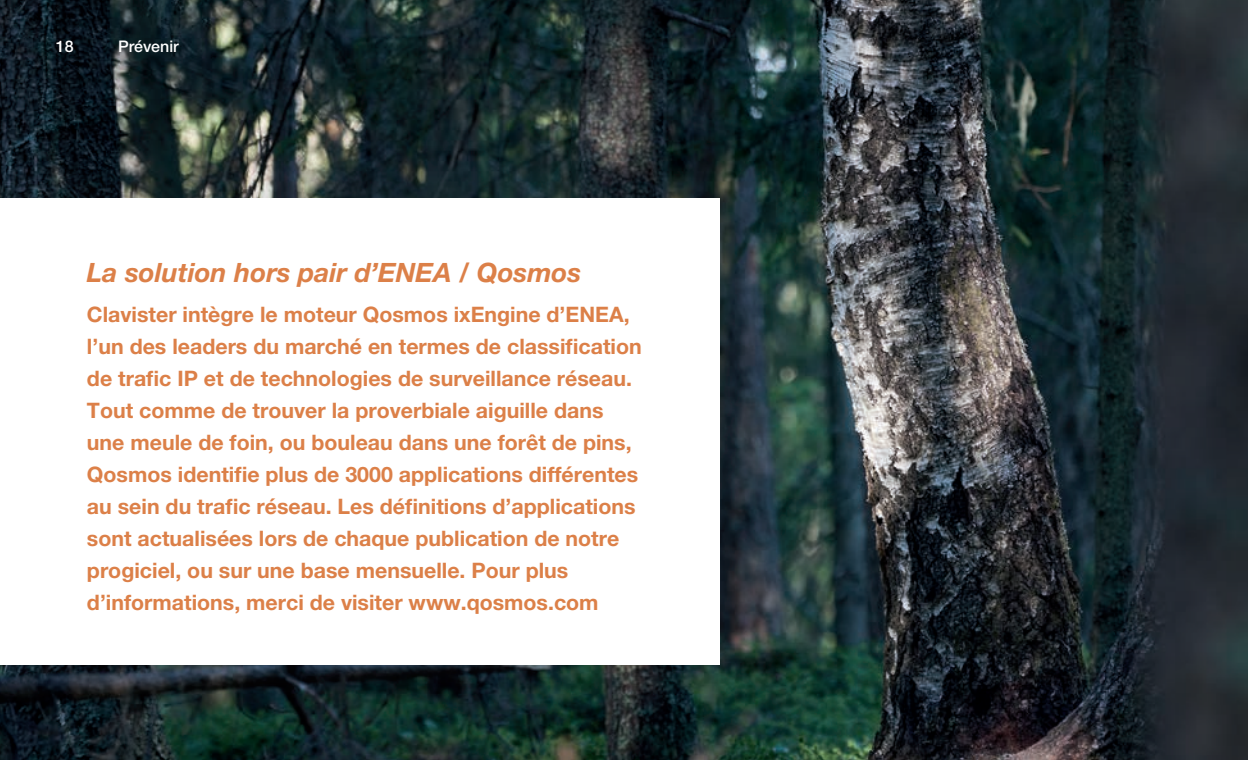
Dans un souci d'exactitude, la base de données est actualisée plusieurs fois par jour afin de garantir que les nouveaux sites soient continuellement ajoutés.

Si vous faites gagner 1 heure par semaine à 100 employés en restreignant l'accès à des sites non strictement liés au travail vous pouvez facilement espérer économiser 100000 EUR par an.

Le résultat

En vous assurant que vos ressources sont utilisées pour les bonnes raisons non seulement vous épargnerez des situations embarrassantes, mais vous gagnerez aussi en productivité.

Vous pouvez en lire davantage à propos du filtrage de contenu Web de Clavister ici :
www.clavister.com/filtering



La solution hors pair d'ENEA / Qosmos

Clavister intègre le moteur Qosmos ixEngine d'ENEA, l'un des leaders du marché en termes de classification de trafic IP et de technologies de surveillance réseau. Tout comme de trouver la proverbiale aiguille dans une meule de foin, ou bouleau dans une forêt de pins, Qosmos identifie plus de 3000 applications différentes au sein du trafic réseau. Les définitions d'applications sont actualisées lors de chaque publication de notre progiciel, ou sur une base mensuelle. Pour plus d'informations, merci de visiter www.qosmos.com

Visibilité et contrôle applicatif

Contrôler applications et comportement des utilisateurs

Les responsables informatiques de toute entreprise se doivent de maîtriser l'utilisation de leur réseau afin de garantir qu'il soit employé à des finalités professionnelles. Certaines applications ont peut-être même besoin d'être priorisées alors que d'autres, considérées comme à risque, devraient être préventivement bloquées. BitTorrent, un client de transfert de données pair à pair, ou les applications liées à Tor, permettant d'accéder au dark web et couramment utilisé par des virus malveillants pour extraire des données de votre réseau en sont deux exemples. L'usage non autorisé de ressources serveur pour le minage de cryptomonnaies, qui impacte fortement la facture énergétique, en est une autre. Ces applications devraient être bloquées.

Tout trafic n'est pas du web. Une large part du trafic transite via une variété de ports ou utilise des protocoles customisés pour communiquer entre serveurs, clients et pairs. C'est pourquoi il est nécessaire d'avoir recours à un moteur d'identification d'applications (autrement appelé inspection des paquets en profondeur ou DPI) pour détecter une application ou service avec précision. Des applications telles que WebEx ou Skype par exemple peuvent être identifiées et leur trafic priorisé afin d'augmenter la qualité des conversations.

Le contrôle applicatif est indispensable pour améliorer l'expérience utilisateur.

Afin de pouvoir administrer le trafic de vos utilisateurs de façon contrôlée et d'identifier des applications, les pare-feu de dernière génération Clavister intègrent l'une des meilleures technologies en termes d'inspection des paquets en profondeur. De plus, Clavister a procédé à une classification en niveaux de risques, ce qui rend la tâche de blocage applicatif plus simple encore.

OUI ! Le trafic crypté peut être classifié

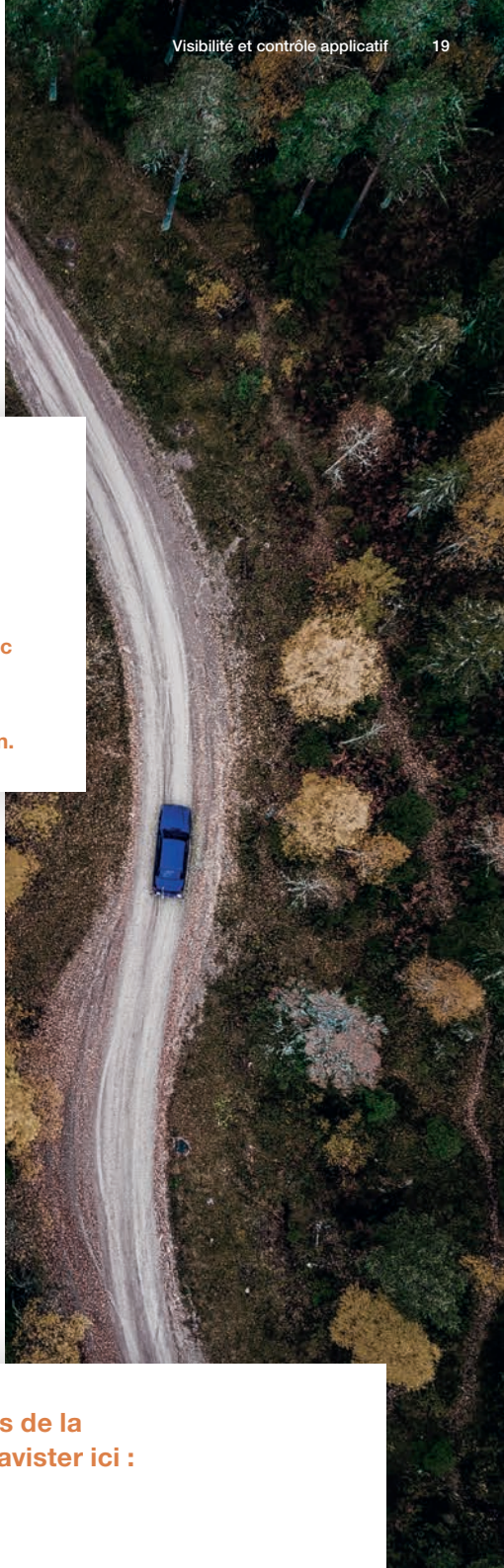
De nos jours, la majeure partie du trafic est cryptée. Toutefois, à l'aide du nom du serveur (SNI) présent dans tout certificat SSL/TLS, par l'emploi d'un protocole d'identification statistique (SPID) et par la recherche d'empreintes binaires dans le flux de trafic le moteur d'inspection en profondeur présent dans un pare-feu de dernière génération Clavister peut détecter des applications avec 90-100% de précision.

L'Internet des objets (IoT)

La visibilité applicative est particulièrement adaptée à la gestion des objets connectés. À l'aide de politiques avancées, vous pouvez n'autoriser que ce que ces objets sont censés faire sur votre réseau. Ainsi, même si un dispositif donné est hacké, il ne pourra pas être utilisé comme levier pour accéder à d'autres ressources.

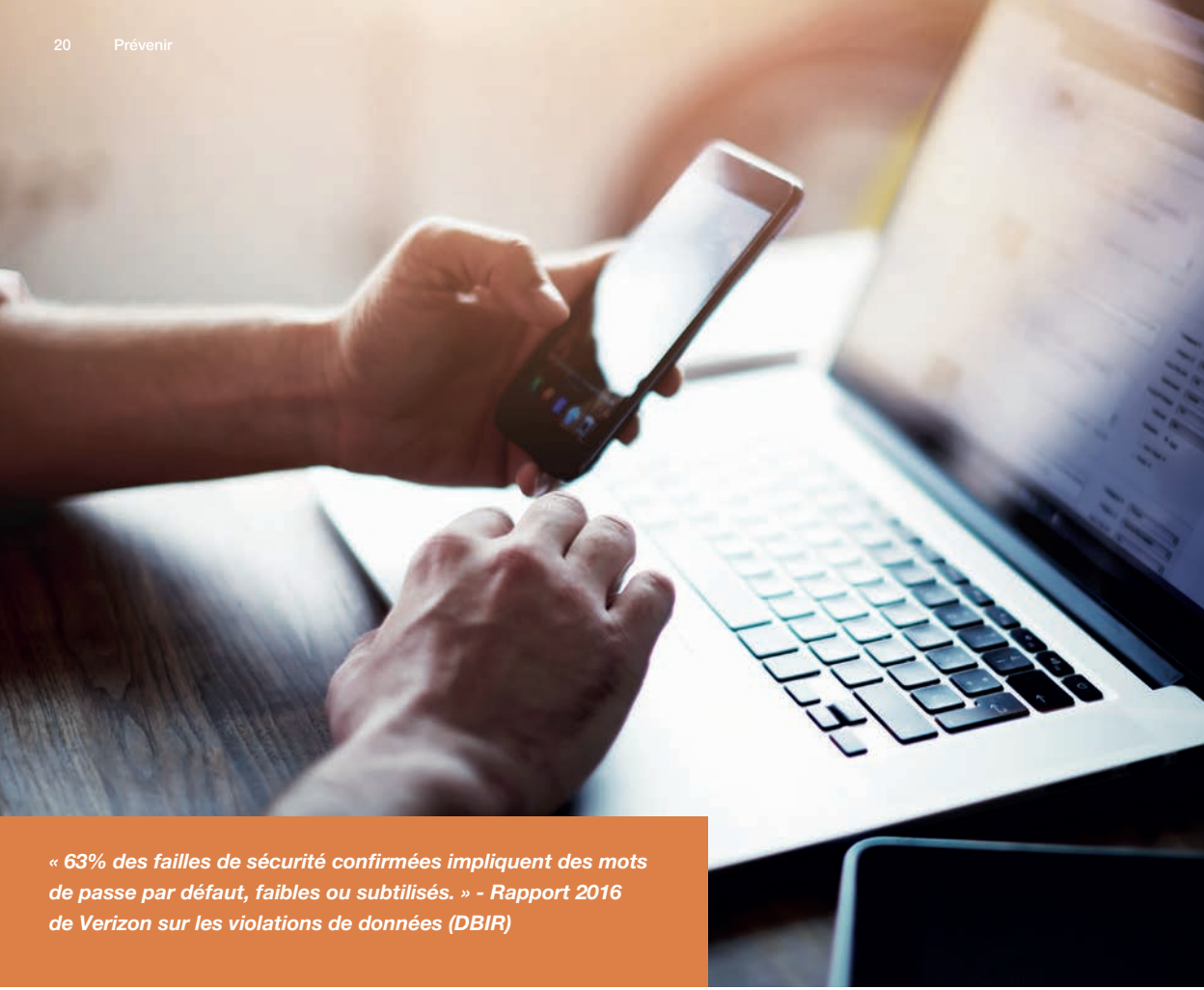
Le résultat

Le contrôle applicatif permet d'être extrêmement spécifique par rapport à ce qui est permis sur votre réseau. En augmentant ainsi le niveau de sécurité, vous vous permettez de pouvoir employer des nouvelles technologies au plus tôt, sans risques inutiles.



Vous pouvez en lire davantage à propos de la visibilité et du contrôle applicatif de Clavister ici :

www.clavister.com/dpi



« 63% des failles de sécurité confirmées impliquent des mots de passe par défaut, faibles ou subtilisés. » - Rapport 2016 de Verizon sur les violations de données (DBIR)

Authentification multi-facteur

Garantir l'authenticité des utilisateurs

Les utilisateurs font généralement peu de cas des mots de passe et en utilisent de trop simples. Ceci ouvre une voie facile pour hacker des comptes. Même si votre système est suffisamment sécurisé, c'est l'intégralité de votre infrastructure qui est en danger si jamais le moindre compte utilisateur est exploité. Ceci arrive souvent du fait que de nombreux d'utilisateurs réutilisent les mêmes mots de passe pour différents services. Un second périmètre de sécurité devrait exister afin de vérifier l'identité des utilisateurs.

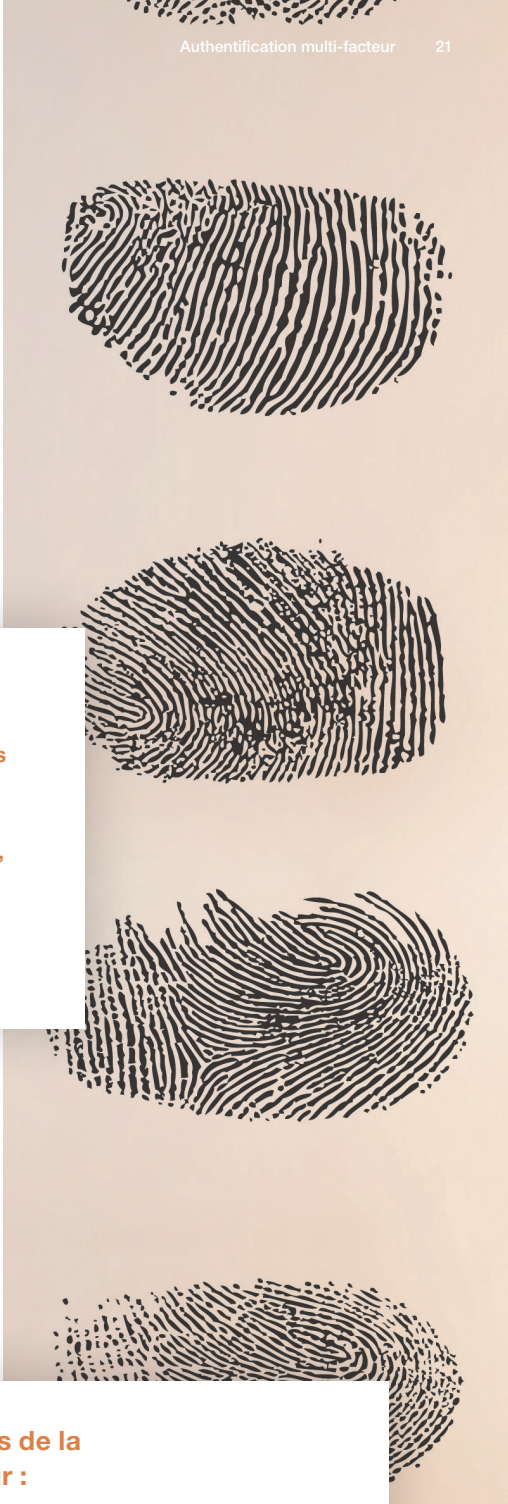
La solution

L'authentification multi-facteur ou à double-facteur est une façon simple et sécurisée pour vos utilisateurs de s'authentifier. Plusieurs méthodes hors bande peuvent être utilisées afin de confirmer l'identité d'un utilisateur. Cela peut impliquer mots de passe à usage unique, SMS, applications mobiles, jetons d'authentification ou certificats.

L'authentification multi-facteur (MFA) Clavister est utilisée par les plus importantes institutions suédoises. Ce produit comprend plusieurs méthodes permettant l'authentification : mots de passe à usage unique, SMS, courriels, applications mobiles, confirmation « one-touch », jetons d'authentification, certificats X.509, etc. Adaptable aux fonctionnalités de haute disponibilité, simple d'utilisation, c'est le niveau supérieur de sécurité dont votre entreprise a besoin.

Le résultat

Avec l'authentification multi-facteur vous obtenez plus de sécurité et il est facile pour l'administrateur de savoir qui est connecté et s'il s'agit bien des personnes supposées l'être. L'accès distant flexible permet à vos utilisateurs de travailler depuis n'importe où de façon sécurisée.



Vous pouvez en lire davantage à propos de la solution d'authentification multi-facteur :

www.clavister.com/mfa

Optimisation active du trafic

Prioriser le trafic et privilégier l'utilisation des ressources

Très souvent, les liens réseau saturent du fait de la manière peu soigneuse dont les applications font usage de la bande passante disponible. Par exemple, cela est typique des applications de partage ou synchronisation de fichiers et d'autres qui établissent en parallèle plusieurs sessions TCP afin de maximiser leur utilisation de bande passante.

En conséquence, il est impossible d'allouer un accès équitable à la bande passante pour tous, ce qui se traduit par une dégradation de service qui impacte les applications les plus vulnérables telles que VoIP et vidéoconférence.
Ceci aboutit à une qualité de communication médiocre, à des déconnexions et à une baisse généralisée de productivité

La solution

À la frontière du réseau votre pare-feu de dernière génération fait office de gardien décidant des différentes priorités de trafic en fonction du type et des utilisateurs. Un niveau de qualité de service peut être défini afin de garantir qu'une portion de la bande passante disponible soit réservée à des applications ou utilisateurs spécifiques.

Les pare-feux de dernière génération de Clavister permettent de différencier le trafic en détail. Des « pipes » virtuels peuvent être organisés en une structure réceptionnant le trafic et celle-ci peut faire appel aux fonctionnalités de détection d'applications ou d'authentification utilisateur afin de planifier l'utilisation de la bande passante.

Le résultat

Mettre en place une optimisation de trafic intelligente permet de faire face aux situations où les limites d'utilisation de bande passante sont atteintes. À titre d'exemple, les télé et vidéoconférences peuvent bénéficier d'une meilleure qualité et de moins d'interruptions aux dépends d'applications de synchronisation de fichiers telles que Dropbox dont le travail peut être ralenti sans que cela n'impacte leur fonctionnement.

Vous pouvez en lire davantage à propos de la différentiation du trafic en consultant notre livre blanc :

www.clavister.com/optimisation

L'importance d'être proactif

Protection du périmètre avancée et connexion sécurisée entre sites sont la base d'une infrastructure réseau solide. Mais bien souvent, les utilisateurs ont, à leur insu, un rôle clé dans les succès répétés de hackers tentant d'accéder aux actifs numériques et ressources d'une entreprise.

L'authentification multi-facteur contribue à résoudre le problème de mots de passe trop faibles ainsi qu'à simplifier l'accès aux différents systèmes de l'entreprise. Les responsables informatiques ont, eux, l'opportunité d'empêcher les utilisateurs de devenir des failles de sécurité en maîtrisant l'accès aux sites et applications à risque. Restreindre l'accès à des sites malveillants en fonction leur réputation et bloquer les applications destinées à accéder au dark web, au minage de cryptomonnaies et autres est un moyen de réduire les risques et de garantir que les ressources de l'entreprise soient destinées à l'usage prévu. Maîtriser le flux de trafic de façon détaillée permet également d'améliorer l'expérience de l'utilisateur en différentiant le trafic d'applications en temps réel critiques (comme par exemple la vidéoconférence) du trafic normal.

Il est temps de penser de façon proactive et d'implémenter des mesures préventives afin d'éviter des incidents de sécurité. Clavister fournit un des moyens avancés de répondre à des cas d'utilisation préventifs dont chacun, sans être expert, peut faire usage et en constater l'efficacité

clavister®

Spécificités de secteurs et tendances mondiales en cybersécurité

SÉCURITÉ POUR LES ENTREPRISES

Les vikings sont là, pour nous protéger

Clavister est une entreprise suédoise dédiée à la cybersécurité et qui est convaincue qu'une sécurité réseau robuste est l'affaire de tous. Prenant en compte la variété des écosystèmes, tout autant physiques que virtuels, nous défendons la continuité d'affaire et nous assurons que nos clients bénéficient d'une sécurité hors pair dans un monde de menaces toujours croissantes. Nous avons peut-être transformé nos épées en code mais nous conservons toujours l'esprit viking et la conviction que la meilleure cyberdéfense, c'est l'attaque.

La « suèditude » de Clavister nous distingue des autres

Les Suédois ont pour réputation d'être innovants, attentifs aux besoins et d'offrir un service client hors pair. Clavister emploie de talentueuses personnes de plus de 50 nationalités. Tout le développement et le support, eux, restent localisés en Suède. Ceci nous permet une flexibilité et une excellence plébiscitée par nos clients année après année. *Security By Sweden*, cela signifie des produits flexibles, pragmatiques et fiables qui sécurisent vos affaires.

#NoBackDoors

Tous les équipements Clavister sont fournis avec cOS Core, un système d'exploitation développé par Clavister. Ce système est propriétaire et intégralement développé en Suède. Grâce à ce niveau de contrôle total, Clavister peut garantir que ses pare-feux de dernière génération sont garantis à 100% sans backdoors.

Les vulnérabilités logicielles telles que "heartbleed", "Shellshock / bash", "Ghost" ou "FREAK", ainsi que des bogues open-source encore à découvrir, n'ont simplement pas cours dans les solutions Clavister. D'autres fournisseurs de solutions de sécurité ont, eux, été affectés par ces problèmes dans le passé (voir tableau ci-dessous).

Une suite logicielle unifiée pour tous les systèmes permet d'empêcher toute différence fonctionnelle entre plateformes, qu'elles soient matérielles ou virtuelles .

	Heartbleed	Shellshock/Bash	Ghost	Freak
Barracuda	●	●	●	●
Checkpoint	●	●	●	●
Cisco	●	●	●	●
Clavister	●	●	●	●
Cyberoam	●	●	–	●
Fortinet	●	●	●	●
Juniper	●	●	●	●
Palo Alto Networks	●	●	●	●
Securepoint	●	●	●	–
Sophos	●	●	●	●
Watchguard	●	●	●	●

● Aucun pare-feu affecté ● Tous les pare-feu affectés ● Quelques pare-feu affectés
● Tous pare-feux affectés, mais invulnérables selon fournisseur
– Pas d'information.

NOTE: Cet état était valide au moment d'occurrence de ces différentes attaques. Les fournisseurs peuvent ou non avoir publié des correctifs entretemps.

Merci de contacter le siège de Clavister : Sjögatan 6J, SE-891 60, Örnsköldsvik, Suède. Téléphone : +46 660-29 92 00
Pour plus d'informations, merci de visiter www.clavister.com ou de nous suivre sur Twitter @Clavister

Tendances mondiales en cybersécurité

De nos jours, la sécurité est devenue un sujet banal dans la presse non spécialisée. Le rapport 2018 sur les risques mondiaux du Forum économique mondial constate que les cyberattaques constituent le 3ème type d'incident le plus susceptible d'avoir lieu et le 6ème le plus dévastateur en termes économiques. Cela est comparable à des catastrophes telles que des phénomènes climatiques extrêmes ou des attentats !

Top 10 des risques en termes de **probabilité**

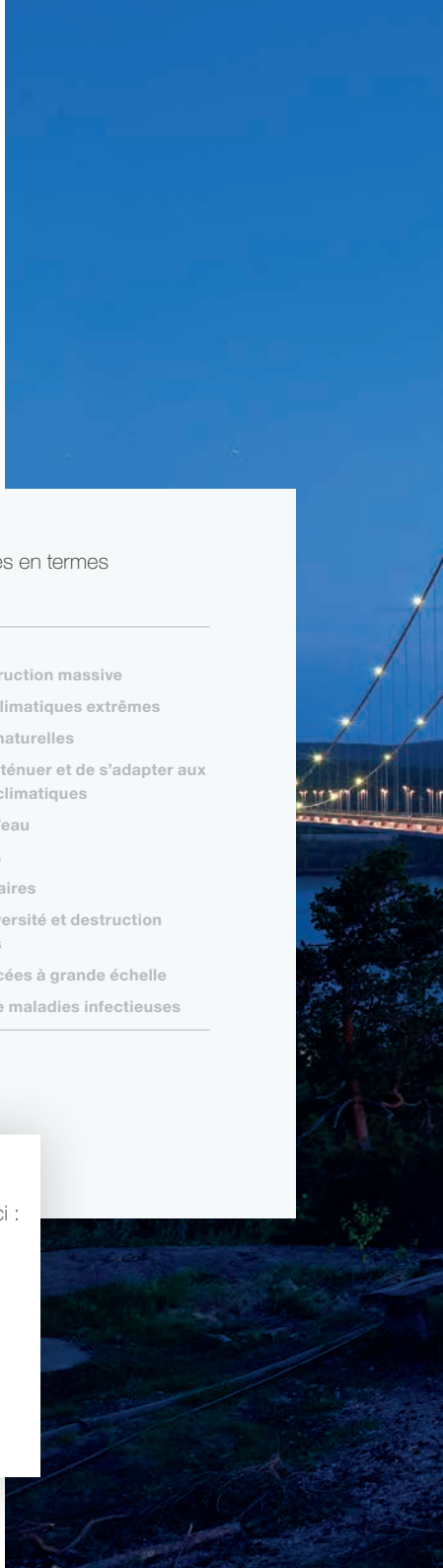
1. Phénomènes climatiques extrêmes
2. Catastrophes naturelles
3. **Cyberattaques**
4. **Vol de données ou fraudes**
5. Incapacité d'atténuer et de s'adapter aux changements climatiques
6. Migrations forcées à grande échelle
7. Catastrophes écologiques d'origine humaine
8. Attentats terroristes
9. Commerce illicite
10. Bulles spéculatives au sein d'une grande économie

Top 10 des risques en termes **d'impact**

1. Armes de destruction massive
2. Phénomènes climatiques extrêmes
3. Catastrophes naturelles
4. Incapacité d'atténuer et de s'adapter aux changements climatiques
5. Crises liées à l'eau
6. **Cyberattaques**
7. Crises alimentaires
8. Perte de biodiversité et destruction d'écosystèmes
9. Migrations forcées à grande échelle
10. Propagation de maladies infectieuses

Source : Rapport 2018 sur les risques mondiaux du Forum économique mondial
www.weforum.org/reports/the-global-risks-report-2018

Vous pouvez en lire davantage à propos de thèmes de sécurité particuliers ici :



Spécificités de secteurs

Chaque secteur d'activité est unique et toute solution nécessite de prendre en compte leurs besoins et règlementations. Le présent support s'articule autour des besoins des secteurs suivants :

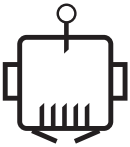
Logiciels rançonneurs

Des logiciels malveillants qui chiffrent vos données et empêchent le bon fonctionnement de vos systèmes

Dans un premier temps, une machine est infectée par un virus ou logiciel malveillant qui y est installé. Leur installation est souvent permise par le biais des utilisateurs en les faisant cliquer sur des liens douteux ou en leur faisant installer des logiciels non autorisés sur leurs systèmes. Une fois infectés, le hacker y publie un message du type « Vos fichiers ont été cryptés et sont inaccessibles. Photos, vidéos, documents, etc. Mais ne vous inquiétez pas, ils n'ont pas encore été effacés. Vous avez 24 heures pour payer 500 dollars en Bitcoins ». Pour donner du poids à leurs affirmations, il est courant de commencer par détruire quelques fichiers puis ensuite plus systématiquement, de façon cadencée et exponentielle. Si vous essayez de redémarrez votre ordinateur, le disque dur est détruit, même chose si vous ne payez pas dans les 72 heures.

De nombreux spécialistes ont tenté en vain de contrecarrer ces logiciels, la meilleure solution restant d'appliquer une protection à travers votre pare-feu et de faire des sauvegardes. Si vous êtes atteint, vous pouvez soit payer, soit voir votre disque dur détruit (et éventuellement en récupérer les données si vous les avez stockées hors ligne).

Vous pouvez en lire davantage à propos des ransomware ici :
www.clavister.com/ransomware



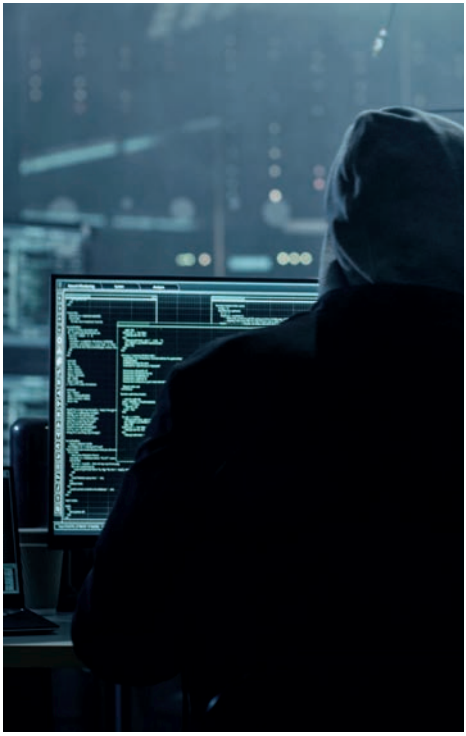
Botnets, menaces zero day

Du code malveillant exécuté depuis votre appareil permettant à un tiers d'y accéder et de le contrôler

Un botnet ou réseau de bots est un ensemble de systèmes interconnectés sur chacun desquels un ou plusieurs bots sont actifs.

Un bot, mot formé à partir de « robot », est un programme qui peut être contrôlé à distance afin d'accomplir une tâche déterminée. Les botnets ont généralement mauvaise presse puisqu'ils peuvent être utilisés dans le cadre d'attaques par déni de service distribuée (DDoS), de vol de données ou d'envoi de courrier indésirable et également puisqu'ils permettent à l'auteur d'une attaque d'accéder à une machine et à ses connexions.
Pour un hacker malveillant, un bot est un outil permettant l'utilisation de ressources locales ou comme levier pour accéder en profondeur à un réseau ou système informatique.

Un exploit jour zéro (également appelé *zero day ou 0-day*) est une cyberattaque ayant lieu aussitôt qu'une vulnérabilité logicielle a été découverte. Elle est typiquement exploitée avant qu'un correctif ait pu être publié par l'éditeur. Les exploits jour zéro sont souvent utilisés par des hackers afin d'installer sur des systèmes des bots dormants pouvant être utilisés ultérieurement dans le cadre d'une attaque.



Vous pouvez en lire davantage à propos de la protection contre les botnets et menaces zero day ici :
www.clavister.com/ipreputation

Attaques par déni de service distribuées (DDoS)

Surcharge de serveur ou de réseau d'origine multiple

Une attaque par déni de service (DoS) est une cyberattaque qui consiste à rendre indisponible un service ou un réseau pour ses utilisateurs prévus. Elle est effectuée en noyant un service donné sous un flot de requêtes qui surcharge les capacités du service ou réseau ou en exploitant des vulnérabilités de service.

Une attaque par déni de service distribuée (DDoS) se distingue par le fait qu'elle utilise un nombre important de différentes ressources afin de créer un flot simultané depuis plusieurs endroits.

Ces attaques ont beau être illégales dans la plupart des pays, il reste par définition difficile d'en identifier l'origine véritable. Au fur et à mesure que des outils d'attaque deviennent plus simples d'accès, le nombre d'entreprises victimes d'attaques ne fait qu'augmenter.

Du fait de la variété de types d'attaques la meilleure protection est obtenue grâce à la combinaison de différentes fonctionnalités. Certaines techniques de défense consistent à réduire ou réguler le débit et à effectuer un contrôle d'accès. Une infrastructure sécurisée se caractérise par un fonctionnement segmenté. Cela signifie que si une interface est surchargée cela n'impacte pas le reste d'entre-elles. En procédant de cette façon, certaines entreprises sont à même de continuer à fonctionner grâce à leurs connexions de secours malgré une attaque DDoS en cours sur leur connexion principale.

Slow DDoS

Toute surcharge d'un système n'est pas nécessairement l'œuvre de hackers ou de cyberterroristes. Des appareils défaillants tels que des téléphones mobiles dotés d'anciens systèmes d'exploitation ou des appareils connectés mal conçus ou mal configurés peuvent envoyer des requêtes répétées au même service, parfois avec d'importants intervalles. Cela tout à fait peut passer inaperçu dans le cas de dizaines ou même de centaines d'appareils, mais lorsqu'il s'agit de milliers cela devient problématique en termes de capacité serveur. Dans ce cas précis, il est nécessaire de détecter dans le trafic des traces de ces dysfonctionnements afin de pouvoir isoler les appareils responsables et ainsi d'éviter toute dégradation de service.

Protection et continuité d'affaires

Les produits Clavister offrent une protection complète contre les attaques de type DoS et DDoS et peuvent être déployés comme élément central de protection ou introduits dans un réseau existant comme couche supplémentaire de protection. Loin de constituer un onéreux produit de niche, Clavister apporte une excellente protection sans augmentation excessive des coûts. Même lors d'une attaque DDoS massive ciblant vos serveurs publics, les techniques de liens multi WAN Clavister vous assurent que votre activité ne sera pas affectée.

Vous pouvez en lire davantage à propos des DDoS et des solutions Clavister ici :

www.clavister.com/ddos

« Le règlement général sur la protection des données (RGPD) a ravivé l'intérêt pour la prévention de pertes de données et devrait influer sur 65% des décisions d'achat en la matière courant 2018 » - Gartner Inc.

Règlement général sur la protection des données (RGPD)

Le règlement européen sur la protection de la vie privée et des données à caractère personnel

Le RGPD est un règlement issu du droit de l'UE sur la protection de la vie privée et des données personnelles des résidents de l'Union. Il est entré en application le 25 mai 2018 et s'agissant d'un règlement et non d'une directive, il est obligatoire et directement applicable sans besoin de transposition en droit national par les différents États membres.
Le RGPD signifie la modernisation des pratiques de sécurité, des technologies et des politiques pour la plupart des entreprises. La définition de données personnelles y est très large puisqu'elle représente toute information pouvant directement ou indirectement être attribuée à un individu. Le RGPD enjoint les entreprises à adopter de nouvelles procédures et méthodes de travail, à faire du signalement et à communiquer, mais également à sécuriser leurs réseaux à l'aide des dernières technologies permettant conscience des risques et mesures préventives, correctives et palliatives.

Cette notion de conscience est fondamentale et sert à justifier la nécessité de procédures de détection de violation de données à caractère personnel.
Les responsables du traitement sont tenus de notifier toute violation dans les 72 heures. La non-notification ou tout manquement de moyens dans la détection de ces violations peuvent occasionner d'importantes amendes.

Les moyens clé de se prémunir contre ces risques sont les stratégies d'authentification multi-facteur qui permet de garantir que les personnes connectées sont authentifiées et autorisées à le faire, et les technologies de prévention de perte de données qui détectent et alertent de mouvements de données hors du périmètre sécurisé.

Vous pouvez en lire davantage à propos du RGPD et des solutions Clavister ici :
www.clavister.com/gdpr

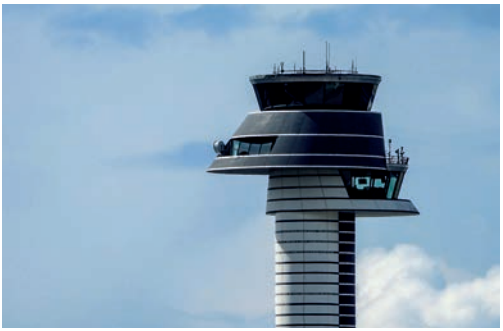
La directive SRI relative à la cybersécurité

La directive européenne sur la sécurisation des systèmes d'information et réseaux

La directive SRI est le tout premier essai de législation de cadre européen en matière de cybersécurité. Elle décrit les moyens légaux de rehausser le niveau général de cybersécurité de l'Union avec pour cible particulière des opérateurs d'infrastructures critiques. Ceci inclut les fournisseurs de service numériques et essentiels tels que fournisseurs d'énergie, d'eau, de chauffage et de gestion des déchets.

La solution

La proposition adoptée en 2016 impose aux États membres d'identifier ce type d'opérateurs d'ici fin 2018. Ils seront alors tenus de signaler les incidents majeurs aux centres de réponse aux incidents de sécurité informatique. Les opérateurs non domiciliés dans l'UE mais y exerçant leur activité sont également tenus au respect de la loi. De la même façon, au regard de la directive les opérateurs sont tenus pour responsables des accidents de sécurité même lorsque la maintenance de leurs systèmes d'information est déléguée à des tiers.



Le résultat

Au nombre des exigences de sécurité figurent des mesures techniques préventives de gestion des risques de violation de données. La directive devrait accroître la sécurité des réseaux et systèmes d'information de l'UE et assurer la protection de notre société face aux hackers et cyberterroristes.

Vous pouvez en lire davantage à propos de la directive SRI et des solutions Clavister destinées aux infrastructures critiques ici :
www.clavister.com/nis

« Les secteurs de la finance et de la distribution sont les plus touchés par les attaques par DDoS. »
– Rapport 2017 de Verizon sur les violations de données

Sécuriser les infrastructures réparties

Distribution et bureaux répartis

Afin d'atteindre leurs objectifs d'efficacité opérationnelle, de réduction des coûts et d'amélioration de l'expérience utilisateur, les points de vente modernes reposent fortement sur leurs systèmes informatiques. Les entreprises à la tête d'une multitude de bureaux, agences ou magasins se heurtent souvent au problème de garantir, pour le bon fonctionnement du système de gestion de stocks, de type SAP ou de caisses, une continuité de service sans l'appui d'administrateurs in situ. Avec l'avènement de technologies dédiées telles que terminaux de point de vente connectés en WiFi, l'accès WiFi gratuit pour les clients, les appareils connectés de type Smart Beacon, les appareils en libre-service, les écrans publicitaires et les réseaux administratifs internes, la complexité ne fait qu'augmenter. Bien que les services informatiques fassent un travail appréciable sur tout ces plans, cela implique autant de risques de failles de sécurité menaçant la continuité d'affaires et l'activité d'une entreprise.

De ce point de vue, les entreprises disposant d'une multitude de points de vente et celles disposant de succursales ont énormément en commun. Ce dont vous avez besoin est d'une solution à la fois centralisée et économique pour la connexion des bureaux « de terrain », sans compromis aucun sur la fonctionnalité ou la sécurité. Ceci implique non seulement des fonctionnalités pare-feu classiques de défense du périmètre, mais également de fonctionnalités dites pare-feu de dernière génération gérant la communication au niveau protocolaire et applicatif pour les cas d'utilisation les plus avancés.

Les solutions Clavister offrent les toutes dernières technologies et fonctionnalités même dans les équipements d'entrée de gamme. Elles permettent une protection efficace, rentable, optimale pour assurer la sécurité de systèmes informatiques au sein de réseaux distribués et une gestion centralisée.

Quelques-uns des ingrédients essentiels qui font de Clavister un choix idéal pour les entreprises de distribution et les entreprises réparties:

• Des liens réseaux virtuels privés et sûrs garantissent que vos données restent confidentielles et que vos différents sites communiquent entre eux et avec la maison mère de façon sécurisée.

• Le routage, la redondance et la répartition de charge permettent de construire une infrastructure fiable et résistante aux défaillances reposant sur des services d'accès haut débit à faible coût plutôt que sur des lignes dédiées.

• La protection contre les attaques réseau/serveur emploie un système intégré de détection et de prévention des intrusions et la protection anti DDoS afin de protéger vos points d'entrée numériques et de fournir des mécanismes assurant une continuité d'affaires en cas de scénarios de surcharge.

• Des rapports entièrement personnalisables montrant graphiquement les informations requises. Également, un monitoring évolutif en temps réel via tableau de bord personnalisable est fourni, assurant un contrôle permanent des tunnels RPV ou de connexions Internet.

Vous pouvez en lire davantage à propos des solutions Clavister pour les entreprises de distribution et multisites ici :
www.clavister.com/retail

Internet des objets (IoT) et transports

De nos jours, pratiquement toutes les machines et systèmes industriels permettent la maintenance à distance ainsi que la collecte de données statistiques et leur analyse centralisée. Ceci suppose un accès sécurisé depuis l'extérieur dont des personnes non autorisées peuvent tirer parti. Par la même, ces accès doivent être protégés dans des conditions changeantes propres aux environnements industriels où les machines peuvent être mobiles.

Les réseaux doivent être segmentés en zones afin d'implémenter des politiques de gestion de trafic et de sécurité différenciées et l'accès aux différents capteurs industriels à la fois possible à distance et strictement contrôlé. D'autres stratégies nécessitent de garantir une certaine portion de bande passante, pour des robots industriels par exemple, qui doivent être disponibles en permanence.

Une étude de cas : sécuriser la maintenance à distance de machines et d'usines

Qu'il s'agisse du niveau de carburant sur un navire ou de la mise à jour logicielle d'un robot industriel, l'accès à distance est de nos jours tout simplement indispensable pour la gestion de machines. Les créneaux de disponibilité, ainsi que le souci de protection contre les usages impropres par des personnes non autorisées, rendent plus importantes encore la rapidité d'accès et la haute disponibilité des machines connectées. Avec les solutions Clavister, ces exigences peuvent être comblées de façon à la fois simple, économique et plus sécurisée.

Quelques-uns des ingrédients essentiels qui font de Clavister un choix idéal pour les objets connectés à usage industriel et les transports :

• Des liens réseaux virtuels privés et sécurisés garantissent que vos données restent confidentielles et que vos différents sites communiquent entre eux et avec la maison mère de façon sécurisée.

• Le routage, la redondance et la répartition de charge permettent de construire une infrastructure fiable et résistante aux défaillances reposant sur des services d'accès haut débit à faible coût plutôt que sur des lignes dédiées.

• Des zones réseau sécurisées permettent une segmentation du réseau et l'application de différentes politiques de sécurité et de qualité afin de fournir la meilleure connexion aux machines appropriées

• Une gestion centralisée à distance qui permet à l'administrateur réseau de tout contrôler et de tout voir en temps réel.

• Les pare-feux de dernière génération virtualisés Clavister répondent à tous les cas de figure avec une consommation mémoire extrêmement limitée et peuvent être installé dans tout type d'hyperviseur.

Vous pouvez en lire davantage à propos des solutions Clavister pour objets connectés et transports ici :
www.clavister.com/iot

La directive SRI relative à la cybersécurité

La nouvelle directive européenne sur la sécurisation des systèmes d'information et réseaux impose aux opérateurs d'infrastructures critiques de sécuriser leurs périmètres, de transférer leurs données de façon cryptée et de maintenir un niveau de vigilance maximal pour tout ce qui concerne la sécurité. Il leur incombe de notifier toute atteinte de sécurité à un centre de réponse aux incidents de sécurité informatiques (CSIRT) national et d'y remédier au plus vite.

Conformité totale, impact ressources minime

Infrastructures critiques

Fournisseurs d'énergie, services municipaux, opérateurs et exploitants tous ont un point commun : ils utilisent une infrastructure critique qui rend notre type de vie possible. Cette infrastructure doit être complétée par une infrastructure de sécurité fournissant un contrôle à distance total et centralisé, ainsi que la collecte de données en temps réel à but de renseignement. L'une des contraintes pesant sur les infrastructures critiques est le manque d'espace physique. Une solution doit parfois être hébergée avec d'autres fonctionnalités telles que des systèmes de collecte de données et autres.

Une étude de cas : la connexion de parcs éoliens et solaires

Un pare-feu de dernière génération déployé comme composant principal de maintenance, dans la nacelle d'une éolienne par exemple, permet d'établir un périmètre de sécurité et de limiter l'accès depuis un réseau distant donné. Il est également possible de limiter cet accès à certains moments de la journée ou à un programme de maintenance particulier. De plus, le pare-feu permet de sécuriser et de crypter la transmission de données vers un datacenter, la quantité d'énergie produite par exemple, pour tout le parc. Très économe en ressources, un pare-feu Clavister peut être déployé virtuellement sur la même plateforme que d'autres composants, pour tout environnement hyperviseur.

Quelques-uns des ingrédients essentiels qui font de Clavister un choix idéal pour les infrastructures critiques :

• Un pare-feu complet répondant à des besoins actuels qui défend votre périmètre réseau

• Des RPV avec cryptage fort garantissant la confidentialité de vos données sensibles.

• Une gestion et une exploitation centralisées qui assurent que les responsables informatiques seront alertés en urgence de tout incident ou intrusion.

• En tant que pare-feu virtualisé, l'intégralité des solutions et fonctionnalités sont fournies tout-en-un avec une économie de ressources remarquable, pour la plupart des environnements hyperviseurs.

Vous pouvez en lire davantage à propos des solutions Clavister pour infrastructures critiques ici :
www.clavister.com/critical

Un contrôle central et individuel avec une identification sécurisée

Enseignement et secteur public

Les nouvelles technologies connectées telles que la formation et collaboration en ligne, ainsi que certains appareils ont amélioré l'expérience d'apprentissage dans bon nombre d'établissements de formation. Mais ces nouvelles technologies et le nombre grandissant d'appareils connectés vont de pair avec un besoin accru en termes d'évolutivité du réseau et de protection de systèmes et de données sensibles. En outre, le secteur public a pour caractéristique d'avoir affaire à des données, et équipements, de valeur et de sensibilité particulière justifiant d'une protection spéciale.

Dans un espace public tel qu'un établissement scolaire, il peut exister des règles strictes imposant des restrictions en termes de contenu et de services accessibles.

Centres d'enseignement et organismes de gouvernement ont besoin d'une solution de sécurité flexible permettant à la fois un contrôle d'accès granulaire, une vision globale de l'usage du réseau et la faculté de tracer les incidents jusqu'à la source.

Une étude de cas : accès WiFi en classe contrôlé par l'enseignant

Élèves et enseignants sont connectés et authentifiés auprès du réseau WiFi de l'établissement. L'enseignant peut exercer un contrôle sur l'accès Internet des élèves présents et au besoin, par exemple, le bloquer temporairement afin de capter leur attention. Un accès temporaire peut être autorisé dans un but de recherche ou un filtrage mis en place afin de bloquer tout utilisation non scolaire telle que les réseaux sociaux. Le pare-feu sécurise le réseau et permet un filtrage web empêchant l'accès à tout contenu indésirable au sein de l'établissement.

Quelques-uns des ingrédients essentiels qui font de Clavister un choix idéal pour les centres d'enseignement et les administrations publiques :

• Un agent d'authentification intégrée aux réseaux WiFi permettant l'identification d'utilisateurs et l'application de conditions d'accès spécifiques

• Identification et contrôle de contenu web et d'applications fournissant à l'enseignant un levier pour la gestion du temps

• Une gestion centralisée et un accès par rôle permettant aux enseignants un contrôle de l'accès Internet de la classe

Vous pouvez en lire davantage à propos des solutions Clavister pour l'enseignement et le secteur public ici :
www.clavister.com/schools

Cloud sécurisé utilisant des ressources minimales

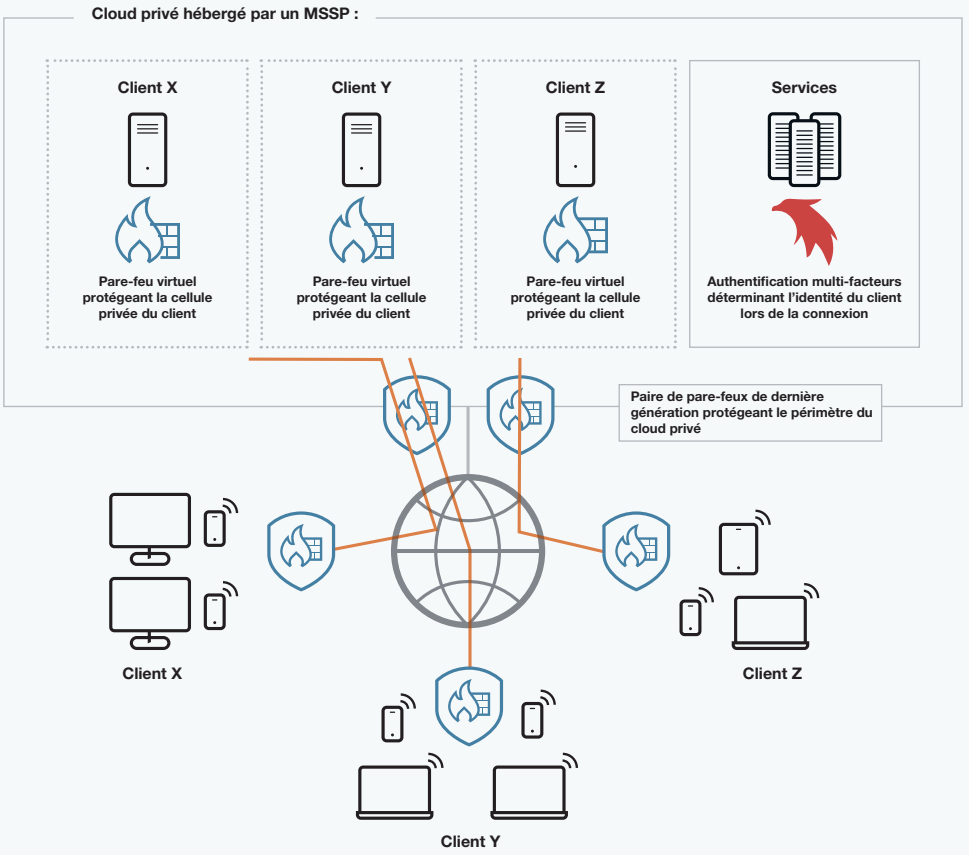
Fournisseurs de service de sécurité

Du fait de l'importance et de la complexité grandissante des infrastructures de sécurité, un nombre croissant d'entreprises fait le choix d'externaliser l'exploitation et la maintenance. Les intégrateurs de systèmes et les revendeurs locaux tentent de rénover leur offre afin de fournir la sécurité sous forme de service « géré ».

Les solutions Clavister se prêtent particulièrement à leur utilisation par des fournisseurs de service de sécurité (MSSP) qui peuvent ainsi compléter leurs services d'hébergement. Puisque nos produits sont disponibles en version matérielle et virtuelle, ils peuvent être utilisés au sein de datacenters afin de protéger des ressources cloud ou sur site.

Une étude de cas : les cellules de sécurité virtuelles

Prenons le cas de certains services informatiques tels que le Bureau à distance, le stockage et partage de fichiers qui sont proposés par les fournisseurs de service aux PME. Ces services sont apportés par des machines virtuelles dédiées hébergées dans un cloud privé. L'infrastructure cloud peut être protégée par une paire de pare-feux de dernière génération Clavister dédiés assurant la protection du périmètre, les machines virtuelles du client par des pare-feux virtuels de dernière génération dédiés.
Un SD-WAN sécurisé est mis en place afin de connecter le réseau du client aux machines virtuelles, fournissant ainsi une cellule sécurisée et confidentielle de bout en bout.



Quelques-uns des ingrédients essentiels qui font de Clavister un choix idéal pour les fournisseurs de services de sécurité :

• En tant que pare-feu virtualisé, l'intégralité des solutions et fonctionnalités sont fournies tout-en-un avec une économie de ressources remarquable, pour la plupart des environnements hyperviseurs.

• Une gestion centralisée avec support à distance qui permet d'importants déploiements pour une multitude de clients, holistique et extrêmement efficace (jusqu'à des milliers d'images virtuelles).

Vous pouvez en lire davantage à propos des solutions MSSP de Clavister ici :

www.clavister.com/mssp

Pare-feux de dernière génération : matériels et virtuels

Gamme de produits

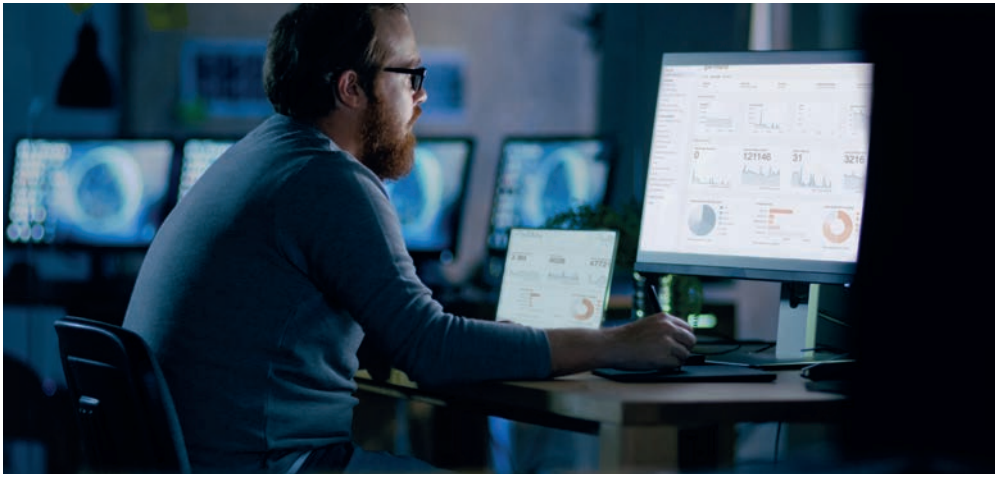
Clavister propose une gamme complète d'équipements depuis des boîtiers réduits, « de table » pour petites entreprises jusqu'aux modèles montés sur racks pour moyennes entreprises. Les modèles adaptés aux datacenters à destination des grandes entreprises et fournisseurs de service incluent des blocs d'alimentations redondants et permutables à chaud, ainsi qu'une variété de modules d'interface permettant de personnaliser la configuration de ports. Les cas d'utilisation sont disponibles sur toutes les plateformes, y compris les virtuelles fonctionnant avec tout type d'hyperviseur moderne, et assurent une sécurisation du périmètre.

clavister		 De table	 Salle serveur	 Datacenter	 Virtuel – Cloud
Modèle		E10 – E80	W20 – W30	W40 – W50	V2 – V10
Capacité	**Pare-feu**	1 – 4 Gbps	4 – 10 Gbps	10 – 55 Gbps	300 Mbps – 10 Gbps*
	RPV	100 Mbps – 1 Gbps	1 – 2 Gbps	2 – 8 Gbps	150 Mbps – 5 Gbps*
Interfaces		4-6 x 1GbE	6 – 9 1GigE. W30 supporte un module d'interface	8 GigE ou 4 x 10GbE par module d'interface	3 – 10 interfaces supportée
Hyperviseurs supportés					VMware vSphere, KVM, Microsoft Hyper-V, OpenStack
Ressources requises					256 MB – 4 GB ou RAM, 256 MB d'espace stockage, 1 vCPU
Haute disponibilité		En option	Actif-Passif, Actif-Actif et Actif-Passif-Actif		Oui
Nombre estimé d'utilisateurs		10 - 25	100 - 200	n/a	n/a
Technologies		Toutes les plateformes supportent les fonctionnalités et technologies de gestion unifiée de menaces (UTM) et de pare-feu de dernière génération (NGFW) telles que IDS/IPS, antivirus, anti-spam, réputation IP, filtrage géographique, contrôle applicatif / inspection des paquets en profondeur (DPI) et filtrage de contenu web, en fonction du type d'abonnement.			
Cas d'utilisation		Tous	Tous	Tous	Tous

** Les performances réelles peuvent varier en fonction des capacités du matériel de l'hôte/serveur, du type d'hyperviseur, etc.*

Gestionnaire de configuration et logiciel opérationnel

Contrôle holistique de bout en bout



Les pare-feux de dernière génération de Clavister disposent de multiples interfaces pour la configuration et la gestion. Une interface web moderne comprenant des assistants d'installation est incluse, ainsi qu'un accès console et des API pour des tâches d'automatisation.

La licence comprend l'accès à un logiciel de gestion centralisée pouvant être employé pour tout pare-feu déployé. Ce logiciel, InControl, permet à l'administrateur d'intervenir à tout moment avec un impact minimal. Des rapports entièrement paramétrables et graphiques peuvent être générés.

Également, un monitoring évolutif en temps réel via tableau de bord personnalisable est fourni, assurant un contrôle permanent des tunnels RPV ou de connexions Internet.

Bien entendu, Clavister s'intègre également dans des solutions de supervision existantes telles que les systèmes implémentant Nagios. Les messages de log peuvent aussi être analysés avec d'autres plateformes telles que syslog ou Splunk. Le paramétrage est simple et rapide.

Vous pouvez en lire davantage à propos de la gamme de produits Clavister ici :

www.clavister.com/product-models

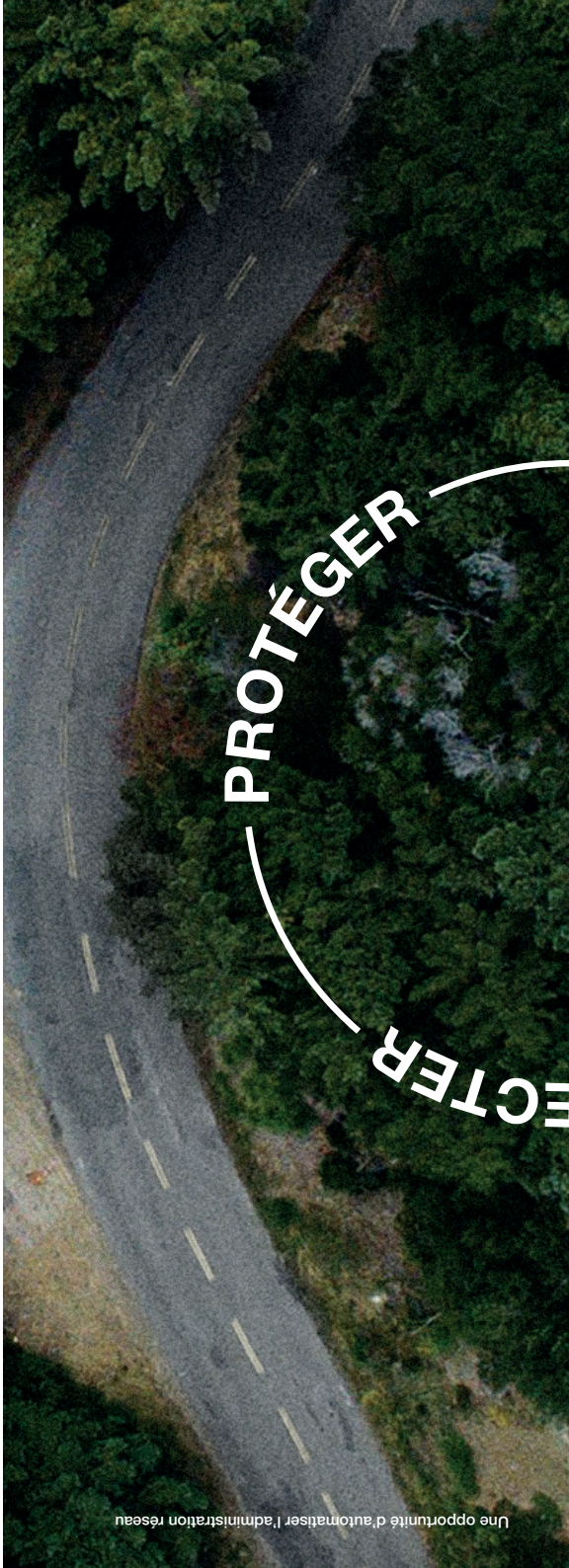
Une opportunité d'automatiser l'administration réseau

Dans un monde en constant mouvement, où de nouvelles menaces apparaissent à chaque heure ou plus souvent encore, les administrateurs réseau se doivent d'être vigilants afin de protéger les actifs numériques de leur entreprise.

La banalisation des objets connectés y compris au sein des réseaux professionnels nécessite une plus grande réactivité.

Afin de rendre ceci possible d'une façon économique, des technologies avancées au nombre desquelles l'apprentissage automatique et l'intelligence artificielle sont rendues nécessaires afin d'identifier, de détecter des variations et de signaler les anomalies. Mais Clavister va au-delà. Lorsque nécessaire, nos solutions agissent automatiquement afin de neutraliser une menace avant même qu'elle n'impacte votre activité.

Vous n'avez pas besoin de devenir un expert en sécurité, Clavister est une solution qui apprend par elle-même et vous protège 24 heures sur 24, 7 jours sur 7.



Une opportunité d'automatiser l'administration réseau