Quelle est la protection adéquate contre les attaques DDoS pour votre entreprise?

Guide de l'acheteur – Solutions de sécurité contre les attaques par déni de service distribué (DDoS)

Bell

Sommaire

Si vous avez déjà déterminé que votre organisation a besoin de protection contre les attaques par déni de service distribué (DDoS), voici la prochaine question à vous poser : « Quel type de solution de sécurité DDoS nous faut-il? »

Le présent guide vous aidera à trouver la réponse en fonction de vos besoins sur le plan des affaires et de la technologie. Il vous renseignera aussi à propos des questions à poser à un fournisseur potentiel de solutions de sécurité.

Table des matières

Comment savoir si vous êtes à risque?

Définir votre profil de risque en matière de sécurité des TI est une première étape essentielle pour déterminer si vous avez besoin d'un quelconque niveau de protection contre les attaques DDoS. Une réponse positive à une ou plusieurs des questions suivantes signifie que votre entreprise est potentiellement vulnérable à une attaque DDoS :

- Appartenez-vous à un secteur d'activité à haut risque?
- Votre organisation a-t-elle une forte présence en ligne?
- Votre présence sur le Web est-elle essentielle à vos activités?
- Une attaque DDoS entraînerait-elle des conséquences négatives importantes pour votre organisation sur le plan financier ou sur celui de la réputation?

Pour effectuer une analyse plus approfondie des risques, téléchargez notre guide d'évaluation des risques liés aux attaques DDoS, à l'adresse bell.ca/evaluationddos.

Savoir contre quoi vous protéger

Avant de rechercher des solutions de sécurité ou un fournisseur, il est important que vos connaissances soient à jour à propos du fonctionnement des attaques DDoS et de l'incidence qu'elles peuvent exercer sur vos activités.

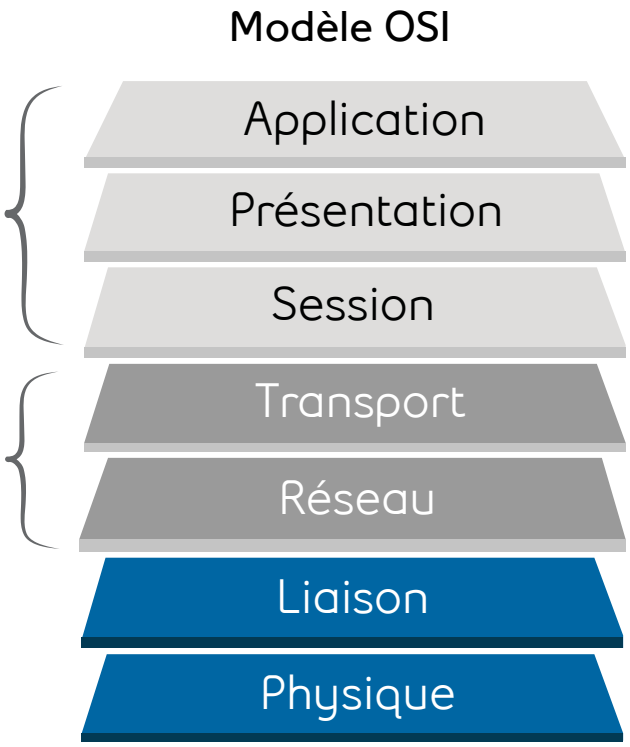
N'oubliez pas que le but d'une telle attaque est d'empêcher les utilisateurs légitimes d'accéder à vos services et ressources en ligne. Deux types principaux d'attaques sont utilisés pour arriver à cette fin :

Attaques sur la couche application

Les attaques sur la couche application surchargent vos serveurs en envoyant une énorme quantité de demandes qui exigent la manipulation et le traitement d'un grand nombre de ressources. Ce type d'attaques cible les protocoles qui recèlent des faiblesses exploitables, comme le protocole de transfert hypertexte (HTTP), le protocole de transfert de courrier simple (SMTP), le protocole de transfert de fichiers (FTP) et le langage d'interrogation structuré (SQL).

Attaques sur la couche réseau

Les attaques sur la couche réseau utilisent la force brute de milliers de demandes d'information simultanées afin d'obstruer votre canal Internet, consommant ainsi une énorme quantité de bande passante et surchargeant vos connexions réseau. Les auteurs des attaques ciblent le réseau en exploitant les vulnérabilités sur des plans comme le protocole de datagramme utilisateur (UDP), le protocole de synchronisation de réseau (NTP) et le système de noms de domaine (DNS).



Étant donné qu'un nombre croissant d'attaques combinées touchent ces couches et vos serveurs simultanément, il est essentiel que toute solution DDoS offre une protection contre l'éventail complet des attaques possibles.

Pour de plus amples renseignements sur le fonctionnement des attaques DDoS et leur incidence potentielle, téléchargez notre livre blanc sur l'introduction aux attaques DDoS, à l'adresse bell.ca/livreblancddos.

Déterminer vos exigences techniques

Qu'attend votre organisation de son infrastructure de TI? La solution DDoS que vous choisirez devra s'harmoniser avec vos besoins particuliers sur le plan technique et des activités et tenir compte des éléments suivants :

Portée de votre présence en ligne

Si votre présence sur le Web est élémentaire, vous n'aurez besoin que d'une solution de base, capable de prendre en charge le trafic HTTP/HTTPS. Si vous utilisez à la fois des sites Web et des serveurs d'applications, vous aurez besoin d'une protection plus évoluée contre les attaques DDoS. Si votre organisation exploite de multiples établissements, la solution choisie devra pouvoir les protéger tous de la même façon.

Connectivité Internet

Si vous avez recours à plusieurs fournisseurs de services Internet pour assurer la redondance et la disponibilité de vos ressources, une protection similaire doit être appliquée dans tous les cas – ce qui pourrait exiger la mise en œuvre (et la gestion) de différentes solutions.

Dans quelle mesure votre solution DDoS doit-elle être réactive?

Le coût des temps d'arrêt et leur incidence sur vos activités détermineront le niveau de performance requis de votre solution de sécurité DDoS. Une réduction du délai d'intervention et de résolution des problèmes peut s'avérer une haute priorité si la disponibilité des sites Web et des applications est cruciale pour vos activités.

Impact potentiel sur vos services

Une solution qui achemine le trafic entrant à un centre de nettoyage en nuage peut filtrer les données malveillantes. Toutefois, le processus de réacheminement risque de provoquer un délai d'acheminement des données qui nuit au rendement et à la stabilité des applications. Ce type de solution n'est sans doute pas propice si vos activités reposent sur de la vidéo de grande qualité ou des transactions financières en temps réel.

Expérience de votre équipe de TI

Il est important de déterminer si votre équipe possède l'expertise permettant d'utiliser efficacement une solution DDoS autogérée, d'autant plus que les attaques gagnent en complexité. Votre équipe doit aussi être prête à apprendre et à s'adapter au fur et à mesure qu'évoluent les attaques.

Pratiques existantes en matière de sécurité

Certaines équipes de TI préfèrent exercer un niveau de contrôle élevé sur toute solution déployée dans leur environnement. Bien que les solutions gérées et activées manuellement permettent d'intervenir de façon plus précise en cas d'attaque, les délais de détection et d'intervention qui les caractérisent peuvent s'avérer plus longs que ceux d'une solution entièrement gérée et à surveillance permanente.

Exigences en matière de gestion des données

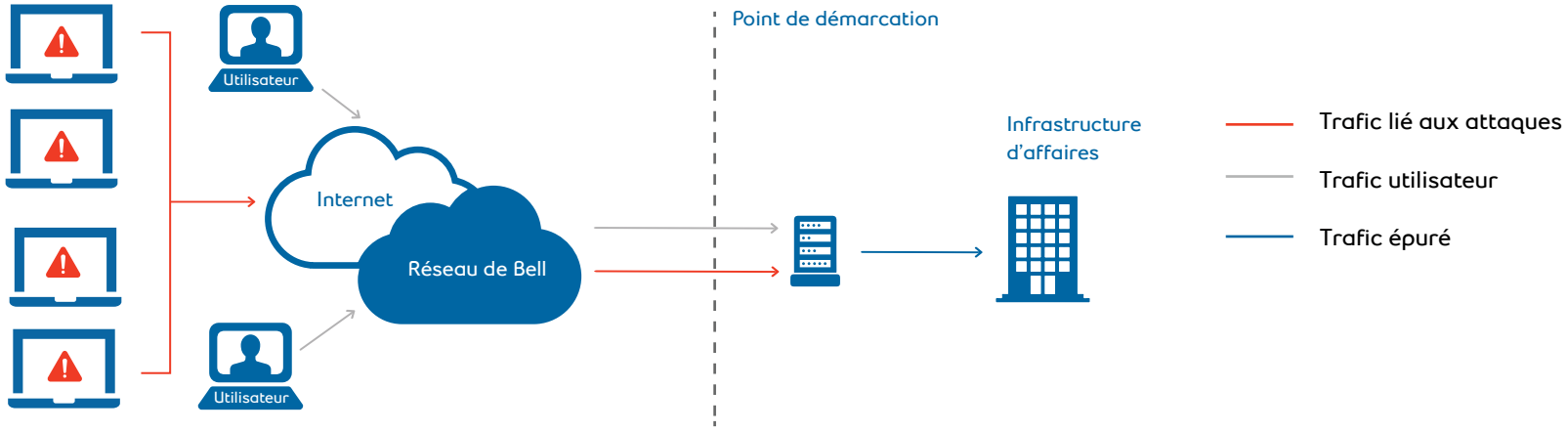
Les gouvernements et les institutions financières sont souvent soumis à des exigences internes ou réglementaires qui les obligent à conserver leur trafic dans les limites d'un pays ou d'une région. Dans ce cas, il faut exclure les solutions de sécurité et les fournisseurs dont les centres de nettoyage du trafic sont situés à l'extérieur du pays.

Déterminer quel est le bon modèle de déploiement

Il y a de nombreuses façons de mettre en œuvre la protection contre les attaques DDoS. Avant de choisir un modèle de déploiement, il est important de connaître les avantages et les inconvénients de chacun d'eux – et d'évaluer votre propre tolérance au risque. Vous devez aussi tenir compte de la valeur relative de chaque modèle en fonction de vos exigences particulières sur le plan technique et des affaires.

Équipement installé sur place

Des dispositifs de sécurité spécialisés et installés sur place détectent les attaques sur la couche application et les attaques chiffrées, puis protègent votre réseau en éliminant tout trafic portant la signature d'une attaque connue. Ce type de dispositif constitue une solution de rechange essentielle aux pare-feu et aux systèmes de prévention d'intrusion, qui peuvent se retrouver débordés par un volume élevé de demandes ouvertes.



Avantages

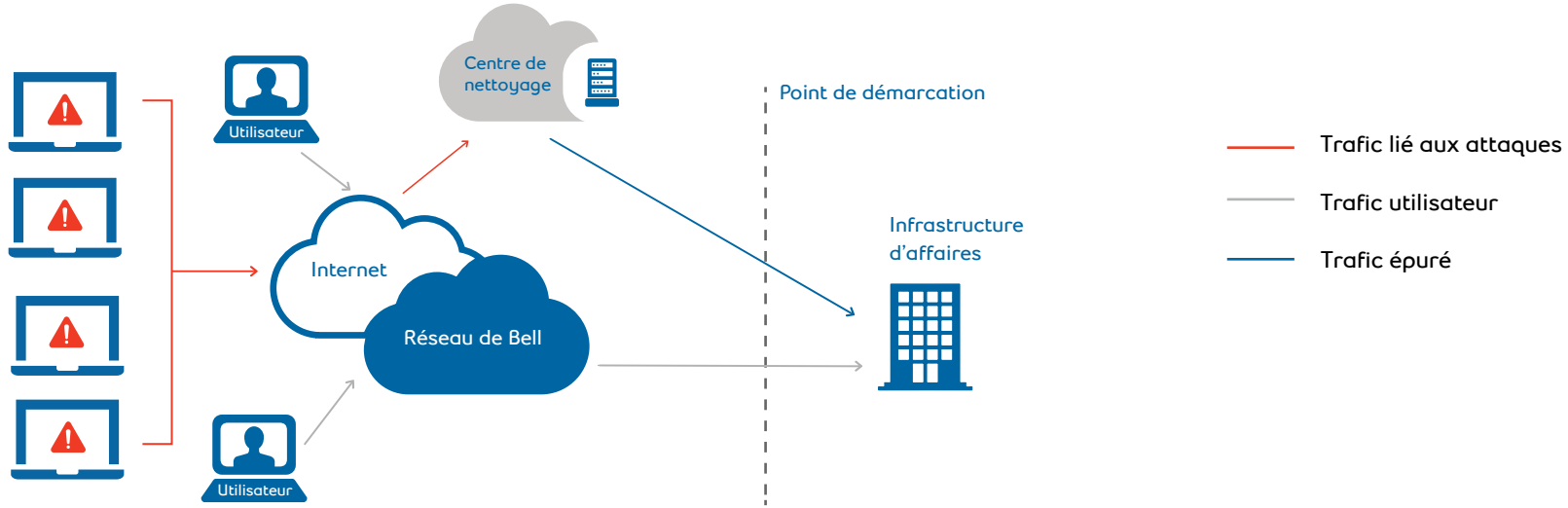
- Excellente protection contre un large éventail d'attaques
- Attention particulière accordée à des seuils très spécifiques d'attaques et de menaces contre la couche application
- Contrôle accru exercé sur la mise en œuvre, la gestion et l'intervention
- Respect des exigences internes ou réglementaires rigoureuses en matière de gestion des données

Inconvénients

- Possibilité de sollicitation intensive du système en cas d'attaques massives
- Gestion et configuration continues afin de rester à jour en matière de menaces

Service de nettoyage en nuage

Les solutions en nuage réacheminent l'ensemble du trafic vers un fournisseur de service en nuage afin qu'un filtrage soit effectué en cas d'attaque. Une fois le « nettoyage » terminé, le trafic légitime est acheminé à votre site. Ce réacheminement peut provoquer un délai et nuire au rendement de l'application. En outre, jusqu'à ce que l'annonce de la route suivie par le protocole de passerelle frontière (BGP) se soit propagée (indiquant à Internet de réacheminer votre trafic), votre site continue à recevoir le trafic de l'attaque. La plupart des services de nettoyage du trafic sont situés à l'extérieur du Canada, ce qui peut contrevenir à vos exigences en matière de gestion des données.



Avantages

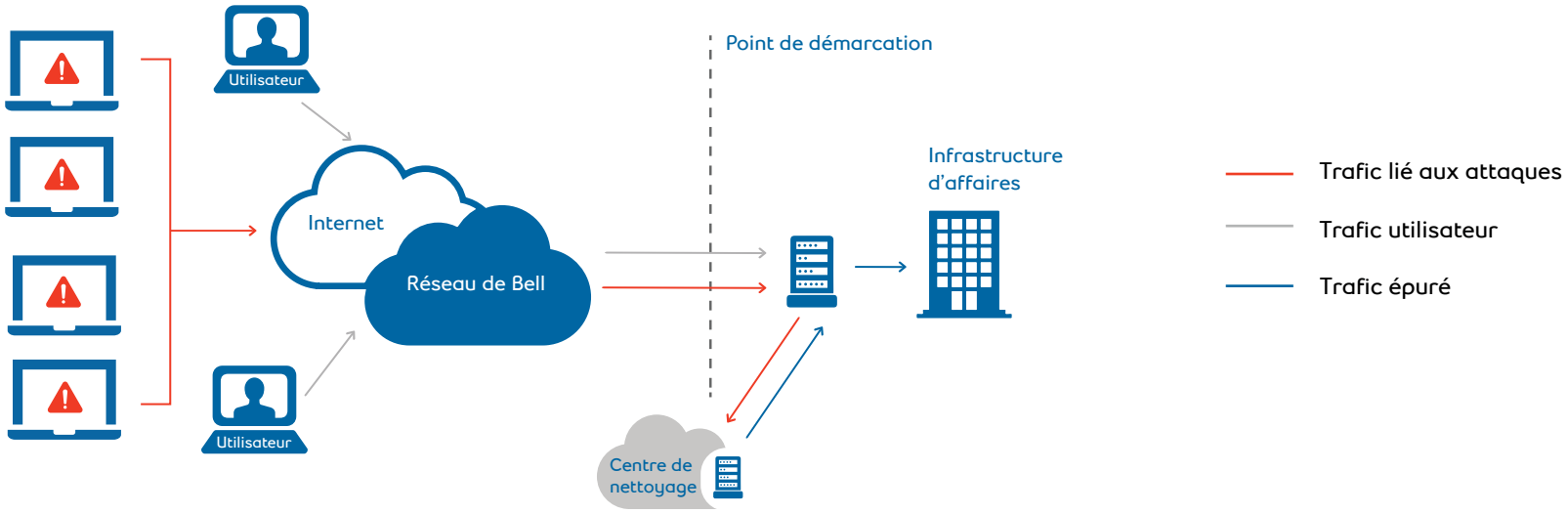
- Meilleure protection contre les attaques massives qu'avec de l'équipement sur place
- Faible taux de faux positifs
- Aucun matériel requis dans les locaux de l'entreprise
- Mise à jour constante

Inconvénients

- Possible détérioration du rendement de l'application en raison des délais d'acheminement du trafic
- Incapacité à bloquer certains types d'attaques sur la couche application
- Nécessaire abandon du contrôle du processus de chiffrement aux fins de la protection du protocole SSL
- Saturation possible du lien réseau en raison de délais dans la propagation de l'annonce de la route suivie
- Préoccupations possibles à propos de la situation géographique des centres de nettoyage du trafic

Solution hybride A : service de nettoyage en nuage + équipement sur place

Une méthode de protection plus efficace contre les attaques DDoS consiste à combiner l'équipement installé dans ses propres locaux et le service de nettoyage en nuage. Le service en nuage procure une meilleure protection contre les attaques massives et un faible taux de faux positifs, tandis que l'équipement sur place confère un contrôle plus étroit du moment et de la façon de réduire l'impact d'une attaque. Seul le trafic légitime étant acheminé à votre site, le risque que votre équipement sur place soit saturé par un flux de trafic malveillant est éliminé – ce qui signifie que l'équipement est disponible afin que vos serveurs et vos applications demeurent en ligne.



Advantages

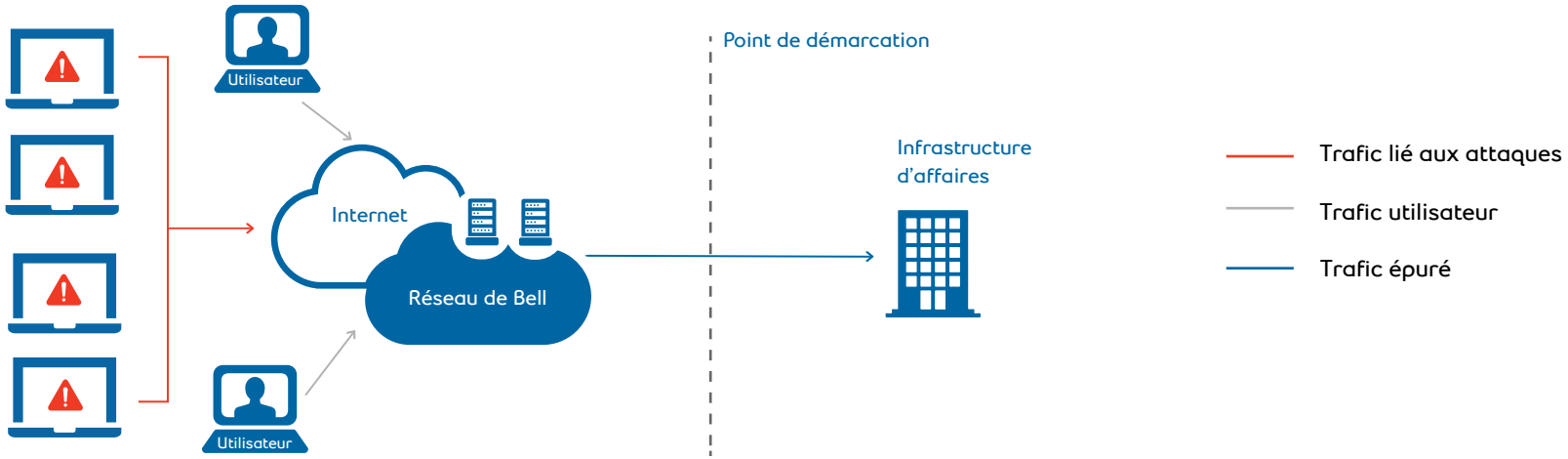
- Couche de protection supplémentaire par rapport à l'utilisation d'une seule des deux solutions
- Meilleure protection contre les attaques massives qu'avec seulement de l'équipement sur place
- Faible taux de faux positifs
- Mise à jour permanente du service de nettoyage en nuage
- Contrôle accru exercé sur la mise en œuvre, la gestion et l'intervention

Inconvénients

- Réacheminement nécessaire du trafic vers le fournisseur de services en nuage en cas d'attaques massives
- Capacité limitée de contrer les attaques massives pendant le délai de réacheminement
- Maintenance et configuration de l'équipement sur place continuellement requises afin de rester à jour face aux menaces les plus récentes

Détection de réseau en ligne

La meilleure solution autonome prévoit la détection et l'atténuation des attaques massives sur la couche application dans le réseau même – avant que le trafic puisse atteindre votre entreprise. Ce type de solution est offert uniquement par des fournisseurs de services réseau qui disposent de fonctions de sécurité évoluées et peuvent mettre en œuvre les mécanismes requis à même leur réseau. La détection de réseau en ligne est plus rapide que le nettoyage en nuage : l'impact d'une attaque peut être réduit dans un délai de 30 secondes après sa détection. La détection en amont des anomalies des paquets et des autres « bruits » gourmands en bande passante réduit les possibilités que cette dernière soit accaparée par le trafic inutile.



Advantages

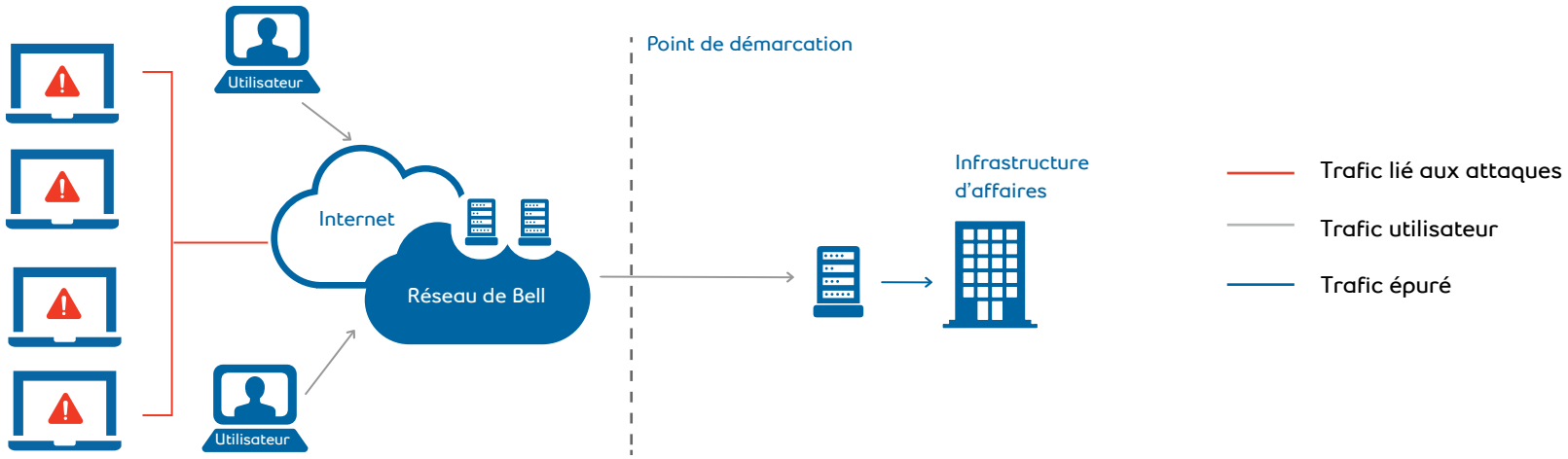
- Très faible temps d'attente (aucun réacheminement à un centre de nettoyage du trafic requis)
- Délais d'intervention et de réduction de l'impact des attaques plus court
- Prise en charge des attaques massives
- Taux de faux positifs extrêmement faible
- Aucun matériel requis dans les locaux de l'entreprise

Inconvénients

- Aucune protection contre les attaques du protocole SSL/SSH
- Accès direct insuffisant à l'équipement de protection

Solution hybride B : détection de réseau en ligne + équipement sur place

La solution la plus complète est celle qui offre le meilleur des deux mondes : détection et réduction de l'impact des attaques en ligne, amplifiées par les capacités plus modulaires d'un dispositif sur place.



Advantages

- Très faible temps d'attente (aucun réacheminement à un centre de nettoyage du trafic requis)
- Délais d'intervention et de réduction de l'impact des attaques plus court
- Prise en charge des attaques massives
- Taux de faux positifs extrêmement faible
- Protection complète grâce à la redondance sur place
- Attention particulière accordée à des seuils très spécifiques d'attaques et de menaces contre la couche application

Inconvénients

- Coûts supplémentaires liés à la mise en œuvre de deux solutions

Que rechercher chez un partenaire de sécurité DDoS

Une fois que vous avez déterminé quel modèle de déploiement répond le mieux à vos besoins, vous devez choisir un fournisseur de services de sécurité. Voici quelques questions à poser à propos de l'expérience, de la qualité du service, de la capacité ainsi que des fonctions et services caractérisant un fournisseur potentiel afin de déterminer s'il convient à votre organisation :

Expérience

Depuis quand offrez-vous des solutions de sécurité DDoS?

Les fournisseurs détenant une expérience directe étendue savent ce qu'il faut faire pour détecter et prévenir les attaques. De façon générale, ils disposent d'infrastructures plus résilientes et de mesures correctives plus efficaces, ce qui les rend plus aptes à traiter des attaques imprévues et immédiates.

De quels types d'attaques avez-vous réduit l'impact?

Les meilleurs fournisseurs ont eu l'occasion de traiter un large éventail de types d'attaques. Si vous savez quels types d'attaques un fournisseur a déjà traités, vous aurez une bonne idée du service auquel vous pouvez vous attendre de lui.

Quelle expérience avez-vous dans la recherche sur les menaces?

Les fournisseurs qui investissent dans la recherche sur les cybermenaces sont en mesure de fournir des renseignements plus éclairés sur l'évolution des menaces – et sur ce que cela signifie pour votre entreprise. Alors que cette évolution se poursuit, l'information devient un élément de plus en plus important d'une protection efficace.

Qualité du service

En cas d'attaque, quel est votre délai pour intervenir/réduire l'impact?

Être en mesure de répondre rapidement à une attaque est crucial. Si une attaque persiste trop longtemps avant que le fournisseur puisse intervenir, votre entreprise pourrait subir un temps d'arrêt important – entraînant une perte de revenus et une détérioration de votre image de marque.

Quelles ententes sur la qualité du service (EQS) ou quels objectifs de qualité du service (OQS) offrez-vous?

Plus la réduction de l'impact d'une attaque dure longtemps, plus la durée de votre exposition au trafic malveillant sera longue – ce qui rend extrêmement importants les temps de réponse garantis dans les EQS/OQS. Un fournisseur qui maintient avec confiance ses EQS/OQS démontre son engagement à fournir un service de qualité.

Quelles redondances avez-vous mises en place pour respecter vos EQS/OQS?

Un fournisseur dont le service tient compte du temps de disponibilité et qui a mis en œuvre des redondances à tous les niveaux est beaucoup mieux à même de respecter ses EQS/OQS. Prenez le temps de comprendre l'architecture du fournisseur pour vous assurer qu'il peut fournir le service tel qu'il le promet.

Capacité

Quels types de bande passante pouvez-vous prendre en charge?

Les attaques DDoS peuvent accaparer massivement la bande passante, dépassant souvent 10 Gbit/s, et même 100 Gbit/s. Vérifiez si le réseau et l'infrastructure du fournisseur peuvent prendre en charge des attaques massives sans être débordés.

Y a-t-il un plafond ou des frais qui varient selon le volume de l'attaque?

La structure de frais de certains fournisseurs comprend un prix de base pour le service en soi, ainsi que des frais d'utilisation qui varient selon la fréquence et le volume des attaques (c'est-à-dire la quantité de bande passante consommée). Une telle structure peut entraîner des frais et des dépenses de TI non prévues. Vérifiez soigneusement ce qui est inclus ou non dans le prix de base, ainsi que les facteurs susceptibles d'influencer les coûts mensuels. Dans la mesure du possible, cherchez à obtenir un prix fixe, non fondé sur la consommation de bande passante.

Fonctions et services offerts

Votre service est-il offert en permanence ou sur demande?

Un service permanent détecte automatiquement les attaques et prend les mesures nécessaires sans que votre équipe ait à intervenir. Avec un service sur demande, par contre, vous devez exercer une surveillance de votre infrastructure et activer manuellement votre réponse à une attaque dès qu'en apparaissent les premiers signes. Le choix de l'une ou l'autre approche dépend de la capacité de surveillance de votre équipe et des délais d'intervention que vous souhaitez obtenir.

Votre service est-il entièrement géré?

Une solution de sécurité entièrement gérée soulage votre équipe d'un poids et vous permet de disposer d'une protection constamment à jour afin de contrer les menaces les plus récentes.

Quels types d'attaques pouvez-vous prévenir (et combien de types d'attaques)?

Lorsque le trafic est réacheminé vers un centre de nettoyage en nuage, ne manquez pas de vérifier si le fournisseur utilise le service de nom de domaine (DNS) ou le protocole BGP.

- Le service DNS est plus facile à mettre en fonction, aucune modification de configuration n'étant requise sur vos serveurs Web. Le routage DNS est permanent, mais ne fonctionne que pour le trafic HTTP.
- Le protocole BGP réachemine le trafic en fonction de la portée du système autonome (AS) de l'adresse IP. La mise en fonction du protocole BGP exige un travail plus long, mais il a pour avantage de protéger la totalité de votre réseau. Le service BGP peut être permanent ou activé sur demande.

Vos installations de protection DDoS sont-elles situées au Canada?

Lorsque le trafic est réacheminé vers un centre de nettoyage, ce dernier peut être situé à l'extérieur du Canada. Il peut s'agir d'une préoccupation pour certaines organisations, le trafic étant alors assujetti à la réglementation (ou non protégé en l'absence de réglementation) des pays où ils sont situés.

Solutions de sécurité de Bell contre les attaques DDoS

Peu importe le modèle de déploiement que vous choisissez, Bell possède l'expertise en matière de sécurité et les capacités de réseau pour vous offrir une solution qui répond à vos besoins – et qui permet à votre entreprise de poursuivre ses activités.

Détection de réseau en ligne

Entièrement géré et ne nécessitant aucun équipement sur place ni aucune intervention manuelle, le service Sécurité du réseau contre les attaques DDoS de Bell tire avantage de la portée du réseau de Bell et de l'information qu'il englobe. Ce service offre une sécurité multicouche permanente de bout en bout au niveau de l'infrastructure. Il détecte les attaques et en réduit l'impact de manière proactive avant qu'elles n'atteignent votre réseau d'entreprise.

Tous les types d'attaques par DDoS sont continuellement surveillés, peu importe leur origine, leur volume ou leur durée.

Le trafic transitant dans notre réseau est constamment nettoyé et filtré, ce qui nous permet de détecter les attaques et d'en réduire l'impact dans un délai maximal de 30 secondes. Parce que les fonctions de nettoyage sont intégrées à notre réseau fédérateur, le temps d'attente est réduit à des millisecondes.

Access near real-time threat reports for deeper insights into your current traffic and potential threats, as well as historical summaries of previous threats encountered.

Cloud-based scrubbing

Notre service de nettoyage du trafic en nuage est idéal pour les entreprises ayant des établissements éloignés à l'échelle internationale qui ne sont pas connectés au réseau de Bell, ainsi que pour celles qui s'en remettent à plusieurs fournisseurs de services Internet pour leur connectivité. Ce service procure en permanence un niveau de protection élevé contre les attaques massives sans qu'il soit nécessaire d'installer quelque équipement que ce soit sur place.

Équipement installé sur place

Notre réseau et nos services en nuage peuvent être augmentés par un ou plusieurs déploiements d'équipement sur place. Vous obtenez alors une défense plus modulaire en ajoutant des profils de protection de la couche application, une fonction de détection des réseaux de zombies dans le trafic sortant et une protection contre les attaques chiffrées. Nous nous chargeons de l'installation et de la configuration et définissons les politiques de sécurité nécessaires à la protection contre les attaques DDoS et autres cyberattaques. Nous pouvons aussi nous charger de la surveillance et de la gestion continues de votre solution afin que l'impact des attaques soit réduit adéquatement et que les seuils d'attaques et les profils de protection soient constamment à jour.

À propos de Bell

Les entreprises qui exigent une infrastructure de TI fiable et hautement sécurisée choisissent Bell. Comme nous faisons partie intégrante de l'infrastructure névralgique du Canada, nous offrons l'expertise la plus pointue au pays en matière de détection, d'atténuation et de prévention des menaces.

À titre de propriétaire et exploitant du plus important réseau de voix et de données au pays, nous voyons mieux que quiconque les menaces qui peuvent peser sur votre entreprise. Nous pouvons agréger d'énormes quantités de données et établir des corrélations entre différentes structures de trafic pour détecter le trafic malveillant de manière proactive et l'atténuer, et réduire les délais d'intervention lorsque surviennent des incidents. Avec une équipe de plus de 300 professionnels de la sécurité et une profonde connaissance des menaces présentes au Canada, nous avons l'expérience nécessaire pour vous aider à planifier, à concevoir, à réaliser et à gérer la solution de sécurité complète qui convient à votre entreprise.

Pour en savoir plus sur nos solutions de sécurité DDoS, demandez qu'un conseiller de Bell communique avec vous en allant à la page bell.ca/contactsecurite. Les liens ci-dessous vous permettront d'obtenir des renseignements sur des ressources connexes :

Service Sécurité du réseau contre les attaques DDoS de Bell – Pour de plus amples renseignements sur les avantages et les capacités de notre service réseau.

Blogue

Introduction aux attaques DDoS – Pour comprendre comment fonctionnent les attaques DDoS et pourquoi elles surviennent.

Blogue

Coûts et conséquences des attaques DDoS – Pour connaître l'impact que peut exercer une attaque sur votre organisation.

Quel est votre profil de risque DDoS? – Pour évaluer les risques encourus par votre organisation et déterminer le niveau de protection dont vous avez besoin.

Blogue

Comment protéger votre entreprise des attaques DDoS – Pour en apprendre davantage sur la façon de protéger vos actifs numériques et votre infrastructure.