Réseaux privés virtuels

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Juin 2024 | ITSAP.80.101

Un réseau privé virtuel (RPV) est une connexion sécurisée entre deux points, comme un ordinateur portable et le réseau d'une organisation. Le RPV sert de tunnel par l'entremise duquel on peut envoyer et recevoir des données sécurisées dans un réseau physique existant. Par exemple, une ou un employé travaillant à distance peut utiliser un RPV pour chiffrer les données alors qu'elles transitent à travers le réseau jusqu'à leur destination. Cette destination peut être une autre personne en travail, un siège social ou d'autres serveurs organisationnels. Cette publication présente quelques risques dont il faut tenir compte avant d'utiliser un RPV.

Fonctionnement des réseaux privés virtuels

Un RPV dissimule les données entrantes et sortantes qui traversent un tunnel sécurisé. Ces données peuvent être déchiffrées une fois qu'elles atteignent la destination prévue. Les tunnels des RPV masquent vos données, votre adresse IP et les autres renseignements personnels lorsque vous accédez à Internet.

Un RPV peut chiffrer les données aux deux points terminaux. Certains RPV peuvent également chiffrer les données en transit. Il est ainsi possible de sécuriser le trafic alors qu'il traverse les passerelles par l'intermédiaire du tunnel. Pour un niveau de sécurité plus élevé, votre organisation devrait envisager d'utiliser un RPV qui permet de chiffrer les données en transit.

La plupart des passerelles de RPV sont intégrées à un pare-feu. Dans plusieurs cas, le point terminal du transfert de données est un serveur particulier auquel l'utilisatrice ou utilisateur peut accéder. Votre organisation devrait exiger que les utilisatrices et utilisateurs saisissent leurs justificatifs d'identité pour accéder aux données chiffrées sur son réseau. Pour un niveau de sécurité plus élevé, votre organisation peut exiger que les utilisatrices et utilisateurs saisissent leurs justificatifs d'identité pour envoyer et recevoir des données chiffrées.

Types de réseaux privés virtuels

Votre organisation peut choisir parmi divers types de RPV.

De passerelle à passerelle : connexion de deux réseaux au moyen d'un RPV établi sur un réseau public qui permet de sécuriser tout le trafic transmis de l'un à l'autre. On utilise généralement ce type de RPV pour connecter des lieux de travail distants.

D'hôte à passerelle (accès à distance) : connexion permettant d'accéder à distance à un réseau d'entreprise (par exemple, à partir du portable d'une ou un employé en télétravail.

D'hôte à hôte : connexion permettant de connecter un hôte à une ressource particulière se trouvant sur un réseau d'entreprise ou à un autre hôte.

RPV tiers : connexion sécurisée entre un point d'accès public (comme le réseau Wi-Fi d'un aéroport ou d'un hôtel) et le RPV d'un fournisseur tiers. Ce dernier redirige alors le trafic de manière à ce qu'il semble provenir de son réseau.

Risques liés à l'utilisation d'un réseau privé virtuel

Les RPV peuvent comporter des risques pour la sécurité de votre organisation. Avant de faire appel à un service de RPV, votre organisation devrait faire des recherches et s'assurer que le service en question est conforme à ses politiques.

Certains facteurs peuvent accroître les risques pour votre organisation dans les circonstances suivantes :

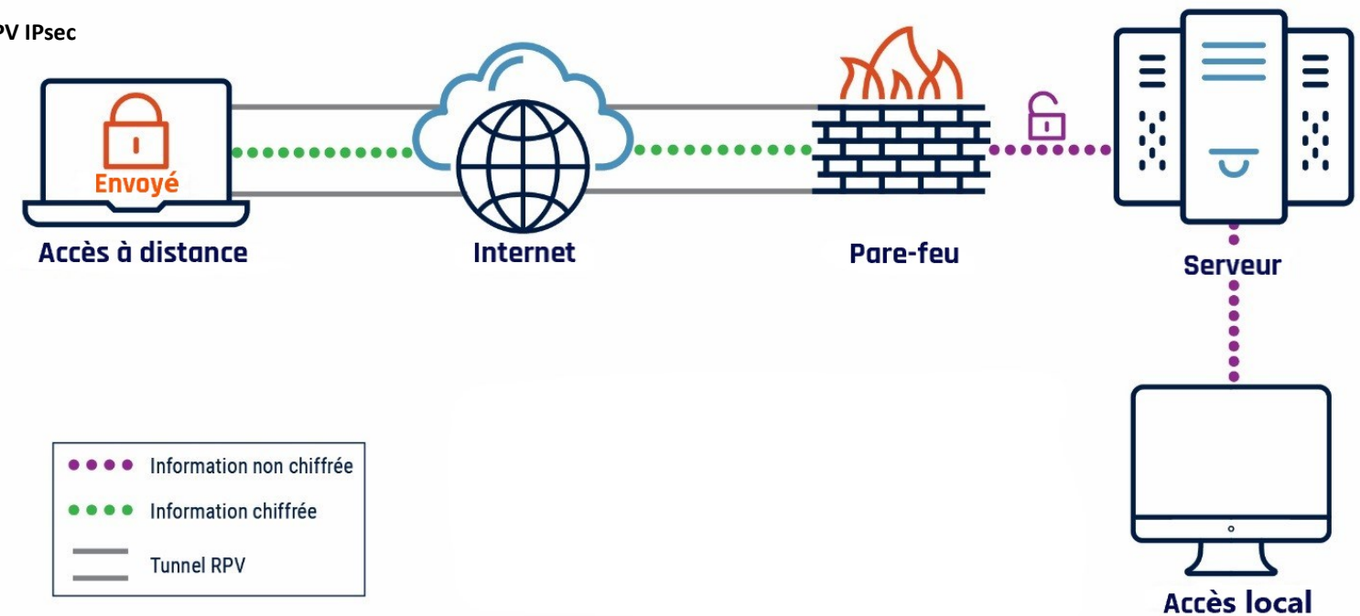
- Un RPV ne peut pas fournir le niveau de sécurité voulu si vous choisissez d'utiliser un réseau non fiable, comme un réseau Wi-Fi gratuit ou s'il y a des maliciels sur le réseau de l'organisation.
- La sécurité de votre information sera mise en péril advenant la compromission de votre clé de chiffrement.
- Certains services de RPV visent à masquer votre identité en ligne plutôt qu'à protéger vos données.

Sélection d'un réseau privé virtuel

Avant de sélectionner un RPV, votre organisation devrait déterminer ses capacités et ses exigences opérationnelles et évaluer les risques. Vous devez également considérer deux catégories de protocoles de sécurité de RPV : le protocole IPsec (Internet Protocol Security) et le protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*). Les protocoles déterminent la façon dont les données sont envoyées, reçues et sécurisées. Par exemple :

- Le protocole **IPsec** fait en sorte de chiffrer vos données et le tunnel à travers duquel elles traversent. Il est ainsi plus difficile pour les auteures et auteurs de menace d'obtenir vos données. Ce protocole exige une authentification des deux côtés pour envoyer et recevoir des données par l'entremise de ce RPV;
- Avec le protocole **TLS**, seul le tunnel à travers duquel les données transitent est chiffré. Si une ou un auteur de menace est en mesure de casser le chiffrement du tunnel, vos données ne seront plus protégées.

Figure 1 : Fonctionnement d'un RPV IPsec



Bien que les deux catégories de protocoles permettent d'assurer la confidentialité, l'intégrité et l'authenticité, ils le font de différentes manières et à différents degrés. Une des principales différences entre les protocoles IPsec et TLS est la couche où ils s'exécutent sur le modèle d'interconnexion de systèmes ouverts (OSI pour *Open Systems Interconnection*). Le modèle OSI comporte sept couches exécutant chacune une fonction différente. Plus le chiffre associé à la couche du modèle OSI sur laquelle s'exécute le RPV est bas, plus grand est le niveau de sécurisation du trafic dans la mesure où il se trouve à une plus grande distance des auteures et auteurs de menace. Le protocole TLS s'exécute dans les couches 4 à 7 (couche transport), tandis que le protocole IPsec s'exécute dans la couche 3 (couche réseau).

Le service des TI de votre ministère devrait déterminer les besoins en matière de sécurité propres à votre organisation avant de choisir un cadriciel pour le protocole de RPV. On recommande d'utiliser le protocole IPsec pour l'accès de site à site. La mise en place d'un tel protocole peut exiger des efforts supplémentaires, mais elle permet d'offrir une cybersécurité plus grande. Le protocole TLS est mieux adapté à l'accès à distance, puisqu'il exige moins de configuration. Consultez les listes comparatives ci-dessous pour en apprendre plus sur chacun des protocoles de RPV.

Sécurité du protocole Internet (IPsec)

- Prend en charge les connexions passerelle à passerelle et hôte à passerelle
- S'exécute dans la couche 3 du modèle OSI et les couches plus élevées et a recours à des protocoles d'authentification exigeant une clé prépartagée entre le client et le serveur
- Chiffre vos données aux points de départ et d'arrivée, de même qu'en transit, permettant ainsi un chiffrement complet de bout en bout
- Utilisation généralement réservée aux appareils fournis par une organisation en raison de ces exigences en matière de sécurité
- Exige l'installation d'une application cliente sur l'appareil terminal de l'utilisatrice ou utilisateur
- Propose un niveau de sécurité élevé en raison de sa surface d'attaque plus petite
- Exécute des tâches dans le noyau du système d'exploitation
- Freine les attaques de type adversaire au milieu en faisant appel à l'authentification par clé secrète partagée
- Permet de vérifier le paquet pour la présence de maliciels avant qu'il ne soit ouvert à sa destination
- Permet d'accéder aux ressources réseau de votre organisation (par exemple, les applications, les portails et les serveurs internes) comme si vous vous trouviez dans les installations
- Permet d'établir des communications entre ordinateurs tout en chiffrant l'ensemble des paquets réseau

Protocole de sécurité de la couche transport (TLS)

- Prend en charge les connexions hôte à passerelle
- S'exécute dans les couches 4 à 7 du modèle OSI
- Permet le chiffrement de l'expéditrice ou expéditeur à la cible indiquée, mais n'offre aucun chiffrement complet de bout en bout
- Peut être utilisé sur des appareils terminaux, comme un portable personnel, sur tous les systèmes d'exploitation et depuis tous les emplacements
- N'exige aucun téléchargement d'application, puisque la plupart des navigateurs sont déjà configurés de manière à prendre en charge le protocole TLS
- Offre un niveau de sécurité inférieur au protocole IPsec, puisque ses tâches s'exécutent depuis l'espace utilisateur dans les couches transport et application
- Exécute les tâches dans une couche plus exposée que l'on peut pirater plus facilement
- Permet une productivité limitée, car on ne peut se connecter à l'organisme qu'au moyen d'un navigateur
- Offre des contrôles d'accès personnalisés en fonction des utilisatrices et utilisateurs

Protection de vos données au moyen d'un réseau privé virtuel

Pour bien comprendre les risques associés à l'utilisation d'un RPV, votre organisation devrait déterminer le type et la valeur des données transmises ou accessibles par l'entremise de ce dernier. Vous devriez mettre en place des politiques claires sur l'utilisation que font les employées et employés du RPV pour accéder à distance aux serveurs de votre organisation.
La cryptographie asymétrique se définit par l'utilisation de deux clés ou justificatifs distincts aux fins de chiffrement et déchiffrement. Dans la mesure du possible, vous devriez configurer votre RPV de manière à avoir recours à la cryptographie asymétrique. Les utilisatrices et utilisateurs devraient donc être invités à saisir leurs justificatifs d'identité pour accéder à l'information.

Les organisations qui utilisent un RPV devraient envisager de faire ce qui suit :

- utiliser un jeton matériel qui ne peut être copié, comme un jeton RSA ou SecurID, pour fournir une sécurité additionnelle;
- activer l'authentification multifacteur;
- demander aux employées et employés de n'accéder aux comptes sensibles que par l'intermédiaire d'un RPV;
- veiller à ce que les employées et employés utilisent des Wi-Fi sécurisés (et non un Wi-Fi public) lorsqu'ils utilisent un RPV.

Renseignements supplémentaires

- *Utiliser le chiffrement pour assurer la sécurité des données sensibles* (ITSAP.40.016)
- *Étapes à suivre pour déployer efficacement l'authentification multifacteur* (ITSAP.00.105)
- *La sécurité du Wi-Fi* (ITSP.80.002)
- *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062)
- *Guide sur la segmentation en unités dans le cadre des services fondés sur l'infonuagique* (ITSP.50.108)