LES RÉSEAUX PRIVÉS VIRTUELS

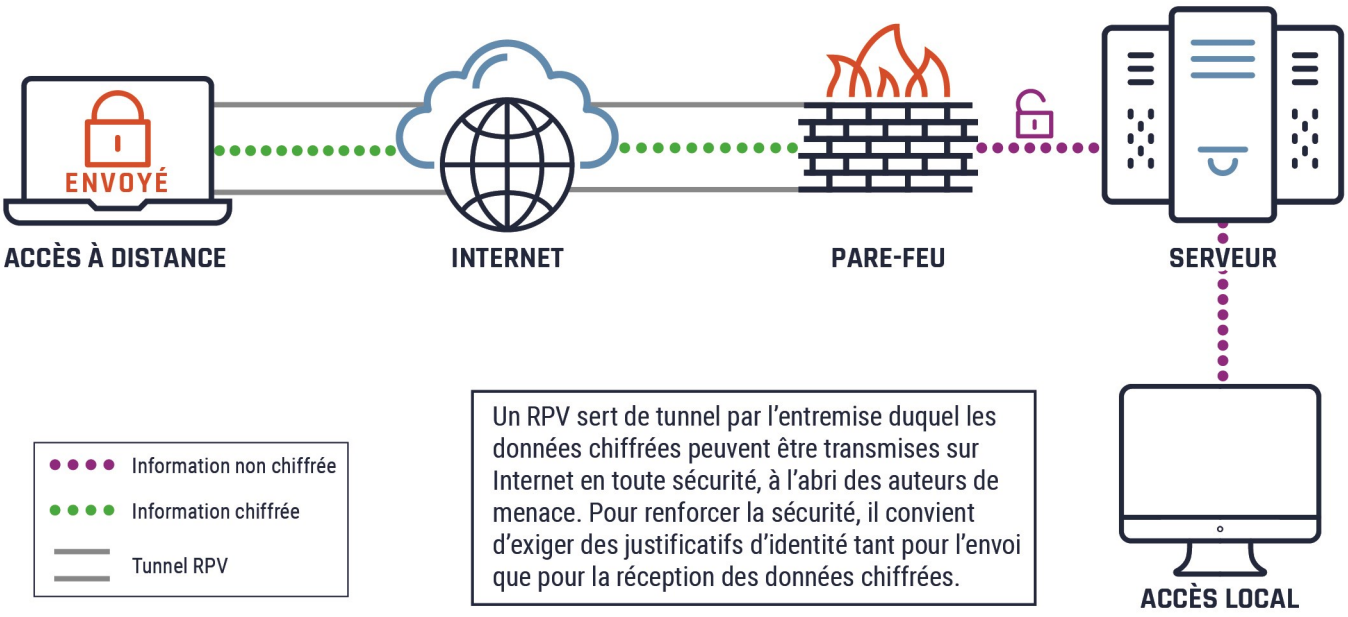
OCTOBRE 2019

ITSAP.80.101

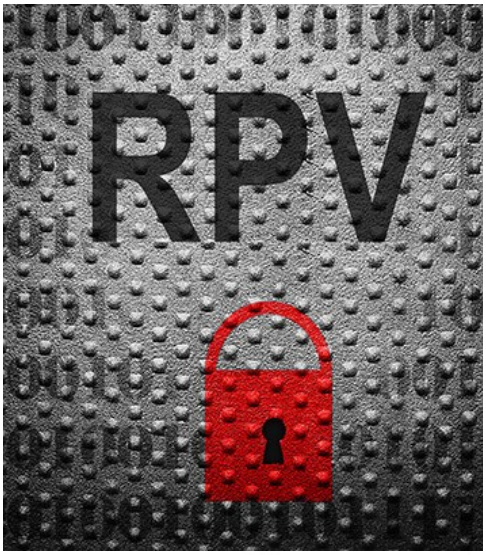
Un réseau privé virtuel (RPV) est une connexion sécurisée entre deux points, comme un ordinateur portable et le réseau d'une organisation. Le RPV sert de tunnel par l'entremise duquel on peut envoyer et recevoir des données sécurisées dans un réseau physique existant. Par exemple, un employé en télétravail pourra utiliser un RPV pour envoyer des données qui seront chiffrées jusqu'à leur destination (comme un serveur dans le lieu de travail, télétravailleur). Nous présentons ici quelques risques et facteurs dont il faut tenir compte avant d'utiliser des services RPV.

COMMENT FONCTIONNENT LES RPV?

L'image ci-dessous illustre comment un utilisateur distant envoie des données chiffrées au serveur de son organisation à l'aide d'un RPV. Les données chiffrées sont transmises par l'entremise d'un « tunnel » qui les protège contre les auteurs de menace. Dans l'image, on suppose que le tunnel de RPV se termine là où les données atteignent le pare-feu ou la passerelle RPV de l'organisation. La plupart des passerelles RPV sont intégrées au pare-feu. Ici, le point terminal du transfert de données est un serveur particulier auquel l'utilisateur peut accéder. L'utilisateur devrait donc être invité à saisir ses justificatifs d'identité pour accéder aux données chiffrées sur le réseau de l'organisation.



SÉRIE SENSIBILISATION



QUELS SONT LES 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 deux lieux de travail distants.

D'hôte à passerelle : connexion permettant à un utilisateur d'accéder à distance à un réseau d'entreprise (par exemple, à partir d'un portable ou d'un dispositif mobile).

D'hôte à hôte : connexion semblable à l'accès à distance par RPV, mais permettant de connecter un hôte à une ressource particulière se trouvant sur un réseau d'entreprise ou un autre hôte.

Protection de la vie privée des 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.

COMMENT PROTÉGER LES DONNÉES QUE L'ON ENVOIE OU AUXQUELLES ON ACCÈDE PAR L'ENTREMISE D'UN RPV?

Pour bien comprendre les risques associés à l'utilisation d'un RPV, votre organisation devrait déterminer quelles seront les données transmises ou accessibles par l'entremise d'un RPV et la valeur de ces données. Des politiques claires devraient être imposées aux employés qui utilisent un RPV pour accéder à distance à un serveur dans le lieu de travail.

Dans la mesure du possible, les paramètres de configuration devraient obliger les destinataires des données chiffrées à saisir leurs justificatifs d'authentification avant de pouvoir accéder à l'information. C'est ce qu'on appelle la cryptographie asymétrique : les fonctions de chiffrement et de déchiffrement exigent deux clés ou justificatifs distincts.

QUELS SONT LES RISQUES?

Les RPV peuvent comporter des risques pour la sécurité de votre organisation. Avant d'utiliser un service RPV, il importe de faire des recherches afin de vous assurer qu'il est conforme à vos politiques. Certains facteurs peuvent accroître les risques, notamment :

- Si vous choisissez d'utiliser un réseau non fiable (comme le Wi-Fi gratuit) ou si le réseau de l'organisation est infecté par des maliciels, un RPV ne permettra pas de vous protéger.
- La sécurité de l'information risque d'être compromise si la clé de chiffrement est divulguée ou volée.
- Certains services de RPV visent à masquer votre identité en ligne plutôt qu'à protéger vos données.

QUELS FACTEURS DOIVENT ÊTRE PRIS EN CONSIDÉRATION AVANT DDUTILISER UN RPV?

Les organisations qui utilisent un RPV devraient suivre les recommandations ci-dessous :

- Utiliser un jeton matériel qui ne peut être copié (p. ex. un jeton RSA) comme mesure de sécurité additionnelle.
- Utiliser l'authentification multifactorielle pour ajouter une couche de sécurité supplémentaire.
- Éviter d'ouvrir une session dans les comptes sensibles à moins d'utiliser un RPV.
- Veiller à ce que les employés utilisent des services de Wi-Fi sécurisés (et non le Wi-Fi gratuit) lorsqu'ils utilisent un RPV.
- Il existe de nombreux services de RPV gratuits et payants. Il convient de choisir celui qui correspond le mieux aux besoins de l'organisation (p. ex., taille, coût).

Vous avez des questions ou besoin d'assistance? Vous voulez en savoir plus sur les questions de cybersécurité? Visitez le site Web du Centre canadien pour la cybersécurité (CCCS) au **cyber.gc.ca.**