IPSSI

13 rue Claude Tillier

75013, Paris

Première

Veille technologique

Effectué le 9 juillet 2023

Spécialité : Technicien Systèmes et réseaux

Réalisé par :

Djimtone Ngarndo Moguidbe

Encadrer par :

Mr Taleb Kamel

SOMMAIRE

SOMMAIRE.....2

INTRODUCTION GENERALE.....3

Première veille technologique.....3

Qu'est-ce que le VPN ? 3

Types.....3

Intérêt.....4

VPN sur les routeurs.....4

Chiffrement.....5

Chiffreur IP.....5

Protocoles.....5

VPN dans les environnements mobiles.....6

Limitations du réseau.....7

Exemple de VPNs.....7

Introduction générale

Dans cette documentation, nous présenterons notre veille technologique qui est les vulnérabilités d'un réseau informatique.
Nous présenterons les outils que nous avons utilisé pour la réalisation de cette documentation et quelques sites importants à visiter.

Première veille technologique

Le sujet principal de ma veille technologique concerne la protection des données privées avec le VPN.

Qu'est-ce que le VPN ?

En informatique, un réseau privé virtuel (RPV) ou réseau virtuel privé (RVP), plus communément abrégé en VPN (de l'anglais : virtual private network), est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

On utilise notamment ce terme dans le télétravail, ainsi que dans le cadre de l'informatique en nuage.

Types

Le VPN peut être de type point à point, utilisé entre un client et un concentrateur VPN (routeur spécialisé, pare-feu, ou logiciel sur ordinateur), sur Internet par le biais d'un logiciel de VPN. Dans une autre acception, le VPN peut exister sous la forme d'un réseau privé virtuel hermétique et distribué sur un nuage MPLS. Les ordinateurs sur ce VPN y sont souvent raccordés physiquement, la notion de «

virtuel » se rapportant alors au fait que l'infrastructure MPLS fait circuler plusieurs réseaux virtuels étanches entre eux. De façon plus générale les VPN peuvent être classés selon les protocoles, services, et type de trafic (couche OSI. 2 ou 3) pouvant circuler en son sein.

Intérêt

Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. Il permet d'avoir un accès au réseau interne (réseau d'entreprise, par exemple) ou de créer un réseau de pairs.

Un VPN dispose généralement aussi d'une « passerelle » permettant d'accéder à l'extérieur, ce qui permet de changer l'adresse IP source apparente de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur : par exemple, les sociétés proposant des VPN gratuits ou payants peuvent récolter les données de navigation de leurs clients, ce qui relativise l'anonymat de ces services. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet.
Le VPN permet également de construire des « réseaux overlay », en construisant un réseau logique sur un réseau sous-jacent, faisant ainsi abstraction de la topologie de ce dernier.

L'utilisation de VPN n'est généralement pas légalement restreinte. Elle l'est en Chine. Jusqu'à mi-2017, le gouvernement semblait tolérer certains usages comme l'accès par un grand nombre de chercheurs chinois à des études publiées en ligne dans le monde mais inaccessibles en Chine en raison d'une censure du Net qui a classé non seulement Google Docs et Dropbox, mais aussi Google Scholar en liste noire. En septembre 2017, il semble que la Chine ait décidé d'encore resserrer l'accès des Chinois à Internet en accroissant la répression pour ceux qui utilisent des réseaux privés virtuels (VPN), donc non contrôlés par le gouvernement. La communauté scientifique internationale (relayée par la revue Science) craint que cette mesure puisse « sérieusement éroder la capacité des scientifiques chinois à rester en contact avec des pairs à l'étranger ».

VPN sur les routeurs

Avec l’utilisation croissante des VPN, beaucoup ont commencé à déployer la connectivité VPN sur les routeurs. Ainsi, l’objectif étant de renforcer la sécurité et le chiffrement de la transmission de données en utilisant diverses techniques cryptographiques. À domicile, les utilisateurs déploient généralement des réseaux privés virtuels sur leurs routeurs pour protéger des périphériques : tels que des téléviseurs intelligents ou des consoles de jeux qui ne sont pas pris en charge par les clients VPN natifs. Les périphériques pris en charge ne sont pas limités à ceux capables d’exécuter un client VPN10. De nombreux fabricants de routeurs fournissent des routeurs avec des clients VPN intégrés. Certains utilisent des microprogrammes open-source tels que DD-WRT, OpenWRT, et Tomato, afin de prendre en charge des protocoles supplémentaires tels que OpenVPN.

Chiffrement

Les connexions VPN ne sont pas nécessairement chiffrées. Cependant, si l'on ne chiffre pas, cela peut permettre à des éléments intermédiaires sur le réseau d'accéder au trafic du VPN, ce qui peut être problématique si les informations qui y transitent sont sensibles. De plus, des techniques de DPI permettent à des pares-feux de filtrer le trafic du VPN s'il n'est pas chiffré.

Chiffreur IP

Un chiffreur IP est un équipement de sécurité du réseau informatique, réalisant la fonction passerelle pour un réseau privé virtuel. Un chiffreur IP est placé au point d'entrée et de sortie d'un réseau local afin d'établir un lien de communication entre plusieurs de ces réseaux locaux, en utilisant un réseau externe considéré comme non sûr. Ce réseau externe peut être, par exemple, Internet. L'établissement de ces liaisons permet de constituer un réseau privé virtuel chiffré, augmentant ainsi la sécurité de la transmission d'informations d'un réseau à un autre, principalement en termes de confidentialité.

Protocoles

Un réseau privé virtuel utilise un ou plusieurs protocoles parmi les suivants :

- GRE (Generic Routing Encapsulation) développé au départ par Cisco, à l'origine protocole transportant des paquets de couche 3, mais pouvant désormais aussi transporter la couche 2.
- PPTP (Point-to-Point tunneling Protocol) est un protocole transportant des trames de couche 2 (du PPP) développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (Layer Two Forwarding) est un protocole transportant des trames PPP (couche 2) développé par Cisco Systems, Nortel et Shiva. Il est désormais obsolète.
  L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 3931) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole transportant des sessions PPP (couche 2).
- IPsec est un protocole transportant des paquets (couche 3), issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est associé au protocole IKE pour l'échange des clés.
- L2TP/IPsec est une association de ces deux protocoles (RFC 3193) pour faire passer du PPP sur L2TP sur IPsec, en vue de faciliter la configuration côté client sous Windows.
- SSL/TLS, déjà utilisé pour sécuriser la navigation sur le web via HTTPS, permet également l'utilisation d'un navigateur Web comme client VPN. Ce protocole est notamment utilisé par OpenVPN.
- SSH permet, entre autres, d'envoyer des paquets depuis un ordinateur auquel on est connecté.
- MPLS permet de créer des VPN distribués (VPRN) sur un nuage MPLS, de niveau 2 (L2VPN) point à point, point à multipoint (VPLS), ou de niveau 3 (L3VPN) notamment en IPv4 (VPNv4) et/ou IPv6 (VPNv6 / 6VPE), par extension et propagation de VRF (Virtual routing and forwarding – tables de routage virtuelles) sur l'ensemble du réseau MPLS.

VPN dans les environnements mobiles

Les réseaux privés virtuels mobiles sont utilisés dans des paramètres où un point de terminaison du VPN n'est pas fixé à une seule adresse IP, mais se déplace à la place sur divers réseaux tels que les réseaux de données d'opérateurs cellulaires

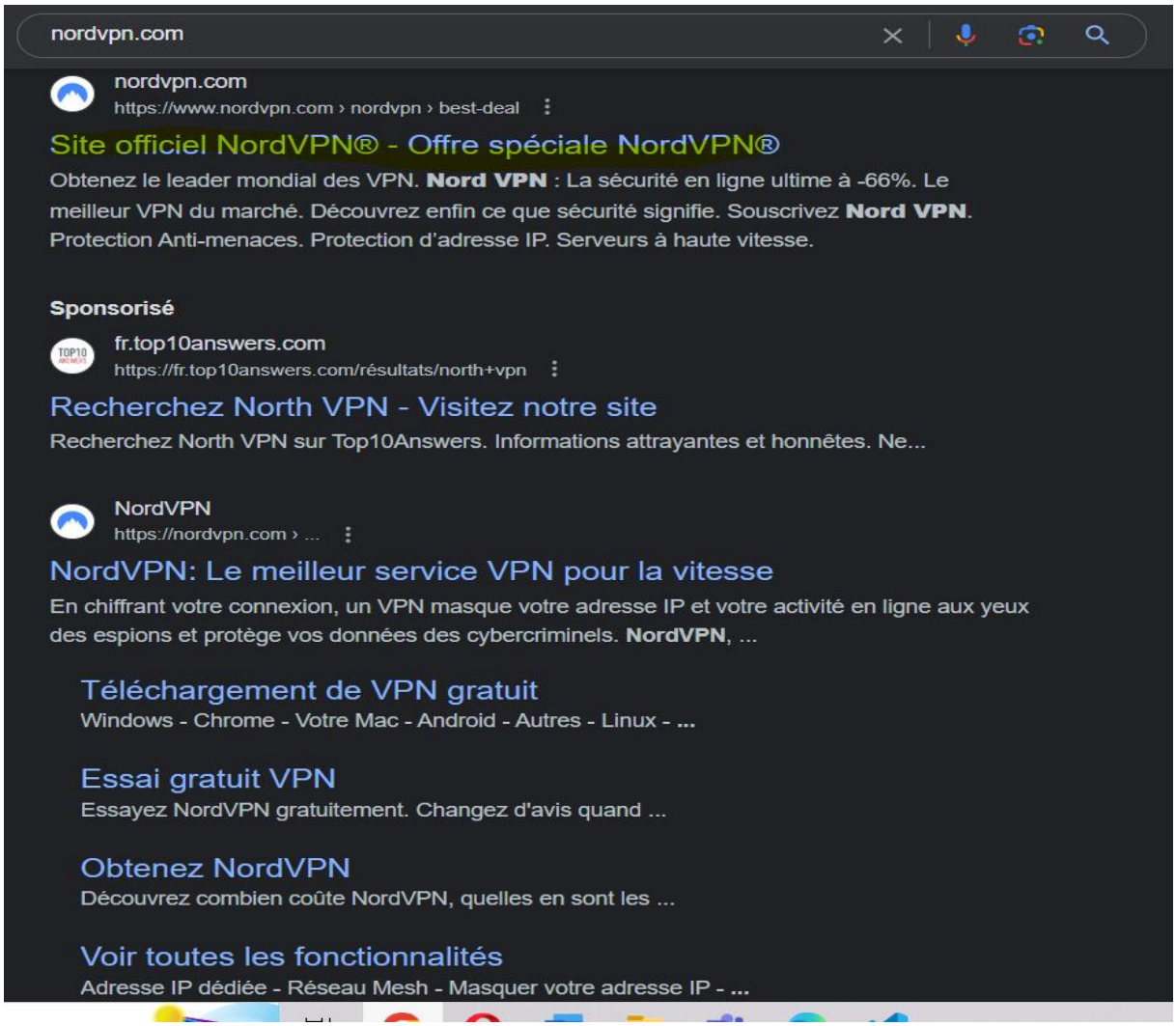
ou entre plusieurs points d'accès Wi-Fi sans abandonner la session VPN sécurisée ou perdre des sessions d'application. Les VPN mobiles sont largement utilisés dans la sécurité publique où ils donnent aux agents des forces de l'ordre l'accès à des applications telles que la répartition assistée par ordinateur et les bases de données criminelles, et dans d'autres organisations ayant des exigences similaires telles que la gestion des services sur le terrain et les soins de santé.

Limitations du réseau.

Une limitation des VPN traditionnels est qu'ils sont des connexions point à point et n'ont pas tendance à prendre en charge les domaines de diffusion ; par conséquent, la communication, les logiciels et la mise en réseau, qui sont basés sur la couche 2 et les paquets de diffusion, tels que NetBIOS, utilisé dans la mise en réseau Windows, peuvent ne pas être entièrement pris en charge comme sur un réseau local. Des variantes de VPN telles que Virtual Private LAN Service (VPLS) et les protocoles de tunneling de couche 2 sont conçues pour surmonter **cette limitation.**

Exemple de VPNs

Lorsque vous vous rendez sur le navigateur Web Google Chrome, et que vous tapez : Nordvpn, le premier lien de site qui apparaît, mène au site NordVPN, site auquel je suis abonné.

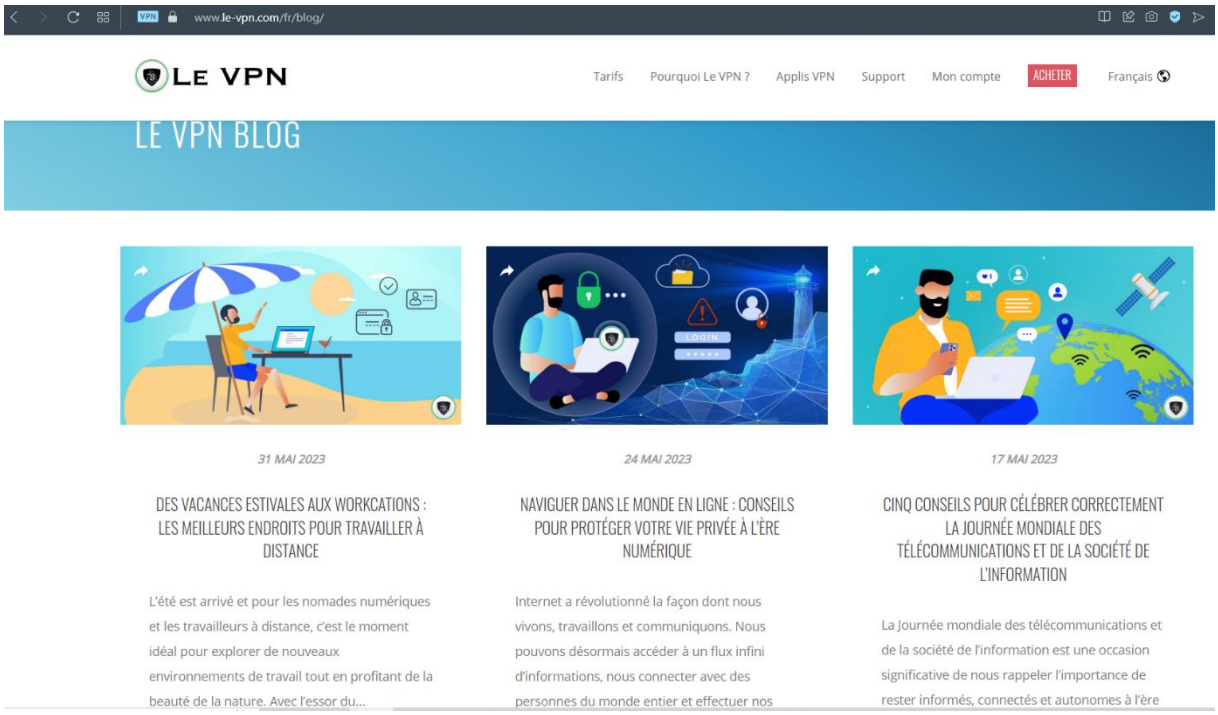


NordVPN est un service de réseau privé virtuel (VPN) fourni par l'entreprise Nord Security (Nordsec Ltd). Il propose des applications de bureau pour Microsoft Windows, macOS et Linux. Des applications mobiles sont disponibles pour Android et iOS ainsi que pour Android TV. La configuration manuelle est notamment disponible pour les routeurs sans fil, les périphériques de serveur de stockage en réseau et autres plateformes utilisable uniquement par abonnement, il donne accès à plus de 5500 serveurs dans 59 pays et permet une utilisation simultanée sur six appareils différents. L'entreprise Nord Security qui possède la marque NordVPN est basée au Panama, paradis fiscal, puisque le pays n'a pas de loi de conservation des données et ne participe pas aux alliances Five Eyes ou Fourteen eye. Elle dispose de bureaux en Lituanie, au Panama, au Royaume-Uni et aux Pays-Bas. Les fondateurs de l'entreprise sont Tom Okman, Eimantas Sabaliauskas, et Jonas Karklys.

Ce site Internet propose 3 VPNs :

- NordVPN (confidentialité et sécurité totales en ligne). Permet de travailler, regarder du contenu en streaming, naviguer sur Internet et jouer en toute sécurité
- NordPas (gestionnaire de mots de passe sécurisé et facile à utiliser).
- NordLocker (protection des fichiers avec stockage cloud sécurisé)

Le VPN a été créé en France, plus précisément à Paris, en novembre 2010 par une équipe de passionnés des questions de liberté et de cybersécurité sur internet, soucieux d'apporter à tous une solution pour protéger la sécurité et la vie privée. Les fondateurs ont uni leurs forces, leurs connaissances et leur expertise en matière de cybersécurité (acquises à l'école d'ingénieurs Centrale Supélec) et de gestion (acquises à l'école de commerce INSEAD), et ont constitué une équipe aux convictions similaires et diversifiées, originaire du monde entier.
Le VPN a même un onglet "Blog & Actualités", où sont publiés des articles sur le sujet de la technologie.


www.le-vpn.com/fr/blog/
LE VPN
Tarifs
Pourquoi Le VPN ?
Applis VPN
Support
Mon compte
ACHETER
Français
LE VPN BLOG
31 MAI 2023
DES VACANCES ESTIVALES AUX WORKCATIONS : LES MEILLEURS ENDROITS POUR TRAVAILLER À DISTANCE
L'été est arrivé et pour les nomades numériques et les travailleurs à distance, c'est le moment idéal pour explorer de nouveaux environnements de travail tout en profitant de la beauté de la nature. Avec l'essor du...
24 MAI 2023
NAVIGUER DANS LE MONDE EN LIGNE : CONSEILS POUR PROTÉGER VOTRE VIE PRIVÉE À L'ÈRE NUMÉRIQUE
Internet a révolutionné la façon dont nous vivons, travaillons et communiquons. Nous pouvons désormais accéder à un flux infini d'informations, nous connecter avec des personnes du monde entier et effectuer nos
17 MAI 2023
CINQ CONSEILS POUR CÉLÉBRER CORRECTEMENT LA JOURNÉE MONDIALE DES TÉLÉCOMMUNICATIONS ET DE LA SOCIÉTÉ DE L'INFORMATION
La Journée mondiale des télécommunications et de la société de l'information est une occasion significative de nous rappeler l'importance de rester informés, connectés et autonomes à l'ère