Soumission indépendante
Demande de commentaires : 5684
Catégorie : Information
ISSN : 2070-1721

P. Srisuresh, EMC Corporation
B. Ford, Université Yale
février 2010
Traduction Claude Brière de L'Isle

Conséquences imprévues des déploiements de NAT avec des espaces d'adresses en chevauchement

Résumé
Ce document identifie deux scénarios de déploiement qui se sont produits à partir de topologies de réseau non conventionnelles formées en utilisant des appareils de traduction d'adresse réseau (NAT, *Network Address Translator*). Tout d'abord, la simplicité de l'administration des réseaux via la combinaison de NAT et DHCP a conduit de plus en plus au déploiement de réseaux privés interconnectés à plusieurs niveaux impliquant des espaces d'adresses IP privés qui se chevauchent. Deuxièmement, la prolifération des réseaux privés dans les entreprises, les hôtels et conférences, ainsi que l'utilisation généralisée des réseaux privés virtuels (VPN) pour accéder à un intranet d'entreprise à partir d'emplacements distants conduisent de plus en plus à un chevauchement de l'espace d'adresses IP privées entre réseaux distants et d'entreprise. Ce document n'écarte pas les scénarios non conventionnels comme invalides, mais les reconnaît comme réels et propose des recommandations pour aider à garantir que ces déploiements peuvent fonctionner sans provoquer de catastrophes.

Table des matières

1. Introduction et portée

À l'origine, l'Internet a été conçu pour utiliser un seul espace d'adresses IP mondial de 32 bits pour identifier de manière univoque les hôtes sur le réseau, permettant des applications sur un hôte pour adresser et initier des communications avec des applications sur tout autre hôte, indépendamment de la localisation topologique ou des domaines administratifs des hôtes respectifs. Pour diverses raisons pratiques, cependant, l'Internet s'est progressivement éloigné du strict respect de cet idéal d'un espace plat d'adresse globale unique et s'est dirigé vers une hiérarchie d'espaces d'adressage "privés" plus petits de la [RFC1918] regroupés autour d'un grand espace d'adresses "public" central. Les causes pratiques les plus importantes de cette évolution involontaire de l'architecture d'Internet semblent être les suivantes.

1. L'épuisement de l'espace d'adresses IPv4 de 32 bits en raison de l'explosion du nombre total d'hôtes sur Internet. Bien que l'IPv6 promette de résoudre ce problème, l'adoption d'IPv6 a été en pratique plus lente que prévu.

2. Sécurité et confidentialité perçues : les appareils de NAT traditionnels offrent une fonction de filtrage qui permet aux flux de session de traverser le NAT dans une seule direction, des hôtes privés vers les hôtes du réseau public. Cette fonction de filtrage est largement perçue comme un avantage en matière de sécurité. De plus, la traduction par le NAT de l'adresse et numéro d'accès IP d'origine d'un hôte dans un réseau privé en une adresse et numéro d'accès externe sans rapport sont perçus par certains comme un avantage en matière de confidentialité.

3. Facilité d'utilisation : les fournisseurs de NAT combinent souvent la fonction de NAT avec une fonction de serveur DHCP dans le même appareil, qui crée une méthode convaincante et efficace "prête à l'emploi" pour la mise en place de petits réseaux personnels connectés à l'Internet souvent beaucoup plus faciles à utiliser en pratique pour des consommateurs non avertis que la configuration d'un sous-réseau IP. Les nombreux appareils de NAT grand public populaires et peu coûteux sur le marché sont généralement configurés "prêt à l'emploi" pour obtenir une adresse IP "publique" unique d'un FAI ou d'un réseau "en amont" via DHCP ([RFC2131]) et l'appareil de NAT agit à son tour comme un serveur DHCP et routeur par défaut pour tous les hôtes "en aval" (et même d'autres NAT) que l'utilisateur y connecte. Les NAT grand public de cette façon créent et gérent efficacement des réseaux domestiques privés automatiquement sans nécessiter aucune connaissance des protocoles réseau ni de gestion de la part de l'utilisateur. L'auto-configuration des hôtes privés font des appareils de NAT une solution convaincante dans ce scénario courant.

La [RFC3027] identifie diverses complications liées aux protocoles d'application dus aux appareils de NAT. Le présent document sert de complément à la [RFC3027]. La portée du document est limitée aux deux scénarios identifiés dans les sections 3 et 4, découlant du déploiement de NAT non conventionnel et du chevauchement de l'espace d'adresses privé. Même si les scénarios semblent non conventionnels, ils n'est pas rare de les trouver. Pour chaque scénario, le document décrit les anomalies apparentes et propose des recommandations sur la meilleure façon de faire fonctionner les topologies.

La Section 2 décrit la terminologie et les conventions utilisées dans le document. La Section 3 décrit le problème du chevauchement de l'espace d'adresses privé dans une topologie de NAT à plusieurs niveaux, les anomalies avec la topologie et des recommandations pour remédier aux anomalies. La Section 4 décrit le problème du chevauchement de l'espace d'adresses privé avec l'accès distant aux connexions de réseaux privés virtuels (VPN) les anomalies avec la topologie et les recommandations pour remédier aux anomalies. La Section 5 décrit les considérations de sécurité dans ces scénarios.

2. Terminologie et conventions utilisées

Dans ce document, les adresses IP 192.0.2.1, 192.0.2.64, 192.0.2.128 et 192.0.2.254 sont utilisées comme exemples d'adresses IP publiques [RFC5735]. Bien que ces adresses proviennent toutes du même réseau /24, il s'agit d'une limitation des exemples d'adresses disponibles dans la [RFC5735]. En pratique, ces adresses seraient sur des réseaux différents.

Les lecteurs sont invités à se référer à la [RFC2663] pour plus d'informations sur la taxonomie et terminologie de NAT. Sauf préfixe avec un type de NAT ou sauf indication contraire explicite, le terme NAT, utilisé dans ce document, fait référence au NAT traditionnel [RFC3022]. Le NAT traditionnel a deux variantes, à savoir, le NAT de base et le traducteur d'adresse/accès réseau (NAPT, *Network Address Port Translator*). Parmi ceux-ci, le NAPT est de loin l'appareil de NAT le plus couramment déployé. Le NAPT permet à plusieurs hôtes privés de partager simultanément une seule adresse IP de réseau public.

3. Topologies de réseau de NAT à plusieurs niveaux

En raison des considérations pratiques discutées dans la section précédente et peut-être d'autres, les NAT sont de plus en plus, et souvent involontairement, utilisés pour créer des grappes interconnectées hiérarchiquement de réseaux privés comme illustré dans la figure 1 ci-dessous. La création de hiérarchies multi-niveaux est souvent involontaire, car chaque niveau de NAT est généralement déployé par une entité administrative distincte telle qu'un FAI, une entreprise ou un particulier.

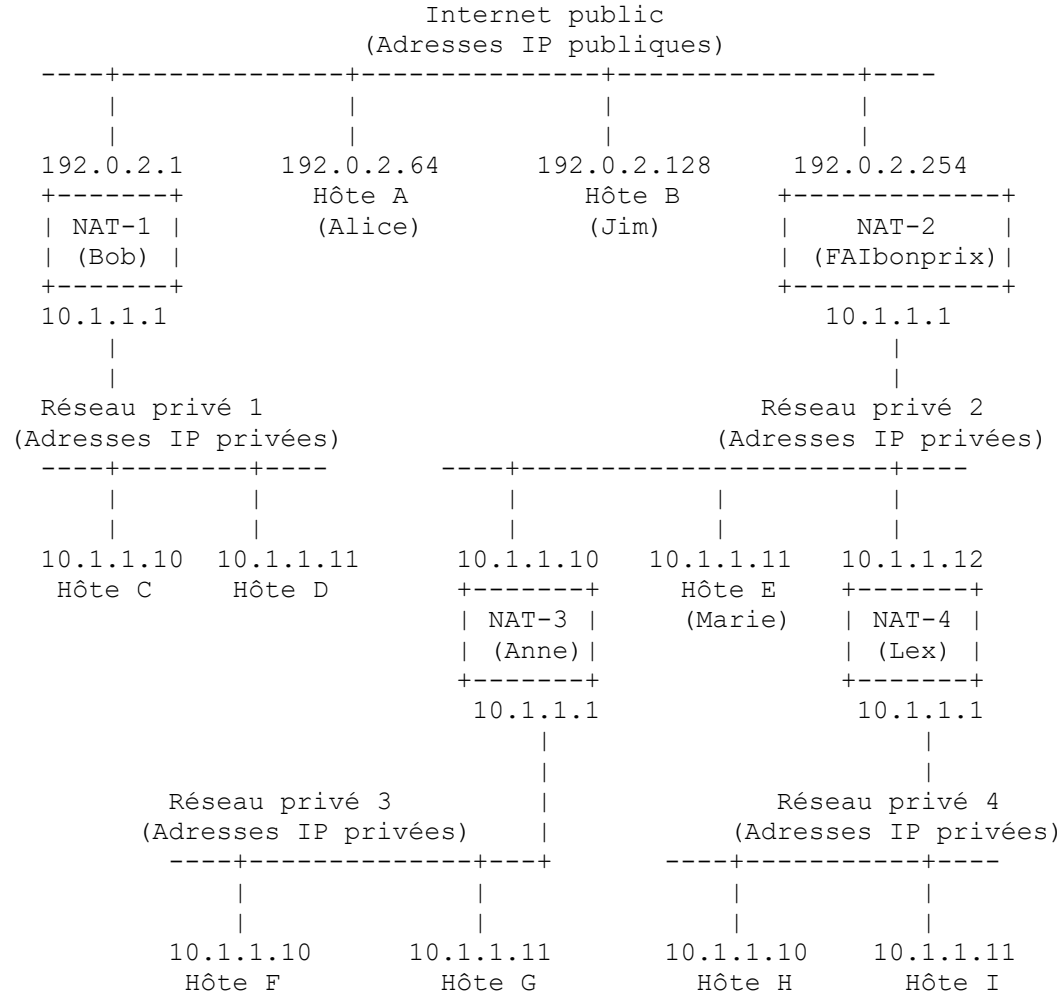


Figure 1. Topologie de NAT à plusieurs niveaux avec chevauchement de l'espace d'adresses

Dans le scénario ci-dessus, Bob, Alice, Jim et FAIbon prix ont chacun obtenu une adresse IP "authentique" et acheminable mondialement à partir d'un prestataire de services en amont. Alice et Jim ont choisi de n'attacher qu'une seule machine à chacune de ces adresses IP publiques, en préservant l'architecture initialement prévue de l'Internet et rendant leurs hôtes, A et B, adressables mondialement sur l'Internet. Bob, en revanche, a acheté et connecté un boîtier de NAT grand public classique. Le NAT de Bob obtient son adresse IP externe (192.0.2.1) du FAI de Bob via DHCP et crée automatiquement un réseau privé 10.1.1.x pour les hôtes C et D de Bob, agissant comme serveur DHCP et routeur par défaut pour ce réseau privé. Bob ne sait probablement même rien au sujet des adresses IP ; il sait simplement qu'en connectant le NAT à l'Internet comme indiqué par le FAI, puis en connectant ses hôtes au NAT comme le manuel du NAT l'indique, tout semble fonctionner et donner à tous ses hôtes accès à l'Internet.

FAIbonprix, un fournisseur de services bon marché, n'a alloué qu'une ou quelques adresses IP acheminables mondialement et utilise le NAT pour partager les adresses IP publiques parmi ses nombreux clients. Un tel arrangement est devenu de plus en plus fréquent, en particulier dans les pays en développement rapide où l'explosion du nombre d'hôtes connectés à l'Internet dépasse largement la capacité des FAI à obtenir pour eux des adresses IP uniques au niveau mondial. FAIbonprix a choisi l'adresse populaire 10.1.1.x pour son réseau privé, car c'est l'un des trois blocs d'adresses IP privées bien connus alloués dans la [RFC1918] spécifiquement à cet effet.

Parmi les trois incitations énumérées dans la section 1 pour le déploiement de NAT, les deux dernières s'appliquent toujours même aux clients des FAI qui utilisent un NAT, résultant en des topologies de NAT à plusieurs niveaux comme illustré au côté droit du diagramme ci-dessus. Même des topologies de NAT à trois niveaux sont connues. Les clients de FAIbonprix, Ann, Mary et Lex ont chacun obtenu une unique adresse IP sur le réseau de FAIbonprix (réseau privé 2) via DHCP. Mary ne connecte qu'un seul hôte à ce stade, mais Ann et Lex achètent et déploient chacun indépendamment des NAT grand public de la même manière que Bob l'a fait ci-dessus. Il s'avère que ces NAT consommateurs utilisent également des adresses 10.1.1.x pour les réseaux privés qu'ils créent, car ce sont les valeurs par défaut de configuration incorporées dans les NAT par leurs fabricants. Ann et Lex ne savent probablement rien sur les adresses IP, et en particulier, ils ne savent probablement pas que les espaces d'adresses IP de leurs propres réseaux privés se chevauchent non seulement entre eux mais aussi avec l'espace d'adresse IP privé utilisé par leur réseau immédiatement en amont.

Néanmoins, malgré ce chevauchement direct, tous les hôtes de NAT "multi-niveaux" - F, G, H et I dans ce cas - fonctionnent tous nominalement et sont capables d'initier des connexions à n'importe quel serveur public sur l'Internet public doté d'une adresse IP acheminable à l'échelle mondiale. Les connexions faites à partir de ces hôtes vers l'Internet principal sont simplement traduites deux fois : une fois par le NAT consommateur (NAT-3 ou NAT-44) dans l'espace d'adresse IP du réseau privé 2 de FAIbonprix, puis à nouveau par le NAT-2 de FAIbonprix dans l'espace d'adresses IP mondial de l'Internet public.

3.1 Détails opérationnels du réseau de NAT à plusieurs niveaux

Dans l'architecture d'adresse Internet "de facto" qui a résulté des incitations pratiques et économiques ci-dessus, seuls les nœuds sur l'Internet public possèdent des adresses IP uniques au niveau mondial allouées par les registres d'adresses IP officiels. Les adresses IP sur les différents réseaux privés sont normalement gérées de manière indépendante, soit manuellement par l'administrateur du réseau privé lui-même, soit automatiquement par le NAT via lequel le réseau privé est connecté à son prestataire de services "en amont".

Par convention, les nœuds des réseaux privés se voient généralement attribuer une adresse IP dans l'une des plages d'espaces d'adresses privées spécifiquement allouées à cet effet dans la RFC 1918, assurant que les adresses IP privées sont facilement reconnaissables et n'entrent pas en conflit avec les adresses IP publiques officiellement attribuées aux hôtes de l'Internet acheminables à l'échelle mondiale. Cependant, lorsque des NAT prêts à l'emploi sont utilisés pour créer des grappes de réseaux privés interconnectées hiérarchiquement, l'adresse IP privée donnée peut être, et est souvent, réutilisée à travers de nombreux réseaux privés différents. Dans la figure 1 ci-dessus, par exemple, les réseaux privés 1, 2, 3 et 4 ont tous un nœud avec l'adresse IP 10.1.1.10.

3.1.1 Communication client/serveur

Lorsqu'un hôte sur un réseau privé initie une session de communication de type client/serveur avec un serveur sur l'Internet public, via l'adresse IP publique du serveur, le NAT intercepte les paquets comprenant cette session (généralement en raison du fait d'être le routeur par défaut pour le réseau privé) et modifie les en-têtes IP et TCP/UDP des paquets afin de faire apparaître la session à l'extérieur comme si elle était initiée par le NAT lui-même.

Par exemple, si l'hôte C ci-dessus initie une connexion à l'hôte A à l'adresse IP 192.0.2.64, NAT-1 modifie les paquets constituant la session afin d'apparaître sur l'Internet public comme si la session provenait de NAT-1. De même, si l'hôte F sur le réseau privé 3 lance une connexion à l'hôte A, NAT-3 modifie le paquet sortant afin que le paquet apparaisse sur le réseau privé 2 comme s'il provenait de NAT-3 à l'adresse IP 10.1.1.10. Lorsque le paquet modifié traverse NAT-2 sur le réseau privé 2, NAT-2 modifie encore le paquet sortant afin d'apparaître sur l'Internet public comme s'il provenait de NAT-2 à l'adresse IP publique 192.0.2.254. Les NAT en vigueur servent de mandataires qui donnent à leurs nœuds clients "en aval" privés une présence temporaire sur les réseaux "en amont" pour accompagner les séssions de communication individuelles.

En résumé, tous les hôtes des réseaux privés 1, 2, 3 et 4 dans la figure 1 ci-dessus sont capables d'établir des sessions de communication de style client/serveur avec des serveurs sur l'Internet public.

3.1.2 Communication d'homologue à homologue

Bien que cette organisation en réseau fonctionne en pratique pour la communication de type client/serveur, lorsque le client est derrière un ou plusieurs niveaux de NAT et que le serveur est sur l'Internet public, le manque d'adresses acheminables mondialement pour les hôtes sur les réseaux privés rend difficile la communication directe d'homologue à homologue entre

ces hôtes. Par exemple, deux hôtes privés F et H sur le réseau illustré ci-dessus pourraient "se rencontrer" et apprendre à se connaître via un serveur bien connu sur l'Internet public, tel que l'hôte A, et désirer établir une communication directe entre G et H sans demander à A de transmettre chaque paquet. Si G et H apprennent simplement les adresses IP (privées) de l'autre à partir d'un registre tenu par A, leurs tentatives de se connecter l'un l'autre échoueront car G et H résident sur des réseaux privés différents. Pire encore, si leurs tentatives de connexion ne sont pas correctement authentifiées, ils peuvent sembler réussir mais finir par parler au mauvais hôte. Par exemple, G peut finir par parler à l'hôte F, l'hôte sur le réseau privé 3 qui se trouve avoir la même adresse IP privée que l'hôte H. L'hôte H pourrait également finir par se connecter involontairement à l'hôte I.

En résumé, la communication d'homologue à homologue entre hôtes sur les réseaux privés disjoints 1, 2, 3 et 4 de la figure 1 ci-dessus constituent un défi sans l'aide d'un serveur connu sur l'Internet public. Cependant, avec l'aide d'un nœud de l'Internet public, tous les hôtes sur les réseaux privés 1, 2, 3 et 4 de la figure 1 ci-dessus sont capables d'établir une session de communication de type homologue à homologue entre eux-mêmes ainsi qu'avec les hôtes sur l'Internet public.

3.2 Anomalies du réseau de NAT multi-niveaux

Même si la sagesse conventionnelle suggère que le réseau décrit ci-dessus est sérieusement cassé, en pratique, il fonctionne toujours de nombreuses façons. Nous divisons la figure 1 en deux sous-figures pour mieux illustrer les anomalies. La figure 1.1 est la moitié gauche de la figure 1 et reflète le déploiement de NAT unique conventionnel qui est largement répandu dans de nombreuses localisations du dernier kilomètre. Le déploiement illustré à la figure 1.1 est généralement considéré comme une solution pragmatique pour contourner le problème de l'épuisement de l'espace d'adresses IPv4 et n'est pas considéré comme cassé. La Figure 1.2 est la moitié droite de la figure 1 et est représentative des anomalies dont nous allons discuter.

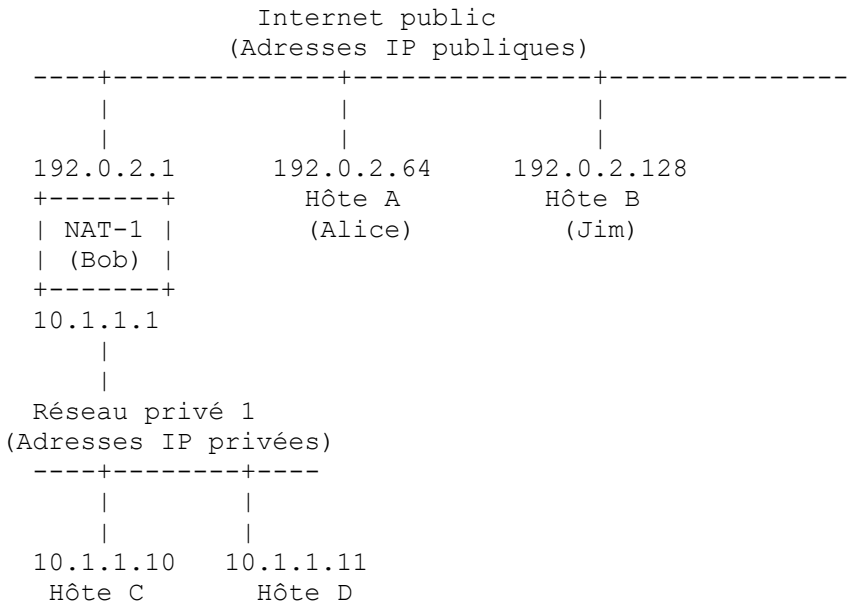
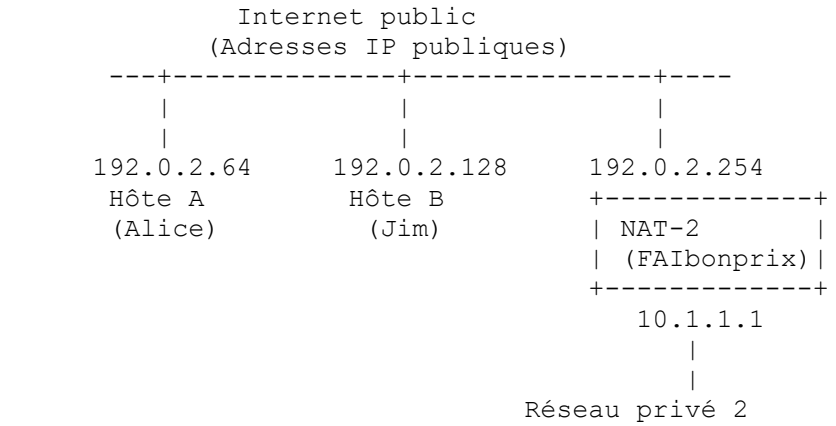


Figure 1.1. Topologie de réseau de NAT classique à un seul niveau



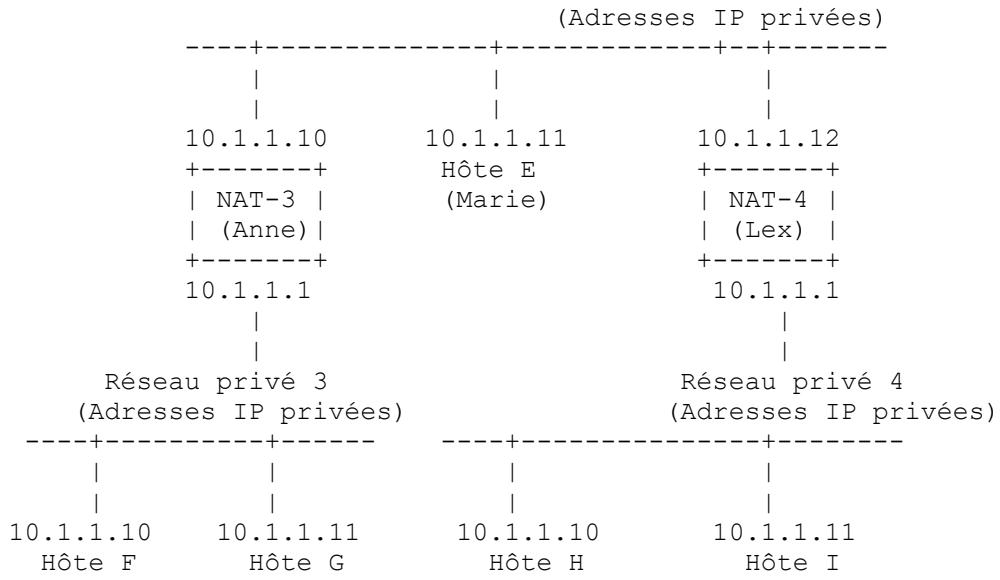


Figure 1.2. Topologie de réseau de NAT multi-niveaux non conventionnelle

3.2.1 Appareils de NAT prêts à l'emploi

Les appareils de NAT grand public sont principalement des appareils de NAT prêts à l'emploi, et supposent une intervention minimale de l'utilisateur lors de la configuration de l'appareil. Les appareils de NAT prêts à l'emploi fournissent un service DHCP sur une interface et la fonction de NAT sur une autre interface. Les fabricants des appareils de NAT grand public font des hypothèses sur la façon dont leurs consommateurs configurent et connectent leurs PC à l'appareil. Lorsque les consommateurs ne respectent pas les hypothèses du fabricant, ils peuvent se retrouver avec un réseau défaillant.

Un appareil de NAT prêt à l'emploi fournit un service DHCP sur le LAN rattaché à l'interface privée, et suppose que tous les hôtes privés du site consommateur ont un client DHCP activé et sont connectés à ce LAN unique. Les consommateurs doivent être conscients que tous les hôtes privés doivent être sur un seul LAN, sans routeur au milieu.

Un appareil de NAT prêt à l'emploi suppose également qu'il n'y a pas d'autre appareil de NAT ou appareil de serveur DHCP sur le même LAN chez le client local. Lorsqu'il existe plusieurs appareils de NAT prêts à l'emploi sur le même LAN, chaque appareil de NAT va offrir un service DHCP sur le même LAN, et peut même provenir du même réservoir d'adresses privées. Cela pourrait entraîner que plusieurs nœuds d'extrémité sur le même LAN se retrouvant avec des adresses IP identiques et une rupture de la connexité au réseau.

Il s'avère que la plupart des déploiements grand public disposent d'un seul LAN dans lequel ils déploient un appareil de NAT prêt à l'emploi et où les préoccupations soulevées ci-dessus n'ont pas été un problème dans la réalité.

3.2.2 Adressage non conventionnel sur les appareils de NAT

Considérons l'adressage non conventionnel avec NAT-3 et NAT-4. NAT-3 et NAT-4 sont apparemment multi-hébergés sur le même sous-réseau via leurs deux interfaces. NAT-3 est sur le sous-réseau 10.1.1/24 via son interface externe face à NAT-2, ainsi que via son interface privée face aux clients de l'hôte F et l'hôte G. De même, NAT-4 a également deux interfaces sur le même sous-réseau 10.1.1/24.

Dans un réseau traditionnel, lorsqu'un nœud possède plusieurs interfaces avec des adresses IP sur le même sous-réseau, il est naturel de supposer que toutes les interfaces avec des adresses sur le même sous-réseau doivent être sur un seul LAN connecté (LAN ponté ou LAN physique unique). De toute évidence, cela ce n'est pas le cas ici. Même si NAT-3 et NAT-4 ont tous deux deux interfaces sur le même sous-réseau 10.1.1/24, les appareils de NAT voient les deux interfaces comme étant sur deux sous-réseaux et domaines d'acheminement disjoints. Les appareils de NAT prêt à l'emploi ne sont pas vraiment multi-hébergés sur le même sous-réseau au sens traditionnel du terme.

Dans un réseau traditionnel, NAT-3 et NAT-4 de la figure 1.2 devraient tous deux être incapables de communiquer de manière fiable en tant que points d'extrémité de transport avec d'autres nœuds sur leurs réseaux adjacents (par exemple, les

réseaux privés 2 et 3 dans le cas de NAT-3 et de réseaux privés 2 et 4 dans le cas de NAT-4). Cela est dû au fait que les applications sur l'un ou l'autre des appareils de NAT ne savent pas différencier les paquets des hôtes sur l'un ou l'autre sous-réseaux portant la même adresse IP. Si NAT-3 tente de résoudre l'adresse IP d'un hôte voisin de manière conventionnelle en diffusant une demande du protocole de résolution d'adresse (ARP, *Address Resolution Protocol*) sur toutes ses interfaces physiques portant le même sous-réseau, il peut obtenir une réponse différente sur chacune de ses interfaces physiques.

Même si NAT-3 et NAT-4 ont tous deux des hôtes portant la même adresse IP sur les réseaux adjacents, les appareils de NAT communiquent efficacement comme points d'extrémité. De nombreux appareils de NAT prêt à l'emploi offrent un nombre limité de services. Par exemple, de nombreux appareils de NAT répondent aux pings des hôtes sur l'une ou l'autre des interfaces. Même si un appareil de NAT n'est souvent pas géré activement, de nombreux appareils de NAT sont équipés pour être gérés à partir de l'interface privée. Cette communication non conventionnelle avec des appareils de NAT est réalisable car de nombreux appareils de NAT sont conformes à la REQ-7 de la [RFC4787] et considèrent les deux interfaces comme étant sur deux domaines d'acheminement disjoints et distinguent les sessions initiées à partir d'hôtes sur l'une ou l'autre interface (privée ou publique).

3.2.3 Traductions de NAT à plusieurs niveaux

L'utilisation d'un seul NAT pour connecter des hôtes privés à l'Internet public comme dans la figure 1.1 est une pratique assez courante. De nombreux NAT grand public sont déployés de cette façon. Cependant, l'utilisation de traductions de NAT à plusieurs niveaux comme dans la figure 1.2 n'est pas une pratique courante et n'est pas bien comprise.

Considérons la traduction de NAT simple conventionnelle de la figure 1.1. Parce que les gammes d'adresses IP publiques et privées sont numériquement disjointes, les nœuds des réseaux privés peuvent utiliser les deux adresses IP publiques et privées lors de l'initiation de sessions de communication réseau. Les nœuds sur un réseau privé peuvent utiliser des adresses IP privées pour se référer à d'autres nœuds sur le même réseau privé et des adresses IP publiques pour faire référence à des nœuds sur l'Internet public. Par exemple, l'hôte C de la figure 1.1 est sur le réseau privé 1 et peut s'adresser directement aux hôtes A, B et D en utilisant leurs adresses IP allouées. C'est en dépit du fait que les hôtes A et B sont sur l'Internet public et que l'hôte D seul est sur le réseau privé.

Ensuite, considérons la topologie de NAT multi-niveaux non conventionnelle dans la figure 1.2. Dans ce scénario, les hôtes privés sont capables de se connecter aux hôtes sur l'Internet public. Mais les hôtes privés ne sont pas en mesure de se connecter à tous les autres hôtes privés. Par exemple, l'hôte F dans la figure 1.2 peut s'adresser directement aux hôtes A, B et G en utilisant leurs adresses IP allouées, mais F n'a aucun moyen de s'adresser à l'un des autres hôtes du diagramme. L'hôte F en particulier ne peut pas s'adresser à l'hôte E par son adresse IP allouée, même si l'hôte E est situé immédiatement dans le réseau privé "en amont" par lequel F est connecté à l'Internet. L'hôte E a la même adresse IP que l'hôte G. Pourtant, cet adressage est "légitime" dans le monde des NAT parce que les deux hôtes sont sur des réseaux privés différents.

Il semblerait que la topologie de la figure 1.2 avec plusieurs traductions de NAT soit cassée parce que les hôtes privés ne sont pas en mesure de s'adresser directement les uns aux autres. Cependant, le réseau n'est pas rompu. Les nœuds sur tout réseau privé n'ont pas de méthode directe pour s'adresser aux nœuds sur les autres réseaux privés. Les réseaux privés 1, 2, 3 et 4 sont tous disjoints. Les hôtes du réseau privé 1 ne peuvent pas s'adresser directement aux nœuds sur les réseaux privés 2, 3 ou 4 et vice versa. Les traductions multiples de NAT n'en sont pas la cause.

Comme décrit aux paragraphes 3.1.1 et 3.1.2, la communication client-serveur et d'homologue à homologue peut et devrait être possible même avec des déploiements à plusieurs niveaux de de topologie de NAT. Un hôte sur n'importe quel réseau privé doit être capable de communiquer avec n'importe quel autre hôte, sans considération du réseau privé auquel l'hôte est rattaché ou de la localisation du réseau privé. L'hôte F devrait être capable de communiquer avec l'hôte E et d'effectuer les communications de client-serveur et d'homologue à homologue, et vice versa. L'hôte F et l'hôte E forment une session en épingle à cheveux à travers NAT-2 pour communiquer entre eux. Chaque hôte utilise le point d'extrémité public alloué par le NAT face à l'Internet (NAT-2) pour s'adresser à son homologue.

Lorsque les appareils de NAT déployés sont conformes aux exigences de la traduction en épingle à cheveux dans les [RFC4787], [RFC5382] et [RFC5508], les nœuds homologues sont capables de se connecter même dans ce type de topologies NAT multi-niveaux.

3.2.4 Erreur d'identité de l'hôte final

Une erreur d'identité de l'hôte final peut entraîner un dysfonctionnement accidentel dans certains cas de déploiements de NAT à plusieurs niveaux. Considérons le scénario de la Figure 1.3. La Figure 1.3 illustre deux niveaux de NAT entre une

extrémité utilisateur dans le réseau privé 3 et l'Internet public.

Supposons que FAIbonprix alloue 10.1.1.11 à son résolveur DNS, ce qu'il annonce via DHCP à NAT-3, la passerelle vers le réseau de rattachement de Anne. NAT-3 à son tour annonce 10.1.1.11 comme résolveur DNS à l'hôte F (10.1.1.10) età*- l'hôte G (10.1.1.11) sur le réseau privé 3. Cependant, lorsque l'hôte F envoie une interrogation du DNS à 10.1.1.11, elle sera livrée localement à l'hôte G sur le réseau privé 3 plutôt que sur le résolveur DNS de FAIbonprix. Il s'agit clairement d'un cas d'identité erronée du fait que FAIbonprix annonce un serveur qui pourrait potentiellement se chevaucher avec les adresses IP de ses consommateurs.

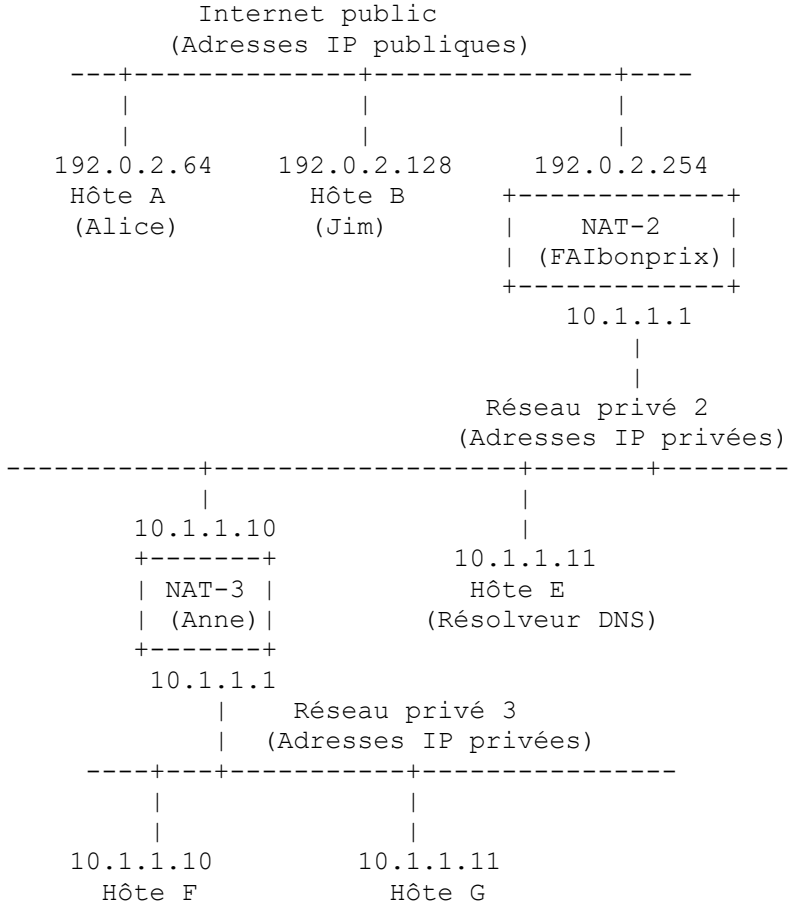


Figure 1.3. Erreur d'identité de serveur dans une topologie de NAT à plusieurs niveaux

Recommandation-1 : les FAI qui utilisent des appareils de NAT pour fournir la connexité aux clients devraient allouer des adresses non chevauchantes aux serveurs annoncés aux consommateurs. Une façon de procéder serait d'allouer des adresses mondiales aux serveurs annoncés.

4. Topologies de réseau VPN d'accès à distance

Les entreprises utilisent un VPN d'accès à distance pour permettre un accès sécurisé aux employés travaillant en dehors des locaux de l'entreprise. En dehors des locaux de l'entreprise, un employé peut être situé à son domicile, bureau, hôtel, conférence ou bureau d'un partenaire. Dans tous les cas, il est souhaitable que l'employé sur le site distant ait un accès libre à son réseau d'entreprise et aux applications exécutées sur le réseau de l'entreprise. Ce faisant, l'employé ne devrait pas mettre en péril l'intégrité et la confidentialité du réseau de l'entreprise et des applications exécutées sur le réseau.

IPsec, protocole de tunnelage de couche 2 (L2TP) et la couche de prises sécurisée (SSL) font partie des technologies de VPN sécurisées bien connues utilisées par les fournisseurs d'accès à distance. En plus d'authentifier les employés pour l'octroi d'accès, les serveurs de VPN d'accès à distance appliquent souvent différentes formes de sécurité (par exemple, IPsec, SSL) pour protéger l'intégrité et confidentialité du trafic d'exécution entre le client VPN et le serveur VPN.

De nombreuses entreprises déploient leurs réseaux internes à l'aide d'espaces d'adresses privées tels que définis dans la RFC 1918 et utilisent des appareils de NAT pour se connecter à l'Internet public. En outre, de nombreuses applications dans le réseau d'entreprises font référence aux informations (telles que les URL) et aux services utilisant des adresses privées dans le réseau d'entreprise. Des applications telles que les systèmes de fichiers réseau (NFS) reposent sur un simple filtrage d'adresse IP de source pour restreindre l'accès aux utilisateurs de l'entreprise. Voici quelques raisons pour lesquelles les serveurs de VPN d'accès à distance sont configurés avec un bloc d'adresses IP du réseau privé de l'entreprise à allouer aux clients d'accès à distance. Les clients de VPN utilisent l'adresse IP virtuelle (VIP) qui leur est allouée (par le serveur VPN de l'entreprise) pour accéder aux applications à l'intérieur du réseau d'entreprise.

Considérons le scénario VPN d'accès à distance dans la Figure 2 ci-dessous.

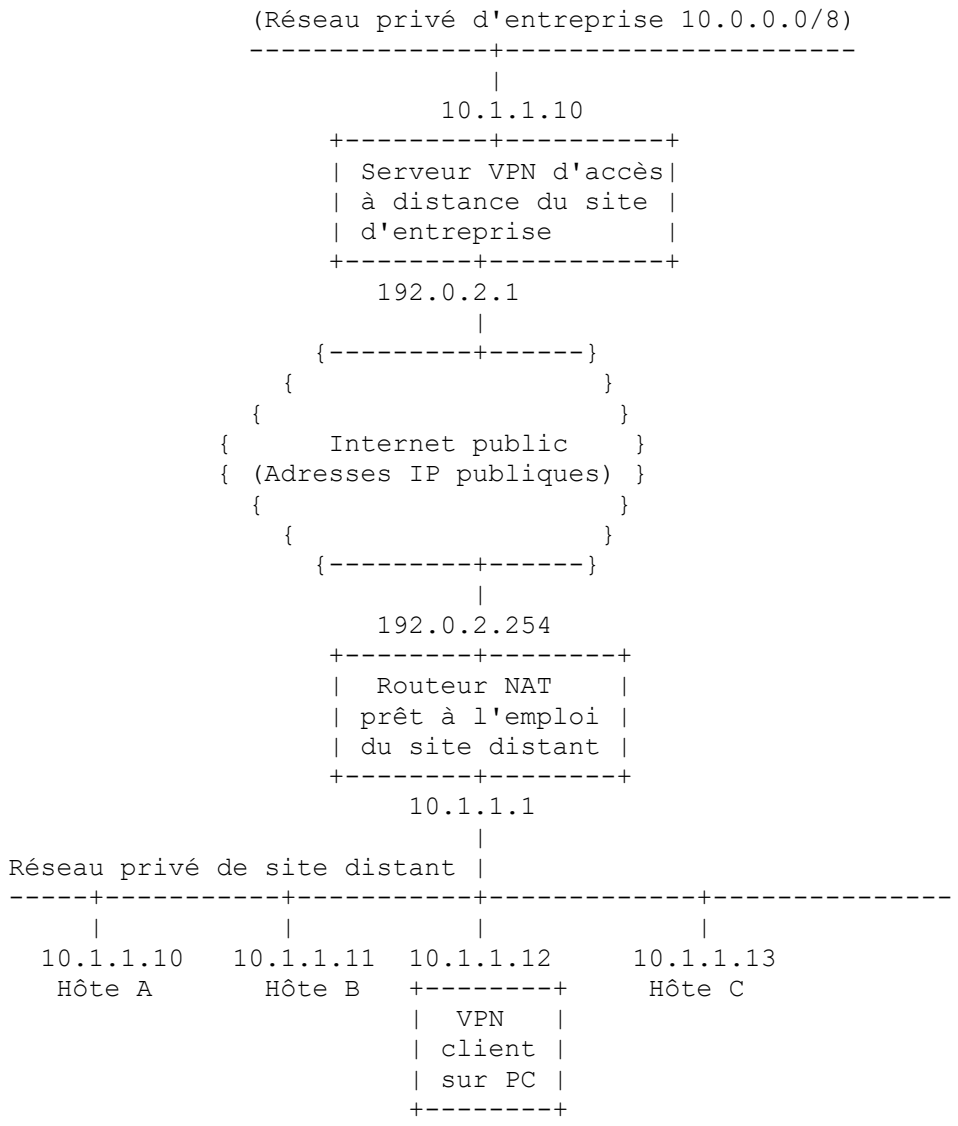


Figure 2. VPN d'accès à distance avec espace d'adresses superposé

Dans le scénario ci-dessus, disons qu'un employé de la société se trouve à un emplacement distant et tente d'accéder au réseau d'entreprise en utilisant le client VPN, le réseau d'entreprise est aménagé à l'aide du réservoir d'adresses de 10.0.0.0/8 tel que défini dans la RFC 1918, et le serveur VPN est configuré avec un bloc d'adresse de 10.1.1.0/24 pour allouer des adresses IP virtuelles aux clients VPN d'accès distant. Maintenant, disons que l'employé du site distant est connecté à un réseau sur le site distant qui utilise également un réseau fondé sur l'espace d'adressage de la RFC 1918 et chevauche par coïncidence le réseau d'entreprise. Dans ce scénario, il est traditionnellement problématique pour le client VPN de se connecter au serveur et aux autres hôtes de l'entreprise.

Néanmoins, malgré le chevauchement d'adresses directes, la connexion VPN d'accès à distance entre le client VPN du site distant et le serveur VPN de l'entreprise devrait rester connectée et devrait fonctionner. C'est-à-dire que l'appareil de NAT

sur le site distant ne devrait pas obstruer la connexion VPN qui le traverse. De plus, l'utilisateur distant devrait pouvoir se connecter à n'importe quel hôte de l'entreprise via le VPN depuis le bureau à distance.

Les paragraphes suivants décrivent les détails opérationnels du VPN, les anomalies avec le chevauchement d'adresses et les recommandations sur la manière de procéder au mieux pour régler la situation.

4.1 Détails opérationnels du réseau VPN d'accès à distance

Comme mentionné précédemment, dans l'architecture d'adresse Internet "de facto", seuls les nœuds de l'Internet public ont des adresses IP mondialement uniques allouées par les registres d'adresses IP officiels. De nombreux réseaux périphériques utilisent des adresses IP privées issues de la RFC 1918 et utilisent des appareils de NAT pour connecter leurs réseaux privés à l'Internet public. De nombreuses entreprises ont adapté l'approche consistant à utiliser des adresses IP privées en interne. Les employés dans les réseaux privés intranet de l'entreprise sont "de confiance" et peuvent se connecter à n'importe lequel des hôtes internes avec des frais généraux minimaux d'application administrative ou de politique. Lorsqu'un employé quitte les locaux de l'entreprise, l'accès VPN à distance fournit le même niveau de connexité intranet à l'utilisateur distant.

L'objectif de cette section est de fournir un aperçu des détails opérationnels d'une application VPN d'accès à distance afin que le lecteur ait une compréhension du problème du chevauchement des espaces d'adresses distantes. Ceci n'est en soi pas un tutoriel ni une spécification de produits de produits de VPN d'accès à distance.

Lorsqu'un employé sur un site distant lance son VPN d'accès à distance client, le serveur VPN dans les locaux de l'entreprise exige que le VPN client s'authentifie. Lorsque l'authentification réussit, le serveur VPN alloue une adresse IP virtuelle (VIP) au client pour se connecter à l'intranet de l'entreprise. À partir de ce moment, pendant que le VPN est actif, les paquets IP sortants dirigés vers les hôtes dans l'intranet de l'entreprise sont tunnelés à travers le VPN, dans la mesure où le VPN le serveur sert de bond suivant et la connexion VPN de liaison de prochain bond pour ces paquets. Au sein de l'intranet de l'entreprise, les paquets IP sortants apparaissent comme provenant de l'adresse VIP. Ainsi, les paquets IP sortants provenant des hôtes de l'entreprise pour l'utilisateur distant sont envoyés à l'adresse VIP de l'utilisateur distant et les paquets IP sont tunnelés vers le PC de l'utilisateur distant via le tunnel VPN.

Cela fonctionne bien tant que les sous-réseaux du réseau d'entreprise ne sont pas en conflit avec les sous-réseaux du site distant où se trouve le PC de l'utilisateur distant. Cependant, lorsque le réseau d'entreprise est construit à l'aide de l'espace d'adresses privé de la RFC 1918 et que l'emplacement distant où le VPN client est lancé utilise également un réseau superposé d'espace d'adresses de la RFC 1918, il peut y avoir des conflits d'adressage. Le PC de l'utilisateur distant aura un conflit en accédant aux nœuds sur le site de l'entreprise et aux nœuds sur le site distant portant simultanément la même adresse IP. Par conséquent, le client VPN peut ne pas être en mesure d'avoir un accès complet au réseau d'entreprise de l'employé et au réseau local du site distant simultanément.

Malgré le chevauchement des adresses, les clients VPN d'accès à distance doivent pouvoir établir avec succès des connexions avec des hôtes intranet dans l'entreprise.

4.2 Anomalies des VPN d'accès à distance

Même si la sagesse conventionnelle suggère que le scénario d'accès à distance à un VPN avec un espace d'adressage qui se chevauche serait sérieusement cassé, dans la pratique, cela fonctionne encore de nombreuses façons. On regarde quelques anomalies où il pourrait y avoir un problème et on identifie des solutions grâce auxquelles l'application VPN d'accès à distance pourrait être mise en œuvre même dans des situations problématiques.

4.2.1 Conflit d'adresse entre le routeur distant et le serveur DHCP

L'acheminement et le service DHCP sont des services d'amorçage essentiels pour un hôte distant pour établir une connexion VPN. Sans prêt DHCP, l'hôte distant ne peut pas communiquer sur le réseau IP. Sans routeur pour se connecter à l'Internet, l'hôte distant ne peut pas accéder au delà du sous-réseau local pour se connecter au serveur VPN de l'entreprise. Il est essentiel qu'aucun de ces services d'amorçage ne soit altéré sur l'hôte distant pour que la connexion VPN reste opérationnelle. Normalement, un appareil de NAT prêt à l'emploi sur le site distant fournit à la fois les services d'acheminement et DHCP à partir de la même adresse IP.

Lorsqu'il y a chevauchement d'adresses entre les hôtes de l'intranet de l'entreprise et les hôtes sur le site distant, l'utilisateur VPN distant n'est souvent pas au courant du conflit d'adresse. Le chevauchement d'adresses pourrait potentiellement

provoquer chez l'utilisateur distant la perte complète de la connexité à l'entreprise ou de perdre la connexité à un bloc arbitraire d'hôtes dans l'entreprise.

Considérons, par exemple, un scénario dans lequel l'adresse IP du serveur DHCP du site distant correspondrait à l'adresse IP d'un hôte du réseau d'entreprise. Lorsque le PC de l'utilisateur distant est prêt à renouveler le prêt de l'adresse IP allouée localement, le client VPN de l'utilisateur distant identifierait à tort le paquet IP comme étant adressé à un hôte de l'entreprise et tunnellerait le paquet de renouvellement DHCP sur le VPN pour le serveur VPN distant. Les demandes de renouvellement DHCP n'atteindront tout simplement pas le serveur DHCP sur le site distant. En conséquence, le PC distant finira par perdre le prêt de l'adresse IP et la connexion VPN à l'entreprise sera rompue.

Considérons un autre scénario dans lequel l'adresse IP du routeur de l'utilisateur distant se superpose à l'adresse IP d'un hôte du réseau de l'entreprise. Si le PC de l'utilisateur distant devait envoyer un ping ou un type de paquets de maintien en vie périodique au routeur (par exemple, pour tester la vivacité du routeur) les paquets seraient interceptés par le client VPN et simplement redirigés vers le tunnel VPN. Ce type de redirection non intentionnelle a le double effet de détourner les paquets critiques adressés au routeur ainsi qu'à ce que l'hôte dans le réseau d'entreprise (portant la même adresse IP que le routeur distant) soit bombardé de paquets de maintien en vie imprévus. La perte de connexité au routeur peut entraîner l'interruption de la connexion VPN.

Il est clair qu'il n'est pas souhaitable d'acheminer le trafic dirigé sur le routeur local ou que le serveur DHCP soit redirigé vers l'intranet de l'entreprise. Un client VPN sur un PC distant devrait être configuré de telle sorte que les paquets IP dont l'adresse IP cible correspond à l'une des suivantes ne soient pas autorisés à être redirigés sur le VPN :

a) Adresse IP du routeur de bond suivant du client VPN, utilisée pour accéder au serveur VPN.

b) Adresse IP du serveur DHCP, fournissant un prêt d'adresse sur l'interface réseau de l'hôte distant.

Recommandation-2 : un client VPN sur un PC distant devrait être configuré de telle sorte que les paquets IP dont l'adresse IP cible correspond à *l'un* des éléments (a) ou (b) ne soient pas autorisés à être redirigés via le VPN :
a) Adresse IP du routeur de bond suivant du client VPN, utilisé pour accéder au serveur VPN.
b) Adresse IP du serveur DHCP, fournissant un prêt d'adresse sur l'interface réseau de l'hôte distant.

4.2.2 Conflit de connectivité simultanée

Idéalement parlant, il n'est pas souhaitable que l'intranet de l'entreprise soit en conflit avec l'un des hôtes du site distant. En règle générale, si la communication simultanée avec les hôtes finaux à l'emplacement distant est importante, il est conseillé d'interdire l'accès à toute ressource de réseau d'entreprise qui chevauche le sous-réseau du client au site distant. En faisant cela, l'utilisateur distant peut se connecter à tous les hôtes locaux simultanément pendant que la connexion VPN est active.

Certains clients VPN permettent au PC distant d'accéder au réseau de l'entreprise via le VPN et tous les autres sous-réseaux directement sans acheminement via le VPN. Une telle configuration est appelée configuration de "VPN partagé". La configuration de "VPN partagé" permet à l'utilisateur distant d'exécuter des applications nécessitant une communication avec les hôtes du site distant ou de l'Internet public, ainsi que les hôtes de l'intranet de l'entreprise, sauf s'il y a chevauchement d'adresse avec le sous-réseau distant. Les applications nécessitant un accès aux hôtes du site distant ou à l'Internet public ne le font pas en traversant le VPN et sont donc susceptibles d'avoir de meilleures performances par rapport à la traversée du VPN. Cela peut être très utile pour les applications sensibles à la latence telles que la voix sur IP (VoIP) et le jeu interactif. S'il n'y a pas de problème de sécurité majeur à accéder directement aux hôtes du site distant ou à l'Internet public, le client VPN sur le PC distant devrait être configuré en mode "VPN partagé".

Si la connexité simultanée aux hôtes du site distant n'est pas importante, le client VPN peut être configuré pour diriger tous le trafic de communication de l'utilisateur distant vers le VPN. Une telle configuration est appelée configuration de "VPN non divisé". La configuration de "VPN non divisé" garantit que toutes les communications depuis la télécommande du PC de l'utilisateur traversent la liaison VPN et sont acheminées via le serveur VPN, à l'exception du trafic dirigé vers le routeur et le serveur DHCP sur le site distant. Aucune autre communication n'a lieu avec les hôtes sur le site distant. Les applications nécessitant un accès à l'Internet public traversent également le VPN. Si l'objectif est de maximiser la sécurité et la fiabilité de la connexité au réseau de l'entreprise, le client VPN sur le PC distant doit être configuré en mode "VPN non divisé". La configuration en "VPN non divisé" minimisera la probabilité de perte d'accès aux hôtes d'entreprise.

Recommandation-3 : un client VPN sur un PC distant devrait être configuré en mode "VPN non divisé" si l'objectif de déploiement est (a), ou en mode "VPN divisé" si l'objectif de déploiement est (b) :

a) Si l'objectif est de maximiser la sécurité et la fiabilité de connexité au réseau d'entreprise, le client VPN sur le PC distant doit être configuré en mode "VPN non divisé". Le mode "VPN non divisé" garantit que le client VPN dirige tout le trafic de l'utilisateur distant sur le serveur VPN (sur le site de l'entreprise) à l'exception du trafic dirigé vers le routeur et le serveur DHCP sur le site distant.

b) Si il n'existe aucun problème de sécurité majeur empêchant l'accès direct des hôtes sur le site distant ou sur l'Internet public, le client VPN sur le PC distant doit être configuré en mode "VPN partagé". Le mode "VPN partagé" garantit que seul le trafic de l'entreprise est dirigé vers le VPN. Tout autre trafic n'a pas les frais généraus de traversée du VPN.

4.2.3 Conflit d'adresse VIP

Lorsque l'adresse VIP allouée au client VPN sur le site distant est en conflit direct avec l'interface de l'adresse IP du réseau existant, le client VPN peut être incapable d'établir la connexion au VPN.

Considérons un scénario dans lequel l'adresse VIP allouée par le serveur VPN correspond directement à l'adresse IP de l'interface réseau au site distant. Lorsque le client VPN sur l'hôte distant tente de définir l'adresse VIP sur un adaptateur virtuel (spécifique de l'application d'accès à distance) la configuration de l'adresse VIP échouera simplement en raison du conflit avec l'adresse IP de l'interface réseau existante. L'échec de la configuration peut à son tour entraîner l'échec de l'établissement du tunnel d'accès à distance du VPN.

Il est clairement déconseillé de faire chevaucher l'adresse VIP avec l'adresse IP de l'interface réseau existante de l'utilisateur distant. En règle générale, il n'est pas conseillé que l'adresse VIP se chevauche avec une adresse IP dans le sous-réseau local de l'utilisateur distant, car le client VPN sur le PC distant pourrait être obligé de répondre aux demandes ARP sur le site distant et le client VPN pourrait ne pas traiter en douceur les demandes d'ARP.

Certains fournisseurs de VPN proposent des dispositions pour détecter les conflits d'adresses VIP avec l'espace d'adresses de site distant et le basculement entre deux réservoirs d'adresses ou plus avec différents sous-réseaux, afin que l'adresse VIP allouée ne soit pas en conflit avec l'espace d'adresses sur le site distant. Il est conseillé aux entreprises qui déploient des VPN qui prennent en charge ce type de provisionnement de fournisseur de configurer le serveur VPN avec un minimum de deux réservoirs distincts d'adresses IP. Cependant, ce n'est pas toujours le cas.

Autrement, les entreprises peuvent déployer deux serveurs VPN ou plus avec différents réservoirs d'adresses. Ce faisant, un client VPN qui détecte un conflit d'adresse VIP avec le sous-réseau du site distant aura la possibilité de passer à un autre serveur VPN qui n'est pas en conflit.

Recommandation-4 : il est conseillé aux entreprises qui déploient des solutions VPN d'accès à distance d'adopter une stratégie (a) ou (b) pour éviter un conflit d'adresse VIP avec le sous-réseau du site distant.

a) Si le serveur VPN en cours de déploiement a été configuré pour configurer deux réservoirs d'adresses ou plus, configurer le serveur VPN avec un minimum de deux réservoirs d'adresses IP distincts.
b) Déployer deux serveurs VPN ou plus avec des réservoirs d'adresses IP distincts. Ce faisant, un client VPN qui détecte des conflits d'adresses VIP avec le sous-réseau sur le site distant aura la possibilité de commuter vers un autre serveur VPN qui n'entrera pas en conflit.

4.2.4 Erreur d'identité de l'hôte final

Lorsque le "VPN partagé" est configuré sur le client VPN sur un PC distant, il peut y avoir une menace potentielle pour la sécurité en raison d'une erreur d'identité. Disons qu'un certain service (par exemple, le service de messagerie SMTP) est configuré sur exactement la même adresse IP sur le site de l'entreprise et sur le site distant. L'utilisateur pourrait sans le savoir utiliser le service sur le site distant, violant ainsi l'intégrité et la confidentialité du contenu relatif à cette application. Potentiellement, les messages électroniques de l'utilisateur distant pourraient être capturés par le serveur de messagerie du FAI.

Les entreprises déployant des serveurs VPN d'accès à distance devraient allouer des adresses IP globales pour les serveurs critiques auxquels les clients VPN distants ont généralement besoin d'accéder. En faisant cela, même si la plupart des réseaux privés d'entreprise utilisent l'espace d'adresses de la RFC 1918, cela va garantir que les clients VPN distants peuvent toujours accéder aux serveurs critiques quel que soit l'espace d'adresses privé utilisé au point de rattachement distant. Ceci est similaire à la recommandation 1 fournie en conjonction avec les déploiements de NAT multi-niveaux.

Recommandation-5 : lorsque un "VPN partagé" est configuré sur un client VPN d'un PC distant, il est conseillé aux

entreprises déployant des serveurs VPN d'accès à distance d'attribuer des adresses IP globales aux serveurs critiques auxquels les clients VPN distants sont susceptibles d'accéder.

5. Résumé des recommandations

Il est conseillé aux fabricants de NAT de se référer aux documents du protocole BEHAVE ([RFC4787], [RFC5382] et [RFC5508]) pour une liste complète des exigences de conformité pour les appareils de NAT.

Ce qui suit est un résumé des recommandations visant à soutenir les topologies de NAT non conventionnelles identifiées dans ce document. Les recommandations sont spécifiques du déploiement et s'adressent aux personnels responsables des déploiements. Ces personnels comprennent les administrateurs de FAI et les administrateurs informatiques d'entreprise.

Recommandation-1 : les FAI utilisent des appareils de NAT pour fournir une connexité aux clients qui doivent attribuer des adresses non chevauchantes aux serveurs annoncés aux clients. Une façon de procéder serait d'attribuer des adresses globales vers les serveurs annoncés.

Recommandation-2 : un client VPN doit être configuré sur un PC distant de telle sorte que les paquets IP dont l'adresse IP cible correspond à *l'un* des éléments (a) ou (b) ne soient pas autorisés à être redirigés via le VPN :
a) Adresse IP du routeur de bond suivant du client VPN, utilisé pour accéder au serveur VPN.
b) Adresse IP du serveur DHCP, fournissant un prêt d'adresse sur l'interface réseau de l'hôte distant.

Recommandation-3 : un client VPN sur un PC distant doit être configuré en mode "VPN non divisé" si l'objectif de déploiement est (a), ou en mode "VPN partagé" si l'objectif de déploiement est (b) :
a) Si l'objectif est de maximiser la sécurité et la fiabilité de connexité au réseau d'entreprise, le client VPN sur le PC distant doit être configuré en mode "VPN non divisé". Le mode "VPN partagé" garantit que le client VPN dirige tout le trafic de l'utilisateur distant au serveur VPN (sur le site de l'entreprise) à l'exception du trafic dirigé vers le routeur et le serveur DHCP sur le site distant.
b) Si il n'existe aucun problème de sécurité majeur empêchant l'accès direct aux hôtes sur le site distant ou sur l'Internet public, le client VPN sur le PC distant doit être configuré en mode "VPN partagé". Le mode "VPN partagé" garantit que seul le trafic de l'entreprise est dirigé vers le VPN. Tout autre trafic n'a pas les frais généraux de traversée du VPN.

Recommandation-4 : il est conseillé aux entreprises déployant des solutions de VPN d'accès à distance d'adopter une stratégie (a) ou (b) pour éviter un conflit d'adresse VIP avec le sous-réseau du site distant.
a) Si le serveur VPN en cours de déploiement a été configuré pour configurer deux réservoirs d'adresses ou plus, configurer le serveur VPN avec un minimum de deux réservoirs d'adresses IP distincts.
b) Déployer deux serveurs VPN ou plus avec des réservoirs d'adresses IP distincts. Ce faisant, un client VPN qui détecte des conflits d'adresses VIP avec le sous-réseau sur le site distant aura la possibilité de commuter vers un autre serveur VPN qui n'entrera pas en conflit.

Recommandation-5 : lorsque un "VPN partagé" est configuré sur un client VPN d'un PC distant, il est conseillé aux entreprises déployant des serveurs VPN d'accès à distance d'attribuer des adresses IP globales aux serveurs critiques auxquels les clients VPN distants sont susceptibles d'accéder.

6. Considérations relatives à la sécurité

Ce document ne crée pas intrinsèquement de nouveaux problèmes de sécurité. Les problèmes de sécurité connus des serveurs DHCP et des appareils de NAT sont applicables, mais pas dans le cadre de ce document. De même, les problèmes de sécurité spécifiques des appareils de VPN d'accès à distance sont également applicables à la topologie VPN d'accès à distance, mais pas dans le cadre de ce document. Les problèmes de sécurité examinés ici ne concernent que ceux qui concernent les topologies décrites dans les sections 2 et 3, en particulier telles qu'elles s'appliquent au chevauchement de l'espace d'adressage privé dans les topologies décrites.

L'identité erronée de l'hôte final est un problème de sécurité présent dans les deux topologies discutées. L'erreur d'identité d'hôte final, décrite aux paragraphes 2.2.4 et 3.2.4 pour chacune des topologies examinées, indique essentiellement la possibilité que les services d'application soient capturés par le mauvais serveur d'application (par exemple, un serveur de messagerie). Une violation de sécurité due à une erreur d'identité de l'hôte final se produit principalement en raison de

l'attribution à des serveurs critiques d'adresses privées de la RFC 1918. La recommandation suggérée pour les deux scénarios est d'attribuer des adresses IP publiques uniques à l'échelle mondiale aux serveurs critiques.

Il est également recommandé au paragraphe 2.1.2 que les applications adaptent l'authentification de bout en bout et ne dépend pas de l'adresse IP de source pour l'authentification. Cela empêchera la capture de connexion et les attaques de déni de service.

7. Remerciements

Les auteurs souhaitent remercier Dan Wing de sa relecture en détails du document et de ses suggestions utiles pour réorganiser le format du document. Les auteurs souhaitent également remercier Ralph Droms pour son aide à la reformulation du texte et de la recommandation 1 du paragraphe 3.2.4 et Cullen Jennings pour avoir aidé à reformuler le texte et la recommandation 3 au paragraphe 4.2.2.

8. Références

8.1 Références normatives

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996, DOI 10.17487/RFC1918.

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", août 1999. *(Information)*

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

[RFC4787] F. Audet, éd., C. Jennings, "Exigences sur le comportement des traducteurs d'adresse réseau (NAT) pour UDP en envoi individuel", janvier 2007, DOI 10.17487/RFC4787. (BCP0127) *(MàJ par* RFC7857)

[RFC5382] S. Guha et autres, "Exigences sur le comportement des NAT pour TCP", octobre 2008, DOI 10.17487/RFC5382. (BCP0142) *(MàJ par* RFC7857)

[RFC5508] P. Srisuresh, B. Ford, S. Sivakumar, S. Guha, "Exigences de comportement des NAT pour ICMP", avril 2009. (BCP0148) *(MàJ par* RFC7857)

8.2 Références pour information

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (MàJ par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC3027] M. Holdrege, P. Srisuresh, "Complications de protocole avec le traducteur d'adresse réseau IP", janvier 2001. *(Info.)*

[RFC5735] M. Cotton, L. Vegoda, "Adresses IPv4 d'utilisation particulière", janvier 2010. BCP0153. *(Remplace* RFC3330 ; *MàJ par* RFC6598 *; Remplacée par* RFC6890)

Adresse des auteurs

Pyda Srisuresh
Société EMC
1161, chemin San Antonio
Mountain View, Californie 94043
USA
téléphone : +1 408 836 4773
mél : srisuresh@yahoo.com

Bryan Ford
Département d'informatique
Université Yale
51, rue Prospect
New Haven, Connecticut 06511
téléphone : +1-203-432-1055
mél : bryan.ford@yale.edu