Attribution d'adresse pour les sites Internet privés

Contenu

Introduction

Ce document est basé sur RFC 1597 et il vous aidera à conserver l'espace d'adressage IP en ne allouant pas d'adresses IP uniques au monde aux hôtes privés de votre réseau. Vous pouvez toujours autoriser la connectivité complète de la couche réseau entre tous les hôtes du réseau et entre tous les hôtes publics sur Internet.

Les hôtes qui utilisent le protocole IP se divisent en trois catégories :

- Hôtes qui n'ont pas besoin d'accéder aux hôtes d'autres entreprises ou à Internet en général. Ces hôtes peuvent utiliser des adresses IP uniques au sein de leur réseau, mais qui ne sont peut-être pas uniques parmi les réseaux externes.
- Les hôtes qui ont besoin d'accéder à un ensemble limité de services externes (par exemple, e-mail, FTP, netnews, connexion à distance) qui peuvent être gérés par des passerelles de couche application. La plupart de ces hôtes peuvent ne pas avoir besoin d'un accès externe illimité (fourni via la connectivité IP) ou le vouloir, pour des raisons de confidentialité ou de sécurité. Comme les hôtes de la première catégorie, ils peuvent utiliser des adresses IP uniques au sein de leur réseau mais pas entre des réseaux externes.
- Hôtes qui ont besoin d'un accès à la couche réseau en dehors de l'entreprise via la connectivité IP. Seuls ces hôtes nécessitent des adresses IP globalement uniques.

De nombreuses applications nécessitent une connectivité au sein d'un seul réseau et n'ont même pas besoin d'une connectivité externe pour la plupart des hôtes internes. Dans les réseaux de grande taille, les hôtes utilisent souvent TCP/IP lorsqu'ils n'ont pas besoin de connectivité de couche réseau en dehors du réseau. Voici quelques exemples de connexions externes inutiles :

- Un grand aéroport qui a son arrivée et son départ affiche une adresse individuelle via TCP/IP.

Il est très peu probable que ces écrans doivent être directement accessibles à partir d'autres réseaux.
- Les grandes entreprises comme les banques et les chaînes de magasins qui utilisent TCP/IP pour leurs communications internes. Un grand nombre de postes de travail locaux, tels que les caisses enregistreuses, les distributeurs d'argent et les équipements des bureaux, ont rarement besoin d'une connectivité externe.
- Les réseaux qui utilisent des passerelles de couche application (pare-feu) pour se connecter à Internet. En règle générale, le réseau interne n'a pas d'accès direct à Internet, de sorte que seul un ou plusieurs hôtes de pare-feu sont visibles depuis Internet. Dans ce cas, le réseau interne peut utiliser des numéros IP non uniques.
- Deux réseaux qui communiquent via leur propre liaison privée. En général, seul un ensemble très limité d'hôtes est accessible entre eux via cette liaison. Seuls ces hôtes ont besoin de numéros IP uniques au monde.
- Interfaces des routeurs sur un réseau interne.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Espace d'adressage privé

L'IANA (Internet Assigned Numbers Authority) a réservé les trois blocs d'espace d'adresses IP suivants aux réseaux privés :

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Le premier bloc est un numéro de réseau de classe A unique, le second bloc est un ensemble de 16 numéros de réseau de classe B contigus et le troisième bloc est un ensemble de 255 numéros de réseau de classe C contigus.

Si vous décidez d'utiliser l'espace d'adressage privé, vous n'avez pas besoin de vous coordonner avec l'IANA ou un registre Internet. Les adresses de cet espace d'adressage privé ne seront uniques que dans votre réseau. N'oubliez pas que si vous avez besoin d'un espace d'adressage unique au niveau mondial, vous devez obtenir des adresses à partir d'un registre Internet.

Afin d'utiliser l'espace d'adressage privé, déterminez quels hôtes n'ont pas besoin d'avoir une

connectivité de couche réseau vers l'extérieur. Ces hôtes sont des hôtes privés et utilisent un espace d'adressage privé. Les hôtes privés peuvent communiquer avec tous les autres hôtes du réseau, publics et privés, mais ils ne peuvent pas avoir de connectivité IP à un hôte externe. Les hôtes privés peuvent toujours accéder aux services externes via des relais de couche application.

Tous les autres hôtes sont publics et utilisent un espace d'adressage unique au monde attribué par un registre Internet. Les hôtes publics peuvent communiquer avec d'autres hôtes du réseau et peuvent avoir une connectivité IP avec des hôtes publics externes. Les hôtes publics ne sont pas connectés aux hôtes privés d'autres réseaux.

Comme les adresses privées n'ont pas de signification globale, les informations de routage sur les réseaux privés ne sont pas propagées sur des liaisons externes et les paquets avec des adresses source ou de destination privées ne doivent pas être transférés sur de telles liaisons. Les routeurs des réseaux qui n'utilisent pas d'espace d'adressage privé, en particulier ceux des fournisseurs de services Internet, doivent être configurés pour rejeter (filtrer) les informations de routage sur les réseaux privés. Ce rejet ne doit pas être traité comme une erreur de protocole de routage.

Les références indirectes à ces adresses (telles que les enregistrements de ressources DNS) doivent être contenues dans le réseau. Les fournisseurs d'accès à Internet devraient prendre des mesures pour prévenir de telles fuites.

Avantages et inconvénients de l'utilisation de l'espace d'adressage privé

L'avantage évident de l'utilisation de l'espace d'adressage privé pour Internet en général est de conserver l'espace d'adressage unique au monde. L'utilisation de l'espace d'adressage privé vous offre également une plus grande flexibilité dans la conception du réseau, car vous disposerez de plus d'espace d'adressage que vous ne pourriez en obtenir à partir du pool unique mondial.

Le principal inconvénient de l'utilisation de l'espace d'adressage privé est que vous devez renuméroter vos adresses IP si vous voulez vous connecter à Internet.

Considérations de conception

Vous devez d'abord concevoir la partie privée de votre réseau et utiliser l'espace d'adressage privé pour toutes les liaisons internes. Planifiez ensuite les sous-réseaux publics et concevez la connectivité externe.

Si un schéma de découpage approprié peut être conçu et pris en charge par votre équipement, utilisez le bloc d'adresses privées de 24 bits et créez un plan d'adressage avec un bon chemin de croissance. Si le découpage en sous-réseaux pose problème, vous pouvez utiliser le bloc de classe C 16 bits.

Pour changer un hôte de privé en public, il faut modifier son adresse et, dans la plupart des cas, sa connectivité physique. Dans les endroits où de telles modifications peuvent être prévues (salles de machines, etc.), vous pouvez configurer des supports physiques distincts pour les sous-réseaux publics et privés, afin de faciliter ces modifications.

Les routeurs qui se connectent à des réseaux externes doivent être configurés avec des filtres de paquets et de routage appropriés aux deux extrémités de la liaison afin d'éviter les fuites. Vous

devez également filtrer les réseaux privés des informations de routage entrantes afin d'éviter les situations de routage ambiguës qui peuvent se produire si les routes vers le point d'espace d'adressage privé en dehors du réseau.

Les groupes d'organisations qui prévoient un besoin de communication mutuelle doivent concevoir un plan d'adressage commun. Si deux sites doivent être connectés à l'aide d'un fournisseur de services externe, ils peuvent envisager d'utiliser un tunnel IP pour empêcher les fuites de paquets du réseau privé.

Une façon d'éviter les fuites de RR DNS est d'exécuter deux serveurs de noms, un serveur externe responsable de toutes les adresses IP uniques au monde de l'entreprise et un serveur interne responsable de toutes les adresses IP, publiques et privées. Afin d'assurer la cohérence, ces deux serveurs doivent recevoir les mêmes données, dont le serveur de noms externe n'utilise qu'une version filtrée.

Les résolveurs sur tous les hôtes internes, publics et privés, n'interrogent que le serveur de noms interne. Le serveur externe résout les requêtes des résolveurs externes et est lié au DNS global. Le serveur interne transmet toutes les requêtes d'informations en dehors de l'entreprise au serveur de noms externe, afin que tous les hôtes internes puissent accéder au DNS global. De cette manière, les informations sur les hôtes privés ne parviennent pas aux résolveurs externes et aux serveurs de noms.

Considérations relatives à la sécurité

Bien que l'utilisation de l'espace d'adressage privé puisse améliorer la sécurité, elle ne remplace pas les mesures de sécurité dédiées.

Conclusion

Avec ce schéma, de nombreux grands réseaux n'ont besoin que d'un bloc d'adresses relativement petit provenant de l'espace d'adresses IP unique au monde. Internet bénéficie en grande partie de la conservation d'un espace d'adressage unique au niveau mondial et les réseaux bénéficient de la flexibilité accrue offerte par un espace d'adressage privé relativement grand.

Informations connexes

- Page d'assistance pour les protocoles de routage IP
- Page de support pour le routage IP
- Support et documentation techniques - Cisco Systems