Attribution d'adresse pour les sites Internet privés

Contenu

Introduction

Ce document est basé sur RFC 1597 , et il vous aidera à économiser l'espace d'adresse IP en n'allouant pas globalement - des adresses IP uniques aux hôtes privés dans votre réseau. Vous pouvez encore permettre la pleine Connectivité de couche réseau entre tous les hôtes dans le réseau et entre tous les hôtes publics en Internet.

Hôtes qui utilisent le ranger IP dans trois catégories :

- Hôtes qui n'exigent pas l'accès aux hôtes en d'autres entreprises ou Internet dans son ensemble. Ces hôtes peuvent utiliser les adresses IP qui sont seules dans leur réseau mais peuvent ne pas être seuls parmi les réseaux extérieurs.
- Hôtes qui ont besoin de l'accès à un ensemble limité de services extérieurs (par exemple, email, FTP, Netnews, remote login) qui peut être manipulé par des passerelles de couche application. Plusieurs de ces hôtes peuvent avoir besoin ou ne pas vouloir de l'accès externe sans restriction (fourni par l'intermédiaire de la connectivité IP), pour l'intimité ou les raisons de sécurité. Comme des hôtes dans la première catégorie, ils peuvent utiliser les adresses IP qui sont seules dans leur réseau mais pas parmi les réseaux extérieurs.
- Les hôtes qui ont besoin de l'accès de couche réseau en dehors de l'entreprise ont fourni par l'intermédiaire de la connectivité IP. Seulement ces hôtes exigent les adresses IP qui sont globalement - seules.

Beaucoup d'applications exigent la Connectivité seulement à moins d'un réseau et n'ont pas besoin même de la Connectivité externe pour les hôtes les plus internes. Dans les réseaux plus vastes, les hôtes utilisent souvent le TCP/IP quand ils n'ont pas besoin de la Connectivité de couche réseau en dehors du réseau. Voici quelques exemples où la Connectivité externe ne pourrait pas être exigée :

- Un grand aéroport qui a son arrivée et départ affiche individuellement adressable par l'intermédiaire du TCP/IP. Il est très peu probable que ces affichages doivent être directement accessibles d'autres réseaux.
- Grands organismes comme les banques et les chaînes de magasins de vente au détail qui utilisent le TCP/IP pour leur communication interne. Un grand nombre de postes de travail locaux comme des caisses enregistreuses, des ordinateurs d'argent, et le matériel aux positions de secrétaire ont besoin rarement de Connectivité extérieure.
- Réseaux qui utilisent des passerelles de couche application (Pare-feu) pour se connecter à l'Internet. Le réseau interne habituellement n'a pas l'accès direct à l'Internet, ainsi seulement un ou plusieurs hôtes de Pare-feu sont visible de l'Internet. Dans ce cas, le réseau interne peut utiliser de non-seuls numéros IP.
- Deux réseaux qui communiquent au-dessus de leur propre lien privé. Habituellement seulement très un ensemble limité d'hôtes est fini mutuellement accessible ce lien. Seulement ces hôtes ont besoin globalement - de seuls numéros IP.
- Interfaces des Routeurs sur un réseau interne.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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.

L'espace d'adressage privé

L'Internet Assigned Numbers Authority (IANA) a réservé les trois blocs suivants de l'espace d'adresse IP pour les 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 network number simple de la classe A, le deuxième bloc est un ensemble de 16 network number contigus de la classe B, et le troisième bloc est un ensemble de 255 network number contigus de C de classe.

Si vous décidez d'utiliser l'espace d'adressage privé, vous n'avez pas besoin de coordonner avec l'IANA ou un Internet Registry. Les adresses dans cet espace d'adressage privé seront seulement seules dans votre réseau. Souvenez-vous, si vous avez besoin globalement - espace adresse d'adresse unique, vous devez obtenir des adresses d'un Internet Registry.

Afin d'utiliser l'espace d'adressage privé, déterminez quels hôtes n'ont pas besoin d'avoir la Connectivité de couche réseau à l'extérieur. Ces hôtes sont les hôtes privés, et utilisent l'espace d'adressage privé. Les hôtes privés peuvent communiquer avec tous autres hôtes dans le réseau, public et privé, mais ils ne peuvent pas avoir la connectivité IP à aucun hôte externe. Les hôtes privés peuvent encore avoir accès aux services externes par l'intermédiaire des relais de couche application.

Tous autres hôtes sont espace adresse publique et d'utilisation globalement - d'adresse unique assignée par un Internet Registry. Les hôtes publics peuvent communiquer avec d'autres hôtes dans le réseau, et peuvent avoir la connectivité IP aux hôtes publics externes. Les hôtes publics n'ont pas la Connectivité aux hôtes privés d'autres réseaux.

Puisque les adresses privées n'ont aucune signification globale, les informations de routage au sujet des réseaux privés ne sont pas propagées sur les liens extérieurs, et des paquets avec la source privée ou les adresses de destination ne devraient pas être expédiés à travers de tels liens. Des Routeurs dans les réseaux qui n'utilisent pas l'espace d'adressage privé, particulièrement ceux des fournisseurs d'accès Internet, devraient être configurés pour rejeter (filtrez) les informations de routage au sujet des réseaux privés. Ce rejet ne devrait pas être traité comme erreur de protocole de routage.

Des références indirectes à de telles adresses (comme des enregistrements de ressource en DN) devraient être contenues dans le réseau. Les fournisseurs d'accès Internet devraient prendre des mesures d'empêcher une telle fuite.

Avantages et inconvénients d'utiliser l'espace d'adressage privé

L'avantage évident d'utiliser l'espace d'adressage privé pour l'Internet dans son ensemble est d'économiser globalement - l'espace adresse d'adresse unique. Utilisant l'espace d'adressage privé te donne également la meilleure flexibilité dans la conception de réseaux, puisque vous aurez plus d'espace d'adressage disponible que vous pourriez obtenir du globalement - seul groupe.

L'inconvénient primaire d'utiliser l'espace d'adressage privé est que vous devez renuméroter vos adresses IP si vous voulez se connecter à l'Internet.

Considérations de conception

Vous devriez concevoir la partie privée de votre réseau d'abord et utiliser l'espace d'adressage privé pour tous les liens internes. Alors prévoyez les sous-réseaux publics et concevez la Connectivité externe.

Si un schéma approprié de sous-réseautage peut être conçu et est pris en charge par votre matériel, utilisez le bloc 24-bit de l'espace d'adressage privé et faites un plan de adressage avec un bon chemin de croissance. Si le sous-réseautage est un problème, vous pouvez utiliser le bloc de 16 bits de C de classe.

Changer un hôte de privé au public exige changer son adresse et, dans la plupart des cas, sa Connectivité physique. Dans les emplacements où de telles modifications peuvent être prévues (des salles d'ordinateur, et ainsi de suite) vous pourriez vouloir configurer des medias physiques distincts pour des sous-réseaux publics et privés, pour faciliter ces modifications.

Des Routeurs qui se connectent aux réseaux externes devraient être installés avec les filtres appropriés de paquet et de routage aux deux fins du lien afin d'empêcher la fuite. Vous devriez également filtrer tous les réseaux privés des informations de routage d'arrivée afin d'empêcher les situations ambiguës de routage qui peuvent se produire si les artères à l'espace d'adressage privé se dirigent en dehors du réseau.

Les groupes d'organismes qui prévoient un besoin de transmission mutuelle doivent concevoir un plan de adressage commun. Si deux sites doivent être connectés utilisant un fournisseur de services externe, ils peuvent envisager d'employer un tunnel IP pour empêcher des fuites de paquet du réseau privé.

Une manière d'éviter la fuite des DN RRs est d'exécuter deux Serveurs de noms, un serveur externe responsable de tous globalement - des adresses IP uniques de l'entreprise et un serveur interne responsable de toutes les adresses IP, publiques et privées. Afin d'assurer à cohérence ces deux serveurs devrait recevoir les mêmes données, dont le Serveur de noms externe utilise seulement une version filtrée.

Les résolveurs sur tous les hôtes internes, publics et privés, questionnent seulement le Serveur de noms interne. Le serveur externe résout des requêtes des résolveurs extérieurs et est incorporé dans les DN globaux. Le serveur interne en avant toutes les requêtes pour les informations en dehors de l'entreprise au Serveur de noms externe, ainsi à tous hôtes internes peut accéder aux DN globaux. De cette façon, des informations sur les hôtes privés n'atteint pas les résolveurs et les Serveurs de noms extérieurs.

Considérations liées à la sécurité

Tandis que l'utilisation de l'espace d'adressage privé peut améliorer la Sécurité, il n'est pas une substitution pour des mesures de sécurité dédiées.

Conclusion

Avec ce schéma beaucoup de grands réseaux ont besoin seulement d'un bloc d'adresses relativement petit globalement - de l'espace adresse d'adresse IP unique. L'Internet à de grands avantages par l'économie de globalement - l'espace adresse d'adresse unique, et les réseaux tirent bénéfice du gain de souplesse fourni 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