Adres toewijzing voor Private Internet

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Private adresruimte](#)
[Voordelen en nadelen van het gebruik van privé-adresruimte](#)
[Ontwerpoverwegingen](#)
[Veiligheidsoverwegingen](#)
[Conclusie](#)
[Gerelateerde informatie](#)

Inleiding

Dit document is gebaseerd op RFC 1597 , en het zal u helpen IP-adresruimte te besparen door geen wereldwijd unieke IP-adressen toe te wijzen aan privé-hosts in uw netwerk. U kunt nog altijd de volledige verbinding van de netwerklaag tussen alle hosts in het netwerk en tussen alle openbare hosts in het internet toestaan.

Organisatoren die IP gebruiken vallen in drie categorieën:

- Hosten die geen toegang tot hosts in andere bedrijven of op het internet in het algemeen vereisen. Deze hosts kunnen gebruik maken van IP-adressen die uniek zijn binnen hun netwerk, maar mogelijk niet uniek zijn onder externe netwerken.
- Hosts die toegang nodig hebben tot een beperkte reeks externe services (bijvoorbeeld e-mail, FTP, netwerknews, Remote login) die kunnen worden verwerkt door toepassingslaaggateways. Veel van deze hosts hebben geen onbeperkte externe toegang nodig of willen (via IP-connectiviteit geboden), om redenen van privacy of veiligheid. Net als hosts in de eerste categorie kunnen zij IP-adressen gebruiken die uniek zijn binnen hun netwerk maar niet onder externe netwerken.
- Hosten die netwerklaagtoegang buiten de onderneming nodig hebben die via IP-connectiviteit beschikbaar is. Alleen deze gastheren vereisen IP adressen die mondiaal uniek zijn.

Vele toepassingen vereisen connectiviteit slechts binnen één netwerk en hebben zelfs geen externe connectiviteit voor de meeste interne gastheren nodig. In grotere netwerken gebruiken hosts vaak TCP/IP wanneer zij geen netwerklaagconnectiviteit buiten het netwerk nodig hebben. Hier zijn een paar voorbeelden waar externe connectiviteit niet zou kunnen worden vereist:

- Een grote luchthaven met aankomst en vertrek toont individueel adresseerbare luchthavens via TCP/IP. Het is zeer onwaarschijnlijk dat deze displays rechtstreeks toegankelijk moeten

zijn via andere netwerken.
- Grote organisaties zoals banken en detailhandelsketens die TCP/IP voor hun interne communicatie gebruiken. Grote aantallen lokale werkstations zoals kassa's, geldautomaten en apparatuur op een administratieve positie hebben zelden een externe connectiviteit nodig.
- netwerken die toepassingslaaggateways (firewalls) gebruiken om verbinding met internet te maken. Het interne netwerk heeft gewoonlijk geen directe toegang tot internet, zodat slechts één of meer firewallhosts zichtbaar zijn vanuit het internet. In dit geval kan het interne netwerk niet-unieke IP-nummers gebruiken.
- Twee netwerken die over hun eigen privé verbinding communiceren. Gewoonlijk is slechts een zeer beperkte reeks hosts wederzijds bereikbaar via deze link. Alleen die hosts hebben wereldwijd unieke IP-nummers nodig.
- Interfaces van routers op een intern netwerk.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Private adresruimte

De Internet Assigned Numbers Authority (IANA) heeft de volgende drie blokken IP-adresruimte voor privénetwerken gereserveerd:

- 10.0.0.0 - 10.25.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Het eerste blok is één klasse A netwerknummer, het tweede blok is een set van 16 aaneengesloten klasse B netwerknummers en het derde blok is een set van 255 aaneengesloten klasse C netwerknummers.

Als u hebt besloten om privé adresruimte te gebruiken, hoeft u niet te coördineren met IANA of een Internet-registratie. Adressen binnen deze privé-adresruimte zijn alleen uniek binnen uw netwerk. Onthoud, als je wereldwijd unieke adresruimte nodig hebt moet je adressen van een internetregister verkrijgen.

Om privé adresruimte te gebruiken, bepalen welke hosts geen netwerklaagconnectiviteit aan de buitenkant nodig hebben. Deze gastheren zijn privé en gebruiken privé adresruimte. Particuliere hosts kunnen met alle andere hosts binnen het netwerk communiceren, zowel openbaar als particulier, maar zij kunnen geen IP-connectiviteit op een externe host hebben. Particuliere hosts

kunnen nog steeds toegang hebben tot externe diensten via relayplaten van de toepassingslaag.

Alle andere hosts zijn openbaar en gebruiken wereldwijd unieke adresruimte die door een internetregister is toegewezen. Openbare hosts kunnen met andere hosts binnen het netwerk communiceren en kunnen IP-connectiviteit hebben op externe publieke hosts. Publieke gastheren hebben geen connectiviteit op privé gastheren van andere netwerken.

Omdat privé adressen geen mondiale betekenis hebben, wordt het routeren van informatie over privé netwerken niet verspreid over buitenbanden, en pakketten met privé bron of bestemmingsadressen niet over dergelijke verbindingen doorgestuurd. Routers in netwerken die geen privé-adresruimte gebruiken, vooral die van Internet-serviceproviders, moeten worden geconfigureerd om het routing van informatie over particuliere netwerken te weigeren (filter uit). Deze afwijzing moet niet worden behandeld als een fout in het routeringsprotocol.

Indirecte verwijzingen naar dergelijke adressen (zoals DNS Resource Records) moeten in het netwerk zijn opgenomen. Internetproviders moeten maatregelen nemen om dergelijke lekken te voorkomen.

Voordelen en nadelen van het gebruik van privé-adresruimte

Het voor de hand liggende voordeel van het gebruik van privé adresruimte voor het internet in zijn geheel is het behouden van de globaal unieke adresruimte. Het gebruiken van privé adrestoewijzing geeft u ook een grotere flexibiliteit in netwerkontwerp, aangezien u meer adresruimte beschikbaar zult hebben dan u zou kunnen krijgen van de wereldwijd unieke pool.

Het primaire nadeel van het gebruiken van privé adresruimte is dat u uw IP adressen moet hernummeren als u met internet wilt verbinden.

Ontwerpoverwegingen

U dient het privégedeelte van het netwerk eerst te ontwerpen en privé-adresruimte te gebruiken voor alle interne koppelingen. Stel dan openbare subnetten in en ontwerp de externe connectiviteit.

Als een geschikt subnetting scheme kan worden ontworpen en door uw apparatuur wordt ondersteund, gebruik het 24-bits blok van privé adresruimte en maak een adresseringsplan met een goed groeitraject. Als subnetting een probleem is, kunt u het 16-bits klasse C blok gebruiken.

Het veranderen van een gastheer van privé in publiek vereist het veranderen van zijn adres en, in de meeste gevallen, zijn fysieke verbinding. Op plaatsen waar dergelijke veranderingen kunnen worden voorzien (machineruimten, enz.) zou u afzonderlijke fysieke media voor openbare en privé subnetten kunnen willen vormen, om deze veranderingen te vergemakkelijken.

Routers die verbinding maken met externe netwerken, moeten worden ingesteld met juiste pakketten en routingfilters aan beide uiteinden van de link om lekkage te voorkomen. U dient ook particuliere netwerken te filteren van inkomende routinginformatie om dubbele routingsituaties te voorkomen die kunnen voorkomen als routes naar het privé adres ruimtepunt buiten het netwerk.

Organisatiegroepen die voorzien in een behoefte aan onderlinge communicatie moeten een gemeenschappelijk adresseringsplan opstellen. Als twee locaties moeten worden aangesloten via een externe serviceprovider, kunnen ze overwegen om een IP-tunnel te gebruiken om

pakketlekkages uit het privénetwerk te voorkomen.

Eén manier om lekkage van DNS-R's te voorkomen, is door twee naamservers te draaien, één externe server verantwoordelijk voor alle wereldwijd unieke IP-adressen van de onderneming en één interne server verantwoordelijk voor alle IP-adressen, zowel openbare als particuliere. Om consistentie te verzekeren zouden beide servers dezelfde gegevens moeten ontvangen, waarvan de externe naamserver alleen een gefilterde versie gebruikt.

In alle interne hosts, zowel openbaar als privé, wordt alleen de interne naamserver gevraagd. De externe server lost vragen van externe oplossers op en is verbonden met de globale DNS. De interne server zendt alle vragen voor informatie buiten de onderneming naar de externe naamserver door, zodat alle interne hosts toegang hebben tot de mondiale DNS. Op deze manier bereikt informatie over private hosts geen externe oplossers en naamservers.

Veiligheidsoverwegingen

Hoewel het gebruik van privé-adresruimte de veiligheid kan verbeteren, is het geen vervanging voor specifieke beveiligingsmaatregelen.

Conclusie

Met deze regeling hebben veel grote netwerken slechts een relatief klein blok adressen van de globaal unieke IP adresruimte nodig. Het internet profiteert in grote mate door het behoud van mondiaal unieke adresruimte, en de netwerken profiteren van de toegenomen flexibiliteit die wordt geboden door een relatief grote privé-adresruimte.

Gerelateerde informatie

- Ondersteuningspagina voor IP-routeringsprotocollen
- Ondersteuningspagina voor IP-routing
- Technische ondersteuning en documentatie – Cisco Systems