تخصيص العنوان لشبكات الإنترنت الخاصة

المحتويات

المقدمة

يستند هذا المستند إلى RFC 1597 ، وسيساعدك في الحفاظ على مساحة عنوان IP من خلال عدم تخصيص عناوين IP الفريدة عالميا للمضيفين الخاصين في شبكتك. لا يزال بإمكانك السماح باتصال طبقة الشبكة الكاملة بين جميع الأجهزة المضيفة في الشبكة وبين جميع الأجهزة المضيفة العامة في الإنترنت.

البيئات المضيفة التي تستخدم IP تقع في ثلاث فئات:

- الأجهزة المضيفة التي لا تتطلب الوصول إلى الأجهزة المضيفة في المؤسسات الأخرى أو الإنترنت بشكل عام. يمكن أن تستخدم هذه الأجهزة المضيفة عناوين IP الفريدة داخل شبكتهم ولكنها قد لا تكون فريدة بين الشبكات الخارجية.
- الأجهزة المضيفة التي تحتاج إلى الوصول إلى مجموعة محدودة من الخدمات الخارجية (على سبيل المثال، البريد الإلكتروني و FTP و NetNews و تسجيل الدخول عن بعد) التي يمكن معالجتها بواسطة بوابات طبقة التطبيقات. قد لا يحتاج العديد من هذه الأجهزة المضيفة إلى وصول خارجي غير مقيد أو لا يريد الوصول إليه (يتم توفيره عبر اتصال IP)، وذلك لأسباب تتعلق بالخصوصية أو الأمان. مثل الأجهزة المضيفة في الفئة الأولى، يمكنها إستخدام عناوين IP الفريدة داخل شبكتهم ولكن ليس بين الشبكات الخارجية.
- الأجهزة المضيفة التي تحتاج إلى الوصول إلى طبقة الشبكة خارج المؤسسة والتي يتم توفيرها عبر اتصال IP. تتطلب هذه الأجهزة المضيفة فقط عناوين IP الفريدة عالميا.

تتطلب العديد من التطبيقات إمكانية الاتصال فقط داخل شبكة واحدة ولا تحتاج حتى إلى اتصال خارجي لمعظم البيئات المضيفة الداخلية. في الشبكات الأكبر، غالبا ما تستخدم الأجهزة المضيفة بروتوكول TCP/IP عندما لا تحتاج إلى اتصال طبقة الشبكة خارج الشبكة. فيما يلي بعض الأمثلة التي قد لا يكون فيها الاتصال الخارجي مطلوبا:

- مطار كبير يعرض عند وصوله ومغادرته بصفة فردية عبر بروتوكول TCP/IP. من غير المرجح جدا أن تكون هذه العروض قابلة للوصول إليها مباشرة من شبكات أخرى.
- المؤسسات الكبيرة مثل البنوك وسلاسل البيع بالتجزئة التي تستخدم بروتوكول TCP/IP في إتصالاتها الداخلية. ذلك أن أعداد كبيرة من محطات العمل المحلية مثل سجلات النقد، والآلات النقدية، والمعدات في مواقع العمل الكتابية نادرا ما تحتاج إلى اتصال خارجي.

- الشبكات التي تستخدم بوابات طبقة التطبيقات (جدران الحماية) للاتصال بالإنترنت. لا تتمتع الشبكة الداخلية عادة بإمكانية الوصول المباشر إلى الإنترنت، لذلك لا يمكن رؤية سوى مضيف واحد أو أكثر من مضيفي جدار الحماية من الإنترنت. في هذه الحالة، يمكن للشبكة الداخلية إستخدام أرقام IP غير الفريدة.
- شبكتين تتواصلان عبر رابطهما الخاص. عادة، لا يمكن الوصول إلى سوى مجموعة محدودة جدا من البيئات المضيفة بشكل متبادل عبر هذا الارتباط. وتحتاج هذه الأجهزة المضيفة فقط إلى أرقام IP فريدة عالميا.
- واجهات الموجهات على شبكة داخلية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، راجع اصطلاحات تلميحات Cisco التقنية.

مساحة العنوان الخاصة

قامت هيئة الأرقام المعينة عبر الإنترنت (ANA) بحفظ الوحدات الثلاث التالية من مساحة عنوان IP للشبكات الخاصة:

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

الكتلة الأولى هي رقم شبكة من الفئة A واحدة، بينما الكتلة الثانية هي مجموعة من 16 رقم شبكة متجاور من الفئة B، والكتل الثالث هو مجموعة من 255 رقم شبكة متجاور من الفئة C.

إذا قررت إستخدام مساحة عنوان خاصة، فلا تحتاج إلى التنسيق مع ANA أو سجل إنترنت. ستكون العناوين الموجودة ضمن مساحة العنوان الخاصة هذه فريدة فقط داخل شبكتك. تذكر، إذا كنت تحتاج إلى مساحة عنوان فريدة بشكل عام، فيجب الحصول على عناوين من سجل إنترنت.

لاستخدام مساحة العنوان الخاصة، حدد البيئات المضيفة التي لا تحتاج إلى اتصال طبقة الشبكة بالخارج. هذه الأجهزة المضيفة هي أجهزة مضيفة خاصة، وتستخدم مساحة عنوان خاصة. يمكن للمضيفين الخاصين الاتصال بجميع الأجهزة المضيفة الأخرى داخل الشبكة، العامة والخاصة على حد سواء، ولكن لا يمكن أن يكون لديهم اتصال IP بأي مضيف خارجي. لا يزال بإمكان المضيفين الخاصين الوصول إلى الخدمات الخارجية عبر مرحلات طبقة التطبيقات.

كل البيئات المضيفة الأخرى عامة وتستخدم مساحة عنوان فريدة بشكل عام تم تعيينها بواسطة سجل إنترنت. يمكن للمضيفين العامين الاتصال بمضيفين آخرين داخل الشبكة، ويمكن أن يكون لهم اتصال IP بالمضيفين العامين الخارجيين. لا تتوفر للمضيفين العامين إمكانية اتصال بالمضيفين الخاصين للشبكات الأخرى.

نظرا لأن العناوين الخاصة ليس لها معنى عمومي، لا يتم نشر معلومات التوجيه حول الشبكات الخاصة على الارتباطات الخارجية، ولا يجب إعادة توجيه الحزم ذات عناوين المصدر الخاص أو الوجهة عبر هذه الارتباطات. يجب تكوين الموجهات في الشبكات التي لا تستخدم مساحة العنوان الخاصة، وخاصة تلك الخاصة بمزودي خدمة الإنترنت، لرفض (تصفية) معلومات التوجيه حول الشبكات الخاصة. لا يجب التعامل مع هذا الرفض كخطأ في بروتوكول التوجيه.

يجب تضمين المراجع غير المباشرة إلى هذه العناوين (مثل سجلات موارد DNS) داخل الشبكة. وينبغي لمقدمي خدمات الإنترنت أن يتخذوا تدابير لمنع هذا التسرب.

مزايا وعيوب إستخدام مساحة العنوان الخاصة

الميزة الواضحة لاستخدام مساحة العنوان الخاصة للإنترنت بشكل عام هي توفير مساحة العنوان الفريدة عالميا. يمنحك إستخدام مساحة العنوان الخاصة أيضا مرونة أكبر في تصميم الشبكة، حيث سيكون لديك مساحة عنوان متوفرة أكثر مما يمكنك الحصول عليه من المجموعة الفريدة عالميا.

العيب الأساسي لاستخدام مساحة العنوان الخاصة هو أنه يجب إعادة ترقيم عناوين IP الخاصة بك إذا كنت تريد الاتصال بالإنترنت.

اعتبارات التصميم

يجب تصميم الجزء الخاص من شبكتك أولا واستخدام مساحة العنوان الخاصة لجميع الارتباطات الداخلية. ثم قم بتخطيط الشبكات الفرعية العامة وتصميم الاتصال الخارجي.

إذا كان من الممكن تصميم مخطط تقسيم شبكة إلى شبكات فرعية مناسب ومدعوم بواسطة أجهزتك، فاستخدم الكتلة ذات 24 بت من مساحة العنوان الخاصة واعمل خطة توجيه مع مسار نمو جيد. إذا كانت تقسيم الشبكة إلى شبكات فرعية مشكلة، فيمكنك إستخدام كتلة 16-بت من الفئة C.

يتطلب تغيير المضيف من خاص إلى عام تغيير عنوانه، وفي معظم الحالات، إتصاله المادي. في المواقع التي يمكن فيها توقع مثل هذه التغييرات (غرف الأجهزة، وما إلى ذلك) قد ترغب في تكوين وسائط مادية منفصلة للشبكات الفرعية العامة والخاصة، لتسهيل هذه التغييرات.

يجب إعداد الموجهات التي تتصل بالشبكات الخارجية باستخدام عوامل تصفية الحزم والتوجيه المناسبة في كلا طرفي الارتباط لمنع التسرب. يجب أيضا تصفية أي شبكات خاصة من معلومات التوجيه الواردة لمنع حالات التوجيه الغامضة التي يمكن أن تحدث إذا تم التوجيه إلى نقطة مساحة العنوان الخاصة خارج الشبكة.

ويتعين على مجموعات المنظمات التي تتوقع الحاجة إلى التواصل المتبادل أن تعمل على تصميم خطة مشتركة لمعالجة هذه القضية. إذا كان يلزم توصيل موقعين باستخدام مزود خدمة خارجي، فيمكنهما التفكير في إستخدام نفق IP لمنع تسريبات الحزم من الشبكة الخاصة.

تتمثل إحدى الطرق لتجنب تسريب DNS RRs في تشغيل خادمين بالاسم، وأحد الخوادم الخارجية مسؤول عن جميع عناوين IP الفريدة عالميا للمؤسسة، وخادم داخلي واحد مسؤول عن جميع عناوين IP، العامة والخاصة على حد سواء. لضمان التناسق، يجب أن تتلقى هذه الخوادم نفس البيانات، التي يستخدم خادم الأسماء الخارجية منها إصدارا تمت تصفيته فقط.

تقوم المحددات الموجودة على كافة الأجهزة المضيفة الداخلية، العامة والخاصة على حد سواء، باستعلام خادم الاسم الداخلي فقط. يقوم الخادم الخارجي بحل الاستعلامات من المحددات الخارجية ويرتبط ب DNS العمومي. يقوم الخادم الداخلي بإعادة توجيه كافة الاستعلامات عن المعلومات خارج المؤسسة إلى خادم الاسم الخارجي، بحيث يمكن لكافة المضيفين الداخليين الوصول إلى DNS العمومي. بهذه الطريقة، لا تصل المعلومات الخاصة بالمضيفين الخاصين إلى المحددات الخارجية وتسمية الخوادم.

اعتبارات أمنية

في حين أن إستخدام مساحة العنوان الخاصة يمكن أن يحسن الأمن، إلا أنه ليس بديلا لتدابير أمنية مخصصة.

القرار

مع هذا النظام، تحتاج العديد من الشبكات الكبيرة فقط إلى كتلة صغيرة نسبيا من العناوين من مساحة عنوان IP الفريدة عالميا. وتستفيد شبكة الإنترنت ككل من خلال الحفاظ على حيز عناوين فريد على الصعيد العالمي، وتستفيد الشبكات من زيادة المرونة التي توفرها مساحة عناوين خاصة كبيرة نسبيا.

معلومات ذات صلة

- صفحة دعم بروتوكولات IP المُوجّهة
- صفحة دعم توجيه IP
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).