تحويل العناوين الرقمية NETWORK ADDRESS TRANSLATION

نظري L8

فاق نمو شبكة الانترنت كل التوقعات، أي أن حجم الشبكة يتزايد ، وكل جهاز يرتبط على شبكة الانترنت يحتاج إلى عنوان رقمي يميزه عن باقي الأجهزة، وهذا ما يعرف (IP Address)، وهذا العنوان الرقمي مكون من 32 خانة ثنائية، أي ما يكفي لإيجاد (4.294.967.296) عنواناً مميزاً. لكن العدد الحقيقي المتاح أصغر من هذا بسبب الطريقة التي تستخدم فيها العناوين الرقمية.

ولمواجهة هذه المشكلة فكر المختصون في إيجاد حلول، كان منها أسلوب تحويل العناوين الرقمية أو (Network Address Translation) (NAT).

1. الفكرة الأساس لتقنية (NAT):

هناك منظمة تتولى إعطاء العناوين الرقمية لمن يطلبها، ولا يكون العنوان معترف به _ وبالتالي صالحاً للاستخدام_ مالم يصدر من تلك المنظمة التي تحرص على أن يكون العنوان الرقمي فريداً، أي أنه يدل على جهاز أو شبكة.
بسبب قلة العدد المتاح من العناوين الرقمية فإنه غالباً ما تعطى شبكة ما_ ولنسمها الشبكة الداخلية_ رقماً واحداً، أو عدداً من الأرقام ليكون معرّفاً لها عند بقية شبكة الانترنت.
ثم تعطى الأجهزة المكونة للشبكة الداخلية عناوين رقمية لغرض الاستخدام الداخلي فقط بحيث لا يتكرر رقم واحد داخل الشبكة المعينة.
غير أن هذه الأرقام تتكرر خارج الشبكة المعينة، أي أن عنواناً رقمياً داخلياً ما قد يستخدم في أكثر من شبكة.
ويأتي دور تقنية NAT عندما يرغب جهاز ما في الشبكة الداخلية الاتصال بجهاز خارج الشبكة الداخلية.
ولأن العنوان الرقمي للجهاز الداخلي غير معترف به خارجياً فإننا ننصب جهازاً وسيطاً بين الشبكة الداخلية وشبكة الانترنت، مهمته تحويل العنوان الرقمي الداخلي إلى رقم خارجي معترف به، ثم يرسل الرزم الالكترونية (packets) إلى الجهاز المقصود حامله الرقم الخارجي على أنه العنوان الرقمي للجهاز المرسل الواقع داخل الشبكة المحلية.
وعند عودة هذه الرزم يبادر الجهاز الوسيط بالنظر إلى عنوان المرسل إليه الموجود فيها ويحولها نحو الجهاز الداخلي المقصود.
غالباً ما يكون الجهاز الوسيط الذي يطبق تقنية NAT إما جداراً نارياً (Firewall) أو موجهّاً (router).

الشكل (1) عمل تقنية NAT

2. كيف تعمل تقنية NAT؟

هناك عدة طرق تعمل بها تقنية NAT، منها:

1) النمط الثابت للتحويل (Static NAT): يخصص الجهاز الوسيط لكل عنوان رقمي داخلي عنواناً رقمياً خارجياً ثابتاً لا يتغير.
2) النمط المتغير للتحويل (Dynamic NAT): في هذا النوع يكون لدى الجهاز الوسيط عدد محدد من العناوين الرقمية الخارجية، وكلما طلب جهاز داخلي الاتصال بشبكة الانترنت أعطاه جهاز التحويل أياً من العناوين الرقمية الخارجية، ويقوم الجهاز الداخلي باستخدام العنوان الرقمي الخارجي عنواناً مؤقتاً له للتواصل مع باقي شبكات الانترنت، أي أنه يضع هذا العنوان المؤقت على الرزم التي يرسلها باعتبار أنه عنوان المرسل.
عند رغبة جهاز موجود في الشبكة في الرد فإنه يستخدم هذا العنوان المؤقت باعتباره عنوان المرسل إليه. وبعد انتهاء المحادثة وقطع الجهاز اتصاله بالانترنت، يعود العنوان المؤقت إلى الجهاز الوسيط الذي قد يمنح هذا العنوان لجهاز آخر فيما بعد، وهكذا فإن العنوان الرقمي الخارجي المعطى لجهاز داخلي ما يختلف من مرة إلى أخرى.

وأيّاً كانت طريقة عمل تقنية NAT فإن الذي يحدث غالباً أن يقوم إداري شبكة الحاسوب في المنشأة بوضع جهاز يقوم بعملية التحويل NAT.
كما ذكرنا سابقاً، أن الجهاز يمكن أن يكون جداراً نارياً أو موجهّاً.
ولنفترض أنه موجه، ولربط الشبكة الداخلية بشبكة الانترنت تطلب المنشأة من المنظمة إعطائها عنواناً رقمياً مميزاً (IP Address) ، ويكون هذا العنوان هو عنوان الموجه، وقد تطلب عدة عناوين رقمية، وفي حال رغبة مستخدم ما داخل الشبكة الداخلية تصفح موقع في شبكة الانترنت فإن جهاز المستخدم يرسل طلباً إلى الموجه موضحاً فيه العنوان الرقمي للموقع، كما أن الطلب فيه العنوان الرقمي لجهاز المستخدم. وبسبب أن الموقع ليس ضمن الشبكة الداخلية، فإن الموجه يرسل الطلب إلى الموقع، ولكنه قبل ذلك يجري عملية مهمة هي موضوع تقنية NAT . ولو أن الموجه حاول إرسال الطلب فإن الموقع

الالكتروني لن يستطبع إرسال الرد، لأن العنوان الرقمي الموجود في الطلب ليس مسجلاً للجهاز الطالب.
وتفادياً لهذه المشكلة يقوم الموجه بتغيير الخانة الخاصة بالعناوين الرقمية للجهاز الطالب في الطلب، بحيث يصبح محتواها أحد العناوين الرقمية المخصصة من قبل المنظمة للموجه نفسه، وبعدها يمكن إرسال الطلب، وعندما يأتي الرد فإنها توجه إلى العنوان الرقمي للموجه. ونظراً لأن هذا العنوان مسجل لدى المنظمة، فإن الرد يرسل إلى الموجه، وهنا يقوم الموجه بمراجعة جدول المتابعة، ويحدد منه العنوان الرقمي للجهاز الداخلي الذي أرسل ذلك الطلب، وعندها يغير الموجه خانة العنوان الرقمي في الرد بحيث تحوي العنوان الرقمي للجهاز الطالب ، ثم يرسل إليه، وتكرر العملية كلما حاول مستخدم ما الاتصال بجهاز أو موقع خارج الشبكة الداخلية.

3) كيف يتحقق الأمن باستخدام NAT؟

إن الجهاز الذي يقوم بتطبيق هذه التقنية يقف حائلاً بين الشبكة الداخلية وشبكة الانترنت، فلا يستطيع من كان مرتبطاً بشبكة الانترنت معرفة العناوين الرقمية للأجهزة المرتبطة بالشبكة الداخلية، وهذا يسهم في حمايتها من عدد كبير من أنواع الهجوم التي تشنّ باستخدام شبكة الانترنت بناء على معرفة العناوين الرقمية.

الخلاصة:

مع أن فكرة تحويل العناوين الرقمية كان الباعث لها قلة العدد المتاح من تلك العناوين، فإنها وسيلة لحماية شبكات المعلومات وعزلها من الأخطار التي تعج بها شبكة الانترنت، والفكرة تقوم على إعطاء عناوين رقمية للأجهزة الواقعة على الشبكة الداخلية بحيث لا يمكن استخدامها من الخارج للوصول إلى تلك الأجهزة لوجود كيان عازل يقوم بتحويل العناوين الداخلية إلى أخرى خارجية عند رغبة المستخدمين داخل الشبكة المحمية الوصول إلى شبكة الانترنت.

ولو اعترض مهاجم ما البيانات القادمة من الأجهزة الموجودة على الشبكة الداخلية فإنه لا يرى سوى العناوين الرقمية الخارجية، ولكن تلك العناوبن توصله فقط على ذلك الكيان العازل ، وبالتالي تبقى الأجهزة الداخلية بعيداً عن متناول المهاجمين.