التشفير بالمفتاح العام

(Public key cryptography)

مقدمة

هو أسلوب من أساليب التشفير يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير، وبالتالي فإنه يسمح بتوزيع صلاحيات التشفير وفك التشفير على الجهات المختلفة بأن يعطي لبعضهم مفاتيح التشفير فقط ويعطي للآخرين مفاتيح فك التشفير.

ويسمى هذا النوع من التشفير أيضا بالتشفير غير المتناظر (Asymmetric Encryption)، لأنك تستطيع أن تنشر أحد المفتاحين وهو يسمى المفتاح العام (public-key)، وتحتفظ بالآخر سريًا، ويسمى المفتاح الخاص (private-key).

وعندما تقوم بنشر المفتاح العام، فإن أي أحد يستطيع استخدامه لتشفير البيانات التي يريد أن يرسلها لك بشكل سري، لكن لن يتمكن أحد من فك تشفير هذه البيانات باستخدام هذا المفتاح العام، أما فك التشفير فيكون باستخدام المفتاح الخاص الذي يكون ملكك أنت فقط، وبالتالي أنت ستكون الشخص الوحيد الذي يمكنه قراءة الرسائل التي شفرت لك باستخدام مفتاحك العام.

نتذكر القاعدة التالية: إذا تم التشفير باستخدام المفتاح العام فسيتم فك التشفير باستخدام المفتاح الخاص وهذه الطريقة مفيدة لتحقيق السرية، و إذا تم التشفير باستخدام المفتاح الخاص فسيتم فك الشفير باستخدام المفتاح العام وهذه الطريقة مفيدة للتحقق من الهوية.

متطلبات التشفير بالمفتاح العام

- كل طرف (بوب مثلاً) يحسب مفتاحين عام PUB وخاص PRB.
- من غير المجدي حسابياً لمهاجم أن يحدد المفتاح الخاص لطرف من خلال معرفته بالمفتاح العام لهذا الطرف.
- من غير المجدي حسابياً معرفة الرسالة الأصلية plaintext من خلال معرفة المفتاح العام والرسالة المشفرة.

استخدامات المفتاح العام

- التشفير وفك التشفير (يؤمن السرية).
- التوقيع الرقمي (يؤمن التوثق).
- تبادل المفاتيح (لإنشاء مفاتيح جلسة).

هناك خوارزميات تنفع لكل الاستخدامات، وخوارزميات مخصصة لاستخدامات معينة فحسب.

خوارزمية RSA

هي خوارزمية للتشفير بواسطة مفتاح عام. ولعلها الأولى المعروفةً على هذا الصعيد، وهي مناسبة للتّوقيع بالإضافة إلى التشفير، وكانت أحد التقدّمات العظيمة الأولى في التشفير بواسطة مفتاح عامّ. آر إس إيه مستخدم في بروتوكولات التّجارة الإلكترونيّة على نطاق واسع، وهي آمنة طالما كان طول المفتاح طويلا جدا مثل: 1024 بت، وهي تعتمد بشكل كبير على أنَّه لا يوجد خوارزمية لتحليل عدد لعوامل بسرعة عالية.

وبشكل أكثر تفصيلاً: جاءت قوت الخوارزمية من الرياضيات المتقطعة حيث تعتبر عملية الرفع إلى الأس Exponent هي عملية سهلة حسابياً بينما عملية العودة باستخدام اللوغاريتمات Logarithm تعتبر صعبة حسابياً، وإن عملية ضرب عددين أولين Multiplication تعتبر سهلة حسابياً بينما عملية العودة باستخدام التحليل إلى عوامل أولية Factorization تعتبر صعبة حسابياً.

مبدأ عمل الخوارزمية

1. نختار عددين أوليين Primes كبيرين: p, q
2. نحسب $n = p * q$ ويسمى n بالأساس Modulus
3. نحسب المعامل: $\varphi(n) = (p-1) * (q-1)$
4. نختار مفتاح عام PU نرمز له e بحيث يحقق الشرطين:

$$1 < e < \varphi(n) \ \&\& \ GCD\left(e, \ \varphi(n)\right) = 1$$

حيث $GCD\left(e, \ \varphi(n)\right)$ هو القاسم المشترك الأكبر Great Common Divider للعددين $\varphi(n)$ و e

ويكون المفتاح العام هو زوج من الأرقام $\mathrm{PU} = \{n, e\}$

5. نحسب المفتاح الخاص PR ونرمز له d كالتالي: $e * d \bmod \varphi(n) = 1$

ونقوم بحساب المعادلة السابقة لاستنتاج d بطريقة اسمها اقليدس الموسعة وسنوضحها بالمثال القادم.

ويكون المفتاح الخاص هو زوج من الأرقام $\mathrm{PR} = \{n, d\}$

للتشفير:

بفرض نريد تشفير الرسالة M يقوم المرسل بالتالي: $C = M^e \bmod n$

لفك التشفير:

بفرض نريد فك تشفير الرسالة المشفرة C يقوم المرسل بالتالي: $M = C^d \bmod n$

ملاحظة: دخل الخوارزمية M هو أرقام وبالتالي: إذا أردنا تشفير حروف فيجب أولاً تحويل الحروف إلى أرقام بأي طريقة، كطريقة الترميز ASCII أو base 10 أو base64... إلخ.

مثال: ليكن لديك العددين $\mathrm{p} = 3, \mathrm{q} = 11$ والمطلوب: أوجد المفتاح الخاص ثم قم بتشفير النص M=5، ثم قم بفك تشفيره

الحل:

1. $p = 3, q = 11$
2. نحسب: $n = 11 * 3 = 33$
3. ومنه نحسب: $\varphi(n) = 10 * 2 = 20$
4. نختار e بحيث يحقق الشرطين:

$$1 < e < 20 \;\&\&\; GCD(e, 20) = 1$$

وليكن $e = 3$

وبالتالي يكون المفتاح العام PU هو:

$$\mathrm{PU} = \{n, e\} = \{33,3\}$$

5. نحسب المفتاح الخاص:

$$e * d \; mod \; \varphi(n) = 1 \Rightarrow 3 * d \; mod \; 20 = 1$$

من طريقة اقليدس الموسعة يمكن كتابة المعادلة السابقة بالشكل التالي:

$$20\,x + 3\,y = 1$$

$$20 = 6(3) + 2$$

$$3 = 1(2) + 1$$

نتوقف عندما يصبح الباقي =1

ثم نبدأ بالتعويض:

$$1 = 3 - 1(2)$$

$$1 = 3 - 1(20 - 6(3))$$

$$1 = 3 - 20 + 6(3)$$

$$1 = \mathbf{7}(3) - 20$$

نجد أن $d = 7$ يحقق الشرط.

وبالتالي يكون المفتاح الخاص PR هو

$$\mathrm{PR} = \{n, d\} = \{33,7\}$$

إذا كانت $M = 5$ تكون:

$$C = M^e \bmod n = 5^3 \bmod 33 = 26$$

ويفك المستقبل تشفير C للحصول على M:

$$M = C^d \bmod n = 26^7 \bmod 33 = 5$$

وظيفة: أوجد e, d إذا علمت أن $p = 5, q = 7$ واحسب تشفير $M = 10$ ومن ثم احسب فك التشفير C.

التشفير المختلط والشهادات الرقمية

(Hybrid Encryption and Digital Certificates)

التشفير المختلط

يدمج التشفير المختلط بين التشفير المتناظر وغير المتناظر، فهو:

- يولد بطريقة عشوائية مفتاح متناظر يسمى مفتاح الجلسة.
- يتم تشفير مفتاح الجلسة بواسطة المفتاح غير المتناظر.
- يتم تشفير البيانات بواسطة مفتاح الجلسة المتناظر.
- سريع في عمليات التشفير وفك التشفير، وقام بحل مشكلة توزيع المفاتيح.

الشهادات الرقمية

لدينا المشكلة التالية: هل المفتاح العام الذي تم استلامه من الطرف الآخر ينتمي فعلاً للطرف الآخر؟ ألا يُخشى من اعتراضه أثناء إرساله بما يعرف بهجمات الرجل في المنصف (Man in The Middle Attacks) وتغييره؟

الحل في الشهادات الرقمية الموقعة من سلطة الشهادات (Certificate Authority :CA) والمعترف والموثوق (Trusted) بها من كل الأطراف. تتحقق سلطة الشهادات من صحة المعلومات الموجودة في الشهادة الرقمية بما في ذلك المفتاح العام الموجود فيها. سنتعرف كيف يتم هذا التحقق في الفقرات التالية:

إصدار الشهادة الرقمية (Issuing a Digital certificate)

تقوم سلطة الشهادات (Certificate Authority: CA) بإصدار[1] الشهادات الرقمية. تحتوي الشهادات الرقمية على المفتاح العمومي للمالك وهويته. لا يتم وضع المفتاح الخاص في الشهادة الرقمية حيث يبقى سرياً مع المالك الذي أنشئ زوج المفاتيح.

يمكن تصنيف سلطات الشهادات إلى عدة أنواع منها سلطة الشهادات المتوسطة (Intermediate CA) وسلطة الشهادات الجذر (Root CA). أشهر أمثلة سلطة الشهادات الجذر وهي التي تهمنا في هذه المحاضرة:

- Versign

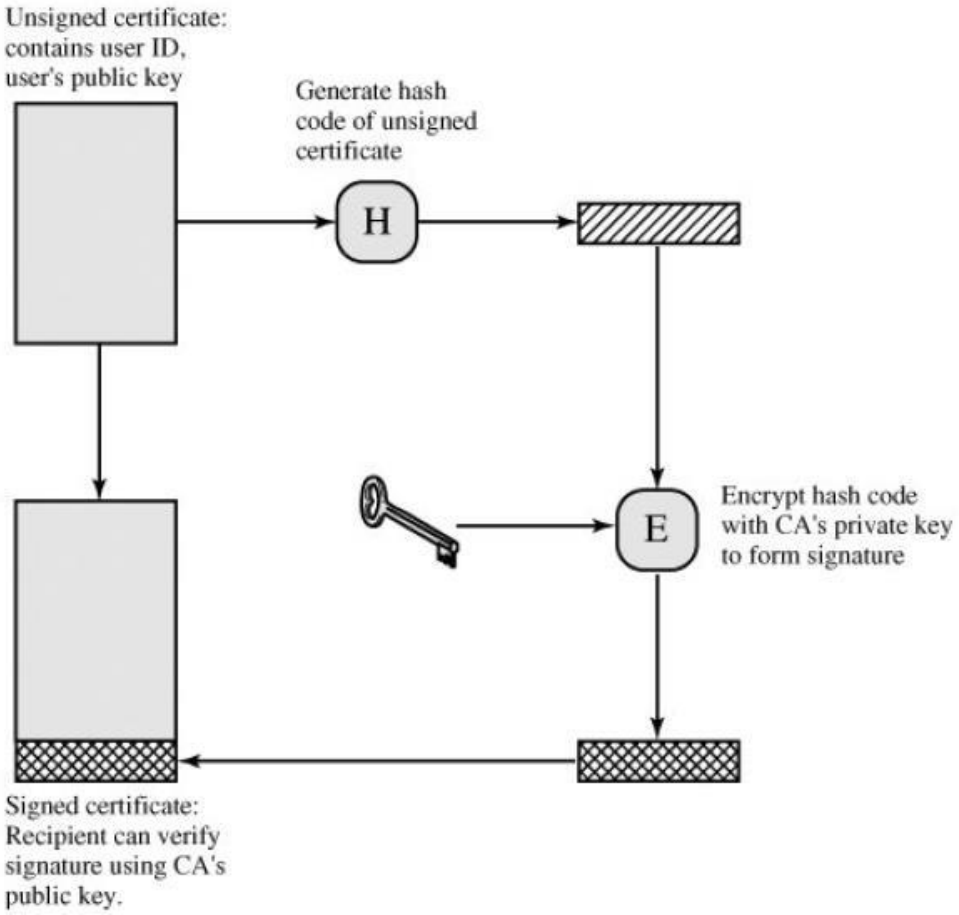
[1] تعرف عملية إصدار الشهادة الرقمية أيضاً بعملية توقيعها

- Comodo
- Digicert

مراحل توليد الشهادة الرقمية

للحصول على شهادة، يجب إنشاء طلب توقيع شهادة (Certificate Signing Request: CSR) في المخدم الخاص بك. تؤدي هذه العملية إلى إنشاء مفتاح خاص ومفتاح عام على المخدم. يحتوي ملف طلب توقيع الشهادة (CSR) الذي سترسله إلى سلطة الشهادات[2] على المفتاح العمومي للمخدم وعلى حقل "الموضوع" (Subject) – والذي يعبر عن هوية مالك الشهادة وهو صاحب موقع الويب – وعلى عنوان صاحب الشهادة...إلخ كما سترد لاحقاً. الجزء الأكثر أهمية في الشهادة هو أن يتم توقيعها رقمياً من قبل سلطة الشهادات.

يبين الشكل التالي شهادة غير موقعة وتحوي على معلومات تعريفية عن صاحب الشهادة بالإضافة إلى مفتاحه العام. تقوم سلطة الشهادات بتطبيق دالة اختزال (Hash) على الشهادة ثم تشفير خرج الدالة بواسطة المفتاح الخاص لسلطة الشهادات.



بمجرد استلام شهادة SSL الموقعة من سلطة الشهادات، يلزم تثبيتها على المخدم.

[2] تسمى سلطة الشهادات أيضاً بجهة إصدار الشهادة (Certificate issuer)

تحوي الشهادة الرقمية الموقعة على عدة بيانات أهمها:

- الرقم التسلسلي: وهو رقم فريد لتمييز الشهادة عن غيرها من الشهادات.
- اسم الكيان الذي أصدرت الشهادة من أجله الشهادة مثلاً اسم شخص أو مؤسسة أو خادم.
- التوقيع الرقمي
- الخوارزمية المستخدمة لإنشاء التوقيع الرقمي
- اسم الجهة المصدرة للشهادة، أي اسم سلطة الشهادات التي وقعت على الشهادة.
- تاريخ بداية ونهاية صلاحية الشهادة.
- المفتاح العام لتشفير الرسالة.

يمكن لأي شخص انشاء شهادة غير موقعة أو أن يقوم بتوقيعها بنفسه، ولكن المتصفحات تثق فقط في الشهادات التي يتم توقيعها من منظمة مدرجة في قائمة سلطة الشهادات داخل المتصفح، حيث تحوي المتصفحات على قائمة مثبتة مسبقاً من سلطة الشهادات الموثوق بها، والمعروفة باسم مخزن سلطات الشهادات الجذر الموثوقة (Trusted Root CA Store). داخل الشهادات الرقمية لسلطة الشهادات الجدر الموثوقة توجد المفاتيح العامة لها والتي يستخدمها المتصفح في التحقق من توقيعها الرقمي على الشهادات الرقمية للمواقع والمخدمات..

ما هي طبقة المقابس الآمنة (Secure Socet Layer: SSL)؟

طبقة المقابس الآمنة (SSL) هي تقنية أمان قياسية لانشاء اتصال مختلط مشفر بين المخدم والعميل. عادة ما يكون المخدم هو مخدم ويب أو مخدم بريد الكتروني، والعميل هو متصفح أو برنامج بريد إلكتروني (على سبيل المثال: Outlook)

تتيح طبقة المقابس الآمنة إرسال معلومات حساسة مثل أرقام بطاقات الائتمان وبيانات تسجيل الدخول بشكل آمن. عندما يتم ارسال البيانات بين المتصفحات ومخدمات الويب في نص صريح، تكون عرضة للتنصت.

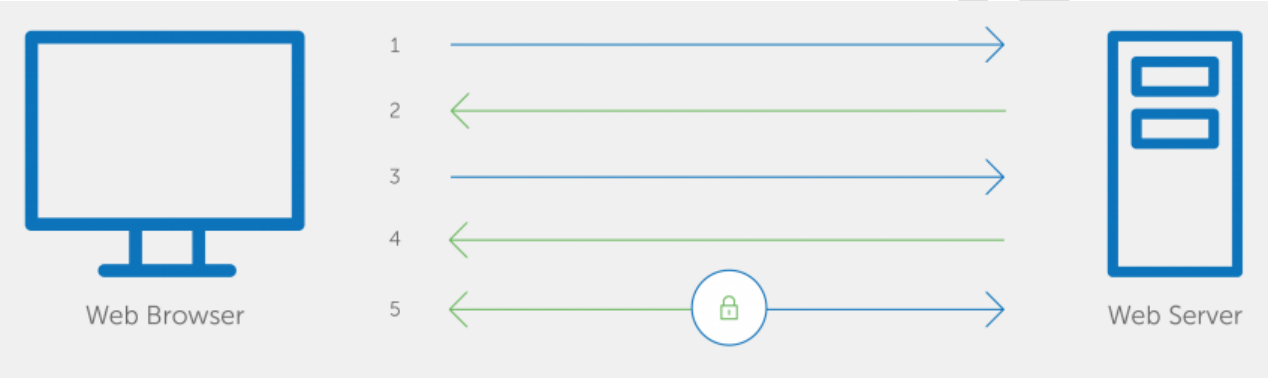
يحمي بروتوكول SSL بيانات الملايين من الأشخاص على الانترنت كل يوم. يعلم مستخدمو الانترنت بحدوث الاتصال الآمن عند ظهور رمز القفل أو شريط العناوين الأخضر في المتصفح، كما تبدأ مواقع الويب بالتحول إلى استخدام بروتوكول HTTPS بدلاً من HTTP.

كيف تقوم شهادة SSL بإنشاء اتصال آمن؟

عندما يحاول المتصفح الوصول إلى موقع ويب مؤمن ببروتوكول SSL، يقوم المتصفح ومخدم الويب بإنشاء اتصال بطبقة المقابس الآمنة باستخدام عملية تسمى "مصافحة SSL" كما هو موضح في الشكل التالي. لاحظ أن مصافحة SSL هي غير مرئية للمستخدم وتحدث على الفور.

يتم استخدام ثلاثة مفاتيح لإعداد اتصال SSL: المفتاح العام والمفتاح الخاص ومفتاح الجلسة. أي شيء مشفر بالمفتاح العمومي يمكن فك تشفيره فقط بالمفتاح الخاص، والعكس بالعكس.

لأن التشفير وفك التشفير غير المتناظر بالمفتاح العام والخاص يستهلك قدراً كبيراً من قوة المعالجة، لذلك يتم استخداماها فقط خلال مصافحة SSL لانشاء مفتاح الجلسة المتناظر (Symmetric). بعد اجراء اتصال آمن، يتم استخدام مفتاح الجلسة لتشفير كافة البيانات المرسلة.



مراحل المصافحة الخمسة هي:

1. يتصل المتصفح بمخدم الويب (الموقع) المؤمن ببروتوكول SSL (HTTPs). يطلب المتصفح أن يقوم المخدم بتعريف نفسه.
2. يرسل المخدم نسخة من شهادة SSL الخاصة به، والتي تحوي على المفتاح العمومي للمخدم.
3. يقوم المتصفح بالتحقق من الشهادة من قائمة سلطة الشهادات الموثوق بها بما في ذلك أن الشهادة غير منتهية الصلاحية، غير مستردة، وأن الاسم هو لموقع الويب الذي يتصل به. إذا تحقق المتصفح من الشهادة فإنه يقوم بانشاء مفتاح جلسة متناظر ويشفره باستخدام المفتاح العمومي للمخدم.
4. يقوم المخدم بفك تشفير مفتاح الجلسة المتناظر باستخدام مفتاحه الخاص ويرسل اشعار موافقة مشفراً بمفتاح الجلسة لبدء الاتصال المشفر.
5. كلا المخدم والمتصفح الآن يشفران كافة البيانات المرسلة عبر مفتاح الجلسة.

هل شهادتي هي SSL أم TLS

يتم استخدام بروتوكول SSL لتشفير وحماية البيانات المرسلة وفي كل مرة تيم اصدار نسخة جديدة أكثر أمناً. يستخدم رقم النسخة فقط لبيان التغيير وعلى أية حال وعندما يحل موعد تحديث الإصدار SSLv3.0 فإنه يتم عادة إعادة تسمية النسخة TLSv1.0 بدلاً من SSLv4.0 ليصبح حالياً TLSv1.2.

مازالت بعض سلطات الشهادات تستخدم الاسم SSL عند الإشارة إلى شهادات أو تصف كيفية تأمين البيانات المنقولة.

المراجع:

[1]: https://www.digicert.com/ssl/

[2]: Cryptography and Network Security (4th Edition)

المهندس باسل دهيمش

جدر الحماية

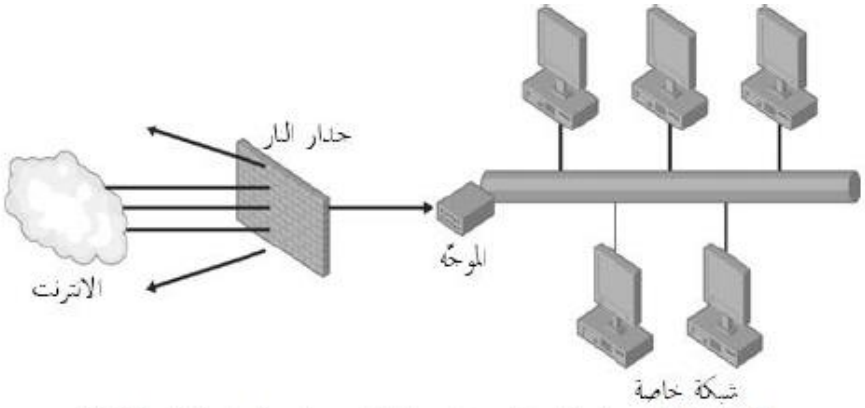
1.8- مقدمة (Introduction):

الوظيفة الرئيسية لمسؤول الشبكة هي ضمان امتلاك المستخدمين وصولاً إلى الخدمات التي يحتاجون إليها عندما يريدون ذلك. هناك عاملان من العوامل الرئيسية التي يمكن أن تتدخّل بذلك الوصول وهما الخروقات الأمنية وأعطال الأجهزة. يناقش هذا الفصل بعض التقنيات التي يمكنك استخدامها لحماية شبكتك من اقتحام المستخدمين غير المرخّصين ومن الوقت والإنتاجية الضائعين نتيجة اختلالات إعدادات الأمان في الشبكة.

2.8- جدار النار (Firewall):

الأمان هو جزء من عمل كل مسؤول شبكة، سواء كانت هناك بيانات سرية مخزّنة في الحواسيب الشبكية أم لا، بل وحتى حماية نظام التشغيل وملفات البرامج الحيوية من الحذف غير المقصود هي وظيفة أمنية. يتم استعمال آليات مختلفة لتزويد أمان الشبكة لأن هناك أنواع مختلفة من الحماية مطلوبة. يستعمل مسؤول الشبكة بشكل كبير الأذونات (Permissions) وآليات أخرى للتحكم بالوصول إلى موارد الشبكة. هذا يمنع المستخدمين الداخليين من الوصول إلى الموارد المحظورة، لكن هناك عالم بأكمله من الأخطار الأمنية المحتملة خارج الشبكة. الاتصال بالانترنت الذي يتوفر في معظم الشبكات هذه الأيام هو الباب الذي يمكن أن تدخل عبره تلك الأخطار. جدار النار (Firewall) هو جهاز أو برنامج يحمي الشبكة من الوصول غير المرخّص من قِبل جهات خارجية، بينما يسمح لحركة المرور الملائمة بالعبور حسب الشكل (1.8). إذا كانت شبكتك موصولة بالانترنت، يجب أن يكون لديك أحد أنواع جدران النار لحمايتها لأن المخترقين (Hackers) يمكن أن يعيثوا فساداً في الشبكة التي بذلت جهداً كبيراً في تصميمها وبنائها.

ملاحظة: تُنشر جدران النار عادة لحماية شبكة خاصة أو شبكة بينية من الوصول غير المرخّص من خلال الانترنت، لكن يمكنك استعمال جدار نار داخلياً أيضاً لحماية أحد أقسام الشبكة من بقية أقسامها. فمثلاً، يمكنك استعمال جدار نار لعزل الشبكة المحلية التي يستعملها قسم المحاسبة في شركتك لكي تمنع المستخدمين الآخرين من الوصول إلى السجلات المالية السرية.



الشكل (1.8): جدار النار يقوم بمنع حركة المرور غير المرخصة في الشبكة.

جدار النار هو في الأساس حاجز بين شبكتين يقيّم كل حركة المرور الواردة أو الصادرة ليحدّد ما إذا كان عليه السماح لها بالمرور إلى الشبكة الأخرى أم لا. يمكن أن يأخذ جدار النار عدة أشكال ويمكنه أن يستعمل معايير مختلفة لتقييم وفحص حركة المرور التي يتلقاها.

بعض جدران النار هي أجهزة مادية مخصصة لأداء مهمة معينة، وهي مراقبة حركة المرور الواردة والصادرة. تستطيع جدران النار أن تستعمل عدة طرق لفحص حركة المرور في الشبكة واكتشاف التهديدات المحتملة، كما وتزوّد خدمات متنوعة أخرى في أغلب الأحيان. فمثلاً أحد منتجات جدار النار وهو المخدم الوكيل (Proxy Server) لا يتيح للمستخدمين الوصول إلى صفحات الويب مع أمان كامل فقط، بل ويمكنه أيضاً أن يخبئ الصفحات الأكثر استعمالاً لكي تتمكن حواسيب الشبكة الأخرى من استخراجها بشكل أسرع.

في الحالات الأخرى، جدران النار هي برامج تشغّل على حاسوب عادي. في أحد الأوقات، كانت كل جدران النار مكلفة جداً ومعقّدة، وتُستعمل فقط في الشبكات المحترفة. لا تزال تلك المنتجات الحديثة متواجدة، لكن يمكنك الآن شراء برامج جدار نار رخيص تحمي شبكة صغيرة أو حتى حاسوباً فرديا من الوصول غير المرخّص القادم من خلال الاتصال الانترنت.

لدينا عدة أنواع من تقنيات جدار النار سنتناولها جميعاً، وسنبدأ بأول نوع وهو جدار نار تصفية الحزم:

1- جدار نار تصفية الحزمة (Packet Filter Firewall):

عامل تصفية الحزم (Packets Filter) هو أبسط أنواع جدران النار، يفحص فيه النظام الذي يطبّق عامل التصفية كل حزمة واردة ويقرّر ما إذا كانت تستوفي المعايير ليحق لها الدخول إلى الشبكة –سنناقش هذه المعايير في الفقرة التالية–. الحزم التي تستوفي معايير الدخول يعالجها النظام بالأسلوب العادي، أما الحزم الأخرى فتُرمى.

تُستعمل تصفية الحزم في المقام الأول من قِبل الموجّهات وجدران النار التي توصل شبكة خاصة بالانترنت، لكن يمكنك استعمالها داخل شبكة خاصة أيضاً لعزل أحد أجزاء الشبكة عن

البقية. هناك قدرات تصفية حزم موجودة في معظم الموجّهات لكي تتمكن من تطبيق عوامل التصفية على الحدود بين الشبكات. المشكلة في دمج عوامل تصفية الحزم في الموجّه هي أن عوامل التصفية يمكنها أن تزيد من الأعباء كثيراً مما يُبطئ أداء الموجّه. يجب أن يفحص الموجّه كل حزمة واردة، ويقارنها بكل عوامل التصفية ثم يقرّر ما إذا كان سيقبلها في الشبكة أم لا. إذا كان لديك عدد كبير ومعقّد من عوامل التصفية، يمكن للفترة الزمنية المطلوبة لكي يعالج الموجّه كل حزمة أن تصبح نقطة اختناق رئيسية في أداء الشبكة. وعند أخذ أعباء المعالجة التي تسبّبها تصفية الحزم بعين الاعتبار، يجب أن تقرر ما هو أفضل مكان لإدارة تلك الأعباء.

تصفية الحزم ليست حلاً أمنيا مثالياً، إذ لا يزال بإمكان المخترقين مهاجمة مخدم باستعمال المنافذ والبروتوكولات التي يسمح لها جدار النار بالعبور أو يجدون طريقة جديدة ذكية لتخطي عوامل التصفية المستخدَمَة. السر في استعمال عوامل تصفية الحزم بفعالية هو بفرض توازن بين إعطاء المستخدمين الشرعيين وصولاً كافياً ومنع ماتبقى من حركة المرور لتزويد الحماية. في بعض الحالات يمكن أن يكون إنشاء عوامل تصفية الحزم معركة متواصلة بين المدافع عن الشبكة وبين المهاجم العنيد الذي يحاول اختراقها. كلما وجد المهاجم طريقة ليخترق عوامل التصفية،

البقية. هناك قدرات تصفية حزم موجودة في معظم الموجّهات لكي تتمكن من تطبيق عوامل التصفية على الحدود بين الشبكات. المشكلة في دمج عوامل تصفية الحزم في الموجّه هي أن عوامل التصفية يمكنها أن تزيد من الأعباء كثيراً مما يُبطئ أداء الموجّه. يجب أن يفحص الموجّه كل حزمة واردة، ويقارنها بكل عوامل التصفية ثم يقرّر ما إذا كان سيقبلها في الشبكة أم لا. إذا كان لديك عدد كبير ومعقّد من عوامل التصفية، يمكن للفترة الزمنية المطلوبة لكي يعالج الموجّه كل حزمة أن تصبح نقطة اختناق رئيسية في أداء الشبكة. وعند أخذ أعباء المعالجة التي تسبّبها تصفية الحزم بعين الاعتبار، يجب أن تقرر ما هو أفضل مكان لإدارة تلك الأعباء.

2.2.8- معايير تصفية الحزم (Packets Filter Standards):

إنشاء عوامل تصفية الحزم هي مسألة انتقاء المعايير المحدَّدة التي تريد أن يفحصها النظام وتحديد القيم المسموحة أو الممنوعة من المرور عبر عامل التصفية. يمكن أن تكون عوامل تصفية الحزم ضمنية أو حصرية.

مع عامل تصفية ضمني، ستبدأ باتصال شبكي محظور كلياً وتستعمل عوامل تصفية لتحدّد ما هي حركة المرور التي يمكنها أن تمرّ عبرها. أما مع عامل تصفية حصري فتبدأ مع اتصال مفتوح كلياً وتحدّد أنواع حركة المرور التي تريد منعها.

عامل تصفية الحزم الضمني أكثر أمناً، لكن إزالة الأخطاء منه يمكن أن تكون أصعب لأنه عليك أن تتأكد أن كل حركة المرور التي يجب أن تمرّ عبر عوامل التصفية تمر فعلاً.

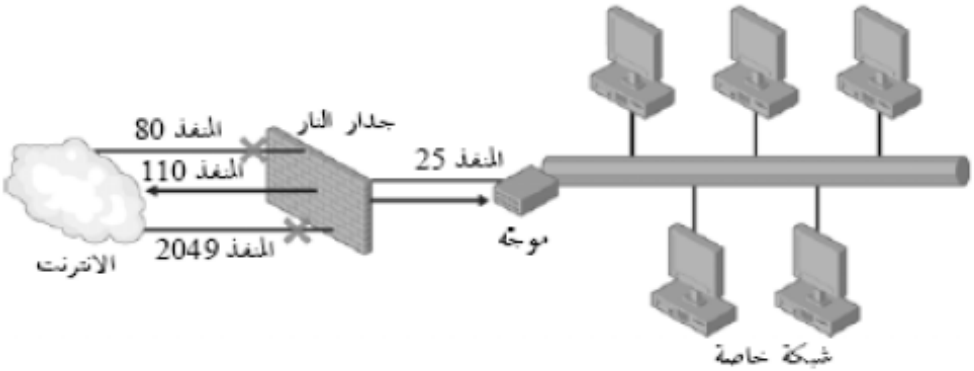
ملاحظة: التصفية الثنائية الاتجاه هي أن تعمل تصفية الحزم في كلا الاتجاهين. فمثلاً، يمكنك استعمال عوامل تصفية لمنع مستخدمي الانترنت من الوصول إلى شبكتك الخاصة، أو يمكنك استعمالها للحد من الوصول الممنوح لمستخدميك المتصلين بالانترنت.

المعايير الأكثر استعمالاً في تصفية الحزم هي كالتالي:

- **أرقام المنافذ:** تعتبر التصفية بأرقام المنافذ، المعروفة أيضاً بالتصفية المعتمِدة على الخدمة (Service-Dependent Filtering) هي النوع الأكثر شيوعاً لتصفية الحزم وأكثرها مرونة، لأن أرقام المنافذ تمثّل برامج محدَّدة يمكنك استعمالها لمنع حركة المرور التي تولّدها تلك البرامج من بلوغ الشبكة.

مثال1: لحماية شبكة تحتوي على مخدمات ويب بشركتك يمكنك إنشاء عوامل تصفية تسمح فقط لحركة المرور التي تستعمل المنفذ 80 من الدخول من الانترنت، مانعة كل منافذ البرامج الأخرى.

مثال2: تستعمل مخدمات البريد الإلكتروني عادة بروتوكول نقل البريد البسيط (SMTP) لحركة المرور الصادرة وبروتوكول مكتب البريد الإصدار 3 (POP3) لحركة المرور الواردة. تستعمل تلك البروتوكولات أرقام المنافذ المشهورة 25 و 110 على التوالي. يمكنك إنشاء عامل تصفية حزم يسمح فقط للحزم المعنونة إلى أرقام المنافذ 25 و 110 بالمرور عبر جدار النار كما في الشكل (2.8)، أما الحزم التي فيها أي أرقام منافذ أخرى تُرمى قبل أن يمكنها التسبّب بأي أضرار.



الشكل (2.8): جدار نار تصفية الحزم حسب أرقام المنافذ.

■ **معرِّفات البروتوكول**: في معظم الحالات، تمثّل الشيفرة بروتوكولاً لطبقة النقل، كبروتوكول TCP أو بروتوكول UDP.

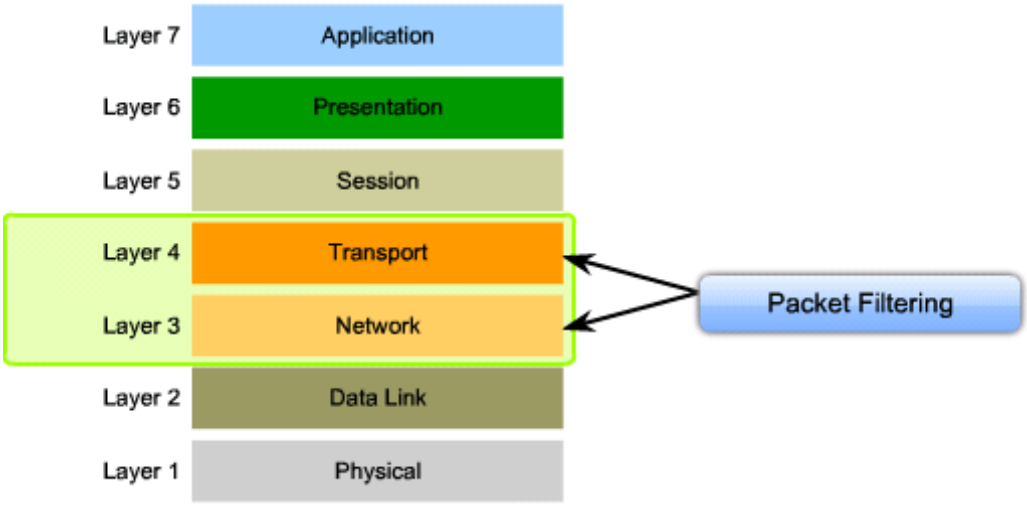
لكن كثيراً ما تحمل رزم IP رسائل ICMP أيضاً. التصفية باستعمال معرِّفات البروتوكول ليست دقيقة جداً لأنها تمنع أو تسمح كل حركة المرور التي تستعمل بروتوكولاً معيناً. لكن منع بروتوكول كامل هو أمر ضروري أحياناً لبعض البرامج، وهو أسهل من توقع البرامج المحددة التي قد يستعملها المهاجم. فمثلاً، إذا كانت لديك شبكة تحتوي على مخدمات ويب ومخدمات FTP فقط، يمكنك استعمال عوامل تصفية معرفات البروتوكول لجعل حركة المرور الواردة تقتصر على حزم TCP لأن تلك المخدمات تعتمد على بروتوكول TCP لتنفذ وظائفها الرئيسية. يمكنك منع كل حركة مرور ICMP و UDP فتمنع المهاجمين الذين يستعملون كل البرامج التي تعتمد على هذين البروتوكولين.

ملاحظة هامة: هناك نوع من الهجمات تسمى الحرمان من الخدمة (Denial of Service: DoS) وهو يستعمل البرنامج Ping في عدة حواسيب لإرسال دفق متواصل من رسائل طلب الصدى (Echo Request) إلى ملقم معين، لذا يصبح الملقم مشغولاً جداً في الرد على طلبات Ping بحيث ينخفض أداؤه بشكل خطير ، مما يمنعه من تنفيذ وظيفته الرئيسية. لمنع هذا النوع من الهجمات يمكنك استبعاد كل حركة مرور ICMP وهذا يمنع طلبات Ping من بلوغ الملقم.

■ **العناوين IP**: تتيح لك تصفية العناوين IP أن تجعل الوصول إلى الشبكة يقتصر على حواسيب محددة. فمثلاً إذا كان لديك مخدم ويب في شبكة LAN فيها حواسيب أخرى وتريد أن يكون عملاء الانترنت قادرين على الوصول إلى ملقم الويب فقط، يمكنك إنشاء عامل تصفية يسمح فقط للحزم المعنونة إلى مخدم الويب بالدخول من الانترنت إلى شبكتك وتحديداً إلى ملقم الويب. يمكنك استعمال تصفية العناوين IP أيضاً لحماية جزء من شبكة خاصة حيث يمكنك إنشاء عوامل تصفية تعطي بعض الحواسيب فقط وصولاً إلى الشبكة LAN المحمية، بينما تمنع كل الحواسيب الأخرى من الوصول إليها.

ملاحظة: التصفية باستعمال العناوين IP ليست آمنة إذا كان المهاجمون المحتملون يملكون طريقة لاكتشاف العناوين IP لحواسيب شبكتك، كإطلاعهم على سجلات نظام أسماء النطاق DNS. فبعد اكتشاف المهاجم لعناوين IP التي يسمح لها عامل التصفية بالوصول إلى الشبكة، من السهل عليه انتحال عنوان IP لحاسوب آخر واستغلال إمكانية هذا الحاسوب بالوصول للشبكة، وهذا ما يعرف بالتزوير (Spoofing).

نادراً ما تُستعمل تصفية العناوين الفيزيائية في موجّهات أو جدران النار الانترنت، لكنها وسيلة مفيدة لتصفية العناوين الفيزيائية الداخلية لتقييد الوصول إلى موارد محدَّدة. يبين الشكل (3.8) معايير تصفية الحزم حسب طبقات OSI.



الشكل (3.8) معايير تصفية الحزم.

تبرز القوة الحقيقية لاستعمال تصفية الحزم كآلية أمان عندما تدمج أنواع مختلفة من عوامل التصفية لإنشاء حل مركب. فمثلاً قد تريد فتح منفذ Telnet ذو الرقم 23 لكي يتمكن مسؤولوا الشبكة من إدارة مخدمات ويب الشركة من المنزل عن بُعد باستعمال الانترنت، لكن ترك هذا المنفذ مفتوحاً يعتبر بمثابة دعوة لمستخدمي الانترنت غير المرخَّصين للوصول إلى مخدماتك.

يمكنك إضافة عامل تصفية يسمح فقط للعناوين IP الخاصة بمسؤولي الشبكة من الوصول إلى المنفذ 23. هذا سيحمي الشبكة من دون أن تتأثر الوظائف التي يحتاج إليها المسؤولون.

أحد عوائق استخدام عامل تصفية الحزم هو:

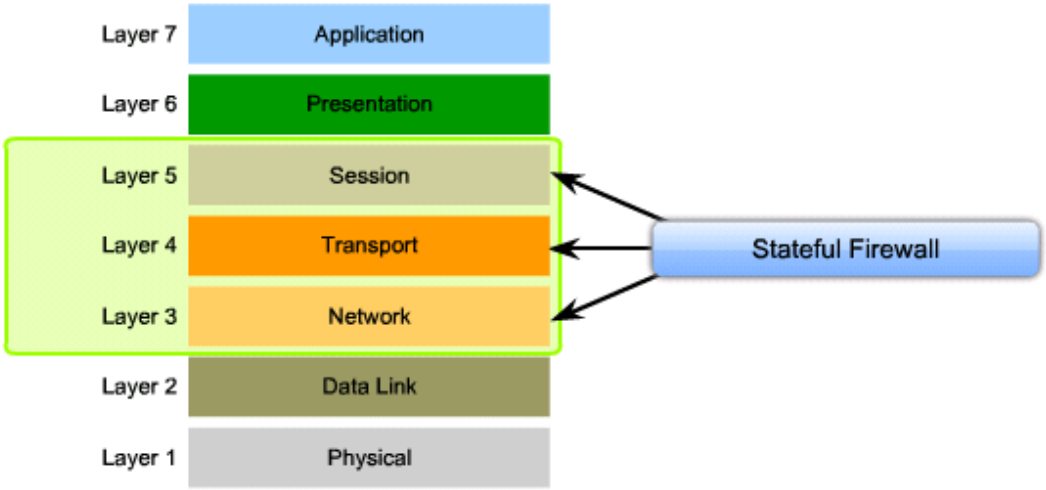
- تستطيع عوامل تصفية الحزم أن تكتشف فقط الهجمات المطبَّقة في رؤوس الحزم. إنها لا تفحص بيانات البرامج الموجودة داخل الحزم. فمثلاً، قد تضبط إعدادات عوامل تصفية الحزم في جدار النار الخاص بك للسماح لكل حركة مرور المنفذ 80 بدخول الشبكة لكي يتمكن مستخدموا الانترنت من الوصول إلى مخدمات الويب لديك، ولكن ذلك سيؤدي في الوقت نفسه إلى قبول الحزم المصممة لمهاجمة خدمة الويب نفسها. لفحص بيانات طبقة البرامج في الحزم، يجب أن تستعمل مخدماً وكيلاً.

تابع جدر الحماية

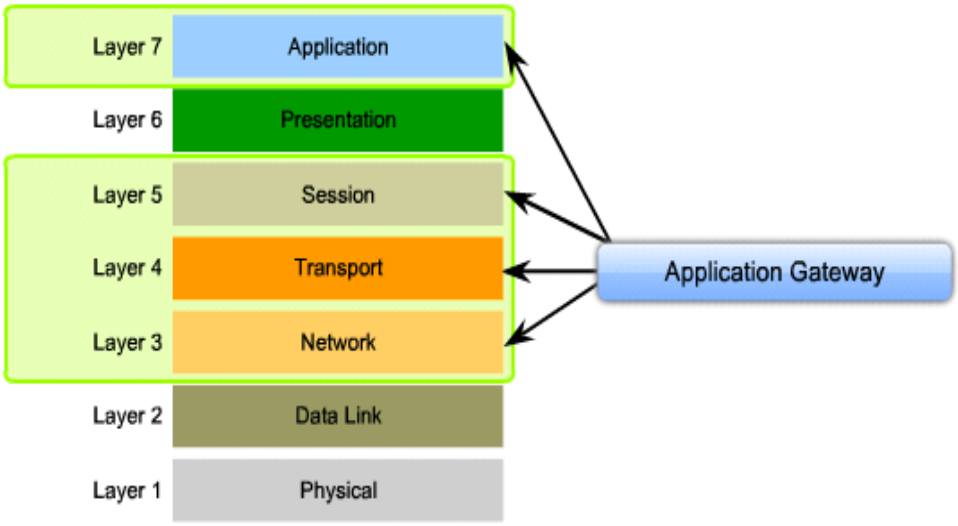
ملاحظة: يسمى جدار نار تصفية الحزم بعديم الحالة (Stateless firewall) فهو لا يفحص الاتصال.

2- جدار نار كامل الحالة (Stateful Firewall): يحافظ على المسار الخاص بحالة الاتصال، ويفحص فيما إذا كان الاتصال قد تم تأسيسه، وأنه قد تم انتقال البيانات، وأنه قد تم إنهائه. يمتد عمل جدار نار كامل الحالة على طبقات النموذج OSI في L3 و L4 و L5.

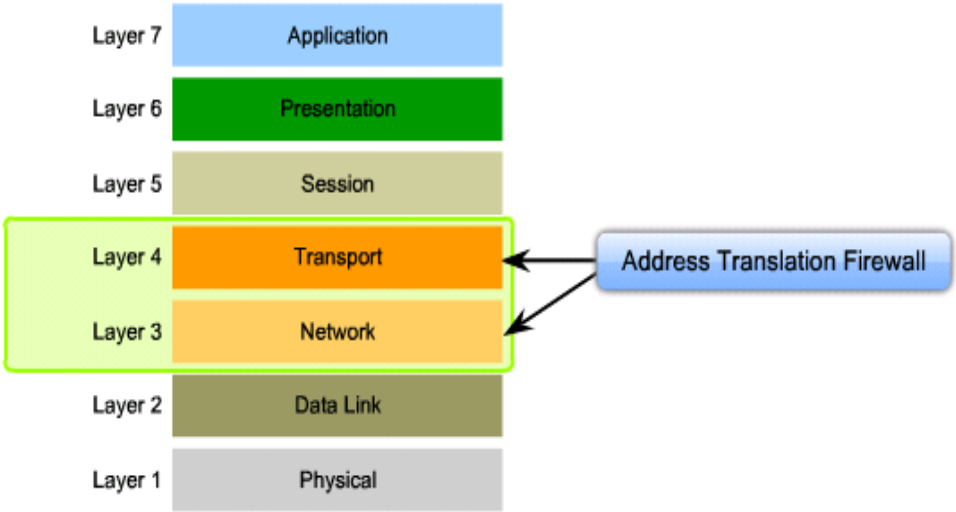
هذا النوع من جدران الحماية مفيد مثلاً عندما نريد أن نحجب تأسيس اتصال من أجهزة الشبكة الخارجية لشبكتنا ولكن نريد في نفس الوقت السماح لأجهزتها بتأسيس اتصال إلى الشبكة الخارجية.



3- جدار نار عبّارة التطبيقات (Application gateway firewall): يقوم بتصفية المعلومات على الطبقات L3 و L4 و L5 و L7. يسمى أيضاً بجدار الحماية الوكيل **(proxy firewall).**



4- جدار النار ترجمة عنوان الشبكة (Network Address-Translation Firewall): ويقوم بإخفاء عناوين الشبكة المحلية عن عناوين الشبكة الخارجية.



5- جدار النار المعتمد على المضيف (Host-based) : قد يكون شخصي على حاسب شخصي أو على شكل مخدم (server or personal)، وتتم عادة عملية التحكم والصفية في هذا النوع على شكل منتج برمجي.

مثال على (Personal Firewall): هو جدار الحماية بنظام التشغيل ويندوز Windows Firewall .

مثال على (Server Firewall): هو جدار الحماية الموجود في منتج Kaspersky Total Security for Business

6- جدار النار الهجين (Hybrid firewall): هو عبارة عن دمج لعدة أنواع من جدر الحماية السابقة ، فمثلاً قد يوجد جدار حماية يدمج تقنية كامل الحالة مع عبارة التطبيقات.

سنتعمق في القسم النظري والعملي بجدار الحماية الوكيل وبجدار حماية ترجمة عنوان الشبكة.

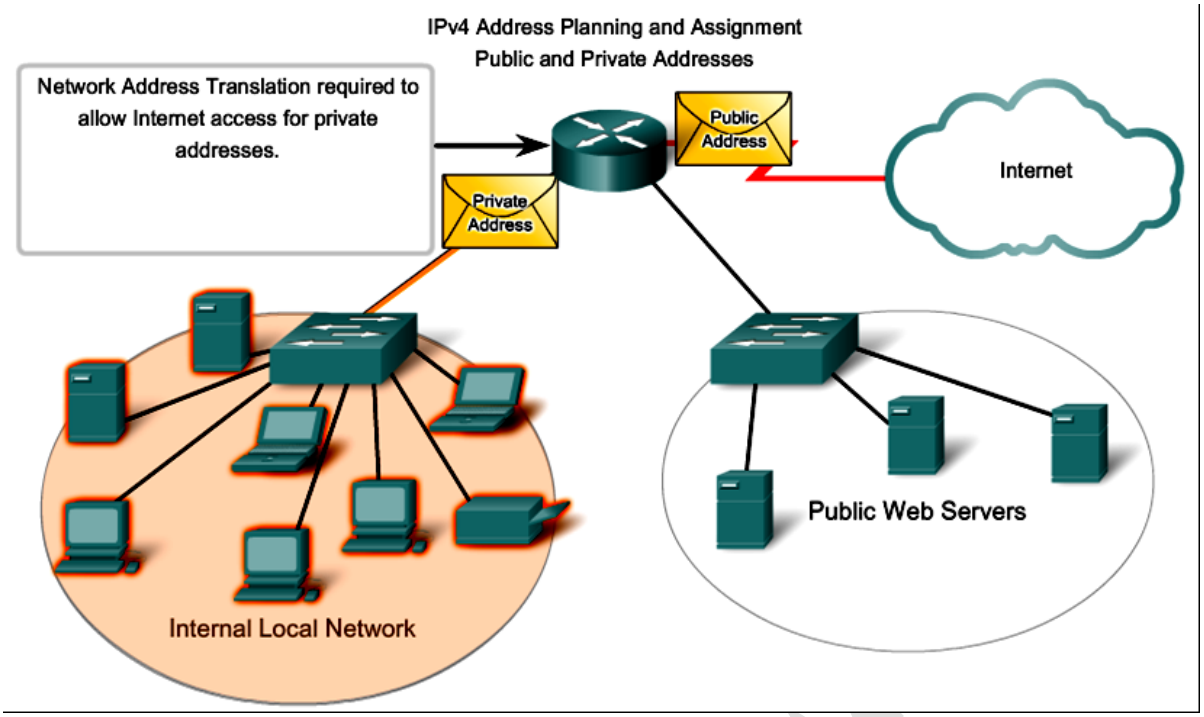
المهندس باسل دهيمش

3.8- ترجمة عنوان الشبكة (Network Address Translation: NAT):

قبل الحديث عن مفهوم ترجمة عنوان الشبكة وفائدته في زيادة أمان الشبكات المحلية، علينا تسليط الضوء أولاً على أقسام عناوين IP حسب مكان استخدامها.

1.3.8- العناوين المسجَّلة وغير المسجَّلة (Registered and Unregistered Addresses):

عندما تم تحديد عناوين IP قُسمت هذه العناوين إلى مجموعتين، المجموعة الأولى سميت العناوين العامة (Public Addresses)، وهي العناوين التي يتم استخدامها على الانترنت وتستخدمها موجهات مزودات خدمة الانترنت لتوجيه حزم البيانات عبر الانترنت. يجب أن لايوجد في هذه العناوين قيم مكررة على الانترنت، بمعنى أن كل مزود يحجز مجموعة من هذه العناوين بحيث لا تتكرر قيمها مع مزود أخر . تقوم جهة دولية بمهمة منح المزودات في كل أنحاء العالم بعناوين الانترنت بشكل منظم. تسمى هذه الجهة ب منظمة الأعداد المعيَّنة للانترنت (Internet Assigned Numbers Authority: IANA). تسمى هذه العناوين عادة بالعناوين المسجلة (Registered IPs)، أو العناوين العامة (Public IPs)، أو عناوين الانترنت (Internet IPs)، أو العناوين الحقيقية (Real IPs). وبسبب الحاجة لحماية وعزل الشبكات المحلية الخاصة عن شبكة الانترنت، وخشية نفاذ واستهلاك عناوين IP V4 بدون فائدة، برزت الحاجة لانشاء المجموعة الثانية من العناوين سميت بالعناوين غير المسجلة (Unregistered IPs)، أو العناوين الخاصة (Private IPs). هذه العناوين تستخدم في الشبكات المحلية الخاصة بالأفراد والشركات، ولايمكن استخدامها كعناوين على الانترنت. لذلك وعند رغبة الحواسيب المحلية ذات العناوين الخاصة الاتصال وتبادل الحزم مع حواسيب الانترنت ذات العناوين العامة تقوم موجهات مزودات الخدمة بتغيير العناوين الخاصة إلى عامة لكي تستطيع هذه الحزم التنقل عبر الانترنت وهو ما يوضحه الشكل (4.8). تسمى هذه التقنية التي تحول العناوين من عناوين خاصة إلى عامة وبالعكس بخدمة ترجمة عنوان الشبكة (Network Address Translation: NAT).



الشكل (4.8): خدمة ترجمة عناوين الشبكة.

لكي يمكن النفاذ إلى حاسوب من الانترنت، يجب أن يملك عنواناً IP عمومياً مسجلاً مع IANA. لكن ليس كل حاسوب يمكنه أن يتصل بالانترنت يجب أن يكون قابلاً للوصول من قبل الحواسيب الأخرى على الانترنت.

عادة تستعمل الحواسيب في شبكة خاصة عناوين IP خاصة وغير مسجَّلة يستطيع مسؤول الشبكة أن يعينها بحرية دون الحصول عليها من مزوّدٍ أو IANA. الغاية من العناوين الخاصة هو استعمالها في الشبكات الخاصة وهي ليست مسجَّلة لأي شخص. عند بناء شبكة خاصة يجب أن تستعمل تلك العناوين بدلاً من اختيار عنوان بشكل عشوائي.

لذا حدّدت IANA ثلاثة مجالات عناوين لتُستعمل في الشبكات الخاصة فقط. مجالات العناوين تلك غير ممنوحة لأي مستخدم انترنت، وبالتالي فهي غير مرئية من الانترنت وبالتالي يمكنك نشرها بأمان في حاسوبك من دون خطر أن يصل إليها مخترقوا الانترنت. لكن هذا يعني أيضاً أن ملقمات الانترنت، بعدما تتلقى طلبات من حواسيب الشبكة الخاصة، لا يمكنها أن ترسل

ردوداً عليها. يحل NAT هذه المشكلة بأن يعمل كوسيط بين الانترنت وحاسوب العميل في شبكة غير مسجَّلة. لكل حزمة يوّلدها العميل، يستبدل موجّه NAT العنوان غير المسجَّل للعميل بعنوان مسجَّل. يوضح الجدول (1.8) العناوين غير المسجَّلة لكل فئة:

Range of IP Addresses	Class of Networks	Number of Networks
10.0.0.0 to 10.255.255.255	A	1
172.16.0.0 to 172.31.255.255	B	16
192.168.0.0 to 192.168.255.255	C	256

الجدول (1.8): العناوين غير المسجلة.

إذاً فترجمة عنوان الشبكة (Network Address Translation: NAT) هو أسلوب توجيه يمكّن الحواسيب التي لها عناوين غير مسجَّلة من الوصول إلى الانترنت. إذا جعلت شبكة تتصل بالانترنت من دون حماية جدار نار من أي نوع كان، يجب أن تستعمل عناوين IP مسجَّلة لحواسيبك لكي يمكنها أن تتصل بالأنظمة الأخرى. لكن عناوين IP المسجَّلة هي مرئية من الانترنت هذا يعني أن أي مستخدم على الانترنت يمكنه أن يصل إلى شبكة حواسيبك، ومع بعض الإبداع القليل، يُحدث فوضى في شبكتك.

تمنع NAT حصول هذا بأن تتيح لك تعيين عناوين IP غير مسجَّلة لحواسيبك، لذلك تعتبر NAT أحد الوسائل الأمنية الهامة في عالم الشبكات.

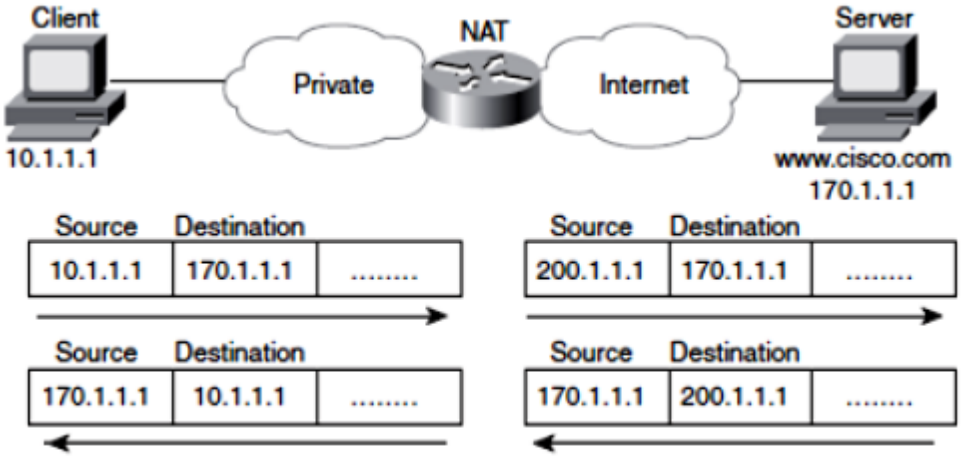
2.3.8- مصطلحات العناوين الخاصة والعامة (Private And Public Addresses Terms):

نعرّف أهم المصطلحات المتعلقة بالعناوين الخاصة والعامة كما يلي:

- ✓ **Inside Local Addresses**: تدل الكلمة Inside على عناوين تستخدم للإشارة إلى الأجهزة التي هي بداخل الشبكة المحلية، أما مصطلح Inside Local فهو العنوان الفعلي للحواسيب الموجودة داخل هذه الشبكة المحلية.
- ✓ **Inside Global Addresses**: تدل الكلمة Inside على عناوين تستخدم للإشارة إلى الأجهزة التي هي بداخل الشبكة المحلية، أما مصطلح Inside Global فيمثّل حواسيب الشبكة المحلية التي ترسل حزم إلى الشبكة الخارجية كشبكة الانترنت مثلاً.
- ✓ **Outside Global Addresses**: تدل الكلمة Outside على عناوين تستخدم للإشارة إلى الأجهزة التي تعمل خارج الشبكة المحلية، أما مصطلح Outside Global فهو العنوان الفعلي للحواسيب الموجودة خارج الشبكة المحلية كشبكة الانترنت مثلاً.

3.3.8- مثال على NAT (NAT Example):

ليكن لدينا زبون (client) موجود ضمن شبكة خاصة يحمل العنوان 10.1.1.1 وهو من النوع Inside Local يريد هذا الجهاز الاتصال بجهاز مخدم (Server) موجود على الشبكة الخارجية (الانترنت) ويحمل العنوان 170.1.1.1 وهو من النوع Outside Global. بما أن العنوان 10.1.1.1 من النوع الخاص ولا يستخدم على شبكة الانترنت، فإن الموجه الذي يقوم بوظيفة NAT يترجم العنوان 10.1.1.1 إلى العنوان 200.1.1.1 وهو من النوع Inside Global. من خلال ذلك نستنتج أن الموجه قام بترجمة عنوان IP المصدر للحزم المتجهة من الشبكة الداخلية إلى الشبكة الخارجية، وقام بوضع نتيجة الترجمة في جدول خاص يسمى جدول NAT (NAT Table) وبالتالي فإن المخدم يستقبل الحزم على أنها قادمة من العنوان 200.1.1.1. وعندما يقوم المخدم بإجابة الطلب يكون عنوان IP الهدف هو 200.1.1.1 ويكون عنوان IP المصدر هو 170.1.1.1. عند وصول الحزم إلى الموجه يقوم هذا الموجه بترجمة عنوان الوجهة من 200.1.1.1 إلى 10.1.1.1، حسب ما يوضح ذلك الشكل (5.8).



الشكل (5.8): مثال على ترجمة عناوين الشبكة.

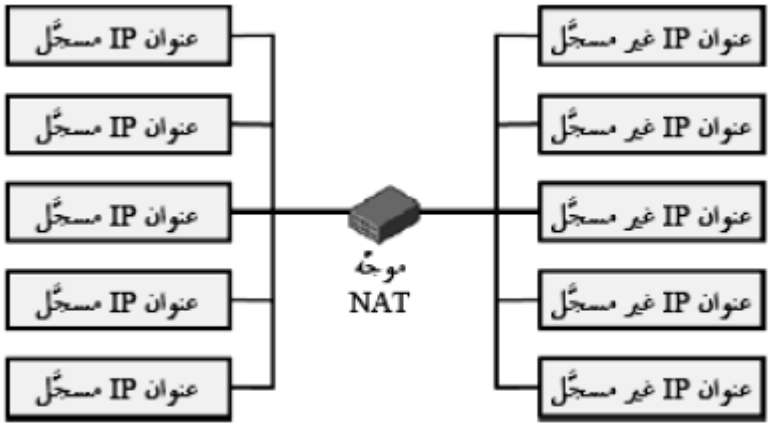
4.3.8- أنواع NAT (NAT Types):

هناك ثلاث أنواع رئيسية من NAT هي:

1- NAT الساكن (Static NAT):

يترجم NAT الساكن "الثابت" عدداً من العناوين IP غير المسجَّلة إلى عدد مساوٍ من العناوين المسجَّلة، مما يتيح لكل عميل أن يستعمل نفس العنوان المسجَّل دائماً.

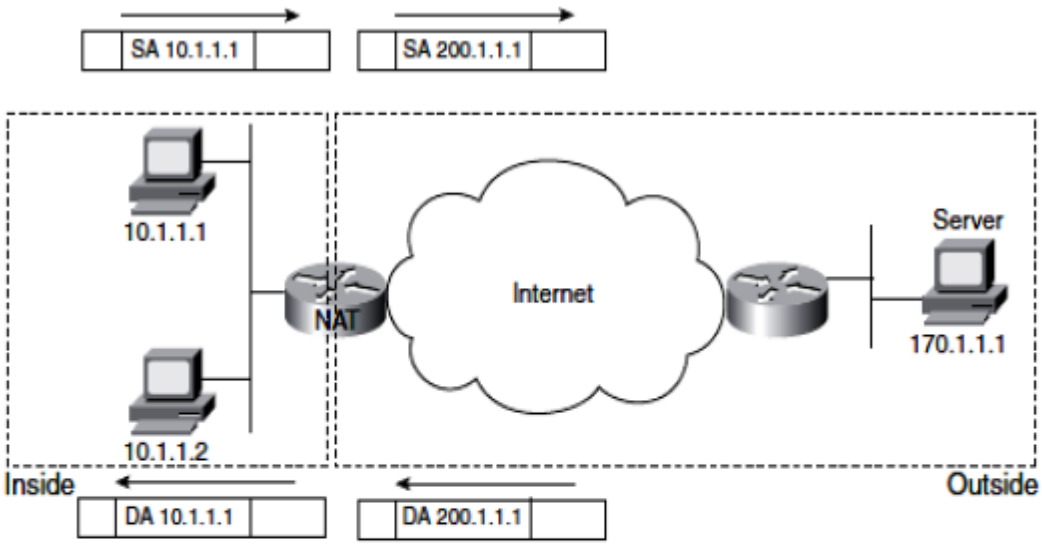
لا يحافظ هذا النوع من NAT على فضاء عناوين IP، لأنك تحتاج إلى عدد عناوين مسجَّلة يساوي عدد العناوين غير المسجَّلة، كما هو مبيّن في الشكل (6.8). يعتبر NAT الساكن ليس آمناً كبقية أنواع NAT لأن كل حاسوب مقترن بشكل دائم بأحد العناوين المسجَّلة، مما يمكن مخترقي الانترنت من توجيه حركة المرور إلى حاسوب معيّن في شبكتك باستعمال ذلك العنوان المسجَّل.



الشكل (6.8): NAT الساكن.

يقوم الموجه بترجمة كل عنوان خاص إلى عنوان عام، وبالتالي يحتاج كل جهاز بالشبكة الداخلية إلى عنوان عام خاص به للاتصال بالشبكة الخارجية أي الانترنت. ويتم إسناد كل عنوان خاص إلى عنوان عام بغض النظر إذا قام الجهاز صاحب العنوان الخاص بالولوج للانترنت أم لا، لذلك لا تخلو هذه الطريقة من السلبيات.

على اعتبار أن مزود الخدمة قام بحجز عناوين الشبكة 200.1.1.0 من النوع العام. لذلك كل جهاز يتصل من الشبكة الداخلية إلى الشبكة الخارجية يجب أن يحجز عنوان ثابت من الشبكة 200.1.1.0 ليتمكن من الاتصال بالانترنت. سنقوم بحجز العنوان 200.1.1.1 من اجل الجهاز 10.1.1.1 والعنوان 200.1.1.2 من أجل الجهاز 10.1.1.2، وهكذا... إذن فمن أجل جميع الحزم القادمة من الجهاز 10.1.1.1 يقوم الموجه بتغير قيمة عنوان IP المصدر فيها إلى 200.1.1.1. عند رجوع الحزم إلى هذا الجهاز يقوم بإعادة العنوان إلى 10.1.1.1، كما في الشكل (7.8):



Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Private Address	Public Address
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

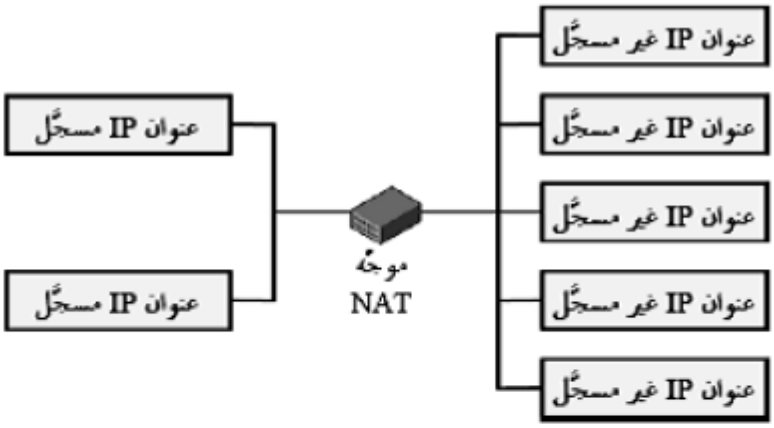
الشكل (7.8): مثال عن NAT الساكن.

2- NAT المتغير (Dynamic NAT):

يُستعمل NAT المتغير إذا كان عدد العناوين IP المسجَّلة لديك أقل من عدد الحواسيب غير المسجَّلة، كما هو مبيّن في الشكل (8.8).

يترجم NAT المتغير كل عنوان غير مسجَّل إلى أحد العناوين المسجَّلة المتوفرة، لأن العنوان المسجَّل المعيّن لكل عميل يتغيّر كثيراً، مما يصعّب على المخترقين ربط عنوان مسجَّل بحاسوب معيّن، كما يحصل في NAT الساكن.

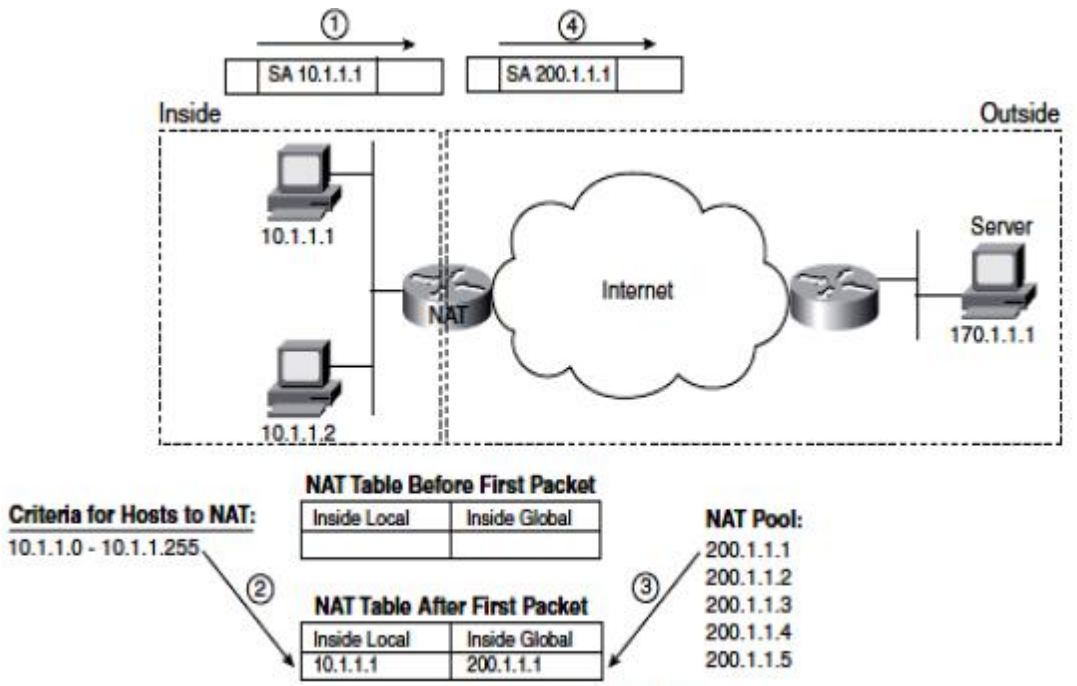
العائق الرئيسي في NAT المتغير هو أنه يمكنه أن يدعم فقط نفس عدد المستخدمين المتزامنين كعدد عناوين IP المسجَّلة المتوفرة. إذا كانت كل العناوين المسجَّلة قيد الاستعمال، سيتلقى العميل الذي يحاول الوصول إلى الانترنت رسالة خطأ.



الشكل (8.8): NAT المتغير.

تعاني الطريقة المتغيرة من سلبية وهي أن عدد الأجهزة الداخلية المتصلة بالانترنت يساوي عدد العناوين العامة، وهي نفسها الموجودة بالطريقة الساكنة. لكنها تتميز بايجابية وهي أن أي جهاز من الشبكة الداخلية الذي قد حجز عنوان خارجي للاتصال بالانترنت سيقوم بتحريره ليتمكن جهاز أخر من استخدامه لاحقاً، أي أن الربط بين العناوين الخاصة والعامة يكون متغيراً بحيث كل أجهزة الشبكة يكون لديها فرصة للاتصال بالانترنت وفق الشكل (9.8).

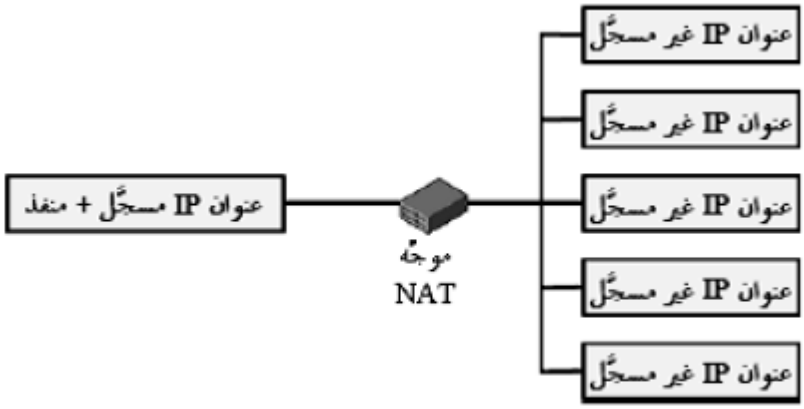
تقوم الطريقة المتغيرة على تشكيل قائمة من العناوين العامة المتاحة على الموجه NAT أو ما يسمى حوض NAT (NAT Pool). كل جهاز يريد الاتصال بالانترنت يحجز أحد عناوين القائمة حتى تنتهي هذه العناوين، ويبقى الجهاز بالشبكة الداخلية يحجز عنوان الانترنت طالما يقوم بإرسال واستقبال بيانات من وإلى الانترنت، أو يستطيع مدير الشبكة تحديد زمن معين لكل جهاز وبعد انتهاء الزمن يقوم الجهاز بتحرير العنوان الذي حجزه. نستطيع كذلك بشكل يدوي استخدام بعض الأوامر لجعل جهاز أو جميع الأجهزة الداخلية تحرر العناوين التي حجزتها.



الشكل (9.8): مثال عن NAT المتغير.

3- ترجمة عنوان المنفذ (Port Address Translation: PAT):

ترجمة عنوان المنفذ والمعروف أيضاً ترجمة العناوين بطريقة التحميل الزائد (Overloading NAT)، يترجم كل العناوين IP غير المسجَّلة في شبكتك باستعمال عنوان IP مسجَّل واحد، كما هو مبيّن في الشكل (10.8). يستعمل موجّه NAT أرقام المنافذ ليميّز بين الحزم التي تولّدها حواسيب وتذهب إلى حواسيب أخرى، لكي يتمكن عدة عملاء من الوصول إلى الانترنت في الوقت نفسه. يزوّد NAT التحميل الزائد أفضل أمان بين أنواع NAT لأن الربط بين العميل غير المسجَّل والتركيبة المكونة من العنوان IP المسجَّل مع رقم المنفذ في موجّه NAT يدوم لاتصال واحد فقط.



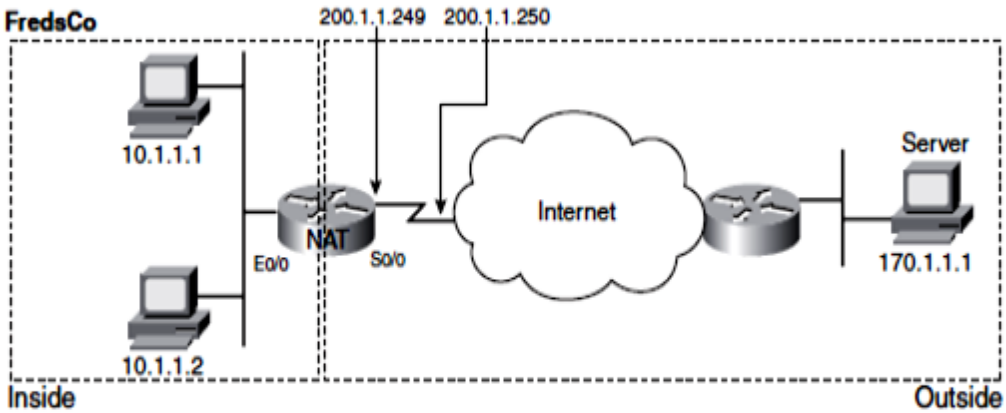
الشكل (10.8): ترجمة عنوان المنفذ.

مر معنا أنه في الطريقة الساكنة والطريقة المتغيرة نحتاج لعناوين انترنت عامة بعدد الأجهزة المراد وصولها إلى الانترنت، وبالتالي فإنه في الشبكات الكبيرة نحتاج لعدد كبير من عناوين الانترنت. لو أخذنا بعين الاعتبار الأجهزة الموجودة في العالم التي تتصل بالانترنت، لأدركنا أنه من الممكن أن تستنفذ عناوين الانترنت خلال سنوات قليلة من البدء باستخدامها. لذلك كان لابد من طريقة تستطيع بواسطتها مجموعة من الأجهزة الداخلية التي تستخدم عنوان عام واحد للوصول إلى الانترنت، تسمى هذه الطريقة PAT.

في الشكل (11.8) نلاحظ أن الجهاز 10.1.1.1 عمل اتصالين بنفس الوقت، والجهاز 10.1.1.2 عمل اتصال واحد. جميع الاتصالات استخدمت نفس العنوان العام، وهذا العنوان هو 200.1.1.249. ولكن السؤال هنا عندما يقوم الجهاز 170.1.1.1 بالرد على الجهاز 10.1.1.2 مثلاً، كيف يستطيع الموجه معرفة الجهاز الذي سيقوم باستقبال حزم البيانات؟

الجواب يكون عندما يقوم الموجه بترجمة الحزم القادمة إلى عنوان واحد فان هذا الموجه يقوم أيضا بترجمة رقم المنفذ المصدر (Source Port Number)، بحيث أن جميع الاتصالات وإن استخدمت نفس عنوان الانترنت العام فإنها من المستحيل أن تستخدم نفس رقم المنفذ.

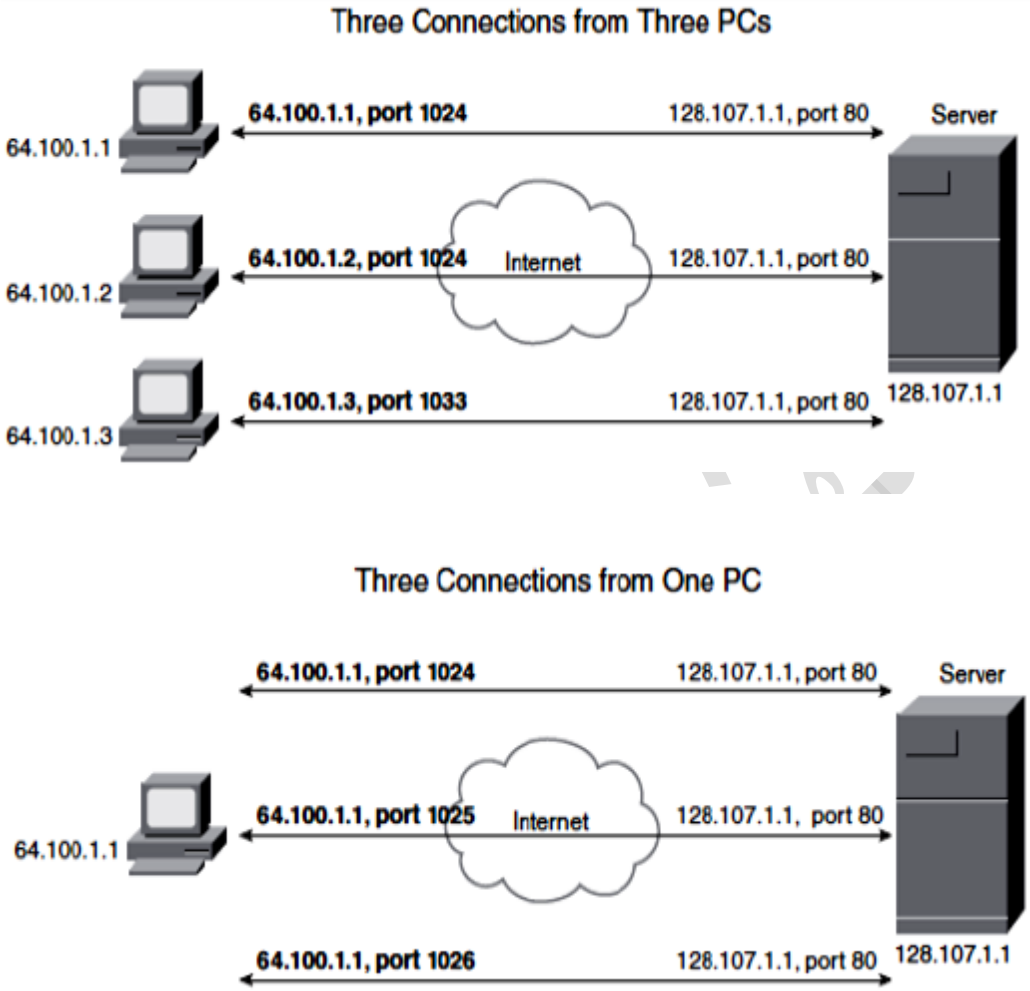
Registered Subnet: 200.1.1.248, Mask 255.255.255.252



Inside Local	Inside Global
10.1.1.1:3212	200.1.1.249:3212
10.1.1.1:3213	200.1.1.249:3213
10.1.1.2:38913	200.1.1.249:38913

الشكل (11.8): مثال عن ترجمة عنوان المنفذ.

لفهم PAT اليك المثال التالي المبين بالشكل (12.8)



الشكل (12.8): توضيح مفهوم PAT.

يظهر الجزء الأعلى من الشكل (12.8) شبكة بثلاثة أجهزة مضيفة متصلة بمخدم ويب باستخدام برتوكول TCP، والجزء السفلي من الشكل يظهر نفس الشبكة الخاصة بثلاث اتصالات TCP من زبون واحد. كما أن الاتصالات الستة تتصل بعنوان IP المخدم 128.107.1.1 والمنفذ 80 -المنفذ المعروف لخدمات الويب-. وفي كل حالة فإن المخدم قادر على أن يميز بين الاتصالات المتنوعة لأن لكل منها تكوين فريد من عنوان IP مع رقم المنفذ. كما أن PAT تستفيد من حقيقة أن المخدم لايهتم فعلياً إذا كان له اتصال وحيد لكل من الأجهزة المضيفة الثلاثة أو ثلاثة اتصالات لعنوان IP لجهاز مضيف وحيد، لذلك ولدعم الكثير من الأجهزة المضيفة المحلية باستخدام عنوان عام مفرد على الموجه، حيث يترجم PAT العناوين الخاصة للأجهزة المضيفة إلى عنوان IP عام، كما أن الموجه يبقي المسار إلى عنوان IP ورقم منفذ TCP أو UDP.

أنواع الهجمات في الشبكات

هناك عدة أنواع من الهجمات أهمها:

أولاً : هجمات تخمين كلمة المرور

تحدث هجمات تخمين كلمة المرور عندما يتم مهاجمة حساب (account) بشكل متكرر ... وتتم هذه الهجمات عن طريق إرسال كلمات المرور المحتملة إلى الحساب (account) بطريقة منتظمة.

تنفذ هذه الهجمات لغرض الحصول على كلمات المرور لاستخدامها فى (الوصول – التعديل) .

هناك نوعان من هجمات تخمين كلمة المرور وهما: (الهجوم العنيف – هجوم القاموس) .

1- الهجوم العنيف (Brute-force attack):

هى محاولة لتخمين كل احتمالات كلمات المرور حتى يحدث التخمين الناجح . عادة ما يستغرق هذا النوع من الهجوم فترات طويلة.

لجعل كلمات المرور أثر صعوبة فى التخمين ... (لا تقل عن ستة أحرف – مركبة – هناك سياسة لغلق وتغيير كلمات المرور).

2- هجوم القاموس (Dictionary attack):

يقوم هذا النوع من الهجمات باستخدام قاموس من الكلمات الشائعة لمحاولة لإيجاد كلمة المرور الخاصة بالمستخدم .

نصائح عامة :

- إعطاء المهاجم فكرة عن اسم المستخدم الصحيح تعتبر فكرة ليست جيدة، وبالتالي يجب بمجرد أن تقوم بتحميل نظام تشغيل Windows جديد أن تقوم بـ (تغيير اسم حساب الـ Administrator - تعطيل حساب Guest)
- ضبط نظام التوثيق (Authentication) الخاص بك بحيث يقوم بـ (إعادة عملية الاتصال كاملة من البداية فى حالة إدخال كلمة مرور خاطئة – يقبل عدد معين من كلمات المرور الخطأ وبعدها يتوقف عن العمل).

ماذا عن هجوم جدول قوس قزح (Rainbow Table)

جدول قوس قزح هو جدول محسوب مسبقاً لعكس تشفير خوارزميات Hash كخوارزمية MD5، ويستخدم لكسر كلمات المرور المشفرة بتلك الخوارزميات.

ثانياً : هجمات الخداع (Spoofing Attacks)

هجمات الخداع (Spoofing) هي محاولة من قبل (شخص ما – شيء ما) للتنكر كشخص آخر ... حيث يحاولون خداع (النظام – المضيف) ليعتقد أنه شخص آخر. وهذا النوع من الهجمات يعتبر عادة هجمات بهدف الوصول .

أكثر هجمات الخداع الشهيرة اليوم هي هجمات (IP spoofing - DNS spoofing)

1- هجمات انتحال IP (IP Spoofing):

في حالة هجمات IP spoofing ... يكون الهدف هو محاولة أن تجعل البيانات تبدو كأنها أتت من host موثوق فيه ... مع أنها ليست كذلك ... (حيث يتم الغش فى عنوان IP الخاصة بالـ Host الذي يقوم بالإرسال .

2- هجمات انتحال DNS (DNS Spoofing):

في حالة هجمات الـ DNS spoofing ... فإن DNS Server يعطى معلومات حول اسم السيرفر الذي يعتقد أنه شرعي ... ولكنه ليس كذلك.

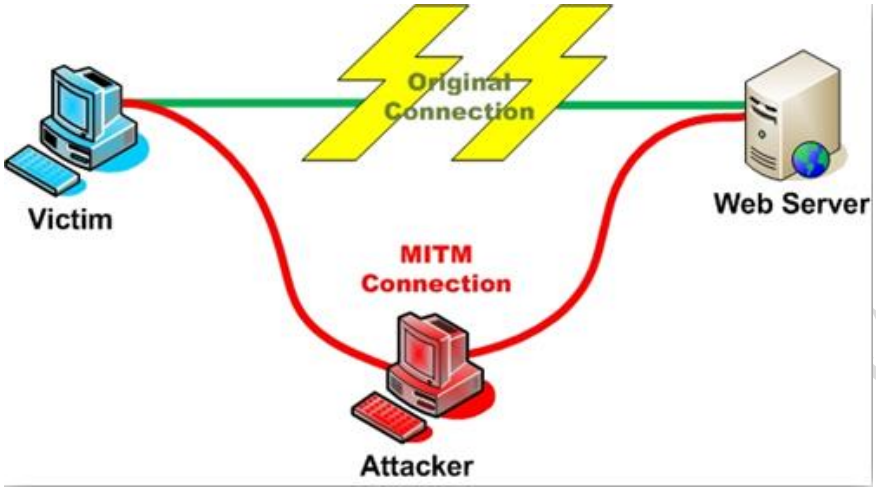
• وبنجاح هذه الهجمة فإنه يمكن أن يتم ارسال المستخدمين إلى مواقع غير التي يرغبون فيها – إعادة توجيه البريد الإلكترونى – عمل أي نوع آخر من عمليات التوجيه للبيانات عن طريق DNS Server الذي يستخدم لتحديد الاتجاه).

ثالثاً : هجمات " رجل في المنتصف " (Man-in-the-Middle)

هجمات " رجل في المنتصف " يشهد لها بأنها (محترفة - متطورة جداً) وهذا النوع من الهجمات يعتبر عادة هجمات وصول ... ولكنه يمكن أن يستخدم كنقطة بداية لهجمات التعديل .

يقوم هذا النوع من الهجمات على فكرة " وضع برنامج بين المستخدم و السيرفر بدون أن يتسبب هذا البرنامج في أي أخطاء أو أعطال على الشبكة ... هذا البرنامج يقوم بتسجيل معلومات المستخدم لغرض (النظر إليها لاحقاً – وربما تعديلها لاختراق أمن النظام).

الشكل التالي يمثل هجوم " رجل فى المنتصف " .



لاحظ أن كل من السيرفر – الزبون يفترض أنه يتعامل مع النظام الشرعى ... حيث أن " رجل في المنتصف " يبدو للسيرفر كأنه هو الزبون ... ويبدو للزبون كأنه هو السيرفر .

هجمات " رجل فى المنتصف " والشبكات اللاسلكية : فى السنوات الأخيرة زادت هجمات " رجل في المنتصف " على الشبكات اللاسلكية ... حيث أنه لم يعد من الضروري الاتصال من خلال الأسلاك ... حيث أن المهاجم يمكن أن يكون خارج المنزل أو المكتب (يعترض حزم البيانات – يعدلها – يرسلها) .

المهندس باسل دهيمش

المناطق معزولة السلاح[3] (Demilitarized Zone: DMZ)

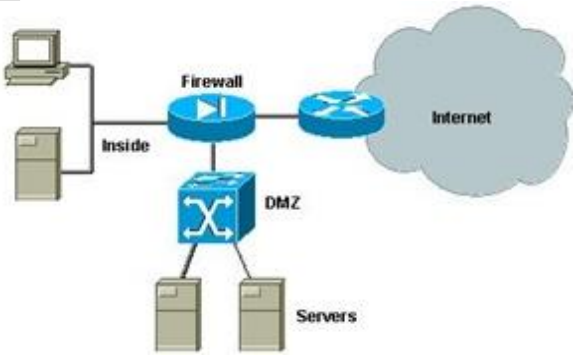
إذا كنت تستخدم الانترنت لأي فترة من الزمن ، وخاصة إذا كنت تعمل في شركة كبيرة وتصفح الويب أثناء وجودك في العمل، وربما كنت قد سمعت مصطلح يستخدم جدار الحماية. على سبيل المثال ، غالبا ما تسمع أحد الموظفين في شركة يقول: **"لا يمكنني استخدام هذا الموقع لأنهم لم يسمحوا له من خلال جدار الحماية"**.

وجدار الحماية هو حاجز للحفاظ على القوى المدمرة مثل المخترقين والفيروسات والديدان الخ... بعيدا عن الممتلكات الخاصة بك .في الواقع ، هذا هو السبب الذي يطلق عليه جدار حماية .وظيفتها تشبه جدار حماية المادية التي يحفظ النار من الانتشار من منطقة إلى أخرى . جدار النار هو مجرد برنامج أو جهاز أو أجهزة تقوم بتصفية المعلومات القادمة من خلال اتصال الإنترنت في شبكة الاتصال الخاصة بك أو نظام الكمبيوتر.

DMZ

ما هي DMZ في أمن شبكات الحاسوب؟ DMZ، المنطقة المجردة من السلاح أو المنطقة المحايدة وتكون مفصولة عن الانترنت عبر جدار نار خارجي، وأيضاً تكون مفصولة عن الشبكة المحلية الداخلية عبر نفس جدار النار أو جدار آخر مختلف. و يتم اللجوء لحل DMZ عند الحاجة لتمكين المستخدمين في الشبكة الخارجية من الوصول إلى بعض الخدمات المحلية مثل Web Server أو .FTP فبدلاً من توفيرها ضمن مجال الشبكة الداخلية بما يشكّله هذا من تعريض الشبكة لخطر الاختراق أو الهجمات، يتم وضع هذه الخدمات ضمن شبكة ثالثة منفصلة عن الشبكة الداخلية. وبذلك تتحقق إمكانية العزل عن الأخطار التي يمكن أن تشكّلها الإنترنت، مع إمكانية توفير الخدمات اللازمة للخارج.

إذاً: المنطقة منزوعة السلاح هي واحدة من هذه المناطق الشبكية والتي تستخدم لتقليل الأخطار المحتملة على شبكة المنظمة الخاصة من الاتصالات غير المسموحة والقادمة من الشبكة العالمية وبالتالي تمنع إمكانية تسرب بيانات المنظمة السريّة. انظر الشكل (1) والذي يوضح فصل المنطقة المحايدة عبر جدار ناري واحد.



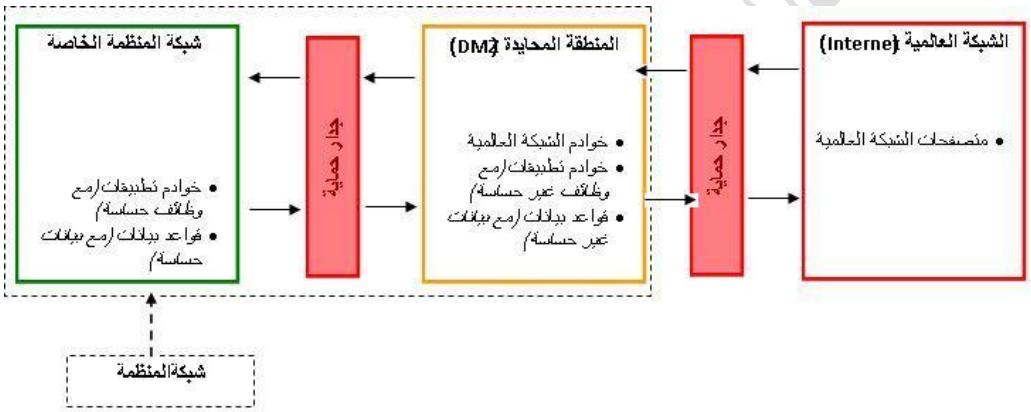
[3] تسمى المنطقة المعزولة من السلاح بالمنطقة المحايدة أيضاً.

الشكل (1)

يوضح الشكل (2) أن بإمكان مستخدمي الشبكة العالمية من الاتصال بالمنطقة المحايدة لشبكة المنظمة لكن ليس بإمكانهم الدخول إلى شبكة المنظمة الخاصة.

في الشكل (2) أيضاً نرى جداريين ناريين، الهدف من الجدار الناري الأول بين الشبكة العالمية والمنطقة المحايدة من شبكة المنظمة هو حماية المخدمات الموجودة في المنطقة المحايدة - والتي بطبيعتها لابد أن تكون مرئية للعالم - من الهجمات عن طريق الشبكة العالمية، وهذه الحماية بناءً على التصفية كالسماح لبروتوكلات معينة بالمرور مثل (HTTP, HTTPS للسماح بالوصول لمخدات الويب مثلاً) ومنع البرتوكولات الأخرى حسب الحاجة.

والهدف من الجدار الناري الثاني بين المنطقة المحايدة والمنطقة الخاصة من شبكة المنظمة هو تزويد حاجز أمني مقوى لحماية المنطقة الخاصة، وأيضا كما في الجدار الثاني هذه الحماية بناءا على التصفية كالسماح لبروتوكولات معينة بالمرور مثل و يجب أن تكون التصفية في هذا الجدار الناري مقيدة أكثر من الجدار الناري الأول، ففي حالة اختراق الجدار الناري الأول فإن احتمالية اختراق الجدار الناري الثاني أقل.



الشكل (2)

المخدمات التي من الممكن وضعها في DMZ:

بشكل عام أفضل مكان للمخدمات وقواعد البيانات المعدة للتعامل مع الشبكة العالمية هو منطقة الشبكة المنزوعة السلاح، ومن الأمثلة على هذه المخدمات التالي:

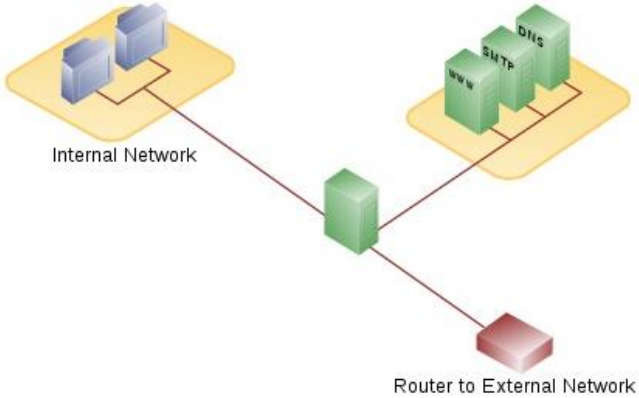
- مخدمات الشبكة العالمية (Web Servers)
- مخدمات بروتوكول نقل الملفات (FTP Servers)
- مخدمات الاتصال البعيد
- مخدمات البريد الإلكتروني.
- مخدمات VoIP

معمارية DMZ

هناك العديد من الطرق المختلفة لتصميم الشبكة مع المنطقة المجردة من السلاح يوجد اثنين من أكثر الوسائل الأساسية مع الجدار الأحادي والمعروفة أيضا باسم نموذج ثلاثي الأرجل .

1- جدار النار الأحادي:

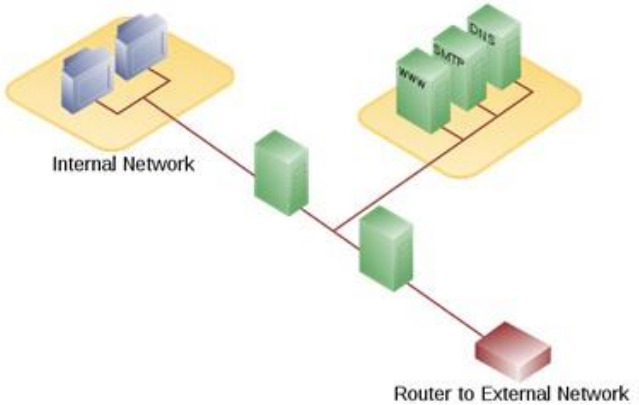
ويمكن استخدام جدار حماية الأحادي ثلاثة مداخل في شبكة DMZ.و يتم تشكيل شبكة خارجية من ISP إلى جدار الحماية على المدخل الشبكة الأولى ، يتم تشكيل شبكة داخلية الى مدخل الشبكة الثانية ، ويتكون من المنطقة المجردة من السلاح واجهة او المدخل الشبكة الثالثة. جدار الحماية يصبح نقطة واحدة للخطر والفشل للشبكة ويجب أن يكون قادر على التعامل مع كل الطرق الذاهبة إلى المنطقة المجردة من السلاح، فضلا عن شبكة الاتصال الداخلية. انظر الشكل (3)



الشكل (3)

2- الجدار المزدوج :

النهج الأكثر أمنا وهو استخدام اثنين من جدران الحماية لإنشاء المنطقة المجردة من السلاح. يجب أن يتم تكوين جدار الحماية الأول (الذي يسمى أيضا "المنطقة الأمامية" لجدار حماية) بالسماح لحركة المرور المتجهة إلى المنطقة المجردة من السلاح فقط. وجدار الحماية الثانية (وتسمى أيضا "المنطقة الخلفية" لجدار حماية) يسمح المرور فقط من المنطقة المجردة من السلاح على الشبكة الداخلية ويمكن الاستفادة من هذه الطريقة كالتالي اذا احد قام باختراق جدار النار الأول المنطقة الأمامية فإنه يحتاج إلى وقت لكي يكسر الجدار النار الثاني .

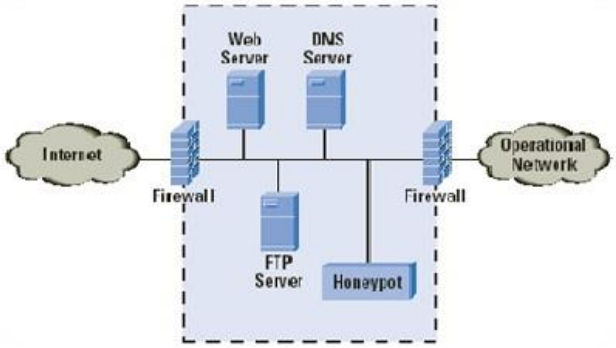


الشكل (4)

أوعية العسل (honey pots):

هي تقنية تستخدم في المناطق المحايدة لإبعاد الاختراقات المحتملة على شبكة المنظمة، و هي عبارة عن مخدمات مزودة ببرامج و بيانات تظهر و كأنها موثوقة و صحيحة لتوجيه أنظار المخترقين إليها و صرفهم عن المخدمات الحقيقية.

فائدة أخرى من هذه التقنية ألا وهي إعطاء انطباع عن أساليب المخترقين للاستفادة منها في صد هجماتهم وتطوير أنظمة الحماية. لكن عدم تجهيز هذه التقنية بالشكل الصحيح قد يشكل خطراً على شبكة المنظمة!. يوضح الشكل (5) توضع أوعية العسل بداخل المنطقة معزولة السلاح.



الشكل (5)

المهندس باسل دهيمش