وزارة التعليم العالي والبحث العلمي

جامعة الفرات الاوسط

المعهد التقني /السماوة

قسم تكنولوجيا المعلومات والاتصالات

مدرس المادة :م.م بيداء هادي محمد سعودي

المحاضرة الخامسة

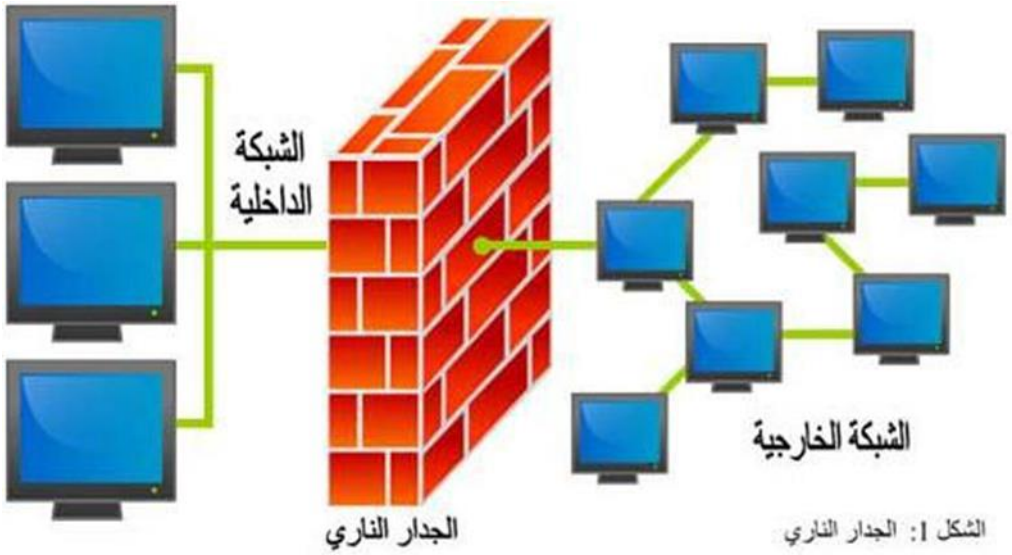
أمنية الحاسبات والبيانات

COMPUTER & DATASECURITY

ما هو الجدار الناري ؟

الجدار الناري هو مجموعة من الاجراءات المتكاملة والمصممة لمنع الوصول الالكتروني الغير معتمد(unauthorized electronic access) إلى شبكة الحاسب .وعادةً ما يكون جهاز أو مجموعة أجهزة تم إعدادها بعدد من العمليات مثل :السماح (permit)و الرفض(deny)والتشفير(encrypt)وفك التشفير (decrypt)أو أعدت لتكون وكيل Proxy ((للتحكم في مرور البيانات بناءا على مجموعة من القيود والمعايير.

إن الوظيفة الاساسية للجدار الناري هو تنظيم تدفق البيانات بين شبكات الحاسب المتفاوتة في مستويات الثقة ، حيث إن شبكة الإنترنت بشكل عام تعتبر معدومة الثقة (zone with no trust) فيتم ربطها بشبكة داخلية والتي هي تتمتع بمستوى عالٍ في الثقة .وعادة ما يكون بين الشبكتين منطقة تكون متوسطة الثقة وتسمى المنطقة المحايدة (Demilitarized zone) (DMZ)



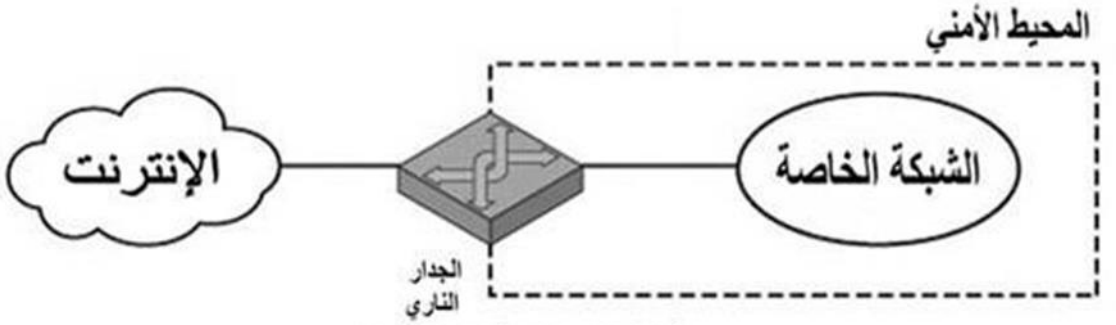
الشكل 1: الجدار الناري

أهداف الجدار الناري:

أن جميع مرور البيانات من الداخل إلى الخارج والعكس يجب أن يمر من خلال الجدار الناري ، ولن يتم تحقيق هذا الهدف إال بوجود حاجز فيزيائي وهو الجدار الناري Firewall (بين الشبكة الداخلية مع العالم الخارجي) .يسمح فقط لمرور البيانات المصرح بها والتي تكون قد عرفت مسبقاً من خلال سياسة الامن المحلية ، ولذلك أوجدت عدة أنواع من الجدار الناري مستخدمة الآن والتي كل منها يلبي سياسات معينة تفرضها الشركة أو المؤسسة.
بما أن الجدار الناري سيكون هو البوابة على العالم الخارجي فيجب أن يكون لديه مناعة عالية عن الاختراق ، وعادة ما يستخدم نظام تشغيل موثوق وآمن

أنواع الجدار الناري :

اولا: تصفية حزم البيانات Network Layer Firewall أو Packet filters



الشكل 2: تصفية حزم البيانات

يكون عمل تصفية حزم اليبانات (Packet filters)بفحص حزمة البيانات فإذا تطابقت مع مجموعة قوانين والتي تكون عادةً مخزنة في الجدار الناري "فإنها تهمل من دون أن تعلم المرسل بذلك" .
إن هذا النوع من الجدار الناري يقوم بالتصفية بناءاً على المعلومات المخزنة داخل حزمة البيانات نفسها (Packet)وغالباً ما تكون هذا المعلومات مركبة من عدة متغيرات وهي :

- عنوان المرسل Source IP address .
- العنوان المرسل إليه Destination IP address .
- نوع بروتوكل الآلي بيIP protocol field
- عنوان المرسل والمستقبل على مستوى طبقة النقل

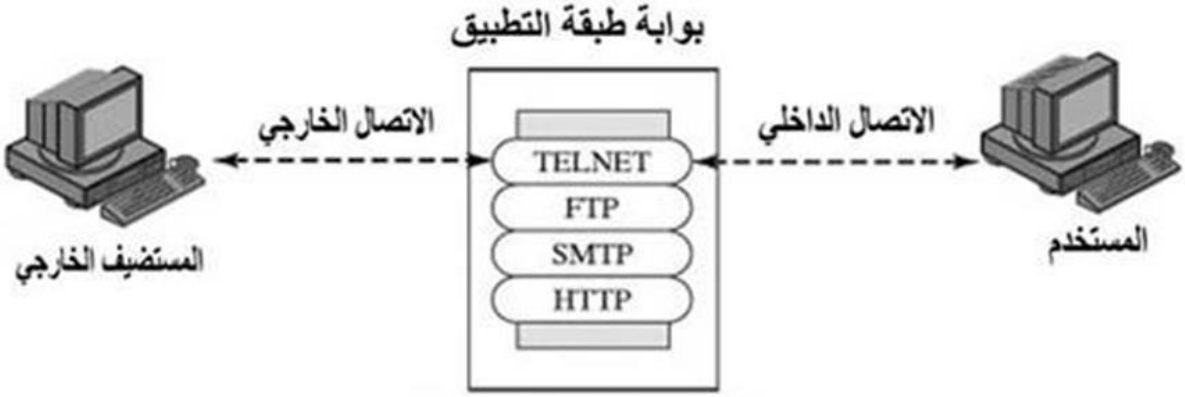
transport-level Source and destination address(:والمقصود رقم المنفذ port number(والتي تعرف نوع التطبيق مثل SNMP or TELNET.
الوصلة Interface :وغالباً نحتاج هذا الحقل في الموجهات Routersحيث يكون لدينا العديد من وصالت RJ-45وكذلك R232، والبد من حفظ الوصلة التي ذهبت منها الحزمة والوصلة التي وصلت إليها ، ويتم التعرف على ذلك من خلال العنوان الفيزيائي MAC addressلكل منهما .

إحدى الصفات الإيجابية لهذا النوع هو بساطته وسرعته ولكن هناك بعض نقاط الضعف أهمها :
1-أن هذا النوع لايفحص أعلى طبقة وهي طبقة البيانات وذلك هو غير قادر على منع الهجمات الصادرة من تلك الطبقة ، حيث لا يمكنك منع المستخدم من تنفيذ أمر معين قد تم إساءة استخدامه .
2-أنه عرضة لاحدى أشهر الهجمات وهو استخدام عنوان الشبكة المزيف IP address spoofingحيث

3- يمكن للدخيل Intruderيرسل حزمة بيانات Packetمن الخارج ولكن عنوان المصدر IP Source addressيحتوي على مضيف داخلي Internal hostمما يجعله يستطيع المرور من خلال القوانين المكتوبة في الجدار الناري .

4- بسبب قلة المتغيرات المتاحة لفرض القوانين عليها ، فإنها عرضة للتحايل وذلك باستغلال الإعدادات الخاطئة للجداري الناري .يمعنى آخر ، سهولة الوقوع في الأخطاء العرضية لدى المسئول عن الجدار الناري ،مما يساعد الدخيل Intruderعلى استغلال هذه الأخطاء البسيطة .

ثانياً :بوابة طبقة التطبيق "Application Layer Gateway "ALG وأيضاً يسمى الخادم الوكيل Proxy server:



الشكل 3: بوابة طبقة التطبيق

وهو يمثل تبادل البيانات على مستوى التطبيقات application-level . يتصل المستخدم بالبوابة gatewayباستخدام أي تطبيق من TCP/IP applicationمثل Telnetأو FTP .ثم تسأل البوابة gatewayالمستخدم عن اسم المضيف البعيد remote hostليتم الدخول عليه.

عندما يدخل المستخدم اسم صحيح ويتم التحقق منها فإن البوابة gatewayتتصل مع التطبيق الموجود المضيف البعيد remote hostويتم تبادل البيانات .

الإيجابيات :

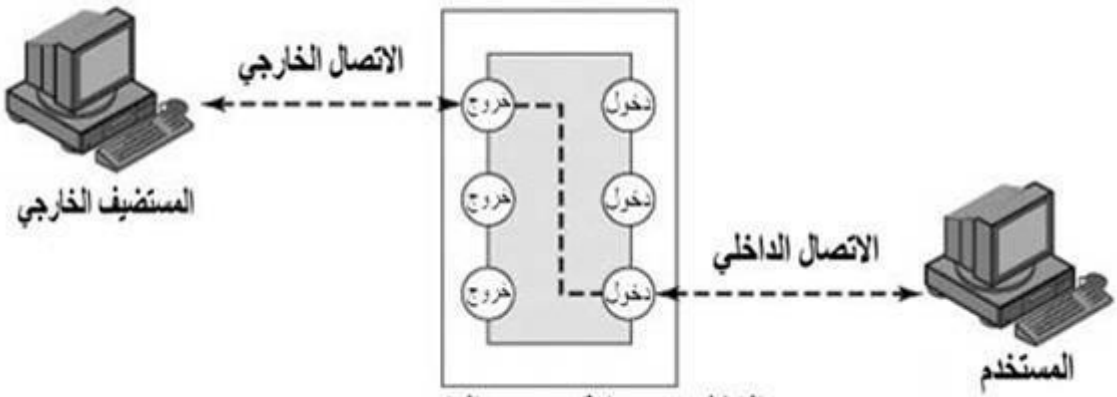
- **السماح لتطبيقات العميل applications clientباستخدام منافذ TCP/ UDPوقتية أو عابرة للتواصل مع منافذ معروفة known ports المستخدمة من قبل تطبيقات الخادم server applicationsحتى لو أن إعدادات الجدار الناري firewall-configurationفقط تسمح بعدد محدود من المنافذ .ولذلك فإن من دون وجود بوابة طبقة التطبيق ALGفإن المنافذ التي استخدمها العميل ستكون مغلقة ، والا فإن على مسؤول الشبكة أن يفتح عدد كبير من المنافذ مما يؤدي إلى زيادة الثغرات على الشبكة من خلال هذه المنافذ.**
- **ذكرنا سابقاً أن هناك أوامر في طبقة التطبيق قد يساء إستخدامها والتي لايستطيع النوع الأول Packet filterكشفها ، ولكن هنا في هذا النوع ALGيستطيع التعرف على هذه الأوامر مما يمنح المسئول السيطرة على هذا النوع من المخاطر .**
- **التزامن بين فترات التعامل مع البيانات sessionsبين المضيفين أثناء تبادل البيانات بينهما .ومثال ذلك : تطبيق FTPيستخدم عدة اتصالات منفصلة عن بعضها للتحكم في تمرير الأوامر لتبادل البيانات بين العميل**

وبين الخادم البعيد .وعندما يرسل العميل ملف كبير فإن احد تلك الاتصالات للـ FTPتكون عاطلة عن العمل وهو اتصال التحكم control connection the. ,ولذلك فإن بوابة طبقة التطبيق ALGتستطيع منع هذا الاتصال من أن يحصل له انتهاء في المدة Tim outقبل أن إكتمال إرسال الملف .

أهم سلبية لهذا النوع :

بسبب المرور المتكرر في كل تطبيق على ALGفإن هذا يسبب تدهور في الأداء على عكس النوع الآخر Packet filterميزة السرعة .

ثالثا:بوابة مستوى الدارة (circuit-level gateway)



الشكل 4: بوابة مستوى الدائرة

هذا النوع ممكن أن يكون نظام مستقل stand-alone system أو يكون على شكل دالة function تنفذ بواسطة بوابة طبقة التطبيق ALG لتطبيقات محددة .

إن هذا النوع من الجدار الناري لا يسمح باتصالات TCP والتي تكون تسمى end-to-end TCP؛ connection وبدلا من ذلك ، فإن البوابة تبدأ باتصالين : TCP

الأول: يكون بين البوابة نفسها وبين مستخدم الـ TCP على المضيف الداخلي an inner host ، والآخر .

الثاني: بين البوابة نفسها وبين مستخدم الـ TCP على المضيف الخارجي.

عندما يؤسس الاتصالين فإنه يتم تبادل البيانات (TCP segment وهي وحدة البيانات على طبقة النقل) Transport Layer عن طريق البوابة من اتصال إلى آخر من دون فحص المحتوى . والوظيفة الأمنية في هذا النوع هي السماح أو المنع الاتصال معين .

إن الاستخدام الأمثل لهذا النوع هو في حالة أن مسئول النظام system administrator يثق بمستخدمين داخليين .

ولذلك فإنه من الممكن إعداد البوابة Gateway ألن تكون نوعين معاً:

الأول: ALG للاتصالات المتجهة للداخل . inbound connections

الثاني: circuit-level للاتصالات المتجهة للخارج . outbound connections

بهذه الطريقة، فإن البوابة تتحمل تكلفة معالجة البيانات المتجهة للداخل حتى لو تكون البيانات أو الأوامر المطلوبة ممنوعة ، ولكن الال تحمل تكلفة البيانات المتجهة للخارج.

Firewalls limitations محدودية استعمال الجدار الناري

هناك مخاطر لا يستطيع الجدار الناري منعها منها :

- **أن الجدار الناري لا يمكنه حماية المخاطر الداخلية والتي تكون من مخترق موجود في داخل الشبكة وهذا المخترق قد يكون موظف ساخط عن العمل ويملك حساب خاص ومصرح له أن يعمل به فيستغله ، أو قد تكون المشكلة من خلال برنامج يكون مخفي خلال عمل تحميل برنامج آخر بواسطة الـ CD أو تحميله من الإنترنت .**
- **لكل جدار ناري ثغرات ولذلك يبقى ان الوضع ليس آمناً تماماً.**