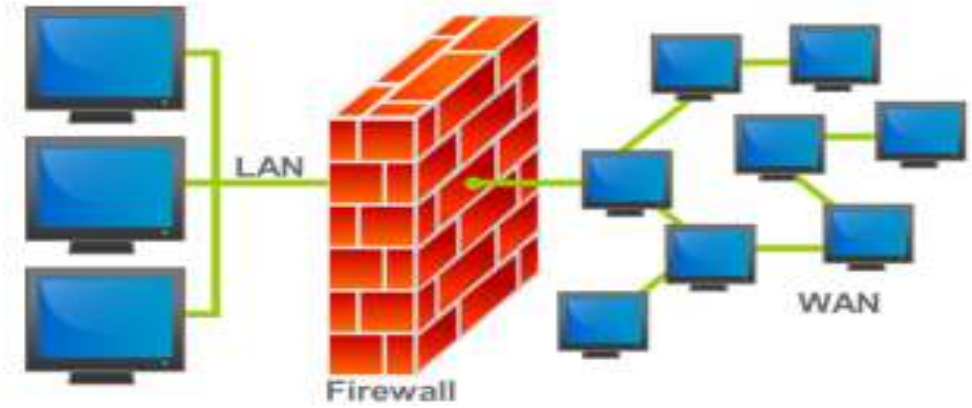
Firewall
الجدار الناري

م . إناس عدي

الجدار الناري : Firewall



هو عبارة عن برنامج أو جهاز يقوم على حماية جهاز الحاسوب أثناء اتصاله بشبكة الإنترنت من المخاطر، حيث يتولى جدار الحماية فحص كل المعلومات والبيانات الواردة من الإنترنت، أو من أي شبكة أخرى، ثم بعد ذلك يقوم بالسماح لها بالمرور والدخول إلى جهاز الحاسوب، إذا كانت متوافقة مع إعدادات جدار الحماية، أو يقوم باستبعادها وطردها إذا من البرامج الخبيثة ، مثل: الفيروسات، وبرامج التجسس، أو إذا كانت غير متوافقة مع إعدادات جدار الحماية، فجدار الحماية هو عبارة عن حد فاصل بين جهاز الحاسوب وشبكة الإنترنت. ويمكن أن نشبه جدار الحماية بنقاط التفتيش أو المراكز الحدودية في الدول الحديثة .

أهمية جدار الحماية

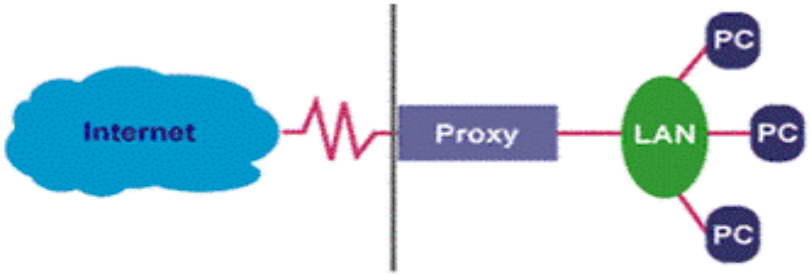
يعتبر جدار الحماية أحد أهم الخطوات التي يجب اتخاذها في سبيل حماية الحاسوب من الاختراق من قبل المتطفلين والبرامج الخبيثة، فمن المعروف أن شبكة الإنترنت غير آمنة، وأنها مليئة بالمخاطر الأمنية، فيجب على المستخدم لهذه الشبكة أن يكون حريصًا على سلامة جهازه أثناء اتصاله بالإنترنت

أشكال الجدار الناري:

1 - (stateless) packet filters:

- ✓ يعمل في الطبقة الثالثة ،لا يسمح لحزم البيانات بالعبور إلا أذا كانت مطابقة للقوانين المحددة له مسبقاً.يحدد هذه القوانين مدير الجدار الناري وإذا لم تحدد فأن القواعد الافتراضية سوف تطبق.
- ✓ لا يقوم بتخزين معلومات عن حالة الاتصال وبالتالي لا يهتم بمعرفة ان هذا ال packet مرسلة من المصدر مباشرة ولم يتم التلاعب بها وتغيرها .

: Proxies filters -2



Proxy Firewall Example

تعمل على جهاز مخصص أو كبرنامج مثبت على جهاز للأغراض العامة, البروكسي هو بوابه (Gateway)من شبكة لآخري لتطبيق معين في الشبكة .(specific network application)

كما يجب أن نعلم أن جميع الطلبات يجب أن تمر عبر خادم البروكسي.

كمثال لو أراد مدير البروكسي بمنع أي موقع يحمل في محتواه كلمه (تحميل), الآن الطلب سوف يمر عبر خادم البروكسي تأتي وظيفة البروكسي ليعمل كمفلتر فيقوم بقراءة محتوى الحزم ويحدد أن كانت سوف تمر أم لا بناءً على القوانين التي تم تحديدها له.

3- Host Based :

قد يكون شخصي على حاسب شخصي أو على شكل مخدم ، وتتم عادة عملية التحكم والتصفية في هذا النوع على شكل منتج برمجي .

مثال عليه الجدار الناري الموجود في نظام ويندوز

4- Statefull Filters:

يحافظ على المسار الخاص بحالة الاتصال ويفحص فيما إذا كان الاتصال قد تم تأسيسه ، وانه قدتم انتقال البيانات ، وانه قد تم إنهائه .

5- Hybrid firewall:

هو عبارة عن دمج لعدة أنواع من الجدار الناري السابقة .

سياسات الجدار الناري – Firewall Polices:

هناك ثلاثة سياسات يتبعها الجدار الناري وهي:

– **DROP** في هذه الحالة الجدار الناري سوف يسُقط الاتصال خارج أو داخل بناءً على القوانين المحددة له مسبقاً

– **ACCEPT** في هذه الحالة الجدار الناري سوف يقوم بقبول الاتصال خارج أو داخل بناءً على القوانين المحددة له مسبقاً

– **DEFAULT POLICY** افتراضيا الجدار الناري يقوم بمنع جميع الحزم الداخلة ويسمح مرور الحزم الخارجة للاتصالات الداخلة, أيضاً قوانين المنع تتجاوز قوانين السماح, وللاتصالات الخارجة قوانين السماح تتجاوز قوانين المنع

DMZ (DEMILITARUZED ZONE) : منطقة منزوعة السلاح

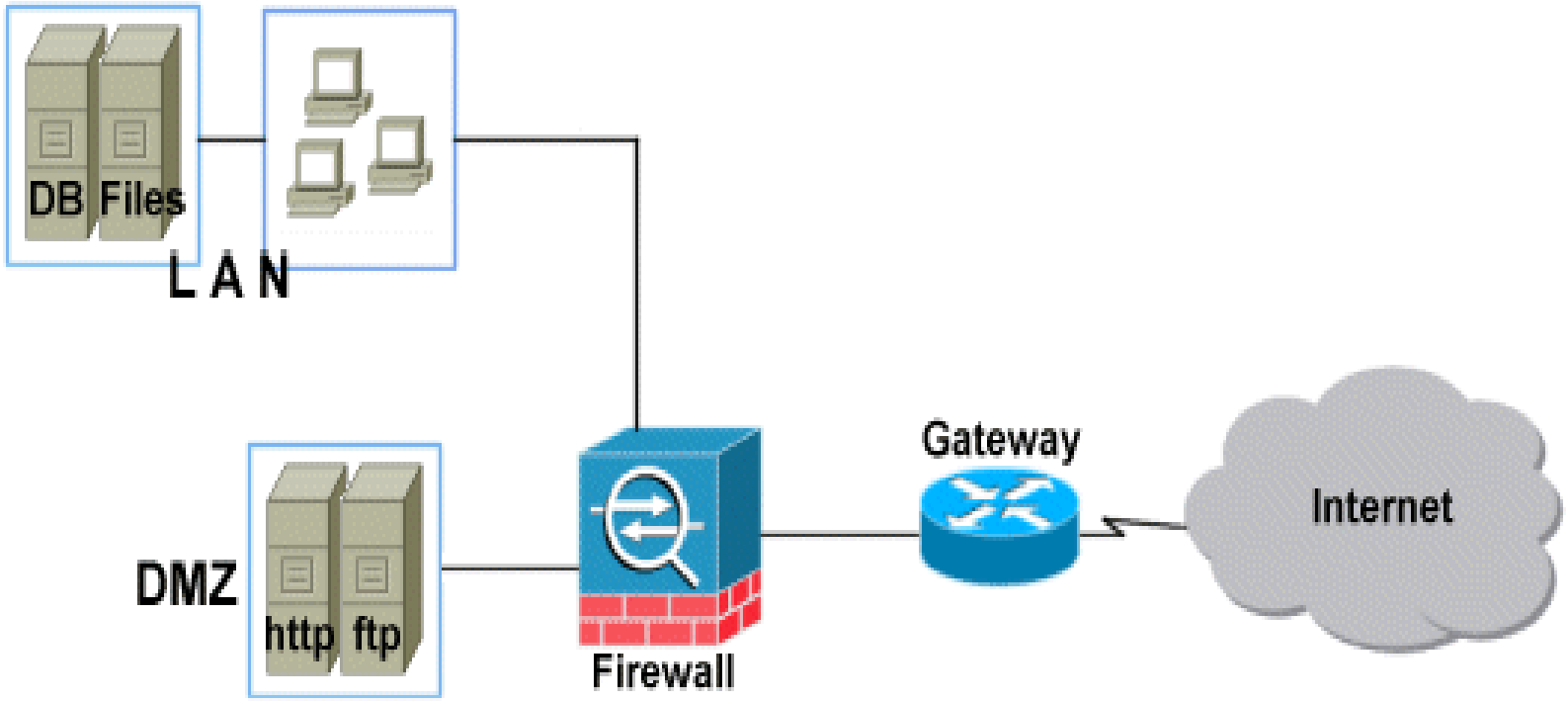
تعني منطقة منزوعة السلاح وهذا يعني في الشبكات بأنها بلا حماية وجدار ناري وكما معروف في الشبكات ان هناك نوعين رئيسين هما :-

1. الشبكة الداخلية (LAN) : واهم ما تتضمنه الأجهزة المركزية (السيرفرات) بالإضافة إلى أجهزة المستخدمين الراوترات وغيرها ومن المفروض أن تكون محمية ومؤمنة من أي تداخل مع أي شبكة خارجية
2. الشبكة الخارجية : بصفتها العامة لاتتوفر فيها مستوى عالي من الحماية وهي بالنسبة لداخلية تشكل مصدرا رئيسيا لحظر الاختراق والتهديدات وعادة يفصل بين هاتين الشبكتين بوسيلة حماية قد تكون ابسط صورة لها جهاز الراوتر او جهاز ناري
3. DMZهي نوع ثالث من الشبكات تقع في مستوى وسط بين النوعين السابقين وهي شبكة محايدة فلا هي محمية ومؤمنة بشكل كلي وكامل كما في الشبكات الداخلية ولاهي مكشوفة بشكل صريح للمستخدمين كما في شبكة الانترنت

يتم اللجوء لحل DMZعند الحاجة لتمكين المستخدمين في الشبكة الخارجية من الوصول إلى بعض الخدمات في الشبكة المحلية مثل Web Serverو FTPفبدلا من توفرها ضمن مجال الشبكة الداخلية بما يشكله هذا من تعريض كامل الشبكة لخطر الاختراق والهجمات ,يتم وضع هذه الخدمات ضمن شبكة منفصلة عن الشبكة الداخلية وذلك لتحقيق إمكانية العزل عن الأخطار التي يمكن أن يشكلها الانترنت.مع إمكانية توفير الخدمات اللازمة للخارج .

وبشكل مختصر فهي تمثل حلقة وصل بين شبكة LANوشبكة WAN .

الشكل التالي يوضح آلية عمل DMZ



يشكّل جهازي الراوتر وجدار النار firewall مستويين من الحماية هنا...وعملياً، يتم التصميم بحيث توضع كل شبكة من الشبكات الثلاث على أحد منافذ الجدار الناريfirewall interface. بالطبع يخصص لكل منها عنوان شبكة network addressومجموعة عناوين IP خاصة بها، ويقوم جدار النار -كما الراوتر- بتوجيه البيانات فيما بين المنافذ.

توضع السياسات المناسبة لكل منفذ، بحيث تمكّن كل طرف من الوصول فقط إلى ما هو مسموح له. مثلاً يستطيع المستخدمون المحليون الوصول إلى الإنترنت للتصفّح، والوصول إلى DMZ لإستعراض أو إضافة أو تعديل محتويات السيرفرات. بينما يمنع جدار النار المستخدمين الخارجيين من الوصول إلى LAN بل الوصول إلى DMZ فقط.