بسم الله الرحمن الرحيم
وصلى على رسول الله الكريم

جامعة افريقيا العالمية
كلية دراسات حاسوب
قسم تقانة المعلومات

تاريخ الجدار الناري Fire Walls& مكافحة الهجمات الموحدة UTM “Unified Threat management”&VPN

اعداد:
ايمان محمد &اسلام حماد

الجدار الناري "FIRE WALLS"

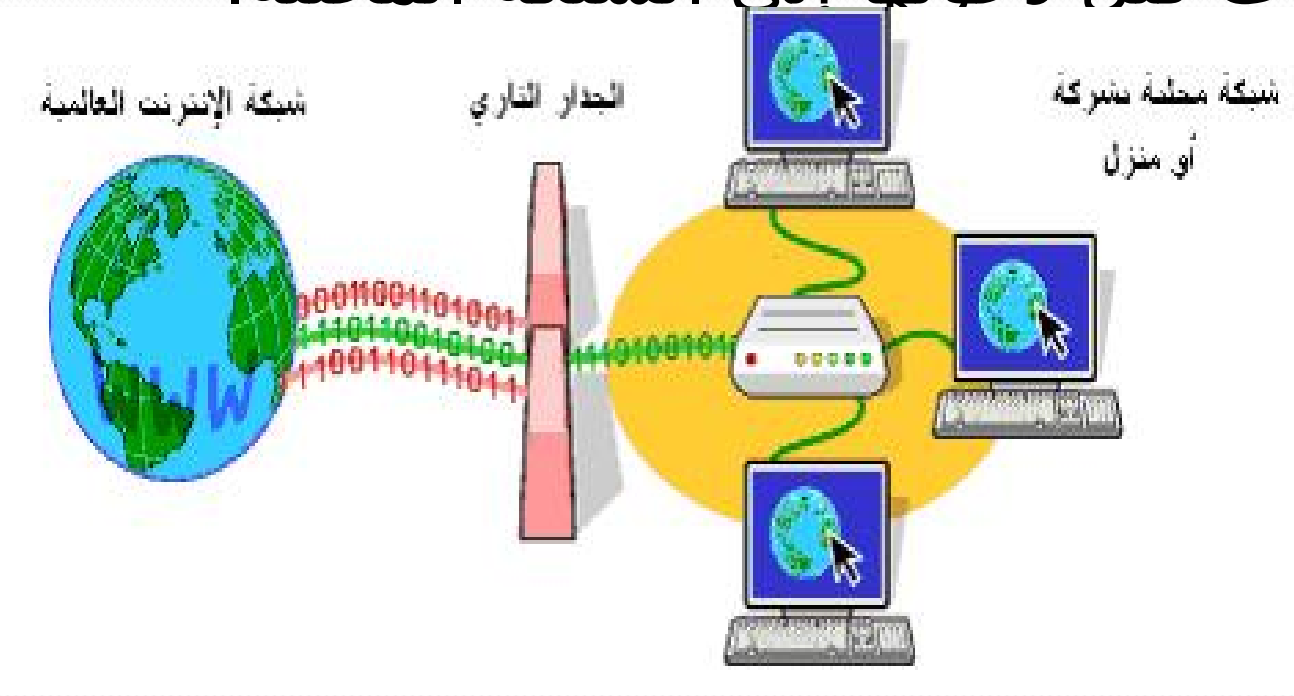
تاريخ الجدار الناري Fire Walls:

- ظهرت تقنية الجدار الناري في أواخر الثمانينات .
- عام 1988، عندما قام مهندسون من (DEC) بتطوير نظام فلترة عرف باسم جدار النار بنظام فلترة العبوة
- **الانواع** :هنالك العديد من فئات الجدران النارية:
  - بناءً على مكان عمل الاتصال.
  - مكان تشفير الاتصال.
  - الحالة التي يتم تتبعها.

الجدار الناري Fire Walls:

تعريف الجدار النارى Fire Walls:

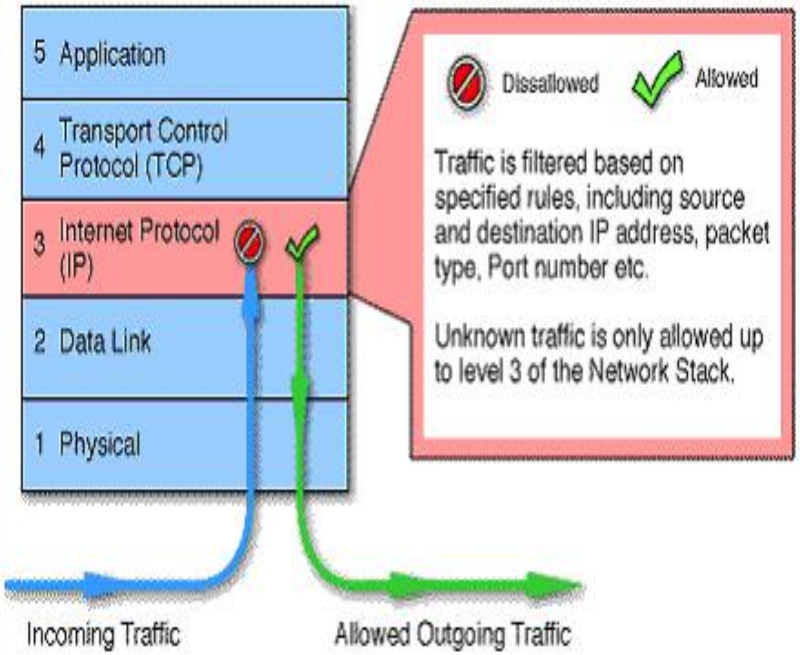
- هو برنامج (Software) أو جهاز (Device) لتنقية البيانات قبل دخولها إلى الشبكة المحلية.

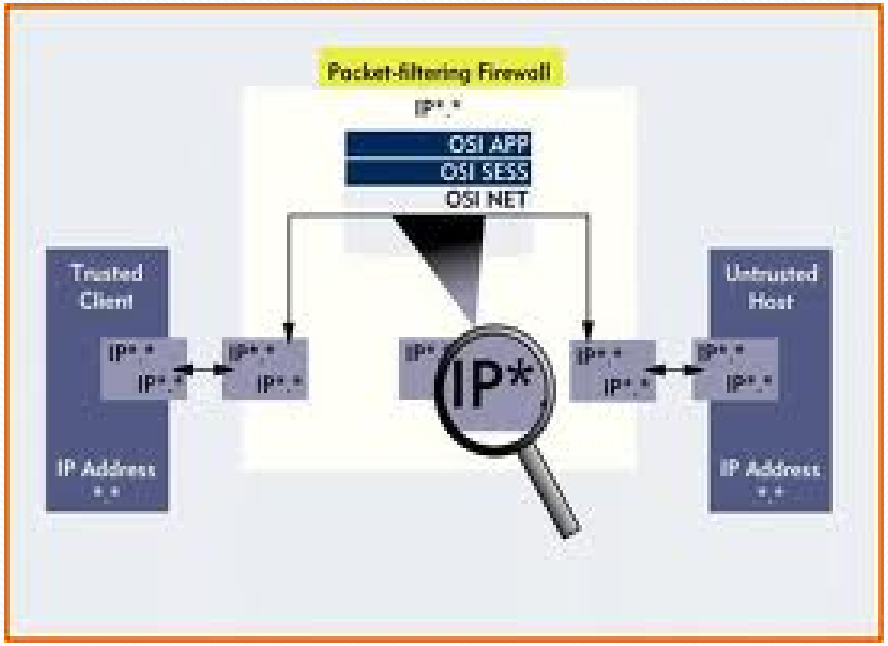


آلية عمل الجدار الناري"Fire Walls":

تعمل الجدران النارية بإحدى الطرق التالية للتحكم بجريان حزم البيانات من الشبكات:

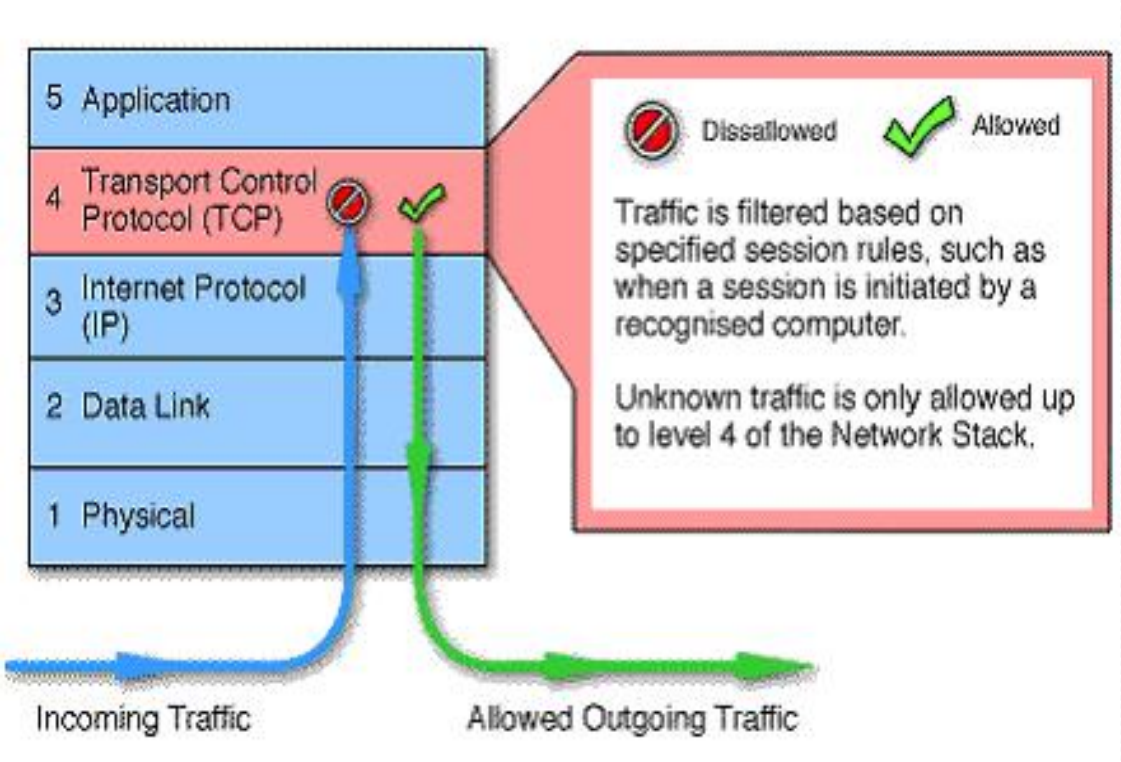
- تصفية الحزم (**Packet filtering**): تجري هذه العملية ضمن طبقة الشبكات (Network Layer) في الطراز OSI أو في طبقة IP منTCP/IP. تشكل هذه الطبقة جزءاً من الموجهات (Routers) ذات الجدران النارية، (**والموجِّه جهاز يستقبل حزم البيانات من شبكة ويوجهها إلى أخرى**) وفي هذه الطريقة تجري معالجة حزم البيانات بتمريرها على عدد من المرشحات ، والحزم التي تجتاز كل مراحل الترشيح يمكن أن تصل إلى مخدمات وحواسيب الشبكة الأخرى. ويُهمل ما تبقى من الحزم.



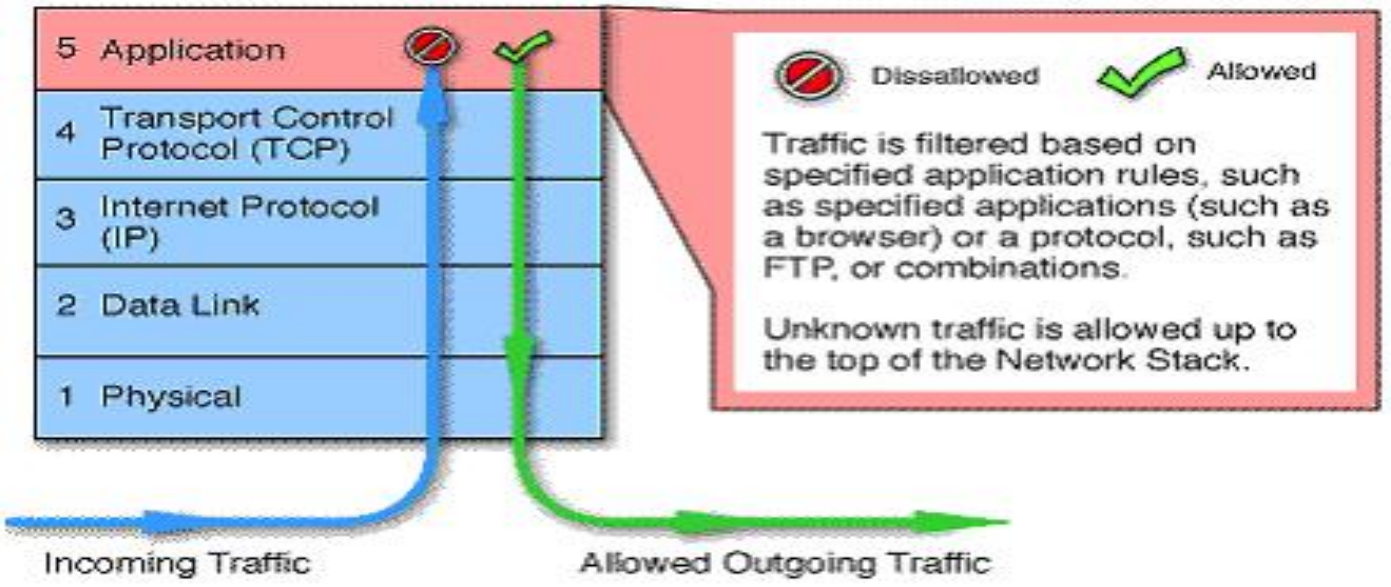


- **بوابات العبور على مستوى الدارات الإلكترونية:** تعمل على طبقة (Session Layer) في البروتوكولات TCP/IP أو عبر الطراز OSI حيث تجري مراقبة البروتوكول TCP لتحديد ما إذا كانت الجلسة (Session) المطلوبة من حاسوب ما عن طريق هذه

حيث تمر البيانات إلى الحاسوب الذي أرسل الطلب عبر بوابة العبور الإلكترونية، وتبدو كأنها موجهة من تلك البوابة، تعتبر هذه العملية مفيدة في إخفاء البيانات الأخرى في الشبكة التي تنتمي إليها هذه البوابات. وتؤدي د

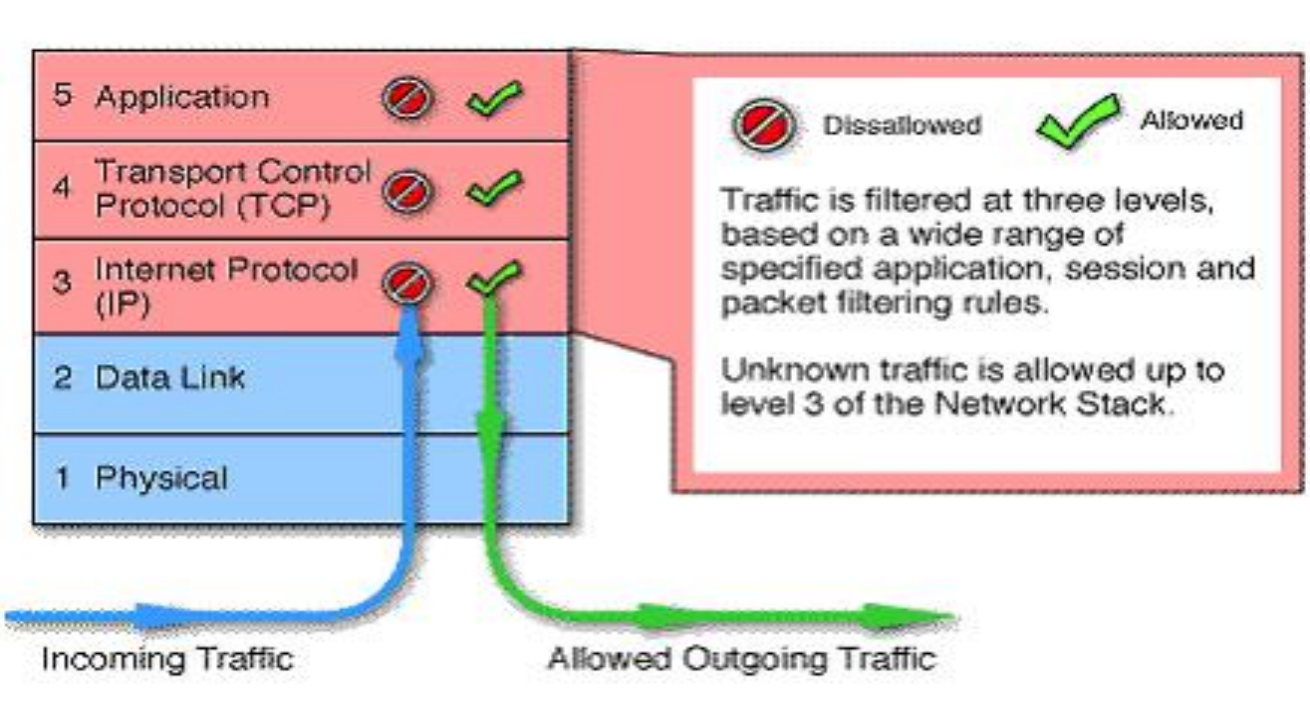


- **باستخدام المخدم الوكيل (Proxy service):**
يجري العمل بهذه الطريقة من خلال طبقة التطبيقات (Application layer) أو المخدم الوكيل، الذي يقوم بإدارة حركة رزم البيانات من الإنترنت إلى الشبكة المحلية وبالعكس، ويمكن التحكم بإعداد المخدم الوكيل ليقوم بترشيح وحذف الطلبات التى تعتبر غير هامة.



- **باستخدام الطرق الثلاث السابقة مجتمعة (Stateful multilayer inspection firewalls):**

تُستخدم كل الميزات التي جرى استعراضها في الأنواع السابقة للحصول على مستوى عال من الحماية.



- **استخدام الرقابة الآنية (State ful inspection):**

وهي طريقة جديدة تقوم بمقارنة بعض الأجزاء المفتاحية لحزم البيانات , بدلاً من مقارنة كامل الحزم ببيانات لمواقع موثوق بها ومخزنة في قاعدة معطيات. عندما تخرج حزم البيانات وتجتاز الجدار الناري إلى الإنترنت يجري تخزين معلومات مفتاحية معينة عنها في قاعدة المعطيات, وعندما تأتي أي حزمه من البيانات من خارج الجدار الناري لتعبر إلى الشبكة المحلية تقارن المعلومات المفتاحية فيها بما هو موجود في قاعدة البيانات , فإن كان هناك تشابه مع البيانات المخزنة في قاعدة البيانات يُسمح لهذه الحزمه بعبور الجدار وإلا فلا.

كيف تجري تصفية البيانات في الجدران النارية:

تتمتع الجدران النارية بمرونة كبيرة، إذ نستطيع أن تضيف عوامل تصفية (Filters) حسب الطلب ضمن شروط محددة منها:

- **عناوين الإنترنت (IP addresses):**

عندما يكتشف الجدار الناري أن أحد العناوين من خارج الشبكة المحلية يقوم بقراءة ملفات عديدة من مزود الخدمة التابع للشبكة المحلية , يستطيع الجدار الناري في هذه الحالة أن يوقف ذلك, ويقوم بحجب كل رزم البيانات التي تأتي من ذلك العنوان.

حقل الأسماء (Domain Names):

تستطيع الشركات التحكم بالولوج إلى شبكاتها المحلية عن طريق إضافة حقول أسماء المواقع التي يراد حجبها , إلى قائمة المواقع المحظورة في الجدار الناري.

البوابات (Ports):

تتصل مزودات الخدمة في الشبكات المحلية عن طريق البوابات، وكل خدمة على مزود الخدمة تحجز بوابة خاصة بها، فإذا كان مزود الخدمة يقوم بتشغيل بروتوكول صفحات الوب HTTP وبرتوكول نقل الملفات FTP فإن التخاطب عبر بروتوكول HTTP يجري بين مزود الخدمة وعالم الإنترنت عن طريق البوابة 80 , والتخاطب عبر البروتوكول FTP يجري عن طريق البوابة 21 بشكل ثابت، وفي معظم الأحيان ترغب الشركات الخاصة أن يجري التعامل مع

البروتوكول FTP بواسطة جهاز واحد فقط في الشركة , و تُحجب المعلومات (المتبادلة عن طريق البوابة 21) عن باقي الأجهزة في الشركة بتهيئة الجدار الناري بالطريقة المناسبة

ملاحظه:

الجهاز الذي يتصل مع الإنترنت دون الأجهزة الأخرى , في حال وجود شبكة محلية منزلية أو مكتبية , يعتبر بوابة عبور

كلمات أو جمل معينة:

يمكن أن نضع في هذا الخيار أي شيء , وسيقوم عندها الجدار الناري بالبحث عن الشيء المطلوب في كل رزمة بيانات تمر عبره , ويقوم بحجب كل رزم البيانات التي تحوي العبارة أو الكلمة المطلوبة بالضبط وكما كتبت.

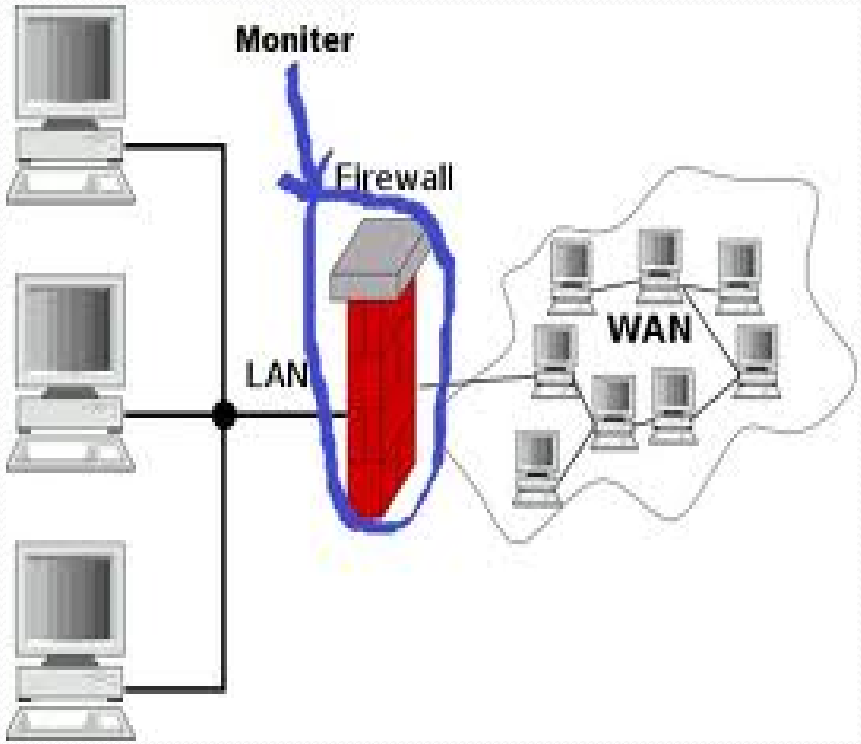
البروتوكولات (Protocols):

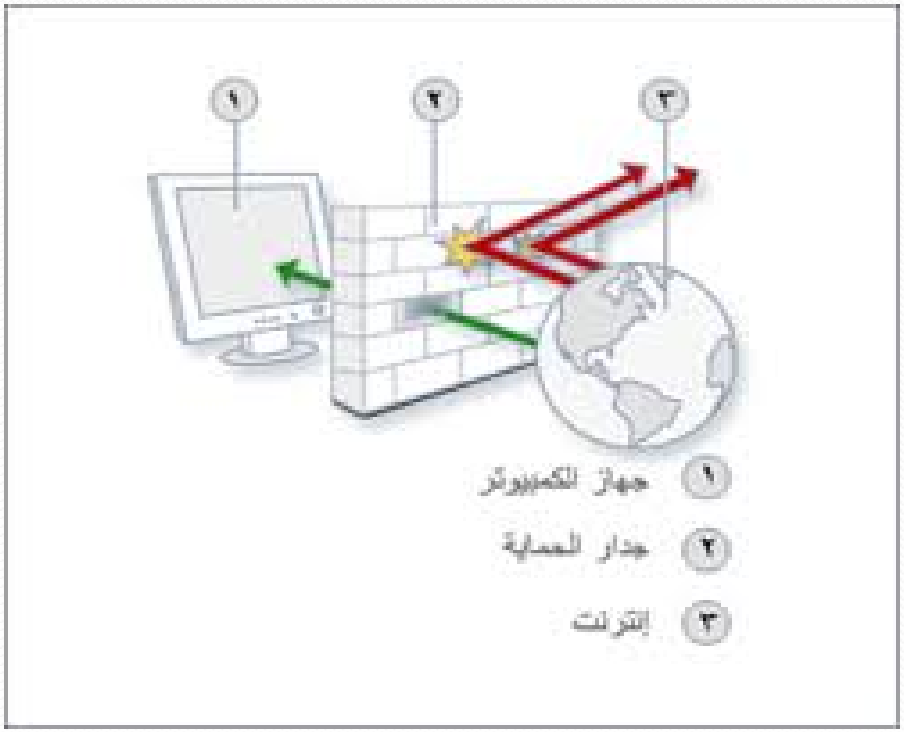
يعرف البروتوكول بأنه طريقة معرفة سلفاً للتخاطب بين طرفين، وفي أغلب الأحيان يكون البروتوكول نصاً يصف كيف تجري عملية التخاطب بين طرفي المحادثة. ونستعرض فيما يلي مجموعة البروتوكولات التي يمكن للجدار الناري أن يقوم بتصفيتها عن طريق السماح أو عدم السماح للمعلومات التي تنقل بوساطة هذه البروتوكولات بالولوج إلى الشبكة المحلية.

1. بروتوكول الإنترنت (Internet Protocol (IP: ويعتبر النظام الأساسي لتبادل البيانات عبر الإنترنت.
2. بروتوكول التحكم بالنقل (Transmission Control Protocol(TCP: يقوم هذا البروتوكول بقولبة البيانات التي ستُنقل عبر الإنترنت.

3. بروتوكول تحويل النصوص الفائقة (Hyper Text Transfer Protocol (HTTP): يستعمل في صفحات الوب (Web Pages).
4. بروتوكول تحويل الملفات (File Transfer Protocol (FTP): يستعمل لنقل الملفات من الإنترنت و إليها.
5. بروتوكول (User Datagram Protocol (UDP: يستعمل مع البيانات التي لا تتطلب رداً من المستلم كإرسال ملفات الفيديو أو الصوت على الإنترنت.
6. بروتوكول التحكم بالرسائل عبر الإنترنت Internet Control Message Protocol (ICMP): يستعمل من قبل الموجهات (Routers) لتبادل البيانات فيما بينها.
7. بروتوكول نقل الرسائل النصية البسيطة Simple Mail Transport Protocol (STMP): يستعمل لإرسال الرسائل النصية البسيطة إلكترونياً.
8. بروتوكول إدارة الشبكة البسيط Simple Network Management Protocol (SNMP): يستعمل لجمع المعلومات عن أنظمة الشبكة بواسطة حاسوب معين.
9. بروتوكول Telnet: يستعمل لإنجاز أوامر معينة على حاسوب معين من خلال الشبكة.

تجري عادة في الشبكات المحلية تهيئة واحد أو اثنين من الحواسيب ليتعامل مع بروتوكول معين ويحجب هذا البروتوكول عن طريق الجدار الناري عن باقي الأجهزة في الشركة.


Moniter
Firewall
LAN
WAN


١
٢
٣
١ جهاز الكمبيوتر
٢ جدار الحماية
٣ إنترنت

مكافحة الهجمات الموحدة UTM “Unified Threat management”:

وقد تم انتاج أجهزة الـ UTM بعد ارتفاع معدلات اختراق الشبكات للشركات وباتت غير قادرة على صد هجمات الهاكرز والكراكرز وغيرهم من مخربي ومجرمي الانترنت ونحن نعرف أن سرية وأمن المعلومات أهم مطلب للشركات..

تعريف (utm):

- هو عبارة عن جهاز لحماية شبكات الكمبيوتر .
- تعتبر أجهزة UTM من أهم وسائل الحماية فهو بمثابة جهاز Firewall ولكن متعدد الوظائف.
- يستخدم تكنولوجيا المسح الضوئى .
- الشكل التالي يوضح نوعين من utm:

متوفر بالاشكال التاليه :

1-كقطعة منفصلة .ware

2-برمجيا . Software

3- كتطبيق افتراضي.

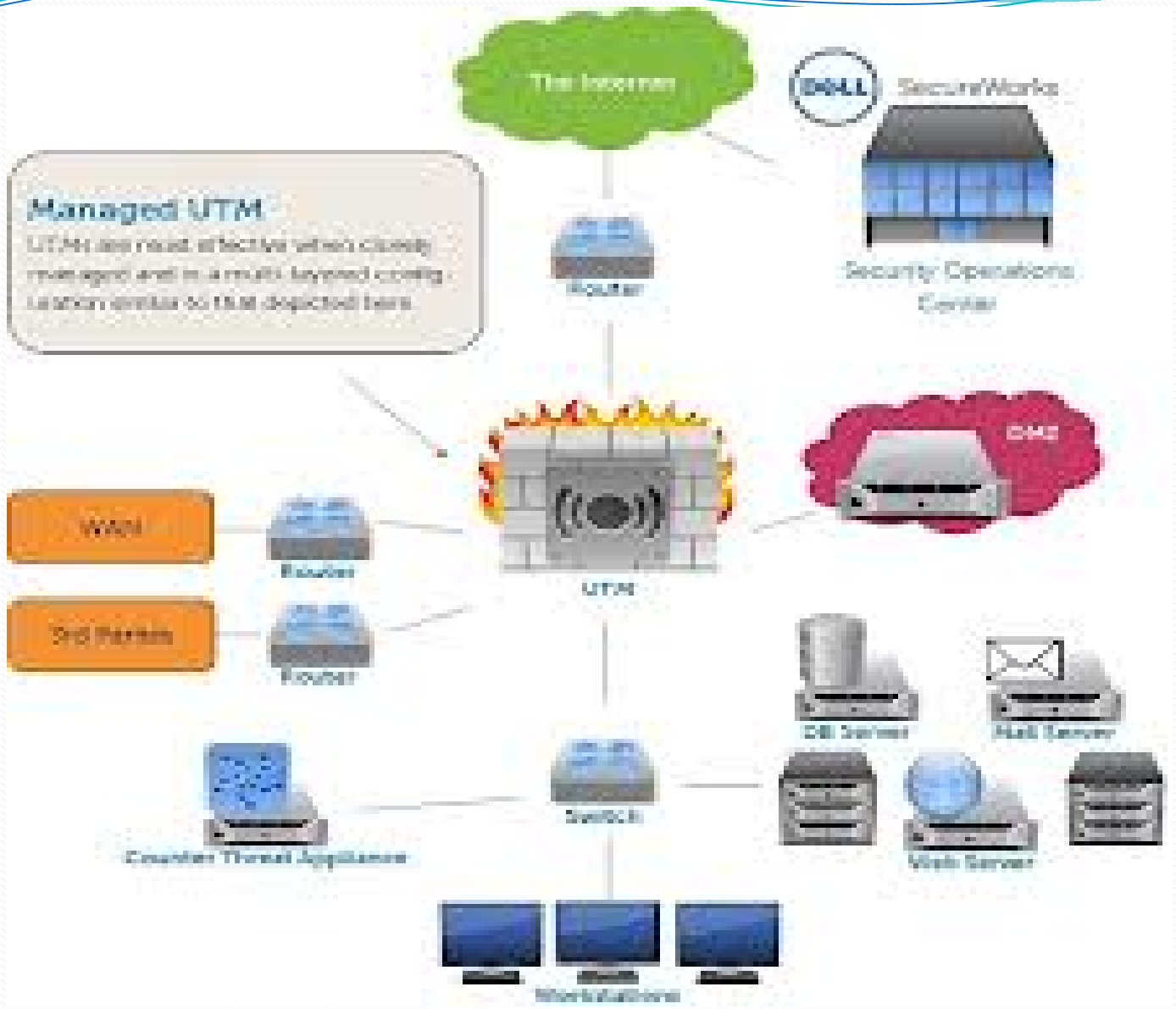
مهام الجهاز :

1- الحماية من الفيروسات وفلترة وتصفية المحتويات ومحاربة البريد المزعج spam

2- مراقبة حركة البريد الالكتروني والحماية من البرمجيات الخبيثة Malware وبرامج التجسس Spyware

3- العمل على بعض أجهزة VPN وغيرها دون الحاجة لاستخدام العديد من البرامج والأدوات لفعل ذلك وكما أنها سهلة التركيب والاستخدام

4- تعطيل عمل برامج P2P والتورنت و برامج Voip وحجب المواقع المزيفة ومراقبة حزم البيانات وحركتها من الطبقة الثانية وحتى السابعة في نموذج Open System Interconnection (OSI) التحكم بالتطبيقات.


Managed UTM
DMZ
UTM

احدث اجهزة الـutm :