البرامج الخبيثة & الجدار الناري
MALWARE& FIREWALL

نظري L6

البرامج الخبيثة Malware

فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات. وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة، والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.

يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطيئه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها.

أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.

أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة، كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.

يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة.

1. الفيروسات وأشباهها (hoax viruses, worms,):

أولاً: <u>أنواعها:</u>

- الفيروسات viruses: هي برامج حاسوبية خبيثة مضرة بالحواسيب، وتنتقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى.
  هناك أنواع للفيروسات، منها ما يبدأ عمله بوقت أو حادثة معينة، حتى أصبح هناك تقويم للفيروسات التي ستعمل في يوم ما، ومنها ما يكون مكوناً من أجزاء متعددة ، ومنها ما تتغير صفاته بشكل دوري، ومنها ما يكون متخفياً حتى عن برامج مكافحة الفيروسات.
- الديدان worms: هي برامج حاسوبية خبيثة ومضرة، وتنتقل بين الحواسيب بعدة طرق، وتمتاز عن الفيروسات باعتمادها على نفسها لتتكاثر وبسرعة الانتقال وصغر الحجم، والديدان لاتقوم عادة بعمل ضار مباشرة، كحذف البيانات ،ولكن سرعة تكاثرها وانتقالها السريع يؤثران سلباً في فعالية الحاسوب وشبكة المعلومات.
- الخداع أو البلاغ الكاذب Hoax: البلاغ الكاذب عن ظهور فيروس، يربك به الناس ويضيع به أوقاتهم، وقد يؤثر في الحاسوب.
  يبدأ من شخص يريد الضرر وينتشر بواسطة أناس صدّقوا الكذبة ونشروا الخبر بغرض المساعدة في التصدي للفيروس أو الدودة.
  قد يأتيك رسائل بريدية كاذبة تحذرك من فيروس معين قد انتشر مؤخراً، ثم يقدم لك خطوات لمعرفة ما إذا كان جهازك قد أصيب به أم لا، وطبعاً سيكون جهازك مصاباً به لأن الخطوات لاكتشاف الفيروس تدل على أن كل جهاز صحيح مصاب لكي يأكل

الطعم، ثم يطلب منك حذف بعض الملفات الأساسية للحماية من الفيروس أو الدودة، وبعد ذلك يتعطل جهازك.

ثانياً: آثارها:

يقوم الفيروس بحذف ملفات أو برامج أو تعطيلها عن العمل، ومنها ما يقوم بزراعة برامج خبيثة أخرى قد تكون تجسسية، ومنها ما يعطل الجهاز كلياً وغيرها من الآثار الضارة.
كذلك الديدان لها تأثيرات ضارة، كما هو معروف فإن كل برنامج يعمل في الجهاز يأخذ من وقت المعالج، ومساحة في الذاكرة والقرص الصلب، وحتى إن كان البرنامج صغير الحجم، فما بالك إذا كان هناك عدد كبير من البرامج، كذلك عند انتقال ملايين البرمجيات الصغيرة عن طريق الشبكة.
إن انتشار الديدان الواسع أدى إلى إضعاف سرعة النقل على الانترنت ، وإلى تعطيل إحدى أكبر شبكات الصراف الآلي في العالم وإبطاء أنظمة التحكم الجوي في كثير من المطارات الدولية وغيرها.

ثالثاً: طرق العلاج:

يعتمد نوع العلاج على نوع الإصابة وتأثير الفيروس، إذا وصل ضرر الفيروس إلى حذف أغلب الملفات، أو عطّل الجهاز فما لديك سوى إعادة تثبيت جميع البرامج والملفات من النسخة الاحتياطية لملفاتك التي أوصينا بالاحتفاظ بها في طرق الوقاية.
أما إذا كان ضرر الفيروس اقل من ذلك، فإن برنامج مكافحة الفيروسات سيساعدك على إصلاح الملفات المعطوبة قدر الإمكان، وحذف الفيروس من الجهاز، ولا تنسى أن تحدّث برنامج مكافحة الفيروسات ليتمكّن من التعرف على الفيروس إن كان من الفيروسات الجديدة.

2. الأحصنة الطروادية (Trojan Horses):

هو برنامج حاسوبي يضمر أعمالاً خبيثة ومضرة، خلاف ما يظهره من أعمال مفيدة، وهو لا يتكاثر مثل الفيروسات والديدان، ولكن يكمن في النظام بشكل خفي، يحاول استغلال حاسوبك لشن الهجوم على حواسيب أخرى، أو التجسس من خلال الاحتفاظ بجميع ما أدخلت عن طريق لوحة المفاتيح، والتي قد تحتوي على رقم بطاقة الائتمان أو كلمة المرور.

- أنواعها:

1) الوصول عن بعد: هذه البرامج تسمح للمهاجم أن يتحكم في جهازك عن بعد بشكل خفي، من أمثلته: Back Orifice ,Netbus.
2) مرسل البيانات Data Sender: هذا البرنامج يرسل بيانات خاصة بالمستخدم للمهاجم دون علم المستخدم، وقد يرسل رقم بطاقات الائتمان، كلمة المرور، محادثاتك المكتوبة وغيرها من البيانات الهامة.

يرسل البيانات بواسطة رسالة بريدية، أو تزويدها لموقع المهاجم مباشرة.

3) معطل الخدمات Denial of service: يعمل هذا البرنامج بالتنسيق مع نسخ مشابهة على أجهزة أخرى مهاجمة على مهاجمة حاسوب معين وإغراق شبكته وشلّها.
4) وسيط Proxy: يسخّر الحاسوب المهاجم وسيطاً يستطيع المهاجم استخدامه للوصول المتخفّي للانترنت، بحيث لو عمل عملاً غير شرعي وتمت متابعة العملية فإن الحاسوب الذي جرى تسخيره هو آخر نقطة يمكن تتبع العملية إليها.
5) معطل البرامج Blocker: يقوم بتعطيل بعض البرامج، خاصة الحساسة، مثل برامج مكافحة الفيروسات، وبرامج جدران الحماية ليجرد جهازك من أي حماية ضد الهجمات المستقبلية.

- آلية عملها:

يقوم المهاجم بزرع برنامج مستقبل او خادم (client/server) (لاستقبال الأوامر والتعليمات) على جهاز الضحية بعدة طرق، ويفتح منفذاً خاصاً به للاتصال عن طريق الانترنت، ثم يقوم البرنامج بإرسال عنوان جهازك على الانترنت (IP) للمهاجم، بعد ذلك يقوم المهاجم بالاتصال بذلك البرنامج ليبدأ التحكم بجهاز الضحية.

- برامج علاجية:

بما أن هناك برنامجاً خبيثاً ومنفذاً مفتوحاً للاتصال فإن الحل الأمثل للعلاج من الأحصنة الطروادية يكمن في نوعين من البرامج:

1) برنامج جدار الحماية (Firewall) : للتحكم في المنافذ ومراقبتها، ومنع المنافذ غير الشرعية من الاتصال بالانترنت، وبالتالي قطع الصلة بالمهاجم، وهذا عمل هام، لكن لايفيد في حال اتخاذ البرنامج الخبيث قناة أخرى غير شرعية للاتصال، كأن يستخدم البريد الاكتروني .
2) برنامج لصيد البرامج الخبيثة بشكل عام وخاصة الأحصنة الطروادية ومكافحتها: إن برامج مكافحة الفيروسات تصيد جزءاً من الأحصنة الطروادية، لكن ليس جميعها، لذا يلزم برامج مكافحة خاصة بالأحصنة الطروادية لحماية جهازك بشكل أفضل، ولا تنس أن تحدّث برامج المكافحة بشكل دوري لصيد البرامج الخبيثة الجديدة.

من برامج مكافحة الأحصنة الطروادية

lockdown2000, Pest Patrol, The Cleaner, Tuscan,) .(Trojan hunter

لا تنس بعد اكتشاف اي حصان طروادي ومكافحته أن تقوم بما يلي:

- استبدال كلمات المرور المسجلة على الجهاز والتي يمكن أن تكون قد سرقت من قبل المهاجم عن طريق الحصان الطروادي.

- تفحّص جهازك باستخدام برنامج مكافحة الفيروسات، تحسّباً من أن يكون المهاجم قد زرع فيروساً في جهازك.

3. رسائل الاصطياد الخادعة (phishing scam):

يستخدم مصطلح (Phishing) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات المصرفية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات المصرفية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع.

هناك برامج لمكافحة اللصوصية Phishing والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروف أو مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

4. البرامج التجسسية وأشباهها Spyware:

هي كل برنامج يراقب سلوكك على جهازك من مراقبة كتاباتك إلى مراقبة المواقع التي تزورها، والهدف منها يكاد ينحصر في أمرين: أولهما: التجسس الخبيث لاستقاء معلومات سرية، مثل كلمات المرور وأرقام الحسابات المصرفية، والآخر: لأغراض تجارية، مثل معرفة أنماط المستخدم الاستهلاكية، أو محركات البحث الأكثر استخداماً، أو المواقع التجارية الأكثر تسوّقاً.

إن تلك البرامج تستنزف طاقات الجهاز والاتصال دون إذن واضح منك، وكما تعلم أن مجرد المراقبة، وتسجيل السلوك أو المعلومات يتطلب وقتاً من المعالج، ومساحة من الذاكرة، ووحدة التخزين الدائمة، وجزءاً من كمية البيانات المرسلة عن طريق وسيط الاتصال.

- أنواعها:

1) برنامج متابعة تصرفات المستخدم أو التجسس البسيط spyware: هي كل برنامج يتجسس على سلوك المستخدم أو معلوماته بعلم، أو بدون علم.
2) برنامج تسجيل نقرات لوحة المفاتيح Keystroke Logger.
3) برامج الإعلانات Adware: برامج هدفها التسويق التجاري بطريقة إجبارية غير مرغوبة. مثلاً تقديم إعلانات لمنتجات معينة بمجرد البحث عن مثيلاتها في محرك البحث، وتعطيل محرك البحث وتقديم محرك بحث آخر مقلد ليخدم مهام الجهة الإعلامية لبرنامج الإعلانات.
4) الصفحات الفقاعية أو الانبثاقية Popup: برامج تخرج بين الحين والآخر كإعلانات أثناء تصفح الانترنت، وتستهلك موارد النظام والاتصال.

- طرق الإصابة بها:

تتمكن تلك البرامج من الدخول للحاسوب باستخدام طريقتين: الأولى عن طريق وجودها مع البرامج المجانية المشبوهة، والأخرى عن طريق استغلال إحدى الثغرات الأمنية في جهازك للوصول إليه.

- طرق معرفة الإصابة بها: هناك عدة طرق للتعرف على الإصابة ببرامج التجسس والمراقبة أهمها كثرة الصفحات الانبثاقية التي ليس لها صلة بالموقع الذي نزوره، ومحاولة الحاسوب الاتصال بالهاتف دون أمرك، ويصبح الحاسوب بطيء الاستجابة لدرجة ملحوظة، وايضاً عندما نقوم بالبحث، فإن المتصفح يستخدم محركاً للبحث غير الذي حددته، ويمكن أن تحتوي قائمة البرامج المفضلة في برنامج تصفح الانترنت على مواقع لم تقم بإضافتها، بالإضافة إلى أن صفحة البداية تشير إلى موقع لم تقم باختياره كصفحة البداية، ويبقى كذلك حتى لو غيرت صفحة البداية.
- طرق الوقاية:

1) داوم على سد الثغرات الأمنية بمتابعة آخر التحديثات لبرامجك الحساسة مثل نظام التشغيل ومتصفح الانترنت وبرنامج البريد الالكتروني.
2) دعّم حاسوبك ببرنامج أو جهاز جدار الحماية لتقليل تعرّضه للاختراق من قبل الغير.
3) دعّم حاسوبك ببرنامج مكافحة الفيروسات.
4) تأكد من مرفقات البريد الاكتروني ولاتقم بفتحها حتى تتأكد من خلوها من الفيروسات، وأنها مرسلة من شخص موثوق به.
5) دعّم حاسوبك ببرامج لمكافحة برامج التجسس والصفحات الفقاعية.

- برامج علاجية:

.Pest Patrol ،Destroy& Search- Spybot ،Ad-Aware Pro

الخلاصة:

البرامج الخبيثة هي برامج يكون كل مهامها أو أحدها عمل ضارّ كالتجسس أو التخريب، أو استنزاف الموارد الحاسوبية، وتنتقل هذه البرامج إلى الحاسوب، أو شبكة المعلومات بوسائل متعددة وملتوية ترتكز في معظمها على استدراج المستخدم، وينبغي أن يدرك المستخدم هذه الطرق، كما ينبغي أن يتتبع الأساليب التي ثبت نجاحها لمنع الإصابة بالبرامج الخبيثة ، أو التعامل الصحيح معها في حال وصولها إلى شبكة المعلومات.

جدار الحماية Firewall

ظهرت تقنيات ومفاهيم متعددة لمقاومة البرامج الخبيثة وما تسببه من آثار سلبية، وتعد جدران الحماية (الجدران النارية) من أكثر هذه التقنيات انتشاراً، وهو عبارة عن نظام مؤلف من برنامج (software) يجري في حاسوب ، وهذا الحاسوب قد يكون حاسوباً عادياً كالحواسيب الشخصية، أو حاسوب بني بمواصفات خاصة ليكون أكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية.

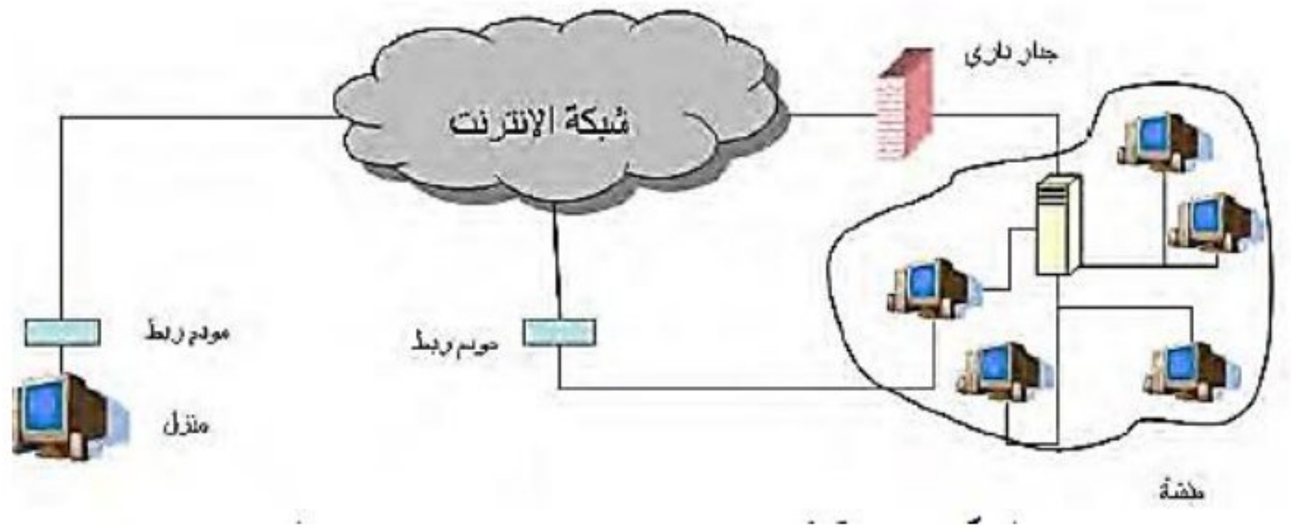
فكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس وتمنع مرور آخرين، بناء على تعليمات مسبقة.

1) وضع جدار الحماية:

لتوفير بعض الحماية لنفسها تقوم بعض المنشآت بوضع جدار حماية لعزل شبكتها الداخلية عن شبكة الانترنت، كما يوضح الشكل (1)، بيد أن هذا العزل يمكن أن يكون كلياً، وذلك للسماح للجمهور بالاستفادة من الخدمات المقدمة، وفي الوقت ذاته منع الطفيليين والمخربين من الدخول، وتتاح من خلال البرنامج الموجود في جدار الحماية مراقبة المعلومات بين الشبكة الداخلية للمنشأة والعالم الخارجي.

الشكل (1) وضع جدار الحماية

ولتحقق الغاية من جدار الحماية فإنه لابد من وضعه في موقع استراتيجي يضمن ألا تخرج المعلومات أو تدخل إلى الشبكة الداخلية إلا عن طريقه.
لذلك فإن الوضع الموضح بالشكل (2) غير مقبول عند المختصين في مجال أمن المعلومات، لأن الوصول للشبكة الداخلية ممكن عن طريق الاتصال بجهاز المودم الذي يشكل في هذه الحالة بوابة خلفية يدخل المخربون عبرها.



الشكل (2) وضع غير محبذ لاستخدام جدار الحماية

2) كيف تعمل جدران الحماية؟

طريقة عملها يحددها تصميم جدران الحماية، لتبسيط هذا الموضوع نقول إن هناك ثلاثة أساليب في تصميم جدار الحماية:

A. أسلوب غربلة ظروف البيانات المرسلة (Packet Filtering):
تنتقل المعلومات على شبكة الانترنت في صورة ظرف الكتروني، وإذا كان جدار الحماية مصمماً بهذه الطريقة فإنه يفحص كل ظرف يمر عبره، ويتحقق من تلبية الظرف لشروط معينة يحددها الشخص الذي يدير جدار الحماية، وهذه الشروط تدخل بطريقة خاصة في البرنامج المكون للجدار الناري.

B. أسلوب غربلة الظروف مع تغيير عناوين الظروف القادمة من الشبكة الداخلية (الظروف الصادرة):
عندما يقوم مستخدم حاسوب ما بالتعامل مع شبكة الانترنت، كأن يتصفح موقع ما، أو يرسل بريداً الكترونياً، فإن هناك أموراً كثيرة تدور خلف الكواليس دون أن يشعر بها المستخدم، ومن ذلك أن نظام التشغيل الموجود في الحاسوب يقوم بإرسال بيانات إلى شبكة الانترنت لتحقيق رغبة المستخدم، سواء كان تصفح موقع، أو إرسال بريد، وهذه البيانات يجمعها الجهاز في ظروف الكترونية تحمل- ضمن ما تحمل من معلومات- العنوان الرقمي المميز للحاسوب الذي أرسلها، أو ما يسمى (IP-Address)، وهذا العنوان يميز هذا الجهاز عن سائر الأجهزة المرتبطة في شبكة الانترنت،وفائدة هذا العنوان هي تمكين الأطراف الأخرى من إرسال الردود المناسبة للحاسوب الذي أرسل البيانات، وبالتالي تقديم الخدمة للمستخدم الذي طلبها، لكن هذا العنوان قد يستخدم من قبل المخربين لشن هجمات على ذلك الحاسوب.

عند اعتماد هذا الأسلوب يقوم جدار الحماية بطمس العنوان المميز للحاسوب الذي أرسل الظرف من الظرف الالكتروني، ووضع العنوان الخاص بالجدار نفسه بدلاً منه، وبهذا لايرى المخربون من الشبكة الداخلية سوى جدار الحماية، فيحجب الجدار كل أجهزة الشبكة المراد حمايتها وينصب نفسه وكيلاً (proxy) عنها.
عندما يرغب الموقع المتصفح الرد فإنه يرسل رده في ظروف تحمل عنوان جدار الحماية، وبهذا تأخذ كل الظروف القادمة (الواردة) إلى الشبكة الداخلية عنوان جدار الحماية ويقوم هو عند استلامها بغربلتها ثم توجيهها إلى وجهتها النهائية، ولابد في هذه الحالة ان يحتفظ الجدار بجدول متابعة يربط فيه بين عناوين الظروف الصادرة والواردة.
هذا التنظيم يوفر مقداراً أكبر من الحماية بالمقارنة بالطريقة الأولى، لأن الجدار يحجب عناوين الشبكة الداخلية، مما يصعب مهمة من أراد مهاجمتها، وهذه التقنية تعرف باسم تحويل العناوين الرقمية (Network Address Translation) (NAT).

C. أسلوب مراقبة السياق (Stateful Inspection):

هنا يقوم جدارالحماية بمراقبة حقول معينة في الظرف الالكتروني، ويقارنها بالحقول المناظرة لها في الظروف الأخرى التي في السياق نفسه، ونعني بالسياق هنا مجموعة الظروف الالكترونية المتبادلة عبر شبكة الانترنت بين جهازين لتنفيذ عملية ما.
وتجري غربلة الظروف التي تنتمي لسياق معين إذا لم تلتزم بقواعده، لأن هذا دليل على أنها زرعت في السياق وليست جزءاً منه، مما يولد غلبة ظن بأنها برامج مسيئة، أو ظروف أرسلها شخص متطفل.
هناك عدة معايير يمكن استخدام واحد منها أو أكثر لتمييز صحيح للظروف، وهي على الشكل التالي:

1) العنوان الرقمي (IP Address): هو كما أشرنا سابقاً رقم يميز كل جهاز مشترك في شبكة الانترنت، فيمكن للجدار الناري أن يحيز مرور ظرف ما، أو يمنعه بناء على العنوان الرقمي للمرسل أو المستقبل.
2) اسم النطاق (Domain Name): ليسهل على المستخدم العادي الوصول إلى المواقع على شبكة الانترنت، فإن المواقع تعطى أسماء ذات معنى، إضافة إلى العناوين الرقمية، فمثلاً اسم النطاق (www.name.gov.sy) يدل على موقع وزارة ما في سوريا، وتمكن برمجة جدار الحماية بحيث يمنع مرور الظروف الالكترونية القادمة من نطاق معين.
3) بروتوكول التخاطب المستخدم: المقصود بالبروتوكول هنا الطريقة المعينة للتخاطب وتبادل المعلومات بين طالب الخدمة والجهة التي تقدم الخدمة، وطالب الخدمة هنا قد يكون إنساناً أو برنامجاً كالمتصفح (Browser)، ويسبب تنوع الخدمات التي تقدم في شبكة الانترنت، فإن الشبكة تعج بالبروتوكولات اللازمة لتسهيل تقديم تلك الخدمات لمن يريدها، ومن هذه البروتوكولات:

_ بروتوكول (HTTP): يستخدم لتبادل المعلومات بين برنامج المتصفح ومزود الخدمة في الموقع الذي يزوره المصفح.
_ بروتوكول (FTP): يستخدم لنقل الملفات خاصة كبيرة الحجم ، بدلاً من إرسالها كمرفقات (Attachments) في البريد الاكتروني.
_ بروتوكول (SMTP): يستخدم لنقل البريد الاكتروني.
_ بروتوكول (SNMP): يستخدم لإدارة الشبكات، وجمع المعلومات عن بعد.
_ بروتوكول (Talnet): يستخدم للدخول على جهاز ما عن بعد، وتنفيذ بعض الأمور داخله.

هنا نقول أن الشخص المسؤول عن جدار الحماية يمكنه برمجة جدار الحماية بحيث يغربل الظروف بناء على البروتوكول المستخدم لإرسال البيانات، وهناك خانة في الظروف تدل على نوع البروتوكول، فيقوم جدار الحماية بمعاينتها، فإن وجد أن البروتوكول مسموح به، فإن جدار الحماية يسمح للظرف بالمرور، وإلا فإنه يحذف الظرف.

هناك معايير أخرى يمكن استخدامها للغربلة، مثل رقم المنفذ الذي سيستقبل الظرف في الجهاز المرسل إليه، كما يمكن برمجة بعض جدران الحماية للبحث عن كلمات أو عبارات معينة في الظروف، فتحذف منها ما يحتوي على تلك العبارات وتمرر الباقي.

3) أنواع جدران الحماية:

يمكن تصنيفها من حيث الجهة المستخدمة كما يلي:

A. جدران نارية لحماية المنشآت الكبيرة: وهذا النوع توفره شركات كبرى متخصصة وغالباً ما توفر الشركة المصنعة أنواعاً متعددة من جدران الحماية تتفاوت من حيث سرعتها والخدمات التي تقدمها ويتميز هذا النوع بما يلي:

- جدار الحماية يكوع غالباً في جهاز قائم بذاته مصمم لغرض معالجة البيانات بسرعة فائقة، أي أنه ليس مجرد برنامج يعمل في جهاز حاسوب عادي.
- تعدد الخدمات التي يقدمها جدار الحماية ، مثل غربلة الظروف والحماية من الفيروسات وحماية البريد الالكتروني والتشفير.
- تشغيل جدار الحماية يحتاج إلى مهارات فنية متقدمة.
- ارتفاع كلفة الشراء والتشغيل.

يوضح الشكل (3) أحد جدران الحماية التي تصنعها شركة CISCO.

الشكل (3) أحد جدران الحماية من شركة CISCO

B. جدران نارية لحماية المنشآت الصغيرة: هذا النوع يشبه سابقه في كونه جهازاً مخصصاً قائماً بذاته، إلا أنه لا يجاريه من حيث سرعة معالجة البيانات أو تعدد الخدمات المقدمة، ولهذا فإنه اقل سعراً من سابقه.
C. جدران نارية لحماية الأجهزة الشخصية: أغلبها برامج تحمل في الحاسوب الشخصي، بحيث تمر من خلالها جميع المعلومات الخارجة من الحاسوب أو الداخلة إليه.
يقدم هذا النوع عدة خدمات كغربلة الظروف والحماية ضد الفيروسات وحماية البريد الالكتروني والتشفير والوقاية من برامج التجسس ، يمكن تحميلها من شبكة الانترنت.

- خلاصة:

بسبب كثرة الأخطار التي تهدد شبكات المعلومات ، نشأت فكرة إقامة جدران الحماية التي تسمى أيضاً الجدران النارية، التي يمكن وصفها بأنها نظام مؤلف من برنامج يعمل في حاسوب، وهذا الحاسوب قد يكون حاسوباً عادياً كالحواسيب الشخصية أو حاسوباً بني بمواصفات خاصة ليكون اكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية، وتتعدد أنوعها بحسب حجم منظومة المعلومات المراد حمايتها والتقنية المستخدمة، ويجب التأكيد على أهمية وجود جدران الحماية الشخصية بوصفها أحد خطوط الدفاع الأخيرة.