كيف يعمل تعد جدران الحماية قياسية في أنظمة الكمبيوتر والشبكات المحلية والشبكات الخاصة. ولكن كيف يمكنهم إيقاف المتسللين أو البرامج الضارة؟ هناك – كما يمكنك أن تتخيل – عدة طبقات لهذا الأمر، لذا سنحاول تقسيمها دون أن يصبح الأمر مربكًا للغاية. بالنسبة للمبتدئين، سيتحقق جدار الحماية من كل حزمة، وإذا كانت تفي بمعايير التصفية، بشكل عام، يحتوي برنامج جدار الحماية على معايير موجودة مسبقًا للحماية من محاولات التطفل الواضحة، مثل مواقع الويب المليئة بالبرامج الضارة وبرامج الاختطاف والاتصالات غير المعروفة. لكن جدران الحماية تسمح أيضًا بمرشحات مخصصة أيضًا، والتي يمكنها حظر الوصول/الحزم حتى لو لم تكن محددة مسبقًا في الأصل. يعد هذا إجراءً أمنيًا قياسيًا. ومع ذلك، تصبح الأمور معقدة. مع عدم وجود جدار حماية، وحسنًا، لذلك، يتم إنشاء جدار حماية لمراقبة كل اتصال. سيكون لكل اتصال قواعد، المعايير التي ذكرناها من قبل. ستختلف جميع القواعد بناءً على المستخدمين والاتصالات التي تحددها إدارة تكنولوجيا المعلومات. هنا مثال: يتم منح الوصول عن بعد لمجموعة من أجهزة الكمبيوتر في شبكة الشركة، مما يسمح لمتخصصي تكنولوجيا المعلومات بالوصول إلى الأنظمة لتقديم المساعدة. يتم منح الوصول بناءً على مجموعة القواعد، مثل البروتوكول ومصدر IP والمنافذ. الحزم لقد ذكرنا مصطلح "الحزم" عدة مرات. هذه طريقة للإشارة إلى حزم TCP (بروتوكول التحكم في النقل). فكر فيها مثل الصناديق الصغيرة التي تحتوي على معلومات. يمكن أن تحتوي المعلومات على جميع أنواع الأشياء،