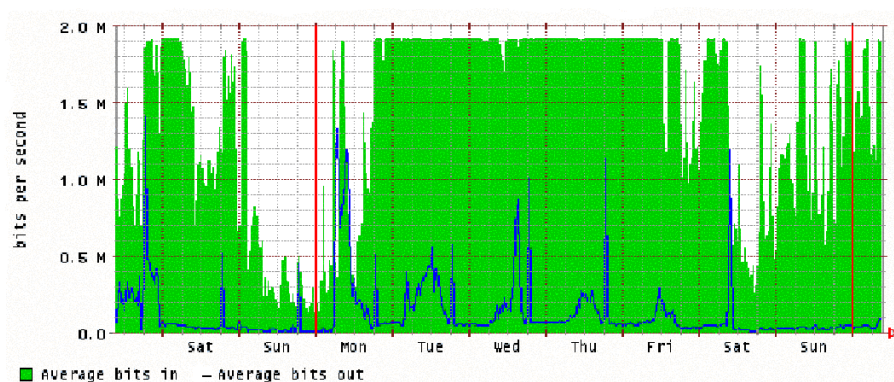


Unusual Traffic

On most network access links the traffic flowing in and out shows a similar pattern. Most communications consist of a request going in one direction and a response coming back in the other. The size of the request and response may be different but the pattern of traffic in time should be roughly similar. However, sometimes the inbound and outbound patterns are completely different. This often indicates that there is a security problem somewhere on the network that needs urgent attention.



The graph above, from the JANET Netsight service, shows a very odd traffic pattern on a site access link. The black line shows a normal pattern of traffic from the JANET backbone into a site – busy during working hours and quiet at night and weekends. The grey trace, of traffic from the site to JANET, has no daily pattern and in fact shows the site filling its access link with packets for nearly four days.

Imbalances in traffic have a large number of possible causes, but most are the result of a small number of well-known problems. These are the first things a site should check when it sees an unusual traffic flow.

When an unusual flow occurs it is important to identify the source within the site quickly. Most routers can report which addresses are generating and receiving traffic; some sites set up a dedicated computer to monitor traffic flows. As a last resort flows can be traced using temporary access control lists on routers, but this takes a lot of effort. It is well worth practising tracing flows before it has to be done in an emergency. Once the type of computer responsible for the traffic has been determined, the following are the most likely causes.

Web server

Vulnerabilities in web servers often allow a web request to run a command on the server. This can be used to perform denial of service attacks or other types of misuse. Evidence of misuse should be clearly visible in the web server logs (look for cmd.exe or /bin/sh). Patches for such vulnerabilities can be found at:

<http://www.ja.net/cert/>

Public web servers are a popular target for intruders and maintenance is essential to keep them secure. When patches are announced by software and operating system vendors, they should be tested and installed as soon as possible. Once a server has been misused it is too late to just patch it. It must be rebuilt from scratch.

Mail server

The server is probably misconfigured and is being used to relay Unsolicited Bulk E-mail (UBE, or 'spam'). The configuration must be corrected as soon as possible. The server will probably not have been compromised but it should be monitored carefully to check for any further suspicious activity. For details see:

<http://www.ja.net/cert>

or:

<http://www.ja.net/services/network-services/mail/anti-spam/STAN.html>

If the server was reported to UBE black-lists then it must be removed from those lists or sites will reject mail from it.

File Transfer Protocol (FTP) server

It is likely that the server was mis-configured with an anonymous upload area that was publicly readable. Such sites are often taken over for the distribution of illegal material, often pirated software or pornography. The configuration must be corrected and unauthorised material removed. Upload areas may be created during break-ins or as a result of worm attacks. In this case the system will need to be rebuilt.

Workstation

A user has probably run a peer-to-peer file sharing program that is now serving files to others. Sites should have a policy for peer-to-peer systems. Procedures to deal with any copyright material are strongly advised and technical controls to conserve network bandwidth may be needed. For details of popular software see:

<http://www.ja.net/cert>

Alternatively the system may have had a 'back-door' program or 'bot' installed during a break-in. Such programs can be used to perform denial of service attacks, to relay junk mail or many other types of misuse. Such systems must be rebuilt and secured from scratch.

Packets coming randomly from all addresses on a subnet

This pattern is normally due to a distributed denial of service tool that is forging packets. The tool may have been installed by a user running a virus or Trojan, or by an intruder who has succeeded in breaking in. A Guidance Note, investigating a denial of service attack, can be found at:

<http://www.ja.net/services/publications/technical-guides/gn-ddos.pdf>

Further information

For further information on tracing flows please see the following websites:

JANET Netsight

<http://www.ja.net/services/network-services/netsight/>

Cisco IOS Netflow®

http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

List of tools

<http://www.switch.ch/tf-tant/floma/software.html>

Cisco® information on characterizing and tracing packet floods

<http://www.cisco.com/warp/public/707/22.html>