packet filtering

Definition of packet filtering in The Network Encyclopedia.

packet filtering

The process of controlling the flow of packets based on packet attributes such as source address, destination address, type, length, and port number.

How It Works

Many routers and proxy servers use some form of packet filtering that provides firewall capabil ties for protecting the network from unauthorized traffic. Administrators can create rules for filtering out unwanted packets and can arrange these rules in the most efficient order. A packet that passes all the rules is allowed through, while a packet that violates any rule is dropped.

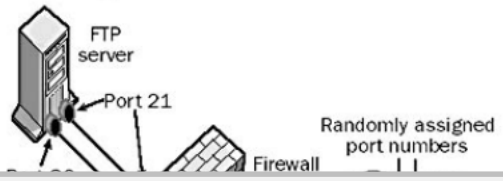
Packet filtering can be implemented on routers and firewall devices in two ways: static filtering and dynamic filtering.

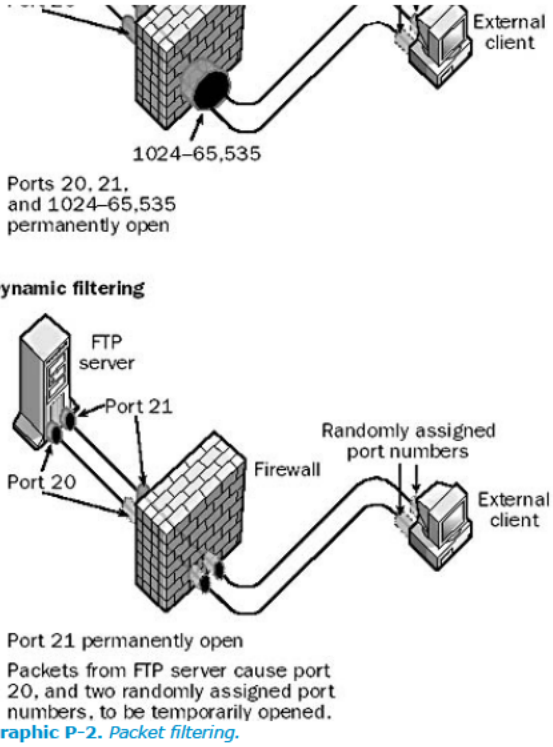
Stat c packet filtering prov des limited security by configuring selected ports as either permanently open or permanently closed. For example, to deny outside packets access to a company intranet server on port 80 (the standard port number for the Hypertext Transfer Protocol, or HTTP) you could configure the router or firewall to block all incoming packets directed toward port 80.

Dynamic packet filtering provides enhanced secur ty by allowing selected ports to be opened at the start of a legitimate session and then closed at the end of the sess on to secure the port against attempts at unauthorized access. This is part cularly useful for protocols that allocate ports dynamically—for example, with the File Transfer Protocol (FTP). If you want to grant outside users secure access to an FTP server behind the firewall (within the corporate network), you need to cons der the following:

- Port 21 (the FTP control port) needs to be left permanently open so that the FTP server can "listen" for connection attempts from outside clients. A static filtering rule can accomplish this.
- Port 20 (the FTP data port) needs to be opened only when data will be uploaded to or downloaded from the FTP server. With stat c filtering this port would have to be configured as permanently open, wh ch could provide a door for hacking attempts. Dynamic filtering allows this port to be opened at the start of an FTP session and then closed at the end of the sess on.
- In order to establish an FTP connection with the client, the FTP server randomly assigns two port numbers in the range 1024 through 65,535 to the client, one for the control connection and one to transfer data. Because these ports are assigned randomly, there is no way to predict which ports above 1024 must be able to be opened by the firewall. W th static filtering, you would therefore have to leave all ports above 1024 permanently open if you wanted to allow FTP access through the firewall, which would be a real security risk. W th dynam c filtering, however, you can configure rules on the firewall that will read the packets issued by the server, dynam cally open the two randomly assigned ports to allow a session to be opened, monitor the flow of packets to ensure that no attempt is made to hijack the session by an unauthorized user, and close the randomly assigned ports when the FTP session ends.

Static filtering





Graphic P-2. *Packet filtering.*

TIP

Microsoft Proxy Server includes a number of predefined filters that you can use to configure exceptions for common protocols. You can use these to quickly configure Proxy Server for securing your network from the Internet.

Packet filtering on a typical router can cause a performance hit of about 30 percent on the router's ability to handle network traff c. This suggests that instead of using a packet-filtering router for a firewall, you should consider installing proper firewall software such as Microsoft Proxy Server on a dedicated server. Proxy Server includes dynamic packet filtering among its security features. If packet filtering is enabled, all incoming and outgoing packets are rejected unless an except on is expl c tly created that allows them to pass. Packet filters can be enabled on Proxy Server only if the machine has an external network interface, such as one connected to a distrusted network (the Internet, for example).

NOTE

Some routers and firewalls can actually ping the source address of each packet to ensure that addresses local to the company network are coming from inside the network and are not being spoofed by a hacker outside the network.

Proxy Server also supports domain filters for allowing or denying access to World Wide Web (WWW) or FTP services based on the source IP address or Domain Name System (DNS) domain name. Proxy Server can issue alerts to inform you when packets are rejected or illegal packets are detected. It will also keep a log of alerts that occur for analysis and record keeping.

Link to this page

You are welcome to link to this page, or to any other page from this website. Please, feel free to copy the html code below and past it to any place in your site or blog.

```
<a
href='http://www.thenetworkencyclop
edia.com/entry/packet-
filtering/'>packet filtering in
```

Left Click to select, then right Click and Copy the Html Code!

For other webmaster tools click here »
To add this page to your favorites cl ck here »

Technology Trends

Cloud
Virtualizat on
IPv6
Open Network Environment

Manufacturers

Cisco Systems
HP (3COM)
D-Link
Dell
ZyXEL

Links