

## CREATING HOST-BASED PACKET FILTERS IN WINDOWS 2000

*Products: Windows 2000 Server or Advanced Server*

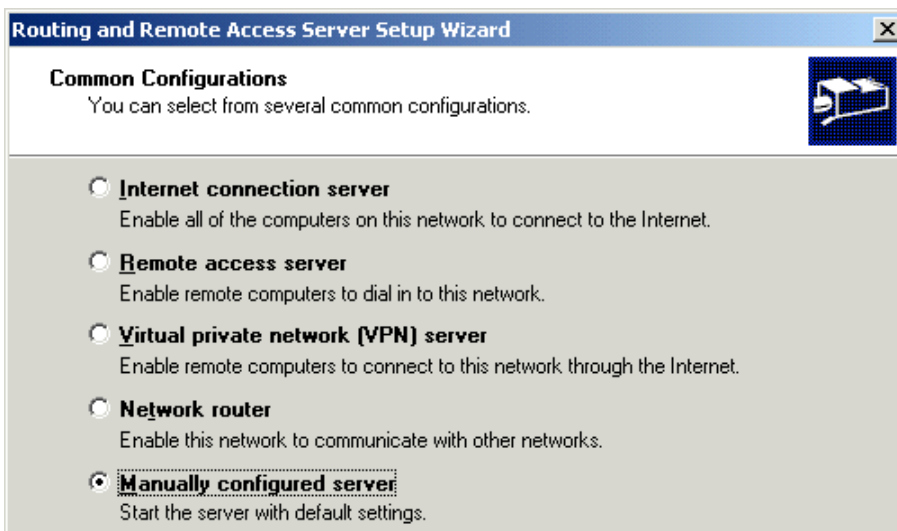
### Overview

Windows 2000 Server and Advanced Server ship with the Routing and Remote Access Service (RRAS), which allows Windows 2000 to act as a LAN router, demand-dial router, or VPN router (or any combination). However, RRAS is not limited to running on servers with multiple interfaces; it can also run on servers with a single network interface. In this case, RRAS' packet filtering capabilities can be applied to this single network interface to create host-based packet filters that can allow or deny traffic based on the source address, protocol, source port, or destination port.

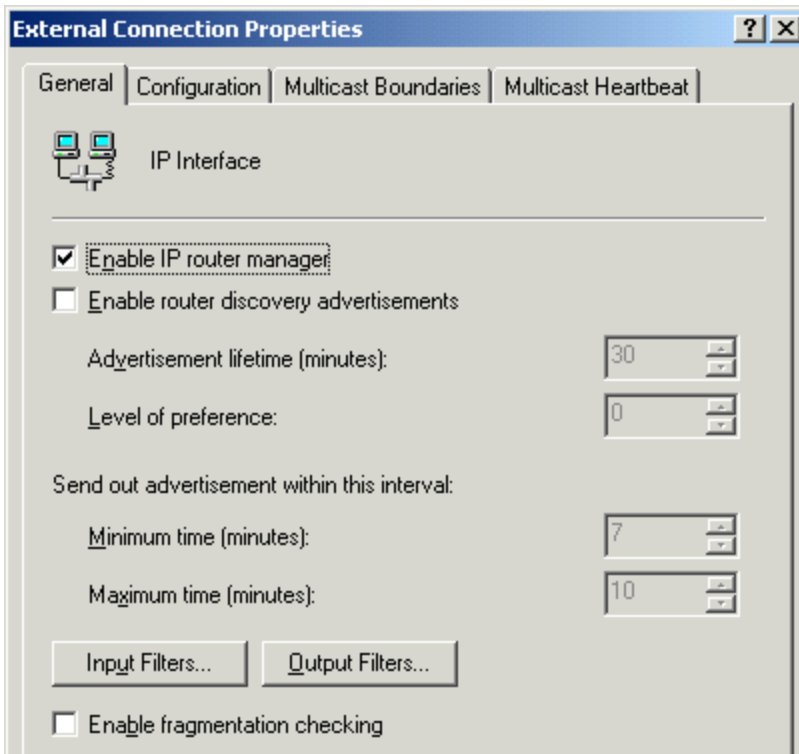
These host-based packet filters can be combined with other methods of network security, including perimeter firewalls and network intrusion detection systems, to provide added security for Windows 2000-based servers. The ability to set host-based packet filters is especially useful in securing bastion hosts placed in the DMZ or in parallel to a firewall.

### More Information

RRAS is installed and configured using the Routing and Remote Access console, available from the Administrative Tools menu. To use RRAS for host-based packet filters, select the "Manually configured server" from the wizard, as shown below.



After RRAS has been installed and configured, packet filters can be added to the network interface to screen traffic. Find the network interface under IP Routing > General, right-click the network interface, and choose Properties. On the Properties dialog box, there are buttons for input filters (traffic inbound on the interface) and output filters (traffic outbound on the interface). The screenshot below illustrates the properties dialog box and the buttons for input and output filters. In most cases, host-based packet filters will be created as input filters, so that only certain types of traffic from certain hosts or networks are accepted by the server.



In the Input Filters or Output Filters dialog box, packets can be accepted by the interface or dropped by the interface based on a number of different criteria. Some of these criteria are discussed in the following list.

- *Source network:* This filters packets based on the source address. This can be a specific host address (using the source host's IP address and a subnet mask of 255.255.255.255, meaning all bits are significant) or a network address. By filtering on source address, Windows 2000 will automatically accept or drop packets based on where the packets are coming from. For example, a server might be configured to drop all packets except those packets originating on the same subnet as the server. Because the packet filters being created are host-based, filtering by source network is really only effective when used in an input filter.
- *Destination network:* In contrast to source network, filtering by destination network is typically only effective when used in an output filter. Filtering by destination network could be used to prevent a server from offering certain types of services to remote hosts or networks. As with source network, a mask of 255.255.255.255 is used to denote a specific host address in the filter properties.
- *Protocol:* Filtering by protocol provides the ability to control what types of traffic are accepted by the server. Selecting a protocol other than "Any" also allows the source and

destination ports (for TCP, TCP [Established], and UDP), type and code (for ICMP), or protocol number (for Other) to also be specified. Typically, filters would be created based on TCP and UDP ports.

The following table provides the well-known ports that a typical Windows 2000 domain controller shows as open with a TCP connect() port scanner.

Service	Port	Service	Port
ftp	TCP port 21	https	TCP port 443
http	TCP port 80	microsoft-ds	TCP port 445
kerberos	TCP port 88	kpasswd	TCP port 464
epmap	TCP port 135	http-rpc-epmap	TCP port 593
netbios-ssn	TCP port 139	ldaps	TCP port 636
ldap	TCP port 389		

The names listed for the services above were taken from the Internet Assigned Numbers Authority (IANA) port list, available from <http://www.iana.org>. IANA can also provide complete details on the ICMP types and codes for use in creating ICMP packet filters.

By using any or all of these criteria in an input or output filter, a Windows 2000-based server can be secured against unwanted and unnecessary network traffic. For example, suppose that a Windows 2000-based web server was deployed in a network. In addition to specifying rules on a firewall to control the type of traffic allowed to that IP address, an input filter could be created with the following criteria:

- Source network: Leave this option unchecked, to allow traffic from any source network or host.
- Destination network: Leave this option unchecked, to allow traffic to any source network or host (not applicable in an input filter).
- Protocol: Set to TCP and specify port 80.

This input filter prevents the Windows 2000-based web server from accepting any traffic other than traffic destined for TCP port 80 (HTTP).

## Other Notes

The RRAS console can also be used to manage remote computers also running RRAS. This allows an administrator to administer host-based packet filters on a number of Windows 2000-based servers from a single console. RRAS does not, however, provide for a mechanism of automatically distributing changes to host-based packet filters.

Using RRAS for host-based packet filters is not without its limitations. There is no ability, for example, to use the “NOT” keyword in the rules. This would make it easier to define certain types of rules; e.g., a rule to accept only HTTP traffic from source networks that are not the local subnet. For more sophisticated rules such as this, a host-based firewall must be deployed.

Note that it is also possible to create host-based packet filters using IPSec policies. This technique would also work on Windows 2000 Professional-based computers, whereas the RRAS solution described above only works with the Server and Advanced Server editions of Windows 2000. Although more limited in the types of packet filters that can be created, IPSec policies can be distributed via Active Directory Group Policy Objects (GPOs), where RRAS packet filters cannot.

For additional information on packet filtering with Routing and Remote Access, also see the technical document titled "Filtering TCP/IP Traffic with RRAS."

### **Related Articles/Resources**

None

### **Legal Information**

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.