

Compatible Systems Tech Notes: Adding Packet Filters using CompatiView

Document ID: 17665

Introduction
Prerequisites
Requirements
Affected Products
Affected Versions
More Information
Related Information

Introduction

This document discusses how to add packet filters using CompatiView v4.x and v5.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Affected Products

900i, 1200i, 1220i, 1250i, 1270i, 2600i, 2900i, 2200R, 2220R, 2250R, 2270R, 3500R, 3800R, VSR-2, and VSR-8

Affected Versions

All versions

More Information

You can add filters to a device using CompatiView. Filters are directional so that they either filter traffic that goes into the router on a particular port (an input filter) or filter traffic that leaves the router (an output filter). First you need to create the filter, then apply it as input or output to a particular port.

In CompatiView v4.x, open up the device and go to the TCP/IP Filtering column and the All row and double click. Then click on the **Packet Filters** button. This opens a new window where you can create the packet filter. Click on the **New** button and name the filter up to 16 characters with no spaces and hit **OK**. Then in the large white box that is now revealed with the cursor, type in your filter set.

When finished, click **OK**, and then click **OK** again. Now you need to apply the filter you have created to a port as either input or output. Then in the TCP/IP Filtering Column and the row of the port you wish to apply the filter, double click to open that box. In the Column for either the input or output Filters, use the pulldown to select the filter you have created. Once you see that your selection is correct, hit **OK**. Now you can save the

configuration to the device and it restarts itself and applies your new filter.

In ComatiView v5.x, open up the device and go to the Global/Filtering/TCPIP Filtering and click the **Packet Filters** button. This opens a new window where you can create the packet filter. Click on the **New** button and name the filter up to 16 characters with no spaces and hit **OK**. Then in the large white box that is now revealed with the cursor, type in your filter set.

When finished, click **OK**, and then click **OK** again. Now you need to apply the filter you have created to a port as either input or output. Open up the port you want to apply it to, say Ethernet 0, and go into the Filtering/TCPIP Filtering section. In the Column for either the input or output Filters, use the pulldown to select the filter you have created. Once you see that your selection is correct, hit **OK**. Now you can save the configuration to the device and it restarts itself and applies your new filter.

It is usually recommended to design your filter as an "input" filter for the port closest to the Internet.

A generic filter that helps protect your network from common attacks, but lets through the most common Internet traffic is this "INPUT Filter" for the port closest to the Internet:

```
#anti-spoofing filter
deny a.b.c.d/e 0.0.0.0 ip
allows #responding packets for tcp sessions originating from your net
permit 0.0.0.0 0.0.0.0 tcp est
dns from other servers
permit 0.0.0.0 0.0.0.0 udp src = 53
email to your smtp servers
permit 0.0.0.0 0.0.0.0 tcp dst = 25
email from outside smtp servers
permit 0.0.0.0 0.0.0.0 tcp src = 25
access to your web servers
permit 0.0.0.0 0.0.0.0 tcp dst = 80
allow established internal connections, required for both FTP Modes
permit 0.0.0.0 0.0.0.0 tcp est
allow internal access to internet Normal Mode FTP Servers
permit 0.0.0.0 0.0.0.0 tcp src = 20
allow internet access to an internal FTP Server
permit 0.0.0.0 0.0.0.0 tcp dst = 21
permit 0.0.0.0 0.0.0.0 tcp src > 1023 dst > 1023
email to your pop server
permit 0.0.0.0 0.0.0.0 tcp dst = 110
email from outside pop server
permit 0.0.0.0 0.0.0.0 tcp src = 110
ports and protocols for the Intraport VPN Server
permit 0.0.0.0 0.0.0.0 UDP dst = 500
permit 0.0.0.0 0.0.0.0 proto = 50
permit 0.0.0.0 0.0.0.0 proto = 51
everything else will be automatically denied
```

a.b.c.d is the network IP address and e is the number of bits in the subnet mask (usually /24 for a class C network).

Related Information

- [Technical Support & Documentation – Cisco Systems](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.
