Global Information Assurance Certification Paper

Improved Filtering on the Firewall Routers
Fixing the "Bad Ping Filter"

Abstract:

More and more there are an increasing number of IP routers that offer packet filtering as a tool to improve total network security. When administrators use this properly, packet filtering can be a very secure and useful tool. To make it totally effective it requires a thorough understanding of its capabilities and weaknesses, as well as the strange behaviors of particular protocols that you would apply these filters to. This paper will identify and examine problems common to many current packet filtering implementations and simple steps to correct these common configuration errors.

OBJECTIVE:

1. Fixing "ping filters" that are already incorrectly configured and implemented
2. See that all future ping filters follow the guidelines set here.

Introduction:

Numerous perimeter routers have packet filters ostensibly set up to allow pinging. They are configured to allow ICMP type 0 and 8, but this is in error. Almost all ICMP traffic is of ICMP type 0. The filters should be configured to allow ICMP traffic with *ICMP type* 0 and 8, which are echo reply and echo request, respectively.

Unfortunately it may cause problems if one goes in and just "fixes" the filter. Because the filter has been broken from the onset, legitimate traffic flows may have come into place without there needing to be changes implemented in the filters applied to that interface. This is explained further in "procedural considerations" below.

Correct Filter Configurations:

1. Set IP Protocol ID equals to 1 (just allow ICMP traffic).
2. Set user-defined IP criteria

EXAMPLES:

If an interface has a filter with type of service criteria equals to 0 and 8 that will open an interface for almost all IP packets. To fix it we need to delete service-type entry and set IP Protocol ID to 1 for ICMP traffic.

The following example has a "bad filter":

wfIpTrafficFilterEntry Entry
wfIpTrafficFilterInterface = 129.111.72.1
wfIpTrafficFilterCircuit = "WILCOP_ENET"
wfIpTrafficFilterRuleNumber = 2
wfIpTrafficFilterFragment = 1
wfIpTrafficFilterDefinition =
service-type: 0,8
Src-addr: 129.111.72.1,129.111.72.10
Dst-addr: 100.107.53.0-147.107.53.255,100.232.50.128,100.232.50.108,100.232.50.157-100.232.50.159,100.232.50.35,100.232.50.65,100.232.50.166
Action: ACCEPT;
wfIpTrafficFilterName = "Ping_Wilcop_Enet"

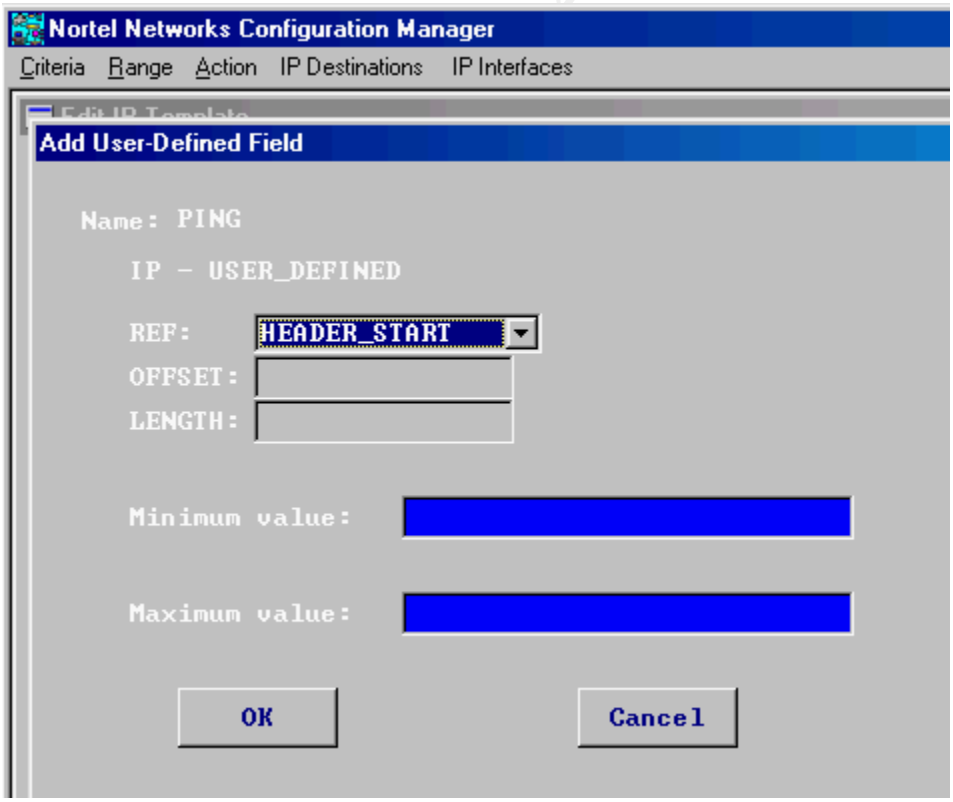
The next example explains how to fix it:

wfIpTrafficFilterEntry Entry
wfIpTrafficFilterInterface = 129.111.72.1
wfIpTrafficFilterCircuit = "WILCOP_ENET"
wfIpTrafficFilterRuleNumber = 2
wfIpTrafficFilterFragment = 1
wfIpTrafficFilterDefinition =
Src-addr: 129.111.72.1,129.111.72.10
Dst-addr: 147.107.53.0-147.107.53.255,100.232.50.128,100.232.50.108,100.232.50.157-100.232.50.159,100.232.50.35,100.232.50.65,100.232.50.166
Protocol: ICMP
Action: ACCEPT;
wfIpTrafficFilterName = "Ping_Wilcop_Enet"

To create an IP traffic filter with user-defined criteria we need to set an offset and length to these reference fields in the IP header:

Reference Field	Description
HEADER_START	Points to the first byte of the type of Service (ToS)
HEADER_END	Points to the last byte of the IP Destination Address

The following picture shows how to implement it using Nortel Networks Configuration Manager.



PROCEDURAL CONSIDERATIONS

Suppose the following scenario:

- Day 1: Filters were placed on the firewalling router that allowed end-user traffic flow (A) and pinging. The filter for (A) was properly implemented, but the ping filter was our problematic filter.

- Day 2: The 3rd party states that it needs end-user traffic flow (B). A project is initiated to add a filter to allow this flow, but to work properly traffic flows (B) and (C) were required. Only a filter for (B) was implemented, but (C) worked too because of the bad ping filter, which allowed flow (C).

- Day 3: A server was added for flow (B), which should have required a filter change, but because of the bad ping filter, application support found that they did not need to engage communications. It worked just fine without an adjustment to the filter.

- Day 4: The ping filter is fixed. Flow (C) fails, and flow (B) fails for the one server. Also, there is a flow (D) that stops working, although it shouldn't be there.

To avoid this problem, it is going to be necessary to review the actual traffic flows prior to implementing the fix. The basic procedure would be:

1. Determine the actual traffic flows using probes or sniffers.
2. Review those traffic flows against those specified in the filters.
3. If there is a discrepancy, review the differences with whoever is providing application support. This will enable you to ascertain if there are traffic flows like (D) above or whether the only distinctions are like those for flows B and C.
4. Implement the proper changes.

References:

http://www.ja.net/CERT/Chapman/Packet_Filtering_Insecurity.htm

http://www.interhack.net/pubs/network-security/

http://www.dnpg.com/dr/routeabout/manuals/ra-isdn/protocol/ipfiltr3.htm

http://www.tis.com/support/ping.html

http://www.livingston.com/tech/docs/pm4-config/filter.html