IP Address Spoofing Filters Policy

Revised to remove obsolete use of "affiliate", September 2013
Prior version, September 1998

Merit's policy on packet filtering is designed to protect against IP address spoofing-that is, sending IP packets that use source addresses which are not assigned to the part of the Internet where the packets originate. We are asking Members with direct LAN attachments to Merit's backbone routers to install packet filters in their own routers (see item #3 from policy). Questions regarding this policy should be directed to your Member Services Support Team.

Discussed and approved by the Merit Joint Technical Staff (MJTS) at their September 17, 1998 meeting.

1. On tail routers at Member sites, Merit will install both the "self defense" and "good citizenship" packet filters. These filters will be installed at the router's serial interface and will check the source IP addresses on both inbound and outbound packets. For packets going from Merit to the Member , Merit will reject packets that have a source address that is assigned to the Member as well as ICMP ping packets with a destination address that is the broadcast address. For packets going from the Member to Merit, Merit will reject packets that do NOT have a source address that is assigned to the Member as well as ICMP ping packets that have a destination address that is the broadcast address.

2. In cases where Member LANs are connected directly to a Merit's backbone router, Merit will install both the "self defense" and "good citizenship" packet filters on the LAN interface.

3. In cases where Member LANs are directly connected to a backbone router AND the backbone router is used to route traffic between the organization's sub-networks, it will not be possible to install the "self defense" packet filters. In these cases the Member should install the filters on their own routers or contact Merit to develop alternatives.

4. The packet filters that will be installed by Merit provide protection at the gateway that connects a Member organization. We encourage Members to seriously consider installing similar packet filters on their own internal routers. For large organizations, installing filters that protect smaller portions of their networks is likely to be much more effective than filters which are designed to protect the network as a whole.

5. From time to time Merit is asked to install specific packet filters by a Member. These filters are often related to network security in some way. In general we discourage Members from using these sorts of non-standard filters in routers managed by Merit, since it is not considered good practice to depend on an outside party such as Merit to implement an organization's internal security policies. However, while we continue to discourage the use of non-standard filters, Merit will install non-standard packet filters on tail routers managed by Merit at a Member's site on request. There will be a fee of $100 a month to install and maintain these non-standard filters. There will be an additional consulting fee of $75 per hour if the Member needs help in designing or specifying these non-standard filters. Merit will NOT install non-standard filters on backbone routers.

Policy Explanations

Merit installs route filters that prevent a Member from announcing routes for IP addresses that they do not own. While route filters are very useful, they do not protect against the same problems that packet filters do.

Packet filters will help do two things:

- Protect our Members from "bad" packets that originate elsewhere; and

- Protect others from “bad” packets that originate at one of our Members.

Thus we have both “self defense” and “good network citizenship” as motives for doing this work.

The “self defense” filters do not prevent spoofing of all Internet addresses, only those of the Member IP addresses, and then only within their own network. In fact, all they protect against is attacks on machines that use local source IP addresses to authenticate (some UNIX systems with rlogins and rsh enabled, some X Windows servers, ...). Thus, “self defense” filters prevent your own IP addresses from being used against you from outside of your network, but they do NOT prevent someone else’s IP addresses from being used against you nor do they prevent your own IP addresses from being used against you from within your own network.

“Good citizenship” filters protect more broadly, but will only be 100% effective only if these filters are installed everywhere throughout the entire Internet.

Merit will do the following under its IP Address Spoofing Filters Policy:

Tail Routers	
Self Defense:	Yes
Good Citizen:	Yes
Non-standard:	Reluctantly, for an extra charge
Backbone Routers	
Self Defense:	Yes
Good Citizen:	Yes
Non-standard:	No

Merit Network, 1000 Oakbrook Drive, Suite 200, Ann Arbor, Michigan 48104-6794
Phone: (734) 527-5700 E-mail: info@merit.edu Web: www.merit.edu

merit