

Chapter Five (a): Description of the Trust Groups

Summary of Chapter:

- ⓘ A definition of each Trust Group that is in the firewall.

Software Revision Required:

- ⓘ Applicable to software revision 5.2.0 > NetPilots

Definitions:

Trust Group: A Trust Group is a group of IP addresses.

Using Trust Groups makes it easier to set up complex permissions by treating groups of addresses in the same way. A single firewall always applies the same set of rules to packets traveling between hosts of different Trust Groups.



We supply a useful collection of Trust Groups and firewalls, which we believe are ideally suited to the most common network scenarios.

Admin: Admin is a special group for Internet hosts that are allowed to use the NetPilot's technical support and administration features remotely.

This group is initially supplied with Equinet's address. A provider of a managed service may wish to add his or her own addresses to this group.

Controlled: Controlled is primarily intended for use where a single organization contains one or more parts, which should be segregated from the others.

Controlled hosts may still have access to all NetPilot services and to the Internet; however, they cannot talk to trusted hosts or to other controlled hosts through the NetPilot. This provides a suitable environment for schools, where individual classrooms should be separate from each other and from the teachers' or administration networks.

We would suggest using this profile on LAN 3 (if fitted), or for hosts connected via VPN tunnels where the VPN clients need access to NetPilot services such as email, but not to other hosts on the LAN.

DMZ: DMZ is designed to provide some safety even when hosts local to the organization must face the world directly.

The assumption is that machines on the DMZ may be compromised, so traffic from the DMZ is not permitted to enter the rest of the organization. These hosts should be placed on a separate DMZ LAN. Only trusted hosts can make connection to DMZ hosts. Selected services may be offered from DMZ hosts to the Internet (ICMP, SMTP, remote desktop, secure shell, secure web, web, FTP, Lotus Notes, VNC, POP, IMAP). We suggest using this profile on LAN 3 (if fitted).

Friends: Friends is a group of hosts on the Internet, which can be given some extra access to the NetPilot or to the networks behind the NetPilot.

The NetPilot's administrator can add individual IP addresses to this list, which is initially empty; therefore no addresses have extra access at default level.

The extra access offered is:

- NetPilot will respond to ICMP ECHO (ping)

- NetPilot may accept incoming SMTP email destined for local users

- NetPilot may forward SSH Secure Shell traffic to the internal network

- NetPilot may forward VNC remote desktop traffic to the internal network

One uses of this would be to accept email from a foreign mail host (such as an ISP). Another might be to offer remote access to hosts behind the firewall.

Internet: Internet is the default Trust Group to which all hosts belong because it matches any address. It is used to set the permissions for all hosts not covered by one of the more specific Trust Groups.

Local: The Local Trust Group represents the NetPilot itself. It appears in the firewall overview, but because of its special meaning, it can't be assigned additional addresses like the other Trust Groups.

Trusted: Trusted is the normal Trust Group for hosts on the LAN 1 subnet.

These hosts may have access to all NetPilot services and to the Internet. Trusted hosts are permitted to talk to each other, whatever network they come from. This Trust Group may be used for hosts connected via VPN tunnels.



Tip!

With an advanced license the user can create new Trust Groups and firewalls.



Information

Setting the Trust Group of a Ethernet connector (e.g. LAN 1) to `Trusted' means that addresses in the same range as the connector itself are trusted, not that all packets entering via that connector are trusted. Packets, which enter via that connector whose source address is not in the same range as the connector, will be discarded unless they match another route---in which case the route will specify the Trust Group to use.