

The Identification (IDENT) Authentication (AUTH) Protocol

By Mark E. Donaldson

THE PROTOCOL

The IDENT (AUTH) protocol is often necessary for the smooth performance and functioning of certain services such as mail, POP3, and IRC. For instance, when sending outgoing mail, the receiving mail server, particularly if it's a sendmail server, will attempt to IDENT the sending mail server on TCP 113 SYN.

THE PROBLEM

Problems occur when the incoming IDENT SYN packets are dropped at the firewall, as the receiving mail server will wait for a SYN/ACK reply to the TCP 113 connection request until it times out.

SECURITY

IDENT is a security concern so IDENT requests must not be answered, and yet they cannot be dropped if service is to function properly.

SOLUTIONS

1. If the firewall has the capability, REJECT instead of DROP IDENT requests at firewall, and return a RESET/ACK back to the requesting server. The server will then be satisfied and continue processing the delivery.
2. If the firewall does not have this capability, a TCP 113 hole must be poked through the firewall for INBOUND. IDENT requests. Then direct the TCP 113 requests to the mail relay server wherein the IDENT service has been disabled. The non-listening IDENT port on the server will then cause the TCP stack to return a RESET/ACK packet to the requesting server.

OUTBOUND

OUTBOUND IDENT requests (TCP 113) must also be allowed through, as well as INBOUND IDENT replies, high port RESET/ACKS, and ICMP "port unreachables".

EXAMPLES

```
# allow inbound IDENT requests and route to mail relay mail relay will return RESET/ACK
permit in on eth1 any port > 1023 to 66.14.166.45 port = 113
permit out on eth1 66.14.166.45 port 113 to any port > 1023
```

```
# allow established outbound IDENT from mail relay
permit in on eth1 any port 113 to 66.14.166.45 port > 1023 established
permit out on eth1 66.14.166.45 port > 1023 to any port = 113
```