

ICMP Packet Filtering

Blocking inbound or outbound ICMP can often be a semi-"religious" issue in some organisations. Most network administrators strongly believe they should have ICMP echo capabilities for network debugging purposes, while security administrators tend to limit even this seemingly benign traffic to what is strictly necessary, as even this can be abused by network tunneling applications.

Below, we will try to maintain a no-nonsense approach to filtering ICMP error messages. Every Network Administrator should keep these in mind as "guidelines", but deviation can always be necessary for specific networks.

List of ICMP Types and Codes

Type 0 Echo-reply
Type 1 Unassigned
Type 2 Unassigned
Type 3 Destination-unreachable
Code 0 network-unreachable
Code 1 host-unreachable
Code 2 protocol-unreachable
Code 3 port-unreachable
Code 4 fragmentation-needed
Code 5 source-route-failed
Code 6 network-unknown
Code 7 host-unknown
Code 8 network-prohibited
Code 9 host-prohibited
Code 10 TOS-network-unreachable
Code 11 TOS-host-unreachable
Code 12 communication-prohibited
Code 13 host-precedence-violation
Code 14 precedence-cutoff
Type 4 Source-quench
Type 5 Redirect
Code 0 network-redirect
Code 1 host-redirect
Code 2 TOS-network-redirect
Code 3 TOS-host-redirect
Type 6 Alternate Host Address
Type 7 Unassigned
Type 8 Echo-request
Type 9 Router-advertisement
Type 10 Router-solicitation
Type 11 Time-exceeded
Code 0 ttl-zero-during-transit
Code 1 ttl-zero-during-reassembly
Type 12 Parameter-problem
Code 0 ip-header-bad
Code 1 required-option-missing
Type 13 Timestamp-request
Type 14 Timestamp-reply
Type 15 Information Request
Type 16 Information Reply
Type 17 Address-mask-request
Revised July 12, 2009

ICMP Packet Filtering

Type 18 Address-mask-reply
Type 19 Reserved
Type 20-29 Reserved
Type 30 Traceroute
Type 31 Datagram Conversion Error
Type 32 Mobile Host Redirect
Type 33 IPv6 Where-Are-You
Type 34 IPv6 I-Am-Here
Type 35 Mobile Registration Request
Type 36 Mobile Registration Reply
Type 37 Domain Name Request
Type 38 Domain Name Reply
Type 39 SKIP
Type 40 Security Failures

Clarification per Message

Type 0 Echo-reply

Advisable to allow this inbound from the internet, in order to enable debugging of the internet link (allowing icmp echo requests to the outside). In stricter conditions, this should be allowed from both the perimeter router at your site, as well as from the first hop ISP router which is known, so that during a network outage, you can at least be sure that the connectivity problem is located on the ISP side.

Type 1 Unassigned
Type 2 Unassigned

These are not assigned yet to any type of service, and should not be allowed, neither in, nor outbound.

Type 3 Destination-unreachable
Code 0 network-unreachable
Code 1 host-unreachable
Code 2 protocol-unreachable
Code 3 port-unreachable
Code 4 fragmentation-needed

This message is used for Path MTU discovery (covered in IP Performance Tuning). It should be allowed both in and outbound on your network border. If not allowed, some connections may not succeed (and your network may be considered a PMTU blackhole).

Code 5 source-route-failed
Code 6 network-unknown
Code 7 host-unknown
Code 8 network-prohibited
Code 9 host-prohibited
Code 10 TOS-network-unreachable
Code 11 TOS-host-unreachable
Code 12 communication-prohibited
Code 13 host-precedence-violation
Code 14 precedence-cutoff
Type 4 Source-quench

ICMP Packet Filtering

ICMP type 4, "source quench" is used to decrease the traffic rate of data messages sent to a host. The use of this message for Denial-of-Service reasons is obvious. Due to the availability of more commonly used flow control techniques (ECN), these packets should be discarded at the perimeter.

```
Type 11 Time-exceeded>
Code 0 ttl-zero-during-transit
```

The message "Time exceeded, TTL zero during transit", indicates that a packet was dropped as the TTL of it decreased to 0. It is important to network operations as it will (a) indicate routing loops, and (b) is used by Unix traceroute. Thus, it is advised to allow this traffic for debugging use.

```
Code 1 ttl-zero-during-reassembly
```

This message is better known as "fragment reassembly time exceeded". It is sent out by a host when it receives a fragmented datagram, with some fragments missing, _if_ those missing parts are not received within an operating system specific value of time. This message is also used for operating system fingerprinting, and should be blocked at the perimeter.

```
Type 31 Datagram Conversion Error
Code 0 Unknown error
Code 1 Don't convert option present
Code 2 Unknown mandatory option present
Code 3 Known unsupported option present
Code 4 Unsupported transport protocol
Code 5 Overall length exceeded
Code 6 IP Header length exceeded
Code 7 Transport protocol > 255
Code 8 Port conversion out of range
Code 9 Transport header length exceeded
Code 10 32-bit rollover missing and ACK set
Code 11 Unknown mandatory transport option present
Type 32 Mobile Host Redirect
```

This ICMP type is only used by the IHMP (Internet Mobile Host) application, and should be dropped on the perimeter. If you believe you need this traffic, verify with the paper "IMHP: A Mobile Host Protocol", by David B. Johnson. If in doubt, it should be blocked at the network perimeter.

```
Type 33 IPv6 Where-Are-You
Type 34 IPv6 I-Am-Here
```

These two ICMP types were part of a proposed RFC, which would have made a great addition to the IP version 6 protocol. However, the proposal was discarded and never translated into an RFC, and thus these are once reserved again. No proof-of-concept code is known which actually used this functionality. Drop at the perimeter.

```
Type 35 Mobile Registration Request
Type 36 Mobile Registration Reply
```

Closely related to ICMP type 32, these are used very rarely. Discard at the perimeter.

ICMP Packet Filtering

Type 37 Domain Name Request

Type 38 Domain Name Reply

Described in RFC 1788, ICMP is also capable of transporting reverse DNS lookups. With this new protocol addition, it would be possible for hosts to directly reply with their own reverse DNS record, instead of having to rely on an (already crowded) DNS server. This protocol was never really converted to the application field, and is not used very often by resolver libraries. Thus, it is safe to discard this traffic on your perimeter router.

Type 39 SKIP

These messages are related to the *Simple Key Management Protocol for IP*. SKIP Algorithm Discovery proposes a set of algorithms for a connection. If the destination does not support this algorithm, it responds with an authenticated ICMP message of type 39.

Type 40 Photuris

Code 0 Bad SPI

Code 1 Authentication Failed

Code 2 Decompression Failed

Code 3 Decryption Failed

Code 4 Need Authentication

Code 5 Need Authorization

ICMP Type 40 is used to notify a sender of "security failures". This is all related to the IPSEC standard. Six different Codes are available, of which the first four relate to the SPI. "Need Authentication" indicates that there may not be an SPI present in the original packet, while "Need Authorization" indicates that the SPI value set did not have enough authorization for the attempted encrypted connection (e.g. telnet). These messages are not correctly processed by every IPSEC implementation, and should only be allowed if the VPN connection is having noticeable problems. However, if the destination IPSEC VPN termination point does support them, and the originator of the connection not, they may still be useful for manual debugging (by using a packet sniffer). By default, these messages should be blocked unless deemed necessary after evaluation.

Other Notes of Importance

Rate limiting

On many devices, e.g. Cisco perimeter routers, it is possible to limit the rate of transmitted ICMP packets. This is done to prevent the router of becoming a victim of a Denial of Service attack, where it would be flooding the internet link with ICMP traffic. As of Cisco IOS 12.0, a maximum of two packets per second for ICMP Unreachables is set (500ms between packets). Rate limiting such as this can, and should also be configured on all hosts, by means of protecting these machines against resource depletion attacks.

```
ip icmp rate-limit unreachable
```

Fragmented ICMP

While they can occur, fragmented ICMP packets are usually not seen, except in conditions which could be labeled as "malicious". It is advised to drop these packets completely, even before further analysing them using regular access lists.

ICMP Packet Filtering

Example Access-lists Cisco IOS

```
Access-list 101 (to be applied to the external interface)
access-list 101 deny icmp any any fragments
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any packet-too-big
access-list 101 deny icmp any any
```

```
Access-list 102 (to be applied to the internal interface)
access-list 102 deny icmp any any fragments
access-list 102 permit icmp any any echo-request
access-list 102 permit icmp any any time-exceeded
access-list 102 permit icmp any any packet-too-big
access-list 102 deny icmp any any
```

Linux iptables

```
iptables -A INPUT -p icmp --fragment -j DROP
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp --icmp-type fragmentation-needed -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type time-exceeded -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type fragmentation-needed -j ACCEPT
iptables -A INPUT -p ICMP -j DROP
iptables -A OUTPUT -p ICMP -j DROP
```