Best Practice - Network Troubleshooting

https://campus.barracuda.com/doc/73718983/

The firewall history page is the most powerful tool for troubleshooting connection issues on your network. It provides real-time and historical information on all network traffic passing the Barracuda Firewall. The following article lists reasons for connection blocking, dropping, or failures:

Deny Reasons

Deny Reasons	Description
Deny by Dynamic Rule	The session request was matched by a dynamic rule, which is set to be denied.
Deny by Rule	A rule denies a session request explicitly.
Deny by Rule Destination Mismatch	A rule with the DENY on Destination Mismatch option selected, matched and resulted in a deny action.
Deny by Rule Service Mismatch	A rule with the DENY on Service Mismatch option selected, matched and resulted in a deny action.
Deny by Rule Source Mismatch	A rule with the DENY on Source Mismatch option selected, matched and resulted in a deny action.
Deny by Rule Time Mismatch	A rule with the DENY on Time Mismatch option selected, matched and resulted in a deny action due to the time mismatch.
Deny Local Loop	A Pass, Map, or Dst NAT rule matched, but the destination is a local system IP address. Use an App Redirect rule instead.
Deny No Address Translation possible	The matching rule contains a address translation table which does not specify how to translate the particular source IP address.

Block Reasons

Block Reasons	Description
Block Broadcast	Broadcasts are not propagated.
Block by Dynamic Rule	The session request was matched by a dynamic rule, which is set to be blocked.
Block by Rule	A rule blocks a session request explicitly.
Block by Rule Destination Mismatch	A rule with this option selected, matched and resulted in a blocking action.
Block by Rule Interface Mismatch	A rule with this option selected, matched and resulted in a blocking action due to the mismatch of the expected network interface.
Block by Rule Service Mismatch	A rule with this option selected, matched and resulted in a blocking action.

Block by Rule Source Mismatch	A rule with the BLOCK on Source Mismatch option selected, matched and resulted in a blocking action.
Block by Rule Time Mismatch	A rule with this option selected, matched and resulted in a blocking action due to the mismatch in time.
Block Echo Session Limit Exceeded	The number of total Echo sessions was exceeded for a request.
Block Local Loop	A passing rule matched, but the destination is a local system IP address. Targeted local IP addresses must be redirected. Use action type **Local Redirect** for IP redirection to a local IP.
Block Multicast	Multicasts are not propagated.
Block No Address Translation possible	The matching rule contains a address translation table which does not specify how to translate the particular source IP address.
Block no Rule Match	No rule matched for the requested session. The default action is to block the request.
Block Other Session Limit Exceeded	The number of total OTHER protocol sessions was exceeded for a request.
Block Pending Session Limit Exceeded	The source IP address has too many pending sessions. Further request which would lead to more pending sessions are blocked.
Block Rule Limit Exceeded	The total number of allowed session for the matched rule was exceeded.
Block Rule Source Limit Exceeded	The number of allowed session per source IP address for the matched rule was exceeded.
Block Size Limit Exceeded	A packet which exceeds the specified ping size limit (for ICMP-Echo; default: 10000 bytes) was received. The effective default values are configured in the ICMP (Global) object of a firewall ruleset (see: Service Objects). Increasing the **Max Ping Size** value will most probably reduce **Block Size Limit Exceeded** entries.
Block Source Echo Session Limit Exceeded	The number of total ECHO sessions per source IP was exceeded for a request.
Block Source Session Limit Exceeded	The number of total sessions per source IP was exceeded for a request.
Block UDP Session Limit Exceeded	The number of total UDP sessions was exceeded for a request.
Forwarding is disabled	A forwarding firewall service does not exist or is inactive.

Routing Triangle	This message indicates that a TCP SYN followed by a TCP ACK has been detected, without the firewall having seen the TCP SYN-ACK from the destination host. This implies that a routing triangle exists in the logical network topology that causes the firewall to only see one side of a connection. This routing misconfiguration causes connections between the affected networks to either not work, or to only work in one direction. Typically, this problem occurs when the firewall is defined as the default gateway IP address for systems on the LAN, and there is a separate routing device, connected to the same LAN with connections to other networks. Often this is seen on networks with a private MPLS router for WAN sites.

Drop Reasons

Drop Reasons	Description
Forwarding not Active	A packet could be assigned to an active session, but the forwarding firewall service is block resulting in temporarily dropping all forwarding traffic.
ICMP Header Checksum is Invalid	The ICMP header checksum did not verify.
ICMP Header is Incomplete	The ICMP header of the packet is shorter that the minimum ICMP header length (8 bytes) or shorter than the indicated ICMP header length.
ICMP Packet is Ignored	An ICMP packet contains a type other than UNREACHABLE or TIME_EXCEEDED and is ignored.
ICMP Reply Without a Request	A ICMP-Echo-Reply packet was received by no associated Echo session was found.
ICMP Type is Invalid	The ICMP header contained an unknown ICMP type.
IP Header Checksum is Invalid	The IP header checksum did not verify.

TCP Packet Belongs to no Active Session	The message can be regarded as purely informational and as an indicator that a TCP session has terminated slightly "out of order". However, it is helpful to know the factors that contribute to unscheduled session termination or to frequent TCP packets that cannot be allotted to an active session. • **Situation 1** Two computers deciding to close their TCP communication do so by exchanging finalization (FIN) and acknowledgement (ACK) messages. A typical connection termination requires a pair of FIN and ACK messages from each connection endpoint. In the most commonly used 3-way-handshake, host A sends a FIN to host B, and host B replies with a FIN & ACK. Host B has thus terminated its end and will no longer send data to the other side. Host A successively terminates its own end by sending an ACK message. The duration the firewall waits for the last ACK is defined by the Last ACK Timeout (s) value in each firewall rule (Firewall > Rule configuration dialogue > Advanced Settings). By default, the firewall waits for the last ACK for 10 seconds and then terminates the session itself. An ACK arriving too late (e.g., because of long response time of host A or because of network congestion) will not be attributable to an active session and will be dropped by the firewall, thus triggering the message stated above. • **Situation 2** Hosts have been observed that respond to a FIN message not only with one but with a second ACK. Again, the second ACK will not be attributable to an active session because the firewall has already terminated it after the first ACK. • **Situation 3** Hosts have been observed that continue sending data even though connection termination has already been confirmed by both TCP endpoints. This data will not be attributable to an active session and will be dropped by the firewall, again triggering the message stated above. • **Situation 4** Typically, in mainframe systems, hosts might be dependent on an exceptional session lifetime because data is exchanged rarely and idle times in between data exchange are long. If the maximum idle time is exceeded, the firewall terminates the session between the mainframe computers. Data that the hosts continue to send later, not recognizing that the connection between them has been disrupted, will not be attributable by the firewall and will be dropped, thus triggering the message stated above. If you observe this message frequently, and at the same time experience network problems of unwanted session termination, the following settings might solve the issue. • Increase **Session Timeout** of Service objects: See How to Create Service Objects • Increase **Last ACK Timeout** of firewall rules: See Advanced Access Rule Settings

Fail Reasons

Fail Reason	Description
Accept Timeout	The accept timeout for TCP session establishment was exceeded (TCP only). Possible IP spoofing attempt.
Connect Timeout	The connection timeout for TCP session establishment was exceeded (TCP only). The destination IP address was found not to be reachable.
Denied by Filter	A next hop denied forwarding by a filter rule.
Fragmentation Needed	The destination cannot be reached with the used MTU size without fragmentation. Only occurs if Path-MTU-Discovery is used by the source or the destination.
Host Access Denied	Access to the destination address was denied by one of the next hops.
Host Unreachable	The destination is accessed through a direct route but does not respond to an ARP request.
Host Unreachable for TOS	The requested IP address is not reachable for the used **T**ype **o**f **S**ervice.
Network Access Denied	Access to the destination network was denied by one of the next hops.
Network Unreachable	The network for the destination of a request is not reachable (No routing entry on one of the next hops).
Network Unreachable for TOS	The requested network is not reachable for the used Type of Service.
No Route to Host	The local system has no routing entry for the requested destination.
Port Unreachable	The destination system does not service the requested port number.
Protocol Unreachable	The destination system does not support the requested protocol.
Routing Triangle	Happens if a SYN followed by an ACK is registered without a SYN-ACK of the destination. This is an indication of a triangle route in the network.
Source Route Failed	Source Routing was requested but could not be performed. Will not occur, since source routed packets are dropped.
Unknown Network Error	Default network error.