

Chapter 21

Stateful Firewall Overview

Routers use firewalls to track and control the flow of traffic. The Adaptive Services PIC employs a type of firewall called a *stateful firewall*. Contrasted with a *stateless* firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts.

Stateful firewalls group relevant *flows* into *conversations*. A flow is identified by the following five properties:

Source address

Source port

Destination address

Destination port

Protocol

A typical TCP or UDP conversation consists of two flows, the initiation flow and the responder flow. However, some conversations, such as an FTP conversation, might consist of two control flows and many data flows.

Firewall rules govern whether the conversation is allowed to be established. If a conversation is allowed, all flows within the conversation are permitted, including flows that are created during the life cycle of the conversation.

You configure stateful firewalls using a powerful rule-driven conversation handling path. A *rule* consists of direction, source address, source port, destination address, destination port, IP protocol value, and application protocol or service. In addition to the specific values you configure, you can assign the value any to rule objects, addresses, or ports, which allows them to match any input value. Finally, you can optionally negate the rule objects, which negates the result of the type-specific match.

Firewall rules are directional. For each new conversation, the router software checks the initiation flow matching the direction specified by the rule.

Firewall rules are ordered. The software checks the rules in the order in which you include them in the configuration. The first time the firewall discovers a match, the router implements the action specified by that rule. The rest of the unchecked rules are ignored.

Firewall Application Protocols Support

By inspecting the application protocol data, the AS PIC firewall can intelligently enforce security policies and allow only the minimal required packet traffic to flow through the firewall.

The firewall rules are configured in relation to an interface. By default, the stateful firewall allows all sessions initiated from the hosts behind the interface to pass through the router.

Stateful Firewall Anomaly Checking

The stateful firewall recognizes the following events as anomalies and sends them to the intrusion detection services (IDS) software for processing:

IP anomalies:

- IP version is not correct.
- IP header length field is too small.
- IP header length is set larger than the entire packet.
- Bad header checksum.
- IP total length field is shorter than header length.
- Packet has incorrect IP options.
- ICMP packet length error.
- Time-to-live (TTL) equals 0.

IP address anomalies:

- IP packet source is a broadcast or multicast.
- Land attack (source IP equals destination IP).

IP fragmentation anomalies:

- IP fragment overlap.
- IP fragment missed.
- IP fragment length error.
- IP packet length is more than 64 KB.
- Tiny fragment attack.

TCP anomalies:

- TCP port 0.
- TCP sequence number 0 and flags 0.

TCP sequence number zero and FIN/PSH/RST flags set.

TCP flags with wrong combination (TCP FIN/RST or SYN/(URG|FIN|RST)).

Bad TCP checksum.

UDP anomalies:

UDP source or destination ports 0.

UDP header length check failed.

Bad UDP checksum.

Anomalies found through stateful TCP or UDP checks:

SYN -> SYN-ACK packets without ACK from initiator.

SYN -> RST packets.

SYN without SYN-ACK.

Non-SYN first flow packet.

ICMP unreachable errors for SYN packets.

ICMP unreachable errors for UDP packets.

Packets dropped according to stateful firewall rules

If you employ stateful anomaly detection in conjunction with stateless detection, IDS can provide early warning for a wide range of attacks, including

TCP or UDP network probes and port scanning

SYN flood attacks

IP fragmentation-based attacks such as teardrop, bonk, and boink

