## 12.3 Stateful Firewall

A stateful firewall filters incoming and outgoing network traffic in a computer system based on state information derived from past communications. State information generally describes whether the incoming packet is part of a new connection, or a continuing communication whose connection was approved previously. In other words, states describe a context for each packet.

### *Example*

We have been able to contain many attacks with PACKET FILTER FIREWALL (405) and PROXY-BASED FIREWALL (411). However, we are still plagued with distributed denial of service attacks that prevent customers from reaching our site. We also have performance problems for high-speed streams. In addition, a more sophisticated group of hackers is attacking us, sending us viruses whose bodies are assembled from parts included in message data and commands.

### *Context*

Computer systems on a local network connected to the Internet and to other external networks. A higher level of network security is needed than static packet or proxy filtering. A PACKET FILTER FIREWALL (405) only inspects the address of the packet, without the knowledge of previous communications of the same network. Similarly, a PROXY-BASED FIREWALL (411) filters based on proxy restrictions for each packet. The knowledge of whether a connection is a new connection or an established connection is important for improved security: in particular, denial of service attacks could be identified more conveniently if we knew the relationship between packets [Nou00].

### *Problem*

How can we correlate incoming packets? This correlation may be useful to see if they include portions of commands or data needed for attacks, or to avoid redundant checks and improve performance.

The solution to this problem must resolve the following forces:

- Network administrators deploy and configure a variety of firewalls, so it is important to have a clear model of what packet correlations are required to be inspected and filtered, and what level of stateful inspection is desired. Otherwise, configuration errors and extra overhead may result.

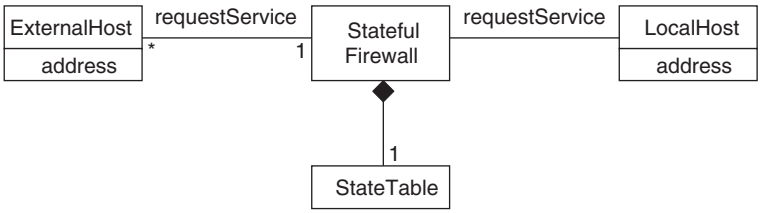
- The configuration of the firewalls must reflect the organization's security policies, otherwise it would be difficult to decide on what to filter and what stateful features to include.
- What is being inspected and filtered is constantly changing, so it should be easy to make changes to the configuration of the firewall.
- It may be necessary to log client requests for auditing and defence purposes.

## Solution

Keep a list or table (a dynamic rule set) with the connections that have been opened, and correlate the type of messages received or sent. This gives the option of not inspecting the packets of a well-established connection.

## Structure

The figure below shows the `Stateful Firewall` class as including a `StateTable` class that describes the existing network connections. The new client (an external host) can only access our local network if a rule exists for authorizing traffic from its address. In addition, if it is a continuing communication from the same client, access is allowed based on whether a corresponding entry is in the `StateTable`. Each association link between the client and local network is therefore controlled by a `Rule` and/or an entry in the `StateTable`. The `Stateful Firewall` includes a set of access rules defined for the organization or local network according to its policies. If a particular request is not satisfied by any of the explicit rules, then the default rule is applied. For every new connection, an entry is made into to `StateTable`.




Class diagram for STATEFUL FIREWALL

## Dynamics

In the figure on page 419 the dynamic aspects of the STATEFUL FIREWALL (417) are described by a sequence diagram that corresponds to the basic use case of filtering a client's request using states.

### Filtering a Client's Request

*Summary.* A remote network requests access to the local network to either transfer or retrieve information. The access request is made through the firewall, which according to a state table, and if necessary a set of rules, determines whether to accept or deny the request.

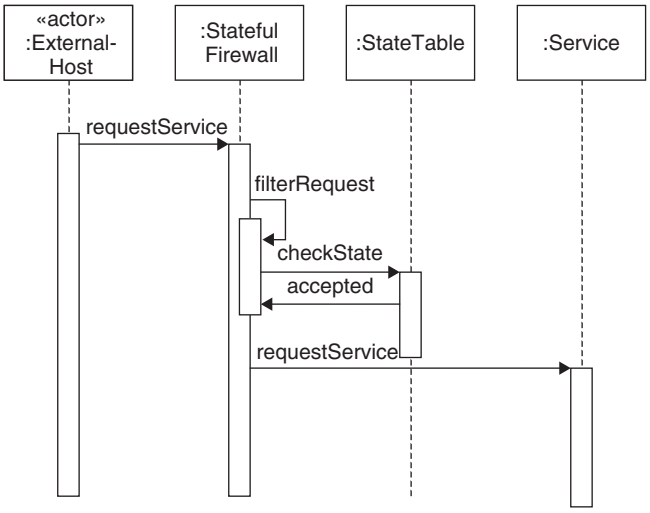
*Actors.* External client.

*Precondition.* The state table contains the list of previously-established connections or connection attempts. If the state table does not allow a request, rules must be consulted as in PACKET FILTER FIREWALL (405).

*Description*:

1. An external network requests access to the local network.
2. A firewall filters the request according to a state table. If the connection exists in the state table, the request is accepted without further inspection.
3. If the connection does not exist in the state table, the request may be filtered based on a set of rules, assuming a packet firewall is part of the combination—see Variants below. If none of the rules are satisfied, then the default rule is used to filter the request, as in PACKET FILTER FIREWALL (405).
4. If the request is accepted, the firewall allows access to the local network.

- *Alternate flow.* If the request if denied, the firewall rejects the access request by the external network to the local network.
- *Postcondition.* The firewall has filtered the access of a client to the local network.




Sequence diagram for providing service to a client via a state table

## Implementation

1. Make a list of the types of attacks we want to prevent.
2. Set the state tables to correlate packets according to these attacks.

## Example Resolved

Typical denial of service attacks start by sending a connection request not followed by an establishment of the connection after its acknowledgement. Our state table keeps a list of all open connections, and if the connections are not established within a given time period, we just cancel them. We also have a catalog of virus patterns and we can make our firewall inspect sequences of messages to detect these attacks.

## Variants

A STATEFUL PACKET FILTER FIREWALL (shown in the next figure) combines address-based filtering with state information, that is, it filters based on the address of the packet and the information in the state table.

The STATEFUL PROXY-BASED FIREWALL (not illustrated here) inspects and filters incoming and outgoing network traffic based on the type of network application they are accessing, and the state of the communication between the networks.

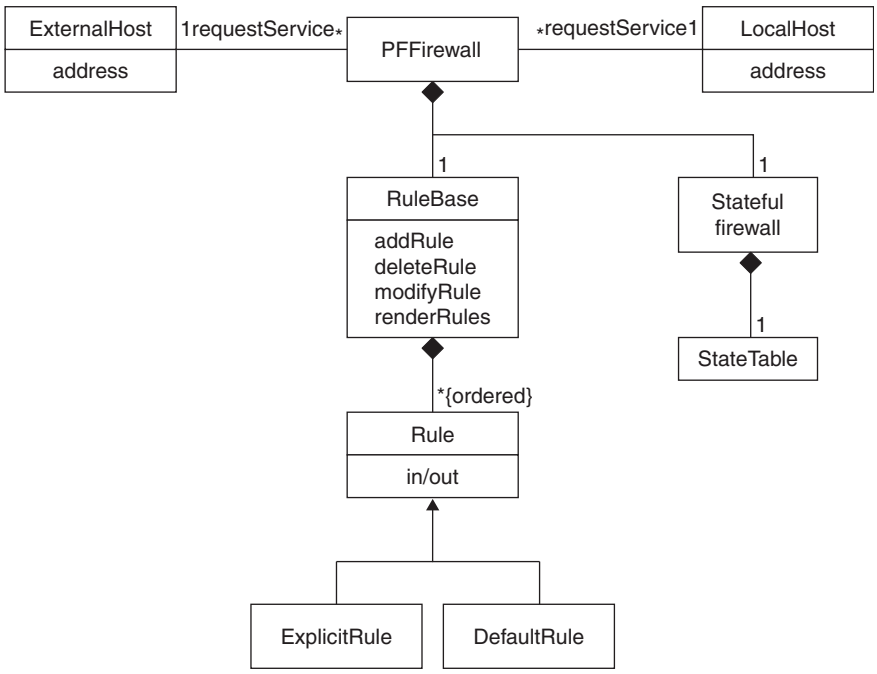
## Known Uses

This pattern can be found in commercial firewall products from organizations such as Software Technologies [Sof03], Check Point Technologies, and CyberGuard [Hen01]. Some specific firewall products that use stateful application proxies are Pipex Security Firewalls [Pip03] and InterGate Firewall [Vicom].

## Consequences

The following benefits may be expected from applying this pattern:

- It is relatively easy to set up the state table once we know what attacks we are expecting.
- It has a low implementation cost, as it requires only a state table.
- If offers good performance. It only needs to look at packet headers for new connections. For existing connections it looks only at the state table.
- It can enhance the security of the other types of firewalls by adding information from different levels about correlated packets.




Stateful Firewall combined with a packet filter firewall

- New attacks only require more ways to correlate packets.
- It allows connection-based logging of traffic. This may be useful for detecting patterns of attack that can be used by intrusion detection systems.

The following potential liabilities may arise from applying this pattern:

- The state table may fill and allow some attacks that take advantage of this fact [Fra01].
- Attack patterns must be defined and coded so they can be recognized.

## *See Also*

This firewall is usually combined with one or both of the previous types of firewalls, PACKET FILTER FIREWALL (405) and PROXY-BASED FIREWALL (411).