12.1 Packet Filter Firewall

Some of the hosts in other networks may try to attack the local network through their IP-level payloads. These payloads may include viruses or application-specific attacks. We need to identify and block those hosts. A packet filter firewall filters incoming and outgoing network traffic in a computer system based on packet inspection at the IP level.

Example

Our system has been attacked recently by a variety of hackers, including somebody who penetrated our operating system and stole our clients' credit card numbers. Our employees are wasting time at work by looking at inappropriate sites on the Internet. If we continue like this we will soon be out of business.

Context

Computer systems on a local network connected to the Internet and to other networks with different levels of trust. A host in a local network receives and sends traffic to other networks. This traffic has several layers or levels. The most basic level is the IP level, made up of packets consisting of headers and bodies (payloads). The headers include the source and destination addresses as well as other routing information, while the bodies include the message payloads.

Problem

Some of the hosts on other networks may try to attack the local network through their IP-level payloads. These payloads may include viruses or application-specific attacks. How can we identify and block those hosts?

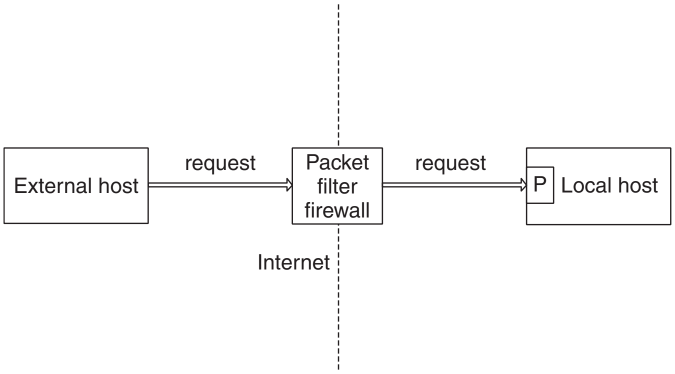
The solution to this problem must resolve the following forces:

- We need to communicate with other networks, so isolating our network is not an option. However, we do not want to take a high risk for doing so.
- The protection mechanism should be able to reflect precisely the security policies of the organization. A too coarse defence may not be useful.
- Any protection mechanism should be transparent to the users. Users should not need to perform special actions to be secure.

- The cost and overhead of the protection mechanism should be relatively low or the system may become too expensive to run.
- Network administrators deploy and configure a variety of protection mechanisms; hence it is important to have a clear model of what is being protected.
- The attacks are constantly changing; hence it should be easy to make changes to the configuration of the protection mechanism.
- It may be necessary to log input and/or output requests for auditing and defence purposes.

Solution

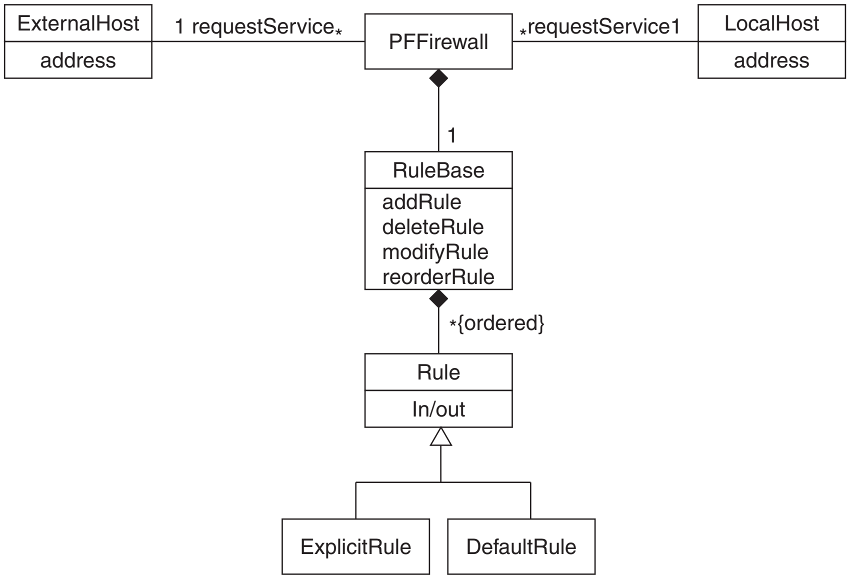
A PACKET FILTER FIREWALL (405) intercepts all traffic coming and going from a port P and inspects its packets (see the figure below). Those coming from or going to mistrusted addresses are rejected. The mistrusted addresses are determined from a set of rules that implement the security policies of the organization. A client from another network can only access the Local Host if a rule exists authorizing traffic from its address. Specific rules may indicate an address or a range of addresses. Rules may be positive (allow traffic from some address) or negative (block traffic from some address). Most commercial products order these rules for efficiency in checking. Additionally, if a request is not satisfied by any of the explicit rules, then a default rule is applied.



The concept of the packet filter firewall

Structure

The figure on page 407 shows an external host requesting access to a local host (a server) through a packet filter firewall. The organization policies are embodied in the objects of class `Rule` collected by the `RuleBase`. The `RuleBase` includes data structures and operations to manage rules in a convenient way. The rules in this set are ordered, and can be explicit or default.



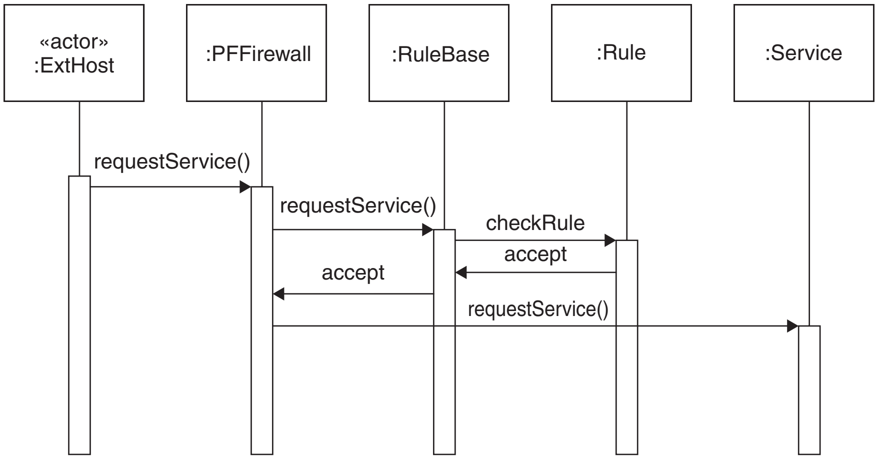
Class diagram for PACKET FILTER FIREWALL

Dynamics

We describe the dynamic aspects of the PACKET FILTER FIREWALL (405) using a sequence diagram for one of its basic use cases. There is a symmetric use case, filtering an outgoing request, which we omit for briefness. We also omit use cases for adding, removing, or reordering rules, because they are straightforward. See the figure on page 408.

Filtering a Client's Request

- *Summary.* A host in a remote network wants access to a local host to either transfer or retrieve information. The access request is made through the firewall, which according to its set of rules determines whether to accept or deny the request—that is, it filters the access request.
- *Actors*. A host on an external network (client).
- *Precondition*. An existing set of rules to filter the request must be in place in the firewall.



Sequence diagram for filtering a client's request

- *Description*:

  1. An external host requests access to the local host.
  2. A firewall filters the request according to a set of ordered rules. If none of the explicit rules in the rule set allows or denies the request, a default rule is used for making a decision.
  3. If the request is accepted, the firewall allows access to the local host.

- *Alternate flow*. The request is denied.
- *Postcondition*. The firewall has accepted the access of a trustworthy client to the local host.

Implementation

1. Define an organization policy about network access, classifying sites according to our trust in them.
2. Convert this policy into a set of access rules. This can be done manually, which may be complex for large systems. An alternative is using an appropriate commercial product, such as Solsoft [Sol].
3. Note that the idea of a single point of access is virtual: there may be several physical firewalls deployed at different places. This means that it is necessary to install firewalls at all external boundaries, such as routers or gateways.
4. Write the rules in each firewall. Again, products such as Solsoft and others automatically propagate the rules to each registered firewall.

5. Configure the corresponding firewalls according to standard architectures. A common deployment architecture is the DEMILITARIZED ZONE (449) (DMZ).

Example Resolved

We were able to trace the addresses of our attackers and we installed a firewall to block requests from those addresses from reaching our system. We also made a list of addresses of inappropriate sites and blocked access to them from the hosts in our network. All this reduced the number of attacks and helped control the behavior of some employees.

Known Uses

This model corresponds to an architecture that is seen in commercial firewall products, such as ARGuE (Advanced Research Guard for Experimentation), which is based on Network Associates' Gauntlet Firewall [Eps99], OpenBSD Packet Filtering Firewall [Rus02], which is the basic firewall architecture for the Berkeley Software Distribution system, and the Linux Firewall [Zie02], which is the basic firewall architecture used with the Linux operating system. PACKET FILTER FIREWALL (405) is used as an underlying architecture for other types of firewalls that include more advanced features.

Consequences

The following benefits may be expected from applying this pattern:

- A firewall transparently filters all the traffic that passes through it, thus lowering the risk of communicating with potentially hostile networks.
- It is possible to express the organization's filtering policies through its filtering rules, with different levels of protection for different parts of the network.
- It is easy to update the rule set to counter new threats.
- Because it intercepts all requests, a firewall allows systematic logging of incoming and outgoing messages. Because of this, a firewall facilitates the detection of possible attacks and helps to hold local users responsible for their actions when interacting with external networks.
- Its low cost enabled it to be included as part of many operating systems and simple network devices such as routers.
- It offers good performance, only needing to look at the headers of IP packets rather than the complete packet.
- It can be combined with intrusion detection systems (IDS) for greater effectiveness. In this case, the IDS can tell the firewall to block suspicious traffic.

The following potential liabilities may arise from applying this pattern:

- The firewall's effectiveness and speed may be limited due to its rule set (order of precedence). Addition of new rules may interfere with existing rules in the rule set, so a careful approach should be taken in adding and updating access rules.
- The firewall can only enforce security policies on traffic that goes through the firewall. This means that one must make changes to the network to ensure that there are no other paths into its hosts.
- An IP-level firewall cannot stop attacks coming through the higher levels of the network. For example, a hacker could put malicious commands or data in header data not used for routing, or in the payload.
- Each packet is analyzed independently, which means that it is necessary to analyze every packet. This may reduce performance.
- A packet filter cannot recognize forged addresses (IP spoofing) because it only examines the header of the IP packet. This can be corrected (at some extra cost) using link layer filtering, in which each IP address is correlated to its hardware address [Fra01].

See Also

AUTHORIZATION (245) defines the standard security model for PACKET FILTER FIREWALL (405). This pattern is also a special case of SINGLE ACCESS POINT (279) and is the basis for other, more complex, types of firewalls described later in this chapter. DEMILITARIZED ZONE (449) (DMZ) defines a way to configure this pattern in a network. This pattern can also be combined with STATEFUL FIREWALL (417).