12.2 Proxy-Based Firewall

A proxy-based firewall inspects and filters incoming and outgoing network traffic based on the type of application service to be accessed, or performing the access. This pattern interposes a proxy between the request and the access, and applies controls through this proxy. This is usually done in addition to the normal filtering based on addresses.

Also Known As

Proxy Firewall, Application Firewall

Example

After we started using a PACKET FILTER FIREWALL (405) most of our problems were reduced. However, some of the messages sent from sites we don't consider suspicious contain malicious payloads, because hackers were spoofing trusted addresses. These payloads sometimes contained incorrect commands or the wrong type and length of parameters. Our PACKET FILTER FIREWALL (405) cannot stop these attacks, because it doesn't look at the message payload, and as a result we are experiencing new problems. It is also hard to block every malicious site.

Context

Computer systems on a local network connected to the Internet and to other networks, where a higher level of security than the one provided by packet filters is needed. Specifically, we want to control attacks at the application layer of the network protocol. Incorrect commands or parameters can produce buffer overflows and other conditions that can be exploited for attacks. In some cases we might also want to authenticate the client to avoid spoofing. Outgoing flows (to malicious sites) can also be damaging in this environment.

Problem

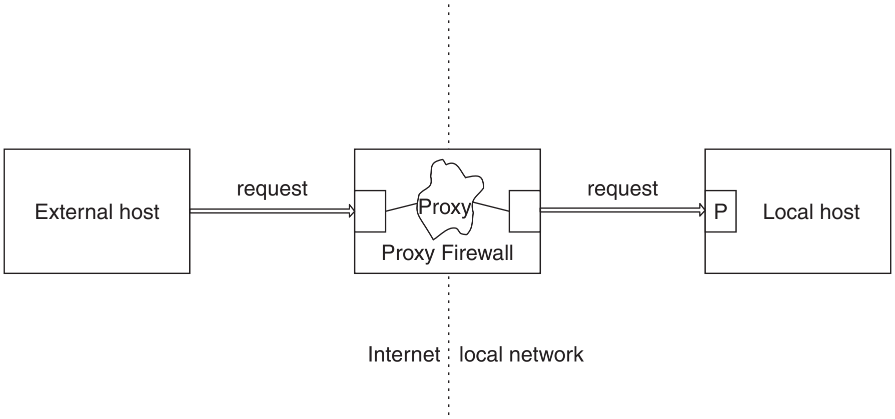
PACKET FILTER FIREWALL (405) only inspects the network addresses when deciding whether to allow access for a request. We can only block supposedly malicious sites. It is hard to know about all of those sites, and we need further defences. Also, how do we protect our network from potential attacks that might be embedded within the data segment of the packets?

The solution to this problem must resolve the following forces:

- We need to let external networks access our services and local users access external sites. Isolation is not acceptable.
- There are a variety of application services in a system, for example mail, file transfer, and others. Hackers can plan specific attacks against them and we need to be prepared for a variety of attacks.
- Network administrators deploy and configure a variety of protection mechanisms, so it is important to have a clear model of what is being protected and what types of attacks are possible.
- The protection mechanism should be able to reflect precisely the security policies of the organization.
- The types of attacks are constantly changing, so it should be easy to make changes to the configuration of the protection mechanisms.
- It may be necessary to log requests for auditing and defence purposes.

Solution

Make the client interact only with a proxy of the service requested, which in turn communicates with the protected service (see the figure below). The client can only receive service from the server if an application proxy exists for the requested service. Each application proxy has its own access rules pre-defined by the administrator that may be used to authenticate, inspect, change, and filter the incoming (or outgoing) messages.



The concept of the proxy-based firewall

Structure

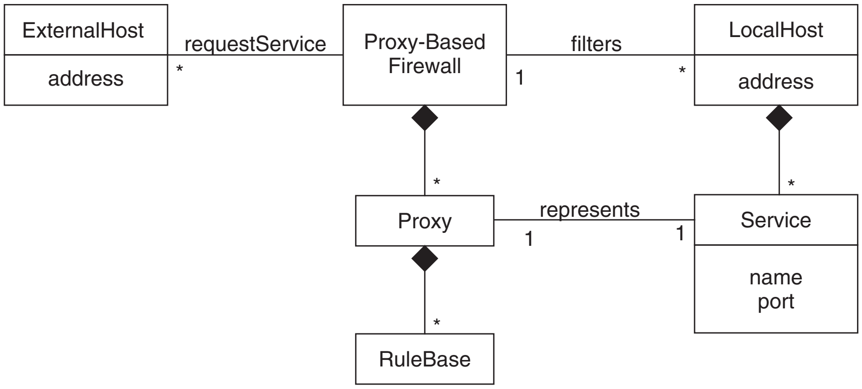
The figure below shows the class diagram for this pattern. We show here only the proxy aspects: the classes shown in the figure on page 407 can be part of this firewall or can be provided separately. This firewall contains `Proxies`, which in turn contain `Rules`, collected in a `RuleBase`. All the hosts of a local network share the firewall. Each local host provides a set of services. The rules may now specify specific constraints for the use the available services.

Dynamics

We illustrate a use case for filtering requests for services. See the sequence diagram on page 414.

Providing Service to a Client

- *Summary.* An external client wants access to a service from a local host. The access request is made through the firewall, which according to its application proxies and their rules determines whether to deny or accept the request.
- *Actors*. External client.
- *Precondition*. None.



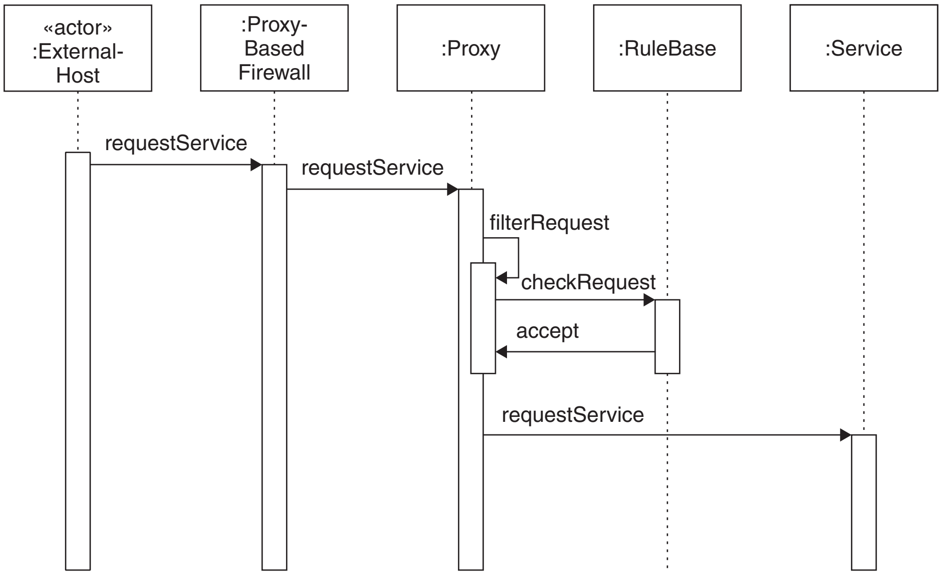
Class diagram for PROXY-BASED FIREWALL

- *Description*. An external network requests a service to the PROXY-BASED FIREWALL (411). The firewall filters the request according to its application proxies and their access rules. If none of the rules in the rule set are satisfied, then a default rule is used to filter the request. If the request is accepted, the client is allowed to access the service through the proxy.

- *Alternate flow*. If the service request is not supported by the PROXY-BASED FIREWALL (411), or the firewall considers the client untrustworthy, the firewall will block the access.
- *Postcondition*. The firewall has accepted the service request from a trustworthy client to the local host.

Implementation

1. According to organization policies, define which services will be made available to clients of the network.
2. Write, reuse, or buy a proxy for each service and assign a location or address to it.
3. Define who can have what type of access to which service and other restrictions on their use.



Sequence diagram for filtering service requests.

4. Implement these constraints in the rule base.
5. Consider configurations such as PROTECTION REVERSE PROXY (457), INTEGRATION REVERSE PROXY (465) or a combination with a PACKET FILTER FIREWALL (405) in a distributed configuration [Cyb03].

Example Resolved

We bought a PROXY-BASED FIREWALL (411) and now every request for a service is authenticated and checked. We can verify that the requests are authentic and filter out some payload attacks, for example, a wrong command for a service, wrong type parameters in the service call, and so on.

Known Uses

Some specific firewall products that use application proxies are Pipex Security Firewalls [Pip03] and InterGate Firewall. The SOCKS Protocol from IETF, although not intended as a firewall, uses a similar principle [Socks]. Postfix filters act as proxy and packet filter firewalls [Haf05].

Consequences

The following benefits may be expected from applying this pattern:

- The firewall inspects and filters all access requests based on predefined application proxies that are transparent to the users of the services. In some cases, it may even modify a request—for example, doing network address translation.
- It is possible to express the organization's filtering policies through its application proxies and their rules.
- The implementation details of the local host can be hidden from the external clients. This also improves security.
- A firewall permits systematic logging and tracking of all service requests going through it. This facilitates the detection of possible attacks and helps hold local users responsible of their actions.
- It provides a higher level of security than packet filters, because it inspects the complete packet including the headers and data segments. This global view may control attacks in the payload and attacks based on the structure and size of the packets.

The following potential liabilities may arise from applying this pattern:

- Possible implementation costs due to the need for specialized proxies. The proxies also need to be configured correctly. On the other hand, proxies already exist for common services.
- Performance overhead due to the need for inspection of the data segment of packets and maybe additional checking.

- Increased complexity of the firewall. A PROXY-BASED FIREWALL (411) may require a change in applications and/or the user's interaction with the system. This is not necessary, however, in a well-designed system.

See Also

This pattern uses the PROXY pattern from [GoF95]. It can be combined with PACKET FILTER FIREWALL (405) and STATEFUL FIREWALL (417).