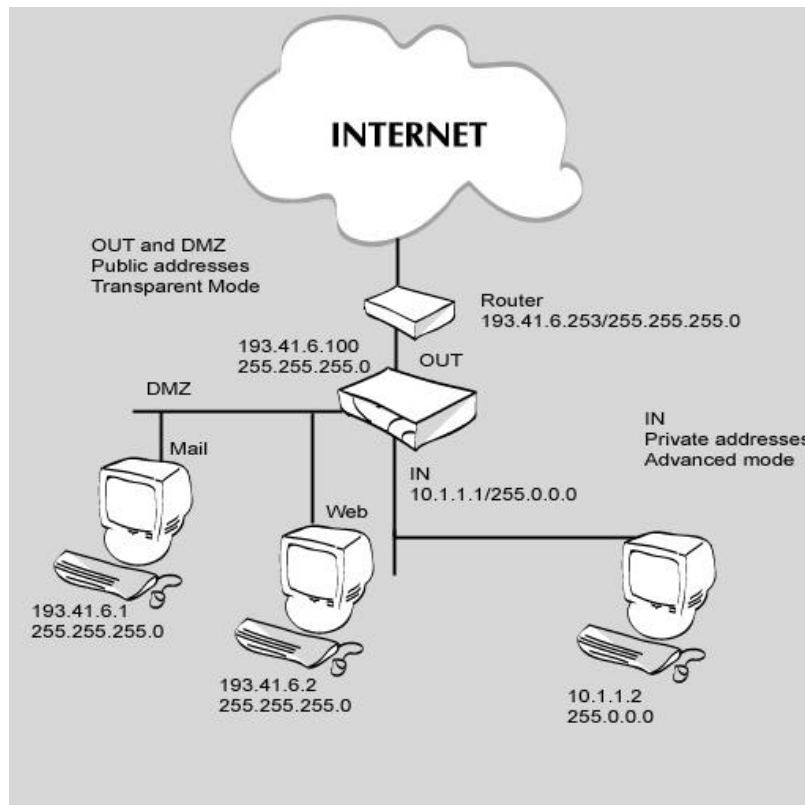


NETASQ firewalls

Hybrid
mode

NETASQ
Secure Internet Connectivity





The firewall's job is to safeguard your network by analysing all the traffic in transit between your LAN and the Internet or solely within your LAN.

It must therefore be installed in your current architecture. It is not always easy to integrate a firewall into an existing network is not always easy and the network configuration usually has to be adapted to the firewall.

These changes are time-consuming and they may give rise to configuration problems for some providers (whose IP address at the time of installation cannot be changed).

The NETASQ solution

NETASQ offers you the Hybrid mode in order to meet all your requirements and to minimise changes of IP addresses. The Hybrid mode combines two operational modes - the transparent mode (bridge principle) and the advanced mode (independent interfaces). The NETASQ firewall accepts both.

The purpose of the hybrid mode is to operate several interfaces in the same class of addresses and others in different classes of address. In this way it is possible for our Firewall to be installed into any configuration.

The security level remains just as high, as you can filter the flow between all the interfaces in the same way.

There are many advantages:

- 1 - Conservation of public addresses, web, mail, ftp providers ... The transparent mode between the OUT interface and the DMZ precludes the need to translate addresses for all public providers.

- 2 - The physical separation of internal networks (compatibility, R & D, ...) and the installation of filtering rules.
- 3 - Easy insertion into an existing network.

Operating principle

The NETASQ Firewall's network interfaces operate by two different modes. They can be part of a bridge (transparent mode) or they can be independent (advanced mode).

In transparent mode the interfaces combined in the bridge are part of the same addressing system and the networks connected to them are in the same address classification.

The two interfaces of a bridge have an identical address for MAC and IP. The Firewall does not carry out routing between these interfaces and only transmits frames (the same operating principle as a switch). The NETASQ updates an ARP table which enables it to know which machines are connected on each interface at any given time.

In advanced mode each interface has an address belonging to a difference classification and the network to which it is connected belongs to the same classification. The NETASQ Firewall therefore behaves like a router, routing the flow between the various interfaces. In this mode the firewall is usually the default gateway for the machines connected to an interface.

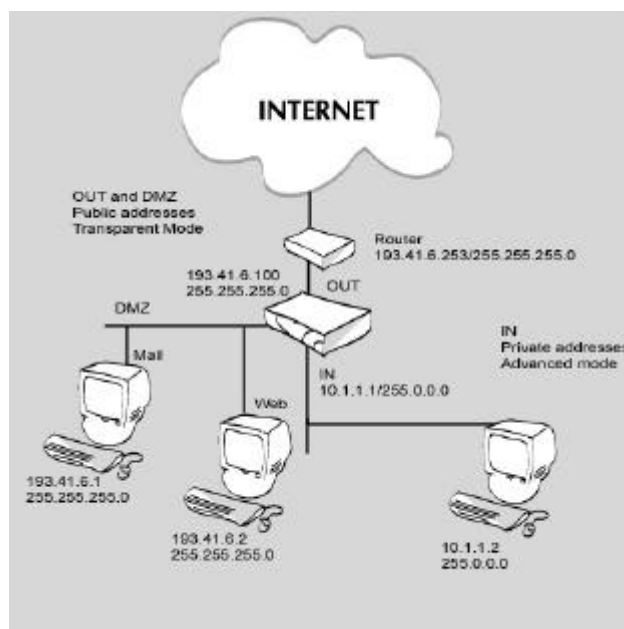
The hybrid mode will be the link between these two operating modes. One NETASQ firewall will combine interfaces in advanced and transparent modes.

Examples

Example 1: Transparent mode for DMZ and OUT

In a 3-zone box you can have the same address classification between the external zone and the DMZ (official addresses, for example) and another address classification (private addresses) for terminals in the internal zone.

Terminals are therefore directly accessible by their public addresses. The firewall is thus transparent. Nevertheless it is still possible (and highly advisable) to filter the traffic between the DMZ and OUT (Internet access).



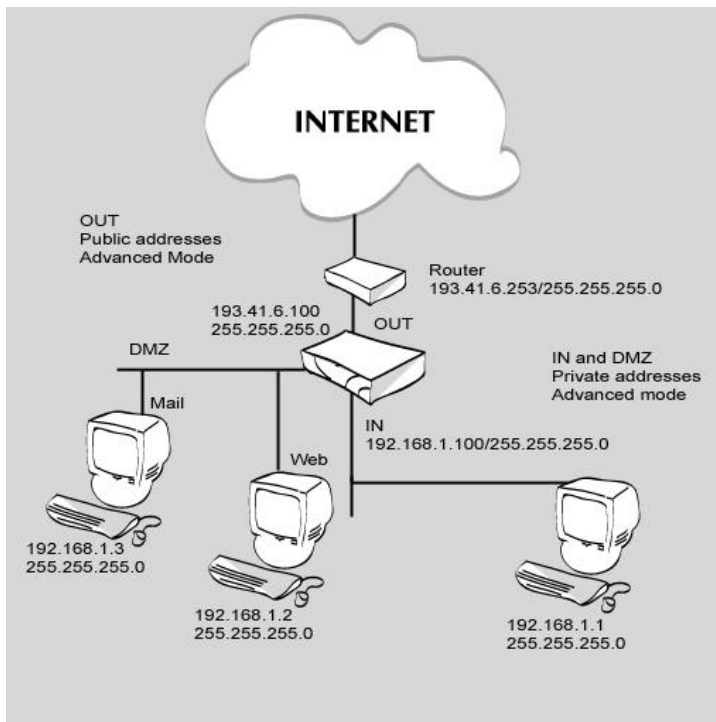
Example 2: Transparent mode for IN and DMZ interfaces

WE often find some public providers inside the LAN. This is not safeguarded.

The internal network must move these terminals to DMZ.

In this case the hybrid mode eliminates the need to change the IP addresses. The transparent mode between the internal network and the DMZ allows you to change the architecture without changing the configuration of user terminals and providers.

Access from outside is possible because the addresses are translated.



Example 3: Separation of departments

The firewall may be inserted into a network to filter the traffic between departments in a company.

The transparent mode is very useful in this case. It enables the NETASQ Firewall to intervene on any terminal in the network.

The addressing plan remains identical. You only have to physically separate the different sections of the LAN and to place the the firewall in the middle (star-shaped architecture).

You may then install the necessary filtering rules between your various departments.

