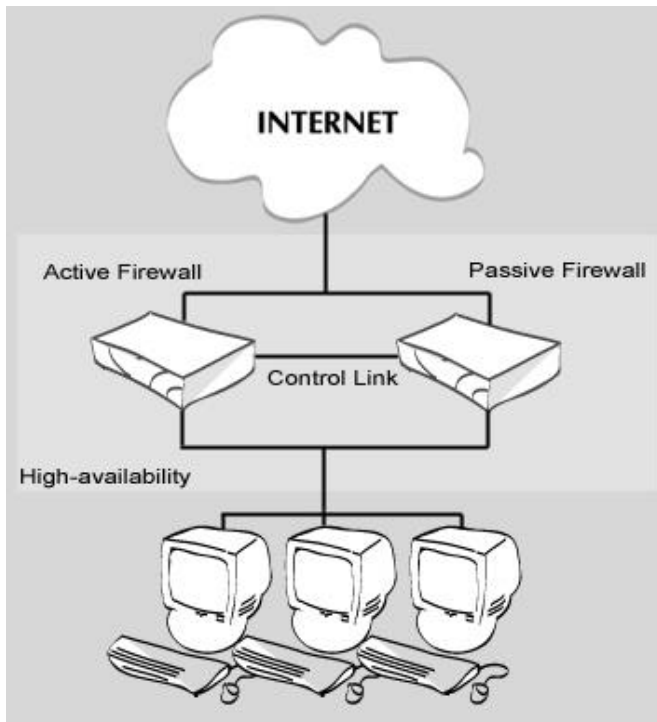


# Netasq Firewalls

High  
Availability

**NETASQ**  
Secure Internet Connectivity





A firewall protects the whole of the network against intrusions. It also safeguards the transmission of data between remote sites - or between a site and a nomad client - by creating VPN tunnels.

As no part of a network can be guaranteed free from the threat of a breakdown you must take precautions against any failure in the firewall, which is the keystone of a secure architecture.

## The NETASQ solution

If there is an incident on the firewall the link between the company's internal network and the exterior is severed. Netasq offers its clients the high availability or breakdown tolerance option to deal with this problem.

The solution is based on a cluster, a group of two identical firewalls each of which monitors the other. If there is a malfunction in the firewall software or hardware during use the second box takes over. The switch from one to the other is wholly transparent to the user.

This option therefore confers a high level of availability to your architecture, at the same time preserving the Netasq solution's simplicity of operation.

If you need further sales information please do not hesitate to contact your supplier or a member of the Netasq team. You will be offered special terms for the purchase of a

## OPERATION

### *Active or Passive states*

Every firewall has a specific status, either active or passive, at any given moment. The active firewall analyses connections, authorizing or rejecting them. The second is passive - its series interface remains active but all the others are inactive.

### *Control link*

The two firewalls are regarded as a single entity. They are linked by a series cable which transmits the data, which monitors the status of the firewalls.

The passive firewall monitors the activity of the other firewall by sending activity signals called Heartbeats. If the active firewall does not reply to passive firewall's demands it takes over. In the same way the active box checks that there has been no incident on the passive box. If there is an incident on either an alert is established in the logs and sent by mail to the administrator.

Other control data are also transited, in particular information for the management of the Master-Slave (\*) relations and the automatic copy of the configuration (\*\*).

### ***(\*)Master-Slave relations***

Each firewall has a specified status - master or slave - at the time of installation, depending on its license key.

The status of master or slave is of outstanding importance if a problem arises or if there is an error in manipulation. For example, if the two NETASQ boxes are activated simultaneously the master remains active and the slave returns to the passive mode.

### ***(\*\*)Automatic copy of the configuration***

Every time the configuration of the active firewall is changed (changes in network configuration, objects, filtering rules, translation rules etc.) the new configuration is copied automatically on the passive firewall. The two firewalls are permanently synchronized.

### ***Incident on the active Firewall***

The passive firewall tests the reaction of the active firewall by sending heartbeats at regular intervals via the control link (the duration is parametrable).

When a certain number of pings (heartbeats) remain unanswered (the number is parametrable) the passive firewall assumes that the other firewall is inactive and takes over automatically, in a way which is transparent to the users.

The network configuration remains identical, so there will be no change and no loss of performance. Both firewalls have the same IP addresses and the same Mac addresses for each interface. The passive firewall, now active, can reply to ARP requests destined for the former firewall.

Finally an alert is given in the alarm logs and by mail to the administrator.

In addition to the activity test described earlier the firewalls cross-test each other:

1 - Each firewall checks the active or passive status of the other regularly in case both are active at once. If this is the case the master firewall remains active and the slave becomes passive. This situation can occur when the series cable is unplugged for a few moments.

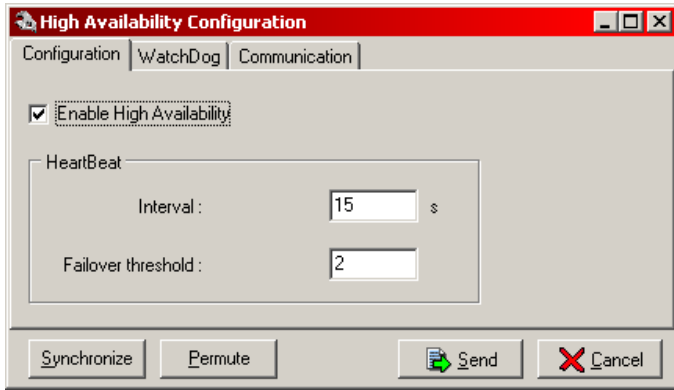
2 - Each firewall checks the number of Ethernet boards which are active on the other firewall. If the active firewall has fewer Ethernet boards in operation than the passive firewall it switches to the passive mode and the passive firewall is activated.

### ***High availability - ease of configuration***

The configuration of high availability on the Netasq box is extremely simple. A new menu is added to the «Firewall» configuration menu.

You only need to connect the two firewalls by their series port and activate the high availability option.



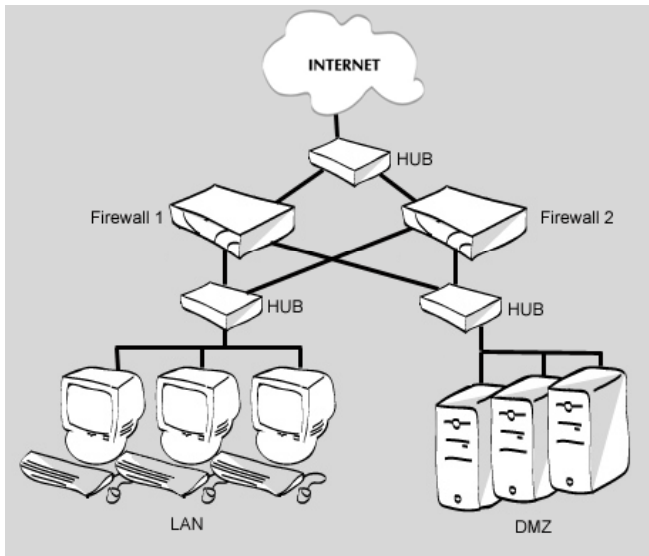


The parameters to be defined are those mentioned earlier - the time interval between heartbeats and the number of heartbeats missed before the firewall's switch over

The association of these two parameters will determine the maximum time during which the network can be cut off.

### **Practical case: installing a high availability architecture**

Your network is divided into an internal network (LAN) and a demilitarised zone (DMZ) to host your public providers.



You want an architecture with a high level of availability, without any break in service for your internal users and for access to your public providers. Therefore you want to install the NETASQ firewall high availability option.

Each network (LAN, DMZ and Internet) must be connected to a HUB. These HUBS will be connected to each firewall in the high availability cluster.

*Note: You can use switches but this is dearer and we do not recommend it.*