EN

# What to do with firewalls in corporate netwerks

**Octalarm**-TOUCH

In some circumstances problems may arise with the connection to portal.octalarm.com. This is usually caused by a firewall in the corporate network. This can lead to a poor/limited connection for the Octalarm-Touch, causing to continually sent messages to the Adésys server, overloading it as a result. For you as an installer / end user, this means that there is a risk that the Octalarm-Touch will not have a stable connection and therefore no VoIP. How can you prevent this?

## Outgoing firewall

A firewall can be present in the end user's network, which blocks all outgoing connections as standard. Due to the dynamic nature of the Octalarm-Touch's configuration process, it is difficult to determine in advance which IP address and which UDP / TCP ports are required for a connection.

To give the Octalarm-Touch enough access to the internet for a successful connection, it is recommended that the installer / system administrator of the end user selects one of the following methods for firewall configuration:

## 1 Firewalling based on source IP

The installer / system administrator of the end user gives the source IP of the Octalarm-Touch access to the entire IPv4 and IPv6 internet. Access must be given to the internet on all ports (https, ICMP ping request and UDP). This can be combined with the installation of the Octalarm-Touch in its own network zone (DMZ). If necessary, further connections between the Octalarm-Touch and the end-user's network can then be specifically secured.

## 2 Firewalling based on DNS name

The installer / system administrator of the end user adds the following DNS names in the firewall of the company network:

- config.octalarm.nl
- config.octalarm.com
- vpn.octalarm.nl
- vpn.octalarm.com

and allows the source IP of the Octalarm-Touch to communicate with them. The DNS names contain both IPv4 (A records) and IPv6 (AAAA records).

Other settings:

- outgoing https on config.octalarm.nl and config.octalarm.com
- outgoing ICMP ping request and UDP (all ports) on vpn.octalarm.nl and vpn.octalarm.com

This method can also be combined with the Octalarm-Touch placed in a DMZ.

**The use of firewalling based on DNS name is preferred because the IP address of the server is automatically permitted, even in the event of server-side updates. If a different method of firewalling is applied, the firewall must be adjusted for each server-side IP-update.**