NL

Wat te doen bij een firewall in het bedrijfsnetwerk

Octalarm-TOUCH

In sommige situaties kunnen er problemen optreden met de verbinding met portal.octalarm.com. Dit wordt meestal veroorzaakt door een firewall in het bedrijfsnetwerk. Dit kan leiden tot een slechte/ beperkte verbinding voor de Octalarm-Touch, waardoor deze voortdurend berichten naar de server van Adésys verzendt. De server raakt hierdoor overbelast. Voor u als installateur/eindgebruiker betekent dit dat het risico bestaat dat de Octalarm-Touch geen stabiele verbinding heeft en dus geen VoIP. Hoe kunt u dit voorkomen?

Uitgaande firewall

Er kan een firewall in het netwerk van de eindgebruiker aanwezig zijn die standaard alle uitgaande verbindingen blokkeert. Vanwege het dynamische karakter van het configuratieproces van de Octalarm-Touch is het moeilijk om vooraf te bepalen welk IP-adres en welke UDP/TCP-poorten vreeist zijn voor een verbinding.

Om de Octalarm-Touch voor een succesvolle verbinding voldoende toegang tot het internet te geven, moet de installateur/systeembeheerder van de eindgebruiker voor de firewall configuratie één van de volgende manieren kiezen:

1 Firewalling op basis van source IP

De installateur/systeembeheerder van de eindgebruiker geeft het source IP van de Octalarm-Touch toegang tot heel het IPv4 en IPv6 internet. Er moet op alle poorten (https, ICMP ping request en UDP) toegang gegeven worden naar het internet. Dit kan worden gecombineerd met de installatie van de Octalarm-Touch in zijn eigen netwerkzone (DMZ). Verdere verbindingen tussen de Octalarm-Touch en het netwerk van de eindgebruiker kunnen dan specifiek beveiligd worden.

2 Firewalling op basis van DNS naam

De installateur/systeembeheerder van de eindgebruiker voegt onderstaande DNS namen toe in de firewall van het bedrijfsnetwerk:

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

en staat toe dat het source IP van de Octalarm-Touch daarmee kan communiceren. De DNS namen bevatten zowel IPv4 (A-records) als IPv6 (AAAA-records).

Overige instellingen:

- uitgaand https op config.octalarm.nl en config.octalarm.com
- uitgaand ICMP ping request en UDP (alle poorten) op vpn.octalarm.nl en vpn.octalarm.com

Deze methode kan ook weer gecombineerd worden met het plaatsen van de Octalarm-Touch in een DMZ.

Het gebruik van firewalling op basis van DNS naam heeft de voorkeur omdat het IP-adres van de server automatisch wordt toegestaan, zelfs in het geval van updates aan de serverzijde. Wanneer er een andere manier van firewalling wordt toegepast moet de firewall worden aangepast voor elke IP-update aan de serverzijde.