IP-ranges

Vanuit de tegel *IP-ranges* van het beheerportaal-Nieuw, kolom *Gebruikers* kan een whitelist beheerd worden met client-ip-adressen.

In deze whitelist kan men instellen welke client-ip-adressen gezien moeten worden als lokale netwerk IP-adressen. Deze lijst kan gebruikt worden voor het uitschakelen van de 2e factor bij 2-factor authenticatie (de aanwezigheid op het netwerk fungeert als 2e factor) of voor het tonen van documentlinks als lokale links naar een fileserver.

Zorg ervoor dat men goed begrijpt wat men instelt of anders hulp vraagt van support hierbij, omdat dit een vrij technische aangelegenheid is die effect heeft op de beveiliging. Nadat de whitelist is ingesteld is het noodzakelijk om (met enige regelmaat) een test te doen van binnen en van buiten het netwerk om te verifiëren dat alles werkt zoals verwacht. Let vooral op dat bij wijzigingen in de netwerkinfrastructuur opnieuw getest wordt.

Bij het invullen van de whitelist moet onderscheid gemaakt worden tussen Cloud en onPremisse installaties. Bij Cloud installaties kan worden volstaan met het invullen van het externe IP-adres van de kantoor-internetaansluiting. Iedere verbinding naar de server van dat IP-adres zal worden gezien als een verbinding vanaf kantoor. Bij onPremisse installaties moet men eerst bepalen of:

- de kantoor IP-adressen door de server gezien worden als interne IP-adressen of externe (alle verbindingen verlopen via de gateway)
- de externe IP-adressen door de server gezien worden als interne IP-adressen of externe (bij reverse proxy lijkt ieder extern adres van het lokale proxy-IP te komen).

Dat is te bepalen door een interne en externe verbinding te maken en in te loggen in het system en dan te kijken in tbsessions (beheertegel *Sessions*). Als blijkt dat extern gezien wordt als extern en intern als intern, dan kan men de hele range interne IP-adressen op de whitelist zetten. Bijv. **192.168.*.***

Als er echter sprake is van alleen intern of alleen extern, dan is een speciale configuratie nodig bij het netwerkbeheer; een interne DNS server met een afwijkende DNS verwijzing voor de onPremisse server in combinatie met een whitelist waarop de gateway/reverseproxy niet op staat. Neem hiervoor altijd contact op met de helpdesk.

Voor ipv6 adressen is de whitelist constructie nog niet geschikt en moet niet worden gebruikt.

Inloggen