

Profielen t.b.v. NAC policies

In dit document staan alleen de profielen uitgewerkt, welke veel gebruikt worden.

Voor zogenaamde specials zullen tijdens het project samen met opdrachtnemer aparte profielen met aparte policies worden uitgewerkt.

Opdrachtnemer moet er rekening mee houden dat er allerlei ontwikkelingen zijn, waarbij b.v. apparaten worden vervangen door nieuwe functionaliteit en laptops anders ingericht worden op basis van nieuw beleid.

Dit document pretendeert dan ook niet volledig te zijn, maar geeft een goede indruk aan opdrachtnemer over de gewenste profielen voor de verschillende groepen apparaten welke aan het netwerk hangen.

Standaard beleid

- Als onbekende en/of onbeheerde apparaten aansluiten op het netwerk, worden ze beschouwd als niet vertrouwd (zero-trust) en krijgen ze alleen toegang tot internet.
- Apparaten zijn van elkaar geïsoleerd tenzij een uitzondering voor een specifieke dienst wordt gemaakt.

De basis Network Access Control (NAC)-implementatie zorgt er voor dat op basis van authenticatie een apparaat geautoriseerd wordt middels een policy. Hiermee wordt het apparaat in een bepaald segment geplaatst en mag het apparaat bepaalde diensten benaderen/gebruiken.

Onderling Microsoft Teams-verkeer

Indien mogelijk wordt bij peer to peer calls van Microsoft Teams het audio- en videoverkeer binnen het lokale netwerk tot stand gebracht.

Indien dit niet mogelijk is een netwerk wordt al het Microsoft Teams-mediaverkeer over internet via het Microsoft Teams-platform geleid.

Om gebruik te maken van de lokale en efficiënte afhandeling van audio- en videoverkeer wordt Microsoft Teams-verkeer op het bekabelde interne netwerk tussen apparaten met Microsoft Teams toegestaan.

Bypass voor VMware Horizon-verkeer

Verkeer van laptops en thinclients naar de VMware Horizon-farm wordt vanaf het interne netwerk niet het internet opgestuurd, maar via een bypass naar het datacenter gerouteerd.

Vernieuwing telefonieplatform

Eén van de projecten waar rekening moet worden gehouden, is de vernieuwing van het telefonieplatform.

Opdrachtgever is voornemens om de oude Mitel-telefonieplatform uit te faseren en ook voor telefonie over te stappen op Microsoft Teams.

Voor beide telefonieplatformen moeten profielen worden gedefinieerd als het Mitel-telefonieplatform nog niet uitgefaseerd is.

Haarlem en Zandvoort

Voor medewerkers van gemeente Haarlem en Zandvoort is er geen verschil gemaakt in de profielen.

Remote toegang tot laptops en PC's

Voor zowel remote support van een virtuele PC als van een lokale Windows is er geen rechtstreekse toegang nodig tot het device;

- Remote support van een virtuele PC gaat via VMware Horizon Administrator, waarbij het verkeer binnen het datacenter blijft.
- Remote support van een Windows-laptop/PC gaat via Teamviewer, waarbij verkeerstroom via Teamviewer-platform gaat.

Apparaat	Gebruiker	802.1x-authenticatie	Segment	Wat is toegankelijk?
Beheerde Windows-laptop (huidige laptops)	Medewerker bekend in AD	Device-certificaat AD-gebruikersnaam/wachtwoord	Niet vertrouwd	Bypass naar VDI Internet-toegang Onderling media-verkeer tussen Teams-clients SCCM/WSUS Interne DNS AD
Beheerde PC met functie thinclient (linux image)	Medewerker bekend in AD	Device-certificaat AD-gebruikersnaam/wachtwoord	Niet vertrouwd	Bypass naar VDI Internet-toegang (beperkt via firewall) Onderling media-verkeer tussen Teams-clients PXE boot om signaal te krijgen voor nieuwe configuratie WoL Interne DNS
Beheerde thinclient	Medewerker bekend in AD	Device-certificaat AD-gebruikersnaam/wachtwoord	Niet vertrouwd	Bypass naar VDI Internet-toegang (beperkt via firewall) Onderling media-verkeer tussen Teams-clients Management thinclients PXE boot om signaal te krijgen voor nieuwe configuratie WoL Interne DNS
Beheerde Macbook	N.v.t.	Geen	Niet-vertrouwd	Bypass naar VDI Internet-toegang

Apparaat	Gebruiker	802.1x-authenticatie	Segment	Wat is toegankelijk?
				Onderling media-verkeer tussen Teams-clients Publieke DNS
Onbeheerde PC/laptop	N.v.t.	Geen	Niet-vertrouwd	Bypass naar VDI Internet-toegang Onderling media-verkeer tussen Teams-clients Publieke DNS
Mitel-telefoon (5330 en 5340)	Toestelnummer en PIN-code	EAP-PEAP	Mitel	Mitel-telefoonplatform Onderling media-verkeer tussen Mitel-toestellen Unilogin-server Interne DNS
Microsoft Teams-telefoon	N.t.b.	N.t.b.	Teams	Beperkt internet-verkeer Microsoft Teams-platform Evt. platform leverancier (updates) Onderling media-verkeer tussen Teams-clients Publieke DNS
Teams Room systemen	N.t.b.	N.t.b.	Teams	Beperkt internet-verkeer Microsoft Teams-platform Evt. platform leverancier (updates) Onderling media-verkeer tussen Teams-clients Publieke DNS
Aanvraagstations identiteitsbewijzen publieksbalies		Geen 802.1x maar karakteristieke device	RAAS	RAAS-server Beperkte toegang tot Diginetwerk Interne DNS

Apparaat	Gebruiker	802.1x-authenticatie	Segment	Wat is toegankelijk?
Multi Functionele Printers	N.t.b.	N.t.b.	Printers	Beperkte internet-toegang Kofax scanserver Printserver Safecom-server Mailserver (SMTP) Beheer printer Interne DNS
Cisco Catalyst 9120 AXI		EAP-TLS, EAP-PEAP, of EAP-FAST	WiFi-AP's	WLC's Interne DNS
NarrowCast systemen (worden vervangen door andere systemen)	N.t.b.	N.t.b.	TNC	Beperkte internet-toegang TNC-server SCCM/WSUS Interne DNS
Gobright-systemen	N.t.b.	N.t.b.	OT	Beperkte internet-toegang Externe DNS