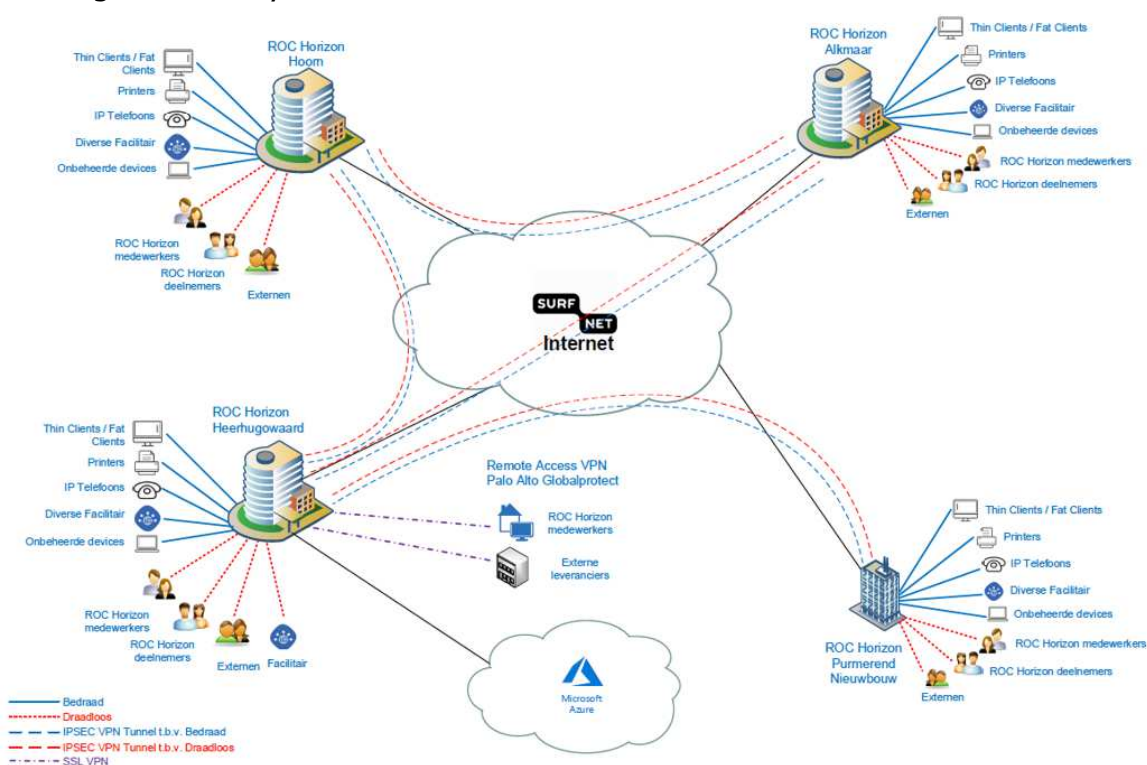


Annex VI - Technische infrastructuur

Horizon College

Onderstaand treft u de omschrijving aan van de technische infrastructuur van de aanbestedende dienst. Deze omschrijving geldt als vertrekpunt voor de door Inschrijver aan te bieden Apparatuur. De door inschrijver aan te bieden apparatuur dient binnen dit netwerk te kunnen functioneren zonder dat dit afbreuk doet aan de functionaliteit(en) van de aangeboden apparatuur.

A.1 Geografisch en fysiek



Het netwerk van de aanbestedende dienst omvat de locaties van het Horizon College en een extern Azure datacenter. De locaties zijn onderling verbonden via IPSEC VPN tunnels over SURFNET internet verbindingen.

A.2 Media Access control-laag

Er wordt gebruik gemaakt van VLAN-isolatie op basis van 802.1Q. De multifunctionals worden op een VLAN toegelaten op grond van IEEE 802.1x (voorkeur) of MAC-adresregistratie. Horizon College maakt als NAC oplossing gebruik van Tesorion Qmanage.

A.3 Datalinklaag

De aanbestedende dienst maakt gebruik van een ethernet-netwerk volgens IEEE 802.3. Multifunctionals zullen worden aangesloten op RJ45 outlets (IEEE 802.3ab).

A.4 Netwerklaag en transportlaag

De communicatie op het netwerk maakt gebruik van IP-protocol versie 4 (IETF RFC 791) . Adressering is dynamisch, IPv4-adressen worden door DHCP-servers uitgereikt (RFC 2131); er wordt gebruik gemaakt van publieke IP-adressen. . De scheiding tussen het netwerk en het internet vindt plaats op een router/firewall. Uitgaand dataverkeer van de multifunctionals naar internet zal worden doorgelaten door de firewall, inkomend dataverkeer zal worden geblokkeerd. Verkeer tussen gebruikersdevices en multifunctionals en vice versa wordt geblokkeerd. Naamresolutie vindt plaats door middel van DNS (IETF RFC 1035).

Op dit moment staat op iedere locatie van het Horizon College een Palo Alto Firewall

A.5 Authenticatie, autorisatie en user provisioning

Vanaf willekeurige internetadressen kan geauthentiseerd en geautoriseerd worden door gebruik te maken van single sign on, met de protocollen SAML2 en OpenID Connect. Provisioning en de-provisioning van user accounts kan worden gerealiseerd middels het protocol SCIMv2.

Horizon College maakt voor identiteiten gebruik van Microsoft Active Directory en Azure Active Directory. Deze Accounts worden automatisch aangemaakt via Microsoft Identity Manager (MIM).

Horizon College maakt voor (mobiele) werkplekbeheer gebruik van Microsoft Intune.

A.6 Gebruikersomgeving

Gebruikers moeten kunnen afdrukken vanaf desktop- en mobiele apparaten, ongeacht het type apparaat, ongeacht het besturingssysteem en vanaf elke locatie waarvandaan een beveiligde internetverbinding kan worden gemaakt. De gangbare systemen dienen ondersteund te worden, in ieder geval Windows, MacOS, ChromeOS, Android, iOS en iPadOS in door de producent ondersteunde versies.

Het moet tevens mogelijk zijn om te kunnen printen vanaf de Citrix remote werkplek en de Azure Virtual Desktop remote werkplek.

A.7 Aanwezige gebruikerspassen

Authenticatie van gebruikers bij de multifunctionals moet mogelijk zijn door het presenteren van een pas of tag en een nader te bepalen alternatief (pincode o.i.d.). De gangbare systemen dienen ondersteund te worden, in ieder geval Mifare DESFire.