Belastingdienst

AANSLUITVOORWAARDEN NETWERKAANSLUITDIENSTEN DATACENTER

Geschikt voor eventuele externe distributie

Datum 30-3-2021
Status 1.6

1 Documenteigenschappen

Versie voor eventuele externe distributie gemaakt door DCS (Data Center Services) afdeling Netwerken op 30-3-2021 met goedkeuring van afdelings-management.

2 Inleiding

Dit document is opgesteld om duidelijkheid te verschaffen in de faciliteiten die door de Belastingdienst netwerk infrastructuur geleverd worden, en de voorwaarden die door de Belastingdienst netwerk infrastructuur gesteld worden aan platformen die aansluiten op deze infrastructuur.

Dit hoofddocument bevat geen of zo min mogelijk vertrouwelijke informatie zodat het eenvoudig te delen is of geschikt te maken is daarvoor. De bijlagen bevatten details omtrent de zonering en zijn daarom gerubriceerd als Departementaal VERTROUWELIJK.

Deze aansluitvoorwaarden zijn van toepassing op de dienst ***Netwerkaansluitdiensten datacenter***.

De aansluitvoorwaarden zijn opgesplitst in 4 secties:

- Aansluitingen in de Business zone
- Aansluitingen in de Beheer en Audit zone
- Aansluitingen in de Belastingdienst DMZ of Kantoor DMZ
- Aansluitingen in Extranet

In het document worden de aansluitvoorwaarden beschreven als STANDAARD, MOGELIJK of OPTIE. Daarmee wordt het volgende bedoeld:

STANDAARD	Een aansluitvoorwaarde die als standaard gedefinieerd is binnen de service.
MOGELIJK	Een keuzemogelijkheid die ontworpen is en beschikbaar binnen de service.
OPTIE	Een optie is een keuzemogelijkheid die niet breed beschikbaar is of verder ontworpen kan worden binnen de service. Opties moeten worden aangevraagd.

Naast aansluitvoorwaarden worden allereerst ook de leveringsvoorwaarden volgens dezelfde indeling uitgewerkt, de voorwaarden waaraan DCS Netwerken door afnemers gehouden kan worden.

3 Toelichting netwerk- en beveiligingsfuncties

3.1 Beveiligingsuitgangspunten

Om risico's te isoleren leveren de Netwerkaansluitdiensten datacenter aansluitingen in verschillende zones. Het bijbehorende zoneringsmodel is geactualiseerd[1] waarbij het nu ook het POD[2] model bevat, aansluit op Overheids DataCenter (ODC) ontwikkelingen zoals het Rijks Overheids Netwerk (RON2.0) en nog steeds conform architectuurprincipes van NORA is. In Bijlage 1 - Toelichting zoneringsmodel staat hiervan een uitleg.

In de verschillende zones gelden verschillende voorwaarden en diensten. De voorwaarden zijn er onder andere om multi-tenancy met gedeelde infrastructuur te kunnen faciliteren.

3.2 QoS

In door DCS beheerde netwerken[3] wordt gebruik gemaakt van Quality of Service.
Tegenwoordig is er meer en meer samenwerking tussen overheidspartijen en hebben we koppelingen naar andere ODC's over een onderliggend netwerk van Defensie. Dit vraagt om standaardisering van de externe koppelvlakken van een bouwsteen.
De interne QoS inrichting mag per bouwsteen best specifiek zijn. Markeringen mogen techniek afhankelijk zijn, bij gebruik van MPLS bijvoorbeeld intern EXP markeringen of bij een L2 bouwsteen intern CoS markeringen om het verkeer met de juiste prioriteit en garanties door de bouwsteen te transporteren.

3.2.1 Interne Koppelvlakken

De onderstaande tabel vormt de basis voor de technische invulling van het interne QoS model voor deze bouwsteen.

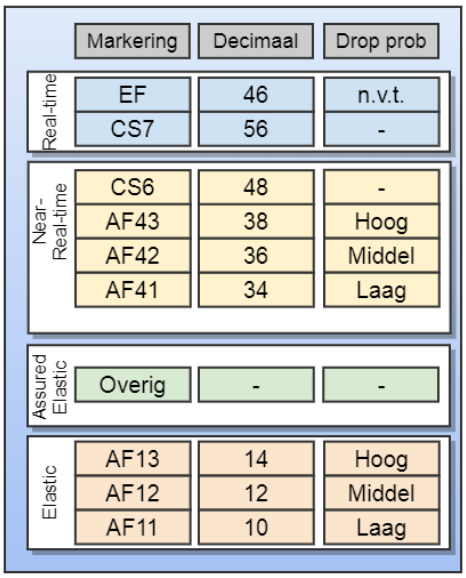
Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Network Control	7	CS7	56	7
Internetworking Control	6	CS6	48	6
Voice	5	EF	46	5
Video	4	AF41	34	4
Call Signaling	3	AF31 → CS3*	26 → 24	3
Transactional Data	2	AF21	18	2
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

Figuur 1 - overzicht QOS intern koppelvlak

3.2.2 Extern Koppelvlak

Voor het externe koppelvlak, de koppelingen tussen bouwstenen onderling, is een standaard model afgesproken. Dat model is intern afgestemd met de afdelingen CCI en MCS en komt overeen met het model dat Logius hanteert op RON. Hierdoor wordt end-to-end QoS tussen de verschillende ODC's mogelijk.
Onderstaande tabel vormt de basis voor de technische invulling van het externe koppelvlak. In Bijlage 4 is de inrichting en onderbouwing hiervan in meer detail beschreven.

1 Globaal Ontwerp Zonering v1.0 - 29-06-2018 - DCS Netwerken
2 In hoofdstuk 5 Begrippen zijn de verschillende onderwerpen rond o.a. informatiebeveiliging uitgewerkt die in dit document gebruikt worden.
3 Bij "Interface specificaties" elders in dit document staat voor welke zones dit van toepassing is.



Figuur 2; overzicht QOS extern koppelvlak

4 Aansluit- en leveringsvoorwaarden

4.1 Uitgangspunten

Voor aansluiting van apparatuur op de netwerk infrastructuur in de datacenters en DMZ van de Belastingdienst zijn een aantal uitgangspunten belangrijk:

- IP Multicast en IPv6 worden momenteel niet actief ondersteund;
- Loadbalancing, NTP, DHCP en DNS worden aangeboden als generieke dienst binnen de Netwerkaansluitdiensten datacenter;
- Microsoft loadbalancing (unicast[4]) is niet toegestaan in verband met het verkeersprofiel binnen een VLAN;
- IP adressen worden door DCS toegekend.

4.2 Leveringsvoorwaarden Netwerkaansluitdiensten datacenter

In onderstaand overzicht staat voor de verschillende plaatsen in het datacenter wat de leveringsvoorwaarden zijn waaraan DCS Netwerken door afnemers gehouden kan worden.

ONTWERP	KEUZE	Business zone	B&A zone	BDMZ / KDMZ	Extranet
LEVERINGSVOORWAARDEN					
Beschikbaar-heidsniveau	**STANDAARD**: De beschikbaarheid van de Netwerkaansluitdiensten datacenter is T2 zoals gespecificeerd in de DCS kaders [5].	√	√	√	√
Beveiligings-niveau	**STANDAARD**: De infrastructuur waarmee Netwerkaansluitdiensten datacenter gerealiseerd is heeft het basisbeveiligingsniveau 2 (BBN2) zoals gedefinieerd in de BIO [6].	√		√	√
	STANDAARD: De infrastructuur waarmee Netwerkaansluitdiensten datacenter gerealiseerd is heeft het basisbeveiligingsniveau 3 (BBN3) zoals gedefinieerd in BIO.		√		
Vertrouwelijk-heidsniveau	**STANDAARD**: De Netwerkaansluitdiensten datacenter zijn geschikt voor het transporteren van Departementaal Vertrouwelijke data.	√	√	√ / Niet richting zone Extern	
	STANDAARD: De Netwerkaansluitdiensten datacenter zijn geschikt voor het aansluiten van systemen met opslag van Departementaal Vertrouwelijke data.	√	√		
Vertrouwens-niveau	**STANDAARD**: De Netwerkaansluitdiensten datacenter zijn in beheer van de afdeling DCS Netwerken. De afdeling voldoet aan de status Vertrouwd.	√	√	√	√
	STANDAARD: De zone en objecten daarbinnen zijn “Vertrouwd”. Ze dienen dan wel te voldoen aan de aansluitvoorwaarden voor de zone.	√	√		
	STANDAARD: De zone en objecten daarbinnen zijn “Semi-vertrouwd”. Ze dienen dan wel te voldoen aan de aansluitvoorwaarden voor de zone.			√	√

4 Nieuw is dat MS multicast met normaal gebruik van IGMP levert; dat is wellicht in overleg wel te ondersteunen.
5 Technische architectuurkaders BCM CIE 1.0 – Belastingdienst IV DCS/Architectuur – 25-06-2015
6 https://cip-overheid.nl/

4.3 Aansluitvoorwaarden Netwerkaansluitdiensten datacenter

In het onderstaande overzicht staan voor de verschillende plaatsen in het datacenter de aansluitvoorwaarden. Een uitgebreide toelichting hiervoor staat in het volgende hoofdstuk.

Onder “Servers” worden aansluitingen bedoeld voor servers geplaatst in de datacenter(s) van de Belastingdienst. Onder ‘Overig’ worden aansluitingen bedoeld daar waar het aansluiten als “server” niet werkbaar of wenselijk is in de datacenter(s) van de belastingdienst, zoals appliances en totaal oplossingen.

4.3.1 Interface specificaties

ONTWERP	KEUZE	Business zone	B&A zone	BDMZ / KDMZ	Extranet
INTERFACE SPECIFICATIES					
100/1000 Mbps koper	**STANDAARD**: Autonegotiate, koper met RJ45 connector	√	√	√	√
	MOGELIJK: 100Mbps fixed [7]	√	√	√	√
1/10Gbps	**STANDAARD:** Autonegotiate, koper met RJ45 connector	√	√	√	√
	MOGELIJK: Multimode fiber, SX LC	√	√	√	√
	OPTIE: Singlemode fiber [8], LX LC	√	√	√	√
40/100Gbps [9]	**OPTIE**: Multimode fiber, SX LC			√	
	OPTIE: Singlemode fiber, LX LC			√	
Connectiviteit	**STANDAARD**: redundant d.m.v. adapter teaming active/passive of active/active	√	√	√	√
	MOGELIJK: Link aggregation door middel van teaming is in overleg toegestaan (bundelen van meerdere interfaces voor meer bandbreedte) op basis van LACP.	√	√	√	√
	OPTIE: In overleg is aansluiten met een enkele aansluiting mogelijk maar altijd met een lager service niveau.	√	√	√	√
MTU	**STANDAARD**: De IP MTU van klantsystemen is maximaal 9000 bytes.	√	√	√	√
Spanning Tree	**STANDAARD**: Systemen dienen loop-free gekoppeld te worden. [10]	√	√	√	√
QoS intern	**STANDAARD**: Verkeer in best effort Queue [11]	√	√		
	MOGELIJK: Bepaalde verkeersstromen in andere QoS klasse	√	√		
	OPTIE: QoS trust	√	√		
	STANDAARD: Geen QoS			√	√
QoS extern	**STANDAARD**: Eigenaar bepaald zelf de QoS markering. Transport van verkeer gebeurt volgens de tabel zoals aangegeven in 3.2.2 van dit document. QoS trust tussen bouwstenen onderling.	√	√		
	STANDAARD: Geen QoS, al het verkeer wordt gehermarkeerd en conform Assured Elastic getransporteerd			√	√

7: 100Mb aansluitingen zijn specifiek bedoeld voor Console aansluitingen. Denk daarbij aan beheer-interfaces van oudere appliances.
8: Single mode in overleg vanwege beperkt gebruik singlemode backbone bekabeling binnen een gebouw.
9: 40 Gbps is normaal op aanvraag maar in nieuwe POD’s vaak al standaard. Ook 100G is in POD’s leverbaar.
10: Het koppelen van devices die richting de belastingdienst netwerk infrastructuur Spanning Tree communiceren is niet toegestaan.
11: Aanvraag voor andere verkeersklassen in overleg.

VLAN	**STANDAARD**: Meerdere VLAN's getrunkt op één interface. (IEEE 802.1q) [12]	Servers	Servers	Servers	
	MOGELIJK: Interface geconfigureerd in één vast VLAN	Servers	Servers	Servers	√
	STANDAARD: Interface geconfigureerd in één vast VLAN	Overig	Overig	Overig	
	MOGELIJK: Meerdere VLAN's getrunkt op één interface (IEEE 802.1q)	Overig	Overig	Overig	√
	STANDAARD: Routering door middel van routeringsprotocollen wordt niet toegestaan.	√	√	√	√
Routering	**OPTIE**: Maatwerk voor een specifiek platform is een optie.	√	√	√	√
	STANDAARD: IP Packet forwarding wordt niet toegestaan.	√	√	√	√
Packet forwarding	**STANDAARD**: Systemen zijn met maximaal één hoofdzone verbonden. M.a.w. systemen gebruiken fysiek gescheiden hardware per zone.	√	√	√	√
Zonering	**STANDAARD**: Systemen dienen te voldoen aan BIO [13] op niveau BBN2 en dienen in beheer zijn bij DCS.	√	√	√	
	STANDAARD: Lijnmanagers van systemen dienen securitymonitoring afspraken middels use-cases te maken met het SOC.	√	√	√	
	STANDAARD: Systemen dienen in deze zone(s) geen opslag van niet-publieke data doen.			√	√
	STANDAARD: Systemen mogen in meerdere sub-zones (ge-firewall-de segmenten) geplaatst worden om bijvoorbeeld presentatie- en applicatie laag van elkaar te scheiden.		√	√	√
	STANDAARD: Een sub-zone is een verantwoordelijkheidsgebied waarvoor DCS-Netwerken één klant (DCS infra team) laat bepalen welke systemen en verkeersstromen aan te sluiten of verwijderen.		√	√	√
	MOGELIJK: Meerdere systemen mogen een sub-zone met elkaar delen als de verantwoordelijken van alle betrokken systemen daarmee akkoord zijn.		√	√	√
	MOGELIJK: Systemen die onbekend zijn voor, en niet in beheer zijn bij DCS en zich in het datacenter van DCS bevinden kunnen aangesloten worden in het Extranet.				√

12: VLAN's zijn transparant over locaties en kastenrijen beschikbaar.

[13] De BIO staat op het intranet maar ook hier https://bio-overheid.nl/ . Als aan te sluiten systemen niet aan de minimale beveiligingseisen voldoen kan dat invloed hebben op andere informatiesystemen. Overleg over aansluiten is dan altijd nodig. Ook als de systemen onder een hoger dreiging vallen dient overleg plaats te vinden. Meestal levert de BIO Baselinetoets vervolgens duidelijkheid https://www.informatiebeveiligingsdienst.nl/product/baselinetoets-bbn-bio/ .

4.3.2 Netwerkverbindingsdiensten

Onderstaande functies en voorwaarden vallen ook onder Netwerkverbindingsdiensten[14] maar worden geleverd door of zijn logisch verbonden met Netwerkaansluitdiensten datacenter en staan daarom in hetzelfde aansluitvoorwaarden document.

ONTWERP	KEUZE	Business zone	B&A zone	BDMZ / KDMZ	Extranet
NETWERKVERBINDINGSDIENSTEN					
IP adres	**STANDAARD**: Dynamische IP adres uitgifte. [15]	√	√		
	MOGELIJK: Statische IP adressen	√	√	√	
	OPTIE: Uitgifte van een IP range	Overig	Overig		√
	STANDAARD: Semi-dynamische IP adres uitgifte, vanuit Belastingdienst IPAM omgeving.			√	√
	OPTIE: Dynamische IP adressen (met een uniek VLAN per platform)			√	
DNS naamgeving	**STANDAARD**: Naamgeving conform RFC 952 Tot 24 karakters lang, letters A-Z, cijfers 0-9 en het minus teken (-) zijn toegestaan. Er wordt géén onderscheid gemaakt tussen hoofd en kleine letters.	√	√	√	
	MOGELIJK: Voor dynamische registratie van service records door AD servers wordt het underscore (_) teken toegestaan.	√	√	√	
DNS entries	**STANDAARD**: Dynamische DNS entry	√	√	√	
	MOGELIJK: Een of meerdere aliassen	√	√	√	
Verkeers-stromen	**STANDAARD**: Systemen hebben vrij IPv4 verkeer binnen de subzone. Een subzone bestaat uit één of meer subnetten en VLAN's waarbinnen geen filtering vanuit de netwerkdienstverlening plaatsvindt.	√	√	√	√
	STANDAARD: Verkeersstromen worden binnen en tussen zones selectief toegestaan. De uitgangssituatie is geen verkeersstromen.		√	√	√
	STANDAARD: Netwerken levert op verzoek IPv4 verbindingen als de betrokken verantwoordelijken[16] voor de sub-zones akkoord zijn (kan dezelfde partij zijn). De locaties van deze dienstverlening zijn met 1 aangemerkt in bijlage 2.	√	√	√	√
	STANDAARD: Netwerken kan en/of mag geen IPv4 verbinding leveren op de locaties zoals aangegeven met een 0 in bijlage 2.	√	√	√	√
	STANDAARD: Aangesloten systemen voeren geen portscans of pingsweeps uit in het netwerk[17] maar gebruiken hiervoor de diensten van Security Tooling of SOC.	√	√	√	√

14: "Netwerkaansluitdiensten datacenter" en "Netwerkverbindingsdiensten" zijn beiden onderdeel van Basisinfrastructuurdienst "Netwerkconnectiviteit".
15: Gebruik van DHCP UserClass-ID voor toekennen van DNS naam, WINS server etc. is mogelijk.
16 De verantwoordelijken / betrokken partijen zijn in bijlage 2 voor alle regels en kolommen ingevuld.
17 Dit bemoeilijkt herkennen van verdacht verkeer.

5 Begrippen

(Basis)beveiligings-Niveau	Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveau's (BBN). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is. De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement.
Grensbescherming	DCS aanduiding voor combinatie van firewall en IPS of IDS.
IP Packet forwarding	Packet forwarding is het routeren van pakketten op laag 3 van de TCP/IP stack op een systeem.
MTU	Maximum Transmission Unit. Grootste formaat dat over een netwerkprotocol laag getransporteerd kan worden in een enkele netwerk transactie. Belangrijk is het onderscheid tussen de interface (Ethernet) MTU en de IP MTU. In dit document is telkens sprake van de IP MTU. De IP MTU is het maximale formaat van het IP pakket over een interface, zonder daarbij de overhead van het omliggende protocol mee te tellen. Ethernet protocol velden zoals source- en destination MAC adres, preamble, SFD en FCS tellen dus niet mee in een IP MTU.
POD	Point Of Delivery. Een POD is een autonome groep IT-infrastructuur (netwerk-infra, server infra, etc.) die aan de routing core van DCS (BKN, Basis Koppel Netwerk) gekoppeld wordt waarbij de verantwoordelijkheid voor de beveiliging (conform Rijksoverheidsrichtlijnen) van de POD bij één klant/afnemer ligt zodat deze de beveiliging over de hele informatieketen van desbetreffende processen zelf kan bepalen. Een POD kent netwerk-gebaseerde demarcatiepunten en aansluitvoorwaarden die verder beschreven zijn in de aansluitvoorwaarden BKN.
Rubriceringsniveau	Zie: vertrouwelijkheidsniveau
Security Level	Zie: beveiligingsniveau
Verkeersstroom	Definitie verkeersstroom Voor verkeersstromen door DCS beheerde infra gelden een aantal regels. Een verkeersstroom wordt als volgt gedefinieerd: • één partij neemt het initiatief voor de verkeersstroom; • een verkeersstroom heeft een logisch begin en eindpunt; • een verkeersstroom kent een richting; • van een verkeersstroom is bekend wat de functie is; • van een verkeersstroom zijn de eigenschappen en omvang bekend.
Vertrouwelijkheidsniveau	Aanduiding van de verwachte nadelige gevolgen aan de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) de informatie bekend wordt bij niet geautoriseerden." Bron: definitie rubriceringsniveau uit VIRBI 2013 [18]. De BIO heeft Departementaal Vertrouwelijk als uitgangspunt voor BBN2 (basisbeveiligingsniveau) zonder hoge dreiging en BBN3 mét hoge dreiging.

18 http://wetten.overheid.nl/jci1.3:c:BWBR0033507&z=2013-06-01&g=2013-06-01

Vertrouwensniveau	Een officiële definitie vanuit de NORA ontbreekt (bron voor de zonering van de datacenter netwerken in beheer van DCS). Wel heeft DCS op basis van de NORA voor ieder vertrouwensniveau aansluitvoorwaarden. De volgende niveaus worden gehanteerd: Onvertrouwd, Semi-vertrouwd en Vertrouwd. Daarnaast is er nog het niveau “extra beveiligd” hetgeen betekend dat er een hoger “beveiligingsniveau” wordt toegepast.
Zones	Zones zijn netwerkcompartimenten met een bepaald niveau van vertrouwen, vertrouwelijkheid en beveiliging. Met deze eigenschappen is een zone goed te beschrijven. In de Bijlage 1 Toelichting zoneringsmodel is dit onder “Beveiligingskenmerken van bouwstenen en zones” concreet gemaakt voor het ODC Belastingdienst.

Bijlage 1 - Toelichting zoneringsmodel

Deze bijlage is Departementaal Vertrouwelijk en is daarom een separaat bestand.

Bijlage 2 - Verkeersstromen matrix ODC Belastingdienst

Deze bijlage is Departementaal Vertrouwelijk en is daarom een separaat bestand.

Bijlage 3 – Standaardisatie inrichting QoS

Deze bijlage is Departementaal Vertrouwelijk en is daarom een separaat bestand.

Bijlage 4 – UBGI

UBGI staat voor Uitvoeren, Beoordelen, Goedkeuren Informeren.

Deze bijlage met namen van medewerkers, functies, review details en akkoorden is niet geschikt voor externe communicatie en is daarom een separaat bestand.