Belastingdienst

AANSLUITVOORWAARDEN ALGEMENE WEB PROXY, NETWERK VIRUSSCANNER & SECURE WEB GATEWAY

Geschikt voor eventuele externe distributie

Datum	21-2-2022
Status	1.0

1 Documenteigenschappen

Versie voor eventuele externe distributie gemaakt door Belastingdienst - IV - DCS (Data Center Services) afdeling Netwerken op 21-2-2022 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:
Algemene Web Proxy
Netwerk Virusscanner
Secure Web Gateway

Termen die komen te vervallen binnen Archimate / detaillering van het dienstenaanbod:
<IS> Bestandsfiltering
<IS> Content Filtering
<IS> Internet op de werkplek web schoning
<IS> Proxying
<IS> Web filtering

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

Buiten scope:

- Cloud gebaseerde SWG functionaliteiten voor mobiele apparaten die zich buiten de infrastructuur van de Belastingdienst bevinden.

4 Aansluit- en leveringsvoorwaarden

4.1 Leveringsvoorwaarden

In onderstaand overzicht staan leveringsvoorwaarden waaraan DCS Netwerken door afgesproken klanten gehouden kan worden.

ONTWERP	KEUZE	Algemene Web Proxy	Netwerk Virus-scanner	Secure Web Gateway (SWG)
Beschikbaar-heidsniveau	**STANDAARD**: De beschikbaarheid van deze diensten[1] is T1 zoals gespecificeerd in de DCS kaders[2].	√	√	√
Beveiligings-niveau	**STANDAARD**: De infrastructuur waarmee deze diensten[1] gerealiseerd zijn (onderdeel van de Netwerk Verbindingsdiensten) hebben basisbeveiligingsniveau 2 (BBN2) zoals gedefinieerd in de BIO[3].	√	√	√
Vertrouwelijk-heidsniveau	**STANDAARD**: De diensten[1] zijn geschikt voor het transporteren van Departementaal Vertrouwelijke data.	√ / Niet met zone Extern	√ / Niet met zone Extern	√ / Niet met zone Extern
	STANDAARD: De diensten[1] zijn geschikt voor het aansluiten van systemen met opslag van Departementaal Vertrouwelijke data.	√	√	√
Vertrouwens-niveau	**STANDAARD**: De diensten[1] zijn in technisch[4] beheer van de afdeling DCS Netwerken. De afdeling voldoet aan de status Vertrouwd.	√	√	√
Privacy	**STANDAARD**: De diensten[1] zijn geschikt[5] voor het transporteren en, indien van toepassing, het opslaan van gegevens die onder de AVG[6] vallen.	√	√	√
HTTP-proxy: logging	**STANDAARD**: De proxy logged van alle sessies van de HTTP headers de request URL en enkele variabelen zoals de categorisering van het domein. Deze logging gaat naar Splunk en is enkel voor het SOC voor het kunnen uitvoeren van security use-cases en het NOC voor het kunnen afhandelen van incidenten en problems.	√		√
	STANDAARD: De proxy logged standaard een SHA256 checksum van bestanden die binnen de HTTP stromen gezien worden. Deze logging voor het SOC voor het kunnen uitvoeren van security user-cases.	√ toekomst	√ AV-toekomst	√ SWG-toekomst

1 De diensten hier zijn onderdeel van de Netwerk Verbindingsdiensten.
2 Technische architectuurkaders BCM CIE 1.0 – Belastingdienst IV DCS/Architectuur – 25-06-2015
3 https://cip-overheid.nl/
4 Niet alles valt onder deze technische verantwoordelijkheid, met name niet de functionele inrichting zoals rules voor een klant. Zie opmerkingen over functioneel beheer elders in de aansluitvoorwaarden.
5 Afdeling Netwerken streeft er in haar diensten naar persoonsgegevens en gedragsgegevens / meta-data in beheer van Belastingdienst-IV personeel en fysiek binnen ODC-Belastingdienst te houden (Overheids DataCenter).
6 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving

4.2 Aansluitvoorwaarden

In onderstaand overzicht staan aansluitvoorwaarden waaronder DCS Netwerken aan afgesproken klanten diensten kan leveren.

ONTWERP	KEUZE	Algemene Web Proxy	Netwerk Virus-scanner	Secure Web Gateway (SWG)
INTERFACE SPECIFICATIES				
Protocol	**STANDAARD**: IPv4 ondersteuning.	√	Nvt	√
	MOGELIJK: IPv6[7] ondersteuning.	√	Nvt	√
QoS	**STANDAARD**: Geen QoS.	√	√	√
Zonering	**STANDAARD**: De proxy functies leveren diensten vanuit de zones KDMZ of BDMZ tussen de zone Extern en interne zones van ODC Belastingdienst.	BDMZ / KDMZ	BDMZ / KDMZ	BDMZ / KDMZ
NETWERKVERBINDINGSDIENSTEN				
Verkeers-stromen	**STANDAARD**: Verkeersstromen worden binnen en tussen zones selectief toegestaan. De uitgangssituatie is geen verkeersstromen.	√	√	√
	STANDAARD: Netwerken levert op verzoek verbindingen als de betrokken verantwoordelijken[8] 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 verbinding leveren op de locaties zoals aangegeven met een 0 in bijlage 2.	√	√	√
	STANDAARD: Verkeersstromen om beveiligingsverkenning mee uit te voeren zijn niet toegestaan (scans).	√	√	√
HTTP-proxy: forward	**STANDAARD**: De HTTP-proxy functie levert diensten aan interne resources om deze af te schermen van externe invloeden. Dit heet ook wel een HTTP-forward-proxy.	√		√
HTTP-proxy: reverse	**OPTIE**: In overleg is het mogelijk een HTTP-reverse-proxy te bieden waarmee minder-vertrouwde devices een selectie van interne webservices kan benaderen. Deze functie kan, in overleg, gebruik maken van onderstaande HTTP-proxy functies. Hierbij dient een expliciete allow list voor interne sites / usergroepen en externe sites op de proxy actief te zijn. Het functionele beheer van deze list en (afstemming met de security organisatie over) de gevolgen voor de gebruikers van deze klantstroom zijn voor verantwoordelijkheid van desbetreffende klant[9].			√
HTTP-proxy: TLS intercept	**STANDAARD**: De proxy maakt inspectie van HTTPS verkeer mogelijk door alle verbindingen met extern te termineren op de proxy en verkeer naar intern te ondertekenen met een CA van de interne-PKI. Voor TLS instellingen worden de richtlijnen[10] van het NCSC gehanteerd.	√		√
HTTP-proxy: verkeerstypen en filters	**STANDAARD**: De proxy ondersteunt HTTP/1.0, HTTP/1.1 en HTTP/2, allemaal zo goed als mogelijk. Overige HTTP typen worden standaard geblokkeerd.	√		√ huidige SWG

7 De apparatuur zelf is geschikt maar de rest van de keten hoeft dat nog niet te zijn.
8 De verantwoordelijken / betrokken partijen zijn in bijlage 2 voor alle regels en kolommen ingevuld.
9 Een klant van de proxy-dienst is altijd een andere dienst binnen IV, nooit direct een eindgebruiker/persoon.
10 https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

	STANDAARD: De proxy ondersteunt HTTP/1.0, HTTP/1.1, HTTP/2, HTTP/3 en QUIC, allemaal zo goed als mogelijk. Overige HTTP typen worden standaard geblokkeerd.	√		√ SWG-toekomst
	STANDAARD: De proxy blokkeert standaard op best-effort basis verkeer met malicieuze HTTP headers.	√		√
	STANDAARD: De proxy schoont standaard verkeer vanaf clients door de Client-IP HTTP-header en vendor-specifieke HTTP-headers te wissen.	√		√
	OPTIE: In overleg zijn andere HTTP header filters mogelijk.	√		√
	STANDAARD: De proxy levert een klassieke HTTP proxy functie: een HTTP request forwarden namens een browser die een proxy-IP adres ingesteld heeft (bijvoorbeeld via een PAC-file).	√		√
	STANDAARD: HTTP verkeer afhandelen voor alle[11] populaire content-types zoals tekst/html, tekst/javascript, tekst/css, jpeg, gif, image/png, application/gzip.	√		√
	STANDAARD: De proxy blokkeert standaard verkeer op best-effort-basis met malicious Java-script.			√
	OPTIE: In overleg is blokkeren of juist accepteren van bepaalde content-types mogelijk.	√		√
	STANDAARD: Radio- en video streams best-effort afhandelen als het de volgende standaard MIME-types[12] bevat: audio/mp4, audio/mpeg, audio/mpeg-generic, audio/aac, video/MP2T, of de volgende niet-standaard MIME-type: x-m4a.	√		
HTTP-proxy: authenticatie	**STANDAARD**: Authenticatie van gebruikers middels NTLM tussen browser en proxy. Autorisatie van gebruikers: vraag van proxy aan AD over lidmaatschap user van AD-groep.			√ huidige SWG
	STANDAARD: Authenticatie van gebruikers middels Kerberos tussen browser en proxy. Autorisatie van gebruikers: vraag van proxy aan AD over lidmaatschap user van AD-groep.	√		√ SWG-toekomst
HTTP-proxy: IP/domain allow/block-list	**MOGELIJK**: Verkeer door de proxy kan voor een klant[13] expliciet toegestaan en/of geblokkeerd worden op basis van: - Internet IP-adressen/domeinnamen; - categorieën van Internet websites[14]. Het functionele beheer van iedere lijst en (afstemming met de security organisatie over) de gevolgen voor de gebruikers van deze klantstroom zijn voor verantwoordelijkheid van desbetreffende klant.			√
	OPTIE: In overleg is filtering op basis van overige URI onderdelen mogelijk.			√
HTTP-proxy: anti-virus	**STANDAARD**: Bestanden best-effort scannen op virussen/malware in een HTTP stroom met een andere[15] scan-engine dan op de DWB werkplek. Ondersteunt zijn Windows executables, javascript, java byte code, plaatjes, MS documents, PDF's, archive's, ISO's en true type fonts. De maximaal ondersteunde bestandsgrootte is 5GB. Niet herkende-, versleutelde of te grote bestanden worden doorgelaten. De actie bij een virus is verwijderen uit de stream, in quarantaine plaatsen en logmelding in Splunk voor het SOC..		√ huidige AV	

11 Vraag indien nodig om onze actuele details.
12 https://www.iana.org/assignments/media-types/media-types.xhtml
13 Een klant van de proxy-dienst is altijd een andere dienst binnen IV, nooit direct een eindgebruiker/persoon.
14 Voor de categorieën en de inhoud daarvan is de proxy dienst afhankelijk van wat de leverancier aanbiedt.
15 Details zijn indien nodig te delen.

	STANDAARD: Bestanden best-effort scannen op virussen/malware in een HTTP stroom met een andere[16] scan-engine dan op de DWB werkplek. Ondersteunt zijn Windows/Linux/Mac/Android binary executables, javascript, Java byte code, Linux shell script, Powershell script, Python code, plaatjes, MS documents, ODF documenten, PDF's, archive's, ISO's en true type fonts. De maximaal ondersteunde bestandsgrootte is 5GB. Niet herkende-, versleutelde of te grote bestanden worden doorgelaten. De actie bij een virus is verwijderen uit de stream, in quarantaine plaatsen en logmelding in Splunk voor het SOC.		√ AV-toekomst	
	MOGELIJK: Blokkeren van bestanden die niet gescanned kunnen worden omdat ze versleuteld zijn, te groot zijn of niet worden herkend.		√	
	OPTIE: Uitschakelen anti-virus/malware op een bepaalde stroom, bijvoorbeeld vanwege performance. Hiervoor dient toestemming van CISO te zijn.		√	
HTTP-proxy: disable functies	**OPTIE**: Verkeer door de proxy kan voor een klant[17] expliciet toegelaten worden zonder: - "HTTP-proxy: TLS intercept"[18]; - "HTTP-proxy: verkeerstypen en filters"; - "HTTP-proxy: IP/domain allow/block-list"; - "HTTP-proxy: anti-virus". *Let op: gebruik van deze functie zorgt voor een afwijking van architectuurrichtlijnen over DMZ gebruik en heeft impact op de beveiliging van de systemen in de lijst.* Het functionele beheer van iedere lijst en (afstemming met de security organisatie over) de gevolgen voor de gebruikers van deze klantstroom zijn voor verantwoordelijkheid van desbetreffende klant.			√
HTTP-proxy: bestanden-filter	**MOGELIJK**: Bestanden in een HTTP stroom best-effort herkennen op basis van inhoud. Actie: de default actie is loggen en doorlaten. Ondersteunt zijn Windows executables, javascript, java byte code, plaatjes, MS documents, PDF's, archive's, ISO's en true type fonts.		√ huidige AV/SWG combi	√ huidige AV/SWG combi
	MOGELIJK: Bestanden in een HTTP stroom best-effort herkennen op basis van inhoud. Actie: de default actie is loggen en doorlaten. Ondersteunt zijn Windows/Linux/Mac/Android binary executables, javascript, Java byte code, Linux shell script, Powershell script, Python code, plaatjes, MS documents, ODF documenten, PDF's, archive's, ISO's en true type fonts.		√ toekomst AV/SWG combi	√ toekomst AV/SWG combi
	MOGELIJK: Actie: bepaalde bestandstypen blokkeren.		√	√
	MOGELIJK: Actie: onbekende bestandstypen blokkeren.		√	√
	MOGELIJK: Actie: versleutelde bestanden blokkeren.		√	√
	MOGELIJK: Actie: bepaalde bestandsnaam-extensies blokkeren.		√	√
	MOGELIJK: Actie: niet matchende combinatie van bestandsnaam-extensie en bestandstype blokkeren.		√	√
HTTP-proxy: Data Leakage Prevention	**MOGELIJK**: Datalekken via de proxy kunnen door een klant[19] expliciet geblokkeerd worden op basis van: - eerder genoemde "HTTP-proxy: bestandenfilter"; - eerder genoemde "HTTP-proxy: IP/domain allow/block-list";			√

16 Details zijn indien nodig te delen.
17 Een klant van de proxy-dienst is altijd een andere dienst binnen IV, nooit direct een eindgebruiker/persoon.
18 Deze functie disabelen maakt ook alle volgende functies in de rij onmogelijk.
19 Een klant van de proxy-dienst is altijd een andere dienst binnen IV, nooit direct een eindgebruiker/persoon.

	Het functionele beheer van deze instellingen en (afstemming met de security organisatie over) de gevolgen voor de gebruikers van deze klantstroom zijn voor verantwoordelijkheid van desbetreffende klant.			
	OPTIE: De proxy kan in overleg verkeer tegenhouden op basis van een kenmerk van een document of content in een document, bijvoorbeeld een kenmerk zoals Departementaal Vertrouwelijk of content zoals een BSN nummer.			√ SWG-toekomst
HTTP-proxy: Advanced Thread Protection	**STANDAARD**: Verkeer door de proxy krijgt standaard een best-effort scan door middel van Advanced thread Protection zoals as-is geleverd door de producent. Verkeersstromen die met hoge zekerheid matchen worden gedropped. De gebruiker krijgt daarvan een melding.			√ SWG-toekomst
Remote browser isolation	**MOGELIJK**: Remote browser isolation (RBI) levert gebruikers een hoge zekerheid van isolatie[20] tussen het Internet en de werkplek van de gebruiker en heeft daarbij niet meer de browser-compatibiliteits-problemen van proxies. RBI beschermt gebruikers vooral tegen hacking/ransomware. Het lekken van data is hierbij nog beperkt mogelijk doordat de gebruiker toetsenbord input heeft en ook korte teksten kan copy-pasten. De RBI functie is aan te vullen met de volgende HTTP-proxy functie: “HTTP-proxy: IP/domain allow/block-list”.			√ SWG-toekomst
	MOGELIJK: Bestandsuitwisseling is mogelijk via een datasluis tussen RBI en de werkplek.			√ SWG-toekomst
CASB	**MOGELIJK**: In overleg is het mogelijk een CASB functie te bieden. Deze functie kan gebruik maken van de eerder genoemde functies en onderstaande CASB functies. Hierbij dient een expliciete allow list voor interne sites / usergroepen en externe sites op de proxy actief te zijn. Het functionele beheer van deze list en (afstemming met de security organisatie over) de gevolgen voor de gebruikers van deze klantstroom zijn voor verantwoordelijkheid van desbetreffende klant[21].			√ SWG-toekomst
	OPTIE: Adaptive access control (AAC): De Oplossing is uit te breiden met CASB functionaliteiten om Cloud toegang te blokkeren van al geautoriseerde gebruikers o.a. op basis van gebruik, tijdstip, locatie en indicaties van diefstal, gecompromitteerde gebruikersgegevens of een geavanceerde cyberaanval.			√ SWG-toekomst
	OPTIE: Application Discovery: De Oplossing biedt CASB functionaliteiten om granulair inzicht te krijgen in het gebruik van websites en Cloud diensten met als doel hier een Cloud applicatie beleid op te kunnen ontwikkelen en om de veiligheidsrisico’s van die Cloud applicaties te helpen beheersen.			√ SWG-toekomst
	OPTIE: Application risk and compliance assessment: De Oplossing biedt CASB functionaliteiten die inzicht bieden in de veiligheidsrisico’s van het gebruik en de mate van conformiteit van Cloud applicaties.			√ SWG-toekomst
	OPTIE: General data- and user-related monitoring and policy enforcement: De Oplossing biedt CASB functionaliteiten voor het toepassen van security policies en de monitoring van data en gebruikers.			√ SWG-toekomst

20 RBI werkt door de browser functie uit te voeren in de appliance en de beeld informatie naar de gebruiker te sturen zodat exploits in bijvoorbeeld HTML5, javascript, CSS, gzip of jpeg afkomstig van extern geen effect meer kunnen hebben op security-bugs in een browser of werkplek van de gebruiker.

21 Een klant van de proxy-dienst is altijd een andere dienst binnen IV, nooit direct een eindgebruiker/persoon.

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.
Klant	Een klant van de proxy-dienst is altijd een andere dienst binnen IV, nooit direct een eindgebruiker/persoon.
NOC	Network Operations Center, synoniem voor het Ops deel van het DevOps team van de afdeling Netwerken binnen Belastingdienst / IV /DCS
Rubriceringsniveau	Zie: vertrouwelijkheidsniveau
SOC	Security Operations Center, afdeling binnen Belastingdienst / IV / DCS voor security monitoring waar alle afdelingen van Belastingdienst IV bij moeten aansluiten.
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 [22]. De BIO heeft Departementaal Vertrouwelijk als uitgangspunt voor BBN2 (basisbeveiligingsniveau) zonder hoge dreiging en BBN3 mét hoge dreiging.
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.

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

6 Bijlage 1 - Toelichting zoneringsmodel

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

7 Bijlage 2 - Verkeersstromen matrix ODC Belastingdienst

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

8 Bijlage 3 – 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.