

Architectuur en koppelingen

Service Management Tool

Service Management Tool
20220630 Architectuur en koppelingen
Datum juni 2022
Joop Jansen

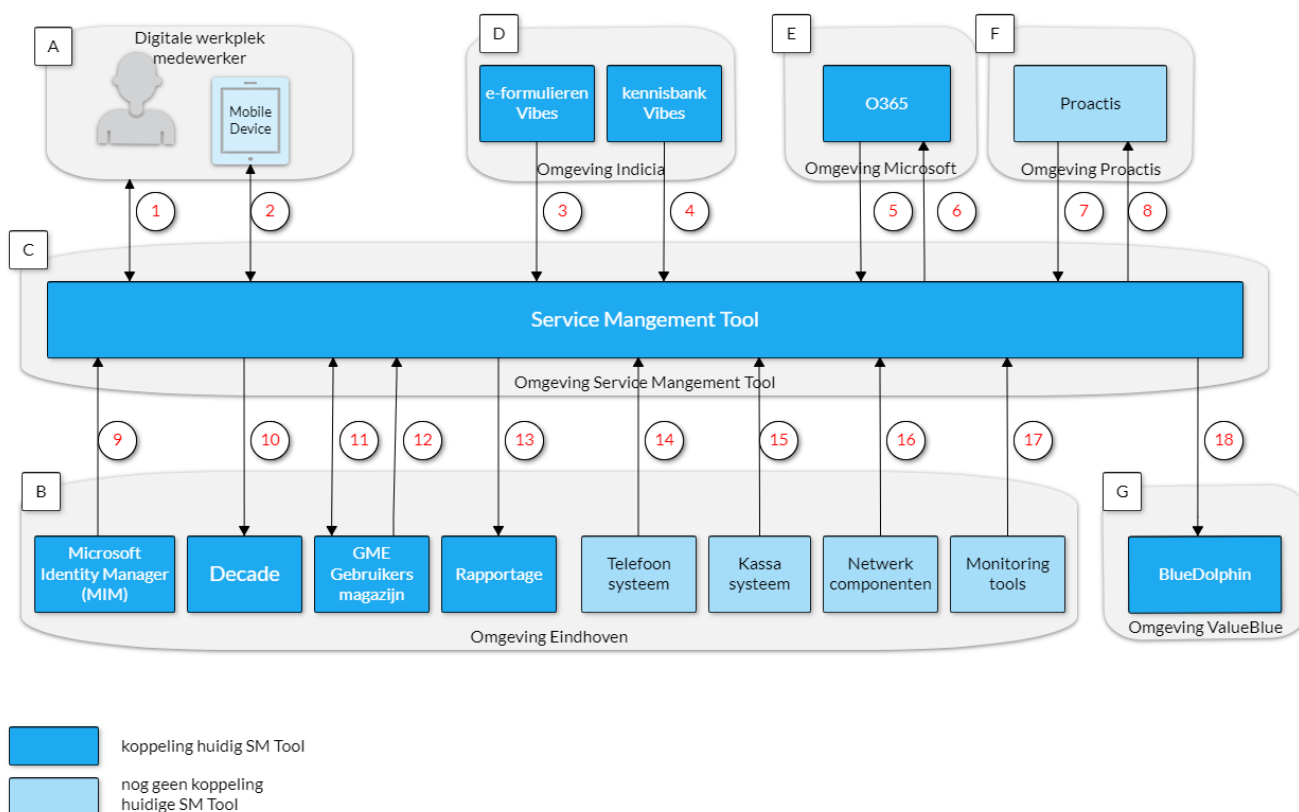
Inhoudsopgave

.....	
Inleiding.....	3
1 Omgevingen	3
(A): Omgeving digitale werkplek gemeente Eindhoven	3
(B): Omgeving gemeente Eindhoven	4
(C): Omgeving Service Management Tool	4
(D): Omgeving Indicia	4
(E): Omgeving Microsoft	4
(F): Omgeving Proactis	4
(G): Omgeving ValueBlue	4
2 Koppelingen.....	5
1 Medewerker vanuit digitale werkplek gemeente Eindhoven.....	5
2 Service Management Tool benaderbaar vanaf zakelijk Mobile Device medewerker	5
3 e-formulieren (Vibes) naar Service Management Tool.....	5
4 Kennisbank (Vibes) naar Service Management Tool	5
5 O365 naar Service Management Tool.....	6
6 Service Management Tool naar O365.....	6
7 Proactis naar Service Management Tool	6
8 Service Management Tool naar Proactis	6
9 Microsoft Identity Manager(MIM) naar Service Management Tool	6
10 Financiëlegegevens van Service Management Tool naar Decade	6
11 Service Management Tool naar GME Gebruikers magazijn	6
12 GME gebruikers magazijn naar Service Management Tool	6
13 Service Management Tool naar Rapportage	7
14 Telefoonsysteem naar Service Management Tool	7
15 Kassa system naar Service Management Tool	7
16 Netwerk componenten naar Service Management Tool.....	7
17 Monitoring Tools naar Service Management Tool.....	7
18 Service Management Tool naar BlueDolphin.....	7
Bijlage: Integratiepatronen	8

Inleiding

Deze bijlage beschrijft de Informatievoorziening van Eindhoven en architectuureisen waaraan Service Management Tool moet voldoen om de integratie met de Informatievoorziening van Eindhoven mogelijk te maken.

Onderstaande afbeelding (Figuur1) is de grafische weergave van de relevante omgevingen en de daarbij behorende koppelingen. Bij iedere omgeving is een letter geplaatst en bij iedere koppeling een nummer, deze worden in hoofdstuk één en twee beschreven.



Figuur 1: Context Service Management Tool

1 Omgevingen

(A): Omgeving digitale werkplek gemeente Eindhoven

Dit is de omgeving waarin de medewerker van de gemeente Eindhoven werkt. Het kan elke medewerker in elke rol zijn. De Medewerker krijgt toegang tot de Service Management Tool via een standaard webbrowser. Uiteraard hoort hier een identificatie-, authenticatie- en autorisatiemechanisme bij dat voldoende beveiliging en betrouwbaarheid biedt.

Devices

De medewerker van de gemeente Eindhoven beschikt over een standaard werkplek. Deze bestaat uit een Windows tablet voorzien van Windows 10.

Daarnaast kunnen medewerkers gebruik maken van een GSM waarbij gekozen kan worden voor een Android of Apple device.

Medewerkers kunnen ook gebruik maken van een IPAD die met behulp van Mobile Device Management wordt beheerd.

Webbrowser

De voorkeurs webbrowser is Microsoft Edge voor de Microsoft Windows devices.

Mobile device

Het zakelijke mobile device van de medewerker wordt gemanaged in de Mobile Device Mangement tooling.

(B): Omgeving gemeente Eindhoven

De Service Management Tool draait in de omgeving van de aanbieder als een zogenaamde Cloud applicatie en wisselt gegevens uit met informatiesystemen binnen de omgeving van de gemeente Eindhoven. Hiervoor zijn de volgende integratie- en beveiligingscomponenten in gebruik:

Firewall & Reverse Proxy/Load Balancer

Voor alle koppelingen geldt dat gegevensuitwisseling veilig gebeurt conform de informatiebeveiligingseisen. Een secure verbinding vanuit de SaaS aanbieder is op basis van SSL en een officieel PKI-certificaat, conform de richtlijnen van het Nationaal Cyber Security Center (TLS1.2 of hoger). Er wordt geen directe koppeling naar interne systemen vanaf het internet toegestaan deze loopt altijd via de Firewall->Reverse Proxy/Load Balancer->Enterprise Service Bus->Doel Systeem.

Enterprise Service Bus (ESB)

Geautomatiseerde gegevensuitwisseling tussen een SaaS applicatie en interne IV-systemen van de gemeente Eindhoven verloopt via de Enterprise Service Bus (ESB) van de gemeente Eindhoven. Op dit moment gebruikt de gemeente Eindhoven de ESB OpenTunnel van leverancier JNET.

In de nabije toekomst zal OpenTunnel worden vervangen door een integratieplatform dat de regie voert over alle koppelingen. Dit zal altijd op basis van geldende en actuele standaarden zijn.

(C): Omgeving Service Management Tool

Vanuit een Cloud omgeving biedt de Service Management Tool de medewerkers toegang tot de applicatie. Er vindt hierbij gegevensuitwisseling plaats met diverse andere systemen in verschillende omgevingen. De autorisatie en authenticatie wordt uitgevoerd door de Service Management Tool. De Service Management Tool garandeert de vertrouwelijkheid van de informatie in het systeem door ervoor te zorgen dat alleen de personen voor wie de informatie bedoeld is er toegang toe hebben op basis van een toegekende gebruikersrol.

(D): Omgeving Indicia

Binnen de omgeving Indicia draait het Intranet (Vibes).

(E): Omgeving Microsoft

Binnen de omgeving Microsoft draaien de toepassingen van Microsoft onder andere O365.

(F): Omgeving Proactis

Binnen de omgeving Proactis draait het Inkoop Management Systeem Proactis.

(G): Omgeving ValueBlue

Binnen de omgeving ValueBlue draait de architectuur-tool BlueDolphin

2 Koppelingen

In dit hoofdstuk worden de koppelingen beschreven, volgens de nummering die is aangegeven in de architectuurplaat. In de architectuurplaat zijn enkele applicaties licht blauw gekleurd. De koppelingen naar deze applicaties is met de huidige Service Management Tool niet gerealiseerd. De donker blauw gekleurde applicaties hebben een koppeling met de huidige Service Management Tool.

Voor de nieuwe Service Management Tool wordt verwacht dat alle genoemde koppelingen worden gerealiseerd.

Koppelingen tussen systemen zijn noodzakelijk op het moment dat er gegevens van een bronsysteem gebruikt moeten worden in een ander systeem, het doelsysteem. Het architectuurprincipe hierbij is dat broninformatie niet apart wordt opgeslagen om vervolgens als bron te dienen voor andere systemen. Dat betekent concreet dat de gewenste data uit het bronsysteem moet worden opgehaald en vervolgens op een veilige manier getransporteerd en geïntegreerd dient te worden in het relevante doelsysteem.

Bij de integratie van data moeten de datadefinities van het bron- en doelsysteem op elkaar worden afgestemd. Daarom is het nodig dat de data “vertaald” wordt zodat het doelsysteem de data van het bronsystemen kan gebruiken. Deze vertaling kan op verschillende plaatsen binnen de keten plaatsvinden.

In de bijlage een beschrijving van de integratiepatronen en hoe deze moeten worden toegepast binnen de gemeente Eindhoven.

Van de reeds bestaande koppelingen is de huidige situatie beschreven. Voor de nieuwe Service Management Tool willen we de meest real time mogelijkheid die kan worden geboden.

1 Medewerker vanuit digitale werkplek gemeente Eindhoven

Doel	Medewerker krijgt geautoriseerde toegang tot Service Management Tool
Patroon	Authenticatie (Single Sign On en Multi factor authenticatie)
Toe te passen Standaard	OAuth / SAML 2.0 protocol
Technische realisatie	Aandachtspunt: Bij een webapplicatie verloopt het netwerkverkeer via het https-protocol over poort 443. Medewerkers van de gemeente Eindhoven zijn opgenomen in de Active Directory (AD). Service Management Tool faciliteert Single-Sign-On (SSO). Single-Sign-On zorgt ervoor dat de medewerker niet een tweede keer - met een ander gebruikers account en wachtwoord - in hoeft in te loggen. De koppeling (trust) wordt via Azure AD gerealiseerd. Voor authenticatie wordt er gebruik gemaakt van multi factor authenticatie indien de medewerker buiten het beveiligd netwerk van de gemeente inlogt in Service Management Tool.

2 Service Management Tool benaderbaar vanaf zakelijk Mobile Device medewerker

Doel	Service Management Tool functionaliteit beschikbaar krijgen op een mobile device
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

3 e-formulieren (Vibes) naar Service Management Tool

Doel	e-formulieren worden met een link opgevraagd uit de Service Management Tool.
Patroon	
Toe te passen Standaard	HTTPS
Technische realisatie	URL

4 Kennisbank (Vibes) naar Service Management Tool

Doel	Kennisbank items worden met een link opgevraagd uit de kennisbank
Patroon	
Toe te passen Standaard	HTTPS
Technische realisatie	URL

5 O365 naar Service Management Tool

Doel	Meerdere mailboxen worden uitgelezen door de Service Management Tool (onder andere mails vanuit Snelbalie en Youforce(Robotics)). Foutmeldingen en meldingen van gebruikers worden als melding aangemaakt in de Service Management Tool.
Patroon	Mail
Toe te passen Standaard	
Technische realisatie	

6 Service Management Tool naar O365

Doel	Mail naar interne medewerkers en externen worden vanuit de Service Management Tool verstuurd.
Patroon	Mail
Toe te passen Standaard	
Technische realisatie	Aandachtspunt: Bij een webapplicatie worden mails, uit naam van de gemeente Eindhoven, aan externen verstuurd via de Relay server in de omgeving van de gemeente Eindhoven.

7 Proactis naar Service Management Tool

Doel	Leveranciergegevens beschikbaar stellen vanuit Proactis in de service Management Tool
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

8 Service Management Tool naar Proactis

Doel	Bestellingen verwerken in inkoopordersysteem Proactis
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

9 Microsoft Identity Manager(MIM) naar Service Management Tool

Doel	In- en externe medewerkers en organisatiestructuur worden geladen in de Service Management tool
Patroon	
Toe te passen Standaard	
Technische realisatie	Database view

10 Financiële gegevens van Service Management Tool naar Decade

Doel	Doorgeven van financiële gegevens naar Decade
Patroon	
Toe te passen Standaard	
Technische realisatie	Batchverwerking met behulp van Cognos

11 Service Management Tool naar GME Gebruikers magazijn

Doel	Externe medewerker gegevens van de Service Management Tool naar het GME gebruikersmagazijn
Patroon	
Toe te passen Standaard	
Technische realisatie	Database view

12 GME gebruikers magazijn naar Service Management Tool

Doel	Gegevens van Mobiele telefoons van GME gebruikersmagazijn naar de Service Management Tool
Patroon	
Toe te passen Standaard	
Technische realisatie	Database view

13 Service Management Tool naar Rapportage

Doel	De Service Mangement Tool levert (niet bewerkte) brondata aan het dataplatform. Rapportages worden gemaakt met de gegevens uit het Dataplatform.
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

14 Telefoonsysteem naar Service Management Tool

Doel	Koppeling met telefoonsysteem zodat automatisch de naam van de beller op de telefoon verschijnt
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

15 Kassa system naar Service Management Tool

Doel	Kassagegevens verwerken in de Service management Tool
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

16 Netwerk componenten naar Service Management Tool

Doel	Automatisch uitlezen van netwerkcomponent gegevens.
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

17 Monitoring Tools naar Service Management Tool

Doel	De Service Mangement Tool kan automatisch events loggen uit Monitoring tools
Patroon	
Toe te passen Standaard	
Technische realisatie	Nog niet gerealiseerd

18 Service Management Tool naar BlueDolphin

Doel	CMDB gegevens beschikbaar stellen aan Bluedolphin
Patroon	Filetransfer / Bronsysteem Omgeving Extern en Doelsysteem Omgeving Extern
Toe te passen Standaard	
Technische realisatie	Export vanuit de Service Management Tool wordt handmatig verwerkt in BlueDolphin

Bijlage: Integratiepatronen

Binnen ons huidige applicatielandschap hebben we te maken met applicaties en systemen die nog niet in staat zijn om integraties te maken met API's. Daarom bevat de Integratie-Platform architectuur alle integratie stijlen en integratie patronen die op dit moment en in de toekomst worden toegepast.

Integratiestijlen

We onderscheiden de volgende integratiestijlen:

- Messaging (Berichtenverkeer)
 - o Transport van Datapakketjes (onder andere vanuit API's)
 - o Het bericht bevat informatie over afleveradres van de Datapakketjes
 - o Context is beperkt tot een enkele vraag of gebeurtenis
 - o Overdracht vindt direct plaats
- File transfer (Bestandsoverdracht)
 - o Transport van Bestanden (bulk van datapakketjes)
 - o Vooraf definiëren van afleveradres
 - o Context omvat samenvoeging van feiten
 - o Overdracht op vooraf afgesproken tijden

De context waarbinnen de integratiestijlen opereren is zo anders dat we ook andere terminologie gebruiken bij de verdere uitwerking per integratiestijl.

Integratiepatronen Messaging

Bij het transport van berichten is een primaire taak van het Integratie-Platform het kunnen uitvoeren van Mediatie & Orkestratie binnen het verkeersstromen beheer waarmee messages worden verwerkt, gevalideerd en gerouteerd. Hierbij spreken we over Context leverancier en Context afnemer als benaming voor de afzender en ontvanger van de data.

De integratiepatronen die met messaging worden uitgevoerd zijn:

Request – Reply



de contextafnemer verstuurt een vraag (query) bericht en de contextleverancier stuurt het antwoord (notify) bericht terug. Verkeersstroombeheer zorgt ervoor dat het vraagbericht van de Context afnemer bij de juiste contextleverancier wordt afgeleverd en dat het antwoord van de Context leverancier weer bij de juiste Contextafnemer wordt afgeleverd.

Publish – Subscribe:



De context afnemer abonneert zich op een bepaalde gebeurtenis van de contextleverancier. Op het moment dat zo'n gebeurtenis plaats vindt publiceert (notify) de Contextleverancier een bericht met het feit van deze gebeurtenis. Verkeersstroombeheer zorgt ervoor dat alle geabonneerden het bericht van deze gebeurtenis ontvangt.

Update:

In veel systemen is de update functionaliteit geïntegreerd bij de Contextleverancier. Maar in het in het kader van de principes van Common Ground wordt de update functionaliteit losgekoppeld van de

Contextleverancier, en wordt vanaf de Context beheerder via berichten verkeer aangeboden aan de Contextleverancier.



De Contextbeheerder stuurt een update bericht naar de Contextleverancier. Verkeersstroombeheer zorgt ervoor dat het update bericht van de Contextbeheerder bij de juiste contextleverancier wordt afgeleverd.

Integratiepatronen Filetransfer

Filetransfer wordt al hele lange tijd toegepast om bestanden van het Bronsysteem naar het Doelsysteem te kopiëren..

Het uitgangspunt bij Filetransfer is dat het overbrengingsproces geheel geautomatiseerd verloopt en er geen menselijke handelingen nodig zijn. Dit om de correctheid en de kwaliteit van de bestanden te kunnen garanderen. Daarnaast moet tijdens het overbrengingsproces encryptie worden toegepast. Wanneer bestanden tijdens het overbrengingsproces tussentijds worden opgeslagen mogen deze locaties niet voor gebruikers toegankelijk zijn en moeten de bestanden in de tussenopslag automatisch worden verwijderd.

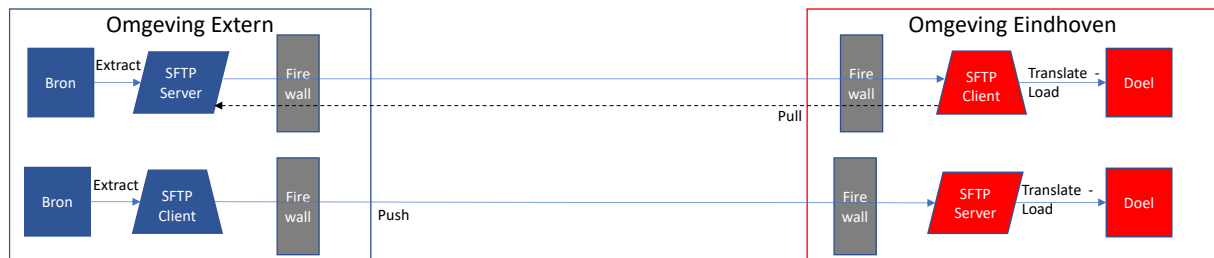
Om het Filetransfer overbrengingsproces geheel te kunnen automatiseren zijn de volgende functionaliteiten noodzakelijk”:

- Proces en/of Workflow scheduler
Om het Filetransfer overbrengingsproces op basis van vooraf afgesproken triggers op te starten en uit te voeren.
- Secure locations
Bestanden mogen op de (tussen) locaties niet door gebruikers te benaderen zijn
- Secure Filetransfer
Het transport moet beveiligd worden uitgevoerd zodat data tijdens het transport niet door onbevoegde kan worden benaderd. Hierbij wordt ook encryptie op de data toegepast.
- Logging
Alle Filetransfers worden geregistreerd in een logbestand, zodat deze herleidbaar is.
- Controle mechanismen
Om zeker te zijn dat er niets in de inhoud van de bestanden is gewijzigd kunnen controlemaatregelen genomen worden zoals hashtotals.

We beschrijven hieronder de integratiepatronen die voor kunnen komen. De terminologie die binnen de schema's worden gebruikt zijn:

- Bron: het zendende systeem van het bestand
- Doel: het ontvangende systeem van het bestand
- Firewall: de beveiligingsmuur van een omgeving waardoor ongewenste bezoekers geen toegang krijgen tot het netwerk
- Omgeving Eindhoven: het systeem staat binnen het beveiligde netwerk van Eindhoven.
- Omgeving Extern: het systeem wordt buitenhet beveiligde netwerk van Eindhoven gehost
- Push: de afzender neemt initiatief om bestand te versturen
- Pull: de ontvanger neemt initiatief om bestand te ontvangen
- Extract: het Bronsysteem genereert automatisch het bestand en plaats deze op een secure location
- Load: Het bestand wordt automatisch geladen (verwerkt) vanaf een secure location in het doelsysteem
- Translate: mogelijke tussenstap wanneer de datadefinitie van het gegenereerde bestand niet overeenkomt met de datadefinitie in het doelsysteem.

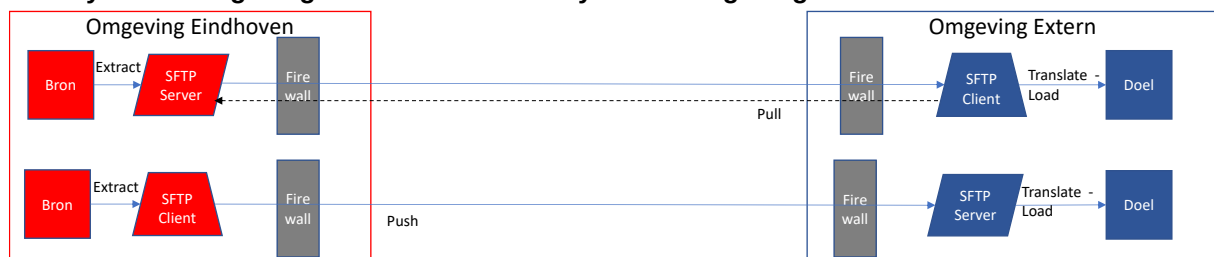
Bronstelsysteem Omgeving Extern en Doelsysteem Omgeving Eindhoven



Pull: vanuit de Omgeving Eindhoven wordt op vooraf gedefinieerde tijdstippen gekeken of er op een vooraf afgesproken locatie op de SFTP server van Omgeving Extern een bestand klaar staat. Op het moment dat een bestand klaar staat wordt deze via een beveiligde SFTP verbinding getransporteerd naar de Omgeving Eindhoven “getrokken”

Push: vanuit de Omgeving Extern wordt op vooraf afgesproken tijdstippen het bestand via een beveiligde SFTP verbinding getransporteerd naar de Omgeving Eindhoven “geduwd”.

Bronstelsysteem Omgeving Eindhoven en Doelsysteem Omgeving Extern



Pull: vanuit de Omgeving Extern wordt op vooraf gedefinieerde tijdstippen gekeken of er op een vooraf afgesproken locatie op de SFTP server van Omgeving Eindhoven een bestand klaar staat. Op het moment dat een bestand klaar staat wordt deze via een beveiligde SFTP verbinding getransporteerd naar de Omgeving Extern “getrokken”

Push: vanuit de Omgeving Eindhoven wordt op vooraf afgesproken tijdstippen het bestand via een beveiligde SFTP verbinding getransporteerd naar de Omgeving Extern “geduwd”.

Bronstelsysteem Omgeving Eindhoven en Doelsysteem Omgeving Eindhoven

In deze situatie kunnen we ook te maken hebben met Firewalls omdat bepaalde onderdelen van het netwerk extra afgeschermd zijn. De Firewall controleert of het transport de juiste autorisatie heeft om door te laten gaan.

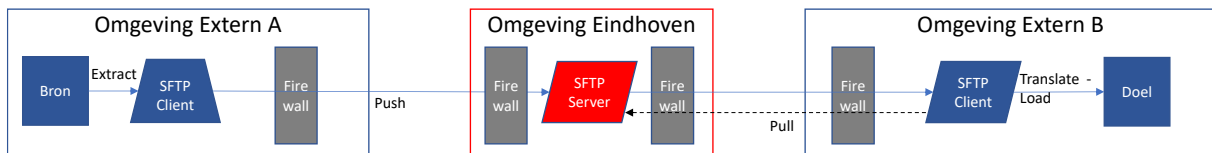


Pull: vanuit netwerksegment A van de Omgeving Extern wordt op vooraf gedefinieerde tijdstippen gekeken of er op een vooraf afgesproken locatie op de SFTP server van netwerksegment B Omgeving Eindhoven een bestand klaar staat. Op het moment dat een bestand klaar staat wordt deze via een beveiligde SFTP verbinding getransporteerd naar de netwerksegment B Omgeving Eindhoven “getrokken”

Push: vanuit netwerksegment A Omgeving Eindhoven wordt op vooraf afgesproken tijdstippen het bestand via een beveiligde SFTP verbinding getransporteerd naar de Netwerksegment B Omgeving Eindhoven “geduwd”.

Bronstelsysteem Omgeving Extern en Doelsysteem Omgeving Extern

In deze situatie wordt data van Eindhoven getransporteerd tussen systemen die allebei in een Externe omgeving worden gehost. Omdat Eindhoven verantwoordelijk is en blijft voor de data, moet in deze situatie het transport via de Omgeving van Eindhoven worden ingericht.



Zowel het Push mechanisme als het Pull mechanisme noodzakelijk voor het transport van Omgeving Extern A naar Omgeving Extern B. Op deze manier is de Omgeving Eindhoven alleen doorgeefluik, maar kan het transport wel loggen.

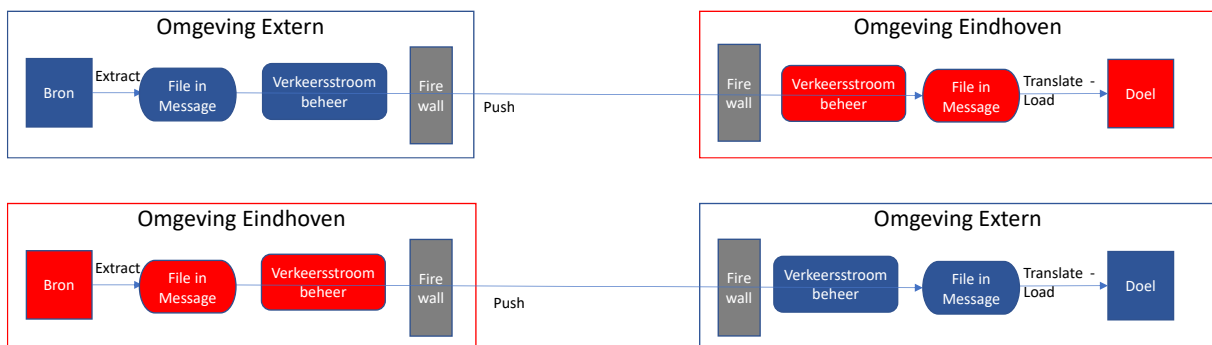
Push: vanuit Omgeving Extern A wordt op vooraf afgesproken tijdstippen het bestand via een beveiligde SFTP verbinding getransporteerd naar de Omgeving Eindhoven “geduwd”.

Pull: vanuit Omgeving Extern B wordt op vooraf gedefinieerde tijdstippen gekeken of er op een vooraf afgesproken locatie op de SFTP server van Omgeving Eindhoven een bestand klaar staat. Op het moment dat een er een bestand klaar staat wordt deze via een beveiligde SFTP verbinding getransporteerd naar de Omgeving Extern B “getrokken”

Bestand wordt ingepakt in een message

In deze situatie wordt een bestand ingepakt zodat het beveiligd transport met behulp van Message tooling kan worden verzorgd.

Het Bronsysteem genereert automatisch het bestand (Extract) en verpakt deze in een message en pushed deze naar de Message tooling. De Message tooling verzorgt het transport naar de Omgeving van het Doelsysteem. De Omgeving van het Doelsysteem haalt het bestand uit de message en zorgt voor de Translate en Load procedure naar het Doelsysteem. In de onderstaande figuren is deze situatie weergegeven voor Bron Omgeving Extern en Bron omgeving Eindhoven



Wanneer zowel Bron als Doel Externe omgevingen zijn ziet de situatie er als volgt uit.



Door het inpakken van een bestand in een message kan het transport direct tussen twee externe partijen via de Omgeving Eindhoven worden gerouteerd en kan het transport door de Omgeving Eindhoven worden gelogd.