

Marktconsultatie Tool verkeersstromen en segmentatie





Centraal Orgaan opvang asielzoekers

Centraal Orgaan opvang Asielzoekers

Wie in Nederland asiel aanvraagt, heeft recht op opvang. COA biedt opvang: veilige huisvesting, noodzakelijke middelen en begeleiding als voorbereiding op een toekomst in Nederland of het land van herkomst.

Het COA is een zelfstandig bestuursorgaan dat opereert onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. Het COA organiseert de eerste opvang van sterk wisselende aantallen asielzoekers in Nederland. Tot het moment dat besloten is over de asielaanvraag worden asielzoekers gehuisvest in één van de azc's van het COA.

In de azc's worden asielzoekers een sober doch humaan pakket materiële voorzieningen geboden. Het COA streeft ernaar om de asielzoekers tijdens hun verblijf in het centrum zo zelfstandig mogelijk te laten functioneren en hen zo goed mogelijk voor te bereiden op een eventueel langdurig verblijf in de Nederlandse samenleving. Het COA hecht grote waarde aan samenwerking met partners die bij het asielbeleid betrokken zijn. Samen met deze partners probeert het COA de komst van asielzoekers voor de overheid en samenleving hanteerbaar te houden.

Aanleiding functionele aanvraag

- Het COA wil tijdig kunnen reageren op securitybedreigingen, sneller afwijkingen kunnen constateren om te voorkomen dat kwaadwillenden toegang krijgen tot de COA-infrastructuur. Verbeterde beveiliging tegen inbreuken en dataverlies.
- Het COA wil operationele efficiëntie verhogen door het creëren van meer inzicht in verkeersstromen, meer inzicht betekent ook operationeel beter kunnen bijsturen
- Het COA wil meer inzicht in het netwerk, wat er gebeurt binnen het netwerk en welke afhankelijkheden er zijn. Dit om incidenten sneller op te kunnen lossen en het doorvoeren van wijzigingen sneller uit te kunnen voeren.
- Het COA wil betere controle van netwerk/dataverkeer
- Het COA wil inzicht in:
 - Gebruikte protocollen (is verkeer encrypted of niet)
 - Kenmerken van end-points (cmdb)
 - Beleidsregels/PEP-functies
 - Integraties van systemen
 - verkeersstromen tussen systemen (clients, servers, internet)
- Het COA wil eenvoudiger en met beperkte verstoringen het netwerk kunnen segmenteren

Doel en uitgangspunten

Doel: Het uitzoeken van een technologie/omgevingsagnostische tool die het COA helpt met:

- Het segmenteren/microsegmenteren van on-prem- en cloud datacenter omgevingen;
- Inzicht krijgen in verkeersstromen van applicaties, tussen systemen;
- Kunnen vaststellen of encryptie plaatsvindt op verkeersstromen;
- Microsegmentatie aanbrengen op de COA infrastructuur;
- Afwijkingen en bedreigingen ten aanzien van informatiestromen inzichtelijk maken en automatisch oplossen.

Uitgangspunten:

Benadrukt wordt dat deze marktconsultatie geen onderdeel uitmaakt van de aanbesteding en er geen rechten aan kunnen worden ontleend. Verkregen inzichten uit de marktconsultatie gebruikt de het COA eventueel in de voorbereiding van een inkooptraject. Het COA behoudt zich het recht voor om deze inzichten niet of niet volledig te gebruiken. Het COA probeert zo transparant mogelijk te werk te gaan, door een verslag van de marktconsultatie bij de aanbestedingsstukken te voegen.

Demo

Het COA ziet graag het volgende 'live' gedemonstreerd:

1. Demonstratie van de gebruiksvriendelijkheid van de interface, inclusief navigatie, rapportagefunctionaliteiten en het instellen van waarschuwingen. Een algemene impressie van de verkeersstromentool. Laat zien hoe de tool gegevens visueel presenteert, zoals kaarten, grafieken en dashboards, om gebruikers een intuïtieve en begrijpelijke weergave te bieden, gebruikersgroepen login, waar zijn de functionaliteiten te vinden?
2. (Near)Realtime verkeersstromen monitoring en hieraan gerelateerde systemen zoals (client-server-agents etc).
3. Laat zien hoe de tool analyses uitvoert op basis van gegevens om verkeerspatronen en -stromen te herkennen en mogelijke congestiepunten en segmentatie te voorspellen.
4. Indien mogelijk 1 of meerdere usecases laten zien (zie slide 8 en verder)

Door deze aspecten uitgebreid te demonstreren, kan de leverancier COA-gebruikers een volledig begrip bieden van de mogelijkheden en voordelen van de verkeersstromentool inclusief segmentatie en policy enformant.

Demo presentatie

Het COA wenst een demo op de mate waarin o.a. de portal als gebruiksvriendelijk en intuïtief wordt ervaren:

1. Een helder en aantrekkelijk ontwerp dat de gebruiker gemakkelijk door de functies van de tool leidt
2. Vlotte en intuïtieve navigatie die gebruikers gemakkelijk door de tool leidt zonder verwarring
3. Begrijpelijke visuele hulpmiddelen die de gebruiker helpen snel functies te herkennen en te begrijpen
4. Flexibiliteit in configuratie om de tool aan te passen aan verschillende gebruikersbehoeften
5. Gemakkelijke toegang tot hulpbronnen die gebruikers ondersteunen bij het begrijpen van de tool en het oplossen van eventuele problemen.
6. Snelle reactietijden die bijdragen aan een vloeiende gebruikerservaring
7. Effectieve onboarding en training om de gebruikersacceptatie te versnellen en de tool efficiënt te kunnen gebruiken

Door deze criteria samen met het MoSCoW model te evalueren, kan COA een goed beeld krijgen van hoe de verkeersstromentool wordt ervaren door gebruikers in termen van gebruiksvriendelijkheid en intuïtiviteit.



Use-cases

Ten behoeve van de marktconsultatie voor een mogelijke tool voor inzicht in verkeerstromen, classificatie, segmentatie en beleidstoepassing binnen het COA, zijn een aantal use-cases uitgewerkt. Vanuit het team van architecten zijn de use-cases benoemd die de meeste waarde voor de COA-organisatie toevoegen.

1. Verkeersstromen visualisatie
2. Classificatie (tagging/labeling) van verkeerstromen op hoofdlijnen en segmentatie van verkeerstromen
3. Integratie in een bestaand netwerk met systemen
4. Rapportage verkeersstromentool
5. Simulatieomgeving

De uitwerking van de use-cases willen wij graag terugzien in de demo.

Uitgangspunten COA-architectuur

- Het COA hanteert “werken met architectuur” als uitgangspunt.
- Werken met architectuur is een werkwijze die bijdraagt aan herkenbare en herbruikbare afspraken, standaarden en oplossingen bij de inrichting van de informatievoorziening in het algemeen en aangaande de tool, de technische middelen in het bijzonder.
- Hierbij worden er referentiearchitecturen gebruikt zoals NORA, RORA & MIRA, normenkaders zoals de BIO en voorschriften zoals VIR en VIR-BI, maar ook relevante wet- en regelgeving, zoals de wet COA.
- Daarbuiten zijn er uitwerkingen vanuit het Ministerie van Justitie en Veiligheid, die in voorkomend geval dwingend zijn of waar er vanuit de COA-organisatie commitment voor uitgesproken is.
- ICT-architectuur vanuit het COA opereert vanuit een centrale repository met architectuur- en solution bouwblokken.
- Het COA gebruikt de applicatie Blue Dolphin voor de vastlegging van architectuurartefacten en processen, volgens de Archimateprincipes.
- Het is dan ook zeker noodzakelijk, dat de beoogde tool hier een aanvulling op is, om zodoende bijvoorbeeld ook het applicatielandschap en de verschillende verkeersstromen inzichtelijk te maken en geautomatiseerd up to date te houden.
- Bij voorkeur is de beoogde tool in staat, dan wel de bijgeleverde informatie, om objecten, elementen en relaties van de tool met de rest van het ICT-landschap weer te geven.



Use-case 1: Verkeersstromen visualisatie

Scenario: Het IT-beheerteam wil de netwerkprestaties en verkeersstromen monitoren en snel reageren op incidenten zoals netwerkcongestie, uitval of abnormale verkeerspatronen.

Demo Focus:

1. Toon een visuele weergave van het netwerkverkeer, inclusief source, destination ip/port/protocol en de tijdsduur van verbindingen waarbij ook rapportage mogelijkheden zijn.
2. Laat zien hoe de tool ongebruikelijke verkeerspatronen detecteert en mogelijke probleemgebieden identificeert. Dit mag ook met behulp van API-koppelingen.
3. Simuleer een optimalisatiescenario waarbij de tool suggesties doet om de netwerkprestaties te verbeteren, zoals het herleiden van verkeersstromen of het optimaliseren van verbindingen.

Use-case 2: Verkeersstromen Classificatie & Segmentatie

Scenario: Het IT – beheerteam wil anticiperen op verkeerstromen inzichtelijk krijgen en duidelijk kunnen classificeren om een goed netwerksegmentatie en zoneringen toe te kunnen passen in de toekomst.

Demo Focus:

1. Presenteer gegevens over netwerkanalyse en classificatie.
2. Toon hoe de tool analyses uitvoert om huidige en toekomstige verkeerstromen te classificeren, [http/https/ftp/sftp](#), encrypted en non encrypted verkeer.
3. Toon aan dat usecases getoets en gevalideerd kunnen worden in een simulatieomgeving en simuleer verschillende scenario's hoe de tool de impact op beheer, inzicht, en reponse heeft.

Deze use-case richt zich op het bieden van diepgaand inzicht in de verkeerstromen binnen het COA-netwerk, waardoor de organisatie proactief kan handelen om de prestaties te verbeteren en te optimaliseren.

Use-case 3: Integratie verkeersstromentool

Scenario: Het COA streeft naar een geautomatiseerd netwerkbeheer met naadloze integratie van de verkeersstromentool met bestaande systemen en netwerkapparatuur.

Demo Focus:

1. Toon de mogelijkheid van de tool om te integreren met verschillende netwerkapparatuur, zoals routers, switches, firewalls, systemen, IAM-tooling, SIEM, servers en agents in een multi-vendor netwerk.
2. Laat zien hoe de tool netwerkconfiguraties en –policy enforcement kan toepassen, kan beheren en automatiseren.
3. Simuleer een scenario waarbij de tool automatisch reageert op veranderende netwerkomstandigheden, bijvoorbeeld door het segmenteren/isoleren op macro- of microniveau van systemen waarbij alleen north-south verkeer mogelijk is, (policy enforcement) en toegang tot kritieke systemen en gevoelige data automatisch blokkeert bij ongeautoriseerde toegang.

Deze use-cases bieden een diepgaande demonstratie van de mogelijkheden van een verkeersstroomtool(s) voor IT-netwerk en systeem infrastructuur, met de nadruk op monitoring, classificatie en integratie met bestaande netwerkcomponenten.

Use-case 4: Rapportage verkeersstromentool (1/2)

Extra use case met rapportagemogelijkheden:

Verkeersstromen en visualisatie

Rapportagemogelijkheden met gedetailleerde visualisaties van de verkeersstromen binnen een netwerk zoals dat van het COA. Dit helpt bij het identificeren van toegestane en verboden verkeersstromen tussen applicaties en workloads, waardoor het COA het netwerksegmentatiebeleid verder kan verfijnen.

Beveiligingsbeleid en regelconformiteit

Rapportagemogelijkheden over het huidige beveiligingsbeleid en de naleving ervan. Deze rapporten kunnen het COA helpen bij het beoordelen van de effectiviteit van het geïmplementeerde beleid en bij het identificeren van gebieden die verbetering behoeven.

Risicoanalyse en kwetsbaarheidsbeheer

Rapportagemogelijkheden over potentiële risico's en kwetsbaarheden binnen het netwerk zoals dat van het COA. Dit omvat het identificeren van workloads die mogelijk blootgesteld zijn aan bekende kwetsbaarheden, waardoor prioriteit kan worden gegeven aan patchbeheer en andere beveiligingsmaatregelen.

Use-case 4: Rapportage verkeersstromentool (2/2)

Compliance rapportage

Rapportagemogelijkheden om te laten zien dat wordt voldaan aan specifieke regelgeving en normen (zoals BIO, AVG enz.)

Incidenten- en bedreigingsdetectie

Rapportagemogelijkheden over gedetecteerde beveiligingsincidenten en potentiële bedreigingen. Dit om inzicht te bieden in aanvalspatronen, betrokken workloads en de effectiviteit van de respons-strategieën.

Optimalisatie en efficiëntie

Rapportagemogelijkheden om inzicht te bieden in de efficiëntie van het netwerk zoals dat van het COA en in de beveiligingsarchitectuur, inclusief aanbevelingen voor optimalisatie.

Use-case 5: Simulatieomgeving

Wat zijn de mogelijkheden van een simulatie-omgeving, alvorens zaken in productie te implementeren. Te denken valt bijvoorbeeld aan:

Evaluatie van beleidsvoorstellen/PEP

Door het voorgestelde beleid en eventuele toepassing van PEP-functies eerst door te voeren in een simulatieomgeving, kan het COA inzicht krijgen hoe het voorgestelde beleid/PEP het netwerkverkeer/ workloads zou kunnen beïnvloeden zonder dat het verkeer/workloads daadwerkelijk worden geblokkeerd of gewijzigd.

Identificatie van risico's en afhankelijkheden

Het kunnen identificeren van onbedoelde gevolgen van een nieuw beleid/PEP-functies, zoals het blokkeren van legitiem verkeer.

Afstemming van beleidsvoorstellen/PEP

Op basis van de inzichten verkregen uit de simulatie kan het COA haar beleidsregels verfijnen, voordat deze worden toegepast. Dit om zo een optimale balans tussen beveiliging en functionaliteit te waarborgen.



PLANNING

Publiceren marktconsultatie

Dinsdag 5 maart 2024

Indienen vragen over consultatie

Donderdag 14 maart 2024 17:00 uur

Vragen van marktpartijen beantwoorden

Dinsdag 19 maart 2024

Marktconsultatiegesprekken

Donderdag 21 maart 2024

- 13:00 - 14:00
- 15:30 - 16:30

(gelieve rekening te houden met uw agenda)

Woensdag 27 maart 2024

- 10:00 - 11:00
- 11:30 - 12:30