THOMAS MORE

SAP BTP Impact and Network Security in SAP Landscapes

Realisatiedocument

Mats Couwenberg
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

2024 - 2025

Inhoudsopgave

Afkortingenlijst

Afkorting	Betekenis
BTP	Business Technology Platform
ERP	**Enterprise Resource Planning**
CRM	**Customer Relationship Management**
HRM	**Human Resource Management**
AI	**Artificial Intelligence**
SSO	**Single Sign-On**
IPS	**Intrusion Prevention System**
VPC	**Virtual Private Cloud**
RDP	**Remote Desktop Protocol**
VIP	**Virtual IP**
UDR	**User Defined Route**
CVE	**Common Vulnerabilites and Exposures**
CVSS	**Common Vulnerability Scoring System**
BSP	**Business Server Pages**
FQDN	**Fully Qualified Domain Name**

1. Inleiding

Tijdens mijn stage bij delaware heb ik gewerkt aan een gevarieerd project waarin zowel theorie als praktijk samenkwamen. Het doel van mijn stage was om nieuwe kennis op te doen én die kennis toe te passen binnen een echte werkomgeving. In dit document beschrijf ik wat ik tijdens mijn stage heb gedaan, wat ik heb geleerd en welke resultaten ik heb behaald.

Het eerste deel van mijn stage draaide vooral om het leren en onderzoeken van SAP BTP (Business Technology Platform). Dit is een relatief nieuw platform van SAP dat op verschillende manieren ingezet kan worden om bedrijfsprocessen te verbeteren, te automatiseren of zelfs helemaal opnieuw op te zetten. Ik heb onderzocht wat SAP BTP precies is, wat je ermee kunt doen en hoe bedrijven het kunnen gebruiken. De informatie die ik heb verzameld, heb ik verwerkt in documentatie voor het SAP-team waarin ik mijn stage liep.

In het tweede deel ben ik praktisch aan de slag gegaan, in samenwerking met het netwerkteam. We werkten aan een concreet project waarbij we “Virtual Patching” testten in productieomgevingen. Tijdens deze fase hielp ik mee bij het opzetten en configureren van de Cloud infrastructuur en het netwerk in de cloud. Denk bijvoorbeeld aan het instellen van user defined routes, het testen van configuraties en het oplossen van technische problemen die tijdens het proces naar voren kwamen. Deze samenwerking gaf me niet alleen meer technische ervaring, maar liet me ook zien hoe belangrijk goede communicatie en teamwork zijn in een professionele werkomgeving.

In dit document vertel ik in detail over alle onderdelen van mijn stage. Eerst leg ik uit wat SAP en SAP BTP zijn en wat ik daarover heb geleerd. Daarna bespreek ik het praktische deel van het project en sluit ik af met een terugblik op mijn leerproces en persoonlijke ontwikkeling. Zo geeft dit realisatiedocument een duidelijk beeld van mijn stageperiode bij delaware.

2. SAP BC

Tijdens mijn stage maakte ik deel uit van het SAP BC-team, wat staat voor SAP BASIS Consultancy. Dit team heeft een breed takenpakket en houdt zich bezig met het opzetten, onderhouden en beheren van SAP-systemen voor verschillende klanten en projecten. Dit varieert van het installeren van nieuwe systemen tot het uitvoeren van updates, patches en het optimaliseren van de prestaties. Naast het reguliere beheer is het team ook verantwoordelijk voor het afbouwen en ontmantelen van SAP-omgevingen die niet langer in gebruik zijn.

Een steeds belangrijker onderdeel van hun werk is het omgaan met SAP BTP (Business Technology Platform). Het team speelt een actieve rol bij het implementeren, beheren en uitbreiden van oplossingen die draaien op dit platform. SAP BTP biedt veel nieuwe mogelijkheden op het gebied van cloudoplossingen, integraties, data en applicatieontwikkeling. Het team helpt klanten om deze technologieën op een efficiënte en veilige manier toe te passen.

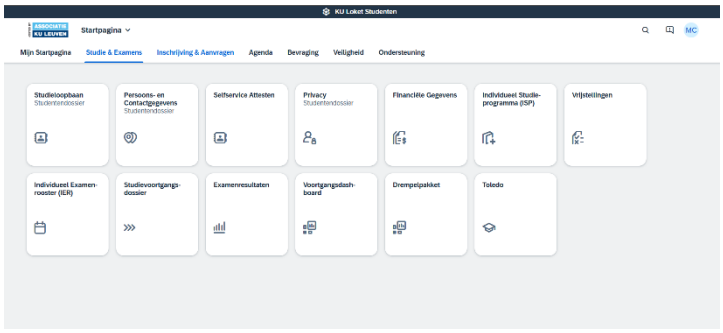
Als stagiair binnen dit team kreeg ik de kans om met veel nieuwe technologieën aan de slag te gaan en tegelijkertijd delaware als organisatie beter te leren kennen. Hierdoor heb ik niet alleen een goed beeld gekregen van het werk van een consultant bij delaware, maar ook waardevolle praktijkervaring opgedaan in een technisch uitdagende werkomgeving.

3. SAP

SAP is een wereldwijd bekend softwarebedrijf dat gespecialiseerd is in het ontwikkelen van bedrijfsoplossingen. De belangrijkste oplossing die SAP biedt is een Enterprise Resource Planning-systeem (ERP-systeem). Dit is software die bedrijven helpt om hun dagelijkse bedrijfsprocessen te beheren, te automatiseren en efficiënter te maken.

Een ERP-systeem van SAP integreert een breed scala aan bedrijfsfuncties, waaronder financiële administratie, logistieke planning, customer relationship management (CRM), supply chain management en human resource management (HRM). Door al deze functies op één platform samen te brengen, kunnen afdelingen binnen een organisatie beter samenwerken en werken ze met dezelfde, actuele data.

SAP-systemen worden op veel verschillende plekken gebruikt. De kans is groot dat je zelf al eens met een SAP-systeem hebt gewerkt zonder het te beseffen. Voor studenten en docenten is bijvoorbeeld het KULoket een bekend voorbeeld van een systeem dat draait op SAP-technologie.



Uiteraard wordt SAP niet alleen gebruikt in het onderwijs. Wereldwijd maken miljoenen gebruikers in allerlei sectoren gebruik van SAP-oplossingen, denk aan productie, retail, energie, gezondheidszorg, overheid en nog veel meer. Zowel grote multinationals als middelgrote bedrijven gebruiken SAP om hun processen beter te organiseren en meer controle te krijgen over hun organisatie. SAP biedt oplossingen die zowel on-premise (op eigen servers) als in de cloud draaien, waardoor bedrijven flexibiliteit hebben in hun implementatie en schaalbaarheid.

SAP biedt verschillende versies van zijn ERP-systeem, waarvan SAP S/4HANA de meest geavanceerde en moderne variant is. S/4HANA is gebouwd op het krachtige SAP HANA-platform, een zogeheten in-memory database, wat zorgt voor extreem snelle gegevensverwerking en realtime analyses. Dit helpt bedrijven om sneller en beter onderbouwde beslissingen te nemen, wat in de huidige tijd een groot voordeel is.

4. SAP BTP

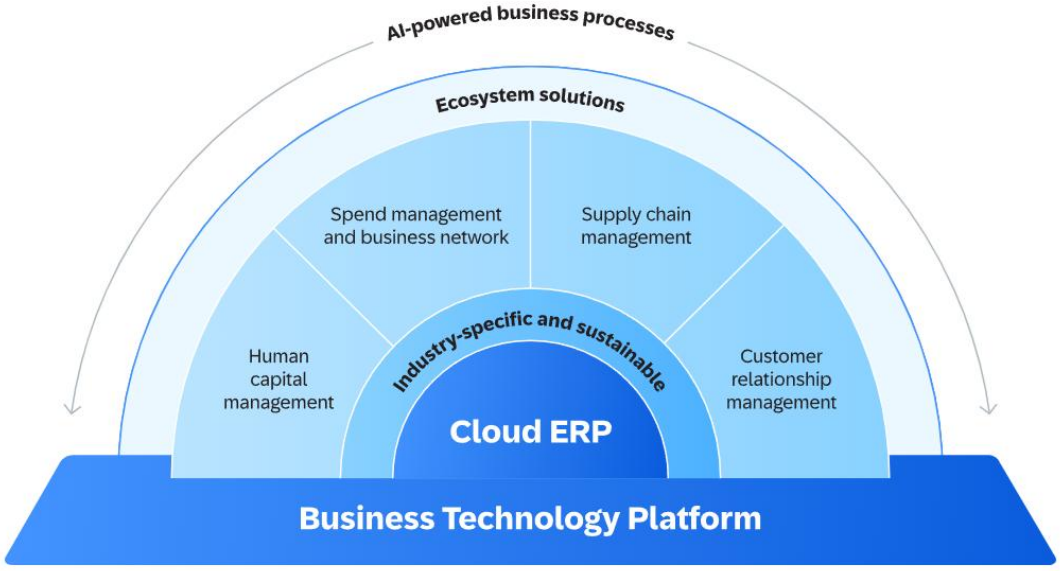
Het SAP Business Technology Platform, kortweg SAP BTP, is een veelzijdig platform dat bedrijven helpt om te innoveren, hun systemen met elkaar te verbinden en hun manier van werken te moderniseren in het digitale tijdperk. Met SAP BTP kunnen organisaties hun bestaande SAP-systemen uitbreiden, gegevens slim gebruiken en processen efficiënter maken.

Een van de belangrijkste voordelen van SAP BTP is dat het bedrijven de mogelijkheid biedt om extra functionaliteiten toe te voegen aan SAP S/4HANA, het kern-ERP-systeem van SAP, zonder dat de kern van het systeem wordt aangepast. Dat is belangrijk, want het zorgt ervoor dat het hoofd-systeem overzichtelijk en stabiel blijft, wat toekomstige updates en onderhoud makkelijker maakt.

Daarnaast maakt SAP BTP het mogelijk om verschillende systemen met elkaar te koppelen, zowel SAP- als niet-SAP-systemen. Denk bijvoorbeeld aan een SAP-systeem dat automatisch gegevens kan uitwisselen met een webshop of een logistiek systeem van een externe partij. Op die manier ontstaat een goed samenwerkend geheel, waarin alle onderdelen van een organisatie beter met elkaar communiceren.

SAP BTP helpt ook bij het automatiseren van bedrijfsprocessen. Veel taken die normaal handmatig worden uitgevoerd, kunnen met behulp van BTP automatisch verlopen. Denk aan goedkeuringsprocessen, meldingen of rapportages. Dit bespaart tijd, voorkomt fouten en maakt het werk efficiënter.

Daarnaast maakt SAP BTP gebruik van Artificial Intelligence (AI) en data-analyse om bedrijven te helpen slimme beslissingen te nemen. Door gegevens op een slimme manier te verzamelen, te analyseren en te presenteren, krijgen bedrijven beter inzicht in hun processen en kunnen ze sneller reageren op veranderingen.



4.1. De basis van SAP BTP

SAP Business Technology Platform (SAP BTP) is opgebouwd rond vijf fundamentele pijlers die organisaties helpen om innovatie te versnellen, processen te optimaliseren en beter gebruik te maken van data. Deze pijlers vormen samen de basis voor het ontwikkelen, integreren, automatiseren en uitbreiden van bedrijfsapplicaties op een flexibele en schaalbare manier.

4.1.1. Application Development

Dit onderdeel van SAP BTP richt zich op het ondersteunen van developers bij het efficiënt creëren, implementeren en beheren van applicaties. Developers kunnen gebruikmaken van diverse ontwikkelingstools en services die verschillende programmeertalen ondersteunen. Een van deze tools is SAP Build Code, ontworpen voor het bouwen en uitbreiden van business applications op het SAP Business Technology Platform. SAP BTP ondersteunt ook low-code development, waarmee business-gebruikers applicaties kunnen bouwen zonder diepgaande programmeerkennis.

4.1.2. Automation

Automatisering binnen SAP BTP verhoogt de efficiëntie door handmatig werk in bedrijfsprocessen te verminderen en repetitieve taken te automatiseren. SAP BTP biedt daarnaast mogelijkheden voor workflow-automatisering. Door routinetaken te automatiseren, kunnen bedrijven middelen vrijmaken en zich richten op belangrijkere activiteiten.

4.1.3. Integration

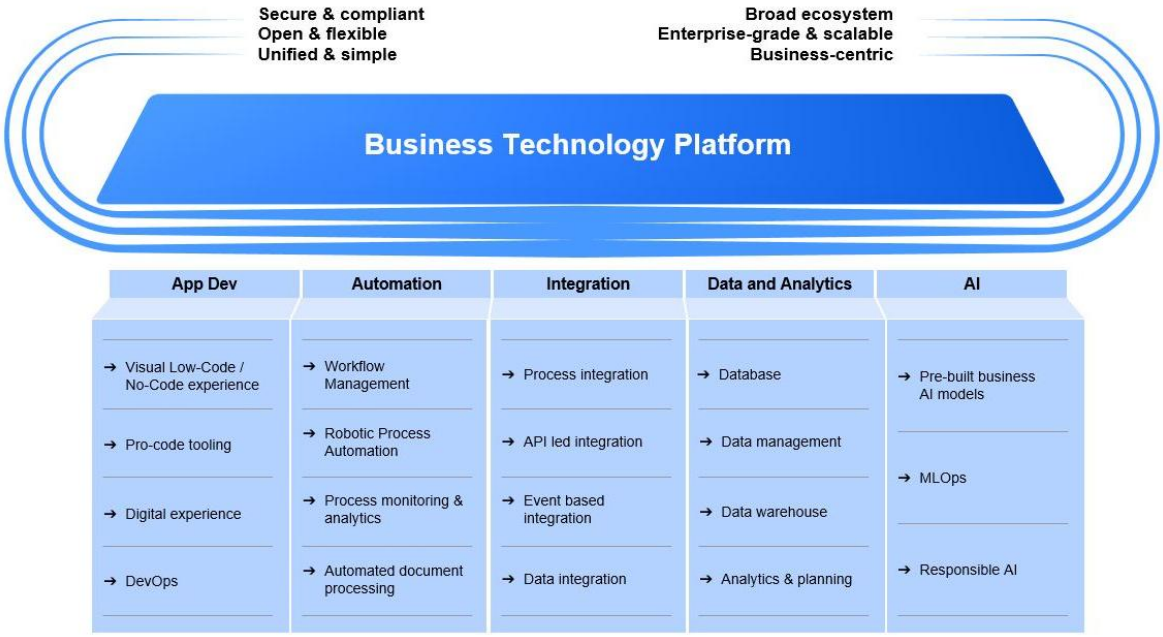
SAP BTP maakt naadloze communicatie en data uitwisseling mogelijk tussen verschillende systemen, applicaties en databronnen. Het ondersteunt de connectiviteit tussen on-premise en cloudomgevingen, wat zorgt voor een soepele integratie. Organisaties kunnen bestaande API’s gebruiken via de SAP Business Accelerator Hub of eigen API’s bouwen met de SAP Integration Suite, afhankelijk van hun specifieke behoeften.

4.1.4. Data & Analytics

SAP BTP biedt krachtige data- en analysetools waarmee organisaties waardevolle inzichten kunnen verkrijgen en data-driven beslissingen kunnen nemen om zakelijk succes te stimuleren. Het platform biedt uitgebreide services voor datawarehousing, modellering en geavanceerde analyses, zodat bedrijven hun data efficiënt kunnen beheren en analyseren. Daarnaast bevat SAP BTP functies voor datavisualisatie en machine learning, waarmee organisaties trends en patronen in hun data kunnen ontdekken.

4.1.5. Artifical Intelligence (AI)

SAP BTP biedt een breed scala aan AI-technologieën en -diensten, zoals SAP AI Business Services en de Generative AI Hub. Deze maken het mogelijk voor organisaties om de kracht van artificial intelligence te benutten voor innovatie, efficiëntieverbetering en extra klantwaarde. Door gebruik te maken van deze AI-mogelijkheden kunnen organisaties concurrerend blijven en succesvol opereren in de digitale economie.



4.2. Voorbeeld van SAP BTP Architectuur

Zoals eerder vermeld, biedt SAP BTP uitgebreide mogelijkheden voor het ontwikkelen, uitbreiden en integreren van zowel SAP- als non-SAP-systemen. Organisaties kunnen SAP BTP inzetten om bestaande systemen, zoals ERP-oplossingen functioneel uit te breiden, bedrijfsprocessen te automatiseren of volledig nieuwe applicaties te ontwikkelen die optimaal inspelen op hun specifieke behoeften.

Een typisch scenario waarin SAP BTP wordt toegepast, is het bouwen en hosten van een cloudapplicatie die geïntegreerd is met een on-premise systeem, zoals SAP S/4HANA. Dit wordt mogelijk gemaakt via de SAP Cloud Connector, die fungeert als een veilige brug tussen de cloudomgeving van SAP BTP en de interne IT-infrastructuur van een organisatie. Hierdoor kunnen bedrijfsapplicaties in de cloud eenvoudig communiceren met systemen die binnen het bedrijfsnetwerk draaien, zonder dat gevoelige data of systemen direct aan het internet blootgesteld worden.

Naast integratie met on-premise systemen, ondersteunt SAP BTP ook de koppeling met andere SAP Cloud-oplossingen, zoals SAP SuccessFactors (Human Resources Management), SAP Ariba (Supply Chain Management) of SAP Customer Experience (Customer Relationship Management). Zo kunnen organisaties een verbonden applicatielandschap creëren waarin data en processen soepel over verschillende platformen heen samenwerken.

Een ander belangrijk aspect van SAP BTP is de ondersteuning van externe identity providers, zoals Microsoft Entra ID. Dit betekent dat gebruikers niet voor elke SAP-applicatie aparte inloggegevens nodig hebben, maar gewoon kunnen inloggen met hun bestaande bedrijfsaccount. Microsoft Entra ID beheert gebruikersidentiteiten en toegangsrechten binnen een organisatie, en door de integratie met SAP BTP kunnen organisaties profiteren van Single Sign-On (SSO), gecentraliseerde toegangscontrole en verbeterde beveiliging. Dit zorgt niet alleen voor een naadloze gebruikerservaring, maar voldoet ook aan moderne beveiligings- en compliance-eisen.

Onderstaande architectuurvisualisatie toont een voorbeeld van een SAP BTP-opstelling waarin een applicatie wordt ontwikkeld, gehost op het platform, verbonden met een on-premise ERP-systeem via de Cloud Connector, en geïntegreerd met externe identiteitsbeheeroplossingen voor veilige gebruikersauthenticatie.

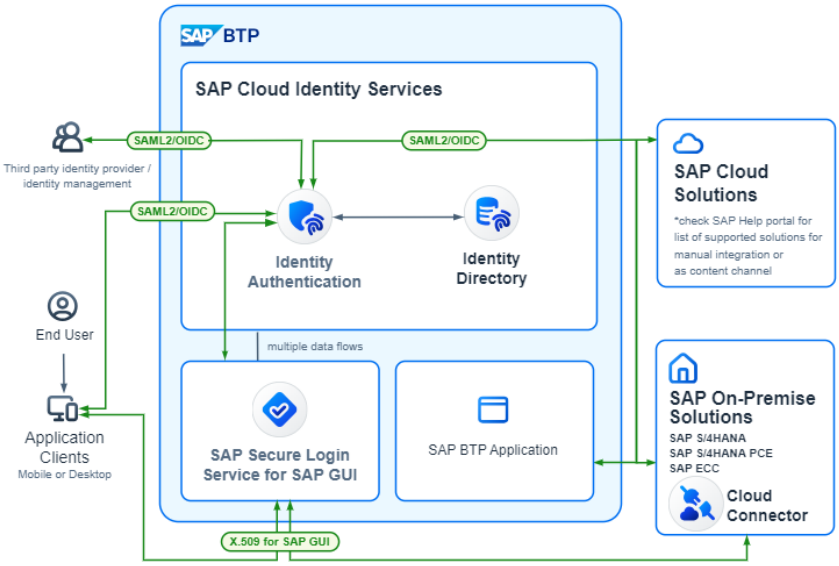


Diagram Level: L1

The main (nonhuman) interacting actors in the model are identity providers, service providers, and the IAM services supported by SAP BTP. As shown in the figure Identity providers are systems that assert user information to service provider systems, vouching for the identity of the users who require access to their services.

Legend

Authentication · SAP BTP Service · Access · Application · Mutual Trust

5. SAP BTP Documentatie

Mijn eerste taak binnen deze stage bestond uit het opstellen van documentatie over SAP Business Technology Platform (SAP BTP). Aangezien het verkennen en vastleggen van SAP BTP centraal staat in mijn stageopdracht, vormde het volgen van meerdere SAP Learning-cursussen en het structureren van de opgedane kennis hierin een logische en waardevolle eerste stap.

Deze documentatie is bedoeld als een beknopte maar volledige samenvatting van de belangrijkste concepten, componenten en toepassingen van SAP BTP. Bij het opstellen heb ik bewust gekozen voor een heldere en overzichtelijke structuur, waarbij overbodige uitleg is vermeden. Op die manier is alle relevante informatie verzameld op één centrale plek, met de nadruk op toepasbaarheid, duidelijkheid en volledigheid.

Het eerste deel van de documentatie biedt een algemene introductie tot SAP BTP en belicht de belangrijkste kernaspecten. In de daaropvolgende hoofdstukken worden de voornaamste onderdelen van het platform verder uitgediept. Elk hoofdstuk is opgebouwd op basis van inzichten en kennis uit de gevolgde SAP Learning-trajecten.

Naast de vijf belangrijke pijlers van SAP BTP is er ook aandacht voor aanvullende thema's zoals connectiviteit, security fundamentals, duurzaamheid en configuratie. Hierbij wordt eveneens ingegaan op mogelijkheden voor het automatiseren van configuratieprocessen, waarmee de praktische toepasbaarheid verder wordt versterkt.

De volledige SAP BTP Documentatie en alle SAP BTP casestudies zijn te vinden in mijn portfolio.

6. SAP BTP Case studies

Een belangrijk onderdeel van mijn documentatie bestond uit het analyseren van diverse casestudy's van bedrijven die SAP BTP inzetten binnen hun digitale transformatie. Door het grondig bestuderen van deze praktijkvoorbeelden kon ik waardevolle inzichten krijgen in de concrete toepassingen, voordelen en strategische impact van het SAP Business Technology Platform in verschillende bedrijven, sectoren en contexten.

Het doel van deze casestudy-analyse was om te onderzoeken op welke manier SAP BTP daadwerkelijk bedrijfsproblemen oplost en hoe organisaties het platform inzetten om hun oplossingen en ideeën te realiseren. Voor elke individuele case ben ik gestart met een korte inleiding over het bedrijf in kwestie, een duidelijke omschrijving van de oorspronkelijke situatie en de bijbehorende probleemstelling. Dit zijn vaak complexe uitdagingen die te maken hebben met zaken zoals verouderde IT-landschappen, beperkte integratiemogelijkheden of inefficiënte processen.

Op basis van deze situaties worden vervolgens de specifieke doelstellingen beschreven die de organisatie met behulp van SAP BTP probeert te behalen. Denk hierbij aan het verbeteren van operationele efficiëntie, het versnellen van innovatie, het verhogen van klanttevredenheid, het automatiseren van repetitieve taken of het creëren van nieuwe digitale diensten.

Na het schetsen van de context en doelstellingen, beschrijf ik in detail de oplossing die is geïmplementeerd met SAP BTP. Hierbij wordt telkens uitgelegd hoe de verschillende BTP-componenten zijn ingezet om de bedrijfsdoelen te ondersteunen. Om de technische aanpak visueel te verduidelijken, bevat elke case een architecture diagram dat de opbouw van de oplossing weergeeft. Dit diagram toont onder andere hoe systemen met elkaar zijn verbonden, welke integraties zijn opgezet, welke databronnen worden gebruikt en hoe de communicatie tussen verschillende lagen binnen de oplossing verloopt.

Verder wordt in elke case nauwkeurig gedocumenteerd welke specifieke SAP- en SAP BTP-diensten of -services zijn toegepast. Daarbij staat telkens ook beschreven welke rol deze services vervullen binnen de oplossing.

Door deze casestudy's te analyseren, kreeg ik niet alleen inzicht in hoe flexibel en breed inzetbaar SAP BTP is, maar ook in hoe belangrijk het is om de juiste combinatie van tools en services te kiezen voor specifieke bedrijfsbehoeften en hoe bestaande systemen een verbetering kunnen krijgen, maar ook hoe helemaal nieuwe systemen gerealiseerd kunnen worden met SAP BTP.

6.1. Case-study: Integration bij Capgemini

Capgemini, een wereldwijd opererend technologie- en consultancybedrijf met hoofdkantoor in Parijs, ondersteunt organisaties bij hun digitale transformatie en groei. Het bedrijf biedt een breed scala aan diensten, van cloudoplossingen en data-analyse tot applicatie-integratie en strategisch advies. Met een aanwezigheid in meer dan 50 landen werkt Capgemini samen met organisaties van elke omvang om hun operaties toekomstbestendig te maken.

6.1.1. De uitdaging

Door de wereldwijde schaal waarop Capgemini opereert, ontstonden er uitdagingen rondom dataconsistentie en procesautomatisering. De organisatie kampte met gefragmenteerde datasystemen, verspreid over diverse regio's en business units. Hierdoor ontstond er een gebrek aan centrale controle over data, wat leidde tot inconsistente kwaliteit en trage besluitvorming.

Daarnaast verliepen veel kernprocessen handmatig, zoals servicelevering, facturatie en toewijzing van middelen. Dit zorgde voor vertragingen, menselijke fouten en knelpunten binnen de operationele keten. Om deze obstakels te overwinnen, was een geïntegreerde, intelligente digitale oplossing nodig.

6.1.2. Doelstellingen

Capgemini stelde een aantal concrete doelstellingen voor de transformatie:

- Het centraliseren en integreren van data uit verschillende bronnen
- Het verbinden van lokale (on-premise) systemen met moderne cloudomgevingen
- Het automatiseren van bedrijfsprocessen, met name binnen service delivery
- Het verbeteren van datakwaliteit en het verrijken van data-analysecapaciteiten

6.1.3. De oplossing

Capgemini koos voor SAP BTP als fundament voor de digitale transformatie. Deze oplossing maakte het mogelijk om een breed scala aan systemen, waaronder on-premise infrastructuur, private cloud en zowel SAP- als niet-SAP-applicaties te integreren in één uniform ecosysteem.

Door SAP BTP te koppelen aan de bestaande identity provider werd veilige en consistente toegang tot alle systemen gewaarborgd. Tegelijkertijd werden met behulp van AI-functies binnen SAP BTP tal van repetitieve taken geautomatiseerd. Denk hierbij aan ticketrouting, voorspellend onderhoud en optimalisatie van resourceallocatie. Werknemers konden zich hierdoor richten op strategischere taken.

Een belangrijk resultaat van deze aanpak was een stijging van 50% in realtime data-integraties. Dit verbeterde de flexibiliteit en snelheid waarmee Capgemini kon inspelen op veranderende omstandigheden binnen de dienstverlening en interne organisatie.

6.1.4. Gebruikte technologieën

Binnen het project maakte Capgemini gebruik van verschillende componenten van SAP BTP:

- SAP Business Application Studio: een cloudgebaseerde ontwikkelomgeving voor het bouwen, testen en uitrollen van SAP-applicaties.
- SAP Analytics Cloud: leverde realtime inzichten die besluitvorming op alle niveaus ondersteunden.
- SAP Integration Suite: zorgde voor de naadloze integratie van on-premise en cloudsystemen, waaronder ook niet-SAP-applicaties.
- AI-functionaliteiten: werden toegepast op onder andere service automation, predictive maintenance en resourceplanning.
- SAP Cloud Identity Services: bood een veilig en centraal gebruikersbeheer via authenticatie-, provisioning- en autorisatiefuncties.

6.1.5. Resultaten

De samenwerking tussen Capgemini en SAP resulteerde in een efficiënter, responsiever en toekomstbestendiger bedrijfsmodel. Door processen te automatiseren en systemen te integreren, kon Capgemini niet alleen sneller opereren, maar ook betere inzichten verkrijgen voor strategische beslissingen. De digitale transformatie legde de basis voor verdere innovatie en groei binnen een steeds digitaler wordende economie.

7. SAP Virtual Patching

7.1. Wat is virtual patching?

Virtual patching is een beveiligingsmaatregel die organisaties beschermt tegen kwetsbaarheden in software zonder dat er direct een aanpassing (patch) aan de sourcecode of het systeem zelf hoeft te worden gedaan. In plaats van te wachten op een officiële softwarepatch of het uitvoeren van een ingrijpende systeemupdate, wordt een tijdelijke beveiligingsregel toegepast, meestal via een beveiligingsoplossing zoals een firewall, intrusion prevention system (IPS) of endpoint protection systeem.

Het doel van virtual patching is tijd winnen: het voorkomt dat een bekende kwetsbaarheid misbruikt wordt, terwijl je organisatie tijd krijgt om een echte (permanente) patch veilig te testen en toe te passen.

7.1.1. Het belang van virtual patching

In complexe IT-landschappen, zoals bij grote bedrijven die SAP-systemen gebruiken, zijn updates vaak lastig en risicovol. Veel van deze systemen zijn bedrijfskritisch: ze beheren financiële gegevens, supply chains, HR-processen of klantrelaties. Downtime van zulke systemen kan miljoenen euro’s kosten, niet alleen door productiviteitsverlies, maar ook door contractuele boetes of imagoschade.

7.1.2. De werking van virtual patching

Bij een traditionele aanpak van het patchen van een vulnerability begint een IT-team met het analyseren van de kwetsbaarheid. Zodra een relevante kwetsbaarheid is geïdentificeerd, plannen ze een onderhoudsvenster in waarin de patch kan worden toegepast. Voordat deze daadwerkelijk wordt uitgerold naar het productiesysteem, wordt de patch eerst grondig getest in een aparte testomgeving om de stabiliteit en compatibiliteit te garanderen. Pas daarna wordt de patch tijdens gepland onderhoud, vaak 's nachts of in het weekend, op het live systeem geïnstalleerd. Gedurende de periode tussen de bekendmaking van de kwetsbaarheid en het moment waarop de patch daadwerkelijk actief is, blijft het systeem echter kwetsbaar voor aanvallen.

Met virtual patching verloopt dit proces anders. Zodra een kwetsbaarheid bekend wordt, wordt er direct een beveiligingsregel toegevoegd aan bijvoorbeeld een firewall of een Intrusion Prevention System (IPS). Deze regel is ontworpen om het specifieke patroon van de aanval te herkennen en blokkeren, bijvoorbeeld verdachte URL-calls of code-injecties die gebruikmaken van de kwetsbaarheid, zoals beschreven in de betreffende CVE. Hierdoor wordt het risico op een aanval vrijwel onmiddellijk weggewerkt, zonder dat het systeem zelf hoeft te worden aangepast of offline gehaald. Terwijl deze virtuele bescherming actief is, kan de IT-afdeling alsnog de tijd nemen om de officiële patch zorgvuldig voor te bereiden en gecontroleerd uit te rollen op een geschikt moment.

7.2. SAP Virtual Patching

Een van de meest technische en interessante projecten tijdens mijn stage was het opzetten en uittesten van een testomgeving binnen Microsoft Azure, met als doel het uitvoeren van virtual patching, in dit geval voor SAP-systemen. Deze aanpak is bedoeld om een alternatief te bieden voor traditionele patchingstrategieën, waarbij systemen vaak tijdelijk offline moeten worden gehaald. Zeker bij SAP-omgevingen, die doorgaans als cruciaal onderdeel van de bedrijfsvoering worden beschouwd kan dit leiden tot ongewenste downtime, verlies van productiviteit en risico's voor bedrijfscontinuïteit.

Het centrale doel van dit project was om te onderzoeken in hoeverre het mogelijk is om kwetsbaarheden (CVE's) in SAP-systemen af te schermen door middel van netwerkmatige bescherming, zonder dat het systeem zelf direct hoeft te worden gepatcht.

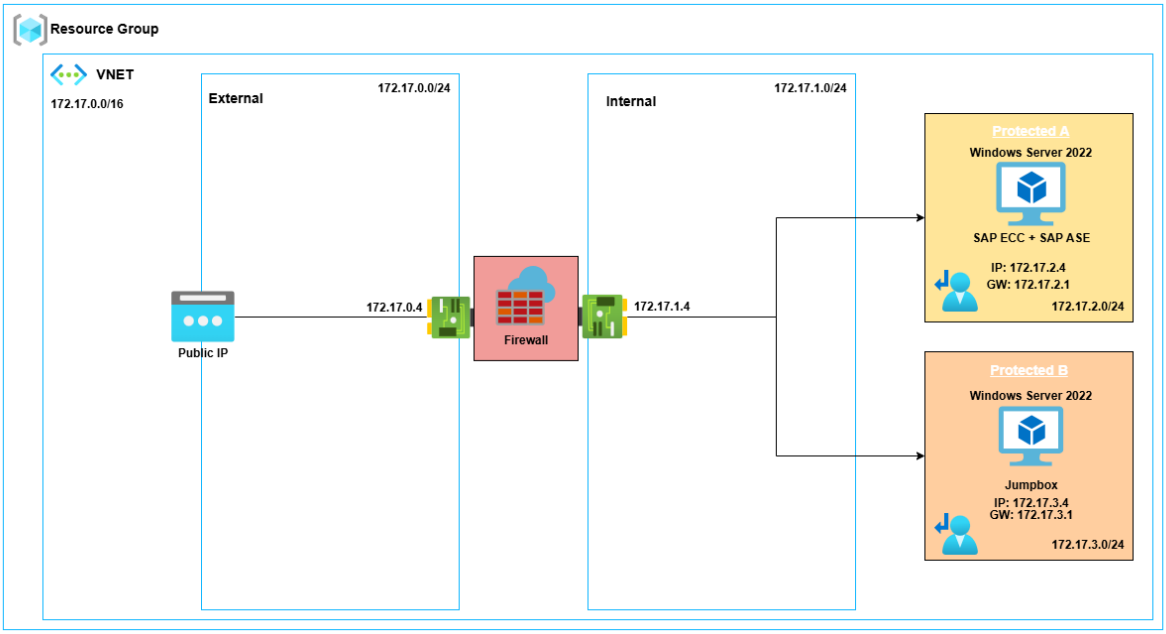
Voor dit project heb ik meegewerkt aan de volledige opzet van een testomgeving binnen Azure. De infrastructuur omvat een kwetsbare SAP-installatie die bewust opgezet is met bekende beveiligingskwetsbaarheden, om zo een realistische aanvalssimulatie mogelijk te maken. Deze kwetsbaarheden zijn gebaseerd op publiek gedocumenteerde CVE's, waarvan bekend is dat ze misbruikt kunnen worden als een systeem onvoldoende is bijgewerkt.

Tijdens de voorbereidende fase werkte ik mee aan het ontwerp van het netwerk en het plannen van de Cloud-infrastructuur op Azure. In deze fase stond samenwerking centraal, waarbij ik nauw samenwerkte met een collega stagiaire uit het netwerkteam.

Hoewel mijn hoofdverantwoordelijkheid lag bij het SAP-gedeelte van de opstelling: het installeren, configureren en onderzoeken van de SAP-systemen zelf, heb ik ook actief bijgedragen aan de netwerkarchitectuur en netwerkconfiguratieconfiguratie binnen Azure. Zo was ik betrokken bij het opzetten van subnets, het instellen van netwerkbeveiligingsgroepen (NSGs), en het configureren van routing en toegang via de bastionhost.

7.3. Azure Architectuur

Voor dit project werd de volledige infrastructuur opgezet binnen Microsoft Azure, en meer specifiek binnen een resource group die werd aangemaakt voor dit project. Een resource group in Azure is een verzamelgroep waarin gerelateerde Azure-resources worden beheerd als een geheel. Dit betekent dat alle componenten die nodig zijn voor deze omgeving zoals virtuele machines, netwerken, IP-adressen, firewalls, enz. logisch gegroepeerd en gezamenlijk beheerd worden. Hierdoor wordt het eenvoudiger om rechten, policies, kosten en lifecycle management op een consistente manier toe te passen over alle onderdelen van het systeem.



7.3.1. Azure VNET

Alle onderdelen van het systeem zijn ondergebracht binnen één enkel Azure Virtual Network (VNET). Een VNET is de fundamentele bouwsteen voor netwerkcommunicatie in Azure. Het biedt een geïsoleerd, private-netwerk waarin Azure-resources zoals virtuele machines, applicaties en databases met elkaar kunnen communiceren, vergelijkbaar met hoe netwerken binnen een traditioneel datacenter functioneren.

Een VNET kan vergeleken worden met een Virtual Private Cloud (VPC) in AWS, beide bieden dezelfde kernfunctionaliteit: een logisch afgescheiden netwerk in de cloud waarin je volledige controle hebt over IP-adressering, subnets, routing en beveiliging. Net als bij een VPC kunnen binnen een VNET meerdere subnets worden gedefinieerd om verschillende netwerksegmenten van elkaar te scheiden.

Binnen het gecreëerde VNET werden verschillende subnets aangemaakt, elk met een specifieke functie binnen het systeem. Deze subnets vormen gescheiden netwerkzones en zorgen voor een duidelijke segmentatie van de infrastructuur. De opdeling is als volgt:

VNET & Subnets	
VNET	172.17.0.0/16
External Subnet	172.17.0.0/24
Internal Subnet	172.17.1.0/24
Protected Subnet A	172.17.2.0/24
Protected Subnet B	172.17.3.0/24

De Internal en External subnets vormen de netwerkomgeving rond de firewall. Het External subnet is verbonden met het publieke internet via een toegewezen Public IP, wat communicatie met externe systemen mogelijk maakt. Het Internal subnet vormt samen met het External subnet de frontzone van de infrastructuur waarin verkeer eerst gefilterd en verwerkt wordt.

De twee Protected subnets dienen voor meer kritieke infrastructuurcomponenten:

- Protected subnet A bevat het SAP-testsysteem.
- Protected subnet B bevat een bastion host.

7.3.2. Bastion Host

Een bastion host is een speciaal ingerichte virtuele machine die dient als veilige toegangspoort tot andere systemen binnen een privénetwerk. In ons geval wordt de bastion host gebruikt om via Remote Desktop Protocol (RDP) toegang te verkrijgen tot het interne netwerk van Azure. Gebruikers verbinden eerst met de bastion host, die zich in een subnet met strikte toegangsregels bevindt. Van daaruit kunnen ze veilig doorverbinden naar andere systemen, zoals het SAP-testsysteem, zonder dat deze systemen zelf direct publiek toegankelijk zijn.

7.3.3. Firewallconfiguratie

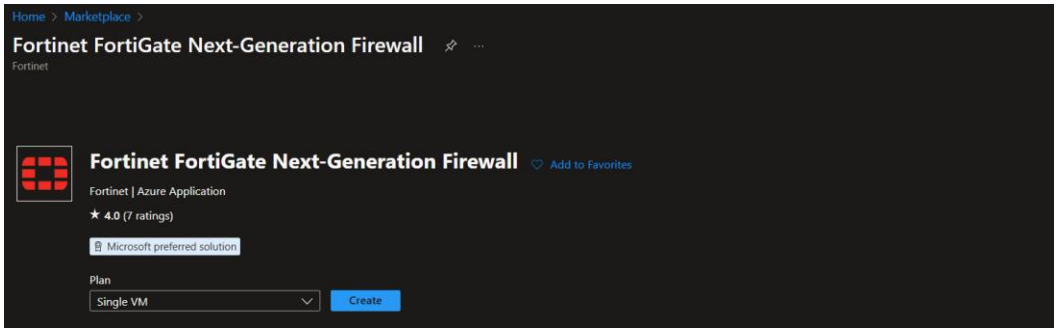
Als firewall werd gekozen voor een FortiGate firewall, die zich als enkele instance tussen de External en Internal subnets bevindt. Deze firewall zorgt voor de centrale beveiliging van al het binnenkomende en uitgaande netwerkverkeer. In een productieomgeving zou men echter gebruikmaken van een opstelling met een dubbele firewall voor meer redundantie.

Hiervoor bestaan twee klassieke configuratiemodellen:

- Active-passive configuratie
  - In dit model is één firewall actief, terwijl de tweede in stand-by blijft. Als de actieve firewall faalt, neemt de passieve firewall automatisch over.
  - Voorbeeld: Firewall A is actief en verwerkt al het verkeer. Firewall B is inactief maar gesynchroniseerd. Wanneer Firewall A uitvalt, wordt Firewall B automatisch actief.

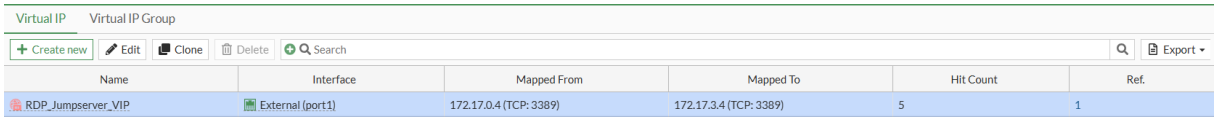
- Active-active configuratie
  - Hier zijn beide firewalls actief en verwerken ze tegelijkertijd verkeer. Deze opstelling biedt betere prestaties maar vereist complexere load balancing.
  - Voorbeeld: Beide firewalls zijn tegelijk actief; verkeer wordt verdeeld via een load balancer. Als één firewall faalt, blijft de andere firewall het verkeer verwerken.

Voor dit testsysteem werd bewust gekozen voor een lichte opstelling met een enkele firewall, aangezien het hier niet gaat om een productieomgeving maar om een tijdelijke testomgeving. Het opzetten van de firewall via Azure werd gedaan met een template, daardoor kon er op een heel eenvoudige manier een VM opgezet worden met een werkende installatie van FortiGate.

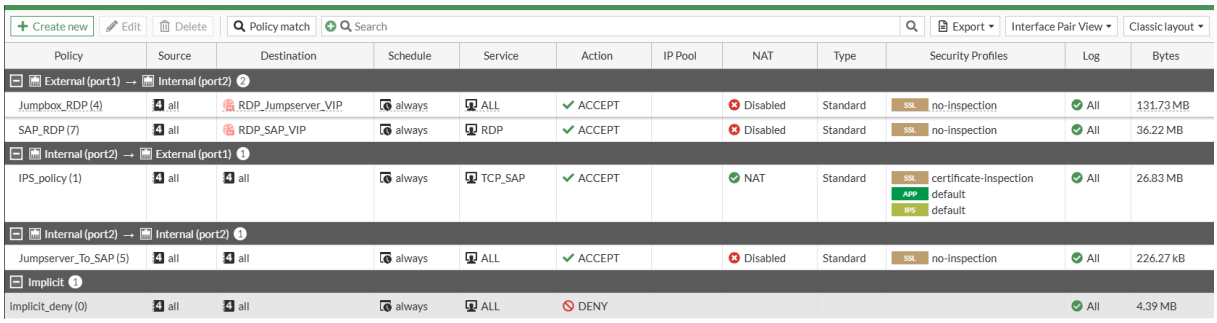


7.3.4. Virtual IP

Om verbinding te maken met de bastion host is een Virtual IP (VIP) geconfigureerd, die al het netwerkverkeer op poort 3389 (RDP) naar het private IP-adres van de bastion host doorstuurt.



7.3.5. Firewall policies

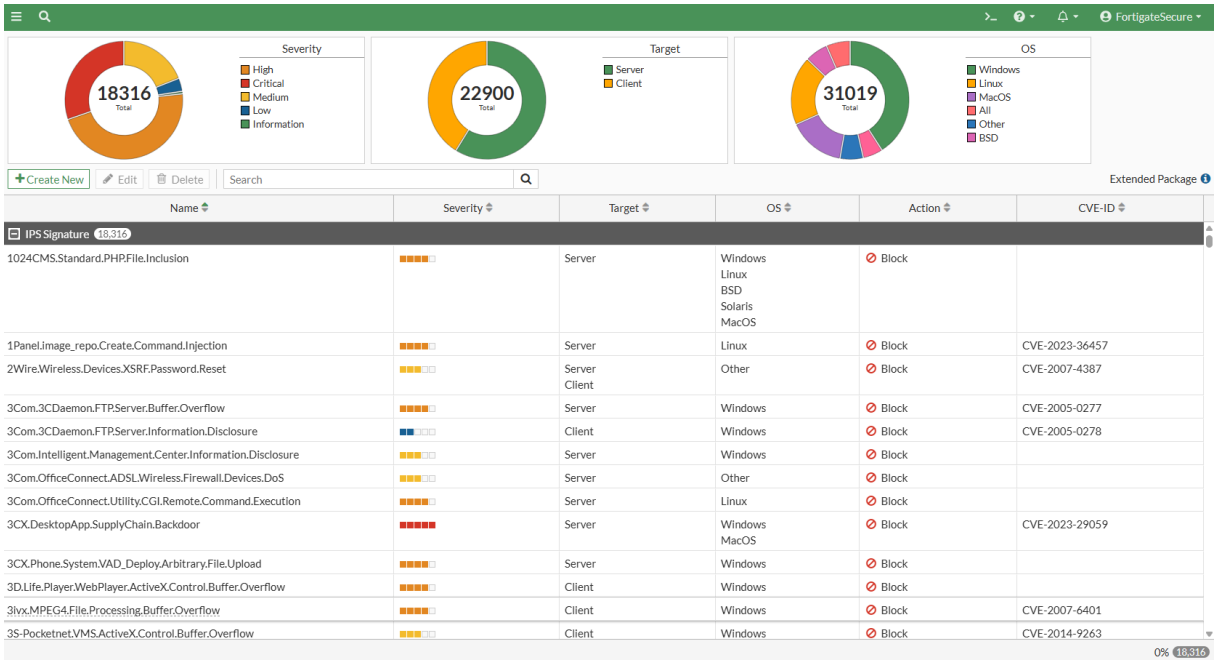


Op de firewall is standaard alle netwerkverkeer geblokkeerd; enkel verkeer dat we expliciet toestaan krijgt toegang tot het netwerk. Voor test- en debugdoeleinden van het SAP-systeem werd tijdelijk een rechtstreekse verbinding opgezet tussen het external subnet en protected subnet A, het subnet waarin de SAP-VM zich bevindt. Hoewel dit praktisch kan zijn tijdens troubleshooting, is dit vanuit security-oogpunt geen best practice. Idealiter verloopt alle toegang via de bastion host, die (zoals eerder vermeld) fungeert als gecontroleerd toegangspunt tot de SAP-VM.

Daarnaast is er een specifieke firewall policy ingesteld om het intrusion prevention system (IPS) van FortiGate te kunnen testen. Deze configuratie maakt het mogelijk om potentiële dreigingen te detecteren en blokkeren tijdens de evaluatie van het netwerkverkeer.

7.3.6. IPS Signatures

De firewall bevat een lijst met IPS-signatures die automatisch wordt bijgewerkt door Fortinet. Voor elke signature in deze lijst is gedetailleerde informatie beschikbaar, zoals het bijbehorende CVE-ID, het doelwit (bijvoorbeeld client of server), het type besturingssysteem, de ernstgraad (severity) en het soort aanval of kwetsbaarheid waarop de signature betrekking heeft. Deze informatie helpt bij het nauwkeurig detecteren en blokkeren van bedreigingen binnen het netwerk. Standaard worden zo goed als alle signatures geblokkeerd uiteraard.



7.3.7. SAP Systeem

Voor het SAP-systeem werd ook gekozen voor een eenvoudigere opstelling. In een klassieke enterprise-omgeving bestaat een SAP-landschap typisch uit drie lagen:

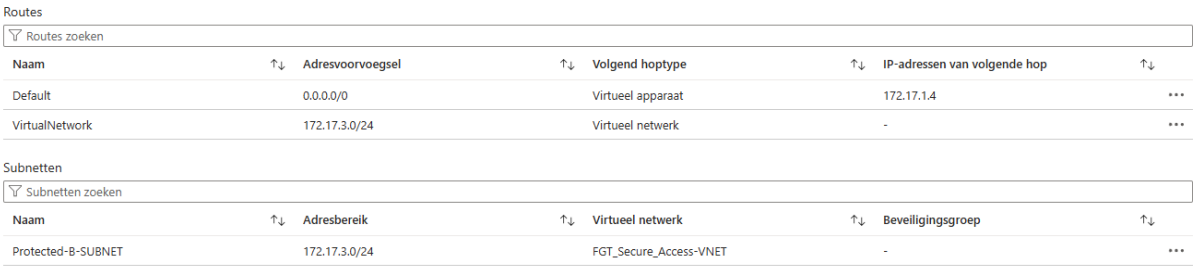
- Development (DEV)
- Quality Assurance System (QAS)
- Production (PRD)

Voor deze testomgeving werd dit vereenvoudigd. Eén SAP-systeem fungeert als productieomgeving aangezien er maar 1 omgeving nodig is om de virtual patching te testen.

7.3.8. User Defined Routes

Een belangrijk beveiligingsprincipe binnen deze architectuur is dat verkeer tussen de verschillende subnets steeds via de firewall moet verlopen. Azure laat standaard communicatie toe tussen subnets binnen hetzelfde VNET. Om dit gedrag te wijzigen en te forceren dat al het verkeer langs de firewall passeert, worden zogenaamde User Defined Routes (UDRs) toegepast.

Een User Defined Route is (zoals de naam al zegt) een door de gebruiker gedefinieerde netwerkroute die standaardrouting overschrijft. Je bepaalt zelf welk subnet welk pad moet volgen om een ander subnet te bereiken. Door aangepaste routes toe te voegen aan de route tabellen van elk subnet, wordt het verkeer van bijvoorbeeld Protected Subnet A naar Protected Subnet B eerst omgeleid naar de firewall, die het vervolgens verwerkt en doorstuurt.



7.4. Kwetsbaarheden bij SAP-systemen

In het kader van netwerkbeveiliging is het essentieel om stil te staan bij kwetsbaarheden (vulnerabilities) die kunnen voorkomen in complexe bedrijfsapplicaties zoals SAP-systemen. SAP vormt voor veel organisaties het hart van hun bedrijfsvoering, het beheert kritische gegevens en processen zoals financiën, logistiek en HR. Daardoor zijn SAP-omgevingen een aantrekkelijk doelwit voor aanvallers.

Een kwetsbaarheid in een systeem of applicatie wordt wereldwijd geregistreerd en gedeeld onder de vorm van een CVE, wat staat voor Common Vulnerabilities and Exposures. Dit is een gestandaardiseerd systeem dat unieke identifiers toekent aan publiek bekende beveiligingslekken. Elke CVE heeft een uniek nummer (bijvoorbeeld: CVE-2023-28765), een korte beschrijving van het probleem, en informatie over de ernst (vaak aangeduid via een CVSS-score, de Common Vulnerability Scoring System).

SAP-systemen bestaan uit vele componenten en modules die regelmatig worden geüpdatet via zogenaamde SAP Security Notes. Deze bevatten vaak oplossingen voor CVE's. Als die updates niet tijdig worden toegepast, kunnen aanvallers misbruik maken van bekende kwetsbaarheden.

7.4.1. Gebruikte CVE

Voordat we konden beginnen met testen, was de eerste belangrijke stap het identificeren van een geschikte CVE (Common Vulnerabilities and Exposures). Deze kwetsbaarheid moest al opgenomen zijn in de lijst met IPS-signatures van FortiGate, én ons SAP-systeem moest er daadwerkelijk vatbaar voor zijn.

Om een kwetsbaarheid te vinden die nog niet gepatcht was in ons SAP-systeem, en tegelijkertijd door FortiGate's Intrusion Prevention System (IPS) werd herkend, hebben we eerst het patchniveau van ons systeem opgezocht. Het systeem draaide op patch level 200 en gebruikte SAP NetWeaver 7.54 ABAP als basis. Uiteindelijk vonden we CVE-2020-6215 terug in de lijst van IPS-signatures.

CVE-2020-6215 is een beveiligingslek in de testapplicatie IT00 van SAP NetWeaver's ABAP Business Server Pages (BSP). Deze kwetsbaarheid maakt het mogelijk voor aanvallers om kwaadaardige links te genereren die gebruikers omleiden naar onbetrouwbare websites, vanwege gebrekkige validatie van URL's. Wanneer een gebruiker op zo'n link klikt, kan hij onbewust gevoelige informatie zoals inloggegevens doorgeven aan een aanvaller. Dit type vulnerability staat bekend als een open redirect.

De kwetsbaarheid heeft een CVSS v3.1-basisscore van 6.1, wat neerkomt op een middelgroot risico.

Aangezien ons SAP-systeem op een compatibele versie van NetWeaver draait en het patchniveau laag genoeg is, is de kwetsbaarheid effectief nog mogelijk om te exploiten.

Om deze kwetsbaarheid zelf te kunnen testen, moest ik eerst de kwetsbare BSP-testapplicatie IT00 handmatig activeren via de SAP GUI.

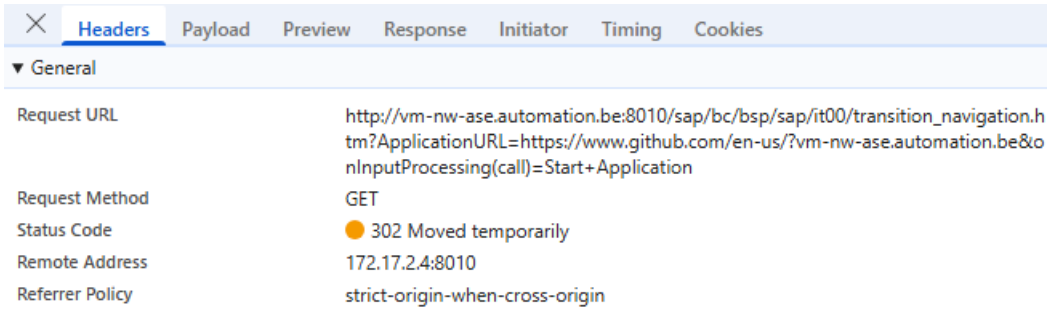
7.4.2. Exploit van de CVE

In een typische situatie openen gebruikers SAP BSP-applicaties via een URL zoals: http://vm-nw-ase.automation.be:8010/sap/bc/bsp/sap/it00

Deze URL leidt naar een echte betrouwbare pagina binnen het SAP-systeem, afkomstig van een vertrouwde Fully Qualified Domain Name (FQDN).

Door een open redirect-kwetsbaarheid in de IT00-testapplicatie (CVE-2020-6215) kan een aanvaller echter een nep URL opstellen die eruitziet alsof deze afkomstig is van het echte SAP-domein, maar de gebruiker in werkelijkheid ongemerkt doorstuurt naar een externe, door de aanvaller beheerde website. Een voorbeeld van zo'n gemanipuleerde URL is: http://vm-nw-ase.automation.be:8010/sap/bc/bsp/sap/it00/transition_navigation.htm?ApplicationURL=https://www.github.com/?vm-nw-ase.automation.be&onInputProcessing(call)=Start+Application

Deze link lijkt afkomstig van het SAP-systeem, maar bij het aanklikken wordt de gebruiker doorgestuurd naar https://www.github.com of eender welk adres de aanvaller kiest.



Dit vormt een ernstig phishingrisico. Een aanvaller kan bijvoorbeeld een valse website opzetten die eruitziet als het SAP NetWeaver-loginpagina en zo nietsvermoedende gebruikers misleiden om hun inloggegevens in te voeren. Omdat de link afkomstig lijkt van het vertrouwde SAP-domein, zijn gebruikers eerder geneigd hem te vertrouwen met alle gevolgen van dien.

Dit type aanval is extra gevaarlijk in bedrijfsomgevingen, waar SAP-systemen vaak verantwoordelijk zijn voor kritieke bedrijfsprocessen en gevoelige gegevens.

7.4.3. Besluit van het virtual patching project

Op basis van dit onderzoek is het duidelijk dat virtual patching weliswaar potentieel biedt als tijdelijke beveiligingsmaatregel voor SAP-systemen, maar dat de effectiviteit ervan momenteel beperkt is. Dit komt vooral door het beperkte aantal relevante en actuele IPS-signatures die beschikbaar zijn in oplossingen zoals FortiGate.

Hoewel het detecteren en blokkeren van aanvallen met de FortiGate IPS goed werkt, blijven veel bekende SAP-kwetsbaarheden, waaronder verschillende kritieke onopgemerkt omdat er simpelweg te veel essentiële signatures ontbreken. Hierdoor kunnen deze kwetsbaarheden ongedekt blijven. Dit betekent dat men moeilijk al het vertrouwen in de IPS-oplossing alleen kan leggen.

Het networking team staat momenteel in contact met FortiGate om te onderzoeken wat de mogelijkheden zijn voor betere ondersteuning van SAP-kwetsbaarheden via hun IPS-oplossing. Deze samenwerking is van cruciaal belang om de bruikbaarheid van virtual patching in de praktijk te vergroten.

Virtual patching moet dan ook niet worden gezien als vervanging voor reguliere systeemupdates, maar eerder als een tijdelijke vorm van risicobeperking. Mits correct toegepast, kan het helpen om het risico op exploits te verlagen in de periode tussen het ontdekken van een kwetsbaarheid en het installeren van een officiële patch of het uitvoeren van gepland onderhoud. Dit is vooral waardevol in SAP-omgevingen, waar het patchen van systemen vaak gepaard gaat met aanzienlijke downtime en verstoring van bedrijfsprocessen.

Voor virtual patching om een écht bruikbare oplossing te zijn, is het essentieel dat vendors hun IPS-signaturedatabases continu en actief bijwerken met nauwkeurige detection rules die specifiek zijn afgestemd op SAP-kwetsbaarheden. Zolang die ondersteuning ontbreekt, blijft virtual patching vooral een theoretisch nuttige aanpak, maar in de praktijk nog te beperkt inzetbaar.

8. Besluit

Deze stage betekende voor mij een belangrijke eerste stap in zowel mijn persoonlijke als professionele groei. Het was mijn eerste échte ervaring binnen een groot IT-bedrijf en tegelijk mijn eerste kennismaking met de wereld van consultancy. Die nieuwe omgeving, in combinatie met de praktische toepassing van mijn opleiding, zorgde ervoor dat ik in korte tijd veel heb kunnen bijleren.

Tijdens mijn stage kreeg ik de kans om aan uiteenlopende projecten mee te werken en in aanraking te komen met diverse technologieën en werkwijzen. Wat me vooral bijblijft, is hoe snel ik mijn theoretische kennis kon omzetten in praktijkervaring. Ik leerde niet alleen werken met complexe software zoals SAP, maar kreeg ook inzicht in hoe IT-omgevingen in de echte bedrijfswereld worden beheerd en beveiligd.

Naast mijn technische groei heeft deze stage me ook geholpen om mijn soft skills verder te ontwikkelen. Door samen te werken met collega's uit verschillende teams, heb ik geleerd om vlotter te communiceren, zelfstandig te werken en me flexibel op te stellen in een professionele context. De combinatie van hands-on ervaring, nieuwe inzichten in networking en security, en het samenwerken in een consultancy-omgeving heeft me een breder beeld gegeven van de IT-sector als geheel.

Wat ik bovendien bijzonder waardeerde, was dat ik ook buiten mijn comfortzone kon werken. Hoewel ik tijdens mijn opleiding zaken zoals Cloud en DevOps het liefste deed, ontdekte ik tijdens deze stage dat ik ook interesse heb voor netwerkbeveiliging en netwerkinfrastructuur.

9. Literatuurlijst

Fortinet. (sd). *FortiGuard IPS Service*. Opgehaald van fortinet.com: https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/intrusion-prevention

Grover, J. (10, September 2024). *Azure vNet, reserved IP range, DHCP, and Palo Alto firewall VM*. Opgehaald van Microsoft Learn: https://learn.microsoft.com/en-us/answers/questions/2046376/azure-vnet-reserved-ip-range-dhcp-and-palo-alto-fi

jvhoof. (2025, February 24). *Fortinet Azure Templates*. Opgehaald van GitHub: https://github.com/fortinet/azure-templates/tree/main/FortiGate/A-Single-VM

MITRE. (sd). *CVE-2020-6215*. Opgehaald van cve.mitre.org: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-6215

NIST. (14, March 2020). *CVE-2020-6215 Detail*. Opgehaald van nvd.nist.gov: https://nvd.nist.gov/vuln/detail/cve-2020-6215

SAP. (sd). *Administrating SAP Business Technology Platform*. Opgehaald van SAP Learning: https://learning.sap.com/learning-journeys/administrating-sap-business-technology-platform

SAP. (sd). *Becoming an SAP BTP Solution Architect*. Opgehaald van SAP Learning: https://learning.sap.com/learning-journeys/becoming-an-sap-btp-solution-architect

SAP BTP Customer Stories. (sd). Opgehaald van sap.com: https://www.sap.com/products/technology-platform/customer-stories.html?sort=latest_desc

SAP. (sd). *Discovering SAP Business Technology Platform*. Opgehaald van SAP Learning: https://learning.sap.com/learning-journeys/discover-sap-business-technology-platform

SAP. (sd). *SAP Security note 3258950*. Opgehaald van sap.com: https://me.sap.com/notes/3258950

Sploitus. (2023, October 6). *Exploit for SAP Application Server ABAP Open Redirection CVE-2020-6215 CVE-2023-6215*. Opgehaald van sploitus.com: https://sploitus.com/exploit?id=PACKETSTORM:174985

YISUSVII. (2024, January 9). *Understanding Azure Virtual IP (VIP) Ranges and Subnet Sizing*. Opgehaald van medium.com: https://yisusvii.medium.com/understanding-azure-virtual-ip-vip-ranges-and-subnet-sizing-aec62d436a5a