REGIONALE ENTERPRISE ARCHITECTUUR PRINCIPES

(2022-0265) Aanbesteding Firewall

Beschrijving van deze werkset

Doel: Sjabloon POA/LIGHT PSA

Auteur(s): Frans Loth, Gerhard Striekwold

Versie: 0.7

Datum: 13-12-2023

Leeswijzer:

(2022-0265) Firewall aanbesteding

De POA/Light PSA geeft op een beknopte wijze inzicht in de gewenste functionaliteit, koppelingen, relaties en - zonodig - de migratie-aanpak.

Indien aan de Light PSA een POA vooraf is gegaan, dan geeft de PSA antwoord op de gestelde vragen, keuzes en inventarisatiepunten.

De PSA vormt de input voor aanbesteding dan wel HLD

GEMMA REFERENTIE COMPONENT

Plaats hier de Gemma referentie component(en) en leg een relatie met de kern van de verandering.

BUITEN SCOPE PLAATSING?

<< GEEF OVERZICHT WAT BUITEN SCOPE VAN HET ONDERWERP IS. Neem bij voorkeur applicatie componenten op. En geef de reden aan>>

RELEVANTE WERKSETS

Regionale Enterprise Architectuur

Denk hierbij aan PROCES platen, context diagrammen, projectoverzicht, etc.

Ontwerpkeuze is gemaakt (veranderint t.o.v. vorige iteratie)

LET OP. Zie begeleidende toelichting. Eventueel uitzoekpunt.

Knelpunt. Nader onderzoek nodig. Keuze noodzakelijk. eventueel exception nodig.

Niet mogelijk of Niet toegetaan

Regionale I-Visie en Strategie

- (I-Visie en Strategie) De inzet van (informatie)technologie draagt bij aan het behalen van onze organisatie doelen/ambities. De behoefte van onze inwoners staat hierbij centraal
- (I-Visie en Strategie) Informatie en data worden ingezet bij operationele, tactische en strategische besluiten
- (I-Visie en Strategie) We kiezen die (innovatieve) informatietechnologie, die past bij een moderne en flexibele organisatie
- (I-Visie en Strategie) We volgen zoveel mogelijk de landelijke standaarden
- (I-Visie en Strategie) De wijze waarop wij informatietechnologie inzetten, sluit nauw aan bij de vraag van de organisatie/afdelingen
- (I-Visie en Strategie) Onze informatiehuishouding (architectuur) past bij de organisatiedoelen en is flexibel en samenhangend (integraal) van opzet
- (I-Visie en Strategie) Onze informatiehuishouding is ingericht op het samenwerken met ketenpartners
- (I-Visie en Strategie) We passen de middelen op een veilige wijze toe met respect voor een leiders privacy en wet- en regelgeving

G3DC REGIONALE ENTERPRISE ARCHITECTUUR PRINCIPES

BUSINESS PRINCIPES

- A11 - We standaardiseren maximaal
- A12 - Aanpassingen worden gedaan naar aanleiding van business behoefte of business belang

INFORMATIE / APPLICATIE ARCHITECTUUR PRINCIPES

TECHNISCHE ARCHITECTUUR PRINCIPES

- T02 - Voor één functie gebruiken we één softwaretoepassing
- T03 - Referentie componenten en Technologie worden hergebruikt
- T04 - Informatietechnologie wordt duurzaam ingericht
- T10 - We gebruiken bij voorkeur alleen bewezen producten en technieken
- T13 - Voor een betrouwbare en schaalbare ICT-infrastructuur, maken we gebruik van modulaire en gestandaardiseerde bouwstenen.

SECURITY ARCHITECTUUR PRINCIPES

- B01 - Vertrouw nooit, verifieer altijd

BEHEER ARCHITECTUUR PRINCIPES

- BEH01 - We streven naar minimalisering van de beheerlast
- BEH03 - De ICT organisatie is zich zeer bewust ten aanzien van de business en de kosten

Nevenstaande principes zijn in het bijzonder geldig voor de gewenste oplossing

Voor volledige mschrijving: zie werkset Regionale Enterprise Architectuur

LEGENDA EA principes

- Is volledig van toepassing
- Er wordt deels afgeweken van het principe
- Er wordt volledig afgeweken van het principe

DOELEN

- (DC) D2 - Continuïteit van de dienstverlening is gebordg
- (DC) D3 - Optimale inzet van middelen tegen de laagste kosten en risico's
- (DC) D8 - We zorgen voor een beveiligde Informatiehuishouding

REQUIREMENTS

<<FUNCTIONEEL ONDERWERP>>

- De oplossing dient schaalbaar te zijn
- De oplossing moet aansluiten op de Microsoft Azure Cloud omgeving
- Aan de Microsoft Azure Cloud dient te worden gekoppeld middels een Expressroute

GOVERNANCE

- AVW-BHR019 Logging relevante acties, handelingen en (beveiligings) meldingen in te zien door specifiek toegewezen rollen vanuit Opdrachtgever. Tevens moet het mogelijk zijn deze (audit)logging realtime, op veilige wijze aan te kunnen bieden aan een SOC/SIEM van de Opdrachtgever.
- De oplossing dient meerdere virtual instances te ondersteunen
- ondersteunt open standaard routing protocollen zoals OSPF
- integratie met on-premises Active Directory om regels en logging aan AD-objecten te kunnen koppelen

SECURITY/PRIVACY

- Bij inkomend verkeer vanaf internet dient SSL inspectie te worden gedaan. (deep inspection)

DATA PROTECTIE

ADOPTIE

–

OVERIG

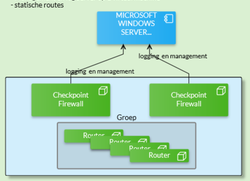
- De G3DC AVW zijn van toepassing.

LEGENDA Requirements

- De requirement is in lijn met de principes
- Deze requirements wijken af van de principes.
- Deze requirements zijn een gevolg van afwijkingen. Er wordt verwezen naar de relevante afwijkingen).

HUIDIGE SITUATIE

2 fysieke firewalls in een clusteropstelling (CheckPoint VSX)
- bevat 8 virtuele instances (gekoppeld aan VRF op netwerklaag; virtuele routing firewall)
- wordt gebruikt voor zowel extern, als interne netwerkverkeer
- functioneert ook als core router
- Extern verkeer gefiltert door: IPS, Antibot, Application control, URL-filtering, Identity awareness, monitoring, Antivirus
- RemoteAccess en Site2Site VPN leveranciers (o.a. L2TP/IPSEC)
- Management en log server op 1 virtual machine
- statische routes



MIGRATIE / TUSSENFASE

(fysieke) koppelvlakken
subnetten
firewall rules
vpn-connecties

NIEUWE SITUATIE

EXTRA INFORMATIE

Plaats hier algemene opmerkingen

LET OP:
Integratie met on-premises Active Directory zal in de toekomst uitgefaseerd worden.

DATACENTER 1

DATACENTER 2

Bedrijfs Architectuur

- A01 - Onze organisatie denkt vanuit de positie van de klant
- A02 - Onze organisatie gebruikt generieke processen en functies
- A04 - Onze organisatie biedt de klant een goede Informatiepositie
- A05 - Onze organisatie digitaliseert haar diensten en processen
- A06 - Onze organisatie stelt openbare gegevens als open data beschikbaar
- A07 - Onze organisatie hergebruikt gegevens
- A08 - Onze organisatie gaat op een vertrouwelijke manier met gegevens om
- A09 - Gebruik end-to-end processen
- A10 - Informatie is een asset

Informatie Architectuur

- I01 - Richt digitale dienstverlening in zoals de klant dat zelf ook prettig vindt
- I04 - Wij maken keuzes in de volgorde gebruik – data – applicatie
- I05 - Biedt selfservice aan gemeenten / inwoner
- I06 - Werk iteratief en verbeter snel
- I08 - We zijn transparant waar mogelijk
- I10 - We leggen gegevens eenmalig vast en vragen op bij de bron
- I11 - We faciliteren regie op gegevens
- I14 - Gemeenschappelijke terminologie en gegevensdefinities
- I15 - Onze informatiehuishouding is ingericht op het samenwerken met ketenpartners

Applicatie Architectuur

- AP1 - Applicaties zijn technologie onafhankelijk
- AP2 - Applicaties zijn eenvoudig te gebruiken
- AP3 - Componenten zijn logisch en herbruikbaar
- AP4 - Applicaties dragen bij aan de bedrijfsdoelen
- AP6 - Applicaties zijn vluchtig gekoppeld
- AP7 - Applicaties sluiten aan op de functionele domeinen
- AP8 - Bij vervanging van Applicaties, conversie tenzij
- AP9 - Applicaties moeten geschikt zijn voor multi tenancy

Technische Architectuur

- T07 - We maken gebruik van landelijk en gemeentelijk beschikbare services
- T08 - We verlenen toegang op basis van rollen, functie en locatie
- T09 - Wij verlenen toegang vanuit één portaal.
- T11 - We werken op basis van een multi tier architectuur
- T12 - Eindgebruikers functionaliteit kan plaats- en tijd onafhankelijk worden gebruikt
- T14 - We ondersteunen de toekomstige Informatievoorziening (Common Ground)
- T16 - Elk object heeft een eigenaar die verantwoordelijk is voor dat object
- T18 - We gebruiken actuele versies van objecten
- T20 - Technologie wordt herbruikt

Beveiliging Architectuur

- B02 - Informatiebeveiliging is van iedereen
- B03 - Informatiebeveiliging is risicobeheersing
- B04 - Risicomanagement is onderdeel van de besluitvorming
- B05 - Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
- B06 - Informatiebeveiliging is een proces
- B07 - Informatiebeveiliging kost geld
- B08 - Onzekerheid dient te worden ingecalculeerd
- B09 - Verbetering komt voort uit leren en ervaring
- B10 - Het bestuur controleert en evalueert
- B11 - Bestuurders bevorderen een veilige cultuur

Beheer Architectuur

- BEH02 - We streven naar minimal management
- BEH04 - De klant kent zijn eigen business, data en processen

Legenda

Objecten
- Applicatiecomponent
- Node
- Principe
- Project

Relaties
- wordt gebruikt door