Nom du service G-Cloud

Internet Access Protection / Security as a Service ***01-01-2020***

Description du service G-Cloud

Le G-Cloud offre aux institutions publiques des services de sécurité informatique par le biais de deux options différentes applicables selon le contexte de l'institution. Techniquement, les deux services sont fort similaires, les différences majeures se situant dans la gouvernance et la forme du contrat.

1. Internet Access Protection

Offre modulaire de composants d'infrastructure de sécurité basée sur une combinaison de cahiers des charges d'infrastructure, de services et de contrats de services fournis par Smals.

Il existe différentes possibilités de gestion permettant aux clients d'opter tant pour un service entièrement géré que pour une infrastructure de sécurité en gestion propre. IAP est géré au sein de la communauté publique, avec une forte concentration sur les besoins du business et des data centers.

La plateforme est installée dans les data centers du G-Cloud (IN et UP), à l'exception d'un service SIEM externe (Proximus).

2. Security as a Service

Security as a Service est un service de gestion des risques, qui comprend un ensemble de services de sécurité et de gouvernance avec une infrastructure sous-jacente, comme un registre des risques et le suivi des risques potentiels détectés.

Ce service est un service entièrement géré, à la suite d'un marché public attribué à Proximus, pour la sécurisation des composants de l'infrastructure. Ce contrat comprend également une forte composante de protection bureautique et repose sur une large base d'utilisateurs du SPF Finances et du SPF Justice comme point de départ.

La plateforme est installée dans les data centers du G-Cloud (Noga et Finto), à l'exception des plateformes de management de Proximus et d'un certain nombre de services externes DNS/Mail security/DDoS et SIEM.

Nom du service G-Cloud

Internet Access Protection ***01-01-2020***

Description du service G-Cloud

Avec IAP, une plateforme centrale est mise à la disposition des institutions fédérales pour sécuriser l'accès à et depuis internet. Cette plateforme s'appelle Internet Access Protection (IAP) et est basée sur le concept de sécurité d'Extranet élaboré par Smals.

IAP permet aux institutions fédérales de communiquer entre elles de façon directe et sécurisée, mais aussi d'échanger des informations sans devoir passer par internet.
Smals offre différentes options de gestion permettant aux clients d'opter tant pour un service géré que pour une infrastructure de sécurité en gestion propre. Le service est créé sous forme modulaire, en fonction des besoins du client, pour garder le contrôle de la sécurité et du business correspondant.

IAP peut être considéré comme la "couche" commune dans la protection de l'information et comporte les services suivants :

Package de base IAP :

- Connexion à internet via FedMAN, sécurisée avec :
  - Firewalling
  - IDP (Intrusion Detection Prevention)
  - Anti-DDoS
  - SIEM (Security information and event management operations)
- DNS (Domain Name System) avec réplication vers un système DNS "externe"
- NTP (Network Time Protocol) service (Stratum 1)

Options IAP :

- Proxy User et antivirus (avec sandboxing) pour la sécurisation du trafic http(s) et (s)ftp
  - Web-filtering / Web reputation
  - Sandboxing (Advanced Threat Protection)
  - SSL-Inspection
- Routage mail avec antispam et antivirus (sandboxing inclus)
  - Antispam / Antipishing et quarantaine management delegation
  - Deux couches de routage mail interne / externe
  - Sandboxing (Advanced Threat Protection)
- VPN (Virtual Private Network) pour un accès à distance avec "advanced identity management" et "compliancy check"

Services complémentaires :

- Site-to-site VPN
- Application Delivery Control (ADC) avec SSL offload et web-app security
- Connectivity et IP compliancy management (NAT). Chaque institution peut prendre des mesures complémentaires pour relier les services à IAP et les sécuriser en interne. Les spécialistes sécurité et réseau du G-Cloud peuvent vous aider et vous conseiller dans ce cadre.

Service owner

BCSS – Jean Jochmans – iap@gcloud.belgium.be

Service level agreements

- Disponibilité : 99,9 %
- Performance : connexion internet < 10ms
- Fenêtre de service : 24/7
- Fenêtre de support : 24/7
- Support 1ère /2e ligne : G-Cloud Frontoffice (frontoffice@gcloud.belgium.be)
- Support 3e ligne : Network Infra Team et autres équipes
- Installation : 2 semaines de travail

Tarifs

Les coûts sont facturés suivant le principe "pay per use".

Quelle est l'évolution prévue pour ce service ?

Les dangers d'internet évoluent en permanence. Le service IAP doit y réagir avec souplesse par une quête continue de l'amélioration.
Des "Technical User Boards" ont lieu régulièrement pour permettre aux membres d'échanger leurs expériences et leurs besoins, ainsi que de discuter de l'évolution technique.

Infos pratiques

Plus d'infos via iap@gcloud.belgium.be

Nom du service G-Cloud

Security as a Service ***01-01-2020***

Description du service G-Cloud

G-Cloud *Security as a Service* inclut aussi bien la protection d'internet que la protection des terminaux internes via une sécurisation basée sur les flux et sur les hôtes. Ce service sécurise le trafic sur toutes les couches du réseau, depuis le LAN jusqu'à internet.

Il englobe le matériel, les licences, l'installation, la migration, la maintenance, la gouvernance, l'assistance CSOC, l'audit, la formation, l'analyse de vulnérabilité, le test d'intrusion et la veille technologique.
Grâce à ces services, l'information transitant entre les utilisateurs et les serveurs via LAN, Wireless LAN, private WAN, internet public et le réseau mobile public est sécurisée.
Security as a Service est un service de gestion des risques qui comprend un ensemble de services de gouvernance de la sécurité avec une infrastructure sous-jacente, comme un registre des risques et le suivi des risques potentiels détectés.

Security as a Service peut être considéré comme une infrastructure partagée pour les services publics fédéraux permettant aussi bien de prévenir et de détecter les incidents de sécurité que d'y réagir et de les anticiper. Les deux aspects sont donc présents : une prévention "state of the art" et une réaction rapide en cas d'incident.

Ce service est basé sur les services de sécurité de Proximus dans le cadre d'un cahier des charges du SPF Finances.

L'infrastructure de sécurité est installée dans les data centers du G-Cloud utilisés par le SPF Finances, à l'exception des plateformes de management de Proximus et d'un certain nombre de services externes DNS/Mail security/DDoS et SIEM.

Le package de base comporte les éléments suivants :

- Installation et assistance au démarrage
- Migration de l'infrastructure existante
- Mise en place du Security Operation Center (SOC)
- Raccordement des réseaux internes et externes et des serveurs à la DMZ
- Sécurité externe
    - Couche pare-feu à double redondance
    - Définition et sécurisation des DMZ
    - Priorisation des flux de données
    - Priorisation de certaines URL
    - Support des réseaux physiques et virtuels
    - Intégrité du trafic web
    - Exclusion de sites web indésirables
    - Site-to-site VPN
    - Détection et prévention de l'intrusion
    - Sécurité basée sur l'hôte
    - Intégrité du trafic de messagerie électronique
    - Antispam et antiphishing

  - Système DNS sécurisé
  - Contrôle sur demande de la présence de malware dans les fichiers
  - Web Application Firewall
  - Sandboxing
  - Advanced Malware protection
  - Advanced Threat protection
  - Distributed Denial Of Service (DDOS) protection - Application based
  - Application control
  - Botware protection
  - Data leakage protection
  - Antivirus protection
  - Compliancy check
  - SSL inspection
  - Surf protection & control
  - Identity awareness
- Sécurité interne
  - Load balancing + Web App Protection
  - Secure messaging with malware / ransomware protection
  - Managed Security Services and Security Operations Center (SOC)

Les options supplémentaires disponibles sont :

- Accès à distance pour les collaborateurs, gestionnaires IT et partenaires avec support des cartes d'identité eID belges, cartes CAC (Common access card), tokens électroniques et OTP (One-time password)
- End point Software Security Agent
- Mobile Device Protection (VPN)
- Remote SSL server
- Network Access Control (NAC)
- IP address management, DNS, DHCP
- Advanced security for end-points
- Security Information & Event Management (SIEM) Surveillance du réseau interne
- DDOS protection and volume based attacks protection
- CSIRT-services (Computer Security Incident Response Team)
- Services Security & GDPR compliancy
  - Vulnerability Management
  - Vulnerability Automatic Assessment & VAM
  - Asset & Lifecycle management
  - Cyber threat feeds
  - Service quality survey & management
  - Technology survey & best practice recommandations
  - Security Awareness
  - Management report
  - Regular Pentesting & compliance audit

Service owner

SPF Finances - Frank Van De Heijning - secaas@gcloud.belgium.be

Service level agreements

- Disponibilité : 99,9 %
- Performance : connexion internet < 50ms
- Fenêtre de service : 24/7
- Incident response time : dans l'heure pour Priority 1
- Incident resolution time : 2 heures
- Clause de pénalité : max. 6,5 % de la redevance sur la base des chiffres mensuels de disponibilité
- Support 1ère/2e ligne : Proximus
- Support 3e ligne : Proximus
- Installation : 2/3 mois

Tarifs

- Pas d'investissement "upfront" nécessaire, uniquement une redevance mensuelle (HW, SW et services compris)
- 2 grands modules : Basic + options
- Prix fixe par utilisateur par an (par bloc de 100 utilisateurs)

Quelle est l'évolution prévue pour ce service ?

- Le service suivra les évolutions et améliorations apportés au produit par le fournisseur pendant la durée du contrat. Le contrat permet d'exécuter des évolutions technologiques ainsi que des modifications de produit.

Infos pratiques

- Contrat-cadre disponible pour tous les SPF pour une période de 7 ans (accès pendant les 4 premières années)
- Accès avec une durée minimale de 3 ans