Segurança

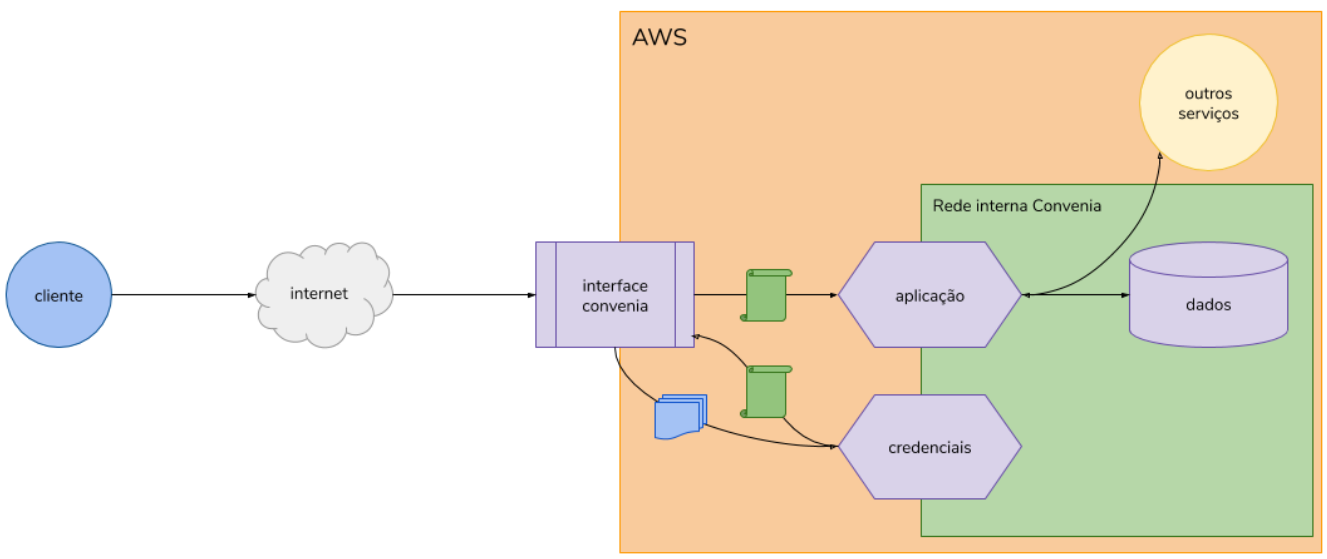
Versão 1.0.0

Introdução

Este documento apresenta uma visão superficial sobre nossa infraestrutura de maneira a clarificar para o cliente Convenia as medidas de segurança que tomamos para garantir a integridade das informações de sua empresa e colaboradores.

Vale ressaltar que este não é um laudo técnico e tem caráter informativo.

Acesso Externo



Contexto

As aplicações da Convenia são softwares de natureza Web (Cliente - Servidor), executados em navegadores de internet que acessam dados através de Interface de Programação de Aplicação (API no termo em inglês). O acesso aos dados e operações se dão pela API. O acesso a mesma é controlado via credenciais de acesso (tokens). Não é possível ter acesso direto ao banco de dados externamente.

Comunicação

A comunicação liberada para acesso é regida pelo protocolo HTTPS, largamente usado na internet. Este protocolo garante que os dados entre as pontas (Cliente e Convenia) são criptografados e somente elas têm acesso ao conteúdo.

Credenciais

Para acessar a interface gráfica dos sistemas Convenia não é necessário nenhuma credencial.

Para que a interface acesse os dados de aplicação é necessária uma credencial obtida com a entrada de usuário e senha a partir da tela de autenticação (login). Tendo uma credencial válida, a interface pode consultar os dados da aplicação referentes a sua identidade. O mesmo é válido para a API Pública, que somente dá acesso aos dados mediante chaves de acesso previamente cadastradas.

Credenciais (Infra)

Os acessos aos servidores da Infra, Banco de Dados e segredos de ambiente são restritos ao time de SRE, Tech Lead e CTO.

O Dev Team possúi seus próprios ambientes de testes (Sandbox)

Utilizamos também o AWS IAM para controle de acesso específico para aplicações e pessoas.

Fronteira

O acesso via internet limita-se ao protocolo HTTPS e apenas a alguns servidores e serviços. O acesso a rede interna é somente disponível via Rede Privada Virtual (VPN) a um grupo restrito de pessoas, responsáveis pela manutenção deste ambiente.

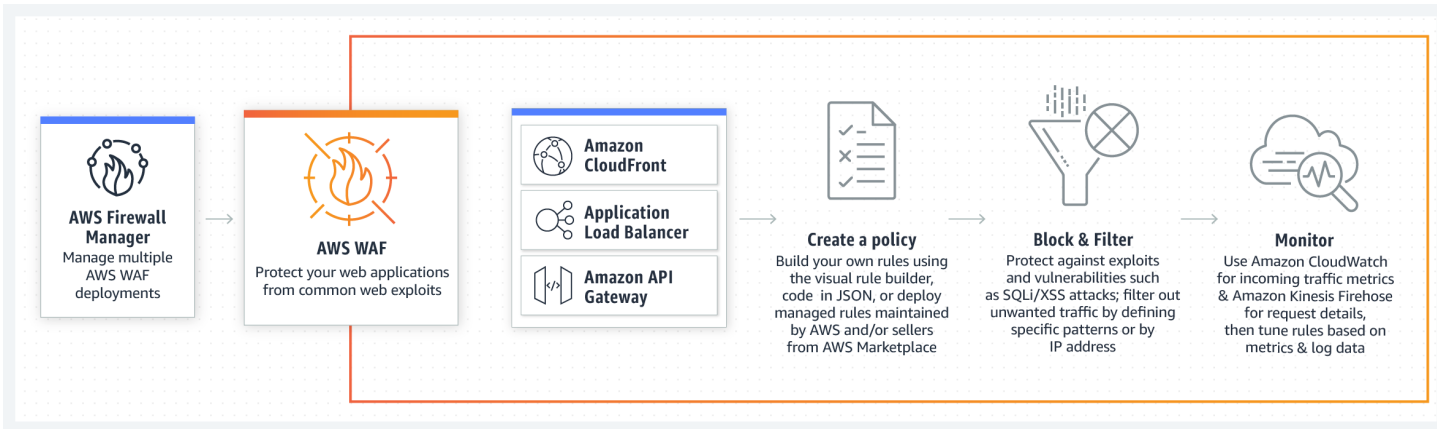
Controle de Vulnerabilidades

Snyk: Analisa vulnerabilidades no ambiente, pacotes instalados nos projetos PHP, Node e Containers.

Infraestrutura

Ambiente de Nuvem: *AWS*

- EC2: Servidores de aplicação
- S3: Armazenamento
- CloudFront: CDN & SPAs
- CloudWatch: Monitoramento
- RDS: Banco de dados
- Route53: DNS
- ElastiCache: banco de dados chave-valor
- Lambda: Funções específicas
- WAF: Firewall de aplicação Web (ModSecurity)
- IAM: Controle de Acesso



Sistema operacional

- Ubuntu

Servidores

- Web: Nginx + ModSecurity & Core Rules Set
- Sistemas: PHP, Laravel
- Processos FastCGI: PHP-FPM
- RabbitMQ (CloudAMQP)

Bancos de Dados

- MySQL
- MongoDB
- ElastiCache (Redis)

Armazenamento

- S3 (Default e Glacier)

Monitoramento

- Registros das Aplicações: Datadog
- Saúde das Aplicações (APM): New Relic
- Saúde dos sistemas: Zabbix
- Dashboard com Grafana, capturando dados do Zabbix, CloudWatch e Prometheus

Backup

Dump: *S3*

Periodicidade	Retenção
3h	6 meses

Snapshot: *RDS*

Periodicidade	Retenção
24h	7 dias

Recuperação

Nosso ambiente está roteirizado de maneira que, caso haja a necessidade, possamos recriá-lo fiel e rapidamente. Utilizamos a ferramenta Terraform para tal.

Podemos recriar nosso ambiente nos seguintes casos:

- Indisponibilidade da região AWS
- Necessidade específica de cliente
- Troca de região
- Troca de fornecedor de Nuvem

Rotina de atualização

Nossos sistemas utilizam sempre a versão mais recente, com suporte estendido, de plataforma disponível. Assim temos atualmente:

- **Sistema operacional base**: Ubuntu
- **Sistema operacional de imagens docker**: Alpine
- Plataforma de execução
    - Legado: PHP
    - Core: PHP
    - Outros: Node
        - Atualização mensal

Atualizações não programadas em caso de relatório urgente de segurança CVE

Serviços externos

O Convenia utiliza-se de serviços especializados em algumas áreas de maneira a oferecer uma melhor experiência para os clientes. Dentre os serviços estão:

- Vindi: Cobrança
- AWS: Armazenamento de arquivos
- Symfony: Checagem de vulnerabilidades
- CloudAMQP: Mensageria
- Atlas: Serviço de dados
- NPM e Packagist: descoberta de pacotes
- Github e Gitlab: Código fonte

Desenvolvimento

O Convenia utiliza-se das versões de suporte estendido mais recentes das ferramentas de desenvolvimento que compõe o sistema.

- PHP
    - Plataforma base, presente em mais de 80% de sistemas na internet.
- Laravel
    - Arcabouço de aplicações que provêm base sólida para o desenvolvimento
- Vue.js
    - Biblioteca de recursos para o cliente web (navegador) provendo as melhores práticas de performance e segurança

O uso de nossas APIs privadas é restrito aos usuários cadastrados de nossos clientes, mediante autenticação realizada em nossa camada de apresentação. Um token JWT (Json Web Token) é atribuído a esta sessão, e que limita o que o usuário autenticado pode, ou não, fazer.

O framework Laravel garante algumas proteções de ataques web, tais como SQL Injection, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), etc.

O desenvolvimento das funcionalidades também é feito de maneira que um usuário só possa acessar ou modificar conteúdo para o qual tenha sido contextualizado via configuração. Há pelo menos quatro sistemas entre a interface web e o banco de dados - quando é comum que exista apenas um sistema entre o usuário e o banco de dados

Last modified 3 November, 2020