fSense Arquitetura

Sumário:

fSense Documento de Arquitetura

Este documento esclarece aspectos técnicos da solução fSense, destina a profissionais de TI, como arquitetos de sistemas, especialistas em infraestrutura, redes e afins. Apresentamos a arquitetura do sistema, seus componentes principais e aspectos de segurança.

Arquitetura

A arquitetura do fSense é composta por quatro componentes principais:

- ### Admin (Sistema Web):

  Interface web centralizada para administração do fSense.

  - Armazena e processa informações coletadas.
  - Exibe gráficos interativos, relatórios e ferramentas de configuração.
  - Processa solicitações do usuário e oferece análise em tempo real.

- ### Agente Desktop

  Aplicativo cliente instalado nas estações estação de trabalho.

  - Captura eventos do usuário (sites, programas acessados) e realiza capturas de tela periódicas.
  - Envia os dados coletados para o Agent API.
  - Opera de forma discreta para garantir um experiência de usuário não intrusiva.

- ### Agent API (Backend):

  API REST responsável pelo processamento das informações.

  - Recebe e processa eventos e screenshots do Agente Desktop.
  - Realiza o tratamento dos dados para extrair informações relevantes.

- Armazena os dados processados no banco de dados.
- Gerencia a comunicação entre o Admin, Agente Desktop e Integration API.

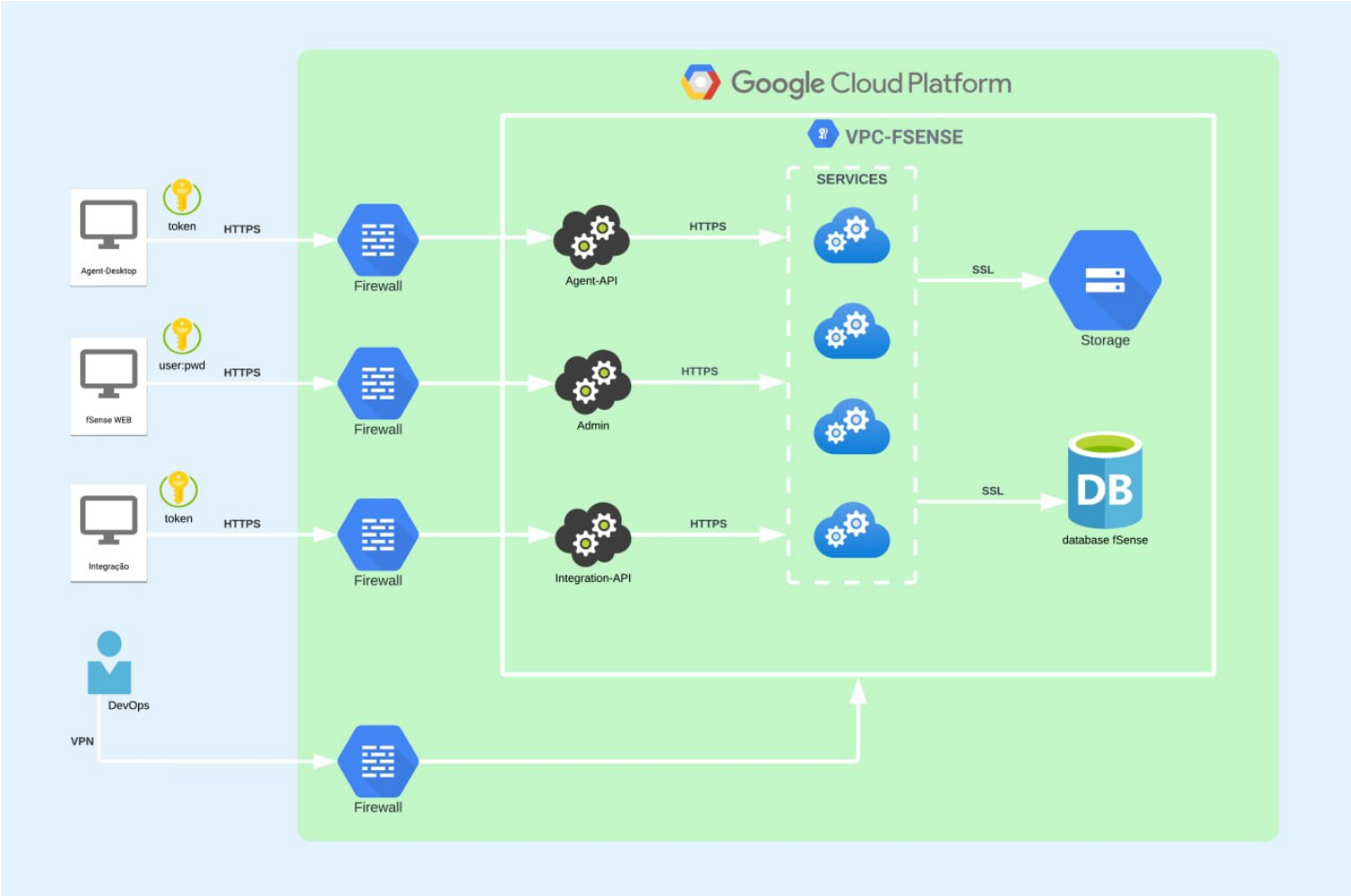
- ## Integration API:
  - A Integration API é o componente dedicado que fornece uma API REST para facilitar os serviços de integração com fSense.

Infraestrutura

- ## VPC (Rede Virtual Privada)

  A arquitetura é implantada em um VPC no Google Cloud Platform(GCP) garantindo isolamento e segurança.

  - **Sub-redes:** são configuradas para separar os componentes do sistema.
  - **Instâncias Virtuais:** O Admin é implantado em instância escalável para lidar com cargas variáveis de requisições. O AgentAPI é implantado em instâncias dedicadas e otimizadas para processamento de dados em tempo real.
  - **Banco de Dados:** O Banco de Dados é configurado com backups automáticos e monitoramento contínuo para garantir a integridade e disponibilidade dos dados.



Segurança dos Dados

- ## Agent-Desktop

  - **Assinatura Digital:** A aplicação possui assinatura digital através de um certificado digital classe 3 (Code Signing). Ao assinar um arquivo com uma assinatura digital, é possível garantir a sua procedência e que o mesmo não foi alterado nem corrompido por terceiros.

  - **Comunicação Segura:** A comunicação entre o agente-desktop e o servidor é realizada através do protocolo HTTPS, uma implementação do protocolo http sobre o protocolo SSL/TLS, garantindo a criptografia dos dados enviados/recebidos pelo servidor não podendo ser visualizadas ou decodificas por terceiros.

- **Autenticação:** A autenticação entre agent-desktop e o servidor são feitas através de oauth2 onde é retornado um token com expiração programada, e todas as comunicações são autenticadas através desse token.

- **Comunicação Restrita:** O Agente Desktop comunica-se exclusivamente com os servidores do fSense, não havendo integração com serviços de terceiros.

Admin

- **Comunicação Segura:** A comunicação é realizada através do protocolo HTTPS, uma implementação do protocolo http sobre o protocolo SSL/TLS, garantindo a criptografia dos dados enviados/recebidos pelo servidor não podendo ser visualizadas ou decodificas por terceiros.

- **Acesso Seguro:** O acesso ao sistema é realizado através do mecanismo de login e senha, definidos pelo próprio usuário. Os dados sensíveis à conta, como senha de acesso, são armazenados de forma criptografada com algoritmo one-way, não podendo ser revertidos. Os dados da conta não podem ser acessados por contas de terceiros.

API’s REST Agent-API e Integration-API

- **Comunicação Segura:** A comunicação é realizada através do protocolo HTTPS, uma implementação do protocolo http sobre o protocolo SSL/TLS, garantindo a criptografia dos dados enviados/recebidos pelo servidor não podendo ser visualizadas ou decodificas por terceiros.
- **Autenticação:** A autenticação é feita através de oauth2 onde é retornado um token com expiração programada, e toda a comunicação e autenticada através desse token.

Banco de dados

- **Armazenamento de Dados:** São armazenadas apenas informações sobre a iteração do usuário com os aplicativos (eventos de foco, cliques, alternância entre janelas,

sites acessados etc).

- **Backups Diários:** São realizados Backups diários do banco de dados do sistema, esses backups são armazenados na própria nuvem, por um período de 7 dias, não sendo possível acesso externo a esses backups.
- **Monitoramento:** Os serviços de banco de dados são monitorados 24 horas por dia, 7 dias por semana para que não haja nenhum tipo de indisponibilidade no sistema.

Compliance

Utilizamos serviços de segurança fornecidos pelo nosso provedor de nuvem. Para mais informações acesse o link:

https://cloud.google.com/security/compliance/compliance-reports-manager?hl=pt-br