



# Security Services

## Cloud Security Services

Center of Electrical Engineering and Informatics  
Federal University of Campina Grande



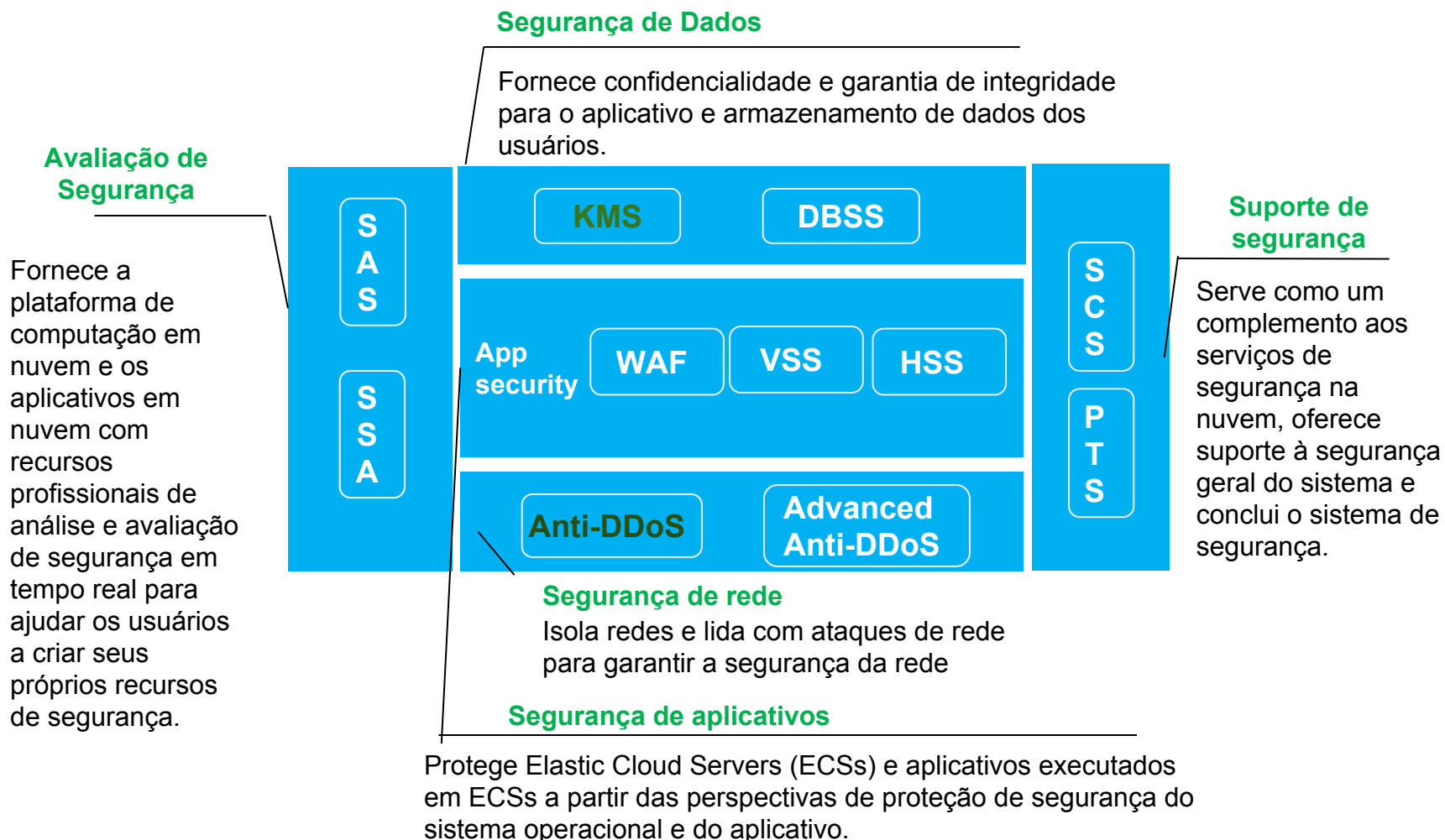
- Introdução
- Principais Serviços

- Na computação em nuvem, os dados e serviços geralmente são terceirizados, o que traz novas preocupações de segurança
  - Por "**terceirização de dados**", os dados são produzidos, usados, armazenados e apagados em sistemas remotos, o que significa que os usuários perdem o controle sobre seus dados, causando problemas de proteção de dados e privacidade
  - Por "**fornecimento de serviços**", os serviços de aplicativos são implantados em sistemas remotos, o que significa que os usuários perdem o controle sobre os recursos físicos, causando problemas de segurança nos aplicativos em nuvem

- Confidencialidade, integridade e disponibilidade ainda são os requisitos de segurança da computação em nuvem
  - Por "**confidencialidade**", os sistemas de computação em nuvem devem ser capazes de proteger os dados dos usuários
  - Por "**integridade**", os sistemas de computação em nuvem devem ser capazes de impedir a falsificação, adulteração e exclusão não autorizada de dados e serviços
  - Por "**disponibilidade**", os dados devem permanecer disponíveis e os aplicativos em execução quando os sistemas de computação em nuvem estiverem sob ataques

- Os serviços de segurança em nuvem devem fornecer soluções de segurança completas
  - Os serviços de segurança na nuvem devem proteger os dados durante todo o seu ciclo de vida
  - Os serviços de segurança na nuvem devem proteger os ambientes em execução (aplicativos, sistemas e redes) para aplicativos
  - Um serviço deve ser capaz de funcionar de forma independente e trabalhar em conjunto com outros serviços
  - Serviços de análise e avaliação de segurança devem ser fornecidos para que os usuários saibam qual produto escolher
  - Os serviços de segurança não são responsáveis pela segurança da plataforma de computação em nuvem

- Introdução
- Principais Serviços

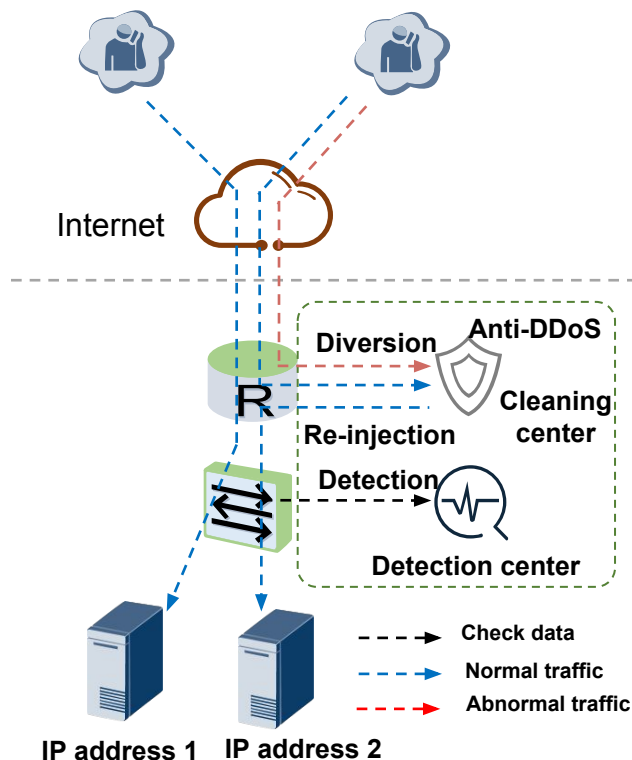


- O Anti-DDoS é um serviço de limpeza de tráfego que protege recursos (como ECSs e instâncias de ELB) contra ataques DDoS em camada de rede e aplicativos
  - Ele notifica os usuários sobre ataques detectados instantaneamente, melhora a utilização da largura de banda de maneira eficaz e garante a execução estável e confiável de serviços
- Funções principais
  - Filtrar pacotes mal formados e pacotes de sonda
  - Defender-se contra ataques baseados em transmissão de rede
  - Evitar ameaças na camada de aplicativos
  - Exibir tendências de ataque e relatórios de tráfego
- Cenários de aplicação
  - Websites
  - Jogos



Fornece serviços de prevenção de DDoS altamente confiável e seguro que pode ser usado sob demanda e escalonados com flexibilidade. Isso ajuda a garantir o funcionamento contínuo dos ECSs.

## Arquitetura de implantação e princípio de funcionamento



O equipamento anti-DDoS é implantado em entradas e saídas de rede.



O centro de detecção verifica o tráfego de acesso com base nas políticas configuradas pelo usuário.



Quando um ataque é detectado, o tráfego é desviado e limpo no centro de limpeza. Tráfego limpo é encaminhado.

## Tipos de ataques que podem ser evitados

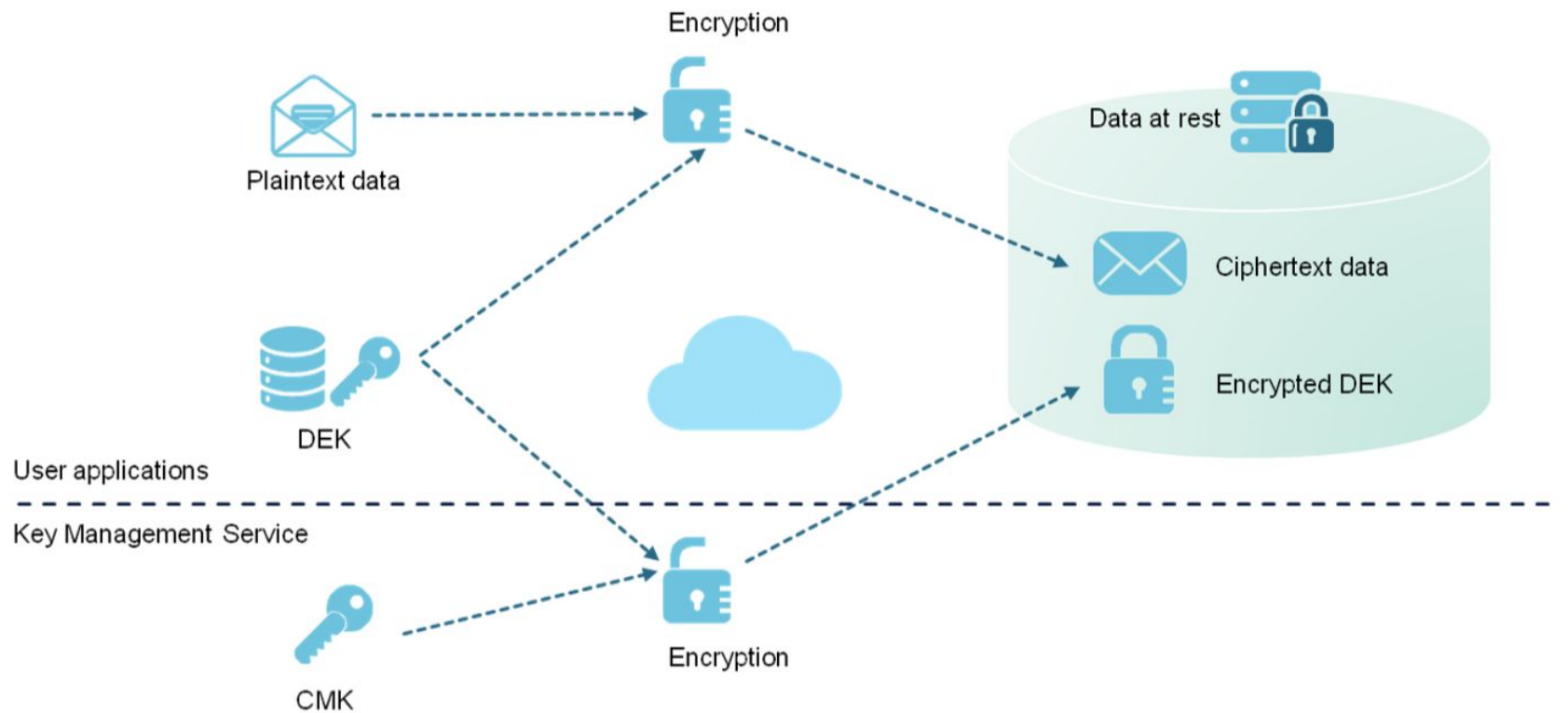
1. **Ataques de tráfego:** flood de SYN, flood de SYN-ACK, inundação de ACK, flood de FIN / RST, flood de UDP, flood do fragmento do IP, e flood do Stream
2. **Ataques de aplicativos:** ataque CC, proteção de URL, flood de conexão, flood HTTPS, flood HTTP Get e flood HTTP Post

## Capacidade

1. Capacidade de proteção  $\geq 2$  Gbit / s
2. Latência de transmissão  $\leq 30$  ms
3. Conexões recém-criadas por segundo  $\geq 100.000$

- O KMS é serviço seguro e fácil de usar que usa Módulos de Segurança de Hardware (HSMs) para proteger suas chaves
  - Ele interage perfeitamente com outros serviços para proteger dados de serviço e pode ser usado para desenvolver aplicativos de criptografia
- Funções principais
  - Gerenciamento de CMK (Customer Master Key)
  - Funções relacionadas a DEK (Data Encryption Keys)
  - Criptografia direta
  - Número aleatório de hardware
- Cenários de aplicação
  - Object Storage Service (OBS)
  - Elastic Volume Service (EVS)
  - Criptografia de arquivos locais
  - Congelamento de dados(Data freezing)

# Key Management Service

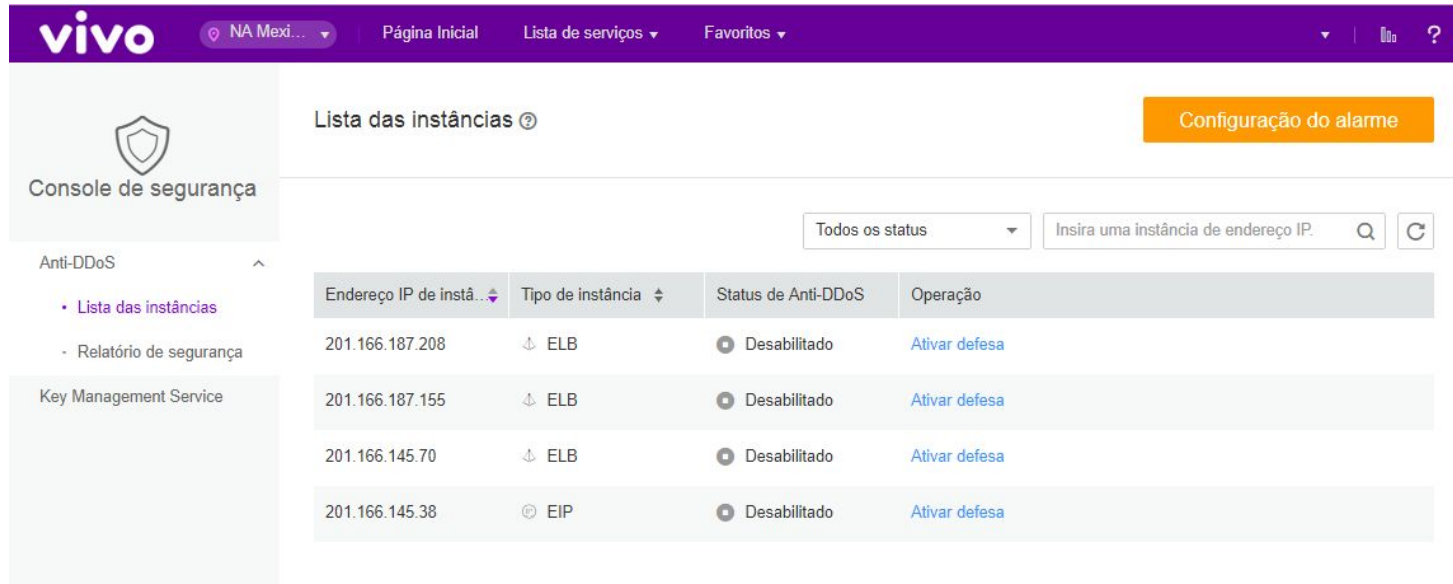


- Anti-DDoS avançado
  - Melhorias e mais opções que o Anti-DDoS padrão
- WAF(Web Application Firewall)
  - É habilmente projetado para manter seu site seguro e protegido
- Vulnerability Scan Service (VSS)
  - Examina servidores e sites para detectar vulnerabilidades e possíveis riscos de segurança

- Host Security Service (HSS)
  - Projetado para melhorar a segurança geral dos hosts
- Database Security Service (DBSS)
  - Serviço de proteção de banco de dados inteligente
- Security Situation Awareness (SSA)
  - Baseado em tecnologias de big data mining e machine learning
- Security Assessment Service (SAS)
  - Serviço profissional prestado conjuntamente pela Huawei e uma autoridade de segurança da informação
- SSL Certificate Service (SCS) and Penetration Testing Service (PTS) foram removidos do portfólio

# Configurar o Anti-DDoS

- Para configurar é necessário possuir um EIP
- O envio de mensagens pelo cloud-eye é opcional



Lista das instâncias

Configuração do alarme

Todos os status

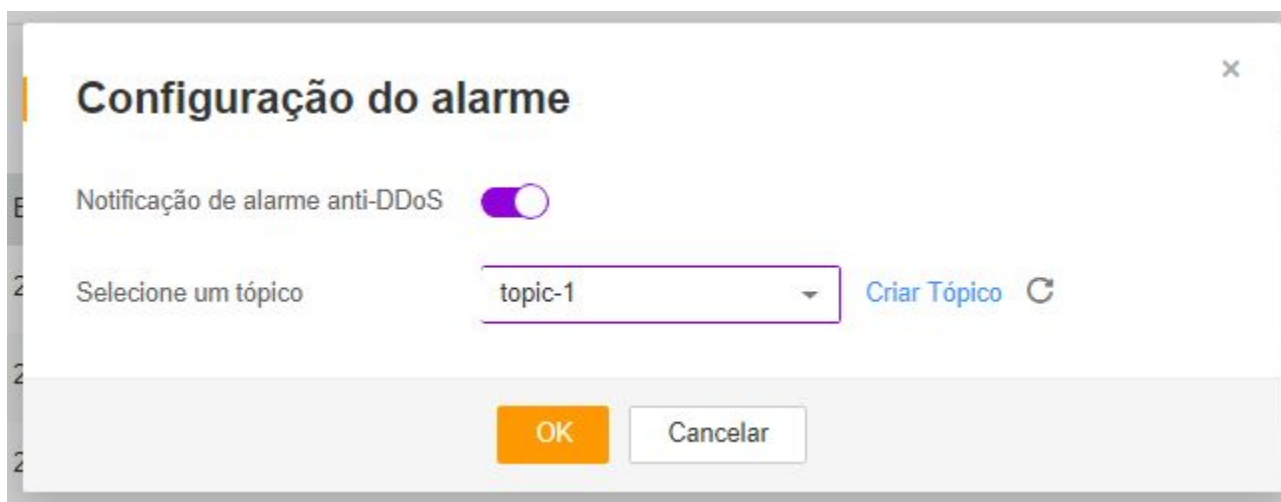
Insira uma instância de endereço IP.

Endereço IP de instância	Tipo de instância	Status de Anti-DDoS	Operação
201.166.187.208	ELB	Desabilitado	<a href="#">Ativar defesa</a>
201.166.187.155	ELB	Desabilitado	<a href="#">Ativar defesa</a>
201.166.145.70	ELB	Desabilitado	<a href="#">Ativar defesa</a>
201.166.145.38	EIP	Desabilitado	<a href="#">Ativar defesa</a>

# Ativar as notificações do Anti-DDoS



- Após as definições de alarme serem configuradas, sempre que houver uma tentativa de ataque, o tópico selecionado será informado



**Configuração do alarme** ×

Notificação de alarme anti-DDoS ☒

Selecione um tópico topic-1 ▼ [Criar Tópico](#) ↺

OK Cancelar

# Ativar a proteção do Anti-DDoS

- Para ativar a proteção basta escolher o EIP na lista de instâncias, e clicar em habilitar proteção

## Ativar defesa

Limite de limpeza de tráfego  ⓘ

Defina um valor do parâmetro sobre a base do tráfego do serviço. É aconselhável o valor definido não ultrapassar a largura de banda comprada.

Defesa CC ☐ Desabilitar ☒ Habilitar

taxa de solicitação HTTP  ⓘ

Defina um valor do parâmetro sobre a base do tráfego normal do sítio web. Se o valor for demasiado grande, o tempo de defesa contra os ataques CC poderia se atrasar.



- Para acompanhar o registros do anti-ddos, clique em **Exibir relatório** no EIP da lista de instâncias

## Relatório de monitoramento



Seu ECS 201.166.145.38 está protegido contra ataques de tráfego pelo Anti-DDoS.

Duração do monitoramento 09/28/2018 09:39:45 GMT-03:00 – 09/29/2018 09:34:45 GMT-03:00

Defesa CC Habilitado

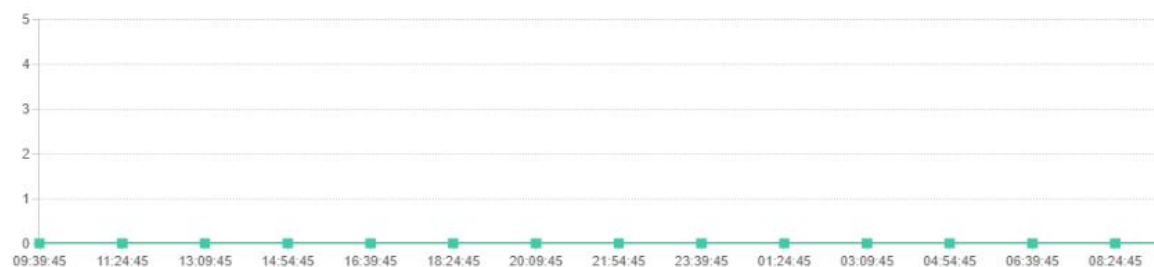
Limite de limpeza limite de limpeza de tráfego:10 Mbps; solicitações HTTP por segundo:100 qps

Configurações de segurança

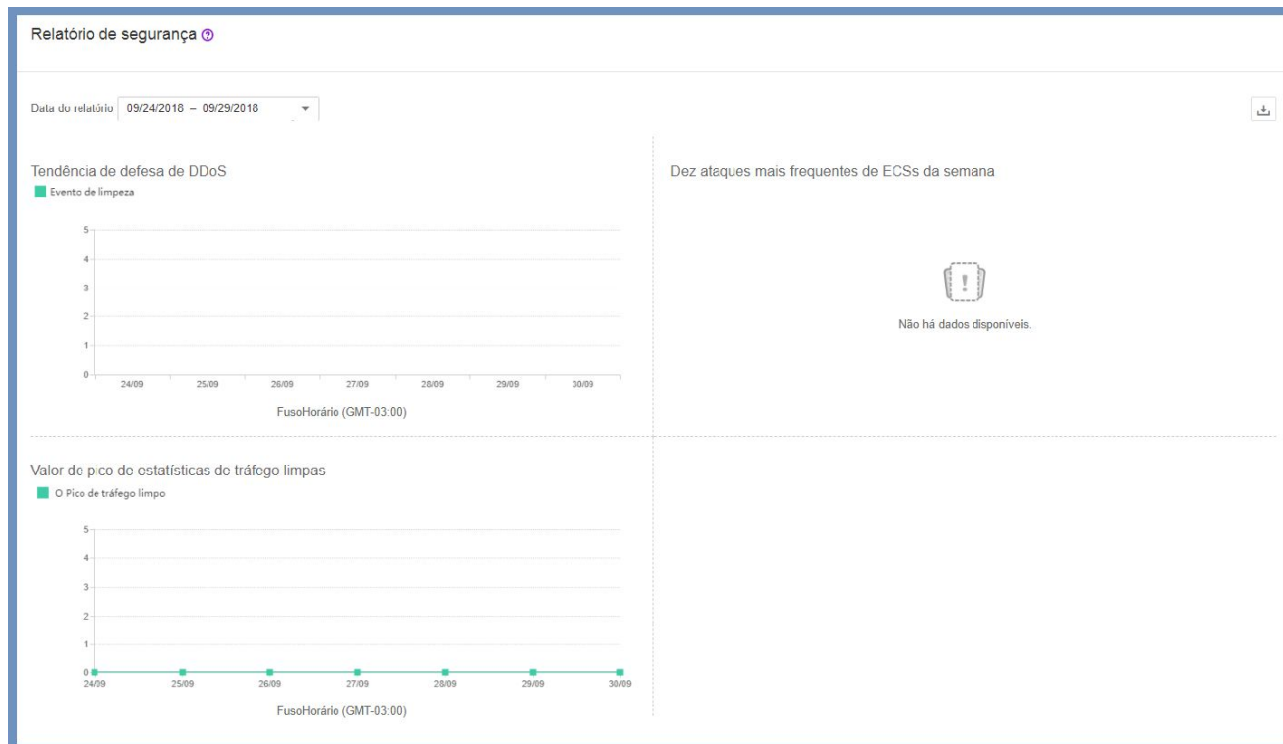


Tráfego (Kbps) Pacotes por segundo (pps)

Tráfego de entrada de ataque Tráfego de entrada normal



- Também é possível obter mais detalhes na aba **Relatório de segurança**



- Ativar o Anti-DDoS para cada EIP
- Página Inicial > Segurança Anti-DDoS
- Console de segurança > Anti-DDoS > Lista das instâncias
- Escolher o EIP > Ativar defesa
- Informar as configurações necessárias



## Contact

### **Angelo Perkusich, D.Sc.**

Professor, CEO

[angelo.perkusich@embedded.ufcg.edu.br](mailto:angelo.perkusich@embedded.ufcg.edu.br)

+55 83 8811.9545

### **Hyggo Almeida, D.Sc.**

Professor, CTO

[hyggo.almeida@embedded.ufcg.edu.br](mailto:hyggo.almeida@embedded.ufcg.edu.br)

+55 83 8875.1894

### **Rohit Gheyi**

Professor, Program Manager

[rohit.gheyi@embedded.ufcg.edu.br](mailto:rohit.gheyi@embedded.ufcg.edu.br)

+55 83 8811 3339

