

### 3.6 Desvio de tráfego e Mitigação Automática

Tráfego anômalo com característica TCP SYN, identificado no alerta ID 2523800, com o propósito de validar os seguintes questionamentos:

#### Desvio de tráfego anômalo e mitigação de forma automática

Resposta: A solução está configurada de forma automática, assim que inicia um tráfego anômalo, após de alguns minutos, já é possível acompanhar os gráficos que demonstra:

- Tráfego em vermelho para o TMS (mitigador) em ação de forma automática sem ação humana.
- Tipos de ataques identificados, volume do tráfego anômalo em Gbps e pps mitigados entre outras.

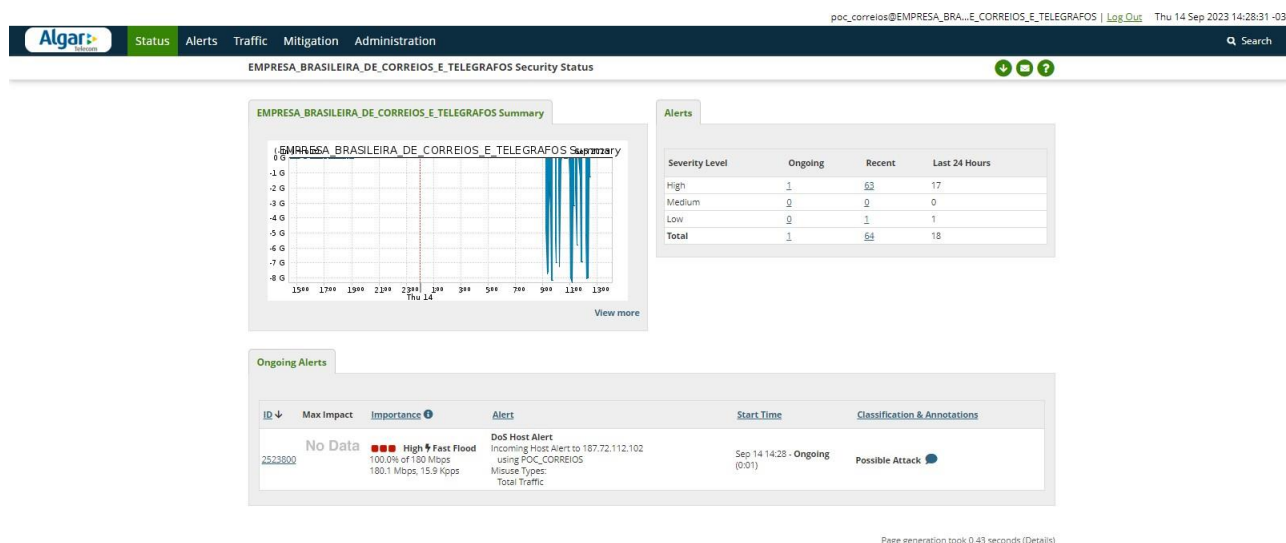


Figura 15 – Identificação do alerta 2523800

#### Endereço de armazenamento eletrônico

Cabe ao usuário a responsabilidade em utilizar e controlar a revisão deste documento em papel. O presente material é de propriedade da Promonlogicalis e qualquer reprodução, utilização ou divulgação do mesmo, sem a prévia e expressa autorização da titular, importa em ato ilícito nos termos da legislação pertinente, através da qual serão imputadas as responsabilidades cabíveis.