

### 3.7.1 Black Lists

Tráfego anômalo com característica TCP SYN, identificado no alerta ID 2523800, com o propósito de validar o seguinte questionamento:

**Deny/Allow Lists, considere IP ofensor seja bloqueado com pacotes maliciosos, e o mesmo IP ao fazer uma requisição com pacotes validos a solução deve deixar passar o tráfego valido.**

Resposta: para esse teste foi desabilitado a função Deny/Allow Lists, assim conseguimos gerar ambas as requisições e evidenciar o cenário proposto.

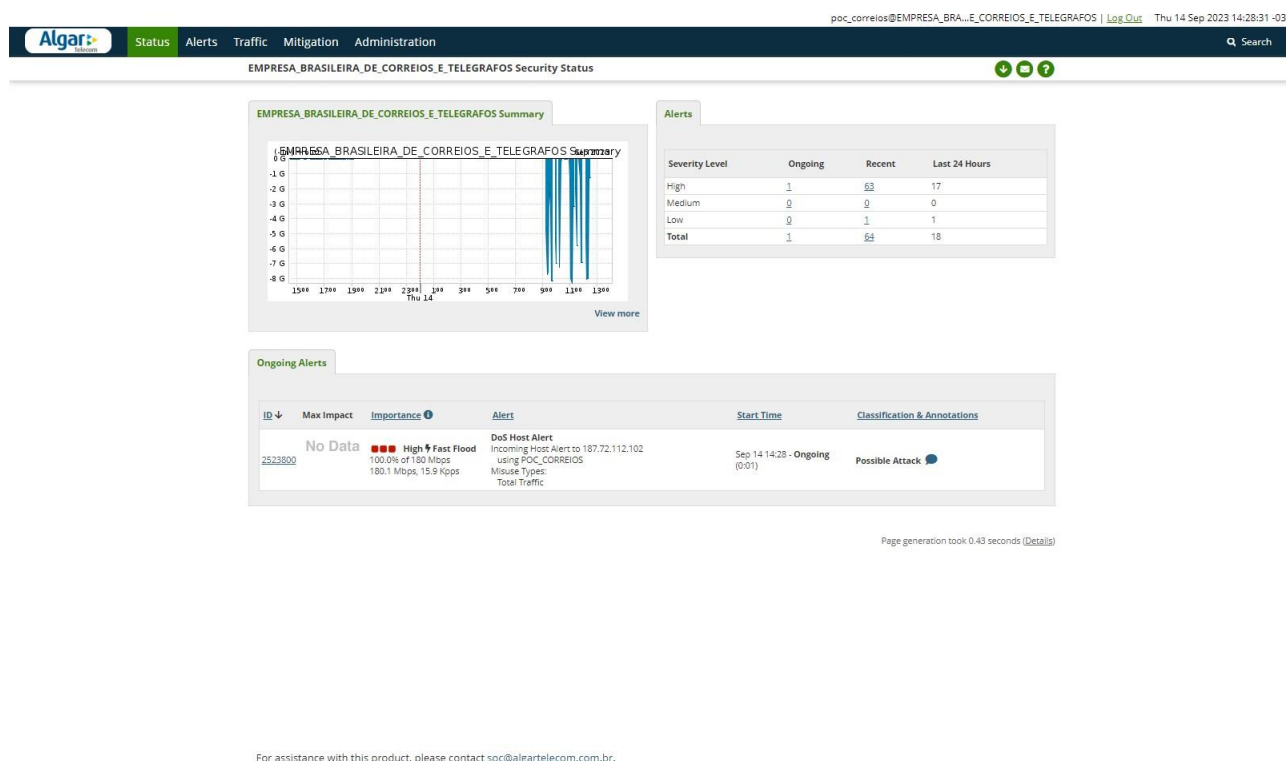


Figura 15 – Identificação do alerta 2523800

#### 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.