Dashboards Netflow

Ajustes / Melhorias

- Anomalias
  - Atualmente atende o seu propósito, podemos apenas pensar em uma reestruturação dos dados exibidos.
- Blocos
  - Sugestão: Permitir a seleção de um bloco e adicionar segmentação por conteúdo.
- Consumo por protocolo
  - Apenas renomear para Consumo aplicações
- Exportadores
  - Sugestão: Adicionar informações de interface de entrada e de saída.
  - OBS: aplicando essas melhorias a dash Análise de ASN teria informação redundante dessa dashboard.
- Fluxos por protocolo
  - Sugestão: eliminar o PIE chart que exibe o volume por IP e adicionar um gráfico de série temporal para exibir o histórico por protocolo. Também renomear a mesma para Tráfego / Consumo por protocolo
- Tráfego de CDN.
  - Renomear para Peering (ou algo que se aplique melhor) e adicionaria uma variável para seleção de quais conteúdos exibir.
- Tráfego por conteúdo
  - Essa será trabalhada a parte de dados como são armazenados direto no banco para identificar quem é o ASN que está gerando o conteúdo de CDN.

Eliminação

- Análise de ASN
  - Atualmente exibimos informação redundante na dashboard Exportadores.
- Geolocalização
  - Ela sozinha não agrega valor, mas pode ser utilizada como complemento de outras dashboards.
- Top tráfego por conteúdo
  - Exibe a mesma informação da dashboard Tráfego de CDN.
- Tráfego por bloco ip4 e ipv6 (duas dashboards)
  - Tem informação redundante já exibido na dashboard Blocos (porém essa possui mais informações).
- Top N-Flows
  - Proposta de substituição pela dashboard DDoS Detect.

- Resumo Geral da Rede [VISÃO GERAL]
  - Objetivo: Oferecer uma visão panorâmica de toda a rede, incluindo os principais ASNs, protocolos e interfaces. Este dashboard é ideal para executivos e líderes técnicos que buscam um resumo claro e estratégico do ambiente.
  - Informações: Uso total de banda, principais ASNs, top protocolos, anomalias (de uma forma geral).

- Detecção de Anomalias de Tráfego
  - Objetivo: Identificar e alertar sobre padrões de tráfego incomuns, como picos abruptos ou uso fora do esperado, que podem indicar problemas de configuração ou ataques à rede. Esse dashboard oferece insights valiosos para fortalecer a segurança e evitar interrupções.
  - Informações a exibir: Volume de Tráfego (Mbps ou GB), número de pacotes por segundo (PPS), top IPs de origem e destino (em tráfego anômalo), ASNs envolvidos, taxa de latência, distribuição geográfica, gráfico de tráfego por horário (para localizar o momento exato da anomalia)
  - Filtros: exportador/caixa, período (intervalo de tempo), ASN, IP de origem/destino, interface, protocolo, país/região, tipo de tráfego (entrada ou saída).
- SUGESTÃO PARA DASH:
  - Gráfico de Linhas: Volume de tráfego ao longo do tempo com destaques de picos.
  - Tabela: Listagem de top IPs, ASNs, ou protocolos anômalos.
  - Mapa Geográfico: Exibir origens/destinos de tráfego suspeito.
  - Painéis de Alertas: Exibir notificações visuais sobre limites excedidos.
  - Gráfico de Barras: Protocolo mais utilizado durante as anomalias.

- Análise de Tráfego por IP
  - Objetivo: Oferecer uma visão detalhada do tráfego gerado por endereços IP individuais na rede, destacando os principais consumidores de banda e suas contribuições ao volume total de dados. Este dashboard é ideal para diagnosticar atividades anormais, como picos de uso inesperados, e auxiliar no gerenciamento de usuários internos e externos.
  - Informações: Top IPs, volume de dados transferidos, horário de maior uso e geolocalização.