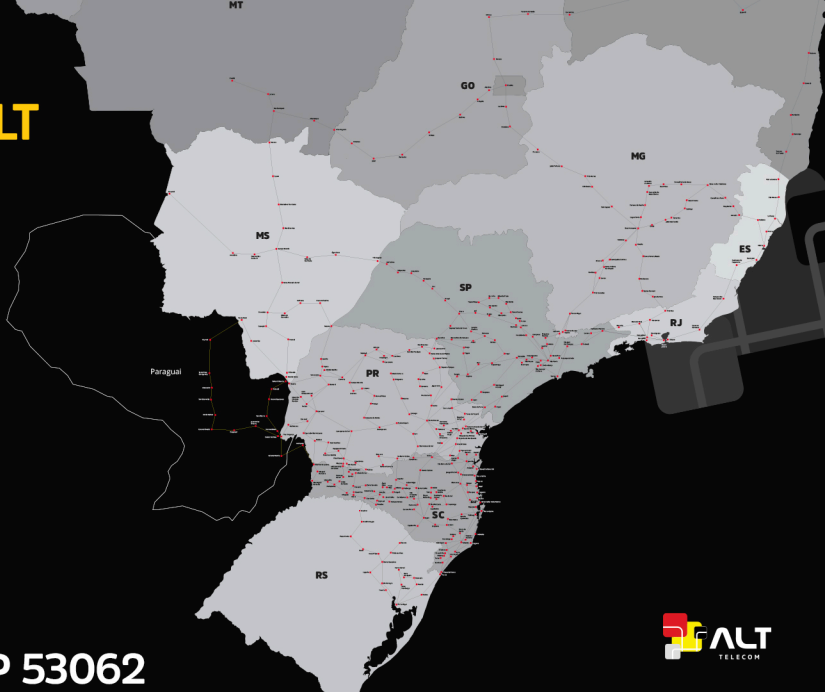
Plano Operacional ALT para Mitigação de Ataques DDoS

Atuação da ALT

ALT Telecom Operadora de Telecomunicações com presença plena ou parcial nos Estados de:

- Santa Catarina
- Paraná
- Rio Grande do Sul
- Mato Grosso do Sul
- Mato Grosso
- Goiás
- São Paulo
- Rio de Janeiro
- Minas Gerais
- Espírito Santo
- Bahia
- Distrito Federal



ASN Backbone IP 53062

Produtos para ISP's:

- Trânsito IP Mitigado
- Transporte Ponto a Ponto (L2 ou L3VPN sobre rede MPLS, Wave)
- Infraestrutura (Canais DWDM, Fibra, Dutos, Sites)

Todos os nossos contratos de Trânsito IP carregam mitigação inclusa em rede própria
(sem GRE). E não há filtragem em circuitos de transportes para IX (ponto de muitos questionamentos).

Estratégias do Modelo Operacional

Detecção e Gatilhos:

- Coletagem e análise dos flows de todas as bordas do backbone IP AS 53062;
- Preferência por bordas Juniper e coletor/analisador Wanguard Sensor utilizando servidor OCP (Open Compute Project) da Datacom;
- O Wanguard Sensor atua, acompanhando os fluxos de forma mais superficial (amostragem) e gerando gatilhos diante de anomalias de tráfego;
- Os gatilhos são personalizados para cada tipo de anomalia e podem ter ações diversas como: filtrar, limitar ou redirecionar o fluxo específico para um analisador de pacotes.

Confira este case: Proteção DDoS para ISPs com Servidor Datacom
(https://www.datacom.com.br/pt/blog/112/estudo-de-caso-protecao-ddos-para-isps-com-servidor-datacom)

Estratégias do Modelo Operacional

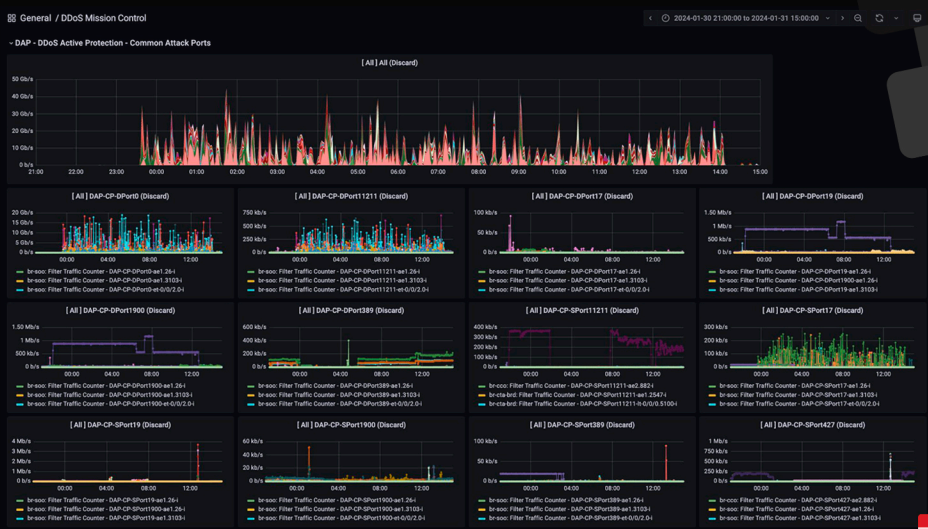
Filtragem - Filtros Fixos - 1ª Trincheira de Defesa

- Chargen (porta UDP 19)
- LDAP
- SSDP (porta UDP 1900)
- MEMCACHE (porta UDP 11211)
- NTP (porta UDP 123)

Para esses ataques conhecidos aplicamos em nossas bordas, por padrão,
filtros fixos de drop ou rate-limit, classificando o tráfego por protocolo/porta/tamanho do pacote,
a fim de criar um barreira sempre ativa e efetiva, sem impacto negativo.

ALT TELECOM

FILTROS FIXOS - PORTAS COMUNS



Estratégias do Modelo Operacional

Filtragem - Gatilhos Dinâmicos - 2ª Trincheira de Defesa

BGP Flowspec é uma extensão do protocolo BGP que permite a especificação e disseminação de regras de filtragem de tráfego em roteadores de provedores de serviços:

- Especificação de regras (Drop, Limit e Redirect);
- Disseminação de regras (anunciar regras e remover de forma dinâmica e automatizada);
- Rápida atualização de políticas;
- Mitigação granular (possibilidade de precisão cirúrgica gerando regra de forma automática baseado em IP e Porta de origem, IP e Porta de destino, protocolo, tamanho do pacote , entre outros) de acordo com a capacidade do router;
- Colaboração entre Provedores (evita consumo de banda desnecessário no Backbone e dos nossos Upstreams);
- Complexidade e segurança (o protocolo possui recursos de validação que devem ser utilizados para evitar a instalação de um filtro indevido por parte de um parceiro);
- Limite de regras em roteadores;
- Wanguard + API + MyISP + Flowspec + automações;
- Automação (MyISP) integrada com o analisador de flows permite customizar regras de flowspec para cada tipo de anomalia identificada;
- A ferramenta interage com a tabela de roteamento a fim de criar as regras de forma mais inteligente possível para que as mesmas sejam validadas e possam ser exportadas para os - Upstreams que suportam Flowspec;

Desta forma conseguimos mitigar o tráfego mais próximo da origem possível de acordo com a capilaridade que nosso Upstreams exportam a regra.

ALT TELECOM

Estratégias do Modelo Operacional

Filtragem - Redirecionar - 3ª Trincheira de Defesa

Uma das ações é redirecionar o tráfego para hardwares específicos;

O tráfego que demanda de uma análise mais profunda (ou seja, olhar mais do que apenas o cabeçalho do pacote) para uma limpeza mais cirurgica, é classificado e redirecionado via Flowspec para caixas de mitigação instaladas em nossa rede ou externas através de parcerias;

À exemplo do tráfego DST-PORT 443 com destino ao bloco x.y.z.w/q (que recebendo um ataque TCP SYN Flood) é redirecionado para uma VRF que vai para um servidor de limpeza onde o ataque pode ser tratado (utilizando syn-proxy, por ex) e devolvido para a rede para ser encaminhado ao destino;

Desta forma conseguimos otimizar os recursos de hardware de mitigação, pois enviamos para eles apenas o tráfego que precisa ser analisado/tratado e não todo o tráfego com destino ao bloco que está sendo atacado;

Quando o tráfego chega em uma caixa de mitigação passamos a olhar mais do que apenas o cabeçalho do pacote a fim de procurar uma assinatura mais específica do ataque.

ALT TELECOM

Estratégias do Modelo Operacional

Evolução dos Ataques

Recentemente vivenciamos muitos clientes recebendo ataques de grande volumetria ao mesmo tempo, principalmente amplificação DNS, ataques tipos carpet bonbing, repetidos em intervalos irregulares;

Ou seja, ataques distribuídos com grande quantiddade de tráfego logo no início e da curta duração;

Vários dwnstream recebendo ataques ao mesmo tempo ou em sequência, gerou problemas de ocupação de portas n x 100Gbps que interconectam nossos roteadores com nossos fornecedores de conectividade;

As características desses ataques inviabilizavam as contramedidas dinâmicas, pois existe um delay entre a identificação do ataque a criação das regras de filtragem;

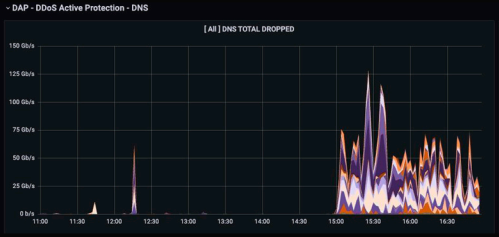
Subtítulo: Ações Tomadas:
• Re-Escrevemos nossa ACL de Filtros fixos, a fim de contemplar essa nova assinatura de ataques;

• Negociamos a aplicação dessa ACL nas portas das operadoras com sentido aos nossos roteadores

Ondas de Ataques

UDP FRAG (PORTA 0)

DNS (UDP SPORT 53)

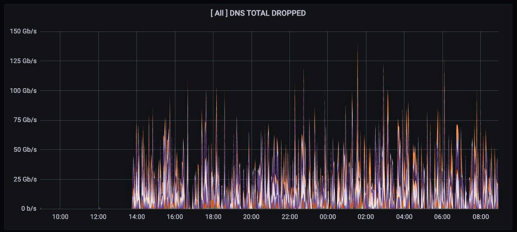


~ 275Gbps de tráfego sujo dropado (DNS AMP + UDP FRAG)

Ondas de Ataques

UDP FRAG (PORTA 0)

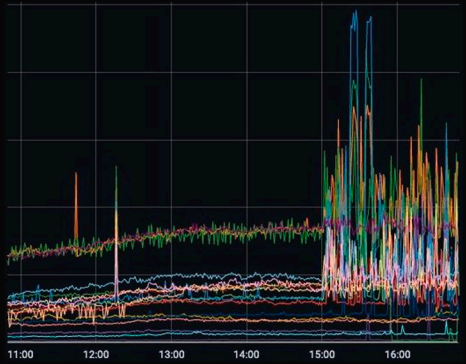
DNS (UDP SPORT 53)

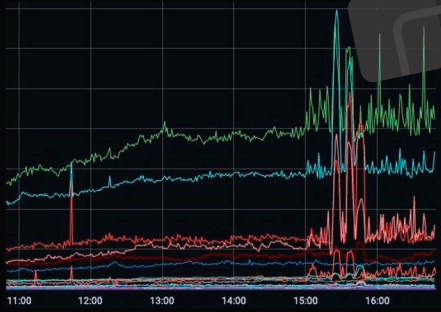


~ 205Gbps de tráfego sujo dropado (DNS AMP + UDP FRAG)

ALT TELECOM

Ondas de Ataques

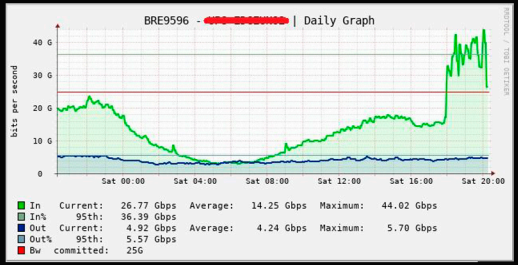


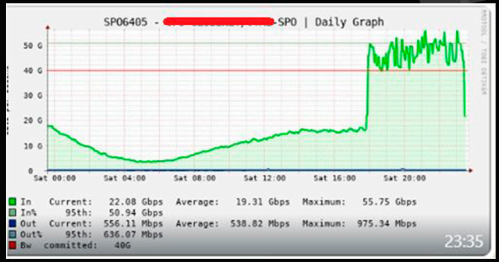


Upstreans/IXPs

ALT TELECOM

Resultados das ACL's





"A evolução na volumetria e complexidade dos ataques exige uma análise mais detalhada sobre onde filtrar e como otimizar a estratégia de combate."

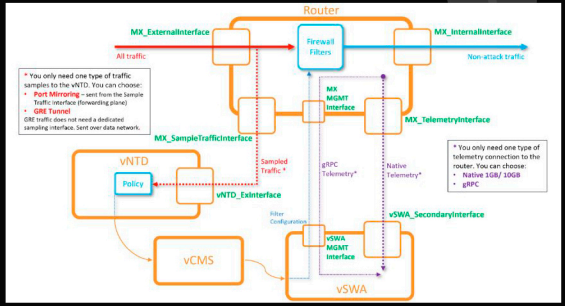
Solução Corero + Juniper

• Uma solução que não analisa apenas amostras de cabeçalhos e sim amostras de pacotes inteiros a fim de procurar assinaturas de ataques;

• O instala filtros direto nos roteadores de bordas Juniper, utilizando a capacidade de filtros flexíveis que conseguem dar match em campos mais profundos do pacote (aplica isso direto no roteador através de netconf + efêmero db;

• Utiliza a infraestrutura existente de bordas juniper;

• Evita a necessidade de redirecionar tráfego;



Insights e Percepções:

- Ninguém sobrevive a ataques DDoS sozinho, é necessário a parceria do fornecedor, o bom senso do gerente da rede e sua consultoria, bom relacionamento e a troca de conhecimento fazem toda a diferença;

- A literatura infantil já ensina o básico, na história dos 3 porquinhos, a casa de pedra se manteve em pé. Então, eliminar Soft Routers conforme sua rede vai crescendo é fundamental para uma maior proteção;

- Seguir lógicas, uma pessoa doente vai ao médico, o médico solicita exames e depois receita os medicamentos (o especilista, o laboratório e a farmácia cobram por seus serviços) de nada adianta contratar um consultor ou pedir uma opinião e não comprar o remédio. Na hora do ataque se a casa não estiver estruturada o que conseguimos fazer é suavizar a dor;

- Esteja sempre interligado com o trânsito em portas maiores do que a banda contratada. Mantenha contrato de on-demand. Quando receber um ataque de volumetria e alguma coisa passar não pode estrangular as portas;

- Foque em um caminho, não fique o tempo todo mudando de anúncio, restrinja a exposição do seu ASN. Anuncie inicialmente para conexões confinadas (IX, PNI) onde não está recebendo ataques e um trânsito mitigado;

- Trânsito com Upstreams A e Upstreams B, onde o A tem mitigação e o B não tem, ao chegar um ataque via Upstreams B e comprometer sua infraestrutura, o tráfego vindo de A também pode sofre o ataque;

"A água suja, pode ser tratada e se tornar potável novamente, mas é provável que a cor ou gosto seja um pouco diferente. Tráfego filtrado tem a mesma percepção."

ALT TELECOM

Dicas de Cuidados

- Anti-spoofing:
Evita que um pacote saia da sua rede com ip de origem que não seja o seu;
Na prática, se estiver recebendo ataque e configurar o anti- spoofing nada vai mudar, mas a sua rede vai parar de ser utilizada para vários tipos de ataques;
Quanto mais empresas aplicam anti-spoofing em suas redes mais os ataques DDOs tendem a perder força.

- Monitoramento de fluxos:
Entender o que está acontecendo na rede, saber por qual interfac a anomalia está entrando e identificar o tipo de tráfego são fatores essenciais.

"Não encontramos uma solução de hardware/software "mágico", onde injetamos tráfego “sujo” em uma porta e saia tráfego “limpo” em outra porta, para que o mesmo possa ser retornado para a rede... mas com um trabalho em conjunto com fornecedor e cliente, podemos atingir resultados com eficiência superior a 90%."

Gilmar Balbinot

Gilmar Balbinot

Diretor Comercial Corporativo e
Operação de Rede e Expansão

(49) 9 9135-3274
www.alt.com.br
e-mail: gilmar@acessoline.net.br

ALT TELECOM