Segurança com o pé direito

Toda **Operação** é um **negócio** e como todo **bom negócio**, precisa ser bem protegido para evitarmos incidentes e desastres que poderiam ser evitados.

Todos nós pensamos primeiro na infraestrutura como: Links IP, IXs, ativos e passivos de rede, sistema ERP para administrarmos o ISP, pessoal técnico para fazer as instalações, suporte ao cliente, equipamentos para montagem do backbone, pessoal de engenharia de redes, OLT, ONT/ONU, CGNAT, IPv6, etc. Tudo para que o assinante se conecte ao Provedor e consiga utilizar a Internet.

Onde estamos falhando ou o que estamos esquecendo de fazer?

Precisamos dar mais atenção para a cibersegurança e boas práticas!

Indivíduos mal intencionados buscam a todo instante brechas ou maneiras de causar impacto às empresas e por isso precisamos fazer o nosso dever de casa para evitar ou minimizar o impacto dessas ações maliciosas.

O trabalho envolve diversos setores da Operação desde **a borda**, até o **CPE** na casa ou empresa do assinante. Segurança da Informação é muito mais abrangente e exige coisas além do que iremos abordar aqui, como sistemas de infraestrutura de TI: anti-malwares, cultura de segurança da informação para os colaboradores, políticas de segurança, sistemas de backup e resposta a incidentes. Afinal ninguém quer ser vítima de um **ransomware**.

Aqui iremos abordar nossa área de Telecom e como podemos melhorar nossa segurança. Abaixo tópicos que abordaremos:

- Rede de Gerência.
- Autenticação, privilégios de acesso, logs e NTP.
- Filtros de Acesso.
- Monitoramento.
- BCP 38/BCP 84.
- Tratamento de Portas de Amplificação abertas e Static Loops.
- Gerência de Porta 25 e Problemas com RBLs.
- CPE.
- IPv6.
- Sistemas de detecção e Mitigação DDoS e Links Protegidos.

Rede de Gerência

Diversas Operações que conheci não fazem uso da **Rede de Gerência** e ela é muito importante para isolar toda a administração da infraestrutura, de acessos não autorizados. Por mais que você tenha um ótimo processo de criar e controlar credenciais de acesso, um assinante jamais deveria alcançar seus **ativos de rede**, nem tão pouco alguém vindo da **Internet**.

Temos basicamente 2 tipos de **Rede de Gerência**:

- **In-Band**: a gerência **in-band** é feita **pela mesma rede de produção** usada pelos dados normais (usuários, aplicações, tráfego corporativo). Ou seja, os pacotes de gerenciamento (SSH, SNMP, API, etc.) trafegam **pelo mesmo caminho** que o tráfego dos clientes ou serviços.

- **Out-of-Band**: a gerência **out-of-band** usa um **canal de comunicação separado** (físico ou lógico) apenas para gerenciamento. Esse canal não depende da rede de produção.

Algumas vantagens da **In-Band**:

- Simples de implementar (sem rede separada).
- Custa menos (não precisa de interfaces extras nem rede paralela).
- Funciona bem em ambientes pequenos.

Algumas desvantagens da **In-Band**:

- Se a rede principal cair, **você perde o acesso de gerenciamento**.
- Menor segurança — o tráfego de gerenciamento compete com o tráfego de produção e pode ser interceptado.
- Dificulta troubleshooting em falhas graves (ex: loops, ACLs erradas, VLANs off-line).

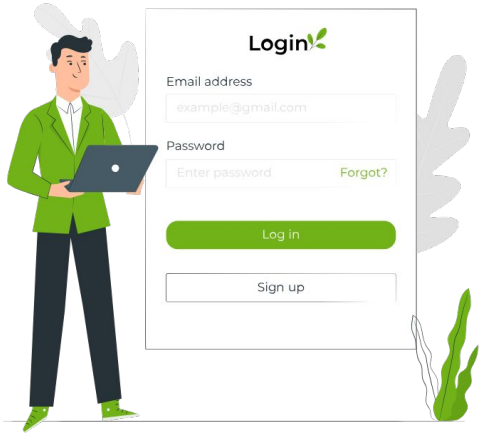
Algumas vantagens da **Out-of-Band**:

- Acesso garantido mesmo se a rede principal estiver fora do ar.
- Maior segurança — você pode isolar o tráfego de gerenciamento.
- Ideal para troubleshooting remoto e automação segura.
- Permite políticas e firewalls dedicados só para administração.

Algumas desvantagens da **Out-of-Band**:

- Custo adicional (precisa de interfaces dedicadas e uma rede separada).
- Maior complexidade de projeto.
- Em data centers grandes, exige switches de gerenciamento e VLANs exclusivas.

Autenticação, privilégios de acesso, logs e NTP



Outro assunto importante a ser abordado é o acesso aos ativos da rede. Nós vimos que o meio correto de acesso é através de uma Gerência de Rede. Mas e quanto às credenciais de acesso? Formas inseguras de acesso:

- Um único usuário e senha para todos os ativos e sistemas. Se alguém sair da empresa ou a senha vazar, faz-se necessário trocar em todos os ativos. Não temos como auditar o sistema.
- Um usuário e senha para cada ativo ou sistema. Mesmo problema anterior.
- Acessos mascarados por NAT. Em casos de credenciais roubadas, dificulta a identificação da origem do acesso.
- Nenhum servidor de logs registrando os acessos. Importante para auditoria identificar quem, quando e onde ocorreu o incidente.
- Ativos e sistemas corporativos com IP público para acesso cômodo através da Internet. Além de facilitar para um belo de um **DDoS** direto neles, ainda corre o risco de uma **vulnerabilidade Zero Day** permitindo acessos não autorizados.

Como posso então melhorar nesse quesito?

- Centralizar as credenciais de acesso com algum sistema **AAA** (authentication authorization and accounting) como por exemplo: **Radius** e **TACACS+**.
- Cada colaborador autorizado precisa ter seu próprio usuário e senha de acesso. Em caso de desligamento, basta desabilitar ou excluir a conta em um só lugar.
- Manter todos os ativos e sistemas com Data e Hora sincronizados utilizando servidores **NTP** (**Network Time Protocol**). É essencial para sistemas de detecção de DDoS e auditorias.
- Utilizar IPv4 privados **RFC1918** ou IPv6 **ULA** (**Unique Local Address**) **RFC4193** em quaisquer locais que não necessitem de IPs públicos ou Globais.
- Ter um servidor de logs para registrar os acessos. Existem algumas opções 0800 como exemplo:
    - Um GNU/Linux rodando um **syslog-ng** (suporte a **SQL** ex.: **MySQL**, **PostgreSQL**, **SQLite**) ou **rsyslog**.
    - Um GNU/Linux rodando um **Graylog** (versão paga tem mais recursos).
- Utilizar um Gerenciador de Senhas com cofre encriptado e criar senhas fortes para cada acesso. Um ótimo programa é o **KeePassXC** que pode ser baixado em: https://keepassxc.org/

Filtros de Acesso

Os filtros de acesso dão um extra na camada de segurança. Além da já comentada **Rede de Gerência**, criar uma **ACL** (**Access Control List**) e definir quem ou que prefixos podem acessar determinados sistemas e ativos. Pode prevenir que um serviço que acabou de se tornar vulnerável, de ficar exposto para ser comprometido. Exemplos de locais que necessitam dos filtros de acesso:

- Edges.
- Switches.
- CPEs.
- OLTs.
- CGNATs.
- BNGs/B-RAS.
- Servidores de Virtualização.
- Servidores de Serviços de Redes: **DNS**, **TACACS+/RADIUS**, **Web Server**, **Mail Server**, **Firewalls**, **servidores de logs**, **NTP Server**, qualquer sistema que possua recurso de **filtro de pacotes**.

Importante que o filtro de acesso seja implementado sempre para IPv4 e também para IPv6.

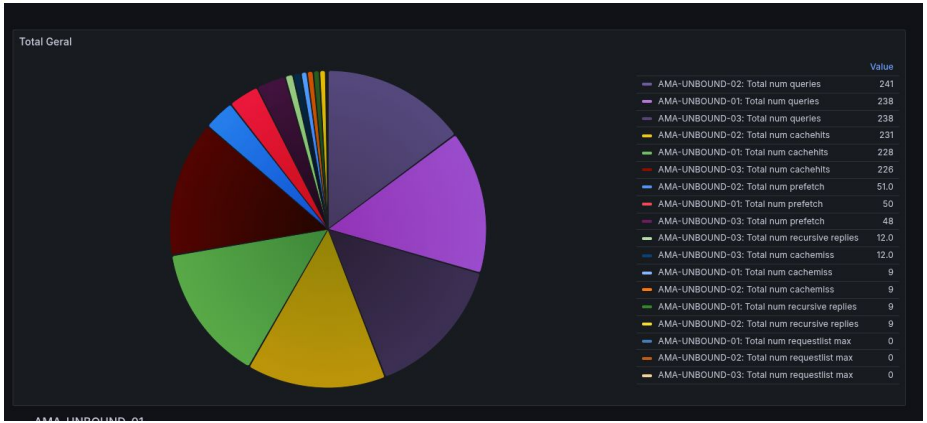
Monitoramento

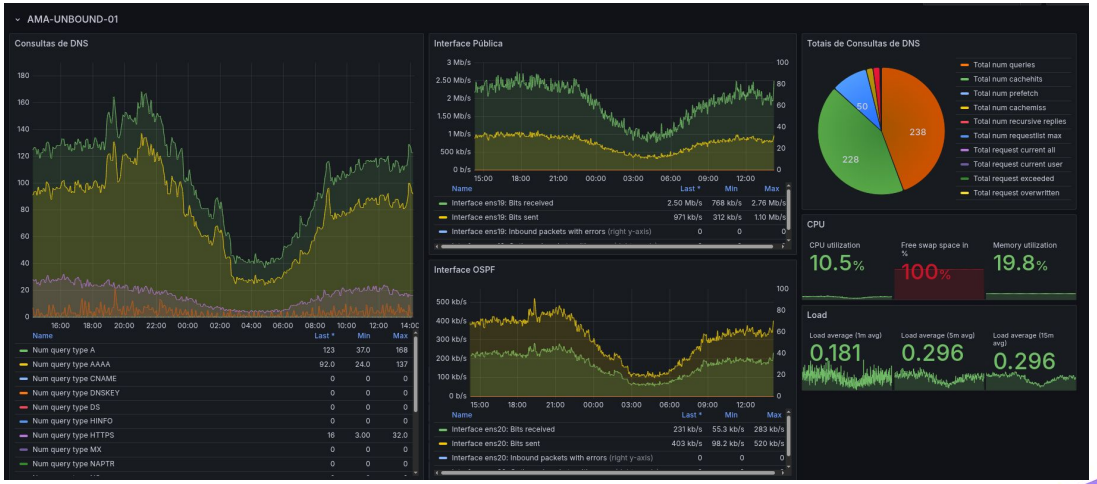
Tenha a visibilidade da sua Operação. Não fique às cegas! O que podemos tirar de proveito de um bom monitoramento?

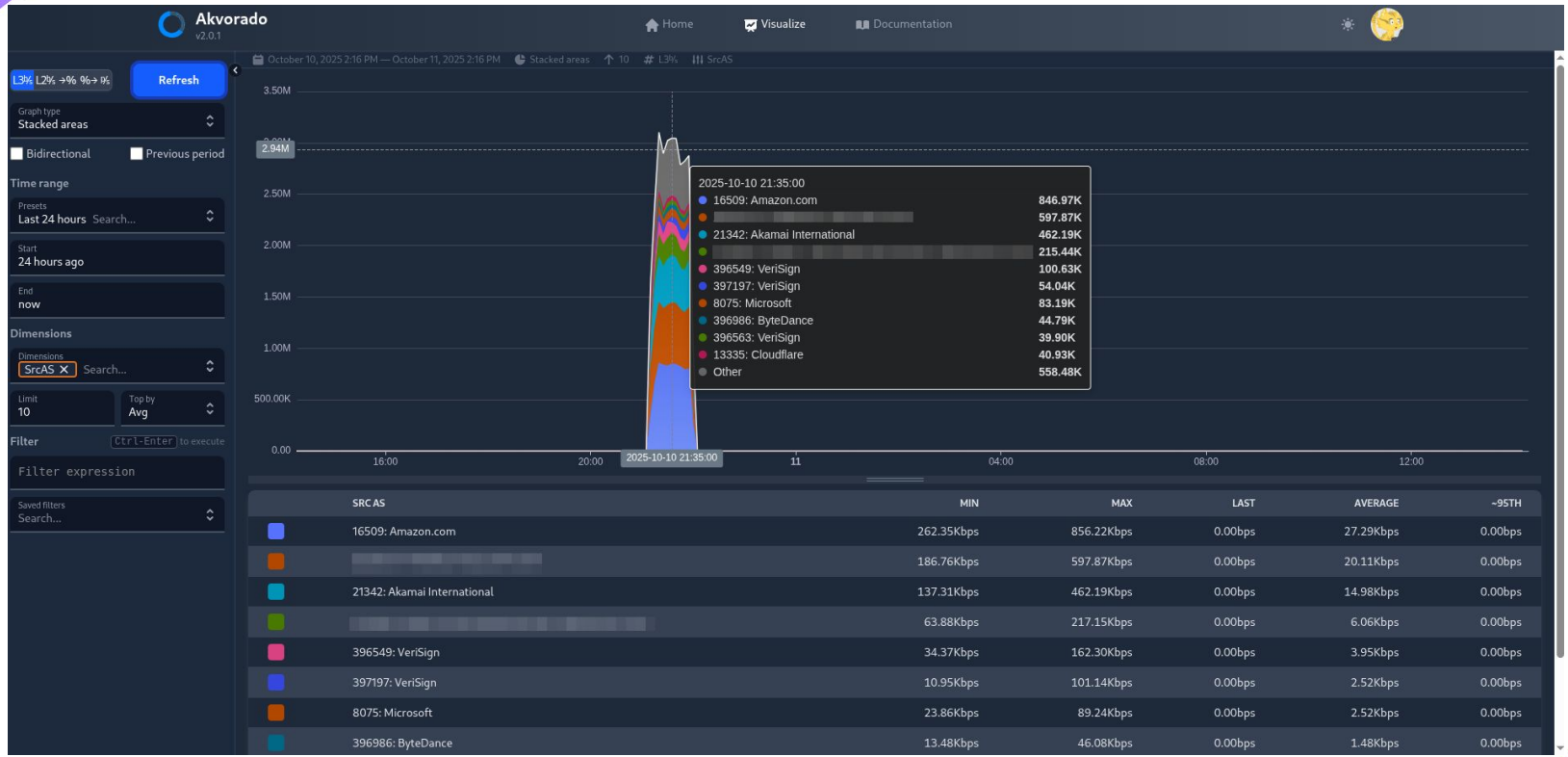
- Consumo de Links e identificação de problemas de tráfego.
- Status das sessões BGP com os upstreams.
- Identificação de problemas em ativos de rede e sistemas (CPU, memória, disco, carga).
- Identificação de problemas em trechos do seu backbone.
- Entendimento do tráfego consumido para se investir em parcerias que atendam a real necessidade dos assinantes.
- Detectar atividades prejudiciais como Botnets.
- Percepção dos volumes de ataques de DDoS e saturações de trechos.
- Alertas para acionamento de equipes conforme problema detectado.
- Como estão as filas de atendimento da Central de Suporte.
- Status de no-breaks, geradores e carga de baterias.

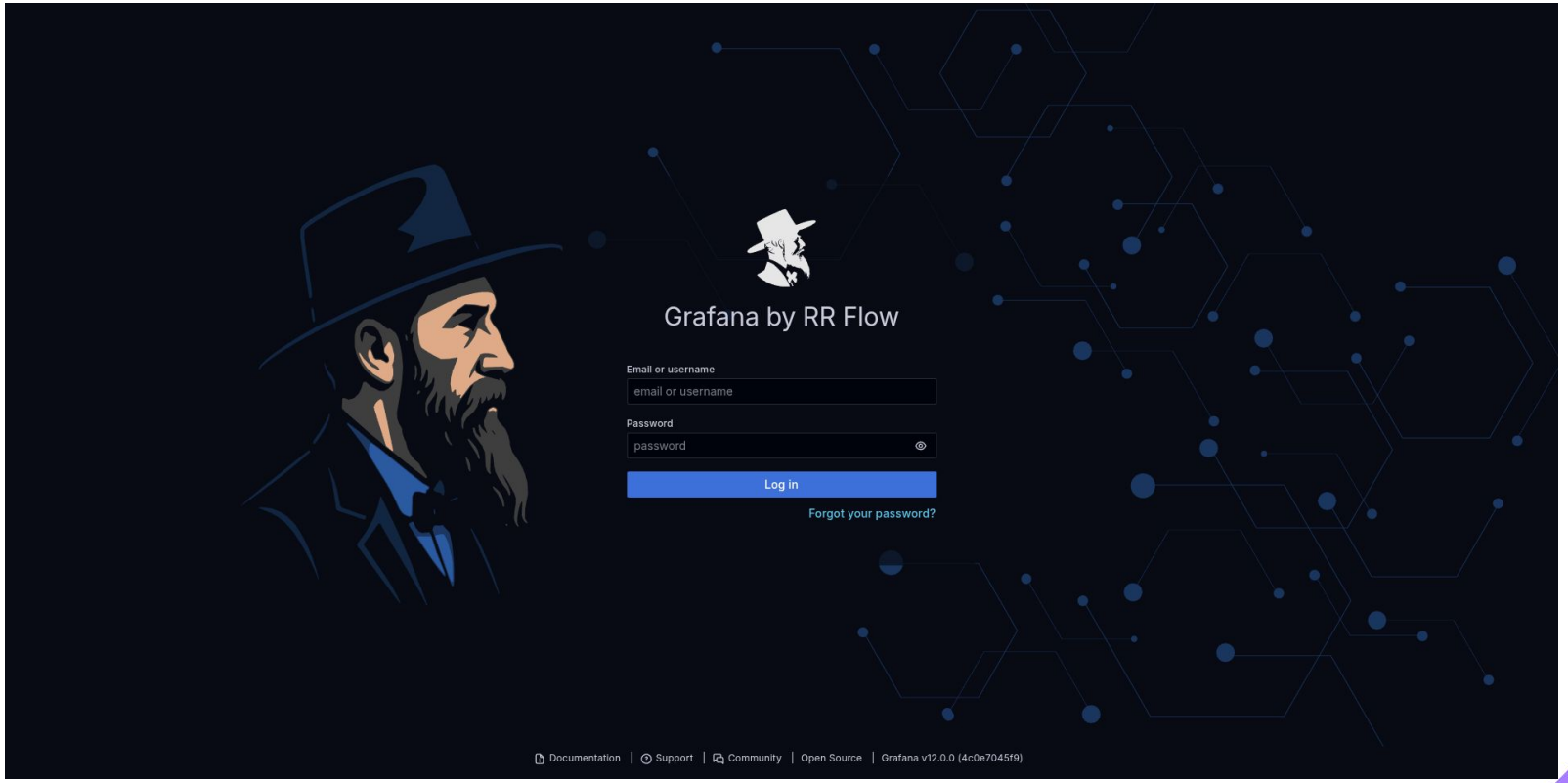
Algumas ferramentas úteis para o monitoramento e engenharia de tráfego:

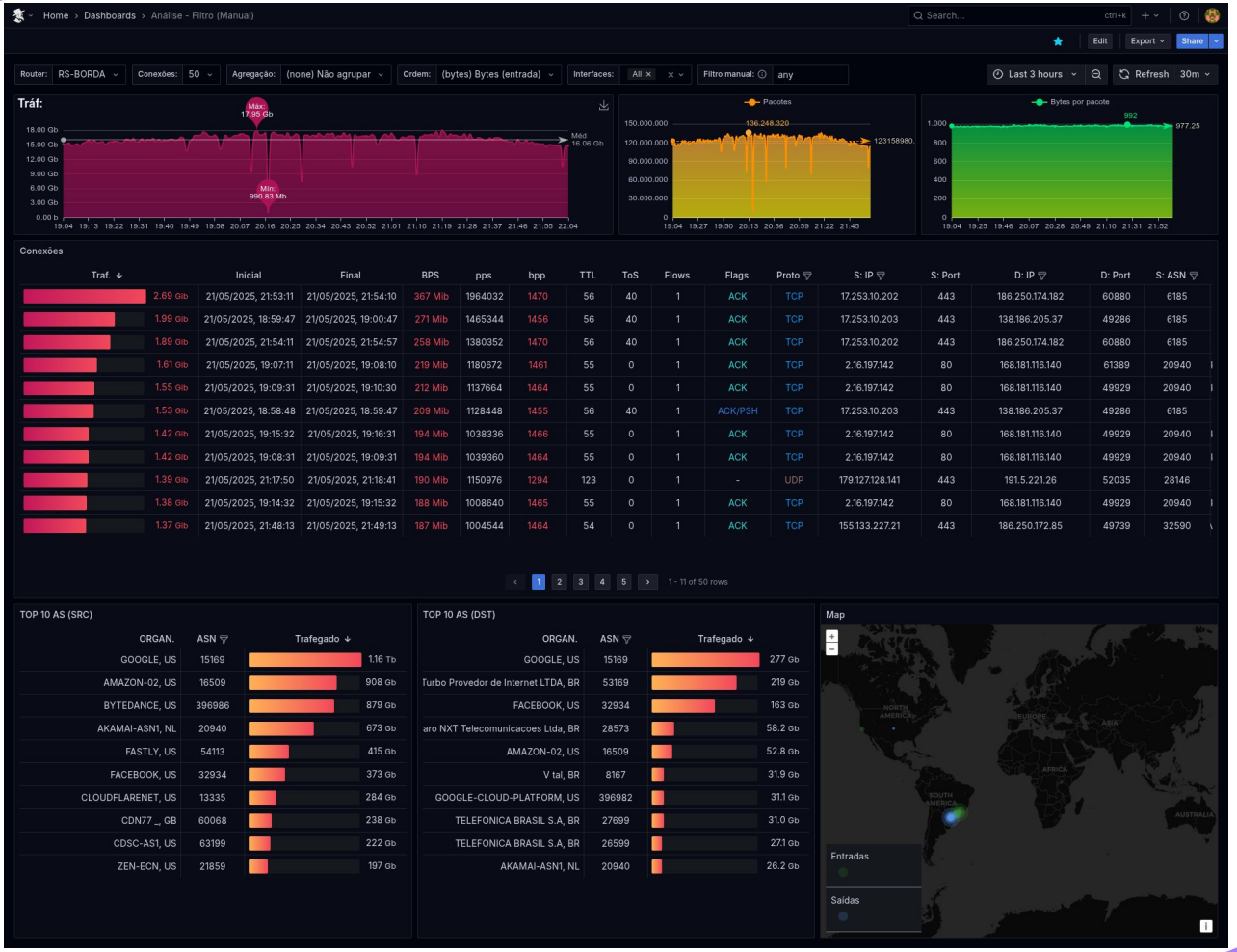
- **Zabbix:** https://www.zabbix.com/download
- **Grafana**: https://grafana.com/grafana/download?pg=oss-graf&plcmt=hero-btn-1
- **Cacti**: https://www.cacti.net/
- **MRTG**: https://oss.oetiker.ch/mrtg/
- **Akvorado**: https://demo.akvorado.net/docs/install
- **RR flow** (Rudimar Remontti): https://doc.rrflow.com.br/
- **Kentik**: https://www.kentik.com/
- **PRTG**: https://www.paessler.com/prtg

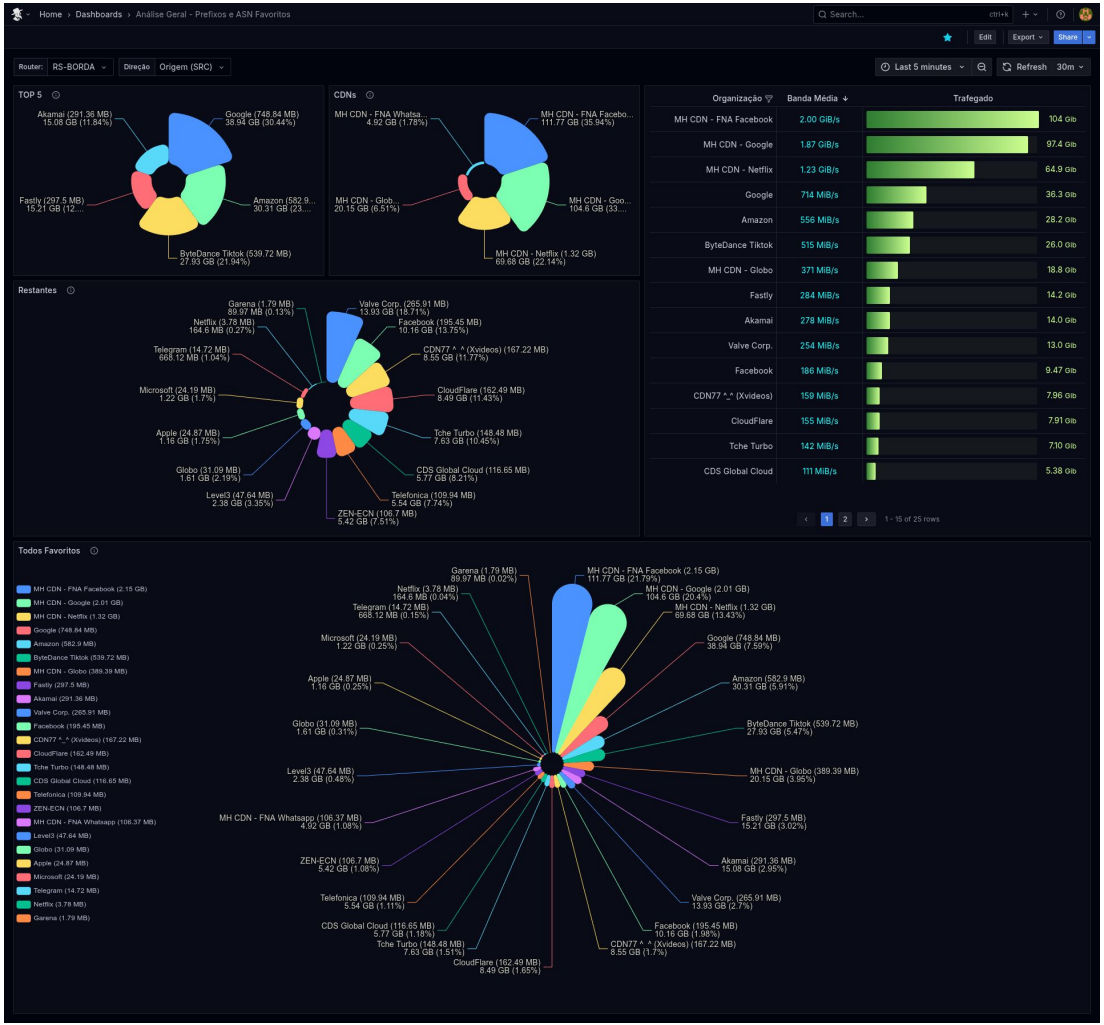












BCP 38/BCP 84

Vamos falar da principal causa dos ataques DDoS existirem, o chamado **spoofing**. Ataques muito utilizados como o de **reflexão/amplificação de DNS** e o **TCP SYN/ACK** são possíveis graças ao **spoofing**. Bloquear o **spoofing** não é complexo, o problema é que para ser efetivo, toda entidade conectada à Internet, deveria executar a **BCP 38** ou **BCP 84**.

- **BCP 38**: http://www.bcp38.info/index.php/Main_Page. O **BCP 38** tem como função bloquear pacotes IP cuja origem não pertença à sua rede. Interessante adicionar também bloqueios de origem IPv4 e IPv6 (**BOGONs**) com destino à Internet. O **BCP 38** pode ser feito diretamente na borda salvo algumas exceções como em casos onde a Operação é uma ITP (Internet Transit Provider). Para esses casos o melhor é partir para o **BCP 84**.

- **BCP 84**: https://www.rfc-editor.org/info/bcp84. O **BCP 84** utiliza um mecanismo chamado **uRPF** (**Unicast Reverse Path Forwarding**). O **uRPF** analisa se o pacote possui uma rota de retorno na tabela de roteamento e em caso negativo, o pacote recebe um drop. O **uRPF** pode trabalhar no modo **strict** (simetria de tráfego) ou **loose** (assimetria de tráfego). Um ótimo artigo sobre esse tema pode ser lido no **Brasil Peering Fórum** em https://wiki.brasilpeeringforum.org/w/Unicast_Reverse_Path_Forwarding do meu amigo **André Dias** da **Hexa Networks**. Lá inclusive você encontra a configuração de alguns vendors como **Huawei**, **Juniper**, **Cisco**, **Nokia** e **Mikrotik**.
  É comum usarmos **uRPF strict em BNGs** e **uRPF loose em bordas**.

Tratamento de Portas de Amplificação abertas e Static Loops

Segurança é um assunto que muitos desconhecem ou ignoram. Por isso certos serviços acabam ficando expostos quando não deveriam e muitos deles são considerados perigosos, pois são utilizados para ataques de amplificação DDoS. Alguns exemplos muito comuns:

- DNS.
- SNMP.
- NTP.

Portas de amplificação DDoS não devem ficar expostas. Devem ser tratadas junto aos seus clientes, senão sua rede poderá ser usada como vetor de ataques DDoS causando sérios problemas, impactando seus clientes e terceiros na Internet.

O CERT.br informa mensalmente sobre problemas de Portas de Amplificação, basta ter seu contato de segurança certo nos dados do seu ASN.

No **Brasil Peering Fórum** tenho um artigo para explicar melhor sobre:

https://wiki.brasilpeeringforum.org/w/Portas_de_Amplifica%C3%A7%C3%A3o_DDoS_e_Botnets

O **Static Loop** é um problema relacionado com rotas estáticas e a falta de configuração que impeça um pacote de entrar em loop entre um **equipamento A** com uma **rota estática** para um **destino B** que não possui esta rota estática em sua **FIB**, mas que tem uma **rota default** retornando para o equipamento com a rota estática. O loop continua até o fim da TTL (Time To Live).

Esse problema pode transformar um inocente tráfego de **10Mbps** em algo grande como **40Gbps**, saturando o trecho entre os dois equipamentos envolvidos no loop. A característica é reconhecida graficamente como **up e down iguais e de grande volumetria em bps**.

O Static Loop pode ser resolvido facilmente com prefixos em blackhole usando um distance alto no equipamento de destino. Para saber se você possui Static Loop em sua rede e conhecer mais dê uma olhada no meu artigo na Brasil Peering Fórum:

https://wiki.brasilpeeringforum.org/w/Static_Loop_-_um_erro_que_pode_matar_seu_ISP/ITP

Gerência de Porta 25 e Problemas com RBLs

A **porta 25/tcp** é uma porta utilizada apenas entre **servidores de correio**, pelo menos deveria ser assim mas muitos **malwares e botnets** utilizam esta porta para envio de **spam**, já que não necessita de autenticação para enviar e-mail. Para combater esse problema diversos sistemas de e-mail passaram a adotar serviços que usam as portas **587/tcp** e **465/tcp** para envio de e-mails, pois necessitam de autenticação para isso.

Uma boa prática é **bloquear conexões com destino à porta 25/tcp para qualquer destino na Internet, vindas de clientes residenciais e permitir apenas de clientes corporativos que tenham servidores de e-mail dentro de suas empresas**. A essa boa prática chamamos de **Gerência de Porta 25**. Não executar essa boa prática pode levar sua Operação a ter problemas com **RBLs** (**Real-time Blackhole List**) e ter seus IPs bloqueados em diversas listas, causando impacto para seus clientes. Um ótimo link para checar como está a saúde do seu **ASN** é o da **UCE Protect**, lá inclusive você consegue saber quais IPs são os ofensores.

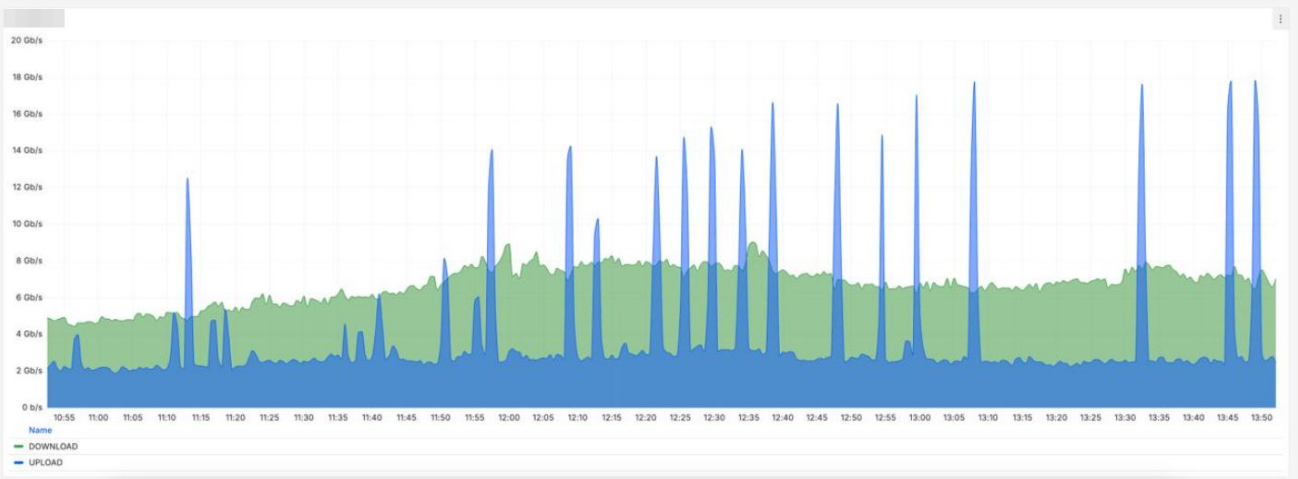
https://www.uceprotect.net/en/rblcheck.php

Uma ótima leitura sobre esse assunto está aqui: https://www.antispam.br/admin/porta25/

CPE

As CPEs são um grande calcanhar de Aquiles para um ISP. São os grandes responsáveis pela entrega do acesso à Internet no assinante, são responsáveis muitas das vezes pelo WiFi e a qualidade desse, pela entrega do IPv6. Se algo estiver ruim nesse equipamento, seu cliente irá reclamar do seu serviço.

Um cenário pior ainda seria uma recente descoberta de uma vulnerabilidade, que permitisse invasores instalarem bots para controle através de uma botnet. Uma vez sob controle de botnets, diversos ataques DDoS podem partir da sua rede e todos podendo utilizar clientes com planos altos entre 500Mbps e 1Gbps, imagine o estrago que isso pode causar à sua infraestrutura.



Para melhorar esse cenário precisamos ter cuidados com nossas CPEs:

- Bloqueios de acessos à CPE permitindo apenas através de uma Rede de Gerência ou pelo menos filtros permitindo acesso de certos prefixos IP. Não deixar o acesso livre às CPEs.
- Alterar o usuário padrão, se possível, e utilizar senhas fortes.
- Procurar por CPEs que tenham suporte ao TR069.
- Que tenham um sistema de atualização de firmware que possa ser feito via TR069.
- Suporte à IPv6 habilitado por padrão durante o provisionamento no cliente.
- Habilitar no provisionamento Firewall entrante tanto em IPv4, quanto em IPv6. **NAT não é Firewall**.

Aqui está a **BCOP CPE,** que trás o que toda **CPE** deveria ter para ser segura:

https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1-portuguese-final.pdf

Outra documentação é esta do meu amigo **Fernando Frediani** com título: **A importância da homologação das CPEs para ISPs**

https://forum.ix.br/files/apresentacao/arquivo/1517/07.pdf

IPv6

IPv6 é um assunto bastante batido e muitos não levam a sua implementação em consideração, porque talvez não acreditem que traga algum benefício para a Operação. Então resolvi listar alguns benefícios consideráveis:

- Todas as grandes CDNs entregam seus conteúdos em IPv6 e os maiores tráfegos vem delas.
- Quanto maior for seu tráfego em IPv6, menor será seu tráfego de CGNAT. Aqui temos economia em CAPEX.
- IPv6 ainda não é o principal protocolo mais usado em ataques DDoS de grandes volumetrias, logo clientes com IPv6 tendem a ter menos problemas durante ataques DDoS.
- CGNAT limita a quantidade de portas por IP e isso trás problemas de acesso em ambientes corporativos com muitas estações de trabalho e servidores. As portas são rapidamente exauridas e servidores não podem ser acessíveis da Internet. Isso não ocorre com sistemas que usam IPv6.
- Cada vez mais jogos estão adotando o IPv6 enquanto o CGNAT continua prejudicando a jogabilidade dos que ainda usam IPv4.

O **NIC.br** disponibiliza diversos treinamentos gratuitos, inclusive o de IPv6. Fique atento aos cursos em:

https://cursoseventos.nic.br/

Sistemas de detecção e Mitigação DDoS e Links Protegidos

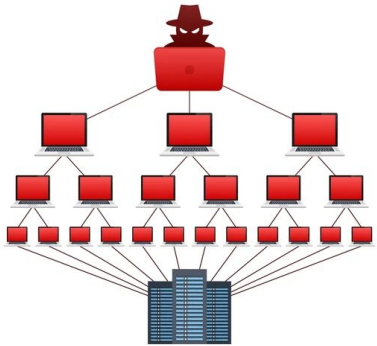
Ataques DDoS crescem mais a cada ano que se passa e se sua Operação ainda não sofreu com esse mal, pode acreditar que é apenas uma questão de tempo para se tornar uma vítima deste.

Tudo começa com um olhar em sua infraestrutura e daí a criação de uma estratégia de defesa mesmo sem antes ter sido atacado. Mas por que?

Toda ferramenta de detecção precisa de **ajustes de falsos positivos** e para isso é importante que tenhamos um ambiente sem ataques, para que seja ajustada a ferramenta para o perfil de tráfego dos seus clientes e serviços. Tentar fazer esses ajustes durante um ataque DDoS é bem mais difícil, mais demorado e no meio de algo que estará impactando bastante seus clientes. Você irá querer que resolva rápido mas não será possível.

É um Lego que precisa ser montado com cuidado e temos algumas peças:

- Sistema de detecção de DDoS.
- Nuvens de mitigação DDoS.
- Caixas de mitigação DDoS.
- Links Protegidos.



- O **sistema de detecção de DDoS** é a ferramenta que irá analisar flows e te dar uma visão do que está ocorrendo podendo também executar uma ação de mitigação: como **executar um flowspec na borda** ou **fazer um desvio de prefixo para uma nuvem de mitigação DDoS**. Utilizar-se de communities para uma engenharia de tráfego para proteção do ISP. É a parte inteligente de toda a proteção. Alguns programas com essa finalidade:
  - **Wanguard**: https://www.andrisoft.com/software/wanguard (ferramenta mais utilizada).
  - **FASTNETMON**: https://fastnetmon.com/
  - **Kentik**: https://www.kentik.com/

- **Nuvens de mitigação DDoS** tem o papel de receber todo o ataque e entregar o tráfego limpo de ataque. Trabalham com desvio de prefixos IP e por isso existe o incômodo da convergência quando este retorna da nuvem de mitigação. Existem muitas empresas que prestam esse tipo de serviço no Brasil, pesquise, consulte amigos que já usem e implante uma que te atenda em custo x benefício x qualidade. Alguns nomes do mercado:
  - **Huge Networks**: https://www.huge-networks.com/
  - **Sage Networks**: https://sagenetworks.com.br/
  - **Telic Technologies**: https://telic.com.br/
  - **UPX**: https://upx.com/

- **Caixas de mitigação DDoS** são peças muito caras no Lego, você além de desembolsar uma quantia considerável, dependendo do vendor, precisará de ter uma borda com capacidade e Links IP com bastante banda para suportar o ataque DDoS, limpar e entregar em sua infraestrutura. Para muitas empresas não será viável economicamente. Alguns vendors:
  - **Corero**: https://www.corero.com/
  - **Appliance da Huge**: https://www.huge-networks.com/
  - **Netscout Arbor**: https://www.netscout.com/arbor

- **Links Protegidos** existem muitos mas embaixo do capô, a maioria conta com o mesmo sistema de desvio de prefixos IP para nuvens de mitigação DDoS ou possuem caixas de mitigação DDoS para limpeza. O que sai um pouco desse conceito são duas tecnologias que estão crescendo no mercado: **Corero** (appliance de limpeza em camada 2) e **Nokia Deepfield** (limpeza direto no roteador de borda com chip dedicado). Nos dois últimos casos é necessário utilizar um **upstream** que utilize uma dessas tecnologias como serviço de limpeza. Trânsitos conhecidos nas duas tecnologias:
  - **Forte Telecom (Corero)**: https://www.fortetelecom.com.br/
  - **K2 Telecom (Deepfield)**: https://k2telecom.com.br/

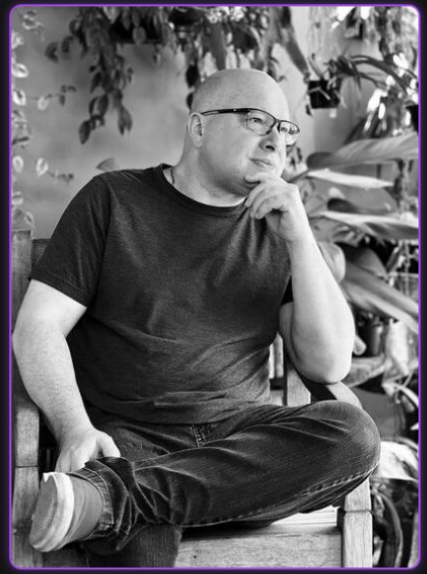
- O **sistema de detecção de DDoS** é a ferramenta que irá analisar flows e te dar uma visão do que está ocorrendo podendo também executar uma ação de mitigação: como **executar um flowspec na borda** ou **fazer um desvio de prefixo para uma nuvem de mitigação DDoS**. Utilizar-se de communities para uma engenharia de tráfego para proteção do ISP. É a parte inteligente de toda a proteção.

- **Nuvens de mitigação DDoS** tem o papel de receber todo o ataque e entregar o tráfego limpo de ataque. Trabalham com desvio de prefixos IP e por isso existe o incômodo da convergência quando este retorna da nuvem de mitigação. Existem muitas empresas que prestam esse tipo de serviço no Brasil, pesquise, consulte amigos que já usem e implante uma que te atenda em custo x benefício x qualidade.

- **Caixas de mitigação DDoS** são peças muito caras no Lego, você além de desembolsar uma quantia considerável, dependendo do vendor, precisará de ter uma borda com capacidade e Links IP com bastante banda para suportar o ataque DDoS, limpar e entregar em sua infraestrutura. Para muitas empresas não será viável economicamente.

- **Links Protegidos** existem muitos mas embaixo do capô, a maioria conta com o mesmo sistema de desvio de prefixos IP para nuvens de mitigação DDoS ou possuem caixas de mitigação DDoS para limpeza. O que sai um pouco desse conceito são duas ferramentas que estão crescendo no mercado: **Corero** (limpeza em camada 2) e **Nokia Deepfield** (limpeza direto no roteador de borda com chip dedicado). Nos dois últimos casos é necessário utilizar um **upstream** que utilize uma dessas tecnologias como serviço de limpeza.

Meus contatos



Marcelo Gondim da Cunha

Especialista em redes e segurança, com experiência desde os anos 1990. Atuou como desenvolvedor, consultor de sistemas GNU/Linux e foi CTO da Nettel Telecom, onde implantou IPv6 em 2013. Contribui com o projeto MANRS. Também liderou o SOC da Brasil TecPar entre 2022 e 2025, focando em defesas contra DDoS, boas práticas e onde desenvolveu uma rede de DNS(s) Recursivos Anycast certificada pelo KINDNS.

- Administração de Sistemas Unix-Like desde 1996.
- Consultor na Conectiva S/A - Unidade Rio em 2000.
- Direção do AS53135 - Nettel Telecomunicações entre 2003 e 2021 atingindo a marca de 41.000 assinantes.
- Diversas palestras em eventos da área de Redes e Serviços e artigos técnicos publicados.

Linkedin: https://www.linkedin.com/in/marcelo-gondim-sysadmin/
E-mail: gondim@ispfocus.net.br