DPR Construindo as redes do futuro

ATIVOS DE REDE

SOLUÇÕES **DPR & NOKIA**

Toda semana uma solução para **deixar a sua rede pronta para o futuro!**

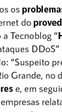
ATAQUES DDoS

Como **ataques DDoS** estão se tornando um **grande risco** para empresários no **investimento em telecomunicações?**

Imagine que grande parte dos seus assinantes resolveram assistir à final da copa do mundo por streaming em alguma plataforma online e na hora da bola rolar, a conexão que você fornece apresenta **desconexões ou lentidão**, seria uma grande frustração, não? Mas pode ser um **problema ainda maior para o seu ISP**, pois possivelmente um ataque DDoS está sendo direcionado para o seu servidor, explorando uma **falta de segurança nos seus equipamentos e rede.**

É importante lembrar que os criminosos calculam a época dos ataques baseados em **eventos que terão grande audiência ou necessidade de tráfego online**, pois assim facilmente conseguem disfarçar e dificultar a detecção da atividade.

Agora além do **problema técnico** para resolver na sua rede e possivelmente uma central de suporte **sobrecarregada**, você talvez também tenha que lidar com **usuários insatisfeitos** com o seu serviço. Imagine qual será o esforço empregado em marketing e pós-venda para tornar esse um c**liente satisfeito novamente e o fidelizar?**



Se não bastassem todos os **problemas operacionais** para resolver, o sinal de internet do **provedor pode ainda ser sequestrado**, segundo a Tecnoblog "**Hackers** já praticaram **extorsão** para cessar ataques DDoS" e segundo a revista digital da Uol, Gizmodo: "Suspeito preso preventivamente na cidade gaúcha de Rio Grande, no dia 6. Ele é investigado por **atacar os provedores** e, em seguida, **exigir valores** para parar as ofensivas. As empresas relataram prejuízo de **mais de R$ 1 milhão**". A operação do seu negócio pode estar em sérios **riscos** ao cair na mão dos criminosos.

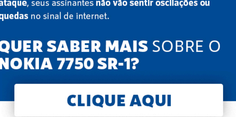
Agora você já sabe que provedores podem **sofrer muitas consequências** a partir do **DDoS**, mas o que é exatamente uma **negação de serviço distribuída?**

Os ataques de negação de serviço, conhecidos como DDoS (Distributed Denial of Service) consistem em sobrecarregar os servidores dos provedores com grande volume de tráfego, impossibilitando que pacotes de dados sejam enviados ou recebidos pelos clientes, fazendo com que qualquer tipo de acesso a sites, aplicativos, vídeos, ou qualquer coisa que exija comunicação com um outro servidor se torne impossível nesse tempo.

Para obter sucesso na **investida**, os **hackers** utilizam diversas **formas de ataques**, mas existem **dois tipos sendo muito utilizados:**

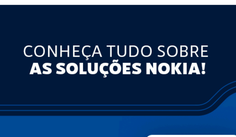
Ataque **Distribuído**

Uma origem envia **um comando** para **milhares de dispositivos conectados** na internet requisitando acesso à **um ou diversos IPs**. Um verdadeiro **exército de zombies**. Os dispositivos utilizados nos ataques normalmente estão **contaminados com um vírus** que os obriga a tomar a ação de **envio de tráfego involuntário** através de uma **central comandante.**



Ataque **Amplificado**

Uma origem envia **milhares de requisições** para **um destino de IP forjado** e em seguida solicita **milhares de pacotes de um Host.** Por exemplo: um IP pode "transmitir" 128 bytes e "receber" 1280 bytes por requisição, sobrecarregando o tráfego disponível no provedor com essas trocas amplificadas.
Pequenos provedores são os alvos desses ataques, pois geralmente possuem **poucos blocos de IPv4 (CGNAT)** disponíveis para tráfego dos usuários, de forma que **sobrecarregar os serviços** desses targets é muito mais simples para os criminosos, exigindo menos recursos empregados para aplicar o ataque.



Como provedores podem **prevenir o DDoS?**

Não existem formas efetivas de prevenir ataques DDoS, pois o aumento do tráfego pode ser repentino, com data e hora agendadas pelos criminosos, **porém é possível mitigar o ataque e evitar a sobrecarga na rede.**

A **DPR** possui um roteador de borda chamado **7750 SR-1 (marca Nokia)**, que além de ter um **desempenho robusto** para atender a necessidade de banda do provedor e realizar **CGNAT, BNG e Peering** em um único **equipamento compacto (até 3 RU de espaço no rack)**, também conta com a tecnologia **exclusiva** da marca, chamada **"Deepfield Defender"**, um software capaz de analisar milhões de entradas de IPs por segundo identificando os ataques, enquanto o SR-1 mitiga com os filtros **ACL.**
Com esse equipamento, os **IPs maliciosos são impedidos** de chegar até o destino e sobrecarregar a rede do provedor, dessa forma mesmo que os criminosos **tentem realizar o ataque**, seus assinantes **não vão sentir oscilações ou quedas** no sinal de internet.

QUER SABER MAIS SOBRE O **NOKIA 7750 SR-1?**

CLIQUE AQUI

O mercado de telecomunicações é competitivo e ter **previsibilidade** sobre o futuro do seu ISP é **imprescindível** para tomar decisões acertadas, por isso **extinguir** a possibilidade de ser afetado por **ataques DDoS** pode ser uma **vantagem competitiva** enorme para o seu negócio, no processo de **fidelizar o seu cliente**.

CONHEÇA TUDO SOBRE **AS SOLUÇÕES NOKIA!**

QUER SABER **MAIS?**

DPR Construindo as redes do futuro

ENTRE EM **CONTATO COMIGO** PELO **WHATSAPP**