SÃO
PAULO
TECH
SCHOOL

Computação e sistemas distribuídos em nuvem

Proxies

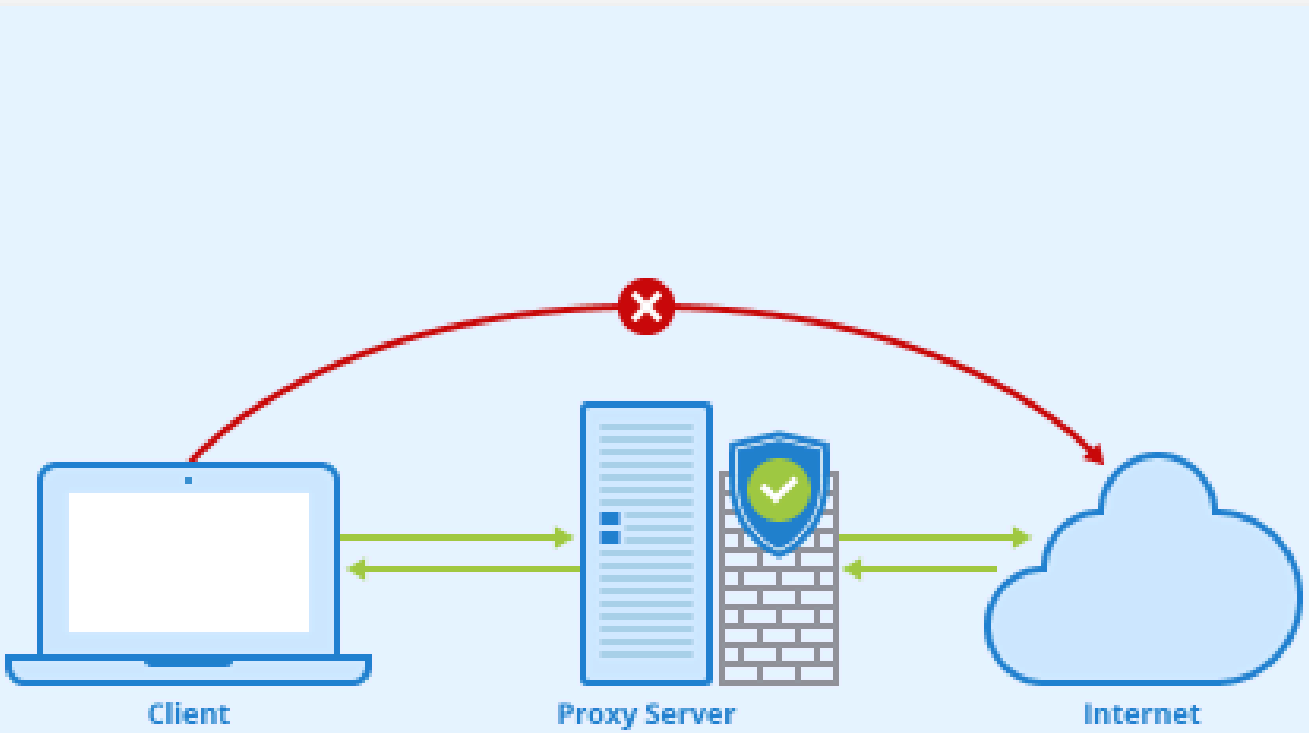
Eduardo Verri

eduardo.verri@sptech.school

Proxies

O que é um servidor proxy?

- Um servidor proxy é uma ferramenta importante para sua privacidade, e está muito ligado ao que a palavra em inglês quer dizer: procuração. Isto é, representa um certo tipo de autoridade dada a uma outra parte para agir em seu nome.
- Um servidor proxy é como uma ponte entre você e a internet. Quando você tenta acessar um site pelo seu dispositivo, o navegador envia uma requisição ao servidor web deste site, o qual retorna com a página que você estava buscando. Assim, sem um proxy, você se comunica diretamente com a internet e com o servidor em que está hospedado o site que você deseja acessar.
- Já quando você utiliza um servidor proxy, sua comunicação passa a ser intermediada por ele.



Assim, pode-se dizer que um servidor proxy é uma máquina na internet colocada entre você, a origem da requisição, e o servidor do site, destino da requisição.

Ele faz o envio da solicitação para acessar o conteúdo em seu nome, e também o movimento contrário, quando o servidor responde à solicitação, ela passa de volta pelo Proxy, o qual entrega a página buscada ao seu navegador

- Um *proxy* serve para intermediar e filtrar fluxos de informações e solicitações – basicamente, todas as interações de um usuário com conteúdo da internet.
- Eles servem para: filtrar conteúdo, dinamizar e acelerar o carregamento de *websites* e conteúdo em geral e, além disso, manter um melhor nível de segurança para os usuários, impedindo certos tipos de ameaças.

Proxy Transparente

É o tipo mais básico, pois não oferece camadas de proteção. O seu IP permanece visível ao servidor, e ele também poderá ver que você está utilizando um Proxy, mesmo que você não saiba que seu computador está usando um (por isso é chamado de transparente).

Esse tipo de proxy geralmente é utilizado por empresas, escolas, bibliotecas e demais ambientes corporativos. Essas instituições normalmente buscam filtrar conteúdos, permitindo ou não o acesso a algumas páginas específicas.

Proxy Anônimo

Este tipo de proxy protege seu IP do servidor. Ainda assim, ele não oculta o fato de que você está utilizando um Proxy. Ele oferece uma proteção maior ao ocultar seu endereço e impedir ameaças como roubo de dados, mas ainda possui limitações.

Por exemplo, ao utilizar um proxy anônimo você não poderá acessar sites que impedem a entrada de visitantes que estejam utilizando um proxy.

Proxy Altamente Anônimo, ou Proxy Elite

Oferece uma camada a mais de proteção com relação aos proxies anônimos. Ou seja, um proxy altamente anônimo oculta seu IP e também a informação de que você está utilizando um proxy.

Além disso, também altera o IP que utiliza com certa frequência, dificultando o monitoramento das origens do tráfego. Por isso, é o tipo de Proxy que oferece o maior nível de anonimato ao navegar na internet

Proxy Reverso

Esse proxy faz é o caminho inverso do que faria um “forward proxy” — aqueles situados entre o computador do usuário e o servidor. Isto é, ele está no intermédio do servidor para com a internet.

Então, um Proxy Reverso filtra informações geradas por visitantes, encaminhando solicitações filtradas para o servidor. Por este motivo, um proxy reverso é mais comumente utilizado para lidar com requisições de servidores de hospedagem de sites, ou por grandes sites que precisam controlar o consumo de banda larga.

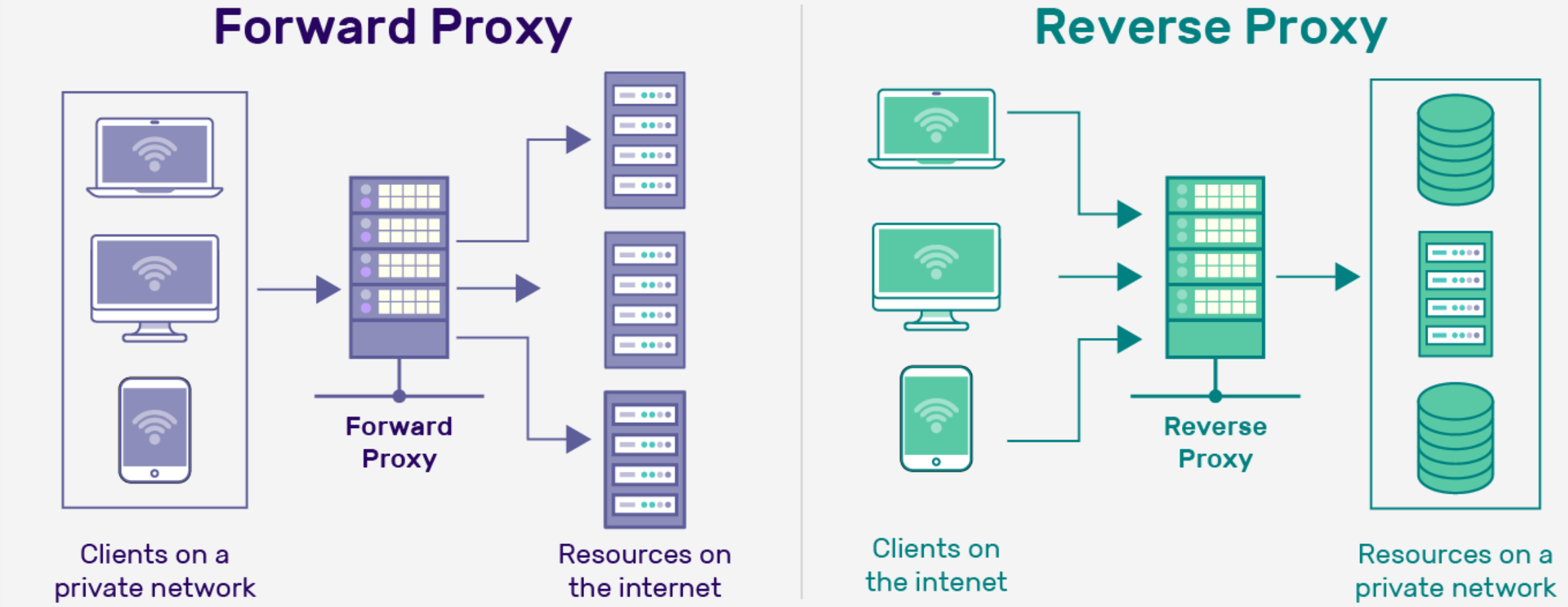
Proxy de Distorção

Esse tipo de servidor proxy se apresenta ao servidor de destino com um IP falso ou incorreto. Assim, mesmo não ocultando do servidor que um proxy está sendo utilizado, ele protege e esconde sua própria identidade. É normalmente utilizado para acessar sites específicos que só estejam disponíveis em um território, pois assim é possível ocultar e manipular a localização do servidor de origem que está tentando o acesso.

Free Proxy

São páginas de internet que fornecem endereços de IP de servidores proxy de forma gratuita, para que qualquer pessoa possa utilizá-los. Este tipo de servidor Proxy é o mais perigoso, pois ainda que seu endereço e dados estejam ocultos do servidor de destino, não estão ocultos do próprio Proxy em si – que pode não ser confiável.

Forward proxy vs Reverse proxy


Forward Proxy
Forward Proxy
Clients on a private network
Resources on the internet
Reverse Proxy
Reverse Proxy
Clients on the intenet
Resources on a private network

Forward Proxy vs Reverse Proxy

Um forward proxy (de encaminhamento ou direto) aceita conexões de computadores em uma rede privada e encaminha essas solicitações para a Internet pública. É o único ponto de saída para usuários de sub-rede que desejam acessar recursos fora de sua rede privada.

O proxy reverso atua como um ponto único de entrada para sistemas externos acessarem recursos em uma sub-rede privada. Em uma arquitetura corporativa, um proxy reverso atua como ponto de acesso público para os usuários acessarem dados e informações armazenados em servidores que residem em uma sub-rede privada e isolada.

Forward Proxy vs Reverse Proxy similaridades

- Ambos protegem os dispositivos conectados a uma rede privada contra ameaças da Internet e de outras redes externas.
- Ambos podem limitar os tipos e tamanhos dos arquivos que passam por eles e impedir que usuários não autenticados enviem solicitações por meio deles.
- Ambos podem realizar comutação de portas e protocolos, o que pode disfarçar ainda mais os padrões de acesso usados para acessar recursos ocultos por trás deles.
- Também é possível usar o mesmo software para configurar um proxy direto e um proxy reverso. Por exemplo, o Nginx e o servidor web Apache são comumente usados como proxy reverso em arquiteturas corporativas e também podem ser configurados para atuar como proxy direto .

Forward Proxy vs Reverse Proxy diferenças

- Um proxy de encaminhamento normalmente é configurado no laptop ou desktop de um funcionário de escritório para fornecer acesso seguro à Internet pública, seja no trabalho no local ou conectado remotamente à rede privada. Além disso, o proxy de encaminhamento deve ser configurado manualmente. Cada computador que queira acessar recursos fora da sub-rede privada do local de trabalho deve ser configurado com o endereço IP e o número da porta do proxy de encaminhamento da rede.
- Ao contrário do proxy de encaminhamento, um proxy reverso não requer clientes pré-configurados. O servidor proxy reverso é acessível publicamente.

Forward Proxy vs Reverse Proxy diferenças

- Um proxy reverso e um proxy direto cumprem uma missão comum em arquiteturas corporativas: facilitar solicitações de recursos entre redes privadas e a Internet pública. No entanto, eles desempenham funções drasticamente diferentes e atendem clientes decididamente diferentes.
- Os proxies de encaminhamento ajudam os usuários em uma sub-rede privada a acessar a Internet pública. Um proxy reverso permite que solicitações provenientes da Internet pública acessem recursos que residem em uma sub-rede privada.

Principais usos de um proxy reverso

Balanceamento de carga: os proxies reversos distribuem o tráfego de rede de entrada em vários servidores para garantir a utilização ideal de recursos, evitar a sobrecarga do servidor e melhorar o desempenho dos aplicativos. Isto é particularmente valioso em sites e aplicativos de alto tráfego.

Terminação SSL: Eles podem lidar com criptografia e descriptografia SSL/TLS em nome de servidores back-end, aliviando a tarefa de gerenciamento de conexões seguras, que consome muitos recursos.

Aceleração e cache da Web: esses servidores podem armazenar em cache conteúdo estático, como imagens, folhas de estilo e scripts, reduzindo a carga nos servidores back-end e acelerando a entrega de conteúdo aos usuários. Este mecanismo de cache melhora o desempenho geral e a capacidade de resposta do site.

Principais usos de um proxy reverso

Segurança e Controle de Acesso: Atua como uma barreira protetora entre a internet pública e os servidores internos. Eles podem implementar medidas de segurança, como firewalls de aplicativos da Web (WAFs) e controles de acesso, para se defenderem contra ataques comuns da Web e acesso não autorizado a recursos confidenciais.

Compactação de conteúdo: pode compactar o conteúdo antes de entregá-lo aos clientes, reduzindo o uso de largura de banda e acelerando o tempo de carregamento da página para os usuários. Isto é particularmente benéfico para usuários com conexões de Internet mais lentas.

Firewall de aplicativos: adiciona uma camada extra de segurança, inspecionando e filtrando o tráfego de entrada em busca de possíveis ameaças e vulnerabilidades, protegendo contra ataques comuns a aplicativos da web.

Principais usos de um proxy reverso

Logon único (SSO): Os proxies reversos podem facilitar soluções de logon único, permitindo que os usuários acessem vários aplicativos com um único conjunto de credenciais. Isso simplifica a autenticação do usuário e melhora a experiência do usuário.

Gateway de API: os proxies reversos geralmente servem como gateways de API, gerenciando e protegendo a comunicação entre clientes e APIs de backend. Eles podem impor autenticação, autorização e gerenciamento de tráfego para solicitações de API.

Desvantagens de um proxy reverso

Maior Complexidade: A implementação e manutenção desses servidores introduzem complexidade à infraestrutura. A configuração adequada e o gerenciamento contínuo são necessários para uma funcionalidade ideal.

Ponto Único de Falha: Depender de um único proxy reverso cria um ponto potencial de falha. O tempo de inatividade ou problemas com o servidor podem interromper os serviços web, destacando a importância da redundância.

Latência: Em certos cenários, eles podem introduzir latência devido ao processamento adicional. Isso pode atrasar um pouco a comunicação entre clientes e servidores web.

Sobrecarga de recursos: a execução consome recursos, principalmente em ambientes de alto tráfego. É necessária uma alocação suficiente de recursos para uma operação tranquila e eficiente.

VPN vs Proxy

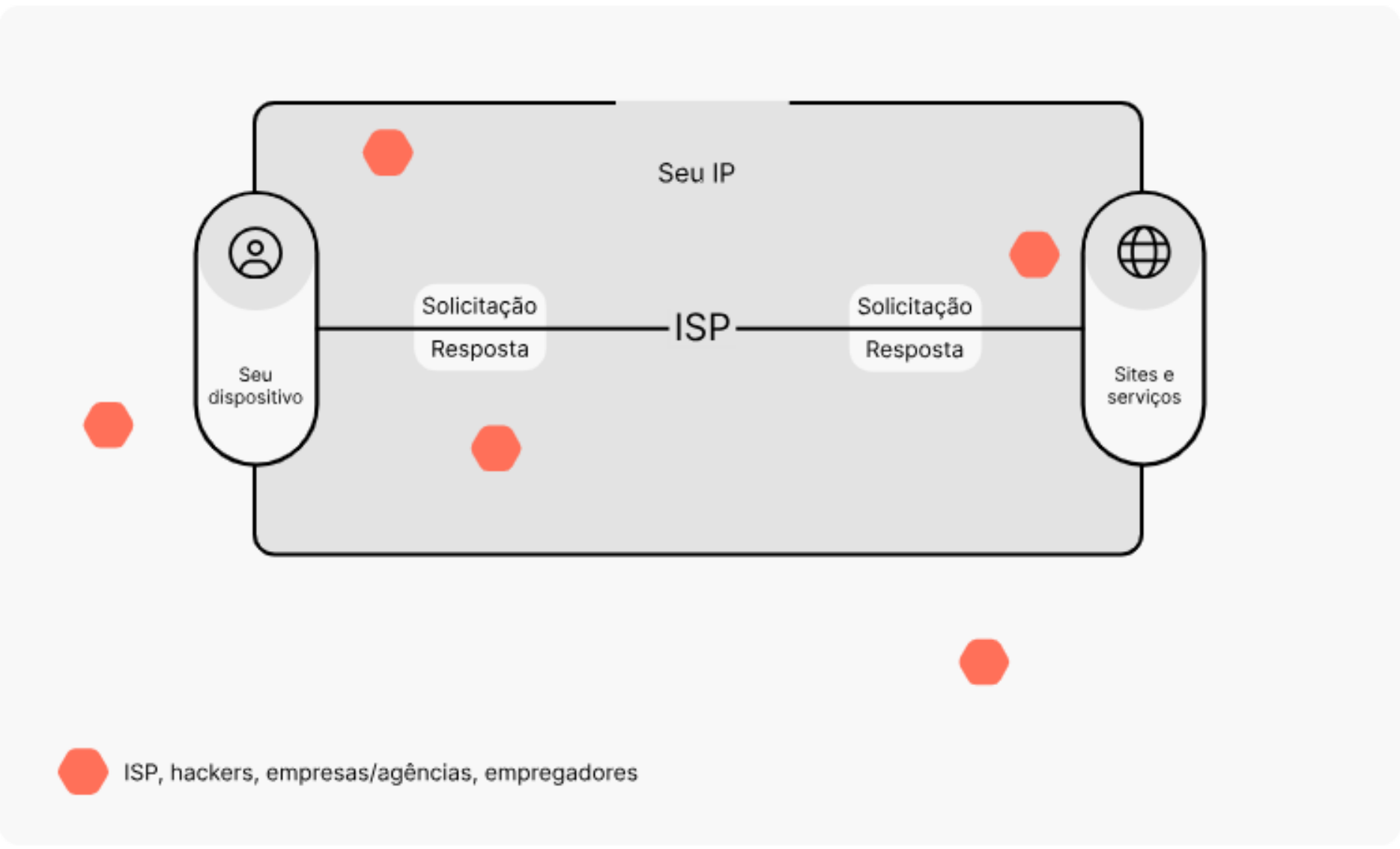
Qual a diferença entre VPN e Proxy?

- Proxies são usados para “ocultar”, “camuflar” sua identidade em interações simples e rotineiras na internet, enquanto que uma VPN protege não só estas interações, mas sua conexão como um todo.
- Um Proxy representa uma simples camada de proteção que oculta seu IP do resto da internet. Já uma VPN não somente oculta seu IP, mas aplica uma camada de proteção extra ao criptografar os dados.
- Além disso, uma VPN protege todos os programas do dispositivo de forma automática, possuindo uma abrangência maior, que vai além do navegador de internet.

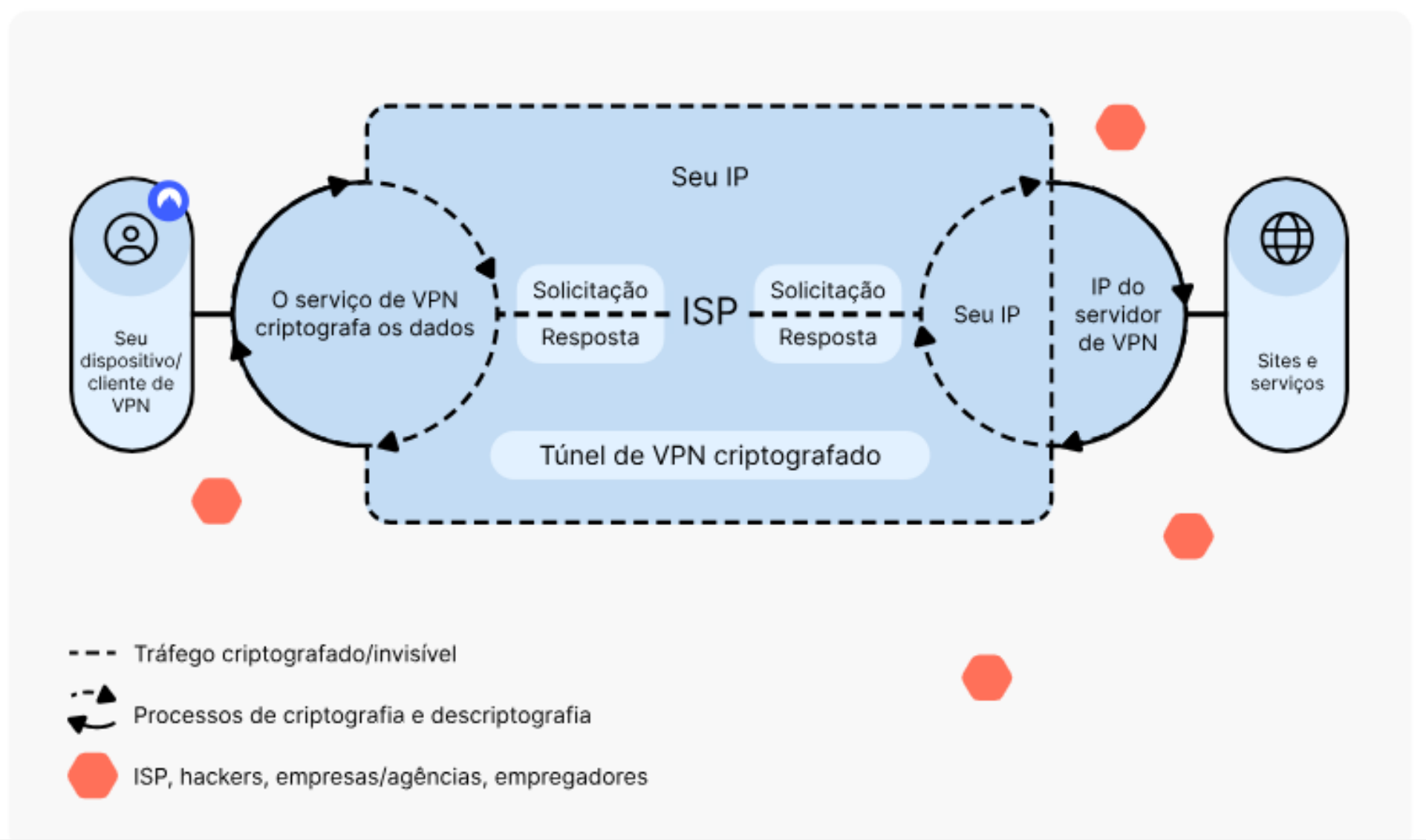
O que a VPN faz?

- Uma VPN redireciona seu tráfego por meio de um servidor remoto, criptografando-o durante o processo. Normalmente, quando você tenta acessar um site, seu ISP (Provedor de Serviços de Internet) recebe a solicitação e redireciona você ao seu destino. Mas quando você se conecta a uma VPN, ela redireciona seu tráfego de Internet por meio de um servidor de VPN primeiro, antes de chegar ao seu destino. Dessa forma, seu ISP não poderá vender todo seu histórico de navegação pelo maior lance.
- Seu IP (e, portanto, sua localização virtual) também permanecerá oculto e você receberá um novo, que pertence ao servidor de VPN, ao qual você estabelecerá uma conexão. Isso garante segurança extra e aumenta significativamente sua privacidade online. Ninguém saberá de qual cidade ou país você está navegando.

Sem VPN


Seu IP
Seu dispositivo
Solicitação
Resposta
ISP
Solicitação
Resposta
Sites e serviços
ISP, hackers, empresas/agências, empregadores

Com VPN


Seu IP
Seu dispositivo/ cliente de VPN
O serviço de VPN criptografa os dados
Solicitação
Resposta
ISP
Solicitação
Resposta
Seu IP
IP do servidor de VPN
Sites e serviços
Túnel de VPN criptografado
Tráfego criptografado/invisível
Processos de criptografia e descriptografia
ISP, hackers, empresas/agências, empregadores

Agradeço
a sua atenção!

Eduardo Verri

eduardo.verri@sptech.school

SÃO PAULO TECH SCHOOL