
nic.br
Núcleo de Informação
e Coordenação do
Ponto BR
cgi.br
Comitê Gestor da
Internet no Brasil
registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Resolvendo os principais incidentes de segurança das redes Brasileiras

Eduardo Barasal Morales
Lucas Jorge da Silva
Tiago Jun Nakamura

cetro.br nic.br cgi.br

Motivação

Perigo: 300 mil rote

apre

atinge 840 Mpps

NOTÍCIAS, TUTORIAIS

Ataque hacker sequestra mais de 200 mil roteadores da MikroTik no Brasil

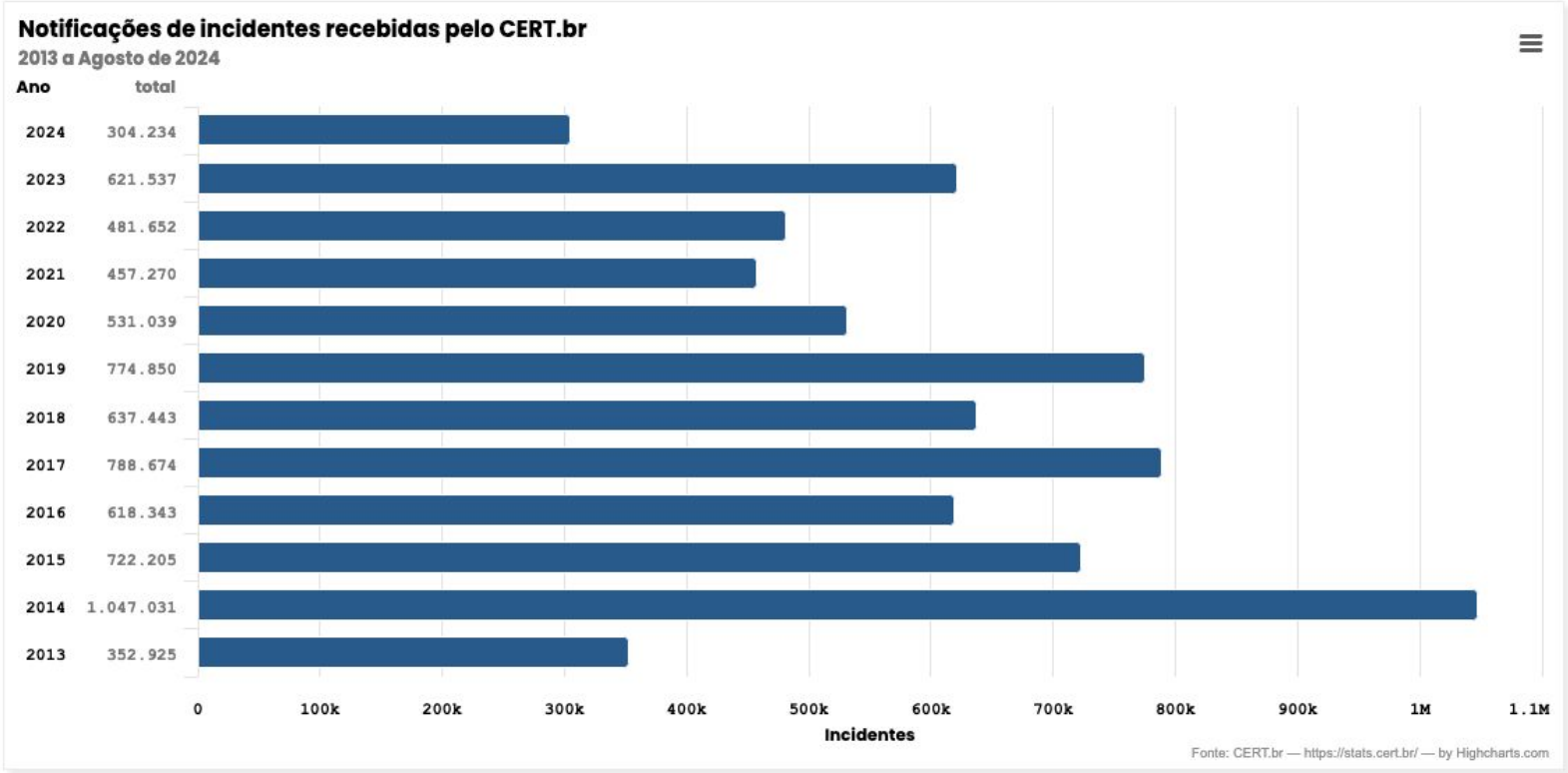
ataque D

constataram uma te

tanto que ataques com capacida

segurança cibernética é de grande preocupaç

Motivação - Incidentes



Motivação - CERT.br

- Notificações aos Sistemas Autônomos
  - Feeds de parceiros
  - **Por email** - cadastro registro.br(**whois**)
- Principais tipos de Notificações
  - **Vulnerabilidades**
    - Zimbra, VMWare, Paloalto, OpenSSH…
  - **Infectados**
    - Microsoft IIS, Mikrotik SOCKS…
  - **Amplificadores** - relacionados a DoS
    - DNS Recursivo, NTP, SNMP, PortMap…

Conceitos básicos sobre Negação de Serviços (DoS)

ceptro.br nic.br cgi.br

O que é Spoofing de endereços?

- Pacotes IP com endereços de origem incorretos
  - **Erro de configuração**
    - Ex: Problema no Software
  - **Teste e Simulação**
    - Ex: Teste de performance
  - **Atitude maliciosa**
    - Esconder a identidade do atacante
    - Fingir ser outro computador na rede
- O spoofing pode ser usado em ataques de negação de serviço e é um problema sério na Internet.

Negação de serviço

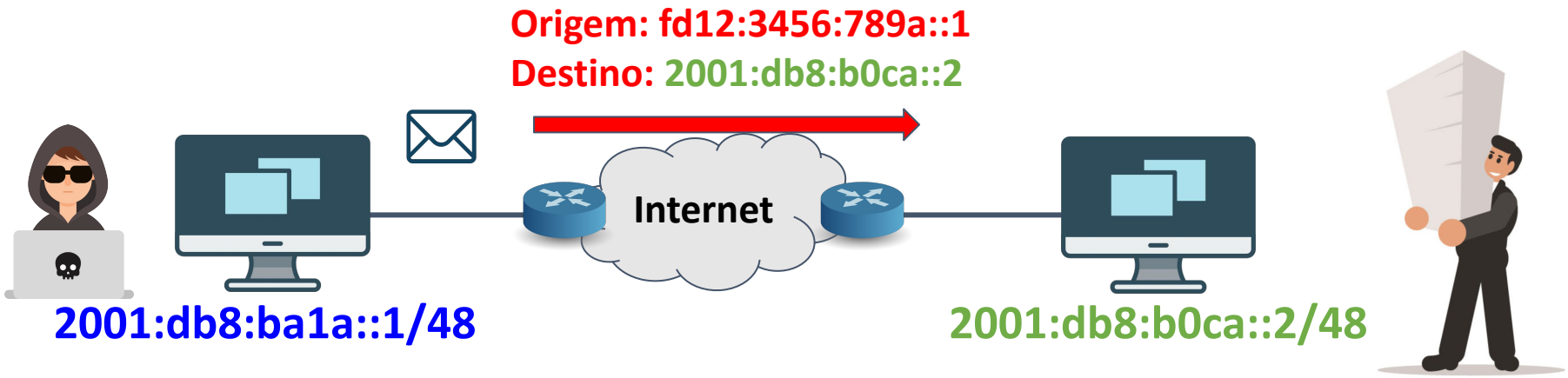
- Técnica pela qual um atacante força a exaustão de recursos e causa indisponibilidade ao alvo.
- 3 tipos básicos
  - Ataques à camada de aplicação
    - Ex: exceder o número máximo de requisições que um servidor Web
  - Ataques de exaustão de recursos de hardware
    - Ex: consumir recursos, como CPU e memória.
  - **Ataques volumétricos**
    - EX: exaurir a banda disponível.

Negação de serviço (DoS 1)

- Ataque **Direto**!
- Usa um endereço de IP reservado, não alocado!

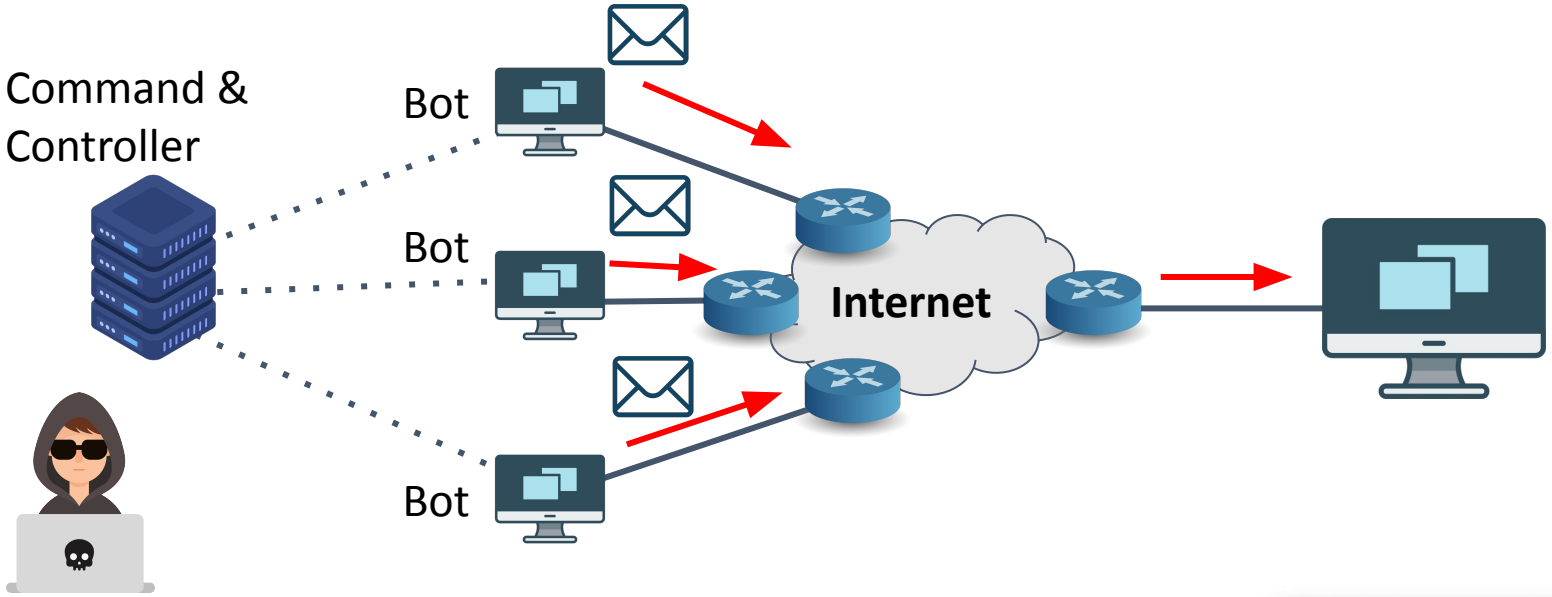
Negação de serviço (DoS 1)

- Ataque **Direto**!
- Exemplo: PING da morte!



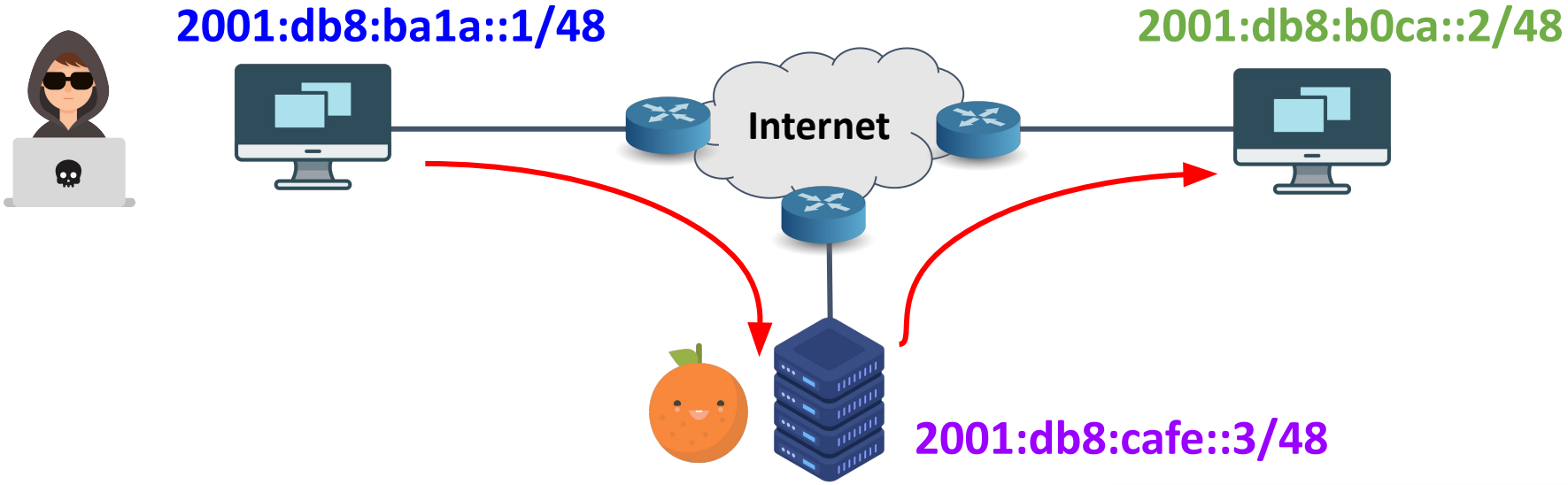
Negação de serviço (DoS 2)

- Ataque Direto e **Distribuído** (**DDoS**)!
- Ex: Ataque de Botnet!



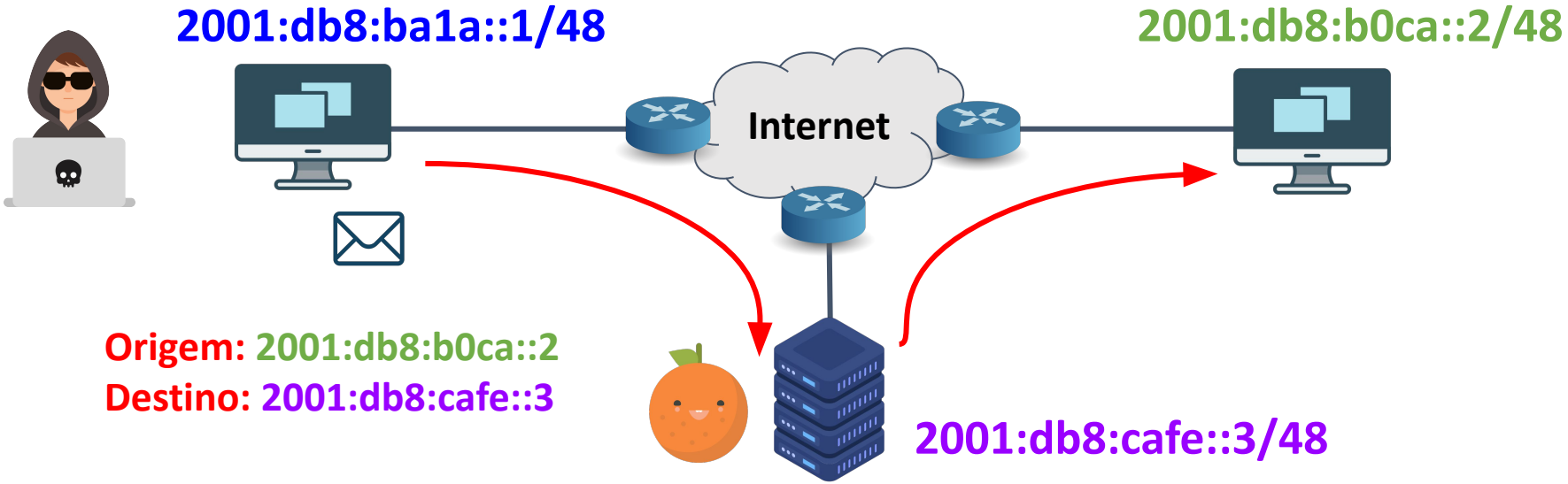
Negação de serviço (DoS 3)

- Ataque **Reflexivo**!
- Utiliza um terceiro para fazer o ataque.



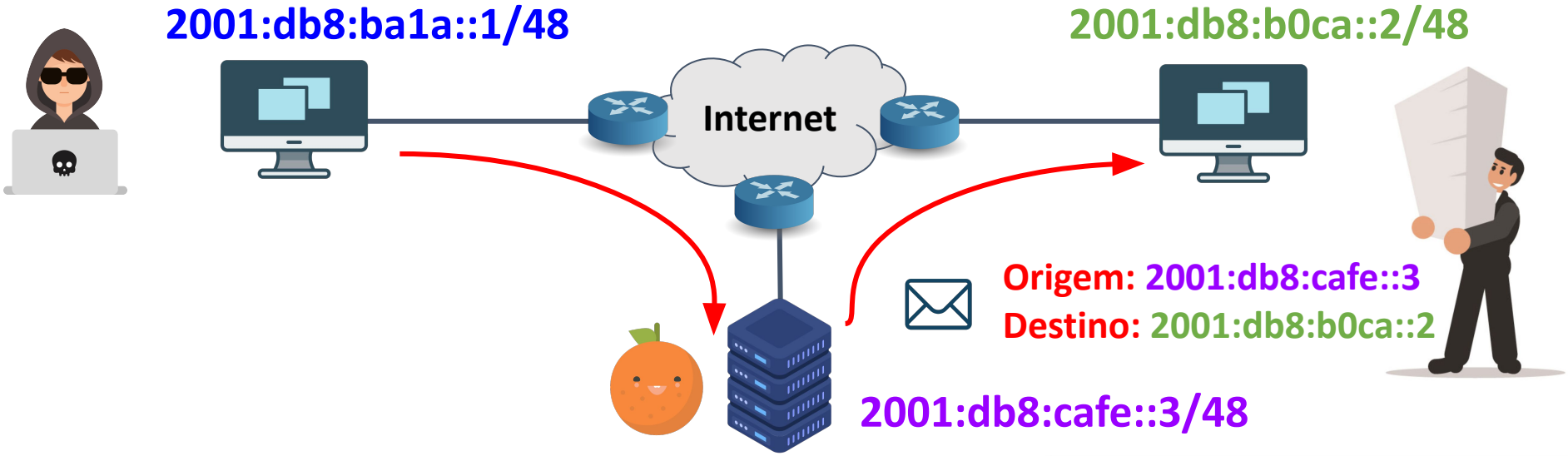
Negação de serviço (DoS 3)

- Ataque **Reflexivo**!
- Utiliza um terceiro para fazer o ataque.



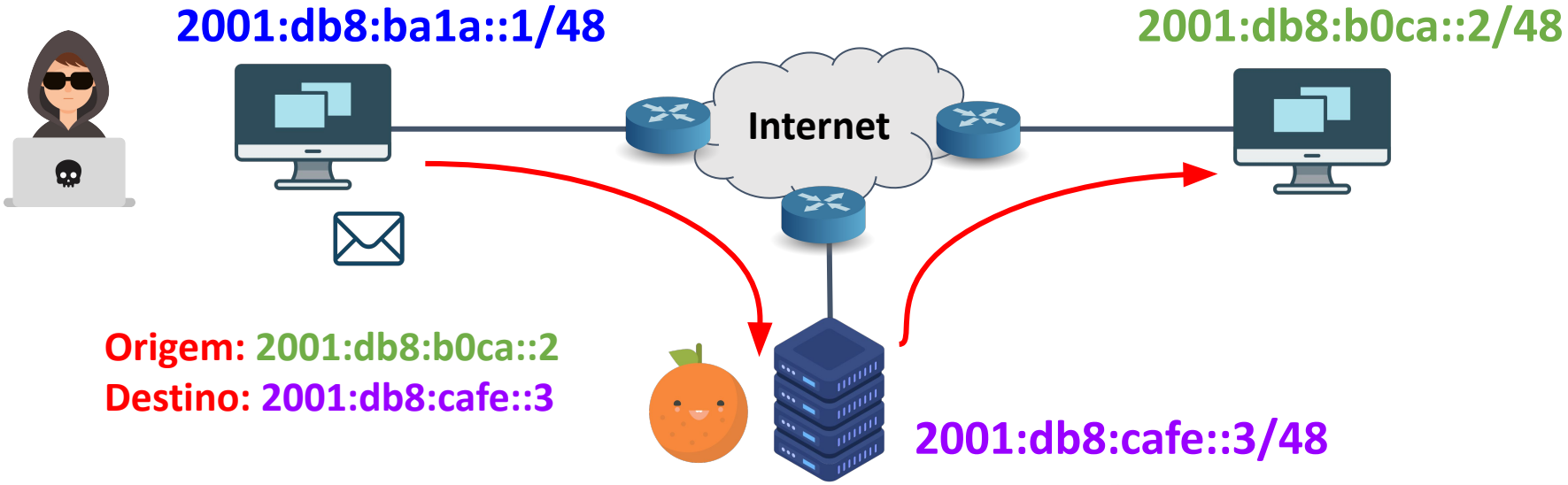
Negação de serviço (DoS 3)

- Ataque **Reflexivo**!
- Utiliza um terceiro para fazer o ataque.



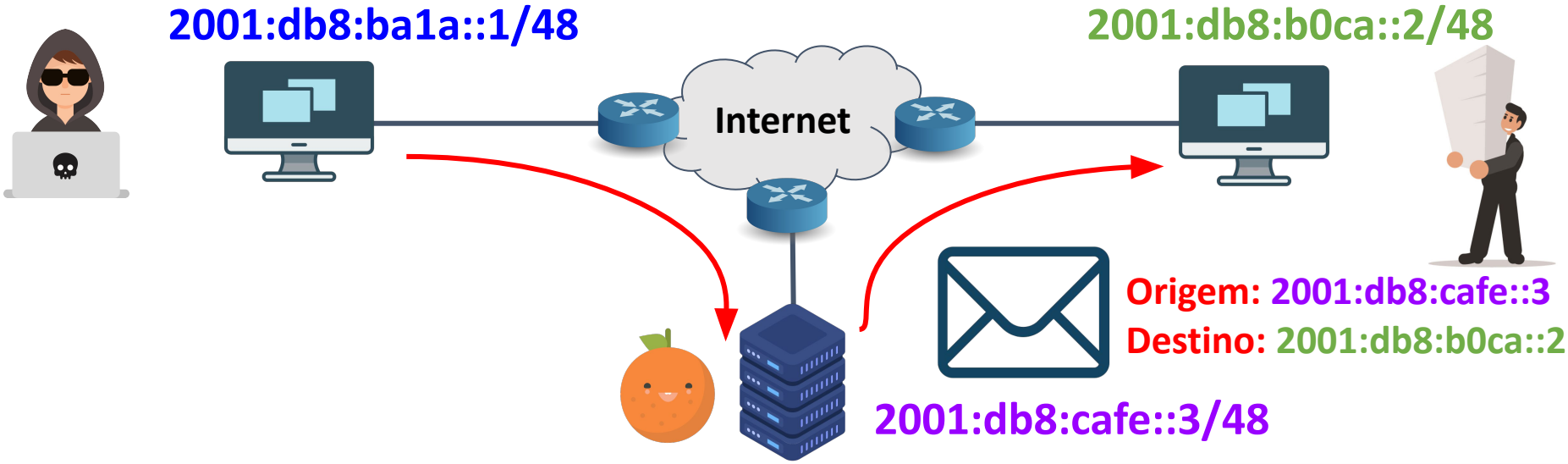
Negação de serviço (DoS 4)

- Ataque Reflexivo e **Amplificado**!
- Um pacote pequeno vira um pacote grande (Normalmente **UDP**).



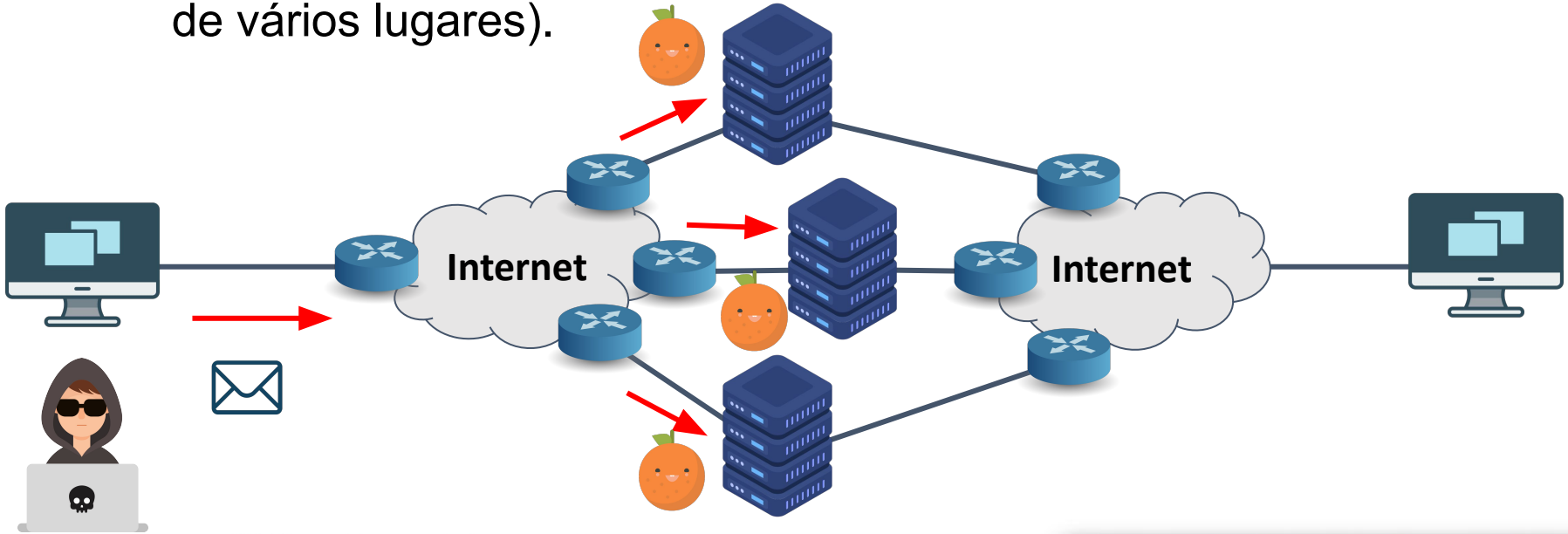
Negação de serviço (DoS 4)

- Ataque Reflexivo e **Amplificado**!
- Um pacote pequeno vira um pacote grande (Normalmente **UDP**).



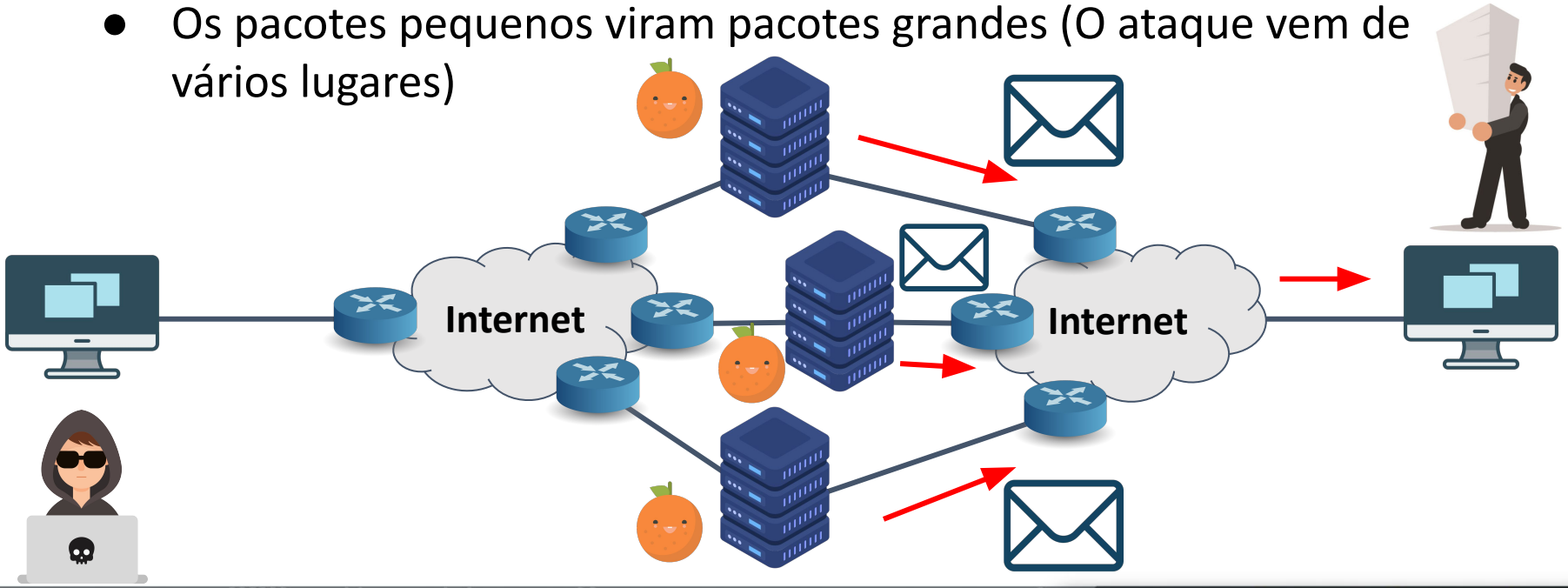
Negação de serviço (DoS 5)

- Ataque Reflexivo, Amplificado e **Distribuído** (**DDoS**)!
- Os pacotes pequenos viram pacotes grandes (O ataque vem de vários lugares).



Negação de serviço (DoS 5)

- Ataque Reflexivo, Amplificado e **Distribuído** (**DDoS**)!
- Os pacotes pequenos viram pacotes grandes (O ataque vem de vários lugares)



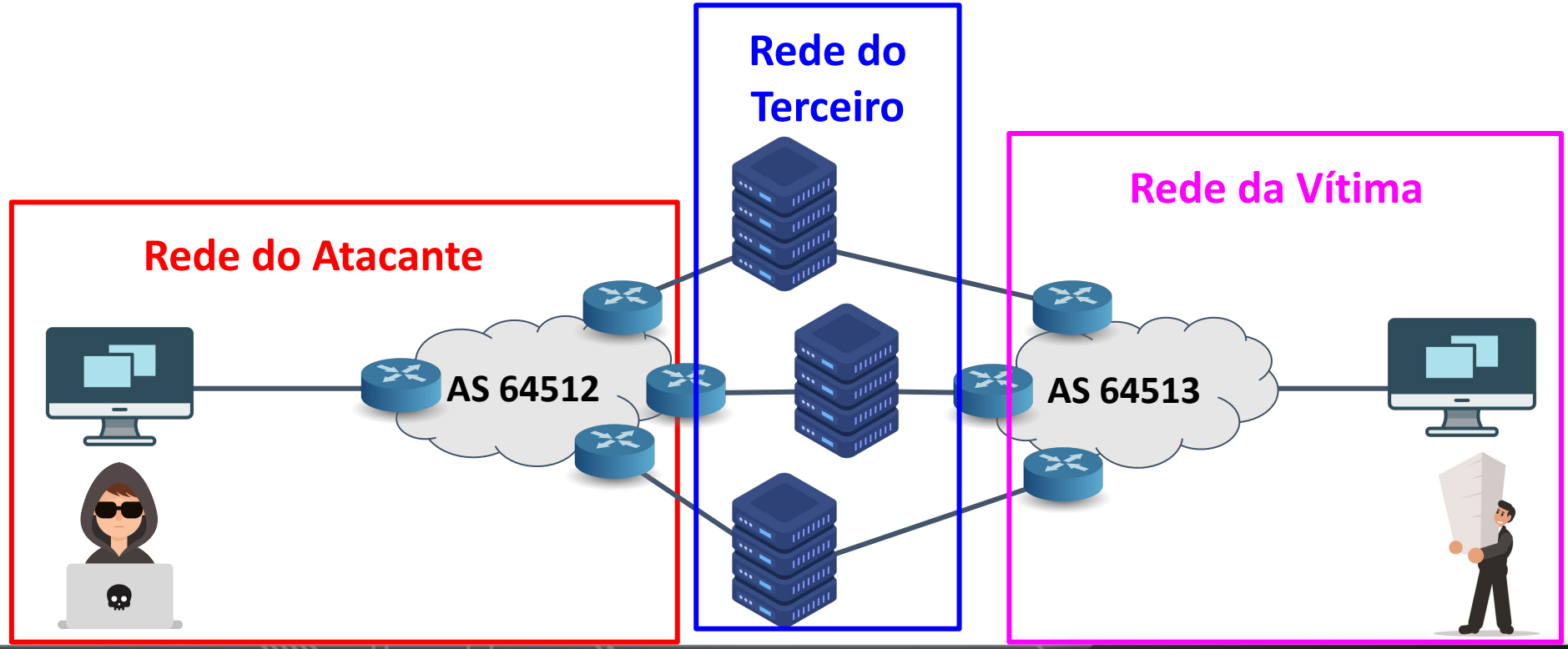
Laboratório 1 - Ataque de DoS usando Spoofing de Endereço

ceptro.br nic.br cgi.br

Resolvendo os Ataque de Negação de Serviço

ceptro.br nic.br cgi.br

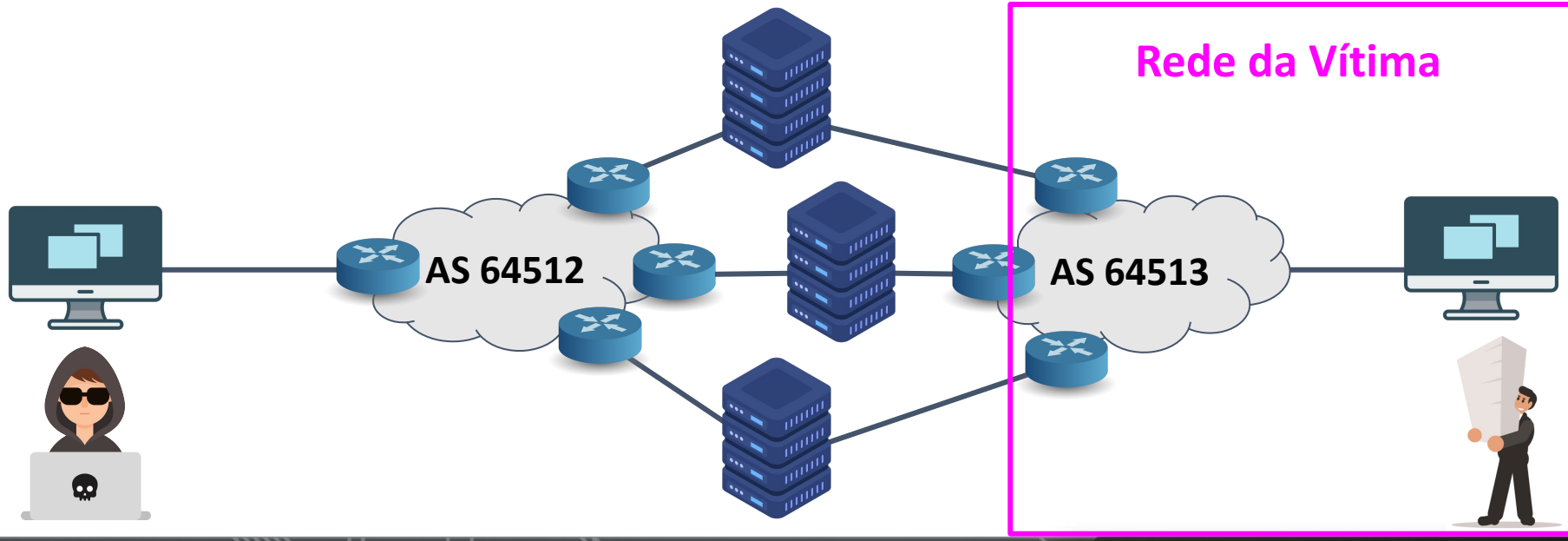
Analisando os 3 cenários



Rede da Vítima:
O que fazer?

ceptro.br nic.br cgi.br

Rede da Vítima



Rede da Vítima

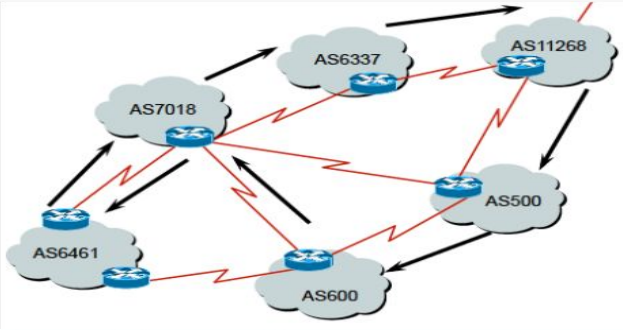
- Comprar uma máquina que faz **limpeza do tráfego**
  - Investimento alto $$$
- Contratar uma **empresa de mitigação** de ataque
  - Investimento razoável, normalmente com custo mensal.
- Utilizar filtros de **Blackhole** (RTBH)
  - Funciona quando o ataque é direcionado a poucos IPs
- Se for um serviço específico
  - Pode se colocar este serviço em uma empresa que **distribui este conteúdo** em vários lugares como **CDNs**

Rede da Vítima: Vulnerabilidade no Roteador que opera o BGP

- **BGP - Border Gateway Protocol**
  - Protocolo de Roteamento usado para trocar informações sobre caminhos entre diferentes redes (ASes diferentes)
  - Usado no backbone da Internet pelos ASes
  - Baseado em sessões TCP (porta 179)
  - Do tipo “path vector”- vetor de caminhos

```
12.6.126.0/24   207.126.96.43   1021   0        6461 7018 6337 11268 i
```

AS Path



Notificação do CERT.br

- Notifica os roteadores com serviços que estão abertos (**179/tcp**) para o mundo.
  - Problema principal
    - Afetar o serviço BGP ou o roteador, prejudicando a operação do Sistemas Autônomos.

Notificação do CERT.br

- **Resolvendo o Problema**
  - Recomenda-se que sejam **implementadas ACLs para que o serviço BGP** seja acessível somente aos roteadores que necessitem estabelecer uma sessão BGP com este equipamento.
- **Como posso ter certeza que resolvi o problema?**
  - De uma **rede externa**, tente executar o comando:
    - **nc -v -z IP_BGP 179**
  - O resultado esperado é uma **mensagem de erro**, que não foi possível conectar na porta 179/tcp.

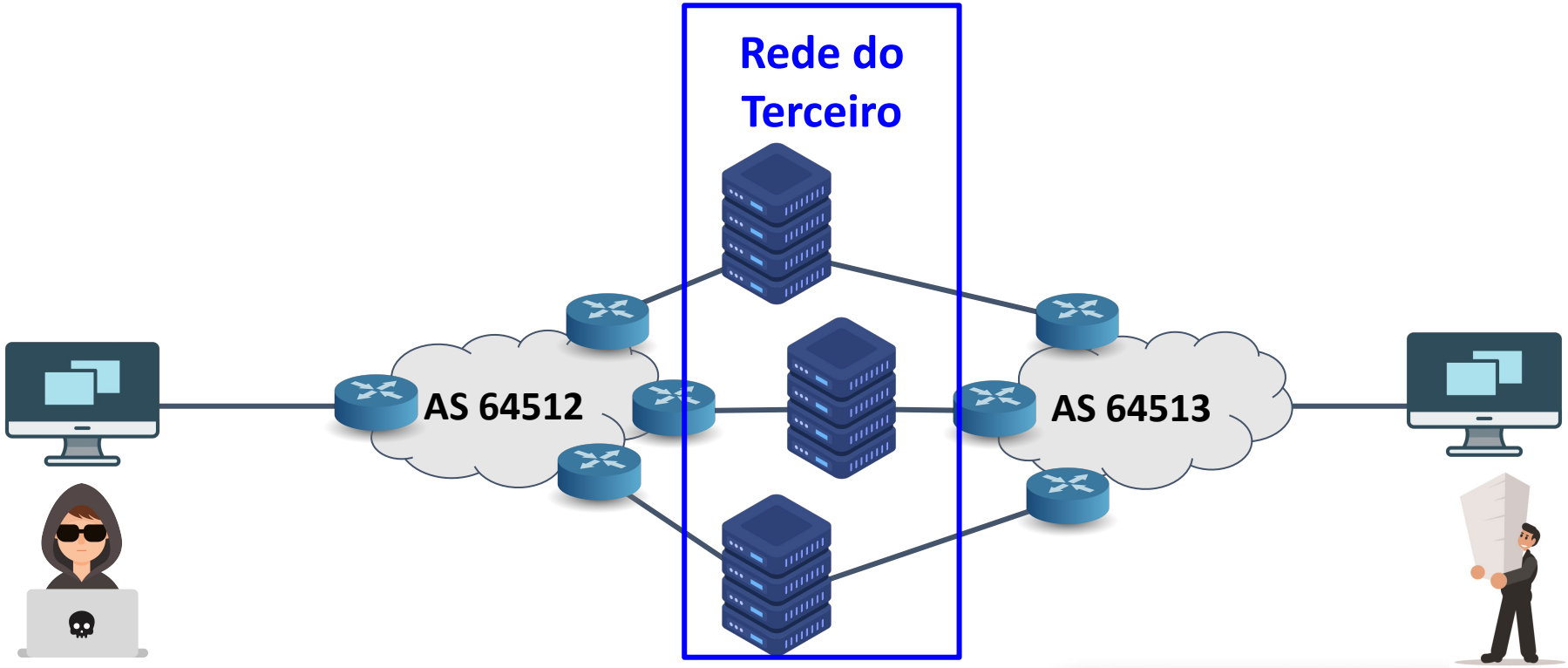
Laboratório 2 - Protegendo o roteador que opera o BGP

ceptro.br nic.br cgi.br

Rede de Terceiro
O que fazer?

ceptro.br nic.br cgi.br

Rede do Terceiro



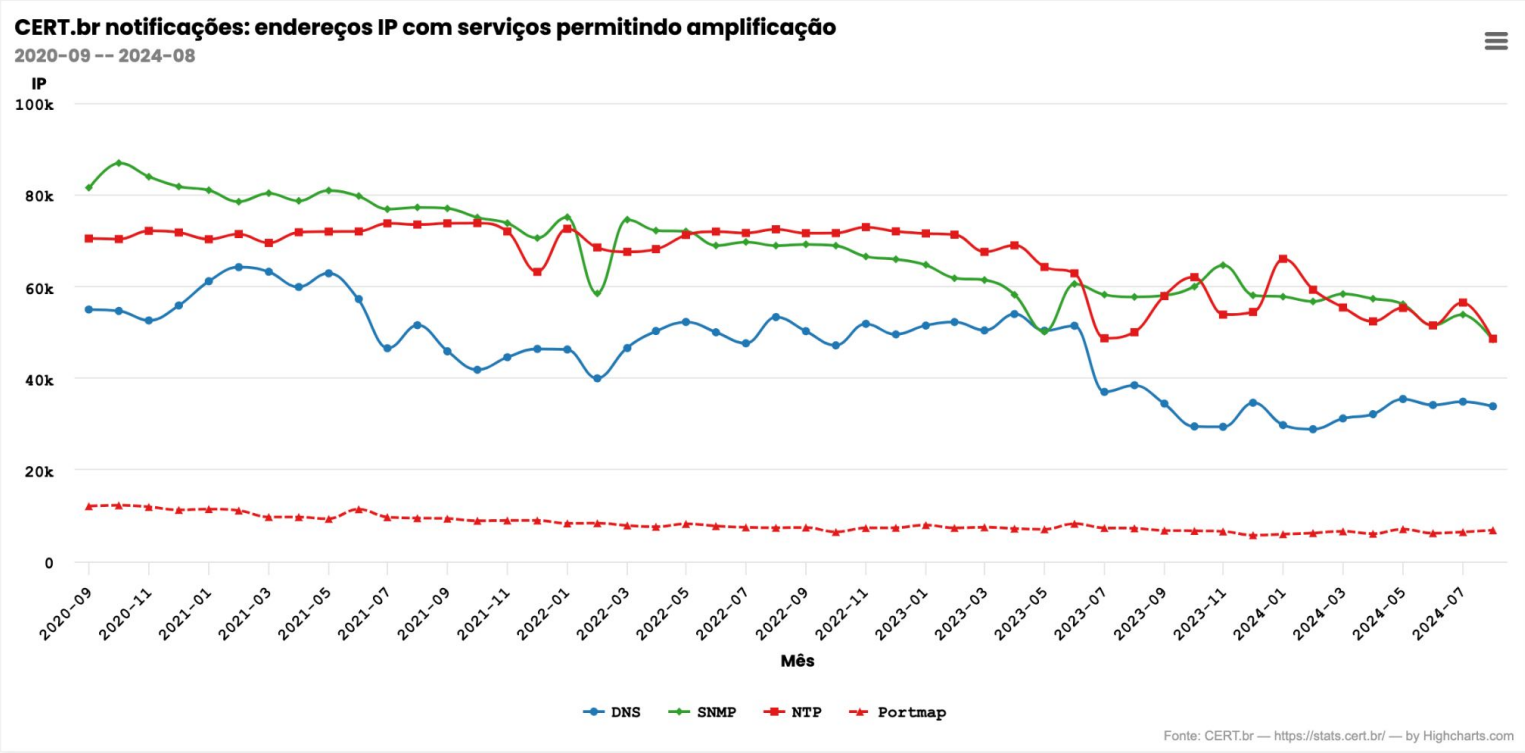
Rede do Terceiro

- Todo protocolo que possui funcionamento pergunta pequena e resposta grande pode ser utilizado.
- O Cert.br notifica diversos serviços que podem ser explorados para fazer ataques amplificados.
  - Podemos categorizar em 3 tipos:
    - **Serviços abertos para o mundo** (que deveriam ser privados) - Ex: DNS recursivo
    - **Má configuração do serviço** (comandos que não deveriam estar habilitados) - Ex: NTP monlist
    - **Serviços que não deveriam ser utilizados**(desatualizados e antigos) - Ex: Chargen

Principais serviços explorados

	DNS		SNMP		NTP		Portmap	
Mês	ASN	IP	ASN	IP	ASN	IP	ASN	IP
2024-01	2.937	29.754	3.539	57.760	1.174	66.012	1.333	5.964
2024-02	3.081	28.861	3.497	56.705	1.175	59.278	1.304	6.214
2024-03	3.104	31.210	3.537	58.352	1.176	55.404	1.300	6.593
2024-04	3.060	32.137	3.502	57.329	1.171	52.376	1.252	6.068
2024-05	3.119	35.435	3.497	56.128	1.160	55.305	1.254	7.056
2024-06	3.125	34.131	3.315	51.510	1.230	51.497	1.240	6.192
2024-07	3.156	34.863	3.480	53.841	1.162	56.477	1.319	6.428
2024-08	3.153	33.847	3.445	48.436	1.179	48.602	1.298	6.832

Principais serviços explorados



Fatores de amplificação

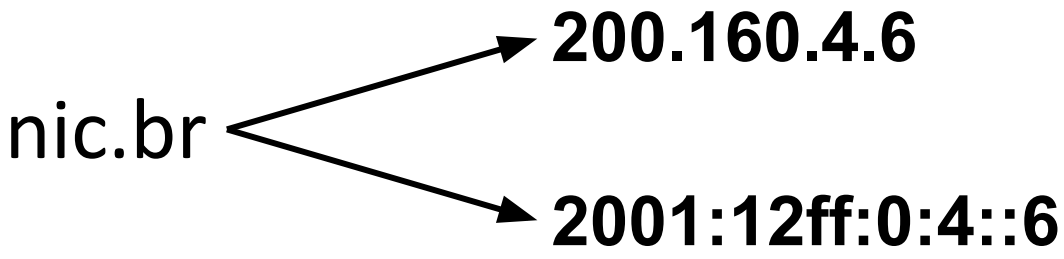
Protocolo	Fator de Amplificação	Comando Vulnerável
DNS	28 a 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
LDAP / CLDAP	46 a 70	Malformed request
SSDP	30.8	SEARCH request
Chargen	358.8	Character generation request

Rede de Terceiro
DNS Recursivo

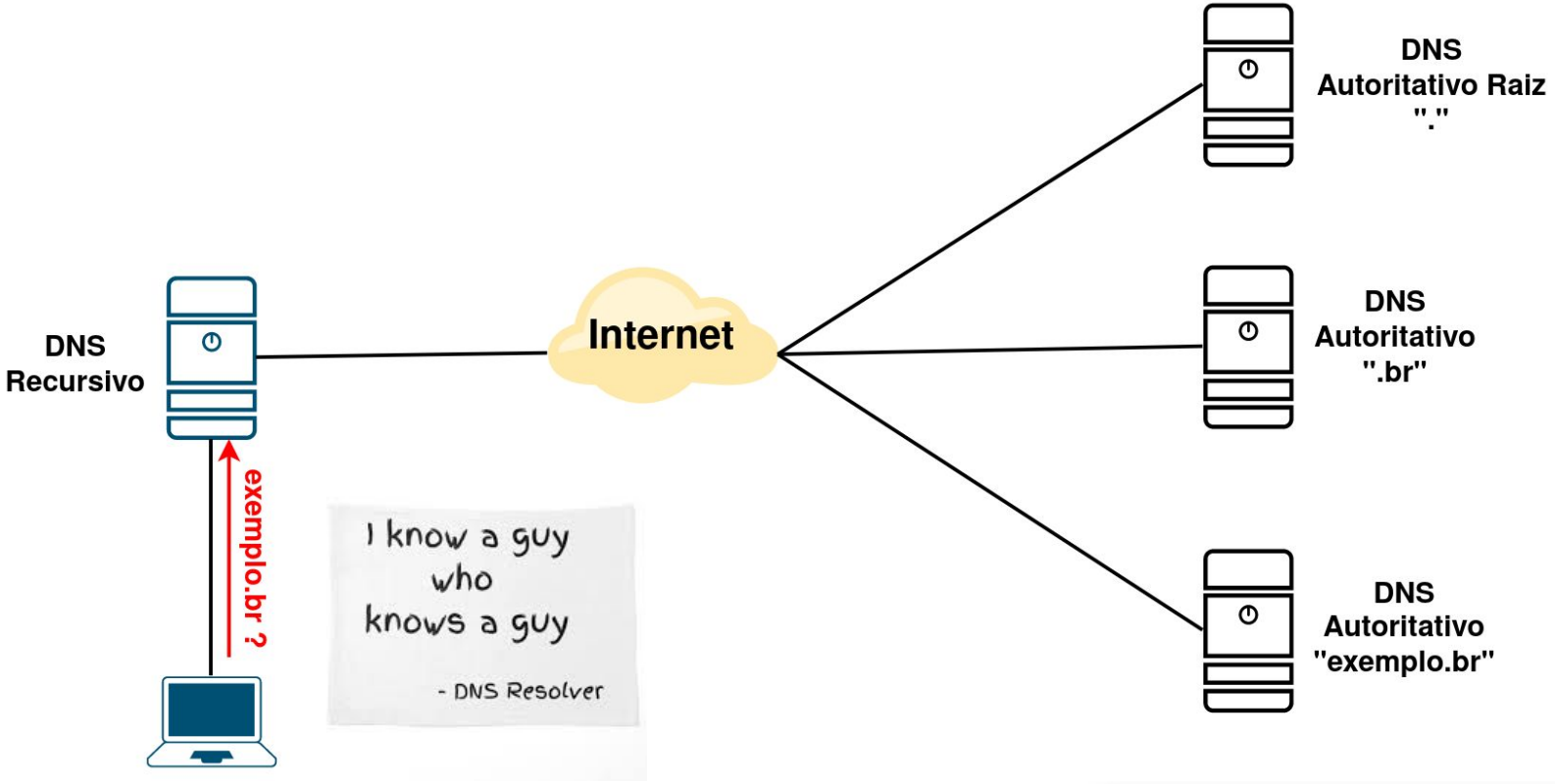
ceptro.br nic.br cgi.br

DNS

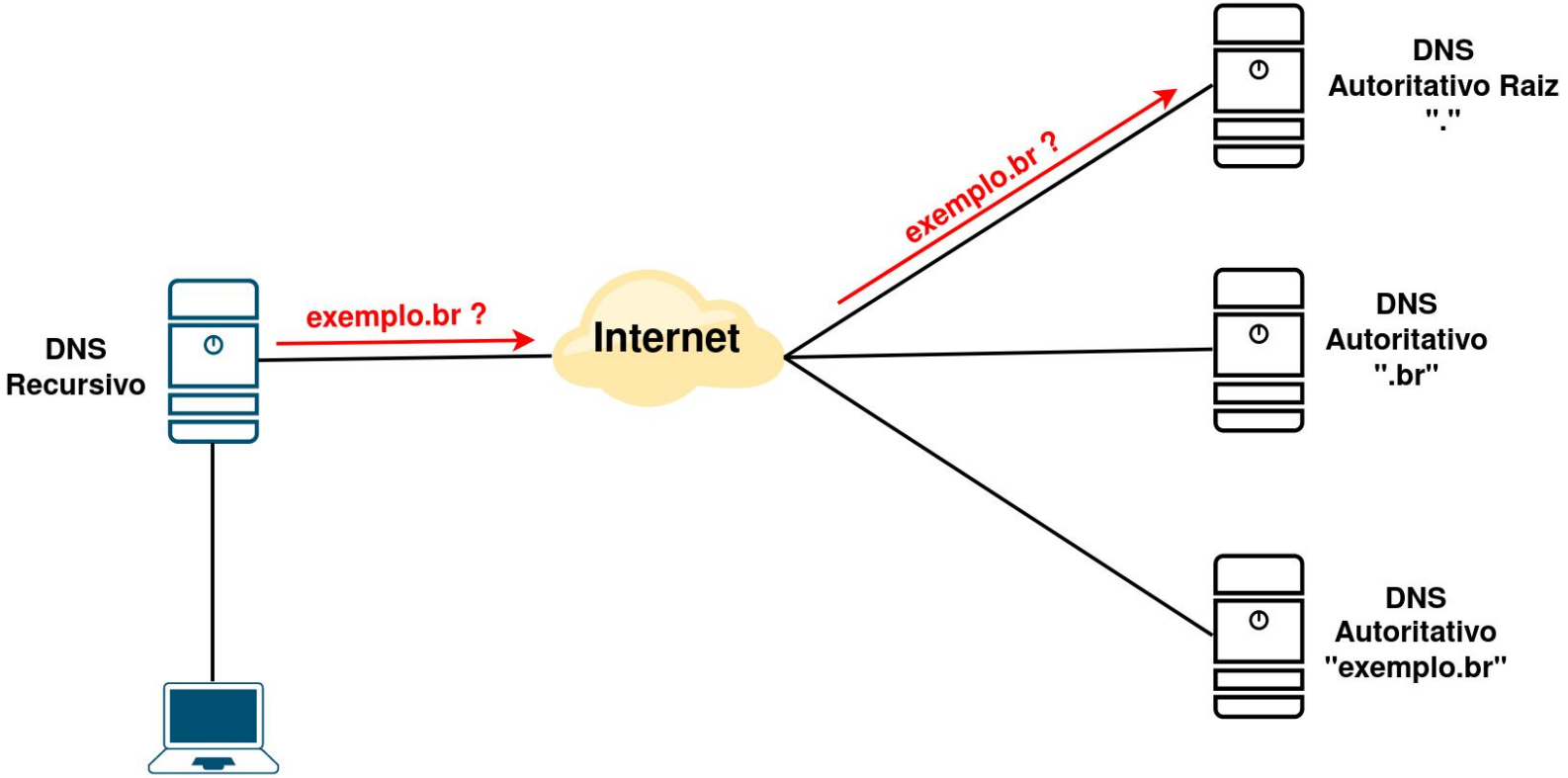
- Domain Name System (DNS)
  - Sistema que associa nomes a endereços IPs



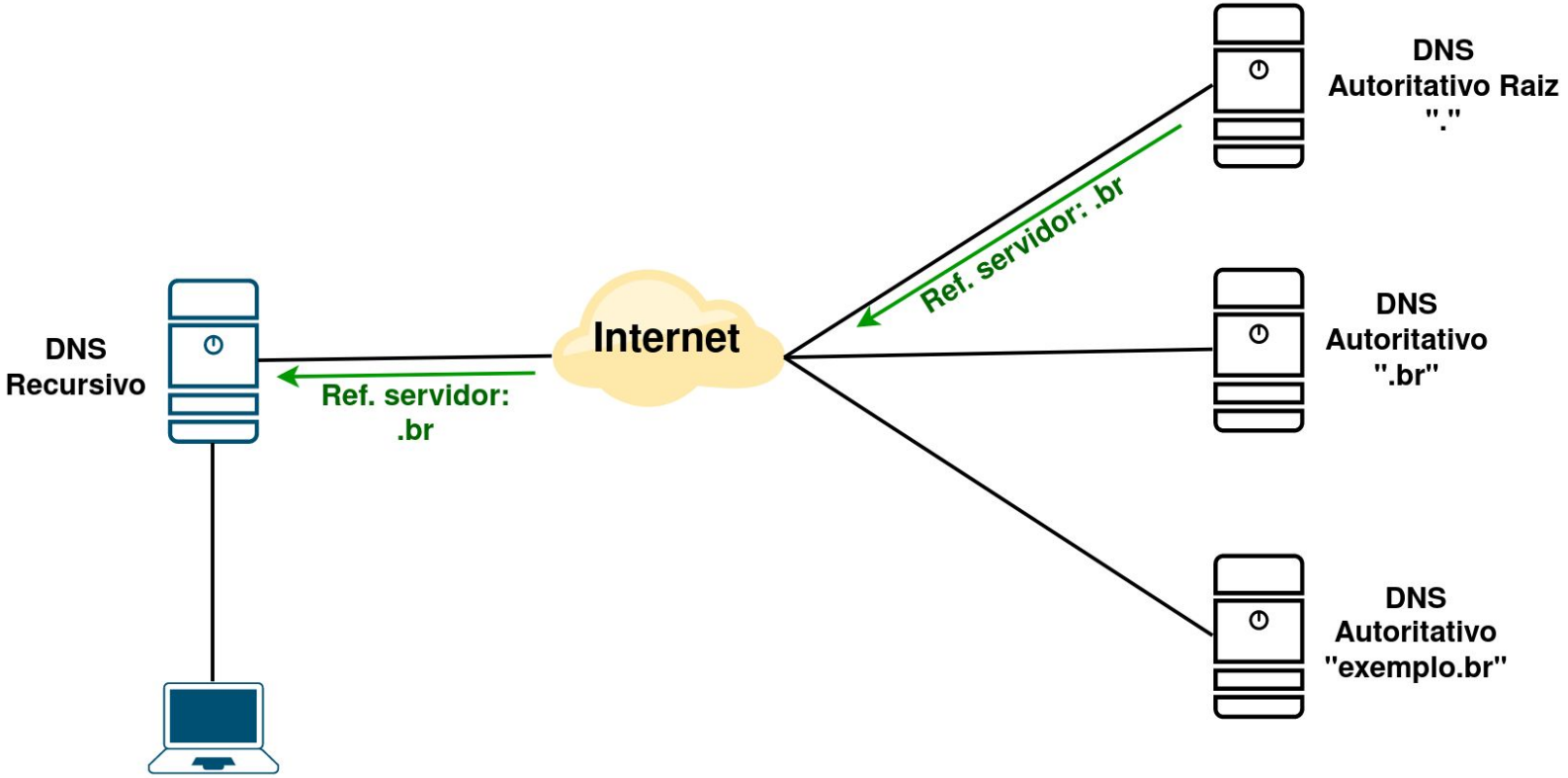
Funcionamento do DNS



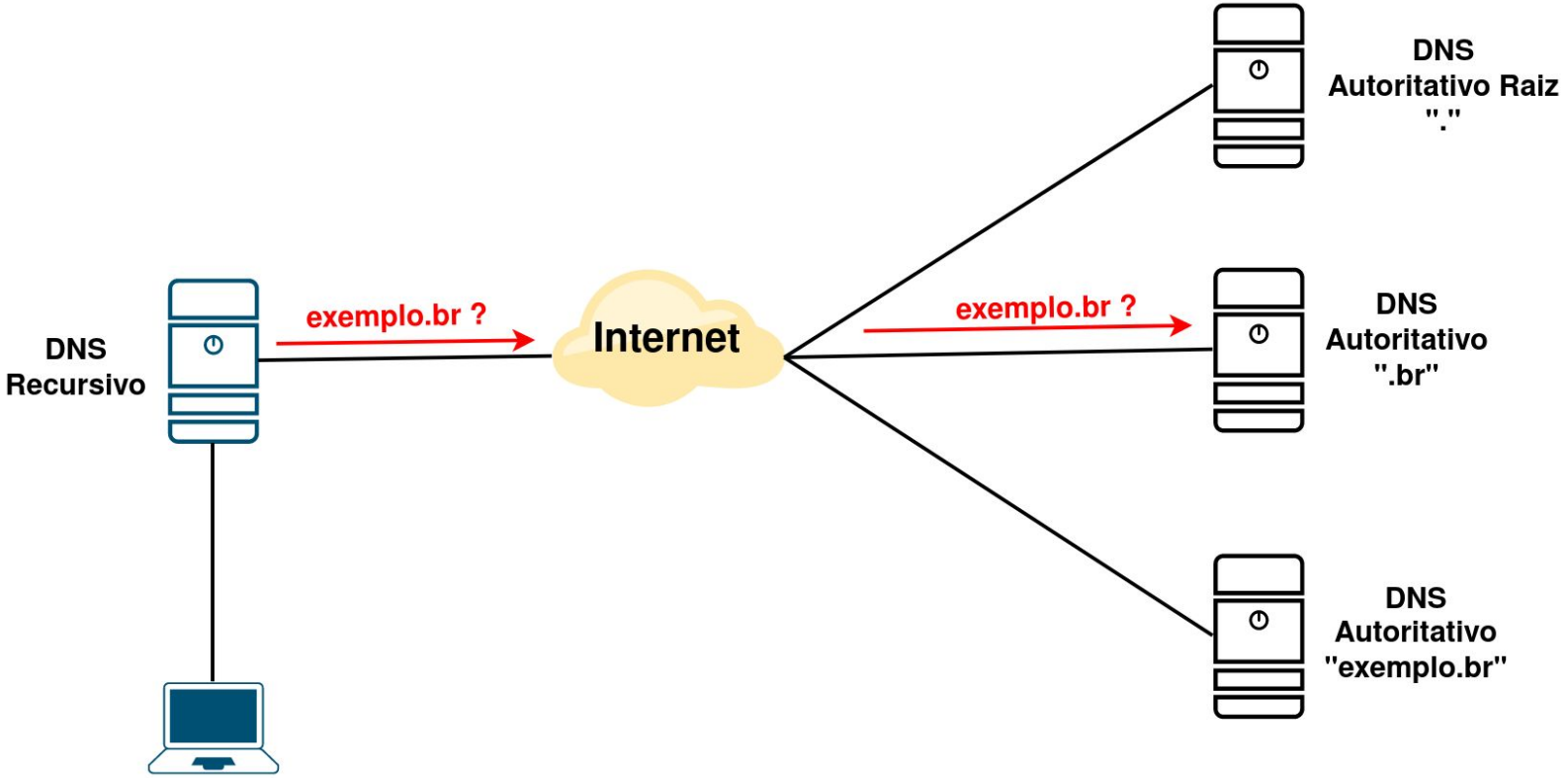
Funcionamento do DNS



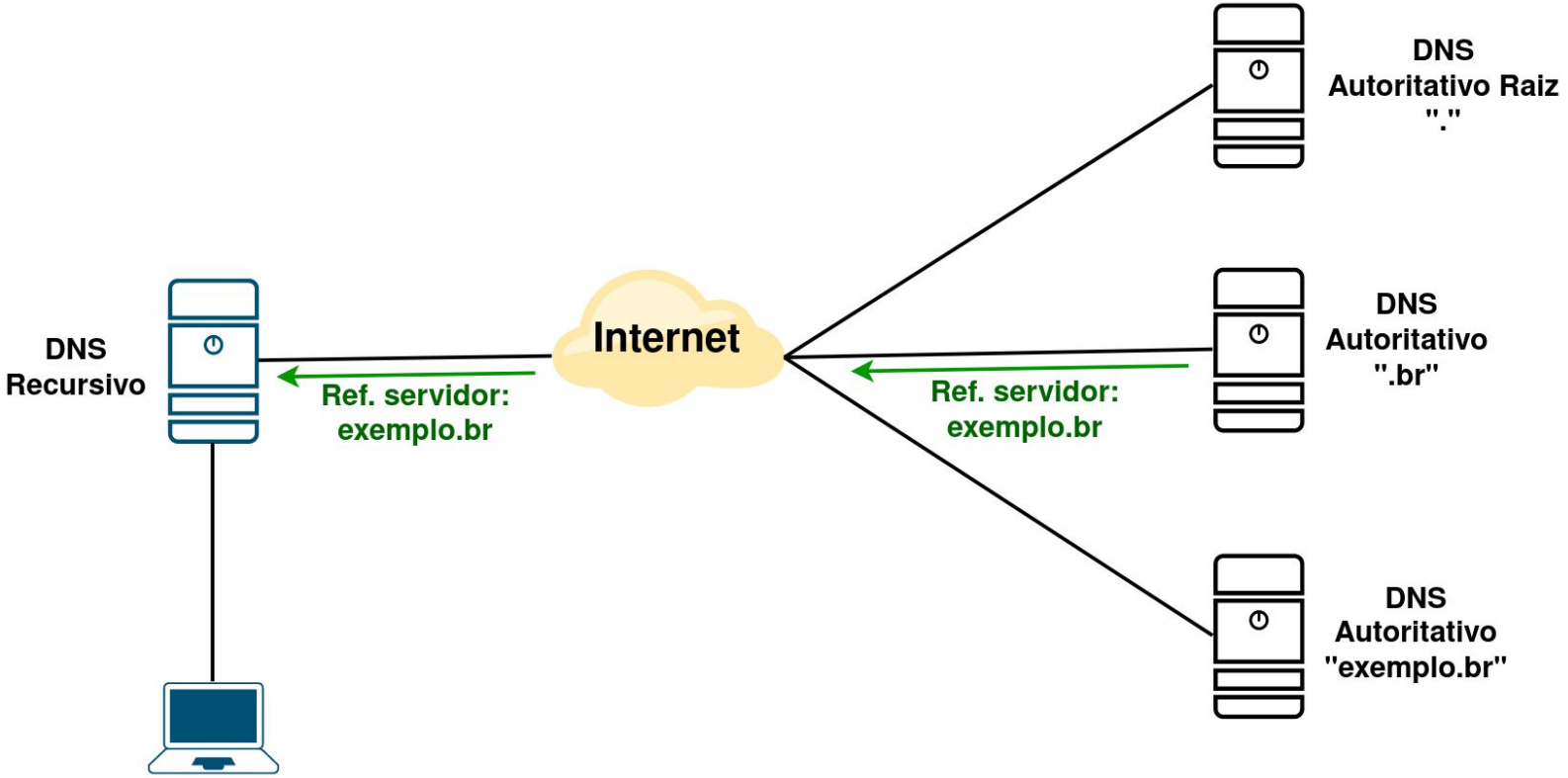
Funcionamento do DNS



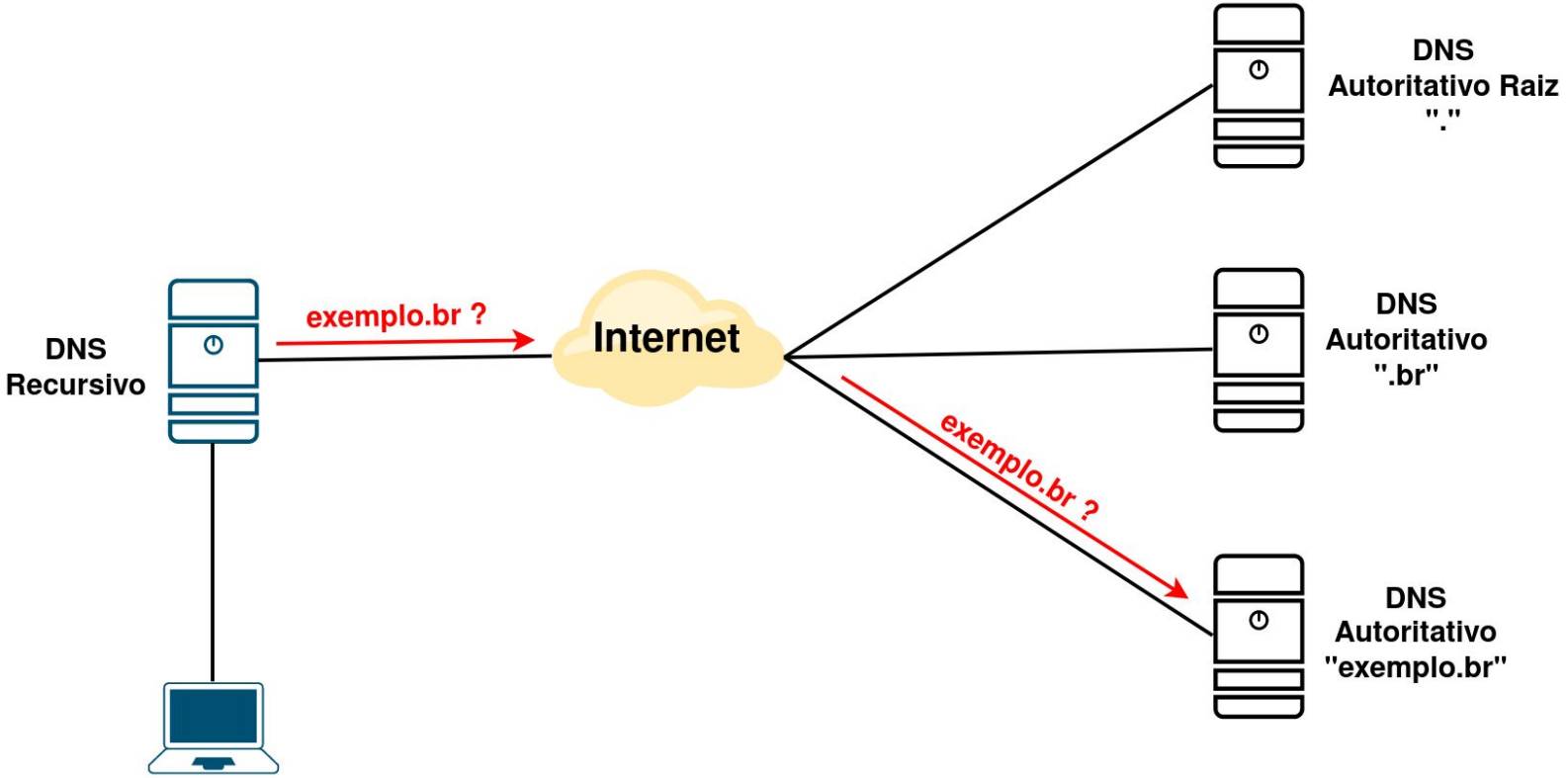
Funcionamento do DNS



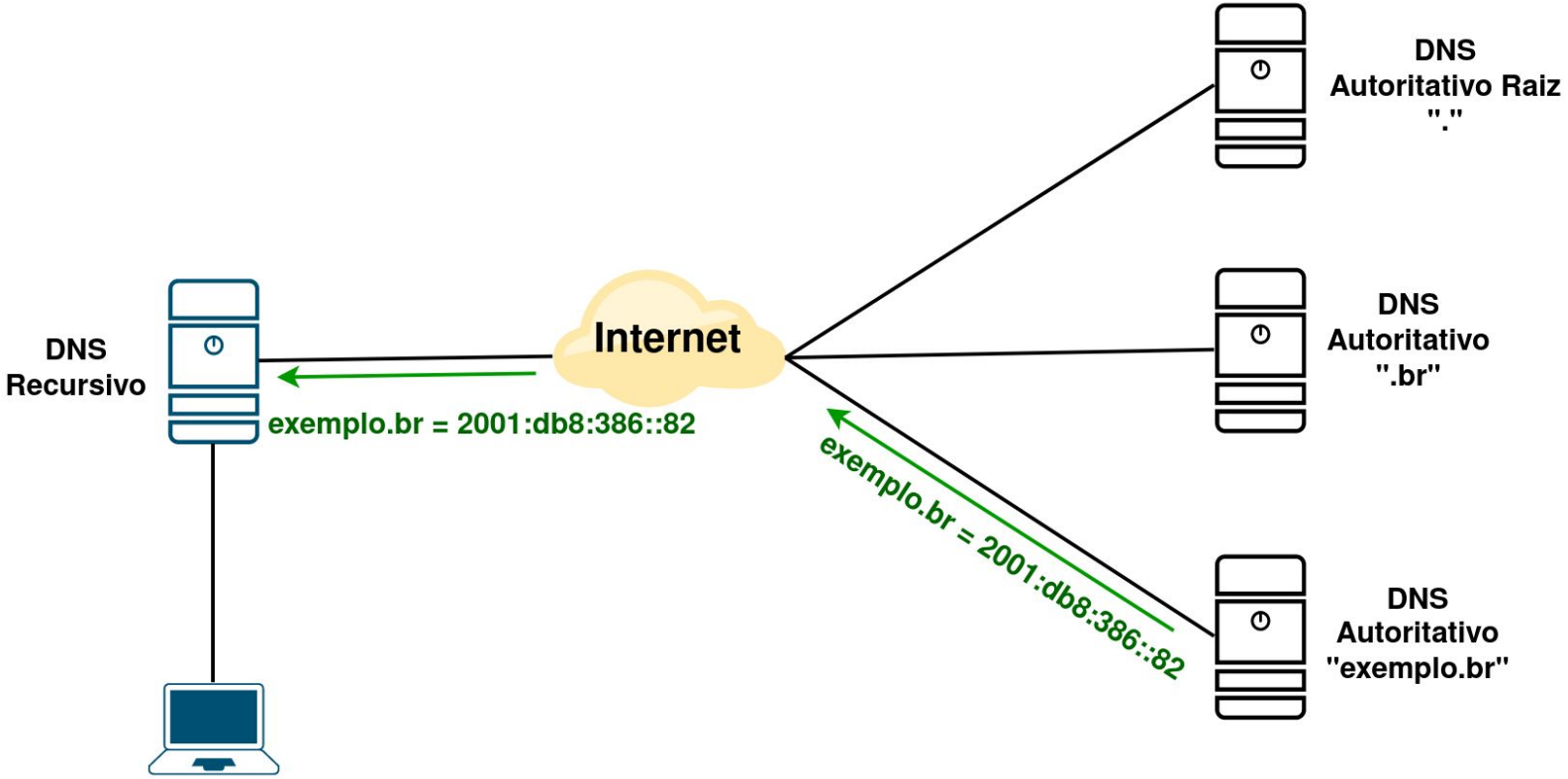
Funcionamento do DNS



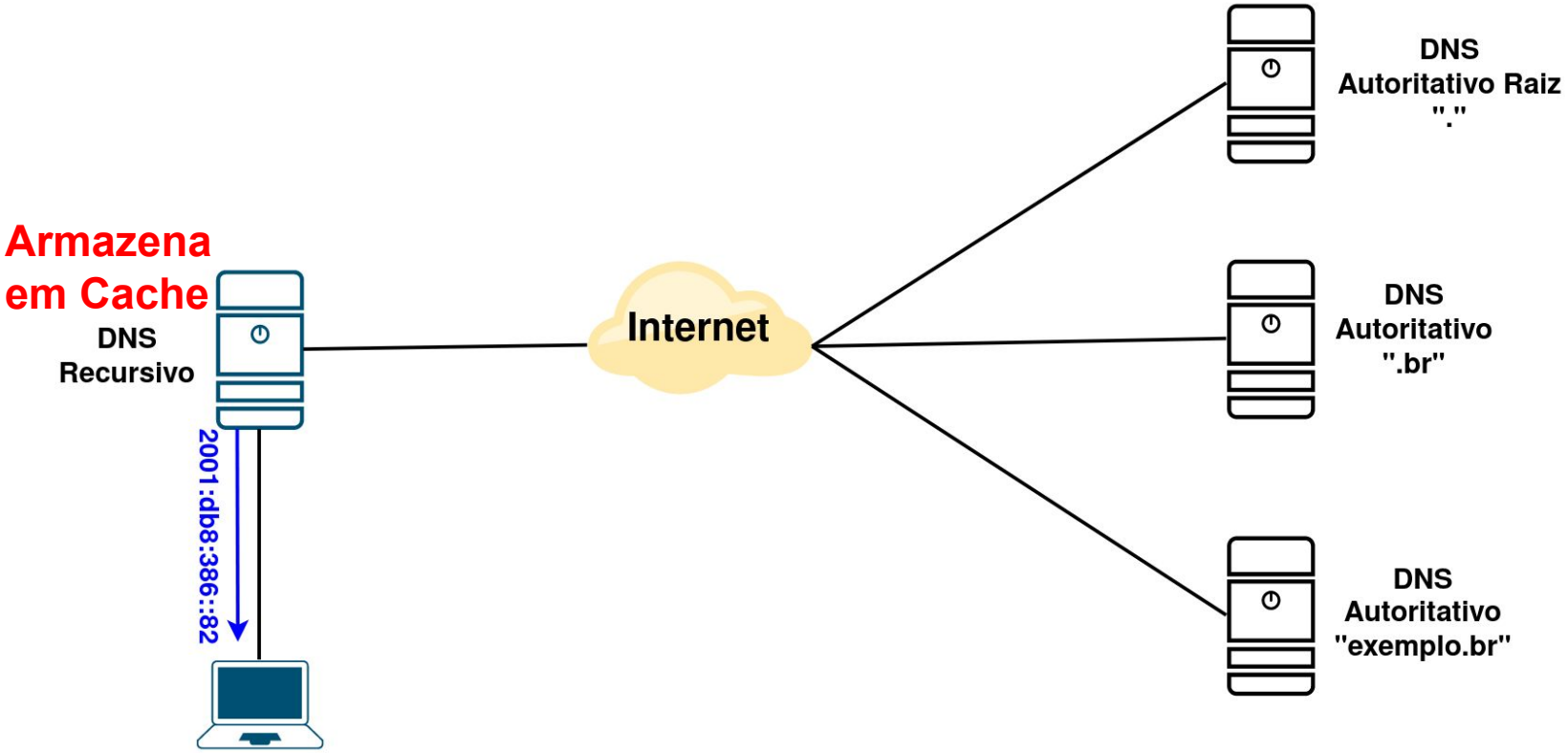
Funcionamento do DNS



Funcionamento do DNS



Funcionamento do DNS



DNS Recursivo

- Também conhecido como "Resolver";
- Servidor responsável por encontrar o endereço IP do nome pedido;
- Faz consultas aos servidores autoritativos;
- Possui cache das informações consultadas.

DNS Recursivo

- 3 formas de operação:
  - **Privado**
    - Empresas(usuário final)
  - **Privado compartilhado**
    - Provedores(ISP)
  - **Público**
    - Google
    - Cloudflare
    - Quad9

KINDNS

- Knowledge-Sharing and Instantiating Norms for DNS and Naming Security
- Promover boas práticas de segurança de DNS
  - Ajuda operadores de DNS a se proteger
  - Medidas simples que se realizadas evitam vulnerabilidades
  - Guias de Configuração

An ICANN Initiative

Notificação do CERT.br

- Notifica os **DNS Recursivo Privado ou Compartilhado** que estão **abertos** (**53/udp**) para o **mundo**.
- Lembrar que outros equipamentos podem estar com a função de DNS recursivo sem que você saiba.
- **Resolvendo o Problema**
  - Restringindo o acesso ao DNS Recursivo aos seus clientes.
  - https://cert.br/docs/whitepapers/dns-recursivo-aberto/
- **Como posso ter certeza que resolvi o problema?**
  - Teste https://www.openresolver.nl/

Laboratório 3 - Utilizando Firewall no Servidor DNS Recursivo

ceptro.br nic.br cgi.br

Laboratório 4 - Mitigando o Problema apenas com configuração do BIND

ceptro.br nic.br cgi.br

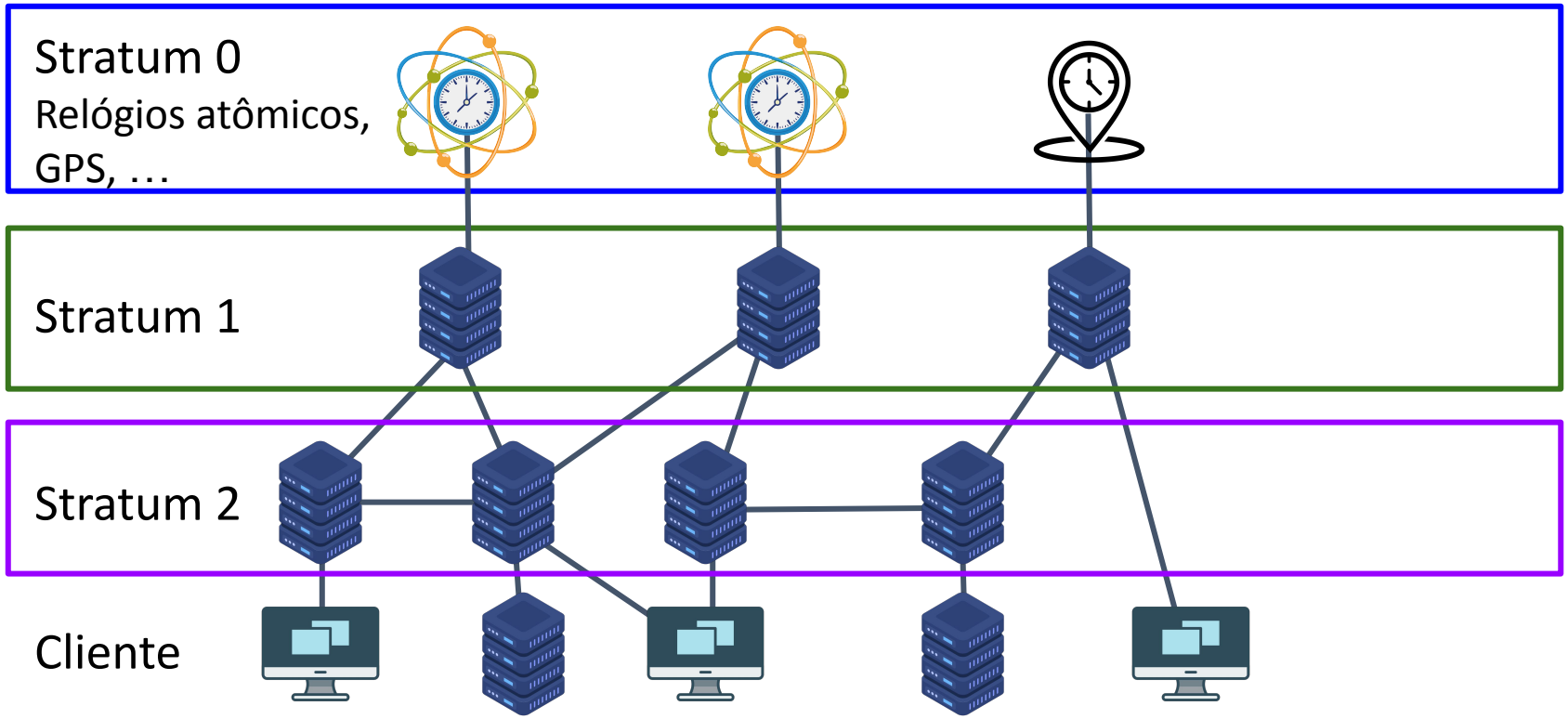
Rede de Terceiro
NTP

ceptro.br nic.br cgi.br

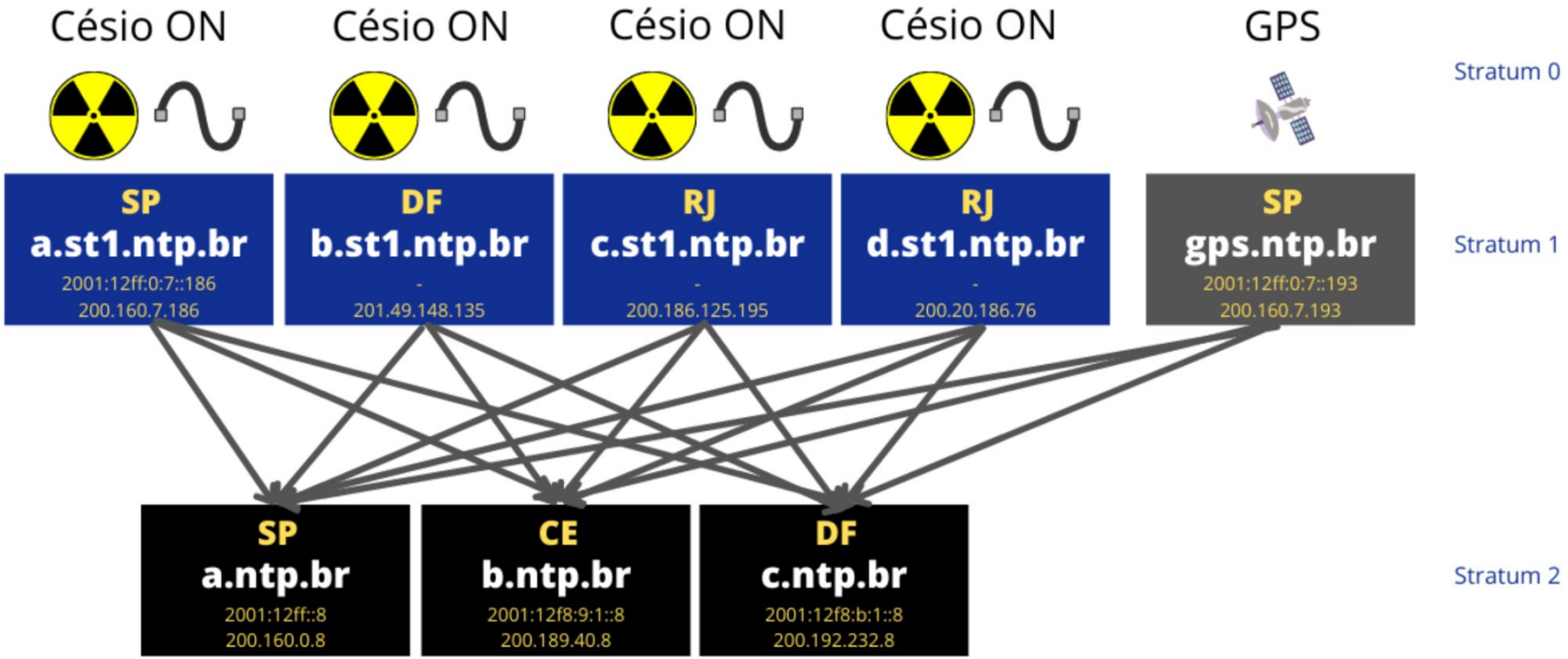
NTP

- Network Time Protocol
- Opera com a sincronização dos relógios dos dispositivos
  - Topologia hierárquica de servidores de tempo (dividida em stratums ou estratos);
  - Servidor (fornece o tempo) e Cliente (consulta o tempo).

NTP


Stratum 0
Relógios atômicos,
GPS, …
Stratum 1
Stratum 2
Cliente

NTP.br


Césio ON
Césio ON
Césio ON
Césio ON
GPS
Stratum 0
SP
a.st1.ntp.br
2001:12ff:0:7::186
200.160.7.186
DF
b.st1.ntp.br
-
201.49.148.135
RJ
c.st1.ntp.br
-
200.186.125.195
RJ
d.st1.ntp.br
-
200.20.186.76
SP
gps.ntp.br
2001:12ff:0:7::193
200.160.7.193
Stratum 1
SP
a.ntp.br
2001:12ff::8
200.160.0.8
CE
b.ntp.br
2001:12f8:9:1::8
200.189.40.8
DF
c.ntp.br
2001:12f8:b:1::8
200.192.232.8
Stratum 2

Notificação do CERT.br

- Notifica os servidores NTPs (**123/udp**) mal configurados.
  - Comandos com problemas:
    - **monlist**
      - Serve para debugging - requisita uma lista de máquinas com quem daemon NTP se comunicou recentemente.
    - **readvar**
      - Mensagem de controle - requisita uma lista de variáveis de configurações de sistema de um daemon NTP.
- Lembrar que outros equipamentos podem estar com a função de servidores NTPs sem que você saiba.

Notificação do CERT.br

- **Resolvendo o Problema**
  - Se você não for utilizar um servidor NTP na sua rede desabilite o serviço;
  - Desabilite os comandos "monlist" e "readvar"
    - Inclua no **ntpd.conf** as seguintes linhas:
      - **disable monitor**
      - **restrict default kod notrap nomodify nopeer noquery**
      - **restrict -6 default kod notrap nomodify nopeer noquery**
    - Ou no caso do monlist, instale a versão 4.2.7p26 ou mais atual, que não possui o comando.

Notificação do CERT.br

- **Como posso ter certeza que resolvi o problema?**
  - Você pode verificar seu servidor através dos seguintes comandos: (preferencialmente execute-os a partir da Internet, ou seja, fora de uma rede interna que tenha permissão de acesso ao servidor).
  - **$ ntpdc -n -c monlist SERVIDOR_NTP**
  - **$ ntpq -c rv SERVIDOR_NTP**

Laboratório 5 - Resolvendo o problema do abuso do NTP

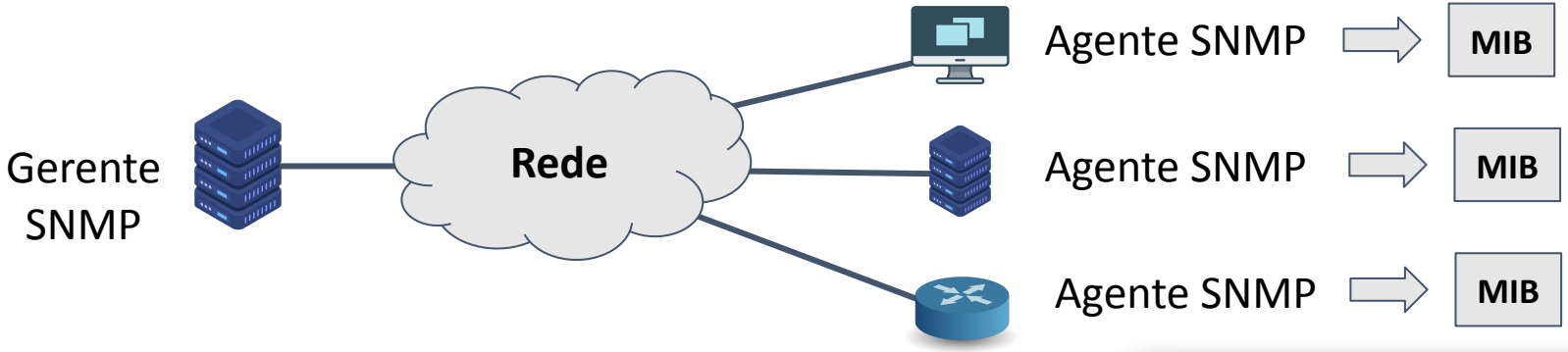
ceptro.br nic.br cgi.br

Rede de Terceiro
SNMP

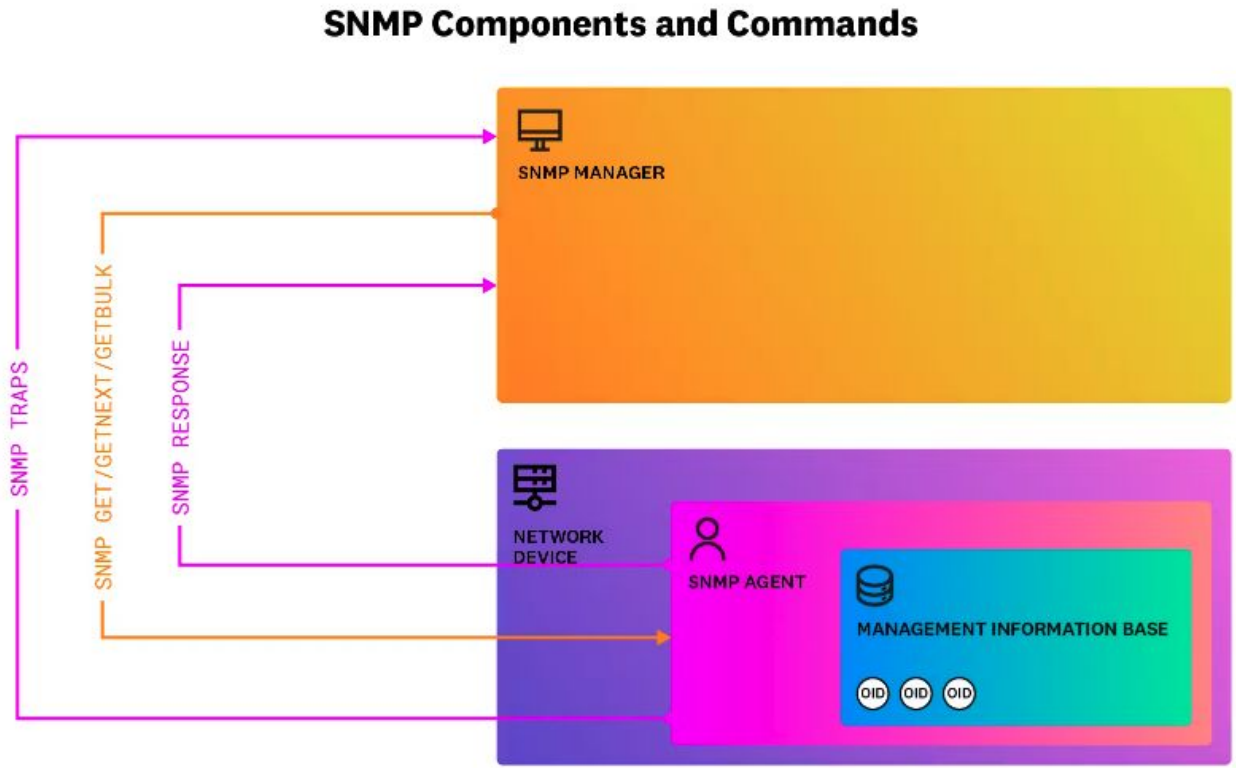
ceptro.br nic.br cgi.br

SNMP

- Simple Network Management Protocol
- Utilizado para gerenciamento e diagnóstico de dispositivos de redes:
  - Opera no modelo Gerente-Agente



SNMP


SNMP Components and Commands
SNMP MANAGER
SNMP TRAPS
SNMP GET/GETNEXT/GETBULK
SNMP RESPONSE
NETWORK DEVICE
SNMP AGENT
MANAGEMENT INFORMATION BASE
OID
OID
OID

Notificação do CERT.br

- Notifica os **agentes SNMP** que estão **abertos** (**161/udp**) para o mundo.
  - Problema principal
    - **Comando GetBulk Request** - O Gerente pode solicitar multiplas partes de informações de um agente (SNMPv2 em diante)
- Lembrar que outros equipamentos podem estar com a função de SNMP sem que você saiba.

Notificação do CERT.br

- **Resolvendo o Problema**
  - Se o SNMP **não for utilizado** na sua rede **desabilite** o serviço.
  - Se o recurso for **utilizado** na rede local, **configure-o de modo que esteja disponível apenas para a rede local**.
  - **Evite** utilizar **comunidades public** e se possível utilize **autenticação** quando disponível.

Notificação do CERT.br

- **Como posso ter certeza que resolvi o problema?**
  - Você pode verificar seu dispositivo através dos seguintes comandos: (preferencialmente execute-os a partir da Internet, ou seja, fora de uma rede interna que tenha permissão de acesso ao dispositivo).
  - **$ snmpget -v 2c -c public IP_SNMP iso.3.6.1.2.1.1.1.0** ou
  - **$ snmpctl snmp get IP_SNMP oid iso.3.6.1.2.1.1.1.0**
    - Antes de executar o comando certifique-se que você tenha as ferramentas **snmpget** ou **snmpctl** instaladas.

Laboratório 6 - Resolvendo o problema do abuso do SNMP

ceptro.br nic.br cgi.br

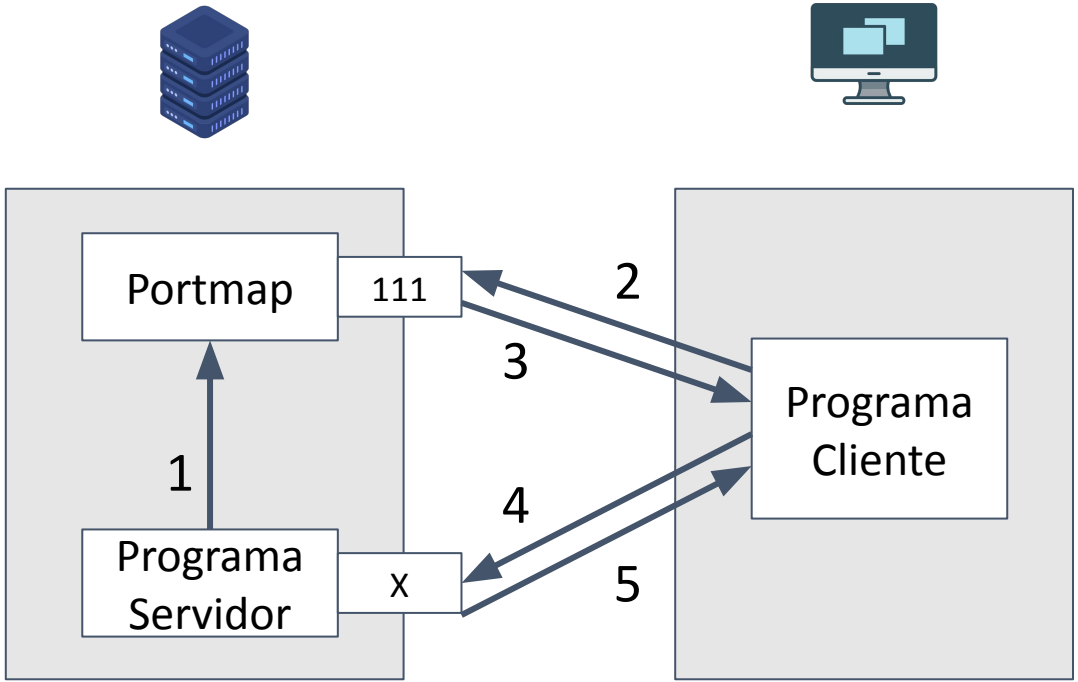
Rede de Terceiro
PORTMAP

PORTMAP

- Também conhecido como **rpc.portmap** ou **portmapper** ou **rpcbind**
- É um protocolo/serviço que mapeia dinamicamente portas TCP/UDP para distintos serviços
- Comumente associado com **RPCs (Remote Procedure Call)**
  - As RPCs são muito utilizadas para a comunicação entre processos entre computadores diferentes na rede. Ex: sistemas distribuídos
- Embora o Portmap tenha várias utilidades, a mais conhecida é a relacionada ao **Network File System (NFS)** que que permite que arquivos de um computador sejam acessados por outro computador, como se fosse algo local.

PORTMAP

1 - Programa servidor registra a porta com o portmap;
2- Cliente pergunta ao portmap sobre o programa servidor;
3 - O portmap responde com a porta que o programa servidor utiliza;
4 - O cliente conecta no programa servidor;
5 - O programa servidor responde para o cliente.



Notificação do CERT.br

- Notifica as máquinas com serviços **Portmap** que estão **abertos** (**111/udp**) para o **mundo**.
  - Problema principal
    - **Requisição UDP mal formada**
- Lembrar que outros equipamentos podem estar com a função de Portmap sem que você saiba.

Notificação do CERT.br

- **Resolvendo o Problema**
  - Configure o serviço Portmap de forma que ele seja a**cessível somente aos dispositivos de sua rede**, que utilizem esse serviço, ou que ele seja acessível **apenas via TCP**.
  - Caso o serviço Portmap seja **desnecessário** nesse servidor, recomendamos que **ele seja desativado**.

Notificação do CERT.br

- **Como posso ter certeza que resolvi o problema?**
  - Você pode verificar seu servidor através do comando:(preferencialmente execute-o a partir da Internet, ou seja, fora da rede interna).
  - **$ rpcinfo -T udp -p IP_SERVIDOR**
    - Recomendamos que utilize um sistema Unix. Antes de executar o comando acima certifique-se que você tem a ferramenta rpcinfo (geralmente parte do pacote rpcbind) instalada.

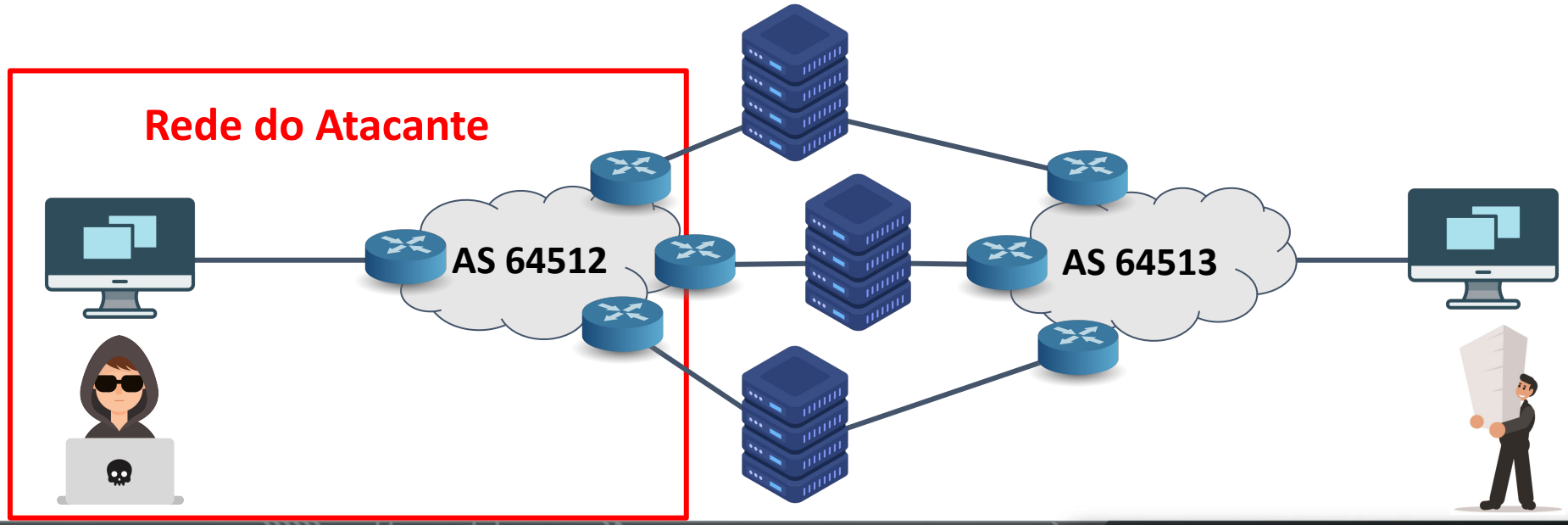
Laboratório 7 - Resolvendo o problema do abuso do Portmap

ceptro.br nic.br cgi.br

Rede Atacante:
O que fazer?

ceptro.br nic.br cgi.br

Rede do Atacante



Rede do Atacante

- Impedir que o ataque saia da rede para atingir outro.
- MANRS - Mutually Agreed Norms for Routing Security:
  - É uma iniciativa global com apoio da ISOC.
  - Consiste em 4 coisas básicas:
    - Filtros
    - Anti-Spoofing
    - Coordenação
    - Validação Global

Rede do Atacante (Anti-Spoofing)

- Técnicas de Anti-Spoofing
  - **Unicast reverse Path Forward (uRPF)**
    - Strict Mode
    - Loose Mode
    - (Enhanced) Feasible-Path
  - **Filtros de entrada (Ingress Access List)**
    - Access Control List (ACLs)
  - **Source Address Validation Improvement (SAVI)**
    - Equipamentos de camada 2

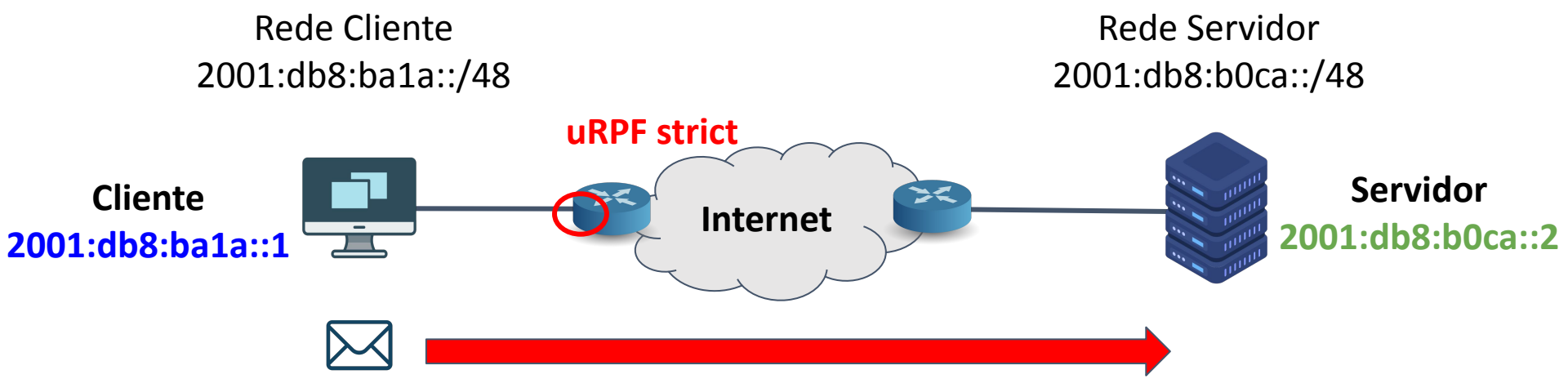
uRPF Strict:
Funcionamento básico

ceptro.br nic.br cgi.br

uRPF Strict

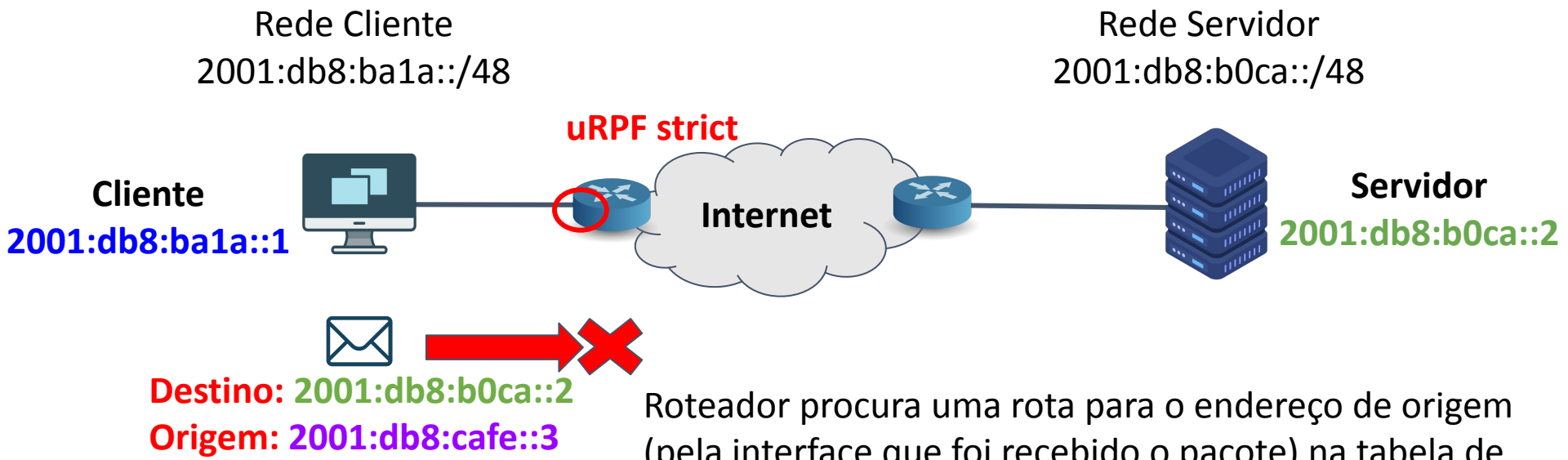
- Checa se a interface entrada vai ser a mesma da volta.
  - Se sim, o pacote passa adiante.
  - Caso contrário é descartado.
- Pode descartar tráfego legítimo! Precisa ficar atento a assimetrias na rede.

uRPF Strict



Roteador procura uma rota para o endereço de origem (pela interface que foi recebido o pacote) na tabela de roteamento. Se encontrar passa o pacote adiante, caso contrário o pacote é descartado.

uRPF Strict



Roteador procura uma rota para o endereço de origem (pela interface que foi recebido o pacote) na tabela de roteamento. Se encontrar passa o pacote adiante, caso contrário o pacote é descartado.

Laboratório 8 - Utilizando uRPF Strict

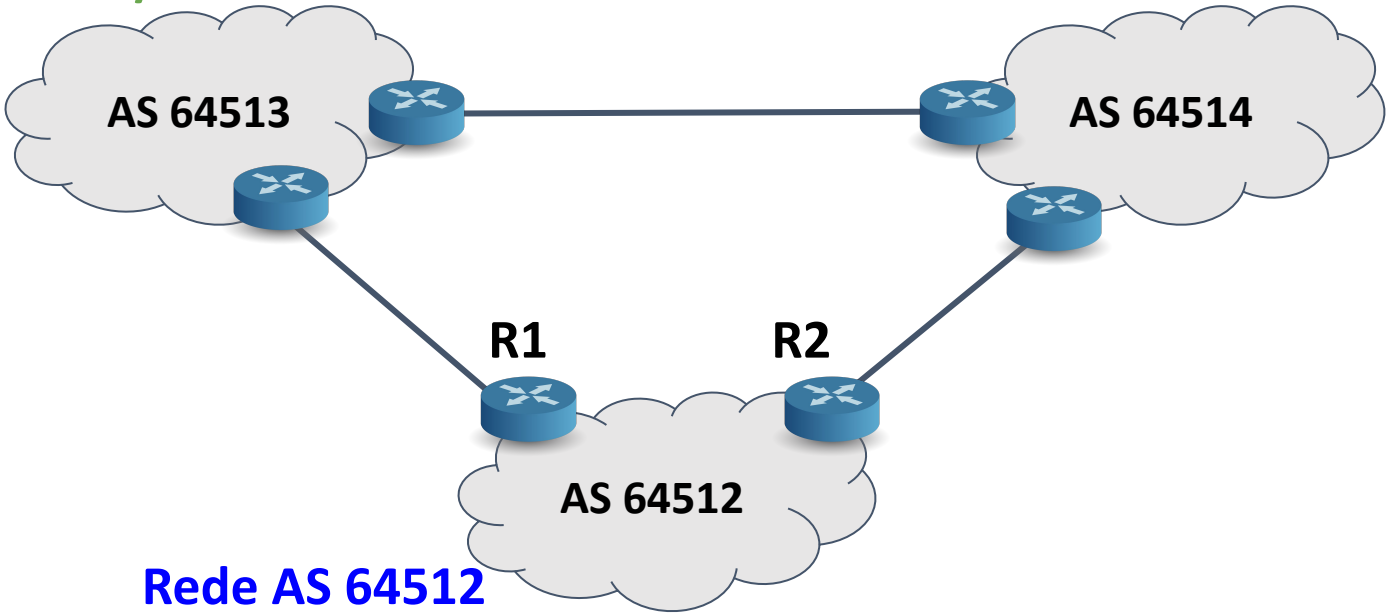
ceptro.br nic.br cgi.br

uRPF Strict
Problema de Assimetria

ceptro.br nic.br cgi.br

Entendendo o cenário

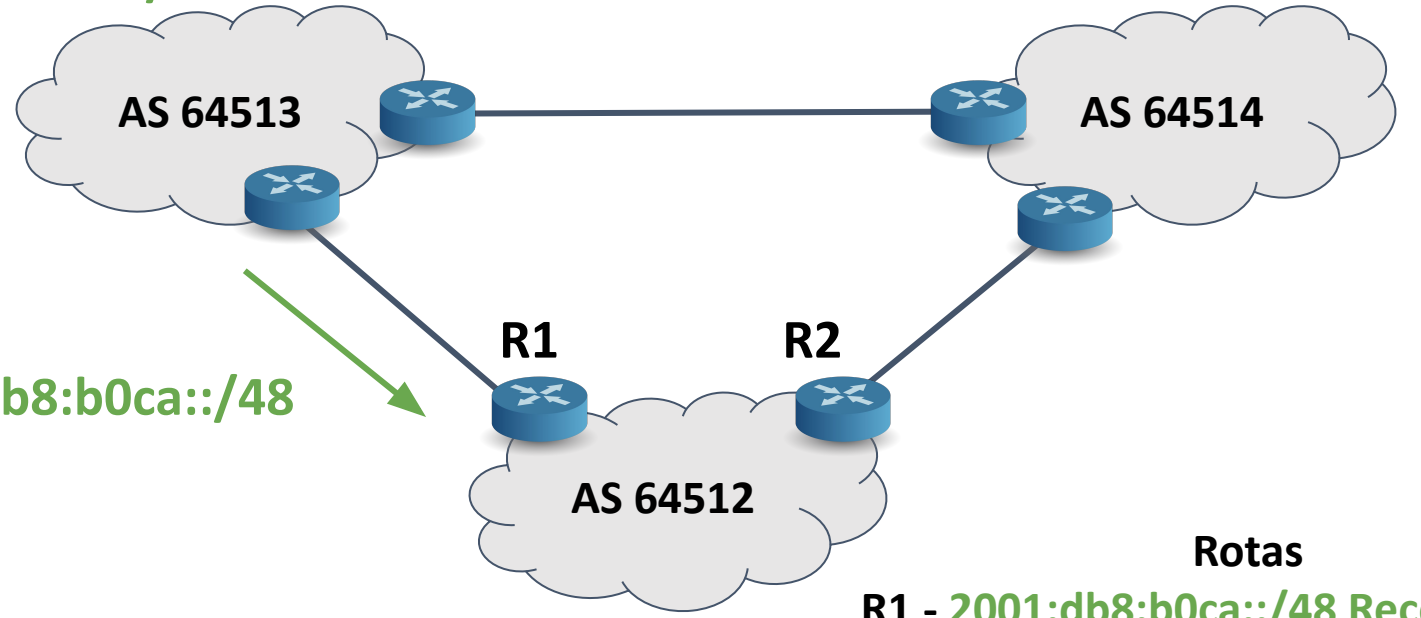
Rede AS 64513
2001:db8:b0ca::/48



Rede AS 64512
2001:db8:ba1a::/48

Entendendo o cenário

Rede AS 64513
2001:db8:b0ca::/48

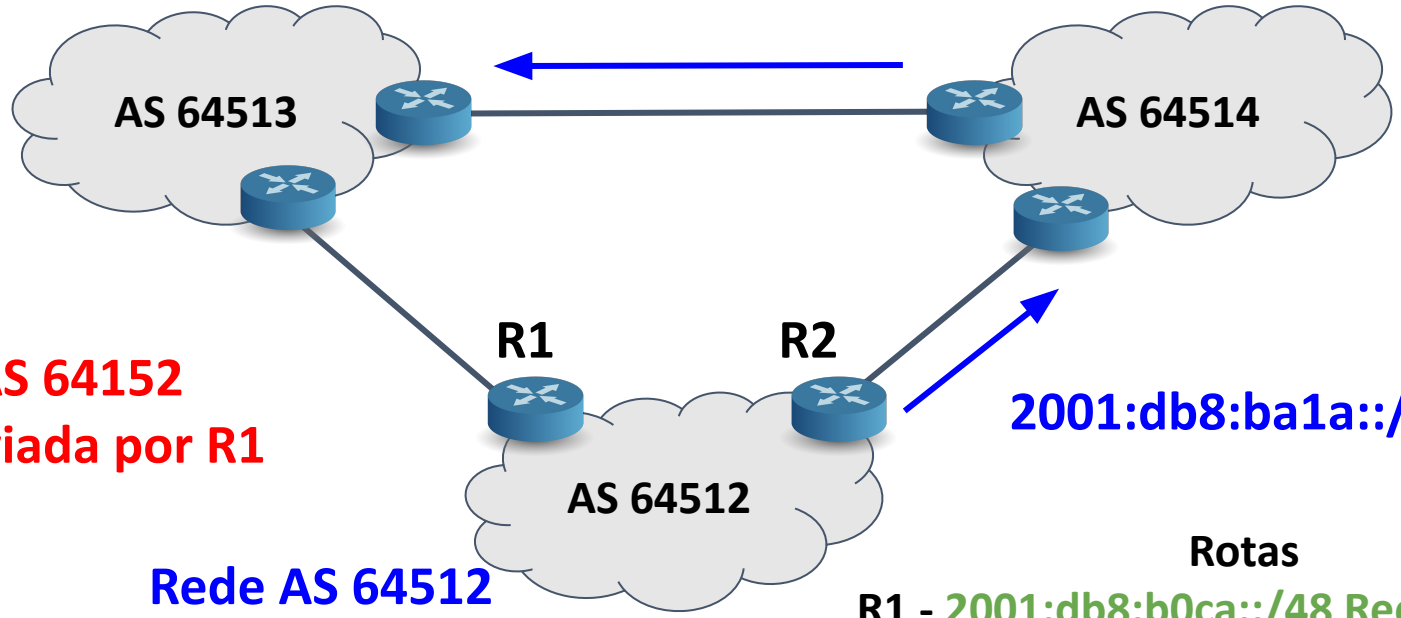


2001:db8:b0ca::/48

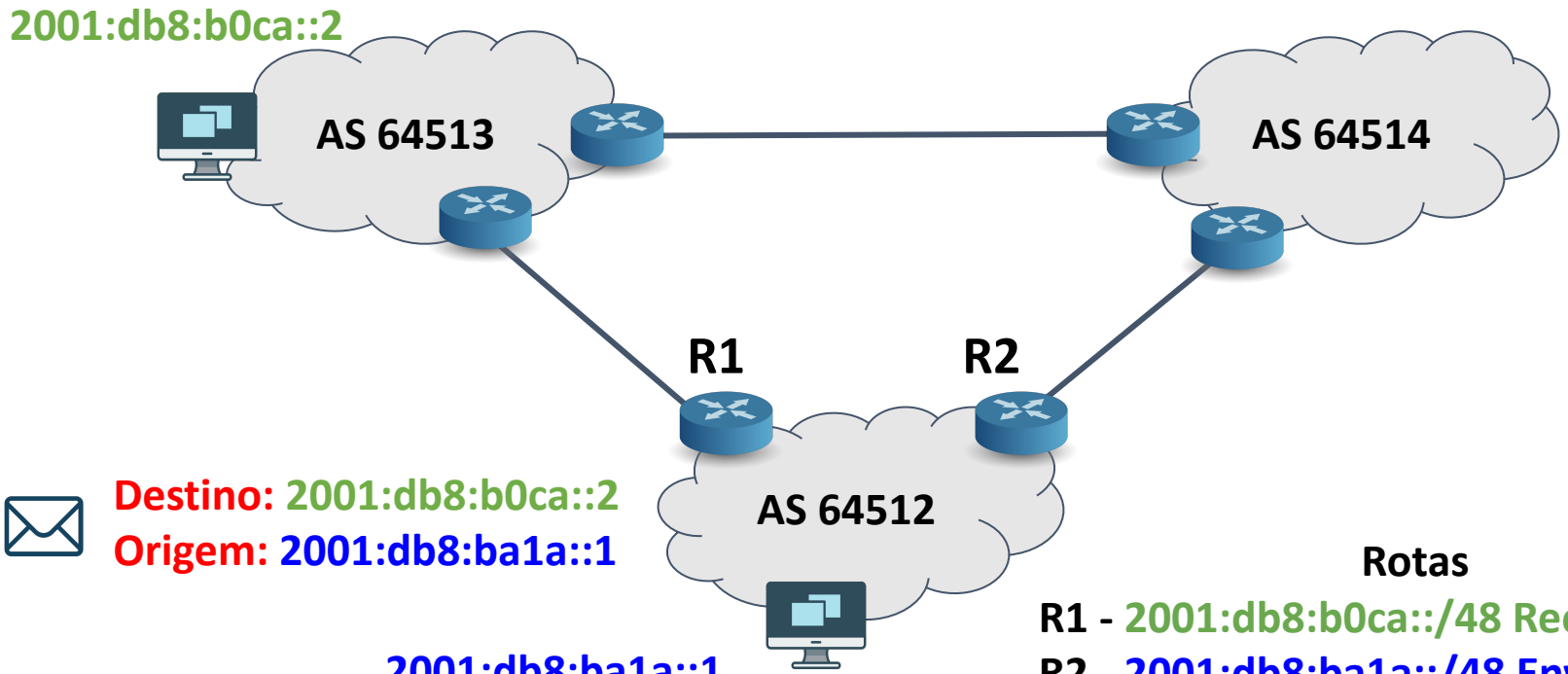
Rotas

R1 - 2001:db8:b0ca::/48 Recebida
R2 - X

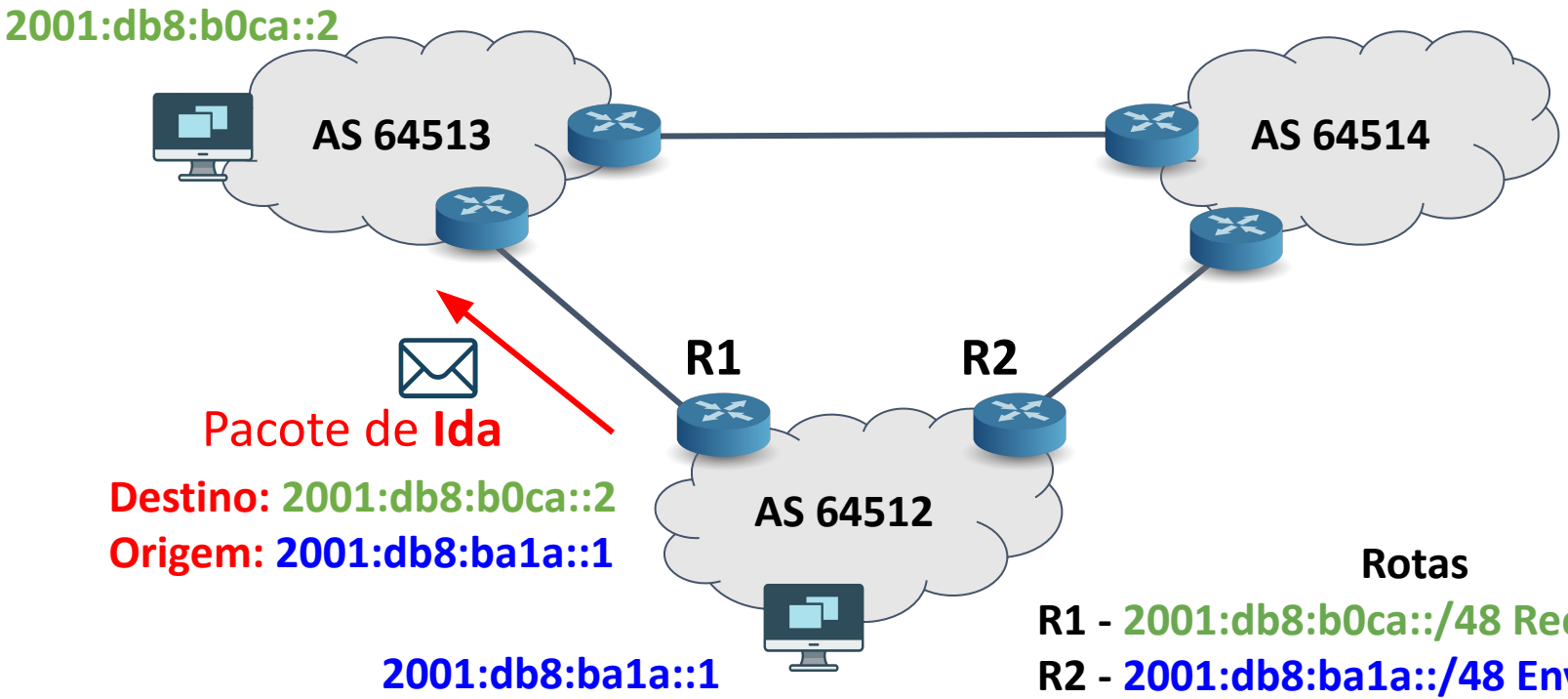
Entendendo o cenário



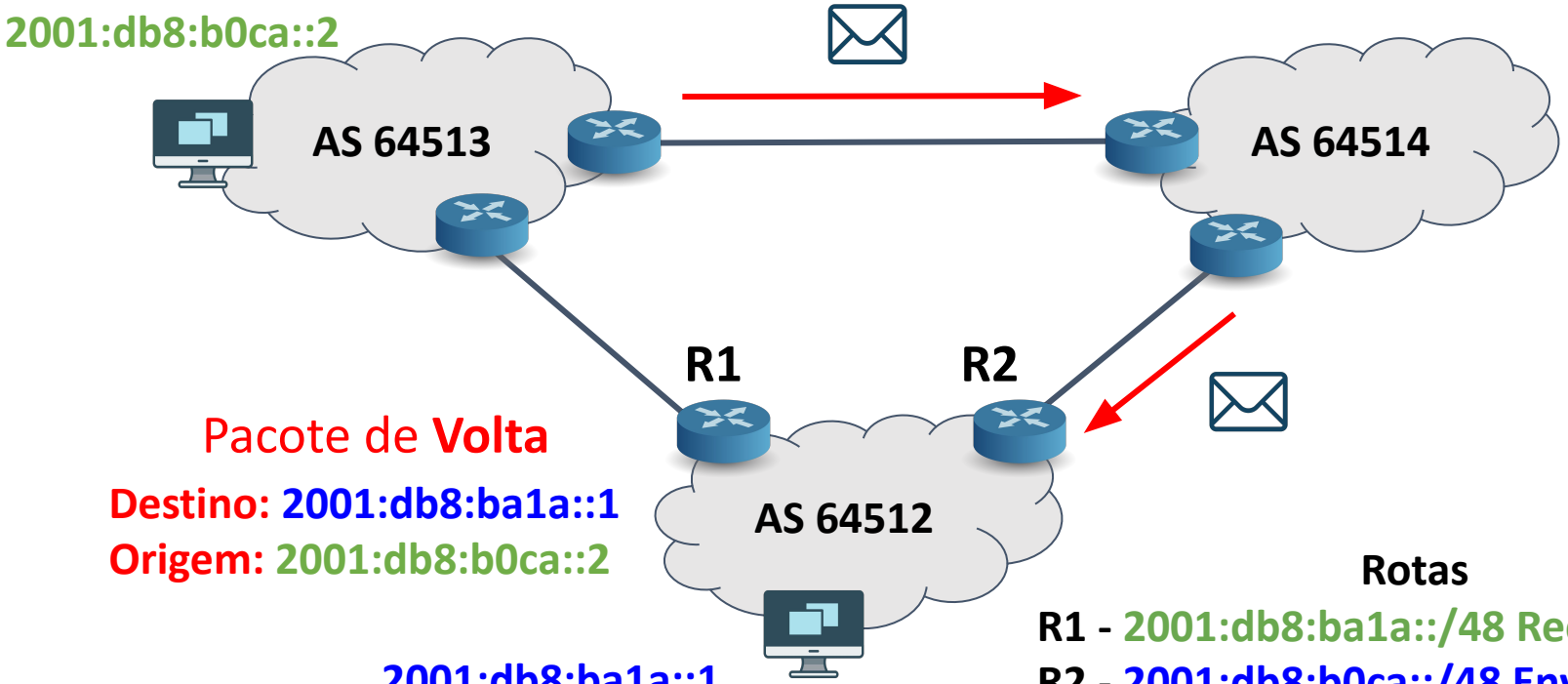
Entendendo o cenário



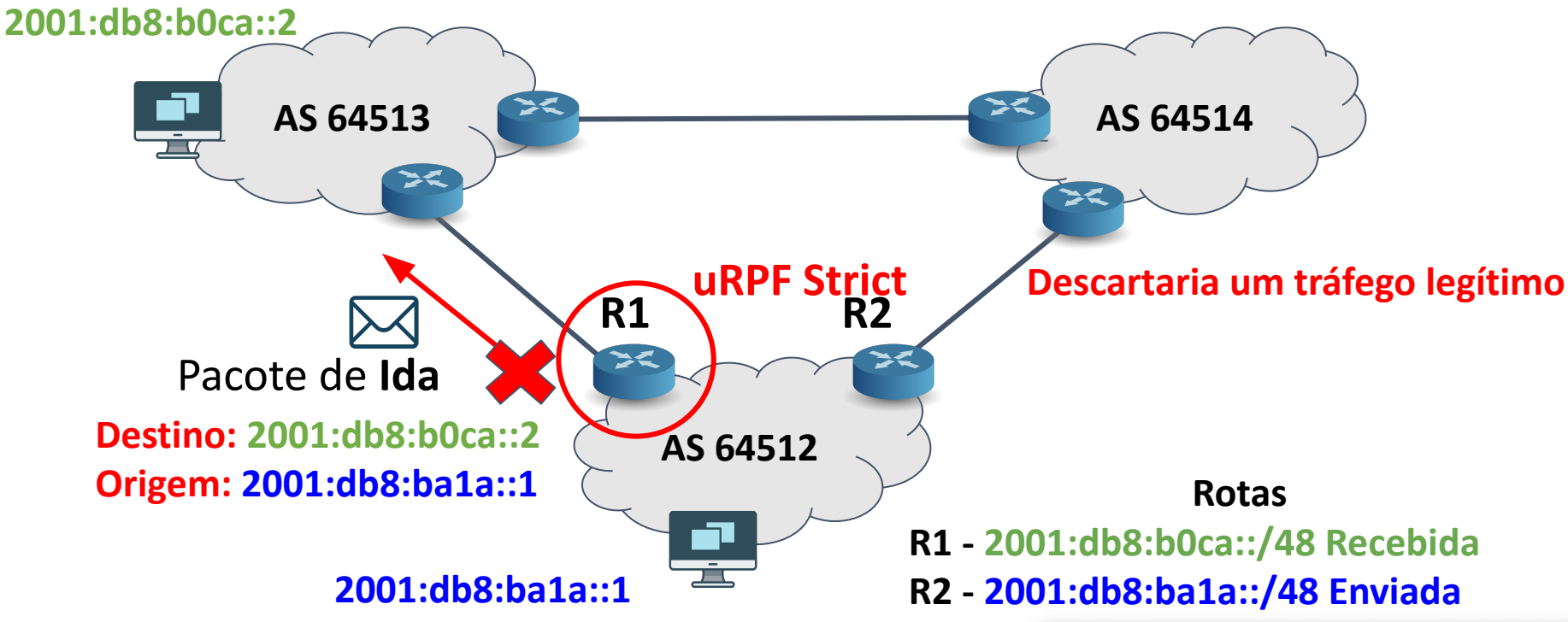
Entendendo o cenário



Entendendo o cenário



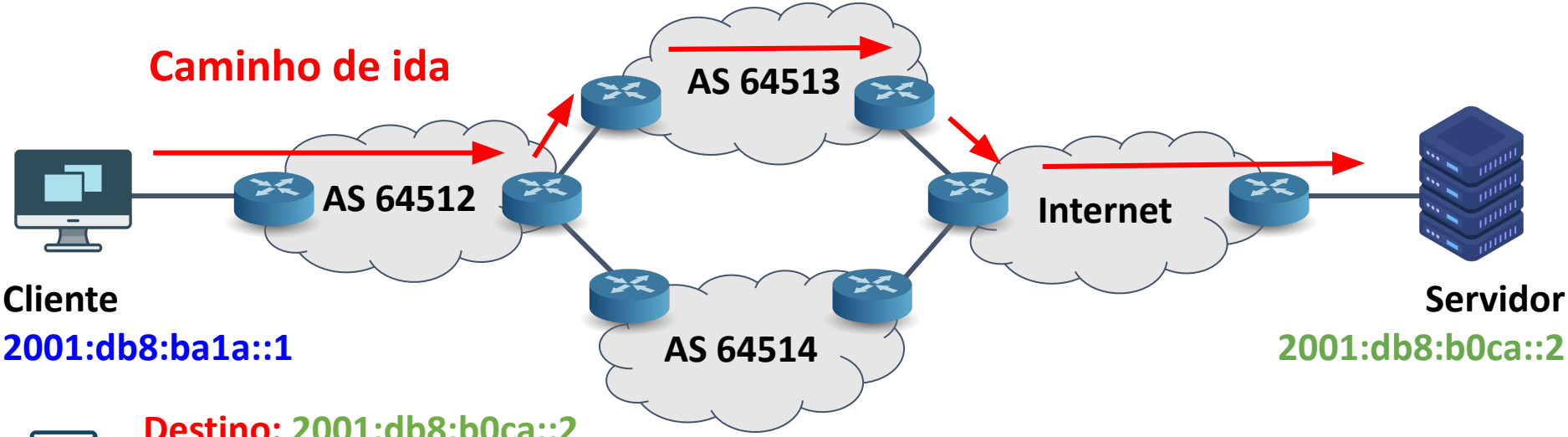
uRPF Strict - Problema Assimetria



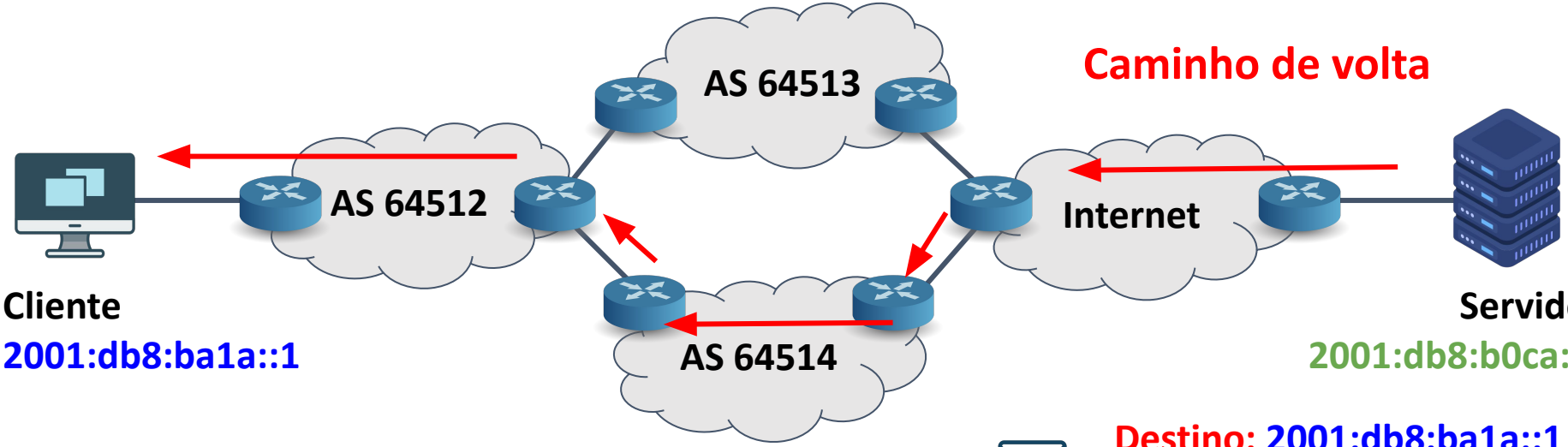
uRPF Loose
Funcionamento básico

ceptro.br nic.br cgi.br

uRPF Loose

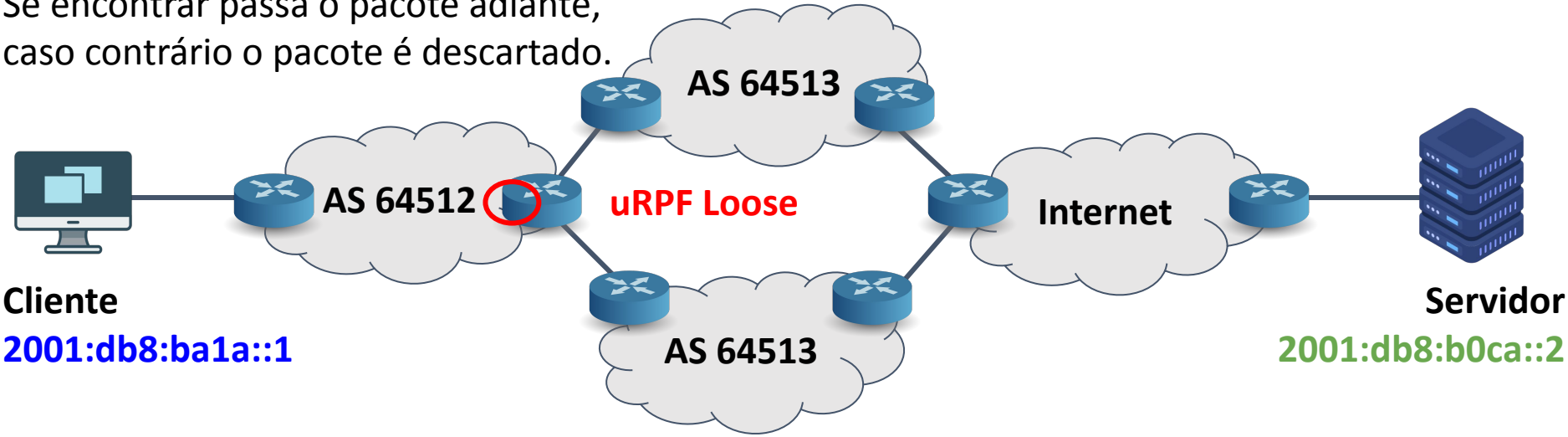

Caminho de ida
AS 64513
AS 64512
Internet
AS 64514
Cliente
2001:db8:ba1a::1
Servidor
2001:db8:b0ca::2
Destino: 2001:db8:b0ca::2
Origem: 2001:db8:ba1a::1

uRPF Loose


Caminho de volta
AS 64513
AS 64512
AS 64514
Internet
Cliente
2001:db8:ba1a::1
Servidor
2001:db8:b0ca::2
Destino: 2001:db8:ba1a::1
Origem: 2001:db8:b0ca::2

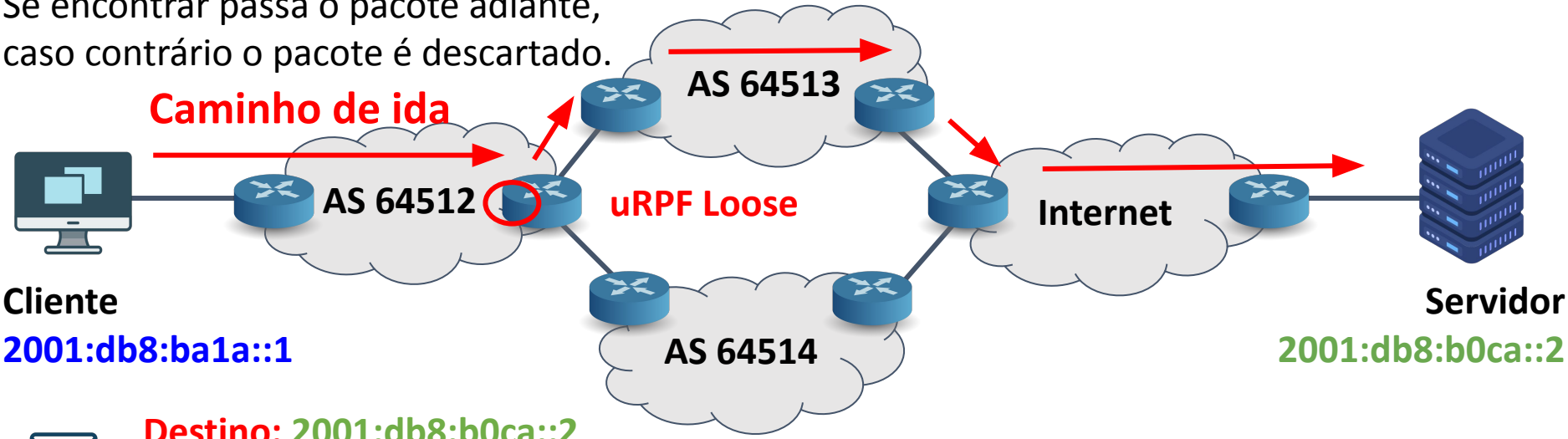
uRPF Loose

Roteador procura uma rota para o endereço de origem (por qualquer interface) na tabela de roteamento. Se encontrar passa o pacote adiante, caso contrário o pacote é descartado.



uRPF Loose

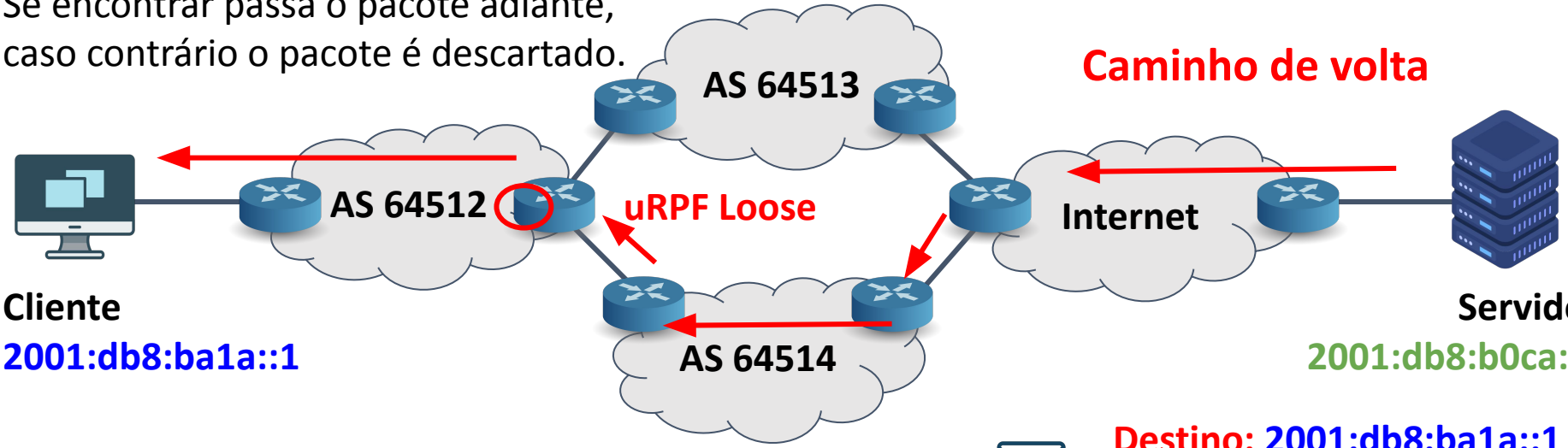
Roteador procura uma rota para o endereço de origem (por qualquer interface) na tabela de roteamento. Se encontrar passa o pacote adiante, caso contrário o pacote é descartado.



Destino: 2001:db8:b0ca::2
Origem: 2001:db8:ba1a::1

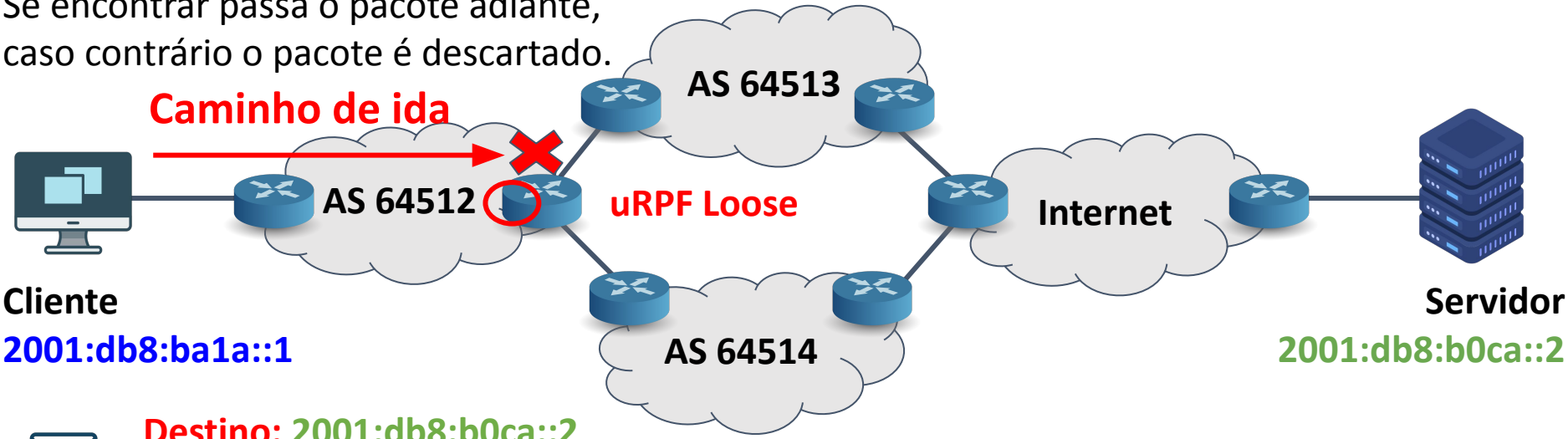
uRPF Loose

Roteador procura uma rota para o endereço de origem (por qualquer interface) na tabela de roteamento. Se encontrar passa o pacote adiante, caso contrário o pacote é descartado.



uRPF Loose

Roteador procura uma rota para o endereço de origem (por qualquer interface) na tabela de roteamento. Se encontrar passa o pacote adiante, caso contrário o pacote é descartado.



Destino: 2001:db8:b0ca::2
Origem: fd12:3456:789a::1

uRPF Loose
Problema tráfego invalido

ceptro.br nic.br cgi.br

uRPF Loose

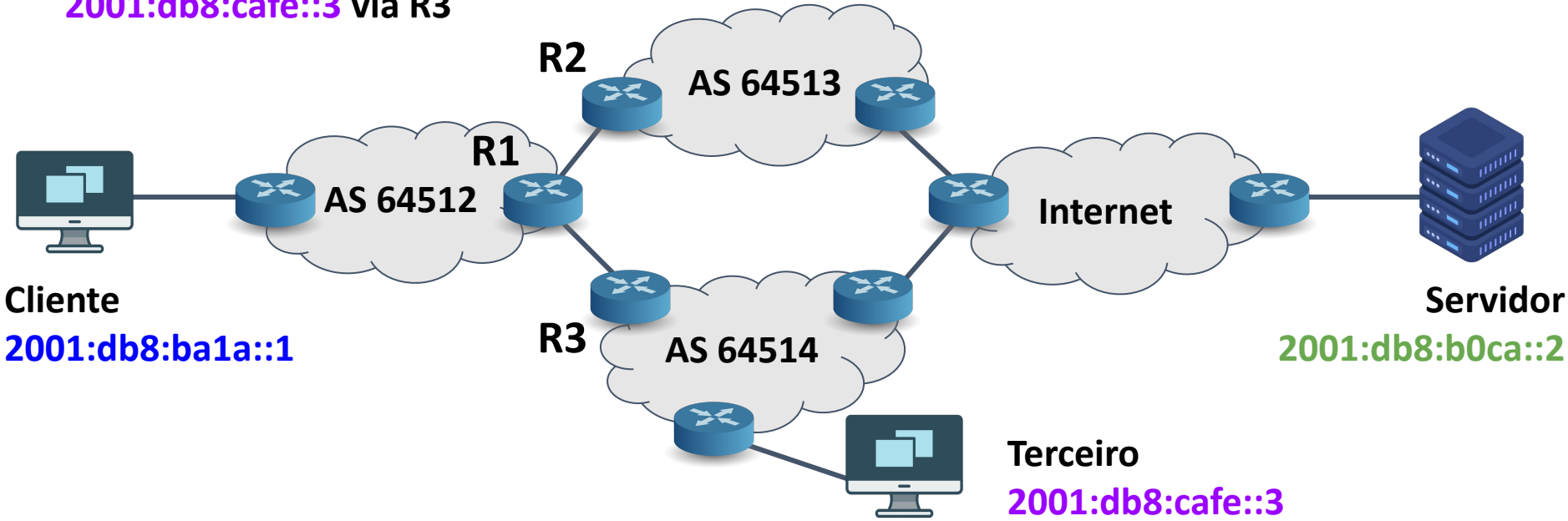
- **Não checa se a interface entrada vai ser a mesma da volta.**
- Só verifica se existe uma **rota válida disponível**.
  - Porém endereços reservados não terão rotas e logo os pacotes com estas origem serão descartados.
  - Rota default pode invalidar o modo Loose! Precisa verificar no fabricante comando que não atrapalha.
- **Pode permitir passar tráfego spoofado! Precisa ficar atento**.
- Exceção:
  - Se o next-hop da rota for Null0 para o endereço de origem o pacote é descartado.
  - Utilizado para o RTBH.

uRPF Loose

Tabela de roteamento R1

2001:db8:b0ca::2 via R2

2001:db8:cafe::3 via R3

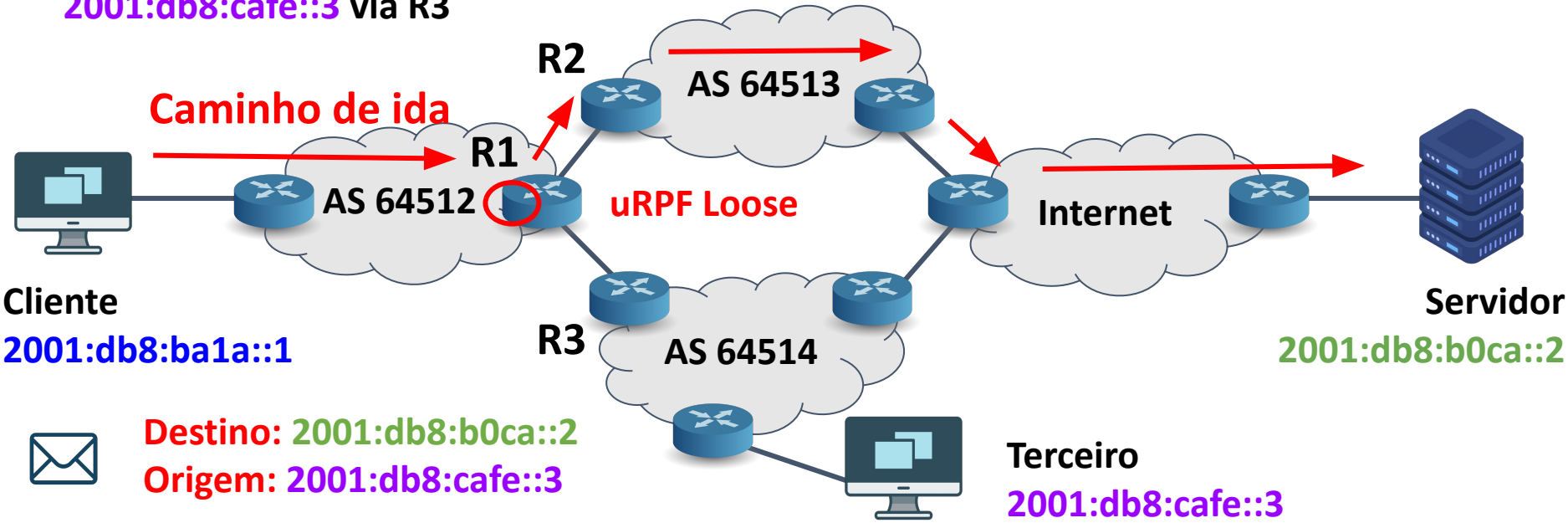


uRPF Loose

Tabela de roteamento R1

2001:db8:b0ca::2 via R2

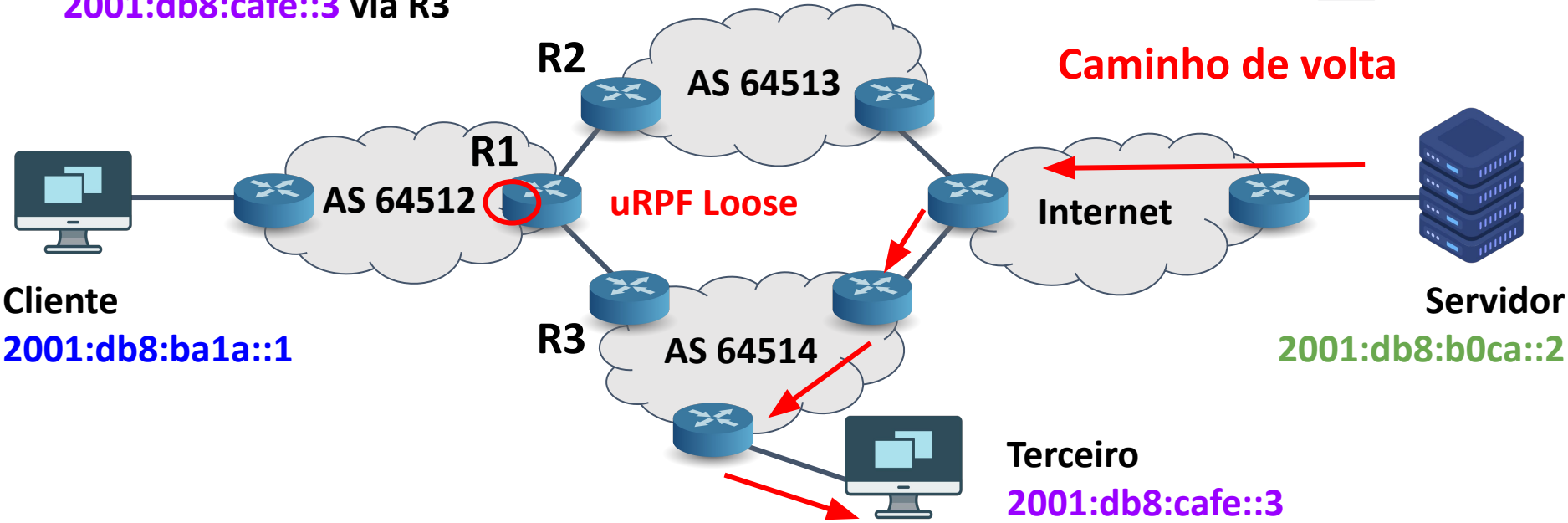
2001:db8:cafe::3 via R3



uRPF Loose

Destino: 2001:db8:cafe::3
Origem: 2001:db8:b0ca::2

Tabela de roteamento R1
2001:db8:b0ca::2 via R2
2001:db8:cafe::3 via R3



Filtros de entrada:
Funcionamento básico

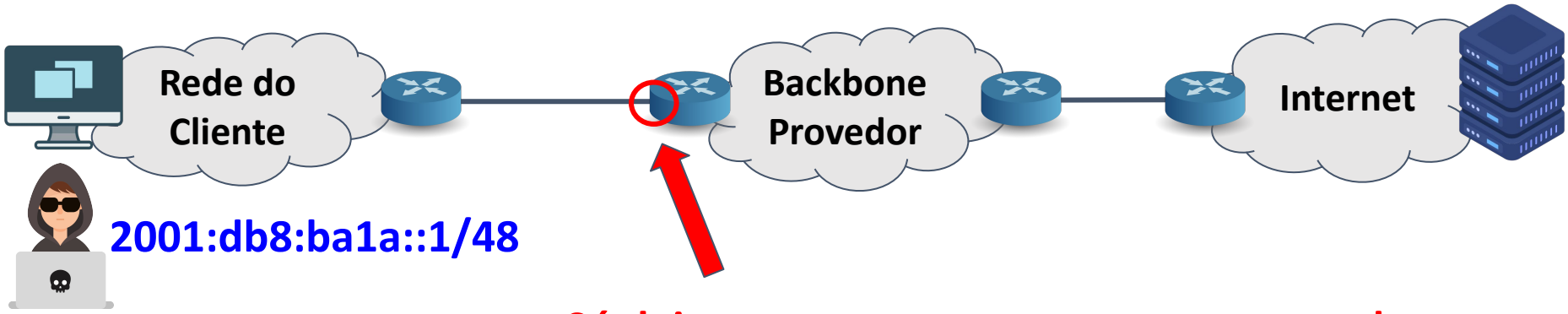
ceptro.br nic.br cgi.br

Filtros de entrada (Ingress Access List)

- Precisa ficar atento pois se tiver mudança na rede, precisa mudar os filtros.
- Pode-se utilizar um filtro abrangente, mas não é 100% eficaz.
- É redundante com o uRPF (não precisa usar os dois).

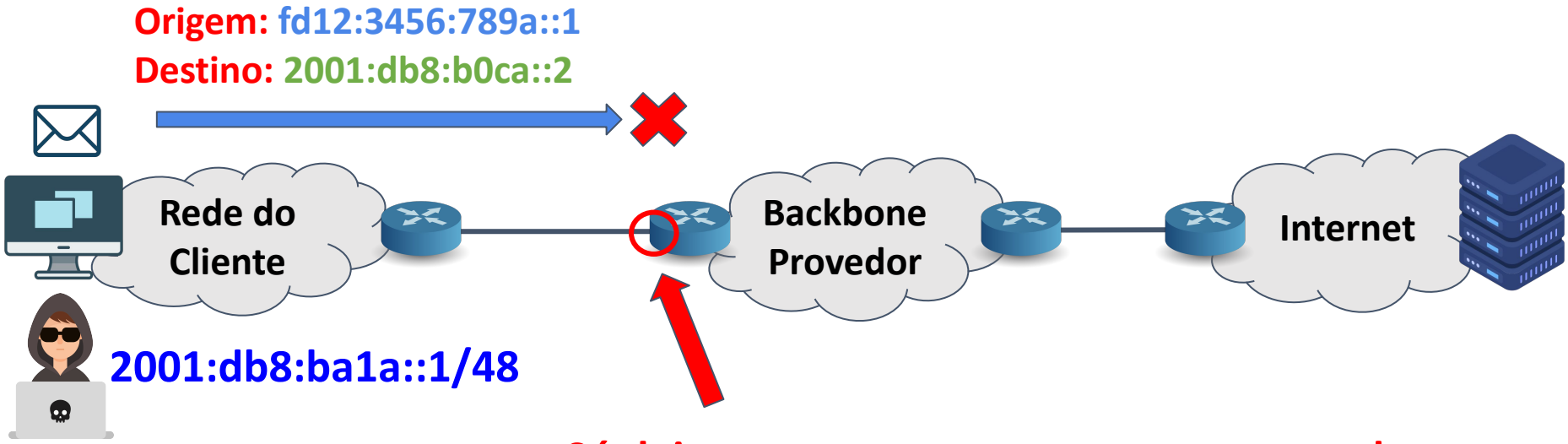
Filtros de entrada (Ingress Access List)

- **BCP 38 - https://www.ietf.org/rfc/bcp/bcp38.html**



Só deixa passar pacotes que possuam endereços de origem dentro do prefixo 2001:db8:ba1a::/48

Filtros de entrada (Ingress Access List)



Só deixa passar pacotes que possuam endereços de origem dentro do prefixo 2001:db8:ba1a::/48

Laboratório 9 - Aplicando Anti Spoofing com ACLs

ceptro.br nic.br cgi.br

Outras Notificações: Vulnerabilidade do OpenSSH

ceptro.br nic.br cgi.br

OpenSSH

- É uma ferramenta para login e execução de comando remoto utilizando SSH.
  - SSH(Secure Shell Protocol) é um protocolo de rede criptográfico
  - Fornece um canal seguro sobre uma rede insegura

Notificação do CERT.br

- Notifica as máquinas com uma possível versão vulnerável de um servidor OpenSSH.
  - Problema principal
    - Vulnerabilidade, descrita pelo CVE-2024-6387, é considerada crítica e um atacante não autenticado, sob certas condições, pode executar código arbitrário remotamente com privilégios de root e assim ganhar acesso ao sistema.
- Lembrar que outros equipamentos podem estar com uma versão vulnerável do OpenSSH sem que você saiba.

Notificação do CERT.br

- Verifique, no site do seu fabricante, se o seu sistema é vulnerável;
- Em caso positivo:
  - Instale as correções disponibilizadas o mais rápido possível, atualize.
  - Verifique o sistema em busca de sinais de comprometimento.

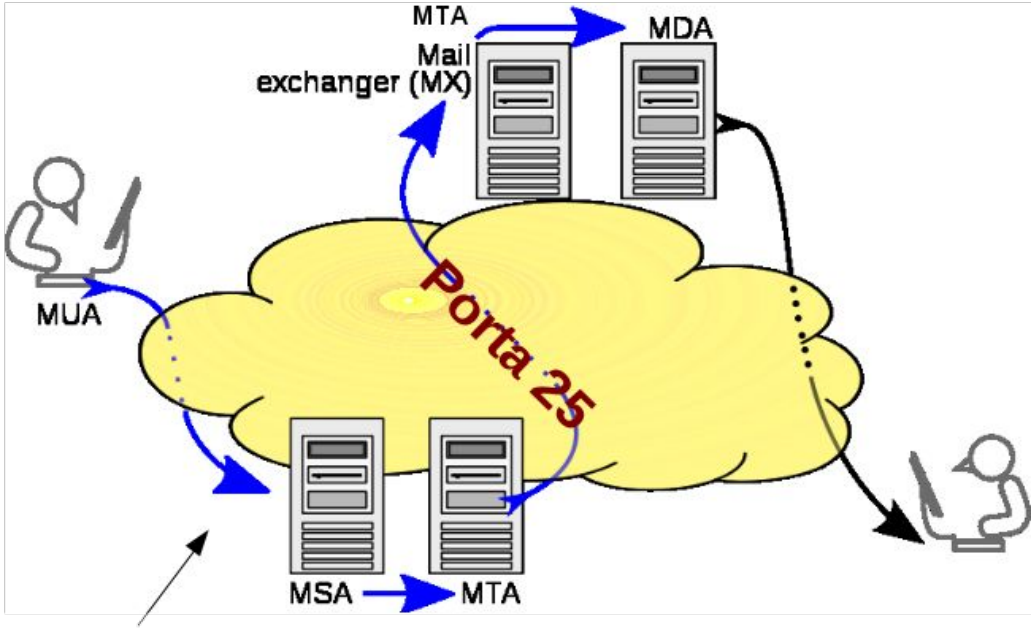
Laboratório 10 - Resolvendo o problema do OpenSSH

ceptro.br nic.br cgi.br

Outras Notificações: Conceitos básicos Antispam

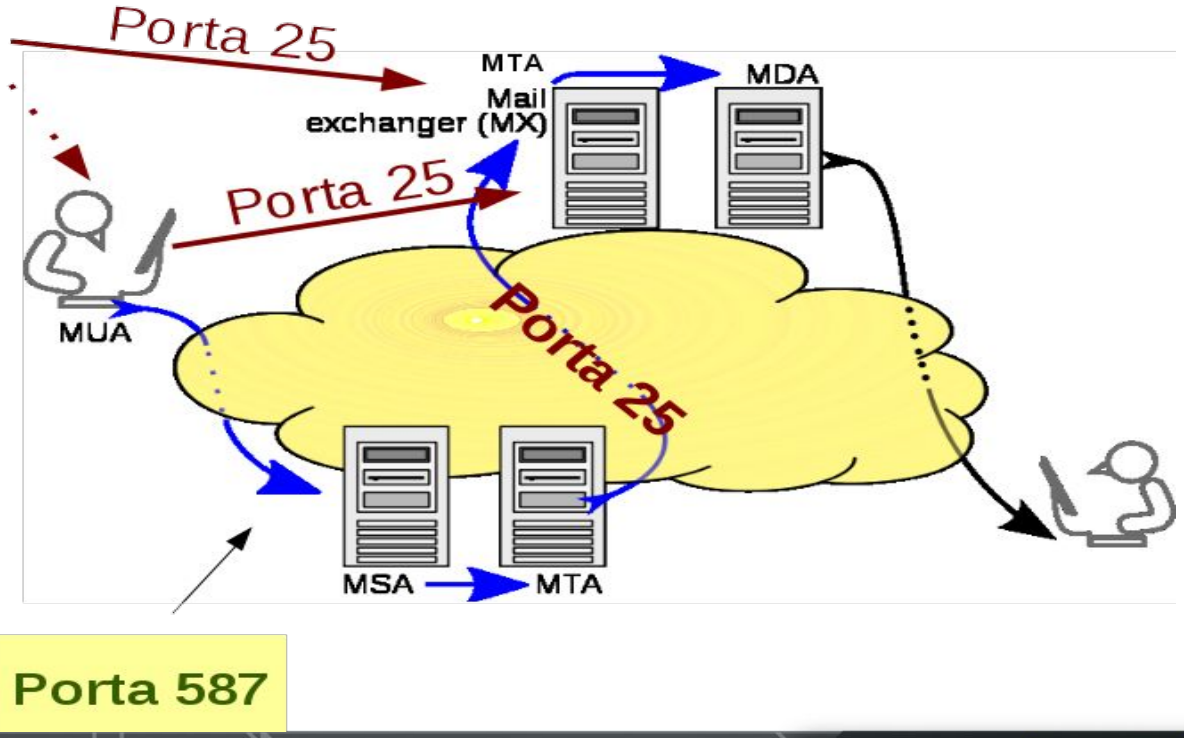
ceptro.br nic.br cgi.br

Funcionamento do email



Porta 587

SPAM


Porta 25
MTA
Mail
exchanger (MX)
MDA
Porta 25
MUA
Porta 25
MSA
MTA
Porta 587

O que é gerência da porta 25?

- É um conjunto de políticas e tecnologias aplicadas em **redes de usuários residenciais**, para **evitar o spam**. Separa as funcionalidades de:
  - Submissão de mensagens de e-mail e
  - Comunicação entre servidores de e-mail

- Projeto **Antispam.br**
  - Boas práticas de configuração

Gerência da porta 25

- Qual o raciocínio?
  - Os **usuários residenciais** normalmente enviam e-mails utilizando:
    - **Mail Submission Port (587)**
    - **Webmail (443)**
- Os spammers, fraudadores, e códigos maliciosos utilizam a **porta 25, que deve ser bloqueada**.

Outras Notificações: Mikrotik Socks(Infectados)

Mikrotik SOCKS

- Mikrotiks **comprometidos (infectados)**
  - Socks habilitado na porta 4145/tcp;
  - Socks atua como um servidor proxy repassando dados antes de passar pelo firewall;
  - Sendo **abusados** intensamente para o envio de **SPAM** na porta 25.

Notificação do CERT.br

- Notifica o mikrotiks com serviço SOCKs que estão abertos (**4145/tcp**) para o mundo.
- **Resolvendo o problema**
  - 1) Verifique a existência de um serviço SOCKS atendendo na porta 4145/tcp, executando o seguinte comando:
    - **/ip socks print**
  - Se o serviço estiver marcado como habilitado (enabled = yes), desabilite-o com o seguinte comando:
    - **/ip socks set enable=no**

Notificação do CERT.br

- 2) **Atualize a versão do Router OS** para a última versão "Long-term/bugfix" ou "Stable/current", de acordo com as instruções do fabricante disponíveis na seguinte URL:
  - https://wiki.mikrotik.com/wiki/Manual:Upgrading_RouterOS
- 3) Apenas depois de atualizar o sistema altere a senha com o comando abaixo:
  - **/user set USUARIO password=NOVA_SENHA**
  - onde USUARIO é o usuário utilizado para conectar no mikrotik.

Laboratório 11 - Resolvendo o problema do Mikrotik Socks e Antispam

ceptro.br nic.br cgi.br

Conclusão

- Ficar atento às **atualizações** dos seus serviços:
  - Correções de Bugs e novas funcionalidades;
  - Olhar site do fabricante e lista de discussões.
- Ficar atento às **novas vulnerabilidades**
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Atualizar os contatos do whois** e ficar atento aos **emails de notificação do Cert.br.**

Obrigado!!!

@ cursosceptro@nic.br

@ ipv6@nic.br

nic.br cgi.br

www.nic.br | www.cgi.br