nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

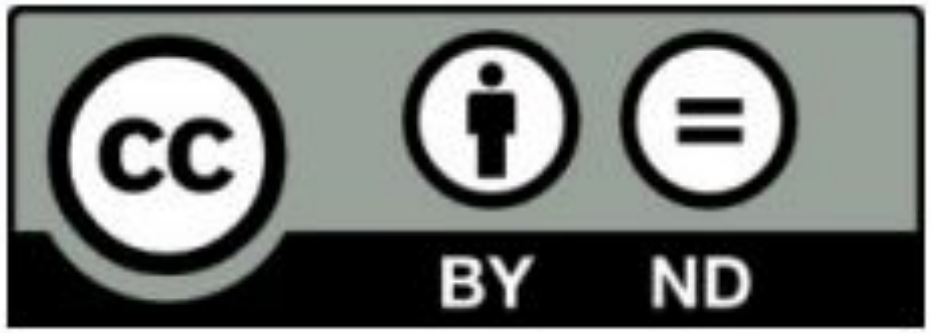
Comitê Gestor da Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons
Atribuição - Sem Derivações 4.0 Internacional (CC BY-ND 4.0)
https://creativecommons.org/licenses/by-nd/4.0/legalcode.pt



Você tem o direito de:

- **Compartilhar -** copiar e redistribuir o **material** em qualquer suporte ou formato para qualquer fim, **mesmo que comercial.**
- *O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.*

De acordo com os termos seguintes:

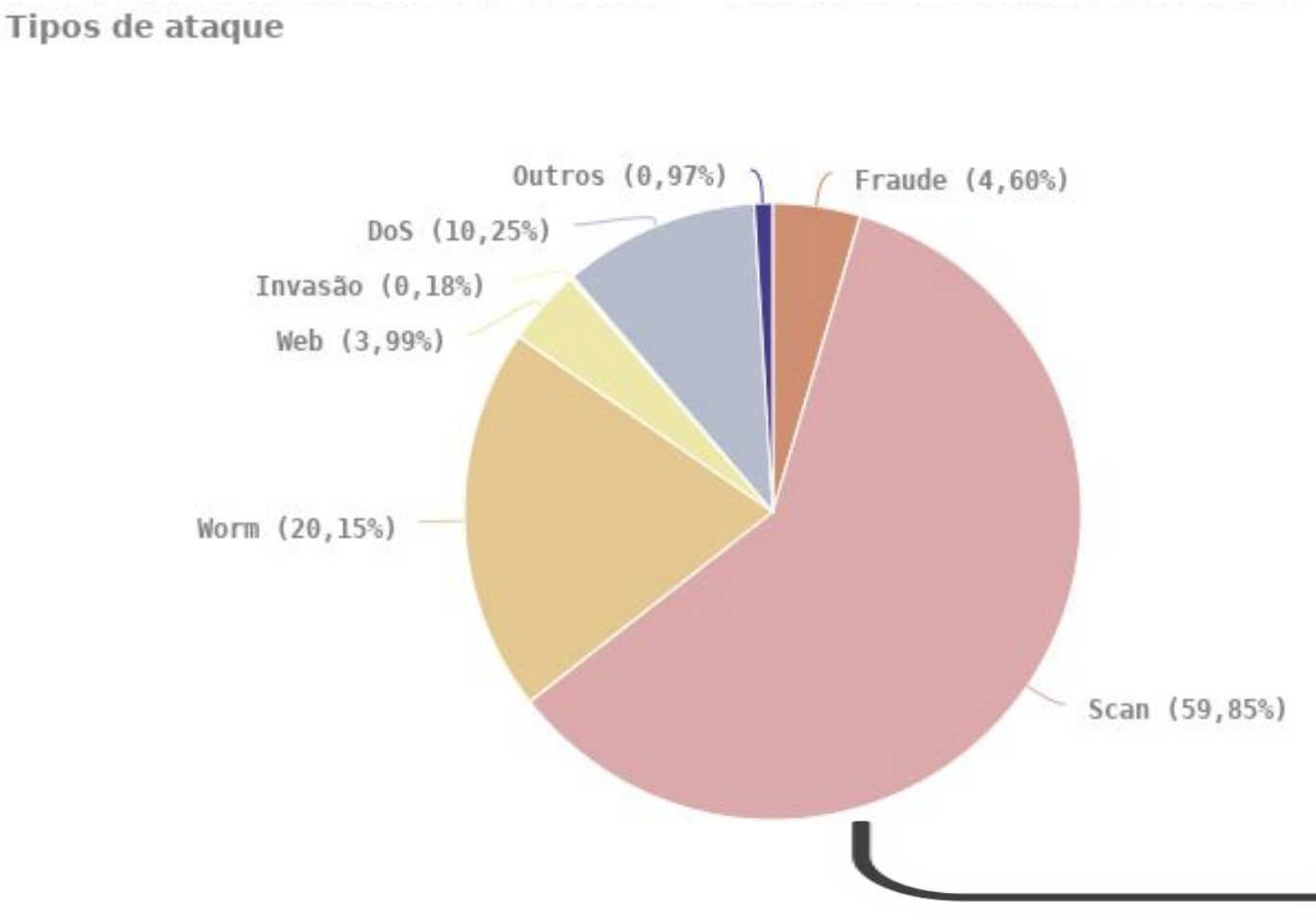
- **Atribuição** - Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso. Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do **Programa Acelera NET do CEPTRO.br/NIC.br**, e que os originais podem ser obtidos em http://ceptro.br. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.
- **Sem Derivações** - Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

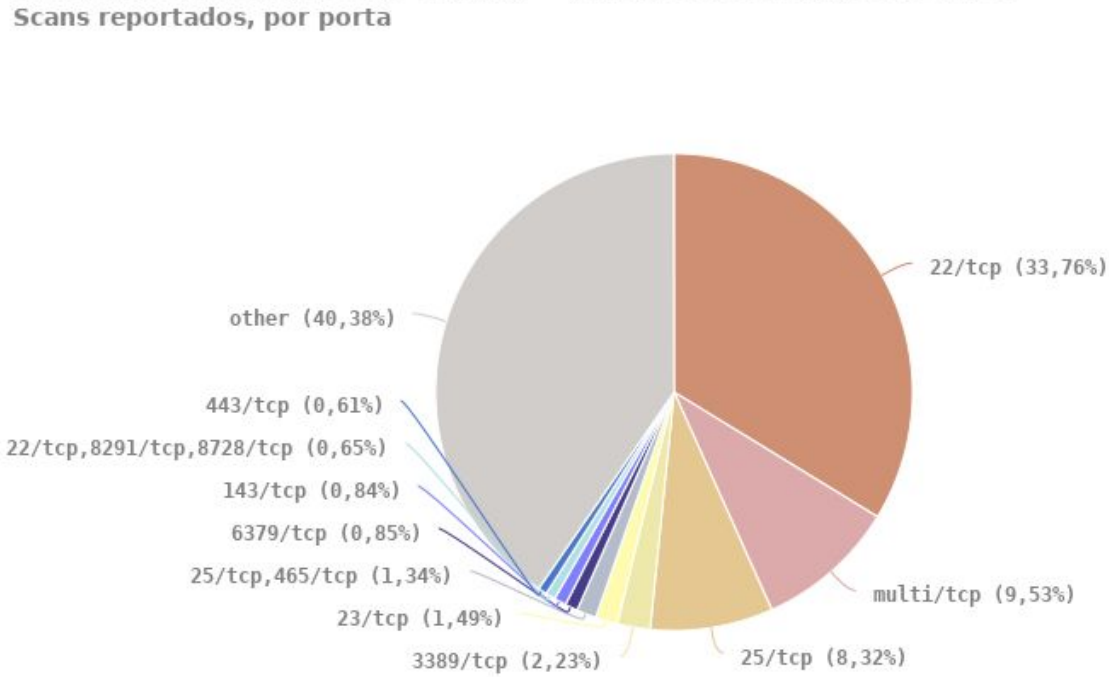
Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

Hardening de Equipamentos

ceptro.br nic.br cgi.br

Ataques dentro da Internet Brasileira





Scan Portas 22 e 23:
Força bruta de senhas de servidores, CPEs e IoT

Fonte: https://stats.cert.br/historico/incidentes/2020-jan-dec/tipos-ataque.html

Alteração de DNS para fraudes

Comprometidos

via força bruta de senhas (geralmente via telnet)

explorando vulnerabilidades

via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos

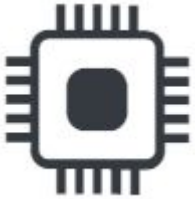
- Colocados em *sites* legítimos comprometidos pelos fraudadores

Objetivos dos ataques

alterar a configuração de DNS para que consultem servidores sob controle dos atacantes

servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*

- casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos



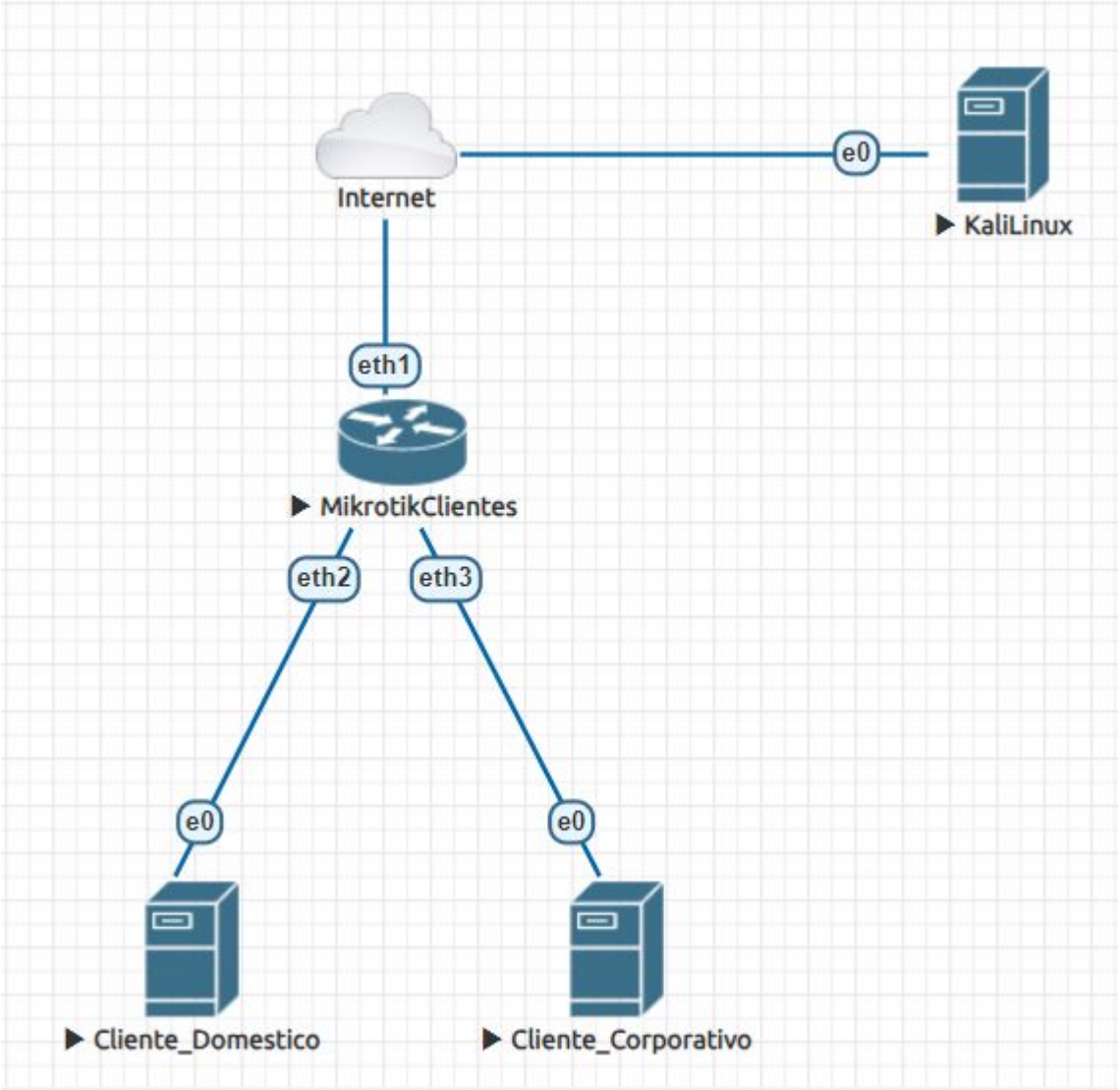
O que é Hardening?

- **É um procedimento para:**
  - **Analisar vulnerabilidades.**
  - **Mapear as ameaças.**
  - **Minimizar/Mitigar riscos.**
  - **Aplicar medidas corretivas.**

- **Proteger**
  - **Ataques vindos de terceiros**
  - **Seus equipamentos façam ataques em outros.**

CENÁRIO DO LABORATÓRIO

- Mikrotik
  - MikrotikClientes
- GNU/Linux
  - Cliente_Domestico
  - Cliente_Corporativo
- Debian/Kali Linux
  - KaliLinux



Lab 1 - Configurações iniciais

ceptro.br nic.br cgi.br

WIRESHARK

- **Wireshark** é um analisador de protocolo de redes.
- Captura o tráfego de redes e o organiza por protocolos.
- Possui uma interface gráfica.
- Permite filtrar os pacotes capturados.

Lab 1a - Observando pacotes com o Wireshark

ceptro.br nic.br cgi.br

Pentest

ceptro.br nic.br cgi.br

Principais fases

- Reconhecimento (Footprinting)
- Varredura (Scanning)
- Enumeração (Enumeration)
- **Exploração (Exploitation)**
- Ganho de Acesso (Gaining Access)

METASPLOIT

- O **Metasploit** é uma ferramenta usada para testes de penetração com o intuito de explorar vulnerabilidades!

- **Exploits** são programas que tiram proveito de falhas de software (vulnerabilidades) para obter resultados indesejados, como execução arbitrária de código, escalação de privilégios, negação de serviço, vazamento de informações e outros.

METASPLOIT

- **Exploits**: é por onde o ataque tem início, pode ser um código malicioso ou um software que utiliza-se de uma vulnerabilidade para atacar o sistema como um todo ou parte dele, assim abrindo caminho para a injeção de outro código, o Payload.

- **Payloads**: após o Exploit “abrir caminho” explorando uma falha ou vulnerabilidade, é executado um código que tem como função comprometer o sistema.

Lab 1b - Utilizando o Metasploit

ceptro.br nic.br cgi.br

Recomendações para Autenticação

- **Básico**
  - **Criar um usuário para cada funcionário.**
    - Desative contas antigas e inutilizadas.
  - **Não deixe os funcionários utilizarem a mesma conta padrão de administração do sistema!!!**
    - Guarde o acesso padrão somente para backup e emergências.

Recomendações para Autenticação

- **Básico**
  - **Não permita senhas fracas de acesso!**
    - O CERT.br possui fascículo sobre recomendações de senhas!
  - **Não armazena sua senhas em texto puro!**
    - Use uma função hash (PBKDF2, Bcrypt, Scrypt e Argon2)

[BAIXE AQUI O PDF]

Recomendações para Autenticação

- **Avançado**
  - Aplique técnicas de **autenticação em 2 fatores.**
    - Coisas que eu **sei**!
      - Ex: Senhas.
    - Coisas que eu **sou**!
      - Ex: Biometria.
    - Coisas que eu **possuo**!
      - Ex: Chave.
  - **Usar 2 coisas do mesmo tipo não caracteriza autenticação em 2 fatores.**
  - O CERT.br possui fascículo com **recomendações sobre o assunto**.

Lab 1c - Ataque de dicionário

ceptro.br nic.br cgi.br

Recomendações para Autorização

- **Básico**
  - **Cada usuário deve ter permissão para acessar o roteador de acordo com o seu trabalho.**
    - Não forneça acesso administrador para todos o seus usuários.
    - Pense no que seu estagiário/agente malicioso poderia fazer no seu sistema.
  - **Em alguns sistemas pode se criar grupos de privilégios.**
  - **Em alguns sistemas é possível escalar privilégios.**

Recomendações para Auditoria

- **Básico**
  - Manter um **registro de cada usuário com suas respectivas permissões**.
  - **Registrar as ações** de cada usuário no sistema.
  - Operar com **nível de criticidade** nos registros.
    - Informativo
    - Aviso
    - Crítico
  - Tipos de registros
    - Documentos
    - Logs
    - Backups de configuração
  - É **importante** guardar a informação com a **data e hora certa**!

Recomendações para Acesso

- **Básico**
  - **Não utilize protocolos inseguros** para acesso.
    - Exemplos:

  - **Desative-os se eles estiverem operando.**

  - **Se for o único meio** de acesso a máquina, **restrinja** o alcance para somente ser utilizada pela **interface de gerencia** (uma rede apartada e protegida).

Recomendações para Acesso

- **Básico**
  - Utilize preferencialmente protocolos com mensagens **criptografadas!**
    - Exemplos:

Winbox
(secure mode)

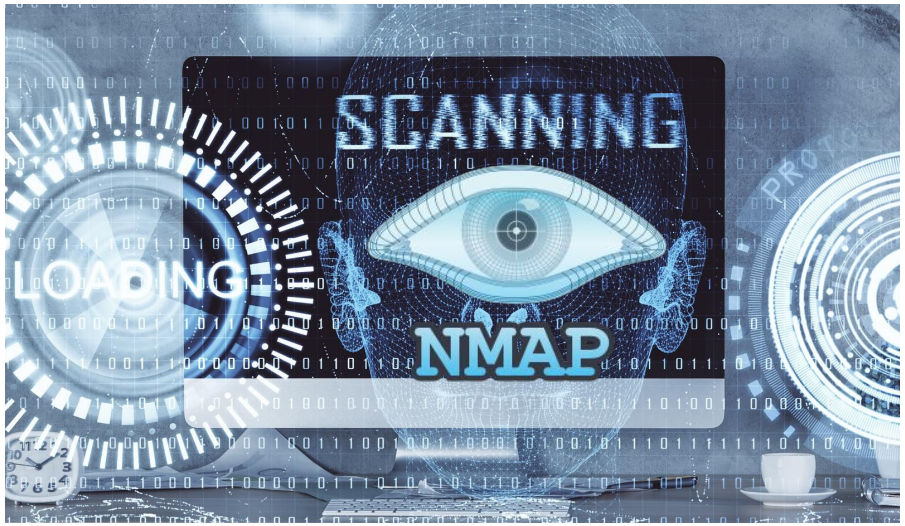
  - Lembre-se de utilizar a última versão estável disponível.
    - SSH v2 com strong crypto

Recomendações para Acesso

- **Básico**
  - Adicione uma **mensagem de login**.
  - **Existem governos que exigem** essas mensagens para o **âmbito legal**.
  - **Exemplo:**
    - “Roteador pertencente a empresa X, acessos não autorizados serão monitorados, investigados e entregues às autoridades responsáveis”

Recomendações para Acesso

- **Básico**
  - Mudar a porta padrão do serviço de acesso.
  - Bloquear acesso a porta padrão.
  - Não é bem uma proteção mas pode ajudar contra um ataque simples que procura portas padrão.



Recomendações para Acesso

- **Básico**
  - Armazene informações para auditoria
    - Log de ações
      - Identifica comandos indevidos
    - Log de tentativas de acesso.
      - Identifica ataque de força bruta
      - Identifica ataque de negação de serviço
      - Identifica tentativa de roubo de informações

  - Crie políticas de mitigação de ataque
      - Filtros
      - Blackhole

Recomendações para Acesso

- **Básico**
  - Utilize a hora legal brasileira com ntp.br

Recomendações para Acesso

- **Básico**
  - Não permita acesso por todas as interfaces dos equipamentos.
  - Escolha uma interface de loopback para os seus serviços:
    - São mais estáveis
    - Não sofrem com variações no link
    - Caso uma interface física fique indisponível os protocolos de roteamento procuram um novo caminho.
  - Faça essa interface parte da sua rede de gerência.

Recomendações para Acesso

- **Básico**
  - Forçar o logout depois de um tempo de inatividade.
    - Isso evita que alguém use sua máquina em seu período ausente.
    - Isso evita que um atacante monitore o seu tempo de inatividade para tomar controle da máquina.
  - Forçar o logout depois de se desconectar o cabo.
    - Isso evita que alguém reconecte o cabo e use o seu login.

Recomendações para Acesso

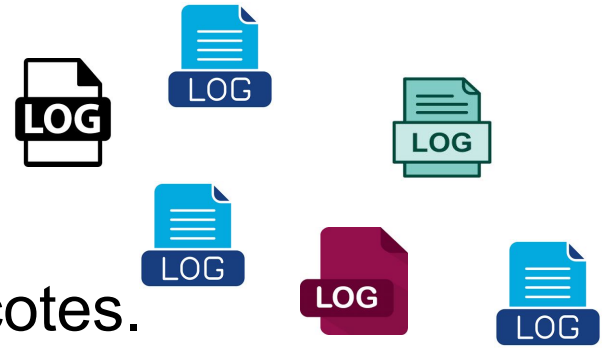
- **Avançado**
  - **Port Knocking**
    - Nenhuma porta aparece aberta no scan
    - Diminui a superfície de ataques
    - Para acessar um serviço
      - Testar uma sequência de portas fechadas.
      - Configurar a mudança de regras de firewall dinamicamente.
      - Conectar na porta desejada.

Lab 1d - Configurando senha no Mikrotik

ceptro.br nic.br cgi.br

Recomendações para Logs

- **Básico**
  - Configure logs com diferentes níveis de criticidade.
  - Evite gerenciar logs dentro dos roteadores.
    - Quanto mais funções o roteador tiver que fazer, menos processamento será utilizado para rotear pacotes.



  - Envie de maneira segura os logs para uma outra máquina.
    - Algum agente malicioso pode interceptá-los.
  - Guarde de maneira segura seus logs.
    - Eles podem te ajudar num processo judicial.

  - Mantenha a hora correta com ntp.br

Recomendações para o Sistema

- **Básico**
  - Desative todas as interfaces não utilizadas.
    - Interfaces que não possuem cabos conectados.

  - Desative todas os serviços não utilizadas, inseguros e que podem ser utilizados para ataques de amplificação.
    - Testador de banda
    - DNS recursivo
    - Servidor NTP
  - Remova ou desative os pacotes de funções extras não utilizados.
    - Pacote wireless

Recomendações para o Sistema

- **Básico**
  - Desabilite protocolos de descoberta de vizinhança:
    - CDP
    - MNDP
    - LLDP
  - Facilita para o atacante descobrir o tipo do seu roteador.
  - Inundam a rede com mensagens desnecessárias.
  - Tome cuidado com o IPV6:
    - Descoberta de vizinhança é essencial.
    - Sem ela, nada funciona.

Recomendações para o Sistema

- **Básico**
  - Mantenha o sistema sempre atualizado na versão estável.
    - Incluindo seus pacotes.
  - Aplique todos os patches de segurança.
  - Procure testar as atualizações, antes de aplicar em produção, num ambiente controlado.
    - Emulador.
    - Simulador.

Lab 1e - Ataque de Sniffing de pacotes em protocolos sem segurança

ceptro.br nic.br cgi.br

Recomendações para Configurações

- **Básico**
  - Mantenha sempre um backup atualizado das configurações atuais.
  - Envie de maneira segura esse backup para uma outra máquina.
    - Email criptografado
    - SCP
    - SFTP
  - Lembre, o operacional da sua empresa está guardado lá!
    - Hashes de senhas podem ser quebrados!

Recomendações para Configurações

- **Básico**
  - Mantenha um script de hardening de roteadores.
  - Assim ao comprar um novo roteador, você saberá as políticas mínimas de segurança que precisam ser aplicadas.
  - Mantenha esse script atualizado. Cada nova política precisa ser agregada ao script.

Lab 1f - Ataque nos hashes vazados

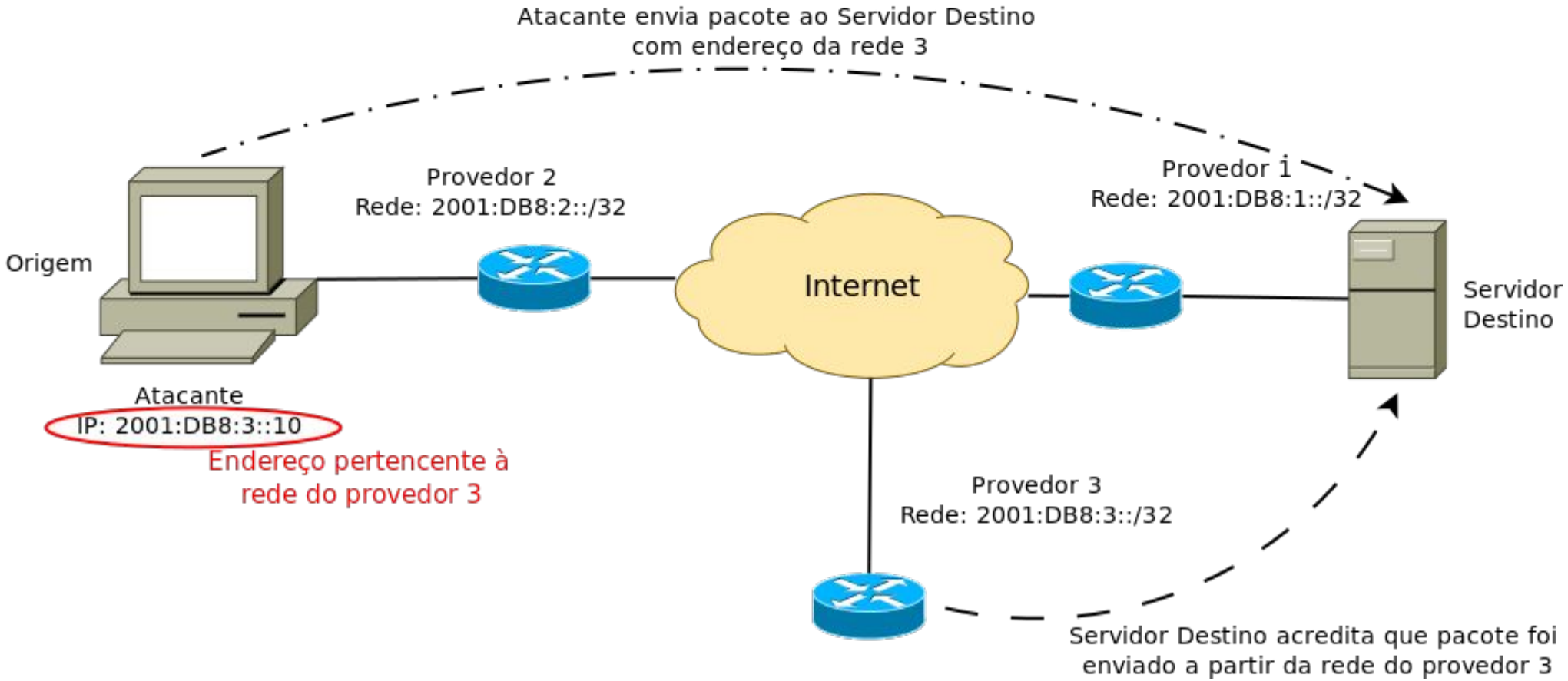
ceptro.br nic.br cgi.br

Antispoofing

- **O que é spoofing?**
  - Pacotes IP com endereços de origem incorretos.
    - **Erro de configuração**
      - Problema de Software
    - **Teste e Simulação**
      - 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.

Antispoofing

- **Ataque usando spoofing**



Antispoofing

- **Recomendações**
  - Implementar um sistema que permita a validação do endereço de origem.
    - Nos seus usuários finais
    - Na sua infraestrutura

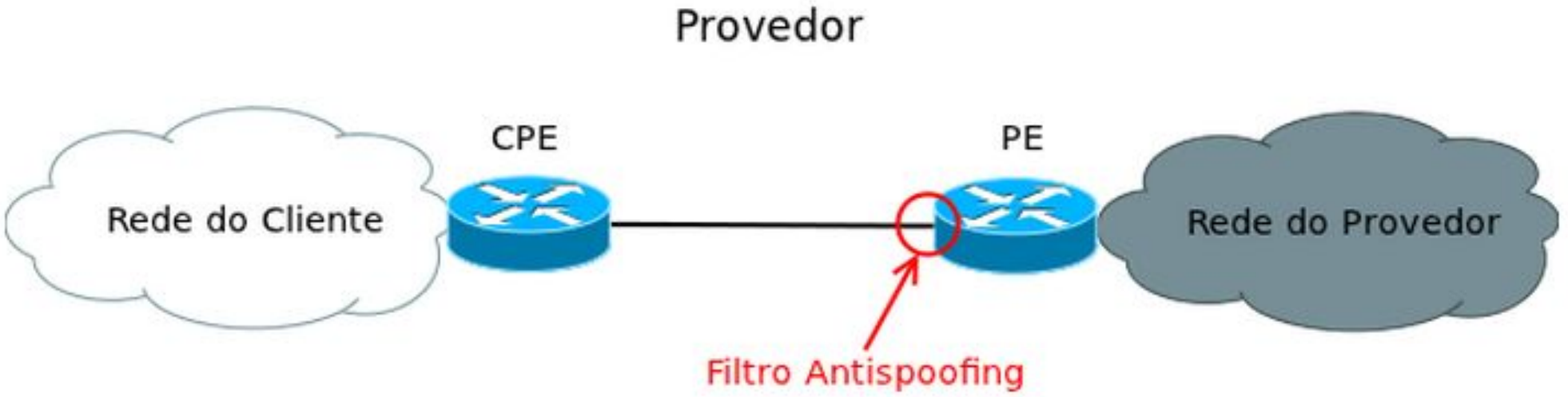
  - Implementar a filtragem contra falsificação de endereço IP de remetente.
    - Impedir que pacotes com endereço IP de remetente incorretos entrem e saiam da rede

Antispoofing

- **Para resolver o problema**
  - **Ingress Access Lists**
    - Access Control List - ACLs
  - **Unicast Reverse Path Forward (uRPF)**
    - Strict Mode
    - Loose Mode
  - **Source Address Validation Improvement (SAVI)**

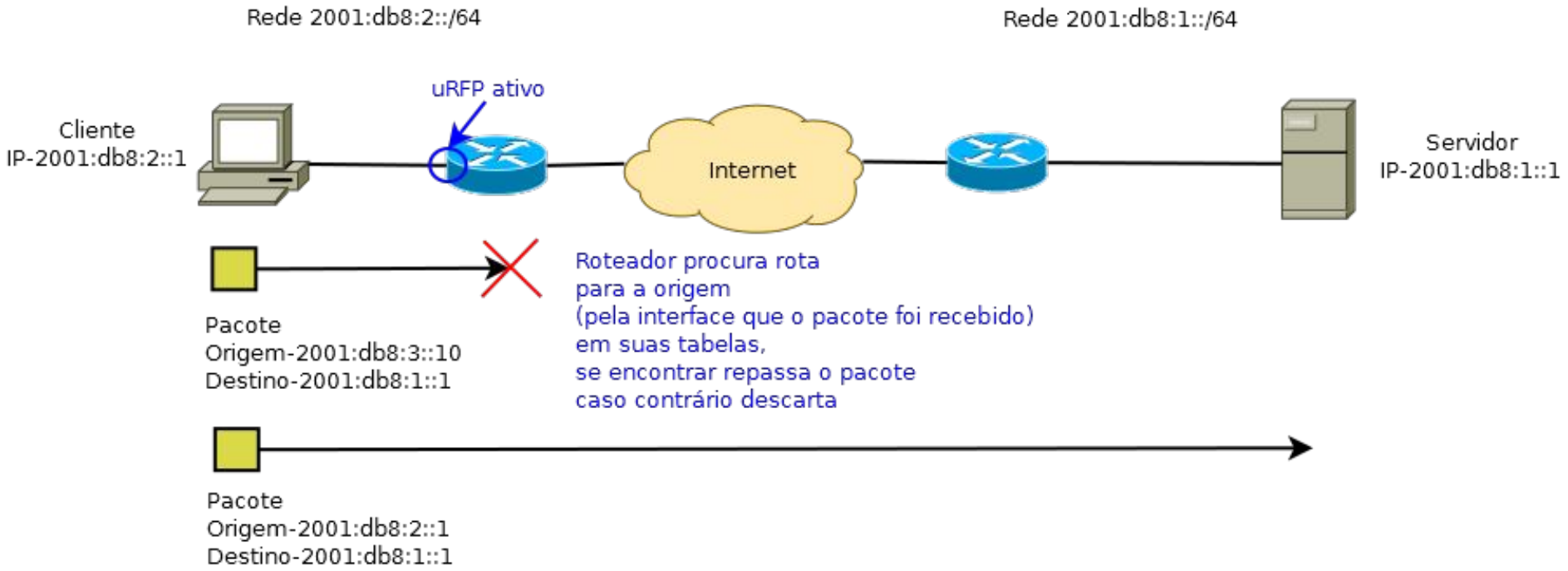
Antispoofing

- **Para resolver o problema**
  - **Ingress Access Lists**
    - Access Control List - ACLs



Antispoofing

- **Para resolver o problema**
  - **Unicast Reverse Path Forward (uRPF)**
    - Strict Mode
    - Loose Mode



Lab 1g - Spoofing

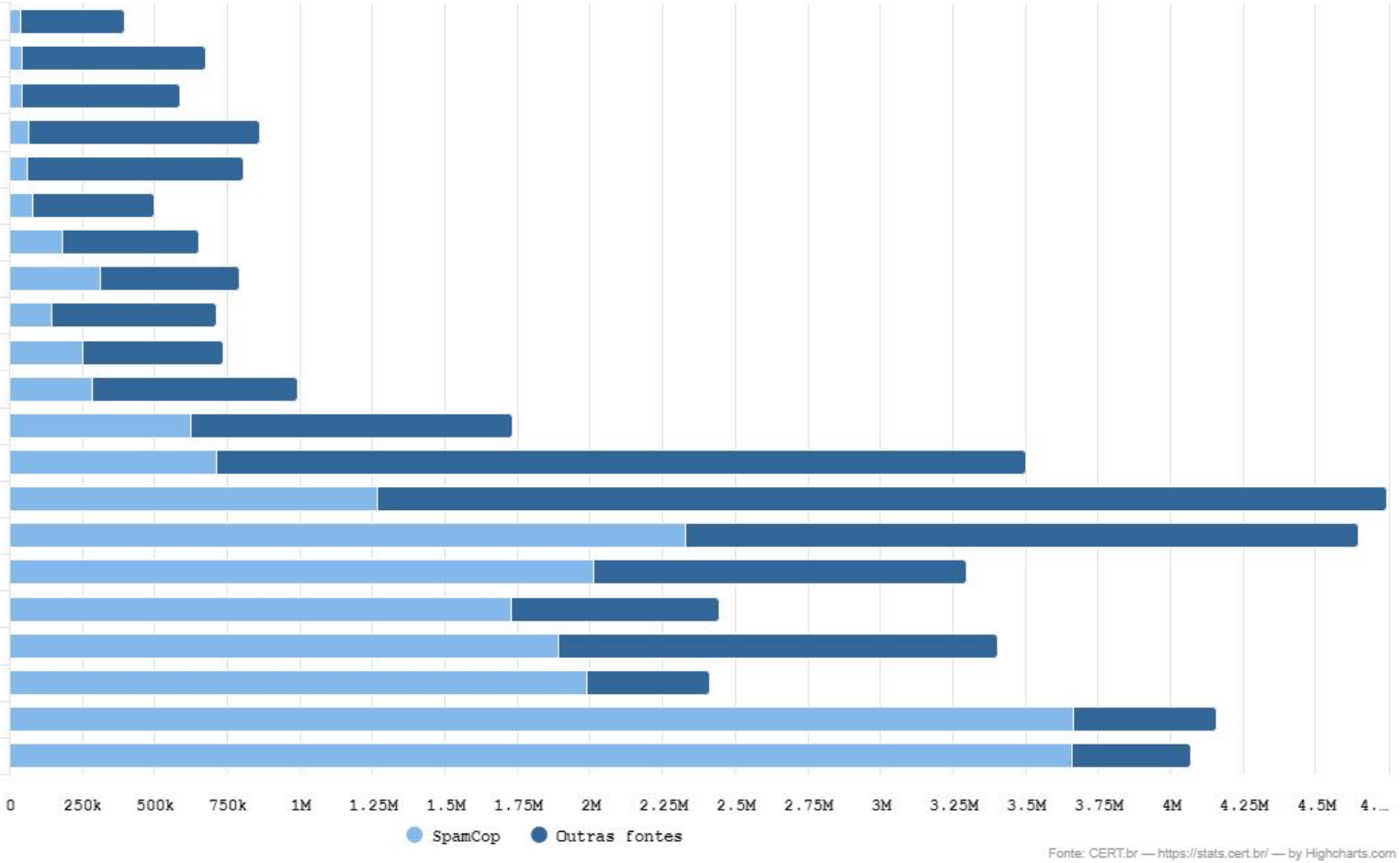
ceptro.br nic.br cgi.br

AntiSpam

Spams Reportados ao CERT.br por Ano

2003 a Agosto de 2023

Ano	SpamCop	Total
2023	36.215	397.928
2022	44.012	674.535
2021	43.770	586.882
2020	65.485	863.459
2019	61.899	806.021
2018	78.679	497.066
2017	180.643	650.292
2016	312.018	791.740
2015	144.267	711.467
2014	250.392	735.262
2013	283.923	993.088
2012	626.312	1.731.842
2011	711.333	3.502.521
2010	1.266.974	4.745.295
2009	2.327.388	4.646.468
2008	2.012.987	3.297.973
2007	1.729.037	2.446.154
2006	1.889.658	3.403.430
2005	1.989.902	2.414.200
2004	3.665.200	4.156.382
2003	3.661.569	4.072.334



Fonte: CERT.br — https://stats.cert.br/ — by Highcharts.com

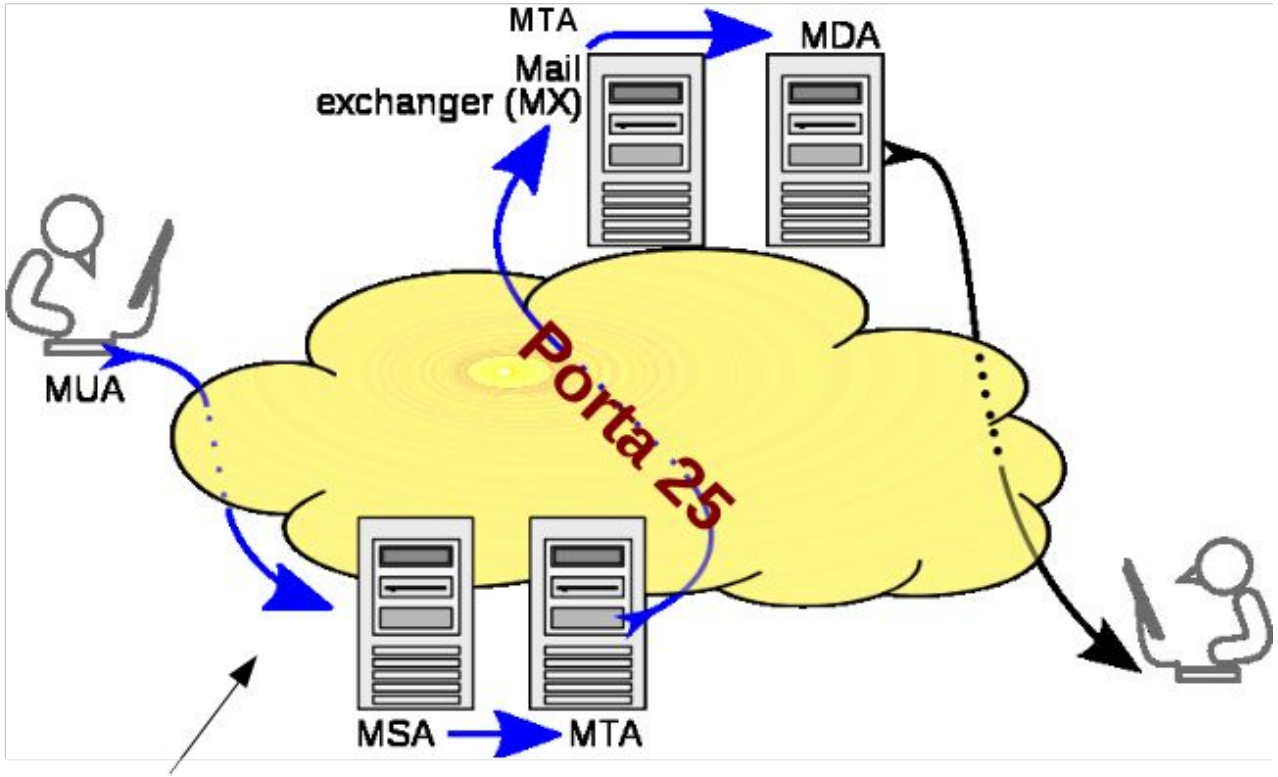
AntiSpam

- **O que é Gerência de 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.**

AntiSpam

- **Funcionamento do email**



Porta 587

- **MUA** – Mail User Agent
- **MSA** – Mail Submission Agent
- **MTA –** Message Transfer Agent
- **MX =** Mail Exchanger
- **MDA =** Mail Delivery Agent

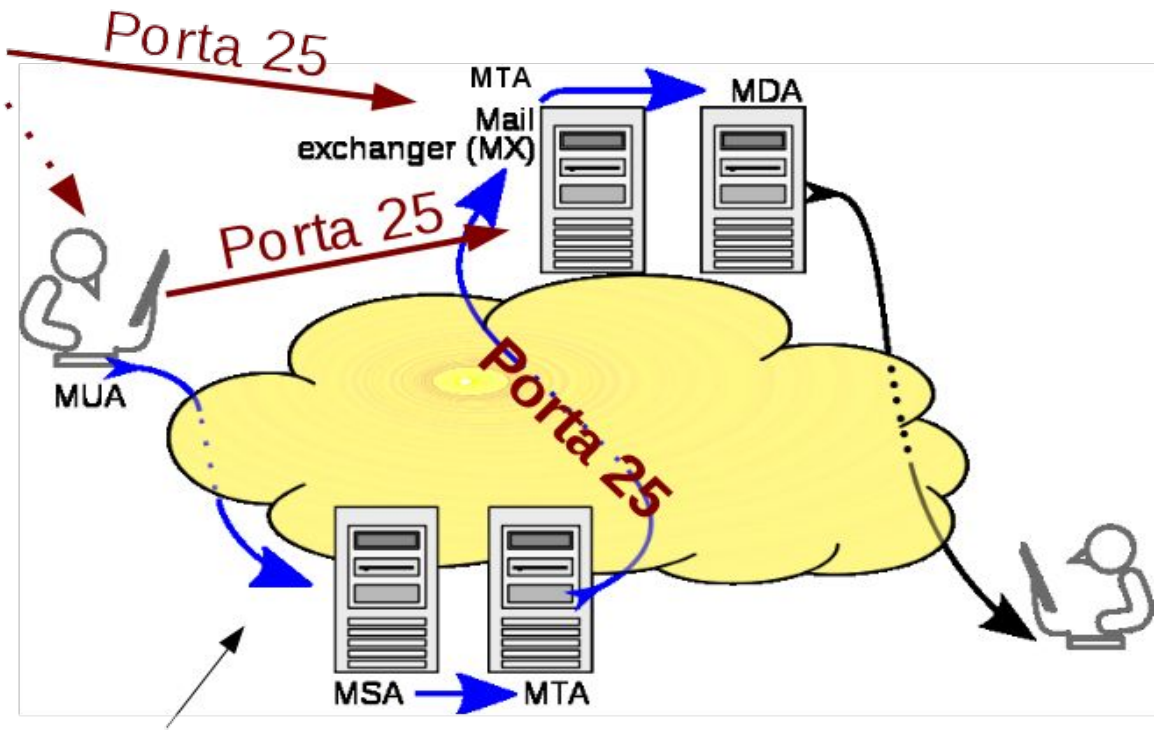
AntiSpam

- **Qual o raciocínio?**
  - Os **usuários residenciais** normalmente enviam e-mails utilizando:
    - Mail Submission Port (587)
    - Web (80)

  - Os **spammers, fraudadores, e códigos maliciosos utilizam a porta 25**.

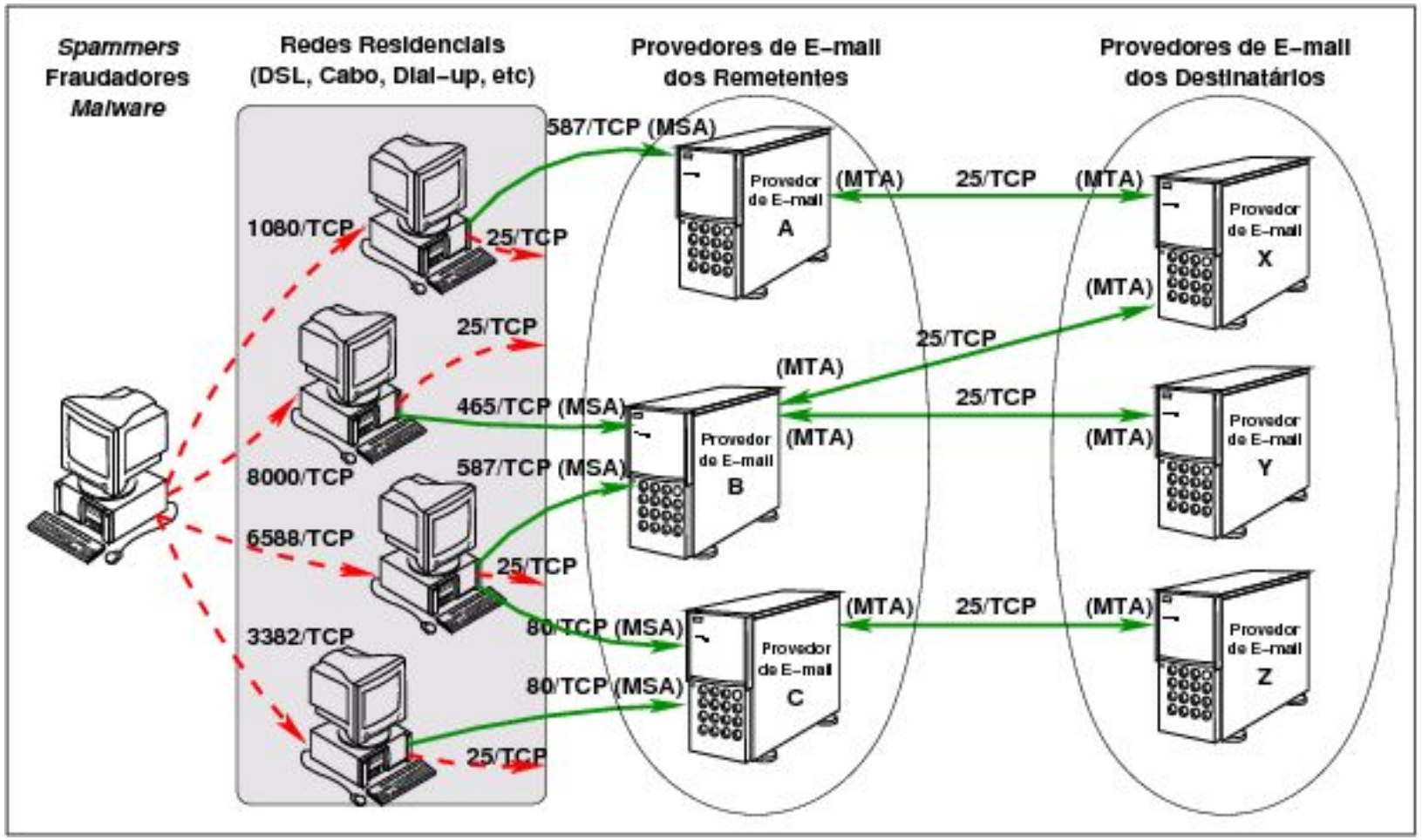
AntiSpam

- **Spammer**



AntiSpam

- **Gerência da Porta 25**



Lab 1h - Filtros: Gerência da porta 25

ceptro.br nic.br cgi.br

Obrigado!

CEPTRO.br Cursos: cursosceptro@nic.br
CEPTRO.br IPv6: ipv6@nic.br

@comunicbr
@nicbr
@NICbrvideos

nic.br cgi.br

www.nic.br | www.cgi.br