# Impactos da Gerência de Porta 25 para os Sistemas Autônomos no Brasil
# ou
# *"Agora Vai!"* :-)

**Cristine Hoepers**
**cristine@cert.br**

**Klaus Steding-Jessen**
**jessen@cert.br**

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

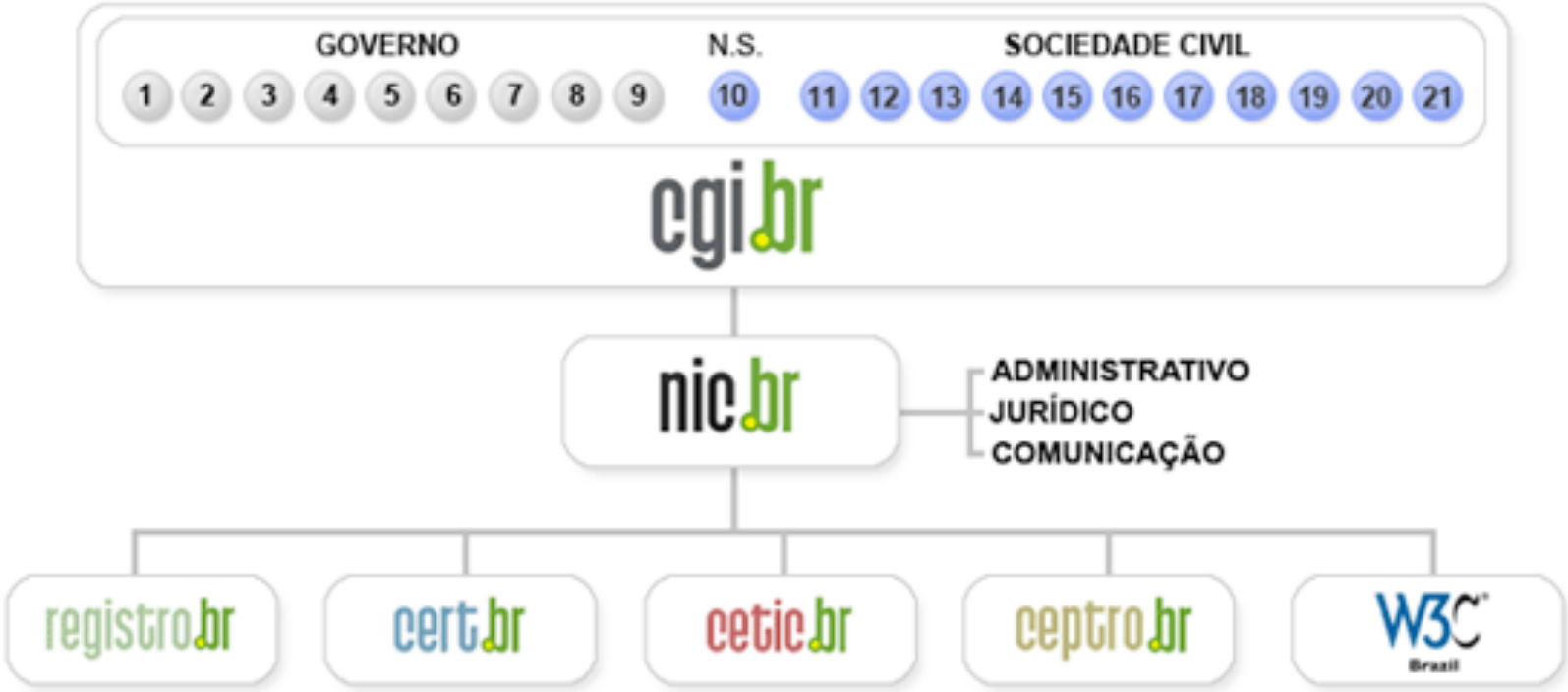
# Comitê Gestor da Internet no Brasil – CGI.br

**Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:**

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre-cg/

# Estrutura do CGI.br e NIC.br




1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

# cert.br

SEI Partner Carnegie Mellon

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT

## Tratamento de Incidentes

- Articulação
- Apoio à recuperação
- Estatísticas

## Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

## Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots

**Criado em 1997 para:**

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

# Agenda

- **Contexto**
  - **O abuso da infra-estrutura de Internet por *spammers***
  - **Gerência de Porta 25**
- **Assinatura do Acordo de Cooperação**
  - **ABTA, Anatel, Associações de Provedores, CGI.br, NIC.br, SindiTelebrasil**
  - **Definição de prazo para adoção – até dez/2012**
- **Como isso pode afetar os ASes no Brasil**
  - **Provedores de conectividade**
  - **Provedores de serviços de correio**

# O Problema do Abuso da Infra-estrutura de Redes do Brasil por *Spammers* Internacionais

**Para ganhar anonimato *spammers* e fraudadores:**

- **infectam computadores conectados via banda larga**
- **subvertem o caminho normal para o envio de *e-mails***

**Estudo do CGI.br mostrou que:**

- **Mais de 90% do tráfego observado era de tentativas de conectar diretamente em um servidor de *e-mails* do destinatário do *spam***
- **Os *spammers* abusam as redes do Brasil**
  - **Cerca de 99,9% de todo *spam* que tentou passar pelos sensores vinha de fora do Brasil**
  - **Mais de 90% tinham como destino redes fora do país**

**Fonte:**

- **Projeto mantido pelo CGI.br/NIC.br, como parte da CT-Spam**
- **Com sensores em 5 operadoras diferentes de cabo e DSL**
  **http://www.cert.br/docs/whitepapers/spampots/**

# Impactos Negativos do Cenário Atual

- **Blocos de IPs das redes brasileiras entram em listas de bloqueio**
  - **servidores de *e-mail* nesses blocos de endereçamento não conseguem enviar *e-mails***
- **A infra-estrutura da Internet banda larga do Brasil está sendo utilizada para atividades ilícitas (fraudes, furto de dados, etc)**
- **A banda está sendo consumida por *spammers***
  - **Para cada *spam* consome-se 2 vezes a banda internacional, para entrar no Brasil e voltar ao exterior**
- **Aumento dos custos operacionais**
  - **mais equipamentos, pessoal e banda para lidar com os *spams***
- **O Brasil é apontado como uma das maiores fontes de *spam* no mundo**

# A Gerência de Porta 25

**A "Gerência de Porta 25" é uma técnica que:**

- **Permite diferenciar**
  - **a submissão de *e-mails* de um usuário para seu(s) provedor(es)**
  - **da transmissão de mensagens entre servidores de serviços de *e-mail***
- **O Acordo aplica-se somente a redes de perfil residencial**
  - **IPs dinâmicos**
  - **ADSLs, Cabo e 3G em suas modalidades domésticas**

# Implementação da Gerência de Porta 25

**Depende da aplicação de medidas por provedores de *e-mail* e prestadoras de serviços de conectividade:**

- **Provedores de *e-mail*:**
  - **Passam a oferecer serviço de submissão de *e-mails* em uma porta diferente (587/TCP ou 465/TCP)**
  - **Instruirão os usuários sobre como configurar seus programas de *e-mail* (como Outlook, Thunderbird, etc)**
  - **Usuários de *webmail* não precisam fazer mudanças**

- **Prestadoras de serviços de conectividade residencial:**
  - **Devem filtrar o tráfego de saída com destino à porta 25/TCP**
  - **Esse filtro se aplicará apenas ao tráfego com origem nessas redes de perfil residencial**

# Benefícios da Adoção da Recomendação

- **Saída das redes brasileiras de listas de bloqueio de IPs envolvidos no envio de *spam***
- **Dificulta o abuso da infra-estrutura da Internet para atividades ilícitas (como fraudes, furto de dados, etc).**
- **Redução do abuso das máquinas dos usuários**
  - **diminuição na carga dos recursos computacionais**
  - **redução do consumo de banda para envio de *spam*, com conseqüente melhora nas condições de utilização da rede**
- **Atua antes do *spam* entrar na infra-estrutura de *e-mail***
  - **menos desperdício de banda e menos esforço de configuração de filtros anti-*spam*.**
  - **diminuição do consumo de banda internacional por *spammers***
  - **diminuição de custos operacionais**
- **Melhora da imagem do Brasil no exterior**

# Histórico do Acordo de Cooperação

**Trabalho desenvolvido pela Comissão de Trabalho Anti-*Spam* do CGI.br e pelo CERT.br, envolvendo as seguintes ações:**

- **Recomendado no Relatório Técnico "Tecnologias e Políticas para Combate ao *Spam*" em maio de 2005**
- **14 reuniões de trabalho com as partes envolvidas de 2008 a 2011**
- **Resolução do CGI sobre Gerência da Porta 25 em 2009**
  - **Resolução CGI.br/RES/2009/002/P**
    **http://www.cgi.br/regulamentacao/resolucao2009-02.htm**
- **Finalização do texto do acordo em julho de 2010**
- **Aprovação do acordo pela Anatel em abril de 2011**
- **Endosso do acordo pelo Departamento de Proteção e Defesa do Consumidor (DPDC/MJ), via Nota Técnica, em outubro de 2011**
- **Assinatura do acordo em 11 de novembro de 2011**
- **Anúncio para a Imprensa em 23 de novembro de 2011**

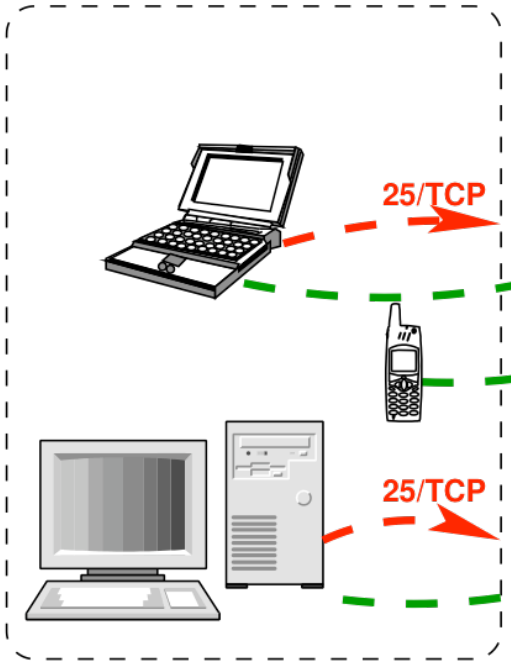
# Etapas para Implementação do Acordo

- **Associações de provedores / prestadores de serviço de *e-mail***
  - **terminar a migração dos usuários para serviços de submissão**
  - **informar o progresso da migração para as associações**
- **Prestadoras de serviço de conectividade**
  - **Bloquear a saída para porta 25/TCP, em serviços de banda larga residenciais, a partir do momento em que os provedores migrarem 90% dos usuários para serviços de submissão**
- **NIC.br**
  - **Acompanhar o processo de implementação desse acordo através de reuniões do grupo de trabalho**
  - **Coordenar o processo de comunicação das medidas**
  - **Apoio, suporte e treinamento**

# Cenário 1: Provedor de Conectividade a Usuário Residencial

**Quem provê a conectividade deve filtrar a saída de tráfego com destino à porta 25/TCP**

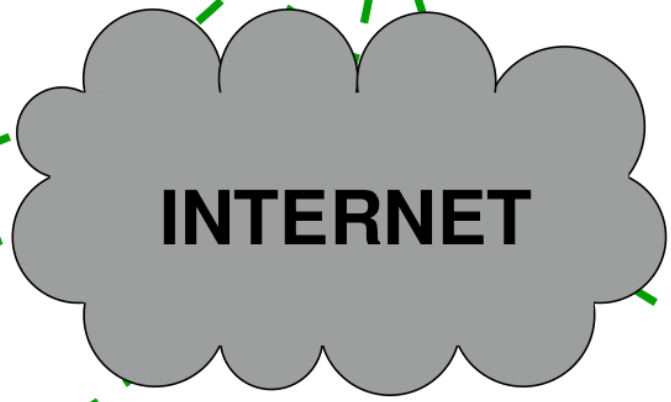
**Usuário Residencial (DSL, Cabo, 3G, Rádio, etc)**





**Quem provê o serviço de submissão deve habilitar o serviço na porta 587/TCP**

587/TCP

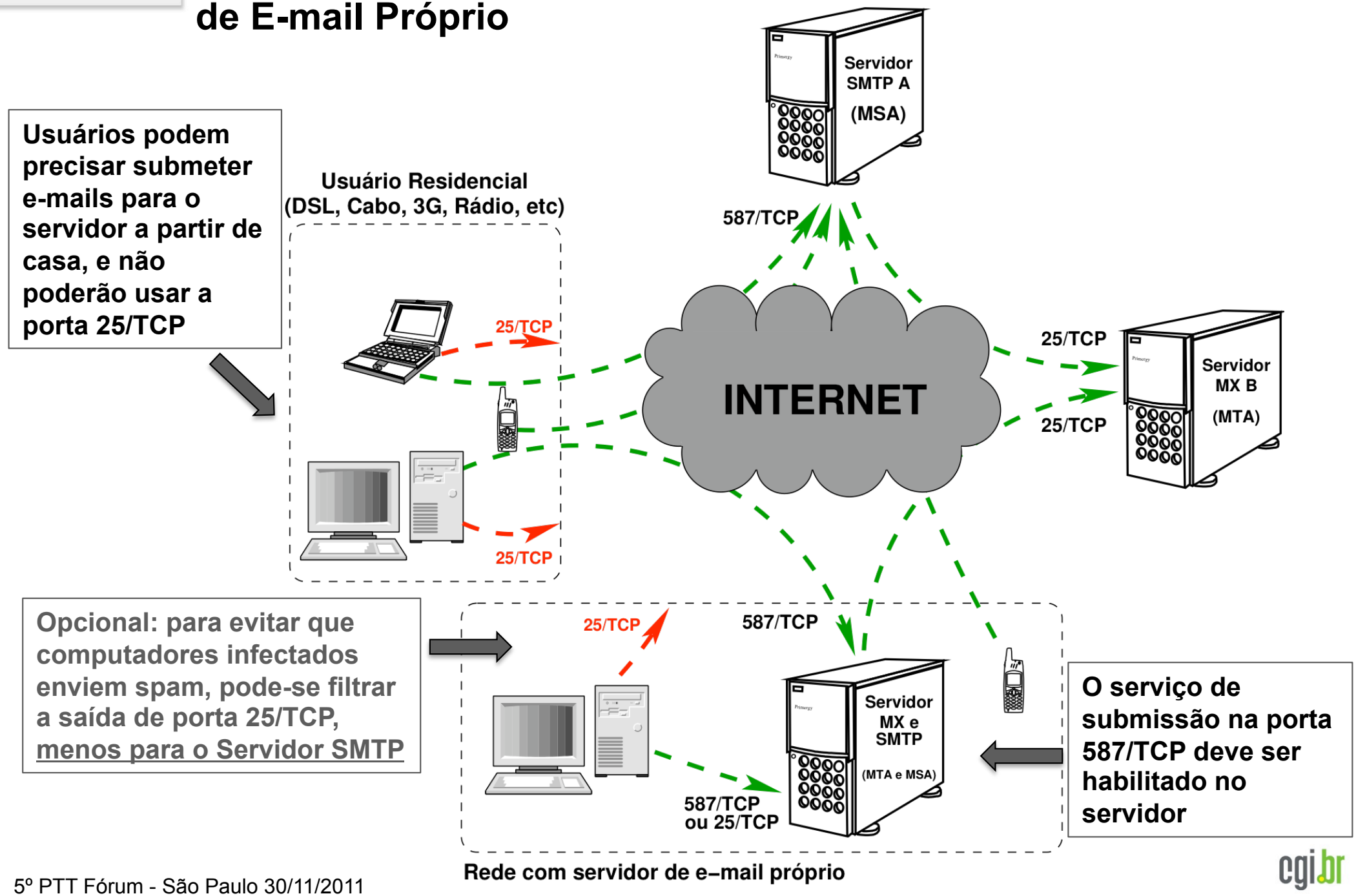



**Nada muda no transporte das mensagens entre MTAs**

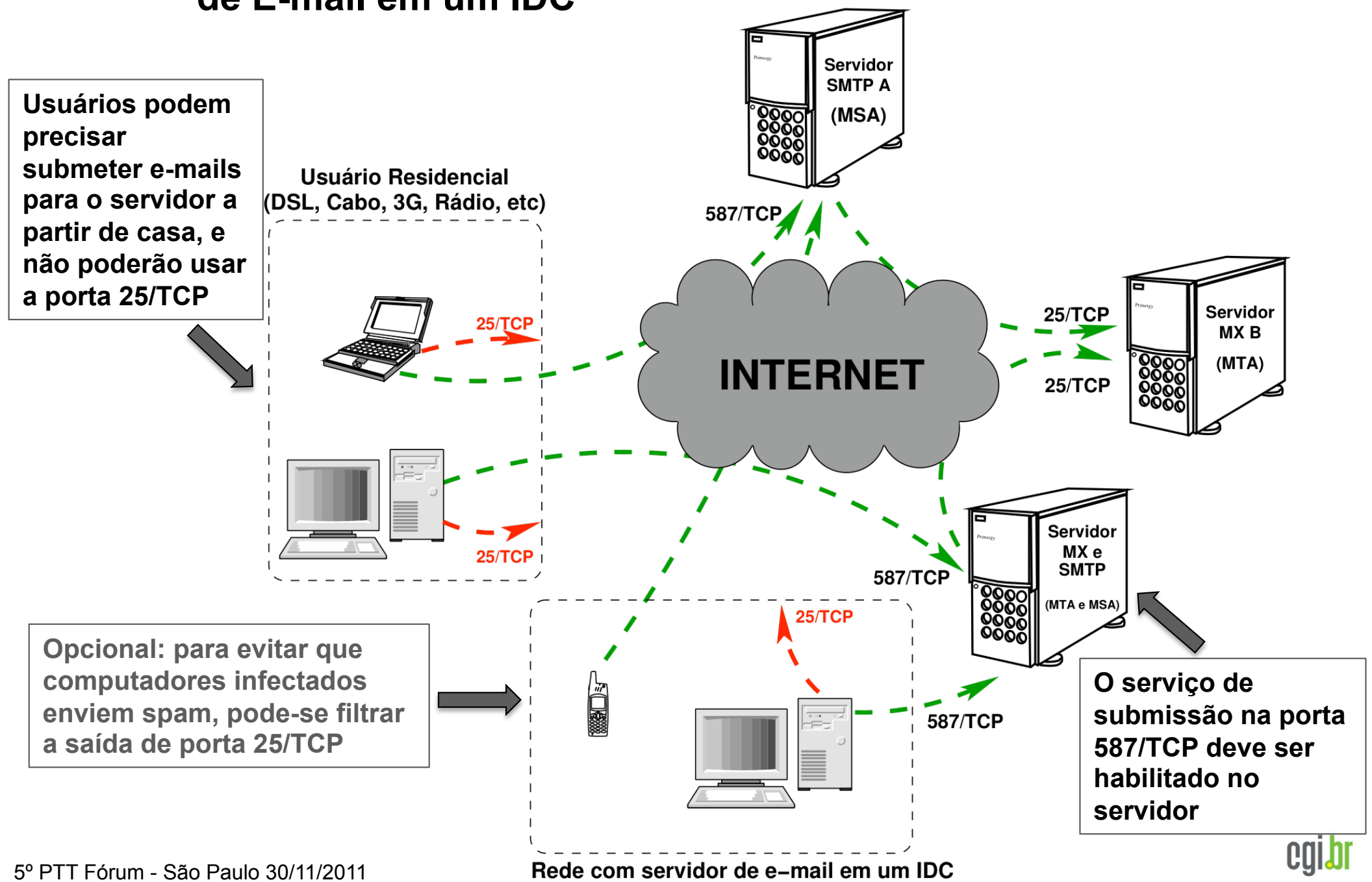
25/TCP


**Obs. 1: Nada muda para usuários de Webmail.**
**Obs. 2: A porta 465/TCP também pode ser usada para submissão.**

# Cenário 2: Provedor de Conectividade para Redes com Servidor de E-mail Próprio



# Cenário 3: Provedor de Conectividade para Redes com Servidor de E-mail em um IDC



# RFCs Relacionadas

- **RFCs Relacionadas**
  - **RFC 4409: Message Submission for Mail (*Standards Track*)**
    **http://www.ietf.org/rfc/rfc4409.txt**
  - **RFC 5068 / BCP 134: Email Submission Operations: Access and Accountability Requirements**
    **http://www.ietf.org/rfc/rfc5068.txt**
  - **RFC 4954: SMTP Service Extension for Authentication**
    **http://www.ietf.org/rfc/rfc4954.txt**
  - **RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security**
    **http://www.ietf.org/rfc/rfc3207.txt**

- **Antispam.br – Gerência de Porta 25**
  **http://www.antispam.br/admin/porta25/**