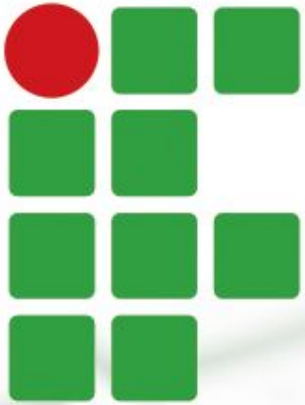


INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Admin. Serviços de Redes

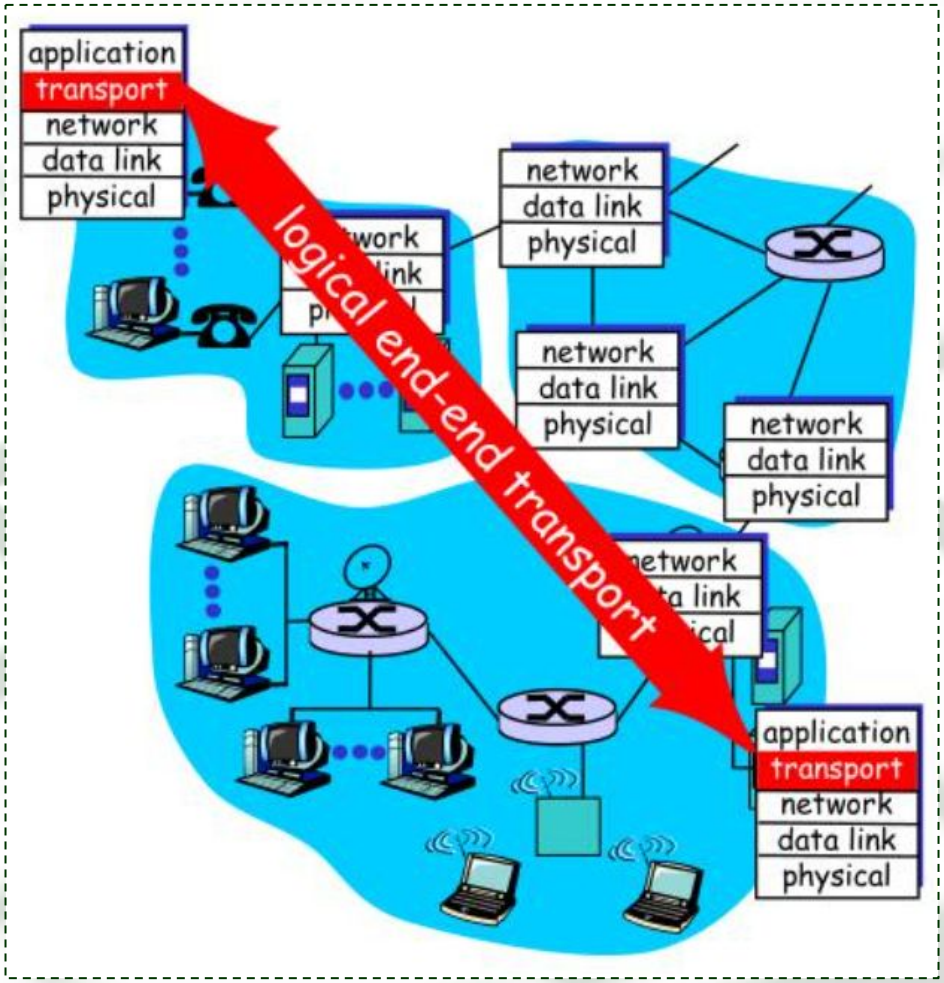
- NAT / CGNAT -

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

TCP / IP

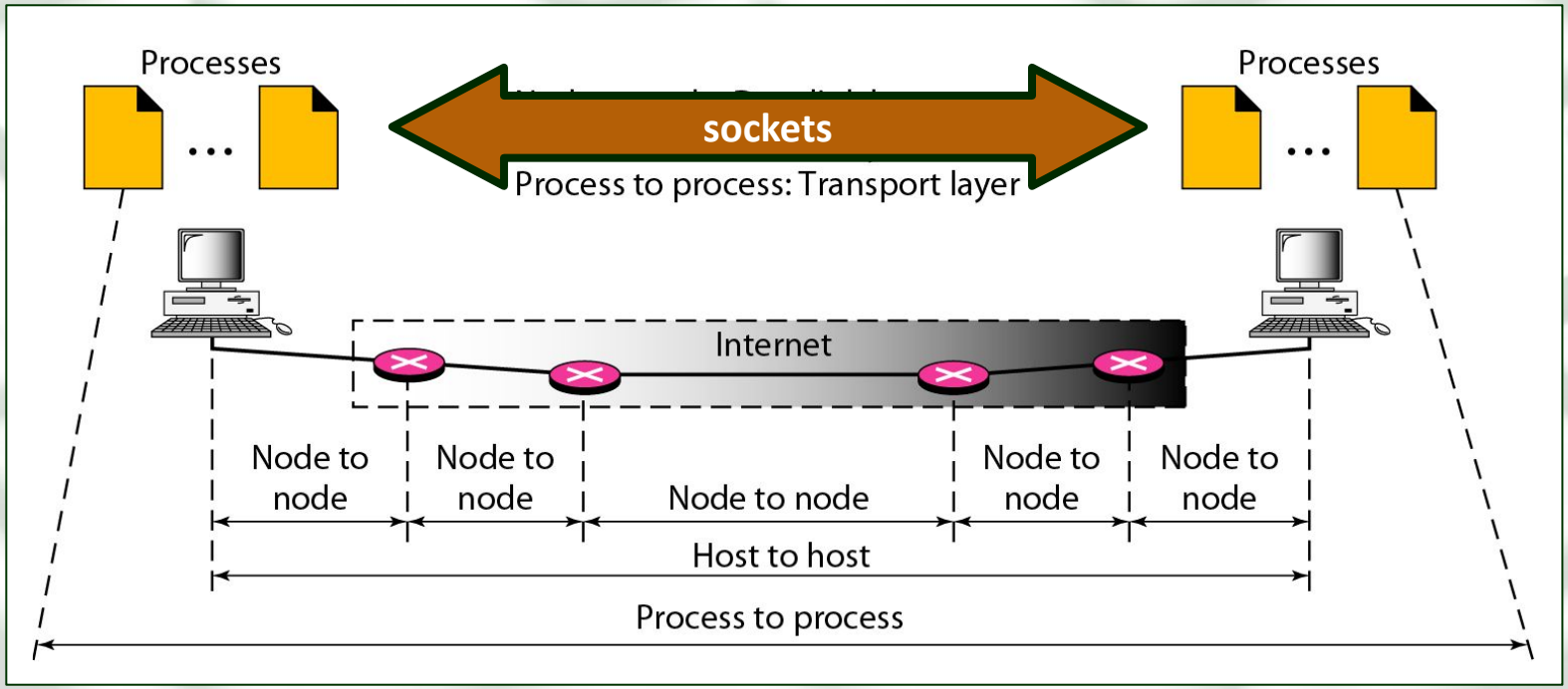
A **Conectividade fim-a-fim** sempre foi uma premissa fundamental da **Arquitetura TCP/IP.**

Isso significa dizer que **qualquer nó da rede pode estabelecer conexão**, de ponta a ponta, **com qualquer outro nó**.



TCP / IP

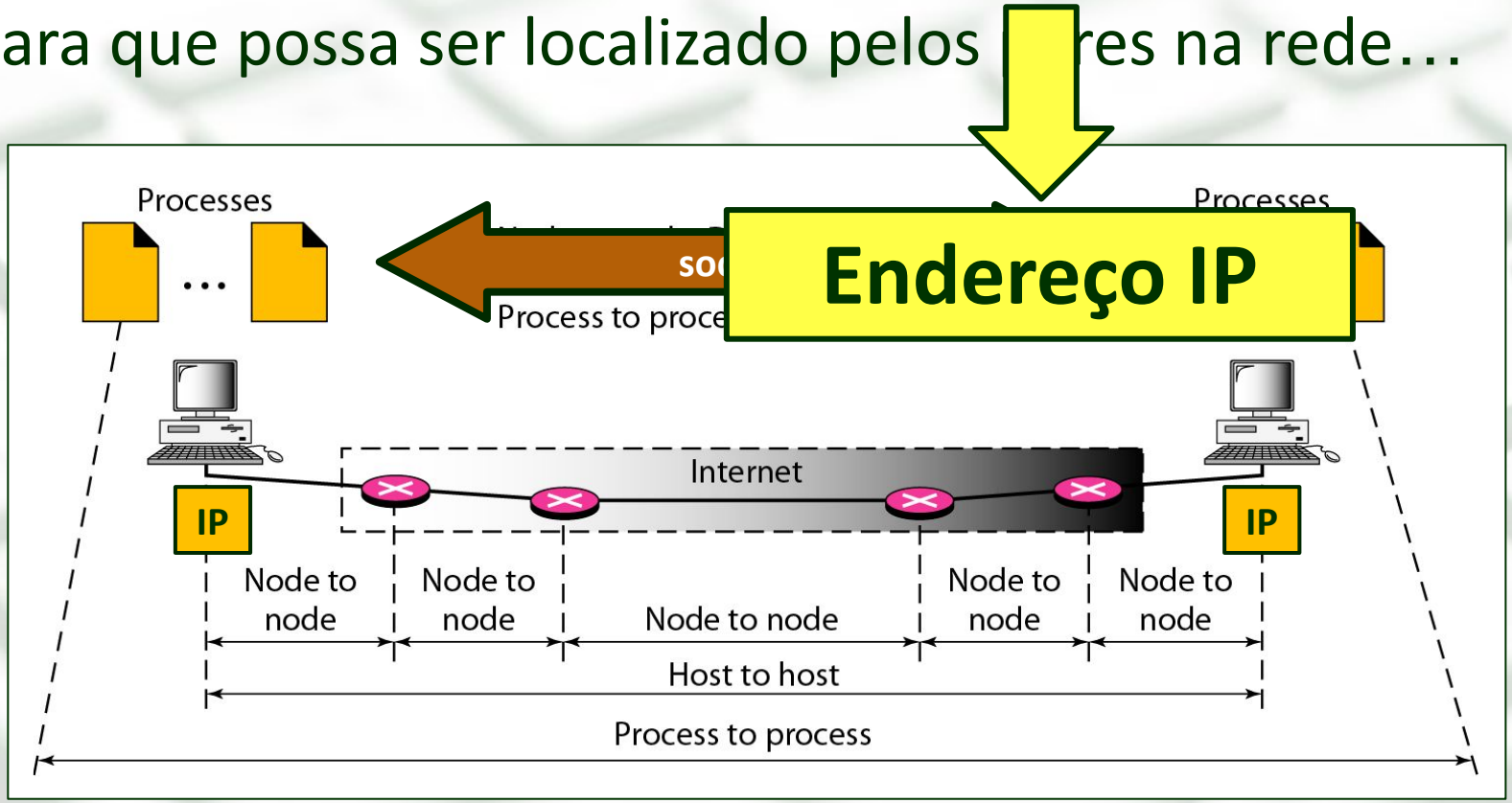
- Contudo, para que isso funcione, é necessário que **cada host possua um endereço globalmente único**, para que possa ser localizado pelos pares na rede…



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

TCP / IP

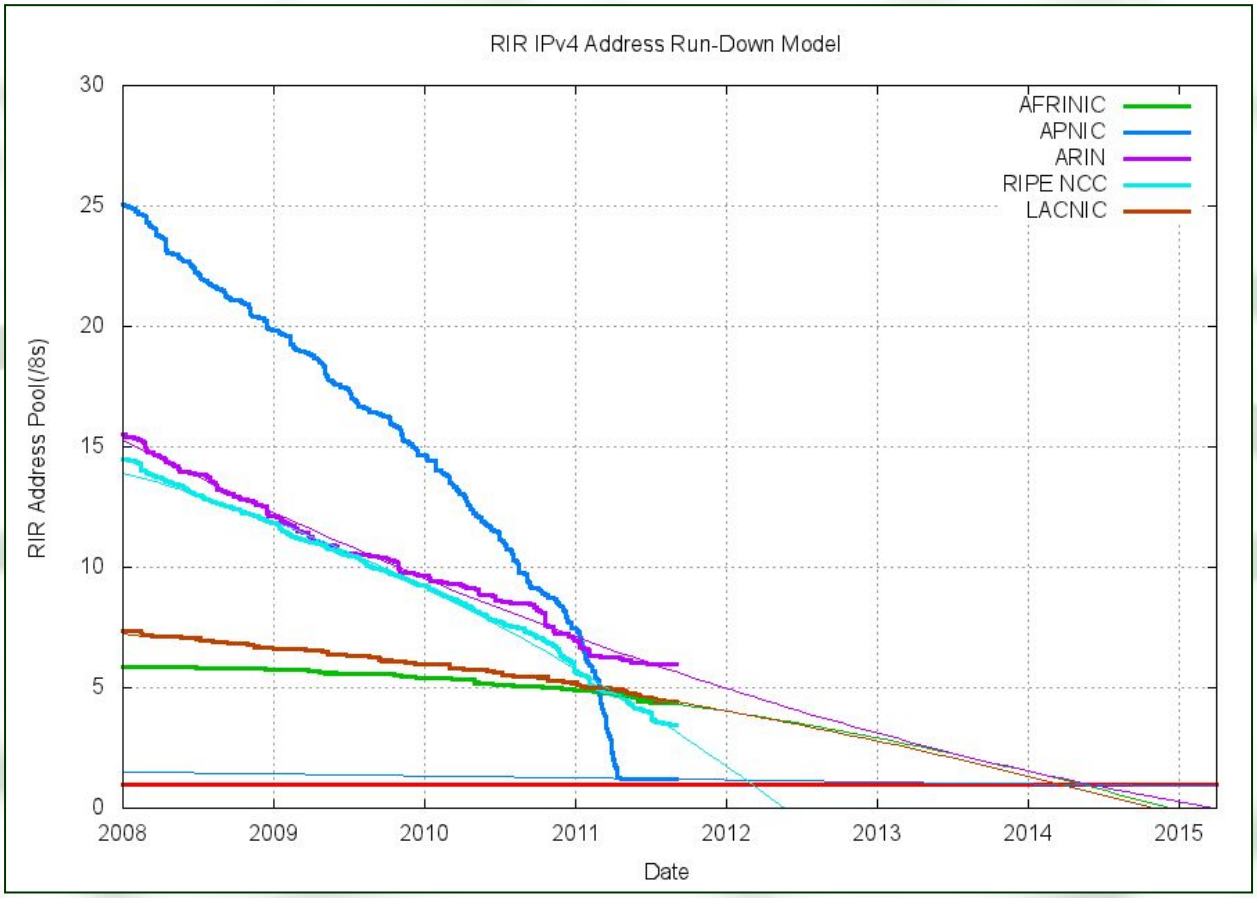
- Contudo, para que isso funcione, é necessário que **cada host possua um endereço globalmente único**, para que possa ser localizado pelos [illegible]res na rede…



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

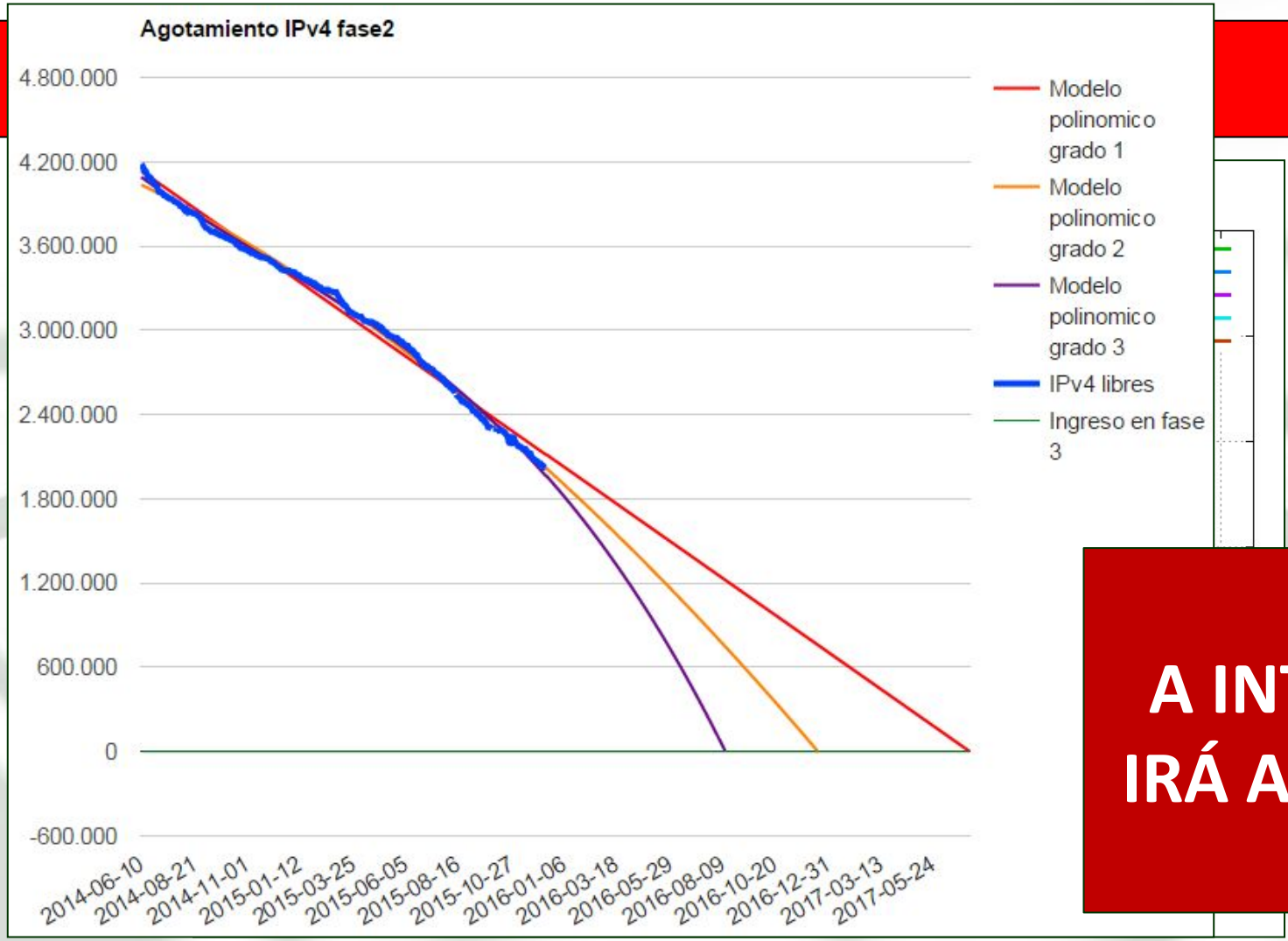
TCP / IP

OS ENDEREÇOS IP IRÃO SE ESGOTAR!



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

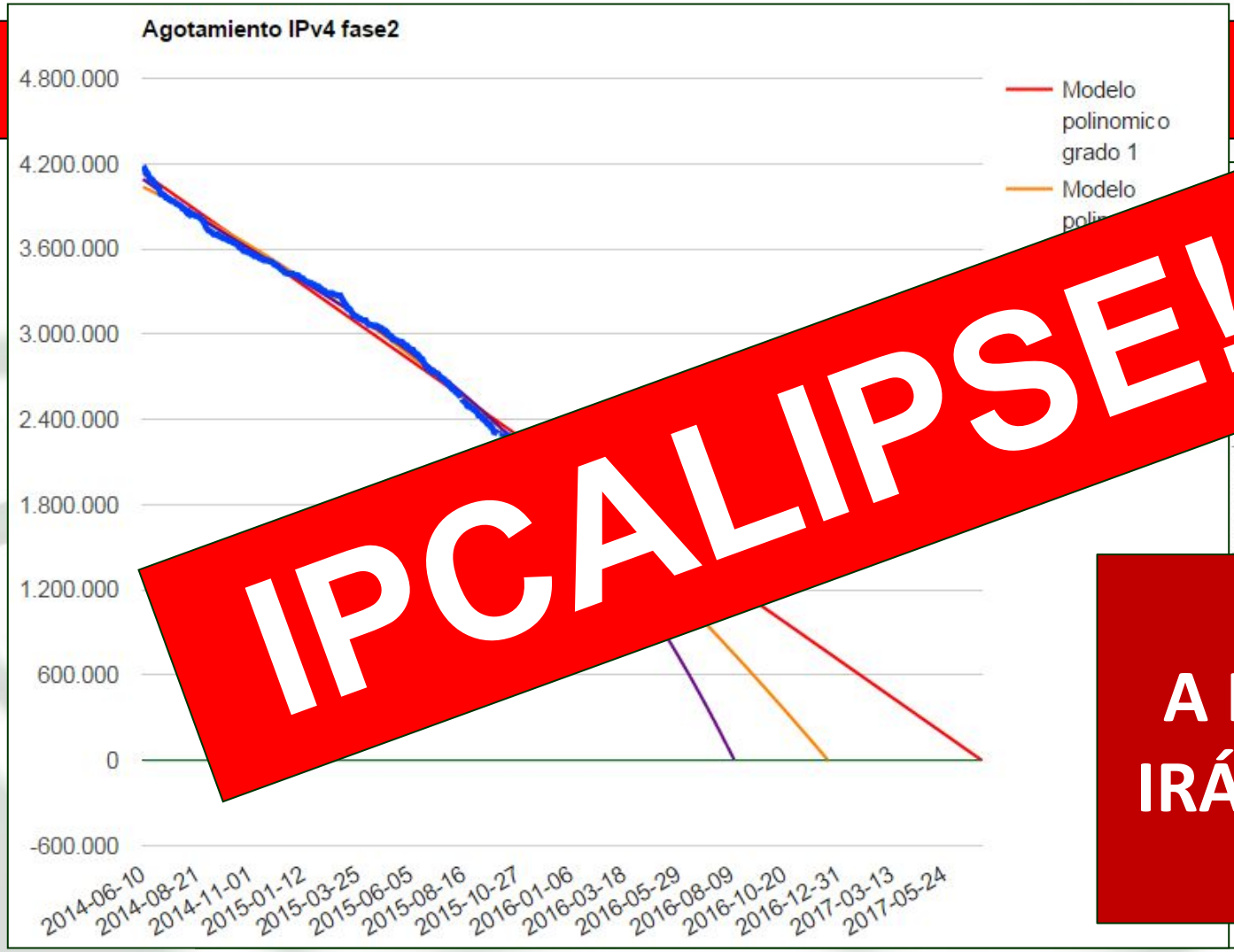
TCP / IP



A INTERNET IRÁ ACABAR!

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

TCP / IP

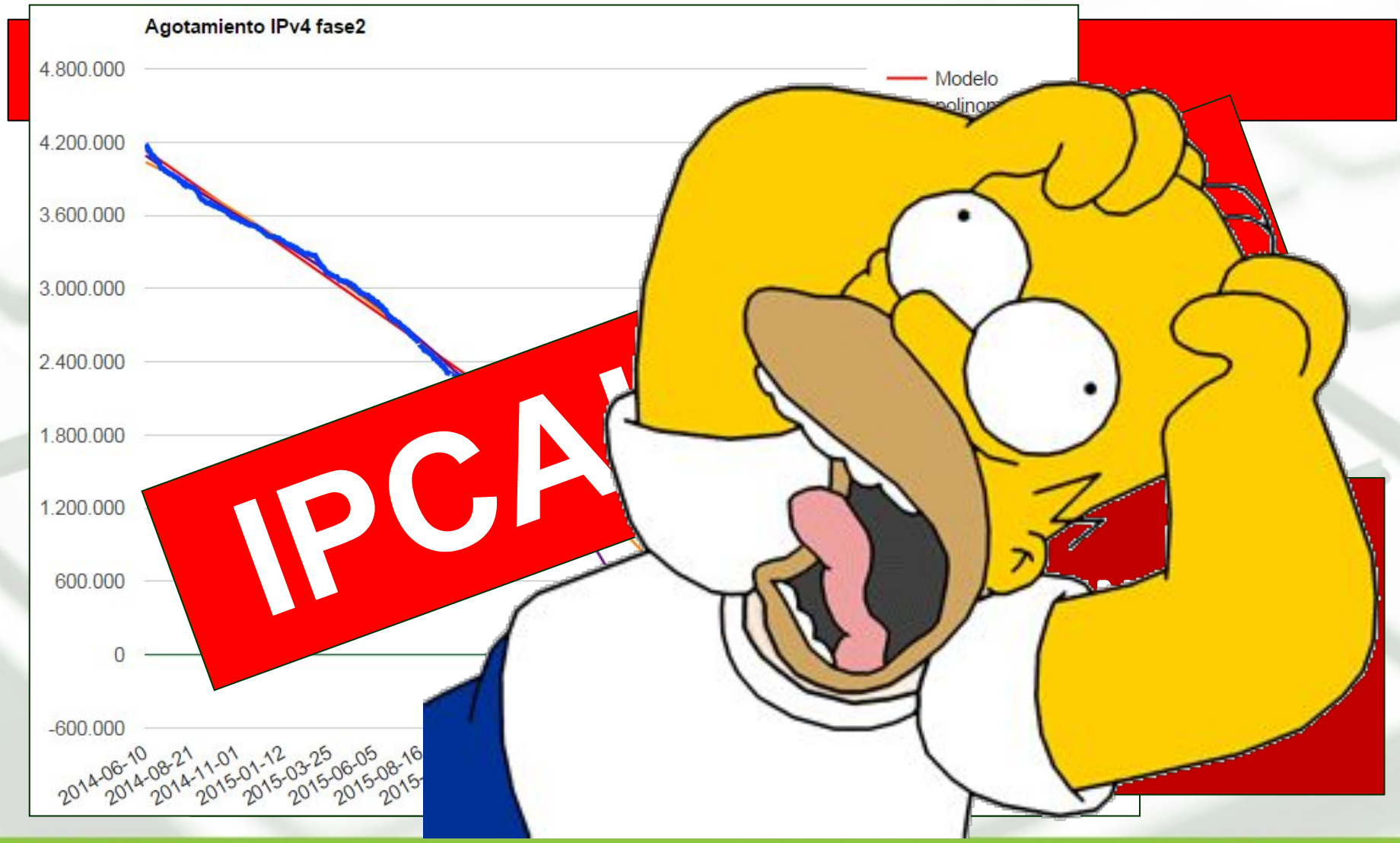


IPCALIPSE!!!

A INTERNET IRÁ ACABAR!

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

TCP / IP



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

TCP / IP

CALMA...

Nada que uma boa GAMBIARRA não resolva...

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

NAT

CALMA...

Nada que uma boa GAMBIARRA não resolva...

NAT

NAT / RFC 1918

- Na década de 90, a **RFC 1918** estabeleceu que 03 faixas de rede IP **não seriam mais roteáveis na Internet**.
- Essas faixas, denominadas faixas de **Rede Privada**, seriam utilizadas apenas para **endereçar hosts internos às redes locais**, sejam domésticas ou empresariais...

RFC 1918 Address Allocation for Private Internets February 1996

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)

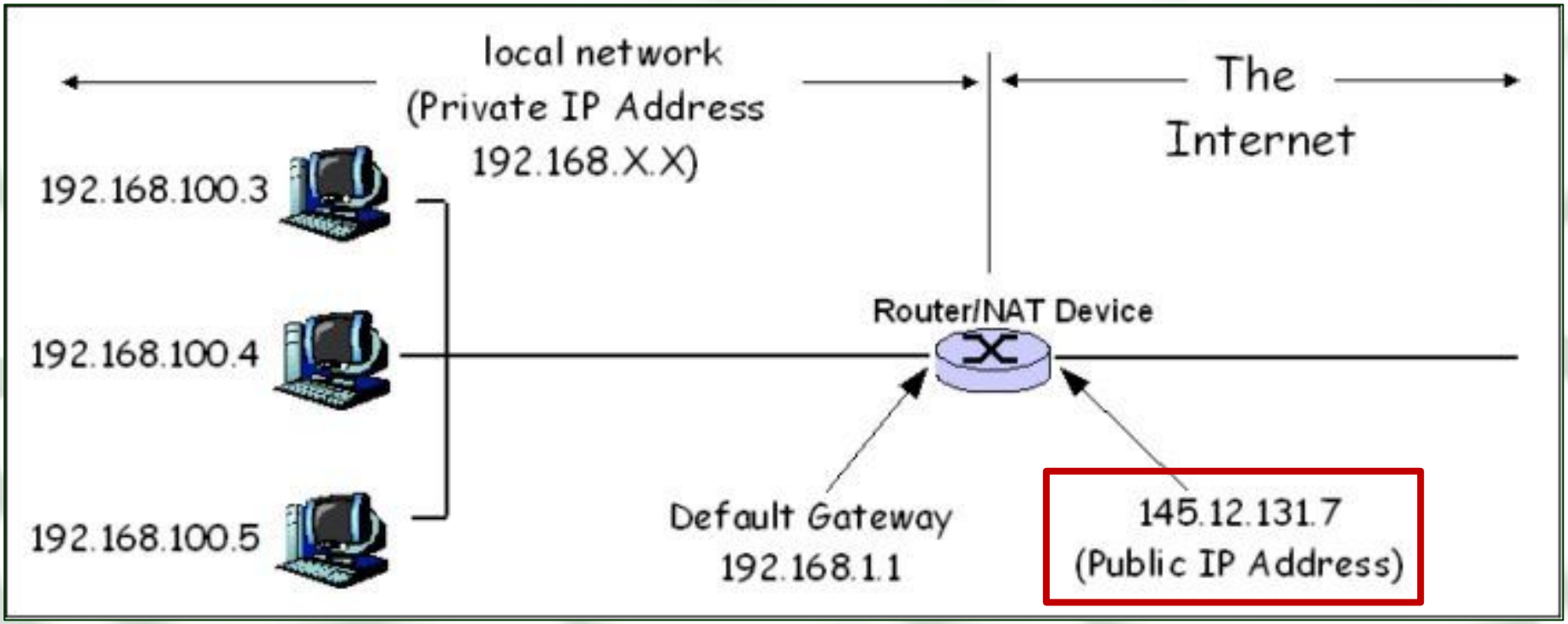
NAT / RFC 1918

- Com essa técnica, os inúmeros hosts das redes LANs não necessitam mais consumir endereços globalmente únicos da Internet (chamados **Endereços Públicos**).
- As diversas redes LANs podem **usar a mesma faixa de rede**, por exemplo, 192.168.10.0/24, **sem que uma interfira no funcionamento das outras**, afinal, eram redes apenas de âmbito local.
- E, caso seja necessário acessar **algum servidor na Internet**, então os hosts locais devem **compartilhar um endereço globalmente válido (endereço público)**.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

NAT / RFC 1918

- NAT (***Network Address Translation***)

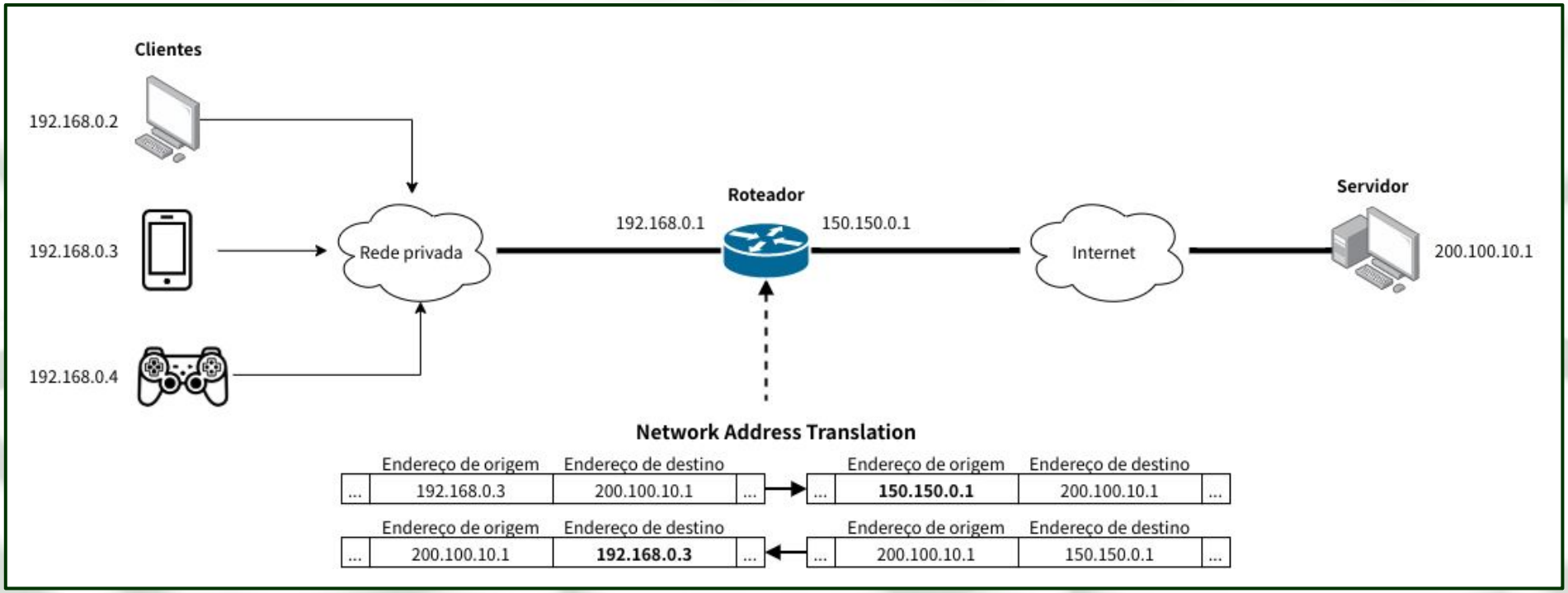


QUANDO UMA REQUISIÇÃO SAI DA REDE PRIVADA, É NECESSÁRIO ALTERAR O ENDEREÇO DE ORIGEM…

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

NAT / RFC 1918

- NAT (***Network Address Translation***)

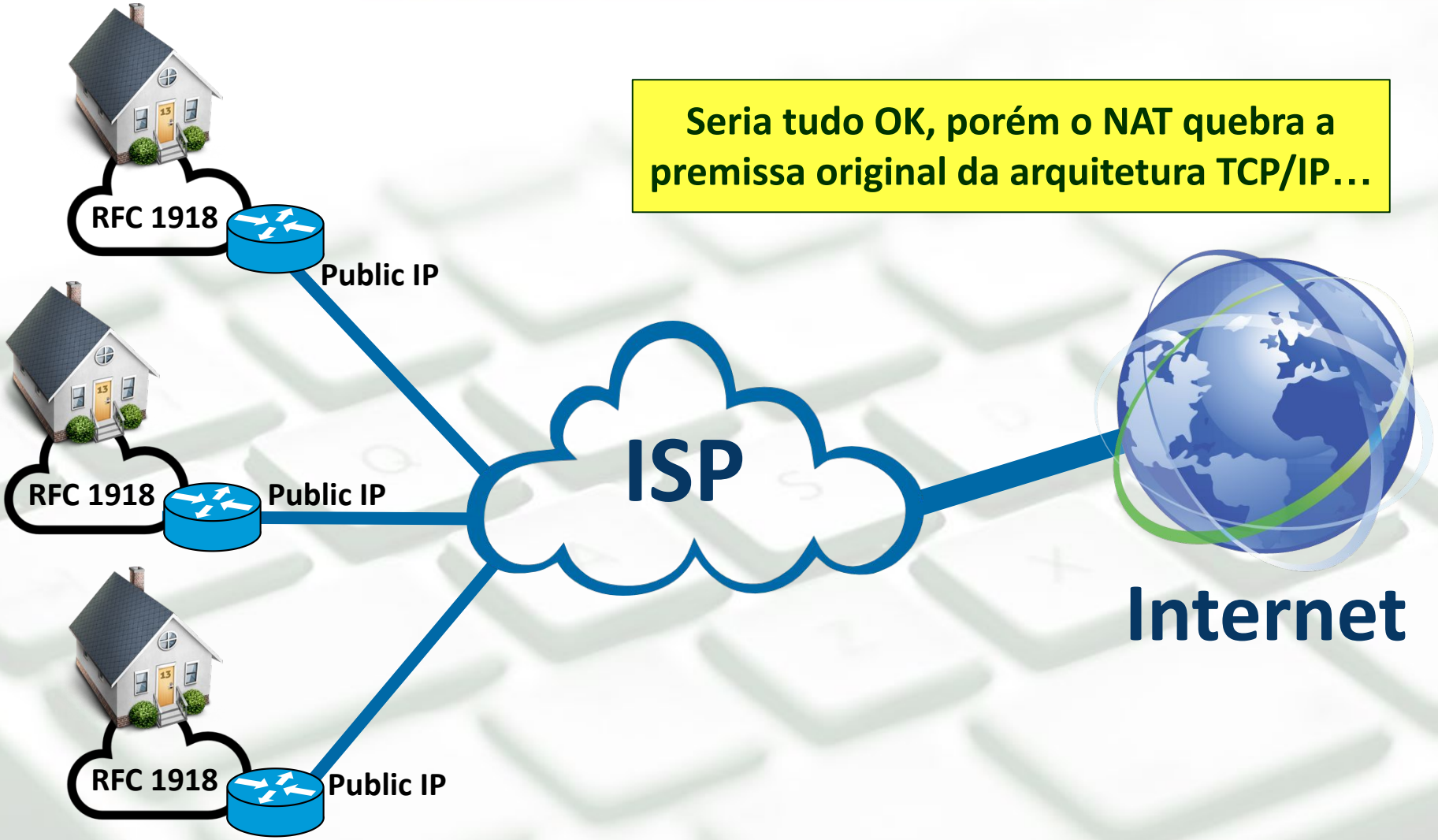


… E QUANDO A RESPOSTA CHEGA, É NECESSÁRIO TRADUZIR O ENDEREÇO PARA O DESTINO DEVIDO

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

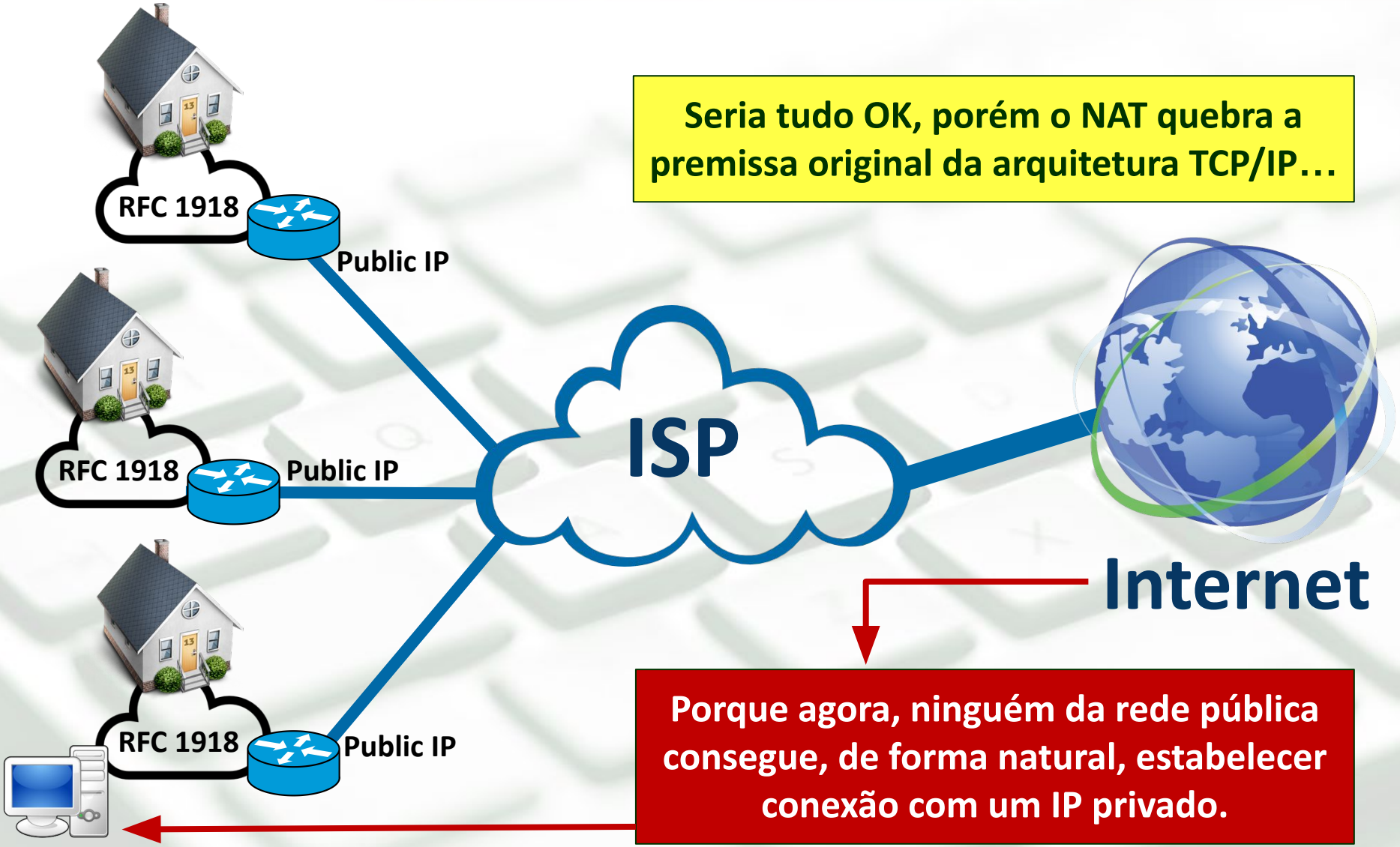
NAT / RFC 1918

Seria tudo OK, porém o NAT quebra a premissa original da arquitetura TCP/IP…



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

NAT / RFC 1918

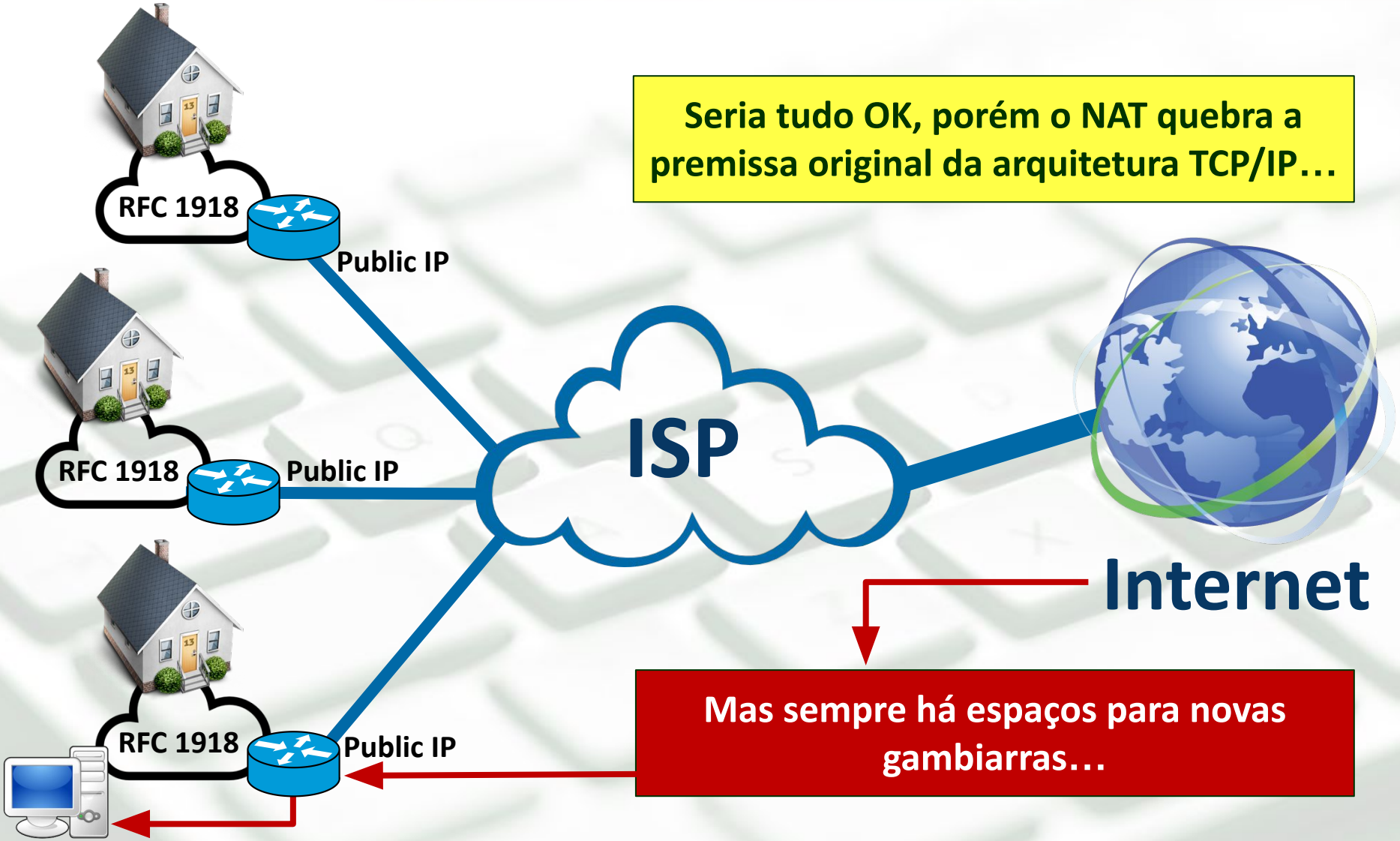


Seria tudo OK, porém o NAT quebra a premissa original da arquitetura TCP/IP…

Porque agora, ninguém da rede pública consegue, de forma natural, estabelecer conexão com um IP privado.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

NAT / RFC 1918

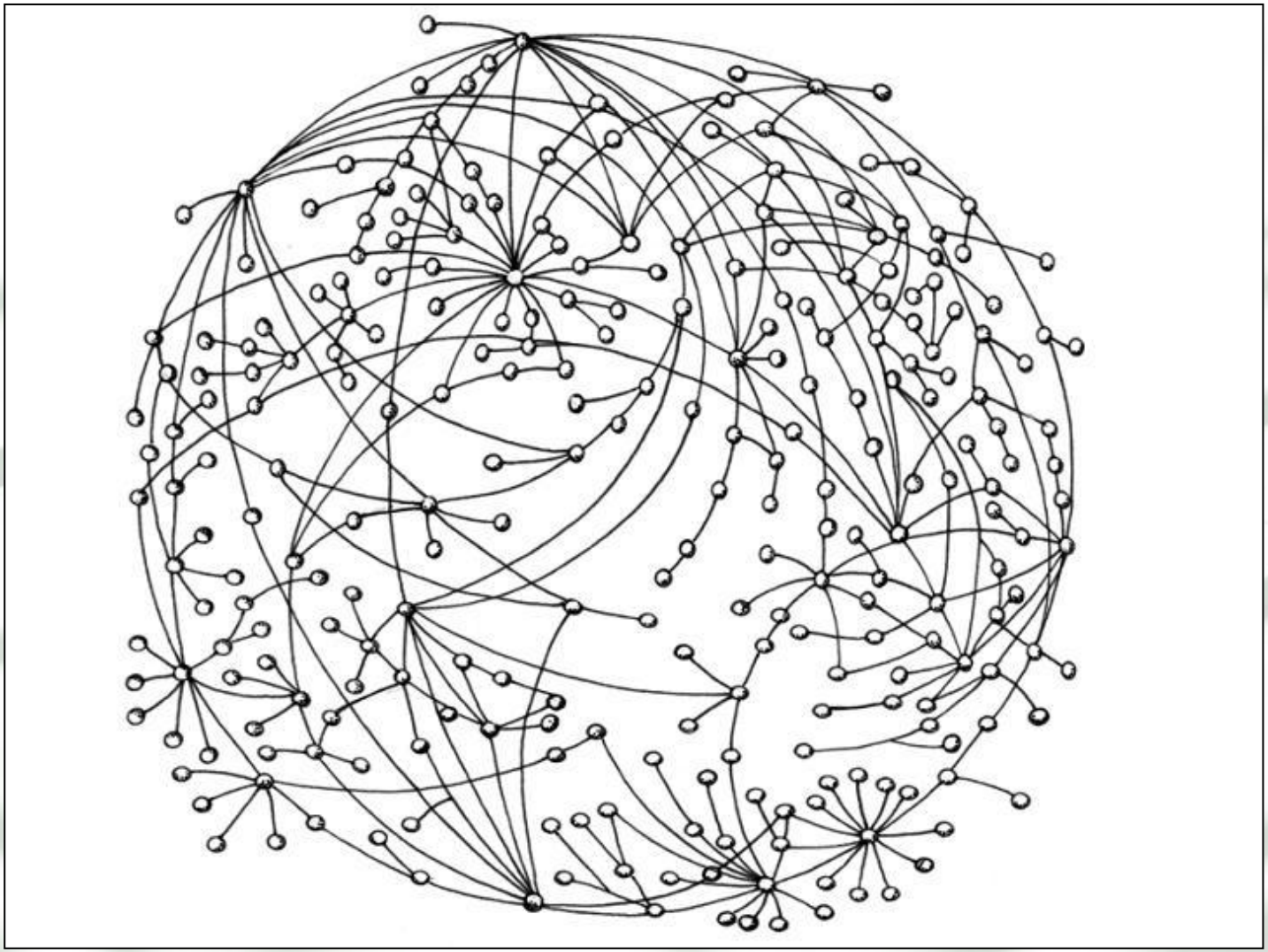


Seria tudo OK, porém o NAT quebra a premissa original da arquitetura TCP/IP…

Mas sempre há espaços para novas gambiarras…

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Mas não há nada ruim que...



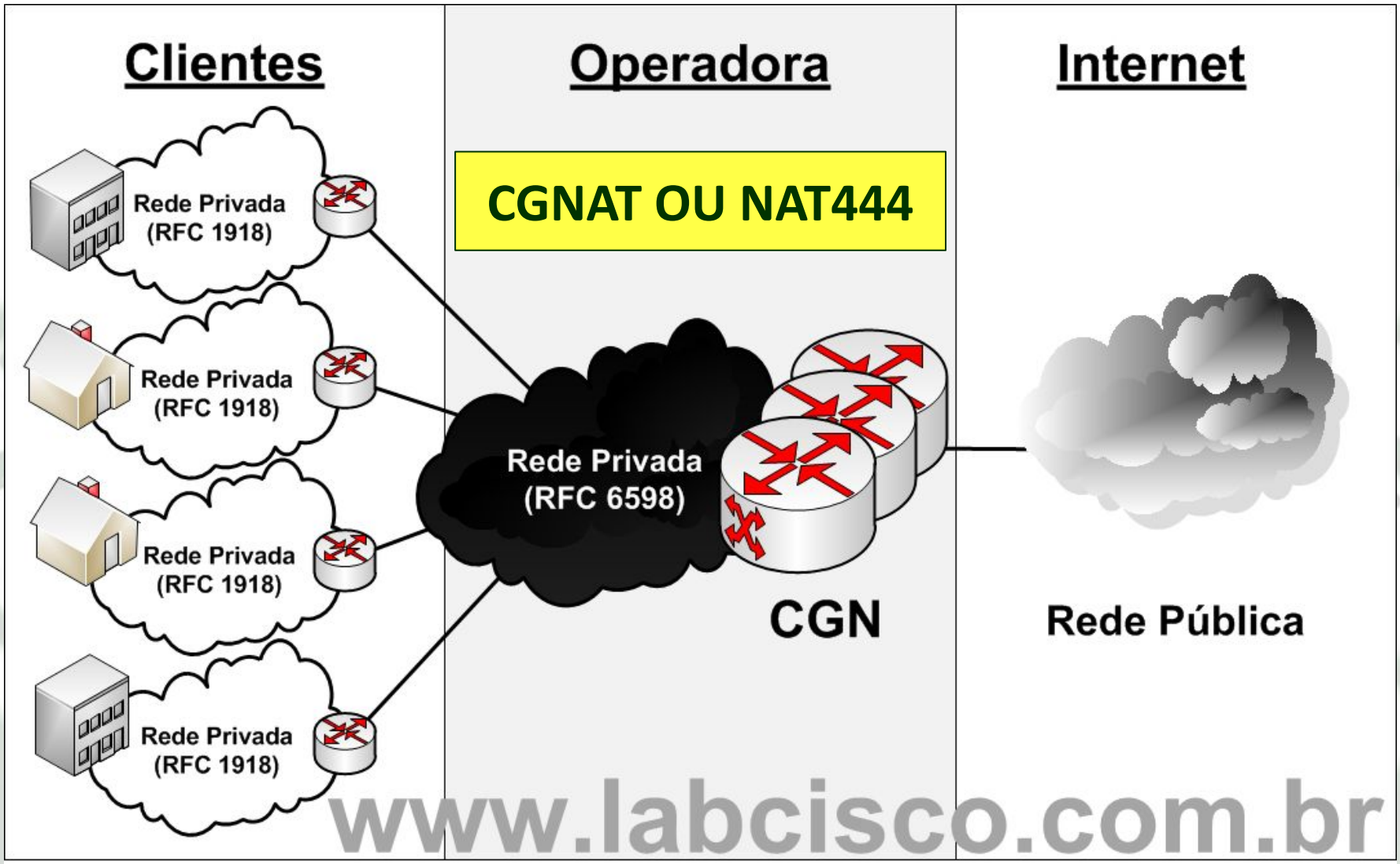
CGNAT / RFC 6598

- Com o número crescente de assinantes de planos de Internet, além do sucesso do 3G/4G, cada vez era maior **a escassez de endereços IP públicos para que os provedores conseguissem atender seus clientes**.
- Em 2012 a IANA estabeleceu uma **nova faixa de endereços privados**, para serem utilizados **exclusivamente por provedores (RFC 6598)**.
- **Essa nova faixa é a 100.64.0.0/10.**

AGORA É NECESSÁRIO FAZER NAT DO NAT... TAMBÉM CHAMADO CGNAT

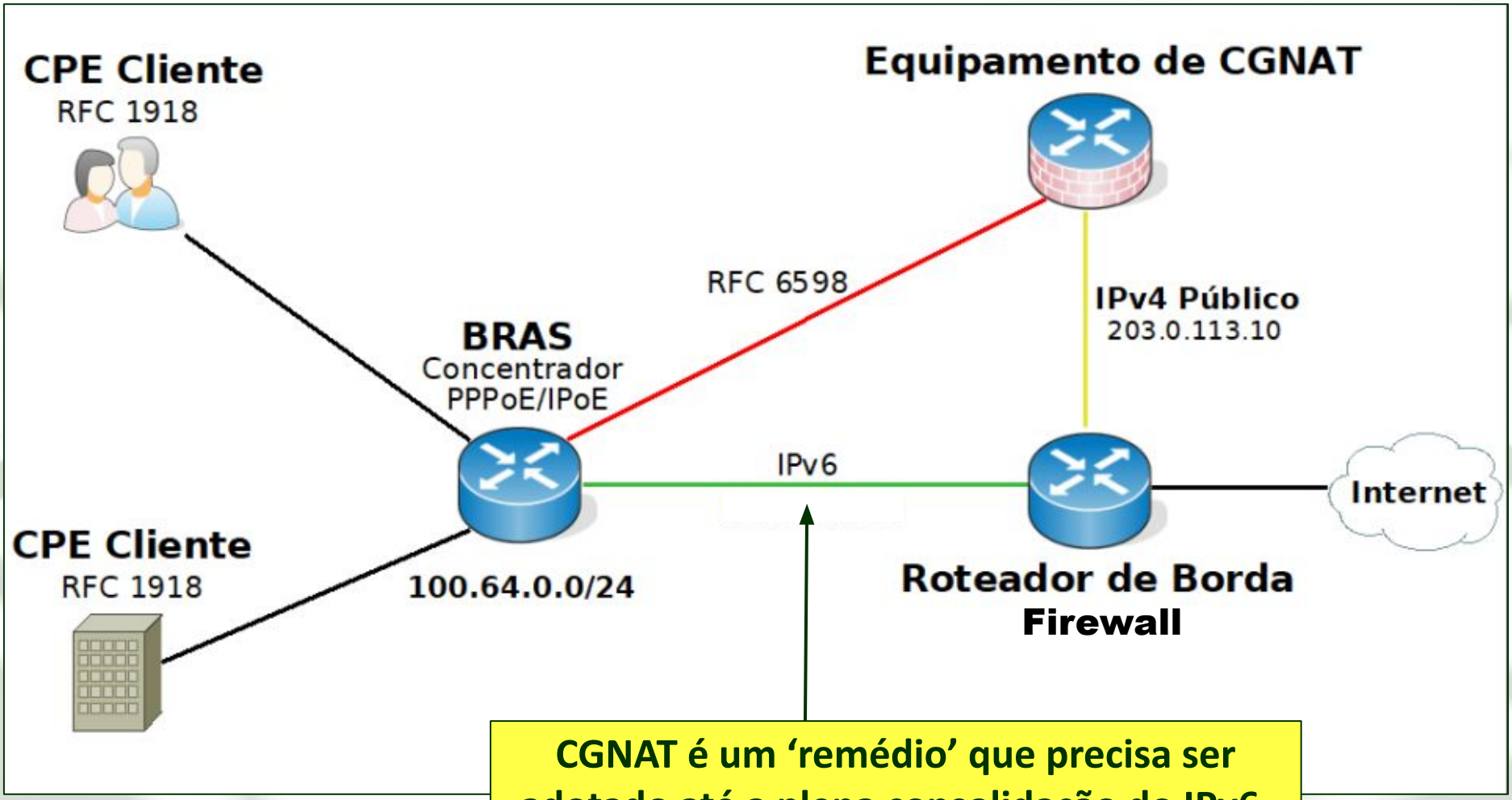
INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

CGNAT / RFC 6598



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

CGNAT / RFC 6598



CGNAT é um 'remédio' que precisa ser adotado até a plena consolidação do IPv6.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

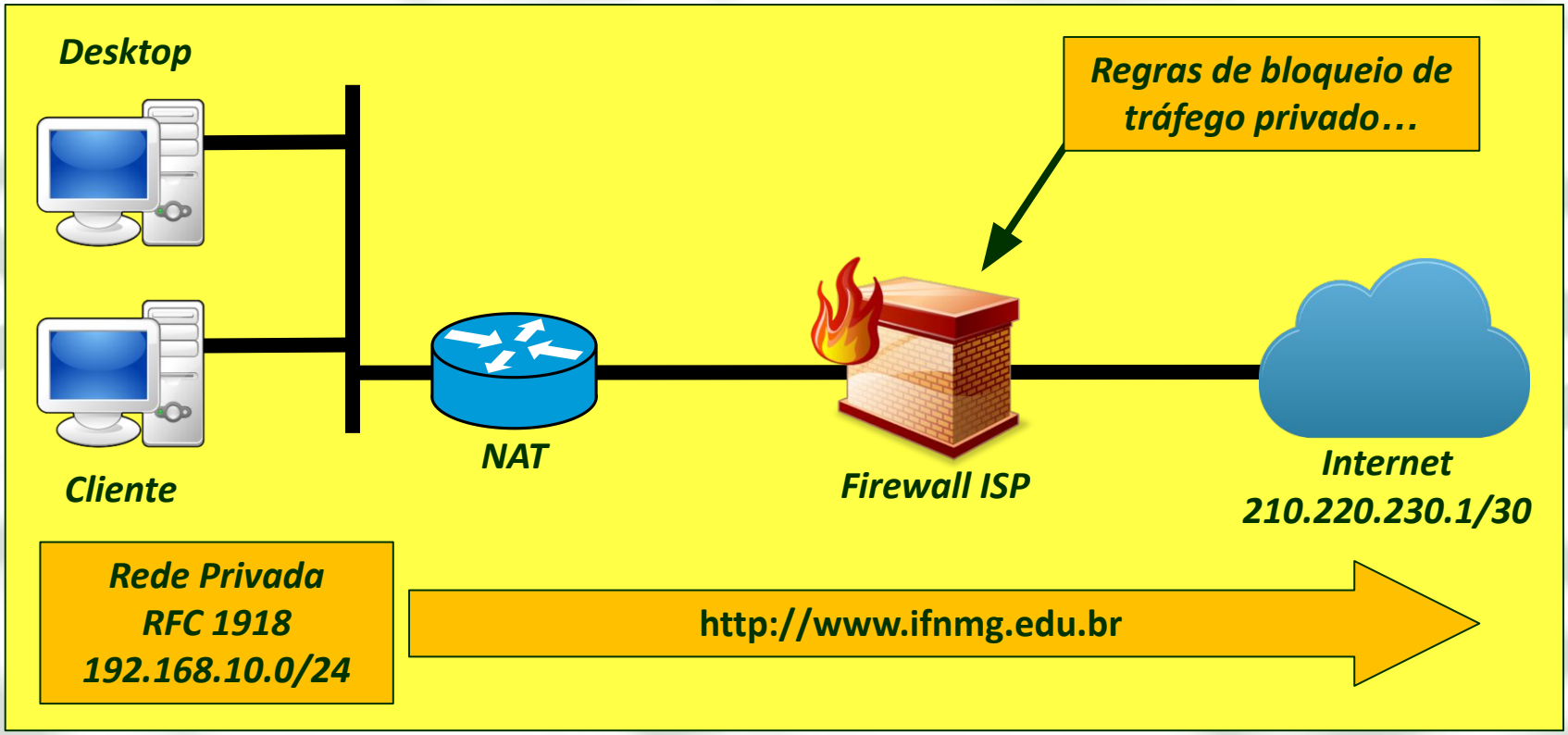
Atividade

- Assista a esse vídeo...
- Leia essa matéria...
- Estude esse conteúdo...

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Mãos na Massa...

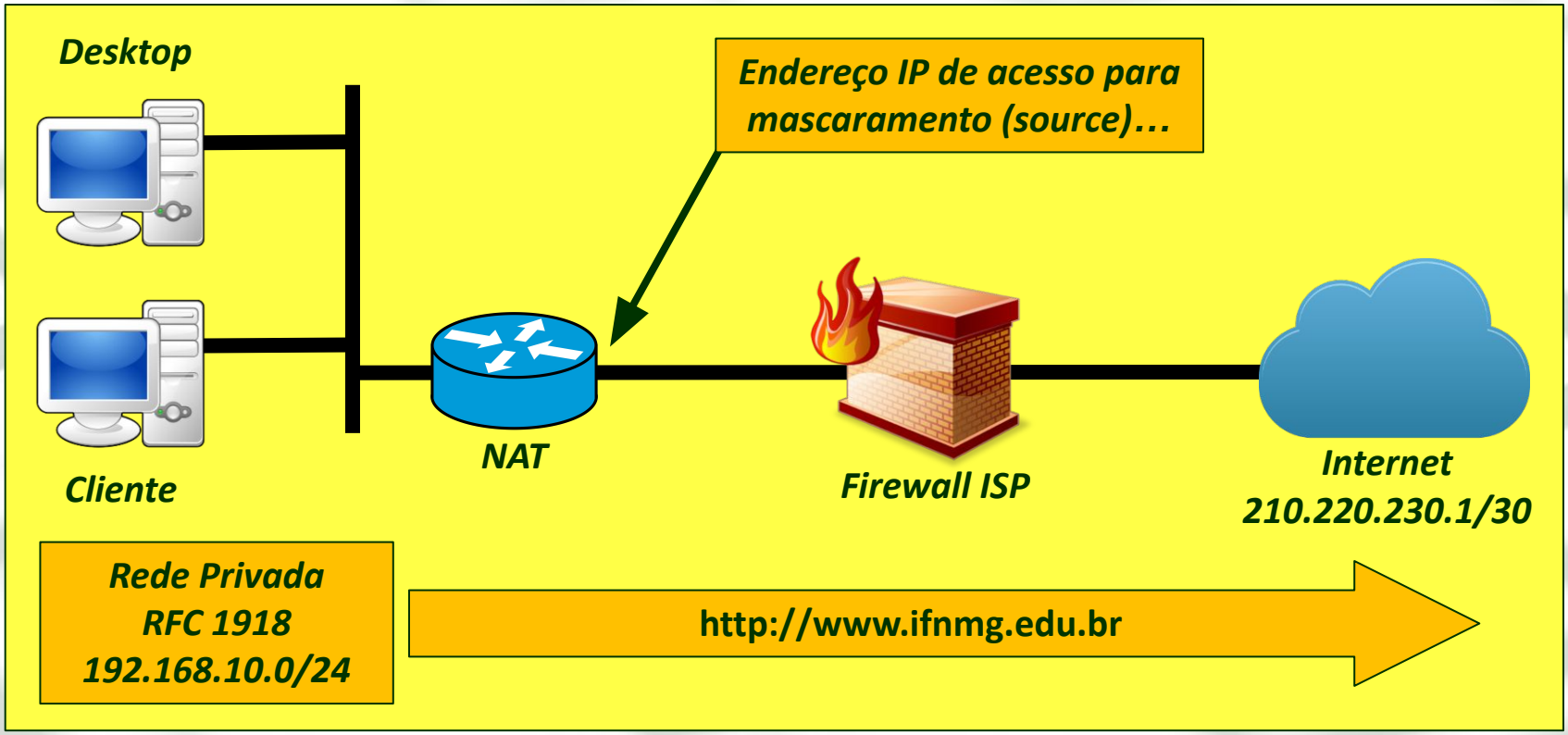
- No mundo real, o cenário abaixo só é possível por meio de NAT



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Mãos na Massa...

- No mundo real, o cenário abaixo só é possível por meio de NAT



SNAT

- **SNAT (*Source NAT*) com IPTables:**
- **Método 1**
  - *Endereço IP de acesso é **Estático**...*

```
# iptables –t nat -A POSTROUTING –o eth1 –j SNAT --to 1.2.3.4
```

Interface de acesso à Internet

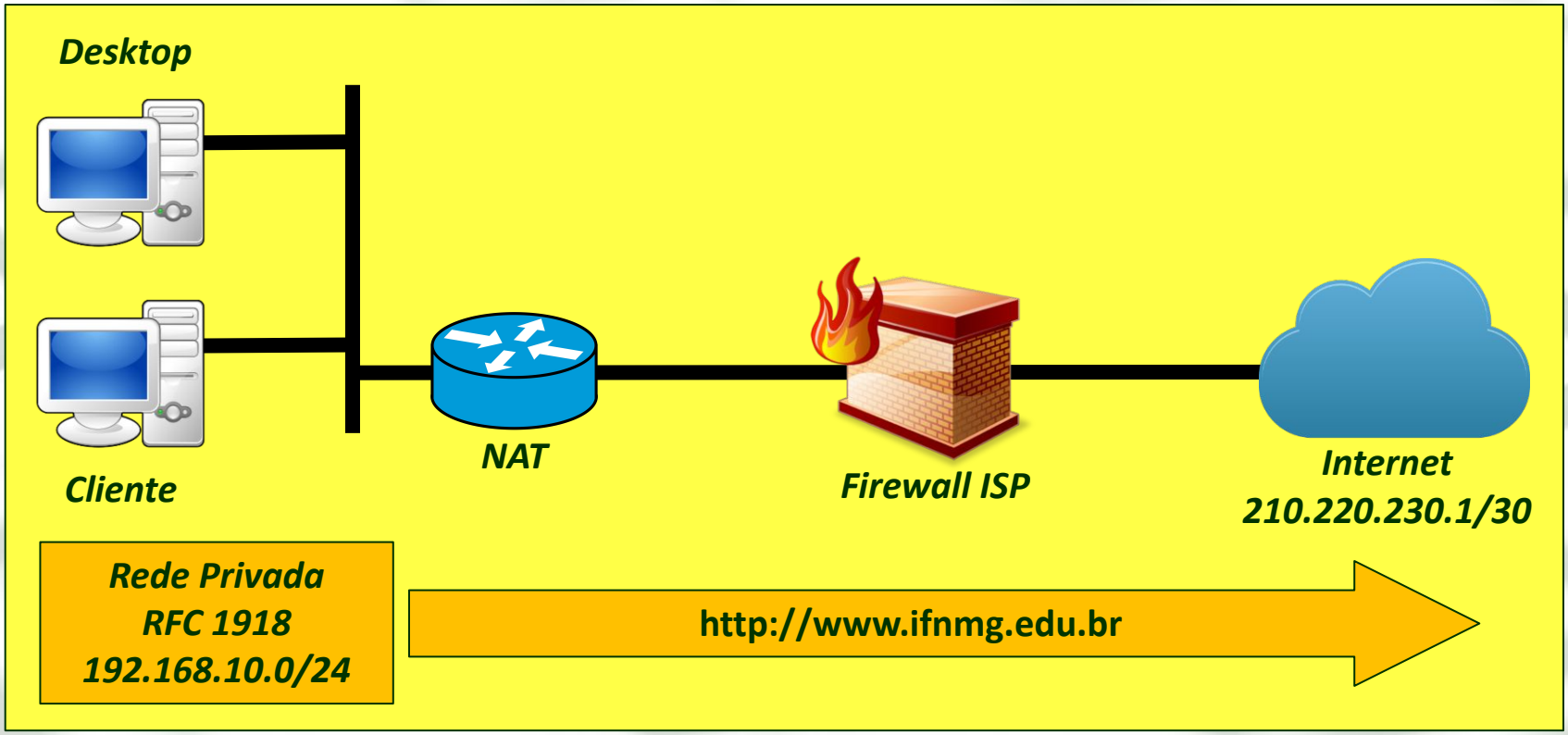
- **Método 2**
  - *Endereço IP de acesso é **Dinâmico**...*
  - *Técnica de Mascaramento (Masquerading)*

```
# iptables –t nat -A POSTROUTING –o eth1 –j MASQUERADE
```

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Laboratório

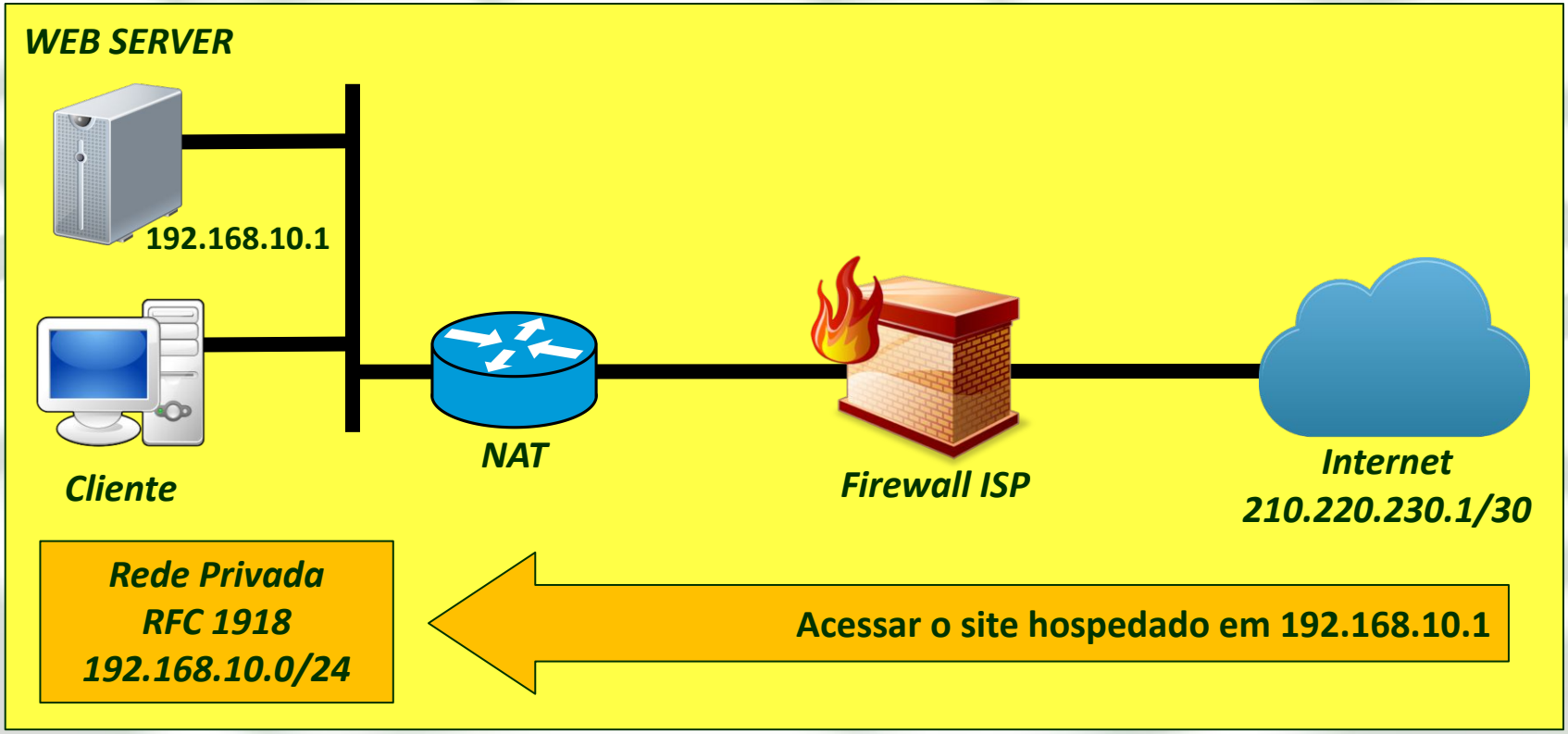
- Implemente o cenário e faça as análises com o **TCPDUMP**



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

DNAT

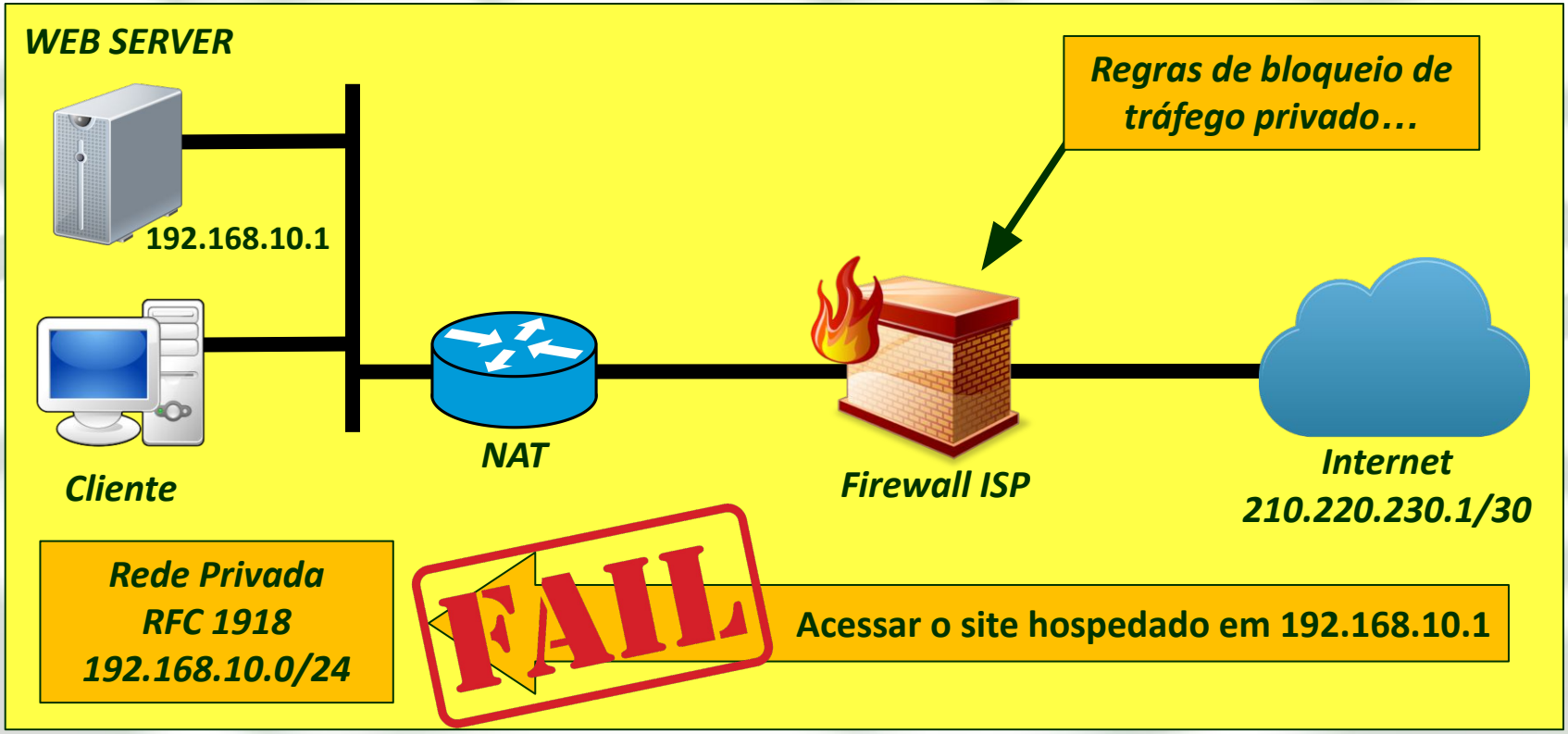
- **Perceba**: O mesmo problema de se tentar acessar a rede pública a partir de uma rede privada, acontece quando **se tenta acessar a rede privada a partir da rede pública**...



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

DNAT

- **Perceba**: O mesmo problema de se tentar acessar a rede pública a partir de uma rede privada, acontece quando **se tenta acessar a rede privada a partir da rede pública**...

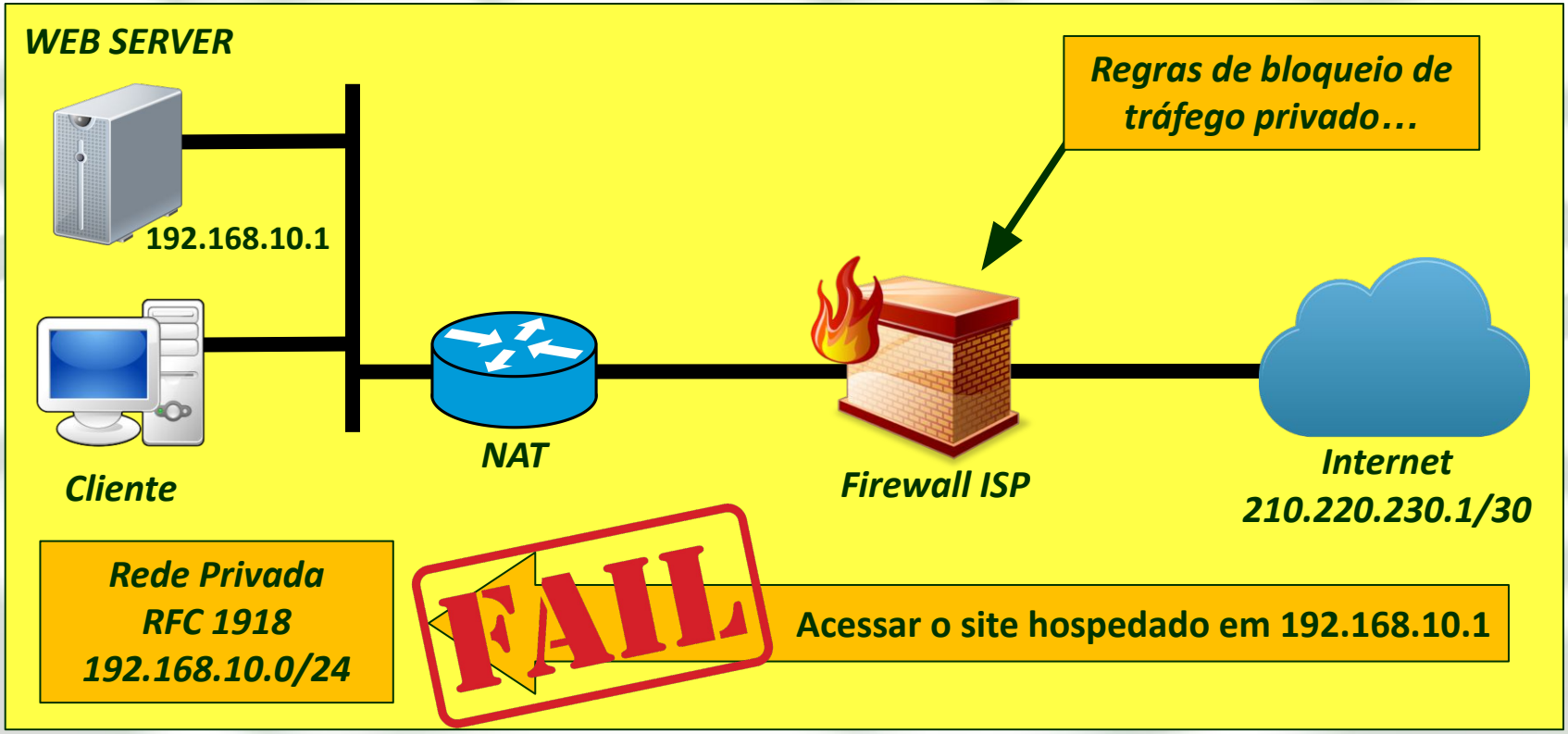


INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

DNAT

- **Perceba**: O m… …ssar a rede pública a par… … quando **se tenta acessa**… …**úblic**a…

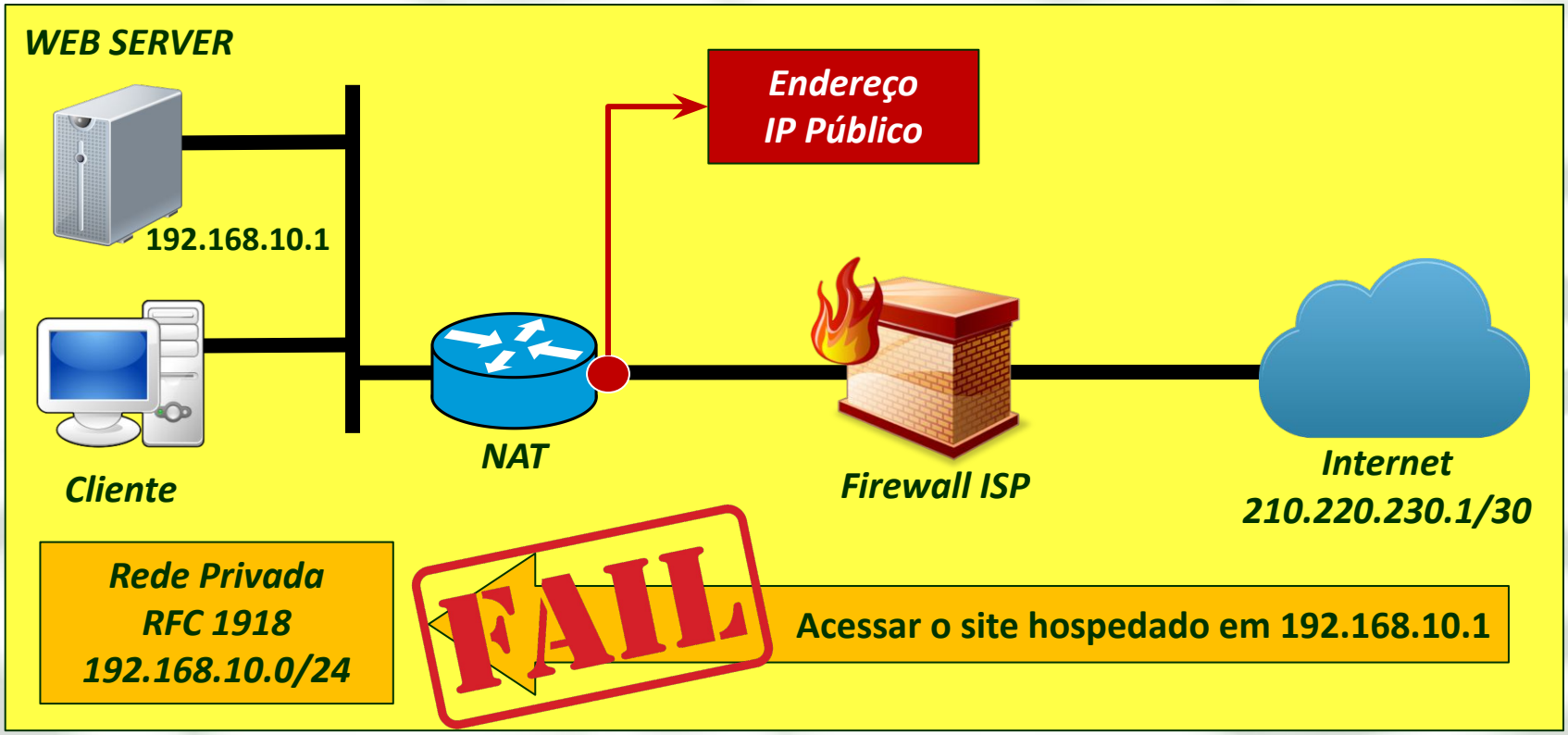
QUAL SOLUÇÃO?



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

DNAT

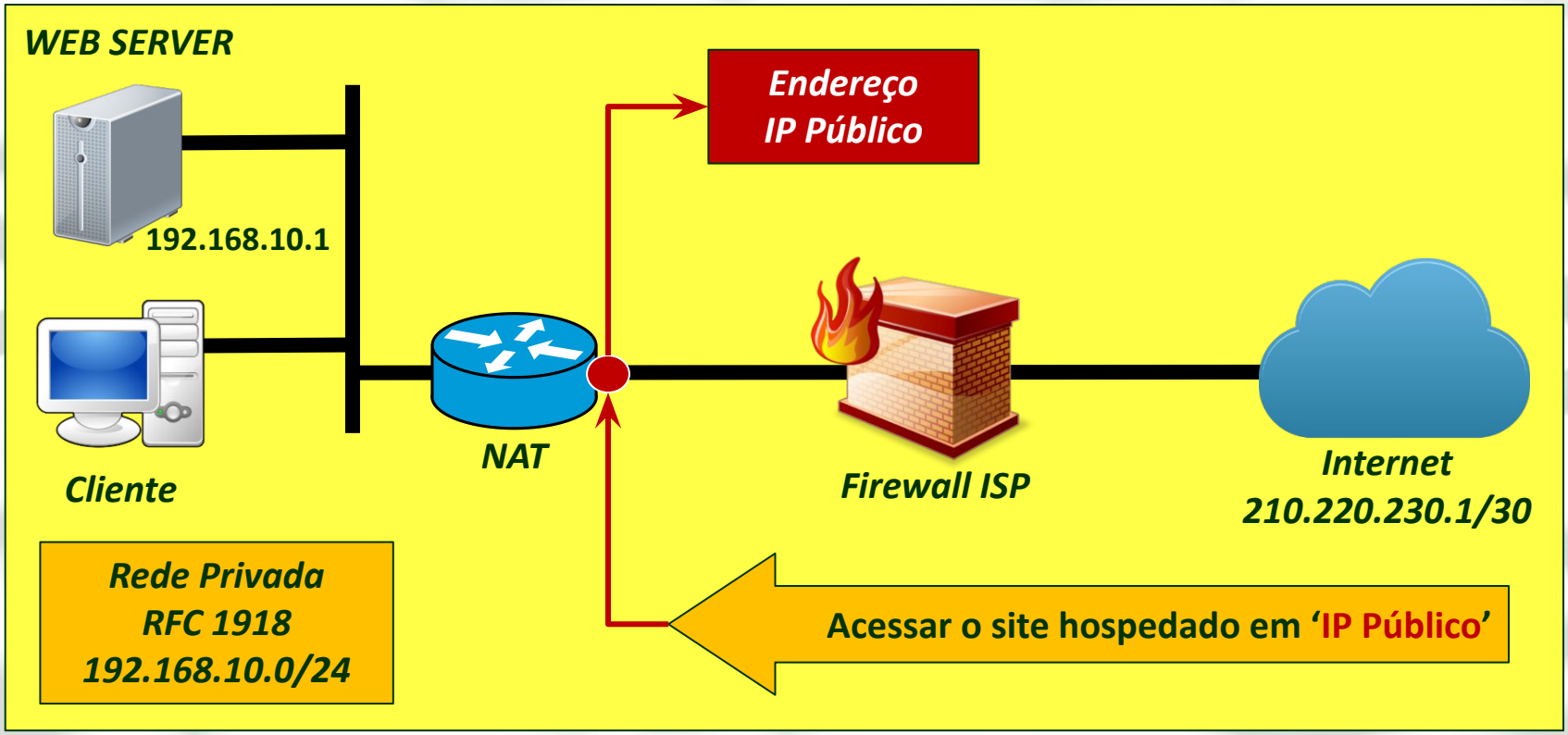
- **DNAT => *Destination NAT***



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

DNAT

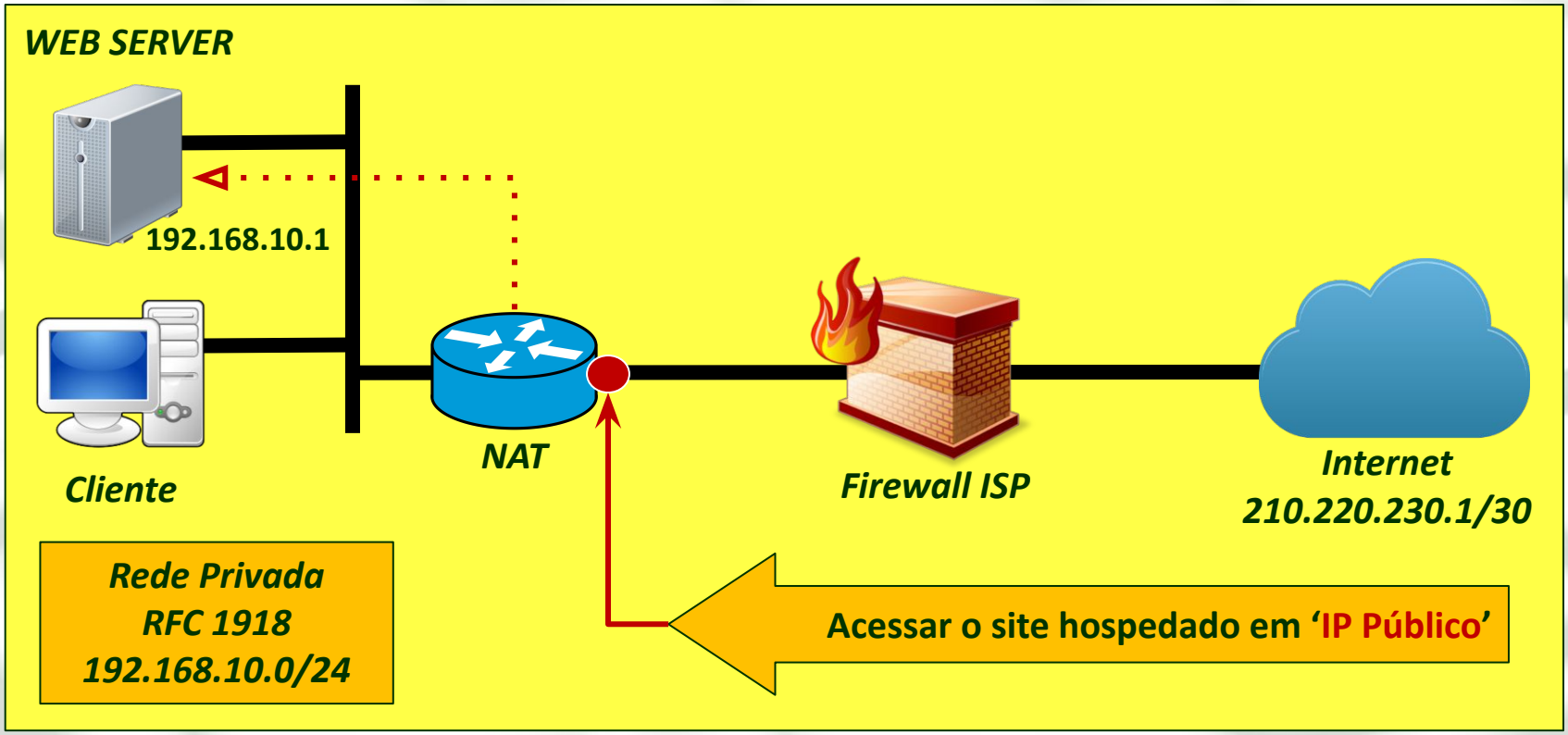
- **DNAT => *Destination NAT***



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

DNAT

- **DNAT => *Destination NAT***



DNAT

- **DNAT** com **IPTables:**
  - A tradução (conversão) do endereço de destino deve acontecer **antes** que o *router* processe o roteamento do pacote.
  - Chain **PREROUTING**.

```
# iptables –t nat -A PREROUTING –i eth1 –j DNAT --to 192.168.10.1
```

Interface com Endereço Público

Todo pacote recebido pela interface eth1 será encaminhado para o endereço 192.168.10.1

DNAT

- Encaminhar apenas protocolos e aplicações específicas:

```
# iptables –t nat -A PREROUTING –i eth1 –p tcp --dport 80 –j DNAT --to 192.168.10.1
```

Redirecionar apenas tráfego WEB.

- Redirecionamento de portas:

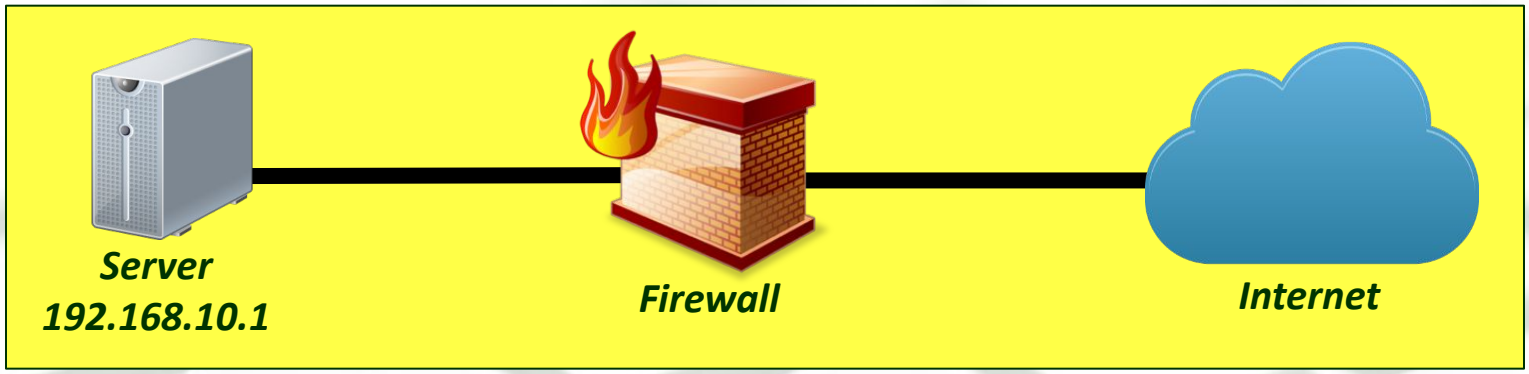
```
# iptables –t nat -A PREROUTING –i eth1 –p tcp –j DNAT --to 192.168.10.1:3128
```

*Todo tráfego com destino para porta 80 é redirecionado para a porta 3128 do IP 192.168.10.1. Útil para implementar um **proxy transparente**.*

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Laboratório

- Crie o ambiente abaixo utilizando o **Kathará**…



- Configure DNAT no Firewall de forma que:
  - De qualquer lugar da Internet seja possível acessar remotamente, via SSH, a VM Server dentro da rede privada.

***REQUISITO A**: A Internet deve acessar o serviço SSH da **VM Server**.*
REQUISITO B**: O SSH do Firewall deve estar disponível para acessos **apenas de dentro da rede privada.

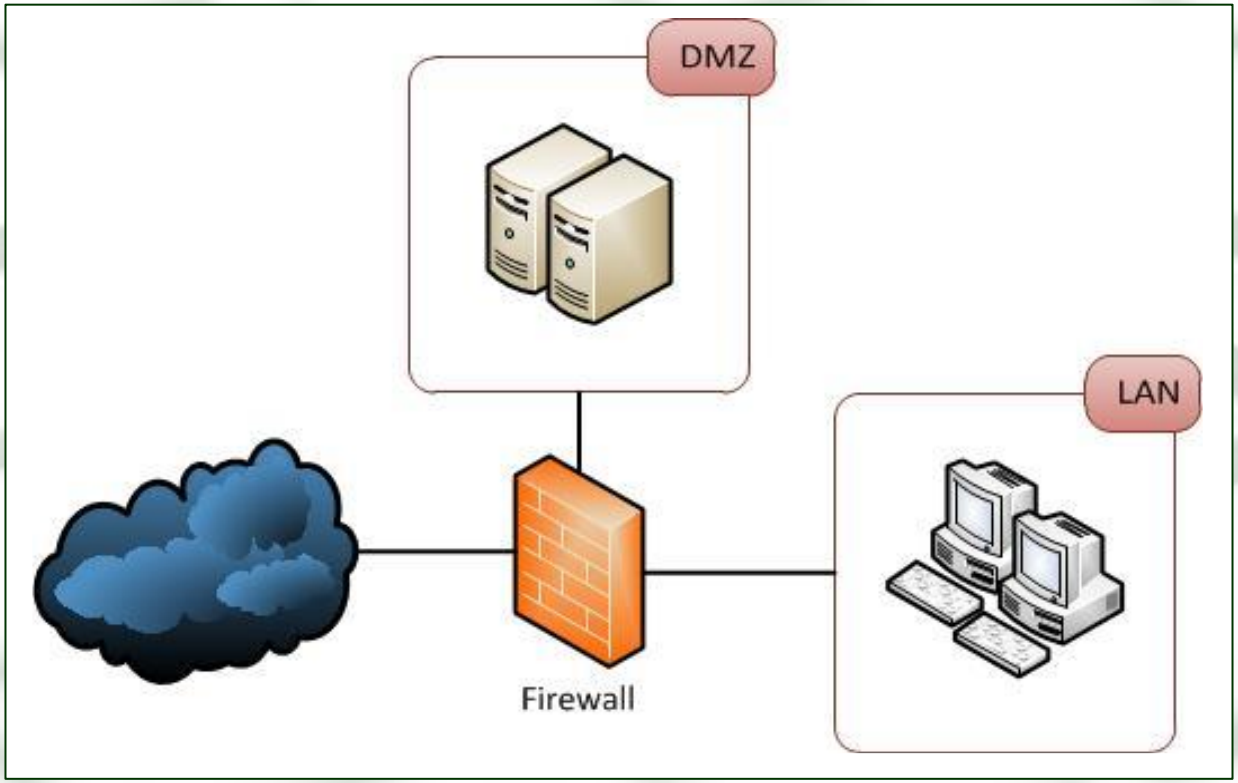
Zonas Desmilitarizadas

- Uma **Zona Desmilitarizada** (**DMZ**) também conhecida por **Rede de Perímetro** é uma Sub-Rede organizacional que mantém serviços disponíveis para acesso universal.

- A correta configuração dessa **zona intermediária**, entre a rede pública e a rede privada, é fundamental para preservar a política de segurança da informação das organizações.

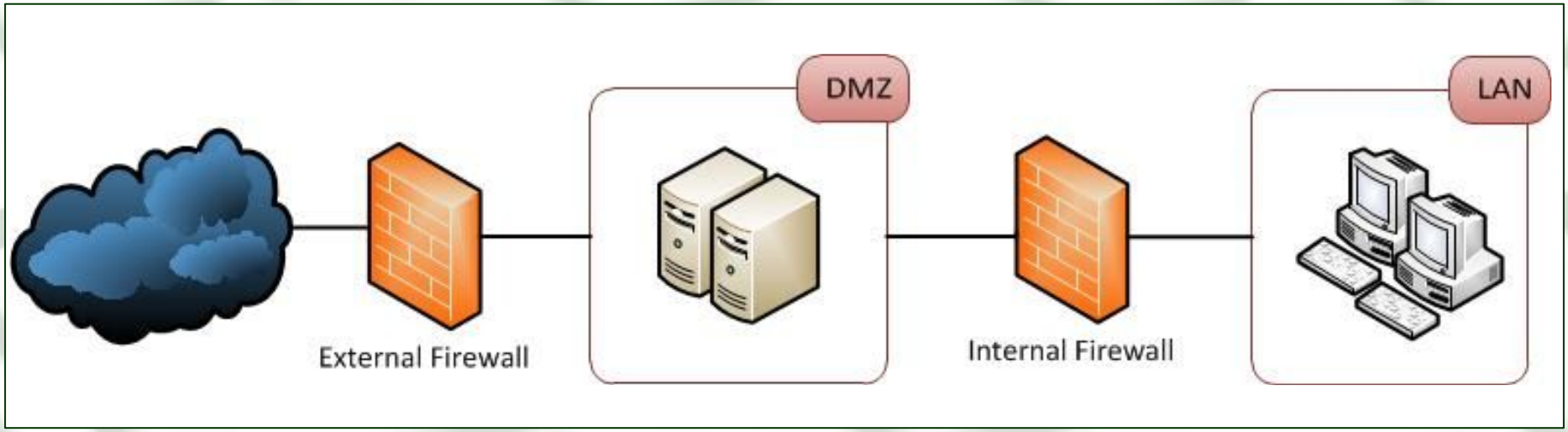
DMZ

- **Arquiteturas de DMZ**
  - *Three-Pronged Firewall* ou *single firewall*



DMZ

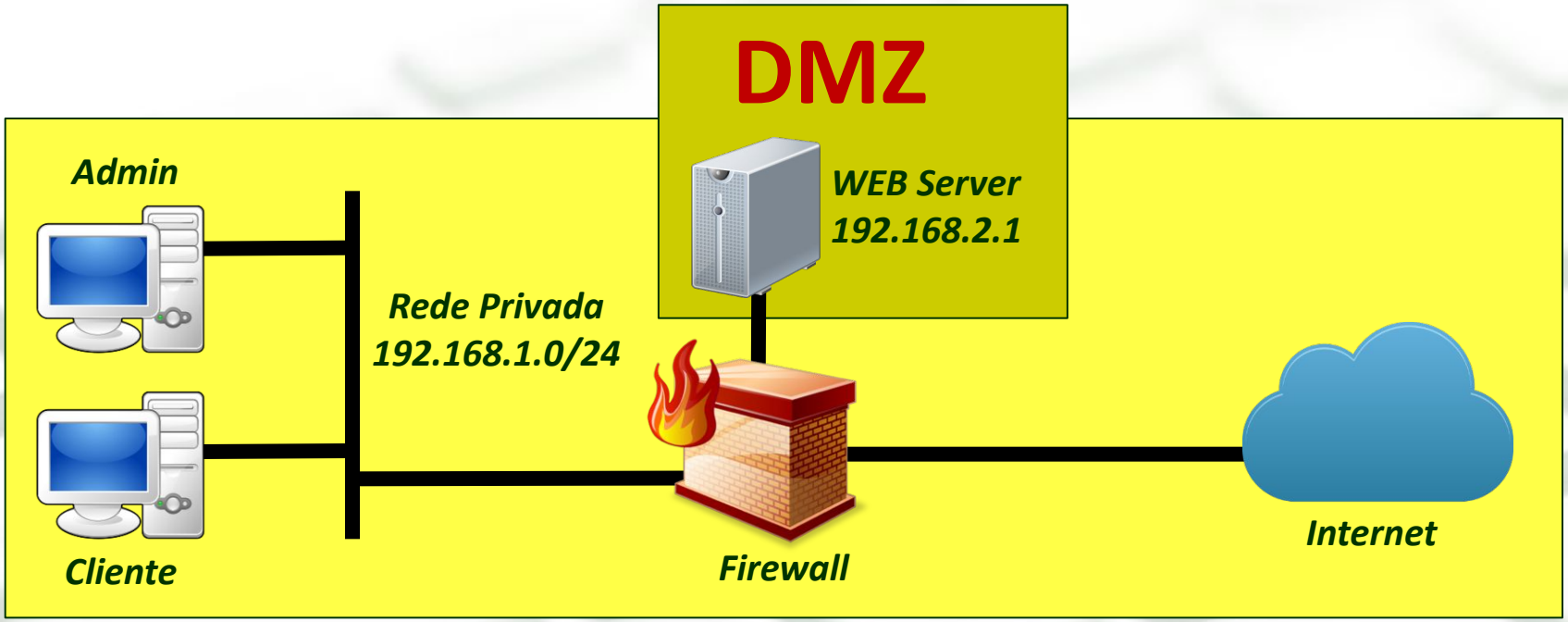
- **Arquiteturas de DMZ**
  - *Multiple Firewall DMZ*



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Laboratório

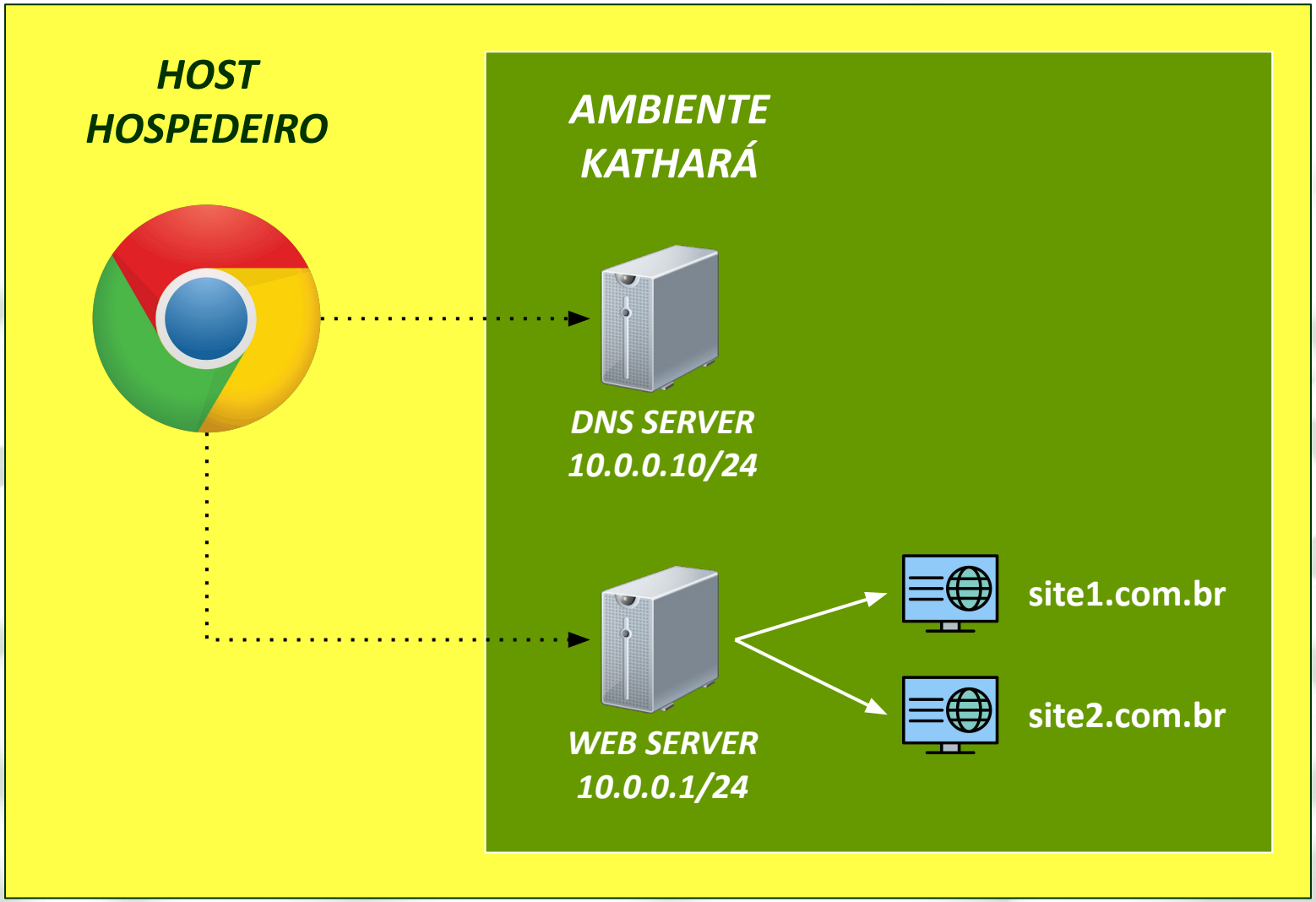
- **Implemente o cenário abaixo no Kathará…**



REQUISITO A: *O Firewall não roteia endereços privados de/para a Internet.*
REQUISITO B*: A DMZ não pode acessar rede interna.*
REQUISITO C*: A rede interna pode acessar tanto DMZ quanto Internet.*

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Laboratório Avaliativo - 10 Pts.



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Referências

- **Guia Foca GNU/Linux**.

Disponível em http://www.guiafoca.org/

- **Documentação NetFilter.**

Disponível em http://www.netfilter.org/documentation/

- **Blog LabCisco**

Disponível em
http://labcisco.blogspot.com/2014/09/cgnat-na-transicao-ipv6-solucao-ou-vilao.html

- **Prof. Ph.D. Edgard Jamhour**

Disponível em https://www.ppgia.pucpr.br/~jamhour/Pessoal/Graduacao/Ciencia/Teoria/

- **Fernando Frediani**

Disponível em https://ftp.registro.br/pub/gter/gter47/03-CGNAT-Bem-feito.pdf

- MORIMOTO, Carlos E; **Servidores Linux – Guia Prático**.