Podemos confiar na Internet?

Hermano Pereira

Professor – Tecnologia em Sistemas para Internet

UTFPR - Câmpus Guarapuava

Fórum Técnico

CELEPAR
Guarapuava

08 de outubro de 2014

Agenda

Introdução

1 – Confiar na Resolução de Domínios?

2 – Confiar no Roteamento de Provedores?

3 – Confiar em Autoridades Certificadoras?

Considerações Finais

aproximadamente 70 minutos

Introdução

Segurança

- Integridade
- Disponibilidade
- Confidencialidade

Introdução

1 – Resolução de Domínios

2 – Roteamento de Provedores

3 – Autoridades Certificadoras

→ *blog Sandro Suffert*

→ *atuação na área*

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

1 -

Podemos confiar na Resolução de Domínios?

1 – Confiar na Resolução de Domínios?

- DNS – Domain Name System

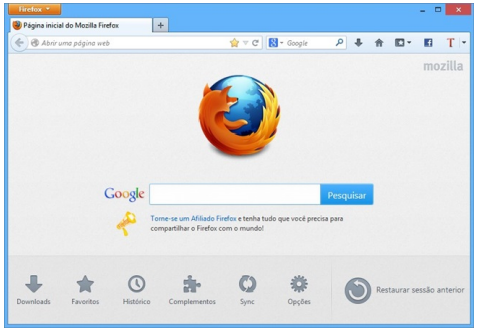
  Documento RFC 1034 (1987)

1 – Confiar na Resolução de Domínios?

Internauta

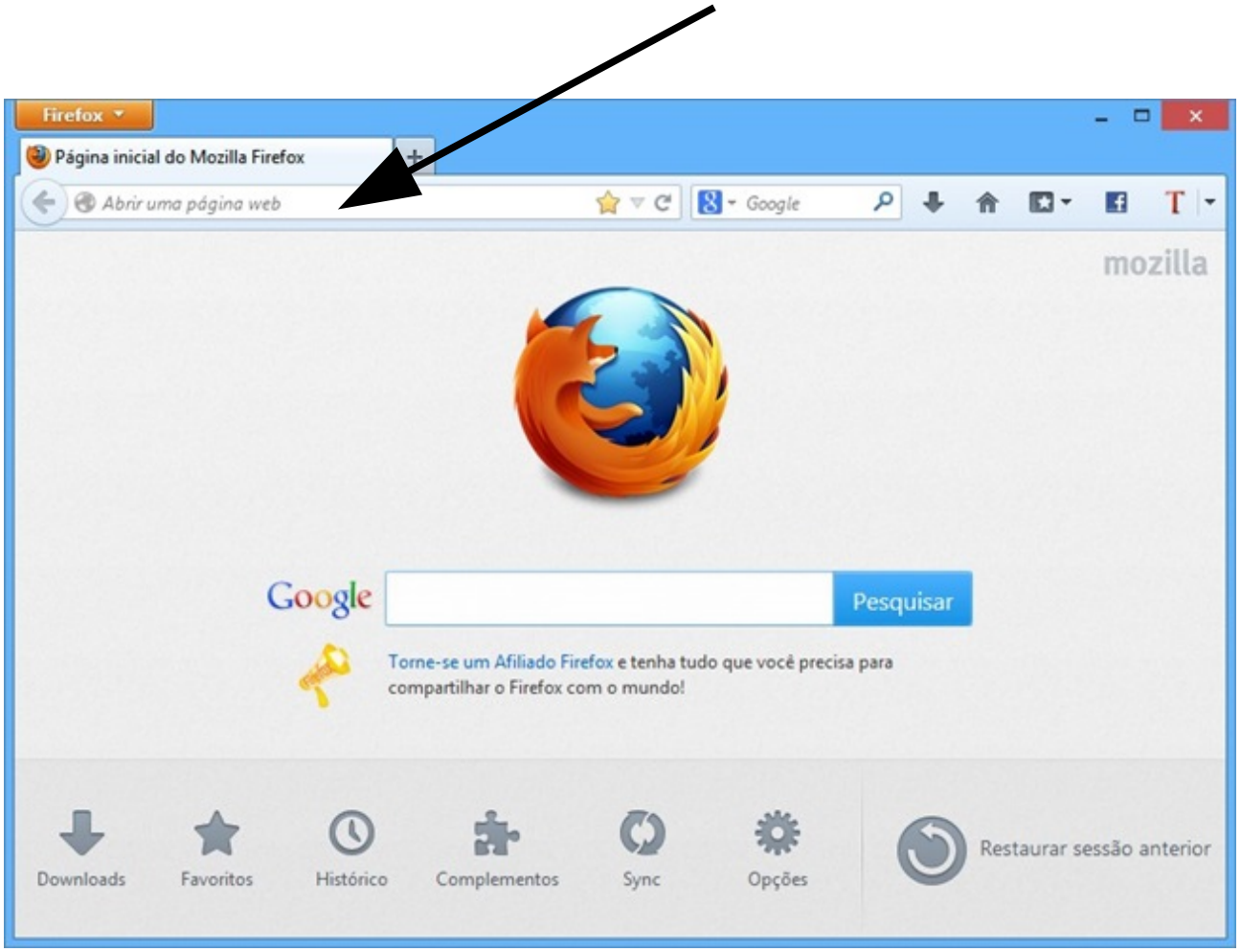
1 – Confiar na Resolução de Domínios?

1 – Confiar na Resolução de Domínios?



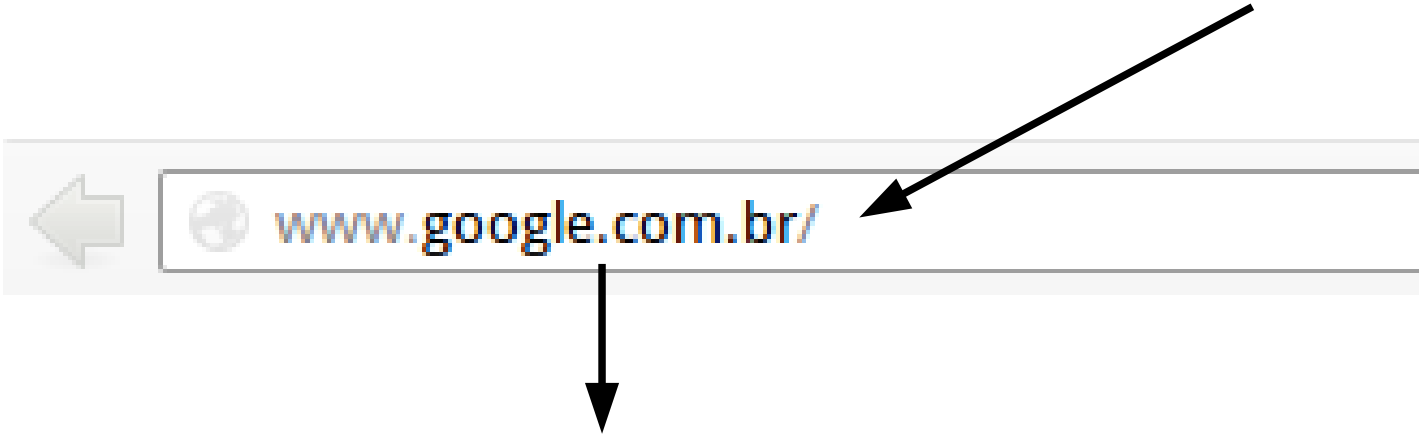
1 – Confiar na Resolução de Domínios?

1 – Confiar na Resolução de Domínios?



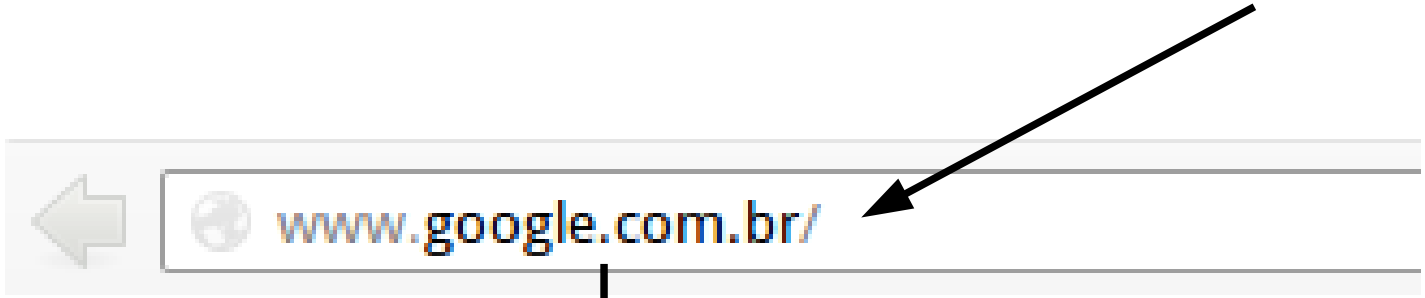
1 – Confiar na Resolução de Domínios?

1 – Confiar na Resolução de Domínios?



Domínio

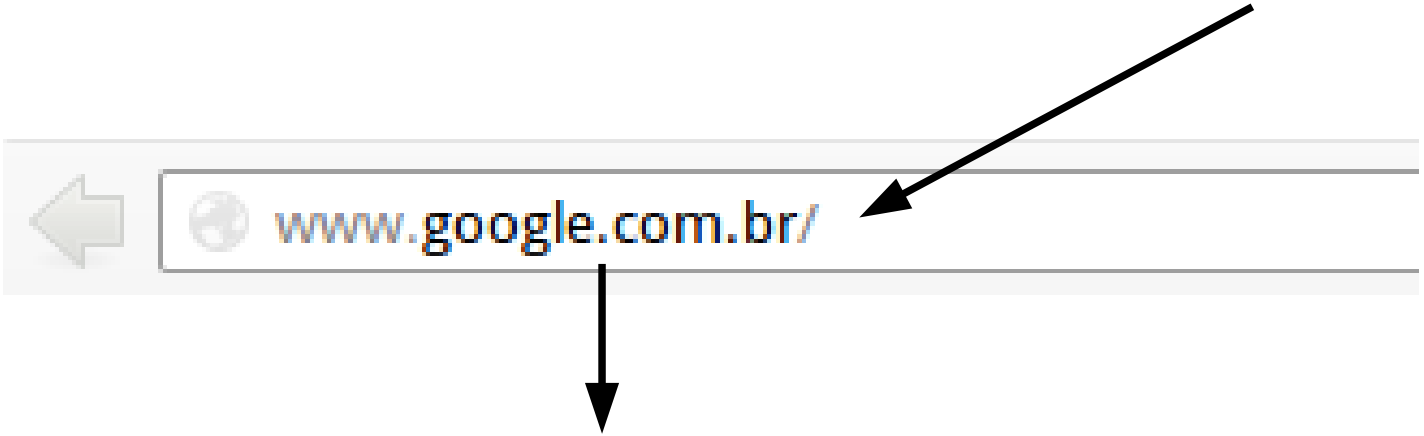
1 – Confiar na Resolução de Domínios?



Domínio

Endereço IP

1 – Confiar na Resolução de Domínios?



Domínio

Endereço IP

74.125.234.23

1 – Confiar na Resolução de Domínios?

Resolver o domínio

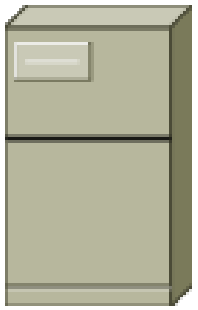
www.google.com.br

Para o endereço IP

74.125.234.23

1 – Confiar na Resolução de Domínios?

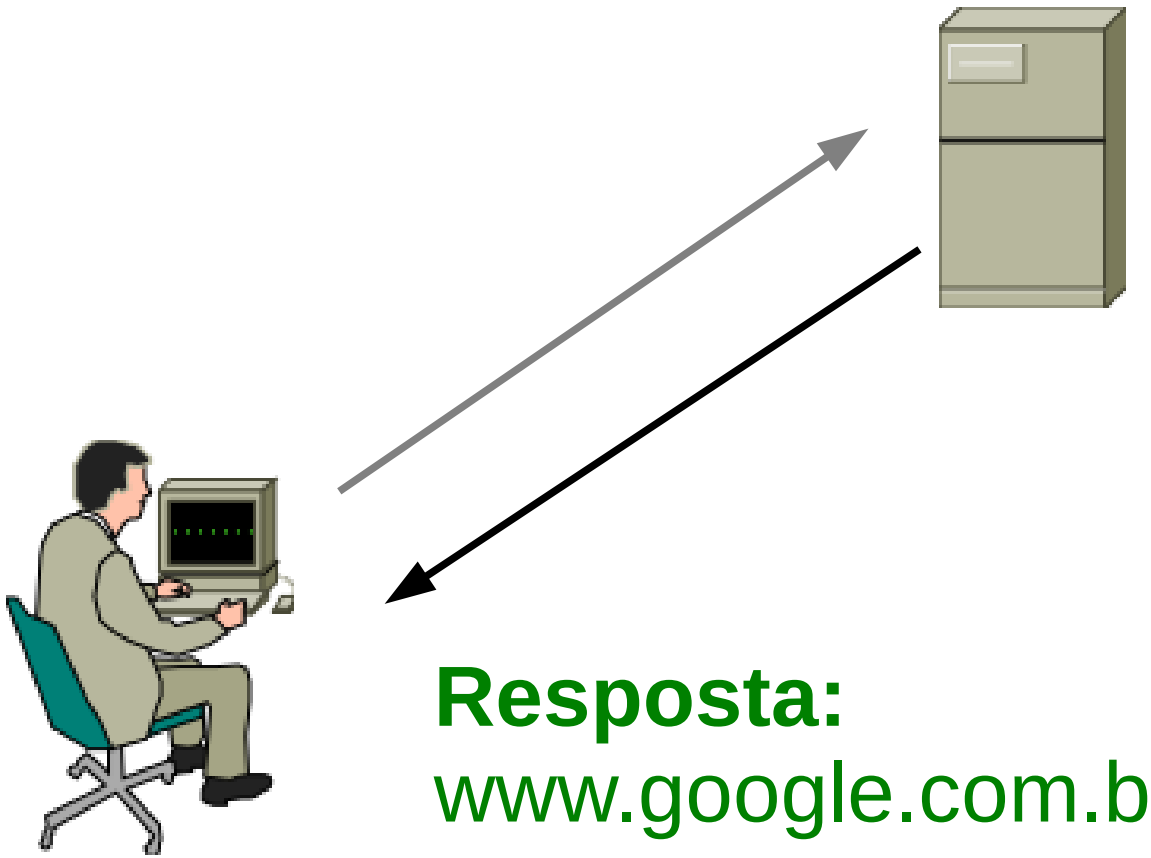
Servidor DNS



Pergunta:
Endereço IP de www.google.com.br?

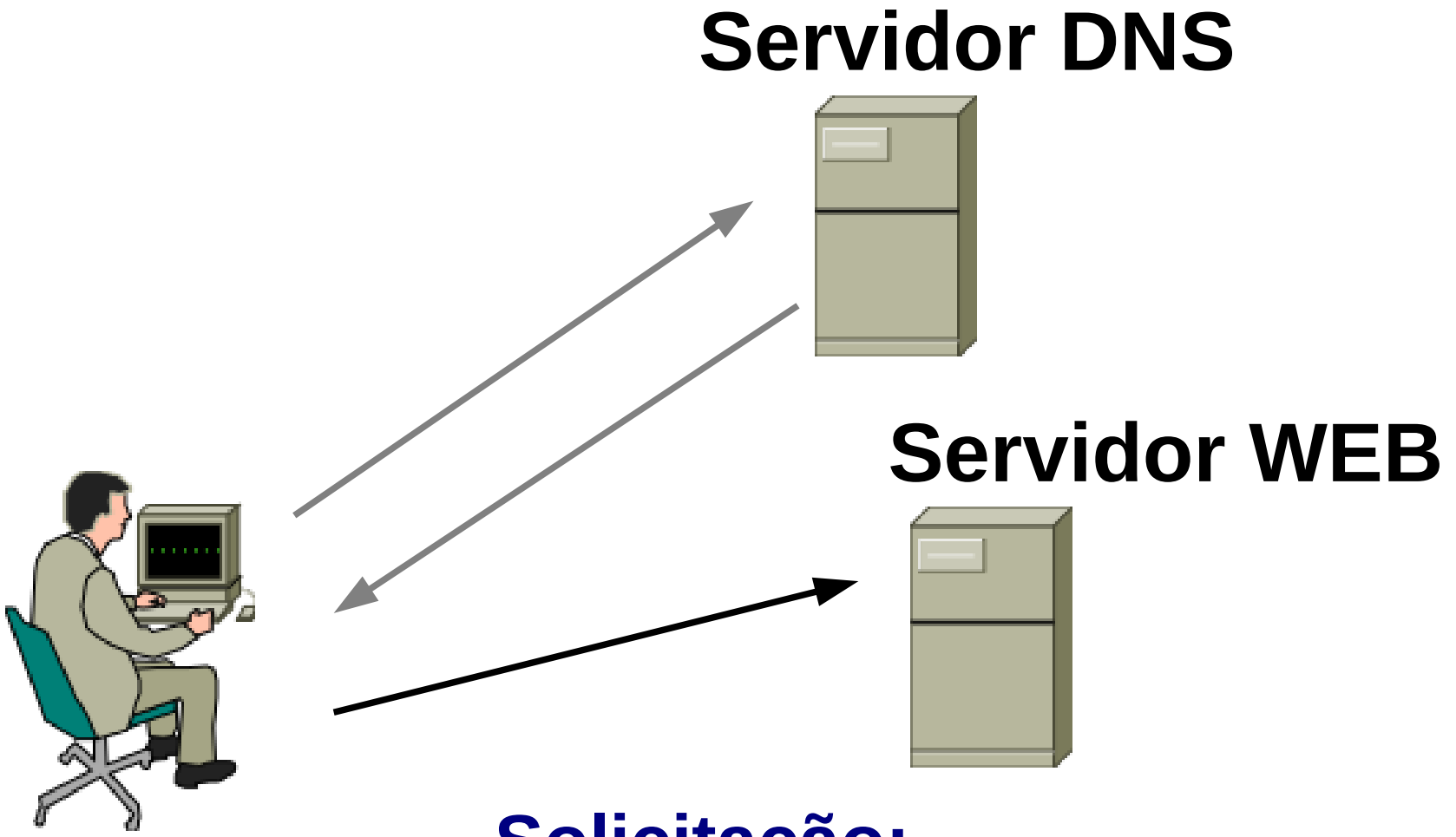
1 – Confiar na Resolução de Domínios?

Servidor DNS



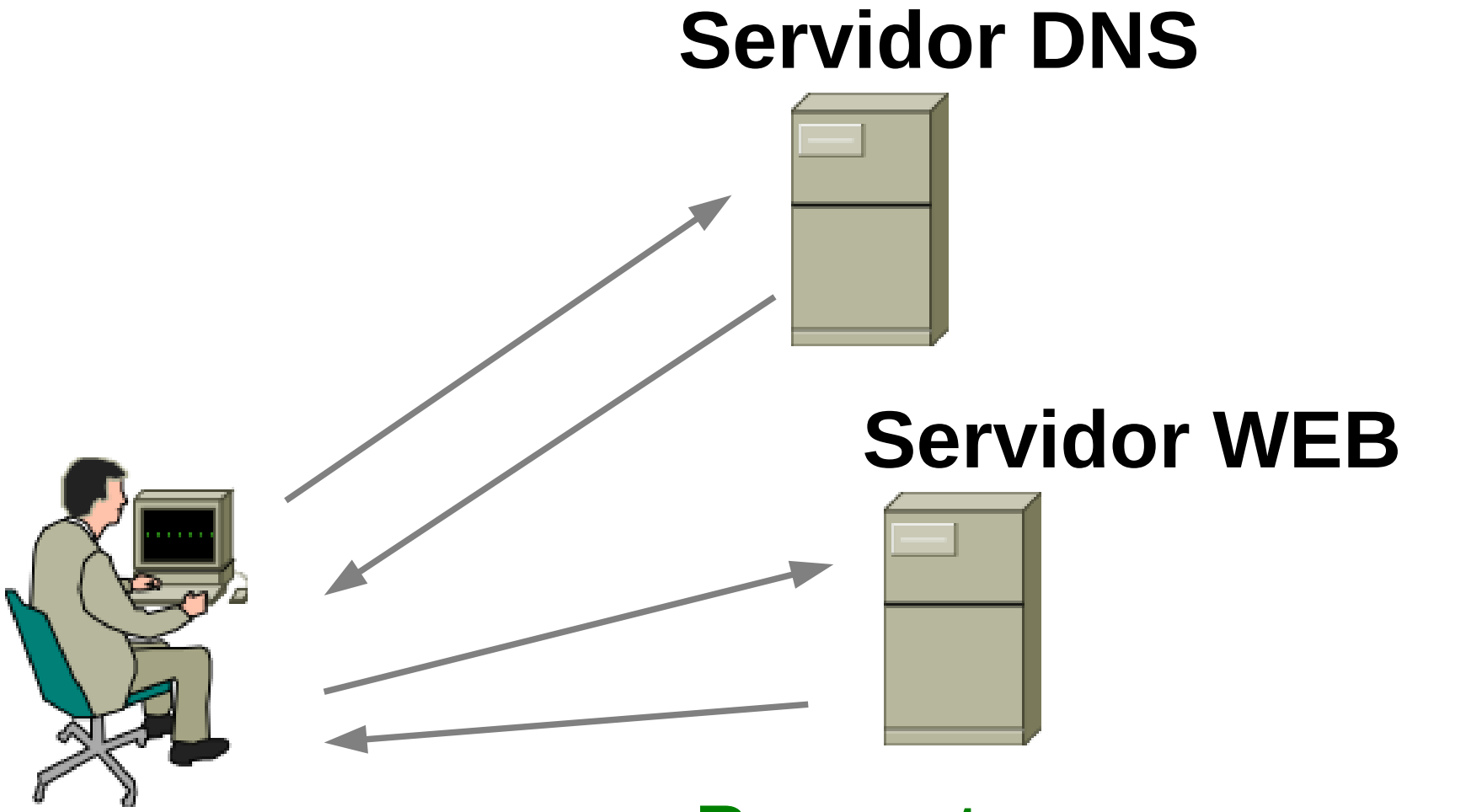
Resposta:
www.google.com.br = 74.125.234.23

1 – Confiar na Resolução de Domínios?



Solicitação:
Página web em 74.125.234.23!

1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?

Google Brasil

Pesquisa Google Estou com sorte

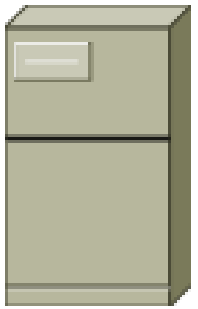
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS

PERGUNTA

RESPOSTA



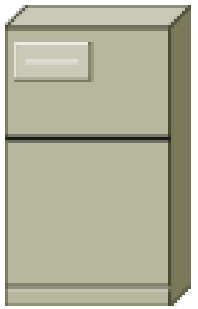
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS

PERGUNTA

RESPOSTA



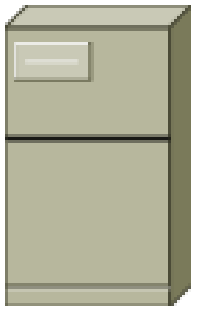
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS

PERGUNTA

RESPOSTA

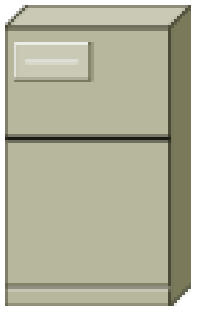


1 – Confiar na Resolução de Domínios?

Internauta

PERGUNTA

Servidor DNS



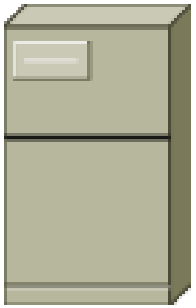
?

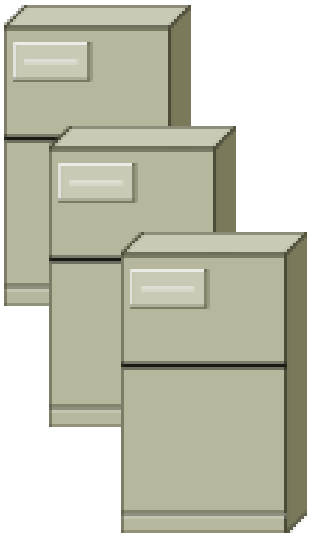
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS

PERGUNTA





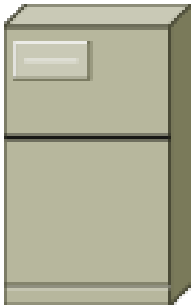
Servidores DNS

1 – Confiar na Resolução de Domínios?

Internauta

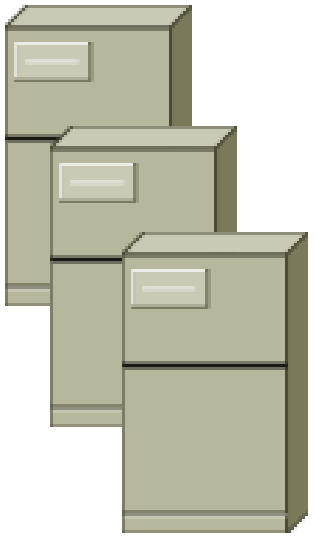
Servidor DNS

PERGUNTA



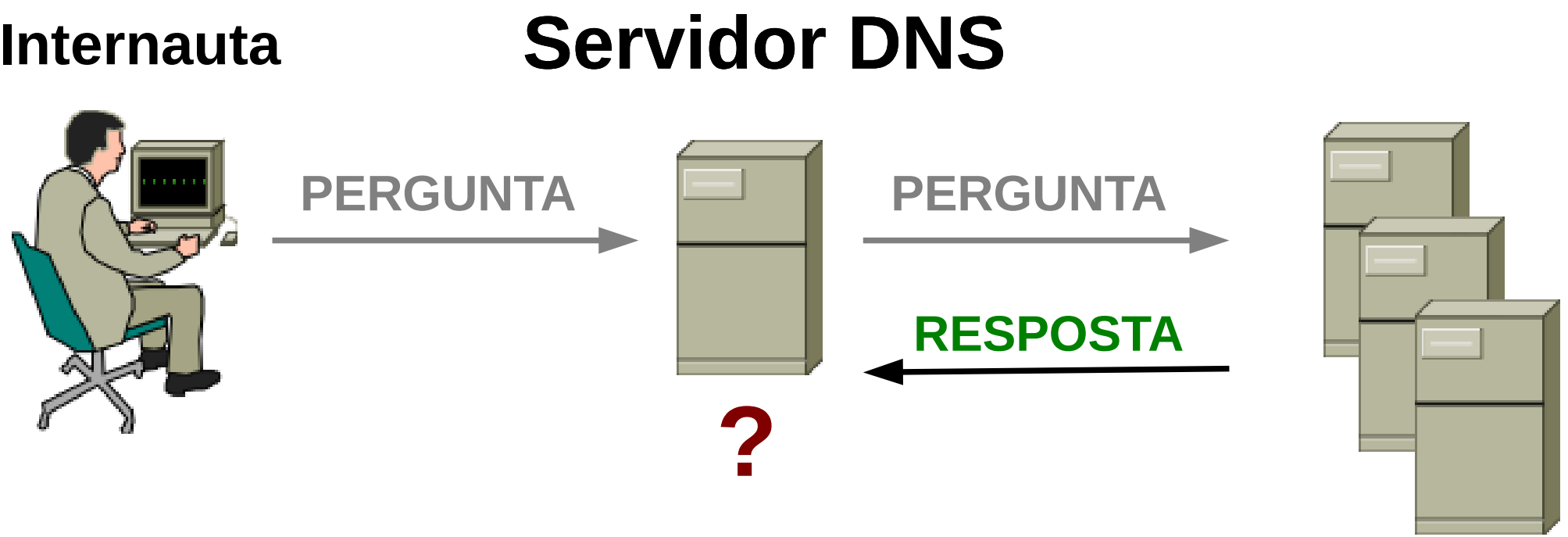
?

PERGUNTA



Servidores DNS

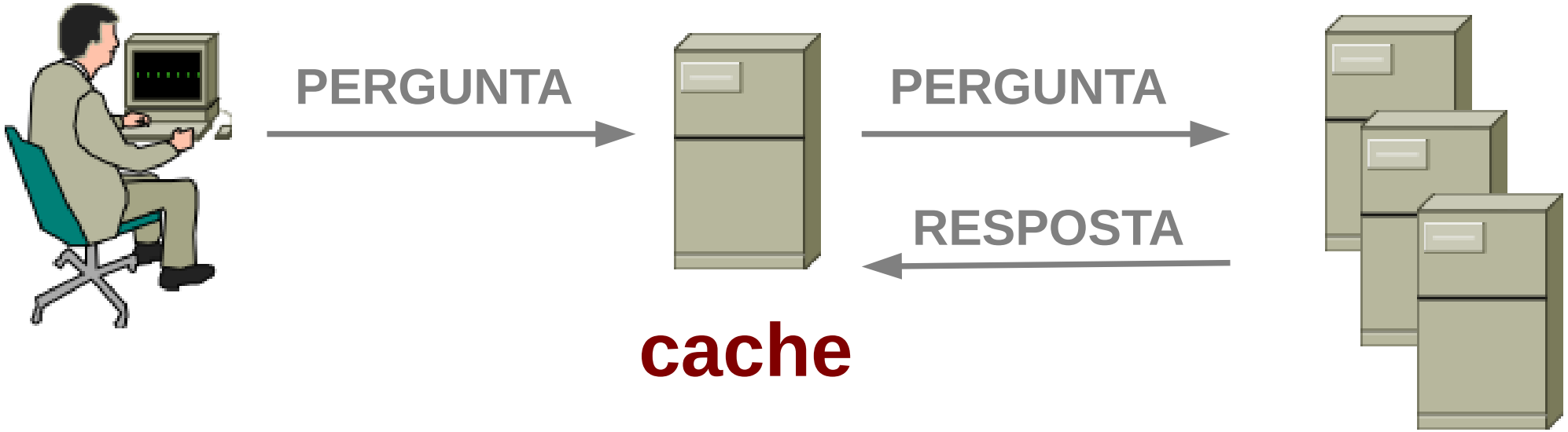
1 – Confiar na Resolução de Domínios?



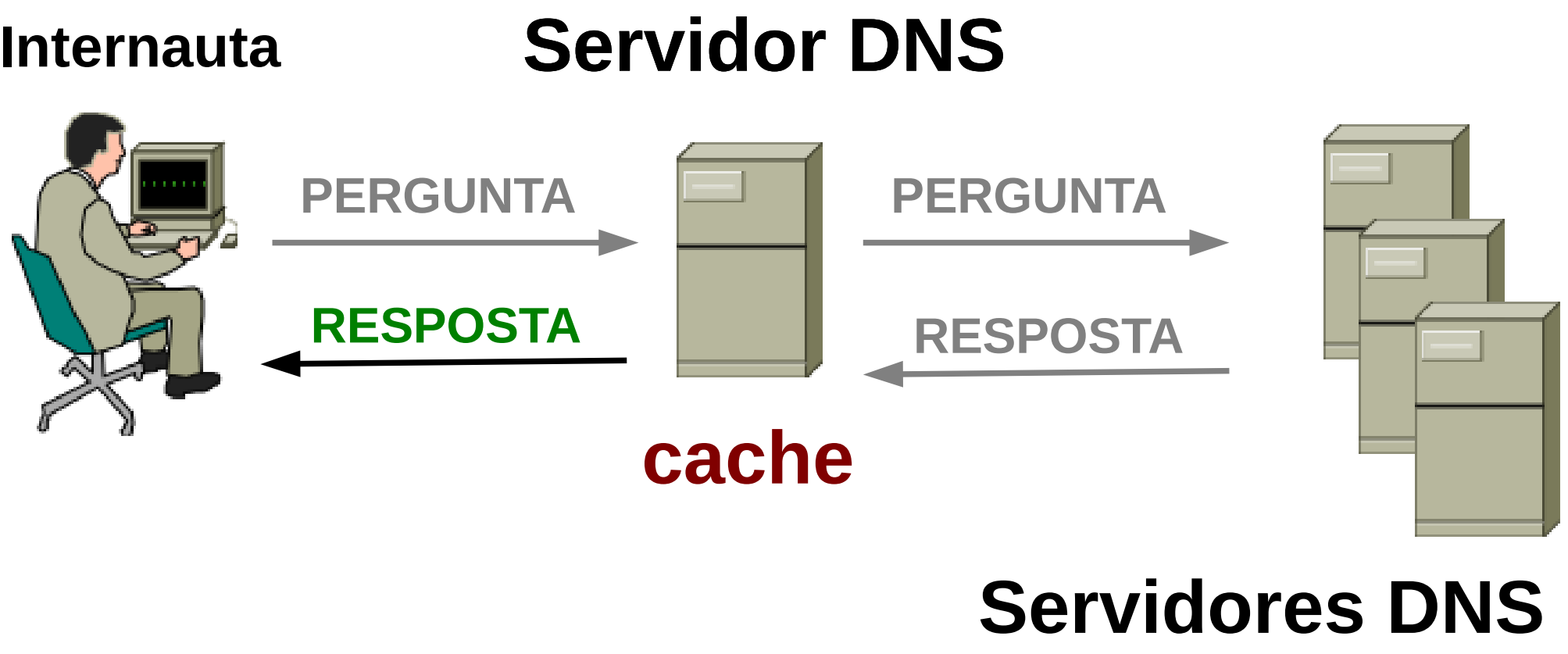
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



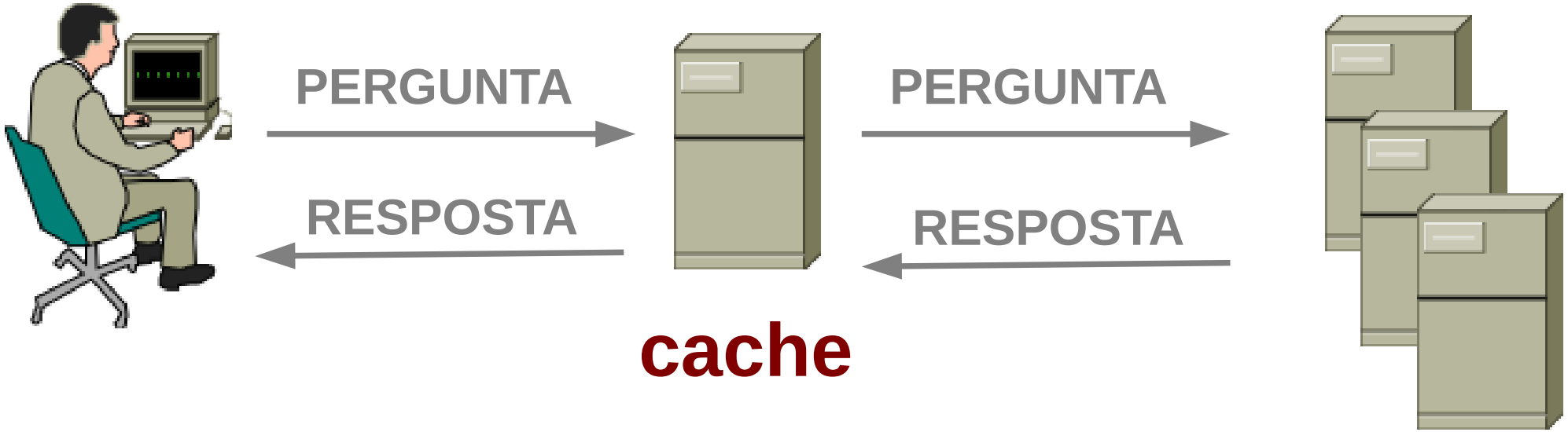
1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



Servidores DNS

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

CVE-2008-1447
DNS Cache Poisoning

Dan Kaminsky

→ Servidores DNSs Vulneráveis

→ Windows

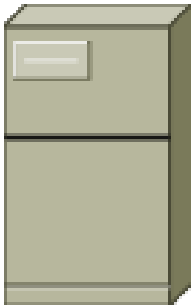
→ Unix/Linux

→ Dispositivos de redes

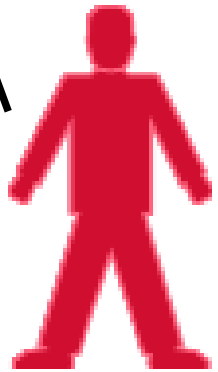
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



PERGUNTAS

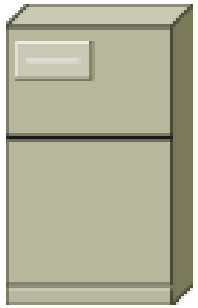


Atacante

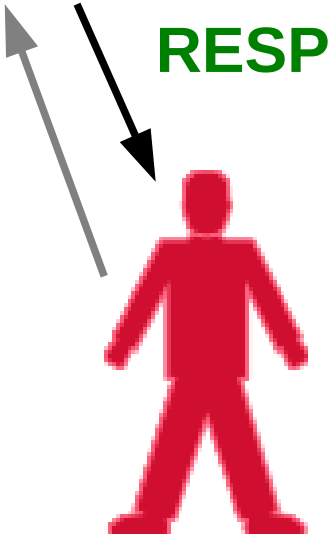
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



RESPOSTAS

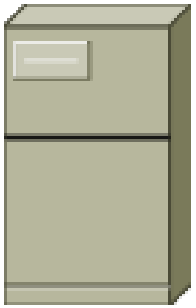


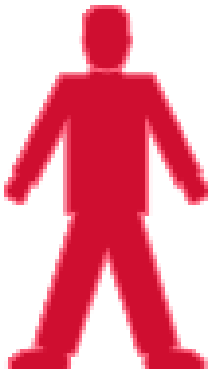
Atacante

1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS





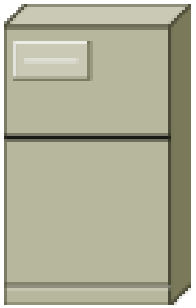
Atacante

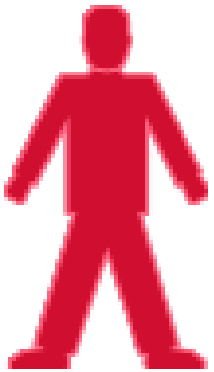
INFORMAÇÕES
- Porta
- ID

1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS





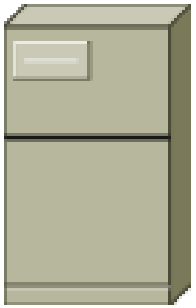
www.banco.com.br
IP = 166.66.66.6

Atacante

1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



ataque

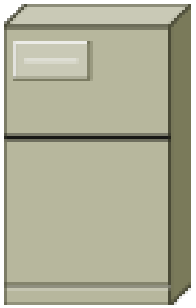
www.banco.com.br
IP = 166.66.66.6

Atacante

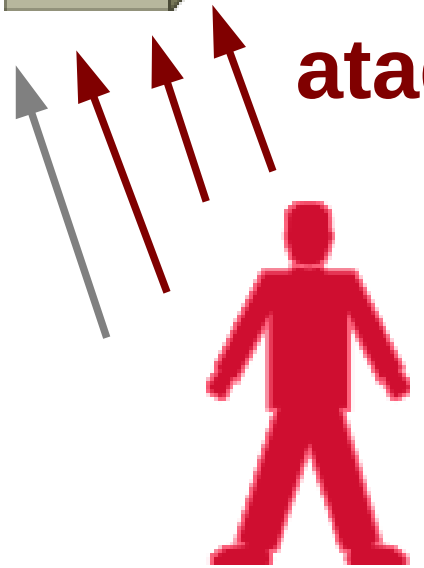
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



ataque



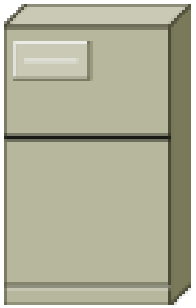
www.banco.com.br
IP = 166.66.66.6

Atacante

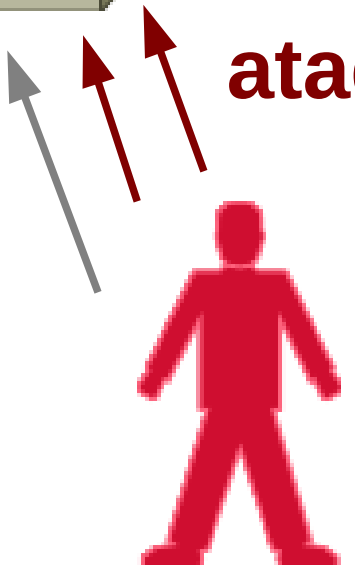
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



ataque



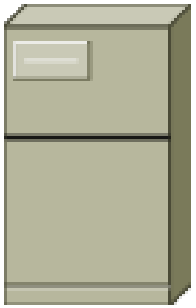
www.banco.com.br
IP = 166.66.66.6

Atacante

1 – Confiar na Resolução de Domínios?

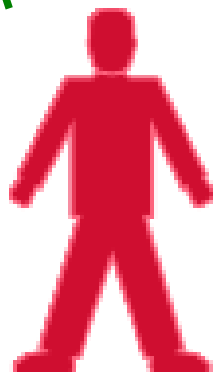
Internauta

Servidor DNS



Cache:
Banco.com.br → 166.66.66.6

ataque



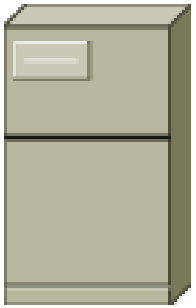
www.banco.com.br
IP = 166.66.66.6

Atacante

1 – Confiar na Resolução de Domínios?

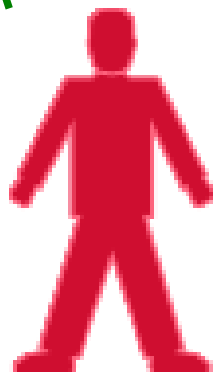
Internauta

Servidor DNS



Cache:
Banco.com.br → 166.66.66.6

ataque



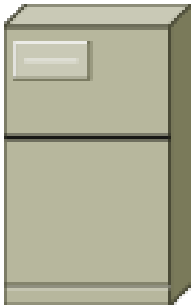
www.banco.com.br
IP = 166.66.66.6

Atacante

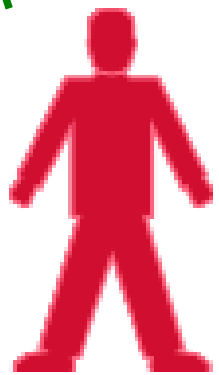
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



Cache:
Banco.com.br → 166.66.66.6



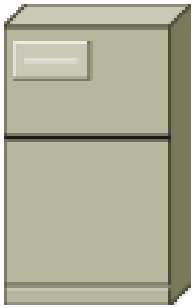
www.banco.com.br
IP = 166.66.66.6

Atacante

1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



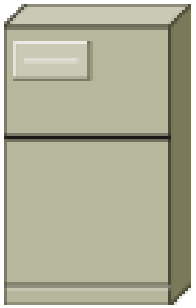
Cache:
Banco.com.br → 166.66.66.6

1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS

Banco.com.br?



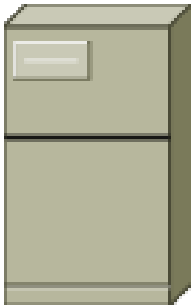
Cache:
Banco.com.br → 166.66.66.6

1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS

Banco.com.br?



166.66.66.6

Cache:
Banco.com.br → 166.66.66.6

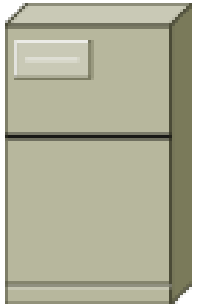
1 – Confiar na Resolução de Domínios?

Internauta

1 – Confiar na Resolução de Domínios?

Internauta

Servidor Web Banco



123.31.123.31

Servidor Web Atacante

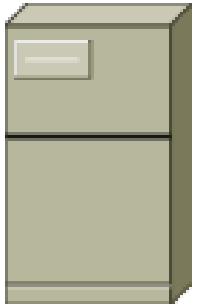
166.66.66.6

1 – Confiar na Resolução de Domínios?

Internauta

Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31

Servidor Web Atacante

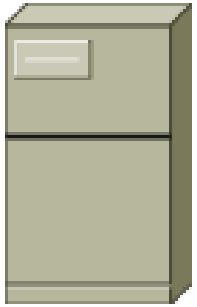
166.66.66.6

1 – Confiar na Resolução de Domínios?

Internauta

Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31

Servidor Web Atacante

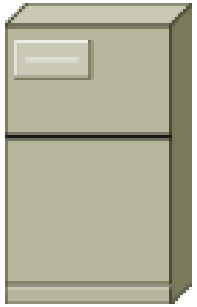
166.66.66.6

1 – Confiar na Resolução de Domínios?

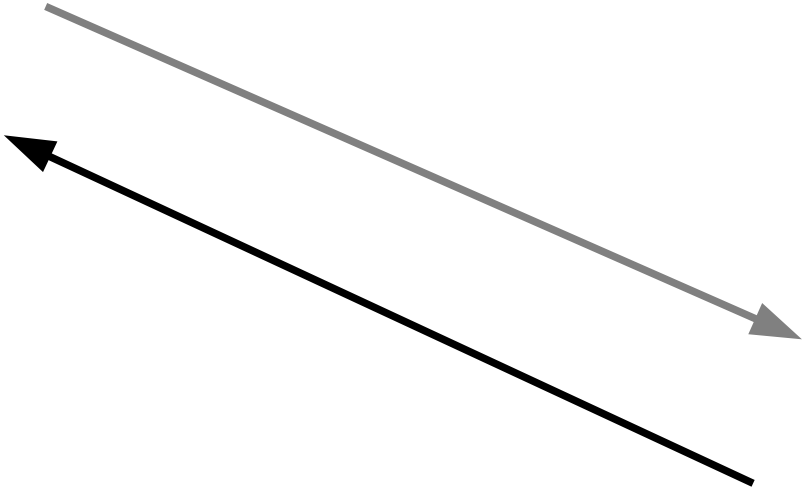
Internauta

Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31



Servidor Web Atacante

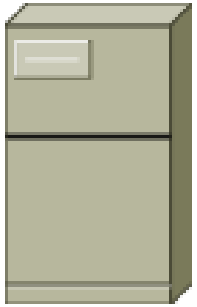
166.66.66.6

1 – Confiar na Resolução de Domínios?

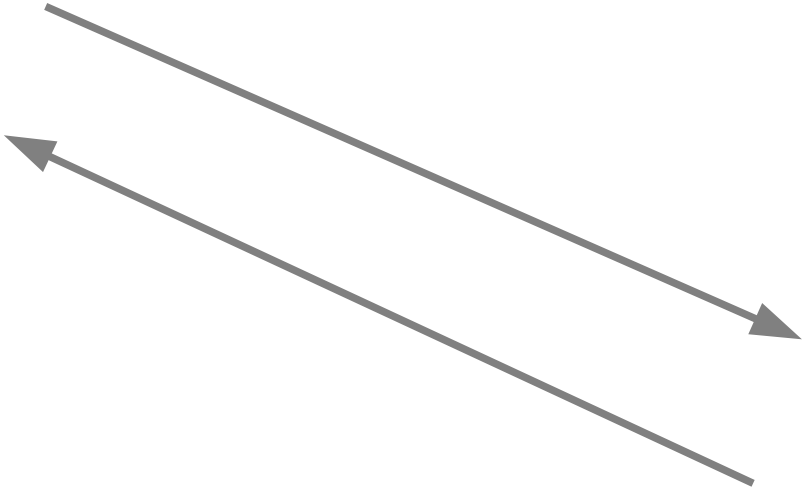
Internauta

Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31



Servidor Web Atacante

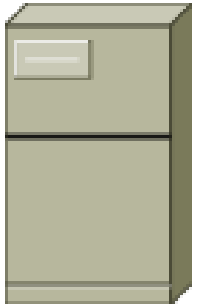
166.66.66.6

1 – Confiar na Resolução de Domínios?

Internauta

Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31

Servidor Web Atacante

166.66.66.6

1 – Confiar na Resolução de Domínios?

Incidente de Segurança – Abril/2009

DNS - Provedor (Net)

WEB - Banco (Brad)

Site hospedado na Ásia usado para roubar senhas e credenciais.

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

Incidentes de Segurança

Malawi (domínios .mw)
Fev/2013

Kenya (domínios .ke)
Abril/2013

Provavelmente DNS Poison

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

Incidentes de Segurança

Malawi (domínios .mw)
Fev/2013

Kenya (domínios .ke)
Abril/2013

Provavelmente DNS Poison

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

China - Jan/2014

The Register®

Data Centre | Software | Networks | **Security** | Business | Hardware | Science | Bootnotes | Video | Forums

SECURITY

DNS poisoning slams web traffic from millions in China into the wrong hole

ISP blames unspecified attack for morning outage

By John Leyden, 21 Jan 2014 Follow 2,990 followers

8

Linux and AIX Bare-Metal Recovery Webinar

A widespread DNS outage hit China on Tuesday, leaving millions of surfers adrift.

RELATED

DNS issues in China between 7am and 9am GMT left millions of domains

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

Malaisia – Out/2013 (google.com.my)

Google Malaysia hit by DNS poisoning (Updated)

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

Solução:

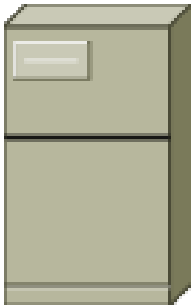
Paliativa
- antes (possibilidade 1 em 65535)
- depois (possibilidade 1 em 134 mi)

1 – Confiar na Resolução de Domínios?

Internauta

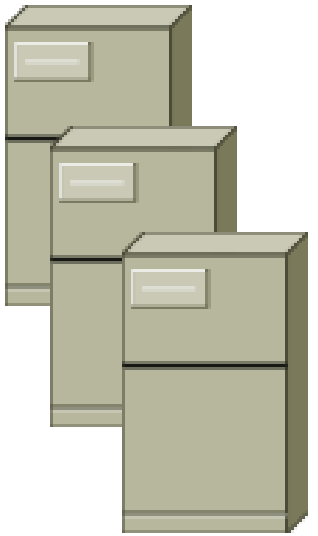
Servidor DNS

PERGUNTA



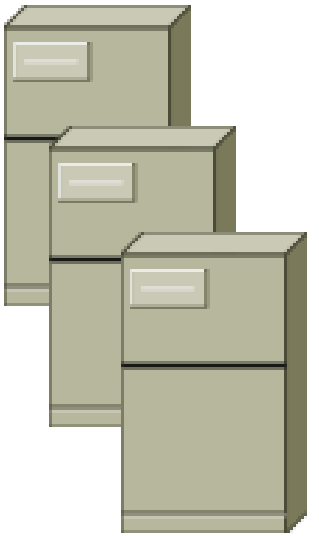
?

PERGUNTA



Servidores DNS

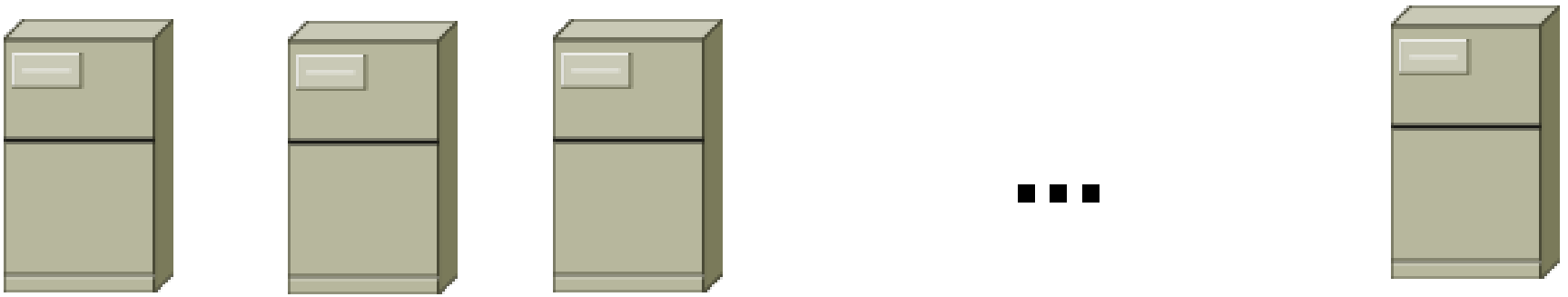
1 – Confiar na Resolução de Domínios?



Servidores DNS

1 – Confiar na Resolução de Domínios?

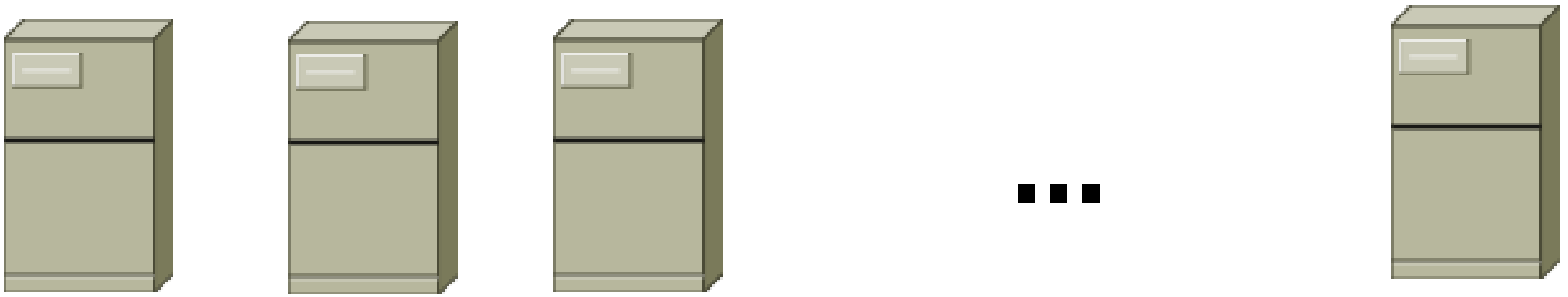
Servidores de DNS Raiz



A B C ... M

1 – Confiar na Resolução de Domínios?

Servidores de DNS Raiz



A **B** **C** **M**

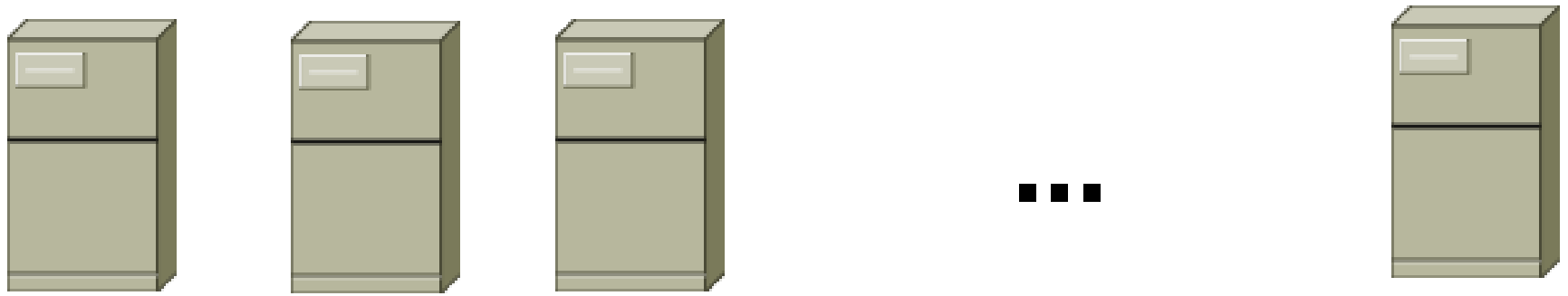
Maior parte nos EUA e na Europa

Domínios TLD → .com, .net, .org, .us, .br ...

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

Servidores de DNS Raiz

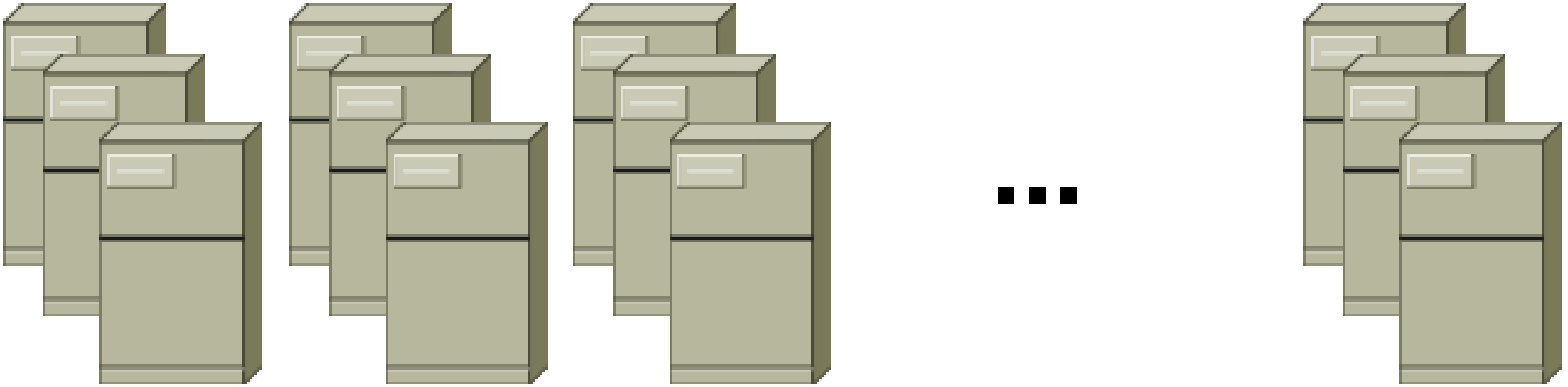


...

A B C

Réplicas pelo Mundo

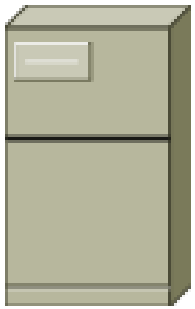
M



...

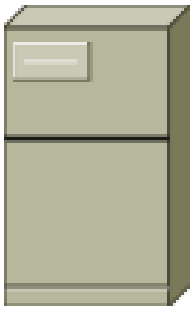
1 – Confiar na Resolução de Domínios?

Incidente de Segurança

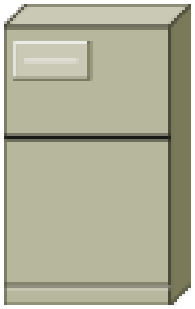


i

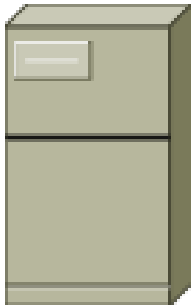
SUÉCIA



i



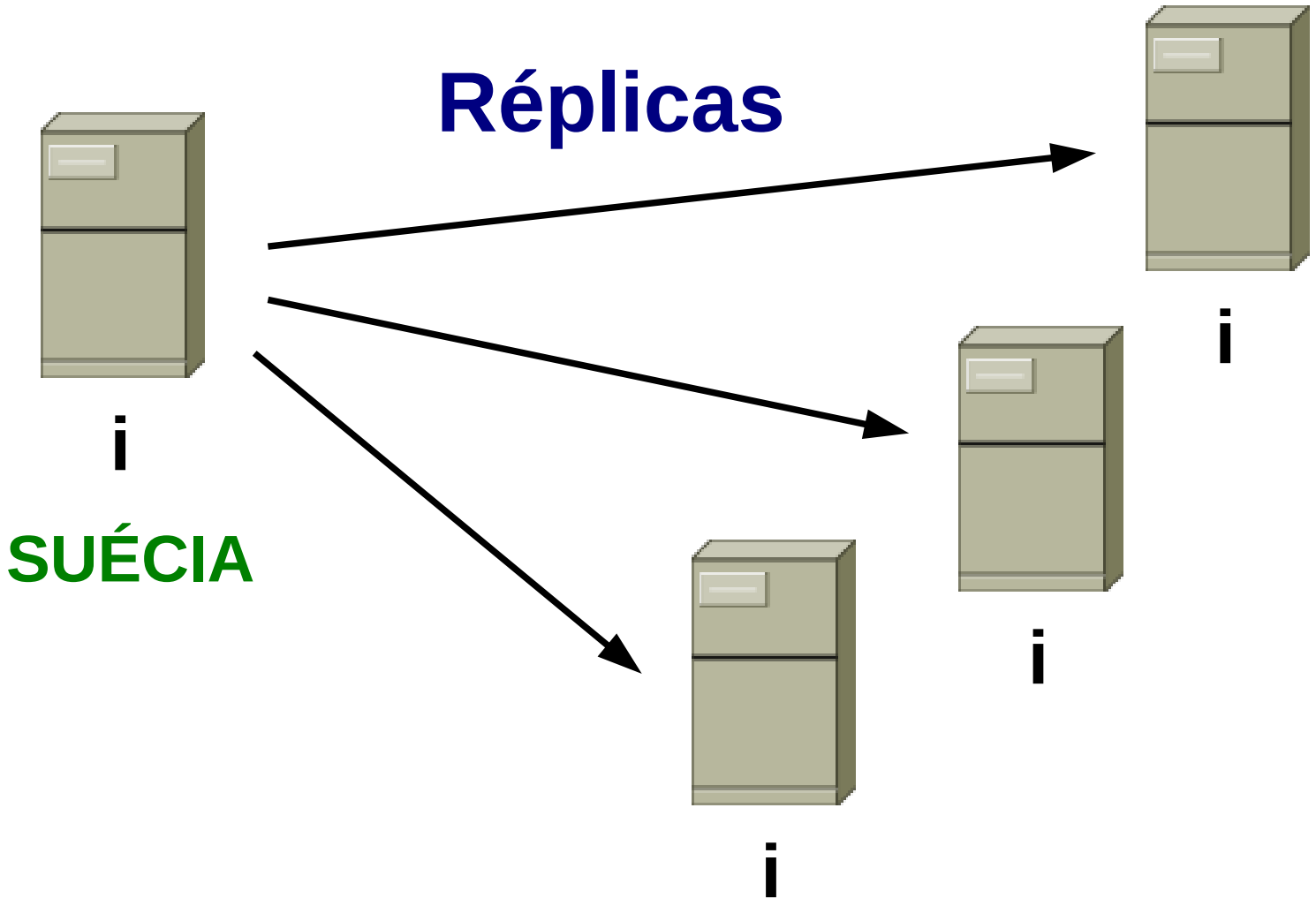
i



i

1 – Confiar na Resolução de Domínios?

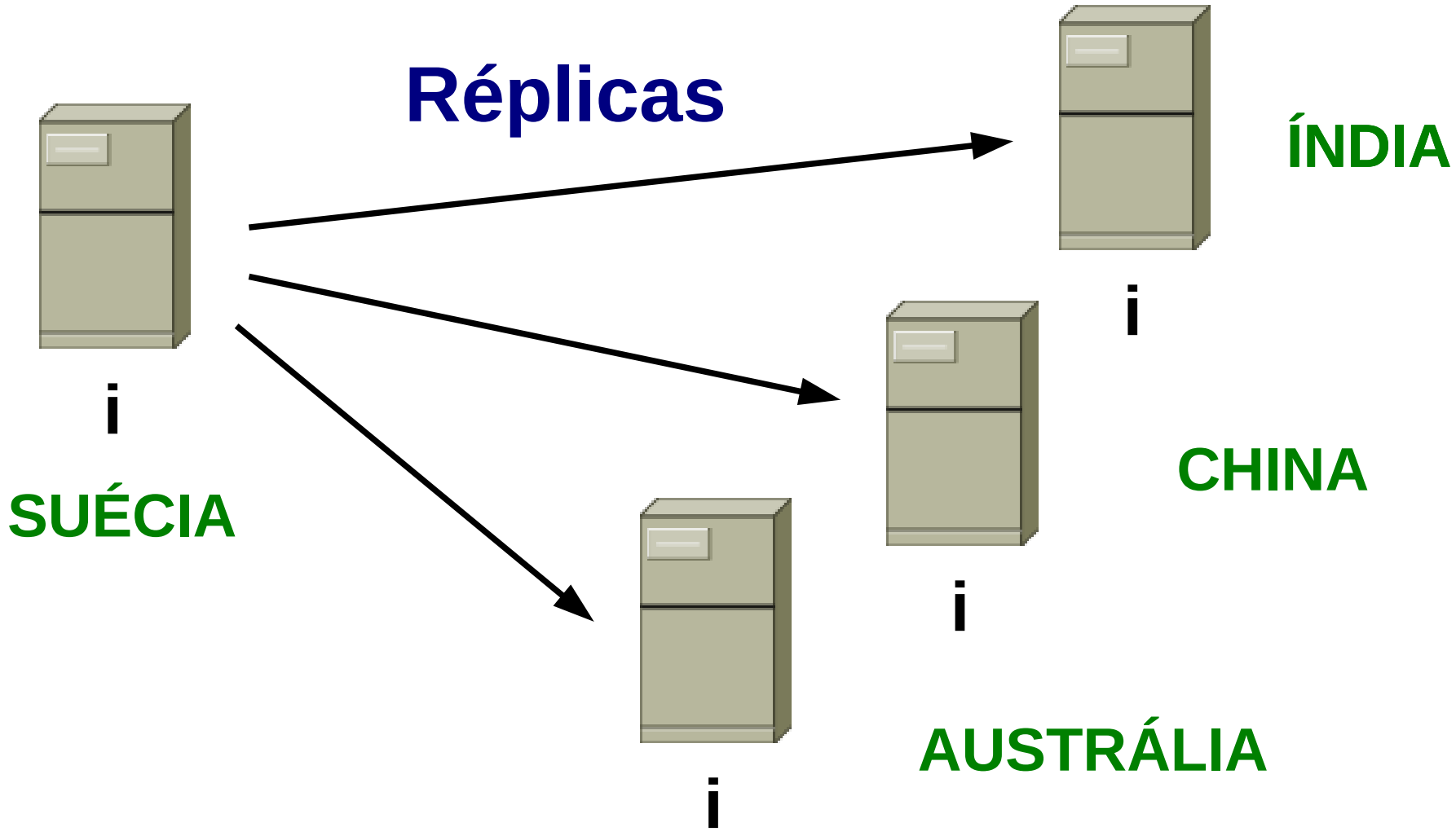
Incidente de Segurança



1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

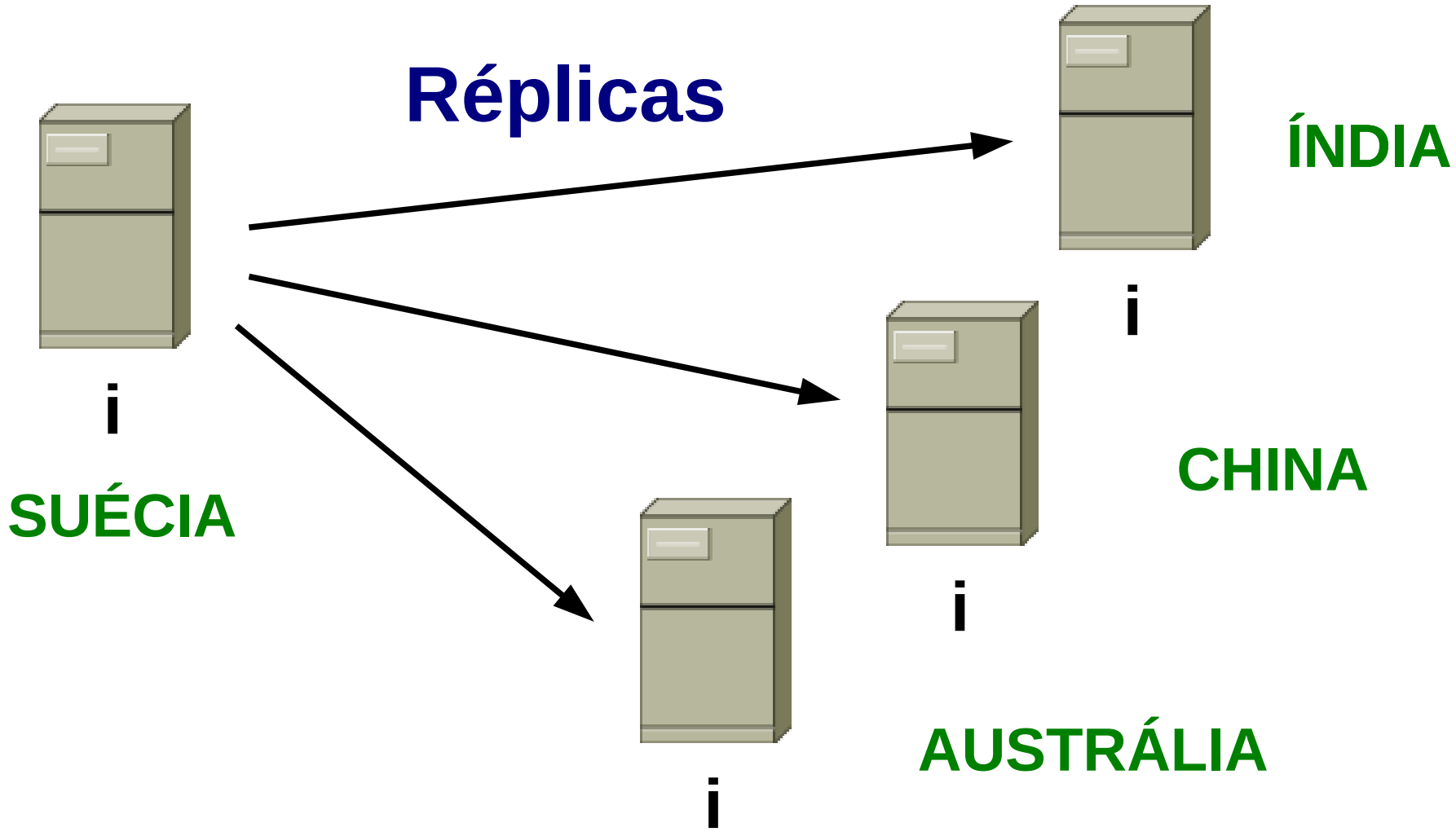
Incidente de Segurança



1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

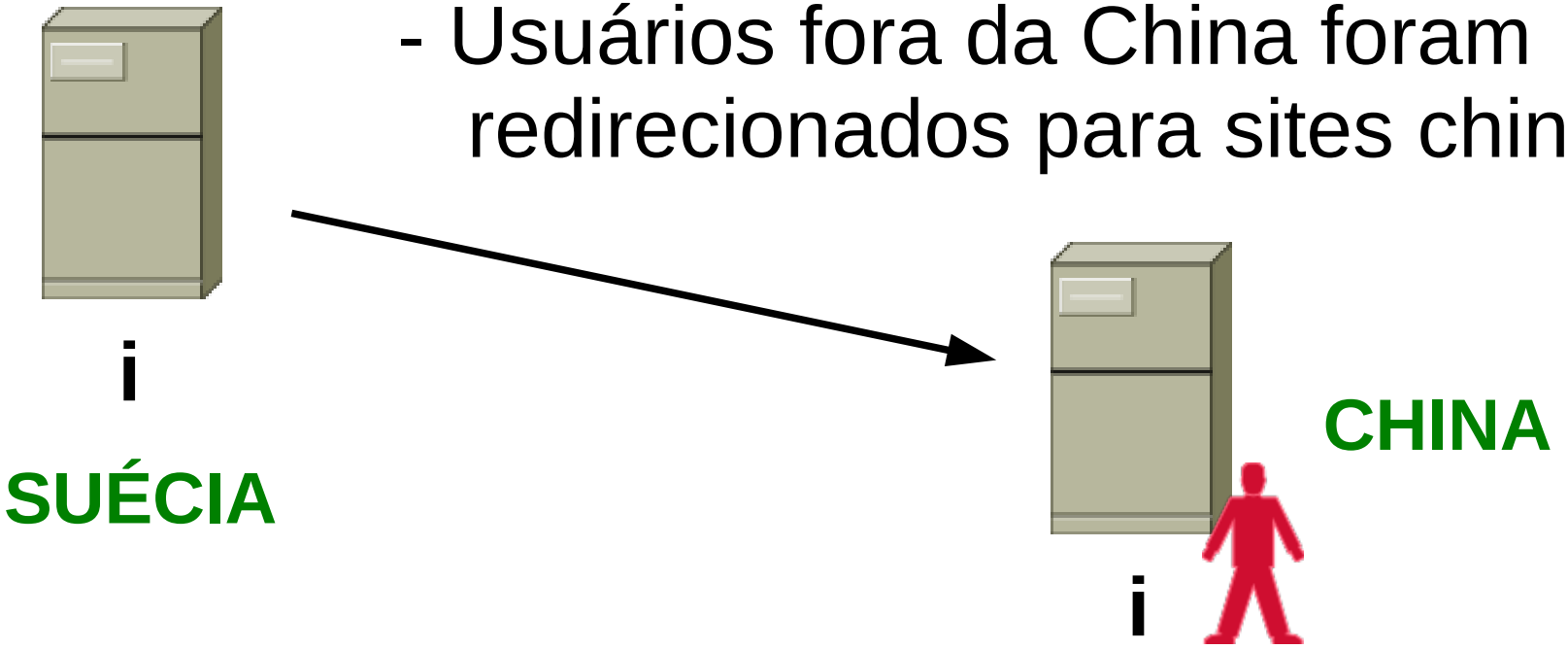
Incidente de Segurança



1 – Confiar na Resolução de Domínios?

Incidente de Segurança

Em março de 2010
- Usuários fora da China foram redirecionados para sites chineses.



- Sites como Facebook, Twitter, Youtube...

1 – Confiar na Resolução de Domínios?

NETWORKING

PCWorld

BUSINESS READY

After DNS Problem, Chinese Root Server Is Shut Down

By Robert McMillan, IDG News Service

Mar 26, 2010 5:10 PM

1 – Confiar na Resolução de Domínios?

CELEPAR INFORMÁTICA do PARANÁ

Solução:

- Empresa Sueca cortou servidor raiz chinês

- Hoje poderia utilizar DNSSEC (DNS Seguro) ?!?

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

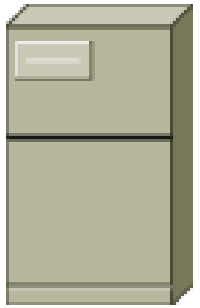
2 -

Podemos confiar no Roteamento de Provedores?

2 – Confiar no Roteamento Provedores?

Internauta

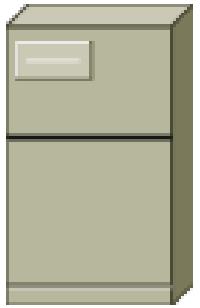
Servidor Web



2 – Confiar no Roteamento Provedores?

Internauta

Servidor Web

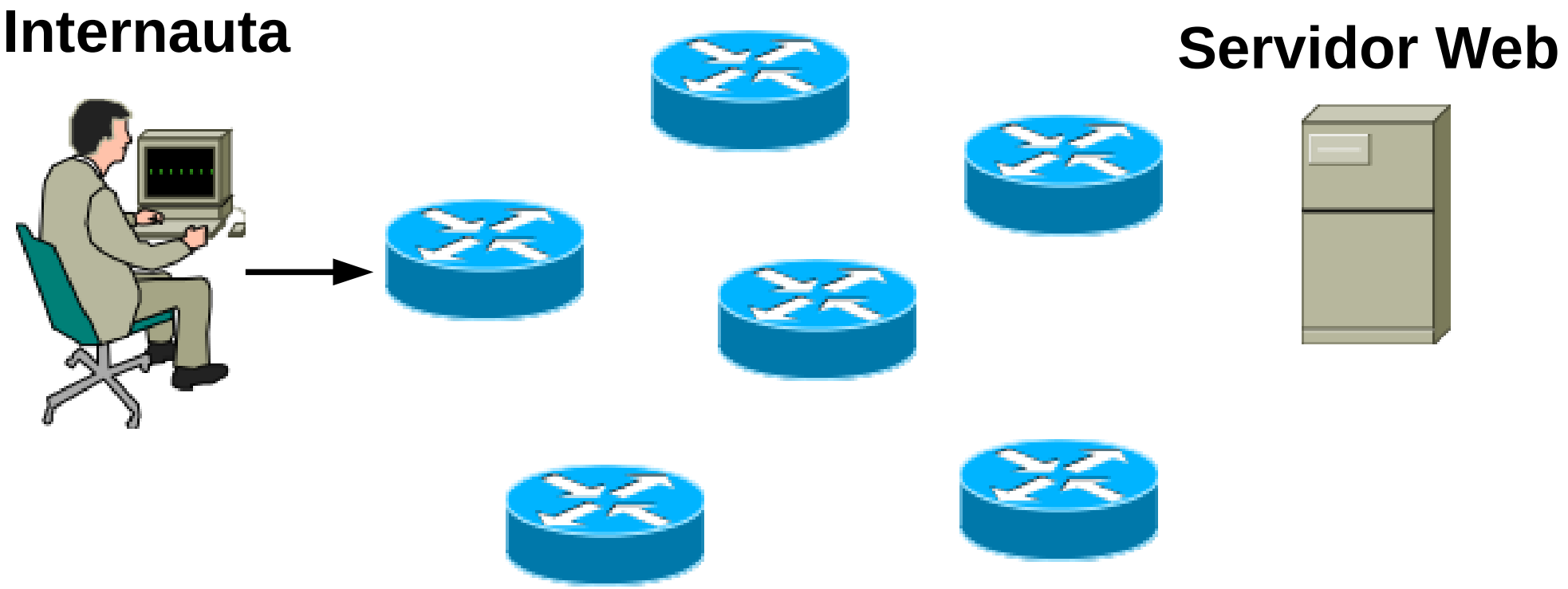


Internet Protocol

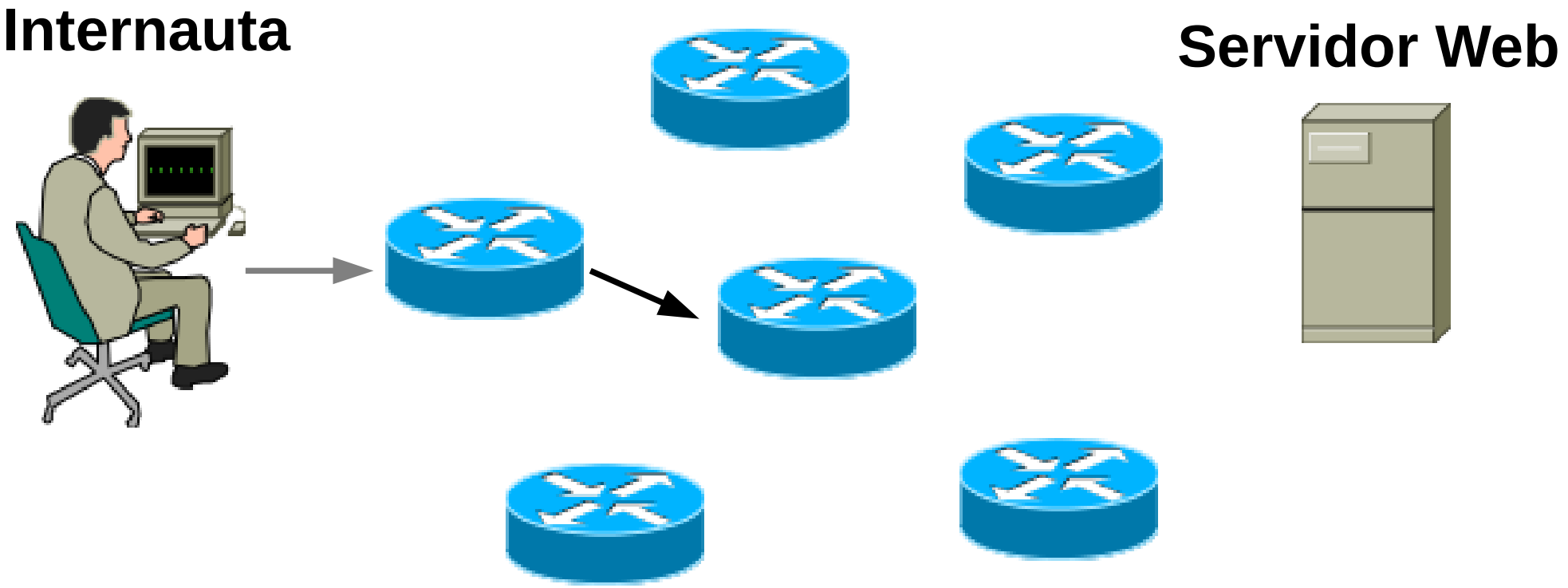
1981

Documento RFC 781

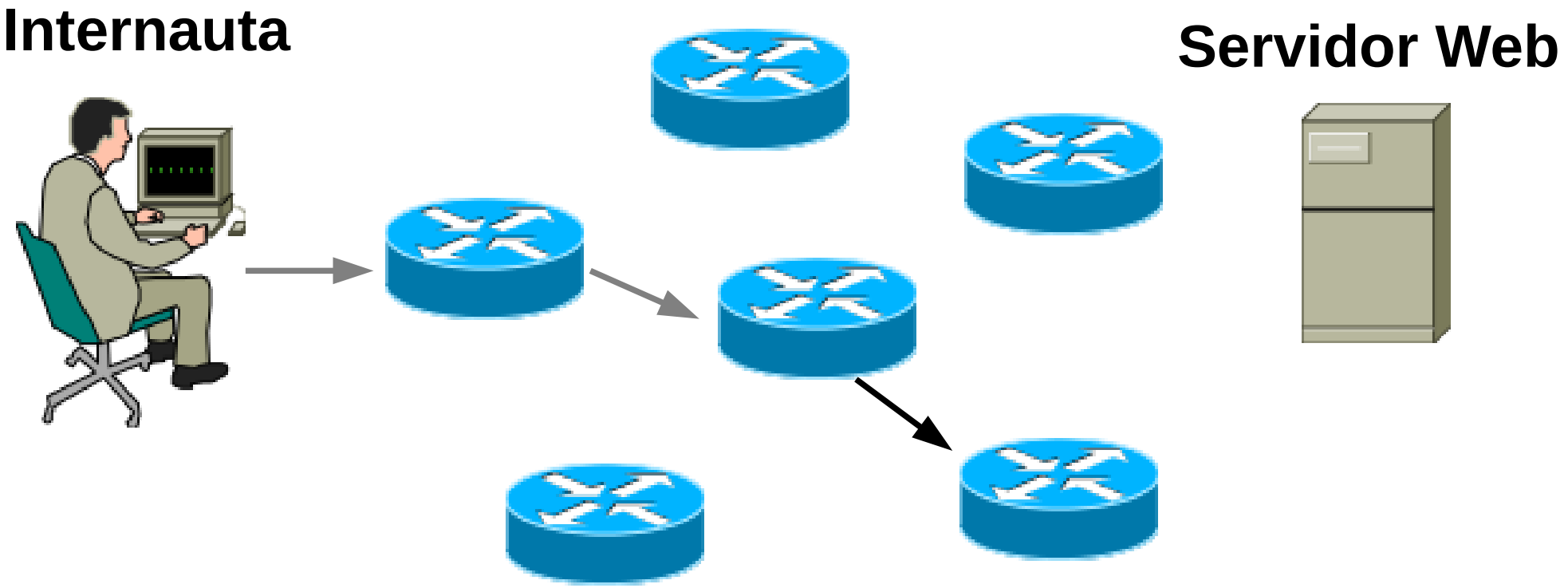
2 – Confiar no Roteamento Provedores?



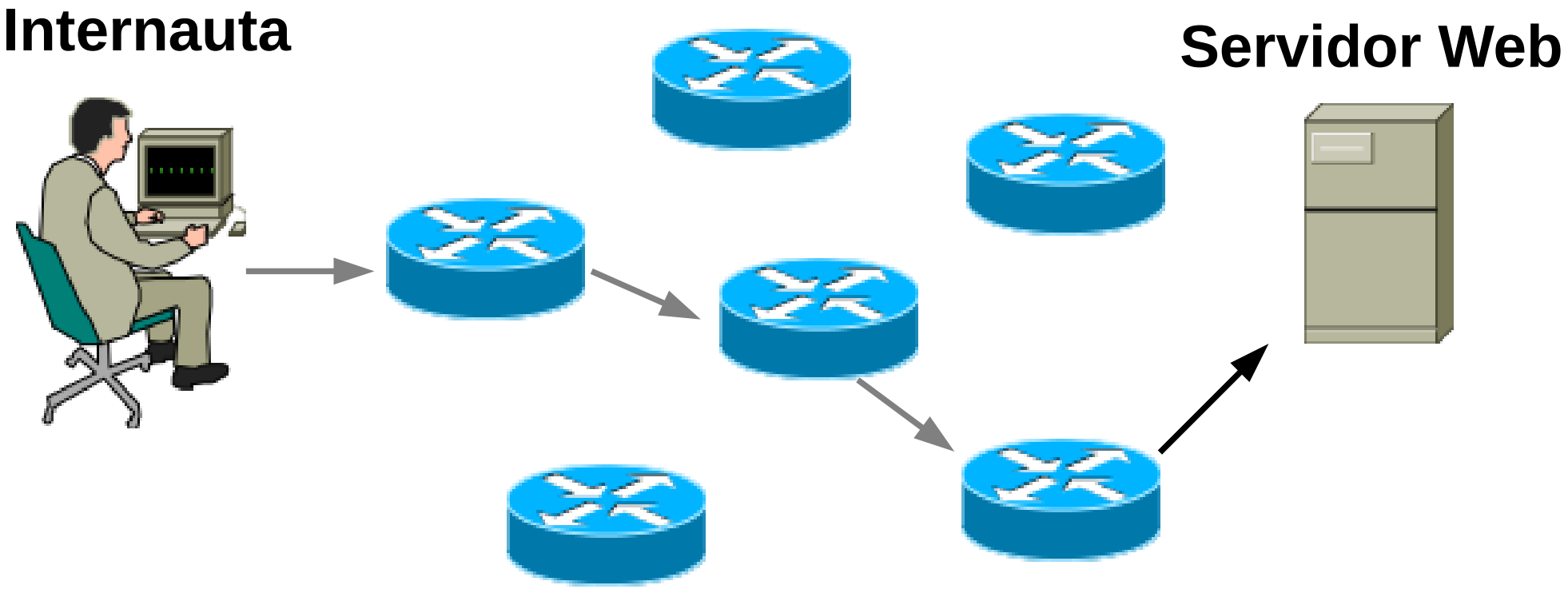
2 – Confiar no Roteamento Provedores?



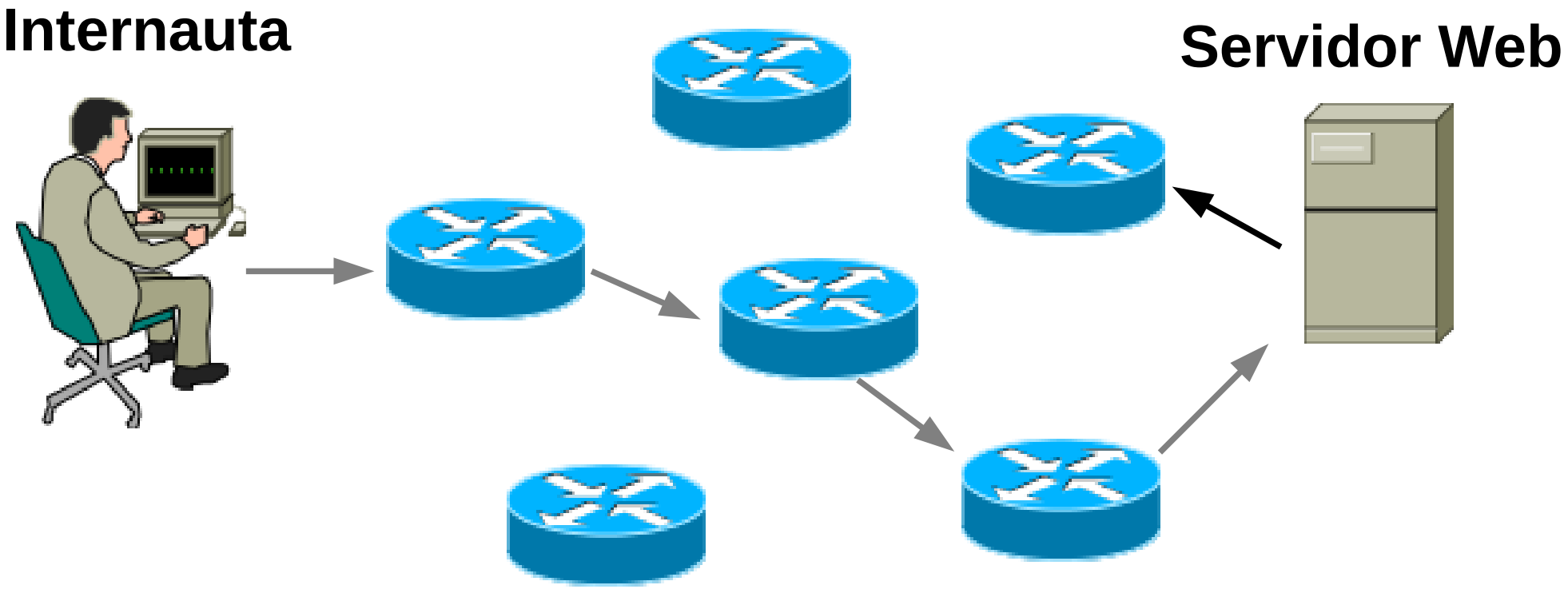
2 – Confiar no Roteamento Provedores?



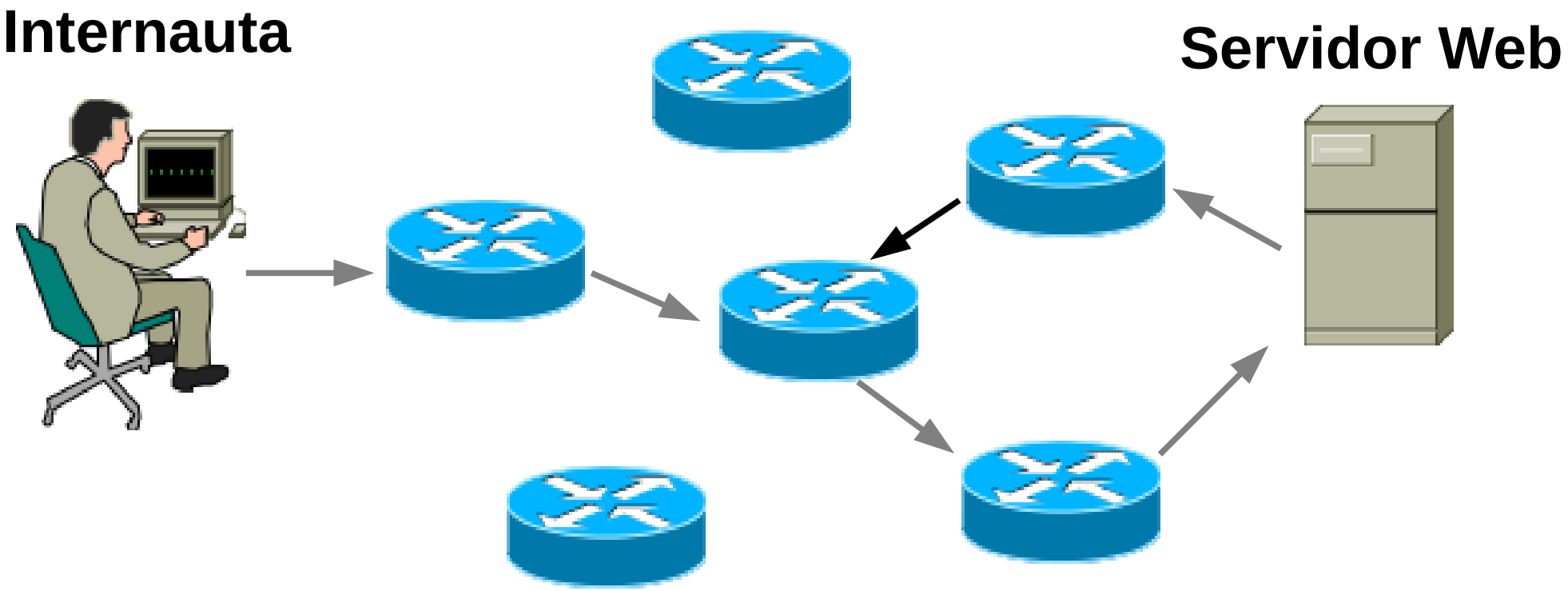
2 – Confiar no Roteamento Provedores?



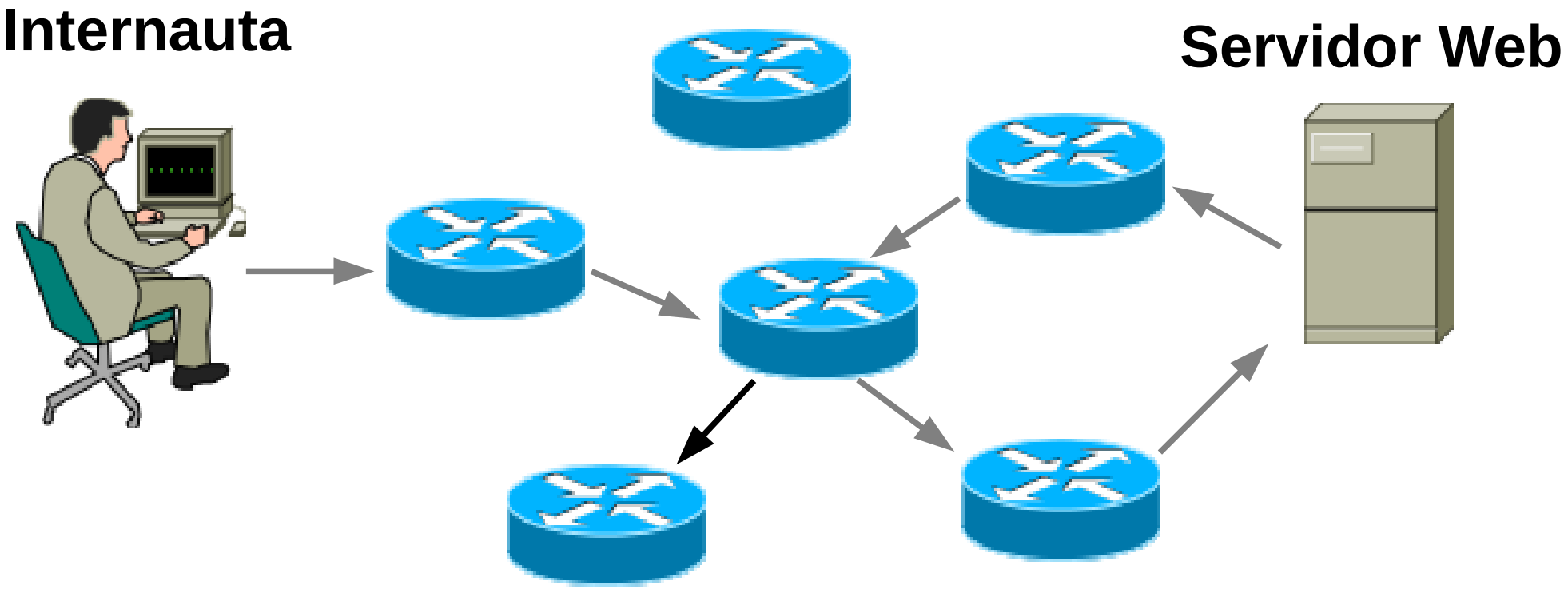
2 – Confiar no Roteamento Provedores?



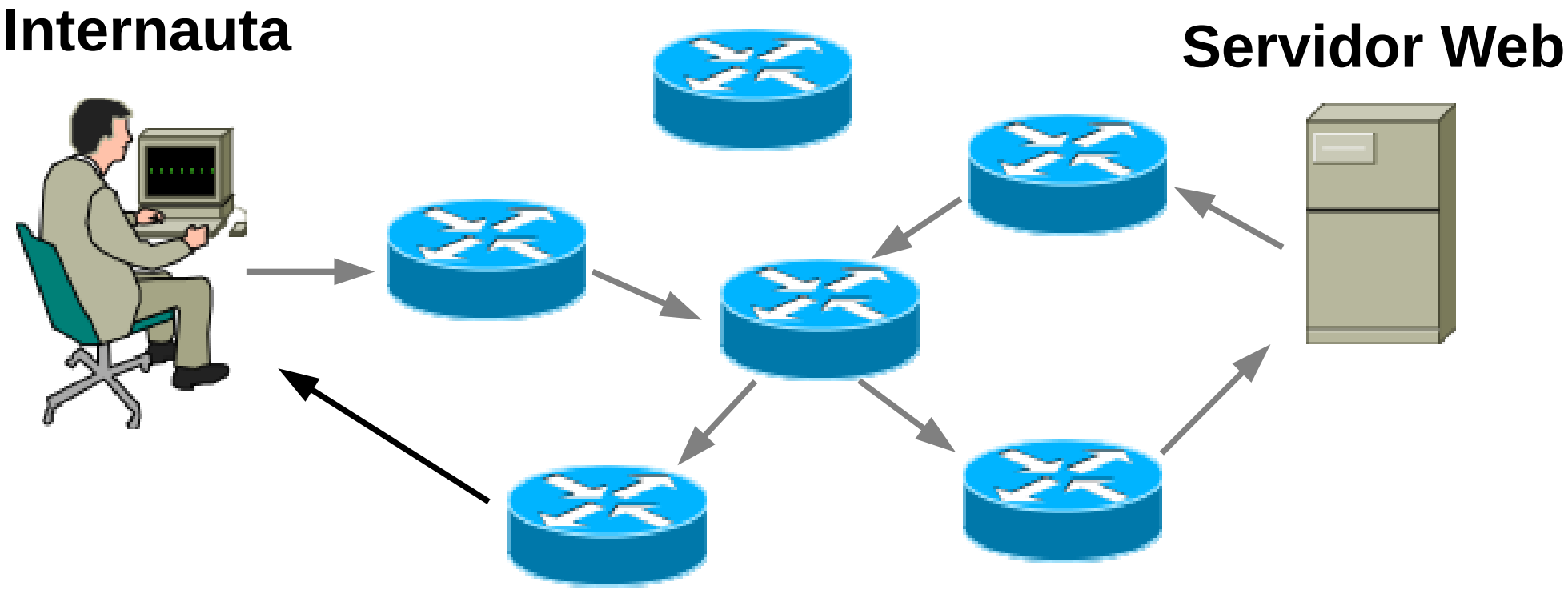
2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?



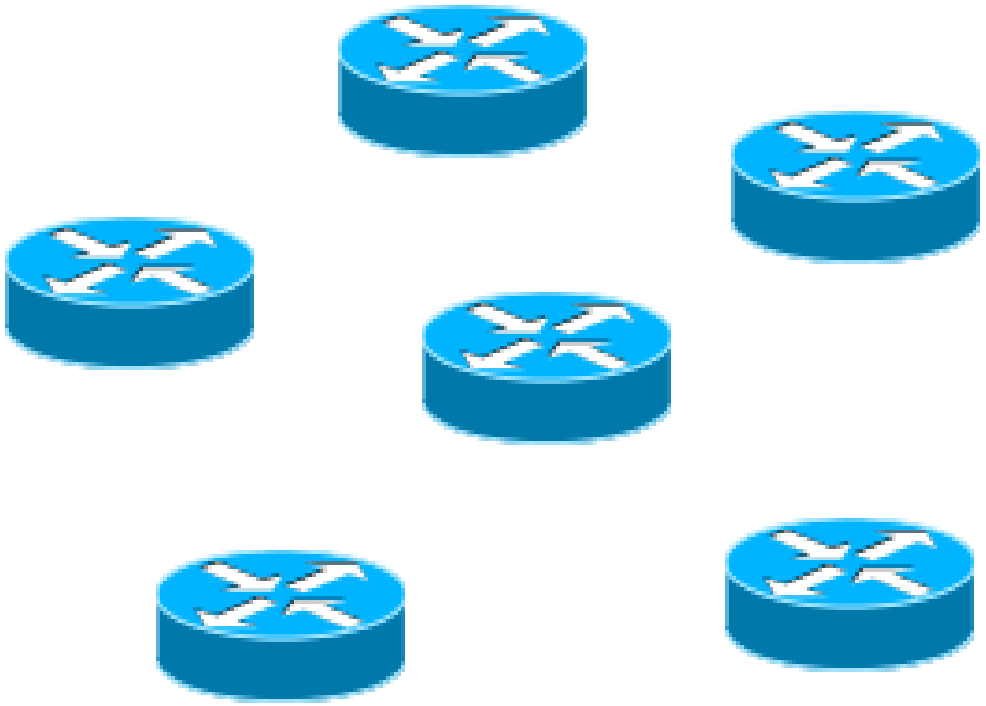
2 – Confiar no Roteamento Provedores?



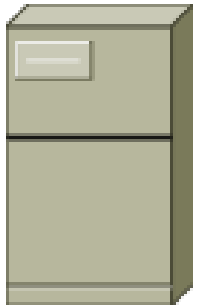
2 – Confiar no Roteamento Provedores?

ROTEAMENTO

Internauta

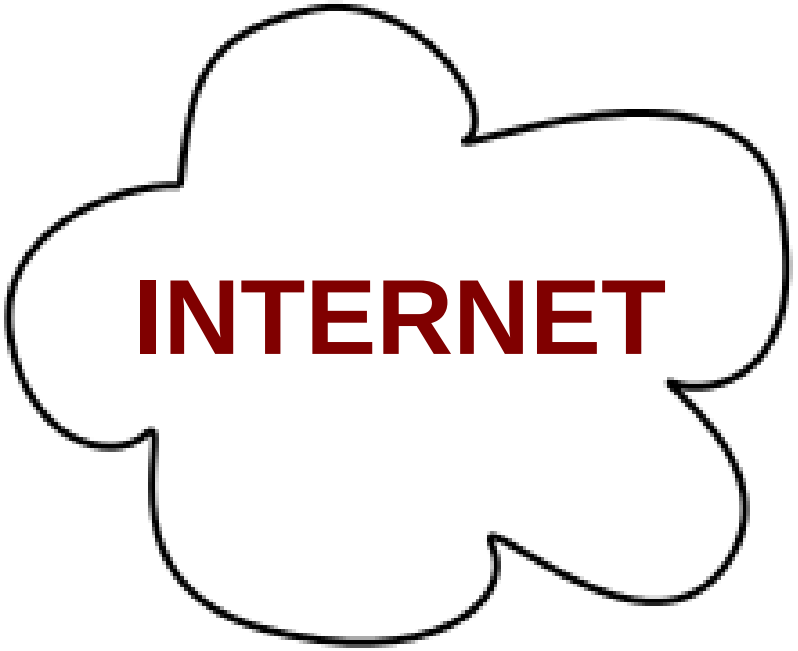


Servidor Web

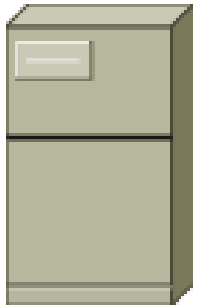


2 – Confiar no Roteamento Provedores?

Internauta



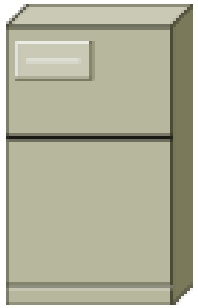
Servidor Web



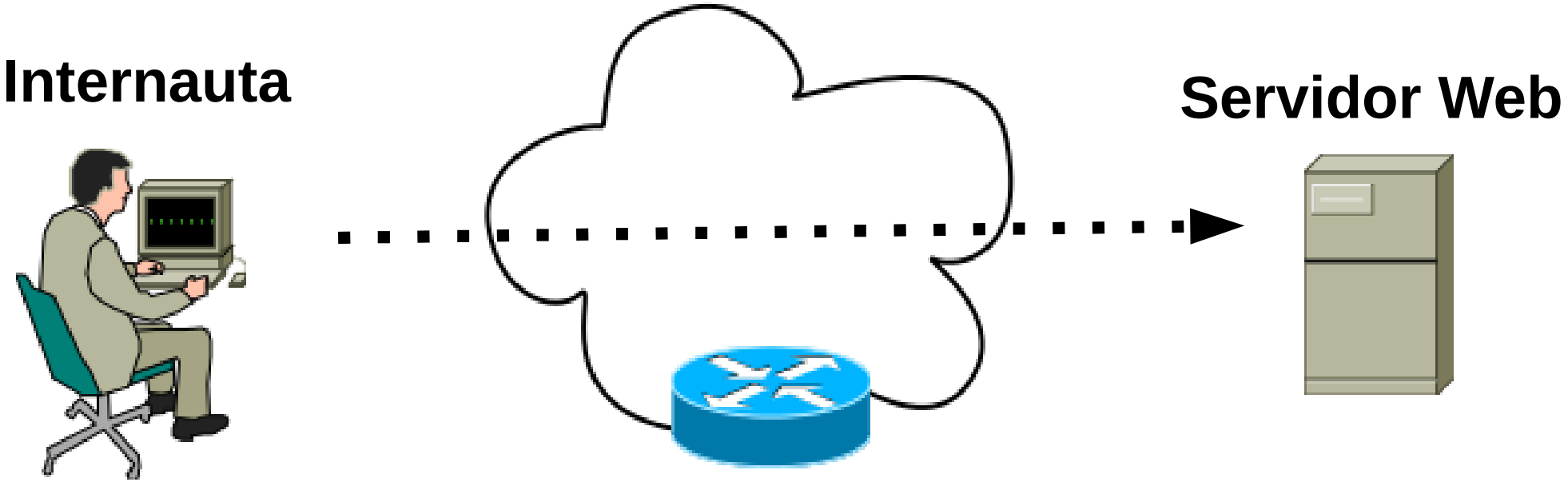
2 – Confiar no Roteamento Provedores?

Internauta

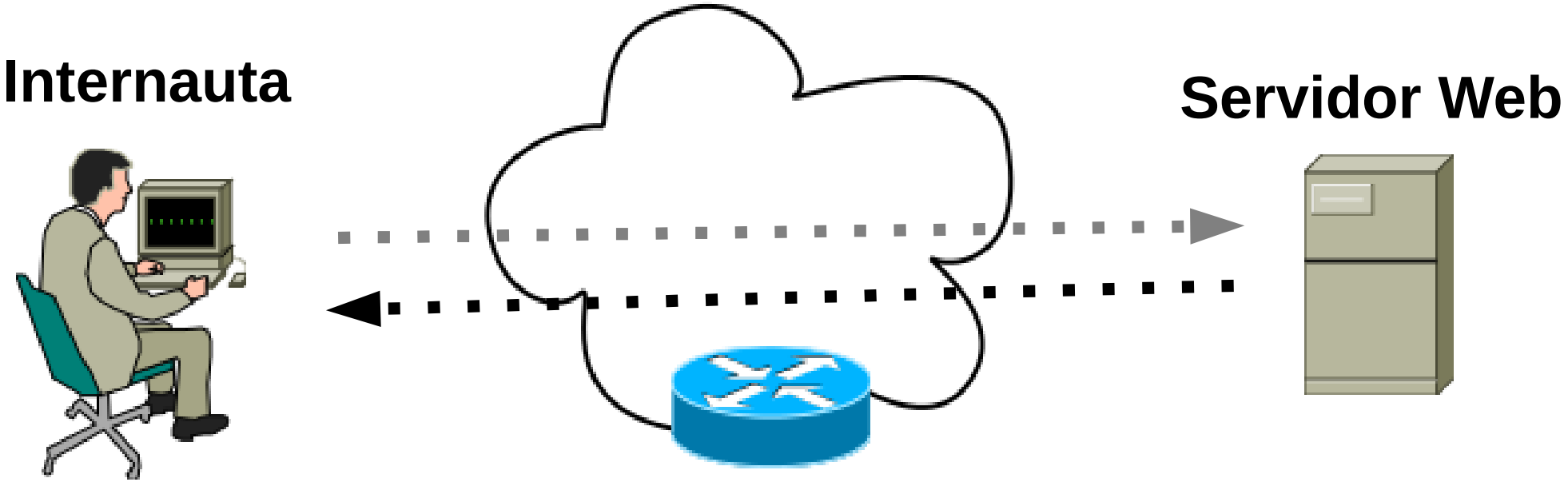
Servidor Web



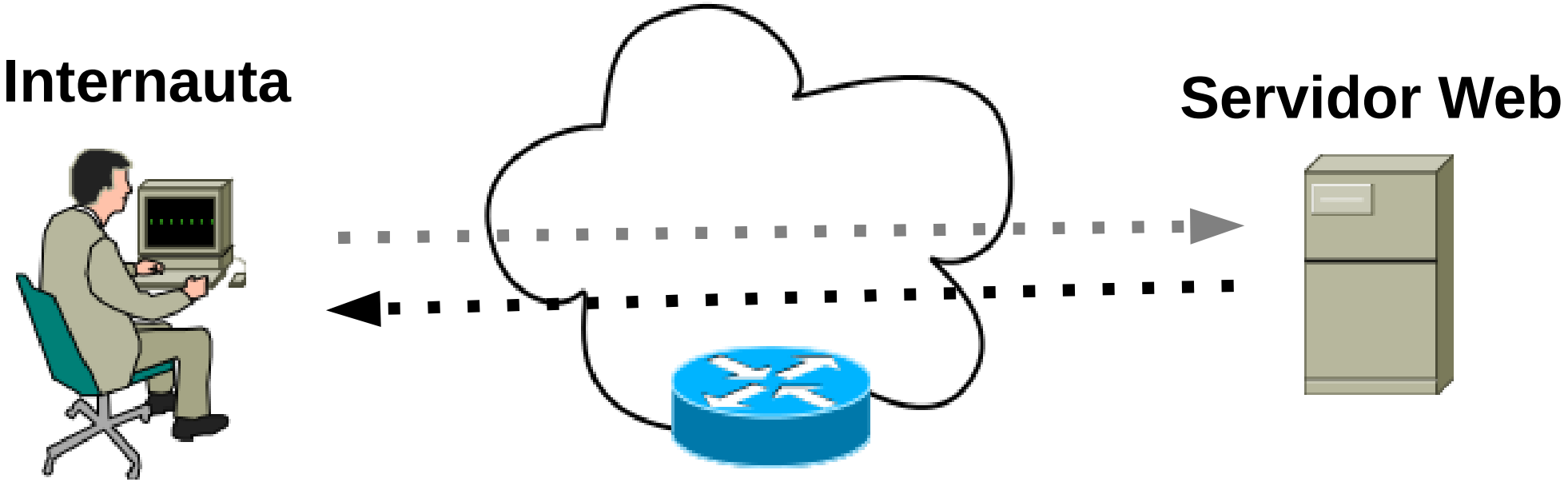
2 – Confiar no Roteamento Provedores?



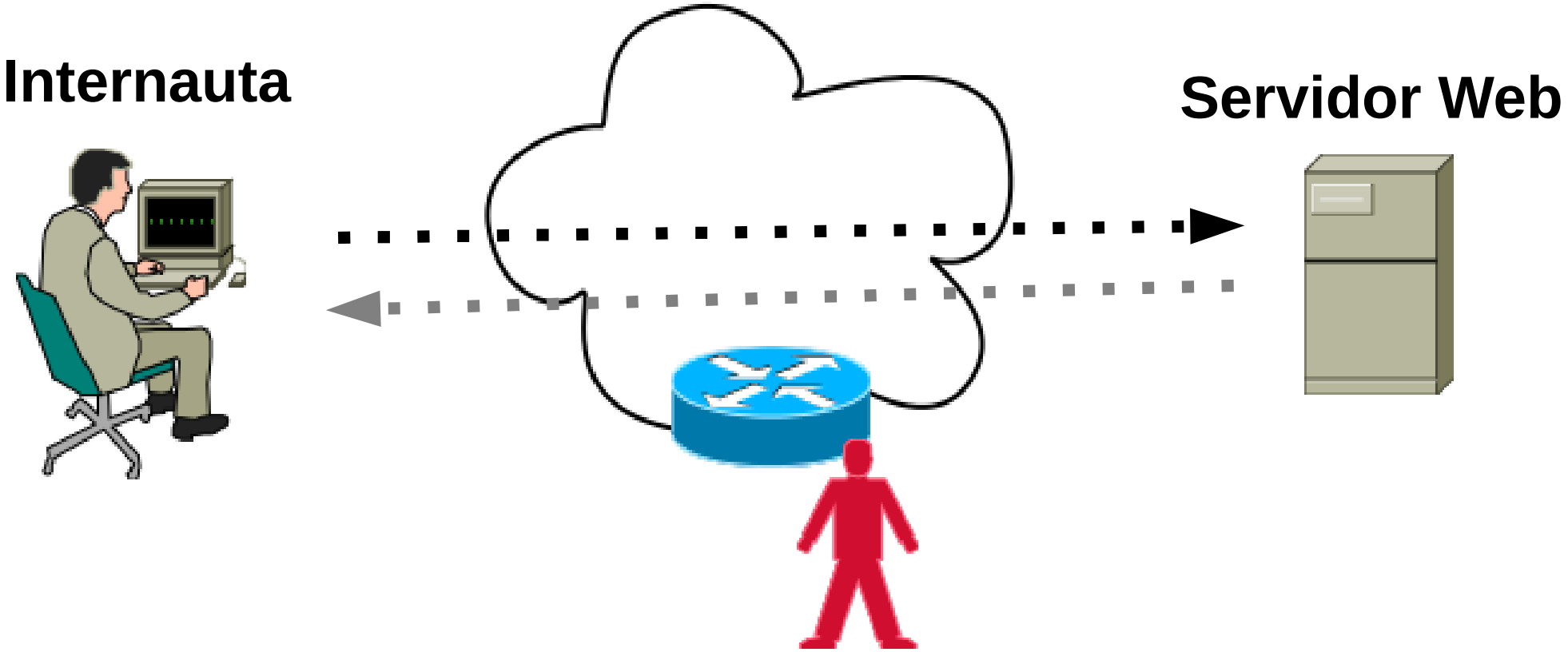
2 – Confiar no Roteamento Provedores?



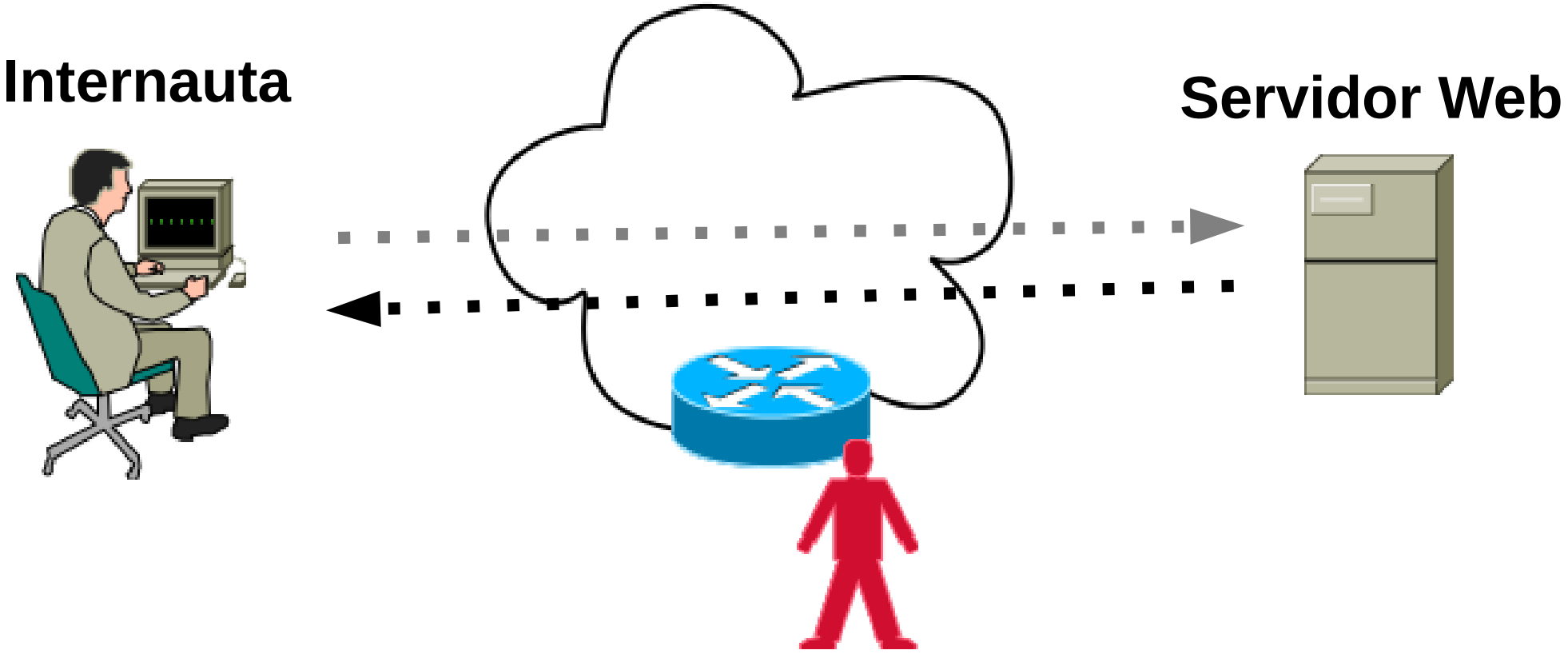
2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?

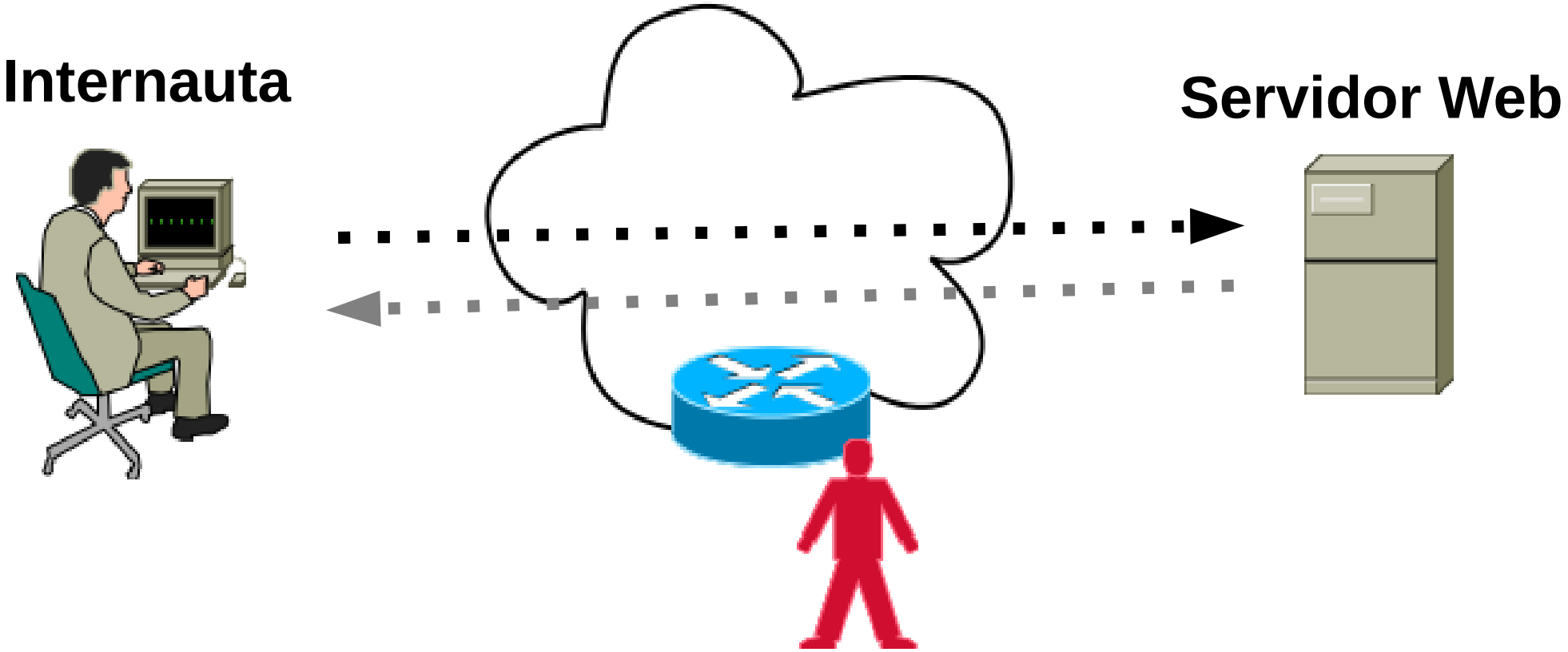


2 – Confiar no Roteamento Provedores?

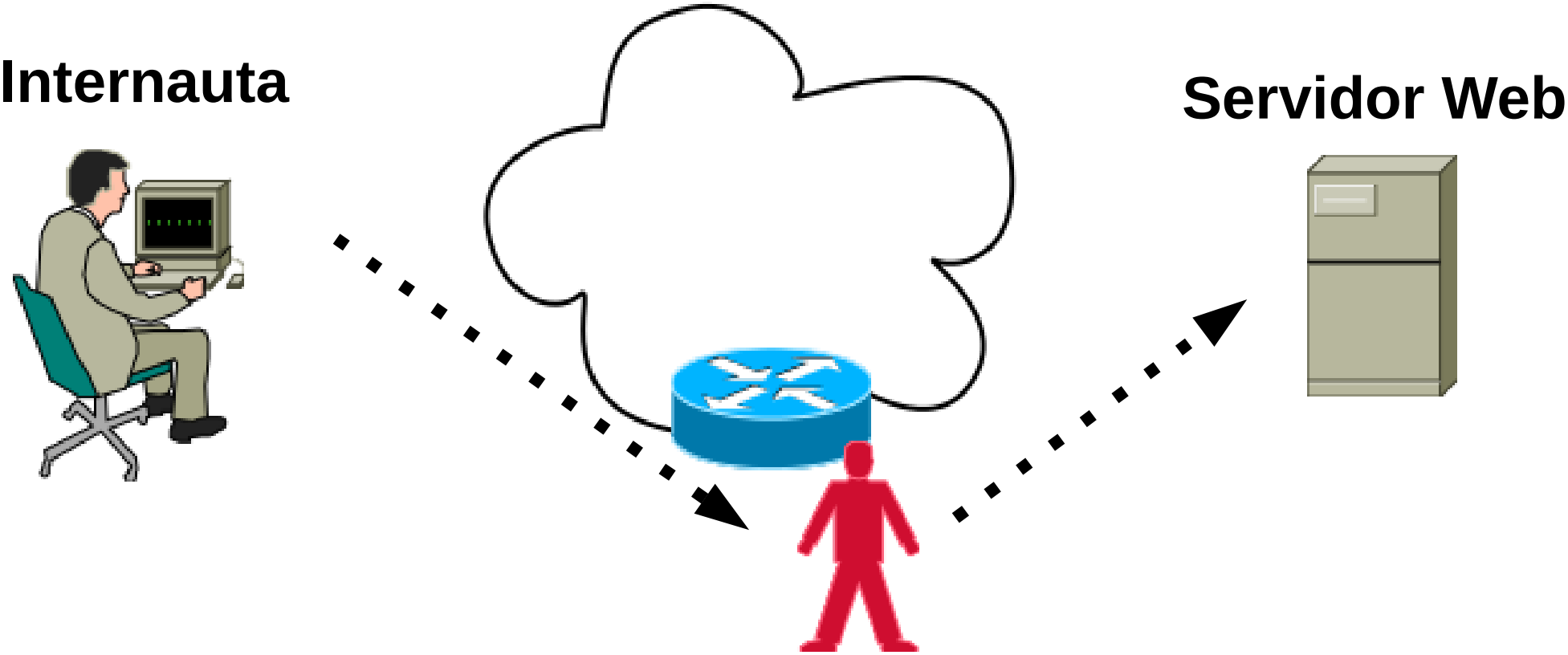


Posso VER o tráfego aberto!

2 – Confiar no Roteamento Provedores?

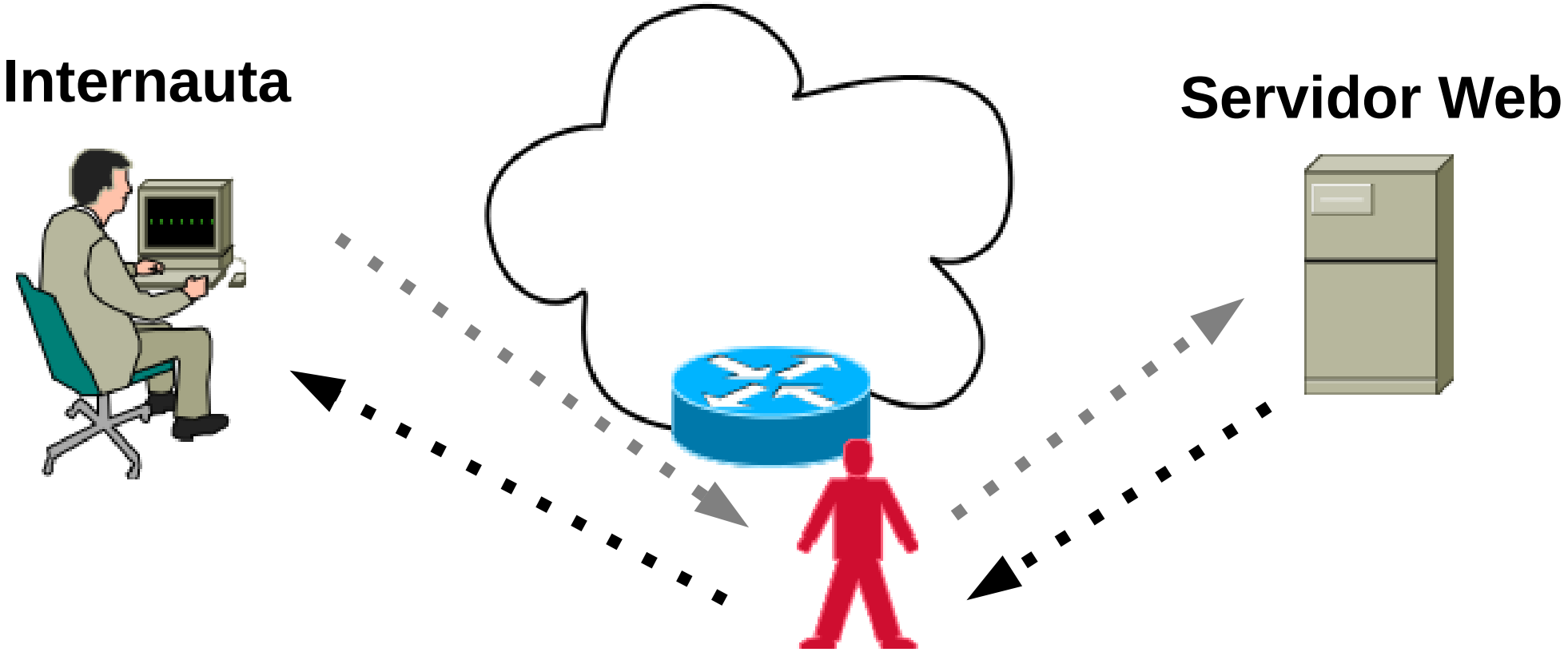


2 – Confiar no Roteamento Provedores?



Posso ALTERAR o tráfego aberto!

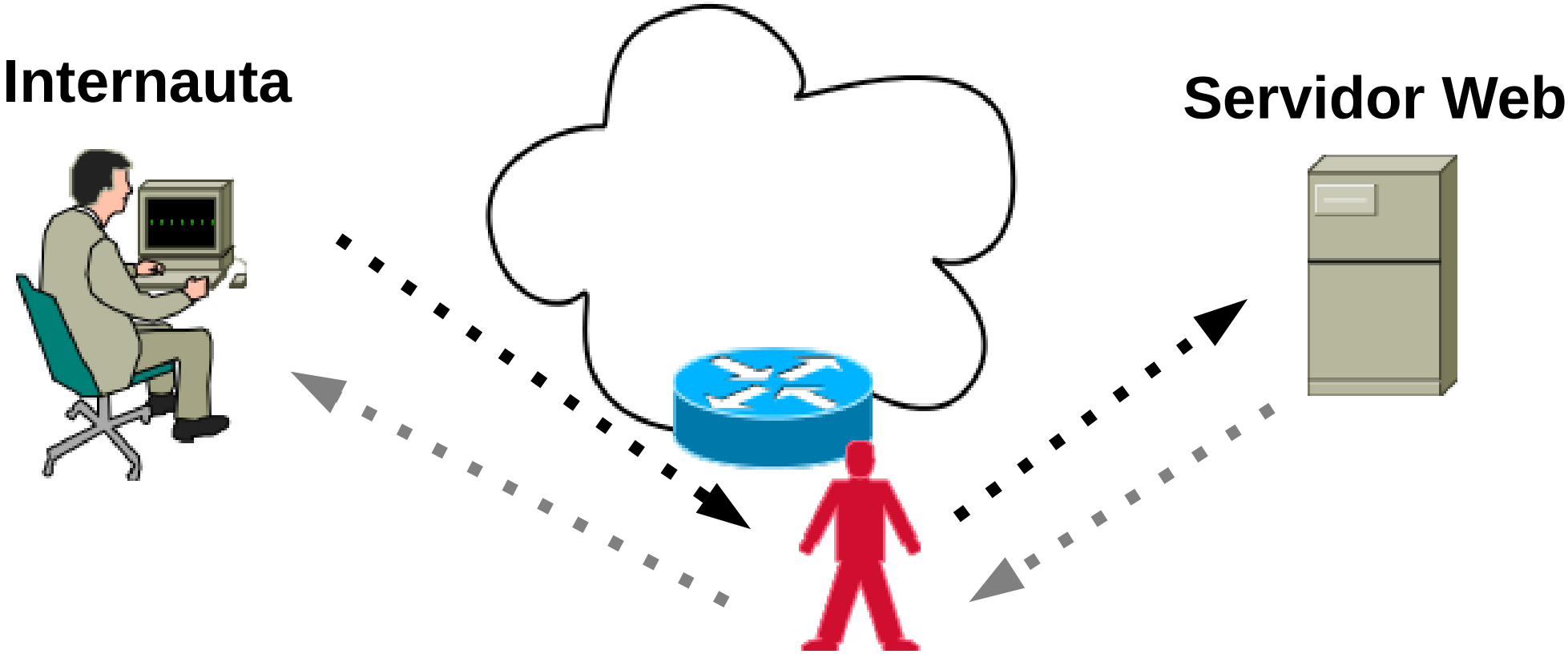
2 – Confiar no Roteamento Provedores?



Posso ALTERAR o tráfego aberto!

2 – Confiar no Roteamento Provedores?

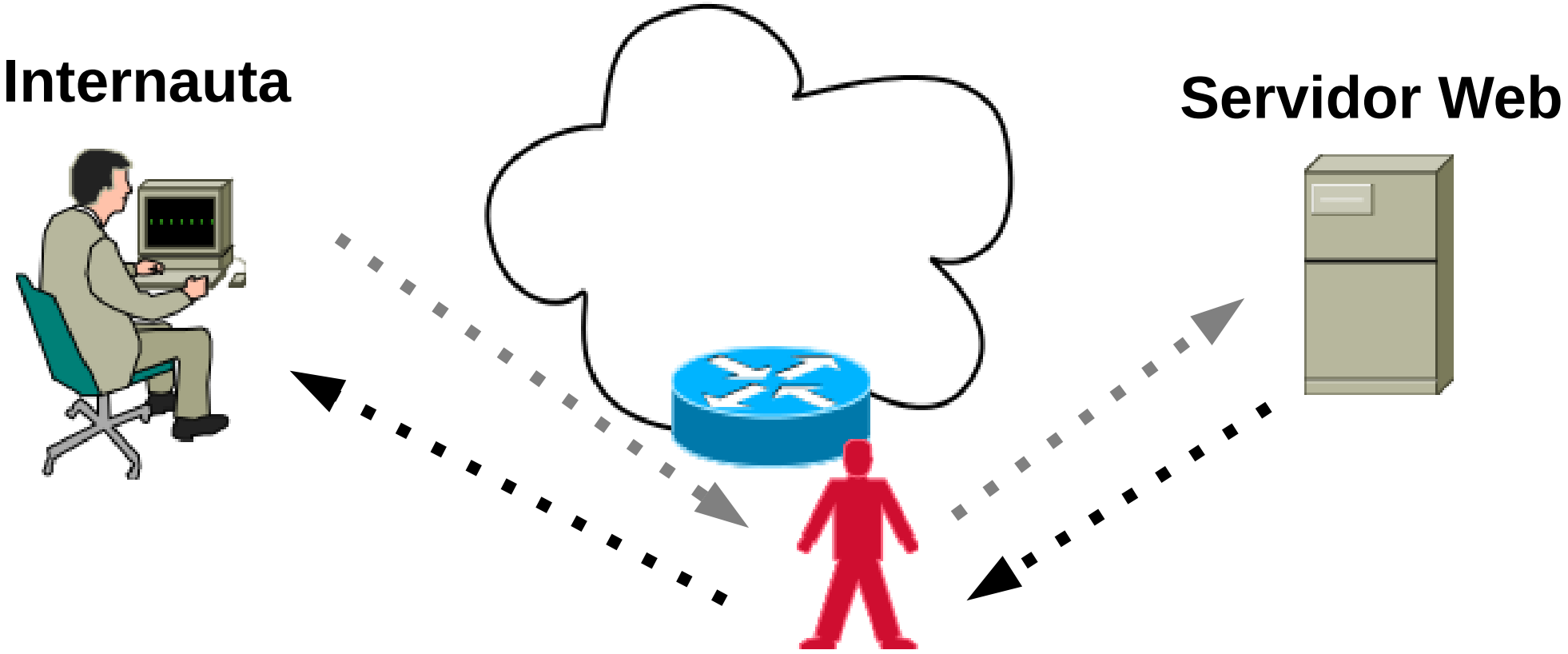
Ataque do Homem Intermediário



Posso ALTERAR o tráfego aberto!

2 – Confiar no Roteamento Provedores?

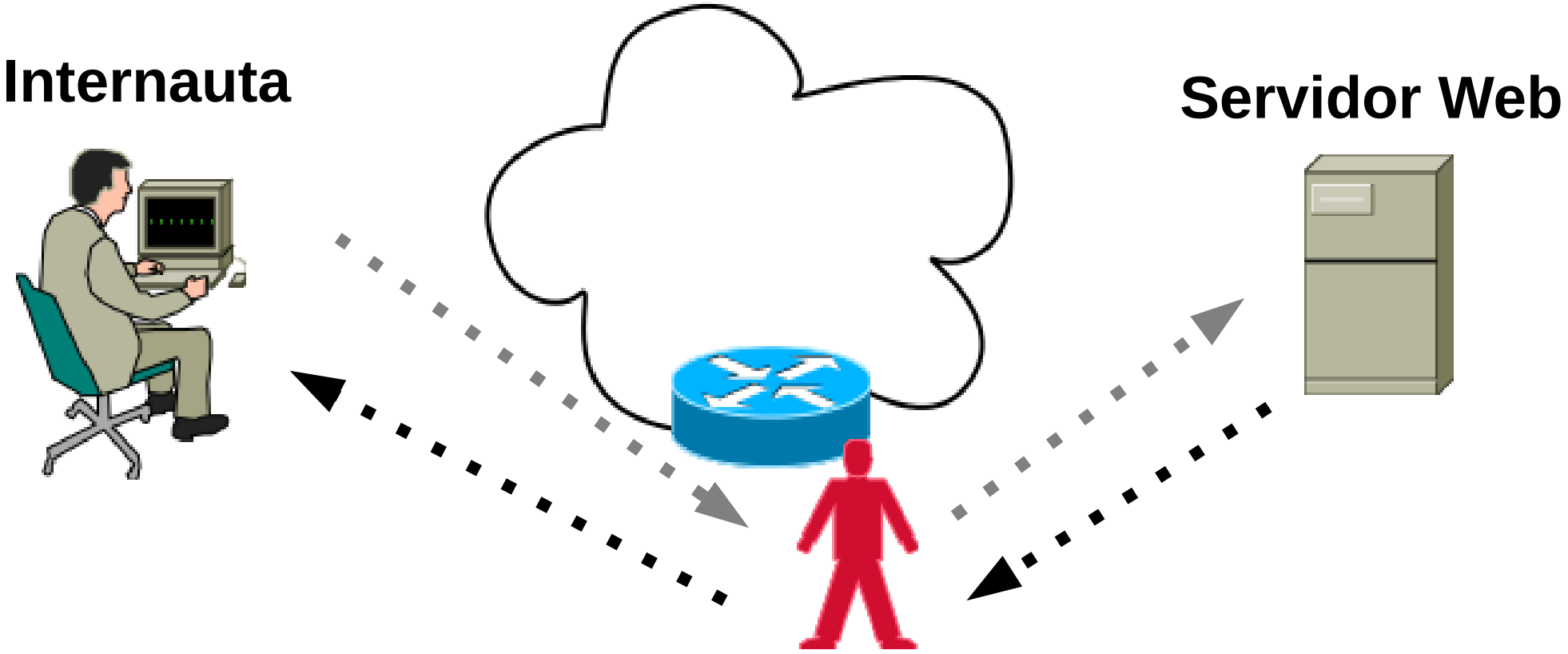
Ataque do Homem Intermediário



Posso ALTERAR o tráfego aberto!

2 – Confiar no Roteamento Provedores?

Ataque do Homem Intermediário

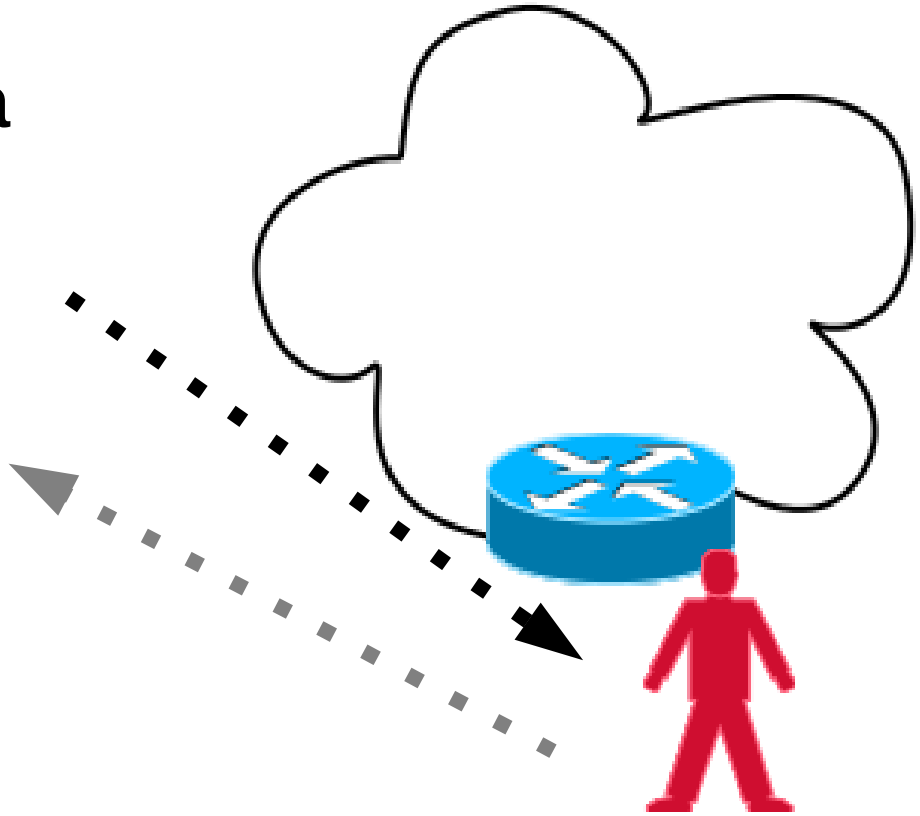


Posso DESVIAR o tráfego!

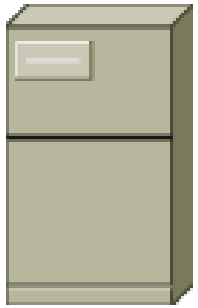
2 – Confiar no Roteamento Provedores?

Ataque do Homem Intermediário

Internauta



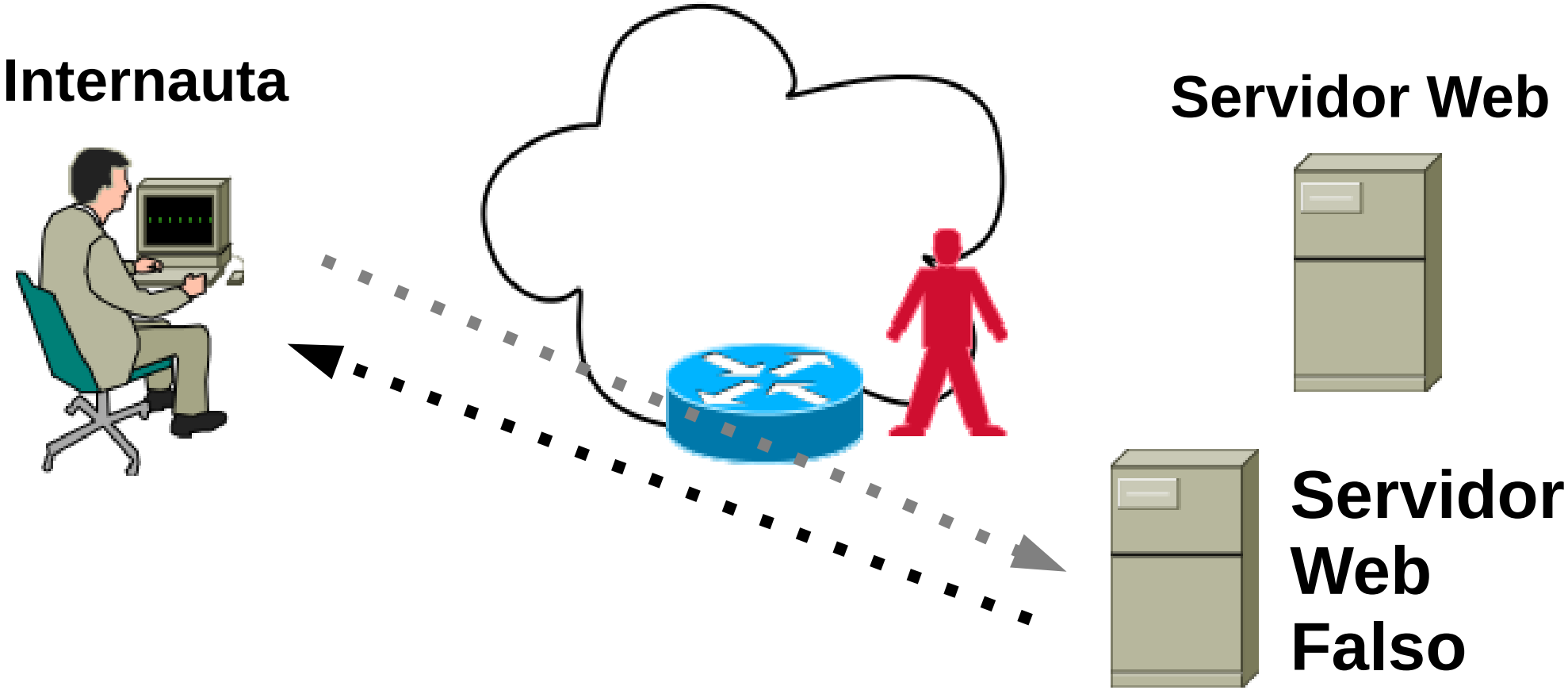
Servidor Web



Posso DESVIAR o tráfego!

2 – Confiar no Roteamento Provedores?

Desvio de rotas!

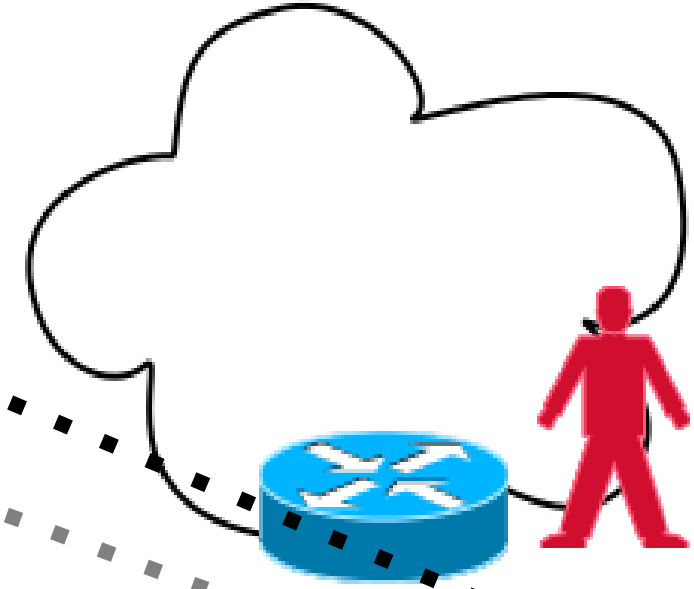


Posso DESVIAR o tráfego!

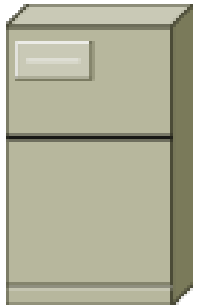
2 – Confiar no Roteamento Provedores?

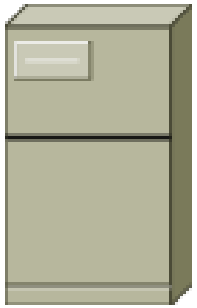
Desvio de rotas!

Internauta



Servidor Web



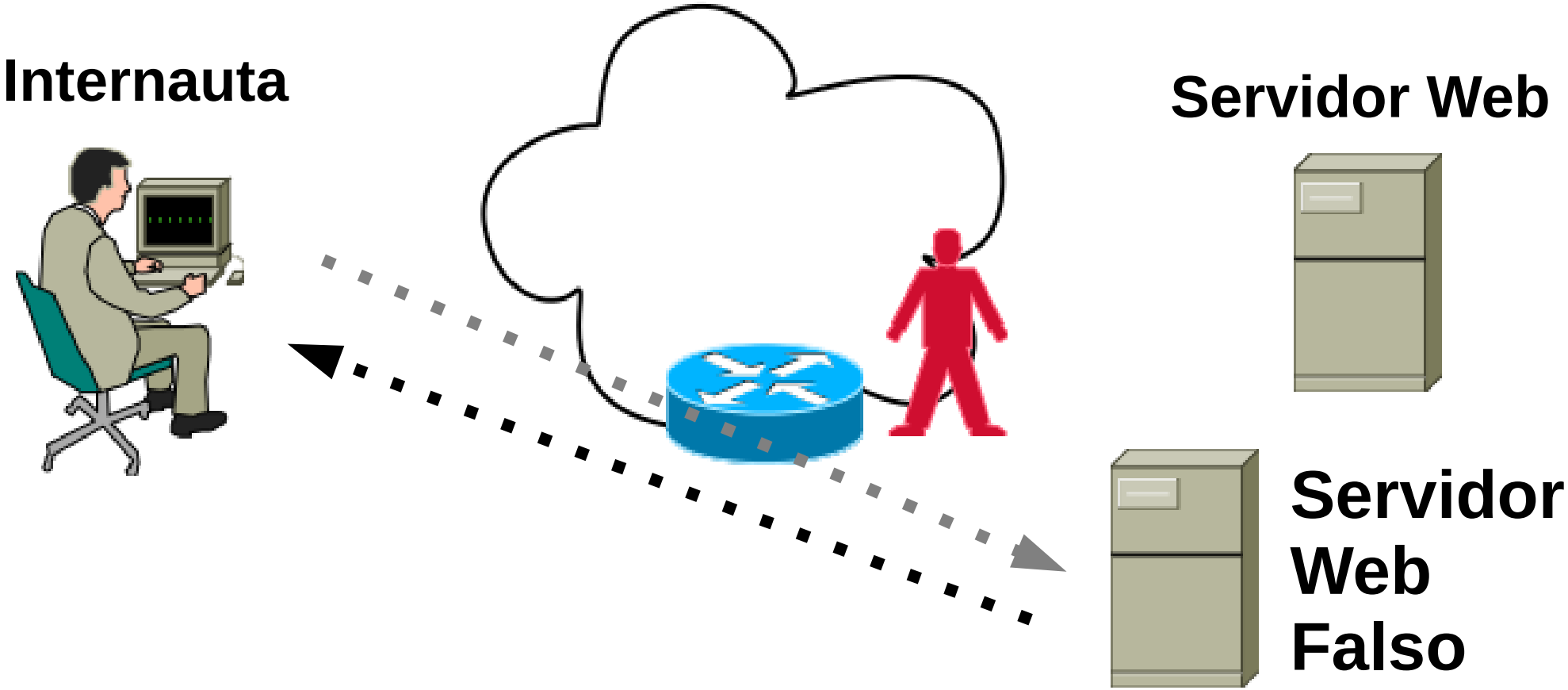


Servidor Web Falso

Posso DESVIAR o tráfego!

2 – Confiar no Roteamento Provedores?

Desvio de rotas!



Posso DESVIAR o tráfego!

2 – Confiar no Roteamento Provedores?

Desvio de rotas!

Internauta

Servidor Web

Servidor Web Falso

DESVIAR o tráfego!

2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

Incidente de Segurança

Renesys identifica rotas estranhas Fev/2013

2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

Incidente de Segurança

Renesys identifica rotas estranhas Fev/2013

Traceroute Path 2: from Denver, CO to Denver, CO via *Iceland*

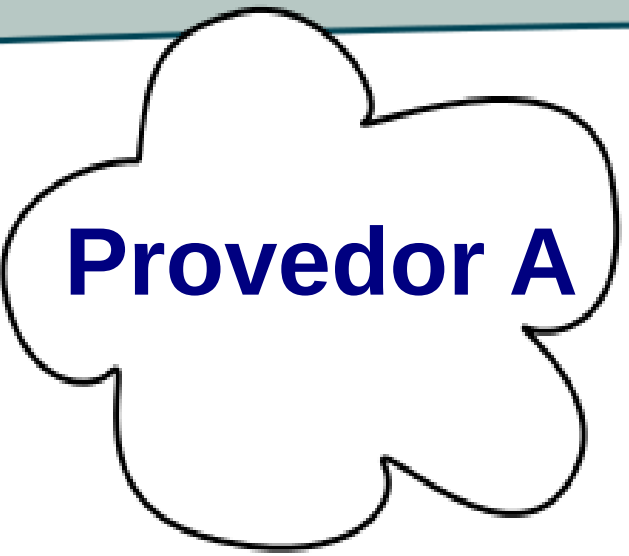
2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

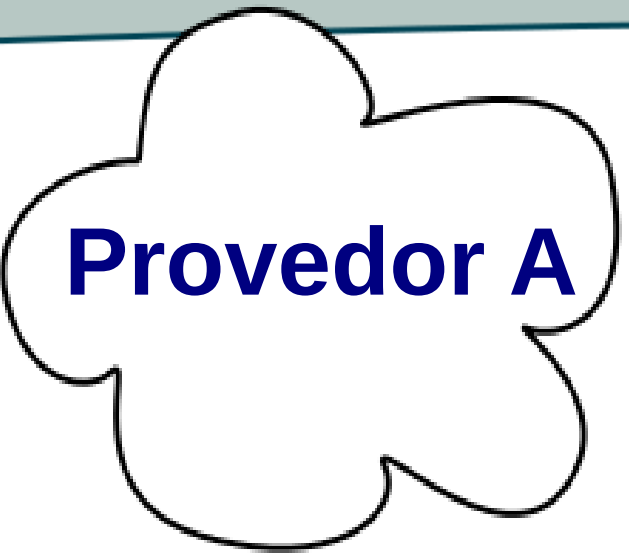
Exemplos de ataques (exploração):

- Sniffing (tráfego aberto)
- Arp Spoofing (rede local)
- Ataque do Homem Intermediário (MITM)
- Desvio de Rotas
- Protocolos de Roteamento?!?

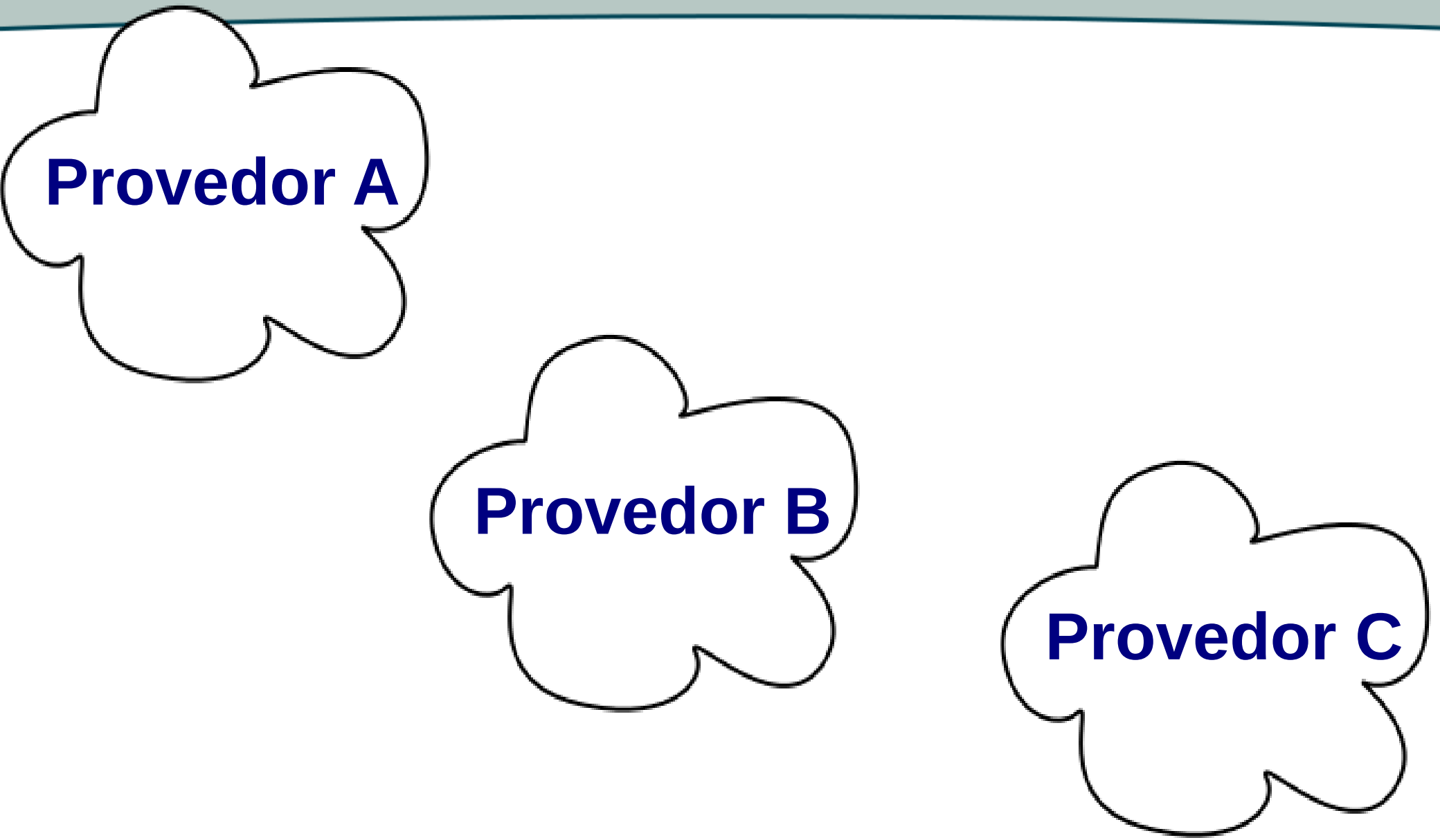
2 – Confiar no Roteamento Provedores?



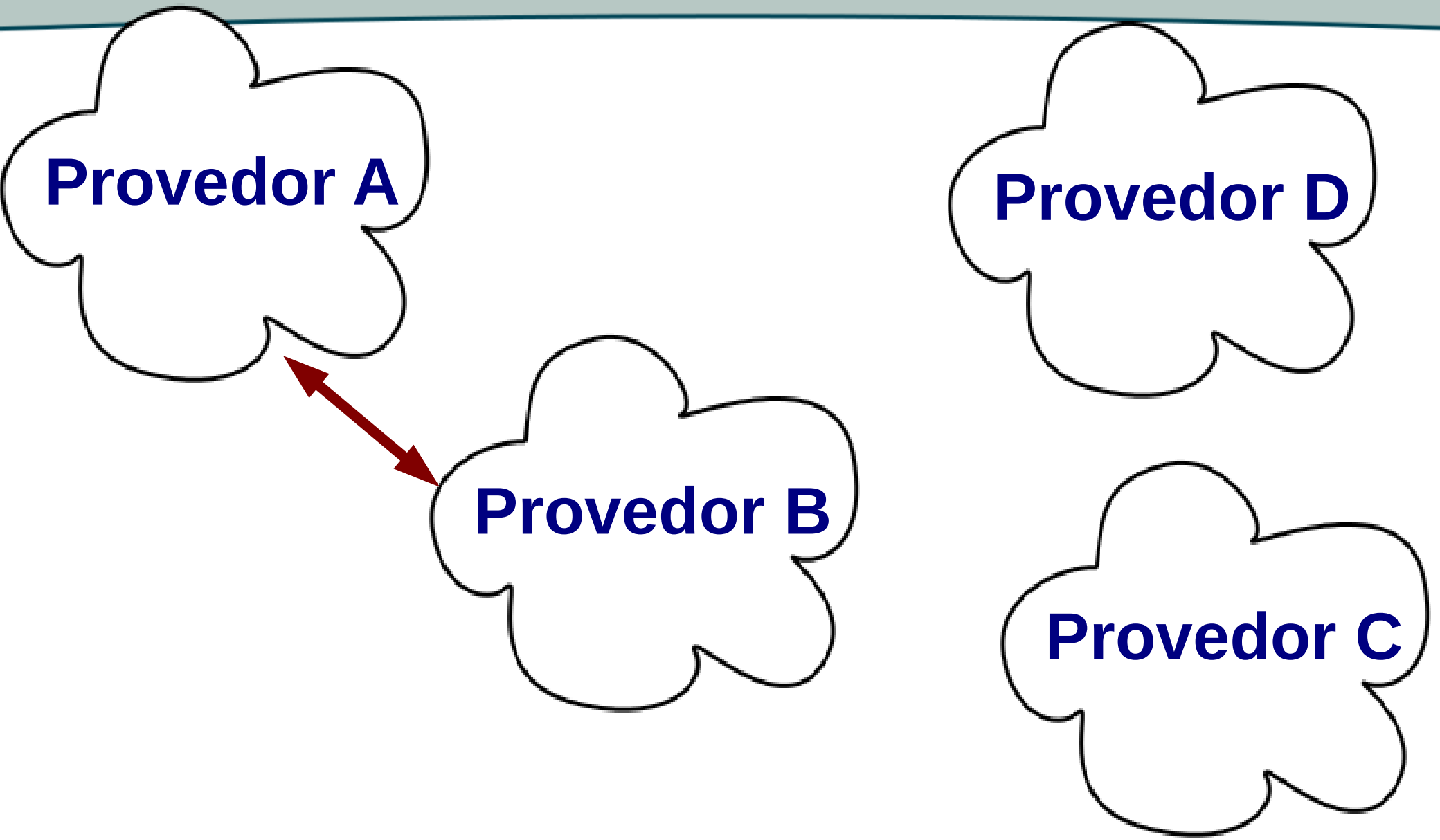
2 – Confiar no Roteamento Provedores?



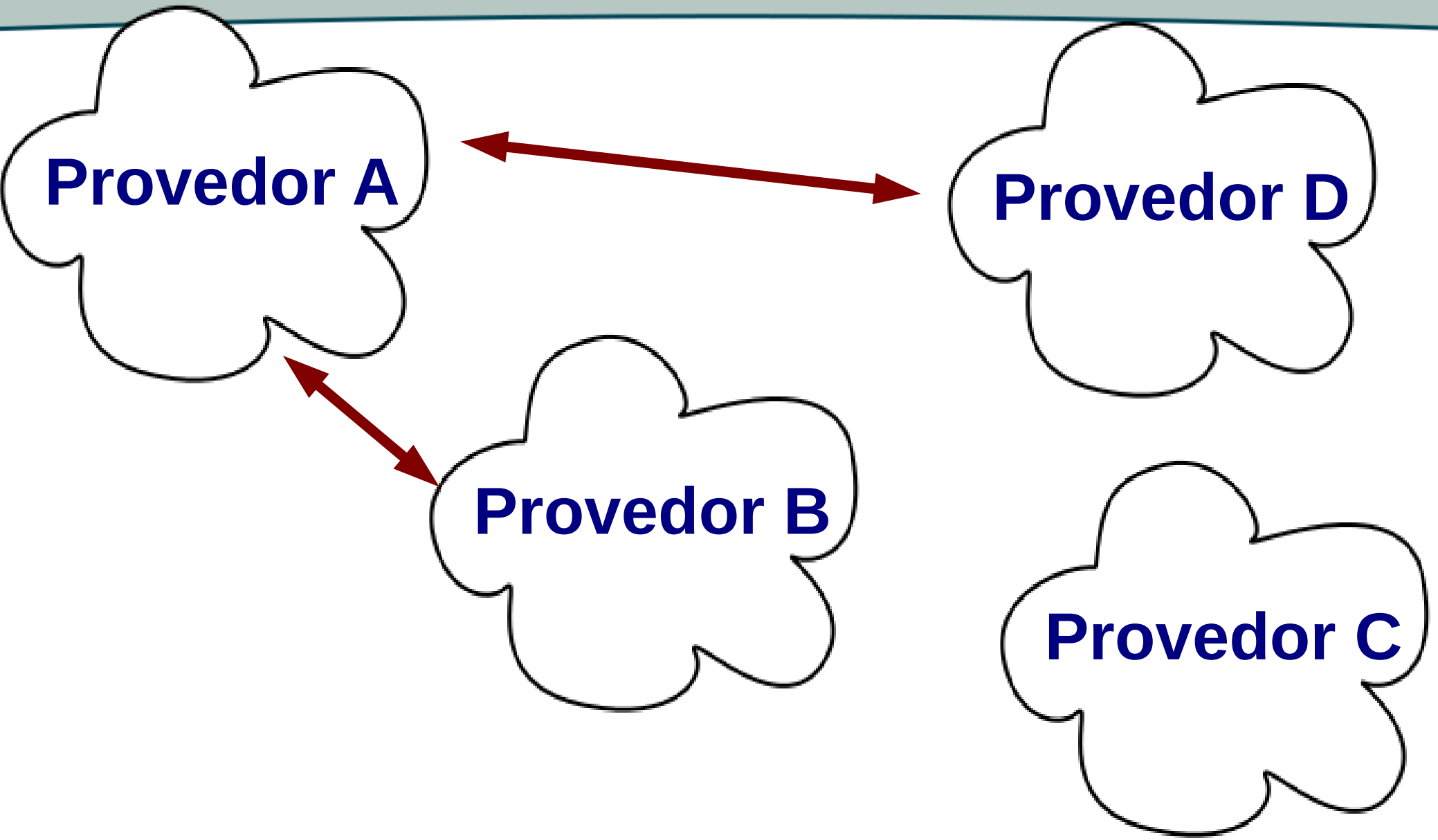
2 – Confiar no Roteamento Provedores?



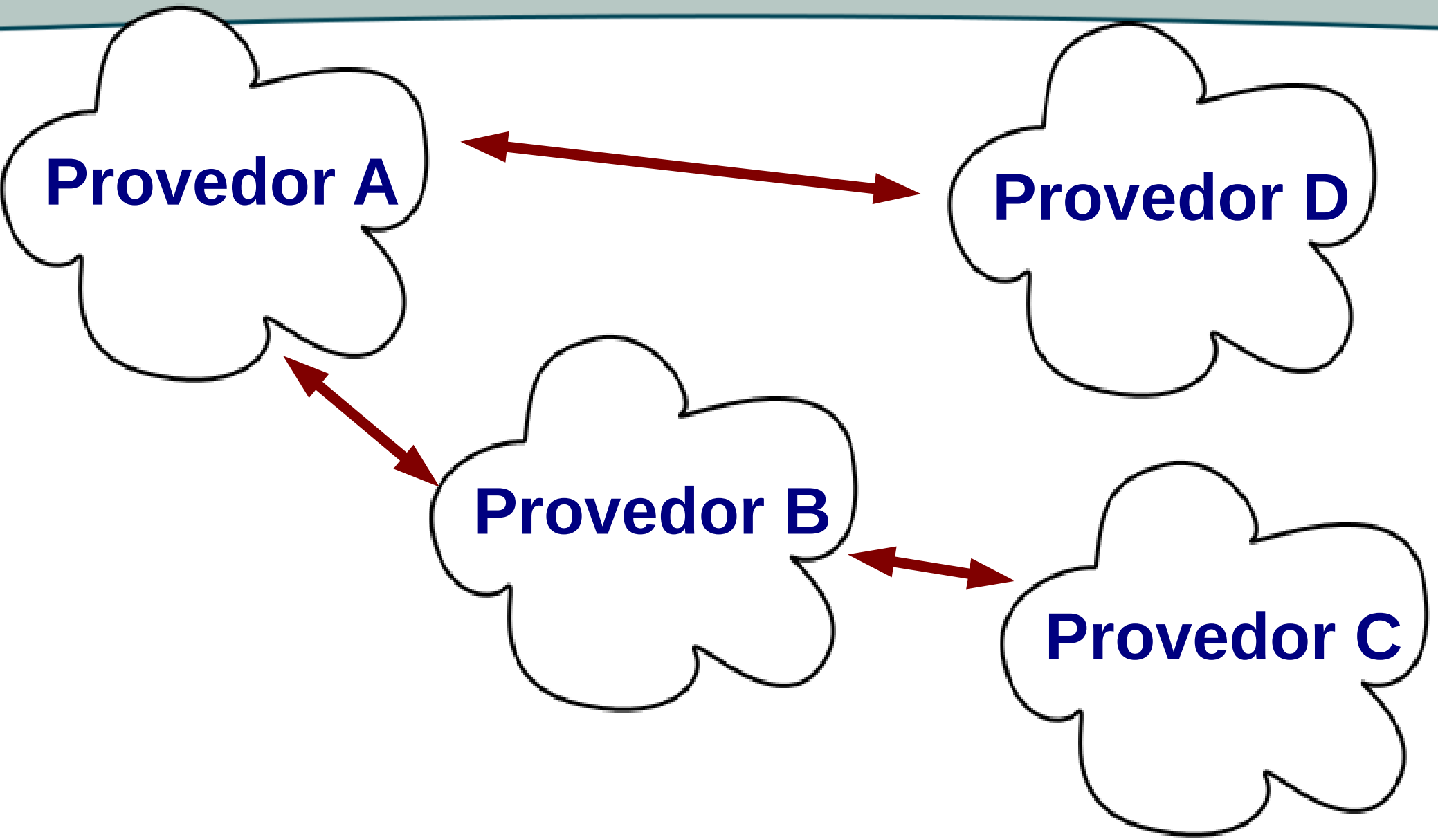
2 – Confiar no Roteamento Provedores?



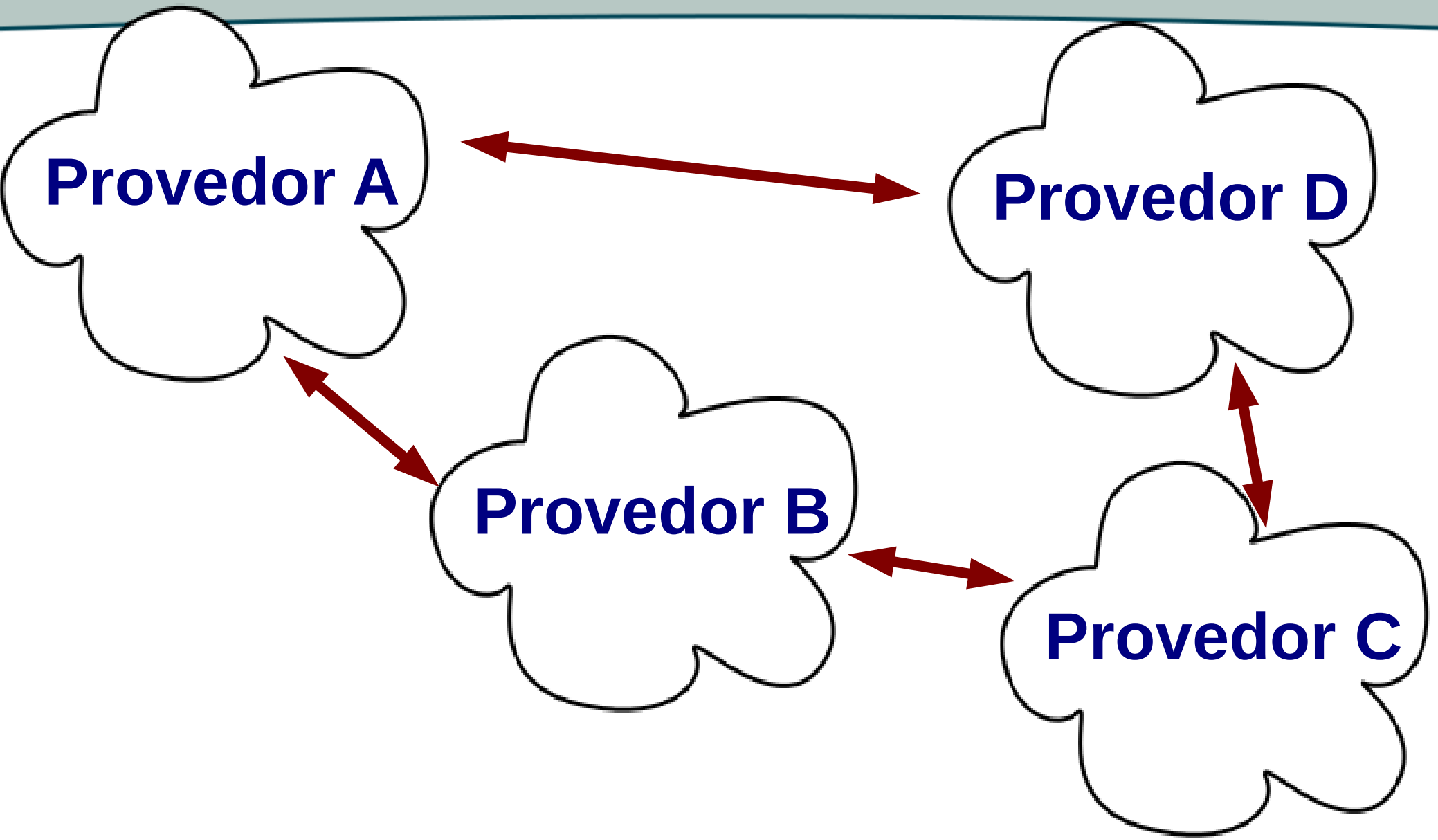
2 – Confiar no Roteamento Provedores?



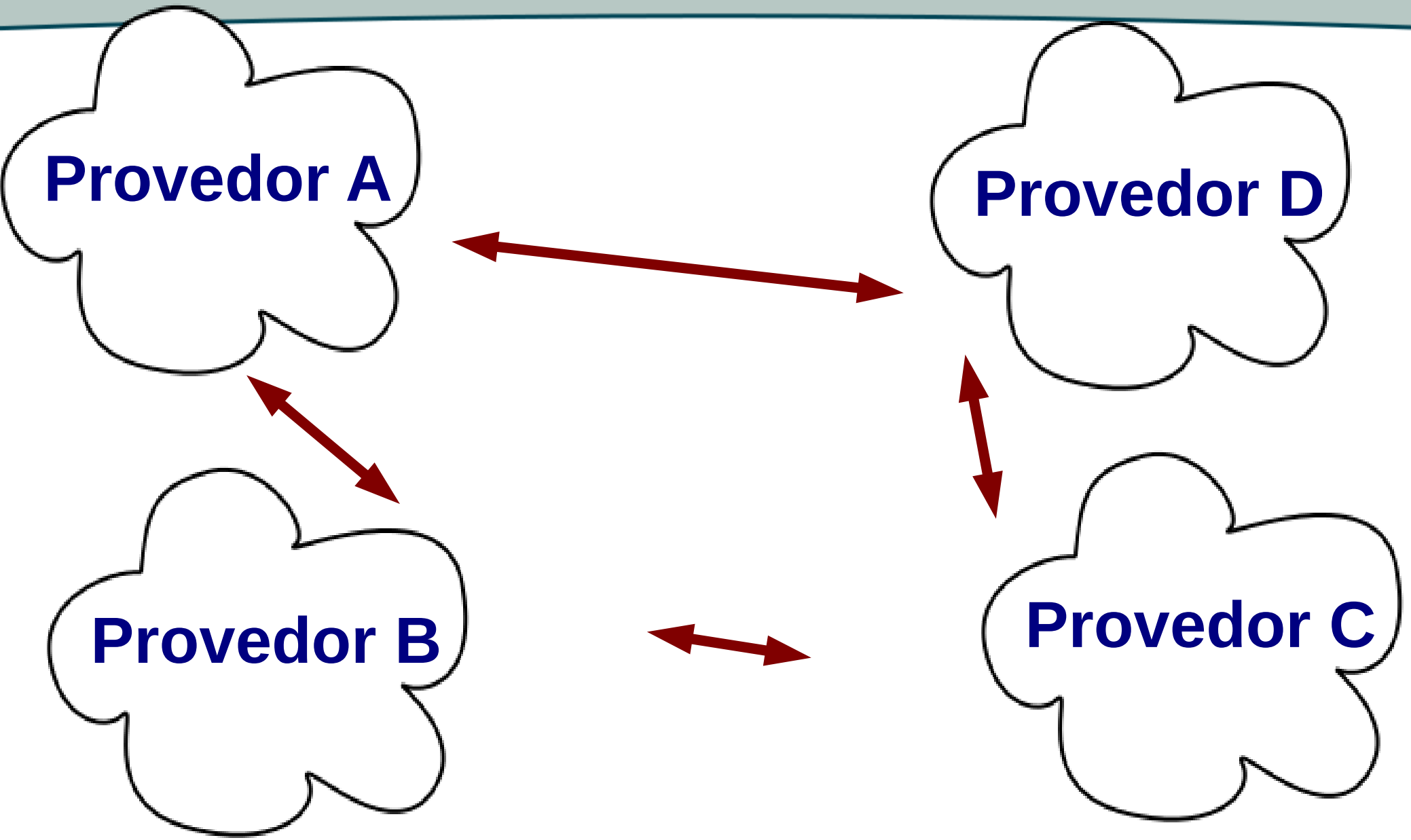
2 – Confiar no Roteamento Provedores?



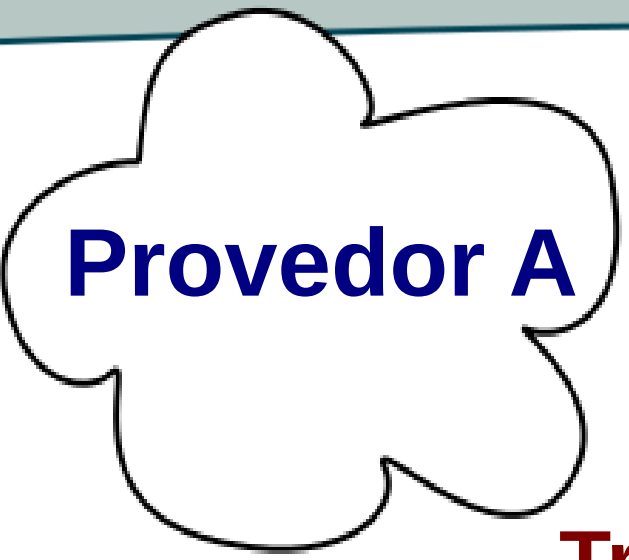
2 – Confiar no Roteamento Provedores?

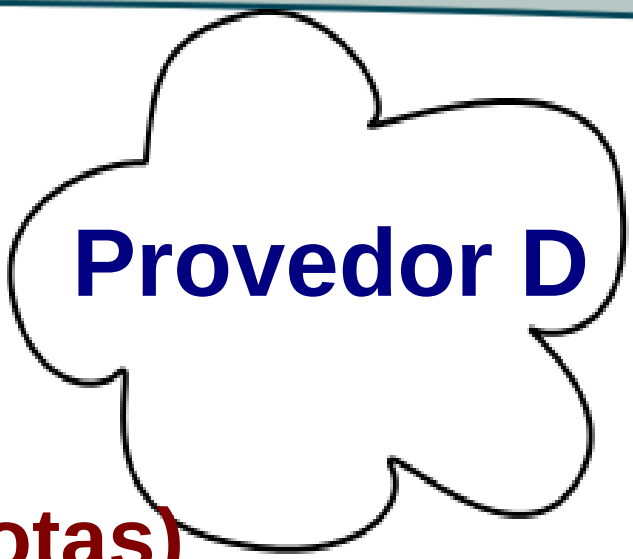


2 – Confiar no Roteamento Provedores?



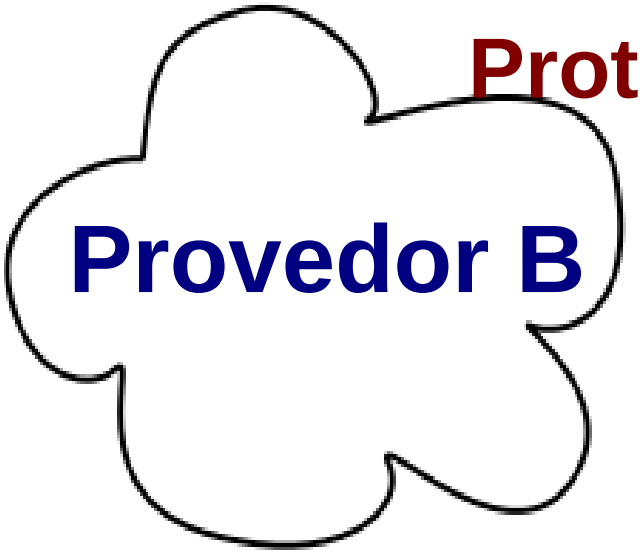
2 – Confiar no Roteamento Provedores?





Trocar Caminhos (rotas)

Protocolo de Roteamento



2 – Confiar no Roteamento Provedores?

Provedor A

Provedor D

PROTOCOLO BGP

RFC 1771 – 1995

Border Gateway Protocol

Provedor B

Provedor C

2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

Sistema Autonomo

Sistema Autonomo

Sistema Autonomo

Sistema Autonomo

2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

Sistema Autonomo

Sistema Autonomo

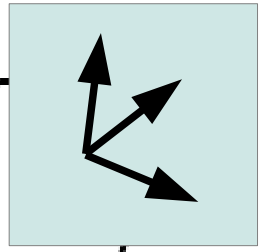
Sistema Autonomo

Sistema Autonomo

2 – Confiar no Roteamento Provedores?

Sistema Autonomo

Sistema Autonomo



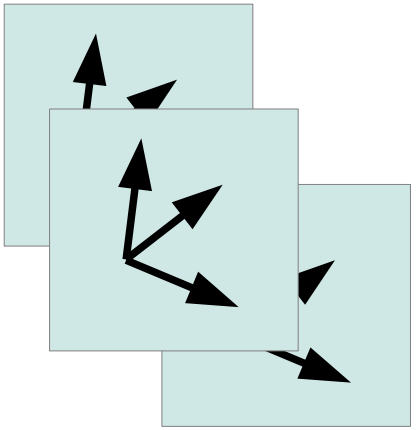
Sistema Autonomo

Sistema Autonomo

2 – Confiar no Roteamento Provedores?

Sistema Autonomo

Sistema Autonomo



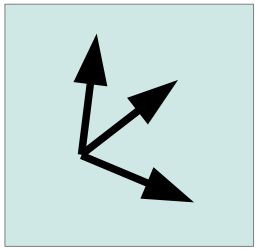
Sistema Autonomo

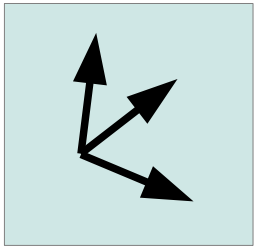
Sistema Autonomo

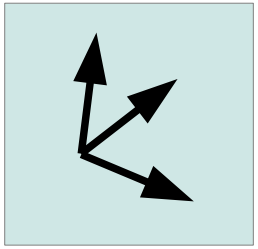
2 – Confiar no Roteamento Provedores?

Sistema Autonomo

Sistema Autonomo



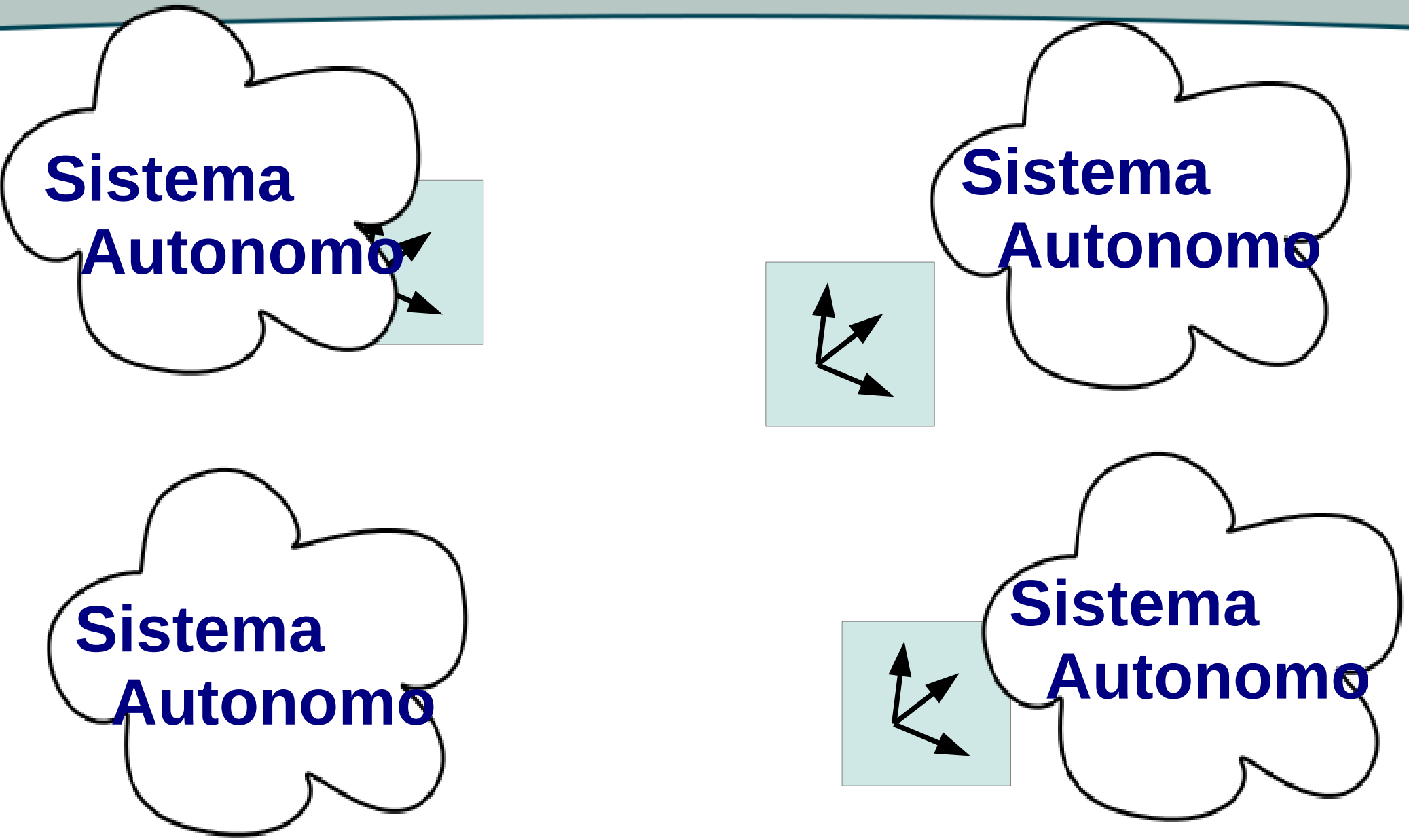




Sistema Autonomo

Sistema Autonomo

2 – Confiar no Roteamento Provedores?

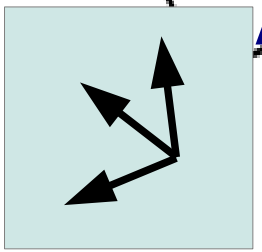


2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

Sistema Autonomo

Sistema Autonomo



Sistema Autonomo

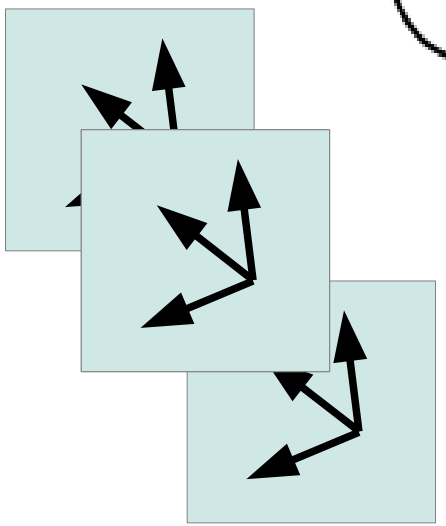
Sistema Autonomo

2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

Sistema Autonomo

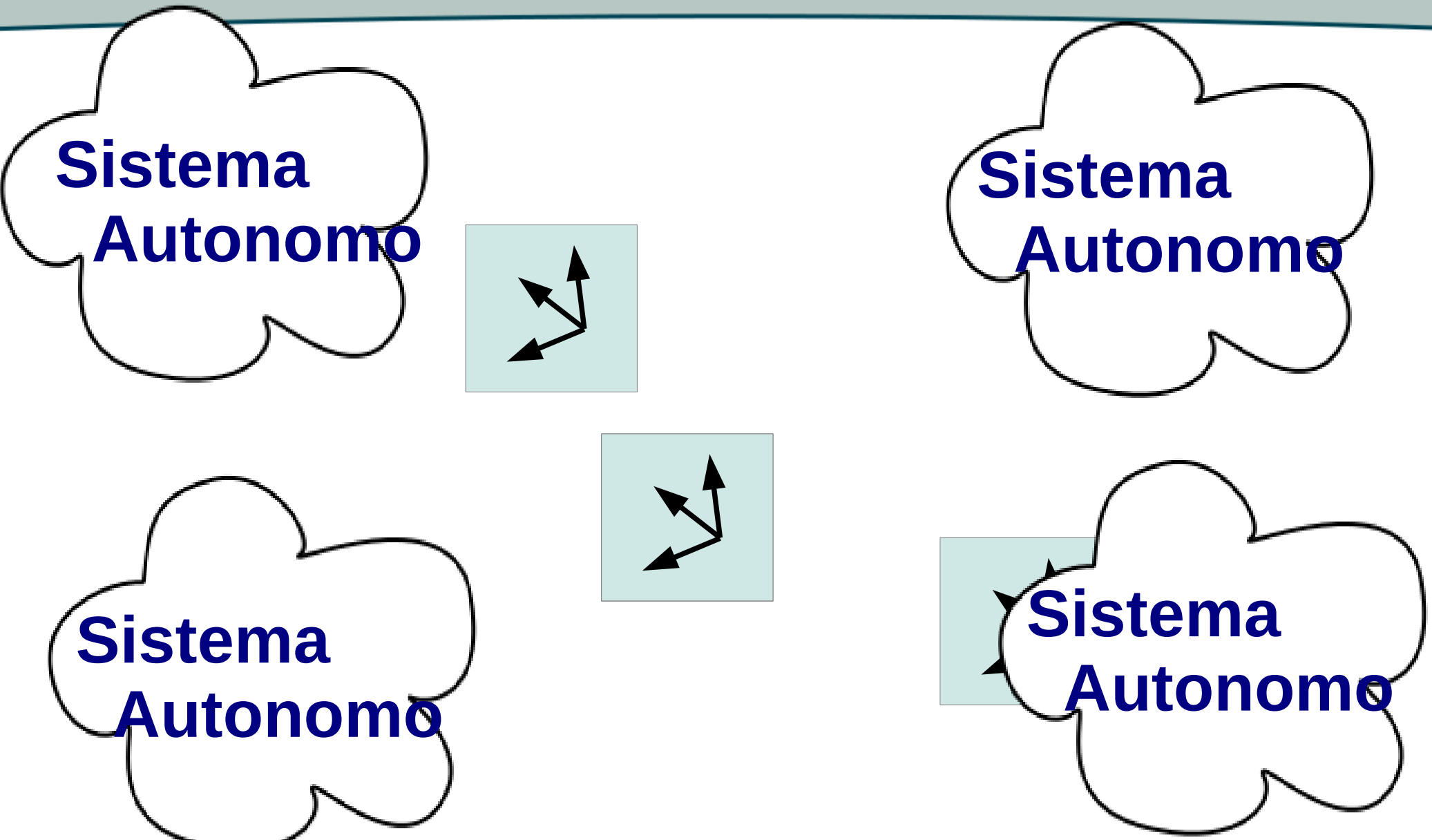
Sistema Autonomo



Sistema Autonomo

Sistema Autonomo

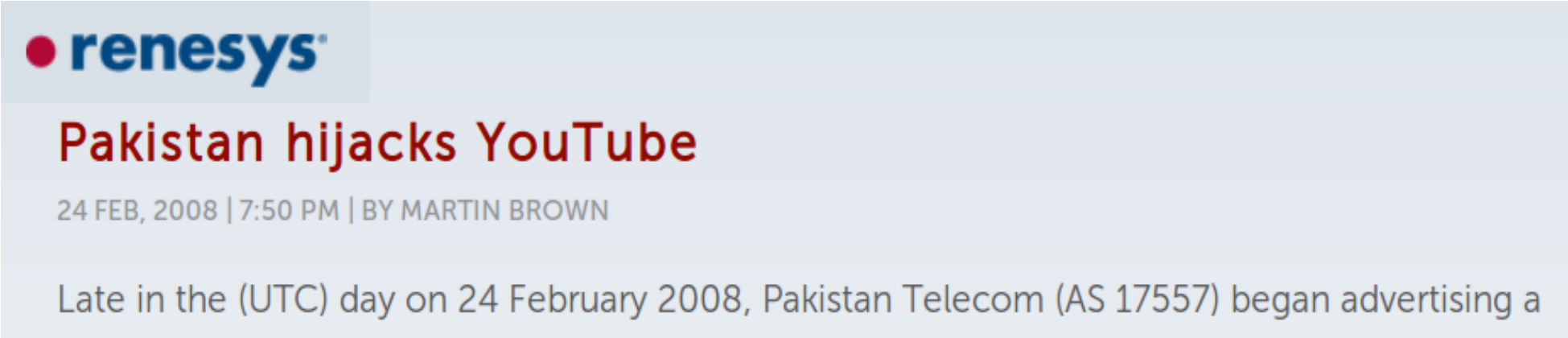
2 – Confiar no Roteamento Provedores?



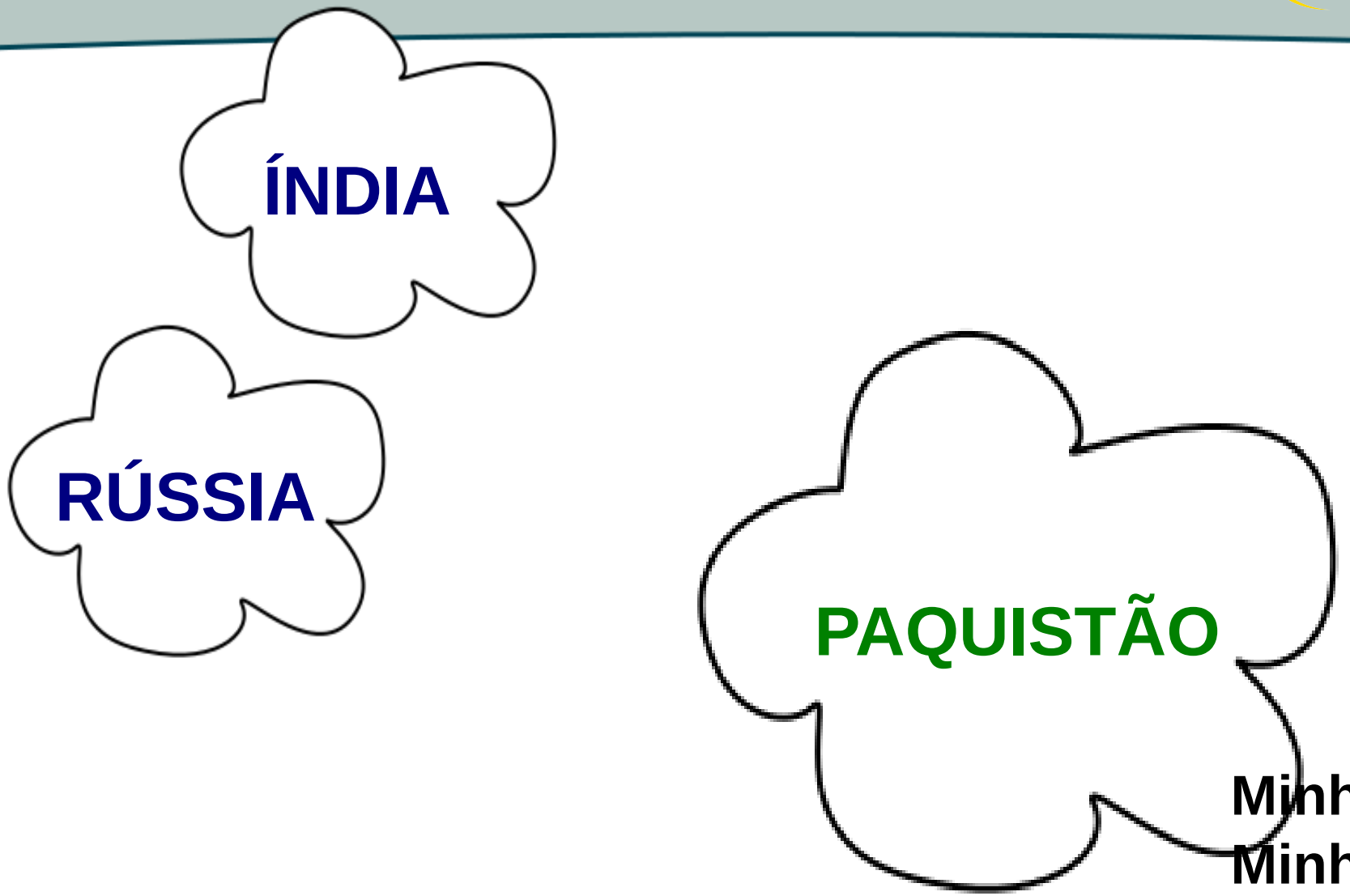
2 – Confiar no Roteamento Provedores?

INCIDENTE DE SEGURANÇA

Em 2008 provedor paquistanês
divulga rede do Youtube!



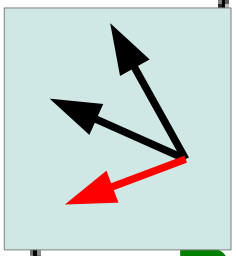
2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?

ÍNDIA

RÚSSIA



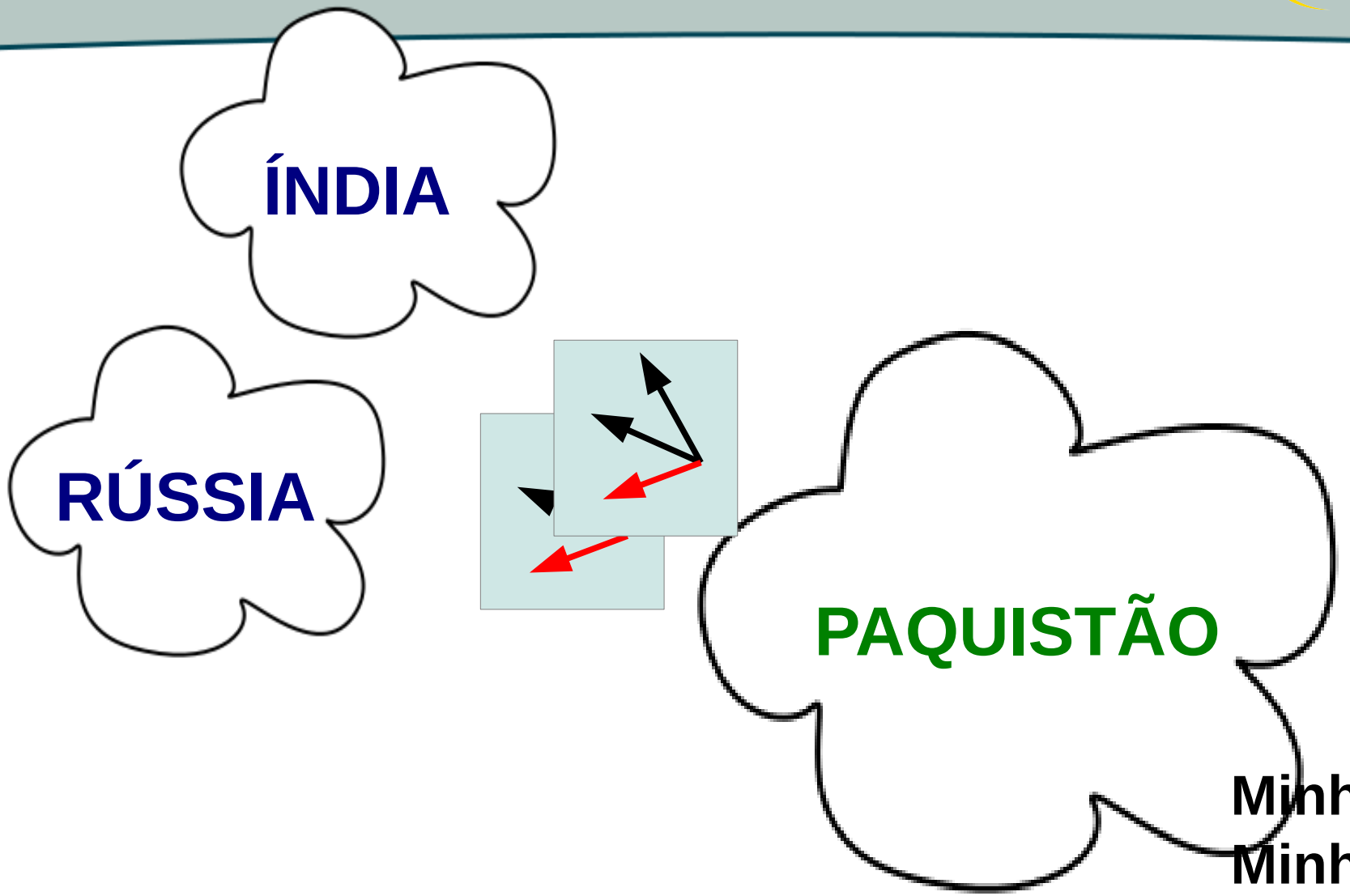
PAQUISTÃO

Minha rede A

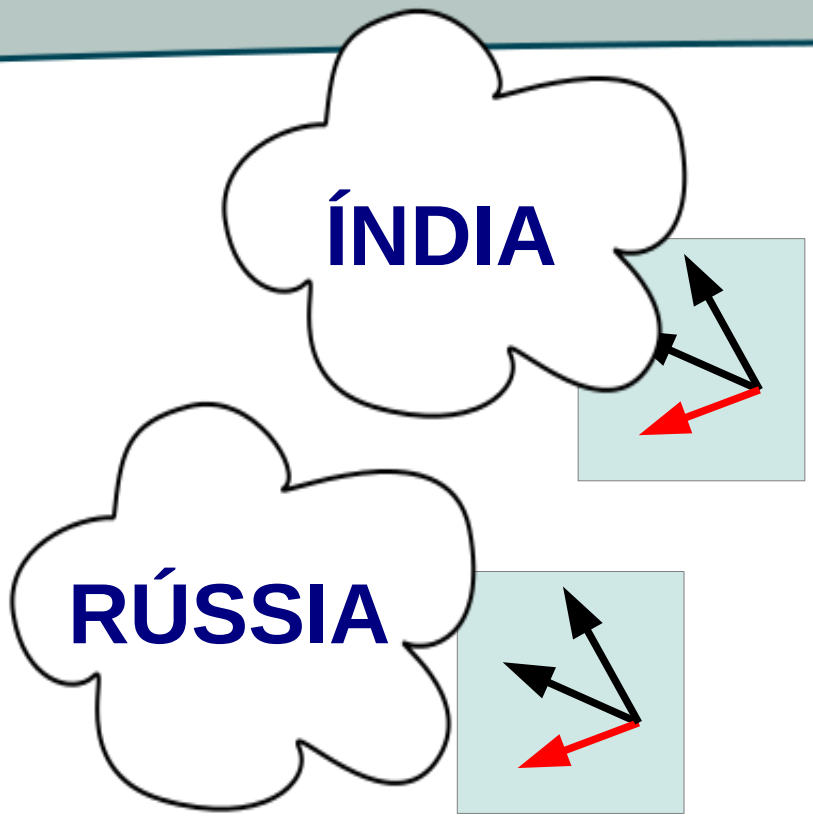
Minha rede B

Minha rede Y (youtube)

2 – Confiar no Roteamento Provedores?



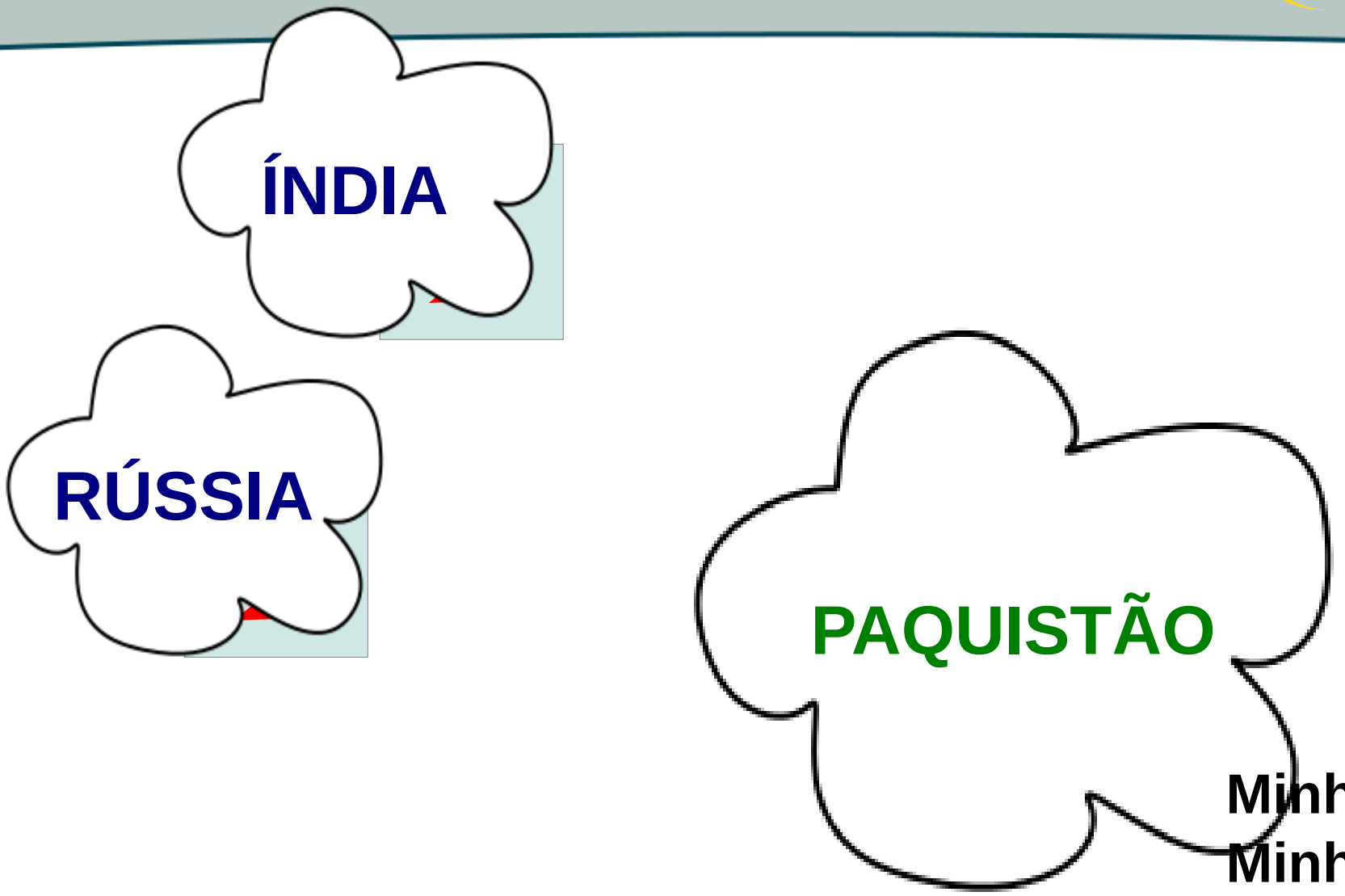
2 – Confiar no Roteamento Provedores?



PAQUISTÃO

Minha rede A
Minha rede B
Minha rede Y (youtube)

2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?

ÍNDIA

RÚSSIA

PAQUISTÃO

www.youtube.com
IP 208....

Minha rede A
Minha rede B
Minha rede Y (youtube)

2 – Confiar no Roteamento Provedores?

ÍNDIA

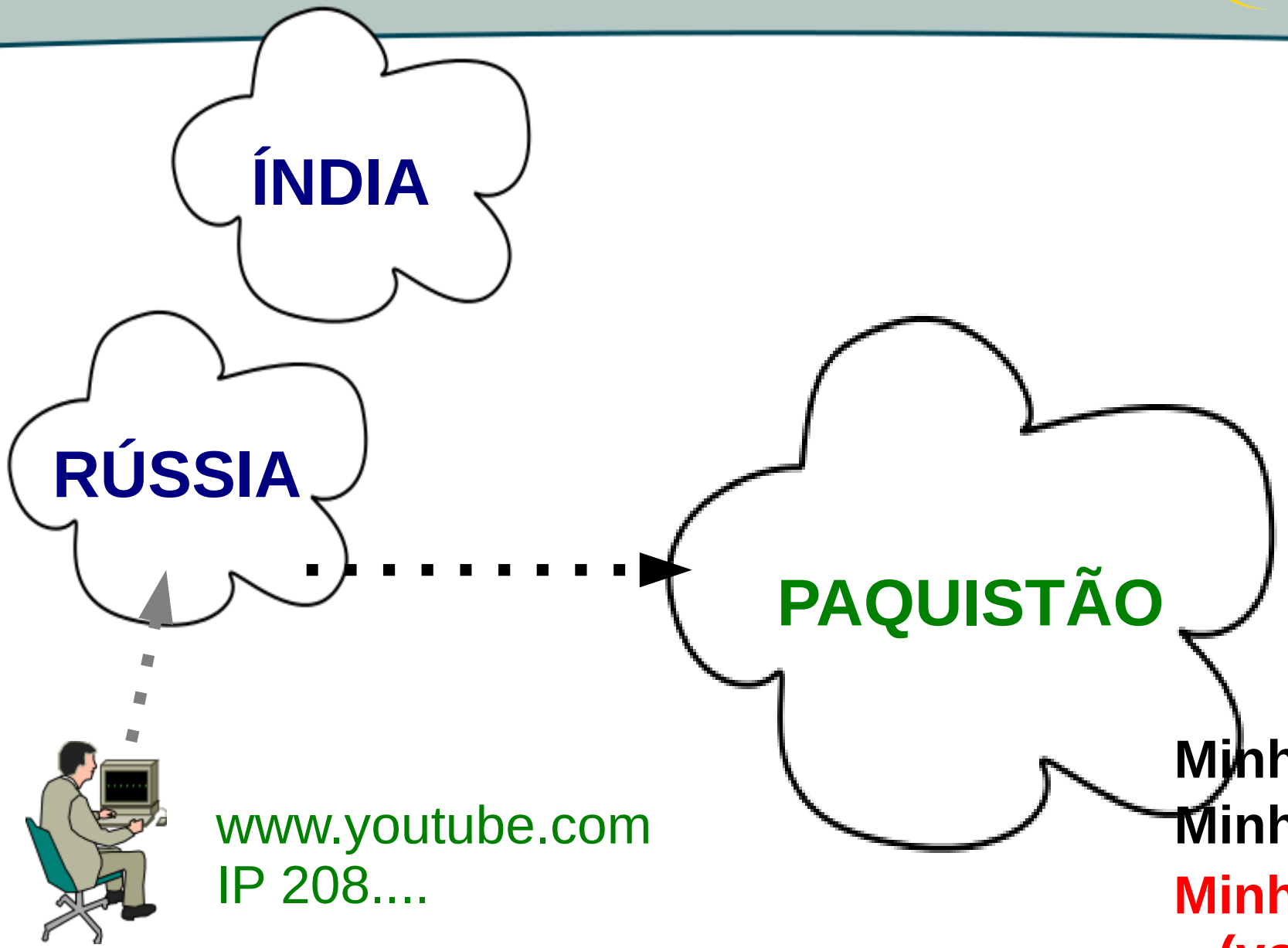
RÚSSIA

PAQUISTÃO

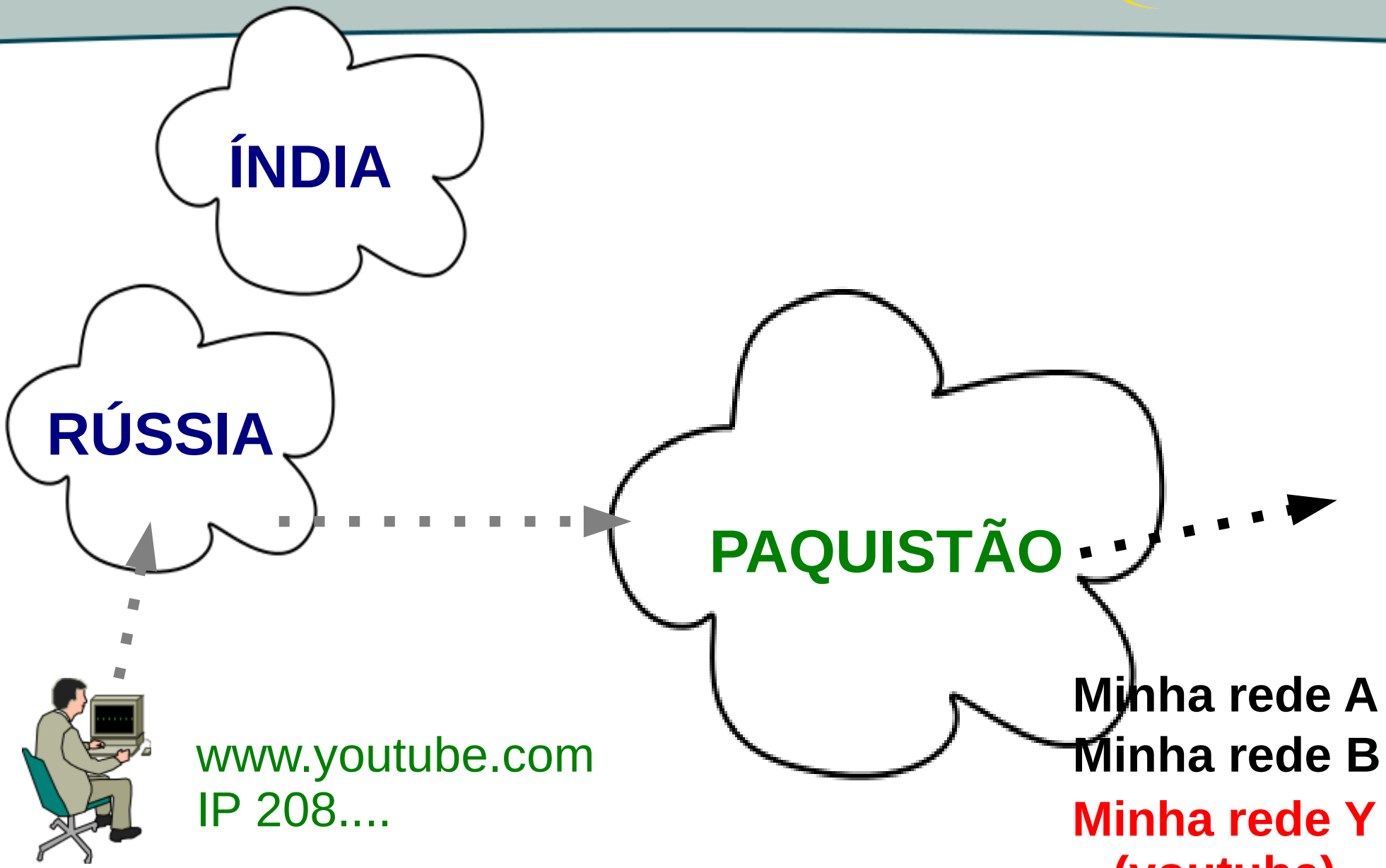
www.youtube.com
IP 208....

Minha rede A
Minha rede B
Minha rede Y (youtube)

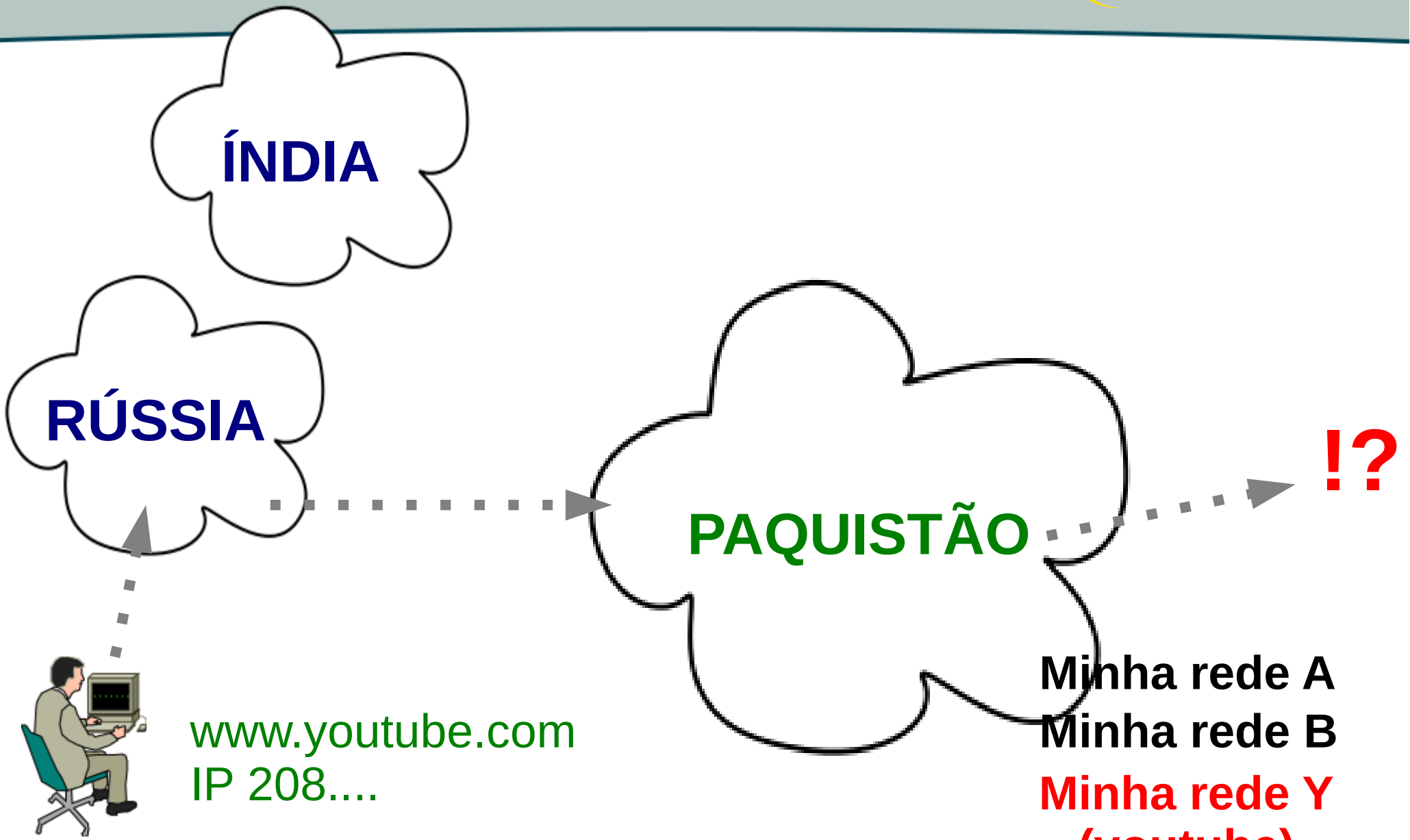
2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?

INCIDENTE DE SEGURANÇA

Em 2008 provedor paquistanês
divulga rede do Youtube!

Em abril de 2010 provedor chinês
diversas redes sequestradas,
Ex: dell.com, cnn.com …


FRIDAY, APRIL 9, 2010

Chinese ISP hijacks the Internet

"This morning many BGPmon.net users received an alert

2 – Confiar no Roteamento Provedores?

CELEPAR INFORMÁTICA do PARANÁ

MAIS INCIDENTES

Google x Venezuela – Mar/2014

Google x Turquia
Mar/2014

2 – Confiar no Roteamento Provedores?

SOLUÇÃO

- Boas práticas
- Recursos BGP (filtros, cripto)
- Acerto entre ASs
- Basta ?!

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

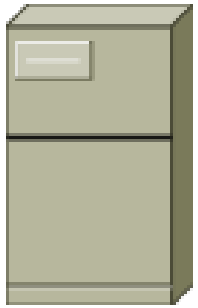
3 -

Podemos confiar em Autoridades Certificadoras?

3 – Confiar Autoridades Certificadoras?

Internauta

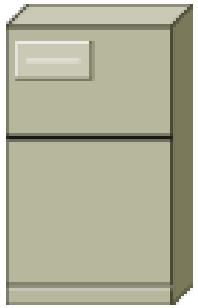
Servidor Web



3 – Confiar Autoridades Certificadoras?

Internauta

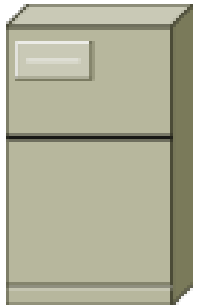
Servidor Web



3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



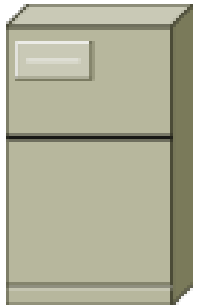
HTTP

Texto Aberto

3 – Confiar Autoridades Certificadoras?

Internauta

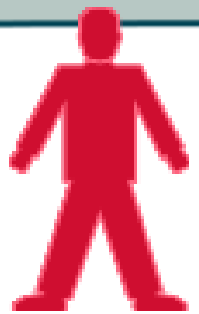
Servidor Web



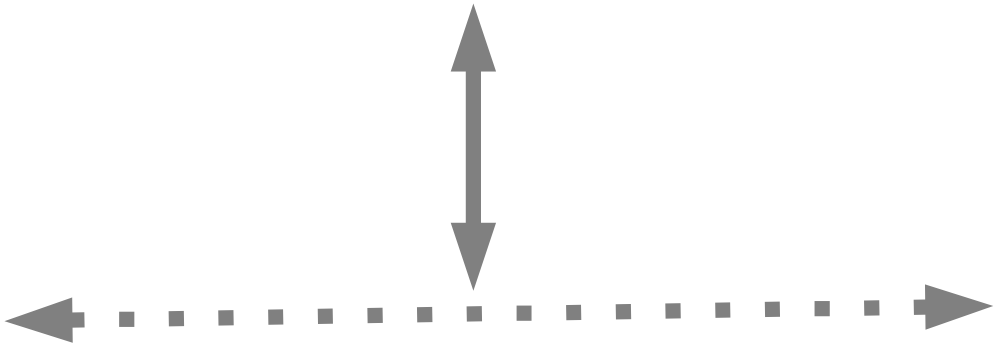
HTTP

Texto Aberto

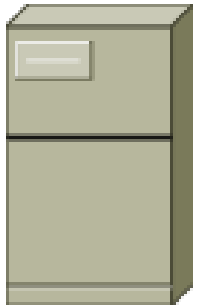
3 – Confiar Autoridades Certificadoras?



Internauta



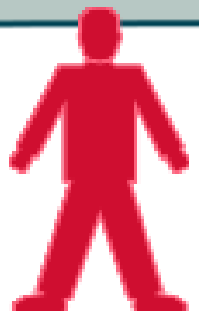
Servidor Web



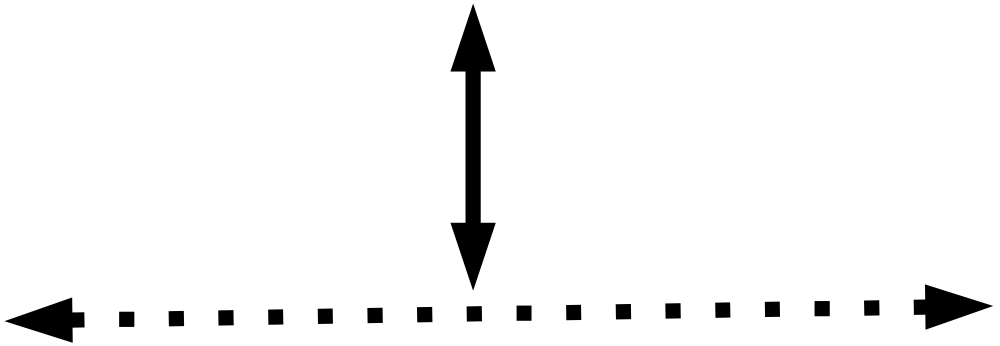
HTTP

Texto Aberto

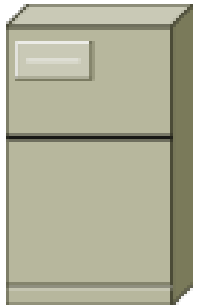
3 – Confiar Autoridades Certificadoras?



Internauta



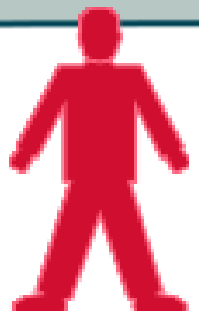
Servidor Web



HTTP

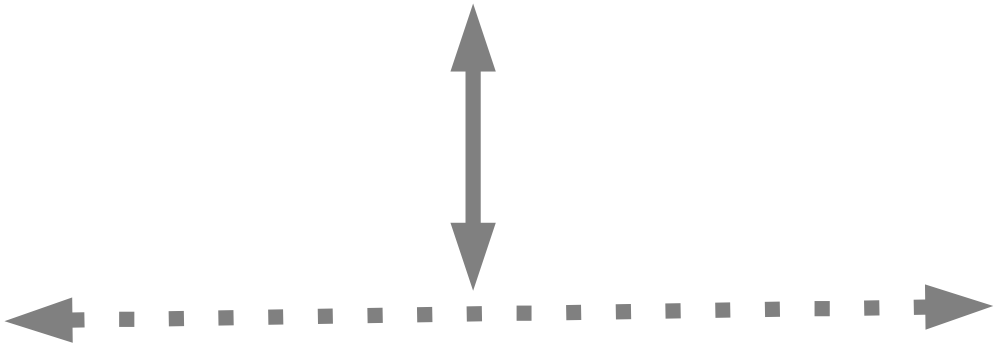
Texto Aberto

3 – Confiar Autoridades Certificadoras?

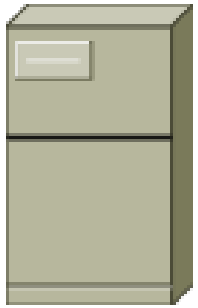


Posso ver o tráfego!

Internauta



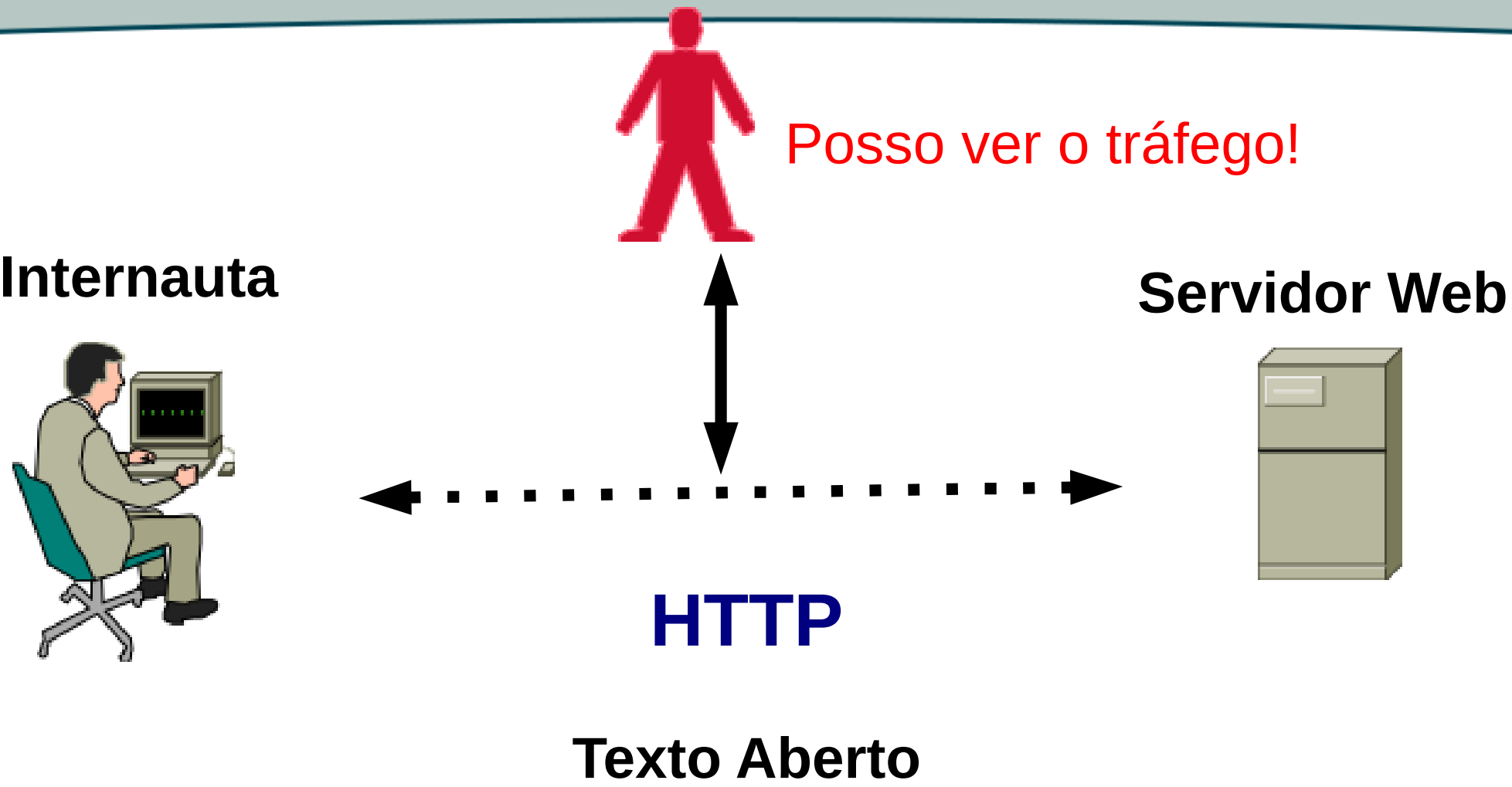
Servidor Web



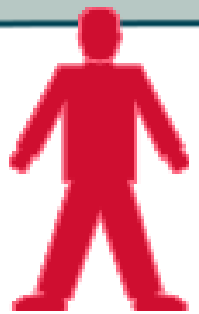
HTTP

Texto Aberto

3 – Confiar Autoridades Certificadoras?

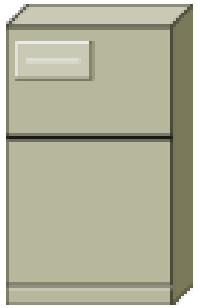


3 – Confiar Autoridades Certificadoras?



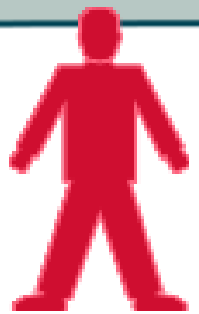
Internauta

Servidor Web

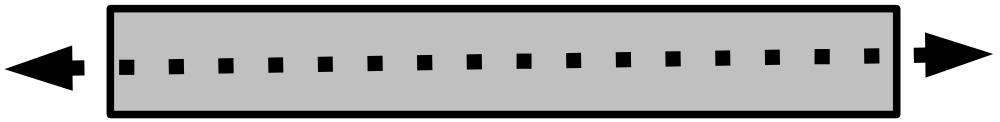


CRIPTOGRAFIA

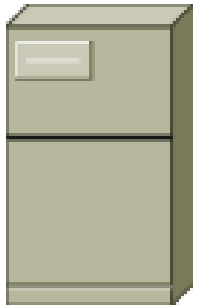
3 – Confiar Autoridades Certificadoras?



Internauta



Servidor Web

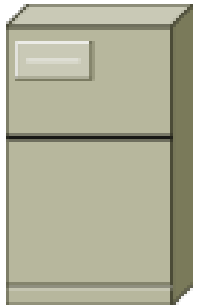


CRIPTOGRAFIA

3 – Confiar Autoridades Certificadoras?

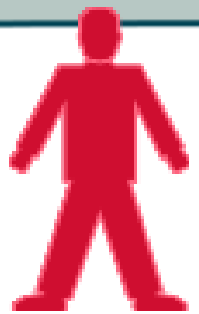
Internauta

Servidor Web



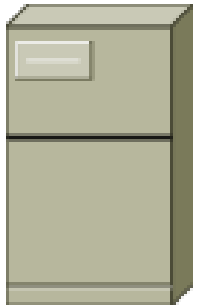
CRIPTOGRAFIA

3 – Confiar Autoridades Certificadoras?



Internauta

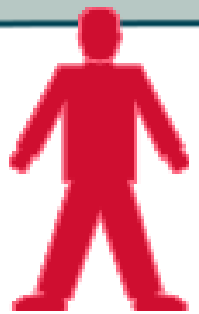
Servidor Web



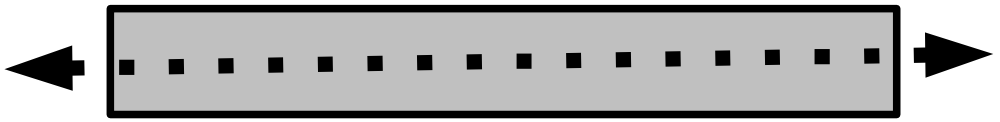
CRIPTOGRAFIA

Chave Secreta

3 – Confiar Autoridades Certificadoras?

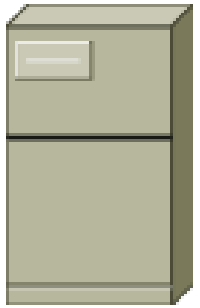


Internauta



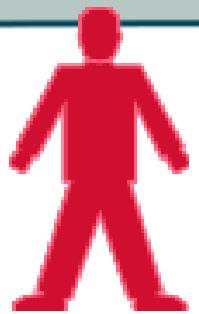
CRIPTOGRAFIA

Servidor Web



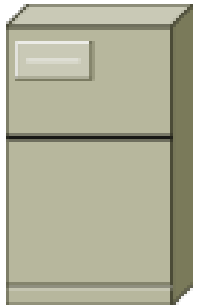
Chave Secreta
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web

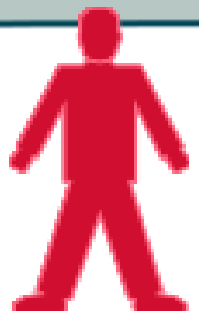


CRIPTOGRAFIA

K

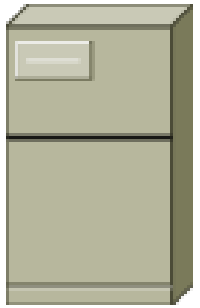
Chave Secreta
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



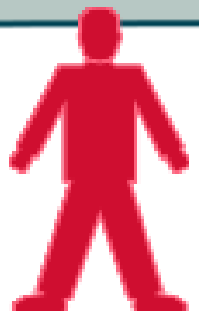
CRIPTOGRAFIA

K K

Chave Secreta

Dados Criptografados

3 – Confiar Autoridades Certificadoras?



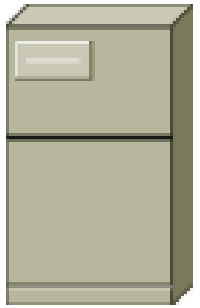
Internauta

K

K

CRIPTOGRAFIA

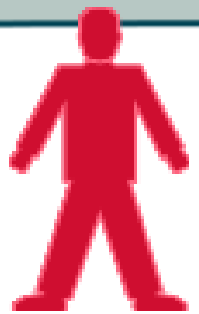
Servidor Web



Chave Secreta

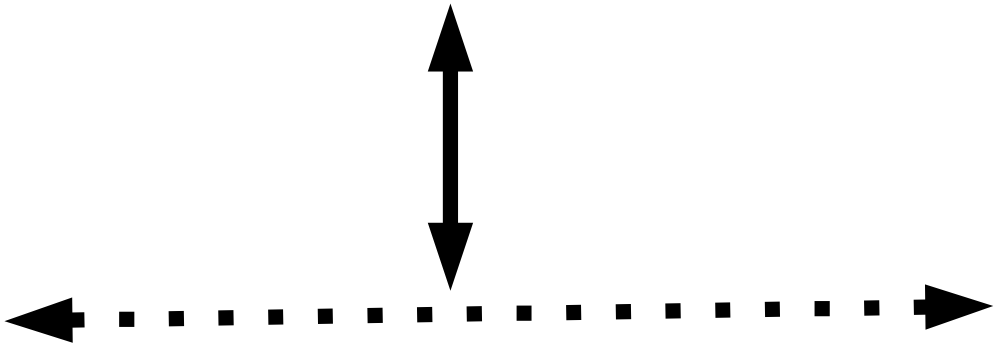
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

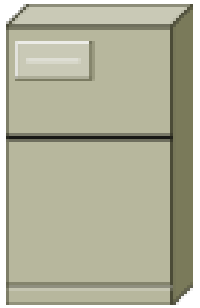
K



K

CRIPTOGRAFIA

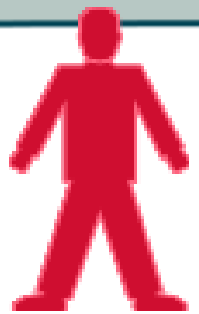
Servidor Web



Chave Secreta

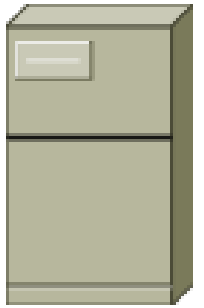
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



K

K

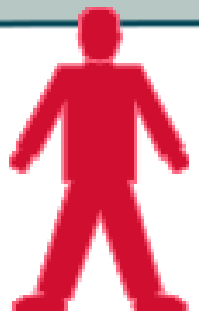
K

CRIPTOGRAFIA

Chave Secreta

Dados Criptografados

3 – Confiar Autoridades Certificadoras?

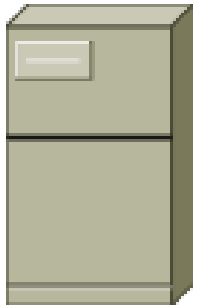


K

Internauta

K

Servidor Web



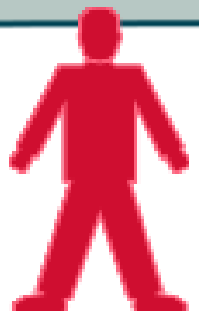
CRIPTOGRAFIA

K

Chave Secreta

Dados Criptografados

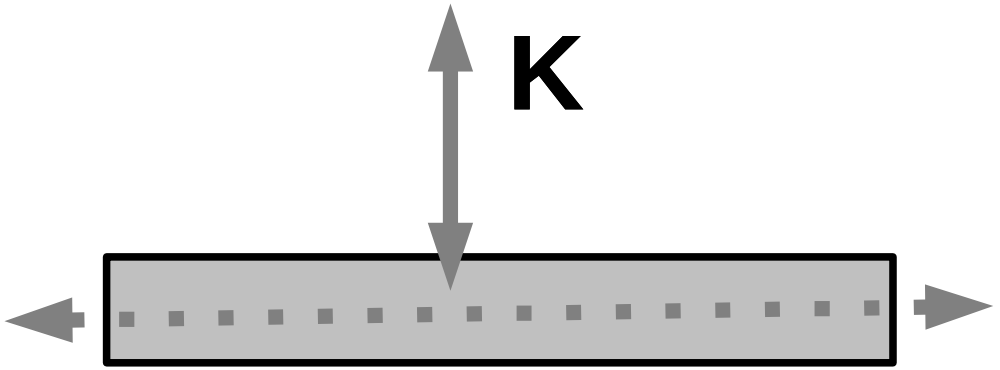
3 – Confiar Autoridades Certificadoras?



Posso ver o tráfego!

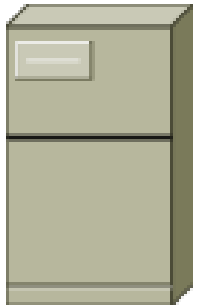
Internauta

K



CRIPTOGRAFIA

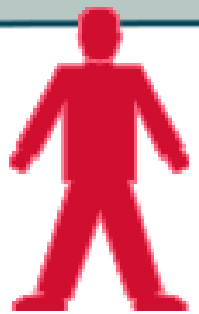
Servidor Web



K

Chave Secreta
Dados Criptografados

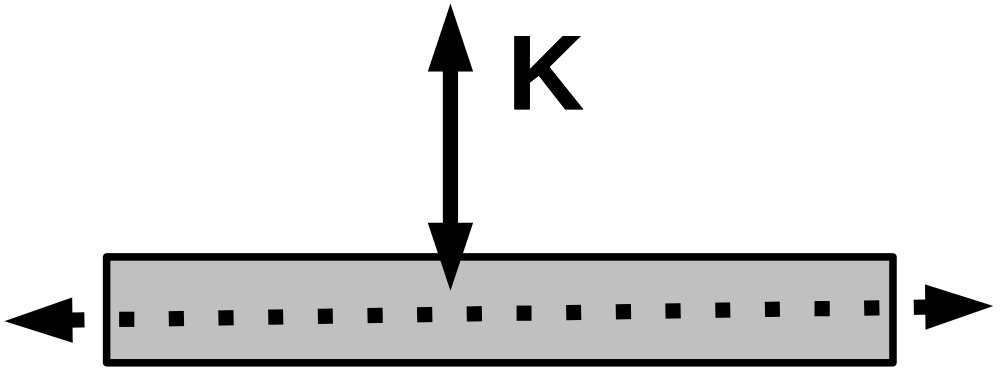
3 – Confiar Autoridades Certificadoras?



Posso ver o tráfego!

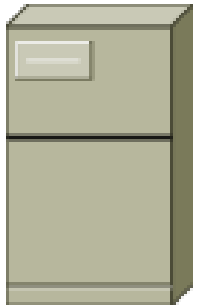
Internauta

K



CRIPTOGRAFIA

Servidor Web



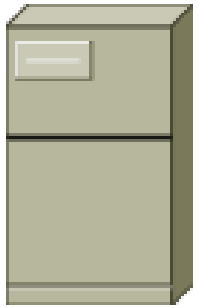
K

Chave Secreta
Dados Criptografados

3 – Confiar Autoridades Certificadoras?

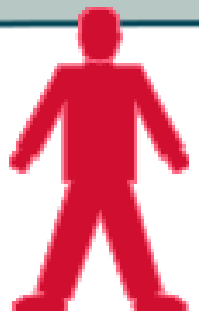
Internauta

Servidor Web



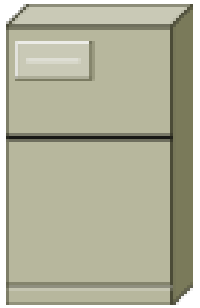
CRIPTOGRAFIA

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



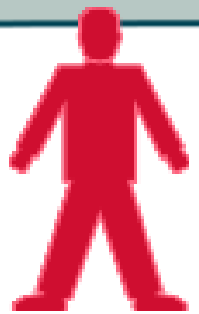
CRIPTOGRAFIA

Chave Pública

Kpriv

Kpub

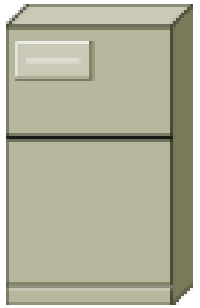
3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web

CRIPTOGRAFIA



K

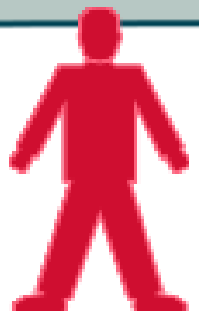
Kpriv

Chave Pública

Kpub

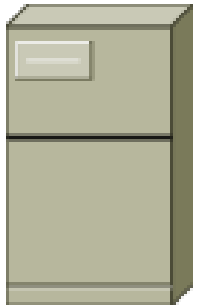
Chave Secreta Criptografada

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



CRIPTOGRAFIA

K

Kpriv

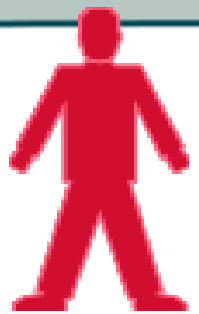
Kpub

Chave Pública

Chave Secreta Criptografada

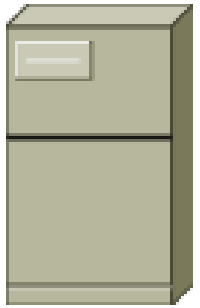
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



CRIPTOGRAFIA

K

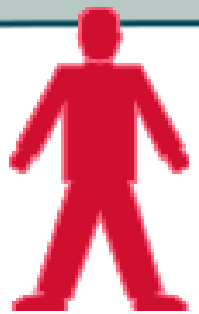
Kpub **Kpriv**

Chave Pública

Chave Secreta Criptografada **Kpub**

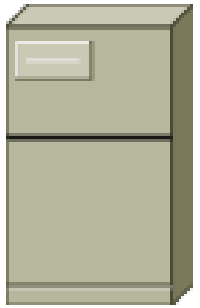
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



CRIPTOGRAFIA **Kpub**

Kpriv

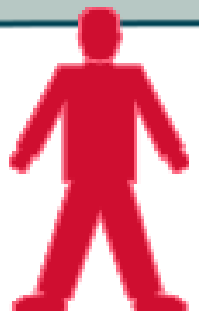
K

Chave Pública **Kpub**

Chave Secreta Criptografada

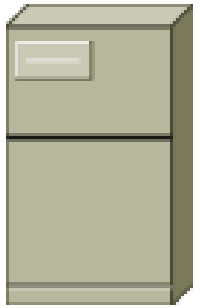
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



Kpub

CRIPTOGRAFIA

K

Kpriv

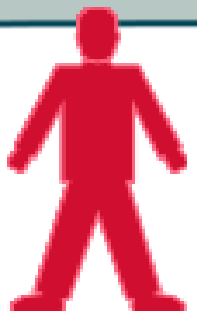
Kpub

Chave Pública

Chave Secreta Criptografada

Dados Criptografados

3 – Confiar Autoridades Certificadoras?

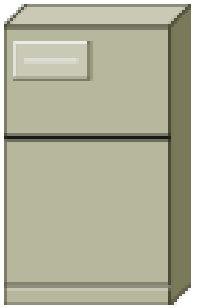


Internauta

Kpub

Kpub

Servidor Web



CRIPTOGRAFIA

K

Kpriv

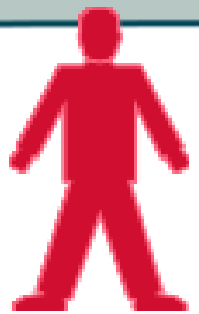
Kpub

Chave Pública

Chave Secreta Criptografada

Dados Criptografados

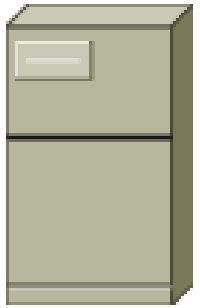
3 – Confiar Autoridades Certificadoras?



Kpub

Internauta

Servidor Web



Kpub **CRIPTOGRAFIA**

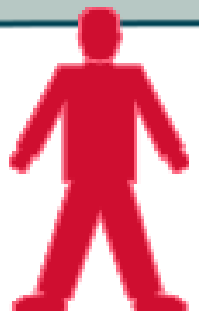
Kpriv

K **Chave Pública** **Kpub**

Chave Secreta Criptografada

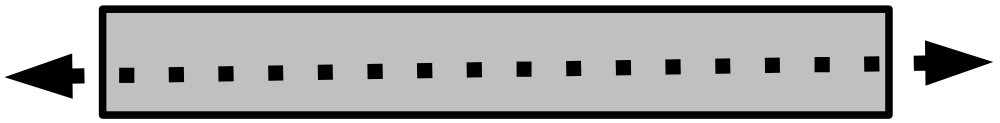
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



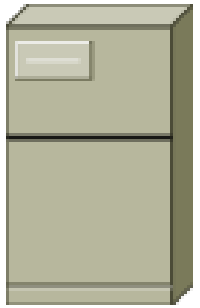
Kpub

Internauta



CRIPTOGRAFIA

Servidor Web



K

K

Kpriv

Kpub

Kpub

Chave Pública

Chave Secreta Criptografada

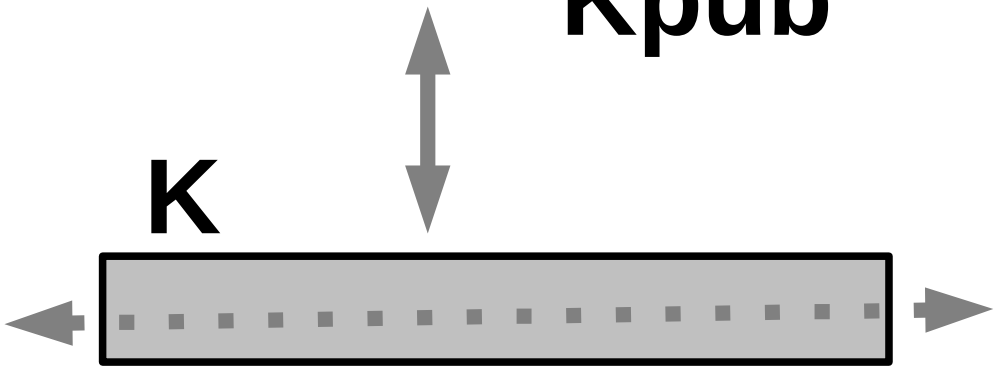
Dados Criptografados

3 – Confiar Autoridades Certificadoras?

Kpub

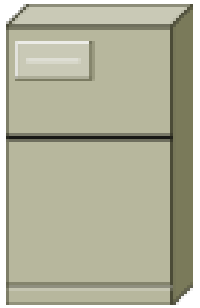
Internauta

K



CRIPTOGRAFIA

Servidor Web



K

Kpub

Chave Pública

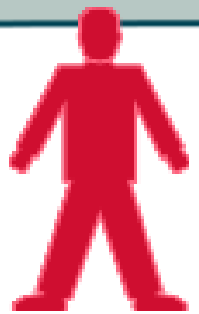
Chave Secreta Criptografada

Dados Criptografados

Kpub **Kpriv**

Kpub

3 – Confiar Autoridades Certificadoras?



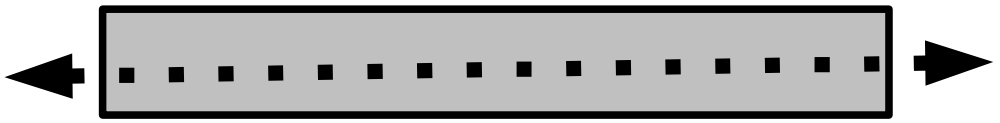
?!?!

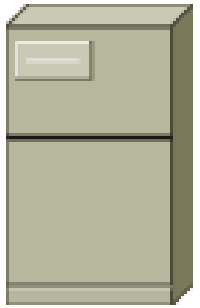
Kpub

Internauta

Servidor Web

K





CRIPTOGRAFIA

K

Kpub

Kpriv

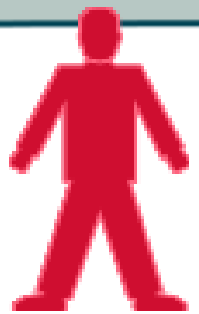
Kpub

Chave Pública

Chave Secreta Criptografada

Dados Criptografados

3 – Confiar Autoridades Certificadoras?



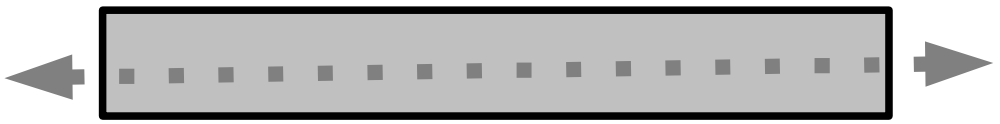
?!?!

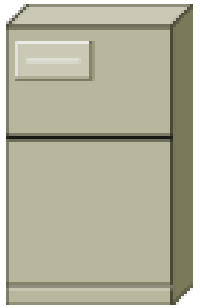
Kpub

Internauta

Servidor Web

K





CRIPTOGRAFIA

Kpriv

Kpub

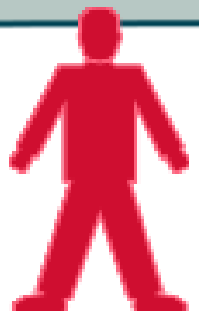
Kpub

Chave Pública

Chave Secreta Criptografada

Dados Criptografados

3 – Confiar Autoridades Certificadoras?

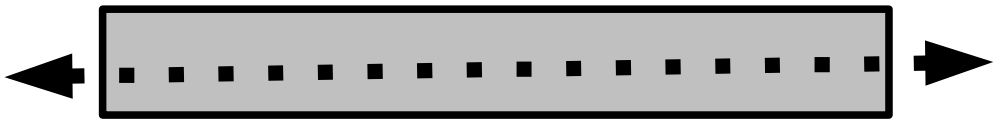


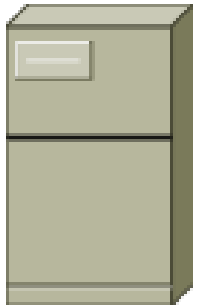
?!?!

Kpub

Internauta

Servidor Web





CRIPTOGRAFIA

K

Kpriv

K

Kpub

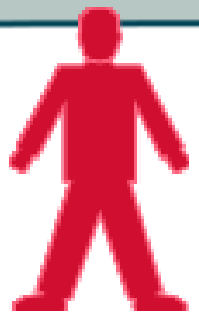
Chave Pública

Chave Secreta Criptografada

Dados Criptografados

Kpub

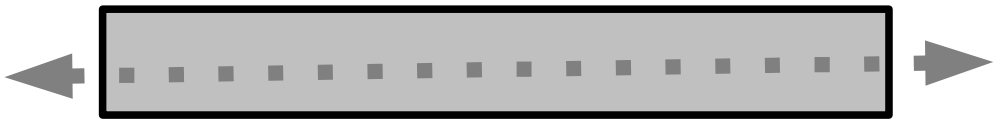
3 – Confiar Autoridades Certificadoras?



?!?!

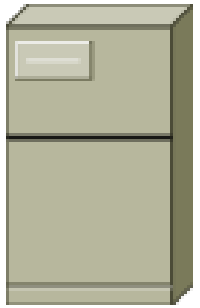
Kpub

Internauta



CRIPTOGRAFIA

Servidor Web



K

Kpub

Chave Pública

Chave Secreta Criptografada

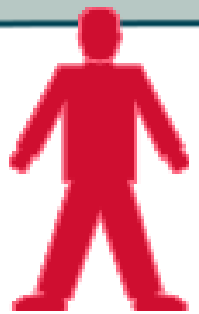
Dados Criptografados

Kpriv

Kpub

K

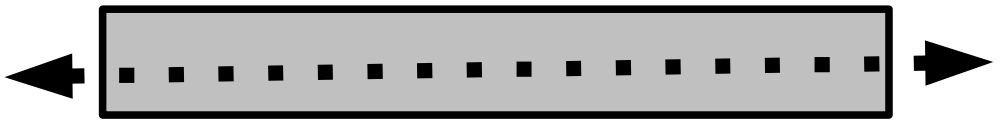
3 – Confiar Autoridades Certificadoras?



?!?!

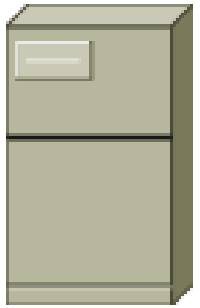
Kpub

Internauta



CRIPTOGRAFIA

Servidor Web



K

Kpub

Chave Pública

Chave Secreta Criptografada

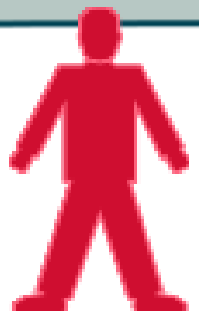
Dados Criptografados

Kpriv

Kpub

K

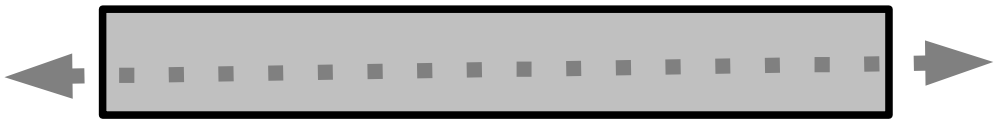
3 – Confiar Autoridades Certificadoras?



?!?!

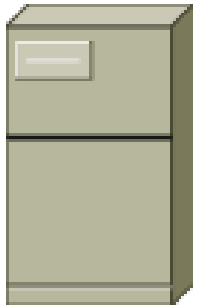
Kpub

Internauta



CRIPTOGRAFIA

Servidor Web



K

Kpub

Chave Pública

Chave Secreta Criptografada

Dados Criptografados

Kpriv

Kpub

K

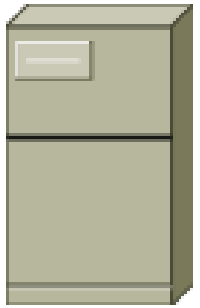
3 – Confiar Autoridades Certificadoras?

Internauta

Protocolo SSL

Netscape
(1994)

Servidor Web



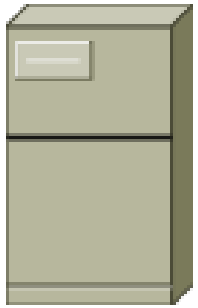
3 – Confiar Autoridades Certificadoras?

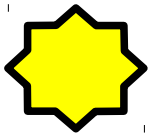
Internauta

Protocolo SSL

Netscape
(1994)

Servidor Web



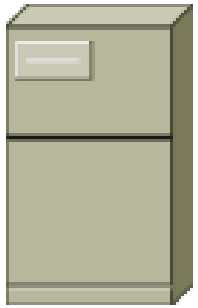


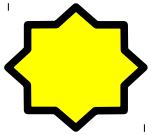
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



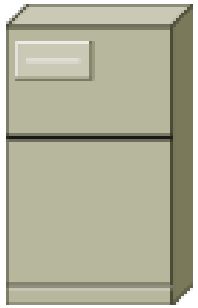


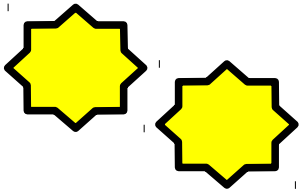
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



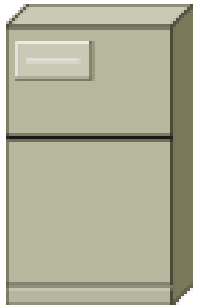


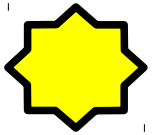
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web

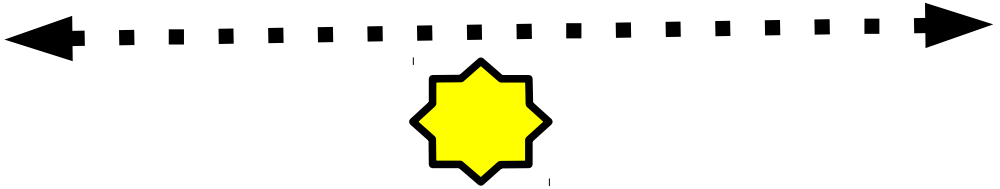




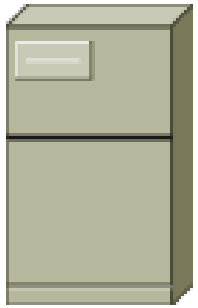
CERTIFICADO DIGITAL

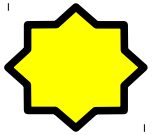
3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



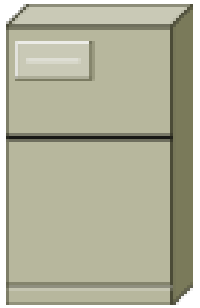


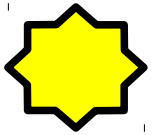
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web

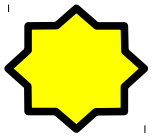




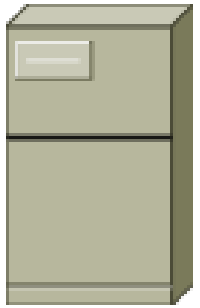
CERTIFICADO DIGITAL

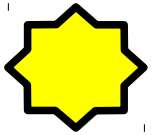
3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



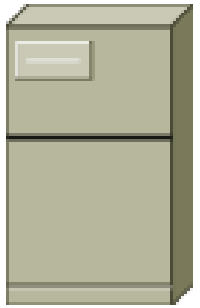


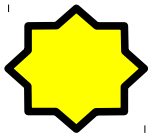
CERTIFICADO DIGITAL

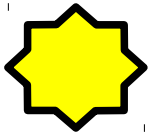
3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



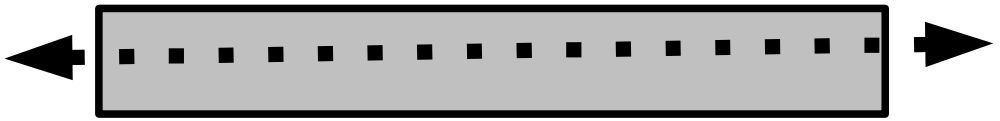




CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

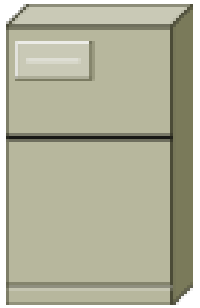


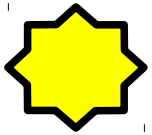
HTTP + SSL

=

HTTPS

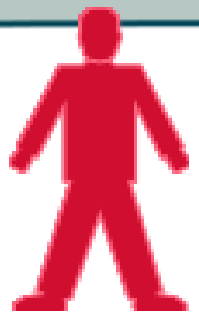
Servidor Web





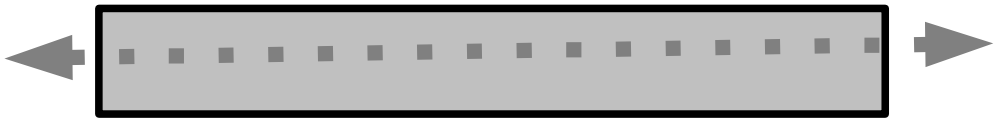
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?



?!?!

Internauta

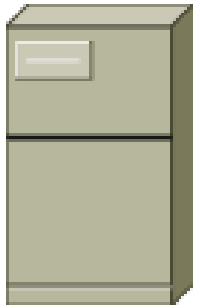


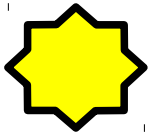
HTTP + SSL

=

HTTPS

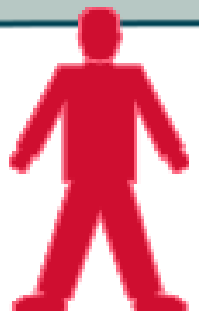
Servidor Web





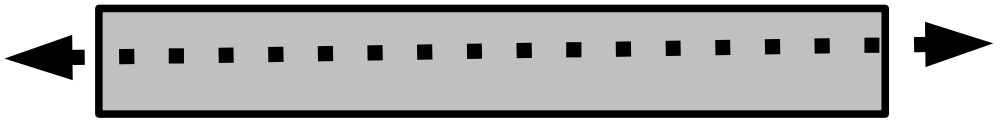
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?



?!?!

Internauta

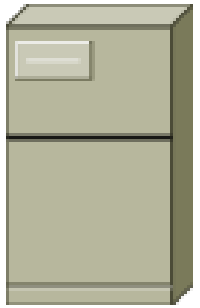


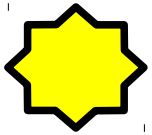
HTTP + SSL

=

HTTPS

Servidor Web



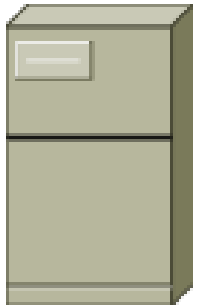


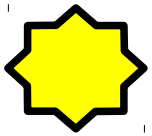
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



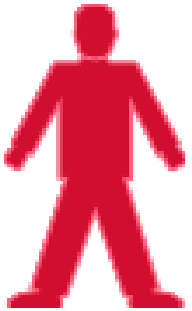


CERTIFICADO DIGITAL

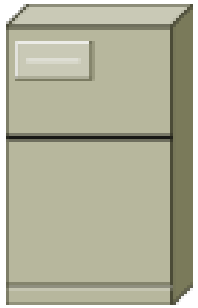
3 – Confiar Autoridades Certificadoras?

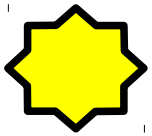
Internauta

Atacante



Servidor Web



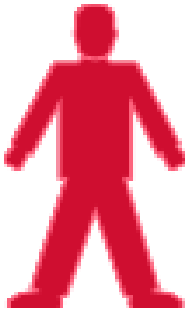


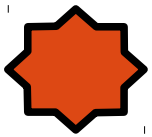
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

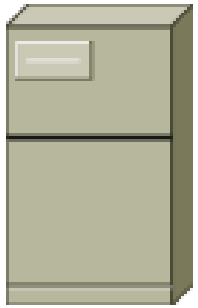
Atacante

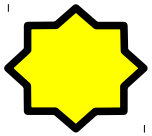




CERTIFICADO DIGITAL

Servidor Web



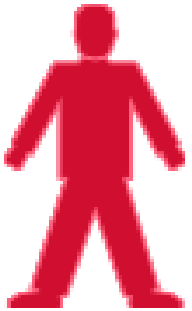


CERTIFICADO DIGITAL

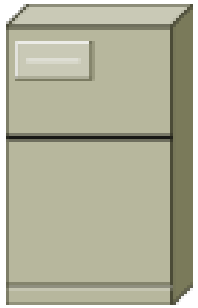
3 – Confiar Autoridades Certificadoras?

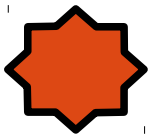
Internauta

Atacante

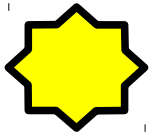


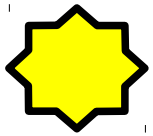
Servidor Web





CERTIFICADO DIGITAL



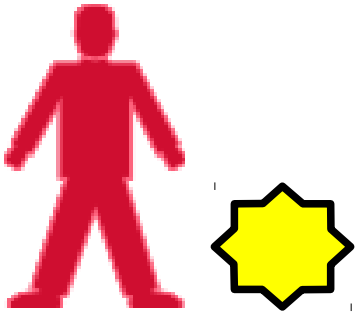


CERTIFICADO DIGITAL

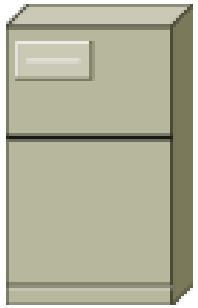
3 – Confiar Autoridades Certificadoras?

Internauta

Atacante



Servidor Web

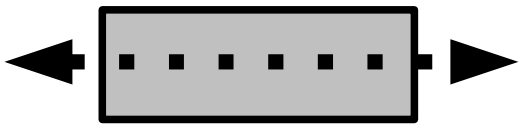


CERTIFICADO DIGITAL

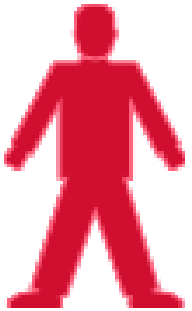
CERTIFICADO DIGITAL

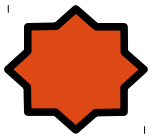
3 – Confiar Autoridades Certificadoras?

Internauta



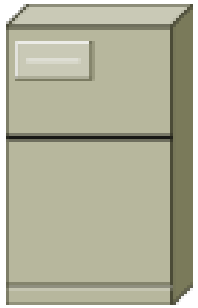
Atacante

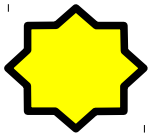




CERTIFICADO DIGITAL

Servidor Web

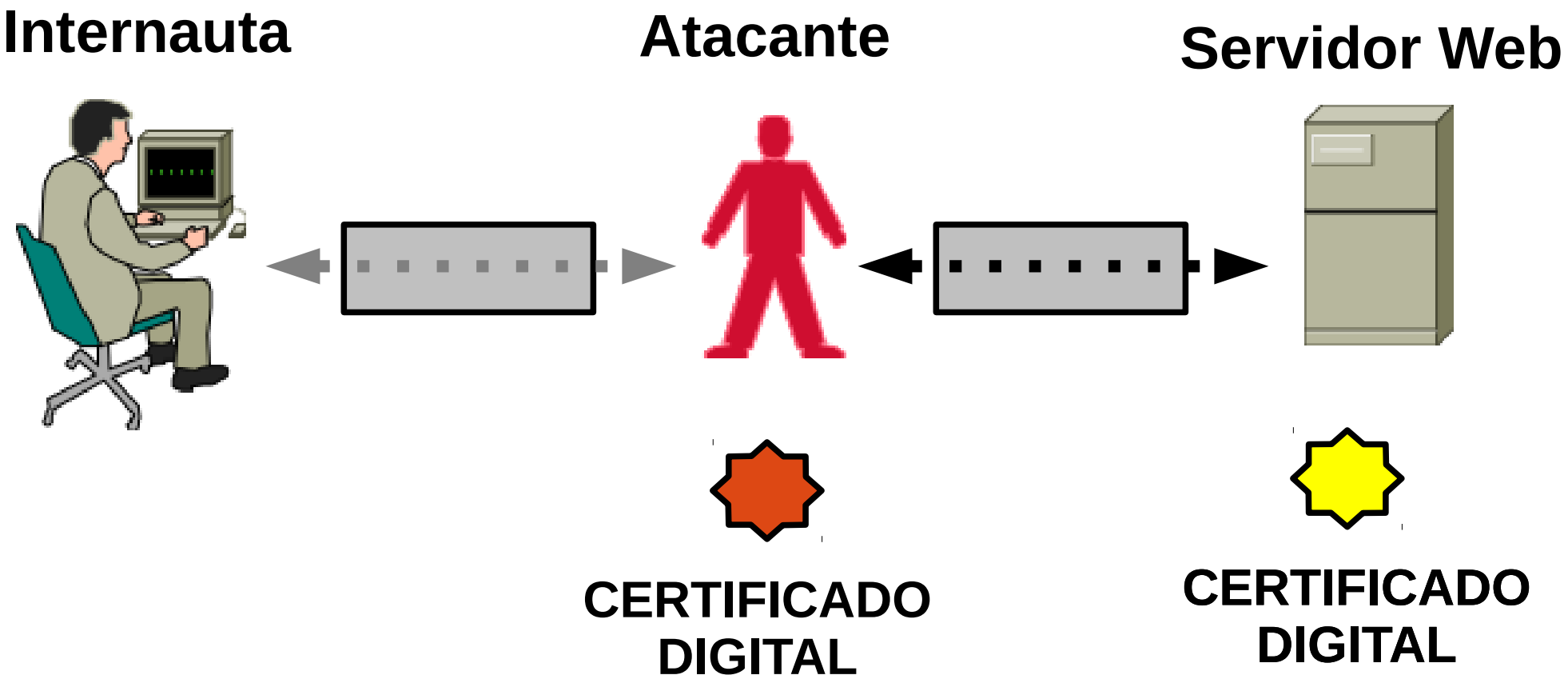




CERTIFICADO DIGITAL

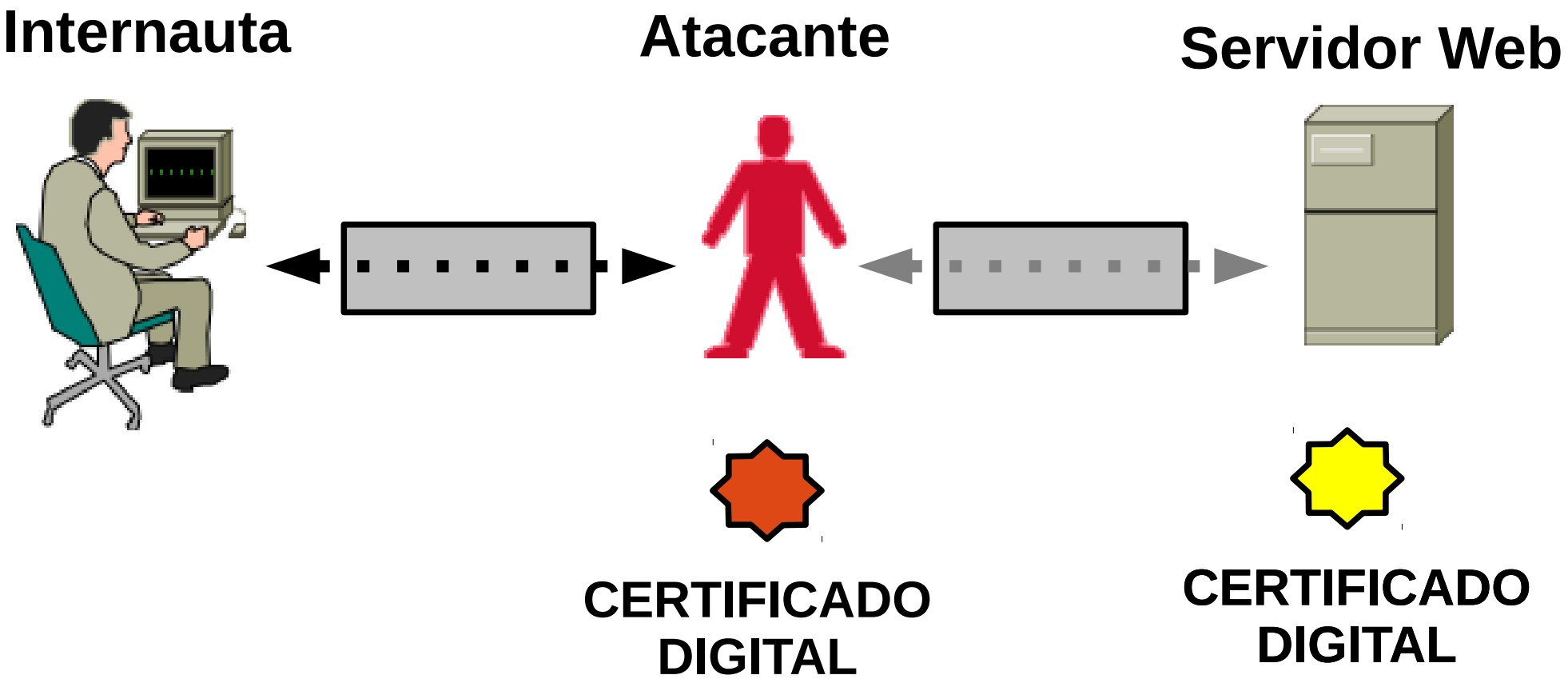
3 – Confiar Autoridades Certificadoras?

Ataque do Homem Intermediário



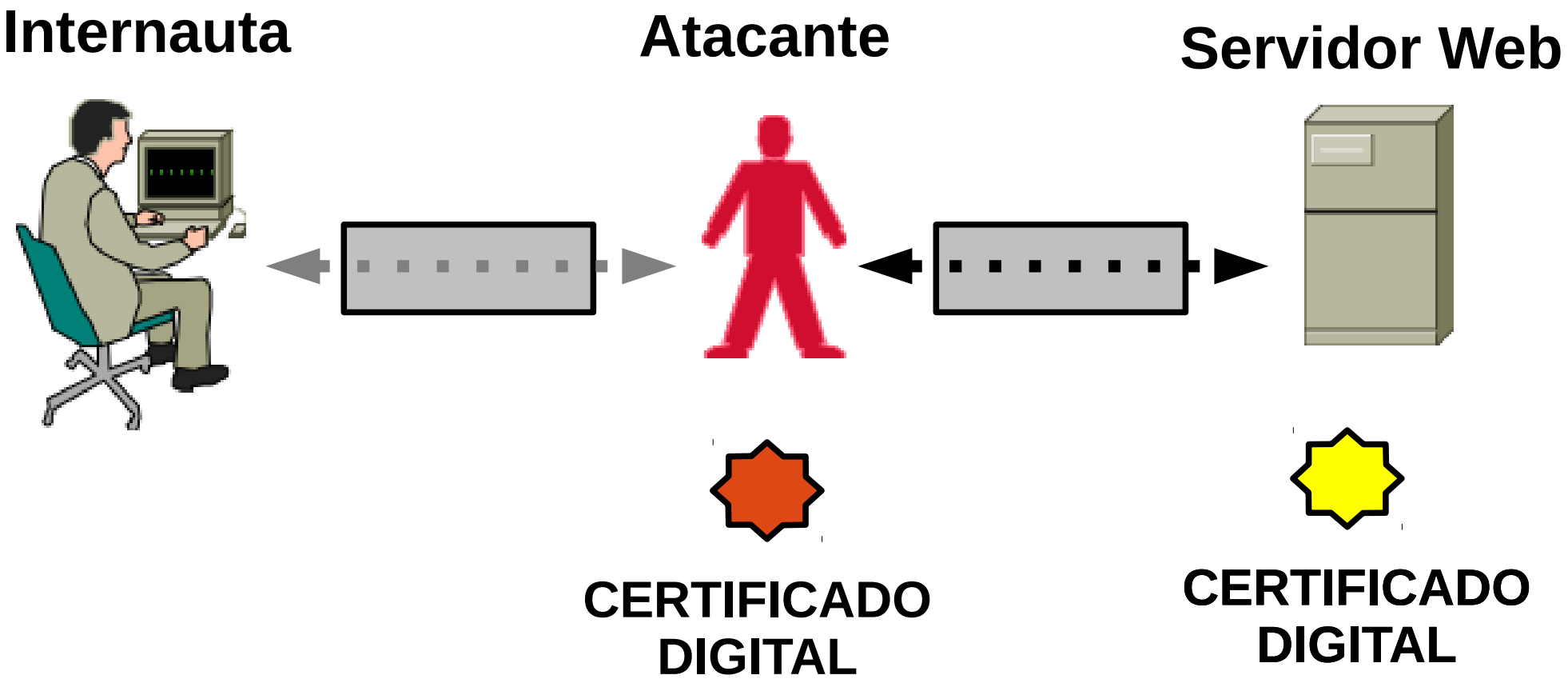
3 – Confiar Autoridades Certificadoras?

Ataque do Homem Intermediário



3 – Confiar Autoridades Certificadoras?

Ataque do Homem Intermediário



3 – Confiar Autoridades Certificadoras?

CELEPAR INFORMÁTICA do PARANÁ

Incidente de Segurança

China
MITM+SSL

GitHub
Jan/2013

Google
Set/2014

Yahoo
Out/2014

Ongoing MITM attack against Yahoo in China confirmed, Chinese Government accused of intercepting traffic

BY SEVAN MAKARACI · OCTOBER 4, 2014

Is it possible to block some search engine queries without blocking the entire website? The answer is yes and it appears that for this very reason there was an ongoing man-in-the-middle (MITM) attack against Yahoo in China. The online censorship monitoring organisation GreatFire sent out a tweet on September 30th saying that "Yahoo appears to under Man-in-the-middle attack in China. 3rd case of country-wide MITM, after Google, Github"

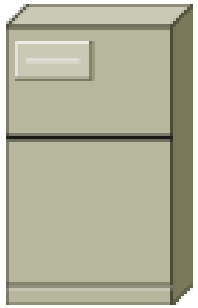
3 – Confiar Autoridades Certificadoras?

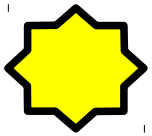
Solução:

Autoridade Certificadora

Internauta

Servidor Web

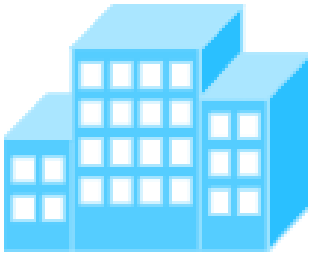


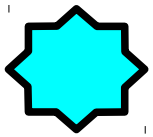


CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

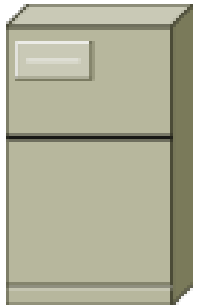
Internauta

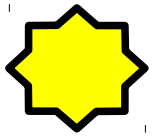




CERTIFICADO DIGITAL AUTORIDADE

Servidor Web



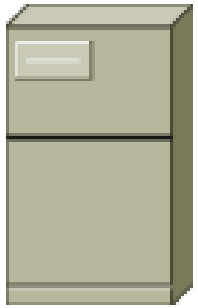


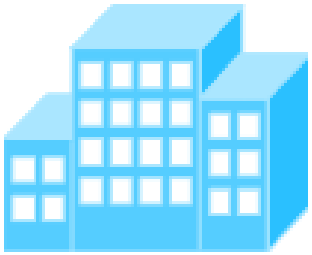
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web





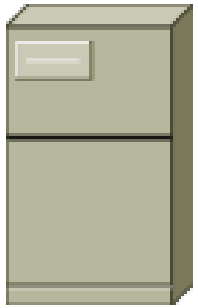
CERTIFICADO DIGITAL AUTORIDADE

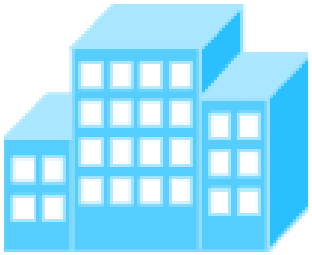
CERTIFICADO DIGITAL

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



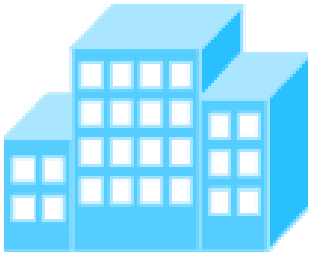


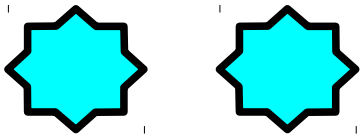
CERTIFICADO DIGITAL AUTORIDADE

CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?

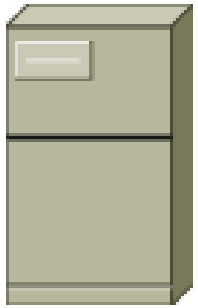
Internauta

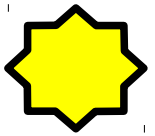




CERTIFICADO DIGITAL AUTORIDADE

Servidor Web



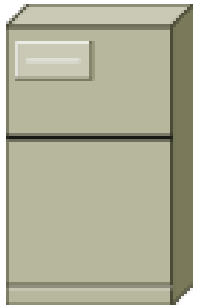


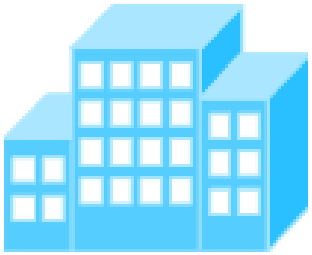
CERTIFICADO DIGITAL VÁLIDO

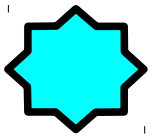
3 – Confiar Autoridades Certificadoras?

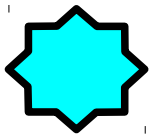
Internauta

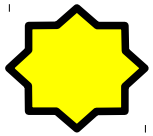
Servidor Web











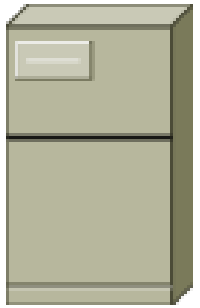
CERTIFICADO DIGITAL AUTORIDADE

CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?

Internauta

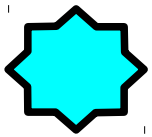
Servidor Web



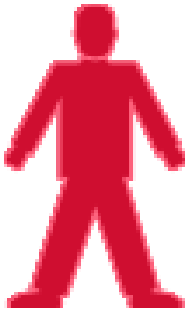
CERTIFICADO DIGITAL VÁLIDO

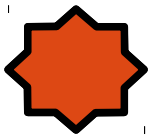
3 – Confiar Autoridades Certificadoras?

Internauta



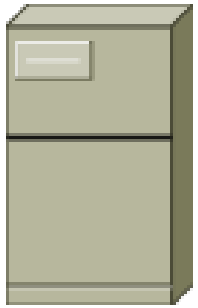
Atacante

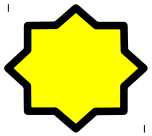




CERTIFICADO DIGITAL

Servidor Web

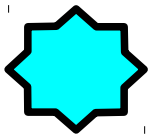




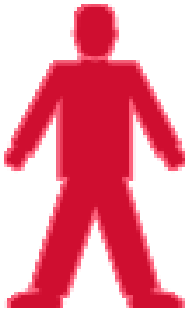
CERTIFICADO DIGITAL VÁLIDO

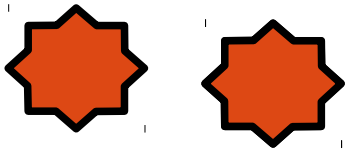
3 – Confiar Autoridades Certificadoras?

Internauta



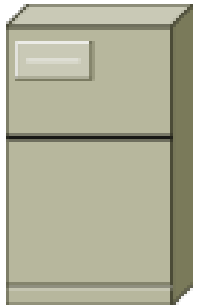
Atacante

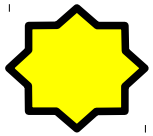




CERTIFICADO DIGITAL

Servidor Web



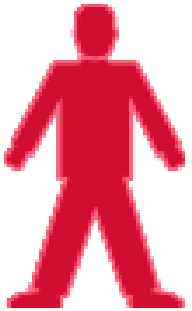


CERTIFICADO DIGITAL VÁLIDO

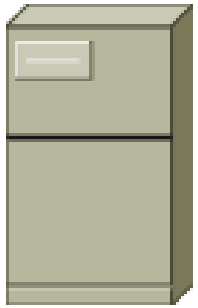
3 – Confiar Autoridades Certificadoras?

Internauta

Atacante



Servidor Web

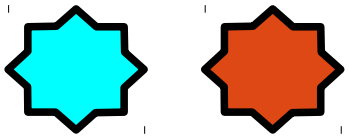


CERTIFICADO DIGITAL

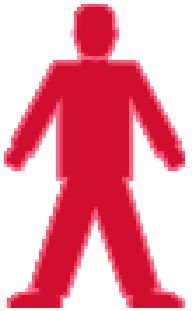
CERTIFICADO DIGITAL VÁLIDO

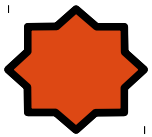
3 – Confiar Autoridades Certificadoras?

Internauta



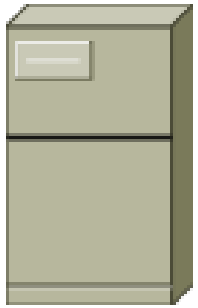
Atacante

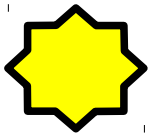




CERTIFICADO DIGITAL

Servidor Web

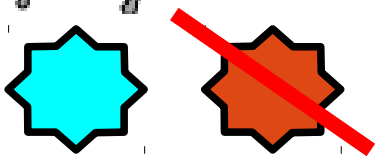




CERTIFICADO DIGITAL VÁLIDO

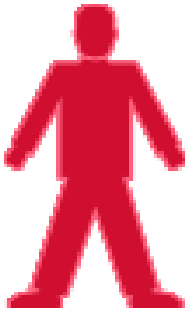
3 – Confiar Autoridades Certificadoras?

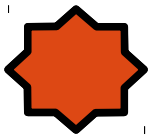
Internauta



Não Aceito!
Certificado INVÁLIDO!

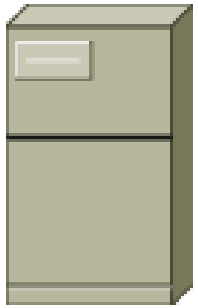
Atacante

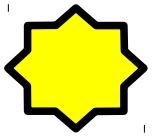




CERTIFICADO DIGITAL

Servidor Web

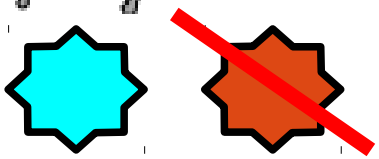




CERTIFICADO DIGITAL VÁLIDO

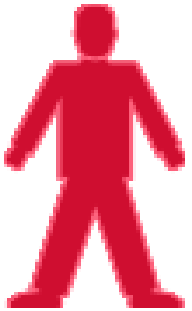
3 – Confiar Autoridades Certificadoras?

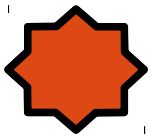
Internauta



Não Aceito!
Certificado INVÁLIDO!

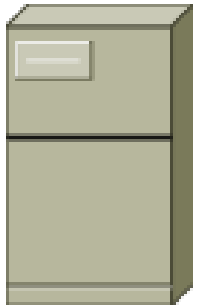
Atacante

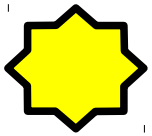




CERTIFICADO DIGITAL

Servidor Web

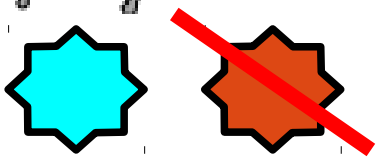




CERTIFICADO DIGITAL VÁLIDO

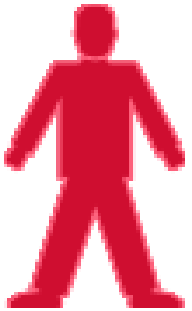
3 – Confiar Autoridades Certificadoras?

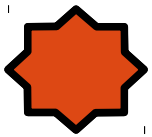
Internauta



Não Aceito!
Certificado INVÁLIDO!

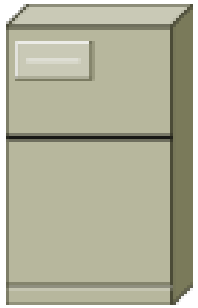
Atacante

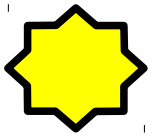




CERTIFICADO DIGITAL

Servidor Web



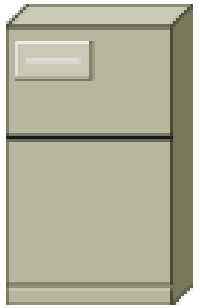


CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web

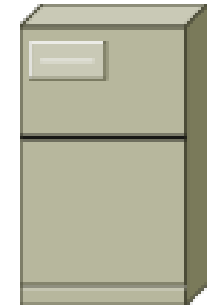


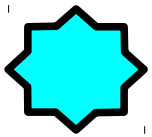
CERTIFICADO DIGITAL VÁLIDO

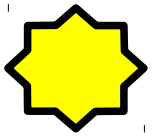
3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web





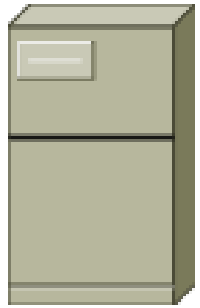


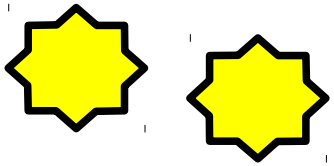
CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



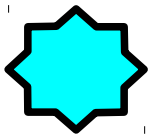


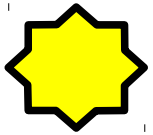
CERTIFICADO DIGITAL VÁLIDO

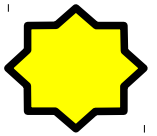
3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web





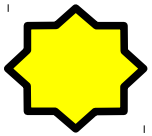


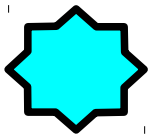
CERTIFICADO DIGITAL VÁLIDO

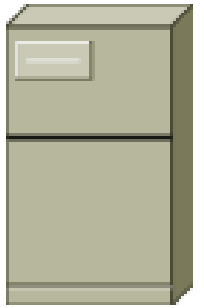
3 – Confiar Autoridades Certificadoras?

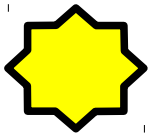
Internauta

Servidor Web







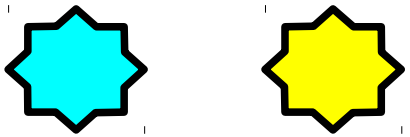


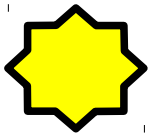
CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



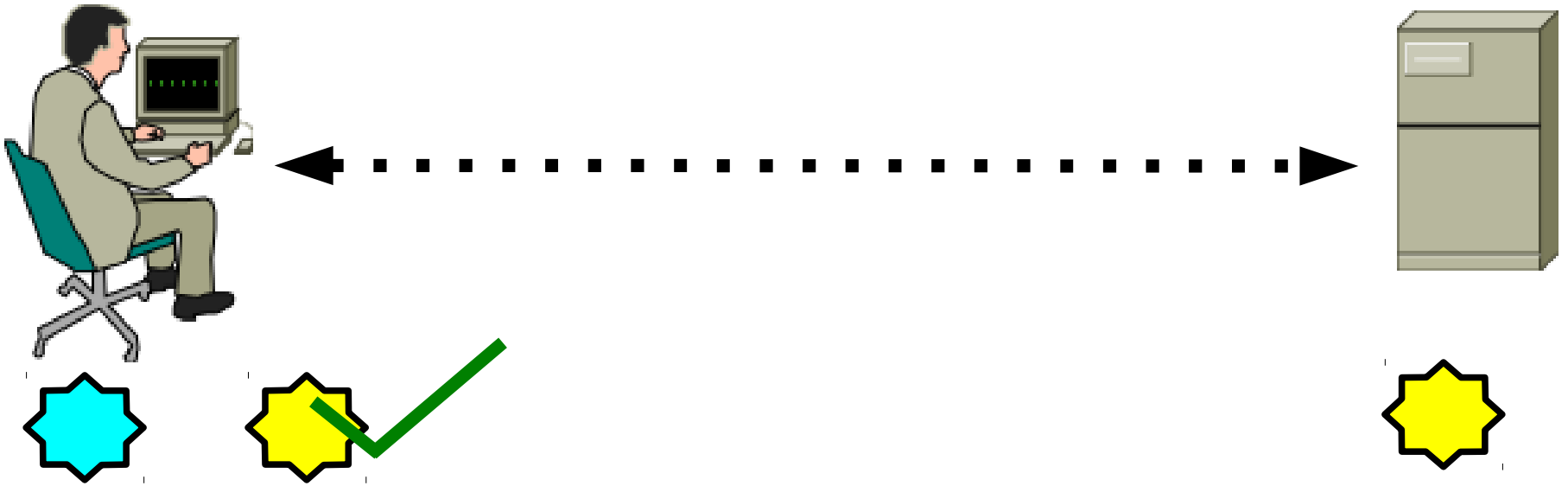


CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



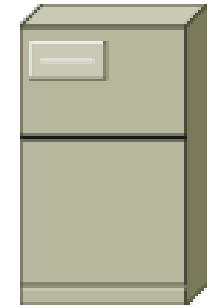
Verificado! Ok!

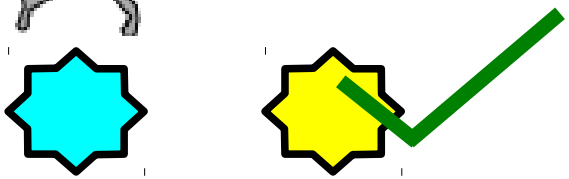
CERTIFICADO DIGITAL VÁLIDO

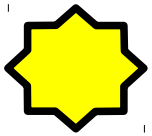
3 – Confiar Autoridades Certificadoras?

Internauta

Servidor Web



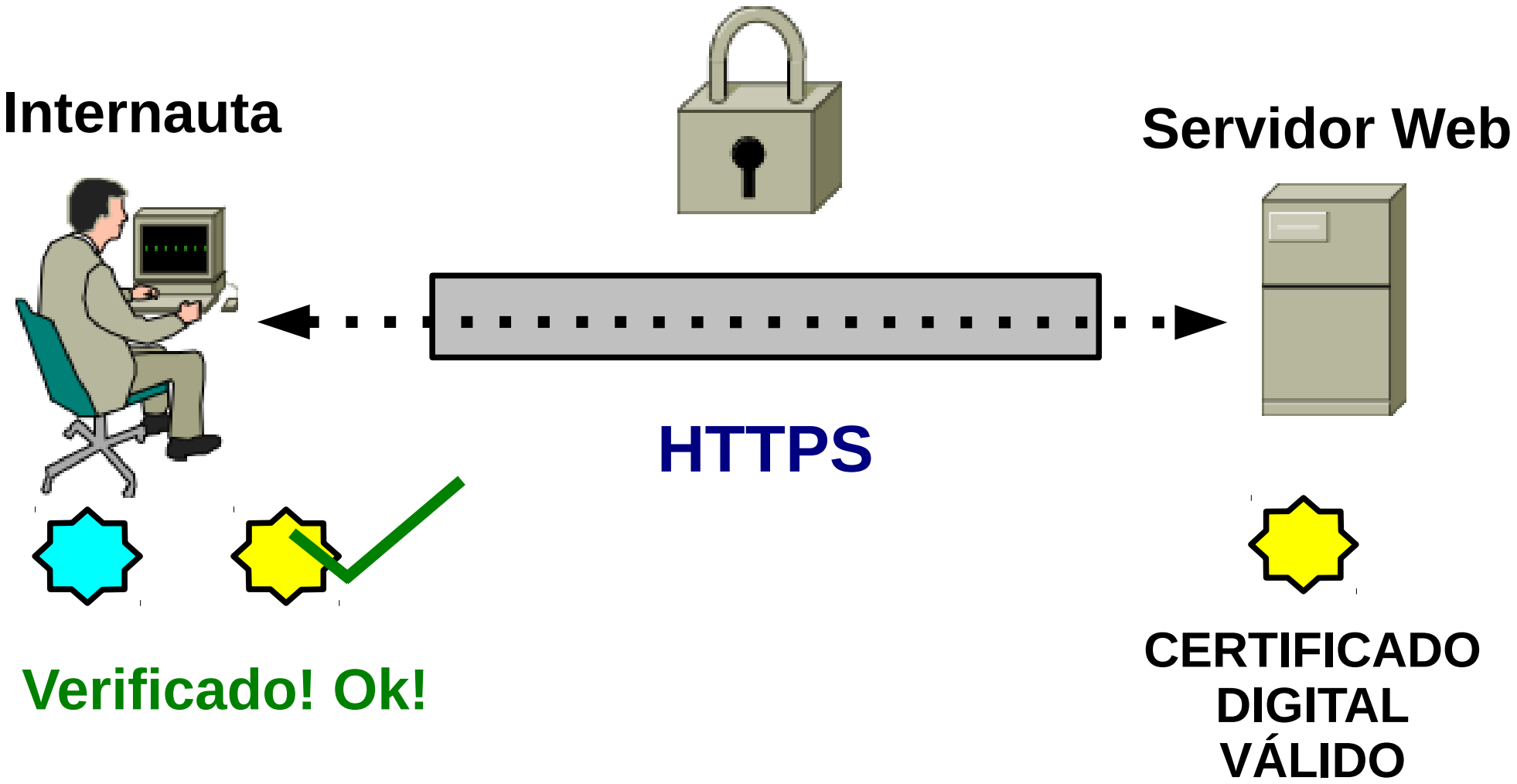




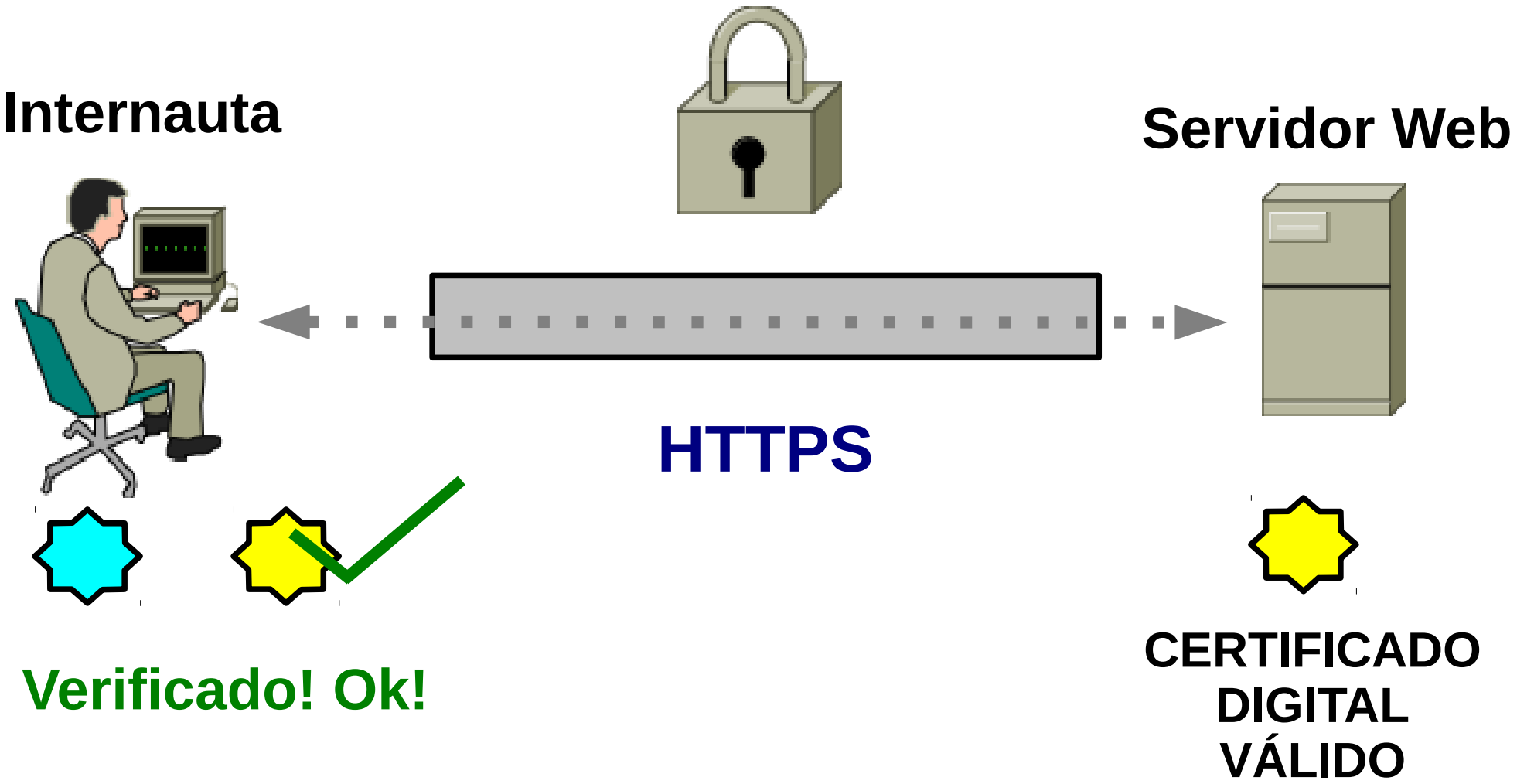
Verificado! Ok!

CERTIFICADO DIGITAL VÁLIDO

3 – Confiar Autoridades Certificadoras?



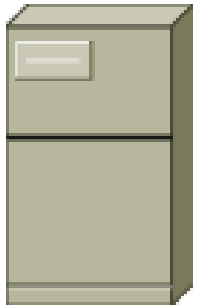
3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?

Internauta

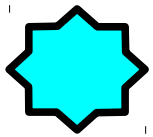
Servidor Web do Atacante

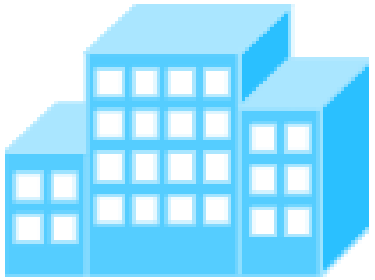


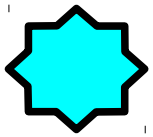
CERTIFICADO DIGITAL INVÁLIDO

3 – Confiar Autoridades Certificadoras?

Internauta

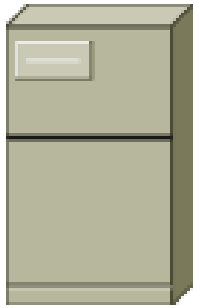






CERTIFICADO AUTORIDADE

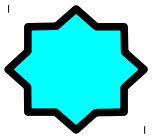
Servidor Web do Atacante

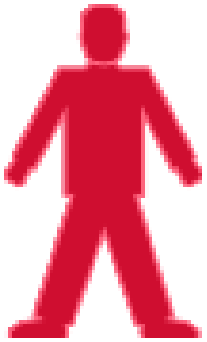


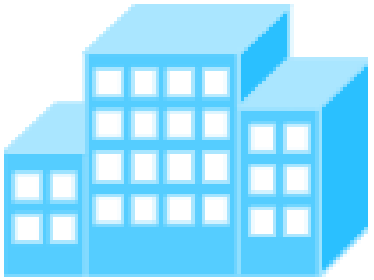
CERTIFICADO DIGITAL INVÁLIDO

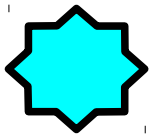
3 – Confiar Autoridades Certificadoras?

Internauta



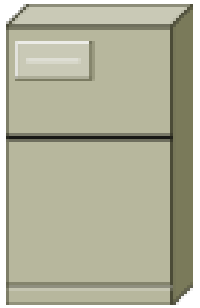






CERTIFICADO AUTORIDADE

Servidor Web do Atacante

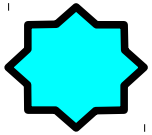


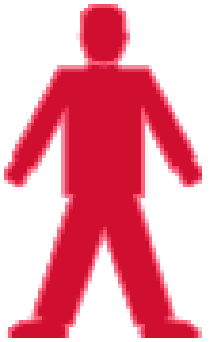
CERTIFICADO DIGITAL INVÁLIDO

3 – Confiar Autoridades Certificadoras?

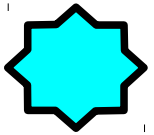
CELEPAR INFORMÁTICA do PARANÁ

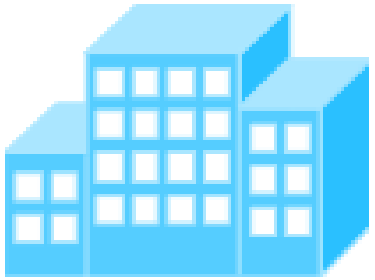
Internauta

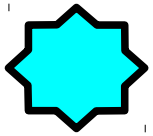




CERTIFICADO COMPROMETIDO

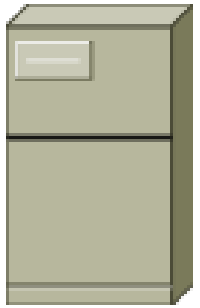






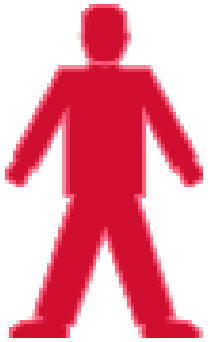
CERTIFICADO AUTORIDADE

Servidor Web do Atacante



CERTIFICADO DIGITAL INVÁLIDO

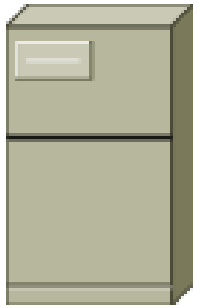
3 – Confiar Autoridades Certificadoras?

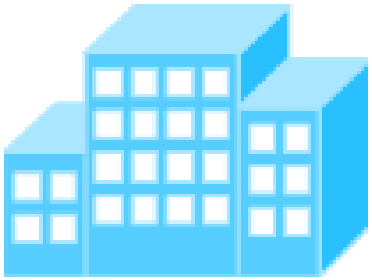


CERTIFICADO COMPROMETIDO

Internauta

Servidor Web do Atacante



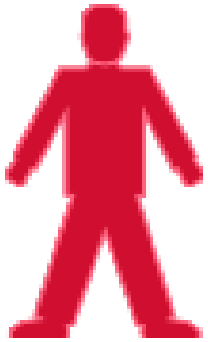


CERTIFICADO AUTORIDADE

CERTIFICADO DIGITAL INVÁLIDO

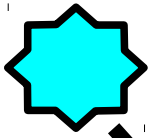
3 – Confiar Autoridades Certificadoras?

CELEPAR INFORMÁTICA do PARANÁ

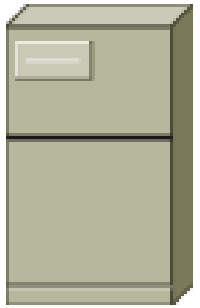


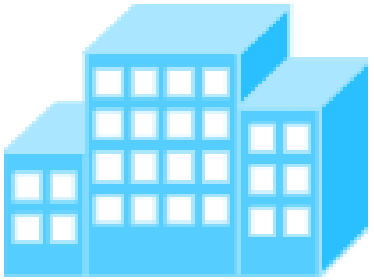
CERTIFICADO COMPROMETIDO

Internauta



Servidor Web do Atacante

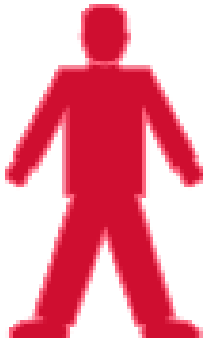




CERTIFICADO AUTORIDADE

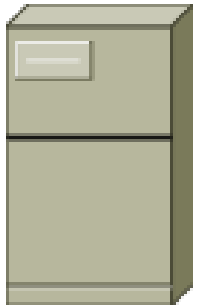
CERTIFICADO DIGITAL INVÁLIDO

3 – Confiar Autoridades Certificadoras?

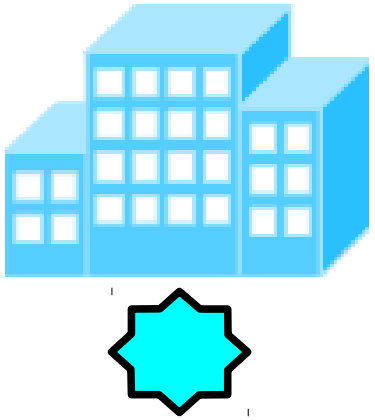


CERTIFICADO COMPROMETIDO

Servidor Web do Atacante



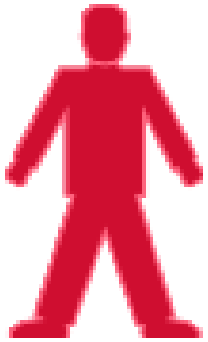
Internauta



CERTIFICADO AUTORIDADE

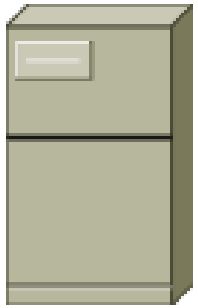
CERTIFICADO DIGITAL INVÁLIDO

3 – Confiar Autoridades Certificadoras?

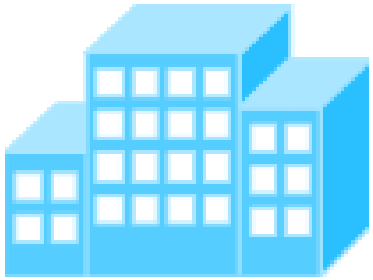


CERTIFICADO COMPROMETIDO

Servidor Web do Atacante



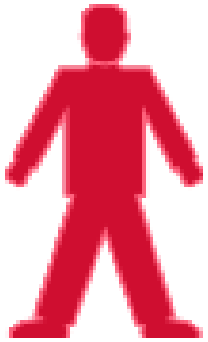
Internauta



CERTIFICADO AUTORIDADE

CERTIFICADO DIGITAL VÁLIDO

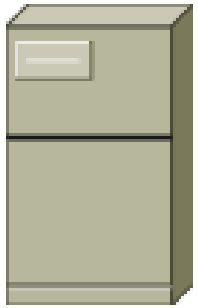
3 – Confiar Autoridades Certificadoras?

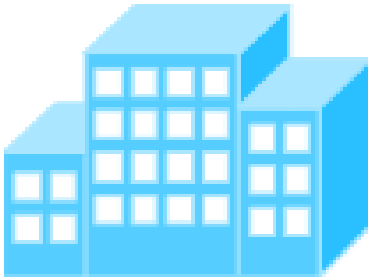


CERTIFICADO COMPROMETIDO

Internauta

Servidor Web do Atacante





CERTIFICADO AUTORIDADE

CERTIFICADO DIGITAL VÁLIDO

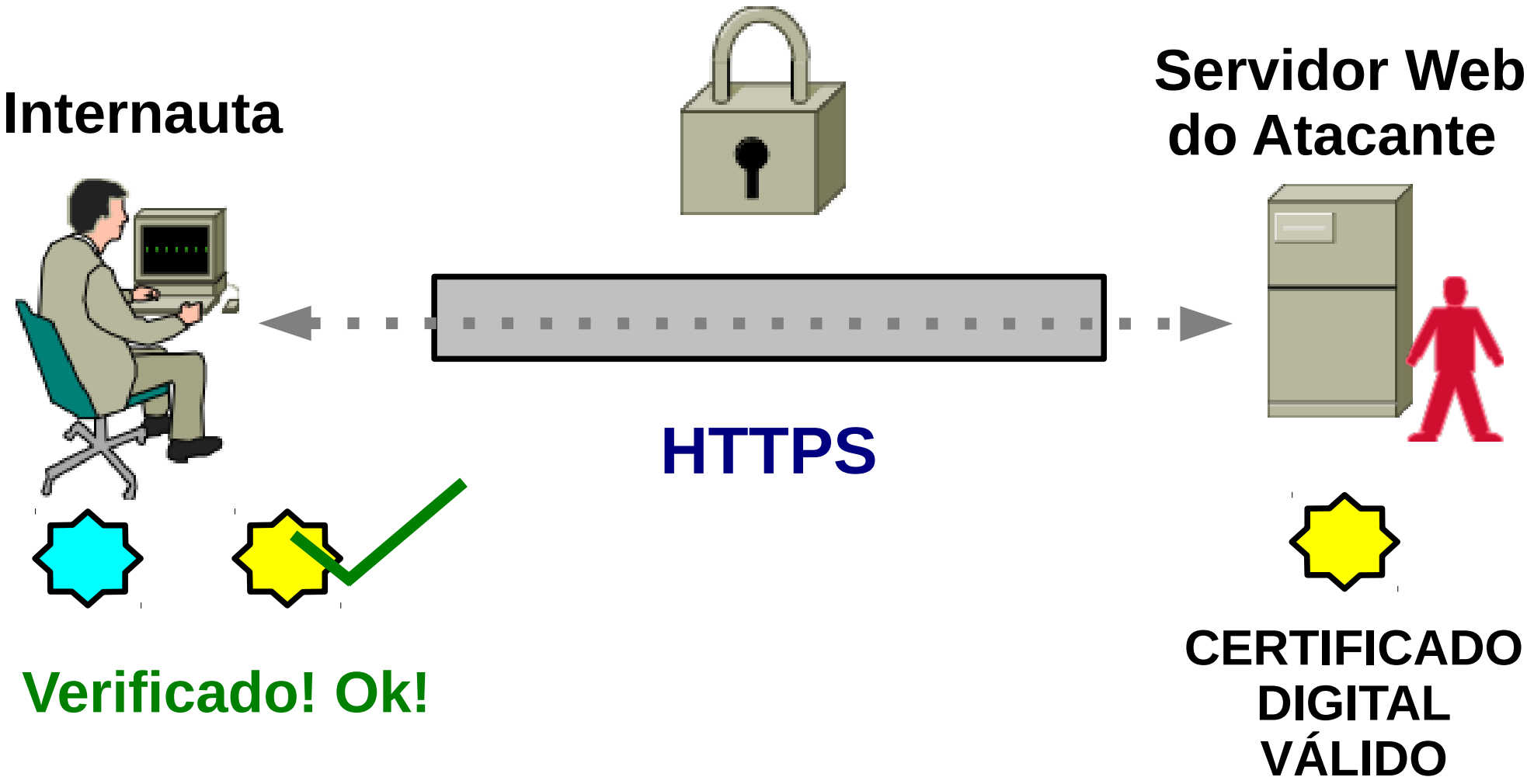
3 – Confiar Autoridades Certificadoras?

Internauta

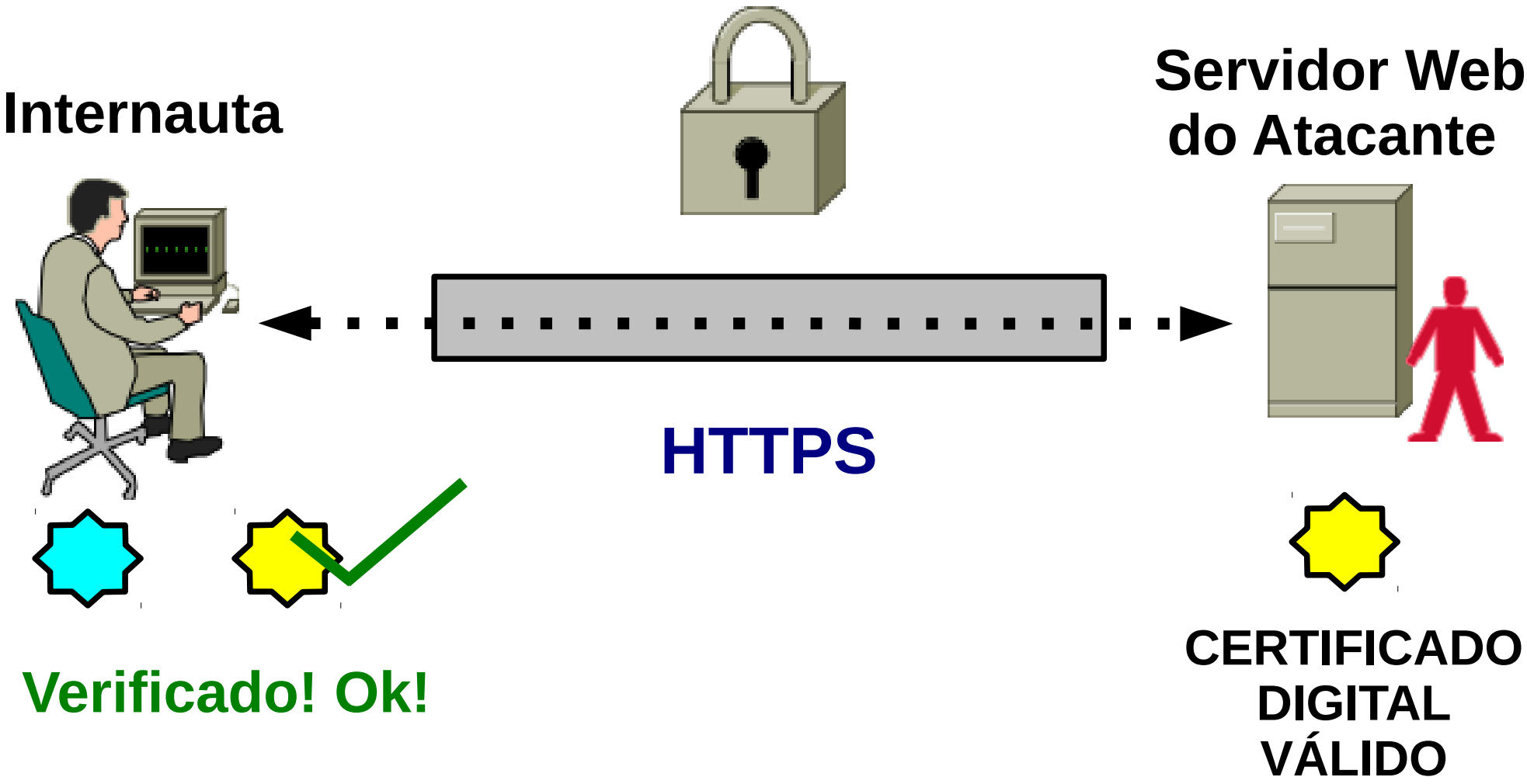
Servidor Web do Atacante

CERTIFICADO DIGITAL VÁLIDO

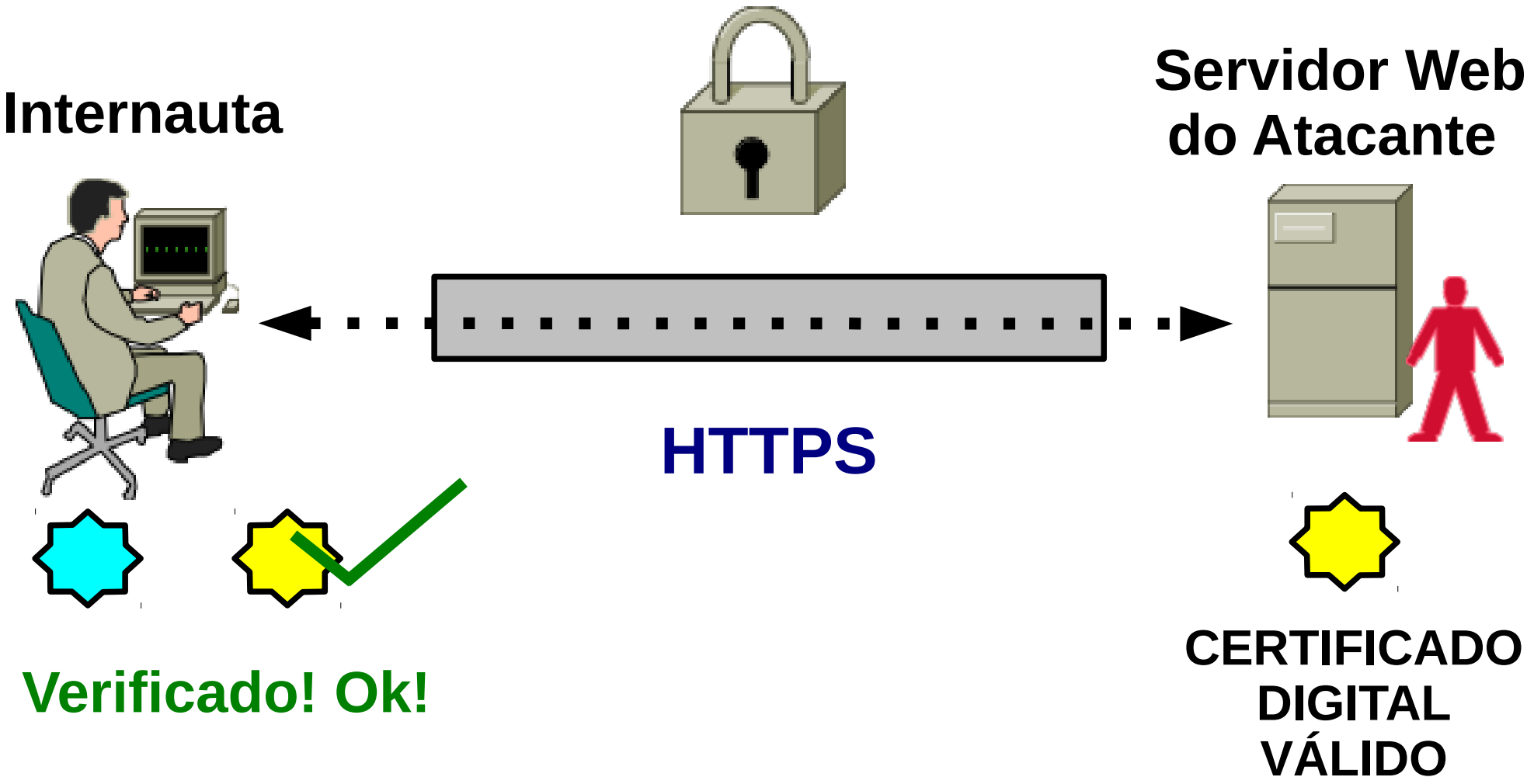
3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



CELEPAR INFORMÁTICA do PARANÁ

Incidente de Segurança

- DigiNotar
- Holanda

Poderia ser utilizado para validar certificações falsas.

Setembro/2011

3 – Confiar Autoridades Certificadoras?

Solução

- Certificados Atualizados
- Conferir Acesso Seguro

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Considerações Finais

Considerações Finais

Confiança:

- Serviços de Domínios (DNS)
- Rotas de Provedores (BGP)
- Autoridades Certificadoras (SSL)

Causa:

- Legado – Internet (década 80/90)
- Além das fronteiras

Considerações Finais

Edward Snowden x NSA

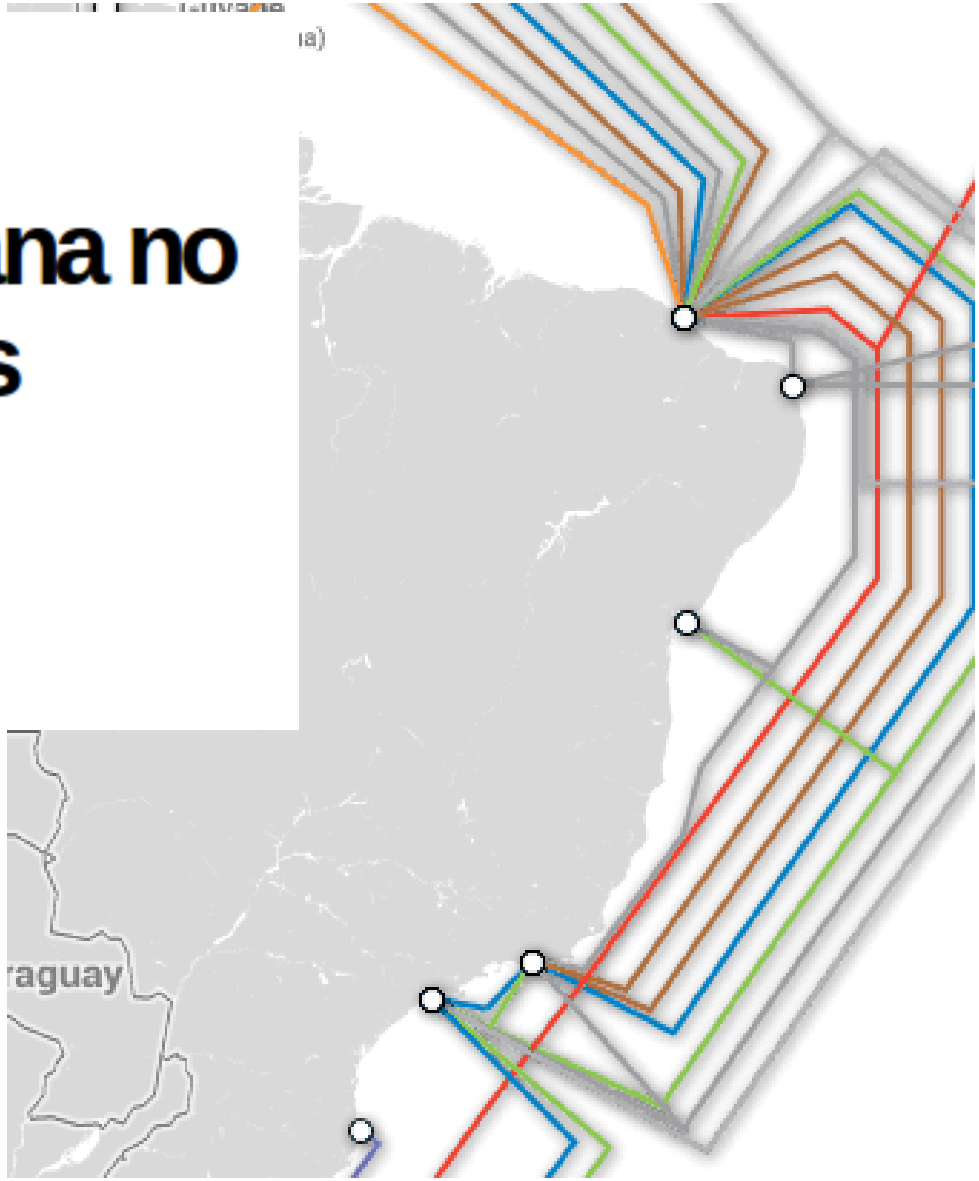
“Assuma que seu adversário é capaz de fazer um trilhão de tentativas por segundo”

Considerações Finais

Grande interesse da espionagem americana no Brasil está nos cabos submarinos 14

Luiz Felipe de Alencastro

29/07/2013 | 11h29



Gleen Greenwald (The Guardian) 08/2013

… os EUA praticam espionagem não apenas para se proteger do terrorismo, mas também para obter vantagens comerciais e industriais

Grato! :)

CELEPAR INFORMÁTICA do PARANÁ

Hermano Pereira

→ pereira@hermano.com.br

Slides e Referências em:

www.hermano.com.br

Obs: as animações que foram apresentadas são meramente ilustrativas.

Referências

Artigo - Sandro Suffert
http://sseguranca.blogspot.com.br/2010/04/root-dns-ca-e-as-uma-questao-de.html

RFC DNS
http://tools.ietf.org/html/rfc1034

CVE Kaminsky
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1447

DNS Poison (Brasil)
http://seiti.eti.br/blog/2009/dns-poisoning-na-net-virtua
http://dosesdiarias.seucaminho.com/index.php/2009/04/servidor-da-net-sofre-ataque-de-dns-poison/
http://www.eweek.com/c/a/Security/Report-Claims-DNS-Cache-Poisoning-Attack-Against-Brazilian-Bank-and-ISP-761709/

DNS Poison (China)
http://www.theregister.co.uk/2014/01/21/china_dns_poisoning_attack/
http://www.eweek.com/cloud/dns-poisoning-suspected-cause-of-huge-internet-outage-in-china.html

DNS Poison (Malawi)
http://www.humanipo.com/news/4027/Malawi-Google-site-hacked-by-Bangladeshi-hacker

DNS Poison (Malaysia)
http://www.thestar.com.my/Tech/Tech-News/2013/10/11/Google-Malaysia-page-redirect/

DNS Poison (Kenya)
http://www.cio.co.ke/news/main-stories/google,-microsoft,-linkedin-hacked-in-kenyan-dns-hijack

Referências (continuação)

DNS Poison (Guia Ilustrado)
http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

DNS China
http://www.cio.com/article/588165/China_s_Great_Firewall_Spreads_Overseas
http://www.pcworld.com/article/192658/article.html

Roteamento Guadalajara – Washington via Bielorrússia
http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/

Protocolo Roteável IP
http://www.ietf.org/rfc/rfc791.txt

Protocolo de Roteamento BGP
http://tools.ietf.org/html/rfc1771

Sequestro de Prefixos (China)
http://blog.layeredsec.com/2010/04/chinese-isp-hijacks-internet.html

Sequestro de Prefixos (Paquistão)
http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/

Sequestro de DNS Google via BGP (Turquia)
http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/

Sequestro de DNS Google via BGP (Venezuela)
http://tecnogeek.com.br/dns-do-google-foi-sequestrado-no-ultimo-fim-de-semana/
http://arstechnica.com/information-technology/2014/03/google-dns-briefly-hijacked-to-venezuela/

Referências (continuação)

Protocolo SSL (História)
http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzain/rzainhistory.htm

China + MITM + SSL
https://en.greatfire.org/blog/2013/jan/china-github-and-man-middle
http://www.infosecurity-magazine.com/news/china-man-in-the-middle-attack/
http://www.securityinform.com/2014/10/04/ongoing-mitm-attack-against-yahoo-in-china-confirmed-chinese-Government-accused-of-intercepting-traffic/

Diginotar (Certificado Comprometido)
http://httpsonline.blogspot.com.br/2011/09/empresa-que-emite-certificados-digitais.html
https://www.cert.be/pro/docs/diginotar-hack

Snowden:
http://info.abril.com.br/noticias/seguranca/2013/08/snowden-usou-ate-cubo-magico-para-se-proteger-da-nsa.shtml
http://operamundi.uol.com.br/conteudo/noticias/30451/eua+espionam+para+obter+vantagens+comerciais+e+industriais+diz+jornalista+do+guardian.shtml

Espionagem no Brasil:
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1
http://terramagazine.terra.com.br/silviomeira/blog/2013/06/07/governo-dos-eua-vigia-todo-mundo/
http://noticias.uol.com.br/blogs-e-colunas/coluna/luiz-felipe-alencastro/2013/07/29/grande-interesse-da-espionagem-americana-no-brasil-esta-nos-cabos-submarinos.htm