



1ª Semana Acadêmica de Computação

UTFPR
Câmpus Pato Branco

01 de agosto de 2013

Podemos confiar na Internet?

(segurança computacional)

Hermano Pereira

Professor – Tecnologia em
Sistemas para Internet

UTFPR - Câmpus Guarapuava

Introdução

1 – Confiar na Resolução de Domínios?

2 – Confiar no Roteamento de Provedores?

3 – Confiar em Autoridades Certificadoras?

Considerações Finais

aproximadamente 60 minutos

Segurança

- Integridade
- Disponibilidade
- Confidencialidade

- 1 – Resolução de Domínios
- 2 – Roteamento de Provedores
- 3 – Autoridades Certificadoras

→ *blog Sandro Suffert*

→ *atuação na área*

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?

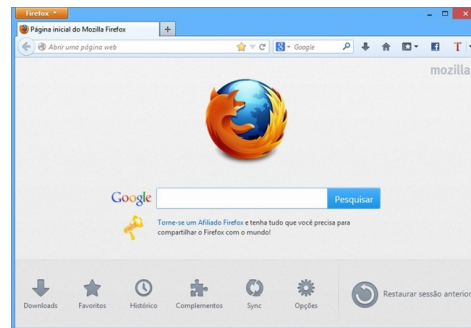
Internauta



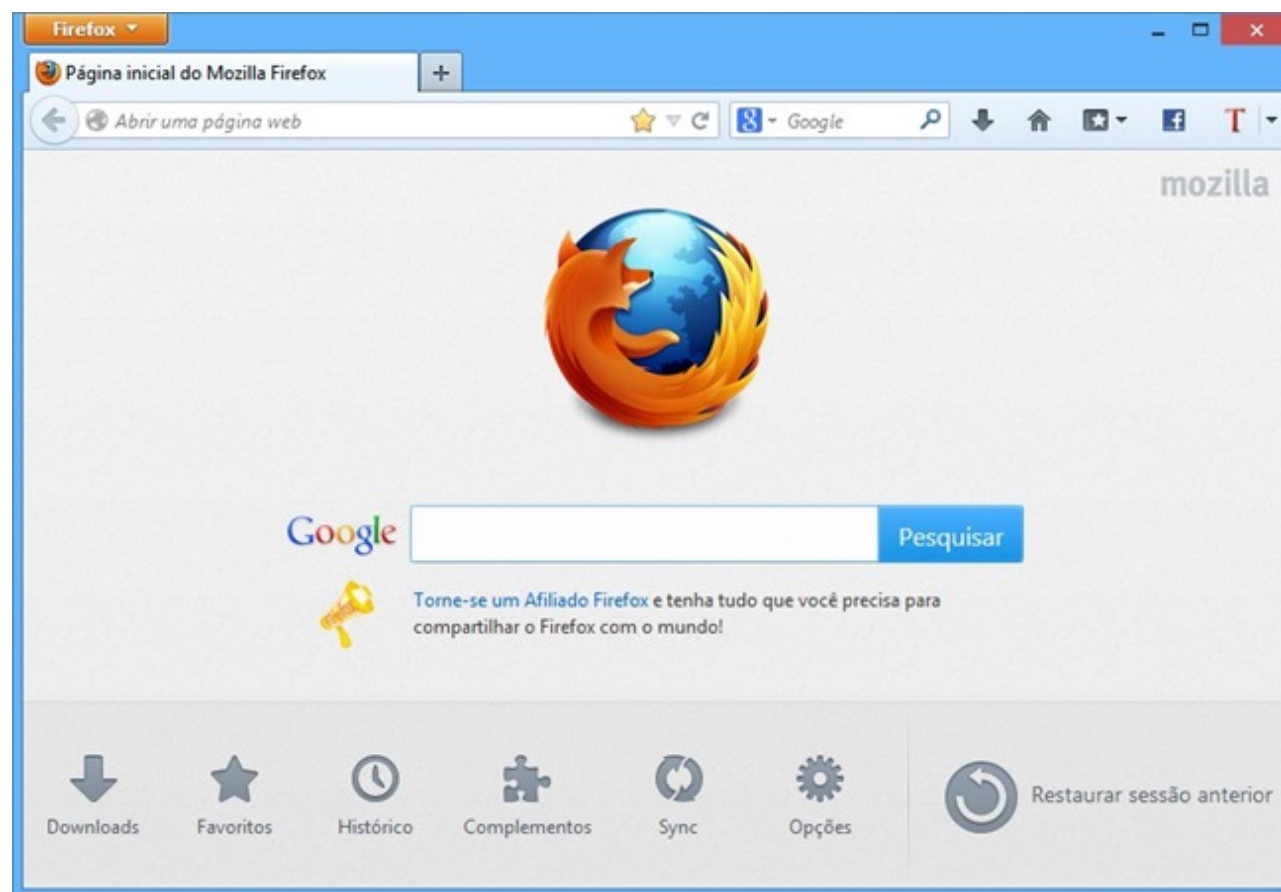
1 – Confiar na Resolução de Domínios?



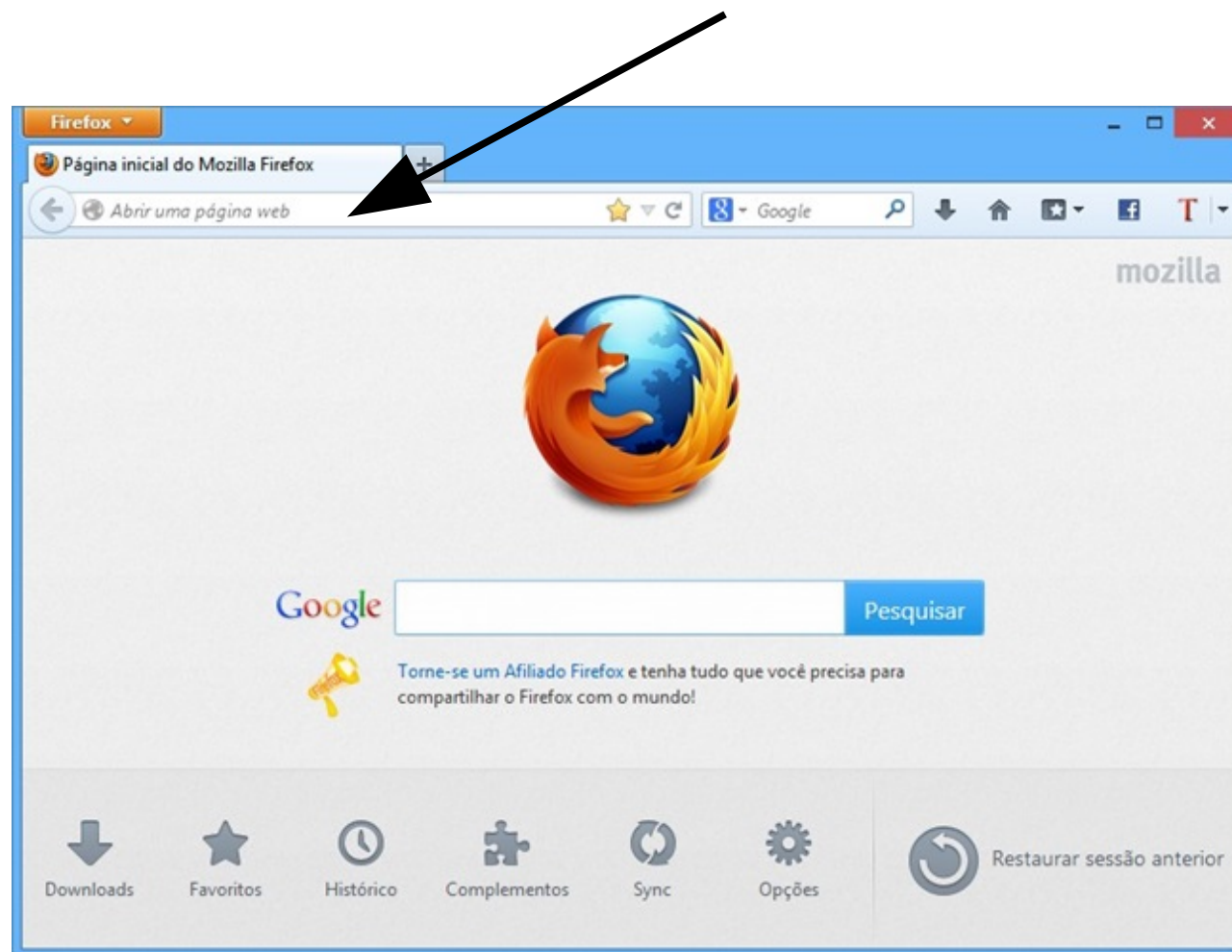
1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?



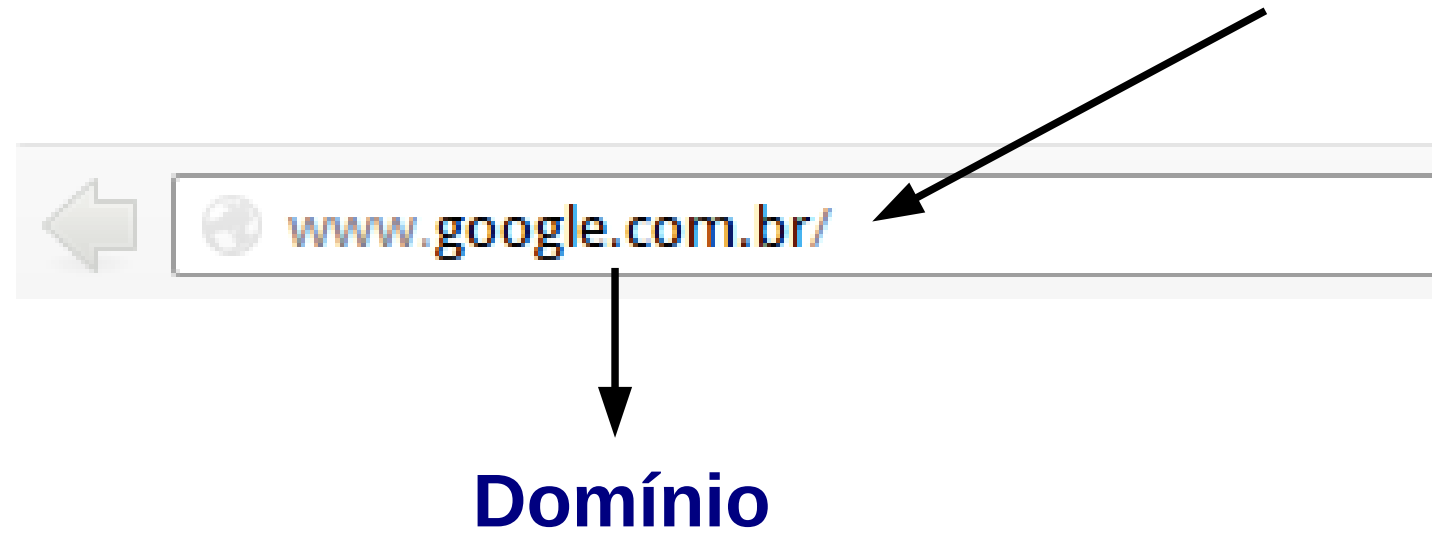
1 – Confiar na Resolução de Domínios?



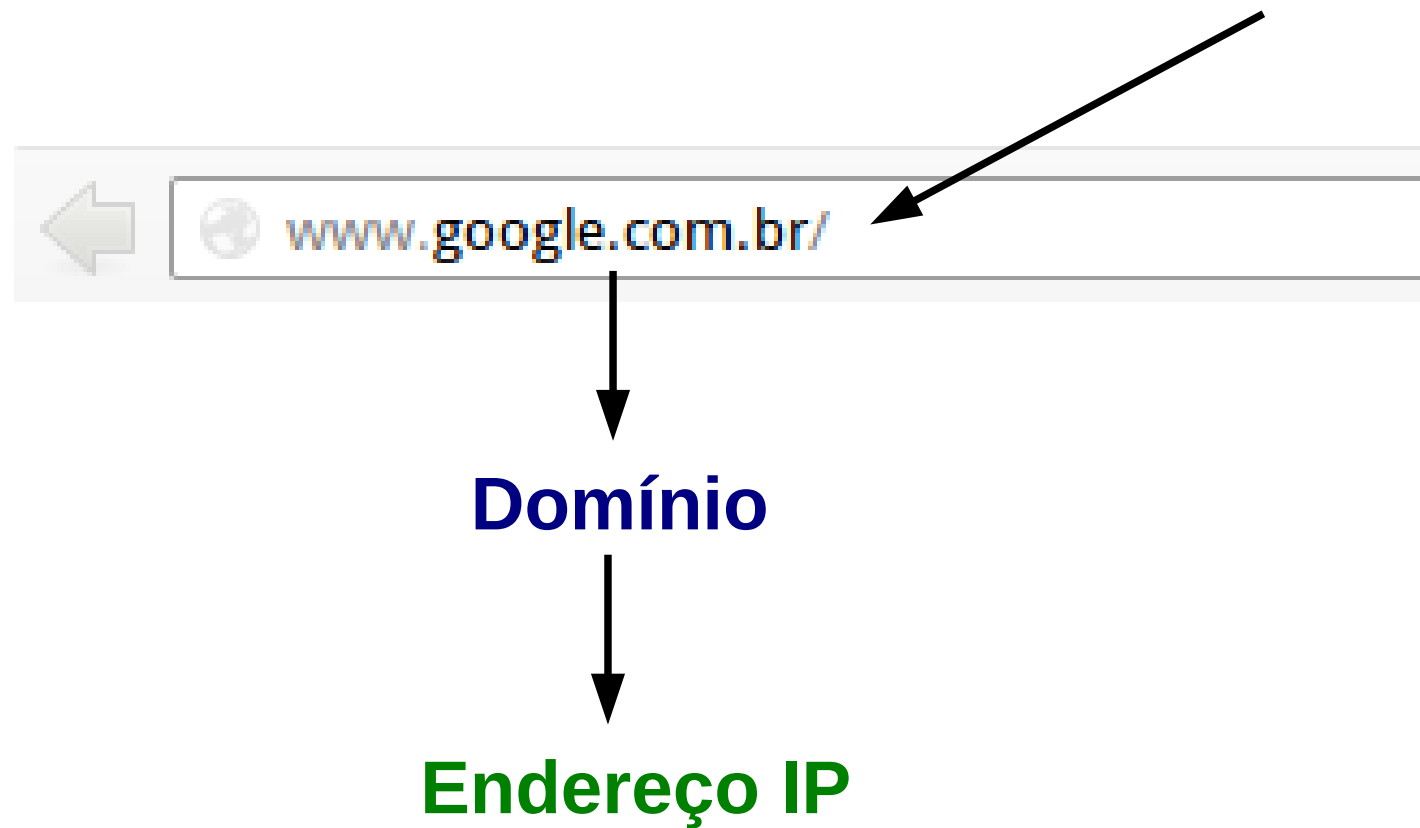
1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?



1 – Confiar na Resolução de Domínios?

Resolver o domínio

www.google.com.br

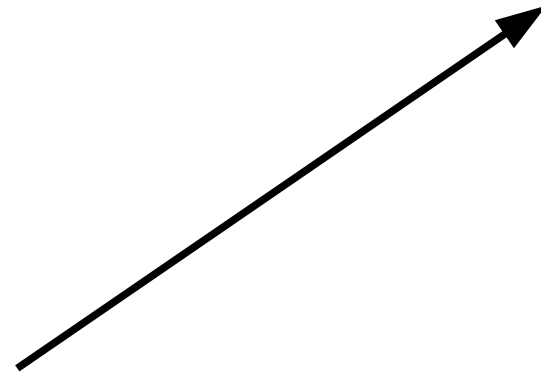
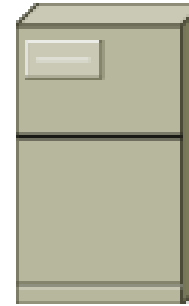
Para o endereço IP

74.125.234.23



1 – Confiar na Resolução de Domínios?

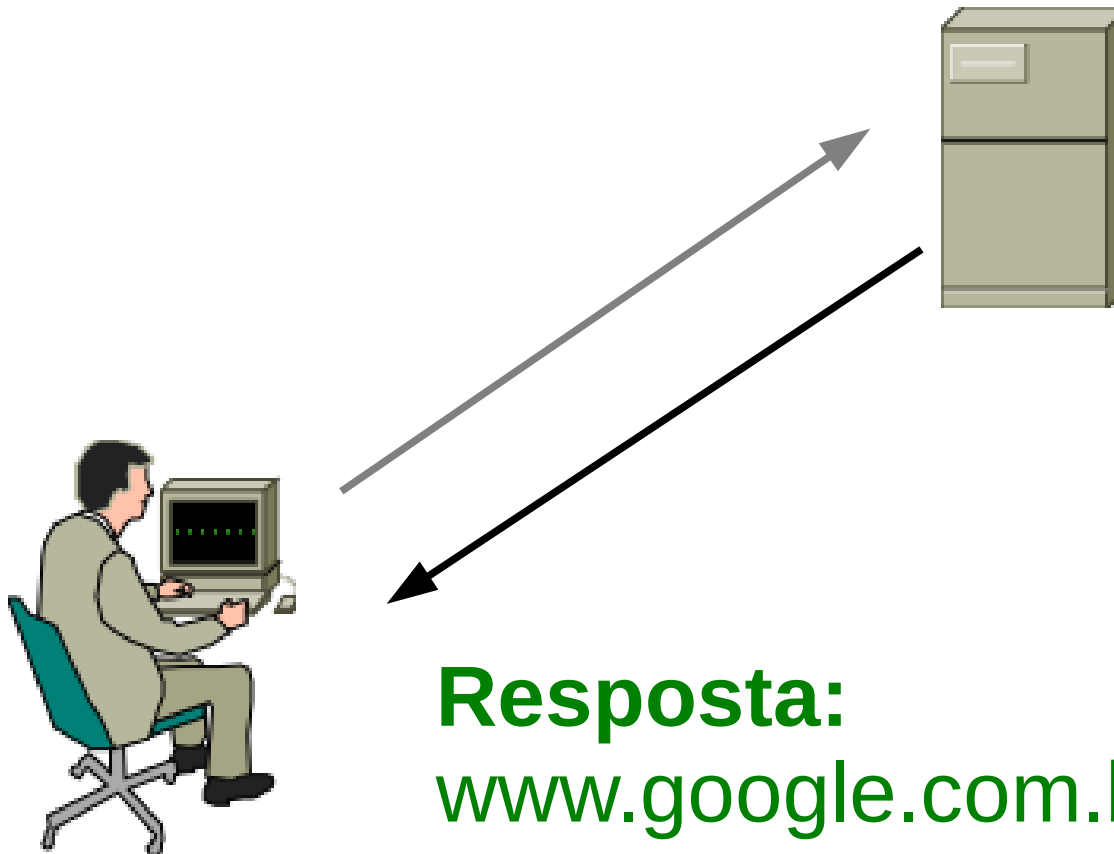
Servidor DNS



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

1 – Confiar na Resolução de Domínios?

Servidor DNS

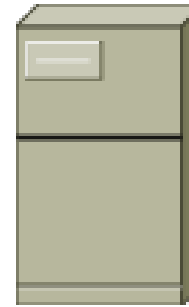


Resposta:

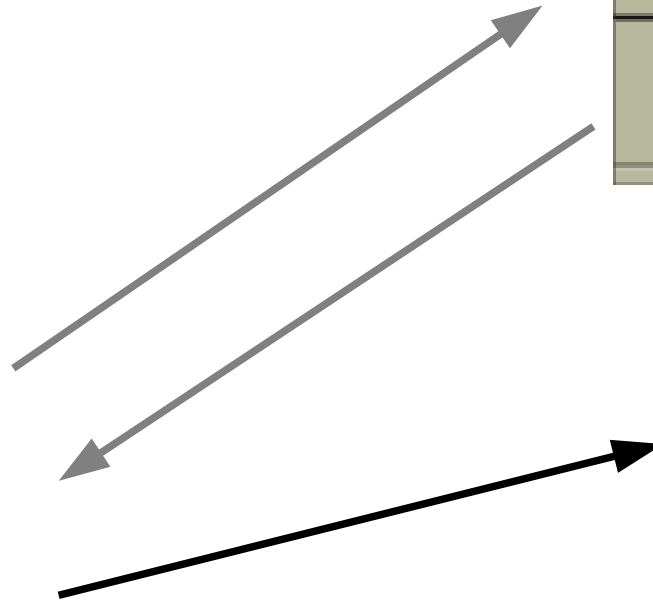
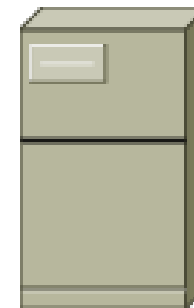
www.google.com.br = 74.125.234.23

1 – Confiar na Resolução de Domínios?

Servidor DNS



Servidor WEB

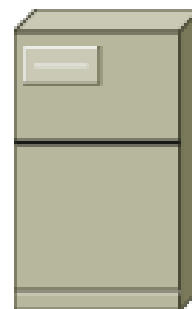


Solicitação:

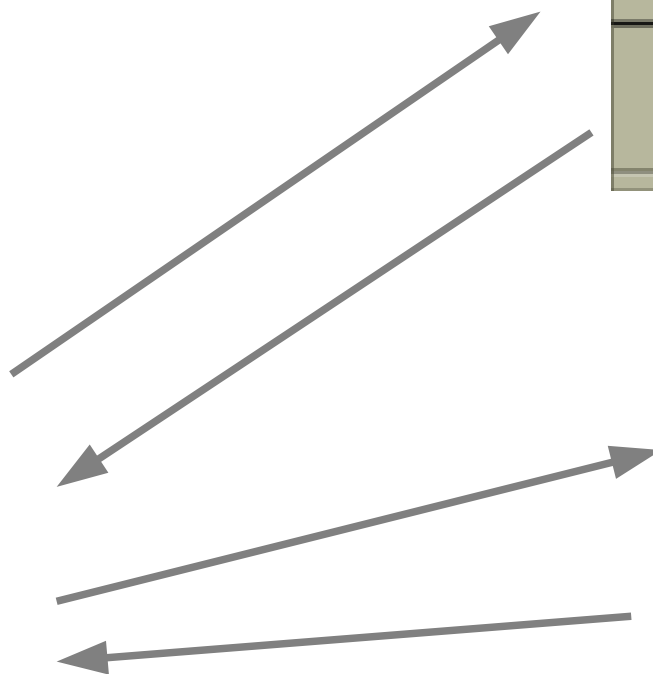
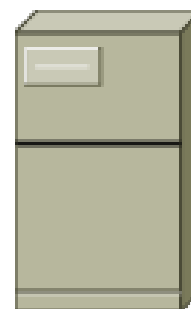
Página web em 74.125.234.23!

1 – Confiar na Resolução de Domínios?

Servidor DNS



Servidor WEB



Resposta:

`<html><head>...</html>`

1 – Confiar na Resolução de Domínios?

Google
Brasil



Pesquisa Google

Estou com sorte

1 – Confiar na Resolução de Domínios?

Internauta



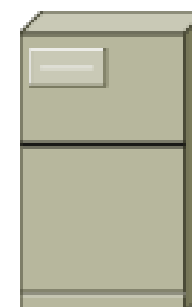
PERGUNTA



RESPOSTA



Servidor DNS

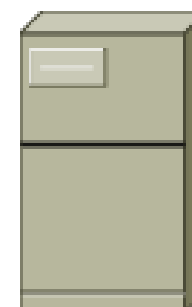


1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



PERGUNTA



RESPOSTA

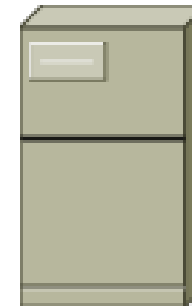


1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



PERGUNTA



RESPOSTA



1 – Confiar na Resolução de Domínios?

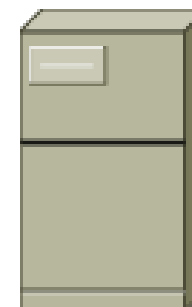
Internauta



PERGUNTA



Servidor DNS



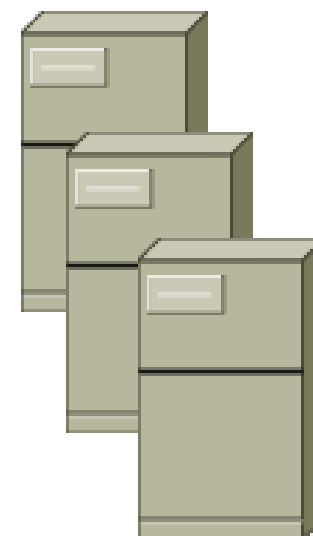
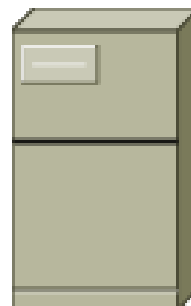
1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS

PERGUNTA



Servidores DNS

1 – Confiar na Resolução de Domínios?

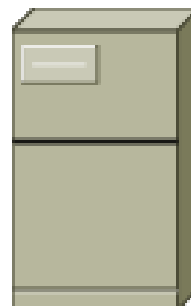
Internauta



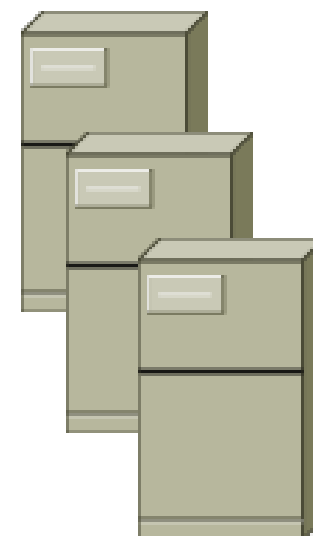
PERGUNTA



Servidor DNS



PERGUNTA



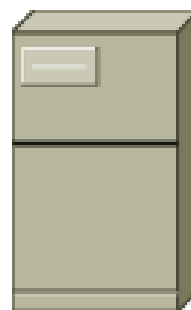
Servidores DNS

1 – Confiar na Resolução de Domínios?

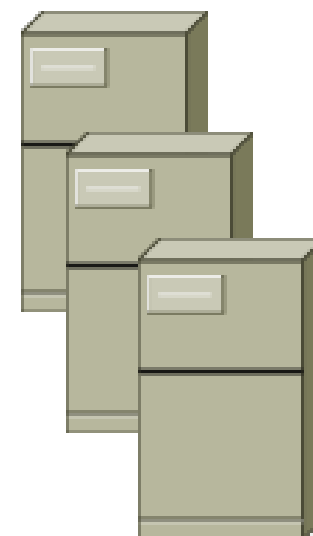
Internauta



Servidor DNS



?



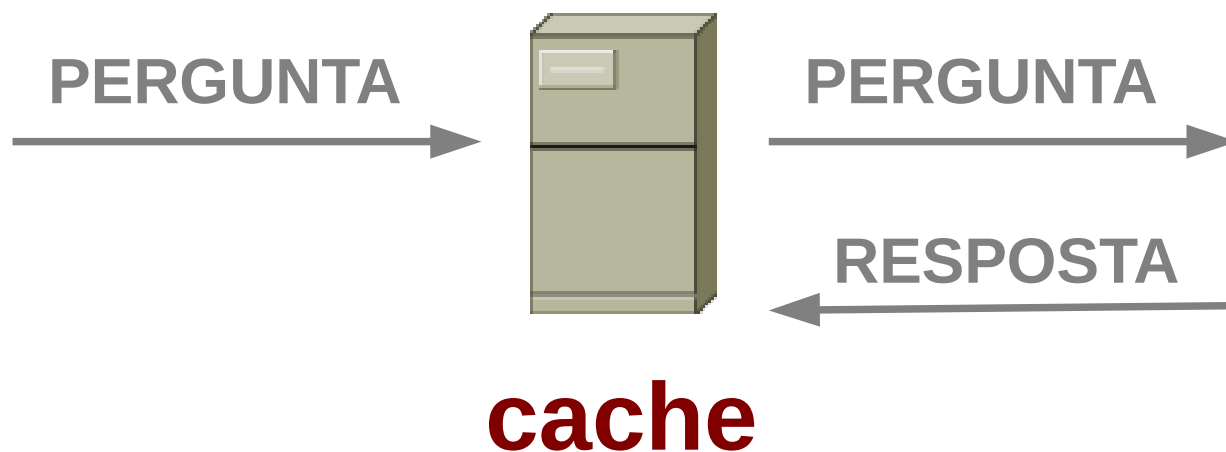
Servidores DNS

1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



Servidores DNS

1 – Confiar na Resolução de Domínios?

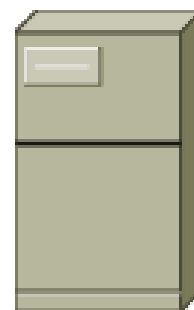
Internauta

Servidor DNS



PERGUNTA

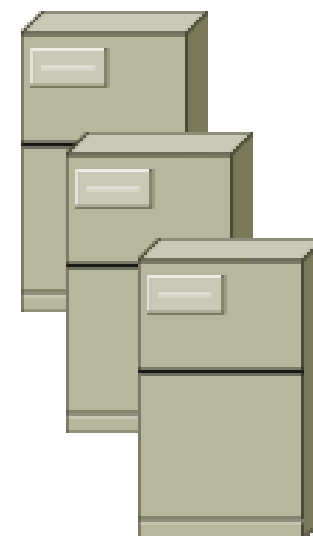
RESPOSTA



cache

PERGUNTA

RESPOSTA



Servidores DNS

1 – Confiar na Resolução de Domínios?

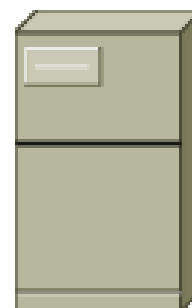
Internauta

Servidor DNS



PERGUNTA

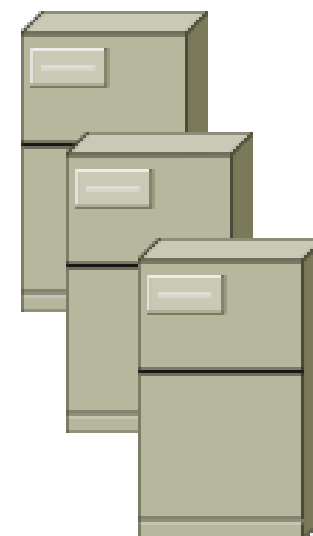
RESPOSTA



cache

PERGUNTA

RESPOSTA



Servidores DNS

CVE-2008-1447

DNS Cache Poisoning

Dan Kaminsky

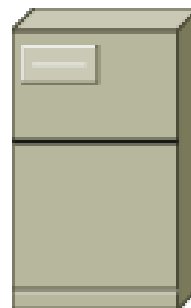
- Servidores DNSs Vulneráveis
- Windows
- Unix/Linux
- Dispositivos de redes

1 – Confiar na Resolução de Domínios?

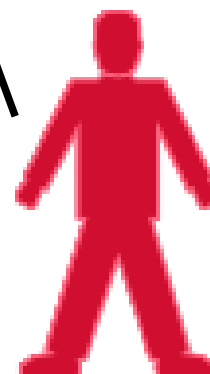
Internauta



Servidor DNS



PERGUNTAS



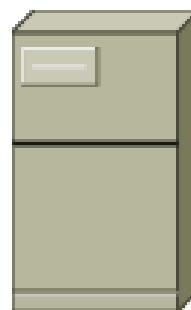
Atacante

1 – Confiar na Resolução de Domínios?

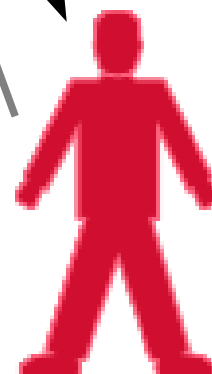
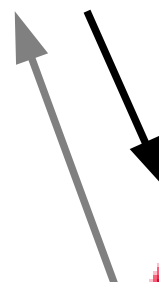
Internauta



Servidor DNS



RESPOSTAS



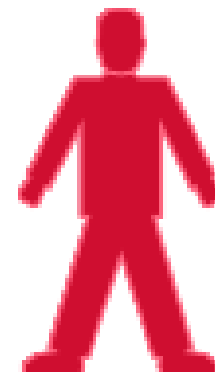
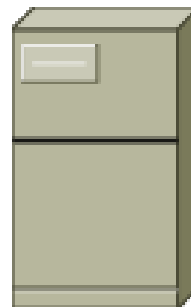
Atacante

1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



Atacante

INFORMAÇÕES

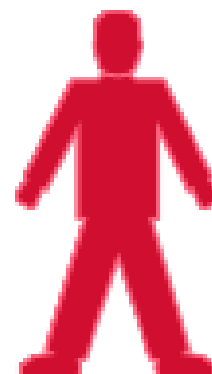
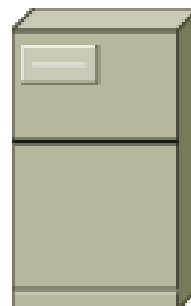
- Porta
- ID

1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



www.banco.com.br
IP = 166.66.66.6

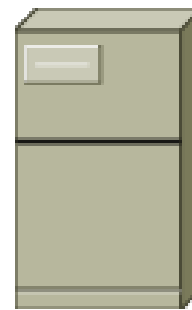
Atacante

1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



Atacante

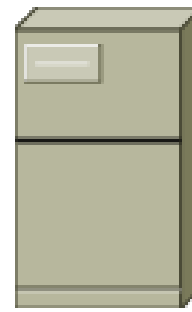
www.banco.com.br
IP = 166.66.66.6

1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



Atacante

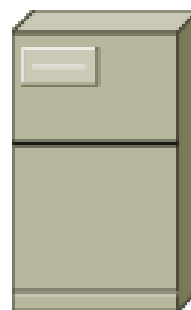
www.banco.com.br
IP = 166.66.66.6

1 – Confiar na Resolução de Domínios?

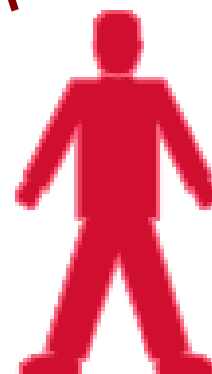
Internauta



Servidor DNS



ataque



Atacante

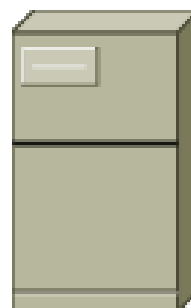
www.banco.com.br
IP = 166.66.66.6

1 – Confiar na Resolução de Domínios?

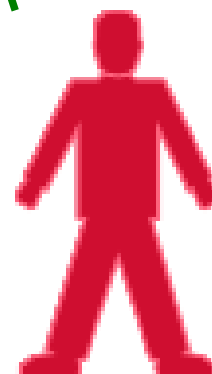
Internauta



Servidor DNS



Cache:
Banco.com.br → 166.66.66.6



www.banco.com.br
IP = 166.66.66.6

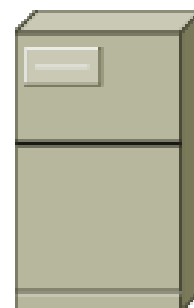
Atacante

1 – Confiar na Resolução de Domínios?

Internauta

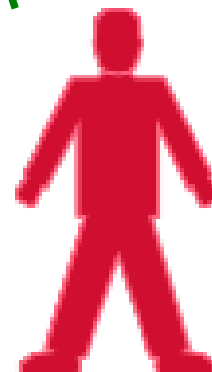


Servidor DNS



Cache:
Banco.com.br → 166.66.66.6

ataque



www.banco.com.br
IP = 166.66.66.6

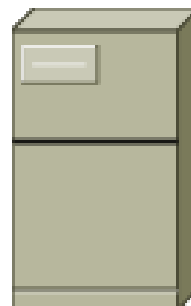
Atacante

1 – Confiar na Resolução de Domínios?

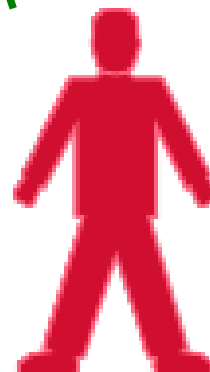
Internauta



Servidor DNS



Cache:
Banco.com.br → 166.66.66.6



www.banco.com.br
IP = 166.66.66.6

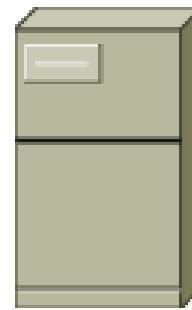
Atacante

1 – Confiar na Resolução de Domínios?

Internauta



Servidor DNS



Cache:

Banco.com.br → 166.66.66.6

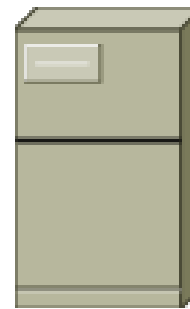
1 – Confiar na Resolução de Domínios?

Internauta

Servidor DNS



Banco.com.br?



Cache:

Banco.com.br → 166.66.66.6

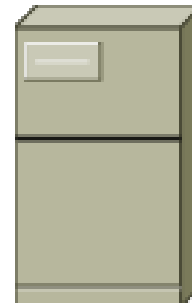
1 – Confiar na Resolução de Domínios?

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

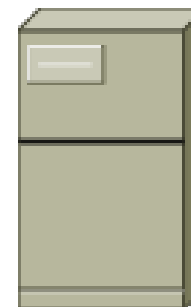


1 – Confiar na Resolução de Domínios?

Internauta

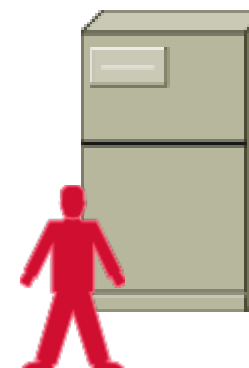


Servidor Web Banco



123.31.123.31

Servidor Web Atacante



166.66.66.6

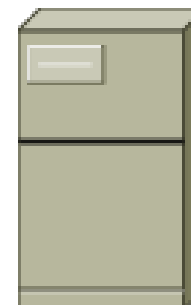
1 – Confiar na Resolução de Domínios?

Internauta



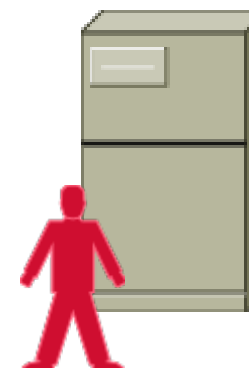
Accessar 166.66.66.6

Servidor Web Banco



123.31.123.31

Servidor Web Atacante



166.66.66.6

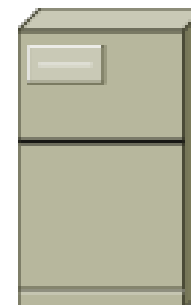
1 – Confiar na Resolução de Domínios?

Internauta



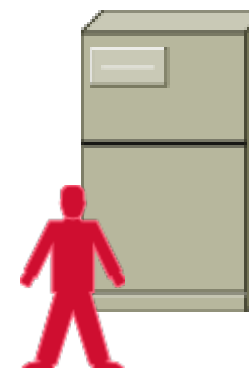
Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31

Servidor Web Atacante



166.66.66.6

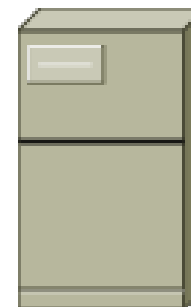
1 – Confiar na Resolução de Domínios?

Internauta



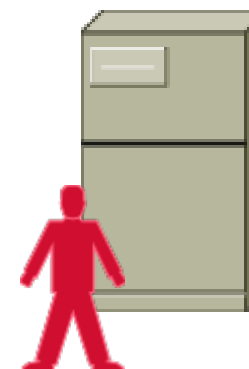
Acessar 166.66.66.6

Servidor Web Banco

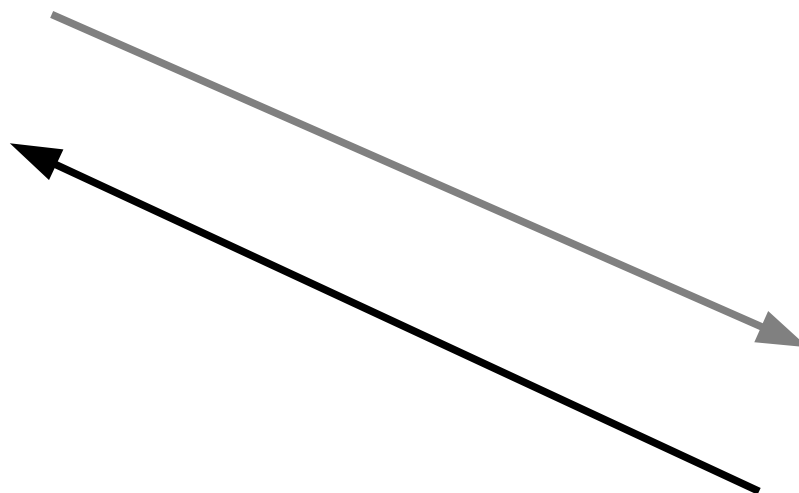


123.31.123.31

Servidor Web Atacante



166.66.66.6



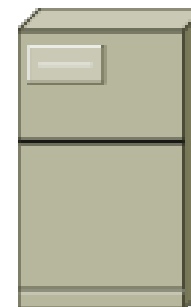
1 – Confiar na Resolução de Domínios?

Internauta



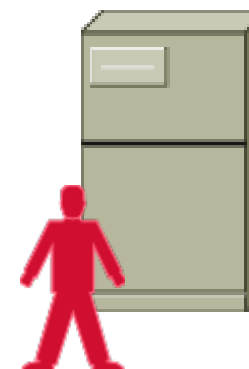
Acessar 166.66.66.6

Servidor Web Banco

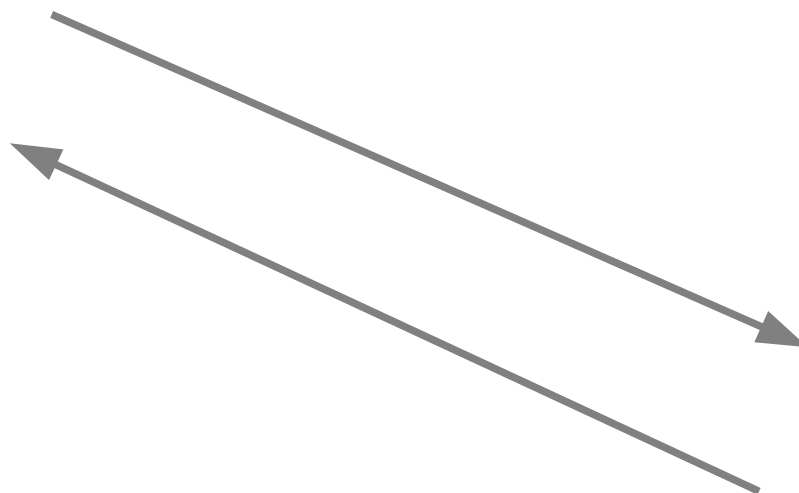


123.31.123.31

Servidor Web Atacante



166.66.66.6



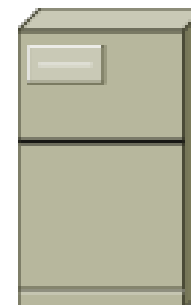
1 – Confiar na Resolução de Domínios?

Internauta



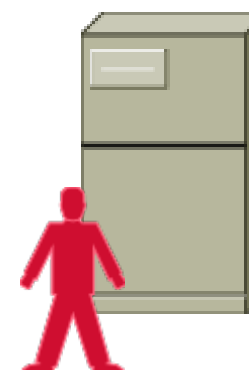
Acessar 166.66.66.6

Servidor Web Banco



123.31.123.31

Servidor Web Atacante



166.66.66.6

YOU HAVE BEEN
HACKED !

1 – Confiar na Resolução de Domínios?

Incidente de Segurança – Abril/2009

DNS - Provedor (Net)

WEB - Banco (Brad)



Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22 [✉ Email](#) [🖨 Print](#)

Site hospedado na Ásia usado para roubar senhas e credenciais.

Incidentes de Segurança

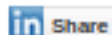
Malawi (domínios .mw)

Fev/2013

Sun, February 17th, 16:46 · Tefo Mohapi

**Malawi Google site hacked by
Bangladeshi hacker**

 **##humanipo**
Home to African Tech

 Share

 +1 0

Kenya (domínios .ke)

Abril/2013

Provavelmente DNS Poison

Solução:

Paliativa

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

1 – Confiar na Resolução de Domínios?

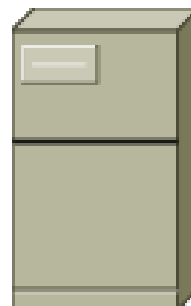
Internauta



PERGUNTA

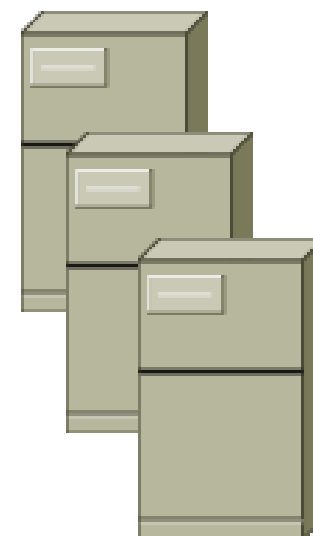


Servidor DNS



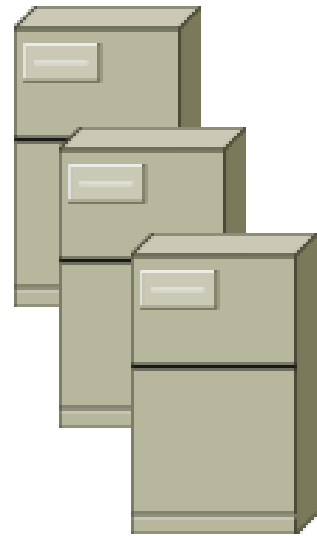
?

PERGUNTA



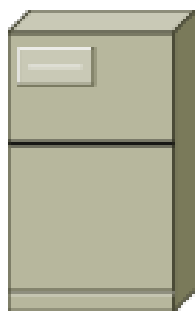
Servidores DNS

1 – Confiar na Resolução de Domínios?

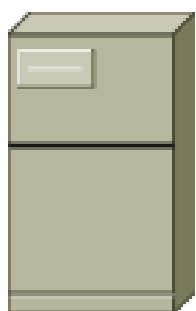


Servidores DNS

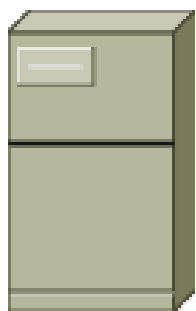
Servidores de DNS Raiz



A

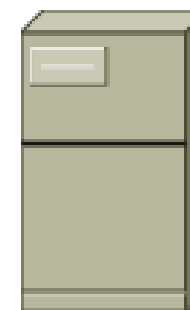


B



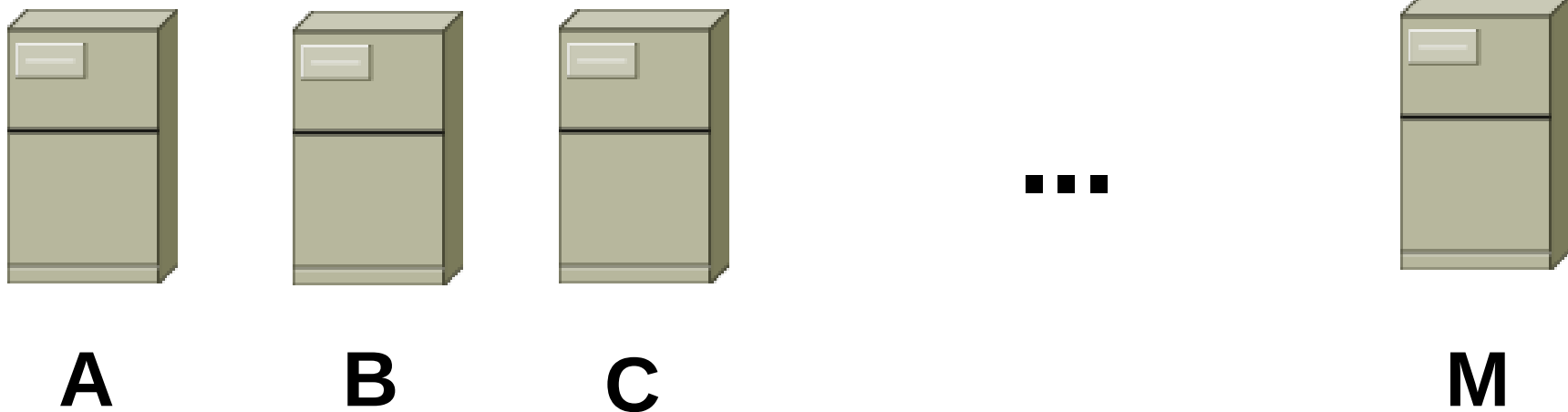
C

...



M

Servidores de DNS Raiz

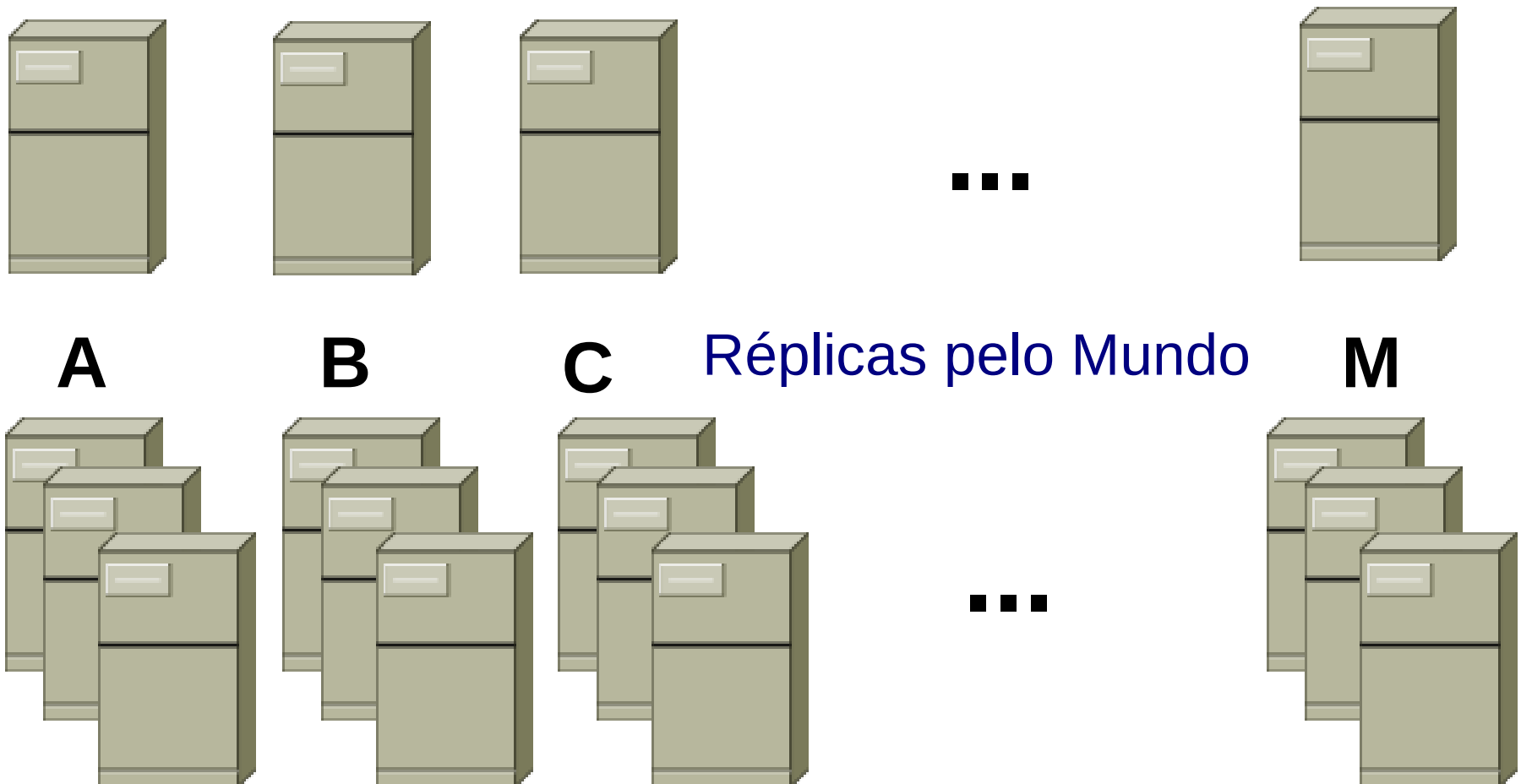


Maior parte nos EUA e na Europa

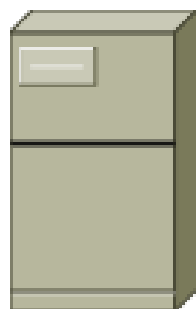
Domínios TLD → .com, .net, .org, .us, .br ...

1 – Confiar na Resolução de Domínios?

Servidores de DNS Raiz

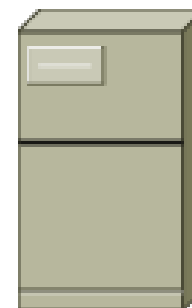


Incidente de Segurança

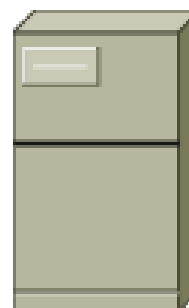


i

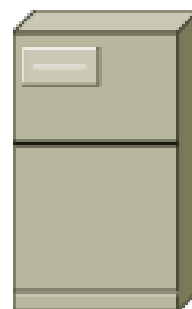
SUÉCIA



i

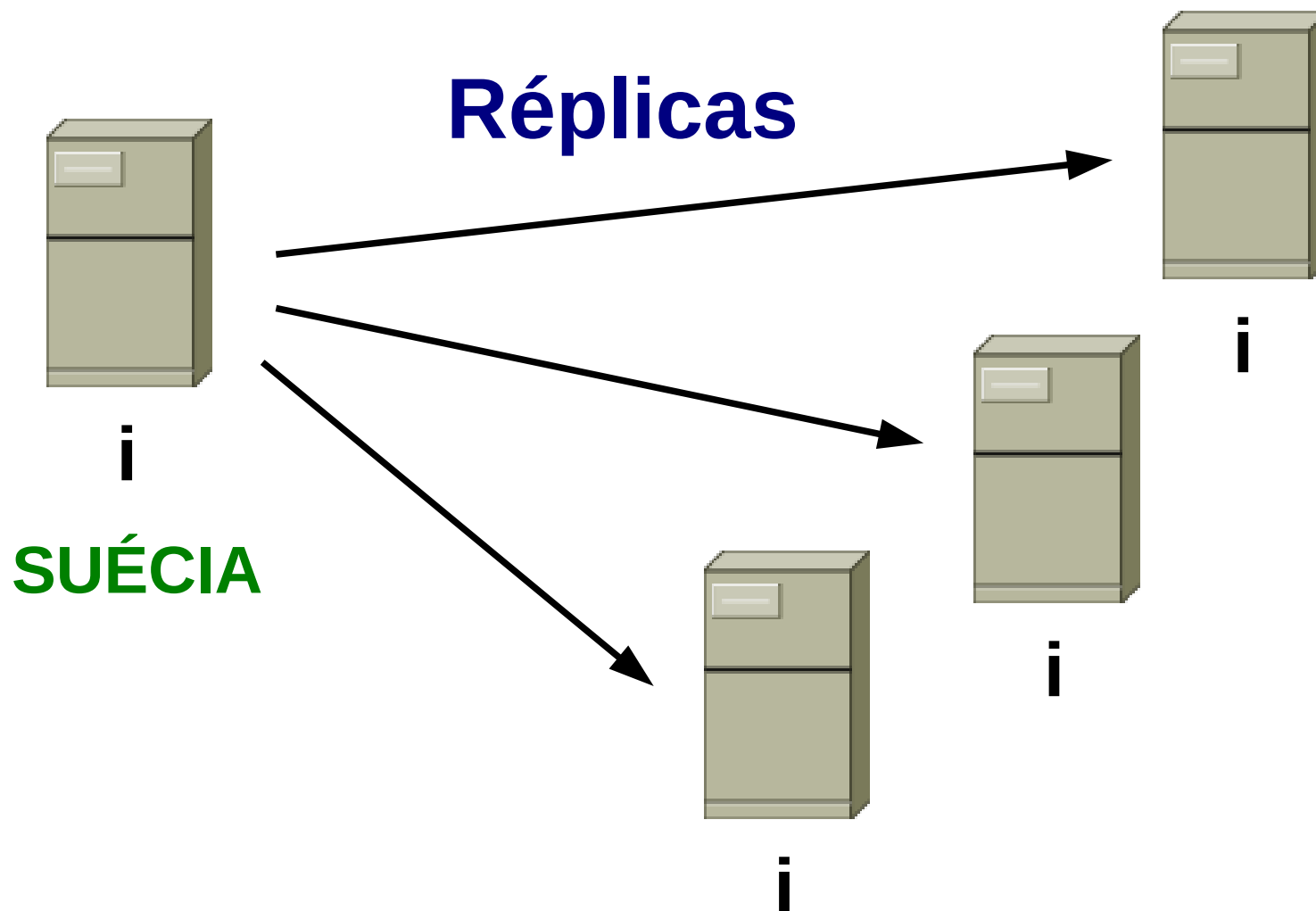


i

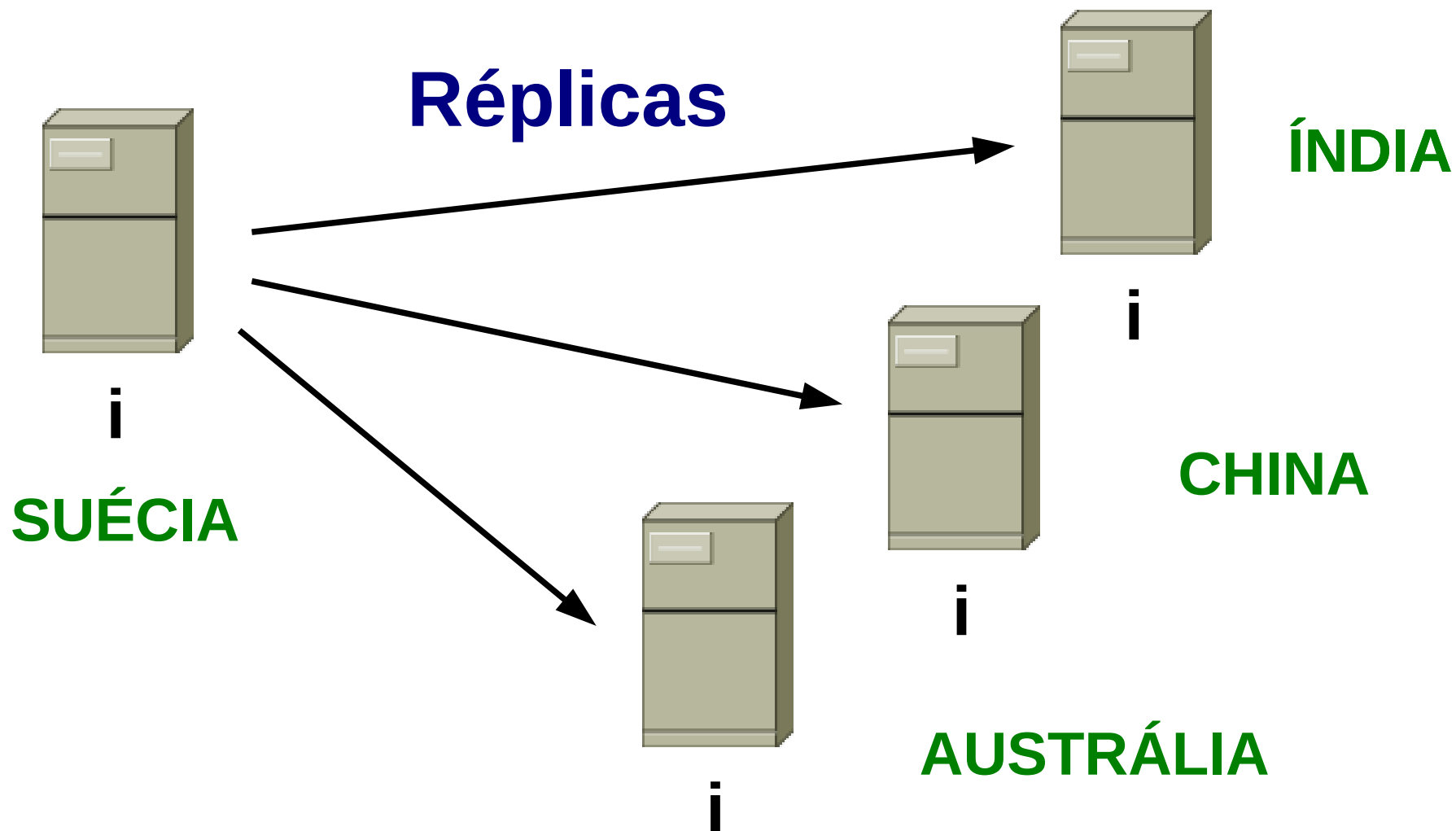


i

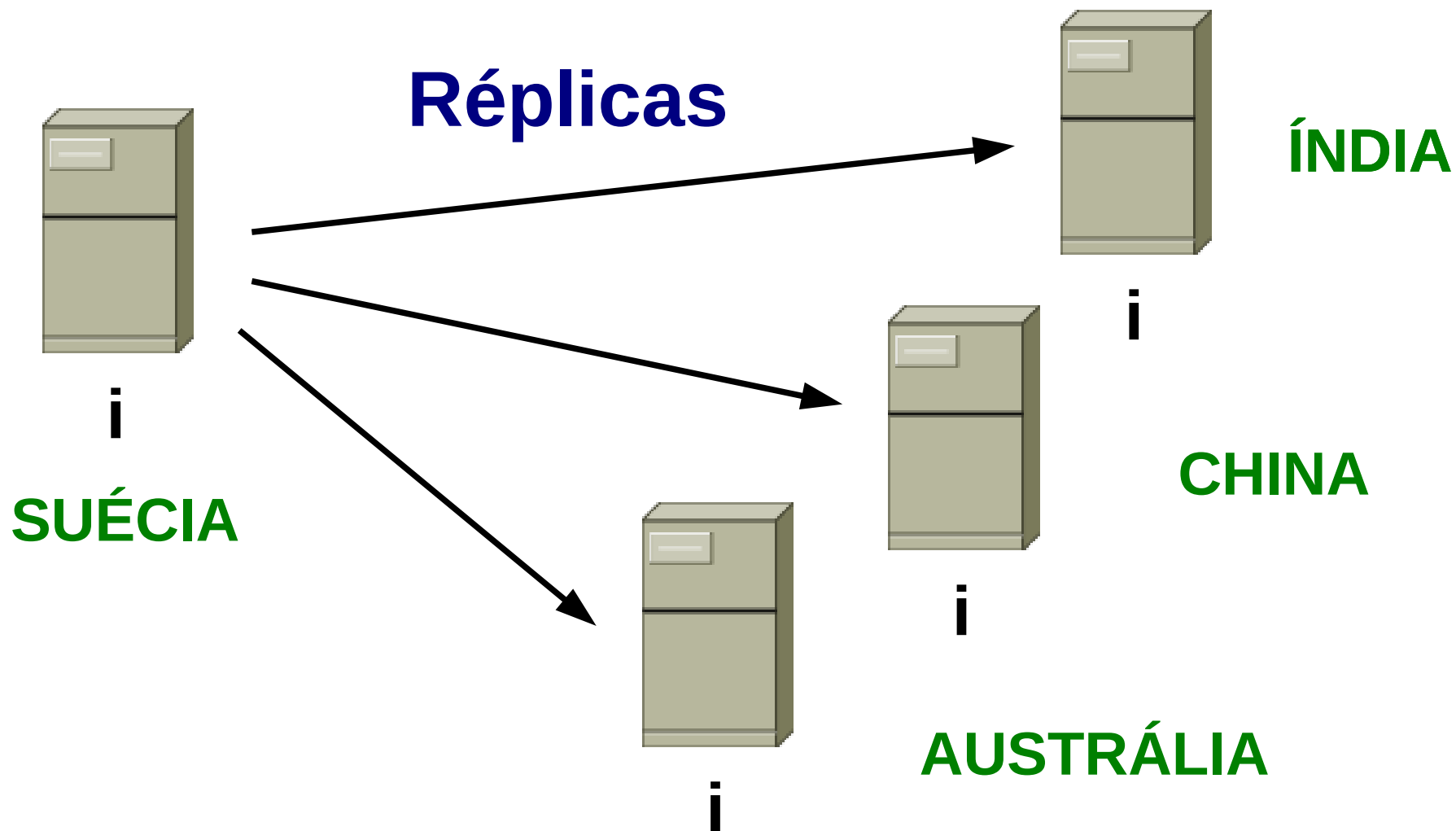
Incidente de Segurança



Incidente de Segurança



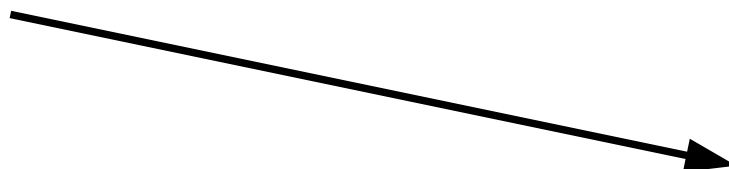
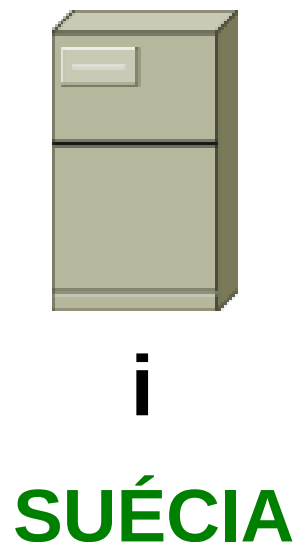
Incidente de Segurança



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?

Solução:

- Empresa Sueca cortou servidor raiz chinês
- Hoje poderia utilizar DNSSEC (DNS Seguro)
?!?

2 -

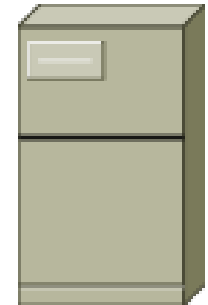
**Podemos confiar
no Roteamento
de Provedores?**

2 – Confiar no Roteamento Provedores?

Internauta



Servidor Web



2 – Confiar no Roteamento Provedores?

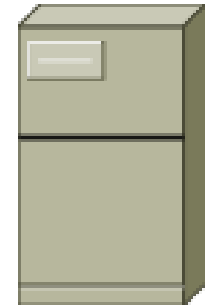
Internauta



Internet Protocol
1981

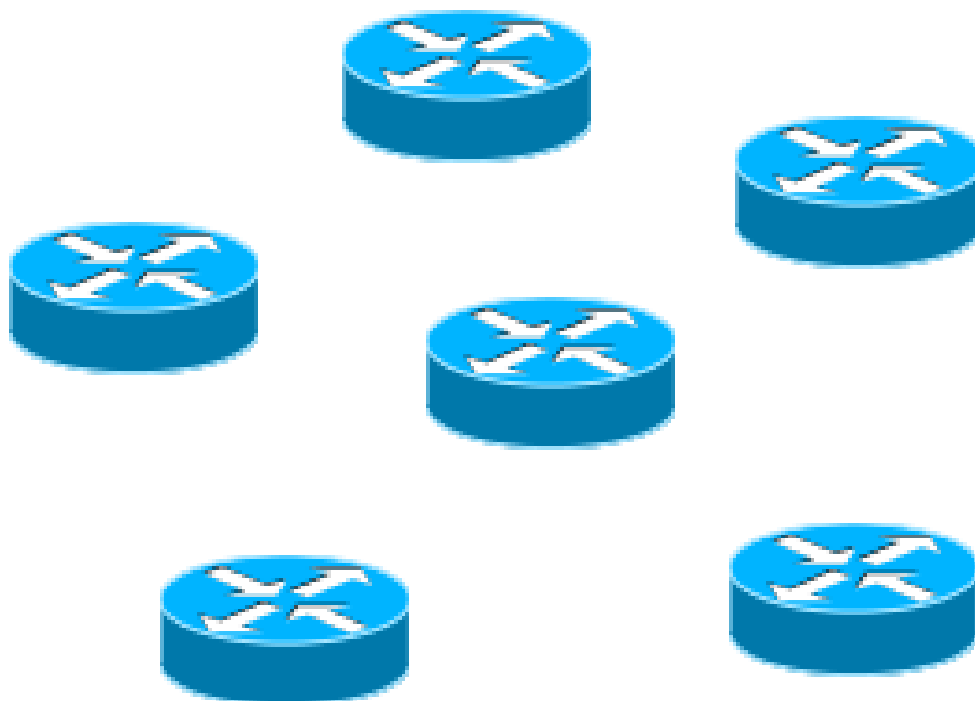
Documento RFC 781

Servidor Web

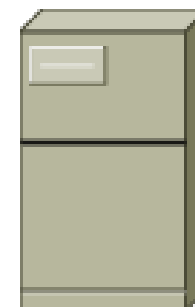


2 – Confiar no Roteamento Provedores?

Internauta

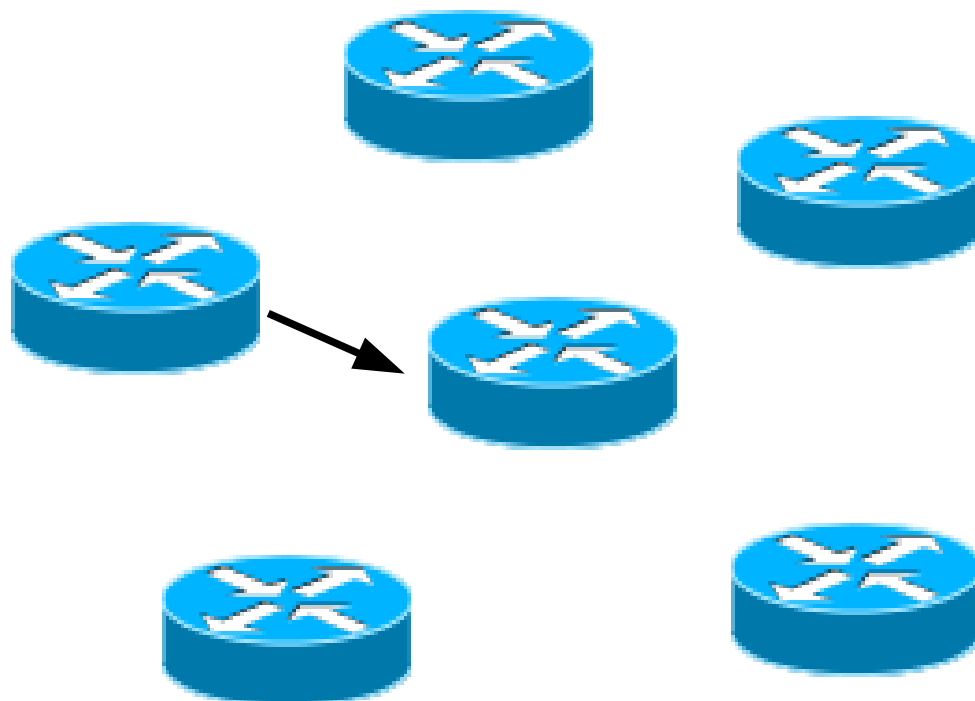


Servidor Web

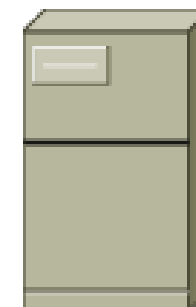


2 – Confiar no Roteamento Provedores?

Internauta

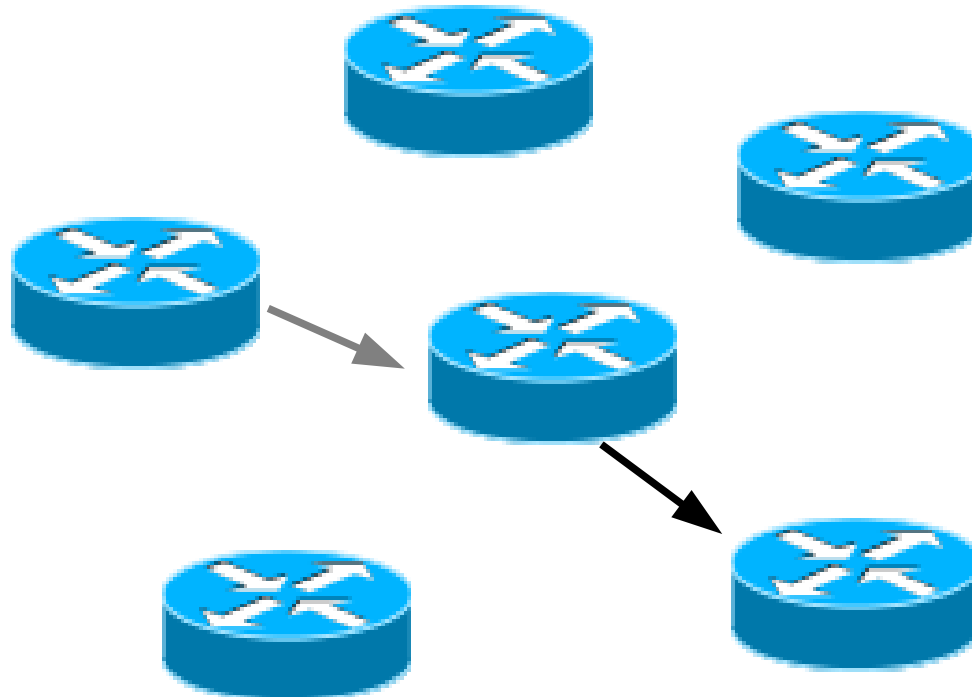


Servidor Web

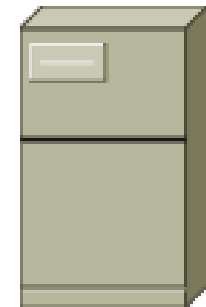


2 – Confiar no Roteamento Provedores?

Internauta

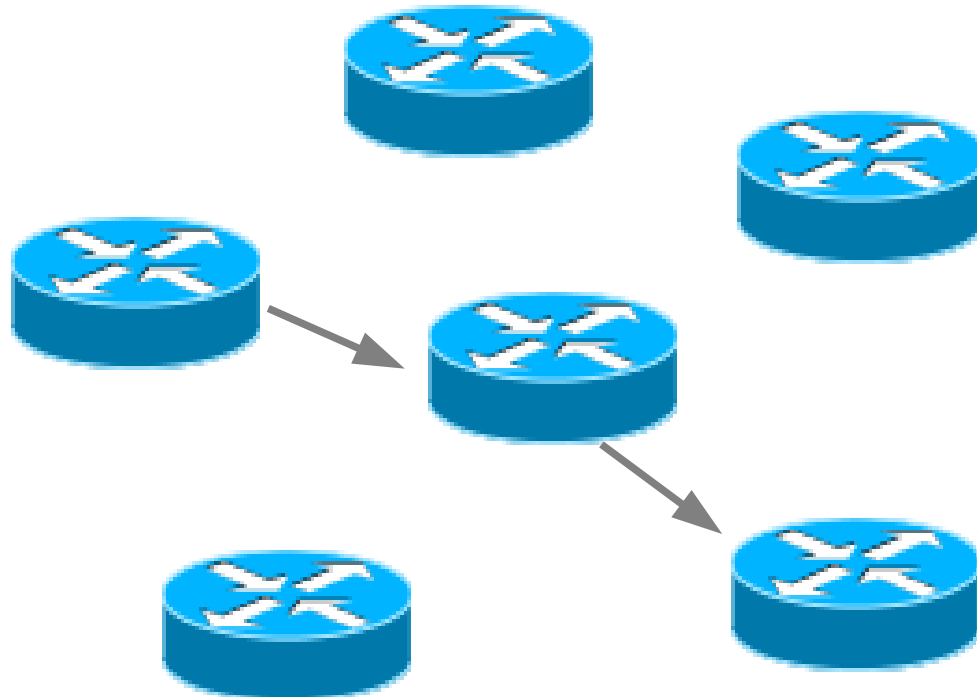


Servidor Web

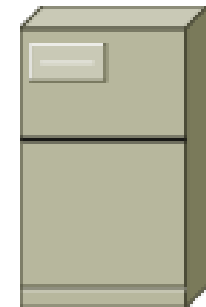


2 – Confiar no Roteamento Provedores?

Internauta

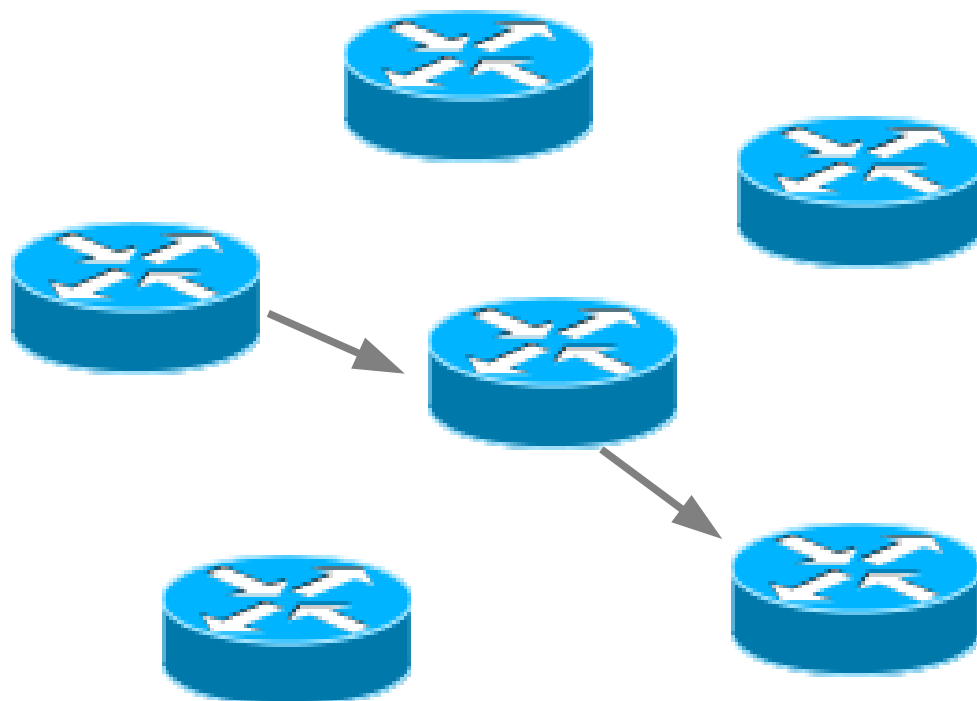


Servidor Web

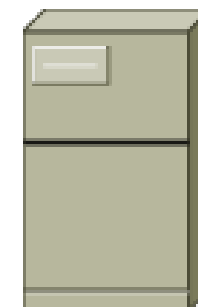


2 – Confiar no Roteamento Provedores?

Internauta

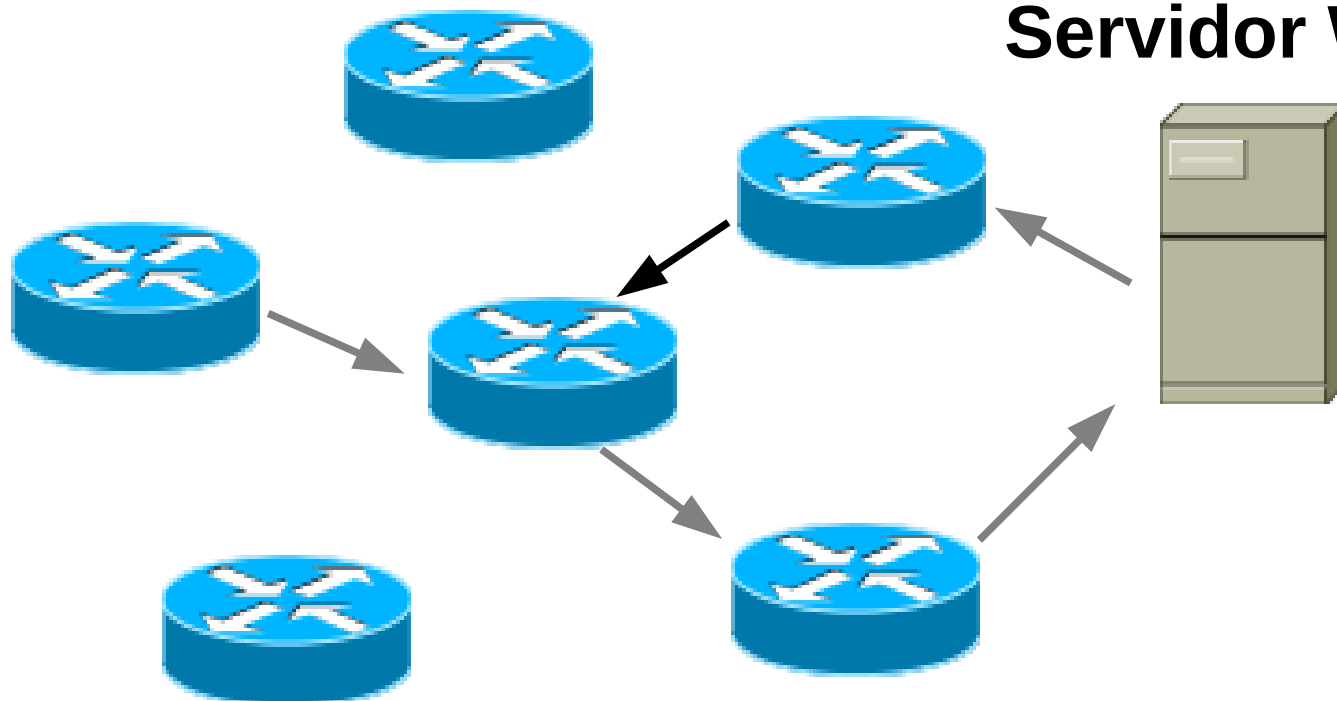


Servidor Web



2 – Confiar no Roteamento Provedores?

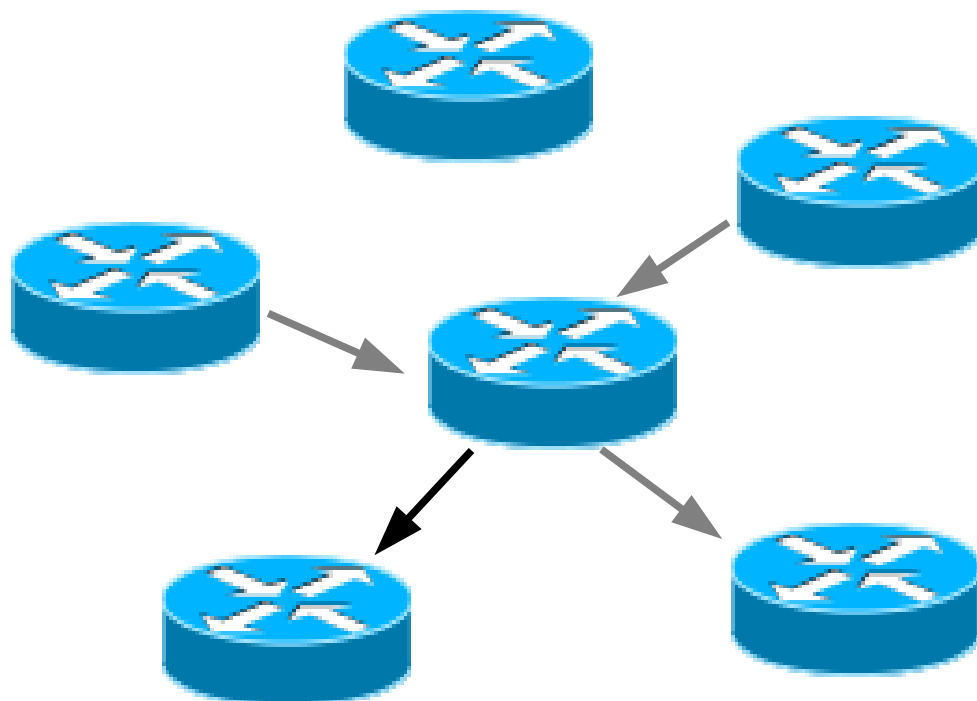
Internauta



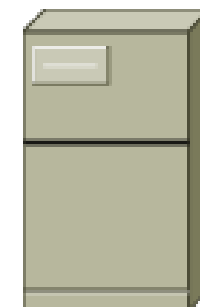
Servidor Web

2 – Confiar no Roteamento Provedores?

Internauta



Servidor Web

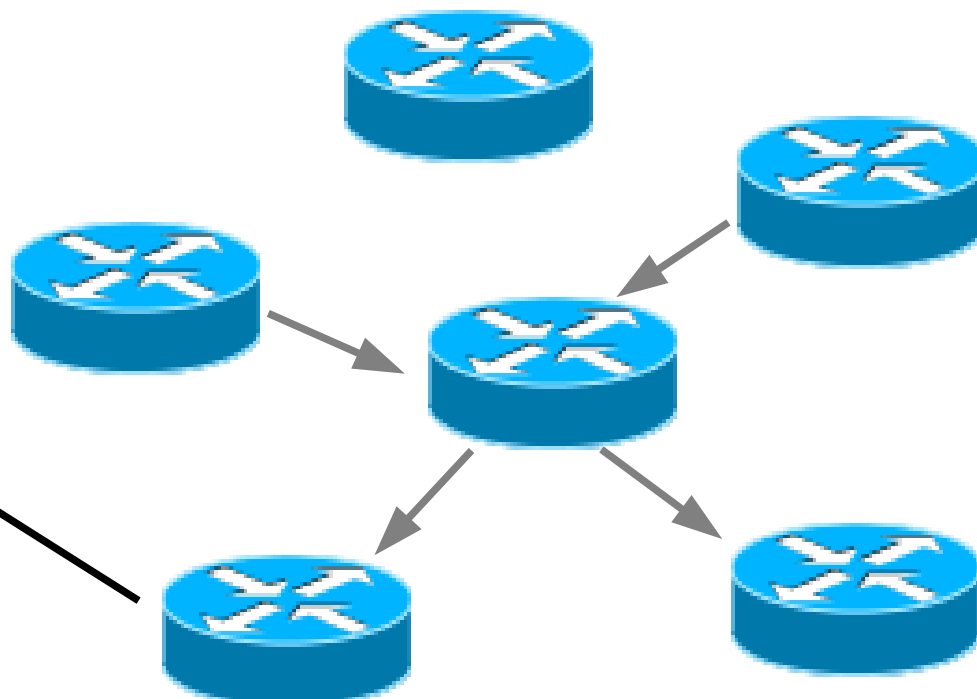
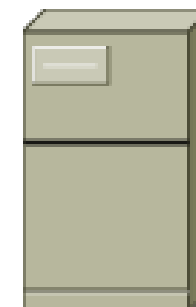


2 – Confiar no Roteamento Provedores?

Internauta



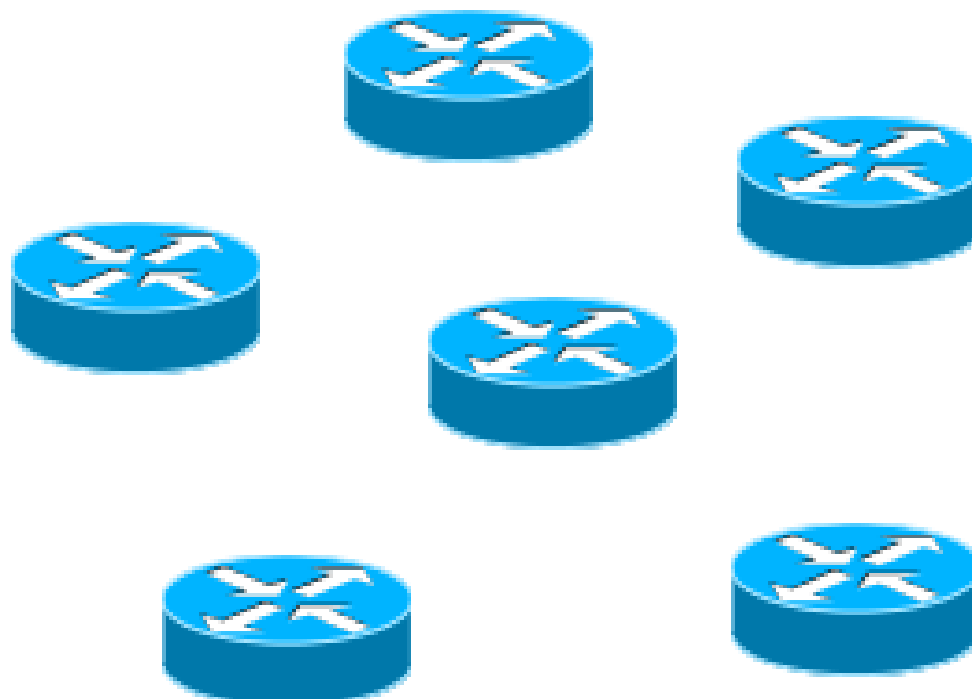
Servidor Web



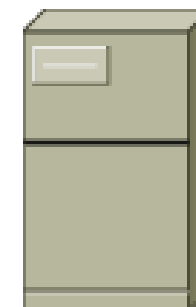
2 – Confiar no Roteamento Provedores?

ROTEAMENTO

Internauta



Servidor Web

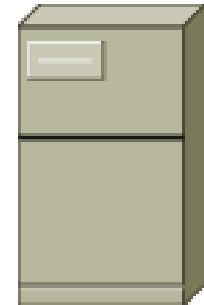


2 – Confiar no Roteamento Provedores?

Internauta

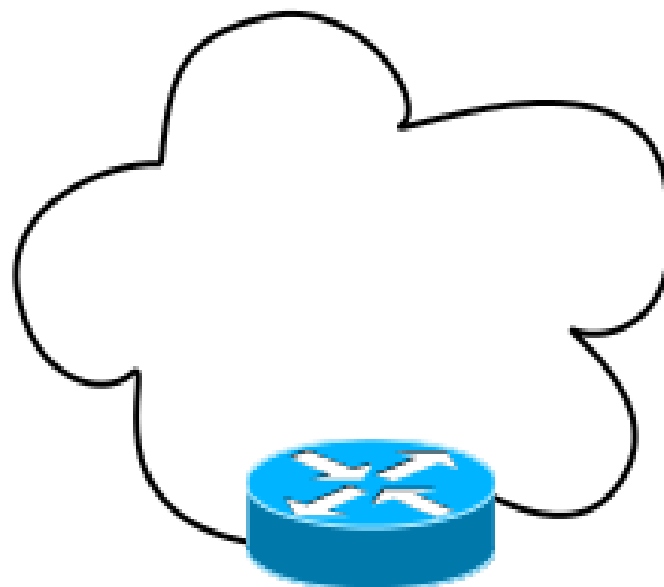


Servidor Web

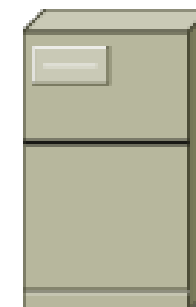


2 – Confiar no Roteamento Provedores?

Internauta

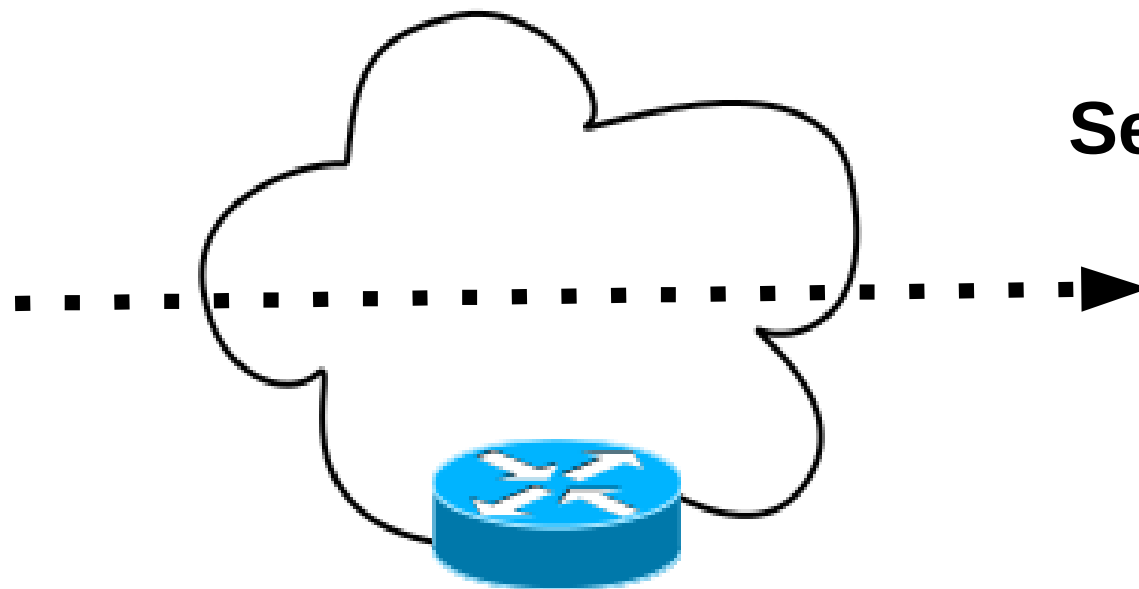


Servidor Web

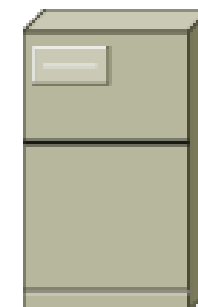


2 – Confiar no Roteamento Provedores?

Internauta

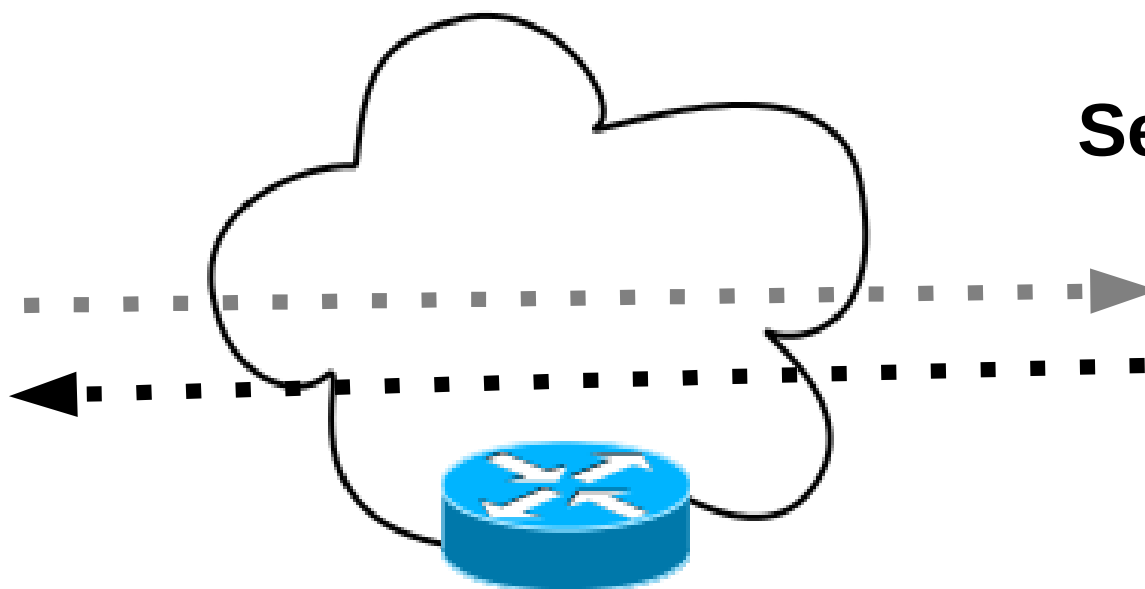


Servidor Web

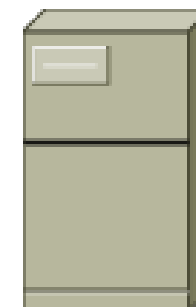


2 – Confiar no Roteamento Provedores?

Internauta

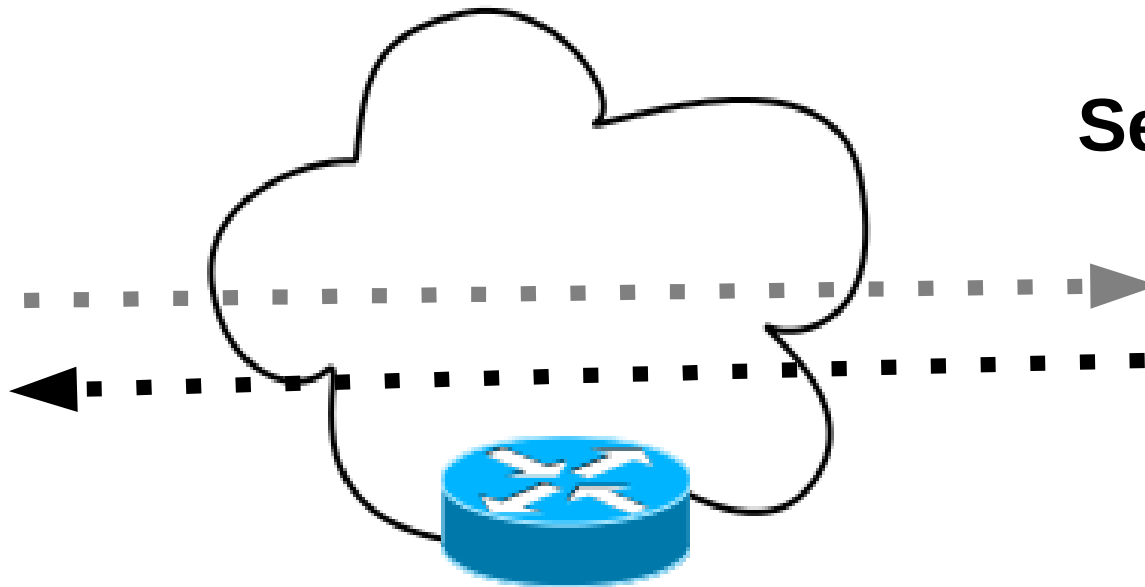


Servidor Web

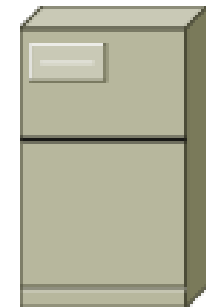


2 – Confiar no Roteamento Provedores?

Internauta

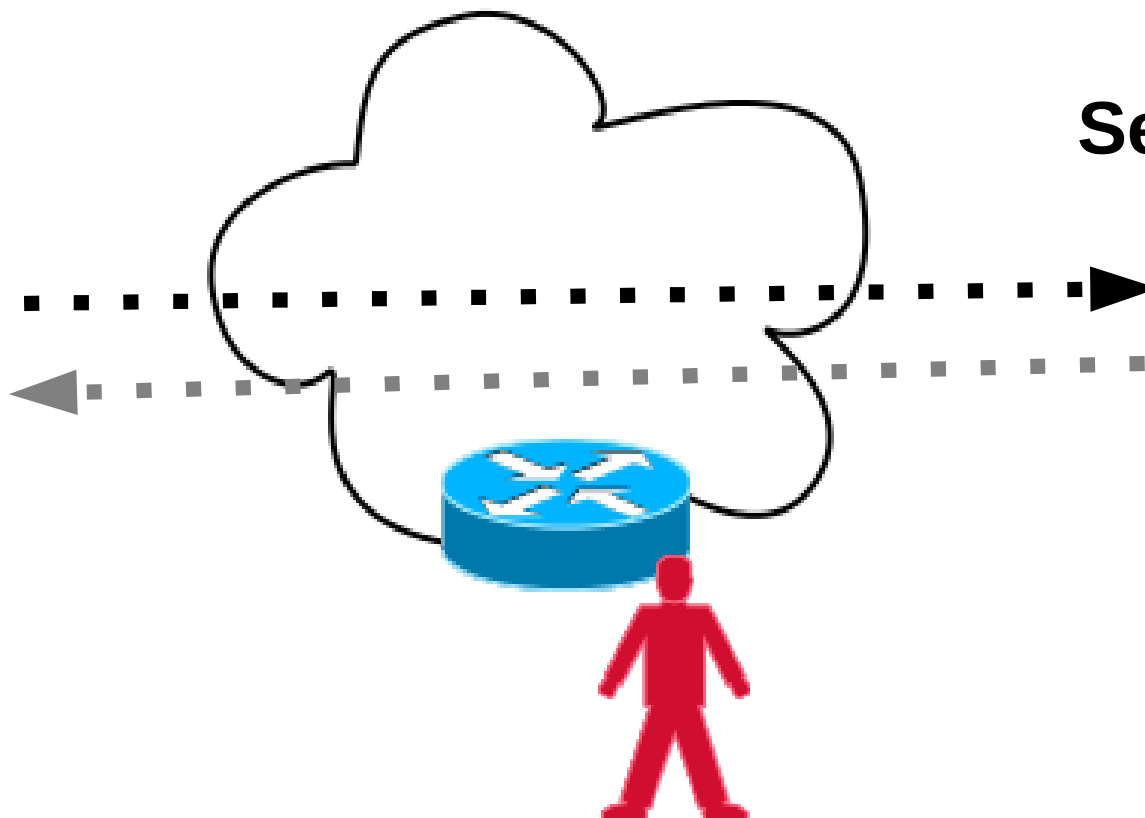


Servidor Web

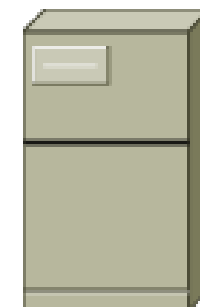


2 – Confiar no Roteamento Provedores?

Internauta

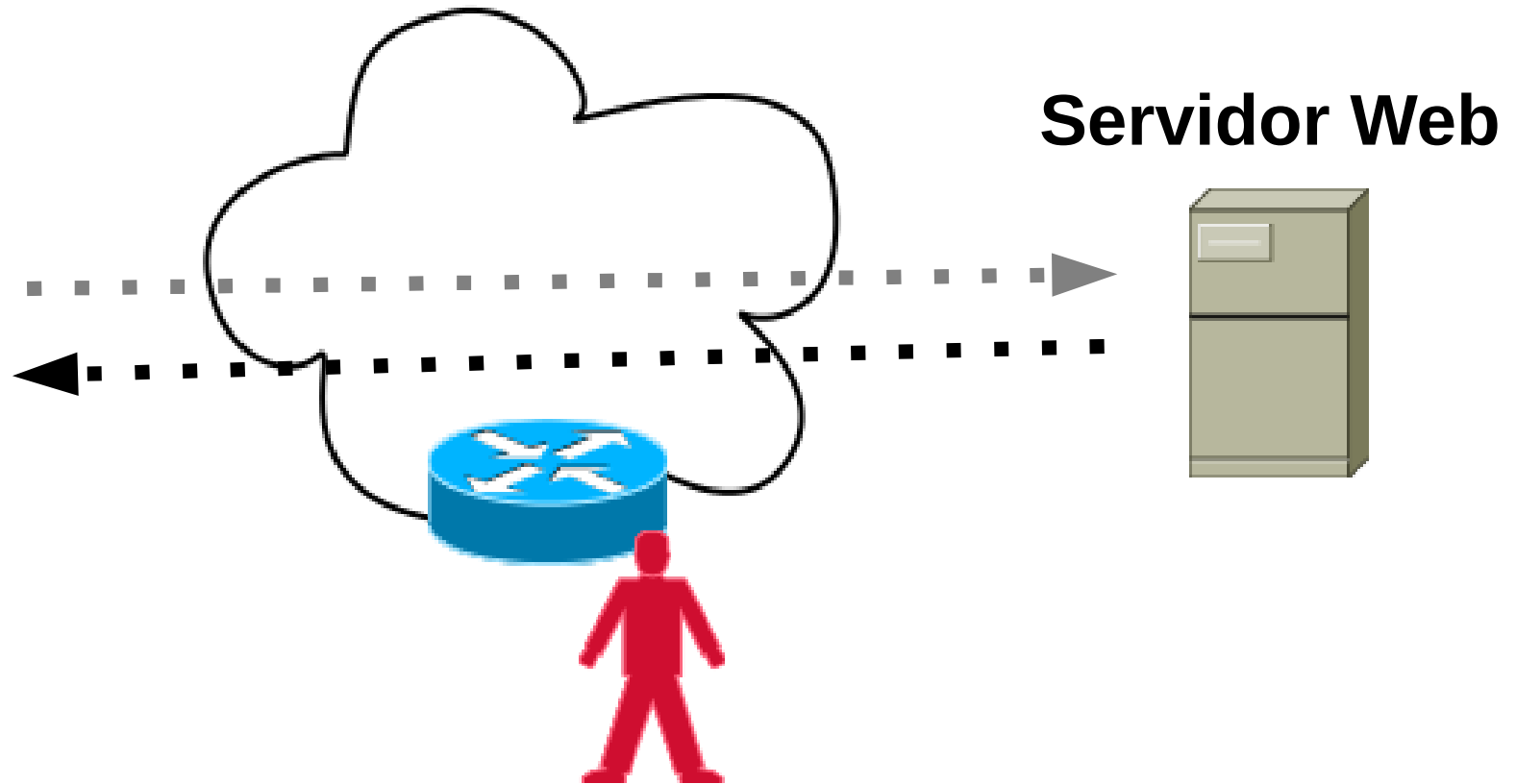


Servidor Web



2 – Confiar no Roteamento Provedores?

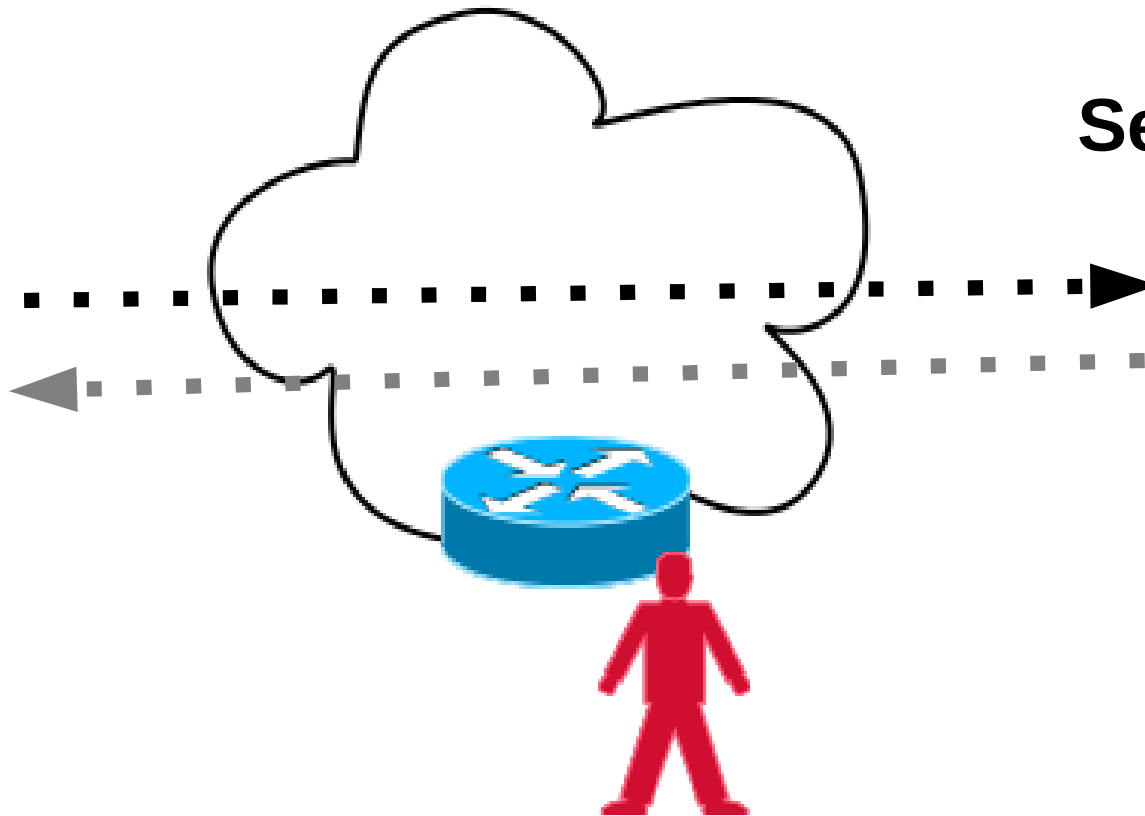
Internauta



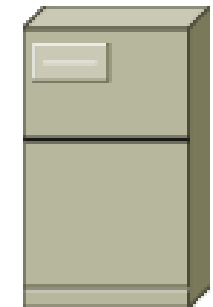
Posso VER o tráfego aberto!

2 – Confiar no Roteamento Provedores?

Internauta

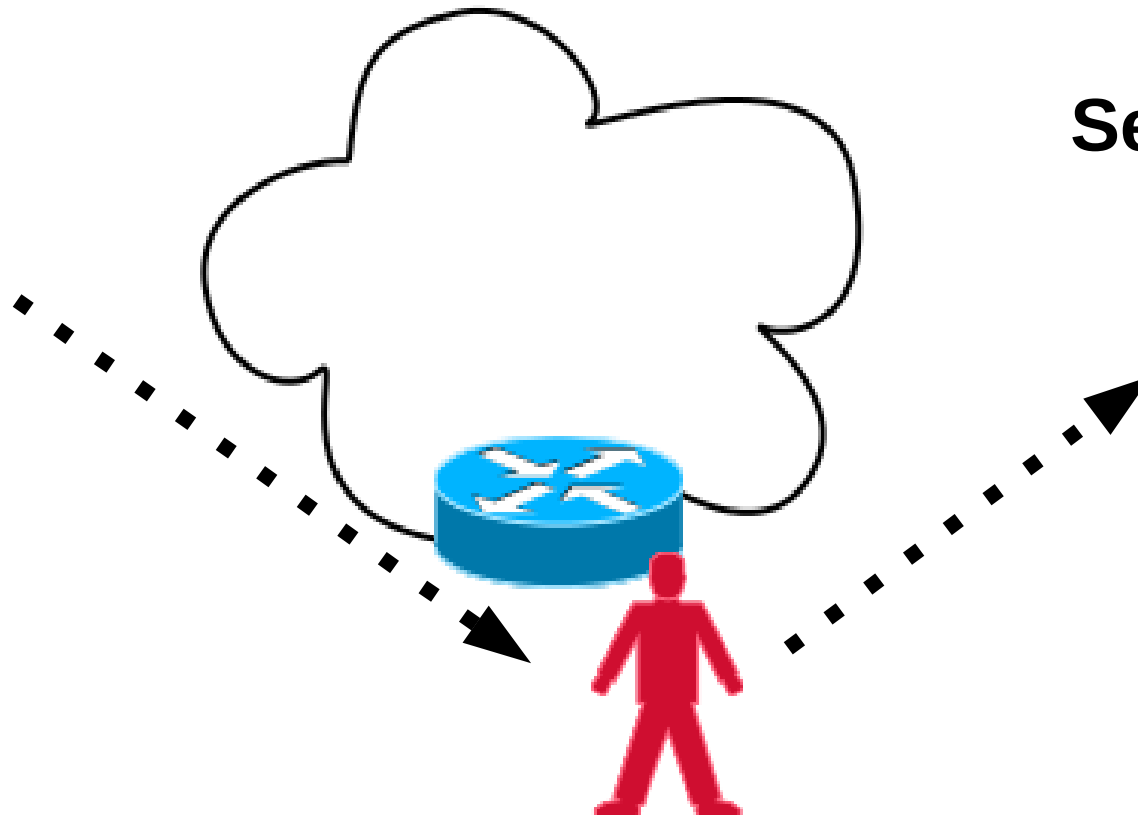


Servidor Web

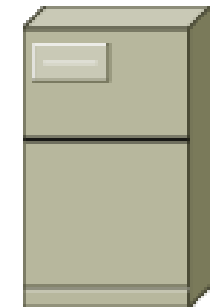


2 – Confiar no Roteamento Provedores?

Internauta



Servidor Web



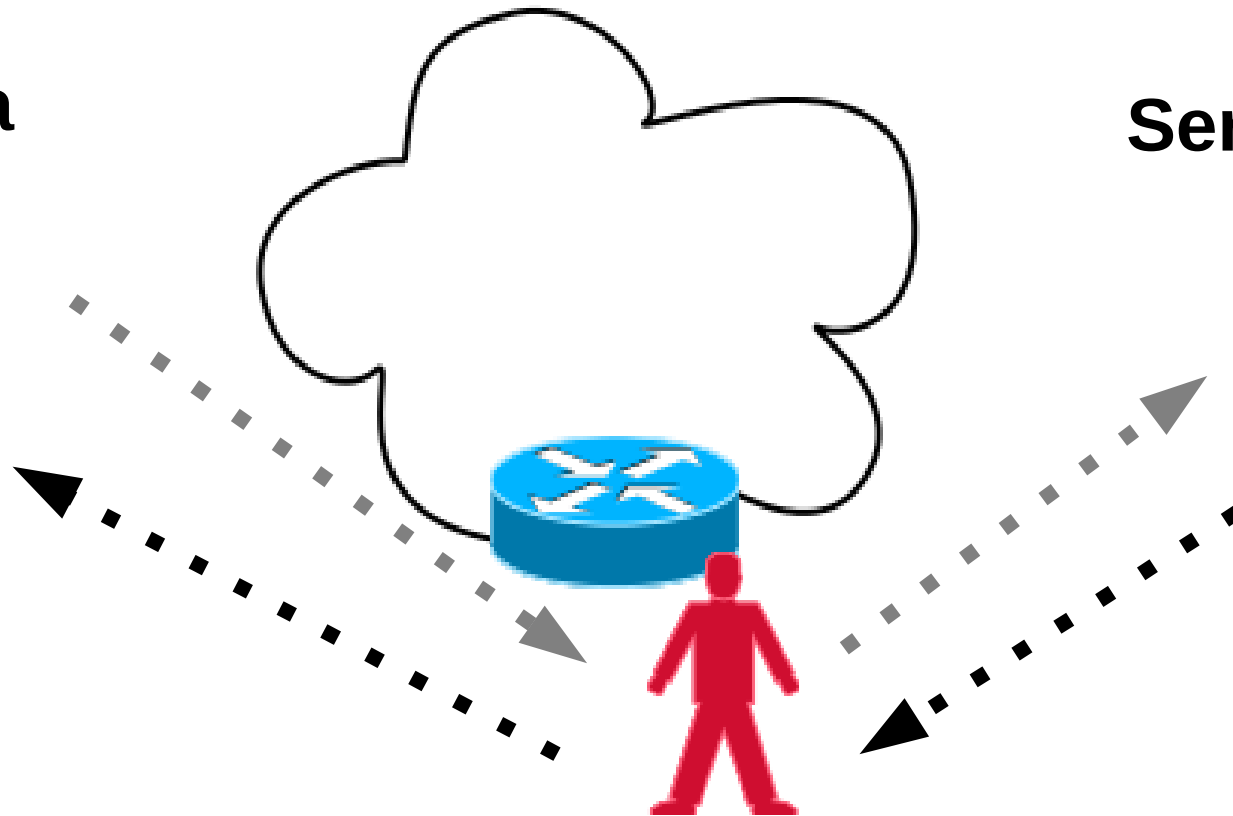
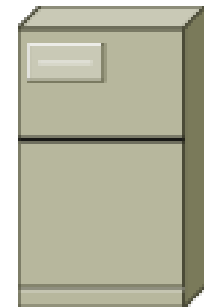
Posso ALTERAR o tráfego aberto!

2 – Confiar no Roteamento Provedores?

Internauta



Servidor Web

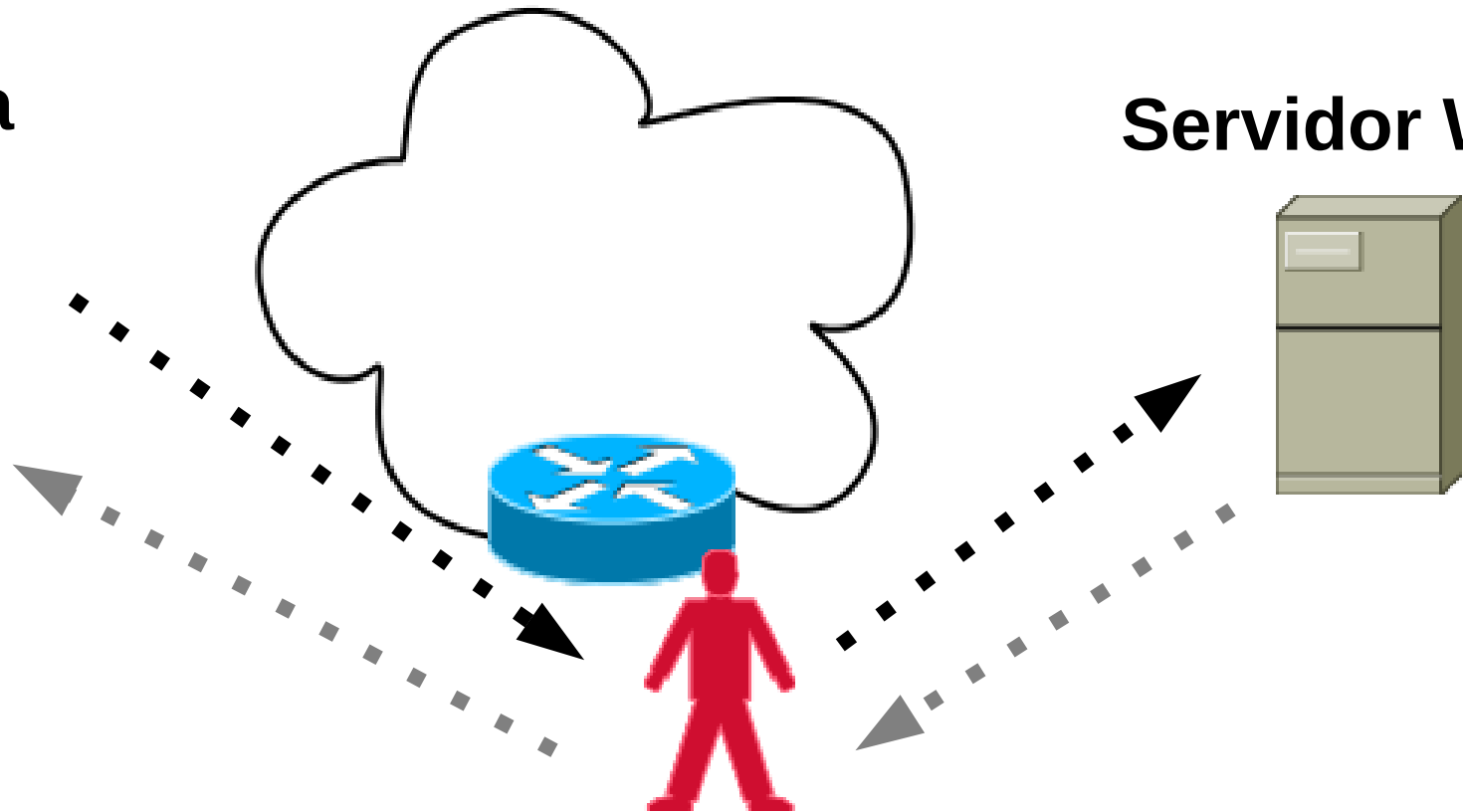


Posso ALTERAR o tráfego aberto!

2 – Confiar no Roteamento Provedores?

Ataque do Homem Intermediário

Internauta

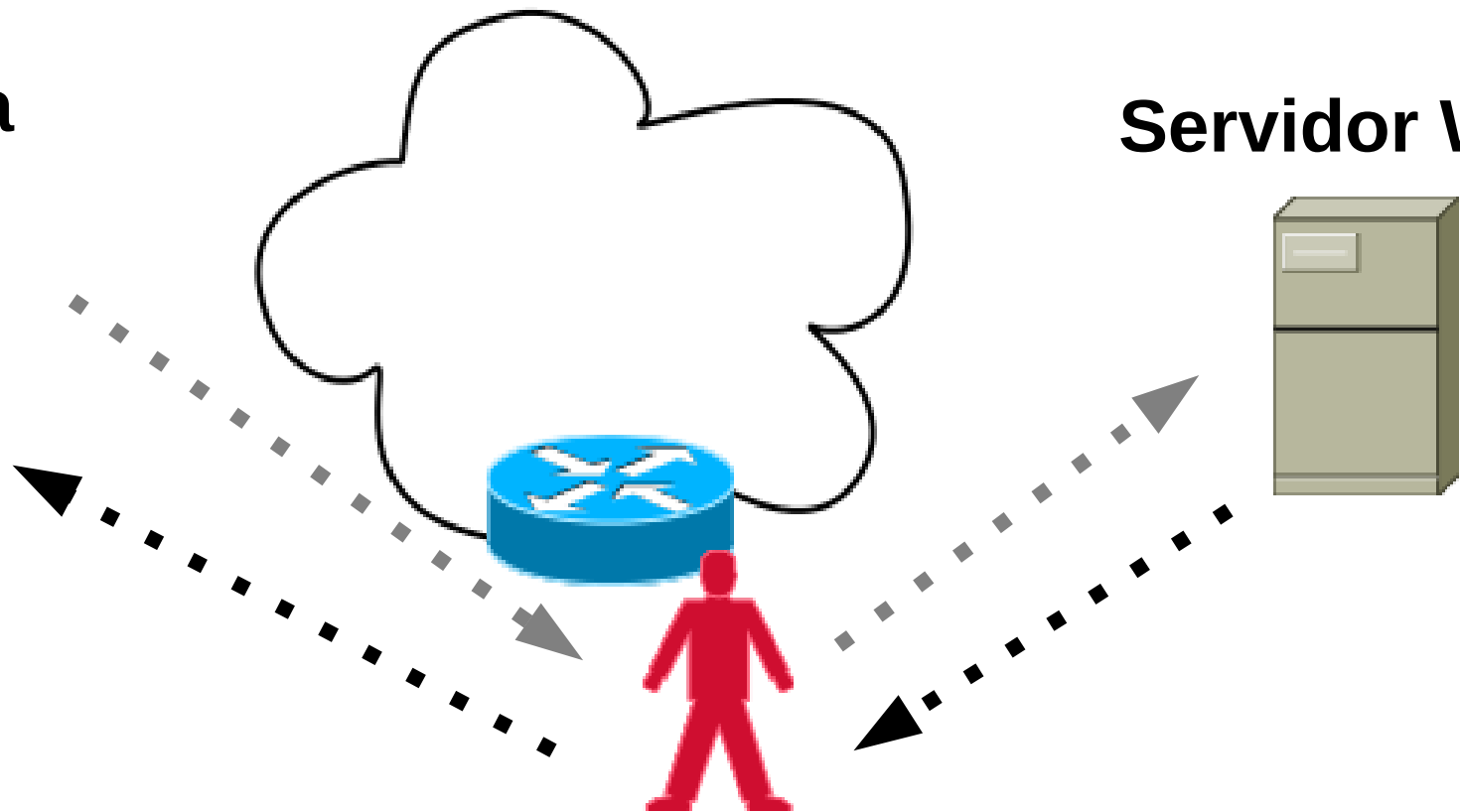


Servidor Web

Posso ALTERAR o tráfego aberto!

Ataque do Homem Intermediário

Internauta

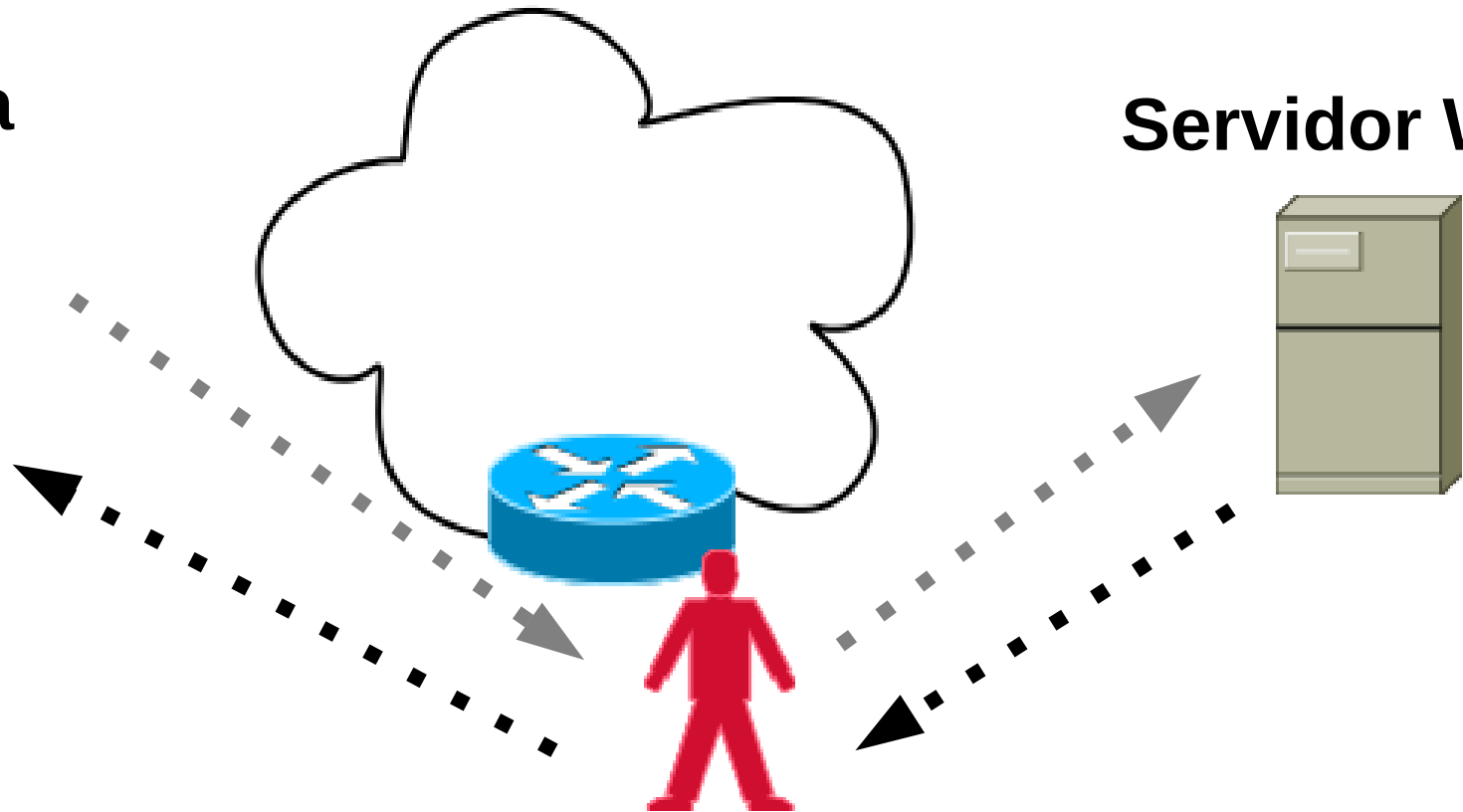


Posso ALTERAR o tráfego aberto!

2 – Confiar no Roteamento Provedores?

Ataque do Homem Intermediário

Internauta



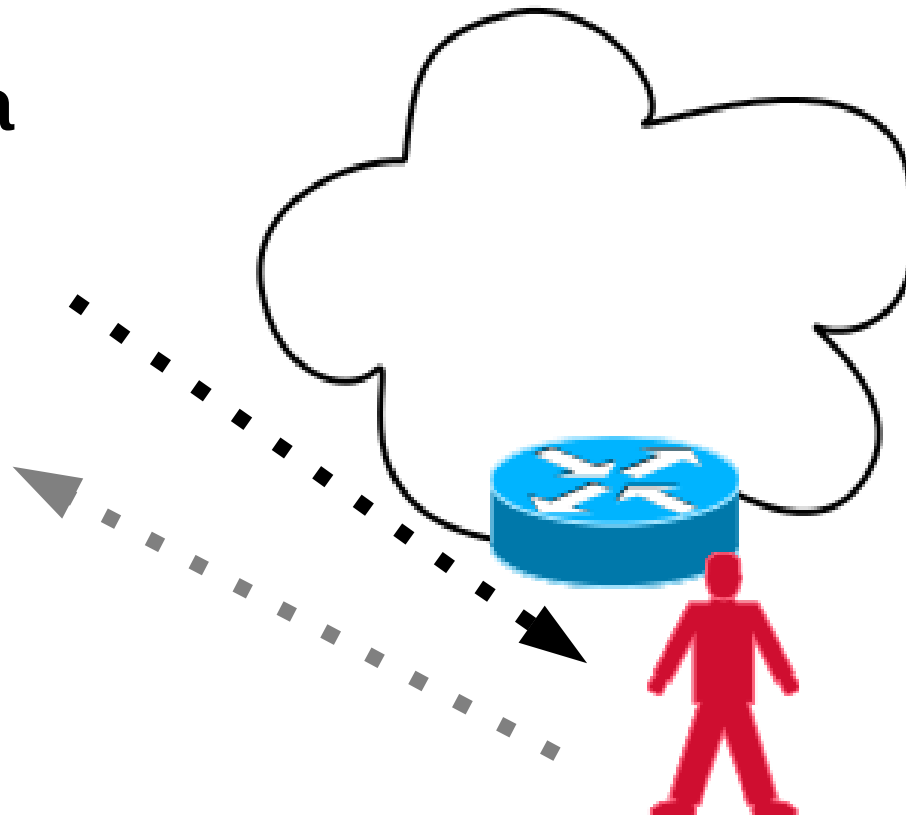
Servidor Web

Posso DESVIAR o tráfego!

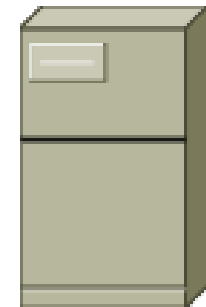
2 – Confiar no Roteamento Provedores?

Ataque do Homem Intermediário

Internauta



Servidor Web

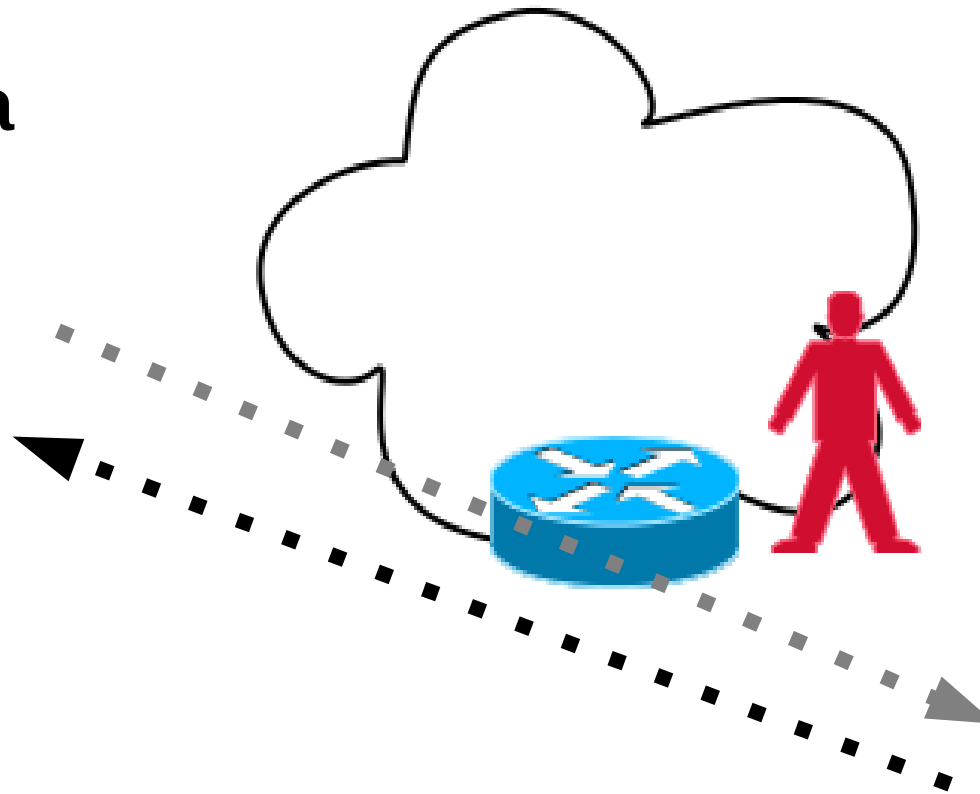


Posso DESVIAR o tráfego!

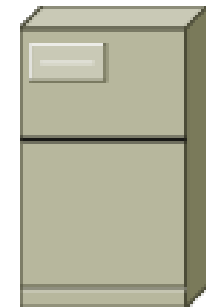
2 – Confiar no Roteamento Provedores?

Desvio de rotas!

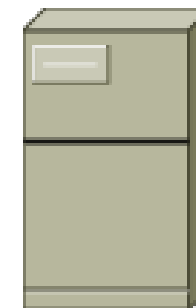
Internauta



Servidor Web



Servidor Web Falso

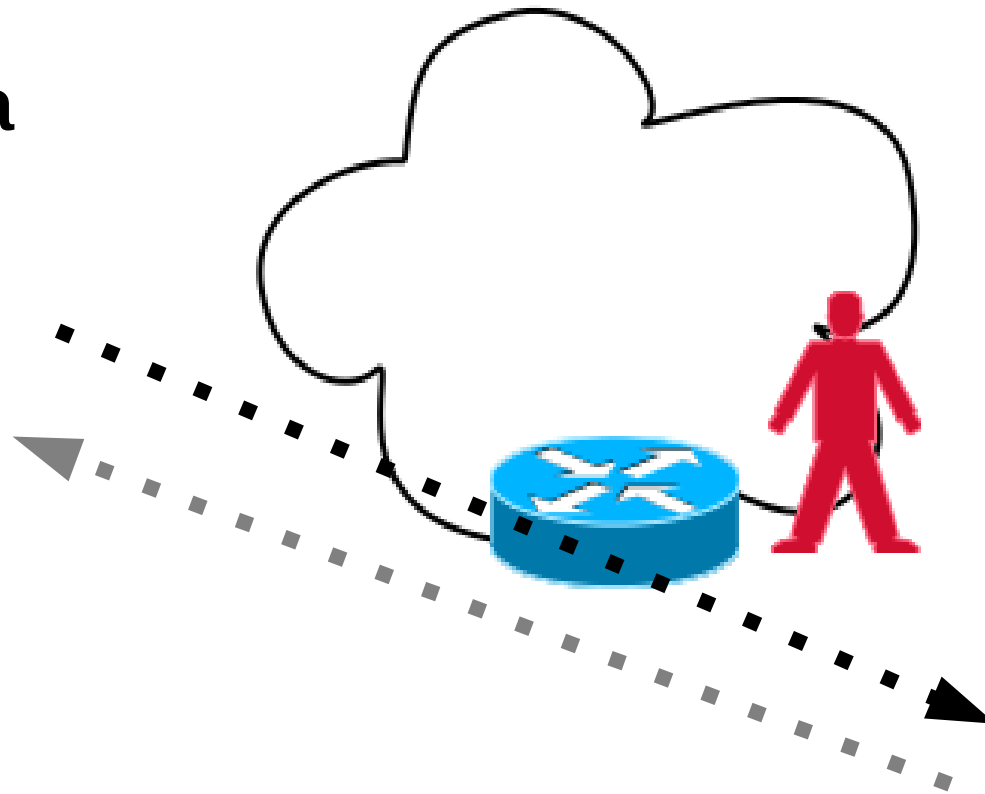


Posso DESVIAR o tráfego!

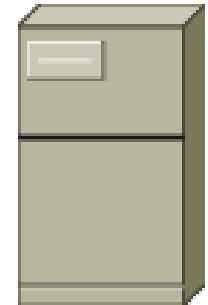
2 – Confiar no Roteamento Provedores?

Desvio de rotas!

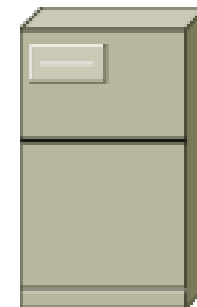
Internauta



Servidor Web



**Servidor
Web
Falso**

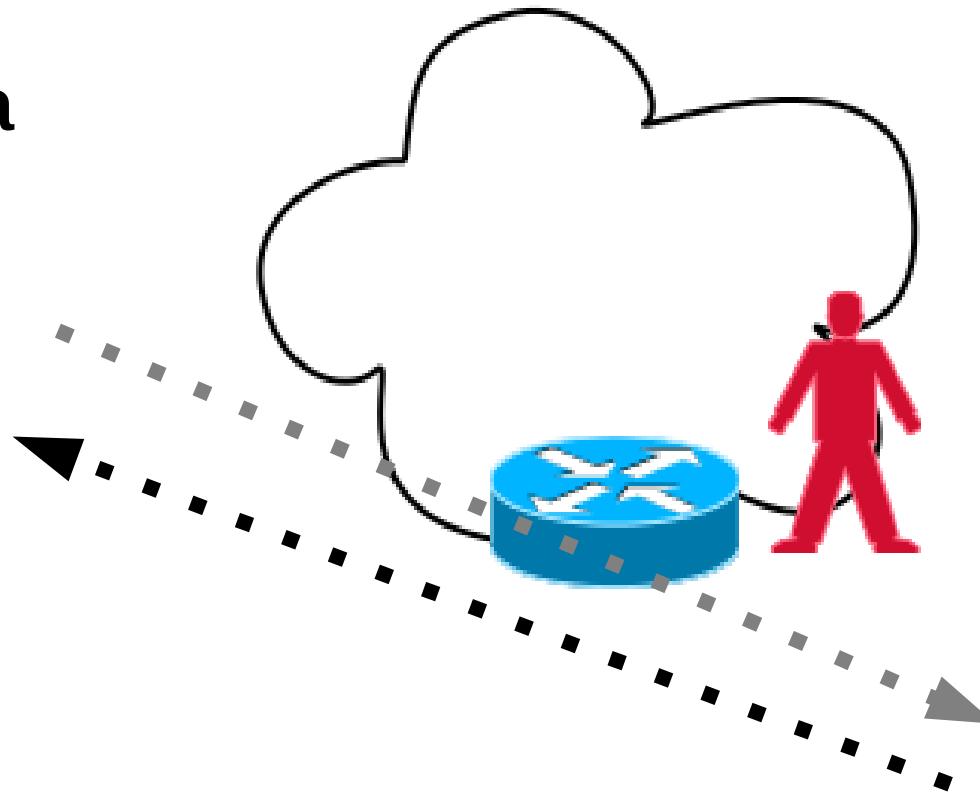


Posso DESVIAR o tráfego!

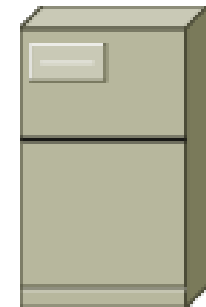
2 – Confiar no Roteamento Provedores?

Desvio de rotas!

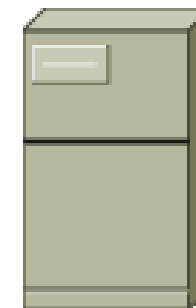
Internauta



Servidor Web



**Servidor
Web
Falso**



Posso DESVIAR o tráfego!

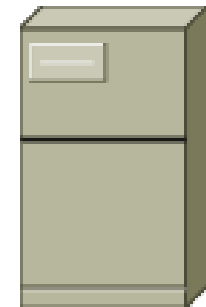
2 – Confiar no Roteamento Provedores?

Desvio de rotas!

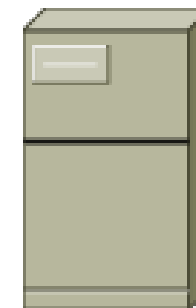
Internauta



Servidor Web



**Servidor
Web
Falso**



**YOU HAVE BEEN
HACKED !**

DESVIAR o tráfego!

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?



Provedor A

2 – Confiar no Roteamento Provedores?



Provedor A



Provedor C

2 – Confiar no Roteamento Provedores?



Provedor A

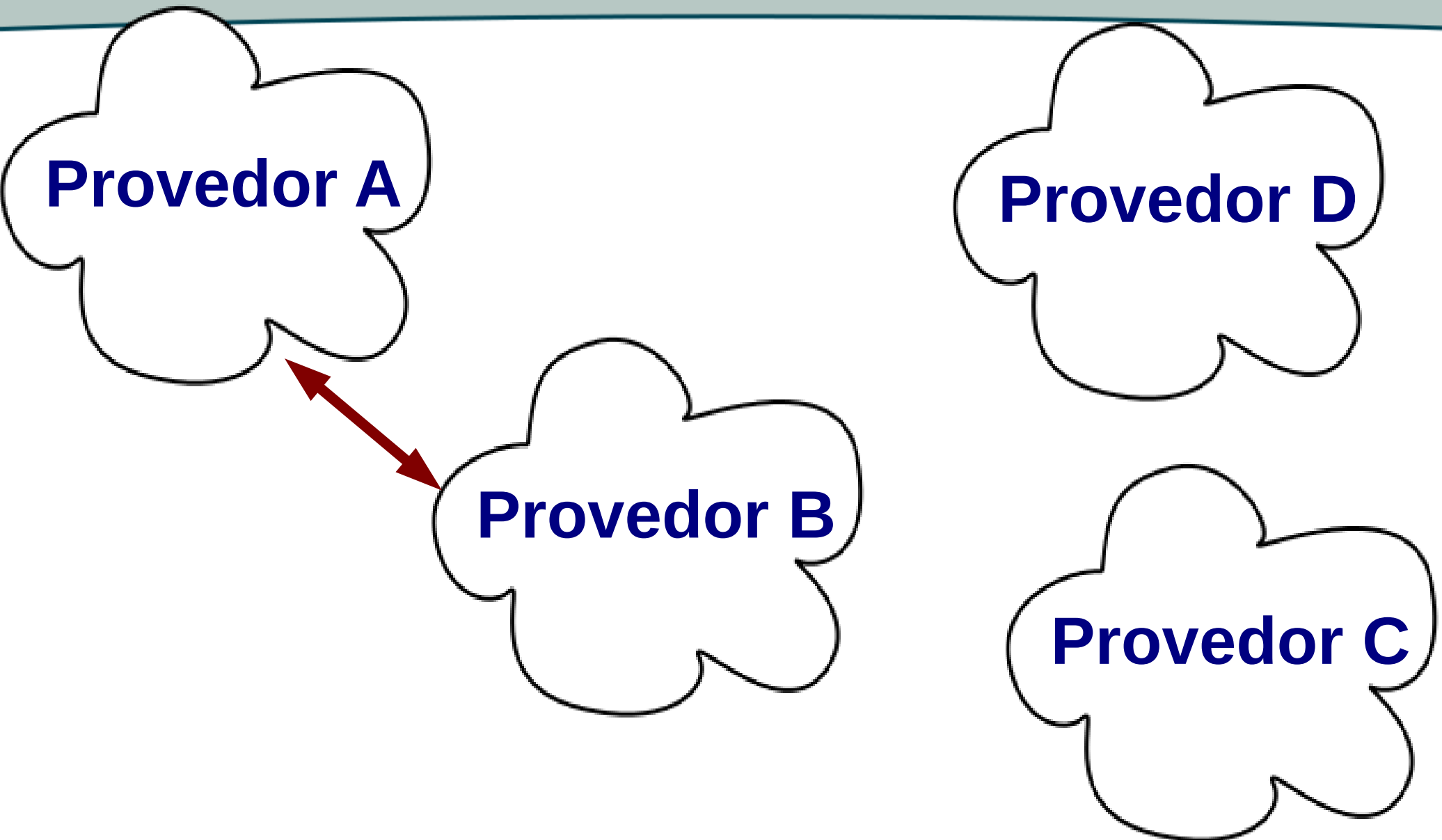


Provedor B

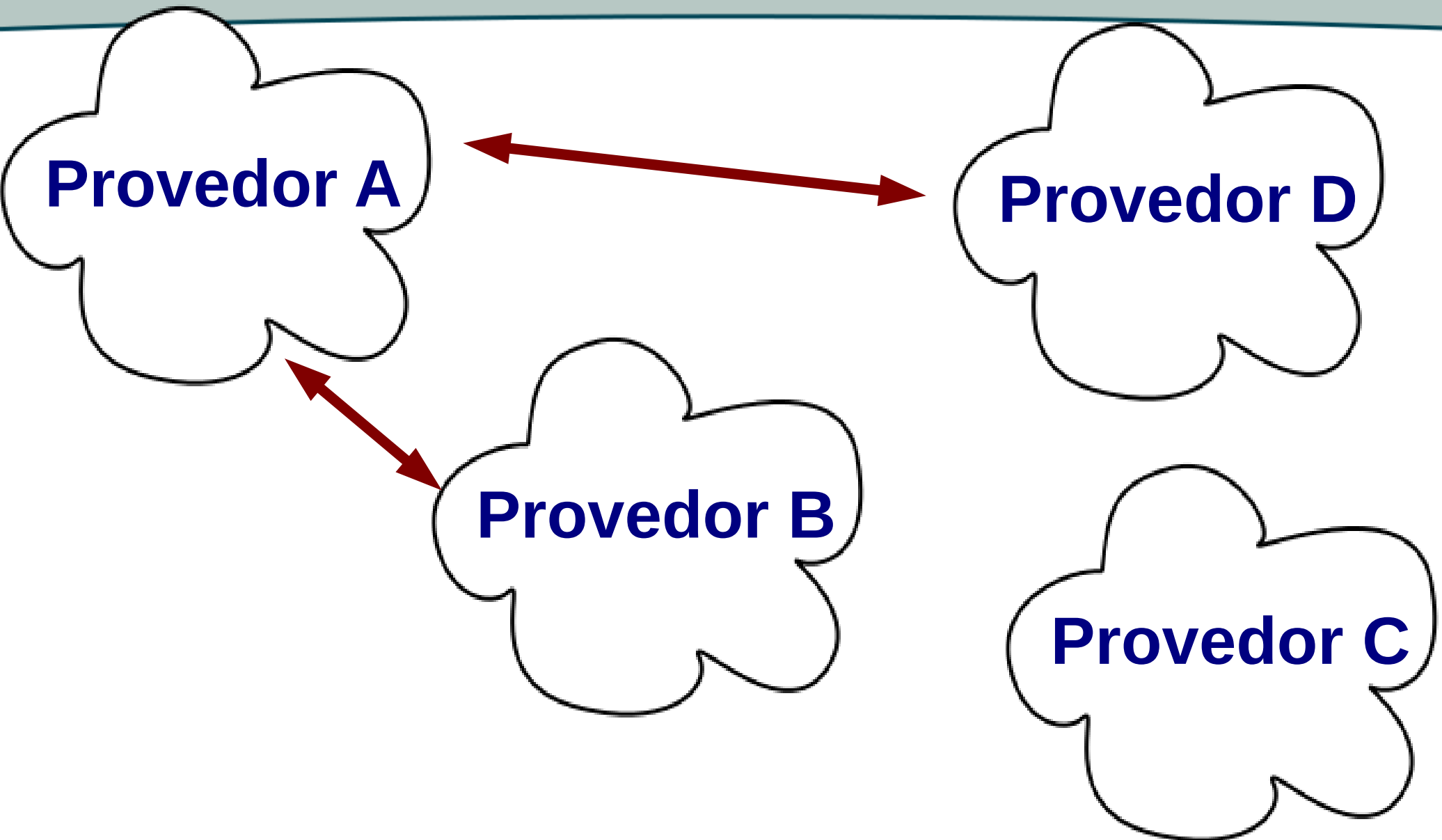


Provedor C

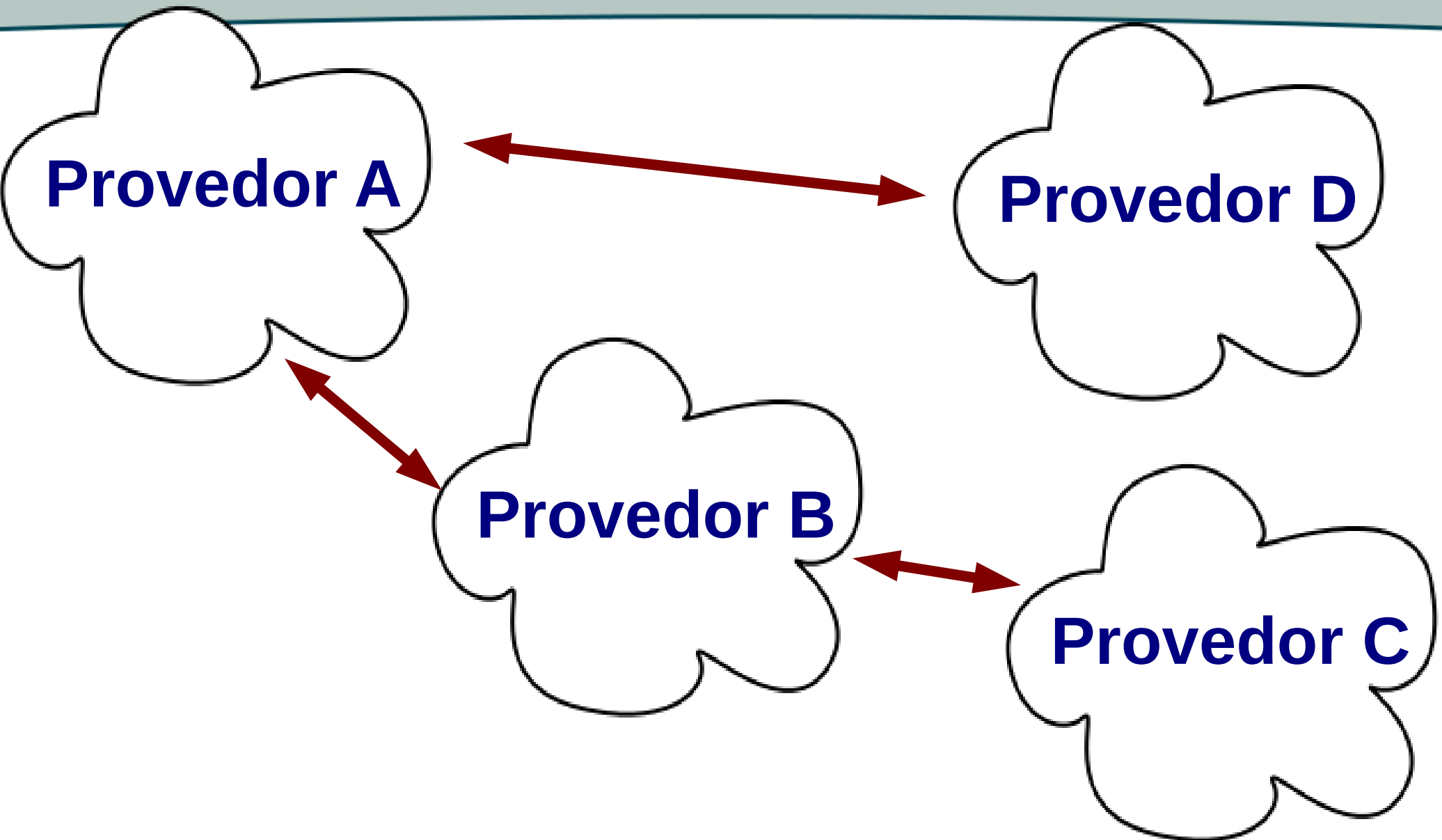
2 – Confiar no Roteamento Proveedores?



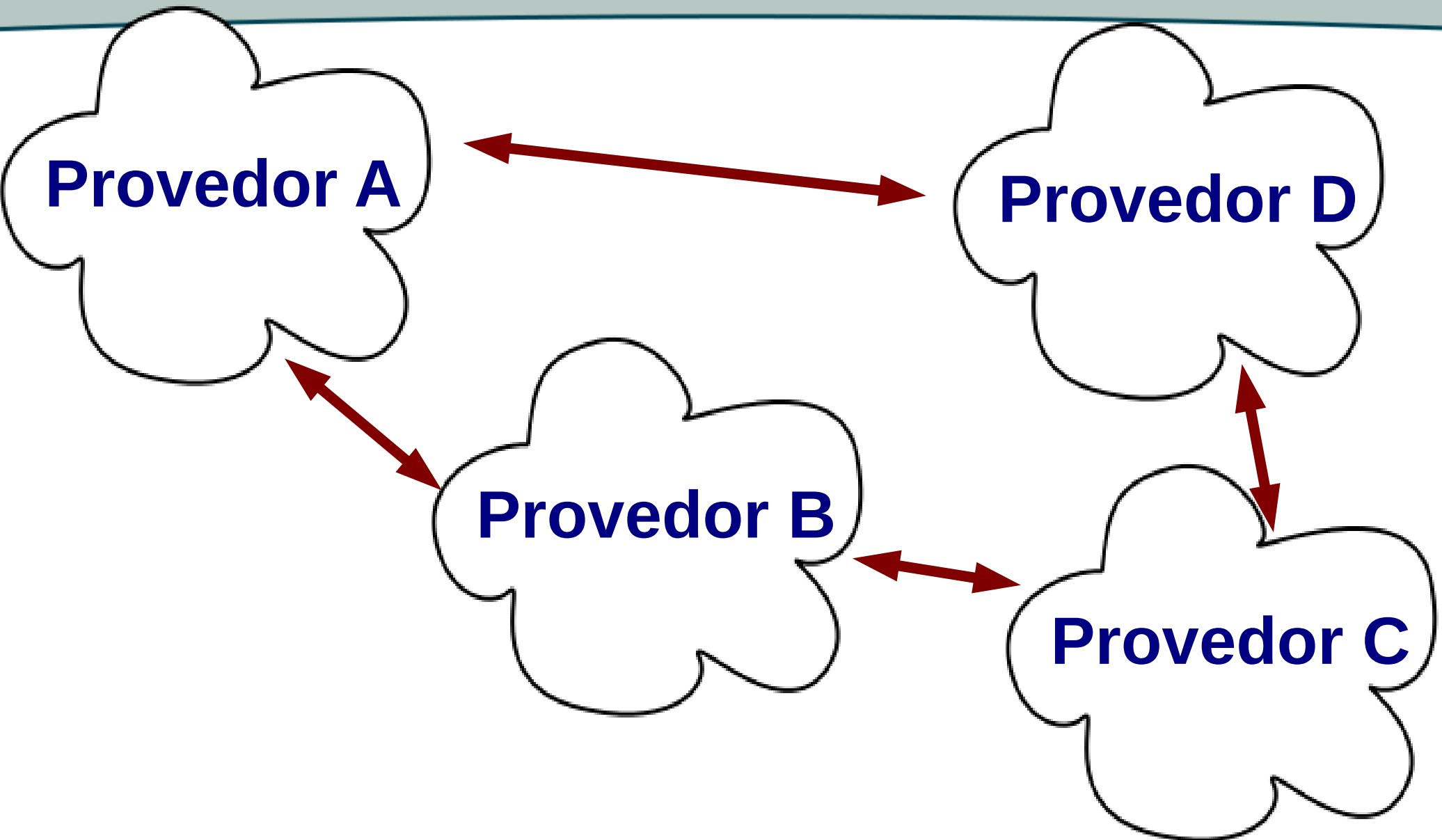
2 – Confiar no Roteamento Proveedores?



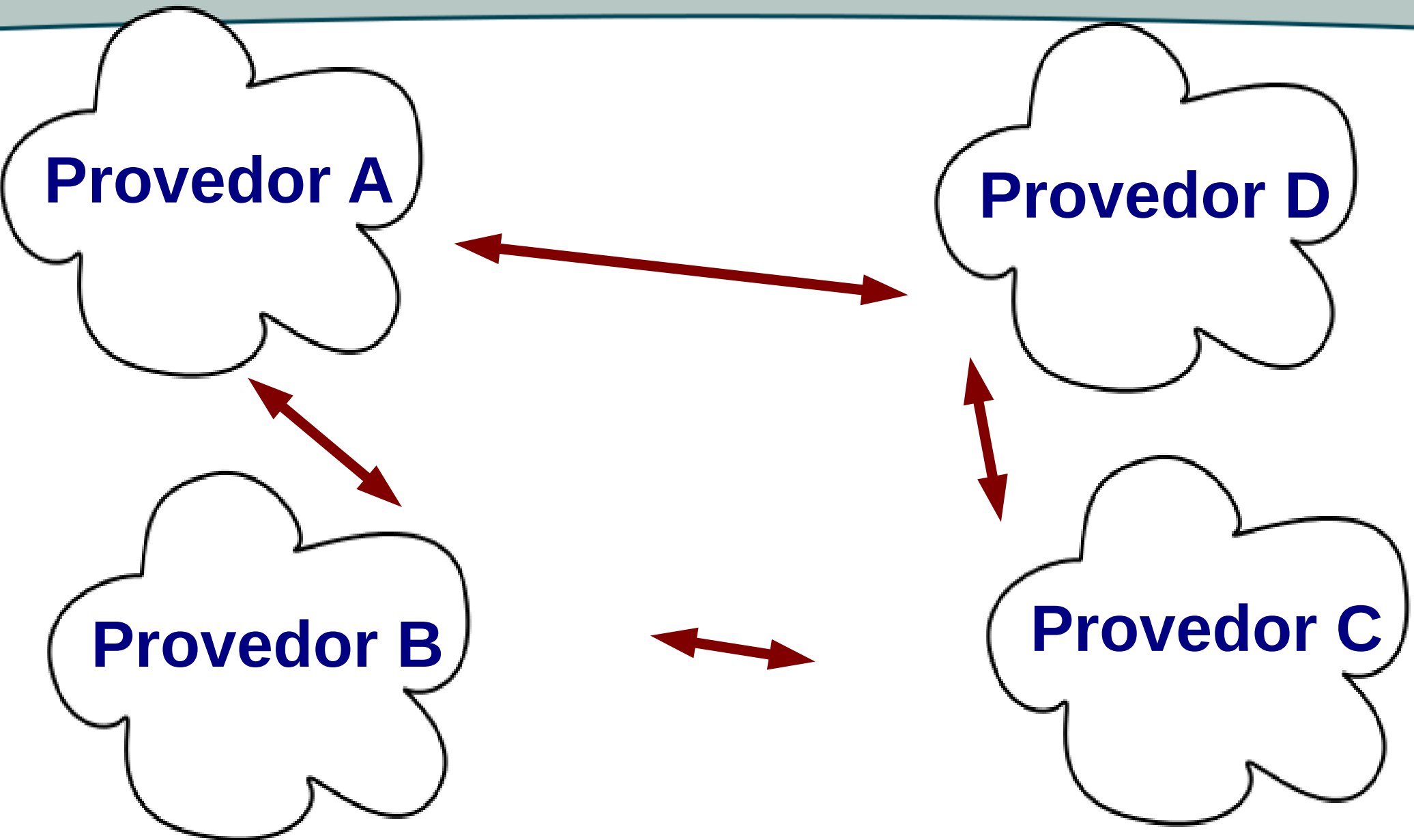
2 – Confiar no Roteamento Proveedores?



2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Proveedores?



2 – Confiar no Roteamento Provedores?

Provedor A

Provedor D

Trocar Caminhos (rotas)

Protocolo de Roteamento

Provedor B

Provedor C

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?

**Sistema
Autonomo**

**Sistema
Autonomo**

**Sistema
Autonomo**

**Sistema
Autonomo**

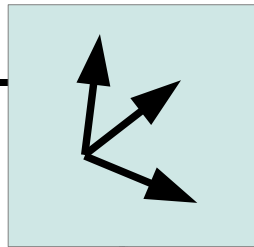


2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**

**Sistema
Autonomo**

**Sistema
Autonomo**



**Sistema
Autonomo**

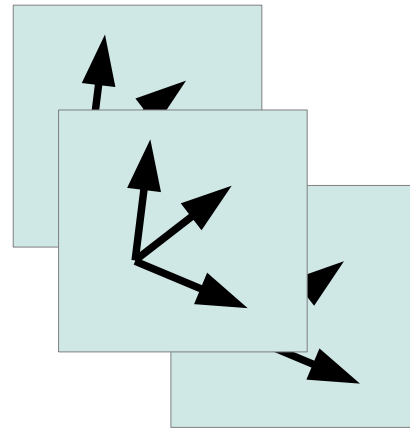
2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**

**Sistema
Autonomo**

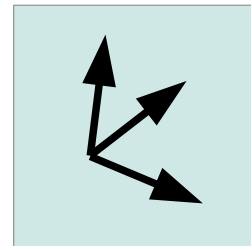
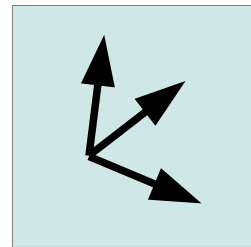
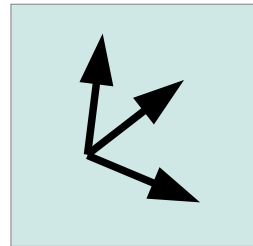
**Sistema
Autonomo**

**Sistema
Autonomo**



2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**



**Sistema
Autonomo**

**Sistema
Autonomo**

**Sistema
Autonomo**

2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**



A cloud-shaped icon representing an autonomous system. Inside the cloud, the text "Sistema Autonomo" is written in blue. To the right of the cloud, a light blue square contains a black icon of a router with three arrows pointing outwards, representing network connectivity.

**Sistema
Autonomo**



A cloud-shaped icon representing an autonomous system. Inside the cloud, the text "Sistema Autonomo" is written in blue. To the left of the cloud, a light blue square contains a black icon of a router with three arrows pointing outwards, representing network connectivity.

**Sistema
Autonomo**



A cloud-shaped icon representing an autonomous system. Inside the cloud, the text "Sistema Autonomo" is written in blue. To the right of the cloud, a light blue square contains a black icon of a router with three arrows pointing outwards, representing network connectivity.

**Sistema
Autonomo**

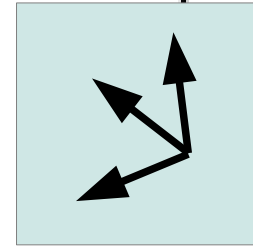


A cloud-shaped icon representing an autonomous system. Inside the cloud, the text "Sistema Autonomo" is written in blue. To the left of the cloud, a light blue square contains a black icon of a router with three arrows pointing outwards, representing network connectivity.

2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**

**Sistema
Autonomo**

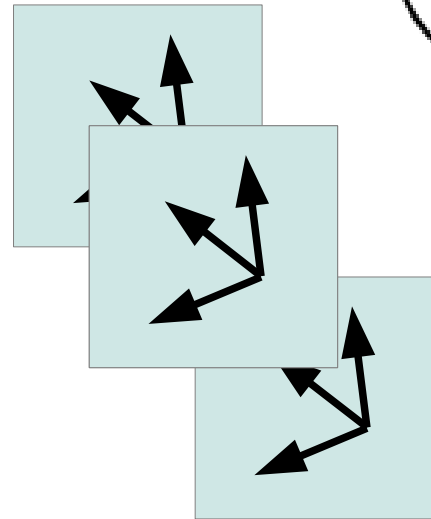


**Sistema
Autonomo**

**Sistema
Autonomo**

2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**



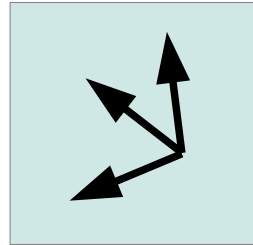
**Sistema
Autonomo**

**Sistema
Autonomo**

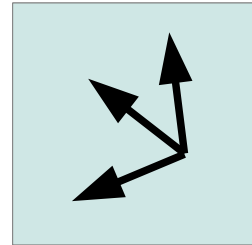
**Sistema
Autonomo**

2 – Confiar no Roteamento Provedores?

**Sistema
Autonomo**



**Sistema
Autonomo**



**Sistema
Autonomo**

**Sistema
Autonomo**

INCIDENTE DE SEGURANÇA

Em 2008 provedor paquistanês
divulga rede do Youtube!



Pakistan hijacks YouTube

24 FEB, 2008 | 7:50 PM | BY MARTIN BROWN

Late in the (UTC) day on 24 February 2008, Pakistan Telecom (AS 17557) began advertising a

2 – Confiar no Roteamento Provedores?

ÍNDIA

RÚSSIA

PAQUISTÃO

Minha rede A

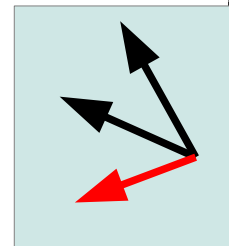
Minha rede B

**Minha rede Y
(youtube)**

2 – Confiar no Roteamento Provedores?

ÍNDIA

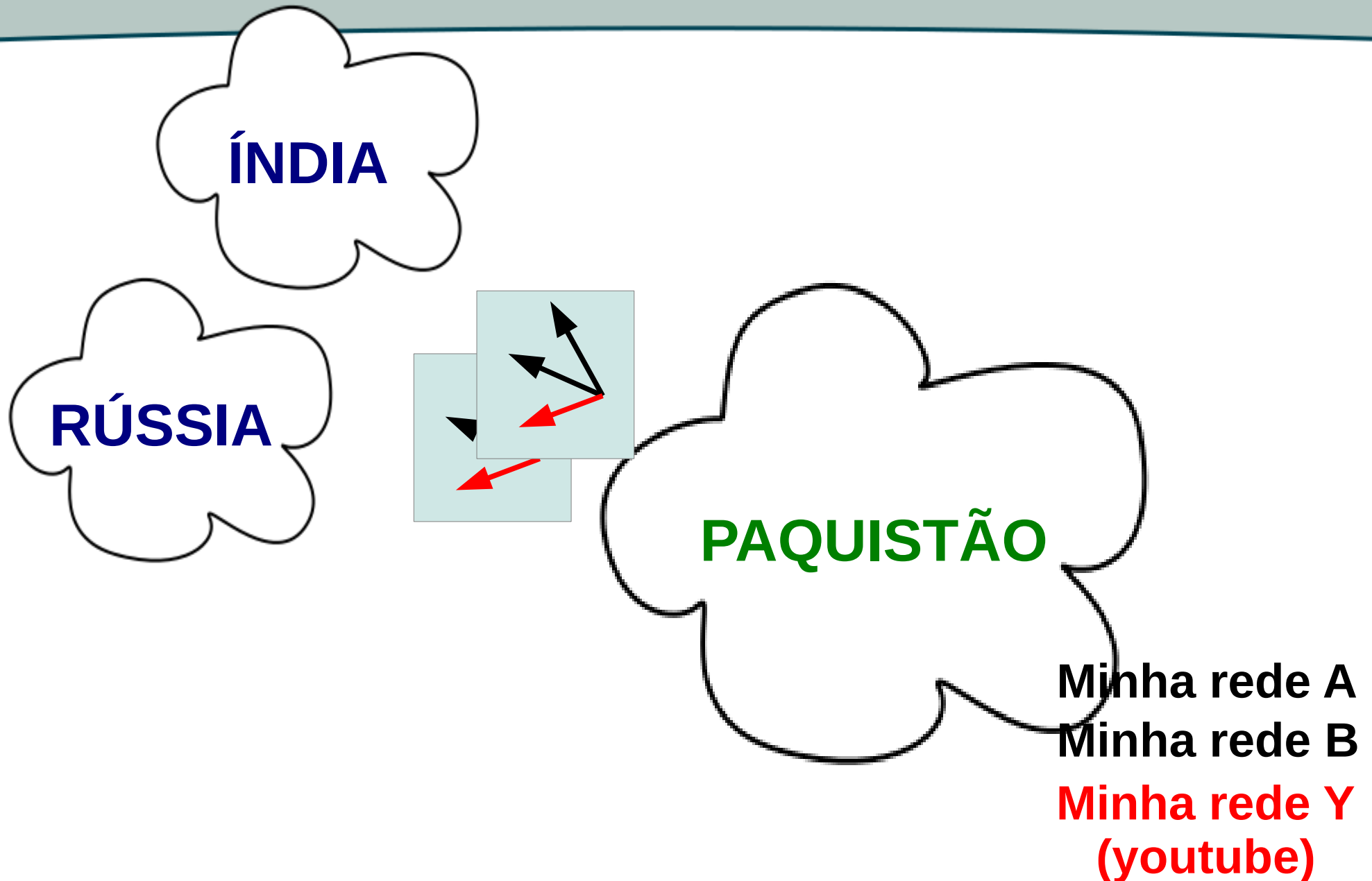
RÚSSIA



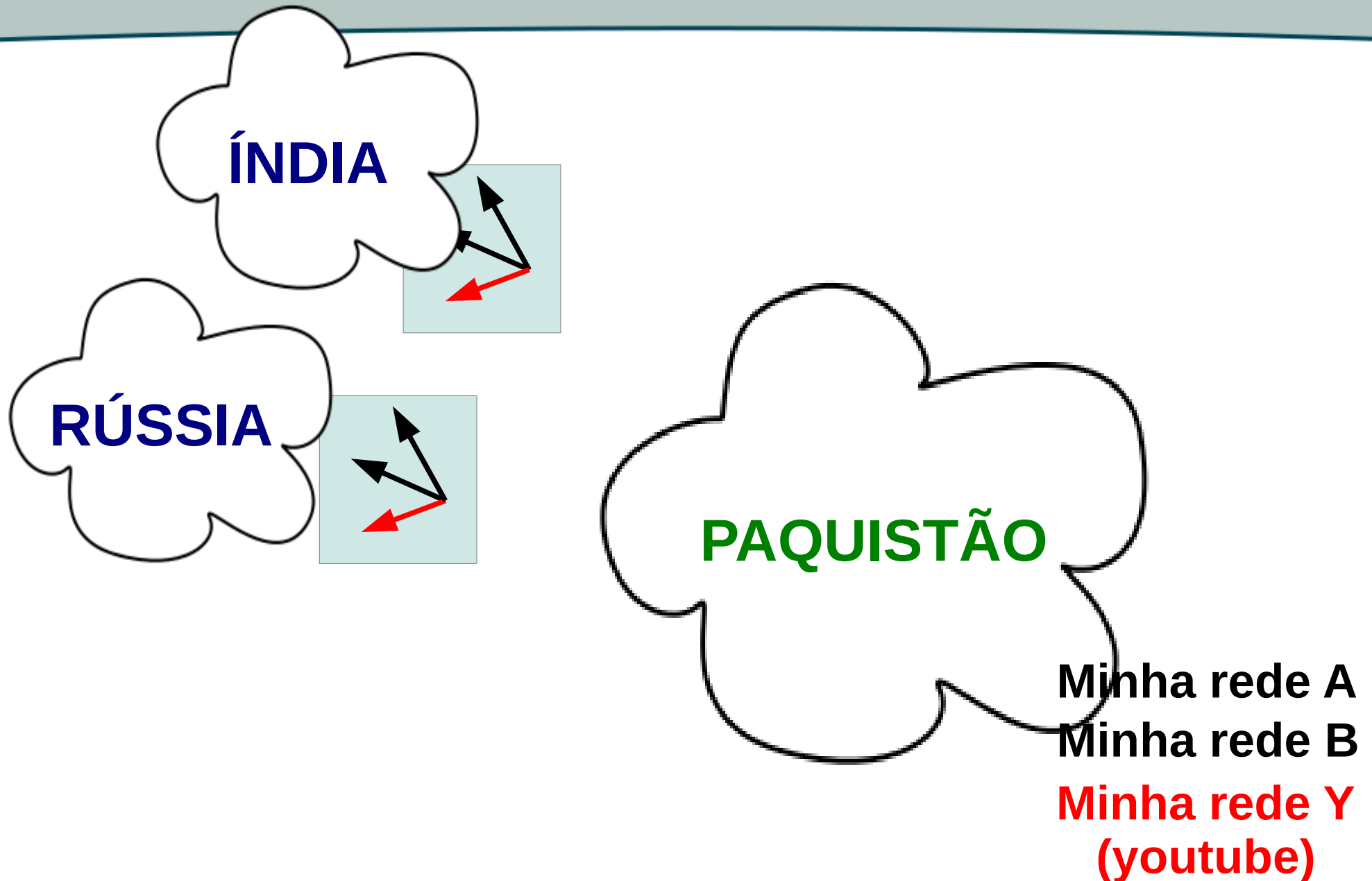
PAQUISTÃO

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

2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?



2 – Confiar no Roteamento Provedores?

ÍNDIA

RÚSSIA

PAQUISTÃO

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?

ÍNDIA

RÚSSIA

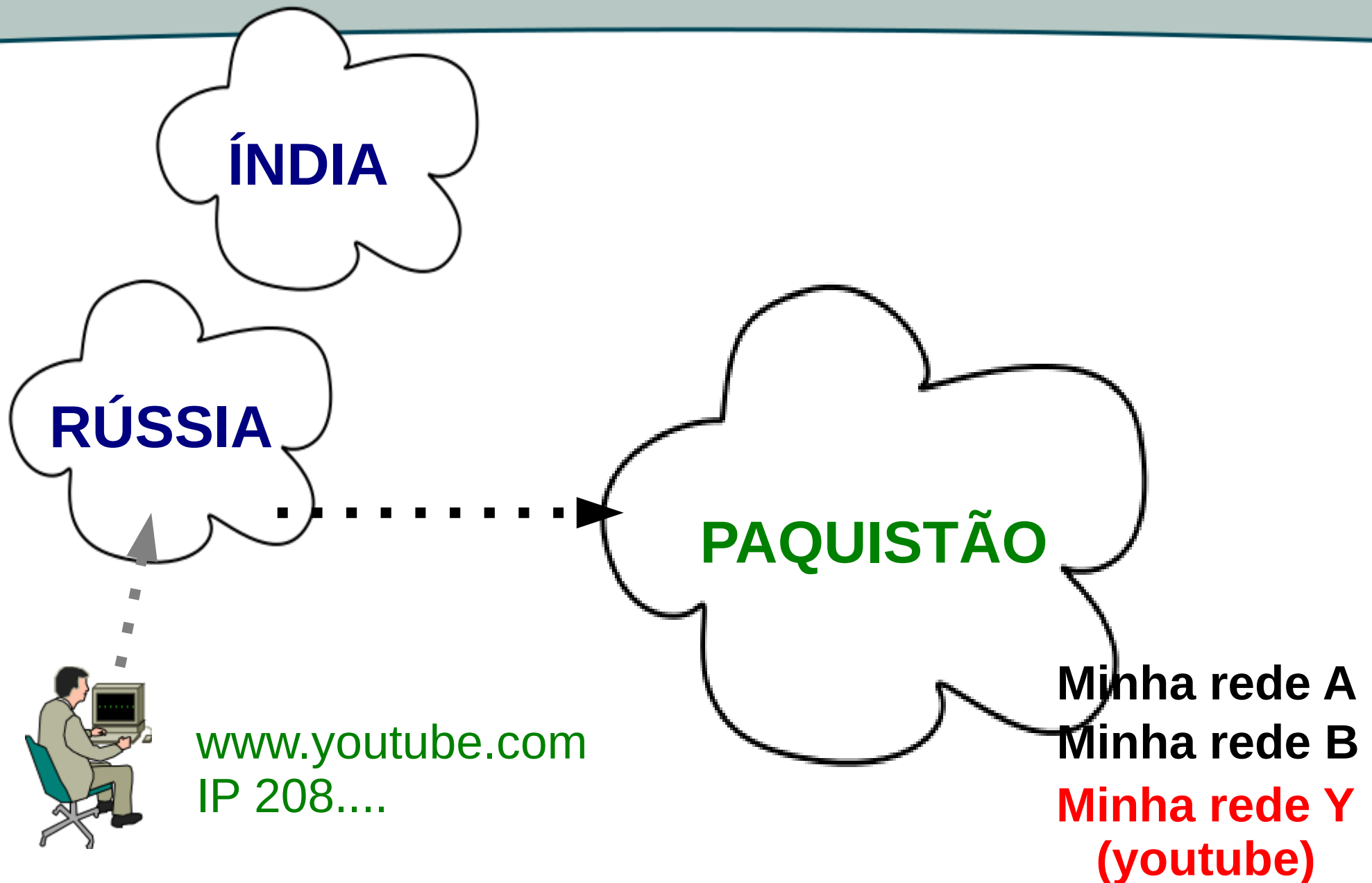
PAQUISTÃO

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

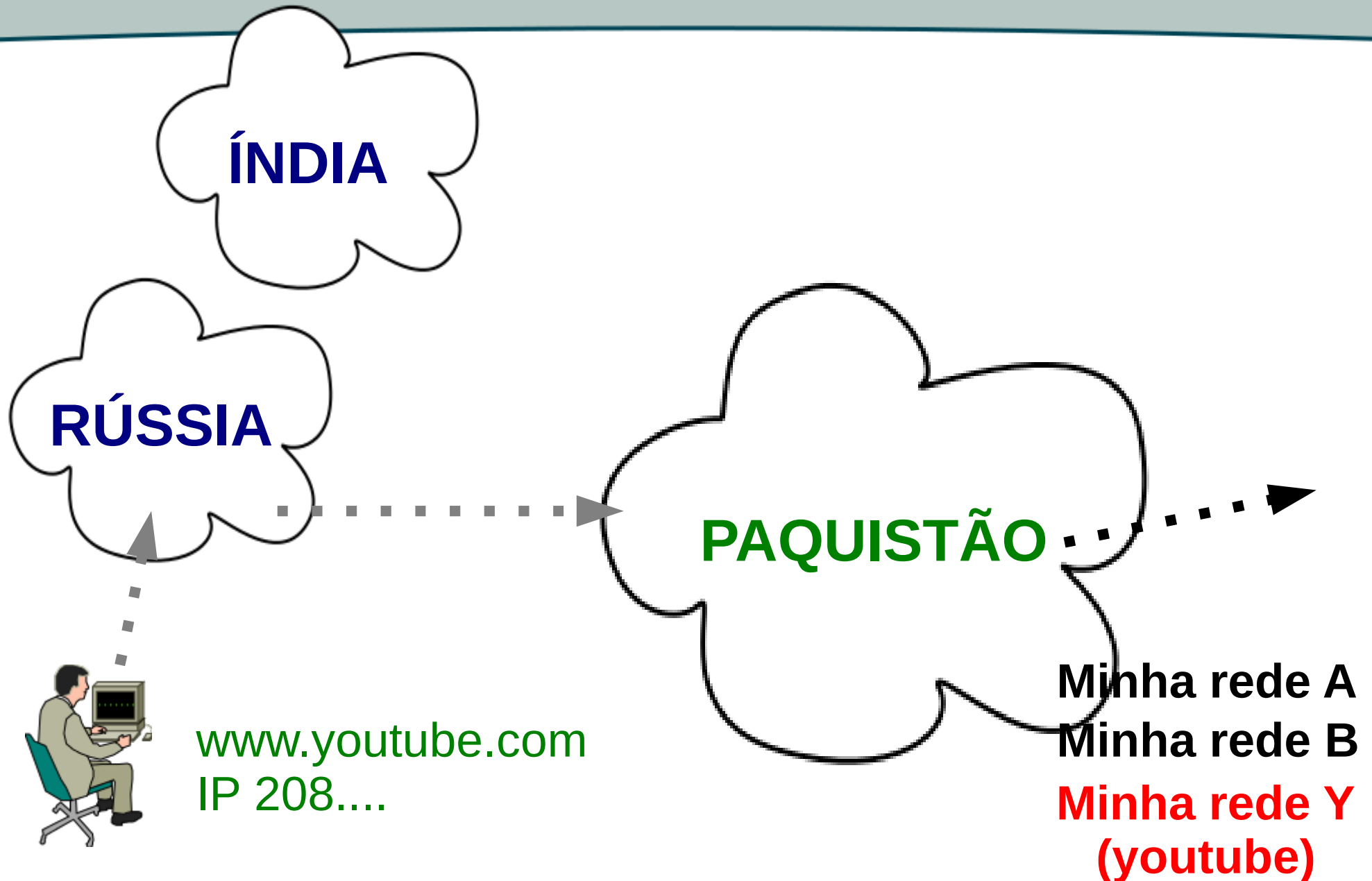
www.youtube.com
IP 208....



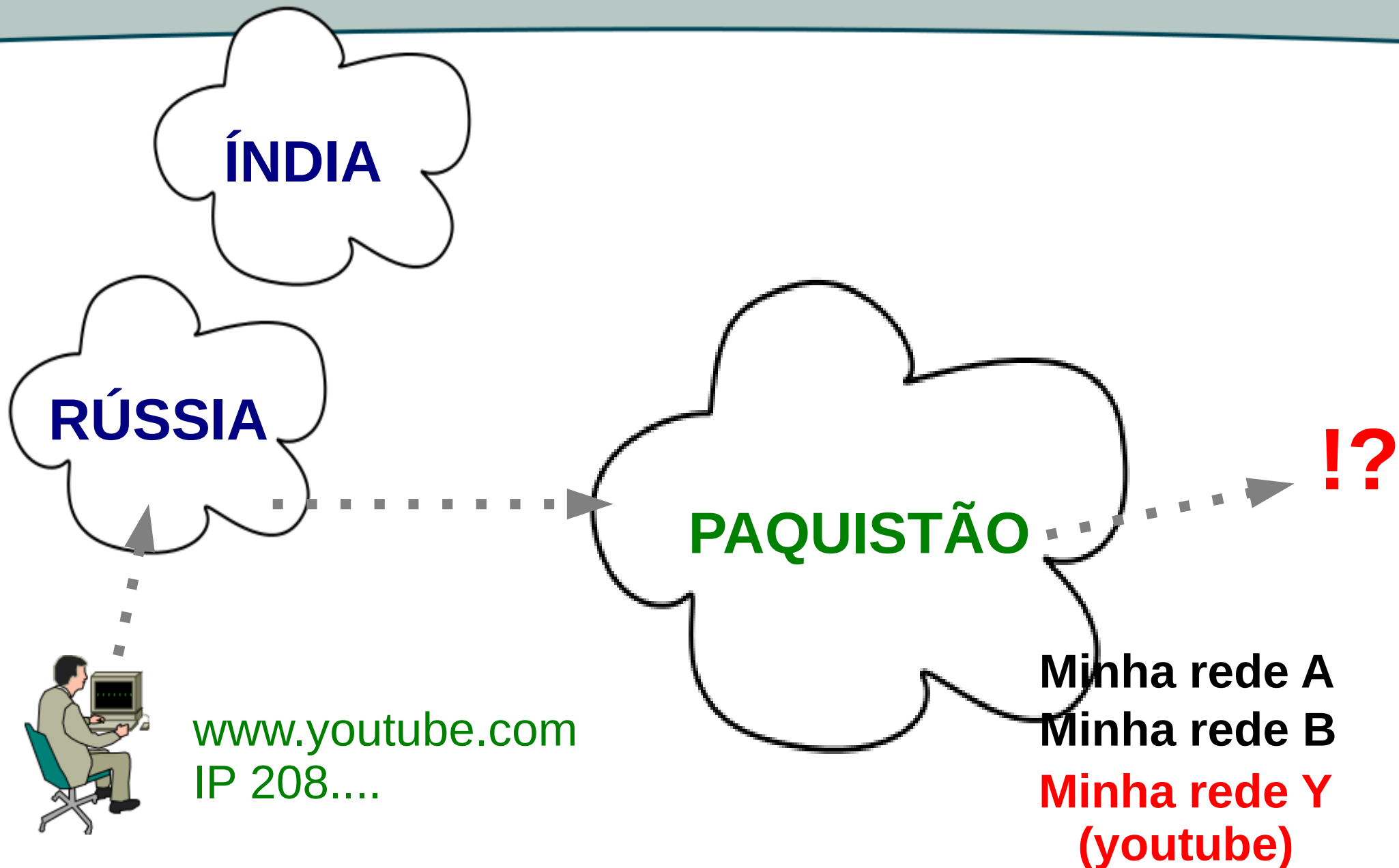
2 – Confiar no Roteamento Provedores?



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

SOLUÇÃO

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

3 -

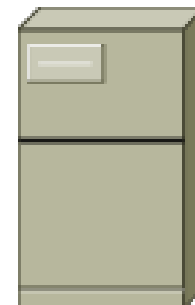
**Podemos confiar
em Autoridades
Certificadoras?**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web

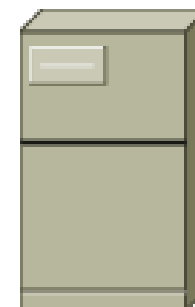


3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web

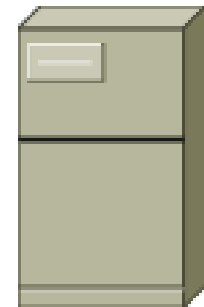


3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



HTTP

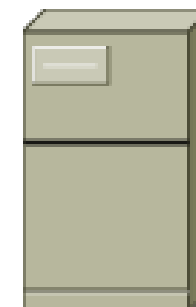
Texto Aberto

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



HTTP

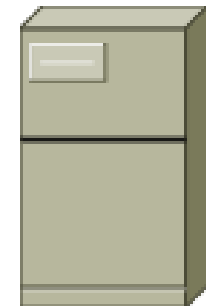
Texto Aberto

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



HTTP

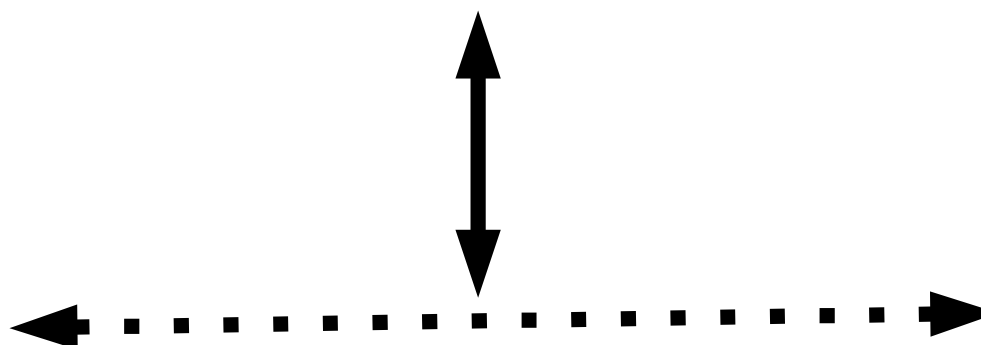
Texto Aberto

3 – Confiar Autoridades Certificadoras?

Internauta



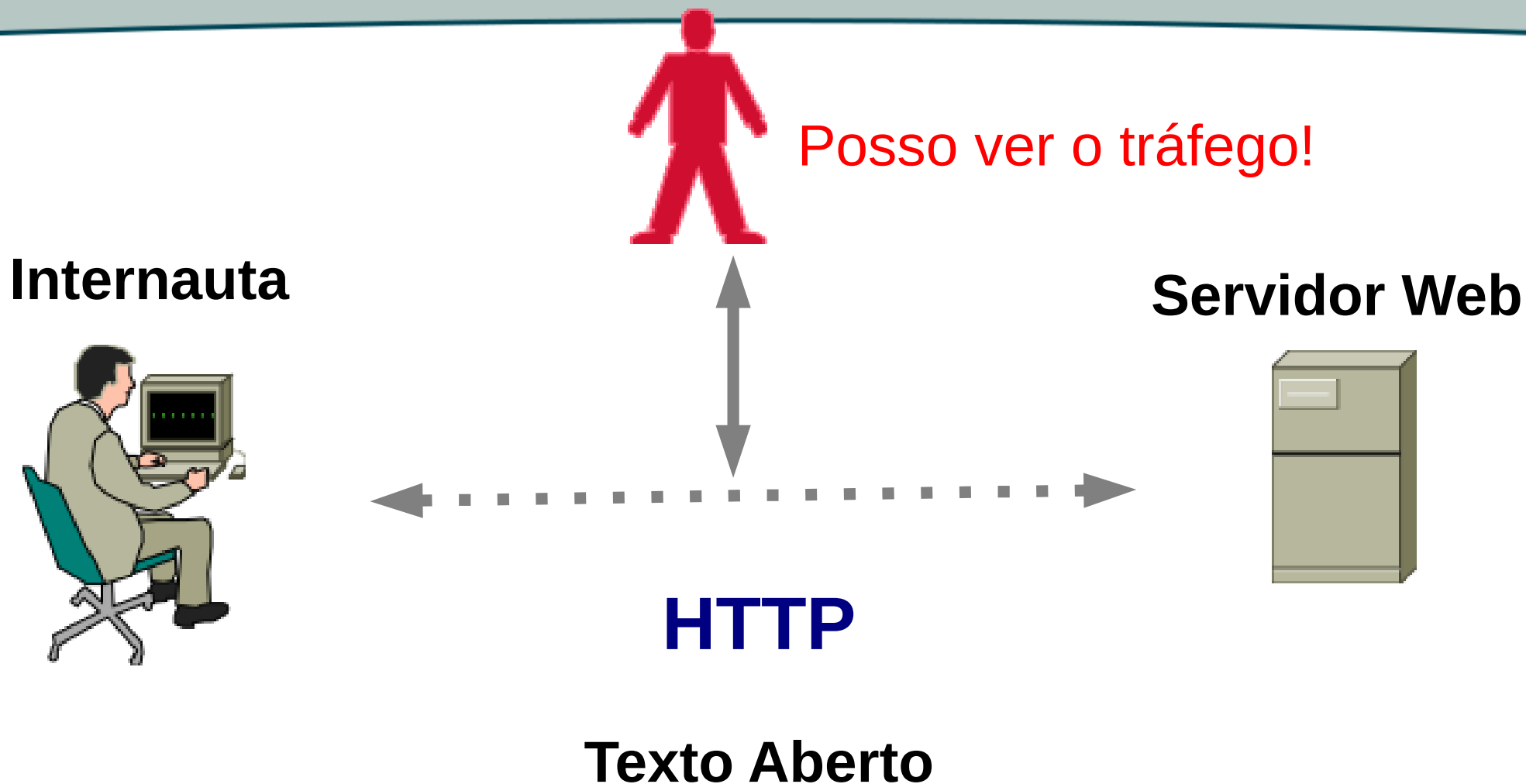
Servidor Web



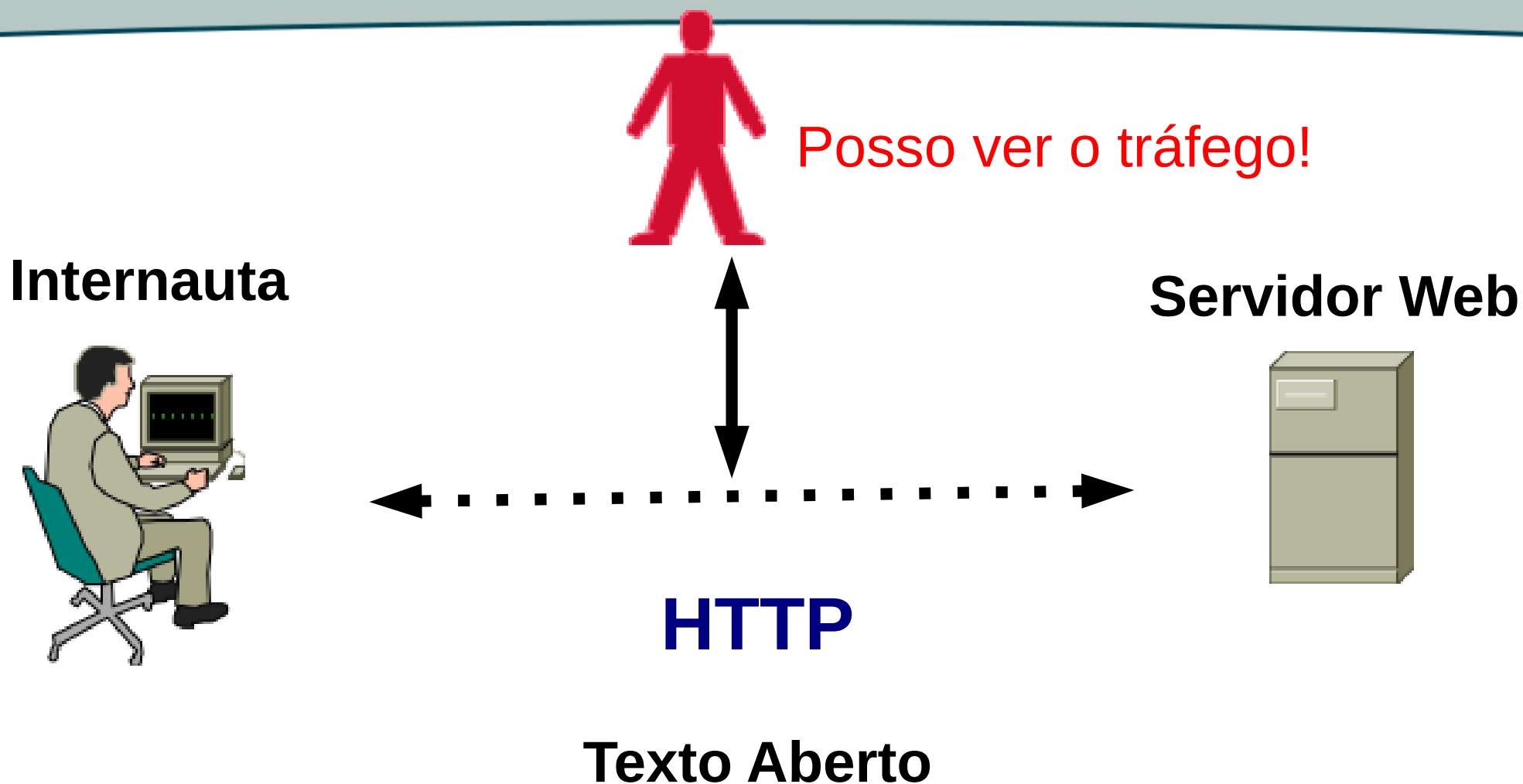
HTTP

Texto Aberto

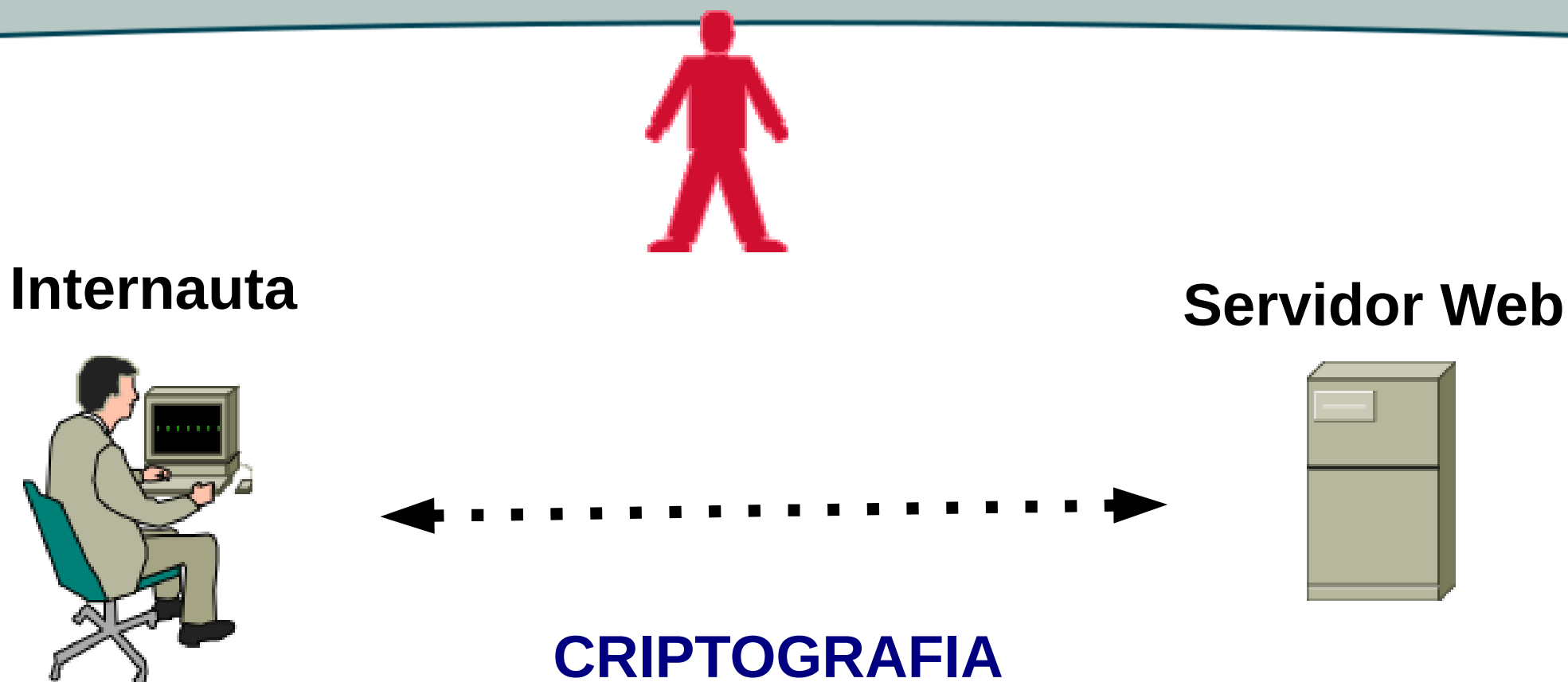
3 – Confiar Autoridades Certificadoras?



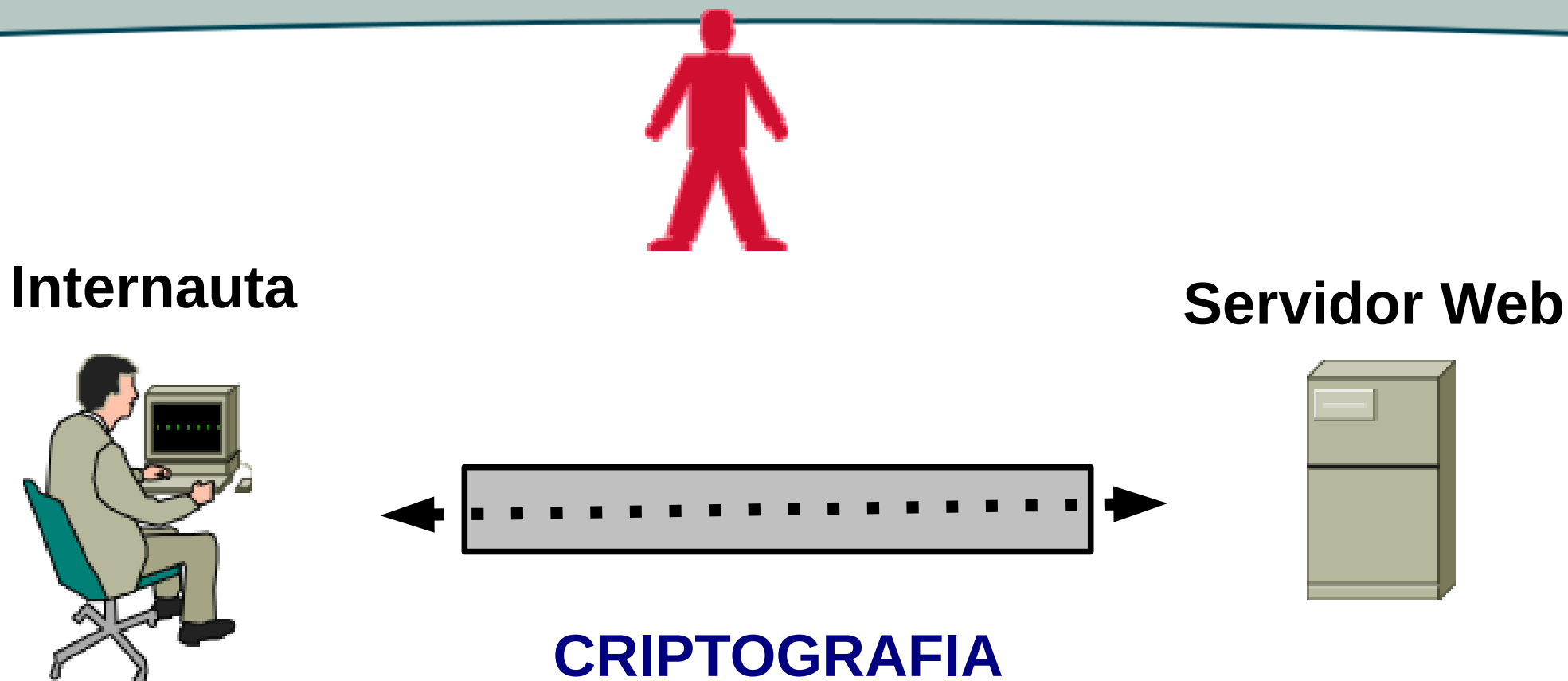
3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?

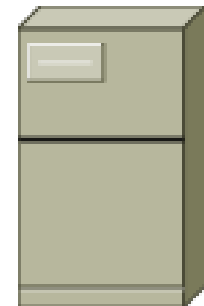


3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web

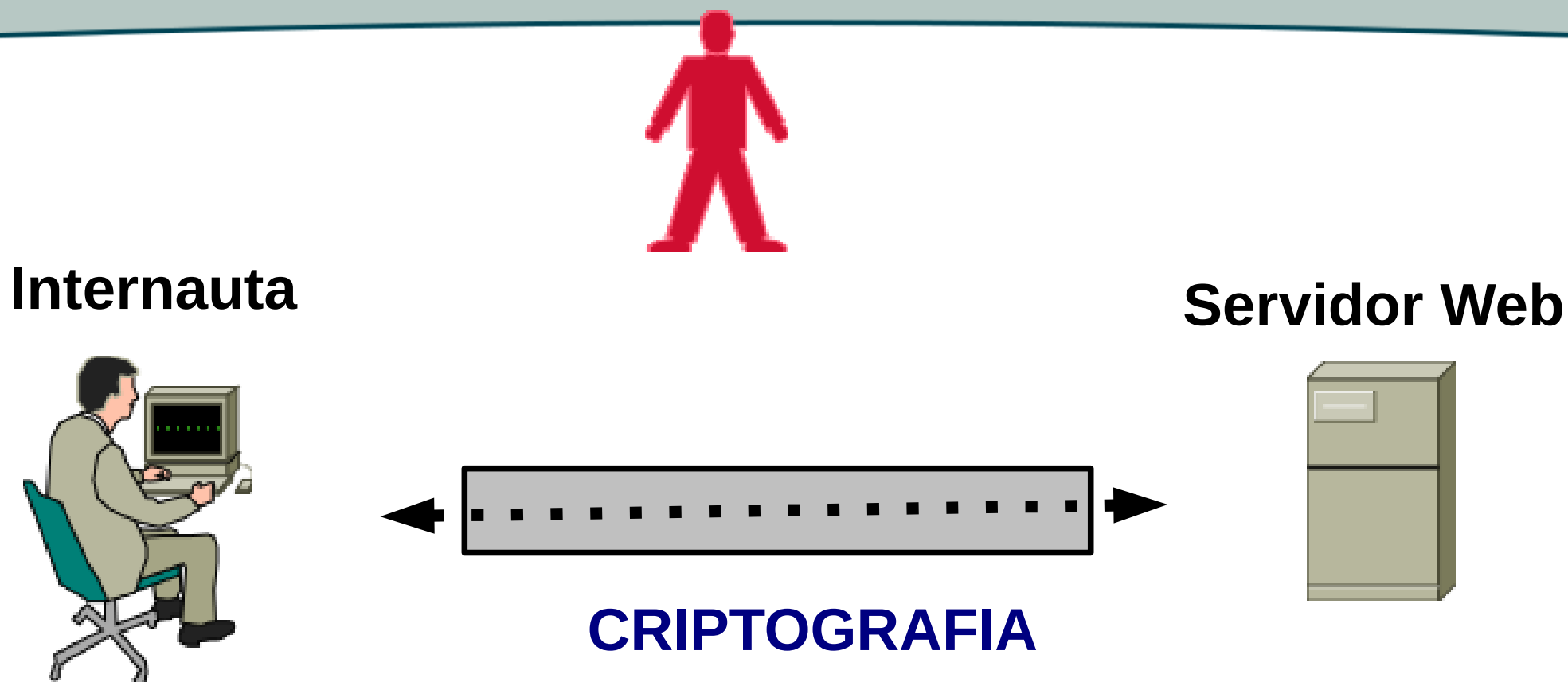


CRIPTOGRAFIA

3 – Confiar Autoridades Certificadoras?

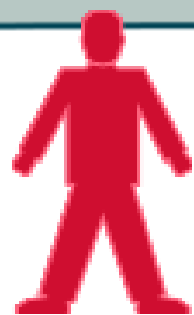


3 – Confiar Autoridades Certificadoras?



Chave Secreta
Dados Criptografados

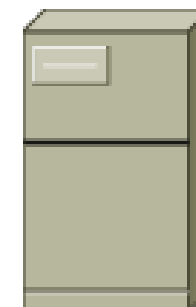
3 – Confiar Autoridades Certificadoras?



Internauta



Servidor Web

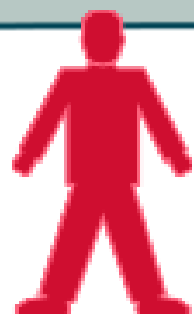


CRIPTOGRAFIA

K

Chave Secreta
Dados Criptografados

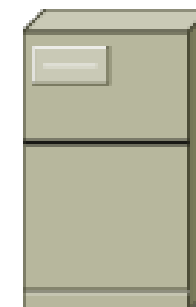
3 – Confiar Autoridades Certificadoras?



Internauta



Servidor Web



CRIPTOGRAFIA

K K

Chave Secreta
Dados Criptografados

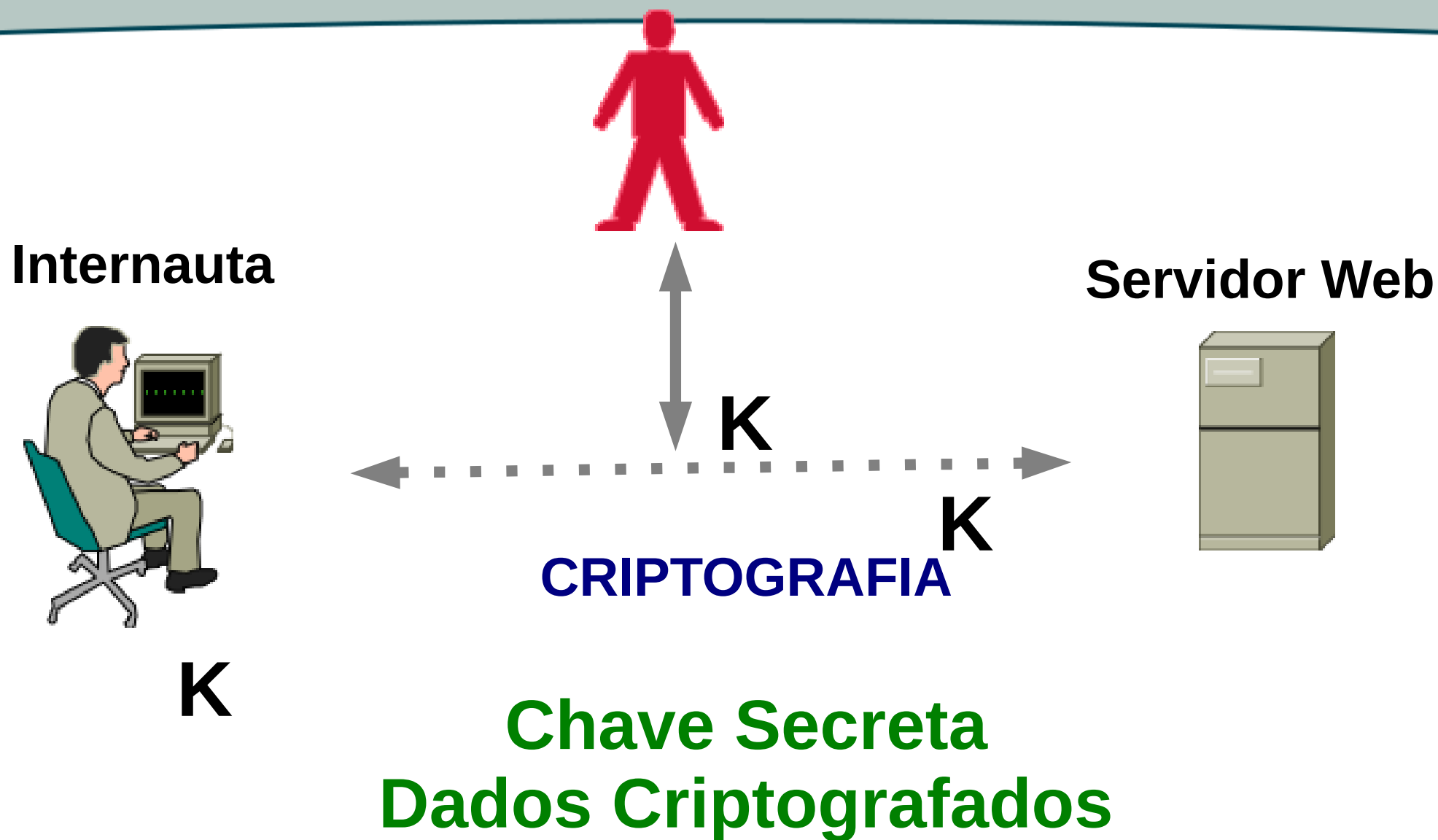
3 – Confiar Autoridades Certificadoras?



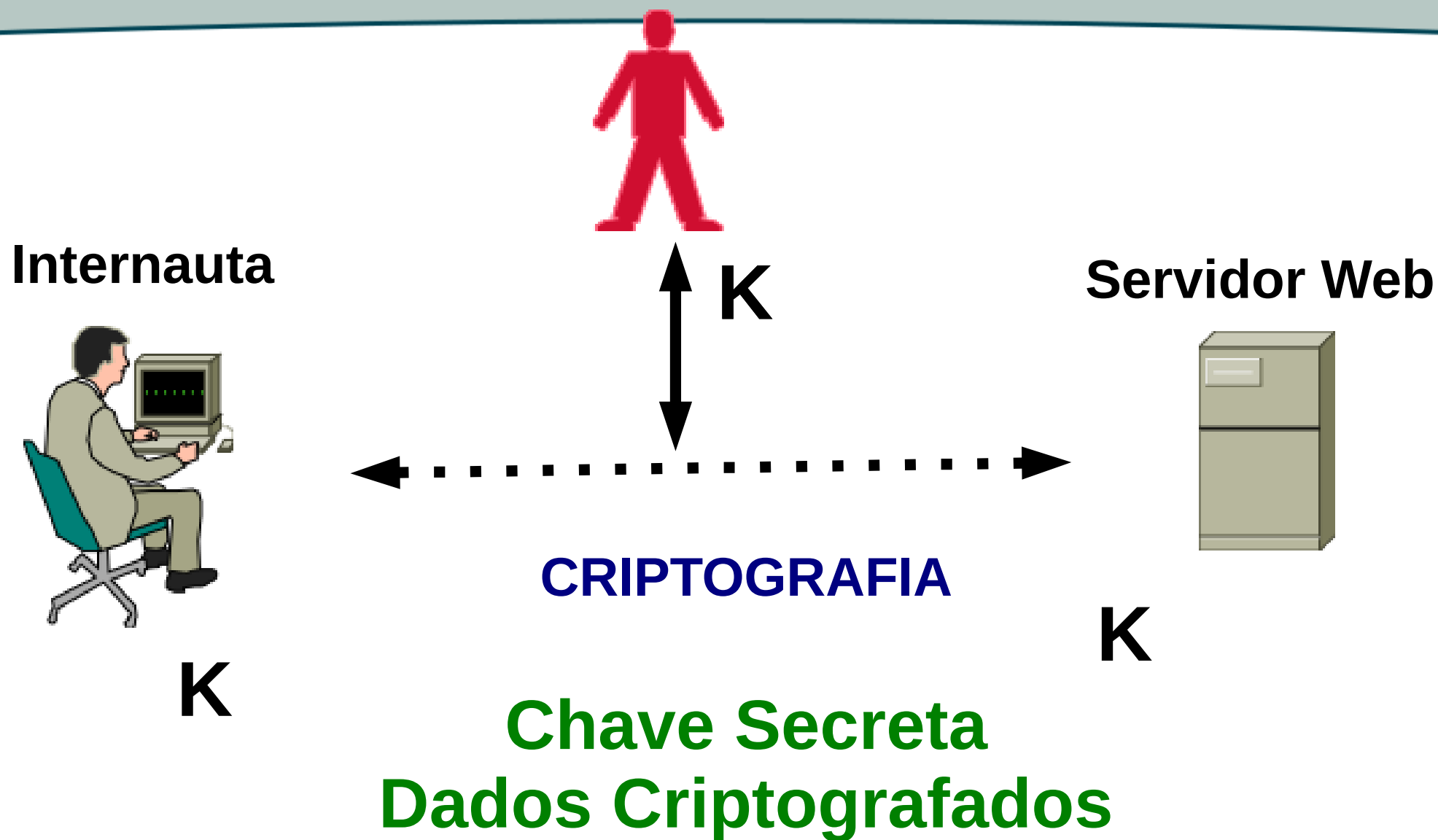
3 – Confiar Autoridades Certificadoras?



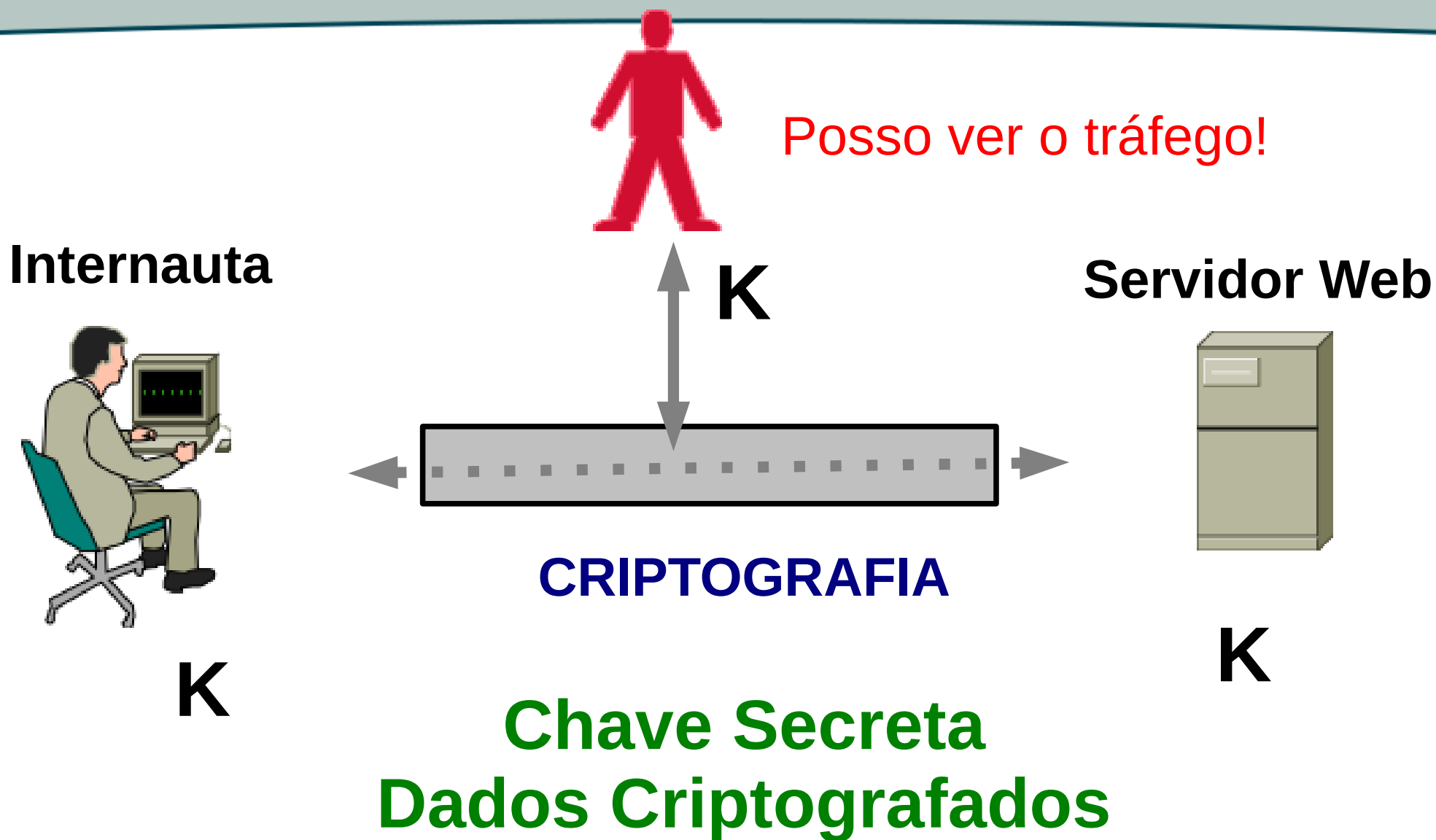
3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?

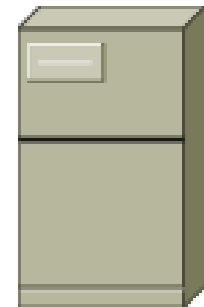


3 – Confiar Autoridades Certificadoras?

Internauta

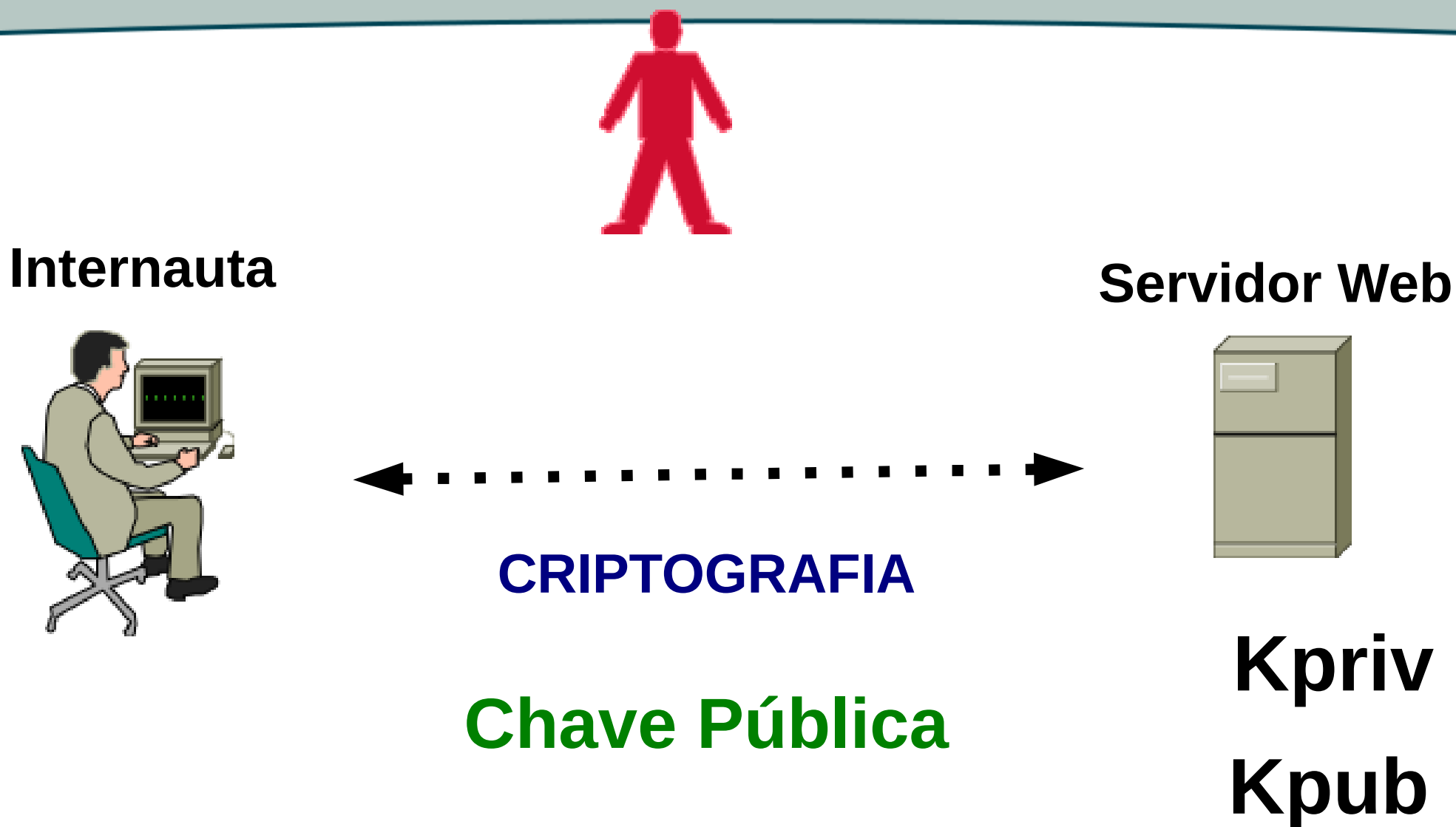


Servidor Web

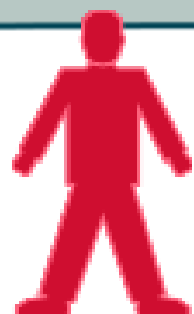


CRIPTOGRAFIA

3 – Confiar Autoridades Certificadoras?



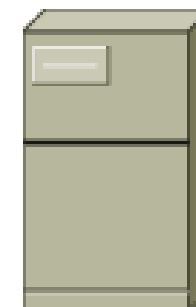
3 – Confiar Autoridades Certificadoras?



Internauta



Servidor Web



CRIPTOGRAFIA

K

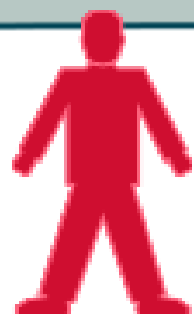
Chave Pública

Chave Secreta Criptografada

Kpriv

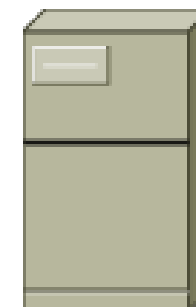
Kpub

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



CRIPTOGRAFIA

K

Chave Pública

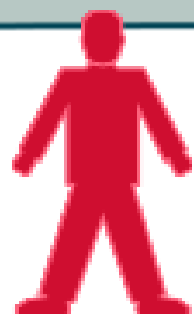
Kpriv

Chave Secreta Criptografada

Kpub

Dados Criptografados

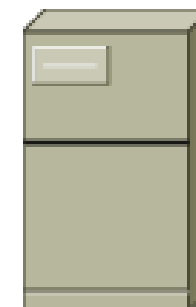
3 – Confiar Autoridades Certificadoras?



Internauta



Servidor Web



CRIPTOGRAFIA

K

Chave Pública

K_{pub}

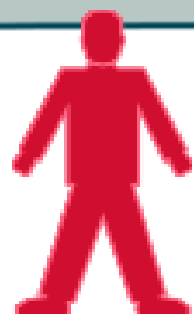
K_{priv}

Chave Secreta Criptografada

K_{pub}

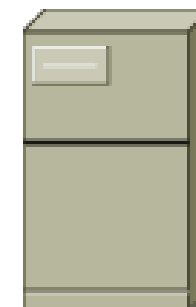
Dados Criptografados

3 – Confiar Autoridades Certificadoras?



Internauta

Servidor Web



CRIPTOGRAFIA K_{pub}

K

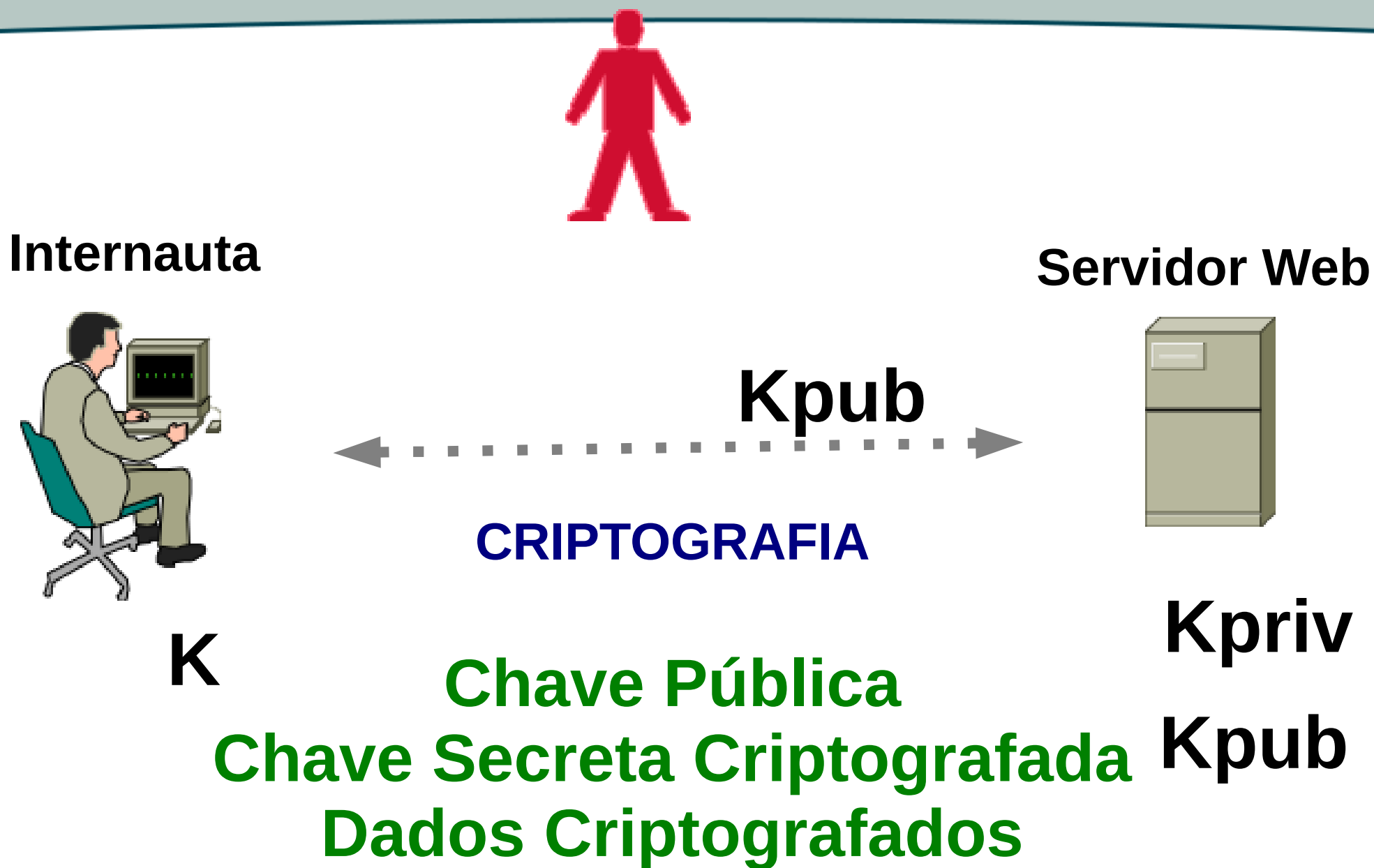
Chave Pública

K_{priv}

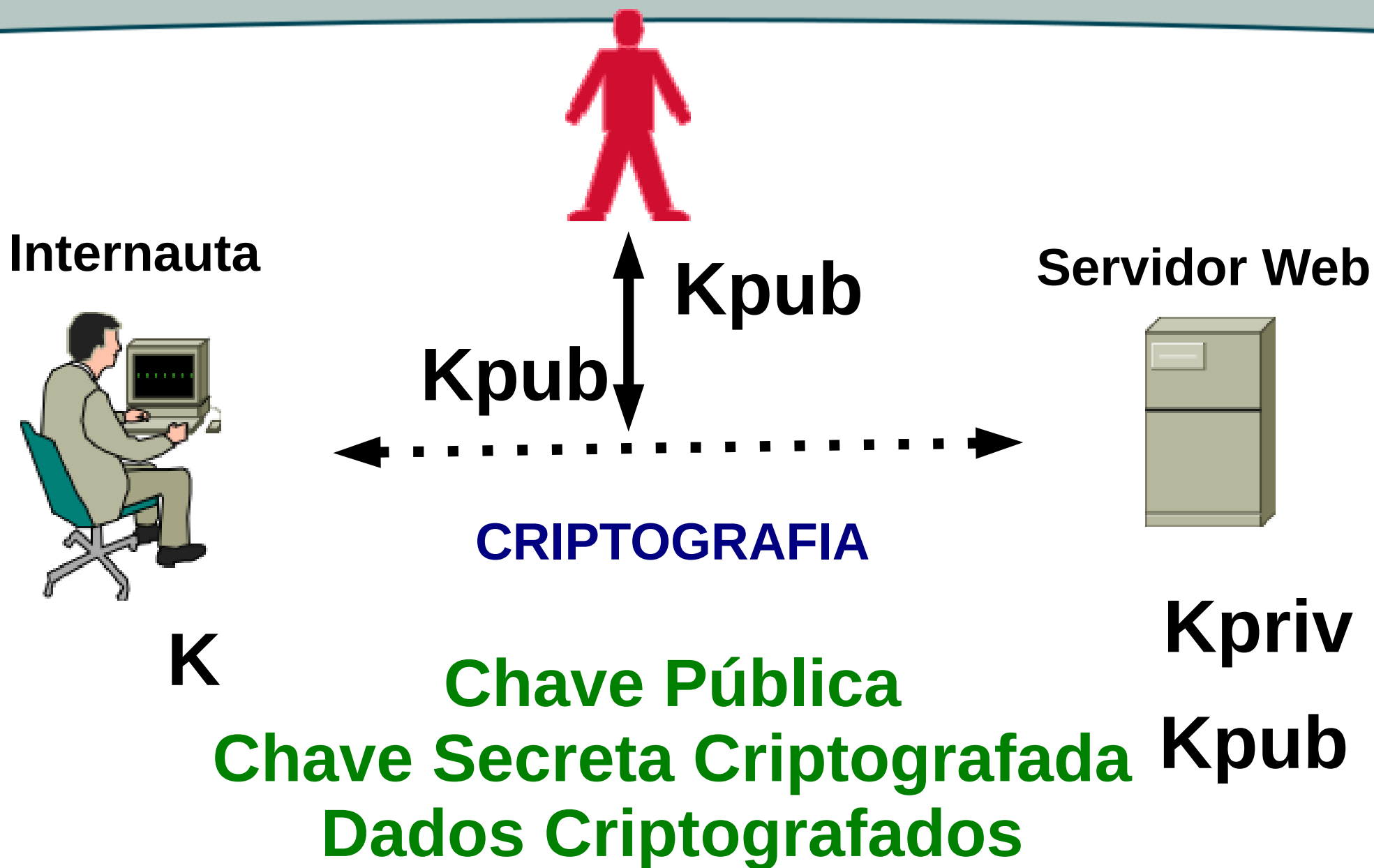
Chave Secreta Criptografada K_{pub}

Dados Criptografados

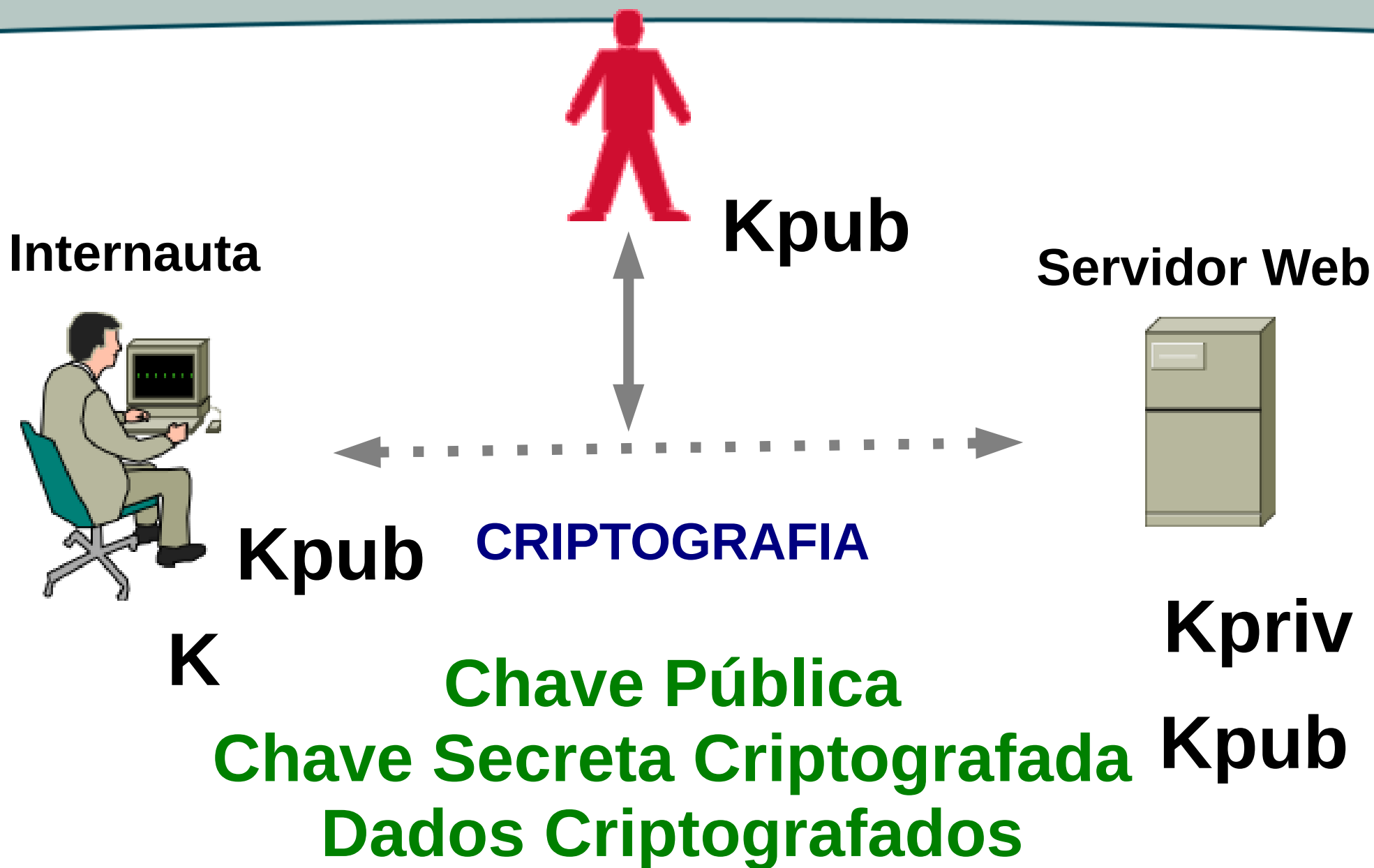
3 – Confiar Autoridades Certificadoras?



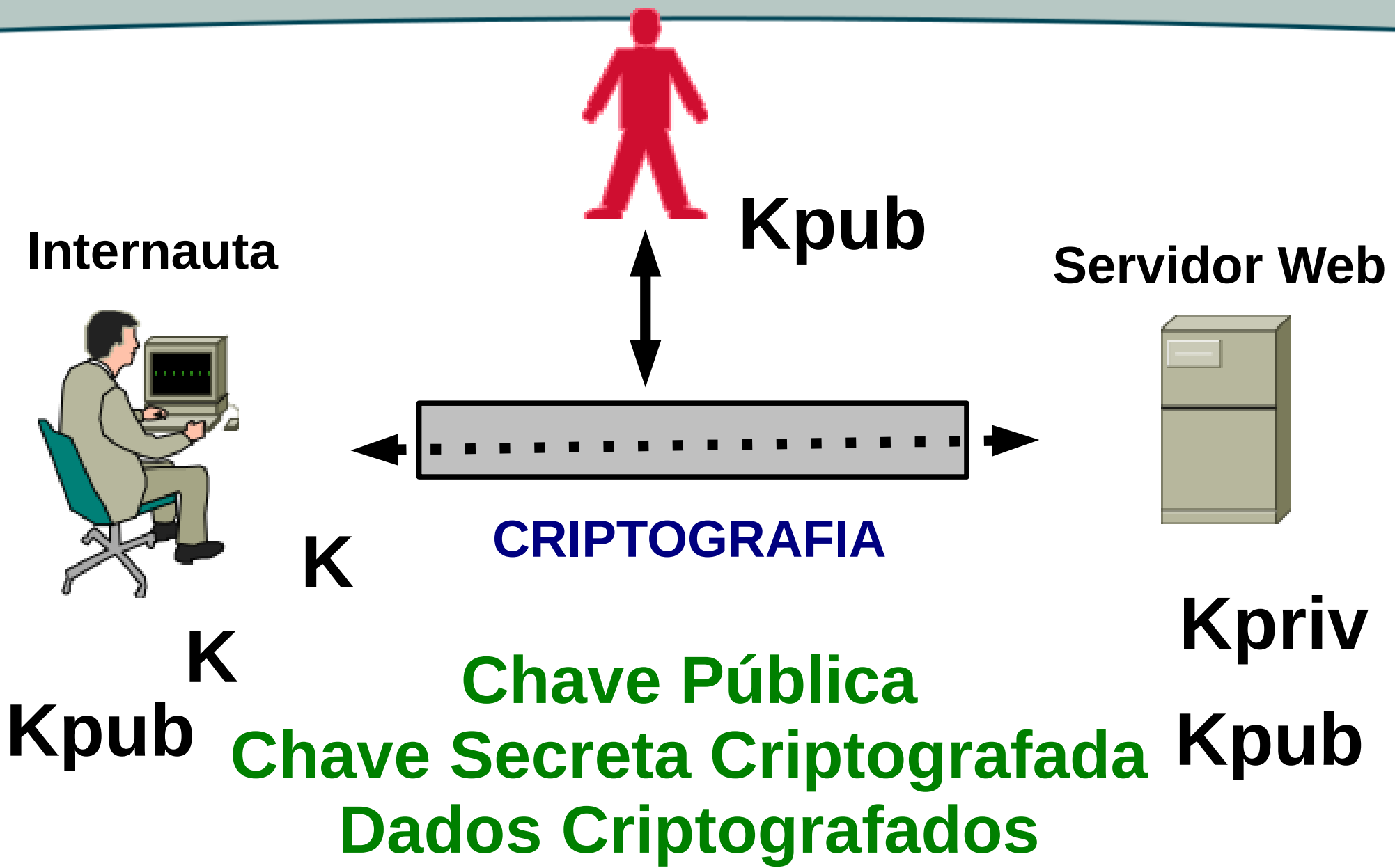
3 – Confiar Autoridades Certificadoras?



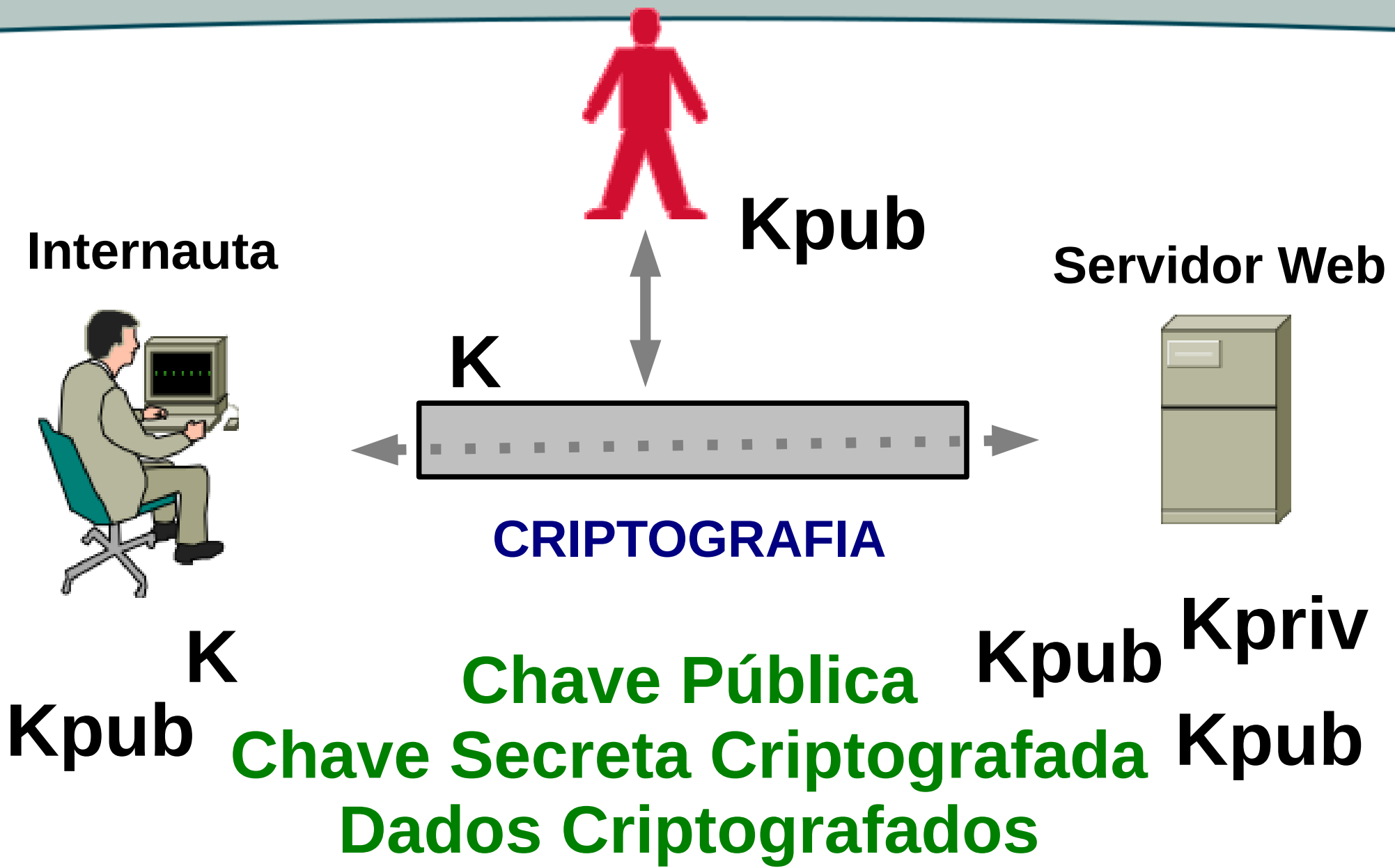
3 – Confiar Autoridades Certificadoras?



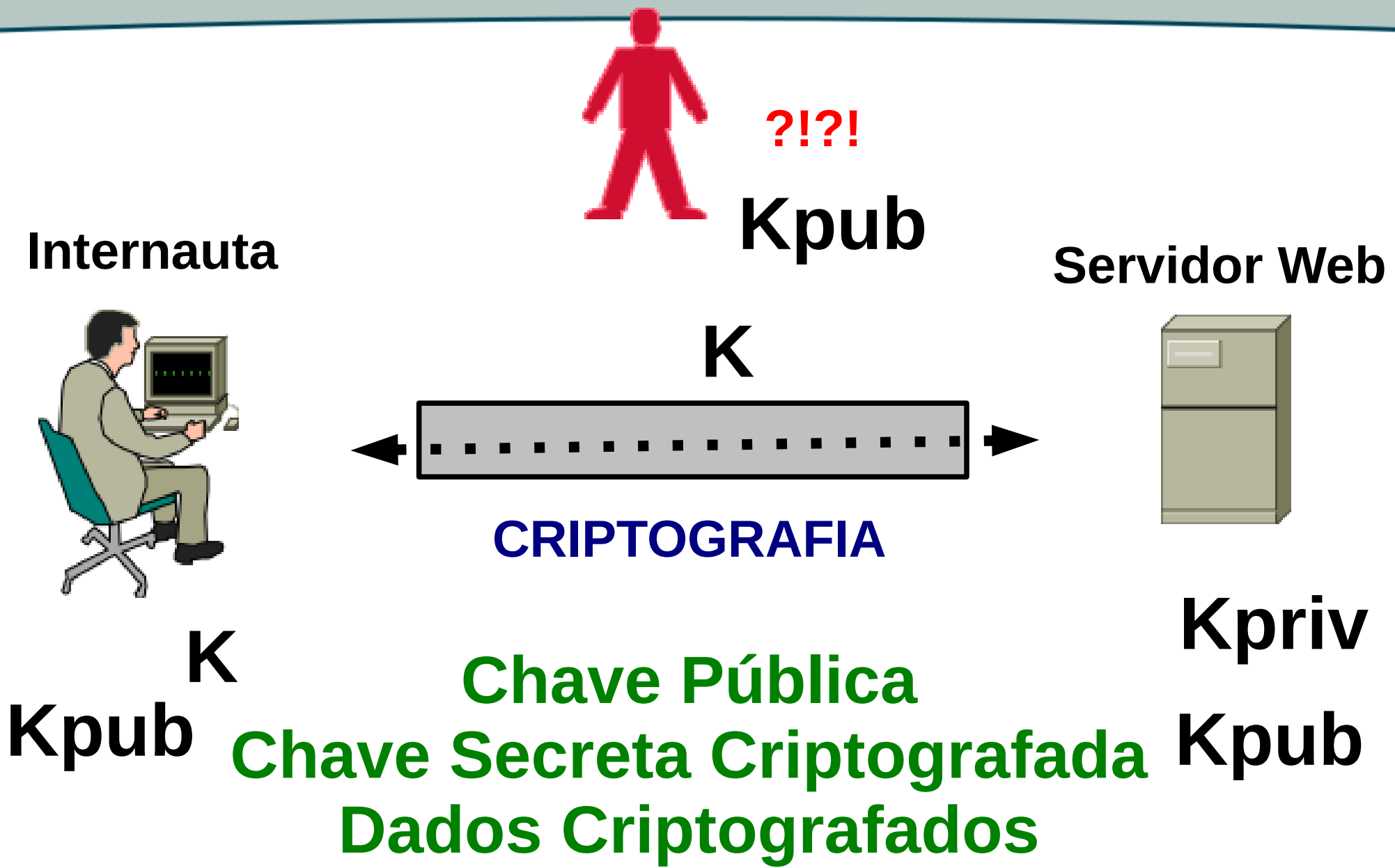
3 – Confiar Autoridades Certificadoras?



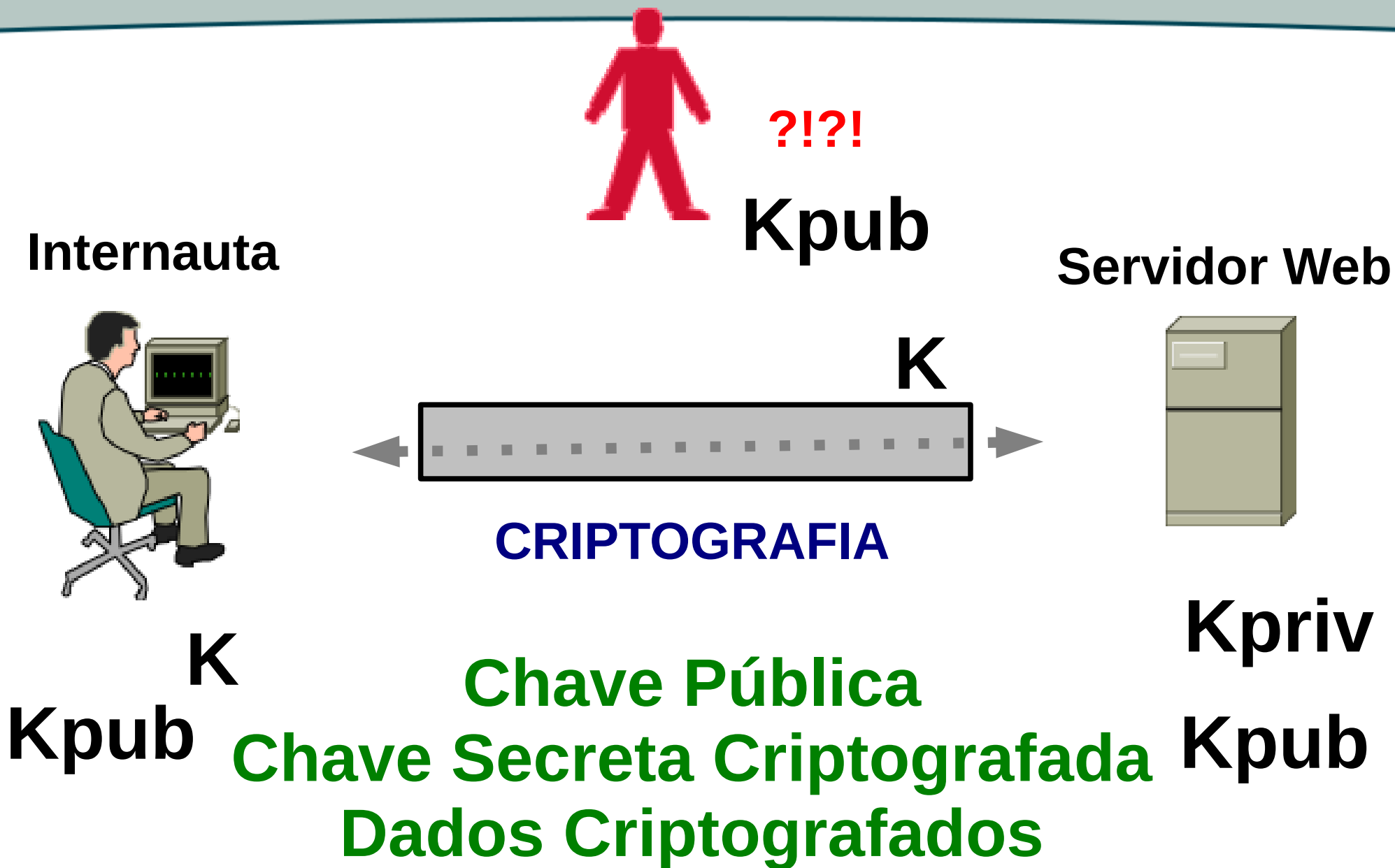
3 – Confiar Autoridades Certificadoras?



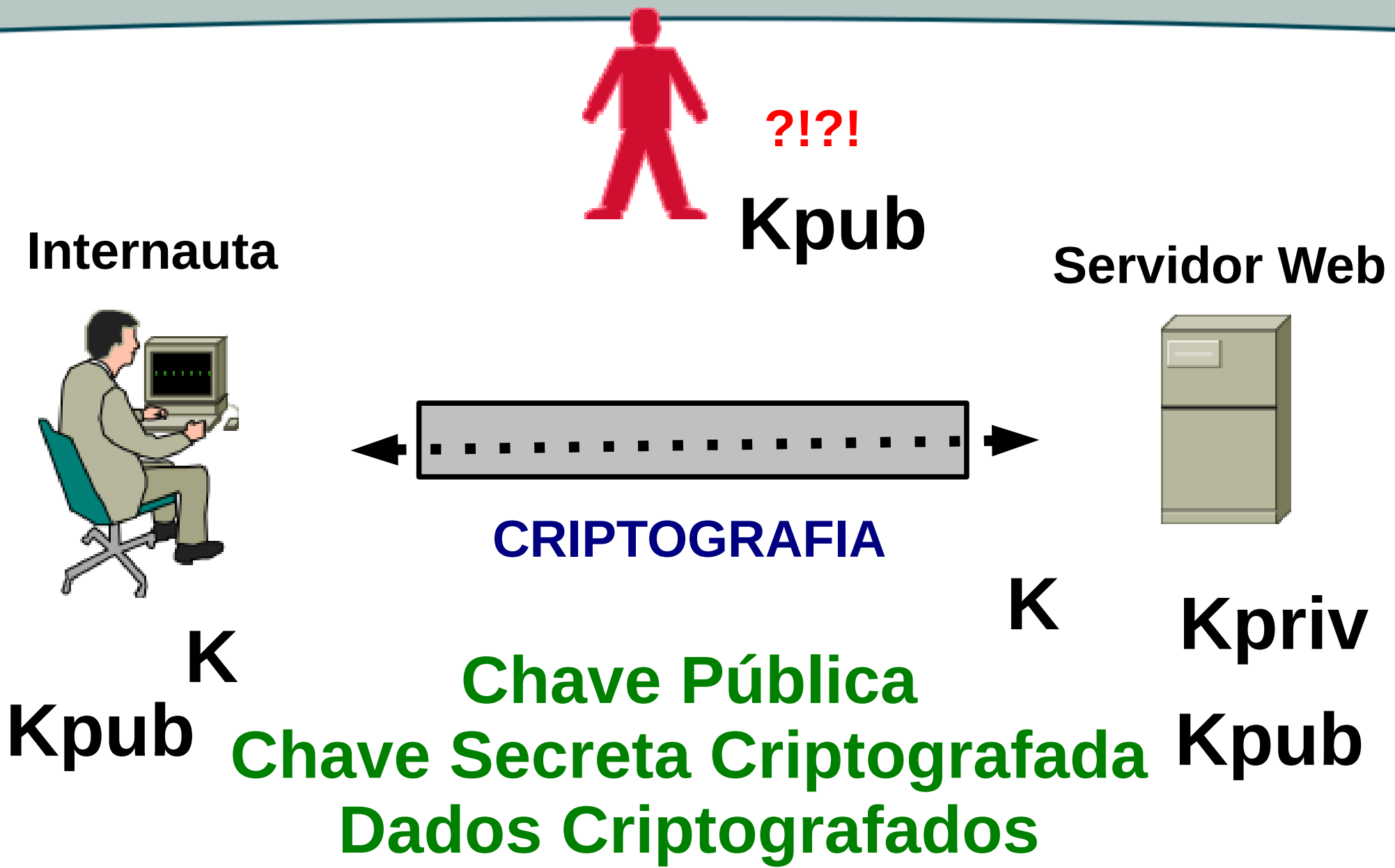
3 – Confiar Autoridades Certificadoras?



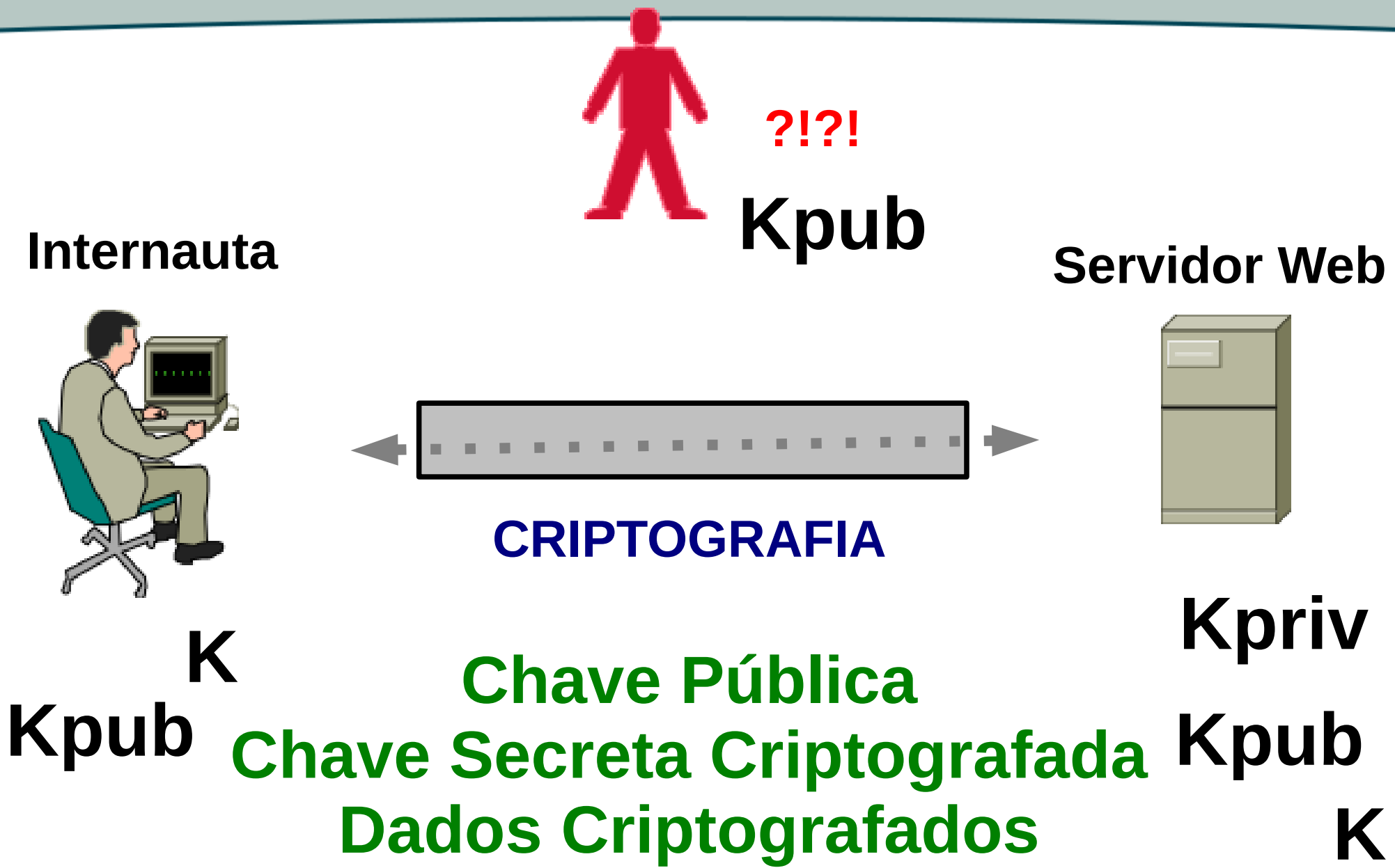
3 – Confiar Autoridades Certificadoras?



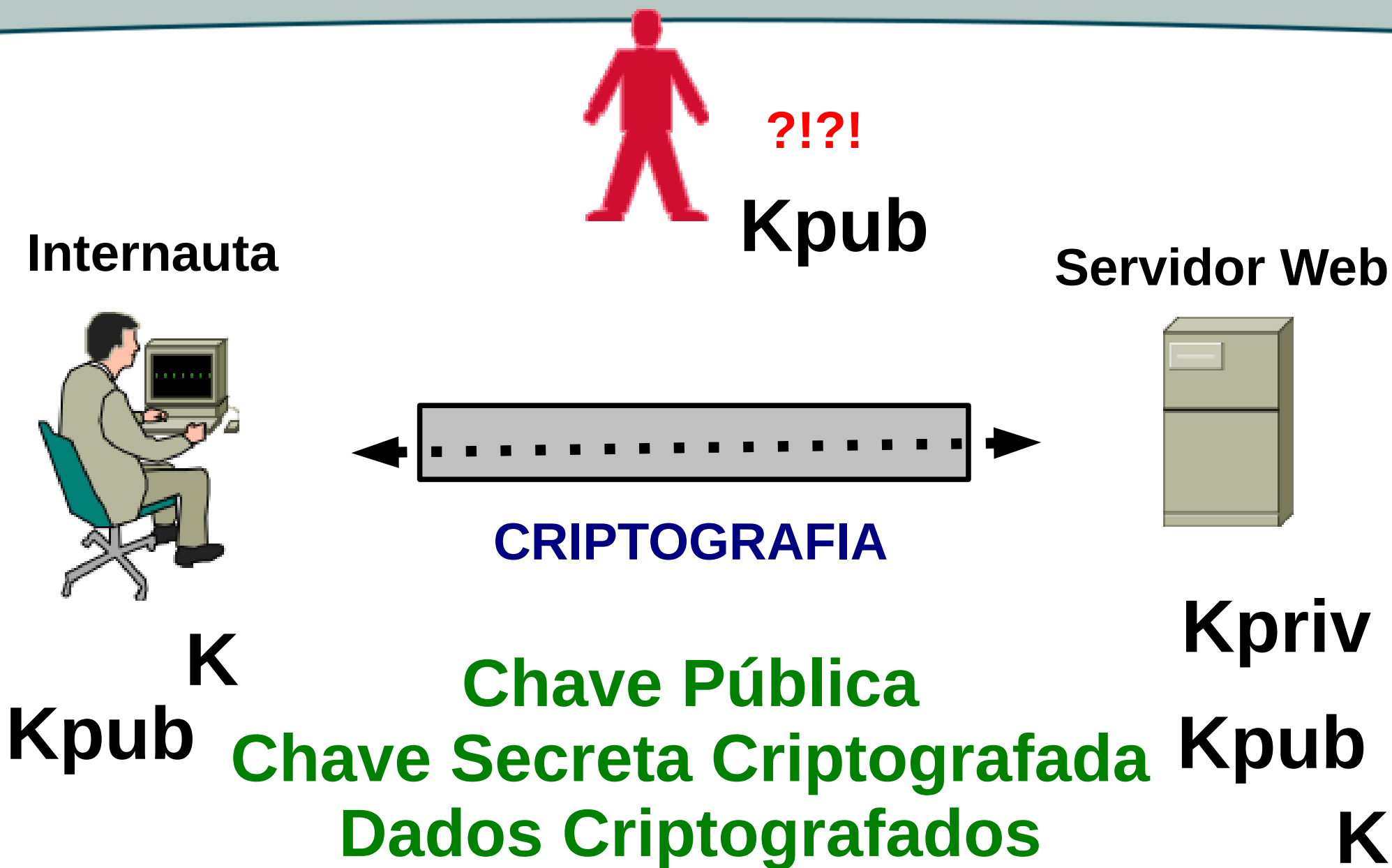
3 – Confiar Autoridades Certificadoras?



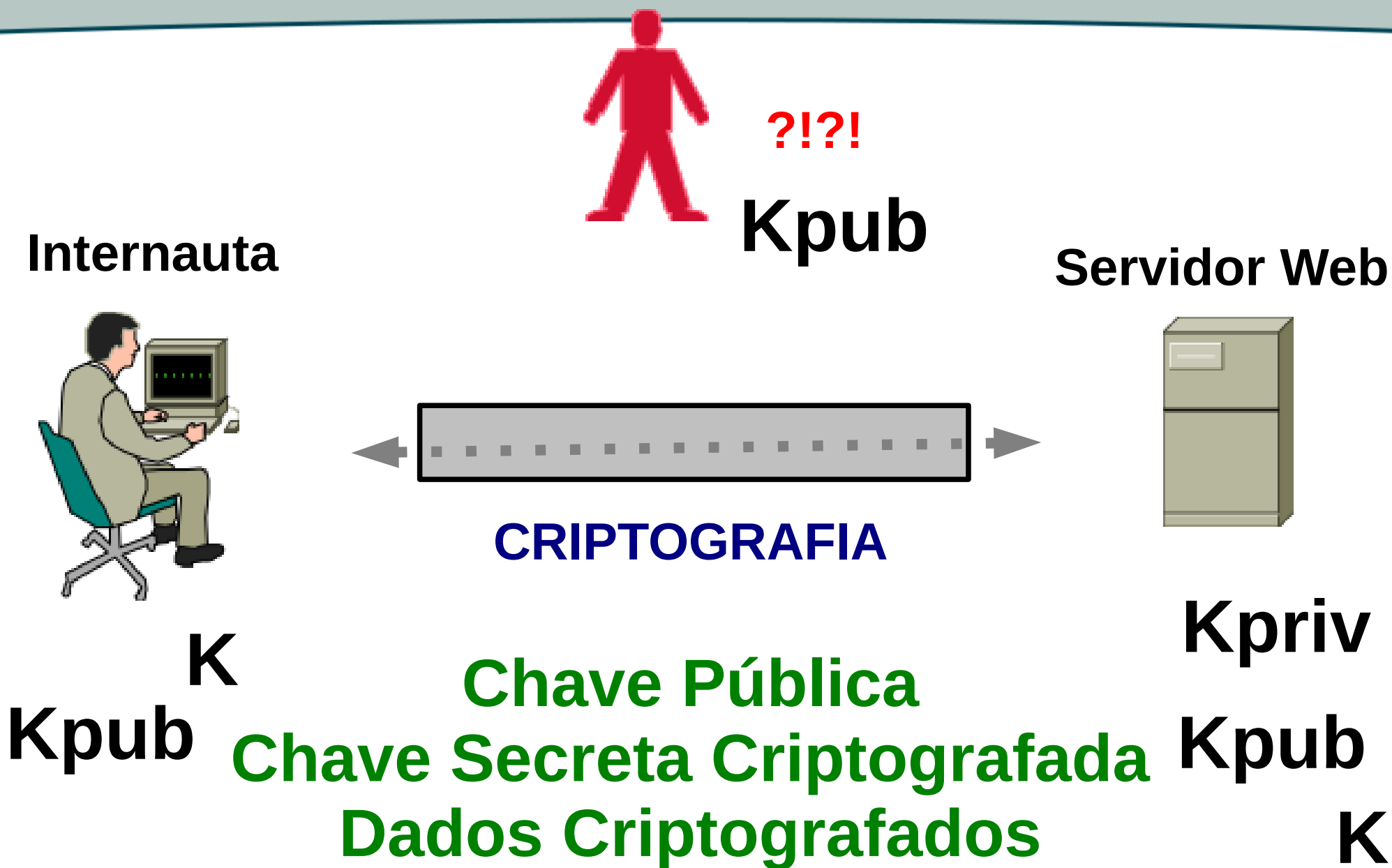
3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



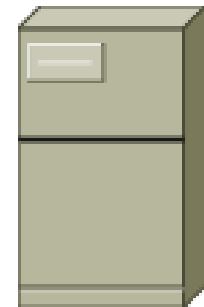
Internauta



Protocolo SSL

**Netscape
(1994)**

Servidor Web



3 – Confiar Autoridades Certificadoras?

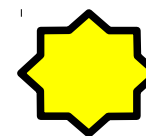
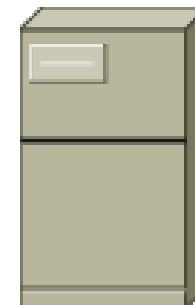
Internauta



Protocolo SSL

**Netscape
(1994)**

Servidor Web



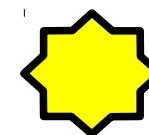
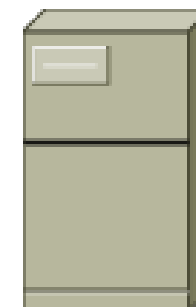
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



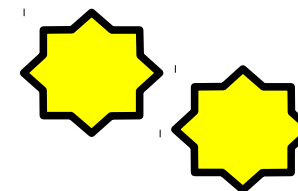
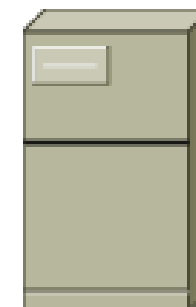
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



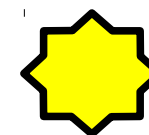
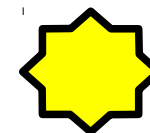
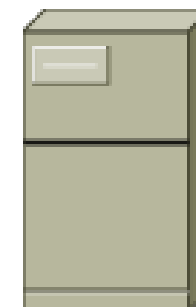
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



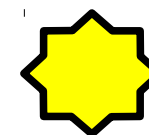
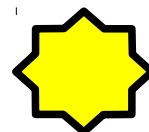
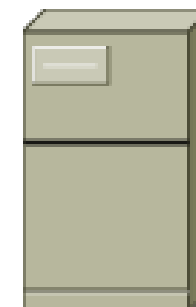
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



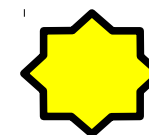
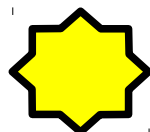
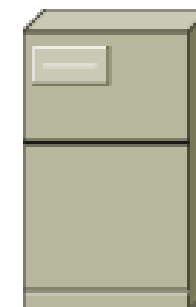
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



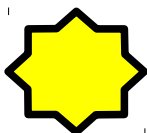
Servidor Web



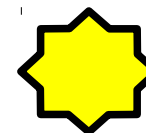
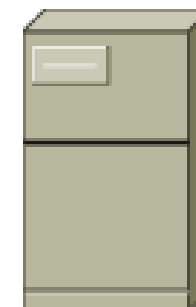
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



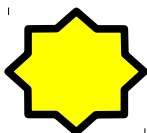
Servidor Web



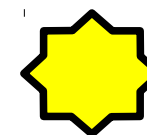
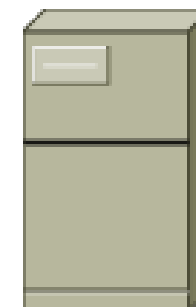
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



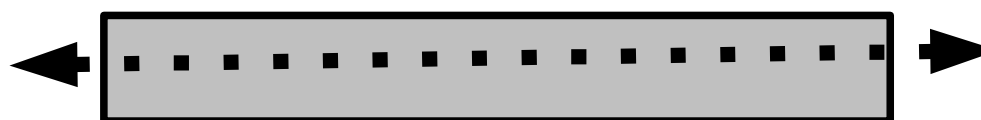
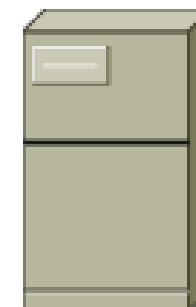
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



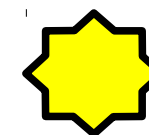
Servidor Web



HTTP + SSL

=

HTTPS



**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

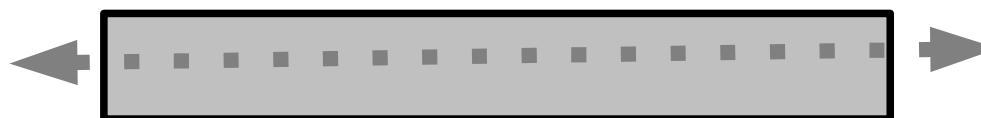
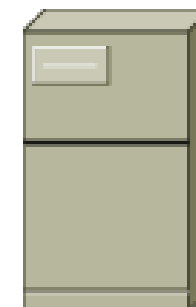


?!?!

Internauta



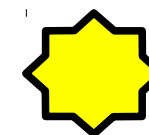
Servidor Web



HTTP + SSL

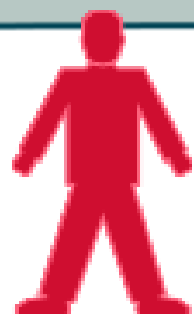
=

HTTPS



**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

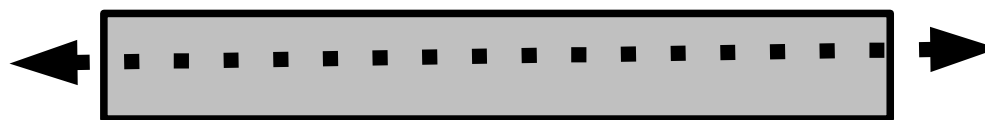
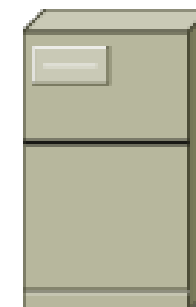


?!?!

Internauta



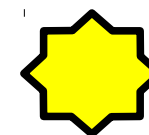
Servidor Web



HTTP + SSL

=

HTTPS



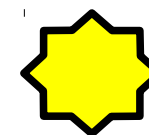
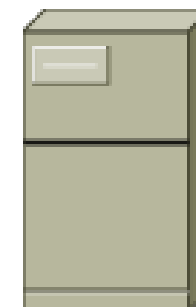
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

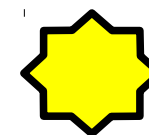
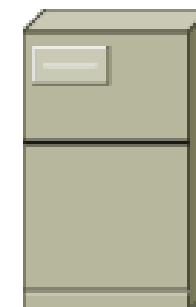
Internauta



Atacante



Servidor Web



**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta

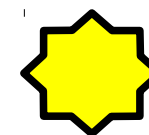
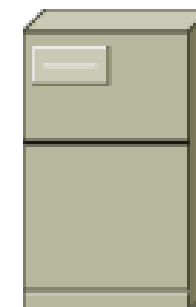


Atacante



**CERTIFICADO
DIGITAL**

Servidor Web



**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

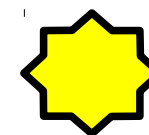
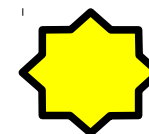
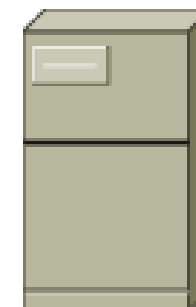
Internauta



Atacante



Servidor Web



**CERTIFICADO
DIGITAL**

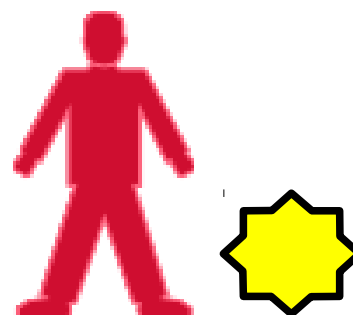
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

Internauta

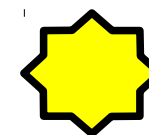
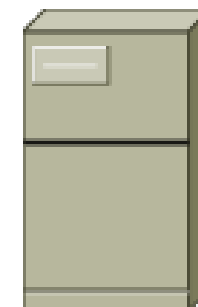


Atacante



**CERTIFICADO
DIGITAL**

Servidor Web



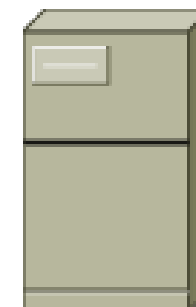
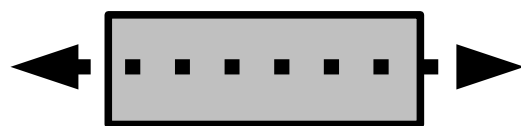
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

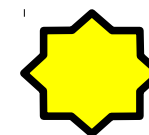
Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**



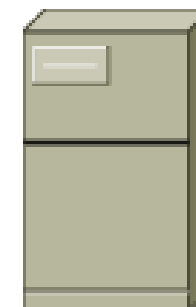
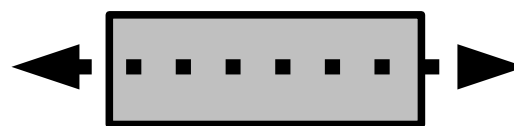
**CERTIFICADO
DIGITAL**

Ataque do Homem Intermediário

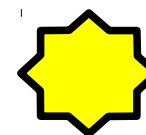
Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**



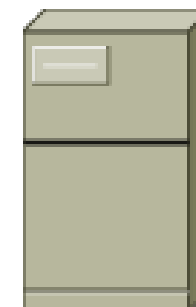
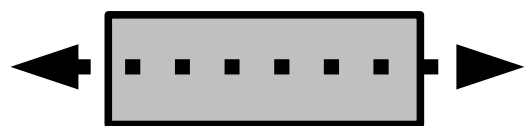
**CERTIFICADO
DIGITAL**

Ataque do Homem Intermediário

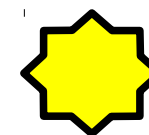
Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**



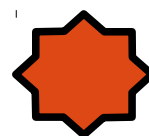
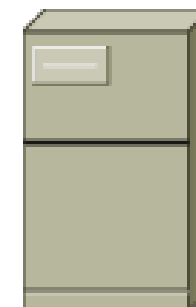
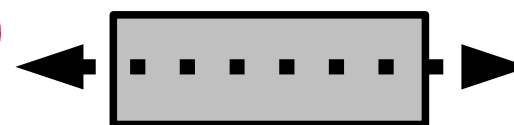
**CERTIFICADO
DIGITAL**

Ataque do Homem Intermediário

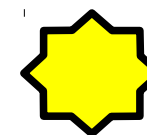
Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**



**CERTIFICADO
DIGITAL**

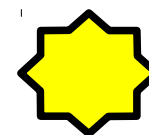
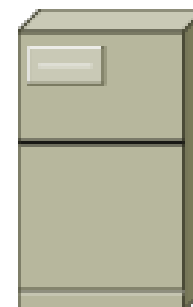
3 – Confiar Autoridades Certificadoras?

Solução: Autoridade Certificadora

Internauta



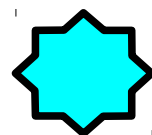
Servidor Web



**CERTIFICADO
DIGITAL**

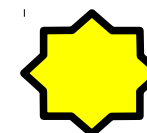
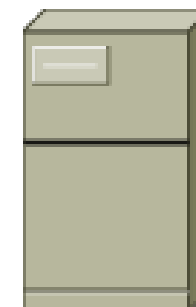
3 – Confiar Autoridades Certificadoras?

Internauta



**CERTIFICADO
DIGITAL
AUTORIDADE**

Servidor Web



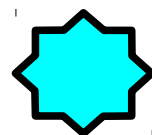
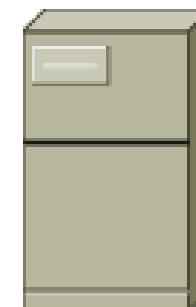
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

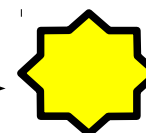
Internauta



Servidor Web



**CERTIFICADO
DIGITAL
AUTORIDADE**



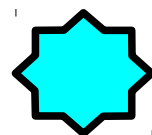
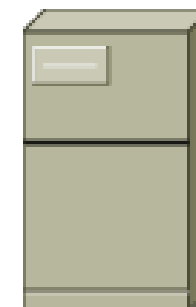
**CERTIFICADO
DIGITAL**

3 – Confiar Autoridades Certificadoras?

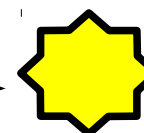
Internauta



Servidor Web



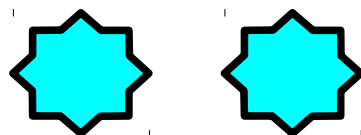
**CERTIFICADO
DIGITAL
AUTORIDADE**



**CERTIFICADO
DIGITAL
VÁLIDO**

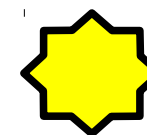
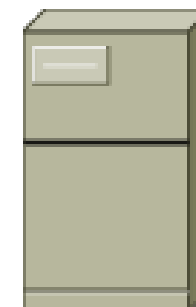
3 – Confiar Autoridades Certificadoras?

Internauta



**CERTIFICADO
DIGITAL
AUTORIDADE**

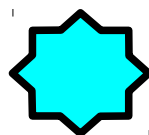
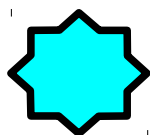
Servidor Web



**CERTIFICADO
DIGITAL
VÁLIDO**

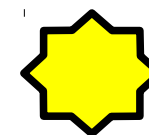
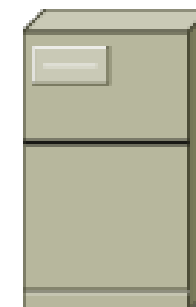
3 – Confiar Autoridades Certificadoras?

Internauta



**CERTIFICADO
DIGITAL
AUTORIDADE**

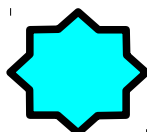
Servidor Web



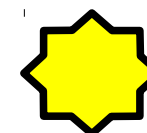
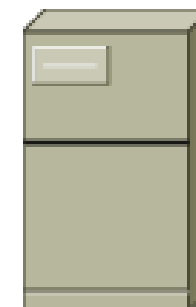
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web



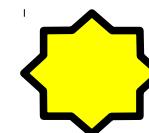
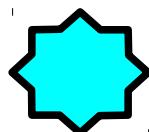
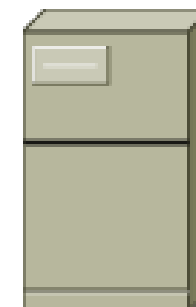
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**

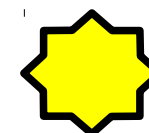
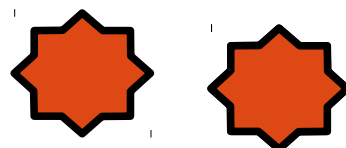
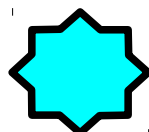
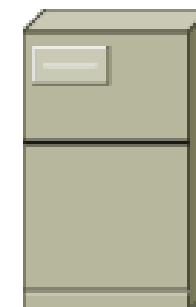
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**

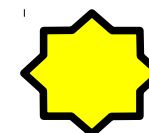
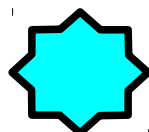
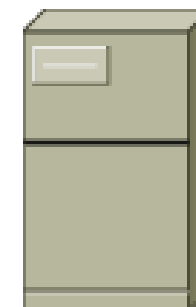
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**

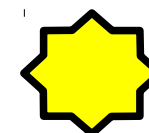
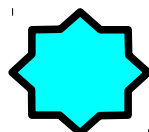
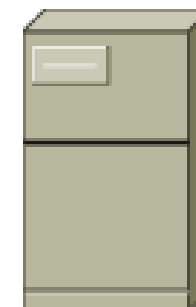
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



**CERTIFICADO
DIGITAL**

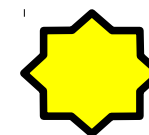
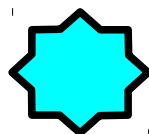
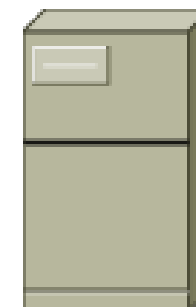
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



Não Aceito!
Certificado INVÁLIDO!

**CERTIFICADO
DIGITAL**

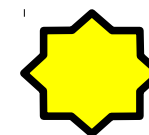
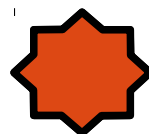
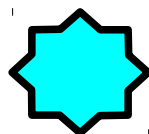
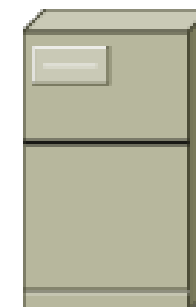
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



**Não Aceito!
Certificado INVÁLIDO!**

**CERTIFICADO
DIGITAL**

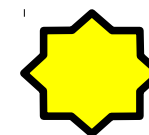
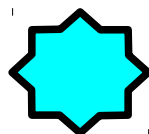
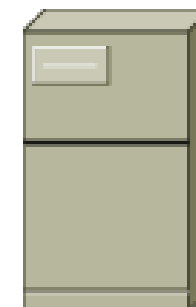
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

Atacante

Servidor Web



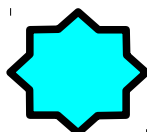
**Não Aceito!
Certificado INVÁLIDO!**

**CERTIFICADO
DIGITAL**

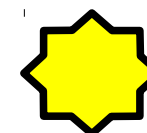
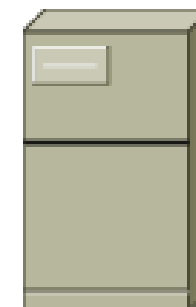
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta



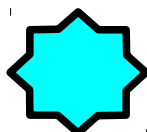
Servidor Web



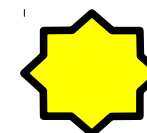
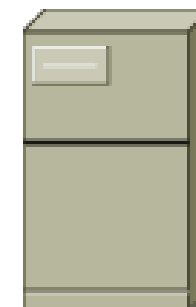
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web

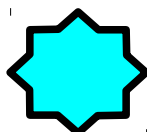


**CERTIFICADO
DIGITAL
VÁLIDO**

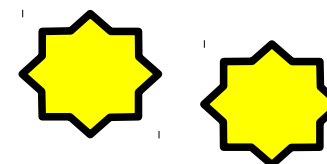
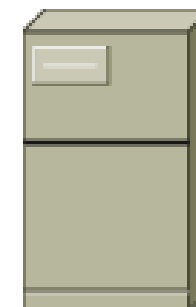


3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web

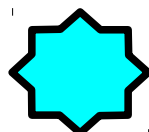


**CERTIFICADO
DIGITAL
VÁLIDO**

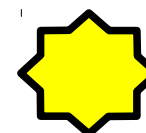


3 – Confiar Autoridades Certificadoras?

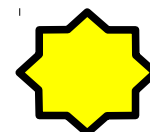
Internauta



Servidor Web



**CERTIFICADO
DIGITAL
VÁLIDO**

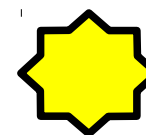
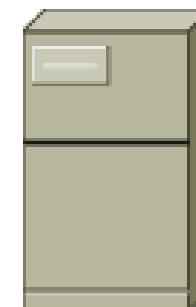


3 – Confiar Autoridades Certificadoras?

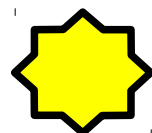
Internauta



Servidor Web

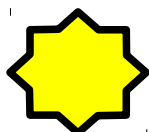
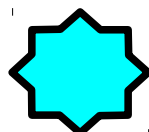


**CERTIFICADO
DIGITAL
VÁLIDO**

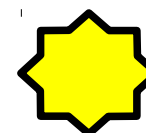
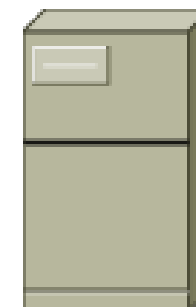


3 – Confiar Autoridades Certificadoras?

Internauta



Servidor Web

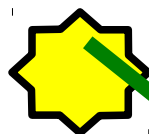
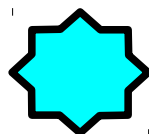


**CERTIFICADO
DIGITAL
VÁLIDO**



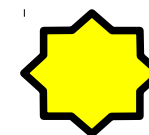
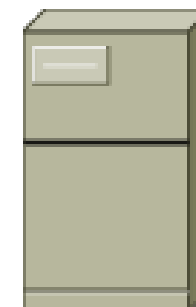
3 – Confiar Autoridades Certificadoras?

Internauta



Verificado! Ok!

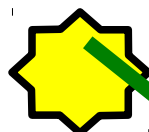
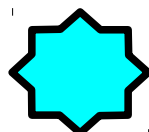
Servidor Web



**CERTIFICADO
DIGITAL
VÁLIDO**

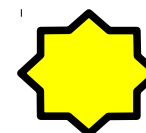
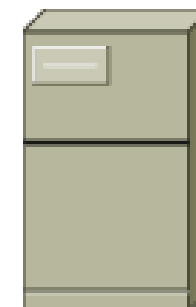
3 – Confiar Autoridades Certificadoras?

Internauta



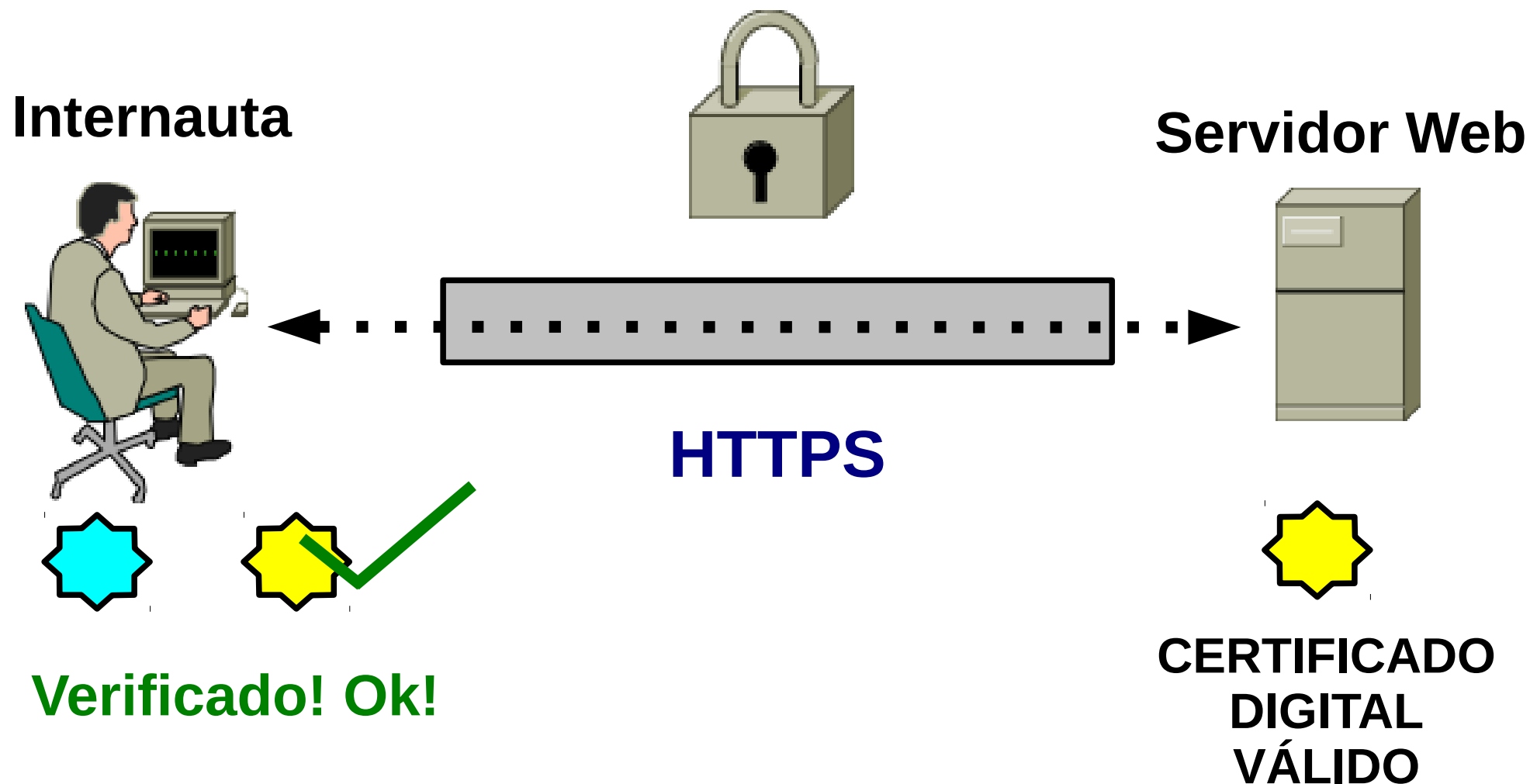
Verificado! Ok!

Servidor Web

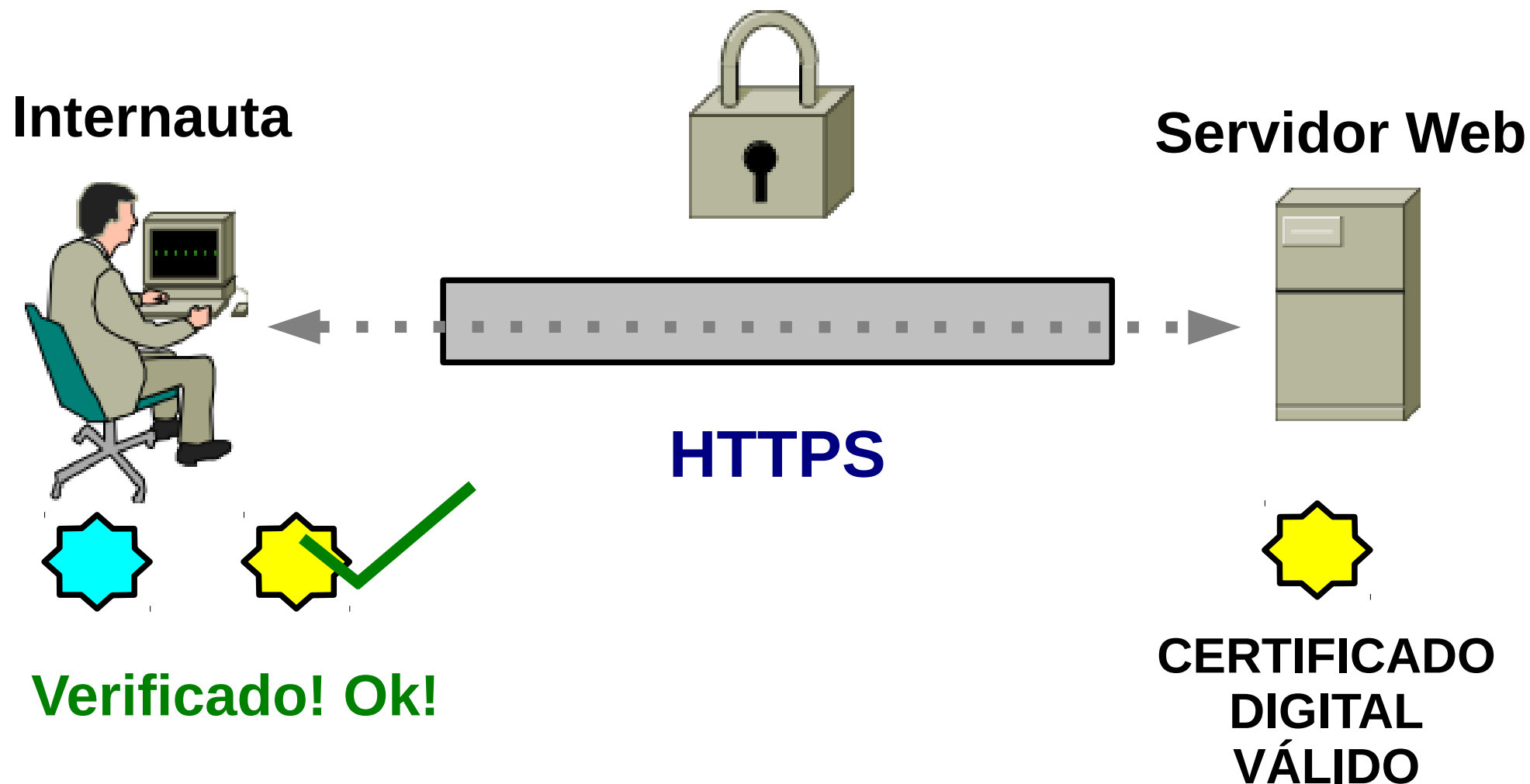


**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

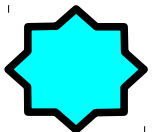


3 – Confiar Autoridades Certificadoras?

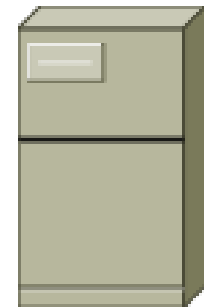


3 – Confiar Autoridades Certificadoras?

Internauta



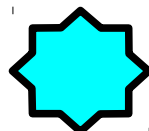
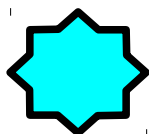
**Servidor Web
do Atacante**



**CERTIFICADO
DIGITAL
INVÁLIDO**

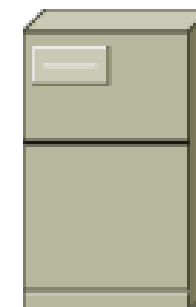
3 – Confiar Autoridades Certificadoras?

Internauta



**CERTIFICADO
AUTORIDADE**

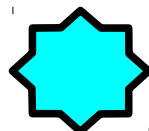
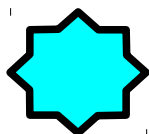
**Servidor Web
do Atacante**



**CERTIFICADO
DIGITAL
INVÁLIDO**

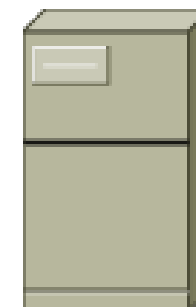
3 – Confiar Autoridades Certificadoras?

Internauta



**CERTIFICADO
AUTORIDADE**

**Servidor Web
do Atacante**



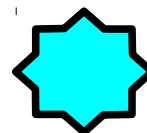
**CERTIFICADO
DIGITAL
INVÁLIDO**

3 – Confiar Autoridades Certificadoras?

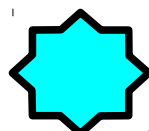
Internauta



**CERTIFICADO
COMPROMETIDO**



**Servidor Web
do Atacante**



**CERTIFICADO
AUTORIDADE**



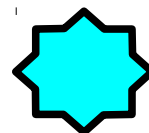
**CERTIFICADO
DIGITAL
INVÁLIDO**

3 – Confiar Autoridades Certificadoras?

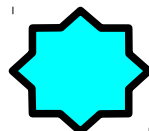
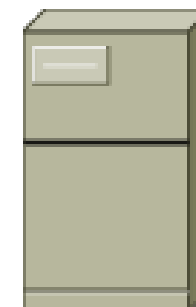
Internauta



**CERTIFICADO
COMPROMETIDO**



**Servidor Web
do Atacante**



**CERTIFICADO
AUTORIDADE**



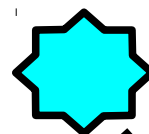
**CERTIFICADO
DIGITAL
INVÁLIDO**

3 – Confiar Autoridades Certificadoras?

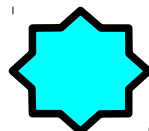
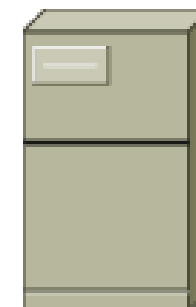
Internauta



**CERTIFICADO
COMPROMETIDO**



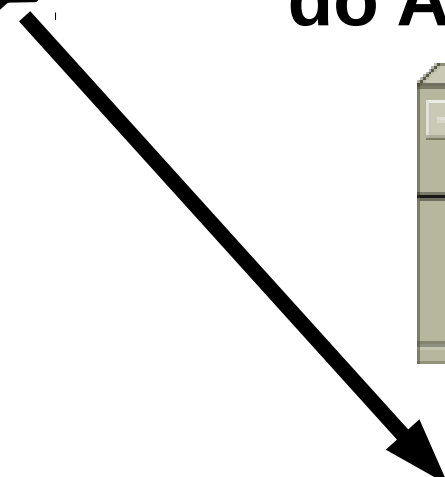
**Servidor Web
do Atacante**



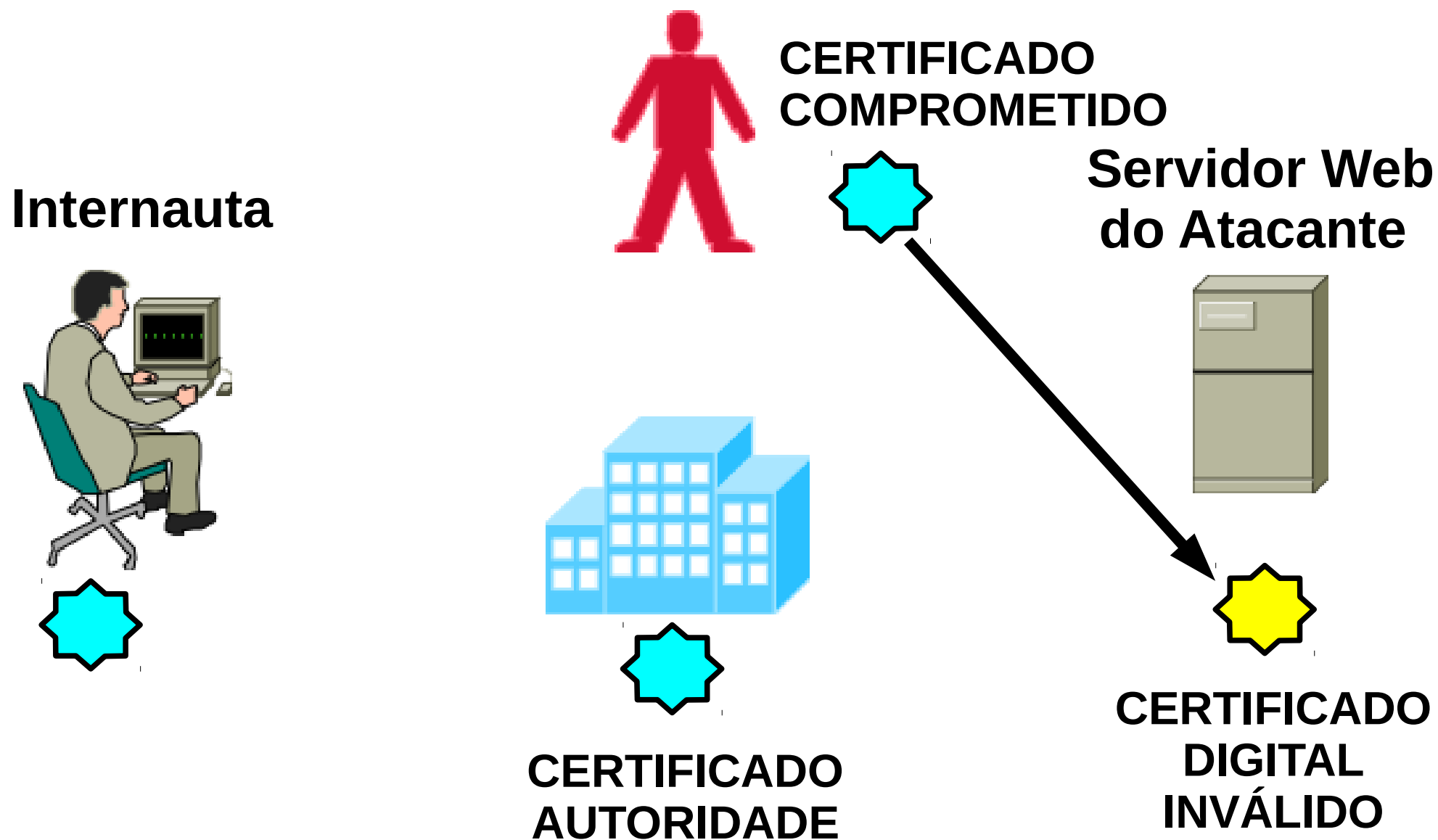
**CERTIFICADO
AUTORIDADE**



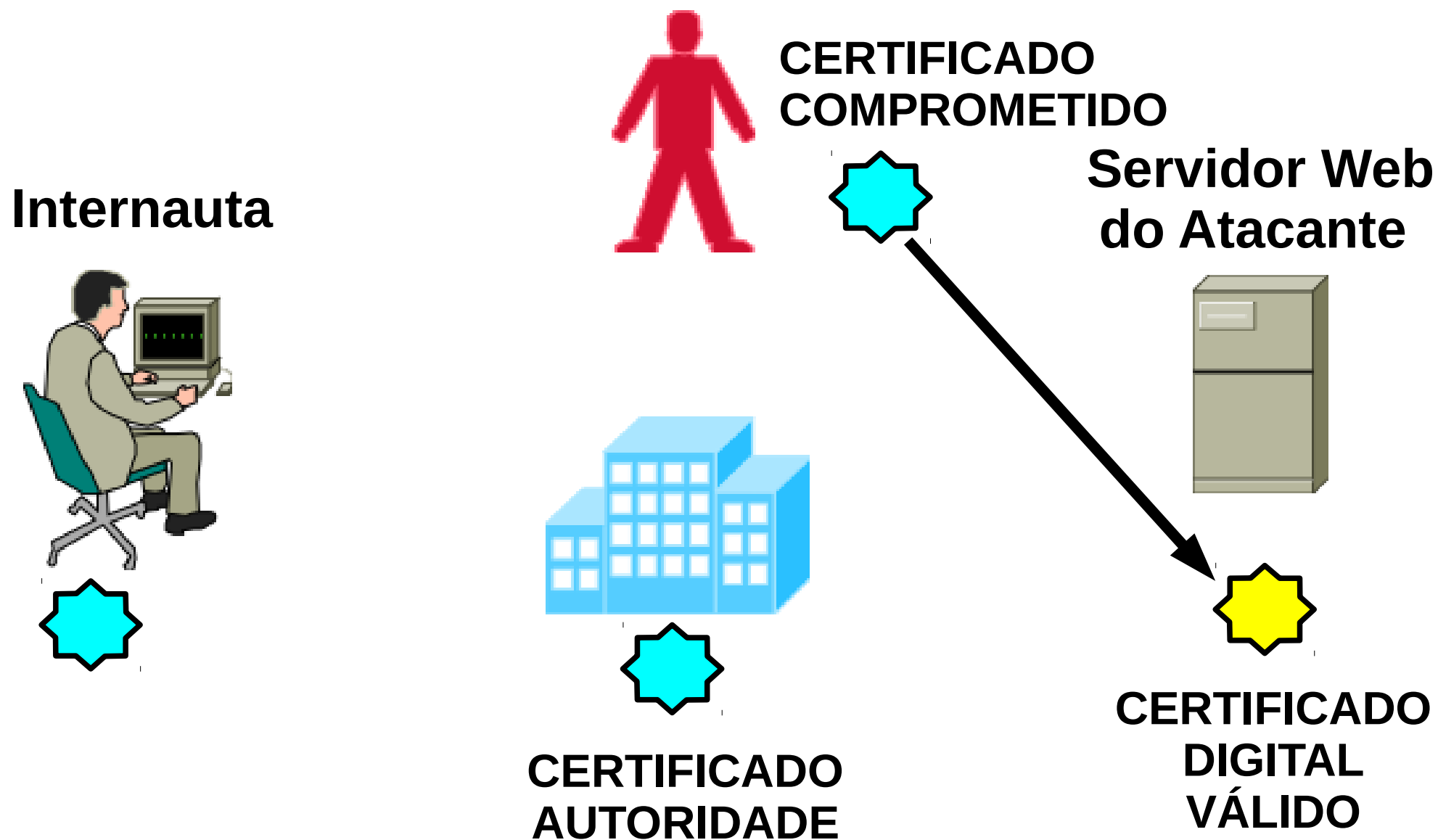
**CERTIFICADO
DIGITAL
INVÁLIDO**



3 – Confiar Autoridades Certificadoras?

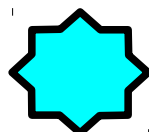


3 – Confiar Autoridades Certificadoras?

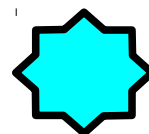


3 – Confiar Autoridades Certificadoras?

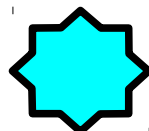
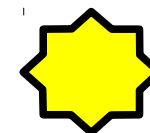
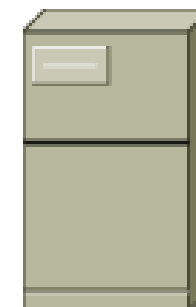
Internauta



**CERTIFICADO
COMPROMETIDO**



**Servidor Web
do Atacante**

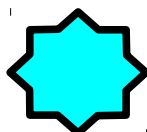


**CERTIFICADO
AUTORIDADE**

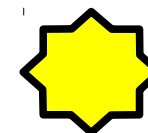
**CERTIFICADO
DIGITAL
VÁLIDO**

3 – Confiar Autoridades Certificadoras?

Internauta

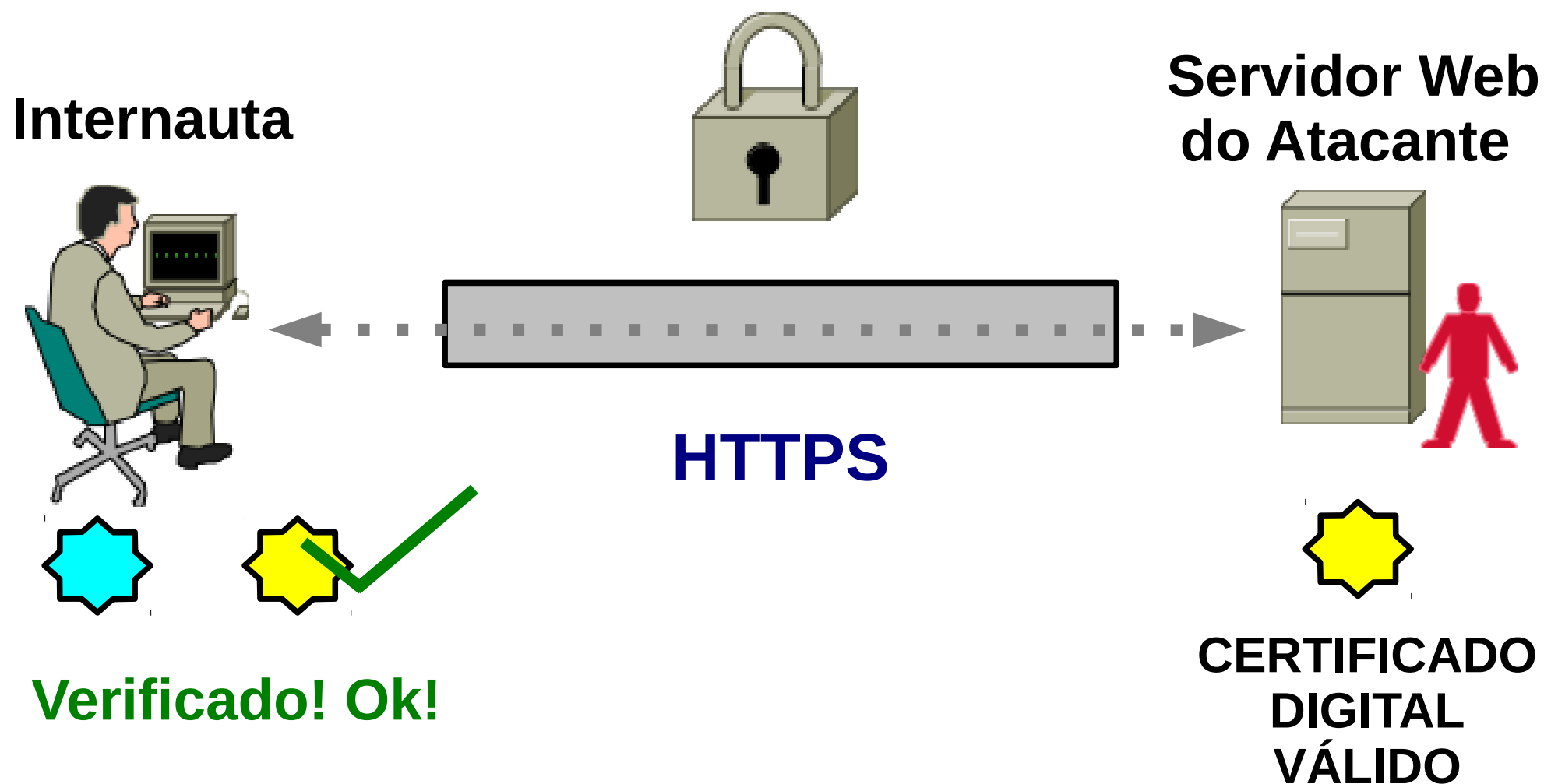


**Servidor Web
do Atacante**

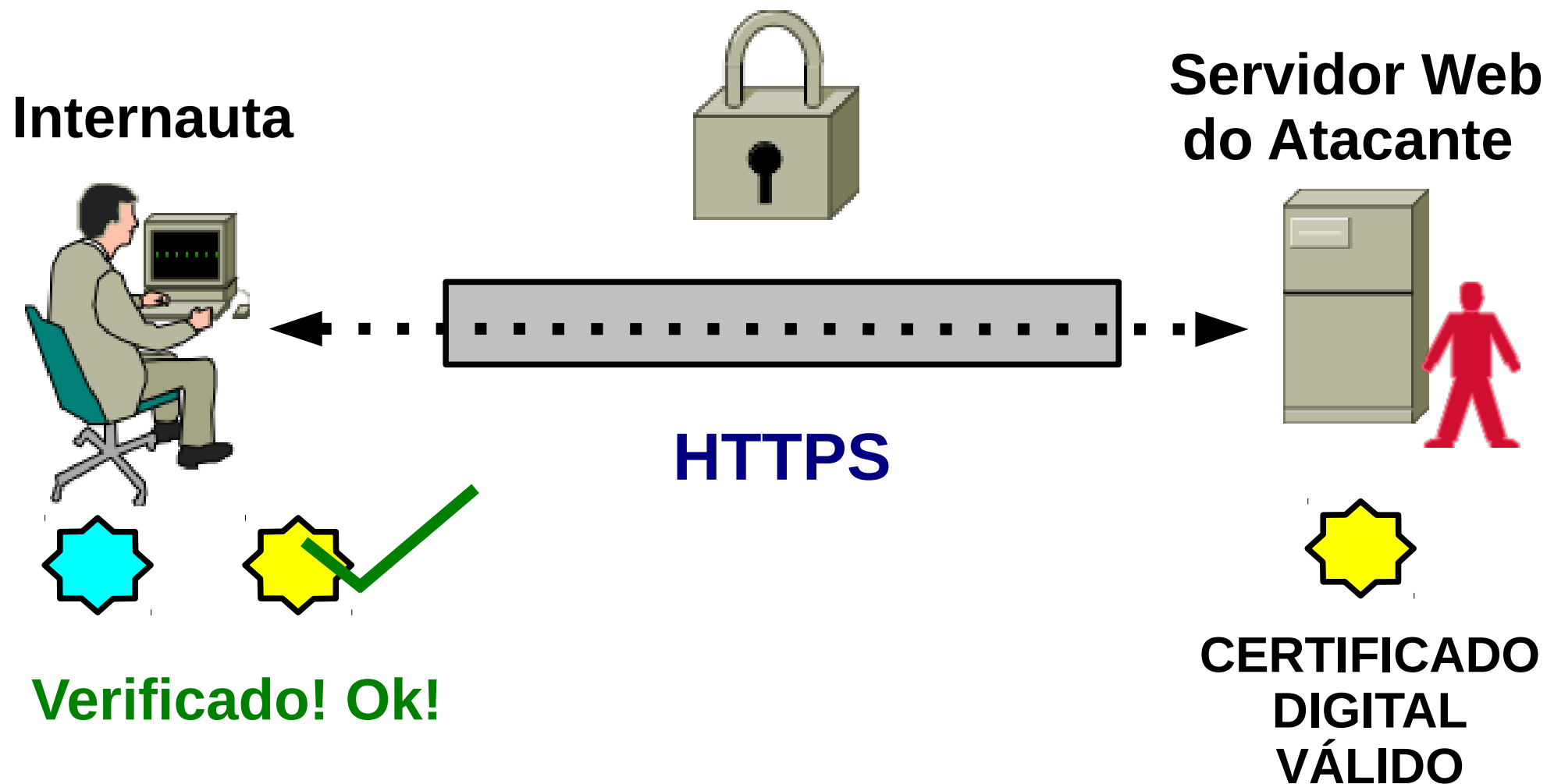


**CERTIFICADO
DIGITAL
VÁLIDO**

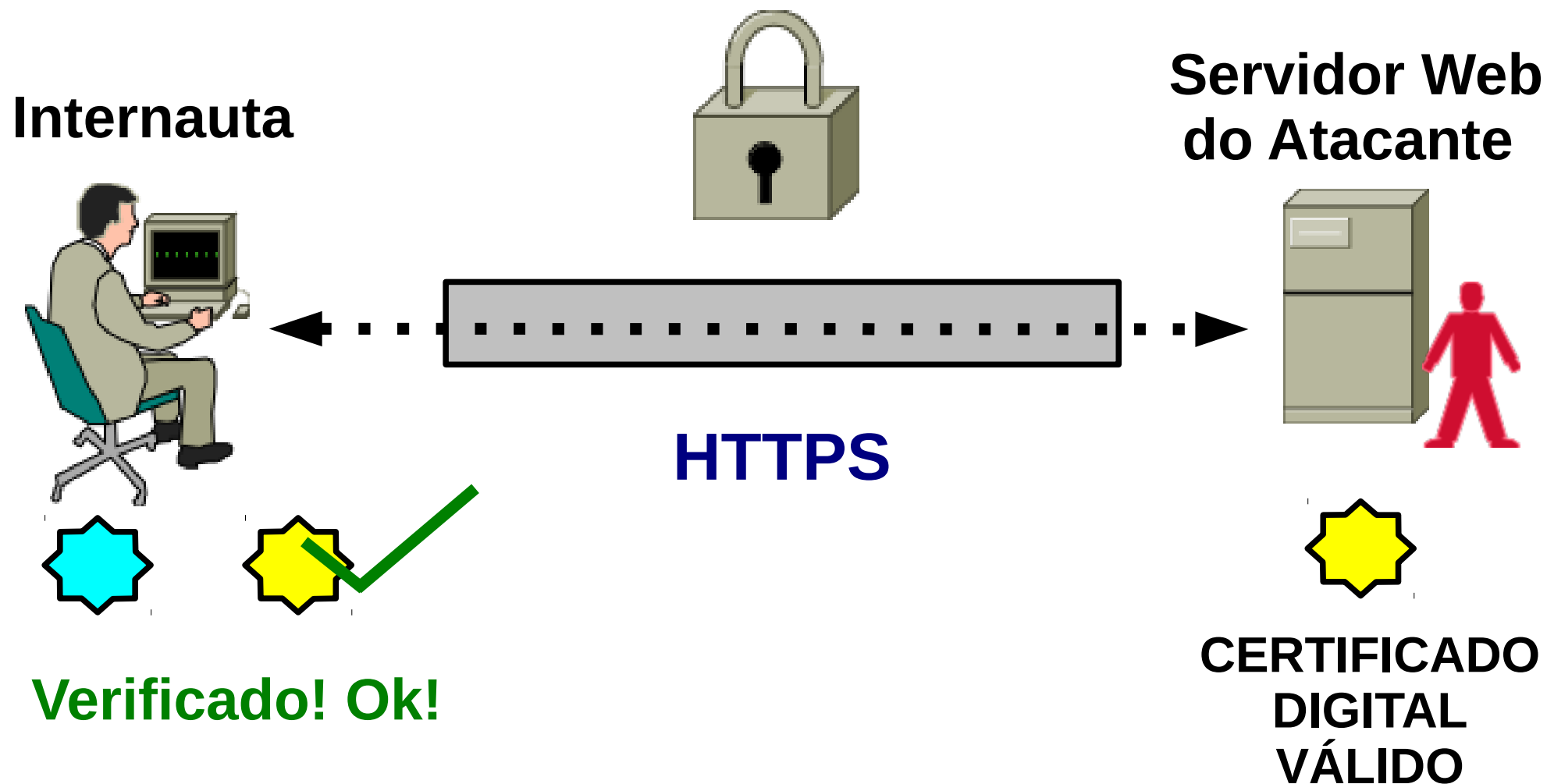
3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



3 – Confiar Autoridades Certificadoras?



Incidente de Segurança

- DigiNotar
- Holanda



Poderia ser utilizado para validar
certificações falsas.
Setembro/2011

Solução

- Certificados Atualizados
- Conferir Acesso Seguro



Considerações Finais

Confiança:

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

Causa:

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

Edward Snowden - NSA

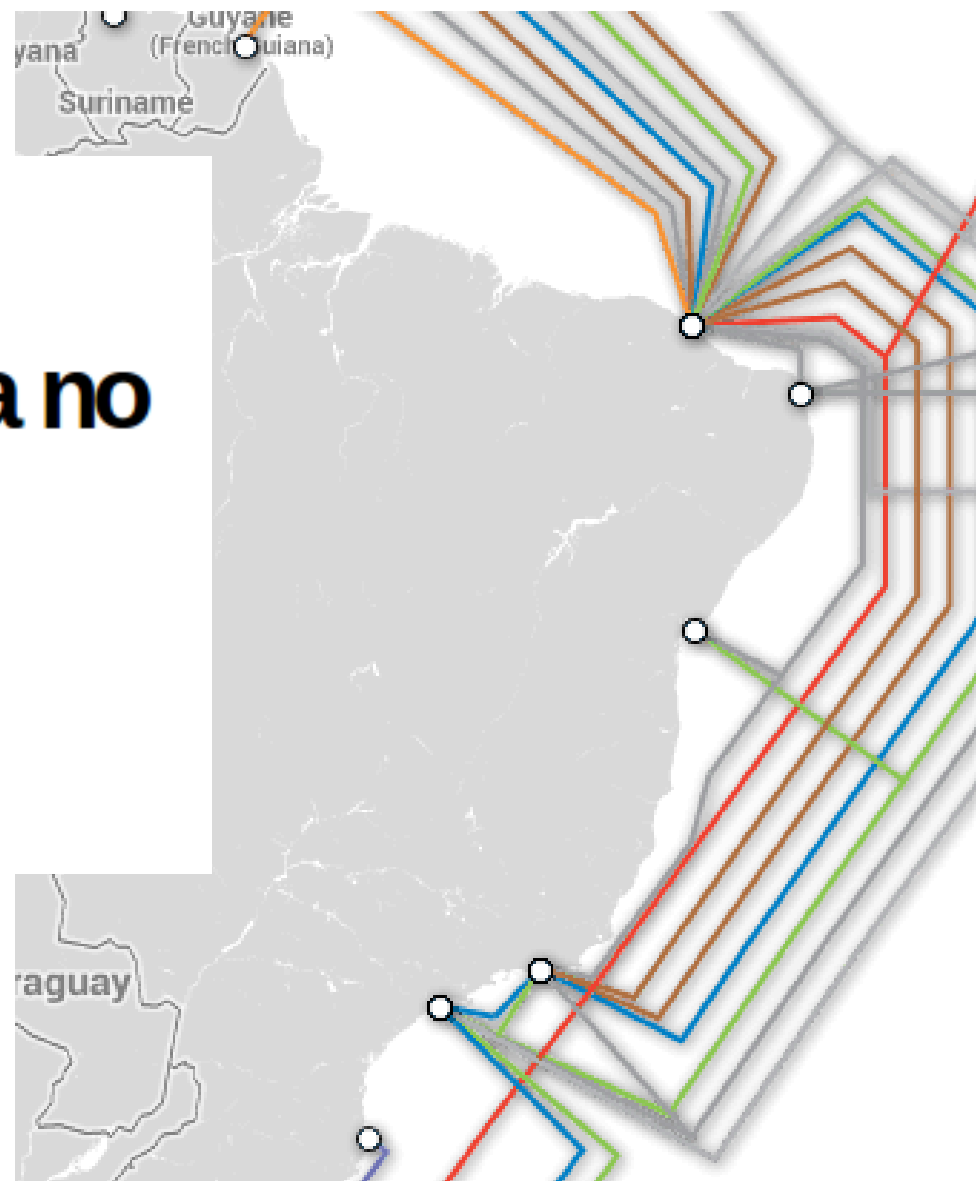


Grande interesse da espionagem americana no Brasil está nos cabos submarinos 🗨️ 14



Luiz Felipe de Alencastro

29/07/2013 | 11h29



Grato! :)

Hermano Pereira

→ hermanopereira@utfpr.edu.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 (Malawi)

<http://www.humanipo.com/news/4027/Malawi-Google-site-hacked-by-Bangladeshi-hacker>

DNS Poison (Kenya)

<http://www.cio.co.ke/news/main-stories/google,-microsoft,-linkedin-hacked-in-kenyan-dns-hijack>

DNS Poison (Guia Ilustrado)

<http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

Referências (continuação)

DNS China

http://www.cio.com/article/588165/China_s_Great_Firewall_Spreads_Overseas

<http://www.pcworld.com/article/192658/article.html>

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/>

Protocolo SSL (História)

<http://publib.boulder.ibm.com/infocenter/iseres/v5r3/index.jsp?topic=/rzain/rzainhistory.htm>

Diginotar (Certificado Comprometido)

<http://httpsonline.blogspot.com.br/2011/09/empresa-que-emite-certificados-digitais.html>

<https://www.cert.be/pro/docs/diginotar-hack>

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>