Monitoramento e Gerenciamento de Redes

- Segurança da Informação -

Mauro Cesar Bernardes

São Paulo, 2023

2º Semestre - 2023

8 AGOSTO

02	Início das aulas.

9 SETEMBRO

07	Independência do Brasil (dia não letivo).
08	Dia não letivo (emenda de feriado).

10 OUTUBRO

12	Nossa Senhora Aparecida (dia não letivo).
13	Dia não letivo (emenda de feriado).
28	NEXT.

11 NOVEMBRO

02	Finados (dia não letivo).
03	Dia não letivo (emenda de feriado).
13	Kick-off da Global Solutions.
13 a 24	Período de aplicação das Avaliações Semestrais Regulares e de DP - Global Solutions
15	Proclamação da república (dia não letivo).
20	Consciência Negra (dia não letivo).
13 a 24	Período de solicitação de todas as Avaliações Substitutivas.
27 a 01/12	Período de vistas das Avaliações e aplicação das Avaliações Substitutivas Regulares e DP.

12 DEZEMBRO

04 a 08	Período de Aplicação dos Exame Finais.
11 a 13	Período de vistas de Exame.
14	Data máxima para divulgação dos resultados dos Exames Finais.

Esta semana

Agosto 2023

Nº	Se	Te	Qu	Qu	Se	Sá	Do
31		1	2	3	4	5	6
32	7	8	9	10	11	12	13
33	14	15	16	17	18	19	20
34	21	22	23	24	25	26	27
35	28	29	30	31			

Setembro 2023

Nº	Se	Te	Qu	Qu	Se	Sá	Do
35					1	2	3
36	4	5	6	7	8	9	10
37	11	12	13	14	15	16	17
38	18	19	20	21	22	23	24
39	25	26	27	28	29	30	

Outubro 2023

Nº	Se	Te	Qu	Qu	Se	Sá	Do
39							1
40	2	3	4	5	6	7	8
41	9	10	11	12	13	14	15
42	16	17	18	19	20	21	22
43	23	24	25	26	27	28	29
44	30	31					

Novembro 2023

Nº	Se	Te	Qu	Qu	Se	Sá	Do
44			1	2	3	4	5
45	6	7	8	9	10	11	12
46	13	14	15	16	17	18	19
47	20	21	22	23	24	25	26
48	27	28	29	30			

Dezembro 2023

Nº	Se	Te	Qu	Qu	Se	Sá	Do
48					1	2	3
49	4	5	6	7	8	9	10
50	11	12	13	14	15	16	17
51	18	19	20	21	22	23	24
52	25	26	27	28	29	30	31

1º checkpoint

2º checkpoint

3º checkpoint

Plano de Aula

- **Objetivo**
  - Compreender os conceitos relacionados a VPN (*Virtual Private Network*)
  - Compreender o funcionamento de uma VPN
  - Analisar a direção da segurança da Internet
- **Conteúdo**
  - Configuração de VPN, Criptografia e certificação digital

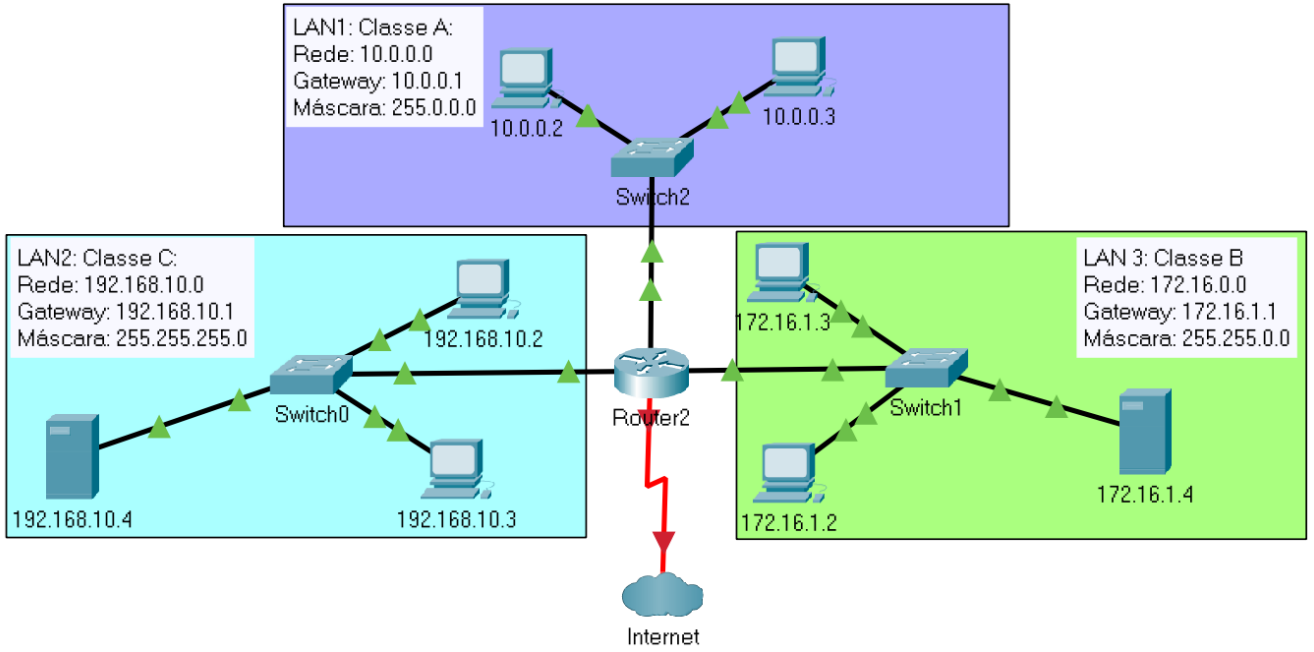
    ,
- **Metodologia**
  - Aula expositiva sobre os conceitos e desenvolvimento de atividade prática com configuração em simulador (*Packet Tracer*)

Breve Revisão do 1° Semestre

Configurar regras ACLs estendida para:

1. Bloquear acesso do ip `10.0.0.2` ao serviço `http` disponível no servidor `192.168.10.4`
2. Bloquear acesso do ip `10.0.0.3` ao serviço `ssh` disponível no servidor `172.16.1.4`
3. Permitir acesso do ip `10.0.0.3` apenas ao serviço `http` disponível no servidor `192.168.10.4`.
4. Implementar uma situação proposta por você (você deve propor e configurar 1 (uma) regra diferente das anteriores).

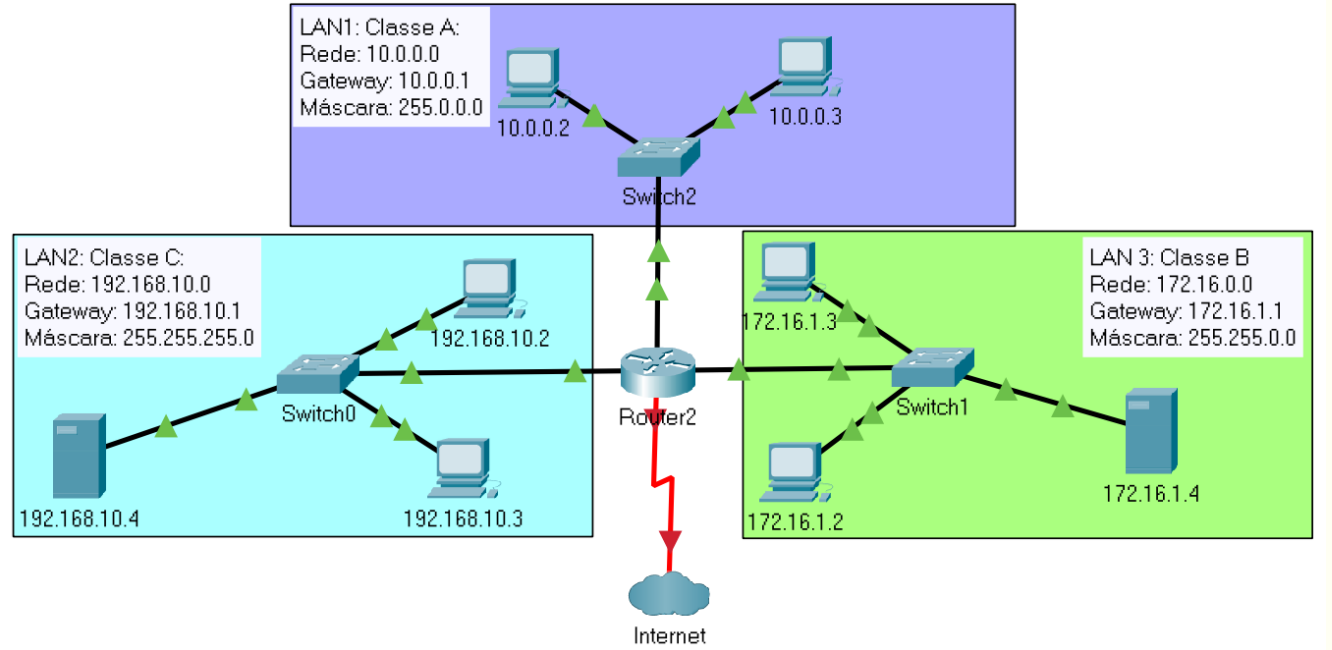
Tudo o que não estiver explícito nas regras acima deve estar **liberado**



Utilize o Arquivo:

2oSem Aula 03 2023 Segurança.pkt

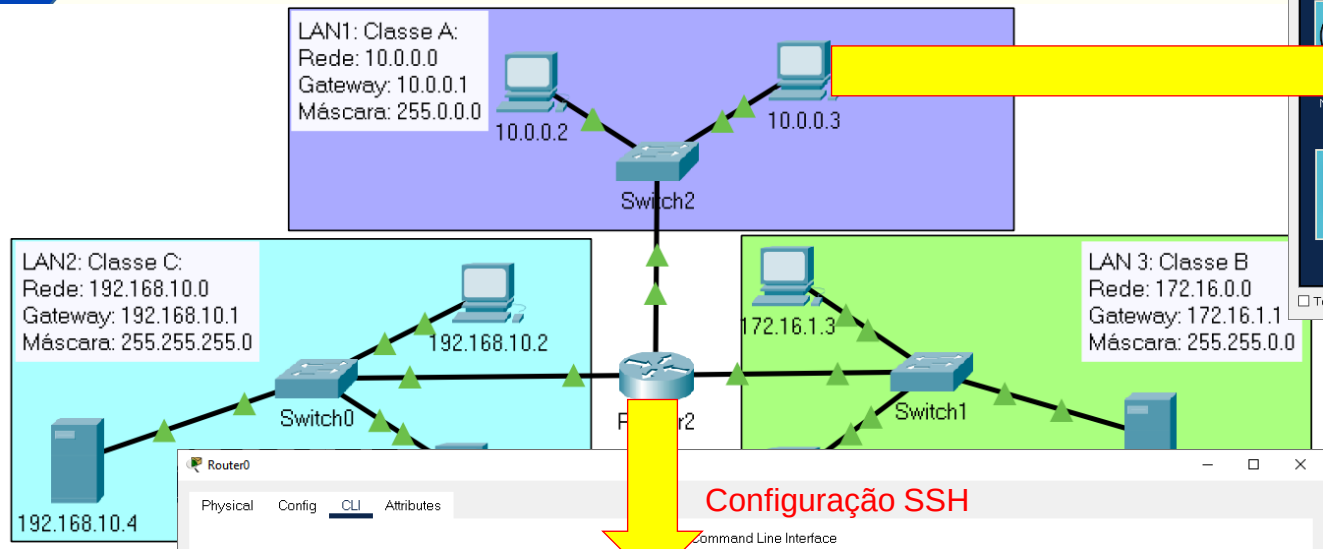
Configuração de acesso SSH ao router

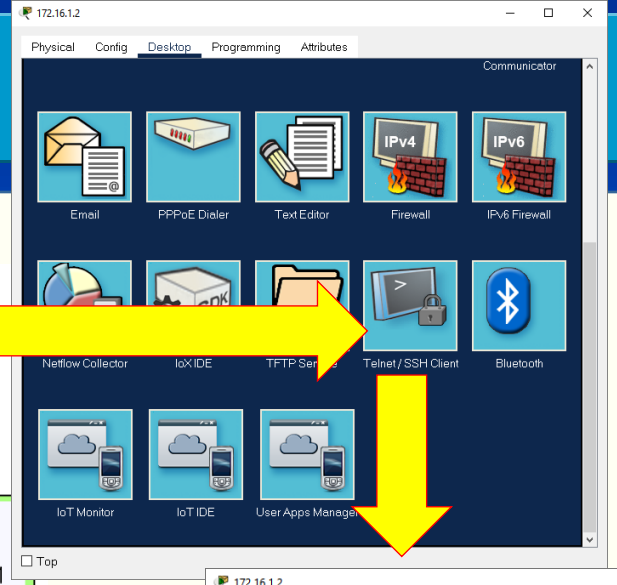


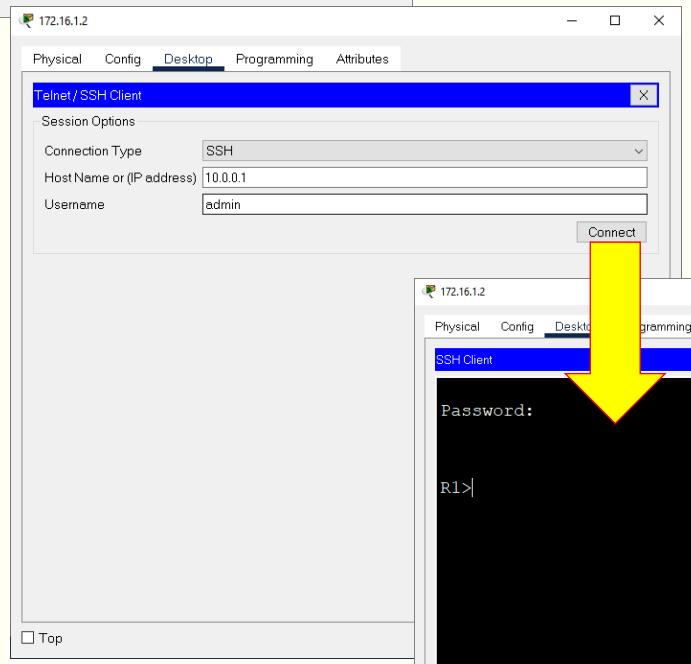

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#ip domain-name aula06
R1(config)#crypto key generate rsa

R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#username admin secret fiap
R1(config)#
```

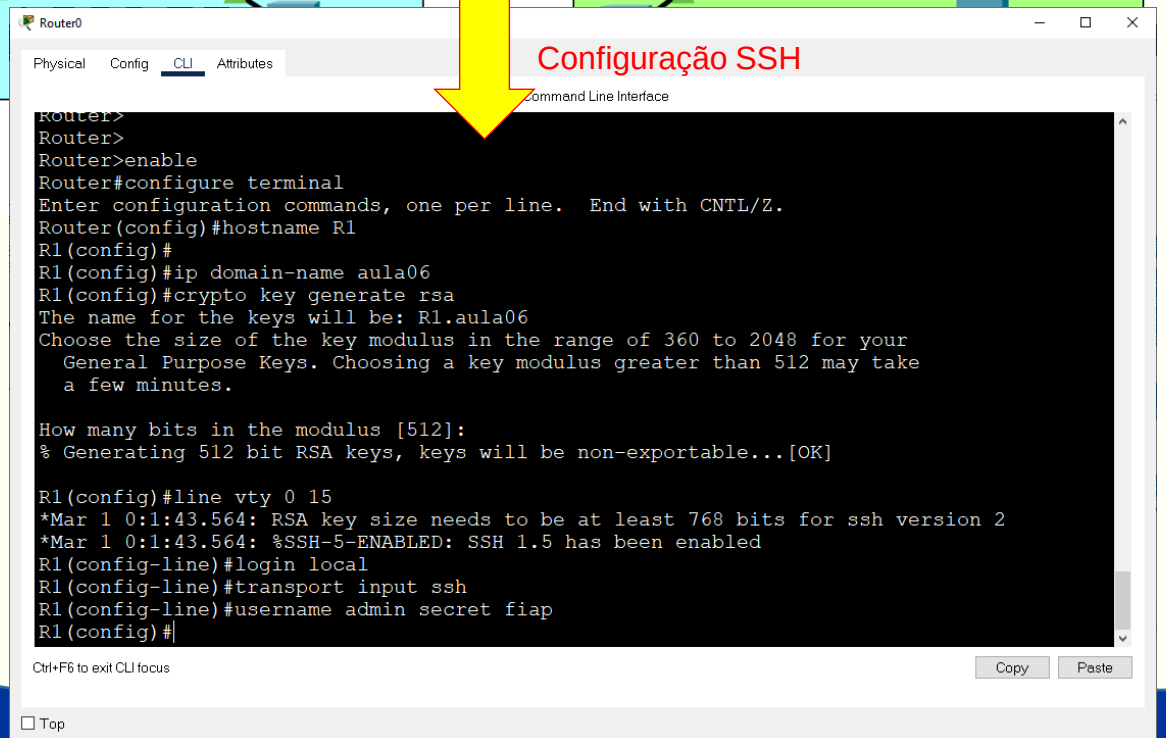
Configurar SSH no roteador

Arquivo: 2oSem Aula 03 2023 Segurança.pkt

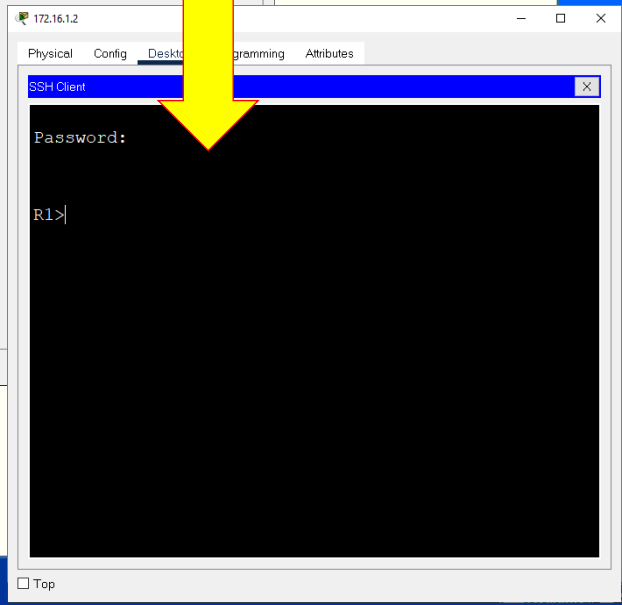








Configuração SSH



Estrutura da Apresentação

- Política de Segurança
- Criptografia
  - Criptografia Assimétrica
  - Criptografia Simétrica
  - Assinatura Digital
  - Infraestrutura de Chaves públicas
  - Principais algoritmos de criptografia
- Firewalls
  - *Network Firewalls*
  - *Personal Firewalls*
- DMZ
- IDS
  - IDS Baseado em Host
  - IDS Baseado em Redes
- Anti-vírus
- Assinatura digital
- VPNs
- Honey Pots

Políticas de Segurança

- “A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida.”

  [NBR ISO/IEC 27.000]

- “Uma política de segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.”

  [SOARES, 1995]

Política de Segurança

NBR ISO/IEC 27.000
Tecnologia da Informação – Código de prática para a gestão da segurança da informação.

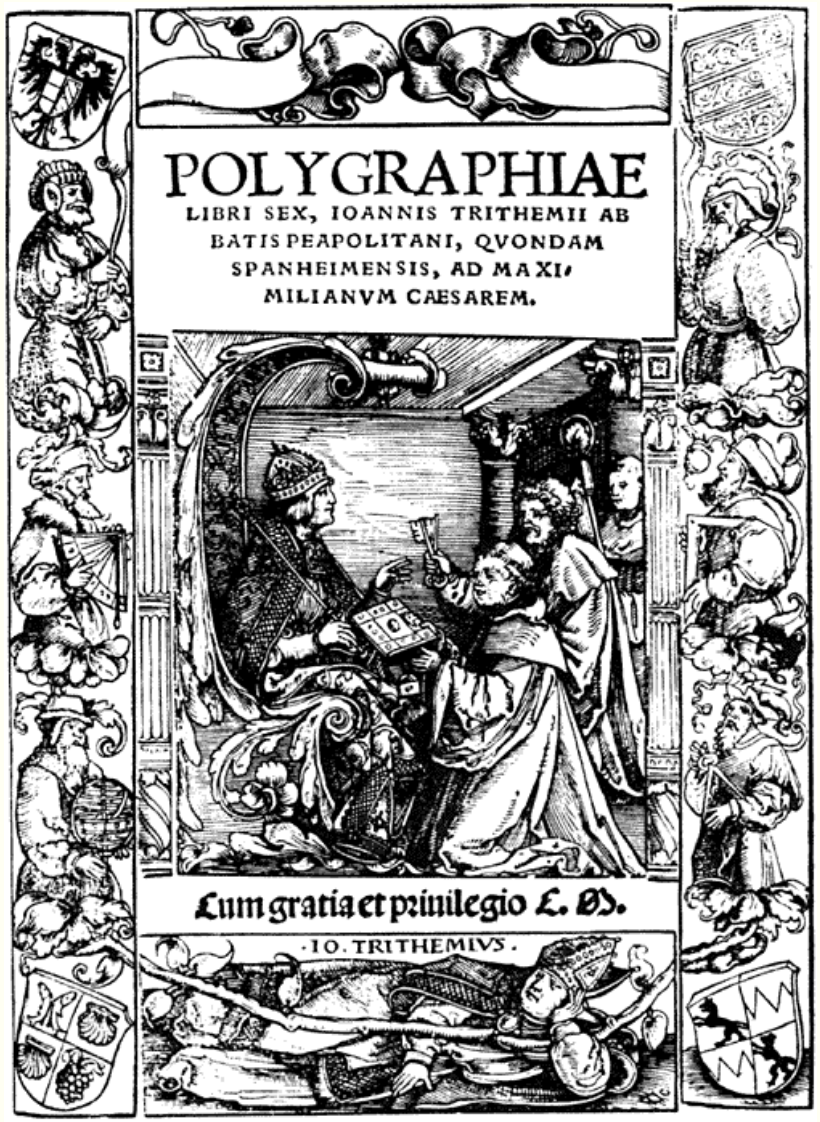
1- Segurança Organizacional;
2 - Classificação e controle dos ativos de informação;
3 - Segurança em pessoas;
4 - Segurança física e do ambiente;
5 - Gerenciamento das operações e comunicações;
6 - Controle de acesso;
7 - Desenvolvimento e manutenção de sistemas;
8 - Gestão da continuidade do negócio;
9 – Conformidade com requisitos legais.

Política de Segurança

Propósitos da Política de Segurança

- Descreve o que está sendo protegido.
- Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo.
- Permite estabelecer um acordo explícito com as várias partes da empresa em relação ao valor da segurança.
- Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário.
- Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”.

Criptografia



Criptografia

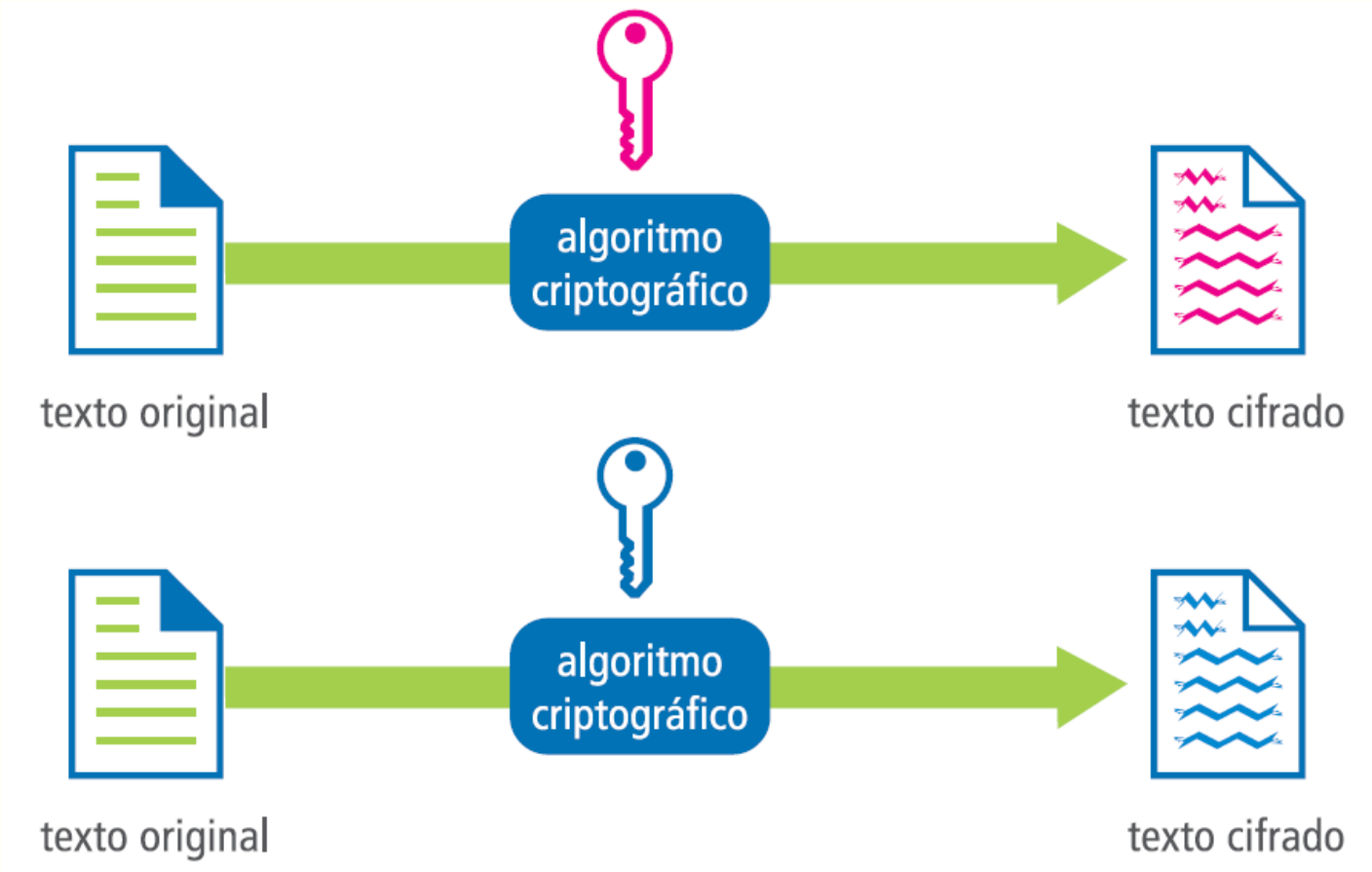
- Criptografia = ciência **de codificar informações**;
- **Existe há centenas de anos** (indícios desde os Egípcios antigos);
- Muito utilizada também no âmbito militar e diplomático;
- Nos últimos anos houve **um grande avanço na criptografia computacional**;
- É usada para garantir:
  - **confidencialidade** (somente usuário autorizados);
  - **integridade** da informação (não alteração da informação);
  - **autenticação** dos participantes (confirmação de identidade)
- Para cifrar ou decifrar dados é necessário uma **chave** ou **senha**
  - Chave – algoritmo matemático de difícil determinação
  - Senha – secreta e de difícil determinação

Criptografia

- **Simétrica** (mesma chave/senha para cifrar e decifrar)
- **Assimétrica** (chaves/senhas diferentes para cifrar e decifrar)

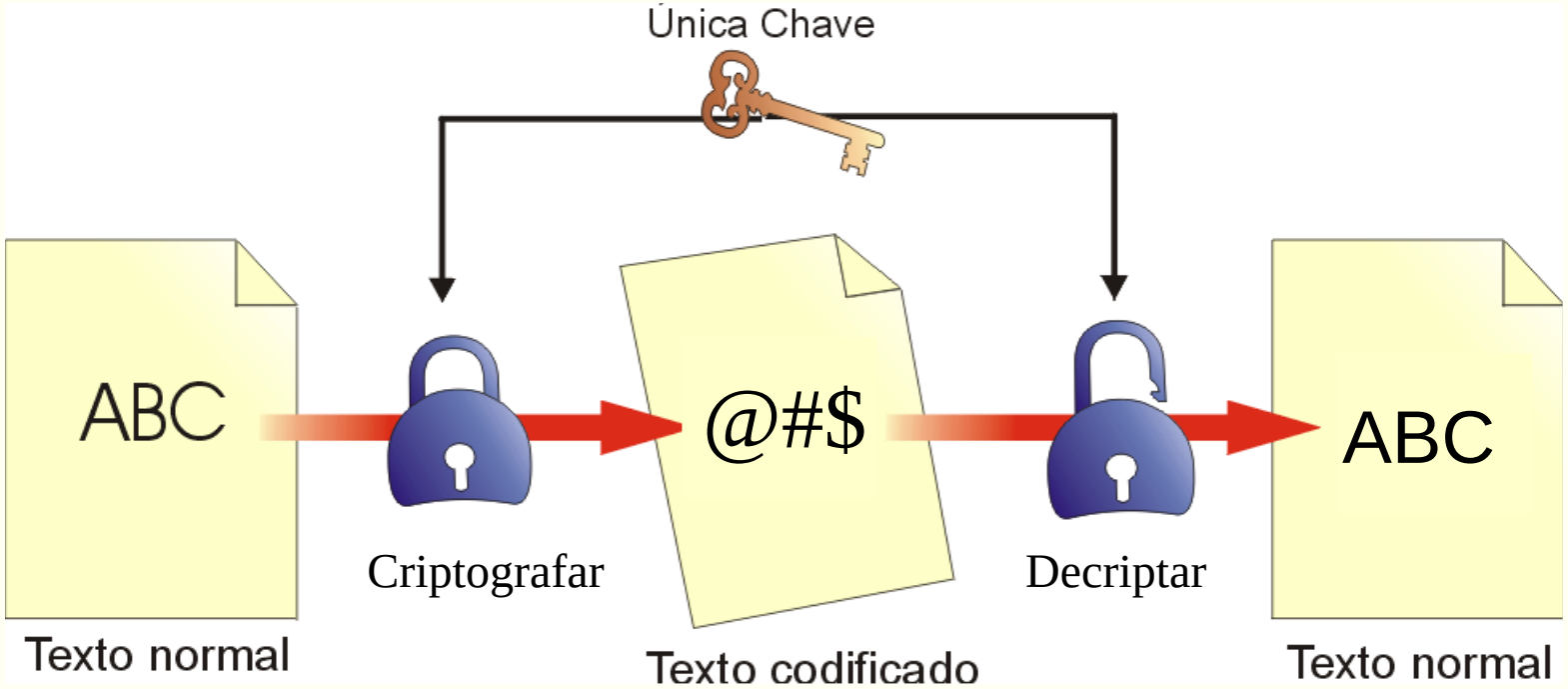
- **Criptografia simétrica**
  - como passar a senha/chave para o destinatário de forma segura ?
  - eficiente em processos temporários de conexão
- **Criptografia assimétrica**
  - chave privada (somente o proprietário a conhece)
  - chave pública (todos podem conhecê-la)
  - teve maior aceitação devido a sua forma de utilização
  - quando mais divulgarmos a chave pública melhor

Criptografia Simétrica



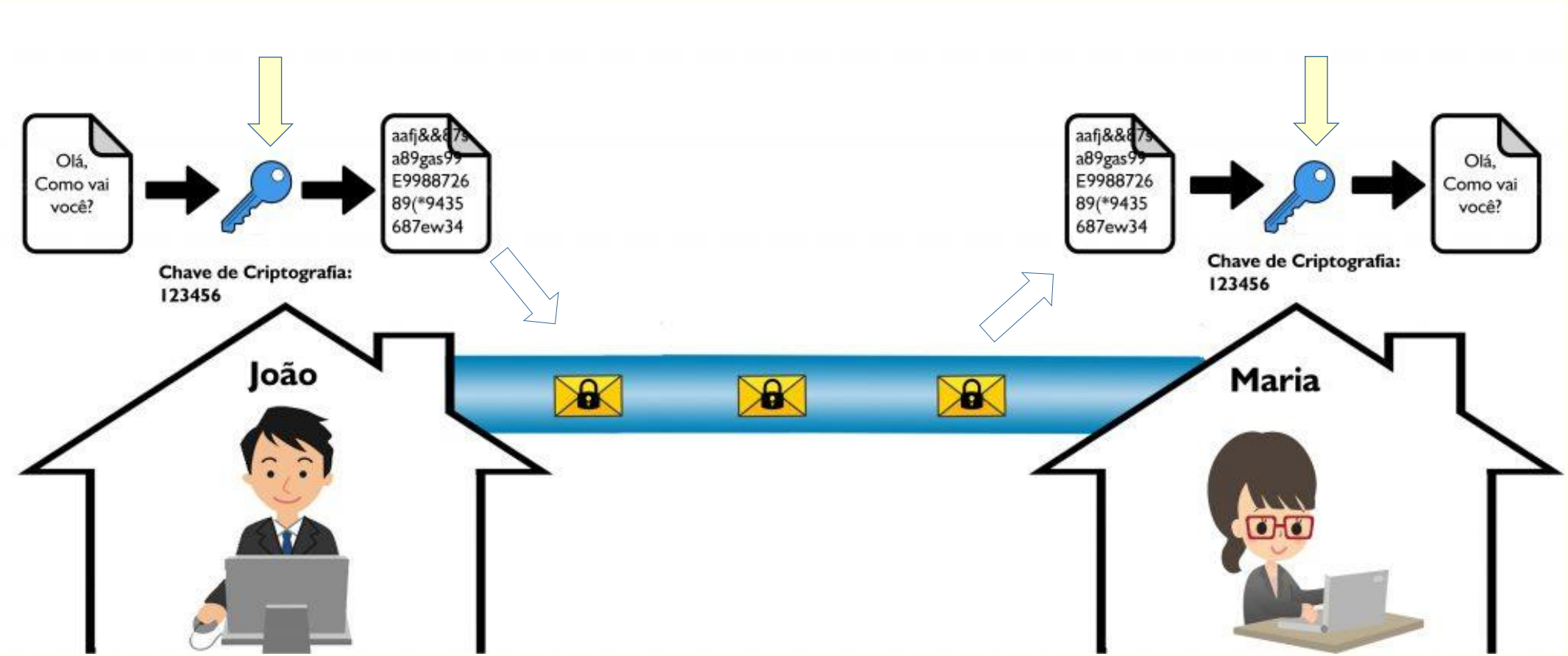
Criptografia Simétrica

Criptografia com chave simétrica;



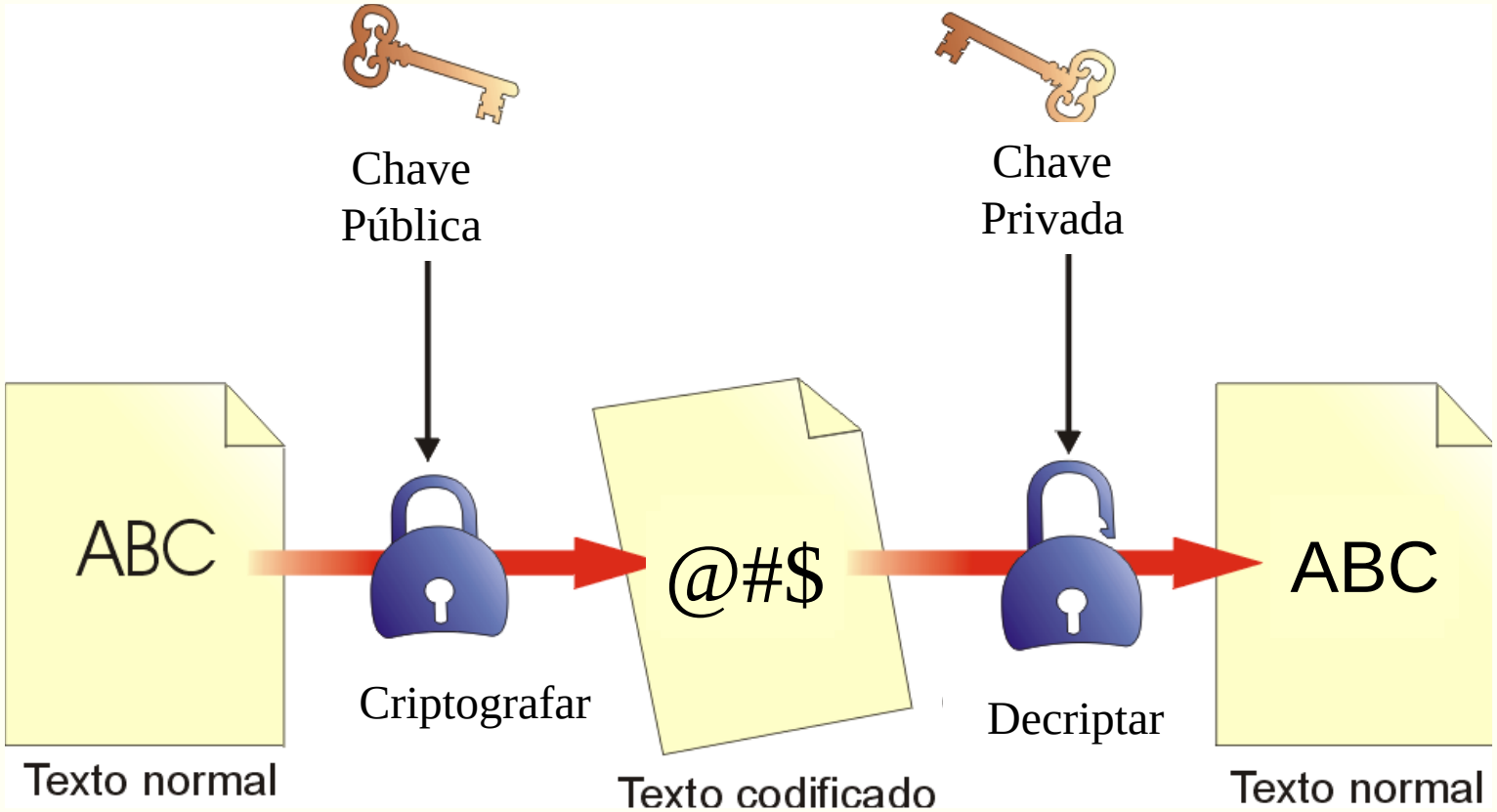
Criptografia Simétrica

Em **criptografia simétrica**, **a mesma chave** utilizada para criptografar é utilizada para decriptar

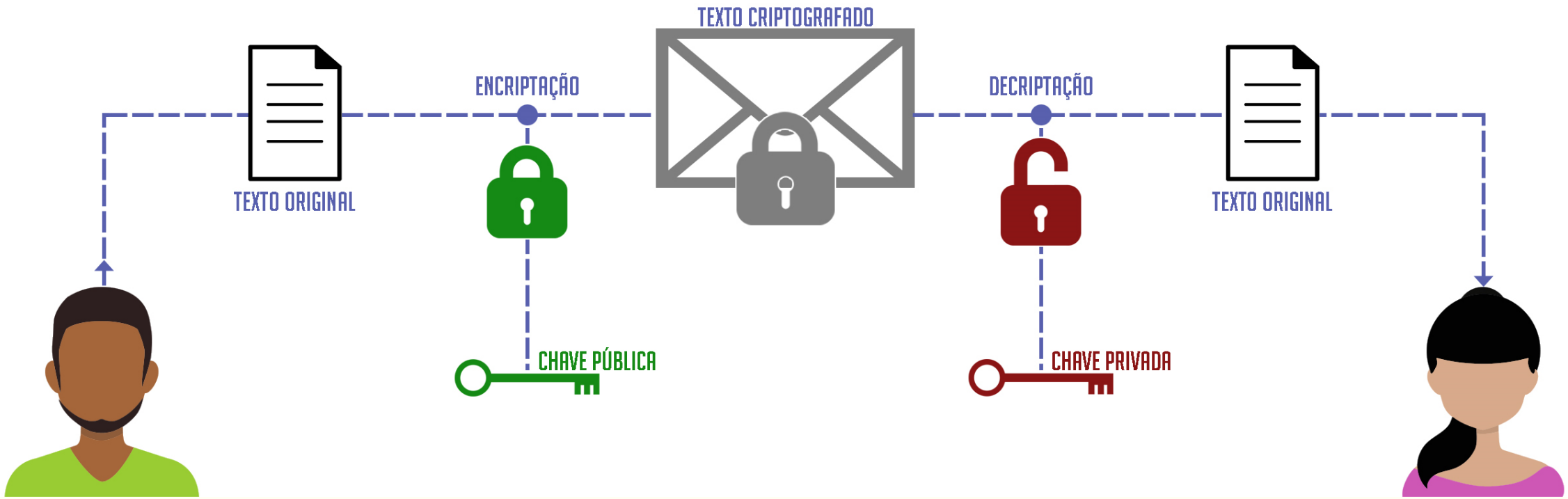


Criptografia Assimétrica

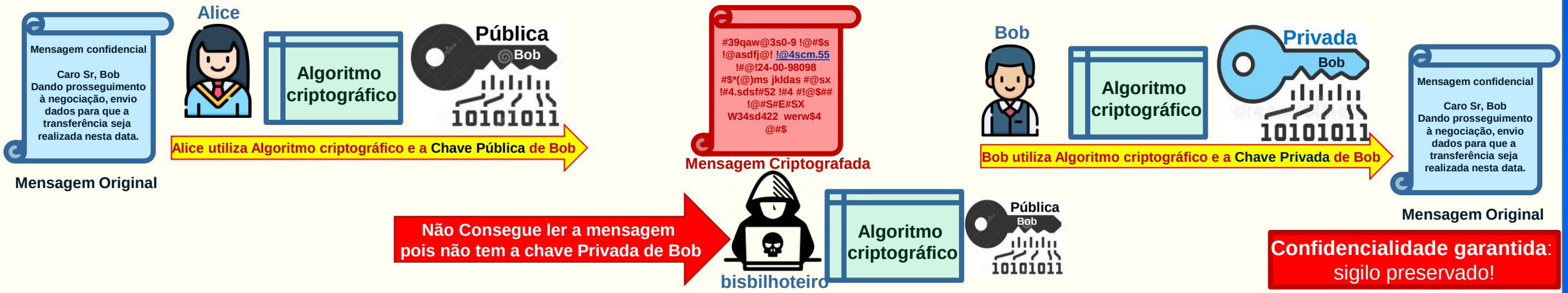
Em **criptografia assimétrica**, **chaves diferentes** são utilizadas para criptografar e para decriptar

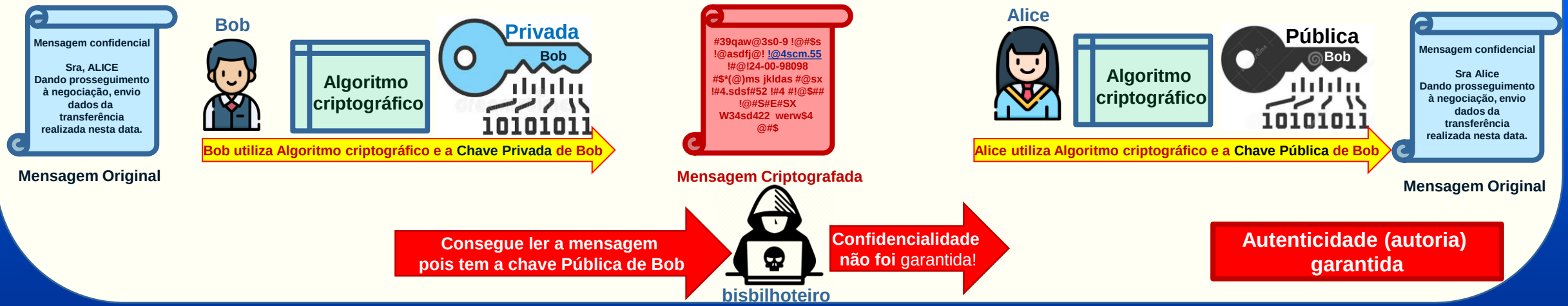


Criptografia Assimétrica

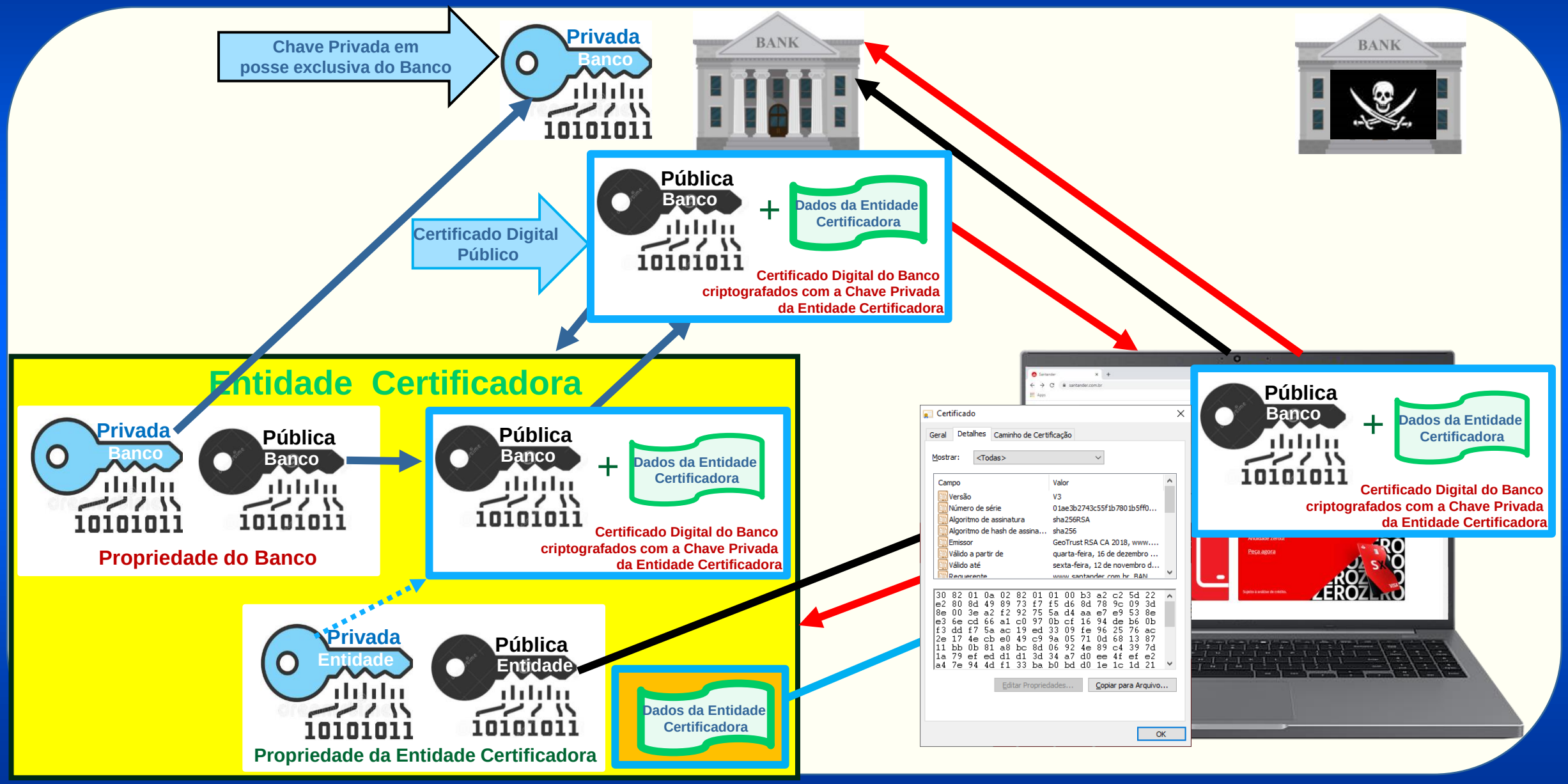


Criptografia Assimétrica

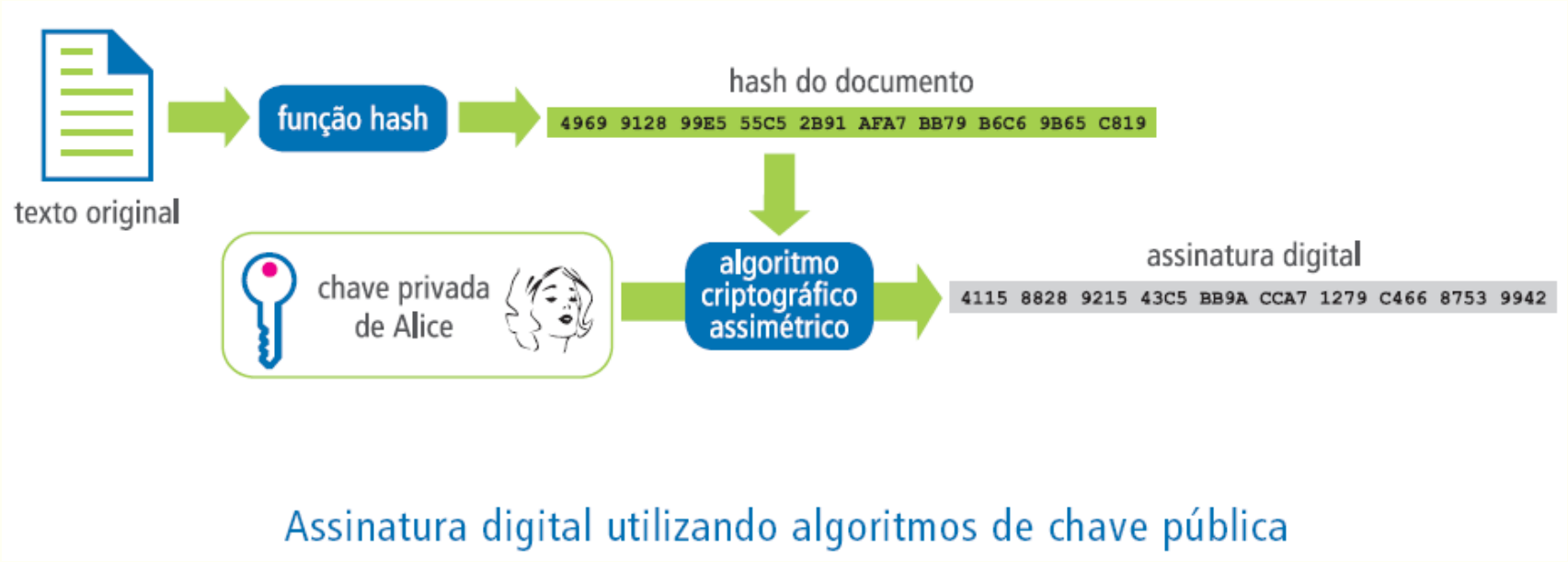




Certificação Digital

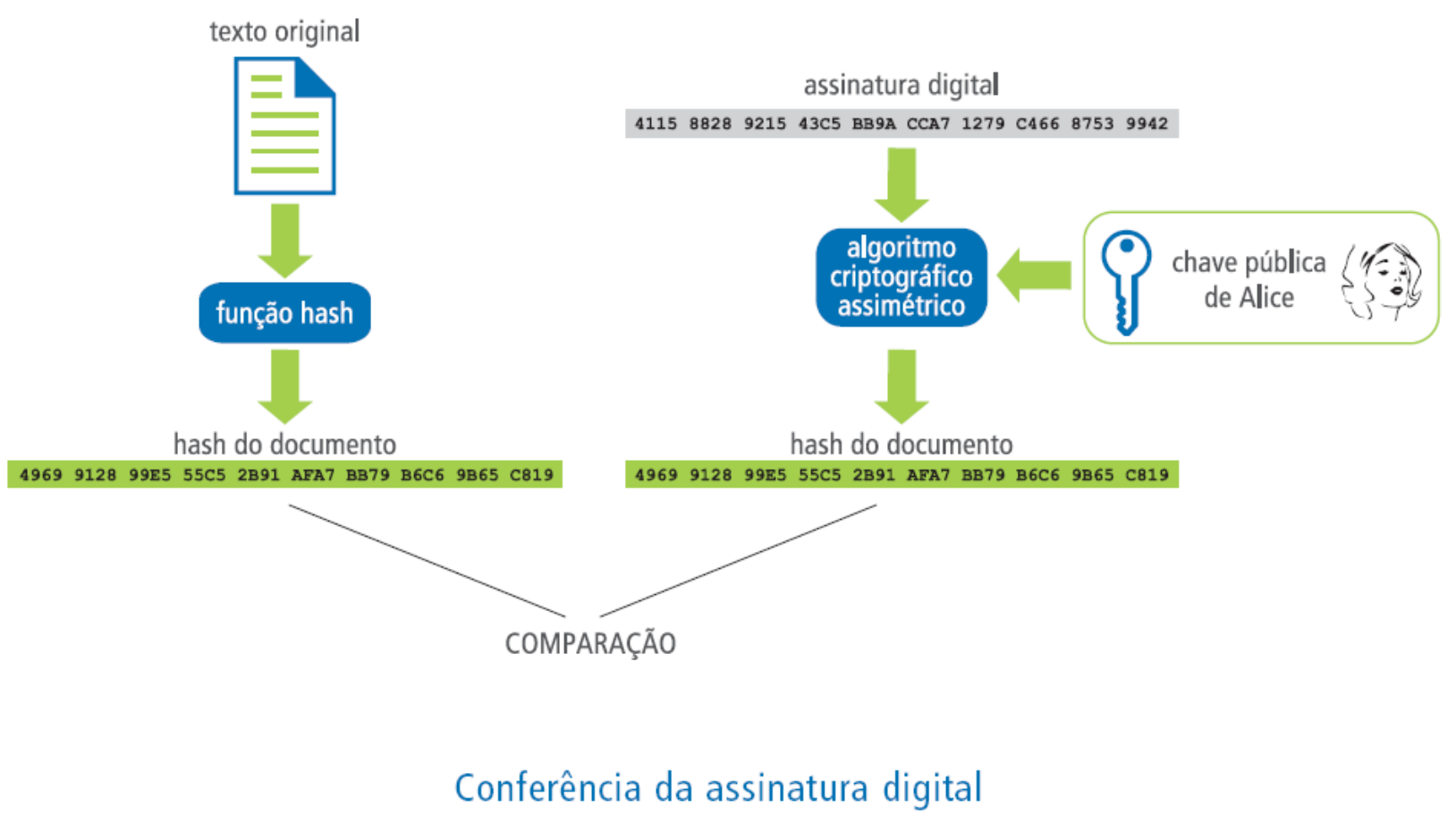


Assinatura Digital



Assinatura digital utilizando algoritmos de chave pública

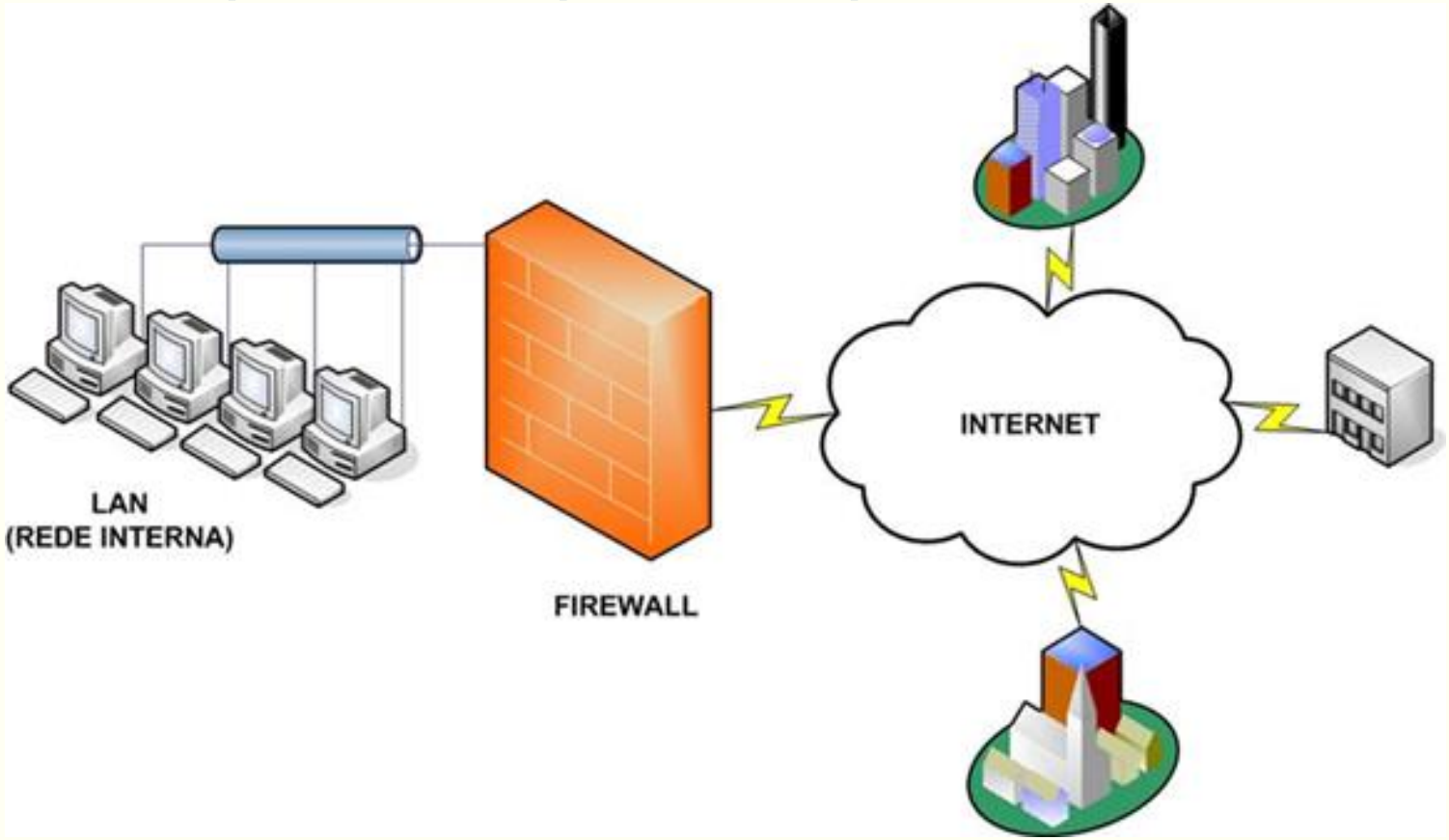
Assinatura Digital



Conferência da assinatura digital

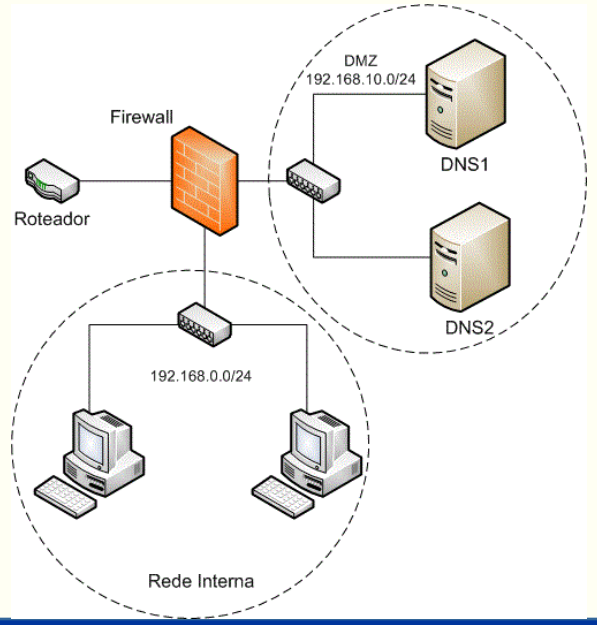
Firewall

- **Abordagens clássicas de configuração:**
  - **O que não é expressamente proibido é permitido;**
  - **O que não é expressamente permitido é proibido;**



DMZs

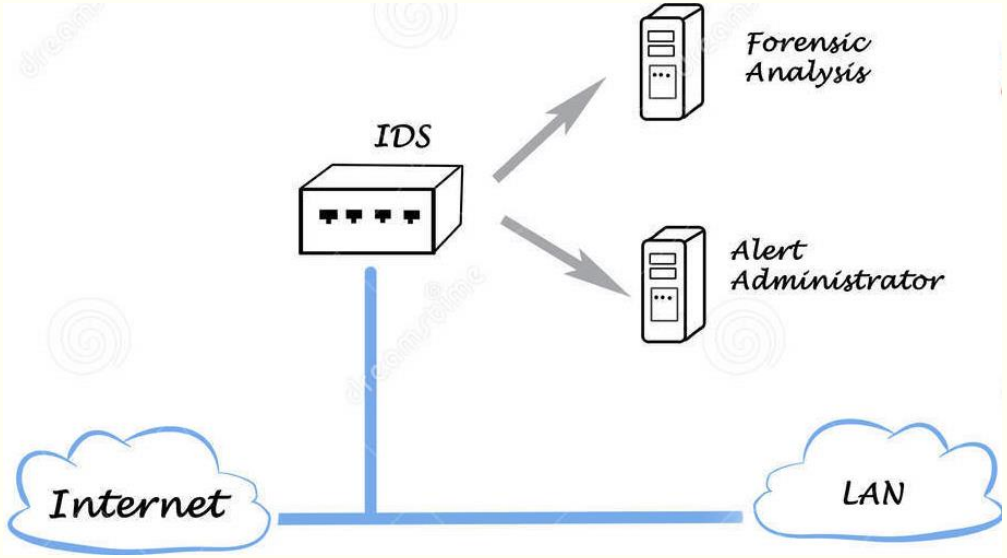
- DMZ (De-Militarized Zone) é o nome dado a uma topologia de rede situada entre uma rede protegida e uma externa considerada por muitos especialistas um ótimo esquema de segurança.
- O ambiente se caracteriza por: ambiente externo (internet), ambiente interno e uma subrede conhecida por abrigar máquinas que provém algum tipo de serviço para a internet.
- Essas máquinas são geralmente apelidadas de *Bastion Host*. O motivo de tal apelido é que elas estão expostas e serão alvo de possíveis atacantes.
- O intuito é prover maior segurança a essas máquinas.



Detecção de Intrusos

- **Habilidade de identificar uma tentativa de acesso à um sistema ou rede e que não esteja em acordo com a política de segurança existente na empresa.**

- **SDI= Sistema de detecção de Intrusão**
- **IDS= *Intrusion Detection System***



Sistemas de Detecção de Intrusão

Classificação:

Formas de Detecção

- Detecção de Uso Indevido;
- Detecção de Anomalias;
- Detecção Híbrida.

Tratamento dos Dados

⇨ *Host Based;*

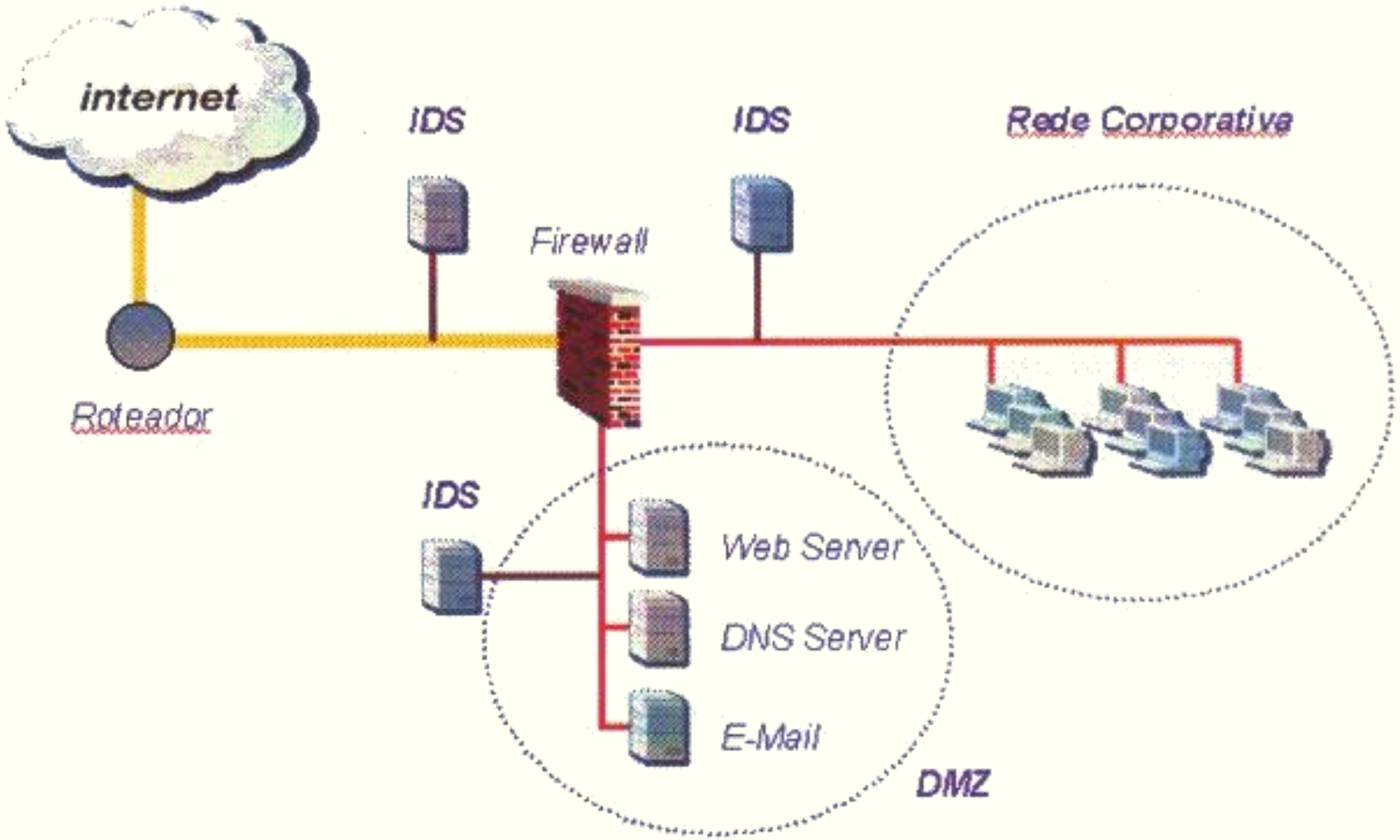
⇨ *Multihost Based;*

⇨ *Network Based.*

Sistemas de Detecção de Intrusão

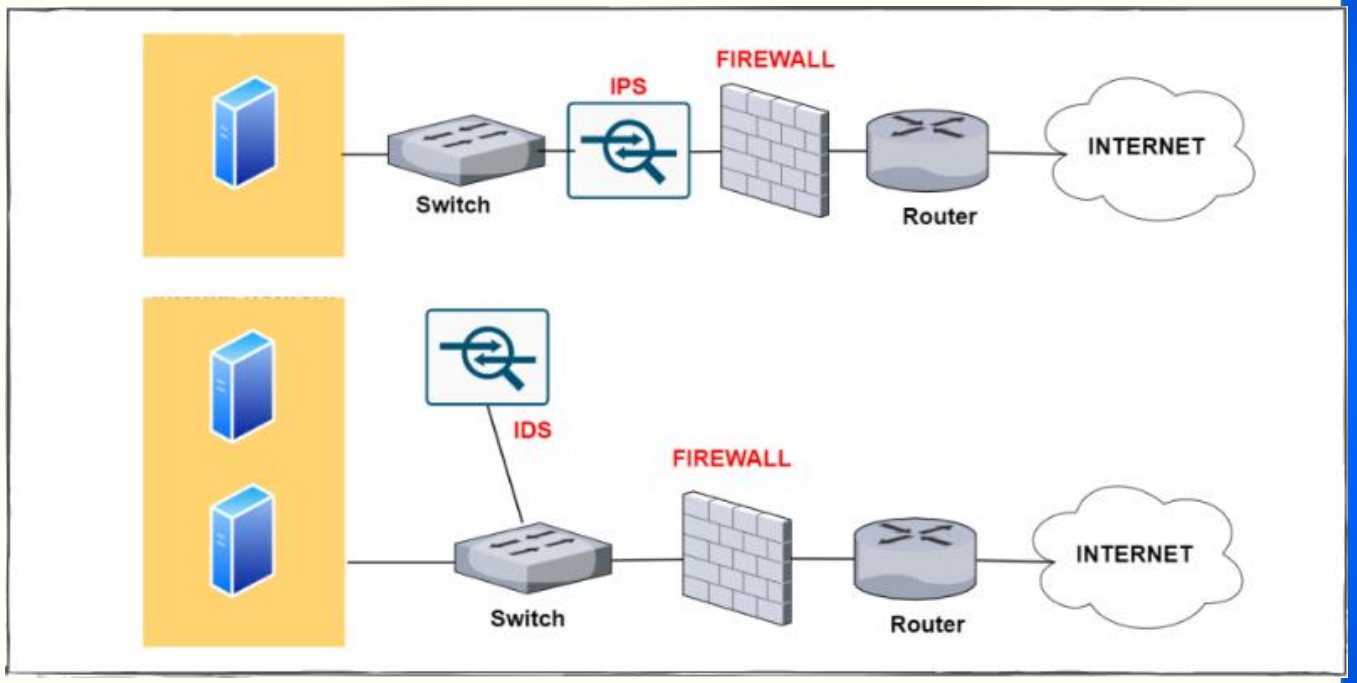
- **Reconhecem atividades que não estejam em acordo com as normas existentes e podem ser configuradas para tomar ações reativas automaticamente como:**
  - **Reconfigurar firewall;**
  - **Enviar alerta;**
  - **Gravar *Log* do ataque;**
  - **Terminar conexão, etc.**

Onde Implementar um SDI



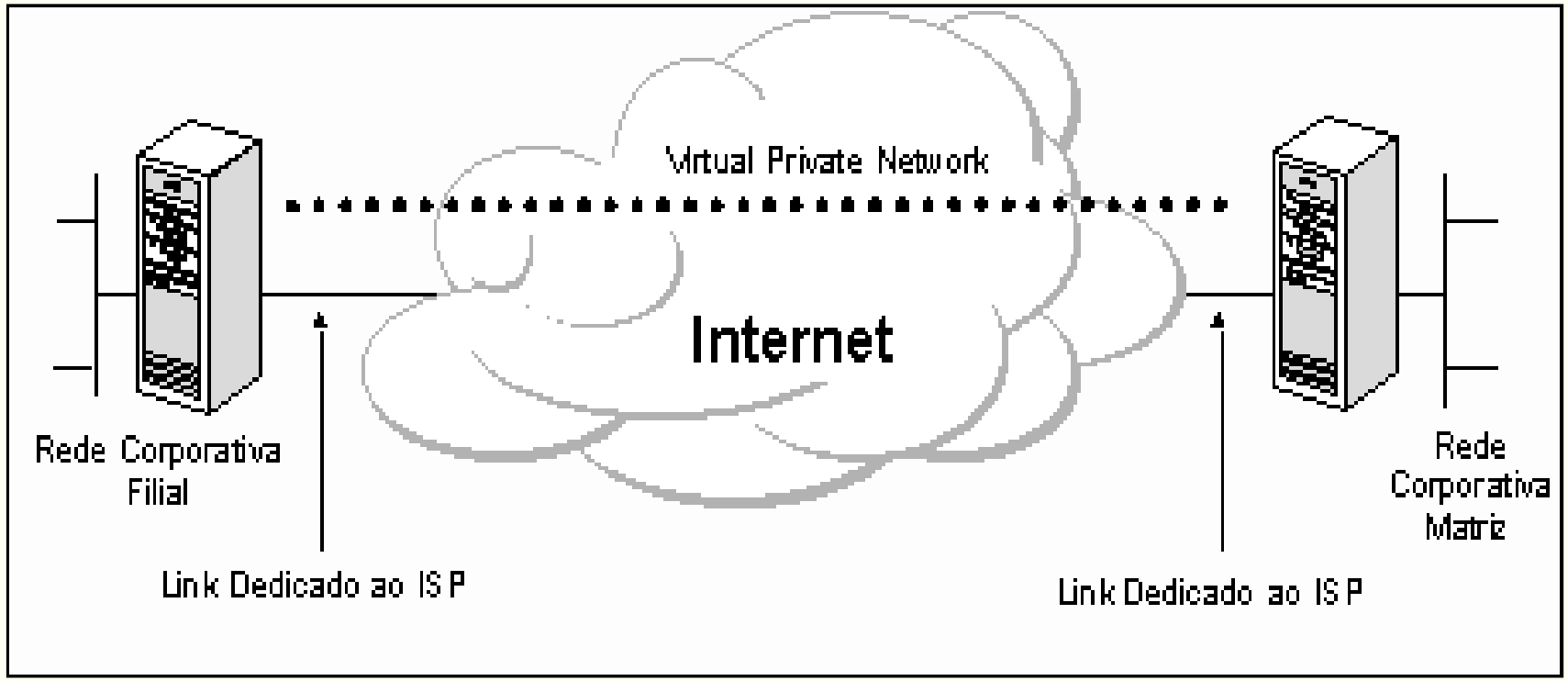
Intrusion Prevention System

- **Um Sistema de Prevenção de Intrusão (IPS) é uma tecnologia de segurança de rede e prevenção de ameaças que examina fluxos de tráfego de rede para detectar e prevenir vulnerabilidades.**
- **Em um cenário em que as atividades das empresas estão cada vez mais atreladas a computadores e dispositivos móveis, soluções que garantam a proteção de suas redes de computadores ganham cada vez mais importância.**
- **De um modo simples, podemos dizer que o dispositivo atua monitorando a rede de uma empresa, em busca de atividades suspeitas.**
- **Isso com a finalidade de interrompê-las e de notificar o time de TI a respeito do ocorrido.**

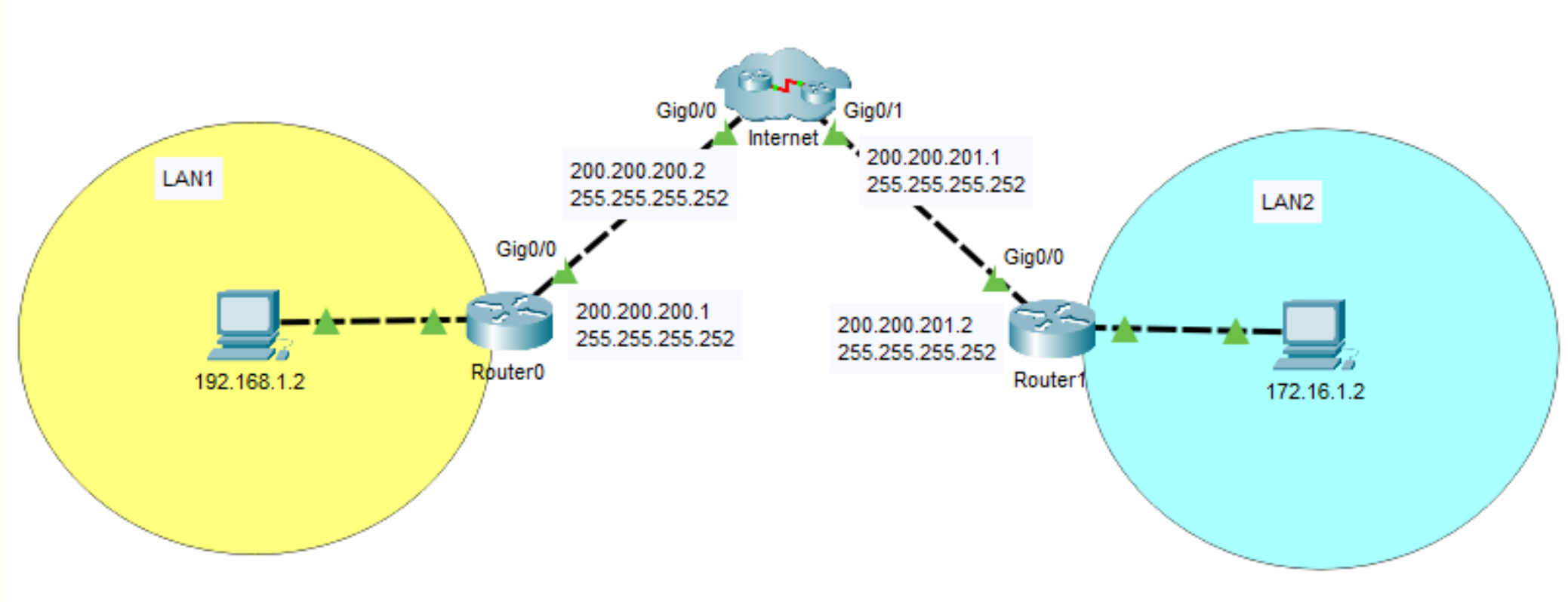


Rede privada virtual (VPN)

Interconexão de redes via Internet

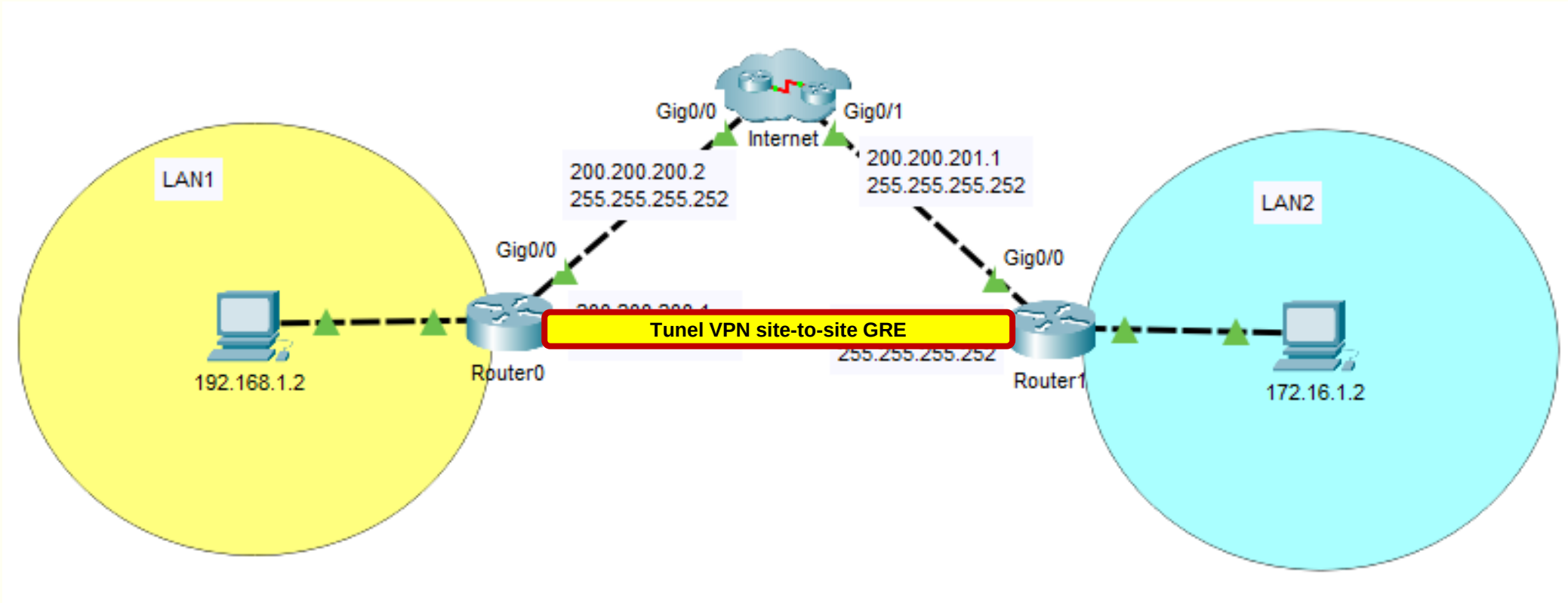


VPN tunnel GRE – *site-to-site*



Deseja-se Criar uma VPN (um "*túnel seguro*") entre o Router0 e o Router1, de forma que as informações que trafegarem pela Internet estejam protegidas.
Por túnel seguro entendemos o envio de pacotes criptografados!

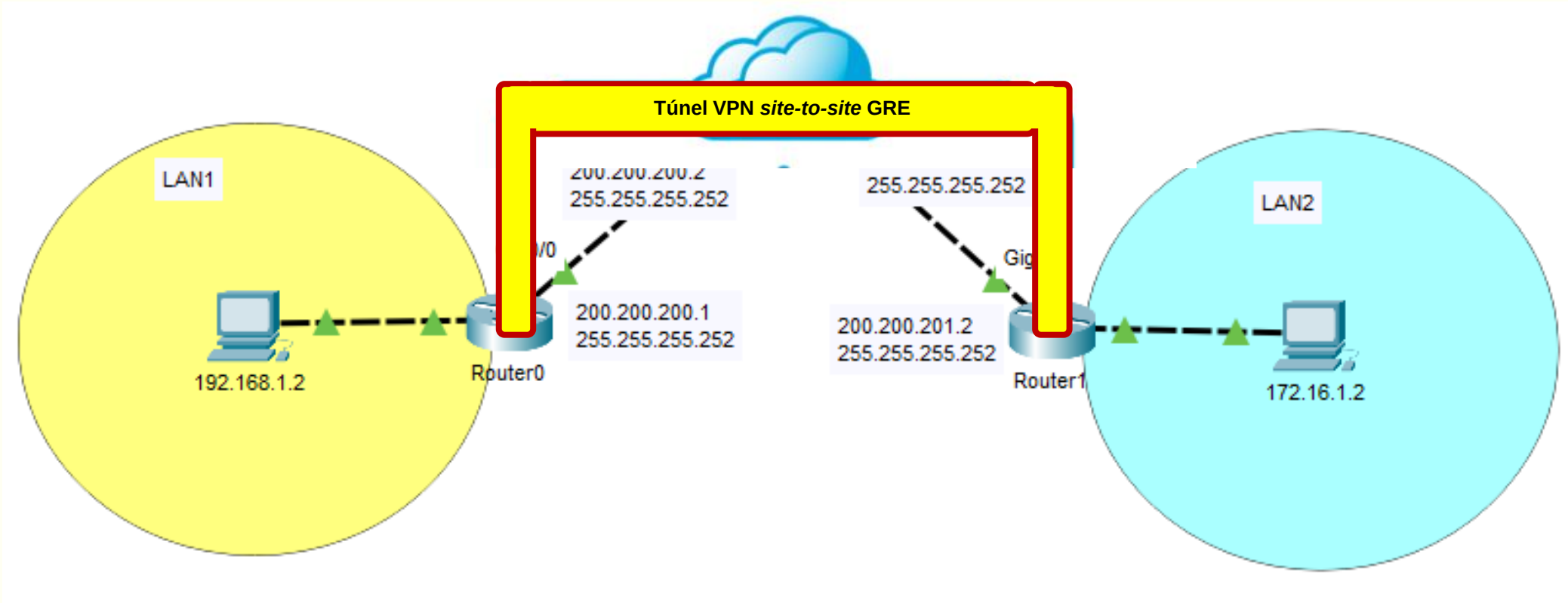
VPN tunnel GRE – *site-to-site*



Deseja-se Criar uma VPN (um "*túnel seguro*") entre o Router0 e o Router1, de forma que as informações que trafegarem pela Internet estejam protegidas.

Por túnel seguro entendemos o envio de pacotes criptografados!

VPN tunnel GRE – *site-to-site*



Deseja-se Criar uma VPN (um "*túnel seguro*") entre o Router0 e o Router1, de forma que as informações que trafegarem pela Internet estejam protegidas.
Por túnel seguro entendemos o envio de pacotes criptografados!

Direção da Segurança na Internet

Direção da Segurança na Internet 1#2

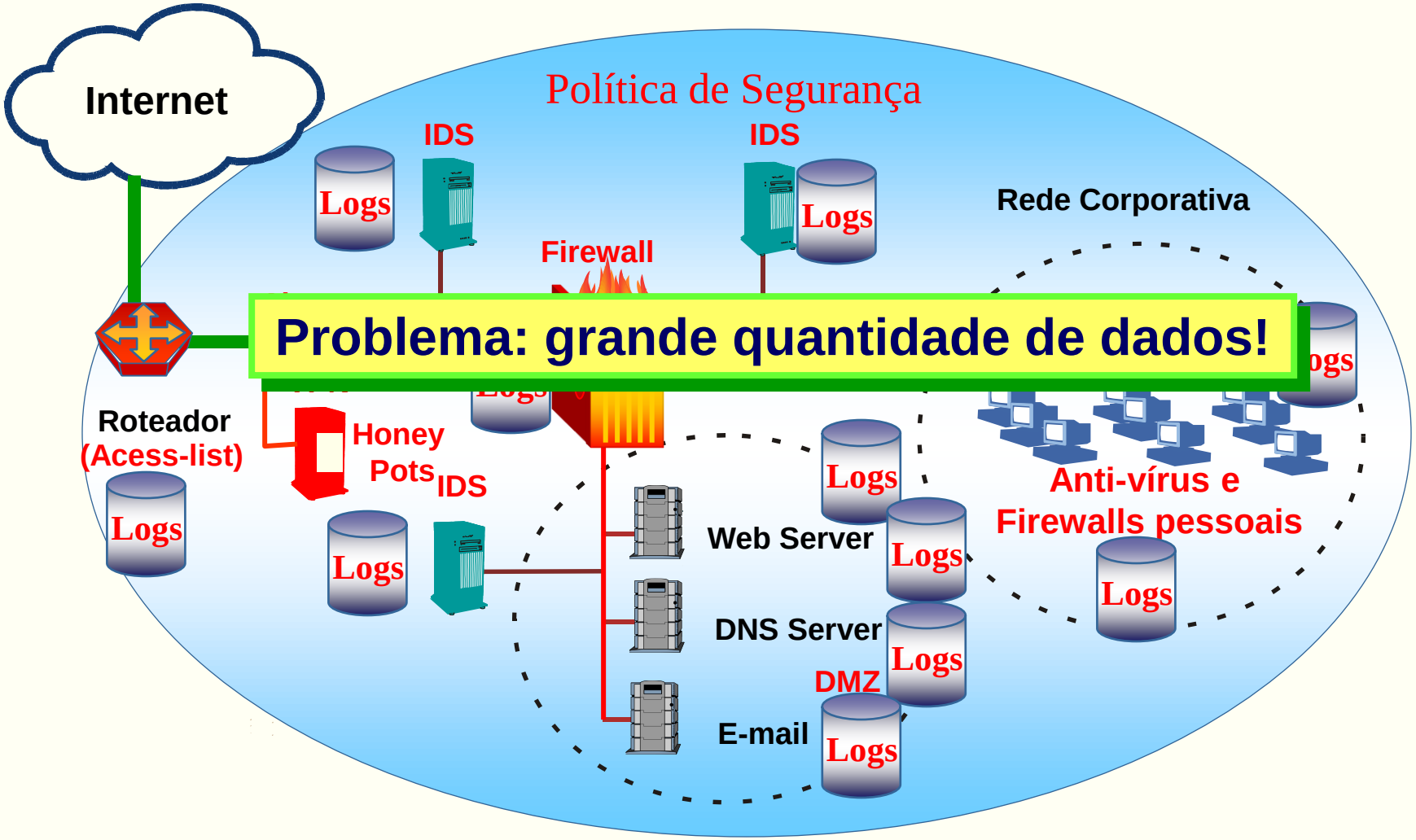
Com o que a comunidade Internet está deparando em termos de segurança nos próximos anos pode ser resumido nos seguintes itens:

- **O conhecimento (*expertise*) dos invasores está crescendo;**
- **A sofisticação dos ataques e ferramentas (*tools/toolkits*) está crescendo;**
- **O sucesso dos invasores está crescendo (conhecimento está sendo passado para intrusos com menos conhecimento e assim, tornando-os especialistas).**

Direção da Segurança na Internet 1#2

- O número de invasores está crescendo
- O número de empresas e usuários da Internet está crescendo
- A complexidade dos protocolos e aplicações executadas nos clientes e servidores conectados à Internet está crescendo

Cenário atual e seus problemas



"O problema onde há um excesso de dados pode ser tão prejudicial quanto a sua falta"

Referências Bibliográficas

Kurose, James F. Redes de computadores e a Internet: uma abordagem top-down/James F. Kurose e Keith W. Ross; 6ª edição, São Paulo: Addison Wesley, 2013. ISBN 978-85-8143-677-7.

Tanenbaum, Andrew S; Wetherall, David. Redes de Computadores. São Paulo: Pearson Prentice Hall, 2011. 5ª edição americana. ISBN 978-85-7605-924-0.

BIRKNER, Mathew H. Projeto de Interconexão de Redes. São Paulo: Pearson Education do Brasil, 2003. ISBN 85.346.1499-7.

Referências Bibliográficas

- Tanenbaum, A.; Wetherall, D. Redes de Computadores. 5ª ed. Pearson, 2011.
- Wikipedia. IEEE 802.1Q. Disponível em http://en.wikipedia.org/wiki/IEEE_802.1Q
- IEEE. 802.1Q-2011 - IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks. Disponível em http://standards.ieee.org/findstds/standard/802.1Q-2011.html
- ODOM, W. CCNA ICND2 – Guia Oficial de Certificação do Exame. 2ª ed. Alta Books, 2008.

Referência Complementar

- **Comer, Douglas E., Interligação de Redes Com Tcp/ip**

Referência Complementar

- GRE over IP Tunnel in Packet Tracer
  - https://www.youtube.com/watch?v=FyQSOAevcyk (17 minutos)
- Site to Site VPN with IPsec on Cisco Router
  - https://www.youtube.com/watch?v=Z7LwU6H5IGE (18 minutos)
  - https://www.youtube.com/watch?v=oamO3tfDUNE (41 minutos)
- Remote Access VPN - Packet Tracer
  - https://www.youtube.com/watch?v=8uWmFkrn6qE (30 minutos)
  - https://www.youtube.com/watch?v=lkUq6Pl6his (36 minutos)