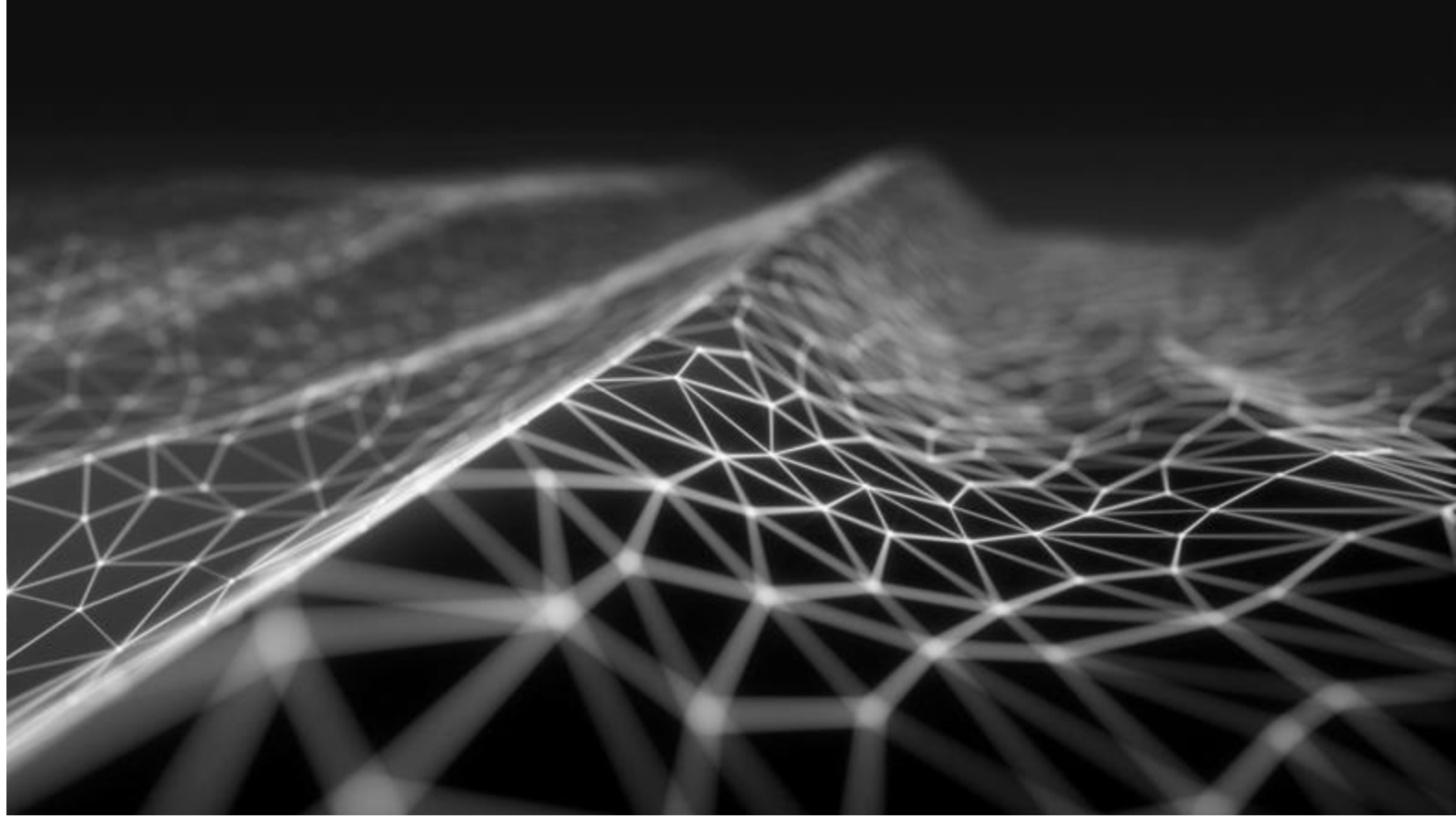


SEGURANÇA DA INFORMAÇÃO

PROFESSORES:

OSMAR DE OLIVEIRA BRAZ JUNIOR

RICHARD HENRIQUE DE SOUZA

OBJETIVOS

- Compreender os fundamentos da segurança da informação.

AFINAL, O QUE É SEGURANÇA DA INFORMAÇÃO?

- Go to **www.menti.com** and use the code **3181 7272**

- **Recurso: nuvem de palavras**
- **Brainstorm tempestade de ideias, é uma atividade desenvolvida para explorar a potencialidade criativa de um indivíduo ou de um grupo.**

SEGURANÇA DA INFORMAÇÃO

- A segurança dos sistemas de informação (SI) engloba um número elevado de questões que poderão estar sob a alçada de um ou vários indivíduos:

  - ✓ segurança de redes;
  - ✓ segurança física;
  - ✓ segurança de computadores;
  - ✓ segurança do pessoal;

SEGURANÇA DA INFORMAÇÃO

Segurança da Informação - envolve um conjunto de medidas necessárias por garantir que a **confidencialidade, integridade e disponibilidade** das informações de uma organização ou indivíduo de forma a preservar esta informação de acordo com necessidades específicas. (Portal Segurança da Informação)

SEGURANÇA DA INFORMAÇÃO

“É a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios” [ISO 27002].

TERMOS DE SEGURANÇA

Termos de segurança	Descrição
Recursos	Um ativo é algo de valor para uma organização. Inclui pessoas, equipamento, recursos e dados.
Vulnerabilidade	Uma vulnerabilidade é uma fraqueza de um sistema ou de seu design, que pode ser explorado por uma ameaça.
Ameaça	Uma ameaça é um perigo potencial para os ativos, dados ou rede de uma empresa FUNCIONALIDADE
Explorar	Um exploit é um mecanismo que tira proveito de uma vulnerabilidade.
Atenuação	A mitigação é a contramedida que reduz a probabilidade ou gravidade de uma ameaça ou risco potencial. Segurança de redes envolve múltiplas técnicas de mitigação.
Risco	Risco é uma probabilidade de uma ameaça explorar a vulnerabilidade de um ativo, com o objetivo de afetar negativamente uma organização. Risco é mensurado usando a probabilidade da ocorrência de um evento e suas consequências.

SITUAÇÃO ATUAL DA SEGURANÇA DE DADOS

- Cibercriminosos com experiência com ferramentas, técnicas a níveis de sofisticação e impactos sem precedentes;
- As violações de segurança de rede podem interromper o comércio eletrônico
- Essas violações podem resultar em perda de receita para empresas, roubo de propriedade intelectual, ações judiciais e até ameaçar a segurança pública.

TERMOS DE SEGURANÇA

Os ativos devem ser identificados e protegidos.

As vulnerabilidades devem ser tratadas antes que se tornem uma ameaça e serem exploradas.

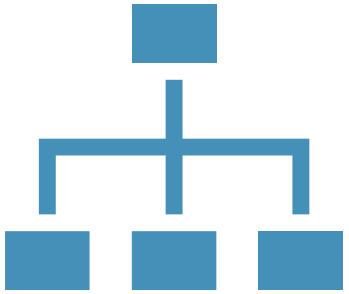
AMEAÇAS INTERNAS E EXTERNAS

- Um usuário interno, como um funcionário, pode acidentalmente ou intencionalmente:
- Roubar e copiar dados confidenciais para mídia removível, e-mail, software de mensagens e outras mídias.
- Comprometer a infraestrutura de rede.
- Desconectar uma conexão de rede crítica e causar uma interrupção na rede.
- Conecte uma unidade USB infectada em um sistema de computador corporativo.

AMEAÇAS INTERNAS

- Ameaças internas têm o potencial de causar tantos prejuízos quanto ameaças externas, pois os usuários internos têm acesso direto ao edifício e seus dispositivos de infraestrutura.
- Os funcionários normalmente têm da rede corporativa, seus recursos e seus dados confidenciais.
- Os profissionais de segurança de rede devem implementar ferramentas e aplicar técnicas para corrigir externos e internos.

PERDA DE DADOS



O ativo mais valioso de uma organização!

Perda ou transferência não autorizada de dados é quando os dados são intencionais ou involuntariamente perdidos, roubados ou vazados para o mundo externo.

VETORES DE ATAQUES

- Um vetor de ataque é um caminho pelo qual um atacante poder obter acesso a um servidor, equipamento ou rede.
- Os vetores de ataque são originários de dentro ou de fora da rede corporativa.

VETORES DE PERDA DE DADOS

- **E-mail / Redes sociais -** E-mail ou mensagens instantâneas interceptados podem ser capturados e revelados informações confidenciais
- **Dispositivos não criptografados -** Se os dados não principais armazenados usando um algoritmo de criptografia, o ladrão pode obter valiosos dados confidenciais.
- **Dispositivos de Armazenamento em nuvem -** Dados confidenciais em nuvem podem ser perdidos se o acesso à nuvem para comprometido devido a falhas de configurações de segurança.
- **Mídia removível -** Um risco é que um funcionário possa realizar uma transferência não autorizada de dado para uma unidade USB. Outro risco é que uma unidade USB contendo dados corporativos valiosos, podem ser perdidos.
- **Controle de acesso inadequado -** Senhas ou senhas que foram comprometidas podem fornecer fácil acesso aos dados corporativos.

O PROFISSIONAL DE SEGURANÇA

- Os profissionais de segurança de rede devem proteger os dados da organização.
- Vários controles de prevenção contra perda de dados devem ser implementados, combinando medidas estratégicas, operacionais e táticas.

VISÃO GERAL

O que é um hacker?

Go to **www.menti.com** and use the code **3181 7272**

O HACKER

- Hacker é um termo comum usado para descrever um ator de ameaça.
- Termos utilizados frequentemente usados para um tipo de hacker:
  - *white hat*
  - *black hat*
  - *gray hat*

WHITE HAT (HACKER ÉTICO)

- São hackers éticos que usam suas habilidades de programação para o bem, fins éticos e legais.
- Hackers White hat pode executar na rede, testes de penetração na tentativa de comprometer redes e sistemas usando seu conhecimento de sistemas de segurança de computadores para descobrir redes vulnerabilidades.
- Especialista em segurança da informação, e, desta forma, auxilia empresas a encontrar vulnerabilidades existentes em seus sistemas. São considerados “hackers do bem”.

GRAY HAT

- São os que cometem crimes e fazem coisas indiscutivelmente antiéticas, mas não para ganho pessoal ou para causar danos.
- Ao encontrar uma vulnerabilidade no sistema de uma empresa, o gray hat observa os dados ali inseridos, por vezes até os divulga, sem cometer crime. Contudo, não informa a empresa sobre a existência da vulnerabilidade.

BLACK HAT

- São criminosos antiéticos que comprometem a segurança de computadores e redes para ganho pessoal ou por motivos maliciosos, como atacando redes
- Os black hats se utilizam das vulnerabilidades que encontram para obter dados sigilosos, como dados pessoais, senhas, dados bancários, etc. São definidos, por alguns autores, como subcategoria dos crackers.

PARA DISCUTIR EM GRUPO

"Existe um abismo entre ser um hacker e um criminoso"

Felipe Prado, hacker ético da IBM

- Divisão em grupos
- 5 min para discutir sobre a temática hacker.
  - Escolher 1 para controlar o horário
  - Escolher 1 colega para anotar a discussão
  - Escolher 1 colega para comentar

DISCUSSÃO DOS GRUPOS

- “Ter acesso não dá o direito de acessar.” (Felipe Prado, hacker ético da IBM)

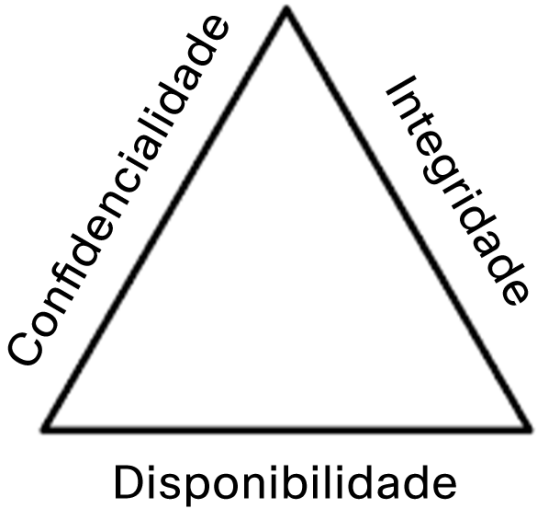
É assim que o profissional de segurança da informação deveria ver o mundo. Quem defende essa ideia é Felipe Prado, hacker ético da IBM, em entrevista ao The Office, podcast de Época NEGÓCIOS sobre futuro do trabalho.

QUAL O VALOR DA INFORMAÇÃO?

QUAL O VALOR DA INFORMAÇÃO?

- Importância estratégica para tomada de decisões
- Medidas de Segurança devem ser equivalentes ao valor da informação

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO



- Esses três princípios são:
- confidencialidade (confidentiality),
- integridade (integrity) e,
- disponibilidade (availability).
- Os princípios oferecem foco e permitem que especialistas em segurança priorizem ações para proteger o mundo digital.

CONFIDENCIALIDADE

Figura 1.1 - Confidencialidade da informação

- Garantir que somente as pessoas autorizadas tenham acesso às informações que queremos distribuir.
- Exige mecanismos de proteção. Ex: senhas, controle de acesso, etc.
  - Furto do nº do cartão e senha
  - Acesso não autorizado ao sistema

INTEGRIDADE

Figura 1.2 - Integridade da informação

- garantir que a informação não tenha sido alterada em seu conteúdo, seja intencionalmente ou não.
- ter a certeza que a informação disponibilizada pelo emissor é a mesma que chegou ao receptor.

DISPONIBILIDADE

Figura 1.3 - Disponibilidade da informação

- A informação deve estar disponível quando necessária;
- possa ser acessada no momento desejado;
- deve estar ao alcance dos usuários e destinatários.

VISÃO GERAL

Quais os objetivos da Segurança da Informação?

OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

- Proteger os Ativos (informação, computadores, equipamentos de conectividade, etc), garantindo a integridade, confidencialidade e disponibilidade das informações.

ATIVOS

- Qualquer elemento que tenha valor para a organização [ISO 27002];
- Os ativos fornecem suporte aos processos de negócios, portanto devem ser protegidos.
- Todo elemento utilizado para armazenar, processar, transportar, armazenar, manusear e descartar a informação, inclusive a própria.

ATIVOS

- O conceito de "segurança da informação" dentro de uma empresa é relativamente intuitivo: refere-se à **proteção das informações daquela empresa.**
- Embora o conceito de informação seja também intuitivo, a razão pela qual ela deve ser protegida nem sempre é clara.
- O conceito fundamental aqui é: informação é um ativo e, portanto, deve ser protegida.

ATIVOS

- Todo elemento que compõe o processo de comunicação (emissor, receptor, meio, etc)
- Possuem valor
- Devem receber proteção adequada para não causar danos
- Tipos: informação, equipamentos, pessoas.

RISCOS

- Probabilidade que as ameaças explorem os pontos fracos (vulnerabilidades)

AMEAÇAS

- Agentes capazes de explorar falhas de segurança;
- Podem provocar prejuízos quanto aos ativos, tais como perdas ou danos.
- Podem ser classificadas por grupos:
  - **naturais (**condições da natureza),
  - **intencionais** (fraudes, invasões, espionagens);
  - **Involuntárias** (vírus, acesso indevido por falta de conhecimento do usuário, falta de conhecimentos)

AMEAÇAS

- Agentes capazes de explorar falhas.
- Percebe-se ao longo da história que as ameaças sempre existiram.
- Conforme a tecnologia avança, novas ameaças surgem em vários contextos.

VULNERABILIDADES

São os pontos fracos que afetam os requisitos da segurança (integridade, confidencialidade e disponibilidade), quando explorados.

Vulnerabilidades (Físicas Naturais, Hardware, Software, Formas de Armazenamento, Comunicação e Humanas)

PROTEÇÕES

Tecnologias - dispositivos e produtos disponíveis para proteger os sistemas de informação e se defender de criminosos virtuais.

Políticas e práticas - procedimentos e orientações que viabilizam que as pessoas do mundo digital fiquem seguros e sigam boas práticas.

Pessoas - conscientes e bem-informadas sobre o mundo e os perigos que as ameaçam.

TIPOS DE ATAQUES

- Engenharia Social
- Vírus
- Ataques baseados em senhas
- Modificação de Dados – captura os dados e altera
- Negação de Serviço (Dos) - pode inundar um computador ou toda a rede com tráfego até que um desligamento ocorra devido à sobrecarga.
- IP Spoofing – mascarar endereços com Ips de endereços falsificados.
- Phishing – obter dados confidenciais por meio de um disfarce de entidade confiável (email falso, msg instantânea)

TIPOS DE FERRAMENTAS DE ATAQUES

- Ferramentas para Quebra se Senhas
- Ferramentas de hackers para redes sem fio
- Scanning em rede e Ferramentas de hacking
- Criação de pacotes
- Sniffers de pacotes
- Ferramentas de criptografia
- Ferramentas de Exploração de vulnerabilidade
- Sistemas Operacionais - Estes são sistemas operam especialmente pré-carregados com ferramentas otimizado para hackers.
- Scanners de vulnerabilidades
- Keylogger

ENGENHARIA SOCIAL

- É uma técnica de ataque:
  - usa persuasão
  - confiança
  - ingenuidade
- Consegue as informações: por telefone, por e-mail, por contato pessoal ou por funcionários.

MALWARE

- O primeiro e mais comum tipo de malware de computador é um vírus.
- Vírus - ação humana para propagar e infectar outros computadores. Por exemplo, um vírus pode infectar um computador quando uma vítima abre um anexo de email, abre um arquivo em uma unidade USB ou baixa um arquivo.
- O vírus se esconde conectando-se um código de computador, software ou documentos no computador. Quando aberto, o vírus é obtido e infecta o computador.

VÍRUS

Tipos de Vírus	Descrição
Vírus de setor de boot	O Vírus ataca o setor de boot, uma tabela de partição ou o sistema de arquivos.
Vírus de Firmware	Vírus ataca ou firmware do dispositivo.
Vírus de macro	O vírus usa o recurso de macro do MS Office ou de outros aplicativos maliciosamente.
Vírus de programas	O vírus se insere em outro programa executável.
Vírus de scripts	O vírus ataca o interpretador do SO, usado para executar scripts.

CAVALOS DE TRÓIA

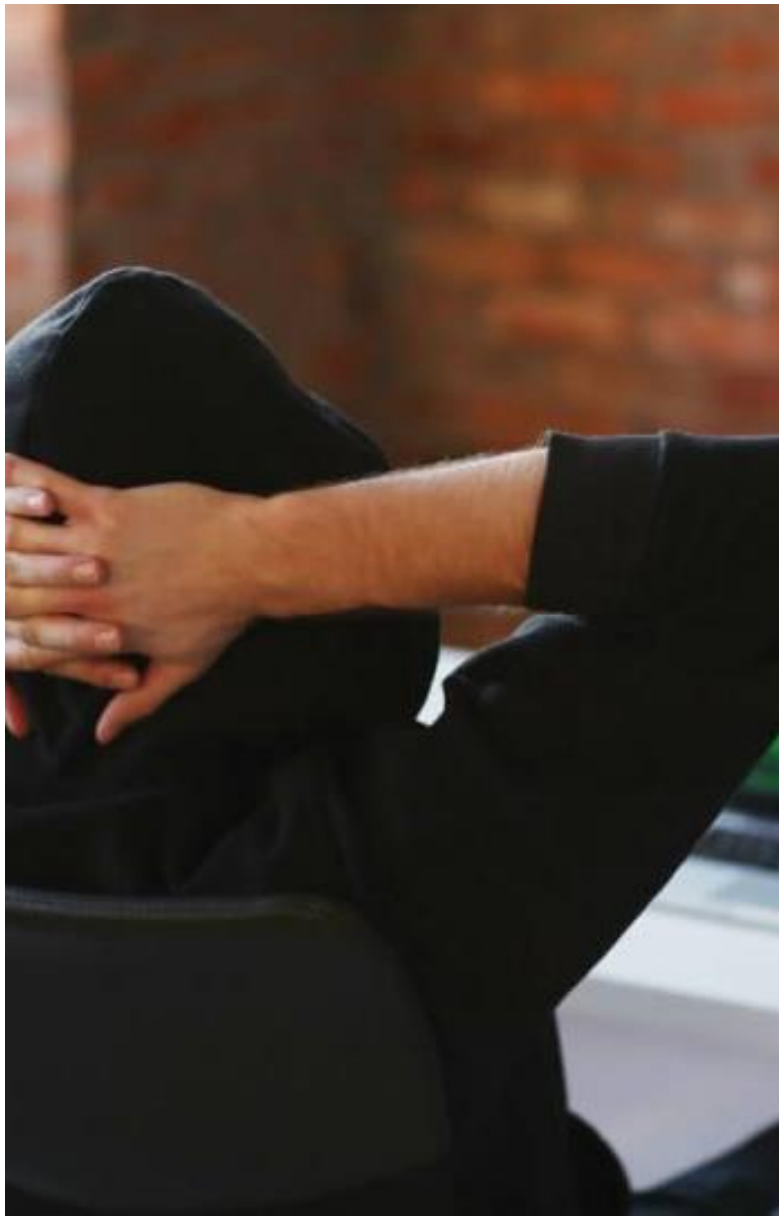
- Um programa que parece útil, mas também carrega código malicioso.
- Os cavalos de Tróia geralmente são oferecidos como programas on-line gratuitos, como jogos de computador. Usuários inocentes baixam e instalam o jogo, junto com o cavalo de Tróia.

TIPOS DE CAVALO DE TROIA

Tipo do Cavalo de Troia	Descrição
Acesso remoto	O cavalo de Tróia permite o acesso remoto não autorizado.
Envio de dados	O cavalo de Tróia oferece ao agente de correção dados confidenciais, como senhas.
Destrutivo	O cavalo de Tróia corrompe ou apaga arquivos
Proxy	O cavalo de Tróia usará o computador da vítima como dispositivo de origem para lançar e realizar outras atividades ilegais.
FTP	O cavalo de Troia permite serviços não autorizados de transferência de arquivos em dispositivos finais. dispositivos.
Desativador do software de segurança	O cavalo de Troia interrompe o funcionamento de programas antivírus ou firewalls.
Negação de Serviço (DoS)	O cavalo de Tróia reduz ou interrompe a atividade de rede.
Agentes de log de digitação	O cavalo de Tróia tenta ativamente roubar informações confidenciais, como números de cartão de crédito, gravando como teclas digitadas em um formulário web. formulário.

OUTROS TIPOS DE MALWARE

- **Adware -** O adware geralmente é distribuído através do download de software online. Janelas pop-up. apresentam propagandas incorporados a softwares e serviços.
- **Rootkit** - são usados por atores de correção para obter acesso no nível da conta de administrador de um computador. Difícil de detectar.
- **Spyware** - software que monitora informações e as envia para terceiros. O software espião pode ser uma ameaça baixa, reunindo dados de navegação ou pode ser uma alta ameaça capturando informações pessoais e financeiras. Spyware podem: monitorar acesso Internet, teclas ou cliques instalar outros programas, capturar informações capturar senhas bancárias/nº cartões crédito, apturar senhas de 57 acesso a sites...
- **Worm** - programa que se propaga automaticamente na rede enviando cópias de si mesmo de computador para computador.
- **Ransomware** - normalmente nega ao usuário acesso aos seus arquivos criptografando os arquivos e exibindo uma mensagem exigindo um resgate pela chave de descriptografia.
- **Keylogger -** captura e armazena teclas digitadas no teclado.

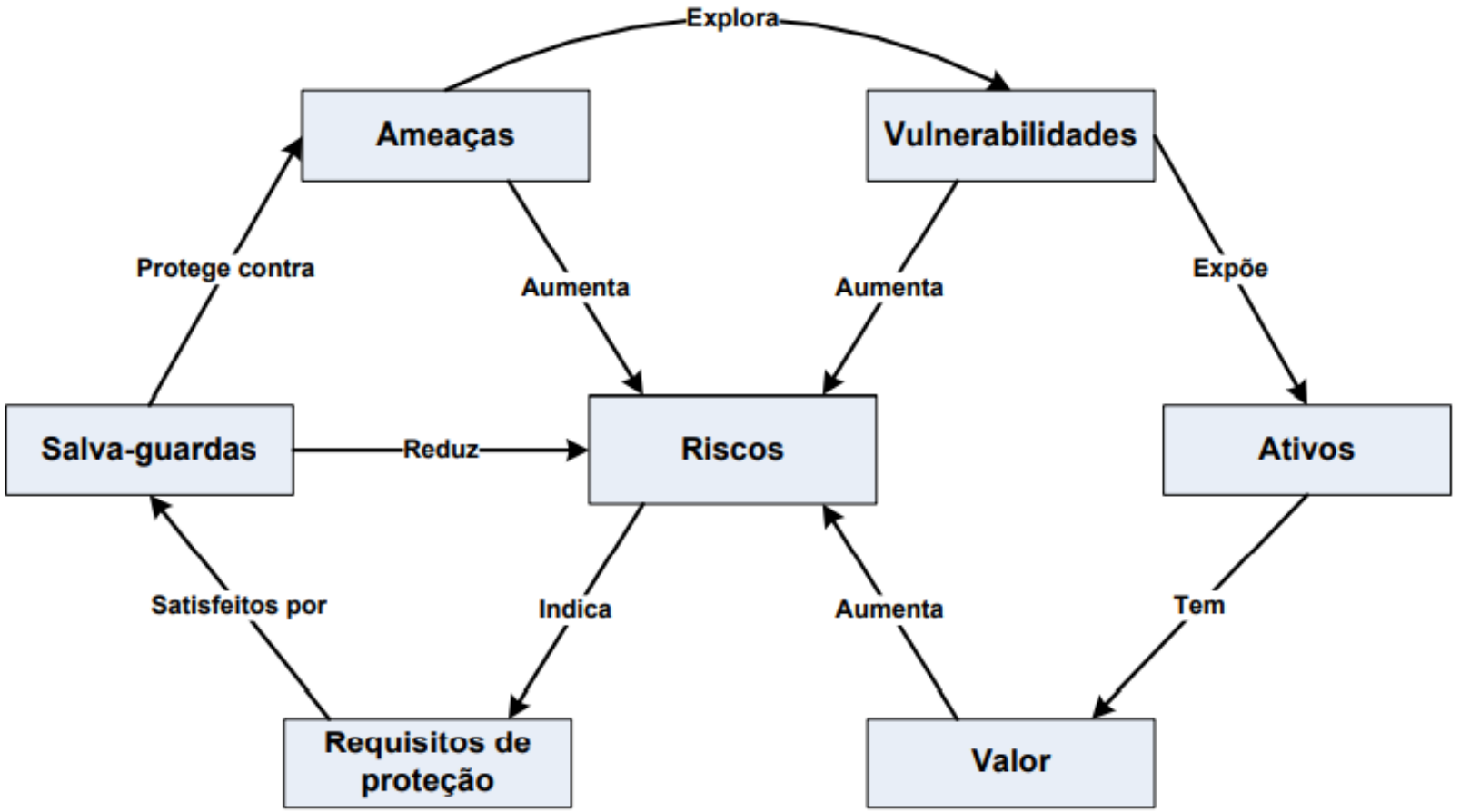


PARA DISCUTIR EM EQUIPE

- Pesquise um case de invasão de dados/ataque causado por vírus ou hacker.
- Para discutir:
  1. O tipo de ataque
  2. Princípio de segurança quebrado
  3. Possíveis tipos de ferramentas utilizadas pelo atacante
  4. Que mecanismos de segurança seriam adequados no estudo desse case.
  5. Elencar algumas práticas de proteção contra a Engenharia Social

VISÃO GERAL

Criptografia


Explora
Ameaças
Vulnerabilidades
Protege contra
Aumenta
Aumenta
Expõe
Salva-guardas
Reduz
Riscos
Ativos
Satisfeitos por
Indica
Aumenta
Tem
Requisitos de proteção
Valor

CRIPTOGRAFIA

- Integridade dos dados
- Uma tendência nas comunicações
- Algoritmos

CRIPTOGRAFIA

- Criptografia é a aplicação de um conjunto de técnicas matemáticas utilizadas para proteger as informações, garantindo a confidencialidade da informação.

CRIPTOANÁLISE

- É a forma de tornar legível uma informação cifrada sem o conhecimento do algoritmo e da chave.
- Ou seja, tenta-se quebrar o "segredo" utilizado para tornar uma informação ilegível.

TIPOS DE CIFRAS

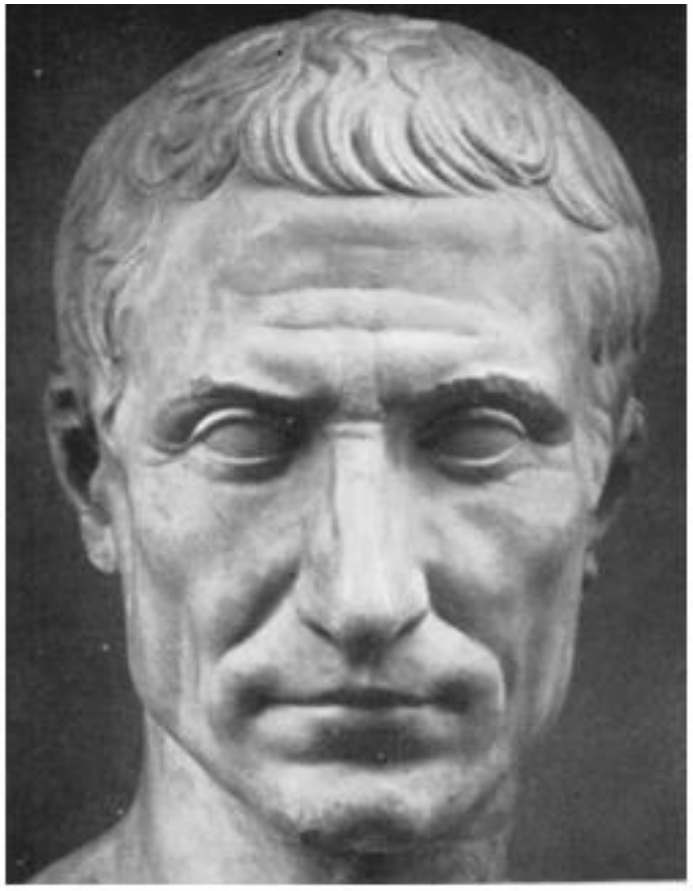
- **Substituição:** as letras/caracteres originais de um texto são substituídos por outras. Troca-se uma coisa por outra.
- **Transposição:** a mensagem é reescrita conforme o número de caracteres pertencentes a chave. Troca-se as coisas de lugar. Usando transposição simples, pode-se escrever a palavra "teste" como "ettse", transpondo uma letra com a sua vizinha.

- O método matemático de substituição para inviabilizar a leitura mais antigo que se tem registro é a cifra de César. Elaborada por Júlio César, esta cifra inaugurou as chamadas cifras de substituição monoalfabéticas.

ESTEGANOGRAFIA

- Esta técnica de esconder mensagens é chamada de *esteganografia* e sua versão moderna consiste em esconder mensagens em imagens ou músicas.
- Ocultação de mensagens em arquivos de texto, imagens ou sons

CIFRAS DE SUBSTITUIÇÃO

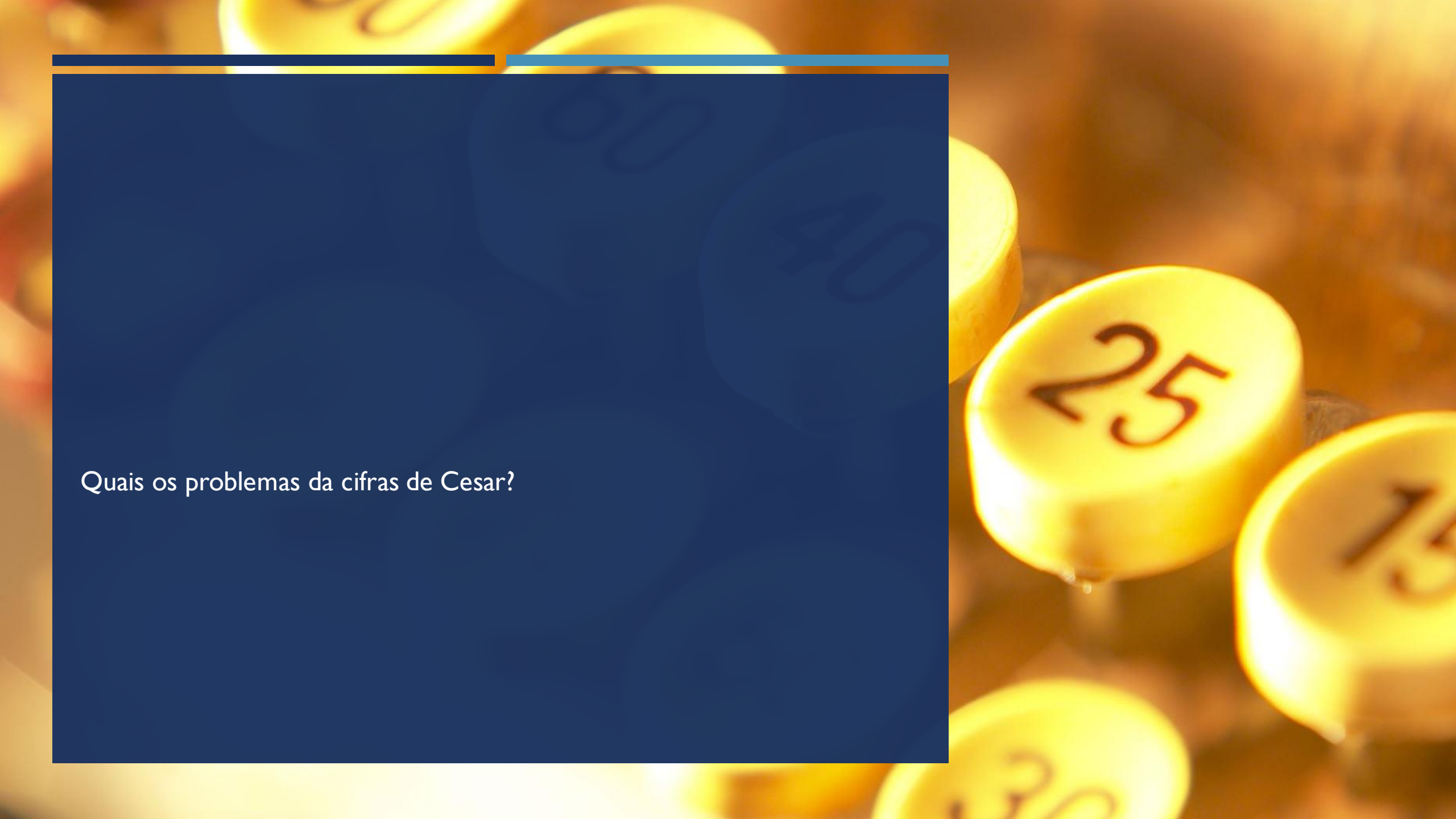


Júlio César

CIFRAS DE CÉSAR

- técnica de criptografia bastante simples!
- **cifra de substituição**, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto porém deslocada um certo número de posições à esquerda ou à direita.
- Por exemplo, se usarmos uma troca de quatro posições à esquerda, cada letra é substituída pela letra que está quatro posições adiante no alfabeto, e nesse caso a letra A seria substituída pela letra E, B por F, C por G, e assim sucessivamente.
- foi utilizada por Júlio César para se comunicar com seus generais, protegendo mensagens militares.
- Um site interessante para se brincar com cifras de césar é o **ROT13**: http://www.rot13.com/

Quais os problemas da cifras de Cesar?



CIFRAS DE CÉSAR

- Uma variação da Cifra de César consiste em trocar a letra pela vizinha k ao invés da 3.
- Tendo k igual a 3, terei que o "A" troca por "D".
- Se usar k=6, terei que o "A" troca por "G", e assim por diante.
- A ideia deste algoritmo é que todos conheçam o método (trocar por um valor de K), mas ninguém sabe por qual vizinha é.
- Tem-se o conceito de chave (K). .

TIPOS DE CRIPTOGRAFIA:

- Simétrica ou de chave única
- Assimétrica: Par de chaves pública e privada

CHAVE SIMÉTRICA

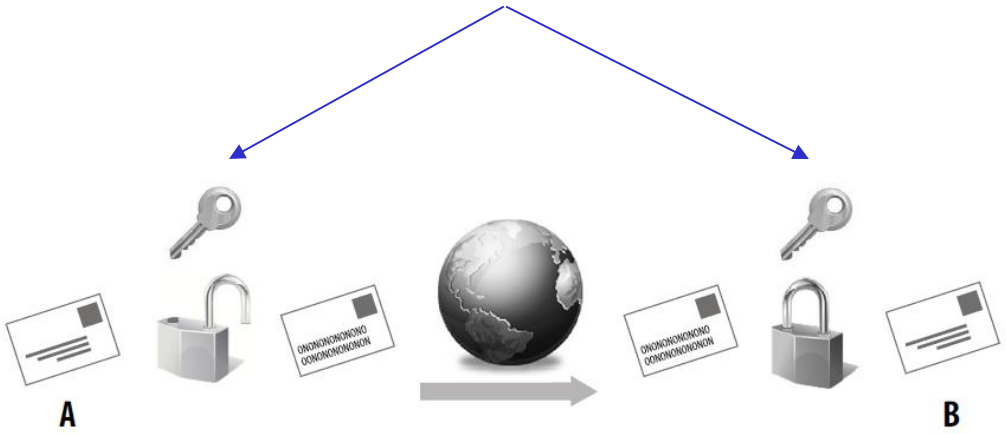


Figura 2.2 – Criptografia Simétrica

- Também conhecida como criptografia de chave privada, utiliza a mesma chave para cifrar e decifrar uma informação.

Algoritmos	Tamanho
DES	56-bit
Triple-DES	~ 120-bit
CAST	40, 64, 80, 128 – bit
RC2	40, 128 – bit
IDEA	128 – bit
AES	128, 256 – bit

CHAVE SIMÉTRICA

ALGORITMOS

CRIPTOGRAFIA SIMÉTRICA – CHAVE SECRETA

- Utilizada desde a antiguidade
- Algoritmos rápidos – confidencialidade no tráfego
- Depende do contato entre as partes

MODELO DE CIFRAS SIMÉTRICAS

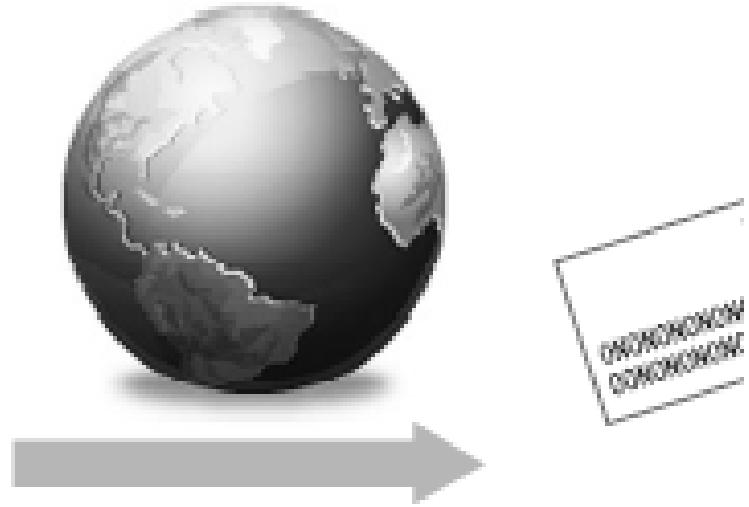
- Texto claro
- Algoritmo de criptografia
- Chave secreta
- Texto cifrado
- Algoritmo de decriptografia

ATAQUES POR FORÇA BRUTA

- Método que testa todas as possibilidades de chaves possíveis
- Considerando o método de Cesar com o valor da chave de K,
- k pode assumir uma variedade limitada de valores. Ele pode ser 0,1, 2, 3, ... 25, sendo que neste último o "A" seria trocado pelo "Z".

ASSIMÉTRICAS

- **Método**: o algoritmo matemático que faz a cifra e a decifragem. Não deve ser segredo.
- **Chave**: único segredo. Uma informação que alimenta o algoritmo para cifrar ou decifrar. Quanto mais possibilidades, mais inviável é o força bruta.



2.7 – Criptografia Assimétrica

CRIPTOGRAFIA ASSIMÉTRICA

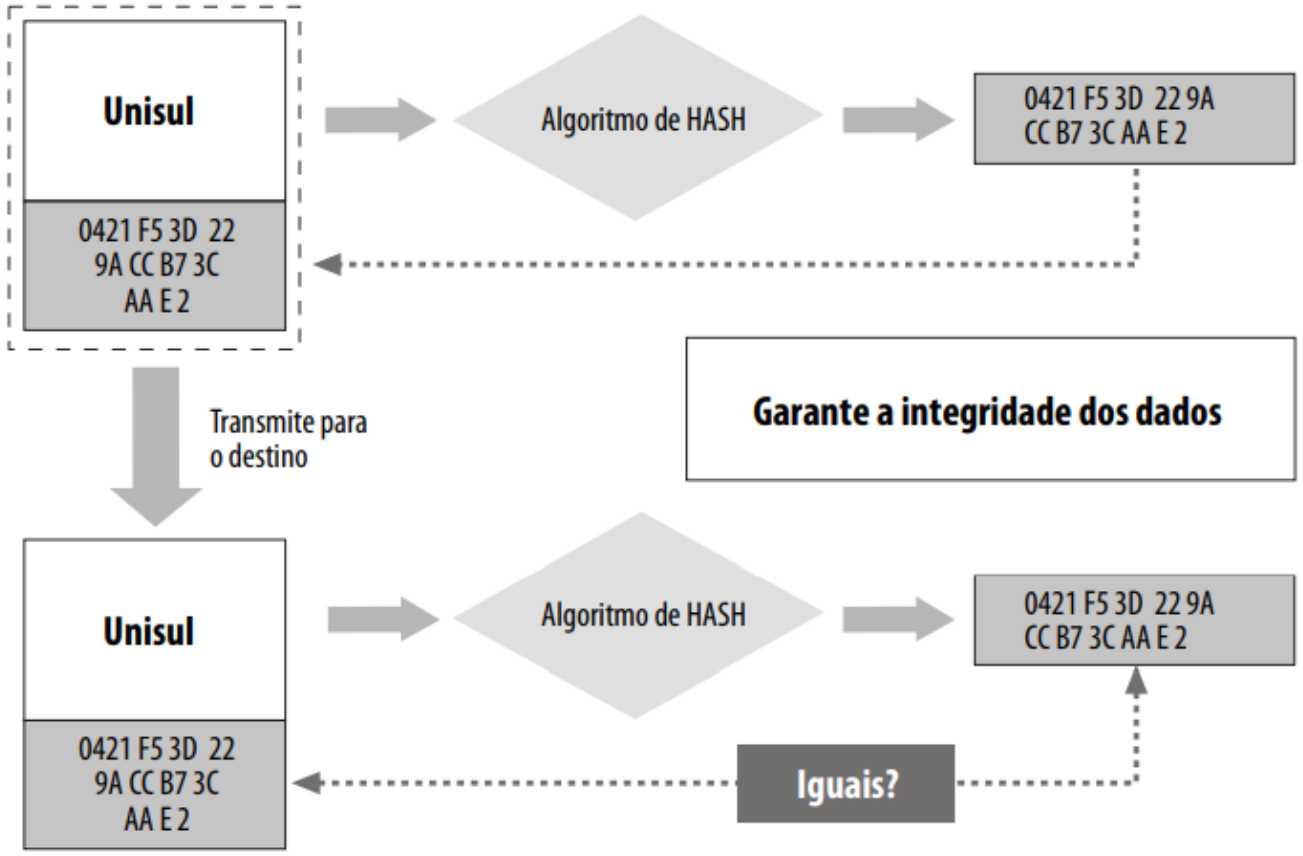
RSA (Rivest, Shamir e Adleman)	Tamanho de chave recomendado: **1024** bits
DSA (*Digital Signature Algorithm*) utilizado somente para assinaturas digitais	Tamanho de chave recomendado: **1024** bits
DH (Diffie Hellman) utilizado para a troca de chaves e criptografia	Tamanho de chave recomendado: **1024** bits
EC (*Elliptc Curves*) similar ao DAS e ao DH em suas funções	Tamanho de chave recomendado: **192** bits

- A criptografia assimétrica é também conhecida como criptografia de chave pública.
- Ela recebe este nome porque utiliza um par de chaves: uma chave pública e uma chave privada.

FUNÇÃO HASH

- É uma função matemática que gera um resumo da mensagem.
- **Função de mão única** – a partir do resultado da função hash não é possível adquirir a informação que a gerou.
- **Tamanho fixo** – independente do tamanho da informação utilizada para gerar o hash, o tamanho de saída é o mesmo. Este fator depende do algoritmo utilizado para gerar o hash.
- Se o algoritmo utilizado for o MD5 então o tamanho resultante será de128b e se for o SHA-1 então o tamanho será de 160b.
- A alteração de apenas 1 bit na informação de entrada mudará totalmente o hash gerado.

ALGORITMO DE HASH



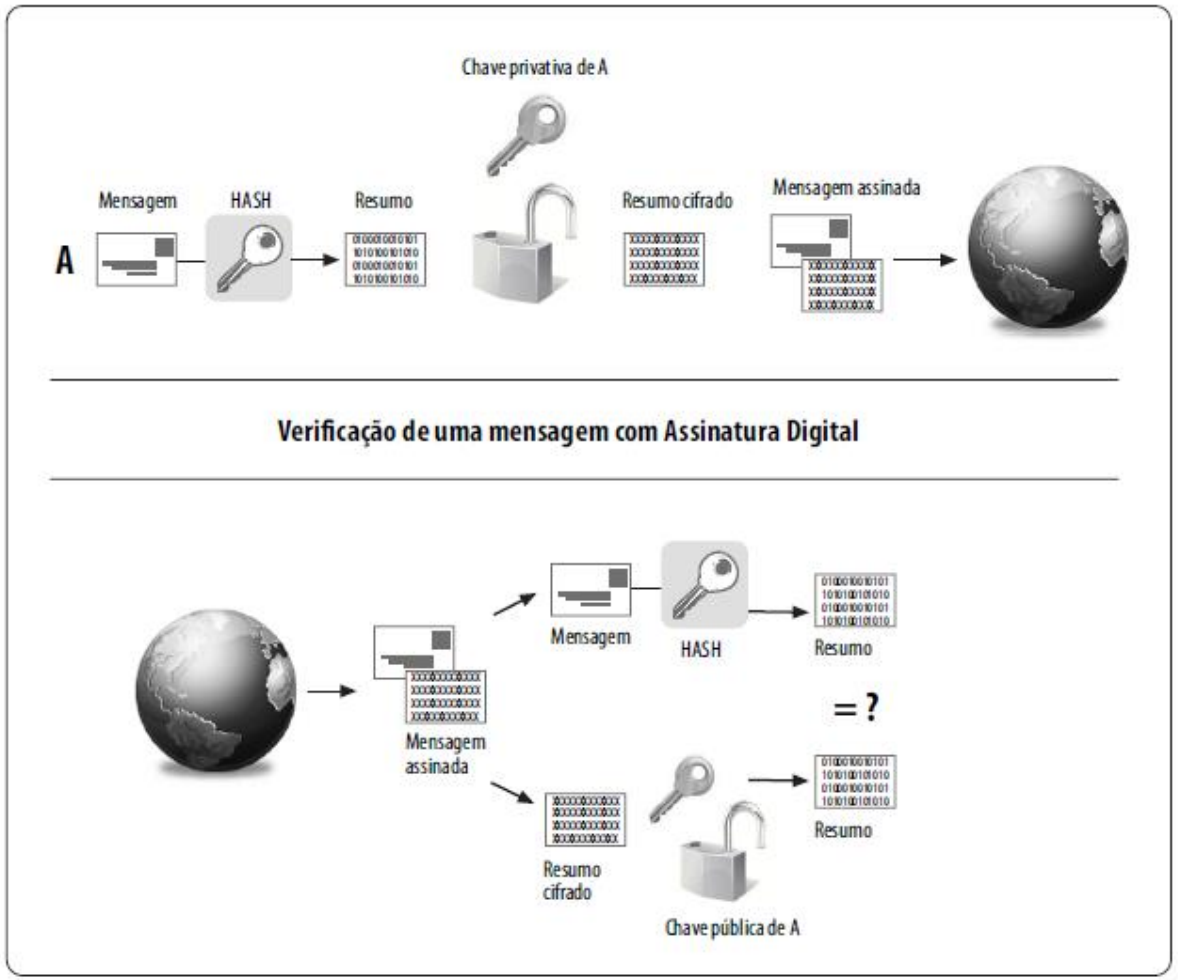
PERGUNTAS....

- Você considera que a função hash, isoladamente garante a integridade da informação?

ASSINATURA DIGITAL

- O hash **é cifrado com a chave privada do emissor** garantindo assim que somente sua chave pública desfaça o processo e garante que realmente foi o emissor que gerou o hash.
- Caso seja a mensagem seja confidencial, será necessário cifrar, no emissor, todo o "pacote" com a chave pública do destinatário, para garantir que somente ele tenha acesso.

ASSINATURA DIGITAL



CERTIFICADOS DIGITAIS

- Autenticar pessoas, equipamentos e entidades e agem como passaporte digital, ao comprovar a veracidade dos dados contidos nele após uma solicitação o processo segue adiante.

PARA DISCUTIR EM EQUIPE

- Para discutir:
  1. Qual princípio da Segurança é garantido pela criptografia?
  2. Pesquise 2 algoritmos de chave simétrica e 2 de chaves assimétricas.
  3. Comente.
  4. Existem 3 algoritmos hash bem conhecidos: MD5 com resumo de 128 bits, Algoritmo de hash SHA e SHA-2
  5. Quais suas características e usos.

LABORATÓRIO – AULA PRESENCIAL

LABORATÓRIO DE PRÁTICA

Neste laboratório, você completará os seguintes objetivos:

- Implementar as Configurações Básicas do Dispositivo
- Implementar as Medidas Básicas de Segurança no Roteador
- Implementar as Medidas Básicas de Segurança no Switch

SEGURANÇA DO DISPOSITIVO

As configurações de segurança são definidas com os valores padrão quando um novo sistema operacional é instalado em um dispositivo. Na maioria dos casos, esse nível de segurança é inadequado. Para roteadores Cisco, o recurso Cisco AutoSecure pode ser usado para ajudar a proteger o sistema.

Além disso, existem algumas etapas simples que podem ser executadas e que se aplicam à maioria dos sistemas:

- Nomes de usuário e senhas padrão devem ser trocados imediatamente.
- O acesso aos recursos do sistema deve ser restrito apenas aos indivíduos que estão autorizados a usá-los.
- Todos os serviços e aplicações desnecessários devem ser desativados e desinstalados assim que possível.
- Em geral, dispositivos vindos de fábrica ficaram estocados em um depósito por um período e não têm os patches mais atuais instalados. É importante atualizar todos os softwares e instalar todos os patches de segurança antes da implementação.

SENHAS

É importante usar senhas fortes para proteger dispositivos de rede. Estas são as diretrizes padrão a serem seguidas:

- Use uma senha de pelo menos 8 caracteres, preferencialmente 10 ou mais caracteres.
- Use senhas complexas. Inclua uma combinação de letras maiúsculas e minúsculas, números, símbolos e espaços, se permitido.
- Evite as senhas com base em repetição, palavras comuns de dicionário, sequências de letras ou números, nomes de usuário, nomes de parentes ou de animais de estimação, informações biográficas, como datas de nascimento, números de identificação, nomes de antepassados ou outras informações facilmente identificáveis.
- Deliberadamente, soletre errado uma senha. Por exemplo, Smith = Smyth = 5mYth ou Security = 5ecur1ty.
- Altere as senhas periodicamente. Se uma senha é inadvertidamente comprometida, a janela de oportunidade para que o invasor a use é limitada.
- Não anote as senhas e muito menos as deixe em locais óbvios, como em sua mesa ou no monitor.

Nos roteadores Cisco, os espaços à esquerda são ignorados em senhas, mas os espaços após o primeiro caractere não são ignorados. Portanto, um método para criar uma senha forte é utilizar a barra de espaço e criar uma frase feita de muitas palavras. Isso se chama uma frase secreta. Uma frase secreta é geralmente mais fácil de lembrar do que uma senha simples. Também é maior e mais difícil de ser descoberta.

SEGURANÇA DE SENHA ADICIONAL

Existem várias etapas que podem ser tomadas para ajudar a garantir que as senhas permaneçam secretas em um roteador e switch Cisco, incluindo estes:

- Criptografe todas as senhas de texto sem formatação com o comando **service password-encryption.**
- Defina um comprimento mínimo aceitável de senha com o comando **security passwords min-length** .
- Impedir ataques de adivinhação de senha de força bruta com o ***comando login block-for # attempts # dentro de #*** **.**
- Desative um acesso de modo EXEC privilegiado inativo após um período especificado de tempo com o comando **exec-timeout** .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

ATIVAÇÃO DO SSH

É possível configurar um dispositivo Cisco para suportar SSH usando as seis etapas a seguir:

1. **Configure um nome de host de dispositivo exclusivo**. Um dispositivo deve ter um nome de host exclusivo diferente do padrão.
2. **Configure o nome do domínio IP.** Configure o nome de domínio IP da rede usando o comando **ip-domain name** do modo de configuração global.
3. **Gere uma chave para criptografar o tráfego SSH**. O SSH criptografa o tráfego entre a origem e o destino. No entanto, para fazer isso, uma chave de autenticação exclusiva deve ser gerada usando o comando de configuração global **crypto key gerar rsa general-keys módulos***bits* . O módulo *bits* determina o tamanho da chave e pode ser configurado de 360 bits a 2048 bits. Quanto maior o valor de bit, mais segura a chave. No entanto, valores de bits maiores também levam mais tempo para criptografar e descriptografar informações. O tamanho mínimo recomendado do módulo é 1024 bits.
4. **Verifique ou crie uma entrada de banco de dados local**. Crie uma entrada de nome de usuário do banco de dados local usando o comando de configuração global **username**.
5. **Os usuários se autenticam no banco de dados local. Use o** comando login local line configuration para autenticar a linha vty no banco de dados local.
6. **Habilite a entrada vty nas sessões SSH. Por padrão, nenhuma sessão de entrada é permitida em linhas vty. Você pode especificar vários protocolos de entrada, incluindo Telnet e SSH, usando o** comando transport input [ssh | telnet].

DESABILITAR SERVIÇOS NÃO UTILIZADOS

Os roteadores e switches Cisco começam com uma lista de serviços ativos que podem ou não ser necessários em sua rede. Desative todos os serviços não utilizados para preservar os recursos do sistema, como ciclos de CPU e RAM, e impedir que os atores ameaçadores explorem esses serviços.

- O tipo de serviços que estão ativados por padrão varia dependendo da versão do IOS. Por exemplo, o IOS-XE normalmente terá apenas portas HTTPS e DHCP abertas. Você pode verificar isso com o comando **show ip ports all** .
- As versões do IOS anteriores ao IOS-XE usam o comando **show control-plane host open-ports** .

PACKET TRACER - CONFIGURAR SENHAS SEGURAS E SSH

Neste Packet Tracer, você configurará senhas e SSH:

- O administrador da rede solicitou que você preparasse o RTA e o SW1 para implantação. Antes de poderem ser conectados à rede, é necessário ativar as medidas de segurança.

LAB — CONFIGURAR DISPOSITIVOS DE REDE COM SSH

Nesse laboratório, você completará os seguintes objetivos:

- Parte 1: Implementar as Configurações Básicas dos Dispositivos
- Parte 2: Configurar o Roteador para o Acesso SSH
- Parte 3: Configurar o Switch para o Acesso SSH
- Parte 4: SSH da CLI no Switch

FIREWALL

FIREWALL - CONCEITO

"Ponto entre duas ou mais redes, no qual circula todo o tráfego. A partir desse ponto é possível controlar e autenticar todo o tráfego." (Cheswick e Bellovin)

"Componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre conjunto de redes." (Chapman)

OBJETIVOS

- Proteger uma rede privada contra “intrusos”
- Impedir acessos a recursos computacionais por usuários não autorizados
- Impedir vazamento de informações não autorizadas
- Controle da segurança

POR QUE FIREWALL ?

- Firewall é um sistema integrado, utilizado em redes de computadores para a sua proteção, composto por filtros de pacotes, filtros de estados, IDS, IPS, proxies, dentre outros, que segue a política de segurança estabelecida pela empresa.
- todo o tráfego que entra e sai para a internet passa pelo firewall, sendo analisado e liberando ou não o acesso.

POR QUE FIREWALL ?

Ele serve para vários propósitos como:

Restringir o acesso de usuários externos à rede interna (a verificação é realizada cuidadosamente, via um ponto de controle).

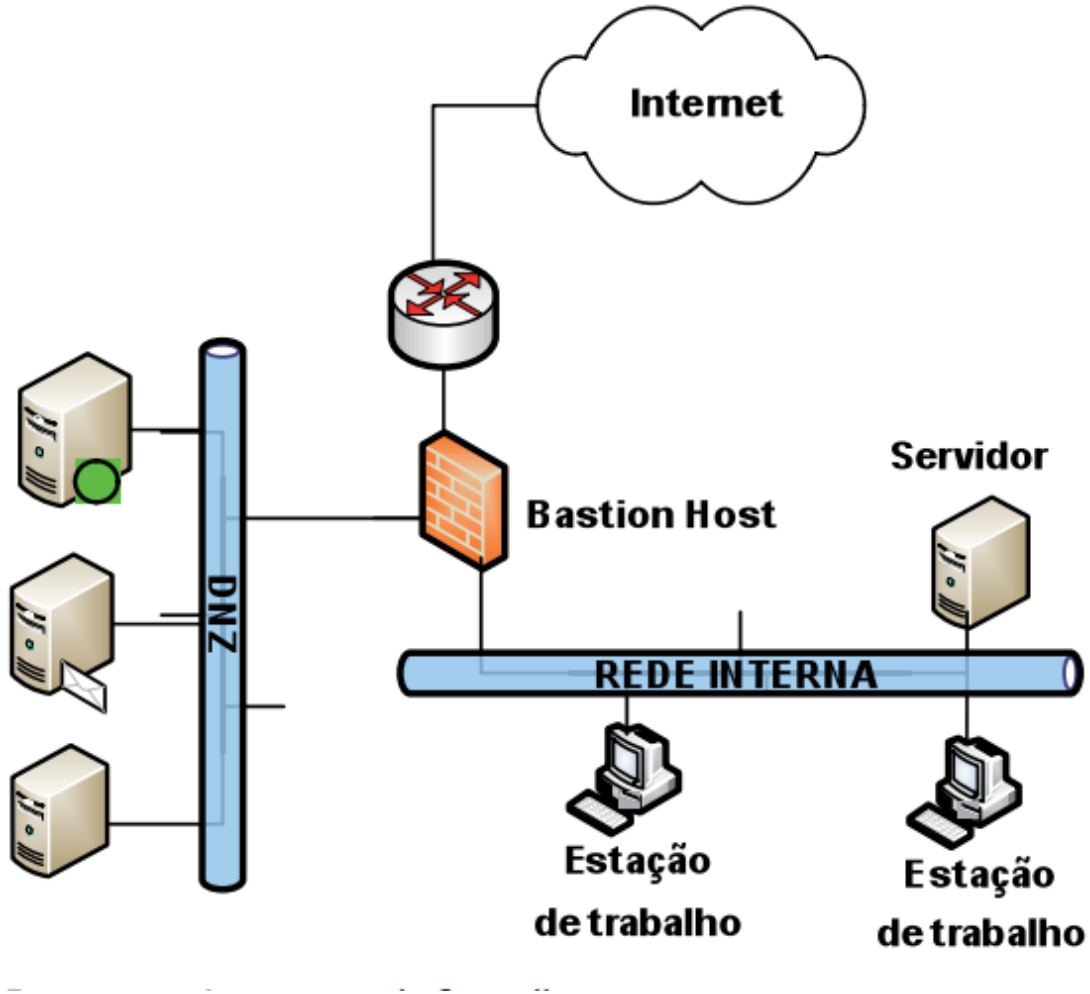
Prevenir contra-ataques.

Restringir que usuários internos da rede tenham acesso à internet e sites não autorizados.

POR QUE FIREWALL ?

- As ameaças passam a vir de todos os lados: **Internet** e **rede interna** (corporativa).

- Um firewall poderá bloquear tanto o acesso externo, como acesso interno, liberando apenas para algumas máquinas.



POR QUE FIREWALL ?

POR QUE FIREWALL ?

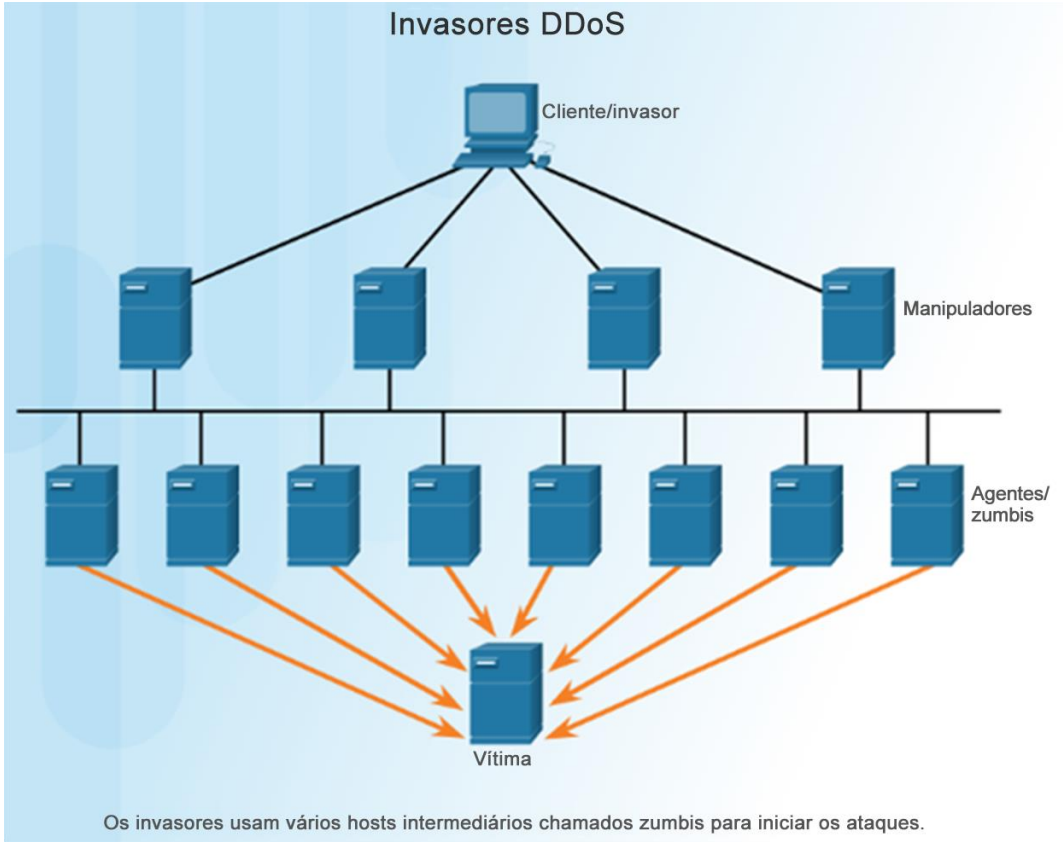
- Um Firewall pode **controlar os pacotes de serviços não confiáveis**:
  - telnet,
  - FTP,
  - NFS,
  - DNS,
  - SMTP, etc.

O QUE UM FIREWALL NÃO PODE REALIZAR?

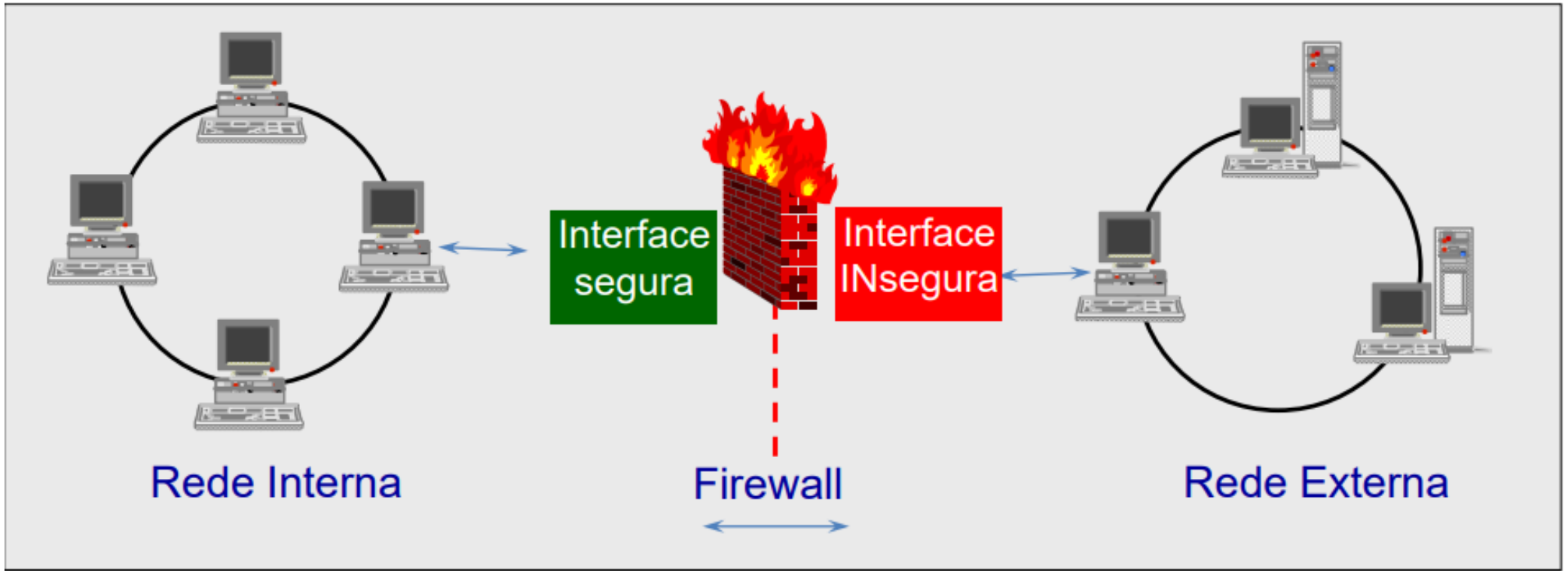
- Proteger contra usuários internos mal intencionados;
- Proteger a empresa de conexões que não passam por ele;
- Proteger contra novas ameaças;
- Proteger contra vírus;
- Ser configurado automaticamente.

DETECÇÃO DE ATAQUES EM TEMPO REAL

- Ataque de dia zero
  - Um hacker explora uma falha em uma parte do software antes do criador poder corrigi-la.
- **Varredura em tempo real da borda para o endpoint**
  - varredura ativa de ataques usando firewall e dispositivos de rede IDS/IPS.
  - detecção com conexões a centros on-line de ameaça global
  - detecção de anomalias de rede usando a detecção de comportamento e análise baseada em contexto
- **Ataques de DDoS e resposta em tempo real**
  - DDoS, uma das maiores ameaças de ataque, pode paralisar os servidores da Internet e a disponibilidade de rede.
  - A DDoS origina centenas, ou milhares de hosts zumbis, e os ataques aparecem como tráfego legítimo.



SISTEMA DE SEGURANÇA - FIREWALL



FIREWALL

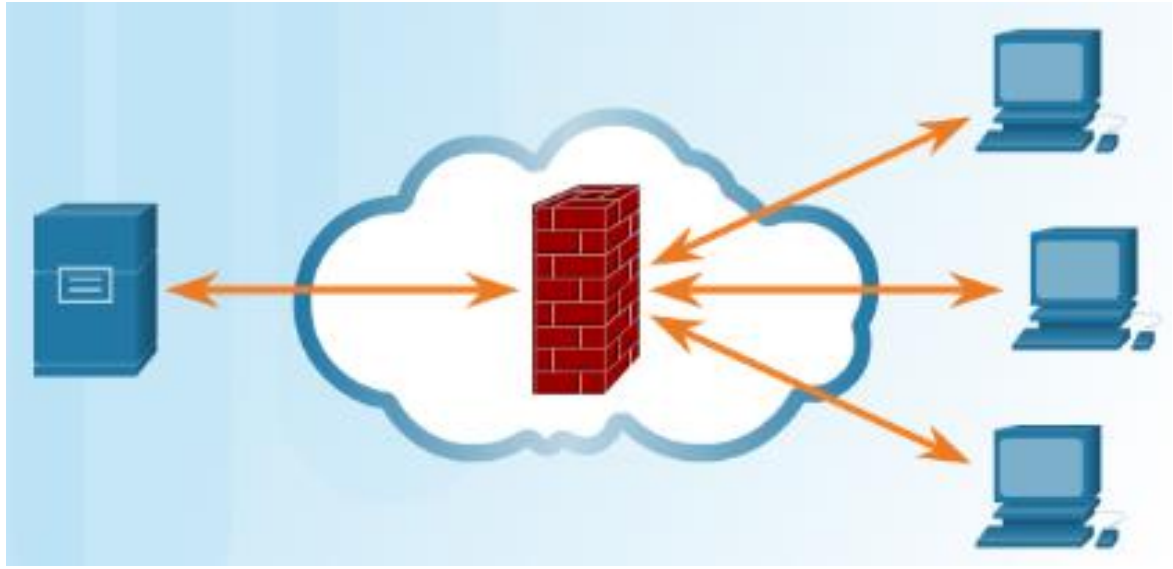
- É um mecanismo de segurança
- Consiste em uma máquina interceptando todo o tráfego de entrada e saída da rede
- Pode ser configurado para filtrar acesso da Internet para a rede interna e vice-versa – De acordo com um conjunto de regras
- Controla quais dados saem e entram na sua rede

FIREWALL

Logicamente é um filtro de pacotes.

Fisicamente é um dispositivo, como por ex um ou vários roteadores ou um computador.

- Tipos de firewall comuns
  - **Firewall de camada de rede** – endereços IP de origem e destino
  - **Firewall de camada de transporte** – portas de dados de origem e destino, estados de conexão
  - **Firewall de camada de aplicação** – aplicativo, programa ou serviço
  - **Firewall de aplicação com reconhecimento de contexto** – usuário, dispositivo, função, tipo de aplicativo e perfil de ameaça
  - **Servidor proxy** – solicitações de conteúdo da Web
  - **Servidor proxy reverso** – protege, esconde, descarrega e distribui o acesso a servidores da Web
  - **Firewall Network Address Translation (NAT)** – oculta ou disfarça os endereços privados de hosts de rede
  - **Firewall baseado em host** – filtragem de portas e chamadas de serviço do sistema em um sistema operacional de computador único



- Os equipamentos de segurança enquadram-se nestas categorias gerais:
  - **Roteadores** – podem ter muitos recursos de firewall: filtragem de tráfego, IPS, criptografia e VPN.
  - **Firewalls** – também pode ter a capacidade de roteador, gerenciamento de rede e análises avançados.
  - **IPS** – dedicado à prevenção de intrusões.
  - **VPN** – projetados para tunelamento criptografado seguro.
  - **Malware/antivírus** – o Cisco Advanced Malware Protection (AMP) vem em roteadores Cisco Next Generation, firewalls, dispositivos IPS, dispositivos de segurança da Web e e-mail e também pode ser instalado como um software em computadores.
  - **Outros dispositivos de segurança** – inclui dispositivos de segurança de Web e e-mail, dispositivos de descriptografia, servidores de controle de acesso para cliente e sistemas de gerenciamento de segurança.

POLÍTICAS DE ADOÇÃO DE REGRAS NO FIREWALL

- 1 – Nega tudo como padrão
- 2 – Permite tudo como padrão

FILTRO DE PACOTES

- Funciona na camada de rede e de transporte TCP/IP, realizando as decisões de filtragem com base nas informações do cabeçalho de pacotes.
- IP: endereço IP de origem e destino
- UDP: porta origem e destino
- TCP: porta de origem e destino

ACLS – LISTAS DE CONTROLE DE ACESSO

As ACLs podem ser classificadas em:

- ACL IP Padrão
- ACL IP Estendida
- ACL IP Nomeada
- ACL IP Numerada

ACL IP Padrão é o primeiro e mais simples tipo de bloqueio de pacotes em uma rede.

O funcionamento básico da ACL consiste em pegar o IP de origem do pacote e fazer uma avaliação com as regras existentes.

ACL PADRÃO

ACL

- Faz uma busca seqüencial na lista de acesso e uma ação é executada.
- Caso não há compatibilidade com nenhuma regra o pacote é descartado em função da regra deny any implícita no final da lista de acesso.
- A principal vantagem das listas padrão é o fato das regras serem extremamente simples.
- Apenas o endereço de origem do pacote é analisado para executar a ação de permitir ou negar que o pacote continue circulando na rede.

Em uma máscara de sub-rede, na qual o binário 1 é igual a uma correspondência e o binário 0 não é uma correspondência.
Na máscara curinga, o inverso é verdadeiro.

As máscaras curinga utilizam as seguintes regras para corresponder ao binário 1s e 0s:

- **Máscara curinga bit 0** - Corresponder ao valor do bit correspondente no endereço
- **Máscara curinga bit 1** - Ignore o valor do bit correspondente no endereço

MÁSCARA CURINGA

Máscara Curinga	Último octeto (em binário)	Significado (0 - correspondência, 1 - ignorar)
0.0.0.0	00000000	Combine todos os octetos.
0.0.0.63	00111111	• Combine os três primeiros octetos • Combine os dois restantes bits do último octeto • Ignore os últimos 6 bits
0.0.0.15	00001111	• Combine os três primeiros octetos • Combine os quatro restantes bits do último octeto • Ignore os últimos 4 bits do último octeto
0.0.0.252	11111100	• Combine os três primeiros octetos • Ignore os seis restantes mais bits do último octeto • Combine os últimos dois bits
0.0.0.255	11111111	• Combine os três primeiros octetos • Ignore o último octeto

EXEMPLO

Exemplo 1

Suponha que você desejasse uma ACE na ACL 10 para permitir o acesso a todos os usuários na rede 192.168.3.0/24. Para calcular a máscara de curinga, subtraia a máscara de sub-rede (i.e., 255.255.255.0) de 255.255.255.255, conforme mostrado na tabela.

A solução produz a máscara curinga 0.0.0.255. Portanto, a ACE seria **access-list 10 permit 192.168.3.0 0.0.0.255.**

Valor inicial	255.255.255.255
Subtrair a máscara de sub-rede	- 255.255.255. 0
Máscara curinga resultante	0. 0. 0.255

PALAVRAS-CHAVE

- **host** - Essa palavra-chave substitui a máscara 0.0.0.0. Essa máscara indica que todos os bits do endereço IPv4 precisam corresponder para filtrar apenas um endereço de host.
- **any** - Essa palavra-chave substitui a máscara 255.255.255.255. Essa máscara instrui o sistema a ignorar todo o endereço IPv4 ou a aceitar qualquer endereço.

ACL

Por exemplo, na saída do comando, duas ACLs são configuradas. A ACL 10 ACE permite apenas o host 192.168.10.10 e a ACL 11 ACE permite todos os hosts.

```
R1(config)# access-list 10 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 11 permit 0.0.0.0 255.255.255.255
R1(config)#
```

Alternativamente, as palavras-chave **host** e **any** poderiam ter sido usadas para substituir a saída realçada.

Os comandos a seguir realizam a mesma tarefa que os comandos anteriores.

```
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# access-list 11 permit any
R1(config)#
```

ACL PADRÃO E ESTENDIDA

- Existem dois tipos de ACLs IPv4:
- **ACLs padrão** - Estes permitem ou negam pacotes com base apenas no endereço IPv4 de origem.
- **ACLs estendidas** - permitem ou negam pacotes com base no endereço IPv4 de origem e endereço IPv4 de destino, tipo de protocolo, portas TCP ou UDP de origem e destino e muito mais.
- No exemplo: a ACL 10 permite hosts na rede de origem 192.168.10.0/24. Por causa da negação implícita no final ("deny any"), todo o tráfego, exceto o tráfego proveniente da rede 192.168.10.0/24, é bloqueado com esta ACL.

Por exemplo, consulte o seguinte comando ACL padrão.

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#
```

EXEMPLO ACL ESTENDIDA

No próximo exemplo, uma ACL 100 estendida permite o tráfego originado de qualquer host na rede 192.168.10.0/24 para qualquer rede IPv4 se a porta do host de destino for 80 (HTTP).

```
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)#
```

ACL NUMERADA

- ACLs número 1 a 99, ou 1300 a 1999 são ACLs padrão, enquanto ACLs número 100 a 199, ou 2000 a 2699 são ACLs estendidas, conforme mostrado na saída.

```
R1(config)# access-list ?
  <1-99> Lista de acesso padrão IP
  <100-199> Lista de acesso estendida IP
  <1100-1199> Lista estendida de acesso a endereços MAC de 48 bits
  <1300-1999> Lista de acesso padrão IP (faixa expandida)
  <200-299> Lista de acesso de código de tipo de protocolo
  <2000-2699>Lista de acesso estendido de IP (intervalo expandido)
  <700-799>Lista de acesso de endereços MAC de 48 bits
  limite de taxa Lista de acesso específica de limite de taxa simples
  modelo Ativar acls de modelo IP
Router(config)# access-list
```

ACL

A SINTAXE DO COMANDO A SEGUIR EXPLORA A ACL:

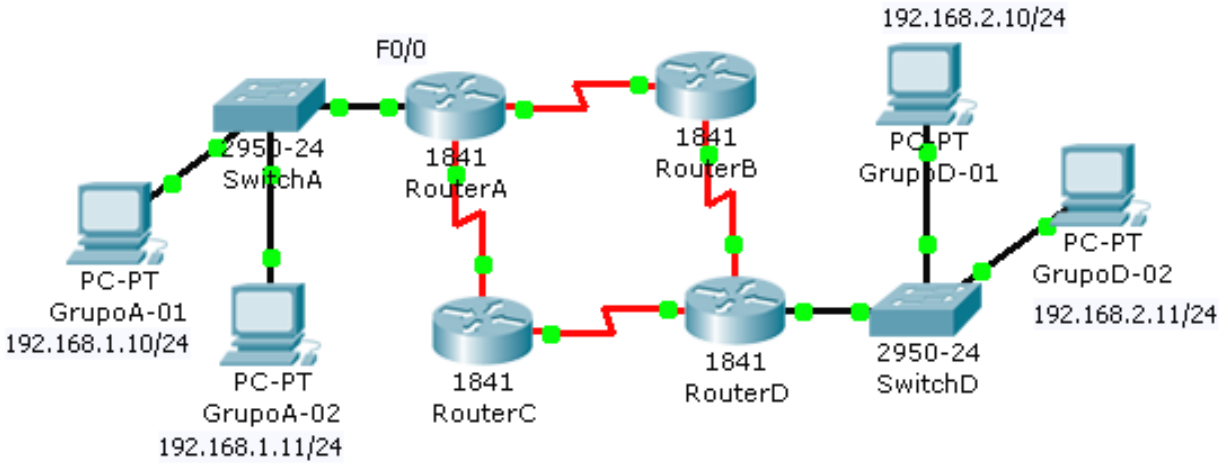
(a) comando
(b) identificação da ACL – pode ser de 1 a 99
(c) ação a ser executada quando a regra combina com o pacote
(d) endereço de origem
(e) máscara curinga(wildcards)

```
                          (a)     (b)   (c)     (d)          (e)
RouterA(config)#access-list 10 deny 192.168.1.10 0.0.0.0
```

Sintaxe ACL IP Padrão

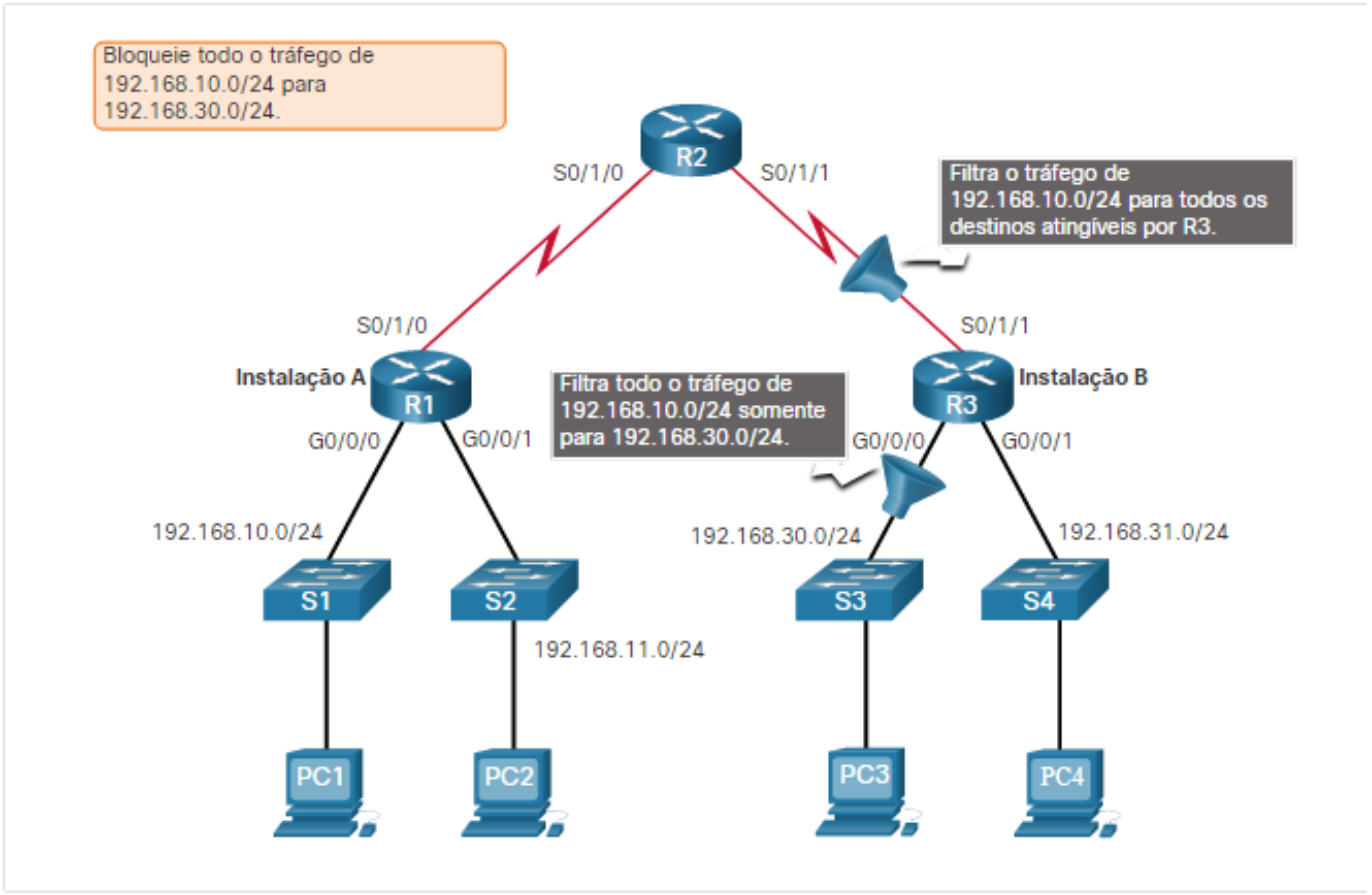
REGRA:

- RouterD>en
- RouterD#conf t
- RouterD(config)#access-list 10 deny host 192.168.1.11 0.0.0.0
- RouterD(config)#access-list 10 permit any
- RouterD(config)#int f0/0
- RouterD(config-if)#ip access-group 10 out



Aplicada a regra, o host 192.168.1.11 não tem acesso ao GrupoD.

ONDE COLOCAR A ACL?



Seguindo as diretrizes básicas de posicionamento, o administrador colocaria uma ACL padrão no roteador R3. Existem duas interfaces possíveis no R3 para aplicar a ACL padrão:

- **Interface R3 S0/1/1 (entrada)** – A ACL padrão pode ser aplicada de entrada na interface R3 S0/1/1 para negar tráfego da rede.10. No entanto, ele também filtraria o tráfego.10 para a rede 192.168.31.0/24 (.31 neste exemplo). Portanto, a ACL padrão não deve ser aplicada a essa interface.
- **Interface R3 G0/0 (saída)** – A ACL padrão pode ser aplicada de saída na interface R3 G0/0/0. Isso não afetará as outras redes acessíveis através do R3. Os pacotes da rede.10 ainda poderão alcançar a rede.31. Essa é a melhor interface para colocar a ACL padrão para atender aos requisitos de tráfego.

ONDE COLOCAR A ACL?

MELHORES PRÁTICAS DE SEGURANÇA

- **Algumas melhores práticas de segurança publicadas:**
  - **Realizar a avaliação de risco** – Saber o valor do que você está protegendo ajudará a justificar as despesas de segurança.
  - **Criar uma política de segurança** – Criar uma política que define claramente as regras da empresa, os deveres e as expectativas do trabalho.
  - **Medidas de segurança física** – Restringir o acesso a racks de rede, locais de servidor, bem como supressão de fogo.
  - **Medidas de segurança de recursos humanos** – Os antecedentes dos funcionários devem ser devidamente pesquisados.
  - **Executar e testar backups** – Fazer backups regulares e teste de recuperação de dados de backups.
  - **Manter atualizações e patches de segurança** – Atualizar regularmente o servidor e os sistemas operacionais e programas de dispositivos de rede e do cliente.
  - **Empregar controles de acesso** – Configurar funções de usuário e níveis de privilégio, bem como autenticação forte ao usuário.
  - **Testar regularmente a resposta a incidentes** – Empregar uma equipe de resposta a incidentes e testar cenários de resposta a emergências.
  - **Implementar uma rede de monitoramento, análise e ferramenta de gerenciamento** – Escolher uma solução de gerenciamento de segurança que se integra a outras tecnologias.
  - **Implementar dispositivos de segurança de rede** – Use roteadores next generation, firewalls e outros dispositivos de segurança.
  - **Implementar uma solução abrangente de segurança de endpoint** – Use software antivírus e antimalware de nível corporativo.
  - **Treinar os usuários** – Treinar os usuários e funcionários nos procedimentos de segurança.
  - **Criptografar dados** – Criptografar todos os dados confidenciais da empresa, incluindo e-mail.

LABORATÓRIO – CONFIGURAÇÃO DE FIREWALL

REFERÊNCIAS

- COMER, Douglas E. Redes de Computadores e Internet. Porto Alegre: Bookman, 2016. https://integrada.minhabiblioteca.com.br/reader/books/9788582603734/
- Cisco
- TANENBAUM, Andrew. Redes de Computadores. 5.ed. São Paulo: Campus, 2011. https://plataforma.bvirtual.com.br/Acervo/Publicacao/2610
- MORAES, Alexandre Fernandes de; Redes de computadores. -- 1. ed. -- São Paulo : Érica, 2014. https://integrada.minhabiblioteca.com.br/reader/books/9788536532981/

OBRIGADA

SILVANA.DALBO@UNISUL.BR