**Professor:** Cleber Ramos

# Segurança de Redes

## ➢ Ementa:

- ✓ Firewall
- ✓ Antivírus
- ✓ Técnicas de Criptografia
- ✓ Politicas de segurança de redes

Professor: Cleber Ramos

# Firewall

A palavra **Firewall** está constantemente relacionados à segurança de redes de computadores. Mas afinal

- O QUE É FIREWALL?
- Para que serve?
- Usar o firewall traz mais segurança para meu computador ?Preciso utilizar?
- Qual a melhor forma de utilizar?
- Onde Utilizar?
- Como  saber se meu firewall está ativo ?

- **Firewall** significa o mesmo que parede **corta-fogo** (em português), um tipo de parede, que contém o fogo em casos de incêndio.

- O conceito de **firewall** na informática é semelhante ao mecanismo de contenção de fogo.

# Conceito

- ✓ Um **FIREWALL** proporciona um meio para que as organizações criem uma camada de tal forma que elas fiquem completamente isoladas de redes externas.

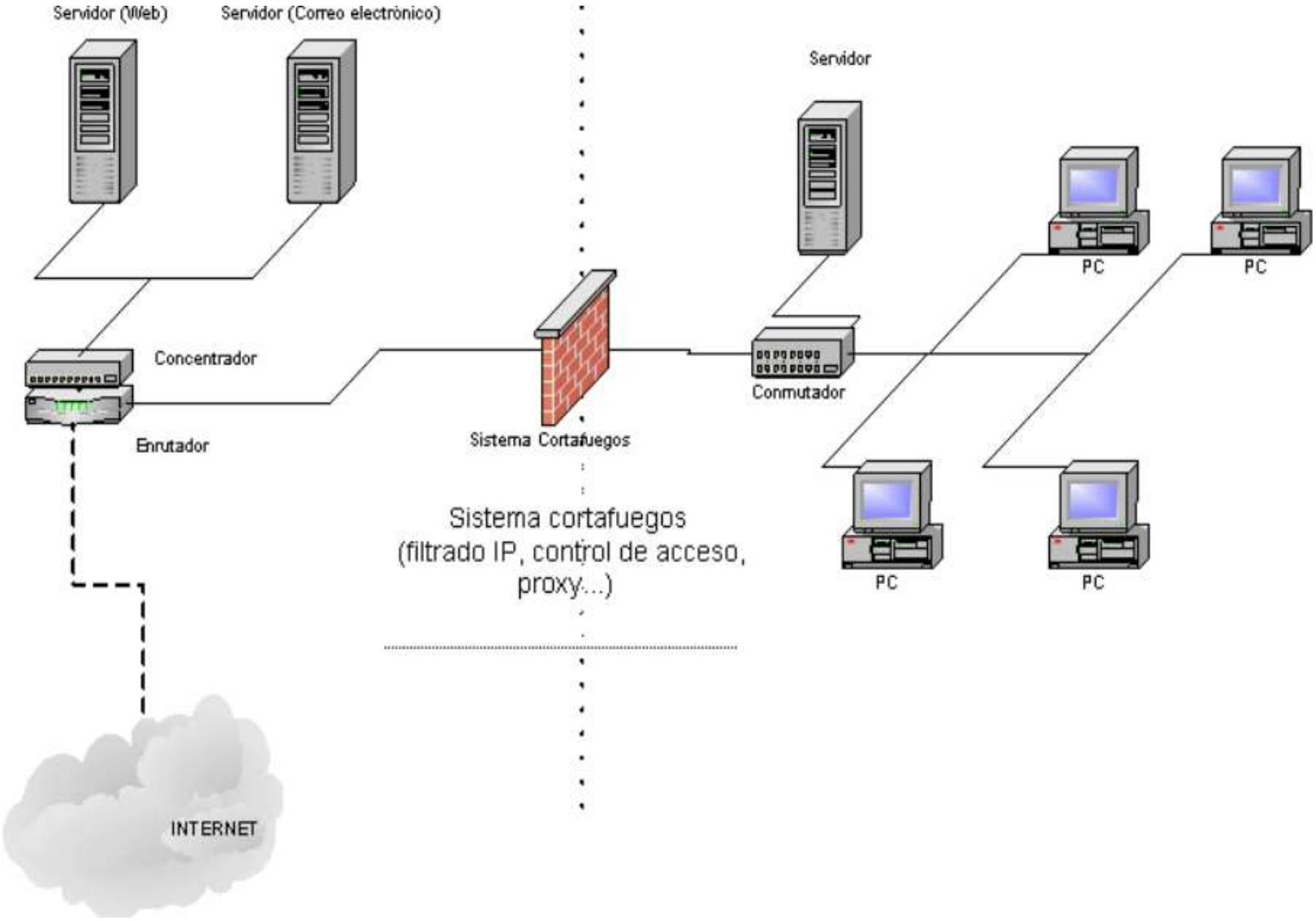
- ✓ Geralmente localizadas entre a rede interna e a rede externa de uma organização, um firewall provê uma forma de controlar o tamanho e o tipo de tráfego entre as duas redes.

Os firewalls evoluem com o passar dos anos e deixaram de ser somente um filtro de pacotes rudimentar para se tornarem sistemas sofisticados e com capacidade de filtragem cada vez mais avançados.

# Conceito

- Assim como a metáfora por trás do nome sugere, **firewall** é uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo. Em inglês, “firewall” é o nome daquelas portas antichamas usadas nas passagens para as escadarias em prédios.

**Professor: Cleber Ramos**



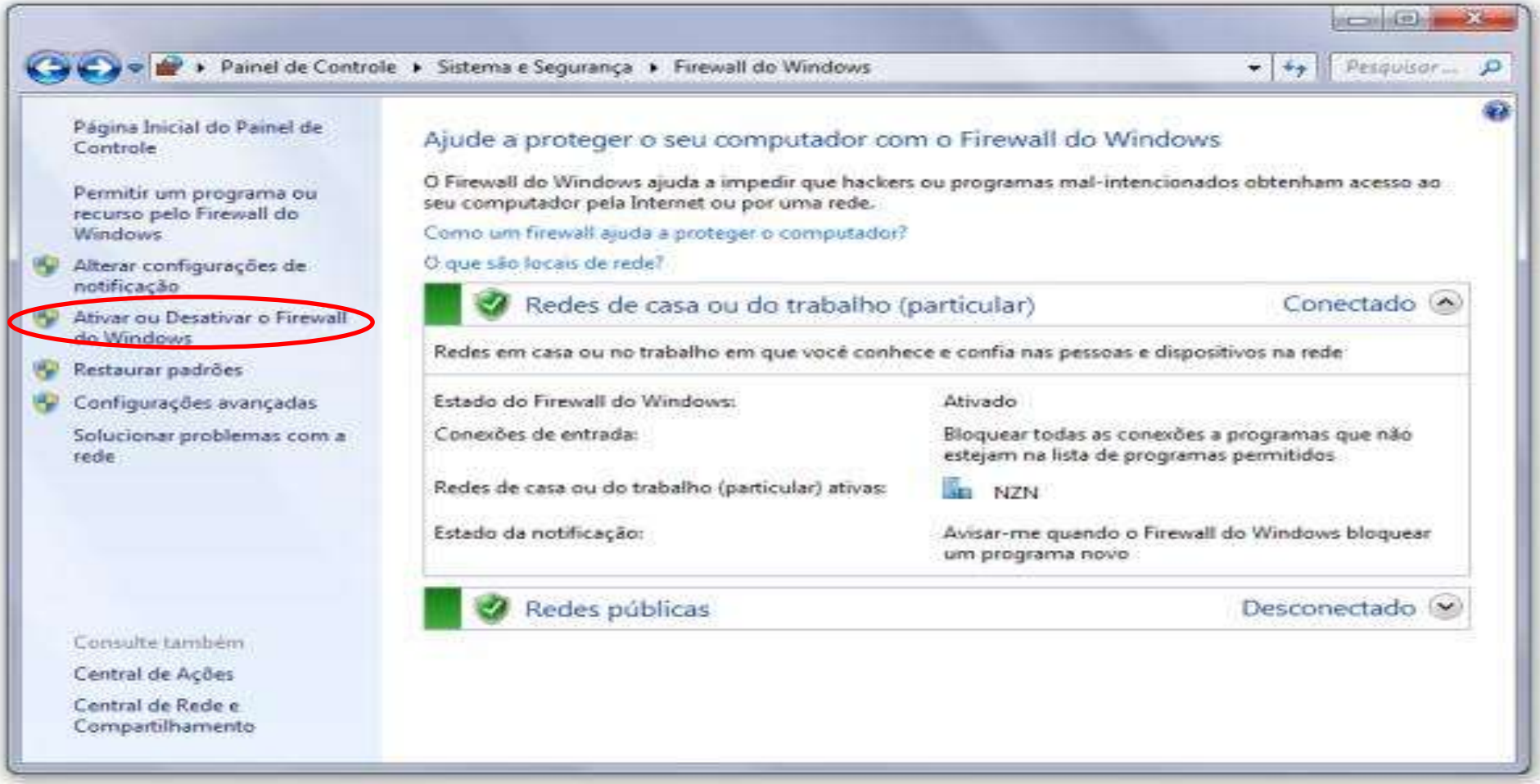

- Em informática, os firewalls são aplicativos ou equipamentos que ficam entre um **link** de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede mas também a confidencialidade deles.

# Firewall em forma de softwares

- Aplicações com a função de **firewall** já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez.

- Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final.

- Todas essas regras podem ser personalizadas à vontade, permitindo que o protocolo de segurança seja modificado de acordo com as suas necessidades. No Windows 7, você pode checar as configurações do firewall entrando em *Painel de Controle > Sistema e Segurança > Firewall do Windows*.



- Outra medida muito usada são os filtros por portas e aplicativos. Com eles, o firewall pode determinar, exatamente, quais programas do seu computador podem ter acesso ao link de internet ou não.

- As portas de comunicação também podem ser controladas da mesma forma, permitindo que as portas mais “visadas” pelos malware sejam bloqueadas terminantemente.

Boa parte dos roteadores de rede domiciliar disponíveis hoje também conta com algum tipo de aplicação de firewall. Uma das mais básicas é o controle sobre os computadores que estejam habilitados a se conectar na rede, impedindo que as “sanguessugas” de plantão usem a sua Wi-Fi sem permissão.

# Firewall como hardware

- Os firewalls em forma de **HARDWARE** são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais.

- A vantagem de usar equipamentos desse tipo é que o hardware é dedicado em vez de compartilhar recursos com outros aplicativos.

- Dessa forma, o firewall pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

Equipamentos de firewall empresariais (Fonte da imagem: Reprodução/eHow)

# Como o Firewall Funciona?

- Com a chegada da internet banda larga, com conexões cada vez mais rápidas, ficou mais fácil para os usuários navegarem, se comunicarem, compartilharem informações, bem como realizar infinitas tarefas diferentes, de forma muito mais rápida do que nas antigas linhas discadas.

Entretanto, nem tudo são flores, pois com os benefícios também chegaram novos tipos de ameaças. A disseminação de vírus, os ataques de hackers a todo tipo de máquina, seja pessoal ou corporativa, estão maiores do que nunca.

- Para não nos tornarmos vítimas de ataques desse tipo de malfeitor, existem diversos programas e ferramentas que se propõem a defender o sistema, mantê-lo funcionando e imunizá-lo através de várias técnicas diferentes.

- Uma dessas técnicas é a utilizada pelo que conhecemos como Firewall.

# Lacrando portas e janelas

- ✓ Para que ladrões não entrem em sua casa, você deve trancar suas portas e janelas, ou instalar grades, alarmes e sistemas de segurança, dificultando o acesso ao interior do imóvel.
- ✓ O Firewall tem função similar, pois **"TRANCA"** todas as portas e janelas do seu computador para que só os autorizados possam entrar e sair.
- ✓ Os Firewalls já são instalados com predefinições de quais portas poderão permanecer abertas para que os programas as usem, mas o usuário pode adicionar permissões conforme a necessidade.

# OBSERVAÇÃO

- O Firewall não dispensa a instalação de um antivírus. Ele funciona como uma alfândega ou filtro que restringe a passagem dos dados recebidos e enviados pelo seu computador.

- O antivírus é necessário porque mesmo as comunicações consideradas seguras pelo Firewall podem trazer ameaças à máquina, geralmente devido à operação incorreta do PC pelo usuário.

# Qual utilizar ?

- Dependendo do tipo de conexão usada no computador, é possível usar dois tipos de firewall, um por hardware e/ou outro por software. Atualmente, os firewalls por hardware mais utilizados são os que já vêm incorporados aos roteadores e modems de banda larga.

- O Windows já vem com um firewall nativo, mas você pode desativá-lo e instalar ferramentas mais robustas, com mais opções de configuração e segurança

# Quando utilizar o Firewall de Hardware?

- A maior vantagem de usar um firewall por hardware é quando sua rede possui mais de um computador.

- Todas as máquinas estarão ligadas ao mesmo roteador, que além de gerenciar as conexões, também poderá executar a função de firewall — logicamente, isso dependerá do modelo de roteador utilizado.

- Verifique esta informação antes de comprar qualquer equipamento. Prefira roteadores que já venham com firewall, para aumentar a segurança das máquinas da rede.

- **Importante:** por mais que você ainda utilize uma conexão discada para se conectar à internet, é imprescindível que seja ativado um software firewall no seu computador, pois nenhum tipo de conexão é seguro sem a proteção do firewall.

- Tanto o **firewall** por hardware como o por software operam de maneira similar. Conforme a configuração definida pelo usuário, o firewall compara os dados recebidos com as diretivas de segurança e libera ou bloqueia os pacotes.

- Para ilustrar o funcionamento, podemos pensar no firewall como uma sacola de compras. Digamos que você é a conexão com a internet e as sacolas de compras são os dados. Considere a sua lista de compras como a lista de permissões do firewall. Ela contém os itens “refrigerante”, “frutas” e “pão”.

- No seu computador, o firewall bloqueará a passagem de qualquer item que seja diferente de “refrigerante”, “frutas” e “pão”, retirando da sacola de compras e deixando passar os que estão na lista de permissões. Daí a importância de configurar corretamente seu firewall, pois se você incluir “rato” ou “barata” nas permissões, seu firewall não os bloqueará.

- Assim como qualquer outra solução de segurança, o firewall não é 100% eficiente, já que existem estudiosos especializados em quebrar essa segurança.

- Hackers mais experientes são capazes de “disfarçar” uma “barata” na pele de um “refrigerante”, conseguindo que os dados passem pela “alfândega” do firewall e, em seguida, ganhando acesso à sua máquina.

# Devo usar firewall por hardware ou por software?

- A resposta para essa pergunta é polêmica, pois muitos têm a opinião de que só um dos dois já é suficiente, mais que isso é exagero, mas o ideal é possuir um firewall por hardware **E** um por software.

- Se você tiver somente um firewall por software e executar um programa malicioso que baixou da internet, tal programa poderá ser capaz de automaticamente reconfigurar seu firewall para aceitar as conexões maliciosas.

já com o firewall por hardware isso não é possível, pois mesmo que sua máquina esteja contaminada, será impossível que o software do computador afete um hardware externo a ele e de funcionamento independente — como os roteadores e modems de banda larga.

# Porque eu preciso de antivírus, mesmo com firewall?

- o firewall funciona como um filtro de conexões, impedindo que sejam enviados e recebidos dados — maliciosos ou não — pelas portas que o firewall estiver bloqueando.

- Porém, as portas utilizadas pelo seu navegador de internet ou programa de e-mail, por exemplo, são sempre liberadas por padrão.

- Ou seja, mensagens de spam, sites com conteúdo malicioso ou mesmo downloads não são protegidos pelo firewall, já que trafegam através de portas liberadas.

- Portanto, nenhum firewall substitui software antivírus, muito menos dispensa uma boa política de uso e educação por parte do usuário, no sentido de não executar programas suspeitos, não abrir e-mails de fontes desconhecidas e não fazer downloads de programas piratas — que costumam ser belas fontes de contaminação por vírus.

# Resumindo...

## O que o firewall faz?

- ✓ Impede que sua máquina seja invadida.
- ✓ Impede que dados indesejáveis entrem no PC.
- ✓ Bloqueia o envio de dados provenientes da sua máquina que não estejam especificados nas configurações.

# Resumindo...

## ➢ O que o firewall NÃO faz?

- ❖ Não protege contra programas baixados pelo usuário.
- ❖ Não impede que programas de e-mail baixem spam.
- ❖ Não impede que o usuário crie exceções errôneas que podem colocar o computador em risco.

# DICAS

A melhor maneira de manter seu computador protegido é configurar o firewall para que ele bloqueie tudo! Pode parecer um pouco drástico, mas esse é só o primeiro passo. Se você bloquear tudo, obviamente nada vai funcionar, mas você poderá obter um controle maior das permissões de tráfego se for liberando manualmente somente os programas que você quer que realmente tenham acesso à internet e possam enviar e receber informações

Se você não sabe ao certo como configurar seu firewall, seja ele por software ou hardware, NÃO utilize o método das tentativas, pois isso pode colocar seu computador em grande risco, causando perda de dados, tráfego de informações indevidas e grandes dores de cabeça. Prefira pedir ajuda para alguém que entende um pouco mais do assunto.

# Qual a utilidade em instalar um firewall pessoal

Os antivírus não são capazes de detectar tentativas de acesso ao computador por meio de um backdoor.

Desde que bem configurado, um firewall não só detecta, como impede o acesso de programas e pessoas ao seu computador.

# BACKDOOR.

- ✓ Também conhecido por **Porta dos fundos**, é uma falha de segurança que pode existir em um programa de computador ou sistema operacional, que pode permitir a invasão do sistema por um cracker para que ele possa obter um total controle da máquina.

- ✓ Muitos crackers utilizam-se de um **Backdoor** para instalar vírus de computador ou outros programas maliciosos, conhecidos como malware.

- ✓ Por isso que muitas vezes, ao instalar um firewall, é preciso liberar os programas que você usa e algumas portas de comunicação.

- ✓ Outra característica importante dos firewalls é a capacidade que eles têm de identificar as origens das tentativas de invasões e exibi-las ao usuário, o que permite o bloqueio da porta ou do IP utilizado.

# O que difere um firewall do outro?

- A função principal do firewall, que é bloquear portas, todos eles fazem.
- Uma das diferenças está no número de portas que um e outro “protegem”.
- Alguns aplicativos cobrem uma quantidade muito grande de portas e, por isso, detectam mais invasões.

- Outros ficam de olho apenas naquelas mais usadas e, por isso, às vezes deixam passar alguma coisa.

- Outra diferença entre um aplicativo e outro é a quantidade de ferramentas auxiliares que eles oferecem e, claro, a interface de uso.

- De nada adianta um firewall cheio de opções se você precisa chamar uma equipe de cientistas para aprender a mexer, certo?

- Quanto mais intuitivo o programa for, maiores são as chances de você configurá-lo corretamente e, consequentemente, mais eficiente ele se torna.

Professor: Cleber Ramos

# Qual a diferenças entre antivírus, antispyware e firewall

# Filtro de pacote

- Os mecanismos de filtragem implementados por roteadores possibilita que se controle o tipo de trafego de rede existente em qualquer seguimento de rede. Consequentemente pode se controlar os tipos de serviços que podem existir no seguimento de rede. Serviços que comprometem a segurança da rede podem, portanto, ser restringidos.

- É importante estarmos cientes de que um filtro de pacote não se encarrega de examinar nenhum **protocolo** de nível superior ao de **TRANSPORTE**, como por exemplo o nível de aplicação, que fica a cargo dos proxy servers. Portanto, qualquer falha de segurança no nível da aplicação, não pode ser evitada utilizando somente um filtro de pacotes.

# Estratégias de segurança

- Menos Privilégio **(Least Privilege)** : O principio desta estratégia significa que qualquer objeto (usuário, administrador, sistema, etc.) deveria ter somente os privilégios realmente necessários para cumprimento de suas tarefas. Mínimo privilégio é um principio importante para limitar a exposição aos ataques e danos causados por estes.

➢ Principais problemas envolvidos à estratégia do privilegio mínimo:

✓ 1) Pode ser complexo de implementar 1113 caso os programas e/ou protocolos não permitam estabelecer privilégios.

✓ 2) Pode-se acabar implementando algo que tenha menos privilégios do que o mínimo estabelecido.

# Defesa em profundidade (*Defense* in depth)

- Este principio determina que não se deve depender de apenas um mecanismo de segurança, não importando quão forte ele pareça ser.
- Ao invés disso, recomenda-se que sejam utilizados múltiplos mecanismos de segurança e que estes estejam configurados no nível mais alto possível de tolerância a falhas e redundância.

# Perguntas Frequentes

- **Quais são as configurações recomendadas para o Windows Firewall?**
- Recomendam as configurações padrão do firewall:

✓ O firewall está ligado.

✓ O firewall está ativado para todos os locais da rede (Casa ou trabalho, Lugar público, ou Domínio).

✓ O firewall está ativado para todas as conexões de rede.

✓ O firewall bloqueia as conexões recebidas que não coincidem com uma exceção.

# Quais são algumas das coisas que um firewall não pode impedir?

✓ **Vírus de e-mail**

- Os vírus de e-mail são anexados às mensagens de e-mail. O firewall não pode determinar o conteúdo da mensagem e, portanto, não pode protegê-lo contra esses tipos de vírus.

- Você deve possui um programa antivírus, não deve abrir um anexo de e-mail se não estiver completamente certo de que ele é seguro.

✓ **Golpes de Phishing**

- Phishing é uma técnica usada para induzir usuários de computador a revelar informações pessoais ou financeiras, como uma senha de conta bancária.

- O phishing começa com um e-mail recebido aparentemente de uma fonte confiável, mas que na verdade direciona os destinatários para que forneçam informações a um site fraudulento. O firewall não pode determinar o conteúdo da mensagem e, portanto, não pode protegê-lo contra esses tipos de vírus.

# Posso usar mais de um firewall no meu computador?

- Sim, mas a execução de mais de um programa de firewall ao mesmo tempo pode causar conflitos. É melhor usar apenas um programa de firewall.

**Se eu tiver um roteador com um firewall incorporado, devo ativar também o Firewall do Windows?**

- Sim, porque os firewalls baseados em HARDWARES fornecem apenas proteção aos computadores na Internet, não aos PCs em sua rede doméstica.

- **POR EXEMPLO**, se um computador portátil ou convidado for conectado a uma outra rede, poderá ser infectado por um worm de computador e, quando for conectado à sua rede doméstica, seu firewall baseado em roteador não conseguirá impedir a disseminação do worm.

- Entretanto, um firewall executado em cada computador de sua rede poderá ajudar a controlar a disseminação de worms.

# PARA CONCLUIR

- A melhor maneira de encontrar o firewall que se “encaixa” ao seu perfil é testando alguns:
- ZoneAlarm Free
- Sygate Personal Firewall
- Comodo Personal Firewall
- Comodo Firewall Pro
- Ashampoo FireWall

Professor: Cleber Ramos

# Agendador de pacotes do Windows

# QoS

- Exexutar>gpedit.msc>
- Modelos Administrativos>
- Rede>
- Agendador de pacotes QoS dê dois cliques em "Limitar largura de banda reservável" deixe em "Ativado" e coloque 0 %.