SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Proteção à rede

- A proteção de uma empresa é feita com o uso de mecanismos de segurança tecnológicos, físicos, processuais e regulatórios. É com a sua implementação que as finalidades de prevenção, detecção e resposta a incidentes são cumpridas.

- A rede de uma empresa é um dos escopos que devem ser protegidos, representando informações em meio digital que existem principalmente em transmissão.

Proteção à rede

- O desafio de proteção à rede é ainda maior porque é pela rede que informações digitais armazenadas em servidores podem ser acessadas. Assim, uma organização básica para a proteção à rede envolve:
  - Proteção de informações que trafegam pela rede: exemplo são configurações ou tecnologias específicas que limitem o número de determinados tipos de conexões e evitem ataques de negação de serviço (DoS).
  - Proteção contra acesso a informações armazenadas em servidores: limitar o acesso a essas informações por meio de alguns controles principais: autenticação (nos níveis de rede e de usuário), controle de acesso de rede, como o firewall, sistema de detecção de intrusão (IDS) e sistema de prevenção de intrusão (IPS).

Proteção à rede

- Proteção contra o acesso de usuários contaminados com malware ou contra a contaminação dos servidores com malwares: usuários legítimos que tenham suas credenciais roubadas podem dar o acesso indevido a uma rede, ou os usuários podem acessar informações de uma forma legítima, mas, caso estejam contaminados com malwares, acabam comprometendo a rede. Alguns dos principais controles de segurança: antivírus, antimalware, DLP, IDS, IPS.

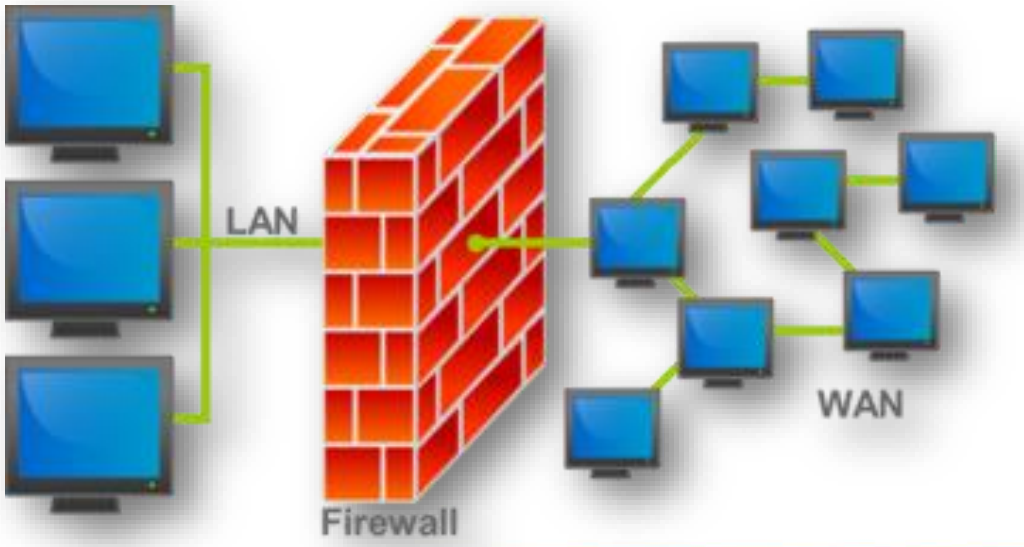
Firewall

- O firewall é um dos mais conhecidos controles de segurança da informação, surgindo juntamente com a própria internet. Os primeiros firewalls foram implementados em roteadores, no final da década de 1980, por serem os pontos de ligação natural entre duas redes. As regras de filtragem dos roteadores, conhecidas também como “listas de controle de acesso” (Access Control List, ACL), tinham como base decisões do tipo “permitir” ou “descartar” os pacotes, que eram tomadas de acordo com a origem, o destino e o tipo das conexões.

- O firewall é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, pelo qual deve passar todo o tráfego, permitindo que o controle, a autenticação e os registros de tráfego sejam realizados. Assim, esse ponto único constitui um mecanismo utilizado geralmente para proteger uma rede confiável de uma rede pública não confiável.

Firewall

- Um ***firewall*** (Parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Pode ser do tipo filtros de pacotes, *proxy* de aplicações, etc.
- O termo em inglês faz uma alusão comparativa à função que o sistema desempenha a fim de evitar o alastramento de dados nocivos dentro de uma rede de computadores, da mesma forma que uma parede o alastramento de incêndios pelos cômodos.



Firewall

- Os sistemas *firewall* nasceram no final dos anos 80, fruto da necessidade de criar restrição de acesso entre as redes existentes, com políticas de segurança no conjunto de protocolos TCP/IP.

- Nesta época a expansão das redes acadêmicas e militares, que culminou com a formação da ARPANET e, posteriormente, a Internet e a popularização dos primeiros computadores tornando-se alvos fáceis para a incipiente comunidade ***hacker***.

Firewall

- Este dispositivo de segurança existe na forma de *software* e de *hardware*, a combinação de ambos é chamado tecnicamente de "appliance" . A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

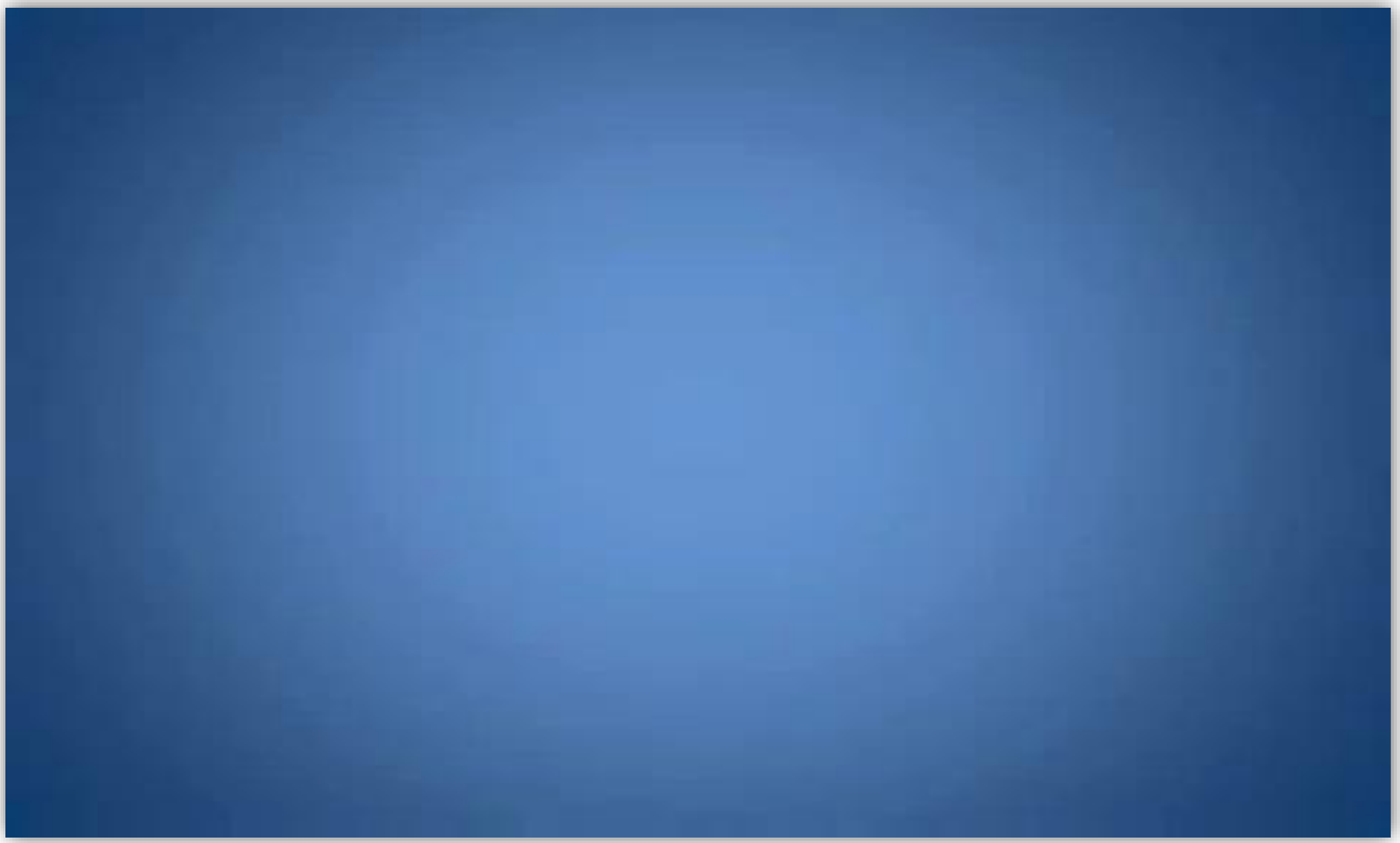
- Existem dois tipos de Firewall: **Firewall de Borda** e **Firewall Pessoal**.
- Os firewalls de borda são aqueles que protegem a rede local inteira.
- Os firewalls pessoais são aqueles que protegem sua própria máquina.

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.
- Assim sendo nada que estiver proibido em sua lista vai poder entrar ou sair da rede.

- Como um firewall não pode simplesmente fechar todas as portas - pois o computador perderia sua utilidade -, o administrador dele fica responsável por determinar quais poderão ficar abertas. Com isso, ele irá capturar todas as informações que entram ou saem da rede e irá liberar ou bloquear os pacotes (conjunto de informações) somente depois de comparar os dados com as diretivas de segurança.

Firewall



Firewall

- Basicamente, o firewall controla as conexões de quem pode acessar qual serviço da rede que está sendo protegida. As regras do firewall que definem esse controle utilizam tradicionalmente dois pares de informações: endereço IP e porta TCP/UDP de origem do acesso, e endereço IP e porta TCP/UDP de destino. Este tipo de firewall é o filtro de pacotes.

- Regras que permitem que usuários internos acessem páginas web que funcionem na porta TCP 80.

Regra	End. de Origem: Porta de Origem	End. de Destino: Porta de Destino	Ação
1	IP da rede interna: porta alta	Qualquer endereço: 80 (HTTP)	Permitir
2	Qualquer endereço: 80 (HTTP)	IP da rede interna: porta alta	Permitir
3	Qualquer endereço: qualquer porta	Qualquer endereço: qualquer porta	Negar

Firewall

- A primeira informação na imagem é que a regra 1 é a requisição, enquanto a regra 2 é a resposta. A regra 3 utiliza um conceito importante: negação de todas as outras conexões.

- Outro ponto importante sobre firewalls é que eles trabalham de uma forma sequencial com suas regras, ou seja, o firewall vai analisando todas as regras existentes consecutivamente, até que uma delas seja verdadeira e a conexão possa seguir em frente ou ser negada. No caso da regra ser do tipo “permitir”, a conexão segue adiante. Se for do tipo “negar”, a conexão é encerrada.

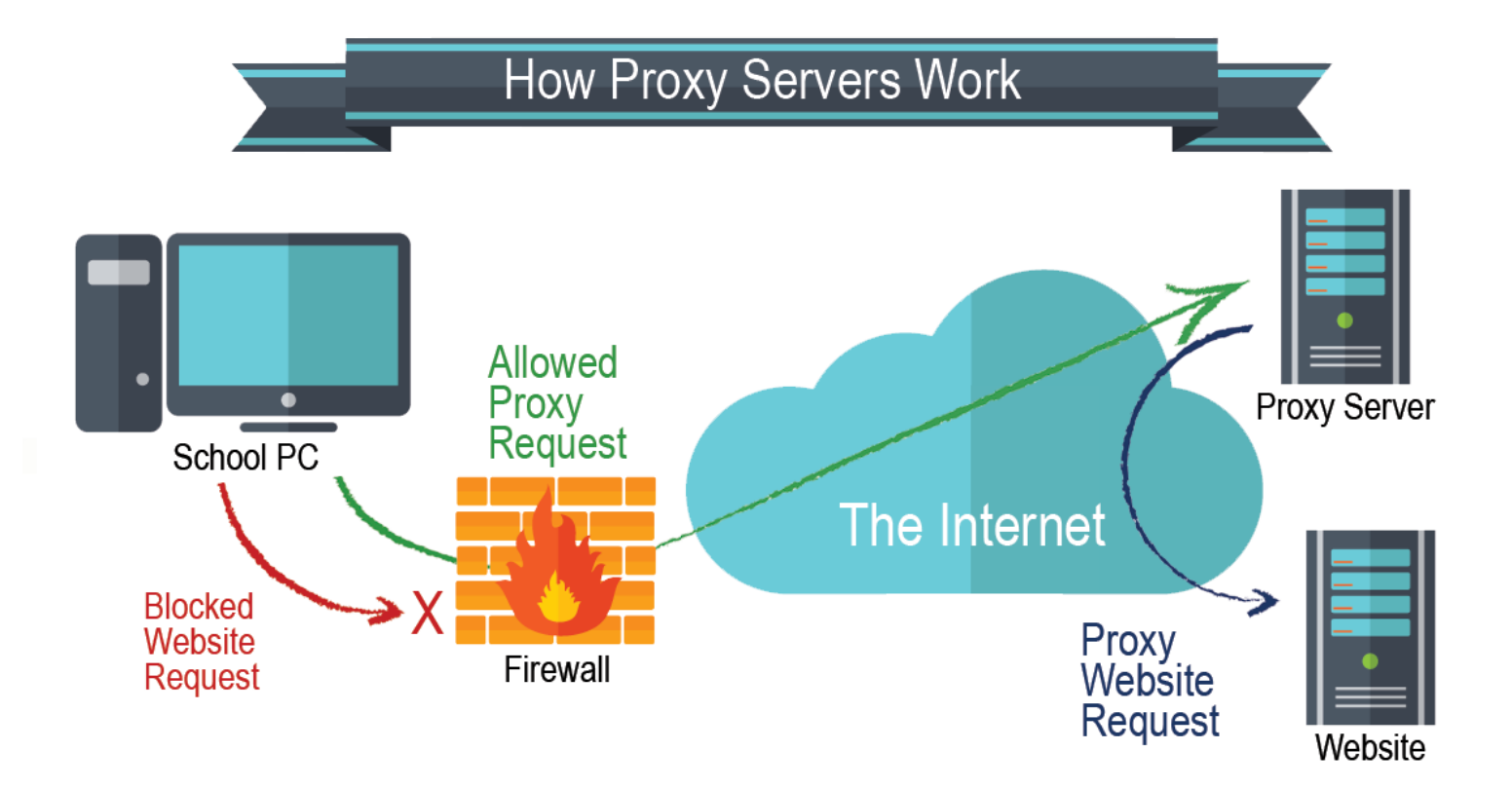
Firewall

- Os firewalls podem atuar ainda no nível de aplicação, o que permite que dados de protocolos como o HTTP, utilizado na web, possam ser analisados. A partir dessa análise, é possível realizar algumas tarefas, como a filtragem de conteúdo, por exemplo. Outra funcionalidade de um firewall que atua no nível de aplicação é o proxy.

- O Proxy é um servidor intermediário que atende a requisições repassando os dados do cliente à frente: um usuário (cliente) conecta-se a um servidor *proxy*, requisitando algum serviço, como um arquivo, conexão, página *web*, ou qualquer outro recurso disponível no outro servidor.

Firewall

- Um servidor proxy geralmente trabalha junto ou no mesmo equipamento que um firewall, sua função além intermediar a conexão também é definir quais sites as máquinas ou usuários podem acessar.



Firewall

- Os proxies ajudam também na aceleração do acesso à internet no caso de empresas que precisam de velocidade na hora de navegar. O registro da página acessada fica guardado na sua cache. Com este arquivo já gravado, o próximo acesso fica muito mais rápido uma vez que não será necessário refazer o primeiro reconhecimento do destino.

ATIVIDADE

- INSTALAR O PFSENSE.

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera