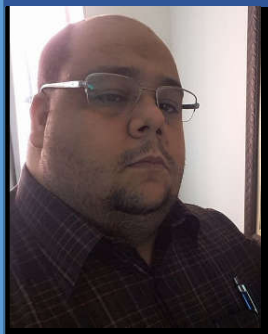
Local: Ceet Vasco Coutinho
Data: 08 de abril de 2017
Hora: 09:00h às 17:00h

Festival Latino Americano de Instalação de Software Livre

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL & PROXY WEB



PALESTRANTE: THIAGO PORTUGAL SOLEDADE

TEMA: A Importância do Firewall e Proxy no Ambiente Corporativo

- Pós Graduando em Cybercrime e Cybersegurança
- Graduando de Direito
- Graduado em Redes de Computadores
- Pós Graduado em Informática em Educação
- Instrutor & Palestrante;
- Consultor de Tecnologias (Projetos de Infra e Seg.)
- Entusiasta da Computação Forense
- Entusiasta e Pesquisador do Direito Digital
- Entusiasta e Pesquisador da Segurança da Informação

Contatos:
Celular: (27) 99840-8613
E-mail: thiagoportugal@yahoo.com.br

Thiago Portugal Soledade
Analista e Consultor de TI

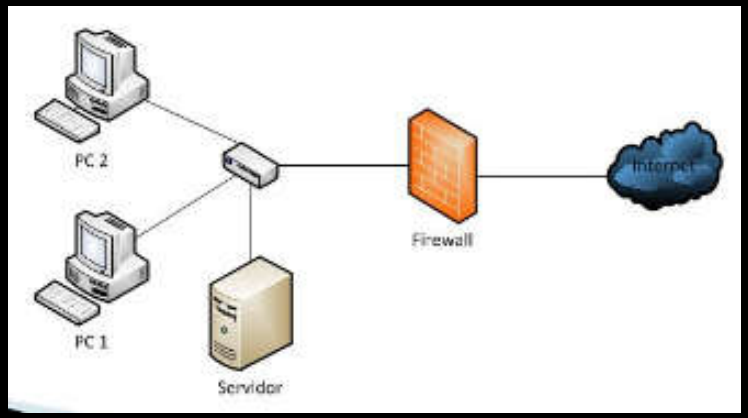
SUMÁRIO

Festival Latino Americano de Instalação de Software Livre

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **FINALIDADE**
  - É uma combinação de hardware e software que isola a rede local de uma organização da internet;
  - Implementação de políticas de controle de acesso, bloqueando ou permitindo a passagem de pacotes;



Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **CARACTERÍSTICAS**

  - Pelo firewall devem passar todos os pacotes que chegam ou saem de uma rede.
  - O firewall deve prover ferramentas para registro e monitoramento do tráfego, como logs e envios de alertas.
  - Características secundárias:
    - Implementação de serviços como NAT e VPN;
    - Realização de auditorias; e
    - Geração de estatísticas do uso da rede.

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **CARACTERÍSTICAS**

NAT – NETWORK ADDRESS TRANSLATIONS

- Conversão de endereços privados para endereços públicos:
  - As máquinas internas utilizam endereços privados
- Esconde a topologia interna da rede:
  - Isola as máquinas da rede interna.
- O gateway faz a tradução de endereços;
  - Qual o verdadeiro papel do GW?

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **TIPOS DE FIREWALL**

Firewalls de filtragem de pacotes: Este tipo de firewall toma as decisões baseadas nos parâmetros do pacote, como porta/endereço de origem/destino, estado da conexão, e outros parâmetros do pacote. O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT).

O **NetFilter** é um excelente firewall que se encaixa nesta categoria.

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **TIPOS DE FIREWALL**

  - **Firewalls de camada de aplicação:** Firewalls deste tipo são mais intrusivos e permitem um controle relacionado com o conteúdo do tráfego. Alguns firewalls em nível de aplicação combinam recursos básicos existentes em firewalls de filtragem de pacotes combinando as funcionalidade de controle de tráfego/controle de acesso em uma só ferramenta.

Obs: Os dois podem ser usados conjuntamente

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **TIPOS DE FIREWALL**

- Firewalls de filtragem de pacotes:

- Aplica sequencialmente uma série de regras de filtragem aos pacotes e então encaminha ou descarta os mesmos;
- As regras são baseadas nas informações contidas nos cabeçalhos dos pacotes:
  - Endereço IP de origem;
  - Endereço IP de destino;
  - Interface de rede;
  - Protocolos (TCP, UDP, ICMP, …)

Em geral, são implementados junto com o processo de roteamento;

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL

- **PROTEÇÃO**
  - **O QUE PROTEGER?**
    - SERVIÇOS (Quais proteger).
    - CONEXÕES (Liberar ou Bloquear).
    - ACESSOS (Máquinas ou Grupos).
    - PRIORIDADES (acesso e Processamento).
    - BLACKLISTS E WHITELIST.
    - Etc…

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL do GNU/Linux

- **NETFILTER**
  - O NETFILTER é o firewall que o GNU/Linux usa desde seu Kernel 2.4.x;
  - O IPTABLES é a ferramenta para configuração do NETFILTER, ou seja, é o programa de linha de comando usado pelo usuário para configurar o conjunto de regras de filtragem de pacotes Linux 2.4.x e posterior.

O iptables utiliza os conceitos de:

- Cadeias (chains)
- Tabelas (Tables)
- Regras (rules)

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL do GNU/Linux

- **NETFILTER/IPTABLES**

Informações

- As regras são comandos (como bloquear ou deixar passar um pacote).
- As regras são armazenadas dentro dos **chains** e processadas na ordem que são inseridas e armazenadas no Kernel.
- Criar um ShellScript de inicialização.

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL do GNU/Linux

- **NETFILTER/IPTABLES**
  - O Netfilter Iptables funciona como um interpretador de código, varrendo o seu texto/script linha a linha.
  - Sempre a primeira regra irá prevalecer, uma vez que ela for lida, exemplo:

```
#iptables -A INPUT -p tcp --dport 80 -j ACCEPT
#iptables -A INPUT -p tcp --dport 80 -j REJECT
#iptables -A INPUT -p tcp --dport 80 -j DROP
```

No exemplo acima, temos aparentemente três regras bem parecidas, a primeira regra libera, a segunda rejeita e a terceira nega o acesso. De acordo com o explicado: "A primeira regra lida terá privilégios", temos então o acesso a porta 80 liberado, mesmo rejeitando e negando o acesso nas regras subsequentes.

Thiago Portugal Soledade
Analista e Consultor de TI

PROXY WEB

- **PROXY WEB (finalidades, características e listas)**
  - **Firewalls de camada de aplicação: Também conhecidos como servidores proxy. Ex: Squid**

- Age como um intermediário das conexões em nível de aplicação;
- Apesar de poderem ser implementados para qualquer aplicação, historicamente são utilizados para os serviços de HTTP e FTP.
- Não protegem o sistema operacional da própria máquina;
- Desempenho inferior ao de filtro de pacotes;
- Função principal é o cache;
- Também realiza o controle de acesso a páginas (Regras e Políticas);

Contatos:
Celular: (27) 99840-8613
E-mail: thiagoportugal@yahoo.com.br

Festival Latino Americano de Instalação de Software Livre

Thiago Portugal Soledade
Analista e Consultor de TI

FIREWALL & PROXY WEB

AGRADECIMENTOS:

- Agradeço a Deus por estar aqui compartilhando com os colegas o conhecimento adquirido.
- Agradeço ao envolvidos no evento.
- Agradeço Amigos, Colegas e Mestres que contribuíram e contribuem para cultura do Software Livre