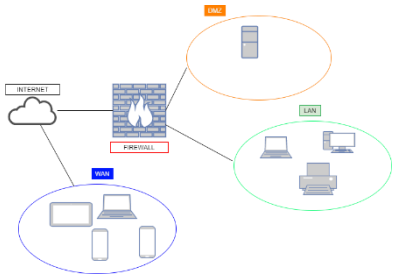
NETWORK SYSTEMS



I. INTRODUCTION

Neste trabalho foi nos proposto que realizássemos uma investigação com vista a encontrar soluções na implementação de firewall físicas e a necessidade de garantir a segurança de redes e sistemas em ambientes empresariais, instalando e configurando uma firewall.

Criámos um cenário parecido a de uma empresa, criando uma rede WAN que é uma rede pública com acesso ilimitado, sem proteção de uma firewall. Criamos uma rede LAN, que é uma rede privada com objetivo de lhe implementar uma firewall para proteção. Por fim, criamos também uma rede DMZ que é configurada com equipamentos de firewall, que vão realizar um acesso entre uma rede local, a internet e a DMZ.

A. *Abbreviations and Acronyms*

LAN - Este termo geralmente refere se a redes de computadores restritas como por exemplo uma casa, escritórios, entre outros. Uma rede sem fio de uma empresa também faz parte da LAN. O que realmente limita a rede LAN é uma faixa de IP restrita à mesma, com uma máscara de rede comum.

WAN - Significa uma rede que cobre uma grande área física, como um shopping, uma cidade, ou até mesmo um país. As redes WAN tornaram-se necessárias pois grandes empresas com milhares de computadores precisavam de trafegar grande quantidade de informações em diferentes localidades geográficas.

IPFIRE - A distribuição Linux IPFIRE permite implementar facilmente serviços de firewall, proxy, file server, VPN e outros serviços de rede. O IPFIRE pode ser instalado numa máquina ou executado a partir de um CD ou dispositivo de armazenamento USB e é direccionado para redes de dados de empresas ou para redes domésticas. O IPFIRE disponibiliza uma interface bastante amigável para o utilizador, onde é possível realizar as configurações.

DHCP - é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente.

B. *Realization*

- Começamos individualmente por idealizar o cenário para a realização da nossa rede, discutimos alguns pontos positivos e alguns pontos negativos, discutimos o número de cenários possíveis e algumas soluções para estes, tendo acabado por optar pelo um cenário realizado por ambos os membros do grupo. Construímos uma rede LAN, constituída por um portátil, um computador fixo, e um fax. Na rede DMZ colocamos um server. Ambas as redes LAN e DMZ estão protegidas por uma firewall através do IPFIRE. Colocamos também uma rede WAN, estando esta não protegida pela firewall.
- Utilizamos o IPFIRE para configurar as interfaces (red, orange, blue, green). As placas de rede da máquina do Windows7 foram configuradas conforme as interfaces do IPFIRE. Foi atribuído um IP à máquina Windows7 através do DHCP. Para configurar a firewall deste cenário foi preciso aceder ao browser e neste configurou-se as opções apresentadas no enunciado.
- Propostas de Hardening – usar palavras-passes únicas e fortes; gerar uma chave SSH; fazer atualização regularmente ao software; fechar portas abertas que estejam escondidas; colocar as atualizações automáticas; apagar software não utilizado.

Network	IP address	Status
INTERNET	192.168.1.70	Connected - (1h 48m 59s)
Hostname:	ipfire.localdomain	
Gateway:	192.168.1.1	

Network	IP address	Status
LAN	192.168.25.1/24	Proxy on (transparent)
Wireless	192.168.100.1/24	Proxy off
DMZ	192.168.200.1/24	Online

Fig1 – Cenário Proposto

Nas próximas imagens, faremos uma breve descrição de algumas configurações realizadas na LAN.

Conseguimos visualizar o tráfego utilizado em diferentes horas/dias/meses, nas diferentes zonas criadas.

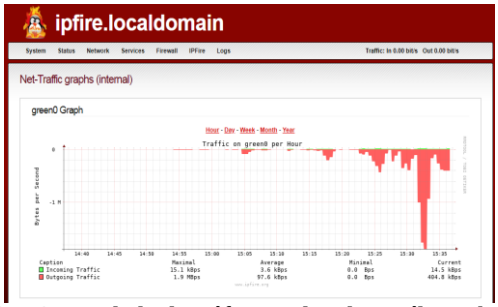


Fig2 – Quantidade de tráfego utilizado na última hora

Bloqueamos alguns sites para os membros deste cenário não ocuparem tráfego desnecessariamente. Nesta imagem, podemos ver o site Twitch.tv bloqueado.

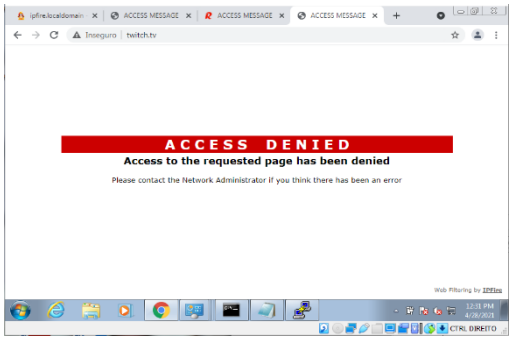


Fig3 – Bloqueio do site Twitch.tv

Neste cenário foi realizado uma proteção à nossa rede contra ataques DNS, forçando que todo o tráfego DNS vá para o DNS do IPFIRE

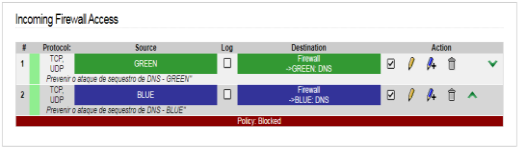


Fig4 - Proteção das redes

Como se pode ver nesta imagem, foi acedido ao putty através do SSH

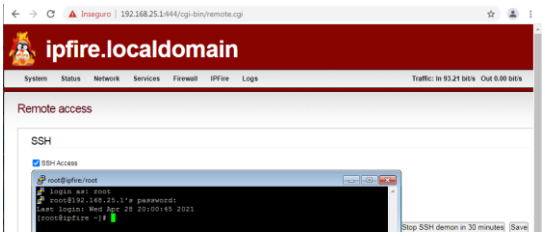


Fig5 – Acesso SSH

A todos os que acedem a esta rede LAN é lhes atribuído um IP entre o 192.168.25.10 e o 192.168.25.100 através do DHCP.

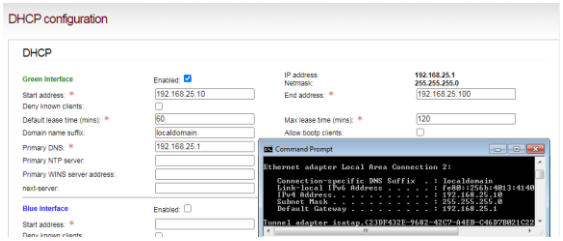


Fig6 – Configuração DHCP

Some Common Mistakes

- Instalamos um servidor web (Django), mas não conseguimos aceder ao servidor.
- Foram cometidos vários erros nas diversas configurações, que serviram para a aprendizagem

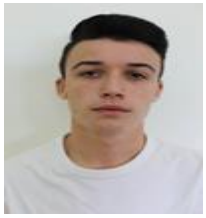
REFERENCES

[1] https://wiki.ipfire.org/configuration/system/ssh
[2] https://wiki.ipfire.org/configuration/firewall/dns
[3] https://computingforgeeks.com/how-to-install-django-on-fedora/

Realizado por:

Luís Oliveira, nº24833, ERSC

Autoavaliação: 13



Bruno Rodrigues, nº23683, ERSC

Autoavaliação: 13