Elaboração de um caderno de experimentos práticos sobre Firewall para uso no laboratório de segurança de redes do Inatel.

Nathália D. Magalhães, Ítalo de Rezende, Alessandra C. Domiciano, Guilherme P. Aquino, Francisco A.S. do Carmo
Instituto Nacional de Telecomunicações - Inatel
nathalia.dias@get.inatel.br, italo.rezende@gec.inatel.br, alessandracarolina@get.inatel.br, guilhermeaquino@inatel.br, francisco.assis@inatel.br

***Resumo*—Atualmente no Inatel (Instituto Nacional de Telecomunicações), no curso de graduação em engenharia de telecomunicações, não há experiências em laboratórios que ensinem aspectos básicos sobre equipamentos de segurança de redes, como Firewalls, IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*). Além disso, o novo currículo em vigência no Inatel prevê a existência de uma nova matéria exclusiva para exploração do conteúdo de segurança de redes e, portanto, será necessária a implantação de um laboratório para abordar esse tema dentro das dependências do Instituto.**

Para suprir essa carência, o objetivo deste trabalho de iniciação científica é gerar um caderno de experimentos práticos que possa ser usado nos laboratórios das matérias que abordem aspectos de segurança de redes. Esses experimentos levarão em consideração a utilização de Firewalls, IDS e IPS instalados dentro das dependências dos laboratórios. De posse desse caderno, professores e alunos poderão realizar experimentos de instalação, avaliação e teste de penetração para fins didáticos, aumentando o conhecimento de todos envolvidos no processo de educação dos cursos de graduação de engenharia de telecomunicações.

Pretende-se utilizar distribuições opensources dos principais equipamentos de Firewall, IDS e IPS já disponíveis e difundidos na Internet. Dessa forma, o custo de implantação destes equipamentos dentro dos laboratórios é minimizado.

***Index Terms*—Firewall, IDS, IPS, Segurança de redes.**

I. Introdução

Quando tratamos de acesso à Internet e as redes em geral devemos ter cuidado com os dados que estão trafegando por estes meios. O uso indiscriminado de informações capturadas nestes ambientes virtuais tem causado grandes impactos tanto para a pessoa física quanto para as grandes organizações.

Uma das soluções de controle para esta situação é a utilização de um Firewall que nada mais é do que um sistema de segurança com a função de restringir ou liberar os acessos entre as redes.

Para [1], é denominado Firewall a utilização em conjunto de hardware e software para isolar e filtrar pacotes que trafegam entre a rede interna e o resto da Internet. Portanto, é correto afirmar que um Firewall é uma barreira entre a rede interna e o resto do mundo e vice versa. Ele opera controlando as entradas e saídas de dados entre as redes existentes e atualmente é um item comum tanto nos computadores pessoais quanto nos grandes servidores e redes de telecomunicações.

Um Firewall pode ser classificado pelo nível de operação em três tipos diferentes: i) filtro de pacotes, ii) Firewall de aplicação ou *proxy* e iii) Firewall de inspeção com estados. O Firewall de filtragem de pacotes analisa todo o tráfego dos pacotes que passa por ele levando-se em conta os critérios de endereçamento IP, tipo do pacote e número de porta da camada de transporte. O Firewall de aplicação ou *proxy* age como um intermediário entre os clientes e servidores da conexão realizando as solicitações no lugar dos clientes e devolvendo as respostas no lugar dos servidores. Por fim, o Firewall de inspeção com estados examina o fluxo de tráfego de ponta a ponta na rede e utilizam-se de uma maneira inteligente para evitar o tráfego de pacotes não autorizados analisando os cabeçalhos dos pacotes e inspecionando o estado de cada fluxo de dados.

O objetivo desse artigo é mostrar os experimentos desenvolvidos para tratar cada tipo de Firewall em um ambiente prático.

Para cumprir com o objetivo desse artigo, o mesmo está dividido da seguinte forma. A Seção II traz uma configuração inicial do PFSense. Logo em seguida, a Seção III mostra todos os passos para se criar uma regra de Firewall de filtragem de pacotes enquanto que a Seção IV mostra os passos para criação de regras para Firewall de nível de aplicação. A Seção V traz as principais conclusões sobre o trabalho.

II. Ajustes inicias para funcionamento do Firewall

Todos os experimentos feitos no caderno do laboratório foram realizados utilizando o sistema de Firewall denominado PFSense [2]. Trata-se de um sistema operacional FreeBSD [3] com funções de filtragem aplicadas às interfaces de conexão de rede. O PFSense será usado em uma máquina virtual com duas interfaces de rede e que está ativa num ambiente de virtualização.

Também serão utilizadas outras duas máquinas virtuais, uma com sistema operacional MS Windows 10 Pro Educacional e outra com sistema Linux Ubuntu Desktop na versão 19.04. Essas máquinas serão usadas para simular o tráfego entre cliente e servidores da rede que contem o Firewall PFSense.

Ao iniciar as atividades, o aluno terá como primeira tarefa ligar o sistema PFSense que está no ambiente de virtualização,

abrir um console remoto e conferir ao final do processo de inicialização, se as duas interfaces de redes estão ativas e com atribuição de endereços IP (*Internet Protocol*), conforme ilustram as Figuras 1 e 2.

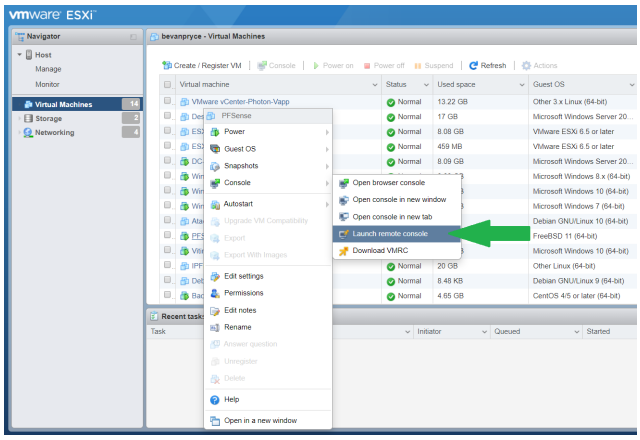

Figura 1. Abrir um console remoto.

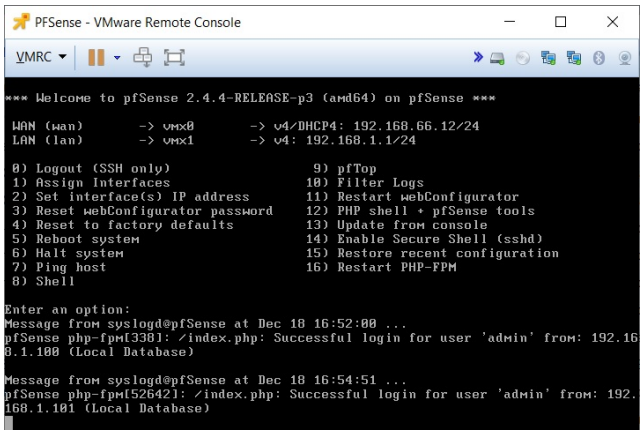

Figura 2. Interfaces de rede com IP atribuído.

A partir da verificação de que as interfaces do PFSense estão com as interfaces de redes com IP atribuído, o aluno poderá efetuar a ligação das outras duas máquinas virtuais envolvidas no experimento que estão no ambiente de virtualização e realizar as ações a seguir:

- Abrir o console remoto da máquina virtual MS Windows 10 Pro Education;
- Realizar o logon com as seguintes credenciais: Usuário = firewall e Senha = firewall123
- Abrir o navegador Google Chrome e digitar o IP 192.168.1.1
- Realizar o logon na interface de configuração do PFSense, com as seguintes credenciais: Usuário = admin e senha = pfsense conforme ilustra a Figura 3

Após a realização do logon, o aluno poderá ver algumas informações sobre o sistema e as diversas guias de acesso existentes no painel de configuração. Dentro do painel de configuração o aluno terá que criar os `Aliases` que serão utilizados nas regras de acesso do Firewall.

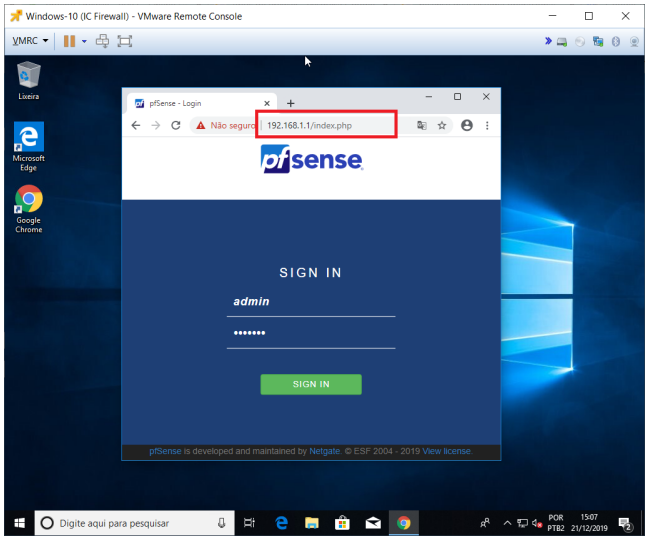

Figura 3. Interface de Logon do PFSense.

Os aliases, também conhecidos como objetos ou endereços, atuam como espaços reservados para agrupar hosts, redes, URLs (*Uniform Resource Locator*) e portas de conexão. Eles são geralmente usados para diminuir o número de alterações que precisam ser feitas quando se cria uma ou mais regras num Firewall. Como exemplo, assuma que você tenha a necessidade de criar uma regra para bloquear um grande número de endereços IP na Internet. Ao criar uma regra para cada um deles a gestão das regras se tornará muito lenta, no entanto, se você criar um `alias` com todos os endereços, bastará aplicar este `alias` em uma única regra e todos eles serão bloqueados de uma única vez facilitando a gestão e garantido a agilidade.

Para a criação do primeiro `Alias`, o aluno terá que acionar a guia Firewall e clicar em Aliases. Perceba, conforme ilustra a Figura 4, que não existem registros criados. A partir desse ponto, o aluno será conduzido a criar um Alias de bloqueio para a URL da rede social Facebook através da guia URLs.

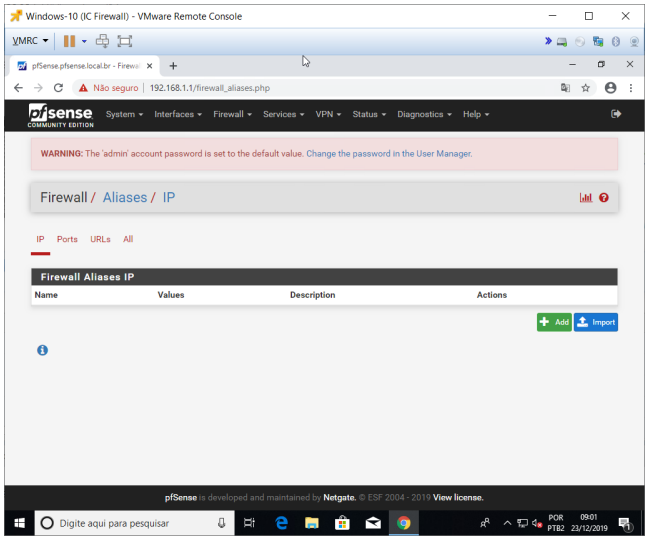

Figura 4. Criando Aliases em URLs.

Para isso, o aluno deverá acionar o botão `Add` e seguir conforme ilustra a Figura 5, preenchendo os campos de acordo com os itens a seguir.

- Nome: Será o nome do alias em relação ao que trata e a rede em que será aplicado;
- Descrição: Uma breve descrição para facilitar a identificação do alias;
- Tipo: Existem sete tipos diferentes para a utilização de uma regra de firewall. O tipo Host(s) deverá ser usado pelo aluno;
- IP ou FQDN (*Fully Qualified Domain Name*): Endereço propriamente dito para o qual pretende-se criar o alias.

É importante observar que FQDN é a sigla para nome de domínio totalmente qualificado ou domínio absoluto e o endereço base de um domínio, tal como em nosso exemplo, facebook.com ou inatel.br. Vale ressaltar que os subdomínios de um domínio raiz também fazem parte do FQDN, ou seja, estão contidos no domínio raiz, um exemplo disso é o endereço pt-br.facebook.com que também é utilizado na criação do alias.

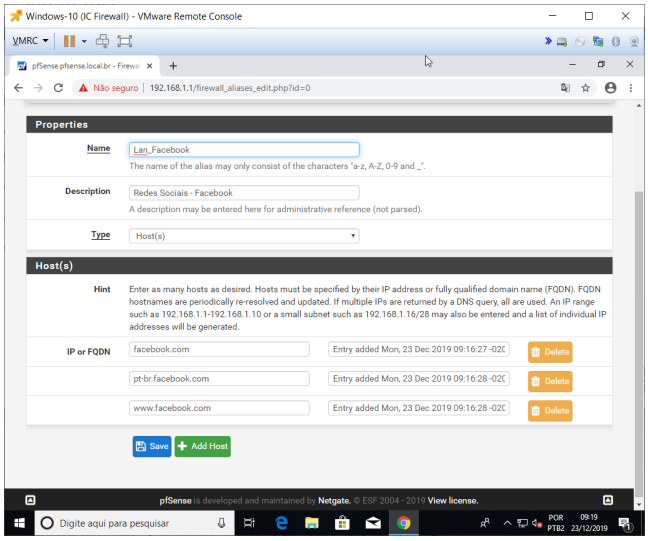

Figura 5. Criando Aliases Facebook.com.

Após a edição, deve-se salvar o alias criado e na sequência aplicar as alterações através do botão `Apply Changes`. A partir daí, o alias já estará disponível para ser utilizado na criação das regras.

III. Criação de Regras do Firewall

No caderno de experimento, o aluno será conduzido a utilizar a guia Firewall e acionar o item `Rules`. Assim, o aluno irá criar a primeira regra de bloqueio ao site do Facebook.com para todos os dispositivos conectados à rede local (LAN – *Local Area Network*) do Firewall. A tela inicial exibe as regras existentes no PFSense, tanto da rede externa (WAN – Wide Area Network) quanto da LAN. O aluno deverá efetuar a criação na guia LAN, conforme ilustra a Figura 6.

Após isso, o aluno deverá ativar o botão `Add` e iniciar a criação da regra preenchendo os campos de acordo com as informações a seguir.

- Action: Block, para criar uma regra de bloqueio;

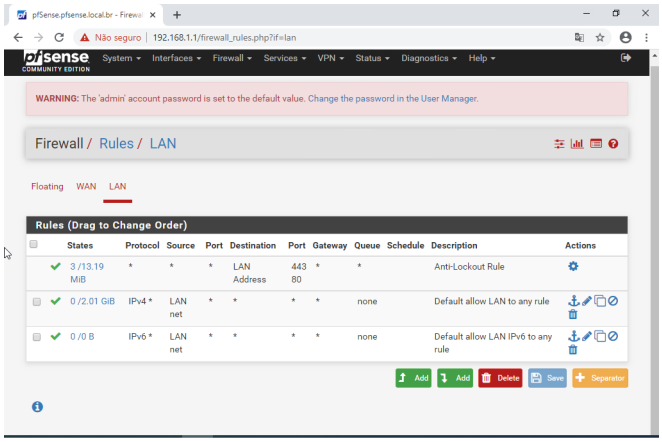

Figura 6. Regras existentes na LAN.

- Disabled: manter desmarcado
- Interface: LAN
- Address Family: IPV4
- Protocol: TCP
- Source: any
- Destination: Single host or alias (digitar no campo Destination Address LanFacebook)
- Destination Port Range: any / any
- Log: permanecer desmarcado
- Description: Bloqueio Facebook

Na sequência o aluno irá salvar a regra e aplicar as alterações. A partir daí, já será possível visualizar a regra na lista de criações da LAN.

Agora, na própria máquina virtual do PFSense, utilizada para efetuar as configurações, o aluno poderá efetuar um teste de acesso ao site do facebook.com e avaliar se realmente a regra já está em funcionamento.

Nesse ponto, todo o acesso aos sites do facebook serão bloqueados quando o aluno tentar fazer um acesso HTTP. Porém, possivelmente, o site https://facebook.com ainda está com o acesso liberado e isso está acontecendo, pois a regra que foi criada, apesar de estar correta, não está posicionada no local onde deve estar na lista de regras. Um firewall tem função hierárquica e conforme a Figura 7, pode-se identificar que existem regras superiores que estão garantindo a liberação de todos os acessos antes da regra da bloqueio do Facebook.

Assim a regra criada não tem efeito algum. Para solucionar esta falha, deve-se posicionar a regra criada logo abaixo da regra `default`, denominada `Anti-Lockout Rule`. Após feito isso, salvar e aplicar as alterações. Agora, efetuando um novo teste ao site do Facebook, o aluno verá que todos os acessos serão bloqueados. Os demais sites podem ser acessados normalmente. Este modelo de criação de regras pode ser utilizado para outros sites, mas lembre-se que tudo começa na criação dos aliases.

IV. Criação de Regras para Firewall de Nível de Aplicação

Além da regra de filtragem apresentada na seção anterior, nesse ponto o aluno será guiado para um experimento que

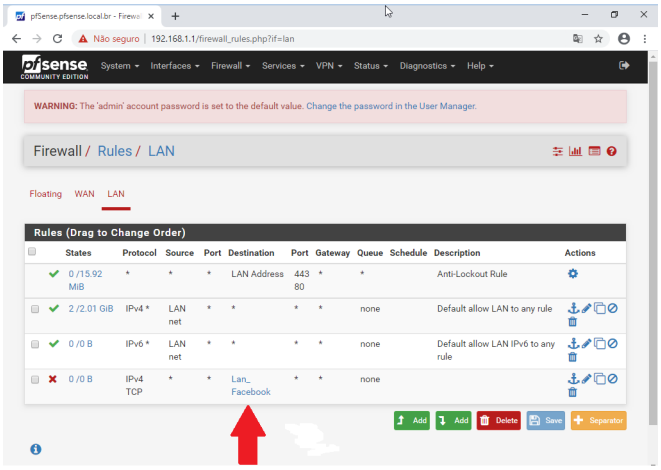

Figura 7. Hierarquia das Regras.

define a criação de regra para portas de conexão FTP (*File Transfer Protocol*), caracterizando um Firewall de nível de aplicação. A sequência de criação do alias é a mesma apresentada anteriormente, com a diferença relacionada ao tipo dele que será Ports. Na Figura 8, tem-se a sequência de criação do alias e a seguir o registro das informações.

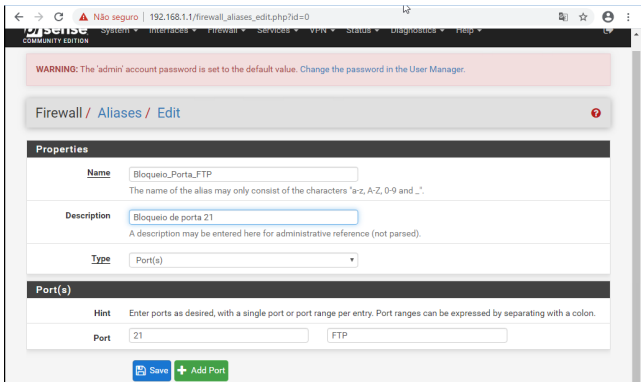

Figura 8. Criando alias para regras de Firewall em nível de aplicação.

- Name: Bloqueio-porta-FTP
- Description: Bloqueio de Porta 21
- Type: Port(s)
- Port: 21
- Description: FTP

Agora, na guia Firewall, o aluno irá escolher o item `Rules` e a interface LAN. Clicar no botão `Add` com seta para baixo e realizar a criação de uma regra utilizando o alias que foi criado. Os itens abaixo são comuns à criação da regra de bloqueio, no entanto, no item `Destination`, o aluno deve configurar os dados de acordo com a Figura 9.

- Action: Block
- Interface: LAN
- Address Family: IPv4
- Protocol: TCP/UDP
- Source: any
- Destination: any
- Destination Port Range: From / To: (other) Custom: Bloqueio-Porta-FTP

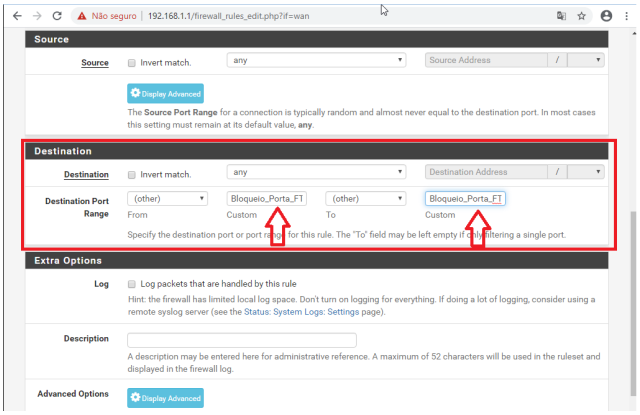

Figura 9. Configuração do item Destination.

No campo `custom`, conforme estão indicando as setas em vermelho, é o local onde deve-se utilizar o alias de bloqueio de porta. Após realizar o preenchimento dos campos, deve-se salvar e aplicar as alterações.

Agora, o aluno poderá realizar o acesso ao site FTP do Inatel no endereço ftp://ftp.inatel.br e se tudo estiver correto, este site não poderá ser aberto e o aluno não deverá visualizar uma caixa de diálogo de logon em seu navegador Web.

Agora, o aluno poderá efetuar um novo acesso a um outro servidor FTP: ftp://ftp.funet.fi/pub/standards/RFC/rfc959.txt, e verificar que a aplicação também foi bloqueada pelo Firewall.

V. Conclusão

Esse artigo resume as experiências práticas que compõem o caderno de experimento que será usado na disciplina de segurança de redes do Inatel. Foram desenvolvidas experiências que guiam o aluno em seus estudos práticos sobre os principais conceitos sobre Firewall. Com o uso do caderno de experimento o aluno terá uma maior aproximação com essa ferramenta que proporcionam um nível de segurança maior às redes de telecomunicações.

Referências

[1] J.F. Kurose and K.W. Ross. *Computer Networking: A Top-down Approach*. Pearson International edition. Addison-Wesley, 2010.

[2] pfSense.org. pfsense a open source security. Disponível em, https://www.pfsense.org.

[3] FreeBSD Project. Freebsd - the power to serve. Disponível em, https://www.freebsd.org.