ARQUITETURA DE **SERVIDORES DE REDE**

Me. Geiza Caruline Costa

INICIAR

introdução

Introdução

Esta unidade contempla a administração de regras no firewall e a análise de seu comportamento por logs. Veremos também como realizar a administração remota de servidores, a virtualização de computadores e a identificação de usuários e seus direitos administrativos em uma rede organizacional.

Manter a segurança de dados usando regras de firewall e monitorar o tráfego usando logs será tratado no tópico 1 desta unidade.

O segundo tópico apresentará a forma de gerenciar o acesso remoto, sua lógica e ativação no servidor.

No terceiro tópico, será abordada a virtualização, seus conceitos, funcionamento e a segurança, nesse contexto.

Na etapa final desta unidade, será tratada a identidade, e acesso de usuários e grupos de uma rede corporativa, bem como as maneiras de aplicar os direitos administrativos nas contas dos usuários.

Firewall

O *firewall* é uma tecnologia que visa contribuir com a segurança de rede, e permite controlar o tráfego de dados por meio da criação e gerenciamento de regras.

As regras de um *firewall* são estritamente importantes à segurança dos dados e ao bom funcionamento da rede, por isso, não basta apenas criar um número grande de regras, se não estiverem devidamente estruturadas. Sendo assim, a quantidade de regras não está relacionada à sua qualidade.

Comer (2016) apresenta uma série de técnicas utilizadas por invasores para atacarem uma rede, conforme destacado no Quadro 2.1:

Técnica	Descrição
Repetição	Enviar pacotes capturados de uma sessão (um pacote enviado contendo uma senha de *login*)
Spoofing de endereço	Falsificar o endereço IP de origem de um pacote, fingindo ser o transmissor, a fim de confundir o receptor no processamento do pacote
DoS e DDoS	Inundar um servidor com pacotes, para impedir que opere normalmente, sobrecarregando seu funcionamento
Port *scanning*	Tentar conexão com cada porta possível, buscando encontrar uma vulnerabilidade

Quadro 2.1 – Algumas técnicas usadas para invadir uma rede de computadores e capturar dados
Fonte: Adaptado de Comer (2016).

Existem várias tecnologias e sistemas utilizados em conjunto para prover segurança a uma rede. O *firewall* é apenas uma dessas ferramentas, que quando configurada adequadamente, pode ajudar a prevenir ataques, como aqueles relacionados no Quadro 2.1. Essas técnicas de ataque se aproveitam de campos dos pacotes ou datagramas, como endereço IP, porta e carga útil (ou *payload*) – que é, efetivamente, o conteúdo trafegado.

Segundo Nemeth, Snyder e Hein (2007), um *firewall* Linux é, geralmente, implementado com os comandos *iptables* contidos em um *script* de inicialização *rc* , normalmente com a estrutura apresentada na figura 2.1.

```
iptables –F nome-da-
cadeia
iptables -P nome-da-
cadeia alvo
iptables -A nome-da-
cadeia -i interface -j alvo
```

Figura 2.1 – Três formas distintas de configuração de regras com o firewall, usando iptables
Fonte: Adaptada de Nemeth, Snyder e Hein (2007).

Onde:

- -F limpa regras anteriores da cadeia
- -P configura uma política padrão
- -A anexa a especificação atual à cadeia

Para começar a implementar um sistema de *firewall* usando Linux, é importante entender as *chains* e as três tabelas (*filter, nat e mangle*). Valle (2010) explica que as chains – ou correntes, em português – são uma espécie de roteamento interno do kernel, pois quando um pacote é recebido, é verificado o destino no cabeçalho do pacote, e então é decidido qual *chain* tratará do pacote. A tabela *filter* (padrão, quando não especificado) trata da filtragem de pacotes em tráfego, e admite as *chains* INPUT, OUTPUT e FORWARD. A tabela *nat* é utilizada quando é preciso substituir algum dos campos contidos no cabeçalho do pacote. Nesse caso, podem ser usadas as *chains* PREROUTING, OUTPUT e POSTROUTING. Por fim, a tabela *mangle* "é usada para marcar pacotes permitindo, por exemplo, o controle de fluxo nas interfaces de entrada e/ou saída" (VALLE, 2010, p. 177).

Descrição	iptables [-t tabela] [opção] [chain] [dados] -j [ação]
Exemplo	iptables -A FORWARD -d 192.168.2.1 -j DROP

Quadro 2.2 – Exemplo de encadeamento de comandos *iptables*
Fonte: Adaptado de Valle (2010).

Caso o comando do Quadro 2.3 seja executado, é acionada, por padrão, a tabela *filter* , uma vez que nenhuma tabela foi especificada. O parâmetro -A anexa a nova regra à cadeia de nome FORWARD; -d 192.168.2.1 especifica que a regra se aplica aos dados cujo destinatário é o endereço IP 192.168.2.1. E, por fim, a ação executada é de descarte, DROP.

O Quadro 2.3 apresenta uma descrição de cada uma das *chains* da tabela *filter* .

INPUT	Quando o destinatário do pacote é a própria máquina *firewall*
OUTPUT	Pacotes gerados pelo *firewall* com qualquer destino
FORWARD	Pacote que trafega pelo *firewall* com origem e destino diferentes

Quadro 2.3 – Chains da tabela *filter*
Fonte: Adaptado de Valle (2010).

Para entender melhor o uso das cadeias da tabela *filter* , observe a Figura 2.2, a seguir:

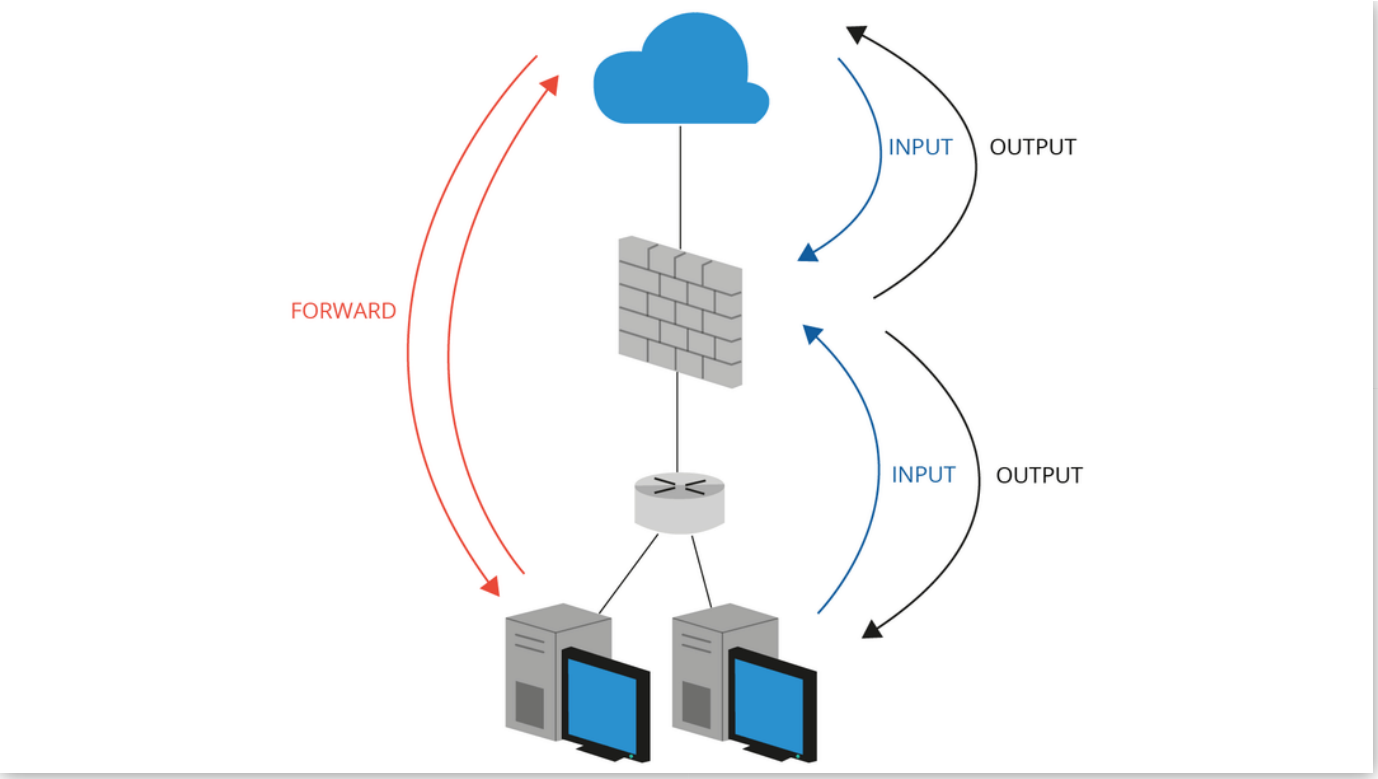


Figura 2.2 – Origem e destino de dados na perspectiva das cadeias da tabela filter
Fonte: Adaptada de Valle (2010).

Note que, para dados oriundos da rede interna, representada pelos computadores conectados ao roteador, destinados ao *firewall* , é usada a *chain* INPUT. Para dados oriundos do *firewall* com destino aos computadores da rede local, é usada a *chain* OUPUT. O mesmo acontece na relação do *firewall* com a rede externa, representada pela nuvem no topo da figura. Em relação a pacotes que apenas passam pelo *firewall* , é usada a *chain* FORWARD.

Comandos da Tabela Filter - Exemplos

O Quadro 2.4 apresenta uma relação de comandos comentados aplicáveis aos *iptables* para a configuração de regras:

Descrição	Comando
Os pacotes vindos de www.site.com deverão ser descartados.	iptables -A FORWARD -d 10.0.0.0/8 -s www.site.com -j DROP
Os pacotes TCP endereçados à porta 25 de qualquer máquina deverão ser aceitos.	iptables -A FORWARD -p tcp --dport 25 -j ACCEPT
Os pacotes destinados à sub-rede 10.0.0.0, vindos de www.site.com.br, deverão ser descartados.	iptables -A FORWARD -d 10.0.0.0/8 -s www.site.com.br -j DROP

Quadro 2.4 – Chains da tabela filter
Fonte: Adaptado de Valle (2010).

Analisando Logs do Firewall

O registro das ações que foram executadas em um sistema é chamado *log* . Para *firewall* são fundamentais, e permitem que o administrador de rede verifique tentativas de ataques e invasões, bem como corrija eventuais falhas em alguma das regras atuais.

A principal ferramenta para monitorar o funcionamento do *firewall* com *iptables* é o *fwlogwatch* . Segundo Wesslowsky (2019), *fwlogwatch* é um analisador de logs de firewall log, e trabalha como um agente de resposta em tempo real.

A gravação de registros de *log* somente é feita caso haja uma instrução

explícita ao *firewall* em comandos *iptables* , requisitando essa ação, conforme apresentado no Figura 2.3:

```
iptables -A INPUT -j LOG
iptables -A OUTPUT -j
LOG
iptables -A FORWARD -j
LOG
```

Figura 2.3 – Estipulando alvo das regras do firewall
Fonte: Adaptada de Duarte (2011).

O Figura 2.3 apresenta três regras aplicadas na tabela *filter* nas *chains* INPUT (linha 1), OUTPUT (linha 2) e FORWARD (linha 3). À medida que essas regras forem sendo aplicadas, durante a filtragem dos pacotes, o parâmetro LOG determina que também seja salvo um registro no *log* .

Para especificar um local onde os *logs* são salvos, deve ser acrescentada uma linha no arquivo de configuração do sistema *syslog* . *conf* semelhante à exibida na Figura 2.4:

```
kern.warn -
/var/log/iptables.log
```

Figura 2.4 – Estipulando alvo das regras do firewall
Fonte: Adaptada de Duarte (2011).

Ao adicionar no arquivo de configuração a linha de comando apresentada na Figura 2.4, fica determinado que o arquivo iptables.log receberá a escrita de todos os registros dos *logs* , dadas as condições especificadas.

A geração de relatórios para consulta e monitoramento pelos administradores de redes e sua equipe pode ser feita com saída para arquivos HTML a serem visualizados no navegador, ou diretamente, pela consulta do arquivo de *logs* .

```
fwlogwatch
/var/log/iptables.log -w -o
index.html
```

Figura 2.5 – Determinando a saída de relatório do firewall para um arquivo HTML
Fonte: Adaptada de Duarte (2011).

Conforme pôde ser observado na Figura 2.5, o comando executado permite a saída do relatório no formato de arquivo HTML. Nesse comando, temos a chamada para o *fwlogwatch* , seguida pelo caminho do registro de logs, finalizando pelo nome do arquivo HTML a ser gerado.

No próximo tópico, serão apresentadas formas de acesso remoto a um servidor de rede, pelas quais será possível, entre outras coisas, monitorar o *firewall* sem acesso físico ao local onde os servidores estão instalados.

Atividade

“O firewall só controla o tráfego que passa por ele. Assim sendo, em ataques provenientes de usuários internos à rede, cujo tráfego não passa pelo firewall, ele não garante proteção”.

MORAES, A. F. **Segurança em Redes** . São Paulo: Érica, 2010.

Considerando a possibilidade de existir um usuário mal-intencionado na rede local, qual seria a melhor forma de proteção, dentre as alternativas a seguir?

- **a)** Incluir uma regra no *firewall* , que bloqueie o tráfego de todos os computadores na LAN.
- **b)** Configurar o *firewall* em uma posição que cubra não somente a comunicação com a *internet* , mas a comunicação entre os dispositivos da rede local.
- **c)** Desligar o *firewall* e analisar os *logs off-line.*
- **d)** Optar por *firewall* Linux.
- **e)** Incluir comandos que permitam salvar *logs* de todas as transações

Administração Remota

A administração remota de servidores é uma prática comum entre os profissionais que trabalham com tecnologia da informação. Dentre os principais benefícios, podemos citar a segurança e a agilidade. Geralmente, quando é preciso instalar um novo servidor na rede, uma das primeiras ações do administrador é configurar o acesso remoto para que seja possível dar continuidade à tarefa em qualquer computador que tenha conectividade ao servidor.

Acesso Remoto

Imagine poder acessar um servidor privado do seu local atual, sem ter de estar fisicamente conectado àquela máquina, mas apenas acessando sua rede. Com o acesso remoto, é possível realizar essa conexão longa e, ainda assim, com segurança na troca de dados. Brito (2017) ressalta:

> *O acesso remoto é tão essencial em servidores que normalmente é o primeiro serviço a ser configurado, depois apenas das configurações básicas de rede. Na realidade, em servidores Debian*

> *GNU/Linux ou Ubuntu Server, esse serviço pode ser pré-instalado durante o próprio processo de instalação do sistema operacional para ser automaticamente executado, bastando para tal selecionar uma opção logo na sequência da instalação dos componentes básicos. (BRITO, 2017, p. 55).*

Conforme o autor afirma, o acesso remoto é um fator crucial e básico para qualquer tipo de servidor, e desse modo, pode-se notar sua real importância no âmbito tecnológico.

No quesito segurança na troca de dados, pode-se utilizar o protocolo SSH, do inglês Secure Shell. Esse protocolo aplica criptografia nos dados trafegados. Para tanto, é necessário realizar a instalação no servidor Linux conforme a figura, a seguir. É importante ressaltar que, ao rodar esse *script* , o SSH é instalado e executado com suas configurações padrão, que podem ser identificadas no arquivo /etc/ssh/sshd_config.

```
apt-get install openssh-
server
```

Figura 2.6 – Comando de instalação e execução SSH
Fonte: Adaptada de Brito (2017).

VPN

Atualmente, no mundo corporativo, é comum enfrentar problemas relacionados ao transporte. Um vendedor farmacêutico passa seu dia visitando clientes, com o intuito de realizar vendas e, precisa verificar os dados da organização, acessando suas informações por meio do sistema. Contudo, para colaborar com seu funcionário e não abrir espaço para falhas na segurança de seus dados, a empresa pode conceder-lhe um acesso remoto por uma VPN (Virtual Private Network).

A VPN concede, ao usuário, a oportunidade de acessar remotamente o sistema da empresa, mantendo sua identidade confidencial em relação à rede pública. Por outro lado, a empresa mantém a rede local em segurança.

Conforme Figura 2.7, o autor Wrightson indica que: “Podemos ver que a comunicação do host A se encontra criptografada até o gateway VPN e, então, é descriptografada diretamente para os hosts pretendidos do local B” (WRIGHTSON, 2014, p. 257).

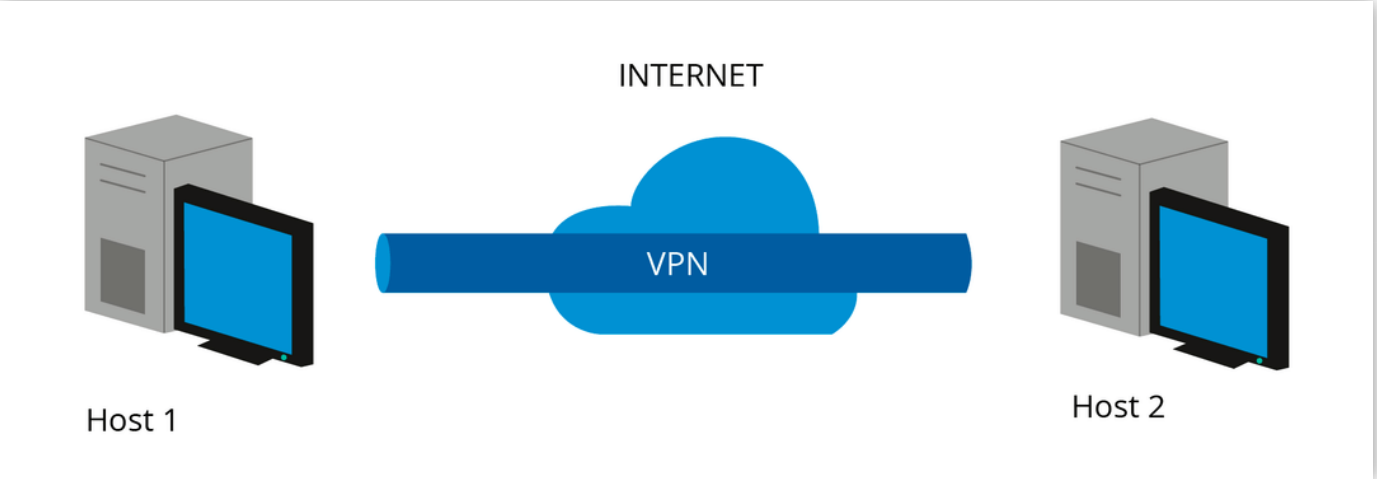


Figura 2.7 – VPN Host para Host
Fonte: Adaptada de Wrightson (2014).

Brito (2017) conceitua esse tipo de conexão VPN como *client-to-site* , rede que possibilita, a um funcionário que esteja fora do espaço físico da empresa, poder conectar recursos de infraestrutura como se estivesse presente no espaço físico de trabalho.

Atividade

Segundo Guimarães (2006), “uma rede VPN implementa a criação de túneis de criptografia através da Internet para transmitir informações entre redes privadas”.

GUIMARÃES, A. G. **Segurança em Redes Privadas Virtuais** . Rio de Janeiro: Brasport, 2006.

Assinale a única alternativa verdadeira, relacionada ao uso de redes virtuais privadas.

- **a)** VPNs são utilizadas, principalmente, para possibilitar o acesso de um usuário da LAN à Internet.
- **b)** VPNs foram criadas com o intuito de permitirem uma conexão de n para m, ou seja, muitos computadores para muitos computadores.
- **c)** Ao usar VPN, é possível, de forma remota, ingressar em uma LAN (Local Area Network).
- **d)** Não existem recursos adicionais que contribuam para a segurança no tráfego de dados na WAN (Wide Area Network).
- **e)** VPN é um tipo específico de rede intermediária entre PAN (Personal Area Network) e LAN (Local Area Network).

Virtualização

Virtualização pode ser definida como uma tecnologia capaz de virtualizar recursos de TI, por exemplo, o *hardware* . Trata-se de um tema estritamente atual e cada dia mais utilizado nas organizações. Esse recurso permite que o sistema operacional de uma máquina seja parcial (aplicações) ou totalmente executado (sistema operacional), virtualmente, dentro de outra máquina.

Conforme Veras, virtualização é "A tecnologia central de um datacenter e essencialmente transforma, obedecidas certas condições, um servidor físico em vários servidores virtuais. Os impactos são muitos e os benefícios também" (VERAS, 2011, p. 85).

Lima (2017) ressalta que, como benefícios reais na utilização dessa tecnologia, temos a redução de custos e de necessidade de manutenção, bem como o aumento de *performance* , flexibilidade e escalabilidade.

Agora, imagine quantas milhares de máquinas não poderão ser economizadas tanto no quesito financeiro quanto ambiental às empresas? Na virtualização, o ambiente virtual é uma cópia idêntica do ambiente real, o que não justifica a utilização de um número de máquina excessivo. Essa nova tecnologia

possibilita a independência da máquina ao *hardware* , que significa que, ao copiar o sistema operacional da máquina A para máquina B, por exemplo, permite que a máquina B opere virtualmente, sem necessitar dos adereços físicos de uma máquina comum, como o teclado e o *mouse* .

Na figura a seguir, o autor Veras ilustra o funcionamento da virtualização, passando de uma máquina física para máquina virtual. Nesse caso, a máquina física 3 foi virtualizada em quatro máquinas virtuais (VMs).

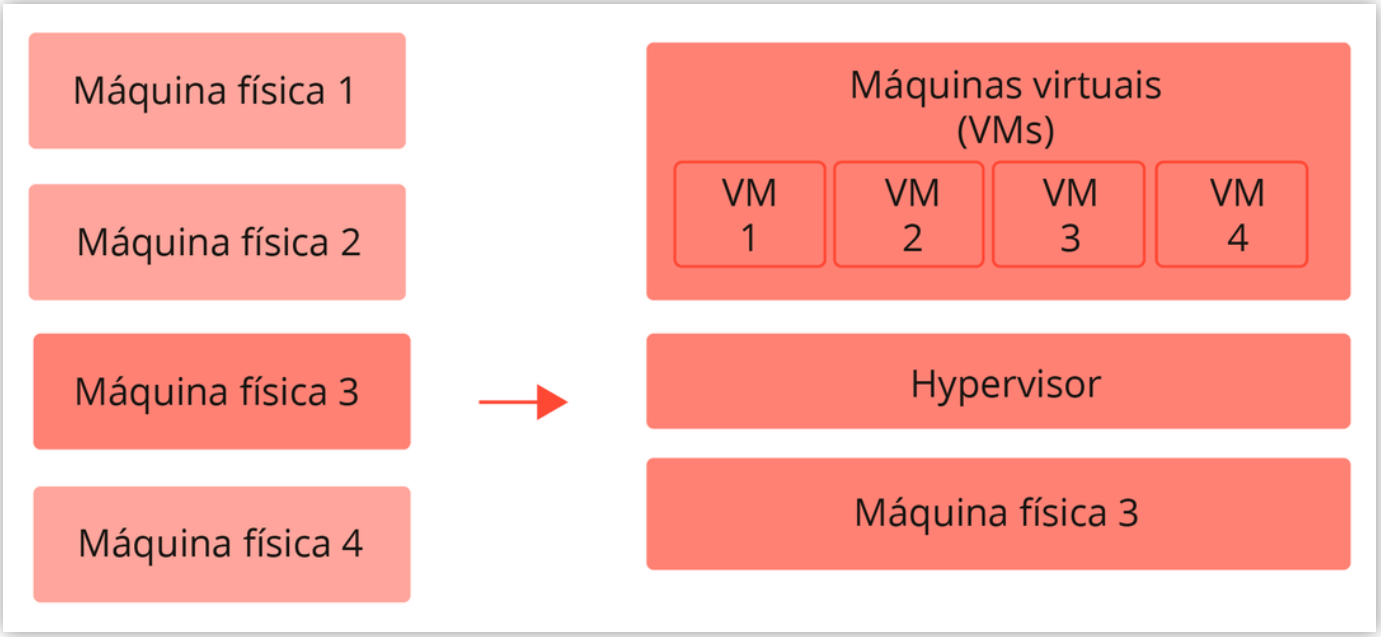


Figura 2.8 - Virtualização
Fonte: Adaptada de Veras (2016).

Como é possível verificar na Figura 2.8, as máquinas virtuais (VM1, VM2, VM3 e VM4) estão "consumindo" o *hardware* da máquina física 3 através do *hypervisor* , que é o responsável por disponibilizar, ao sistema operacional, a abstração da máquina virtual, controlando o acesso entre máquina virtual e *hardware* da máquina real. Como cada máquina possui seu próprio sistema operacional independente, é possível instalar diferentes sistemas operacionais nas máquinas, por exemplo, duas máquinas utilizando Windows e as demais, Linux.

Velloso (2017) relata a existência de três tipos de virtualização:

1. **Hardware:** conforme mencionado anteriormente, foca em rodar diversas máquinas virtuais, por meio do sistema operacional, dentro

de uma máquina real. A vantagem de se utilizar essa tecnologia visa tanto o âmbito físico quanto a compatibilidade de aplicativos.
2. **Apresentação:** possibilita o acesso ao computador sem, necessariamente, estar fisicamente nele, como é o caso da máquina virtual. Por esse tipo de virtualização, é possível acessar a máquina remotamente, de onde quer que esteja.
3. **Aplicativos:** esse tipo de virtualização permite impossibilitar conflitos entre aplicativos. O aplicativo original é copiado em uma máquina de servidor virtual de fácil acesso aos usuários, possibilitando sua utilização sem, necessariamente, instalá-lo.

Atualmente, existem vários tipos de ferramentas de uso para virtualização, como VMWare, VirtualBox, Xen, KVM e OpenVZ.

Segurança

Conforme citado no item anterior, o *hypervisor* é a camada responsável por realizar a comunicação entre máquina e lógica. Sendo assim, o *hypervisor* realiza a "tradução" de informações entre o *hardware* e *software* , com o intuito de possibilitar a virtualização do computador. Ele também é o responsável pelo controle de acesso dos usuários virtuais aos componentes físicos da máquina real.

Segundo Veras (2011), essa camada é a responsável pela segurança, pois possui mecanismos para identificar invasores e realiza o controle de acesso à rede e discos.

Contudo, um fato importante para reflexão é a dependência existente entre a máquina física e as máquinas virtuais vinculadas. Por exemplo, no caso de a máquina física A receber algum tipo de invasão de segurança, as máquinas virtuais atreladas a ela também estarão comprometidas.

saiba mais

Saiba mais

Assista ao vídeo “Fundamentos da virtualização - VMWare”, que destaca os benefícios e justificativas de seu uso, bem como fornece uma breve explicação sobre a ferramenta.

ASSISTIR

Atividade

A virtualização é uma realidade nos dias atuais, sendo uma tecnologia imprescindível no contexto empresarial, pois simplifica o gerenciamento, e flexibiliza e amplia o poder de processamento.

VERAS, M. **Virtualização** : componente central do *data center* . Rio de Janeiro: Brasport, 2011.

Dentre os benefícios passíveis de uma máquina virtual, verifique a alternativa coerente à sua aplicação no âmbito de um escritório em uma organização de Tecnologia da Informação.

- **a)** Não utilizar máquina física.
- **b)** Uso de sistema operacional único.
- **c)** Aumento dos custos de TI.
- **d)** Espaço físico TI reduzido.
- **e)** Maior aquisição de máquinas físicas.

Identidade e Acesso

Na medida em que a rede corporativa aumenta, mais difícil é seu gerenciamento e seu controle, pois, provavelmente, haverá mais usuários, mais serviços e maior tráfego na rede.

Surge, então, a necessidade de controlar o acesso dos usuários por meio da gestão de identidades, configuração de permissões, grupos e funções administrativas.

O Lightweight Directory Access Protocol (LDAP) é um protocolo leve, para acesso a serviços de diretório (VALLE, 2010). Sua implementação em um sistema operacional de distribuição Linux é dada pelo OpenLDAP, o qual centraliza os recursos de rede, facilitando sua administração.

> *O OpenLDAP é um pacote do LDAP adicionado de recursos e softwares necessários para torná-lo funcional, que oferece um serviço de diretório prático e seguro. Este serviço é usado para armazenar todos os dados da rede, como senhas, IDs de usuários, nomes, endereços, além de outros, centralizando as pesquisas e consultas em si, esta centralização é a chave para abrir um*

> *caminho que leva a praticidade na administração de uma rede de qualquer tamanho. (RIBEIRO JÚNIOR, 2008, on-line).*

O sistema OpenLDAP permite a centralização de recursos, pois pode armazenar, em sua base de dados, as informações de todos os usuários da organização cadastrados e facilitar a gestão de identidades (autenticação), inclusive quando o login for feito em diversos sistemas corporativos, como *e-mail e proxy* .

Figura 2.9 – Um usuário, geralmente, precisa informar suas credenciais em vários sistemas
Fonte: anyaberkut / 123RF.

Ao contrário de um banco de dados relacional, o LDAP funciona como uma base de dados hierarquizada, por meio de diretórios. “Esta estrutura guia o usuário para facilitar a procura de uma informação, passando desde a raiz, depois pelos diretórios subjacentes até se chegar à informação desejada” (RIBEIRO JÚNIOR, 2008, *on-line*).

Uma vez instalado e previamente configurado o serviço OpenLDAP, é preciso fazer o cadastramento de grupos e usuários para, então, atribuir privilégios e realizar outras configurações. Uma forma de fazer isso é usando arquivos de

texto em formato LDIF (LDAP Data interchange Format).

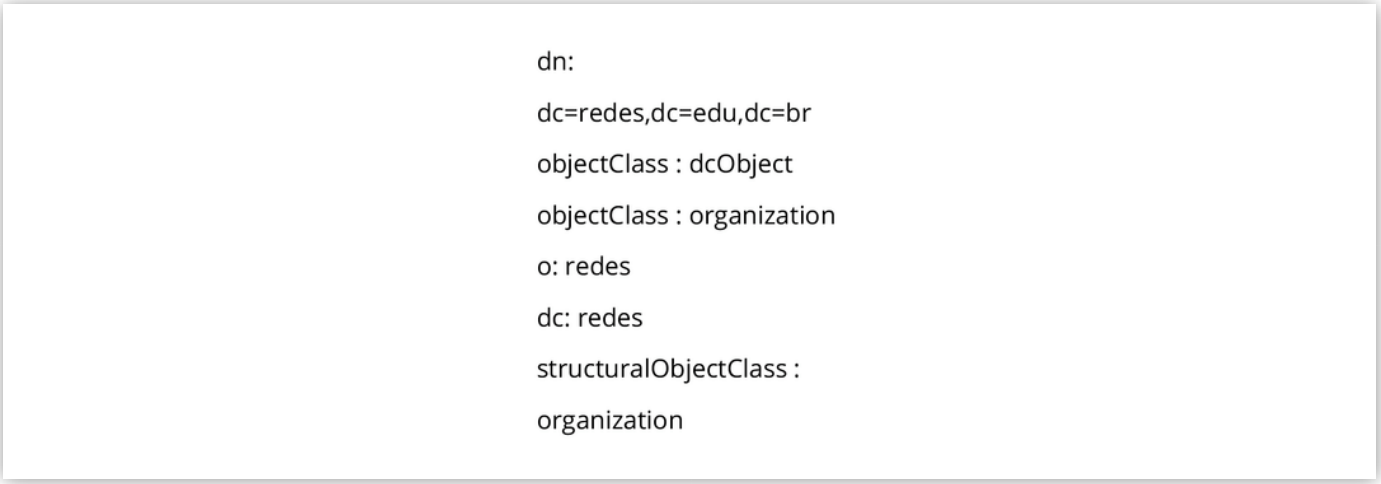


Figura 2.10 - Parte 1 de configuração arquivo LDIF
Fonte: Adaptada de Valle (2010).

Todo o arquivo apresenta uma estrutura hierárquica. Na Figura 2.10, é representada a criação de uma organização. Com base nesse objeto, será possível criar uma série de unidades organizacionais, conforme a necessidade.

Figura 2.11 - Parte 2 de configuração arquivo LDIF
Fonte: Adaptada de Valle (2010).

Na Figura 2.11, é representada a criação de unidades organizacionais. As unidades organizacionais (organizationalUnit) dependem de uma classe superior, que neste caso é representada por top. Isso significa que a classe organizationalUnit herda alguns campos da classe top.

Tendo sido criada essa estrutura de organização e unidade organizacional, podem ser usadas ferramentas ou comandos específicos para a criação e

gerenciamento de usuários, por exemplo, o phpLDAPadmin, que é uma ferramenta que consiste em uma interface gráfica baseada na web para gerenciar o servidor LDAP (VALLE, 2010).

reflita

Reflita

"Ferramentas tão variadas quanto o servidor Web Apache e o automontador autofs também podem ser configuradas para prestar atenção no LDAP" (NEMETH; SNYDER; HEIN, 2007, p. 362 e 363). Você acredita que a administração centralizada de recursos da rede em um único sistema poderia atribuir um grau de vulnerabilidade ao ponto focal da rede corporativa?

Fonte: Nemeth, Snyder e Hein (2007).

Atividade

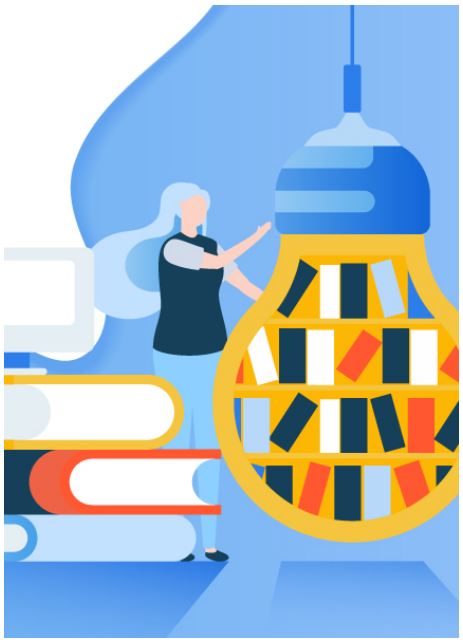
O fato de o LDAP representar um modelo de acesso específico para as aplicações e em razão da forma como os dados são esquematizados levaram o LDAP a ser desenvolvido como um sistema completo e independente, tornando-se um padrão (NEMETH; SNYDER; HEIN, 2007). É correto afirmar que LDAP é:

NEMETH, E. SNYDER, G. HEIN, T. R. **Manual completo do Linux** : guia do administrador. 2. ed. São Paulo: Pearson Prentice Hall, 2007. p. 361.

- **a)** Um banco de dados.
- **b)** Uma regra.
- **c)** Uma interface.
- **d)** Um protocolo.
- **e)** Um site.

indicações

Material Complementar



LIVRO

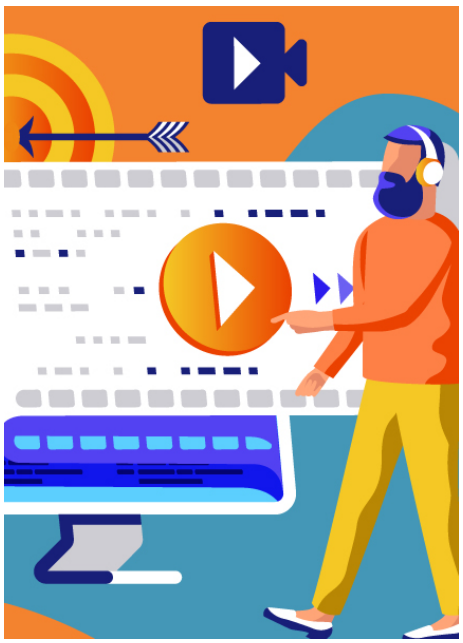
Firewalls: segurança no controle de acesso

Alexandre Fernandes de Moraes

Editora: Érica

ISBN: 8536514736

Comentário: em 120 páginas, o autor mergulha no sistema firewall e vai muito além da filtragem de pacotes. Confira esse título para saber mais do potencial do firewall e da aplicação prática dos pilares de segurança da informação.



FILME

Passageiros

Ano: 2017

Comentário: a história desse filme se passa em uma viagem interestelar, em que os tripulantes enfrentam severas dificuldades. Observe que a identificação dos usuários é crucial para o funcionamento do sistema apresentado. Quais as consequências para os personagens você prevê, em caso de falha na gestão dos acessos e dos recursos?

TRAILER

conclusão

Conclusão

Nesta unidade, percebemos que a identificação de dispositivos na rede, dada pelos seus endereços IP e portas, tem papel fundamental na segurança de dados. A segurança dos servidores de rede, dos grupos de usuários e da LAN, em relação a possíveis invasores externos ou usuários mal-intencionados, foram assuntos explorados nesta unidade, quando aprendemos sobre o funcionamento do *firewall* . Vimos que a gestão de identidade dos usuários e grupos em uma rede corporativa facilita o trabalho do administrador de rede, em termos de organização e eficiência, quando são usadas ferramentas como LDAP. Além disso, foi apresentada a configuração do acesso remoto nos servidores, o que, hoje, é uma funcionalidade indispensável para qualquer administrador de rede que não quer, e nem deve, ser figura frequente no *data center* .

referências

Referências Bibliográficas

BRITO, S. H. B. **Serviços de Redes em Servidores Linux.** São Paulo: Novatec, 2017.

COMER, D. E. **Redes de Computadores e a Internet.** 6. ed. São Paulo: Bookman, 2016.

DUARTE, D. Logs no Iptables - Parte 1. **PuraInfo** , ago. 2011. Disponível em: < https://purainfo.com.br/logs-no-iptables-parte-i/ > Acesso em: 18 abr. 2019.

GUIMARÃES, A. G. **Segurança em Redes Privadas Virtuais** . Rio de Janeiro: Brasport, 2006.

LIMA, A. C. de. Segurança na Computação em Nuvem. São Paulo: Senac, 2018.

NEMETH, E. SNYDER, G. HEIN, T. R. **Manual Completo do Linux** : guia do administrador. 2. ed. São Paulo: Pearson Prentice Hall, 2007.

RIBEIRO JÚNIOR, J. OpenLDAP: a chave é a centralização. **Viva o Linux** , dez. 2008. Disponível em: < http://www.vivaolinux.com.br/artigo/openldap-a-chave-e-a-centralizacao. > Acesso em: 18 abr. 2019.

VALLE, O. T. **Administração de redes com Linux** : fundamentos e práticas. Florianópolis: Publicações do IF-SC, 2010.

VELLOSO, F. **Informática:** conceitos básicos. Rio de Janeiro: Elsevier, 2017.

VERAS, M. **Virtualização** : componente central do data center. Rio de Janeiro: Brasport, 2011.

_____. **Virtualização** : tecnologia central do data center. 2. ed. Rio de Janeiro: Brasport, 2016.

WESSLOWSKY, B. Canonical 2019. **Ubuntu Manuals** . Disponível em: < http://manpages.ubuntu.com/manpages/trusty/man8/fwlogwatch.8.html >. Acesso em 18 abr. 2019.

WRIGHTSON, T. **Segurança de redes sem fio** : guia do iniciante. Brasil: Bookman, 2014.

IMPRIMIR