UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

JACKSON LAURENCE LANSKI

INSTALAÇÃO E CONFIGURAÇÃO DE UMA VPN ENTRE SERVIDORES LINUX PARA TRANSFERENCIA DE DADOS COM SEGURANÇA PELA INTERNET

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2017

JACKSON LAURENCE LANSKI

INSTALAÇÃO E CONFIGURAÇÃO DE UMA VPN ENTRE SERVIDORES LINUX PARA TRANSFERENCIA DE DADOS COM SEGURANÇA PELA INTERNET

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Juliano de M. Pedroso.

CURITIBA

2017

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba

DIRPPG
DAELN
GESER

TERMO DE APROVAÇÃO

INSTALAÇÃO E CONFIGURAÇÃO DE UMA VPN ENTRE SERVIDORES LINUX PARA TRANSPARENCIA DE DADOS COM SEGURANÇA PELA INTERNET

por

JACKSON LAURENCE LANSKI

Esta Monografia foi apresentada em 05 de dezembro de 2017 como requisito parcial para a obtenção do título de Especialista em Gerenciamento de Servidores e Equipamentos de Rede. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Augusto Foronda
Prof. Coordenador do Curso

_____
Juliano de Mello Pedroso
Prof. Orientador

_____
Kleber Kendy Horikawa Nabas
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

RESUMO

Como a redução de custos passou a ser uma necessidade que devemos priorizar, esta monografia tem a intenção de mostrar como implementar segurança na transmissão de dados pela *internet* (rede mundial de computadores), que se trata de uma rede de baixo custo, porém com pouca segurança. Serão utilizados programas com licença gratuitas, como o Linux e o OpenVPN, para explicar como configurar uma replicação de banco de dados MySQL entre dois servidores. Um servidor ficará alocado no cliente e outro em um *datacenter* (local projetado para armazenar servidores e equipamentos destinados a efetuar armazenamento de informações) em outra localidade, servindo como forma de *backup* (copia de segurança) em caso de desastre. A comunicação entre os dois servidores será feita utilizando uma VPN que cria um túnel criptografado entre os servidores.

Palavras-chave: OpenVPN, Banco de Dados MySQL, Replicação Remota, Backup.

ABSTRACT

As the cost reduction has become a necessity that we must prioritize, this monograph intends to show how to implement security in the transmission of data over the internet, which is a low cost network, but also low security. Free softwares like Linux and OpenVPN will be used to explain how to set up a MySQL database replication between two servers. One server will be allocated on the client and another on a datacenter in another location, serving as backup in the event of a disaster. Communication between the two servers will be done using a VPN that creates an encrypted tunnel between servers.

Keywords: OpenVPN, Database MySQL, Remote Replication, Backup.

LISTA DE GRÁFICOS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BD	Banco de Dados
IEC	*International Electrotechnical Commission*
IP	*Internet Protocol*
ISO	*International Organization of Standardization*
LTS	*Long Term Support* - Suporte a Longo Prazo
NBR	Normas Brasileira
PKI	*Public Key Infrastructures*
PSI	Política de Segurança da Informação
SGBD	Sistema Gerenciador de Banco de Dados
TI	Tecnologia da Informação
VM	*Virtual Machine* - Máquina Virtual
VPN	*Virtual Private Network* - Rede Virtual Privada

SUMÁRIO

1 INTRODUÇÃO

Esta monografia tem a intenção de mostrar como implementar uma comunicação segura entre dois servidores de banco de dados, utilizando a *Internet* (rede mundial de computadores) como meio de comunicação, hoje esta comunicação é feita através de um *link* (canal de comunicação) dedicado, o que esta saindo muito caro para o cliente. Como a *Internet* (rede mundial de computadores) não é um meio seguro de comunicação, este trabalho visa explicar como deixar esta transferência de dados segura, utilizando uma VPN que cria um túnel criptografado entre os servidores.

Neste trabalho será explicado como configurar uma replicação do banco de dados MySQL entre dois servidores, um servidor ficará alocado no cliente e outro em um *datacenter* (local projetado para armazenar servidores e equipamentos destinados a efetuar armazenamento de informações) em uma localidade distinta, que irá funcionar como replicação remota. Esta funcionalidade esta sendo exigida em alguns estados brasileiros devido aos problemas encontrados com sequestro de informações, ou mesmo a vulnerabilidade com relação aos dispositivos de armazenamento de dados.

O banco de dados MySQL permite um tipo de replicação conhecida como *master-slave* (mestre-escravo) onde todas as alterações efetuadas no banco de dados do servidor *master* (mestre) são gravadas em um *log* (arquivos de registro de dados), os quais são imediatamente replicadas para o servidor *slave* (escravo) e para que isto ocorra, é necessário que os dois servidores estejam na mesma rede.

2 REFERENCIAL TEORICO

Com o objetivo de esclarecer os detalhes sobre as tecnologias utilizadas nesta monografia, proporcionando um melhor entendimento, este tópico tem a intenção de fundamenta-las dando consistência ao estudo e apresentando um embasamento já publicado sobre as mesmas.

Todo este trabalho de pesquisa esta baseado em redes de computadores e segundo Tanembaum (1994) uma das funções de uma rede de computadores é promover a comunicação estre equipamentos dispersos geograficamente, permitindo que pessoas de varias localidades tenham acesso ao mesmo arquivo com a possibilidade de altera-lo simultaneamente.

Serão utilizadas VMs e conforme Laureano (2006) explica, maquinas virtuais são sistemas que implementam instruções passadas pela máquina real em um ambiente abstrato de *software* (programa), permitindo rodar aplicativos de uma plataforma em outra. Uma maquina virtual é um programa que simula um computador real, permitindo que as operações da máquina real sejam executadas em um programa. Máquina virtual é um ambiente criado por um monitor de máquina virtual, que pode ser denominado “sistema operacional para sistemas operacionais” ou *hypervisor*. O monitor pode criar uma ou mais máquinas virtuais sobre uma única máquina real.

As maquinas virtuais tem a funcionalidade de trabalhar em rede, a qual é extremante útil quando esta sendo utilizado um sistema gerenciador de banco de dados, conforme Silberschatz, Korth e Sudarshan (2006) um sistema de gerenciamento de dados é um conjunto de dados relacionados e um sistema para acesso a estes dados, pode ser chamado de banco de dados, o qual possui informações significativas para a empresa. Os bancos de dados foram criados para trabalhar com grande quantidade de informações, permitindo a manipulação destas informações.

Para Elmasri e Navathe (2011), banco de dados e SGBD (sistema gerenciador de banco de dados) são fundamentais na sociedade moderna, a maioria das pessoas encontram em suas atividades diárias integração com banco de dados, ao utilizarmos o banco para efetuar saques e depósitos, fazer reservas de hotel, até para compras em supermercados, o qual atualiza seu estoque para controle dos itens vendidos.

Estes exemplos podem ser chamados de aplicações de banco de dados tradicionais e com o avanço da tecnologia, surgiram novas aplicações para os bancos de dados, como banco de dados multimídia, para armazenar áudio, imagens e clipes de vídeos, sistema de *data warehousing* (sistema de armazenamento de dados) para extrair e analisar informações comerciais uteis para as empresas.

Com a comodidade de trabalhar com os dados em tempo real em diversas localidades simultaneamente, vem à preocupação com a segurança na transferência destes dados. Como explica Caruso e Steffen (1999), a *internet* (rede mundial de computadores) como esta configurada agora não é o meio seguro para transferência de dados, por este motivo, precisamos utilizar a criptografia na transferência das informações.

Stalling (2014) fundamenta um pouco sobre segurança, descreve que uma mensagem que precisa ser transferida de um local para outro utilizando algum tipo de rede, necessita de um canal de informação lógico, que quando é estabelecido, define uma rota pela rede iniciando na origem e terminando no destino. A segurança começa a atuar quando é preciso proteger esta transmissão de um inimigo que possa apresentar ameaça à confidencialidade, autenticidade ou disponibilidade.

Uma das técnicas utilizadas para garantir a segurança consiste em uma transformação da informação a ser enviada, que se resume em *encriptar* a mensagem, os seja “embaralhar” os dados de forma que fique ilegível para quem não tem a chave para “desembaralhar”. O acréscimo de um código na informação pode ser usado para verificar a identidade do emissor, utilizando informações secretas compartilhadas.

Para Burnett e Paine (2002) a criptografia é a tecnologia que quando aplicada em dados que podem ser lidos por qualquer pessoa os transformam em códigos que não possuem significado algum, e que quando necessário podem ser recuperados à sua forma original utilizando para isso formulas e algoritmos extremamente complexos.

A criptografia está se tornando provavelmente o aspecto mais importante da segurança nas comunicações, esta cada vez mais importante como um componente básico para segurança do computador.

Conforme explica Stalling (2014), existem três conceitos que formam o que pode ser chamado de tríade CIA (do inglês, *confidentiality, integrity and availability* -

confidencialidade, integridade e disponibilidade). Sendo considerados os objetivos fundamentais da segurança da informação:

Confidencialidade: Garante que as informações particulares e confidenciais não sejam acessadas por indivíduos não autorizados. Procura preservar e restringir o acesso das informações. Uma forma de perder a confidencialidade seria a divulgação de uma informação não autorizada.

Integridade: Assegura que as informações ou os programas não sejam modificados ou alterados sem autorização, garantindo que os mesmos se mantenham da forma como foram criados e disponibilizados pelo proprietário. Uma forma de perder a integridade seria a modificação não autorizada de uma informação.

Disponibilidade: Garante que os sistemas não parem de operar seus serviços ou fiquem indisponíveis para usuários. Assegurar o acesso e o uso da informação em tempo integral. Uma forma de perda de disponibilidade é a parada de um sistema de informação.

Todas as normas e recomendações de segurança a serem utilizadas no *backup* (copia de segurança), devem pertencer a política de segurança da Empresa e precisam ser fundamentadas na política de segurança da informação (PSI) utilizando estratégias que permitam proteger as informações relevantes para os negócios da organização.

A norma NBR ISO/IEC 17799 (ABNT, 2005) sugere que os Planos de Continuidade de Negócios da empresa sejam criados e realizados com a intenção de garantir que os processos sejam capazes de ser recuperados o mais rápido possível. Estes planos precisam ser mantidos e testados de tal forma que se tornem parte de todos os outros processos de gerência.

Mesmo com a criptografia aplicada aos dados, os mesmos podem se interceptados e desencripitados deixando a informações legíveis para o interceptor, por este motivo para melhorar ainda mais a segurança, uma opção é configurar uma VPN, conforme explica Filippetti (2008) Rede Virtual Privada é uma forma segura de transmitir informações pela *internet* (rede mundial de computadores) compartilhada por milhares de usuários, pois toda a transmissão é criptografada, e quando um túnel VPN é fechado entre dois pontos, temos uma conexão ponto a ponto, a qual permite a configuração de rotas, ou mesmo a utilização de protocolos de roteamento. Antes de fechar o túnel de VPN, é necessário autenticar todos os elementos participantes, o

que vai garantir a integridade dos dados que passam por esta conexão. Ao trabalhar com uma rede ponto a ponto a segurança das informações transmitidas é muito maior.

Para Nakamura e Geus (2003) as redes virtuais privadas tem uma importância fundamental para as organizações, pois podem substituir as conexões dedicadas, por conexões publicas como a *Internet* (rede mundial de computadores), diminuindo radicalmente o custo da comunicação. Outra funcionalidade é substituir o acesso remoto direto e para isso é indicado à utilização de uma autenticação forte, já que os recursos utilizados estão sendo acessados diretamente pelos usuários remotamente.

Caruso e Steffen (1999) informam que um *firewall* (sistema de segurança instalado no computador) pode ser um *software* (programa) ou *hardware* (equipamento) que tem o papel de realizar analises do fluxo de pacotes de dados, filtragens e registros dentro de uma estrutura de rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

Peterson e Davie (2004) descrevem um *firewall* (sistema de segurança instalado no computador) como um roteador programado exclusivamente, que se localiza entre uma instalação e o restante da rede, ele pode ser considerado um roteador, pois esta conectado a duas ou mais redes e encaminha pacotes entre elas, fazendo um filtro nos pacotes que passam por ele. Através de suas regras, pode descartar ou encaminhar os pacotes que passam por ele, impedindo que pessoas externas tenham acesso a rede interna da empresa aumentando a segurança da rede.

Como todas estas tecnologias trabalham diretamente em servidores de informática, ou seja, equipamentos físicos, os quais podem apresentar problemas, falhas ou mesmo acontecer uma catástrofe perdendo todas as informações. Neste caso surge a necessidade da configuração de um *backup* (copia de segurança) em tempo real, com a possibilidade de manter uma cópia dos dados do servidor, em outro equipamento localizado fisicamente em outra cidade.

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2005), é muito importante as cópias de segurança obtidas com as informações e também com as aplicações dos sistemas utilizados pela empresa, tenha uma rotina de testes efetuados regularmente, conforme a política utilizada e definida pela empresa.

Estas normas e recomendações aplicadas na segurança da informação, utilizadas para gerar o *backup* (copia de segurança) dos dados precisam pertencer as políticas de Segurança da Informação e obrigatoriamente devem estar baseadas em

estratégias que visam assegurar que as informações indispensáveis para os negócios da organização não apresentem dano e tenha, uma rápida recuperação em caso de catástrofe.

3 MÉTODO

Esta monografia visa explicar como instalar o banco de dados MySQL, configurar sua replicação, instalar e configurar uma VPN para a transferência segura entre dois servidores Linux utilizando a *Internet* (rede mundial de computadores) como meio de comunicação.

Hoje esta replicação é feita sem nenhuma segurança implantada na transmissão dos dados, os quais passam limpos pela *internet* (rede mundial de computadores), sem nenhuma criptografia, ou qualquer outra forma de proteção, ficando passiveis de interceptação por pessoas mau intencionadas. Existem apenas dois *firewalls* (sistema de segurança instalado no computador) configurados em cada ponta da rede, um no cliente e outro no *datacenter* (local projetado para armazenar servidores e equipamentos destinados a efetuar armazenamento de informações), liberando acesso apenas aos IPs de cada servidor.

Os dados que passam por esta conexão, são *logs* (arquivos de registro de dados) do MySQL que servem para manter os dois servidores espelhados, ou seja, toda a informação alterada no cartório é replicada automaticamente para o servidor instalado no *datacenter* (local projetado para armazenar servidores e equipamentos destinados a efetuar armazenamento de informações), configurado em uma outra localidade.

Para o cenário proposto neste trabalho serão utilizados três servidores com sistema operacional Linux instalada a distribuição Ubuntu 16.04.2 LTS, os três serão virtualizados com o VMware Workstation 12 Player.

Um dos servidores será utilizado como servidor de VPN e ficará alocado na empresa que presta suporte para o cliente, ele vai utilizar duas placas de rede, uma para sua rede interna com o IP: 192.168.0.1 e outra para acesso a *internet* (rede mundial de computadores) e saída para a VPN com o IP: 192.168.25.215. Ele terá acesso a monitorar a replicação do cliente com o *datacenter* (local projetado para armazenar servidores e equipamentos destinados a efetuar armazenamento de informações).

O segundo servidor será o servidor do cliente que fica em um cartório e utiliza o MySQL 5.5 como banco de dados de sua aplicação local, este é o servidor principal e gera *logs* (arquivos de registro de dados) de todas as alterações efetuadas em seu banco de dados. Ele utiliza duas placas de rede, uma para sua rede interna com o IP: 192.168.10.1 e outra para acesso a *internet* (rede mundial de computadores) e saída da VPN com o IP: 192.168.25.44.

O terceiro servidor será um servidor alocado em um *datacenter* (local projetado para armazenar servidores e equipamentos destinados a efetuar armazenamento de informações) e terá o banco de dados instalado como replicação do servidor principal, ele se encontra em uma localidade diferente do cliente e servirá como *backup* (copia de segurança) do banco de dados em tempo real. Vai utilizar duas placas de rede, uma para sua rede local com o IP: 192.168.20.1 e outra para acesso a *internet* (rede mundial de computadores) e saída da VPN com o IP: 192.168.25.144.

Na figura 1 podemos visualizar o cenário proposto neste trabalho, detalhando as configurações para um entendimento mais fácil.

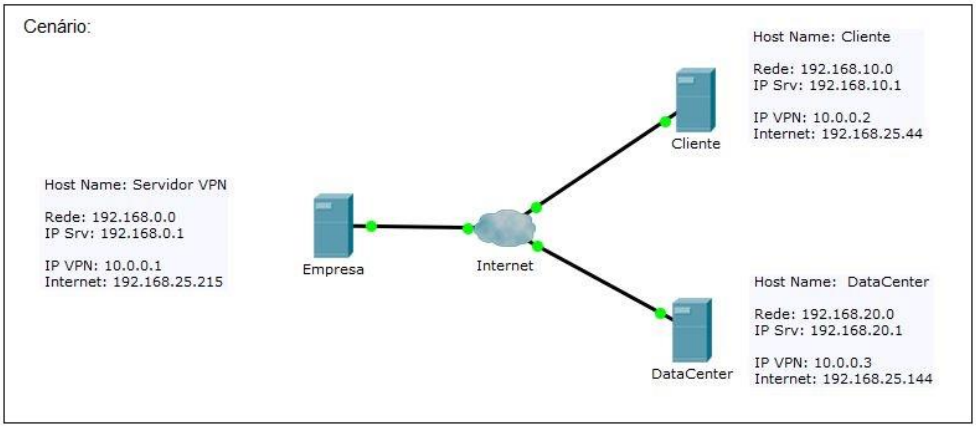

Figura 1 - Cenário do trabalho
Fonte: Própria autoria.

3.1 INSTALAÇAO E CONFIGURAÇÃO DO BANCO DE DADOS

Todos os procedimentos para a instalação e configuração do banco de dados MySQL foram retirados do site da empresa que disponibiliza o aplicativo, no caminho: http://www.mysql.com/.

Para instalar o banco de dados é necessário acessar a página da *internet* (rede mundial de computadores) da MySQL no caminho: http://www.mysql.com, selecionar a opção *downloads* (transferências) e escolher as versões do *community*

(comunidade), para este trabalho foi utilizada a versão 5.5.46 no formato *compressed arquive* (arquivo comprimido). Para baixar o instalador é necessário ter cadastro na página da *internet* (rede mundial de computadores) da MySQL, o qual pode ser feito gratuitamente. Seguem as telas do site onde foi baixado o aplicativo e a versão utilizada.

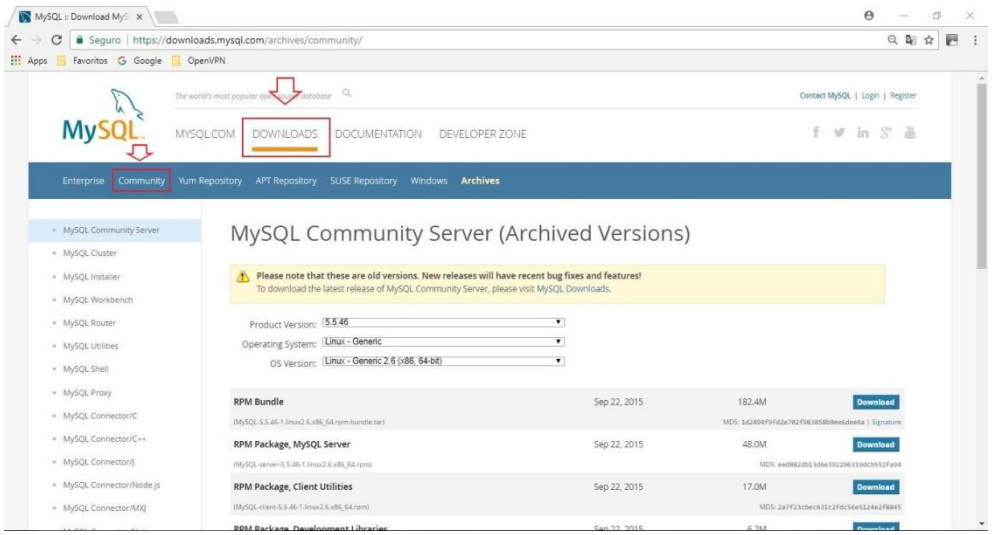

Figura 2 - Local para baixar o MySQL
Fonte: Página da internet da empresa MySQL.

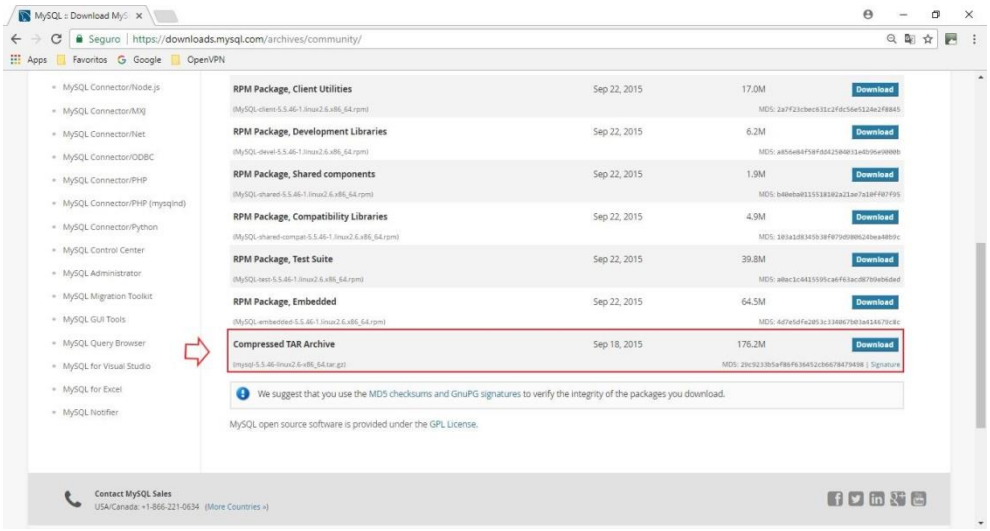

Figura 3 – Versão do MySQL baixado
Fonte: Página da internet da empresa MySQL.

3.1.1 Instalação no servidor principal

Para efetuar a instalação do banco de dados MySQL 5.5 no servidor do cliente deixando ele configurado como servidor principal, gerando os *logs* (arquivos de registro de dados) das alterações executadas no banco, seguir os passos abaixo:

Baixar o aplicativo da página da internet (rede mundial de computadores) da MySQL, copiar o arquivo: mysql-5.5.46-linux2.6-x86_64.tar.gz no caminho: /usr/local/ no servidor, descompactar o arquivo, mover a pasta descompactada para a pasta mysql e deixar o usuário root como proprietário da pasta, para isto utilizar os seguinte comandos:

Exemplos

```
root@Cliente:/usr/local# tar -zvxf mysql-5.5.46-linux2.6-x86_64.tar.gz
root@Cliente:/usr/local# mv mysql-5.5.46-linux2.6-x86_64.tar.gz mysql
root@Cliente:/usr/local# chown root:root -R mysql
```

Dentro da pasta mysql que acabou de ser descompactada, há uma pasta com o nome *support-files* (arquivos de suporte), onde se encontram os modelos dos arquivos de configuração do MySQL para servidores de pequeno, médio e grande porte. Utilizar o modelo que se adaptar melhor as necessidades. Efetuar as customizações caso seja necessário, ajustando para um melhor desempenho. O arquivo modelo é todo comentado para ajudar nesta customização.

Para que este servidor seja configurado como principal e crie os *logs* (arquivos de registro de dados) das alterações efetuadas em seus dados, gerando arquivos que serão transferidos para o servidor de replicação, precisa ser adicionado no final do seu arquivo de configuração as seguintes linhas:

Exemplos

```
# Replication Server

log-bin                 = /banco/replication/logbin
max_binlog_size         = 10M
log-bin-index           = /banco/replication/logbin.index
```

Ao concluir as alterações deixar o arquivo com o nome my.cnf e mover para a pasta /etc, devido a restrições do MySQL, é necessário alterar as permissões do

arquivo my.cnf, para isso acessar a pasta /etc e alterar as permissões, utilizar os seguintes comandos:

Exemplos

---

root@Cliente:/usr/local/mysql/support-files# mv my.cnf /etc
root@Cliente:/usr/local/mysql/support-files# cd /etc
root@Cliente:/etc# chmod 755 my.cnf

Para iniciar, acessar e parar o banco o Mysql seguem os comandos à ser utilizados na sequencia:

Exemplos

---

root@:/root# /usr/local/mysql/bin/mysqld_safe --defaults-file = /etc/my.cnf &
root@Cliente:/root# /usr/local/mysql/bin/mysql -uroot -p
root@Cliente:/root# /usr/local/mysql/bin/mysqladmin shutdown -uroot -p

---

3.1.2 Instalação no servidor de replicação

Para efetuar a instalação do banco de dados MySQL 5.5 no servidor de replicação, utilizar o instalador do servidor principal, copiar o arquivo mysql-5.5.46-linux2.6-x86_64.tar.gz para o caminho: /usr/local/ no servidor, descompactar o arquivo, mover a pasta descompactada para a pasta mysql e deixar o usuário root como proprietário, para isto utilizar os comandos neste sequencia:

Exemplos

---

root@Cliente:/usr/local# tar -zvxf mysql-5.5.46-linux2.6-x86_64.tar.gz
root@Cliente:/usr/local# mv mysql-5.5.46-linux2.6-x86_64.tar.gz mysql
root@Cliente:/usr/local# chown root:root mysql

Utilizar o my.cnf do servidor principal, alterando os parâmetros do *Replication Server* para *Replication Slave* conforme segue o modelo:

Exemplos

```
# Replication Slave

server-id = 2
log-warnings
max-relay-log-size = 10M
relay-log = /banco/logs/relaylog
relay-log-index = /banco/logs/relaylog.index
relay-log-info-file = /banco/logs/relaylog.info
master-info-file = /banco/logs/master.info
replicate-wild-ignore-table=test.%
replicate-wild-ignore-table=mysql.%
slave-skip-errors=all
slave_compressed_protocol=1
```

Ao concluir as alterações mover o arquivo my.cnf para a pasta /etc alterando as permissões conforme a necessidade do aplicativo, para isso seguem os comando a serem utilizados:

Exemplos

```
root@Cliente:/root# mv my.cnf /etc

root@Cliente:/root# chmod 755 /etc/my.cnf
```

Para iniciar, acessar e parar o banco de dados Mysql, seguem os comandos na sequencia:

Exemplos

```
root@:/root# /usr/local/mysql/bin/mysqld_safe --defaults-file=/etc/my.cnf &
root@Cliente:/root# /usr/local/mysql/bin/mysql -uroot -p
root@Cliente:/root# /usr/local/mysql/bin/mysqladmin shutdown -uroot -p
```

Para iniciar a replicação do banco de dados no servidor de replicação, é necessário conectar no banco e executar os comandos que seguem na sequencia apresentada:

Exemplos

```
mysql> change master to master_host ='10.0.0.2', master_user ='root', master_password ='root';
mysql> start slave;
```

Para verificar se a replicação esta funcional executar o comando:

Exemplo

```
mysql> show slave status;
```

3.2 INSTALAÇAO E CONFIGURAÇÃO DO OPENVPN

Todos os procedimentos para a instalação e configuração do OpenVPN foram retirados da página da *internet* (rede mundial de computadores) da empresa que disponibiliza o aplicativo, no caminho: https://openvpn.net/. A instalação nos servidores foi feita utilizando os repositórios padrões da distribuição do Ubuntu.

As figuras a seguintes mostram o local exato na da página da *internet* (rede mundial de computadores) da empresa OpenVPN onde é possível encontrar as informações de instalação e configuração do aplicativo para o servidor e para o cliente.

Figura 4 - Instalação do OpenVPN

Fonte: Página da internet da empresa OpenVPN.

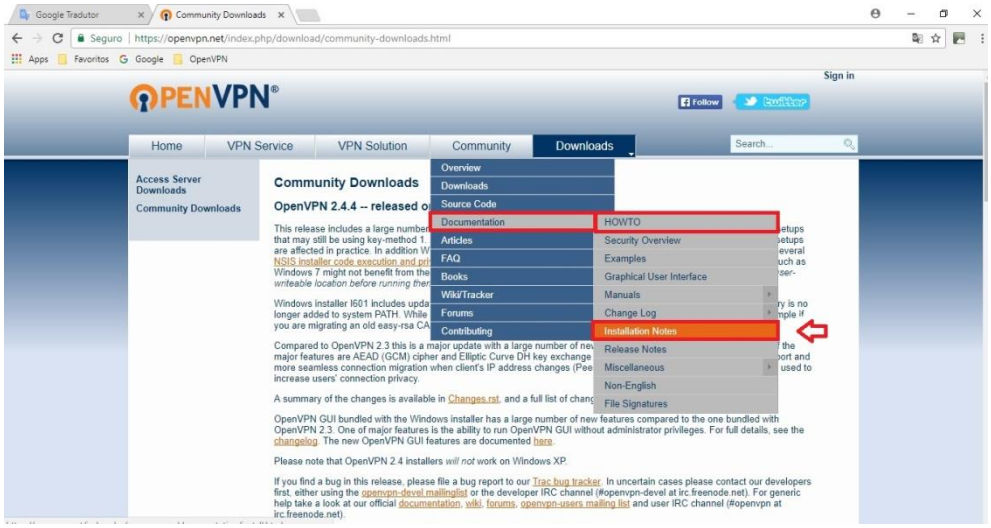

Figura 5 – Configuração do OpenVPN
Fonte: Página da internet da empresa OpenVPN.

3.2.1 Instalação do servidor

Para instalar o servidor do OpenVPN é necessário, atualizar repositórios da distribuição do Ubuntu, instalar o aplicativo, o OpenSSL e os *scripts* (roteiros) para configurar a unidade certificadora, chaves entre outros. Seguem os comandos a serem executados na sequencia necessária para sua instalação:

Exemplos

---

root@ServidorVPN:/ # apt-get update

root@ServidorVPN:/ # apt-get install openvpn

root@ServidorVPN:/ # apt-get install openssl

root@ServidorVPN:/ # apt-get install easy-rsa

Na ordem em que foram executados os comandos, o primeiro comando atualiza os repositórios da distribuição, o segundo comando instala o OpenVPN na pasta /etc e o terceiro comando instala o SSL *(Secure Sockets Layer)* protocolo

proprietário da Netscape que provê uma conexão segura. Em seguida é executado o comando que instala os *scripts* (roteiros) para configurar a autoridade certificadora, chaves Diffie Hellman, chaves do servidor, clientes, entre outros, o caminho padrão para a criação do repositório é o:

Exemplo

root@ServidorVPN:/ # usr/share/easy-rsa

Após a instalação do aplicativo, é necessário copiar pasta easy-rsa que contem todos os *scripts* (roteiros) para sua instalação e configuração, para o caminho /etc/openvpn/*,* para isso segue o comando utilizado:

Exemplo

root@ServidorVPN:/ # cp -R /usr/share/easy-rsa/ /etc/openvpn/

Com o aplicativo instalado no servidor e disponibilizado no caminho correto, é necessário iniciar a sua configuração e para isso será utilizado uma sequencia de procedimentos, os quais serão detalhados na ordem de execução:

- Criar a autoridade certificadora para gerar o certificado raiz do servidor;
- Criar o certificado do servidor;
- Criar os certificados dos clientes;
- Criar o DH (Diffie Helman) para aumentar a segurança;

Para criar a autoridade certificadora e gerar o certificado raiz para o servidor OpenVPN executar os comandos abaixo na sequencia em que estão apresentados:

Exemplo

root@ServidorVPN:/etc/openvpn/easy-rsa# nano vars

Com este comando será possível editar as variáveis de ambiente utilizadas para gerar os certificados do servidor OpenVPN e dos clientes, segue algumas variáveis e sua função na aplicação, alterar conforme necessidade pessoal:

Exemplos

- *export KEY_SIZE* = 2048: Tamanho da chave de negociação TLS;
- *export CA_EXPIRE* = 3650: Tempo para expirar o certificado da Autoridade certificadora, tempo estipulado em dias. Tempo predefinido 10 anos;
- *export KEY_EXPIRE* = 3650: Tempo para expirar o certificado gerado, também estipulado em dias. Tempo predefinido 10 anos;
- *export KEY_COUNTRY*="*US*": Pais;
- *export KEY_PROVINCE*="*CA*": Estado;
- *export KEY_CITY*="*SanFrancisco*": Cidade;
- *export KEY_ORG*="*Fort-Funston*": Empresa;
- *export KEY_EMAIL*="*me@myhost.mydomain*": e-mail;
- *export KEY_OU*="*MyOrganizationalUnit*": Dominio;

Para este trabalho, as variáveis foram alteradas conforme segue:

Exemplos

- *export KEY_SIZE* = 2048
- *export CA_EXPIRE* = 365
- *export KEY_EXPIRE* = 365
- *export KEY_COUNTRY*="BR"
- *export KEY_PROVINCE*="PR"
- *export KEY_CITY*="Curitiba"
- *export KEY_ORG*="jllinformatica"
- *export KEY_EMAIL*="suporte@jllinformatica.com.br"
- *export KEY_OU*="jllinformatica”

Executar as variáveis de ambiente e limpar qualquer configuração feita anteriormente, para isso seguem os comandos:

Exemplos

---

root@ServidorVPN:/etc/openvpn/easy-rsa# source vars

root@ServidorVPN:/etc/openvpn/easy-rsa# ./clean-all

Para criar o certificado raiz CA, segue:

Exemplo

---

root@ServidorVPN:/etc/openvpn/easy-rsa# ./build-ca

Para este trabalho, as informações ficaram assim:

Exemplos

Country Name [BR]: BR

State or Province Name [PR]: PR

Locality Name [Curitiba]: Curitiba

Organization Name [jllinformatica]: jllinformatica

Organizational Unit Name [jllinformatica]: ServidorVPN

Common Name [CA]: ServidorVPN

Name [EasyRSA]:jllinformatica

Email Address [suporte@jllinformatica.com.br]: suporte@jllinformatica.com.br

---

Com isso será criado o diretório *keys* na pasta *easy-rsa* com os seguintes arquivos:

ca.crt;

ca.key;

index.txt;

serial

Criar o certificado do servidor utilizando o comando:

Exemplo

root@ServidorVPN:/etc/openvpn/easy-rsa# ./build-key-server ServidorVPN

Para este trabalho, as informações ficaram assim:

Exemplos

Country Name [BR]: BR
State or Province Name [PR]: PR
Locality Name [Curitiba]: Curitiba
Organization Name [jllinformatica]: jllInformatica
Organizational Unit Name [jllinformatica]: ServidorVPN
Common Name: ServidorVPN
Name [*EasyRSA*]:jllinformatica
Email Address [*email@domain.com*]: suporte@jllinformatica.com.br

Para criação do certificado, é necessário confirmar a data de validade do certificado e a confirmação de sua criação.

Para criar o certificado do datacenter utilizar o comando:

Exemplo

root@ServidorVPN:/etc/openvpn/easy-rsa# ./build-key DataCenter

Para este trabalho, as informações ficaram assim:

Exemplos

Country Name [BR]: BR
State or Province Name [PR]: PR
Locality Name [Curitiba]: Curitiba
Organization Name [jllinformatica]: jllInformatica
Organizational Unit Name [jllinformatica]: DataCenter
Common Name: DataCenter

Name [EasyRSA]:jllinformatica
Email Address [*email@domain.com*]: suporte@jllinformatica.com.br

Para criação do certificado, é necessário confirmar a data de validade do certificado e a confirmação da criação.

Para criar o certificado do cliente utilizar o comando:

Exemplo

root@ServidorVPN:/etc/openvpn/easy-rsa# ./build-key cliente

Para este trabalho, as informações ficaram assim:

Exemplos

Country Name [BR]: BR
State or Province Name [PR]: PR
Locality Name [Curitiba]: Curitiba
Organization Name [jllinformatica]: jllInformatica
Organizational Unit Name [jllinformatica]: cliente
Common Name: cliente
Name [*EasyRSA*]:jllinformatica
Email Address [*email@domain.com*]: suporte@jllinformatica.com.br

Para criação do certificado, é necessário confirmar a data de validade do certificado e a confirmação da criação.

Para concluir, executar o comando build-dh que aumenta a segurança entre o servidor e cliente no momento da conexão em que são trocadas as chaves de forma segura confirmando os certificados. Utilizar o comando:

Exemplo

root@ServidorVPN:/etc/openvpn/easy-rsa/keys# ./build-dh

Agora que já foram criadas as chaves e certificados necessários para a configuração da VPN, é necessário disponibilizar estas chaves e certificados no local correto. Precisa criar a pasta key no servidor dentro da pasta /etc/openvpn e colocar os arquivos ca.crt, dh1024.pem, ServidorVPN.crt, ServidorVPN.key nesta pasta, para isto utilizar os comandos:

Exemplos

---

root@ServidorVPN:~# mkdir /etc/openvpn/keys
root@ServidorVPN:~# cd /etc/openvpn/easy-rsa/keys/
root@ServidorVPN:/.../keys# cp -a ca.crt dh1024.pem servidor.crt servidor.key /etc/openvpn/keys

---

Agora que o OpenVPN esta instalado, os certificados foram criados, os arquivos estão disponibilizados no caminho correto, é necessário configurar os parâmetros da VPN que será utilizada neste servidor. Para isso é necessário copiar e descompactar o arquivo server.conf.gz localizado no diretório /usr/share/doc/openvpn/examples/sample-config-files na pasta /etc/openvpn, para isto utilizar os comandos:

Exemplos

---

root@ServidorVPN:~# cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn
root@ServidorVPN:~# cd /etc/openvpn
root@ServidorVPN:/etc/openvpn# gunzip server.conf.gz

Editar este arquivo, utilizando um editor do Linux, neste trabalho este arquivo foi editado com o editor nano, segue as linhas do arquivo e um pequeno comentário sobre sua funcionalidade:

Exemplos

---

local a.b.c.d: Aqui deve ser inserido o endereço local utilizado pelo OpenVPN;
port 1194: Porta utilizada pelo serviço do OpenVPN;
proto udp: Protocolo utilizado, pode ser TCP ou UDP;
dev tap: Cria um túnel ethernet;
dev tun: Cria um IP roteado, elimina pacotes de broadcast;
ca ca.crt: Indica o caminho do certificado da autoridade certificadora;
cert server.crt: Indica o caminho do certificado do servidor;
key server.key: Indica o caminho da chave do servidor;
dh dh2048.pem: Indica o caminho do arquivo Diffie Helman;
server 10.8.0.0 255.255.255.0: Define o IP e mascara da rede VPN;
ifconfig-pool-persist ipp.txt: Cria o arquivo ipp.txt com todos os ip's utilizados;
server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100: Cria um range de Ip's para ser utilizado como Bridge;
push "route 192.168.20.0 255.255.255.0": Permite criar uma rota para acesso a rede atrás do servidor;
cliente-to-client: Permite que os clientes tenham acesso uns aos outros;
cipher AES-128-CBC: Seleciona a criptografia utilizada;
comp-lzo: Habilita a compressão na comunicação VPN;
max-clients 100: Limita o numero máximo de clientes;
persist-key: Mantem a chave;
persist-tun: Mantem o túnel;
log openvpn.log: cria um log com o nome openvpn.log;

Agora que esta instalada e configurada a VPN no servidor, utilizar os comandos que seguem para iniciar e parar a mesma:

Exemplos

---

root@ServidorVPN:/etc/openvpn# /etc/init.d/openvpn start
root@ServidorVPN:/etc/openvpn# /etc/init.d/openvpn stop

3.2.2 Instalação do cliente

Para instalar o cliente OpenVPN é necessário, atualizar repositórios da distribuição do Ubuntu e instalar o aplicativo. Para isso utilizar os comandos a seguir:

Exemplo

---

root@ServidorVPN:/ # apt-get update
root@ServidorVPN:/ # apt-get install openvpn

Após instalado o aplicativo como cliente, é necessário colocar os arquivos de configuração na pasta /etc/openvpn. Estes arquivos serão encontrados no servidor OpenVPN e são os seguintes:

- ca.crt;
- dh1024.pem;
- cliente.crt;
- cliente.key

Agora que esta instalada e configurada a VPN no servidor, utilizar os comandos que seguem para iniciar e parar a mesma:

Exemplo

---

root@ServidorVPN:/etc/openvpn# /etc/init.d/openvpn start
root@ServidorVPN:/etc/openvpn# /etc/init.d/openvpn stop

Com isso concluímos a instalação do OpenVPN no cliente.

4 RESULTADOS

Após a implantação da VPN foi feito uma comparação de tempo gasto ao executar um ping do servidor do cliente para o data center, utilizando a VPN e sem utilizar a VPN, foi executado o comando ping enviando 5 pacotes e com 1000 bytes, e com a resposta deste comando foi gerado a tabela de comparação.

Tabela 1 – Comparação de tempo gasto na utilização da VPN

Estatistica:	Tempo com VPN	Tempo sem VPN
Mínima	1,11 ms	0,30 ms

Média	2,29 ms	0,57 ms
Máxima	2,70 ms	0,94 ms

Fonte: Própria autoria

Com esta comparação foi verificado que em média a conexão fica aproximadamente 35% mais lenta, utilizando a VPN, o que justifica seu uso devido a toda segurança proporcionada.

5 CONCLUSÃO

Há uma exigência legal de alguns estados brasileiros que obriga o cliente a ter uma copia de seu banco de dados fora do seu estabelecimento, devido aos problemas encontrados com sequestro de informações, ou mesmo a vulnerabilidade em relação às mídias de armazenamento utilizadas atualmente.

Com a necessidade constante da redução de custos, este trabalho explica como configurar uma replicação entre dois servidores de banco de dados utilizando *softwares* (programas) gratuitos, mantendo uma copia em tempo real do banco de dados em outra localidade.

A utilização de uma VPN na transferência de informações pela *Internet* (rede mundial de computadores) torna-se indispensável devido à segurança que

proporciona, ela cria um túnel criptografado entre as partes, dificultando a interpretação das informações transmitidas.

Desta forma a solução apresentada neste trabalho é totalmente necessária e útil para os clientes que utilizam esta aplicação e querem garantir a redução de custos sem perder em relação à segurança.

6 REFERENCIAS BIBLIOGRAFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: Código de prática para a gestão da Segurança da Informação. Rio de Janeiro, 2005.

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança: O guia oficial RSA**. Rio de Janeiro: Campus, 2002.

CARUSO, Carlos A. A.; STEFFEN, Flavio D. **Segurança em informática e de informações**. 2. ed. São Paulo: Senac, 1999.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistema de banco de dados**. 6. ed. São Paulo: Pearson, 2011.

FILIPPETTI, Marco A. **CCNA 4.1: guia completo de estudos**. Florianópolis: Visual Books, 2008.

LAUREANO, Marcos A. P.; **Máquinas Virtuais e Emuladores - Conceitos, Técnicas e Aplicações**. São Paulo: Novatec, 2006.

NAKAMURA, Emilio T.; GEUS, Paulo Lício de **Segurança de redes: em ambientes corporativos**. 2. ed. São Paulo: Futura, 2003.

PETERSON, Larry L.; DAVIE, Bruce S.; **Redes de Computadores: uma abordagem de sistemas**. 3. ed. Rio de Janeiro: Campus, 2004.

SILBERSCHATZ, Abrahan; KORTH, Henry F.; SUDARSHAN, S. **Sistema de Banco de Dados**. 5. ed. Rio de Janeiro: Campus, 2006.

STALLINGS, Willian. **Criptografia e Segurança de Redes: princípios e praticas**. 6. ed. São Paulo: Pearson, 2014.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Campus, 1994.