UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE COMPUTAÇÃO
CURSO DE CIÊNCIA DA COMPUTAÇÃO

FELIPE JHONAS MELLER

COMPARATIVO DOS PROTOCOLOS IPSEC E SSL NA UTILIZAÇÃO DE VPNS CORPORATIVAS

TRABALHO DE CONCLUSÃO DE CURSO

MEDIANEIRA

2018

FELIPE JHONAS MELLER

COMPARATIVO DOS PROTOCOLOS IPSEC E SSL NA UTILIZAÇÃO DE VPNS CORPORATIVAS

Trabalho de Conclusão de Curso apresentado ao Departamento Acadêmico de Computação da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Bacharel em Computação".

Orientador: Prof. Dr. Neylor Michel

MEDIANEIRA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Graduação e Educação Profissional
Coordenação do Curso de Ciência da Computação

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TERMO DE APROVAÇÃO

COMPARATIVO DOS PROTOCOLOS IPSEC E SSL NA UTILIZAÇÃO DE VPNS CORPORATIVAS

Por

FELIPE JHONAS MELLER

Este Trabalho de Conclusão de Curso foi apresentado às 14:00h do dia 12 de junho de 2018 como requisito parcial para a obtenção do título de Bacharel no Curso de Ciência da Computação, da Universidade Tecnológica Federal do Paraná, Câmpus Medianeira. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____

Prof. Dr. Neylor Michel
UTFPR - Câmpus Medianeira

_____

Prof. Dr. Nelson Miguel Betzek
UTFPR - Câmpus Medianeira

_____

Prof. Msc. Hamilton Pereira da Silva
UTFPR - Câmpus Medianeira

A folha de aprovação assinada encontra-se na Coordenação do Curso.

RESUMO

MELLER, Felipe Jhonas. COMPARATIVO DOS PROTOCOLOS IPSEC E SSL NA UTILIZAÇÃO DE VPNS CORPORATIVAS. 59 f. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Tecnológica Federal do Paraná. Medianeira, 2018.

A Internet tornou-se uma infraestrutura de baixo custo, porém é um ambiente de comunicação inseguro. As redes privadas virtuais (VPNs) são usadas por muitas organizações para fornecer comunicações seguras e confidenciais em redes não confiáveis, sendo uma opção economicamente viável para atender a essa necessidade. Utiliza combinação de fortes tecnologias de criptografia e autenticação. Os dados são protegidos na forma de um túnel criptografado para transmitir através da internet, este túnel liga dois pontos definidos. Uma VPN fornece ao usuário final garantia de autenticidade e confidencialidade dos pacotes de dados. Objetiva-se deste trabalho apresentar a implementação de VPNs com as duas principais tecnologias usadas atualmente, os protocolos IPSec e SSL. Foi necessário configurar e implementar alguns protocolos de Internet e segurança. Neste trabalho conclui-se que não é possível realizar uma comparação justa de desempenho devido a metodologia de implementação que foi utilizada ser em ambiente virtual, mas atende o objetivo de apresentar o funcionamento e a implementação de VPNs para tornar o meio de comunicação de dados das empresas seguro. Conclui-se que não é possível realizar uma comparação de desempenho e segurança entre as VPNs devido a metodologia utilizada para o desenvolvimento deste trabalho.

Palavras-chave: tunelamento, criptografia, segurança de dados

ABSTRACT

MELLER, Felipe Jhonas. COMPARISON OF IPSEC AND SSL PROTOCOLS IN USING CORPORATE VPNS. 59 f. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Tecnológica Federal do Paraná. Medianeira, 2018.

The Internet has become a low-cost infrastructure, but it is an environment of unsafe communication. Virtual private networks (VPNs) are used by many organizations to provide secure and confidential communications over untrusted networks and are an economically viable option to meet this need. Uses combination of strong encryption and authentication technologies. The data is protected in the form of an encrypted tunnel to transmit over the internet, this tunnel connects two defined points. A VPN provides the end user with assurance of authenticity and confidentiality of the data packets. The objective of this work is to present the implementation of VPNs with the two main technologies currently used, the IPSec and SSL protocols. It was necessary to configure and implement some Internet and security protocols. In this work it is concluded that it is not possible to perform a fair comparison of performance due to the implementation methodology that was used in a virtual environment, but it serves the purpose of presenting the operation and the implementation of VPNs to make the data communication medium of the companies insurance. It is concluded that it is not possible to perform a performance and security comparison between VPNs due to the methodology used for the development of this work.

Keywords: tunneling, encryption, data security

Ao Curso de Ciência da Computação, e às pessoas com que convivi nesse ambiente da Universidade ao longo desses anos. A experiência de uma produção compartilhada com amigos foram a melhor experiência da minha formação acadêmica. Agradeço em especial a colega Gabriela, que esteve do meu lado durante esses anos, sempre me motivando e ajudando a conquistar meus objetivos.

LISTA DE SIGLAS

AAA	Authentication Authorization Accounting
AC	Autoridade Certificadora
ACL	Lista de Controle de Acesso
AES	Advanced Encryption Standard
AH	Authentication Header
AR	Autoridade Registradora
CLI	Comand-Line Interface
CPU	Central Processing Unit
DES	Data Encryption Standard
DH	Diffie-Hellman
ESP	Encapsulation Security Payload
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ITI	Instituto Nacional de Tecnologia da Informação
LAN	Local Area Network
MAC	Message Authentication Code
MD5	Message Digest 5
MTU	Maximum Transmission Unit
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
RAS	Remote Access Server
RSA	Rivest-Shamir-Adleman
SA	Security Association
SADB	Security Association Data Base
SEAL	Software Optimized Encryption Algorithm
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
SVC	SSL VPN Client
TFTP	Trivial File Transfer Protocol
URL	Uniform Resource Locator
WAN	Wide Area Network

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Soluções, tais como os vários métodos de criptografia e *Public Key Infrastructure* (PKI) permitem que as empresas possam estender com segurança as suas redes através da Internet. Uma maneira em que as empresas podem realizar esta extensão é por meio de *Virtual Private Networks* (VPNs).

As organizações utilizam VPNs para criar uma conexão de rede privada por meio de redes de terceiros, tais como a Internet ou extranets, em uma espécie de túnel. O túnel elimina a barreira da distância e permite que usuários remotos acessem recursos de rede local centrais. No entanto, VPNs não podem garantir que a informação permanece segura ao atravessar o túnel. Por esta razão, são aplicados protocolos de criptografia nas VPNs para estabelecer conexões de forma segura e privada.

Uma VPN é dada por meio do estabelecimento de uma conexão virtual ponto-a-ponto, utilizando-se de conexões dedicadas, protocolos de encapsulamento virtuais, ou criptografia de tráfego (SHARMA, 2015). A VPN estende-se de uma rede privada por meio de uma rede pública, como a Internet, permitindo que um computador ou dispositivo envie e receba dados por meio de redes compartilhadas ou públicas, como se estivesse conectado diretamente à rede privada, se beneficiando da funcionalidade, segurança e das políticas de gerenciamento da rede privada. O ambiente de comunicação da VPN, tem o acesso rigorosamente controlado para permitir conexões de pares dentro de uma comunidade de interesse definida. A confidencialidade é obtida por criptografar o tráfego dentro desse ambiente.

Criptologia é a ciência de codificar os dados de comunicação e de armazenamento de forma segura e preferencialmente secreta, que engloba criptografia e criptoanálise. O desenvolvimento e a utilização de códigos são chamados de criptografia e a recuperação dos dados codificados sem a chave denomina-se criptoanálise (ACADEMIC, 2016). Os princípios da criptologia podem ser usados para explicar como os protocolos e os algoritmos são utilizados para proteger as comunicações (CISCO, 2012).

Algoritmos de criptografia simétrica são baseados na premissa de que cada uma das partes que estabeleceram a conexão para se comunicar sabem a chave, uma chave pré-compartilhada (*Pre-Shared Key* ou PSK), usando um canal seguro. Algoritmos de criptografia

assimétrica baseiam-se no pressuposto de que as duas partes que se comunicam ainda não tenham compartilhado um segredo e deve estabelecer um método seguro para fazê-lo.

O acesso remoto VPN permite que usuários individuais possam estabelecer conexões seguras com uma rede remota. Os usuários podem acessar os recursos seguros da rede conectada, como se estivessem diretamente conectados aos servidores da rede. Existem dois métodos principais para implantar VPNs de acesso remoto: Secure Sockets Layer (SSL); e Internet Protocol Security (IPsec).

O protocolo IPsec fornece uma estrutura para configurar VPNs seguras e é comumente implantado por meio da Internet para conectar filiais, funcionários remotos e parceiros de negócios. É uma maneira confiável para manter a privacidade da comunicação, enquanto simplificação das operações, reduzindo custos e permitindo a administração de rede flexível. Internet Protocol Security é um padrão IETF (RFC 2401-2412) que define como um VPN pode ser configurada usando o endereçamento IP protocolo. IPsec é uma estrutura de padrões abertos que explicita as regras para comunicações seguras. IPsec funciona na camada de rede do modelo OSI, protegendo e realizando autenticação de pacotes IP entre pares de dispositivos IPsec conectados.

Secure Socket Layer é um protocolo desenvolvido pela Netscape que permite que um navegador web e um servidor web possam se comunicar de forma segura. Ele permite que o navegador web faça autenticação do servidor web. O protocolo SSL requer um servidor web para ter um certificado digital instalado para que uma conexão SSL para ser feito. O funcionamento é dado utilizando uma chave pública para criptografar dados que são transferidos por meio da conexão SSL. Por convenção, o Uniform Resource Locator (URL) que requerem uma conexão SSL começam com https em vez de http (BHIOGADE, 2002).

Portanto, esse trabalho apresentará um estudo dos conceitos fundamentais de VPNs, comparação dos protocolos IPsec e SSL na implementação de uma VPN, a implementação de redes virtuais públicas em um ambiente real e a posterior ánalise em aspectos definidos e importantes, para contribuir e justificar o uso dos protocolos citados em VPNs para obtenção de acesso remoto de forma segura.

1.1 OBJETIVO GERAL

Realizar um estudo comparativo entre os protocolos IPsec e SSL na criação de VPN, analisando os requisitos de segurança e velocidade de transferência de arquivos, para apresentar uma solução de acesso remoto segura.

1.2 OBJETIVOS ESPECÍFICOS

Este trabalho será composto pelos seguintes objetivos específicos:

- descrever os conceitos fundamentais e tecnologias de VPNs;
- descrever os dois métodos de acesso remoto à rede comuns usados em redes corporativas utilizando IPsec e SSL;
- Implementar uma VPN usando o protocolo SSL;
- Implementar uma VPN usando o protocolo IPsec;
- avaliar os requisitos de segurança das VPNs, e realizar testes de velocidade de transferência de arquivos e utilização da Unidade Central de Processamento (CPU) dos roteadores.

1.3 JUSTIFICATIVA

A dinâmica de negócios modernos impõe padrões de comunicação mais exigentes e flexíveis. Há uma crescente necessidade de conectar-se aos computadores dentro da empresa ou para utilizar diferentes recursos do computador.

Considerando a troca de informações pela internet em redes públicas por uma empresa, os dados podem conter informações importantes e sigilosas, com a possibilidade de serem interceptados no caminho por um dispositivo que tenha acesso a essa mesma rede, já que é uma rede pública, por isso é preciso usar ferramentas que aumentam a segurança da transmissão

desses dados, como uma VPN.

Uma VPN fornece o nível mais elevado possível de segurança através de túneis criptografados de VPNs de IPSec e SSL e tecnologias de autenticação. Elas protegem dados que atravessam a VPN de acesso não autorizado. As empresas podem aproveitar a infraestrutura da Internet de fácil provisão da VPN para adicionar rapidamente novos pontos ou usuários, e também podem aumentar o alcance da VPN sem expandir consideravelmente a infraestrutura.

Cada realidade de negócios demanda necessidades especificas, acredita-se que este trabalho possa oferecer uma solução viável de acesso remoto e ajudar em qual protocolo dos apresentados seria mais indicado para a empresa interessada.

2 REFERENCIAL TEÓRICO

Neste capitulo apresenta-se o que são redes privadas virtuais (VPNs), e como as técnicas de criptografia são utilizadas para obter segurança e outras funcionalidades essenciais. Este capitulo também é utilizado para mostrar como o protocolo IPsec e o SLL são utilizados na criação de uma VPN e todo o seu funcionamento interno.

2.1 PUBLIC KEY INFRASTRUCTURE

As organizações utilizam uma infraestrutura de chave pública (Public-Key Infrastructure - PKI) para suportar os processos internos de negócios, implementar redes privadas virtuais, e proteger arquivos corporativos.

Atualmente existe grande aceitação e utilização da tecnologia de chave pública. Protocolos de rede e aplicações utilizam para garantir forte autenticação e privacidade. No entanto, existe o problema da alta complexidade para configurar uma PKI em uma empresa que tem relações com entidades externas.

Dentro de uma arquitetura de segurança, uma PKI é essencial para o gerenciamento dos certificados digitas e todas suas funções, quando o ambiente é caracterizado pela complexidade das conexões e pelos diferentes níveis de usuários que têm de ser autenticados e controlados (NAKARUMA; GEUS, 2007). PKI é o mecanismo de segurança criptográfica subjacente para certificados digitais e diretórios certificados, que são usadas para autenticar o remetente da mensagem(MISRA et al., 2016).

A PKI é uma estrutura para a distribuição e identificação de chaves públicas e certificados. A PKI é responsável pela emissão, manutenção e revogação por meio de redes inseguras. Permite que os usuários troquem dados pela rede externa com o uso de um par de chaves pública e privada que é obtida e compartilhada por meio de uma autoridade confiável para verificar a identidade das partes que estão se comunicando(ZHANG et al., 2009a).

A PKI refere-se a um ambiente em que o conjunto de pessoas, computadores, e entidades de rede possuem chaves públicas e privadas, utilizando algum protocolo que transmita para outros esse conhecimento das chaves públicas de uma maneira confiável (CHESWICK et al., 2005). Com isso, torna-se uma forma segura e eficiente para fornecer chaves privadas e gerenciar certificados de chave pública, permitindo assim o uso de autenticação, e confidencialidade nos serviços de segurança (GÓMEZ et al., 2003).

Segundo Silva (2004), as aplicações em uma infraestrutura de chave pública operam com as seguintes características:

- autenticação – Identificação das partes envolvidas no processo;
- privacidade – As informações são compreensíveis exclusivamente para os pares na comunicação;
- integridade – As informações não podem ser modificadas em trânsito na rede;
- não-repúdio – A autoria das comunicações não pode ser contestada;
- autorização - As informações são acessíveis exclusivamente para entidades credenciadas;
- auditoria – Todas as etapas do processo podem e devem ser auditadas.

O Comitê Gestor da Infra-estrutura de Chave Publica-Brasil estabelece a política, os critérios e as normas para licenciamento de Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviços de suporte em todos os níveis da cadeia de certificação, credenciando as respectivas empresas na emissão de certificados no meio digital brasileiro.

2.1.1 Autoridade Certificadora e Autoridade Registradora

O Instituto Nacional de Tecnologia da Informação (ITI) é a Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil. A Autoridade Certificadora tem como função emitir certificados digitais. Diversos tipos de entidades, como: pessoa, computador, empresa, podem ter esses certificados digitais emitidos.

A autoridade certificadora é responsável por gerar um certificado para um usuário com nome único, em todo o seu sistema, chamado de Nome Distinto (Distinguished Name - DN), e associar a ele sua chave pública, obrigatória para comprovação da sua identidade.

Segundo Silva (2004), o certificado contém uma assinatura digital da AC, para gerar um relacionamento de confiança entre a entidade que deseja confirmar a identidade de um

usuário. Qualquer entidade que confiar na autenticidade da AC, irá confiar no conteúdo dos certificados emitidos por ela, consequentemente na identidade dos usuários que tiverem seu certificados digitais emitidos pela AC.

Uma AR é responsável pela interface entre o usuário e a AC. A AR pode ter duas atribuições bem claras e específicas, que são fornecer os mecanismos para adicionar novos usuários na AC, e verificar os dados de um certificado para uma AC. Mais detalhadamente tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes.

2.2 CRIPTOGRAFIA

Segundo Silva (2004) tentar impedir alguém de capturar um pacote que trafega em vários equipamentos como roteadores, switches e computadores é extremamente difícil. A criptografia é a ciência de manter as mensagens seguras, que tem importância fundamental para a segurança da informação, ao servir de base para as diversas tecnologias e protocolos. As propriedades da criptografia garantem o armazenamento, as comunicações e transações seguras, essenciais no mundo atual (NAKARUMA; GEUS, 2007). A criptografia provavelmente é o aspecto mais importante da segurança de comunicações e está se tornando cada vez mais importante como um componente básico para a segurança do computador (COUNCIL, 1991).

Segundo Moreno e Chiaramonte (2005) a criptografia pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível. Stallings (2008), Moreno e Chiaramonte (2005) afirmam que os algoritmos são baseados em dois princípios gerais, a substituição em que cada elemento no texto claro é mapeado em outro, e a transposição em que os elementos são reorganizados. O requisito fundamental é que nenhuma informação seja perdida nesse processo. As pessoas autorizadas podem ter acesso às informações originais mediante o processo inverso conhecendo o processo de cifragem .

A cifragem (*encryption*) é o processo de disfarçar a mensagem original, o texto claro (*plaintext*), de tal modo que sua substância é escondida em uma mensagem com texto cifrado (*ciphertext*), enquanto a decifragem (*decryption*) é o processo de transformar o texto cifrado de volta em texto claro original (SCHNEIER, 1996; KAPOOR et al., 2011).

Os processos de cifragem e decifragem são realizados via uso de algorítimos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos

cifrados, que são ilegíveis. Segundo Terada (2008) algoritmos criptográficos basicamente objetivam esconder informações sigilosas que qualquer pessoa mal-intencionada que não tenha conhecimento da chave secreta de criptografia.

Segundo Nakaruma e Geus (2007) a criptografia possibilita que as propriedades importantes para a proteção da informação sejam alcançadas, dentre elas :

- autenticidade – garantir que a mensagem não é uma falsificação, que vem da fonte que afirma vir;
- integridade – garantir que não seja alterada ou interceptada a mensagem;
- confidencialidade - garantir que não seja decifrada a mensagem quando capturada.

O problema existente está na necessidade de distribuição das chaves secretas a serem utilizadas pelos usuários, que deve ser feita de maneira segura, pela dificuldade de enviar a chave gerada para o usuário, pois o canal de comunicação não é seguro (NAKARUMA; GEUS, 2007).

2.3 VIRTUAL PRIVATE NETWORK

Uma rede virtual privada (VPN) é um meio para transmitir com segurança e privacidade dados por meio de uma infraestrutura de rede não segura e compartilhada. VPNs protegem os dados transmitidos por encapsular ou criptografar. O encapsulamento é muitas vezes referido como túneis, porque os dados são transmitidos a partir de uma rede para outra de forma transparente por meio de uma infraestrutura de rede pública. Normalmente, uma VPN é uma conexão protegida entre duas entidades (dispositivos específicos ou redes particulares) que não estão necessariamente ligados diretamente (NIEMIEC; MACHNIK, 2016).

As VPNs por permitirem que as conexões dedicadas sejam substituídas pelas conexões públicas exercem uma importância fundamental para as organizações, principalmente no seu aspecto econômico. Também é possível obter economia com a substituição das estruturas de conexões remotas, que podem ser eliminadas em função da utilização dos clientes e provedores VPN (NAKARUMA; GEUS, 2007). As tecnologias VPN podem ser classificados em termos gerais sobre estes modelos de conexão lógica como VPNs de Camada 2 ou VPNs de Camada 3 (CISCO, 2012).

As organizações utilizam VPNs para criar uma conexão de rede privada *end-to-end* (túnel) por meio de redes de terceiros, tais como a Internet ou extranets. O túnel elimina a

barreira da distância e permite que usuários remotos acessem recursos de rede local centrais. No entanto, VPNs não podem garantir que a informação permanece segura ao atravessar o túnel. Por esta razão, os métodos de criptografia são aplicadas a VPNs para estabelecer conexões de rede *end-to-end* segura e privada (CISCO, 2012).

Segundo Niemiec e Machnik (2016) uma boa solução de VPN deve abordar todos os seguintes problemas:

- proteger os dados dos interceptadores, usando criptografia;
- proteger pacotes de adulterações usando funções *hash* para assegurar a integridade do pacote;
- proteger contra ataques *man-in-the-middle*, usando mecanismos de autenticação de identidade;
- proteção contra ataques de repetição, usando números de sequência durante a transmissão de dados protegidos;
- definir a mecânica de como os dados são encapsulados e protegidos, e como o tráfego protegido é transmitido entre os dispositivos;
- definir qual trafego realmente precisa ser protegido.

Uma VPN é uma rede privada que serve para estabelecer um canal seguro através da criação de um tunelamento de uma rede pública. O tunelamento é definido por Yuan e Strayer (2001) como uma estrutura de camadas de protocolos repetidas, de maneira que uma topologia virtual é criada sobre a topologia física.

Por meio desse tunelamento, usuários, parceiros de negócios, escritórios da mesma empresa, podem trocar informações de forma confiável usando conexões virtuais roteadas a partir da organização para o site remoto. A VPN agregou um grande benefício à Internet, porque permitiu utilizar a rede pública de uma forma privada sem comprometer e expor a informação (SILVA, 2004).

Uma VPN é um ambiente de comunicações em que o acesso é rigorosamente controlado para permitir conexões de pares dentro de uma comunidade definida de interesse. Segundo Nakaruma e Geus (2007) a criptografia é utilizada para garantir a autenticidade, o sigilo e a integridades das conexões de uma VPN. VPNs tem muitos benefícios:

- redução de custos - VPNs permitem que as organizações usem redes de terceiros para transporte de dados com baixo custo, conectando escritórios e usuários remotos ao site corporativo principal. Segundo Nakaruma e Geus (2007) as conexões privadas e as estruturas de acesso remoto têm custos mais elevados. Silva (2002) diz que talvez o principal benefício da VPN seja o próprio custo envolvido, existe uma grande vantagem comparando com a rede privada baseada em linha dedicada;

- segurança - VPNs fornecem o mais alto nível de segurança usando criptografia e autenticação com protocolos avançados que protegem os dados contra acesso não autorizado. A VPN deve proteger os dados enquanto ele está viajando na rede pública. Se intrusos tentarem capturar os dados, eles devem ser incapazes de ler ou usá-lo. Silva (2004) apresenta que a autenticação por meio de certificados digitais é o mais escalonável e confinável método disponível, que é usado como base de autenticação na VPN;
- escalabilidade - Como uma empresa cresce, ela deve ser capaz de estender seus serviços de VPN para lidar com esse crescimento sem substituir a tecnologia VPN . Silva (2002) afirma que pode-se de forma fácil adicionar filiais ou usuários remotos à medida que for necessário para o negócio da empresa;
- compatibilidade com a tecnologia de banda larga - VPNs permitem que os trabalhadores móveis, telecomunicações, e as pessoas que desejam estender sua jornada de trabalho para aproveitar a alta velocidade, conectividade de banda larga para obter acesso a suas redes corporativas, fornecendo trabalhadores flexíveis de forma eficiente. Conexões de banda larga de alta velocidade fornecem uma solução de custo eficaz para conectar escritórios remotos;
- confiabilidade - Os funcionários e escritórios remotos devem ser capazes de conectar-se a VPN sem problemas a qualquer momento, e a VPN deve proporcionar a mesma qualidade de conexão para cada usuário, mesmo quando se está a lidar com seu número máximo de conexões simultâneas.

Como mencionado anteriormente, para evitar a espionagem dos dados em uma VPN é necessário criptografar os dados. A encriptação de dados é alcançada através da implantação de dispositivos de criptografia em cada local.

Existem dois tipos básicos de redes VPN site-to-site (*gateway-to-gateway*) e de acesso remoto (*client-to-gateway*) (CISCO, 2012; NAKARUMA; GEUS, 2007; LAKBABI et al., 2012) :

- um *site-to-site* VPN é criado quando os dispositivos de conexão em ambos os lados da conexão VPN está ciente da configuração com antecedência. Silva (2002) fala que o tráfego protegido pelo túnel VPN é totalmente transparente ao usuário de dentro da rede;
- uma VPN de acesso remoto é criado quando a informação VPN não está estaticamente configurado, mas em vez disso permite que a informação seja dinâmica e pode ser ativada e desativada. Silva (2002) apresenta que esta conexão não é transparente, porque é necessária uma fase de estabelecimento de sessão entre o equipamento do usuário e o servidor ao qual se deseja estabelecer a VPN.

Esses dois modelos de redes VPNs apresentados anteriormente vão ser detalhados na

sequencia.

2.3.1 Site-to-Site VPN

Site-to-site VPN é um tipo de conexão VPN que é criado entre dois locais separados, duas redes remotas, tornando-se uma conexão permanente (LAKBABI et al., 2012). A VPN fornece a capacidade de conectar locais ou redes geograficamente separadas, geralmente por meio da ligação à Internet ou uma conexão de Rede de Longa Distância (WAN).

Uma VPN *site-to-site* é composto de dois ou mais VPN *Gateways* que podem se comunicar uns com os outros em um relacionamento bi-direcional. As redes conectadas funcionam como uma única rede. Estende a rede da empresa, fazendo com que os recursos do computador de um local estejam disponíveis para os funcionários em outros locais. Esse tipo de VPN pode ser usada para engrenar ramos de escritório em uma rede corporativa.

Existem dois tipos de VPNs de *site-to-site*:

- Intranet, se uma empresa tem um ou mais locais remotos que desejam ingressar em uma única rede privada (CISCO, 2012). Conecta a matriz a departamentos e filiais de uma mesma organização. Exige tecnologia de ponta que supra as conexões de grande velocidade além de confiabilidade suficiente em aplicações críticas (NAKARUMA; GEUS, 2007);
- Extranet, segundo Cisco (2012) e Nakaruma e Geus (2007) quando uma empresa tem uma relação estreita com outra empresa, como um parceiro estratégico, fornecedores ou clientes, pode construir uma VPN extranet que conecta as LANs dessas empresas. Este extranet VPN permite que as empresas possam trabalhar juntos em um ambiente de rede compartilhado seguro enquanto impede o acesso a suas intranets separadas. Ainda que a extranet requer a utilização de um protocolo de tunelamento para assegurar a interoperabilidade para evitar os gargalos e que a resposta as requisições de informações críticas sejam rápidas.

Segundo Silva (2002), as políticas de acesso, como por exemplo, definir quais usuários irão trafegar pela Internet e, dentre estes, quais irão inscrever-se no túnel VPN, são configuradas no *gateway* que irá permitir ou não o ingresso destes usuários. Os servidores são responsáveis por enviar e receber tráfego TCP / IP por meio de um *gateway* de VPN, que pode ser um roteador ou *firewall*. O *gateway* de VPN é responsável por encapsular e criptografar o tráfego de saída a

partir de um determinado site e enviá-lo através de um túnel VPN por meio da Internet para um *gateway* de VPN no local de destino. Após a recepção, o *gateway* VPN retira os cabeçalhos, descriptografa o conteúdo e retransmite o pacote para o host de destino dentro da sua rede privada (CISCO, 2012).

Mesmo que o propósito de uma VPN *site-to-site* é diferente da de uma VPN de acesso remoto, pode usar alguns dos mesmos software e equipamentos. Idealmente, porém, uma VPN *site-to-site* deve eliminar a necessidade de cada computador executar software cliente VPN como se fosse em uma VPN de acesso remoto.

2.3.2 Remote-Access VPN

VPNs tornaram-se a solução lógica para a conectividade de acesso remoto, por muitas razões. Fornecem comunicações seguras com direitos de acesso adaptados para usuários individuais. As VPNs também aumentam a produtividade estendendo a rede corporativa enquanto reduz os custos de comunicação e aumenta a flexibilidade. Segundo Lakbabi et al. (2012) essas VPNs são normalmente estabelecidas a partir de uma única máquina para uma rede remota, e eles são criadas e destruídas sob demanda, o acesso existe apenas durante o tempo que o usuário requer a conexão.

Usando a tecnologia VPN de acesso remoto, os funcionários, usuários portáteis e escritórios remotos podem, essencialmente, ser conectados na WAN da empresa fornecendo acesso aos recursos da rede seguros como se estivessem diretamente conectados aos servidores (ELKEELANY et al., 2004). VPNs também podem permitir acesso limitado para os empreiteiros e parceiros aos servidores específicos, páginas da Web ou arquivos necessários. Este acesso à rede permite-lhes contribuir para a produtividade do negócio, sem comprometer a segurança da rede.

O rápido desenvolvimento da tecnologia de redes e o aumento da implantação de acessos remotos para os recursos privado e serviços da rede, fez surgir a necessidade da eficiência para autenticar e assegurar a troca de dados de acessos remotos (BADRA; HAJJEH, 2006). Em uma VPN de acesso remoto, cada *host* tem tipicamente o software de cliente VPN. Sempre que o servidor tenta enviar o tráfego destinado para a VPN, o software de cliente VPN encapsula e criptografa o tráfego antes de enviá-lo através da Internet para o *gateway* de VPN na rede alvo. Após o recebimento, o *gateway* de VPN retira os cabeçalhos, descriptografa o

conteúdo e retransmite o pacote para o host de destino dentro da sua rede privada (CISCO, 2012).

Há dois componentes necessários em uma VPN de acesso remoto. O primeiro é um servidor de acesso à rede, chamado de gateway de mídia ou um servidor de acesso remoto (RAS - Remote Access Server). O outro componente necessário de VPNs de acesso remoto é um software cliente. Em outras palavras, os funcionários que querem usar a VPN a partir de seus computadores requerem software nos computadores que podem estabelecer e manter uma conexão com a VPN. A maioria dos sistemas operacionais têm embutido um software que pode conectar-se a VPNs de acesso remoto, embora algumas VPNs podem exigir que os usuários instalem um aplicativo específico em vez disso. O software cliente configura a conexão encapsulada, que o usuário indica por seu endereço Internet. O software também gerencia a criptografia para manter a conexão segura (TYSON; CRAWFORD, 2016).

2.4 INTERNET PROTOCOL SECURITY

Em função da época que foi desenvolvido e de seu contexto de aplicação, o protocolo Internet Protocol (IP) foi concebido sem nenhuma característica de proteção ou segurança inerente (CARISSIMI et al., 2009; LUIS et al., 2003). Na prática, as principais vulnerabilidades a que o IP está sujeito são três: autenticidade, integridade e confidencialidade. Os campos de endereço IP destino e IP origem podem ser facilmente modificados por qualquer programa malicioso. Assim, não há como garantir que um datagrama IP foi realmente enviado pela máquina que se apresenta com o endereço IP origem. Outro ponto importante diz respeito as alterações que podem ser feitas na área de dados. Por fim, os datagramas IP trafegam em uma rede em texto claro, sendo assim possível que um terceiro capture os datagramas na rede e tenha acesso às informações (CARISSIMI et al., 2009).

Os primeiros esforços de padronização (RFC1825/1829) para IP com segurança, autenticação e cifragem de datagramas surgiu em 1995, como uma resposta para necessidade de segurança contra o monitoramento e o controle do tráfego não autorizado na rede. Segundo Carissimi et al. (2009) é uma solução para as vulnerabilidades apresentadas pelo protocolo IP.

O IPsec é um padrão da Internet Engineering Task Force (IETF)(RFC 2401-2412) que define como uma VPN pode ser configurada usando o endereçamento IP (STALLINGS, 1998). Segundo Silva (2004) IPsec oferece seus serviços independente do algoritmo de criptografia usado, não está vinculado a qualquer criptografia específica, autenticação, algoritmos de

segurança, ou tecnologia de codificação. Possui uma arquitetura aberta no sentido de possibilitar a inclusão de outros algoritmos existentes para implementar autenticação e criptografia. Um dos protocolos mais usados porque possui uma estrutura completa para VPNs. Este protocolo está sendo adotado a cada vez por mais fabricantes (LUIS et al., 2003). Não vincula o IPsec com algoritmos específicos, permite que algoritmos mais recentes e melhores possam ser implementados sem alterar as normas IPsec existentes.

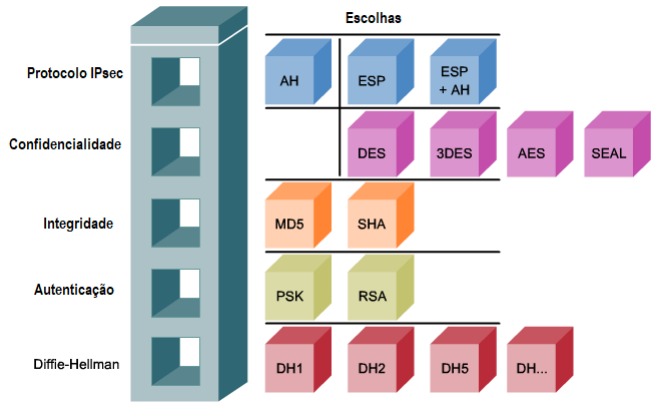

Figura 1 – Framework do protocolo IPSec

Fonte: (CISCO, 2012)

Conforme apresentado na Figura 1, o quadro IPsec é composto por cinco blocos de construção (CISCO, 2012):

- o primeiro representa o protocolo IPsec. Abrange o formato de pacote, sendo usado Encapsulation Security Payload (ESP) ou Authentication Header (AH);
- o segundo representa o tipo de confidencialidade implementado usando um algoritmo de criptografia como Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES), Software Optimized Encryption Algorithm (SEAL). A escolha depende do nível de segurança exigido;
- o terceiro representa integridade que pode ser implementado utilizando tanto Message Digest 5 (MD5) ou Secure Hash Algorithm (SHA);
- a quarta representa a autenticação, como a chave secreta compartilhada é estabelecida. Os dois métodos são chave pré-compartilhada ou assinaturas digitais usando Rivest-Shamir-Adleman (RSA);
- o quinto bloco representa o grupo Diffie-Hellman (DH). Há quatro DH-chaves algoritmos de troca separadas para escolher. O tipo de grupo selecionado depende das necessidades

específicas.

IPsec funciona na camada de rede do modelo OSI, realizando a proteção e autenticação de pacotes IP entre os pares de dispositivos participantes. Como resultado, o IPsec pode proteger praticamente todo o tráfego de aplicação, porque a proteção pode ser implementada a partir da camada 4 até a camada 7 do modelo OSI. Todas as implementações de IPsec tem um texto de cabeçalho simples camada 3, para que não haja problemas com roteamento. Segundo Silva (2004) os serviços do nível de rede OSI relativos à interconexão de redes distintas são implementados na arquitetura TCP/IP pelo protocolo IP, ou seja, só existe uma opção de protocolo e serviço para essa subcamada do nível de rede, o protocolo IP, cujo serviço de datagrama não é confiável, essa é umas das principais razões do sucesso do protocolo IPsec.

IPsec é um conjunto de protocolos para proteger comunicações IP, autenticando e criptografando cada pacote IP de um fluxo de dados. IPsec inclui também protocolos para estabelecer a autenticação mútua entre os agentes no início da sessão de negociação e de chaves criptográficas para ser usado durante a sessão. IPsec pode ser usado para proteger o fluxo de dados entre um par de *hosts*, entre um par de *gateways* de segurança (por exemplo, roteadores ou firewalls), ou entre um *gateway* de segurança e um *host*. IPsec é um modo dual, *end-to-end*, sistema de segurança que opera na camada de Internet do Internet Protocol Suite ou modelo OSI camada 3 (DHALL et al., 2011) (NARAYAN et al., 2009).

Segundo Nakaruma e Geus (2007),Zhang et al. (2009b), Luis et al. (2003), Diab et al. (2008) e (NARAYAN et al., 2009) o conjunto de protocolos IPsec tem três principais componentes:

- cabeçalho de autenticação (AH), que fornece a integridade dos pacotes e a autenticação de sua origem;
- cabeçalho de encapsulamento do payload (ESP), que fornece a confidencialidade dos dados que trafegam pela rede pública e autenticação;
- protocolo de negociação e troca de chaves (Internet Key Exchange - IKE), que permite a negociação das chaves de comunicação entre as organizações de modo seguro, fazendo autenticação e escolha das chaves criptográficas.

IPsec fornece dois modos de criptografia diferentes: Transporte e Túnel. No modo de transporte, há a transmissão direta dos dados protegidos pelo IPsec entre os *hosts*. Fornece apenas criptografia para a parte de dados (*payload*) de cada pacote. Enquanto o modo túnel proporciona segurança entre duas redes, geralmente utilizado pelos *gateways* IPsec, protegendo todo o pacote IP. Mais seguro, criptografa o cabeçalho e o seu conteúdo. Ambos intranet e extranet VPNs são construídas através desta modalidade (DIAB et al., 2008; NARAYAN et al., 2009; NAKARUMA; GEUS, 2007).

2.4.1 Secure Exchange Key

Algoritmos de criptografia como DES, 3DES e AES, bem como os algoritmos de *hash* MD5 e SHA-1 requerem uma chave secreta simétrica, compartilhada para executar a criptografia e descriptografia.

O acordo de chave Diffie-Hellman (DH) é um método de troca de chave pública que fornece uma maneira para dois pares estabelecer uma chave secreta compartilhada que só eles sabem, mesmo que eles estão se comunicando por meio de um canal inseguro. Fornece um protocolo de *secure key exchange* baseado no uso de assinaturas digitais como meio de autenticação de chave pública do protocolo e para fornecer proteção aos pares de entidades contra invasores da rede (KRAWCZYK, 2003). Variações da troca de chaves DH são especificados como grupos DH. Segundo Cisco (2012) existem vários grupos DH:

- Grupos DH 1, 2 e 5 com um tamanho de chave de 768 bits, 1024 bits e 1536 bits, respectivamente. Estes grupos não são recomendados para uso a partir de 2012;
- Grupos DH 14, 15 e 16 usam tamanhos de chaves maiores com 2048 bits, 3072 bits, e 4096 bits, respectivamente, e são recomendados para uso até 2030;
- Grupos DH 19, 20 e 24 suporta Elliptical Curve Cryptography (ECC), que reduz o tempo necessário para gerar chaves. Com a respectiva chave tamanhos de 256 bits, 384 bits, e 2048 bits.

O grupo DH escolhido deve ser suficientemente forte para proteger as chaves de IPsec durante a negociação. Por exemplo, o grupo DH 1 é forte o suficiente para suportar apenas DES e criptografia 3DES, mas não AES. Durante a configuração do túnel, pares VPN negociam qual grupo DH de usar.

2.4.2 Authentication Header

Como descrito na RFC 4302, Authentication Header (AH) é o protocolo IP 51, é o protocolo apropriado para usar quando a confidencialidade não é exigida ou permitida. O AH fornece autenticação e integridade de dados para pacotes IP que são passados entre dois sistemas. Assegura-se a origem dos dados e verifica que os dados não foram alterados durante o trânsito. AH não fornece confidencialidade de dados (criptografia) de pacotes. Todo o texto

é transportado sem criptografia. Se o protocolo AH é usado sozinho, ele fornece fraca proteção (CISCO, 2012).

O cabeçalho de autenticação oferece suporte para integridade de dados e autenticidade dos pacotes IP. O recurso de integridade de dados garante que seja possível a detecção da modificação do conteúdo de um pacote em trânsito. O recurso de autenticação permite que um sistema final ou dispositivo de rede autentique o usuário e filtre o trafego adequadamente (STALLINGS, 2008) (SILVA, 2004).

O AH pode ser usado no modo transporte ou no modo túnel (SILVA, 2004) (STALLINGS, 2008). No modo transporte é usado o mesmo cabeçalho original e troca-se somente o campo Protocolo, já no modo túnel, é gerado um novo cabeçalho, contendo o cabeçalho original encapsulado, seguido pelo cabeçalho de autenticação (SILVA, 2004).

Segundo Stallings (2008) o AH no modo transporte a autenticação abrange o pacote inteiro, excluindo campos mutáveis no cabeçalho IP que são definidos como zero para o calculo do código de autenticação de mensagens (MAC - Message Authentication Code). Para o AH no modo túnel, o pacote IP original inteiro é autenticado, e o AH é inserido entre o cabeçalho de IP original que transporta os últimos endereços de origem e destino, e um novo cabeçalho de IP externo que pode conter diferentes endereços de IP.

A autenticação baseia-se no uso de um MAC, e a chave é negociada durante o processo de estabelecimento da Security Association (SA) (STALLINGS, 2008) (SILVA, 2004). AH alcança autenticidade por meio da aplicação de uma função *hash* unidirecional com chave para o pacote para criar um *hash* ou síntese da mensagem. O *hash* é combinado com o texto e é transmitido. O receptor detecta alterações em qualquer parte do pacote que ocorrem durante o trânsito realizando a mesma função *hash* unidirecional no pacote recebido e comparando o resultado com o valor da mensagem que o remetente forneceu. O fato de que o *one-way hash* também envolve uma chave secreta compartilhada entre os dois sistemas significa que a autenticidade é garantida.

O processo de AH ocorre nesta ordem:

1. O cabeçalho IP e carga de dados são *hashed* usando a chave secreta compartilhada;
2. O *hash* constrói um novo cabeçalho AH, que é inserido no pacote original;
3. O novo pacote é transmitido para o roteador de ponta IPsec;
4. O roteador *hashes* o cabeçalho IP e os dados de carga usando a chave secreta compartilhada, extrai o *hash* transmitido a partir do cabeçalho AH, e compara os dois *hashes*;

Os *hashes* devem corresponder exatamente. Se um bit é alterado no pacote transmitido, a saída de *hash* sobre as alterações do pacote recebido e o cabeçalho AH não irão corresponder.

2.4.3 Encapsulating Security Payload

Definido na RFC 4303, Encapsulating Security Payload (ESP) é o protocolo IP 50, pode fornecer confidencialidade e autenticação. O ESP fornece confidencialidade por meio da realização de criptografia no pacote IP. A criptografia de pacotes IP esconde a carga de dados e as identidades da fonte e destino. ESP fornece autenticação para o conteúdo e cabeçalho do pacote IP. Fornece autenticação da origem de dados e integridade de dados. Embora a criptografia e autenticação são opcionais no ESP, no mínimo, um deles deve ser selecionado (CISCO, 2012).

ESP fornece a confidencialidade criptografando o conteúdo do pacote (SILVA, 2004). O ESP suporta uma variedade de algoritmos de criptografia simétrica. Se ESP é selecionado como o protocolo IPsec, um algoritmo de criptografia também deve ser selecionado. O algoritmo padrão para IPsec é DES de 56 bits (CISCO, 2012). Se nenhum algoritmo de criptografia for utilizado, o protocolo ESP só oferecerá o serviço de autenticação (SILVA, 2004).

ESP também pode fornecer integridade e autenticação (SILVA, 2004). Em primeiro lugar, a carga é codificada. Em seguida, a carga criptografada é enviada através de um algoritmo de *hash*, HMAC-MD5 ou HMAC-SHA-1. O *hash* fornece autenticação e integridade de dados para a carga de dados (CISCO, 2012).

Como o pacote IP é um datagrama, cada pacote deve conter informações necessárias para estabelecer o sincronismo da criptografia, permitindo que a descriptografia ocorra na entidade de destino (SILVA, 2004). Segundo Stallings (2008) o modo transporte é satisfatório para proteger conexões entre *hosts* que suportam o recurso ESP, o modo túnel é útil em uma configuração que incluiu um firewall ou outro tipo de *gateway* de segurança que protege uma rede confiável conta redes externas.

No modo de transporte, o ESP é usado para criptografar e, opcionalmente, autenticar os dados carregados pelo IP (STALLINGS, 2008). O cabeçalho ESP é inserido entre o cabeçalho IP e os dados (SILVA, 2004). A segurança é fornecida apenas para a camada de transporte do modelo OSI e acima. O modo de transporte protege a carga útil do pacote, mas deixa o endereço IP original em texto simples. O endereço IP original é usado para encaminhar o pacote através da Internet.

O modo de túnel, o ESP é usado para criptografar o pacote de IP inteiro (STALLINGS, 2008). Proporciona segurança completa para o pacote IP original. Todo pacote original é colocado dentro de um novo pacote, sendo gerado um novo cabeçalho IP e cabeçalho ESP (SILVA, 2004). O pacote IP original é cifrado e, em seguida, ele é encapsulado em outro pacote

IP. O endereço IP no pacote IP exterior é usado para encaminhar o pacote através da Internet. O modo de túnel ESP é usado entre um *host* e um *gateway* de segurança ou entre dois *gateways* de segurança.

O modo de túnel ESP é usado no aplicativo de acesso remoto IPsec. Um escritório em casa pode não ter um roteador para realizar o encapsulamento IPsec e criptografia. Neste caso, um cliente de IPsec executa no microcomputador o encapsulamento e criptografia. Na sede da empresa, o roteador desencapsula e decifra o pacote (CISCO, 2012).

2.4.4 Internet Key Exchange

A solução IPsec VPN negocia parâmetros de troca de chaves, estabelece uma chave compartilhada, autentica os pares, e negocia os parâmetros de criptografia. Os parâmetros negociados entre dois dispositivos são conhecidos como uma associação de segurança (SA - Security Association) (CISCO, 2012). Uma SA define os tipos de medidas de segurança que devem ser aplicadas aos pacote baseados em quem está enviando os pacote, para onde eles estão indo e que tipo de dados eles estão transportando (SILVA, 2004).

Uma SA é um bloco de construção básico de IPsec. Associações de segurança são mantidas dentro de uma base de dados SA (SADB), que é estabelecida por cada dispositivo. Uma VPN tem SA entradas que definem os parâmetros de criptografia IPsec, bem como entradas SA para definir os parâmetros de troca de chaves. Várias SAs precisam ser empregadas para que o mesmo fluxo de tráfego alcance os serviços IPsec desejados. O termo combinação se associação de segurança refere-se a uma sequência de SAs através das quais o tráfego precisa ser processado para fornecer o conjunto de serviços desejados do IPsec (STALLINGS, 2008).

As informações das SAs que irão fazer parte da VPN podem ser trocadas dinamicamente entre as entidades que irão fazer uso das informações da SA no momento em que as entidades desejarem utilizar um serviço de segurança oferecido pelo IPsec (SILVA, 2004).

Todos os sistemas criptográficos, incluindo a cifra de César, Vigenere cifra, máquina Enigma, algoritmos de criptografia modernos, têm de lidar com questões fundamentais de gestão. DH é usado para criar a chave de segredo compartilhado. No entanto, IPsec usa o protocolo Internet Key Exchange (IKE) para estabelecer o processo de troca de chaves (CISCO, 2012).

Em vez de transmitir as chaves diretamente através de uma rede, IKE calcula chaves partilhadas com base na troca de uma série de pacotes de dados. Isso desativa a possibilidade de

um interceptor descriptografar as chaves mesmo que ele capture todos os dados que são usados para calcular as chaves trocadas.

IKE é definido na RFC 2409. É um protocolo híbrido, combinando a Internet Security Association e Key Management Protocol (ISAKMP) e os métodos Oakley e SKEME de troca de chaves. ISAKMP define o formato de mensagem, a mecânica de um protocolo de troca de chaves, e o processo de negociação para construir uma SA de IPsec. O ISAKMP não define como as chaves são geridas ou compartilhadas entre os dois pares IPsec.

2.5 SECURY SOCKETS LAYER

Segundo (STALLINGS, 2008) praticamente todas as empresas, a maioria dos órgãos do governo e muitos usuários possuem sites Web. As empresas demonstram grande interesse em utilizar a Web para comércio eletrônico (SILVA, 2004; STALLINGS, 2008). A realidade de que a Internet e Web são ambientes extremamente vulneráveis a riscos, aumenta a demanda por serviços Web seguros. SLL tem sido amplamente utilizado para autenticação e transmissão de dados codificados entre o navegador e o servidor.

SSL é um protocolo projetado pela Netscape Comunnications Corporation para fornecer um canal seguro entre duas máquinas na rede. SSL destina-se a dar segurança durante a transmissão de dados pela Internet (CHEN et al., 2013).

SSL fornece criptografia de dados, autenticação de servidor e integridade de mensagens para transmissão de dados pela Internet. A versão 3.0 do SSL suporta tanto a autenticação de cliente como a de servidor. Projetado para fornecer uma segurança confiável em serviços end-to-end para o protocolo TCP. Composto por vários protocolos, como o SSL Handshake Protocol, SSL Change Cipher Spec Protocol, SSL Alert Protocol e SSL Record Protocol. Sua arquitetura é mostrada na Tabela 1.

Tabela 1 – Arquitetura protocolo SSL

Aplication Layer Protocol		
SSL Handshake Protocol	SSL Change Cipher Spec Protocol	SSL Alert Protocol
SSL Record Protocol		
Transmission Control Protocol		
Internet Protocol		

Fonte: (LIU et al., 2008)

Segundo Stallings (2008), dois conceitos importantes do SSL são a sessão SSL e

conexão SSL, definidos a seguir da seguinte maneira:

- **conexão:** conexão SSL é um transporte que oferece um tipo adequado de serviço e descreve como são transmitidos e recebidos os dados. Essa conexão são relacionamentos peer-to-peer. As conexão são transientes, ou seja, temporárias e cada conexão está associada a uma sessão (STALLINGS, 2008; CHEN et al., 2013);
- **sessão:** sessão SSL é uma associação entre o servidor e o cliente. A sessão é criada pelo SSL Handshake. As sessões definem um conjunto de parâmetros de segurança criptográficos (STALLINGS, 2008; CHEN et al., 2013).

Em primeiro lugar, é necessário estabelecer um canal seguro entre o cliente e servidor pelo acordo do handshake SSL. O protocolo SSL Record encapsula os dados do aplicativo em vários registros por meio de medidas como segmentação e compressão, acrescentando o MAC e realizando criptografia.

O autor Liu et al. (2008) apresenta os algoritmos de criptografia suportados pelo protocolo SSL separados por sua funcionalidade :

- cifra simétrica: Blowfish, CAST, DES, IDEA, RC2, RC4, RC5;
- criptografia de chave pública e acordo de chaves: DSA, DH, RSA;
- certificação: x509, x509v3;
- autenticação e Função Hash: HMAC, MD2, MD4, MD5,MDC2, RIPEMD, SHA.

Alguns desses algoritmos estão descritos na sessão Internet Protocol Security. Os seguintes tópicos explicam o funcionamento de cada protocolo que compõem a arquitetura do SSL.

SSL Handshake Protocol: É o protocolo responsável pela autenticação do cliente e do servidor, além de fornecer os parâmetros para o funcionamento do SSL Record Protocol. O Handshake é usado antes que quaisquer dados de aplicação sejam transmitidos, assim, todas as mensagens de handshake são negociadas usando um algoritmo de criptografia e MAC para dar mais segurança desde o início do processo. O protocolo de handshake é constituído por uma série de mensagens trocadas entre cliente e o servidor (STALLINGS, 2008).

Change Cipher Spec Protocol: Este protocolo é o responsável pela troca dos algoritmos de criptografia utilizados. Consiste em uma variável que indica qual o método de criptografia será utilizado. A alteração desta variável pode ser realizada tanto pelo cliente quanto pelo servidor.

Alert Protocol: É o protocolo responsável por supervisionar os erros existentes durante as transações do SSL, a cada erro encontrado o Alert Protocol envia uma mensagem de alerta para a outra extremidade da conexão. As mensagens de alerta são compactadas e criptografadas. Cada mensagem consiste em dois bytes, o primeiro tem o valor warning (1)

ou fatal (2) para transportar o grau de gravidade da mensagem. Se o nível for fatal, a conexão será imediatamente encerrada. O Segundo byte contém um código que se refere a descrição do alerta (STALLINGS, 2008).

SSL Record: O protocolo recebe uma mensagem da aplicação, camada superior, a ser transmitida. Fragmenta os dados em blocos gerenciáveis, dependendo dos parâmetros recebidos da fase de negociação do protocolo de handshake os dados são ou não compactados, em seguida aplica-se um MAC com uma das funções de hash como MD5 ou SHA-1. Após o processo de criptografia, os dados são criptografados com o algoritmo definido e finalmente transmite a unidade resultante em um segmento TCP (STALLINGS, 2008).

2.6 COMPONENTES DE INFRAESTRUTURA DE UMA VPN

A implementação de uma VPN é construída sobre uma infraestrutura de rede com equipamentos CISCO, que é compostas por vários componentes que serão descritos a seguir apenas os utilizados neste trabalho.

2.6.1 Software

Sistema Operacional: Um sistema operacional pode ser definido como um conjunto de programas especialmente feitos para a execução de várias tarefas, entre as quais servir de intermediário entre o utilizador e o computador. Um sistema operacional, tem também como função, gerir todos os periféricos de um computador.

Cisco IOS Comand-Line Interface: A Comand-Line Interface (CLI) é a principal interface de usuário usado para configuração, monitoramento e manutenção de dispositivos Cisco. Essa interface de usuário permite que você execute diretamente e simplesmente comandos Cisco IOS, seja através de um console de roteador ou terminal, ou usando métodos de acesso remoto. Para ajudar na configuração de dispositivos Cisco, a CLI é dividida em diferentes modos de comando. Cada modo de comando tem seu próprio conjunto de comandos disponíveis para a configuração, manutenção e monitoramento de operações do roteador e da

rede.

Cisco Internetwork Operating System: A função central do Cisco Internetwork Operating System (IOS) é permitir a comunicação de dados entre os nós da rede. Além de roteamento e comutação, Cisco IOS oferece dezenas de serviços adicionais que um administrador pode usar para melhorar o desempenho e a segurança do tráfego de rede. Tais serviços incluem criptografia, autenticação, VPNs, firewall, aplicação de políticas, inspeção profunda de pacotes, qualidade de serviço, roteamento inteligente (CISCO, 2012).

PuTTY: O PuTTY é um software *free* e *open source* de emulação de terminal. Suporta SSH, destinado a suportar o acesso remoto a servidores via *shell* e a construção de túneis cifrados entre servidores. Também suporta conexão direta, telnet e por porta serial.

Cisco AnyConnect Secure Mobility Client: O Cisco AnyConnect é um agente unificado que oferece vários serviços de segurança para proteger a empresa. Confere a visibilidade e o controle necessários para identificar quem e qual dispositivo estão acessando a empresa estendida antes, durante e depois de um ataque. O AnyConnect Secure Mobility Client oferece uma plataforma de segurança de endpoint ampla com funcionalidade de acesso remoto, aplicação de postura e recursos de segurança da Web. O AnyConnect oferece ao departamento de TI todos os recursos de acesso seguro necessários para proporcionar uma experiência móvel robusta, simplificada e altamente segura. É um produto de software de endpoint multifacetado. Isso significa que ele não oferece apenas acesso de VPN através de Secure Sockets Layer (SSL) e IPsec IKE, mas também oferece segurança avançada por meio de vários módulos internos.

2.6.2 Hardware

Switch: O Switch é um dispositivo utilizado em redes de computadores para reencaminhar pacotes (frames) entre os diversos nós. O Switch possui portas, segmenta a rede internamente, sendo que a cada porta corresponde a um domínio de colisão diferente, isto é, não haverá colisões entre pacotes de segmentos diferentes. Um Switch Cisco é gerenciável, com a capacidade de criar VLANS, deste modo a rede gerida será divida em menores segmentos, onde identifica cada porta e envia os pacotes somente para a porta destino, evitando assim que outros nós recebam os pacotes.

Roteador: Um roteador é um dispositivo de rede que encaminha pacotes de dados entre redes de computadores. Roteadores realizam a função de direcionar o tráfego na rede.

Um pacote de dados é normalmente encaminhado de um roteador para outro por meio das redes que constituem o conjunto de redes até atingir o nó de destino. Um roteador é ligado a duas ou mais linhas de dados a partir de diferentes redes. Quando um pacote de dados entra em uma das linhas, o roteador lê a informação de endereço no pacote para determinar o destino final.

Microcomputador: É um conjunto de artifícios eletrônicos capazes de realizar processamento de dados, ou seja, é utilizado para processar informações. Composto por duas partes distintas: Software e Hardware. Um microcomputador é caracterizado pela presença de um único microprocessador. Tem dimensões e capacidade computacional limitado.

3 MATERIAIS E MÉTODOS

Após estudos realizados sobre redes privadas virtuais e aplicações técnicas utilizando o protocolo IPSec e SLL, é importante definir as ferramentas e procedimentos utilizados, que foram necessários para a implementação das VPNs. Portanto, neste capítulo serão descritos os materiais e métodos utilizados para o desenvolvimento das VPNs utilizadas neste trabalho para realizar a comparação.

3.1 HARDWARE E SOFTWARE

Para a implementação das VPNs utilizou-se dos hardwares e softwares, que são descritos a seguir:

- Sistema Operacional Microsoft Windows 10;
- GNS3;
- Imagem do roteador Cisco modelo 7200 com IOS versão 15.0;
- Imagem do switch Cisco modelo 3640 com IOS versão 12.2;
- Oracle VM VirtualBox;
- Cisco AnyConnect Secure Mobility Client.

3.2 MÉTODOS

Para o desenvolvimento do trabalho proposto houve a necessidade de uma pesquisa bibliográfica aprofundada em temas relacionados à implementação de VPNs com o uso dos protocolos IPsec e SSL, pode ser visualizado no Capítulo 2. Diante dessa necessidade foi

preciso configurar e implementar alguns protocolos de Internet e segurança.

3.2.1 Configuração das VPNs IPSec e SSL

Definiu-se um ambiente virtual utilizando o programa GNS3 com a topologia de rede Site-to-Site (Figura 2), o qual foi utilizado para implementação dos dois protocolos em projetos separados. A topologia é constituída por três roteadores Cisco, que foram criados utilizando a Imagem do roteador Cisco modelo 7200 com IOS versão 15.0. Escolheu-se essa versão devido ao suporte de pacotes de segurança necessários para a implementação de VPNs.

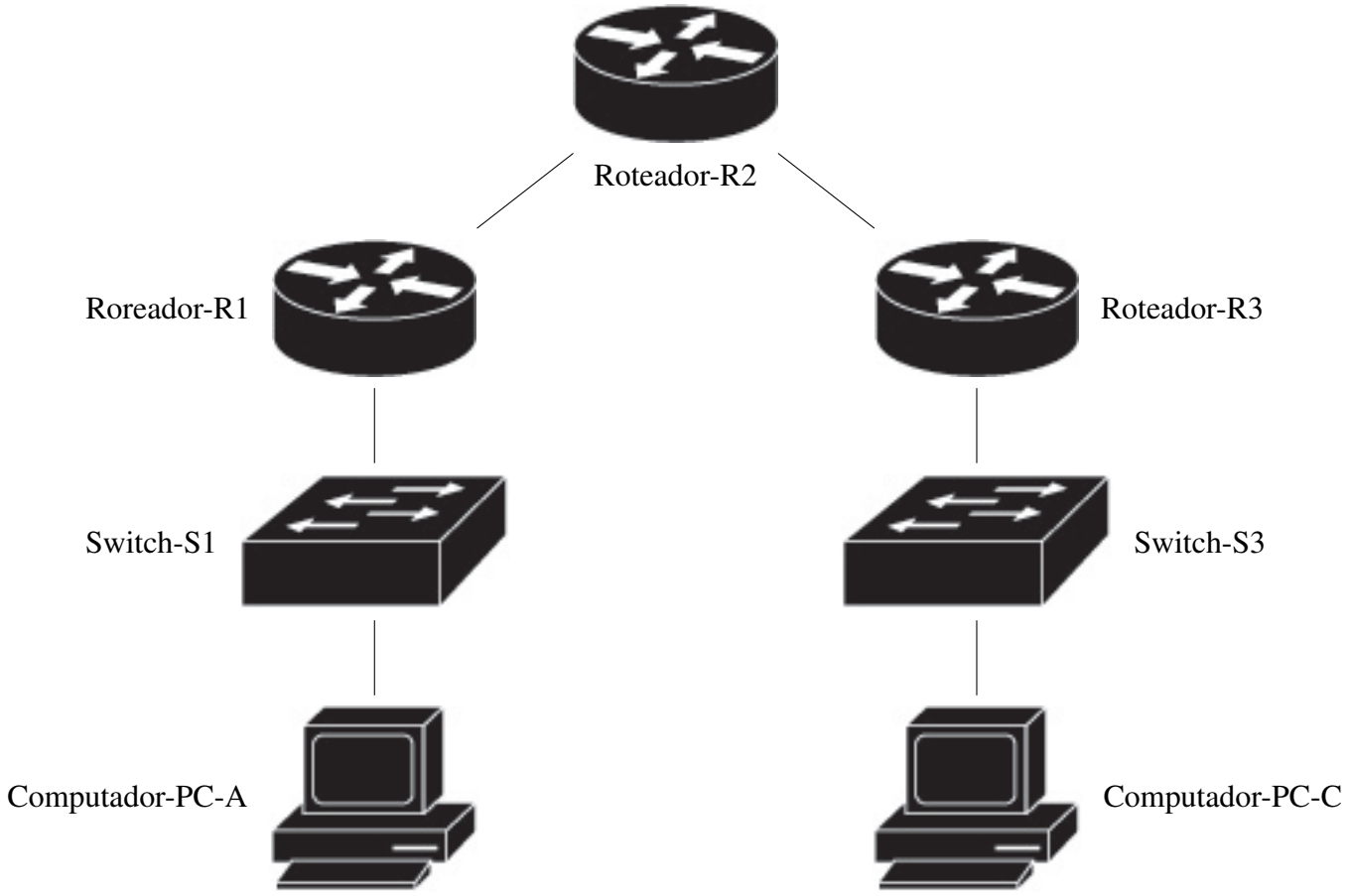

Figura 2 – Topologia de rede Site-to-Site de implementação das VPNs

Fonte: Autoria própria.

A configuração do túnel VPN foi criada entre o roteador R1 e o roteador R3, o roteador R2 é apresentado na topologia (Figura 2) para representar a Internet. Ambos os roteadores R1

e R3 estão conectados a um Switch, criados utilizando a Imagem do switch Cisco modelo 3640 com IOS versão 12.2, os switchs são utilizados apenas para fazer a conexão dos computadores com a rede. Criou-se duas máquinas virtuais por meio do VirtualBox, com o sistema operacional Windows 10, que são tratadas neste trabalho como PC-A e PC-C, utilizadas para teste das VPNs.

Algumas tarefas básicas foram realizadas para configurar um *site-to-site* IPsec VPN :

- certificou-se de que a Lista de Controle de Acesso (ACL) configurada em interfaces são compatíveis com a configuração IPsec. Normalmente, há restrições sobre a interface que o tráfego VPN usa. Por exemplo, bloquear todo o tráfego que não é IPsec ou IKE;
- criar uma política de Internet Security Association and Key Management Protocol (ISAKMP). Esta política determina os parâmetros ISAKMP que serão usados para estabelecer o túnel;
- configurar o conjunto de tranformações IPsec. O conjunto define os parâmetros que o túnel IPsec usa. O conjunto pode incluir os algoritmos de criptografia e integridade;
- criar uma ACL de criptografia. A ACL de criptografia define qual o tráfego enviado através do túnel IPsec é protegido pelo processo de criptografia;
- criar e aplicar um mapa de criptografia. Os parâmetros do mapa de criptografia devem ser previamente configurados em conjunto e definir os pares de dispositivos IPsec. O mapa de criptografia é aplicado na interface de saída do roteador da VPN.

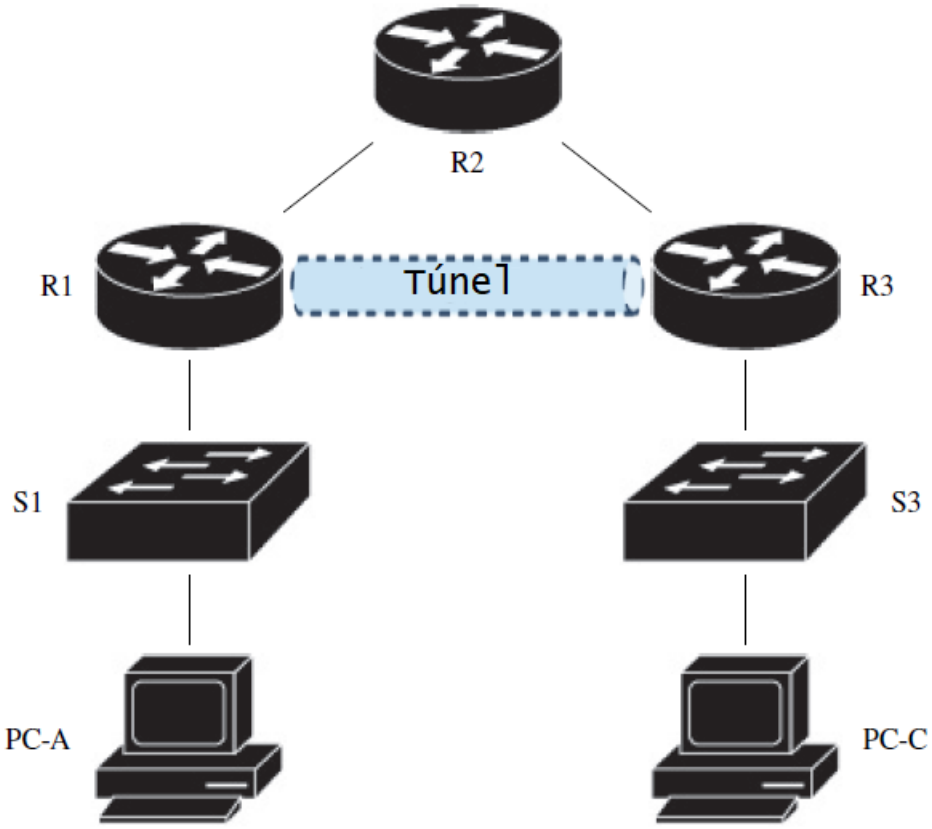

Figura 3 – Túnel da VPN

Fonte: Autoria própria.

Para estabelecer uma sessão de uma VPN SSL foi necessário implementar as seguintes etapas no ambiente virtual:

- transferir e instalar o pacote de arquivos AnyConnect para o roteador principal R1;
- permitir o servidor HTTP e HTTPs no roteador R1;
- geração de um par de chaves RSA para fazer a assinatura do certificado digital;
- configurar contas de usuário locais para a VPN;
- criar uma lista de acesso para definir o tráfego que deve ou não deve ser enviado através do túnel;
- configurar o gateway WebVPN, o contexto WebVPN e a politica de grupo.

VPNs podem ser complexas e às vezes não funcionam como esperado. Por esta razão, há uma variedade de comandos do CLI úteis para verificar a operação da VPN e solucionar problemas quando necessário.

A implementação virtual executou-se no software GNS3 na tentativa de possibilitar a implementação das VPNs e atingir os objetivos do trabalho. Por não fazer parte dos objetivos

deste trabalho, a instalação do GNS3 não será abordada.

Neste trabalho foi construído e configurado uma rede com múltiplos roteadores, usando o Cisco IOS CLI para configuração de uma topologia de VPN site-to-site. A implementação foi realizada baseando-se nas configurações de redes de computadores que são apresentadas na Tabela 2, na qual verifica-se os endereços IP que foram adicionados nas interfaces dos roteadores. O túnel de VPN foi criado entre o roteador R1 para o R3, através do R2. O R2 age como uma passagem e não tem nenhum conhecimento sobre a VPN, uma representação ilustrativa deste túnel criado é apresentado na Figura 3.

Tabela 2 – Tabela de Endereços IP

Dispositivo	Interface	Endereço IP	Mascara Sub-rede	Gateway Padrão	Porta Switch
R1	G0/1	192.68.1.1	255.255.255.0		S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252		
R2	S0/0/0	10.1.1.2	255.255.255.252		
	S0/0/1	10.2.2.2	255.255.255.252		
R3	G0/1	192.168.3.1	255.255.255.0		S3 F0/1
	S0/0/1	10.2.2.1	255.255.255.252		
PC-A	ETH0	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-C	ETH0	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/2

Tendo como base a topologia da Figura 2, configurou-se os hostnames dos roteadores, e adicionou-se os endereços IP nas interfaces dos roteadores conforme a Tabela 2, e também configou-se o clockrate rate de 64000 nas interfaces seriais dos roteadores que possuem o cabo serial DCE conectado. Em seguida configurou-se o protocolo de roteamento dinâmico OSPF nos roteadores R1, R2 e R3 para tornar possível a transmissão dos dados entre os roteadores.

Os comandos seguintes foram utilizados para configuração do roteamento dinâmicos OSPF.

Algoritmo 1: Roteamento Dinâmico OSPF

```
1   R1(config)# router ospf 101
2   R1(config-router)# network 192.168.1.0 .0.0.0.255 area 0
3   R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
4
5   R2(config)# router ospf 101
6   R2(config-router)# network 10.1.1.0 .0.0.0.3 area 0
7   R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
8
9   R3(config)# router ospf 101
10  R3(config-router)# network 192.168.3.0 .0.0.0.255 area 0
11  R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

Para finalizar as configurações básicas adicionou-se um endereço IP, máscara de sub-rede e gateway padrão para os PC-A e PC-C como está mostrado na Tabela 2. Na subseção seguinte está descrito detalhadamente os comandos utilizados para configurar a VPN e o que resulta destes comandos quando executados.

3.3 IMPLEMENTAÇÃO COM PROTOCOLO IPSEC

Existem dois elementos principais de configuração na implementação de uma VPN IPsec:

- implementar os parâmetros IKE;
- implementar os parâmetros IPsec.

O IKE precisar estar habilitado para o funcionamento do IPsec, e pode ser ser habilitado por meio do comando **crypto isakmp enable**, descrito no Algoritmo 2 .

Algoritmo 2: Ativação ISAKMP

```
1   R1(config)# crypto isakmp enable
2
3   R3(config)# crypto isakmp enable
```

Uma política ISAKMP define os algoritmos de autenticação, criptografia e a função hash usada para enviar tráfego de controle entre os dois pontos de extremidade da VPN.

Configurou-se uma política ISAKMP com uma prioridade de nível 10. Usou-se a chave pré-compartilhada como o tipo de autenticação, AES 256 para o algoritmo de criptografia, SHA como o algoritmo hash e a troca de chaves do grupo 14 Diffie-Hellman. Atribuiu-se a política uma vida útil de 3600 segundos (uma hora). A mesma configuração é feita para os roteadores R1 e R3, com a execução dos comandos apresentados no Algoritmo 3.

Algoritmo 3: Política ISAKMP

```
1  R1(config)# crypto isakmp policy 10
2  R1(config-isakmp)# hash sha
3  R1(config-isakmp)# authentication pre-share
4  R1(config-isakmp)# group 14
5  R1(config-isakmp)# lifetime 3600
6  R1(config-isakmp)# encryption aes 256
7  R1(config-isakmp)# end
```

É possível verificar a politica ISAKMP utilizando o comando **show crypto isakmp policy**, que resulta no Algoritmo 4.

Algoritmo 4: Resultado configuração ISAKMP

```
1  R1# show crypto isakmp policy
2  Global IKE policy
3  Protection suite of priority 10
4  encryption algorithm:   AES - Advanced Encryption
      Standard (256 bit keys).
5  hash algorithm:         Secure Hash Standard
6  authentication method:  Pre-Shared Key
7  Diffie-Hellman group:   #14 (2048 bit)
8  lifetime:               3600 seconds, no volume limit
```

Como as chaves pré-compartilhadas são usadas como o método de autenticação na política IKE, foi necessário configurar uma chave em cada roteador que aponte para o outro ponto de extremidade da VPN. Essas chaves devem corresponder para que a autenticação fosse bem-sucedida.

Algoritmo 5: Chaves pré-compartilhadas

```
1  R1(config)# crypto isakmp key cisco123 address 10.2.2.1
2  R3(config)# crypto isakmp key cisco123 address 10.1.1.1
```

Nos roteadores R1 e R3,criou-se um conjunto de transformação com tag 50 e usamos uma transformação ESP com uma cifra AES 256 e ESP com a função hash SHA. Os conjuntos

de transformações devem corresponder nos roteadores.

Algoritmo 6: Conjunto de transformação IPsec

```
1  R1(config)# crypto ipsec transform-set 50 esp-aes 256
       esp-sha-hmac
2
3  R3(config)# crypto ipsec transform-set 50 esp-aes 256
       esp-sha-hmac
```

Para utilizar a criptografia IPsec com a VPN, foi necessário definir listas de acesso estendidas para informar ao roteador qual tráfego criptografar. Um pacote permitido por uma lista de acesso usada para definir o tráfego IPsec foi criptografado se a sessão IPsec estiver configurada corretamente. Um pacote negado por uma dessas listas de acesso não é descartado, ele é enviado sem criptografia. Além disso, como qualquer outra lista de acesso, há uma negação implícita no final, o que significa que a ação padrão é não criptografar o tráfego. Se não houver nenhuma associação de segurança IPsec configurada corretamente, nenhum tráfego será criptografado e o tráfego será encaminhado sem criptografia. Nesse cenário do trabalho, da perspectiva de R1, o tráfego que se deseja criptografar é o tráfego da LAN Ethernet de R1 para a LAN Ethernet de R3 ou vice-versa na perspectiva de R3. Essas listas de acesso são usadas nas interfaces das pontas da VPN e devem espelhar-se mutuamente, que foram criadas no Algoritmo 7.

Algoritmo 7: Lista de acesso IPsec

```
1  R1(config)# access-list 101 permit ip 192.168.1.0
       0.0.0.255 192.168.3.0 0.0.0.255
2
3  R3(config)# access-list 101 permit ip 192.168.3.0
       0.0.0.255 192.168.1.0 0.0.0.255
```

Um mapa de criptografia associa o tráfego que corresponde a uma lista de acesso a um par e a várias configurações de IKE e IPsec. Depois que o mapa de criptografia é criado, pode ser aplicado a uma ou mais interfaces. As interfaces às quais se aplica o mapa de criptografia devem ser aquelas que estão dedicadas para o par IPsec. Usou-se o tipo ipsec-isakmp, para estabelecer associações de segurança do IPsec por meio das configurações de IKE.

Algoritmo 8: Mapa de criptografia IPsec

```
1  R1(config)# crypto map CMAP 10 ipsec-isakmp
2  R1(config-crypto-map)# match address 101
3  R1(config-crypto-map)# set peer 10.2.2.1
4  R1(config-crypto-map)# set pfs group14
5  R1(config-crypto-map)# set transform-set 50
6  R1(config-crypto-map)# set security-association lifetime
       seconds 900
```

O comando **match address 101** é usado para especificar qual lista de acesso define qual tráfego criptografar, neste caso utilizou-se lista de acesso 101 que foi criada anteriormente no Algoritmo 7. A definição de um IP ou nome de host é necessária. Definiu-se a interface de ponto de extremidade da VPN remota do R3 usando o comando **set peer 10.2.2.1**. Para fazer a associação com o conjunto de transformação, usamos **set transform-set 50**. Usa-se o comando **set** do conjunto de transformações para codificar o conjunto de transformações a ser usado com esse par. Para o sigilo de encaminhamento perfeito, utilizou-se o comando **set pfs group14** e modificou-se o tempo de vida de associação de segurança IPsec padrão com o comando **set security-association lifetime seconds 900**. Essa mesma configuração é feita no roteador R3 apenas trocando o par apontando para o ponto de extremidade da VPN remoto do R1 (Algoritmo 9).

Algoritmo 9: Host do mapa de criptografia no roteador R3

```
1  R3(config-crypto-map)# set peer 10.1.1.1
```

A ultima configuração realizada para completar a implementação da VPN IPsec foi aplicar o mapa de criptografia às interfaces apropriadas nos roteadores R1 e R3. Os roteadores geram uma notificação que a criptografia está ativada.

Algoritmo 10: Mapa de criptografia aplicado em interface

```
1  R1(config)# interface S0/0/0
2  R1(config-if)# crypto map CMAP
3  *Feb 12 04:08:04.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is
       ON
4  R1(config)# end
5
6  R3(config)# interface S0/0/1
7  R3(config-if)# crypto map CMAP
8  *Feb 12 04:09:34.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is
       ON
9  R3(config)# end
```

3.4 IMPLEMENTAÇÃO COM PROTOCOLO SSL

Para a implementação da VPN SSL utilizou-se a mesma topologia da Figura 2, parte-se diretamente às configurações utilizadas para a o funcionamento da VPN. O primeiro passo executado foi a transferência do pacote AnyConnect para o roteador principal R1 através do protocolo Trivial File Transfer Protocol (TFTP), o arquivo está armazenado na máquina virtual PC-A, onde possui instalado um servidor básico tfpt para tornar possível a execução desta tarefa. Para realizar a transferência de arquivos pela rede para a memória flash do roteador utiliza-se o

comando **copy tftp: flash/disk0/** que é apresentado no Algoritmo 11.

Algoritmo 11: Upload pacote AnyConnect

```
1  R1# copy tftp: flash:/disk0/
2
3  Address or name of remote host []? 192.168.1.3
4  Source filename []? anyconnect-win-3.1.08009-k9.pkg
5  Destination filename [/disk0/anyconnect-win-3.1.08009-k9
      .pkg]?
6  Accessing tftp://192.168.1.3/anyconnect-win-3.1.08009-k9
      .pkg...
7  Loading anyconnect-win-3.1.08009-k9.pkg from
      192.168.100.100
8  (via GigabitEthernet0):
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
9  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

10 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

11 [OK - 37997096 bytes]
12
13 37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

Após copiado o pacote AnyConnect para a memória flash do roteador, é preciso que ele seja instalado usando a linha de comando. Vários pacotes AnyConnect podem ser instalados quando é especificado no final do comando de instalação **sequence number**, com um número diferente para cada pacote. Para isso utilizou-se os comandos apresentados no Algoritmo 12.

Algoritmo 12: Instalação pacote AnyConnect

```
1  R1(config)# crypto vpn anyconnect flash:/webvpn/
      anyconnect-win-3.1.08009-k9.pkg sequence 1
2
3  SSLVPN Package SSL-VPN-Client (seq:1): installed
      successfully
```

Tendo o pacote AnyConnect instalado, é necessário fazer a ativação do servidor HTTP e HTTPS no roteador R1, o que inclui a ativação do navegador web Cisco, que foi utilizado para o acessar e baixar o cliente AnyConnect do pacote instalado, necessário para realizar a conexão

da VPN SLL (Algoritmo 13).

Algoritmo 13: Ativação servidor HTTPS

```
1    R1(config)# ip http server
2    R1(config)# ip http secure-server
```

Em uma configuração de VPN SSL que implementa um PKI e certificados digitais , um par de chaves RSA é requerida para fazer a assinatura do certificado. O Seguinte comando **crypto key generate rsa label SSLVPN KEYPAIR modulus 2048** gera o par de chaves para ser utilizado na assinatura (Algoritmo 14). O modulo de 2048 bits foi escolhido por ser o maior disponível para a segurança. A geração da chave pode ser confirmada com o comando **show crypto key mypubkey rsa**.

Algoritmo 14: Geração de chaves RSA

```
1    R1(config)# crypto key generate rsa label SSLVPN_KEYPAIR
         modulus 2048
2
3    The name for the keys will be: SSLVPN_KEYPAIR
4
5    % The key modulus size is 2048 bits
6    % Generating 2048 bit RSA keys, keys will be exportable
        ...
7    [OK] (elapsed time was 3 seconds)
```

Uma vez que o par de chave RSA foi gerado com sucesso, um ponto confiável PKI é configurado com informação do par de chave RSA do roteador R1 (Algoritmo 15).

Algoritmo 15: Ponto confiável PKI

```
1    R1(config)# crypto pki trustpoint SSLVPN_CERTIFICADO
2    R1(ca-trustpoint)#enrollment selfsigned
3    R1(ca-trustpoint)#rsakeypair SSLVPN_KEYPAIR
```

Depois que o ponto confiável foi definido corretamente, o roteador deve gerar o certificado usando o comando **crypto pki enroll** (Algoritmo 16). Com este processo, é possível especificar alguns parâmetros tais como o número de série e o endereço IP do roteador.

Contudo, isto não é exigido.

Algoritmo 16: Geração do Certificado Digital

```
1  R1(config)# crypto pki enroll SSLVPN_CERTIFICADO
2  % Include the router serial number in the subject name?
       [yes/no]: no
3  % Include an IP address in the subject name? [no]: no
4  Generate Self Signed Router Certificate? [yes/no]: yes
5  Router Self Signed Certificate successfully created
```

Quando possível, é recomendado utilizar para maior segurança, um servidor externo para Authentication, Authorization, and Accounting (AAA), mas neste trabalho foi utilizado a autenticação local, os comandos mostrados abaixo criam um usuário da VPN com uma lista de autenticação AAA nomeada SSLVPN AAA (Algoritmo 17).

Algoritmo 17: Criação de usuário VPN

```
1  R1(config)# aaa new-model
2  R1(config)# aaa authentication login SSLVPN_AAA local
3  R1(config)# username VPNUSER password FELIPE
```

Um pool de endereços IP locais é criado para que os usuários do AnyConnect obtenham um endereço IP que faz parte da rede do roteador R1. Por padrão o AnyConnect opera em modo de túnel completo, significa que todo o tráfego da máquina será enviado pelo túnel criptografado, é possível a criação de uma lista de acesso para definir o trafego que deve ou não ser enviado por meio do túnel, neste trabalho foi configurado da forma com que se apresenta no Algoritmo 18.

Algoritmo 18: Pool de endereços IP

```
1  R1(config)# ip local pool SSLVPN_POOL 192.168.1.11
       192.168.1.21
2  R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

O WebVPN Gateway é o que define o endereço IP e a porta que é usado pelo AnyConnect, o algoritmo de criptografia SLL e também o certificado PKI, que será apresentado

para os clientes (Algoritmo 19).

Algoritmo 19: WebVPN Gateway

```
1  R1(config)# webvpn gateway SSLVPN_GATEWAY
2  R1(config-webvpn-gateway)# ip address 10.1.1.1  port 443
3  R1(config-webvpn-gateway)# http-redirect port 80
4  R1(config-webvpn-gateway)# ssl trustpoint SSLVPN_CERT
5  R1(config-webvpn-gateway)# ssl encryption rc4-md5
6  R1(config-webvpn-gateway)# inservice
```

A política do contexto e do grupo WebVPN define alguns parâmetros adicionais que serão usados para a conexão de cliente de AnyConnect. Para uma configuração básica de AnyConnect, o contexto serve simplesmente como um mecanismo usado para chamar a política do grupo padrão que será usada para AnyConnect. Contudo, o contexto pode ser usado para personalizar a página inicial WebVPN e a operação WebVPN. No grupo de política definida, a lista SSLVPN AAA é configurada como a lista da autenticação de AAA de que os usuários são um membro. O comando **functions svc-enabled** é a parte de configuração que permite que os usuários conectem com o AnyConnect SSL VPN Client (SVC). Por final, os comandos SVC adicionais definem os parâmetros que são relevantes somente às conexões SVC: **svc address-pool** diz para o gateway a pool de endereços que serão utilizadas pelos clientes, **svc split include** define a política de lista de acesso a ser usado, e **svc dns-server** define o servidor DNS que será utilizado (Algoritmo 20).

Algoritmo 20: Contexto SSL VPN

```
1  R1(config)#webvpn context SSL_Context
2  R1(config-webvpn-context)# gateway SSLVPN_GATEWAY
3  R1(config-webvpn-context)# inservice
4  R1(config-webvpn-context)# policy group SSL_Policy
5  R1(config-webvpn-context)# aaa authentication list
      SSLVPN_AAA
6  R1(config-webvpn-context)# functions svc-enabled
7  R1(config-webvpn-context)# svc address-pool "SSLVPN_POOL
      " netmask 255.255.255.0
8  R1(config-webvpn-context)# svc split include acl 1
9  R1(config-webvpn-context)# svc dns-server primary
      8.8.8.8
10 R1(config-webvpn-context)# default-group-policy
      SSL_Policy
```

4 RESULTADOS E DISCUSSÕES

Quando concluído a codificação necessária para a implementação, pode-se fazer a verificação da VPN IPsec site-to-site executando alguns comandos. O comando **show crypto ipsec transform-set** mostra o conjunto de transformações (Algoritmo 21) e **show crypto map** o mapa de criptografia (Algoritmo 22). Para verificar se a VPN estava operando e realizando a criptografia, executou-se o comando **show crypto ipsec sa**. Por meio deste comando, verificou-se o funcionamento da VPN nas linhas 10 e 11 do Algoritmo 23, onde apresenta a quantidade de pacotes que foram encapsulados e criptografados. Apresenta-se no Algoritmo 21, Algoritmo 22, Algoritmo 23 apenas as implementações realizadas para o roteador R1 e não do R3, pois realizou-se da mesma maneira para os dois roteadores.

Algoritmo 21: Resultado do conjunto de transformação do IPsec

```
1  R1# show crypto ipsec transform-set
2  Transform set 50: { esp-256-aes esp-sha-hmac  }
3  will negotiate = { Tunnel,  },
4  ...
```

Algoritmo 22: Resultado do mapa de criptografia do IPsec

```
1  R1# show crypto map
2  Crypto Map "CMAP" 10 ipsec-isakmp
3  Peer = 10.2.2.1
4  Extended IP access list 101
5  access-list 101 permit ip 192.168.1.0 0.0.0.255
      192.168.3.0 0.0.0.255
6  Current peer: 10.2.2.1
7  PFS (Y/N): Y
8  DH group:  group14
9  Transform sets={
10 50:  { esp-256-aes esp-sha-hmac  } ,
11 }
12 Interfaces using crypto map CMAP:
13 Serial0/0/0
```

Algoritmo 23: Resultado do IPsec em funcionamento

```
1  R1#show crypto ipsec sa
2  interface: Serial1/0
3  Crypto map tag: CMAP, local addr 10.1.1.1
4  local  ident (addr/mask/prot/port):
      (192.168.1.0/255.255.255.0/0/0)
5  remote ident (addr/mask/prot/port):
      (192.168.3.0/255.255.255.0/0/0)
6  current_peer 10.2.2.1 port 500
7  PERMIT, flags={origin_is_acl,}
8  #pkts encaps: 1925, #pkts encrypt: 1925, #pkts digest:
      1925
9  #pkts decaps: 44253, #pkts decrypt: 44253, #pkts verify:
       44253
10 #pkts compressed: 0, #pkts decompressed: 0
11 #pkts not compressed: 0, #pkts compr. failed: 0
12 #pkts not decompressed: 0, #pkts decompress failed: 0
13 #send errors 1, #recv errors 0
14 local crypto endpt.: 10.1.1.1, remote crypto endpt.:
      10.2.2.1
15 path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
```

Finalizado a configuração da VPN SSL, acessa-se com o PC-C o endereço do Gateway definido por meio de um navegador, o qual retorna a página inicial de login do WebVPN, criada anteriormente e apresentada na Figura 4.

Para efetuar o login utilizou-se o usuário criado no Algoritmo 17. Com o login efetuado, o site redireciona para a página index do WebVPN que é apresentado na Figura 5.

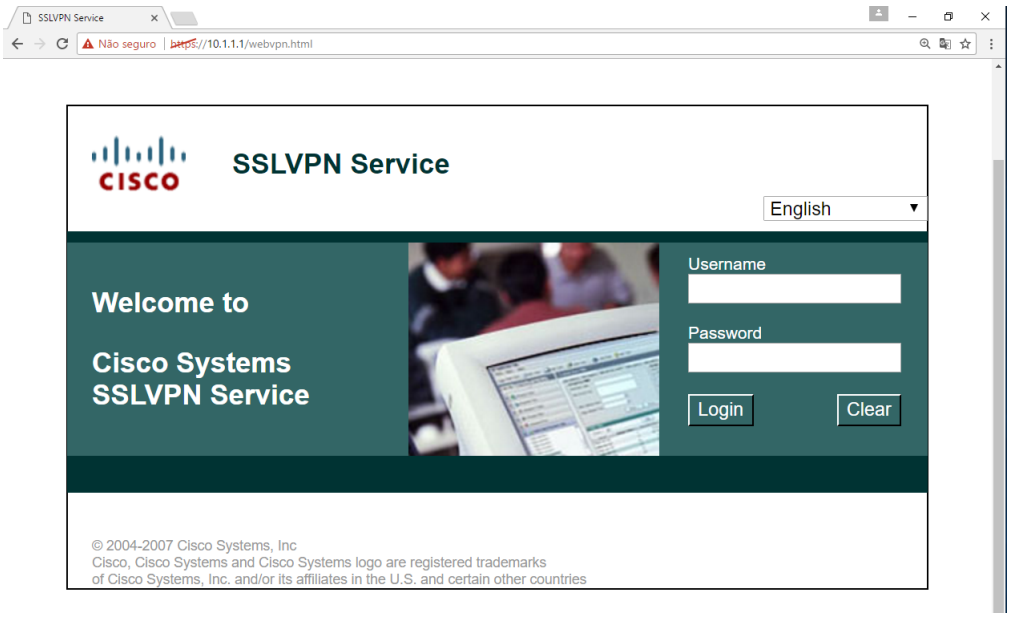

Figura 4 – Página de Login WebVPN

Fonte: Autoria própria.

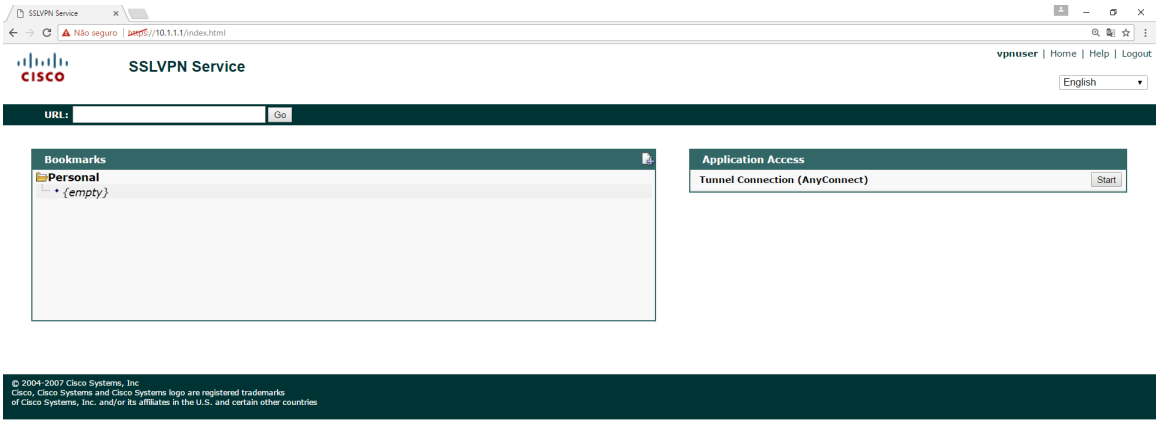

Figura 5 – Página Index WebVPN

Fonte: Autoria própria.

Na página Index, encontramos o menu Application Access, local que irá fornecer a auto-instalação do pacote AnyConnect que foi instalado no roteador R1 no Algoritmo 12. Ao clicar no botão Start, o site abre uma nova janela, que é apresentada na Figura 6. Devido a incompatibilidade do sistema operacional instalado na máquina virtual PC-C, a instalação Web-based não executou corretamente. Assim, foi preciso fazer o download e a instalação manualmente do pacote AnyConnect clicando na área demarcada, e também com uma flecha direcionada para a área correta.

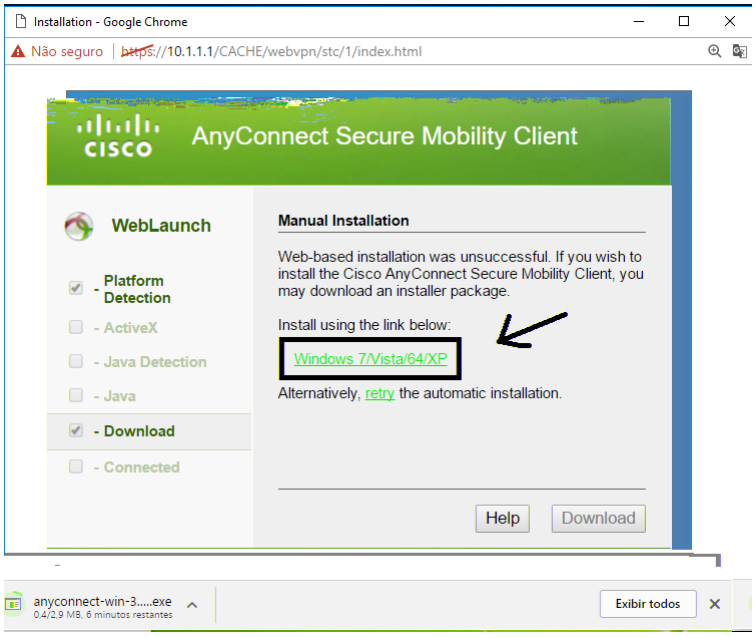

Figura 6 – Página de Download AnyConnect

Fonte: Autoria própria.

Finalizado a instalação do pacote AnyConnect, o programa é executado e se insere os dados necessários para a conexão com a VPN, como pode ser visto na Figura 7.

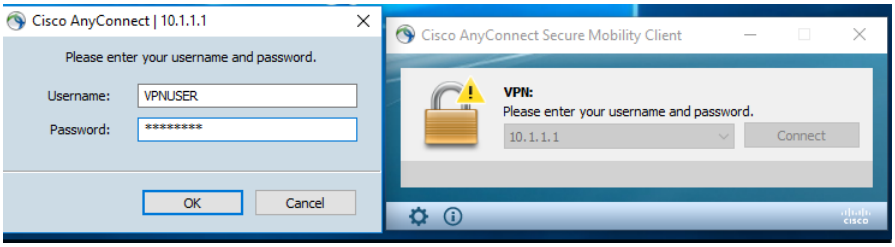

Figura 7 – Conexão com a VPN SSL

Fonte: Autoria própria.

Existem duas maneiras de fazer a verificação da VPN SSL em funcionamento, uma delas é por meio da aba estatísticas do programa AnyConnect, utlizado no PC-C, conforme Figura 8. A Segunda maneira é utilizando o comando **show webvpn session user VPNUSER context SSL Context** no roteador R1, onde foi realizado toda a configuração da VPN SSL, o resultado do comando é apresentado no Algoritmo 24. Nota-se com o resultado das duas maneiras de verificação que é criado uma nova interface virtual de ethernet para o PC-C, com o endereço IP 192.168.1.11 atribuído a ela, isso significa que o PC-C agora também faz parte da rede interna do roteador R1 devido a conexão SSL realizada utilizando o programa AnyConnect.

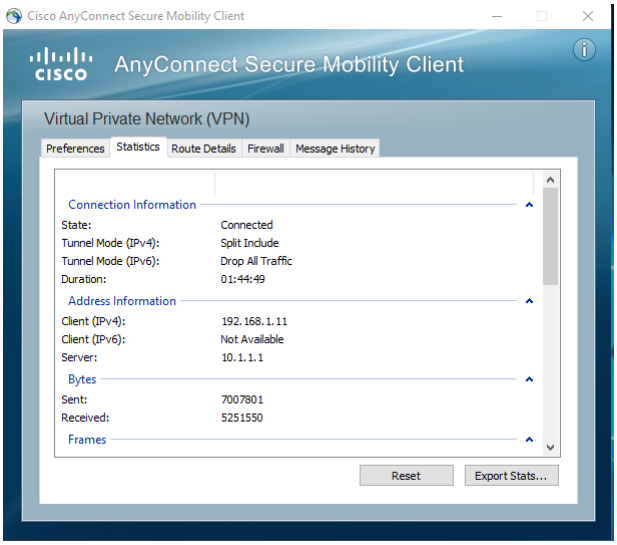

Figura 8 – Estatísticas da Sessão SSL

Fonte: Autoria própria.

Algoritmo 24: Sessão do usuário VPNUSER

```
1  R1#show webvpn session user VPNUSER context
       SSL_Context
2  Session Type       : Full Tunnel
3  Client User-Agent  : AnyConnect Windows 3.1.03103
4  Username           : VPNUSER
5  Num Connection     : 1
6  Public IP          : 192.168.3.3
7  VRF Name           : None
8  Context            : SSL_Context
9  Policy Group       : SSL_Policy
10 Created            : *23:14:30.751 UTC Sat May 19
       2018
11 DNS primary serve  : 8.8.8.8
12 Address Pool       : SSLVPN_POOL
13 MTU Size           : 1399
14 Tunnel IP          : 192.168.1.11
15 Netmask            : 255.255.255.0
16 Split Include      : ACL 1
```

Finaliza-se os resultados das configuração realizadas para a implementação das VPNs SSL e IPsec. Na próxima seção mostraremos os resultados de testes que foram possíveis realizar

com as máquinas virtuais PC-A e PC-C que estão conectadas pelas VPNs.

Com a finalidade de realizar uma comparação dos resultados entre as duas VPNs, realizou-se dois tipos de testes diferentes, o primeiro teste, com intenção de obter a velocidade de transferência dos dados de um ponto de extremidade da VPN para o outro ponto de extremidade, neste trabalho, estes pontos são representados pelas máquinas virtuais PC-A e PC-C. O segundo teste para obter o uso da CPU. Como no trabalho, utilizou-se uma implementação virtual através do programa GNS3, este programa foi instalado em um microcomputador físico, então os dados foram extraídos analisando o uso da CPU do microcomputador. Esta analise é possível utilizando o Gerenciador de Tarefas no SO windows, que apresenta todos os processos que estão em execução no computador em tempo real. É importante ressaltar que o programa GNS3 cria processos separados para cada roteador, deste modo é possível analisar a utilização da CPU individualmente para o roteador R1 e o roteador R3. Os valores de médias apresentados no trabalho, foram calculados utilizando média aritmética.

4.1 TESTE DA VELOCIDADE DE TRANSFERÊNCIA E UTILIZAÇÃO DA CPU

Para realizar o teste de transferência de dados entre as máquinas virtuais, efetuou-se a instalação de um servidor e cliente TFTP em cada máquina. Pode ser visualizado um exemplo do teste de transferência na Figura 9. O lado esquerdo da Figura 9 representa o cliente TFTP, que está enviando um arquivo da máquina PC-A para o PC-C, e do lado direito da Figura representa o servidor TFTP recebendo o arquivo na máquina PC-C que está sendo enviada pelo PC-A.

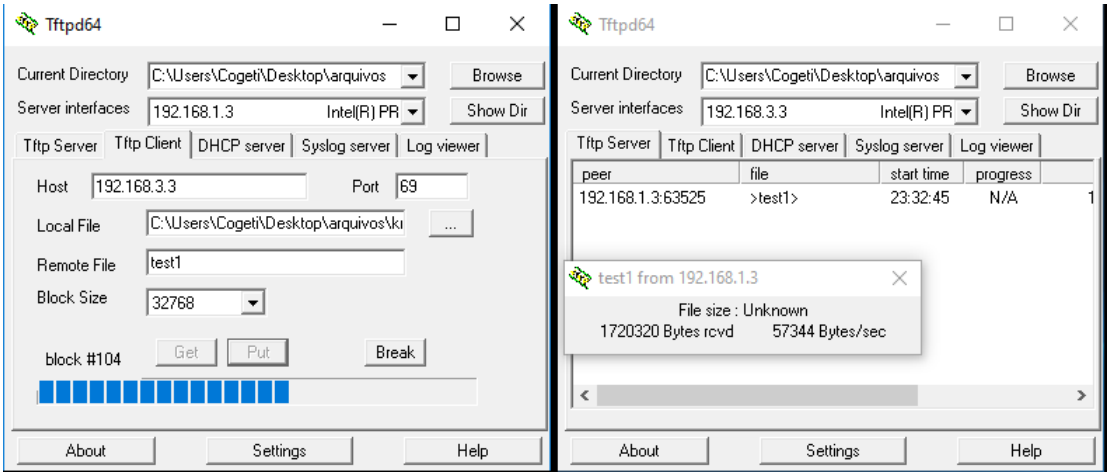

Figura 9 – Cliente e servidor TFTP

Fonte: Autoria própria.

No teste de transferência utilizamos um arquivo de imagem no formato .png. Para nos certificarmos de que a velocidade de transferência de dados seria a mesma indiferente do tipo de arquivo, realizamos o testes com outros tipos de arquivos, e o resultado obtido foi de que a velocidade permanece a mesma, em ambas a VPNs IPsec e SSL. Por este motivo apenas abordaremos os testes realizados com o arquivo de imagem. Outro ponto a ser destacado, realizamos testes com outros servidores e clientes TFTP para verificar se houve diferença entre as velocidades de transferência dos arquivos, e os testes provaram que não houve alteração, sendo assim, utilizou-se para realizar os testes apenas o cliente e servidor TFTP apresentado na Figura 9.

Na Tabela 3, verifica-se os resultados obtidos nos testes de comparação entre as duas VPNS implementadas. Apresentaremos apenas os resultados dos testes realizados em relação a máquina PC-A para a máquina PC-C, devido ao teste inverso apresentar um resultado muito próximo, que podemos dizer igual, tanto nos testes de velocidade de transferência quanto no teste de utilização da CPU.

Tabela 3 – Teste de velocidade de transferência

VPN	Block size	Tamanho arquivo	Tempo médio	Velocidade média
VPN IPsec	32768 bits	2950 KBytes	53,4 segundos	55,25 KB/s
VPN SSL	1024 bits	275 KBytes	38,4 segundos	7,16 KB/s

Para obter os dados de tempo médio e velocidade média apresentado na Tabela 3, realizou-se o teste de transferência 10 vezes, número considerado o suficiente para realizar este tipo de teste devido a ser um ambiente controlado, onde não apresentam variações nos

resultados. O tamanho do bloco de medida é selecionado no cliente TFTP, que pode ser visualizado na Figura 9, no campo Block Size, as opções disponíveis são de 128 bits para o valor mais baixo, até 32768 bits o valor mais alto. Para os testes executados na VPN IPsec utilizou-se o tamanho de bloco 32768 bits, devido ao fato da velocidade ser maior conforme o tamanho do bloco era aumentado. Para a VPN SSL usou-se o tamanho de bloco 1024 bits, porque em tamanhos menores a velocidade diminuía, e em tamanhos maiores a velocidade apresentava mudanças para menos ou para mais. Muitos blocos eram necessários serem retransmitidos por alguma falha no envio, assim fazendo com que o tempo para transferir o arquivo fosse elevado. O dado mais importante que pode ser visualizado na Tabela 3 é a média de velocidade das VPNs, a qual foi utilizada como informação principal para comparação dos testes. Os resultados apresentados na Tabela 3, apresentam que a VPN IPsec obteve melhor desempenho em relação a VPN SSL, pois a diferença de velocidade média, em percentual, entre as duas VPNs, foi de 771,64% maior na velocidade de transferência da VPN IPsec com relação a VPN SSL. Contudo, com está diferença na velocidade, desconsiderou-se estes resultados como um fator de decisão entre qual protocolo oferece uma melhor velocidade de transferência em uma infraestrutura física, porque eles não refletem no desempenho real que as VPNs teriam em um ambiente real, configurados em roteadores físicos.

O segundo teste realizado com as VPNs, foi o teste de utilização da CPU pelos processos do SO windows que representam a emulação de roteador. Os resultados deste teste são apresentados na Tabela 4.

Tabela 4 – Utilização da CPU pelos roteadores

Nome	Roteador	Uso médio da CPU
VPN IPsec	R1	2,10 %
	R3	1,44%
VPN SSL	R1	0,80 %
	R3	0,66 %

Para obter os dados de uso médio da CPU pelos roteadores, executamos uma transferência de dados de uma máquina virtual para outra, e anotamos as oscilaçoes do uso da CPU durante um período de 5 minutos. Neste resultado da Tabela 4, na VPN IPsec o uso do roteador R1 é mais alto porque no teste enviamos os arquivos da máquina virtual PC-A para a máquina virtual PC-C, se o teste fosse inverso, o uso do roteador R3 seria maior neste caso. Para a VPN SSL o uso da CPU do roteador R1 é maior em ambos os casos de testes, tendo o mesmo resultado indiferente do envio de dados ser realizado de PC-A para PC-C ou o inverso, devido a implementação do VPN SSL ser configurada apenas no roteador R1, que realiza todo o processamento de tunelamento com o cliente que conectar-se a VPN utilizando o AnyConnect, que neste trabalho, é instalado na máquina virtual PC-C que pertence a rede do roteador R3.

Comparando os dados entre as duas VPNs, pode-se notar que a VPN IPsec tem uma maior utilização da CPU em relação a VPN SSL em ambos os roteadores R1 e R3. Apesar dos valores serem baixos, se calcularmos a porcentagem entre as duas VPNs, o roteador R1 da VPN IPsec tem um uso 162,5% maior que o roteador R1 na VPN SSL, da mesma maneira no roteador R2 com uso de 118,18% maior. Após a análise dos dados de utilização da CPU, notou-se que o valor da porcentagem de uso do processador é inferior, o que levou a realização de uma pesquisa sobre os processadores que são utilizados nos roteadores físicos, e aplicar uma comparação com o processador do computador em que desenvolvemos os projetos. Os resultados desta busca são apresentados na Tabela 5.

Tabela 5 – Comparação dos Processadores

Modelo	Motorola Freescale 7448	AMD FX-8350
Núcleos/Threads	1	8/8
Clock speed	1,67 ghz	4,0 ghz
Memória cache	32KB L1 + 1MB L2	384KB L1 + 8MB L2 + 8M L3

A comparação entre os processadores usados em roteadores físicos com o processador utilizado na máquina de execução dos projetos que emula os roteadores virtuais, não faz parte dos objetivos do trabalho, então apenas utilizou-se os dados parar ter uma noção de como pode ser impactante o uso da CPU em um ambiente real. Como pode ser visto na Tabela 5, as especificações do processador FX-8350 utilizado na computador é muito superior ao processador Freescale 7448, o que pode se concluir com estes dados, é que nos deparando com os dados da Tabela 4, que tem valores muitos baixos, a pequena diferença que existia em quantidade entre o uso das duas VPNs, seria bem elevada se os resultados dos dados obtidos no ambiente virtual, refletissem na mesma proporção para o ambiente real. Com esta análise que realizamos, não se pode garantir que em uma estrutura física de implementação de VPN, os resultados seriam próximos como indicado neste trabalho, mas se fossem, esse seria uma fator muito importante de decisão na escolha de qual protocolo utilizar pra a criação de VPNs entre o protocolo SSL e o IPsec.

4.2 ANÁLISE DA SEGURANÇA DAS VPNS

Existem dois fatores importantes quando comparamos IPSec e SSL, a autenticação e a criptografia. A autenticação garante a identidade do usuário ou sistema, garantindo que outras pessoas ou sistemas não autorizados não se passem por verdadeiros. A criptografia é usada para manter a privacidade dos dados que trafegam pela Internet. Ambos os protocolos suportam o uso de criprografia. O IPSec suporta os algorítimos RC4 (40 ou 128 bit), AES (256 bit), DES (56 bit) e o 3DES (112 ou 168 bit). Tipicamente o IPSec utiliza o DES (56 bit) ou 3DES (112 ou 168 bit). Já o SSL suporta RC4 (40 ou 128 bit), DES (56 bit) e 3DES (112 ou 168 bit). Ao contrário da criptografia, tanto o IPSec quanto o SSL podem utilizar as mesmas técnicas de autenticação. Porém, a VPN IPsec pode ser considerada mais segura, devido a autenticação do IPSec ser associado aos roteadores em que a VPN é configurada. No caso da VPN SSL usuários podem acessar o WebVPN gateway, realizar o download do AnyConnect, e configurar a conexão e obter acesso a rede protegida, se o usuário tiver um conta de acesso, mas não é possível garantir a identidade do usuário, pois apenas o dados que trafegam no túnel são criptografados, e a conta de acesso pode ser interceptada quando utilizada no dispositivo para realizar a conexão.

5 CONCLUSÃO

Conclui-se que não é possível realizar uma comparação justa de desempenho entre as VPNs IPsec e SSL por meio dos testes realizados, não sendo pela metodologia dos testes não ser eficaz, e sim devido a implementação de VPNs em um ambiente virtual como utilizando o programa GNS3 não conseguir reproduzir de forma coerente o desempenho de uma VPN.

O resultado de comparação do uso da CPU pelso roteadores apresentado nos leva a concluir que a VPN SSl obteve um resultado melhor no teste de utilização da CPU, por utilizar uma porcentagem bem menor em relação a VPN IPsec.

Não é possível também comparar analisando a segurança das VPNs devido as criptografias disponíveis para utilização serem muito próximas, ou as mesmas em muitos casos. Embora seja perfeitamente possível realizar a implementação de VPNs conforme foi apresentado no trabalho, e verificar o seu funcionamento. Como objeto para estudo e entendimento de como funciona cada parte de uma VPN e como realizar toda a configuração em um ambiente virtual e inclusive real, este trabalho atende muito bem a este objetivo. Este trabalho serve de referência para quem deseja estudar VPNs e realizar trabalhos nesta área de segurança de redes que é importante no mundo da informática.

O método de implementação virtual empregado no trabalho não se mostrou eficiente, assim o método de implementação real seria o indicado para se realizar testes e comparação dos resultados entre as VPNs IPsec e SSL.

5.1 TRABALHOS FUTUROS

Buscar alternativas para realizar a implementação em ambiente real para verificar o desempenho real das VPNs e realizar uma comparação eficiente. Como trabalho futuro, pode-se buscar uma metodologia para solucionar o problema de fragmentação dos pacotes enviados pelos roteadores, devido à sobrecarga sobre o cabeçalho dos pacotes IP ocasionados pela

criptografia das VPNs que acrescentam bytes no cabeçalho dos pacotes, assim ultrapassando o Maximum Transmission Unit (MTU) que é o tamanho máximo possível do número de bytes que um pacote pode ter, de valor 1500 bytes.

Em trabalhos futuros podem ser utilizadas técnicas, como a alteração do tamanho do MTU antes da aplicação da criptografia sobre os pacotes, ou então a pré-fragmentação dos pacotes a fim de obter resultados melhores no desempenho da VPN. E por último, para tentar melhorar o desempenho, é possível usar a compressão dos pacotes IP para enviar os dados, e analisar os resultados obtidos, o que complementa as implementações utilizadas neste trabalho.

REFERÊNCIAS

ACADEMIC, B. **Cryptology**. August 2016. Disponível em: <http://academic-eb-britannica.ez48.periodicos.capes.gov.br/levels/collegiate/article/109639>.

BADRA, M.; HAJJEH, I. Enabling VPN and secure remote access using TLS protocol. **IEEE International Conference on Wireless and Mobile Computing, Networking and Communications 2006, WiMob 2006**, p. 308–314, 2006.

BHIOGADE, M. S. **Secure Socket Layer**. 2002. 85,90 p.

CARISSIMI, A. da S.; GRANVILLER, L. Z.; ROCHOL, J. **Redes de Computadores: Volume 20 da Série Livros didáticos informática UFRGS**. 20. ed. São Paulo: BOOKMAN COMPANHIA ED, 2009. 392 p.

CHEN, F. et al. The research and implementation of the vpn gateway based on ssl. In: . [S.l.: s.n.], 2013. p. 1376–1379.

CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN, A. D. **Firewalls e Segurança na Internet**: Repelindo o hacker ardiloso. 2. ed. Porto Alegre: Bookman, 2005. 400 p.

CISCO, S. **CCNA Security**. [S.l.], 2012.

COUNCIL, N. R. **Computers at Risk: Safe Computing in the Information Age**. Washington, DC: The National Academies Press, 1991. ISBN 978-0-309-07481-0. Disponível em: <https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information-age>.

DHALL, H. et al. Implementation of ipsec protocol. In: . [S.l.: s.n.], 2011. p. 176–181.

DIAB, W. B.; YVELINES, S.-q.; BASSIL, C. VPN Analysis and New Perspective for Securing Voice over VPN Networks. **Fourth International Conference on Networking and Services VPN**, p. 73–78, 2008.

ELKEELANY, O.; MATALGAH, M. M.; QADDOUR, J. Remote access virtual private network architecture for high-speed wireless internet users. **Wireless Communications and Mobile Computing**, v. 4, n. 5, p. 567–578, 2004. ISSN 15308669.

GÓMEZ, A. F.; MART, G.; CÁNOVAS, Ó. New security services based on PKI. **Future Generation Computer Systems**, Elsevier, v. 19, p. 251–262, 2003.

KAPOOR, B.; PANDYA, P.; SHERIF, J. S. Cryptography A security pillar of privacy , integrity and authenticity of data communication. **Kybernetes**, v. 40, n. 9/10, p. 1422 – 1439, 2011.

KRAWCZYK, H. Sigma: The 'sign-and-mac' approach to authenticated diffie-hellman and its use in the ike protocols. **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**, v. 2729, p. 400–425, 2003.

LAKBABI, A. et al. VPN IPSEC & SSL Technology. **Next Generation Networks and Services NGNS**, n. December, p. 2–4, 2012.

LIU, N. et al. Security analysis and configuration of ssl protocol. In: . [S.l.: s.n.], 2008. p. 216–219.

LUIS, A. et al. **IPSec Segurança de Redes – INF542**. 2003. 1–49 p.

MISRA, S. et al. Design and implementation analysis of a public key infrastructure-enabled security framework for ZigBee sensor networks. **INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS**, n. November 2014, p. 1992–2014, 2016.

MORENO, E. D.; CHIARAMONTE, R. B. **Criptografia em Software e Hardware**. [S.l.: s.n.], 2005. 288 p. ISBN 85-7522-069-1.

NAKARUMA, E. T.; GEUS, P. L. de. **Segurança de Redes**: em ambientes cooperativos. 1. ed. São Paulo: Novatec, 2007. 482 p.

NARAYAN, S.; BROOKING, K.; VERE, S. D. Network Performance Analysis of VPN Protocols : An empirical comparison on different operating systems. 2009.

NIEMIEC, M.; MACHNIK, P. Authentication in virtual private networks based on quantum key distribution methods. **Multimedia Tools and Applications**, Springer Netherlands, p. 10691–10707, 2016.

SCHNEIER, B. **Applied Cryptography**: Protocols, algorthms, and source code in c. [S.l.: s.n.], 1996. 666 p. ISBN 0471128457.

SHARMA, T. Security in Virtual private network. **International Journal of Innovations & Advancement in Computer Science**, v. 4, p. 669–675, 2015.

SILVA, L. S. da. **Virtual Private Network**: Aprenda a construir redes privadas virtuais em plataformas linux e windows. 1. ed. São Paulo: Novatec, 2002. 1 p.

SILVA, L. S. da. **Public Kei Infrastructure - PKI**. [S.l.: s.n.], 2004.

STALLINGS, W. **Information Security**: A secure foundation for vpns. 1. ed. [S.l.: s.n.], 1998.

STALLINGS, W. **Criptografia e segurança de redes**: Princípios e práticas. 4. ed. São Paulo: Pearson Education, 2008. 492 p.

TERADA, R. **Segurança de Dados**: Criptografia em rede de computador. 2. ed. São Paulo: Blucher, 2008. 305 p.

TYSON, J.; CRAWFORD, S. **How VPNs Work**. 2016. Disponível em: <http://computer.howstuffworks.com/vpn3.htm>.

YUAN, R.; STRAYER, W. T. **Virtual Private Networks**: Techonologies and solutions. 1. ed. [S.l.: s.n.], 2001. 1 p.

ZHANG, X.; SONG, M.; SONG, J. A solution of electronic authentication services based on pki for enabling e-business. In: . [S.l.: s.n.], 2009. p. 431–436.

ZHANG, Y. et al. A New Approach for Accelerating IPSec Communication. **International Conference on Multimedia Information Networking and Security**, 2009.