MARINHA DO BRASIL

DIRETORIA DE ENSINO DA MARINHA

CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM

SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ANÁLISE DE TECNOLOGIAS DE PROTEÇÃO:

um estudo do uso da conexão segura para a Marinha do Brasil

1T (QC-CA) Rodrigo Giovanni Ferreira Cruz Andrade

Rio de Janeiro

2020

1T(QC-CA) Rodrigo Giovanni Ferreira Cruz Andrade

ANÁLISE DE TECNOLOGIAS DE PROTEÇÃO:
um estudo do uso da conexão segura para a Marinha do Brasil

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk da Marinha do Brasil como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientador Técnico: CF (RM1-T) William Augusto Rodrigues de Souza

Orientador Acadêmico: Prof. Dr. Anderson Oliveira da Silva

CIAW

Rio de Janeiro

2020

ANDRADE, Rodrigo Giovanni Ferreira Cruz.
Análise de Tecnologias de Proteção: um estudo do uso da conexão segura para a Marinha do Brasil / Rodrigo Giovanni Ferreira Cruz Andrade. Rio de Janeiro: CIAW, 2020.
Total de folhas. 95f.: il.

Orientadores: CF(RM1-T) William Augusto Rodrigues de Souza; Dr. Anderson Oliveira da Silva.

Monografia (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada, Rio de Janeiro, 2020.

1. Comunicação Segura. 2. TLS. 3. VPN. 4. SSL. I. Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada. II. Título.

1T (QC-CA) Rodrigo Giovanni Ferreira Cruz Andrade

ANÁLISE DE TECNOLOGIAS DE PROTEÇÃO:

um estudo do uso da conexão segura para a Marinha do Brasil

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk da Marinha do Brasil como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida, MSc. (Banca Examinadora)

Marinha do Brasil

CF (RM1-T) William Augusto Rodrigues de Souza, PhD (Orientador Técnico)

Marinha do Brasil

Prof. Anderson Oliveira da Silva, PhD (Orientador Acadêmico)

PUC-RJ

Rio de Janeiro, 24 de março de 2020.

Dedico este trabalho àqueles que, por algum motivo, possam utilizar seu conteúdo para auxiliar em outros trabalhos ou adquirir algum conhecimento sobre o assunto.

AGRADECIMENTOS

Primeiramente ao nosso Senhor Jesus Cristo, que pôde me abençoar e dar sabedoria nos momentos de maior dificuldade.

Aos meus pais, Geraldo e Eliana, que mesmo longe intercederam para a realização deste trabalho.

À Dona Leci, Liliana, Marina, João e seus familiares pelo apoio no meu primeiro ano de carreira no Rio de Janeiro.

À Professora Márcia pela ajuda da elaboração da matriz analítica inicial sobre o tema proposto.

Ao meu Orientador, Professor Anderson Oliveira da Silva, pelo fornecimento de material acadêmico e do delineamento no qual o trabalho deveria prosseguir.

Ao Capitão de Fragata William Augusto Rodrigues de Souza pela orientação, sugestão e verificação da produção deste trabalho.

Aos oficiais Fernando (da DCTIM) e Augusto (do CTIM) e colegas de turma Zandonai, Pereira e Edson pelas opiniões, correções, sugestões e indicação de material de consulta para realização deste trabalho.

Aos usuários do OS: EgonRunner, foxmanrj, Kinopio, konde10 e Sephirothrx7.

À oficial Sabrina e ao amigo e irmão em Cristo Pedro pelo auxílio na obtenção de normas técnicas para consulta e realização deste trabalho.

“Defenda a sua causa contra o seu vizinho, mas não revele nada que alguém lhe tenha contado a respeito do assunto. Do contrário todos ficarão sabendo que você não consegue guardar segredos, e você nunca mais se livrará desta vergonha.”

(Provérbios 25, 9-10).

RESUMO

O grande problema de segurança da informação que se enfrenta no uso da rede de computadores, sobretudo em redes públicas, é a garantia de se manter a integridade, autenticidade e sigilo das informações trafegadas. Nesse sentido, o objetivo deste trabalho é apresentar duas soluções criadas para prover comunicação segura, são elas a *Transport Layer Security* (TLS) e a *Virtual Private Network* (VPN). O TLS apresentou várias atualizações desde a sua concepção no antigo *Security Socket Layer* (SSL) e, atualmente, encontra-se na versão 1.3. Neste estudo, a análise foi realizada por meio da ferramenta Qualys no servidor *web* da Marinha do Brasil (MB), e verificou-se que a versão 1.3 ainda não é utilizada. O uso de um protocolo desatualizado pode, futuramente, comprometer a segurança da informação trafegada caso alguma vulnerabilidade seja explorada. Em relação à VPN, foi realizado um estudo de soluções *open source* e corporativas existentes para implementação. Como não foi possível obter informações atualizadas sobre a infraestrutura VPN utilizada na Rede de Comunicações Integradas da Marinha (RECIM), o estudo foi elaborado com a plataforma VMware *Citrix XenApp 6.5 Plantium*.. Até 2017 essa era a solução adota pela Marinha do Brasil, para fornecer acesso remoto aos usuários credenciados. Apesar disso, foi verificado pelos órgãos de TI, que essa solução apresentou obsolescência sendo necessária a busca de uma nova implementação para o serviço de VPN de acesso remoto. Nesse sentido, este trabalho propõe a adoção de uma solução open source como medida de mitigar os custos de licenciamento de software e manutenção, bem como recomendar a utilização do manual de boas práticas de seleção de VPN proposto pela ISO/IEC 27033-5.

Palavras-chave: Criptografia. VPN. TLS. SSL. Comunicação Segura.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade certificadora
ACL	*Access Control List*
AEAD	*Authenticated encryption with associated data*
AH	*Autentication header*
BITS	*Bump-in-The-Stack*
BITW	*Bump-in-The-Wire*
C-ApA-SIC	Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações
CCE	Criptografia de curvas elípticas
DH	*Diffie-Hellman*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
DPI	*Deep packet inspection*
DSS	*Digital Signature Standard*
DTLS	*Datagram Transport Layer Security*
EAP	*Extensible Authentication Protocol*
EB	Exército Brasileiro
ECC	*Elliptic curve cryptography*
ESP	*Encapsulating Security Payload*
EUA	Estados Unidos da América
FAB	Força Aérea Brasileira
FTP	*File Transfer Protocol*
GNU	*General Public License*
HMAC	*Hashed Message Authentication Code*
HTML	*Hypertext Markup Language*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IDS	*Intrusion detection system*
IETF	*Internet Engineering Task Force*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*

ISAKMP	*Internet Security Association and Key Management Protocol*
ISO	*International Organization for Standardization*
ITI	Instituto Nacional de Tecnologia da Informação
ITU	*International Telecommunication Union*
KDC	*Key Distribution Center*
L2TP	*Layer 2 Tunneling Protocol*
LAN	*Local Area Network*
LCR	Lista de Certificados Revogados
MAC	*Message Authentication Code*
MB	Marinha do Brasil
MITM	*Man-in-the-middle*
MPLS	*MultiProtocol Label Switching*
NAT	*Network Adress Translation*
NIST	National Institute of Standards and Technology
NSA	*National Security Agency*
OCSP	*Online Certificate Status Protocol*
OSI	*Open System Interconnection*
PFS	*Perfect Forward Secrecy*
PKI	*Public-Key Infrastructure*
POODLE	*Padding Oracle on Downgraded Legacy Encryption*
RECIM	Rede de Comunicações Integradas da Marinha
RSA	*Rivest-Shamir-Adleman*
SA	*Security Association*
SMTP	*Simple Mail Transfer Protocol*
SPI	*Security Parameters Index*
SSL	*Security Socket Layer*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
TLS	*Transport Layer Security*
TOR	*The Onion Router Project*
TTL	*Time to Live*
UDP	*User Datagram Protocol*
VPN	*Virtual Private Networks*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

Com a crescente utilização de computadores e redes de computadores, as tecnologias de segurança tornaram-se um requisito essencial. Apesar de parte das informações que trafegam nas redes de comunicação ser de acesso público, há operações que requerem algum nível de confidencialidade, principalmente quando consideramos a rede de uma organização militar como a Marinha do Brasil (MB). Existem várias soluções tecnológicas de proteção para garantir conexões seguras, porém, mesmo com tantas opções disponíveis, os principais aspectos almejados pelas organizações são a garantia da integridade, autenticidade, não repúdio e sigilo das informações trafegadas na rede. Para implementação dessa segurança, podem ser adotadas políticas para o norteamento do modo de utilização da rede de comunicação, abordando tanto aspectos da tecnologia quanto o próprio comportamento dos usuários na rede.

Existem tecnologias de segurança que colocam em ação algoritmos e protocolos específicos. Normalmente, uma das infraestruturas empregadas em rede de computadores e discutida na literatura é a do sistema de assinaturas e certificados digitais baseados na criptografia de chaves públicas. Com o intuito de facilitar o gerenciamento, tal infraestrutura necessita de certas padronizações para ser implementada, permitindo que redes de computadores instalados em locais físicos distintos possam se comunicar entre si.

Nesse contexto, este trabalho buscou discutir alguns dos recursos que podem ser utilizados para garantir uma comunicação segura em uma rede de computadores. Serão abordadas as Redes Privadas Virtuais, ou *Virtual Private Networks* (VPN), com discussões sobre o protocolo *Security Socket Layer* (SSL) e seu o sucessor, o *Transport Layer Security* (TLS).

1.1 Apresentação do problema

O problema tratado neste trabalho baseou-se na discussão das ferramentas de proteção que a MB pode utilizar para uma conexão mais segura ou, ainda, melhorar a infraestrutura atual.

1.2 Justificativa e relevância

O estudo das ferramentas de tecnologia de proteção é importante para ampliar a compreensão sobre o modo como essas ferramentas são implementadas e utilizadas enquanto política de proteção para uma conexão segura.

Ressalta-se a necessidade dessa proteção por se tratar de dados sigilosos da MB, exigindo, portanto, uma política de segurança eficiente e eficaz, compatível com o nível de segurança exigido da instituição. Destaca-se, ainda, a importância cada vez maior de se utilizar ferramentas de Tecnologia da Informação (TI) de qualidade para uma comunicação satisfatória, interna e externa, garantindo uma política adequada de segurança da informação da MB.

1.3 Objetivo

Os objetivos desta pesquisa foram definidos de forma a trazer conhecimento para a MB em relação à estrutura de algumas das tecnologias empregadas para viabilização de uma comunicação segura.

1.3.1 Objetivo geral

Descrever como é realizado o trabalho que envolve as tecnologias de comunicação segura, como o protocolo SSL e sua versão mais recente, o TLS, assim como a tecnologia VPN para proteção das comunicações na MB.

1.3.2 Objetivo específico

Além da importância para a MB, esta pesquisa também tem a função de servir como material de estudo para futuros oficiais que realizarão as disciplinas do Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações (C-ApA-SIC).

2 REFERENCIAL TEÓRICO

Este capítulo introduz os principais conceitos sobre: o funcionamento de uma comunicação segura; os mecanismos que esta utiliza, como a criptografia; o resumo de mensagens; a assinatura digital; o certificado digital e a infraestrutura de chaves públicas. Ao final, serão abordadas as tecnologias de proteção segura TLS e VPN, que são o foco de estudo desta pesquisa.

2.1 Segurança de redes de computadores

Atualmente, com a crescente utilização da rede de computadores e principalmente da internet, há uma preocupação constante no que diz respeito à segurança dos dados trafegados entre instituições públicas e privadas, ambientes acadêmicos e organizações militares. No entanto, essa preocupação nem sempre esteve presente durante as primeiras décadas do surgimento de mecanismos que interligassem computadores. No início, segundo Tanenbaum e Wetherall (2011), não havia preocupação em relação à segurança, justamente pelo número reduzido de pessoas que utilizavam a infraestrutura. A partir do momento em que o uso das redes de computadores se tornou um serviço acessível a milhões de pessoas, foi necessário oferecer dispositivos que pudessem garantir a segurança no tráfego de dados, principalmente daqueles sigilosos.

Em geral, o grande problema de segurança na rede de computadores está relacionado à ação de pessoas mal-intencionadas, que buscam roubar informação ou até mesmo prejudicar alguém. Segundo Forouzan (2007), há quatro princípios básicos ou serviços que devem ser levados em consideração na criação de um processo de comunicação segura de uma mensagem: confidencialidade, integridade, autenticação, não repúdio. Tais serviços estão descritos a seguir (Figura 1):

a) **Integridade**: consiste em garantir que a informação enviada esteja protegida contra modificações sem a permissão explícita do emissor daquela mensagem. Segundo Abílio *et al*. (2007), a modificação de integridade pode ser feita por ações de escrita, alteração de conteúdo da mensagem, alteração de *status*, remoção e criação de informações;
b) **Autenticação**: consiste em garantir que o receptor da mensagem esteja certo de que a informação recebida corresponda a um determinado emissor. Segundo Abílio *et al*.

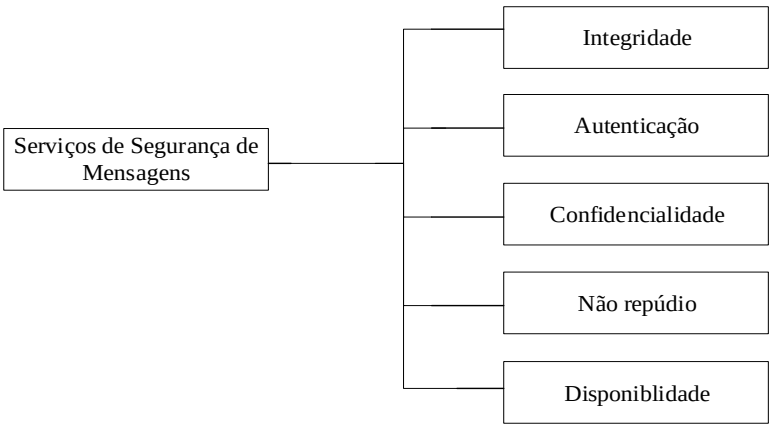
(2007), a verificação de autenticidade é um mecanismo de proteção de um serviço/informação contra a personificação por intrusos;

c) **Confidencialidade**: consiste em garantir que somente o emissor e o receptor da mensagem consigam compreender o conteúdo da informação. Esse serviço de segurança será garantido pelo uso de criptografia da informação, transformando um **texto claro** em um **texto cifrado**. O texto cifrado é então enviado ao receptor, e este possui mecanismos para transformar, novamente, a informação em texto claro igual ao emitido (KURY ABÍLIO, CONCEIÇÃO DA GRAÇA, et al., 2007). Essa criptografia pode ser feita por dois métodos que serão abordados na seção 2.2.

d) **Não repúdio**: representa o serviço em que um emissor não deva ser capaz de rejeitar uma informação que ele próprio criou. Essa propriedade garante ao receptor a irretratabilidade do emissor (TANENBAUM e WETHERALL, 2011).

e) **Disponibilidade**: está relacionada à permanência da acessibilidade dos dados durante a comunicação (FERNANDES DE MORAES, 2010).

Figura 1 – Serviços de segurança de mensagem



Fonte: elaborado pelo autor.

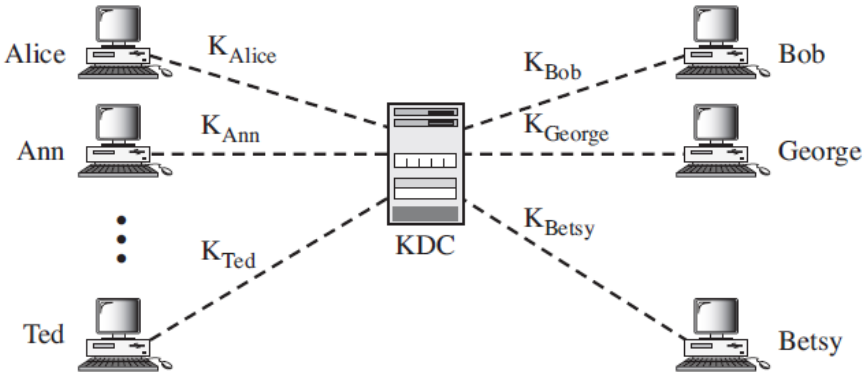
2.1.1 Infraestrutura de comunicação segura

O modelo de uma infraestrutura de comunicação segura visa garantir os princípios básicos de confidencialidade, integridade, autenticidade e não repúdio. O processo que a informação irá sofrer para ser enviada de forma segura está descrito na Figura 3 (parte do emissor) e Figura 4 (parte do receptor).

Quanto à descrição das etapas que ocorrem no emissor (numeração conforme Figura 3):

1. Incialmente, é criada a mensagem em texto claro (que pode ser entendido por uma pessoa que conheça o idioma em questão) pelo emissor;
2. O emissor gera um *digest* (seção 2.3) da mensagem por meio de um cálculo matemático que, por sua vez, gera um resumo, também conhecido como código *hash* (utilizando uma função *hash*). Esse cálculo cria uma representação compactada (ou resumo) da mensagem que pode ser usada para uma posterior comparação com a mensagem original, verificando assim a sua integridade. Segundo Forouzan (2007), a mensagem e o *digest*, nesse modelo de comunicação segura, podem ser trabalhados separadamente, salientando que o *digest*, quando enviado ao receptor, deve permanecer em local seguro ou criptografado;
3. Por meio de um algoritmo assimétrico (seção 2.2.2), o *digest* é assinado com a chave privada do emissor, gerando sua assinatura digital (seção 2.4). Segundo Stallings (2015), a assinatura digital pode fornecer dois requisitos de segurança, como proteção contra falsificação (integridade) e função de autenticidade. A integridade é mantida porque sistemas de assinatura atuais usam uma função *hash* nos algoritmos de assinatura. E a autenticação é garantida porque a chave privada de um usuário X não é capaz de gerar a mesma assinatura que a chave de outro usuário Y;
4. O emissor realiza a concatenação da mensagem em texto claro com a assinatura digital do *digest*,e seu certificado digital obtendo a mensagem assinada digitalmente;
5. O emissor gera uma chave de sessão que é estabelecida entre duas partes uma única vez. O esquema de geração dessa chave, que é simétrica (sessão 2.2.1), é aleatório. Porém, utiliza um sistema específico para sua geração. Em alguns sistemas, utiliza-se uma solução conhecida como *Key Distribution Center* (KDC), ou Centro de Distribuição de Chaves (Figura 2). Esse sistema permite reduzir o número de chaves de sessão criadas, pois elas são estabelecidas pelas solicitações de cada usuário. Apesar de ser criada uma chave de sessão entre dois usuários, o KDC necessita que cada membro tenha uma chave secreta para comunicação (FOROUZAN, 2007);

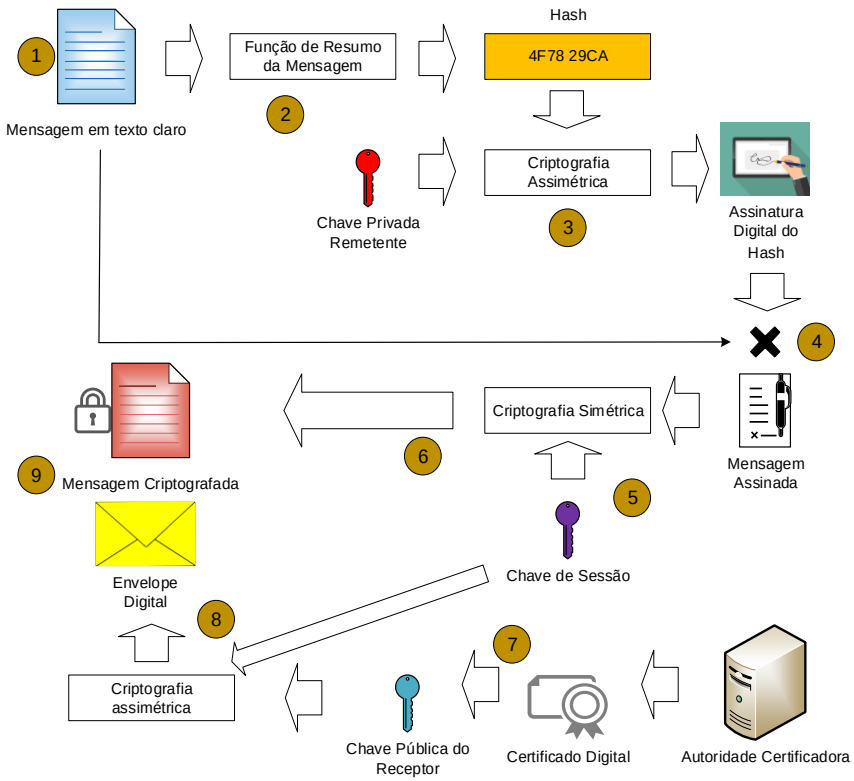
Figura 2 – Centro de distribuição de chaves de sessão



Fonte: (FOROUZAN, 2007, p. 982).

6. O Emissor utiliza então a chave de sessão criada pelo KDC para criptografar a mensagem assinada com um algoritmo simétrico;
7. Para realizar o envio da chave de sessão para o receptor, o emissor necessita da chave pública do emissor, que é obtida a partir do certificado digital do receptor. Esse certificado é emitido por uma Autoridade Certificadora (AC) confiável tanto pelo emissor quanto pelo receptor;
8. Com a chave pública do receptor certificada, o emissor criptografa a chave de sessão utilizando um algoritmo assimétrico, que irá gerar uma cifra denominada envelope digital;
9. A partir de então, o emissor envia ao receptor a mensagem assinada criptografada com o envelope digital.

Figura 3 – Esquema do processo de comunicação segura no emissor



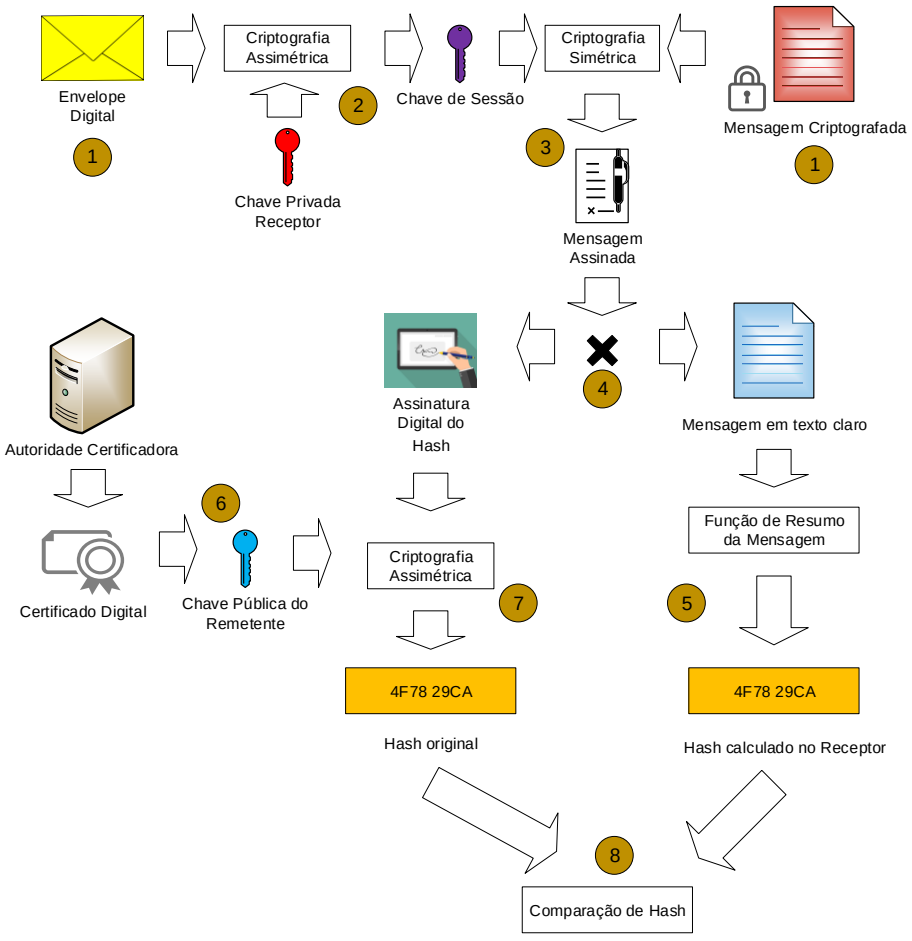
Fonte: elaborado pelo autor.
Nota: procedimento de criptografia do texto claro pela chave pública do destinatário, assinatura da cifra pelo emissor e geração do envelope digital com a chave simétrica de decriptação.

Quanto à descrição das etapas que ocorrem no receptor (numeração conforme Figura 4):

1. O receptor recebe do emissor tanto a mensagem criptografada quanto o envelope digital;
2. O receptor, usa chave privada, para realiza a decriptação do envelope digital com um algoritmo assimétrico e obter a chave de sessão enviada pelo emissor;
3. A chave de sessão é utilizada pelo emissor para decifrar a mensagem criptografada e, assim, obter a mensagem assinada digitalmente;
4. O receptor, a partir da mensagem assinada, separa a mensagem em texto claro do seu *digest* correspondente;
5. O receptor usa uma função *hash*, com base na mensagem em texto claro, para gerar um novo *digest* da mensagem;
6. O receptor obtém a chave pública do emissor validada por uma entidade confiável por meio do certificado digital do emissor;
7. Com a chave pública do emissor, o receptor usa um algoritmo assimétrico para decriptar a assinatura do emissor;

8. O receptor, de posse de dois *digests* (um calculado e outro recebido do emissor), realiza a comparação. Caso ambos sejam iguais, a comunicação será autenticada ou, caso contrário, rejeitada.
9. Terminada a sessão de comunicação, tanto o emissor quanto o receptor realizam o descarte da chave de sessão.

Figura 4 – Esquema do processo de comunicação segura no receptor



Fonte: elaborado pelo autor.
Nota: o emissor recebe a cifra e o envelope digital para realizar a decriptação da mensagem, verificando sua integridade e autenticidade.

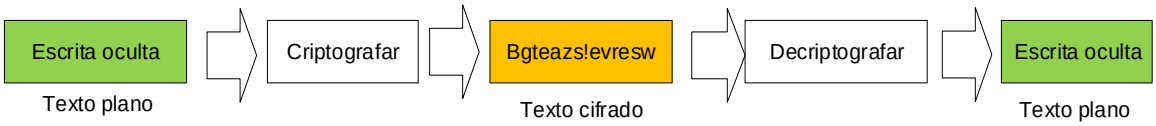
2.2 Criptografia

A seção 2.1 abordou a implementação dos serviços de autenticação, integridade e sigilo de mensagens pelo uso de certificados digitais, assinaturas digitais e infraestrutura de chaves públicas. Um ponto importante a ser comentado é que, para essas implementações serem

satisfeitas, vários recursos criptográficos são necessários. Nas próximas seções estão apresentados alguns tipos de criptografias empregados nos sistemas de comunicação segura.

Em linhas gerais, a criptografia é a técnica de converter um texto claro (mensagem original ou em texto plano) em um texto codificado, denominado cifra. Esse processo de transformação é conhecido como cifração ou encriptação (STALLINGS, 2015). Essa transformação só é possível pelo uso de algum protocolo que ambos, o emissor e o receptor, tenham estabelecido. Dessa forma é possível codificar e decodificar a mensagem sem que um terceiro possa ter acesso ao seu conteúdo. Um exemplo desse processo pode ser visto na Figura 5. Para obter um texto cifrado, é necessário um algoritmo de cifração (ou criptografia) e decriptação.

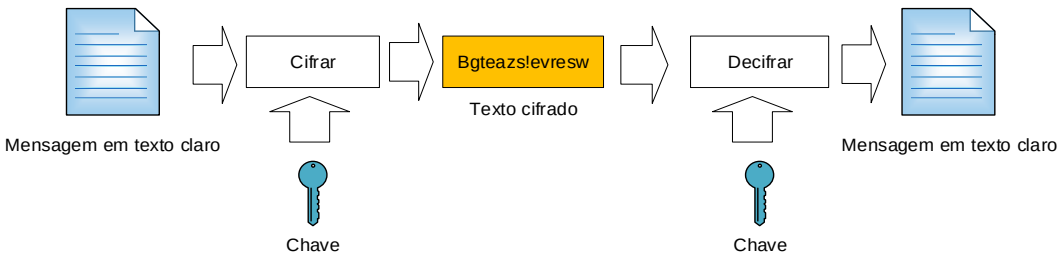
Figura 5 – Processo de criptografia



Fonte: elaborado pelo autor.

Quando consideramos os sistemas de TI, uma técnica empregada para implementar um sistema criptográfico baseia-se no uso de chaves criptográficas. A chave é um valor independente da mensagem em claro e do algoritmo que produzirá uma saída diferente (texto cifrado) (STALLINGS, 2015). Aplicando a chave no algoritmo (Figura 6), o receptor só conseguirá ter compreensão da informação se possuir uma chave compatível com a chave de cifração usada pelo emissor.

Figura 6 – Criptografia digital usando chaves



Fonte: elaborado pelo autor.

Em geral, além da segurança proporcionada pelo criptação do texto, um algoritmo de criptográfico deve ser elaborado de forma a suportar um possível ataque de texto claro

conhecido (STALLINGS, 2015):. Em outras palavras, que seja fácil de se realizar uma criptoanálise do algoritmo. De acordo com sua capacidade de resistir a ataques de criptoanálise, um sistema de encriptação é definido de duas maneiras (STALLINGS, 2015):

a) **Incondicionalmente seguro**: o texto cifrado gerado por ele não possui qualquer informação que determine parte do texto claro. Para ser implementado esse algoritmo deve possuir chave aleatória, e mais recursos devem ser gastos para o transporte dessa chave. Um exemplo é o algoritmo de chave simétrica *One-Time-Pad*.
b) **Computacionalmente seguro**: um algoritmo desse tipo deve ter custo de quebra da cifra superior ao valor da informação criptografada, e o tempo exigido para essa quebra deve ser superior ao tempo de vida útil da informação. Algoritmos que possuem essa característica são o RC4, DES, 3DES, AES (simétricos), RSA e *Dilf-Hellman* (assimétricos). Alguns desses algoritmos utilizam o conceito de chaves simétricas e assimétricas, que são um dos recursos empregados nos protocolos de comunicação segura.

2.2.1 Criptografia simétrica

A criptografia simétrica é caracterizada por possuir apenas uma chave para realizar encriptação e decriptação. A confidencialidade e a integridade da mensagem estão garantidas pelo fato de a chave de decriptografia ser a mesma usada para criptografar a mensagem, assegurando que o emissor seja o verdadeiro gerador dos dados (STALLINGS, 2015). Outra característica é a velocidade de seu processamento de cifragem/decifragemem em relação à criptografia assimétrica (ANTONIO MOTA TRINTA e CAVALCANTI DE MACÊDO, 1998). Apesar dessa vantagem, o problema desse tipo de criptografia reside no processo de envio da chave secreta por um meio seja seguro e na quantidade de chaves que seriam necessárias quando se inserem mais usuários na comunicação (ANTONIO MOTA TRINTA e CAVALCANTI DE MACÊDO, 1998).

Pela forma que tratam os dados, os algoritmos de chave aplicados na criptografia simétrica podem ser divididos em duas categorias (ABÍLIO *et al*., 2007):

a) **Algoritmos de blocos**: realizam uma subdivisão dos *bits* da mensagem em blocos de tamanho fixo. Cada bloco é cifrado individualmente, gerando um bloco de mesmo tamanho;
b) **Algoritmos de fluxo**: diferentemente do caso anterior, os algoritmos de fluxo operam em blocos de tamanho reduzido. A cifração normalmente é realizada por uma operação XOR entre a chave simétrica e o texto.

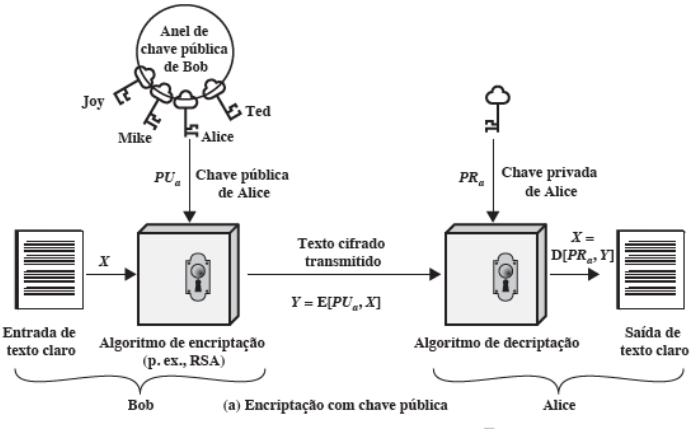
2.2.2 Criptografia assimétrica

A criptografia assimétrica é caracterizada por possuir um par de chaves diferentes, sendo uma para realizar cifração e a outra para decriptação e vice-versa. As chaves são denominadas pública e privada. A chave pública, de acordo com seu nome, deve ter acesso público, e a chave privada deve ser de conhecimento particular de seu portador (ABÍLIO *et al*., 2007).

Essa criptografia criou um conceito maior, a criptografia de chave pública baseados em funções matemáticas (STALLINGS, 2015). Diferentemente da simétrica, trouxe a solução para o problema da distribuição da chave (STALLINGS, 2015). Agora, sem a necessidade de transportar a chave entre emissor e receptor, as comunicações podem ser feitas sem a preocupação de se manter o sigilo total da comunicação. Além dessa vantagem, conforme visto na seção 2.4, a estrutura de chaves públicas permitiu o uso do conceito de assinatura digital (STALLINGS, 2015).

Para exemplificar o funcionamento de uma criptografia de chave pública, a Figura 7 mostra o funcionamento do algoritmo *Rivest-Shamir-Adleman* (RSA) supondo que Bob queira enviar uma mensagem criptografada para Alice. No sistema de chave pública ou *Public Key Infraestruct* (PKI), Bob tem acesso a várias chaves públicas, incluindo a de Alice. Bob criptografa o texto claro utilizando um algoritmo de encriptação com a chave pública de Alice, enviando a cifra a ela. Alice utiliza sua chave privada e decripta a cifra, usando o mesmo algoritmo de cifragem e obtendo, assim, o texto que Bob enviou. Observe que, tendo uma chave pública, o envio de chave não é mais necessário. A única preocupação nesse esquema é que os usuários sempre mantenham a posse de sua chave privada, pois a sua violação irá comprometer o sigilo da informação. Portanto, é possível identificar os principais protagonistas de uma cifragem assimétrica, que são: texto em claro, algoritmo criptográfico, chaves pública e privada e texto cifrado (STALLINGS, 2015).

Figura 7 – Encriptação com chave pública



Fonte: (STALLINGS, 2015, p. 202).

Apesar dos benefícios, a criptografia de chave pública apresenta alguns inconvenientes. Alguns algoritmos assimétricos possuem chaves muito grandes, geram textos cifrados maiores com seu correspondente em texto claro e em geral são bastante lentos. Se analisados sob essa perspectiva, pode-se chegar à conclusão de que não são ideais para aplicações em tempo real ou para lidar com um grande volume de dados (ABÍLIO *et al*., 2007).

No caso específico do problema do tamanho de chaves, há uma implementação denominada curvas elípticas, que fornece segurança comparável a sistemas criptográficos assimétricos como o RSA, com chaves de tamanho reduzido (STALLINGS, 2015). Vale destacar que as curvas elípticas não são um novo sistema criptográfico, mas permitem implementar o método de corpos finitos (não abordado neste trabalho) nos algoritmos criptográficos existentes. Alguns algoritmos criptográficos de chave pública usados em sistemas de comunicação segura são o RSA e *Diffie-Hellman* (STALLINGS, 2015).

2.3 Resumo de mensagem

O resumo de mensagem, ou *Message Digest*, é um recurso empregado para verificação de integridade de dados que utiliza alguns algoritmos criptográficos para realizar essa função. Esses algoritmos empregam uma função matemática que, inserida uma mensagem de tamanho variável (ou dado), produz uma sequência de informação denominada *hash* de tamanho fixo (*hash* = função matemática [mensagem]). (STALLINGS, 2015)

O que se espera de uma função *hash* é que se consiga produzir saídas igualmente distribuídas e aleatórias ao ser aplicado um grande conjunto de entradas (STALLINGS, 2015).

Dessa forma, qualquer alteração em parte da informação original poderá provocar uma mudança do código *hash.* Comparando-se o *hash* original com um posteriormente calculado, uma determinada entidade poderá verificar a integridade das informações obtidas. Vale destacar que o *hash* contém apenas uma assinatura da informação original. Sendo assim, é computacionalmente inviável recuperar a informação com base na saída gerada por uma função de hash criptográfica, visto que a transformação é feita em apenas uma única direção (STALLINGS, 2015).

De acordo com o exemplo de algoritmo hash MD5 demonstrado no Quadro 1, é feito um teste para verificar a sua saída pela modificação da entrada.

Quadro 1 – Exemplo de *digest* MD5

Mensagem	MD5
Brasil	aa43becf0d21463be7540bf3b40bf243 (33 caracteres)
Brazil	42537f0fb56e31e20ab9c2305752087d (33 caracteres)
Marinha do Brasil	4415fd5d05d0e2264f3dbcdbe025fff9 (33 caracteres)

Fonte: exemplo realizado em Webconfs (2018)

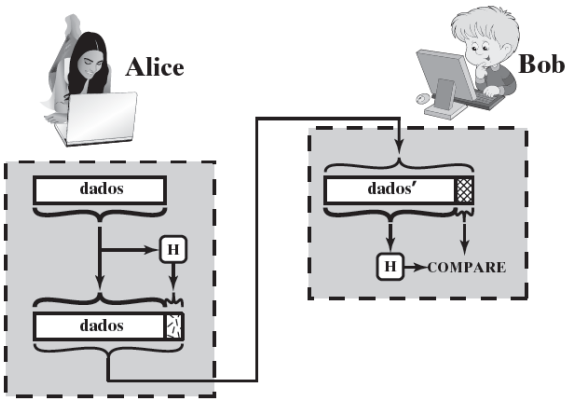
A partir do teste, as seguintes observações sobre a estrutura do *hash* observadas pelo Quadro 1 foram:

a) O resumo da mensagem possui tamanho fixo e não relacionado com o tamanho da mensagem. No teste a saída do algoritmo MD5 sempre gera 33 caracteres. Isso confirma a característica unidirecional do algoritmo (TANENBAUM; WETHERALL, 2011);
b) Qualquer alteração mínima em algum caractere, como Brasil e *Brazil*, provocará resultados de *hash* totalmente diferentes. Esse Efeito é denominado avalanche definido que uma mudança em um bit do texto claro ou um bit da chave deverá produzir uma modificação em muitos bits do texto cifrado (STALLINGS, 2015).

Tendo em vista o seu funcionamento, o resumo de mensagens pode ser utilizado para várias aplicações, como integridade de arquivos, segurança de senhas e assinaturas digitais (ABÍLIO *et al*., 2007). Considerando o caso de uma comunicação segura, o interesse do resumo de mensagem está focado na verificação de integridade da mensagem, como na Figura 8. Nesse exemplo, Alice usa uma função *hash* em seus dados e obtém o *digest* correspondente. Esse *digest* é anexado aos dados, e o conjunto enviado a Bob. Bob então separa os dados recebidos

de Alice com o *digest* de Alice. Bob realiza um novo cálculo do *digest* com base nos dados recebidos e o compara com o *digest* enviado por Alice, verificando a integridade da mensagem.

Figura 8 – *Hash* para verificação de integridade de mensagens



Fonte: (STALLINGS, 2015, p. 248).

Alguns exemplos de algoritmos de resumo de mensagens são o MD5, SHA, HMAC.

2.4 Assinatura digital

A garantia de autenticidade de informações digitais, assim como os outros mecanismos vistos na sessão 2.1 são necessários para o estabelecimento de uma comunicação segura. Diferentemente da forma convencional de assinatura de papel, os sistemas digitais devem implementar alguma maneira de identificar uma assinatura verdadeira de uma mensagem de modo que ela não possa ser forjada.

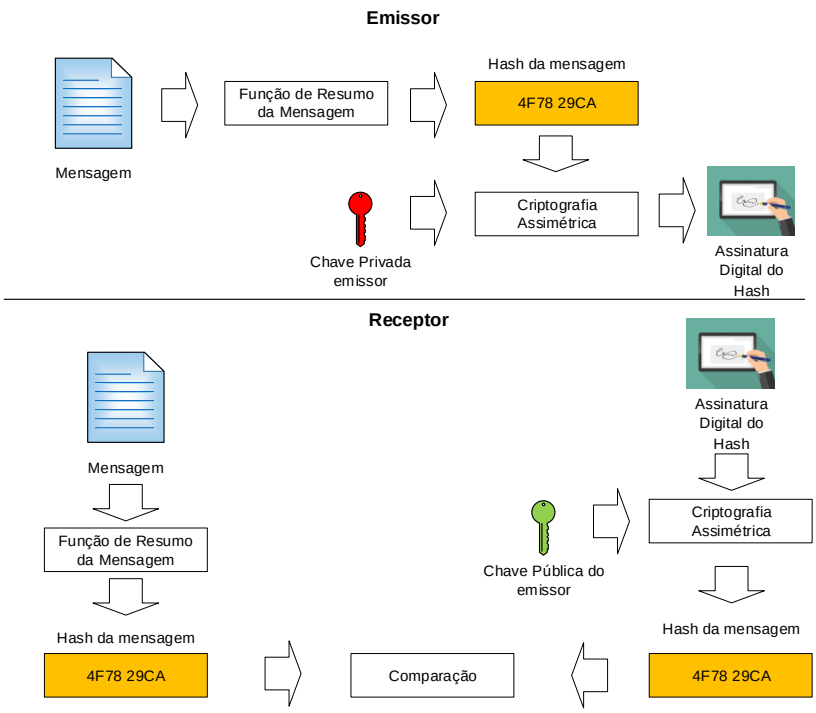
De acordo com Abílio *et al*. (2007), a assinatura digital é um tipo de assinatura eletrônica que utiliza um algoritmo de criptografia assimétrica para verificar a origem e a integridade de uma informação. Quando essa assinatura é criada, sua "marca" é vinculada ao documento eletrônico, e qualquer alteração tornará a assinatura inválida. É importante destacar que apesar de a assinatura digital ser uma técnica criptográfica, ela não torna a informação assinada sigilosa.

O mecanismo de assinatura digital utiliza a criptografia de chave pública em vez da criptografia de chave simétrica (TANENBAUM; WETHERALL, 2011). A criptografia de chave simétrica necessitaria de uma entidade central que soubesse de tudo, e na qual tanto o emissor quanto o receptor pudessem confiar. A criptografia de chave pública ou assimétrica utiliza um par de chaves (uma pública e outra privada) pertencentes a cada entidade da

comunicação. Esse esquema permite que, por exemplo, o emissor assine um documento com sua chave privada e o receptor confirme a autoria do emissor utilizando a chave pública do emissor, conforme visto na Figura 9. Assim, uma assinatura digital deve ser capaz de:

a) Ser individual para cada mensagem ou documento;
b) Identificar a autoria de quem criou o documento ou dado;
c) Possibilitar a verificação da integridade do documento ou dado caso ocorra alguma mudança em sua estrutura;
d) Garantir ao receptor do documento ou dado a capacidade de não repúdio da informação, visto que a chave privada do emissor é a única capaz de gerar uma determinada assinatura.

Figura 9 – Funcionamento da assinatura digital



Fonte: elaborado pelo autor.

Em relação à criptografia, qualquer algoritmo de chave pública pode ser utilizado para implementação da assinatura digital. O algoritmo RSA é o mais empregado, porém, em 1991, o *National Institute of Standards and Technology* (NIST) propôs a utilização do algoritmo de chave pública de *ElGamal* baseado no acordo de chave *Diffie-Hellman* em seu novo padrão, denominado *Digital Signature Standard* (DSS) (TANENBAUM; WETHERALL, 2011).

2.5 Certificado digital

Conforme mencionado na seção 2.1, o estabelecimento de uma comunicação segura necessita da ação de toda uma infraestrutura para reconhecimento das partes envolvidas. No esquema demonstrado, a criptografia baseia-se no conceito de criptografia de chave pública, em que as partes envolvidas (emissor e destinatário) não precisam compartilhar uma chave em comum. Isso é uma grande vantagem quando emissor e destinatário se conhecem, mas, muitas vezes, não é possível na prática. Dessa forma, é necessário algum método para que o receptor e o emissor possam recuperar a chave pública da outra parte assegurando que essa chave realmente seja dela. Até este momento, pode-se pensar que a estrutura do KDC, mencionada anteriormente, poderia ser uma solução, porém seria necessário que seu serviço estivesse disponível *on-line* 24 horas por dia, tornando o sistema de recuperação de chaves inviável perante uma indisponibilidade do serviço (TANENBAUM; WETHERALL, 2011).

Em virtude desse impasse, foi desenvolvida uma solução que não exige que um KDC esteja *on-line* ininterruptamente (TANENBAUM; WETHERALL, 2011). Essa solução é baseada em uma autoridade certificadora (AC), que possui a notoriedade de certificar chaves públicas pertencentes a instituições, organizações e pessoas. A função de um certificado digital é vincular uma chave pública ao nome de uma entidade (empresa, pessoa ou organização), sendo o seu conhecimento de acesso ostensivo (Figura 10). A AC tem sua própria chave pública conhecida e não pode ser falsificada, permitindo que ela possa gravar certificados em chaves públicas de qualquer entidade. Feito isso, qualquer um conseguirá baixar o certificado assinado e utilizar a chave pública da AC para extrair a chave pública da entidade a que ser quer comunicar. Em resumo, a utilização do certificado digital é vincular determinada chave pública a algum indivíduo. (TANENBAUM; WETHERALL, 2011)

Figura 10 – Geração de um certificado digital

Fonte: elaborado pelo autor.
Nota: para obtenção do certificado digital, o usuário submete sua chave pública a uma autoridade de registro, que realiza a interface do usuário e a AC, recebendo, validando e encaminhando solicitação de emissão ou revogação de certificados. A AC irá criar e assinar digitalmente o certificado do usuário para publicá-lo em uma lista de certificados válidos para consulta de autenticidade caso necessário.

2.5.1 Padrão X.509

Até o presente momento, foi visto que uma AC possui competência de reconhecer chaves públicas de usuários. Porém, como existem centenas de usuários que necessitam desse serviço, é preciso várias ACs para manter a infraestrutura de certificação digital. Considerando a presença de várias ACs, surge um problema: o padrão que cada certificado irá apresentar. Objetivando eliminar esse problema, o *International Telecommunication Union* (ITU) desenvolveu um protocolo chamado X.509, que descreve os dados do certificado de forma estruturada (FOROUZAN, 2007). O X.509 passou por três versões desde a sua padronização inicial em 1988, tendo sido descrito pela RFC 2549 (TANENBAUM; WETHERALL, 2011). Em linhas gerais, a sua formação pode ser vista no Quadro 2.

Quadro 2 – Campos de um certificado X.509

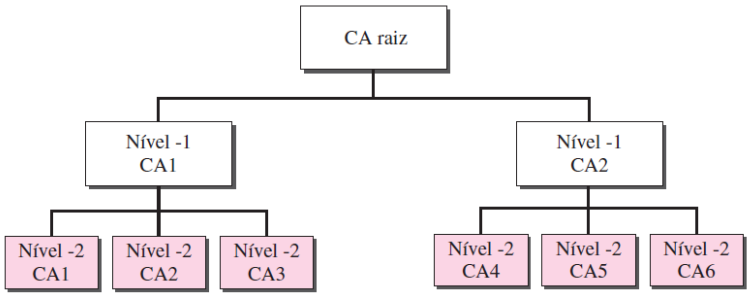
Campo	Significado
Version	Define a versão do X.509
Serial number	Este número, somado ao nome da CA, identifica o certificado de forma exclusiva
Signature algorithm	O algoritmo usado para assinar o certificado
Issuer	Nome X.500 da AC que emitiu o certificado
Validity period	Períodos inicial e final de validade do certificado
Subject name	A entidade cuja chave está sendo certificada
Public key	A chave pública da entidade certificada e a ID do algoritmo utilizado
Issuer ID	Uma ID opcional que identifica de forma exclusiva o emissor do certificado
Subject ID	Uma ID opcional que identifica de forma exclusiva a entidade certificada
Extensions	Permite que emissores acrescentem mais informações privadas ao certificado
Signature	A assinatura do certificado (assinado pela chave privada da AC)

Fonte: (TANENBAUM; WETHERALL, 2011, p. 508).

2.6 Infraestrutura de chaves públicas

A implementação do mecanismo de certificação digital, conforme visto anteriormente, necessita de uma infraestrutura que possa distribuir as chaves públicas de modo universal para acesso de qualquer entidade da comunicação. Apenas um KDC não seria suficiente para atender dezenas de requisições de acesso de chaves públicas. Para contornar esse problema de consultas a chaves públicas, foi criada uma estrutura hierárquica denominada *Public-Key Infrastructure* (PKI), exemplificada na Figura 11 (FOROUZAN, 2007).

Figura 11 – Hierarquia da infraestrutura de chaves públicas



Fonte: (FOROUZAN, 2007, p. 990).

A PKI implementa uma infraestrutura necessária para garantir a autenticidade, integridade e validade jurídica aos certificados digitais. Ela é composta por uma cadeia de autoridades certificadoras. No topo da pirâmide encontra-se a AC raiz capaz de certificar o desempenho das ACs de nível 1. No Brasil, a AC raiz é regulamentada pelo Instituto Nacional de Tecnologia da Informação (ITI) conforme determinação da Medida Provisória n. 2.200-2, (BRASIL, 2001), que estabelece os fundamentos técnicos para um sistema de certificação digital de chaves públicas.

2.7 Protocolos de comunicação segura

2.7.1 SSL

Nos primórdios da *web,* as redes de computadores se baseavam na distribuição de páginas estáticas para os usuários sem a necessidade de troca de informação entre emissor (servidor) e receptor (usuário da rede). Assim que houve a necessidade de realização de transações de mercado financeiro, bancárias e de mercadorias, houve a ideia de utilização dessa infraestrutura *web* para esse fim. Para atender essa demanda crescente de conexão segura de dados, a *Netscape Communication Corp*. introduziu, em 1995, o protocolo de segurança denominado SSL (*Secure Socket Layer*) em seus navegadores (TANENBAUM; WETHERALL, 2011). Esse protocolo permitiu a garantia dos serviços de segurança de sigilo e integridade na comunicação entre emissor e receptor pelo uso de criptografia (ABÍLIO *et al*., 2007).

Basicamente, o SSL permite a criação de um canal seguro entre duas entidades para a transferência de dados, independentemente de aplicações. Esse canal é garantido pela autenticação do servidor (sendo a autenticação do cliente opcional) de destino seguida da encriptação dos dados, adicionando um mecanismo que permite verificar a integridade das mensagens trafegadas. Pode-se definir o SSL pela seguinte estrutura (TANENBAUM; WETHERALL, 2011):

a) Negociação de parâmetros entre cliente e servidor pela comunicação inicial (ou *handshake*) utilizando chaves assimétricas;
b) Autenticação do servidor e cliente (opcional) utilizando algoritmos assimétricos, como RSA ou DSS;
c) Comunicação secreta garantida pela criptografia dos dados (utilização de troca de chaves simétricas de algoritmos, como DES ou RC4);
d) Proteção da integridade dos dados pelo uso do código de autenticação de mensagens, o *Message Authentication Code* (MAC).

Em relação ao modelo *Open System Interconnection* (OSI) da *International Organization for Standardization* (ISO), o SSL trabalha entre a camada de aplicação e

transporte. Após o estabelecimento da conexão segura, o SSL realiza a compactação e a criptografia dos dados (TANENBAUM; WETHERALL, 2011).

Um questionamento do uso do SSL é como isso pode ser visto na prática. Quando se utiliza um serviço da *web*, normalmente um protocolo bastante utilizado é o *Hypertext Transfer Protocol* (HTTP), que é um protocolo de requisição resposta. Ele permite que, após a requisição de um usuário, um servidor remoto envie uma resposta com o conteúdo da página acessada, como arquivos *Hypertext Markup Language* (HTML) e outros. Para um usuário comum, quando se utiliza o SSL isso é percebido na prática quando o HTTP é substituído pelo *Hypertext Transfer Protocol Secure* (HTTPS) (porta 443), embora seja o protocolo HTTP padrão (porta 80). Além do protocolo HTTP, ele também pode operar com *File Transfer Protocol* (FTP), *Simple Mail Transfer Protocol* (SMTP) e Telnet (ABÍLIO *et al*., 2007). É importante destacar que o SSL não se limita ao uso de navegadores da *web*, mas essa é a sua aplicação mais comum. Ele também pode oferecer autenticação mútua (TANENBAUM; WETHERALL, 2011).

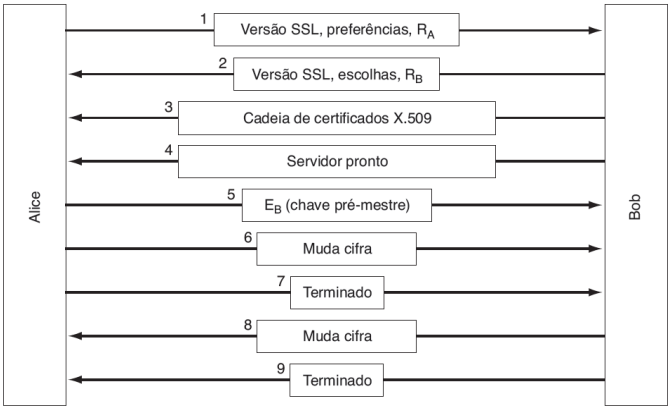
O SSL passou por três versões durante seu desenvolvimento, tendo sido a sua última versão descrita pela RFC 6101, tornando-se padrão para conexão segura na época de seu lançamento, mesmo não tendo sido formalmente publicado pelo IETF (*Internet Engineering Task Force*) (IETF, 2011). Mesmo com três versões, o funcionamento do protocolo é semelhante e está descrito a seguir.

O SSL realiza dois procedimentos para uma conexão segura: o primeiro para estabelecer o canal seguro e o segundo para realizar o tráfego da mensagem nesse canal seguro criado. A Figura 12 demostra uma situação hipotética, em que Alice (usuário) quer estabelecer uma comunicação segura com Bob. Inicialmente, Alice envia a mensagem 1 contendo a informação da versão do SSL, sua preferência de algoritmo de criptografia e um número aleatório (R_A). Por sua vez, Bob (servidor) envia sua escolha de algoritmo de criptografia, que Alice deve ser capaz de implementar, e um número aleatório (R_B). Os números aleatórios, nesse caso, são utilizados para garantir que comunicações antigas não sejam utilizadas em algum tipo de ataque. Em seguida, Bob envia um certificado digital com sua chave pública, permitindo que Alice possa verificar a autoria dessa chave. Bob fica no estado de pronto para receber a chave pré-mestre de Alice. Conforme comentado anteriormente, Alice pode também enviar seu certificado com sua chave pública a Bob, mas esse procedimento é opcional.

Após recebimento da chave pública de Bob, Alice envia a Bob a mensagem 5 com a chave pré-mestre aleatória de 384 *bits* (TANENBAUM; WETHERALL, 2011) codificada com a chave pública de Bob. A chave de sessão utilizada por Bob e Alice para o estabelecimento da

conexão será calculada com base na chave pré-mestre e nos valores aleatórios R_A e R_B em cada nó da conexão. Alice então indica Bob pela mensagem 6 para utilizar a nova cifra (chave de sessão) criada (mensagem 7). As mensagens 8 e 9 são utilizadas por Bob para finalizar o acordo ou *handshake*.

Figura 12 – Modelo de funcionamento do protocolo SSL



Fonte: (TANENBAUM; WETHERALL, 2011, p. 535).

Em relação aos algoritmos de criptografia utilizados pelo SSL, o protocolo pode suportar vários tipos, e a escolha de um deles é feita na fase do *handshake*. No Quadro 3 estão listados alguns dos principais algoritmos de criptografia utilizados pelo SSL. Segundo Tanenbaum e Wetherall (2011), o DES triplo e SHA-1 utilizados em conjunto são lentos, porém garantem uma maior segurança para aplicações que necessitam desse requisito.

Quadro 3 – Exemplos de algoritmos usados no SSL 3.0

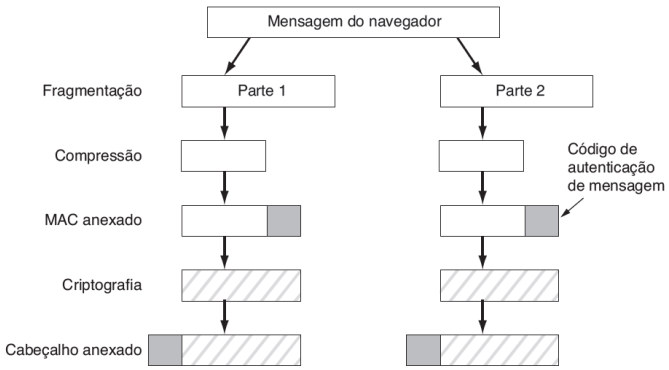
Algoritmo	Funcionalidade
DES triplo	Cifragem de mensagem
SHA-1	Controle de integridade
RC4	Cifragem de mensagem
MD5	Autenticação de mensagens

Fonte: (ABÍLIO et al., 2007).

Até então foi explanado como ocorre o acordo de cifras para início da transmissão da mensagem. O segundo passo diz respeito ao envio da mensagem pelo canal seguro. A mensagem a ser enviada ao navegador, nesse caso, passa por um processo de fragmentação. Caso a opção de compactação esteja ativa no SSL, cada unidade fragmentada será compactada.

A chave secreta gerada pela combinação da chave pré-mestre e dos números aleatórios R_A e R_B será concatenada ao fragmento compactado, resultando em um *hash*. O *hash* gerado será anexado como um código de autenticação de mensagens, ou MAC (Figura 13) (TANENBAUM; WETHERALL, 2011).

Figura 13 – Transmissão de mensagens no SSL



Fonte: (TANENBAUM; WETHERALL, 2011, p. 536).

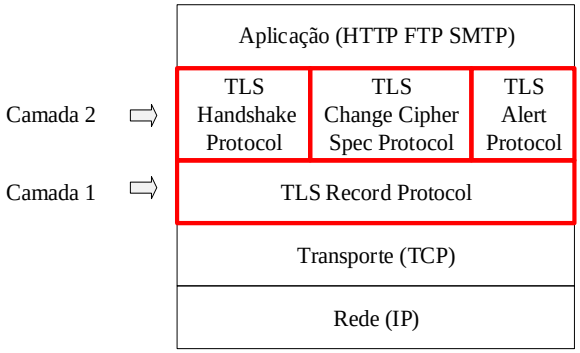
O SSL 3.0 utiliza uma combinação MD5 e RC4 que é vulnerável em virtude de o RC4 apresentar algumas chaves fracas (TANENBAUM; WETHERALL, 2011). A alternativa seria utilizar DES triplo e SHA-1, porém eles são lentos. Outro problema do SSL 3.0 é que o protocolo deixou de ser utilizado em virtude da vulnerabilidade denominada *Padding Oracle on Downgraded Legacy Encryption* (POODLE), descoberta em outubro de 2014 (MÖLLER; DUONG; KOTOWICZ, 2014). O POODLE serve-se de uma vulnerabilidade durante a fase de acordo que força o SSL a utilizar versões menores e, consequentemente, cifras fracas.

2.7.2 TLS

Até então, o SSL 3.0 era uma implementação da Netscape em seus navegadores sem alguma padronização. Em 1996, o SSL foi então submetido ao *Internet Engineering Task Force* (IETF) para padronização, surgindo, assim, um novo protocolo denominado TLS (*Transport Layer Security*), descrito pela RFC 2246 (TLS 1.0), RFC 4346 (TLS 1.1), RFC 5246 (TLS 1.2) e mais recentemente a RFC 8446 (TLS 1.3, de agosto de 2018). O TLS surgiu como uma atualização do SSL 3.0, operando entre as camadas de sessão e transporte e oferecendo integridade, dupla autenticação, sigilo e não repúdio (ABÍLIO *et al*., 2007).

O funcionamento do TLS pode ser subdividido em duas camadas: a camada 1, composta pelo protocolo TLS *Record*, e a camada 2, composta pelo conjunto de protocolos TLS *Handshake*, TLS *Change Cipher Spec* e TLS *Alert*, conforme visto na Figura 14 (ABÍLIO *et al*., 2007).

Figura 14 – Protocolos do TLS



Fonte: elaborado pelo autor.

TLS *Record* é o protocolo responsável por realizar a fragmentação e compactação dos dados das camadas superiores, gerando um MAC que será adicionado à mensagem de forma semelhante à do SSL. Esse protocolo irá auxiliar o receptor a identificar a mensagem e quaisquer alterações feitas pelo emissor (CABRAL; LEITE, 2003).

O protocolo TLS *Handshake* é responsável por realizar o acordo para estabelecimento no canal seguro e executa as funções expostas no Quadro 4 (CABRAL; LEITE, 2003).

Quadro 4 – Itens para realizar a conexão no TLS

Item	Descrição
Identificador de sessão	Uma sequência de *bytes* definida pelo servidor para identificar uma sessão segura.
Método de compressão	O algoritmo utilizado para compressão dos dados a serem criptografados.
Especificação da criptografia	Especifica o algoritmo de criptografia (RC4, DES, etc.) e o algoritmo MAC. Também define os atributos criptográficos.
Código mestre	Código de 20 *bytes* compartilhado entre o cliente e o servidor.
Modo do número de sequência	O esquema da sequência numérica a ser utilizado (chave criptográfica, cálculo de MAC).
Atualização de chave	Define como será realizada a atualização dos cálculos de alguns valores de estado de conexão (código MAC, chave criptográfica).
Resumo	Uma *flag* indicando onde a sessão segura pode ser utilizada para iniciar novas conexões seguras.

Fonte: (CABRAL; LEITE, 2003).

O protocolo TLS *Change Cipher SPec* aciona uma mensagem enviada para as entidades da conexão para que se use uma determinada regra de criptografia que satisfaça a negociação de ambos. O último protocolo, o TLS *Alert*, é responsável por gerar alertas para notificar as condições normais e de erro. Os tipos de mensagem podem ser de alertas de encerramento (quando a conexão é encerrada) e o alerta de erro (quando alguma anormalidade é detectada no funcionamento do TLS) (ABÍLIO *et al*., 2007). A descrição de cada alerta por ser vista no Quadro 5.

Quadro 5 – Sinais de alertas do TLS

Alerta	Descrição
No_connection	Uma mensagem foi recebida enquanto não havia uma conexão segura com o emissor. Essa mensagem pode ser fatal ou crítica.
Handshake_failure	A recepção desse alerta indica que o emissor não pode negociar ou aceitar o conjunto de parâmetros de segurança proposto. Esse é um erro fatal.
Session_not_ready	Ocorre quando a sessão segura não está pronta para receber novas conexões por razões administrativas, como a manutenção do servidor. Geralmente, esse é um alerta crítico.

Fonte: (CABRAL; LEITE, 2003).

2.7.3 TLS e SSL

As diferenças entre os protocolos TLS e SSL estão descritas no Quadro 6.

Quadro 6 – Diferenças entre TLS e SSL

(Continua)

Parâmetro	SSL	TLS
Alerta de erro	Durante a execução do protocolo *Handshake*, o servidor deverá esperar pela resposta do cliente. Se o servidor enviar uma mensagem de requisição do certificado, o cliente deverá enviar a mensagem com o certificado ou um alerta *no_certificate*.	Uma vez que o servidor envie uma mensagem solicitando o certificado, a resposta deverá ser enviada pelo cliente contendo o certificado.
Algoritmo para troca de chave	No SSL, os algoritmos de troca de chaves existentes são RSA, *Diffie Hellman* e *Fortezza Kea*. Quanto ao protocolo, o *Fortezza* é similiar ao *Diffie-Hellman*, com valores públicos fixos, contidos nos certificados.	TLS não suporta o algoritmo de troca de chaves *Fortezza Kea*.

Parâmetro	SSL	TLS
Cálculo MAC	No SSL, não se insere o tipo de conteúdo nem a versão do protocolo no cálculo do MAC, portanto esses campos não são protegidos de ataques contra sua integridade.	Os campos tipo de conteúdo e versão do protocolo são protegidos, estando incluídos no cálculo MAC.

Fonte: (CABRAL; LEITE, 2003).

Uma observação necessária é que o SSL, durante a fase de encriptação dos dados, acrescenta um preenchimento à mensagem do usuário para que a quantidade mínima exigida do bloco dos dados seja um múltiplo do tamanho de bloco da cifra. No ataque POODLE, esse mecanismo é explorado para tentar recuperar *bits* cifrados. Esse problema no TLS é solucionado, pois o preenchimento pode ser de qualquer quantidade que resulte em um total que seja um múltiplo do tamanho do bloco da cifra até um máximo de 255 *bytes* (STALLINGS, 2015).

Sobre a nova versão do TLS (v1.3), a RFC 8446 lista algumas pequenas diferenças em relação à versão anterior (vale comentar que a RFC 8446 considera a RFC 5446 TLS v1.2 obsoleta):

a) Todas as mensagens de *handshake*, após o *ServerHello* (item 2 da Figura 12), agora estão criptografadas, melhorando a proteção e confidencialidade;
b) Algoritmos de curva elíptica, *elliptic curve cryptography* (ECC), estão na especificação base da versão. Basicamente, o ECC é um concorrente do RSA que proporciona segurança semelhante, utilizando menor custo de processamento;
c) Todos mecanismos de troca de chaves baseados em chave pública agora fornecem sigilo de encaminhamento, chamado *Perfect Forward Secrecy* (PFS). Mesmo que uma das chaves do servidor seja comprometida, as chaves geradas anteriormente são seguras, pois não há método que possa regenerá-las (também denominadas chaves efêmeras);
d) Foi adicionado um modo de tempo de ida e volta zero (0-*Round time trip*) para economizar o tempo de tráfego de algumas aplicações pelo custo de algumas propriedades de segurança;
e) A lista de algoritmos de criptografia simétrica suportada foi removida de todos os algoritmos considerados herdados. Todos os algoritmos que sobraram possuem dados associados com autenticação e encriptação, ou *authenticated encryption with associated data* (AEAD). O conceito de suíte de cifras foi alterado para separar os mecanismos de

autenticação e troca de chaves dos algoritmos de proteção de registros, incluindo o comprimento da chave secreta, e um *hash* a ser usado com a função de derivação de chave e código de autenticação de mensagens de *handshake* (MAC).

2.8 VPN

Nos primórdios da comunicação, quando não havia uma rede pública de dados, as instituições contratavam linhas de comunicação dedicadas das companhias telefônicas para se comunicarem com suas filiais em outros locais geográficos. Essa rede que permitia o tráfego dedicado, também denominada rede privada, permitia que a informação pudesse trafegar de forma segura, dificultando a interceptação por algum terceiro não pertencente à instituição. Com o surgimento das redes públicas de dados, e consequentemente da internet, muitas instituições optaram por migrar para essa estrutura, que permitia o tráfego de dados e voz com um custo inferior ao canal dedicado. Apesar dessa vantagem, era importante que o tráfego da informação continuasse a ser feito de modo seguro (TANENBAUM; WETHERALL, 2011).

Em virtude dessa necessidade, foram criadas as redes privadas virtuais, ou **VPN**, que são túneis criados nas redes públicas ou internet. Quando se usa uma VPN, seu sistema é iniciado e cada par de *firewall*s realiza sua associação de segurança, ou *Security Association* (SA), estabelecendo os serviços, modos, algoritmos e chaves (TANENBAUM; WETHERALL, 2011). Uma possibilidade de VPN é a utilização do *Internet Protocol Security* (IPSec) para realizar o tunelamento ou conexão especial entre dois hosts e garantir a segurança em uma pilha do TCP/IP versão 4 (BRAGHETTO; SILVA; BARBOSA, 2003).

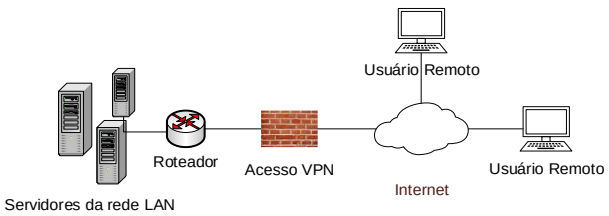
Esse recurso da VPN pode ser encontrado em roteadores e principalmente *firewall*s que lidam diretamente com questões de segurança. O *Firewall* é um mecanismo implementado em *hardware* e *software* capaz de monitorar uma rede de dados conforme uma política de regras baseada em instruções, delimitando os tipos de dados que podem entrar e sair de uma rede. Dessa forma, por exemplo, um roteador irá lidar com o pacote como se fosse um fragmento qualquer, porém esse pacote apresenta um cabeçalho diferenciado determinado pelo IPSec. Além do IPSec, um outro recurso disponível e que é empregado por muitas empresas provedoras de serviço de internet é o *MultiProtocol Label Switching* (MPLS), que não será abordado neste estudo. A grande vantagem da VPN é sua transparência para o usuário final, bastando apenas ao administrador da rede a tarefa de realizar a sua configuração (TANENBAUM; WETHERALL, 2011).

2.8.1 Tipos de VPN

Como forma de apresentar um conceito genérico de como a VPN funciona em uma rede de computadores, alguns exemplos de sua implementação estão descritos a seguir. Segundo Braghetto, Silva e Barbosa (2003), existem três tipos de VPN:

a) ***Remote-Acess* VPN**: o cliente externo, por exemplo na internet, utiliza um *software* para conectar-se a um servidor VPN. Esse servidor irá verificar as credenciais do usuário antes de liberar seu acesso de conexão na *Local Area Network* (LAN) (Figura 15);

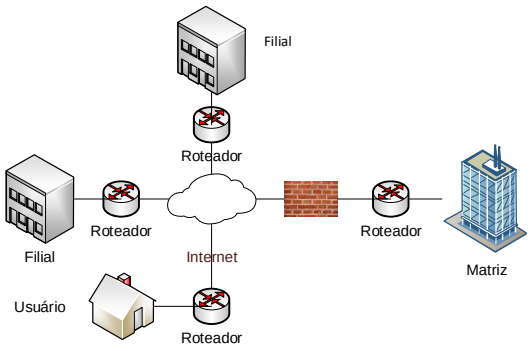
Figura 15 – Topologia *Remote-Acess* VPN



Fonte: elaborado pelo autor.

b) ***Site-to-Site***: nesse tipo, ocorre a conexão local de redes distintas entre si de maneira segura. A autenticação, criação do túnel e roteamento dos pacotes são implementados pelos servidores ou *gateway*s. Esse tipo de topologia é ideal para conectar filiais de organizações à sua matriz ou permitir que um usuário externo da rede da organização possa eventualmente conectar-se à rede (Figura 16);

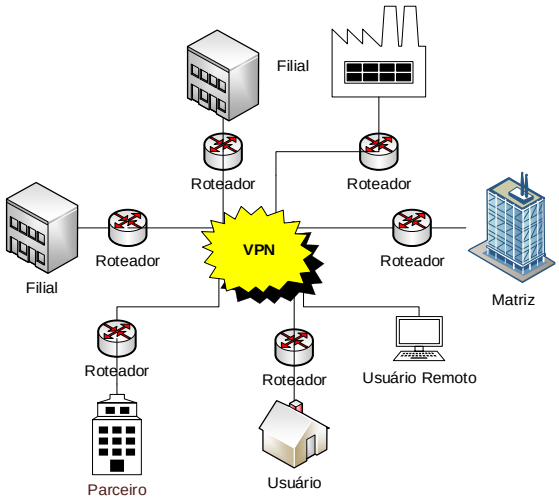
Figura 16 – Topologia *Site-to-Site* VPN



Fonte: elaborado pelo autor.

c) ***Extranet* VPN**: membros distribuídos fisicamente e parceiros externos de uma determinada organização se comunicam por meio da rede pública utilizando *gateway*s VPN e clientes de VPN (Figura 17).

Figura 17 – *Extranet* VPN



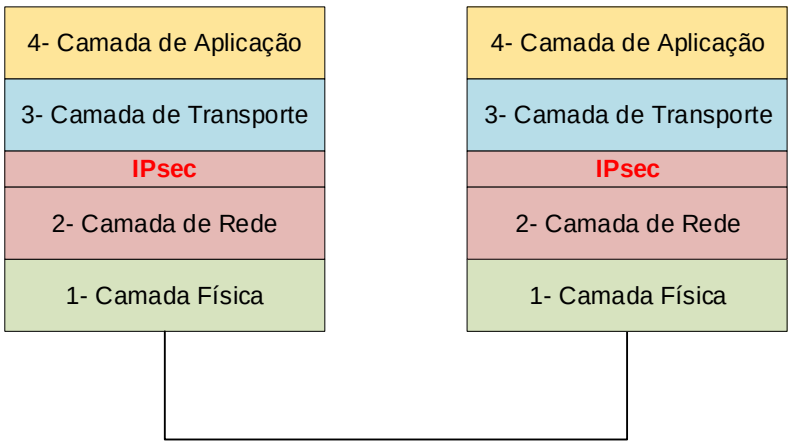
Fonte: elaborado pelo autor.

Além da arquitetura física demonstrada anteriormente, uma segunda classificação diz respeito ao modelo OSI, que diferencia três arquiteturas principais de VPN nas camadas de enlace, rede e camadas superiores. VPN da camada de enlace possuem a característica de simular uma infraestrutura LAN, permitindo a conexão de *hosts* de uma organização localizados em pontos geograficamente diferentes. VPN da camada de rede podem simular uma *Wide Area Network* (WAN) sobre uma infraestrutura de rede, permitindo o uso de IPs privados sobre uma rede pública. O IPsec é um exemplo desse modelo, comumente utilizado em VPN, e seus aspectos estão descritos na seção 2.8.2. VPN de camada superior são utilizadas para proteger transações em redes públicas entre aplicações, garantindo confidencialidade e integridade dos dados durante a comunicação. Esse tipo de VPN é conhecido como camada 4, geralmente por ser estabelecido pelo *Transmission Control Protocol* (TCP) (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013).

2.8.2 IPSec

Na tentativa de realizar um maior controle de integridade e criptografia dos dados de forma mais confiável, considerando o modelo OSI ou *ethernet*, chega-se à seguinte conclusão: quanto mais próximo do nível de aplicação melhor será essa proteção para um tráfego VPN. No entanto, a elaboração de um protocolo desse tipo necessitaria que todas as aplicações fossem adaptadas ou modificadas para adequar um protocolo de comunicação do tipo fim a fim. Para contornar esse problema, não dependendo da aplicação, a abordagem seria implementá-la no nível da camada de rede, tornando o processo de comunicação seguro (TANENBAUM; WETHERALL, 2011) (Figura 18). A grande vantagem seria, de certo modo, tornar o processo não perceptível para usuários conscientes ou não conscientes sobre segurança da informação. Nessa abordagem de implementação surgiu o projeto IPSec, descrito principalmente pelas RFCs 2401, 2402 e 2406, com seu mecanismo principal aplicado em redes VPN.

Figura 18 – IPSec do modelo internet



Fonte: elaborado pelo autor.

O IPSec é um conjunto de algoritmos e serviços, criado pela IETF, que fornece sigilo, integridade e autenticação em ambientes IPv4 e IPv6 na camada de rede IP, utilizando criptografia de chave simétrica e orientando a conexão (ABÍLIO *et al*., 2007). O IPv4, desde sua concepção, não possui características de proteção para os pacotes, tendo sido as primeiras tentativas de padronização realizadas em 1995 pela RFC 1825/1829 (BRAGHETTO; SILVA; BARBOSA, 2003). Apesar disso, o IPv6, em sua estrutura, já apresenta padronização para o IPsec. O IPSec garante a segurança na camada de rede no modelo internet utilizando sistemas de criptografia, e surgiu justamente como resposta pela falha de segurança do IPv4.

No IPSec, uma conexão é denominada **SA**, que cria um identificador de segurança transportado por pacotes entre as duas extremidades da conexão para pesquisar chaves. O IPSec apresenta três componentes para prover a encriptação do conteúdo da mensagem 1829 (BRAGHETTO; SILVA; BARBOSA, 2003):

a) Cabeçalho de autenticação, ou *autentication header* (AH), para o pacote IP;
b) Cabeçalho de encapsulamento de carga útil, ou *Encapsulating Security Payload* (ESP), que fornece a autenticação e cifragem do datagrama;
c) Troca da chave internet, ou *Internet Key Exchange* (IKE), que realiza a troca de chaves secretas da sessão.

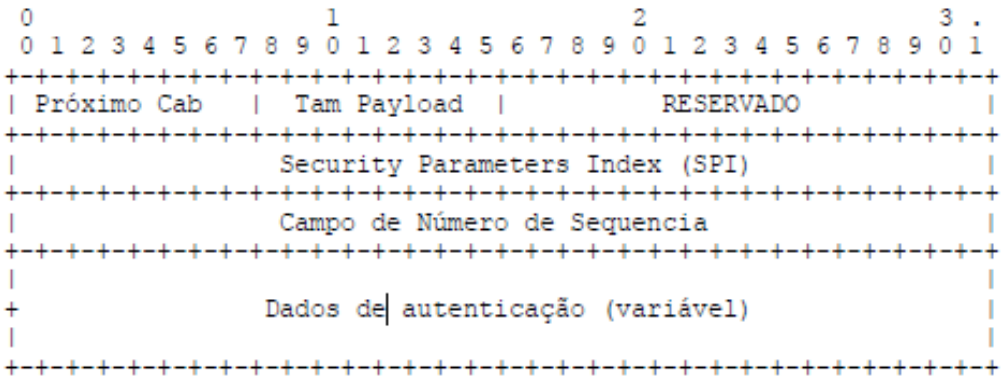
Dentre as principais características do IPSec que garantem a autenticação, integridade e sigilo da comunicação podem ser citadas (BRAGHETTO; SILVA; BARBOSA, 2003):

a) Utilização de certificação digital para validação das chaves públicas;
b) *Hash* dos datagramas;
c) Utilização do algoritmo *Diffie-Hellman* para troca de chaves públicas e obtenção da chave secreta entre origem e destinatário da mensagem, evitando ataques *Man-in-the-middle* (MITM);
d) Utilização da criptografia assimétrica para assinar as chaves públicas durante as trocas entre origem e destinatário.

2.8.2.1 Cabeçalhos

O **AH** é um cabeçalho inserido no IP que realiza a verificação de integridade e autenticação dos dados. Ele é inserido entre o cabeçalho IP e o TCP no IPv4. O campo do AH (Figura 19) contém informações para executar sua função, e será descrito a seguir (BRAGHETTO; SILVA; BARBOSA, 2003):

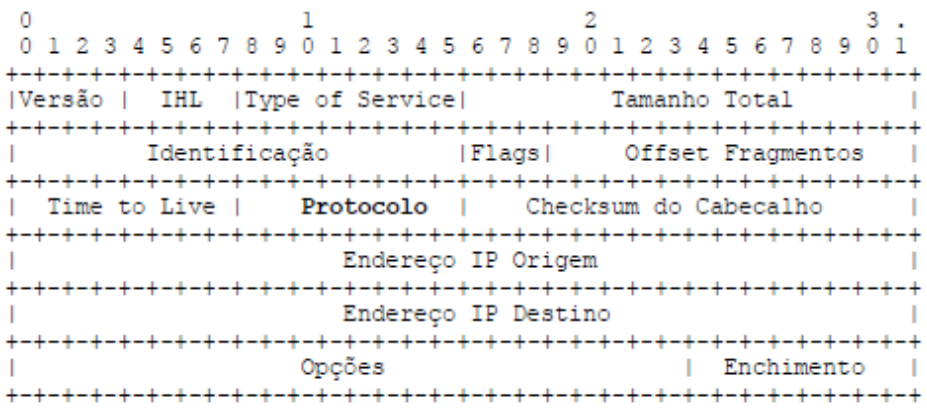
Figura 19 – Cabeçalho de autenticação para o IPv4



Fonte: (BRAGHETTO; SILVA; BARBOSA, 2003).

a) O campo Próximo Cabeçalho armazena o valor contido no campo “Protocolo” do cabeçalho IP (Figura 20), e para iniciar o AH ele armazena o valor 51;
b) O tamanho do *payload*, ou carga útil, armazena o tamanho da palavra de AH de 32 *bits*. O índice de parâmetros da conexão, ou *Security Parameters Index* (SPI), armazena o identificador da conexão e contém a chave compartilhada enviada do transmissor para o receptor;
c) O “Campo de Número de Sequência” realiza a numeração exclusiva de todos os pacotes do SA, evitando ataques de reprodução;
d) O campo de autenticação dos dados contém a assinatura digital da carga útil. Nesse caso, quando o SA é estabelecido, ocorre a negociação da criptografia de chave simétrica, pois ela tem capacidade de processar os pacotes IP de forma eficientemente rápida. Para realizar a autenticação, é feito o processo de *Hashed Message Authentication Code* (HMAC), que soma a chave ao pacote IP, executa sobre ele um algoritmo de resumo de mensagem e, posteriormente, um RSA sobre o resultado. Assim que a chave é compartilhada é calculada a assinatura.

Figura 20 – Cabeçalho IP

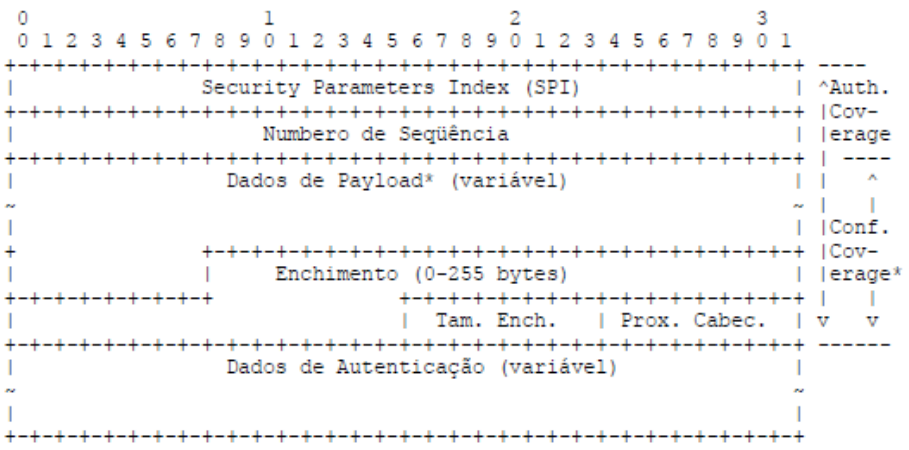


Fonte: (BRAGHETTO; SILVA; BARBOSA, 2003).

Vale destacar que o processo de autenticação do AH não inclui verificação de confidencialidade pois isso é feito pelo protocolo ESP. A vantagem é que ele permite garantir que o remetente enviou a informação para o IP de destino correto, impedindo a entrega a um IP falso (Spoofing IP) do pacote inteiro sem realizar criptografia (ABÍLIO *et al*., 2007).

O **ESP** é uma segunda opção de cabeçalho que consiste em duas palavras de 32 *bits* (Figura 21). A diferença dele para o AH é que, além de fornecer verificações de integridade do HMAC, ele possibilita que os dados trafeguem em sigilo. O ESP possui um vetor de referência que realiza a criptografia dos dados. Em resumo, durante a comunicação entre um cliente e um servidor, por exemplo, o IPSec estabelece a criação de um túnel de comunicação seguro entre o *gateway* de origem (que irá adicionar ao IP os dois cabeçalhos, AH e ESP, realizando a cifragem) e o *gateway* de destino (que irá remover os dados do pacote IP e decifrá-los) (BRAGHETTO; SILVA; BARBOSA, 2003).

Figura 21 – Cabeçalho de encapsulamento de carga útil no IPv4



Fonte: (BRAGHETTO; SILVA; BARBOSA, 2003).

O **IKE** v2.0 (RFC 7296) é um protocolo que realiza a troca de chaves em um processo chamado *Internet Security Association and Key Management Protocol* (ISAKMP), e sua função é iniciar e manter o SA. Ele autentica o *host*, *gateway* ou servidor para manipulação e negociação de chaves públicas PKI. Essa troca é feita usando o protocolo de chaves públicas *Diffie-Hellman* para estabelecer uma sessão em um meio que pode ou não ser seguro. O IKE provê quatro funcionalidades (BRAGHETTO; SILVA; BARBOSA, 2003):

a) Permite à origem e ao destino negociar os protocolos, algoritmos e chaves utilizadas na conexão;
b) Garante a identificação do remetente e destinatário;
c) Realiza o gerenciamento das chaves;
d) Permite assegurar que a troca de mensagens ocorra em um meio seguro.

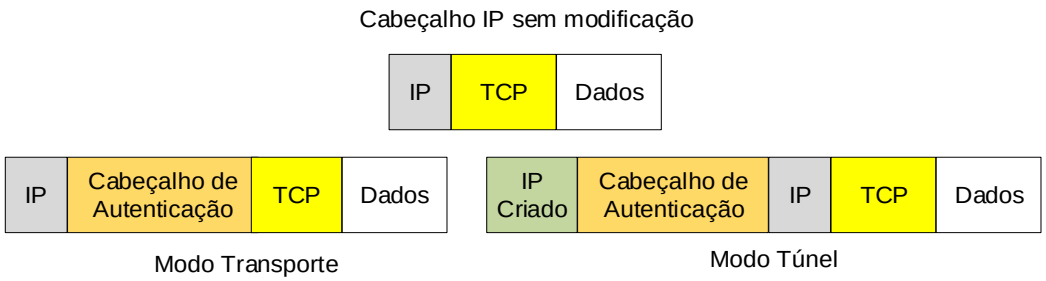
2.8.2.2 Modos de operação

O IPSec utiliza dois modos de operação para transporte dos pacotes (Figura 22) (BRAGHETTO; SILVA; BARBOSA, 2003):

a) **Modo transporte**: o cabeçalho IPSec é adicionado ao cabeçalho IP do datagrama original. A autenticação e cifração é feita no *payload* dos protocolos das camadas superiores. Como é utilizado apenas o cabeçalho AH, somente são permitidas a autenticação e integridade dos pacotes sem a verificação do sigilo;

b) **Modo túnel**: o cabeçalho IP, IPSec e *payload* são cifrados, criando outro cabeçalho IP. Dessa forma, apenas o novo IP criado é transparente na rede de comunicação. Para esse modo, a integridade, autenticidade e sigilo são garantidos. Nessa rede de comunicação, o tráfego IP só é feito em um sentido (*unicast*). Caso se queira realizar uma transmissão *multicast*, deve-se utilizar o *Layer 2 Tunneling Protocol* (L2TP). A grande vantagem do modo túnel é a possibilidade de tratar um conjunto de conexões TCP como um único fluxo codificado (TANENBAUM; WETHERALL, 2011). Isso, de certa forma, permite anular estudos de análise de tráfego sobre uma rede. Essa vantagem é muito importante em um ambiente de comunicação militar, pois um atacante fica impossibilitado de analisar o tráfego de dados durante alguma crise. A desvantagem do modo túnel é justamente o tamanho do pacote de dados gerado pela utilização do cabeçalho do ESP, diferentemente do modo transporte.

Figura 22 – Modos IPSec



Fonte: elaborado pelo autor.

2.8.2.3 Implementação do IPSec

O IPSec pode ser implementado em dispositivos de *gateway*, servidores ou *firewall*. Segundo Braghetto, Silva e Barbosa (2003), as formas comumente utilizadas são:

a) Inserção do algoritmo IPSec na pilha de protocolo TCP/IP existente em equipamentos de rede;
b) Utilização do *Bump-in-The-Wire* (BITW), que utiliza um processador dedicado para realizar a criptografia e que possui um IP para identificação. Essa implementação é ideal para sistemas militares;

c) Utilização *Bump-in-The-Stack* (BITS), em que o IPSec é adicionado entre a camada TCP/IP nativa e o *driver* de rede local, não sendo necessária alteração do código fonte do equipamento.

Mesmo sendo uma implementação reconhecida desde 1998 pela RFC 2411 e, portanto, utilizada por mais de 20 anos, Adrian *et al*. (2015) abordaram uma vulnerabilidade denominada *Logjam* e sugeriram que a *National Security Agency* (NSA) possa ter comprometido o protocolo IPsec, minando o algoritmo *Diffie-Hellman* .

2.8.3 L2TP

O L2TP, descrito pela RFC 2661 e semelhante ao IPSec, também possui dois modos de operação, sendo um voluntário e outro compulsório. O modo compulsório é ideal para usuários em trânsito que utilizam serviço discado para um provedor. O modo compulsório também é feito sob uma conexão discada, porém a formação do túnel é feita de forma automática. O ponto de falha do L2TP é que ele não possui processo de gerenciamento de chaves criptográficas. Para isso, ele utiliza um protocolo de encriptação, como o IPSec, para a criptografia e gerenciamento das chaves (ALVES FAGUNDES, 2007). Em virtude dessa dependência do IPSec, sua utilização não é adequada para redes VPN, apesar de ser capaz de criar mais de um túnel entre duas entidades realizando uma conexão *multicast* (BRAGHETTO; SILVA; BARBOSA, 2003).

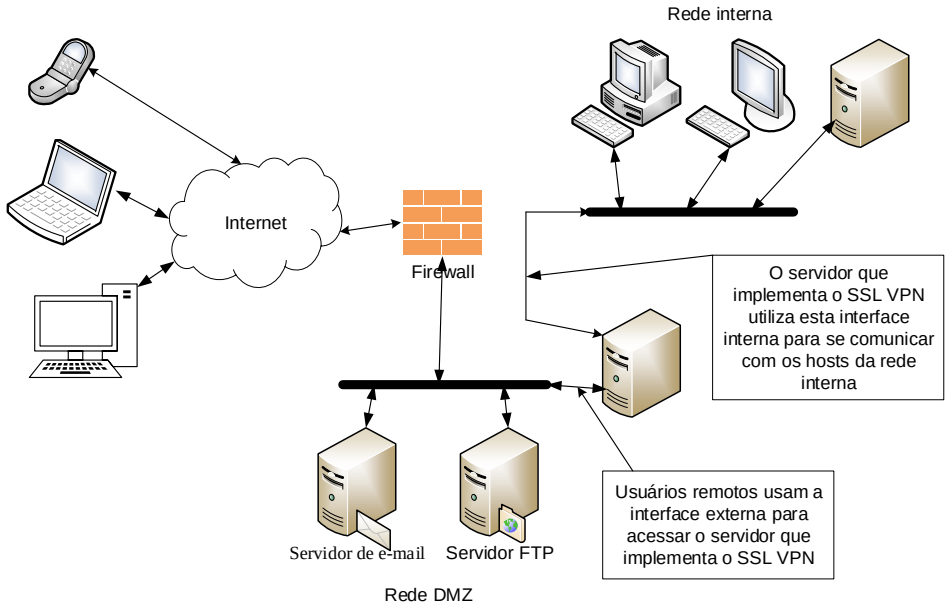
2.8.4 SSL VPN

O SSL VPN (Figura 23) é uma tecnologia VPN que oferece recursos de acesso remoto, usando o protocolo SSL/TLS já incorporados nos navegadores Web. Essa tecnologia permite que usuários, possuindo credenciais de ingresso, possam de qualquer local usando um navegador Web estabelecer conexões VPN de acesso remoto. Ela permite o acesso ao ambiente corporativo tenha maior disponibilidade, além de redução nos custos de TI para suporte nos softwares de clientes VPN. Em linhas gerais, existem dois tipos de SSL VPN implementáveis (FRANKEL , HOFFMAN , *et al.*, 2008)

a) O **Túnel SSL/TLS VPN** é uma implementação que realiza o encapsulamento do tráfego por um *middlebox* (que realiza a função de transformar, inspecionar, filtra e manipula tráfego) para um cliente. Seu funcionamento, em essência, age de forma semelhante ao Túnel IPSec mas emprega o SSL/TLS para criptografia utilizando algum mecanismo proprietário para encapsulamento e roteamento.

b) O **Portal SSL/TLS VPN** é um *middlebox* que oferece uma plataforma adicionando segurança em sites não seguros. Ele geralmente é implementado usando um protocolo como o HTTP para ter acesso a serviços específicos em uma rede. O acesso ao portal, neste caso, seria feito usando uma URL da mesma forma a qual é feito usando o HTTPS. Normalmente esse tipo de VPN é usado para fornecer acesso a usuários remotos que necessitam de informações específicas dos serviços disponíveis pela rede. Isso facilita, por exemplo, um controle mais preciso do acesso que o usuário irá realizar. Além disso, o Portal permite o acesso de qualquer lugar em que o acesso remoto esteja localizado não importando se o tráfego utiliza os protocolos IPv4 ou IPv6.

Figura 23– SSL VPN em uma rede DMZ com interface dupla no firewall



Fonte: adaptado de Frankel (2008).

Uma das vantagens de se utilizar o SSL VPN é na facilidade no acesso à rede pois não é necessário, por parte do usuário, realizar qualquer configuração de algum cliente pois o acesso é feito via navegador Web. Em relação à segurança as vantagens são (FRANKEL , HOFFMAN , *et al.*, 2008):

a) O comprometimento do dispositivo cliente não garante que o atacante terá acesso completo à rede interna.
b) O tráfego entre cliente e a rede interna está submetido às políticas implementadas no Firewall.
c) É possível realizar a análise de tráfego contra atividades maliciosas pela implantação de um IDS junto ao DMZ (Uma *Demilitarized Zone* é uma estrutura que permite manter um isolamento físico entre uma rede confiável e uma não confiável).
d) O tráfego externo da DMZ quanto da DMZ para a rede interna devem passar pelo firewall. Caso algum host da DMZ seja comprometido o atacante não poderá acessar a rede interna ao menos que o dispositivo VPN também esteja comprometido.

A desvantagem é que a utilização de um navegador Web dificulta a utilização de serviços de rede como compartilhamento de arquivos, impressoras ou armazenamento centralizado por exemplo. Em relação à segurança as desvantagens são (FRANKEL , HOFFMAN , *et al.*, 2008):

a) Algumas portas devem ser abertas entre o firewall e o hosts do SSL VPN. Isso pode ser explorado por alguma vulnerabilidade.
b) Existe a possibilidade de simplificação dessa topologia aonde o tráfego passa somente uma vez pelo firewall, porém a garantia da segurança é reduzida. Considerando a abordagem da Figura 23, que garante maior segurança pela passagem do tráfego duas vezes pelo firewall, existe a introdução de maior complexidade no roteamento dos pacotes.

3 METODOLOGIA

Este trabalho adotou o delineamento de pesquisa qualitativa baseada em documentos de produção acadêmica, bem como revisão e pesquisa bibliográfica na área de TI.

3.1 Classificação

3.1.1 Quanto aos fins

A metodologia aplicou uma análise que justificou a adoção do protocolo TLS 1.3 e algumas soluções VPN *open source* e produtos oferecidos por empresas do ramo de TI, para implantação de uma comunicação segura.

3.1.2 Quanto aos meios

Este estudo baseou-se no delineamento descritivo e intervencionista em razão da análise de uma conexão TLS utilizando um sítio da MB. Já a revisão abordou a tecnologia VPN quanto às possíveis soluções de implementação.

3.2 Limitação

A limitação do método relacionou-se à validade da pesquisa prática dos resultados encontrados em virtude da variedade de ferramentas e tecnologias existentes. Para manter e verificar uma conexão segura são necessárias políticas de segurança requeridas pela instituição. Em razão da área de TI da MB ser um setor que lida com assuntos sigilosos, não foi possível obter informações atualizadas de sua infraestrutura de rede, bem como de equipamentos e soluções adotados. Dessa forma, esta pesquisa constitui-se apenas como uma sugestão observada que pode ou não ser empregada.

3.3 Universo e amostragem

O estudo foi realizado por meio de busca de ferramentas ou soluções que pudessem ser pesquisadas ou analisadas de forma livre e com informações encontradas na Internet.

3.4 Coleta e tratamento dos dados ou das informações

3.4.1 TLS

Na parte de TLS, a tentativa foi de verificar a situação da rede da MB comparada à sua tecnologia em função dos padrões estabelecidos e mais recentemente divulgados na área de TI. Desse modo, foi realizado um teste sobre os parâmetros TLS empregados no *site* da MB (MARINHA DO BRASIL, 2019a) no dia 27 de dezembro de 2019, empregando a ferramenta SSL *Reporter* v1.36.3 do SSL *Labs* (QUALYS, 2009). De acordo com o *site* do projeto, o SSL *Labs* é uma pesquisa não comercial desenvolvida pela Qualys. Ela é composta por uma coleção de documentos e ferramentas relacionada ao SSL que, na tentativa de torná-la melhor, possui o objetivo de difundir como o SSL é implantado.

Dessa forma, foi possível obter informações a respeito da versão do TLS implementado no servidor da MB em que a URL pesquisada estava hospeda. Os resultados obtidos estão descritos a seguir:

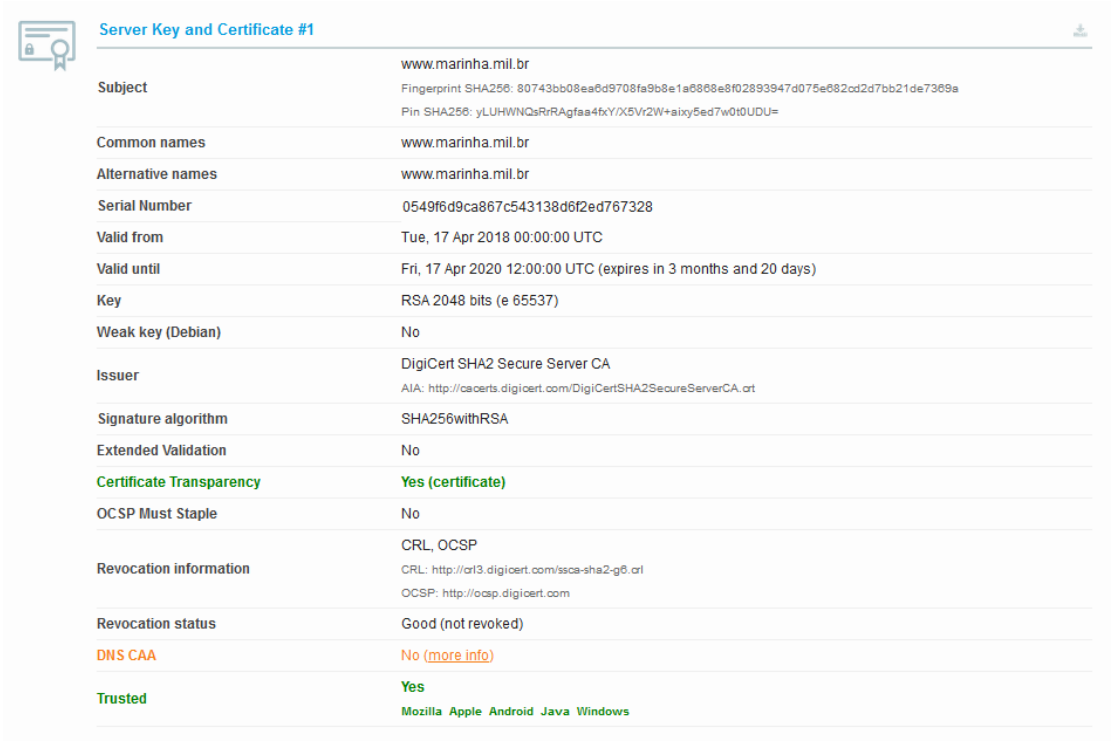
a) **Certificados e chaves do servidor**: o primeiro resultado fornecido pelo *SSL Reporter* está demonstrado nas Figuras 23 e 24. Das informações obtidas, algumas são de interesse, conforme visto no capítulo anterior, e estão listadas no Quadro 7;

Quadro 7 – Parâmetros do certificado do servidor

Item	Descrição
Algoritmo de assinatura	SHA-256
Chave utilizada	RSA 2048 *bits*
Modo de consulta de certificados	OCSP e LCR
Algoritmo de assinatura	SHA-256 com RSA

Fonte: (QUALYS, 2009).

Figura 24 – Chave do servidor e certificados do *site*

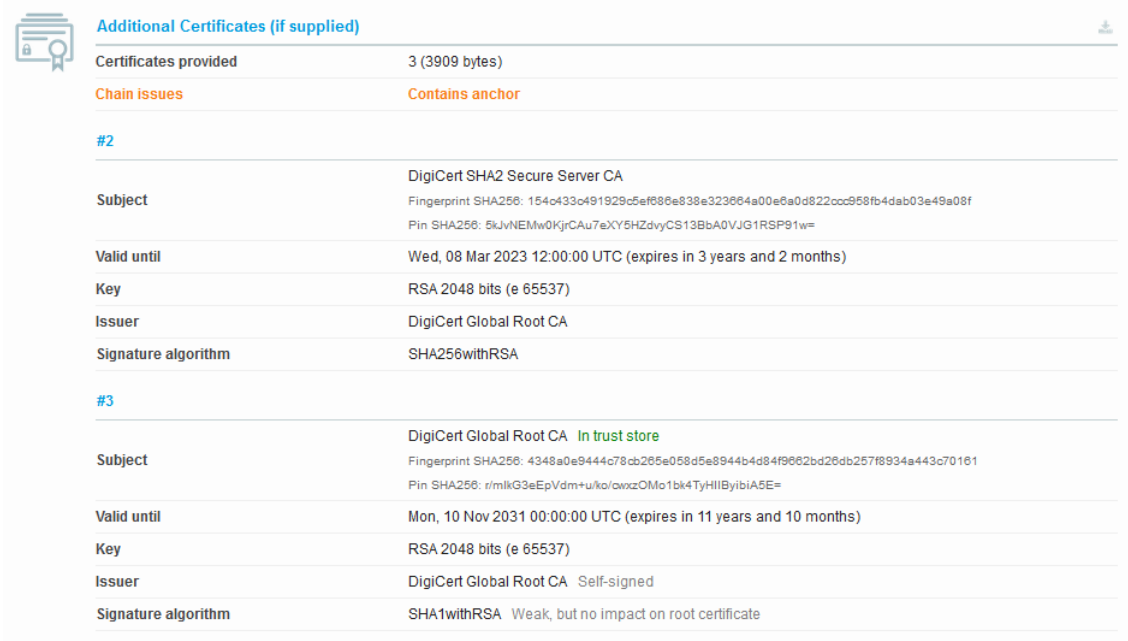


Server Key and Certificate #1

Subject	www.marinha.mil.br Fingerprint SHA256: 80743bb08ea6d9708fa9b8e1a6868e8f02893947d075e682cd2d7bb21de7369a Pin SHA256: yLUHWNQsRrRAgfaa4fxY/X5Vr2W+aixy5ed7w0t0UDU=
Common names	www.marinha.mil.br
Alternative names	www.marinha.mil.br
Serial Number	0549f6d9ca867c543138d6f2ed767328
Valid from	Tue, 17 Apr 2018 00:00:00 UTC
Valid until	Fri, 17 Apr 2020 12:00:00 UTC (expires in 3 months and 20 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert SHA2 Secure Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/ssca-sha2-g6.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Fonte: (QUALYS, 2009).

Figura 25 – Informações adicionais do certificado



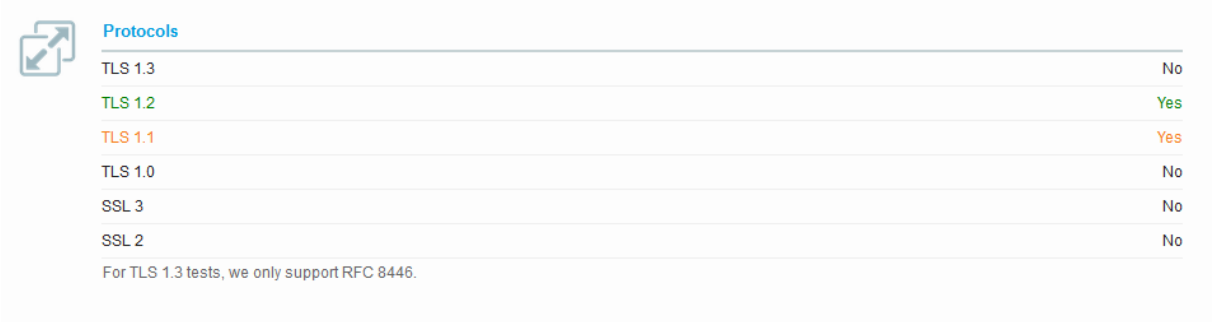
Additional Certificates (if supplied)

Certificates provided	3 (3909 bytes)
Chain issues	Contains anchor
#2	
Subject	DigiCert SHA2 Secure Server CA Fingerprint SHA256: 154c433c491929c5ef686e838e323664a00e6a0d822ccc958fb4dab03e49a08f Pin SHA256: 5kJvNEMw0KjrCAu7eXY5HZdvyCS13BbA0VJG1RSP91w=
Valid until	Wed, 08 Mar 2023 12:00:00 UTC (expires in 3 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root CA
Signature algorithm	SHA256withRSA
#3	
Subject	DigiCert Global Root CA In trust store Fingerprint SHA256: 4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161 Pin SHA256: r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E=
Valid until	Mon, 10 Nov 2031 00:00:00 UTC (expires in 11 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root CA Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Fonte: (QUALYS, 2009).

b) **Versão do TLS**: a Figura 26 mostra uma análise sobre as versões suportadas pelo servidor. Foi constatado que o servidor suportava as versões do TLS 1.1 e 1.2, e não suportava o TLS 1.3 e as antigas versões do SSL.

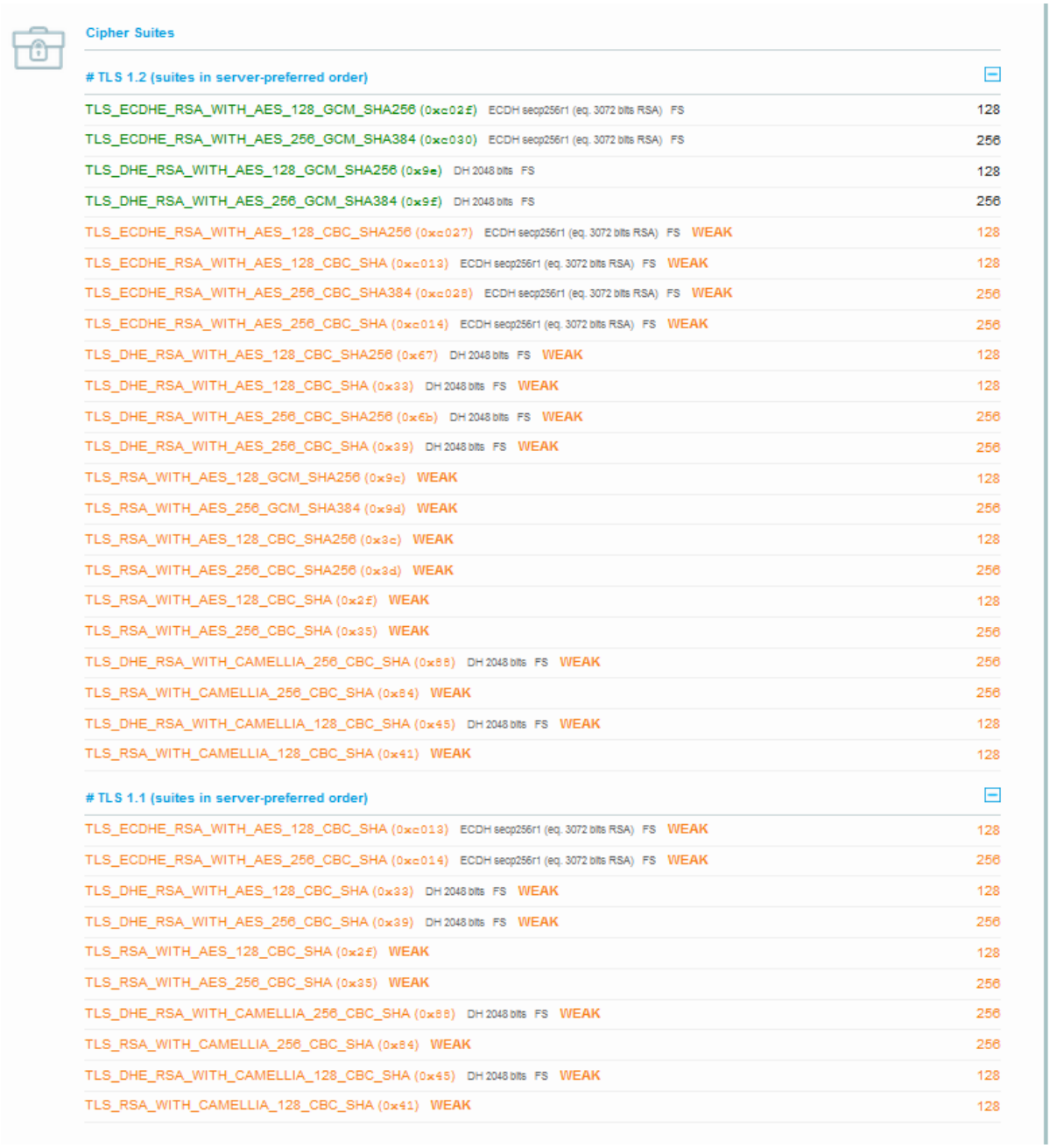
Figura 26 – Versão do TLS



Fonte: (QUALYS, 2009).

Além das versões, a ferramenta permitiu verificar os tipos de cifras suportados pelo TLS 1.1 e 1.2 implementadas no servidor, como mostrado na Figura 27. A informação contém o número de *bits* empregados na cifra, sinalizando se o algoritmo é fraco ou não.

Figura 27 – Pacote de cifras suportados por cada versão de TLS implementada



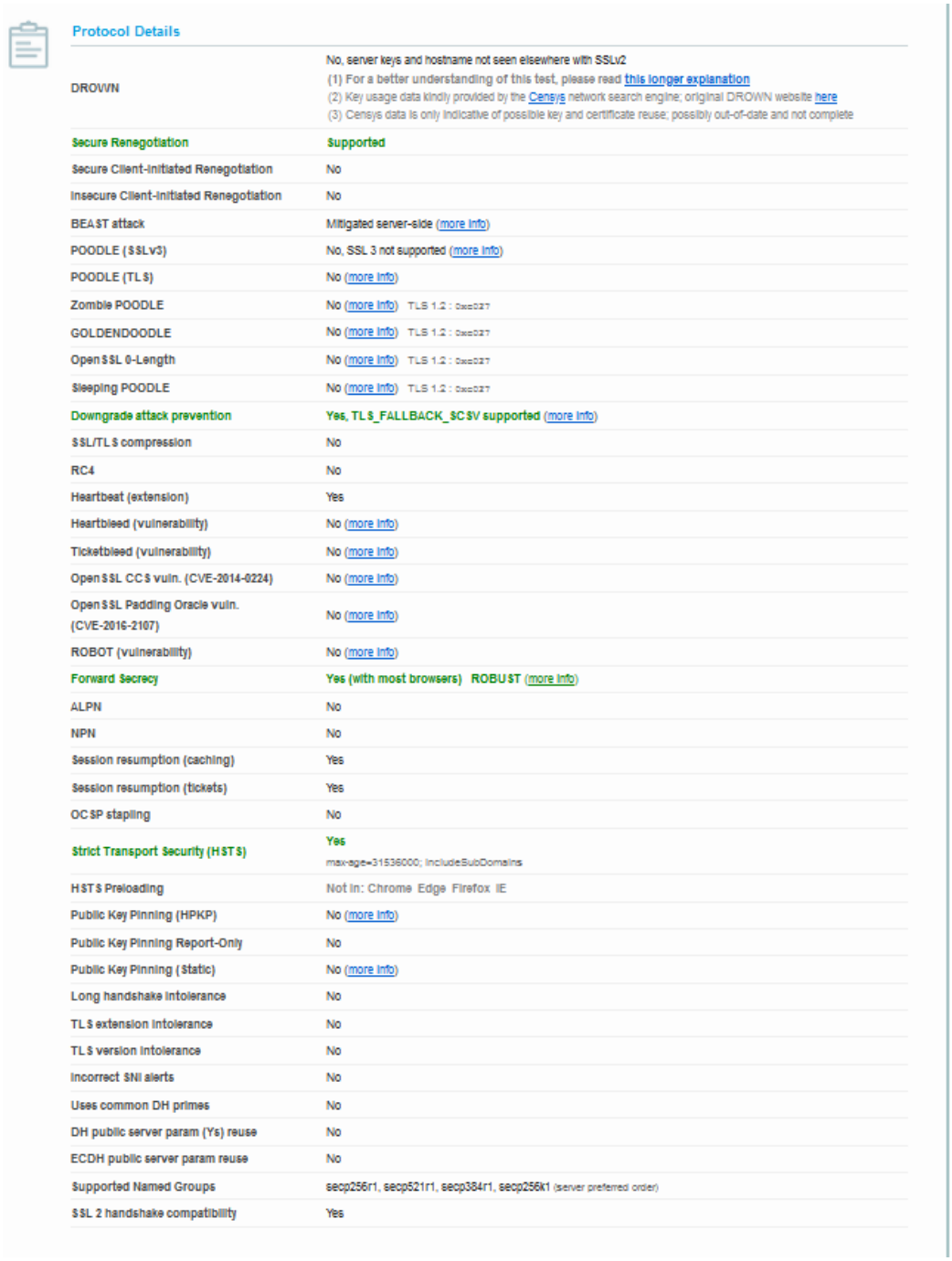
Cipher Suites

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128
# TLS 1.1 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128

Fonte: (QUALYS, 2009).

c) **Detalhes do protocolo**: o último resultado análisado revelou detalhes sobre o protocolo quanto a vulnerabilidades que poderiam existir no servidor, além de outras informações (Figura 28).

Figura 28 – Detalhes do protocolo



Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-initiated Renegotiation	No
Insecure Client-initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp521r1, secp384r1, secp256k1 (server preferred order)
SSL 2 handshake compatibility	Yes

Fonte: (QUALYS, 2009).

3.4.2 Ferramentas de VPN

A escolha de um bom serviço de VPN dependerá do nível de risco a que a informação está sendo submetida. Uma forma de delinear quais parâmetros são necessários para a escolha de uma VPN, considerada no presente estudo, pode ser encontrada na norma ISO/IEC 27033-

5: *Securing communications across network using Virtual Private Networks* (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013). A ISO/IEC 27033-5 estabelece cinco aspectos para a escolha de uma VPN, sendo requerimentos de segurança, controles de segurança, técnicas de *design*, aspectos regulatórios e legislativos e aspectos da arquitetura (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013):

a) **Requerimentos de segurança**: as ameaças contra a VPN são do tipo negação de serviço e intrusão. A proteção contra esses ataques dependerá da capacidade de filtragem do tráfego indesejado. Dessa forma, a garantia da proteção da infraestrutura, gerenciamento e informação da rede pode ser alcançada pela implementação da confidencialidade dos dados, integridade dos dados, autenticidade e acesso de usuários e administrador, disponibilidade dos terminais VPN e segurança dos *endpoint* (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013). A confidencialidade é garantida quando os dados transmitidos no túnel não são visíveis para outros usuários. Apesar de existir técnicas para tal, essa informação pode não ser protegida contra analisadores ou interceptadores de dados. Quando se tem o conhecimento da existência dessas ferramentas e sabendo que a informação a ser transmitida é sensível, o recomendado é realizar a encriptação *off-line* da informação antes de ser enviada sobre uma VPN. A integridade da informação de uma VPN deve suportar mecanismos de verificação de mensagem, códigos de autenticação e contra replicação de dados. Caso essa proteção de integridade não possa ser implementada no túnel, ela deve ser realizada no sistema de destino. A autenticidade da informação é garantida quando cada ponta do túnel possui mecanismos de controle que permitam a identificação correta entre cada ponta do túnel. Considerando o caso uma rede pública, seria a identificação correta do endereço IP entre origem e destino. Complementado o mecanismo de autenticidade, a autorização deve suportar mecanismos que implementem uma lista de controle de acesso, ou *Access Control List* (ACL), em cada ponta do túnel, garantindo que a fonte da informação possua autorização no fluxo de dados. A disponibilidade do túnel VPN é garantida pela implementação que se consiga incorporar contra medidas de ataque de negação de serviço na infraestrutura. Finalmente, a segurança do *endpoint* do túnel VPN deve garantir que haja apenas tráfego de rede controlado entre a rede de hospedagem e

a VPN, como pela desabilitação do roteamento e o uso de filtro de pacotes ou tecnologia de *firewall*;

b) **Controles de segurança**: primeiramente, devem ser baseados no próprio túnel criado. Apesar dos túneis estarem ocultos, por exemplo, em uma rede pública, eles podem ser detectados por inspeções de invasores utilizando-se analisadores e interceptadores de dados. Mesmo com o uso de criptografia, o invasor, nesse caso, poderia ter acesso ao tráfego de informação, bem como dos pontos de extremidade do túnel, que podem estar desprotegidos de ataques lógicos não autorizados. Dessa forma, a segurança do túnel deve ser realizada de acordo com a política de segurança da organização, que deve prever o nível de risco aceitável de acesso aos dados considerando essa situação. Vale destacar que mesmo não tendo acesso ao conteúdo da informação, a simples determinação da localização física do *endpoint* já é um fator a ser considerado, principalmente em um ambiente militar onde o local físico da rede possa ser uma informação sigilosa;

c) **Técnicas de *design***: uma VPN é construída em uma rede física pelo uso de criptografia e ou encapsulado de pacotes. Essa infraestrutura permite que uma VPN possa ser utilizada tanto em redes privadas quanto em redes públicas, sendo a pública o meio de maior custo benefício que suporta WAN e acesso remoto para várias aplicações. A rede pública, considerando nesse caso a internet, implica que uma infraestrutura de VPN deva ser bem dimensionada para garantir a segurança da informação em virtude de seu grau de incerteza dos provedores quanto à confidencialidade. Além disso, aspectos de flexibilidade do túnel, como ativação e desativação da rede ou necessidade de mudar a estrutura da rede física, devem ser suportados pela VPN. Assim, o *design* de uma rede VPN deve considerar três tipos de modelagem de túnel: circuitos virtuais, comutação de rótulos multiprotocolo ou encapsulamento de protocolo (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013). Os circuitos virtuais, criados na camada de enlace do modelo OSI, implementam tecnologias de comutação de pacotes em WAN, permitindo que o fluxo de dados entre túneis seja separado entre si. A comutação de rótulos multiprotocolo, criada na camada de enlace ou rede, estabelece um túnel em que cada pacote de dado seja atribuído a uma etiqueta de identificação, garantindo que pacotes com rótulos diferentes sejam excluídos. A técnica de encapsulamento de protocolo realiza um empacotamento de um protocolo que é transportado por outro, conforme visto na seção 2.8.2;

d) **Aspectos regulatórios e legislativos**: A utilização de uma VPN deve considerar os aspectos regulatórios e legislativos de agências governamentais locais. Os principais aspectos a serem considerados incluem proteção e privacidade dos dados, uso da tecnologia de criptografia e riscos operacionais de governança e gerenciamento (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013). A respeito do gerenciamento, ele deve ser claro e considerar as responsabilidades de todas as entidades associadas à VPN, incluindo a de que os usuários devem estar cientes dos riscos inerentes à segurança e das áreas de controle relacionadas a essa conexão. Esse fator é importante, pois definirá todo o processo de decisão do órgão em relação à manutenção e controle de segurança da VPN;

e) **Aspectos da arquitetura**: a seleção da arquitetura da VPN deve levar em conta os seguintes aspectos (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013):

- **A segurança do *endpoint***: envolve a segurança de dispositivos e aplicações que, se comprometidos, podem tornar a rede vulnerável. O ideal é que se use um número reduzido de *endpoint*, principalmente quando existe a possibilidade de eles se conectarem a redes diferentes, como na internet;
- **Segurança das terminações**: envolve o uso de autenticação do usuário antes de permitir o acesso à rede, feito por meio de *login* e senha ou utilizando, por exemplo, um *token*, cartão ou tecnologia biométrica;
- **Proteção contra *softwares* maliciosos**: devem ser implementados mecanismos que detectem a ação de *softwares* maliciosos embutidos nos dados transmitidos na forma de *scripts*. O ideal é que tal mecanismo esteja ativo no receptor da informação;
- **Autenticação**: o ideal é que cada entidade da sessão VPN realize sua autenticação, utilizando métodos como de chaves pré-compartilhadas ou pelo uso de certificados;
- **Sistema de detecção de intrusão**: deve-se considerar o uso de algum sistema de detecção de intrusão, ou *intrusion detection system* (IDS), implementado nos dois lados da VPN. O alerta do IDS deve ser realizado por mecanismo, permitindo que possa ser realizado um registro de auditoria;
- **Segurança dos *gateways***: inclui a seleção apropriada de um *firewall*;
- **Projeto da rede**: deve considerar que uma VPN termine em um *firewall* externo ou dentro de sua própria sub-rede confiável, comumente denominada *Demilitarized Zone*;

- **Outras conectividades**: deve-se ter atenção nos pontos de conectividade da extremidade da VPN. A presença de outros canais de conexão nas extremidades pode abrir oportunidades de um ataque, comprometendo a segurança. O projeto da rede deve levar em conta essa situação, principalmente nos casos de conexão da organização com uma entidade terceira ou em sistemas que utilizem *modem* para conexão remota. Nesse caso, o ideal é que haja garantia de segregação física e lógica do ambiente que a entidade possa utilizar;
- **Divisão do tunelamento**: a utilização de uma única conexão para suportar uma VPN e outra conexão (VPN ou não) deve ser evitada. O comprometimento de um túnel por ataque, caso se divida a conexão, pode comprometer o túnel adjacente a uma rede remota;
- **Registro de auditoria e monitoramento de rede**: a solução VPN deve manter *logs* de auditoria para análise de todo o tráfego em cada nó da extremidade. Além disso, os *logs* gerados devem ser protegidos contra uso indevido e corrupção da informação. Isso se faz necessário porque a informação gerada para auditoria pode ser utilizada em processos legais e, consequentemente, sua integridade deve ser comprovada;
- **Gerenciamento técnico de vulnerabilidades**: o gerenciamento de possíveis vulnerabilidades técnicas inerentes à tecnologia devem ser presente em todos os dispositivos VPN. Nesse sentido, é importante que as soluções adotadas sejam acompanhadas em suas atualizações para correção de possíveis erros técnicos que possam existir;
- **Criptografia de rota de rede pública**: a utilização de um roteamento por meio de uma rede de terceiros não confiável pode tornar a VPN vulnerável a algum tipo de análise de dados. Mesmo com o uso de criptografia, em alguns casos, os nós das extremidades podem ser identificados. Caso seja um requisito para a ofuscação das extremidades, é necessário adicionar mecanismos aos nós da extremidade para manter os usuários ocultos. Como exemplo, podem ser citados os *proxies* virtuais e o *The Onion Router Project* (TOR).

Tendo em vista alguns requisitos da tecnologia VPN, de acordo com a ISO/IEC 207033-5, foi realizada uma pesquisa de soluções *open source* disponíveis para implementação. Foram encontradas sete opções, que estão listadas a seguir com algumas características inerente a elas.

3.4.2.1 OpenVPN

O OpenVPN (Figura 29) é uma ferramenta alternativa de implantação de redes virtuais privadas que realiza a criptografia de pacotes de dados e os envia pela Internet. Segundo Freitas Júnior *et al.* (2015), o OpenVPN possui código aberto e gratuito disponível em várias plataformas, como Windows, MacOS X e distribuições Unix. O processo para garantir a integridade e confidencialidade dos pacotes no OpenVPN se dá pela utilização da criptografia dos protocolos SSL/TLS dos pacotes que irão trafegar na rede pública e a utilização da porta 1194 padrão de qualquer *firewall* (FREITAS JUNIOR *et al.*, 2015).

Durante a transmissão dos pacotes, o OpenVPN cria um adaptador de rede virtual com conexão *User Datagram Protocol* (UDP), permitindo que somente os níveis superiores e aplicações sejam capazes de fazer a verificação e retransmissão de pacotes, além de distinguir os dados. Isso permite que a informação só possa ser recuperada pelo cliente que possuir a chave criptográfica correta. Além disso, o OpenVPN permite que os usuários possam criar políticas especificas de controle de acesso (CAMPINHOS; BARCELLOS, 2007). A principal característica do OpenVPN é que ele vem equipado com uma chave 256-AES-CBC e *Diffie-Hellman* de 2048 *bits* para usuários do Windows. Para usuários do Linux, iOS e MacOS, o OpenVPN criptografa informações por meio do protocolo IKEv2/IPsec com uma chave AES-256-CGM e *Diffie-Hellman* de 3072 *bits*. No Quadro 8 estão sintetizadas as suas características (OPENVPN, 2019).

Quadro 8 – Características OpenVPN v2.4.8

Itens	Características
Sistemas operacionais suportados	Android, iOS, Linux, MacOS e Windows.
Conexão	*Site-to-Site* e acesso remoto.
Criptografia	Negociação de cifra de canal de dados utiliza AES-256-GCM (*default*); Canal de controle TLS suporta curvas elípticas *Diffie-Hellmann*.
Protocolos	SSL VPN com suporte ao TLS 1.3 (não suporta clientes com TLS 1.0); Ipv4 e Ipv6; Não opera com IPsec e L2TP; Suporta protocolos TCP e UDP (sobrepassa *firewalls*).
Certificados	Utiliza LCR; Tratados pela biblioteca OpenSSL; Não necessita de PKI oficial. Pode utilizar uma AC fictícia; Padrão X.509.

Fonte: (OPENVPN, 2019).

Figura 29 – Ferramenta OpenVPN

Fonte: (OPENVPN, 2020)

Segundo Campinhos e Barcellos (2007), o OpenVPN apresenta as seguintes características:

a) Permite criar túnel para qualquer sub-rede IP ou adaptador *ethernet* por protocolo UDP ou TCP. O TCP é menos usual, pois piora o desempenho da VPN, já que o protocolo verifica e retransmite pacotes perdidos (FREITAS JUNIOR *et al.*, 2015);
b) Utiliza a encriptação, autenticação e certificação da biblioteca OpenSSL, possibilitando uma variedade de cifragens, tamanho de chave e autenticação;
c) Permite a criptografia baseada em chave estática ou certificados baseados em encriptação de chave pública;
d) Permite criar túneis em *firewall*, sem a necessidade de criação de regras específicas;
e) Possui *software* independente do sistema operacional, o que o torna não dependente de atualizações que o sistema possa sofrer;
f) Possui a grande vantagem de possibilitar o seu funcionamento em redes com *firewall* e roteadores que utilizam o protocolo *Network Adress Translation* (NAT).

O OpenVPN é uma alternativa ao modelo tradicional que utiliza o IPSec, pois esse protocolo possui a desvantagem de não impedir que o tráfego de rede seja monitorado (GUIMARÃES, 2004). Isso permite que provedores de serviço de internet realizem mecanismos para bloquear protocolos do IPSec, possibilitando a monetização do serviço.

3.4.2.2 FreeS/WAN e Libreswan

O FreeS/Wan (Figura 30) foi um projeto de implementação de VPN no Linux que utilizou o protocolo IPSec para autenticação e criptografia dos pacotes de dados. Segundo Campinhos e Barcellos (2007), a iniciativa do projeto foi realizada por John Gilmore, porém, na década de 90, o projeto obteve entraves em seu desenvolvimento nos Estados Unidos da

América (EUA). Segundo o regulamento americano, para que um *software* criptográfico pudesse ser exportado, ele deveria usar apenas pares de chaves RSA de 512 *bits* ou menos, com o objetivo de permitir que somente a Agência de Segurança Nacional dos EUA, a *National Security Agency* (NSA), pudesse quebrar o algoritmo caso fosse necessário. Em virtude desse empecilho, inicialmente o FreeS/Wan foi desenvolvido por um grupo do Canadá: Hugh Redelmeier, Richard Guy Briggs, Michael Richardson, Claudia Schmeing e Sam Sgro. Além do apoio da equipe canadense, o projeto também contou sua inclusão em várias distribuições Linux de uso geral, principalmente em países com leis mais brandas em relação à criptografia. Gilmore *et al*. (2004) citaram as seguintes contribuições: SuSE Linux (Alemanha), Conectiva (Brasil), Mandrake (França), Debian, distribuição Linux polonesa e Best Linux (Finlândia).

A ideia inicial do projeto visava padronizar o IPSec, permitindo que a internet tivesse um nível de segurança nativo para estabelecer a troca de pacotes de dados. A vantagem do FreeS/WAN seria a de que cada usuário com o *software* instalado pudesse se comunicar de forma segura com outros usuários que possuíssem o mesmo sistema sem a necessidade de um administrador. De acordo com Campinhos e Barcellos (2007), os principais objetivos do FresS/WAN são:

a) Padronizar o IPSec na internet;
b) Disponibilizar gratuitamente o código-fonte do IPSec;
c) Permitir o uso em sistemas Linux;
d) Permitir que o IPSec realize a conexão sem a necessidade de configuração de um administrador;
e) Permitir que uma parcela considerável do tráfego da rede mundial seja feita de forma criptografada.

Figura 30 – Ferramenta FreeS/WAN

Fonte: (GILMORE *et al*., 2004).

Na época em que foi concebido, o FreeS/WAN permitia obter uma solução econômica para a plataforma Linux, pois não era necessário um *hardware* de VPN dedicado para realizar a comunicação segura. Um simples microcomputador com duas placas de rede já permitia a implementação da VPN de forma satisfatória. Apesar dos benefícios citados, o FreeS/WAN lançou sua última versão em 22 de abril de 2004, a v2.06, considerada como precursora do projeto Openswan (GILMORE *et al*., 2004).

Seu sucessor, o Libreswan (Figura 31), está em desenvolvimento ativo há mais de 15 anos. O Libreswan suporta as versões 1 e 2 do IKE, podendo ser executado no Linux 2.4 a 5.x, FreeBSD e Apple OSX. No Linux, usa a pilha IPsec "XFRM" integrada (Linux-IPSec) e a biblioteca de criptografia NSS (LIBRESWAN, 2019) (Quadro 9).

Quadro 9 – Características Libreswan

Itens	Características
Sistemas operacionais suportados	Linux 2.4 a 5.x
Conexão	*Site-to-Site* e acesso remoto
Criptografia	IPsec
Protocolos	IKEv1, IKEv2
Certificados	...

Fonte: (LIBRESWAN, 2019).

Figura 31 – Ferramenta Libreswan

Fonte: (LIBRESWAN, 2019).

3.4.2.3 Openswan

O Openswan (Figura 32) é um *software* livre que implementa VPN no sistema operacional Linux utilizando os protocolos de IPSec. Seu surgimento deve-se à primeira solução de IPSec do Linux, o FreeS/WAN, encerrado em março de 2004 (CAMPINHOS;

BARCELLOS, 2007). As principais características do Openswan são, segundo Campinhos e Barcellos (2007):

a) Segurança oferecida pelo protocolo IPSec;
b) Ferramenta conhecida na área de TI com Linux;
c) Compatível com sistemas Unix;
d) Constantes atualizações (no momento de realização deste trabalho foi possível encontrá-lo disponível na versão 2.6.51.5, lançado em junho de 2019).

O Openswan, mesmo sendo um *software open source*, conta com o patrocínio de grandes organizações, como:

a) Xelerance Corporation (2020), desenvolvedora do Openswan da versão 1.0 à versão 2.6.36;
b) RedHat (2020), desenvolvedora do protocolo IKEv2.
c) Sony, patrocinadora do desenvolvimento do IPsec/L2TP;
d) Siemens, patrocinadora do desenvolvimento do IPsec/L2TP;
e) Packt Publishing (2020), contribuição de 5% da venda de livros sobre Openswan;
f) HP (2020), fornecedora de hardware;
g) Cyberoam (2020), contribuição em várias correções;
h) Emagister, patrocinadora do desenvolvimento do IPsec/L2TP;
i) Astaro (2020), contribuição de correções e *hardware*.

O auxílio de vários colaboradores permite que o desenvolvimento do projeto seja feito de forma cooperativa, possibilitando que falhas sejam identificadas e corrigidas rapidamente. Além disso, sua documentação é extensa e pode ser encontrada em *sites* relacionados sobre o assunto. Um resumo das características do Openswan está disposto no Quadro 10.

Quadro 10 – Características Openswan

Itens	Características
Sistemas operacionais suportados	Linux
Conexão	...
Criptografia	IPsec e L2TP; IKEv2
Protocolos	Suporte a NAT transversal
Autenticação	Padrão X509

Fonte: (XELERANCE CORPORATION, 2016).

Figura 32 – Ferramenta Openswan

Fonte: (XELERANCE CORPORATION, 2016).

3.4.2.4 Tcpcrypt

O protocolo Tcpcrypt (Figura 33) é uma solução VPN que não necessita de configuração, alterações nos aplicativos ou mudanças visíveis na sua conexão de rede. Ele opera usando algo conhecido como "criptografia oportunista", trabalhando com o protocolo TCP na camada de transporte (BITTAU *et al.*, 2014a). Isso significa que, se a outra extremidade da conexão se comunicar com Tcpcrypt, o tráfego será criptografado. Caso contrário, poderá ser visto como texto não criptografado.

Outra característica é o conceito de ID de sessão criado em cada extremidade dos nós da VPN, permitindo que o ID gerado com um segredo compartilhado (como uma senha) possa ser autenticado pelo emissor e receptor. Isso permite que emissor e receptor possam trocar os *hash* criptográficos oriundos do segredo compartilhado e do ID de sessão, garantindo a autenticidade da conexão. O grupo criador do Tcpcrypt tentou padronizar no IETF a extensão do protocolo TCP desenvolvido, gerando a RFC 8548 (BHARGAVAN; LEURENT, 2016). O protocolo sofreu várias atualizações robustas que o tornaram mais protegido contra ataques passivos e ativos. O Tcpcrypt pode ser uma boa solução no caso de informações de conteúdo menos sensíveis. O Quadro 11 sintetiza as suas características.

Quadro 11 – Características Tcpcrypt

Itens	Características
Sistemas operacionais suportados	Windows, Linux, MacOS X e FreeBSD.
Conexão	...
Criptografia	Encriptação oportunista; confidencialidade feita nos segmentos TCP
Protocolos	Ipv4.
Autenticação	Produz somente ID de sessão, permitindo que qualquer método de autenticação possa ser implementado (menor custo no uso de chaves RSA).

Fonte: (BITTAU *et al.*, 2014a).

Figura 33 – Ferramenta Tcpcrypt

Fonte: (BITTAU *et al.*, 2014b).

3.4.2.5 Tinc VPN

O Tinc (Figura 34) é um *software* livre, licenciado pela *General Public License* (GNU). Diferentemente de outras VPN, inclusive do OpenVPN, oferece uma variedade de recursos exclusivos, como criptografia, compactação opcional, roteamento automático de malha e fácil expansão (Quadro 12). O Tinc é uma solução ideal para empresas que desejam criar uma VPN com base em inúmeras redes menores, geograficamente distantes.

Quadro 12 – Características Tinc

Itens	Características
Sistemas operacionais suportados	Linux, FreeBSD, OpenBSD, NetBSD, MacOS X, Solaris, Windows 2000, Windows XP.
Conexão	...
Criptografia	OpenSSL (e autenticação) e LibreSSL; Encriptação: AES-256-CTR; Resumo de mensagem: HMAC-SHA-256; *Zlib* (compressão).
Protocolos	Suporta NAT transversal; IPv4 e Ipv6.
Certificados	...

Fonte: (TIMMERMANS; SLIEPEN, 2015).

Figura 34 – Ferramenta Tinc

Fonte: (TIMMERMANS; SLIEPEN, 2015).

3.4.2.6 SoftEther VPN

A VPN SoftEther (Figura 35) é uma solução que utiliza uma função de clone para o servidor OpenVPN, permitindo migrar perfeitamente do OpenVPN para a SoftEther VPN. A SoftEther também é compatível com os protocolos L2TP e IPsec, permitindo maior personalização. A principal desvantagem da SoftEther diz respeito à compatibilidade. Algumas de suas características são (NOBORI *et al.*, 2013) (Quadro 13):

a) *Software* livre e de código aberto;
b) Fácil estabelecimento de acesso remoto do tipo *Site-to-Site*;
c) Resistência a *firewall* altamente restrito;
d) *Domain Name System* (DNS) dinâmico incorporado e NAT transversal para que nenhum endereço IP, fixo ou estático, seja necessário;
e) Criptografia AES de 256 *bits* e RSA de 4096 *bits*.;
f) Suporte às plataformas Windows, Linux, Mac, Android, iPhone, iPad e Windows Mobile.

Quadro 13 – Características SoftEther

(continua)

Itens	Características
Suportabilidade	4096 *hubs* virtuais; 10.000 usuário por grupo e 10.000 grupos por *hub*.
Requerimentos	RAM (servidor): 32 MB (mínimo) e 128 MB (recomendado); RAM (cliente): 16 MB (mínimo) e 32 MB (recomendado); 100 MB (mínimo) e 2 GB (recomendado) de armazenamento em disco.
Sistemas operacionais suportados	Windows, MacOS X, Android, Linux, NetBSD, OpenBSD, Solaris.
Conexão	Acesso remoto e *Site-to-Site.*

Itens	Características
Criptografia	Resumo de mensagem: RC4-MD5, RC4-SHA, AES128-SHA, AES256-SHA, DES-CBC-SHA and DES-CBC3-SHA; Cifra (L2TP): DES-CBC, 3DES-CBC, AES-CBC /Resumo: MD5/SHA-1; Cifra (OpenVPN): AES-128-CBC, AES-192-CBC, AES-256-CBC, BF-CBC, CAST-CBC, CAST5-CBC, DES-CBC, DES-EDE-CBC, DES-EDE3-CBC, DESX-CBC, RC2-40-CBC, RC2-64-CBC e RC2-CBC/; Resumo: SHA, SHA1, MD5, MD4 e RMD160; AES 256 *bits* e RSA 4096 *bits*.

Fonte: (NOBORI *et al.*, 2013).

Figura 35 – Ferramenta SoftEther

Fonte: (NOBORI *et al.*, 2013).

3.4.2.7 strongSwan

A strongSwan (Figura 36) é uma implementação *open source* IPSec baseada no antigo projeto FreeS/WAN *eno patch* X.509. O projeto foi lançado em 2005 e conta com suporte para as plataformas Linux, Android, FreeBSD, MacOS X, Windows e roteadores (Quadro 14). Atualmente, o projeto é mantido pelo Professor de Segurança em Comunicação Andreas Steffen, do Institute for Networked Solutions at the University of Applied Sciences Rapperswil, na Suíça.

De acordo com o *site* do projeto (STEFFEN, 2018a), a strongSwan é focada nas seguintes premissas (NOBORI *et al.*, 2013):

a) Simplicidade da configuração;
b) Forte método de encriptação e autenticação;
c) Política de IPSec forte que suporta grandes e complexos sistemas de VPN;
d) Topologia modular e de grande capacidade de expansão.

Quadro 14 – Características strongSwan

Itens	Características
Sistemas operacionais suportados	Windows 7/8, Linux, Android 4+, MacOS X, iOS 8+.
Conexão	*Site-to-Site*, *host-to-host* e acesso remoto.
Criptografia	Utiliza IKEv1 e IKEv2 (STEFFEN, 2018b).
Protocolos	Opera com IPsec; Utiliza NAT transversal para mapear dispositivos em NAT (encapsula NAT em UDP).
Certificados	Utiliza LCR e OCSP (protocolo de *status* de certificados *on-line*); Permite o uso de *smart card* para prever comprometimento da PKI; Permite armazenamento de chaves privadas.
Autenticação	EAP-MD5, EAP-MSCHAPv2, EAP-GTC (*login* e senha) EAP-TLS, EAP-TTLS, EAP-PEAP.

Fonte: (STEFFEN, 2018a).

Figura 36 – Ferramenta strongSwan

Fonte: (STEFFEN, 2018a)

3.4.3 Soluções VPN empresariais

Na seção 3.4.2 foram descritas algumas soluções *open source* disponíveis na *web*. Nesta seção estão exemplificadas algumas soluções empregadas pelo meio empresarial e grandes corporações (PIROCLASTO, 2020). Seus produtos incluem as áreas de segurança de rede, segurança multinuvem, acesso seguro, operações de segurança, operações de rede, *endpoint* e proteção de dispositivos e segurança de aplicativos.

3.4.3.1 Fortinet

Fundada em 2000, a Fortinet (Figura 37) é uma empresa multinacional americana que realiza o desenvolvimento e comercialização de produtos e serviços na área de segurança de rede (FORTINET, 2000). Na área de redes privadas virtuais, o FortiClient VPN permite o acesso remoto por meio de técnicas de IPSec, discutidas anteriormente, e de SSL VPN. A vantagem dessa solução é que o usuário final só utiliza o próprio navegador *web*, sem a necessidade de realizar configuração de clientes VPN. Além disso, o uso do protocolo SSL é mais difícil de ser detectado se comparado ao IPSec (CISCO, 2014).

Figura 37 – Fortinet

Fonte: (Fortinet, 2000)

Informações sobre alguns clientes no Brasil que utilizam o serviço podem ser encontradas no *site* da empresa (FORTINET, 2020).

3.4.3.2 Check Point

A empresa Check Point (Figura 38) atua desde 1993 no ramo de segurança para internet oferecendo soluções de *firewall*, *antirransomware*; segurança de *endpoint*, nuvem, *internet of things* e VPN. A solução de VPN da Check Point inclui os produtos: Endpoint Security VPN, SecuRemote, Check Point Capsule Workspace, Mobile Access/SSL VPN, Endpoint Security Client com suporte às plataformas Windows, Mc, iOS, Linux e Android. Dentre os produtos ofertados, os principais protocolos empregados são o IPsec (não aplicado em sistemas Linux) e o SSL VPN. No *site* da empresa há informações sobre os produtos ofertados e as especificações técnicas (CHECK POINT, 2020a), além dos clientes que utilizam o serviço (CHECK POINT, 2020b).

Figura 38 – Check Point

Fonte: (CHECK POINT, 2020c).

3.4.3.3 F5

A F5 Networks (Figura 39) é uma empresa americana com foco na entrega de melhoria de desempenho, segurança e disponibilidade para aplicativos utilizados na *web*. Um de seus produtos é o BIG-IP APM, que fornece uma solução de SSL VPN por meio de *hardware* ou de virtualização. A solução é compatível com os sistemas operacionais Apple MacOS/iOS, Windows, Linux, Android e Chromebook. De acordo com a empresa, o BIG-IP APM fornece a facilidade de consolidar, na infraestrutura de um ambiente corporativo, os serviços de rede, nuvem e aplicação em uma única interface de gerenciamento. No *site* da empresa há informações sobre os produtos ofertados (F5 NETWORKS, 2020a), além da listagem de alguns clientes que utilizam o serviço (F5 NETWORKS, 2020b).

Figura 39 – Soluções BIG-IP da F5

Fonte: (F5 NETWORKS, 2020c).

3.4.3.4 AnyConnect

AnyConnect (Figura 40) é uma solução VPN da Cisco que, além de oferecer as características de uma rede privada de comunicação, oferece outras vantagens, como proteção contra *malware* e inspeção *web*. De acordo com a ficha de dados do produto, essa solução pode utilizar o método de encapsulamento de protocolo *Datagram Transport Layer Security* (DTLS) para aplicações sensíveis à latência, como o tráfego de VoIP ou acesso a aplicativos baseados em TCP, além do suporte para encapsulamento IPsec IKEv2 (CISCO, 2017).

Atualmente na versão 4.X, o AnyConnect é divido em duas camadas de pacotes de serviços. A primeira é o AnyConnect Plus, que inclui serviços básicos de VPN, detecção de redes confiáveis, gerenciamento de acesso a redes pelo protocolo 802.1X e módulo de segurança para nuvens *web*. A segunda é o AnyConnect Apex, que inclui detecção dos terminais de *endpoint*, VPN de acesso remoto sem cliente e utilização de criptografia VPN, incluindo o *Suite* B, conjunto de algoritmos divulgados pela NSA como parte de um projeto para

modernização de algoritmos criptográficos (HOUSLEY *et al*. 2018). Mais informações sobre o AnyConnect estão disponíveis (CISCO, 2017), assim como uma lista de clientes que utilizam o serviço (CISCO, 2020a).

Figura 40 – AnyConnect

Fonte: (CISCO, 2020b).

3.4.4 Soluções VPN utilizadas pela Marinha do Brasil

A DGMM-0540 (Normas de TI da Marinha) estabelece a possibilidade de usuários credenciados, o acesso a alguns serviços disponibilizados pela Rede de comunicações Integrada da Marinha (RECIM). Basicamente a RECIM permite a interligação de redes locais corporativas usadas pelas Organizações Militares (OM), localizadas em território nacional, em países do exterior, no continente Antártico, além dos navios em missão. O acesso a RECIM pode ser feito por duas formas sendo a primeira realizada por conexões dedicadas em terra através de uma WAN (*Wide area Network*), no território nacional, ou por conexão através do Portal de Serviços da MB por qualquer conexão via Internet (EMGEPRON, 2017). Esse acesso pode ser realizado através da plataforma Web **Portal da Marinha** (https://portal.marinha.mil.br/vpn/index.html). O Portal da Marinha permite o acesso de várias aplicações como a ferramenta de busca da Intranet Bussola, Catálogo MB da Diretoria de Administração da Marinha (DadM), acesso à Intranet pelos navegadores *Mozilla* e *Internet Explorer*, aplicativo de mensagem instantânea *Spark*, Sistema de Gerenciamento de Documentos Eletrônicos da Marinha no ambiente Web (Sigdem WEB) e o correio eletrônico Lotus Note (atualmente solução de E-mail Corporativo Zimbra) (MARINHA DO BRASIL, 2020). A utilização desses recursos permite por exemplo que seja realizado cursos Extra-MB no país e exterior, acesso ao Adidos Navais e de Defesa, acesso à Internet de navios em missão dentre outras utilidades. A DGMM-0540 rev3 em seu capítulo 12.5 não especifica o uso de VPN em dispositivos móveis para acesso à RECIM por parte dos usuários. Na tentativa de obter alguma informação sobre a tecnologia VPN implementada no portal, não foi possível conhecer a infraestrutura, junto aos órgãos responsáveis, em virtude do caráter sigiloso. Apesar disso, foi

possível obter indícios da tecnologia utilizada pela Marinha através de pedidos de licitação requeridos pela instituição.

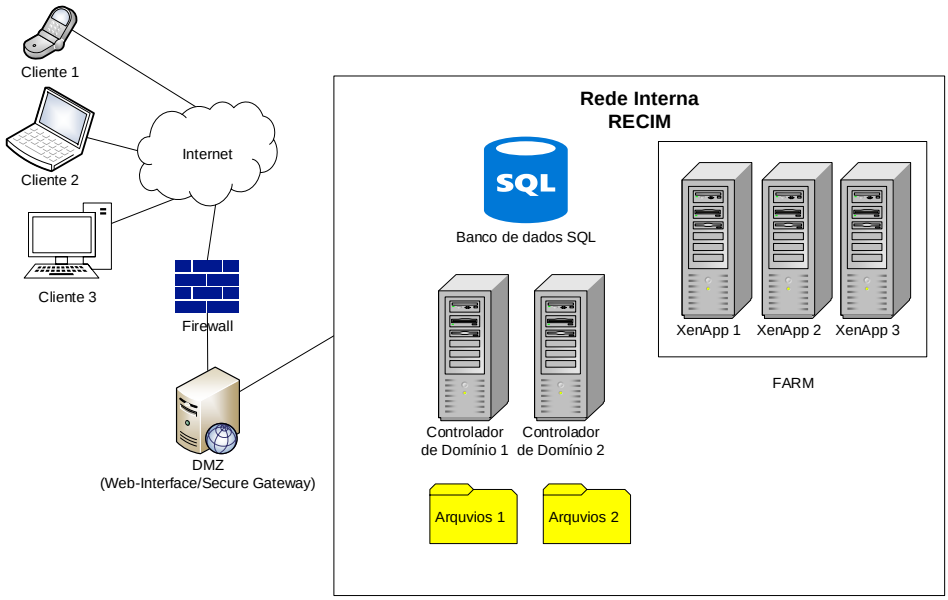
De acordo com a licitação N° 052/2017 da empresa Empresa Gerencial de Projetos Navais (EMGEPRON), a qual é uma empresa estatal ligada ao Ministério da Defesa, foi realizado a contratação de serviço de atualização da solução de virtualização da empresa Citrix para acesso remoto à RECIM através do Portal de Serviços da Marinha. Até junho de 2018 a solução adotada pelo Portal da MB utilizou a aplicação sobre VMware, por meio de servidores virtuais "Citrix XenApp 6.5 Plantium" que estavam em processo de descontinuidade em virtude de ser instalado no sistema operacional Windows Server 2008 Enterpreise R2 o qual o suporte foi finalizado em 2015. A infraestrutura utilizada, até então, era composta por um Secure Gateway que fornece acesso ao Portal e garante a segurança de acesso ao Metaframe server denominado FARM. O FARM (Figura 41) é composto por três servidores virtuais XenApp 6.5. Dessa forma a interface Web bem como o Secure Gateway são executados pelo sistema Windows server 2008 em um servidor instalado em uma DMZ fornecendo encriptação SSL. A virtualização adotada permite que o Portal seja integrado: a servidores Active Directory (AD)/arquivo e um servidor SQL sendo que o servidor de arquivos é o responsável por manter e criar os perfis de usuários que acessam a FARM.

Sobre a aplicação *XenApp Plantium*, de acordo com a empresa desenvolvedora do software CITRIX (https://www.citrix.com/pt-br/products/citrix-virtual-apps-and-desktops/feature-matrix.html) ela atualmente foi substituída pela versão *Citrix Virtual Apps*. De acordo com as informações fornecidas no site, é utilizado a implementação do SSL VPN, porém não é possível confirmar se atualmente a solução adotada pela MB continua sendo a *XenApp Plantium 6.5* ou a nova versão oferecida pela CITRIX. De acordo com informações disponibilizadas para os usuários do Portal MB, o acesso à Intranet da instituição é feita pela instalação do programa *Citrix Receiver* sendo o acesso feito por meio do navegador Web (MARINHA,2020) utilizando uma conexão segura, do tipo SSL (EMGEPRON).

Em relação a conexão à RECIM via conexão dedicada por WAN não foi possível obter detalhes técnicos de alguma solução VPN utilizada. As soluções disponibilizadas para grandes corporações, verificadas nas seções anteriores, costumam utilizar o protocolo IPsec com troca de chaves de *Diffie-Hellman*. Nesse sentido a única informação obtida sobre a infraestrutura de

comunicação na MB é que se se utiliza VPN IPsec em modo túnel de criptografia simétrica com troca de chave *Diffie Hellman* (informação escrita)[1].

Figura 41 – Topologia do Portal MB



Fonte: adaptado de EMGEPRON (2017).

Nota: Clientes acessam a RECIM através de uma DMZ via Internet. A DMZ fornece a encriptação das informações oferecendo um acesso seguro. Na RECIM o FARM permite a integração do DMZ com o servidor de banco de dados e permitindo que seja feita a autenticação dos usuários pelos controladores de domínio para acesso aos arquivos da rede.

[1] Esclarecimento sobre soluções VPN fornecida pelo 1º Ten (T) Augusto César da Fonseca dos Santos, do Centro de Tecnologia da Informação da Marinha (CTIM), em 4 de fevereiro de 2020 às 19:20 por meio de mensagem eletrônica. Transcrição da conversa no Apêndice B deste trabalho.

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Em face da pesquisa realizada sobre as versões TLS utilizadas pela MB e por outras corporações, além das soluções de VPN presentes no mercado, algumas conclusões acerca dos métodos empregados estão descritas nesta seção.

4.1 Análise TLS

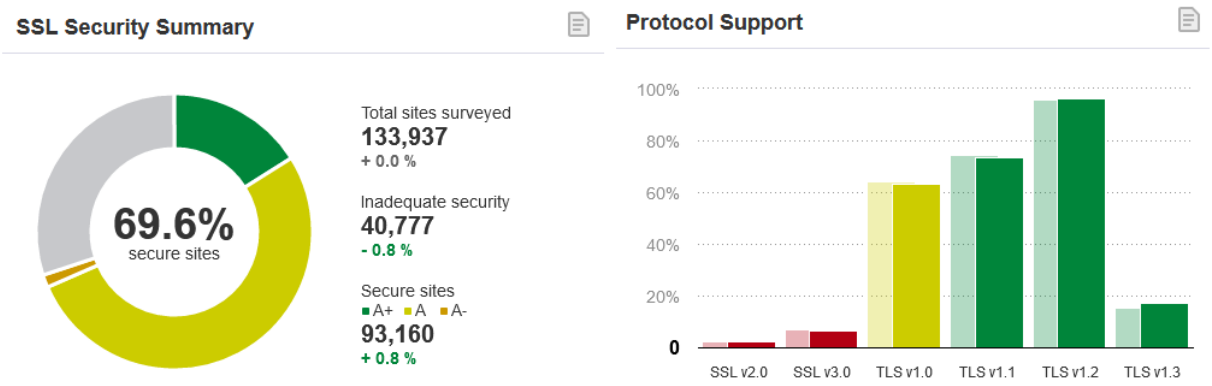
Pelo teste realizado, foi possível constatar que o servidor Web da URL da MB utiliza o algoritmo de resumo de mensagem para assinatura de certificados SHA-256, pertencente à família SHA-2. Cabe ressaltar a existência de uma implementação do SHA-3 mais recente. No entanto, isso não representa um problema, pois o SHA-2 não apresentou vulnerabilidade até o momento de conclusão deste estudo. Porém, o SHA-3 mostra-se como uma alternativa de *backup* caso o SHA-2 apresente pontos fracos.

Uma segunda observação relaciona-se ao protocolo TLS implementado. No servidor da URL pesquisada, as versões 1.1 e 1.2 ainda são suportadas. Vale destacar que foram descobertas vulnerabilidades nessas versões, como o SLOTH e DROWN.

O ataque DROWN é um *bug* de segurança entre protocolos que ataca servidores com modernos conjuntos de protocolos TLS utilizando seu suporte para o protocolo SSL v2 inseguro. Aviram *et al.* (2016) identificaram uma implementação de um ataque DROW que pode descriptografar um *handshake* TLS 1.2. Segundo Bhargavan e Leurent (2016), o SLOTH ataca funções *hash* inseguras com MD5 e SHA1 utilizados no TLS 1.0 e 1.1.

Para se ter uma ideia da tendência atual de versões do TLS, o SSL *Labs* possui uma ferramenta chamada *SSL Pulse* (QUALYS, 2019), que realiza estatísticas mensais em servidores da internet. Uma pesquisa fornecida em 3 de dezembro de 2019 (Figura 40, à esquerda) mostrou que, de um total de 133.937 *sites*, apenas 16,3% apresentavam alta segurança (grade A+), 53% (grade A) e 0,3% (grade A-) estavam seguros e 30,4% apresentavam segurança inadequada. Nessa pesquisa, a maior utilização ainda foi do TLS 1.2, tendo sido o TLS 1.3 menos utilizado que o antigo TLS 1.0 e 1.1 (Figura 42, à direita).

Figura 42 – Estatísticas do uso do TLS em 3 de dezembro de 2019



Fonte: (QUALYS, 2019).

Segundo o *site* ActiveWeb (2019), os fornecedores de navegadores como o Google, Microsoft, Mozilla e Apple irão descontinuar as versões 1.0 e 1.1 do TLS em 2020. Para comparação do suporte ao TLS, foram realizados testes em alguns dos servidores Google, Microsoft, Mozilla, e Apple, além dos servidores do portal do Exército Brasileiro (EB) e da Força Aérea Brasileira (FAB). O resultado geral encontra-se sumarizado no Quadro 15.

Quadro 15 – Comparação de suporte de servidores ao TLS

Servidor	URL	Suporte ao TLS
Google	www.google.com.br	TLS 1.3 Sim TLS 1.2 Sim TLS 1.1 Sim TLS 1.0 Sim
Microsoft	www.microsoft.com	TLS 1.3 Não TLS 1.2 Sim TLS 1.1 Sim TLS 1.0 Sim
Mozilla	www.mozilla.org	TLS 1.3 Sim TLS 1.2 Sim TLS 1.1 Sim TLS 1.0 Sim
Apple	www.apple.com	TLS 1.3 Sim TLS 1.2 Sim TLS 1.1 Sim TLS 1.0 Sim
Exército Brasileiro	www.eb.mil.br	TLS 1.3 Não TLS 1.2 Sim TLS 1.1 Sim TLS 1.0 Sim
Força Aérea Brasileira	www.fab.mil.br	TLS 1.3 Não TLS 1.2 Não TLS 1.1 Não TLS 1.0 Sim
Marinha do Brasil	www.marinha.mil.br	TLS 1.3 Não TLS 1.2 Sim TLS 1.1 Sim TLS 1.0 Sim

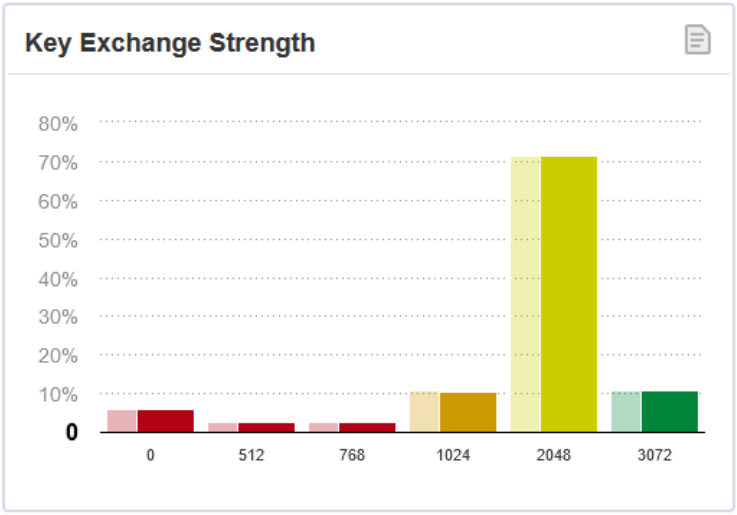
Fonte: adaptado de Qualys (2019).
Nota: os testes foram realizados em 8 de fevereiro de 2020. No teste do servidor da FAB foi identificado certificado expirado em 12 de outubro de 2015.

O Quadro 15 mostra que grandes empresas adotam o TLS 1.3 em seus servidores. O TLS 1.0 e 1.1 ainda é suportado provavelmente por questões de interoperabilidade com sistemas antigos. Em relação ao EB e à FAB, os servidores *web* não suportavam o TLS 1.3 e, diferentemente da MB, ainda suportam o TLS 1.0. Dessa forma, o recomendado seria uma

atualização dos servidores para o TLS 1.3, conforme a tendência das grandes empresas, deixando ainda o TLS 1.2 como segunda opção para clientes que o utilizam.

Quanto ao tamanho das chaves de troca utilizado no protocolo TLS, 71,5% dos servidores utilizavam 2048 *bits*, considerado pelo *site* como requisito mínimo. Apenas 10,8% utilizavam 3072 *bits*. O resumo de uso das chaves está ilustrado na Figura 43.

Figura 43 – Tamanho de chaves utilizado



Fonte: (QUALYS, 2019).

4.2 Pesquisa VPN

De acordo com a ISO/IEC 27033-5, a implementação de uma VPN segura requer a consideração dos seguintes aspectos:

a) **Seleção do protocolo de transporte**: baseada nas necessidades da organização, capacidade de interoperabilidade segundo padrões proprietários ou internacional, percepção do mercado, robustez e vulnerabilidades conhecidas;
b) **Gerenciador de dispositivos VPN**: inclui a configuração da rede, acesso às portas, instalação de certificados e o monitoramento contínuo da rede. Além disso, a implantação de VPN por meio de mídia removível deve ser controlada, impedindo sua execução além do previsto;
c) **Monitoramento de segurança da VPN**: inclui o monitoramento continuado, principalmente dos canais que possuem acesso remoto em redes corporativas. Nesse caso, os pontos finais do túnel devem impedir que o caminho seguro da rede tenha

brechas para invasores. Um dos mecanismos para auxiliar o administrador da rede nessa situação poderia ser a implantação de um IDS, alarmes de segurança ou incidente, *logs* para auditoria e inspeções rotineiras, além de treinamento dos usuários para identificar e reportar informações sobre incidentes de segurança.

Com base nas soluções apresentadas (OpenVPN, Libreswan, Openswan, Tcpcrypt, Tinc VPN, SoftEther VPN e strongSwan) e levando em consideração alguns aspectos da norma ISO/IEC 27033-5, foi possível realizar observações importantes acerca das opções de VPN disponíveis.

A primeira é sobre a **seleção do protocolo de transporte** utilizado (Quadro 16). Dentre as soluções, somente o OpenVPN, Tcpcrypt e Tinc VPN possuem soluções específicas de protocolos de VPN em vez do IPSec. Com base na pesquisa realizada, sabe-se que o IPSec tenha, possivelmente, alguma vulnerabilidade explorada pela NSA durante o processo de troca de algoritmo criptográfico *Diffie-Hellman* (ADRIAN *et al*., 2015). Em virtude disso e considerando um ambiente de tráfego de informações sigilosas, talvez uma solução IPSec não seja vantajosa. Porém, deve-se considerar o grau de risco e o nível de confidencialidade requerido para o trâmite de mensagens da organização. Somado a isso, o IPSec possui as seguintes desvantagens: não prevenir análise de tráfego por meio dos endereços de destino e origem dos *gateways*, autenticar os usuários nos *endpoints* e prevenir ação de ataques de negação de serviço (GUIMARÃES, 2004).

Cabe ressaltar que o SSL VPN também apresenta desvantagens como (SONG, 2005):

a) Falta de softwares de segurança em hosts de máquinas públicas somado a facilidade de conexão de qualquer lugar da Internet, a uma rede interna corporativa, podem propiciar a propagação de malwares;

b) Se um computador remoto tiver uma conexão de rede estabelecida com a sua rede interna e o usuário deixar a sessão aberta, sua rede interna estará exposta a pessoas que tenham acesso físico à máquina;

c) As máquinas clientes da VPN SSL podem estar mais vulneráveis a ataques de *Keylogger*, pois computadores acessíveis ao público podem não atender às políticas de segurança corporativa;

d) Possibilidade de perda de informações confidenciais e propriedade intelectual da corporação por meio de uma máquina remota compartilhada em domínio público;

e) Interceptação do tráfego do usuário através de ataques de *man-in-the-middle*;

f) Limitação de hardware dos hosts remotos podem de usuários corporativos podem impossibilitar que sejam implementados recursos de autenticação como leitores de cartões e dispositivos biométricos.

Das soluções com algoritmo próprio, o OpenVPN tem a vantagem de utiliza o SSL VPN que facilita a portabilidade entre sistemas operacionais e arquiteturas de processador em contraste com o protocolo IPSec que foi projetado para ser implementado como uma modificação da pilha IP no espaço do kernel e, portanto, cada sistema operacional requer sua própria implementação independente (OPENVPN, 2010). Além disso é possível a obtenção de informações de suporte em fóruns de discussão de usuários e da própria empresa desenvolvedora. As soluções com protocolos Tcprypt e Tinc, apesar de apresentarem mecanismos diferentes dos usualmente empregados em VPN, como o IPsec, podem ter sua confiabilidade questionada em virtude da pouca percepção no mercado. Apesar dessas considerações, o conceito principal é que a solução adotada deve estar de acordo com as necessidades da organização e com os riscos envolvidos.

Quadro 16 – Protocolos das soluções VPN

VPN	Observação
OpenVPN	Possui protocolo de rede específico para VPN (trabalhando em modo túnel)
Libreswan	IPSEC
Openswan	IPSEC e L2TP
Tcpcrypt	Criptografia na camada de transporte
Tinc VPN	Protocolo específico
SoftEther VPN	L2TP e IPSEC
strongSwan	IPSEC

Fonte: elaborado pelo autor.

A segunda observação relaciona-se às opções de sistemas operacionais suportados (Quadro 17). Somente o Libreswan e Openswan apresentaram o Linux como único sistema operacional suportado. As demais opções apresentaram uma boa compatibilidade com os aqueles mais usados no mercado. Essas possibilidades permitem que sejam implementadas VPN que consigam acessar diversos dispositivos com sistemas operacionais distintos, facilitando o uso de conexão do tipo remoto. Apesar dessa facilidade, o acesso remoto exigirá mais recursos de segurança em virtude de o acesso ser feito externamente ao ambiente

operacional. Assim, os requisitos de **segurança das terminações** e **controles de segurança** devem ser levados em consideração, pois o acesso de uma rede corporativa, como a internet, que utilize algum dispositivo móvel ou computador fora da rede irá exigir mecanismos de autenticação de usuário e o uso de ferramentas de **proteção contra *softwares* maliciosos** que possam estar nas máquinas remotas. Outro ponto é que, além da confidencialidade da informação promovida pela criptografia, considerando a aplicação de uma VPN em uma organização militar, a não revelação da localização geográfica dos usuários nos *endpoints* pode ser um requisito necessário para a comunicação.

Quadro 17 – Sistemas operacionais suportados

(contínua)

VPN	Observação
OpenVPN,	Android, iOS, Linux, MacOS e Windows.
Libreswan	Linux
Openswan	Linux
Tcpcrypt	Windows, Linux, MacOS X e FreeBSD
Tinc VPN	Linux, FreeBSD, OpenBSD, NetBSD, MacOS X, Solaris, Windows 2000, Windows XP
Softether VPN	Windows, MacOS X, Android, Linux, NetBSD, OpenBSD, Solaris
strongSwan	Windows 7/8, Linux, Android 4+, MacOS X, iOS 8+

Fonte: elaborado pelo autor.

A terceira observação refere-se aos **aspectos da arquitetura**. Com base nas informações coletadas, as soluções do SoftEther e strongSwan foram as que mais forneceram dados relacionados ao seu funcionamento, como: tipos de criptografia e protocolos utilizados, método de autenticação, velocidade de conexão e certificado. Quanto mais características da VPN o cliente obtiver conhecimento, melhor será a escolha da VPN. Dessa forma, pode-se determinar o grau de risco a que a informação será submetida.

A última observação, não relacionada diretamente às tecnologias abordadas, diz respeito aos **aspectos regulatórios e legislativos**. Antes de se utilizar um serviço de VPN, deve-se ter em mente a legislação local do país referente ao tráfego de dados de rede, sobretudo da rede pública. Existem países com leis rígidas, que limitam o uso de informações na internet. Seja por questões políticas, esforços para manter os valores sociais e tradições e outros fatores relacionados à segurança nacional, a restrição de VPN abrange desde a seleção de determinados produtos, permitidos pela legislação local, até a proibição de qualquer conexão que permita o anonimato. Janssen (2019) listou alguns países que aplicam algum tipo de restrição a VPN,

como visto no Quadro 18. Assim, o uso de uma solução de VPN deve considerar os critérios estabelecidos pelas legislações locais.

Quadro 18 – Países com restrição ao uso de VPN

(continua)

País	Observação
Bielorrúsia	VPN e uso do navegador **TOR** foram proibidos em 2015, e o uso de redes ou conexões de anonimatos são considerados ilegais.
China	Permite o uso de alguns serviços VPN legalmente. Em 2018 ameaçou bloquear VPN estrangeiras, porém ainda assim é possível utilizá-las.
Egito	O governo tem utilizado o d*eep packet inspection* (DPI) para bloquear vários protocolos de VPN (PPTP, L2TP, OpenVPN) desde 2017. Embora as VPN não sejam oficialmente ilegais, o Egito tem dificultado o uso das VPN para aproveitar a internet com liberdade dentro de suas fronteiras.
Iraque	O Iraque baniu completamente as VPN em 2014, quando também bloqueou algumas redes sociais e outros serviços. O país alegou que essas ações ajudariam a combater o Estado Islâmico.
Irã	O Irã baniu oficialmente o uso de muitas VPN a partir de março de 2013. Divulgar e vender essas VPN é proibido e pode resultar em prisão. Apenas as VPN com aprovação do governo podem ser utilizadas.
Coreia do Norte	Não permitem que cidadãos utilizem a internet comum. VPN são proibidas, mas como o país é totalmente fechado em relação ao resto do mundo, as consequências do uso de VPN são desconhecidas.
Omã	O uso de VPN é proibido para a maioria dos cidadãos de Omã. Apenas empresas licenciadas podem utilizar VPN. Além disso, apenas os serviços de VPN aprovados pelo governo podem ser utilizados legalmente.
Rússia	Desde julho de 2017, os provedores de VPN só podem oferecer seus serviços para a população russa se compartilharem todos os dados de seus usuários com o governo. Em 2019, o *Roskomnadzor*, força nacional russa de controle de mídia, deu 30 dias de prazo para as principais VPN concederem acesso a todos os dados russos e permanecer dentro das leis russas. Muitas VPN responderam a esse ato encerrando seus servidores russos.
Síria	O uso de VPN não é exatamente ilegal na Síria. No entanto, desde 2011, algumas conexões de VPN vêm sendo bloqueadas, com o governo atacando os protocolos de VPN.
Turquia	O governo se esforça para detectar e bloquear conexões VPN pelo uso de DPI. Portanto, nem sempre uma VPN funcionará no país.

(continua)

País	Observação
Uganda	Em 2018, a taxa de mídia social foi introduzida em Uganda. Para burlar essa taxa, muitos cidadãos recorreram ao uso das VPN. Hoje, o governo bloqueia as conexões VPN e desestimulam seu uso. No entanto, o uso de VPN não é oficialmente ilegal.
Emirados Árabes Unidos	Nos EAU, o uso de VPN só é permitido para empresas. O uso de VPN é ilegal para cidadãos que a utilizam com propósitos criminosos. No entanto, nos EAU, visitar *sites* de encontros e a Netflix americana também são considerados atos criminosos. Serviços de VoIP, como o Skype, também não são permitidos.

Fonte: (JANSSEN, 2019).

5 CONCLUSÃO

Conforme verificado, a adoção do protocolo TLS 1.3 é uma medida necessária para manter a garantia da segurança da rede, pois apresenta o padrão mais moderno para realizar conexão segura dentro ou fora de um ambiente corporativo. Mesmo com a sua adoção, ainda é válida a expressão que muitos profissionais da área de TI utilizam: “não existe uma rede 100% segura”. Assim, são necessárias responsabilidades por parte dos usuários em relação à navegação em *sites* que possam ser inseguros. Deve-se, ainda, observar o que os usuários estão tentando acessar e quais as possíveis vulnerabilidades existentes nos *softwares* aplicativos (navegadores, programas *e-mail*, etc.) e sistemas operacionais.

Como exemplo, em 16 de janeiro de 2018, a Microsoft lançou uma correção da vulnerabilidade *CurveBall* (CVE-2020-0601) descoberta pela NSA (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020). A *CurveBall* é uma vulnerabilidade do tipo *spoofing* existente no CRYPT32.DLL, responsável por fazer reconhecimento de assinaturas de certificados no Windows 10 e Windows Server 2016 e 2019 e que poderia, por exemplo, comprometer uma conexão TLS. A vulnerabilidade age no processo em que a criptografia de curvas elípticas (CCE), uma aproximação de uma criptografia de chave pública, não realiza a verificação correta da assinatura de certificados. A CCE necessita de vários parâmetros padronizados para seu funcionamento, inclusive o chamado parâmetro gerador. No caso, o parâmetro gerador apresentava uma vulnerabilidade, permitindo que um atacante pudesse fornecer seu próprio gerador. Isso permite, por exemplo, que executáveis maliciosos possam ser executados como arquivos de uma fonte legítima, além de permitir decriptação de informações sigilosas de conexões (GATLAN, 2020). Uma das ações resultantes seria a interceptação e modificação por um MITMAN de uma comunicação TLS ou *sopofing* de uma assinatura digital (GATLAN, 2020). Mesmo com esse problema, o TLS ainda sim é uma ferramenta essencial para manter o fluxo de dados de informação íntegro e autêntico.

Apesar de problemas de vulnerabilidades serem possíveis, o TLS mostra-se como um protocolo necessário para navegação na *web*. E para entender como a versão mais recente do TLS 1.3 está sendo empregada, foi realizada uma pesquisa para verificar se grandes corporações e os portais *web* das Forças Armadas do Brasil estão utilizando esse protocolo. Foi verificado que algumas corporações, como Mozilla, Apple e Google, já implementam o TLS 1.3 em seus servidores. Em relação às Forças Armadas do Brasil, o TLS 1.3 ainda não foi implementado.

Quanto às VPN pesquisadas, verificaram-se várias soluções existentes, tanto *open source* (OpenVPN, Libreswan, Openswan, Tcpcrypt, Tinc VPN, SoftEther VPN e strongSwan) quanto corporativa (Fortinet, Check Point, F5 e AnyConnect), que adotam principalmente o protocolo IPSec e outros protocolos, como o SSL/TLS VPN, L2TP e Tcpcrypt. Com base na análise realizada, verificou-se a existência de uma gama de soluções que poderiam ser aplicadas no ambiente institucional da MB, que vão desde a comunicação segura entre organizações militares e suas unidades operativas até uma simples VPN de acesso à rede sem fio por meio de uma *Demilitarized Zone* (DMZ).

A respeito do parecer 052/2017 percebe-se que existem problemas relativos a suporte e manutenção de sistemas corporativos adquiridos por empresas de TI em virtude do alto custo que isso traz para manter os serviços tanto para manter o software atualizado como o suporte para manutenção (EMGEPRON, 2017). Conforme descrito, em alguns casos, o único recurso para solução de problemas, quando não se tem suporte da empresa proprietária ou quando o sistema é descontinuado, baseia-se em informações colhidas em sítios e fóruns da internet. Outro ponto observado a respeito do Portal da MB é que seu acesso é realizado por autenticação monofator utilizando apenas login e senha para identificação de usuários. A autenticação é um fator previsto pela ISO/IEC 27033-5 na segurança das terminações e dependendo do grau de sigilo das informações trafegadas, recursos adicionais devem ser empregados como o uso de *token* ou biometria.

5.1 Considerações finais

Em virtude da adoção de antigas versões TLS abaixo da 1.3, recomenda-se que sejam realizados estudos para implementação dessa nova versão. Tal medida é necessária para garantir a continuidade dos serviços de forma segura, com integridade, autenticidade e sigilo na navegação feita pelos usuários.

Em relação à VPN, atualmente não se sabe qual estratégia a MB utiliza em seu Portal MB porém caso não se tenha uma alternativa, uma estratégia que poderia mitigar o risco de operar com um sistema desatualizado ou sem suporte, mesmo que de forma reduzida, seria a adoção de uma VPN Open Source tendo como base de implementação o manual de boas práticas para o uso de VPN ISO/IEC 27033-5. Mesmo que exista e já esteja em operação uma VPN que atenda ao Portal MB quanto a comunicação por meio de uma WAN, em território nacional, uma outra utilização de VPN que poderia trazer bons resultados para a instituição

relaciona-se ao fornecimento seguro de acesso à internet sem a necessidade de acesso à rede interna da MB pelo usuário. Um exemplo típico seria o fornecimento de acesso à internet para alunos dos Centros de Instrução da MB através de uma solução VPN *open source*. Uma VPN pode ser utilizada nessas instituições para conexão da máquina pessoal dos alunos em uma DMZ dedicada ao acesso à internet. Assim, seria possível um acesso à *web* sem a necessidade de acesso aos recursos da rede interna. Isso promoveria maior segurança da instituição somado a um melhor aproveitamento de recursos oferecidos aos alunos além de difundir mais o uso de redes VPN nas Organizações Militares da MB.

5.2 Sugestões para futuros trabalhos

Este trabalho abordou algumas das tecnologias utilizadas nos mecanismos para assegurar uma comunicação segura. A intenção inicial era tentar obter informações sobre a infraestrutura de comunicação da MB para realizar uma pesquisa mais focada na infraestrutura existente. E em virtude de os sistemas de comunicação serem um recurso estratégico e de caráter sigiloso, não foi possível obter informações sobre especificidades das tecnologias empregadas pela Rede de Comunicações Integradas da Marinha (RECIM) com os órgãos responsáveis. Talvez, recursos mais aprimorados já sejam empregados na MB, reforçando as tecnologias de proteção para conexão segura do TLS e VPN e indicando que não seja necessário, a curto prazo, adotar soluções mais modernas. No entanto, mesmo não apresentando características dos sistemas empregados, o trabalho desenvolvido é de interesse da área de TI da MB. Ressalta-se a importância de mais oportunidades por parte dos órgãos responsáveis quanto ao fornecimento de informações sobre possíveis problemas enfrentados na atualidade a fim de que possam ser realizadas pesquisas com foco em soluções que auxiliem efetivamente na garantia de uma comunicação segura.

REFERÊNCIAS

ABÍLIO, A. K. *et al*. **Comunicação segura na internet: métodos, infraestrutura de chaves públicas e padrões.** Monografia (Especialização em Redes de Computadores) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

ACTIVEWEB. O fim do TLS 1.0 e 1.1. **ActiveWeb Segurança Digital**, São Paulo, 23 ago. 2019. Disponível em: https://www.rapidssl.com.br/blog/o-fim-do-tls-1-0-and-1-1/64. Acesso em: 18 fev. 2020.

ADRIAN, D. *et al*. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. *In*: CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 22., 2015, Denver. **Proceedings [...]**. Denver: ACM, 2015, p. 1-13. Disponível em: https://dl.acm.org/doi/10.1145/2810103.2813707. Acesso em: 17 fev. 2020.

ALVES FAGUNDES,. **Uma Implementação de VPN**. Fundação de Apoio à Escola Técnica do Estado do Rio de Janeiro. Petrópolis, p. 76. 2007.

ASTARO. **Astaro**. [*S. l.*]: Sophos Ltd., 2020. Disponível em: http://www.astaro.de/. Acesso em: 18 fev. 2020.

ANTONIO MOTA TRINTA, ; CAVALCANTI DE MACÊDO,. **Um Estudo sobre Criptografia e Assinatura Digital**. Universidade Federal de Pernambuco, 1998. Disponivel em: <https://www.cin.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 17 Abril 2020.

AVIRAM, N. *et al*. DROWN: Breaking TLS using SSLv2. *In*: USENIX SECURITY SYMPOSIUM, 25., 2016, Austin. **Proceedings [...]**. Berkele: USENIX, 2016, p. 689-706. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_aviram.pdf. Acesso em: 17 fev. 2020.

BHARGAVAN, K.; LEURENT, G. Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH. *In*: NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, 16., 2016, San Diego. **Proceedings [...]**. Reston: Internet Society, 2016, p. 1-17. Disponível em: https://www.ndss-symposium.org/wp-content/uploads/2017/09/transcript-collision-attacks-breaking-authentication-tls-ike-ssh.pdf. Acesso em: 17 fev. 2020.

BITTAU, A. *et al*. **Cryptographic protection of TCP Streams (tcpcrypt)**. [*S. l.*]: Tcpcrypt, 2014a. Disponível em: https://tools.ietf.org/html/draft-bittau-tcpinc-01#page-7. Acesso em: 24 jan. 2020.

BITTAU, A. *et al*. **Tcpcrypt - Encrypting the Internet**. [*S. l.*]: Tcpcrypt, 2014b. Disponível em: tcpcrypt.org/docs.php. Acesso em: 18 fev. 2020.

BRAGHETTO, L. F. B.; SILVA, S. C.; BARBOSA, A. M. **IPSec: Segurança de Redes – INF542**. 2003. Monografia (Especialização em Redes de Computadores) - Universidade Estadual de Campinas, Campinas, 2003.

BRASIL. **Medida provisória n. 2.200-2, de 24 de agosto de 2001**. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 25 dez. 2019.

CABRAL, J. L. M.; LEITE, L. M. **Segurança em Transações e Aplicações WAP (7)**. [*S. l.*]: WirelessBR, 2003. Disponível em: http://www.wirelessbrasil.org/wirelessbr/colaboradores/cabral_leite/seg_wap_07.html. Acesso em: 26 dez. 2019.

CAMPINHOS, E. C.; BARCELLOS, R. L. S. **Topologia de VPN: otimizando eficiência e segurança**. 2007. Monografia (Especialização em Segurança de Redes de Computadores) - Faculdade Salesiana de Vitória, Vitória, 2007.

CHECK POINT. **Check Point Remote Access Solutions**. [*S. l.*]: Check Point, 2020a. Disponível em: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk67820. Acesso em: 18 fev. 2020.

CHECK POINT. **Customer Stories**. [*S. l.*]: Check Point, 2020b. Disponível em: https://www.checkpoint.com/customer-stories/. Acesso em: 18 fev. 2020.

CHECK POINT. **Check Point Software Technologies Ltd**. [*S. l.*]: Check Point, 2020c. Disponível em: https://www.checkpoint.com/products/remote-access-vpn/. Acesso em: 18 fev. 2020.

CISCO. **Cisco AnyConnect: Ordering Guide**. San Jose: CISCO, 2017. Disponível em: https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf. Acesso em: 18 fev. 2020.

CISCO. **Customer Stories - Full listing**. San Jose: CISCO, 2020a. Disponível em: https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/customer-stories-listing.html. Acesso em: 18 fev. 2020.

CISCO. **Clientes de segurança de VPN e de endpoints**. San Jose: CISCO, 2020b. Disponível em: https://www.cisco.com/c/pt_br/products/security/anyconnect-secure-mobility-client/index.html. Acesso em: 18 fev. 2020.

CISCO. **SSL VPN Security**. San Jose: CISCO, 2014. Disponível em: https://tools.cisco.com/security/center/resources/ssl_vpn_security. Acesso em: 08 jan. 2020.

CYBEROAM. **Cyberoam: Securing you**. [*S. l.*]: Sophos Technologies, 2020. Disponível em: http://www.cyberoam.com/. Acesso em: 18 fev. 2020.

EMGEPRON. **Edital de Licitação 052/2017: Pregão Eletrônico**, 2017. Disponível em: https://www1.emgepron.mar.mil.br/licitacao/login_cliente.php. Acesso em:18 fev 2020.

F5 NETWORKS**. Access Policy Manager**. Seattle: F5 Networks Inc., 2020a. Disponível em: https://www.f5.com/products/security/access-policy-manager. Acesso em: 18 fev. 2020.

F5 NETWORKS. **48 of Fortune 50 companies are F5 customers**. Seattle: F5 Networks Inc., 2020b. Disponível em: https://www.f5.com/customer-stories. Acesso em: 18 fev. 2020.

F5 NETWORKS. **Big-Ip Access Policy Manager**. Seattle: F5 Networks Inc., 2020c. Disponível em: https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf. Acesso em: 18 fev. 2020.

FERNANDES DE MORAES,. **Redes Sem Fio**. 1ª. ed. São Paulo: Érica, 2010.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. Tradução de Ariovaldo Griesi. 4. ed. Porto Alegre: AMGH, 2007.

FORTINET. **Fortinet**. Union City: Fortinet Inc., 2000. Disponível em: https://www.fortinet.com. Acesso em: 8 fev. 2020.

FORTINET. **Fortinet: Clientes**. Sunnyvale: Fortinet Inc., 2020. Disponível em: https://www.fortinet.com/br/customers.html. Acesso em: 18 fev. 2020.

FRANKEL, et al. **Guide to SSL VPN**, 2008. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf. Acesso em 18 fev 2019.

FREITAS JUNIOR, V. *et al*. **Tecnologia e Redes de Computadores: Estudos aplicados**. Sombrio: Instituto Federal Catarinense, 2015.

GATLAN, S. PoCs for Windows CryptoAPI Bug Are Out, Show Real-Life Exploit Risks. **Bleeping Computer**, Nova York, 16 jan. 2020. Disponível em: https://www.bleepingcomputer.com/news/security/pocs-for-windows-cryptoapi-bug-are-out-show-real-life-exploit-risks/. Acesso em: 18 jan. 2020.

GILMORE, J. *et al*. **FreeS/WAN Download**. [*S. l.*]: FreeS/WAN, 2004. Disponível em: https://www.freeswan.org/download.html. Acesso em: 25 nov. 2019.

GUIMARÃES, A. A. G. **Proposta de um modelo de segurança para VPN na interligação de redes corporativas**. 2004. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal de Pernambuco, Recife, 2004.

HOUSLEY, R. *et al*. **Internet Engineering Task Force RFC 8423**. [*S. l.*]: IETF Tools, 2018. Disponível em: https://tools.ietf.org/html/rfc8423. Acesso em: 16 fev. 2020.

HP. **HP Development Company**. [*S. l.*]: HP, 2020. Disponível em: https://www8.hp.com/br/pt/home.html. Acesso em 18 fev. 2020.

IETF. IETF Tools. **Internet Engineering Task Force RFC 6101**, 2011. Disponível em: <https://tools.ietf.org/html/rfc6101>. Acesso em: 17 Abril 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27033-5: Securing communications across networks using Virtual Private Networks (VPN)**. Geneva: ISO/IEC, 2013.

JANSSEN, D. **Is it legal to use a VPN?** Nijmegen: VPNoverview, 2019. Disponível em: https://vpnoverview.com/vpn-information/is-vpn-legal/. Acesso em: 28 jan. 2020.

LIBRESWAN. **The Libreswan Project**. [*S. l.*]: Libreswan, 2019. Disponível em: https://libreswan.org/wiki/. Acesso em: 27 jan. 2020.

MARINHA DO BRASIL. **Site da Marinha do Brasil**. Brasília: Ministério da Defesa, 2019a. Disponível em: www.marinha.mil.br. Acesso em: 27 dez. 2019.

MARINHA DO BRASIL. **DGMM-0540: Normas de Tecnologia da Informação da Marinha**. 3. rev. Rio de Janeiro: Diretoria-Geral do Material da Marinha, 2019b.

MARINHA DO BRASIL. **Portal de Serviços da Marinha do Brasil**. Rio de Janeiro: Centro de Tecnologia da Informação da Marinha do Brasil, 2020.

MÖLLER, B.; DUONG, T; KOTOWICZ, K. **This POODLE Bites: Exploiting the SSL 3.0 Fallback**. [*S. l.*]: OpenSSL, 2014. Disponível em: https://www.openssl.org/~bodo/ssl-poodle.pdf. Acesso em: 5 nov. 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **CVE-2020-0601 Detail**. Gaithersburg: NIST, 2020. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2020-0601. Acesso em: 18 jan. 2020.

NOBORI, D. *et al.* **SoftEther VPN Project**. [*S. l.*]: SoftEther, 2013. Disponível em: https://www.softether.org/. Acesso em: 26 dez. 2019.

OPENVPN. **OpenVPN: Community Downloads.** Pleasanton: OpenVPN Inc., 2020. Disponível em: https://openvpn.net/community-downloads/. Acesso em: 18 fev. 2020.

OPENVPN. **Why SSL VPN**. Pleasanton: OpenVPN Inc, 2010. Disponível em: https://openvpn.net/faq/why-ssl-vpn/. Acesso em: 18 Abril 18.

OPENVPN. **Overview of changes in 2.4** [*S. l.*]: GitHub, 2019. Disponível em: https://github.com/OpenVPN/openvpn/blob/release/2.4/Changes.rst. Acesso em: 24 jan. 2020.

PACKT PUBLISHING. **Packt: Programming Books, eBooks & Videos for Developers**. [*S. l.*]: Packt Publishing, 2020. Disponível em: https://www.packtpub.com/. Acesso em: 18 fev. 2020.

PIROCLASTO. **[Ajuda do Pessoal de TI] VPNs empregadas por grandes corporações**. Fórum Outerspace, seção PC, Hardware & Gadgets - Discussão geral. Disponível em: https://forum.outerspace.com.br/index.php?threads/ajuda-do-pessoal-de-ti-vpns-empregadas-por-grandes-corpora%C3%A7%C3%B5es.556984/#post-17511127. Acesso em 18 Abr 2020.

PROVÉRBIOS. *In*: **BÍBLIA SAGRADA: Nova Tradução na Linguagem de Hoje**. Barueri: Sociedade Bíblica do Brasil, 2014.

QUALYS. **SSL Pulse**. Foster City: Qualys, 2019. Disponível em: https://www.ssllabs.com/ssl-pulse/. Acesso em: 18 fev. 2020.

QUALYS. **SSL Server Test**. Foster City: Qualys, 2009. Disponível em: https://www.ssllabs.com/ssltest/index.html. Acesso em: 27 dez. 2019.

REDHAT. **RedHat: We create better technology the open source way**. Raleigh: RedHat, 2020. Disponível em: http://www.redhat.com/. Acesso em: 18 fev. 2020.

SONG,. SSL VPN Security. **CISCO**, 2005. Disponivel em: https://tools.cisco.com/security/center/resources/ssl_vpn_security. Acesso em: 18 Abril 2020

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson, 2015.

STEFFEN, A. **strongSwan Project**. [*S. l.*]: strongSwan, 2018a. Disponível em: https://www.strongswan.org/. Acesso em: 26 dez. 2019.

STEFFEN, A. **IKEv1 Cipher Suites**. [*S. l.*]: strongSwan, 2018b. Disponível em: https://wiki.strongswan.org/projects/strongswan/wiki/IKEv1CipherSuites. Acesso em: 24 jan. 2020.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

TIMMERMANS, I.; SLIEPEN, G. **Tinc Manual**. [*S. l.*]: Tinc, 2015. Disponível em: http://www.tinc-vpn.org/documentation/. Acesso em: 24 jan. 2020.

WEBCONFS. **Web Tools: Online MD5 Generator**. [*S. l.*]: Webconfs, 2018. Disponível em: https://www.webconfs.com/online-md5-generator.php. Acesso em: 29 dez. 2020.

XELERANCE CORPORATION. **Openswan.** [*S. l.*]: Xelerance Corp., 2016. Disponível em: https://www.openswan.org/. Acesso em: 25 nov. 2019.

XELERANCE CORPORATION. **Xelerance: Services**. [*S. l.*]: Xelerance Corp., 2020. Disponível em: https://www.xelerance.com/. Acesso em: 18 fev. 2019.

APÊNDICE

APÊNDICE A – Pesquisa sobre comunicação segura

Durante a elaboração deste trabalho, foi pensado na elaboração de um questionário a ser realizado com militares da Marinha do Brasil a respeito da tecnologia TLS e VPN. O objetivo do teste seria avaliar como os militares da MB utilizam as ferramentas para garantir a uma conexão segura em uma rede de computadores (não necessariamente a rede de computadores institucional). As perguntas foram elaboradas levando em conta aspectos práticos do uso cotidiano dessas duas tecnologias que não são percebidas facilmente por usuários comuns. Em virtude da quantidade de testes a serem feitos serem grandes e a dificuldade de difundi-los, a pesquisa não pode ser realizada, porém permanece como uma proposta para futuros trabalhos.

1- Normalmente quando acessa algum site na internet (compras, redes sociais, instituições bancárias e etc) você verifica se a URL se inicia com a sintaxe http ou https?

- **Sim**
- **Não**

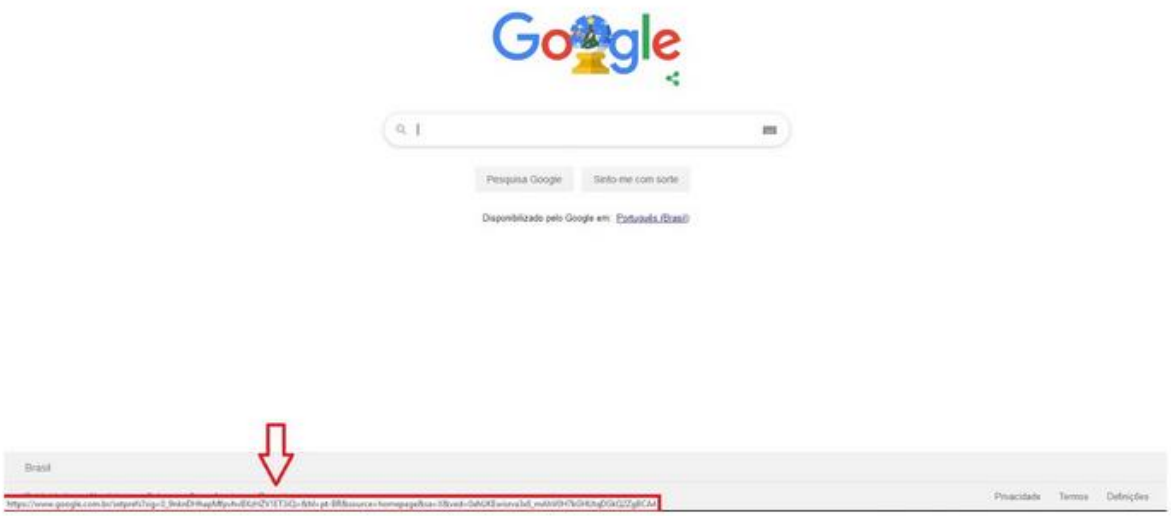
2- Em seu dispositivo móvel de uso pessoal (tablets e smartphones) você utiliza algum antivírus?

- **Sim**
- **Não**

3- Quando navegando na Internet você já se deparou com a seguinte mensagem "Esta conexão não é confiável" (exemplo da figura abaixo)? Caso afirmativo, normalmente qual a sua ação?

- **Saio imediatamente do site.**
- **Entendo os riscos e clico no botão "Adicionar exceção".**
- **Nunca presenciei essa mensagem enquanto estou navegando.**

4- Normalmente antes de acessar algum link em algum site/e-mail você verifica antes se a URL pertence a um site a qual o link se refere? (normalmente quando se posiciona o indicador do mouse sobre o link, o navegador mostra a URL na parte inferior no navegador como marcado de vermelho na figura abaixo)



- **Sim**
- **Não**

5- Caso utilize algum programa de recurso criptológico para assinar documentos digitalmente (uso pessoal ou institucional a exemplo do Orion) você mantém a cópia ou backup do arquivo de sua chave secreta em local em que somente você tenha acesso?

- **Sim**
- **Não**
- **Não possuo backup de minha chave secreta**
- **Não utilizo programa de recurso criptológico para assinar documentos**

6- Você possui alguma assinatura de rede virtual privada (VPN) quando utiliza uma rede WI-FI pública (restaurante, aeroporto, hotel e etc) para garantir acesso seguro às suas informações?

- **Sim**
- **Não**
- **Desconheço o que seja serviço de VPN**

APÊNDICE B – Esclarecimento sobre soluções VPN

Entrevistado: 1º Ten Augusto César da Fonseca dos Santos (CTIM)
Data: 4 de fevereiro de 2020, 19:20
Meio: Mensagem Eletrônica

P. Quais as soluções VPN que normalmente são utilizadas por empresas e existe alguma VPN mais moderna no que diz respeito ao estado da arte?
R. A Grande Maioria das organizações, além da Marinha, utilizam VPN IPsec de modo túnel, criptografia simétrica com troca de chave *Diffie Hellman*.