UNIVERSIDADE POLITÉCNICA

A POLITÉCNICA

Instituto Superior de Gestão, Ciências e Tecnologia

ÁREA DE FORMAÇÃO:

Licenciatura em Engenharia Informática e Telecomunicações

(Trabalho de Fim de Curso)

TEMA:

SEGURANÇA DE DADOS BASEADOS NO PROTOCOLO SECURE SOCKET LAYER (SSL), NAS REDES DEFINIDAS POR SOFTWARE (SDN)

(REDES DO GRUPO IPS)

Ivo Sancho Quipiço

Maputo, Março de 2021

UNIVERSIDADE POLITÉCNICA

A POLITÉCNICA

Instituto Superior de Gestão, Ciências e Tecnologia

ÁREA DE FORMAÇÃO:

Licenciatura em Engenharia Informática e Telecomunicações

(Trabalho de Fim de Curso)

TEMA:

SEGURANÇA DE DADOS BASEADOS NO PROTOCOLO SECURE SOCKET LAYER (SSL), NAS REDES DEFINIDAS POR SOFTWARE (SDN)

(REDES DO GRUPO IPS)

Ivo Sancho Quipiço

Monografia apresentada à Universidade Politécnica para obtenção do grau de Licenciatura em Engenharia Informática e de Telecomunicações, sob a orientação do Mestre:

Arlindo Mondlane

Maputo, Março de 2021

Monografia apresentada à Universidade Politécnica como parte dos requisitos para obtenção do grau de Licenciatura em Engenharia Informática e de Telecomunicações.

Nome do Autor: Ivo Sancho Quipiço

Nome do Supervisor/Orientador: Arlindo Mondlane

Título da Monografia: Segurança de Dados Baseados no Protocolo Secure Socket Layer (SSL), nas Redes Definidas por Softaware (SDN).

Parecer do Supervisor

1- Introdução

O candidato desenvolveu um trabalho cujo objectivo foi Projectar mecanismos de segurança de modo a colmatar a vulnerabilidade da rede SDN a ataques externos, implementando o protocolo *Secure Socket Layer* (SSL), tendo como caso do estudo as redes do grupo IPS.

2- Execução do trabalho

A execução do trabalho compreendeu três etapas, sendo a primeira inteiramente ao estudo teórico do assunto, fazendo pesquisas sobre o tema através da busca de informações em livros, artigos, pela *Internet* e através de entrevistas informais aos profissionais da área.

Na segunda etapa, o candidato centrou suas actividades nas entrevistas ao pessoal da área de informática do IST (Serviços e Tecnologias, Lda), como por exemplo: Dr. Rony, Dr. Stélio, etc. A procura de soluções relacionadas com o tema e concepção mecanismos de protecção adequada às de rede da instituição.

A terceira compreendeu a elaboração e organização do relatório final do trabalho, de acordo com o regulamento de orientação do trabalho do final do curso em vigor na Universidade Politécnica.

3- Estrutura do Relatório

O relatório elaborado divide-se em três partes:

Na primeira parte o candidato apresenta o índice geral, os agradecimentos, a dedicatória, a declaração de honra, o índice de tabelas, o índice de figuras, a lista de abreviaturas e o resumo do trabalho realizado.

Na segunda parte o candidato faz a introdução do tema, formulação do problema, apresentação dos objectivos gerais e específicos do trabalho a desenvolver, método de execução do trabalho, e ainda definições gerais de alguns conceitos de segurança de redes. Isto compõe o capítulo 1.

No capítulo 2 apresenta aspectos teóricos do tema em estudo, proporcionando uma compreensão geral sobre redes de dados e sua segurança, seu planeamento e operacionalização nas organizações.

No capítulo 3 faz uma apresentação do grupo IPS, sua estrutura de recursos bem como o seu estado actual no que concerne à rede de dados.

O quarto capítulo é reservado a da metodologia de solução do problema e apresentação dos resultados. É aqui que se apresenta a descrição da situação actual da segurança da rede, propõe as alterações necessárias para se obter a uma segurança baseada em SSL sobre as redes SDN, apresentado suas respectivas vantagens e os ganhos que a instituição poderá obter.

Finalmente, no último capítulo é apresentada a conclusão do trabalho, contribuições e sugestões para trabalhos futuros.

Na terceira e última parte do relatório, o candidato apresenta as referências bibliográficas e a bibliografia.

4- Conteúdo do Trabalho

O candidato desenvolveu um trabalho investigativo aceitável, no que diz respeito às redes de dados e sua respectiva segurança, sua inserção nas organizações. Isso lhe permitiu tirar conclusões concretas sobre a necessidade de implementar Sistemas de segurança de rede que respondem às reais necessidades das organizações em termos de prestação de serviços e eficiência das suas operações.

O relativo zelo na escrita e linguagem evidenciados no relatório são o reflexo da capacidade de análise, autonomia e sentido de entrega do candidato durante a execução de trabalho. Ainda assim, o trabalho não está livre de algumas imperfeições que, a meu ver, não lhe retiram o mérito.

5- Conclusão

Face às constatações acima referidas, proponho que o trabalho seja aprovado e que ao candidato lhe seja dado a oportunidade para a sua defesa.

Maputo, 19 de Março de 2021

_____

Arlindo Mondlane

DECLARAÇÃO DE HONRA

Eu, Ivo Sancho Quipiço, declaro por minha honra, que o presente trabalho é resultado da minha própria investigação e das orientações do meu supervisor, e que esta é a primeira vez que submeto para obter um grau académico nesta instituição – Licenciatura em Engenharia Informática e de Telecomunicações, da Universidade Politécnica.

Autor

_____

(Ivo Sancho Quipiço)

Aprovação do Júri

A presente Monografia julgada adequada para a obtenção do grau de Licenciatura em Engenharia Informática e de Telecomunicações, aprovada em forma final pelo Departamento de Engenharias.

_____

(Supervisor)

_____

(Arguente)

_____

(Presidente)

Dedicatória

Dedico este trabalho a mim, a minha mãe e a Deus!

Agradecimentos

Em primeiro lugar quero agradecer a **Deus** por ter-me concedido todas as forças e condições necessárias para que pudesse concluir o curso de Engenharia Informática e de Telecomunicações e este trabalho, também agradecer a Ele pelo seu amor incondicional, pelos momentos bons e maus e por tudo o que Ele tem feito em minha vida (**I Tessalonicenses 5:18**).

A minha **Mãe** que tudo fez para que eu pudesse concluir o curso com êxito com o apoio de **Deus** (**Colossenses 3:21**).

Ao Engº._MSc **Arlindo Mondlane** por ter aceite supervisionar-me neste trabalho, pela paciência que teve comigo durante a elaboração do trabalho e pela sua contribuição na concretização deste trabalho. Também à todos os docentes do curso de Engenharia Informática e de Telecomunicações pelo ensinamento proporcionado.

À minha **Família** e aos meus **Amigos** que de forma directa ou indirecta estiveram comigo nesta longa e difícil jornada, apoiando-me de forma incondicional em todos os momentos.

Aos meus colegas de turma, pelo imenso apoio proporcionado e por partilharem os seus conhecimentos comigo.

ÍNDICE

LISTA DE FIGURAS

LISTA DE GRAFICOS

LISTA DE SIGLAS E ACRÓNIMOS

SSL	Secure Socket Layer
TCP	Transport Control Protocol
SDN	Software Defined Network
HTTP	Hypertext Transfer Protocol
WWW	World Wide Web
HTTPs	Hypertext Transfer Protocol Secure
TLS	Transport Layer Security
VNF	Virtualized Network Functions
FIFO	First in First out
IPS	Instituto Superios Politécnico
IRC	Internet Relay Chat
UDP	User Datagram Protocol
IP	Internet Protocol
ICMP	Internet Control Message Protocol
P2P	Peer-to-Peer
DNS	Domain Name System
DMZ	Demilitarized zone
DSL	Digital Subscriber Line
WAP	Wi-Fi Protected Access

RESUMO

O uso de tecnologias actualmente tem facilitado várias áreas de conhecimento, tais como Medicina, Física, Química, Engenharia, entre outros campos de saber, mas o uso das tecnologias em si, pode constituir um grande peso para a economia em Moçambique, uma vez que para implantação de mesma requer-se fundos avultados para o desenvolvimento destes sistemas.

O presente trabalho tem como objectivo analisar o nível da vulnerabilidade na rede do Instituto Superior Politécnico. Tendo em conta que é uma rede centralizada a ameaça a este tipo de rede é relativamente maior. Com isso há uma necessidade de implementar mecanismos de segurança de modo a colmatar essa vulnerabilidade.

Embora as redes definidas por software sejam ideais para alta largura de banda e para a natureza dinâmica dos aplicativos atuais, o que permite ter uma rede mais flexíveis e eficientes. A falta de segurança na rede pode significar um grande problema visto que em caso de invasão toda a rede poderá ser comprometida. No presente trabalho foi feito um estudo sobre a segurança dos dados na rede do Instituto Superior Politécnico, e concluiu-se que o protocolo SSL poderá ser a solução mais viável para combater a deficiência da segurança na rede.

Palavras-chave: Redes**,** Software**,** SSL**,** SDN e Segurança.

ABSTRACT

The use of technologies has currently facilitated several areas of knowledge, such as Medicine, Physics, Chemistry, Engineering, among other fields of knowing, but the use of technologies themselves, can be a major burden for the economy in Mozambique, since for its implementation, large funds are required to complete the system.

The present work aims to analyze the level of vulnerability in the Polytechnic Higher Institute, Bearing in mind that is a centralized network and the threat to the network is relatively larger. Thus, there is a need to implement security mechanisms in order to address the vulnerability.

Although software-defined networks are ideal for high bandwidth and the dynamic nature of today's applications, which allows for a more flexible and efficient network. The lack of security on the network can mean a big problem since in case of invasion the entire network can be compromised. In the present work, a study was done on data security in Polytechnic Higher Institute, and it was concluded that the SSL protocol may be the most viable solution to combat the deficiency of network security.

Key words: Networking, Software, SSL, SDN and Security.

CAPÍTULO I

1. INTRODUÇÃO

Há algum tempo observa-se o surgimento da necessidade de maior abertura e flexibilidade dos equipamentos de rede, especialmente com o propósito de pesquisa e inovação. Os roteadores atuais implementam uma arquitectura composta por uma camada de software fechada, que é executada em um hardware proprietário. Esse modelo resulta em soluções de alto custo, dificulta a inserção de novas funcionalidades e inviabiliza a experimentação de novas ideias. Com o avanço da padronização do protocolo *openflow* para programar a rede para o encaminhamento dos pacotes, o conceito de redes programáveis por software traz um novo paradigma de inovação cujo potencial disruptivo assemelha-se ao da introdução de sistemas operacionais em computadores e, mais recentemente, em dispositivos móveis.

Serviços de computação em nuvem relacionados à infra-estrutura vêm se tornando cada vez mais importantes. Nessa linha de negócio, a virtualização garante uma forma de oferecer flexibilidade, isolamento e funcionalidades extras. A tecnologia abriu espaço para o *cloud computing* (modelo de computação em nuvem) em *datacenters*, onde o cliente não só poderia alugar uma máquina virtual como uma rede local inteira de máquinas virtuais dentro da infra-estrutura do provedor (Nunes, 2012).

Apesar das soluções de virtualização oferecerem boas soluções para o isolamento de recursos como CPU e memória, esse modelo de negócio requer soluções para o isolamento do tráfego de rede de cada cliente, são caras e pouco escaláveis (Capacidade de um sistema conseguir se adaptar para entregar um produto de igual qualidade a um número maior ou menor de clientes), na actualidade, como uso de *VLANs*. Alguns académicos recentemente têm focado bastante no conceito de redes definidas por software (*SDNs*) por conta do padrão *openflow* (Nunes, 2012).

Esta nova abordagem permite organizar a rede de uma forma bem mais flexível, com uma visão global e centralizada da rede. Permite implementar uma visão de rede virtual para cada cliente de um serviço de computação em nuvem multi-inquilino sem a utilização de hardware

especializado. Ele usa o sistema operacional para redes *POX* (traz uma interface mais moderna e uma implementação mais elegante, além de oferecer melhor desempenho) em conjunto com o gerenciador de computação em nuvem *openstack* que controla máquinas com monitores de máquinas virtuais *Xen*. Essas máquinas são conectadas por switches virtuais *opens vSwitch* que utilizam o protocolo *openflow.*

Como a rede é toda desenvolvida em cima de protocolos públicos, ou seja, abertos "*open source*", é necessário que se tenha um canal para que possa trocar de forma segura informações entre o "*switch*" e o controlador, sem que sofra ataque de elementos mal-intencionados. A interface de acesso recomendada é o protocolo *Secure Socket Layer* (SSL). Interfaces alternativas (passivas ou activas) incluindo-se o TCP são essenciais em ambientes virtuais e experimentais pela facilidade de utilização, pois não necessitam de chaves criptográficas (Diego Duque, 2012).

Segundo Lins (2015), As Potenciais vulnerabilidades de segurança existem em toda a plataforma SDN. Além disso, com a introdução no SDN de interfaces abertas e protocolos conhecidos para simplificar a programação de rede por qualquer provedor de aplicação, a porta fica escancarada para os atacantes. Com o conhecimento total de como controlar a rede, com acesso para o controlador, o funcionamento da rede pode ser rápida e facilmente ser aproveitado para o benefício do atacante. Mesmo em um nível inferior, nós individuais da rede, *hosts* ou os usuários podem ser direccionados, minando o desempenho da rede desejada. Tais questões devem receber a devida atenção no design da plataforma SDN.

No entanto, a segurança na rede SDN deve ser tão boa se uma política de segurança à altura for definida. Implementação de mecanismos de autenticação e autorização existentes podem resolver alguns aspectos do desafio de segurança. Enquanto isso, técnicas de detecção e protecção contra ameaças continuarão a evoluir. A chave, porém, é para organizações individuais, que de forma eficaz e abrangente devem definir seus mecanismos de proteção, a fim de explorar toda a extensão disponível de protecção da rede.

1.1. Objectivos da Investigação

1.1.1. Geral:

- Impementar mecanismos de segurança de modo a colmatar a vulnerabilidade da rede SDN (Instituto Superior Politécnico) a ataques externos, implementando o protocolo *Secure Socket Layer* (SSL).

1.1.2. Específicos:

- Analisar o nível de ataques a rede as redes definidas por software;
- Apontar mecanismos para reduzir a vulnerabilidade da rede do IPS;
- Solucionar os pontos fracos na rede do Instituto Superior Politécnico;
- Descrever a importância, vantagens e desvantagens do protocolo SSL.

1.2 Problema de Pesquisa

A segurança da informação é um assunto que a cada dia se torna mais relevante para arquitectos e engenheiros de redes de dados. No momento da sua concepção, as redes de dados tinham um objectivo puramente académico, com poucos e conhecidos usuários, onde era possível confiar no meio utilizado para trafegar os dados e nos seus pares. A utilização massiva e amplamente interligada para a qual estas redes evoluíram abriram não só um imenso leque de possibilidades de crescimento e acesso à informação, mas também, com ele, a preocupação com a integridade dos sistemas e a privacidade de dados.

Redes de dados, sejam elas privadas ou públicas, estão a todo o momento vulneráveis à ataques de usuários ou sistemas mal-intencionados em busca de informações que possam ser trocadas ou vendidas. Prover a segurança destes ambientes é tão importante que se tornou não só um campo de pesquisa, mas também um nicho de mercado altamente aquecido. Para quantificar esta ideia, no relatório da Symantec, realizado no ano de 2015, utilizando dados do ano anterior, estão descritos diversos tipos de ataques que se valem de falhas nas muitas plataformas que actualmente podem ser interconectadas através de uma rede de dados. Como exemplo do ambiente hostil que estes sistemas estão expostos, há o número de 496,657 ataques a sites por dia na Internet (Fernandes,2016).

Com a mudança de paradigma trazida pela implementação de uma rede de dados definida por software (SDN - Software Defined Networking), novas possibilidades surgem para a gerência e o controle da rede. Na SDN, existe uma separação física entre o plano de dados e o plano de controle da rede, ou seja, acontece uma migração da inteligência que hoje existe em cada elemento da rede para um ou mais controladores. Assim, com esse novo paradigma de rede, busca-se diminuir a curva de aprendizagem e o tempo desprendido para manutenção e reconfiguração de elementos, podendo também, trazer boas práticas e todo conhecimento acumulado no desenvolvimento de *software* para a administração de redes de dados.

No entanto, com a introdução de novos elementos no ambiente das redes de dados, tem-se uma mudança brusca na arquitectura que se tem actualmente, gerando novas preocupações de segurança que se somam às preocupações já existentes. Como era de se esperar, as soluções

aplicadas na estrutura actual não são completamente aderentes ao novo modelo proposto pela SDN e precisam ser remodeladas e avaliadas (Fernandes,2016).

Como a rede foi toda desenvolvida em cima de protocolos públicos, a falta de segurança ou a implementação de um protocolo de segurança fraco na rede do IPS pode trazer danos maiores, pois em caso de invasão por pessoas mal-intencionadas a rede toda pode ficar comprometida. É necessário ter um canal seguro para a troca de informações, e a interface de acesso recomendada é o protocolo Secure Socket Layer (SSL).

Em função do problema colocado, a pesquisa pretende responder as seguintes questões:

- De que maneira o protocolo Secure Socket Layer (SSL), pode garantir melhor segurança na rede do Instituto Superior Politécnico, em relação aos protocolos usados atualmente(WAP e IPsec)?
- Será que com a implementação do protocolo de segurança SSL na rede do Instituto Superior Politécnico, se pode ter melhorias na segurança de dados?

1.3. Hipóteses

Deste modo as hipóteses investigadas poderão ser formuladas da seguinte forma:

H (0): A falta de um forte protocolo de segurança na rede do IPS, poderia ter um impacto negativo no desempenho das infraestruturas e nas actividades dos colaboradores do grupo IPS.

H (1): Com a implementação do protocolo SSL na rede do IPS, poderia ter um impacto positivo no desempenho das infraestruturas e nas actividades dos colaboradores do grupo IPS.

H (2): Com a implementação do protocolo SSL na rede do IPS, permitir-se-á a troca de informações de forma mais segura.

1.4. Justificativa

A inserção de novas tecnologias que dependam de alterações do *hardware* a ser utilizado, inviabiliza ainda mais o desenvolvimento de novas tecnologias e protocolos de segurança para as redes definidas por software. A quantidade e variedade de aplicações de rede que podem ser desenvolvidas com rapidez e maior facilidade por meio das APIs e linguagens de programação é um dos argumentos mais fortes para a adoção de uma SDN (Campos et al, 2015).

Um dos grandes problemas das redes atuais e que é resolvido pelas redes definidas por software é: as atuais redes são integradas verticalmente, isto é, **os planos de controle e de dados são agrupados** enquanto a grande promessa das redes definidas por software (**SDN**) é **quebrar essa integração vertical**, separando a lógica de controle da rede dos roteadores e comutadores subjacentes, promovendo a centralização da lógica de controle da rede. Ao separar o problema de controle da rede em pedaços menores e mais fáceis de serem resolvidos, essa rede se torna extremamente flexível, fácil de ser gerenciada e facilita na criação e introdução de abstrações no contexto de redes de computadores. Além disso, estas redes introduzem uma habilidade essencial para contornar alguns dos problemas descritos acima das redes atuais: elas são programáveis. Dessa forma, novas tecnologias podem ser implementadas na rede de forma gradual, o que hoje é inviável (Campos et al, 2015).

A segurança de uma rede de computadores é um dos pilares responsáveis por gerar um ambiente propício a sua utilização. Ao longo dos anos, com o surgimento de ataques com propósitos diversos, também houve o aperfeiçoamento dos mecanismos de prevenção. Dentre estes mecanismos, podemos citar *firewalls*, que eram constituídos por um *hardware* especializado, cujo objetivo era funcionar como filtro, selecionando o que estaria permitido passar por ele e o que deveria ser retido. Este componente pode ser utilizado tanto para prevenir que informações sigilosas, por exemplo, sejam enviadas para redes externas quanto para impedir que arquivos maliciosos entrem na rede interna (Gomes et al, 2015).

Contudo, estes componentes, como relatados anteriormente, eram formados por *hardware* especializado, gerando a necessidade de desenvolver *hardware*s dedicados para desempenhar funções específicas, o que acarretava custos com equipes de desenvolvimento, além de grande incompatibilidade entre os produtos oferecidos por diferentes fornecedores.

Imagine então se fosse possível, a partir da utilização de um *hardware* genérico, simplesmente instalar estas aplicações de segurança como se fossem um programa que uma pessoa comum pode instalar em seu computador. As SDNs permitem que isto seja feito por meio da utilização de APIs como o *OpenFlow* para definição de quais aplicações devem ser instaladas nos comutadores desejados (Gomes et al, 2015).

Todavia, apesar dos benefícios gerados pelas SDNs, diversos desafios de segurança surgiram devido à presença de um controlador centralizado.

1.5. Delimitação do trabalho

O presente trabalho de investigação tem como objectivo, implementar um protocolo de segurança dentro da rede definida por software (Rede do IPS) e garantir que possa existir uma comunicação segura entre o *switch* e o controlador na transmissão de dados.

- Foi definido no período de estudo que compreende entre 2002 e 2021 por razões de acesso a informação para as diferentes variáveis utilizadas.
- A análise terá em consideração o nível de tamanho da rede local do ISP.

1.6. Estrutura do Trabalho

O trabalho comporta mais (...) capítulos, nomeadamente:

O PRIMEIRO CAPÍTULO

INTRODUÇÃO, tratará do processo de investigação, incluindo a formulação do problema e da pergunta a investigar, as hipóteses a considerar, delimitações, seguindo dos objectivos da investigação e sua importância, apresenta-se o calendário para a elaboração da monografia finalmente a bibliografia.

O SEGUNDO CAPÍTULO

CONCEPTUALIZAÇÃO, descreverá os resultados da revisão bibliográfica e caracterização da segurança das redes informáticas dentro das organizações, bem como a sua relevância para a sua implementação e a CONTEXTUALIZAÇÃO.

O TERCEIRO CAPÍTULO

METODOLOGIA. Descreverá os paradigmas de investigação e as metodologias utilizadas e IMPACTO DA IMPLEMENTAÇÃO, fará uma abordagem sobre as variáveis consideradas medidas para o sucesso da mesma.

O QUARTO CAPÍTULO

ANÁLISE E INTERPRETAÇÃO DAS VARIÁVEIS, será dedicado a análise de dados recolhidos.

NO QUINTO CAPÍTULO

CONCLUSÕES e RECOMENDAÇÕES, serão apresentadas as conclusões, e tecerá as recomendações que possam parecer pertinentes e apropriadas.

CAPÍTULO II

2. REVISÃO LITERÁRIA

Com o intuito de facilitar a compreensão do presente trabalho, apresenta-se alguns conceitos que estão especialmente ligados com a análise dos factos inerentes ao mesmo. Contudo os mesmos conceitos não devem ser assumidos de forma acabada ou isolada, pois a sua apresentação e explicação foram estruturadas com relação à sua relevância e enquadramento específico para o presente trabalho, reflectindo a percepção dos mesmos.

Segundo Hinden (2014) - Antes de as empresas adotarem redes definidas por software, ou SDNs (Software Defined Networks), devem considerar os riscos de segurança inerentes, o especialista da Check Point, Robert Hinden disse durante a RSA Conference (Centralizar o controle da rede em um só servidor pode criar vulnerabilidades estratégicas com resultados devastadores, no ano de 2014), este veterano do setor colocou uma questão: depois de implantar o controle centralizado da rede em um servidor, o que acontece se esse servidor é atacado? E se um *hacker* assumir o controle de um controlador de SDN?

Teoricamente, o *hacker* poderia direcionar o tráfego evitando *firewalls*, inserir *malware* na rede, e executar ataques de interceptação ou "man-in -the-middle". Pode também enviar tráfego para nós comprometidos da rede.

Os dispositivos físicos de leem os cabeçalhos dos pacotes e usam tabelas de routing para enviá-los a determinado ponto. Mas o SDN é baseado em fluxos, o que é bom, pois permitem aos gestores de rede criarem políticas mais refinadas Por outro lado , todas as entradas de fluxo devem ser enviadas para todos os dispositivos na rede. Hinden teme que isso poderá ser demasiado complexo para gerir.

No entanto, Hinden aponta vários pontos positivos na segurança das SDNs. O controlador pode, por exemplo, disseminar as políticas de segurança para todos os *routers* e *switches* na rede, criando uma política uniforme de segurança SDN para todo o tráfego.

Além disso, se houver um dispositivo anfitrião comprometido, por exemplo, o controlador também pode facilmente isolar esse anfitrião a partir do resto da rede, diz. Embora esteja numa fase muito inicial no ciclo de adoção das SDN, Hinden recomenda que as equipes de redes e segurança trabalhem em conjunto, por num mundo SDN," toda a equipe de redes será responsável pela segurança".

Para RAMOS et al (2013) - As principais causas de preocupação encontram-se justamente nos principais benefícios das Redes Definidas por Software: a programação da rede e a centralização da lógica de controle. Esses recursos introduzem novas falhas e ataques aos planos, abrindo as portas para novas ameaças que não existiam antes ou eram mais difíceis de explorar. Redes tradicionais têm "proteções naturais" contra o que seriam vulnerabilidades comuns em sistemas de TI convencionais. Ou seja, a natureza fechada, proprietária, dos dispositivos de rede, o seu projeto bastante estático, a heterogeneidade do software, bem como a natureza descentralizada do plano de controle representam defesas contra ameaças comuns. Por exemplo, um ataque explorando uma vulnerabilidade peculiar de um conjunto específico de dispositivos de um único fornecedor, potencialmente prejudica apenas uma parte da rede. Esta diversidade é comparativamente menor em SDNs. Um padrão comum entre os fornecedores e os clientes, como o OpenFlow, também pode aumentar o risco e a eventual introdução de falhas comuns em implementações desses protocolos e do software de plano de controle.

Vulnerabilidade de componentes não é um desafio de segurança exclusivo desse novo paradigma de rede, mas torna-se mais crítico, pois uma vulnerabilidade em um nó controlador torna toda a rede vulnerável. Existem três possíveis fontes de vulnerabilidade de componentes: comutadores, controlador e estações de gerenciamento. Uma vulnerabilidade em um comutador pode permitir que um atacante que obtenha acesso a um comutador execute um ataque contra o plano de controle, a exemplo da falsificação de mensagens de outros comutadores para esgotar os recursos do controlador. Uma vulnerabilidade no controlador pode permitir que um atacante altere o plano de controle ou até mesmo execute uma nova aplicação de controle da rede. Uma vulnerabilidade em uma estação de gerenciamento permite que o atacante faça configurações no plano de controle diferentes das corretas (DUARTE et al, 2014).

De acordo com Mattos et al (2014), Natarajan et al (2015), a negação de serviço pode ocorrer tanto no plano de dados quanto no plano de controle. No plano de dados, uma estação maliciosa que gere fluxos falsos pode esgotar tanto os recursos de banda, quanto os recursos de memória, ou tabela de fluxos dos comutadores da rede. A negação de serviço no plano de controle pode ser causada em dois pontos distintos da rede: no controlador e na comunicação do controlador com os comutadores. É possível esgotar a capacidade de processamento do controlador de rede enviando uma grande quantidade de pacotes com diferentes cabeçalhos. Todo pacote é analisado e um pacote com cabeçalho que não corresponde a nenhum fluxo já definido deve ser enviado ao controlador de rede. Assim, em um cenário em que um comutador envia uma quantidade atípica de novos cabeçalhos de pacotes para o controlador, este pode ter seus recursos de processamento exauridos e não ser capaz de responder a pedidos de novos fluxos em tempo hábil. Da mesma forma, a negação de serviço pode ser alcançada quando o enlace de conexão entre o controlador e os comutadores na rede é intencionalmente congestionado. Caso não haja redundância ou banda suficiente no enlace que conecta os comutadores ao controlador, um comutador malicioso pode gerar tráfego suficiente para sobrecarregar esse enlace e, em consequencia, impedir a comunicação do controlador com os demais comutadores

Segundo Ross et al (2010), o SSL é usado para oferecer segurança em transações que ocorrem através do HTTP. Entretanto, como o SSL protege o TCP, ele pode ser empregado por qualquer aplicação que execute o TCP. Ele é um protocolo de transporte que provê serviços do TCP aprimorados com serviços de segurança.

Conforme Carneiro (2002), A segurança da informação deve ter como objectivo a sua protecção, a possibilidade de viabilizar as aplicações, de modo a que os níveis estratégicos das empresas possam utilizar os recursos informáticos no sentido de tornarem as grandes decisões, ficando protegidos em relação à utilização do SI por outros utilizadores que podem perturbar o respectivo equilíbrio.

2.1. Conceptualização

As Redes Definidas por Software (SDN - Software-Defined Networking) surgiram como um promissor conceito para o projeto de novas arquiteturas para a Internet. SDN é uma proposta baseada na separação dos planos de dados e de controle em uma interface uniforme, independente de fornecedor, para o mecanismo de encaminhamento (ex.: OpenFlow [McKeown et al. 2008]) e com um plano de controle logicamente centralizado.

Lantz et al (2010), explica que em uma rede definida por software o plano de controle (ou "sistema operacional de rede") e separado do plano de dados. Normalmente, o sistema operacional de rede observa e controla o estado de toda a rede a partir de um ponto centralizado, oferecendo recursos como: protocolos de roteamento, controle de acesso, virtualização de rede, gestão de energia e também prototipação de novos de protocolos. A principal consequência das SDN é que as funcionalidades da rede podem ser alteradas ou mesmo definidas apos a rede ter sido implantada. Novas funcionalidades podem ser adicionadas, sem a necessidade de se modificar o hardware, permitindo que o comportamento da rede evolua na mesma velocidade que o software

. Casado et al (2012), apresenta características desejaveis para SDN, separando em características de hardware e de software. O hardware deve ser simples, barato, facil de operar e independente de fabricante, evitando que os usuários sejam obrigados a usar equipamentos de um único fornecedor. Também deve suportar inovações futuras, evitando atualizações desnecessárias. Com relação ao software, Casado entende que ele deve ser flexível, estruturado e capaz de suportar uma ampla variedade de requisitos (virtualização, engenharia de tráfego, controle de acesso, etc). Também deve ser modular e expansível, permitindo inclusão e alteração de módulos.

Por sua vez, pode-se dizer que a rede definida por software (SDN) foi projetada para tornar a rede flexível e ágil. A SDN permite que o administrador projete, crie e gerencie redes, separando os planos de controle e de encaminhamento. Como resultado, o plano de controle é diretamente programável e retira a infraestrutura subjacente de aplicações e serviços.

A inteligência de rede é centralizada de forma lógica com controladores SDN programáveis. Implementado no software, esses controladores mantém uma visão coerente do

domínio de rede. Nos mecanismos de política e aplicações, a SDN parece com um único *switch* lógico.

Segundo Kurose (2010), A camada de soquete segura (SSL) é usado para oferecer segurança em transações que ocorrem através do HTTP. Entretanto, como o SSL protege o TCP, ele pode ser empregado por qualquer aplicação que execute o TCP. Ele é um protocolo de transporte que provê serviços do TCP aprimorados com serviços de segurança.

2.2. Contextualização

Apesar da evolução formidável da Internet, em termos de aplicações, sua tecnologia, Transmission Control Protocol / Internet Protocol (TCP/IP), não evoluiu o suficientemente nos últimos vinte anos. Nesses, a Internet tornou-se comercial e os equipamentos de rede tornaram-se "caixas pretas", ou seja, são soluções integradas verticalmente baseadas em software fechado rodando em um hardware proprietário. O resultado desse modelo é o já engessamento da Internet (Duque, 2012).

Isso significa um grande avanço por permitir aos utilizadores destas redes definirem fluxos de dados e de determinarem os caminhos destes fluxos usando software independentemente do hardware, ou seja, as redes passam a ser abertas, no sentido de que os utilizadores podem integrar o software representado pelo modelo Open Systems Interconnection (OSI) e pelos protocolos do modelo, de um determinado fabricante ao hardware de outro, criando-se uma forma de abrir a competitividade do mercado, não sendo preciso comprar um determinado software e em conjunto o hardware do mesmo fabricante, representando este fato o principal objetivo dos proponentes da tecnologia de Redes SDN (Duque, 2012).

Na Arquitetura SDN proposta, tudo o que é inteligência de sistema operativo fica concentrada num sítio, onde haja "visibilidade global" sobre toda a rede. Portanto, em vez de replicar todos os protocolos de roteamento em todos os dispositivos, eles ficam num só lugar. Com este sistema operativo implantado em plataformas abertas de servidores, linguagens e outros sistemas operacionais, a introdução de aplicações e funcionalidades torna-se uma questão de instalação de pequenos programas, elaborados por quem os quiser programar, podendo ser um fabricante ou um operador da rede (Duque, 2012).

CAPÍTULO III

3. METODOLOGIA DE PESQUISA

3.1. Instrumentos de Pesquisa

A Metodologia de investigação que irá ser usada no presente trabalho será o design descritivo. Este método usa um conjunto de técnicas para descrever fenómenos que ocorrem na sua forma normal, usando dados que podem ser recolhidos tanto em primeira mão como dados já existentes. Na pesquisa descritiva realiza-se o estudo, a análise, o registro e a interpretação dos fatos do mundo físico sem a interferência do pesquisador. O processo descritivo visa a identificação, registro e análise das características, fatores ou variáveis que se relacionam com o fenômeno ou processo. Esse tipo de pesquisa pode ser entendido como um estudo de caso em que, após a coleta de dados, é realizada uma análise das relações entre as variáveis para uma posterior determinação dos efeitos resultantes em uma empresa, sistema de produção ou produto

Para a realização deste trabalho, foi feita incialmente baseando-se em pesquisa bibliográficas, em textos e documentos publicados sobre o tema escolhido para este trabalho e foi feita análise de documentos recolhidos com informações importantes que abordam a temática a partir de conceitos-chave como redes definidas por software (SDN), camada segura do soquete (SSL), segurança, entrevistas aos mebros do IST, internet, monografias, documentos publicados, etc.

CAPÍTULO IV

4. Rede do grupo IPS – Maputo

O IPS – soletrado é Instituto Superior Politécnico Lda, é uma empresa detentora de vários negócios cujo principal é o ensino. A actividade é desenvolvida pela Universidade Politécnica, Instituto Médio Politécnico e a Escola Secundária das Acácias. O IPS.Lda faz uso das TICs, para o seu processo de funcionamento, pautando pelo processo de gestão na base de sistemas informáticos como Primavera (Gestão empresarial), UNIMESTRE (Gestão académica).

A rede do IPS, é uma rede integrada, possuindo serviços de dados, voz, e Internet a fluir na mesma infraestrutura. Comporta redes Ethernet, cat 5 e 5e, conjugados com *backbones* de fibra óptica e redes sem fio

O IPS criou um sistema que faz a gestão de dados de toda a rede que é composta pela Universidade Politécnica, Instituto Médio Politécnico e a Escola Secundária das Acácias. A rede é gerenciada e manipulada pelos IST (Serviços e Tecnologias, LDA), que tem como objectivo analisar os processos e equipamentos dos pontos centrais da infraestrutura de rede para determinar as melhores soluções de configuração da rede, Configurar Router Central (DMZ), configurar políticas de segurança no router central.

Mediante este ambiente de insegurança onde os dados estão inseridos e fluem nos sistemas e redes de computadores, foi feito um estudo na universidade politécnica sobre a vulnerabilidade na rede do IPS, e constatou-se que o maior problema que a rede tem enfrentado são os diversos tipos de ataques a rede. Estes ataques visam invadir a rede, roubar a informação, alterar configurações no sistema, etc. E os tipos de ataques que a rede tem sofrido são: **Spoofing, Flooding e worn.**

4.1. Spoofing

Spoofing é um tipo de ataque hacker dos mais populares nos últimos tempos, em que uma pessoa se passa por outra ou uma empresa legítima, no intuito de roubar dados, invadir sistemas e espalhar *malwares.*

O termo **spoofing** vem do verbo em inglês ***spoof*** (imitar, fingir), que em Tecnologia da Informação é um jargão usado para falsificação. Em geral, o termo descreve o ato de enganar um *site*, um serviço, um servidor ou uma pessoa afirmando que a fonte de uma informação é legítima, quando não é. É mais simples do que se pode imaginar.

Quando se recebe um e-mail "suspeito" de um contato conhecido e confiável (pode ser um amigo, um familiar, uma empresa ou mesmo o seu banco), com todas as informações do cabeçalho aparentemente corretas (nome, endereço de e-mail, remetente, etc.) mas com um conteúdo estranho, pedindo para clicar em links encurtados e/ou enviar dados sensíveis, por exemplo, trata-se de um ataque *spoofing*. Como o *spoofing* pode ser usado de maneira muito ampla, pode ser difícil identificar cada ataque. Por isso, é muito importante se equipar com uma segurança de internet forte e confiável (Gogoni, 2013).

4.1.2. Tipos de spoofing

Spoofing de ID: Um *hacker* faz uma requisição a um *site* ou servidor se passando por um IP legítimo, de forma que a vítima não consiga identificar o atacante;

Spoofing de e-mail: Um dos mais comuns, mira usuários e consiste em e-mails falsos, se passando por outra pessoa ou uma empresa real.

Spoofing de DNS: O hacker manipula as conexões de rede (alterando o DNS de roteadores em larga escala) e desvia acessos a um site legítimo para uma cópia falsa, de modo a roubar dados. Sites de bancos são os alvos mais comuns;

Spoofing de chamadas e/ou SMS: O atacante faz chamadas ou envia mensagens SMS se passando por um número legítimo, tentando enganar outros usuários;

Caller ID Spoofing: Este é um método mais elaborado. O *hacker* tenta acessar serviços de telefonia ou de apps através de um número de celular clonado, de modo a invadir contas de e-mail, mensageiros e redes sociais do usuário copiado (Gogoni, 2013).

4.2. Worms

Um **worm** é um software malicioso que se replica a si próprio de um computador para outro com o objetivo de controlar por completo uma rede informática. A maioria dos worms é desenhada para se infiltrar nos sistemas explorando as falhas de segurança existentes, e, além disso, alguns worms também tentam alterar as configurações do sistema. Mesmo não o conseguindo, os worms continuam a ser extremamente perigosos, dado que consomem muita largura de banda e outros recursos preciosos (SotfwareLab, 2014).

4.2.1. Tipos de Worms

Não há nenhuma classificação oficial de worms, mas estes podem ser organizados em tipos consoante a forma como se propagam entre computadores. Os cinco tipos mais comuns são os seguintes:

4.2.2. Worms de Internet

Tal como acontece com as redes de computadores, os worms também atacam websites populares que não estejam suficientemente protegidos. Quando conseguem infetar o website, os worms de Internet têm a capacidade de se replicar para qualquer computador que esteja a ser usado para aceder ao website em questão. A partir daí, estes worms são distribuídos para outros computadores ligados através da Internet e de ligações de rede locais.

4.2.3. Worms de E-mail

Os worms de e-mail são normalmente distribuídos através de anexos de e-mail comprometidos. De uma maneira geral, são ficheiros com extensão dupla, para que o recetor da mensagem pense que são ficheiros multimédia e não programas maliciosos. Quando a vítima clica no anexo, faz com que sejam enviadas cópias do ficheiro infetado para todos os contactos da lista.

Uma mensagem de e-mail não tem de conter um anexo para espalhar um worm. Em alternativa, o corpo da mensagem pode conter um link abreviado de forma a que o utilizador não perceba o contexto sem clicar no link. Quando clica no link, o utilizador é levado para um

website infetado que automaticamente começa a descarregar software malicioso para o computador.

4.2.4. Worms de Mensagem Instantânea

Os worms de mensagem instantânea funcionam exatamente da mesma forma que os worms de e-mail, sendo que a única diferença é a sua forma de distribuição. Novamente, estes worms disfarçam-se sob anexos ou links para websites. Muitas vezes são acompanhados de expressões como "LOL" para tentar levar a vítima a pensar que o amigo lhe está a enviar um vídeo cómico.

Quando o utilizador clica no link ou anexo – seja no Messenger, WhatsApp, Skype, ou qualquer outra aplicação de mensagens instantâneas – a mesma mensagem é enviada a todos os seus contactos. Os utilizadores podem geralmente resolver este problema alterando a sua palavra-passe, a menos que o worm se tenha replicado para o seu computador.

4.2.5. Worms de Partilha de Ficheiros

Apesar de ilegais, as transferências de partilha de ficheiros e peer-to-peer continuam a ser usadas por milhões de pessoas por esse mundo fora. Ao continuar esta prática, estas pessoas estão a expor o seu computador à ameaça de worms de partilha de ficheiros sem o saberem. Tal como os worms de e-mail e de mensagem instantânea, estes programas disfarçam-se de ficheiros multimédia com duplas extensões.

Quando a vítima abre o ficheiro descarregado para o ver ou ouvir, acaba por descarregar o worm para o seu computador. E mesmo que pareça que o utilizador descarregou um ficheiro verdadeiro de multimídia, pode estar escondido na mesma pasta um ficheiro malicioso executável que é discretamente instalado quando o ficheiro multimídia é aberto.

4.2.6. Worms de IRC

O IRC (Internet Relay Chat) é uma aplicação de mensagens que está fora de moda hoje em dia, mas que teve o seu auge ao virar do século. Da mesma forma que acontece com as plataformas de mensagens instantâneas atualmente, os worms eram distribuídos por mensagens

que continham links e anexos. Estes últimos não eram tão eficazes, devido a uma camada de segurança que obrigava os utilizadores a aceitar um ficheiro antes que este pudesse ser transferido para o seu computador (SotfwareLab, 2014).

4.3. Flooding (Ataques por Inundação)

Ataques por inundação são caracterizados por causar um grande volume de tráfego no sistema da vítima primária, de maneira que sua banda fique congestionada, por meio da utlização de pacotes UDP (*User Datagram Protocol*) ou ICMP (*Internet Control Message Protocol*). Esta forma de ataque pode tanto deixar o sistema lento quanto derrubá-lo por completo.

O UDP é um dos principais protocolos de rede da *Internet*, e permite que aplicações enviem mensagens de tamanho fixo (neste caso chamadas de datagramas, especificamente) encapsuladas em pacotes IPv4 ou IPv6 a um destino escolhido. Neste tipo de protocolo não há garantia da chegada do pacote.

O ICMP é um dos principais protocolos de rede da *Internet*, e é utilizado para o envio de relatórios de erro à fonte original. Mensagens ICMP costumam ser enviadas automaticamente quando um pacote não consegue chegar a seu destino, por exemplo (Duarte, 2013).

4.3.1. Tipos de Ataques

4.3.2. Inundação por ICMP (ICMP Flood)

Também conhecido como inundação *ping*, ou *ping flood*, este tipo de ataque se baseia no envio constante a partir de um endereço IP mascarado de uma grande quantidade de pacotes *echo request* (*ping*) até que o limite de *requests* por segundo seja ultrapassado.

Para tal, o atacante necessita de certos privilégios no sistema alvo, além de precisar de uma vantagem de banda significativa em relação ao alvo para ter sucesso (por exemplo, um sistema *dial-up* seria alvo fácil para um atacante que possuísse um sistema com conexão DSL de alta velocidade, mas o contrário não teria sucesso).

Se o ataque for bem-sucedido, a banda do alvo é, rapidamente, completamente consumida pelos pacotes ICMP que chegam e os pacotes de resposta que envia, impedindo que *echo requests* legítimos sejam atendidos.

4.3.3. Inundação SYN (SYN Flood)

Neste tipo de ataque, o atacante inunda a rede com pacotes TCP SYN, frequentemente com um endereço IP de origem mascarado. Cada um desses pacotes representa uma intenção de conexão, o que leva o servidor alvo a alocar, para cada um deles, uma determinada quantidade de memória para a nova conexão a ser criada e enviar de volta um pacote TCP SYN-ACK, para o qual espera uma nova resposta (TCP ACK) que permitirá efetivamente estabelecer a nova conexão.

Como os pacotes ACK esperados nunca são enviados pela origem, quando a memória do servidor é completamente alocada os pedidos legítimos de conexão são impedidos de ser atendidos até que o ataque acabe. Além disso, as conexões parciais resultantes possibilitam ao atacante acessar arquivos do servidor

4.3.4. Ataques peer-to-peer

Este tipo de ataque difere dos ataques baseados em botnet, mais frequentes. Nele, não há botnet e o atacante não precisa se comunicar com os clientes sabotados; em vez disso, ele trabalha enviando instruções a clientes de grandes redes peer-to-peer (p2p) para compartilhamento de arquivos. Tais instruções fazem com que esses clientes se desconectem da rede peer-to-peer e se conectem ao alvo. Como resultado, uma grande quantidade de novas conexões com o alvo tenta ser iniciada, parando o servidor ou levando a uma queda significativa do seu desempenho

4.3.5. Ataques distribuídos (DDoS)

Neste tipo de ataque, múltiplos sistemas (e não apenas um) inundam a banda ou os recursos de rede de um alvo, frequentemente pelo uso de botnets, e impedem a formação de novas conexões. As vantagens, para o atacante, de um DDoS em relação a um ataque de negação de serviço feito a partir de um único sistema são a maior facilidade para gerar um tráfego de ataque mais intenso e a maior dificuldade para o alvo anular o ataque.

Este tipo de ataque pode ser feito por *malware*, por exemplo. Um dos mais conhecidos *malwares* para DDoS é o MyDoom, que possui um endereço IP alvo *hardcoded*, e seu mecanismo de ataque de negação de serviço é ativado em uma data e uma hora específicas.

Assim, não é necessário mais nenhum tipo de interação por parte do atacante para que o ataque ocorra.

DDoS também pode ser feito por meio de um trojan, que contém ou faz download de um programa que transforma o sistema em um "zumbi". Ou seja, é estabelecida uma botnet. Diferentemente do ataque que utiliza *malware*, a utilização de um trojan permite que o endereço IP alvo seja alterado após a infecção.

As soluções para os ataques passaram por reforço das regras dos FireWalls, implementação de antivírus centralizados e actualizados, segmentação das redes por departamento e por tipo de tráfego (Duarte, 2013).

4.4. Protocolos de Segurança usados para proteção da Rede do IPS

O IST que é a instituição que veta pela protecção da rede dos IPS. Com isso o IST adoptou políticas de segurança, que são conjuntos de regras, leis e práticas de gestão visando à protecção dos dados na rede, tendo com isso implementado os seguintes protocolos de segurança: **IPsec** e **Wap** de modo a combater os diversos tipos de ataques que a rede tem sofrido. Esses protocolos visam garantir a Integridade dos dados enviados, a privacidade dos usuários e autenticação dos usurários.

O Protocolo **IPSec** implementa uma forma de tunelamento na camada da rede (IP) e é parte das especificações da pilha de protocolos IPV6. Ele fornece autenticação em nível da rede, a verificação da integridade de dados e transmissão com criptografia e chaves fortes de 128 bits. Implementa um alto grau de segurança na transmissão das informações.

O protocolo IPSec dificulta de maneira permanente uma eventual tentativa de ataque vindo por parte do *hacker*, tornando muito difícil fazer um grampo em linhas de comunicação e obter qualquer informação útil do tráfego da rede.

O IPSec utiliza os seguintes elementos principais para proteger a comunicação via rede:

Cabeçalho de autenticação (AH) – efetua uma autenticação e verificação da integridade dos dados. O processo de autenticação impede a recepção em estações sem autorização, evita eventuais tentativas de falsificação ou alteração de informações ao longo da rota. Não permite a

criptografia dos dados, portanto é útil principalmente quando a verificação da integridade é necessária, mas não o sigilo.

Carga de empacotamento (ESP) – é uma forma de transporte segura e tempo finalidade evitar a interceptação, a leitura dos dados por terceiros, ou uma eventual cópia dos dados. Além disso, ele também fornece verificação de integridade.

O protocolo **WAP** (Acesso WiFi Protegido) - É uma tecnologia desenvolvida para proteger o acesso à Internet para redes Wi-Fi. Antes disso, o WEP ou Wired Equivalency Privacy era a única tecnologia de **segurança** disponível, mas foi posteriormente atualizada, já que seus recursos de autenticação e criptografia eram fracos

O WPA funciona a partir de uma chave secreta contendo entre 32 e 512 bits conhecida como PMK, ou Chave Mestra Dupla, que gera uma PTK, ou Chave Transiente de Dupla (do inglês "Pairwise Transient Key"), a partir de alguns parâmetros obtidos durante a conexão, sendo compartilhada entre o computador e o ponto de acesso.

Com intuito de melhorar a Segurança da rede do Instituto Superior Politécnico, foi feito um estudo sobre que protocolo de segurança que permitiria ter uma rede mais segura e constatou-se que o potocolo SSL é mais viavel para combater os ataques que rede tem sofrido, pois O protocolo SSL oferece serviços a protocolos do nível de aplicação proporcionando confidencialidade, integridade e autenticação dos dados. Ele utiliza para transporte o protocolo TCP, reside acima da camada de transporte, é independente das aplicações da camada superior e por isso é considerado um protocolo de segurança que não depende do protocolo de aplicação.

O SSL estabelece um conjunto criptográfico e um método de compreensão a ser utilizado. O conjunto criptográfico constitui-se de um algoritmo para troca de chaves, um algoritmo para cifragem de dados e um algoritmo para inserção de redundância nas mensagens. O algoritmo para troca de chaves será de criptografia de chave pública, usado no envio da chave privada do algoritmo de cifragem de dados, assim o SSL utiliza um algoritmo assimétrico para criar um canal seguro enviando a chave secreta que será utilizada para cifragem dos dados por um algoritmo simétrico. Por fim, o algoritmo de inserção de redundância é utilizado para garantir a integridade da mensagem que recebe o nome de MAC (*Message Autentication Code*). As mensagens do protocolo de aplicação são então comprimidas, inseridas as MAC e então cifradas

antes de serem envidadas ao TCP. Após a mensagem ser decifrada no destino, a autenticidade da mensagem é verificada sendo comparada com a MAC, quando então é descomprimida e envida para a camada de aplicação. Isso permite-nos ter uma rede mais segura para a troca de Informações.

4.4.1 A diferença entre os Protocolos de Segurança IPSec e SSL

A segurança da Internet é muito importante, e as pessoas descobriram várias maneiras de garantir que terceiros não recuperem seus dados. SSL e IPSec garantem segurança em diferentes níveis.

- ✓ No IPSec, a criptografia é feita no nível da rede, enquanto o SSL é feito nos níveis superiores.
- ✓ O IPSec introduz cabeçalhos para garantir a segurança, enquanto o SSL usa dois subprotocolos para se comunicar.
- ✓ SSL é escolhido em vez de IPSec em transações do tipo web da Internet devido à sua simplicidade em relação ao IPSec.

Rede do IPS. Ela esta dividida da seguinte maneira: área da Internet Solutions, área do DMZ/Firewall (Central onde é feito o controle de toda a rede) que esta na biblioteca da faculdade , área da Rede publica, área da Rede interna e a área da Rede wireless (Antenas), como está ilustrada na figura abaixo:

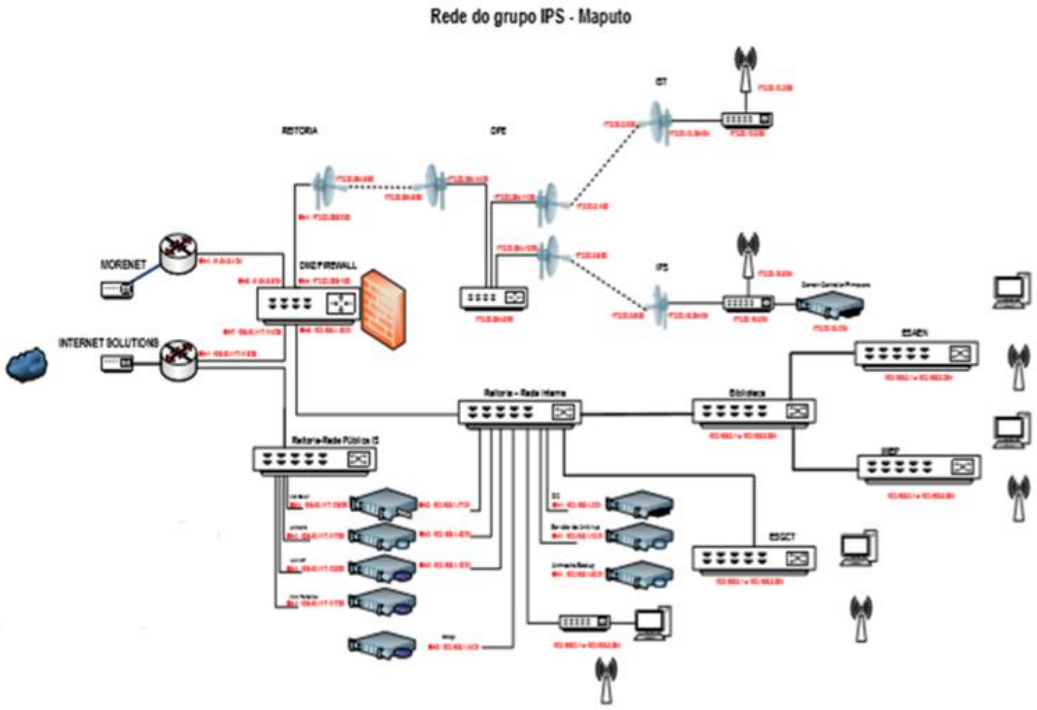


Figura 4.1: redes do grupo IPS

4.5. Componentes da rede do IPS

- Provedor de internet;
- Router P.I;
- Switchs;
- Servidores;
- Antenas;
- Computadores;
- Cabos de fibra.

4.6. Funcionamento da rede do IPS

A rede funciona da seguinte maneira: a Internet Solutions (provedor de internet), manda o sinal para a DMZ/Firewall que tem a função de controlar toda a rede, isto é, toda a rede é manipulada, gerenciada, configurada e protegida pela DMZ que é a central da rede. A central manda o sinal para o switch da rede publica que distribui o sinal para os diferentes servidores da rede pública que são Mail server, Unimestre server, www IST server e politecnica server, que recebem IPs públicos. Por sua vez os servidores da rede pública mandam sinal para o switch da rede interna que distribui pelos seus servidores que são DC server, servidor do antivírus e Unimestre backup onde são armazenadas as informações da página, do Unimestre, etc.

Atravez do switch cisco da rede interna o sinal é enviado por cabos de fibra para o switch da Biblioteca e o switch da ESGCT, o *swich* da Biblioteca envia o sinal para o *switch* do ESAEN e do IMEP onde é distribuído para os diferentes departamentos da faculdade. A DMZ também envia o sinal para a Antena da Reitoria que por sua ver partilha o sinal com as antenas da DPE, IST e IPS.

Esta é uma rede centralizada, onde todo o controle da rede é feito através de um determinado ponto, a configuração é feita no Router central (DMZ) e também foram configuradas políticas de segurança no router central e router para ACCESS-POINT ”wireless”. O controle da rede é programável directamente pelos administradores, permitindo configurar, gerenciar, proteger e optimizar os recursos de rede muito rapidamente através de dinâmicas e programas SDN automatizados

CAPÍTULO V

5. APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

Redes Definidas por Software (Software Defined Networks) SDN é uma nova abordagem para redes de computadores com uma proposta mais dinâmica, gerenciável, adaptável e com uma boa relação custo-benefício. O que faz do SDN ideal para alta largura de banda e para a natureza dinâmica dos aplicativos atuais, pois tornam as redes de computadores mais flexíveis e eficientes (Lins, 2015).

5.1. Características do SDN

As principais características da abordagem SDN são:

- **Programável:** o controle da rede é programável directamente pelos administradores, permitindo configurar, gerenciar, proteger e optimizar os recursos de rede muito rapidamente através de dinâmicas e programas SDN automatizados.
- **Agilidade:** permite os administradores ajustar dinamicamente o fluxo de tráfego em toda a rede para atender as demandas de mudança.
- **Gerenciamento central:** toda inteligência da rede é logicamente centralizada nos controladores baseados em *software* que possuem uma visão global da rede.
- **Abertura:** implementado por meio de padrões abertos, SDN simplifica o projecto e operação de rede porque as instruções são fornecidas pelos controladores de SDN em vez de dispositivos específicos de fornecedores e protocolos.

De acordo com Stutz (2017), As redes definidas por software, ganham força no mercado como um modelo de arquitetura, capaz de permitir provisionamento automatizado e virtualização. Segundo uma pesquisa do IDC, a estimativa é que o setor movimente US$ 12,5 bilhões até 2020 em todo o mundo, um aumento de 53,9% em relação a 2014.

Apesar de a rede física continuar sendo a maior responsável pelo segmento desse mercado em 2020, o crescimento mais rápido será nas duas categorias de software, a camada de virtualização e controle, e as aplicações SDN que, juntas, devem atingir cerca de US$ 5,9 bilhões, segundo perspectiva da IDC.

Com a transformação digital, que toma conta da agenda de companhias de todos os portes e segmentos, a TI precisa se reposicionar e trabalhar de maneira mais proativa, com a mudança na forma de entregar os serviços. A SDN entra exatamente, nesse cenário: para mudar a maneira de operar a infraestrutura, respondendo às novas formas de trabalho, com melhor controle e acesso das aplicações e informações da companhia, utilização da infraestrutura de maneira mais eficiente e políticas de segurança mais eficazes.

Mas, assim como acontece com todo novo processo, a rede SDN exige uma preparação da empresa. Não se trata de algo meramente operacional, com a instalação de um software e pronto. Além de se atentar às questões de negócios, treinamento de usuário final, implantação de processos e formas de usar a tecnologia, a área de TI também precisa ser revista. Isso porque, SDN não é uma ferramenta que organiza a infraestrutura, mas uma evolução da rede. De maneira mais simples, o papel da rede de dados é interconectar serviços, computadores, máquinas e pessoas, mas até então, esse era um trabalho manual sujeito a erros. Com a tecnologia das redes definidas por software, o controle, gerenciamento e funcionamento centralizado da rede ficam mais simples e organizados, com menos variáveis, menos pontos de mudança e menos erros.

Dessa forma, com a mudança para a SDN, é preciso contar com um parceiro de tecnologia que tenha implementado este tipo de solução em uma maior escala e, preferencialmente, com a arquitetura SDN baseada em padrões abertos, que permita a evolução da plataforma para suportar o máximo de soluções disponíveis no mercado. Além disso, tão importante quanto a implementação correta, é avaliar a capacidade deste parceiro de tecnologia em manter a nova infraestrutura atualizada, já que a tecnologia estará em constante evolução para que possa incorporar novos serviços por demanda.

Mas o esforço vale com a tecnologia é possível, desde otimizar custos, já que as companhias passam a usar menos equipamentos; até aperfeiçoar as políticas de segurança da informação e de aplicações, que passam a ser controladas de maneira mais organizada. Com uma

rede programável, todos conseguem acompanhar o crescimento corporativo e inovar com uso de recursos sob demanda. E o objetivo de qualquer atualização tecnológica tem sempre de estar ligado à melhoria da produtividade para todos: clientes internos e externos.

5.2. Desafios

Uma pesquisa foi conduzida em 2016, onde 50 engenheiros de Empresas de primeira linha em redes de computadores fizeram um esudo sobre as deficiências da rede definida por software e o resultado foi o seguinte:

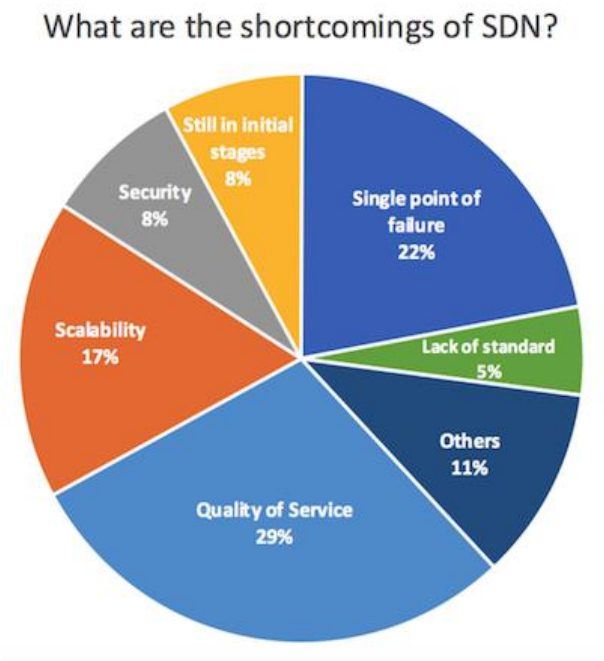
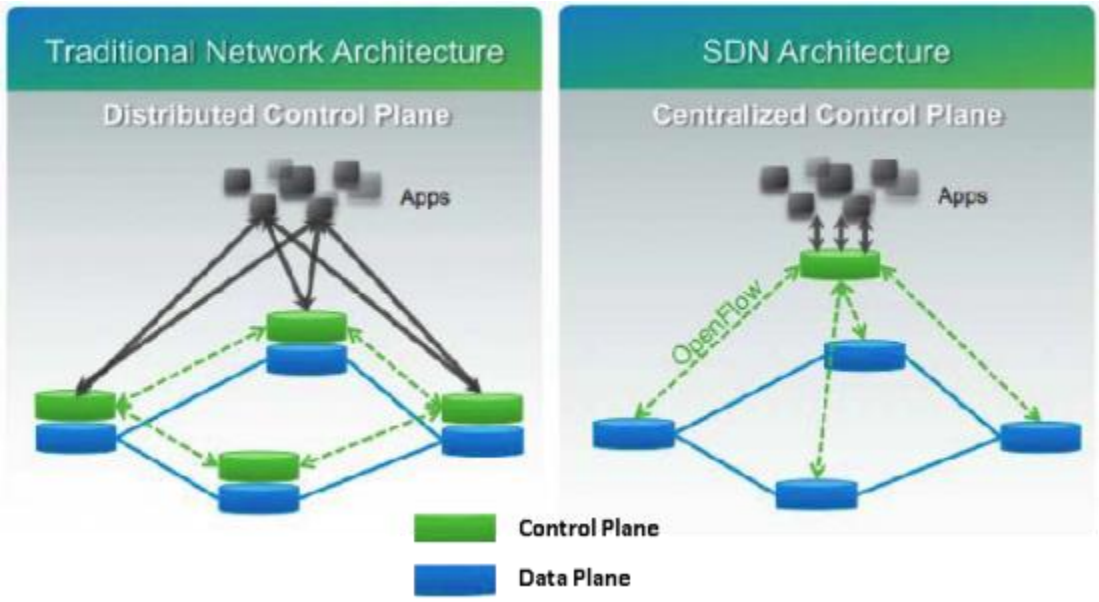


Gráfico 5.1: Os defeitos da SDN

Se a administração das redes tradicionais apresenta falta de automatismos para auxílio nas configurações, então a administração por SDN deve configurar novos dispositivos e novas aplicações para que os serviços de configuração deixem de ser feitos manualmente e individualmente. Este princípio facilitará vida aos administradores da rede, que criarão automatismos para aplicação das políticas de segurança e das configurações. Com apenas alguns cliques aplicar, por exemplo, Quality of Service (QoS) em setores específicos de rede, monitorizar serviços, executar configurações e analisar tráfego. Criar e manter relatórios de toda a rede com gestão centralizada. Possuir um único painel de bordo em que se visualiza toda rede:

topologia, tráfego, caminho se dispositivos numa única interface amigável desenhado por software. Ter a possibilidade de trabalhar as fontes da informação para obter os resultados desejados a partir do dito interface. Sem a necessidade de visitar todos os ativos de rede, libertar-se do tempo que passa normalmente por análise individual dos equipamentos com as ferramentas do SDN inovar de forma a reduzir o tempo médio da resolução de incidentes, quer na fase da identificação, quer na apresentação da solução. Trabalhar na melhoria dos processos de execução destas ações, para reduzir tempo na sua execução, tornando-os mais precisos e rápidos através de novos automatismos. Isto seria o sonho de qualquer administrador de rede (Cisco, Duong, 2015).

5.3. Rede convencional vs SDN



Fonte: http://decom.ufop.br/imobilis/redes-definidas-por-software-software-defined-networks-sdn/

Figura 4.2: Rede convencional vs SDN

A figura acima faz a comparação entre a rede convencional e o SDN, demostrando as suas diferenças. Nas redes convencionais o *control plane* está distribuído enquanto na SDN o *control plane* está centralizado.

5.3.1. Plano de controle

O plano de controle é o domínio responsável pela lógica a ser implementada. Por ele, todos os elementos da rede irão enviar fluxos desconhecidos até o controlador da rede, para assim, o controlador identificar e tomar decisões sobre como proceder de acordo com suas regras e configurar os fluxos. Como toda a parte lógica gera um questionamento ao controlador, a configuração dos fluxos e suas rotas ótimas fica a cargo dele, gerando a facilidade de um ponto único de configuração. Uma grande vantagem, é ter a noção do todo no momento de tomar as decisões, assim possibilitando variar o comportamento de acordo com o estado atual da rede (Fernandes, 2016).

É importante ressaltar que o controlador não é centralizado ou único, ele é uma parte do plano de controle. As funções do plano de controle em uma analogia com a rede atual de dados são:

- Estabilização do conjunto de dados locais;
- Manter o conjunto de dados;
- Manutenção da Routing Information Base – RIB;
- Manutenção da Forwarding Information Base – FIB.

5.3.2. Plano de dados

O plano de dados é responsável apenas pelo encaminhamento dos pacotes. É importante reforçar que o equipamento responsável pelo encaminhamento não mais participa da decisão de qual regra será criada, ele apenas possui uma tabela, FIB, a qual, quando confrontada com as características do pacote recebido, descreverá o comportamento que a ele deve ser aplicado (Fernandes, 2016).

As decisões de encaminhamento são regras simples, baseadas em parâmetros dos pacotes. Caso o equipamento não tenha regra definida para o pacote, esse pacote, em geral, é enviado para o controlador, onde o plano de controle entra em ação. Os pacotes sem regra, também podem ser descartados, dependendo da implementação da SDN. As funções do plano de dados incluem:

- Encaminhar pacotes baseados na FIB;

- Encaminhar pacotes para o plano de controle.

A figura ilustra ambos os planos de controle e de dados:

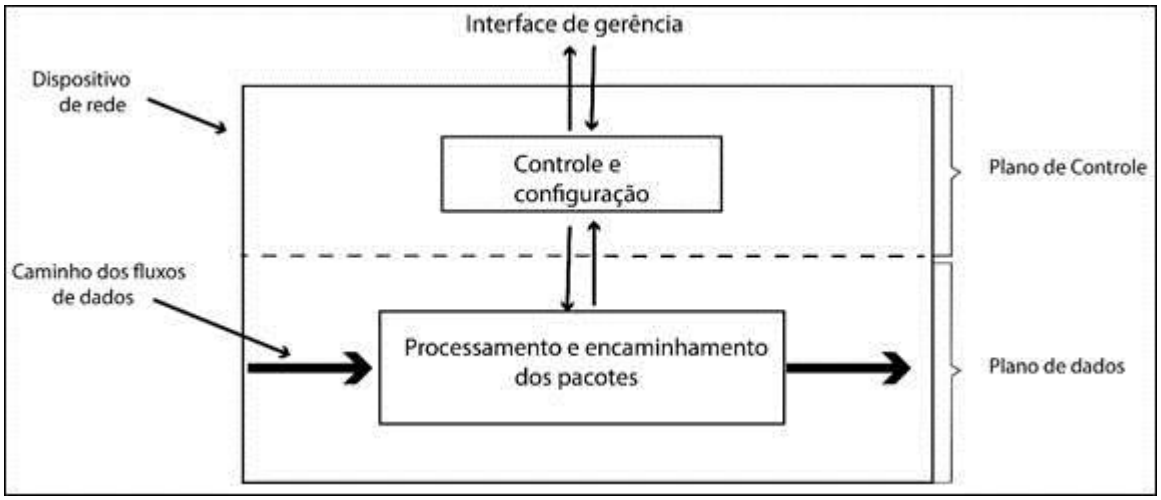
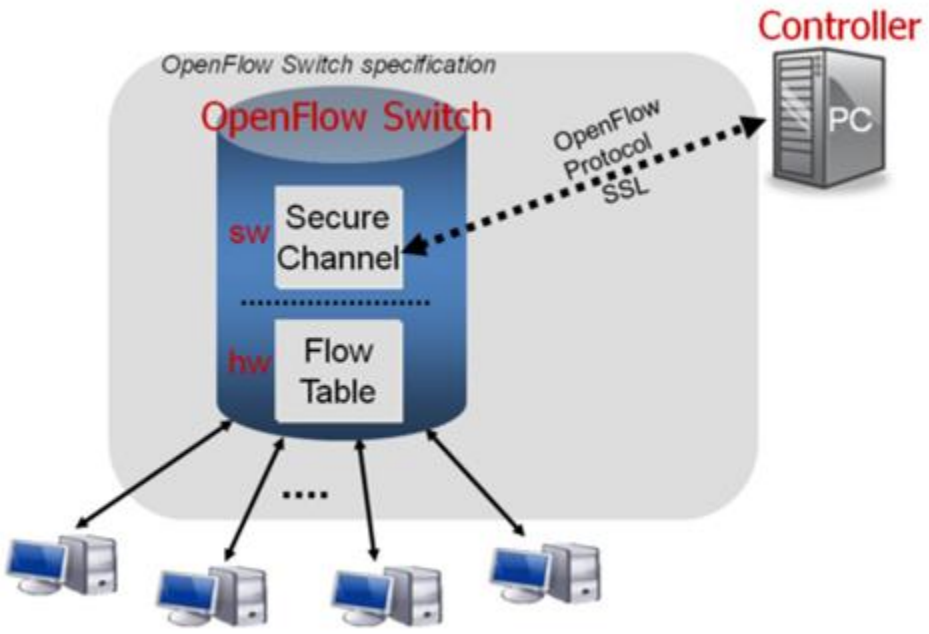


Figura 4.3: Planos de controle e dados

Fonte: Comer, 2013

5.4. Elementos de uma Rede Definida por Software



Fonte: http://yuba.stanford.edu/cs244wiki/index.php/Overview

Figura 4.4: Elementos de uma Rede Definida por Software

Basicamente, uma Rede Definida por Software utilizando o protocolo OpenFlow, consiste em elementos de rede habilitados para que o estado das tabelas de encaminhamento possa ser instalado através de um canal seguro, conforme as decisões de um controlador em software. Os componentes da arquitectura destas redes são: a tabela de fluxos, o canal seguro, o protocolo OpenFlow e o controlador.

5.4.1. Tabelas de fluxos

A entrada na tabela de fluxos do hardware de uma Rede Definida por Software consiste em regras, acções e contadores. A regra a ser aplicada a um determinado fluxo entrante na rede é formada com referência na definição de um ou mais campos do cabeçalho do pacote. Associa-se a ela um conjunto de acções que definem o modo com que os pacotes devem ser processados e para onde eles devem ser encaminhados. Os contadores são usados com a finalidade de manter estatísticas de utilização e também servem para remover fluxos inactivos (Duque, 2012).

5.4.2. Canal Seguro

Como a rede é toda desenvolvida em cima de protocolos públicos, ou seja, abertos "open source", é necessário que se tenha um canal para que possa trocar de forma segura informações entre o "switch" e o controlador, sem que sofra ataque de elementos mal-intencionados. A interface de acesso recomendada é o protocolo Secure Socket Layer (SSL). Interfaces alternativas (passivas ou ativas) incluindo-se o TCP são essenciais em ambientes virtuais e experimentais pela facilidade de utilização, pois não necessitam de chaves criptográficas (Duque, 2012).

5.4.3. Protocolo OpenFlow

O protocolo OpenFlow é um protocolo aberto utilizado para a comunicação, fazendo uso de uma interface de acesso, para a troca de mensagens entre os equipamentos de rede e os controladores (Duque, 2012).

5.4.4. Controlador

É o *software* responsável por tomar decisões e adicionar e/ou remover as entradas na tabela de fluxos, de acordo com o objectivo desejado. Exerce a função de uma camada de abstração da infraestrutura física, permitindo de forma mais fácil a criação de aplicações e serviços que gerenciem as entradas de fluxos na rede. A programação do controlador permite a evolução das tecnologias nos planos de dados e as inovações na lógica das aplicações de controle (Duque, 2012).

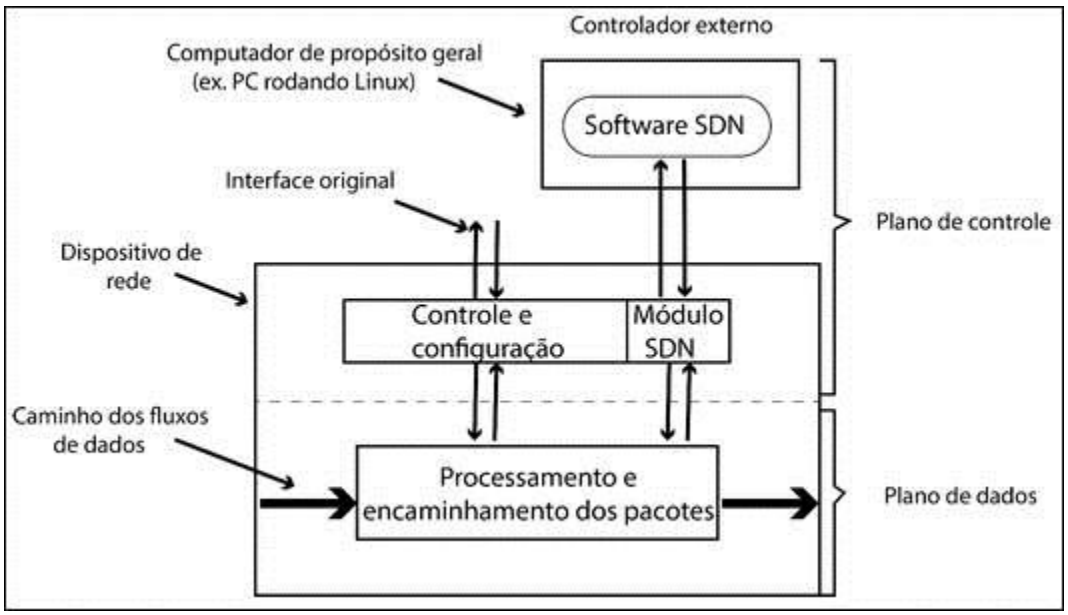


Figura 4.5: Configuração básica SDN: controlador externo configura o dispositivo de rede

Fonte: Comer, 2013

5.5. Segurança

Para Gabriela et al (2018), A arquitetura SDN retorna com alguns problemas de segurança que eram mitigados pela arquitetura antiga. Com dispositivos de rede proprietário dos fabricantes e de configuração, antes, um ataque que explorava uma vulnerabilidade de um modelo e afetava apenas a parte da rede composta pelos respectivos dispositivos. Agora com a alta configuração provida por um modelo centralizado, de interface aberta e conhecida, torna-se extremamente sensível, onde um ataque pode comprometer a rede como um todo.

Potenciais vulnerabilidades podem existir, por exemplo, pela camada de autenticação e autorização, pois o sistema pode ser controlado por diferentes organizações que têm acesso a rede. Diferentes níveis de acesso são necessários, pois diferentes agentes podem interagir com a configuração da rede. Além disso, por se tratar de padrões abertos e conhecidos, a fim de facilitar a integração por diferentes fabricantes, permite que atacantes conheçam toda a arquitetura e comandos. Uma vez invadida, o atacante torna-se capaz rapidamente e facilmente ter controle, podendo manipular a rede, os nós, e até usuários individuais.

Outro potencial vulnerabilidade se origina da centralização do controle da rede. Nesse nó está sujeito a ataques, por exemplo, de negação de serviço (DOS/DDOS). Pela arquitetura da SDN, quando um novo fluxo não encontrado na tabela é recebido, há duas opções, enviar o pacote completo ou apenas o cabeçalho para o controlador resolver o fluxo. Enviar o fluxo completo sobrecarrega esse canal, podendo congestionar o mesmo e comprometer a performance da rede. Caso seja enviado somente o cabeçalho, o restante do pacote precisa ser armazenado em um *buffer*. Este, por sua vez, é custoso e limitado, podendo ser consumido por completo, acarretando na perda de pacotes.

5.5.1. Canal seguro de comunicação OpenFlow

De acordo com Fernandes (2016), O canal seguro de comunicação é o meio utilizado para a comunicação entre *switch* OpenFlow e o controlador OpenFlow. Ele permite a troca de comandos e pacotes entre esses dois elementos. Por se tratar de parte crucial em um sistema distribuído, a comunicação entre os elementos deve ser altamente segura, evitando que este seja um vetor de ataques de elementos mal-intencionados na rede. Para dar confiabilidade ao canal, a interface de acesso recomendada é o protocolo Secure Socket Layer - SSL, já amplamente utilizado, que utiliza a encriptação dos dados trafegados utilizando certificados confiáveis reconhecidos pelos participantes da transação e que, em teoria, não podem ser quebrados. A comunicação entre o controlador e o switch é feita integralmente utilizando o Protocolo OpenFlow. Assim como em outros protocolos, nele existem alguns tipos básicos de mensagens que podem ser trocadas entre os elementos. Essas mensagens são classificadas como:

- Simétricas: São mensagens geradas sem solicitação dos elementos, em qualquer direção. Exemplos são as mensagens *hello* e *echo*. A primeira é trocada entre o controlador e o *switch* na inicialização da rede, a segunda é usada, principalmente, para verificar se a conexão entre o *switch* e o controlador continua ativa e para identificação de latência e banda.
- Assíncronas: São mensagens enviadas pelo switch sem a solicitação do controlador. Informam eventos na rede, erros, mudanças no estado do switch e chegada de pacotes. Um exemplo desse tipo de mensagem é a Packet In, que notifica a chegada de um fluxo não configurado no switch.
- Controlador para switch: São mensagens iniciadas pelo controlador, usadas para gerenciar diretamente ou inspecionar o estado do *switch*. Estas mensagens permitem que o controlador configure o *switch*, modifique estados e entradas de fluxo, dentre outras características.

5.6. Secure Socket Layer

O SSL (Secure Socket Layer) – é um padrão global em tecnologia de segurança desenvolvida pela Netscape em 1994. Ele cria um canal criptográfico entre um servidor Web e um navegador (browser), para garantir que todos os dados transmitidos sejam sigilosos e seguros.

A Camada de Soquetes Segura (Secure Sockets Layer ou SSL) e a Segurança da Camada de Transporte (Transport Layer Security ou TLS) são protocolos de segurança usados hoje em dia. Esses protocolos estabelecem um canal seguro entre dois computadores conectados via Internet ou uma rede interna. Em nosso cotidiano, onde a Internet desempenha um papel tão proeminente, é muito comum encontrar conexões entre navegadores e servidores web utilizando conexões de Internet não seguras, sem a presença da tecnologia SSL.

O SSL é composto por quatro mecanismos de segurança:

- Autenticação - Identifica a fonte dos dados;
- Integridade - Garante que dados não foram indevidamente alterados;
- Criptografia - Garante um conjunto de regras que visa codificar a informação de forma que o emissor e o receptor possam ter acesso;
- Troca de chaves criptográficas - Aumenta a segurança do mecanismo de criptografia utilizado.

5.6.1. Funcionamento do SSL

O SSL (Secure Sockets Layer)**,** usa um sistema de criptografia que utiliza duas chaves para criptografar os dados, uma chave pública conhecida por todos e uma chave privada conhecida apenas pelo destinatário. O SSL é a única e eficaz maneira de obter segurança de dados em comércio electrónico. Quando um SSL – Certificado Digital está instalado no website, um ícone de um cadeado aparece no navegador e o endereço começa com https:// ao invés de http:// informando que os dados serão criptografados.

A criptografia faz uso de chaves para bloquear e desbloquear suas informações, o que significa que você precisa da chave certa para “abrir” ou descodificar informações protegidas.

Cada certificado SSL vem com duas chaves: Uma chave pública, que é usada para criptografar (embaralhar) as informações e uma chave privada, que é usada para desincriptar (desembaralhar) as informações e restaurá-las em seu formato original tornando-as legíveis.

Para o usuário comum o processo é automático e imediato, mas é assim que funciona em segundo plano:

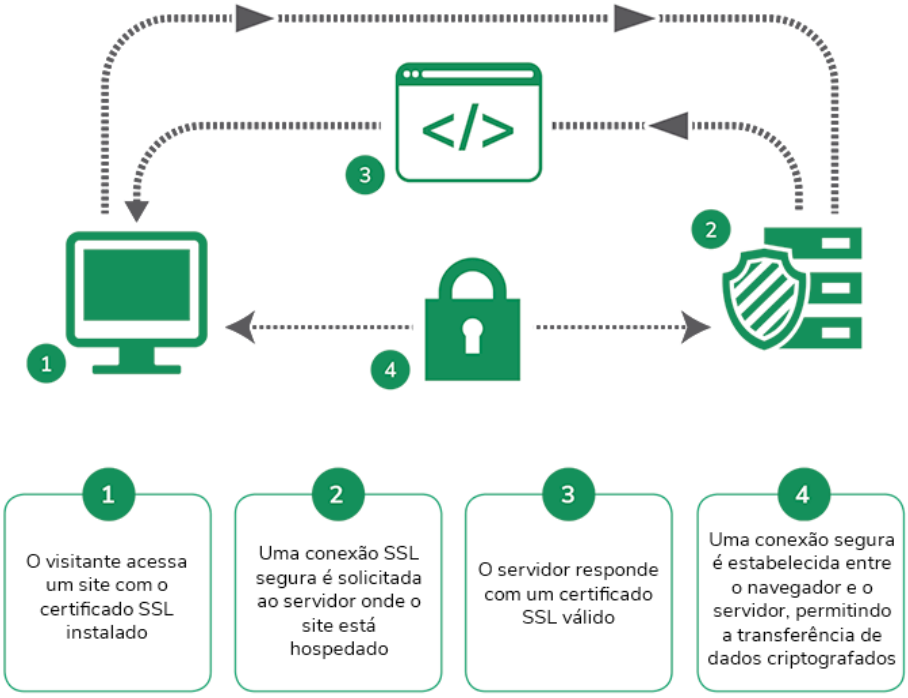


Figura 4.6: Funcionamento do SSL

Fonte: https://www.sectigo.com.br/ssl-o-que-e.php

5.6.2. Fluxo de Funcionamento do SSL

Ao iniciar uma conexão, o primeiro passo é o chamado *handshake*, onde o cliente envia para o servidor um apanhado de especificações para a conexão, como por exemplo a versão de SSL que está rodando, conjunto de criptografias possíveis para a conexão, etc. O servidor recebe essa mensagem e toma decisões baseado no que recebeu. Por exemplo, o servidor escolhe a maior versão possível de SSL para utilizar por motivos de segurança e escolhe o algoritmo de criptografia baseado em algum critério. Feito isso, o servidor envia para o cliente seu certificado

digital. Este, contém sua chave pública, contida no certificado digital, que será usada pelo cliente para dar início a uma conexão segura e verificar a autenticidade da chave com a *Certification Authority*. De posse da chave pública do servidor, o cliente responde enviando uma chave criada com o método de criptografia combinado previamente, que poderia ser por exemplo um método de chave simétrica, criptografando esta mensagem usando a chave pública recebida. O servidor, único detentor da chave privada capaz de descriptografar a mensagem enviada pelo cliente, lê a mensagem e a partir dali dá início a uma conexão baseada no método de criptografia escolhido. Com a posse das chaves simétrica a serem utilizadas, o processo de *handshake* está terminado e a partir de agora cliente e servidor trocarão mensagens seguramente nesta sessão SSL. Após concluída as tarefas a serem feitas nesta comunicação, a sessão SSL é destruída (Tinoco et al, 2015).

5.6.3. O handshake SSL

O processo de estabelecimento de uma conexão segura é conhecido como "handshake SSL". Não é como o handshake antiquado que todos fazemos todos os dias. Em vez disso, é uma versão moderna de um aperto de mão (assim como a geração "cool" faz). Este aperto de mão envolve três etapas (nenhum dabbing envolvido). Olá, verificação do servidor e transferência de chaves.

Olá: Como nós (bem, a maioria de nós) todos fazemos ao encontrar alguém, o cliente e o servidor se cumprimentam. O cliente envia uma mensagem ClientHello ao servidor. Este “Hello” contém algumas informações do certificado SSL. Em resposta a esta mensagem ClientHello, o servidor responde a ela pela mensagem ServerHello. Da mesma forma, também consiste em informações semelhantes à mensagem ClientHello.

Verificação do servidor: agora, existe uma conexão segura entre o cliente e o servidor (uma boa quantidade de conforto entre os dois). Agora, esta é a etapa em que o cliente verifica a identidade do servidor por meio de um certificado SSL. Um certificado SSL contém informações do proprietário / organização, sua chave pública de localização, datas de validade, etc. O cliente garante que uma autoridade de certificação (CA) válida validou o certificado.

Transferência de chaves: uma vez que o cliente verifica e autêntica o servidor, é hora de ambas as partes compartilharem suas chaves. Após a verificação do servidor, o cliente usa a

chave pública para gerar uma chave pré-mestra. Em seguida, essa chave pré-mestra é enviada ao servidor. O servidor descriptografa essa chave pré-mestra usando sua chave privada. Desta forma, uma nova chave é calculada pelo cliente e pelo servidor. Este é um exemplo de criptografia assimétrica. Essa chave mestra é usada para criptografar e descriptografar as informações transferidas entre o cliente e o servidor. Isso é chamado de criptografia simétrica. Assim, ambas as técnicas de criptografia são implantadas para garantir uma conexão segura. Como ilustra a figura abaixo:

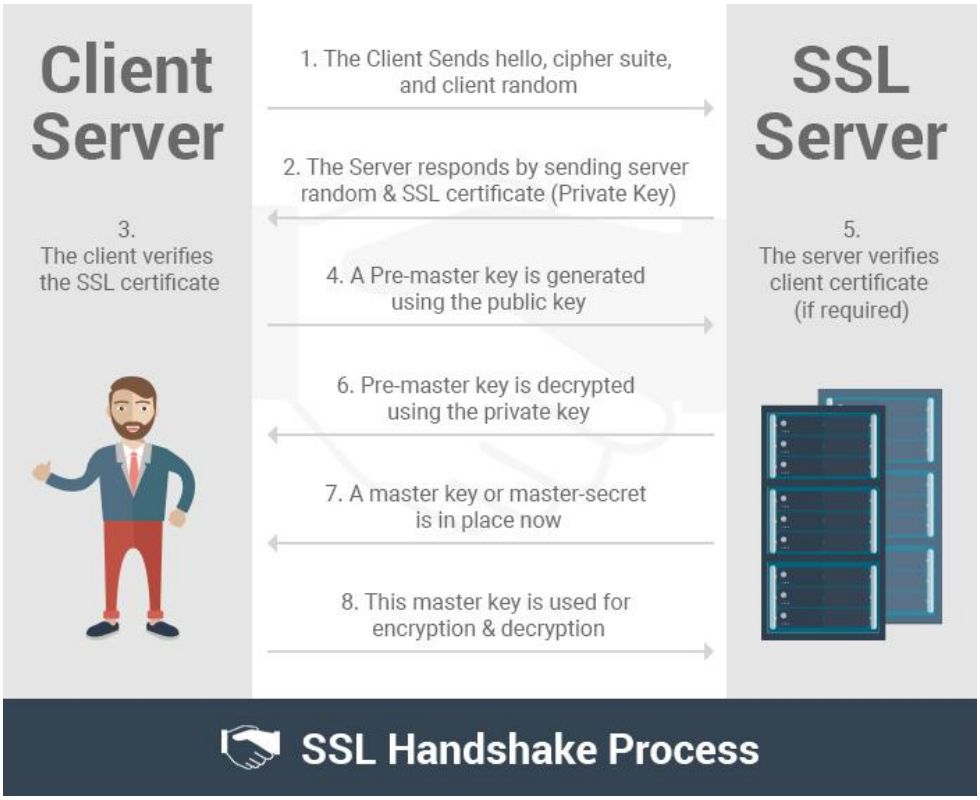


Figure 4.7: Handshake process

Fonte: https://dzone.com/articles/what-is-ssl-how-do-ssl-certificates-work

Dados protegidos por SSL são sempre transmitidos em um formato que incorpora um *checksum* criptográfico, e um identificador de segurança. Quando dois *hosts* iniciam uma sessão utilizando SSL, as mensagens iniciais utilizam um protocolo de *handshake* que estabelece os algoritmos de criptografia e chaves criptográficas a serem utilizados.

Os certificados SSL devem ser utlizados em qualquer situação em que as informações precisem ser transmitidas em segurança.

- Comunicações entre o seu site e os navegadores de internet dos seus clientes.
- Comunicações internas em sua intranet corporativa.
- Comunicações por e-mail enviadas de/e para sua rede (ou endereço de e-mail particular).
- Informações entre servidores internos e externos.
- Informações enviadas e recebidas da IoT (Internet of Things) e dispositivos móveis

SSL (*Secure Sockets Layer*), ou Camada de Soquetes Segura, é um protocolo que fornece um serviço de segurança para dados transmitidos entre aplicações.

É implementado de modo a atuar como uma subcamada da camada Aplicação da arquitetura TCP/IP, posicionada entre esta e a camada Transporte. Dados específicos enviados por aplicativos que utilizam SSL são protegidos por técnicas de criptografia e autenticação, garantindo a integridade e a privacidade dos mesmos.

Figura 4.8 - Camada SSL

Uma vez que este protocolo garante a integridade dos dados enviados, é necessário que seja utilizado um protocolo de transporte confiável orientado a conexão, como o TCP, a fim de garantir que não haja erros de transmissão.

O SSL fornece um serviço de comunicação segura entre cliente e servidor, permitindo autenticação mútua e garantindo integridade dos dados pelo uso de assinaturas digitais, e privacidade pelo uso de criptografia.

O protocolo foi projetado de modo a suportar diversos algoritmos de criptografia e assinatura digital, permitindo a seleção dos algoritmos mais convenientes para cada situação, assim como a utilização de novos algoritmos, a medida em que estes vão evoluindo. Estas escolhas são negociadas entre o cliente e o servidor durante o estabelecimento de uma sessão.

O termo *sockets* refere-se ao método utilizado para troca de dados entre programas cliente e um servidor em uma rede ou entre camadas de programas em um mesmo computador.

5.6.4. Os Impactos positivos que o SSL pode causar no cliente

O certificado SSL é uma garantia ao usuário de que ele está navegando em um ambiente digital totalmente seguro. Páginas web com a tecnologia SSL têm claros sinais visuais que notificam ao visitante que o site visitado é autêntico e confiável.

Quando um usuário visita um *site*, o navegador solicita ao servidor um certificado digital de forma automática. Se o certificado SSL é validado, as informações são criptografadas e é possível navegar normalmente.

Os dados só podem ser decifrados com uma chave de segurança especial. Assim, eles não podem ser interceptados no meio do caminho, tal qual um cofre de segurança que um invasor com más intenções não sabe o código para abri-lo.

Se o certificado não for validado, surge, então, na tela do internauta, uma notificação alertando-o. Dessa forma, o visitante tem a possibilidade de encerrar a sessão ou seguir navegando por sua própria conta e risco.

Como visto ao longo do texto, o certificado SSL é uma necessidade para qualquer tipo de página web profissional. No caso de um e-commerce, é imprescindível ter essa forma de

autenticação para assegurar os clientes de que a loja virtual é realmente segura para compras. Além do fator de segurança, um site certificado leva vantagem no ranking em mecanismos de busca.

5.6.5. Características do SSL

Muitas pessoas não sabem, mas elas se deparam com o certificado SSL várias vezes enquanto estão navegando na internet. É bem fácil reconhecer a presença dele na web. Quando um site é protegido por esse certificado, ele apresenta dois elementos na sua barra de endereço. Um deles é a sigla “HTTPS” e o outro é um ícone no formato de cadeado. A sigla “HTTPS” aparece antes do endereço do site, enquanto o ícone do cadeado pode surgir ao lado da sigla ou, dependendo do caso, no final da barra de endereço. O HTTPS é o elemento conhecido pelos profissionais de programação como protocolo HTTP (Protocolo de Transferência de Hipertexto). O “S” no final designa o termo “Secure”.

Esse termo informa ao usuário que o site em que ele está acessando possui o certificado SSL. Ou seja, é um site seguro e as trocas de dados realizadas nele estão devidamente protegidas.

A principal área de atuação do certificado SSL são em sites como lojas virtuais e de bancos. Tais sites apresentam a realização de trocas de dados importantes e sigilosos, tais como senhas, RG e CPF dos usuários.

5.6.6. Por que é necessário SSL?

A *Kaspersky Lab* identificou aumento de 43% em 2018 na incidência de ataques com vírus *ransomware*. É aquele que se apropria das informações da empresa e cobra resgate para devolver o acesso a elas. Um dos episódios mais famosos ficou conhecido como *WannaCry*, fazendo mais de 170 milhões de vítimas. Veja como é importante ter um SSL é essencial para proteger informações sensíveis. Entre elas, nomes de usuário, senhas e informações de pagamento. Mas há outras razões que valem ser citadas:

- Você ganha vantagem competitiva ao mostrar que tem um site confiável e legítimo;
- Aumenta a confiança dos visitantes, que se sentem mais seguros ao acessá-lo;
- Reduz o risco de imprevistos, porque ninguém vai poder acessar os dados dos usuários;
- O SSL melhora o tempo de carregamento e, assim, o desempenho das páginas;
- Seu site será mais bem posicionado em mecanismos de busca, como o Google, que favorecem sites seguros;
- Estará atendendo às exigências do PCI (*Payment Card Industry*) para que possa oferecer pagamentos via cartão de crédito.

CAPÍTULO VI

6. CONCLUSÕES E RECOMENDAÇÕES

6.1 Conclusões

Com a elaboração deste trabalho, foi possível observar algumas questões básicas de segurança que devem estar presentes em uma implementação deste tipo de rede. Como a rede definida por software foi toda ela desenvolvida em cima de protocolos públicos, ou seja, abertos, permite que diferentes organizações tenham acesso a rede. Diferentes níveis de acesso são necessários, pois diferentes agentes podem interagir com a configuração da rede. Além disso, por se tratar de padrões abertos e conhecidos, a fim de facilitar a integração por diferentes fabricantes, permite que atacantes conheçam toda a arquitetura e comandos. Uma vez invadida, o atacante torna-se capaz rapidamente e facilmente ter controle, podendo manipular a rede, os nós, e até usuários individuais.

A Implementação de um de um forte protocolo de segurança na rede do Instituto Superior Politecnico é Importante. O protocolo de segurança Secure Socket Layer (SSL), poderá ser uma solução viável no combate a ataques de pessoas mal intecionadas na rede do Instituto Superior Politecnico, pois o SSL permite que os dados enviados sejam protegidos por técnicas de criptografia e autenticação, garantindo a integridade e a privacidade dos mesmos. O SSL fornece um serviço de comunicação segura entre cliente e servidor, permitindo autenticação mútua e garantindo integridade dos dados pelo uso de assinaturas digitais, e privacidade pelo uso de criptografia.

Actualmente o IST tem usado o protocolo de segurança Ipsec e WAp para proteger a rede do IPS, pois este protocolo oferece autenticação, integridade e criptografica dos dados, mas com a implementação do protocolo SSL na rede do IPS permitirá ter uma rede mais segura, pois para além de oferecer autenticação que identifica a fonte dos dados, a integridade que garante que dados não foram indevidamente alterados e a criptografia que garante a privacidade dos dados, o protocolo SSL também oferece a troca de chaves criptográficas que aumenta a segurança do mecanismo de criptografia utilizado e também oferece sigilo. a criptografia é feito nos níveis

superiores o que permite ter segura em toda a rede. E isso permitirá ter uma rede mais segura, de modo que os dados possam fluir de na rede de forma segura, e em caso de tentativa de invasão por parte dos invasores a rede não será comprometida.

6.2 Recomendações

- ✓ Criar mecanismos de controle da rede definidas por software de modo a colmatar a vulnerabilidade na rede;
- ✓ Implementar o protocolo da Camada de Soquetes Segura de modo a proteger os dados que são trocados entre os usuários;
- ✓ Identificar todos as deficiências na rede definida por software com o intuito de soluciona-los;

7. REFERÊNCIAS BIBLIOGRÁFICA

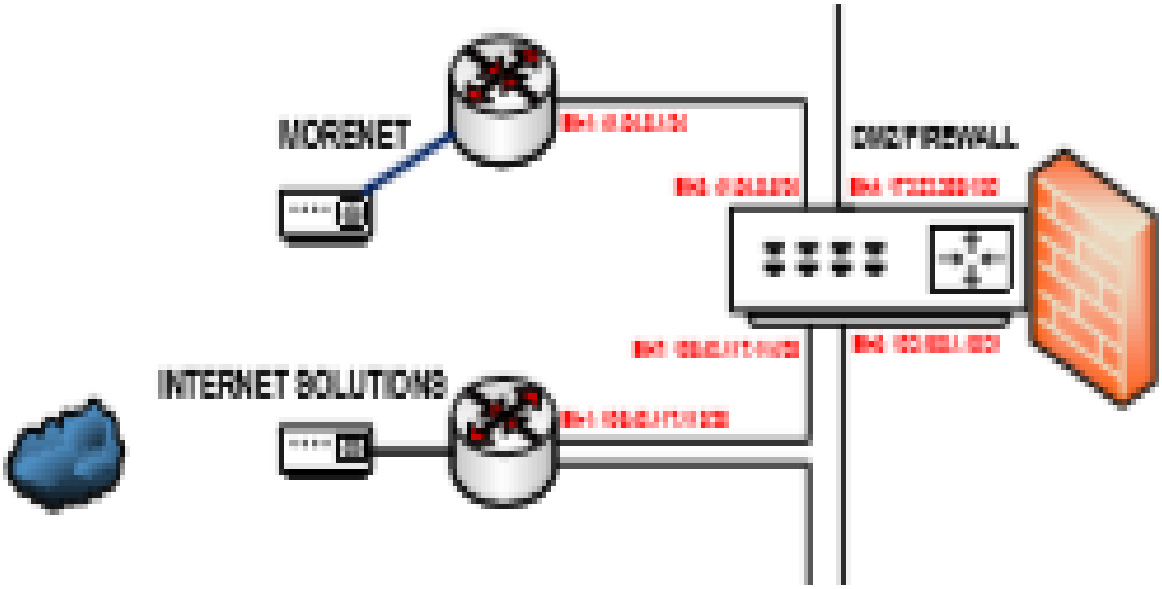
- Carneiro, A. (2002) *Introdução á Segurança dos Sistema de Informação*. Lisboa: FCA-Editora de Informática
- DANTAS, Marcus L. (2011) *Segurança da Informação*: Uma Abordagem Focada em Gestão de Riscos. Lisboa: Portugal.
- Kurose, J e Ross, K. (2010) *Redes de Computadores e a Internet*: Uma abordagem top-down. São Paulo: Addison Wesley.[5 edição].
- Stallings, w. (2008) *Criptografia e Segurança de rede*: princípios e práticas. São Paulo. [4ª edição].
- Tanenbaum, Andrew S. e Wetherall, D. (2011) *Redes de Computadores*: comunicação de dados. São Paulo: Pearson Prentice Hall.[5ª edição].
- Ataques - https://www.gta.ufrj.br/grad/13_1/dos/ataques.html
- Antivirus e Segurança - https://tecnoblog.net/299805/o-que-e-spoofing/
- Dissertação.pdf - https://app.uff.br/riuff/bitstream/1/3939/1/Henrique_Fernandes%20Disserta%C3%A7%C3%A3o.pdf
- Os cinco tipos de worms de computadores - https://softwarelab.org/pt/worm-informatico/
- O que é SSL e qual é a sua importancia? - https://www.escoladeecommerce.com/artigos/o-que-e-ssl-e-qual-e-a-importancia-dele-para-o-meu-e-commerce/
- O que é WAP? - https://www.speedcheck.org/pt/wiki/wpa/
- Protocolos de Criptogafia - http://uab.ifsul.edu.br/tsiad/conteudo/modulo5/src/ua/1/5.html
- https://www.monografias.com/pt/trabalhos3/redes-definidas-software/redes-definidas-software2.shtml
- Provendo segurança em redes definidas por software através da integração com sistemas de detecção e prevenção de intrusão - https://app.uff.br/riuff/bitstream/1/3939/1/Henrique_Fernandes%20Disserta%C3%A7%C3%A3o.pdf

- Redes definidas por software pode ser o pesadelo de segurança?- https://computerworld.com.br/2015/02/27/rede-definida-por-software-pode-ser-o-pesadelo-de-seguranca/
- Redes definidas por software (Software Defined Network) SDN- http://www.decom.ufop.br/imobilis/redes-definidas-por-software-software-defined-networks-sdn/
- https://repositorio.ufsc.br/bitstream/handle/123456789/171402/monografia_tcc_paulo_centeno.pdf?sequence=1&isAllowed=y
- Redes definidas por software - Cisco - https://www.cisco.com/c/pt_br/solutions/software-defined-networking/overview.html#~stickynav=4
- Software Defined Network - Https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/SDN/motivation.html
- Redes definidas por software - https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-vf/sdn/
- https://comum.rcaap.pt/bitstream/10400.26/17342/1/SDN_Um%20conjunto%20de%20boas%20pr%C3%A1ticas.pdf
- Redes Definidas por Software - http://www2.decom.ufop.br/imobilis/redes-definidas-por-software-software-defined-networks-sdn/
- Redes Definidas por Software – Monografias.com - https://www.monografias.com/pt/trabalhos3/redes-definidas-software/redes-definidas-software2.shtml
- Redes Definidas por Software - https://www.monografias.com/pt/trabalhos3/redes-definidas-software/redes-definidas-software.shtm
- Redes definidas por software pode ser um pesadelo a segurança? https://computerworld.com.br/seguranca/rede-definida-por-software-pode-ser-o-pesadelo-de-seguranca/
- https://pt.strephonsays.com/ipsec-and-vs-ssl-13145
- Redes definidas por software - http://www2.decom.ufop.br/imobilis/redes-definidas-por-software-software-defined-networks-sdn/

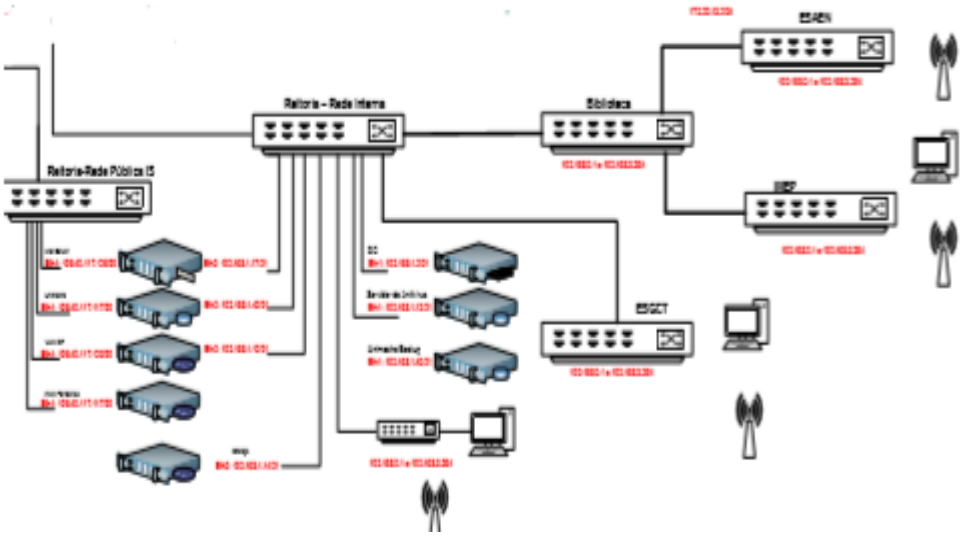
- SDN: Uma nova forma de pensar negócios – TI Especialistas - https://www.tiespecialistas.com.br/sdn-uma-nova-forma-de-pensar-negocios/
- SDN-SoftwareDefinedNetwork https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/SDN/security.html
- SDN: uma nova forma de pensar negócio - https://www.tiespecialistas.com.br/sdn-uma-nova-forma-de-pensar-negocios/
- SDN - https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/SDN/index.html
- SSL (Secure Socket Layer) – https://www.gta.ufrj.br/seminarios/semin2000_1/ssl/funcionamento.htm
- SSL (Secure Socket Layer)- https://www.gta.ufrj.br/seminarios/semin2000_1/ssl/introducao.htm
- Security Socket Layer TransportLayerSecurity- https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/Seguranca/conteudo/SSL-TLS/Como_funciona-o-SSL.html#post
- SSL: o que significa e qual é a importancia para o seu site - https://neilpatel.com/br/blog/ssl-o-que-e/
- https://repositorio.ufmg.br/bitstream/1843/ESBF-8XFMCK/1/rog_riovinhal.pdf
- Uma analise de seguranca de redes definidas por software sobre o protocol OpenFlow - https://core.ac.uk/download/pdf/78552339.pdf
- Versão_final_TCC_SBC.pdf - https://repositorio.ufsc.br/bitstream/handle/123456789/202491/VERSAO_FINAL_TCC_SBC.pdf?sequence=1
- What is SSL? - https://www.globalsign.com/pt-br/ssl-information-center/what-is-ssl/

8. ANEXOS: Rede do IPS

Provedor de Internet



Zona Publica e Privada da rede



Redes Wireless