UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ELDER THIAGO COSTA MOREIRA

# ESTUDO DE CASO DA IMPLANTAÇÃO DE CONTROLE DE ACESSO SEGURO PARA AS REDES SEM FIO ABERTAS NA UNIVERSIDADE FEDERAL DO PARÁ

Belém
2017

ELDER THIAGO COSTA MOREIRA

# ESTUDO DE CASO DA IMPLANTAÇÃO DE CONTROLE DE ACESSO SEGURO PARA AS REDES SEM FIO ABERTAS NA UNIVERSIDADE FEDERAL DO PARÁ

Trabalho de conclusão de curso de graduação apresentado ao Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.
Orientador: Professor Dr. Raimundo Viégas Junior

Belém

2017

ELDER THIAGO COSTA MOREIRA

# ESTUDO DE CASO DA IMPLANTAÇÃO DE CONTROLE DE ACESSO SEGURO PARA AS REDES SEM FIO ABERTAS NA UNIVERSIDADE FEDERAL DO PARÁ

Trabalho de conclusão de curso de graduação apresentado ao Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.
Orientador: Professor Dr. Raimundo Viégas Junior

Conceito: _____

**BANCA EXAMINADORA**

_____
Prof. Dr. Raimundo Viégas Junior
Orientador

_____
Esp. Edson Lucas da Silva Dias
Coorientador

_____
MSc. Fiterlinge Martins de Sousa
Examinador 1

_____
Prof. Dr. Eloi Luiz Favero
Examinador 2

## DEDICATÓRIAS

Dedico este trabalho primeiramente, a Deus que me deu a oportunidade de iniciar este curso e pelas forças para concluí-lo e a minha Mãe Norma, meu Pai José, minha irmã Elane e minha Bisavó Maria, pois confiaram em mim e me deram esta oportunidade de concretizar e encerrar mais uma caminhada de minha vida. Sei que eles não mediram esforços para que este sonho se realizasse, sem a compreensão, ajuda e confiança deles nada disso seria possível hoje. A eles além da dedicatória desta conquista dedico a minha vida, pois se hoje estou aqui, devo muitas coisas a eles por seus ensinamentos e valores passados. Obrigado por tudo!

Aos meus amigos, que me apoiaram e que sempre estiveram ao meu lado durante esta longa caminhada, em especial meus amigos Alisson e Robson, que muitas vezes compartilhei momentos de tristezas, alegrias, angústias e ansiedade, mas que sempre estiveram ao meu lado me apoiando e me ajudando. Não poderia deixar de dedicar a estas pessoas especiais em minha vida, amigos fundamentais em minha vida, sempre me escutando e me apoiando. A vocês meus amigos dedico este trabalho e todo meu carinho.

E por último, porém não menos importante, Tainara à você quero dedicar e agradecer este, pois sem sua ajuda, confiança e compreensão, meu sonho não teria sido realizado, você foi fundamental porque sempre dispôs de paciência em momentos que estive em crise existencial, me deu a mão quando o jogo estava perdido, você aturou diversos surtos quando as soluções não eram claras. No fim dedico este grande feito em minha vida.

Vocês são tudo para mim! Muito obrigado por tudo!

## AGRADECIMENTOS

À Universidade Federal do Pará, por ter proporcionado ensino de qualidade e excelente formação acadêmica.

Ao CTIC pelo incentivo, apoio e infraestrutura para o desenvolvimento e conclusão deste projeto. Um agradecimento especial aos amigos da Coordenadoria de Segurança e Serviços de Internet por todo o esforço e dedicação para manter e melhorar o CTIC e consequentemente a UFPA.

Ao Profº. Dr. Raimundo Viégas Junior, orientador, professor e amigo, muito obrigado pela dedicação e ajuda por esses meses de trabalho.

Muito obrigado aos meus amigos Lucas Dias, Rafael Martins e Rômulo Albuquerque pelo aprendizado e dedicação por esses meses que trabalhamos juntos, e também pela compreensão e profissionalismo.

Um agradecimento muito especial aos meus queridos amigos, companheiros e irmãos da turma de 2011 e agregados do curso de Sistemas de Informação da Universidade Federal do Pará.

E finalmente, agradeço a todos que me ajudaram direto ou indiretamente para o desenvolvimento deste projeto. Um muito obrigado a todos vocês!

## EPÍGRAFE

**“**Então, se você sente como se estivesse em um buraco negro, não desista. Sempre existe uma forma de sair. ”

Stephen Hawking

## RESUMO

A Universidade Federal do Pará, como instituição de ensino, oferece o serviço de rede sem fio aberta para visitantes. Porém, para que esse seja fornecida de forma adequada é necessário que tenha alguns cuidados de segurança, com o propósito de evitar práticas virtuais ilícitas dentro do domínio institucional. Este trabalho tem como escopo apresentar uma proposta de reestruturação da rede sem fio visitante da Universidade Federal do Pará, demonstrando através de implantação e utilização do software PacketFence, a gestão acesso dos usuários e dispositivos, para que seja possível controlar e/ou identificar os acessos dos usuários que na rede adentram, adequando-se às leis do país. A ausência dos registros de conexão e informações pessoais se configura como incidentes de inimputabilidade da informação, sendo assim, a instituição torna-se responsável pelos atos ocorridos em sua rede. Usando dos recursos tecnológicos é possível que particularidades como estas sejam tratadas e, assim, sendo garantir os previstos nos artigos da Lei 12.965, de 23/04/2014 Marco Civil da Internet ou Marco Regulatório da Internet.



Palavras-Chave: Gestão de Rede Sem Fio; Captive Portal; Controle de Acesso; Marco Civil da Internet.

**ABSTRACT**

The Federal University of Pará as educational institution offers an open wireless network service to the visitors. However, in order to provide this service in an appropriated manner, some security measures are needed, aiming to avoid illicit virtual practices inside of the institutional domain. This study aims to present a proposal for reconstructing the wireless visitor network of the Federal University of Pará through to deployment and use of the PacketFence software, which manages the users' access and devices in order to be possible to control and/or identify the access of the users of this network, adapting to the laws of the country. The absence of connection record and personal information is configured as incidents of imputability of information, so that the institution becomes responsible for any acts occurred inside of its network. Using this technological resource is possible to treat this particularity and then ensure those provided in the article of the law 12.965, from 23/04/2014, Civil Internet Framework or Regulatory internet framework.
Key-words: Management of wireless network, Portal Captive, Control of access; Civil Internet Framework.

## LISTA DE ABREVIAÇÕES

ANSI - *American National Standards Institute*

AP - *Access Point*

ASF - *Advanced Systems Format*

BSD - *Berkeley Software Distribution*

CERT - Centro De Estudos Para Resposta E Tratamento De Incidentes Em Computadores

CGI - Comitê Gestor Da Internet

CPF - Cadastro De Pessoas Físicas

CSSI - Coordenadoria De Segurança E Serviços De Internet

CTIC - Centro De Tecnologia Da Informação E Comunicação

DHCP - *Dynamic Host Configuration Protocol*

DNS - *Domain Name System*

DSO - *Data Source Object*

FTP - *File Transfer Protocol*

HBO - *Home Box Office*

HTTP - *Hypertext Transfer Protocol*

ID - *Identity*

IEEE - *Institute Of Electrical And Electronics Engineers*

IES - Instituto De Ensino Superior

INC - *Incorporation*

IP - *Internet Protocol*

IPV4 - *Internet Protocol Version 4*

IPV6 - *Internet Protocol Version 6*

ISP - *Internet Service Provider*

MAC - *Media Access Control*

MD5 - *Message Digest Algorithm 5*

MIB - *Management Information Base*

NAT - *Network Address Translation*

NOSQL - *Not Only SQL*

P2P - *Peer To Peer*

PIN - *Personal Identification Number*

QOS - *Quality Of Service*

RNP - Rede Nacional De Ensino E Pesquisa

SGBD - Sistema De Gerenciamento De Banco De Dados

SMS - *Short Message Service*

SNMP - *Simple Network Management Protocol*

SQL - *Structured Query Language*

SSH - *Secure Shell*

SSL - *Secure Socket Layer*

TCP - *Transmission Control Protocol*

TI - Tecnologia Da Informação

TIC - Tecnologias Da Informação E Comunicação

UFPA - Universidade Federal Do Pará

VLAN - Virtual Local Area Network *Wireless Local Area Network*

VM - *Virtual Machine*

WIFI - *Wireless Fidelity*

WLAN - *Wireless Local Area Network*

WPA2 - *Wifi Protected Access*

## LISTA DE FIGURAS

# LISTA DE TABELAS

**SUMÁRIO**

# 1. INTRODUÇÃO

Desde a sua criação, a informática, em conjunto com os avanços das telecomunicações, foi um dos principais fomentadores do desenvolvimento tecnológico (TANENBAUM, 2011). Como resultante, diferentes e avançados dispositivos estão sendo criados em larga escala, capazes de processar, transmitir dados, imagens, vídeos e sons, acessar em banda larga aos sistemas corporativos e à Internet, utilizando redes cabeadas e sem fio (ou móvel) (KUROSE e ROSS, 2013). A rede sem fio, por exemplo, tem propiciado a redução dos custos de equipamentos e no aumento da capacidade de conexões (FLICKENGER, 2008).

A popularização das redes sem fio, também chamada *Wireless* ou *Wifi*, vai além do investimento financeiro, onde uma rede sem fio pode ser implantada com custo muito baixo, comparada a estruturas cabeadas, isto é, devido à mobilidade geográfica e a portabilidade dos dispositivos existentes - *laptops*, celulares, tablets etc. (KUROSE e ROSS, 2013).

GONÇALVES e FERREIRA (2012) descrevem sobre a indispensabilidade de estar conectado à Internet estimulando a adoção de medidas locais para converter espaços sociais em ambientes de conexão permanente; e tais ações favorecem a construção de redes coletivas que abrangem, geograficamente, as atuais condições de mobilidade. Tal argumentação explica a razão das redes sem fio estarem presente no cotidiano, em ambientes acadêmicos, empresariais, residenciais e públicos, como: hotéis, restaurantes, bares, em meios de transportes como: carros, ônibus, trens, navios, aviões, entre outros.

No Brasil, o avanço das redes sem fio, públicas ou privadas, acompanha o ritmo mundial. Em 2014, o país conquistou o 8º lugar em número de *hotspots Wifi*, com mais de 1,6 milhões de *hotspots* comerciais, residenciais e comunidade (IPASS, 2017). Em 2017, já se totalizam 8,6 milhões de áreas *Wifi* pelo Brasil (IPASS, 2017). A exemplo de instituições que utilizam o controle de acesso, encontram-se a rede de cafeterias Starbucks, que fornece acesso ilimitado e gratuito em todas as suas lojas mediante cadastro de usuário (STARBUCKS, 2017) e o Aeroporto Internacional de Guarulhos, por meio da Boingo *Wireless*, fornece acesso à internet mediante cadastro e pagamento, após os primeiros trinta minutos de acesso gratuito (SINDIGRU, 2014).

Em virtude desse crescimento, as instituições estão a oferecer o serviço de *hotspot* como um diferencial de negócio, porém, para que esse seja fornecida de forma satisfatória é necessário que tenha adaptações às legislações vigentes para que não ocorram incidentes de inimputabilidade da informação.

## 1.1. JUSTIFICATIVA

A tecnologia *wifi*, presente nos mais variados tipos de dispositivos, permite ao usuário estar constantemente conectado, seja por uma rede aberta ou por uma rede de fácil e/ou conhecida autenticação, em parques, *shoppings*, aeroportos, universidades dentre outros.

Para o usuário, características como flexibilidade e mobilidade colaboram para sucesso e expansão na utilização das redes sem fio (CARDOSO, 2006). Porém, para aqueles que provêm o meio de acesso *wireless*, a segurança e rastreabilidade são aspectos fundamentais para a continuidade do fornecimento do serviço (RUFINO, 2015).

Muitas instituições de ensino superior (IES), tanto públicas quanto privadas, disponibilizam o acesso à Internet (cabeada ou sem fio) para a comunidade acadêmica. Podendo essa ser restrita aos participantes ou aberta para uso geral. A exemplo disso temos a Universidade Federal do Rio Grande do Sul (UFRGS) fornecendo rede aberta ao colegiado e a Universidade Estadual de Campinas (UNICAMP), que fornece rede sem fio mediante a cadastro prévio.

No contexto das redes abertas, entra em discussão questões relativas à segurança e o atendimento a legislação vigente: é preciso haver controle sobre aspectos que vão desde os registros de conexão e acesso até os direitos e garantias sobre inviolabilidade da vida privada como previsto nos artigos da Lei 12.965, de 23/04/2014, é referida como Marco Civil da Internet ou Marco Regulatório da Internet.

## 1.2. MOTIVAÇÃO

A rede de acesso *wireless* da Universidade Federal do Pará (UFPA) é destinado a toda comunidade por meio de duas conexões: Institucional e Visitante (CTIC, 2016b).

- **Institucional:** Destinado a comunidade acadêmica. Para o usuário acessar essa rede sem fio é necessário possuir um *e-mail*, previamente cadastrado, da instituição, este será utilizado como credenciais para realizar a autenticação.
- **Visitante:** Destinado a comunidade geral, com ou sem vínculo com a instituição. Rede sem fio aberta, onde não necessita de autenticação. Apesar de fornecidas pela UFPA, a rede visitante não faz acesso a rede interna da instituição.

A figura 1 mostra a atual arquitetura da rede sem fio da Universidade Federal do Pará.

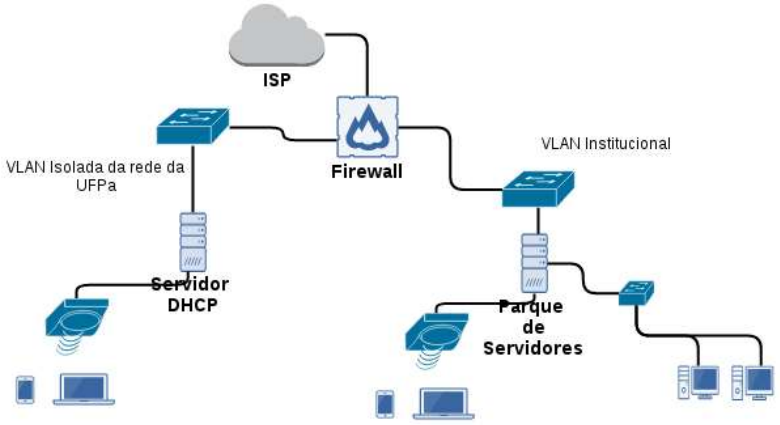



Figura 1 - Organização da rede sem fio da UFPA.
Fonte: CTIC, 2016a.

A partir do que foi descrito, conclui-se que a instituição provê serviço de rede sem fio aberta, onde não é possível controlar e/ou identificar os acessos dos usuários que nela adentram. Isto pode facilitar práticas virtuais ilícitas dentro do domínio institucional, como também, na ausência do usuário infringente, tornar o órgão responsável pelas devidas atividades irregulares (BRASIL, 2015).

## 1.3. OBJETIVO GERAL

Este trabalho visa à implantação de uma rede *wireless* de acesso livre e rastreável na Universidade Federal do Pará (UFPA), utilizando a ferramenta de controle de acesso e *captive portal* PacketFence operando adequadamente dentro da regulamentação do Marco Civil da Internet.

## 1.4. OBJETIVOS ESPECÍFICOS

- Realizar um estudo sobre redes sem fio e controle de acesso;
- Realizar levantamento sobre a implantação de redes wireless com *hotspot* em Instituições de Ensino Superior (IES);
- Realizar um estudo sobre o Marco Civil da Internet e legislações relacionadas;
- Propor uma solução de controle de acesso otimizada na rede da UFPA.

## 1.5. CONTRIBUIÇÕES DO TRABALHO

Este trabalho tem como finalidade propor uma alternativa ao modelo atual de rede sem fio aberta da Universidade Federal do Pará, no qual cumpra com os descritos legais previstos no Marco Civil da Internet e em outras legislações vigentes. Podendo assim, preencher as lacunas existentes no que diz respeito as falhas de segurança da rede atual, o projeto utiliza de *software* livre capaz de prover uma solução de acesso autenticado, flexível e acessível atendendo a comunidade visitante que frequenta o campus universitário e ao mesmo tempo facilitando o tratamento de quaisquer incidentes de inimputabilidade da informação.

## 1.6. ORGANIZAÇÃO DO TRABALHO

O capítulo 1 faz uma introdução aos avanços tecnológicos e descreve, brevemente, o cenário atual, expondo suas problemáticas. Também são traçados os objetivos pretendidos, além de apresentar as contribuições do trabalho.

O capítulo 2 é feita a fundamentação teórica para dar base ao trabalho, apresentando e explicitando as principais técnicas e ferramentas.

O capítulo 3 trata dos trabalhos relacionados, agrupando projetos com soluções disponíveis que exploram os conceitos semelhantes e apresentação de um breve levantamento sobre as redes sem fio em outras instituições de ensino superior.

A metodologia de ensino da proposta, o capitulo 4, ilustra o estudo de caso no Centro de Tecnologia de Informação e Comunicação (CTIC) e o cenário atual com mais profundidade.

O capítulo 5, apresenta-se a proposta, explorado com maior detalhamento o PacketFence, demonstrando suas características, componentes e as vantagens de sua utilização. Também, destaca-se a realização de teste e exibição dos resultados obtidos em conformidade com os objetivos.

# 2. REFERENCIAL TEÓRICO

## 2.1. REDE SEM FIO

Proporcionalmente ao crescimento da utilização de dispositivos móveis de comunicação e computação, está o crescimento da demanda em conectá-los à Internet (TANENBAUM, 2011). A rede sem fio possui como principal tecnologia, a família de protocolos IEEE 802.11 (WNDW, 2008), que permite uma maior mobilidade e redução de custo em relação às redes tradicionais, porque sua instalação é mais simples e rápida (RNP, 2010).

### 2.1.1. Arquitetura

A arquitetura da rede sem fio possui duas topologias distintas, porém, compartilham características em comum: Topologia AD-HOC e Infraestrutura (KUROSE e ROSS, 2013).

Conforme TANENBAUM (2011), os clientes da rede AD-HOC (b) se comunicam sem a utilização de cabos, apenas por placas *wireless*. Cada *host* é capaz de transmitir e receber informações da rede que pertence. Nas redes de Infraestrutura (a), a comunicação entre os dispositivos ocorre por meio de um *Access Point* (AP). A figura 2 ilustra ambas topologias.

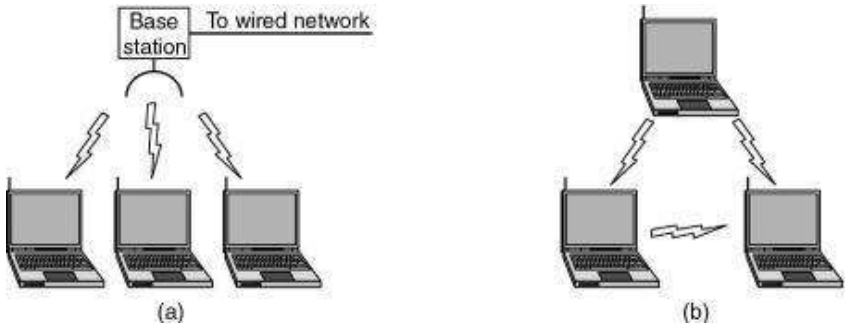



Figura 2 - (a) Rede sem fio conectado a um AP. (b) Rede AD-HOC
Fonte: TANENBAUM, 2011

### 2.1.2. Características

As redes sem fio apresentam características que as tornam atrativas, se compararmos à uma infraestrutura cabeada, destacam-se: flexibilidade, mobilidade e baixo custo de implantação (ISHIKIRIYAMA, 2006):

- **Flexibilidade:** Dentro da área do AP, um *host* pode se comunicar sem nenhum impedimento, além de, permitir que a rede alcance locais não acessíveis por meio de

cabos.

- **Mobilidade:** Permite que os usuários se desloquem para qualquer local, dentro da área de cobertura, sem perda de conexão.
- **Baixo custo:** Por não necessitar de cabos, o custo de investimento em uma rede sem fio é mais baixo. Além disso, o tempo de implantação também é reduzido.

## 2.2. PROTOCOLOS

### 2.2.1. TCP/IP

O Protocolo de Controle de Transmissão (TCP) e o Protocolo de Internet (IP) são considerados os protocolos mais importantes da Internet (KUROSE e ROSS, 2013), sendo este último, responsável por especificar o formato do protocolo que são enviados e recebidos entre os roteadores e sistemas finais.

**a) TCP**: O protocolo foi desenvolvido para fornecer, de maneira confiável, um fluxo de *bytes* entre *hosts*, em uma inter-rede não confiável (TANENBAUM, 2011). O TCP é o protocolo orientado para conexão, pois antes que o processo de aplicação possa iniciar, os processos envolvidos devem enviar segmentos preliminares um ao outro para definir parâmetros da transferência (KUROSE e ROSS, 2013). O estabelecimento de conexão TCP pode ocorrer em condições normais ou com colisão entre chamadas, por meio de *handshake*, ilustrada na figura 3.

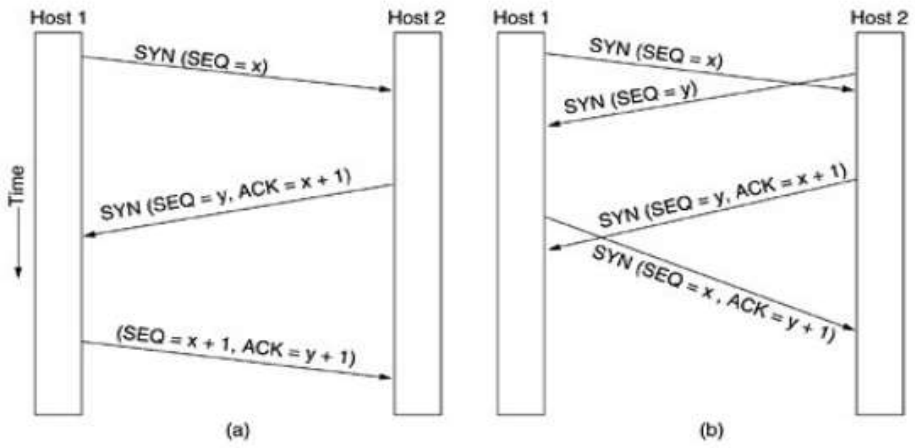



Figura 3 - (a) Estabelecimento de uma conexão TCP em condições normais. (b) Colisão entre chamadas.
Fonte: TANENBAUM (2011).

Tanenbaum (2011), descreve o estabelecimento de conexão em condições normais - ilustrado na Figura 3 (a) - quando um processo, que está escutando a porta, recebe um segmento TCP de entrada, podendo aceitar ou recusar a conexão. Caso aceito, um segmento de confirmação é retornado. No caso de dois *hosts* tentarem estabelecer uma conexão entre os mesmos soquetes simultaneamente, ocorrerá a colisão entre chamadas - Figura 3 (b). Dessa maneira, apenas uma conexão será estabelecida.

**b) IP:** O protocolo IP foi projetado com o objetivo de interligar redes distintas. Na Internet, *hosts* e roteadores possuem um IP. Através da combinação dos IPs de origem e destino é possível criar uma rota que os comunique. O IP procura da melhor maneira possível, porém não garantida, transportar datagramas de origem para o destino. Nesse caso, a confiabilidade de administrar e garantir que os datagramas serão entregues na sequência correta é tarefa do TCP (TANENBAUM, 2011).

### 2.2.2. DHCP

O Protocolo Dinâmico de Configuração de *Host* (DHCP), do inglês *Dynamic Host Configuration Protocol*, possibilita os dispositivos conectados em uma rede de obterem informações TCP/IP (endereçamento, máscara de rede, roteamento, DNS) automaticamente (SOUZA e LOPES, 2011).

O DHCP tem sido muito utilizado por parte dos ISPs por permitir a atribuição de endereços IP temporários a seus clientes conectados. Desta forma, torna-se desnecessário obter um endereço para cada cliente, devendo-se apenas designar endereços dinamicamente, através de seu servidor DHCP. Este servidor terá uma lista de endereços IP disponíveis e toda vez que um novo cliente se desconectar, o endereço é devolvido (MOREIRAS, 2012).

Tanenbaum (2011) descreve que a atribuição automática de endereços IP de um *pool* é o tempo durante o qual um endereço IP deve ser alocado. Se um host deixar a rede e não retornar seu endereço IP ao servidor DHCP, esse endereço será perdido. Depois de um certo período, muitos endereços poderão se perder. Para evitar, a atribuição de IP pode se referir a um período fixo, uma técnica chamada arrendamento (*leasing*). Pouco antes de expirar o prazo de arrendamento, o *host* deve solicitar ao DHCP uma renovação. Se ele deixar de fazer uma solicitação ou se a solicitação for negada, o host não poderá mais usar o endereço IP que recebeu antes.

A) DHCP fingerprint

FINGERBANK (2016) define o *fingerprint* como uma impressão digital, um identificador do dispositivo cliente. Por meio desse valor é possível determinar o tipo e o Sistema Operacional do dispositivo que está conectado na rede. O DHCP *Fingerprint* combina o serviço DHCP com uma solução de controle de acesso à rede.

Após a conexão em uma rede, com fio ou *wireless*, o dispositivo solicita a descoberta de DHCP. Cada sistema operacional requisita as opções DHCP em uma sequência específica. Isso torna possível a impressão digital de DHCP (INFLOBOX, 2016). Além disso, a solicitação DHCP expõe ao servidor o endereço MAC do cliente. Os fornecedores dos aparelhos têm padrões de endereço MAC. Dessa forma, é possível identificar tipo e fabricante do dispositivo conectado (FINGERBANK, 2016).

O projeto FingerBank disponibiliza os identificadores já capturados. Estes identificadores se compilam em um banco, também, denominado *fingerbank* (SOUZA e LOPES, 2011). As informações são utilizadas por ferramentas de controle de acesso para conceder acesso de rede diferente com base no tipo de dispositivo ou por soluções baseadas na *Web* para diferenciar dispositivos móveis de computadores *desktop* (FINGERBANK, 2016).

### 2.2.3. Network Address Translation (NAT)

A NAT (*Network Address Translation*) foi uma das medidas desenvolvidas para resolver, ou minimizar, o problema dos esgotamentos dos endereços IPv4. Constitui-se, basicamente, vários dispositivos consigam trafegar na Internet através de um único endereço IP (BALCHUNAS, 2013).

O funcionamento é simples em uma rede, cada computador recebe um IP privado único, que é utilizado para roteamento do tráfego interno. Quando um pacote precisa ser roteado para fora da rede, uma tradução de endereço é realizada, convertendo os IP privados em endereços IPs públicos válidos (MOREIRAS, 2012). A figura 4 ilustra o processo de tradução realizado pelo NAT.

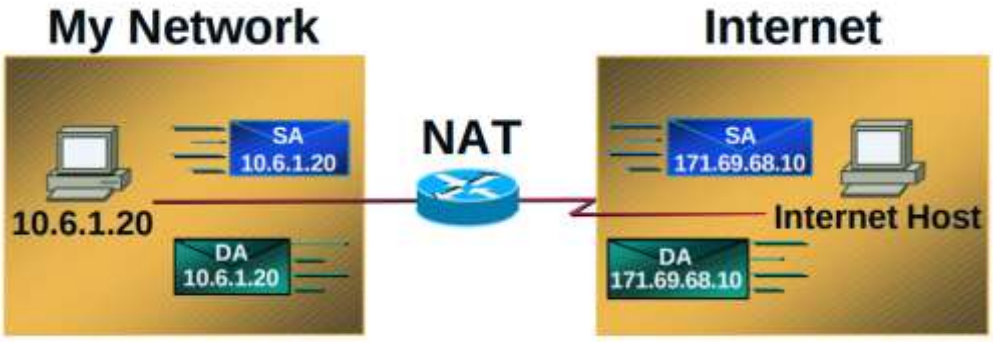



Figura 4 - Funcionamento do NAT
Fonte: Cisco Systems INC (2000)

O NAT permite que dispositivos com acesso particular acessem redes registradas (ex. Internet), sem exigir endereços IP únicos a nível mundial em *hosts* finais, traduzindo endereços IP privados para endereços IP registrados sempre que necessário (CISCO, 2000).

## 2.3. NETWORK ACCESS CONTROL (NAC)

Nos últimos anos, o aumento do número de dispositivos móveis que necessitam de acesso a redes corporativas, sendo estes membros ou não da organização, modificou a ideia de perímetro da rede. As requisições de acesso podem vir de qualquer pessoa e em qualquer lugar. Devido a isso, as organizações estão se voltando para as tecnologias de controle de acesso à rede (CZARNY, 2008).

As soluções de *Network Access Control* (NAC) protegem as redes corporativas implementando políticas que devem ser cumpridas por todos os dispositivos que se conectam à rede. Se um dispositivo não cumpre com as políticas, este não poderá interagir com outros elementos da rede até que se verifique o cumprimento das mesmas. A NAC concede acesso à rede considerando fatores como proteção *anti-malwares*, avaliação de *firewall* pessoal, autenticação de usuário, localização e, até mesmo o horário (CZARNY, 2008; IREO, 2017).

Por que universidades precisam da NAC? Segundo JUCC (2013), o setor de educação tem sido um grande cliente das soluções existentes NAC no mundo. A razão, segundo fornecedores, seria o grande número de dispositivos não gerenciados em faculdades e universidades. Os dispositivos são, principalmente, dos estudantes que precisam se conectar à Internet, de maneira segura, portanto as instituições de ensino e os responsáveis de TI precisam, de alguma forma, verificar se eles fornecem essa proteção.

I) Arquitetura para rede 802.1X

Uma rede 802.1X requer os seguintes três componentes para operar (JUCC, 2013):

**1. Agente NAC:** ele é carregado no dispositivo do usuário e é usado para solicitar acesso à rede.

**2. Dispositivo de rede NAC:** infraestrutura de rede utilizada para executar autenticação em, por exemplo, pontos de acesso sem fio.

**3. Servidor NAC:** recebe mensagens de autenticação remota no serviço de usuário (RADIUS) e as usa para verificar as credenciais de autenticação em um banco de dados de autenticação de *back-end*.

II) O Processo NAC

O NAC detecta primeiro o dispositivo que está se conectando à rede. Assim que reconhecido, o servidor NAC iniciará o processo de autenticação e avaliação de segurança. Se o dispositivo satisfizer a política de segurança definida da rede protegida, o acesso será concedido ao dispositivo de acordo com sua função ou identidade. Dispositivos considerados inseguros serão isolados em uma área em quarentena até que seja reintroduzida na rede e avaliada para atender aos requisitos de segurança. A correção pode ser sugerida pela solução NAC para o dispositivo de ponto final, dependendo do risco de tentativa maliciosa de acesso à rede (JUCC, 2013).

### 2.3.1. Hotspot

Genericamente, um *hotspot* é uma área que provê acesso à internet sem fio. Geralmente encontrados em lugares públicos, como aeroportos, hotéis, restaurantes, universidades (MICHIGAN, 2016).

Segundo MKT e LANCORE (2012), *hotspot* pode ser utilizado para conceder acesso controlado a uma rede, com ou sem fio, por meio de autenticação do usuário. Dentro da área de abrangência do *hotspot*, um dispositivo que solicita acesso à Internet é direcionado para a página do *hotspot (Captive Portal)* que solicita credenciais para continuar com a navegação *Web*. Quando autorizado, o usuário ganha acesso à Internet, podendo sua atividade ser controlada e enumerada.

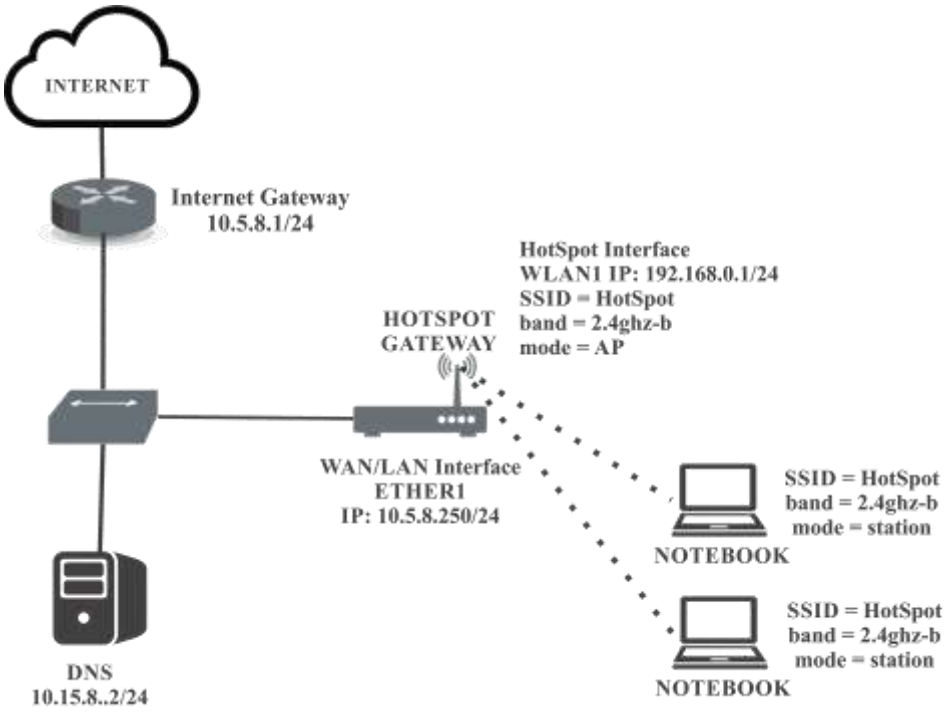



Figura 5 - Arquitetura Básica Hotspot
Fonte: Adaptado de MICHIGAN (2016).

### 2.3.2. Captive portal

O *Captive Portal* é uma ferramenta que permite forçar a autenticação ou o redirecionamento para uma página de autenticação para ter acesso à rede. Isso adiciona uma camada adicional de segurança em matéria de acesso sem fio (NETGATE, 2017).

SOUZA e LOPES (2011), descrevem *Captive Portal* como:

> Um *software* responsável por gerenciar o acesso à Internet em redes públicas, por exemplo, em locais como restaurantes, aeroportos, provedores de Internet sem fio, entre outros. *Captive portal* consiste de um aplicativo de *Firewall* que captura os pacotes do cliente e redireciona o tráfego para uma página *Web* que solicita uma autenticação. Através do uso do *Captive portal* é permitido limitar ou restringir o acesso à rede (SOUZA e LOPES, 2011, p. 12).

A Figura 6 ilustra a conexão de um usuário na rede que, por após de autenticação via *Captive Portal*, concede acesso à Internet.

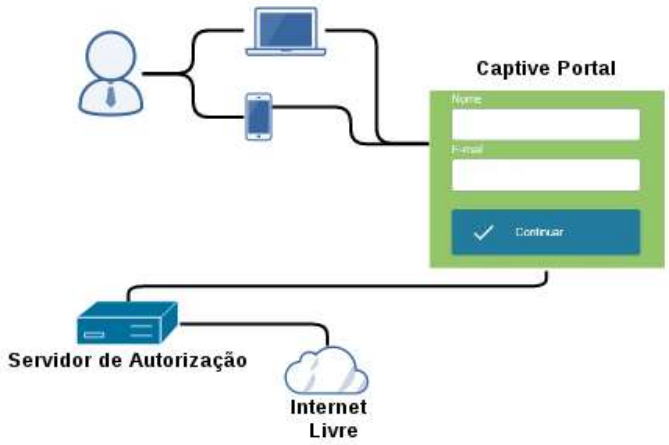



Figura 6 - *Captive Portal*
Fonte: Elaborado pelo autor (2017)

## 2.4. FERRAMENTAS DE CONTROLE

### 2.4.1. PacketFence

PacketFence é um software gratuito e uma solução código aberto (*Open Source*) para Controle de Acesso à Rede. Desenvolvida pela Inverse INC, PacketFence é uma ferramenta que possui inúmeras funcionalidades e pode ser efetivamente utilizado para proteger pequenas e grandes redes heterogêneas (INVERSE, 2017). Uma ferramenta ampla que conta com uma comunidade online para adição de contribuições e melhorias.

O PacketFence concede o acesso à rede para qualquer dispositivo ou usuário, somente após o mesmo ser registrado e autenticado por código enviado via SMS, fazendo com que se tenha uma maior segurança à rede e os dados da organização. Com a ferramenta é possível utilizar os seguintes recursos oferecidos: registro, detecção de atividades de rede anormal, *scans* de vulnerabilidade, isolamento de dispositivos problemáticos, 802.1X, integração sem fio e DHCP *fingerprinting* (INVERSE, 2017).

## 2.5. **ASPECTOS LEGAIS**

### 2.5.1. Marco Civil da Internet

O Marco Civil da Internet é a denominação para a Lei nº 12.965 de 23/04/2014. Considerada por muitos, como uma iniciativa que "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2015). A legislação reduziu a chamada

“insegurança política”, pois estabeleceu normas fixas para as diversas discricionariedades jurídicas geradas anterior a lei, devido à ausência de leis claras e pela baixa (ou mesmo falta) de intimidade com a própria Internet (RONCOLATO, 2013).

Um dos principais pontos da Lei 12.965/14 se refere a guarda dos registros de conexão dos usuários. Esta permite a identificação do usuário, permitindo legalmente seu monitoramento com as devidas restrições informadas no Marco Civil. O controle de registro de conexões facilita a investigação, por ordem judicial, de ilícitos.

Para entendimento, o artigo 5º do Marco Civil considera:

> Artigo 5º Para os efeitos desta Lei, considera-se:
>
> I - Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; [...]
> IV - Administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> V - Conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. (BRASIL, 2015).

O item IV do artigo 5º define o administrador de sistema autônomo como uma entidade (física ou jurídica) que gerencia um bloco de IP devidamente cadastrado no órgão de registro. Nesse caso, encaixa-se instituições públicas (Universidades, autarquias etc.) que oferecem conexão à Internet para comunidade.

A Universidade Federal do Pará (UFPA) disponibiliza acesso livre à Internet para a comunidade (alunos, professores, técnicos-administrativos e participantes em geral), por meio de rede sem fio. Logo, cabe a instituição monitorar e controlar os registros de conexão dos usuários participantes.

As garantias de guarda de registros de conexão estão definidas no artigo 13 do Marco Civil da Internet. Nele dispõem:

> Artigo 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3º Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2o, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3o.
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência (BRASIL, 2015).

Da responsabilidade por Danos gerados por Terceiros, ilustrados pelos artigos 18 e 19, definem sobre a devida incumbência das irregularidades originados por usuários e a não responsabilização do administrador do sistema:

> Artigo 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
> Artigo 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
> § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no artigo 5o da Constituição Federal.
> § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.
> § 4º O juiz, inclusive no procedimento previsto no § 3o, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação (BRASIL, 2015).

### 2.5.2. Lei nº 10.703 de 18/07/2003

Baseado na Lei 10.703 de 18 de julho de 2003, dispõe sobre o cadastramento de usuários de telefones celulares pelas prestadoras de serviço de telecomunicações. O artigo 1º delimita os dados solicitados para registro:

> Artigo 1º Incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários.
> § 1º O cadastro referido no caput, além do nome e do endereço completos, deverá conter:
> I - No caso de pessoa física, o número do documento de identidade ou o número de registro no cadastro do Ministério da Fazenda;
> II - No caso de pessoa jurídica, o número de registro no cadastro do Ministério da Fazenda (BRASIL, 2003).

Para solicitação dos dados cadastrados junto a operadora é necessária uma requisição judicial como informado no artigo 3º da lei em questão:

> Artigo 3º Os prestadores de serviços de que trata esta Lei devem disponibilizar para consulta do juiz, do Ministério Público ou da autoridade policial, mediante requisição, listagem das ocorrências de roubos e furtos de aparelhos de telefone celular, contendo nome do assinante, número de série e código dos telefones (BRASIL, 2003).

## 3. TRABALHOS RELACIONADOS

Este trabalho pretende descrever a implantação de uma solução de controle de acesso para a Universidade Federal do Pará, com o objetivo de se adequar as legislações vigentes no país. Semelhante a (OLIVEIRA e CUNHA, 2012) optou-se pela modificação da infraestrutura da rede padrão, por uma solução confiável, que atendesse os requisitos de segurança e de baixo custo de implantação. (SILVA e MENDES, 2016), propõem uma inserção de um *hotspot wireles*s com intuito de facilitar o acesso à informação a qualquer pessoa que possua um dispositivo *wifi* e esteja dentro do raio de cobertura da rede *wifi* da universidade estudada.

Segundo JUCC (2013), o âmbito acadêmico tem sido um grande utilizador das soluções de controle de acesso, juntamente com o governo, saúde e instituições financeiras. A razão, segundo a instituição, seria o grande número de dispositivos não gerenciados pertencentes, principalmente, aos estudantes.

Atualmente nas Instituições de Ensino Superior (IES), existe uma forte demanda pelo acesso sem fio, tanto para acesso aos sistemas internos à instituição quanto aos serviços externos tais como: *e-mail*, noticiários ou redes sociais. Cabe às Unidades Superiores de cada instituição definir o método de fornecimento do serviço de Internet *Wifi*.

A Tabela 1, descreve informações quanto ao fornecimento de Internet sem fios nas principais instituições de ensino superior do Brasil, detalhando a abrangência do fornecimento, a qual público se destina, o método de validação e autenticação do usuário na rede.

Analisando os dados da Tabela 1 abaixo, podemos obter informações que em nove das quatorze instituições que oferecem o serviço de rede sem fio aberta a todos, no entanto, apenas quatro das nove que são abertas a todos utilizam o método de autenticação do *captive portal*, que por sua vez apenas duas destas quatro usam como método de validação o uso do *SMS*.

**Tabela 1** - Comparativo IES x Métodos de Autenticação.

| Instituição | Abrangência | Validação | Autenticação |
|---|---|---|---|
| **UFBA** | Aberta a todos. | Não necessita credenciamento. | Rede Aberta |
| **UTFPR** | Aberta a todos. | Nome de usuário e senha previamente fornecidos pela COGETI do Campus ou pela DIRGTI. | WPA2-Enterprise |
| **PUC-RIO** | Aberto a todos. | A abertura da conta de usuário deverá ser feita no guichê de "Atendimento ao Usuário" | WPA2-Enterprise |
| **PUC-RS** | Aberto a todos. | O acesso será validado mediante a concordância com as políticas de acesso estabelecidas pela Universidade. | Captive Portal |
| **UNISINOS** | Aberto a todos. | Validação via SMS após cadastro pelo Captive Portal | Captive Portal |
| **UFF** | Aberto a todos. | Validação via SMS após cadastro pelo Captive Portal | Captive Portal |
| **UFRGS** | Aberto a todos. | Tíquete de acesso, com usuário e senha, é fornecido no Portal de Serviço da instituição | Captive Portal |
| **UFRJ** | Aberto a todos. | Não necessita credenciamento. | Rede aberta |
| **UFSC** | Visitantes devem ser previamente cadastrados. | O cadastro deverá ser feito pelo membro da instituição. | Captive Portal |
| **UNISUL** | Visitantes devem ser previamente cadastrados. | Tíquete de acesso, com usuário e senha, é fornecido no Portal de Serviço da instituição | Captive Portal |
| **UNICAMP** | Visitantes devem ser previamente cadastrados. | A abertura da conta de usuário deverá ser feita no portal da instituição. | Rede Aberta |
| **UFMG** | Somente para membros da instituição e pesquisadores convidados. | Devem realizar cadastro, via Web, antes de acessar a rede. | WPA2-Enterprise |
| **USP** | Somente para membros da instituição. | Devem realizar cadastro, via Web, antes de acessar a rede. | Captive Portal |
| **UFPA** | Aberto a todos. | Não necessita credenciamento. | Rede Aberta |

# 4. PROPOSTA DE CONTROLE DE ACESSO

## 4.1. METODOLOGIA

O desenvolvimento do trabalho foi dividido em duas etapas: levantamento bibliográfico e projeto/implantação.

A primeira etapa refere-se a pesquisa textual e literária, através de livros, artigos, sites de instituições sobre redes de computadores, legislações e jurisprudências relacionadas à Internet, controle de registro, autenticação e outros. Além disso, um levantamento entre ferramentas de controle de acesso foi realizado a fim de encontrar a solução mais adequada à proposta de implementação do projeto *hotspot*.

Posteriormente, na segunda etapa, foi desenvolvido um ambiente isolado, exclusivo para a implantação da ferramenta de *hotspot*, a fim de evitar que ocorressem erros capazes de prejudicar o andamento das tarefas do *Data Center*. Foi disponibilizado uma máquina virtual (VM) executando o Sistema Operacional Linux Debian Jessie com suas configurações básicas. A VM serviu de incubadora para receber o *software* escolhido, após instalação e configuração da ferramenta a rede foi propagada para alguns APs da instituição. Os testes realizados possibilitaram aos usuários o acesso à Internet de forma autenticada e controlada.

## 4.2. ESTUDO DE CASO

### 4.2.1. O CTIC

O Centro de Tecnologia da Informação e Comunicação (CTIC) é um órgão suplementar da Universidade Federal do Pará, voltado ao desenvolvimento de serviços de Tecnologia de Informação e Comunicação (TIC) para a comunidade universitária (CONSELHO UNIVERSITÁRIO, 2011).

Segundo o artigo 2º, compete ao CTIC planejar, padronizar e, quando couber, executar as ações para manter a qualidade dos sistemas de informação, assim como os serviços de Internet mantendo a consistência, segurança e confiabilidade das informações e conhecimento gerados a partir deles; difundir e fomentar soluções de TICs e novas tecnologias para a comunidade acadêmica (CONSELHO UNIVERSITÁRIO, 2011).

A Coordenadoria de Segurança e Serviços de Internet (CSSI) é integrante da estrutura organizacional do CTIC, conforme Figura 7.

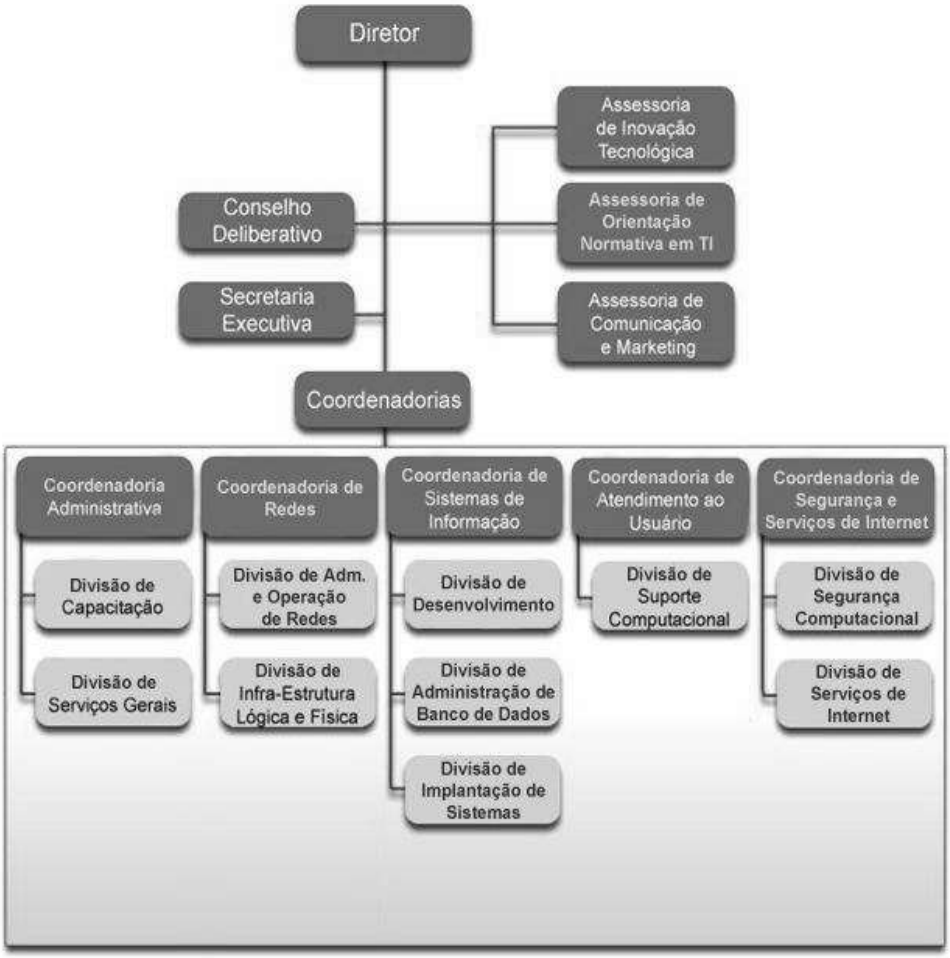



Figura 7 - Organograma do CTIC
Fonte: http://www.ctic.ufpa.br/images/imagens/OrganogramaCTIC.jpg (2016)

A CSSI tem como responsabilidade e subdivisões:

> [...] A manutenção dos serviços de Internet da Universidade Federal do Pará (UFPA), como: *E-mail* institucional, domínios de Internet, sistemas institucionais, entre outros; o gerenciamento e a segurança de informações que trafegam pela rede da UFPA e pela manutenção dos servidores (computadores) hospedados no *Data Center* do CTIC, além de sua importante participação, como membro, no Comitê de Segurança da Informação da UFPA, com propostas de políticas de segurança em TI.
>
> A Coordenadoria é integrada pela Divisão de Segurança da Informação e pela Divisão de Serviços de Internet:
>
> I) Divisão de Segurança: responsável pela prevenção, detecção e resolução de incidentes de segurança em servidores e na rede da Instituição; implantação de ferramentas destinadas a auxiliar na segurança da informação.
>
> II) Divisão de Serviços: responsável pela a instalação, configuração, administração dos serviços de Internet fornecidos à UFPA. (CTIC, 2016a)

### 4.2.2. Cenário atual

Atualmente, a rede sem fio aberta da UFPA, também chamada de “UFPA 2.0 – Visitantes”, está organizada da seguinte maneira: O usuário, pelo dispositivo móvel, requisita ingresso à rede. A requisição é enviada ao AP, este faz uma conexão com o servidor DHCP, que retorna um endereço interno de rede privada para o dispositivo, permitindo acesso à internet, conforme figura 8:

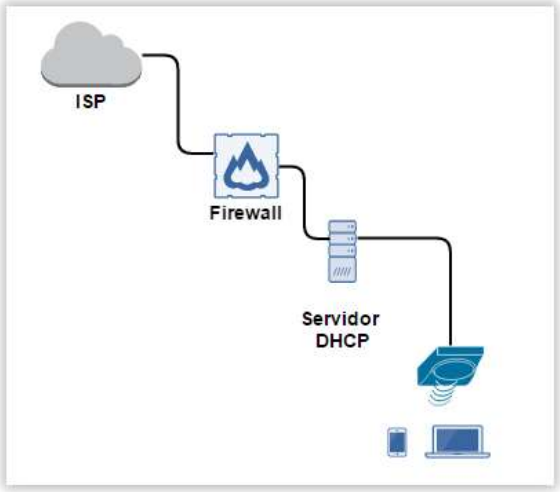



Figura 8 - Cenário Atual.
Fonte: Elaborado pelo autor (2016)

A Instituição recebe diariamente, uma grande quantidade de usuários que necessitam utilizar a rede por um determinado momento, porém não possuem vínculo institucional - casos de Eventos, Congressos, atendimento ao público e entre outros. Baseado nos descritos anteriormente, é possível identificar, na atual infraestrutura, problemas de segurança e rastreabilidade, pois não há um controle de acesso de usuários para rede em questão.

## 4.3. **CENÁRIO PROPOSTO**

### 4.3.1. ESPECIFICAÇÃO GERAL

A proposta de reestruturação da Rede Visitante da Universidade Federal do Pará (UFPA), leva em consideração o gerenciamento de usuários e eventualidades (incidentes), em relação à segurança da informação, sendo o controle de conexão o ponto fundamental para alcançar os objetivos relativos a inimputabilidade, uma vez que, ao disponibilizar o serviço de

rede sem fio aberta à comunidade acadêmica, considera-se não somente o acesso, mas uma infraestrutura capaz de oferecer facilidade de acesso e gerenciamento de *hosts* e usuários conectados, visto que em casos de incidentes de segurança da informação, seja possível a instituição identificar o infrator e a este transferir a responsabilidade dos atos.

Tendo em vista os problemas apresentados nos capítulos anteriores, a ferramenta PacketFence terá o papel de suprir com os objetivos já descritos neste trabalho, em razão que a solução escolhida propõe gestão de *hosts* e usuários, sendo capaz de identificar um nó que esteja infringindo políticas definidas no termo de uso, facilitando o administrador a responder uma possível notificação de violação oriunda de órgãos superiores que regulam a internet no Brasil.

Conclui-se que, para chegar aos objetivos do trabalho é necessário fazer a junção teórica da ferramenta com as legislações vigentes no Brasil. Os parágrafos a seguir, demonstram os aspectos capazes de validar com a proposta do trabalho.

No entendimento do artigo 5º do Marco Civil inciso VI, considera que é necessário para o administrador da rede, armazenar registros de conexões dos usuários a partir da obtenção de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados (BRASIL, 2015).

Baseando-se no artigo 13º do Marco Civil da Internet, onde na provisão de conexão à Internet, cabe ao administrador de sistema o respectivo dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. Ficando entendido que a rastreabilidade é uma exigência legal.  Além disso, é um elemento básico em planos de segurança e de gestão na organização. Garantindo o controle completo sobre a complexidade de informações e dados, independente do volume.

Os requisitos de rastreabilidade estão ligados às legislações e normas que devem ser adequados à finalidade. Visando adequar a uma realidade acessível da Universidade Federal do Pará, é necessário realizar um cadastro contendo nome, telefone e e-mail. A partir do envio dessas informações, o usuário recebe uma chave de acesso de autenticação, permitindo a conexão.

A Lei Federal nº 10.703 de 18/07/2003 foi a norma que estruturou os requisitos solicitados no cadastro de acesso à rede sem fio.  Que dispõe sobre o cadastramento de usuários

de telefones celulares pelas prestadoras de serviço de telecomunicações. A lei incumbe às operadoras de telecomunicações, em operação no território nacional, manter cadastro atualizado de usuários, que inclui nome, endereço completos e o número de identificação (CPF), no caso de pessoa física. Em investigação de ações ilícitas, as informações cadastradas junto a prestadora, podem ser solicitadas para atender solicitação da autoridade judicial.

### 4.3.2. FERRAMENTA DE CONTROLE: PACKETFENCE

PacketFence é uma solução de NAC confiável, livre e de código aberto. Com um conjunto de recursos incluindo um *captive portal* para registro, gerenciamento centralizado com e sem fio; PacketFence pode ser usado eficazmente em pequenas e grandes redes heterogêneas (INVERSE, 2017).

#### A) Características

O PacketFence conta com uma grande quantidade de características e funcionalidades. Abaixo se descreve os atributos utilizados no projeto:

- ***Inline Enforcement*:** O modo *inline* é configurado para agregar equipamentos de rede que não são gerenciáveis. Proporcionando escalabilidade e segurança, para que os hardwares mais antigos possam ser utilizados com segurança.

- **Integração *Wireless*:** PacketFence integra perfeitamente com redes sem fio. Permite ao usuário autenticar-se em redes com fio e redes sem fio através do *captive portal*, deixando, desta forma, a autenticação centralizada. A integração suporta vários *Access Points* (AP) e controladores sem fio de diferentes fabricantes, tornando o ambiente heterogêneo.

- **Registro:** PacketFence utiliza uma solução similar ao *captive portal* para realizar o registro dos dispositivos. Diferentemente de soluções comuns de *captive portal*, a solução do PacketFence recorda os usuários previamente registrados, pois este verifica se o usuário está devidamente registrado juntamente com o dispositivo na base de dados do PacketFence. Caso exista o registro do dispositivo, o mesmo não será interceptado pelo *captive portal* e consequentemente não será pedido para se registrar novamente. Desta forma, o usuário consegue acesso sem outra autenticação. Contudo, os usuários não poderão ter acesso à rede sem primeiramente aceitar os termos da Política de Uso.

- **Linha de comando e gerenciamento baseado na *Web*:** O PacketFence oferece dois modos de gerenciamento da ferramenta: gerenciamento baseado em linha de comando e baseado na *Web*. Todas as tarefas podem ser realizadas, independentemente do modo de gerenciamento escolhido.

- **Acesso a Visitantes:** O PacketFence suporta acesso a visitante ou convidado. Este somente irá ter acesso à Internet depois que estiver registrado. Para isso, o PacketFence utiliza um Registro e um *captive portal*. Para registrar um convidado, existem várias possibilidades, tais como: registro manual, auto registro, acesso ao visitante com ativação por *e-mail* e ativação por telefone celular via *Short Message Service* (SMS).

- **Suporte à *Hotspot*:** PacketFence também pode ser configurado como *hotspot*.

### B) Componentes

A figura 9 ilustra as principais tecnologias presentes no PacketFence.

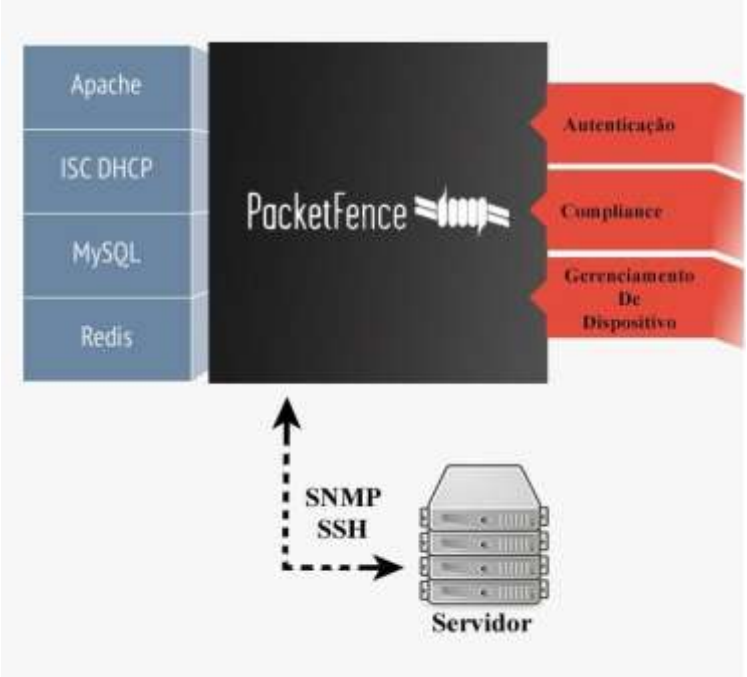



Figura 9 - Componentes do PacketFence.
Fonte: Elaborado pelo autor (2017).

#### A) Apache

Um servidor *Web* é "um software que utiliza como forma de comunicação a arquitetura cliente-servidor, capaz de aceitar requisições HTTP e enviar respostas sob o mesmo protocolo"

(GOUVÊA e MAGALHÃES, 2013). Em sintaxe, esta é a principal função do servidor *web* Apache. Sua facilidade de instalação e configuração, suporte aos principais SGBDs e sua capacidade multiplataforma, tornaram o Apache um dos servidores mais utilizados no mundo (NETCRAFT, 2017).

O Apache é escrito em C ANSI, é um software *Open Source* distribuído pela ASF (*Apache Software Foundation*), por meio do site www.apache.org. Implementada por uma comunidade de desenvolvedores voluntários distribuídos pelo mundo, em um esforço intelectual para criar um servidor *web* com características inovadoras (ALBUQUERQUE e MAESTRELLI, 2000).

A. Características

Abaixo estão algumas características que fazem esse servidor *web* o preferido entre os administradores de sistemas (ORACLE, 2017b):

- Suporte a *scripts* CGI;
- Autenticação de usuário para acesso de página, arquivo ou sub-diretório (suportando criptografia via *Crypto* e MD5);
- Negociação de conteúdo, permitindo a exibição da página *Web* no idioma requisitado pelo Cliente (navegador *Web*);
- Personalização de *logs*;
- Suporte a virtual *hosting*;
- Suporte a IP e *name* virtual *hosting*;
- Suporte a criptografia via SSL, Certificados digitais etc.;
- Módulos DSO (*Dynamic Shared Objects*) permitem adicionar/remover funcionalidades e recursos sem necessidade de recompilação do programa.

B) MYSQL

Criada nos anos 1980 pela MySQL AB e atualmente desenvolvida pela *Oracle Corporation*, o MySQL é o mais popular Banco de Dados SQL *Open Source* do Mundo (DB-Engines, 2017). Características como desempenho, confiabilidade e facilidade de uso, tornaram o MySQL a principal escolha de banco de dados para aplicativos baseados na *web*, utilizada por grandes companhias, tais como: Facebook, Google, GitHub, Amazon, entre outras (ORACLE, 2017a).

O site oficial do MySQL define que este é um sistema gerenciador de bancos de dados (SGBD) relacional. Um banco de dados relacional armazena dados em tabelas separadas, porém, todos os dados ficam armazenados num único local. As tabelas são unidas por relações definidas, tornando possível combinar dados de diferentes tabelas nas requisições. Isso proporciona velocidade e flexibilidade (ORACLE, 2017a).

A. Características

A seguir estão descritas algumas das características importantes do MySQL, existentes em todas as versões (ORACLE, 2017b):

- Escrito em C e C ++;
- Testado com uma ampla gama de compiladores diferentes;
- Multiplataforma;
- Suporte à portabilidade (com o CMake);
- Usa design de servidor multicamadas com módulos independentes;
- Projetado para ser *multi-threaded* com uso do *kernel threads*;
- Fornece mecanismos de armazenamento transacionais e não-transacionais;
- Utiliza tabelas de disco de árvore B (MyISAM) com compressão de índice;
- Implementa tabelas de *hash* de memória, que são usadas como tabelas temporárias.

C) Redis

O Redis (*REmote DIctionary Server*) é um SGBD, desenvolvido por Salvatore Sanfilippo, que utiliza o modelo de armazenamento de valor-chave (*key-value*). É uma aplicação de código aberta (*Open Source*) sob a licença BSD. Diferentemente de um banco de dados tradicional, o Redis é categorizado como um banco de dados não relacional, referenciado pela sigla NOSQL, do inglês *Not Only SQL* (LAZOTI, 2014).

Para Lazoti (2014), a principal característica do Redis é que ele armazena seus dados em memória, porém é possível persistir os dados fisicamente. O armazenamento dos dados em memória torna o SGBD extremamente rápido, tanto para escrita como para leitura de dados. Uma outra característica importante é que todos os comandos executados no Redis são

atômicos, e isso é garantido pela forma com que o Redis é executado, que é como uma aplicação *single-threaded*, ou seja, enquanto um comando está sendo executado, nenhum outro comando será executado (conforme Figura 10).

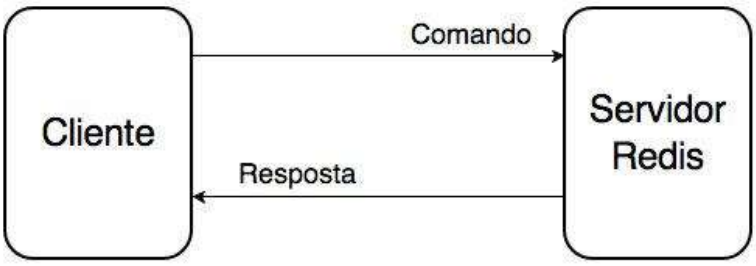



Figura 10 - Estrutura *single-threaded* do Redis.
Disponível em: http://www.e-reading.club/illustrations/1029/1029579-_3.jpg
Acesso em: 19 mar. 2017

D) DHCP

Como abordado no item 2.2.2 deste trabalho, o protocolo fornece de maneira automática, um endereço IP a um host, além de informações adicionais da rede, tais como *netmask* (máscara de subrede), *gateway* (endereço do roteador padrão) e o endereço do servidor DNS local. O serviço DHCP é designado por um servidor especial que atribui endereços IP aos aparelhos que solicitam um endereço, sendo que esta distribuição pode ser manual ou dinâmica (TANENBAUM, 2011).

Na atribuição dinâmica, o servidor gerencia os dispositivos clientes de modo a não permitir repetição e conflitos de endereçamento, alocando e reutilizando os IPs disponíveis ao longo do tempo (BATTISTI, 2006).

E) Autenticação de usuários

Com o crescimento das redes sem fio abertas, questões como segurança de acesso se tornaram mais frequentes. Tais como problemas como roubo de senhas, interrupção de serviços e problemas de personificação (pessoa passa-se por outra para obter acesso privilegiado). Nesse sentido, o serviço de autenticação do usuário permite validar o usuário que está se identificando (GUIMARÃES, 2006).

Segundo Kurose e Ross (2013), autenticação é um dos princípios de segurança de redes que consiste quando os envolvidos (transmissor e receptor) querem confirmar a identidade um do outro.

Para Fiorese (2000), os tipos de autenticação de usuários se dividem em três categorias: baseados no conhecimento, baseados em propriedade e baseados em características. Em síntese, estes podem ser definidos:

**Baseados no conhecimento:** Mecanismo mais utilizado para prover uma identidade a um computador. Baseia-se no fornecimento de uma informação secreta. Dentre os métodos destacam-se senhas, PIN (*Personal Identification Number*), chaves de criptografia etc.

**Baseados em propriedade:** Solução de autenticação baseado em um objeto físico pertencente ao usuário. Este objeto pode ser um *smartcard* (cartão inteligente), uma chave (dispositivo) ou um *token*. Geralmente, combina-se o método de autenticação por propriedade com autenticação baseada em senhas.

**Baseados em características:** São métodos que podem ser usados para alcançar uma identificação positiva, com um alto grau de confiança, baseados em alguma característica humana, física ou comportamental. Exemplos de autenticações baseadas em características: biometria, reconhecimento facial, íris e/ou de voz.

F) Compliance

A Endeavor Brasil (2015) define *compliance* a partir de *comply*, em inglês, significa "agir em sintonia com as regras". *Compliance*, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. É a atividade que assegura que a empresa está cumprindo à risca todas as imposições dos órgãos de regulamentação, dentro de todos os padrões exigidos de seu segmento. E isso vale para as esferas trabalhista, fiscal, contábil, financeira, ambiental, jurídica, previdenciária, ética etc.

Em termos de tecnologia, a *compliance checks* (verificação de conformidade) é um método de auditoria de conformidade. A auditoria de conformidade determina se um sistema está configurado de acordo com uma política estabelecida. Esses requisitos de conformidade são linhas de base mínimas que podem ser interpretadas de forma diferente dependendo dos

objetivos de negócios da organização, a fim de garantir que os riscos sejam adequadamente identificados e mitigados (TANEBLE, 2017).

G) Gerenciamento de dispositivos

O gerenciamento de dispositivo é uma aplicação capaz de exibir graficamente os *hardwares* conectados no sistema.

No caso de sistemas que utilizam o *captive portal*, os dispositivos dos usuários conectados (autorizados ou não) são registrados. Uma vez conectado, o portal solicitará que eles insiram o endereço MAC do dispositivo que será comparado com uma lista predefinida de MAC autorizada. O dispositivo será registrado com o ID do usuário e pode ser atribuído a uma categoria específica para facilitar o gerenciamento (INVERSE, 2017).

H) SSH

SSH, do inglês, *Secure Shell* é um protocolo a nível de aplicação que permite serviços de rede seguros através de uma rede insegura, como a Internet. O SSH veio para substituir protocolos e serviços inseguros, incluindo Telnet e FTP (SSH, 2000). SSH é uma abordagem para a segurança de rede. Seu funcionamento consiste, genericamente, na transmissão segura dos dados, ou seja, sempre que os dados são enviados por um computador, o SSH os criptografa. Em seguida, ao chegarem ao destinatário pretendido, o SSH descriptografa-o automaticamente (BARRETT, SILVERMAN e BYRNES, 2005).

Algumas das vantagens da utilização do SSH (H3C, 2009):

- Envia dados em texto cifrado, garantindo a confidencialidade da informação trocada;
- Transmite informações de autenticação de usuário em texto criptografado;
- As chaves de criptografia e descriptografia para comunicação entre servidor e cliente SSH são geradas em processos dinâmicos de troca de chaves, ganhando, assim, maior segurança do que as chaves configuradas manualmente;
- Os clientes SSH podem autenticar as identidades de seus servidores, evitando ser falsificados por pseudo-servidores.

I) SNMP

SNMP, do inglês, *Simple Network Management Protocol*, em português Protocolo Simples de Gerência de Rede, foi introduzido em 1988 para atender os usuários com um "simples" conjunto de operações que permite que os dispositivos sejam gerenciados remotamente (MAURO e SCHMIDT, 2005). O modelo utilizado para gerenciamento de redes TCP/IP é composto pelos seguintes elementos: Gerenciador SNMP (gerente), Agente, Base de Informações Gerenciais (MIB), o SMI e o protocolo de gerenciamento de redes SNMP (RNP, 1997).

A figura 11 ilustra os elementos que compõem o gerenciamento de redes:

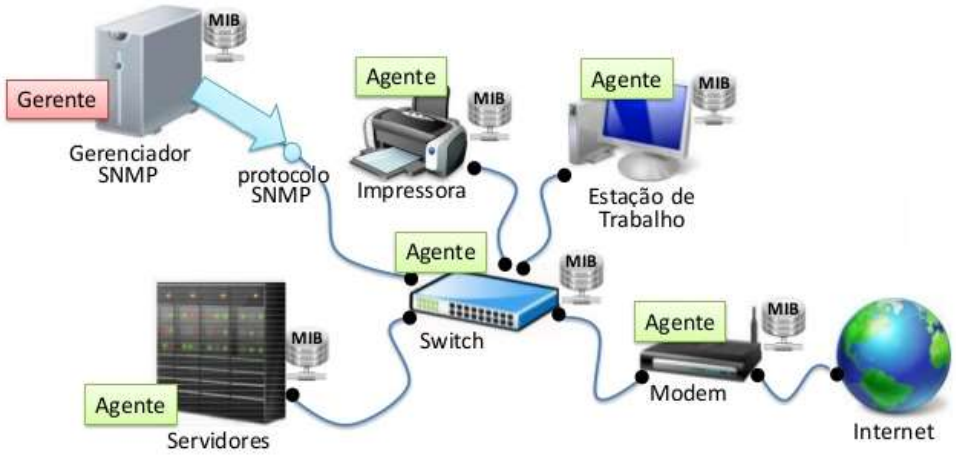



Figura 11 - Elementos do Gerenciamento de Redes
Disponível em: https://image.slidesharecdn.com/protocolosnmp-131107134352-phpapp01/95/protocolo-snmp-18-638.jpg
Acesso em: 19 mar. 2017

O Gerenciador SNMP (gerente) é servidor que executa o software de gerenciamento para uma rede. É responsável por consultar e receber as notificações dos agentes conectados na rede. Durante as pesquisas (consulta aos agentes), o gerente pode determinar a existência de um evento catastrófico e executa uma solução. O agente é um software que executa no cliente e responde às solicitações de informações e ações. Em casos de falha, denominada trap, o agente notifica o gerente para a resolução dessa. A comunicação entre o agente e o gerente é feita pelo protocolo SNMP (CISCO, 2004; MAURO e SCHMIDT, 2005).

Os recursos gerenciados são representados como objetos, a Estrutura de Informações de Gerenciamento, do inglês *Structure of Management Information* (SMI), fornece uma maneira

de definir objetos gerenciados e seu comportamento. Um agente tem em posse uma lista dos objetos que o acompanha. E a MIB, Base de Informações Gerenciais (*Management Information Base*), é o banco de dados de objetos gerenciados que acompanha o agente. Qualquer tipo de status ou informações estatísticas que podem ser acessadas pelo Gerenciador SNMP é definido em um MIB (CISCO, 2004; MAURO e SCHMIDT, 2005; RNP, 1997).

### 4.3.3. Rede sem fio aberta com controle de acesso

Baseado no controle de acesso e nas características legais que o envolve, a figura 12 ilustra a arquitetura da rede sem fio visitante proposta, onde o acesso à internet é intermediado pelo servidor Packetfence. Este, por meio do seu *captive portal*, coleta as informações dos dispositivos, recebe as informações dos usuários, valida a chave de acesso e autoriza acesso à rede.

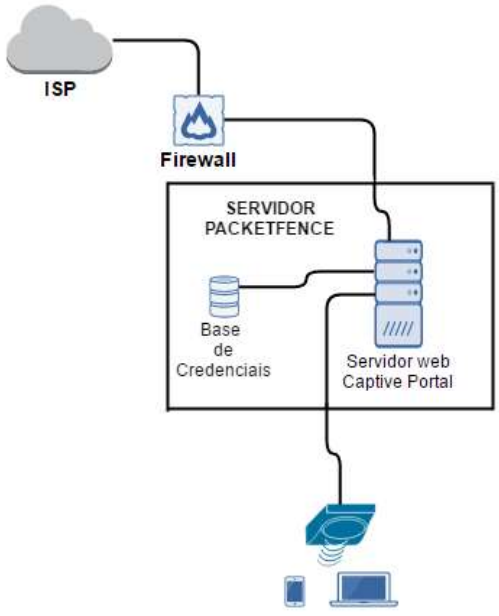



Figura 12 - Cenário Proposto: Rede aberta com controle de acesso PacketFence
Fonte: Elaborado pelo autor (2016)

A nova arquitetura fornece um novo modelo de acesso pelo usuário, ilustrado na figura 13, no qual a liberação de acesso é feita após aceitação dos termos de responsabilidade e preenchimento de formulário, contendo: nome, *e-mail* e telefone. Posteriormente, a aplicação

envia, via SMS, um PIN de autenticação. O usuário retorna esta chave de acesso ao servidor e, se as chaves combinarem, o acesso é liberado.

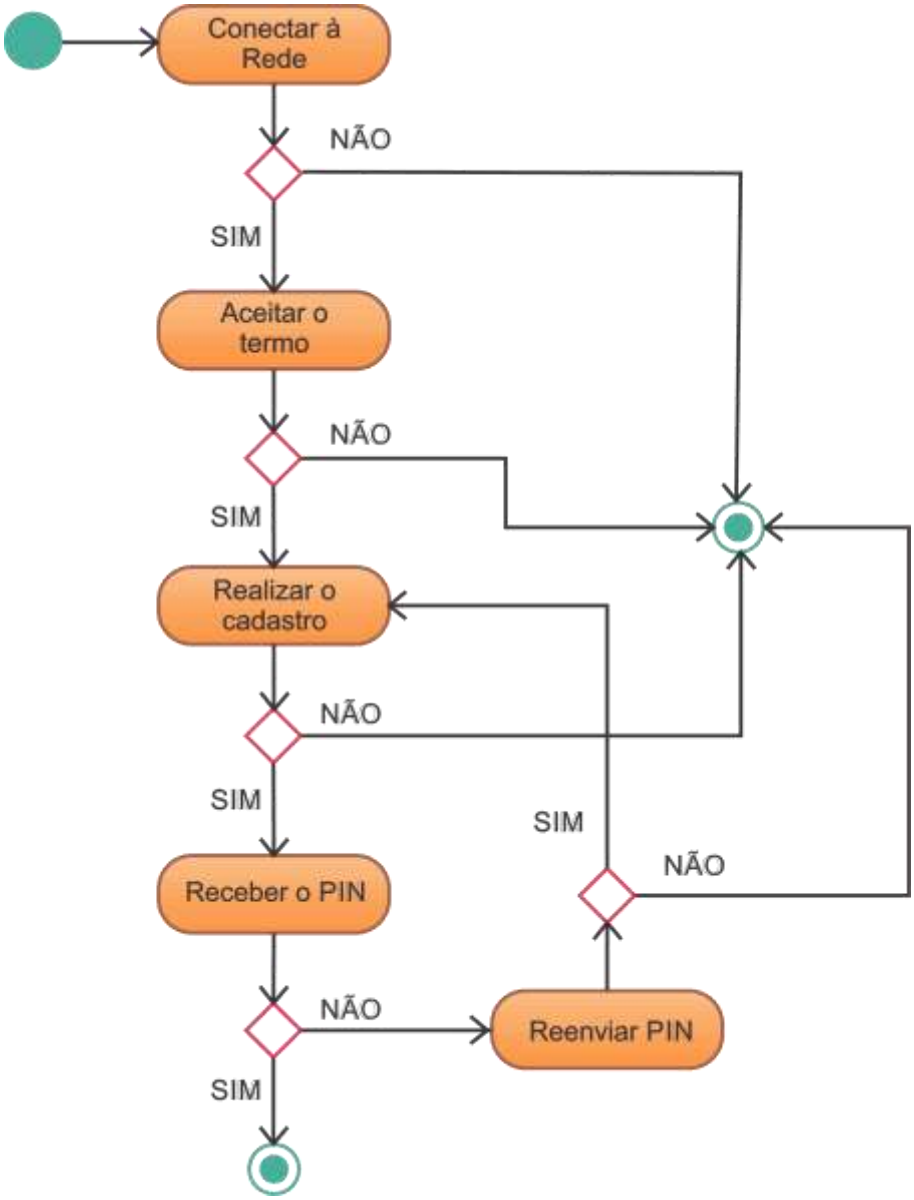



Figura 13 - Modelo de conexão pelo usuário.
Fonte: Elaborado pelo autor (2017).

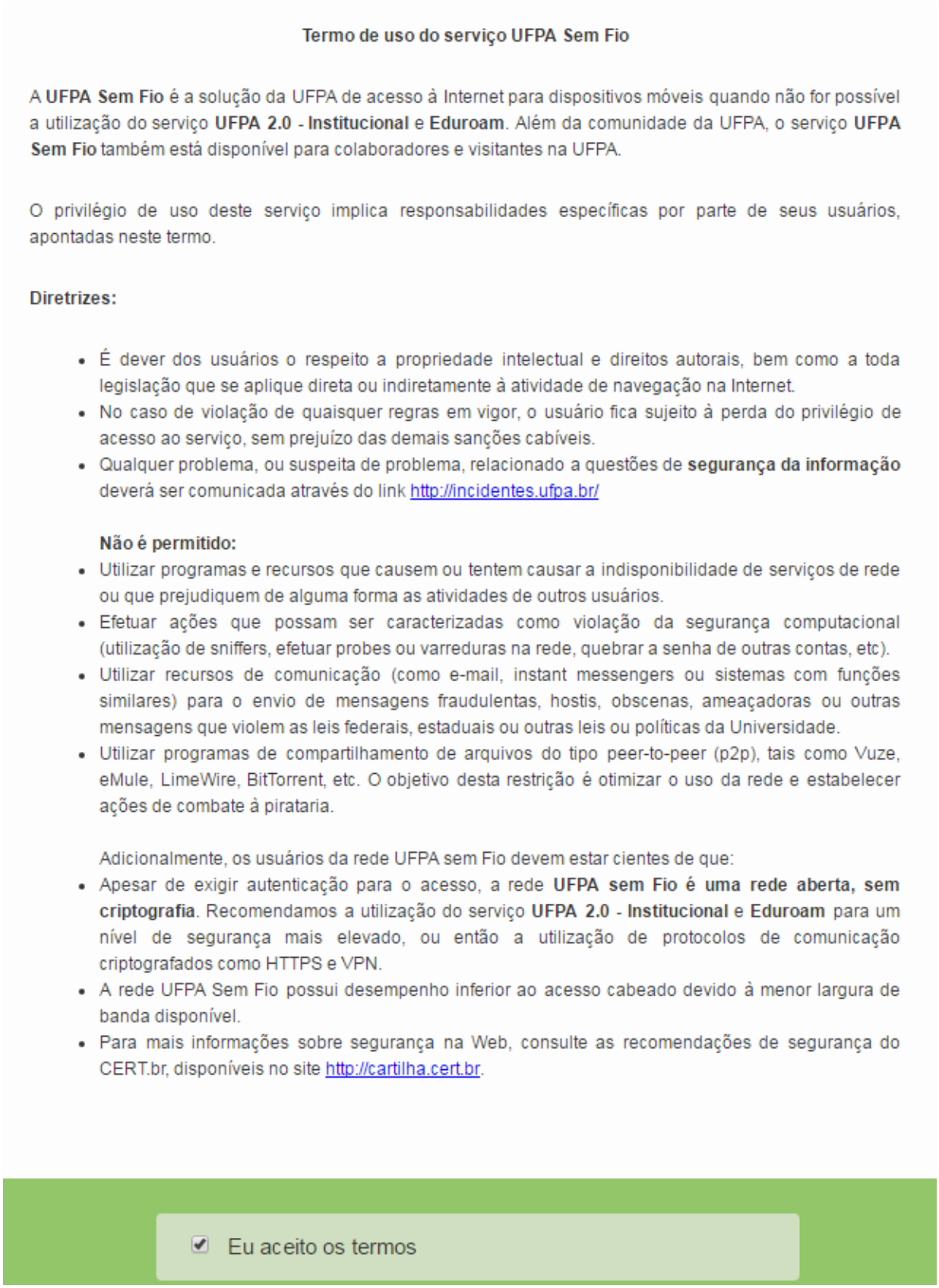
# 5. RESULTADOS OBTIDOS

### 5.1.1. **Cenário de teste**

Os testes com o PacketFence foram realizados no Centro de Tecnologia da Informação e Comunicação (CTIC), tendo como participantes alunos, funcionários e membros da comunidade em geral. A rede de teste foi propagada em um *Access Point* do CTIC, em paralelo com as redes existentes da Universidade.

### **5.1.2. Captive portal**

O ponto de partida do usuário, para acesso à Internet, é conectar-se à rede de teste. Ao solicitar conexão, o usuário é direcionado ao portal de captura, onde é exibido o termo de responsabilidade (Figura 14). O aceite deste é obrigatório para prosseguir com o ingresso.



**Termo de uso do serviço UFPA Sem Fio**

A **UFPA Sem Fio** é a solução da UFPA de acesso à Internet para dispositivos móveis quando não for possível a utilização do serviço **UFPA 2.0 - Institucional** e **Eduroam**. Além da comunidade da UFPA, o serviço **UFPA Sem Fio** também está disponível para colaboradores e visitantes na UFPA.

O privilégio de uso deste serviço implica responsabilidades específicas por parte de seus usuários, apontadas neste termo.

**Diretrizes:**

- É dever dos usuários o respeito a propriedade intelectual e direitos autorais, bem como a toda legislação que se aplique direta ou indiretamente à atividade de navegação na Internet.
- No caso de violação de quaisquer regras em vigor, o usuário fica sujeito à perda do privilégio de acesso ao serviço, sem prejuízo das demais sanções cabíveis.
- Qualquer problema, ou suspeita de problema, relacionado a questões de **segurança da informação** deverá ser comunicada através do link http://incidentes.ufpa.br/

**Não é permitido:**

- Utilizar programas e recursos que causem ou tentem causar a indisponibilidade de serviços de rede ou que prejudiquem de alguma forma as atividades de outros usuários.
- Efetuar ações que possam ser caracterizadas como violação da segurança computacional (utilização de sniffers, efetuar probes ou varreduras na rede, quebrar a senha de outras contas, etc).
- Utilizar recursos de comunicação (como e-mail, instant messengers ou sistemas com funções similares) para o envio de mensagens fraudulentas, hostis, obscenas, ameaçadoras ou outras mensagens que violem as leis federais, estaduais ou outras leis ou políticas da Universidade.
- Utilizar programas de compartilhamento de arquivos do tipo peer-to-peer (p2p), tais como Vuze, eMule, LimeWire, BitTorrent, etc. O objetivo desta restrição é otimizar o uso da rede e estabelecer ações de combate à pirataria.

Adicionalmente, os usuários da rede UFPA sem Fio devem estar cientes de que:

- Apesar de exigir autenticação para o acesso, a rede **UFPA sem Fio é uma rede aberta, sem criptografia**. Recomendamos a utilização do serviço **UFPA 2.0 - Institucional** e **Eduroam** para um nível de segurança mais elevado, ou então a utilização de protocolos de comunicação criptografados como HTTPS e VPN.
- A rede UFPA Sem Fio possui desempenho inferior ao acesso cabeado devido à menor largura de banda disponível.
- Para mais informações sobre segurança na Web, consulte as recomendações de segurança do CERT.br, disponíveis no site http://cartilha.cert.br.



Figura 14 - Termo de Responsabilidade
Fonte: Elaborado pelo autor (2017)

A segunda etapa consiste no cadastro dos dados pelo usuário. Estas informações são resultadas dos requisitos coletados, seguindo as exigências das legislações vigentes, contendo nome, *e-mail* e telefone. Ao telefone é enviado o PIN para a autenticação. A figura 15 demonstra o formulário cadastral.

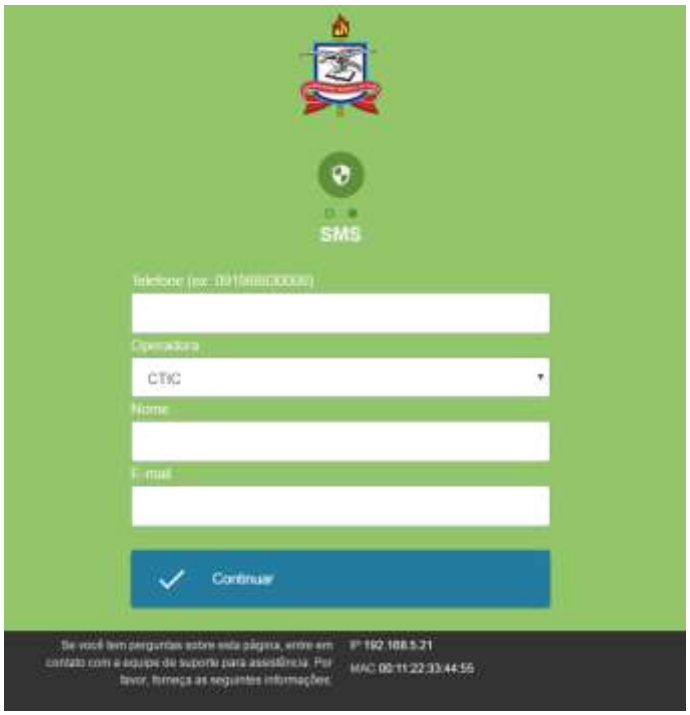



Figura 15 - Formulário de cadastro
Fonte: Elaborado pelo autor (2017)

Ao receber o SMS, o usuário informa o PIN recebido (Figura 16). O servidor PacketFence compara as chaves enviadas com a informada pelo usuário. Caso iguais, o acesso é habilitado e liberado (Figura 17).


Figura 16 - Confirmação do PIN recebido.
Fonte: Elaborado pelo autor (2017)


Figura 17 - Acesso autorizado.
Fonte: Elaborado pelo autor (2017)

### 5.1.3. Relatórios

O PacketFence exibe as informações armazenadas dos usuários registrados. Será apresentado três pontos importantes para o controle e gerenciamento dos usuários e suas conexões: registo de acesso, controle de usuário e dispositivos, e rastreabilidade de incidentes. Este último, consiste na análise das informações coletadas com uma notificação de violação de direitos autorais.

#### 5.1.3.1. Controle de usuário/dispositivos

O controle de usuário envolve o gerenciamento das conexões e informações pessoais. O controle de dispositivos relaciona os dispositivos de um usuário. Por meio dessa gerência, é possível rastrear as conexões e vincular o responsável ao dispositivo conectado.

A figura 18 exibe a consulta por *username*, retornando o número de telefone e *e-mail* cadastrados e o quantitativo dos dispositivos vinculados ao usuário (*nodes*). Os detalhes adicionais do usuário (figura 19) exibem os dados informados durante a etapa de cadastro no *Captive Portal* (seção 5.1.2). A figura 20 ilustra os aparelhos vinculados ao *username*, apresentado o endereço MAC, a classe do dispositivo e o atual *status* de conexão.


Figura 18 - Consulta no PacketFence por *username*.
Fonte: Elaborado pelo autor (2017)


Figura 19 - Exibição das informações gerais do usuário.
Fonte: Elaborado pelo autor (2017)

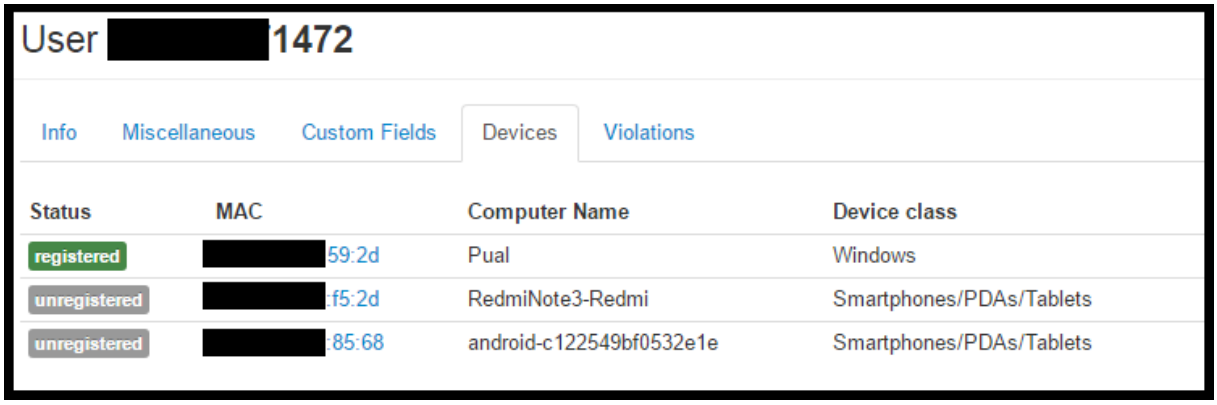



Figura 20 - Detalhes dos dispositivos vinculados ao usuário.
Fonte: Elaborado pelo autor (2017)

O gerenciamento de dispositivo é fundamental para armazenar o histórico de conexão, o quantitativo e os tipos de dispositivos, controle de acesso e também gerenciar usuários. A figura 21 demonstra a consulta por *username*. O retorno exibe o último IP atribuído ao dispositivo, MAC do usuário e o *status* da conexão. A figura 22, exibe o quantitativo e os tipos de sistemas operacionais conectados na rede em um determinado período.

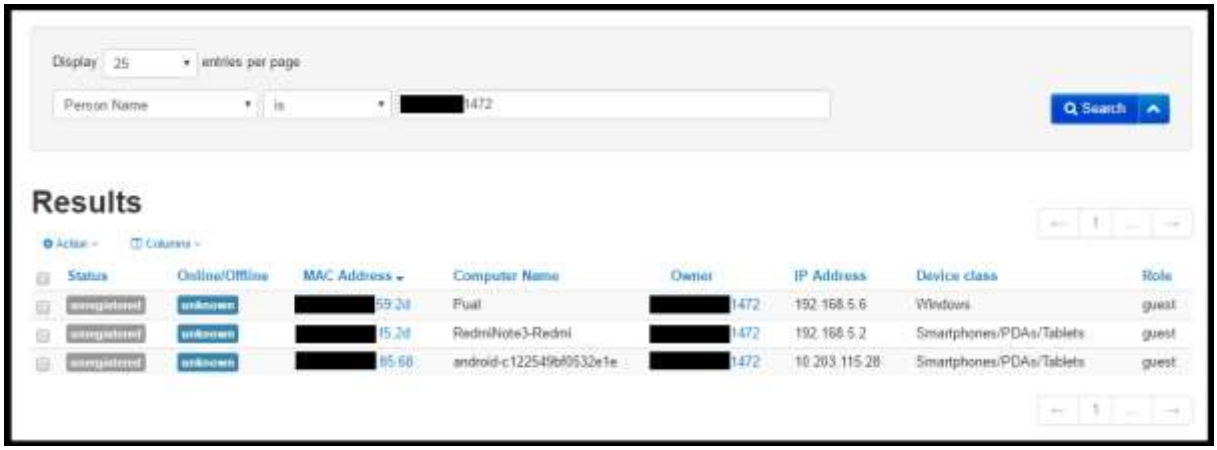



Figura 21 - Consulta por *username*.
Fonte: Elaborado pelo autor (2017)

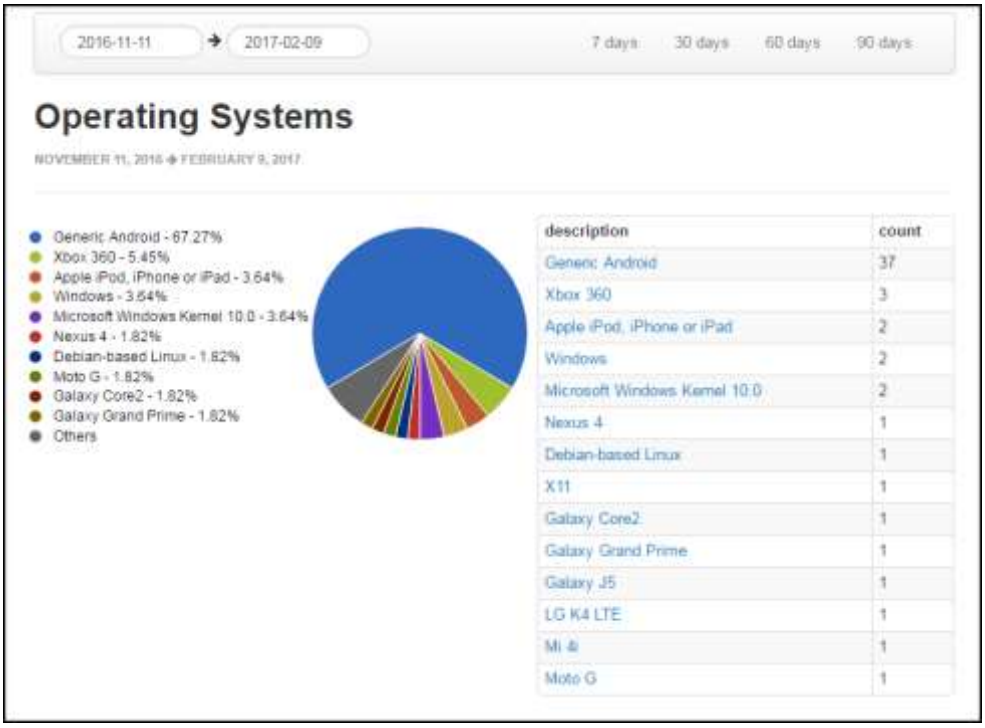



Figura 22 - Tela de consulta dos sistemas operacionais registrados na aplicação.
Fonte: Elaborado pelo autor (2017)

#### 5.1.3.2. Registros de acesso

A figura 23 exibe as informações de um determinado *host* por meio do seu MAC. A partir desse, na aba "*info*", é possível obter os dados dos registros de acesso, o atual endereço IP atribuído ao dispositivo e o *status* de conexão. A figura 24, contêm os dados *fingerbank* do usuário. O fingerbank define o *fingerprint*, ou seja, informações exclusivas que identifica o dispositivo cliente (FINGERBANK, 2016), tais como: tipo de dispositivo, versão do sistema operacional, DHCP *fingerprint* e seus agentes. Na aba "*IP Address*", figura 25, exibe o relatório

de todos os endereços IP concedidos ao aparelho e seus respectivos. A figura 26, informa a localização física do AP conectado, sua VLAN, tipo de conexão e o horário de entrada e saída do ponto de acesso.

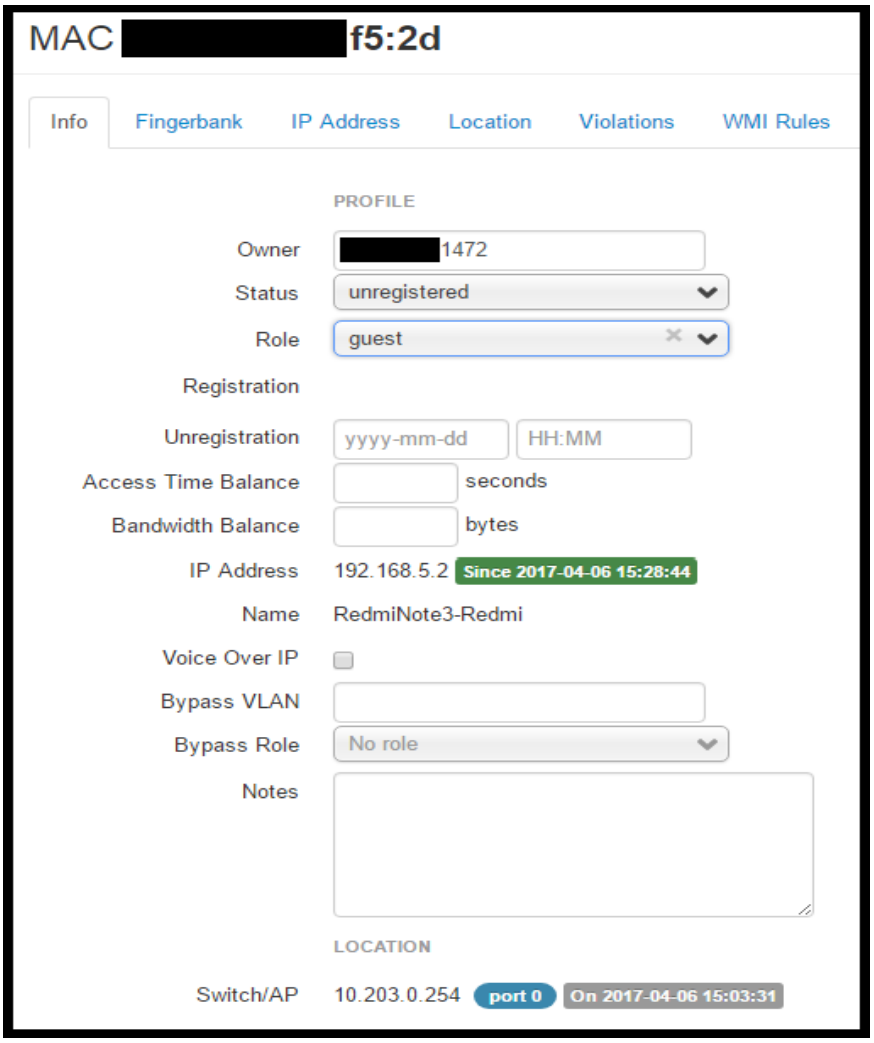



Figura 23 - Informações de um *host*.
Fonte: Elaborado pelo autor (2017)


Figura 24 - Dados *fingerbank* do usuário.
Fonte: Elaborado pelo autor (2017)

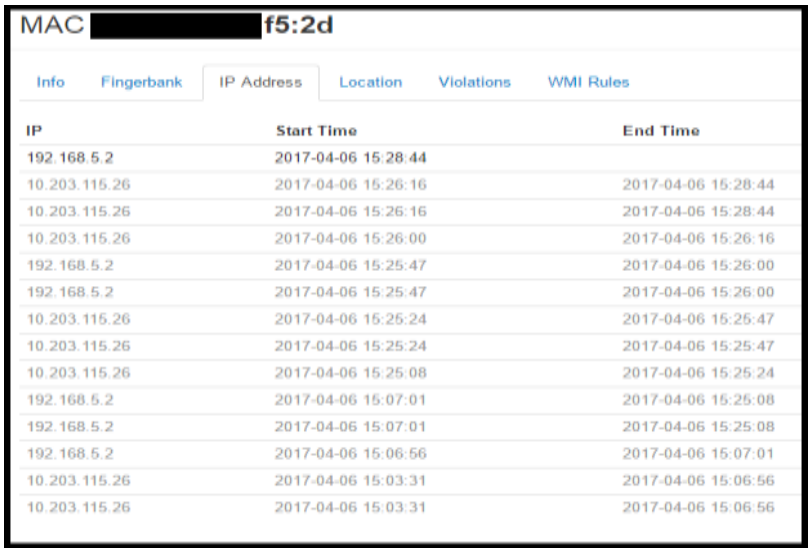



Figura 25 - Endereços IPs destinados a um *host.*
Fonte: Elaborado pelo autor (2017)

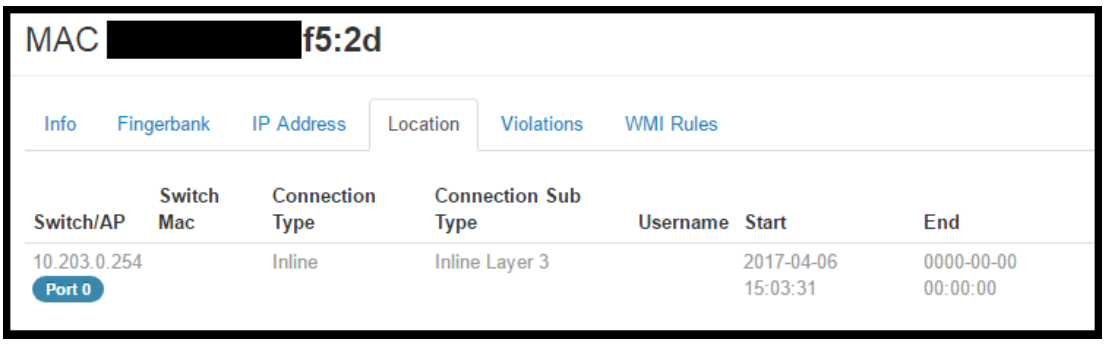
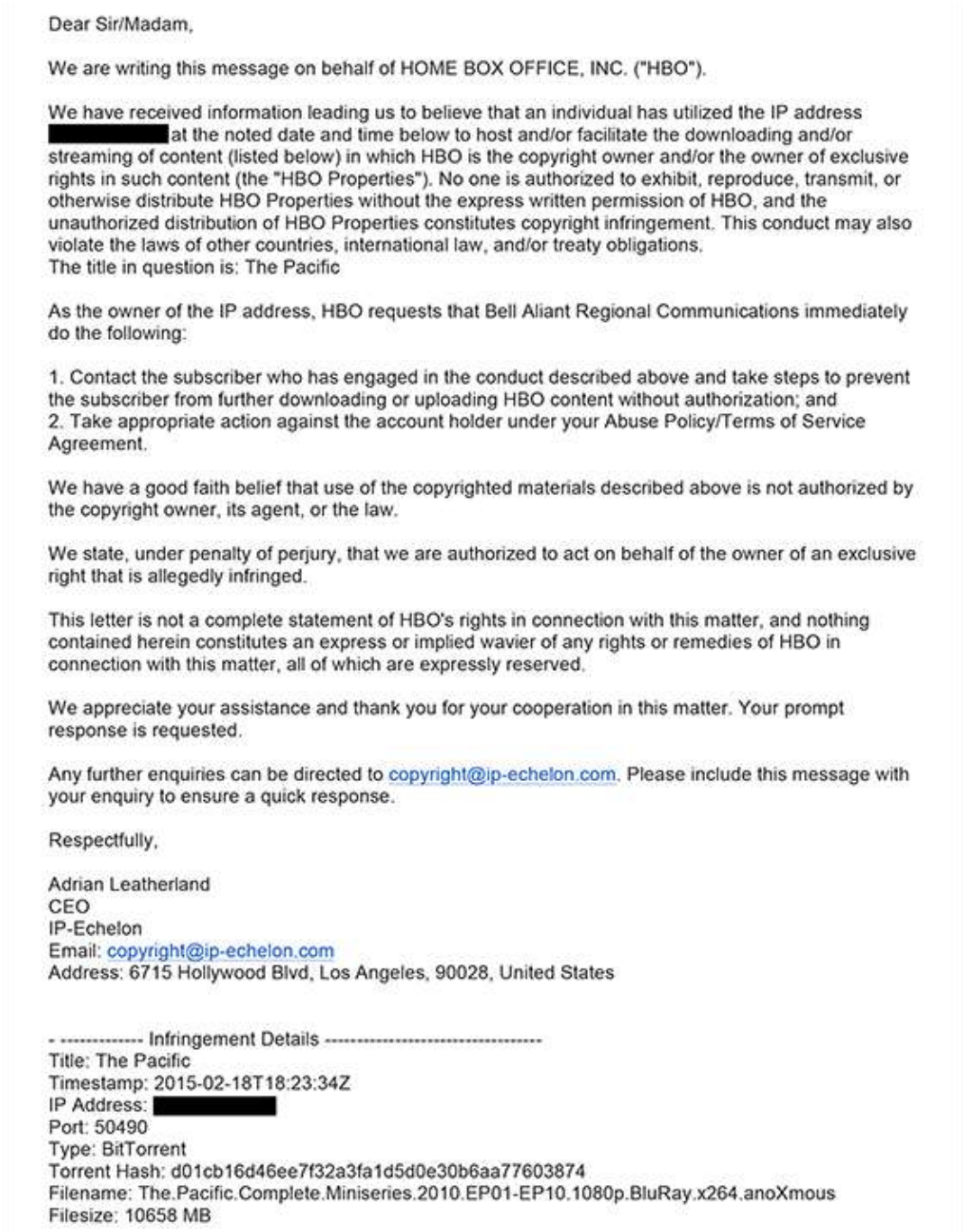



Figura 26 - Localização física do AP.
Fonte: Elaborado pelo autor (2017)

### 5.1.4. Rastreabilidades de incidentes

Dentre os principais incidentes de segurança que envolve ações dos usuários está a violação dos direitos autorais. Geralmente, as infrações estão relacionadas ao compartilhamento de conteúdo protegido por direitos autorais através de comunicação entre pares (*peer-to-peer*), sendo o *bittorrent* o mais utilizado (CERT.BR, 2015). A figura 27 exemplifica uma notificação de violação de *Copyright*. Dentre as informações sobre a identificação do infringente, consta o endereço IP, porta, o tipo (protocolo) e a data do incidente.

Em ambientes não controlados, a rastreabilidade desses infratores é complexa e, provavelmente, exige investigação das autoridades legais competentes. Porém, em redes onde o acesso é controlado, a atribuição de responsabilidade é mais eficaz. A exemplo disso, no cenário de controle de acesso com o PacketFence, é possível traçar um histórico do responsável pelo compartilhamento irregular do conteúdo. Uma consulta por IP, no PacketFence, retorna todos os dispositivos em que aquele endereço foi atribuído, incluindo o horário de conexão (figura 28 e figura 25). Sendo assim, é possível extrair todas as informações expostas no aviso de infração (*infringement notice*), atribuindo a culpabilidade ao devido responsável.



Dear Sir/Madam,

We are writing this message on behalf of HOME BOX OFFICE, INC. ("HBO").

We have received information leading us to believe that an individual has utilized the IP address [redacted] at the noted date and time below to host and/or facilitate the downloading and/or streaming of content (listed below) in which HBO is the copyright owner and/or the owner of exclusive rights in such content (the "HBO Properties"). No one is authorized to exhibit, reproduce, transmit, or otherwise distribute HBO Properties without the express written permission of HBO, and the unauthorized distribution of HBO Properties constitutes copyright infringement. This conduct may also violate the laws of other countries, international law, and/or treaty obligations.
The title in question is: The Pacific

As the owner of the IP address, HBO requests that Bell Aliant Regional Communications immediately do the following:

1. Contact the subscriber who has engaged in the conduct described above and take steps to prevent the subscriber from further downloading or uploading HBO content without authorization; and
2. Take appropriate action against the account holder under your Abuse Policy/Terms of Service Agreement.

We have a good faith belief that use of the copyrighted materials described above is not authorized by the copyright owner, its agent, or the law.

We state, under penalty of perjury, that we are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

This letter is not a complete statement of HBO's rights in connection with this matter, and nothing contained herein constitutes an express or implied wavier of any rights or remedies of HBO in connection with this matter, all of which are expressly reserved.

We appreciate your assistance and thank you for your cooperation in this matter. Your prompt response is requested.

Any further enquiries can be directed to copyright@ip-echelon.com. Please include this message with your enquiry to ensure a quick response.

Respectfully,

Adrian Leatherland
CEO
IP-Echelon
Email: copyright@ip-echelon.com
Address: 6715 Hollywood Blvd, Los Angeles, 90028, United States

- ---------- Infringement Details ----------
Title: The Pacific
Timestamp: 2015-02-18T18:23:34Z
IP Address: [redacted]
Port: 50490
Type: BitTorrent
Torrent Hash: d01cb16d46ee7f32a3fa1d5d0e30b6aa77603874
Filename: The.Pacific.Complete.Miniseries.2010.EP01-EP10.1080p.BluRay.x264.anoXmous
Filesize: 10658 MB

Figura 27 - *Infringement notice*
Disponível em: http://images.huffingtonpost.com/2015-03-06-1425600176-8686041-Bell_Notice_Small-thumb.png
Acesso em: 19 mar. 2017


Figura 28 - Busca por IP.
Fonte: Elaborado pelo autor (2017)

Os resultados apresentados no cenário proposto deste trabalho aduzem proventos importantes com o que foi definido como objetivos, proporcionando através do *captive portal* a obtenção de dados dos usuários, que posteriormente como relatórios são capazes de fazer o controle sobre os usuários e dispositivos, sendo possível auferir registros de acessos na rede, assim possibilitando ocorrer a rastreabilidade de incidentes.

# 6. CONCLUSÃO

## 6.1. CONSIDERAÇÕES FINAIS

A gestão das redes sem fio é algo importante, pois no contexto das redes abertas, existem as questões relacionadas à segurança e o atendimento a legislação vigente. No atual modelo de rede sem fio destinado a visitantes, oferecido pela instituição, o utilizador não necessita realizar qualquer tipo de autenticação, fazendo com que não seja possível controlar e/ou identificar os acessos dos usuários que nela adentram. Diante disso abre-se brechas para possíveis práticas virtuais ilícitas dentro do domínio institucional. Nesta situação, segundo consta em lei, a ausência do usuário infringente, torna o órgão responsável pelas devidas atividades irregulares.

Para alcançar os objetivos pretendidos, apresenta-se uma proposta para reestruturação da rede destinada aos visitantes da Universidade Federal do Pará, utilizando-se do PacketFence, um software livre, com uma variedade de recursos e intuitividade na utilização, facilitando a gerência de redes.

O software, as legislações vigentes e os requisitos levantados são itens necessários para existir o gerenciamento de usuários e dispositivos e, consequentemente, atender aos incidentes de informação. A ferramenta utilizada, Packetfence, através do controle de acesso via captive portal, atende ao pretendido: ao realizar o cadastro dos dados solicitado, o usuário fornece uma informação verdadeira (número do celular) para o recebimento do PIN, este registro é uma garantia que o provedor de conexão (CTIC) tem para rastrear usuários em casos de atitudes ilícitas. Nesse caso, é possível acionar as autoridades competentes e repassar as informações obtidas para a responsabilização dos envolvidos.

Desta forma, este trabalho apresentou uma proposta capaz de adequar-se as legislações e melhorar a gestão de acesso à rede sem fio visitante, proporcionando uma resposta de forma eficaz a quaisquer práticas virtuais ilícitas.

## 6.2. **TRABALHOS FUTUROS**

Diante dos problemas e soluções demonstrados, existe um grande interesse em dar continuidade ao projeto. Por meio do conhecimento adquirido foi possível observar que ainda existem várias melhorias, pode-se citar algumas:

- Integração com o IPv6: Com o esgotamento dos endereços IPv4, faz-se

necessário tornar a aplicação compatível com endereçamento ipv6, sendo assim a instituição poderá utilizar IPs válidos quando achar necessário;

- Validação de informações cadastrais (CPF) por meio de Webservice da Receita Federal.

- Implementação dos módulos de bloqueio de atividades maliciosas com violações: Permitir que se restrinja o acesso baseado em violações de determinadas políticas. Por exemplo, se na rede não é permitido o tráfego do tipo P2P, e o usuário estiver executando o software, o PacketFence dará a esse cliente uma página "bloqueada" o informando a violação da política;

- Implementar sensores de QoS: Limitar o abuso de largura de banda, mantendo a qualidade no acesso e evitando uso indiscriminado de banda;

- Implementação de conexão criptografada: Permitir que clientes consigam se autenticar em rede WIFI de forma autenticada e com criptografia aumentando o nível de segurança.

**REFERÊNCIAS**

ALBUQUERQUE, A; MAESTRELLI, M. **Web-Server Seguro:APACHE**. 2000. Disponível em <http://www.rederio.br/downloads/pdf/nt00900.pdf>. Acessado em 28 mar. 2017.

BALCHUNAS, A. **Network Address Translation**. 2013. Disponível em <http://www.routeralley.com/guides/nat.pdf>. Acessado em 28 mar. 2017.

BARRETT, D; SILVERMAN, R; BYRNES, R. **SSH, The Secure Shell - The definitive guide**. O'Reilly. Sebastopol, CA, 2005.

BATTISTI, J. **Tutorial de TCP/IP - Parte 09 Introdução ao DHCP**. 2006. Disponível em <http://www.juliobattisti.com.br/artigos/windows/tcpip_p9.asp>. Acessado em 25 mar. 2017.

BRASIL. Lei n. 10.703, de 18 de julho de 2003. Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências. Brasília: Casa Civil, 2003.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Marco civil da internet [recurso eletrônico]: Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. – 2. ed. – Brasília: Câmara dos Deputados, Edições Câmara, 2015. – (Série legislação; n. 164).

CARDOSO, L. **Utilização da tecnologia sem fio na administração de serviços**. CONTECSI, 2006. Disponível em <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/3contecsi/paper/download/2070/1174>. Acessado em 28 mar. 2017.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015: Tentativas de fraude reportadas**. 2015. Disponível em < https://www.cert.br/stats/incidentes/2015-jan-dec/fraude.html>. Acessado em 04 abr. 2017.

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CTIC). **Acervo Interno**. UFPA. Belém, 2016a.

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CTIC). **Wiki CTIC – Categoria: Rede sem Fio**. 2016b. Disponível em <http://wiki.ctic.ufpa.br/index.php/Categoria:Rede_sem_Fio>. Acessado em 21 dez. 2016.

CISCO SYSTEMS INC. **Introduction to Network Address Translation**. 2000. Disponível em <http://www.cisco.com/networkers/nw00/pres/2211.pdf>. Acessado em 28 mar. 2017.

CISCO SYSTEMS INC. **Introduction to SNMP and MIB**. 2004. Disponível em <http://www.cisco.com/networkers/nw04/presos/docs/NMS-1N02.pdf>. Acessado em 28 mar. 2017.

CONSELHO UNIVERSITÁRIO. Dispõe sobre o Regimento Interno do Centro de Tecnologia da Informação e Comunicação (CTIC). Resolução n. 693, de 20 de janeiro de 2011. **Lex:** Centro de Tecnologia da Informação e Comunicação (CTIC), Belém, 2011. Disponível em <https://www.ctic.ufpa.br/publicacoes/documentos/RI_CTIC.pdf>. Acessado em 21 dez. 2016.

CZARNY, B. **Network Access Control Technologies**. 2008. Disponível em: <https://www.opswat.com/sites/default/files/Network_Access_Control_Technologies.pdf>. Acesso em 13 mar. 2017.

DB-ENGINES. **DB-Engines Ranking**. 2017. Disponível em <http://db-engines.com/en/ranking>. Acessado em 28 mar. 2017.

ENDEAVOR BRASIL. **Prevenindo com o Compliance para não remediar com o caixa**. 2015. Disponível em <https://endeavor.org.br/compliance/>. Acessado em 28 mar. 2017.

FIORESE, M. **Uma Proposta de autenticação de usuários para ensino a distância**. UFGRS. Porto Alegre, 2000. Disponível em <http://www.lume.ufrgs.br/bitstream/handle/10183/80127/000277096.pdf>. Acessado em 28 mar. 2017.

FINGERBANK. **What is fingerbank?**. 2ª ed. Hacker Friendly LLC. Seattle, 2008. Disponível em <http://wndw.net/pdf/wndw-pt/wndw-pt-ebook.pdf>. Acessado em 25 out. 2016

FLICKENGER, R. **Redes sem fio no Mundo em Desenvolvimento**. 2ª ed. Hacker Friendly LLC. Seattle, 2008. Disponível em <http://wndw.net/pdf/wndw-pt/wndw-pt-ebook.pdf>. Acessado em 25 out. 2016.

GONÇALVES, F; FERREIRA, P. Cidades Conectadas: experiências de redes públicas de Internet sem fio em Barcelona, Taipei, Paris e Helsinque**. Caminhos para a universalização da internet banda larga: experiências internacionais e desafios brasileiros**. Intervozes: São Paulo, 1ª ed, p. 153-166, 2012. Disponível em <http://www.caminhosdabandalarga.org.br/wp-content/uploads/2012/10/Caminhos-para-a-universaliza%C3%A7%C3%A3o-da-Internet-banda-larga.pdf>. Acesso em 19 out. 2016.

GOUVÊA, J; MAGALHÃES, A. **Redes de Computadores - Curso Completo**. 10ª ed. Editora FCA, 2013.

GUIMARÃES, R. **Análise comparativa de "sistemas de autenticação" utilizados em Internetbanking**. 2006. Disponível em <http://www.lsi.usp.br/~volnys/academic/trabalhos-orientados/Analise-comparativa-de-sistemas-de-autenticacao-utilizados-em-internetbanking.pdf>. Acessado em 28 mar. 2017.

H3C TECHNOLOGIES CO. **SSH Technology White Paper**. 2009. Disponível em: <http://www.h3c.com.hk/Products___Technology/Products/Switches/Data_Center_Switches/H3C_S12500_Series_Switches/White_Paper/200906/641548_57_0.htm>. Acesso em 13 mar. 2017.

INFLOBOX. **Infoblox DHCP Fingerprinting Enabling Endpoint Discovery and Control**. 2016. Disponível em <https://www.infoblox.com/wp-content/uploads/2016/04/Infoblox-note-dhcp-fingerprinting-enabling-end-point-discovery-and-control.pdf>. Acessado em 21 dez. 2016.

INVERSE. **Packetfence: Administration Guide**. 2017. Disponível em <https://packetfence.org/doc/PacketFence_Administration_Guide.html>. Acessado em 28 mar. 2017.

IPASS. **Wifi Growth Map**. 2017. Disponível em <http://www.ipass.com/wifi-growth-map/>. Acessado em 20 jan. 2017.

IREO. **Network Access Control**. 2017. Disponível em: <http://www.ireo.com/pt/solucoes/seguranca/network-access-control-nac/>. Acesso em 13 mar. 2017.

ISHIKIRIYAMA, L. **Medição de throughput nas redes em malha sem fio**. 2006. Disponível em <http://www.midiacom.uff.br/~schara/alunos/leonardo-mt.pdf>. Acessado em 20 dez. 2016.

JUCC - JOINT UNIVERSITIES COMPUTER CENTRE. **Network Access Control**. 2013. Disponível em <https://ito.hkbu.edu.hk/pub/is_newsletter/professional/Issue_09_NAC/JUCC%20Newsletter-IT-9%20NAC.pdf>. Acessado em 29 mar. 2017.

KUROSE, R; ROSS, K. **Redes de Computadores e a Internet. Uma Abordagem Top Down**. 6ª ed. PEARSON. São Paulo, 2013.

LAZOTI, R. **Armazenando dados com Redis**. 1ª ed. Casa do Código. São Paulo, 2014.

MAURO, D; SCHMIDT, K. **Essential SNMP**. O'Reilly. Sebastopol, CA, 2005.

MICHIGAN. **Hotspot Mikrotik**. 2016. Disponível em <http://www.michigan.com.br/downloads/mikrotik/Hotspot-Mikrotik.pdf>. Acessado em 21 dez. 2016.

MOREIRAS, A. et al. **IPv6 Básico**. NIC.br. São Paulo, 2012.

MKT SOLUTION; LANCORE NETWORKS. Treinamento Mikrotik - Certificação MTCNA. 2012. Disponível em: <https://mikrotikbrasil.files.wordpress.com/2012/10/treinamento-mikrotik-mtcna.pdf>. Acessado em 19 out. 2016.

NETCRAFT. **February 2017 Web Server Survey**. 2017. Disponível em: <https://news.netcraft.com/archives/2017/02/27/february-2017-web-server-survey.html>. Acesso em 13 mar. 2017.

NETGATE. **Service Providers**. 2017. Disponível em: <https://www.netgate.com/appliances/pfsense-service-providers.html>. Acesso em 13 mar. 2017.

OLIVEIRA, A; CUNHA, P. Implementação da solução Mikrotik para reestruturação da rede da Fundação Nacional de Saúde no Estado do Pará. CESUPA. Belém, 2012. Disponível em: <http://getlan.blogspot.com.br/2012/07/tcc-implementacao-da-solucao-mikrotik.html>. Acessado em 19 out. 2016.

ORACLE CORPORATION. **About MySQL**. 2017a. Disponível em: <https://www.mysql.com/about/>. Acesso em 13 mar. 2017.

ORACLE CORPORATION. **MySQL 5.7 Reference Manual: The Main Features of MySQL**. 2017b. Disponível em: <https://dev.mysql.com/doc/refman/5.7/en/features.html>. Acesso em 13 mar. 2017.

REDE NACIONAL DE ENSINO E PESQUISA (RNP). **Introdução a Gerenciamento de Redes TCP/IP**. 1997. Disponível em <https://memoria.rnp.br/newsgen/9708/n3-2.html#ng-simple>. Acessado em 28 mar. 2017.

RONCOLATO, M. Marco Civil – Apoio é o que não falta. **Revista .Br - Publicação do Comitê Gestor da Internet no Brasil**. Brasília, 5ª ed., ano 4, p. 5 -11, 2013.

RUFINO, N. **Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambientes Wifi e Bluetooth**. 3ª ed. São Paulo, 2015.

SILVA, D; MENDES, L. Proposta de Implementação de hotspot wireless na Unipac - Campus Magnus. UNIPAC. Barbacena, 2016. Disponível em: <http://www.unipac.br/site/bb/tcc/tcc-19b225ca0c6a52895fad5a7a783e3b49.pdf>. Acessado em 19 mar. 2017.

SINDIGRU. **GRU Airport amplia wifi grátis para usuários**. 2014. Disponível em <http://sindigru.org.br/noticia/779-gru-wifi-usuarios>. Acessado em 20 jan. 2017.

SOUZA, A; LOPES, D. **Controle de Acesso à Rede com PacketFence**. SENAI. Goiânia, 2011. Disponível em <http://www.academia.edu/8657388/Controle_de_Acesso_a_Rede_com_PacketFence>. Acessado em 12 nov. 2016.

SSH COMMUNICATIONS SECURITY CORP. **SSH SecureShell for UNIX Servers Administrator's Guide**. 2000. Disponível em <http://www.if.usp.br/pub/unix/security/ssh2-adminguide.pdf>. Acessado em 28 mar. 2017.

STARBUCKS. **Wifi**. 2017. Disponível em <https://www.starbucks.com.br/coffeehouse/wireless-internet>. Acessado em 20 jan. 2017.

TANABLE NETWORK SECURITY. **Nessus Compliance Checks: Auditing System Configurations and Content**. 2017. Disponível em <https://support.tenable.com/support-center/nessus_compliance_checks.pdf>. Acessado em 28 mar. 2017.

TANENBAUM, A. **Rede de Computadores**. 5ª ed. Elsevier. Rio de Janeiro, 2011.

WNDW. **Redes sem fio no Mundo em Desenvolvimento**. 2008. Disponível em <http://wndw.net/pdf/wndw-pt/wndw-pt-ebook.pdf>. Acessado em 17 nov. 2016.

# APENDICE

# APENDICE A – INSTALAÇÃO E CONFIGURAÇÃO DO PACKETFENCE

## 1. REQUISITOS DE SISTEMA

PacketFence utiliza muitos componentes em uma infraestrutura. Assim, os seguintes componentes são necessários estarem instalados e configurados:

- Servidor de Banco de Dados: MySQL
- DHCP *Server*: ISC DHCP

### 1.1. REQUISITOS MÍNIMOS DE HARDWARE

- Processador Intel ou AMD CPU 3 GHz
- 8 GB de memória RAM
- 100 GB de espaço livre em disco rígido (RAID 1 recomendado)
- Uma placa de rede (recomenda-se duas placas)

### 1.2. REQUISITOS DO SISTEMA OPERACIONAL

- Red Hat Enterprise Linux 6.x e 7.x Server
- *Community Enterprise Operating System* (CentOS) 6.x ou 7.x
- Debian 7.0 (Wheezy) ou Debian 8.0 (Jessie)

## 2. INSTALAÇÃO E CONFIGURAÇÃO DO PACKETFENCE

A instalação a seguir foi feita em uma Máquina Virtual (VM), com utilizando Debian 8.0 (Jessie).

### 2.1. INSTALAÇÃO

I). Primeiramente, realizar o *update* e *upgrade* do sistema.

```
$ sudo apt-get update
```

```
$ sudo apt-get upgrade
```

II). Ativar o encaminhamento IP no servidor. Para fazê-lo permanentemente, procure no */etc/sysctl.conf* e defina a seguinte linha:

```
# Controls IP packet forwarding
```

```
net.ipv4.ip_forward = 1
```

III). Fazer as devidas configurações do DHCP nos arquivos */etc/default/isc-dhcp-server* e */etc/dhcp/dhcpd.conf*. Verifique as configurações do seu sistema operacional.

IV). Para disponibilizar e usar o repositório, criar um arquivo chamado */etc/apt/sources.list.d/packetfence.list*, contendo:

```
echo 'deb http://inverse.ca/downloads/PacketFence/debian jessie jessie' > /etc/apt/sources.list.d/packetfence.list
```

V). Uma vez definido o repositório, instalar o PacketFence com todas as suas dependências e os serviços externos necessários. Obs.: Os pacotes para ajudar na tradução de novos arquivos são, também, instalados:

```
$ sudo apt-key adv --keyserver keys.gnupg.net --recv-key 0x810273C4
$ sudo apt-get update
$ sudo apt-get install packetfence perlmagick libswitch-perl liblocale-msgfmt-perl gettext
```

VI). Uma vez instalado, a interface de configuração baseada na Web será iniciada automaticamente. Caso contrário, acessar em*: https://@IP_Packetfence:1443/configurator*.

## 2.2. CONFIGURAÇÃO

**Passo 1:** Aplicação - Escolher o mecanismo da aplicação.

I) Selecione a opção "*Inline enforcement*".

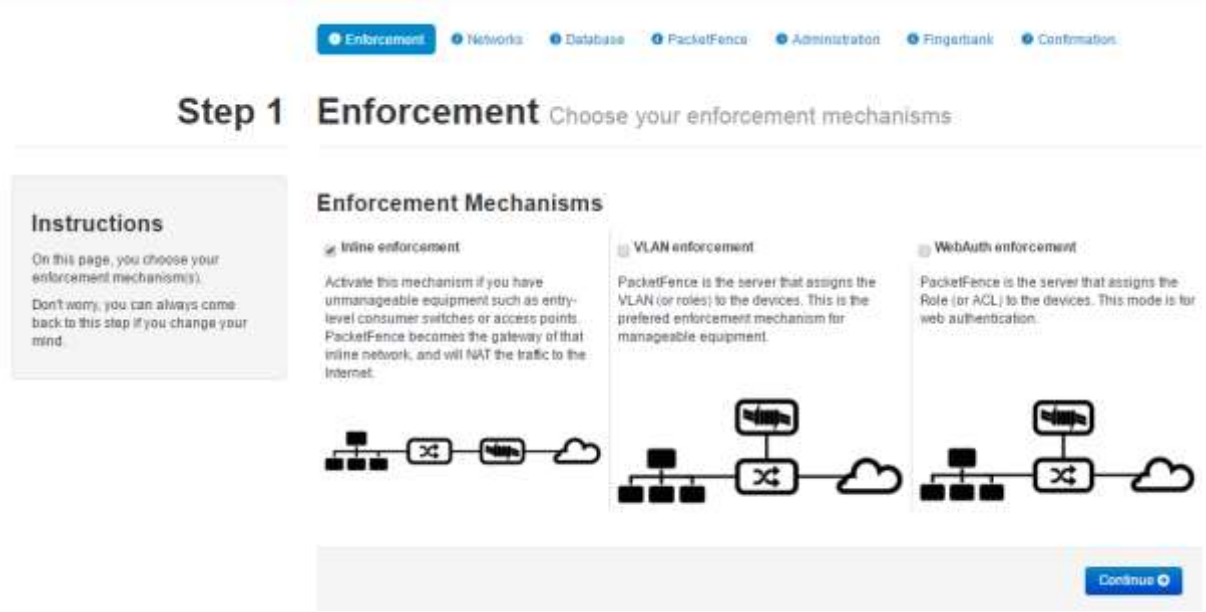



Figura 29 - Tela dos Mecanismos da Aplicação
Fonte: Elaborado pelo autor (2017)

**Passo 2:** Rede - Ativação das interfaces de rede e criação de *VLANs*

I). Configurar as interfaces de rede e *IPs* para *management* e *inline layer 2*.


Figura 30 - Tela de Configuração de Redes
Fonte: Elaborado pelo autor (2017)

**Passo 3:** Configuração da Base de Dados - Criação de usuário e Base de Dados no MySQL *Server*

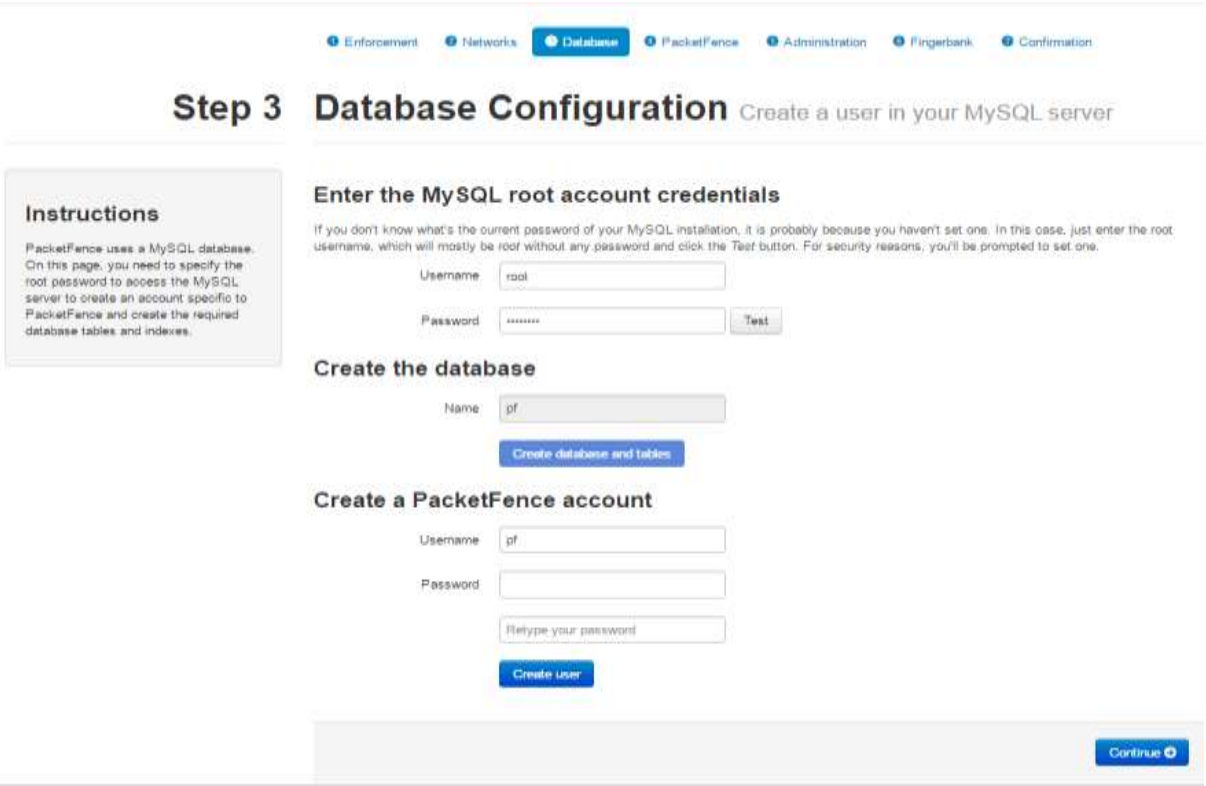



Figura 31 - Tela de Configuração do MySQL
Fonte: Elaborado pelo autor (2017)

**Passo 4:** Configuração do PacketFence - Informações referentes ao NAC

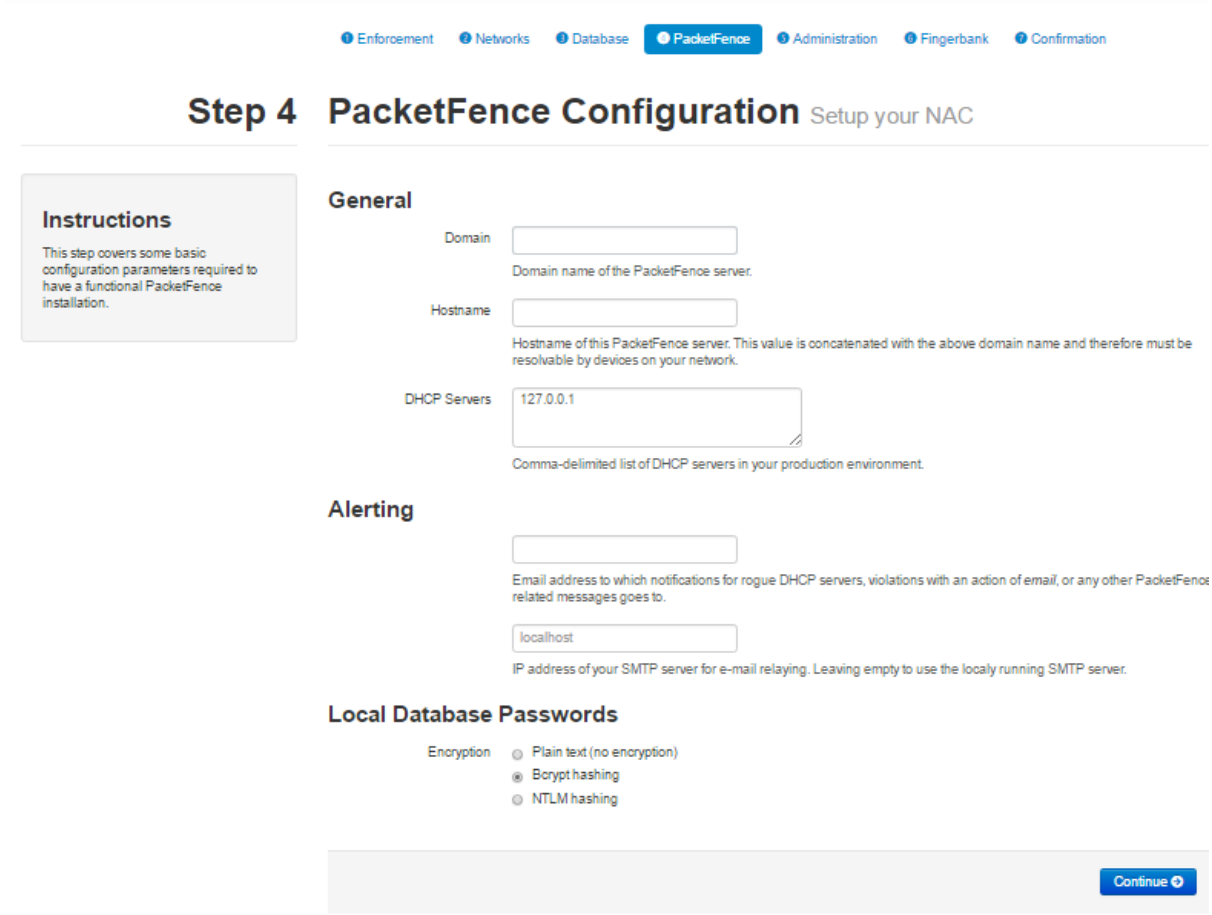



Figura 32 - Tela de Configuração do PacketFence
Fonte: Elaborado pelo autor (2017)

**Passo 5:** Administração - Acessar interface de administração

I) Informar a Senha de acesso ao sistema

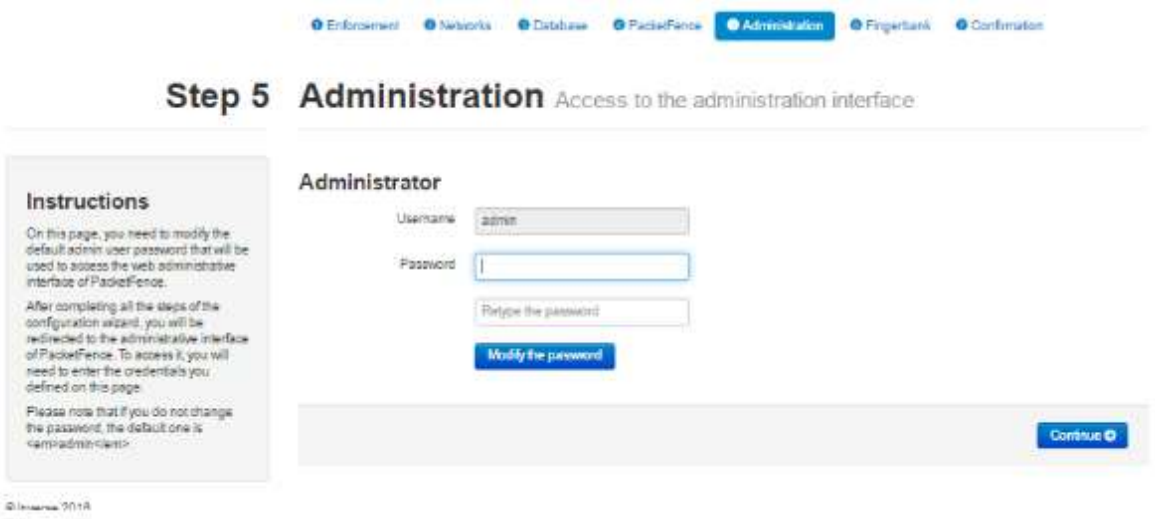



Figura 33 - Tela de Administração – Login
Fonte: Elaborado pelo autor (2017)

**Passo 6:** Fingerbank

I). Continuar

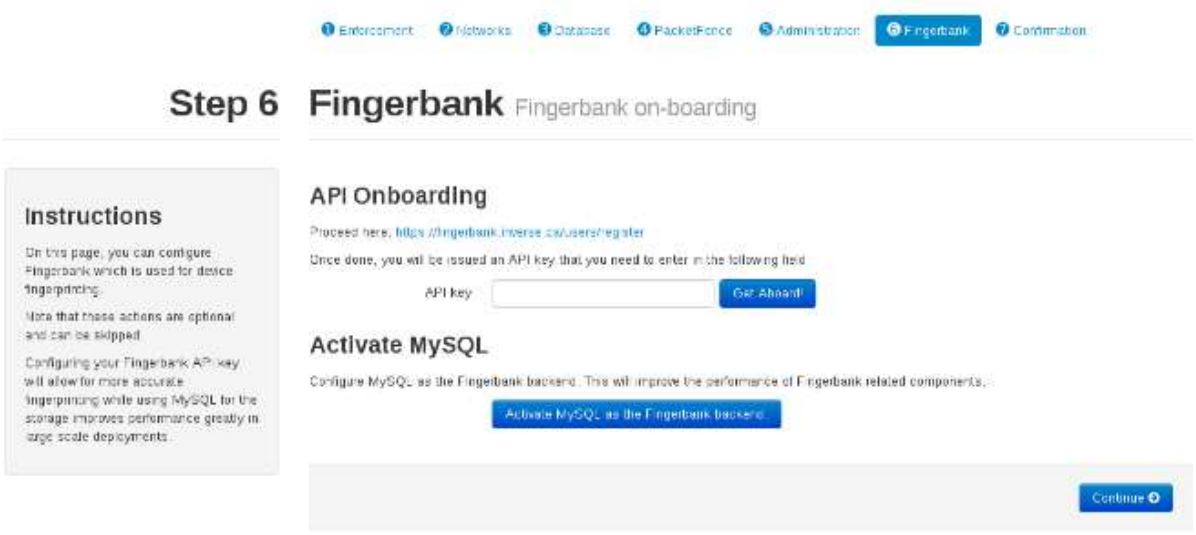



Figura 34 - Tela de Fingerbank
Fonte: Elaborado pelo autor (2017)

**Passo 7:** Iniciar os serviços - Proteção de Rede

I). Iniciar todos os serviços

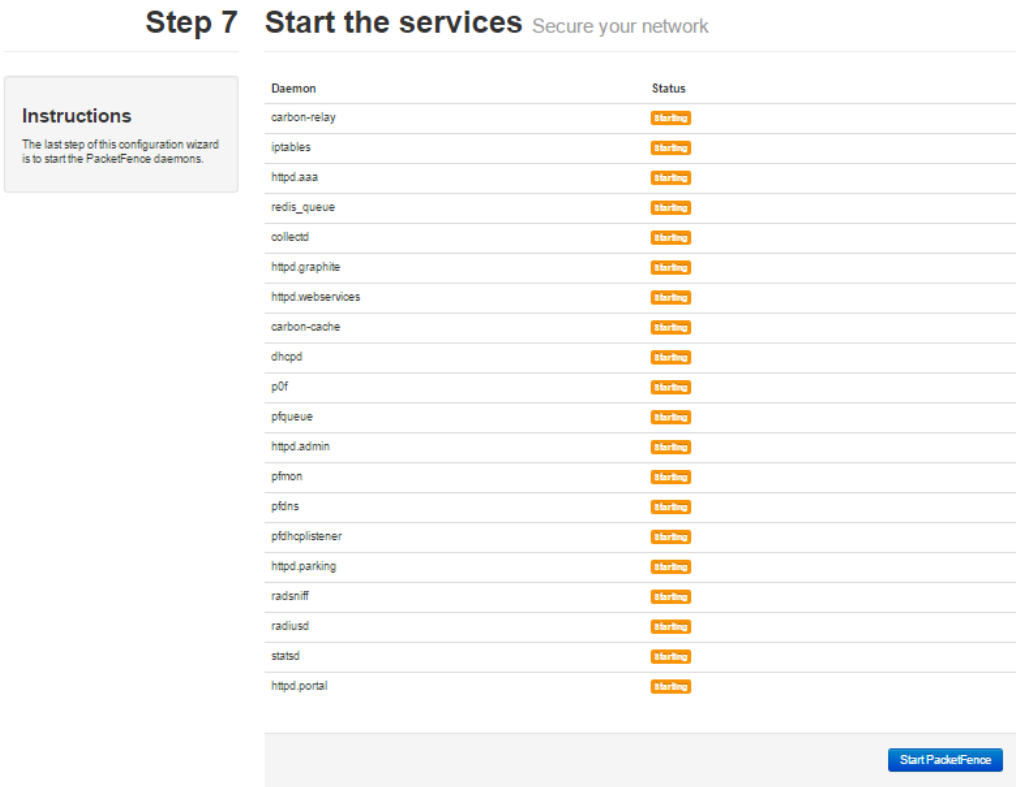



Figura 35 - Tela de Serviços
Fonte: Elaborado pelo autor (2017)

**Passo 8:** Conclusão

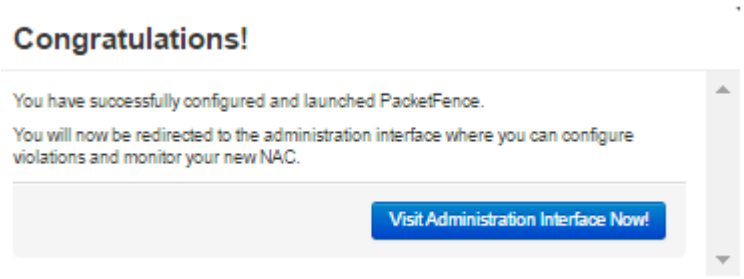



Figura 36 - Tela de finalização da Configuração do PacketFence
Fonte: Elaborado pelo autor (2017)

## 3. PACKETFENCE - PORTAL ADMINISTRAÇÃO

I). Iniciar o portal

```
$ sudo /usr/local/pf/bin/pfcmd service httpd.portal start
```

II) acessar a interface *Web* pelo IP configurado. Ex: https://@IP_Packetfence:1443/admin.

III) adicionar o método SMS como autenticação: *Configuration* → *Sources* → *Add Source* → *External* → *SMS* → *New Source* (Figura 37)

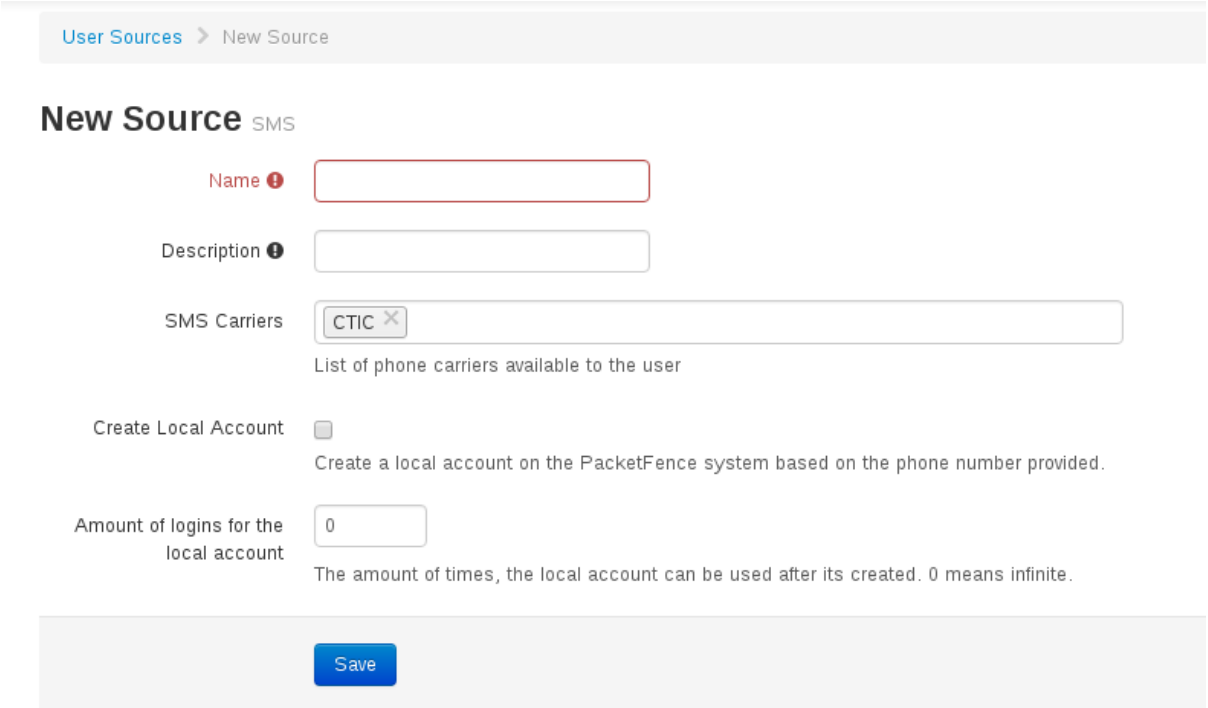



Figura 37 - Tela para adicionar nova fonte
Fonte: Elaborado pelo autor (2017)

.

IV) ativar o SMS como método de ingresso

a) *Configuration →Portal Profiles → Default → Settings → Sources →* + (adicionar)

b) selecionar o método *SMS* e salvar. Após, a janela "*Add Rule*" solicitará informações a respeito das regras (Figura 38).

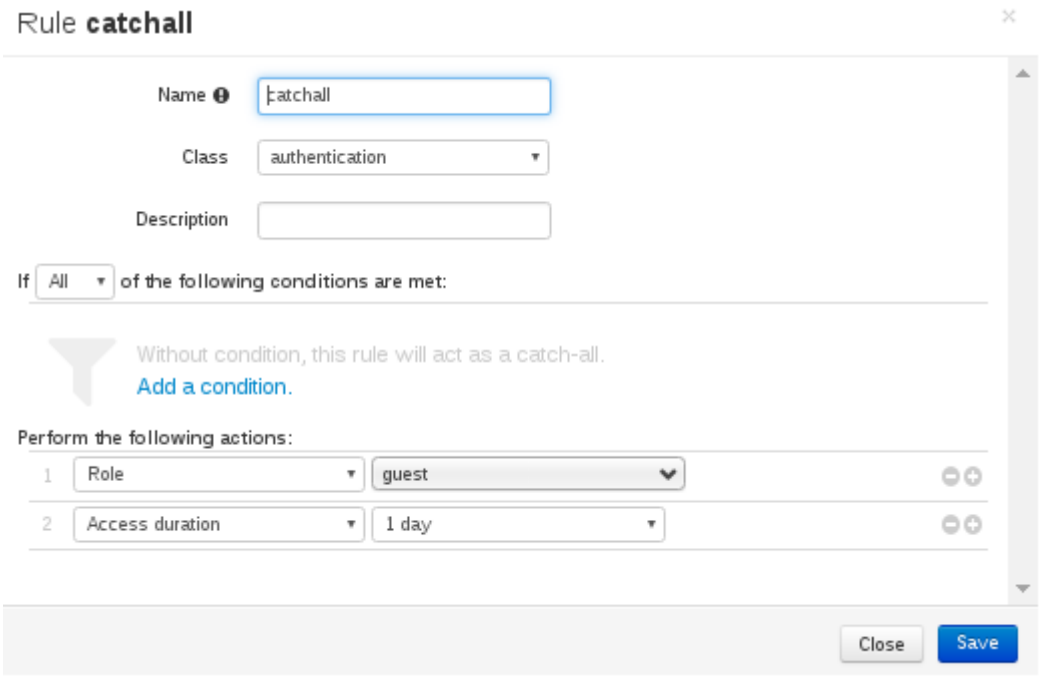



Figura 38 - Tela para adicionar as regras
Fonte: Elaborado pelo autor (2017)

c) preencha os campos *Name* e *Class* com os valores *catchall* e *authentication*, respectivamente;

d) acione as seguintes condições (*Perform the following actions*):

*a) Role → guest;*
*b) Access duration →* 1 *day*.

V) Alterar o Termos de Uso: *Configuration →Portal Profiles →default →Captive Portal →files → aup_text.html*

VI) alterar imagem (logo) e idioma do portal de captura: *Configuration →Portal Profiles →default →Captive Portal* (Figura 39)

a) logo;
b) *languages*;

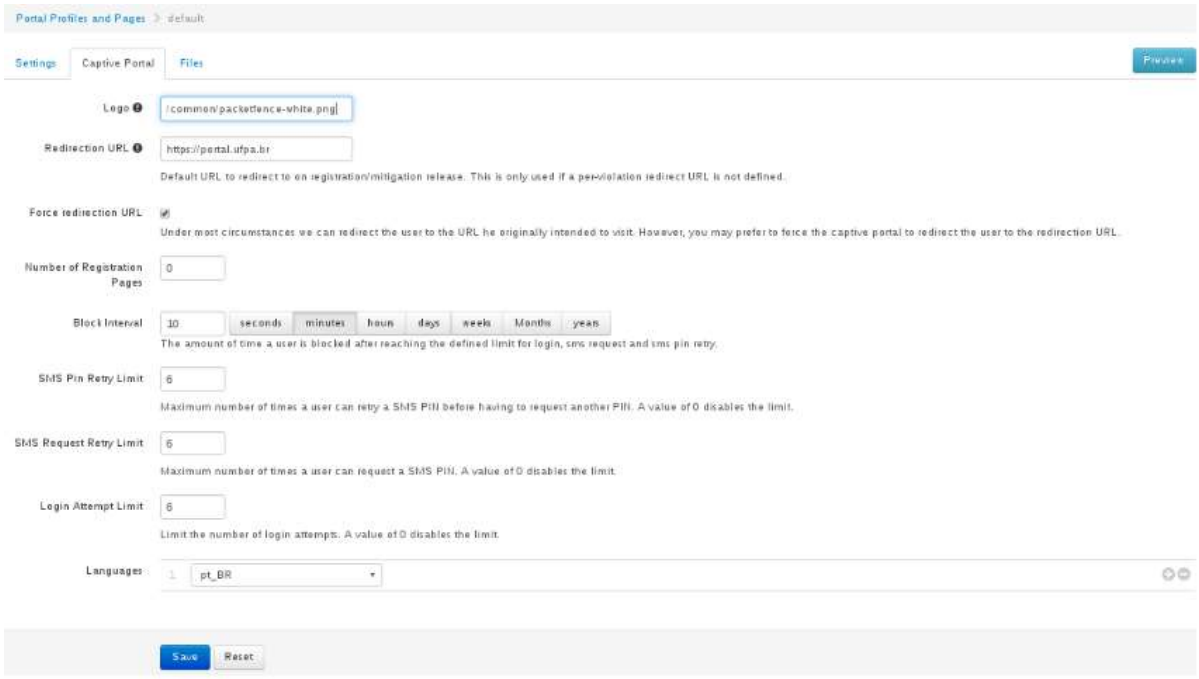



Figura 39 - Tela Configurações do Captive Portal
Fonte: Elaborado pelo autor (2017)

VII) alterar tempo de duração dos acessos dos usuários: *Configuration→ Access Duration*

VIII) adicionar os campos obrigatórios no método de ingresso do *Captive Portal* (Figura 40): *Configuration →Portal Module →Authentication → default_guest_policy →Mandatory fields*

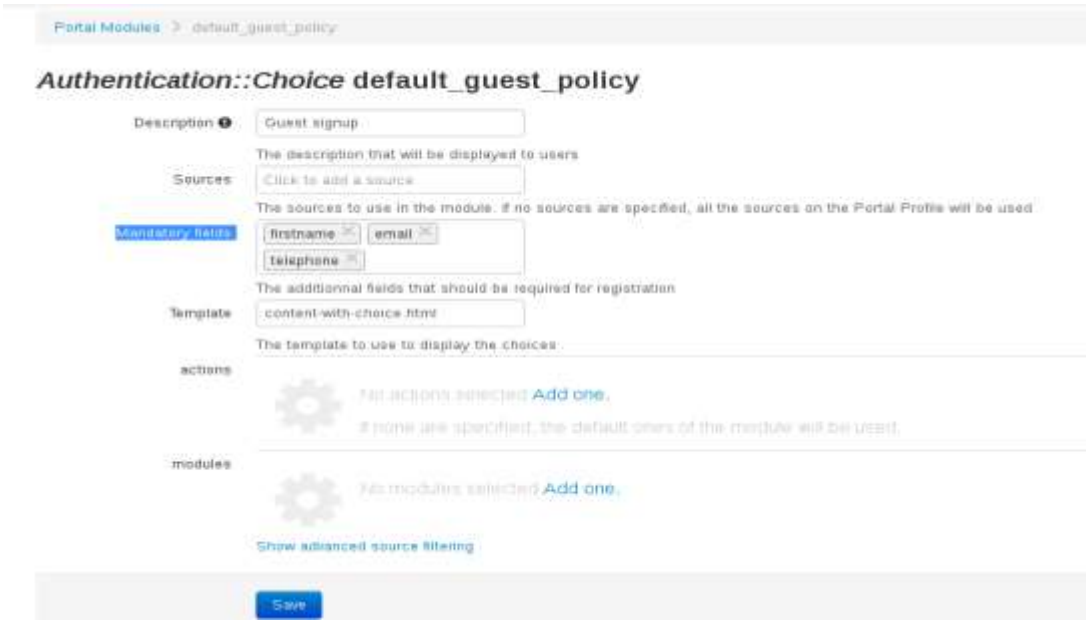



Figura 40 - Tela Autenticação: adicionar campos obrigatórios
Fonte: Elaborado pelo autor (2017)

3.1. TRADUÇÃO DO SISTEMA

I) Arquivo de tradução em português

/usr/local/pf/conf/locale/pt_BR/LC_MESSAGES/packetfence.po

II) gerar o bin de tradução

$ sudo /usr/bin/msgfmt packetfence.po --output-file packetfence.mo

## 4. CONFIGURAÇÕES EXTRAS

Importante ressaltar a necessidade de configurar, de acordo com o Sistema Operacional utilizado, os seguintes arquivos:

I) *Firewall*

/usr/local/pf/conf/iptables.conf

II) Diretórios SSL

/usr/local/pf/raddb/certs/server.key

/usr/local/pf/conf/ssl/apodi.crt

III) Arquivos importantes de log do PacketFence:

- PacketFence Core Log: /usr/local/pf/logs/packetfence.log
- Captive Portal Access Log (Apache): /usr/local/pf/logs/httpd.portal.access
- Captive Portal Error Log (Apache): /usr/local/pf/logs/httpd.portal.error
- Web Admin/Services Access Log (Apache): /usr/local/pf/logs/httpd.admin.access
- Web Admin/Services Error Log (Apache): /usr/local/pf/logs/httpd.admin.error
- Webservices Access Log (Apache): /usr/local/pf/logs/httpd.webservices.access
- Webservices Error Log (Apache): /usr/local/pf/logs/httpd.webservices.error
- AAA Access Log (Apache): /usr/local/pf/logs/httpd.aaa.access
- AAA Error Log (Apache): /usr/local/pf/logs/httpd.aaa.error