CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Manoel Américo Zancheta

MECANISMOS DE SEGURANÇA DA INFORMAÇÃO APLICADOS À DOMÓTICA

Americana, SP

2017

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Manoel Américo Zancheta

MECANISMOS DE SEGURANÇA DA INFORMAÇÃO APLICADOS À DOMÓTICA

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do Prof.(o) especialista Edson Roberto Gaseta.

Área de concentração: mecanismos de Segurança Informação.

Americana, SP

2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Z31m ZANCHETA, Manoel Américo

Mecanismos de segurança da informação aplicados à domótica ./ Manoel Américo Zancheta. – Americana: 2017.

63f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp.Edson Roberto Gaseta

1. Comunicação de dados 2. Segurança em sistemas de informação I.GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519
681.518.5

Manoel Américo Zancheta

MECANISMOS DE SEGURANÇA DA INFORMAÇÃO APLICADOS À DOMÓTICA

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação.

Americana, 26 de Junho de 2017.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)

Especialista

FATEC Americana

Diógenes de Oliveira (Membro)

Mestre

FATEC Americana

Renato Kraide Soffner (Membro)

Doutor

FATEC Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus por me dar forças para concluir o curso, aos meus pais, amigos de sala, corpo docente e todas as pessoas que de direta ou indiretamente me incentivaram a continuar os estudos.

DEDICATÓRIA

Aos meus pais pelo apoio de sempre e aos meus filhos, como exemplo para que tenham gosto pelos estudos desde pequenos.

RESUMO

O presente trabalho de conclusão de curso tem por objetivo mostrar o conceito de domótica, os protocolos de comunicação, equipamentos e os fundamentos de Segurança da Informação aplicados à sua implementação. Domótica (do latim Domus (casa) mais a junção de robótica), é o termo utilizado para definir a automação de residências, permitindo que eletro eletrônicos (portões, lâmpadas, TVs, micro-ondas, alarmes, etc) sejam controlados de qualquer lugar, bastando para isso apenas, ter uma conexão de internet disponível. São diversas as finalidades de aplicação da domótica, tais como: conforto, segurança, acessibilidade (idosos, portadores de deficiências temporárias e/ou permanentes), monitoramento, economia de energia, etc. Em contra partida a todos estes benefícios oferecidos pela domótica, a disponibilidade global de acesso à mesma expõem o controle da automação à pessoas não autorizadas, logo torna-se imprescindível aplicar mecanismos de segurança da informação. Estes mecanismos de segurança visam manter a automação a níveis aceitáveis de segurança e nesse contexto, serão estudados os seguintes mecanismos: Injection de SQL (inserção de comandos SQL no login de acesso de aplicações), criptografia de dados (“embaralhamento de dados”), logs de acessos à automação (histórico dos acessos na automação em base MySQL(banco de dados)) e implementação de *Firewall* no Linux (ipTables).

Palavras Chave: domótica; segurança; portas de comunicação.

ABSTRACT

This The present work of course completion aims to show the concept of home automation, communication protocols, equipment and the fundamentals of Information Security applied to its implementation. Domotic (from the Latin Domus plus the robotic junction) is the term used to define home automation, allowing electronic electronics (gates, lamps, TVs, microwaves, alarms, etc.) to be controlled from anywhere , Just by having an internet connection available. There are several purposes for the application of home automation, such as: comfort, safety, accessibility (elderly, temporary and / or permanent deficiency), monitoring, energy saving, etc. Contrary to all these benefits offered by domotics, the global availability of access to it exposes the control of automation to unauthorized persons, so it becomes imperative to apply information security mechanisms. These security mechanisms aim to maintain automation to acceptable levels of security and in this context, the following mechanisms will be studied: Injection of SQL (insertion of SQL commands in the login of applications access), data encryption ("data shuffling"), Logs of access to automation (history of accesses in the automation in base MySQL (database)) and implementation of Firewall in Linux (ipTables).

Keywords: *home automation; safety; Communication ports.*

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIAÇÕES

AC – *Alternating Current* (Corrente alternada).

ADSL - *Asymmetric Digital Subscriber Line*.

AR – Automação Residencial.

AURESIDE - Associação Brasileira de Automação Residencial e Predial.

BACNET - *Building Automation and Control Network.*

BPS – bits por segundo.

CEBUS - *Consumer Eletronics Bus*.

CID – Confidencialidade, Integridade e Disponibilidade.

CLP - Controladores Lógico-Programáveis.

CSMA - *Carrier Sense Multiple Access*.

CSMA/CA - *Carrier Sense Multiple Access With Collision Avoidance*.

CSMA/CD - *Carrier Sense Multiple Access Collision Detection*.

DHCP - *Dynamic Host Configuration Protocol* - Protocolo de Configuração Dinâmica de Host.

DNS - *Domain Name System* – Sistema de Nomes de Domínios.

EIB - *European Installation Bus.*

EEPROM - *Electrically-Erasable Programmable Read-Only Memory.*

EHS - *European Home Systems.*

FO – Fibra Óptica.

HDTV - *High-Definition Television.*

HTTP – *Hypertext Transfer Protocol* – Protocolo de Transferência de Hipertexto.

IoT - *Internet of Things* (Internet das Coisas).

IDE - *Integrated Development Environment* - Ambiente de Desenvolvimento Integrado)

IETF - *Internet Engineering Task Force.*

IP - *Internet Protocol.* É o principal protocolo de comunicação da Internet.

IR - infra vermelho.

MBPS - megabit por segundo.

OSI - *Open Systems Interconnection.*

RAM - *Random Access Memory.*

RF - rádio frequência.

RFC - *Request for Comments.*

ROM - *Read Only Memory.*

RS232 – *Recommend Standard* – 232 (Comunicação Serial)

SI – Segurança da Informação.

UPB - *Universal Powerline Bus.*

UTP - *Unshielded Twisted Pair.*

VCR - V*ideo Cassette Recorder.*

VDC - *Voltage Direct Current.*

XSS ou **CSS** - *Cross-Site Scripting*

SUMÁRIO

1. INTRODUÇÃO

Na década de 60, a automação estava mais voltada para a indústria com o intuito de desenvolver máquinas para realizar tarefas feitas até então pelo homem. Com o passar do tempo, porém, a automação passou a fazer parte dos lares, principalmente em prédios e condomínios. No início, os equipamentos e as tecnologias disponíveis eram muito caros, sendo considerados então, como artigos de luxo acessível somente à classe alta.

Com o avanço tecnológico e o barateamento dos equipamentos, a automação residencial popularizou-se e passou a ser utilizada para racionamento de recursos de água e energia, segurança, como auxílio à deficientes físicos e idosos. A automação residencial, passou a oferecer além de conforto, uma melhora considerável na qualidade de vida das pessoas.

O aumento da expectativa de vida, a inclusão da mão-de-obra feminina no mercado de trabalho, o crescimento da violência, a urbanização e redução do número de filhos tem aumentado significativamente o isolamento das pessoas em suas residências, gerando novas necessidades.

No caso de idosos, a automação residencial oferece benefícios que minimizam as barreiras que dificultam suas atividades da vida independente. Conforme Camarano (2002, p. 7), “viver só pode ser um estágio temporário do ciclo de vida e pode estar refletindo preferências”. Na Europa onde a expectativa de vida é alta, os projetos visando atender aos idosos fomentaram o crescimento da domótica.

Bolzani (2004) enfatiza ainda que, embora existam equipamentos entre mecânicos e elétricos, que proporcionam certa autonomia a um deficiente físico, estes equipamentos tendem a ter valores altos e possuir uma estrutura delicada. Os sistemas de automação residencial surgem como uma alternativa em relação a custo e soluções a fim de auxiliar portadores de deficiência. Um sistema de automação residencial possibilitaria controlar a iluminação, abertura e fechamento de portas, cortinas, monitoramento das câmeras de segurança em qualquer ponto da residência através de um simples controle remoto

O número de casas automatizadas vem crescendo no mundo todo e segundo a AURESIDE - Associação Brasileira de Automação Residencial e Predial, “globalmente o mercado de automação deve crescer de US$ 32 bilhões em 2015 para U$ 78 bilhões em 2022, uma taxa composta de 12,5%” (AURESIDE, 2016).

Pode-se citar como fomentadores deste fato, o crescimento do mercado de IoT (*Internet of Things*), a redução de custos, o grande número de fabricantes e a crescente importância do monitoramento remoto das residências (AURESIDE, 2016).

Muratori e Dal Bó (2014, p.197-198), dizem o seguinte sobre IoT:

> “A Internet tal qual a conhecemos desde a década de 90 é apenas o início de uma era de conectividade crescente a quase infinita... Hoje ainda a maior parte dos *end-nodes* conectados à internet é representada por pessoas utilizando seu computadores, *notebooks*, *tablets* e *smartphones*. No entanto, isso está mudando muito rapidamente e equipamentos tão diversos como câmeras, veículos, *set_top_boxes* e outros estão aumentando o saldo de nós representados por máquinas e não pessoas conectadas. No futuro próximo, claramente a quantidade de nós representados por coisas vai superar em grande escala a internet das pessoas. As previsões falam em algo como 100 para 1, só para começar...”

Na IoT, os objetos devem ser capazes de interagir e comunicar-se entre si, trocar informações coletadas do ambiente, reagindo de forma autônoma aos eventos do mundo real, bem como influenciar este contexto sem intervenção direta do homem.

Vale ressaltar porém, que a IoT contempla todas as coisas, inclusive a domótica, mas não obrigatoriamente. Outras formas de controles podem ser utilizadas para controle de objetos, como sensores e relês, mesmo que os objetos a serem controlados não possuam um protocolo próprio de comunicação e/ou um IP (*Internet Protocol)* para comunicação na rede.

Com todo este avanço nos controles de dispositivos e ativos de forma remota, vários são os casos de invasões em sistemas automatizados, onde o invasor passa a ter o controle da automação de forma não autorizada.

Um fato ocorrido em 2015 nos Estados Unidos com um automóvel da fabricante Chrysler (GUSMÃO, 2015), obrigou a empresa a realizar um *recall* de 1,4

milhão de carros para corrigir uma brecha de segurança para incluir um bloqueio da vulnerabilidade na rede operadora norte-americana Sprint, usada por *hackers* para rastrear carros.

Em Moscou (OLHAR DIGITAL, 2011), uma outra ocorrência sobre invasão chamou a atenção nos meios de comunicação. Um hacker russo, Igor Blinnikov, pegou um ano e cinco meses de prisão após conseguir invadir um *outdoor* eletrônico na região de Garden Ring Road, no centro de Moscou, e transmitir imagens pornográficas. Igor realizou a invasão usando o próprio computador na cidade de Novorossiysk, distante 1,2 mil Km do local.

Fato semelhante (MOREIRA, 2016), ocorreu em 30/09/2016 em Jacarta (cidade com maior população islâmica do mundo e leis rígidas contra a pornografia), Indonésia, onde cenas de um filme pornográfico foram exibidas por cinco minutos, no horário do rush, em um outdoor eletrônico. Responsáveis da empresa que operam o outdoor, justificaram o problema como consequência de uma ação de infecção por vírus.

Estes fatos mencionados, e tantos outros ocorridos, e o crescimento da demanda por automação residencial no Brasil, justificam a escolha do tema para a elaboração deste trabalho, oferecendo mecanismos de segurança da informação aplicados à domótica com o objetivo de minimizar riscos e tentativas de invasões por terceiros e consequentemente, evitar que os mesmos obtenham o controle da automação da residência.

O **objetivo geral** é implantar mecanismos de segurança da informação aplicados à domótica em um ambiente residencial real, a fim de realizar o controle seguro da automação e diagnosticar possíveis tentativas de invasão por usuários não autorizados, minimizando os riscos de possíveis ataques.

Os **objetivos específicos** são: promover a segurança em uma ambiente residencial real através de *firewall*, levantar possíveis portas com permissão de acesso externo, verificar as tentativas de acesso à automação, desenvolver sistema de criptografia para os dados trafegados, levantar estatísticas de fluxo na rede, colaborar para que a automação possa trazer mais conforto e praticidade ao lar, não sendo somente um aparato tecnológico que ofereça apenas comodidade.

O presente trabalho está divido nos seguintes capítulos:

- Capítulo 1 Introdução
- Capítulo 2 Conceitos de domótica
- Capítulo 3 Mercado
- Capítulo 4 Protocolos de comunicação
- Capítulo 5 Microcontroladores
- Capítulo 6 Estudo de Caso
- Capítulo 7 Conclusão

A elaboração do presente trabalho contempla as etapas elencadas abaixo:

- **Levantamento Bibliográfico:** a metodologia empregada para este trabalho baseou-se em pesquisas bibliográficas, sendo pesquisados como palavras-chaves os termos domótica e automação residencial, apresentados no capítulo 2, existentes em revistas, livros e internet;

- **Seleção do Material Bibliográfico:** após a leitura bibliográfica, haverá uma seleção do material a ser utilizado para a realização do trabalho escrito e da parte prática do mesmo;

- **Comparação dos Protocolos/Microcontroladores existentes:** será efetuada uma comparação entre protocolos de comunicação e micro controladores para análise de custo/benefício e utilização prática;

- **Modelo:** após a análise do material coletado, será escolhido um protocolo padrão a ser utilizado e do micro controlador para exemplificar a utilização do mesmo em automação residencial, propondo soluções e melhorias para o projeto;

- **Exemplos de Aplicação em Maquete:** construção de uma maquete para demonstrar a viabilidade da aplicação de automação residencial e demonstrar os conceitos utilizados na mesma. O projeto contemplará os recursos de automação

residencial porém não haverá preocupação com o quesito segurança da informação, o que a tornará um exemplo vulnerável

- **Exemplos de Aplicação em Ambiente Real:** elaboração de um projeto de automação residencial em ambiente real, aplicando conceitos de segurança da informação e oferecendo propostas de melhorias em relação ao projeto realizado na maquete.

2. DOMÓTICA

2.1. CONCEITO DE DOMÓTICA

Segundo Muratori e Dal Bó (2014, p.15), na Europa, a definição de domótica refere-se ao resultado da junção da palavra latina *Domus* (casa) com Robótica (controle automatizado).

Ainda Muratori e Dal Bó (2014, p.15), definem domótica da seguinte forma: “É um processo que, usando diferentes soluções e equipamentos, possibilita ao usuário usufruir o máximo de qualidade de vida na sua habitação”.

2.2. TIPOS DE INSTALAÇÕES ELÉTRICAS

2.2.1. AUTOMAÇÃO CENTRALIZADA

Na automação centralizada todos os retornos de lâmpadas, tomadas, cortinas, etc devem ser levados até um quadro de automação, sendo que, se a instalação for muito grande, é aconselhável ter mais de um quadro (MURATORI; DAL BÓ, 2014, p.93).

2.2.2. AUTOMAÇÃO DISTRIBUÍDA

Na automação distribuída os módulos de controles são instalados junto ao acionamento das cargas, permitindo uma independência entre os controles, pois se houver uma falha, ela é apenas local e não em toda a automação. Os módulos independentes podem ser interligados sem fio formando um sistema mais complexo (MURATORI; DAL BÓ, 2014, p. 97).

2.2.3. CONTROLADORES AUTÔNOMOS (*STAND ALONE*)

São controladores para automação de pequeno porte que tem por objetivo automatizar um único ambiente com vários equipamentos e várias interfaces de

acionamento (pulsadores, *keypads*, receptores infra vermelho, etc) (MURATORI; DAL BÓ, 2014, p. 97).

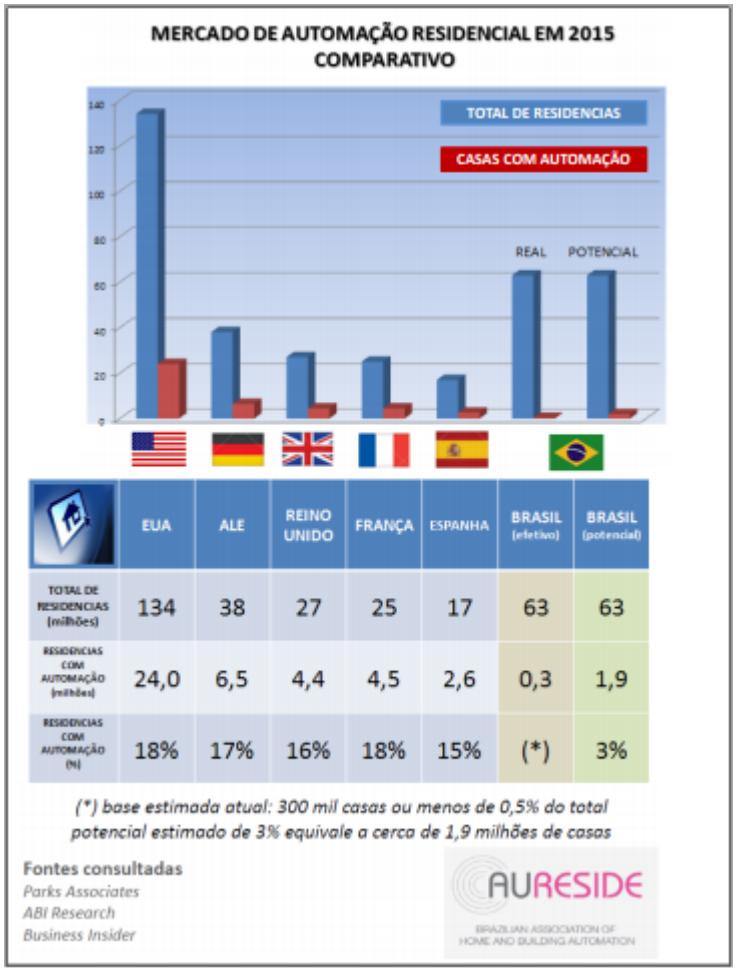
2.2.4. CENTRAIS DE AUTOMAÇÃO

As centrais de automação são voltadas para automações maiores, com mais pontos de entrada e saída, e normalmente são utilizados CLPs (Controladores Lógico-Programáveis), que normalmente possuem um alto custo além de possuir programação proprietária.

2.2.5. MERCADO DE AUTOMAÇÃO RESIDENCIAL

Conforme a figura 1, o gráfico demonstra o potencial de mercado, comparando o mercado brasileiro com o americano e o europeu. Neste demonstrativo, fica claro a maior demanda nos mercados americano e europeu e o potencial de crescimento do mercado brasileiro.

Figura 1 : Mercado Automação Residencial 2015



	EUA	ALE	REINO UNIDO	FRANÇA	ESPANHA	BRASIL (efetivo)	BRASIL (potencial)
TOTAL DE RESIDENCIAS (milhões)	134	38	27	25	17	63	63
RESIDENCIAS COM AUTOMAÇÃO (milhões)	24,0	6,5	4,4	4,5	2,6	0,3	1,9
RESIDENCIAS COM AUTOMAÇÃO (%)	18%	17%	16%	18%	15%	(*)	3%

(*) base estimada atual: 300 mil casas ou menos de 0,5% do total potencial estimado de 3% equivale a cerca de 1,9 milhões de casas

Fontes consultadas
Parks Associates
ABI Research
Business Insider

AURESIDE
BRAZILIAN ASSOCIATION OF HOME AND BUILDING AUTOMATION

Fonte: AURESIDE[1]

Segundo a AURESIDE (2016), a demanda por automação é maior nos países desenvolvidos do que nos emergentes (em crescimento), com uma grande evolução na eficiência de soluções de automação, principalmente no que se refere em automatizar qualquer processo doméstico. Diferentes empresas trabalham para padronizar a comunicação entre dispositivos, possibilitando a conexão entre eles. A internet de alta velocidade, desempenha um papel chave no crescimento da automação residencial nos EUA, Alemanha e França. A automação residencial tem um forte apelo no sentido de conservação de energia, por possibilitar que os aparelhos fiquem em *stand by*. Na América do Norte, EUA e Canadá possuem tecnologias avançadas que facilitam a adaptação de usuários para as novas

[1] Disponível em: < http://www.aureside.org.br/_pdf/potencial_2015.pdf>. Acessado em: abr. 2017.

tendências em domótica. Europa e Ásia seguem a América do Norte no consumo de soluções de automação com forte aumento da demanda para os próximos anos.

Conforme Muratori e Dal Bó (2014), a automação era vista como símbolo de *status*, um artigo de luxo. Com o crescimento de fabricantes e produtos e o consequente aumento na oferta, barateiram os custos dos mesmos, permitindo automatizações de portes menores para clientes de menor poder aquisitivo. Além do conforto proporcionado pela automação, outras tarefas da residência podem ser automatizadas e podem oferecer racionamento no consumo de energia e melhor segurança da residência. Pessoas com necessidades especiais e idosos também podem beneficiar-se de recursos que os auxiliarão no dia a dia como por exemplo: acionamento de luzes por comandos de voz, sensor de presença, etc. A oferta de internet banda larga e o uso de *tablets* e *smartphones*, auxiliam cada vez mais no controle remoto da automação residencial.

As novas tendências, segundo Muratori e Dal Bó (2014) para o mercado são:

- Automação para residências já existentes (reformas) pois até então, a maioria dos projetos eram feitos para novas residências;
- Migração de dados para a nuvem (*cloud computing*) onde ficam disponíveis servidores mais potentes e externos à residência;
- Aumento do monitoramento à distância, podendo ser oferecidos serviços remotos de acompanhamento de deficientes, doentes, idosos, etc;
- Aumento dos produtos do tipo *plug and play*, sem a necessidade de profissionais especializados;
- Padronização de protocolos com o intuito de tornar os sistemas interoperáveis;

- Aumento dos *end-nodes*, os pontos finais de uso, que hoje em dia são na maioria dos casos *smartphones*, *tablets* e *notebooks* pois com a popularização da IoT, todas as coisas passarão a ter um IP e fazer parte da rede (internet).

3. PROTOCOLOS DE COMUNICAÇÃO

3.1. DEFINIÇÃO DE PROTOCOLO

Conforme Tanenbaum (2011, p. 29), “um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação”.

De modo mais simplificado, um protocolo é um conjunto de regras e convenções para estabelecer comunicação entre dois equipamentos. Alguns protocolos são específicos para a AR (Automação Residencial), outros derivaram de protocolos já existentes e alguns possuem protocolos proprietários (protocolo do fabricante do equipamento).

“Um protocolo é representado por um conjunto de regras que definem a maneira como os equipamentos irão se comunicar em uma rede de dados” (MURATORI; DAL BÓ, 2014, p. 103).

Já Kurose e Ross (2013, p .7), comparam um protocolo fazendo uma analogia ao diálogo entre duas pessoas que pretendem iniciar uma conversa, onde o emissor inicia o diálogo e o destinatário pode, ou não, aceitar a solicitação do emissor:

> “Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento”.

Os protocolos utilizados no estudo de caso serão o protocolo serial (para o ambiente não seguro) e o protocolo TCP/IP para o ambiente seguro.

3.2. PROTOCOLO SERIAL

Conforme a National Instruments (2014), na comunicação serial, a porta serial envia e recebe bytes de informação um bit de cada vez. É mais lenta que a comunicação paralela por enviar um bit por vez contra um byte, porém pode atingir

distâncias maiores. Normalmente este protocolo é utilizado por interfaces seriais RS232.

A National Instruments (2014), define assim a comunicação serial:

> "Normalmente, a serial é usada para transmitir dados ASCII. A comunicação é completada usando 3 linhas de transmissão: (1) Terra, (2) Transmissão, e (3) Recepção. Visto que a serial é assíncrona, a porta está apta a transmitir dados em uma linha enquanto recebe dados em outra. Outras linhas estão disponíveis para *handshaking*, mas não são requeridas. As características importantes da serial são taxa de transmissão (*baud rate*), bits de dados (data bits), bits de parada (*stop bits*), e paridade."

De acordo com Dantas (2010), a interface serial RS232 surgiu na década de 60, foi criado pelo laboratório Bell para padronizar a interface de conexão entre equipamentos de dados e comunicação. Este protocolo possui uma limitação de 15 metros de distância para utilização e taxa de transferência de 20 kbps.

Dantas (2010, p. 101), define assim a interface RS232:

> "A versão mais popular do padrão RS-232 é a revisão C. No final dos anos oitenta, a revisão D foi proposta e no início os anos noventa foi apresentada a revisão E. As três versões tem um núcleo comum de funções e operações que nos levam a denominação da interface de RS-232. O Padrão RS-232 como um todo engloba as áreas das características mecânicas da interface, os sinais elétricos através da interface, a função de cada sinal e um subconjunto de sinais para determinadas aplicações".

3.3. PROTOCOLO TCP/IP

O protocolo TCP/IP é formado por quatro camadas e apresenta uma solução prática ao modelo OSI, que nunca chegou a ser implementado. As camadas que formam o TCP/IP são: rede, internet, transporte e aplicação (KUROSE; ROSS, 2010).

O protocolo TCP/IP surgiu no final dos anos sessenta, devido ao interesse das agências governamentais americanas de criar uma arquitetura de protocolo que pudesse interoperar computadores diversos com ambientes diferentes de hardware e software, sendo concluída entre os anos de 1977 e 1979, sendo denominada TCP/IP.

Dantas (2010, p. 153), define assim o protocolo TCP/IP:

> “Com certeza o modelo de referência mais conhecido (e um dos mais antigos) é o modelo de referência TCP/IP. Ele surgiu da rede ARPANET, que foi uma rede de pesquisa criada pelo Departamento de Defesa do governo americano visando a conexão de inúmeras redes. Como cada rede tinha a sua conexão e a ARPANET se conectava através de diferentes tipos de enlaces (exemplos: enlaces de rádio e satélites), vários problemas começaram a surgir e a necessidade de um modelo ficou patente. O modelo de referência concebido foi o modelo TCP/IP”.

Conforme Dantas (2010, p. 153), o modelo TCP/IP foi projetado em quatro camadas: rede, inter-rede, transporte e aplicação.

A primeira camada é a camada de rede, que cuidará das funções de acesso físico e lógico ao meio físico.

A camada de inter-rede, é a responsável por envio dos datagramas de um computador para outro. O protocolo IP (*Internet Protocol*) da arquitetura TCP/IP, é um protocolo desta camada.

A camada de transporte tem a função de garantir uma conexão fim a fim com a qualidade solicitada na camada de aplicação, independente dos serviços oferecidos pelas camadas anteriores à ela.

Na camada de aplicação, estão os protocolos que dão suporte às aplicações dos usuários como transferência de dados, acesso remoto, correio eletrônico, gerenciamento de redes entre outros.

3.4. PROTOCOLO ETHERNET

Ethernet é uma tecnologia de comunicação em rede local com meio de transmissão compartilhado, padronizado como padrão IEEE 802.3 (TANENBAUM, 2003).

Essa tecnologia permite taxas de transmissão que podem chegar a 10 Gbp sendo amplamente utilizada em empresas e, mais recentemente, nas residências. Os padrões mais conhecidos e utilizados hoje são 10BaseT, com velocidade de até 10 Mbps, 100BaseTX, com velocidade de até 100 Mbps e 1000BaseT, com velocidade de até 1000 Mbps. Vários protocolos da AR (Automação Residencial)

utilizam Ethernet como meio de transporte. Algumas empresas desenvolvem adaptadores pensando na interoperabilidade com o padrão Ethernet, pois isso facilita a aceitação desses produtos no mercado (BOLZANI, 2004).

3.5. PROTOCOLO IEEE 802.11

Foi criada nos anos 90 e é conhecida popularmente como Wi-Fi. A evolução no desenvolvimento da tecnologia permitiu um aumento na taxa de transferência, passando a ser vista como promissora e a receber maior atenção de empresas como IBM, CISCO e 3COM (BOLZANI, 2004).

Os padrões para 802.11 (802.11ª, 802.11b e 802.11g) utilizam um protocolo de acesso ao meio conhecido como CSMA/CA (c*arrier sense multiple access with collision avoidance*), e usam a mesma estrutura de quadros - camada de enlace - e podem funcionar em modo infraestrutura (utiliza pontos de acesso - APs) ou ad hoc, pois não utiliza pontos de acesso (KUROSE; ROSS, 2006).

Existe ainda o padrão 802.11n que opera em outra faixa de frequência que pode dar novos rumos à comunicação sem fio.

Além dos protocolos mencionados, que serão utilizados no estudo de caso, existem outros protocolos de automação conforme menciona Muratori e Dal Bó (2014):

- Protocolos de automação *Power Line* (utilizam a própria rede elétrica): X10, UPB (*Universal Powerline Bus*) e HomePlug;
- Protocolos de Automação sem fio: ZigBee, Z-Wave e UHF (*Ultra–High Frequency*) e;
- Protocolos de automação híbridos: CEBus (*Consumer Electronics Bus*), Insteon, LonWorks e KNX.

4. MICROCONTROLADORES

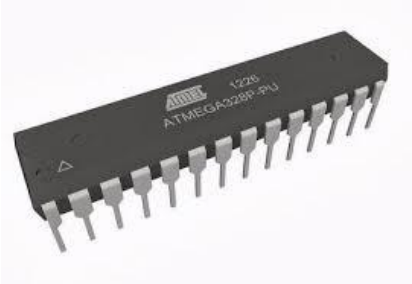
Em toda automação, há um controle feito por um microcontrolador e nos atentaremos principalmente ao Atmel, que será o microcontrolador utilizado no estudo de caso. Há outras opções de microcontroladores para automação residencial como o CLP e o PIC.

Segundo Souza (2005, p. 21) “... poderíamos definir o microcontrolador como um “pequeno” componente eletrônico, dotado de uma “inteligência” programável, utilizado no controle de processos lógicos”. Um microcontrolador é um sistema computacional pequeno contendo um processador, uma memória primária e uma memória de armazenamento. Em contrapartida aos microprocessadores atuais, o microcontrolador é um sistema de propósito específico, escolhido exatamente para determinada tarefa, de forma oposta aos microprocessadores, que são fabricados com base em maximizar a capacidade de processamento.

4.1. MICROCONTROLADOR ATMEL

Conforme a Atmel (2016), os microcontroladores (MCUs) Atmel® oferecem baixo consumo de energia, conectividade de alta velocidade, largura de banda de dados ideal e suporte avançado para interfaces, além de suporte para integração contínua de tecnologia de toque capacitivo e para a implantação de botões.

Figura 2 : Microcontrolador Atmel



Fonte: Vinitrônica[2]

O microcontrolador Atmel será utilizado juntamente com a placa de prototipagem Arduino.

Soares K. (2013), define esta placa da seguinte forma:

> "O Arduino trata-se de uma placa fabricada na Itália utilizada como plataforma de prototipagem eletrônica que torna a robótica mais acessível a todos. Projeto italiano iniciado em 2005 tinha primeiramente cunho educacional e interagia com aplicações escolares".

O desenvolvimento desta placa *open source* (arquitetura aberta, qualquer um pode montar sua placa), vendeu mais de 50 mil cópias, rendendo um documentário em 2010.

Soares K.(2013), acrescenta:

> "As unidades são constituídas por controladora Atmel AVR de 8 bits, pinos digitais e analógicos de entrada e saída, entrada USB – o que permite conexão com computadores – ou serial e possui código aberto, que quando modificado, dá origem a outros derivados "ino" – que por questões comerciais – levam nomes como Netduino, Produino e Garagino. A placa Arduino não possui recursos de rede, mas pode ser combinada com outros Arduinos criando extensões chamadas de *Shields"*.

Figura 3 : Arduino UNO

[2] Disponível em: < http://www.vinitronica.com.br/pd-25ab15-microcontrolador-atmel-atmega328p-pu.html> . Acessado em: 05 abr. 2017

Fonte: Deviante[3]

Banzi (2014, p. 1) descreve o Arduino:

> “Trata-se de hardware e software de fonte aberta, se desejar, você pode baixar o esquema do circuito, comprar todos os componentes, e fazer o seu próprio, sem pagar nada para os fabricantes de Arduino”.

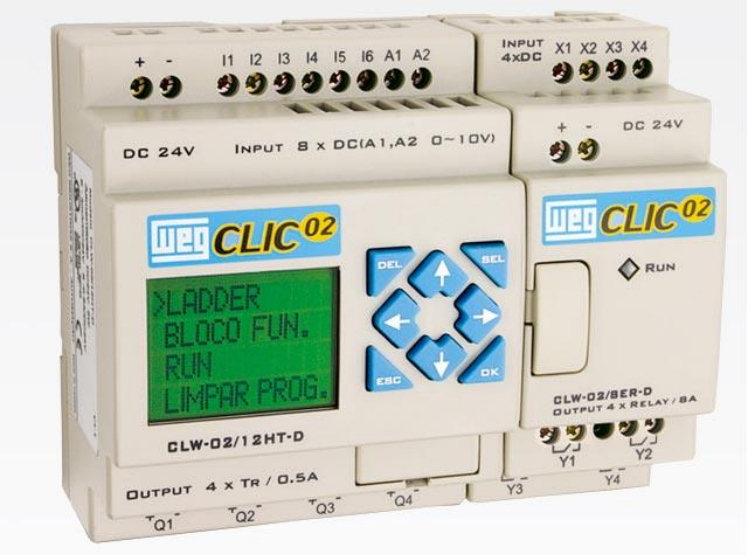
4.2. CLP (CONTROLADOR LÓGICO PROGRAMÁVEL)

O CLP é mais comumente utilizado em automação industrial, porém, vem popularizando-se na automação residencial. É mais utilizado em projetos de grande porte mas ainda possui um alto custo.

Conforme Silva Filho (2004), desenvolvido para atender as necessidade da indústria automobilística, tornou-se muito utilizado em sistemas de automação flexíveis. Permitem desenvolver facilmente a lógica para saídas em função das entradas, permitindo utilizar inúmeros pontos de entrada de sinal para controlar pontos de saída.

[3] Disponível em: <http://www.deviante.com.br/noticias/tecnologia/arduino-como-desenvolver-automacoes-sem-conhecimento-previo-de-eletronica/>. Acessado em: 18 abr. 2017

Figura 4 : CLP WEG CLIC02



Fonte: ERG[4]

4.3. MICROCONTROLADOR PIC

O PIC pertence à classe de microcontroladores de arquitetura Harvard, possui memória RAM, memória EEPROM, memória de programa, controladores de E/S em uma CPU de conjunto reduzido de instruções em um único chip. Pode ser programado para diversas tarefas, é simples, tem disponibilidade e baixo custo.

Figura 5 : Microcontrolador PIC

Fonte: Display Max[5]

[4]Disponível em: http://www.ergmotoreseletricos.com.br/produtos-weg/drives/clps-weg/clp-linha-clic02.php. Acessado em: 05 abr. 2017

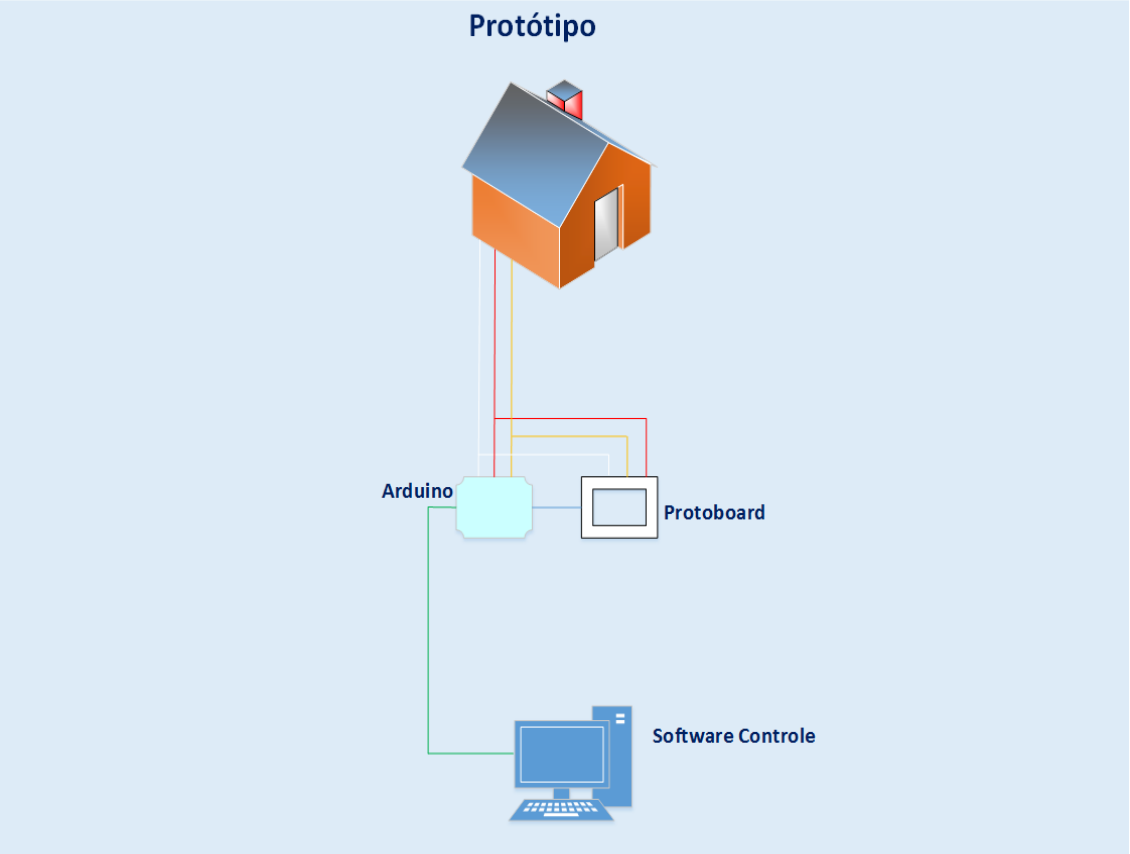
[5] Disponível em: http://www.displaymax.net.br/produto/91496/microcontrolador-pic16f628a-ip. Acessado em: 05 abr. 2017

5. ESTUDO DE CASO

5.1. PROTÓTIPO – MAQUETE

A finalidade da maquete é ter um protótipo para laboratório de testes, servindo como base de conhecimento para a implementação em ambiente real e apresentar alguns recursos e benefícios oferecidos pela automação residencial. Abaixo, segue o esquema de funcionamento do protótipo, integrando o aplicativo de controle, o Arduino e a maquete.

Figura 6 : Protótipo – Visão geral



Fonte: elaborada pelo autor

A maquete servirá como modelo de residência para aplicar recursos de domótica e controlar funcionalidades como acender/apagar luzes, acionar alarme, etc. Abaixo, segue a maquete da residência:

Figura 7 : Protótipo - Maquete

Fonte: elaborada pelo autor

O protótipo preocupa-se apenas em apresentar os recursos da automação residencial, pode-se afirmar então, que este é um ambiente automatizado não seguro.

Lyra (2008, p. 4), diz o seguinte sobre segurança da informação:

> "Quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente."

A automação não prevê nenhuma restrição quanto aos usuários que a acessam, assim há perda do controle de confidencialidade sobre a mesma.

Um ambiente não seguro, viola um dos princípios do tripé da segurança da informação conhecido como CID (Confidencialidade, Integridade e Disponibilidade).

Lyra (2008), os define assim:

- Confidencialidade: somente usuários autorizados acessam as informações;

- Integridade: informação deve ser correta, verdadeira e não estar corrompida;
- Disponibilidade: a informação deve estar disponível para quem precise utilizá-la.

Não menos importantes que o tripé CID (Confidencialidade, Integridade e Disponibilidade) citados acima, há outros aspectos de grande relevância que devem ser considerados também. Quando a automação não é capaz de garantir que um usuário é de fato quem alega ser, ela viola o aspecto da autenticação. Se a mesma não tem a capacidade de provar que determinado usuário executou determinada ação na automação, ela viola o aspecto de não-repúdio. Quando não tem a capacidade de manter anônima uma ação em relação à quem a executou, viola o aspecto da privacidade. Um sistema de automação que não tenha um controle de logs para auditar tudo o que foi feito pelo usuário, não contempla o aspecto auditoria.

O mesmo autor (2008, p. 4), define assim estes outros aspectos da segurança da informação:

- Autenticação: garantir que o usuário é quem realmente alegar ser;
- Não-repúdio: capacidade provar que um determinado usuário executou determinada operação;
- Legalidade: estar em conformidade com as leis vigentes;
- Privacidade: manter anônimo um usuário em relação às suas ações;
- Auditoria: capacidade de poder auditar tudo o que foi feito, permitindo identificar possíveis fraudes ou tentativas de ataque.

Apesar da automação não estar exposta para acesso externo (acesso remoto), o protótipo não prevê nada que identifique uma violação de segurança. Uma violação de segurança, denomina-se ataque, e Lyra (2008, p. 5) a define assim: “Um tipo de incidente de segurança caracterizado pela existência de um agente que busca obter algum tipo de retorno, atingindo algum ativo de valor”.

É muito importante também que a automação proteja os ativos de valor da residência. Como ativos de valor, podemos entender não somente os bens materiais

de valor, mas também ativos computacionais de valor como arquivos de mídias digitais que tenham relevante importância para o proprietário.

Lyra (2008, p. 5), define assim ativo de informação:

> "A informação é um bem de grande valor para os processos de negócios da organização, mas também devemos considerar a tecnologia, o meio que a suporta, que a mantém e que permite que ela exista, as pessoas que a manipulam e o ambiente onde ela está inserida. Assim podemos descrever que ativo da informação é composto pela informação e tudo aquilo que a suporta ou se utiliza dela".

O protótipo viola também outro aspecto de segurança da informação que é a vulnerabilidade, ou seja, não tem nada previsto que proteja os pontos fracos da automação, tornando-a vulnerável a um ataque. Ainda Lyra (2008, p. 6), diz o seguinte sobre vulnerabilidade:

> "Os ativos de informação possuem vulnerabilidades ou fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade, a quebra de confidencialidade ou integridade. A vulnerabilidade de um ativo é o seu ponto fraco. Essas vulnerabilidades poderão ser exploradas ou não, sendo possível que um ativo da informação apresente um ponto fraco que nunca será efetivamente explorado"

5.1.1. COMPOSIÇÃO E FUNCIONAMENTO DO PROTÓTIPO

O protótipo é composto pela maquete, um painel de controle e um software gerenciador.

O painel de controle é o responsável por todo o controle lógico da automação e acionamento manual pelos interruptores sendo composto por placas Arduino, *protoboard*, relês e interruptores. O painel completo pode ser visualizado na imagem abaixo:

Figura 8 : Painel de Controle

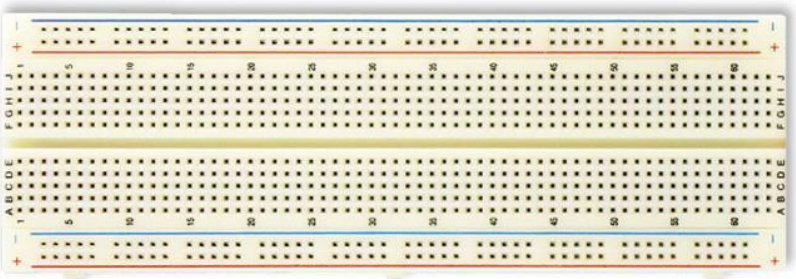
Fonte: elaborada pelo autor

5.1.2. PROTOBOARD

A *protoboard* é uma matriz de contatos para experimentos de projetos e foi assim definida por Soares, J.C.(2015):

> "*Protoboard* é um dos equipamentos mais úteis no aprendizado do técnico em eletrônica. Consiste em uma placa didática composta de uma matriz de contatos que permite a construção de circuitos experimentais sem a necessidade de efetuar a soldagem dos componentes, isso permite que seja efetuada uma série de experimentos com os mesmos componentes inserindo ou removendo os mesmos com rapidez, agilidade e segurança".

Figura 9 : Protoboard



Fonte: Eletronite[6]

[6] Disponível em: http://www.eletronite.com.br/aprenda/protoboard-agilidade-e-praticidade.html. Acessado em: 23 abr. 2017

A maior vantagem da *protoboard* é a possibilidade de retirar os componentes para serem utilizados novamente em novos projetos.

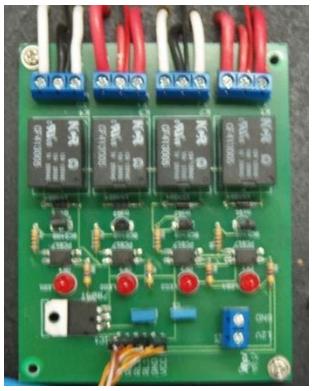
5.1.3. RELÊ

Outro componente presente no painel de controle é o relê, é através dele que é possível acionar os equipamentos da automação.

Cunha (2009), define relê da seguinte forma:

> "O relê é um dispositivo destinado a produzir modificações súbitas e predeterminadas em um ou mais circuitos elétricos de saída, quando alcançadas determinadas condições no circuito de entrada, que controla o dispositivo. Assim, o relê não possui a função de interromper o circuito principal, mas sim de fazer atuar o seu sistema de manobra".

Figura 10 : Relês



Fonte: elaborado pelo autor

Silva (2009), ainda diz sobre o relê:

> "Esse equipamento, quando ligado à uma instalação, tem como função principal permitir o funcionamento de outros aparelhos conectados ao mesmo ou em outro circuito elétrico que estejam ligados ao relê, devido a uma alteração nas condições do equipamento pela passagem de corrente elétrica".

5.1.4. PROGRAMACÃO DO MICROCONTROLADOR

A programação do microcontrolador Atmel na plataforma Arduino foi desenvolvida na linguagem C (com certas particularidades referentes ao microcontrolador), utilizando a interface de desenvolvimento disponível junto com o Arduino.

A gravação do software desenvolvido para o microcontrolador dá-se por meio de conexão com cabo serial, sendo possível fazer uma interação entre o software desenvolvido e o microcontrolador, enviando e recebendo informações de comandos e respostas. A IDE (*Integrated Development Environment* - Ambiente de Desenvolvimento Integrado) do microcontrolador pode ser vista abaixo com comandos para acender/apagar uma lâmpada.

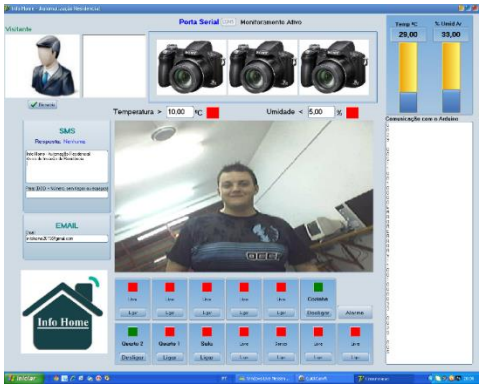
Figura 11 : Programação do Arduino

Fonte: elaborado pelo autor

5.1.5. SOFTWARE DE GERENCIAMENTO

O software de gerenciamento da automação foi desenvolvido com a linguagem de programação Object Pascal e IDE (*Integrated Development Environment* - Ambiente de Desenvolvimento Integrado) Delphi 7.0 com interface final conforme figura abaixo:

Figura 12 : Software de Controle



Fonte: elaborado pelo autor

5.1.6. COMUNICAÇÃO SERIAL

A comunicação é serial entre o software de gerenciamento e o microcontrolador. Simultaneamente, o software de gerenciamento pode enviar comandos para o microcontrolador como pode também receber informações dele. O layout do protocolo é uma cadeia de caracteres pré-definida no desenvolvimento do software de gerenciamento e no software do microcontrolador, para que uma comunicação se estabeleça entre ambos e seja compreendida. Na figura abaixo, exemplo das informações recebidas do microcontrolador:

Figura 13 : Comunicação Serial

Fonte: elaborado pelo autor

5.2. AMBIENTE REAL – AMBIENTE SEGURO COM MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

A proposta é implementar mecanismos de Segurança da Informação não existentes no protótipo em um ambiente real automatizado e disponível para acesso e controle na *web*.

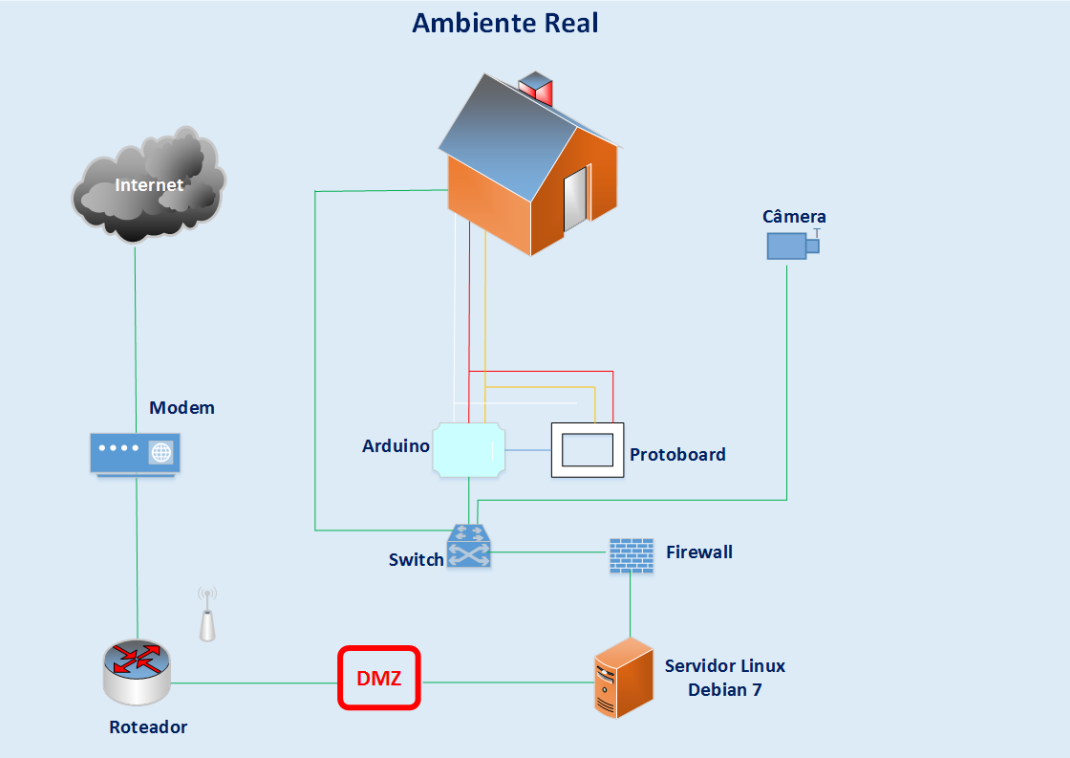
Partindo do fato que a automação agora está exposta para o mundo, os critérios de segurança devem garantir que a automação seja utilizada apenas por pessoas autorizadas, portanto, deverão ser implementados mecanismos de Segurança da Informação no *site*, na estrutura da rede, no banco de dados, criar

logs de acessos, criar logs de monitoramento de acessos, implementar *firewall*, entre outros. Vale salientar porém, que será dada atenção especial à implementação do *firewall*, portanto o mesmo será o objeto principal do estudo de caso da automação em ambiente real

O projeto contempla o acesso remoto a um *website* que estará hospedado em um servidor Linux Debian 7, na própria residência a ser automatizada, O acesso ao site, ocorrerá através da solicitação de *login* e senha de usuário, portando só pessoas autorizadas terão acesso à automação.

A nova estrutura terá as características apresentadas na visão geral do projeto logo abaixo:

Figura 14 : Ambiente Real - Visão Geral



Fonte: elaborado pelo autor

5.2.1. FIXANDO O IP PARA ACESSO EXTERNO

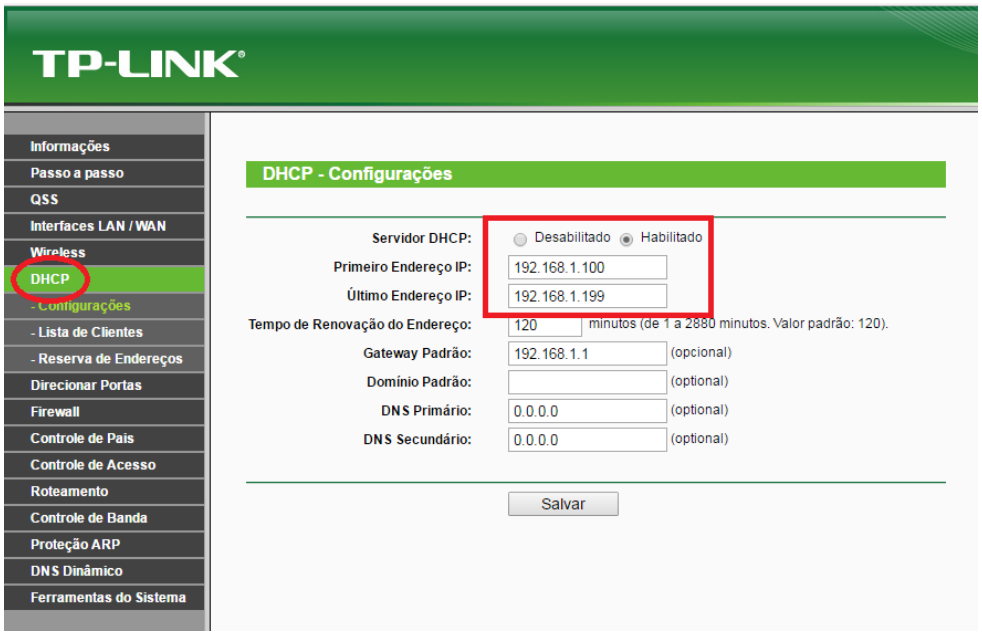
Para que seja possível o acesso externo ao roteador da automação, foi criado um DNS (*Domain Name System* – Sistema de Nomes de Domínios) com

software NO-IP e redirecionamento da conexão HTTP (*Hypertext Transfer Protocol* - Protocolo de Transferência de Hipertexto) para a porta 8081, permitindo que a automação tenha um IP (*Internet Protocol* – é um número que identifica um dispositivo) fixo resolvido pelo DNS.

5.2.2. CONFIGURAÇÕES DO ROTEADOR

O roteador foi configurado para ter uma faixa de IPs exclusiva para a rede *wireless* (do IP 192.168.1.100 ao IP 192.168.1.199), atribuindo IPs por DHCP (*Dynamic Host Configuration Protocol* - Protocolo de Configuração Dinâmica de Host) aos *hosts* conectados na mesma. Desta forma, fica garantido que os acessos à rede *wireless* permitam apenas o acesso à internet, ou seja, os *hosts* nela conectados apenas utilizam a internet porém não tem acesso à rede interna (cabeada), que possui IPs fixos (configurados no servidor Linux Debian 7) atrelados ao MAC-ADDRESS dos hosts pertencentes à ela.

Figura 15 : Roteador - DHCP Rede Wireless

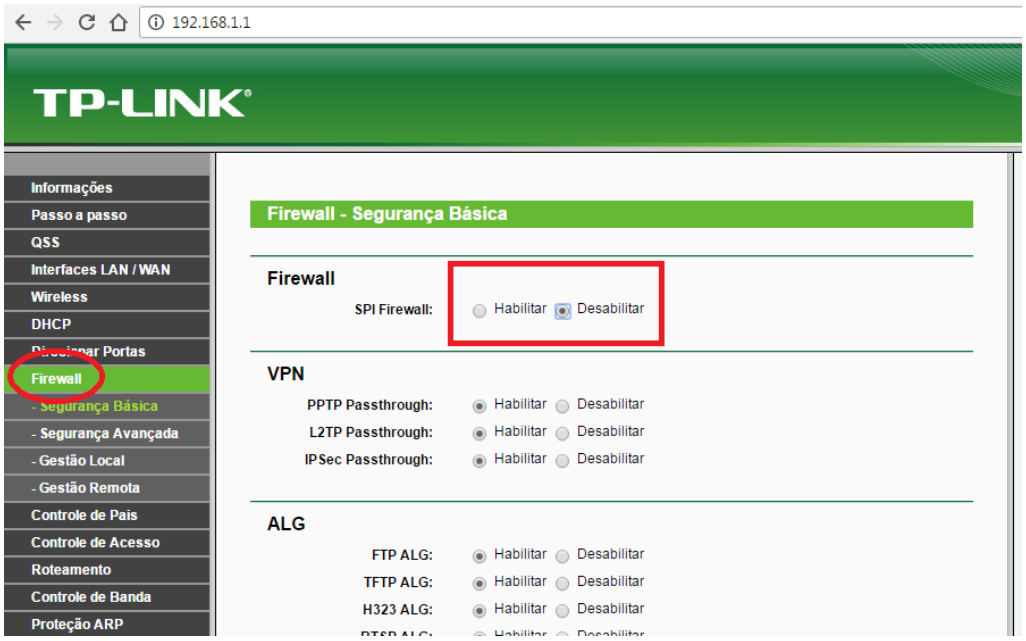


Fonte: elaborado pelo autor

Outra configuração realizada no roteador foi a criação de uma DMZ (*demilitarized zone* – zona desmilitarizada), para permitir que uma requisição externa na porta 8081, redirecione a solicitação para o IP do servidor Linux Debian 7. Para

que fosse possível a configuração da DMZ, foi desabilitado o *firewall* do roteador, sendo criado posteriormente, um *firewall* no Linux.

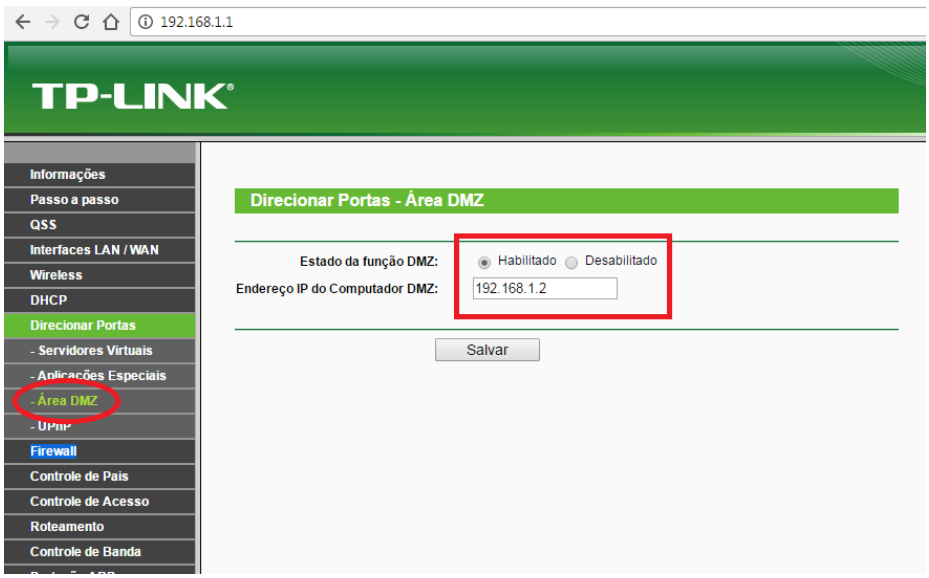
Figura 16 : Roteador - *Firewall*



Fonte: elaborado pelo autor

A configuração de DMZ, faz com que todas as solicitações externas sejam redirecionas para o IP 192.168.1.2, que é o IP da placa de entrada de rede do servidor Linux. Vide exemplo logo abaixo:

Figura 17 : Roteador – DMZ

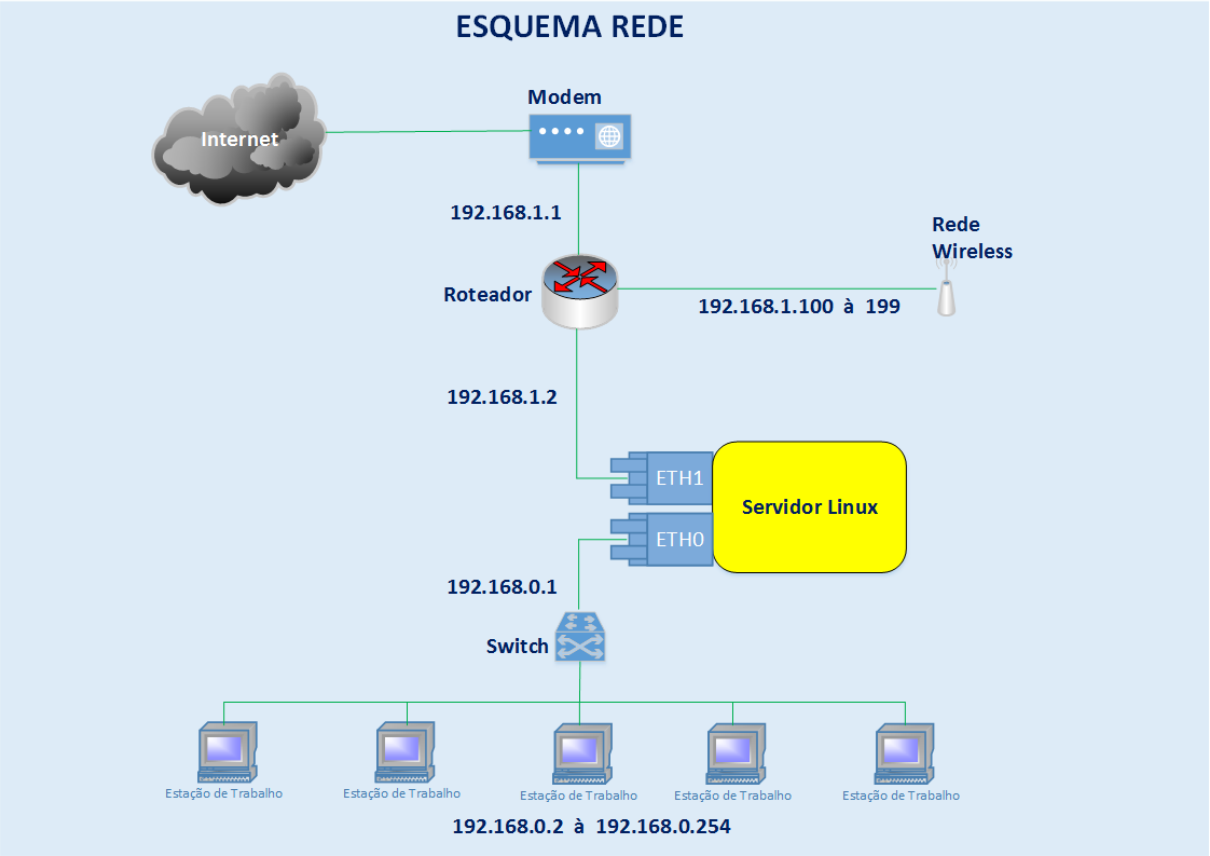


Fonte: elaborado pelo autor

5.2.3. CONFIGURAÇÕES DA REDE NO LINUX

A rede interna da automação, foi configurada no servidor Linux em uma faixa diferente da rede *wireless* configurada no roteador. Haverá então, duas faixas de redes distintas, uma para acesso wireless e outra para a rede cabeada. Abaixo, segue o esquema das redes e seus IPs:

Figura 18 : Esquema Rede

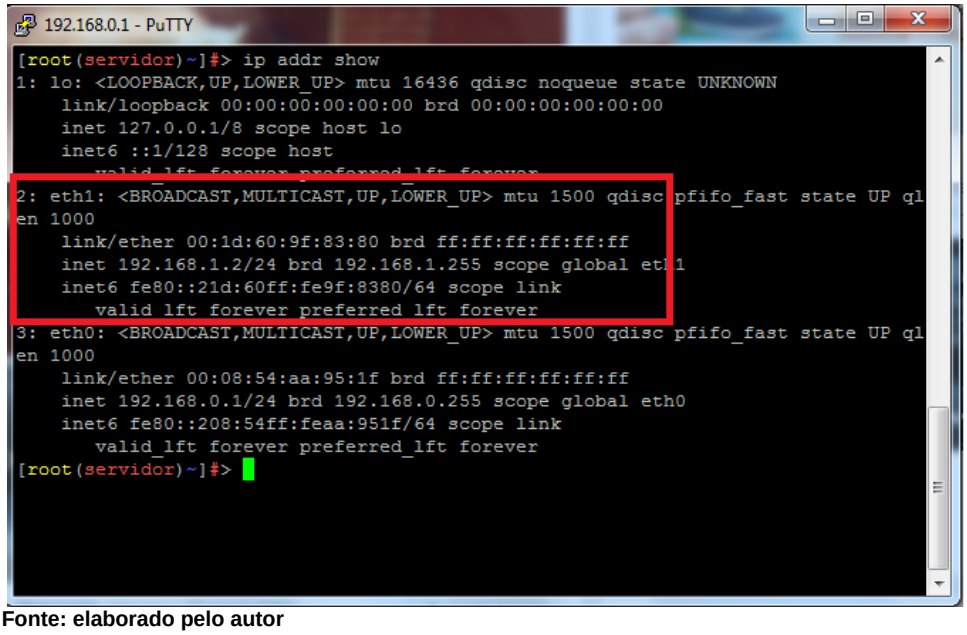


Fonte: elaborado pelo autor

Como o servidor Linux possui duas placas de rede, elas ficaram configuradas da seguinte maneira:

- Placa de rede ETH1 – IP 192.168.1.2: esta é a placa de rede de entrada da Internet, ela foi configurada com o primeiro IP disponível desta faixa do roteador para não conflitar com a faixa de IPs de 192.168.1.100 à 192.168.1.199 atribuídos por DHCP pelo roteador à rede *wireless*.

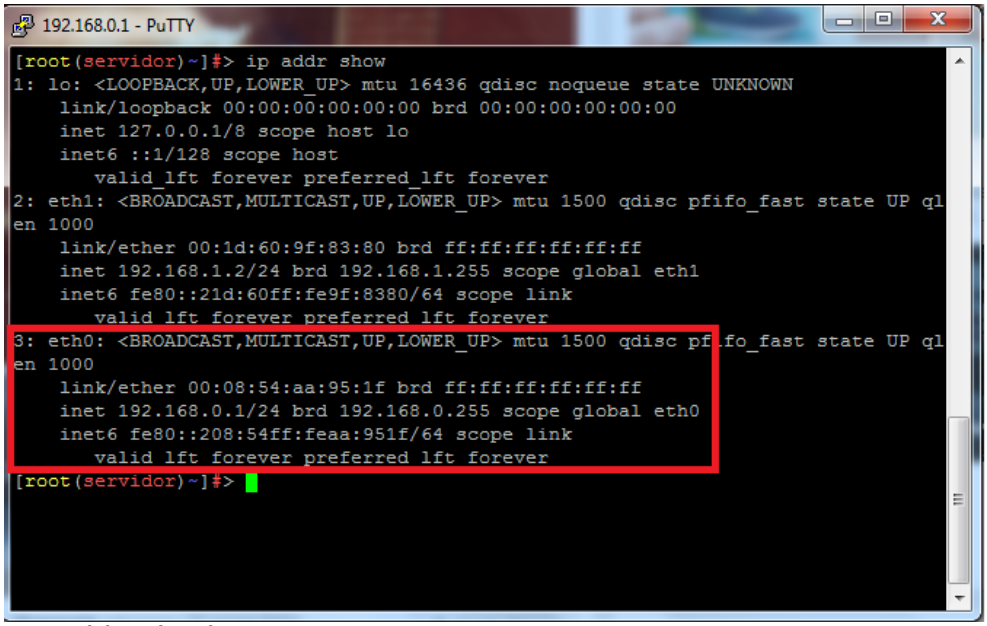
Figura 19 : Interface ETH1 - IP 192.168.1.2 (entrada internet)



Fonte: elaborado pelo autor

- Placa de rede ETH0 – IP 192.168.0.1 - a segunda placa de rede (saída internet) será utilizada para a rede interna e consequentemente, para a automação residencial.

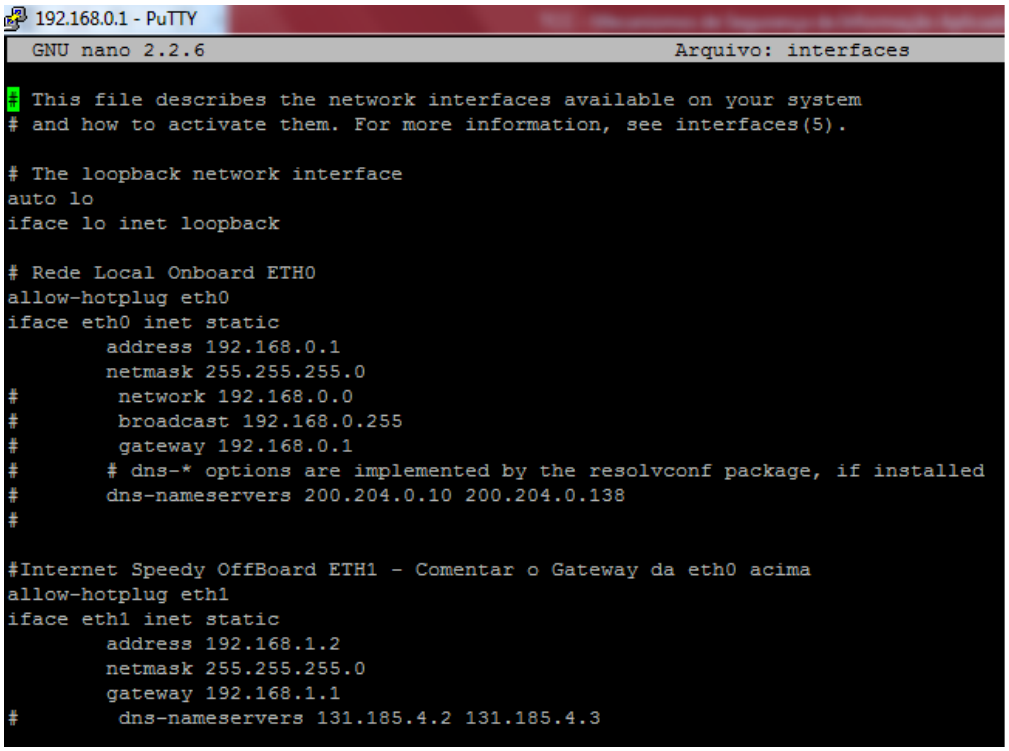
Figura 20 : Interface ETH0 - IP 192.168.0.1 (saída internet)



Fonte: elaborado pelo autor

A configuração das placas foi realizada no arquivo **interfaces,** localizado na pasta **/etc/network** com o editor **nano**, conforme imagem abaixo:

Figura 21 : Configuração Interfaces ETH0 e ETH1

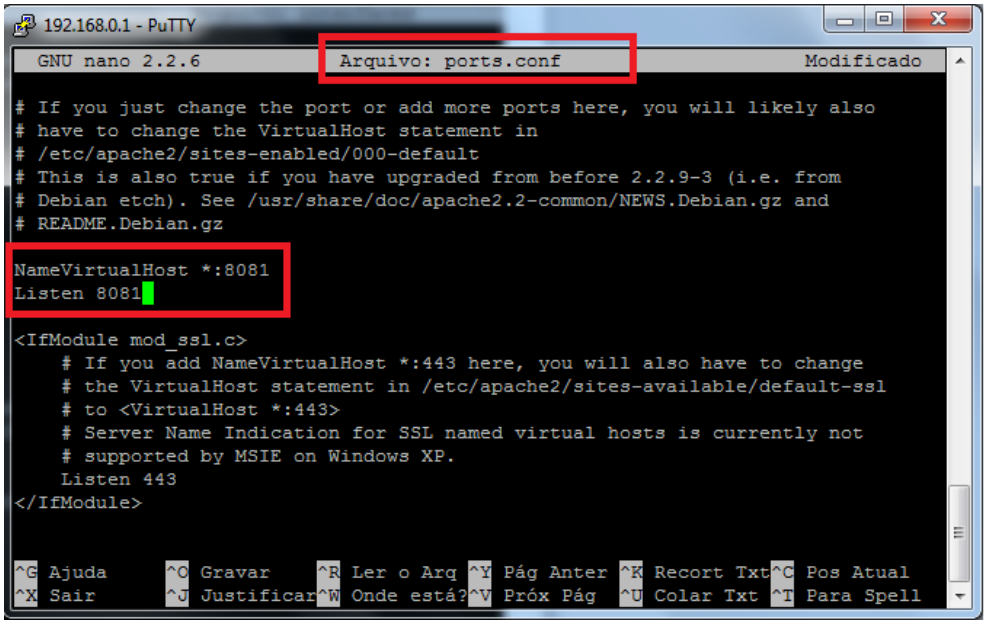


Fonte: elaborado pelo autor

5.2.4. CONFIGURAÇÕES DO SERVIDOR APACHE

O servidor *web* Apache é o responsável por hospedar o site de gerenciamento da automação. Por padrão, todo acesso ao *website*, dá-se por meio de uma requisição HTTP na porta 80 e, com o intuito de dificultar o acesso (para pessoas não autorizadas) à essa porta, o Apache foi configurado na porta 8081. Para realizar esta mudança, foi editado o arquivo **ports.conf** na pasta **etc/apache2** com o editor de texto nano conforme imagem a seguir:

Figura 22 : Configuração da porta do Apache



Fonte : elaborado pelo autor

5.2.5. CUIDADOS COM O WEBSITE E BANCO DE DADOS

No que diz respeito ao *website*, o mesmo possui um cadastro de usuários com *login* e senha. Algumas regras foram definidas para o controle de usuário e senha, tais como:

- Tamanho da senha: a senha deverá conter no mínimo oito caracteres;
- Toca de senha: a senha deverá ser trocada a cada quatro meses;
- Bloqueio de usuário: o usuário será bloqueado após três tentativas fracassadas de acesso;
- Caracteres obrigatórios: a senha deve conter obrigatoriamente uma letra maiúscula, uma letra minúscula, um número e um caractere especial;

Outros controles além dos citados acima, foram implementados também com o intuito de garantir a segurança do ambiente e do acesso ao banco de dados. São eles:

- Nomes diferentes para cookies de sessão: IDs dificultam a ação de crackers que queiram se aproveitar da aplicação;
- Acesso a cookies: ativando no PHP, a opção *session.cookie_httponly*, os cookies de seção só poderão ser acessados via HTTP, evitando assim, que scripts Javascript sejam barrados ao tentar fazer o mesmo. Isso evita ataques do tipo XSS (*Cross-Site Scripting*);
- Tempo de vida para as sessões: foi atribuído um tempo de vida para a sessão de 10 minutos;
- Variável que contém senha: nenhuma variável que contenha o valor de uma senha usa texto puro, sempre há a criptografia antes o armazenamento;
- SQL Injection: evitar falhas de acesso na base de dados através de comandos SQL injetados no *login* e/ou senha do usuário.

5.2.6. FIREWALL

O *firewall* será o ponto principal a ser considerado, dentro dos mecanismos de segurança implementados no projeto. Foi utilizado o *firewall* do Linux, que é baseado no iptables, que nada mais é que um conjunto de regras e também o *firewall* de *proxy* baseado no Squid.

O *firewall* é um dos principais componentes de segurança, além de ser o mais conhecido e antigo. A tradução literal de *firewall* significa “barreira de fogo”, fazendo uma analogia à uma barreira de proteção. Uma outra analogia comum em relação ao *firewall*, é compará-lo à um edifício, onde o porteiro “filtra” a entrada das pessoas, permitindo ou não a entrada da mesma e garantindo certa segurança ao edifício. A principal finalidade do *firewall* é impedir que os usuários da internet acessem dados das intranets, limitando o caminho das informações, como as permissões de cada um. Os bloqueios das portas de acesso, funcionam como uma barreira de proteção entre duas redes, permitindo ou não o acesso aos dados.

CISCO (2017), define assim o *firewall*:

> “Um *firewall* é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Os *firewalls* tem sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a internet. Um *firewall* pode ser hardware, software ou ambos”.

No projeto de automação, o *firewall* poderia ter sido implementado de duas formas: no próprio roteador ou no Linux. Foi implementado no Linux por ser mais seguro e porque no roteador, o *firewall* teve que ser desabilitado para poder habilitar a DMZ. Uma terceira forma, poderia ser um firewall por hardware, porém com alto custo.

O projeto será baseado nos *firewalls* de filtro de pacotes e *proxy*;

- Filtro de pacotes (IPTABLES): o módulo do IPTABLES é um conjunto de regras de filtros que são acessados no framework *netfilter* dentro do KERNEL Linux. Thomaz (2005), define assim o IPTABLES: “O IPTABLES é uma ferramenta de edição da tabela de filtragem de pacotes, ou seja, com ele você é capaz de analisar o cabeçalho (*header*) e tomar decisões sobre os destinos destes pacotes”.

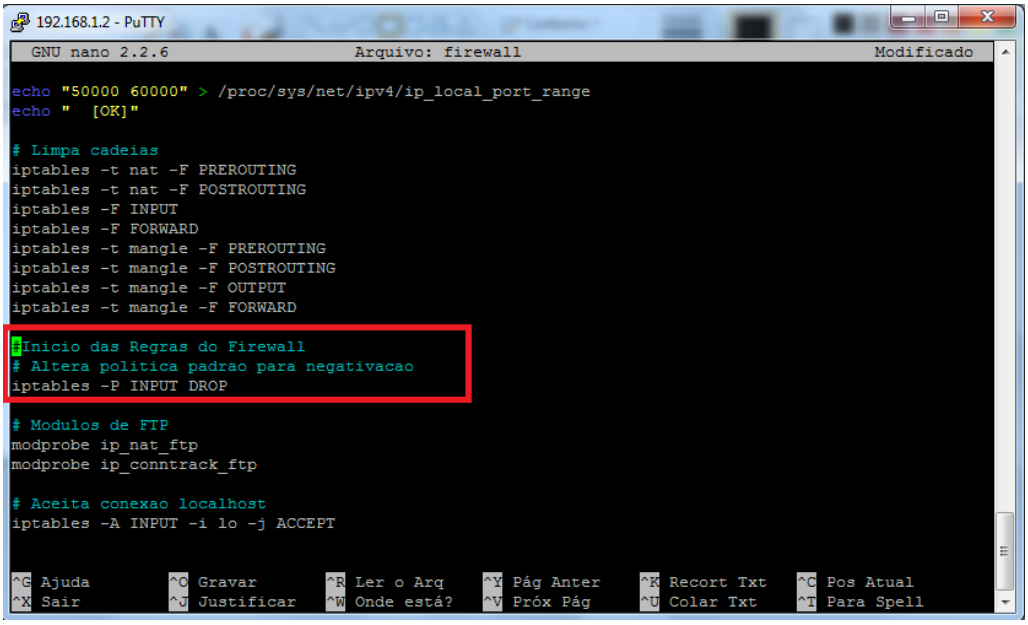
  O IPTABLES é um *firewall* com estado, que é denominado *firewall stateful* e é assim descrito por Thomaz (2005):

  > “O tipo de filtragem *stateful* (IPTABLES) cria um poderoso sistema de *firewall* que “se lembra” das conexões, evitando ataques do tipo *Stealth Scans*, que trazem *flags* especiais para técnicas de *port scanning*, como o uso da *flag* ACK para enganar tais *firewalls*”.

Há também o *firewall* do tipo *statless* (sem estado), mais simples de implementar por tratar cada pacote roteado pelo *firewall*, como individuais. Pode ser utilizado onde há regras de nível de rede simples, possibilitando um melhor desempenho.

O *firewall* é composto por diversas regras, algumas para liberar acessos às portas, outras para negar o acesso às mesmas. Na imagem abaixo, há uma regra inicial para bloquear tudo, e nas regras que seguem posteriormente, há a configuração do que é necessário liberar.

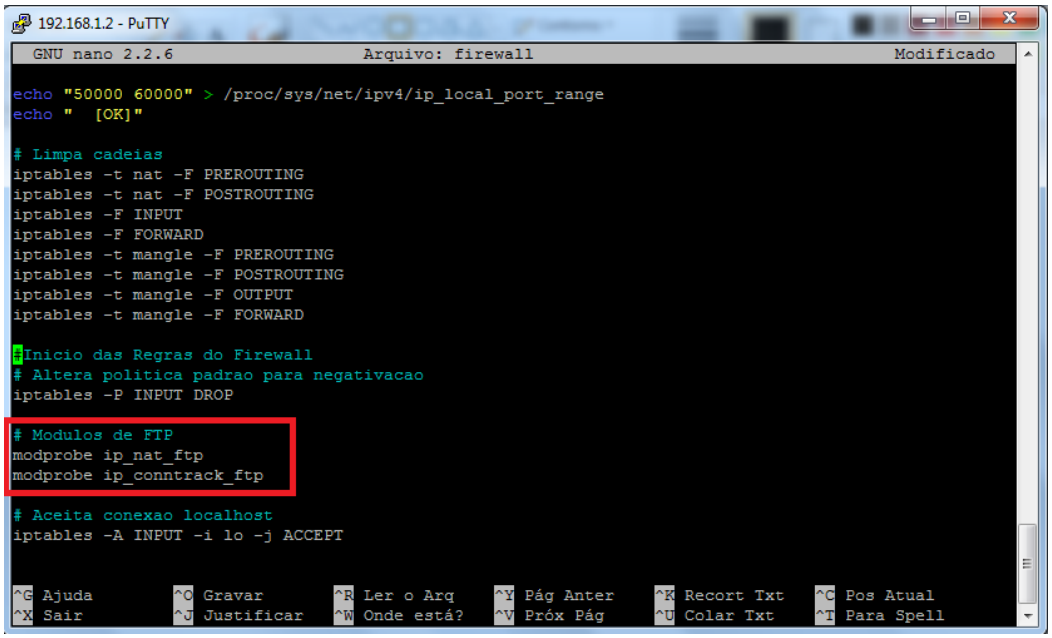
Figura 23 : *Firewall* regra de bloqueio geral



Fonte: elaborado pelo autor

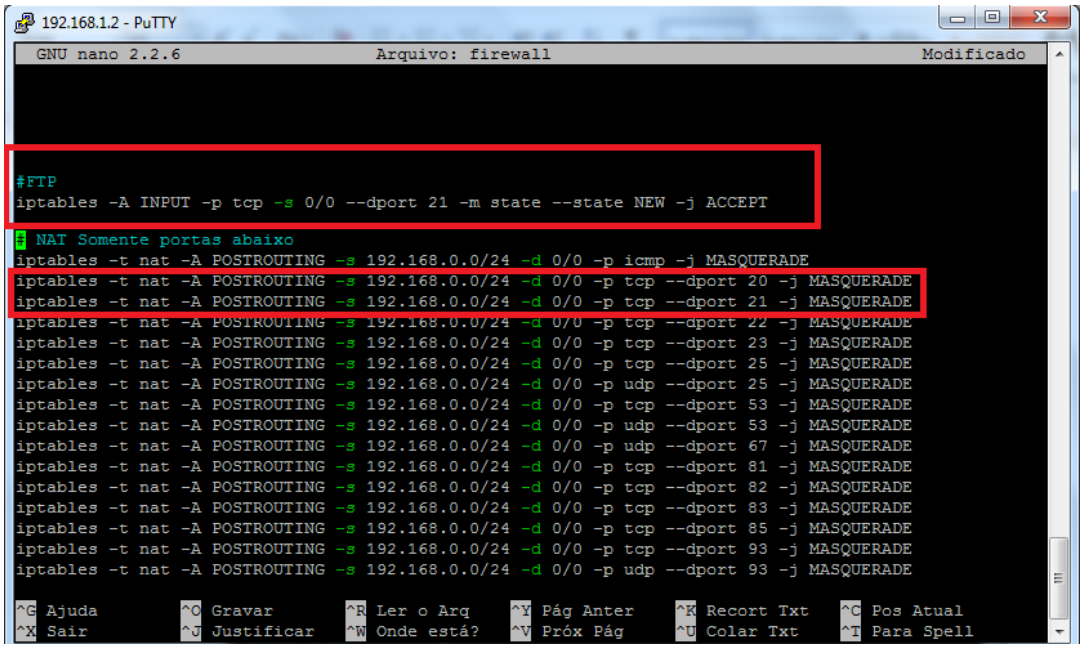
Toda vez que se faz necessário “subir” algum arquivo atualizado para o site da automação, é necessário utilizar o FTP para tal tarefa. A seguir, a configuração no *firewall* mostra as imagens de como são carregados os módulos do FTP e como dá-se permissão de acesso nas portas 20 e 21, utilizadas pelo FTP, respectivamente:

Figura 24 : *Firewall* - Carregando módulos do FTP



Fonte: elaborado pelo autor

Figura 25 : *Firewall* - Liberando portas 20 e 21 do FTP

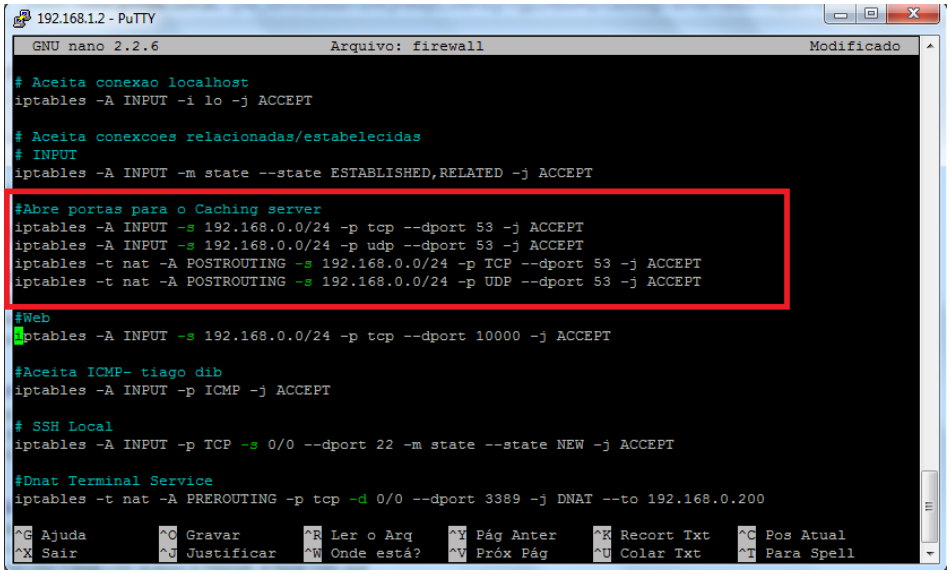


Fonte: elaborado pelo autor

O servidor Linux contempla um *Server Caching* (pode ser utilizado por *proxy* ou DNS e, no caso do projeto é o *proxy* SQUID), cuja finalidade é manter um arquivo das últimas solicitações ao site, assim toda vez que o usuário solicitar uma requisição ao mesmo, haverá uma cópia que tornará o acesso mais rápido. No

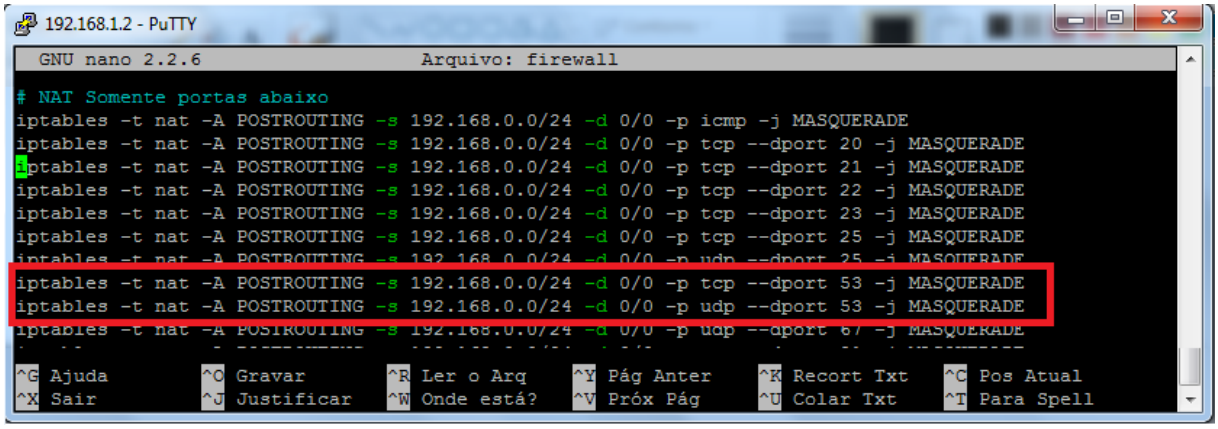
firewall, são configuradas regras pra liberação da porta 53 (TCP e UDP), conforme imagens abaixo:

Figura 26 : *Firewall* - *Server Caching* porta 53 (TCP e UDP)



Fonte: elaborado pelo autor

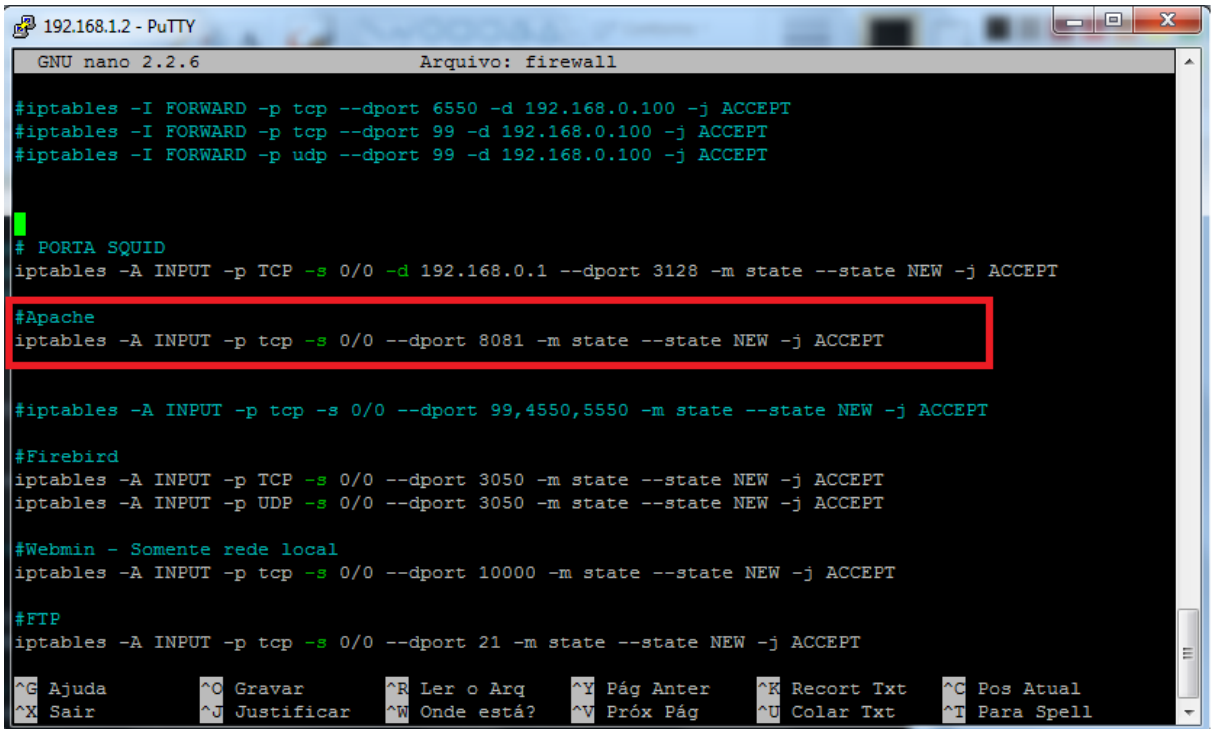
Figura 27 : *Firewall* - Liberação porta 53 TCP e UDP



Fonte: elaborado pelo autor

O *website* da automação é executado pelo servidor *web* Apache, sendo que o mesmo está configurado fora da porta padrão HTTP (80), sendo utilizada a porta 8081. A liberação da porta 8081 para o servidor Apache pode ser vista na imagem abaixo:

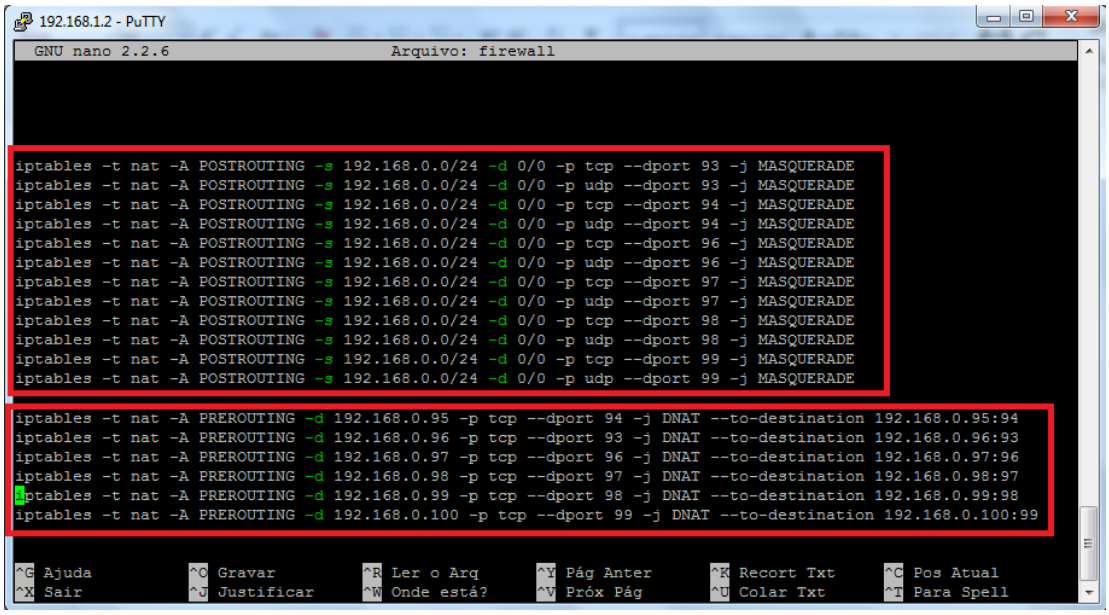
Figura 28 : *Firewall* - Liberação porta 8081 para o Apache



Fonte: elaborado pelo autor

A automação residencial possui câmeras de vídeo IP para o monitoramento dos cômodos e para visualização do estado dos equipamentos, como verificar se uma lâmpada está acesa, se o portão da garagem está aberto, entre outros. No *firewall* foram configuradas regras para acesso às portas das câmeras e para permitir a "saída" da imagem captada para o *website*. Abaixo, segue a imagem com as devidas configurações de *firewall*:

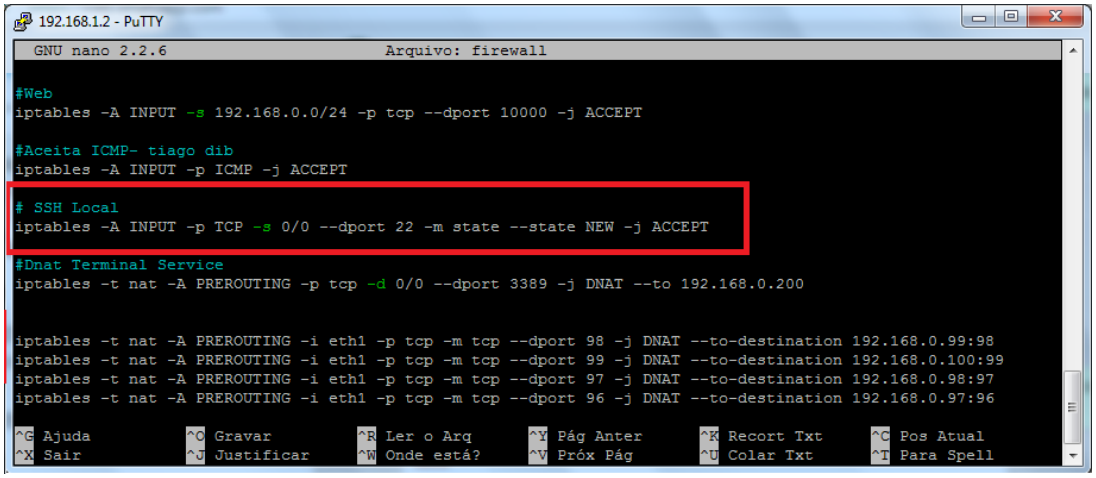
Figura 29 : *Firewall* - Liberação portas das câmeras



Fonte: elaborado pelo autor

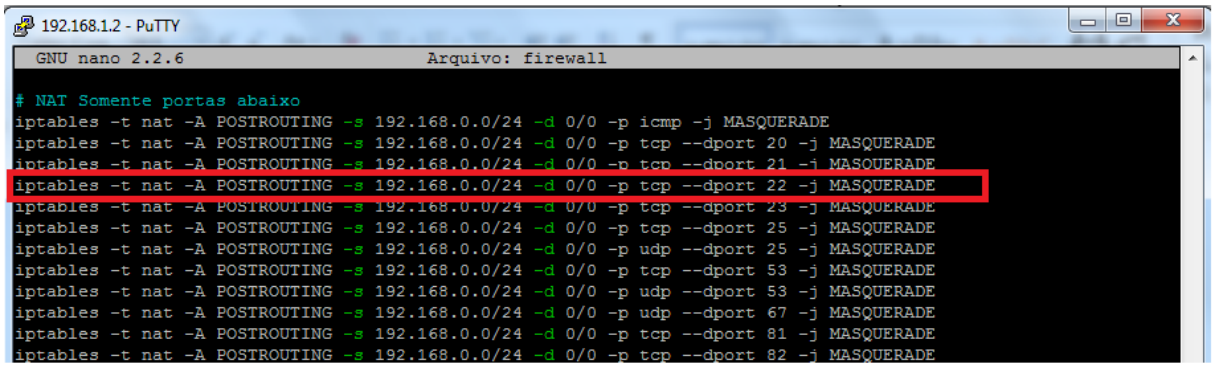
No *firewall*, foi criada uma regra para liberar o acesso ao servidor Linux utilizando o protocolo SSH. O protocolo SSH permite a utilização de software para acesso ao servidor para realizar manutenção em arquivos do Linux. Durante a elaboração do projeto, os acessos ao servidor foram feitos utilizando o software Putty.

Figura 30 : *Firewall* - Liberação porta SSH



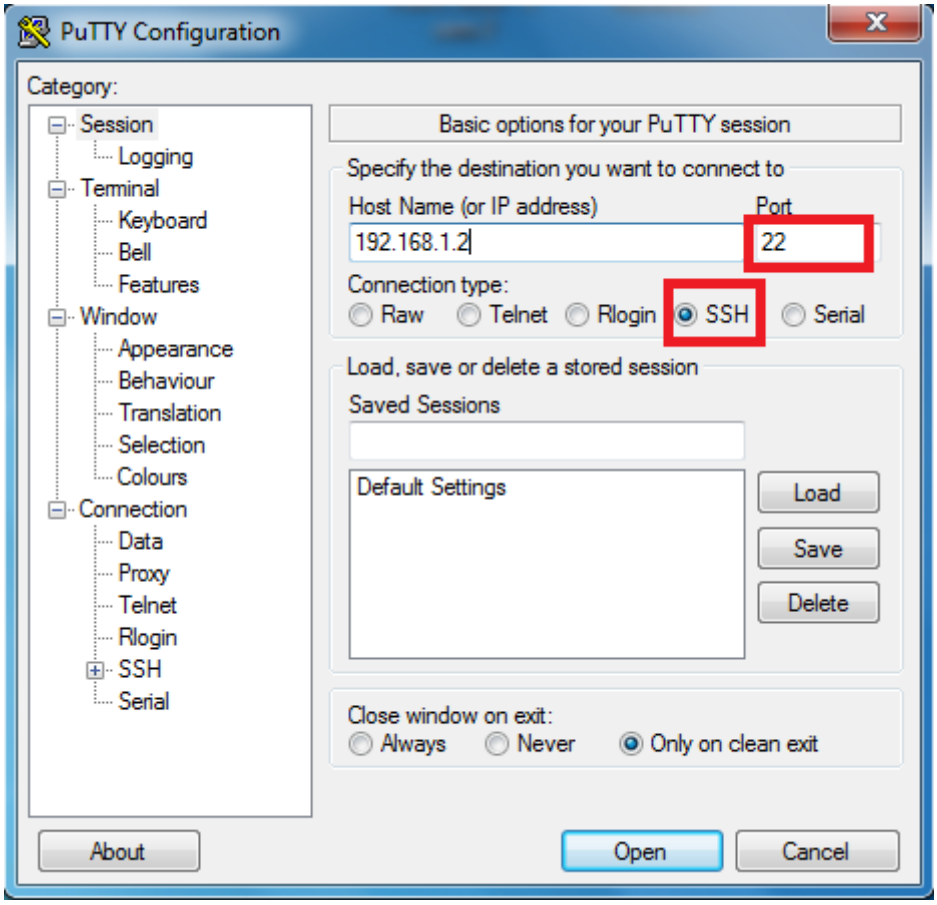
Fonte: elaborado pelo autor

Figura 31 : *Firewall* - Liberação porta SSH



Fonte: elaborado pelo autor

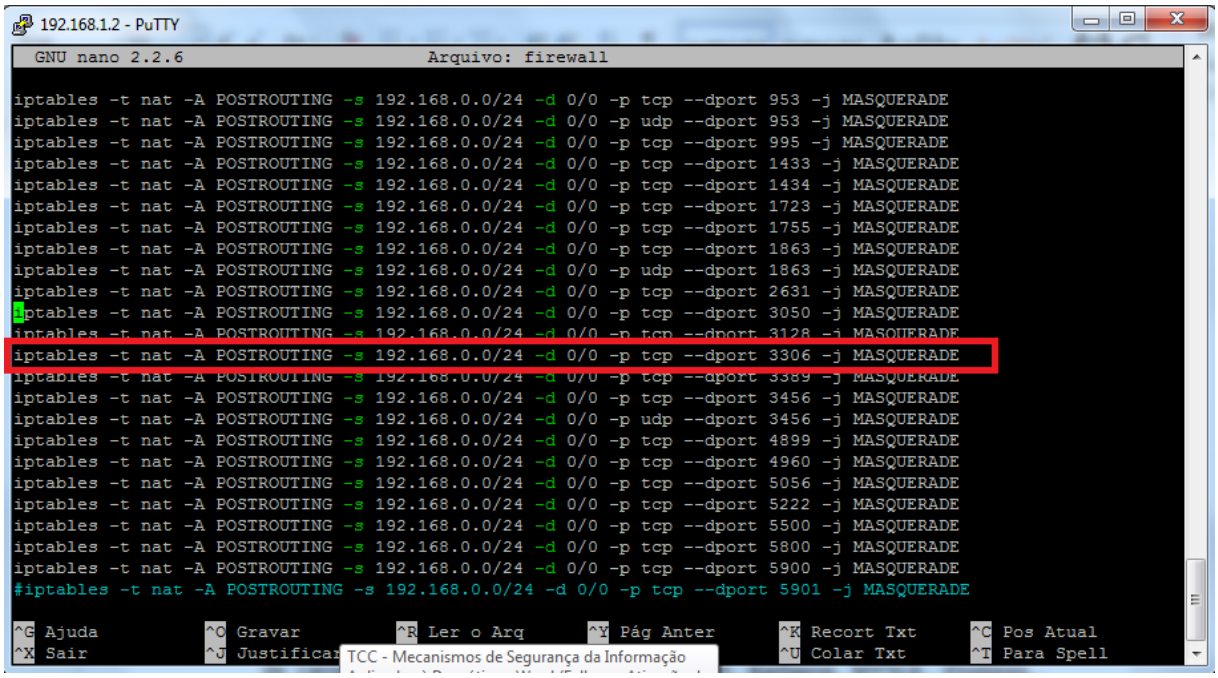
Figura 32 : Putty - Acesso SSH no servidor Linux



Fonte : elaborado pelo autor

Por fim, ainda há a configuração do banco de dados MYSQL, onde ficam gravadas as informações das ações executadas no *website*.

Figura 33 : *Firewall* - Liberação porta MYSQL

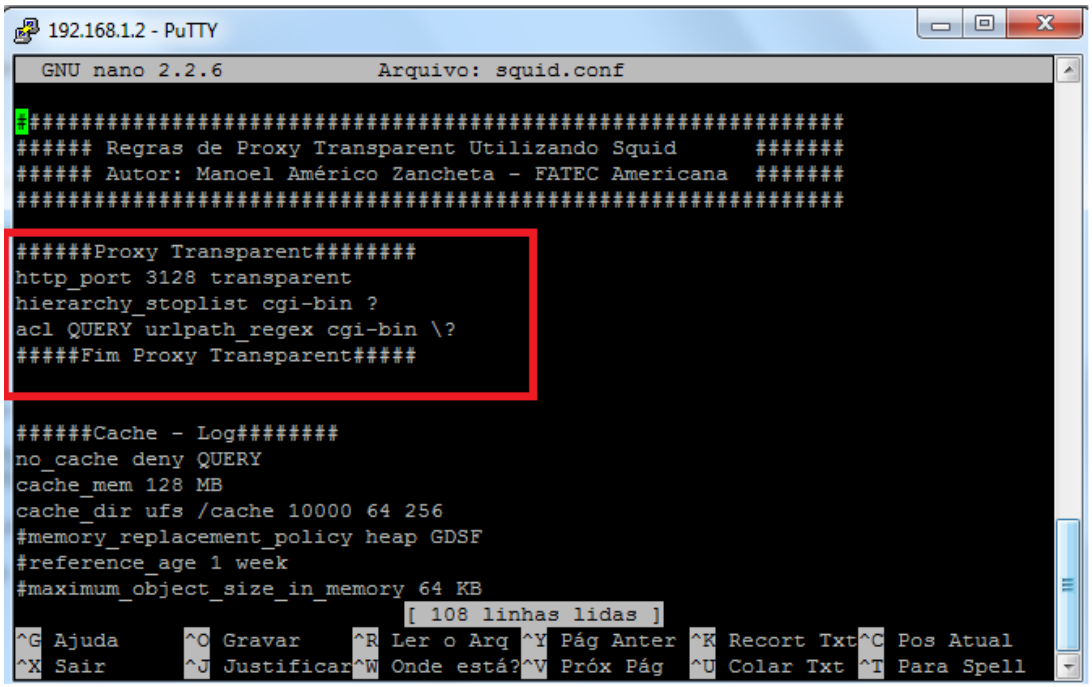


Fonte: elaborado pelo autor

- *Proxy* (SQUID): O SQUID é um *firewall* de aplicação (*proxy*), que possibilita máquinas de uma rede privada, acessarem uma rede pública (internet). O servidor *proxy* é instalado na máquina com acesso direto à internet e as demais máquinas da rede, fazem solicitações de acesso à ela. As principais vantagens ao utilizar o SQUID são: possibilidade de ocultar sessões repetidas, esconder www, DNS e outros recursos de rede compartilhados para um grupo de pessoas, pode ser utilizado principalmente para protocolos HTTP e FTP (tem suporte também para TLS, SSL e HTTPS), permite trabalhar com níveis de acesso, permite distribuição de carga, permite autenticações como SAMBA, Kerberos, MYSQL, Postgres, Ldap, AD e outros.

Conforme a imagem abaixo, do arquivo de configuração do SQUID (**/etc/squid/squid.conf**), o *proxy* foi configurado como *proxy* transparente. Utilizar o *proxy* desta maneira, evita que o administrador tenha que configurar o navegador *web* de cada ponto da rede (*proxy* é despercebido pelo usuário), evitando que o usuário o desabilite e consiga navegar diretamente na internet.

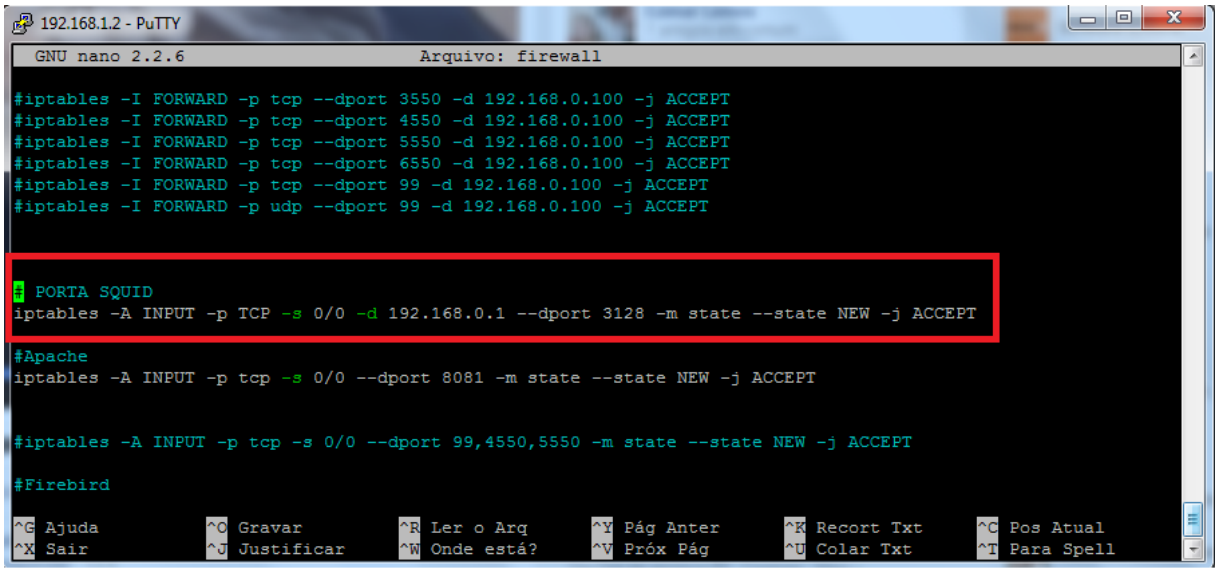
Figura 34 : Configuração *proxy* SQUID



Fonte: elaborado pelo autor

No arquivo do firewall **(/etc/init.d/firewall**), no que diz respeito ao SQUID, foi adicionada uma regra no protocolo TCP no IP 192.168.0.1 para a porta de destino 3128, fazendo "pular" para o alvo especificado quando um pacote coincidir com uma regra particular. A configuração pode ser vista na imagem que segue:

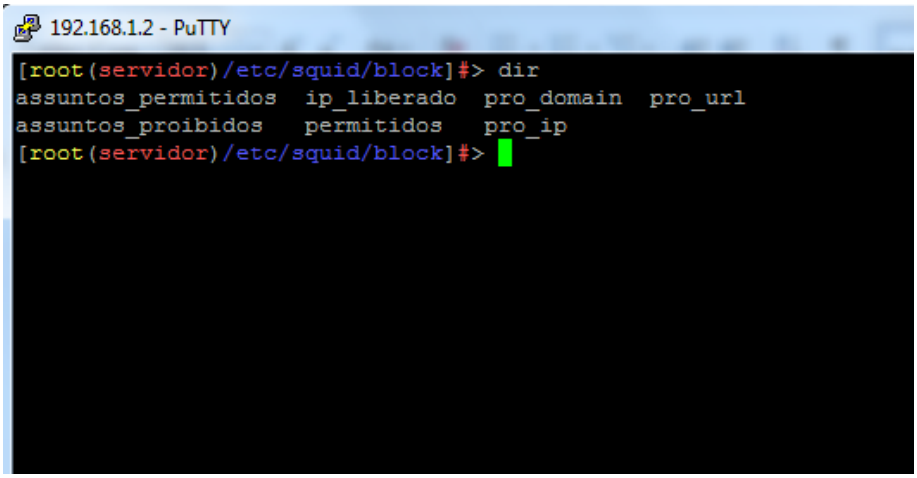
Figura 35 : Regra do SQUID no *firewall*



Fonte : elaborado pelo autor

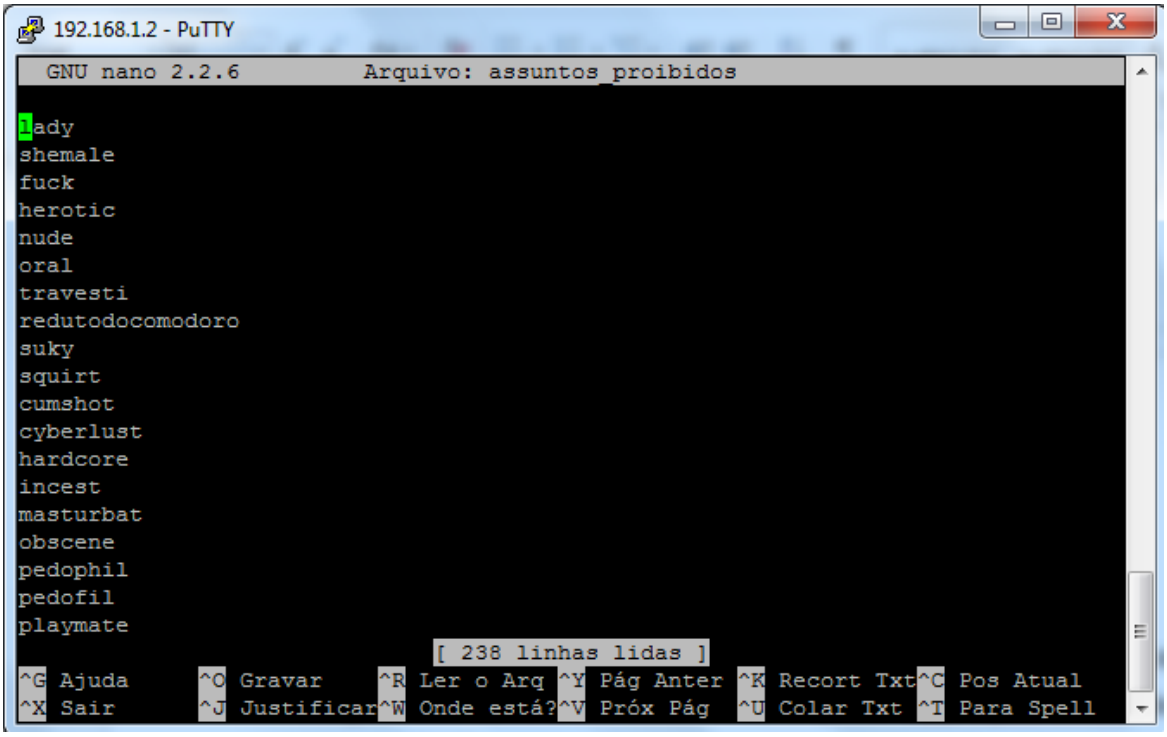
Conforme apresentado na imagem abaixo, foram criados vários arquivos (**/etc/squid/block**) de configuração para o SQUID que permitem ou negam o acesso a sites, bloqueiam o uso da internet em determinado horário, liberam acessos para IPs específicos, entre outros:

Figura 36 : Aquivos bloqueios/permissões do SQUID



Fonte: elaborado pelo autor

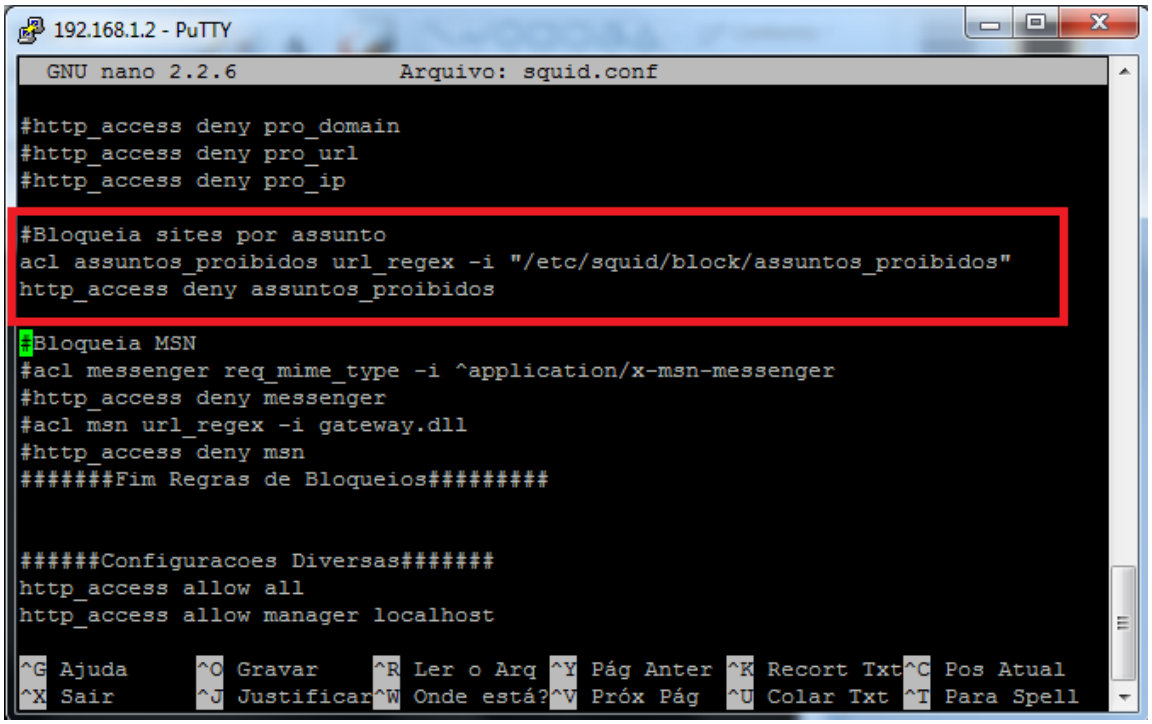
Figura 37 : Arquivo assuntos proibidos SQUID



Fonte: elaborado pelo autor

No SQUID, pode-se observar o uso destes arquivos, conforme a figura abaixo:

Figura 38 : SQUID bloqueio por assunto



Fonte : elaborado pelo autor

6. CONCLUSÃO

O desenvolvimento do presente trabalho, possibilitou uma análise sistemática de como implementar mecanismos de segurança da informação à automação residencial, permitindo que os recursos tecnológicos da mesma sejam utilizados com níveis de segurança aceitáveis dentro de um orçamento acessível ao proprietário da residência. Um estudo cuidadoso, permitiu escolher a melhor relação custo x benefício para a seleção do microcontrolador utilizado (Atmel), o tipo de *firewall* (*firewall* por *software* do Linux em detrimento de um firewall por hardware), a hospedagem do *website* em servidor próprio (servidor *web* Apache), o uso do protocolo TCP/IP por ser comum na maioria das residências. Além disso, permitiu conhecer melhor o mercado atual de domótica e quebrar o paradigma de que a automação é acessível somente à classe alta e que a automação está diretamente relacionada a status. Estudos demostram que, com o avanço da tecnologia e o aumento na oferta de produtos para automação, os equipamentos estão mais acessíveis a todas as classes sociais. Antes considerada artigo de luxo, atualmente os benefícios da automação proporcionaram aos idosos, a opção de vida independente por usufruírem de facilidades proporcionadas pela mesma.

De um modo geral, pode-se afirmar que o ponto central dos requisitos de segurança implementados, diz respeito à implementação do *firewall* no Linux Debian 7. É na configuração do *script* do *firewall* que constam todas as regras de permissões de acesso de entrada/saída às portas de comunicação, liberação ou não de protocolos de comunicação, entre outros. Como complemento ao firewall que atua na camada de rede, a implementação de um *proxy* transparente aumenta o nível de segurança por atuar na camada de aplicação, restringindo acessos não contemplados pelo firewall.

Ao aplicar testes em ambiente residencial real, apurou-se que os objetivos em relação à segurança dentro do que foi proposto, foram alcançados. Além da segurança proporcionada pelo conjunto *firewall* x *proxy*, outras implementações complementares de segurança ofereceram proteção maior ao cenário. Destaca-se

entre estas implementações, a criptografia de senhas de usuários do sistema, as regras rígidas para geração de senhas de acesso, o controle de sessões de usuários, o cuidado com injeções de SQL no banco de dados. A configuração da rede separando a rede interna (cabeada) da rede wireless em faixas diferentes, contribui também com a segurança do ambiente, forçando que todo acesso pela rede wireless direcione sempre o usuário para a internet e nunca para a intranet da automação.

Todos os equipamentos da automação são acionados pelo conjunto Arduino x relês e notou-se durante as pesquisas, que o mercado tende a usar cada vez mais o conceito de internet das coisas (IoT), onde a internet passa a ser baseada nas coisas e não nas pessoas, ou seja, casa coisa da casa (televisão, geladeira, lâmpada, micro-ondas, etc) passa a ser um *end node* da rede (ponto da rede na internet) e não somente o usuário da internet. Estes equipamentos, além de poderem comunicar-se com a central da automação tem a capacidade de comunicar-se entre si. Na Europa, Estados Unidos e Canadá estes equipamentos são oferecidos por diversos fabricantes e a tendência é chegar a um protocolo de comunicação universal, assim como ocorreu com o protocolo de rede.

Como sugestão de continuidade do projeto e proposta de melhorias, propõem-se maior atenção aos equipamento que contemplam IoT, os mesmos são tendências de mercado e mesmo não havendo uma grande oferta no mercado nacional, é importante entender estes novos conceitos e preparar-se para eles. Em relação ao *website*, seria interessante uma implementação de logs das operações dos usuários para posterior consulta. Uma rotina de envio de mensagens poderia ser adicionado para que, toda vez que a automação fosse acionada, um aviso fosse enviado ao gestor da automação através de uma mensagem eletrônica. Seria muito interessante também uma implementação futura de monitoramento convencional (vivo/morto on/off), acompanhamento de desempenho de aplicações, análise de experiência de usuário e análise de causa raiz em ambientes complexos, através do servidor Zabbix. Outras sugestões desejáveis, que envolvem um investimento maior, seria a instalação de um *firewall* por *hardware* e um *link* de internet exclusivo para a automação e um segundo *link* exclusivo para outras finalidades da residência.

Portanto, automatizar uma residência vai muito além de simples recursos eletrônicos, é uma tendência para gestão racional de energia, independência de vida para idosos e deficientes, segurança e conforto entre outros e que pode ser implementada a baixo custo.

REFERÊNCIAS BIBLIOGRÁFICAS

AURESIDE. **Previsões para o mercado global de automação residencial.** 2016. Disponível em: <http://aureside.blogspot.com.br/2016/10/previsoes-para-o-mercado-global-de.htm>. Acessado em: 19 mar. 2017

MICROPCHIP ATMEL**.** **Microcontroladores**. Disponível em: <http://www.atmel.com/pt/br/products/microcontrollers/default.aspx>. Acesso em: 05 abr. 2017.

BANZI, Massimo. **Getting started with Arduino**. 3rd. U.S.A: O'Reilly, 2017

DIAS, C. **Segurança e auditoria em tecnologia da informação**. Rio de Janeiro: Axcel, 2000.

GUSMÂO, Gustavo. **Chrysler faz recall de 1,4 milhão de carros para corrigir brecha de segurança**,2015. Disponível em: <http://exame.abril.com.br/tecnologia/chrysler-faz-recall-de-1-4-milhao-de-carros-apos-veiculo-ser-hackeado-remotamente>. Acesso em 19 mar. 2017

KUROSE, J.F; ROSS K.W. **Redes de computadores e internet:** Uma abordagem top-down. 6 ed. São Paulo: Addison Wesley, 2013.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação**. 2008

Rio de Janeiro: Editora Ciência Moderna Ltda.

MOREIRA, Fernando. **Hacker invade sistema de outdoor eletrônico e exibe pornô em Jacarta**, 2016. Disponível em: <http://blogs.oglobo.globo.com/pagenotfound/post/hacker-invade-sistema-de-outdoor-eletronico-e-exibe-porno-em-jacarta.html>. Acesso em: 19 mar. 2017

NATIONAL INSTRUMENTS. **Conceitos gerais de comunicação serial**, 2014. Disponível em: <http://digital.ni.com/public.nsf/allkb/32679C566F4B9700862576A20051FE8F>. Acesso em: 16 abr. 2017

PLATAFORMA CONECTAR. **Tendências Mundiais na Automação Residencial**. Dezembro 2016. Disponível em: http://plataformaconectar.blogspot.com.br/2016/12/automacao-residencial-e-as-tendencias.htm>l. Acesso em: 30 mar. 2017.

REDAÇÃO OLHAR DIGITAL. **Hacker é condenado à prisão por transmitir pornografia em outdoor**. 2011. Disponível em: <https://olhardigital.uol.com.br/fique_seguro/noticia/hacker_condenado_a_prisao_por_transmitir_pornografia_em_outdoor/17098>. Acesso em: 19 mar. 2017

SILVA FILHO, C.R. **CLP:** Definição. Disponível em: <http://livrozilla.com/doc/9122/clp---definicao>. Acesso em: 04 abr. 2017.

SILVA FILHO, Antonio Mendes: **Revista espaço acadêmico N42. Segurança da Informação: Sobre a necessidade de proteção de sistemas de informação**, Novembro 2004. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm>. Acesso em: 23 abr. 2017.

SOARES, Jéssica C. **Protoboard**, Julho 2015. Disponível em:<http://www.eletronite.com.br/aprenda/protoboard-agilidade-e-praticidade.html>. Acesso em: 23 abr. 2017.

SOARES, Karla. **O que é um Arduino e o que pode ser feito com ele?** Outubro 2013. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2013/10/o-que-e-um-arduino-e-o-que-pode-ser-feito-com-ele.html>. Acesso em: 18 abr. 2017.

SOUZA, David José de. **Desbravando o PIC: ampliado e atualizado para PIC16F628A**. São Paulo: Érica, 2005.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de Computadores**. 5. ed. Pearson Education do Brasil, 2011