UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

PROPOSTA DE IMPLEMENTAÇÃO DE UM SISTEMA DE CONTROLE DE ACESSO DE DISPOSITIVOS E UTILIZADORES À REDE CORPORATIVA.

Caso de estudo: **Novo Banco Popular S.A.**

Autor:

CHAMANGO, Arsénio Francisco

Supervisor:

Eng.° Rúben Moisés Manhiça

Maputo, Maio de 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

PROPOSTA DE IMPLEMENTAÇÃO DE UM SISTEMA DE CONTROLE DE ACESSO DE DISPOSITIVOS E UTILIZADORES À REDE CORPORATIVA.

Caso de estudo: **Novo Banco Popular S.A.**

Autor:

CHAMANGO, Arsénio Francisco

Supervisor:

Eng.° Rúben Moisés Manhiça

Maputo, Maio de 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ENTREGA DE RELATÓRIO DO TRABALHO DE LICENCIATURA

Declaro que o estudante **Arsénio Francisco Chamango** entregou no dia 08/05/2023 as 03 cópias do relatório do seu Trabalho de Licenciatura com a referência: **2023EITLN___**, intitulado: Proposta de Implementação de um Sistema de Controle de Acesso de Dispositivos e Utilizadores à Rede Corporativa.

Maputo, 08 de Maio de 2023

O Chefe da Secretaria

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

DECLARACAO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharias da Universidade Eduardo Mondlane.

.

Maputo, 08 de Maio de 2023

O Autor

_____

(Arsénio Francisco Chamango)

Dedicatória

Aos meus pais, Francisco e Ana

A minha esposa, Edna

Aos meus filhos, Warrick e Kendrick

Agradecimentos

Agradeço, em primeiro lugar à Deus pelo dom da vida, protecção, entendimento e força ao longo de todo meu percurso estudantil.

Aos meus pais, pelo apoio, amor e carinho, pela sua dedicação a mim, por me terem dado forças, suporte emocional e financeiro que foi investir na minha educação. Sei que não mediram esforços para que este sonho se realizasse, e sem a compreensão, ajuda e confiança deles nada disso seria possível hoje. A eles além da dedicatória e agradecimento 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!

Ao meu supervisor, Eng.º Ruben Manhiça durante a elaboração do presente trabalho, ao Doutor Eng.º Lourino Chemane pelos ensinamentos fascinantes que depositara em mim durante o meu processo estudantil, o meu muito obrigado.

Aos meus docentes, Eng.º Felizardo Munguambe, dr. Valy Issufo e a Eng.ª Ivone Cipriano pelos ensinamentos ao longo do meu percurso académico.

Agradeço ainda aos meus amigos Alberto, Hélio, Mauro e Dércio e a todos os colegas que comigo trilharam os sinuosos caminhos a busca do saber.

E por último, porém não menos importante, a minha esposa Edna Chamango quero dedicar e agradecer, pois sem sua ajuda, confiança e compreensão, meu sonho não teria sido realizado, ela foi fundamental porque sempre dispôs do suporte moral durante este percurso longo que por vezes sacrificou alguns momentos familiares, e me deu a mão quando eu pensava em desistir. Por isso, dedico ela este grande feito em minha vida.

Por fim, a todos que de forma directa ou indirecta contribuíram para a minha formação académica, o meu khanimambo.

Epígrafe

"A educação é o nosso passaporte para o futuro,

pois o amanhã só pertence ao povo que prepara o hoje."

Malcolm X

Resumo

Com o crescente número de dispositivos de acesso à rede, como *smartphones* e até computadores pessoais que se ligam à uma rede corporativa, é necessário garantir uma visibilidade e maior controle aos dispositivos e os recursos que os mesmos acedem**,** principalmente dentro de uma empresa em que dados críticos e sensíveis não podem ser acedidos por qualquer um. O presente trabalho apresenta uma abordagem teórica e prática sobre a implementação de um sistema de controle de acesso de dispositivos e utilizadores à rede de dados, tendo o foco o ambiente corporativo do Novo Banco Popular, SA, considerando como o objectivo geral do trabalho é propor um sistema que garanta maior visibilidade e controle sobre os dispositivos e utilizadores que se conectam à rede corporativa.

Para atingir esse objectivo, o trabalho se propõe a analisar os procedimentos existentes para garantir o acesso à rede corporativa do Novo Banco Popular SA, apresentar conceitos relacionados a redes de computadores, políticas de segurança, protocolos e tipos de controle de acesso à rede aplicáveis ao contexto do banco, analisar soluções tecnológicas disponíveis para o controle de acesso à rede corporativa e, por fim, implementar uma prova de conceito da solução proposta em um ambiente de testes.

A implementação desse sistema de controle de acesso visa aprimorar a segurança da rede corporativa do Novo Banco Popular SA, permitindo uma melhor visibilidade e controle dos dispositivos e utilizadores autorizados a se conectar. Isso contribuirá para proteger os activos de informação do banco, mitigar possíveis riscos de segurança e garantir o cumprimento das políticas de segurança estabelecidas.

O estudo evidência de que há necessidade de investimentos em medidas de segurança dinâmica da rede de dados, o que pressupõe a vulnerabilidades na rede devido ao controlo limitado do estado dos dispositivos e utilizadores na rede interna. Nessa perspectiva, o presente trabalho visa implementar uma prova de conceito com a finalidade de garantir o controle do acesso dos dispositivos e utilizadores à rede interna, com vista a proteger do uso indesejado da rede, ameaças de segurança intencionais e não intencionais, de *worms*, vírus e mais através de sistemas finais vulneráveis.

Palavras-chave: Autenticação. Autorização Avaliação. Remediação, Quarentena, NAC (Network Access Control), NBP (Novo Banco Popular).

Abstract

With the growing number of network access devices, such as smartphones and even personal computers that connect to a corporate network, it is necessary to ensure visibility and greater control over the devices and the resources they access, especially within a company where critical and sensitive data cannot be accessible by just anyone. The present work presents a theoretical and practical approach on the implementation of a device and user access control system to the data network, focusing on the corporate environment of Novo Banco Popular, SA, considering how the general objective of the work is to propose a system that guarantees greater visibility and control over the devices and users that connect to the corporate network.

To achieve this objective, the work proposes to analysis of the existing procedures to guarantee access to the corporate network of Novo Banco Popular SA. The work presents concepts related to computer networks, security policies, protocols and types of access control to the network applicable to the context of the bank, analyze available technological solutions for controlling access to the corporate network and, finally, implement a proof of concept of the proposed solution in a test environment.

The implementation of this access control system aims to improve the security of the corporate network of Novo Banco Popular SA, allowing better visibility and control of devices and users authorized to connect. This will help protect the bank's information assets, mitigate possible security risks and ensure compliance with established security policies.

The study shows that there is a need for investments in dynamic data network security measures, which presupposes network vulnerabilities due to limited control of the state of devices and users on the internal network. In this perspective, the present work aims to implement a proof of concept in order to guarantee the access control of devices and users to the internal network, in order to protect against unwanted use of the network, intentional and unintentional security threats, worms, viruses and more through vulnerable end systems.

Keywords: Authentication. Authorization, Accountability, Remediation, Quarantine, NAC (Network Access Control), NBP (Novo Banco Popular)

Lista de abreviaturas e acrónimos

AAA – Authentication Authorization Accoutability

ACL – Access Control List

AD – Active Directory

ADOS - Application Deployment Engine Operating System

ATM – Automated Teller Machine

AP – Access Points

ARP - Address Resolution Protocol

BOOTP - Bootstrap Protocol

BYOD – Bring Your Own Device

CIA - Confidentiality, Integrity, Availability

CIMC - Cisco Integrated Management Controller

CCTV – Closed-circuit Television

CHAP – Challenge-Handshake Authentication Protocol

DR – Disaster Recovery

DNS – Domain Name Service

DTI – Departamento de Tecnologias de Informação

DHCP – Dynamic Host Configuration Protocol

EAP – Extensible Authentication Protocol

EAPOL - Extensible Authentication Protocol over LAN

FQDN – Fully Qualified Domain Name

GTC – Generic Token Card

GUI - Graphical User Interface

HTTP – Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

ICS – Industrial Control System

ICMP – Internet Control Message protocol

IGMP – Internet Group Management Protocol

IP – Internet Protocol

IPSec - Internet Protocol Security

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

IoT – Internet of Things

IEEE - Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

ISO - International Organization for Standardization

LAN – Local Area Network

LED – Light-emitting Diode

MAB – Mac Address Bypass

MAC – Media Access Control

MDM – Mobile Device Management

MD5 – Message Digest Algorithm

NAC – Network Access Control

NAK – Negative Acknowledgment

NIC – Network Interface Card

OSI – Open Systems Interconnection

OTP – One Time Password

PAP - Password Authentication Protocol

PEAP – Protected Extensible Authentication Protocol

RADIUS - Remote Authentication Dial-In User Service

RFC - Request for Comments

TI – Tecnologias de informação

TICs – Tecnologias de Informação e Comunicação.

TCP/IP – Transmission Control Protocol/Internet Protocol

TCG – Trust Computing Group

TLS - Transport Layer Security

TTLS - Tunnelled Transport Layer Security

TACACS - Terminal Access Controller Access Control System

LLD – Low Level Design

SAML - Security Assertion Markup Language

SSH – Secure Shell

SNMP - Simple Network Management Protocol

URL – Universal Resource Locator

UTP - Unshielded twisted pair

USB - Universal Serial Bus

VPN – Virtual Private Network

VLAN - Virtual Local Area Network

WAN – Wide area Network

Glossário de Termos

Autenticação – é um processo de segurança para verificar a veracidade e autenticidade de uma pessoa ou objecto.

Autorização - Autorização é a acção e o efeito de autorizar (reconhecer a faculdade ou o direito de uma pessoa para fazer algo).

Access Point – é um dispositivo em uma rede sem fio que realiza a interconexão entre os dispositivos móveis.

Antivírus – é um *software* que detecta, impede e actua na remoção de programas de *software* maliciosos, como vírus e *worms*.

Boostrap - é o programa que inicializa o sistema operativo (SO) durante a inicialização.

Broadcast - é um método de transferência de mensagem para todos os receptores simultaneamente

Covid-19 - É uma doença respiratória causada pelo vírus SARS-CoV-2 e apresenta como principais sintomas febre, tosse seca e dificuldade respiratória.

Firewall – é um elemento de uma rede, sendo baseado em *software* ou em *hardware*, que controla o tráfego de entrada e saída de informação, através da análise dos pacotes de dados, e assim determinando se eles podem passar ou não, baseando-se em uma série de regras.

Gateway – fornece comunicação com uma rede remota ou um sistema autónomo que está fora dos limites para os nós da rede local

Hyperterminal - é uma ferramenta de comunicação que permite aos usuários conectar e se comunicar com dispositivos remotos usando vários protocolos, como serial, telnet e *modem.*

Malware – é qualquer *software* intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores.

Hardware – é a parte física de computadores e outros sistemas microelectrónicos.

Hub – Dispositivo não gerenciável que conecta dois ou mais equipamentos de rede.

Patch - é um programa de computador criado para actualizar ou corrigir um *software* de forma a melhorar sua usabilidade ou performance.

Phishing – é uma técnica de engenharia social usada para enganar usuários de *internet* usando fraude electrónica para obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito. São comunicações falsificadas praticada por criminosos chamados *phishers* que parecem vir de uma fonte confiável.

Intranet – é uma rede de computadores privada que assenta sobre a suíte de protocolos da Internet, porém, de uso exclusivo de um determinado local, como, por exemplo, a rede de uma empresa, que só pode ser acedida pelos seus utilizadores ou colaboradores internos.

Internet – é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos (Internet Protocol Suite ou TCP/IP) com o propósito de servir progressivamente usuários no mundo inteiro.

ISO - é uma imagem de CD, DVD ou BD de um sistema de ficheiros

Log – é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.

Roteador - é um dispositivo que encaminha pacotes de dados entre redes de computadores, criando um conjunto de redes de sobreposição.

Software - é um conjunto de instruções escritas para serem interpretadas por um computador com o objectivo de executar tarefas específicas, ou seja, representa a parte lógica do computador.

Switch – é um dispositivo equipado com várias portas de comunicação que conecta os elementos dentro da rede para a transmissão de dados, vídeo ou voz. Trata-se de um intermediário que recebe os pacotes de dados enviados por qualquer dispositivo da LAN e os redirecciona para seu respectivo destino.

Sniffers - é um programa de computador ou *hardware* que pode interceptar e registrar tráfego que passa sobre uma rede digital ou parte de uma rede.

Survey - é um tipo de investigação quantitativa. Ela pode ser definida como uma forma de colectar dados e informações a partir de características e opiniões de grupos de indivíduos.

Spyware – é um tipo de programa automático intruso (ou *malware*) destinado a infiltrar-se em um sistema de computadores e *smartphones*, para colectar informações pessoais ou confidenciais do utilizador de forma ilícita, e encaminhar para uma entidade externa via Internet para fins maliciosos, ou análise de marketing e financeiros.

Telnet - é um protocolo de rede na Internet ou redes locais para proporcionar uma facilidade de comunicação baseada em texto interactivo bidireccional usando uma conexão de terminal virtual. Os dados do usuário são intercalados em banda com informações de controle *Telnet* em um *byte* de conexão 8-bit de dados orientado sobre o *Transmission Control Protocol* (TCP).

Utilizador - é o termo utilizado para referenciar a qualquer um que utiliza determinado recurso ou serviço.

Virus – é um *software* malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

Wireless - é uma infra-estrutura das comunicações sem fio que permite a transmissão de dados e informações sem a necessidade do uso de cabos – sejam eles telefónicos, coaxiais ou ópticos.

Worms - é um programa independente (*standalone*), do tipo *malware*, que se replica com o objectivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino para acede-lo.

Índice

Lista de figuras

Lista de tabelas

1. Capítulo I - Introdução

1.1. Contextualização

O Novo Banco Popular S.A. (NBP) é um nome fictício de uma instituição de crédito e sistemas financeiros pertencente a um grupo com sede em Joanesburgo, África do Sul e que por questões de confidencialidade foi atribuído um nome fictício para omitir o verdadeiro nome da instituição bancária. O banco foi fundado a mais de 30 anos e oferece serviços bancários transaccionais, poupança, empréstimos, investimentos, seguros, gerenciamento de risco, gerenciamento de património e serviços de consultoria para seus clientes. Segundo um recente estudo das melhores instituições e sociedades de crédito moçambicanas, o NBP é considerado como um dos três melhores bancos comerciais de moçambique.

Uma das áreas de apoio ao negócio do Banco é o departamento de tecnologias e de informação (DTI), onde um dos desafios da equipe técnica é a prestação de serviços de qualidade e segurança que vão de acordo com as expectativas do negócio da instituição. Esta questão tornou-se cada vez mais preocupante com o surgimento da pandemia da COVID-19 que forçou os colaboradores da instituição a trabalhar em um regime de rotatividade e de trabalho remoto a partir das suas residências. Dado que a instituição não estava preparada para alocar computadores portáteis a todos colaboradores, se transigiu também pela aprovação do uso dos dispositivos pessoais para acesso à rede interna para trabalhar a partir de qualquer lugar.

Neste sentido, como forma de materializar esta nova forma de trabalho, o Conselho de Administração aprovou, por consenso, o normativo do regime de trabalho remoto e de rotatividade dos colaboradores da instituição, com o objectivo de garantir a continuidade do negócio e prestação de serviços aos clientes.

O NBP dispõe de um parque tecnológico vasto e complexo com vários tipos de dispositivos de acesso à rede de dados interna e privada como computadores, *tablets, smartphones, access points*, telefones IP, ATMs e também de dispositivos de segurança electrónica conhecidos como *Internet* das coisas (IoT) nomeadamente câmaras CCTV, controle de acessos, e sistemas de raio X. Importa referir que a gestão deste todo parque tecnológico é feita pelo departamento de tecnologias e sistemas de informação (DTI).

De acordo a nova forma de trabalho, preocupa ao DTI o controle de dispositivos, utilizadores e de como estes acedem aos recursos disponíveis na rede interna e privada, pois actualmente este controle é assegurado por meio ao método tradicional baseado na autenticação à rede interna por credenciais pessoais do domínio institucional. O método vigente permite com que a equipe do DTI tenha a administração centralizada de quem acede à rede interna, mas não garante a visibilidade e o controle do estado dos dispositivos que acedem a rede e que tipo de informação é acedida.
Dentro do contexto do DTI voltada a prestação de serviços de qualidade e segurança para o apoio ao negócio do Banco, o presente estudo propõe um sistema com uma arquitectura de segurança melhorada, que salvaguarda a confidencialidade, integridade e disponibilidade das informações, através das seguintes funcionalidades:

- Visibilidade e gestão de identidade dos vários tipos de dispositivos conectados à rede;
- Avaliação dos dispositivos antes de se conectarem à rede interna e privada (pré-conexão) e depois de conectados à rede interna e privada (pós-conexão);
- Assistências de remedição para dispositivos e/ou utilizadores que não estiverem em conformidade com as políticas de segurança da rede;
- Relatórios de conformidade que detalhem a localização dos dispositivos na rede e o que eles estavam a fazer na rede.

Partindo do entendimento sobre os actuais procedimentos tomados para garantir o acesso à rede interna do NBP, e tomando em consideração o actual funcionamento da instituição, na qual se verifica utilizadores que trazem computadores pessoais, dentre outros dispositivos dentro e fora da instituição; Os utilizadores com o acesso remoto que se conectam a partir de suas residências ou locais públicos; A terceirização de negócios que requer o acesso à rede interna por parte dos parceiros, visitantes, fornecedores e até contratados com acesso físico à rede interna para realizar seu trabalho, o presente estudo procura propor um sistema que aprovisiona melhorias de segurança da rede interna do NBP com finalidade de resguardar um ambiente de negócios mais seguro e eficiente.

1.2. Definição do problema

Como referido na secção anterior, um dos desafios da equipe técnica do DTI é a prestação de serviços de qualidade e segurança que vão de acordo com as expectativas do negócio da instituição. O NBP tem envidado esforços no sentido de fornecer acesso às informações aos utilizadores a qualquer hora e de qualquer lugar para executarem os seus trabalhos. Com os colaboradores,

utilizadores e até visitantes a fazerem o uso dos seus próprios dispositivos dentro e fora dos escritórios para aceder a rede interna do Banco, a instituição corre o risco de expor a informação confidencial aos diversos tipos de ataques e ameaças cibernéticas, devido a fraca visibilidade e controle do estado dos dispositivos internos e externos que se conectam à rede interna do Banco, e como consequência podem levar à perda de informação, privacidade pessoal, e outros dados críticos.

1.3. Justificativa

O presente trabalho surge como fruto da dificuldade encontrada pelo DTI em garantir o acesso controlado e seguro à rede interna e privada, por meio à vários dispositivos sem comprometer a informação confidencial. Uma vez que a instituição tem recebido visitantes, consultores e até colaboradores que trazem dispositivos pessoais e que necessitam de acesso aos recursos internos da rede, é necessário garantir que tais dispositivos que se conectam à rede cumpram com os requisitos mínimos de forma a mitigar contra diversas ameaças cibernéticas. Com a resolução deste problema perspectiva-se a melhoria da segurança da rede de dados no ambiente corporativo do Banco.

1.4. Objectivos

1.4.1. Objectivos gerais:

- Propor um sistema que assegura maior visibilidade e controle dos dispositivos e utilizadores que se ligam à rede corporativa do Novo Banco Popular SA;

1.4.2. Específicos:

- Descrever os procedimentos tomados para garantir o acesso à rede corporativa do Novo Banco Popular SA;
- Apresentar os conceitos sobre redes de computadores, politicas de segurança, protocolos, e tipos de controle de acesso à rede que possam ser aplicados ao Novo Banco Popular SA;
- Analisar as diferentes soluções tecnológicas de controle do acesso à rede corporativa; e
- Implementar uma prova de conceito da solução proposta em um ambiente de testes.

1.5. Metodologia

Nesta secção apresenta-se todos os métodos que foram utilizados para atingir o objectivo do trabalho, mostrando como foram realizadas a pesquisa e a investigação.

1.5.1. Questões de Pesquisa

Segundo Marconi & Lakatos (2003, p.159), o problema deve ser levantado e formulado, de preferência em forma interrogativa e delimitado com indicações das variáveis. O resultado do trabalho realizado teve como fundamento a necessidade de responder a seguinte questão:

- De que maneira o Novo Banco Popular poderá assegurar que os recursos da rede corporativa são acedidos por dispositivos e utilizadores legítimos?

1.5.2. Tipo de Pesquisa

Para além da apresentação da questão que deve ser respondida ao se realizar a pesquisa, importa referenciar o tipo de pesquisa destacado para este trabalho, que toma como base os critérios de classificação apresentados em Prodanov & Freitas (2013). Para o presente estudo, foram identificadas as seguintes metodologias de pesquisa:

1.5.2.1. **Quanto à natureza**:

- **Aplicada**: objectiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos envolvendo verdades e interesses da instituição. Seguindo esta lógica e a própria natureza de um Banco Comercial, que presta serviços aos clientes, o interesse deste estudo é a sua aplicação prática, na tentativa de dar algum contributo ao nível de implementação de melhorias de segurança informática da rede interna do NBP.

1.5.2.2. **Quanto aos procedimentos**:

Segundo Fonseca (2002), a pesquisa científica é o resultado de um questionário ou exame minucioso, realizado com o objectivo de resolver um problema, recorrendo-se a procedimentos científicos como experimental, bibliográfica, documental, de campo, ex-post-facto, de levantamento, com *survey*, estudo de caso, participante, acção, etnográfica ou etnometodológica. A presente pesquisa foi baseada nos seguintes tipos: pesquisa bibliográfica, documental, de campo, e estudo de caso.

- **Bibliográfica**: Segundo (Marconi e Lakatos 2003) faz uso da bibliografia tornada pública em relação ao tema de estudo. Para o presente trabalho é indispensável a consulta de livros digitais, referências publicadas na *internet* em *websites* credíveis;

- **Pesquisa documental**: Segundo (Marconi e Lakatos 2003) a fonte de colecta de dados são documentos, escritos ou não. Para o presente trabalho são tidos em conta trabalhos

científicos relacionados ao tema proposto de forma a poder inferir quais as lacunas e possíveis soluções que podem ser adoptadas.

- **Pesquisa de campo:** Segundo Gerhardt & Silveira (2009), as pesquisas de campo caracterizam-se pelas investigações em além de pesquisa bibliográfica e/ou documental, se realiza a colecta de dados junto as pessoas, com recurso a diferentes tipos de pesquisa. O presente trabalho consistiu em preparar questões (Anexo 2) sobre as metodologias utilizadas para garantir o acesso à rede interna aos dispositivos e utilizadores autorizados, de maneira que se pudesse obter informações gerais e específicas da NBP, no que tange à confidencialidade, integridade e disponibilidade dos dados.

- **Estudo de caso**: envolve o estudo profundo e exaustivo de um ou mais objectos de maneira que se permita o seu amplo e detalhado conhecimento (Silva e Menezes 2005).

1.5.3. Técnicas de recolha de dados

De acordo com Gerhardt & Silveira (2009), a recolha de dados é a busca por informações para a elucidação do fenómeno ou facto que o pesquisador quer desvendar. Para o desenvolvimento do presente estudo, aplicou-se a técnica de pesquisa qualitativa. Desta forma, em primeira instância, a efectivação da pesquisa foi mediante a documentação indirecta, que incluiu a pesquisa bibliográfica e a pesquisa documental.

Na pesquisa bibliográfica se recorreu ao material já escrito sobre o controle de aceso à rede (NAC), particularmente a sua correlação com a melhoria nos aspectos de segurança de acesso à informação em uma rede corporativa, onde abrangeu livros, artigos científicos, e casos de estudo.

Na pesquisa documental se recorreu aos documentos publicados por instituições credíveis sobre implementações de segurança da informação e pesquisas académicas com casos de usos.

1.5.4. Técnicas de análise de Dados

Para a análise e interpretação de dados desta pesquisa foi usada técnica de análise de dados qualitativa. Nesse contexto a seguir são apresentadas as técnicas de análise de dados que foram empregues:

- ✓ **A análise de conteúdo -** do ponto de vista operacional, a análise de conteúdo nesta pesquisa é baseada em dados textuais, como entrevistas, documentos técnicos e relatórios

relacionados ao tema do trabalho que preconiza o controle de acesso à rede, observando-se o uso predominante da técnica de análise de conteúdo no capítulo de revisão bibliográfica, onde a mesma foi usada de modo a permitir que fossem feitas inferências de conhecimentos colhidos relativos a segurança da rede interna.

- ✓ **A Análise de rede** - Esta técnica envolve a análise da topologia da rede empregue no ambiente corporativo do NBP e a identificação de pontos de vulnerabilidade que podem ser mitigados com a implementação de um sistema de controle de acesso à rede. A análise da topologia de rede auxiliou na identificação dos pontos vulneráveis mais críticos na rede e permitiu avaliar o impacto do NAC na segurança desses pontos identificados.

1.5.5. Metodologia para a implementação do Controle de acesso à rede (NAC)

A representação para resolução do problema identificado no ponto 1.2 passa por propor um sistema que inicialmente, se apresenta uma prova de conceito com as funcionalidades propostas, implementadas a um grupo restrito de dispositivos, activos de rede e utilizadores do NBP, seguindo as seguintes acções:

- Efectuar a configuração de um servidor central responsável pela autenticação dos dispositivos e de utilizadores à rede interna, e gerenciador de politicas de segurança da rede interna;
- Configuração de um autenticador à rede, que neste estudo é preconizado um *switch* de acesso, responsável por permitir a conectividade e comunicação entre os dispositivos na rede interna;
- Configuração de um *software* denominado agente/ suplicante em um computador.

Neste sentido uma abordagem em fases é o método preferido para a implementação de uma solução NAC. Em geral, uma implementação NAC pode ser separada nas seguintes fases (*Understanding NAC*, 2010):

Fase 1. Detecção e rastreamento dos dispositivos finais: nesta fase é feita a colecta de informação sobre todos os dispositivos finais, sem causar nenhuma alteração em conexões existentes. Este procedimento consiste basicamente em realizar um inventário dos dispositivos finais conectados na rede. Pode ser feito com ou sem autenticação dos dispositivos finais e/ou utilizadores.

Fase 2. Autorização dos dispositivos finais: nesta fase são consideradas as politicas de acesso que neste caso são regras que definem os acessos e/ou restrições relacionadas ao acesso a rede. Esta fase inicialmente requer a autenticação para garantir que políticas de acesso às redes específicas possam ser aplicadas para cada tipo de dispositivo final e utilizador que se ligar a rede.

Fase 3. Autorização dos dispositivos finais com avaliação: nesta fase é feita a avaliação de todos os dispositivos finais, isto é, são validadas informações típicas como: a versão do sistema operativo, tipo de antivírus, *patches* de segurança, *firewall* interna, dentre outras informações, ao critério da instituição.

Fase 4. Autorização dos dispositivos finais com avaliação e remediação: nesta fase depois que as políticas de acesso a rede são aplicadas aos dispositivos finais individualmente, usando o resultado dos dados da avaliação. Os utilizadores são informados sobre essa avaliação e recebem a oportunidade de remediação caso não estejam em conformidade com as políticas de segurança estabelecidas.

1.6. Estrutura do Trabalho

O presente trabalho é composto por seis (6) capítulos, devidamente enumerados, e, ainda, por mais duas (2) secções não enumeradas referentes a bibliografia e anexos, respectivamente:

Capítulo I – Introdução

Neste capitulo é apresentada a contextualização, na qual se argumenta sobre os desafios do DTI na prestação de serviços aos clientes, em segunda perspectiva, é apresentado a formulação do problema, seguido da pergunta de partida, objectivos e justificativa da pesquisa.

Capítulo II - Revisão da Literatura

Neste capítulo apresenta-se uma síntese, referente ao trabalho e aos dados pertinentes a pesquisa, o enquadramento teórico de todos os aspectos relevantes para a realização do trabalho. Deste modo fez-se um levantamento teórico de todo material bibliográfico e documental existente e considerado cientificamente autêntico em relação aos sistemas de segurança da rede especificamente a solução de controle de acesso à rede corporativa.

Capítulo III - Caso de Estudo

Neste capítulo se apresenta os procedimentos tomados para garantir o controle e admissão dos dispositivos e dos utilizadores finais do NBP durante o acesso à rede corporativa. São explicados os métodos de segurança empregues pelo DTI, os constrangimentos encontrados e a proposta de solução.

Capítulo IV - Desenvolvimento da solução proposta

Neste capitulo, após a apresentação clara e precisa do problema, dá-se a solução proposta para que possa resolver os constrangimentos anteriormente identificados.

Capítulo V: Discussão dos Resultados

Neste capítulo apresenta-se os resultados dos estudos realizados e o impacto que a solução criou quando testada e comparada com o estado anterior, através da revisão da literatura e do caso de estudo (relação entre a teoria e factos).

Capítulo VI: Conclusão e Recomendações

Neste capítulo apresentam-se a análise dos dados e a interpretação dos resultados, focando-se na verificação do cumprimento dos objectivos, inicialmente, propostos para se obter um sistema lógico de controle de acesso à rede interna. No caso de incumprimento ou deficiência de algum objectivo, deixou-se recomendações para que sejam melhoradas nas próximas pesquisas relacionadas com o assunto em estudo.

2. Capítulo II – Revisão da Literatura

Neste capítulo pretende-se fazer um enquadramento teórico em torno dos assuntos ligados ao tema. Sendo assim mostrou-se conveniente abordar sobre a rede de computadores, os protocolos que constituem um sistema de controle de acesso à rede, segurança da informação e do que se trata em um sistema de controlo de acessos em uma rede corporativa, de modo a evitar quaisquer ambiguidades.

2.1. Rede de computadores

O termo "Redes de Computadores" serve para descrever um conjunto de computadores conectados por um único meio. Uma rede de computadores consiste, basicamente, em interligar dois ou mais computadores com o objectivo de compartilhar dados. Esta conexão pode ser feita por meio de cabos de cobre, fibras ópticas, micro-ondas, ondas de infravermelho e satélite de comunicações. Existem vários tipos de redes, de várias formas, tamanhos e modelos. Geralmente elas estão conectadas a fim de criar redes maiores. A Internet é o exemplo mais conhecido de uma rede de computadores (TANENBAUM; WETHERALL, 2011).

Existem seis componentes básicos de uma rede de computadores, e entender esses componentes pode ser fundamental para ajudar a proteger a rede apropriada para seu uso tanto doméstico quando empresarial (HUGHES, 2013):

- **Interfaces de rede:** todo dispositivo em uma rede deve ter alguma forma de interface, que às vezes é chamada de NIC ("*Network Interface Card*", placa de interface de rede) e pode estar integrada à placa-mãe de um computador ou separada dela. A NIC é o componente que toma a informação do computador e a envia pelo cabo de rede ou pelo ar, no caso de uma rede sem fio;
- ***Hubs:*** Quando vários computadores são conectados em uma rede, eles se comunicam com um dispositivo central, chamado "*hub*". Esse componente é responsável por mover o sinal de rede de um cabo para outro. No caso de um "*hub*" básico, o sinal de um computador é enviado para todos os outros; cada NIC decide se a informação recebida é para ela, e a descarta em caso negativo;
- ***Switches:*** os *switches* são *hubs* inteligentes, pois podem criar tabelas que permitem saber qual computador está conectado a cada uma das portas. Com essa inteligência, um *switch* não transmite toda a informação para todos os outros computadores conectados a ele e, sim, apenas ao computador destino. A tecnologia de *switching* ajuda a reduzir o

congestionamento de uma rede e deve ser utilizada em redes de 10 (dez) ou mais computadores;

- **Roteadores:** os roteadores são *switches* inteligentes, pois são cientes da existência de outras redes (os *hubs* e *switches* são cientes apenas da rede à qual servem). Os roteadores são utilizados para conectar uma rede local (LAN – *Local Area Network*) com outra, muitas vezes através de grandes distâncias, usando portadoras de dados comerciais. Os roteadores podem actualizar a informação de encaminhamento automaticamente e detectar quando um caminho para uma rede não funciona e, nesse caso, acabam buscando outro caminho disponível;
- **Meios cabeados:** logicamente, nenhum destes dispositivos funcionará se eles não estiverem conectados uns aos outros, e isso pode ser feito por vários meios. O mais comum é utilizar cabeamento *Ethernet*, que é uma das várias categorias de cabeamento de par trançado não blindado UTP (*Unshielded Twisted Pair*, Par Trançado sem Blindagem). Quanto mais alta for a categoria do cabo (Cat5, Cat6, Cat7), maior será a largura de banda suportada pelo mesmo. Além disso, existe a fibra óptica, que é mais cara e usa luz *laser* ou *led* ao invés de pulsos eléctricos. As redes *wireless* (sem fio) se tornaram populares nas casas, pois são fáceis e baratas de montar. O meio de transmissão em uma rede sem fio é o ar, através do qual as NICs transmitem sinais de rádio que levam a informação;
- **Software:** O *software* é a inteligência que permite que todos os componentes funcionem juntos. Os *softwares* de rede mais populares de hoje usam o que se conhece como suíte de protocolos, ou pilha, TCP/IP (*Transmission Control Protocol/Internet Protocol*, Protocolo de Controle de Transmissão). A suíte é composta por camadas de *software*, tendo cada uma delas funções definidas. Embora o modelo OSI (*Open System Interconnection*) de 7 camadas (física, enlace, rede, transporte, sessão, apresentação e aplicação) seja o ponto de início das pilhas de rede, o modelo Internet possui 4 (quatro) camadas (enlace, Internet, transporte e aplicação) que combinam as do modelo OSI de uma forma particular. No entanto, ambas as pilhas trabalham com as mesmas regras, fazendo com que os sistemas de computadores heterogéneos possam comunicar-se uns com os outros, sem importar as diferenças no *hardware* ou no sistema operativo.

2.2. Componentes lógicos e protocolos usados em NAC

2.2.1. VLANs (Virtual Local Network)

Uma LAN (*Local Area Network*) inclui todos os dispositivos em um mesmo domínio *broadcast*, que funciona da seguinte forma: quando um dispositivo envia algum *frame* de *broadcast*, todos os outros dispositivos da LAN recebem uma cópia deste *frame* (BEGNAMI; MOREIRA, 2013).

A VLAN nada mais é que a segmentação de uma LAN, feita de forma lógica. As VLANs funcionam de maneira semelhante a uma LAN, mas a grande diferença é que cada VLAN possui seu próprio domínio de *broadcast*, diminuindo o tráfego de maneira significativa. Quando não se utiliza VLAN, o *switch* considera que todas as interfaces estão na mesma LAN. Com a utilização de VLAN, podem-se criar vários domínios de *broadcast* e colocar cada dispositivo em domínios distintos. É importante entender também que, quando a rede é plana, ou seja, quando não se utiliza VLAN, um grande problema de segurança ocorre, pois, os dispositivos da rede "enxergam" todos os outros dispositivos (BEGNAMI; MOREIRA, 2013).

Como se pode ver na Figura 1, existem duas VLANs, com dois dispositivos em cada uma, em apenas um *switch*.

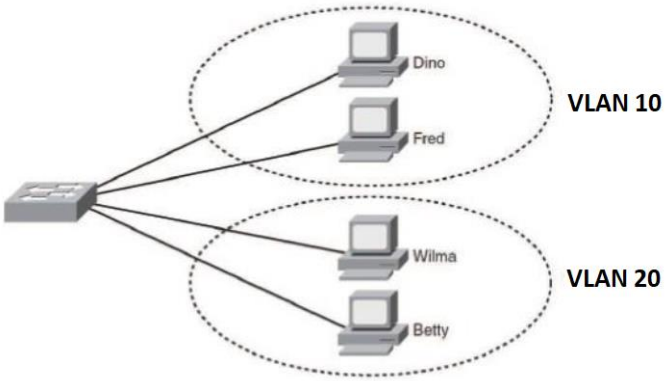

Figura 1: VLANs (Fonte: WENDELL et al., 2008)

Existem 3 tipos de níveis para VLANs: o nível 1 (VLAN por porta ou *port-based*), o nível 2 (VLAN por MAC ou *MAC-based*) e o nível 3 (VLAN por protocolo ou *protocol-based*) (BEGNAMI; MOREIRA, 2013):

- Nível 1: define uma VLAN para cada porta do *switch*;
- Nível 2: define uma VLAN para cada endereço MAC dos dispositivos. Este tipo de VLAN é muito mais flexível que a do nível 1, pois a VLAN é configurada independentemente da localização física do dispositivo;

- Nível 3: Define uma VLAN por protocolo, agrupando todos os dispositivos que utilizam o mesmo protocolo em uma mesma VLAN.

2.2.3. DHCP

Dynamic Host Configuration Protocol (DHCP) é um protocolo dinâmico de configuração de dispositivos (Droms, 1997) ou seja, é um protocolo baseado no modelo cliente/servidor que possibilita aos computadores em uma rede obterem configurações *Transmission Control Protocol/Internet Protocol* (TCP/IP), tais como: endereço IP, DNS, *gateway*, máscara de rede, entre outros de forma automática.

O protocolo DHCP é uma evolução do antigo protocolo *BOOTstrap Protocol* (BOOTP), este bastante utilizado em sistemas Unix. O BOOTP permitia a configuração automática de dispositivos em uma rede, como impressoras e máquinas finais.

No início da década de 90, a *Internet Engineering Task Force* (IETF) trabalhou para desenvolver um protocolo que superasse as limitações do BOOTP com adições de novos recursos, surgindo assim o DHCP. O protocolo DHCP está definido na RFC 2131 (Droms, 1997). O DHCP permite o envio de vários parâmetros por meio de um campo existente no cabeçalho do protocolo, de nome "*option*". Entretanto, é possível além de enviar as configurações, receber determinadas informações referente ao cliente, por exemplo, sistema operativo e outros.

Para se obter as informações do cliente como, por exemplo: o sistema operativo, é necessário que se active o uso da "*option code 61*", as opções são definidas na RFC 2132 (Alexander e Droms 1997). Através do uso deste parâmetro, é possível receber a informação do cliente referente ao sistema operativo em uso, essa técnica é conhecida como DHCP *Fingerprint*.

2.2.3.1 DHCP Fingerprint

DHCP *Fingerprint* é um identificador quase único para um determinado sistema operativo específico ou dispositivo (FingerBank, 2011). Através desse identificador é possível saber o sistema operativo do cliente. Esse identificador é a ordem em que o cliente solicita as opções referente às configurações, como *gateway*, máscara de rede, DNS, entre outras. Através dessa ordem de opções, é possível reconhecer o sistema operativo do cliente, pois cada sistema operativo possui um identificador único. Devido à difusão do protocolo DHCP, essa é a maneira mais simples de se obter informação referente ao cliente. Como definido na RFC 2132, obter a identificação do cliente é possível com o uso da opção "*Option Code 61 - Client Identification*".

Actualmente, existe um projecto (*FingerBank*, 2011) que disponibiliza esses identificadores que estão disponíveis através de um arquivo contendo vários identificadores, chamados de assinaturas

fingerbank. A maioria das ferramentas de análise de rede, como *sniffers* de rede, analisadores de protocolo, e soluções NAC fazem uso destas assinaturas.

2.2.4. IEEE 802.1X

O protocolo *Institute of Electrical and Electronics Engineers* (IEEE) 802.1X foi proposto pelo IEEE 802 LAN/WAN, e é utilizado em redes *Ethernet* como um mecanismo de controle de porta de acesso (*H3C Technologies* 2011). Quando é conectado um dispositivo à um activo de rede como por exemplo, um *switch*, e se esse *switch* estiver com o protocolo de autenticação 802.1x habilitado em sua porta física, o acesso dos recursos da rede só poderá ser feito após a autenticação. Deste modo é possível controlar quem pode aceder à rede de dados.

De acordo com (*H3C Technologies*, 2011), o funcionamento do protocolo é baseado na arquitectura cliente/servidor, nesse caso são definidas três entidades: cliente, dispositivo e o servidor, como demonstrado na Figura 2, a seguir:

Figura 2: EAPOL (Fonte: Cisco, 2011)

Cliente é uma entidade que busca acesso à LAN tal como um computador portátil. A autenticação 802.1X é accionada quando o cliente executa um aplicativo, denominado suplicante, capaz de fazer tal autenticação. Esse aplicativo deve suportar o protocolo *Extensible Authentication Protocol over LAN* (EAPOL).

Dispositivo geralmente é um equipamento de rede com suporte ao protocolo 802.1X e fornece portas de acesso físicas (redes cabeadas) e lógicas (redes sem fio – *wireless*) para clientes que pretendem aceder a LAN, como um exemplo de dispositivo é o *switch*.

A última entidade, é o **Servidor**, que fornece serviços de autenticação para os dispositivos. Esse equipamento normalmente executa *Remote Authentication Dial In User Service* (RADIUS). Esse serviço fornece a autenticação, autorização e contabilidade de serviços para os utilizadores. Esse sistema utiliza o *Extensible Authentication Protocol* (EAP) para trocar informações de autenticação entre o cliente e dispositivo e servidor de autenticação. Entre o cliente e o dispositivo, os pacotes EAP são encapsulados utilizando o EAPOL (EAP sobre LAN) para serem transferidos na rede.

Deste modo, entre o dispositivo e o servidor RADIUS, os pacotes EAP podem ser trocados em dois modos: EAP *relay* e EAP *termination*. No modo *relay*, os pacotes são encapsulados em EAP sobre RADIUS (EAPOR) no dispositivo, e então transmitidos pelo dispositivo para o servidor RADIUS, conforme a Figura 3. Entretanto no modo *termination*, os pacotes são terminados no dispositivo, e convertidos em pacotes RADIUS que com o *Password Authentication Protocol* (PAP) ou *Challenge Handshake Authentication Protocol* (CHAP) atribuído, são depois transferidos para o servidor RADIUS, conforme a figura 3 abaixo:

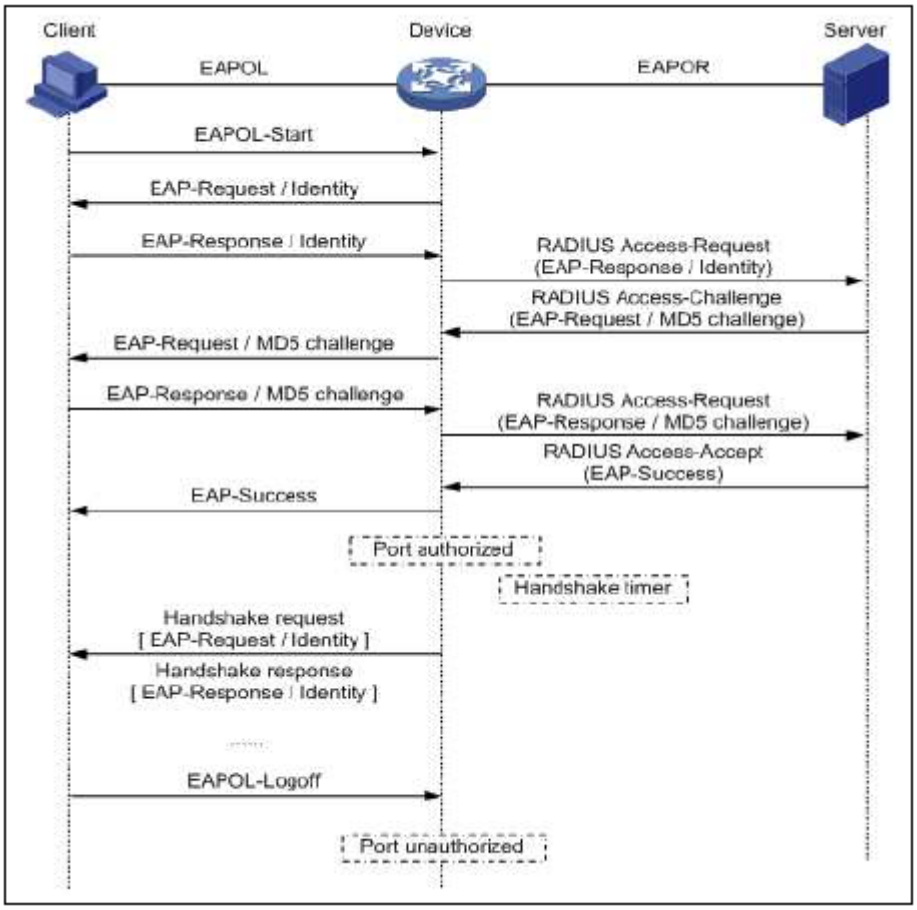

Figura 3: Troca de pacotes EAP *relay* **(Fonte: Cisco, 2011)**

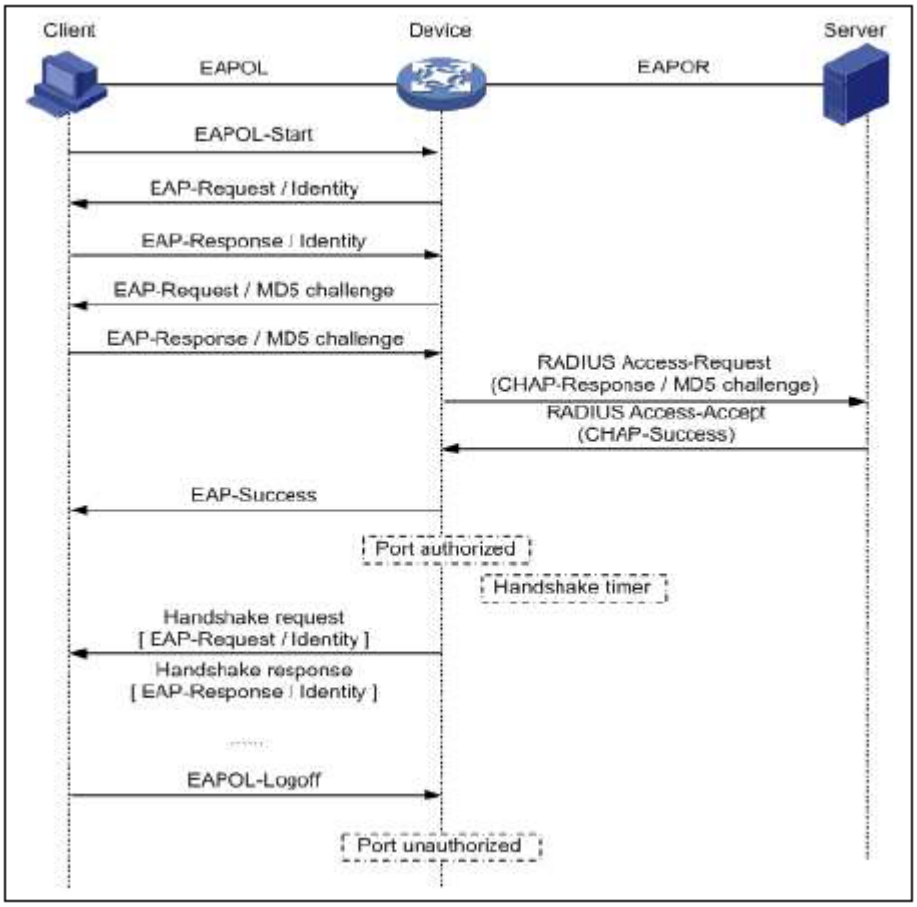

Figura 4: Troca de pacotes EAP *termination* **(Fonte: Cisco, 2011)**

Os conceitos básicos envolvidos no 802.1X são: a) porta controlada/porta não controlada; b) estado autorizado/ não autorizado; e c) direcção de controle.

a) Porta controlada e não controlada é quando um dispositivo fornece uma porta para os clientes acederem a rede, cada porta física pode ser considerada como duas portas lógicas, que seria uma porta controlada e uma porta não controlada. Todos os dados que chegam à porta física são visíveis para ambas as portas lógicas.

   Uma porta no modo não controlada está aberta em ambas as direcções de entrada e saída, isso permite a passagem de pacotes do protocolo EAPOL. Desse modo, o cliente pode enviar e receber pacotes de autenticação.

   Quando a porta está no modo aberta controlada, ela permite o tráfego de dados somente quando ela está no estado autorizado, ou seja, após autenticação.

b) Estado autorizado e não autorizado é a porta controlada que pode estar em qualquer estado, autorizado ou não autorizado. O estado depende do resultado da autenticação, com sucesso a porta fica no estado autorizado, senão, ela ficará no estado não autorizado.

De acordo com (*H3C Technologies*, 2011), o estado de autorização da porta pode ser controlado de três formas:

- Forçar a autorização - permite o acesso de clientes não autenticados;
- Forçar a não autorização - a porta fica no estado não-autorizada e negando todos os pedidos de acesso dos clientes; e por último,
- O modo *auto* – nesse modo a porta fica inicialmente no estado autorizada para permitir apenas pacotes EAPOL para permitir a autenticação de clientes, após a autenticação, o estado da porta passa para autorizada. Esta escolha é mais comum, pois permite que qualquer cliente utilize a porta para autenticação.

c) Controle de direcção indica o estado da porta controlada e não autorizada que pode ser configurada para negar o tráfego de e para o cliente ou apenas o tráfego do cliente.

2.2.5. Extensible Authentication Protocol

O *Extensible Authentication Protocol* (EAP) é um conjunto de padrões definidos pelo IETF e descrito na RFC3478 (Leelanivas, Rekhter e Aggarwal 2003) e revisado na RFC5247 (Aboba, Simon e Eronen 2008). Esse protocolo é comumente utilizado em redes sem fio (wireless) mas também pode ser utilizado para autenticar clientes em redes de cablagem estruturada. Ele padroniza a troca de mensagens para que o servidor autentique o cliente utilizando métodos de autenticação suportado por ambas as partes.

No EAP são definidos quatro tipos de pacotes: *request, response, success e failure* (JANET, 2011). Ao conectar um dispositivo em uma porta com o 802.1x habilitado, acontece o procedimento descrito na Figura abaixo.

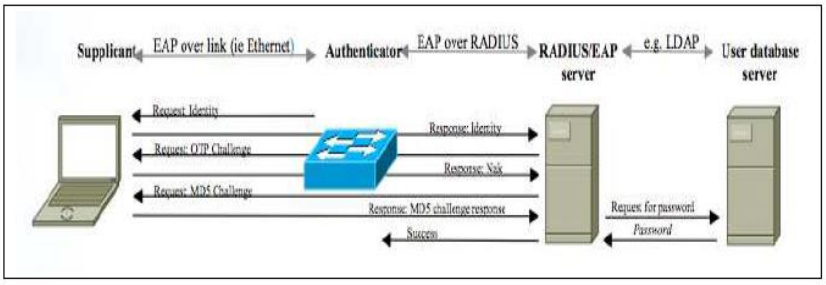

Figura 5: Procedimento de autenticação **(Fonte: Cisco, 2011)**

São especificados três tipos de autenticação: EAP (*MD5-Challenge, Generic Token Card* (GTC) e *One-Time Password* (OTP), e três tipos de não autenticação (*Identity, Negative Acknowledgement* (NAK) e *Notification*). O tipo *Identity* é utilizado pelo autenticador para solicitar ao suplicante o nome de utilizador. O NAK é utilizado pelo par (suplicante) para indicar

que o protocolo proposto pelo autenticador não é suportado, o autenticador pode tentar outro protocolo que seja suportado pelo suplicante. O tipo *Notification* é usado para retornar mensagem que será apresentada ao utilizador.

De acordo com (JANET, 2011), o EAP faz uso do *pass-through*, ou seja, permite que o autenticador repasse as respostas, usando o protocolo RADIUS para o servidor EAP. A partir desse momento, o servidor assume o papel de autenticador para o restante da sessão EAP, e tenta fazer a autenticação do suplicante, no caso da Figura 5, é utilizando uma base de dados centralizada para autenticação. Além dos três tipos de autenticação citados, também pode ser usado o *Transport Layer Security* (TLS), *Tunneled Transport Layer Security* (TTLS) e o *Protected Extensible Authentication Protocol* (PEAP). O EAP-TLS é baseado no TLS e usa um certificado de utilizador para autenticar o suplicante. O EAP-TTLS também utiliza o TLS, mas diferente do primeiro o EAP-TLS não utiliza um certificado de utilizador para fazer a autenticação. O PEAP também utiliza TLS, mas difere dos demais, pois só pode proteger outros tipos de EAP.

2.3. Segurança da Informação

A segurança da informação pode ser usada como se fosse uma arma estratégica em qualquer tipo de instituição e, também, é um processo de vital importância dentro de uma organização. A segurança da informação tem, como finalidade, administrar e proteger internamente a organização prevendo situações de risco. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos" (*BLUEPHOENIX*, 2008).

A informação está em toda parte, podendo ser armazenada em qualquer tipo de meio, tais como imagens, vídeos, papéis impressos, electronicamente, ficheiros, banco de dados e até mesmo em conversas entre os colaboradores. Porém, na grande maioria das vezes, a informação só tem a devida importância quando ela é perdida, destruída ou até mesmo roubada. "O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir" (DAVIS, 1997 citado por *BLUEPHOENIX*, 2008). O custo citado por Davis tem como significado apurar o valor das perdas tanto em dinheiro quanto na questão da reputação da organização, na confiança e nos outros valores que a organização mantém como princípio de sua missão como empresa.

Para que se possa implantar um projecto de segurança de informação dentro de uma determinada instituição é necessário, primeiramente, estabelecer conceitos, directrizes, mecanismo de segurança, políticas e procedimentos, ferramentas de protecção e autenticação, além da sua relação custo-benefício. É extremamente fundamental estabelecer o nível de segurança. Este nível de

segurança deve garantir que, cada funcionário só poderá aceder o conteúdo que lhe é permitido; por exemplo, um tesoureiro deve ter acesso apenas ao conteúdo de informação que faz parte do seu trabalho e não poderá aceder um dado que for de outro departamento que não tenha nenhuma relação com as funções as quais ele desempenha; Este exemplo citado demonstra que a informação deve estar segura e disponível apenas para quem está autorizado. "Em termos organizacionais, a informação tem um papel vital no que diz respeito à gestão, à organização e subsistência das entidades. O valor que a informação representa não é mensurável e a sua perda pode resultar em paragens, produtividade, desorganização e instabilidade" (*BLUEPHOENIX*, 2008).

Para que se garantam informações seguras é necessário se levar em conta alguns conceitos, tais como: riscos associados à falta de segurança; benefícios e custos de implementação dos mecanismos de segurança. Existem diversos riscos que podem ser associados à falta de segurança de informações. Sendo assim, todos os arquivos e dados podem ser perdidos, excluídos ou até mesmo roubados. Por exemplo, o ataque de pessoas com más intenções, tais como *hackers.* Eles podem explorar falhas em uma base de dados e conseguir se infiltrar dentro do sistema da organização. Após se infiltrarem dentro do sistema, eles podem ter acesso a todos os dados relacionados à empresa, bem como os dados de seus clientes. Desta forma, é necessário adoptar uma politica de segurança de informação, levando em conta não só esses factores, mas também factores naturais, tais como incêndios e inundações. (SÊMOLA, 2003).

Os benefícios esperados com a implantação de técnicas de segurança da informação são o de evitar vazamentos, fraudes, espionagem comercial, uso indevido, sabotagens e diversos outros problemas que possam prejudicar uma determinada empresa. A questão da segurança visa, também, aumentar a produtividade dos funcionários, por meio de um ambiente mais organizado, além de viabilizar aplicações críticas das empresas. Os custos de implementação dos mecanismos variam de acordo com o que a organização pretende implementar.

2.3.3. Ameaças, perigos e vulnerabilidades a segurança

Existem diversas formas de ameaças à questão da segurança nas empresas e organizações, tanto por causas naturais como por falhas humanas, como por exemplo, falhas de energia, sabotagem, vandalismo, roubo e incêndio, entre outras. Com o passar do tempo e aumento da necessidade de se usar a *Internet* dentro das organizações, outras preocupações começaram a ocorrer. O uso da *Internet* trouxe novas vulnerabilidades na rede interna. Como se não bastassem as preocupações existentes com espionagem comercial, fraudes, erros e acidentes, agora as empresas também precisam se preocupar com os *hackers*, invasões, vírus e outras ameaças que penetram através

desta nova porta de acesso. Os principais pontos de vulnerabilidade e risco vêm das redes de computadores, base de dados, sistemas de informações, sistemas de energia e comunicação. Sendo assim, é necessário aplicar alguns elementos básicos para que se possa ter uma maior segurança na Internet ou Intranet, sendo eles: *1) segurança na estação (cliente); 2) segurança no meio de transporte; 3) segurança no servidor e 4) segurança na rede interna* (SÊMOLA, 2003).

2.3.4. Políticas de segurança

Uma política de segurança é um instrumento importante para proteger uma organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida, neste contexto, como a quebra de uma ou mais de suas três propriedades fundamentais, que são: confidencialidade, integridade e disponibilidade. A política de segurança não define procedimentos específicos de manipulação e protecção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação (CERT.br, 2015).

Definir uma política de segurança é uma tarefa complicada, já que cada organização deve decidir que aspectos de protecção são mais importantes e, frequentemente, assumir um balanço entre segurança e a facilidade de uso. Tradicionalmente, a segurança de informação tem sido definida nos termos do acrónimo C.I.D. (do inglês C.I.A., *Confidentiality, Integrity, Availability*), que significa confidencialidade, integridade e disponibilidade (GOODRICH; TAMASSIA, 2013). Sendo assim, uma organização, visando garantir a segurança da informação, deve considerar (COMER, 2007):

- **Autenticidade:** garantirá que a mensagem ou arquivo é autêntico;
- **Disponibilidade:** indica se o serviço usado está ou não disponível para acesso;
- **Confidencialidade:** garante que as informações circulam de uma maneira sigilosa;
- **Integridade:** refere-se justamente à integridade da mensagem, se está realmente tudo inteiro, que nada foi corrompido.

A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples preocupa-se em impedir que pessoas mal-intencionadas leiam, ou pior ainda, modifiquem mensagens secretamente enviadas a outros destinatários. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas. A maior parte dos problemas de segurança é causada por pessoas que tentam obter algum benefício, chamar atenção ou prejudicar alguém (TANENBAUM; WETHERALL, 2011).

A sociedade precisa de mais profissionais de computação treinados em segurança, que possam defender e evitar, com sucesso, ataques contra computadores, bem como utilizadores treinados em segurança, que possam gerenciar de forma segura sua própria informação e os sistemas que usam.

2.4. Controle de acesso à rede (NAC, *Network Access Control*)

Nos últimos anos, o aumento do número de dispositivos 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. O NAC concede acesso à rede considerando factores como protecção *anti-malwares*, avaliação de *firewall* pessoal, autenticação de utilizador, localização e, até mesmo o horário (CZARNY, 2008; IREO, 2017).

Network Access Control (NAC) é uma abordagem unificada de tecnologias a fim de prover acções de segurança em uma rede de computadores, tais como: antivírus, detecção de intrusão e avaliação de vulnerabilidades, entre outras.

O conceito NAC é antigo, ou seja, surgiu desde os primórdios da telecomunicação, e foi idealizado através da patente de (Harris, Jackson e Petty 1987). Inicialmente, o padrão definido pelo *Institute of Electrical and Electronics Engineers* (IEEE) 802.1X também foi pensado como um NAC.

Existia uma disputa que gerava a falta de padronização quanto às soluções NAC, pois cada fornecedor/empresa implementava recursos e desenvolvia suas próprias soluções agregadas as suas próprias ferramentas, não estendendo para outros fabricantes, pois não existia um padrão a ser seguido como modelo, a fim de garantir compatibilidade entre soluções distintas.

Com o pensamento de acabar com a disputa das soluções NAC, o *Internet Engineering Task Force* (IETF) aprovou 2 padrões propostos pelo T*rusted Computing Group* (TCG), a partir de então considerados como dois padrões NAC a serem implementados pela indústria. Tais padrões estão definidos nas *Requests For Comments* (RFC) de números 5792 (Sangster e Narayan 2010) e 5793 (Sahita et al. 2010).

NAC pode ser definido como um conjunto de tecnologias de redes de computadores cujo objetivo é fornecer segurança e controle de acesso à rede, permitindo ou não o acesso de dispositivos. Esses dispositivos deverão estar em conformidade com as políticas de segurança e de controle definidas

pela organização, como, por exemplo, para antivírus com um nível de protecção, para configuração e para a actualização do sistema.

De acordo com (INTEROP LABS 2006) NAC é definida como sendo um controle genérico de acesso à rede que autentica e autoriza o tráfego. Tal controle de acesso simplesmente poderia ser implementado com o uso de políticas de acesso ou definindo regras na *firewall*. Como o NAC é um sistema de controle diferente, ele possui ferramentas disponíveis para fornecer o controle de acesso focado no utilizador, ao contrário da *firewall*, cujo controle é definido por regras aplicadas sobre o cabeçalho e/ou dados de um pacote Através do NAC é possível verificar a saúde dos dispositivos, ou seja, verificar se possuem vírus ou outras pragas virtuais, tais como *spyware* e *malware*. Um benefício importante ao se utilizar um NAC é a redução e a prevenção de ataques *zero-day* e outros similares (Edwards 2008).

Ataques *zero-day* são ataques que tentam explorar as vulnerabilidades de aplicativos que são desconhecidos pelos próprios desenvolvedores, ou seja, pelo próprio criador do aplicativo. Ataques *zero-day* podem destruir ou devastar uma rede, pois este é um ataque que explora uma falha desconhecida ao qual não existe um *patch* para a correcção do problema. Ao explorar uma falha desta magnitude, os atacantes podem entrar em uma rede para execução de código ou obter o controle total do computador da vítima.

2.4.3. Tipos de NAC

Segundo (Edwards 2008), pode-se apontar os seguintes tipos de NAC:

- ***Agent-based* (Com agente):** Este tipo de NAC conta com um *software* que requer ser instalado nos dispositivos dos utilizadores. Esta é uma abordagem simples, porém inflexível requerendo software especial a ser instalado;
- ***Agentless* (Sem agente):** Este tipo de NAC não requer a instalação de agentes nos dispositivos dos utilizadores.
- ***Inline*:** neste tipo de NAC, todo o tráfego do cliente passa pela ferramenta NAC. Esta abordagem pode gerar gargalos de *throughput* em redes maiores, além de aumentar os custos já que mais dispositivos podem ser agregados, também se agrega a função de firewall na qual se aplica as políticas de segurança na camada de rede.
- ***Out-of-Band*:** neste tipo de NAC é possível controlar uma infra-estrutura em escala geográfica, ou seja, em espaços físicos diferentes, desde que utilize a tecnologia certa, como a porta de segurança e que haja comunicação entre as redes.

2.4.4. NAC: Primeira Geração

As organizações estão a cada dia querendo controlar o acesso à rede com o uso de tecnologias que melhor atenda e proteja as redes e dados delas.

A primeira versão NAC trouxe um modelo defeituoso, pois não atendeu aos diferentes grupos que compõem as infra-estruturas tecnológicas em uma organização, pois crescia a demanda por proteger os dispositivos móveis2, por grandes quantidades de dispositivos, levando à falta de agilidade em termos de segurança. As ameaças e vulnerabilidades cresciam constantemente e o modelo NAC 1.0 (primeira geração) não conseguiu se adaptar as regras de negócio, pois, com o surgimento de novas ferramentas antivírus e *anti-malwares*, no geral, não foi possível agregar melhores gerenciamentos do NAC com estas. Desta forma, tornou-se uma ameaça e riscos aos dispositivos gerenciados. Devido aos riscos, poderia ocasionar em perdas de dados devastadores nos dispositivos gerenciados.

De acordo com (Manlio 2009), a geração NAC 1.0 falhou devido ao foco em bloqueio de clientes e a falta de agilidade, pois as ocorrências de ameaças novas e constantes, além das vulnerabilidades que surgiam se somavam a um problema muito maior em termos de segurança de uma organização. Desta forma, os fornecedores (fabricantes) de softwares lançavam constantemente
actualizações para detectar e limpar as ameaças. Como resultado desta situação, temos um problema de segurança, cujo modelo NAC de primeira geração não conseguiu acompanhar.

2.4.5. NAC: Segunda Geração

A segunda geração NAC ou NAC 2.0 surgiu devido à necessidade de uma abordagem para o ambiente de novas ameaças e vulnerabilidades, já que este mudava constantemente - surgimento de novas pragas virtuais. Desta forma, tornava-se necessário criar soluções com a capacidade de abranger as necessidades de segurança.

2.4.6. Funcionalidades do NAC

No mercado actual, existem inúmeras soluções NAC disponíveis. Diferentes empresas têm seus próprios objetivos de alto nível para definir o NAC. Não há uma padronização unificada do NAC. O NAC deve passar por três fases principais, uma fase de conscientização do NAC, fase de padrões (proprietários e não proprietários) e interoperabilidade de tais padrões.

Actualmente, o NAC está de alguma forma na segunda fase, a fase dos padrões. Como o foco actual do mercado NAC está em padrões, pessoas de várias empresas estão colaborando para

padronizar o NAC. A seguir estão um conjunto mínimo de funcionalidades que uma solução NAC pode ter:

- **Detecção do nodo**
- **Autenticação**
- **Avaliação da postura (ou Avaliação de segurança do dispositivo)**
- **Autorização**
- **Aplicação de politicas**
- **Quarentena**
- **Remediação**
- **Controle Pós-Admissão**

2.4.6.1. Detecção do nodo

A capacidade de detecção do nodo refere-se à detecção de um elemento acessando a rede protegida. Esta funcionalidade é muito importante para NAC, pois o NAC deve estar ciente de qualquer nodo ou elemento conectado à rede interna, para que possa interagir com as outras funcionalidades do NAC (como a autenticação, avaliação da postura, autorização, etc.)
Há várias maneiras de detectar um nodo que acede a rede corporativa. A detecção de nodos é feita em várias camadas, dependendo do método de acesso. Os métodos de acesso mais comuns são; LAN com fio, LAN sem fio, e VPN.

A seguir e apresentada as diferentes maneiras de detectar um elemento que se conecta à rede:

- O *Address Resolution Protocol* (ARP) precisa resolver um endereço IP para seu endereço MAC ou Ethernet. O nodo transmite um pacote de solicitação ARP. Esta transmissão pode ser detectada pelo equipamento NAC e, portanto, o elemento por este meio é detectado.
- Em uma configuração de controle de acesso baseado em porta usando o protocolo 802.1X, um *switch* pode detectar um elemento solicitando acesso à rede corporativa, pois o nó envia pacotes de solicitação do *Extended Authentication Protocol* (EAP).
- Alguns *switches* têm a capacidade de gerar alarmes do protocolo (SNMP), quando detectam um endereço *Ethernet* à ser registrado no *switch*.
- Um elemento pode ser descoberto quando o pedido do protocolo DHCP é transmitido pela rede para requisitar um endereço IP.
- Tráfego da camada de rede (como por exemplo: ICMP, IGMP, etc.) pode ser identificado quando passa por um determinado equipamento de rede como por exemplo um roteador.

- Através do uso de um suplicante ou *software* é um terminal, um nodo pode ser detectado. Portanto em configurações como 802.1X ou VPN, um *software* suplicante está presente no nodo que pretende ter a conectividade de rede. Sempre que, o nodo se conecta à rede protegida, este suplicante pode notificar ao NAC sobre a sua presença.
- *Appliances* (*hardware* especializado) também podem detectar um nodo, quando um tráfego específico é passado por eles, por exemplo, um firewall pode detectar o tráfego desconhecido quando estiver a passar por ela.

2.4.6.2. Autenticação

Um sistema NAC deve ser capaz de autenticar todo e qualquer utilizador que acede à rede interna e privada. Actualmente a autenticação envolve os seguintes métodos (alguns são os seguintes):

- *IEEE's 802.1X* padrão para redes com fios e rede wireless networks (baseado em EAP Types)
- *Dynamic Host Configuration Protocol (DHCP)*
- *IPSec (IP security)*
- *Transport Layer Security/Secure Socket Layer (TLS/SSL)*
- *Virtual Private Network (SSL VPN or IPSec VPN)*
- *Secure HTTP (HTTPS)*

2.4.6.3. Avaliação da postura

A avaliação da postura é uma funcionalidade exclusiva do NAC que é responsável por questionar a conformidade de um dispositivo. Em termos simples, é o procedimento de verificar a conformidade de um dispositivo. Conforme discutido no capítulo 1, na prática, os utilizadores estão sujeitos apenas a esquemas de autenticação, mas se a conformidade do dispositivo não é levada em consideração e esses *endpoints* estes podem ser os principais portadores de *malware*.

A avaliação da postura é um procedimento de execução de vários testes em um dispositivo terminal para coletar observações (ou medições) e relatar esses dados aos servidores de políticas para avaliar o nível de conformidade da máquina. No contexto da avaliação de postura podemos considerar "*compliance*" como uma palavra abstrata, ele pode ser composto de várias especificações. Por exemplo, para:

- Verificar o número de versão do *software* instalado em um dispositivo terminal (por exemplo: Sistema operativo, antivírus, *browser*, etc.);
- Verificar a presença de patches atualizados;

- Coletar e comparar o resultado das verificações (*scan*) do antivírus ou *anti-spyware* com as políticas pré-definidas;
- Coletar arquivos contendo assinaturas para *firewalls* ou sistemas de prevenção de intrusões;
- Coletar e verificar a lista de aplicações permitidas na rede interna;
- Validar certificados digitais;

2.4.6.4. Autorização

Quando um utilizador está conectado à rede protegida (depois de passar pela etapa de autenticação e avaliação de postura, e é considerado compatível), depois, o NAC verifica todas as permissões de acesso do utilizador aos recursos residentes na rede interna. A política é definida com base na identidade e medidas de avaliação de postura. A etapa de autorização geralmente é implementada pelo sistema AAA. Os protocolos usados para AAA são RADIUS, DIAMETER, TACACS+, etc.

2.4.6.5. Aplicação de políticas

A aplicação de políticas é a função por meio da qual o NAC impõe políticas definidas em máquinas terminais. O sistema AAA avalia a política para a máquina (que está se conectando à rede privada) e encaminha essas decisões para o aplicador de política ou pontos de aplicação (onde a política pode ser aplicada). Exemplo de cenários de acesso são; acesso é negado, acesso total é concedido, encaminhamento para a quarentena (discutido abaixo) ou acesso limitado, a decisão da política é aplicada de acordo.

As tecnologias usadas para aplicar a política são as seguintes:

- *Access Control List* (ACL, Lista de Controle de Acesso) define uma lista de permissões. A lista especifica as regras de acesso. A política avaliada é formulada na forma de ACL (s) e é/são encaminhados para o switch, roteador ou um dispositivo para aplicação dessas políticas;
- Virtual LAN (VLAN) também é usada para aplicação de políticas. De acordo com, às decisões formuladas, o utilizador está sujeito a uma determinada VLAN, disponíveis com recursos específicos da política (que são/são definidos pela política);
- *Firewalls* também podem impor políticas, com base no uso de diferentes parâmetros, por exemplo, uso de regras definidas, listas de URLs, portas permitidas, etc., dependendo da capacidade do firewall, a política é aplicada adequadamente. A *firewall* pode ser um

dispositivo que impõe a política na rede privada ou pode ser *firewall* que reside na máquina do cliente impondo políticas localmente.

2.4.6.6. Quarentena

A funcionalidade quarentena é um novo modelo associado à visão NAC. Um dos objetivos da tecnologia NAC é isolar os dispositivos não compatíveis com a rede privada rede (ou protegida), para que a rede permaneça segura e não afetada por não conformidade máquinas. Isso é feito por uma atribuição de VLAN a uma rede separada, ou um endereço IP temporário é atribuído que só pode comunicar (ou encaminhar mensagens) para recursos específicos, como configuração de quarentena.

2.4.6.7. Remediação

Quando um dispositivo é colocado em quarentena, o nodo torna-se parte da rede de quarentena (ou configuração de quarentena) e pode acessar um conjunto definido de recursos de correção. Os recursos de correção podem permitir que o utilizador se recupere de *status* de não conformidade para uma máquina em conformidade, para que o dispositivo possa ser reconectado a rede privada. A correção envolve a instalação de *patches*, atualização *software* antivírus, actualização de assinaturas para antivírus ou prevenção de intrusão sistema, ou habilitando um *firewall*, etc., dependendo dos requisitos de segurança.

Após a máquina adquirir todas as actualizações conforme exigido pela política, o dispositivo pode passar novamente pela etapa de avaliação de postura, se comprovada a conformidade, o dispositivo é admitido de volta à rede privada, senão colocado em quarentena novamente.

2.4.6.8. Controle Pós-admissão

O controle pós-admissão é semelhante à mitigação de ameaças. Quando um dispositivo é considerado em conformidade e conectado à rede privada; utilizadores, nós e suas sessões são monitorados quanto a qualquer actividade de *malware* ou violação de política. Se tal actividade for detectado, então o acesso do utilizador pode ser moderado por quarentena ou desligado da sessão. O controle pós-admissão funciona de maneira semelhante à funcionalidade de Sistemas de Prevenção de Intrusão (IPS). O controle pós-admissão define os procedimentos para mitigar ameaças de recursos legítimos.

2.4.7. Componentes do NAC

Os componentes envolvidos no processo de controle de acesso à rede são identificados abaixo:

- Cliente
    - Cliente com agente
    - Cliente sem agente
- Pontos de aplicação
- Servidores de políticas
- Rede de quarentena
- Servidores de remediação

2.4.7.1. Cliente

Um cliente é um dispositivo que solicita acesso à rede privada. Existem duas categorias de tais clientes que são específicas para a tecnologia NAC; um tipo de cliente inclui *software* de terminal executado neles e é conhecido como cliente com agente. Na segunda categoria de clientes, não há *software* instalado nestes dispositivos, e é chamado cliente sem agente.

- Um dispositivo cliente com um agente compatível com NAC ao solicitar acesso à rede privada, este agente pode sentir a requisição de conexão e pode realizar avaliação de postura antes de qualquer conectividade. Em outro caso, o NAC pode detectar um dispositivo solicitando acesso à rede protegida e pode interagir com o agente para obter informações de postura.

  O *software* do agente é responsável por conduzir a avaliação da postura. Agente pode por si só ou pode colaborar adicionalmente com outro *software* de segurança pacotes (específicos para aplicações de segurança como antivírus, *firewall*, etc.) para colectar a postura do dispositivo (discutido em 2.4.6.3). Mais adiante, o agente encaminha essas observações colectadas para o(s) servidor(es) de políticas. Esses servidores são responsáveis por avaliar a conformidade do dispositivo e, consequentemente, a política é aplicada nos pontos de execução. O agente também pode colaborar com aplicativos de segurança para controle pós-admissão (discutido acima em 2.4.6.8). O cliente com agente também pode actuar como um ponto de imposição (agindo como uma *firewall* baseada em dispositivo).
- Quando um cliente sem agente se conecta à rede, o NAC pode determinar que não há nenhum *software* de terminal instalado no dispositivo. O NAC pode instanciar um diálogo

com este cliente tornando possível que baixe e instale o *software* do agente. E terminado este processo, o cliente actuará como um cliente com agente.

2.4.7.2. Pontos de Aplicação

Os pontos de aplicação, ou seja, de fiscalização em uma plataforma NAC são de grande importância, pois os clientes comunicam-se com esses pontos para poder aceder a rede privada. Portanto através destes pontos, um sistema NAC tem controle sobre os dispositivos finais e, portanto, pode assumir acção específica para a aplicação da política. A seguir estão descriminados os diferentes pontos de aplicação e ou/fiscalização na configuração do NAC:

- *Switch*
- Roteador
- Equipamento VPN (servidor ou dispositivo)
- *Firewall*
- Servidor de aplicação
- Cliente com agente

    - Um *switch* de rede pode impor políticas ao nível da porta de acesso (camada 2), que é possível através do padrão 802.1X do IEEE para LANs com e sem fio. Alguns *switches* têm a capacidade de definir ACL pela qual o tráfego pode ser controlado.
    - Um roteador pode implementar ACLs pelas quais pode moderar o tráfego e aplicar a política ao nível da camada IP (camada 3).
    - O equipamento VPN (servidor ou dispositivo) usado na configuração remota também pode ser utilizado para moderar o acesso à rede privada. Como esses são os pontos a partir do qual as máquinas remotas interagem para se conectar a rede privada. O software de VPN instalado na máquina também pode impor políticas limitadas.
    - A tecnologia de *firewall* também pode ajudar a moderar o acesso à rede interna definindo regras de acordo com a política da instituição. *Firewalls* podem impor políticas na camada de aplicação ou na camada de rede monitorando os pacotes que passam através de uma sub-rede e pode colaborar com outros pontos de fiscalização, como *switch* ou roteador para maior segurança. Os clientes com agente também podem se comunicar com uma *firewall* para impor uma política. Por

exemplo, o *software* do agente pode detectar uma violação da política e relata a uma *firewall* que pode aplicar uma política de acordo.

- A categoria de servidor de fiscalização abrange todos os tipos de dispositivos de serviço que têm a capacidade de impor uma política de acordo com seu projecto função. Por exemplo, se considerarmos um servidor DHCP que é responsável para alugar endereços IP, pode liberar um endereço IP em uma violação de política, e mais adiante pode colaborar com um *switch*, roteador ou *firewall* para a aplicação de políticas. Da mesma forma, um servidor de concessão de certificados pode invalidar um certificado em uma violação de política.
- O cliente com agente (suplicante) também pode actuar como um ponto de aplicação, como o *software* do agente varia em termos de funcionalidade. Em uma política de violação pode não permitir que o cliente se comunique com a rede privada. Este *software* pode ter a funcionalidade de uma *firewall* (baseada em dispositivo) e pode se comunicar com uma *firewall/IPS* na rede para aplicação de políticas.

Dado o exposto acima, podemos identificar três classificações de aplicação, conforme ilustrado na figura abaixo:

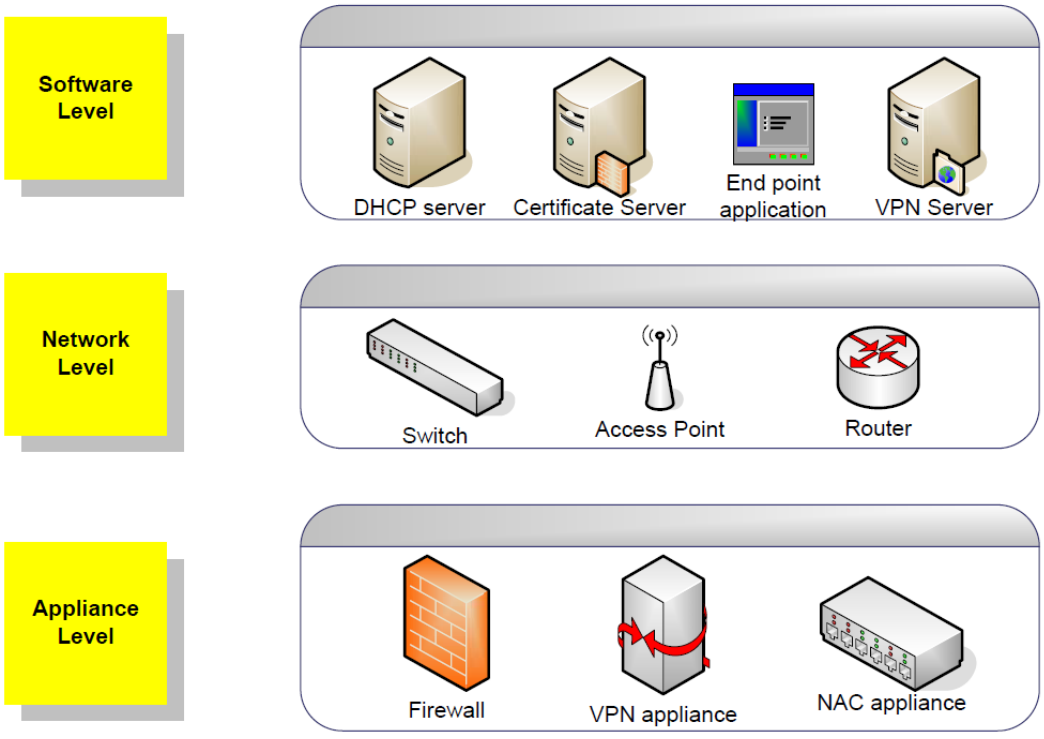

Figura 6: Níveis de aplicação de politicas (Fonte: Hasham, 2007)

2.4.7.3. Servidores de Politicas

Os servidores de política são responsáveis por administrar as decisões de controle de acesso. Um servidor de política é um servidor central que está envolvido na definição, configuração e gerenciamento das políticas de segurança da rede interna e privada. Na prática, um servidor de políticas é uma máquina que suporta a arquitectura de Autenticação, Autorização e Contabilidade (AAA) e geralmente implementa serviço de RADIUS.

Os servidores de política colectam o resumo dos testes de conformidade executados em um dispositivo final (referido na etapa de avaliação de postura 2.4.6.3) e relacionar esses resultados com as políticas de segurança predefinidas, para determinar as decisões de controle de acesso e direccionar essas decisões para pontos de execução para aplicação de políticas. Na prática, para controle de acesso robusto, os servidores de políticas também podem interagir com servidores de políticas, especializados para um determinado domínio de segurança.

2.4.7.4. Rede de Quarentena

Uma rede de quarentena é uma rede separada com segurança reforçada onde os dispositivos em quarentena residem. Dentro desta rede, um dispositivo pode se comunicar com um conjunto de recursos limitados que incluem principalmente os servidores de remediação, servidor DHCP, etc. Uma máquina permanece na rede de quarentena quando o apresenta um estado fora de conformidade. O principal objectivo da rede de quarentena é manter a rede interna protegida tanto quanto possível e isole as máquinas afectadas de forma eficaz.

2.4.7.5. Servidores de Remediação

Os servidores de remediação, ou seja, correcção são os recursos que ajudam os clientes que se encontram em quarentena a recuperarem o seu estado para conformidade. Portanto, essas máquinas podem se conectar novamente a rede interna. Os servidores de correcção podem actualizar automaticamente ou manualmente *software* dos dispositivos, sistema operativo, antivírus, instalação de *patches*, assinaturas para *software* de detecção de intrusão, etc.

2.4.8. Fluxo do NAC

A Figura 7 a seguir apresenta o fluxo típico de informações trocadas durante o processo do NAC:

1. O utilizador tenta conectar-se à rede interna.
2. O NAC detecta a presença de um dispositivo (detecção de nodo), e solicita os dados do cliente para o controle de admissão (autenticação e avaliação de postura).
3. O utilizador fornece os dados de controle de admissão aos componentes do NAC (*switch*, roteador, servidor, etc.).
4. Os componentes de rede encaminham esses dados para o servidor de política para as decisões de controle de acesso.
5. O servidor de políticas autentica o cliente (autenticação) e envia os dados de postura para o servidor de políticas.
6. Servidor de políticas que é ou são específicos para um aplicativo de segurança, verifica os dados de postura e retorna sua recomendação para o servidor de política.
7. O servidor de políticas estabelece as políticas de acesso para o cliente e envia dados de imposição para as partes de imposição da rede (autorização).
8. Entidades de execução impõem a política e respondem ao cliente sobre a política (aplicação de políticas); seja permitido, negado ou colocado em quarentena.
9. Com base nas decisões políticas, o cliente está sujeito a rede interna ou a rede de quarentena.

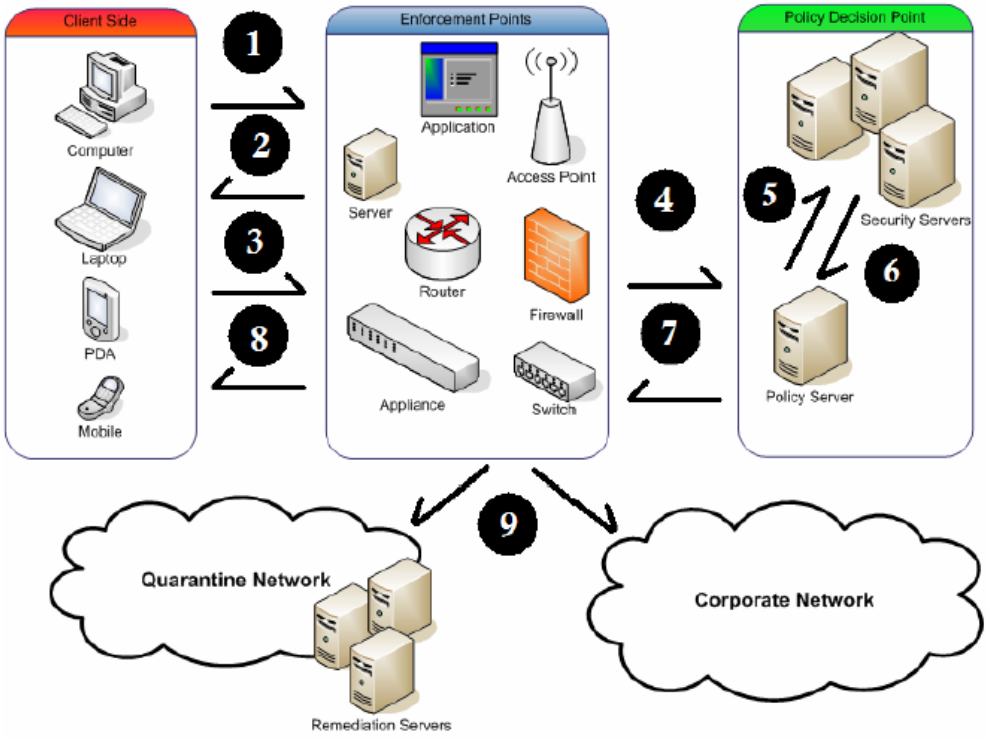

Figura 7: Fluxo de mensagens básico em um paradigma do NAC (Fonte: Hasham, 2007)

2.5. Análise comparativa de diferentes tecnologias de NAC

O conceito da tecnologia *Network Access Control* (NAC) é recente sendo uma nova iniciativa em gênero de segurança de rede. O NAC é composto por diferentes componentes e tecnologias emergentes variando de várias entidades de *hardware* e *software*. De acordo com a pesquisa *Forrester*, cerca de 40% das empresas começaram a adoptar iniciativas NAC em 2006 e cerca de 52% das empresas indicaram a necessidade de garantir o controle de acesso em todas as redes meios: com fio, sem fio e acesso remoto.

Há uma grande necessidade de padronização e interoperabilidade do NAC. As empresas precisam proteger seus investimentos em infra-estrutura de rede. De forma a aderir aos padrões, esses investimentos podem ser utilizados de forma eficiente com a inovação do NAC. Sem padrões, o mundo NAC é um amálgama de tecnologias e continuará a ser um obstáculo para as empresas adoptá-lo. A seguir estão os principais problemas que são obstáculos para a ampla adoção do NAC:

- A presença de inúmeras plataformas torna o mercado NAC confuso. Todas empresas estão oferecendo sua solução com um conjunto específico de funcionalidades e com uma arquitetura única. Alguns estão aderindo a um conjunto de padrões e alguns estão seguindo

padrões proprietários. Ninguém está fornecendo uma solução completa do NAC com todas as funcionalidades necessárias, mas apenas um subconjunto de funcionalidades.

- Actualmente, o NAC está em fase de padronização. Mas apresenta uma fraca interoperabilidade entre suas peças funcionais e arquitetônicas. Tal obstrução bloqueia o cliente com a abordagem de um determinado fornecedor para NAC. Como soluções que não são interoperáveis, os clientes ficam sem escolha, ou eles têm que seguir o mesmo fornecedor ou têm que descartar sua infra-estrutura existente para substituí-la pela configuração do fornecedor, que é quase impraticável e resulta em grande perda financeira. Os clientes precisam de garantia que seus investimentos sejam seguros e sejam melhor utilizados.
- **Questões de investimento:** A tecnologia NAC introduz novos elementos à infra-estrutura de rede. Algumas plataformas aproveitam de infra-estrutura, alguns requerem a introdução de novas entidades com substituição de equipamentos de rede existentes, resultando em investimentos pesados.

  As empresas devem avaliar sua motivação para o NAC, que inclui os potenciais custos/benefícios, como gestão e instalação de novo equipamento levanta preocupações monetárias. Para determinar o retorno do investimento (ROI) de uma solução de segurança é uma tarefa difícil, antes da adopção do NAC as empresas devem avaliar o custo envolvido na instalação de elementos arquitectônicos e funcionais do NAC.

2.5.3. Tabela comparativa de tecnologias NAC

Tabela 1. Estudo comparativo das funcionalidades de algumas tecnologias do NAC

Funcionalidades	Tecnologias			
	ForeScout Technologies - Counter ACT	Aruba Networks - HPEClearPass	Juniper Networks Inc. - Juniper UAC	Cisco Systems - Cisco ISE
Protocolo de conectividade à rede	SNMP	802.1X / DHCP	802.1X / DHCP	Usa o protocolo 802.1x / SNMP / DHCP
802.1X	Sim. Limitado	Limitado	Sim. Limitado	Sim
Third party devices	Sim	Sim	Sim	Sim
SAML	Não	Limitado	Limitado	Sim
TACACS+	Não	Limitado	Não	Sim

Visibilidade dos dispositivos	Sim	Sim	Sim	Sim
Visibilidade das aplicações	Sim	Não	Sim	Sim
Visibilidade e controle de dispositivos IOT	Sim	Sim	Sim	Sim
Visibilidade da rede	Sim	Sim	Sim	Sim
Serviços para visitantes	Limitado	Sim	Sim	Sim
Bring Your Own Devices (BYOD)	Limitado	Limitado	Limitado	Sim
Serviços MDM	Sim	Sim	Sim	Sim
Serviços de localização	Não	Não	Sim	Sim
Postura e verificação de comportamentos anómalos	Sim. Limitado	Sim. Limitado	Sim. Limitado	Sim
Quarentena	VLAN, ACL	VLAN, ACL	VLA.N, ACL, Agente	VLAN, ACL, Agente
Auto remediação	Sim. Limitado	Sim. Limitado	Sim. Limitado	Sim
Threat centric NAC	Sim	Não	Não	Sim
Rapid threat Containment	Sim	Sim	Sim	Sim
Integração API	Sim	Sim	Sim	Sim
Gateway de *internet* com Segurança de rede	Não	Não	Não	Sim
Politicas baseadas em grupos	Sim	Não	Não	Sim

Fonte: Elaborado pelo autor (2022)

Tabela 2: Estudo comparativo da arquitectura de algumas tecnologias de NAC

Arquitectura	Tecnologias			
	ForeScout Technologies - Counter ACT	Aruba Networks - HPEClearPass	Juniper Networks Inc. - Juniper UAC	Cisco Systems - Cisco ISE
Plataforma	*Appliance / Software*	*Appliance / Software*	*Appliance*	*Appliance / Software*
Pontos de aplicação ou fiscalização	*Switch* com 802.1X, *Access point* com 802.1X *VPN Server / Appliance*	*Switch* com 802.1X, *Access point* com 802.1X	*Switch* com 802.1X, *Access point* com 802.1X *Juniper Firewall*	*Switch* com 802.1X, *Access point* com 802.1X *VPN Server / Appliance*
Tipo de implementação	*Inline / Out of band*	*Inline / Out of band*	*Inline firewall, switch out of band*	*Inline / Out of band*
Métodos de aplicação de politicas	802.1X	802.1X	802.1X IPSec SSL VPN	802.1X IPSec SSL VPN DHCP

Após a análise comparativa de diferentes tecnologias de NAC, para melhor auxiliar no entendimento sobre os fornecedores desta tecnologia, foi indispensável recorrer a mais informação sobre como funciona o mercado tecnológico mundialmente, e para tal o quadrante mágico da Gartner foi imprescindível para obter esta informação, visto que a Gartner é uma empresa líder em pesquisa e consultoria em tecnologia, com uma equipe de analistas especializados em segurança de rede e tecnologias de NAC. As avaliações da Gartner são bem respeitadas na indústria e podem ajudar a identificar as tecnologias mais avançadas e eficazes disponíveis no mercado.

A comparação de tecnologias de NAC da Gartner pode fornecer uma visão geral das funcionalidades e recursos oferecidos por diferentes fornecedores de soluções de NAC, de forma ajudar a determinar quais tecnologias são mais adequadas para uma rede corporativa, com base nas necessidades específicas de segurança e controle de acesso.

Figura 8: Quadrante mágico da tecnologia NAC (Fonte: Gartner, 2014)

As funcionalidades e a arquitectura das tecnologias de NAC, foram representadas de acordo com os objectivos que se pretendem alcançar com o sistema proposto, uma vez que existem várias tecnologias de controle de acesso, as funcionalidades devem assentar-se no que o sistema proposto deve oferecer. Segundo (NAC COMPARISON, 2007) é importante notar que algumas soluções de NAC omitem a funcionalidade de autenticação, e utilizam apenas o método de identificação em combinação com a avaliação para determinar se o dispositivo ou utilizador deveriam estar na rede. Conforme a comparação feita, a funcionalidade de controle de acesso do dispositivo baseado em portas 802.1X, a postura e a auto remediação que são uma das funcionalidades principais para a resolução dos problemas identificados na pesquisa do presente trabalho, constatou-se que a tecnologia Cisco ISE apresentou maior robustez em relação as funcionalidades referenciadas, sendo por essa razão que esta foi a tecnologia seleccionada como proposta de solução do presente relatório.

3. Capítulo III – Caso de Estudo

3.1. Novo Banco Popular SA

O NBP é uma instituição de crédito e sociedade financeira mais antiga a desempenhar as suas operações em Moçambique. Actualmente conta com um total de 55 balcões e 1.265 colaboradores espalhados pelo vasto território nacional (2018, O País). O Banco possui uma infra-estrutura tecnologia vasta e com diversos tipos de dispositivos que se ligam à rede interna da instituição.

Segundo a estrutura organizacional, compete ao Departamento de Tecnologias de Informação planejar, padronizar e quando, couber, executar as acções para manter a qualidade e disponibilidade dos sistemas de informação, assim como os serviços da instituição garantindo a consistência, segurança e confiabilidade das informações geradas na instituição; difundir e fomentar soluções de TICs e novas tecnologias para o desenvolvimento da instituição.

O DTI tem como responsabilidades e subdivisões:

- A manutenção dos serviços do Banco Popular S.A. como: E-mail institucional, sistemas institucionais, entre outros; O gerenciamento e a segurança de informações que trafegam pela rede do NBP e pela manutenção dos servidores (computadores) hospedados no Data Center do NBP, além de sua importante participação, como membro, no Comitê de Segurança da Informação da NBP, com propostas de políticas de segurança em TI.

O Departamento de tecnologias de informação é integrada pela Divisão de Segurança da Informação (DSI):

  - 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.

3.2. Descrição da situação actual

Actualmente, a rede interna da instituição é acessível da seguinte maneira: O utilizador pelo dispositivo móvel ou computador, requisita o acesso à rede. A requisição é enviada ao *switch*, *Access Point* ou VPN, este faz uma conexão com o servidor DHCP, que retorna um endereço interno de rede privada para o dispositivo, e utilizador poderá introduzir as credenciais do domínio institucional permitindo deste modo o acesso à rede interna conforme ilustra a topologia de rede ilustrada na figura 9:

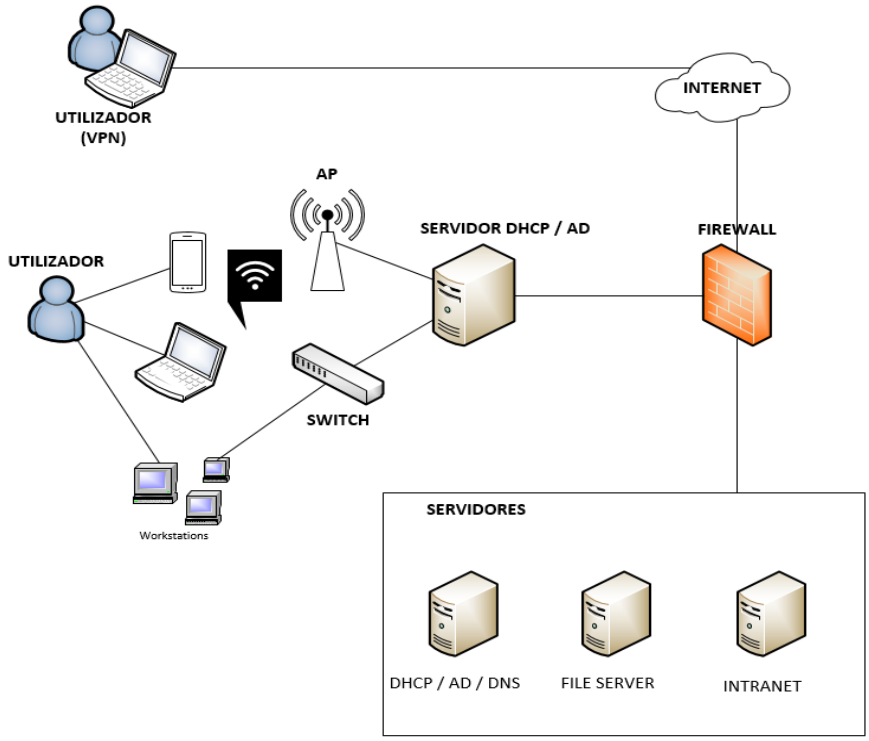

Figura 9: Cenário actual (Fonte: Elaborado pelo autor, 2022)

A instituição recebe diariamente, uma grande quantidade de utilizadores que necessitam de acesso à rede interna a todo momento e de qualquer lugar através do acesso físico e remoto, porém nem todos possuem vínculo institucional. Baseado nos descritos anteriormente, é possível identificar na actual infra-estrutura, problemas de segurança e rastreabilidade, pois denota-se que o sistema em produção apresenta limitações no processo de controle de acesso de utilizadores e de dispositivos para rede em questão.

3.3. Constrangimentos e limitações existentes no sistema actual

O processo actual de acesso à rede interna apresenta alguns constrangimentos e limitações que serão citadas nos pontos abaixo:

- **Visibilidade**

O actual sistema reconhece os utilizadores e dispositivos do domínio, mas não tem visibilidade e controle dos utilizadores e dispositivos que não fazem parte do domínio institucional, sendo que tanto os dispositivos como utilizadores que não são da instituição tem o acesso à rede interna e recursos existentes sem restrições.

- **Estado dos dispositivos**

O actual sistema não reconhece o estado de saúde de todos os dispositivos que se ligam a rede, embora exista um sistema de gestão de antivírus denominado SCCM, que consegue validar o estado de antivírus dos dispositivos que fazem parte do domínio da instituição e em casos de dispositivos externos, esta verificação do estado de saúde dos dispositivos não acontece.

- **Segurança**

O actual sistema não reconhece quem está a se ligar a rede interna e com que dispositivo, isto é, dispositivos não autorizados podem se conectar à rede corporativa e acessar recursos confidenciais; utilizadores mal-intencionados podem se fazer passar por utilizadores legítimos e obter acesso à rede corporativa; Dispositivos infectados por *malware* podem se conectar à rede sem serem detectados, permitindo que o *malware* se espalhe para outros dispositivos na rede;

3.4. Sistema proposto

A proposta de implementação de um sistema de controle de acesso à rede interna do NBP, leva em consideração a gestão de utilizadores e de dispositivos, 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 acesso aos sistemas da instituição, considera-se não somente o acesso, mas a informação e dados corporativos da Instituição na infra-estrutura, então em casos de incidentes de segurança da informação, seja possível, a instituição identificar o infractor e a este transferir a responsabilidade dos actos.

Conclui-se que, para chegar aos objetivos do trabalho é necessário realizar uma prova de conceito da solução, e aplicar a um grupo restrito de dispositivos e utilizadores de forma a aferir o funcionamento da solução.

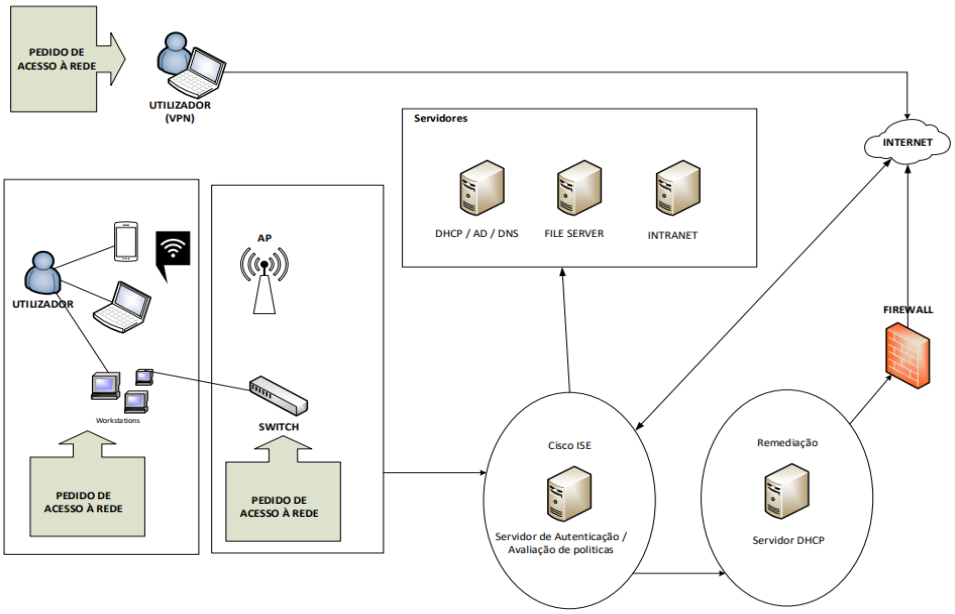

Figura 10: Cenário proposto (Fonte: Elaborado pelo autor, 2022)

3.4.1. Resultados do sistema proposto

Com a utilização do sistema proposto para o controle de acesso e admissão de dispositivos e utilizadores à rede interna, os resultados consistem em obter resposta as seguintes questões:

- **Quem está permitido a conectar à rede?**

  O sistema através de regras de autenticação definidas e configuradas, garante que, somente dispositivos e utilizadores que cumprem com os requisitos de autenticação definidos, são autorizados a conectar à rede interna. Nos casos em que um dispositivo ou utilizador não possui os requisitos são colocados em uma área de quarentena sem acesso à rede interna, até que cumpram com os requisitos para ganhar o acesso à rede.

- **Como os dispositivos são visualizados na rede?**

  O sistema através de regras de avaliação definidas e configuradas, oferece informações dos dispositivos como: se o *firewall* está activo e sendo executado? Se há algum *software* de antivírus instalado e com assinaturas actualizadas? Qual é o sistema operativo do dispositivo? Qual é a versão de *patch* do sistema? Existe uma conectividade com o agente? Quais *softwares* estão instalados no dispositivo? Quais processos e serviços estão a ser executados no dispositivo?

- **O que os utilizadores estão autorizados a aceder?**

  O sistema através de regras de autorização definidas e configuradas, garante que, os utilizadores autenticados a rede interna, tem acesso as informações especificas, isto é, cada tipo de utilizador tem acesso a informação de direito.

- **Onde os utilizadores devem ter o acesso?**

  O sistema através do endereçamento atribuído por DHCP, o perfil atribuído ao dispositivo e a identificação do utilizador, tem a capacidade de indicar a localização física dos dispositivos, reportando a seguinte informação, o local, o *switch* ou *access point* conectado e em que porta está conectado.

3.4.2. Constrangimentos resolvidos com o sistema proposto

Com a aplicação proposta os problemas anteriormente identificados são resolvidos, no que se pode observar o seguinte:

- **Visibilidade**

Maior visibilidade de dispositivos e utilizadores que se ligam a rede interna, através de diversas análises realizadas pelo sistema em colaboração com o agente instalado no dispositivo para determinar a identidade, classificação e postura do dispositivo. Em outras palavras a solução é capaz de identificar o sistema operativo de cada *endpoint*, seja computadores pessoais, *smartphones*, dispositivos como impressoras e inúmeros outros. Essa identificação automática permite a criação de regras de acesso baseadas também no tipo de dispositivo permitido na rede.

- **Estado do dispositivo**

O sistema através das políticas de conformidade antes que o dispositivo se conecte a rede interna, ele verifica se o dispositivo atende aos requisitos de segurança da rede, como a conformidade com políticas de segurança corporativa, requisitos de regulamentação e padrões de segurança (antivírus, *patches*, *firewall*, etc) e se o dispositivo atender aos requisitos de segurança e conformidade, o NAC concede autorização de acesso à rede interna. Importa referir que o NAC monitora continuamente o estado do dispositivo e pode bloquear o acesso do dispositivo à rede caso seja detectada uma violação de segurança ou uma mudança no estado de conformidade.

- **Controle**

O sistema permite o controle da rede de forma a limitar os acessos à recursos específicos, isto é, o acesso de um dispositivo não é restringido na totalidade, mas sim os recursos cruciais não permitidos por meio de uma combinação de políticas de segurança, tecnologias de autenticação e monitoria;

- **Segurança**

A solução mitiga os riscos de acesso não autorizado e de *malware*, faz o bloqueio de uma lacuna significativa na segurança da rede, negando o acesso à rede para dispositivos de utilizadores que não estão em conformidade com as políticas de acesso à rede interna. O agente do cliente NAC que executado em um computador ou no celular do utilizador garante que estes dispositivos conectados à rede tenham as actualizações de segurança mais recentes. A rede segregada de quarentena e remediação fornece uma linha final de defesa para manter os dispositivos comprometidos e não compactíveis fora da rede.

- **Rede de convidados (*Guest Network)* e BYOD**

A rede *Guest* é uma rede separada, normalmente com acesso limitado à *internet* e recursos de rede básicos, como impressoras compartilhadas e acesso Wi-Fi. Os utilizadores que se conectam a esta rede geralmente não têm acesso aos recursos da rede corporativa principal, como servidores de arquivos e base de dados. Em vez disso, são mantidos separados da rede corporativa para minimizar o risco de acesso não autorizado. O NAC é utilizado na rede *guest* para garantir que os utilizadores que se conectam à rede tenham sido autenticados e que suas actividades sejam monitoradas para detectar actividades maliciosas. Isso pode incluir políticas de acesso limitado e segregação de rede para impedir que utilizadores desconhecidos acessem recursos críticos da rede.

O BYOD é outra consideração importante no NAC, pois os funcionários podem trazer seus próprios dispositivos, como *smartphones* e *tablets*, para uso na rede corporativa. O NAC é usado para garantir que esses dispositivos estejam em conformidade com as políticas de segurança corporativa, como atualizações de *software*, configurações de segurança e aplicativos aprovados. Isso geralmente envolve a instalação de agentes de segurança em dispositivos BYOD para garantir que eles estejam em conformidade com as políticas da organização.

4. Capítulo IV – Desenvolvimento da solução proposta

A metodologia para o desenvolvimento da solução proposta segue o princípio apresentado no Capítulo I, que consiste na implementação de uma prova de conceito à um certo grupo restrito de dispositivos e utilizadores. Assim, são apresentadas detalhadamente as atividades desenvolvidas para a efetivação das fases relativas ao modelo de implementação do NAC.

4.1. Configuração do hardware

4.1.1. Servidor

A implementação e configuração da ferramenta foi realizada utilizando-se a tecnologia para virtualização, ou seja, fazendo uso de máquina virtual para a realização de todos os procedimentos, a fim de obter os resultados esperados pela proposta da ferramenta. A seguir, a configuração utilizada pela máquina virtual:

- Processador: Intel Dual Core de 3.0GHZ;
- Memória: 1,5 GB de RAM;
- Hard Disk: 30GB;
- Rede: 2 (duas) interfaces de rede, sendo uma para gerenciamento e outra para monitoramento, conectadas a rede numa conexão de 1Gbps cada.

4.2. Modelo da Topologia

Na Tabela 2, é demonstrado as informações propostas, referentes à topologia a ser implementada.

Tabela 3. Informação de rede

VLAN	Descrição	Cisco ISE	Rede	Interface
10	Gestão	10.10.10.1	10.10.10.0/24	Eth0
20	Quarentena	Modo *trunk*	192.168.1.0/24	Eth1
30	Telefones IP	Modo *trunk*	10.20.30.0/24	Eth1
40	Utilizadores	Modo *trunk*	10.20.40.0/24	Eth1
50	Impressoras	Modo *trunk*	10.20.50.0/24	Eth1
60	Servidores	Modo *trunk*	10.10.60.0/24	Eth1

Fonte: Elaborado pelo autor, 2022

A Figura 10 é uma representação gráfica da topologia apresentada na Tabela 2, e a seguir, uma breve descrição dos tipos de VLAN adoptadas para a implementação desta topologia:

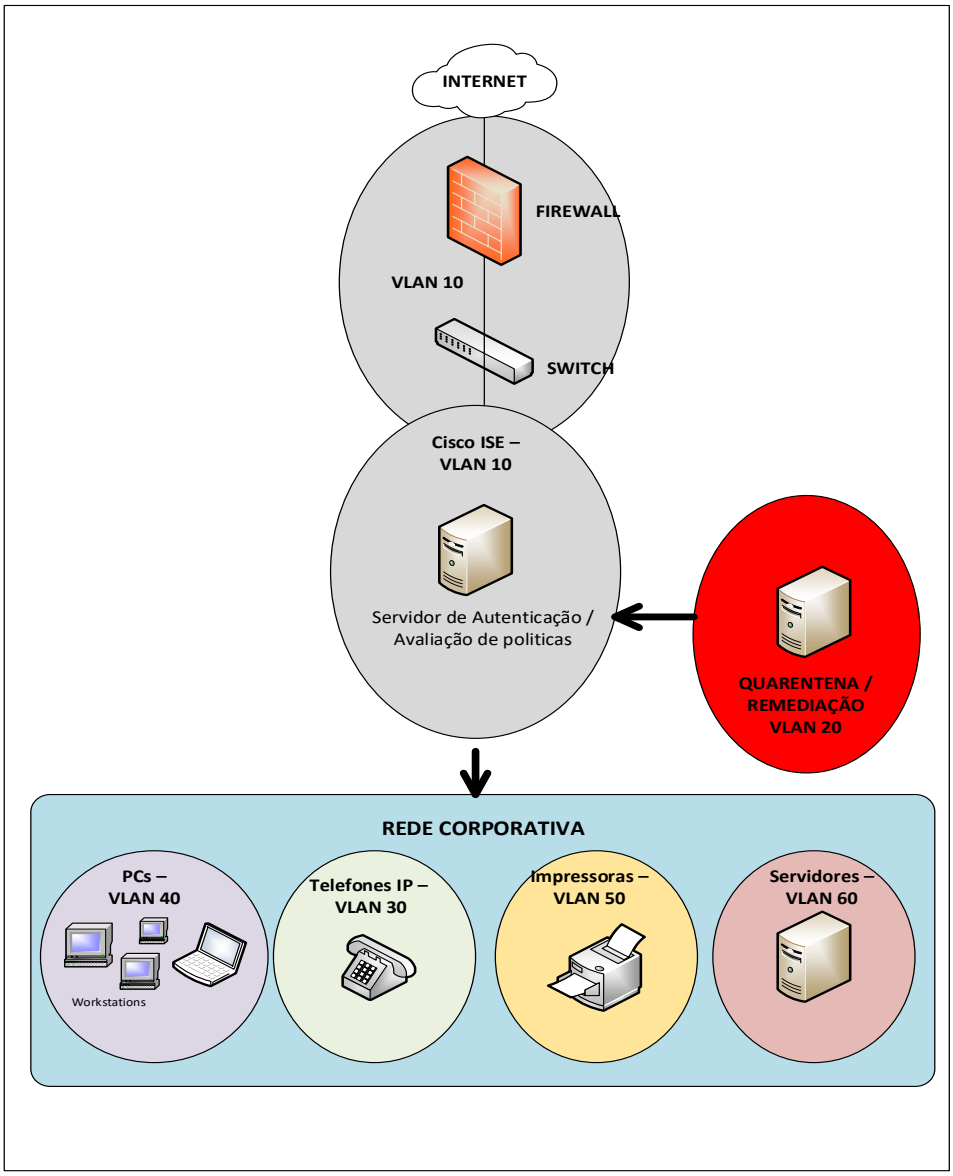

Figura 11: Topologia de rede (Fonte: Elaborado pelo autor, 2022)

- VLAN 10 - Gestão: é a VLAN utilizada para a gestão da ferramenta Cisco ISE aos *switches*, ou seja, é nesta que estão todos os dispositivos que o Cisco ISE acede;
- VLAN 20 - Quarentena: é a VLAN utilizada para isolar dispositivos que não estejam em conformidade, isto é, com problemas, vulnerabilidades, vírus, execução de software P2P. A fim de remediar estes dispositivos, ou seja, corrigir estes problemas, de forma automática ou manual;
- VLAN 30 – Telefones IP: é a VLAN dos telefones IP, considerada como uma rede normal pertencente a rede corporativa
- VLAN 40 – Utilizadores: é a VLAN dos utilizadores de um piso especifico, considerada como uma rede normal pertencente a rede corporativa

- VLAN 50 – Impressoras: é a VLAN das impressoras, considerada como uma rede normal pertencente a rede corporativa;
- VLAN 60 – Servidores: é a VLAN dos servidores, considerada como uma rede normal pertencente a rede corporativa onde estão alocados todos servidores com serviços como DHCP, CISCO ISE, AD, etc.

4.3. Configurações

O sistema operativo utilizado para a implementação e configuração da ferramenta Cisco ISE foi o *Community ENTerprise Operating System* (CentOS) 6. Durante o processo de inicio da instalação foi necessário fazer o *download* da imagem do ISE em formato. ova na página da Cisco e importar a imagem no servidor com o VMWARE *Workstation*.

Na configuração inicial do sistema são feitas configurações básicas do dispositivo a descrever: IP, máscara, NTP, DNS, *Hostname*. E de seguida o nome do administrador do sistema e a respectiva senha, o ISE de seguida realiza os testes de leitura e escrita de memória e inicia a criação da base de dados.

Finalizado este processo, é verificado um *prompt* de *login*, onde pode-se aceder ao sistema e ver toda a configuração inicial por linha de comando CLI e por interface gráfica GUI.

A instalação do Cisco ISE não será abordada nesta parte do trabalho, porém pode ser consultada a secção Anexo 1 para saber como instalar a ferramenta.

4.4. Configuração do *switch*

As configurações do *switch* podem ser realizadas de duas formas: pela porta de consola ou via acesso remoto usando *telnet*. Este último deve-se saber o endereço IP do equipamento. Através da porta de consola, é conectado um cabo serial na porta console do equipamento e a outra ponta do cabo deve ser conectada na porta serial do computador. Para aceder o *switch* será necessário um *software*, como por exemplo, o Hyper Terminal ou PUTTY

Será demonstrado a seguir dois modos de configuração do *switch* nomeadamente o modo de acesso e o modo com autenticação 802.1x.

4.4.1 Modo Accesso

As portas do *switch* ao serem configuradas em modo acesso, permitem ao ISE utilizar qualquer método de autenticação para o registro do utilizador, diferentemente do modo 802.1X (*port-security*), sendo obrigatório o uso de autenticação RADIUS ou TACACS. A seguir, será apresentando os comandos para a configuração do *switch* em modo acesso.

- **Criação de VLAN**

```
#Conf t
(config)#Vlan 10
(config)#Name Mgmt
(config)#Vlan 20
(config)#Name Quarentena
(config)#Vlan 30
(config)#Name TelefonesIP
(config)#Vlan 40
(config)#Name Utilizadores
(config)#Vlan 50
(config)#Name Impressoras
(config)#Vlan 60
(config)#Name Servidores
(config)#exit
```

vlan x - adiciona a VLAN, sendo x um número que pode variar de 1 à 4096.

- **SNMP**

SNMP deverá ser habilitado no *switch* para que este envie *traps* ao ISE ao detectar a mudança do status da porta, ou seja, *linkup* e *linkdown*.

```
snmp-server group NBPSNMPCampus v3 auth
snmp-server community NBPSNMPCampus RW
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.10.10.1 version 2c Snmp123 mac-notification
snmp-server host 10.10.10.2 version 2c Snmp123 mac-notification
```

- *snmp-server* - configura o snmp do *switch*;
- *snmp-server group* – define o grupo de segurança e a versão do SNMP;
- *snmp-server community* - define o *string* de acesso;
- *snmp-server host* - configura o IP que o *switch* enviará as *traps*;
- *trap* - configura o tipo de *trap* a ser activada.

Ao configurar as portas em modo acesso, elas devem ser configuradas em cada interface do *switch* onde estarão conectados os dispositivos finais. A seguir, os comandos a serem executados no *switch* para realizar as configurações, sendo x substituído por um número inteiro, ou seja, o número da porta do *switch* na qual se pretende configurar.

```
interface gigabitethernet 1/0/X
switchport access vlan 40
switchport mode access
switchport voice vlan 30
Exit
```

Configurando a porta do *switch* que se liga ao servidor ISE, este deverá ficar em uma porta como *trunk*, pois deve permitir que o tráfego das outras VLAN's cheguem ao ISE.

```
interface gigabitethernet 1/0/X
switchport trunk allowed vlan 20,30,40,50,60
switchport mode trunk
Exit
```

4.4.2. Modo 802.1x

No modo de autenticação 802.1x, se deve utilizar o método de autenticação RADIUS ou TACACS. As configurações que devem ser realizadas no *switch* para habilitar este modo consistem em configurar um *schema* RADIUS/TACACS, sendo que neste é informado o endereço IP do servidor RADIUS e a porta; configurar a *shared secret* a ser utilizada para a comunicação do *switch* e o RADIUS; informar que os *logins* serão sem o prefixo do domínio institucional, por exemplo, nbp/Test1; informar o domínio; activar o *schema* para este domínio; atribuir VLAN por *string*, ou seja, por texto; habilitar o domínio como sendo o domínio padrão a ser utilizado; e especificar o método de autenticação, além de activar a *port-security*, ou seja, segurança por porta.

- **Configuração global**

A seguir, os comandos necessários para realizar as configurações descritas anteriormente, a fim de habilitar o modo 802.1x no *switch*:

Configuração usando o RADIUS

```
radius server RADIUS-01
 address ipv4 10.10.10.1 auth-port 1812 acct-port 1813
 key 7 135747213F0116187A
!
!
radius server RADIUS-02
 address ipv4 10.10.10.2 auth-port 1812 acct-port 1813
 key 7 124B552426061E367B
!
!
aaa group server radius ISE-SERVER
 server name RADIUS-01
 server name RADIUS-02
 ip radius source-interface Vlan X
!
aaa authentication dot1x default group ISE-MAP
aaa authorization network default group ISE-MAP
aaa accounting update newinfo
aaa accounting dot1x default start-stop group ISE-MAP
!
aaa server radius dynamic-author
 client 10.10.10.1 server-key 7 00564335305619345E
 client 10.10.10.2 server-key 7 00564335305619345E
```

```
 auth-type any
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 10 tries 3
radius-server deadtime 15
```

Configuração usando o TACACS

```
!
aaa group server tacacs+ tacacs+
 server 10.10.10.1
 server 10.10.10.2
!
tacacs-server host 10.10.10.1 key 7 0351681E0F2B207E1F
tacacs-server host 10.10.10.2 key 7 0351681E0F2B207E1F
!
aaa authentication login default group tacacs+ local line enable
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
```

Ao configurar as portas em modo acesso, elas devem ser configuradas em cada interface do *switch* onde estarão conectados os dispositivos finais. A seguir, os comandos a serem executados no *switch* para realizar as configurações, sendo x substituído por um número inteiro, ou seja, o número da porta do *switch* na qual se pretende configurar.

```
interface gigabitethernet 1/0/X
switchport access vlan 40
 switchport mode access
 switchport voice vlan 30
 authentication host-mode multi-domain
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 Mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 dot1x max-reauth-req 5
 spanning-tree portfast
Exit
```

4.5. Descrição das fases de implementação do sistema proposto

4.5.3. Detecção e rastreamento dos dispositivos finais

O ISE monitora os atributos específicos e perfis dos dispositivos que se ligam a rede, recolhendo toda informação do dispositivo como sistema operativo, tipo de dispositivo, endereço IP através do protocolo MAB, 802.1X, e a identificação da classe DHCP, conforme se pode verificar na figura 12.

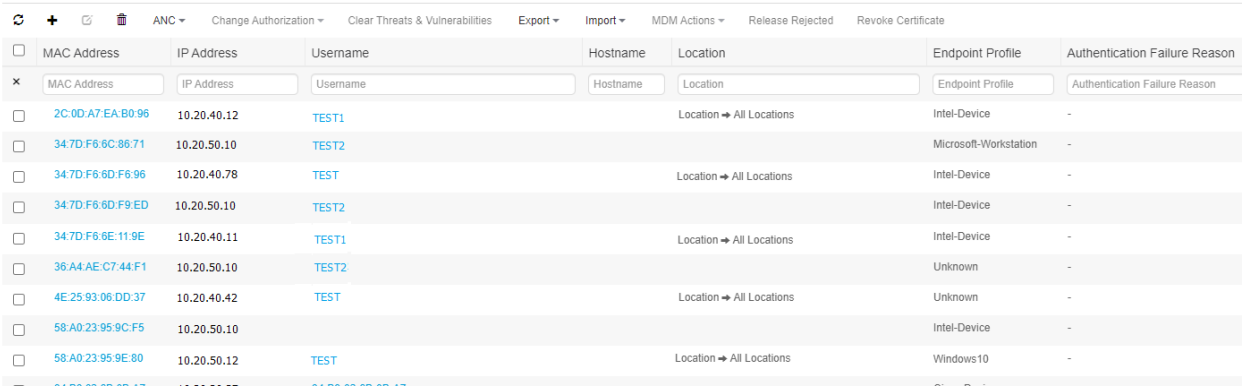

Figura 12: Dispositivos detectados pelo ISE (Fonte: Elaborado pelo autor, 2022)

Uma vez que os dispositivos são detectados e identificados, o NAC pode aplicar políticas de acesso à rede, como autorizar ou negar o acesso, com base nas informações colectadas sobre os dispositivos e utilizadores. O rastreamento contínuo dos dispositivos é essencial para garantir que apenas dispositivos autorizados permaneçam na rede e que as políticas de segurança sejam aplicadas correctamente.

A figura 13 exibe as informações de um determinado dispositivo por meio do seu MAC. É possível obter os dados dos registros de acesso, o endereço IP atribuído ao dispositivo, e os dados *fingerprint*, ou seja, informações exclusivas que identificam o dispositivo final (FINGERBANK, 2016).

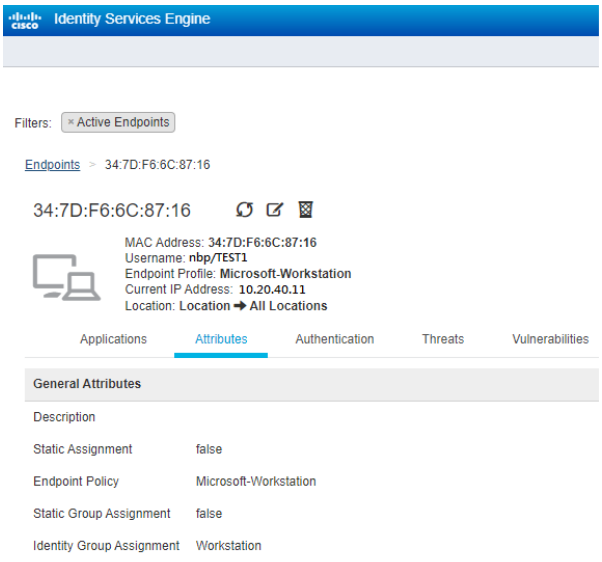

Figura 13: Interface com a informação do dispositivo ligado à rede interna

4.5.4. Autorização dos dispositivos finais

O ISE permite realizar a configuração de políticas de autorização, com base em requisitos acordados pela instituição, neste caso a autorização apôs a autenticação que é preconizada na tabela abaixo é somente para dispositivos e utilizadores que fazem parte do domínio institucional (AD SERVER) e dispositivos existentes na base de dados do ISE através do protocolo MAB.

Tabela 4: Regra de autenticação de dispositivos e utilizadores

Nome da regra	**Condição**	**Uso**	**Protocolos permitidos**
Wired - MAB	Wired_MAB	Internal Endpoints	MAB
Wired - Dot1X	Wired_802.1X	AD_SERVER	Dot1X

Fonte: Elaborado pelo autor, 2022

Abaixo a imagem retirada do ISE, que demostra a configuração de autenticação usando as condições de MAB e 801.X, e protocolos de segurança EAP-TLS como requisitos para autenticação a rede de dados.

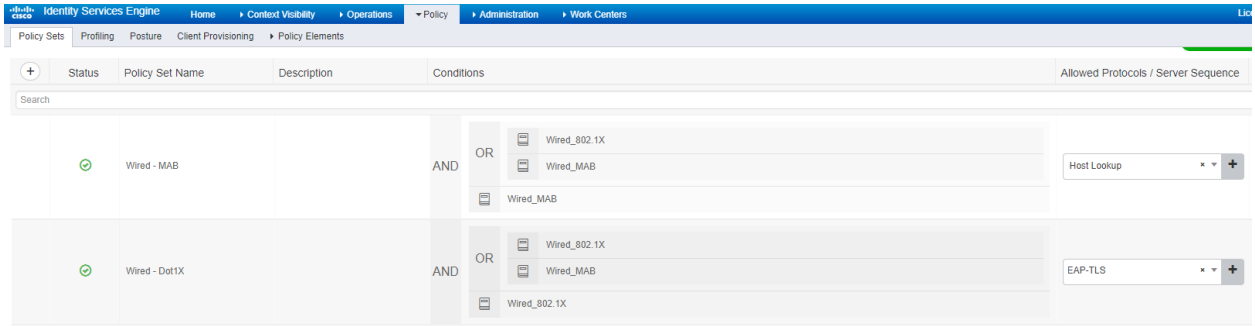

Figura 14: Interface com a configuração da regra de autenticação (Fonte: Elaborado pelo autor, 2022)

Tabela 5: Regra de autorização de dispositivos e utilizadores

Nome da regra	**Condição da regra**		**Protocolo permitido**	**Resultado**
NBP -IP-Phones	Endpoints LogicalProfile EQUALS IP-Phone		MAB	IP-Phone - Access
NBP -Computers	AD SERVER: ExternalGroups EQUALS bancomoc.mz/Users/DomainComputers		Dot1x with EAP-TLS	Workstation - Access
NBP -User-Unknwon	AND	AD SERVER: ExternalGroups EQUALS bancomoc.mz/Users/DomainUsers Session: PostureStatus EQUALS Unknown	EAP-TLS	User-Unknown
NBP -User-NonCompliant	AND	AD SERVER: ExternalGroups EQUALS bancomoc.mz/Users/DomainUsers Session: PostureStatus EQUALS NonCompliant	EAP-TLS	NonComplaint
NBP -User-Complaint	AND	AD SERVER: ExternalGroups EQUALS bancomoc.mz/Users/DomainUsers Session: PostureStatus EQUALS Complaint	EAP-TLS	User-Complaint

Fonte: Elaborado pelo autor, 2022

Abaixo a imagem retirada do ISE com a configuração de regras de autorização mediante aos seguintes requisitos pré-definidos.

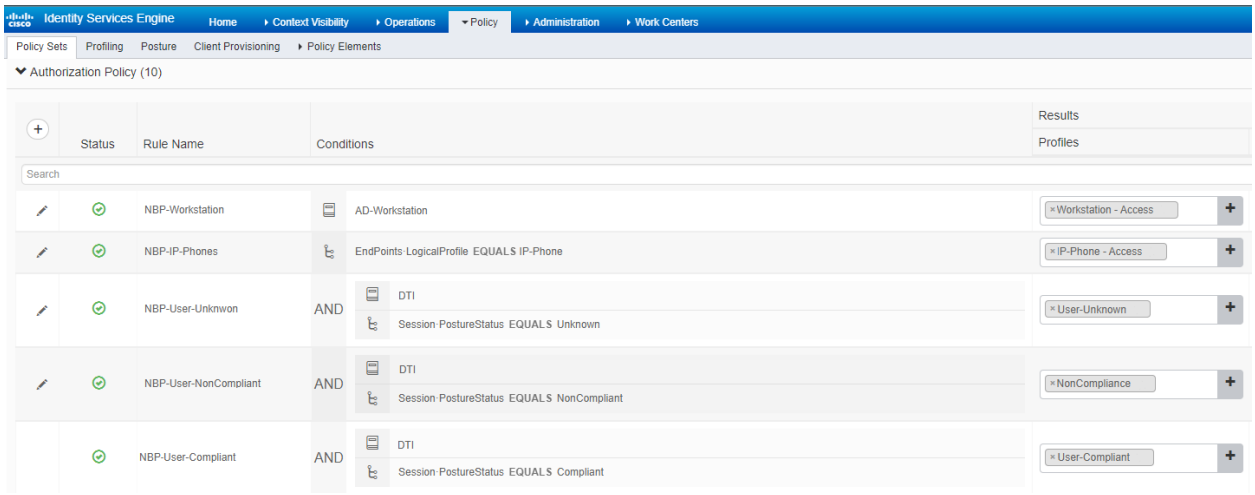

Figura 15: Interface com a configuração da regra de autorização (Fonte: Elaborado pelo autor, 2022)

4.5.5. Autorização dos dispositivos finais com avaliação

O ISE de forma a reforçar a segurança durante a pré-conexão, através de regras de autorização com avaliação de postura, permite através de um agente reforçar que somente dispositivos que cumpram com os requisitos pré-definidos tem acesso à rede, neste caso para efeitos de testes somente dispositivos com sistema operativo *Windows*, conforme atesta a imagem abaixo:

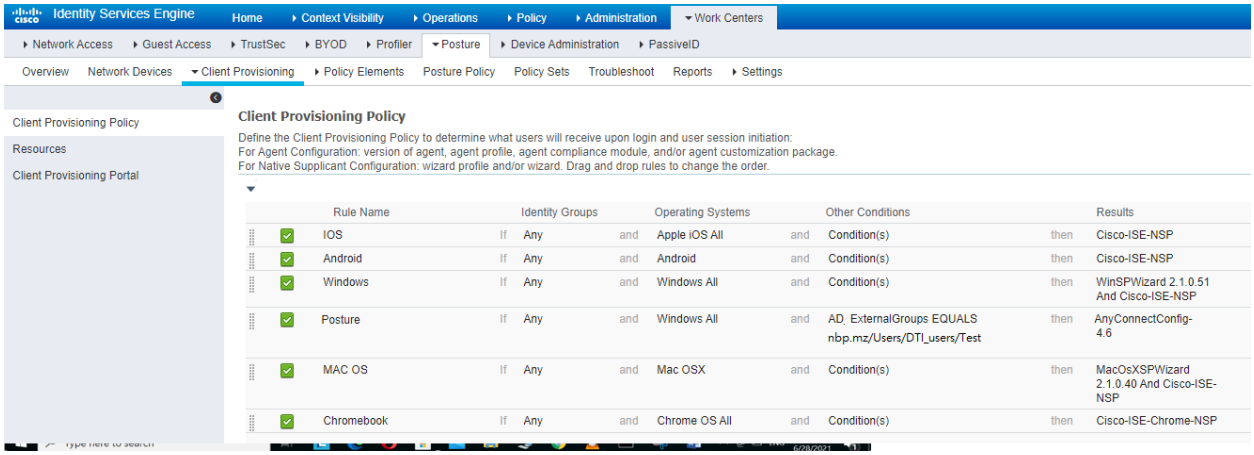

Figura 16: Interface de configuração da regra de avaliação (Fonte: Elaborado pelo autor, 2022)

4.5.6. Autorização dos dispositivos finais com avaliação e remediação

Na mesma regra de configuração da avaliação é possível adicionar mais requisitos para permitir o acesso à rede e a configurar a remediação que consiste em impor nos dispositivos os requisitos para acesso à rede, como por exemplo fazer a instalação de aplicações, bloquear o USB e dentre outros como demonstra a imagem abaixo:

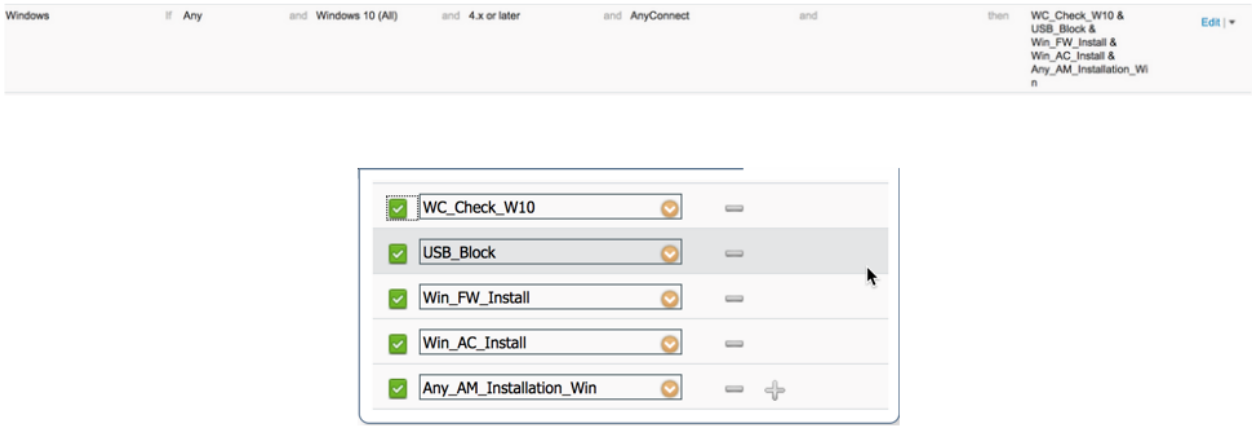

Figura 17: Interface de configuração da regra de avaliação com remediação (Fonte: Elaborado pelo autor, 2022)

4.6. Resultados obtidos do Sistema Proposto

4.6.1. Cenário de testes

Os testes com o ISE foram realizados em um ambiente isolado e de testes no Novo Banco Popular (NBP), tendo como participantes um computador, um telefone IP e uma conta de um utilizador de testes. A rede de teste foi propagada em um *switch* de acesso, em paralelo com as redes existentes no Banco. Importa referir que, as figuras apresentadas nesta parte do documento, foram retiradas do *log* de acesso ao Cisco ISE, e do computador utilizado para os testes.

4.8.1.1 Cenário 1

Neste cenário é feita a ligação de um computador que não pertence ao dominio da instituição, em um ponto de rede sem a configuração do NAC, isto é, no estado actual da infraestrutura.
Inicialmente as portas de ligações do *switch* aos dispositivos estão configuradas em modo acesso, sem nenhuma configuração de protocolo de autenticação.

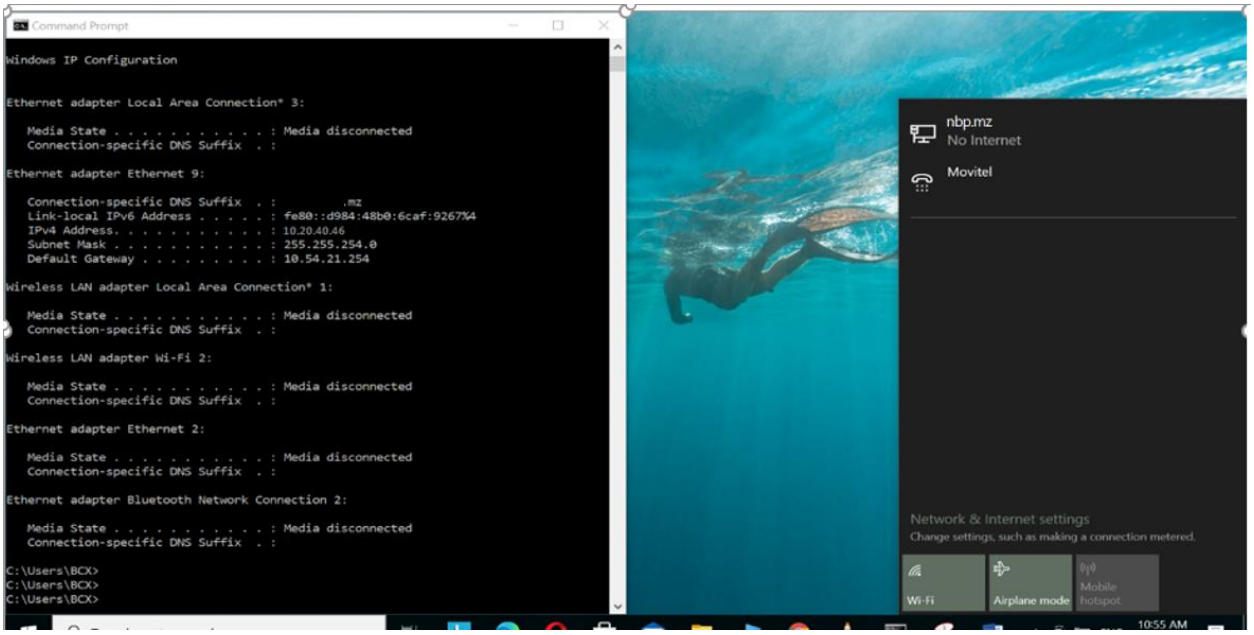

Figura 18: Imagem de um computador externo sem configuração do NAC à aceder a rede

Observação: verifica-se que o computador recebe um IP pelo DHCP e tem acesso a rede interna do NBP, sem ser feita nenhuma verificação e restrição de segurança no dispositivo.

4.8.1.2 Cenário 2

Procedeu-se com a ligação de um computador que não pertence ao dominio da instituição, em um ponto de rede contendo a configuração de protocolo de autenticação 802.1X.

Neste caso as portas de ligações do *switch* aos dispositivos estão configuradas em modo acesso, com a configuração de protocolo de autenticação 802.1x.

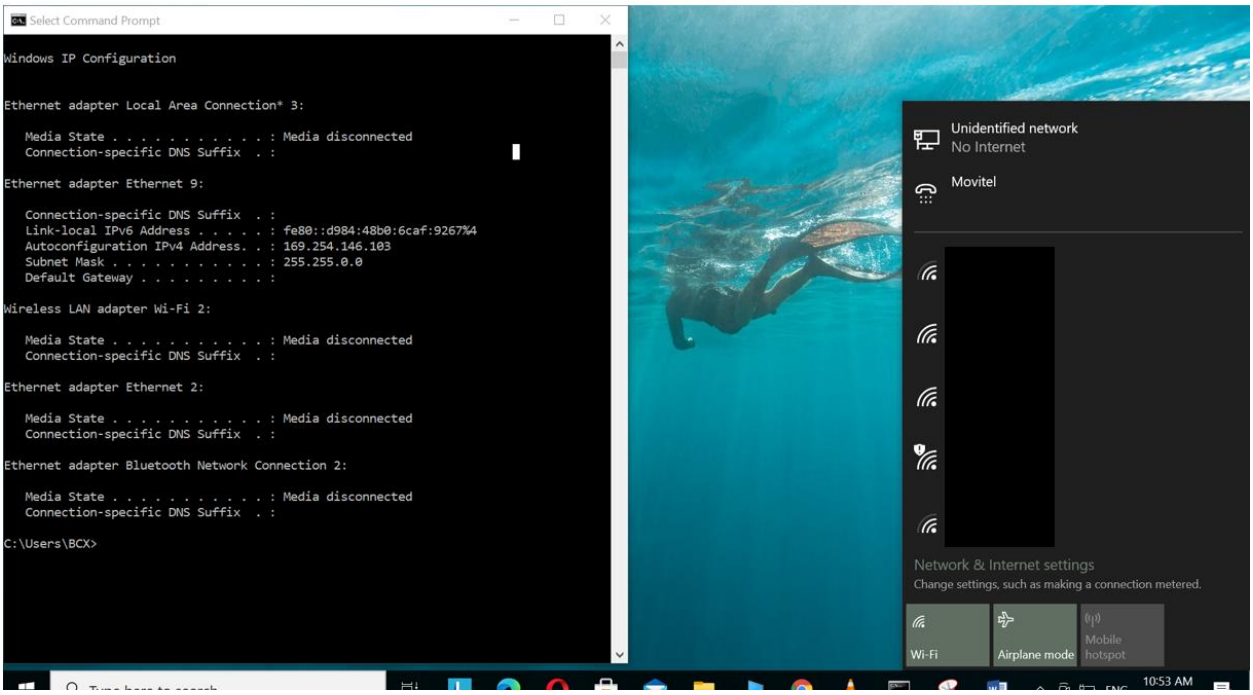

Figura 19: Imagem de um computador externo com configuração do NAC à aceder a rede

Observação: O computador não recebe nenhum IP e consequentemente não tem acesso à rede interna do NBP.

Abaixo o *log* no servidor ISE com a tentativa de acesso à rede sem sucesso.

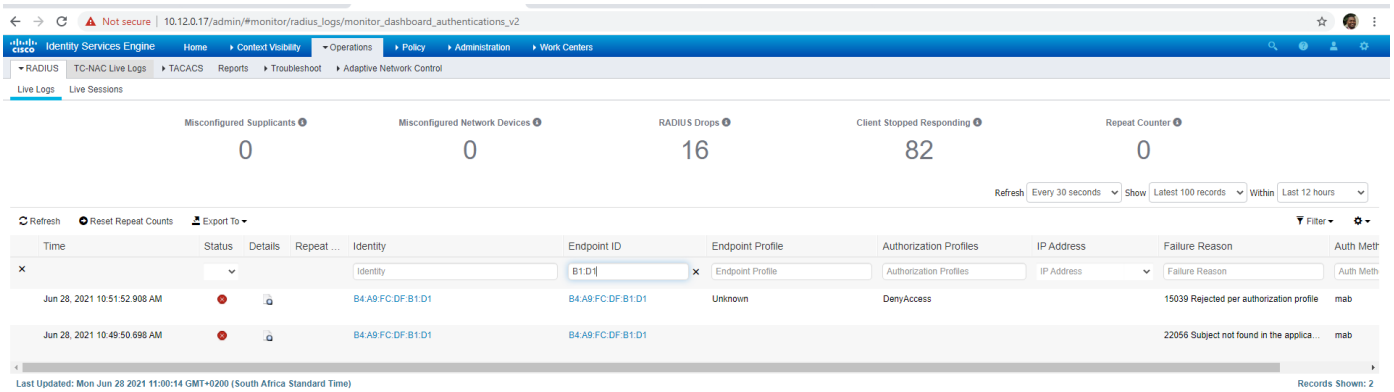

Figura 20: Interface com resultado da tentativa de acesso a rede por um computador não autorizado

4.8.1.3 Cenário 3

Neste cenário é feita a ligação de um computador que pertence ao dominio da instituição, com o agente *anyconct* instalado, e com a configuração do NAC na porta de acesso no *switch*. E conforme demonstra a imagem abaixo, apôs autenticar a rede é iniciado o processo de autorização onde e validade a conformidade do dispositivo e do utilizador atravees das regras AAA configuradas.

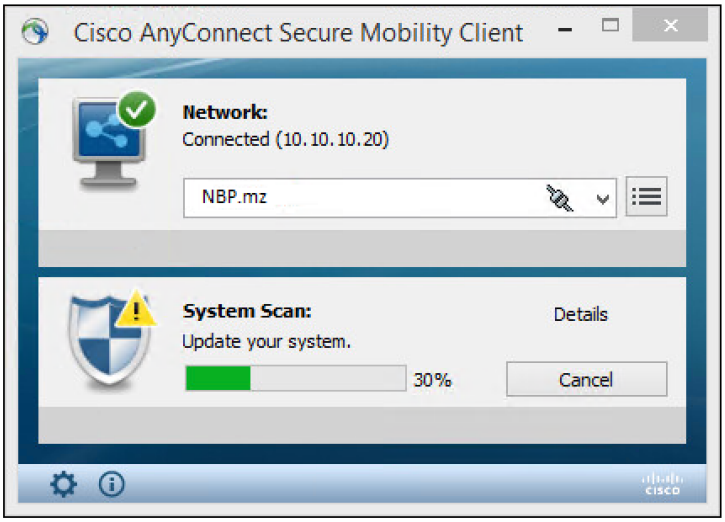

Figura 21: Interface do cliente no processo de avaliação da postura

Apôs validar a postura do dispositivo e do utilizador é garantido então o acesso a rede conforme atesta a figura abaixo:

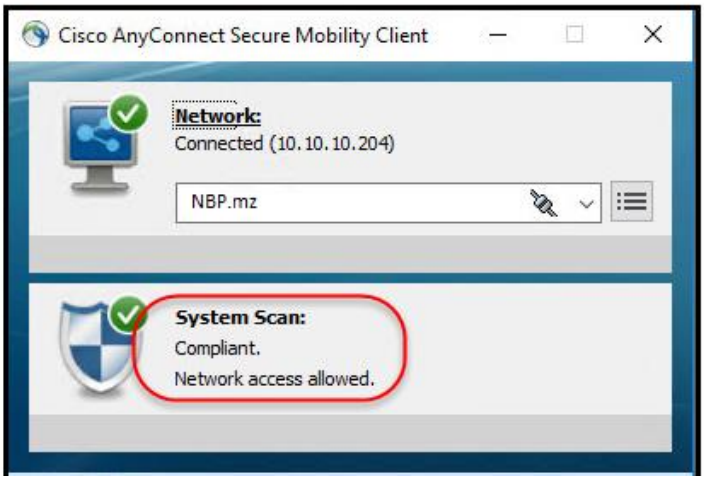

Figura 22: Interface do cliente apôs a avaliação da postura

A figura abaixo é do log no Cisco ISE contendo a informação dos dispositivos que obtiveram o acesso à rede de dados apôs passaram por todas etapas de autenticação, e autorização.

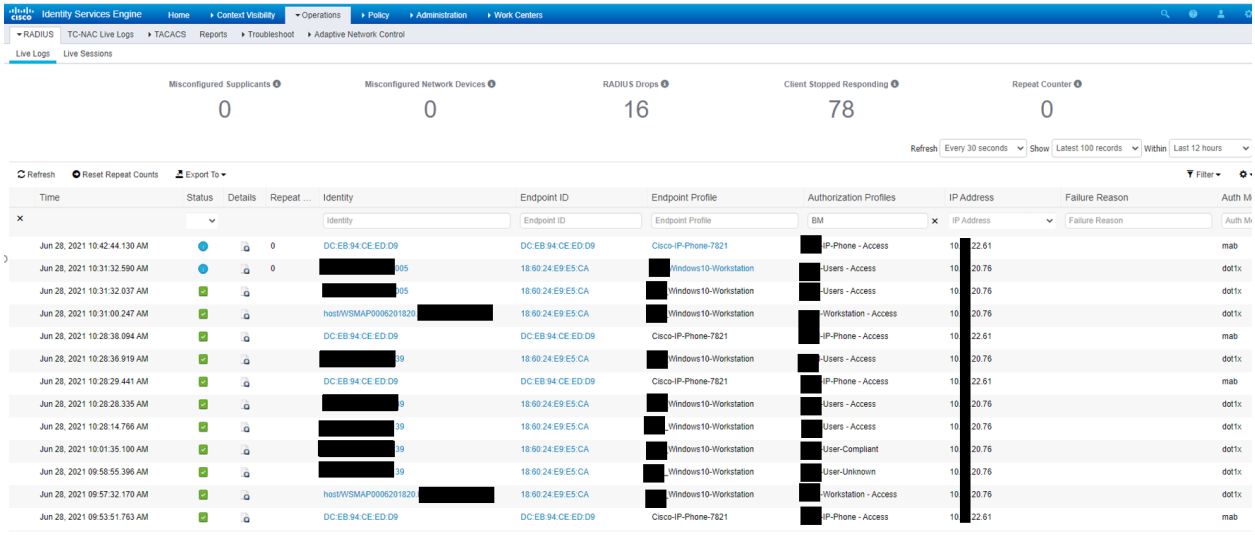

Figura 23: Interface com resultado de acesso a rede por um computador, e telefone IP autorizado

5. Capitulo V – Discussão dos resultados

Inicialmente procurou-se estabelecer um enquadramento teórico considerado adequado ao trabalho a desenvolver, na perspectiva das diversas vertentes a analisar, o levantamento do estado actual da infra-estrutura, a informação e a necessidade de segurança, as diferentes soluções tecnológicas do NAC e os protocolos para implementação. De um modo genérico, os resultados obtidos permitiram reforçar a percepção inicial do desenvolvimento de um sistema de controle de acesso lógico a rede em termos tecnológicos e a segurança da informação que transita nela, assim como a possibilidade de integração com as infra-estruturas existentes nas organizações, as vantagens que poderão advir, permitindo-nos identificar os constrangimentos que podem ser resolvidos na rede.

É importante destacar que a proposta de implementação de um sistema de controle de acesso de dispositivos e utilizadores a rede corporativa baseado no Cisco ISE foi considerada viável e promissora para atender às necessidades do Banco em relação à segurança da rede corporativa.

Os resultados da pesquisa indicaram que o Cisco ISE é uma solução eficaz para garantir a autenticação e autorização de dispositivos e utilizadores, bem como para implementar políticas de segurança na rede corporativa. Além disso, a solução permite uma maior visibilidade e controle sobre a rede, o que ajuda a identificar possíveis ameaças e vulnerabilidades.

A implementação da prova de conceito do sistema proposto em um ambiente de testes também foi considerada bem-sucedida, com os resultados indicando que a solução apresentou um bom desempenho em termos de autenticação, autorização e aplicação de políticas de segurança.

No entanto, a pesquisa também identificou alguns desafios e limitações na implementação do sistema proposto. Um dos principais desafios é a necessidade de treinamento e capacitação dos técnicos do DTI do NBP para lidar com a complexidade do Cisco ISE e garantir uma configuração adequada da solução e a exploração de mais funcionalidades. Além disso, a implementação do sistema pode exigir investimentos significativos em infra-estrutura e equipamentos.

Em resumo, os resultados do relatório indicaram que a proposta de implementação de um sistema de controle de acesso de dispositivos e utilizadores a rede corporativa baseado no Cisco ISE é uma solução viável e promissora para atender às necessidades de segurança do Banco. A discussão desses resultados pode ajudar a orientar futuras pesquisas e implementações na área de segurança de redes corporativas.

6. Capitulo VI – Considerações finais

6.1. Conclusões

O controle da rede de dados em um ambiente corporativo é algo extremamente importante, tendo em consideração que em certos casos como por exemplo, onde uma tomada de rede de dados que não se encontra protegida, é ligada um equipamento de rede como um *switch* com o serviço de DHCP, pode permitir o acesso para dentro da instituição, de utilizadores com o objectivo de roubar dados sensíveis do negócio da instituição. Porém, para fazer esse controle são necessárias ferramentas que consigam de forma automatizada controlar quem pode ou não pode utilizar um ponto de rede para acesso a rede interna, pois dependendo da quantidade de pontos existentes, fica humanamente impossível realizar este tipo de controle.

Em conclusão, a proposta de implementação de um sistema de controle de acesso à rede corporativa tem como objetivo principal garantir maior visibilidade e controle dos dispositivos e utilizadores que se conectam à rede, reduzindo significativamente o risco de acesso não autorizado, violações de segurança e danos à rede corporativa.

Através do estudo realizado, foram identificadas diversas ameaças cibernéticas que podem comprometer a segurança da rede corporativa do Banco, como ataques de *phishing*, *malware* entre outros. Além disso, foram apresentados os protocolos de segurança de rede, tais como o TLS, e o EAP, e os procedimentos de controle de acesso à rede, como o 802.1X e o *Network Access Control* (NAC).

A solução proposta para controle de acesso à rede corporativa do Banco é baseada na implementação do NAC, que permite a autenticação e verificação do estado do dispositivo antes de permitir o acesso à rede. Além disso, a solução inclui políticas de acesso baseadas em função, que limitam o acesso não autorizado a recursos confidenciais e o monitoramento contínuo dos dispositivos e utilizadores na rede, para detectar actividades maliciosas e comportamentos anormais.

A implementação da prova de conceito da solução proposta em um ambiente de testes permitiu a validação da eficácia da solução e a identificação de possíveis melhorias e ajustes para sua implementação em ambiente de produção. Com a implementação do sistema de controle de acesso proposto, o Banco terá maior visibilidade e controle sobre os dispositivos e utilizadores que se conectam à rede corporativa, garantindo a integridade e a segurança dos dados e sistemas do Banco.

Em resumo, a implementação de um sistema de controle de acesso à rede corporativa é essencial para garantir a segurança e a integridade dos dados e sistemas do Banco. A solução proposta é

eficaz e permite uma maior visibilidade e controle dos dispositivos e utilizadores que se conectam à rede, além de ser baseada em tecnologias e protocolos amplamente utilizados no mercado, garantindo a compatibilidade e a interoperabilidade com outros sistemas e soluções já em uso pelo Banco.

6.2. Recomendações

A mobilidade faz hoje parte da vida das pessoas, integrando a sua vida pessoal e profissional. A utilização crescente de *smart devices*, dentro e fora do local de trabalho, mudou totalmente a forma como as pessoas interagem e trabalham. Neste impasse, recomenda-se ao departamento de tecnologias de informação a exploração do presente sistema, de modo a garantir maior segurança dos dispositivos, utilizadores e dos dados móveis. Para implementarem esta mudança, as organizações necessitam de definir como ultrapassar alguns obstáculos, tais como a gestão dos dispositivos, a segurança e protecção da informação e a convivência de dados corporativos com dados pessoais no mesmo equipamento. Existem muitas abordagens tecnológicas disponíveis, com vista à integração dos dispositivos móveis no ambiente corporativo. Porém, a diversidade de opções dificulta a escolha por parte das organizações, preocupadas em proteger o seu investimento e definir soluções para o futuro.

Recomenda-se que seja definido uma política clara de segurança da informação, pois é fundamental que a instituição tenha uma política de segurança da informação bem definida e comunicada a todos os colaboradores e utilizadores da rede. Essa política deve incluir normas de uso dos dispositivos e da rede, requisitos de senhas seguras, actualização de *software*, entre outros aspectos relevantes para garantir a segurança dos dados.

Antes de implantar a tecnologia Cisco ISE em ambiente de produção, é importante explorar mais funcionalidades e testes em um ambiente de teste para garantir a compatibilidade e a eficácia da solução. Além disso, é fundamental fornecer treinamentos para os colaboradores e utilizadores da rede, para que saibam como utilizar a solução de forma adequada. É importante monitorar continuamente a rede, com o objectivo de identificar possíveis ameaças e detectar comportamentos suspeitos. A monitoração deve ser realizada de forma constante, para garantir a efectividade da solução de segurança.

E por fim é importante manter o Cisco ISE actualizado, com as últimas versões de *software* e de segurança. Além disso, é importante realizar testes de vulnerabilidade com frequência para garantir que a solução ainda é eficaz contra as últimas ameaças de segurança.

Bibliografia

Referências bibliográficas

1. Awati, R. (2021, July 26). What is network access control (NAC) and how does it work? https://www.techtarget.com/searchnetworking/definition/network-access-control, 07 de Janeiro 2023
2. A. Gal and J. Feise, "Cisco NAC Appliance Agent Installation Bypass Vulnerability", Security Focus, Aug. 2006 http://www.securityfocus.com/archive/1/444737/30/0/threaded, 04 de Novembro de 2022
3. A. Harding and R. Risser, "Secured and Assured Networking with an Enterprise Infranet", white paper, Juniper Networks; http://www.juniper.net/solutions/literature/white_papers/200144.pdf. 22 de Março 2023
4. ALLEN, Julia H.. The CERT Guide to System and Network Security Practices. First printing, Boston-MA-EUA, Addison-Wesley, 2001.
5. AMOROSO, Edward. Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and Response. Sparta-NJ-EUA, Intrusion.Net Books, 1999.
6. ANDERSON, James P.. Computer Security Threat Monitoring and Surveillance. Fort Washington, James P. Anderson Co., 1980.
7. Australian National Audit Office. (2005). IT Security Management Audit Report. Australian National Audit Office. Retrieved from www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf 22 de Março 2023
8. Angela, A. I. (2014, July). Evaluation of Enhanced Security Solutions in 802.11-Based Networks. International Journal of Network Security & Its Applications (IJNSA), 6(4), 29-42. doi:10.5121/ijnsa.2014.6403
9. CSI/FBI–2003. Computer Crime and Security Survey. http://www.gocsi.com
10. Cisco Identity Services Engine Installation Guide, Release 3.0. (2021, December). https://www.cisco.com/c/en/us/td/docs/security/ise/30/install_guide/b_ise_InstallationGuide30.pdf 22 de Março 2023
11. Cisco Systems. (2011). *Cisco TrustSec™ 2.0: Design and Implementation Guide.* Cisco System. Cisco Public Information.
12. "Cisco NAC Appliance Enforcing Host Security with Clean Access Jamey Heary," CCIE® No. 7680, 2007.
13. CISCO NAC – EXECUTIVE OVERVIEW. 2009. https://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/net_implementation_white_paper0900aecd80557152.pdf
14. D. Hendrickson, Network Admission and Access Control, Product Selection Guide, Version 2.0., tech. report, Secure Access Central Security Portal, Apr. 2007;
15. Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review,, 31*(12), 243-256.
16. Deng, D. J., Chen, K. C., & Cheng, R. S. (2014, August). IEEE 802.11 ax: Next generation wireless local area networks. In Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine). *2014 10th International Conference on* (pp. 77-82). IEEE.

17. HAGEN, Richard D.. A User's Guide to Security Threats on the Desktop. <http:// sans.org >
18. IEEE 802.11. (2012). *Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. New York: Institute of Electrical and Electronics Engineers.
19. ISO/IEC 27033-3. (2010). *Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues*. International Standards Organization.
20. ISO/IEC 27033-4. (2014). *Securing communications between networks using security gateways*. International Standard Organization.
21. ISO/IEC 27033-5. (2013). *Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*. International Standards Organization. http://sslvpn.breakawaymg.com/breakaway/NAC%20PSG.php. 26 de Março 2023
22. Juniper Unified Access Control. http://www.juniper.net/us/en/products-services/security/uac/#overview 22 de Março 2023
23. Mark Smallwood (2016, May) 802.1X Network Access Control (NAC) https://www.juniper.net/documentation/en_US/learn-about/LA_802.1X_NAC.pdf 22 de Março 2023
24. McCLURE, Stuart. ; SCAMBRAY, Joel; KURTZ, George. Hackers Expostos: Segredos e Soluções para a Segurança de Redes. 1ª edição, São Paulo, Makron Books, 2000.
25. NAC WHITEPAPER. 2008. http://www.enterasys.com/company/literature/nac-wp.pdf..
26. "Getting the Knack of NAC: Understanding Network Access Control", A Mirage Networks Industry Report, white paper, Mirage Networks, Jan. 2006; http://www.miragenetworks.com/documents/white_papers/MirageNAC_IndustryReport.pdf. 22 de Março 2023
27. Gartner, Information Technology Research and Advisory. www.gartner.com 28 de Março 2023
28. Wired 802.1X deployment guide. (2011, September). https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_199/Dot1X_Deployment/Dot1x_Dep_Guide.html 22 de Fevereiro 2023

Outras bibliografias consultadas

1. NIST SP 800-94. (2007, February). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST).
2. Santos, A. P., & Barbosa, R. R. (2011). Desafios da Mobilidade Corporativa para a Gestão da Informação e do Conhecimento. Informação & Sociedade: Estudos, 21(2), 49-62
3. Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2010). Tecnologia da informação para gestão. Porto Alegre: Bookman.

Anexos

Anexo 1: Tutorial de instalação do Cisco ISE

1. O tutorial mostra o processo de inicialização e instalação do Cisco ISE versão 2.1. Mas deve-se tomar em consideração que antes de iniciar, é necessário certificar de que todas as informações descritas abaixo se encontram preparadas durante o *bootstrap*:

Tabela 6: Requisitos para configuração inicial

Endereçamento
o IP, Máscara, Gateway
o Name Servers, NTP Servers, Time Zone
Nomes
o Hostnames, Deployment naming
o DNS
Certificados
o Considerar certificados comas funcionalidades (Admin, EAP, Portals, pxGRID)

2. De seguida fazer o *download* da imagem ISO do Cisco ISE.
    a. Aceder a URL http://www.cisco.com/go/ise. É necessária uma conta válida da Cisco para acesso a imagem.
    b. Clicar em ***Download Software for this Product***.

Nota: A imagem ISO do Cisco ISE vem com uma licença temporária de 90 dias já instalada, que permite testar todos os serviços do Cisco ISE quando a instalação e a configuração inicial estiverem concluídas.

3. Inicializar o servidor físico ou servidor virtual.
    a. Servidor físico da Cisco:
        - Conectar ao CIMC e fazer o *login* usando as credenciais do CIMC.
        - Iniciar a consola de KVM.
        - Escolher a opção Virtual Media > Activate Virtual Devices.

- Escolher a opção Virtual Media > mapear CD/DVD e seleccionar a imagem ISO do Cisco ISE e clicar no Map Device.
- Escolher a opção Macros > Static Macros > Ctrl-Alt-Del para reiniciar o dispositivo com a imagem ISO do Cisco ISE.
- Pressionar no F6 para trazer o *boot* menu. Então uma imagem similar a figura 24 que se encontra abaixo irá aparecer:

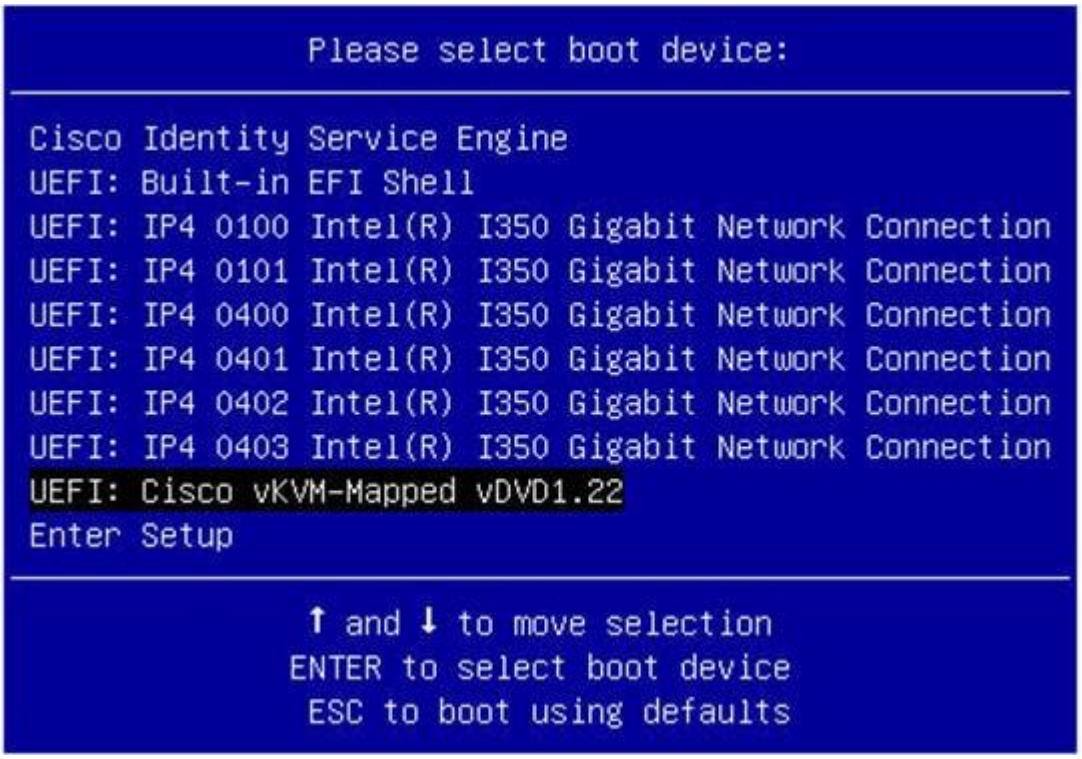

Figura 24: Imagem para seleccionar o método de inicialização

Nota: se os servidores físicos estiverem instalados em um local remoto (por exemplo, um centro de dados), na qual não se tem o acesso físico e é necessário realizar a instalação do CIMC a partir de servidores remotos, deste modo a instalação pode levar muitas horas. É recomendado realizar a cópia do arquivo ISO em uma unidade USB e usar fisicamente no servidor para acelerar o processo de instalação.

b. Servidor virtual:

- Mapear o CD/DVD para a imagem ISO. E de seguida uma tela como o menu semelhante à figura 25 é exibida.

- Menu de selecção

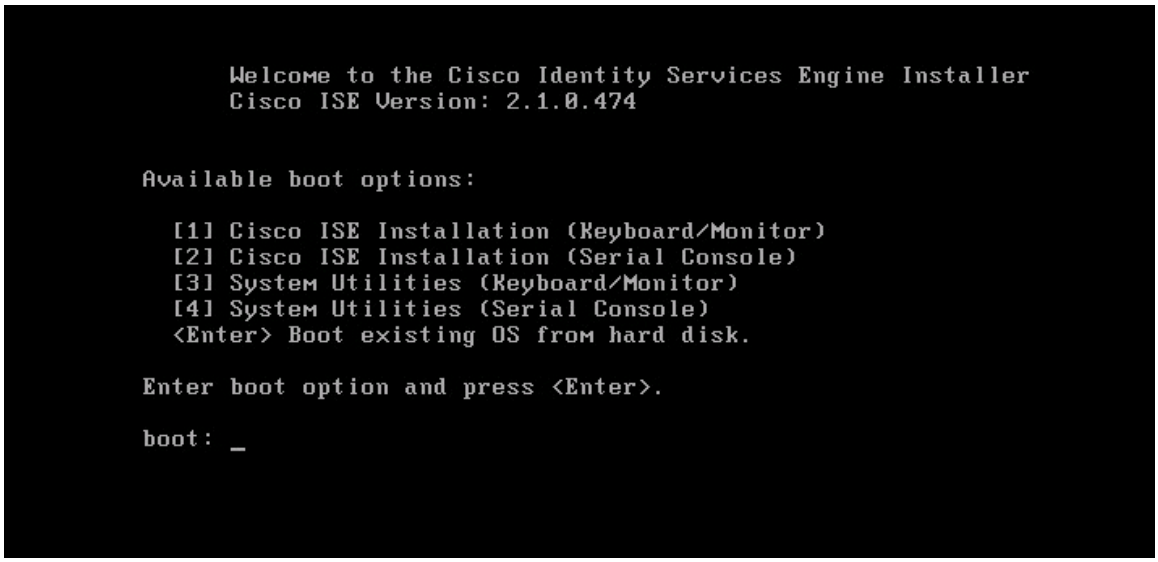

Figura 25: Menu de selecção apos inicializar a imagem ISO

- Menu de selecção – escolhendo a opção 1 (um)

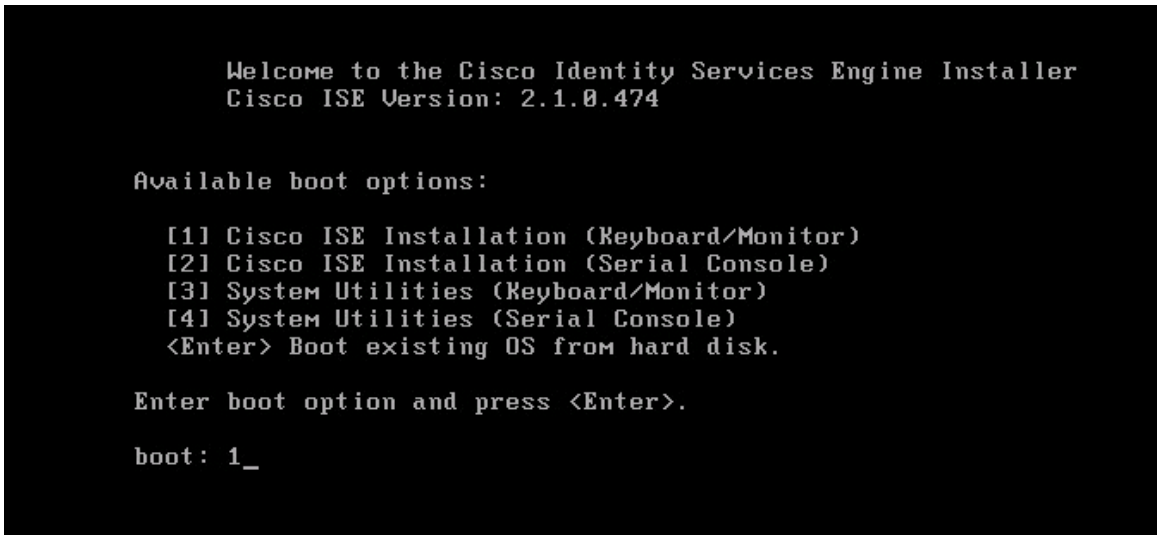

Figura 26: Menu de selecção, opção 1 (um)

- Bootstrap – processo de instalação em andamento 1 (um)

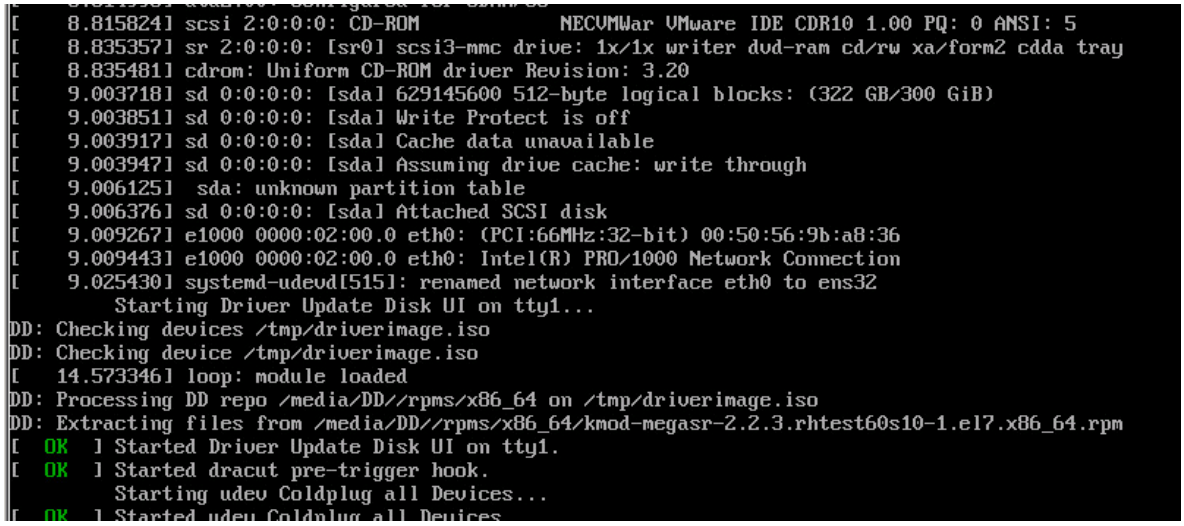

Figura 27: processo de instalação do ISO

- Bootstrap – processo de instalação em andamento 2 (dois)

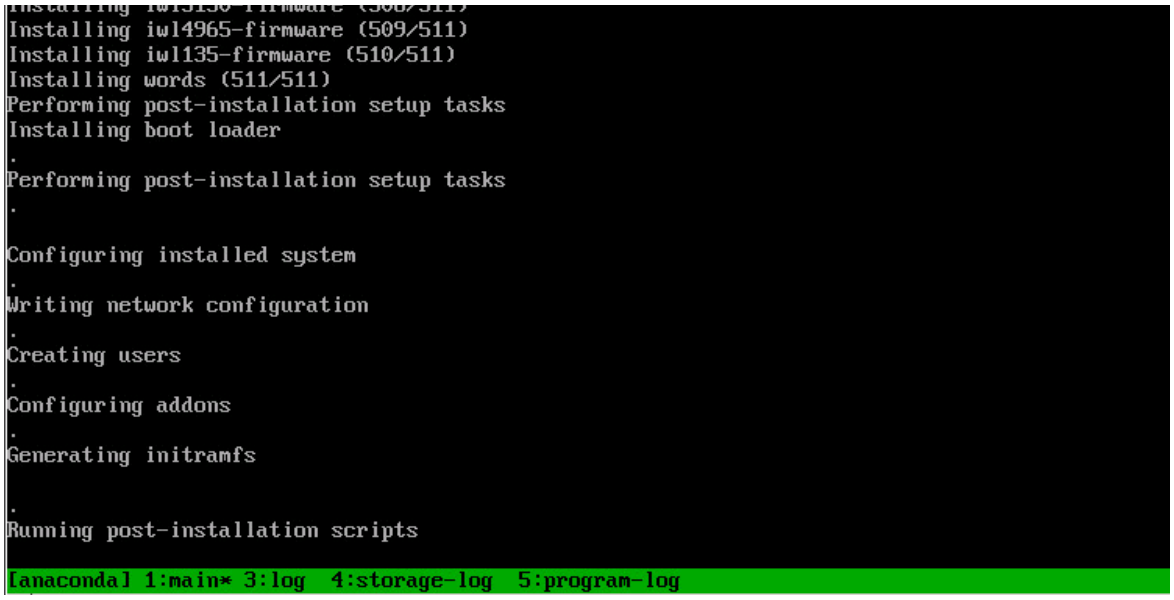

Figura 28: Processo de instalação do ISO

- Bootstrap – processo de instalação: *setup*

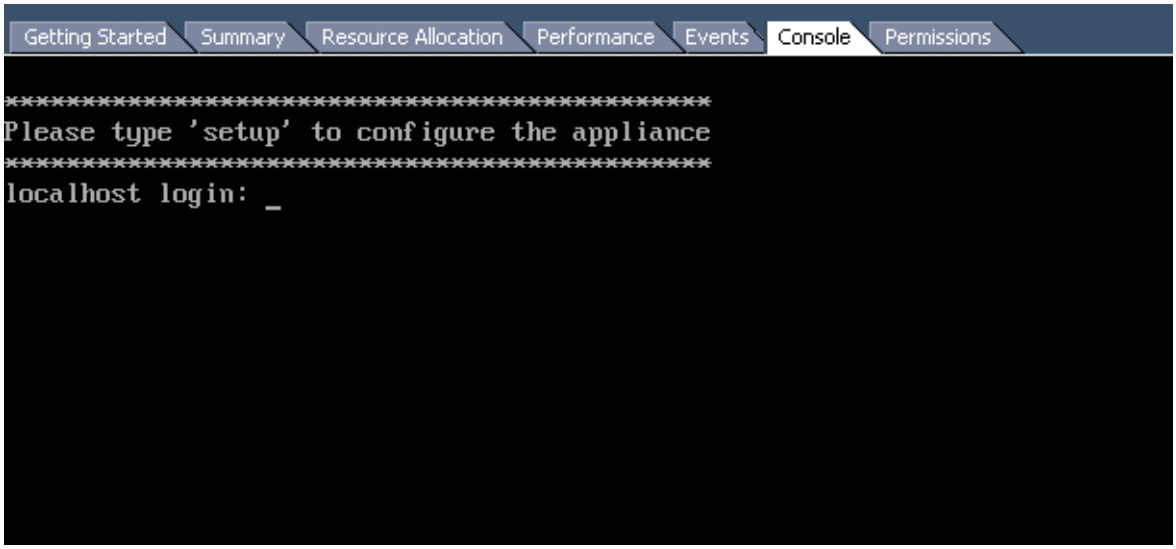

Figura 29: Processo de instalação do Setup do ISSO

- Bootstrap – processo de instalação: por linha de comando (CLI ADE-OS) com os detalhes de configuração

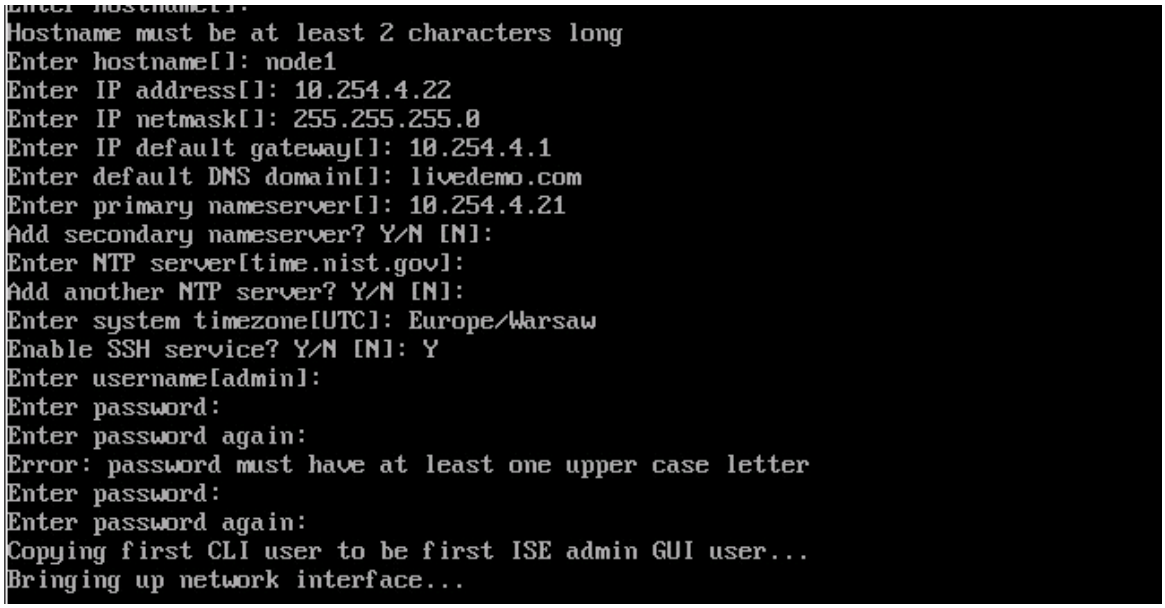

Figura 30: Configuração inicial

- Bootstrap – processo de instalação: CLI ADE-OS com os detalhes de configuração – continuação

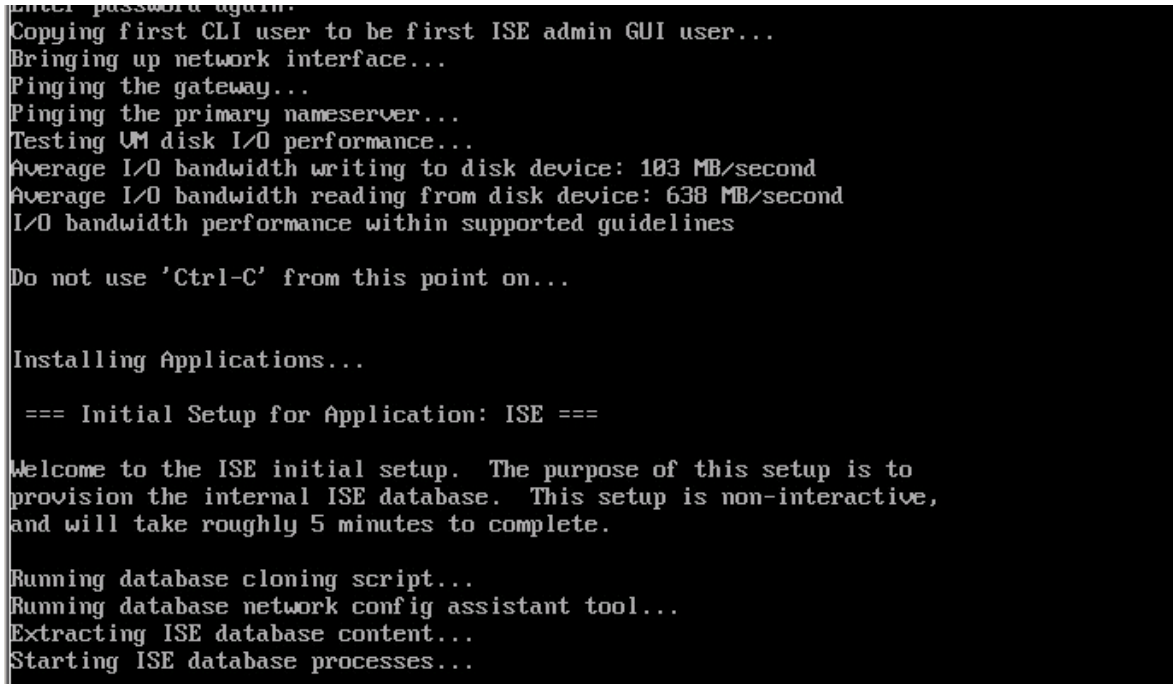

Figura 31: Continuação da configuração inicial

- Bootstrap – depois da instalação, usar o comando **show run** para verificar a configuração inicial do ADE OS

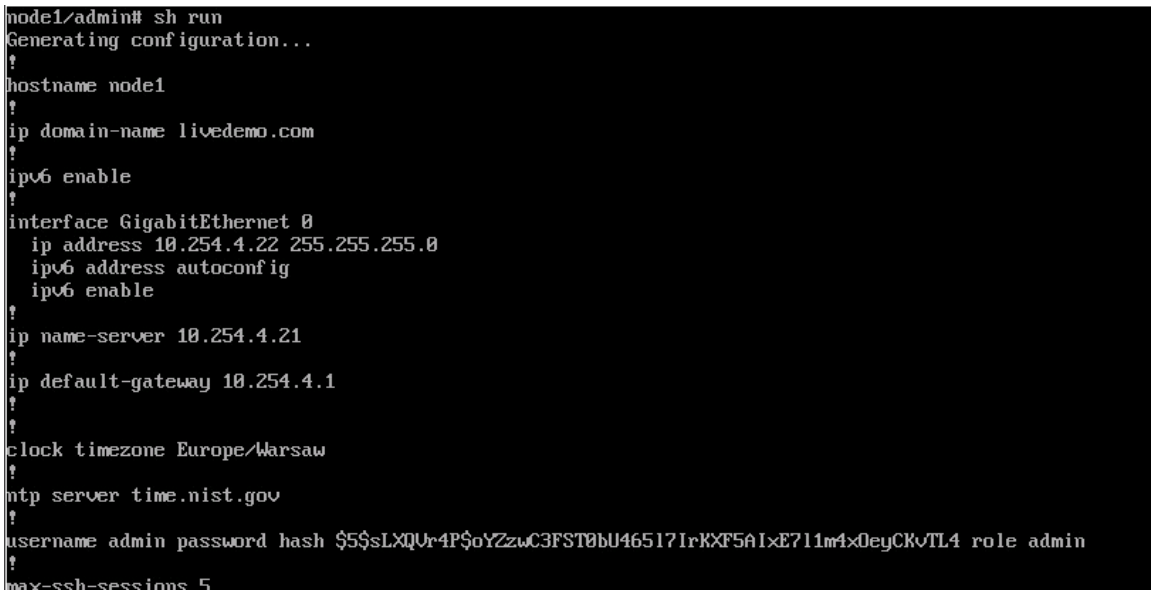

Figura 32: Verificação das configurações iniciais

- Apôs a instalação usar o comando: **node1/admin#show application status ise** para verificar os serviços que se encontram em execução (*running*). Deve-se observar que até que o serviço *application server* não esteja em execução, a interface *web* (GUI) ainda não está pronta para interacção

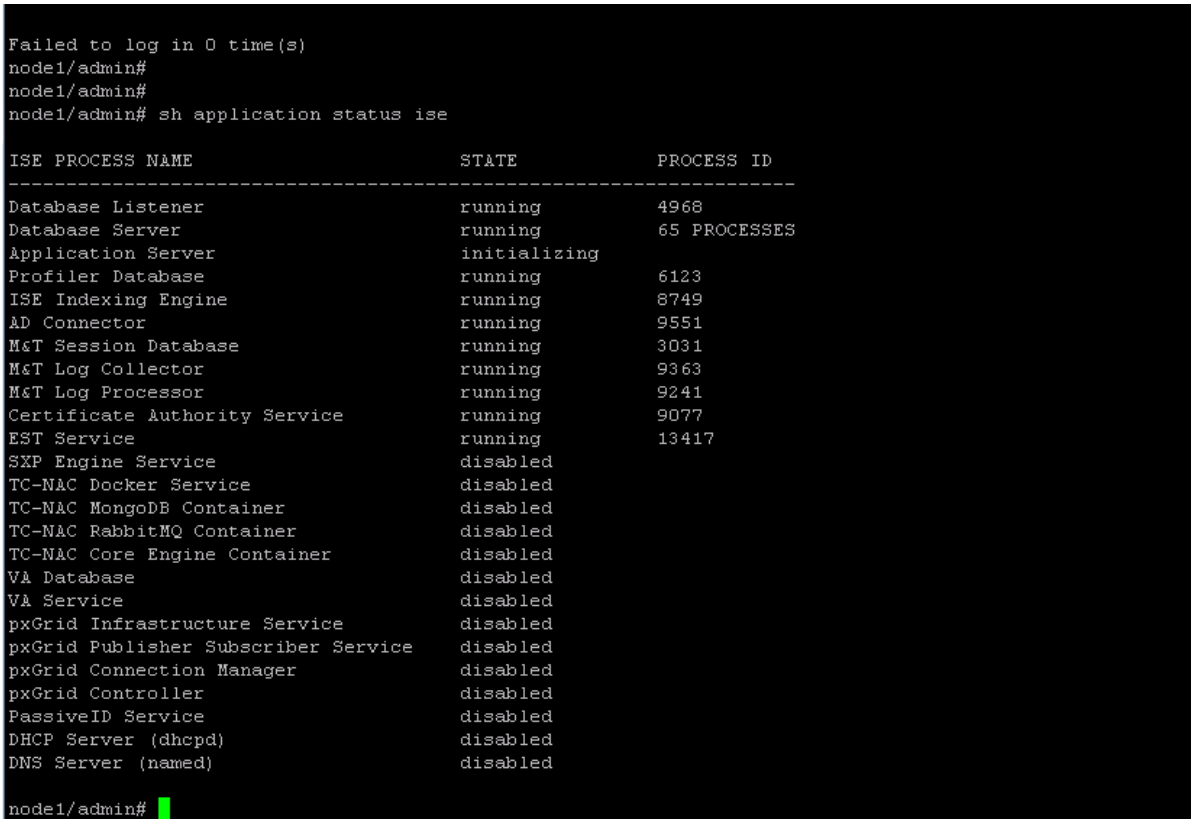

Figura 33: Verificação do estado dos serviços da aplicação

- Após a conclusão da instalação, pode-se fazer o *login* na interface *web* GUI, apresentada na figura 34.

- **Interface web do ISE (GUI)**
  - O serviço *application server* deve estar em execução (*running)*, para poder aceder a URL com os dados de endereçamento ou *hostname*.
    https://*ise_ip_address_or_name*
  - Deve-se aceder colocando o primeiro *login* usado durante o inicio da instalação da imagem ISO.

- E por fim validar a versão da aplicação ISE e a versão do ADE-OS, conforme atesta a figura 34.

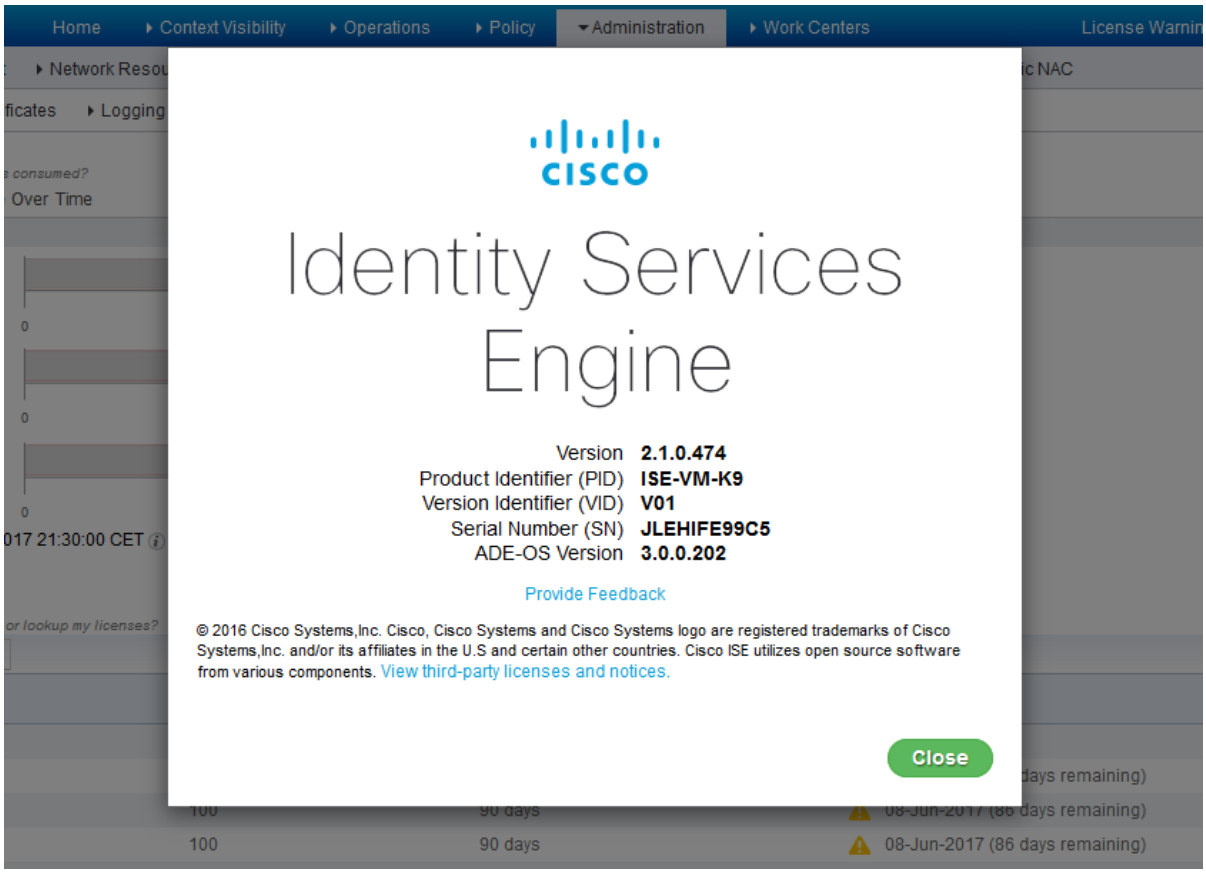

Figura 34: Imagem da interface gráfica do ISE

Anexo 2: Guia das questões

1. Como os dispositivos e utilizadores tem acesso à rede interna?
2. Quais os constrangimentos verificados?
3. Em que fases do processo de acesso à rede se verificam maiores constrangimentos?
4. Como têm sido superados tais constrangimentos?
5. Existe registos de perda ou vazamento de informação confidencial?
6. Actualmente é possível visualizar os dispositivos e utilizadores conectados a rede interna?
7. Existe alguma restrição lógica aos dados e ou/ informação confidencial da instituição?
8. Como são tratados os visitantes, e ou entidades externas que necessitam de acesso à rede interna?

Respostas

1.R: os utilizadores que se conectam a rede cabeada e a rede wireless, tem acesso a rede interna, através da autenticação pelo domínio institucional. Os dispositivos têm acesso directo desde que estejam ligadas a um ponto de rede activo.

2.R: qualquer dispositivo que se conecta a um ponto de rede activo tem acesso a rede interna.

3.R: durante o processo de autenticação, em que não se verificam os dispositivos e utilizadores que não pertencem a instituição.

4.R: somente os pontos de rede que devem ser alocados dispositivos é que são activadas e através de configuração de listas de controle de acesso.

5.R: Sim.

6.R: verificamos apenas os endereços IP, não temos visibilidade da localização e as características dos dispositivos.

7.R: sim, parcialmente através de listas de controle de acesso.

8.R: tem acesso a toda rede com a supervisão de um técnico da área para acompanhamento dos trabalhos.