



Relatório Final - Supermercado

RELATÓRIO FINAL

UNIVERSIDADE LUSÓFONA – PÓS-GRADUAÇÃO CIBERSEGURANÇA APLICADA

SEGURANÇA EM REDE E DISPOSITIVOS IoT

Daniel Rodrigues | Rafael Azevedo

6 de janeiro de 2026

Conteúdo

Índice de Figuras	1
Índice de Tabelas	2
1 Introdução	3
2 Cenário Alvo	4
2.1 Descrição Cenário e Estrutura Organizacional	4
2.2 Áreas	4
2.2.1 IT	4
2.2.2 Administração	4
2.2.3 Área de Fornecedores	4
2.2.4 Recursos Humanos	4
2.2.5 Área de Segurança	5
2.2.6 Área Logística e Transporte	5
2.2.7 Área de Venda	5
2.2.8 Marketing	5
2.2.9 Área de Controlo de Qualidade	5
2.2.10 Apoio ao Cliente	5
2.2.11 Gestão de Stocks	5
2.2.12 Área E-Commerce	5
3 Design da Rede	6
4 Protocolos e Medidas de Segurança	7
4.1 Segurança com o IPV6	7
4.2 SSH	7
4.2.1 O que é?	7
4.2.2 Como Funciona?	8
4.2.3 Para que é utilizado?	8
4.2.4 <i>Malware(s)</i> Protegido(s) pelo SSH	9
4.2.5 Relação com o Cenário (Supermercado)	9
4.3 IPSec	10
4.3.1 O que é?	10
4.3.2 Como Funciona?	10
4.3.3 Para que é utilizado?	10
4.3.4 <i>Malware(s)</i> Protegido(s) pelo IPSec	11
4.3.5 Relação com o Cenário (Supermercado)	11
4.4 SSL/TLS	12

4.4.1	O que é	12
4.4.2	Como Funciona?	12
4.4.3	Para que é utilizado	12
4.4.4	<i>Malware(s)</i> Protegido(s) pelo SSL/TLS	13
4.4.5	Relação com o Cenário (Supermercado)	13
4.5	<i>Firewall</i>	14
4.5.1	O que é?	14
4.5.2	Ponto de Ação da <i>Firewall</i> ?	15
4.5.3	Tipo de <i>Firewall</i> utilizado?	16
4.5.4	O que vai ser permitido?	16
4.5.5	Qual o fluxo de tráfego permitido?	17
4.5.6	<i>Malware(s)</i> Protegido(s) pela <i>Firewall</i>	18
4.6	<i>IDS/IPS</i>	18
4.6.1	O que é?	18
4.6.2	Ponto de Ação do IDS e IPS	19
4.6.3	<i>Malware(s)</i> Protegido(s) pelo <i>IPS/IDS</i>	19
4.6.4	Relação com o Cenário (Supermercado)	19
4.7	<i>VPN</i>	20
4.7.1	O que é?	20
4.7.2	Ponto de Ação da <i>VPN</i>	20
4.7.3	<i>Malware(s)</i> Protegido(s) pela <i>VPN</i>	21
4.7.4	Relação com o Cenário (Supermercado)	21
4.8	Desenho com Dispositivos de Segurança	22
5	Servidores	23
5.1	DNS	23
5.2	DHCP	23
5.3	AD	23
5.4	Servidor Página Web (SPW)	23
5.5	Gestor de Ficheiros (GP)	23
5.6	Servidor de IoT (IoT)	23
5.7	Servidor de Backup (Backup)	24
5.8	Servidor de Base de Dados (Base de Dados)	24
5.9	Servidor de Atualizações (Atualizações)	24
5.10	Servidor de Aplicações Comerciais (AC)	24
5.11	Servidor de VoIP (VoIP)	24
5.12	Servidor de Impressão (Impressão)	24
5.13	Servidor de Análise de Dados (Data)	24
6	Níveis de Credenciais e Políticas de Acesso	25

6.1	Níveis de Credenciais	25
6.2	Políticas de Acesso	25
6.2.1	Autenticação	25
6.2.2	Monitorização	26
6.2.3	Controlo de Sessão	26
6.2.4	Segmentação	26
7	Plano de Endereços IPV6	27
8	Técnicas de Rede	32
8.1	Switches	32
8.1.1	Medidas de Segurança	32
8.2	ACL	32
8.2.1	Regras ACL para a Sede	32
8.2.2	Regras ACL para a Sucursal	33
8.2.3	Regras ACL para o Acesso Remoto	33
9	Backups	34
9.1	Tipos de Backup	34
9.2	Estratégias	35
9.3	Plano de Backup para o Supermercado	35
9.3.1	Plano de Backup para Configuração dos Dispositivos Intermédios -	35
9.3.2	Plano de Backup para Dados Operacionais -	36
10	IoT	37
10.1	Ameaças e Vulnerabilidades	37
10.2	Melhores Práticas	37
10.3	Protocolo de Publish	38
10.4	Cenário	38
10.4.1	MQTT	39
10.5	Cenário com Dispositivos IoT	40
11	Conclusão	41
12	Anexos	42
12.1	Configurações dos Routers	42
12.1.1	Router Sede	42
12.1.2	Router Sucursal	42
12.2	Configurações dos Switches	43
12.2.1	Configuração de Vlans	43
12.2.2	Configuração de Dispositivos nas Vlans - Servidores	44

12.2.3 Configuração de Dispositivos nas Vlans - Switch IT	47
12.2.4 Configuração de Dispositivos nas Vlans - Switch Administração	47
12.2.5 Configuração de Dispositivos nas Vlans - Switch Fornecedores	48
12.2.6 Configuração de Dispositivos nas Vlans - Recursos Humanos	49
12.2.7 Configuração de Dispositivos nas Vlans - Segurança	50
12.2.8 Configuração de Dispositivos nas Vlans - Logística e Transporte	50
12.2.9 Configuração de Dispositivos nas Vlans - Vendas	51
12.2.10 Configuração de Dispositivos nas Vlans - Marketing	52
12.2.11 Configuração de Dispositivos nas Vlans - Ecommerce	53
12.2.12 Configuração de Dispositivos nas Vlans - Gestão de Stocks	53
12.2.13 Configuração de Dispositivos nas Vlans - Apoio ao Cliente	54
12.2.14 Configuração de Dispositivos nas Vlans - Controlo de Qualidade	55
12.2.15 Configuração de Dispositivos nas Vlans - IoT	56
12.3 Configuração de Ligação entre Switches e Routers	58
12.4 Configuração de Métodos de Segurança	58

Índice de Figuras

1	Topologia Inicial	6
2	Protocolo SSH	8
3	Protocolo IPSec	10
4	Protocolo SSL/TLS	12
5	<i>Firewall</i>	14
6	Ponto de Ação da <i>Firewall</i>	15
7	Ponto de Ação dos IDS/IPS	20
8	Ponto de Ação da VPN	21
9	Desenho da Rede com Dispositivos de Segurança	22
10	Cenário com Dispositivos IoT	40
11	Infraestrutura de Rede no EVE	59

Índice de Tabelas

1	Restrições da <i>Firewall</i>	17
2	Fluxo Permitido Final e Otimizado	18
3	Níveis de Credenciais	25
4	Tabela de Endereços da Sede	30
5	Tabela de Endereços da Sucursal	31
6	Tabela de Endereços do Trabalho Remoto	31
7	Regras ACL para a Sede	32
8	Regras ACL para a Sucursal	33
9	Regras ACL para o Acesso Remoto	33

1 Introdução

No âmbito da unidade curricular de "Segurança de Redes de Dados e IoT" foi pedido um relatório cujo objetivo é planear uma rede de computadores com o foco virado para a segurança, tendo em conta um cenário hipotético de um supermercado onde existe por base as boas práticas da área de redes de dados e integração com dispositivos IoT.

A infraestrutura do supermercado precisa de uma rede robusta e segura para que exista uma gestão de operações críticas como o controlo de stock, sistemas de ponto de venda, e-commerce e até comunicação com os fornecedores e clientes. O desenho da rede deve atender aos requisitos funcionais e de segurança, considerando a estrutura da sede, uma sucursal e o ambiente de trabalho remoto.

No seguinte relatório será apresentada uma visão detalhada do design da rede do supermercado com a inclusão da descrição das áreas funcionais, tipologia da rede, servidores implementados e também a implementação de diferentes níveis de credenciais de forma a garantir o controlo de acesso aos recursos da rede

2 Cenário Alvo

2.1 Descrição Cenário e Estrutura Organizacional

Para o desenvolvimento deste projeto, é simulado um ambiente real, onde é feito um pedido, por parte de um supermercado fictício denominado "*Products A Lot*", que consiste na contratação de uma equipa com capacidades para implementar e configurar um sistema de rede que ofereça segurança e eficiência para a sede desta empresa, uma sucursal e um ambiente remoto. O orçamento proposto pela empresa é ilimitado, isto é, devem ser tomadas as melhores e mais avançadas medidas para alcançar a robustez máxima do ambiente de rede.

A estrutura da organização vai ao encontro da descrição feita acima, onde é indicado que a empresa está subdividida em três secções, a sede, onde estão centralizados todos os componentes da empresa, a sucursal, que apesar de não conter os mesmos atributos que a sede, atua de forma independente e o ambiente remoto, onde colaboradores serão capazes de aceder aos recursos disponibilizados pela organização.

2.2 Áreas

No seguinte tópico serão tratadas as diferentes áreas que acompanham o cenário simulado e que vão ao encontro do supermercado, resumindo os objetivos de cada área, respetivamente, de forma sucinta.

2.2.1 IT

Nesta área, serão geridas tarefas como gestão da infraestrutura de rede e servidores, monitorização e manutenção do sistema e controlo de acessos à rede.

2.2.2 Administração

Área responsável pela gestão geral da empresa, incluindo a tomada de decisões estratégicas e também coordena operações financeiras, jurídicas e administrativas.

2.2.3 Área de Fornecedores

Gere as relações com os fornecedores incluindo a negociação de preços e contratos e também garante que existe sempre stock no supermercado.

2.2.4 Recursos Humanos

Gere o recrutamento, treino e desenvolvimento dos funcionários cuidando dos seus salários, benefícios e relações.

2.2.5 Área de Segurança

Monitoriza e protege os sistemas digitais implementando sistemas de vigilância, alarmes e políticas de acesso. Realiza também auditorias de segurança.

2.2.6 Área Logística e Transporte

Coordena a movimentação de mercadorias entre os fornecedores e as lojas gerindo frotas de veículos e armazéns e garantindo eficientemente a entrega pontual dos produtos encomendados.

2.2.7 Área de Venda

Faz o atendimento ao cliente garantindo que os produtos estejam bem apresentados e disponíveis para compra.

2.2.8 Marketing

Cria e desenvolve estratégias de marketing analisando o comportamento do consumidor para atrair mais clientes e aumentar as vendas através de publicidades, promoções e branding.

2.2.9 Área de Controlo de Qualidade

Garante que os produtos vendidos atendem os padrões de qualidade e segurança fazendo regularmente inspeções e testes às mercadorias.

2.2.10 Apoio ao Cliente

Responde a dúvidas, reclamações e pedidos dos clientes oferecendo também suporte pós-venda de forma a melhorar a experiência dos clientes.

2.2.11 Gestão de Stocks

Controla os níveis de stock nos armazéns e lojas e previne a falta ou até excesso de inventário.

2.2.12 Área E-Commerce

Gere a loja online do supermercado garantindo que a experiência de utilização do site incluindo a navegação e pagamento seja o melhor possível. Também coordena a logística de entrega dos pedidos online.

3 Design da Rede

Numa fase inicial, foi realizado um estudo da topologia de rede, de forma a organizar, da melhor forma, a possível infraestrutura de rede do supermercado. Nesta secção, o estudo foi desprovido de qualquer equipamento ou técnica de segurança. Sendo assim, na imagem abaixo, apenas são representados os equipamentos mínimos necessários na sede, filial e acesso remoto da empresa, bem como as áreas de negócio da mesma.

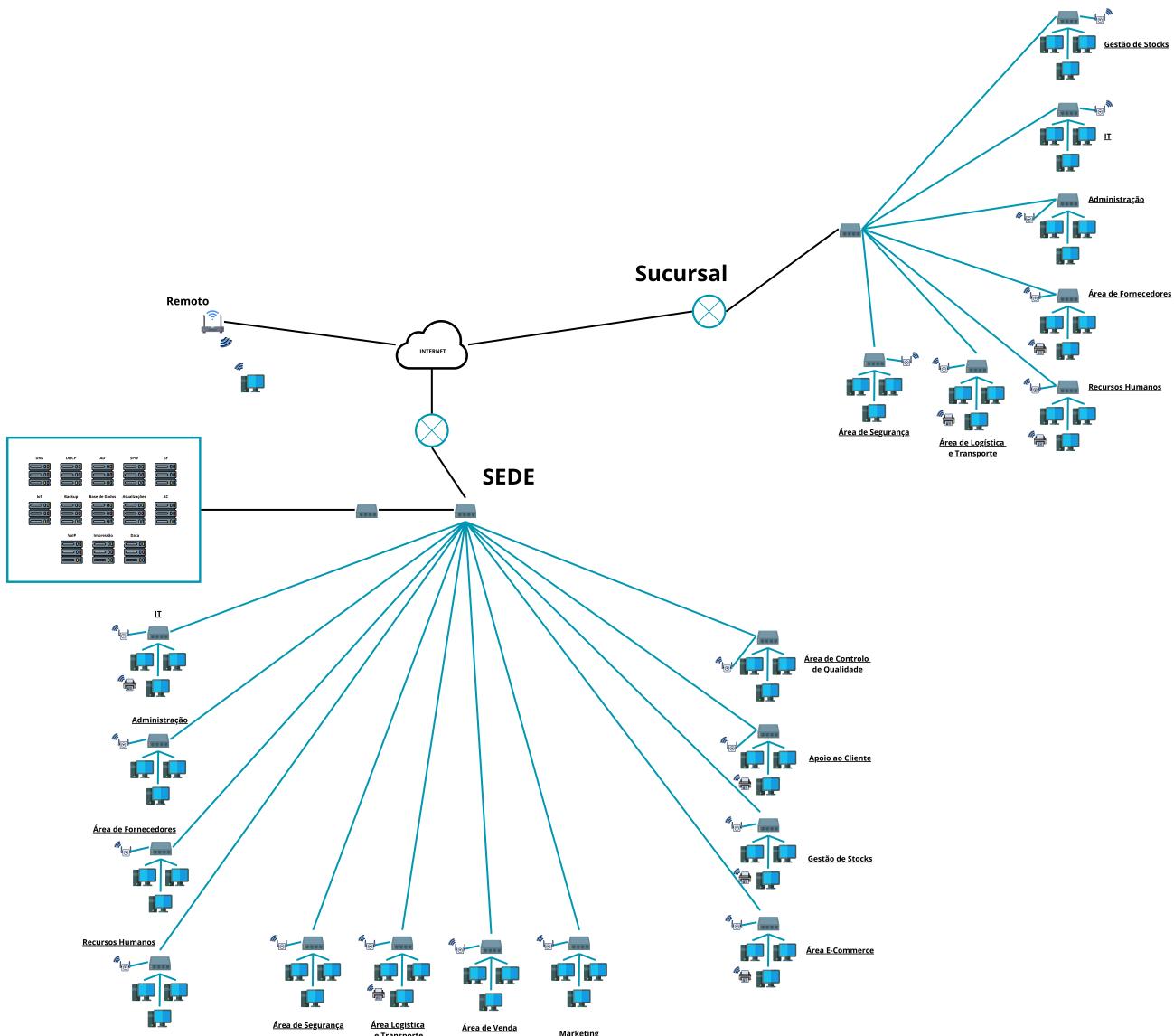


Figura 1: Topologia Inicial

4 Protocolos e Medidas de Segurança

4.1 Segurança com o IPV6

O IPV6 é a versão mais recente do protocolo de internet. Esta atualização surgiu através da necessidade de expandir o alcance dos endereços, que o IPV4 já não conseguia alcançar. Para além desta particularidade, o IPV6 é considerado uma melhoria significativa, em relação ao seu antecessor, no tópico da segurança. O protocolo mais recente apresenta opções de criptografia e autenticação, o que fornece integridade e confidencialidade às comunicações.

O IPV6 não consegue proteger contra nenhum tipo de *malware* de forma direta, no entanto, através de outros protocolos e características do próprio, a segurança é significativamente reforçada face ao IPV4. A projeção do IPV6 com a inclusão do IPSec fornece vários apoios na confidencialidade e integridade dos dados, esta característica pode prevenir *malwares* que intercetem ou manipulem pacotes, como é o exemplo dos ataques *Man-in-the-Middle*. Para além desta característica, o largo espaço de endereçamento, eliminação do *Network Address Translation* e vasta configuração de *malwares* direcionados apenas ao IPV4, são algumas razões para tornar a nova versão do protocolo de internet mais seguro.

Como exemplos práticos no cenário em questão, o IPv6, juntamente com o IPSec, referido acima, pode incluir autenticação e encriptação na comunicação entre os servidores, nos terminais de pagamento do supermercado e até nos dispositivos IoT utilizados pela empresa, portegendo-a de ataques *Man-in-the-Middle*. Além desta proteção, o IPv6, face ao seu maior alcance de endereços, torna quase impossível ao intruso, fazer um *scan* à rede da empresa. Por fim, a comunicação entre a Sede e Sucursal da empresa, torna-se segura, possibilitando troca de dados sem tantas preocupações, visto que o IPv6 facilita a implementação de VPNs baseadas no IPSec.

4.2 SSH

4.2.1 O que é?

Nesta secção, será abordada a importância da utilização do protocolo SSH, a forma como se obteve e a identificação dos equipamentos que utilizam esta tecnologia.

O SSH (*Secure Shell*) é um protocolo de rede que fornece aos utilizadores uma forma segura de aceder, ou enviar comandos a um computador através de uma rede não segura. O SSH também oferece palavras-passe seguras e autenticação com chaves públicas, assim como trocas de dados encriptadas entre duas máquinas conectadas através de uma rede aberta.

4.2.2 Como Funciona?

O protocolo SSH trabalha através do protocolo TCP/IP, que funciona como um protocolo de transporte e o SSH apenas transforma e traduz os dados transmitidos de modo aos mesmos conseguirem ser interpretados pelas aplicações. O SSH foi criado com o intuito de substituir o protocolo TELNET, face aos seus atributos de segurança. Também pode substituir protocolos de transmissão de ficheiros como o FTP.



Figura 2: Protocolo SSH

4.2.3 Para que é utilizado?

O SSH é utilizado para fazer diferentes tipos de conexões de forma segura entre uma máquina local e uma remota, incluindo o acesso remoto, seguro, a recursos, execução remota de comandos, atualizações e outros tipos de tarefas administrativas.

No caso do super-mercado, o protocolo SSH será utilizado para fazer a gestão dos diferentes recursos, a partir da área de administração e da área de IT, de modo a acederem, de forma segura, a todas as outras áreas para fazer transferências de recursos, atualizações e execução de comandos, face ao perfil de Administradores que estas áreas possuem.

A área de IT, através do protocolo SSH, também é capaz de fazer a manutenção de routers e do hardware dos servidores, bem como a manutenção dos sistemas. Desta forma, através deste protocolo, podem ser criados túneis seguros para outros protocolos. Qualquer tipo de ação, desde transferência de ficheiros entre departamentos, navegação na internet, entre outras, é encriptada, tornando as ações privadas.

De forma sucinta, o protocolo SSH, no super-mercado, pode ser utilizado para os seguintes propósitos:

- Manutenção, de forma remota, de servidores, infraestruturas de rede ou computadores de funcionários;

- Fazer transferência de ficheiros entre departamentos, de forma segura (substituindo o FTP);
- Aceder a possíveis serviços na *cloud*, não expondo nenhuma porta da máquina utilizada;
- Conectar remotamente a serviços através de uma rede privada;
- Ultrapassar restrições da *firewall*.

4.2.4 Malware(s) Protegido(s) pelo SSH

Apesar do protocolo SSH não defender a rede, de forma direta, de *malwares*, este protocolo previne e pode mitigar ameaças como ataques *Man-in-the-Middle* e ataques de *spoofing*, face à sua criptografia forte.

A criptografia utilizada pelo protocolo SSH, permite um acesso seguro, de forma remota e por parte das equipas autorizadas, aos servidores da organização. As mesmas equipas, através deste protocolo, são também capazes de configurar, em segurança, equipamentos ou dispositivos, sem terem que se preocupar com ataques *Man-in-the-Middle*, face à criptografia forte do SSH. A utilização de uma chave pública por parte deste protocolo, previne ataques de *brute force*, pois a autenticação desta forma torna o acesso mais difícil por parte de um intruso. Aliada a todas estas medidas, qualquer mensagem transmitida através deste protocolo é totalmente criptografada, impedindo interceções de dados.

4.2.5 Relação com o Cenário (Supermercado)

No contexto do cenário em questão, o protocolo SSH é implementado visando garantir a segurança e eficiência dos sistemas da empresa.

O protocolo SSH seria utilizado pelo departamento de IT de modo a gerir, de forma segura, os recursos essenciais, como, os servidores, isto é, o departamento, através do protocolo SSH será capaz de atualizar, configurar e resolver problemas sem necessidade de aceder fisicamente aos respetivos servidores. A manutenção dos equipamentos de rede, como routers e a própria infraestrutura podem ser geridos através deste protocolo. Por fim, o acesso remoto aos dispositivos dos funcionários é também possível para realizar atualizações ou diagnósticos às respetivas máquinas.

Com a utilização do protocolo SSH, é feita a transferência de ficheiros, de forma segura, entre departamentos da empresa, excluindo assim, a utilização do protocolo FTP, uma opção menos segura.

Com este protocolo, é reduzida a possibilidade de ataques *Man-in-the-Middle*, ou ataques de *Spoofing* à empresa, pois o SSH consegue garantir conexões encriptadas entre sistemas, prevenindo as tentativas de intrusão de utilizadores externos.

4.3 IPSec

4.3.1 O que é?

Na década de 1990 foi desenvolvido pela Internet Engineering Task Force o chamado IPSec que serve para garantir a confidencialidade, integridade e autenticidade dos dados. Nos parágrafos que se seguem será apresentado um resumo do que é o IPSec, como funciona, quais são os seus usos e também que malware o próprio potege numa rede de computadores.

O IPSec trata-se de um conjunto de regras que permite a configuração de conexões seguras numa rede. No fundo o que o IPSec faz é adicionar encriptação e autenticação ao protocolo IP para oferecer uma camada de segurança naquele que é o protocolo padrão e que determina o tráfego dos dados na internet.

4.3.2 Como Funciona?

O IPSec estabelece uma conexão segura ou um túnel que permite a transmissão de dados pela rede, mesmo que esta seja uma rede Wi-Fi pública. Primeiramente o IPSec facilita uma conexão segura que permite a troca de chaves cujo propósito é encriptar e desencriptar dados. Seguido disso os dados são divididos em pacotes onde cada um contém payload e metadados e onde o IPSec cria uma nova camada de segurança através da adição de metadados de segurança na forma de cabeçalhos. O IPSec depois autentica todos os pacotes para verificar a fonte e após autenticar encripta os dados para que a transmissão dos dados possa ocorrer de forma segura. Por fim existe do outro lado uma desencriptação com as chaves inicialmente trocadas de forma a que as aplicações consigam ler os dados.



Figura 3: Protocolo IPSec

4.3.3 Para que é utilizado?

O IPSec pode ser usado para:

- Garantir a segurança do router quando dados são enviados pela internet pública.
- Encriptar os dados da aplicação.
- Caso os dados sejam provenientes de uma origem conhecida, fazer uma rápida autenticação dos dados.

- Os túneis IPSec encriptam todos os dados provenientes de dois endpoints pelo que protegem os dados da rede.

4.3.4 Malware(s) Protegido(s) pelo IPSec

O IPSec é vastamente utilizado nas organizações para prevenir ataques de "*Man-In-The-Middle*" onde os atacantes tentam intercetar e possivelmente alterar uma transmissão que está a ocorrer, reencaminhando os dados para um computador intermediário. Para impedir este tipo de ataques o IPSec atribui um número sequencial a cada pacote de forma a fazer verificações para detetar se certo pacote foi duplicado.

4.3.5 Relação com o Cenário (Supermercado)

A relação que o protocolo IPSec terá com o cenário do Supermercado será na comunicação de dados sensíveis entre as áreas da empresa e os serviços externos, de forma protegida.

Focando o aspeto da existência de uma sucursal da empresa, é necessária fazer a comunicação segura entre a sede e a respetiva sucursal. Deste modo, a utilização do IPSec na criação de VPNs, assegura a transmissão de dados sem que exista a possibilidade dos mesmos serem intercetados durante o processo, como por exemplo, na transmissão de dados de inventários, pedidos de mercadoria ou até atualizações de stock.

Este protocolo também auxiliará nas transações financeiras que o supermercado realizar, seja na transmissão de dados dos terminais de pagamento para o sistema de faturação da empresa, ou até em processos de pagamentos externos, garantido transações seguras.

No sentido da proteção das redes internas da organização, o IPSec servirá como protetor de comunicações entre equipamentos, como servidores e ainda de pontos de acesso Wi-Fi, utilizados, por vezes, por utilizadores. É ainda considerada a ajuda deste protocolo no controlo da comunicação de elementos de segurança físicos da empresa, como câmaras de segurança e gravações que as mesmas enviam.

Por fim, na relação do protocolo com a existência de ataques ou *malwares* à empresa, este, através dos seus métodos de encriptação e autenticação, reduzirá a possibilidade de acesso a máquinas externas à rede da organização e à fuga de dados dos utilizadores ou da própria empresa.

4.4 SSL/TLS

4.4.1 O que é

O protocolo *Secure Sockets Layer* (SSL) e *Transport Layer Security* (TLS), apesar de servirem o mesmo propósito, são bastante distintos. O SSL é um protocolo que cria uma ligação segura entre duas aplicações ou dispositivos em rede. Apesar de se afirmar uma ligação segura, o SSL é uma tecnologia antiga e apresenta algumas vulnerabilidades. Com a necessidade de mitigar este problema, surgiu o TLS, o protocolo que será utilizado pelo supermercado para fazer a comunicação em rede. O TLS é capaz de autenticar, com maior eficiência e oferecer suporte aos canais de comunicação criptografados.

4.4.2 Como Funciona?

O processo de funcionamento destes dois protocolos inicia quando o navegador utiliza um certificado SSL/TLS para iniciar uma conexão segura, através de um *handshake*, SSL/TLS. Este *handshake*, faz parte da tecnologia de comunicação do protocolo *HTTPS*. Esta fase começa pela abertura, por parte do navegador, de um site seguro pelo SSL/TLS e faz a conexão com o servidor web. Após este processo, o navegador, através de informação solicitada, procura verificar a autenticidade do servidor web. De seguida, é enviado um certificado SSL/TLS por parte do servidor web, que contém uma chave pública como resposta. Caso o certificado satisfaça o navegador, este utilizará a chave pública para criptografar e enviar uma mensagem que contenha uma chave de sessão secreta. Seguidamente, o servidor web utiliza a sua chave privada para descriptografar a mensagem e recuperar a chave da sessão. Como passo final, após o servidor web utilizar a chave de sessão para criptografar e enviar uma mensagem de confirmação para o navegador, os dois mudam para a mesma chave de sessão, de modo a trocarem informação de forma segura.

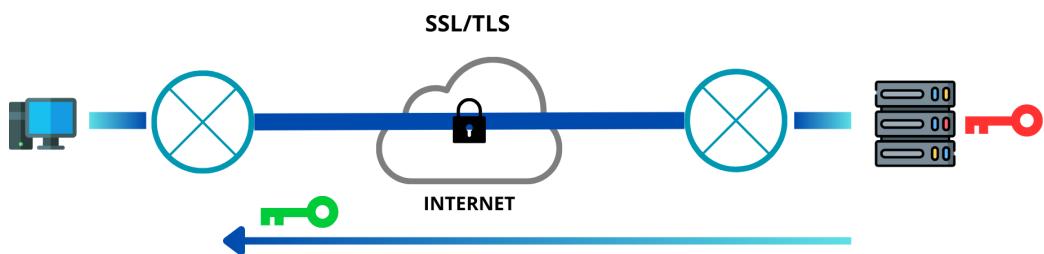


Figura 4: Protocolo SSL/TLS

4.4.3 Para que é utilizado

Tal como indicado acima, de forma detalhada, este protocolo é utilizado para permitir aos sistemas fazer uma verificação de identidade e posteriormente, estabelecer uma ligação segura e encriptada com outro sistema.

No caso do supermercado, este protocolo será utilizado para fazer as comunicações dos diferentes dispositivos da empresa com o servidor, de forma segura e encriptada.

4.4.4 Malware(s) Protegido(s) pelo SSL/TLS

Tal como o seu antecessor, o protocolo TLS protege os sistemas, de forma indireta , de ataques *Man-in-the-Middle*, ataques que exploram o roubo de sessão (*Session Hijacking*) e *malwares* de injecção de pacotes. Com este protocolo bem aplicado, a probabilidade de sofrer um destes ataques reduz significativamente.

Em casos práticos, estas medidas resultam, por exemplo, em transações financeiras seguras, pois as mesmas encontrar-se-ão criptografadas. Não existirá qualquer tipo de exposição dos dados ou credenciais dos clientes, caso os mesmos decidam realizar, por exemplo, pagamentos online, face a esta mesma criptografia disponibilizada pelo TLS. De forma interna, este protocolo protege na transmissão de dados entre os servidores da empresa.

4.4.5 Relação com o Cenário (Supermercado)

O protocolo TLS em complemento com o protocolo anterior (IPSec), auxiliará na proteção da comunicação de dados sensíveis da empresa e dos seus cliente, face às suas características de encritpação e integridade de informações transmitidas.

Este protocolo será responsável pela segurança das transações de pagamentos da empresa, isto é, qualquer transação efetuada num terminal de pagamento, será abordada por este protocolo, garantido assim que existe encriptação nos dados financeiros dos clientes, com por exemplo, as informações dos cartões bancários, impedindo assim que estes dados sensíveis sejam intercetados por um atacante.

O TLS também irá proteger os clientes nos serviços online da empresa, em concreto, nas situações de compra online. O protocolo será utilizado também pela equipa de IT em momentos de gestão de serviços web internos da empresa. A administração da empresa poderá também fazer uso deste protocolo, quando pretenderem fazer a gestão ou consulta de inventários.

Apesar de não fazer parte do cenário descrito, se os supermercados oferecerem Wi-Fi público aos seus clientes, é crucial a implementação deste protocolo, no sentido em que o mesmo protegerá as conexões dos clientes, caso os mesmos tentem efetuar pesquisas ou transações nestes locais.

Por fim, relacionando o TLS com os possíveis ataques ou *malwares*, entende-se que o mesmo previna o sistema de sofrer intrusões face à sua encriptação de dados, autenticação de serviços e verificação de certificados digitais, de modo a garantir a identidade dos serviços acedidos.

4.5 Firewall

4.5.1 O que é?

Uma *firewall* é um dispositivo ou *software* que separa uma rede interna "de confiança" de uma rede externa na qual não se confia, no caso, a internet. Este sistema monitoriza e controla o tráfego na rede, com base em algumas regras de segurança definidas previamente. Deste conceito surge o termo que categoriza a *firewall* como um escudo que protege uma rede interna de acessos não autorizados e atividades ou ameaças maliciosas, por parte de atacantes externos a esta rede.

Na figura 2, é possível visualizar, na forma de um esboço, o funcionamento de uma *firewall*, numa situação de exemplo.

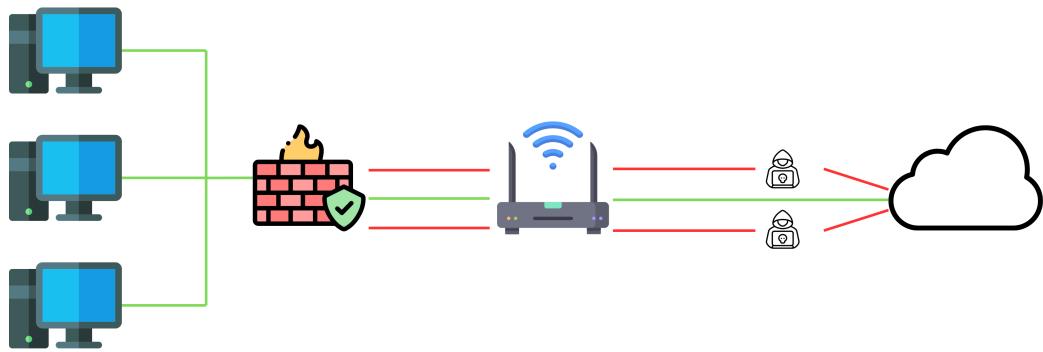


Figura 5: Firewall

4.5.2 Ponto de Ação da Firewall?

Para demonstrar o ponto de ação da *Firewall* na topologia de rede do cenário do supermercado, foi elaborado um pequeno esboço (*Figura 3*) para visualizar a zona de atuação deste dispositivo.

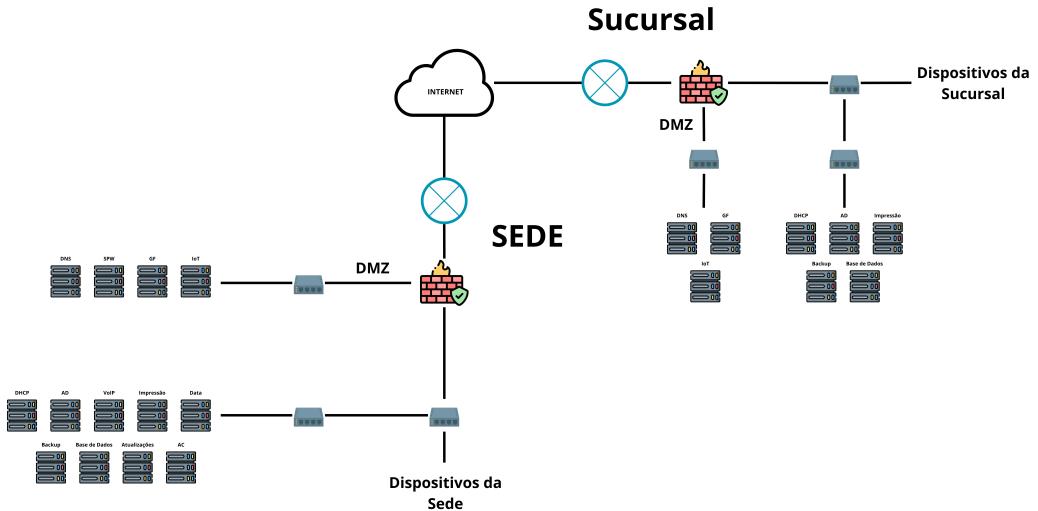


Figura 6: Ponto de Ação da *Firewall*

Observando a *Figura 3*, conclui-se que são utilizadas duas *Firewalls*, uma na Sede da empresa e outra na Sucursal. A opção de colocar a *Firewall* logo após o *router*, baseia-se, em parte, no facto da mesma não ser sobrecarregada com dados desnecessários, que serão filtrados pelo *router* que por sua vez, também será capacitado de uma *firewall* (como software). Isto faz com que o tráfego abordado pela *firewall* externa seja reduzido, aumentando o seu desempenho e eficácia.

Numa abordagem seguinte, verificamos a utilização de uma DMZ (*Demilitarized Zone*), tanto na Sede como na Sucursal. No caso da Sede, esta zona será provida de um *switch* que ligará todos os servidores da organização que necessitem de acesso externo, sendo estes, o servidor de DNS, o servidor de Página Web, o servidor Gestor de Ficheiros e o Servidor dos IoT. É feita uma separação destes servidores devido à sua necessidade de contacto com redes externas, que torna estes equipamentos mais propícios a ataques e desta forma, é necessária mais atenção. Por outro lado, é feita uma ligação normal da *firewall* a um *switch*, que por sua vez ligar-se-á a dois outros *switches*, um que se conecta com os servidores internos à rede e o outro que fará a ligação aos diferentes departamentos. Concluído o caso da Sede, passa-se à estrutura da Sucursal que seguirá os mesmos princípios da Sede, sofrendo apenas uma alteração na alocação dos servidores, onde são descartados aqueles que não são necessários.

4.5.3 Tipo de *Firewall* utilizado?

De acordo com o cenário e necessidades da empresa, foram levantadas diversas questões relacionadas com o tipo de *Firewall* a ser utilizado. Após uma discussão, decidiu-se que tanto na Sede, como na Sucursal, seriam implementadas *Firewalls* do tipo *Stateful*. Deste modo, o servidor DHCPv6 da empresa, seria responsável pela atribuição e controlo dos endereços de IP dos diferentes dispositivos, bem como as suas configurações. A seleção deste tipo de *Firewall* para ambas as estruturas acontece devido ao funcionamento independente da sucursal, face à sede.

As vantagens que esta abordagem traria, passam pela possibilidade de controlo total por parte dos administradores sobre a atribuição dos endereços de IP, uma fácil monitorização e manutenção e a possibilidade de configurar, de forma completa e detalhada, os dispositivos da organização.

Apesar dos pontos positivos, tem-se em conta algumas das desvantagens que esta abordagem proporciona, como a complexidade de utilização, face à necessidade de gestão de um servidor e a dependência total do mesmo, isto é, se o servidor falhar, os dispositivos podem sofrer consequências, como perda de configurações ou conectividade. Para combater estes problemas, um plano de recuperação à perda é obrigatório.

4.5.4 O que vai ser permitido?

De forma a tornar a infraestrutura de rede o mais segura possível, foram criadas algumas regras para os diferentes utilizadores e dispositivos partilharem informação e dados de forma segura. Assim, no ponto de vista do tráfego interno à organização, é essencial permitir a comunicação entre dispositivos e servidores internos. Como exemplo, os funcionários devem conseguir aceder ao AD para se conseguirem autenticar, devem conseguir aceder ao servidor de ficheiros para partilhar ou armazenar documentos e devem ainda conseguir aceder à base de dados e DNS e DHCP, de modo a serem capazes de realizar tarefas nas aplicações comerciais ou atribuição de IPs. O acesso ao VoIP e à impressão é também fundamental para os funcionários comunicarem internamente. Por fim, relacionado aos dispositivos IoT e sistemas internos, deve ser permitida a comunicação entre o servidor para este efeito e os dispositivos com acesso.

No ponto de vista externo à empresa, ou seja, internet e DMZ, os funcionários devem ser capazes de aceder à internet, no entanto, de forma controlada, bloqueando acesso a websites não permitidos pela empresa. O tráfego externo será apenas permitido para os servidores que se encontram na DMZ, neste tráfego incluem-se, o website da empresa, e possíveis atualizações ou *patches* de segurança. A *Firewall* deve ainda permitir a comunicação com entre a sede e a sucursal da empresa, mas sempre com recurso a uma VPN, que será explicada no ponto 4.7 do documento. Para restringir o acesso remoto aos servidores, a *Firewall* deve apenas permitir a equipa de IT, com IPs autorizados a aceder remotamente aos servidores da organização. Por fim, deve ser permitida a comunicação entre os servidores de *backup*, de modo a tornar a recuperação de uma possível perda de informação, mais

simples.

Além das permissões, é necessário ter em conta regras de bloqueio e restrições de acessos à rede da empresa. Assim, estabelece-se que qualquer tentativa de acesso, externo à rede, não autorizado, deve ser bloqueado. Não deverá ser permitida, também, a utilização de protocolos inseguros tais como, Telnet e FTP sem encriptação. Por fim, a *Firewall* conterá regras de deteção de ataques DoS e tentativas de intrusão, de modo a mitigar estas ameaças.

Na tabela 1 podemos verificar as regras num formato mais conciso.

Origem	Destino	Protocolo	Estado
Rede Interna	Internet	HTTPS, DNS	Permitido com Restrições
Internet	Rede Externa (DMZ)	HTTPS	Permitido com Restrições
Sede	Sucursal	VPN IPsev	Permitido
Administradores e IT	Servidores	SSH, VPN	Permitido
Internet	Rede Interna	Qualquer	Bloqueado

Tabela 1: Restrições da *Firewall*

4.5.5 Qual o fluxo de tráfego permitido?

O fluxo de tráfego permitido pela empresa, de modo a tornar o ambiente de rede o mais seguro possível, deve apenas permitir apenas comunicações essenciais, para isto, apenas equipas ou indivíduos com cargos para uma gestão mais aprofundada da rede devem de ter privilégios maiores. De acordo com o cenário em questão, o tráfego passará apenas pela rede interna da empresa, rede externa, seja internet ou DMZ e a comunicação entre a sede e sucursal. De forma a apresentar o fluxo permitido foi criada a tabela 2 para auxiliar na interpretação. De notar que as regras se aplicam da mesma forma à Sede da empresa e à Sucursal.

Origem	Destino	Protocolo	Porta	Estado
Dispositivos IoT	Internet	Qualquer	-	Bloqueado
VLANs Diferentes	Qualquer	Qualquer	-	Bloqueado (Exceto Casos Específicos)
Rede Interna	Servidores Internos	AD, DNS, DHCP, Ficheiros	389, 636, 53, 445	Permitido
IoT	Servidor IoT	MQTT, HTTPS	1883, 443	Permitido
Computadores Internos	Internet	HTTPS, DNS	443, 53	Permitido
Clientes Externos	Servidor Web	HTTPS	443	Permitido
Sede	Sucursal	VPN IPSec	500, 4500	Permitido
Backup Sucursal	Backup Sede	SFTP	22	Permitido
Administradores	Rede Interna	SSH, RDP, VPN	22, 3389	Permitido (Apenas IT)
Qualquer	Qualquer	Qualquer	-	Bloqueado (Padrão)

Tabela 2: Fluxo Permitido Final e Otimizado

4.5.6 Malware(s) Protegido(s) pela Firewall

A *Firewall* é uma ferramenta essencial para a defesa da estrutura e sistema da organização. O bloqueio do tráfego não autorizado e as regras definidas podem defender de ataques de *Ransomware* e *Worms*. O bloqueio de portas não utilizadas pela *Firewall* impedem a propagação de *worms* pelo sistema.

O bloqueio de tentativas de conexões suspeitas à rede da organização permite uma melhor defesa contra ataques *Trojans*. A análise de *Firewalls* com capacidade para identificar *malwares* já conhecidos, também contribui para este efeito. Aliado a este conceito, o bloqueio de certas conexões também permite prevenir contra ataques DDoS e até contra *Exploits*.

4.6 IDS/IPS

4.6.1 O que é?

O IDS, tal como o nome indica, *Intrusion Detection System*, é um sistema de deteção de intrusões. Este sistema monitoriza o tráfego na rede e procura por padrões ou identificadores de ataques já conhecidos e quando deteta algo suspeito, emite um alerta. Após este alerta, o tráfego continua.

IPS, *Intrusion Prevention System*, é um sistema de prevenção contra intrusões, que também monitoriza o tráfego na rede, no entanto, a diferença para o IDS é que este, ao detetar algo suspeito, pára o tráfego até existir intervenção do ser humano em relação a este alerta.

4.6.2 Ponto de Ação do IDS e IPS

No nosso cenário o IDS e IPS encontra-se localizado após a *Firewall* porque permite assim analisar o tráfego que já passou por uma filtragem inicial. Com este posicionamento um possível ataque que tenha atravessado a *Firewall* pode ser detetado e bloqueado antes de chegar a afetar os dispositivos conectados à rede. Assim, a rede garante uma deteção precoce de ameaças e neutralização de possíveis ataques antes destes causarem danos.

4.6.3 Malware(s) Protegido(s) pelo IPS/IDS

O IDS e IPS, diferente da *Firewall* que se limita a bloquear tráfego com base nas regras previamente definidas, analisam comportamentos ditos suspeitos e padrões de ataque de forma a detetar e mitigar ameaças que podem comprometer a rede.

Com base no funcionamento do IDS e IPS, estes conseguem prevenir alguns ataques como *DDoS*, *Ransomware*, ataques *Zero-Day*, ataques de *Phishing*, *Lateral Movement*, ataques de *Code Injection* e também *Botnets*. Os ataques *DDoS* são encontrados através da deteção de um número elevado de solicitações com origem em várias fontes e podem bloquear os endereços IP considerados maliciosos. No que toca a *Ransomware* é identificado qualquer comportamento que possa ser suspeito como por exemplo a encriptação em massa de ficheiros e permite bloquear a infeção antes que o *Ransomware* se espalhe. Para a deteção de ataques *Zero-Day* é monitorizado o tráfego da rede enquanto se procura por assinaturas de ataques conhecidos e são bloqueadas tentativas de exploração de vulnerabilidades em sistemas não atualizados. Os ataques de *Phishing* são detetados por tentativas de redirecionamento para sites que possam ser fraudulentos. No que toca ao *Lateral Movement* são identificadas tentativas de um atacante comprometer vários dispositivos dentro da rede. O IDS e IPS é capaz de analisar pedidos HTTP e detetar padrões que indicam injeção de código malicioso em aplicações web, fazendo assim a deteção de ataques de *Code Injection*. Por fim os *Botnets* é identificado tráfego de rede característico de máquinas que foram infetadas e pertencem a redes de bots controladas por atacantes.

4.6.4 Relação com o Cenário (Supermercado)

A implementação do IDS e IPS no contexto do supermercado é fundamental devido a monitorizar os servidores de bases de dados, gestão de stock e faturação e impedir possíveis ataques. Para além disso é garantido que nenhum tráfego malicioso passe despercebido na comunicação entre a sede e a sucursal, além de prevenir os ataques referidos anteriormente.

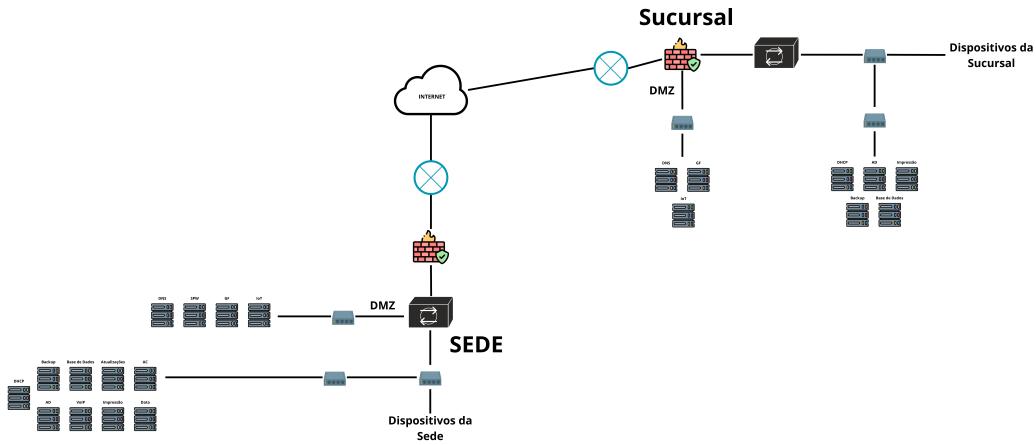


Figura 7: Ponto de Ação dos IDS/IPS

4.7 VPN

4.7.1 O que é?

Uma VPN, *Virtual Private Network*, é uma conexão encriptada, sobre a internet, entre dois dispositivos. É estabelecida uma conexão digital entre um computador e um servidor remoto, controlado por um provedor de VPN, criando um túnel ponto-a-ponto, que encripta os dados pessoais do utilizador, máscara o endereço IP do mesmo e permite contornar websites bloqueados e *firewalls* na internet. Esta tecnologia assegura uma experiência online privada, protegida e mais segura.

4.7.2 Ponto de Ação da VPN

No que toca ao ponto de ação da VPN estará situada no router que se encontra antes da *Firewall*. A colocação da VPN neste local permite que o tráfego que chega à rede interna seja protegido antes de chegar à *Firewall*, pelo que com o posicionamento da VPN antes da *Firewall* todo o tráfego será autenticado e encriptado no ponto de entrada da rede e dessa forma a *Firewall* não tem que lidar com o conteúdo não encriptado, reduzindo a carga da *Firewall*.

Para além disso esta posição permite centralizar e controlar o acesso remoto de forma mais organizada permitindo a todos os dispositivos remotos a autenticação e estabelecimento de uma conexão segura através da VPN, além de ser possível gerir conexões externas visto que a *Firewall* pode ser configurada de modo a permitir ou negar conexões específicas de acordo com a sua origem.

Por fim existe também a vantagem de minimizar o risco de *Data Leaks* sendo que todo o tráfego externo não vai ser processado sem estar protegido por encriptação.

4.7.3 Malware(s) Protegido(s) pela VPN

A VPN oferece uma camada de proteção contra vários tipos de malware e ataques informáticos como por exemplo *Packet Sniffing*, *Packet Injection*, *Ransomware* (via exploração de conexões remotas) e *Spyware* e *Keyloggers* baseados em rede. O *Packet Sniffing* trata-se da captura de pacotes em redes, que é contrariado com a VPN sendo que esta encapsula e encripta os pacotes tornando os dados inúteis para os atacantes. Os ataques de *Packet Injection* são ataques cujo objetivo é modificar pacotes de dados antes da chegada ao destino. A exploração de conexões remotas desprotegidas pode ser usada por algumas variantes de *Ransomware* de forma a que estes se infiltram na rede empresarial. E por fim o *Spyware* e os *Keyloggers* baseados em rede tentam a obtenção de informações que possam ser sensíveis através da monitorização do tráfego da rede, no entanto como a VPN oculta este tráfego, a missão destes tipos de malware é dificultada.

4.7.4 Relação com o Cenário (Supermercado)

No que toca a relação com o cenário em causa, a implementação da VPN é fulcral para garantir a segurança das comunicações entre a sede, sucursal e o ambiente remoto.

Tendo em conta as informações que circulam constantemente na infraestrutura da empresa a VPN garante a segurança de tais informações assim como permite que os funcionários administrativos e da área do IT accedam aos sistemas internos do supermercado sem risco de expôr os dados na internet pública. Para além disso os terminais de pagamento trocam informações com o sistema de faturação que precisa de ser mantida em segurança para impedir que os dados bancários dos clientes sejam interceptados por possíveis ataques. A transmissão de dados entre a sede e a sucursal também precisa de ser mantida em segurança e encriptada assim como o acesso a servidores e bases de dados. Por fim, os dispositivos IoT como sensores de temperatura, câmeras de segurança e outros que possam existir no supermercado benficiam da VPN para reduzir a exposição a malwares direcionados a estes dispositivos.

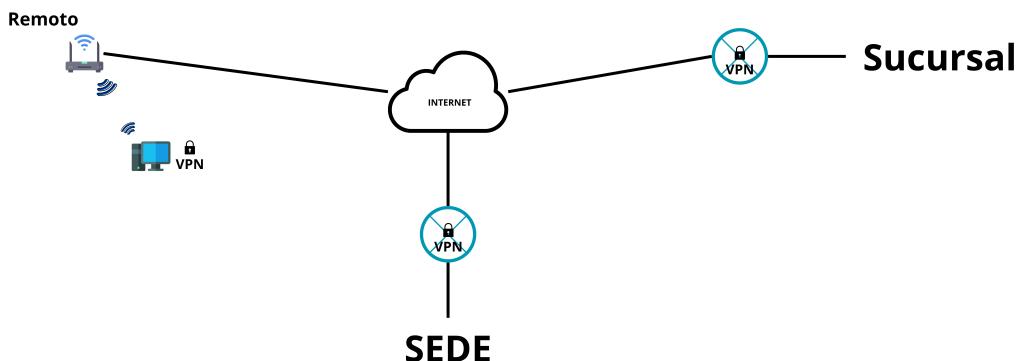


Figura 8: Ponto de Ação da VPN

4.8 Desenho com Dispositivos de Segurança

Após a especificação dos dispositivos e medidas de segurança optadas para o cenário do supermercado, foi elaborada uma atualização no desenho da rede visto na Figura 1.

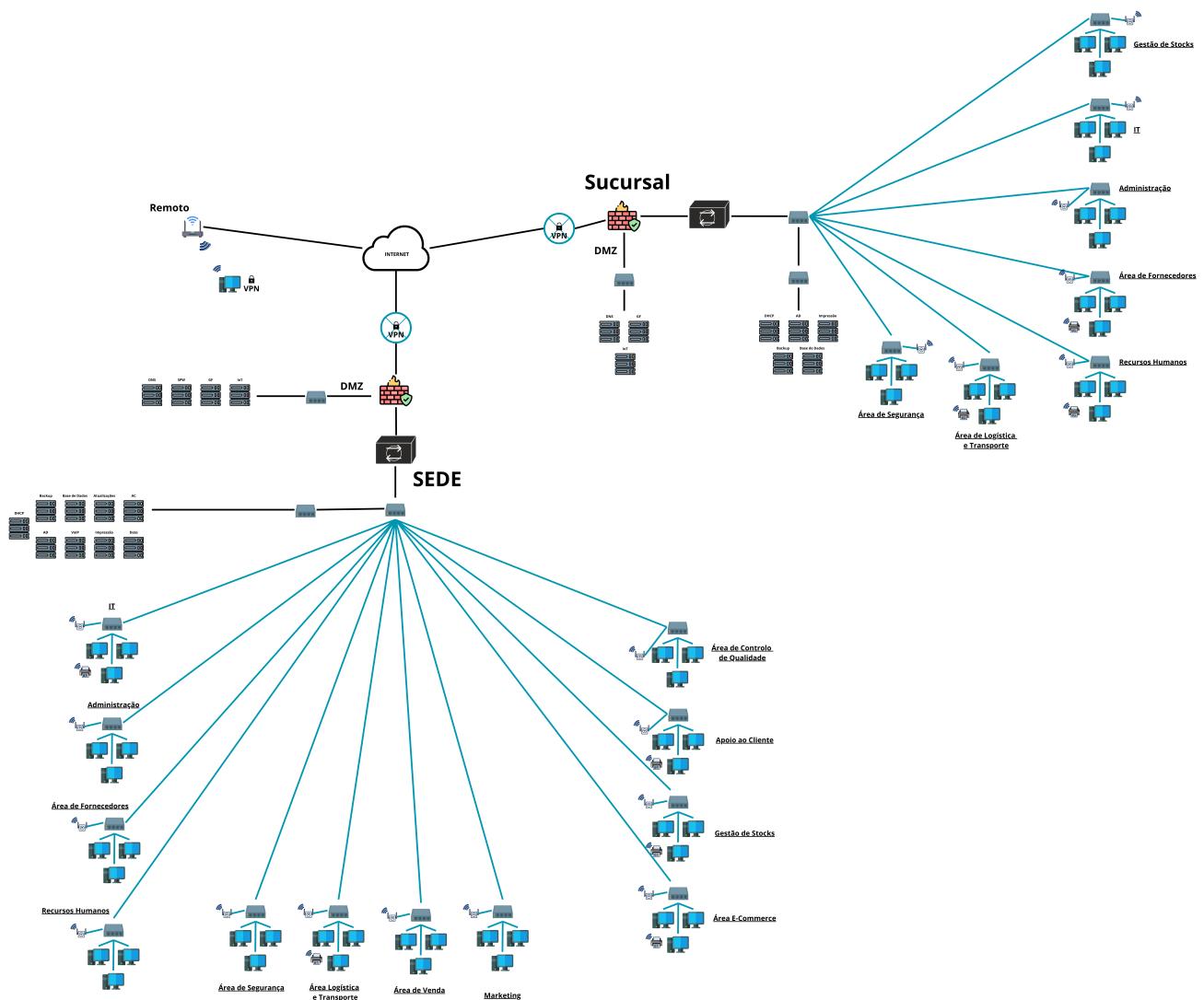


Figura 9: Desenho da Rede com Dispositivos de Segurança

5 Servidores

Nesta secção foram enumerados os servidores usados e fornecida uma breve descrição do propósito de cada um.

5.1 DNS

- Este servidor resolve os nomes de domínio nos endereços IP e vice-versa, o que facilita o acesso a sistemas internos e externos através do uso de nomes mais amigáveis e é essencial para a comunicação entre dispositivos na rede.

5.2 DHCP

- Automatiza a atribuição de endereços IP, máscaras de sub-rede, gateways e garante que dispositivos ligados à rede como terminais de ponto de venda, computadores, impressoras e dispositivos IoT recebam as configurações de rede sem intervenção manual

5.3 AD

- Centraliza a autenticação e autorização de utilizadores, dispositivos e serviços numa rede oferecendo diretórios para organizar e gerir recursos. Este servidor controla quem possa aceder a diferentes áreas da rede como ficheiros, sistemas ou aplicações específicas. Também implementa políticas de segurança como bloqueios de ecrã automáticos ou restrições de acesso a dispositivos USB.

5.4 Servidor Página Web (SPW)

- Serve para dar host a páginas web que são acessíveis internamente ou externamente e suporta sistemas internos acessíveis via web como intranet, ferramentas de gestão de stock ou relatórios de vendas.

5.5 Gestor de Ficheiros (GP)

- Armazena, organiza e distribui ficheiros numa rede o que facilita a partilha de documentos entre departamentos como por exemplo listas de stock, relatórios financeiros e políticas de RH.

5.6 Servidor de IoT (IoT)

- Faz a gestão de dispositivos IoT conectados na rede do supermercado assim como sensores de temperatura, câmeras de segurança, entre outros.

5.7 Servidor de Backup (Backup)

- Armazena cópias de segurança de dados críticos como ficheiros, bases de dados e configurações do sistema.

5.8 Servidor de Base de Dados (Base de Dados)

- Gere e armazena informações como dados de clientes.

5.9 Servidor de Atualizações (Atualizações)

- Centraliza e distribui atualizações de sistemas operativos e softwares.

5.10 Servidor de Aplicações Comerciais (AC)

- Serve para hospedar sistemas como software de gestão de stock, sistemas de ponto de venda, entre outros.

5.11 Servidor de VoIP (VoIP)

- Suporta comunicações telefónicas baseadas em IP o que reduzirá os custos de telecomunicação.

5.12 Servidor de Impressão (Impressão)

- Serve para centralizar a gestão de impressoras e consequentes filas de impressão.

5.13 Servidor de Análise de Dados (Data)

- Usado para processar grandes volumes de dados que posteriormente serão analisados para compreender o comportamento dos clientes e tendências atuais.

6 Níveis de Credenciais e Políticas de Acesso

Através da definição de níveis de credenciais e da existência de políticas de acesso bem estruturadas podemos garantir a segurança da informação do nosso cenário. Adotamos o princípio do menor privilégio para que cada utilizador tenha as permissões necessárias apenas para desempenhar a sua função. Minimizando os riscos de acessos indevidos e ameaças à rede.

Com a implementação de tais níveis de credenciais e políticas de acesso garantimos que os utilizadores não tenham acesso indevido a informação que pode ser sensível, para além de que garantir que a empresa minimize o risco de possíveis ataques ou até falhas humanas.

Definimos três níveis de acesso para os utilizadores:

6.1 Níveis de Credenciais

Nível de Credencial	Descrição	Permissões
Total	Acesso irrestrito a toda a infraestrutura e dados da empresa.	Gestão completa de servidores, firewalls, IDS/IPS, VPN, credenciais e logs.
Intermédio	Acesso concedido a funcionários que precisam de permissões adicionais para cumprir a sua função	Gestão de utilizadores dentro do departamento, acesso a bases de dados e sistemas do seu departamento em específico no entanto sem acesso a configurações de rede ou dados sensíveis de outros departamentos.
Mínimo	Acesso mínimo onde apenas é possível interagir com sistemas que são essenciais ao seu trabalho	Acesso apenas aos serviços necessários e sem permissões para ver ou alterar outros dados.

Tabela 3: Níveis de Credenciais

6.2 Políticas de Acesso

Com o intuito de reforçar a segurança aplicamos políticas de acesso que evitam acessos indevidos e fazem o controlo de acesso.

6.2.1 Autenticação

- Autenticação Multi-Fatorial (2FA) obrigatória para todos os utilizadores com acesso total ou intermediário.

- Palavras-passe com um mínimo de 12 caracteres e renovação obrigatória num período de tempo.
- Conta bloqueada após errar cinco tentativas da palavra-passe.

6.2.2 Monitorização

- Todas as atividades realizadas por utilizadores com acesso total ou intermédio devem ser registadas.
- Logs de acesso guardados durante 6 meses para fins de auditorias e investigações.
- Para tentativas de acesso suspeitas existir alertas automáticos.

6.2.3 Controlo de Sessão

- Sesões encerradas automaticamente após 10 minutos de inatividade.
- Para aceder a sistemas críticos o dispositivo tem de ser registado.
- Para evitar *Data Leaks* as portas USB são desativadas.

6.2.4 Segmentação

- Acesso a servidores limitado por função e área.
- Comunicação entre áreas deve ser controlada e registada.
- Para acessos remotos a utilização de VPN é obrigatória.

7 Plano de Endereços IPV6

Nesta secção do documento, são apresentadas as tabelas 5 e 6 que contém os planos de endereços IPV6 dirigidos ao cenário do super-mercado. É atribuído um endereço específico a cada equipamento, considerando sempre a divisão entre locais e departamentos.

Lista de Endereços Sede	
Equipamento	Endereço IPV6
Router_Sede	9999:8888:7777::/48
Switch_Servers_Sede	-
Server_DNS	9999:8888:7777:0001::1/64
Server_DHCP	9999:8888:7777:0001::2/64
Server_AD	9999:8888:7777:0001::3/64
Server_SPW	9999:8888:7777:0001::4/64
Server_GF	9999:8888:7777:0001::5/64
Server_IoT	9999:8888:7777:0001::6/64
Server_Backup	9999:8888:7777:0001::7/64
Server_BD	9999:8888:7777:0001::8/64
Server_Updates	9999:8888:7777:0001::9/64
Server_AC	9999:8888:7777:0001::a/64
Server_VoIP	9999:8888:7777:0001::b/64
Server_Printer	9999:8888:7777:0001::c/64
Server_Data	9999:8888:7777:0001::d/64

Área IT	
Equipamento	Endereço IPV6
Switch_IT	-
PC_IT1	9999:8888:7777:0002::2/64
PC_IT2	9999:8888:7777:0002::3/64
PC_IT3	9999:8888:7777:0002::4/64
AP_IT	9999:8888:7777:0002::5/64
Printer_IT	9999:8888:7777:0002::6/64

Área Administração	
Equipamento	Endereço IPV6
Switch_ADMIN	-
PC_ADMIN1	9999:8888:7777:0003::2/64
PC_ADMIN2	9999:8888:7777:0003::3/64
PC_ADMIN3	9999:8888:7777:0003::4/64
AP_ADMIN	9999:8888:7777:0003::5/64

Área Fornecedores	
Equipamento	Endereço IPV6
Switch_FORN	-
PC_FORN1	9999:8888:7777:0004::2/64
PC_FORN2	9999:8888:7777:0004::3/64
PC_FORN3	9999:8888:7777:0004::4/64
AP_FORN	9999:8888:7777:0004::5/64

Área Recursos Humanos	
Equipamento	Endereço IPV6
Switch_RH	-
PC_RH1	9999:8888:7777:0005::2/64
PC_RH2	9999:8888:7777:0005::3/64
PC_RH3	9999:8888:7777:0005::4/64
AP_RH	9999:8888:7777:0005::5/64

Área Segurança	
Equipamento	Endereço IPV6
Switch SEG	-
PC_SEG1	9999:8888:7777:0006::2/64
PC_SEG2	9999:8888:7777:0006::3/64
PC_SEG3	9999:8888:7777:0006::4/64
AP_SEG	9999:8888:7777:0006::5/64

Área Logística e Transporte	
Equipamento	Endereço IPV6
Switch_LOG_TRA	-
PC_LOG_TRA1	9999:8888:7777:0007::2/64
PC_LOG_TRA2	9999:8888:7777:0007::3/64
PC_LOG_TRA3	9999:8888:7777:0007::4/64
AP_LOG_TRA	9999:8888:7777:0007::5/64
Printer_LOG_TRA	9999:8888:7777:0007::6/64

Área Venda	
Equipamento	Endereço IPV6
Switch_VENDA	-
PC_VENDA1	9999:8888:7777:0008::2/64
PC_VENDA2	9999:8888:7777:0008::3/64
PC_VENDA3	9999:8888:7777:0008::4/64
AP_VENDA	9999:8888:7777:0008::5/64

Área Marketing	
Equipamento	Endereço IPv6
Switch_MARKETING	-
PC_MARKETING1	9999:8888:7777:0009::2/64
PC_MARKETING2	9999:8888:7777:0009::3/64
PC_MARKETING3	9999:8888:7777:0009::4/64
AP_MARKETING	9999:8888:7777:0009::5/64
Área Ecommerce	
Equipamento	Endereço IPv6
Switch_ECOMMERCE	-
PC_ECOMMERCE1	9999:8888:7777:000a::2/64
PC_ECOMMERCE2	9999:8888:7777:000a::3/64
PC_ECOMMERCE3	9999:8888:7777:000a::4/64
AP_ECOMMERCE	9999:8888:7777:000a::5/64
Printer_ECOMMERCE	9999:8888:7777:000a::6/64
Área Gestão de Stocks	
Equipamento	Endereço IPv6
Switch_GEST_STOCKS	-
PC_GEST_STOCKS1	9999:8888:7777:000b::2/64
PC_GEST_STOCKS2	9999:8888:7777:000b::3/64
PC_GEST_STOCKS3	9999:8888:7777:000b::4/64
AP_GEST_STOCKS	9999:8888:7777:000b::5/64
Printer_GEST_STOCKS	9999:8888:7777:000b::6/64
Área Apoio ao Cliente	
Equipamento	Endereço IPv6
Switch_AP_CLI	-
PC_AP_CLI1	9999:8888:7777:000c::2/64
PC_AP_CLI2	9999:8888:7777:000c::3/64
PC_AP_CLI3	9999:8888:7777:000c::4/64
AP_AP_CLI	9999:8888:7777:000c::5/64
Printer_AP_CLI	9999:8888:7777:000c::6/64
Área Controlo de Qualidade	
Equipamento	Endereço IPv6
Switch_CONTROL_QUAL	-
PC_CONTROL_QUAL1	9999:8888:7777:000d::2/64
PC_CONTROL_QUAL2	9999:8888:7777:000d::3/64
PC_CONTROL_QUAL3	9999:8888:7777:000d::4/64
AP_CONTROL_QUAL	9999:8888:7777:000d::5/64

Tabela 4: Tabela de Endereços da Sede

Lista de Endereços Sucursal	
Equipamento	Endereço IPV6
Router_Sucursal	-
Server_DNS	9999:8888:6666:0001::1/64
Server_GF	9999:8888:6666:0001::2/64
Server_IoT	9999:8888:6666:0001::3/64
Server_DHCP	9999:8888:6666:0001::4/64
Server_AD	9999:8888:6666:0001::5/64
Server_Printer	9999:8888:6666:0001::6/64
Server_Backup	9999:8888:6666:0001::7/64
Server_BD	9999:8888:6666:0001::8/64
Área IT Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_IT	-
PC_SUC_IT1	9999:8888:6666:0002::2/64
PC_SUC_IT2	9999:8888:6666:0002::3/64
PC_SUC_IT3	9999:8888:6666:0002::4/64
AP_SUC_IT	9999:8888:6666:0002::5/64
Área Administração Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_ADMIN	-
PC_SUC_ADMIN1	9999:8888:6666:0003::2/64
PC_SUC_ADMIN2	9999:8888:6666:0003::3/64
PC_SUC_ADMIN3	9999:8888:6666:0003::4/64
AP_SUC_ADMIN	9999:8888:6666:0003::5/64
Área Stocks Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_STOCKS	-
PC_SUC_STOCKS1	9999:8888:6666:000b::2/64
PC_SUC_STOCKS2	9999:8888:6666:000b::3/64
PC_SUC_STOCKS3	9999:8888:6666:000b::4/64
AP_SUC_STOCKS	9999:8888:6666:000b::5/64

Área Fornecedores Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_FORN	-
PC_SUC_FORN1	9999:8888:6666:0004::2/64
PC_SUC_FORN2	9999:8888:6666:0004::3/64
PC_SUC_FORN3	9999:8888:6666:0004::4/64
AP_SUC_FORN	9999:8888:6666:0004::5/64

Área Recursos Humanos Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_RH	-
PC_SUC_RH1	9999:8888:6666:0005::2/64
PC_SUC_RH2	9999:8888:6666:0005::3/64
PC_SUC_RH3	9999:8888:6666:0005::4/64
AP_SUC_RH	9999:8888:6666:0005::5/64

Área Logística e Transporte Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_LOG_TRA	-
PC_SUC_LOG_TRA1	9999:8888:6666:0007::2/64
PC_SUC_LOG_TRA2	9999:8888:6666:0007::3/64
PC_SUC_LOG_TRA3	9999:8888:6666:0007::4/64
AP_SUC_LOG_TRA	9999:8888:6666:0007::5/64

Área Segurança Sucursal	
Equipamento	Endereço IPV6
Switch_SUC_SEG	-
PC_SUC_SEG1	9999:8888:6666:0006::2/64
PC_SUC_SEG2	9999:8888:6666:0006::3/64
PC_SUC_SEG3	9999:8888:6666:0006::4/64
AP_SUC_SEG	9999:8888:6666:0006::5/64

Tabela 5: Tabela de Endereços da Sucursal

Lista de Endereços Remoto	
Equipamento	Endereço IPV6
Router_Remoto	9999:8888:5555::/48
PC_Remoto	9999:8888:5555:0001::1/64

Tabela 6: Tabela de Endereços do Trabalho Remoto

8 Técnicas de Rede

8.1 Switches

De forma a criar uma outra camada de segurança e proteger ainda mais a nossa rede, existem algumas medidas e soluções que podemos adotar para os nossos switches de forma a que estes previnam ataques e acessos não autorizados aos dispositivos por eles geridos.

8.1.1 Medidas de Segurança

- **Segmentação da Rede com VLANs** - A implementação de VLANs nas portas físicas do router é feita para isolar os diferentes tipos de tráfego, impedindo que os dispositivos IoT inseguros possam ter acesso a serviços críticos.
- **Utilização da Firewall** - A firewall assume o controlo de quem pode aceder ao que, como já referido nos capítulos passados, reduzindo o risco de acessos não autorizados e protegendo informações sensíveis.
- **Controlo de endereço MAC no Servidor DHCP** - O servidor DHCP pode restringir quais dispositivos podem obter um IP na rede, através do controlo do endereço MAC, garantindo assim que apenas dispositivos confiáveis operem na rede e evitando conexões não autorizadas.

Como regra universal para proteger todos os switches utilizamos a filtragem de endereços MAC no servidor DHCP que, como referido anteriormente, permite conexões apenas aos dispositivos previamente autorizados o que reforça a segurança dos switches.

8.2 ACL

8.2.1 Regras ACL para a Sede

Origem	Destino	Serviço/Protocolo	Ação
Rede Administrativa	Servidor AD/DNS	LDAP, DNS (53/UDP)	Permitir
Rede Interna	Internet	HTTP/HTTPS (80,443)	Permitir
IoT	Rede Administrativa	Qualquer	Bloquear
Qualquer	Firewall	Telnet (23)	Bloquear

Tabela 7: Regras ACL para a Sede

8.2.2 Regras ACL para a Sucursal

Origem	Destino	Serviço/Protocolo	Ação
Sucursal	Sede	IPSec (ESP, ISAKMP)	Permitir
Sucursal	Servidor DNS da Sede	DNS (53)	Permitir
IoT na Sucursal	Servidores Internos	Qualquer	Bloquear

Tabela 8: Regras ACL para a Sucursal

8.2.3 Regras ACL para o Acesso Remoto

Origem	Destino	Serviço/Protocolo	Ação
Internet (Remoto)	Firewall VPN	VPN SSL (443)	Permitir
Qualquer IP Externo	Rede Interna	Qualquer	Bloquear

Tabela 9: Regras ACL para o Acesso Remoto

9 Backups

Nesta secção, será apresentado o plano de *backup* definido pelos arquitetos de rede, que procura transmitir a forma como são mantidas as configurações dos dispositivos intermédios da empresa, incluíndo Sede e Sucursal e como serão mantidos os dados operacionais da organização.

9.1 Tipos de Backup

Para percebermos que tipo de plano de *backup* irá ser utilizado no nosso cenário, primeiro precisamos de entender que tipos de *backup* existem.

- **Backup Normal** - Neste tipo de *backups* todos os ficheiros selecionados são copiados, o que torna este o tipo de *backup* mais demorado e que exige maior capacidade de armazenamento. No entanto, como fazem a cópia dos ficheiros na totalidade, estes também são os mais eficientes para restaurar um sistema.
- **Backup Incremental** - Este tipo de *backups* são os mais rápidos e reduzidos. Durante um *backup* incremental, se este for feito um dia depois de um *backup* normal, apenas os ficheiros criados ou alterados nesse espaço de tempo serão copiados. No entanto para restaurar um sistema é necessário o *backup* normal e depois restaurar todos os *backups* incrementais na sua ordem de criação, tornando este tipo o menos eficiente.
- **Backup Diferencial** - Os *backups* diferenciais são um meio termo entre os dois tipos anteriores. Durante a realização de um *backup* diferencial todos os ficheiros que foram alterados ou criados desde o último *backup* normal são copiados pelo que ao longo do tempo o tamanho deste *backup* aumenta até que um novo *backup* normal seja feito.
- **Backup de Cópia** - O *backup* de cópia é parecido com o *backup* normal no entanto este não marca os ficheiros como copiados, o que o torna útil para mover dados entre sistemas ou criar uma cópia adicional dos dados sem afetar os procedimentos normais de *backups*.
- **Backup Diários** - Os *backups* diários são *backups* que copiam apenas os ficheiros criados ou modificados naquele dia em específico, sem verificar os *backups* anteriores.
- **Backups Combinados** -
 - **Backups Normal e Diferencial** - A combinação entre este tipo de *backups* é feita de forma a que seja realizado um *backup* normal periodicamente e nos dias restantes é feito um *backup* diferencial. Assim, caso os dados se corrompam por exemplo numa sexta-feira, é restaurado o *backup* normal de domingo e o *backup* diferencial de quinta-feira.
 - **Backups Normal e Incremental** - Esta segunda combinação é parecida com a anterior no entanto para ser efetuado um restauro é necessário todos os *backups* incrementais por ordem desde o último *backup* normal feito.

9.2 Estratégias

Será necessário explicar algumas estratégias a ter em conta na gestão dos servidores de *backup* e alguns dispositivos para garantir uma chance de perda de dados mínima para a empresa. Por estas estratégias passam as seguintes:

- **Equipamentos Redundantes** - A utilização de servidores, links, switches e até routers redundantes garante a prevenção em caso de uma falha do equipamento principal.
- **Backups Regulares** - A realização de *backups* com regularidade e num definido intervalo de tempo garante que em caso de ocorrer algum problema existe um ponto de restauro disponível e pronto a usar.
- **Regra 3-2-1** - A regra 3-2-1 é uma forma simples e eficaz de garantir a integridade dos dados. Esta regra propõe a existência de 3 cópias dos dados, distribuída em 2 tipos de media diferentes, e com uma das cópias a ser guardada fora do local onde as restantes se encontram, de preferência, num local relativamente longe de forma a que uma possível catástrofe não ponha em risco todos os dados.
- **Documentação dos Backups** - A documentação dos *backups* faz com que os responsáveis pela realização dos *backups* esteja sempre a par de quando foi feito o último *backup*, qual o conteúdo de tal *backup* e também para onde este foi feito. Dessa forma são evitadas duplicações.
- **Uso de Dispositivos Confiáveis** - O uso de dispositivos antigos, com pouco espaço disponível ou até desatualizados irá poderá colocar em risco os dados porque, a qualquer momento, estes poderão ser corrompidos ou até poderá acabar o armazenamento durante um *backup*.

9.3 Plano de Backup para o Supermercado

9.3.1 Plano de Backup para Configuração dos Dispositivos Intermédios -

O plano de *backup* para a configuração dos dispositivos intermédios garante que as configurações de dispositivos como firewall, switches, routers ou servidores possam ser rapidamente restauradas em caso de um ataque, falha ou erro humano.

Decidimos então fazer um *backup* normal com a frequência de 1 vez por semana onde copiamos todas as configurações de todos os dispositivos intermédios seguido de *backups* diferenciais diárias onde copiamos apenas as alterações realizadas desde o último *backup* normal. Para além disso decidimos fazer um *backup* de cópia antes de qualquer atualização ou alteração na configuração de dispositivos da rede.

O local de armazenamento destes *backups* é um servidor interno seguro e um backup externo encriptado num servidor remoto. O procedimento de recuperação em caso de falha passa pela restauração da última configuração válida do dispositivo e caso seja necessário a aplicação de backups diferenciais para restaurar as alterações mais recentes.

9.3.2 Plano de Backup para Dados Operacionais -

O plano de *backup* para dados operacionais visa assegurar a integridade e disponibilidade dos dados considerados críticos do nosso cenário, que no caso passam por stock, vendas, faturação e registo de clientes.

Primeiramente é feito um *backup* normal semanal tal como no plano apresentado anteriormente com um cópia na integra de todos os dados operacionais críticos. De seguida efetuamos também *backups* diferenciais diários onde copiamos os dados alterados desde o último *backup* normal. Por fim fazemos também diariamente um *backup* dos registos de acesso e câmeras de vigilância dos últimos 90 dias.

Para o armazenamento destes *backups* usamos um servidor interno seguro, um *backup* externo encriptado num servidor remoto e dispositivos físicos como discos externos situados off-site. Como procedimento de recuperação primeiramente restauramos o último *backup* normal, seguido dos *backups* diferenciais.

10 IoT

10.1 Ameaças e Vulnerabilidades

- **Falha em Formatos de Autenticação** - Muitos dispositivos IoT não exigem métodos seguros de login pelo que podem depois ser comprometidos através de ataques *brute force* ou até *spoofing*
- **Falsificação da Camada MAC** - Este tipo de ameaças ocorre quando o atacante clona um endereço MAC de um dispositivo e através disso consegue ganhar acesso à rede. Isto acontece porque os dispositivos IoT podem não possuir poder de processamento suficiente para encriptação.
- **Falta de Privacidade dos Dados** - As aplicações que controlam os dispositivos IoT podem transmitir dados considerados sensíveis sem a devida proteção e dessa forma pode haver uma coleta não autorizada de informações sobre clientes ou até outras operações.
- **Ataques não exclusivos de cenários IoT** - Outros tipos de ataques comuns a dispositivos IoT são os ataques MITM (*Man-In-The-Middle*), DDoS (*Distributed Denial of Service*), *SQL Injection* ou também *Eavesdropping/Sniffing*.

10.2 Melhores Práticas

De forma a mitigar os riscos de ameaças mencionadas acima existem algumas boas práticas de segurança que podemos utilizar:

- **Segurança por Design** - Escolher dispositivos IoT que possuam recursos de segurança embutidos.
- **Hardening de Dispositivos IoT** - Desativar os serviços desnecessários e que não estão a ser utilizados assim como alterar as credenciais que vem de fábrica.
- **Autenticação e Encriptação** - Implementação de passwords fortes e utilização de encriptação SSL/TLS para comunicação segura entre dispositivos.
- **Segmentação da Rede IoT** - Isolar os dispositivos IoT em VLANs separadas de forma a impedir que um dispositivo que possa ser ou ter sido comprometido e infetado consiga afetar o resto da rede do supermercado.
- **Monitorização e Logs** - Registar todas as atividades dos dispositivos IoT e analisar possíveis anomalias.
- **Atualizações e Inventário** - Manter sempre os firmwares atualizados e documentar todos os dispositivos que se encontram conectados à rede.

10.3 Protocolo de Publish

No IoT um dos protocolos mais utilizados é o MQTT (Message Queuing Telemetry Transport). Este protocolo permite que dispositivos IoT e servidores comuniquem eficientemente. Este protocolo utiliza conexões TCP e pode também ser protegido por encriptação SSL/TLS de forma a reforçar a segurança dos dados transmitidos.

O MQTT permite a conexão entre dispositivos IoT e servidores sem conexões diretas através de um modelo *publish/subscribe*. Existe um *publisher* que no caso é um dispositivo IoT e que envia mensagens para um determinado tópico que é um canal usado para classificar mensagens. O *broker* é um servidor intermediário que tem como função receber e distribuir as mensagens publicadas para os *subscribers* apropriados, que são dispositivos ou aplicações que recebem mensagens de um determinado tópico. Por fim existe o QoS (*Quality of Service*) que define a confiabilidade da entrega das mensagens.

10.4 Cenário

No cenário do supermercado e a nível de dispositivos IoT decidimos utilizar

- **Câmeras de Segurança** - Usadas para monitorizar corredores, caixas, áreas restritas, prevendo roubos e garantindo a segurança dos clientes e funcionários.
- **Balanças Digitais** - Utilizadas para a pesagem de legumes e frutas ou produtos que sejam vendidos por peso.
- **Sensores de Temperatura e Humidade** - Instalados em frigoríficos, congeladores, arcas entre outros locais que sejam necessários de forma a monitorizar a temperatura e impedir que os alimentos estejam em condições que possam causar o seu estrago.
- **Sensores de Porta e Movimento** - Usados para monitorizar a entrada e saída de pessoas e para a abertura de portas automáticas.
- **Tags RFID** - Aplicadas em produtos para conseguirmos monitorizar o inventário em tempo real.
- **Tomadas de Energia Inteligente** - Utilizadas para notificar o responsável quando a energia falha, de forma a que exista uma rápida resposta.
- **Impressora de Etiquetas** - Estes dispositivos são usados para impressão de etiquetas com o preço atualizado em tempo real.
- **Terminais de Pagamento por Cartão** - São usados para processar de forma segura transações financeiras e garantir a segurança dos dados bancários dos clientes.

10.4.1 MQTT

No nosso cenário do supermercado um uso exemplo do MQTT pode ser nos sensores de temperatura dos frigoríficos que publicam as leituras num determinado tópico e o servidor de monitorização recebe as leituras em tempo real. Caso a temperatura ultrapasse um dos limites inferior ou superior determinados previamente, o servidor aciona automaticamente um alerta.

10.5 Cenário com Dispositivos IoT

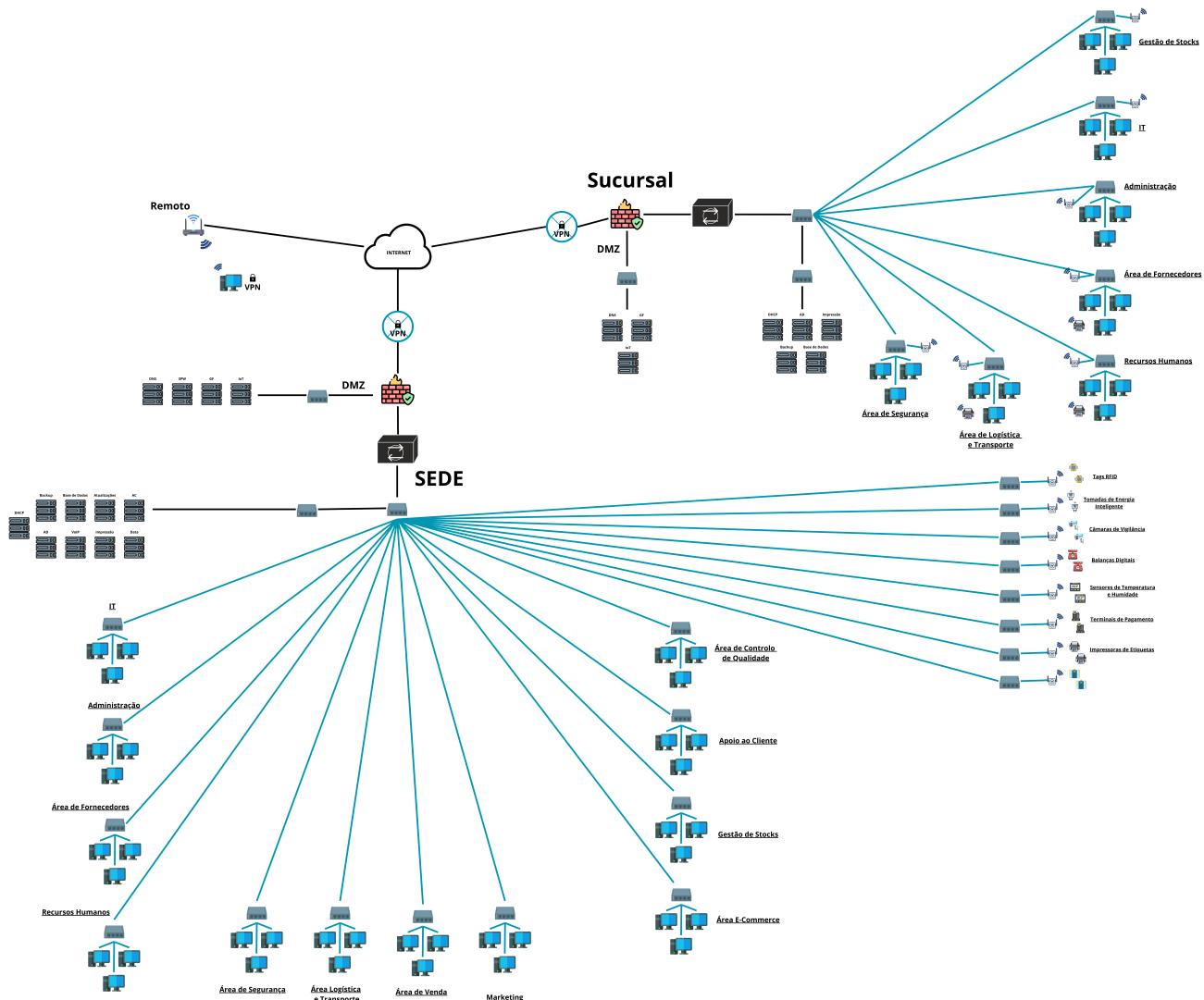


Figura 10: Cenário com Dispositivos IoT

11 Conclusão

Este trabalho demonstrou a importância de uma infraestrutura eficiente e segura no cenário de um supermercado. Durante o desenvolvimento do projeto conseguimos aprender que a segurança de uma rede depende de um conjunto de estratégias e medidas que envolvem *firewalls*, VPNs, ACLs e até boas práticas de segmentação, para além de perceber que os dispositivos IoT precisam de isolamento devido a serem alvos frequentes de ataques e serem mais vulneráveis, podendo comprometer o resto da rede se não houver o devido cuidado. Além disso percebemos também que os backups regulares e planeados são fundamentais para que possamos garantir a recuperação de todas as configurações e dados operacionais no caso de uma falha. Aprendemos a importância do planeamento e implementação de políticas de segurança adequadas e que garantem proteção contra ameaças, continuidade operacional e também um ambiente confiável para os sistemas existentes no supermercado.

A nível de dificuldades sentimos algumas na configuração de dispositivos dentro do Eve o que nos levou a algumas horas perdidas. Consideramos que a curva de aprendizagem desta plataforma é exigente e tornou-se no fundo um desafio. Com isto não deixamos de retirar que foi aprofundado o nosso conhecimento também na área da emulação de redes e resolução de problemas técnicos que são habilidades necessárias para ambientes de redes complexas.

12 Anexos

12.1 Configurações dos Routers

12.1.1 Router Sede

- eanble
- configure terminal
- hostname ROUTER_SEDE
- ipv6 unicast-routing
- interface GigabitEthernet0/0
- ipv6 enable
- ipv6 address 9999:8888:7777:0002::1/64
- ipv6 FE80::1 link-local
- exit
- interface GigabitEthernet0/1
- ipv6 enable
- address 9999:8888:7777:0001::1/64
- ipv6 address FE80::2 link-local
- exit
- write memory

12.1.2 Router Sucursal

- eanble
 - configure terminal
 - hostname ROUTER_SUCURSAL
 - ipv6 unicast-routing
 - interface GigabitEthernet0/0
-

- ipv6 enable
- ipv6 address 9999:8888:7777:0002::2/64
- ipv6 FE80::3 link-local
- exit
- interface GigabitEthernet0/1
- ipv6 enable
- address 9999:8888:7777:0003::1/64
- ipv6 address FE80::4 link-local
- exit
- write memory

12.2 Configurações dos Switches

12.2.1 Configuração de Vlans

- enable
 - configure terminal
 - vlan 10
 - name Servidores
 - vlan 20
 - name IT
 - vlan 30
 - name Administracao
 - vlan 40
 - name Fornecedores
 - vlan 50
 - name Recursos_Humanos
-

- vlan 60
- name Segurança
- vlan 70
- name Logistica
- vlan 80
- name Venda
- vlan 90
- name Marketing
- vlan 100
- name Ecommerce
- vlan 110
- name Gestao_Stocks
- vlan 120
- name Apoio_Cliente
- vlan 130
- name Controlo_Qualidade
- vlan 140
- name IoT
- exit

12.2.2 Configuração de Dispositivos nas Vlans - Servidores

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 10
 - description Ligação para DHCP
-

- exit
- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 10
- description Ligação para Backup
- exit
- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 10
- description Ligação para AD
- exit
- interface GigabitEthernet0/4
- switchport mode access
- switchport access vlan 10
- description Ligação para BD
- exit
- interface GigabitEthernet0/5
- switchport mode access
- switchport access vlan 10
- description Ligação para VoIP
- exit

- interface GigabitEthernet0/6
 - switchport mode access
 - switchport access vlan 10
 - description Ligação para Atualizacoes
 - exit
- interface GigabitEthernet0/7
 - switchport mode access
 - switchport access vlan 10
 - description Ligação para Impressao
 - exit
- interface GigabitEthernet0/8
 - switchport mode access
 - switchport access vlan 10
 - description Ligação para AC
 - exit
- interface GigabitEthernet0/9
 - switchport mode access
 - switchport access vlan 10
 - description Ligação para Data
 - exit

12.2.3 Configuração de Dispositivos nas Vlans - Switch IT

- interface GigabitEthernet0/1
- switchport mode access
- switchport access vlan 20
- description Ligação para PC_IT1
- exit

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 20
- description Ligação para PC_IT2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 20
- description Ligação para PC_IT3
- exit

12.2.4 Configuração de Dispositivos nas Vlans - Switch Administração

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 30
 - description Ligação para PC_ADMIN1
 - exit
-

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 30
- description Ligação para PC_ADMIN2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 30
- description Ligação para PC_ADMIN3
- exit

12.2.5 Configuração de Dispositivos nas Vlans - Switch Fornecedores

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 40
 - description Ligação para PC_FORNECEDORES1
 - exit

 - interface GigabitEthernet0/2
 - switchport mode access
 - switchport access vlan 40
 - description Ligação para PC_FORNECEDORES2
 - exit

 - interface GigabitEthernet0/3
-

- switchport mode access
- switchport access vlan 40
- description Ligação para PC_FORNECEDORES3
- exit

12.2.6 Configuração de Dispositivos nas Vlans - Recursos Humanos

- interface GigabitEthernet0/1
- switchport mode access
- switchport access vlan 50
- description Ligação para PC_RH1
- exit

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 50
- description Ligação para PC_RH2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 50
- description Ligação para PC_RH3
- exit

12.2.7 Configuração de Dispositivos nas Vlans - Segurança

- interface GigabitEthernet0/1
- switchport mode access
- switchport access vlan 60
- description Ligação para PC_SEGURANCA1
- exit

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 60
- description Ligação para PC_SEGURANCA2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 60
- description Ligação para PC_SEGURANCA3
- exit

12.2.8 Configuração de Dispositivos nas Vlans - Logística e Transporte

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 70
 - description Ligação para PC_LOGI_TRAN1
 - exit
-

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 70
- description Ligação para PC_LOGI_TRAN2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 70
- description Ligação para PC_LOGI_TRAN3
- exit

12.2.9 Configuração de Dispositivos nas Vlans - Vendas

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 80
 - description Ligação para PC_VENDAS1
 - exit

 - interface GigabitEthernet0/2
 - switchport mode access
 - switchport access vlan 80
 - description Ligação para PC_VENDAS2
 - exit

 - interface GigabitEthernet0/3
-

- switchport mode access
- switchport access vlan 80
- description Ligação para PC_VENDAS3
- exit

12.2.10 Configuração de Dispositivos nas Vlans - Marketing

- interface GigabitEthernet0/1
- switchport mode access
- switchport access vlan 90
- description Ligação para PC_MARKETING1
- exit

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 90
- description Ligação para PC_MARKETING2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 90
- description Ligação para PC_MARKETING3
- exit

12.2.11 Configuração de Dispositivos nas Vlans - Ecommerce

- interface GigabitEthernet0/1
- switchport mode access
- switchport access vlan 100
- description Ligação para PC_ECOMMERCE1
- exit

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 100
- description Ligação para PC_ECOMMERCE2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 100
- description Ligação para PC_ECOMMERCE3
- exit

12.2.12 Configuração de Dispositivos nas Vlans - Gestão de Stocks

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 110
 - description Ligação para PC_STOCKS1
 - exit
-

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 110
- description Ligação para PC_STOCKS2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 110
- description Ligação para PC_STOCKS3
- exit

12.2.13 Configuração de Dispositivos nas Vlans - Apoio ao Cliente

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 120
 - description Ligação para PC_APOIO_CLIENTE1
 - exit

 - interface GigabitEthernet0/2
 - switchport mode access
 - switchport access vlan 120
 - description Ligação para PC_APOIO_CLIENTE2
 - exit

 - interface GigabitEthernet0/3
-

- switchport mode access
- switchport access vlan 120
- description Ligação para PC_APOIO_CLIENTE3
- exit

12.2.14 Configuração de Dispositivos nas Vlans - Controlo de Qualidade

- interface GigabitEthernet0/1
- switchport mode access
- switchport access vlan 130
- description Ligação para PC_CONTROLO_QUAL1
- exit

- interface GigabitEthernet0/2
- switchport mode access
- switchport access vlan 130
- description Ligação para PC_CONTROLO_QUAL2
- exit

- interface GigabitEthernet0/3
- switchport mode access
- switchport access vlan 130
- description Ligação para PC_CONTROLO_QUAL3
- exit

12.2.15 Configuração de Dispositivos nas Vlans - IoT

- interface GigabitEthernet0/1
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP1
 - exit

 - interface GigabitEthernet0/2
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP2
 - exit

 - interface GigabitEthernet0/3
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP3
 - exit

 - interface GigabitEthernet0/4
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP4
 - exit

 - interface GigabitEthernet0/5
-

- switchport mode access
 - switchport access vlan 140
 - description Ligação para AP5
 - exit
-
- interface GigabitEthernet0/6
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP6
 - exit
-
- interface GigabitEthernet0/7
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP7
 - exit
-
- interface GigabitEthernet0/8
 - switchport mode access
 - switchport access vlan 140
 - description Ligação para AP8
 - exit

12.3 Configuração de Ligação entre Switches e Routers

- interface GigabitEthernet0/24
- switchport mode trunk
- switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,130
- exit

12.4 Configuração de Métodos de Segurança

- interface range GigabitEthernet0/10-23
- shutdown
- exit
- interface GigabitEthernet0/1
- switchport port-security
- switchport port-security maximum 2
- switchport port-security violation restrict
- exit
- write memory

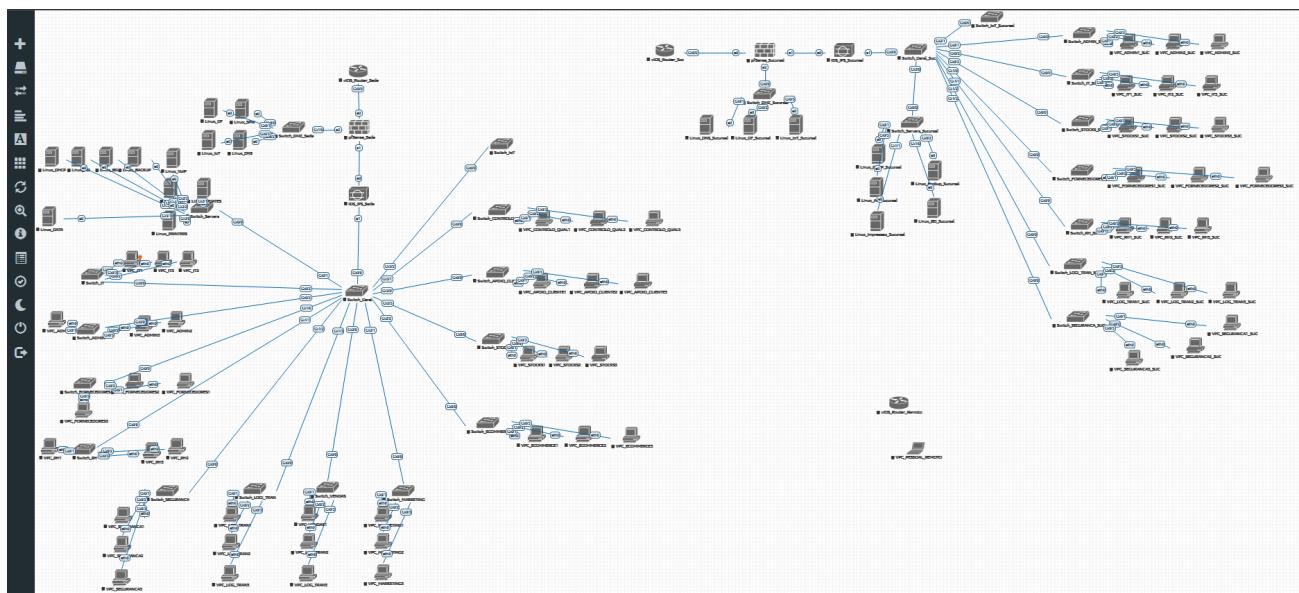


Figura 11: Infraestrutura de Rede no EVE