INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO – CAMPUS MORRINHOS

DIONE ALVINO COSTA GONÇALVES

RELATÓRIO DE ATIVIDADES PROFISSIONAIS REALIZADAS NA ÁREA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

MORRINHOS

2025

DIONE ALVINO COSTA GONÇALVES

RELATÓRIO DE ATIVIDADES PROFISSIONAIS REALIZADAS NA ÁREA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

Trabalho de Conclusão apresentado ao Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal Goiano – Campus Morrinhos, como parte dos requisitos necessários à obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador: Prof. Dr. Antônio Neco de Oliveira

MORRINHOS

2025

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema Integrado de Bibliotecas do IF Goiano - SIBi

Gonçalves, Dione Alvino Costa
G635 Relatório de atividades profissionais realizadas na área de infraestrutura de Tecnologia da Informação / Dione Alvino Costa Gonçalves. Morrinhos 2025.

32f. il.

Orientador: Prof. Dr. Antônio Neco de Oliveira.
Tcc (Tecnólogo) - Instituto Federal Goiano, curso de 0421171 - [MO.GRAD] Curso Superior de Tecnologia em Sistemas para Internet - Morrinhos (Campus Morrinhos).
1. Recursos tecnológicos. 2. Infraestrutura de TI. 3. Tecnologias inovadoras. 4. Agronegócio. 5. Cadeia produtiva. I. Título.

INSTITUTO FEDERAL
Goiano

Repositório Institucional do IF Goiano - RIIF Goiano
Sistema Integrado de Bibliotecas

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☑ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor: Dione Alvino Costa Gonçalves

Matrícula: 2015104211710012

Título do trabalho: Relatório de atividades profissionais realizadas na área de Infraestrutura de Tecnologia da Informação

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☑ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: 9 / 4 / 25

O documento está sujeito a registro de patente? ☐ Sim ☑ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☑ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

gov.br Documento assinado digitalmente
DIONE ALVINO COSTA GONCALVES
Data: 10/04/2025 09:55:47-0300
Verifique em https://validar.iti.gov.br

Morrinhos (Local) — 9 / 4 / 25 (Data)

Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo:

Assinatura do(a) gov.br Documento assinado digitalmente
ANTONIO NECO DE OLIVEIRA
Data: 10/04/2025 10:07:10-0300
Verifique em https://validar.iti.gov.br

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 1/2025 - CCSTSI-MO/DE-MO/CMPMHOS/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Aos oito dias do mês de abril de 2025, às 20 horas, reuniu-se a banca examinadora composta pelos docentes: Dr. Antônio Neco de Oliveira (orientador), Ma. Ana Maria Martins Carvalho (membro), Esp. José Pereira Alves (membro), para examinar o Trabalho de Curso intitulado "RELATÓRIO DE ATIVIDADES PROFISSIONAIS REALIZADAS NA ÁREA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO" do estudante DIONE ALVINO COSTA GONÇALVES, Matrícula nº 2015104211710012, do Curso de Tecnologia em Sistemas para Internet, do IF Goiano – Campus Morrinhos. A palavra foi concedida ao estudante para a apresentação oral do TC, seguida de arguição pelos membros da banca examinadora. Após essa etapa, a banca examinadora decidiu pela APROVAÇÃO do estudante. Ao final da sessão pública de defesa, foi lavrada a presente ata, a qual segue assinada pelos membros da banca examinadora.

(Assinado Eletronicamente)

Dr. Antônio Neco de Oliveira
Orientador

(Assinado Eletronicamente)

Ma. Ana Maria Martins Carvalho
Membro

(Assinado Eletronicamente)

Esp. José Pereira Alves
Membro

Documento assinado eletronicamente por:

- **Antonio Neco de Oliveira**, **DIRETOR(A) - CD0003 - DE-MO**, em 09/04/2025 15:53:06.
- **Ana Maria Martins Carvalho**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 09/04/2025 16:35:15.
- **Jose Pereira Alves**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 09/04/2025 16:39:40.

Este documento foi emitido pelo SUAP em 09/04/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 697056
Código de Autenticação: e00c06fd7b

INSTITUTO FEDERAL GOIANO
Campus Morrinhos
Rodovia BR-153, Km 633, Zona Rural, SN, Zona Rural, MORRINHOS / GO, CEP 75650-000
(64) 3413-7900

Dedico este trabalho à professora Ana Maria Martins Carvalho, que, mesmo não sendo minha orientadora, sempre acreditou no meu potencial e me incentivou a perseverar até a conclusão desta jornada.

AGRADECIMENTOS

Agradeço especialmente à minha namorada, Nara Marques, por dedicar seu tempo e apoio essenciais para a conclusão deste trabalho. Também expresso minha gratidão aos professores Antônio Neco de Oliveira e Rodrigo Elias Francisco pelo valioso suporte e orientação ao longo deste percurso.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AD – Active Directory

BGP – Border Gateway Protocol

CA – Certificate Authority

DNS – Domain Name System

DPI – Deep Packet Inspection

HA – Alta Disponibilidade

Hyper-V – Hypervisor Virtual

IoT – Internet das Coisas

IPS – Intrusion Prevention System

iSCSI – Internet Small Computer Systems Interface

LDAP – Lightweight Directory Access Protocol

NGFW – Next Generation Firewall

NPS – Network Policy Server

RADIUS – Remote Authentication Dial-In User Service

SD-WAN – Software-Defined Wide Area Network

SLA – Service Level Agreement

SSL/SSH – Secure Sockets Layer / Secure Shell

SSL/TLS – Secure Sockets Layer / Transport Layer Security

SSO – Single Sign-On

TCP/IP – Transmission Control Protocol / Internet Protocol

TI – Tecnologia da Informação

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

SUMÁRIO

1. INTRODUÇÃO

Relatório de atividades profissionais realizadas na empresa Agrex do Brasil Ltda., pelo Analista de Infraestrutura de Tecnologia da Informação(TI), Dione Alvino Costa Gonçalves.

Durante o período de atuação na empresa, foram desenvolvidas diversas atividades voltadas para a otimização da infraestrutura de TI, com foco em segurança, disponibilidade de serviços e gerenciamento eficiente dos recursos tecnológicos. As principais atividades realizadas incluem:

- Configuração do *firewall Fortigate* para controle de acessos e segmentação da rede, garantindo maior segurança e gerenciamento adequado do tráfego;
- Integração do *firewall* com o *Active Directory* (AD) para autenticação centralizada dos usuários, permitindo a aplicação de políticas de acesso baseadas em grupos específicos;
- Implementação do *Network Policy Server* (NPS) para autenticação via *RADIUS*, assegurando um acesso seguro e controlado à rede corporativa;
- Configuração e gerenciamento de *clusters Hyper-V*, garantindo alta disponibilidade dos serviços críticos e minimizando o impacto de falhas em servidores físicos;
- Implementação e monitoramento de *backup* com *Veeam Backup & Replication*, assegurando a proteção dos dados por meio de cópias locais e replicação na nuvem;
- Otimização do tráfego de rede com *Software-Defined Wide Area Network (*SD-WAN), para melhorar a conectividade entre filiais, assegurando balanceamento de carga e roteamento eficiente;
- Monitoramento e manutenção de políticas de segurança, incluindo filtros de conteúdo, controle de aplicações e prevenção contra intrusões *(Intrusion Prevention System - IPS)*.

Essas atividades contribuíram para a melhoria da infraestrutura de TI da empresa, proporcionando maior controle, segurança e eficiência operacional. Nos tópicos seguintes, serão apresentados detalhes sobre cada uma dessas implementações, seus benefícios e os impactos observados no ambiente corporativo. Os objetivos são: configurar e gerenciar a segurança de rede; autenticar computadores e usuários de forma centralizada; promover a alta

disponibilidade de servidores; gerir políticas de backup e recuperação de dados.

No que se refere a empresa, a Agrex do Brasil Ltda. é uma organização do setor agroindustrial, especializada no comércio e distribuição de insumos agrícolas, originação de grãos e soluções integradas para produtores rurais. Com sede localizada em Goiânia-Go, ela atua em diversas regiões do país, contribuindo para o desenvolvimento do agronegócio brasileiro por meio de tecnologias inovadoras e serviços estratégicos.

Entre suas principais atividades, destacam-se a originação, comercialização e exportação de grãos , além do fornecimento de fertilizantes, defensivos agricolas e sementes. A empresa busca agregar valor à cadeia produtiva do agronegócio, oferecendo suporte técnico e soluções personalizadas para melhorar a produtividade e a rentabilidade dos produtores rurais.

Por ser uma empresa que movimenta um alto volume de informações estratégicas e operações em grande escala, a infraestrutura de TI da Agrex desempenha um papel fundamental na garantia da segurança, conectividade e eficiência dos processos internos. A companhia investe continuamente em inovações tecnológicas para melhorar a comunicação entre suas unidades, melhorar a gestão de dados e garantir a confiabilidade dos sistemas usados nas operações diárias.

A equipe de Infraestrutura de TI da Agrex é responsável por manter e aprimorar um ambiente tecnológico robusto, composto por servidores físicos e virtuais, redes corporativas, sistemas de segurança da informação e diversas soluções em nuvem. Esses recursos garantem alta disponibilidade e desempenho dos serviços, minimizando riscos operacionais e otimizando a produtividade da empresa.

A Figura 1 apresenta um organograma da estrutura organizacional de cargo e setores de Tecnologia da Informação da Agrex.

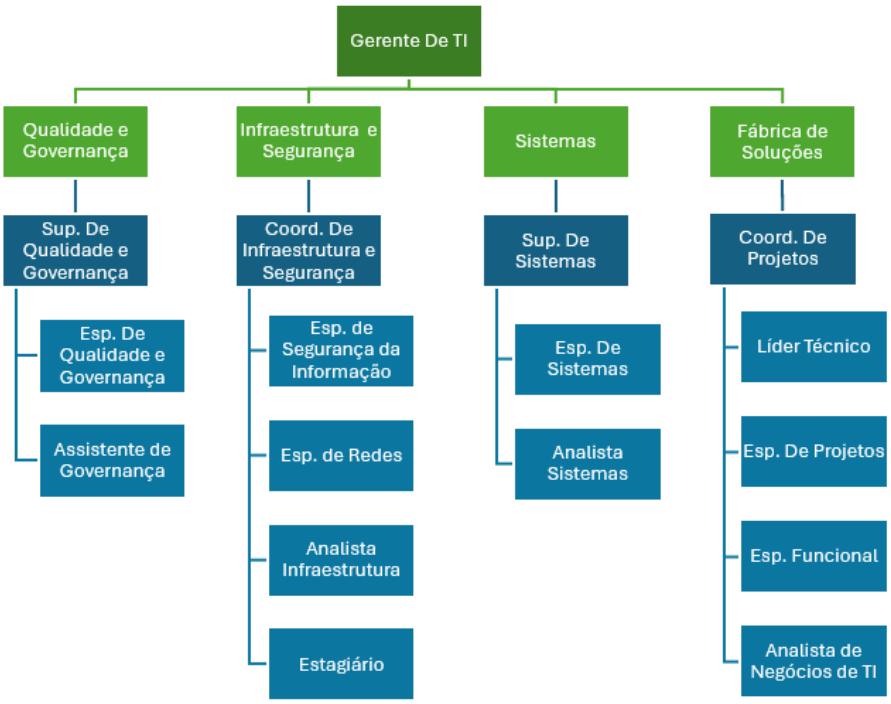

Figura 1. Estrutura Organizacional do Departamento de TI

Fonte: o autor (2025).

Este relatório tem como objetivo documentar as atividades profissionais desenvolvidas na empresa Agrex destacando as soluções implementadas, seus benefícios e impactos no ambiente de TI dessa. Além disso, este documento apresenta uma análise dos resultados obtidos e sua relevância para o aprimoramento da infraestrutura de TI.

2. DESENVOLVIMENTO

A Tecnologia da Informação (TI) desempenha um papel fundamental no suporte às operações empresariais, garantindo segurança, eficiência e disponibilidade dos serviços digitais. A crescente complexidade dos ambientes de TI exige a adoção de soluções avançadas para gerenciamento de redes, proteção de dados e alta disponibilidade de servidores. Nesse contexto, a implementação de tecnologias como *firewall, clusters* de alta disponiilidade e uma robusta solução de *Backup & Replication* se torna essencial para assegurar a continuidade operacional e a proteção das informações corporativas.

2.1 Comunicação e Autenticação de Rede

A comunicação e autenticação de rede são fundamentais para garantir a segurança e a eficiência dos acessos dentro da infraestrutura corporativa. O que evidencia a necessidade da implementação de um *firewall* robusto e a adoção de políticas de autenticação permitem um controle refinado do tráfego e dos acessos dos usuários e dispositivos (MORAES, 2024).

Um *firewall* é um sistema de segurança de rede que monitora e controla o tráfego de entrada e saída com base em regras de segurança predefinidas. Ele age como uma barreira entre uma rede confiável e redes externas potencialmente não seguras (MORAES, 2024). Nesse cenário foram adotadas soluções como o *firewall Fortigate* e a autenticação via NPS, garantindo segmentação, segurança e otimização do tráfego de rede.

2.1.1 Configuração de Firewall Fortigate

O *firewall Fortigate* se destaca por ser um *firewall* de próxima geração (*Next Generation Firewall - NGFW*), oferecendo inspeção profunda de pacotes *Deep inspection* - DPI, prevenção contra intrusões *IPS* avançado, controle detalhado de aplicações e inteligência de ameaças em tempo real. A DPI é uma técnica de segurança que examina o conteúdo dos pacotes de dados que trafegam pela rede, permitindo a detecção e a prevenção de ameaças ocultas em níveis mais profundos, como *vírus, malware e exploits*. Já a prevenção contra intrusões IPS é um mecanismo que monitora o tráfego da rede em busca de comportamentos suspeitos ou ataques conhecidos, bloqueando automaticamente qualquer tentativa de intrusão antes que ela afete a rede. Essas capacidades tornam a solução altamente eficaz na defesa contra ameaças cibernéticas sofisticadas, garantindo maior segurança e controle sobre o tráfego de

rede (FORTINET, 2025).

A Figura 2 mostra a tela de edição de um perfil de inspeção SSL/SSH no *firewall FortiGate*. Esse perfil permite configurar a DPI do tráfego SSL/TLS. Na figura é possível o CA *certificate* (certificado digital) utilizado para inspeção do tráfego, esse recurso permite que o *firewall* intercepte o tráfego SSL/TSL entre clientes e servidores para detectar *malwares,* ataques e outras ameaças que podem estar ocultas dentro de conexões seguras.

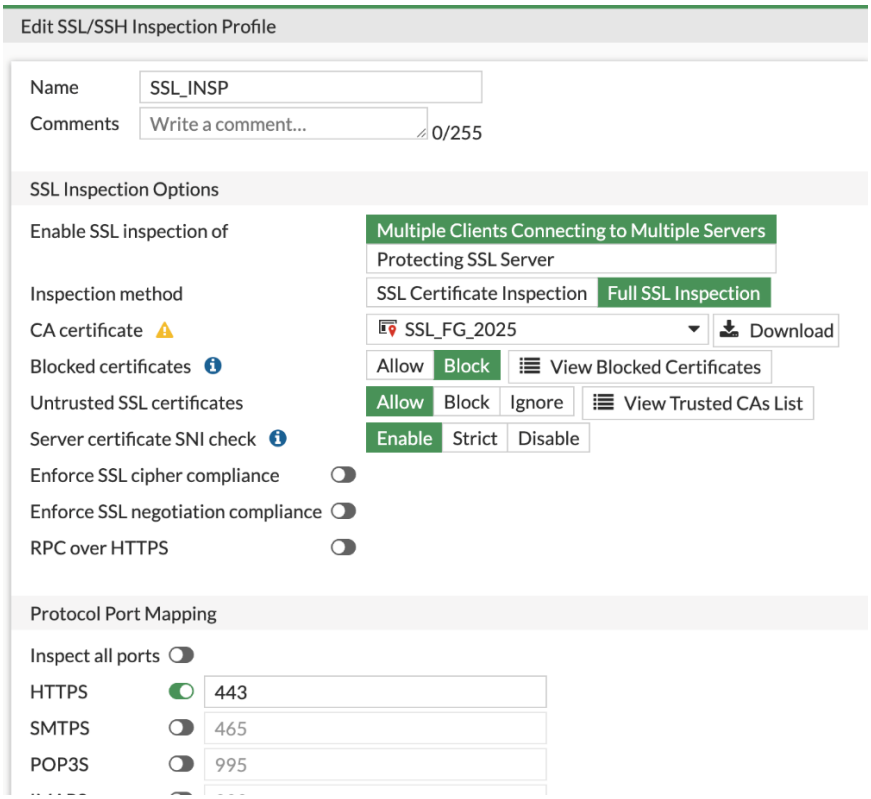

Figura 2. Deep Inspection (DPI)

Fonte: o autor (2025).

Além disso, a inspeção profunda de pacotes (DPI) no FortiGate possibilita a aplicação de políticas de segurança mais granulares, permitindo o bloqueio ou a liberação de tráfego com base no conteúdo analisado. Esse recurso é fundamental para garantir a conformidade com as políticas de segurança da empresa, prevenindo acessos não autorizados e protegendo a rede contra ameaças avançadas, como ataques de phishing e malwares que utilizam criptografia para evitar a detecção.

A Figura 3 mostra a tela de configuração de assinaturas do IPS no *firewall FortiGate*. O IPS é responsável por detectar e bloquear tráfego malicioso, ataques e explorações de vulnerabilidades em tempo real.

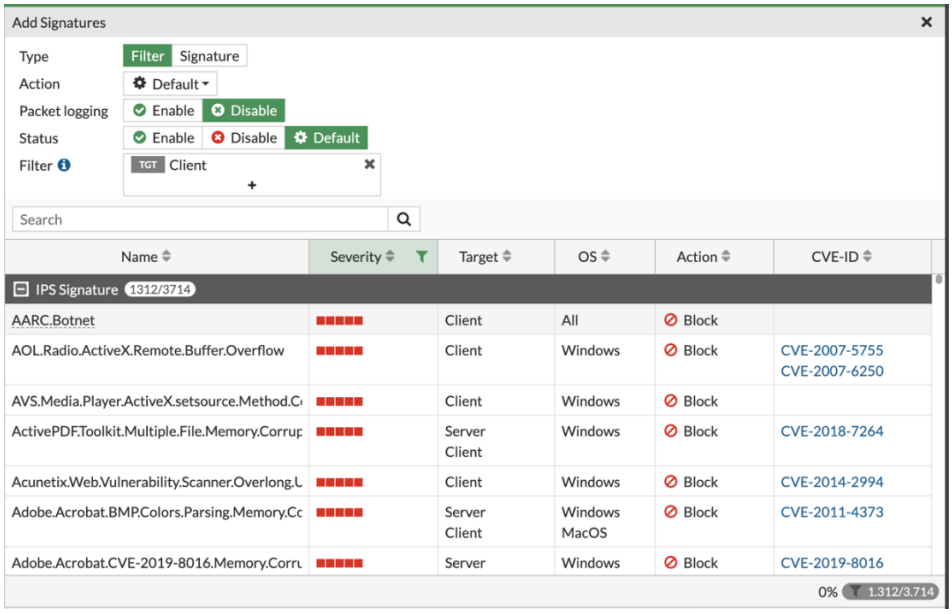

Figura 3. Intrusion Prevention System (IPS)

Fonte: o autor (2025).

Para garantir um ambiente de rede seguro e confiável, são implementados diversos recursos de segurança no *firewall*. Sendo eles, o Antivirus que oferece proteção contra *malwares* e arquivos maliciosos, o *Web Filter* que permite o controle de acesso a sites com base em categorias e regras empresariais. O DNS Filter que reforça a segurança ao filtrar a resolução de nomes de domínios (DNS) e prevenir ataques cibernéticos. O *Application Control* monitora e bloqueia aplicações não autorizadas, assegurando que apenas softwares aprovados possam ser utilizados.

A Figura 4 mostra a configuração de um perfil de filtro da web (web filter) no *firewall Fortigate*. Essa configuração é utilizada para controlar o acesso à Internet dos usuários da rede, bloqueando ou permitindo categorias específicas de sites conforme regras definidas.

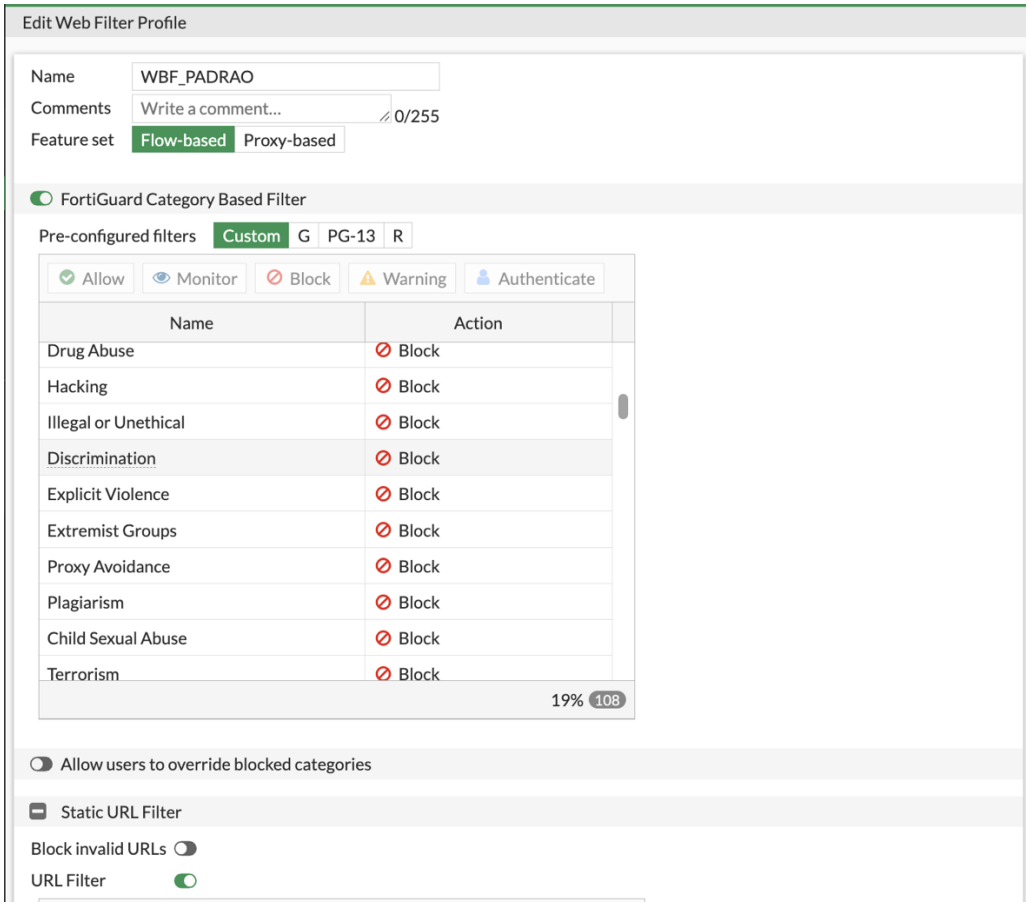

Figura 4. Configuração de Web Filter

Fonte: o autor (2025).

A Figura 5 apresenta a configuração de um perfil de filtro de DNS no *firewall Fortigate,* utilizado para controlar e restringir o acesso a domínios específicos com base nas categorias definidas pela *FortiGuard,* um serviço de inteligência de segurança da Fortinet que atualiza e categoriza automaticamente domínios e sites para proteção contra ameaças cibernéticas.

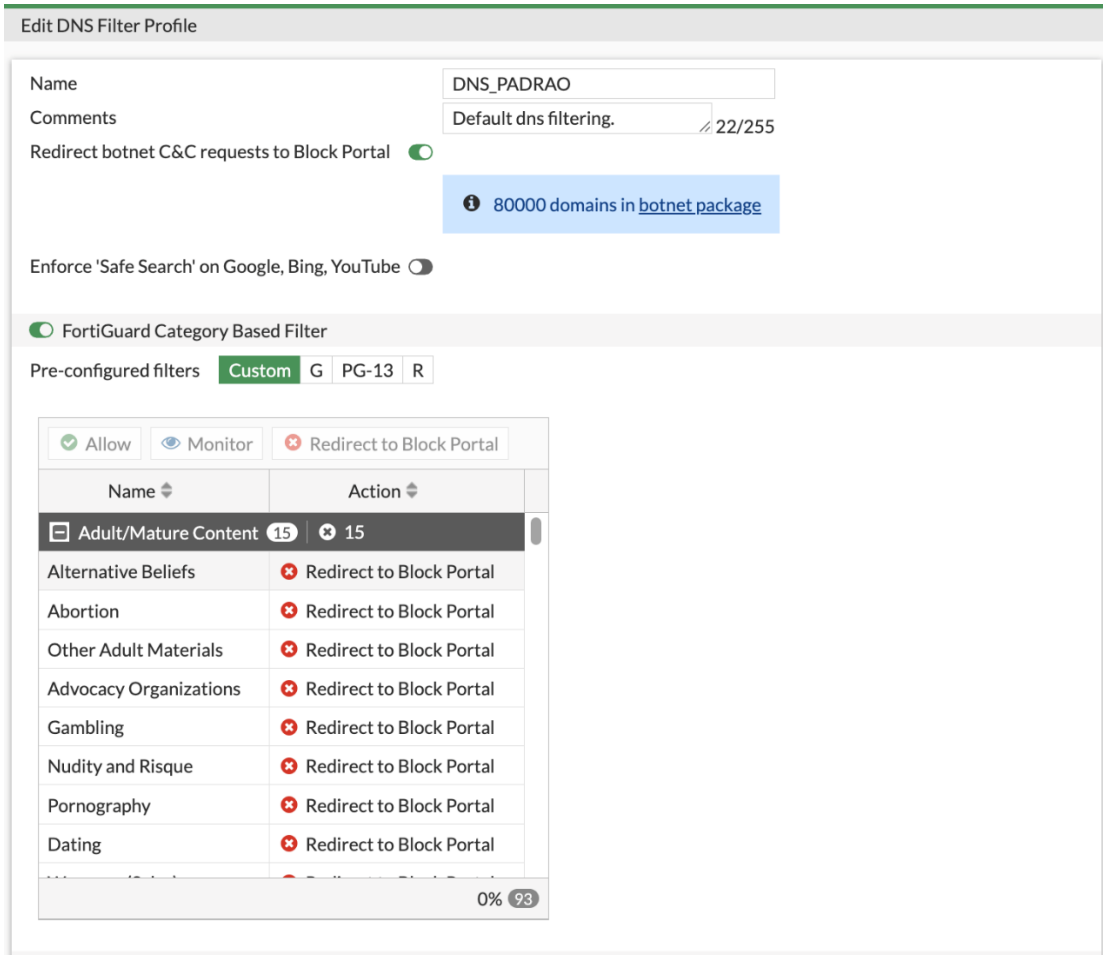

Figura 5. Configuração de Filtro DNS

Fonte: o autor (2025).

Além de bloquear o acesso a domínios maliciosos, o filtro de DNS também permite a criação de listas personalizadas para atender às necessidades específicas da organização, como a restrição de sites de redes sociais ou de streaming durante o horário de trabalho. Esse recurso contribui para o aumento da produtividade, a redução de riscos relacionados a acessos não autorizados.

A Figura 6 apresenta a configuração de um perfil de controle de aplicações no *firewall Fortigate*, conhecido como *Application Control*. Esse recurso permite identificar, monitorar e controlar aplicações que trafegam na rede com base em categorias, independentemente da porta ou do protocolo utilizado.

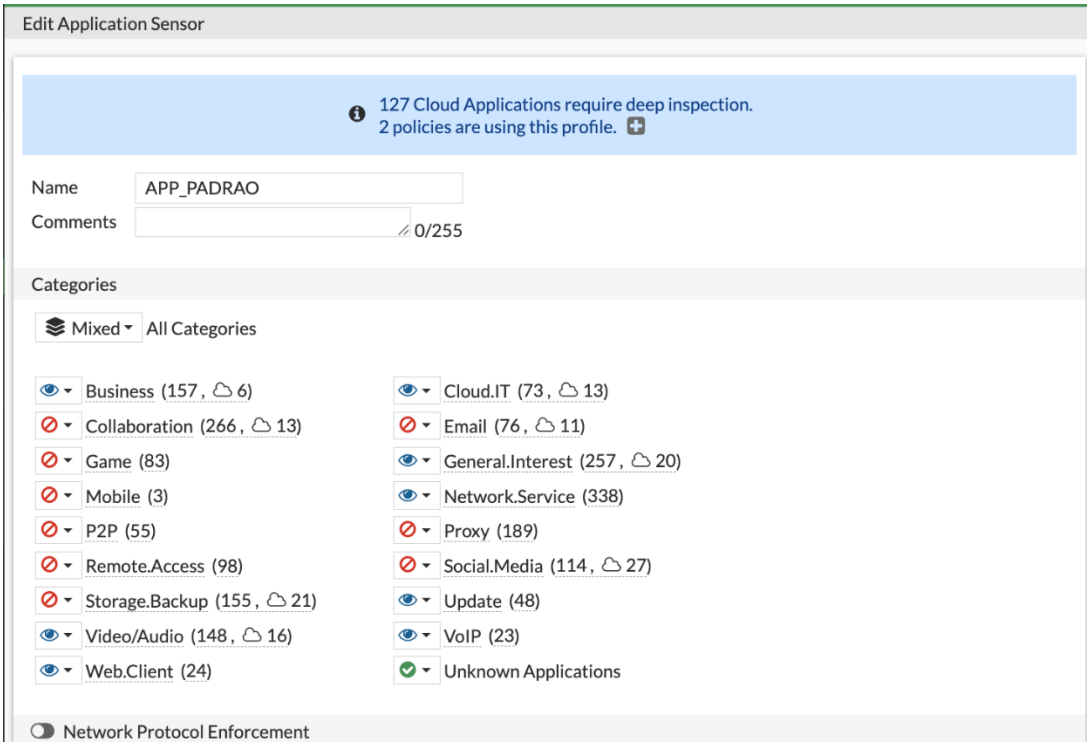

Figura 6. Configuração de Application Control

Fonte: o autor (2025).

Além de proporcionar maior visibilidade sobre o uso de aplicações na rede, o Application Control permite a implementação de políticas de segurança mais rigorosas, como a restrição de aplicativos não autorizados ou o bloqueio de softwares que possam representar riscos à organização. Dessa forma, o firewall FortiGate contribui para a otimização do desempenho da rede e para a proteção contra ameaças associadas ao uso indevido de aplicações.

A integração do firewall Fortigate com o *Active Directory* (AD), que é um serviço de diretório desenvolvido pela Microsoft para gerenciamento centralizado de recursos e autenticação de usuários em redes corporativas, permite a segregação da navegação por meio de grupos de usuários, garantindo um controle de acesso refinado e personalizado. A configuração envolve a utilização de autenticação via *Lightweight Directory Access Protocol* (LDAP) para sincronização com o AD, possibilitando a criação de políticas de acesso baseadas em grupos específicos adicionalmente com a implementação de *Single Sign-On* (SSO), que facilita a autenticação dos usuários, promovendo uma experiência mais fluida e segura.

Os grupos de navegação são estruturados em diferentes perfis, como FG-RESTRITO, destinado a safristas e jovens aprendizes, com acesso mais limitado; FG-PADRAO, que abrange a maioria dos colaboradores, seguindo as permissões padrão da organização; FG-PADRAO-WHATS, semelhante ao grupo FG-PADRAO, porém com a liberação adicional do WhatsApp

Web; e FG-PADRAO-RS, voltado para áreas como Marketing, Comunicação e Recursos Humanos, garantindo acesso a serviços específicos para essas funções.

Além da gestão de navegação na Internet por grupos de usuários, é realizada a segmentação da rede por VLANs (*Virtual Local Area Networks*), que permite isolar diferentes tipos de tráfego, aumentando tanto a segurança quanto o desempenho da infraestrutura. Cada VLAN funciona como uma rede lógica separada, permitindo que dispositivos em uma mesma VLAN se comuniquem entre si, mas restringindo a comunicação com dispositivos de outras VLANs, a menos que seja explicitamente permitido. Entre as VLANs configuradas, destacam-se: a VLAN Corporativa, destinada ao tráfego de usuários corporativos e recursos empresariais; a VLAN IoT (Internet das coisas), que gerencia dispositivos inteligentes e sensores, com restrições de acesso a outros segmentos da rede para evitar vulnerabilidades; a VLAN Servidores, que assegura segregação e controle estrito de acesso aos servidores internos, protegendo dados sensíveis e recursos críticos; e a VLAN Visitantes, que permite um acesso restrito à Internet sem qualquer conexão com recursos internos da empresa. Para reforçar a segurança, são implementadas políticas de firewall que restringem a comunicação entre VLANs conforme as necessidades da empresa, garantindo que o tráfego entre diferentes segmentos seja devidamente controlado e monitorado.

A Figura 7 apresenta um exemplo da configuração de políticas de *firewall (Firewall Policies)* no Fortigate, com foco nas regras aplicadas para a VLAN corporativa (VLAN_CORP). Essas políticas são responsáveis por definir quais comunicações de rede são permitidas ou bloqueadas, aplicando perfis de segurança específicos para proteger a infraestrutura. Na imagem é possível visualizar a origem do tráfego (*Source*), o destino (*Destination*), o *Schedule* que significa quando essa política entra em vigor, qual serviço está aplicado a cada política (portas TCP e UDP), o *Action* (ação) negar ou aceitar, e o *Security Profiles* (perfis de segurança) onde é possível definir quais políticas de DNS filter, antivírus, web filter, application control, IPS e DPI para cada política de tráfego. Também pode-se notar que foi criado uma política para cada grupo de navegação: FG_RESTRITO, FG_PADRAO, FG_PADRAO_WHATS e FG_PADRAO_WHATS_RS.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
		Microsoft-WNS					
FG_RESTRITO_VLAN_CORP	FG_RESTRITO VLAN_CORP_GTB	all	always	ALL	ACCEPT	Enabled	AV AV_PADRAO WEB WBF_RESTRITO DNS DNS_PADRAO APP APP_RESTRITO IPS protect_client SSL SSL_INSP
FG_PADRAO_VLAN_CORP	FG_PADRAO VLAN_CORP_GTB	all	always	ALL	ACCEPT	Enabled	AV AV_PADRAO WEB WBF_PADRAO DNS DNS_PADRAO APP APP_PADRAO IPS protect_client SSL SSL_INSP
FG_PADRAO_WHATS_META	FG_PADRAO_WHATS FG_PADRAO_WHATS_RS VLAN_CORP_GTB	Meta-DNS Meta-Whatsapp	always	Internet Service	ACCEPT	Enabled	AV AV_PADRAO IPS protect_client SSL SSL_INSP
FG_PADRAO_WHATS_VLAN_CORP	FG_PADRAO_WHATS VLAN_CORP_GTB	all	always	ALL	ACCEPT	Enabled	AV AV_PADRAO WEB WBF_PADRAO_W DNS DNS_PADRAO APP APP_PADRAO_WI IPS protect_client SSL SSL_INSP
FG_PADRAO_WHATS_RS_VLAN_CORP	FG_PADRAO_WHATS_RS VLAN_CORP_GTB	all	always	ALL	ACCEPT	Enabled	AV AV_PADRAO WEB WBF_PADRAO_W DNS DNS_PADRAO APP APP_PADRAO_WI IPS protect_client SSL SSL_INSP

Figura 7. Políticas de Navegação firewall

Fonte: o autor (2025).

Por fim, para melhorar a conectividade entre filiais, utiliza-se o SD-WAN que otimiza o uso de *links* de Internet garantindo maior eficiência no tráfego de dados, disponibilidade e desempenho contínuo, realizando o balanceamento de carga entre múltiplos *links* de Internet, distribuindo o tráfego de forma inteligente.

A Figura 8 apresenta a configuração de um SLA de Desempenho (Performance SLA) no Fortigate para o recurso de SD-WAN VPN. Esse recurso permite gerenciar múltiplos links de Internet ou conexões VPN de maneira eficiente, distribuindo o tráfego de acordo com a qualidade de cada link. O objetivo é garantir alta disponibilidade e desempenho otimizado. Na imagem é possível 3 participantes (DCA-1, DCA-2 e DCA-3) sendo cada um deles uma VPN ativa entre a filial e a matriz. Nesta configuração são aplicados alguns parâmetros como latência, jitter e perda de pacotes da conexão, de forma que a SD-WAN ajusta automaticamente a melhor rota para a matriz com base nessas métricas.

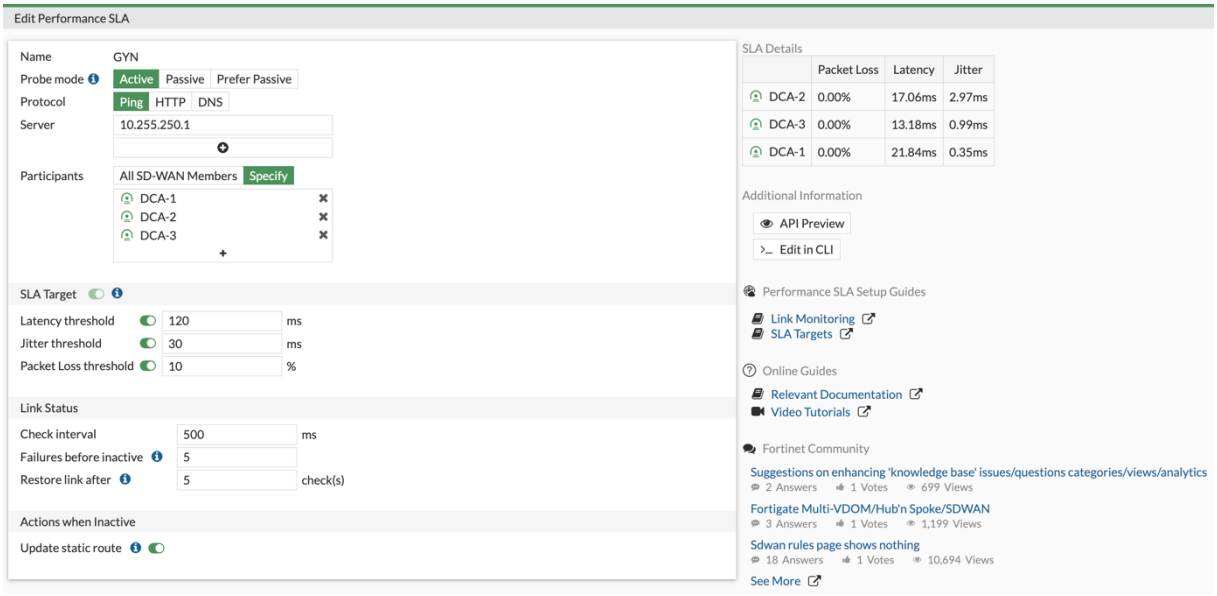

Figura 8. Configuração de SD-WAN SLA

Fonte: o autor (2025).

2.1.2 Implementação do NPS (Network Policy Server)

A autenticação de usuários é realizada via *Network Policy Server* (NPS) do Windows Server, um servidor de políticas de rede responsável por autenticar, autorizar e registrar solicitações de conexão em ambientes corporativos. Esse processo é aplicado tanto em redes cabeadas quanto sem fio. Para a autenticação, os computadores corporativos utilizam o *Remote Authentication Dial-In User Service* (RADIUS) com o protocolo 802.1X, que controla o acesso com base em portas. O 802.1X envolve três componentes: o autenticador (neste caso, os equipamentos Ubiquiti Unifi para switches e pontos de acesso sem fio), o solicitante (computadores corporativos) e o servidor de autenticação (NPS). Esse mecanismo assegura que somente dispositivos autorizados, definidos no *Active Directory* (AD), possam acessar a infraestrutura, com base em grupos de usuários e dispositivos.

Com essa configuração, a infraestrutura se torna altamente segura e eficiente. Cada dispositivo ou usuário precisa ser autenticado rigorosamente antes de obter acesso. O 802.1X atua como um controle de entrada, permitindo somente dispositivos previamente autorizados. Além disso, a segmentação por VLANs e o controle de tráfego permitem um monitoramento eficaz, garantindo que o acesso a recursos seja restrito e que o tráfego indesejado seja bloqueado. O controle granular sobre autenticação e acesso melhora tanto a segurança quanto

o desempenho, prevenindo acessos não autorizados e reduzindo o risco de ameaças, ao mesmo tempo em que facilita a gestão da rede e otimiza o uso dos recursos.

A Figura 9 ilustra uma janela de Propriedades de conexões sem fio seguras do servidor de política de rede (NPS) do Windows que especifica os grupos de usuários (UG_Wireless) e os grupos de computadores (CG_Wireless) do *Active Directory* que estão autorizados a se autenticarem no servidor NPS.

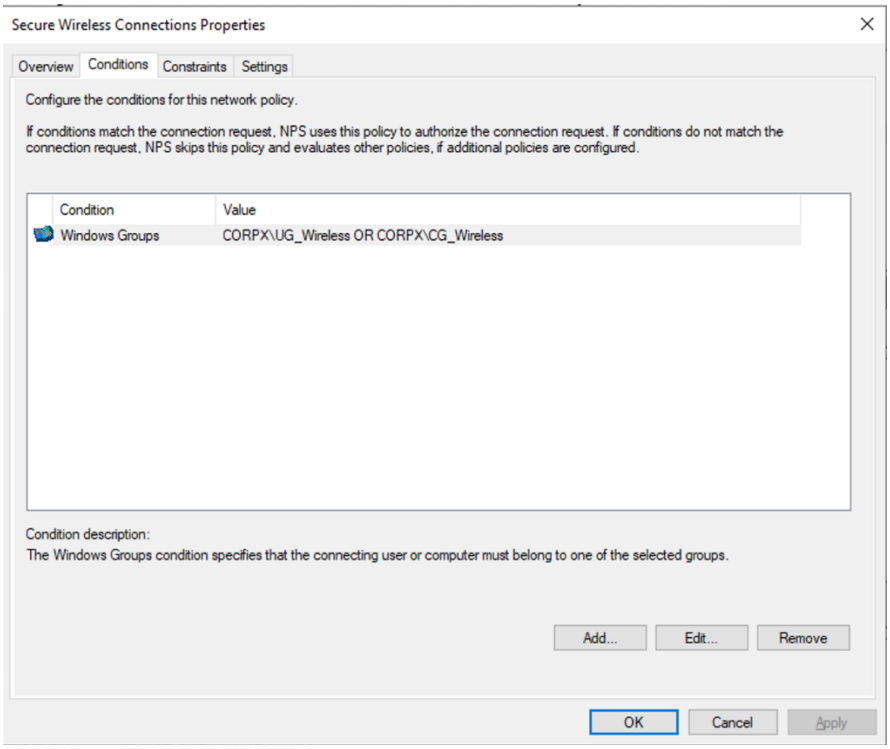

Figura 9. Network Policy Server

Fonte: o autor (2025).

2.2 Alta Disponibilidade em Cluster Hyper-V

A alta disponibilidade (HA) em ambientes virtualizados é essencial para garantir a continuidade dos serviços e minimizar o impacto de falhas em hardware ou software. *O Hyper-V* permite a criação de *clusters* que asseguram a redundância e a resiliência dos serviços críticos, distribuindo máquinas virtuais entre múltiplos *hosts* físicos e garantindo que, em caso de falha, as cargas de trabalho sejam transferidas automaticamente para outro nó do *cluster* (VIEIRA, 2022).

2.2.1 Configuração e Gerenciamento de Clusters

Um *cluster* é um conjunto de servidores interconectados que trabalham juntos para fornecer alta disponibilidade, redundância e desempenho aprimorado para aplicações e serviços. Os nós do cluster incluem recursos e podem assumir funções uns dos outros em caso de falhas, garantindo a continuidade dos serviços (VIEIRA, 2022).

A infraestrutura de cluster da empresa é composta por três servidores físicos Dell PowerEdge R440, que atuam como nós do *cluster*, garantindo a redundância necessária para alta disponibilidade. O armazenamento das máquinas virtuais é realizado por meio de um storage Dell ME4024, que oferece alta performance e confiabilidade para os dados.

A configuração do cluster *Hyper-V* inicia-se com a instalação e ativação do recurso de Failover Clustering nos servidores físicos. Em seguida, é realizada a validação da configuração por meio do *Cluster Validation Wizard,* garantindo que todos os componentes atendam aos requisitos de alta disponibilidade. O *storage* Dell ME4024 é configurado como armazenamento compartilhado utilizando o protocolo iSCSI (*Internet Small Computer System Interface),* um protocolo de transporte que permite a transmissão de comandos SCSI por redes TCP/IP. Essa tecnologia possibilita que os servidores *Hyper-V* acessem os volumes do storage de maneira eficiente e confiável. A conectividade iSCSI é configurada para garantir alta performance e redundância, utilizando múltiplos caminhos de acesso para evitar pontos únicos de falha, assegurando maior disponibilidade e segurança na comunicação entre os servidores e o storage.

O gerenciamento do cluster é realizado por meio do *Failover Cluster Manager*, ferramenta que possibilita a administração centralizada dos nós e a configuração de regras de failover. A configuração de políticas de balanceamento de carga garante a distribuição eficiente dos recursos computacionais, otimizando o desempenho e prevenindo sobrecargas em determinados servidores. Com essas configurações, a infraestrutura virtualizada torna-se altamente disponível, resiliente e preparada para suportar demandas operacionais críticas, minimizando tempos de inatividade e garantindo a continuidade dos serviços empresariais.

A Figura 10 mostra a interface do *Failover Cluster Manager*, uma ferramenta do Windows Server usada para gerenciar clusters de alta disponibilidade. Vou explicar cada parte da figura e como a configuração é realizada. A seguir, é detalhado cada parte da interface e sua função.

Painel esquerdo (Árvore de Navegação):

- **Roles (Regras):** Lista os servidores virtualizados no cluster;
- **Nodes (Nós)**: Mostra os servidores físicos (nós) que compõem o cluster;
- **Storage (Armazenamento)**: Gerencia discos compartilhados e pools de armazenamento usados pelo cluster;

- **Networks (Redes)**: Configura e exibe as redes utilizadas pelo cluster;
- **Cluster Events (Eventos de Cluster)**: Mostra logs e eventos relacionados ao cluster.

A configuração do Failover Cluster Manager começa com a criação do cluster, onde adiciona os servidores e realiza a validação de compatibilidade. Em seguida, foi configurado o quorum utilizando o *Disk Witness*, que é um disco compartilhado usado como "testemunha" para garantir o funcionamento do cluster, mesmo em casos de falha ou divisão entre os servidores. Esse disco ajuda a evitar o estado de “cérebro dividido”, onde dois grupos de servidores tentam controlar os recursos simultaneamente. Após isso é adicionado o armazenamento compartilhado, garantindo que todos os servidores possam acessá-lo. São adicionados os servidores virtuais na guia roles e ajustado as redes para conexões internas e externas.

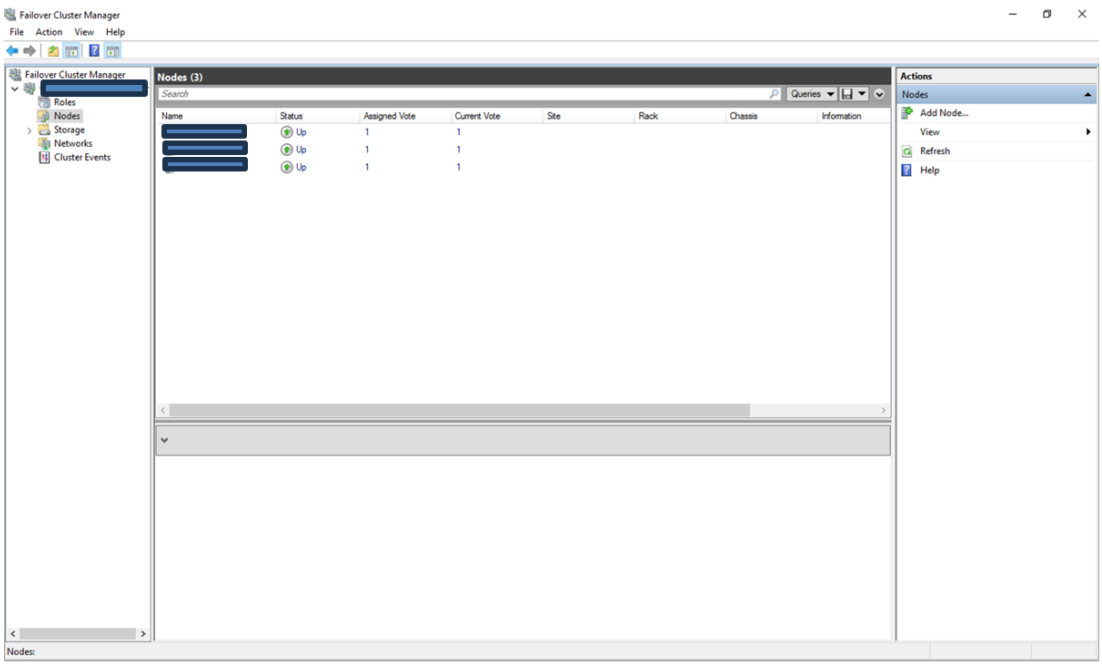

Figura 10. Interface do Failover Cluster Manager

Fonte: o autor (2025).

2.3 Backup com Veeam Backup

O Veeam é uma solução de backup e recuperação dos ambientes críticos de TI, garantindo a continuidade dos sistemas em caso de falhas ou desastres (VEEAM, 2024).

Na Agrex do Brasil a implementação do Veeam Backup é realizada em uma máquina virtual dedicada, responsável por gerenciar as tarefas de backup dos servidores e máquinas

virtuais. O armazenamento dos dados segue uma abordagem estruturada para garantir redundância e segurança:

1. Backup Primário: Os dados são armazenados em um storage de rede, garantindo fácil acesso e recuperação ágil em caso de necessidade;
2. Replicação para a Nuvem: Após a conclusão do backup local, os dados são replicados para um blob (*Binary Large Objects)* na nuvem da Microsoft, conhecida como Azure. O Azure é a plataforma de computação em nuvem da Microsoft, que oferece uma vasta gama de serviços, como armazenamento, computação, análise de dados e inteligência artificial. O Azure Blob Storage é uma solução de armazenamento na nuvem altamente escalável e robusta, projetada para armazenar grandes volumes de dados não estruturados, como documentos, imagens, vídeos e backups. Um blob é uma unidade de armazenamento que pode conter dados de qualquer tipo ou formato, com flexibilidade para ser acessado de maneira eficiente. Com a replicação para o Azure Blob Storage, os dados são mantidos em um ambiente seguro, protegido contra falhas críticas, ataques cibernéticos e desastres físicos, garantindo assim a continuidade do acesso e a integridade dos dados em cenários adversos.

A seguir, a Figura 11 mostra a seção Backup Infrastructure, onde os repositórios de backup são configurados e gerenciados. Na lista de Backup Repositories, podemos ver três repositórios configurados: AgrexBRVeeamBackup do tipo Microsoft Azure Blob Storage, armazenamento no Azure do backup realizado com o total de 8,7TB de espaço consumido e BackupRepository01 que é o repositório no storage local com 19,9TB de espaço consumido.

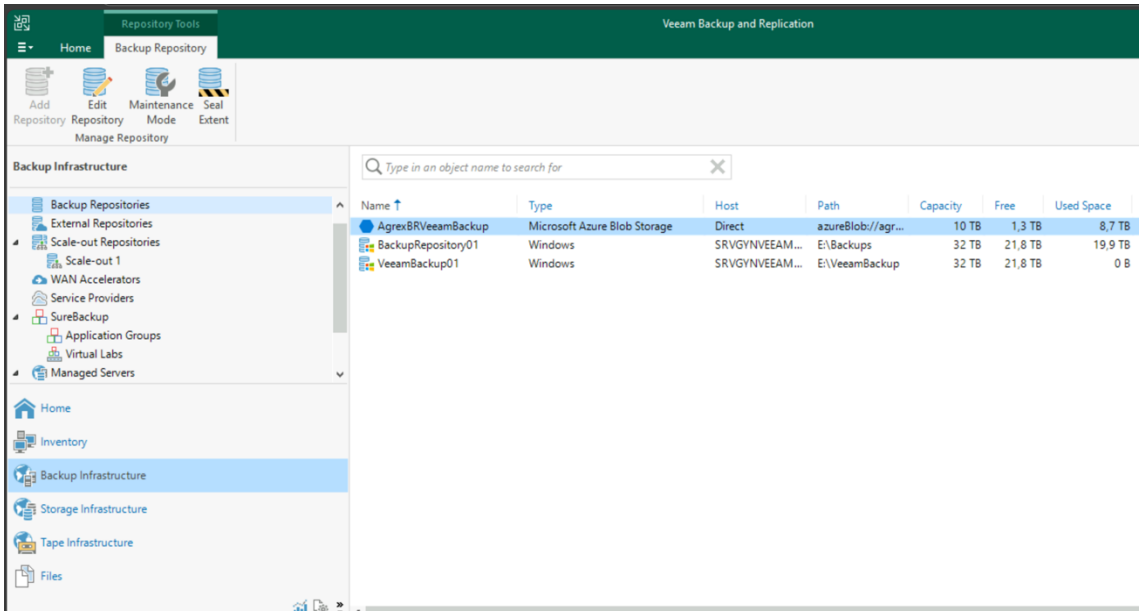

Figura 11. Repositórios de Armazenamento do Veeam Backup.

Fonte: O autor (2025)

Esse modelo de backup híbrido assegura que, mesmo em casos de falhas no ambiente *On-Premises*, a recuperação dos dados pode ser realizada a partir da cópia armazenada na nuvem.

A implementação de uma solução robusta de backup, como o Veeam Backup & Replication**,** é essencial para garantir a continuidade dos negócios e a proteção contra perdas de dados. No cenário de qualquer empresa a perda de dados pode ter implicações devastadoras, incluindo interrupções nos serviços, perda de informações críticas e até danos irreparáveis à reputação da empresa.

A perda de dados pode ocorrer devido a uma variedade de razões, como falhas de hardware, erros humanos, ataques cibernéticos (como ransomware) ou desastres naturais. Ransomware é um tipo de malware projetado para bloquear o acesso a sistemas ou dados de uma vítima, geralmente criptografando os arquivos, e exigindo um resgate para liberá-los. Esses ataques podem ser devastadores, pois além de causarem a perda temporária de acesso aos dados, podem resultar em danos financeiros significativos, caso a organização ceda ao pagamento do resgate. Quando uma organização não possui backups adequados ou uma estratégia de recuperação de desastres bem definida, ela corre o risco de sofrer custos financeiros elevados e prejuízos de longo prazo (VEEAM, 2014).

Segundo o estudo *"As empresas gastaram mais de US$ 2 milhões por ano com falhas na disponibilidade de dados"* divulgado pela Veeam em 2014, as empresas gastaram, em média, mais de US$ 2 milhões por ano devido a falhas na disponibilidade de dados. Esses custos

incluem perda de produtividade, impacto na receita e danos à comissão corporativa (VEEAM, 2014). Portanto, investir em soluções de backup e recuperação de desastres não é apenas uma precaução contra perdas inesperadas, mas uma estratégia essencial para garantir a continuidade operacional e minimizar impactos financeiros significativos.

2.3.1 Procedimento de Backups

Os backups no Veeam são configurados por meio de tarefas de Backup, que especificam quais máquinas virtuais, servidores e bancos de dados devem ser protegidos. A execução dos backups segue o cronograma abaixo:

- **Local**: Goiânia;
- **Frequência**: Diário/Semanal;
- **Retenção mínima**: 21 dias.

O acesso para verificação das tarefas de backup é realizado diretamente no servidor de backup, onde os administradores podem acompanhar a execução, identificar falhas e iniciar processos de recuperação de dados conforme necessário. Caso haja necessidade de backups pontuais ou recuperação de arquivos específicos, o solicitante deve registrar um chamado na ferramenta de suporte técnico para que a equipe de infraestrutura tome as devidas providências.

A Figura 12 exibe a tela do Veeam Backup and Replication, destacando os Jobs de Backup configurados, sua última execução, próximo agendamento, status e destino de armazenamento. A maioria dos jobs está com status *"Stopped"* e resultado *"Success",* indicando estabilidade, com apenas um alerta (*Warning*). O destino dos backups, identificado como *Scale-out* 1 inclui o repositório na nuvem Microsoft Azure Blob Storage, que oferece escalabilidade, resiliência e é ideal para retenção de longo prazo e recuperação de desastres.

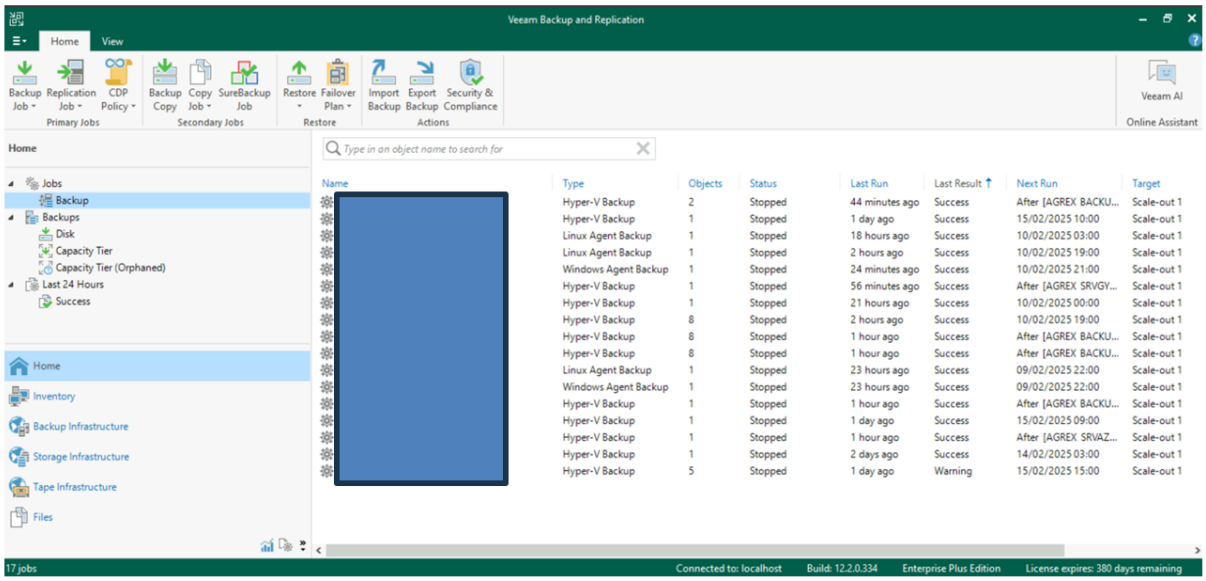

Figura 12. Tarefas de Backup do Veeam

Fonte: O autor (2025).

2.3.2 Monitoramento e Restauração de Dados

O monitoramento do backup é uma atividade que consiste no acompanhamento rotineiro da execução das tarefas de backup no Veeam, esse é um processo essencial para garantir que os dados estejam devidamente protegidos. Para isso, o analista de infraestrutura segue um protocolo baseado em checklist:

1. Abertura de chamado no Service Desk – nas atividades diárias, um chamado é aberto na ferramenta de suporte técnico para verificar se os backups foram executados corretamente;
2. Análise do status do backup – A equipe responsável acessa o Veeam Backup & Replication para conferir logs e relatórios da execução dos backups. Caso alguma falha seja identificada, um novo chamado é aberto para investigação;
3. Tratamento de falhas – Se um backup falhar, o analista de infraestrutura abre um chamado específico para correção, com aprovação da gestão de TI antes de qualquer ação corretiva;
4. Alertas automáticos – O sistema de backup está configurado para enviar alertas automáticos por e-mail para a lista de e-mail, notificando falhas e permitindo ações rápidas.

A recuperação de dados pode ser feita a partir do storage de rede ou, em casos mais críticos, por meio da replicação armazenada no Azure (nuvem da Microsoft). O processo de restauração depende do tipo de dado a ser recuperado e segue os padrões definidos pela equipe de infraestrutura.

A Regra 3-2-1 de Backup

A regra de backup 3-2-1 é uma estratégia eficaz para garantir a segurança dos dados e evitar perdas irreparáveis. Ela consiste em manter três cópias dos dados (o original e pelo menos duas de backup), armazená-las em dois tipos diferentes de mídia, como um disco rígido local e uma solução de armazenamento em nuvem, e manter uma cópia fora do local, em um espaço físico diferente, como um data center remoto ou na nuvem. Esse método proporciona redundância, minimiza riscos de falhas simultâneas e protege os dados contra desastres locais, como incêndios ou inundações. Na Agrex do Brasil, a Regra 3-2-1 é implementada da seguinte forma:

1. **Dados Originais nos Servidores de Produção**: Os dados de produção da Agrex estão armazenados nos servidores locais da empresa, garantindo que os dados operacionais estejam sempre disponíveis e acessíveis;
2. **Backup em Storage de Rede**: A primeira cópia de backup é feita em um **storage de rede** dedicado, que armazena os dados de forma centralizada e permite fácil acesso e recuperação, caso necessário;
3. **Replicação do Backup na Nuvem Microsoft Azure**: A segunda cópia de backup é replicada para a nuvem da Microsoft (Azure). A utilização do Azure Blob Storage garante que os dados estejam protegidos fora do local físico da empresa, oferecendo segurança adicional contra desastres ou falhas que possam afetar os backups locais.

Dessa forma, a Agrex segue a Regra 3-2-1, garantindo que seus dados estejam sempre protegidos, seguros e disponíveis para recuperação, minimizando riscos e impactos de possíveis falhas ou incidentes.

3. CONCLUSÃO

A implementação das soluções descritas ao longo deste relatório trouxe melhorias significativas para a infraestrutura de Tecnologia da Informação (TI) da Agrex do Brasil Ltda., fortalecendo a segurança, a disponibilidade e a eficiência operacional da empresa. A adoção de práticas robustas, como a configuração do *firewall Fortigate,* a implementação de clusters *Hyper-V* para alta disponibilidade e a estratégia de backup *com Veeam Backup & Replication,* garantiu maior proteção dos dados, continuidade dos serviços em caso de incidente de segurança e um gerenciamento de rede mais eficiente.

Além de contribuir para a segurança e resiliência dos sistemas corporativos, este trabalho proporcionou um aprendizado prático valioso, reforçando a importância de uma abordagem estratégica para a TI. A experiência adquirida ao longo da execução das atividades permitiu a aplicação dos conhecimentos teóricos obtidos durante a graduação, consolidando habilidades essenciais para o mercado de trabalho, como a análise de riscos, a tomada de decisões estratégicas e a implementação de soluções tecnológicas inovadoras.

Diante dos desafios cada vez mais complexos enfrentados pelas empresas no cenário digital, recomenda-se a adoção de práticas adicionais para aprimorar ainda mais a infraestrutura de TI da Agrex. Entre elas, destaca-se a implementação da imutabilidade nos backups, garantindo que os dados armazenados não possam ser alterados ou excluídos indevidamente, e a replicação do ambiente de virtualização como parte de um plano de *disaster recovery* eficiente. Essas melhorias permitirão um nível ainda maior de proteção e continuidade dos negócios.

Por fim, este relatório reforça a importância do investimento contínuo em tecnologia e boas práticas de gestão de TI para garantir a competitividade e a segurança das operações empresariais. O aprendizado obtido ao longo desse processo serve como base para futuras implementações e aprimoramentos, consolidando a infraestrutura tecnológica da empresa e assegurando sua preparação para os desafios do futuro.

REFERÊNCIAS

FORTINET. **Firewall de última geração**. Disponível em: https://www.fortinet.com/products/next-generation-firewall . Acesso em: 12 fev. 2025.

MORAES, Wellington Soares de; SILVA, Solange da. **Estudo do firewall Fortigate da Fortinet para auxiliar na segurança de dados de uma empresa**. In: III Jornada Científica da Escola Politécnica . Pontifícia Universidade Católica de Goiás, Goiânia, 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7991/1/artigo%20final%20rag.pdf. Acesso em: 12 fev. 2025.

VEEM. **Visão geral do Veeam Backup & Replication** . 2024. Disponível em: https://helpcenter.veeam.com/docs/backup/vsphere/overview.html?ver=120 . Acesso em: 12 fev. 2025.

VEEM. **As empresas gastaram mais de US$ 2 milhões por ano com falhas na disponibilidade de dados** . 2014. Disponível em: https://www.veeam.com/pt/company/press-release/empresas-gastam-mais-de-us2-milhoes-por-ano-com-falhas-na-disponibilidade-de-dados.html . Acesso em: 12 fev. 2025.

VIEIRA, Samuel Antonio. Cluster de alta disponibilidade com balanceamento de carga em máquinas virtuais: gerenciando banco de dados MariaDB com Galera Cluster. In: 19º Congresso Latino-Americano de Software Livre e Tecnologias Abertas , 2022. Disponível em: https://doi.org/10.5753/latinoware.2022.228075 Acesso em: 12 fev. 2025.

ANEXOS

D E C L A R A Ç Ã O

Declaramos para os devidos fins que se fizerem necessários que o(a) Sr(a). DIONE ALVINO COSTA GONÇALVES, portador(a) da carteira de identidade sob o nº 5746515/SSP-GO e CPF sob o nº 045.015.771-77, é nosso(a) colaborador(a) na empresa AGREX DO BRASIL LTDA inscrita sob o CNPJ 10.515.785/0003-50, admitido(a) em 13/12/2021, exercendo atualmente a função de ANALISTA DE INFRAESTRUTURA PL.

Tendo como principais atividades vinculadas a sua função:

Responsável pela gestão completa da infraestrutura de TI da empresa, com foco em redes, firewalls, servidores e soluções de backup. Suas atribuições incluem a implantação, manutenção, monitoramento e segurança desses sistemas essenciais, assegurando a disponibilidade, confiabilidade e integridade dos ativos de TI. Atua na administração de equipamentos como switches, servidores e access points, além de gerenciar políticas de segurança para proteger os dados e garantir a continuidade das operações.

Por ser verdade, firmamos a presente.

AGREX DO BRASIL LTDA

Goiânia – GO, 24 de março de 2025.

Carteira de Trabalho Digital

Data de emissão: 02/08/2019

Dados Pessoais

Nome civil
DIONE ALVINO COSTA GONCALVES

CPF [redacted]

Data de nascimento [redacted]

Contratos de trabalho

13/12/2021 - Aberto

Empregador
AGREX DO BRASIL LTDA.
CNPJ RAIZ: 10.515.785

Estabelecimento
AGREX DO BRASIL LTDA.
CNPJ: 10.515.785/0003-50
ROD GO 320 KM 3,0 SN 75600000 ZONA RURAL GOIATUBA GO

Cargo
ANALISTA DE INFRAESTRUTURA PL

CBO Cargo
2124-20

Tipo de contrato
Prazo indeterminado

Salário contratual [redacted]

Relação de trabalho
Empregado

Tipo de admissão
Admissão

Fonte da informação
ESOCIAL

ANOTAÇÕES

21/11/2024 - Férias 21/11/2024 a 05/12/2024
01/07/2024 - Salário definido [redacted]
01/07/2024 a (atual) - Cargo exercido de ANALISTA DE INFRAESTRUTURA PL
01/07/2024 - Relação de trabalho definida para Empregado
01/04/2024 - Férias 01/04/2024 a 15/04/2024
02/08/2023 - Férias 02/08/2023 a 19/08/2023
01/08/2023 - Salário definido [redacted]
01/07/2023 - Salário definido [redacted]
01/07/2023 a (atual) - Cargo exercido de ANALISTA DE INFRAESTRUTURA
30/01/2023 - Férias 30/01/2023 a 10/02/2023
01/12/2022 - Salário definido [redacted]
01/07/2022 - Salário definido [redacted]
01/07/2022 a (atual) - Cargo exercido de ANALISTA DE TI - INFRAESTRUTUR
13/03/2022 - Tipo de contrato definido para Prazo indeterminado
27/01/2022 a 12/03/2022 - Cargo exercido de ANALISTA DE TI - INFRAESTRUTURA
01/01/2022 - Estabelecimento definido para AGREX DO BRASIL LTDA.
13/12/2021 - Salário definido [redacted]
13/12/2021 - Tipo de contrato definido para Prazo determinado, definido em dias
13/12/2021 - Estabelecimento definido para AGREX DO BRASIL LTDA.
13/12/2021 a (atual) - CBO Cargo exercido 2124-20
13/12/2021 - Admissão