



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

RELATÓRIO TÉCNICO

**SEGURANÇA E POLÍTICA:
REDES DE COMPUTADORES**

GRUPO

Augusto Henrique Lage

Camila Ferreira Borges

Kener de Almeida Silva

Pedro Henrique Rodrigues da Silva

Sergio de Oliveira Bernardes Nunes

Raynan Rainer Ferreira de Almeida

2023

SUMÁRIO

1 Introdução	4
2 Objetivos.....	4
3 Dever de todos.....	5
4 Requisitos de Segurança	6
4.1 Aspectos importantes	6
4.1.1 Confidencialidade	6
4.1.2 Integridade	7
4.1.3 Disponibilidade	7
4.1.4 Autenticidade	8
5 Política de Segurança	9
5.1 Gerenciamento de Acesso	9
5.2 Responsabilidades do Usuário.....	9
5.3 Monitoramento e Auditoria.....	9
5.4 Métodos de Autenticação	9
5.5 Treinamento e Conscientização.....	10
5.6 Monitoramento e Melhoria Contínua.....	11
5.7 Conformidade com Regulamentos	12
6.1 Avaliação da Infraestrutura Existente	12
7 CONSTRUÇÃO DE UMA NOVA REDE.....	14
7.1 Implementação de um Firewall	14
7.2 Configuração iniciais do pfSense	15
7.3 Configurado o certificado de confiança.....	18
7.4 Backup do Firewall.....	20
7.5 FailOver	21
7.5 Loadbalance	22
7.6 Teste primário de intrusão.....	23
7.7 IDS/IPS Snort.....	25
7.7.1 O que é um IDS?.....	25
7.7.2 Métodos de detecção.....	25
7.8 Controle de navegação Squid Web Proxy	28
7.8.1 - Logs de Acesso	31
7.8.1 - Logs de Acesso	32
8 SERVIDORES DE AUTENTICAÇÃO E FILE SERVER	34

8.1 Exemplo de acesso para um usuário do setor Financeiro	35
8.3 Servidor de Autenticação – Política de grupo.....	37
9 BACKUP	40
9.1 O que é backup?	40
9.2 Por que é importante manter o backup atualizado?	40
9.2 Implementação da Ferramenta	41
11.1 Interfaces de gerenciamento no Host.....	50
12 SOLUÇÃO WIRELESS - ACCESS POINTS	52
12.1 Configurações iniciais dos access point	53
13 GERENCIAMENTO DE ATIVOS.....	54
13.1 Qual importância do gerenciamento de ativos?.....	54
13.2 Como pode ser realizado a gestão de ativos?	55
13.3 Upgrade das estações.....	56
14 CONSCIENTIZAÇÃO E CAPACITAÇÃO.....	58
REFERÊNCIAS	59

LISTA DE FIGURAS

Figura 1 – Topologia proposta.....	14
Figura 2 – Informações de sistema do pfSense	15
Figura 3 – Interfaces de rede	16
Figura 4 – Interfaces de vLan configuradas	16
Figura 5 - Regras interface da interface vLan Servidores	16
Figura 6 – Regras interface da interface vLan Estações.....	17
Figura 7 – Confiança Firewall x Domínio – Sem certificado.....	18
Figura 8 – Configurando Autoridade Certificadora – Certificado de Servidor.....	19
Figura 9 – AC – Certificado de Instalado.....	19
Figura 10 - Configurando o Auto Backup do Firewall.....	20
Figura 11 - Comportamento dos Backups	21
Figura 12 - Device Key - pfSense	21
Figura 13 - Configuração do Failover no pfSense.....	22
Figura 14 - Configuração do Failover no pfSense.....	22
Figura 15 – Configuração do balanceamento de Links	23
Figura 16 – Aplicação do balanceamento de Links.....	23
Figura 17 – Teste de Intrusão Inicial	24
Figura 18 – Log pfSense durante o teste de intrusão.....	24
Figura 19 – Log de tráfego IDS na interface vLan20.....	26
Figura 20 – Log de tráfego IDS na interface Wan	27
Figura 21 – Bloqueio de endereços ip	28
Figura 22 – Filtros por categorias do SquidGuard	29
Figura 23 – Log do SquidGuard.....	29
Figura 24 – Grupos de controle de acesso web - SquidGuard.....	30
Figura 25 – Grupos para controle de acesso Web - ADDS	30
Figura 26 – Tela de Bloqueio com Inspeção SSL - 1	31
Figura 27 – Tela de Bloqueio com Inspeção SSL - 2.....	31
Figura 28 – Log do Squid	31
Figura 29 – Log do SquidGuard	32
Figura 30 – Relatório do Squid – Parte 1	32
Figura 31 – Relatório do Squid – Parte 2	33
Figura 32 – Relatório do Squid – Parte 3	33
Figura 33 – Estrutura de domínio da empresa	34
Figura 34 – Estrutura de domínio da empresa – Permissões de rede - Parte 1.....	35
Figura 35 – Estrutura de domínio da empresa – Permissões de rede - Parte 2.....	36
Figura 36 – Estrutura de domínio da empresa – Enumeração baseada em acesso	36
Figura 37 – Estrutura de diretórios – Permissão de acesso total	37
Figura 38 – Estrutura Organizada – Aplicação de GPOS básicas	38
Figura 39 – Estrutura Organizada – Aplicação da GPO Default.....	39
Figura 40 – Estrutura Organizada – Servidores Primário e Secundário	39
Figura 41 – Job de Backups no console de Administração do Veeam.....	42
Figura 42 – Configuração da aba de manutenção da solução Veeam	43
Figura 43 – Resultado do job de Backup.....	44

Figura 44 – Storage de Armazenamento	44
Figura 45 – Exclusão servidores AD e File Server	45
Figura 46 – Resumo das configurações do recovery	46
Figura 47 – Console de Administração do WSUS	47
Figura 48 – Dashboard de Gerenciamento	48
Figura 49 – Eventos do dispositivo	49
Figura 50 – Status do Dispositivo	49
Figura 51 –Políticas de Endpoint	50
Figura 52 –Guia de Status	51
Figura 53 – Guia de Eventos	51
Figura 54 – Guia Detecções.....	52
Figura 55 – Página de configuração dos SSIDs dos Access Point	53
Figura 56 – Página de configuração das vlans 30 e 31.....	53
Figura 57 – Visibilidade dos Aps	54
Figura 58 – Exemplo de controle de ativos de TI no GLPI.....	55
Figura 59 – Dashboard dos reports GLPI.....	56
Figura 60 – Ficha técnica do computador Novo OptiPlex Micro da Dell	57

1 Introdução

A segurança da rede de computadores seja ela em uma empresa de pequeno, médio ou grande porte é um aspecto crítico que deve ter a devida atenção para proteger as informações e recursos tecnológicos contra ameaças cibernéticas.

Segundo o relatório da Kaspersky, empresa internacional de cibersegurança e privacidade digital, os ataques hackers em pequenas e médias empresas Brasileiras cresceram 41% de janeiro a abril de 2022, em comparação ao mesmo período do ano passado. Esse crescimento é alarmante, pois em uma pesquisa da National Cyber Security Alliance em 2017, foi identificado que 60% das empresas médias e pequenas que sofrem um ciberaataque fecham as portas 6 meses depois do ocorrido.

As redes de computadores são cada vez mais complexas e interconectadas, tornando-se cada vez mais um alvo atraente para os cibercriminosos. Estes ataques podem causar uma variedade de danos, incluindo roubo de dados, interrupção de serviços, ataques físicos e até mesmo a falência de uma empresa. Abordaremos ao decorrer deste documento algumas formas de tentar reduzir estes ataques.

A informação pode existir em diversos formatos tais como: impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio eletrônico e/ou por outros meios eletrônicos, mostrada em filmes ou falada em conversas. Independentemente de sua natureza ou de sua origem, e da forma apresentada, compartilhada e/ou armazenada, ela deve estar protegida de acordo com sua relevância em relação ao negócio das empresas.

2 Objetivos

Garantir a confidencialidade, integridade, disponibilidade e legalidade da informação necessária para o negócio.

A implementação dessa política é importante para sustentar e demonstrar a capacidade e integridade em lidar com todas as partes interessadas. Portanto, essa política assegura que:

- As informações estão protegidas contra acesso não autorizado;
- A confidencialidade da informação é mantida;
- As informações não são divulgadas às entidades não autorizadas por meio de ações deliberadas ou descuidadas;
- A integridade das informações é mantida para impedir modificações não autorizadas;

- As informações estão disponíveis para usuários autorizados, quando necessário;
- Requisitos contratuais, de regulamentação e legais são cumpridos;
- Sempre que ocorrer alterações legais, regulamentares ou normativas que impactem o negócio, uma análise crítica é realizada a fim de que as adequações, se necessário, sejam realizadas;
- Os planos de continuidade da atividade são produzidos, mantidos e testados de acordo com as expectativas da gestão;
- Treinamento de segurança da informação e privacidade são dados a todos os colaboradores e, quando aplicável, a provedores externos;
- Potenciais violações de segurança da informação e suspeitas de vulnerabilidades sejam relatadas, investigadas e mitigadas;
- Cada indivíduo tenha conhecimento adequado dos controles de gestão, dos controles operacionais e técnicos que ajudam a proteger os recursos e bens tecnológicos de informação;
- As metas e objetivos são divulgados para as partes interessadas envolvidas, para que cada indivíduo tenha uma compreensão adequada de seu papel e responsabilidade em relação à segurança da informação e à missão da organização;
- As políticas, procedimentos e práticas são comunicados às partes;

3 Dever de todos

- I. Zelar pela Segurança da Informação na Empresa/Instituição;
- II. Seguir as diretrizes contidas nesta política e demais políticas e procedimentos de segurança da informação;
- III. Manter a segurança física de equipamentos e informações;
- IV. Participar dos programas de conscientização providos;
- V. Informar fragilidades, vulnerabilidades e riscos pertinentes a Segurança da Informação que venham a ter conhecimento;
- VI. Acompanhar incidentes e propor melhorias, evitando reincidências de problemas;
- VII. Utilizar com responsabilidade e para fins de trabalho e de forma profissional, ética e legal os ativos de tecnologia da informação;
- VIII. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

- IX. Garantir que os sistemas e informações sob sua responsabilidade estejam protegidos;
- X. Comunicar qualquer descumprimento da Política de Segurança da Informação.

4 Requisitos de Segurança

Existe uma série de diretrizes que podem ser seguidas para proteger as redes de computadores contra-ataques. Essas diretrizes incluem:

- Políticas e procedimentos de segurança;
- Implementar tecnologias de segurança;
- Capacitar os usuários;
- Monitorar o ambiente;
- Usar política de senhas fortes;
- Autenticação de dois fatores (2FA);
- Sistemas atualizados;
- Uso de VPN para conexões remotas;
- Restrições de acesso;
- Backup;
- Antivírus;

4.1 Aspectos importantes

4.1.1 Confidencialidade

Segundo o Princípio da Confidencialidade, a informação pode ser acessada apenas por pessoas autorizadas – isso significa o sigilo da informação. Portanto, a confidencialidade garante o sigilo da informação e impede que pessoas não autorizadas tenham acesso ao conteúdo.

Exemplo de ferramenta: A Criptografia.

É uma técnica que embaralha a informação por meio de algoritmos, e faz com que a informação se transforme em algo ininteligível.

4.1.2 Integridade

De acordo com o Princípio da Integridade, **a informação só pode ser alterada por pessoas autorizadas**, ou seja, a Integridade garante o controle das alterações, impedindo que pessoas não autorizadas façam alterações indevidas na informação. O princípio da integridade também garante a completude da informação, para que não haja perda de partes da informação.

Exemplo de ferramenta: Assinatura Digital e Backup.

Assinatura Digital: Quando o usuário assina digitalmente um documento, qualquer alteração que for feita no documento violará essa assinatura. Portanto, se houver alteração em um documento assinado digitalmente ou eletronicamente, ele precisará ser assinado novamente, pois a assinatura anterior foi violada. A assinatura garante o controle das alterações.

Backup: A completude faz parte do backup. Quando parte da informação se corrompe e o usuário restaura o backup, a totalidade da informação é recuperada, tornando-se íntegra novamente.

4.1.3 Disponibilidade

De acordo com o Princípio da Disponibilidade, a informação estará disponível sempre que for preciso. Esse aspecto é de suma importância, principalmente para sistemas que não podem ficar indisponíveis, pois essas falhas comprometem o serviço.

As ferramentas que garantem o princípio da Disponibilidade são o Nobreak, o Firewall e o Backup.

Nobreak: Dispositivo alimentado por baterias, capaz de fornecer energia elétrica a um sistema durante um determinado período, em situações de emergência, no caso de interrupção do fornecimento de energia da rede pública. Ou seja, o Nobreak impede que o sistema desligue e é uma ferramenta de Disponibilidade.

Firewall: O Firewall é uma barreira de proteção e um dispositivo indispensável dentro de uma organização. Ele impede que ataques de intrusão e de negação de serviço sejam efetuados no ambiente.

Backup: Quando uma informação é corrompida, ela se torna indisponível. O backup recupera essa informação, tornando-a disponível novamente.

4.1.4 Autenticidade

O Princípio da Autenticidade garante a veracidade da autoria da informação, porém, não garante a veracidade do conteúdo da informação. A autenticidade garante a veracidade do autor, de quem de fato produziu aquela informação, não importando se o conteúdo é verdadeiro ou falso.

Não Repúdio: A Autenticidade garante também um subproduto, que é o Não Repúdio. *O Não Repúdio está contido na autenticidade e significa que o autor da informação não tem como negar que ele é o verdadeiro autor.*

Ferramentas que garantem o Princípio da Autenticidade

Biometria: A Biometria é uma ferramenta que verifica algumas características físicas da pessoa para certificar que aquela característica identifica a pessoa unicamente. A Biometria é muito utilizada nos bancos.

Assinatura Digital: A assinatura digital identifica unicamente o autor da informação, garantindo a autenticidade.

Certificados Digitais: Os certificados Digitais garantem a autenticidade da autoria dos sites. Ex.: Quando um usuário acessa um site de comércio eletrônico, geralmente há um cadeado no canto da tela, que mostra o certificado digital do site, afirmando que aquele site de fato pertence àquela empresa.

5 Política de Segurança

Estabelecer diretrizes para garantir a segurança das informações corporativas, buscando o equilíbrio entre performance e confiabilidade, objetivando a perenidade dos negócios da empresa/instituição, fundamentadas nos seguintes itens:

5.1 Gerenciamento de Acesso

A equipe de TI é responsável por atribuir, modificar e revogar direitos de acesso de acordo com a aprovação e a política da empresa.

Revisões regulares das permissões de acesso serão realizadas para garantir que os usuários ainda tenham apenas o acesso necessário para realizar suas funções.

5.2 Responsabilidades do Usuário

Os usuários são responsáveis por manter suas credenciais de acesso seguras e não devem compartilhá-las com outros indivíduos.

Os usuários devem seguir as práticas de segurança definidas pela empresa, incluindo a utilização de senhas fortes e a adoção de medidas de proteção contra malware.

5.3 Monitoramento e Auditoria

A atividade de acesso à rede pode ser monitorada para fins de auditoria e detecção de atividades suspeitas, é nesse ponto que a contratação de um bom serviço de proteção de endpoint se torna o principal aliado, trazendo logs e relatórios sobre a atividade do usuário.

A violação desta política ou tentativas de acesso não autorizado podem resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho.

5.4 Métodos de Autenticação

Definir os métodos de autenticação a serem utilizados para proteger o acesso aos sistemas e recursos de tecnologia da informação.

- a) Senha:** Todos os usuários devem ter uma senha única e forte para acessar os sistemas. Senhas devem seguir as seguintes diretrizes:
- ✓ Ter no mínimo 8 caracteres.
 - ✓ Incluir pelo menos uma letra maiúscula e uma letra minúscula.
 - ✓ Incluir pelo menos um número.
 - ✓ Incluir pelo menos um caractere especial.
 - ✓ Senhas devem ser alteradas a cada 90 dias.
 - ✓ Senhas antigas não podem ser reutilizadas.

As senhas devem ser mantidas confidenciais e não compartilhadas com outros usuários.

- b) Autenticação Multifator (MFA):** Para acesso a sistemas e recursos críticos, a autenticação multifator é obrigatória. Isso inclui, pelo menos, dois dos seguintes fatores:
1. Algo que você sabe: Senha ou PIN.
 2. Algo que você possui: Token de autenticação, aplicativo de autenticação móvel, cartão inteligente.
 3. Algo que você é: Biometria (impressão digital, reconhecimento facial etc.).
- c) Certificados Digitais:** Para acessar recursos especialmente sensíveis, o uso de certificados digitais pode ser requerido. Esses certificados devem ser emitidos e gerenciados pela equipe de TI da [Nome da Empresa].
- d) Autenticação por Token:** Alguns usuários poderão usar dispositivos de token físico ou aplicativos de autenticação móvel para autenticar o acesso. Esses tokens geram códigos únicos que são inseridos junto com a senha.

5.5 Treinamento e Conscientização

- a) Conscientização:** Os usuários serão capacitados sobre a importância de senhas fortes e práticas de segurança de senhas por meio de treinamentos regulares de segurança da Informação além da divulgação dos comunicados encaminhados via e-mail.
- b) Melhores Práticas:** Os usuários receberão orientações sobre como criar senhas seguras e como protegê-las para que possam pôr em prática.
- c) Testes de Capacitação:** Podem ser feitos na admissão do funcionário para atestar a capacidade de adaptação aos sistemas e ferramentas internas reduzindo assim a chance de algum erro operacional. Os treinamentos também podem ser realizados sempre que

a empresa perceber que é necessário reforçar a conscientização dos funcionários ou quando houver alteração de funções e remanejamento de funcionários.

- d) Trabalho em conjunto:** É de suma importância a parceria com outros setores como Marketing, RH e Jurídico para o desenvolvimento de ações de divulgação, conscientização e confecção de regras e penalidades por violações de segurança, por exemplo, trabalhar junto ao Marketing para desenvolver comunicados de alterações ou atualizações nas regras de segurança via cartazes/banners, hotspot ou newsletters. O Jurídico pode ajudar no desenvolvimento de termos de responsabilidade/confidencialidade e na aplicação de sanções legais quanto a violação de leis e de protocolos internos e o RH na conscientização dos colaboradores já no primeiro contato com a empresa.

Todos os usuários serão treinados na correta utilização dos métodos de autenticação, incluindo a importância de manter suas senhas confidenciais e adotar práticas de segurança adequadas.

5.6 Monitoramento e Melhoria Contínua

Esta política será revisada anualmente para garantir a sua relevância e eficácia. Alterações na política serão comunicadas a todos os usuários e aprovadas pela alta direção.

Esta política de acesso à rede é um exemplo genérico e deve ser adaptada às necessidades, regulamentos e características específicas da organização em questão. Ela serve como um guia para estabelecer diretrizes claras para o acesso à rede, a fim de garantir a segurança e o uso apropriado dos recursos de TI.

A eficácia dos métodos de autenticação será periodicamente avaliada pela equipe de TI.

Serão realizados testes de penetração para avaliar a resistência dos métodos de autenticação a ataques.

Novos ataques surgem constantemente e é importante repassar essas informações aos colaboradores, principalmente da equipe de TI. Por isso a atualização constante é uma parte fundamental, afinal há sempre novas estratégias sendo criadas por cibercriminosos. Deve ser compartilhado com os colaboradores dicas periodicamente, a parceria com empresas especializadas para a realização de treinamentos e certificação também é um dos meios de

preparação da equipe diante da apresentação de novos modelos de ameaças como, por exemplo, spear phishing e maneiras de como identificar links e-mails mal-intencionados.

5.7 Conformidade com Regulamentos

Garantir que a política de métodos de autenticação esteja em conformidade com regulamentos de segurança de dados e outras leis aplicáveis.

Esta política de métodos de autenticação é um exemplo que pode ser adaptado para atender às necessidades e regulamentos específicos da organização. A segurança da autenticação é crucial para proteger os sistemas e recursos da empresa contra ameaças internas e externas.

6.0 INFRAESTRUTURA – PROJETO

Esta etapa visa garantir a eficácia na avaliação da infraestrutura existente, seus pontos fortes e fracos, e também, as possibilidades de aproveitamento que podem surgir durante o processo de implementação dos novos processos e reestruturação da empresa

6.1 Avaliação da Infraestrutura Existente

Nossa equipe foi contactada por uma empresa no ramo de educação para fazer uma avaliação da sua infraestrutura atual, pois estavam enfrentando muitos problemas com lentidão, travamentos, quedas na conexão e reclamações recorrentes.

Ao chegamos ao local foi feito um checklist para verificar primeiramente as coisas básicas. Nos deparamos com uma infraestrutura precária, em que não havia qualquer tipo de padrão, organização e garantias de continuidade.

- Não havia um CPD, Rack, Patch Painel ou qualquer organização para a rede;
- O acesso à rede wireless era através de roteadores convencionais.
- Com apenas um link de 200mb a conexão é feita pelo roteador da operadora, sem quaisquer tipos controle.
- Havia muitos switchs 10/100 que criavam pontes e aumentava o broadcast da rede e ainda não aproveitavam os 200mb disponíveis para uso.
- Os acessos nas estações de trabalho eram feitos de forma local sem qualquer restrição,

- Os arquivos eram salvos em um computador comum com uma pasta compartilhada publicamente.
- Não havia nenhum firewall para fazer um controle mais adequado da rede;
- Não havia nenhum switch gerenciável para possível segmentação da rede;
- Não havia redundância de links;
- Não havia controle de acesso com diretivas de senhas;
- Não havia um serviço de diretório com níveis de permissão;

Sendo assim, fomos diretamente no que era básico e crítico em que a empresa precisaria para começar a tomar um corpo, devido ao limite de orçamento inicial.

Para isso, precisamos realizar uma análise do impacto da indisponibilidade apresentada, avaliando-se os processos e ferramentas dos componentes de serviços críticos, juntamente com a análise dos pontos fracos em relação a infraestrutura existente e acima de tudo, levantamento de medidas preventivas e recomendações para evitar tal indisponibilidade e fragilidade da segurança.

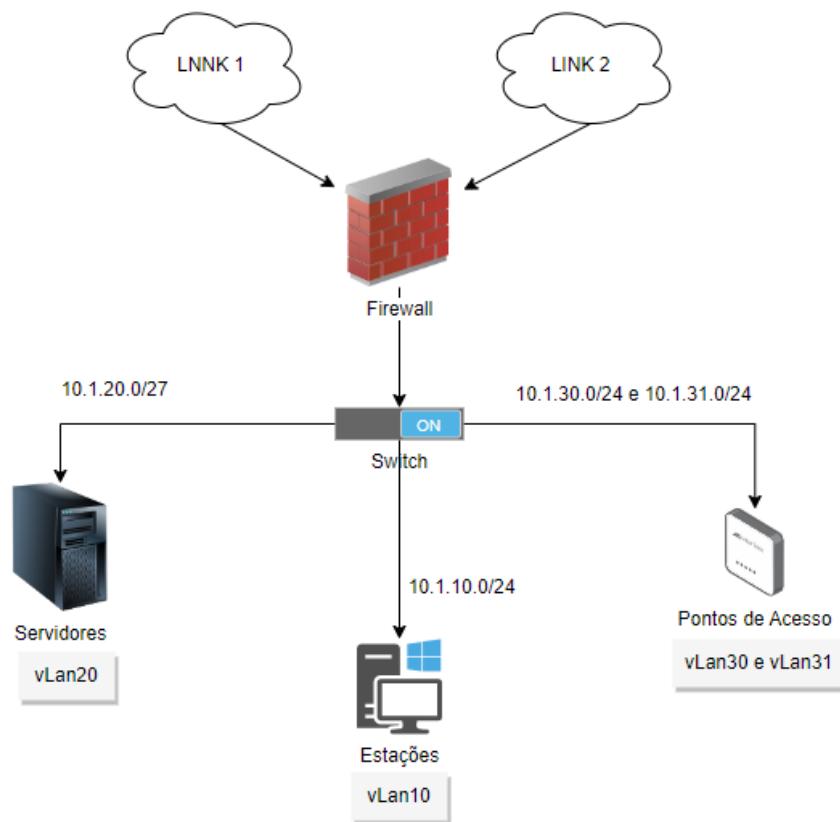
Após a realização da identificação, análise e tratamento de riscos, seu gerenciamento precisa ser constantemente monitorado e revisto. O monitoramento deve ser feito com base na vigilância cotidiana dos sistemas, tendo em vista que os cenários são dinâmicos e susceptíveis a mudanças. A revisão do processo deve ocorrer frequentemente levando em conta as variáveis do ambiente com o intuito de mantê-los atualizados. (DANTAS,2011)

- ✓ Firewall;
- ✓ Um Servidor de controle de acesso e autenticação
- ✓ Um File Server;
- ✓ Um servidor de Backup.

7 CONSTRUÇÃO DE UMA NOVA REDE

Considerado os pontos citados anteriormente, começamos as tarefas estudando qual seria a melhor forma de fazer essa reestruturação de forma que o impacto financeiro não fosse tão grande. Optamos por trabalhar com virtualização dos servidores, utilizando o Microsoft Hyper-V. Inicialmente nós iremos implementar as soluções mais críticas como mencionado anteriormente. A topologia proposta está logo abaixo.

Figura 1 – Topologia proposta



Fonte: o autor

7.1 Implementação de um Firewall

O Firewall será um dos maiores desafios, uma vez que o mesmo nos possibilita fazer o controle do que pode ou não ter acessado dentro de uma empresa. Como os usuários desta empresa estão mal-acostumados a acessar qualquer conteúdo, um firewall pode causar um ruído enorme em uma equipe. O que nos levará a todo um processo de treinamento e conscientização do uso da internet em um ambiente corporativo.

Para reduzir os custos, optamos em implementar o pfSense que atualmente está na versão 2.7. Um firewall Open Source globalmente usado e de grande escala, será o suficiente para conseguir fazer um belo upgrade neste projeto.

Iremos separar as redes por vlan e configurar a segmentação conforme necessidade para redução de broadcast:

- ✓ **Lan:** Trabalhando com a parte gerencial no range 192.168.1.0/24;
- ✓ **Estações:** vLan 10 com a range de endereços: 10.1.10.0/24;
- ✓ **Servidores:** vLan 20 com a range de endereços: 10.1.20.0/27;
- ✓ **Wireless:** vLan 30 e 31 com os range 10.1.30.0/24, 10.1.31.0/24;

7.2 Configuração iniciais do pfSense

Ainda iremos abordar neste documento, mas já foram instalados e disponibilizados os servidores de Active Directory da empresa, denominado com o domínio cecc.edu. Abaixo é apresentado parte da Dashboard interna do firewall pfSense, começaremos com o básico, colocar a internet para funcionar e os usuários para autenticarem no domínio **cecc.edu**.

Figura 2 – Informações de sistema do pfSense

System Information	
Name	fw.cecc.edu
User	admin@192.168.10.200 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: df4e31743fa5a468508b
BIOS	Vendor: Microsoft Corporation Version: Hyper-V UEFI Release v4.1 Release Date: Thu Dec 3 2020
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT
<i>Unable to check for updates</i>	

Fonte: o autor

Logo abaixo, demonstramos as interfaces instaladas no pfSense: WAN, LAN e DMZ.

Figura 3 – Interfaces de rede

Interface	Network port
WAN_LINK1	hn0 (00:15:5d:0a:c8:0d)
LAN	hn1 (00:15:5d:0a:c8:19)
DMZ	hn2 (00:15:5d:0a:c8:1c)

Fonte: o autor

As interfaces que configuramos as vlans para segmentação da rede.

Figura 4 – Interfaces de vLan configuradas

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	
hn1 (lan)	10		vLAN_ESTACOES	
hn1 (lan)	20		vLAN_SERVIDORES	
hn1 (lan)	30		vLAN_WIFI CORPORATIVO	
hn1 (lan)	31		vLAN_WIFI VISITANTES	

Fonte: o autor

Algumas regras básicas foram configuradas no firewall para limitar a comunicação entre as redes, principalmente quanto aos servidores. A princípio trataremos o firewall de forma restritiva, o State-Ful posteriormente será liberado conforme necessidade.

Figura 5 - Regras interface da interface vLan Servidores

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B +≡	IPv4 TCP	VLAN20_SERVIDORES net	*	This Firewall	4443	*	none		Liberar WebGUI - FW	
BLOQUEIOS											
<input type="checkbox"/>	0/0 B ✖+≡	IPv4 TCP/UDP	VLAN20_SERVIDORES net	*	BLACKLIST	*	*	none		BLACKLIST	
<input type="checkbox"/>	0/0 B ⌚+≡	IPv4 TCP	VLAN20_SERVIDORES net	*	*	LOG_NOISE	*	none		Redução de Log Noise	
LIBERA LAN TO WAN											
<input type="checkbox"/>	0/2 Kib <u>echoreq, echored</u>	IPv4 ICMP	VLAN20_SERVIDORES net	*	*	*	*	none		Libera ICMP	
<input type="checkbox"/>	2/13.41 Mib +≡	IPv4 TCP/UDP	VLAN20_SERVIDORES net	*	*	WEB_PORTS	*	none		Liberar acesso Web	
<input type="checkbox"/>	69/425 Kib	IPv4 UDP	VLAN20_SERVIDORES net	*	*	53 (DNS)	*	none		Liberar consulta DNS	

Fonte: o autor

Figura 6 – Regras interface da interface vLan Estações

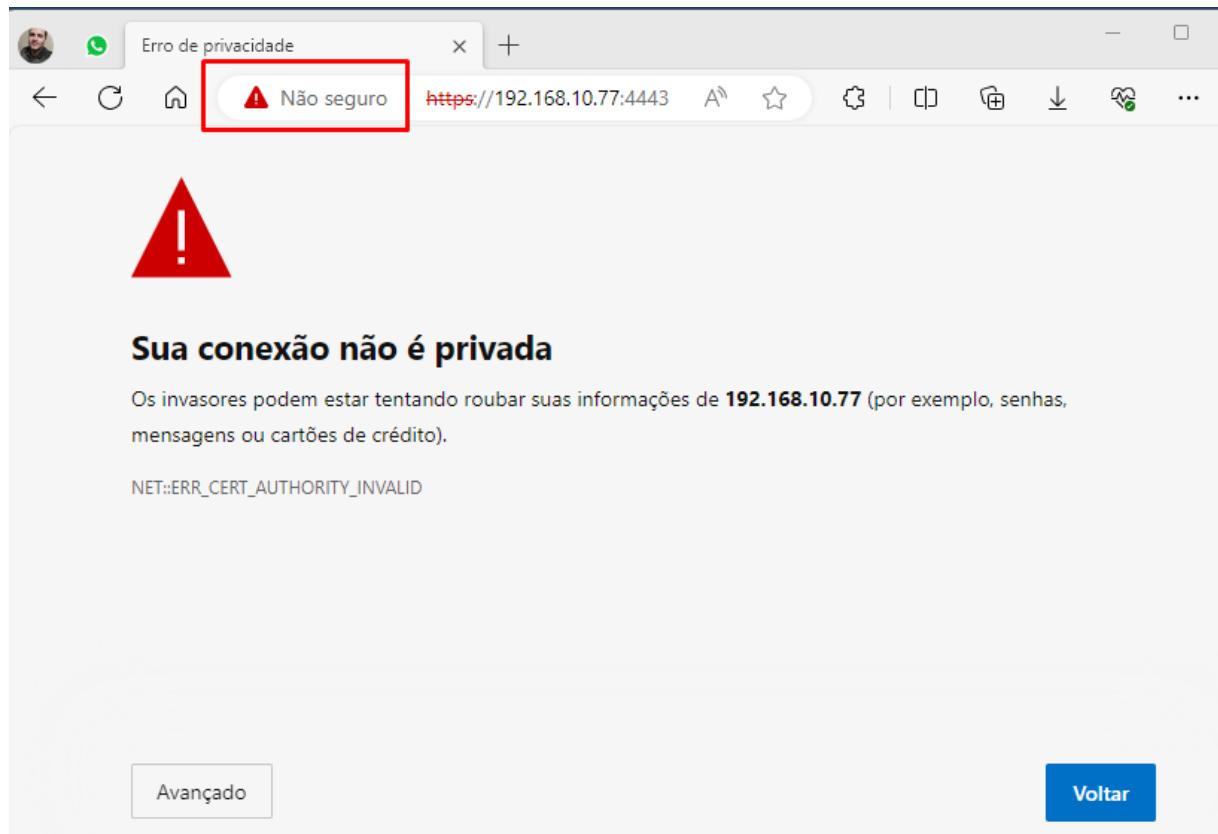
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/0 B KIB	IPv4 TCP net	VLAN10_ESTACOES	*	This Firewall	4443	*	none	Liberar WebGui - FW	
LIBERAÇÕES INTERNAS											
<input type="checkbox"/>		0/84 KIB	IPv4 UDP net	VLAN10_ESTACOES	*	DNS_INTERNO	53 (DNS)	*	none	Libera consulta DNS	
<input type="checkbox"/>		1/817 KIB	IPv4 TCP/UDP net	VLAN10_ESTACOES	*	VLAN20_SERVIDORES net	ADDS_PORTS	*	none	Libera Serviços Windows	
<input type="checkbox"/>		0/30 KIB	IPv4 TCP/UDP net	VLAN10_ESTACOES	*	ADDS_DOMAINS	49152 - 65535	*	none	Portas Dinâmicas no Windows Server	
BLOQUEIOS											
<input type="checkbox"/>		0/0 B KIB	IPv4 TCP/UDP net	VLAN10_ESTACOES	*	BLACKLIST	*	*	none	BLACKLIST	
<input type="checkbox"/>		0/0 B	IPv4 TCP net	VLAN10_ESTACOES	*	*	LOG_NOISE	*	none	Redução de Log Noise	
LIBERA LAN TO WAN											
<input type="checkbox"/>		0/3 KIB echoreq, echoreq	IPv4 ICMP net	VLAN10_ESTACOES	*	*	*	*	none	Libera Ping	
<input type="checkbox"/>		0/0 B	IPv4 TCP net	VLAN10_ESTACOES	*	DNS_EXTERNO	53 (DNS)	*	none	DNS_EXTERNO	
<input type="checkbox"/>		3/943 KIB	IPv4 TCP/UDP net	VLAN10_ESTACOES	*	*	WEB_PORTS	*	none	Liberar acesso Web	
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP net	VLAN10_ESTACOES	*	*	EMAIL_PORTS	*	none	Portas de serviço de email	

Fonte: o autor

7.3 Configurado o certificado de confiança

Por padrão, ao acessar a interface web do pfSense nos deparamos com uma notificação que pode até assustar um usuário final:

Figura 7 – Confiança Firewall x Domínio – Sem certificado



Fonte: o autor

Embora não tenha um impacto no comportamento do firewall, é importante manter tudo alinhado e configurado. Sendo assim, configuramos uma **Autoridade Certificadora** dentro do pfSense e geramos um certificado para que as estações e servidores do domínio passem a confiar no firewall, podemos verificar o mesmo na figura 7. Para aumentar a segurança do firewall, ainda configuramos para o mesmo ser acessado apenas via protocolo **https**, ajustando ainda uma porta mais alta tirando do padrão que é a 443. Assim, tornamos nosso firewall mais seguro dificultando um possível ataque ou invasão, veja o exemplo na figura 8.

Figura 8 – Configurando Autoridade Certificadora – Certificado de Servidor

The screenshot shows the 'Authorities' tab selected in the 'Certificates / Authorities' menu. A search bar at the top allows for searching by certificate name or distinguished name. Below the search bar is a table titled 'Certificate Authorities' with the following columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. One entry is listed:

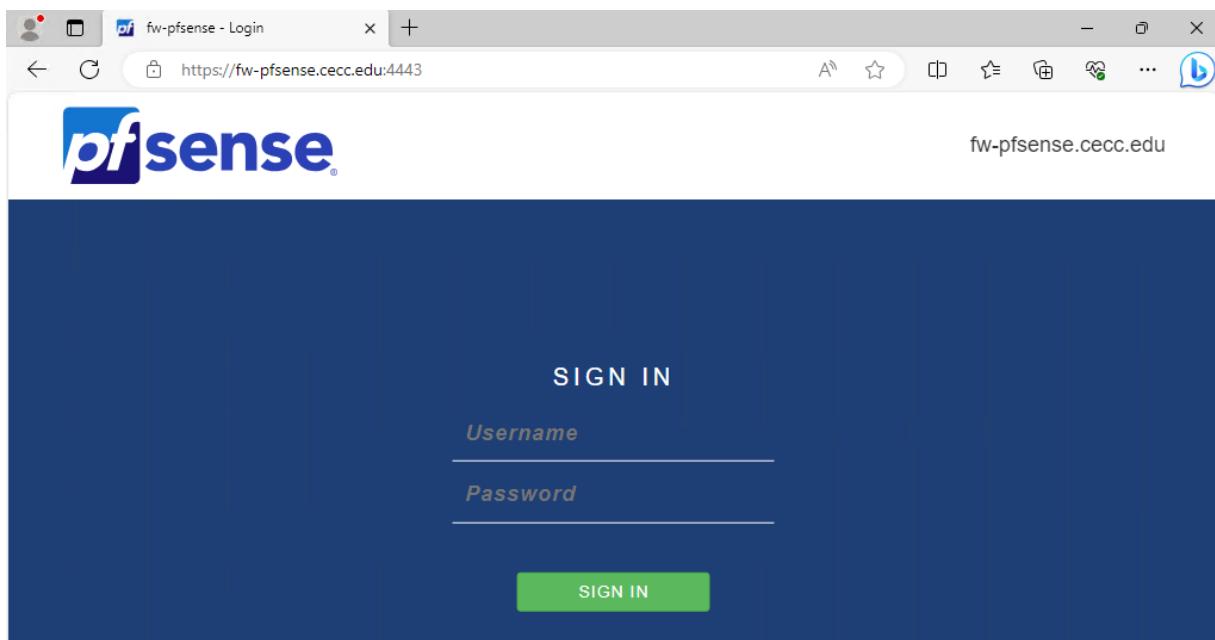
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-FIRWall	✓	self-signed	1	ST=MG, OU=TI, O=CECC, L=GV, CN=CA-FIREWALL, C=BR <small>i</small>		

Details for the CA-FIRWall entry:

- Valid From: Thu, 21 Sep 2023 11:47:03 -0300
- Valid Until: Sun, 18 Sep 2033 11:47:03 -0300

Fonte: o autor

Figura 9 – AC – Certificado de Instalado



Fonte: o autor

7.4 Backup do Firewall

Para garantirmos uma confiabilidade maior, nós utilizamos uma função no pfSense que nos permite efetuar um backup direto na nuvem da Netgate, criadora e mantenedora do pfSense. Configuramos um auto backup para o firewall pfSense como podemos verificar na figura 10, este modelo de backup nativo do pfSense permite que a cada alteração feita no firewall um backup é feito na nuvem da Netgate.

Figura 10 - Configurando o Auto Backup do Firewall

The screenshot shows the 'Auto Configuration Backup / Settings' page in the pfSense web interface. The 'Settings' tab is selected. The main section is titled 'Auto Config Backup'. It includes fields for enabling automatic backups, setting the backup frequency (either 'Automatically backup on every configuration change' or 'Automatically backup on a regular schedule'), entering an encryption password (with two input fields for the password and a 'Confirm' button), providing a hint/identifier (e.g., 'FW:cecc.edu-projeto-puc'), and specifying how many manual backups to keep (a maximum of 50). There is also an option to list backups in descending order by date.

Auto Config Backup		
Enable ACB	<input checked="" type="checkbox"/> Enable automatic configuration backups Auto Configuration Backup automatically encrypts configuration backup content using the Encryption Password below and then securely uploads the encrypted backup over HTTPS to Netgate servers.	
Backup Frequency	<input checked="" type="radio"/> Automatically backup on every configuration change <input type="radio"/> Automatically backup on a regular schedule	
Encryption Password The best practice for security is to use a long and complex password. Confirm
Hint/Identifier	FW:cecc.edu-projeto-puc You may optionally provide an identifier which will be stored in plain text along with each encrypted backup. This may allow the Netgate support team to locate your key should you lose it.	
Manual backups to keep	It may be useful to specify how many manual backups are retained on the server so that automatic backups do not overwrite them. A maximum of 50 retained manual backups (of the 100 total backups) is permitted.	
Descending Order by Date	<input type="checkbox"/> List backups in descending order List backups in descending order (newest first) when viewing the restore section.	

Fonte: o autor

Na figura 11, podemos ver todos os backups que foram gerados por cada alteração feita no firewall, podemos então, restaurar, fazer o download ou deletar o checkpoint disponíveis.

Figura 11 - Comportamento dos Backups

Date	Configuration Change	Actions
Fri, 29 Sep 2023 03:14:03 -0300	psilva@10.1.20.225 (LDAP/AUTH-AD): Removed cron job for /usr/bin/nice -n20 /usr/local/bin/php /usr/local/sbin/execacb.php	
Fri, 29 Sep 2023 03:15:01 -0300	psilva@10.1.20.225 (LDAP/AUTH-AD): Firewall: Rules - saved/edited a firewall rule.	
Fri, 29 Sep 2023 03:19:00 -0300	admin@10.1.20.225 (Local Database Fallback): AutoConfigBackup settings updated	
Fri, 29 Sep 2023 03:19:01 -0300	admin@10.1.20.225 (Local Database Fallback): Removed cron job for /usr/bin/nice -n20 /usr/local/bin/php /usr/local/sbin/execacb.php	
Fri, 29 Sep 2023 03:22:01 -0300	admin@192.168.10.28 (Local Database Fallback): Firewall: Rules - disabled a firewall rule.	

Fonte: o autor

Na figura x, podemos ver a **Device Key**. Esta chave é extremamente importante e não podemos de forma alguma ignorá-la, é esta Key que nos possibilita recuperar o backup em caso de um desastre. Com esta chave, caso seja necessário podemos subir um novo servidor e restaurar o backup através da lista que de backups disponíveis. Contudo, é interessante manter uma rotina de backup manual para salvar em um outro ambiente.

Figura 12 - Device Key - pfSense

Fonte: o autor

7.5 FailOver

Failover em computação é uma técnica de tolerância a falhas. Quando um sistema, servidor ou outro componente de hardware ou software fica indisponível, um componente secundário assume operações sem que haja interrupção nos serviços. Failover é a capacidade de alternar perfeita e automaticamente para um sistema de backup confiável.

Criamos no pfSense a configuração de failover, agrupando as interfaces que recebem o link de internet. Após isso, é criado um gateway apontando para esse grupo.

Figura 13 - Configuração do Failover no pfSense

Fonte: o autor

Configuramos como gateway padrão a opção Failover que foi criado no passo anterior, assim, onde definimos que o link1 tem prioridade e o link2 fica de stand-by. O Critério para alterar o link preferencial é a perda de pacotes ou a alta latência.

Figura 14 - Configuração do Failover no pfSense

Fonte: o autor

7.5 Loadbalance

Balanceamento de carga ou loadbalance é uma técnica utilizada para manter a estabilidade de um servidor quando o tráfego ou o volume de dados é muito grande. O ponto principal é otimizar o tráfego de informações e garantir o funcionamento de um sistema para o usuário, estabilizando a navegação.

Na figura 15, é mostrado a configuração e os parâmetros usados para configurar o grupo de interfaces que nomeamos de Loadbalance, após essa configuração é criado um Gateway de saída para internet, posteriormente, será usado nas regras de firewall.

Figura 15 – Configuração do balanceamento de Links

The screenshot shows the 'Edit Gateway Group Entry' page with the following details:

- Group Name:** LOADBALANCE
- Gateway Priority:**
 - WAN_LINK1_DHCP Tier 1 Interface Address GW_WAN_LINK1
 - GW_WAN_LINK2 Tier 1 Interface Address GW_WAN_LINK2
- Link Priority:** The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.
- Virtual IP:** The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.
- Trigger Level:** Packet Loss or High Latency
- Description:** Loadbalance

Fonte: o autor

Para que o loadbalance funcione de forma efetiva, nós aplicamos diretamente das regras de firewall o gateway de saída que é criado na etapa anterior, apontando assim, para o grupo de interfaces que o balance está configurado, podemos validar na figura 16.

Figura 16 – Aplicação do balanceamento de Links

The screenshot shows the 'Rules (Drag to Change Order)' table with the following rules listed under 'REGAS BÁSICAS':

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/3.38 MiB	IPv4 TCP	VLAN20_SERVIDORES net	*	This Firewall	4443	*	none		Liberar WebGUI - FW	
0/0 B	IPv4 TCP/UDP	VLAN20_SERVIDORES net	*	*	53 (DNS)	LOADBALANCE	none		Libera DNS	
0/91.21 MiB	IPv4 TCP	VLAN20_SERVIDORES net	*	*	80 (HTTP)	LOADBALANCE	none		Libera HTTP	
0/1.32 GiB	IPv4 TCP	VLAN20_SERVIDORES net	*	*	443 (HTTPS)	LOADBALANCE	none		Libera HTTPS	
0/0 B	IPv4 ICMP any	VLAN20_SERVIDORES net	*	VLAN10_ESTACOES net	*	*	none			

Fonte: o autor

7.6 Teste primário de intrusão

Para testar a confiabilidade da rede configurada até com os recursos nativos do firewall, nós usamos um script disponibilizado no GitHub da CITRAIT que testa as conexões estressando o firewall. Na página do GitHub <https://github.com/citrait>, fizemos o teste com o script chamado “**check_data_exfiltration**”. Utilizamos algumas listas oficiais de endereços ip

que são reportados por órgãos que cuidam deste cenário de invasão, criamos um alias e logo após criamos uma regra proibindo o acesso a esses endereços.

Figura 17 – Teste de Intrusão Inicial

```
Successfully blocked connection 192.42.116.25:80
Successfully blocked connection 192.42.116.25:23
Successfully blocked connection 185.220.100.255:22
Successfully blocked connection 185.220.100.255:9000
Successfully blocked connection 185.220.100.255:9001
Successfully blocked connection 185.220.100.255:9100
Successfully blocked connection 185.220.100.255:9101
Successfully blocked connection 199.249.230.185:22
Successfully blocked connection 199.249.230.185:80
Successfully blocked connection 199.249.230.185:111
Successfully blocked connection 199.249.230.185:443
Successfully blocked connection 185.220.100.252:22
Successfully blocked connection 185.220.100.252:9000
Successfully blocked connection 185.220.100.252:9001
Successfully blocked connection 185.220.100.252:9100
Successfully blocked connection 185.220.100.252:9101
Não é possível chamar um método em uma expressão de valor nulo.
No C:\Users\psilva\Desktop\check_data_exfiltration-main\Test_Exfiltration.ps1:34 caractere:2
+     ForEach($target_port in $ports.Split(","))
+
+     + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
+     + FullyQualifiedErrorId : InvokeMethodOnNull

-----
Summary
-----
STATUS: Failed!
Sorry, you need to investigate why not all connections where blocked. Try Again!
Blocked connections: 872
Successfull connections: 29
PS C:\Users\psilva\Desktop\check_data_exfiltration-main>
```

Fonte: o Autor

Percebemos na imagem anterior, que a maior parte das tentativas de acesso foram bloqueadas. Infelizmente em qualquer firewall não seria correto dizer que a rede passa a ser 100% confiável, por tanto o que devemos fazer em um firewall é dificultar ao máximo qualquer tentativa de ataque.

Figura 18 – Log pfSense durante o teste de intrusão

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Oct 10 10:23:35	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49959	193.218.118.182:9001	TCP:S
✗	Oct 10 10:23:35	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49975	185.220.100.245:9100	TCP:S
✗	Oct 10 10:23:35	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49974	185.220.100.245:9001	TCP:S
✗	Oct 10 10:23:35	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49972	185.220.100.245:22	TCP:S
✗	Oct 10 10:23:35	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49968	199.249.230.174:22	TCP:S
✗	Oct 10 10:23:34	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49958	193.218.118.182:443	TCP:S
✗	Oct 10 10:23:34	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49974	185.220.100.245:9001	TCP:S
✗	Oct 10 10:23:34	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49973	185.220.100.245:9000	TCP:S
✗	Oct 10 10:23:34	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49971	199.249.230.174:443	TCP:S
✗	Oct 10 10:23:34	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49967	185.220.101.59:80	TCP:S
✗	Oct 10 10:23:33	VLAN10_ESTACOES	BLACKLIST (1696896860)	10.1.10.1:49957	193.218.118.182:22	TCP:S

Fonte: o Autor

7.7 IDS/IPS Snort

O Snort é um sistema de prevenção a intrusões na rede (intrusion prevention system – IPS) open source, mantido e desenvolvido pela Cisco há cerca de cinco anos. A ferramenta se destaca por sua capacidade de analisar tráfegos em tempo real e registrar pacotes de protocolo TCP (Transmission Control Protocol).

Em função dessa versatilidade, o Snort consegue desempenhar o papel de três tipos de aplicações cruciais para monitorar um servidor. Logo, ele pode ser usado como sniffer de pacotes (de modo similar ao tcpdump), registrador de pacotes e / ou um sistema avançado de prevenção à intrusão.

7.7.1 O que é um IDS?

IDS é a sigla para Intrusion Detection System (sistema de detecção de intrusão). Podemos dizer que um IDS representa, em si, boa parte do que expliquei até aqui sobre monitoramento, mapeamento, identificação e notificação de atividades suspeitas.

Numa comparação mais didática, um IDS exerce funções semelhantes a um sistema de vigilância, porém abstrato. Isso porque ambos monitoram, contam com sensores e alertas, e são controlados por uma equipe de pessoas que tomam as decisões cabíveis a cada evento.

É só isso? Definitivamente, não. Há diferentes tipos de sistemas de detecção de intrusão, bem como diferentes modos de uso e funcionamento entre eles. A seguir, confira uma abordagem enxuta sobre essa distinção.

7.7.2 Métodos de detecção

As ameaças são detectadas pelo Snort por meio de assinaturas e esta é uma das funcionalidades-chave do programa. Ainda que tal abordagem tenha os seus pontos fracos (como todas as outras), ela funciona muito bem no Snort de modo similar a um antivírus.

Figura 19 – Log de tráfego IDS na interface vLan20

Alert Log View Settings																	
Interface to Inspect		VLAN10_ESTACOES	<input type="checkbox"/> Auto-refresh view		250	<input checked="" type="checkbox"/> Save											
Choose interface...																	
Alert Log Actions																	
Alert Log View Filter																	
186 Entries in Active Log																	
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description							
2023-10-11 22:08:22	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	53049	120:3 ⊕ ✘	(http_Inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE							
2023-10-11 22:08:22	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	53049	120:18 ⊕ ✘	(http_Inspect) PROTOCOL-OTHER HTTP server response before client request							
2023-10-11 22:08:22	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	53049	120:18 ⊕ ✘	(http_Inspect) PROTOCOL-OTHER HTTP server response before client request							
2023-10-11 22:07:57	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	53046	120:3 ⊕ ✘	(http_Inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE							
2023-10-11 22:07:57	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	53046	120:18 ⊕ ✘	(http_Inspect) PROTOCOL-OTHER HTTP server response before client request							
2023-10-11 22:07:57	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	53046	120:18 ⊕ ✘	(http_Inspect) PROTOCOL-OTHER HTTP server response before client request							
2023-10-11 22:04:43	⚠️	2	UDP	Potentially Bad Traffic	10.1.10.1	62792	10.1.20.225	53	1:2027863 ⊕ ✘	ET INFO Observed DNS Query to .biz TLD							
2023-10-11 22:04:43	⚠️	2	UDP	Potentially Bad Traffic	10.1.10.1	61100	10.1.20.225	53	1:2027863 ⊕ ✘	ET INFO Observed DNS Query to .biz TLD							
2023-10-11 22:04:42	⚠️	2	UDP	Potentially Bad Traffic	10.1.10.1	62877	10.1.20.225	53	1:2027863 ⊕ ✘	ET INFO Observed DNS Query to .biz TLD							
2023-10-11 22:04:42	⚠️	2	UDP	Potentially Bad Traffic	10.1.10.1	51390	10.1.20.225	53	1:2027863 ⊕ ✘	ET INFO Observed DNS Query to .biz TLD							
2023-10-11 22:02:15	⚠️	3	TCP	Unknown Traffic	10.1.20.225	88	10.1.10.1	52711	120:3 ⊕ ✘	(http_Inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE							

Fonte: O Autor

Na imagem acima o snort detectou na interface "LAN" várias ocorrências de algo suspeito ou potencialmente malicioso relacionado a essa comunicação. O IDS gera alertas com base em regras de detecção definidas.

Conforme demonstrado na imagem acima, no registro de alerta de tráfego capturado pelo IDS (Sistema de Detecção de Intrusões), podemos analisar que ele identificou múltiplos alertas no endereço IP 10.1.20.225, na porta 88, com o IP de destino 10.1.10.1, na porta 51659."

Figura 20 – Log de tráfego IDS na interface Wan

The screenshot shows the pfSense Snort Alerts log interface. At the top, there's a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below that is a breadcrumb trail: Services / Snort / Alerts. The main area has tabs for Snort Interfaces, Global Settings, Updates, Alerts (which is selected), Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. Under the Alerts tab, there's a section for Alert Log View Settings with fields for Interface to Inspect (set to WAN_LINK1 (hn0)), Auto-refresh view (unchecked), and Alert lines to display (set to 250). There are also Download and Clear buttons. Below this is an Alert Log Actions section with similar buttons. The main content area is titled 'Alert Log View Filter' and shows '2 Entries in Active Log'. A table lists the following data:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-10-10 18:19:17	⚠️	1	TCP	Potential Corporate Privacy Violation	200.25.87.0	80	192.168.10.77	58435	1:2018959	ET POLICY PE EXE or DLL Windows file download HTTP
2023-10-10 15:27:10	⚠️	3	TCP	Unknown Traffic	8.241.243.254	80	192.168.10.77	35900	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

Fonte: O Autor

É possível identificar na imagem acima que houve alerta de tráfego na interface WAN, na rede externa, com o IP de origem 200.25.87.0, na porta 80, com destino ao IP 192.168.10.77, na porta 58435. Além disso, registramos tentativas de comunicação na interface WAN com o IP de origem 8.241.243.254, na porta 80, direcionadas ao IP de destino 192.168.10.77, na porta 35900.

Pode-se observar um bloqueio na rede causado pelo recurso de IPS do Snort. Ele identificou um ataque suspeito e procedeu ao bloqueio do IP de origem 8.241.243.254, como demonstrado na figura 21, logo em seguida.

Figura 21 – Bloqueio de endereços ip

#	IP	Alert Descriptions and Event Times	Remove
1	8.241.243.254	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE – 2023-10-10 15:27:10	X

Fonte: O Autor

7.8 Controle de navegação Squid Web Proxy

O que é o squid?

O Squid é um servidor proxy que suporta requisições de conexões http, https e outros. Ele reduz a utilização da conexão e melhora os tempos de resposta fazendo cache das requisições mais frequentes de páginas web numa rede de computadores. Ele também é usado para controlar o conteúdo acessado dentro na rede da empresa. Websites de conteúdo adulto, rede sociais e plataformas streaming, são exemplos simples de sites que tiram toda a produtividade do colaborador, além de coloca em risco a rede corporativa acessando sites indevidos. O Squid veio para sanar este problema.

Para tanto, dentro da rede da CECC, optamos por fazer a aplicação desta ferramenta para fazer o controle dos acessos web. Na figura 22, podemos ver algumas das várias categorias de sites que podemos fazer o bloqueio.

Figura 22 – Filtros por categorias do SquidGuard

The screenshot shows the 'Common ACL' tab selected in the top navigation bar. Below it, the 'Target Rules' section contains the rule: !Blacklist !blk_BL_hobby_pets !blk_BL_porn !blk_BL_sex_lingerie !blk_BL. The 'Target Rules List' section shows a single entry with a '+' button. The 'Target Categories' section lists various categories with their access levels: [Blacklist] deny, [blk_BL_adv] access, [blk_BL_aggressive] access, [blk_BL_alcohol] access, [blk_BL_anonvpn] access, [blk_BL_automobile_bikes] access, [blk_BL_automobile_boats] access, [blk_BL_automobile_cars] access, [blk_BL_automobile_planes] access, and [blk_BL_chat] access.

Fonte: O Autor

Na figura 23, podemos ver o log de acessos do todo conteúdo que está sendo bloqueado. Por padrão sites com o protocolo https, não apresentam um banner na tela de bloqueio na tela devido a inspeção ssl, eles simplesmente derrubam a conexão, mas isso é resolvido com algumas modificações. Nesta situação, a configuração vale para todos os usuários. O que é bom, mas não é o ideal.

Figura 23 – Log do SquidGuard

The screenshot shows the 'Log' tab selected in the top navigation bar. The 'Blacklist Update' section displays a table of blocked entries. The table has columns for date, source IP, destination URL, and action. The entries show multiple requests from 10.1.10.1 to www.instagram.com:443, all labeled as 'Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT'.

Date	Source IP	Destination URL	Action
16.10.2023 16:11:01	10.1.10.1/10.1.10.1	www.instagram.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
16.10.2023 16:11:01	10.1.10.1/10.1.10.1	www.instagram.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
16.10.2023 16:11:01	10.1.10.1/10.1.10.1	www.instagram.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
16.10.2023 16:11:01	10.1.10.1/10.1.10.1	www.instagram.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
16.10.2023 16:01:01	10.1.10.1/10.1.10.1	www.instagram.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
16.10.2023 16:01:01	10.1.10.1/10.1.10.1	www.instagram.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT

Fonte: O Autor

Já na figura 24 e 25, após os ajustes necessários, podemos ver a tela de bloqueio que será apresentada. Ela mostrará para o usuário algumas informações como, usuário, grupo e categoria. Isso porque fizemos os ajustes para trabalhar com grupo ao invés de usuários.

Fizemos a criação de três grupos com permissões de acessos web diferentes e fizemos a integração com o servidor Active Directory para que aconteça a autenticação transparente, aproveitando o benefício do Single Sign-On.

- INTERNET_BASICO – Onde o usuário terá acesso com menor permissão.
- INTERNET_VIP – Onde o usuário terá acesso com maior permissão, mas ainda com restrições.
- INTERNET_TI – Acesso total

Figura 24 – Grupos de controle de acesso web - SquidGuard

The screenshot shows a web-based configuration interface for SquidGuard. The top navigation bar includes links for Package, Proxy filter SquidGuard, Groups Access Control List (ACL), Groups ACL, General settings, Common ACL, Target categories, Times, Rewrites, Blacklist, Log, and XMLRPC Sync. The Groups ACL tab is currently selected. Below the tabs is a table with columns: Disabled, Name, Time, and Description. The table contains three entries:

Disabled	Name	Time	Description
INTERNET_BASICA	Grupo de liberação de internet para usuários com menos permissão de acesso web.		
INTERNET_VIP	Grupo de liberação de internet para usuários com mais permissão de acesso web.		
INTERNET_TI	Grupo de liberação de internet para usuários de TI.		

A green 'Add' button is located at the bottom right of the table area.

Fonte: O Autor

Figura 25 – Grupos para controle de acesso Web - ADDS

The screenshot shows the Active Directory Users and Computers (ADUC) management console. On the left is a navigation tree under the 'CECC.EDU' domain, with several organizational units (OU) listed: 01.CECC, 02.SERVidores, 03.ESTAÇÕES, 04.SECURITYGROUP, and 05.INTERNET_CONTROL. The 'SECURITYGROUP' OU is currently selected. On the right is a table listing three new security groups:

Name	Type	Description
GRP_INTERNET_BASIC	Security Group...	
GRP_INTERNET_TI	Security Group...	
GRP_INTERNET_VIP	Security Group...	

Fonte: O Autor

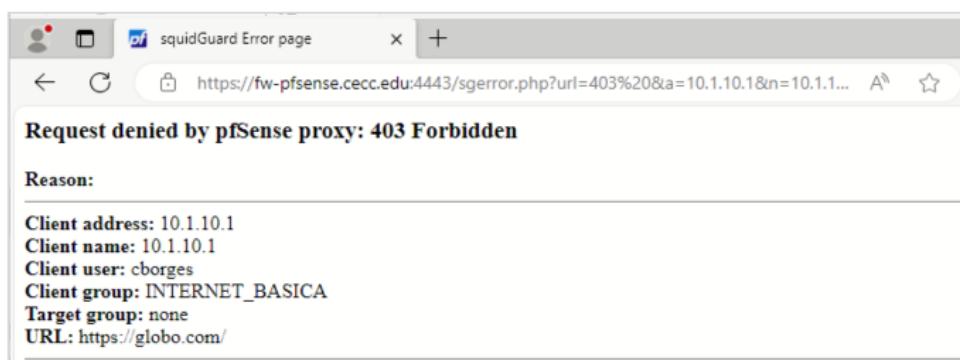
Com essas configurações, agora podemos ter mais controle sobre o acesso web dentro da CECC controlando o acesso a nível de grupo de usuários, o que nos garante uma melhor gestão do cenário. Na figura 26 e 27 já podemos ver a mensagem de bloqueio agora também para o protocolo HTTPS, o que nos permitiu fazer isso, foi a configuração da CA no nosso Firewall, item visto no tópico 7.3; e que posteriormente foi instalada por políticas de grupo em todas as estações. Perceba que agora ele nos traz as informações mencionadas anteriormente.

Figura 26 – Tela de Bloqueio com Inspeção SSL - 1



Fonte: O Autor

Figura 27 – Tela de Bloqueio com Inspeção SSL - 2



Fonte: O Autor

7.8.1 - Logs de Acesso

Nas figuras 28 e 29, podemos ver o log das ações anteriores, os bloqueios e também os sites que são acessados, estes logs servem para refinar as permissões de acesso.

Figura 28 – Log do Squid

Squid Access Table					
Squid - Access Logs				User	Destination
Date	IP	Status	Address	-	-
18.10.2023 09:17:46	10.1.10.1	TCP_DENIED/407	www.bing.com:443	-	-
18.10.2023 09:17:41	10.1.10.1	TCP_TUNNEL/200	fw-pfsense.cecc.edu:4443	-	192.168.1.254
18.10.2023 09:17:41	10.1.10.1	TCP_TUNNEL/200	fw-pfsense.cecc.edu:4443	-	192.168.1.254
18.10.2023 09:17:37	10.1.10.1	TCP_REDIRECT/302	https://ntp.msn.com/edge/ntp/service-worker.js?	cborges	-
18.10.2023 09:17:37	10.1.10.1	NONE_NONE/200	ntp.msn.com:443	cborges	204.79.197.203
18.10.2023 09:17:37	10.1.10.1	TCP_DENIED/407	ntp.msn.com:443	-	-
18.10.2023 09:17:36	10.1.10.1	TCP_REDIRECT/302	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3	cborges	-
18.10.2023 09:17:36	10.1.10.1	NONE_NONE/200	nav-edge.smartscreen.microsoft.com:443	cborges	20.201.67.116
18.10.2023 09:17:36	10.1.10.1	TCP_DENIED/407	nav-edge.smartscreen.microsoft.com:443	-	-
18.10.2023 09:17:36	10.1.10.1	TCP_REDIRECT/302	https://ntp.msn.com/edge/ntp?	cborges	-
18.10.2023 09:17:36	10.1.10.1	NONE_NONE/200	ntp.msn.com:443	cborges	204.79.197.203
18.10.2023 09:17:36	10.1.10.1	TCP_DENIED/407	ntp.msn.com:443	-	-
18.10.2023 09:17:32	10.1.10.1	TCP_REDIRECT/302	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3	cborges	-
18.10.2023 09:17:32	10.1.10.1	NONE_NONE/200	nav-edge.smartscreen.microsoft.com:443	cborges	20.201.67.116
18.10.2023 09:17:32	10.1.10.1	TCP_DENIED/407	nav-edge.smartscreen.microsoft.com:443	-	-
18.10.2023 09:17:32	10.1.10.1	TCP_REDIRECT/302	https://uo1.com.br/	cborges	-
18.10.2023 09:17:32	10.1.10.1	NONE_NONE/200	uo1.com.br:443	cborges	200.147.3.157
18.10.2023 09:17:32	10.1.10.1	NONE_NONE/200	fw-pfsense.cecc.edu:4443	-	-
18.10.2023 09:17:32	10.1.10.1	TCP_REDIRECT/302	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3	cborges	-

Fonte: O Autor

Figura 29 – Log do SquidGuard

SquidGuard Table		SquidGuard Logs		
Date-Time	ACL	Address	Host	User
18.10.2023 09:17:37	Request(INTERNET_BASICA/none/-)	https://ntp.msn.com/edge/ntp/service-worker.js?riverAgeMinutes=1440&ena bleNetworkFirst=true&navAgeMinutes=2880&enableNavPreload=true&enableEmptySectionRoute=true&enableFallbackVerticalsFeed=true&networkTimeoutSeconds=5	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:17:36	Request(INTERNET_BASICA/none/-)	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:17:36	Request(INTERNET_BASICA/none/-)	https://ntp.msn.com/edge/ntp/locale=pt-BR&ttitle=Nova%20guia&re=1&sp=dsp=1&sp=Bing&prerender=1	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:17:32	Request(INTERNET_BASICA/none/-)	https://uol.com.br/	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:17:32	Request(INTERNET_BASICA/none/-)	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:17:32	Request(INTERNET_BASICA/none/-)	https://config.edge.skyape.com/config/v1/Edge/118.0.2088.46?clientid=806969 1009918620840&agents=EdgeRuntimeConfig&osname=win&client=edge&a mp;channel=stable&scfull=0&scfree=0&scver=0&osarch=x86_64&osver =10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=188&np.rmgd=1&installdate= 1697583038&edu=0&bphint=0&soobedate=1697583029&fg=1 https://edge.microsoft.com/extensionrevocation/v1/threatListUpdates:fetch?	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:14:48	Request(INTERNET_BASICA/none/-)	jeq=ChckKBm1zZWRnZRINMTE4LjAuMjA40C40NhoMCAEQCCIEAgElgIIAQ==&ct=appl ication/x-protobuf&key=d14dd49db345fa8000e32adc81b362&e=N https://login.microsoftonline.com/common/UserRealm/?user=CECC.EDU&api-v ersion=1.&checkForMicrosoftAccount=false	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:14:39	Request(INTERNET_BASICA/none/-)	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3	10.1.10.1/10.1.10.1cborges	
18.10.2023 09:14:08	Request(INTERNET_BASICA/none/-)	https://arc.msn.com/v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34 988683ac7&pid=338388&adm=2&w=1&h=1&px=1&fmt=json&cctp=app& v=1.0.0.10.1cborges	10.1.10.1/10.1.10.1cborges	

Fonte: O Autor

7.8.1 - Logs de Acesso

Finalizando as configurações mais críticas do firewall podemos contar ainda com relatórios de acesso web. Estes além de necessários, servem para auditorias e otimização contínua dos processos de educação tecnológica dentro da empresa. Embora de interface simples, no exemplo da figura 30 podemos verificar como a ferramenta nos possibilita fazer a auditoria, primeiramente escolhendo o ano e o dia.

Figura 30 – Relatório do Squid – Parte 1

Relatório de Acesso							Home
Período: 2023							
Calendar							
2023							
Data	Grupo	Usuários	Acima do limite	Bytes	Média	Hit %	Top Sites
18 Out 2023	grp	4	0	11.0 M	2.7 M	0.00%	ANO
Total/Média:			0	11.0 M	2.7 M	0.00%	

Fonte: O Autor

Na figura 31 será mostrado todos os hosts ou usuários que fizeram acesso à internet e classificará por percentual de uso, o que já nos dá uma noção de algum usuário que possa estar estressando a rede.

Figura 31 – Relatório do Squid – Parte 2

Relatório de Acesso							Home
Data: 18 Out 2023 (Atualizar :: 10:05 :: 18 Out 2023)							
Top Sites Relatório							
Arquivos grandes Relatório							
#	Hora	Usuário	Real Name	Conexões	Bytes	%	Grupo
1	18/10/2023 10:05:00	psilva	?	512	9.0 M	81.8% ?	
2	18/10/2023 10:05:00	chorges	?	366	1.5 M	13.7% ?	
3	18/10/2023 10:05:00	10.1.10.1	?	188	358 082	3.1% ?	
4	18/10/2023 10:05:00	pc001S	?	69	148 458	1.2% ?	

Fonte: O Autor

Na figura 32 podemos contemplar todos os sites que o usuário selecionado utilizou no dia selecionado, neste caso, **psilva**. Estas informações são de extrema importância, pois, através delas podemos ter uma noção da aderência dos treinamentos de segurança da informação além de outras opções já usa.

Figura 32 – Relatório do Squid – Parte 3

Relatório de Acesso							Home
Usuário: psilva (?)							
Grupo: ?							
Data: 18 Out 2023							
=+ =+ =+							
User download "Big Files"							
Total	#	Sites acessados	Conexões	Bytes	Soma	%	9.0 M
	1	msedge.b.flu.dl.delivery.mp.microsoft.com	1	4.8 M	4.8 M	53.6%	
	2	tse1.mm.bing.net	6	1.9 M	6.8 M	21.6%	
	3	th.bing.com	52	632 450	7.4 M	6.7%	
	4	ntp.msn.com	4	453 863	7.8 M	4.8%	
	5	www.bing.com	69	304 170	8.1 M	3.2%	
	6	securepubads.g.doubleclick.net	2	166 221	8.3 M	1.7%	
	7	www.uol.com.br	4	143 013	8.4 M	1.5%	
	8	www.googletagmanager.com	1	88 579	8.5 M	0.9%	
	9	conteudo.imgur.com.br	7	78 917	8.6 M	0.8%	
	10	assets.msn.com	14	78 824	8.6 M	0.8%	
	11	script.hotjar.com	1	57 279	8.7 M	0.6%	
	12	fundingchoicesmessages.google.com	1	54 530	8.7 M	0.5%	
	13	thumb.mais.uol.com.br	1	41 663	8.8 M	0.4%	
	14	http://srv-f601/	5	32 875	8.8 M	0.3%	
	15	arc.msn.com	2	28 428	8.8 M	0.3%	
	16	srib.msn.com	10	26 980	8.9 M	0.2%	
	17	edge.microsoft.com	25	21 700	8.9 M	0.2%	

Fonte: O Autor

8 SERVIDORES DE AUTENTICAÇÃO E FILE SERVER

Nesta etapa do projeto, implementamos um serviço para controle de acesso ao conteúdo da empresa. Este servidor se chama Active Directory Domain Services ou para os mais íntimos ADDS. Qualquer empresa que se preze tem um servidor de autenticação para controlar o que pode ou não ser acessado dentro da estrutura da empresa. Como a empresa que faz parte deste projeto não tinha nenhum tipo de serviço para fazer isso, nós implementamos o ADDS. Perceba na figura 6, que é apresentada logo abaixo, que a estrutura foi organizada com duas unidades organizacionais (**OU**) **01. CCEC** e **02. SERVIDORES**. Senho a primeira para os usuários, e a segunda para os servidores, ambos visando uma futura aplicação de política de segurança (GPO).

Figura 333 – Estrutura de domínio da empresa

Name	Type	Description
COORDENACAO	Organizational...	
DIRETORIA	Organizational...	
FINANCIERO	Organizational...	
PROFESSORES	Organizational...	
RH	Organizational...	
SECRETARIA	Organizational...	
TI	Organizational...	
CECC-TOTAL	Security Group...	
CECC-COMUM	Security Group...	

Fonte: o Autor

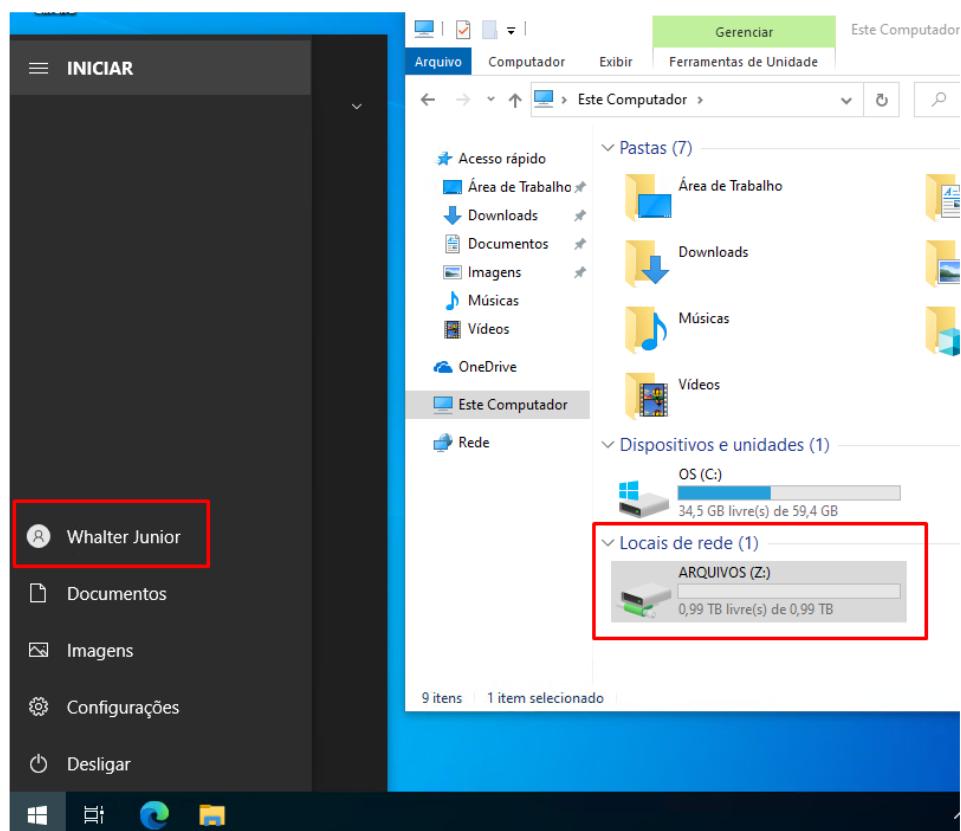
01.CCEC – Dentro desta unidade organizacional nós criamos os demais setores da empresa para facilitar uma gestão centralizada de usuários. Tornando fácil alocar o usuário no devido setor, o que já implica diretamente nas permissões de acesso. Pois, no File Server, as credenciais usadas são as configuradas no ADDS.

02.SERVIDORES – Nesta OU, nós alocamos os servidores para melhor organização e possíveis políticas.

8.1 Exemplo de acesso para um usuário do setor Financeiro

Neste exemplo apresentando na figura 34, autenticamos com o usuário do colaborador Whalter Junior, já mostramos a unidade de rede mapeada para seu usuário com as devidas permissões de acesso, o que podemos ver na figura 35.

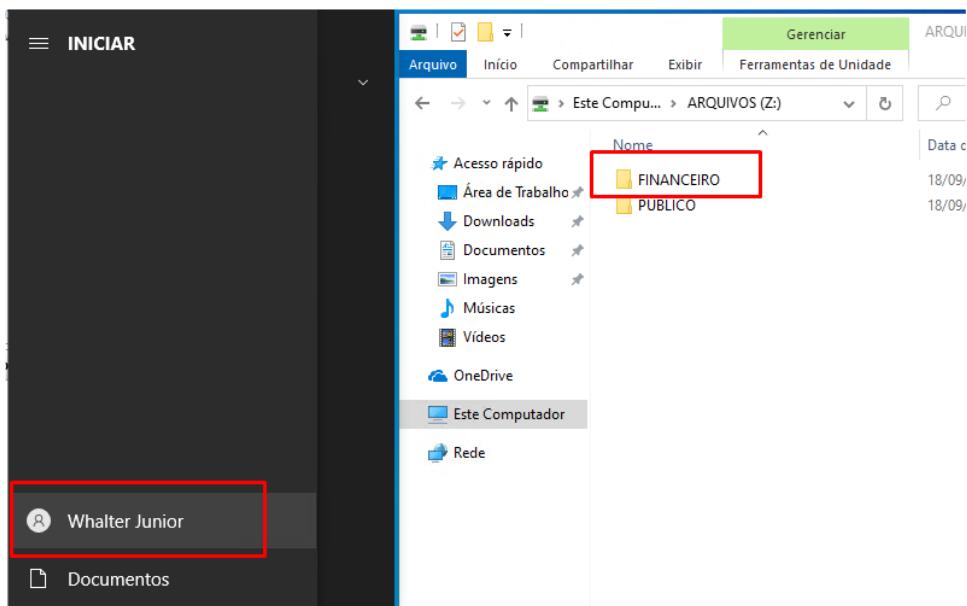
Figura 34 – Estrutura de domínio da empresa – Permissões de rede - Parte 1



Fonte: o Autor

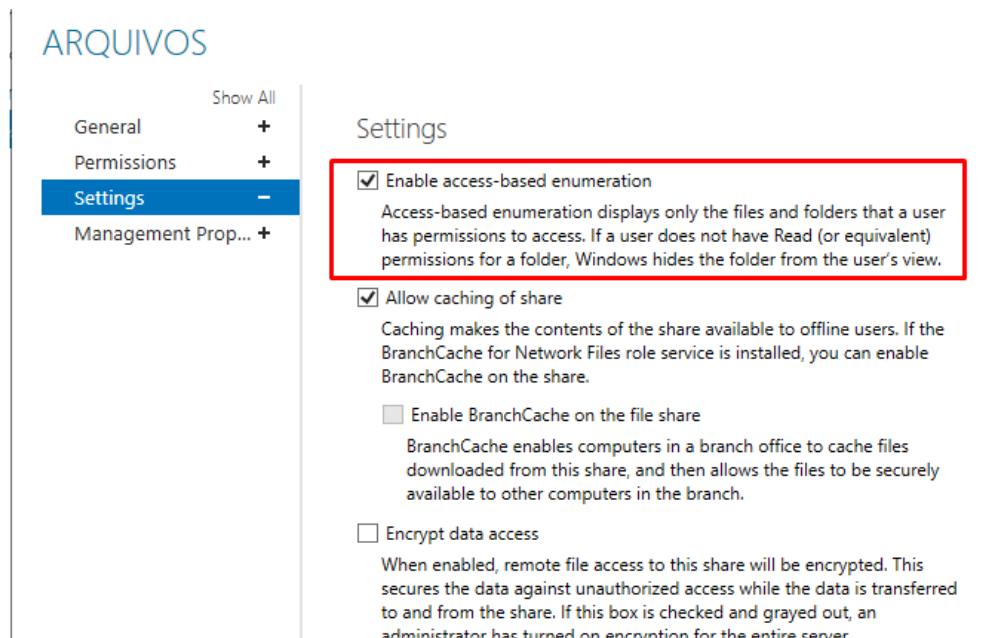
Aqui, podemos confirmar que ele tem acesso apenas aos diretórios que lhe foram atribuídos. Vemos ainda que, os outros diretórios sequer irão ser listados para ele, pois nós habilitamos a enumeração baseada em acesso. Essa função do sistema nos permite configurar a opção em que o usuário só terá visibilidade do que ele realmente tem permissão.

Figura 35 – Estrutura de domínio da empresa – Permissões de rede - Parte 2



Fonte: o Autor

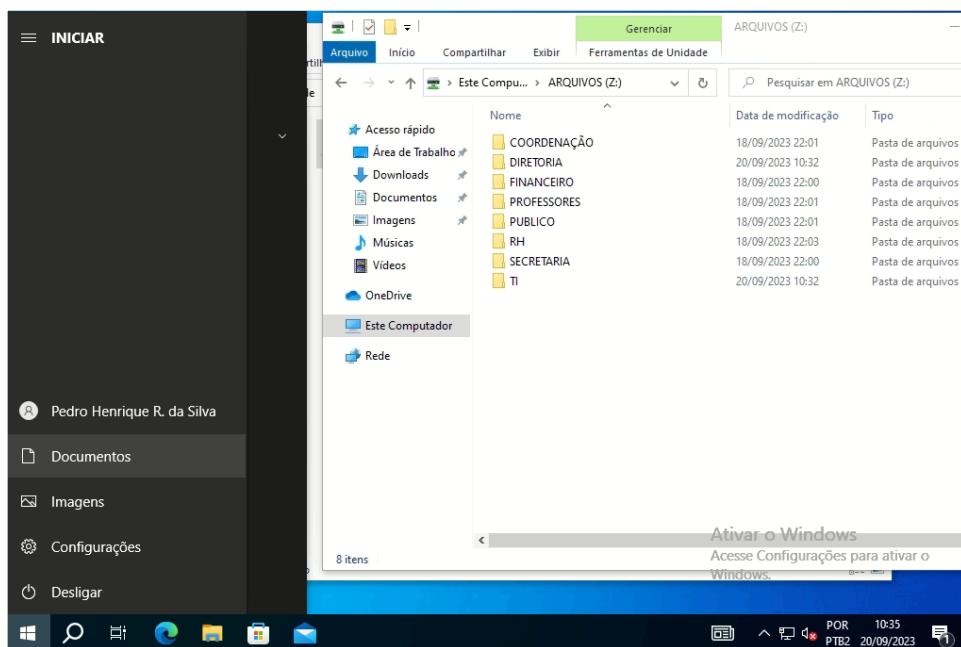
Figura 36 – Estrutura de domínio da empresa – Enumeração baseada em acesso



Fonte: o Autor

Vamos verificar o usuário de um outro setor, dessa vez um que tem acesso a todos os diretórios. Utilizamos o usuário do colaborador Pedro para poder exemplificar o nível de permissão. Este, além de pertencer ao grupo **TI**, também pertence ao grupo **CECC-TOTAL**, que tem acesso a todos os diretórios compartilhados na rede. ver figura 36 para validação dos grupos.

Figura 37 – Estrutura de diretórios – Permissão de acesso total



Fonte: o Autor

Uma vez definido as regras de acesso, o que, geralmente fazemos baseado em grupos, basta adicionar o usuário ao grupo correspondente ao setor que ele irá pertencer que ele automaticamente herda as permissões conforme configurado no servidor de arquivos.

8.3 Servidor de Autenticação – Política de grupo

Não menos importante, neste servidor nós implementamos algumas políticas de grupo, a fim de aumentar a segurança e definir alguns padrões corporativos nas estações de trabalho. É nele que também fazemos o gerenciamento de usuários, grupos e objetos do Active Directory.

Aqui apresentamos a estrutura de domínio que já citamos algumas coisas a respeito em assuntos anteriores. Abordaremos mais um pouco dessa solução.

Serviços utilizados no servidor de domínio:

- Políticas de grupo
- Administração de grupos e usuários
- Servidor DNS

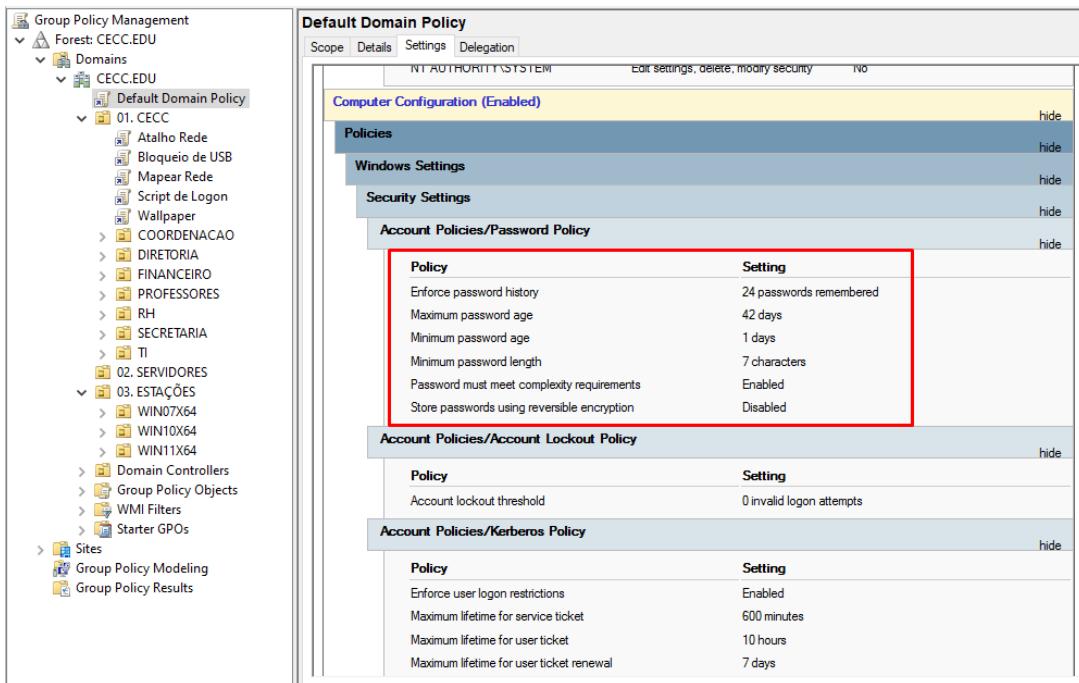
Explanando um pouco o cenário, vemos abaixo a estrutura desenhada para configurações das políticas de grupos iniciais que consideramos importantes, e a possibilidade de políticas futuras, como um possível serviço de controle de atualizações dedicados para servidores e versões de diferentes sistemas Windows. Neste cenário, aplicamos as GPOs dentro das OUs desejadas, uma vez que é uma estrutura hierárquica. Na figura a seguir, podemos ver algumas GPOs. Estas, se aplicam apenas para as OUs que estão dentro da OU “**01. CECC**”, diferente a GPO padrão, “**Default Domain Policy**”, que se aplica a todo o domínio. Essa modelo permite aplicar políticas específicas para cada situação, onde podemos por exemplo criar uma política para adicionar impressora específica apenas para o grupo RH. Aproveitando, outro ponto importante sobre a política padrão, é que ele já vem com uma parametrização que obriga os usuários a alterarem a senha a cada 42 dias.

Figura 38 – Estrutura Organizada – Aplicação de GPOS básicas

The screenshot displays the Group Policy Management console. On the left, the navigation pane shows the forest structure under 'Group Policy Management'. The 'CECC.EDU' domain is expanded, revealing several organizational units (OUs): '01. CECC', '02. SERVIDORES', '03. ESTAÇÕES', and others like 'Atalho Rede', 'Bloqueio de USB', 'Mapear Rede', 'Script de Logon', 'Wallpaper', 'COORDENACAO', 'DIRETORIA', 'FINANCIERO', 'PROFESSORES', 'RH', 'SECRETARIA', 'TI', and 'Domain Controllers'. Under '03. ESTAÇÕES', there are sub-OUs for different Windows versions: 'WIN07X64', 'WIN10X64', and 'WIN11X64'. Below these are 'Group Policy Objects', 'WMI Filters', and 'Starter GPOs'. At the bottom of the navigation pane, there are links for 'Sites', 'Group Policy Modeling', and 'Group Policy Results'. To the right, the main pane is titled 'CECC.EDU' and shows the 'Status' tab of the 'Group Policy Objects' page. It includes sections for 'Status Details' (noting SRV-DC01.CECC.EDU as the baseline domain controller), 'Infrastructure Status' (no information exists), and a 'Detect Now' button. Navigation tabs at the top of the right pane include 'Status', 'Linked Group Policy Objects', 'Group Policy Inheritance', and 'Delegation'.

Fonte: o Autor

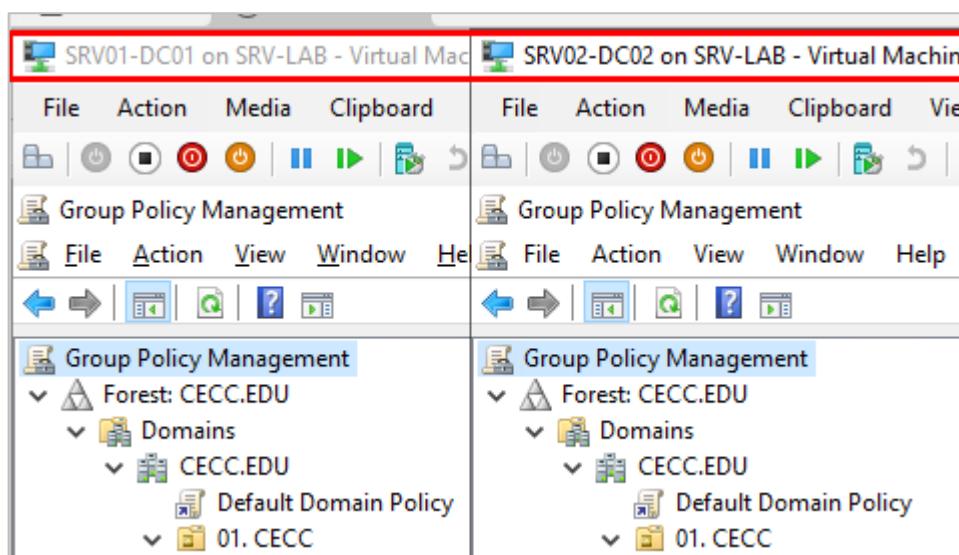
Figura 39 – Estrutura Organizada – Aplicação da GPO Default



Fonte: o Autor

Por hora, finalizamos aqui o servidor controlador de domínio. Vale ressaltar que foi configurado um servidor secundário para garantir a redundância do serviço de autenticação em caso de falhas no servidor primário cabendo ao administrador de TI fazer as devidas configurações para promoção do servidor secundário.

Figura 40 – Estrutura Organizada – Servidores Primário e Secundário



Fonte: o Autor

9 BACKUP

Num mundo cada vez mais digital, nossas informações importantes quase sempre estão vulneráveis. Falhas de hardware, a corrupção de arquivos ou erros humanos são apenas alguns imprevistos que podem causar a perda de dados.

Além disso, softwares maliciosos, a ação de hackers ou vírus podem comprometer a segurança de nossa vida digital. Independentemente da eficácia da máquina, todas estão sujeitas a complicações técnicas. Contudo, esses cenários, põem em riscos a integridade dos arquivos armazenados, como ter a certeza de que nossos arquivos estarão sempre seguros e disponíveis?

9.1 O que é backup?

Backup é o ato de fazer cópias de segurança de um ambiente, aplicação ou dados em um determinado momento. O termo significa fazer cópia dos softwares, arquivos e outros dados em diferentes dispositivos de armazenamento para a recuperação do sistema em caso de falhas.

Como definição, backup é o ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) de dispositivos eletrônicos para sistemas de armazenamento secundários, buscando a preservação do ambiente em caso de qualquer problema.

9.2 Por que é importante manter o backup atualizado?

Somos todos reféns de nossas informações, sejam elas apenas uma lista de contatos do celular ou até milhares de prontuários médicos armazenados dentro de grandes servidores.

O objetivo de montar um procedimento de backup, corporativo ou residencial, é ter uma ou mais cópias de segurança fora do sistema principal, seja ele um celular, computador pessoal ou servidor corporativo. A ideia é ter os arquivos em duplicidade para recuperação dos dados em caso de desastre.

Muitas empresas e usuários domésticos utilizam equipamentos como HDs externos, pendrives, drives de mídias ópticas ou sistemas de armazenamento profissionais baseados em fita ou disco para duplicar suas informações.

Além disso, com a redução dos preços dos serviços de transmissão de dados, muitos usuários têm armazenado as cópias de segurança de suas agendas, vídeos e fotos em servidores remotos de terceiros, também conhecidos como servidores de nuvem.

Ao entenderem e atribuírem valor às informações armazenadas em seus dispositivos eletrônicos, empresas e usuários têm buscado alternativas cada vez mais profissionais para fazer suas cópias de segurança.

Existem diversas formas de fazer backup e o processo para recuperar arquivos em caso de acidente é conhecido como restauração. Mais importante que ter e manter as cópias de segurança atualizadas é conseguir restaurá-las em caso de desastre.

Para este ambiente, escolhemos a ferramenta Veeam Backup, que tem a interface amigável, além de ser bem intuitiva. Embora seja uma solução paga para usufruir de todos os recursos, na versão Community Edition podemos fazer o backup de até 10 instâncias gratuitamente. Com essa nova infraestrutura não teremos essa quantidade de servidores, sendo assim, o Veeam Backup nos atenderá perfeitamente.

O Veeam Backup permite realizar backup e recuperação de ambientes virtuais, físicos ou em nuvem e a escolha do destino dos backups, a ideia é manter o ambiente sempre disponível e protegido

9.2 Implementação da Ferramenta

Iniciamos essa sessão conceituando as definições da ferramenta escolhida pelo time para a implementação da ferramenta Veeam Backup.

Na figura 41 abaixo, possuímos um job de backup que possui duas rotinas de backup configuradas: “BKP ARQUIVOS” e “BKP VM SERVIDORES”. As duas tarefas são incrementais, ou seja, realiza a cópia dos dados modificados após o último trabalho realizado ou incremental, ocupa menos espaço no armazenamento por essa razão e consequentemente o processamento é rápido. Definimos como dias padrões para execução as terças-feiras e quintas-feiras a partir das 22:00h.

Figura 41 – Job de Backups no console de Administração do Veeam

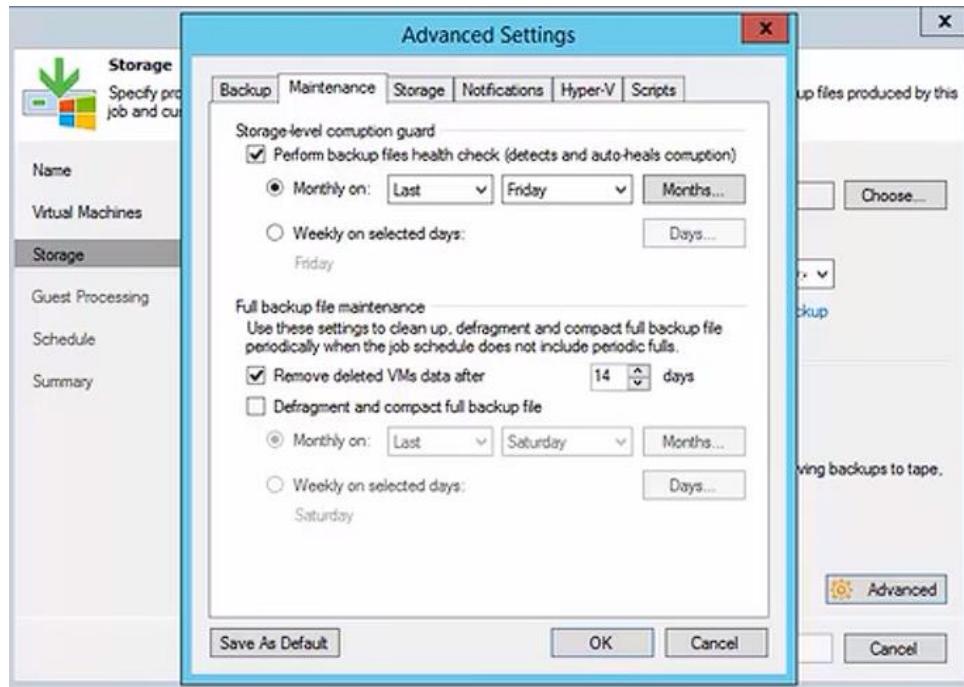
Name	Type	Objects	Status	Last Run	Last Result	Next Run
BKP ARQUIVOS	File Backup	1	Stopped	5 days ago	Success	03/10/2023
BKP VM SERVIDORES	Windows Agent Backup	3	Stopped	6 days ago	Success	03/10/2023

Fonte: o Autor

Não menos importante, foi configurado um job de backup completo, este é feito uma vez por mês no primeiro sábado de cada mês, é importante ressaltar a diferença em relação ao dia pois, sendo um backup completo, exige maior espaço de armazenamento, maior tempo de execução e maior banda para transmissão na rede. Todos os backups também serão armazenados em storage com 12TB (terabytes) de armazenamento disponível e terão 2 anos em relação ao período de Retenção.

Referente ao detalhamento das configurações avançadas do jobs de backup dentro do wizard da solução Veeam. Na aba de “**Backup**” foi selecionado o checkbox “Forward incremental backup”. Foi também selecionado a opção de backup sintético para o dia de sábado. Ativado a criação do full backup com periodicidade para todo o primeiro sábado de cada mês. Agora, na aba de “**Maintenance**” foi selecionado o campo de checagem e recuperação de arquivos corrompidos das VM’s. Ainda na aba de manutenção, foi marcado o campo “**Remove deleted VMs data after**” e colocado 14 dias de retenção para esta opção, ou seja, após esse período os dados da VM excluída serão limpos do storage, garantindo a liberação de espaço para arquivos inúteis.

Figura 42 – Configuração da aba de manutenção da solução Veeam



Fonte: o Autor

Ainda sobre as configurações avançadas do Veeam. No campo “**Storage**”, foi mantido as configurações default. Na aba “**Notifications**” foi selecionado o campo de envio de e-mail com notificação para alertas e erros. Na aba com o nome do Hyper-V onde o Veeam foi provisionado (Hyper-V, VmWare) não foi realizado nenhuma alteração na configuração. Na aba de “**Script**” não foi realizado nenhuma configuração pré e pós do job de backup.

Na figura 43 podemos ver especificamente o que cada backup trata. O “BKP ARQUIVOS” é responsável por realizar as cópias de segurança dos arquivos do SRV-FS01 enquanto o “BKP VM SERVIDORES” como o próprio nome explana, é responsável por realizar as cópias das VMs em si. Dessa forma, podemos ter o máximo de segurança de nossos arquivos e servidores de forma organizada, como iremos ver nas próximas imagens.

Há ainda a possibilidade de subir estes backups para um armazenamento em nuvem e garantir uma maior segurança, porém, os custos devem ser considerados.

Figura 43 – Resultado do job de Backup

Job Name	Creation Time	Restore Points	Repository
BKP ARQUIVOS	25/09/2023 21:06		
SRV-FS01	27/09/2023 18:00	3	
BKP VM SERVIDORES	25/09/2023 21:13		
SRV-DC01	26/09/2023 22:12	2	
SRV-DC02	26/09/2023 22:12	2	
SRV-FS01	26/09/2023 22:12	2	

Fonte: o Autor

Na figura 44, mostramos o local de armazenamento dos backups “DADOS”. E os respectivos arquivos separados por diretório. Como exemplo, usamos o SRV-FS01.

Figura 44 – Storage de Armazenamento

Name	Date modified	Type	Size
BKP VM SERVIDORES - SRV-FS01	26/09/2023 22:14	Veeam backup ch...	75 KB
BKP VM SERVIDORES - SRV-FS01D2023-0...	25/09/2023 21:20	Veeam full backup...	8.207.776 KB
BKP VM SERVIDORES - SRV-FS01D2023-0...	26/09/2023 22:14	Veeam increment...	363.568 KB

Fonte: o Autor

Com o objetivo de garantir a segurança e integridade dos dados de backup, a solução Veeam será replicada em ambiente de nuvem. A replicação será realizada utilizando o recurso de integração do Veeam às soluções cloud. Essa integração é com o objetivo de reduzir o impacto no ambiente, caso haja perda física do servidor de backup on-premisse. Para essa redundância foi utilizado o Google Cloud.

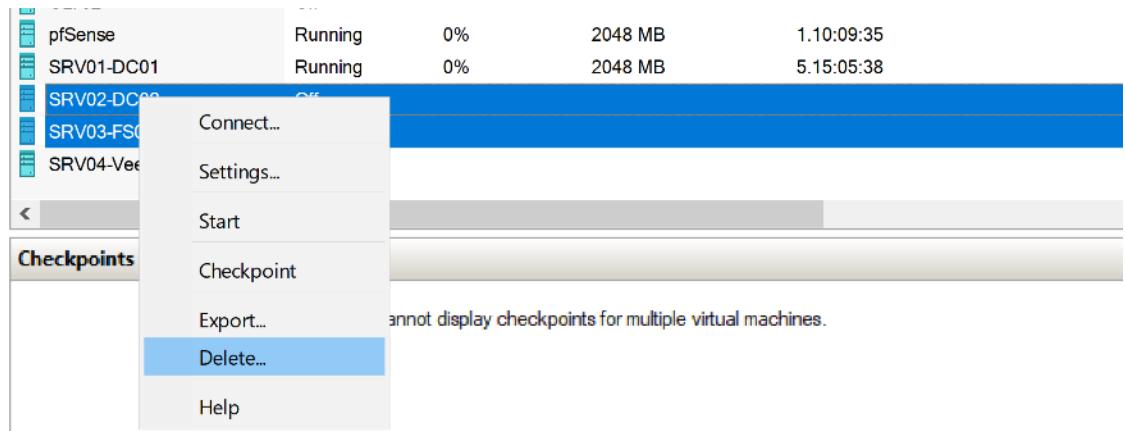
É importante ressaltar, as políticas de Teste de Recuperação (Recovery), fazemos o seguinte questionamento quando comentamos sobre esse tema: “Qual é o valor dos seus dados?”. A resposta é difícil de mensurar, porém, não podemos realizar o backup apenas quando precisarmos dele, é de grande importância que sejam feitos testes de backup para garantir que

estejam funcionando perfeitamente. Sem esses check-ups, temos um enorme risco de perca e falha na recuperação dos dados.

Sendo assim, uma boa prática que definimos de forma periódica, foi inserir a validação após os backups terem sido gerados, ou seja, verificar se de fato, o backup funcionou corretamente, sem deixar de lado a verificação da eficácia do armazenamento. Essa validação é uma excelente oportunidade para averiguarmos vulnerabilidades indispensáveis.

Referente ao procedimento realizado, primeiramente foi realizado a exclusão do SRV-DC02 (Backup do servidor de AD) e do SRV-FS01(Servidor de arquivos), que serão utilizados para o teste.

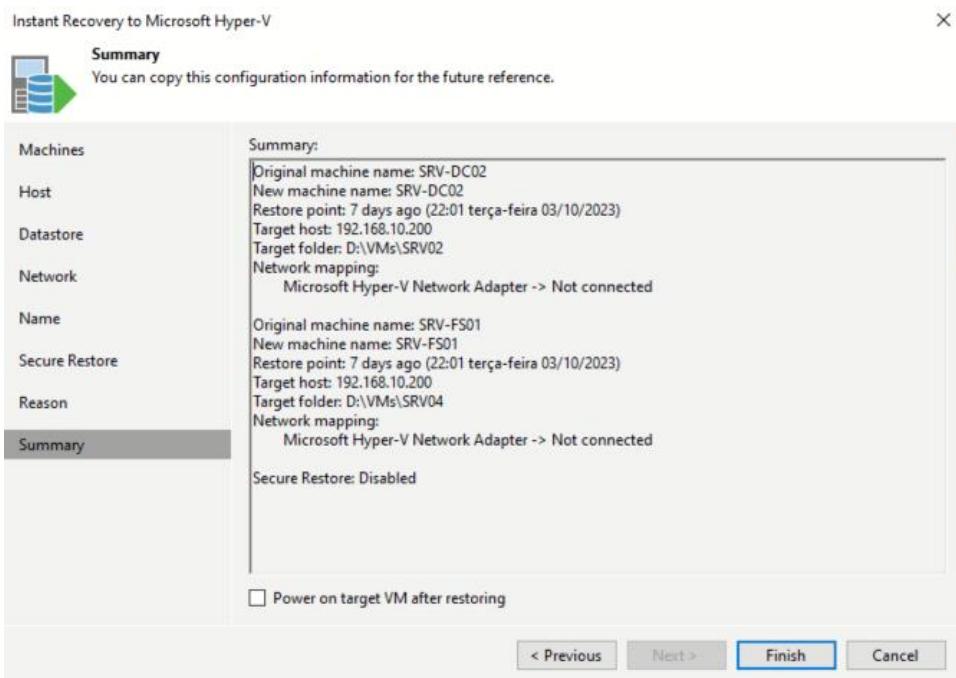
Figura 45 – Exclusão servidores AD e File Server



Fonte: o Autor

Após a exclusão dos servidores, iniciamos o processo de recovery da ferramenta Veeam. O processo é bem intuitivo e é realizado por etapas. Sendo divididas em: **Machines** (seleção das máquinas com informações sobre o tamanho e o ponto de restauração); **Host** (seleção das máquinas com a informação de seu endereço de rede); **Datastore** (seleção dos volumes que deseja recuperar); **Network** (selecionar o mapeamento de rede da máquina original para máquina nova); **Name** (criar o novo nome para as VM's recuperadas); **Reason** (motivo da restauração). As configurações destas etapas foram configuradas de acordo com o pré-requisito do ambiente.

Figura 46 – Resumo das configurações do recovery



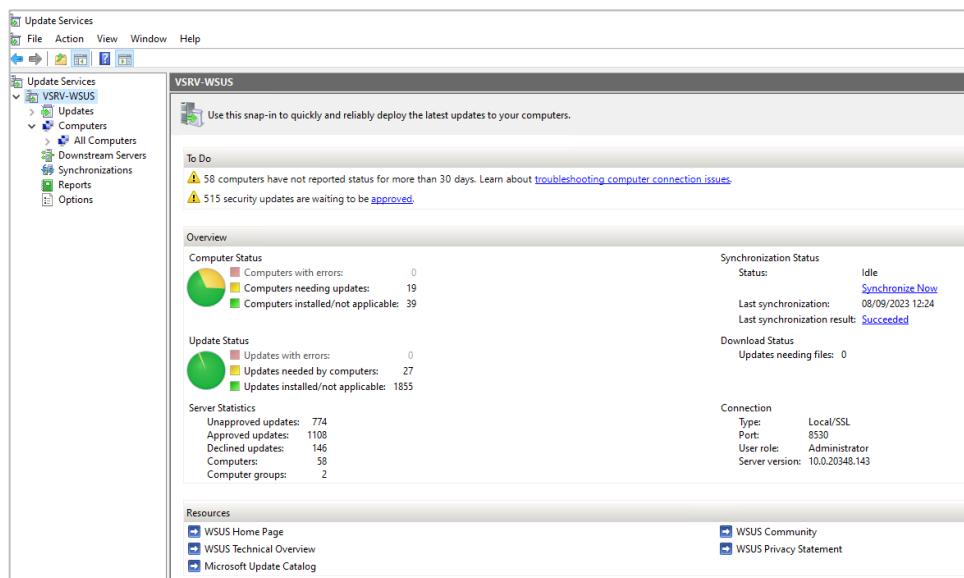
Fonte: o Autor

Foi criado um cronograma trimestral para a restauração do backup do Veeam. A iniciativa dessa ação é para garantir que os dados estejam em conformidade e a operação ocorra sem falhas. Nesta ação será restaurado todos os servidores backupeados no Veeam em um ambiente de teste.

10 WINDOWS UPDATE SERVICE

A ferramenta é essencial quando se tem um parque tecnológico com muitas estações de trabalho. Ela permite centralizar as atualizações em um único ponto de armazenamento, logo após isso, criamos uma política para forçar as estações de trabalho baixarem as atualizações que estão aloquadas neste servidor ao invés de baixar tudo novamente na internet. Essa prática poupará os recursos de rede da empresa, uma vez que podemos agendar o melhor momento para essas atualizações acontecerem. Na figura 47, podemos ver a console de administração do WSUS.

Figura 47 – Console de Administração do WSUS



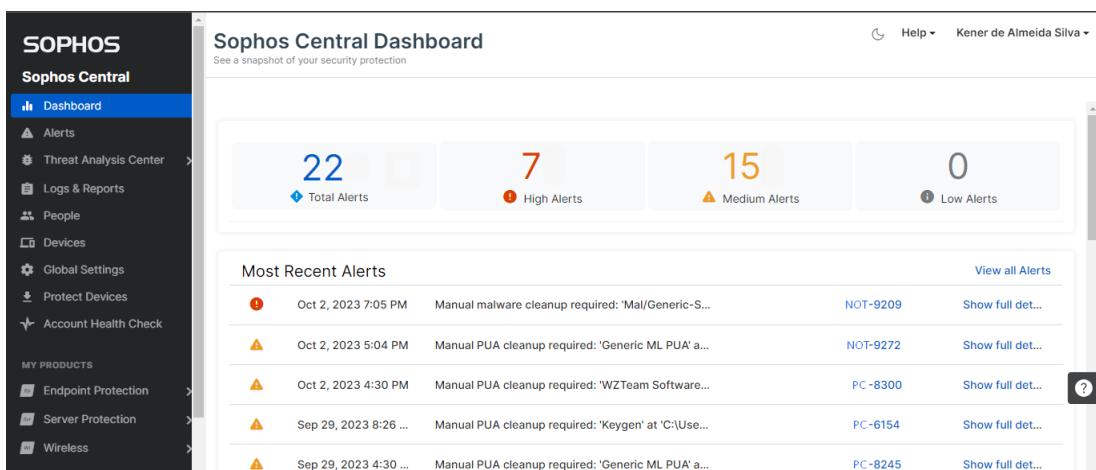
Fonte: o Autor

Inicialmente ficaram acordados para as atualizações serem aplicadas no ambiente a cada 15 dias. A partir das 18 horas. Durante o expediente é feito o download dessas atualizações do servidor para as estações e após este download, os usuários são notificados que existem atualizações para serem aplicadas. Ao desligarem as estações no final do expediente, estas atualizações são aplicadas de forma automática.

11 ANTI-VIRUS

O antivírus é um software que tem o propósito de detectar e eliminar vírus e outros programas prejudiciais antes ou depois de ingressar no sistema. Os vírus, worms, trojans, spyware, rootkits, exploits, ransomware e etc são tipos de programas de software que são implementados sem o consentimento (e inclusive conhecimento) do usuário ou proprietário de um computador e que cumprem diversas funções nocivas para o sistema. Entre elas, o roubo e perda de dados, alteração de funcionamento, interrupção do sistema e propagação para outros computadores. Os antivírus são aplicações projetadas como medida de proteção e segurança para resguardar os dados e o funcionamento de softwares de outras aplicações conhecidas comumente como vírus ou malware que tem a função de alterar, perturbar ou destruir o correto desempenho dos computadores. Os antivírus podem registrar tanto os arquivos encontrados dentro do sistema como aqueles que procuram ingressar ou interagir com o mesmo. Como novos vírus são criados de maneira quase constante, sempre é preciso manter atualizado o programa antivírus de maneira de que possa reconhecer as novas versões maliciosas. Assim, o antivírus pode permanecer em execução durante todo tempo que o software permaneça ligado, ou registrar um arquivo ou série de arquivos cada vez que o usuário exija. Normalmente, o antivírus também pode verificar e-mails e sites de entrada e saída visitados. Um antivírus pode ser complementado por outros aplicativos de segurança, como firewalls ou anti-spywares que cumprem funções auxiliares para evitar a entrada de vírus.

Figura 48 – Dashboard de Gerenciamento



Fonte: o Autor

Na figura 48 podemos observar em destaque os alertas, os hosts apontados com alerta e as opções de gerenciamento da plataforma contratada.

Figura 49 – Eventos do dispositivo

The screenshot shows the Sophos Central interface for device NOT-9209. The left sidebar has 'Devices' selected. The main area shows a summary of the device (Windows 10, IP: 192.168.0.14, last user: edmilson.santos) and a list of events. The 'EVENTS' tab is active. The event list includes:

- Oct 2, 2023 7:41 PM: 'https://media.fvix1-1.fna.whatsapp.net/v/162.7118-24/19426203_12719167442105' (Yellow Box)
- Oct 2, 2023 7:31 PM: 'https://media.fvix1-1.fna.whatsapp.net/v/162.7118-24/19426203_127191674421058' (Yellow Box)
- Oct 2, 2023 7:10 PM: 'https://142.250.78.238/' blocked due to tag 'Financeiro' (Orange Box)
- Oct 2, 2023 7:05 PM: Manual malware cleanup required: 'Mal/Generic-S' at 'C:\Users\Del\Desktop\igor\D' (Red Box)

Fonte: o Autor

Na figura acima podemos observar os eventos detectados durante o dia do usuário, em destaque amarelo temos logs de arquivos baixados em determinado site, em laranja temos uma negação de acesso a site feita por categoria da URL e em vermelho temos a notificação da necessidade de realizar uma limpeza manual com o caminho do arquivo malicioso.

Figura 50 – Status do Dispositivo

The screenshot shows the Sophos Central interface for device NOT-9209. The left sidebar has 'Devices' selected. The main area shows a summary of the device (Windows 10, IP: 192.168.0.14, last user: edmilson.santos) and a 'STATUS' section. The 'STATUS' tab is active. The security health section includes:

- Security Health** (Yellow Box)
 - Running malware in quarantine or cleanup failure (Yellow Box)
 - Last Sophos Central Activity: an hour ago (Green Checkmark)
 - Sophos services running (Green Checkmark)
 - HitmanPro Alert service
 - Sophos Endpoint Defense
 - Sophos Endpoint Defense Service
 - Sophos File Scanner

Fonte: o Autor

A figura acima mostra o status de segurança do dispositivo e as ações que o antivírus executou, em destaque a notificação de execução de um determinado arquivo em quarentena e a falha na limpeza do mesmo (o que gera a necessidade de limpeza manual como ilustrado na figura de eventos).

Figura 51 –Políticas de Endpoint

The screenshot shows the Sophos Central interface for managing devices. On the left, a sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices (which is selected), Global Settings, Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are sections for Endpoint Protection, Server Protection, Wireless, Firewall Management, and Cloud Native Security. The main content area is titled 'NOT-9209' and shows a summary for the device. It includes a warning icon, the device name 'NOT-9209', its operating system 'Windows 10', its IP address '192.168.0.14', and the last user 'edmilson.santos'. Below this are buttons for 'Update now', 'Delete', and 'More actions'. A message at the top states: 'Support for Windows 7, Windows 2008 R2 and Windows SBS 2011 has stopped. Updates have stopped and devices are no longer protected.' A 'More details' button is also present. The 'Events' tab is selected in the navigation bar. A table titled 'Policies below apply to' lists several endpoint protection policies:

Type	Name
Endpoint Protection: Application Control (user)	Base Policy - Application Control
Endpoint Protection: Data Loss Prevention (user)	Base Policy - Data Loss Prevention
Endpoint Protection: Windows Firewall (user)	Base Policy - Windows Firewall
Endpoint Protection: Peripheral Control (device)	Controle de Periféricos_Alow
Endpoint Protection: Threat Protection (user)	Base Policy - Threat Protection
Endpoint Protection: Update Management (user)	Base Policy - Update Management
Endpoint Protection: Web Control (user)	Liberação do WhatsApp WEB

The last two rows, 'Controle de Periféricos_Alow' and 'Liberação do WhatsApp WEB', are highlighted with red boxes.

Fonte: o Autor

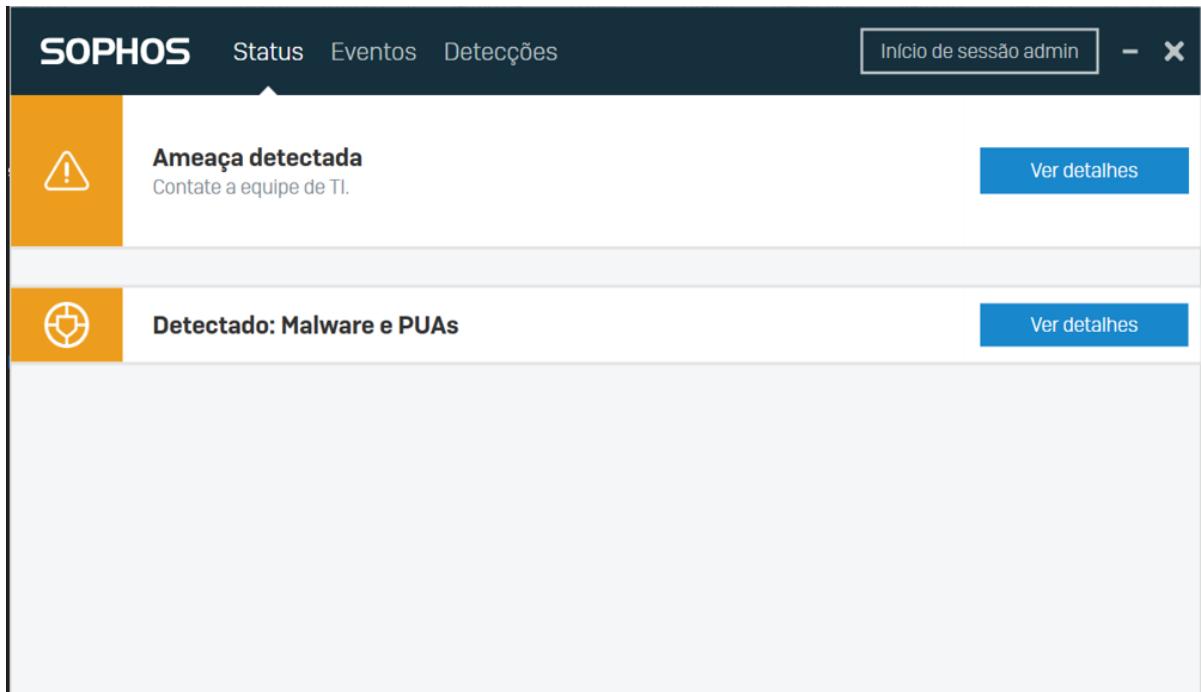
A figura acima mostra a aplicação das políticas de endpoint e dois exemplos em destaque de controles de acesso.

- Controle de Periféricos_Alow – Faz a liberação de periféricos ex: pendrive e bluetooth.
- Liberação do WhatsApp WEB – Faz a liberação da plataforma web para os usuários que fazem o uso profissional da mesma.

11.1 Interfaces de gerenciamento no Host

Os exemplos a seguir mostram a opções gerenciamento no host assim como os alertas e eventos detectados.

Figura 52 –Guia de Status



Fonte: o Autor

A figura acima mostra a página de status do endpoint já com um alerta a ser tratado, ao clicar na opção ‘ver detalhes’ há o redirecionamento para a guia de Eventos, como o mostrado na figura a seguir.

Figura 53 – Guia de Eventos

The screenshot shows the Sophos Endpoint Protection interface with the 'Eventos' tab selected. At the top, there's a navigation bar with the Sophos logo, 'Status', 'Eventos', and 'Detecções' buttons, and a 'Início de sessão admin' button. Below the navigation bar, there are two dropdown menus: 'Todos os Eventos' and 'Todas as fontes', and a 'Renovar Eventos' button. The main area is a table with columns 'Data' and 'Descrição'. The table lists several events, each with a green checkmark icon, a shield icon, a date (e.g., 18/09/2023 13:15:12), and a detailed description of the threat (e.g., 'Ameaça identificada', 'Mal/Generic-S detectada em C:\Users\kener\Documents\TI publico\Programs.zip'). Each event row has a right-pointing arrow icon at the end.

Fonte: o Autor

De acordo com o exemplo acima, o software identificou vários arquivos potencialmente maliciosos e solicita uma limpeza manual, especificando o caminho onde o arquivo se localiza.

Figura 54 – Guia Detecções

Categoria	Detecções
Malware e PUAs	52
Ameaças da Web	7
Comportamento malicioso	0
Itens Controlados	413
Tráfego Mal-Intencionado	0
Explorações	0

Fonte: o Autor

Após a exclusão do arquivo identificado o software inicia uma varredura completa em busca de novos alertas (configuração opcional) e após a execução se não houver outro arquivo suspeito a notificação muda o status para 'resolvido' na central de gerenciamento.

12 SOLUÇÃO WIRELESS - ACCESS POINTS

Os access points são dispositivos de rede usados para estender a cobertura de redes de internet, o access point pode ser entendido como um tipo de repetidor de maior desempenho que usa cabos e não pode ser usado como um substituto a um roteador. O aparelho funciona conectado via cabo a um roteador – ou um switch – e distribui sinal Wi-Fi na outra ponta.

Em geral, é possível controlar de forma centralizada os equipamentos via software do fabricante, ajustando a configuração em massa para cada aparelho e a segurança avançada do Wi-Fi. Também é possível controlar todos os dispositivos conectados, customizando o portal

de acesso. O controle centralizado e a segurança ajudam a explicar por que o access point é comum em ambientes corporativos, já que controlar acesso e oferecer padrões de segurança são características desejáveis em empresas.

Para resolvemos o problema com a rede wireless na CECC, optamos pela linha de APs corporativos Unifi, da fabricante Ubiquiti Networks que possui poderosas soluções para o segmento de redes corporativas.

Com estes Aps, podemos configurar vLans separadas para atender as necessidades da empresa, separando a rede corporativa da rede convidada usando o mesmo access point.

12.1 Configurações iniciais dos access point

Na figura 55 que vemos logo abaixo podemos verificar a configuração dos SSIDs para propagação da rede wireless. Podemos também conferir na figura 56 as configurações de vlan, onde configuramos as vlans 30 e 31 como já citado no escopo inicial do projeto.

Figura 55 – Página de configuração dos SSIDs dos Access Point

Nome	Rede	APs De Broadcast	Clientes (Pico)	Segurança	Experiência
Corporativa	Corporativa	UAP-LR	0 (0)	WPA Personal	N/A
Visitantes	Visitantes	UAP-LR	0 (0)	WPA Personal	N/A

[Criar novo](#) [Gerenciar](#)

Fonte: o autor

Figura 56 – Página de configuração das vlans 30 e 31

Nome	ID Da VLAN	Roteador	Sub-Rede	Internet	Concessões De
Corporativa	30	Gateway de terceiros	-	-	0
Visitantes	31	Gateway de terceiros	-	-	0

[Nova rede virtual](#) [Gerenciar](#)

Fonte: o autor

Na figura 57, podemos ver o resultado deste investimento. Os Aps concentram o número de usuários conectados de forma equilibrada, atendendo com qualidade e segurança. Embora o

todos os usuários estejam conectados nos mesmos Aps, eles estão separados de forma lógica, devido às vlans configuradas.

Figura 57 – Visibilidade dos Aps

Network				
		UniFi Devices		
Type	Name	Model	IP Address	Clients
•	AP-ADM-01	UAP-AC-LR	10.1.30.1	38
•	AP-ADM-02	UAP-AC-LR	10.1.30.2	18
•	AP-ADM-03	UAP-AC-LR	10.1.30.3	18

Fonte: o autor

13 GERENCIAMENTO DE ATIVOS

Também conhecido como ITAM (IT Asset Management), o gerenciamento de ativos consiste em realizar o controle dos equipamentos de TI dentro do ambiente corporativo. O controle normalmente é realizado de forma física e lógica. Fisicamente é por meio da colagem de etiquetas, conhecidas como etiquetas de patrimônio. O gerenciamento de forma lógica, é realizado em equipamentos de TI que possuem conexão à rede, e normalmente é utilizado softwares específicos para esta tarefa.

13.1 Qual importância do gerenciamento de ativos?

O ITAM é de suma importância para as empresas, porque esse processo garante que os ativos possam ser gerenciados de forma correta, inviabilizando o risco de perda ou furto sem o conhecimento da empresa, garantindo o ciclo de vida adequado, processos para descarte de itens obsoletos, e até conformidade dos softwares homologados pela empresa.

O ITAM facilita no fluxo de abertura de incidentes pelos usuários, pois o patrimônio do ativo é um insumo importante nos atendimentos field service e help desk. Além disso, pode ser realizado extrações de incidentes usando os patrimônios como referência, para identificar recorrências de falhas incomuns, que poderão servir de indicadores para reduzir o impacto de falhas no ambiente.

13.2 Como pode ser realizado a gestão de ativos?

A priori, a inventariação física é o primeiro passo. Para isso, é necessário realizar os registros de todos os ativos de TI pegando como referência o número de série do fabricante. Catalogar esse levantamento e adicionar as etiquetas de patrimônio ao respectivo número de série. Ressaltamos a importância do registro da data de homologação do ativo, pois está é uma informação crucial para mensurar a data de ciclo de vida do ativo, que normalmente é de 5-7 anos, após isto é necessário seguir com o fluxo de descarte.

O padrão para as etiquetas vai ser de acordo com o tipo de equipamento e uma numeração escolhida pelo autor da atividade. Por exemplo: Notebook (NOT-0000X), Impressora (IMP-0000X), Monitor (MON-0000X), Access Point (ACP-0000X). Esse gerenciamento pode ser realizado pelo GLPI, ferramenta open source para gerenciamento de inventário. De forma resumida, a ferramenta disponibiliza agentes que podem ser instalados em ativos gerenciáveis (com conexão à rede), e o agente realiza um scan das informações físicas e lógicas do ativo. Ativos que não gerenciáveis devem ser cadastrados manualmente na plataforma. O agente pode ser distribuído via GPO.

Figura 58 – Exemplo de controle de ativos de TI no GLPI

	Nome	Status	Número de Série	Tipo	Modelo	Sistema Operacional - Nome	Última Atualização	Componentes - Processador	Componentes - Tipo de Disco Rígido	Componentes - Tamanho de Disco Rígido	Componentes - Tipo de Memória	Componente Memória
	ADM001	Ativo	GR5N8BZ	Low Profile Desktop	OptiPlex 3020M	Microsoft Windows 10 Pro	13-10-2023 11:23	Intel Core i3-4160T CPU @ 3.10GHz	CT240BX500SSD1	234.43 GB	DDR3 - SODIMM	4 GB
	ADM002	Ativo	BC773N2	Desktop	OptiPlex 3050 Pro	Microsoft Windows 10 Pro	13-10-2023 11:55	Intel Core i5-7500T CPU @ 2.70GHz	KINGSTON SA400S37240G	234.43 GB	DDR4 - SODIMM	8 GB
	ADM003	Ativo	26Y29T2	Docking Station	Inspiron 15-3587 Pro	Microsoft Windows 10 Pro	12-10-2023 12:12	Intel Core i5-7200U CPU @ 2.50GHz	CT240BX500SSD1	234.43 GB	DDR4 - SODIMM	8 GB
	ADM004	Ativo	4JVHF22	Low Profile Desktop	OptiPlex 3020M	Microsoft Windows 10 Pro	13-10-2023 10:57	Intel Core i5-4590T CPU @ 2.00GHz	ST500LM021-1KJ152	488.39 GB	DDR3 - SODIMM	4 GB
	ADM005	Ativo	6Q4P4V3	Desktop	Vostro 3710 Pro	Microsoft Windows 11 Pro	13-10-2023 11:30	12th Gen Intel Core i7-12700 Pro	IM2P33F3A NVMe ADATA 512GB	476.94 GB	DDR4 - DIMM	16 GB
	ADM006	Ativo	8JRNL02	Desktop	OptiPlex 3040 Pro	Microsoft Windows 10 Pro	13-10-2023 11:16	Intel Core i5-6500T CPU @ 2.50GHz	KINGSTON SA400S37240G	234.43 GB	DDR3 - SODIMM	4 GB
	ADM007	Ativo	BRIH6MD2	Desktop	OptiPlex 3040 Pro	Microsoft Windows 10 Pro	10-10-2023 17:39	Intel Core i3-6100T CPU @ 3.20GHz	TOSHIBA MQ01ACF050	488.39 GB	DDR3 - SODIMM	4 GB
	ADM008	Ativo	FRO1542	Low Profile Desktop	OptiPlex 3020M Pro	Microsoft Windows 10 Pro	13-10-2023 11:33	Intel Core i5-4590T CPU @ 2.00GHz	CT240BX500SSD1	234.43 GB	DDR3 - SODIMM	4 GB
	ADM009	Ativo	DHVHF22	Low Profile Desktop	OptiPlex 3020M Pro	Microsoft Windows 10 Pro	13-10-2023 13:00	Intel Core i5-4590T CPU @ 2.00GHz	ST500LM021-1KJ152	488.39 GB	DDR3 - SODIMM	4 GB
	ADM010	Ativo	9NPY9B2	Low Profile Desktop	OptiPlex 3020M Pro	Microsoft Windows 10 Pro	13-10-2023 11:43	Intel Core i5-4590T CPU @ 2.00GHz	CT240BX500SSD1	234.43 GB	DDR3 - SODIMM	4 GB
	ADM011	Ativo	8JRQL02	Desktop	OptiPlex 3040 Pro	Microsoft Windows 10 Pro	13-10-2023 11:56	Intel Core i5-6500T CPU @ 2.50GHz	CT240BX500SSD1	234.43 GB	DDR3 - SODIMM	4 GB
	ADM012	Ativo	26W49T2	Docking Station	Inspiron 15-3587 Pro	Microsoft Windows 10 Pro	11-10-2023 17:19	Intel Core i5-7200U CPU @ 2.50GHz	PNY CS900 240GB SSD	234.43 GB	DDR4 - SODIMM	8 GB
	ADM013	Ativo	9NRZB2	Low Profile Desktop	OptiPlex 3020M Pro	Microsoft Windows 10 Pro	13-10-2023 12:57	Intel Core i5-4590T CPU @ 2.00GHz	CT240BX500SSD1	234.43 GB	DDR3 - SODIMM	4 GB
	ADM014	Ativo	SSW33T2	Desktop	OptiPlex 3080 Pro	Microsoft Windows 10 Pro	13-10-2023 13:09	Intel Core i5-6500T CPU @ 2.10GHz	KINGSTON SA400S37240G	234.43 GB	DDR4 - SODIMM	8 GB

Fonte: o autor

Outro fator determinante para a utilização de ferramentas de inventário, é para gestão dos softwares de SI, pois com a ferramenta é possível extrair relatórios que nos informam a versão do software, se está instalado ou não, informações essenciais para validar a conformidade no gerenciamento de vulnerabilidades no ambiente.

Mensalmente serão realizado um trabalho de sustentação em cima de workstations que o agente do GLPI não comunica há mais de 45 dias. Este é um trabalho para identificar se existe uma falha de comunicação do agente na máquina ou se o ativo se encontra ocioso.

Figura 59 – Dashboard dos reports GLPI



Fonte: o autor

A ferramenta do GLPI disponibiliza recursos de criação de dashboards com filtros criado com a nossa preferência. Esta interface facilita na gestão dos ativos em nosso ambiente.

13.3 Upgrade das estações

A modernização e renovação dos equipamentos de Tecnologia da Informação (TI) da empresa são passos cruciais para manter a competitividade e eficiência nos negócios. Dentro do escopo do projeto, há também a necessidade de atualizar os equipamentos atuais para atender às crescentes demandas do mercado e garantir que as operações sejam eficazes e seguras. Esta iniciativa de renovação trouxe uma série de benefícios significativos para a empresa.

Além do servidor, outra parte dos investimentos foi novas estações de trabalho para os colaboradores da CECC. Os sistemas que eram usados eram antigos e não havia mais suporte. As estações antigas não teriam um bom desempenho para as novas versões do sistema operacional Windows. Com os novos computadores, será possível um aumento considerável no conforto e na produtividade, uma vez que as tarefas agora são realizadas de maneira mais rápida e eficiente.

Abaixo, na figura x, vemos o modelo escolhido para a substituição das antigas estações:

Figura 60 – Ficha técnica do computador Novo OptiPlex Micro da Dell



Novo OptiPlex Micro

★★★★★ (0) Fazer uma pergunta

13ª Geração Intel® Core™ i5-13500T (14 Núcleos, 24MB, 1.60 GHz to 4.60 GHz, 35W)
 Windows 11 Pro, Português, Inglês, Francês, Espanhol
(A Dell Technologies recomenda o Windows 11 Pro para empresas)

8 GB: 1 de 8 GB, DDR4, Brasil
 SSD de 256GB PCIe NVMe M.2 (Classe 35)

OptiPlex Micro com CPU de 35W
 Portas e slots

De	R\$ 4.357,00
Desconto	R\$ 538,00
Preço	R\$ 3.819,00

Ofertas especiais

Adicionar ao carrinho

Fonte: https://www.dell.com/pt-br/shop/computadores-all-in-ones-e-workstations/desktop-optiplex-micro/spd/optiplex-7010-micro/cto02o7010mffbcc_on_1?redirectTo=SOC

Os computadores não estavam em mau estado, somente não atendiam mais as necessidades da empresa, portanto, a CECC decidiu doar os computadores para escolas públicas de ensino infantil dos anos iniciais. Sendo assim, estas escolas já conseguem fazer a inclusão digital destes alunos, dando a eles acesso à internet. Vale ressaltar que estes computadores passaram por todo processo de reciclagem e todos eles foram devidamente formatados para garantir que nenhum dado da empresa fosse com os equipamentos antigos.

14 CONSCIENTIZAÇÃO E CAPACITAÇÃO

No tópico 5.5 de Treinamento e Conscientização, declaramos a devida importância que a conscientização das mudanças e a aplicação da prática da capacitação realizada com os funcionários deve ser feita. Portanto, a nossa equipe não apenas foi contatada para fazer uma avaliação da sua infraestrutura atual e correção, como também, aplicação da reciclagem técnica e operacional.

Logo no início das alterações produzidas na CECC, enviamos comunicados por e-mail sobre a conscientização e orientação dos processos modificados e a sua importância para a empresa, sinalizamos sobre os testes de capacitação que são cruciais para a melhoria e desenvolvimento dos funcionários para que acarrete menores erros, esses testes são constituídos de 10 perguntas de múltipla escolha e possuem meta de pontuação para que sejam aprovados, caso o funcionário atinja a nota acima de 80%, estará automaticamente aprovado, caso fique abaixo, o mesmo ficará reprovado e será necessário a repetição do treinamento e um novo teste deverá ser realizado.

Todos esses processos, definimos como reciclagem pois, não podemos deixar que nosso nível de criticidade em relação aos erros seja atenuado, ou seja, o máximo de otimização deve ser efetuado. Portanto, após todo o processo ser concluído com sucesso, os funcionários estarão aptos a laborar as suas atividades novamente.

REFERÊNCIAS

PSI-002 – Política de Segurança da Informação Pública

NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.

NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.

NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes.

Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais).

ISO 27000, Lei Nº 9.609

<https://cloudinfrastructureservices.co.uk/active-directory-ports/>

<https://hmlolina.dev/p/hyper-v-vlan-trunking-for-pfsense/>

<https://secbitrez.files.wordpress.com/2018/09/rules-firewall-pfsense2.pdf>

<https://secbitrez.wordpress.com/firewall-pfsense/>

<https://docs.brascloud.com.br/pages/viewpage.action?pageId=40967512#>

<https://www.controle.net/faq/o-que-e-backup>

<https://www.portalgsti.com.br/2017/12/pfsense-backup-e-restore.html>

<https://infonova.com.br/o-que-e-failover-importante/>

<https://www.monitoratec.com.br/blog/load-balance/>

<https://blog.starti.com.br/>

<https://reciclablu.mob.tec.br/reciclar-computadores/como-descartar-computadores-antigos/>

<https://e-tinet.com/snort-monitor-redes/>

<https://www.snort.org/>

<https://mundodacomputacaointegral.blogspot.com/2021/05/conhecendo-o-snort.html>

<https://www.udemy.com/course/ninja-pfsense/>

<https://www.microserviceit.com.br/teste-de-backup/>

https://helpcenter.veeam.com/docs/backup/vsphere/cloud_credentials_google.html?ver=120