



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

CYBER SECURITY

AMBIENTE PROTEGIDO

Documento apresentado no Eixo 5 do curso superior de
Tecnologia em Redes de Computadores
Orientador: Luiz Ferreira

Elaborado por:
André Souza
Brandon Heringer
Israel Oliveira
Júlio César Araújo da Luz

SUMÁRIO	
1. RESUMO	3
2. INTODUÇÃO.....	4
3. COMPONENTES DA REDE	5
3.1. Ambiente de Rede.....	5
4. TOPOLOGIA.....	6
4.1. Servidor AD: Active Directory.....	7
4.2. Servidor de Arquivo – File Server.....	8
4.2.1. Permissão de Acesso – File Server.....	9
4.2.2. Usuários.....	10
4.2.3. Pasta com acesso	10
4.2.4. Pasta sem acesso	11
4.3. Desktops – Host Cliente	11
5. MEDIDAS DE SEGURANÇA CIBERNÉTICA.....	11
5.1. Fortinet.....	13
5.1.1. Política de Firewall.....	13
5.1.2. Políticas de Objetos.....	14
5.1.3. Interface de Configuração.....	14
5.1.4. Stateful Inspection (Inspeção de Estado).....	15
5.1.5. Filtragem de Tráfego por Porta e Protocolo.....	15
5.1.6. VPN (Rede Virtual Privada).....	15
6. PENTEST: TESTE DE INTRUSÃO.....	16
6.1. Owasp Zap	17
6.1.1. Report Pentest	18
7. CERTIFICADO DIGITAL	19
8. TREINAMENTOS: PREPARAÇÃO DOS CLIENTES INTERNOS.....	20
9. CONCLUSÃO	21
10. REFERÊNCIAS	22

1. RESUMO

Neste documento, o grupo 03 do curso superior de Tecnologia em Redes de Computadores, apresenta a configuração de uma infraestrutura de rede, com um foco especial em medidas de segurança cibernética, para proteger as informações, dados confidenciais e acessos a vários diretórios e serviços de ambiente de rede. Esse enfoque é essencial para garantir a integridade e a confidencialidade das informações e ativos.

A implementação de políticas de segurança da informação, incluindo planos de contingência, é crucial para garantir a confidencialidade, integridade e disponibilidade dos dados, especialmente diante de eventos imprevistos como desastres naturais e possíveis invasões de hackers.

2. INTRODUÇÃO

A Tecnologia da Informação (TI) tem desempenhado um papel fundamental no enriquecimento de todo o processo organizacional nas empresas modernas. Por meio de avanços tecnológicos, sistemas e softwares inovadores, a TI se estabeleceu como uma ferramenta indispensável para aprimorar a eficiência das atividades, facilitar a comunicação interna e externa, e elevar o processo decisório a novos patamares.

No mundo corporativo, a otimização das atividades é essencial para o sucesso e a competitividade. A TI tornou possível automatizar tarefas repetitivas, economizando tempo e recursos valiosos. Isso permite que os profissionais se concentrem em atividades mais estratégicas e criativas, contribuindo para o crescimento e a inovação da organização.

Além disso, a TI desempenha um papel crucial na melhoria da comunicação dentro e fora da empresa. Através de ferramentas como e-mails, videoconferências e aplicativos de mensagens, as barreiras geográficas são superadas, permitindo que equipes trabalhem de forma colaborativa, independentemente de sua localização. Isso não apenas acelera a tomada de decisões, mas também promove uma cultura de colaboração que é fundamental nos ambientes de negócios atuais.

No entanto, à medida que a TI se torna cada vez mais integrada aos processos organizacionais, uma preocupação crescente com a segurança das informações surge naturalmente. Com a eficiência e a eficácia aprimoradas, o volume de dados e informações críticas também aumenta. É essencial proteger esses ativos valiosos contra ameaças cibernéticas, roubo de dados e acessos não autorizados.

Nesse sentido, as empresas estão investindo em soluções de segurança cibernética robustas, como firewalls avançados, sistemas de detecção de intrusão, autenticação multifatorial e treinamento em segurança da informação. A proteção adequada dos dados não apenas protege a reputação da organização, mas também evita perdas financeiras significativas e garante a conformidade com regulamentações de privacidade de dados cada vez mais rigorosas.

Em resumo, a Tecnologia da Informação está desempenhando um papel vital na transformação das empresas modernas. Ela otimiza as operações, melhora a comunicação e impulsiona o processo decisório. No entanto, à medida que as

informações se tornam mais eficientes e eficazes, a segurança torna-se uma prioridade crítica. Portanto, o investimento em segurança cibernética é tão essencial quanto a adoção de novas tecnologias, garantindo que as organizações possam colher os benefícios da TI de maneira segura e sustentável.

3. COMPONENTES DA REDE

A rede é composta por itens essenciais que garantem a funcionalidade e segurança do ambiente. É formada por um servidor que desempenha funções importantes, incluindo Active Directory, DNS, File Server e um servidor web. Além disso, contamos com um firewall para segurança dos ativos e desktops.

Servidor de Domínio (AD)

Sistema Operacional: Windows Server 2022

Funções: Active Directory, DNS e File Server

Servidor Web

Sistema Operacional: Linux Debian 12

Funções: Página web com Apache

Firewall

Appliance

Solução: Fortigate 7.0.12

Desktop

Sistema Operacional: Windows 10 Pro

Função: Workstation

3.1. Ambiente de Rede

A topologia de rede é a forma como os dispositivos de uma rede estão conectados entre si, como computadores, servidores, switches, firewalls, access points e outros componentes. Em essência, representa a estrutura fundamental da rede, podendo ser descrita tanto de forma lógica quanto física.

Em nosso escopo, apresentamos uma infraestrutura de rede organizada, com setorizações segregadas e VLANs implementadas de acordo com a estruturação. Os componentes principais dessa estrutura incluem servidores, switches, firewalls e computadores clientes.

Definimos as configurações das redes, parametrizando os acessos através de VLANs, segmentando as áreas de acordo com os departamentos. As vlans de dados

não se comunicam entre si, apenas com a vlan de servidores com os serviços e permissões necessários.

4. TOPOLOGIA

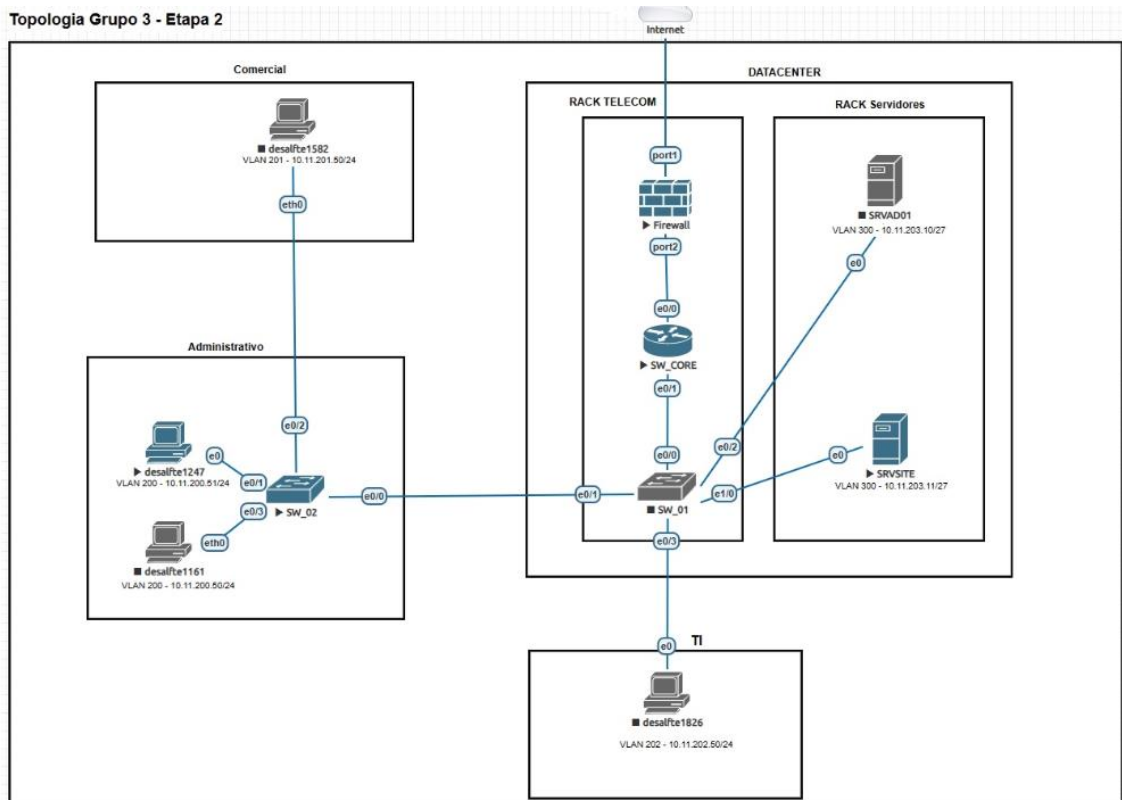


Figura1: Topologia demonstrando as redes com os endereços IPs

Vlan 200 – Administrativo - DP, Financeiro, Jurídico, Projetos - 10.11.200.1/24

Vlan 201 – Comercial - Marketing, Central de relacionamento 10.11.201.1/24

Vlan 202 – TI – Setores de Infraestrutura, Sistemas - 10.11.202.1/24

Vlan 300 – Servidores - Administração Telecom - 10.11.203.1/27

4.1. Servidor AD: Active Directory

O Active Directory é um serviço de diretório desenvolvido pela Microsoft para ambientes de rede Windows. Ele armazena informações sobre objetos na rede, como usuários, computadores, grupos, impressoras e recursos compartilhados. Essas informações são organizadas em uma estrutura hierárquica que facilita a localização e o gerenciamento de recursos.

Suas principais funções são:

Autenticação: O AD permite que os usuários se autentiquem em uma rede, verificando suas identidades usando nomes de usuário e senhas.

Autorização ou Permissão de Acesso: Ele controla o acesso a recursos da rede com base nas permissões atribuídas aos usuários ou grupos. Isso ajuda a garantir que apenas pessoas autorizadas tenham acesso a determinados dados ou serviços.

Políticas de Segurança: O AD permite a aplicação de políticas de segurança em toda a rede. Isso inclui políticas de senha, restrições de acesso e auditoria.

Gerenciamento Centralizado: Facilita a administração centralizada de contas de usuário, dispositivos, servidores e políticas de grupo em toda a rede.

Replicação de Dados: O AD suporta replicação de dados entre servidores para garantir a disponibilidade e a redundância das informações.

Integração com Aplicações: Muitos aplicativos e serviços, especialmente aqueles desenvolvidos pela Microsoft, podem ser integrados ao Active Directory para simplificar a autenticação e o gerenciamento de usuários.

Em resumo, o Active Directory é um item fundamental da infraestrutura de rede em ambientes corporativos. Ele simplifica o gerenciamento de recursos de rede, melhora a segurança e facilita a administração de usuários e dispositivos em uma rede Windows.

4.2. Servidor de Arquivo – File Server

O File Server, é um componente essencial em redes de computadores que armazena, gerencia e fornece acesso a arquivos e pastas compartilhadas para os usuários da rede. A seguir estão algumas das principais funções e características de um servidor de arquivos:

Integração com Diretórios e Contas de Usuário: Em redes corporativas, os servidores de arquivos geralmente se integram a sistemas de diretórios, como o Active Directory da Microsoft, para simplificar a gestão de contas de usuário e permissões de acesso.

Armazenamento Centralizado: O servidor de arquivos centraliza o armazenamento de dados em um único local na rede. Isso facilita o backup, a recuperação e o gerenciamento de dados, pois todos os arquivos estão em um único local.

Compartilhamento de Arquivos: Ele permite que os usuários compartilhem arquivos e pastas com outros usuários na rede. Isso é útil para colaboração e compartilhamento de documentos.

Controle de Acesso: Um servidor de arquivos permite que os administradores controlem quem tem permissão para acessar pastas e arquivos específicos. Isso é feito por meio de permissões de acesso, como leitura, gravação e execução.

Segurança de Dados: Ele pode fornecer medidas de segurança para proteger os dados armazenados, incluindo criptografia, controle de acesso baseado em função e auditoria.

Backup e Recuperação: Facilita o backup regular dos dados armazenados, permitindo a recuperação de arquivos em caso de perda de dados ou falha de hardware.

Redundância e Tolerância a Falhas: Em ambientes críticos, servidores de arquivos podem ser configurados com redundância para garantir a disponibilidade contínua dos dados, mesmo em caso de falha de hardware.

Auditoria de Acesso: É possível rastrear quem acessou, modificou ou excluiu arquivos usando recursos de auditoria, o que é útil para fins de segurança e conformidade.

Capacidade de Escalabilidade: Os servidores de arquivos podem ser dimensionados para atender às necessidades crescentes de armazenamento de dados à medida que uma organização cresce.

Em resumo, um servidor de arquivos desempenha um papel crucial na gestão e compartilhamento de dados em uma rede, tornando mais fácil para os usuários acessarem, compartilhar e proteger seus arquivos e pastas de maneira organizada e controlada.

4.2.1. Permissão de Acesso – File Server

O gerenciamento de acesso as pastas são feitos com base em grupos de usuários do AD, sempre criando um grupo de usuários com permissão de leitura e um grupo com permissão de escrita.

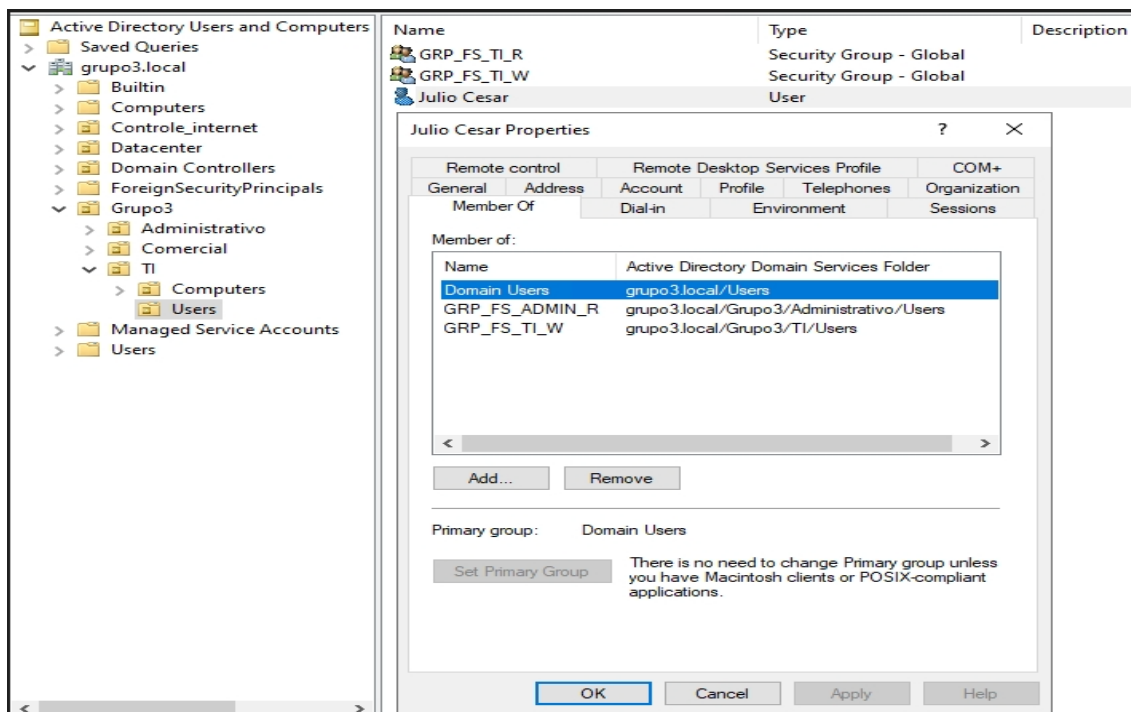
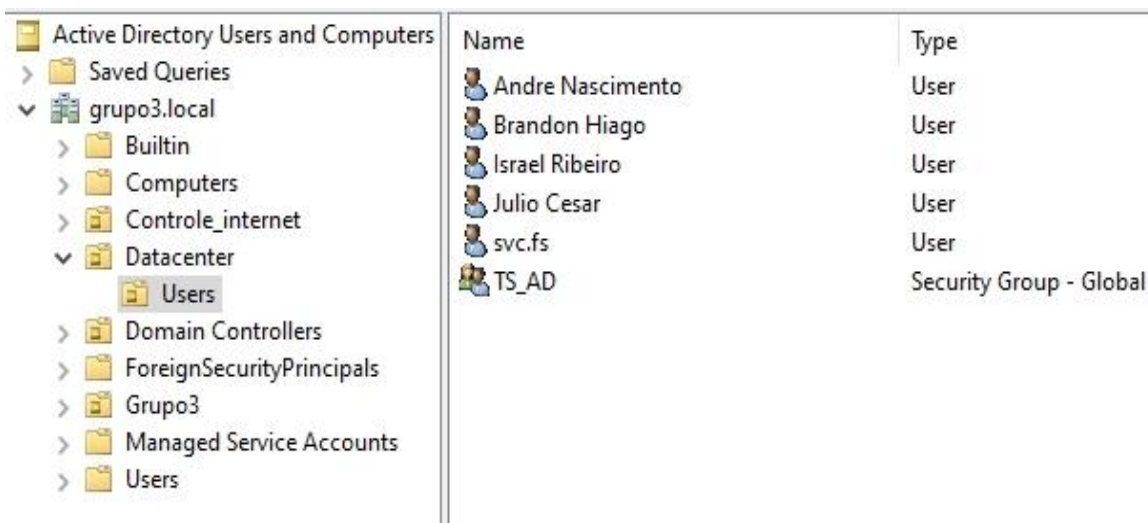


Figura2: Exemplo de grupos atribuídos a conta de usuário, onde ele está vinculado a dois grupos com permissões diferentes.

4.2.2. Usuários



Name	Type
Andre Nascimento	User
Brandon Hiago	User
Israel Ribeiro	User
Julio Cesar	User
svc.fs	User
TS_AD	Security Group - Global

The screenshot shows the 'Active Directory Users and Computers' console. The left pane displays a tree view with 'grupo3.local' expanded, showing folders like 'Built-in', 'Computers', 'Controle_internet', 'Datacenter', 'Users', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Grupo3', 'Managed Service Accounts', and 'Users'. The right pane shows a list of users and a security group.

Figura3: Contas de serviço criadas no Active Directory (AD) para gerenciamento de servidores.

4.2.3. Pasta com acesso

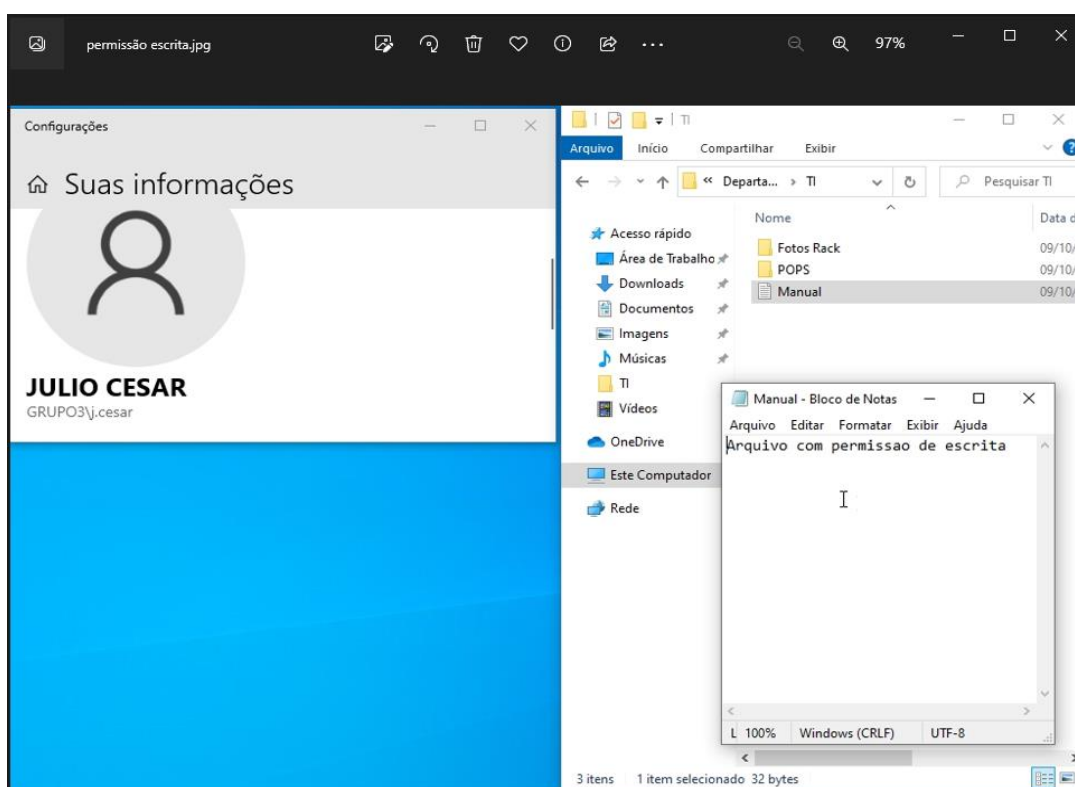


Figura4: Usuário com permissão de escrita na pasta TI.

4.2.4. Pasta sem acesso

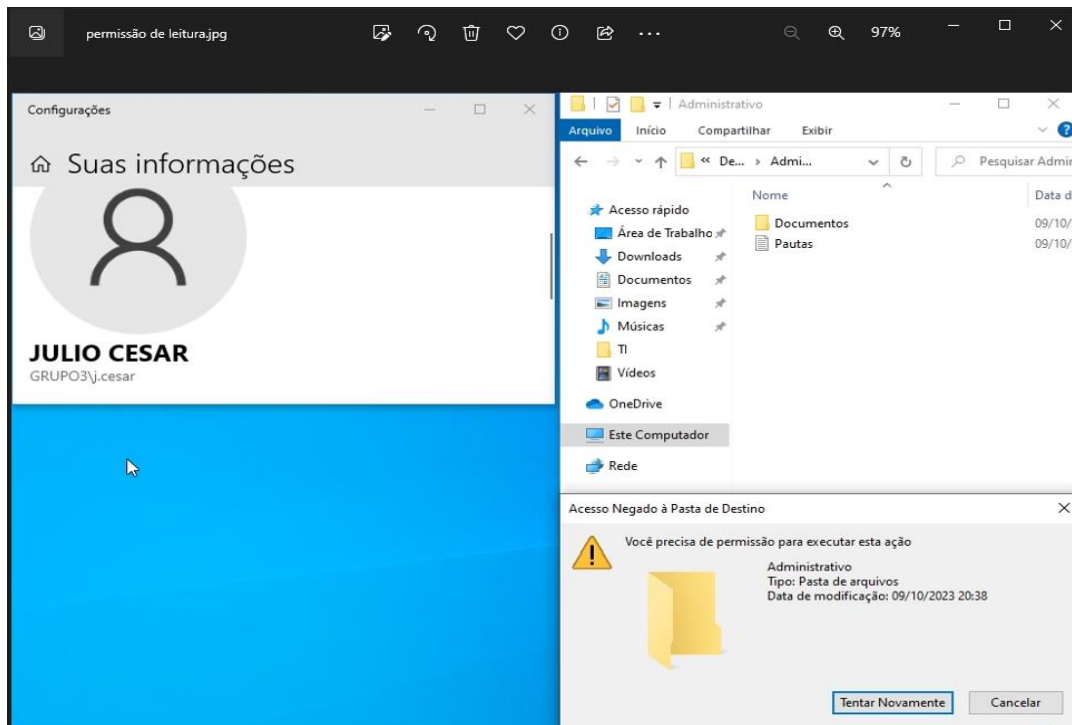


Figura5: Usuário com acesso apenas leitura na pasta Administrativo.

4.3. Desktops – Host Cliente

Para os desktops, foi utilizado o Windows 10, pois é um sistema operacional popular, oferece uma variedade de recursos e funcionalidades que atendem às necessidades de usuários empresariais com boa compatibilidade, custo e confiabilidade.

5. MEDIDAS DE SEGURANÇA CIBERNÉTICA

Segurança cibernética é a prática de proteger sistemas essenciais e informações sensíveis contra ataques digitais. Também conhecida como segurança da tecnologia da informação (TI), as medidas de segurança cibernética são concebidas para combater ameaças contra sistemas de aplicações em rede, quer essas ameaças sejam provenientes de dentro ou de fora de uma organização. Para garantir a segurança cibernética de nossa rede, foram implementadas as seguintes medidas:

Atualizações de Software: Todos os sistemas operacionais e aplicativos são atualizados regularmente para corrigir vulnerabilidades conhecidas.

Políticas de Acesso: Políticas de controle de acesso são aplicadas para controlar quem tem permissão para acessar recursos da rede.

Deteção de Intrusões: Sistema de deteção de intrusões (IDS) será implementada para identificar possíveis ameaças à segurança.

Políticas de Senha: Como boas práticas, as contas de usuários estão com comprimento mínimo de 8 caracteres, requisitos de complexidade habilitadas (exige o uso de caracteres especiais, letras e números), histórico de senha (proíbe a reutilização da mesma senha) e tempo de expiração de senha habilitado.

Backup: É de suma importância a utilização de uma ferramenta confiável de backup, o monitoramento se as rotinas estão sendo realizadas e frequentes testes de restore, homologando a eficácia da rotina.

Firewall: Configurado um firewall de perímetro robusto que estará direcionado para proteger toda a rede contra ameaças externas.

Como exemplo, consideramos o uso de um dispositivo Fortigate nesta etapa.

O Fortigate atua como uma barreira de segurança, controlando o tráfego de rede entre redes de diferentes níveis de confiança. Funciona como um filtro que permite ou bloqueia o tráfego com base nas regras que são definidas.

Além disso, o Firewall Fortinet mantém registros de eventos de segurança, permitindo a auditoria e análise das atividades na rede. Essa funcionalidade é fundamental para identificar possíveis violações de segurança e outras questões relevantes.

É importante notar que a configuração específica de um firewall Fortinet pode variar, dependendo das necessidades de segurança específicas da rede e da versão do software em uso. Para configurações detalhadas e personalizadas, recomenda-se consultar a documentação oficial da Fortinet ou buscar a assistência de um profissional de segurança de rede experiente.

Os dispositivos de segurança de rede podem ser usados como proxies de aplicação para inspecionar e controlar o tráfego de aplicativos específicos, como HTTP, FTP, SMTP, entre outros.

5.1. Fortinet

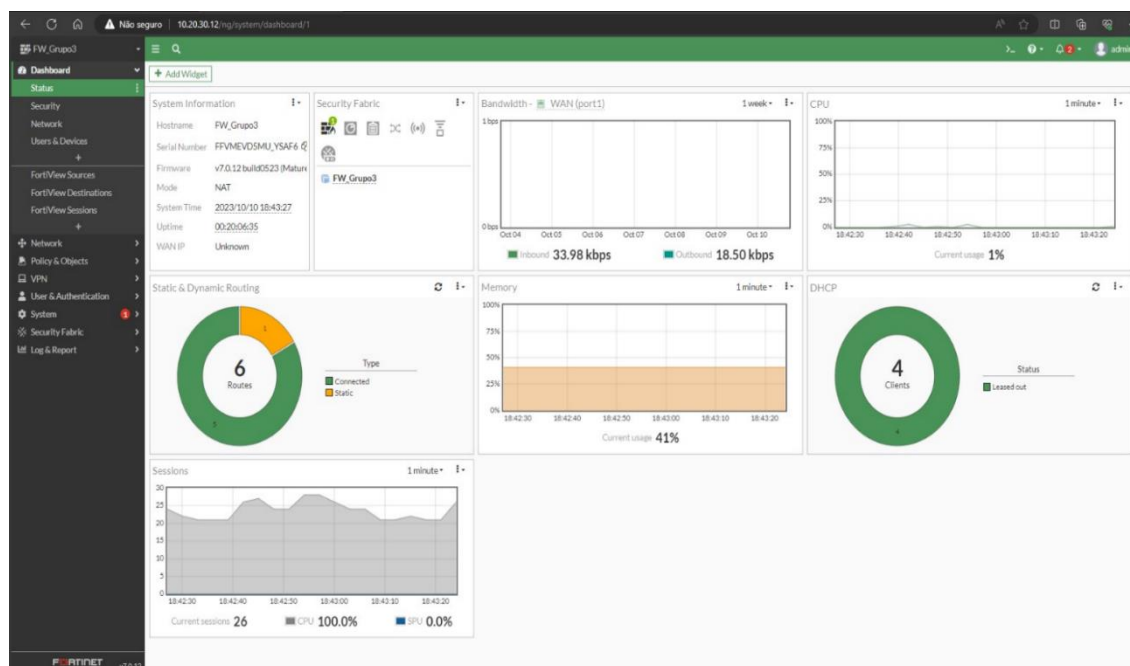


Figura6: Firewall – Dashboard fortinet

5.1.1. Política de Firewall

A política de firewall consiste em um conjunto de regras que determina o tratamento do tráfego de rede. Essas regras abrangem a permissão ou bloqueio de determinados tipos de tráfego com base em endereços IP, portas, protocolos e outras condições específicas.

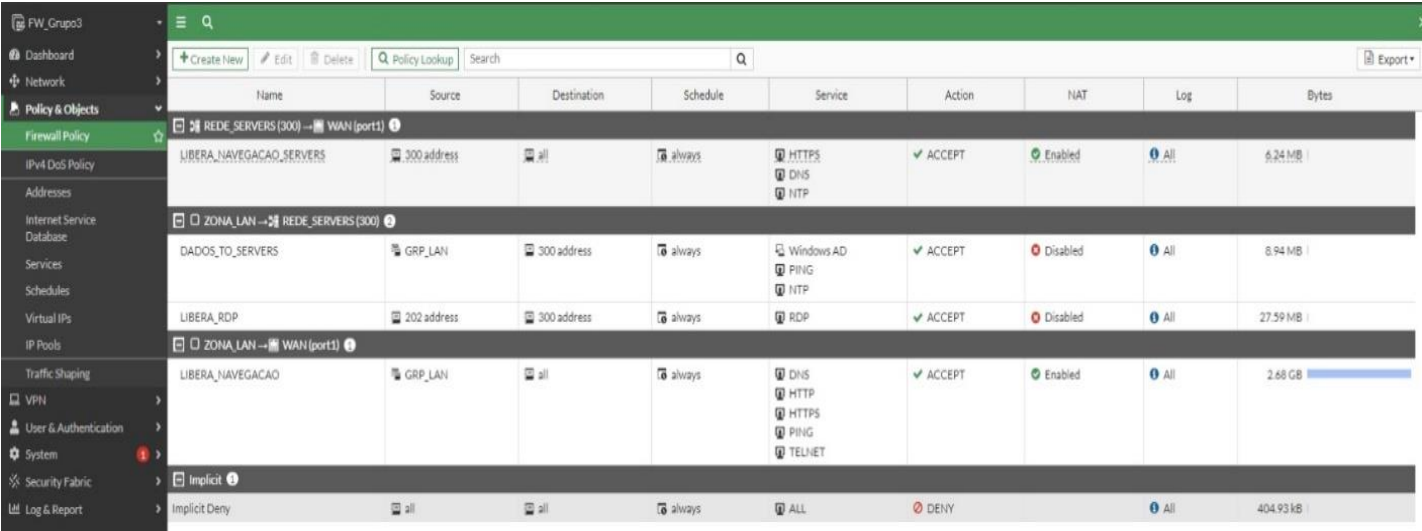
Por outro lado, as políticas de segurança englobam conjuntos de regras que estabelecem a maneira como os firewalls Fortinet devem proteger a rede. Isso inclui a implementação de políticas de autenticação, criptografia, prevenção de ameaças e outras diretrizes de segurança.

As regras de firewall constituem instruções específicas que determinam o tratamento do tráfego. Cada regra pode especificar o tipo de tráfego a ser permitido ou bloqueado, juntamente com os endereços de origem e destino, portas e protocolos correspondentes. Inicialmente, configuramos nossas políticas como um meio de aprofundar nosso conhecimento na ferramenta e entender o ambiente de forma abrangente.

O NAT é uma técnica usada para modificar endereços IP e portas de origem e destino de pacotes de rede, muitas vezes para permitir que dispositivos em uma rede

privada se comuniquem com dispositivos em uma rede pública, como a internet, de forma segura. A configuração do NAT é feita em cada política.

5.1.2. Políticas de Objetos

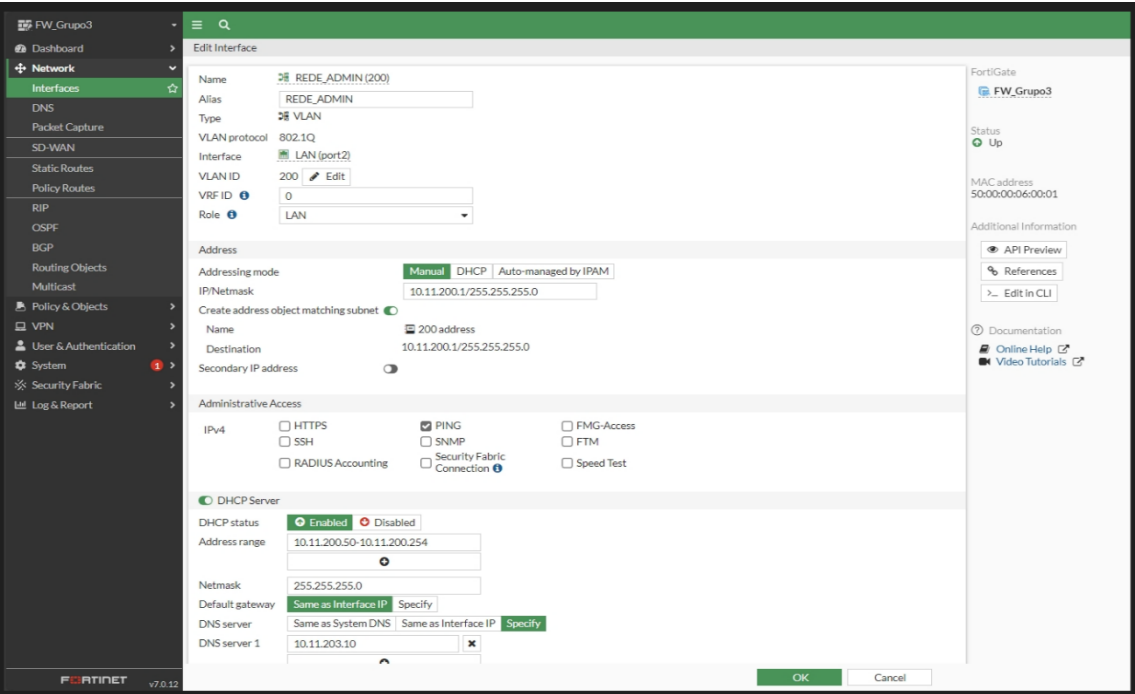


The screenshot shows the 'Policy & Objects' section in the FortiGate GUI. The 'Firewall Policy' tab is selected, displaying a table of configured policies. The table has columns for Name, Source, Destination, Schedule, Service, Action, NAT, Log, and Bytes. There are four policies listed: 1. 'REDE_SERVERS (300) -> WAN (port1)' with source 'LIBERA_NAVEGACAO_SERVERS', destination '300 address', schedule 'always', services 'HTTPS, DNS, HTTP', action 'ACCEPT', NAT 'Enabled', log 'All', and size '6.24 MB'. 2. 'ZONA_LAN -> REDE_SERVERS (300)' with source 'DADOS_TO_SERVERS', destination '300 address', schedule 'always', services 'Windows AD, PING, HTTP', action 'ACCEPT', NAT 'Disabled', log 'All', and size '8.94 MB'. 3. 'ZONA_LAN -> WAN (port1)' with source 'LIBERA_RDP', destination '300 address', schedule 'always', service 'RDP', action 'ACCEPT', NAT 'Disabled', log 'All', and size '27.59 MB'. 4. 'LIBERA_NAVEGACAO' with source 'GRP_LAN', destination 'all', schedule 'always', services 'DNS, HTTP, HTTPS, PING, TELNET', action 'ACCEPT', NAT 'Enabled', log 'All', and size '2.68 GB'. At the bottom, there is an 'Implicit Deny' policy with action 'DENY' and size '404.93 KB'.

Name	Source	Destination	Schedule	Service	Action	NAT	Log	Bytes
REDE_SERVERS (300) -> WAN (port1)	LIBERA_NAVEGACAO_SERVERS	300 address	always	HTTPS DNS HTTP	ACCEPT	Enabled	All	6.24 MB
ZONA_LAN -> REDE_SERVERS (300)	DADOS_TO_SERVERS	300 address	always	Windows AD PING HTTP	ACCEPT	Disabled	All	8.94 MB
ZONA_LAN -> WAN (port1)	LIBERA_RDP	300 address	always	RDP	ACCEPT	Disabled	All	27.59 MB
LIBERA_NAVEGACAO	GRP_LAN	all	always	DNS HTTP HTTPS PING TELNET	ACCEPT	Enabled	All	2.68 GB
Implicit Deny	all	all	always	ALL	DENY		All	404.93 KB

Figura7: Políticas e NAT (Network Address Translation): São estabelecidas políticas e configurações de roteamento.

5.1.3. Interface de Configuração



The screenshot shows the 'Edit Interface' configuration page for 'REDE_ADMIN (200)'. The interface is a VLAN type with protocol 802.1Q, connected to LAN (port2). The address is 10.11.200.1/255.255.255.0. The DHCP server is enabled with address range 10.11.200.50-10.11.200.254. Administrative access is configured for IPv4 with protocols PING, SSH, and SNMP. The DHCP status is 'Enabled'. The address range is '10.11.200.50-10.11.200.254'. The netmask is '255.255.255.0'. The default gateway is 'Same as Interface IP'. The DNS server is 'Same as System DNS'. The DNS server 1 is '10.11.203.10'. The interface is connected to 'FW_Grupo3' and has a status of 'Up'. The MAC address is '50:00:00:06:00:01'. There are links for 'API Preview', 'References', 'Edit in CLI', 'Documentation', 'Online Help', and 'Video Tutorials'.

Figura8: Configuração de interface

5.1.4. Stateful Inspection (Inspeção de Estado)

O Stateful Inspection é uma técnica usada pelos firewalls para monitorar o estado das conexões de rede e permitir ou bloquear pacotes com base no estado da conexão. Isso ajuda a proteger contra ameaças como ataques de negação de serviço (DoS).

Habilitado Stateful Inspection, para permitir a realização de inspeção de estado para acompanhar a situação das conexões e liberar apenas o tráfego legítimo associado a essas conexões.

5.1.5. Filtragem de Tráfego por Porta e Protocolo

Configuração de regras para permitir ou bloquear o tráfego com base nas portas de serviço e protocolos utilizados. Isso ajuda a controlar quais serviços podem ser acessados de dentro ou fora da rede.

Políticas de controle de acesso com base em endereços IP. Isso permite limitar quem pode se conectar à rede ou a determinados serviços.

5.1.6. VPN (Rede Virtual Privada)

O uso de VPNs é uma medida fundamental para garantir a segurança das comunicações de rede, especialmente quando se trata de conexões remotas. Com uma VPN, você pode estabelecer túneis criptografados entre dispositivos remotos e sua rede, garantindo que os dados transmitidos sejam seguros e confidenciais.

Convém certificar que sua VPN seja configurada com autenticação forte, como autenticação multifatorial (MFA), para proteger ainda mais o acesso à rede por meio da VPN.

Monitore e registre as conexões VPN para detectar atividades suspeitas e garantir que apenas dispositivos e usuários autorizados tenham acesso à sua rede interna por meio da VPN.

Implementado MFA para autenticação de usuários para garantir que apenas pessoas autorizadas tenham acesso à rede.

6. PENTEST: TESTE DE INTRUSÃO

Pentest, ou Teste de intrusão, em uma rede de computadores é uma atividade de segurança cibernética que envolve a avaliação proativa da segurança de um sistema de informações, em particular, de uma rede de computadores, simulando um ataque de um hacker mal-intencionado. O objetivo principal de um Pentest é identificar vulnerabilidades de segurança potenciais em um sistema de TI, incluindo sua rede, aplicativos e sistemas operacionais. É um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa.

Durante um Pentest, um especialista em segurança cibernética, conhecido como testador de penetração, tenta identificar e explorar com segurança quaisquer brechas de segurança que possam existir no sistema. Isso pode envolver tentativas de invasão de redes, obtenção de acesso não autorizado a sistemas, exploração de vulnerabilidades de software e hardware, entre outras técnicas.

O resultado de um Pentest é um relatório detalhado que descreve as vulnerabilidades descobertas, incluindo as formas como foram exploradas, juntamente com recomendações para mitigar ou corrigir essas vulnerabilidades. Essas recomendações são essenciais para fortalecer a segurança do sistema e proteger a rede contra possíveis ataques maliciosos.

É fundamental que as empresas adotem o teste de invasão como uma prática de segurança rotineira. Testar o sistema regularmente é a melhor maneira de prevenir e minimizar os danos que podem ser causados por acessos não autorizados.

À medida que as organizações buscam inovação e transformam seus negócios para estimular o crescimento e a vantagem competitiva, elas enfrentam o desafio de proteger identidades, dados e cargas de trabalho na nuvem híbrida.

6.1. Owasp Zap

É um scanner de segurança de aplicativos da Web de código aberto. Destina-se a ser usado tanto por iniciantes em segurança de aplicativos quanto por testadores de penetração profissionais. Tem sido um dos projetos mais ativos do Open Web Application Security Project.

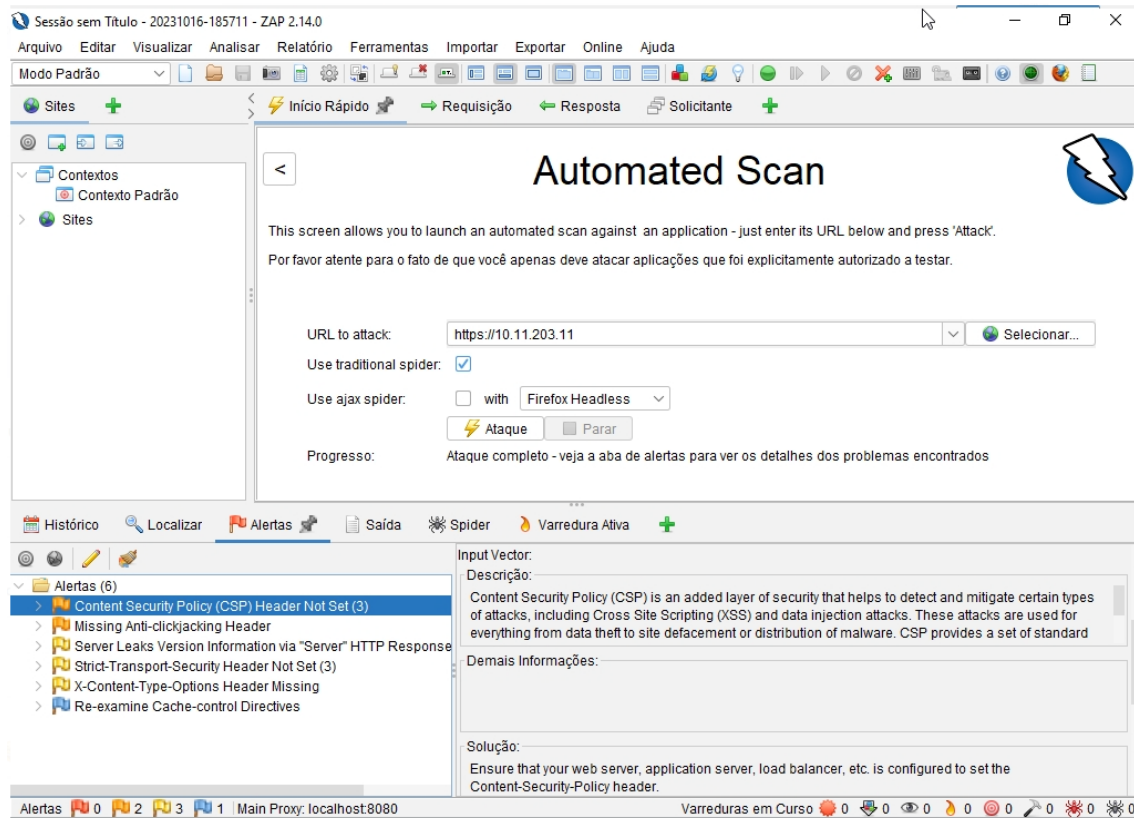


Figura09: Tela inicial OWASP – Configurações e Parâmetros

6.1.1. Report Pentest

Utilizamos como ferramenta de análise de vulnerabilidades WEB, o OWASP ZAP, auxiliando na detecção para correção de ameaças que podem infectar todo o ambiente de sistema web – Application Web

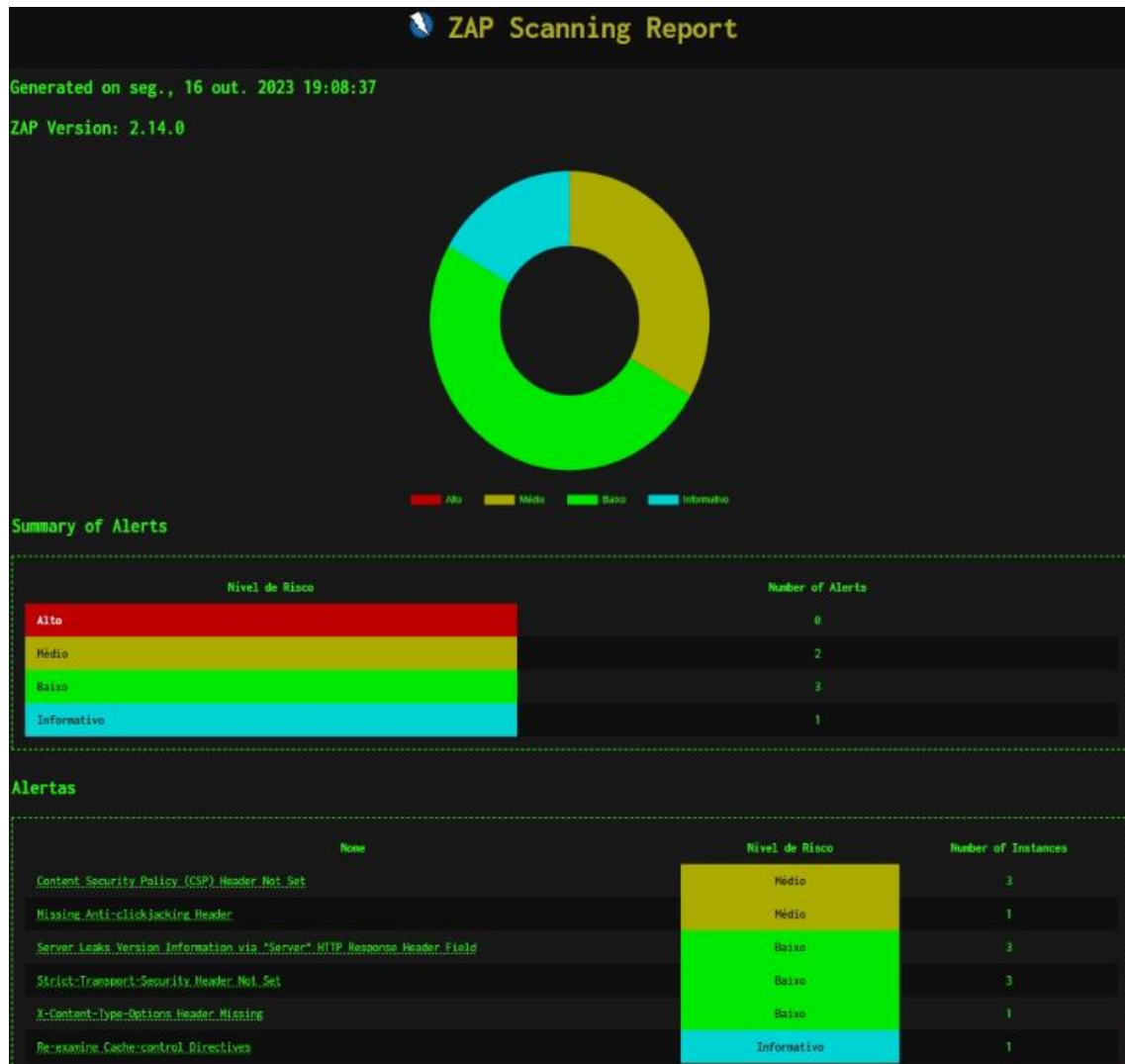


Figura10: Report de Pentest utilizando a ferramenta ZAP tendo como alvo nossa página web.

7. CERTIFICADO DIGITAL

O certificado digital é um documento eletrônico que garante a autenticidade de um site e a segurança das informações trocadas entre ele e o usuário. É um elemento essencial para qualquer site que coleta ou processa dados pessoais, como endereço de e-mail, senhas, números de cartão de crédito etc. O certificado digital criptografa as informações transmitidas entre o site e o usuário, tornando-as inacessíveis a terceiros. Isso protege os dados contra roubo, fraude e outros ataques cibernéticos.

Garante também que o site é legítimo e confiável. O usuário pode verificar a identidade do site através do cadeado de segurança que aparece na barra de endereços do navegador.

Além disso, os sites com certificado digital são mais bem avaliados pelos usuários e pelos buscadores, o que pode melhorar seu posicionamento nos resultados de busca.

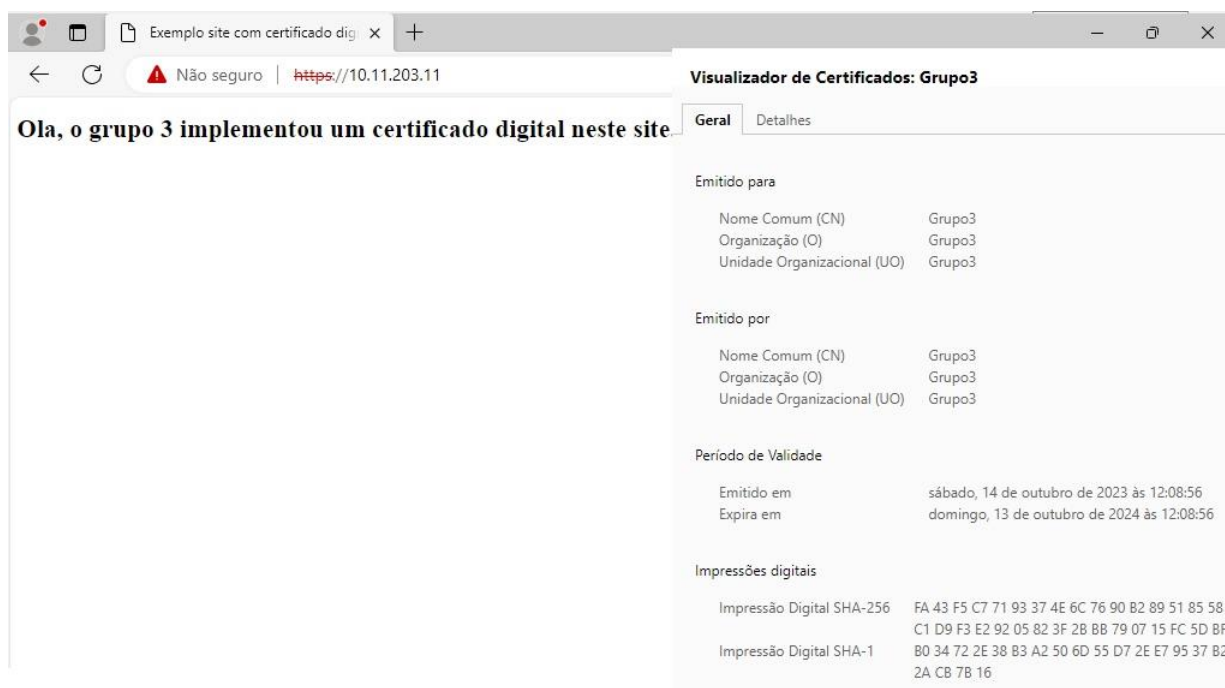


Figura11: Certificado Implementado para navegação em página web

8. TREINAMENTOS: PREPARAÇÃO DOS CLIENTES INTERNOS



Figura12: Treinamento de usuários. Definir diretivas para medidas de segurança dentro da infraestrutura.

A segurança cibernética é uma das medidas mais importantes a serem tomadas ao treinar funcionários novos ou atuais. A importância de formar continuamente os funcionários em segurança cibernética advém do rápido avanço da tecnologia na nossa era digital, o que significa que devem ser tomadas medidas adicionais para garantir que as nossas informações e conhecimentos estejam atualizados.

Proteger os ativos digitais e as informações da empresa está se tornando cada vez mais importante à medida que os funcionários fazem seu trabalho em laptops que eles podem tirar do escritório a qualquer momento. É necessário criarmos diferentes ferramentas de treinamento em cibersegurança que podem ajudar a educar todas as equipes sobre como evitar, detectar e responder a riscos cibernéticos.

Os usuários podem ser treinados para apagar anexos suspeitos de e-mail, evitar o uso de dispositivos USB desconhecidos, não acessar links recebidos de fora da organização, relatar possível perda de informações ao time de segurança.

A superfície de risco ainda está se expandindo, com milhares de novas vulnerabilidades sendo relatadas em aplicações e dispositivos antigos e novos. E as oportunidades de erro humano - especificamente por funcionários negligentes ou contratados que involuntariamente causam uma violação de dados - continuam aumentando.

A superfície de risco está em constante expansão, à medida que milhares de novas vulnerabilidades são relatadas em aplicações e dispositivos antigos e novos. Além disso, as oportunidades de erro humano, especialmente causadas por

funcionários negligentes ou contratados que inadvertidamente contribuem para violações de dados, estão em constante crescimento.

9. CONCLUSÃO

O projeto de construção do ambiente de rede, englobando servidores, switches e o Firewall Fortigate, reflete nosso compromisso inabalável com a segurança cibernética e a proteção da infraestrutura.

Com base na descrição do ambiente de rede e das medidas de segurança implementadas, fica evidente que a segurança da rede constitui a espinha dorsal de nossas operações. A integração de um Firewall Fortigate, equipado com recursos abrangentes de segurança, como antivírus, IPS, IDS e políticas de tráfego, reflete nosso compromisso em proteger dados e prevenir acessos não autorizados.

A utilização de um Active Directory (AD) e um servidor DNS contribui para a administração eficiente da rede e das identidades dos usuários, enquanto o servidor de arquivos (File Server) possibilita o compartilhamento seguro de dados no ambiente de rede. Adicionalmente, a segmentação de redes por meio de VLANs aprimora a eficiência e a segurança do tráfego de dados, reduzindo potenciais riscos decorrentes de acessos não autorizados.

Reconhecemos a importância de investir em treinamentos abrangentes para todos os colaboradores, a fim de garantir a conscientização sobre os riscos associados a dados sensíveis e a acessos não autorizados. Esses treinamentos se concentrarão não apenas em boas práticas de segurança cibernética, mas também em técnicas para identificar e lidar com possíveis ameaças, seja por meio da web (sites, e-mails) ou de dispositivos externos, como pendrives, discos rígidos externos e smartphones.

10. REFERÊNCIAS

<https://www.fortinet.com/br/resources/cyberglossary/firewall>

<https://pplware.sapo.pt/tutoriais/networking/fortigate-61f-primeiras-configuracoes-na-appliance-da-fortinet/>

<https://www.edapp.com/blog/pt-br/10-ferramentas-de-treinamento-em-cybersecurity/>

https://repositorio.utfpr.edu.br/jspui/bitstream/1/16765/4/PG_COADS_2016_1_01.pdf

LIMA, J. R. **Monitoramento de Redes..** Editora Brasport. 2014.

PROJETO DE REDES. **Gerenciamento de Redes de Computadores:** uma breve introdução. 2014.

Disponível em:

http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php

TELECO, Inteligência em Telecomunicações. **Gerenciamento e Monitoramento de Rede I:** Teoria de gerência de redes. 2014. Disponível em:

http://www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_3.asp

<https://www.stefaninirafael.com/?p=4278>

Guias de melhores práticas, como os fornecidos pelo Center for Internet Security (CIS) e pela National Cyber Security Centre (NCSC).

http://efaidnbmnnnibpcajpcgicfindmkaj/https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf