Proteção de Redes Corporativas contra Dispositivos não Autorizados em órgãos públicos

Gilvandson Costa Cavalcante[1], **Taiguara Indigina de Brasil**[2], **Hugo Barca Diniz Borges**[2], **Flavio Ferreira Lima**[3], **Éder Souza Gualberto**[1]

[1]Universidade de Brasília (UNB)
CEP: 70910-900 – Brasília – DF – Brazil

[2]Qintess Tecnologia e Participações Ltda, CEP: 01415-906 - Brazil
Durham, U.K.

[3]Departamento Nacional de Infraestrutura de Transporte - DNIT
CEP 70040-902, etor de Autarquias Norte, Quadra 3, Bloco A,
Edifício Núcleo dos Transportes – Brasília –DF

Abstract. *This paper presents the implementation of the IEEE 802.1X protocol as a network access control measure in public institutions. The main objective is to restrict the connection of unauthorized devices, mitigating risks such as the installation of illegitimate software, exposure of sensitive data, and compromise of network integrity. The proposed architecture includes certificate-based authentication, device segmentation via Group Policy Objects (GPO), and the use of MAC Allowlisting (MAB) for legacy equipment. The results demonstrate a significant improvement in access control and the feasibility of replicating the model on a national scale.*

Resumo. *Este artigo apresenta a implantação do protocolo IEEE 802.1X como medida de controle de acesso à rede em instituições públicas. O objetivo principal é restringir a conexão de dispositivos não autorizados, mitigando riscos como a instalação de softwares ilegítimos, exposição de dados sensíveis e comprometimento da integridade da rede. A arquitetura proposta inclui autenticação baseada em certificados digitais, segmentação de dispositivos via políticas de grupo (GPO), e uso de listas de permissões por MAC (MAB) para equipamentos legados. Os resultados demonstram aumento significativo no controle de acesso e possibilidade de replicação do modelo em escala nacional.*

Palavras Chaves: Protocolo 802.1x, GPOs, Active Directory, CRP, Supplicant, Client, DHCP.

1. Introdução

Os órgãos públicos brasileiros são responsáveis pela guarda e processamento de grandes volumes de dados classificados como sensíveis, incluindo informações pessoais, estratégicas e operacionais [CGU 2025]. A crescente digitalização dos serviços e o uso intensivo de recursos de tecnologia da informação tornaram esses ambientes alvos preferenciais de ameaças cibernéticas. Nesse cenário, torna-se imperativo adotar políticas de

segurança robustas, fundamentadas em padrões internacionais e práticas consolidadas de governança em segurança da informação [GSI/PR 2018].

Para garantir a proteção eficaz desses ativos, é necessário alcançar elevados níveis de maturidade em segurança cibernética. Isso envolve não apenas a aplicação de controles técnicos, mas também a promoção de uma cultura institucional de prevenção, monitoramento contínuo e resposta a incidentes. A mitigação proativa de vulnerabilidades — ou seja, antes que possam ser exploradas — é considerada uma estratégia essencial para reduzir a superfície de ataque e proteger os dados contra acessos indevidos, interceptações, vazamentos ou alterações não autorizadas.

Atualmente, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) lidera a condução de ações estruturantes voltadas ao fortalecimento da segurança digital no setor público federal. Entre as iniciativas em curso, destaca-se o Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria nº 852/2023 [MGI 2023], que estabelece diretrizes para o tratamento de informações e a proteção da infraestrutura crítica de tecnologia.

A partir dessas diretrizes, foi iniciado um projeto de fortalecimento da segurança da rede em um órgão público, com foco na limitação do acesso físico e lógico à rede local. O ponto de partida foi a análise de frameworks de segurança amplamente reconhecidos, como os publicados pelo National Institute of Standards and Technology (NIST), que fornecem diretrizes para a proteção de redes corporativas baseadas em autenticação, segmentação e controle de acesso [CISCO 2021].

Considerando a crescente sofisticação dos ataques cibernéticos e a possibilidade de uso de dispositivos não autorizados (como notebooks pessoais, dispositivos móveis, roteadores ou equipamentos sem gerenciamento de TI), este estudo propõe a adoção de mecanismos de segurança avançados que visam à mitigação de riscos específicos. Entre as soluções aplicadas, destaca-se a implementação do protocolo IEEE 802.1X como uma medida técnica eficaz de controle de acesso à rede, baseada na autenticação dos dispositivos e usuários conectados.

O IEEE 802.1X é um padrão internacional que define um mecanismo de autenticação para redes de computadores baseado em portas. Ele permite que apenas usuários ou dispositivos autenticados tenham acesso à rede, funcionando como um sistema de defesa perimetral no nível da camada de enlace (camada 2 do modelo OSI). Na prática, esse protocolo atua como um "porteiro digital", verificando as credenciais apresentadas antes de liberar ou negar o tráfego de dados entre o endpoint e a rede interna, seja por meio de conexões cabeadas (Ethernet) ou redes sem fio (Wi-Fi), conforme as definições da IEEE Standards Association IEEE [IEEE 2020b].

O escopo deste projeto compreende a infraestrutura de TI voltada à rede local com conexão cabeada (wired), onde o protocolo IEEE 802.1X foi implementado de forma progressiva. O principal objetivo é impedir que dispositivos não autorizados — sejam eles mal-intencionados ou apenas não homologados — consigam acessar recursos da rede institucional, como sistemas internos, servidores, bancos de dados ou impressoras corporativas.

Portanto, a adoção do protocolo IEEE 802.1X representa, portanto, um passo estratégico no amadurecimento da postura de segurança da informação em instituições

públicas [ZHANG 2022], contribuindo diretamente para a proteção dos dados, o cumprimento de regulamentações vigentes e a continuidade segura das operações governamentais.

2. Metodologia

A metodologia adotada para a implementação do protocolo IEEE 802.1X foi estruturada em três eixos principais, de modo a garantir a segurança, a padronização e a possibilidade de expansão do modelo para outros órgãos públicos. Cada etapa foi planejada e executada com atenção às especificidades do ambiente técnico e às normas de conformidade aplicáveis.

1. **Avaliação dos impactos operacionais:** Nesta etapa inicial, foi realizada uma análise criteriosa de compatibilidade entre os equipamentos de rede existentes (switches de acesso, roteadores, controladoras e pontos de acesso) e os requisitos do protocolo 802.1X. Essa análise prévia permitiu minimizar riscos de indisponibilidade e garantir uma adoção gradual e controlada da solução. Foram avaliados:

    - Necessidade de atualização de firmware em dispositivos de rede, de modo a garantir suporte nativo ao padrão IEEE 802.1X e às funcionalidades de autenticação avançada.

    - Identificação de limitações em dispositivos legados, como impressoras de rede, telefones IP e equipamentos industriais que não suportam autenticação 802.1X. Para esses casos, foi planejada a aplicação de mecanismos alternativos, como MAC Authentication Bypass (MAB).

    - Impacto nas rotinas operacionais: verificou-se a necessidade de ajustes em fluxos de trabalho de usuários e administradores, a fim de reduzir atritos durante a fase de transição.

    - Planos de contingência: foram estabelecidos mecanismos de fallback para situações em que a autenticação não fosse possível, assegurando a continuidade das atividades críticas.

2. **Arquitetura tecnológica implementada:** A arquitetura foi concebida para integrar de forma centralizada e automatizada os mecanismos de autenticação e autorização dos dispositivos conectados à rede. Os principais componentes e integrações foram:

    - Active Directory (AD): atuando como repositório central de identidades de usuários e dispositivos, garantindo consistência e governança na autenticação.

- Servidores RADIUS (NPS – Network Policy Server): responsáveis por intermediar as solicitações de autenticação enviadas pelos switches de acesso, validando credenciais e certificados no AD.

- Políticas de Grupo (GPOs): utilizadas para automatizar a configuração dos clientes Windows, aplicando regras de autenticação via 802.1X sem necessidade de intervenção manual do usuário.

- Certificados Digitais (PKI): empregados para autenticação segura via EAP-TLS, reduzindo riscos associados a senhas estáticas e fortalecendo a segurança contra ataques de interceptação.

- Switches de Acesso: configurados como authenticators, encaminhando solicitações para o servidor RADIUS e aplicando automaticamente as políticas de VLAN de acordo com o perfil do usuário/dispositivo [TANENBAUM 2011].

- Logs e Monitoramento: integrados ao sistema GrayLog, permitindo auditoria detalhada, rastreabilidade e geração de relatórios de conformidade.

3. **Potencial de replicação em escala nacional:** A metodologia adotada não se limitou ao atendimento local, mas foi planejada para servir como modelo de referência para outros órgãos públicos que compartilhem características semelhantes. Esse potencial de replicação contribui para elevar o nível de maturidade em segurança cibernética da Administração Pública como um todo, além de otimizar recursos, reduzir vulnerabilidades e reforçar a interoperabilidade entre sistemas governamentais.

    - Escalabilidade: a arquitetura modular permite expansão progressiva, seja para novas unidades administrativas ou para integração com redes sem fio (Wi-Fi).

    - Padronização: o uso de tecnologias amplamente difundidas (Active Directory, RADIUS, GPOs e PKI) facilita a adoção em diferentes cenários institucionais.

    - Conformidade: o modelo respeita legislações e normas aplicáveis, como a LGPD (Lei Geral de Proteção de Dados)[Planalto 2018], a ISO/IEC 27001 (gestão de segurança da informação) e as diretrizes do CIS Controls v8 [CIS 2023], garantindo alinhamento com práticas reconhecidas de cibersegurança.

    - Replicabilidade: a documentação produzida (procedimentos, fluxos, manuais de configuração) foi concebida de forma padronizada, possibilitando que outros órgãos utilizem o mesmo guia como base para implementação.

2.1. Avaliação dos impactos operacionais.

Com o objetivo de impedir o uso de equipamentos particulares não gerenciados pela área de Tecnologia da Informação (TI), adotou-se a estratégia de implementar um sistema de autenticação baseado em identificação de dispositivos em vez de autenticação por usuários. Essa abordagem reduz significativamente o risco de conexão de dispositivos não homologados à rede corporativa, reforçando a política de controle de acesso físico e lógico.

Considerando essa problemática, deu-se início à implantação da solução por meio da instalação e configuração do serviço Microsoft Network Policy Server (NPS) [NPS 2023], componente nativo do ecossistema Windows utilizado para prover serviços de autenticação, autorização e auditoria (AAA) via protocolo RADIUS [RIVEST 2025]. O serviço foi instalado em uma máquina virtual dedicada, hospedada em um servidor pertencente ao domínio corporativo, com Windows Server 2016 Standard Edition como sistema operacional base.

Durante o processo de configuração, foram adotadas medidas críticas de segurança para garantir a integridade e a proteção do ambiente NPS. Entre essas medidas, destaca-se a instalação de solução antivírus Bitdefender, reconhecida por sua eficácia na detecção de ameaças em tempo real. Adicionalmente, foram aplicadas políticas de segmentação de rede e restrição de portas por meio da plataforma pfSense, com o intuito de limitar o tráfego entre segmentos e evitar acessos indevidos à infraestrutura crítica.

A Tabela I a seguir apresenta os principais componentes da solução implementada com base no protocolo IEEE 802.1X, detalhando o papel de cada elemento na arquitetura de controle de acesso:

Para isso, foram estabelecidas duas abordagens técnicas:

1. Dispositivos integrantes do domínio, que recebem certificados digitais para autenticação automática.

2. Equipamentos incompatíveis com o domínio (como telefones VoIP, impressoras e outros): São incluídos em uma lista de bypass (MAB - MAC Authentication Bypass), permitindo acesso controlado sem integração ao Active Directory.

Table 1. Componentes utilizados na configuração do protocolo 802.1x

Nome da ferramenta	**Função no IEEE 802.1x**
Microsoft Net. Policy Server (NPS)	Servidor Radius responsável pela autenticação
Switches Gerenciáveis	Clientes RADIUS, controlam o acesso físico à rede
Supplicant	Dispositivos finais (endpoint) que solicitam acesso
Microsoft Active Directory	Diretório central de autenticação e identidade
Group Policy Object	Configuração automatizada dos dispositivos
DHCP	Atribuição dinâmica de endereços IP

Esta fase do projeto envolveu a configuração crítica para estabelecer comunicação segura entre os dispositivos suplicantes e o servidor RADIUS/NPS Microsoft, implementando dois conjuntos de políticas fundamentais:

1. Connection Request Policies (CRP) - Responsáveis pelo filtro inicial e roteamento das solicitações de autenticação; e

2. Network Policies - Definindo os parâmetros de autorização e condições de acesso para cada tipo de conexão.

Os suplicantes que receberam uma decisão de aprovação pela CRP, no item 1, devem, em seguida, ser avaliados conforme os critérios estabelecidos no item 2.

Nesse trabalho foi atribuido o nome ao CRP de ”CRP - Computer Certificate”, no qual será desmembrados em outras políticas:

1. **CRP - 00-15-65 - Telefones Philips**, para tratar as requisições dos suplicantes (telefone voip philips).

2. **CRP XX:XX:XX**, referente as requisições dos suplicantes (impressoras). A variável X representa os numeros de MAC que identificam o fabricante. Exemplo: MAC 00:1A:79:XX:XX:XX $\rightarrow$ OUI 00-1A-79 pertence à Google LLC.

2.2. Arquitetura tecnológica implementada.

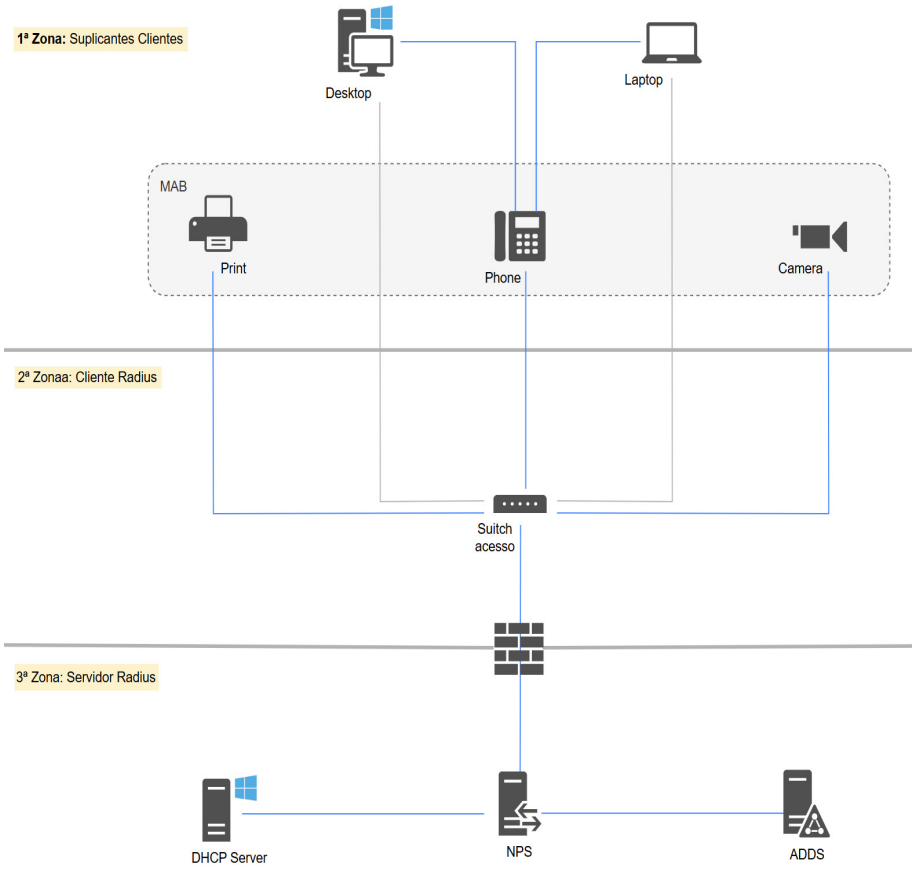

Figure 1. Representação esquemática da arquitetura 802.1X, destacando os elementos essenciais da infraestrutura de autenticação.

Na primeira camada de autenticação (1º zona), Figura 1, estão os suplicantes (supplicants) do serviço 802.1X, que realizam autenticação por meio de certificados digitais associados ao domínio corporativo. Dispositivos não gerenciados podem ser autorizados mediante inclusão em uma lista de acesso pré-configurada (whitelist).

A infraestrutura contempla dois cenários distintos de conexão:

1. Conexão direta via switch de camada 2 para dispositivos padrão.

2. Topologia com dispositivos IP phones atuando como gateways para terminais conectados em sua porta downstream.

Na segunda camada (Zona 2), implementou-se o protocolo 802.1X para autenticação baseada em porta, conforme detalhado na Figura 2. Esta configuração envolveu:

- Parametrização do Switch:
  - Habilitou-se o protocolo 802.1X com suporte a autenticação EAP (Extensible Authentication Protocol).
  - Configurou-se o redirecionamento de solicitações de autenticação para o servidor RADIUS [CISCO 2023].
  - Definiu-se políticas de controle de acesso baseadas nos resultados da autenticação.
- Integração com a Infraestrutura Existente:
  - Estabeleceu-se comunicação segura entre os switches e o servidor RADIUS utilizando o protocolo EAP.
  - Implementou-se certificados digitais para autenticação mútua nos casos que exigiam EAP-TLS.
  - Configurou-se fallback para métodos alternativos (como PEAP ou EAP-TTLS) quando aplicável.

O EAP (Extensible Authentication Protocol) atua como protocolo fundamental para a autenticação unificada entre os dispositivos em toda a infraestrutura do Parque Tecnológico IEEE8021X, permitindo :

- Autenticação centralizada de dispositivos.
- Controle granular de acesso à rede.
- Compatibilidade com múltiplos tipos de credenciais (certificados, credenciais MS-CHAP, etc.).

Na terceira camada (3ª zona), ilustrada na Figura 1, estão os elementos responsáveis pelos processos de autenticação e autorização. Dentre esses componentes, destaca-se o NPS (Network Policy Server), que atua como o principal validador e direcionador das requisições.

Os switches foram cadastrados como clientes RADIUS no NPS, utilizando criptografia e uma chave de autenticação compartilhada para assegurar a comunicação com o servidor e a segurança necessária para mitigar as vulnerabilidades [Natalia Olifer 2006].

Como parte da implementação do NPS, criou-se políticas de acesso segmentadas para diferentes tipos de dispositivos suplicantes: telefones IP, estações de trabalho (notebooks e desktops) e impressoras de rede. Para os dispositivos que não suportam autenticação via Política de Grupo (GPO), foi estabelecido um método alternativo de autorização baseado no endereço Media Access Control (MAC).

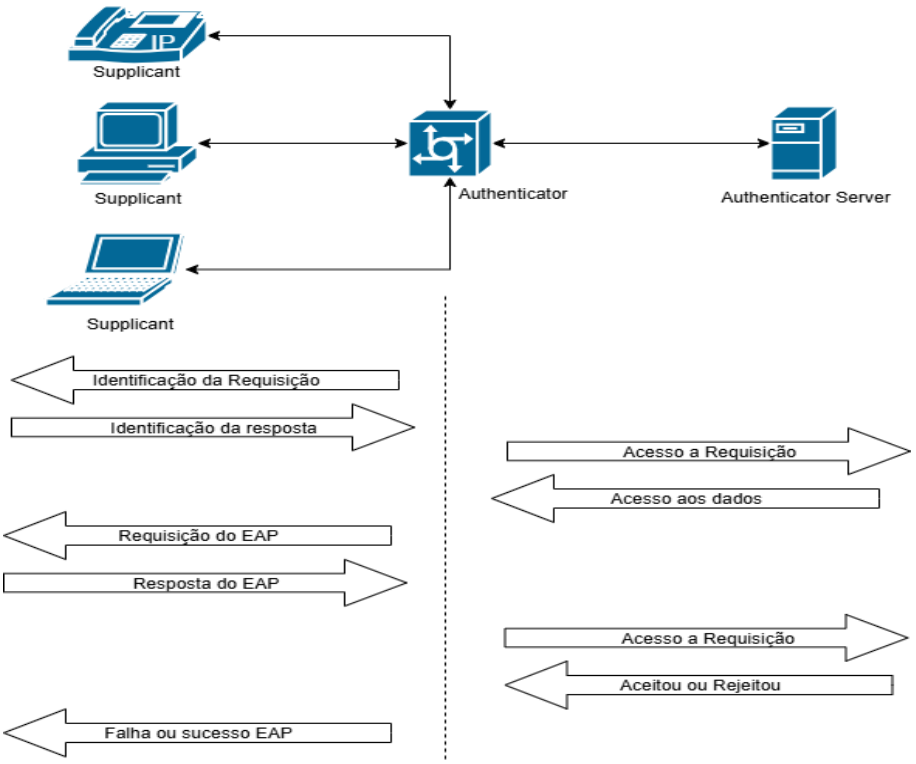

Figure 2. Exemplo do processo de comunicação utilizando o protocolo IEEE 802.1x, por meio do EAP.

As configurações da GPO (Group Policy Object) são aplicadas de forma centralizada e automatizada a todos os clientes (computadores membros do domínio).

Cada cliente possui um agente de software integrado que recebe e aplica os parâmetros de configuração via GPO. Esse processo é padrão em ambientes com Active Directory, onde as políticas são gerenciadas no controlador de domínio e distribuídas aos dispositivos vinculados.

A GPO "Wired 802.1X Supplicant" é uma política de grupo criada com o objetivo de automatizar e padronizar a configuração do cliente 802.1X em estações de trabalho que utilizam conexões cabeadas (Ethernet) no ambiente de domínio. Essa política é essencial para garantir que os dispositivos corporativos sejam autenticados de forma segura antes de obterem acesso à rede local (LAN). A política foi aplicada ao grupo "Domain Computers" e vinculada a diversas Unidades Organizacionais (OUs), como DF, GO, e TestesInfra, conforme mostrado na aba Scope, Figure 3. Isso garante que todos os computadores dessas unidades recebam as configurações automaticamente ao serem inicializados.

As principais definições configuradas na GPO foram:

- **Autenticação IEEE 802.1X ativada:** A política habilita o uso obrigatório de autenticação 802.1X nas interfaces de rede cabeada dos dispositivos.

- **Modo de autenticação:** Configurado para **"Computer only"**, o que significa que a autenticação ocorre no nível do dispositivo, antes do login do usuário.

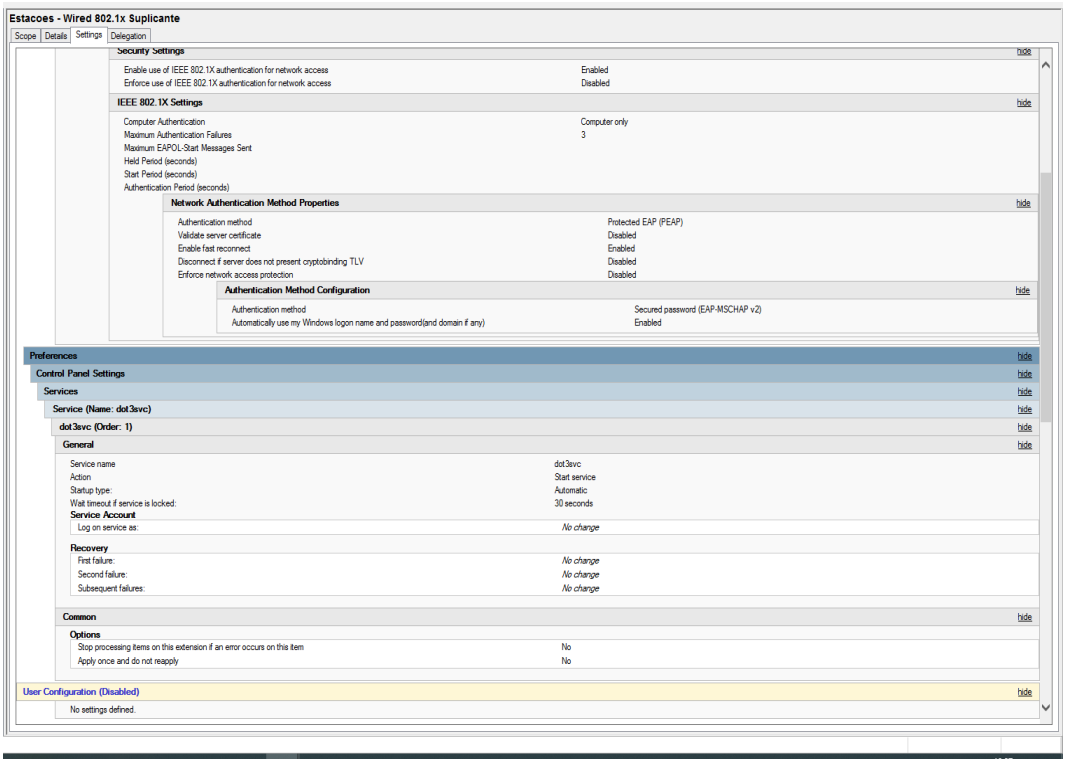

Figure 3. Nesta tela está sendo ilustrada como foi configurada as políticas de GPO aplicadas.

- **Método de autenticação:** Utiliza **PEAP (Protected EAP)** com senha segura EAP-MSCHAPv2, baseado nas credenciais do domínio.

- **Integração com Active Directory:** A opção **"Usar automaticamente meu nome de usuário e senha do Windows"** está habilitada, permitindo a autenticação transparente com as credenciais da conta de computador.

- **Serviço dot3svc:** É o serviço responsável por gerenciar a autenticação IEEE 802.1X nas interfaces Ethernet. A GPO garante que esse serviço seja iniciado automaticamente durante o boot.

A implementação desta GPO traz diversos benefícios:

- **Segurança aprimorada da rede:** Impede que dispositivos não autorizados acessem a rede, mesmo que fisicamente conectados ao switch.

- **Automação e padronização:** Evita configurações manuais em cada estação, garantindo consistência e reduzindo erros operacionais.

- **Conformidade com normas e auditorias:** Alinha-se às exigências de normas como ISO 27001, NIST, e CIS Controls, promovendo práticas de segurança

cibernética robustas.

- **Base para controle de acesso com NAC:** É um passo essencial para integrar a rede a sistemas de Network Access Control (NAC) [IEEE 2020a].

- **Redução da superfície de ataque:** Minimiza os vetores de intrusão por meio de conexões não autenticadas em portas de rede abertas.

2.3. Potencial de replicacão em escala nacional.

A metodologia utilizada no desenvolvimento do protocolo IEEE 802.1X apresenta um grande potencial de replicação em outras localidades, uma vez que já foi implementada com sucesso por diversos fabricantes de telefones e impressoras.

Além disso, a escalabilidade da solução é comprovada pela sua compatibilidade com dispositivos de diferentes fabricantes, o que reforça sua adaptabilidade a novos contextos.

Atualmente, o Ministério da Gestão e Inovação, por meio do Programa de Privacidade e Segurança da Informação, exige que as instituições adotem medidas para elevar o nível de maturidade em segurança cibernética. Nesse contexto, a implementação do protocolo IEEE 802.1X representa um avanço significativo na proteção dos dados e na infraestrutura de redes.

O protocolo atende às diretrizes governamentais e reduz vulnerabilidades em ambientes críticos.

3. Resultados e Discursões

A implantação do protocolo IEEE 802.1X demonstrou resultados significativos na elevação do nível de segurança da rede corporativa, trazendo maior controle, automação e rastreabilidade para os acessos realizados nos ambientes críticos da instituição. Essa seção detalha os principais impactos observados, correlacionando-os às figuras apresentadas e às boas práticas adotadas no projeto. A autenticação baseada em EAP-TLS, com uso de certificados digitais distribuídos por meio da infraestrutura de chaves públicas (PKI), garantiu um nível de segurança superior ao substituir credenciais estáticas (usuário/senha) por certificados criptograficamente validados. Esse modelo trouxe os seguintes ganhos:

- Eliminação da reutilização de credenciais: prevenindo o risco de compartilhamento indevido de senhas.

- Resiliência contra ataques de força bruta e phishing: certificados não podem ser explorados por simples tentativa de adivinhação.

- Autenticação transparente: usuários passaram a ter acesso sem necessidade de interações manuais, reduzindo falhas humanas e aumentando a produtividade.

Além disso, o controle de acesso granular via servidor RADIUS (NPS) permitiu a associação automática de cada dispositivo a VLANs específicas, criando uma camada adicional de isolamento entre diferentes perfis de uso. Com isso, estabeleceu-se um ambiente mais resiliente contra movimentação lateral em caso de comprometimento de dispositivos.

A Figura 4 detalha o fluxo de autenticação no modelo IEEE 802.1X, evidenciando a interação entre os três papéis centrais do processo:

- Supplicant (cliente): estação de trabalho ou dispositivo que solicita o acesso à rede. No log exibido, o cliente é identificado pelo nome de host e conta associada ao domínio Active Directory. Ele inicia o processo de autenticação utilizando EAP (Extensible Authentication Protocol) encapsulado sobre LAN.

- Authenticator (switch ou AP de acesso): atua como ponto de controle, recebendo a tentativa de conexão do cliente e encapsulando as mensagens EAP em pacotes RADIUS, que são então encaminhados ao servidor de autenticação. O log mostra o endereço do NAS (Network Access Server), incluindo IP, porta física e identificadores de sessão, que permitem rastrear a origem da requisição.

- Authentication Server (RADIUS/NPS): neste caso, o Microsoft Network Policy Server validou a autenticação. A política de requisição identificada foi a CRP – Computer Certificate, vinculada ao método PEAP (Protected EAP) com uso de EAP-MSCHAP v2. O servidor responsável pela autenticação, bem como o provedor utilizado (Windows), estão registrados no evento, reforçando a rastreabilidade do processo.

O diagrama lógico desse processo evidencia a sequência de troca de mensagens EAPOL (Extensible Authentication Protocol over LAN) entre cliente e autenticador, o encapsulamento RADIUS realizado pelo switch de acesso e a validação final junto ao Active Directory. Esse fluxo garante que, até a autenticação ser concluída, o cliente permanece em estado de restrição, sem acesso pleno à rede corporativa. Do ponto de vista prático, essa arquitetura atua como um verdadeiro “porteiro digital”, permitindo apenas a entrada de dispositivos devidamente validados por certificado ou credenciais corretas. Além de reforçar a segurança perimetral, o modelo reduz significativamente a superfície de ataque e a probabilidade de acessos não autorizados, assegurando que cada sessão de rede seja vinculada a uma identidade autenticada e auditável.

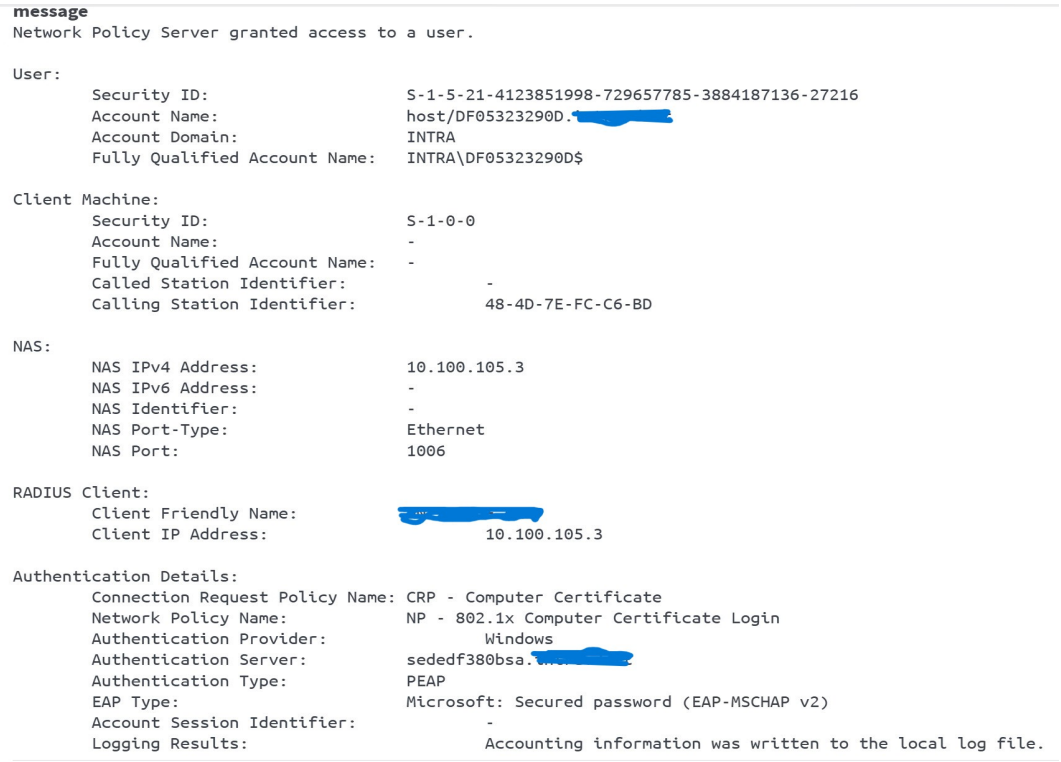

Figure 4. Estes são os logs retirados do sistema GrayLog. Nesse caso, o dispositivo foi autorizado a fazer parte da infraestrutura de rede.

A figura 5 ilustra a aplicação prática das VLANs dinâmicas como parte integrante da solução baseada no protocolo IEEE 802.1X. Esse recurso trouxe avanços significativos em termos de segurança, automação e governança da rede, permitindo que a segmentação lógica fosse atribuída de maneira automática, com base no perfil do usuário ou dispositivo autenticado.

No modelo tradicional, a associação de dispositivos a VLANs específicas dependia de configurações manuais em portas de switch, o que gerava um processo trabalhoso, sujeito a erros e de difícil escalabilidade. Com a integração entre o servidor RADIUS (NPS), o Active Directory e os switches de acesso, tornou-se possível automatizar essa tarefa, de forma centralizada e consistente. O funcionamento das VLANs dinâmicas está diretamente vinculado ao processo de autenticação do protocolo IEEE 802.1X e ao uso do servidor RADIUS como elemento central de decisão. Diferentemente do modelo estático, onde cada porta do switch é configurada manualmente com uma VLAN específica, o método dinâmico possibilita que a definição da VLAN seja feita em tempo real, conforme o perfil do dispositivo ou usuário que solicita acesso. Isso garante maior flexibilidade e automação no gerenciamento da rede, reduzindo erros humanos e aumentando a segurança.

- Quando o dispositivo (supplicant) solicita acesso à rede, inicia-se o processo de autenticação via 802.1X.

- O switch de acesso (authenticator) encaminha a solicitação ao servidor RADIUS.

- O RADIUS, após validar o usuário/dispositivo junto ao Active Directory, aplica as políticas de autenticação previamente configuradas.

- A resposta enviada ao switch contém não apenas a autorização de acesso, mas também a atribuição automática da VLAN.

- O dispositivo é então conectado ao segmento de rede apropriado, sem a necessidade de intervenção manual.

Neste contexto, considerando os cenários de aplicação prática, a ação de VLANs dinâmicas pode ser observada em diferentes situações operacionais que exigem segregação lógica da rede. Cada perfil de usuário ou tipo de dispositivo pode ser alocado em uma VLAN específica, garantindo que apenas os recursos necessários fiquem disponíveis. Esse modelo oferece flexibilidade para lidar com ambientes heterogêneos, onde coexistem equipamentos modernos, dispositivos legados e acessos temporários.

- Usuários corporativos autenticados: alocados em VLANs de produção, com acesso integral aos serviços internos.

- Dispositivos IoT e impressoras: isolados em VLANs específicas, com restrição de comunicação lateral e acesso apenas ao que for indispensável.

- Usuários visitantes: encaminhados para VLANs de acesso restrito, normalmente limitadas à internet.

- Dispositivos em quarentena: equipamentos que falharam na autenticação ou apresentam comportamento suspeito são movidos para VLANs de contenção, sujeitas a monitoramento e validação.

Portanto, a utilização de VLANs dinâmicas proporciona uma série de benefícios tangíveis para a gestão de redes corporativas. Além de aumentar o nível de segurança, essa abordagem reduz significativamente o esforço operacional, garantindo que a segmentação de rede acompanhe a evolução das políticas de segurança da instituição. O resultado é uma rede mais confiável, flexível e alinhada às boas práticas de governança em segurança da informação.

- Segurança reforçada: dispositivos e usuários são isolados em segmentos específicos, limitando a superfície de ataque.

- Escalabilidade: políticas centralizadas no RADIUS permitem expansão sem necessidade de reconfiguração manual em cada switch.

- Eficiência operacional: automação do processo de alocação de VLAN reduz falhas humanas e tempo de provisionamento.

- Flexibilidade: regras podem ser adaptadas em tempo real com base em critérios como horário, tipo de dispositivo ou perfil de usuário.

Figure 5. Estes são os logs retirados do sistema GrayLog. Nesse caso, o dispositivo não foi autorizado.

A figura 6 apresenta a arquitetura de monitoramento via GrayLog, que centraliza e correlaciona todos os registros de autenticação, falhas e tentativas de acesso não autorizado. Esse componente desempenhou papel essencial na detecção de anomalias, análise de tendências e conformidade regulatória. Nessa figura, é possivel identificar um evento de falha de autenticação gerado pelo Network Policy Server (NPS) com ID 6273. Esse log ocorre quando um usuário ou dispositivo tenta se autenticar na rede, mas não atende aos critérios definidos na política de segurança. O funcionamento do sistema de monitoramento baseia-se na coleta, correlação e análise centralizada de eventos oriundos de diferentes componentes da rede, como switches de acesso, servidores RADIUS e Active Directory. Os dados coletados incluem tanto logs de autenticação bem-sucedida quanto tentativas falhas e acessos não autorizados.

O GrayLog organiza essas informações em painéis interativos (dashboards), permitindo análises em tempo real e geração de relatórios detalhados. Além disso, é possível configurar alertas automatizados, que notificam a equipe técnica em caso de eventos críticos, como excesso de falhas de login ou detecção de dispositivos não cadastrados. A centralização dos registros trouxe ganhos expressivos em diferentes situações práticas. A análise em tempo real permitiu identificar comportamentos suspeitos, como múltiplas tentativas de login em um curto intervalo de tempo, o que pode indicar um ataque de força bruta. Da mesma forma, o monitoramento contínuo possibilitou verificar se determinados dispositivos estavam se conectando em horários incomuns, reforçando a detecção de acessos anômalos[ISO/IEC 2022].

Além disso, os relatórios periódicos gerados a partir dos dados coletados serviram

como subsídio para auditorias internas e externas, atendendo exigências normativas e garantindo a rastreabilidade das ações de autenticação e acesso.

Por fim, o uso do GrayLog como ferramenta de monitoramento centralizado trouxe benefícios que extrapolam o aspecto técnico, alcançando também a governança e a conformidade institucional. A visibilidade ampliada da rede proporcionou maior confiança para a tomada de decisões e fortaleceu a postura de segurança da organização, explorando os seguites aspectos:

- Visibilidade completa: rastreamento em tempo real de todos os eventos de autenticação.
- Detecção proativa de incidentes: alertas automáticos para tentativas suspeitas de acesso.
- Rastreabilidade: registros históricos detalhados para suporte a auditorias e investigações.
- Agilidade operacional: dashboards intuitivos que permitem respostas rápidas da equipe técnica.
- Governança e conformidade: alinhamento às melhores práticas de segurança e atendimento às normas regulatórias.

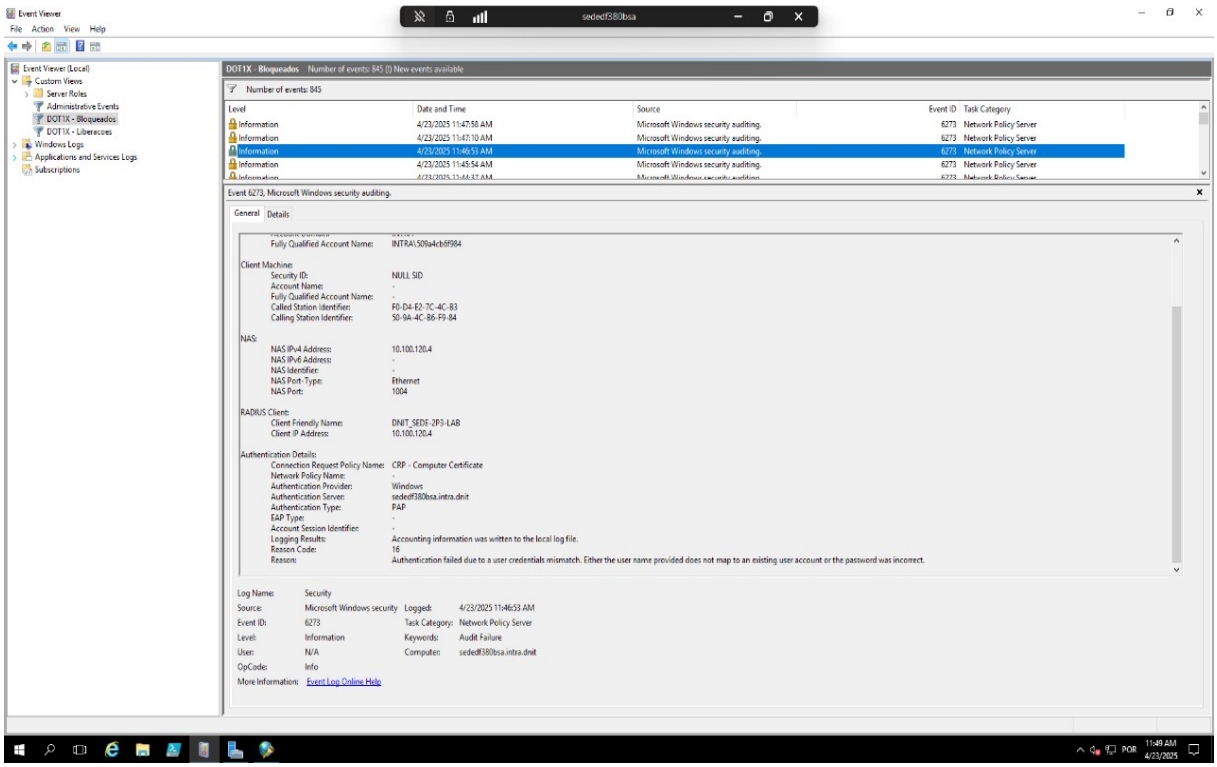

Figure 6. A tela do Radius apresenta informações referentes ao bloqueio de um dispositivos.

4. Conclusões e trabalhos futuros

A adoção do protocolo IEEE 802.1X na infraestrutura de rede institucional, representou um marco na evolução da postura de segurança da informação, estabelecendo um sistema abrangente de controle de acesso baseado em identidade digital. Esta solução foi cuidadosamente planejada para atender a quatro pilares fundamentais: Excelência Técnica, Arquitetura Escalável, Conformidade Regulatória e Eficiência Operacional Mensurável.

Esta iniciativa não apenas elevou os padrões de segurança, mas também serviu como alicerce para a transformação digital da instituição, garantindo proteção robusta dos ativos de informação enquanto possibilita inovação tecnológica segura.

Os resultados oriundos da implentação do protocolo IEEE 802.1x, mostram que o nível de maturidade em segurança da informação, aumentou bastante, uma vez que, software como Graylog e o próprio Radius, analisam as tantativas de entrada de um dispositivo que não faz parte do dominio tranzendo informações para facilitar a rastreabilidade. Este fato, mitiga muito a possibilidade de notebook ou computadores com softwares não licenciados, acessarem a rede de computadores da instituição.

Próximos passos:

1. Atualmente, a infraestrutura de Wi-Fi apresenta algumas vulnerabilidades significativa, permitindo que dispositivos não cadastrados no Active Directory acessem a rede indiscriminadamente. Esta brecha de segurança expõe a organização a riscos como: a) Acesso não autorizado a recursos da rede; b) Possíveis violações de dados sensíveis; c) Comprometimento da performance da rede; e d)Dificuldade de auditoria e conformidade.

2. A implementação de uma solução de Network Access Control (NAC) é essencial para garantir que apenas dispositivos autorizados e em conformidade com as políticas de segurança tenham acesso à rede. Nesse sentido, em casos que exigem cooperação com órgãos de segurança pública, a implementação de mecanismos robustos de investigação digital, quando acionados por solicitação formal da Polícia Federal, proporcionaria significativos avanços na capacidade de rastreabilidade.
3. Expandir a implementação do protocolo abordado nesse artigo, para as demais unidades adminstrativas da instituíção.

References

CGU (2025). Guia de segurança da informação e proteção de dados na administração pública. https://www.gov.br/cgu/pt-br, Acesso em: 16 ago. 2025.

CIS (2023). enter for internet security, cis controls v8: Implementation group 1 (ig1). https://www.cisecurity.org/controls/cis-controls-list, Acessado em 2023.

CISCO (2021). Aborda impactos operacionais, vantagens de segurança e desafios na implantação em redes corporativas (802.1x). In *Secure Network Access Control*. Cisco White Paper.

CISCO (2023). Radius configuration guide. cisco systems. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html, Acesso em: 16 ago. 2025.

GSI/PR (2018). In nº 04/2018 do gabinete de segurança institucional (gsi/pr). diretrizes para a política de segurança da informação nos Órgãos federais. https://www.gov.br/gsi/pt-br, Acesso em: 16 ago. 2025, Acesso em: 16 ago. 2025.

IEEE (2020a). Ieee standard, "802.1x-2020 - port-based network access control". https://standards.ieee.org/standard/$802_1X - 2020.html, Acessadoem16/09/2024.$

IEEE, S. A. (2020b). Ieee standard for port-based network access control (ieee std 802.1x-2020). https://standards.ieee.org.

ISO/IEC (2022). *iso/iec 27001:2022 — information security management systems — requirements*. https://www.iso.org/standard/82875.html.

MGI (2023). *Portaria n.º 852, de 28 de março de 2023*. Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI, ed. 62, seção 1, pt. 92 edition.

Natalia Olifer, V. O. (2006). Computer networks: Principles, technologies and protocols for network design. page 1008. Wiley.

NPS, N. P. S. (2023). Microsoft learn. https://learn.microsoft.com/pt-br/windows-server/networking/technologies/nps/nps-top, Acessado em 12/05/2024,.

Planalto (2018). Lei nº 13.709, de 14 de agosto de 2018 (lei geral de proteção de dados pessoais - lgpd). http://www.planalto.gov.br/ccivil$_03/_ato2015 - 2018/2018/lei/l13709.htm, Acessadoem20/08/2024.$

RIVEST, R. e. a. (2025). Rfc 2865: Remote authentication dial-in user service (radius). internet engineering task force (ietf). https://tools.ietf.org/html/rfc2865, Acessado em 16/09/2024.

TANENBAUM, A. S. (2011). Wetherall, d. computer networks. In Pearson, editor, *5º ed.* https://www.gov.br/gsi/pt-br, Acesso em: 16 ago. 2025, Acesso em: 16 ago. 2025.

ZHANG, Y.; CHEN, J. (2022). Impacts of 802.1x on enterprise network security: A case study. In v. 15, n. ., editor, *Journal of Network Security*, pages 45–60. https://standards.ieee.org.