**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS ESCOLA POLITÉCNICA E DE ARTES**

**GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO**

****

**SEGURANÇA E GESTÃO DE REDES CORPORATIVAS COM FOCO NA PLATAFORMA BLUEPEX**

**JOÃO PEDRO ARANTES RIBEIRO**

GOIÂNIA 2025

**JOÃO PEDRO ARANTES RIBEIRO**

**SEGURANÇA E GESTÃO DE REDES CORPORATIVAS COM FOCO NA PLATAFORMA BLUEPEX**

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Engenharia da Computação

Orientador (a):

Prof. Me. Rafael Leal Martins Banca examinadora:

Prof. Me. Fernando Gonçalves Abadia Prof. ?????????

GOIÂNIA 2025

**SEGURANÇA E GESTÃO DE REDES CORPORATIVAS COM FOCO NA PLATAFORMA BLUEPEX**

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia da Computação, em: / / .

Orientador (a): Prof. Me. Rafael Leal Martins

Prof. Me. Fernando Gonçalves Abadia

Prof. ???????????????????

GOIÂNIA 2025

Dedico este trabalho para todas as amizades que construí no tempo que estive na universidade, aos meus avós e principalmente aos meus pais por todo apoio e carinho em todos os momentos da minha vida.

**AGRADECIMENTOS**

Agradeço a Deus e minha família minha mãe Andiara Arantes Silva Ribeiro, meu pai Sergio Chaves Ribeiro, minhas avós Amanda Aparecida Arantes Silva e Lourdes Chaves Ribeiro e ao meu avô Antônio Justiniano Ribeiro, por sempre me apoiarem e incentivar a conquistar meus objetivos.

Um agradecimento especial ao meu orientador Rafael Leal Martins, por todo apoio e paciência para a realização deste trabalho.

E a todos os professores que contribuíram de alguma forma para este trabalho.

**RESUMO**

Este trabalho analisa a criticidade da segurança e da gestão de redes corporativas diante do avanço da transformação digital e do aumento da sofisticação de ameaças cibernéticas, com foco na plataforma BluePex como solução integrada. A pesquisa combina uma abordagem qualitativa, por meio de revisão bibliográfica fundamentada em autores como Tanenbaum, Kurose e Stallings, e análise prática, explorando as funcionalidades da BluePex, uma ferramenta brasileira voltada para pequenas e médias empresas. São detalhados os quatro pilares da plataforma – segurança, controle, disponibilidade e conformidade – que sustentam suas soluções, incluindo Firewall UTM/NGFW, proteção e controle de endpoints, backup em nuvem, segurança avançada de e-mails e proteção de websites. Esses recursos são projetados para mitigar ameaças como ataques de negação de serviço (DoS), ransomware, phishing, injeção de SQL e acessos não autorizados, conforme orientações da Cartilha de Segurança para Internet.

Um estudo de caso fictício, centrado na Empresa X, uma organização do setor imobiliário com 20 funcionários, ilustra a aplicação prática do BluePex 1500. A rede da empresa, composta por dois links de internet (ALGAR 300 Mbps e TIM 1 Gbps), servidores físicos e virtuais, e dispositivos cabeados e sem fio, foi configurada com regras de firewall para segmentação de tráfego, serviços de DHCP para atribuição dinâmica de IPs, DNS (incluindo DNS Dinâmico), NTP para sincronização de tempo e VPN com túneis IPsec e OpenVPN, garantindo acesso remoto seguro. A implementação abordou desafios como gestão de ameaças, controle de acessos e otimização de conectividade, reforçando a proteção de dados sensíveis e a continuidade operacional.

A análise comparativa entre BluePex, Splunk e SonicWall destaca a simplicidade e o custo acessível da BluePex, ideal para empresas de menor porte, frente à escalabilidade do Splunk, voltada para grandes corporações, e ao equilíbrio custo-benefício da SonicWall. Aspectos legais e normativos, como a conformidade com a Lei Geral de Proteção de Dados (LGPD) e as normas ISO/IEC 27001 e 27002, são enfatizados, evidenciando a capacidade da BluePex em atender exigências regulatórias por meio de controles de acesso, criptografia e monitoramento contínuo. A pesquisa conclui que a BluePex oferece uma solução robusta, acessível e alinhada às necessidades de segurança cibernética, promovendo a proteção de redes corporativas e a confiança no ambiente digital, com potencial para futuras explorações em cenários mais complexos.

**Palavras-chave**: Segurança cibernética, gestão de redes, BluePex, Firewall, IP, VPN

**SUMÁRIO**

1. [INTRODUÇÃO 9](#_TOC_250045)
   1. [Objetivos 9](#_TOC_250044)
   2. [Justificativa 9](#_TOC_250043)
   3. [Metodologia 9](#_TOC_250042)
2. [REFERENCIAL TEÓRICO 10](#_TOC_250041)
   1. [Fundamentos de Redes 10](#_TOC_250040)
   2. [Gerência de Redes 11](#_TOC_250039)
   3. [Gerência de Segurança 13](#_TOC_250038)
   4. [Ferramenta Específica 14](#_TOC_250037)
      1. [BluePex 14](#_TOC_250036)
      2. [Os 4 Pilares da BluePex 15](#_TOC_250035)
      3. [Soluções da BluePex 16](#_TOC_250034)
      4. [Ameaças 18](#_TOC_250033)
3. [ANÁLISE DA FERRAMENTA E DE ALTERNATIVAS 20](#_TOC_250032)
   1. [BluePex 20](#_TOC_250031)
   2. [Splunk 20](#_TOC_250030)
   3. [SonicWall 20](#_TOC_250029)
   4. [Tabela de Comparação 21](#_TOC_250028)
4. [ASPECTOS LEGAIS E NORMATIVOS 21](#_TOC_250027)
   1. [LGPD (Lei Geral de Proteção de Dados) 21](#_TOC_250026)
   2. [ISO/IEC 27001 22](#_TOC_250025)
   3. [ISO/IEC 27002 22](#_TOC_250024)
5. [ESTUDO DE CASO 23](#_TOC_250023)
   1. [Sobre a Empresa 23](#_TOC_250022)
   2. [Infraestrutura de Rede 24](#_TOC_250021)
      1. [Conectividade com a Internet 24](#_TOC_250020)
      2. [Firewall e Segurança (BluePex 1500) 24](#_TOC_250019)
      3. [Rede Cabeada e Wireless 24](#_TOC_250018)
      4. [Servidores e Virtualização 24](#_TOC_250017)
      5. [Armazenamento e Backup 25](#_TOC_250016)
   3. [Considerações sobre a Rede 25](#_TOC_250015)
   4. [BluePex na Rede 27](#_TOC_250014)
      1. [Regras de Firewall 27](#_TOC_250013)
      2. [Servidor DHCP 37](#_TOC_250012)
         1. [Servidor DHCP LAN 38](#_TOC_250011)
         2. [Servidor DHCP WAN\_TIM\_1GBPS 38](#_TOC_250010)
         3. [Servidor DHCP VLAN 38](#_TOC_250009)
   5. [Serviços de DNS 39](#_TOC_250008)
      1. [DNS Dinâmico 39](#_TOC_250007)
   6. [Serviço NTP 40](#_TOC_250006)
   7. [Web Filter 40](#_TOC_250005)
   8. [VPN. 41](#_TOC_250004)
      1. [Túnel IPsec Configurado 41](#_TOC_250003)
      2. [Configuração VPN. 42](#_TOC_250002)
6. [CONCLUSÃO 47](#_TOC_250001)
7. [REFERÊNCIAS 48](#_TOC_250000)

# INTRODUÇÃO

A crescente digitalização de processos e a interconexão de sistemas têm transformado as redes corporativas em elementos estratégicos para empresas de todos os portes. No entanto, esse avanço tecnológico também ampliou o cenário de ameaças cibernéticas, tornando indispensável uma abordagem robusta para a gerência de redes e segurança da informação. Este trabalho de conclusão de curso apresenta uma análise detalhada sobre a aplicação de práticas de gerência de rede, com foco na segurança, e explora as vantagens do uso da plataforma BluePex como solução integrada para proteção e gestão de redes corporativas.

## Objetivos

O principal objetivo deste trabalho é demonstrar a importância de uma boa gerência de rede, com ênfase na implementação de ferramentas de segurança como firewalls, para garantir a integridade, disponibilidade e confidencialidade das informações. Especificamente, o trabalho busca:

* Analisar os desafios enfrentados por redes corporativas no contexto atual.
* Explorar os recursos e benefícios proporcionados pela plataforma BluePex.
* Evidenciar como ferramentas de segurança podem mitigar vulnerabilidades e prevenir incidentes cibernéticos.

## Justificativa

A segurança de redes corporativas é um tema de relevância crescente, dada a frequência e a sofisticação de ataques cibernéticos. Uma boa gerência de rede não apenas protege ativos digitais, mas também garante a continuidade dos negócios, reduzindo riscos e custos associados a falhas e violações de segurança. Este trabalho visa reforçar o entendimento da importância da segurança da informação no ambiente corporativo e destacar a utilidade prática de ferramentas como firewalls no contexto da defesa cibernética.

## Metodologia

A metodologia adotada neste trabalho consiste em uma abordagem qualitativa, combinando revisão bibliográfica e análise prática da ferramenta BluePex. Inicialmente, são explorados os fundamentos de redes e segurança por meio de um levantamento teórico com base em publicações acadêmicas e documentos técnicos. Em seguida, é realizada uma análise detalhada das funcionalidades da BluePex, incluindo estudos de caso e comparação com outras soluções do mercado. O trabalho também incorpora a análise de cenários hipotéticos para demonstrar a aplicação prática das ferramentas de gerência de redes.

Este estudo contribui para a conscientização sobre a relevância da segurança cibernética e oferece um guia prático para profissionais que desejam implementar soluções eficazes em redes corporativas.

# REFERENCIAL TEÓRICO

## Fundamentos de Redes

As redes de computadores estão no coração da comunicação digital que usamos diariamente. Elas permitem que dispositivos, como computadores, smartphones e servidores, estejam conectados e troquem informações de maneira eficiente. Seja compartilhando arquivos, rodando aplicativos ou viabilizando chamadas de vídeo, as redes tornam essas interações possíveis. Como bem define Tanenbaum (2010), uma rede de computadores nada mais é do que "um sistema de interconexão de dispositivos que compartilham recursos e trocam dados". E para que tudo isso funcione, é essencial compreender os pilares que sustentam o universo das redes: topologias, protocolos e modelos de referência.

Um desses pilares, a topologia, trata de como os dispositivos estão organizados dentro de uma rede. Imagine uma sala cheia de amigos conversando: alguns preferem falar diretamente com todos (topologia em estrela), enquanto outros falam com quem está ao lado e deixam as mensagens circularem (topologia em malha). Essa organização é crucial, pois define a eficiência, escalabilidade e até a velocidade com que as informações chegam ao destino. Comer (2014) reforça que uma topologia bem planejada pode simplificar o gerenciamento e minimizar problemas, especialmente em redes mais comPexas.

Outro ponto-chave no funcionamento das redes é o uso de modelos de referência, como o famoso modelo OSI e a pilha TCP/IP. Esses modelos funcionam como guias para entender como os dados são enviados e recebidos entre dispositivos. Pense no modelo OSI como uma receita bem estruturada, com sete camadas, onde cada etapa tem sua função, desde o preparo dos ingredientes (camada física) até a finalização do prato (aplicação). Já o TCP/IP, usado amplamente na Internet, simplifica algumas etapas, mas continua sendo essencial para conectar redes ao redor do mundo (FOROUZAN, 2012).

Não podemos esquecer dos protocolos de comunicação, que são como as regras de uma conversa. Eles garantem que mesmo dispositivos de diferentes "línguas" consigam se entender. O TCP/IP, por exemplo, é um dos mais usados, sendo responsável por organizar os dados, definir os endereços e garantir que tudo chegue ao destino certo. Minoli (2002) destaca que a robustez desses protocolos é indispensável para manter a confiabilidade, mesmo em redes que misturam diversos dispositivos e tecnologias.

Entender tudo isso – topologias, modelos de referência e protocolos – é mais do que apenas um exercício técnico. É a base que permite criar redes eficientes, seguras e confiáveis, adaptadas às necessidades de cada situação. Comer (2014) ressalta que esse conhecimento é essencial para projetar redes que atendam demandas específicas, otimizando recursos e garantindo a segurança das informações. No fim das contas, entender redes é entender como as conexões que usamos no dia a dia são possíveis.

## Gerência de Redes

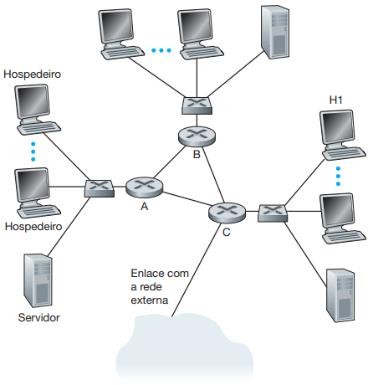
As redes de computadores desempenham um papel essencial no mundo moderno, conectando dispositivos, sistemas e pessoas em uma ampla variedade de ambientes. Desde pequenas redes domésticas até grandes infraestruturas corporativas, as redes permitem a comunicação, o compartilhamento de recursos e o acesso a informações de forma eficiente e segura. No nível mais básico, uma rede de computadores pode ser definida como "um conjunto de dispositivos interligados, que utilizam protocolos específicos para trocarem informações entre si" (TANENBAUM, 2010), sejam esses dispositivos computadores, servidores, smartphones ou qualquer outro equipamento habilitado para comunicação digital. Essa definição é complementada por Forouzan (2012), que enfatiza que as redes viabilizam a troca de informações e a utilização compartilhada de recursos, independentemente da localização física dos dispositivos.

A comPexidade e a importância das redes de computadores aumentam proporcionalmente ao seu tamanho e ao volume de dados que trafegam por elas. A interligação de diferentes sub- redes e dispositivos exige uma administração eficiente para garantir o desempenho, a segurança e a disponibilidade. É nesse contexto que a Gerência de Redes se torna fundamental, uma vez que "ela é responsável por monitorar, controlar e otimizar a rede, assegurando que tudo funcione conforme o esperado" (STALLINGS, 2014), minimizando falhas e garantindo a continuidade dos serviços. Segundo Minoli (2002), a gestão de redes eficaz é indispensável para que organizações alcancem alta disponibilidade e resiliência em um ambiente cada vez mais conectado.

A Gerência de Redes é composta por várias funções, entre elas a gerência de configuração, falhas, desempenho, segurança e contabilização. Cada uma dessas áreas atua em conjunto para manter o funcionamento ideal de toda a rede, oferecendo visibilidade e controle detalhado sobre o comportamento dos dispositivos e o fluxo de dados. Segundo Kurose e Ross (2016), "a gerência de falhas busca identificar, isolar e corrigir problemas antes que eles afetem os usuários, enquanto a gerência de segurança se concentra em proteger a rede contra acessos não autorizados e ataques maliciosos". Além disso, Forouzan (2012) destaca que a gerência de configuração é essencial para documentar e manter atualizadas todas as alterações na rede, prevenindo conflitos entre dispositivos.

Outro aspecto relevante da Gerência de Redes é o papel da gerência de desempenho, que busca garantir que os recursos da rede sejam utilizados de maneira eficiente e que os tempos de resposta estejam dentro dos parâmetros aceitáveis. Isso inclui a análise de métricas como latência, largura de banda e taxa de perda de pacotes, além do monitoramento contínuo para identificar possíveis gargalos ou quedas de desempenho. Segundo Stallings (2014), a identificação precoce de problemas de desempenho permite que ajustes proativos sejam feitos, como a redistribuição de carga ou o aumento da capacidade de links, garantindo assim que a rede atenda às necessidades dos usuários finais de maneira consistente.

Figura 1 – Cenário simples que ilustra a utilização do gerenciamento de rede



Fonte: Redes de Computadores, Jim Kurose, pág.557

A Figura 1, retirada do livro de Jim Kurose e Keith Ross, oferece um exemplo claro de uma rede simples composta por roteadores, hospedeiros e servidores. Embora pareça uma infraestrutura básica, esse cenário ilustra bem como as ferramentas de gerenciamento de redes são essenciais, mesmo em redes menores. Como mencionado no trecho, "mesmo para uma rede tão simples, há muitos cenários em que o administrador muito se beneficiará por ter à mão as ferramentas de gerenciamento adequadas" (KUROSE; ROSS, 2013). Essa gestão eficiente torna-se fundamental para garantir o funcionamento ininterrupto da rede e para prevenir problemas antes que se tornem críticos.

A primeira questão abordada é a detecção de falhas em interfaces, seja em hospedeiros ou roteadores. No exemplo da rede da Figura 1, caso uma interface do roteador A apresente falhas, como aumento de erros de soma de verificação em quadros, o administrador poderá ser alertado por ferramentas de gerenciamento antes que a falha impacte os usuários. Como destacado no trecho do livro, "um administrador de rede que monitora e analisa de maneira ativa o tráfego pode realmente impressionar o usuário [...] detectando problemas na interface bem antes" (KUROSE; ROSS, 2013). Essa proatividade reduz o tempo de inatividade da rede, mantendo a eficiência. Segundo Comer (2014), a capacidade de monitorar proativamente os componentes da rede permite identificar gargalos e otimizar o fluxo de dados.

Outro ponto importante citado por Kurose e Ross (2013) é a monitoração de tráfego e sua utilidade para o oferecimento de recursos. O administrador pode monitorar padrões de tráfego entre diferentes segmentos da rede, como os roteadores A, B e C mostrados na figura. Ao detectar congestionamentos, ele pode optar por reconfigurar a rede ou até mesmo sugerir upgrades de infraestrutura, como o aumento da largura de banda do enlace com a rede externa, o que poderia evitar sobrecargas e melhorar o desempenho sem a necessidade de grandes investimentos iniciais.

Além disso, a gerência de redes também atua na detecção de mudanças rápidas nas tabelas de roteamento, que podem indicar instabilidades ou má configuração. No cenário da Figura 1, se houver mudanças constantes nas rotas dos roteadores, o administrador será alertado e poderá corrigir o problema antes que ele cause uma falha maior. Como explicado no livro, "a alternância de rotas pode indicar instabilidades no roteamento ou um roteador mal configurado" (KUROSE; ROSS, 2013). Forouzan (2012) acrescenta que o uso de ferramentas automatizadas

de monitoramento ajuda a reduzir significativamente o tempo de resposta a essas mudanças, garantindo maior estabilidade para a rede.

Portanto, mesmo em um cenário simples como o ilustrado, o gerenciamento de redes é indispensável para garantir a estabilidade, segurança e eficiência do ambiente. Com ferramentas de monitoramento adequadas, os administradores podem prevenir falhas, otimizar o desempenho e garantir que os Acordos de Nível de Serviço (SLAs) sejam atendidos, assegurando a satisfação dos usuários e a continuidade dos serviços de rede.

## Gerência de Segurança

A gerência de segurança em redes de computadores é um dos pilares fundamentais para garantir a proteção dos dados e a integridade das comunicações entre dispositivos. Em um ambiente cada vez mais interconectado, as redes estão sujeitas a diversos tipos de ameaças, desde ataques maliciosos, como invasões e espionagem, até erros humanos e falhas de hardware. Portanto, a segurança de redes não pode ser tratada como um aspecto secundário, mas sim como uma parte integral da gestão de TI. A gerência de segurança tem como objetivo proteger a rede contra acessos não autorizados, detectar atividades suspeitas e garantir a confidencialidade, integridade e disponibilidade dos dados que trafegam pela rede.

Um dos principais aspectos da gerência de segurança é a autenticação e o controle de acesso. Esses mecanismos garantem que apenas usuários e dispositivos autorizados possam acessar determinados recursos da rede. Ferramentas como firewalls, sistemas de controle de acesso (ACLs) e autenticação multifator (MFA) são amplamente utilizadas para verificar a identidade de quem está tentando acessar a rede e determinar quais permissões eles têm. O controle de acesso é vital para evitar que informações sensíveis sejam acessadas por indivíduos não autorizados, além de mitigar o risco de ataques internos.

Outro componente crucial da gerência de segurança é a detecção e resposta a incidentes. Com o aumento dos ataques cibernéticos, é essencial que a rede seja monitorada constantemente em busca de sinais de atividades suspeitas. Sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS) desempenham um papel importante nesse aspecto, ao analisar o tráfego de rede em tempo real e identificar padrões de comportamento que possam indicar uma violação de segurança. Uma resposta rápida a esses incidentes é fundamental para minimizar os danos e restaurar a segurança o mais rápido possível.

A criptografia também faz parte da gerência de segurança, sendo uma das ferramentas mais eficazes para garantir a confidencialidade dos dados transmitidos. Tanto em redes locais quanto em redes públicas, como a Internet, a criptografia assegura que apenas as partes autorizadas possam decifrar e acessar as informações trocadas. Isso é particularmente importante em comunicações sensíveis, como transações financeiras e transferências de dados pessoais. Segundo Stallings, "a criptografia é um componente chave para assegurar a confidencialidade dos dados em trânsito e, quando combinada com outras técnicas de segurança, oferece uma camada robusta de proteção contra ameaças" (STALLINGS, 2014).

A gerência de segurança, portanto, engloba uma série de práticas e ferramentas que visam proteger os recursos da rede de ameaças internas e externas. Autenticação, controle de acesso, detecção de intrusões e criptografia são apenas algumas das técnicas utilizadas para garantir que a rede permaneça segura e operando de forma eficiente. Nos próximos parágrafos, discutiremos como essas técnicas podem ser implementadas de forma integrada para criar uma infraestrutura de segurança robusta, alinhada com as necessidades e particularidades de cada ambiente de rede.

## Ferramenta Específica

Neste trabalho, vamos explorar a ferramenta BluePex, destacando suas principais funcionalidades e aplicações. A BluePex tem se mostrado eficaz em (especificar o campo ou função, como segurança, análise de dados etc.), oferecendo uma interface intuitiva e recursos avançados que facilitam o trabalho dos usuários e otimizam processos. Nossa análise busca mostrar como essa ferramenta se diferencia no mercado, quais benefícios traz em cenários específicos e como atende às necessidades atuais do setor.

## BluePex

A BluePex é uma empresa dedicada à cibersegurança, com soluções desenvolvidas para proteger dispositivos de maneira proativa. Suas tecnologias estão centralizadas em uma plataforma intuitiva, facilitando a gestão integrada de Firewall/UTM, proteção e controle de endpoints, backup em nuvem, além de segurança para e-mails e websites.

Figura 2 – Logo da BluePex

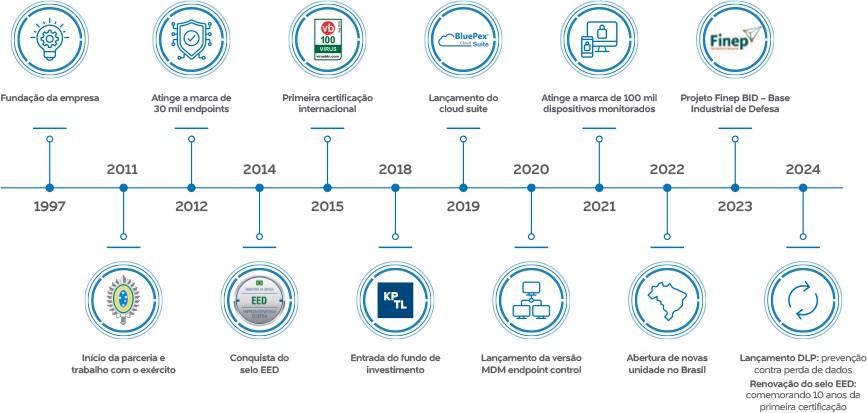


Fonte: Google Search

Com mais de 20 anos de atuação, a BluePex protege diariamente uma ampla base de dispositivos e, desde 2016, é reconhecida por sua qualidade com o selo internacional VB-

100. No Brasil, é reconhecida como Empresa Estratégica de Defesa pelo Ministério da Defesa, destacando-se também como uma das pioneiras em pesquisa antimalware no país.

Figura 3 – Linha cronológica da BluePex



Fonte: Site oficial da BluePex

A empresa oferece ainda suporte técnico 24 horas por dia em português e realiza monitoramento contínuo dos riscos, reforçando seu compromisso com a segurança de seus clientes.

## Os 4 pilares da BluePex

A segurança das redes corporativas é fundamental para que uma empresa funcione de forma eficiente e resiliente, especialmente diante do aumento de ameaças cibernéticas. A BluePex organiza sua estratégia de proteção em quatro pilares principais, que juntos visam proteger dados, gerenciar acessos, garantir que os sistemas estejam sempre disponíveis e assegurar que a empresa esteja em conformidade com as leis. Esses pilares, que vão além da simples implementação de ferramentas, ajudam a criar um ambiente tecnológico mais seguro e confiável.

1. Segurança: Esse primeiro pilar é voltado à defesa ativa contra ameaças externas e internas. A ideia é que a empresa esteja sempre protegida contra vírus, ataques e invasões, por meio de práticas como instalação de antivírus atualizado, firewalls bem configurados e backups frequentes e confiáveis. Essas medidas são a base para manter a integridade dos dados e a segurança geral da rede.
2. Controle: No pilar de controle, o foco é administrar e monitorar o uso dos recursos da rede, garantindo que tudo esteja de acordo com as políticas da empresa. Isso envolve o controle de acesso à internet, restrição de sites perigosos, bloqueio de acessos indevidos e monitoramento constante de estações de trabalho e servidores. Além disso, o controle rigoroso sobre os e-mails recebidos ajuda a evitar riscos de

phishing e outras ameaças. Esse pilar é essencial para manter a rede em ordem e reduzir vulnerabilidades.

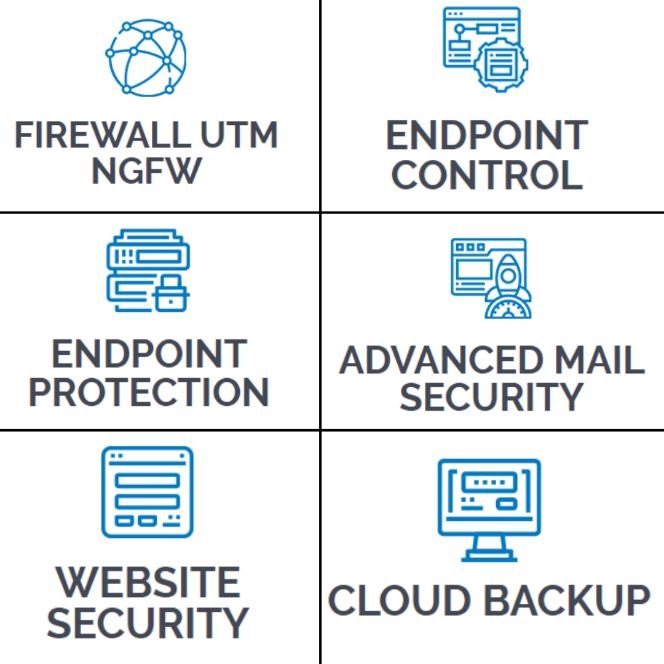
1. Disponibilidade: Garantir que os sistemas estejam sempre disponíveis e funcionando é essencial para que a empresa não enfrente paradas que possam prejudicar suas operações. Esse pilar se refere a assegurar que a internet, os servidores e as estações de trabalho operem sem interrupções e com bom desempenho. Isso inclui não só resolver problemas rapidamente, mas também prevenir falhas através de monitoramento constante e manutenção preventiva.
2. Conformidade: O pilar de conformidade garante que a empresa atue em conformidade com leis e regulamentações, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD). A conformidade não é apenas uma exigência legal, mas também uma forma de construir uma relação de confiança com os clientes e parceiros, ao demonstrar que a empresa cuida e respeita os dados de todos os envolvidos.

Esses pilares – segurança, controle, disponibilidade e conformidade – formam a base da abordagem da BluePex para criar uma rede segura, gerenciável e em conformidade com as regulamentações, fortalecendo a continuidade dos negócios e a confiança no ambiente digital da empresa.

## Soluções da BluePex

A BluePex oferece um portfólio robusto de soluções tecnológicas voltadas para a segurança e o gerenciamento de redes corporativas, atendendo às necessidades de empresas que buscam proteger seus dados e operações de forma eficiente. Com o avanço das ameaças digitais, é indispensável contar com ferramentas que atuem de maneira integrada, prevenindo e mitigando riscos. Nesse contexto, as soluções da BluePex destacam-se por sua capacidade de atender desde a proteção de dispositivos individuais até a segurança de sistemas completos na nuvem, proporcionando confiabilidade e desempenho às organizações.

Figura 4 – Exemplos de soluções ofertados pela BluePex



Fonte: Elaborado pelo autor, imagens retiradas da página web da BluePex

A seguir, apresentamos uma visão detalhada sobre cada solução oferecida pela BluePex e seus benefícios:

1. **Firewall UTM/NGFW**: O Firewall UTM (Unified Threat Management) e NGFW (Next Generation Firewall) são soluções avançadas de segurança que oferecem proteção abrangente contra ameaças à rede. Além de filtrar o tráfego, essas ferramentas integram funcionalidades como controle de aplicativos, prevenção contra invasões, proteção contra malware e gerenciamento unificado, garantindo que a rede corporativa esteja protegida contra-ataques comPexos e direcionados.
2. **Endpoint Control**: Essa solução oferece o gerenciamento centralizado dos dispositivos conectados à rede, como computadores e notebooks, permitindo monitorar e controlar as configurações de segurança, acesso a recursos e o comportamento dos endpoints. É uma ferramenta essencial para prevenir violações de dados e proteger dispositivos contra-ataques cibernéticos.
3. **Endpoint Protection EDR**: O Endpoint Detection and Response (EDR) é uma solução avançada que combina proteção de endpoints com capacidade de detecção, investigação e resposta a incidentes. Ela analisa continuamente o comportamento dos dispositivos para identificar ameaças avançadas e responder de forma rápida e automatizada a ataques.
4. **Cloud Backup**: Essa solução permite o armazenamento seguro de dados na nuvem, garantindo que informações importantes estejam protegidas contra perda, corrupção ou ataques. Com backup automático e recuperação fácil, as empresas podem assegurar a continuidade dos negócios mesmo em caso de falhas ou desastres.
5. **Advanced Mail Security**: Essa ferramenta protege os sistemas de e-mail contra ameaças como phishing, spam, malware e ataques de engenharia social. Com tecnologias avançadas de filtragem e análise, ela garante que apenas mensagens seguras cheguem às caixas de entrada dos usuários, reduzindo significativamente os riscos para a empresa.
6. **Segurança para Websites**: Essa solução é projetada para proteger websites corporativos contra-ataques, como injeção de SQL, ataques DDoS e exploração de vulnerabilidades. Com monitoramento contínuo e medidas de mitigação, garante que os sites permaneçam acessíveis, confiáveis e seguros para os usuários.
7. **Gerenciamento por Territórios**: Ferramenta voltada para empresas com múltiplas localizações geográficas, permitindo a centralização do gerenciamento de recursos de TI e políticas de segurança. Essa abordagem simplifica a administração e garante que todas as unidades sigam os mesmos padrões de proteção.
8. **Cloud Suite**: Um conjunto de soluções integradas na nuvem que oferecem segurança, produtividade e gerenciamento centralizado para empresas. Essa suite pode incluir desde ferramentas de colaboração até recursos de proteção de dados, tudo em um único ambiente seguro e eficiente.

Dessa forma, as soluções da BluePex abordam uma ampla gama de necessidades, garantindo uma rede mais segura e eficiente. A seguir, será apresentada uma análise dos tipos de ataques que cada uma dessas ferramentas busca prevenir e combater, evidenciando como a integração dessas tecnologias pode mitigar os principais riscos enfrentados pelas empresas atualmente.

## Ameaças

As soluções da BluePex têm como objetivo proteger as empresas contra diversas ameaças cibernéticas que podem comprometer a segurança, a privacidade e a continuidade das operações. A seguir, explicamos cada uma dessas ameaças e como as soluções podem ajudar a preveni-las, com base nas diretrizes da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>):

1. **Ataques de negação de serviço (DoS):** Esses ataques sobrecarregam sistemas e redes com tráfego excessivo, tornando-os indisponíveis para usuários legítimos. Soluções como o **Firewall UTM/NGFW** atuam filtrando e bloqueando o tráfego malicioso, garantindo a continuidade do serviço.
2. **Tentativas de intrusão e acesso não autorizado**: Esses ataques têm como objetivo explorar vulnerabilidades na rede para obter acesso indevido a sistemas ou dados. O Firewall UTM/NGFW impede essas tentativas, monitorando e restringindo acessos não autorizados.
3. **Códigos maliciosos (vírus, trojans e worms)**: Esses programas são projetados para infectar dispositivos, roubar informações ou causar danos. O **Endpoint Control** e o **Endpoint Protection EDR** monitoram e bloqueiam a execução desses códigos, garantindo a integridade dos dispositivos conectados.
4. **Ransomware**: Trata-se de um tipo de malware que criptografa os dados da vítima, exigindo um pagamento para desbloqueá-los. Soluções como o **Cloud Backup** são essenciais para recuperar informações sem a necessidade de atender às demandas dos criminosos.
5. **Phishing e spam**: O phishing é uma prática em que atacantes enganam usuários para obter dados confidenciais, como senhas e informações bancárias, geralmente por meio de e-mails falsos. Já o spam dissemina mensagens indesejadas, muitas vezes contendo links maliciosos. O **Advanced Mail Security** protege contra essas ameaças ao filtrar mensagens suspeitas.
6. **Ataques a websites (injeção de SQL e cross-site scripting - XSS)**: A injeção de SQL ocorre quando um invasor insere comandos maliciosos em formulários ou URLs para manipular bancos de dados. Já o XSS é uma técnica que injeta scripts maliciosos em páginas web, afetando usuários que acessam o site. A **Segurança para Websites** identifica e bloqueia essas vulnerabilidades, protegendo o ambiente digital.
7. **Inconsistências em múltiplas redes**: Em empresas com várias localizações geográficas, falhas no gerenciamento de redes podem criar pontos de entrada para atacantes. O **Gerenciamento por Territórios** centraliza e padroniza a segurança, evitando brechas que possam ser exploradas.
8. **Sequestro de contas e acesso não autorizado a dados na nuvem**: Essas ameaças envolvem o comprometimento de credenciais ou a exploração de falhas em sistemas na nuvem. A **Cloud Suite** garante a proteção dos dados corporativos armazenados remotamente, utilizando controles de acesso e criptografia.

Compreender essas ameaças é fundamental para que as empresas adotem medidas preventivas eficazes. No próximo tópico, será abordado como essas ameaças impactam os negócios e a importância de uma estratégia integrada de segurança cibernética para mitigar esses riscos.

# ANÁLISE DA FERRAMENTA E DE ALTERNATIVAS

Quando falamos em segurança de redes, escolher a ferramenta certa é essencial para proteger dados e garantir que tudo funcione sem interrupções. Para ajudar nessa escolha, comparamos três soluções: BluePex, Splunk e SonicWall. Cada uma atende a diferentes tipos de empresas, dependendo do tamanho, orçamento e necessidade de proteção.

## BluePex

A BluePex é uma ferramenta brasileira desenvolvida para empresas de pequeno e médio porte. Ela tem o objetivo de simplificar a gestão de segurança, oferecendo uma solução "tudo em um". Isso inclui proteção contra vírus, controle de acessos, backups na nuvem e suporte técnico em português, disponível 24 horas por dia.

Pontos fortes:

* Fácil de usar, mesmo para equipes de TI com experiência moderada.
* Suporte técnico próximo e em português.
* Excelente integração de várias funcionalidades em uma única plataforma. Desafios:
* Pode ser cara para empresas pequenas.
* Foca mais na proteção básica e integração do que em análises avançadas.

## Splunk

O Splunk é uma solução poderosa para empresas grandes que lidam com um alto volume de dados e precisam de análises profundas para detectar ameaças. Ele é como um "detetive digital", que coleta e analisa todos os dados de uma rede para encontrar problemas antes que eles virem crises.

Pontos fortes:

* Extremamente escalável, ideal para grandes empresas.
* Tecnologia de ponta para prever e prevenir ataques.
* Permite criar relatórios personalizados e detalhados. Desafios:
* É muito caro, tanto para adquirir quanto para manter.
* Requer profissionais experientes para usá-lo bem.
* O suporte técnico está disponível apenas em inglês.

## SonicWall

A SonicWall é conhecida por seus firewalls de última geração, combinando proteção robusta contra ataques e facilidade de gerenciamento. É ideal para empresas que precisam proteger redes comPexas, mas com um custo razoável.

Pontos fortes:

* Bom custo-benefício, especialmente para empresas de médio porte.
* Proteção avançada contra ataques como ransomware e exploits.
* Suporte técnico disponível em português. Desafios:
* Algumas funções mais avançadas exigem licenças adicionais.
* Requer um nível intermediário de conhecimento técnico para configuração e otimização.

## Tabela de Comparação

|  |  |  |  |
| --- | --- | --- | --- |
| Cenário | BluePex | Splunk | SonicWall |
| Facilidade de uso | Alta | Média | Média |
| Funcionalidade | Ampla | Avançada | Ampla |
| Adequação ao LGPD | Alta | Média | Alta |
| Custo | Moderado para baixo | Muito Alto | Moderado |
| Proteção avançada | Sim | Sim | Sim |
| Suporte técnico | Português (24h) | Inglês | Português |
| Melhor para | Pequenas e médias empresas | Grandes corporações | Pequenas e médias empresas |

# ASPECTOS LEGAIS E NORMATIVOS

A proteção da informação dentro das redes corporativas vai além da aplicação de medidas técnicas, ela também deve seguir os requisitos legais e regulatórios aplicáveis. O cumprimento dessas obrigações assegura não apenas a integridade e confidencialidade dos dados, mas também protege a organização contra sanções legais e fortalece sua reputação no mercado.

Com o aumento da digitalização e o avanço das ameaças cibernéticas, torna-se essencial que empresas adotem políticas de segurança da informação embasadas em legislações nacionais e normas internacionais reconhecidas. A seguir, destacam-se as principais diretrizes legais e normativas aplicáveis ao contexto de redes empresariais.

## LGPD (Lei Geral de Proteção de Dados)

A Lei Geral de Proteção de Dados Pessoais (nº 13.709/2018) é o principal marco regulatório brasileiro sobre privacidade e uso de dados. Seu objetivo é garantir que dados pessoais sejam tratados de forma transparente, segura e dentro dos direitos dos indivíduos.

No contexto de redes corporativas, a conformidade com a LGPD exige medidas que visam prevenir o uso indevido de informações. Entre as principais práticas estão:

* **Gerenciamento de acessos**, limitando a visualização e manipulação de dados sensíveis apenas a usuários devidamente autorizados.
* **Aplicação de técnicas de criptografia**, assegurando que as informações trafeguem e permaneçam armazenadas de maneira protegida.
* **Registro sistemático de eventos (logs)**, que permite rastrear atividades dentro da rede e identificar possíveis falhas ou acessos não autorizados.
* **Procedimentos de resposta a incidentes**, com planos definidos para lidar com vazamentos de dados, incluindo comunicação com os titulares e órgãos reguladores.

O descumprimento da LGPD pode resultar em penalidades financeiras e restrições operacionais, além de danos à imagem institucional.

# ISO/IEC 27001

A norma ISO/IEC 27001 apresenta uma metodologia estruturada para gerenciar a segurança da informação. Trata-se de uma referência global que orienta a criação de um **Sistema de Gestão de Segurança da Informação (SGSI)**, com foco em identificar riscos, definir controles apropriados e promover a melhoria contínua.

Entre os pontos essenciais da norma, destacam-se:

* **Análise e tratamento de riscos**, considerando o impacto potencial de ameaças e vulnerabilidades sobre os ativos informacionais.
* **Definição de políticas e processos de segurança**, integrando diretrizes para o uso adequado dos recursos tecnológicos da organização.
* **Aplicação de controles técnicos e administrativos**, como autenticação multifator, gestão de permissões, e proteção de sistemas contra acessos indevidos.
* **Auditorias internas e externas**, realizadas periodicamente para verificar se os processos estão sendo seguidos e identificar oportunidades de melhoria.
* **Treinamento e sensibilização dos colaboradores**, reforçando a cultura de segurança como um pilar da operação empresarial.

A BluePex atua fortemente nesse cenário, oferecendo soluções que contribuem para o cumprimento dos requisitos da ISO/IEC 27001, especialmente no que se refere à proteção de redes, monitoramento contínuo e controle de acessos. A empresa também é reconhecida como uma **Empresa Estratégica de Defesa (EED)**, certificada pelo Ministério da Defesa, o que reforça sua relevância no desenvolvimento de tecnologias de interesse nacional.

# ISO/IEC 27002

A norma ISO/IEC 27002 complementa a ISO/IEC 27001 ao apresentar um conjunto detalhado de práticas recomendadas para a implementação dos controles de segurança. Ela não estabelece exigências obrigatórias, mas fornece orientações práticas que auxiliam organizações a protegerem melhor seus ativos de informação.

Essa norma abrange diversas áreas, entre elas:

* **Proteção física e do ambiente de trabalho**, com foco na segurança de instalações e controle de acesso a áreas restritas.
* **Gestão operacional segura**, incluindo procedimentos de backup, prevenção contra malware e configuração segura de sistemas.
* **Segurança de redes e comunicações**, com medidas como segmentação de rede, uso de VPNs e firewalls.
* **Gestão do ciclo de vida da informação**, garantindo que dados sejam protegidos desde sua criação até o descarte adequado.
* **Monitoramento e resposta a incidentes**, incluindo a capacidade de detectar comportamentos anômalos e reagir de forma coordenada.

Adotar os controles sugeridos pela ISO/IEC 27002 permite que as organizações construam um ambiente digital mais robusto, alinhado às exigências normativas e preparado para lidar com ameaças de forma proativa. Além disso, a norma serve como guia prático para que equipes técnicas possam implementar medidas de segurança consistentes e adaptadas à realidade de cada empresa.

# ESTUDO DE CASO

Este capítulo tem como objetivo ilustrar a aplicação da ferramenta BluePex em um ambiente corporativo por meio da criação de uma empresa fictícia. A escolha por um cenário simulado permite uma abordagem detalhada e realista, explorando os desafios comuns enfrentados pelas organizações na segurança e gestão de redes.

A empresa fictícia será estruturada com uma rede corporativa típica, contendo servidores, dispositivos conectados e protocolos de segurança que precisam ser aprimorados. Com isso, será possível demonstrar como a solução BluePex pode ser utilizada para fortalecer a proteção contra ameaças, otimizar o gerenciamento da rede e garantir a integridade das informações.

Ao longo do capítulo, serão apresentados os principais desafios enfrentados pela organização, as estratégias adotadas para mitigá-los e os resultados obtidos após a implementação da ferramenta. Dessa forma, busca-se exemplificar, de maneira prática, os benefícios da BluePex na segurança e no gerenciamento de infraestruturas corporativas.

## Sobre a Empresa

A Empresa X é uma organização do setor imobiliário que atua na intermediação de compra, venda e administração de imóveis. Com 20 funcionários, a empresa depende fortemente de sua infraestrutura de TI para garantir o funcionamento eficiente de suas operações diárias, incluindo comunicação interna e externa, armazenamento seguro de dados e acesso remoto a informações críticas.

Para sustentar essas operações, a Empresa X conta com uma rede corporativa estruturada para suportar múltiplos dispositivos, conexões seguras à internet e gerenciamento centralizado de recursos. No entanto, a empresa enfrenta desafios relacionados à segurança da informação, disponibilidade de rede e monitoramento de ameaças, os quais serão abordados com a implementação da solução BluePex.

## Infraestrutura de Rede

A rede da **Empresa X** foi projetada para garantir conectividade, desempenho e segurança, sendo composta pelos seguintes elementos principais:

## Conectividade com a Internet

A empresa possui dois links de internet para garantir redundância e maior disponibilidade:

* Link ALGAR – 300 Mbps
* Link TIM – 1 Gbps

Ambos os links são conectados ao **BluePex 1500**, que atua como firewall e solução de segurança para o tráfego de rede.

## Firewall e Segurança (BluePex 1500)

O BluePex 1500 é o principal dispositivo de segurança da empresa, sendo responsável pelo controle de tráfego, proteção contra ameaças e gerenciamento de acessos. Ele está configurado com as seguintes interfaces:

* Eth0: Rede Pérola
* Eth0: VLAN 10 DMZ (10.1.1.1/24) – Rede de visitantes
* Eth1: Link ALGAR – 300 Mbps
* Eth2: Link TIM – 1 Gbps
* Eth3 & Eth4: Interfaces Default

O firewall da BluePex garante que a rede corporativa esteja protegida contra acessos não autorizados e ataques cibernéticos, além de permitir um melhor gerenciamento de banda entre os dois provedores de internet.

## Rede Cabeada e Wireless

A rede interna da empresa opera em uma topologia estruturada, utilizando switches de camada 2 para conectar os dispositivos físicos, como servidores e estações de trabalho. Há também um ponto de acesso WiFi Unifi, que fornece conectividade sem fio para até 4 dispositivos simultaneamente.

## Servidores e Virtualização

A Empresa X utiliza um ambiente misto de servidores físicos e máquinas virtuais para gerenciar seus serviços internos:

* GYNX01-DC01 (Servidor Físico)

o IP: 172.16.15.10/24

* + Sistema Operacional: Windows Server 2016
  + Serviços: Active Directory (AD), DHCP, DNS e DFS
  + Finalidade: Controlador de domínio e gerenciamento centralizado da rede
* GYNX01-VM01 (Servidor Virtualizado)
  + IP: 172.16.23.5/24
  + Configuração: 10 GB de RAM / 8 TB de armazenamento
  + Sistema Operacional: VMware ESXi 6.7
  + Serviço: Virtualização de servidores
  + Hardware: Dell PowerEdge T420
* SRV02EMPRESAX (Servidor de Aplicações)
  + IP: 172.16.23.14/24
  + Sistema Operacional: Windows Server 2008 R2
  + Serviço: Gestão e Hyper-V

## Armazenamento e Backup

A política de armazenamento da empresa inclui dispositivos dedicados para backup e arquivamento de dados:

* HD Externo 5 TB: Backup local dos servidores
* HD 2 TB: Armazenamento de arquivos antigos

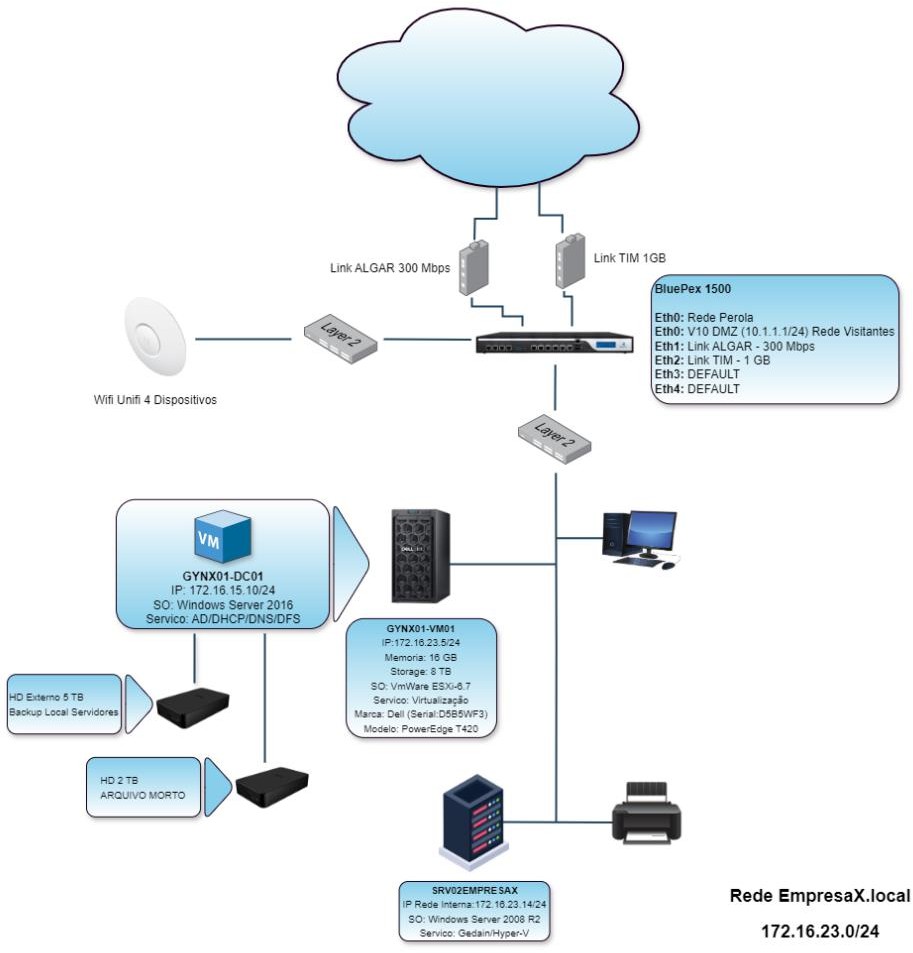
## Considerações sobre a Rede

A topologia da rede da Empresa X foi estruturada para garantir conectividade eficiente e segura. No entanto, antes da implementação da BluePex, a empresa enfrenta desafios relacionados à:

* Gestão de ameaças cibernéticas, devido à falta de monitoramento contínuo e proteção contra ataques externos.
* Gerenciamento de acessos, especialmente no controle de dispositivos conectados via Wi-Fi e segmentação de visitantes.
* Otimização da conectividade, garantindo que os links de internet sejam utilizados da forma mais eficiente possível.
* Segurança e integridade dos dados, incluindo a proteção contra perda de informações sensíveis e vazamentos.

A implementação da BluePex será fundamental para mitigar esses desafios e proporcionar um ambiente de TI mais seguro e gerenciável. Nos próximos tópicos, será detalhado como a solução foi aplicada e os resultados obtidos com sua implementação.

Figura 5 – Layout da Rede da Empresa X



Fonte: Elaborado pelo autor com draw.io, imagens retiradas do Google

## BluePex na Rede

O uso da ferramenta BluePex veio para criar uma segmentação da rede de forma mais eficiente, ele irá fazer a entrega de IP´s e também o controle do tráfego do que será acessado dentro da rede.

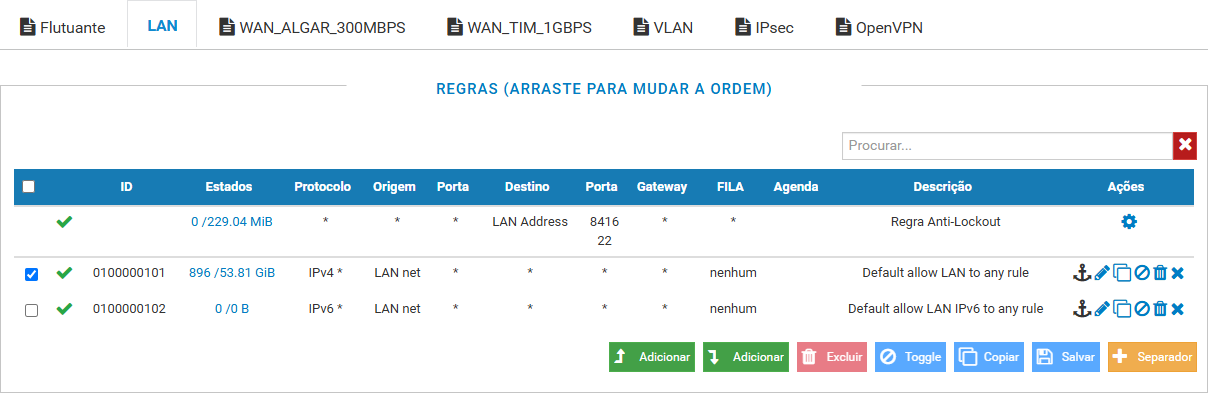
Como já havia dito a BluePex é uma ferramenta com vários tipos de serviços, sendo de proteção de máquina, o de firewall e alguns outros. Nessa empresa nós estaremos usando apenas o serviço de firewall dele. Nós elaboramos algumas regras de firewall para essa empresa, para que haja uma melhorar organização e desempenho do que cada regra deve adotar.

## Regras de Firewall

Dentro da BluePex foi criado 6 regras para utilização da ferramenta, sendo elas:

* Flutuante: Não foi definida nenhuma regra, criada apenas por protocolo se houver necessidade futura.
* LAN:
  + Criado uma regra de Anti-Lockout, para evitar que o administrador se bloqueie acidentalmente.

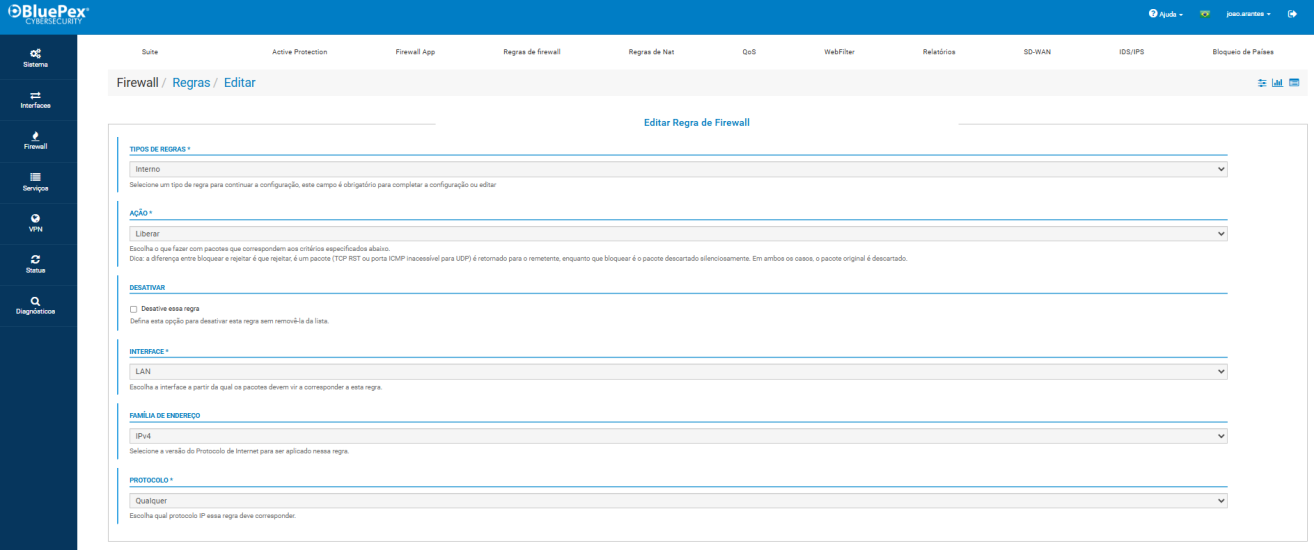
Figura 6 – Regras da LAN



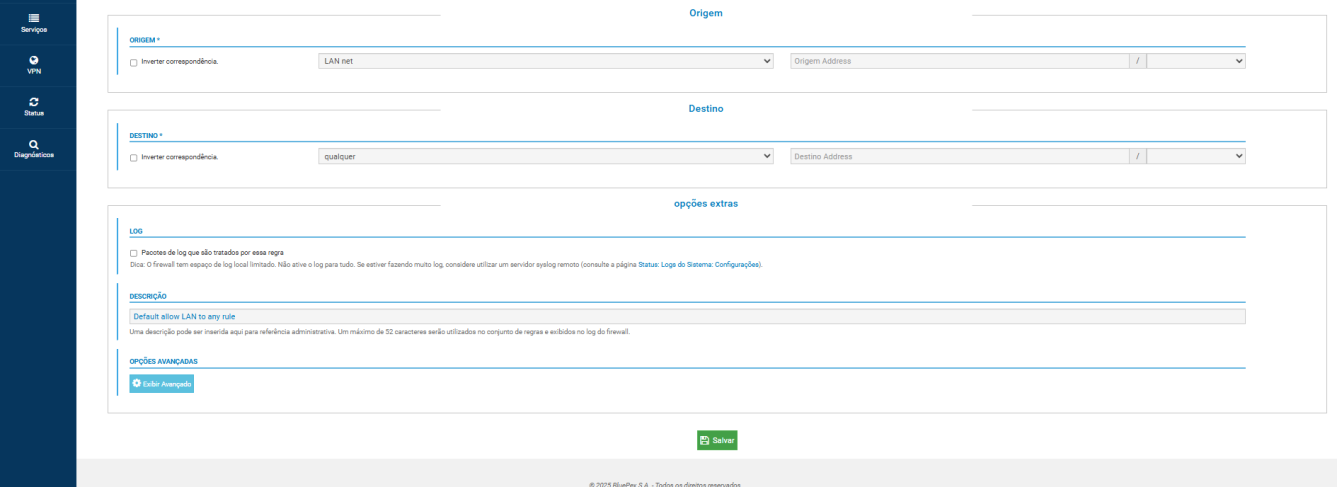
Fonte: BluePex Cloud

* + Criado uma regra para o IPv4 permitir que a LAN acesse qualquer destino.

Figura 7 – Regras da LAN IPv4

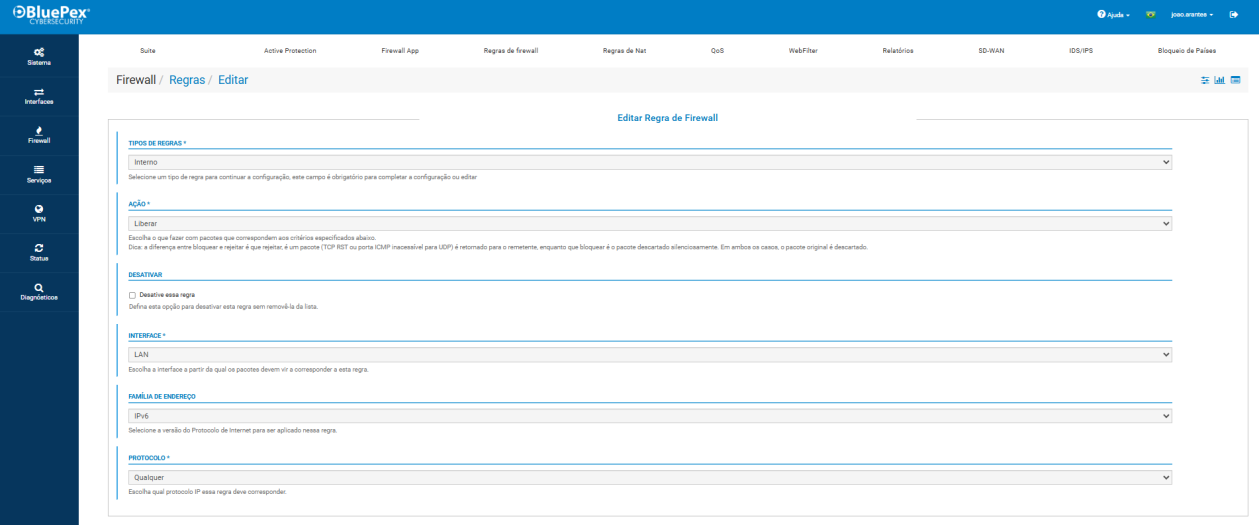


Fonte: BluePex Cloud Figura 8 – Regras da LAN IPv4

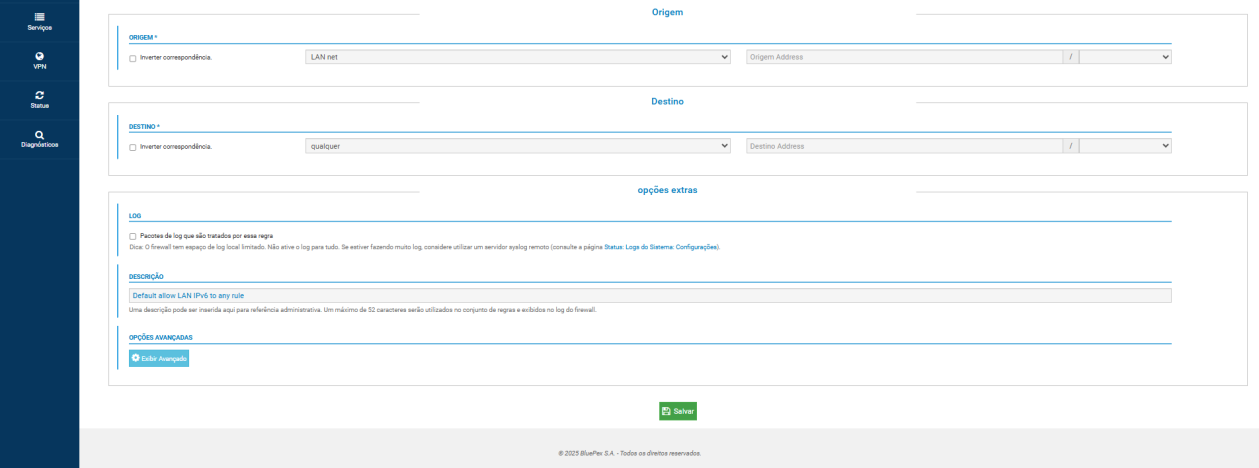
Fonte: BluePex Cloud

* + Criado uma regra para o IPv6 permitir acesso de qualquer destino.

Figura 9 – Regras da LAN IPv6



Fonte: BluePex Cloud Figura 10 – Regras da LAN IPv6



Fonte: BluePex Cloud

* WAN\_ALGAR\_300MBPS:

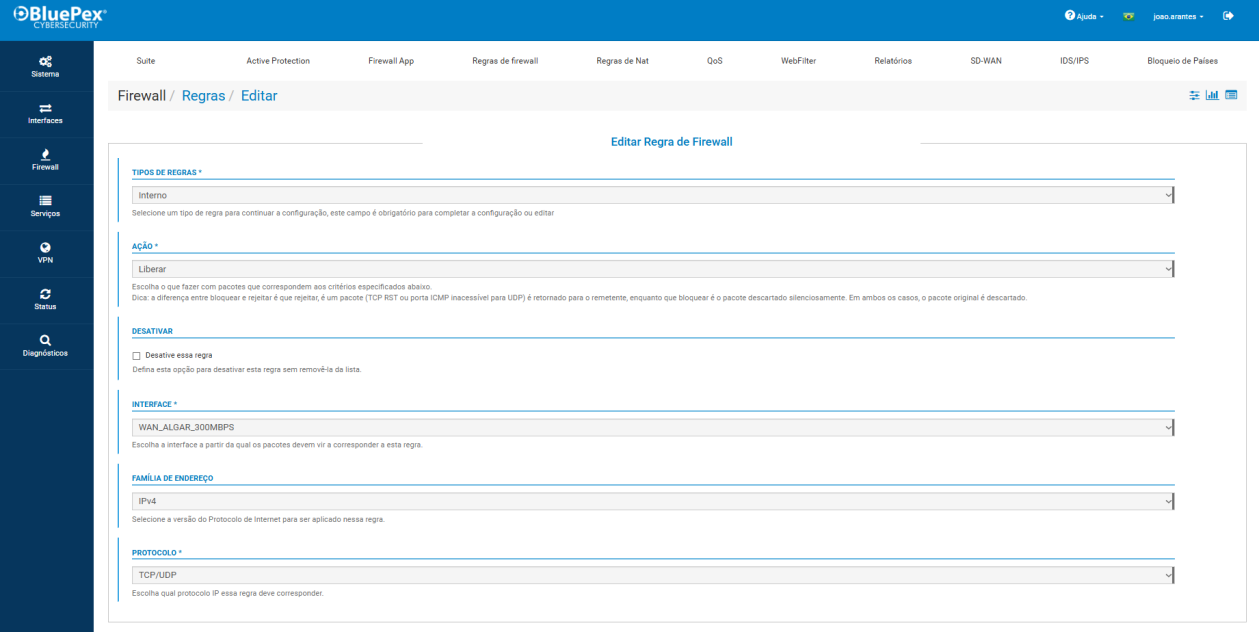
Figura 11 – Regras da WAN\_ALGAR\_300MBPS



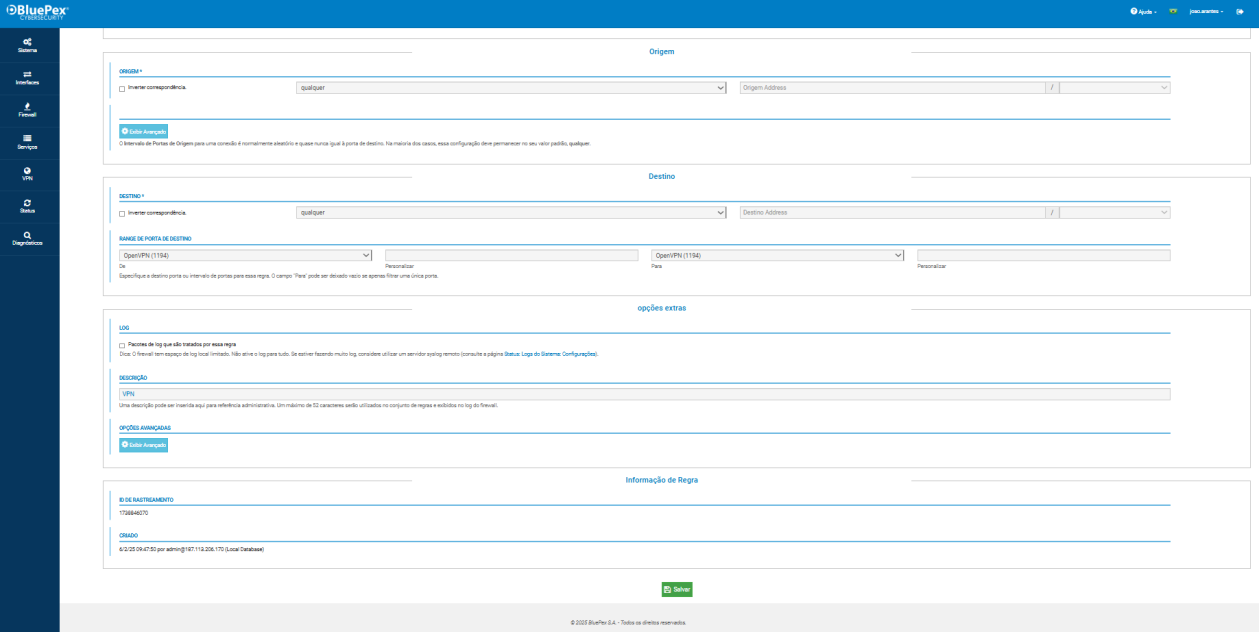
Fonte: BluePex Cloud

* + Devido uma necessidade de VPN para alguns setores da empresa, foi elaborado uma regra onde defini o protocola IPv4 TCP/UDP para porta 1194 que terá como função de liberar o acesso a OpenVPN.

Figura 12 – Regras da OpenVPN



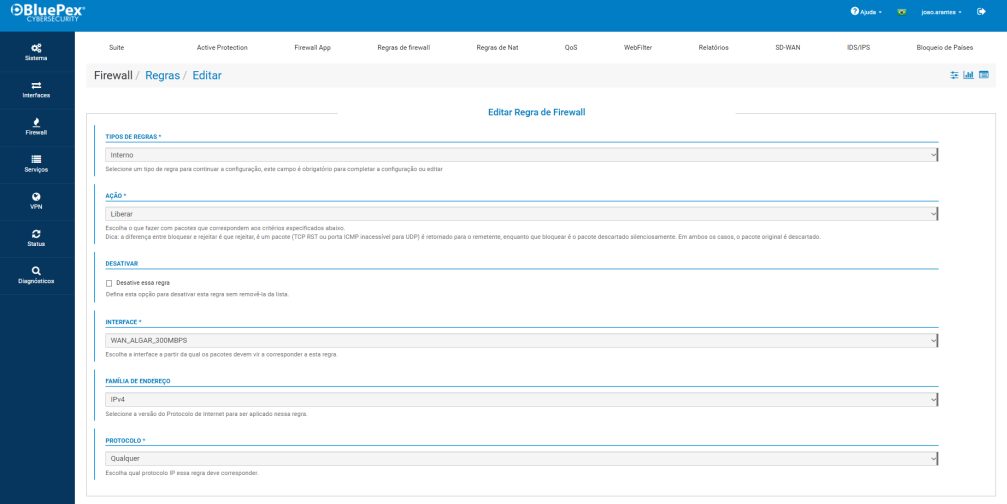
Fonte: BluePex Cloud Figura 13 – Regras da OpenVPN



Fonte: BluePex Cloud

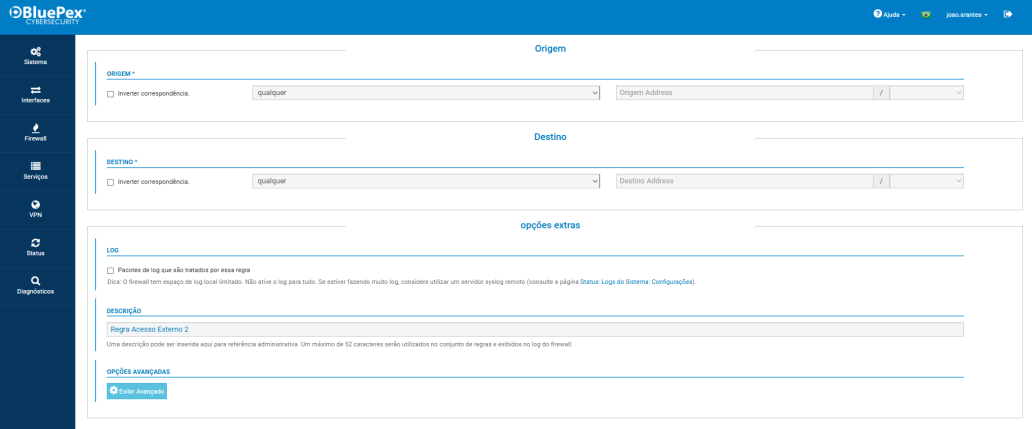
* + Foi elaborado uma regra para fazer a conexão ao Cloud da BluePex por um acesso externo, ou seja, por uma rede de fora da empresa.

Figura 14 – Regras do Acesso Externo



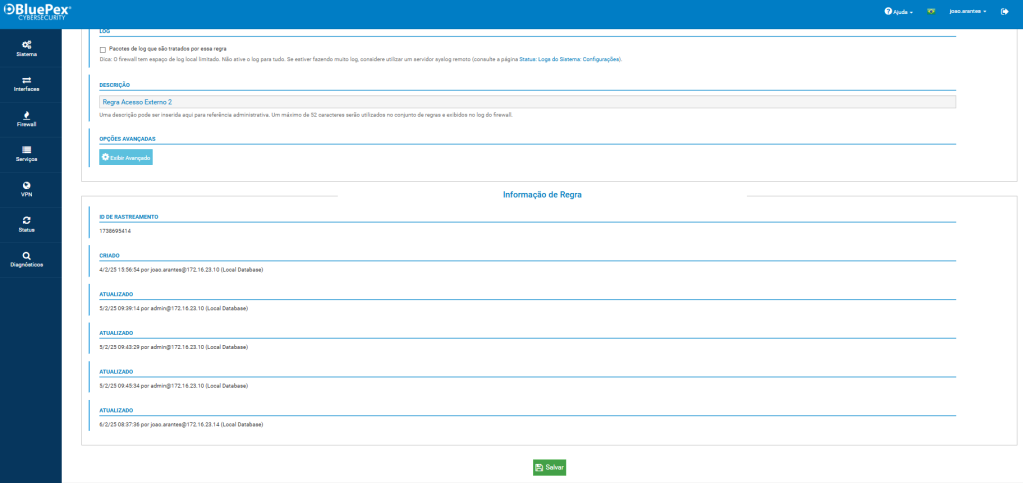
Fonte: BluePex Cloud

Figura 15 – Regras do Acesso Externo



Fonte: BluePex Cloud

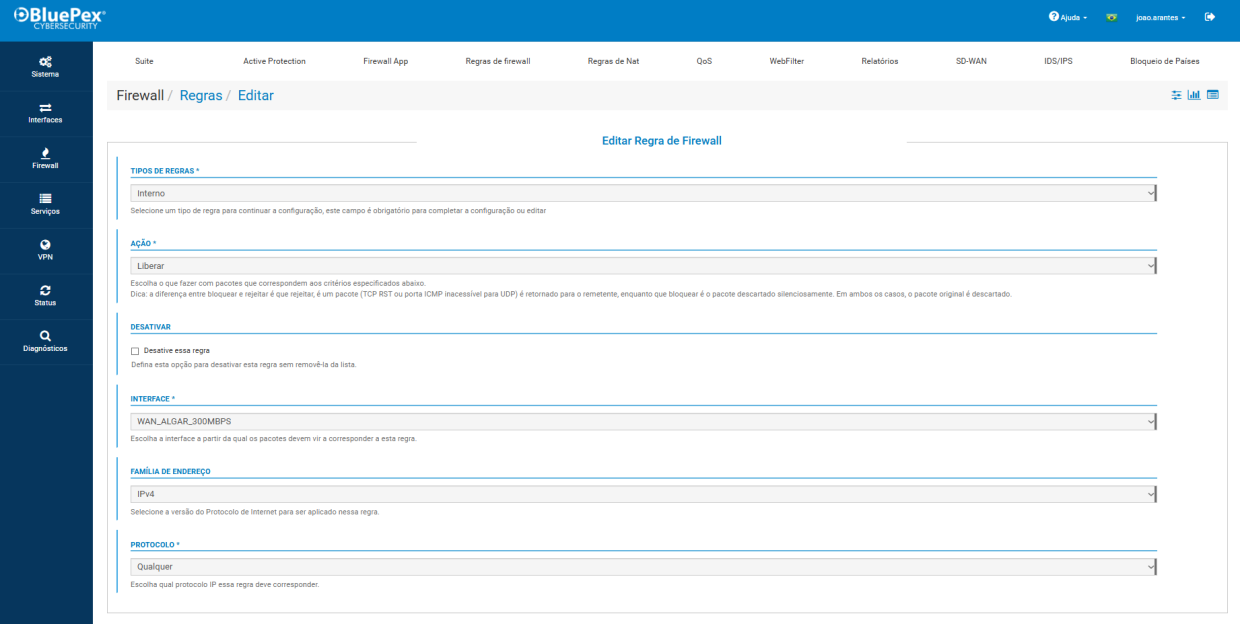
Figura 16 – Regras do Acesso Externo



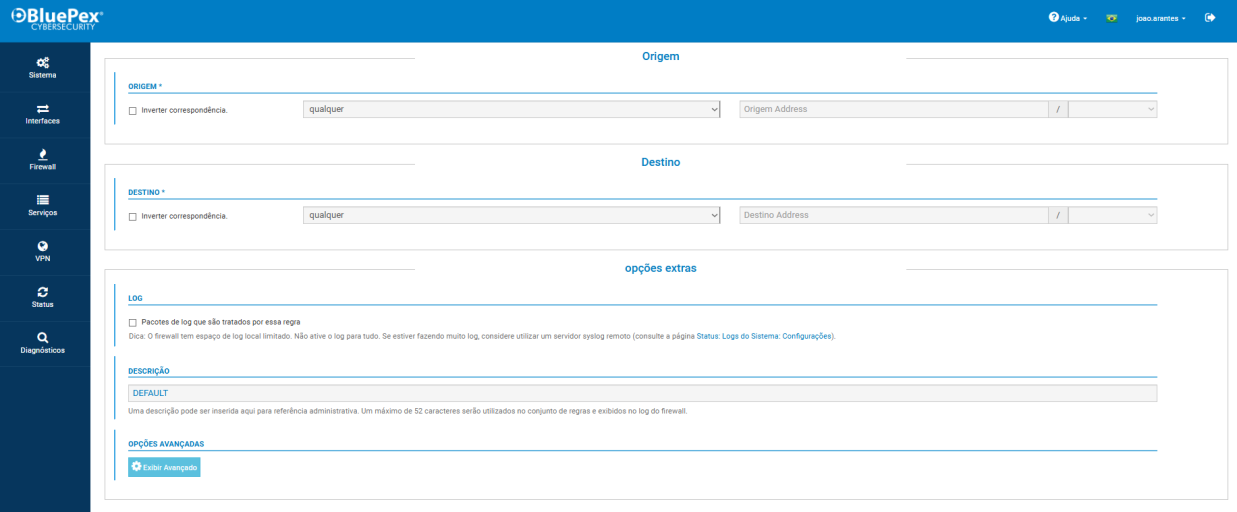
Fonte: BluePex Cloud

* + Há uma regra DEFAULT para liberar tudo no firewall, não barrar nada.

Figura 17 – Regras do DEFAULT



Fonte: BluePex Cloud Figura 18 – Regras do DEFAULT



Fonte: BluePex Cloud Figura 19 – Regras do DEFAULT



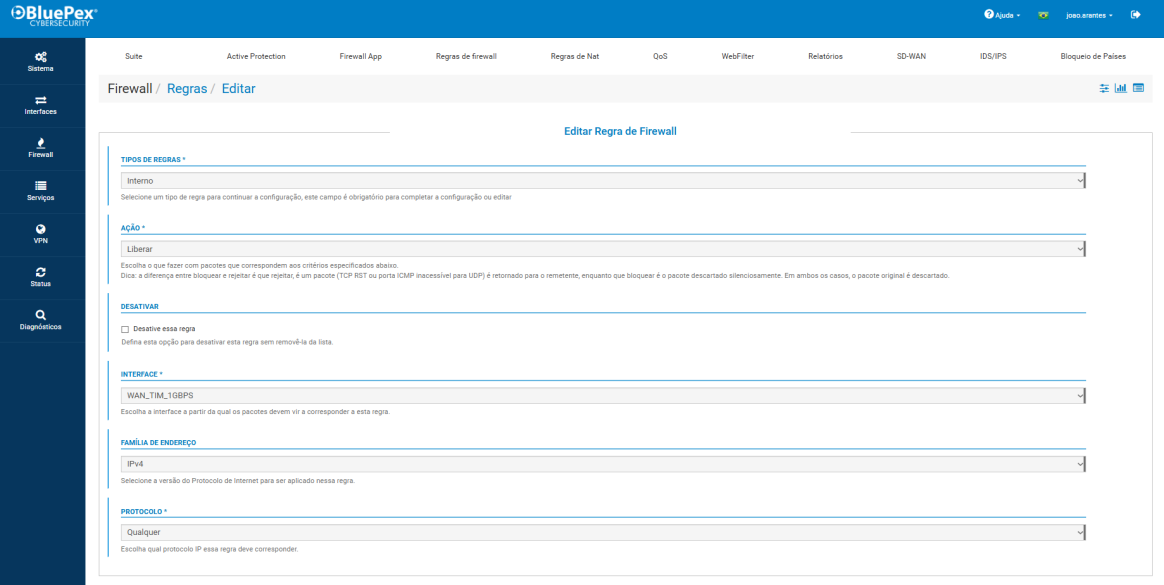
Fonte: BluePex Cloud

* WAN\_TIM\_1GBPS:

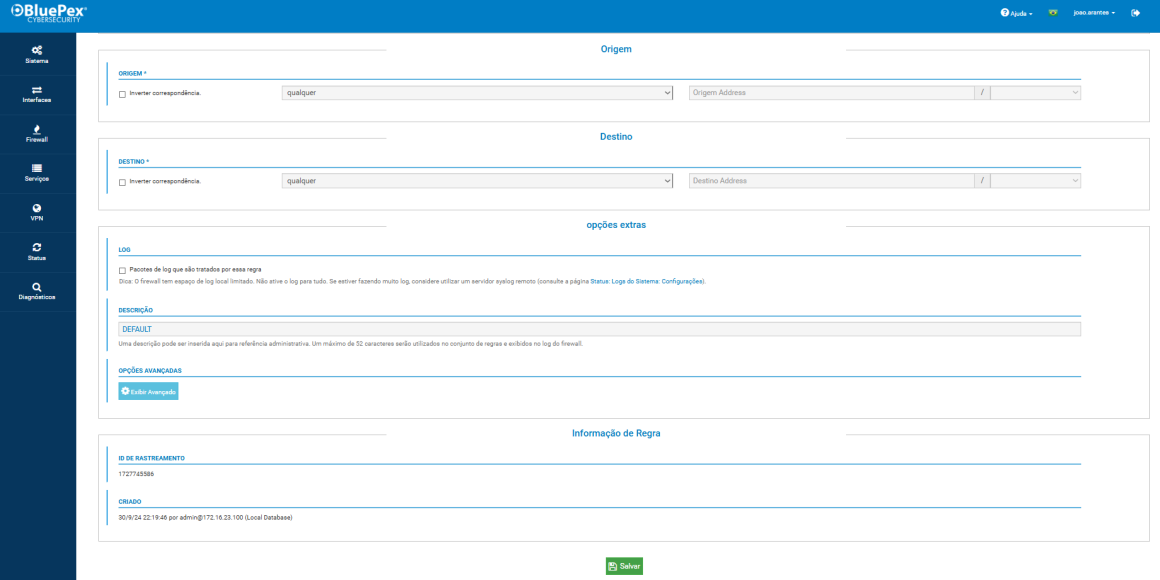
Figura 20 – Regras da WAN\_TIM\_1GBPS

Fonte: BluePex Cloud

* + Foi elaborado apenas a regra de DEFAULT, para liberar todo tipo de acesso.

Figura 21 – Regras do DEFAULT

Fonte: BluePex Cloud Figura 22 – Regras do DEFAULT



Fonte: BluePex Cloud

* VLAN:

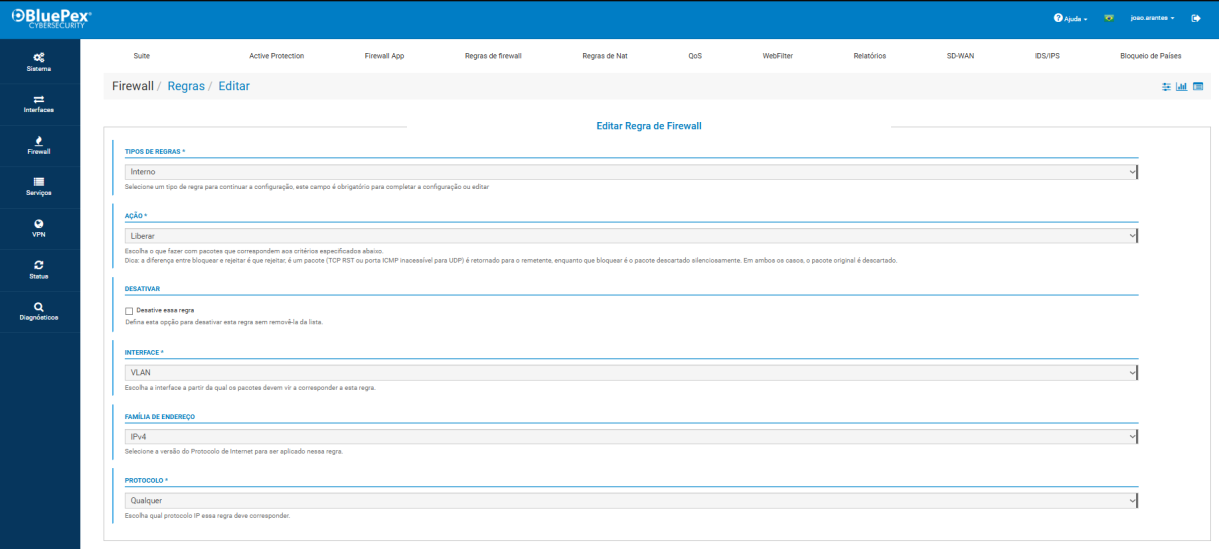
Figura 23 – Regras da VLAN



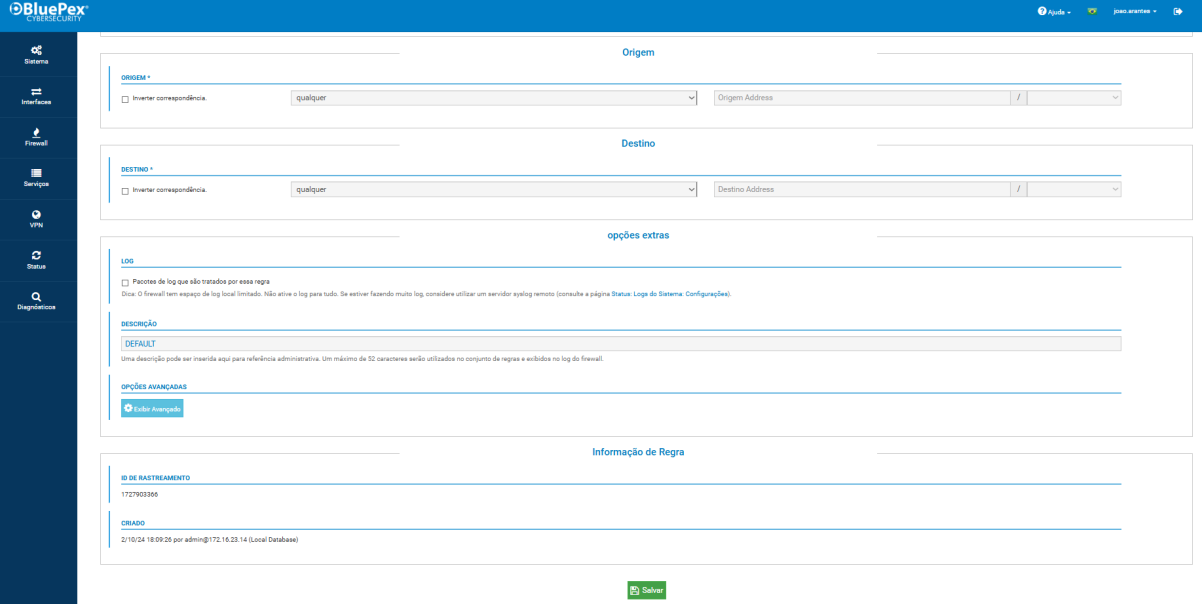
Fonte: BluePex Cloud

* + Não teve a criação de nenhuma outra regra fora a DEFAULT.

Figura 24 – Regras da DEFAULT



Fonte: BluePex Cloud Figura 25 – Regras da DEFAULT



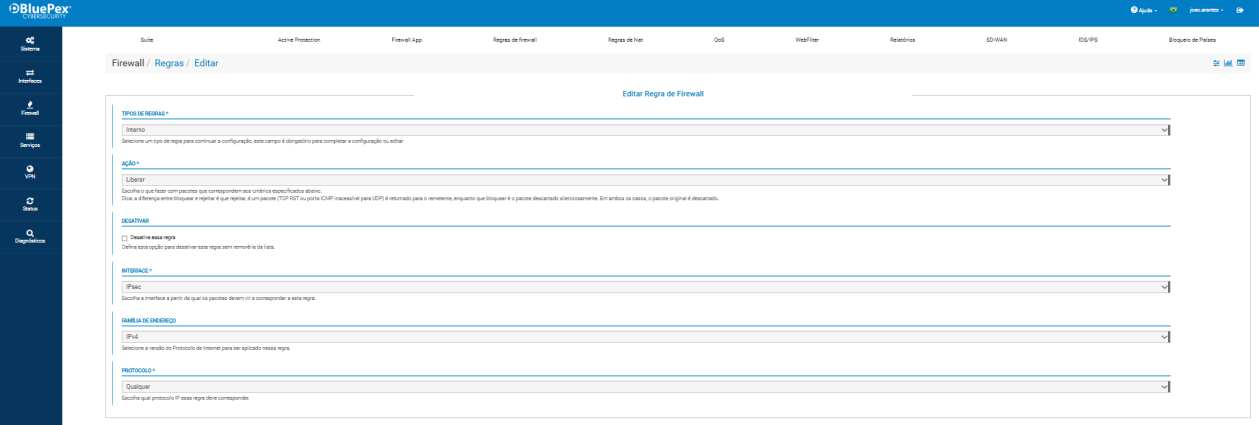
Fonte: BluePex Cloud

* IPsec:

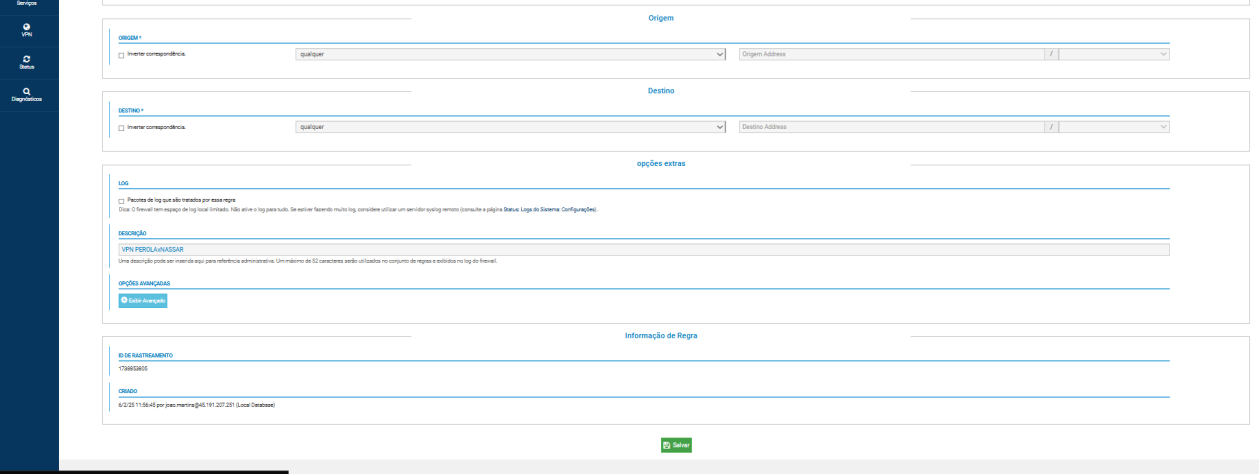
Figura 26 – Regras do IPsec

Fonte: BluePex Cloud

* + Regra VPN site to site, ou seja, comunicação direta entre a Empresa X e a empresa de suporte de TI que fica externamente.

Figura 27 – Regras da comunicação direta

Fonte: BluePex Cloud

Figura 28 – Regras da comunicação direta

Fonte: BluePex Cloud

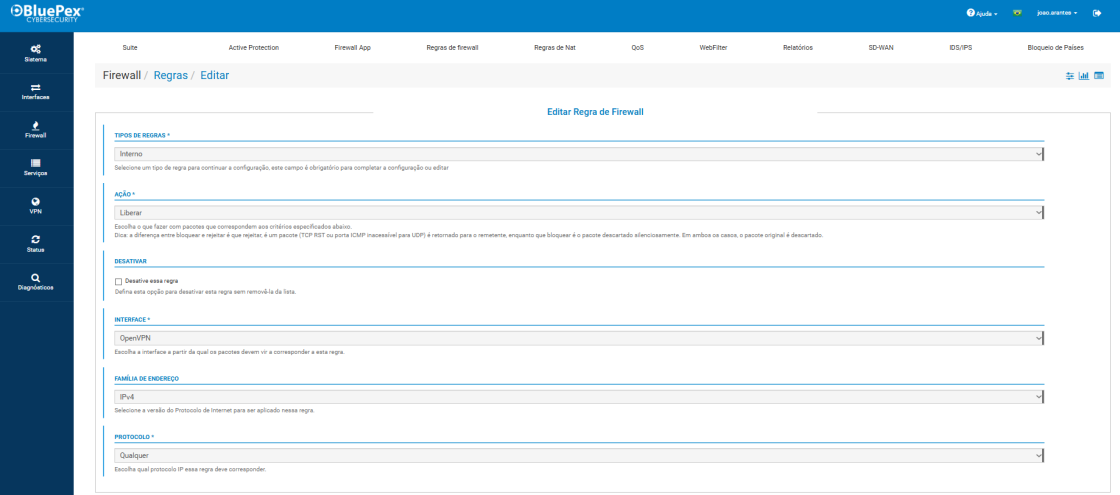
* OpenVPN:

Figura 29 – Regras da OpenVPN

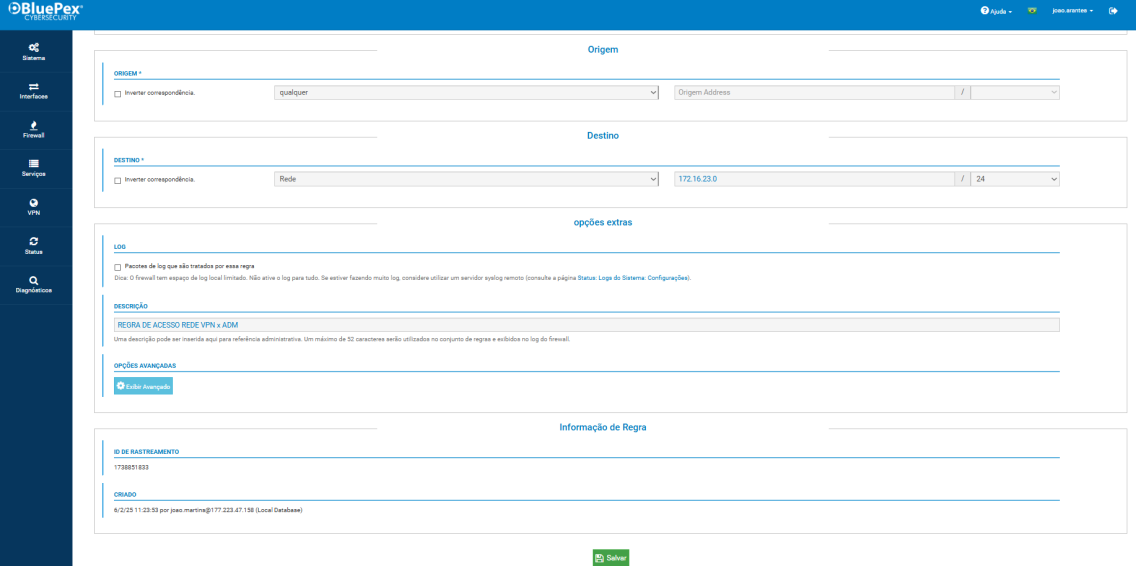
Fonte: BluePex Cloud

* + Foi criado a regra que autoriza que quem tenha acessado a VPN consiga acessar a rede administrativa, ou seja, possa conectar ao Active Directory (AD) e assim acessar as pastas de rede.

Figura 30 – Regras da OpenVPN

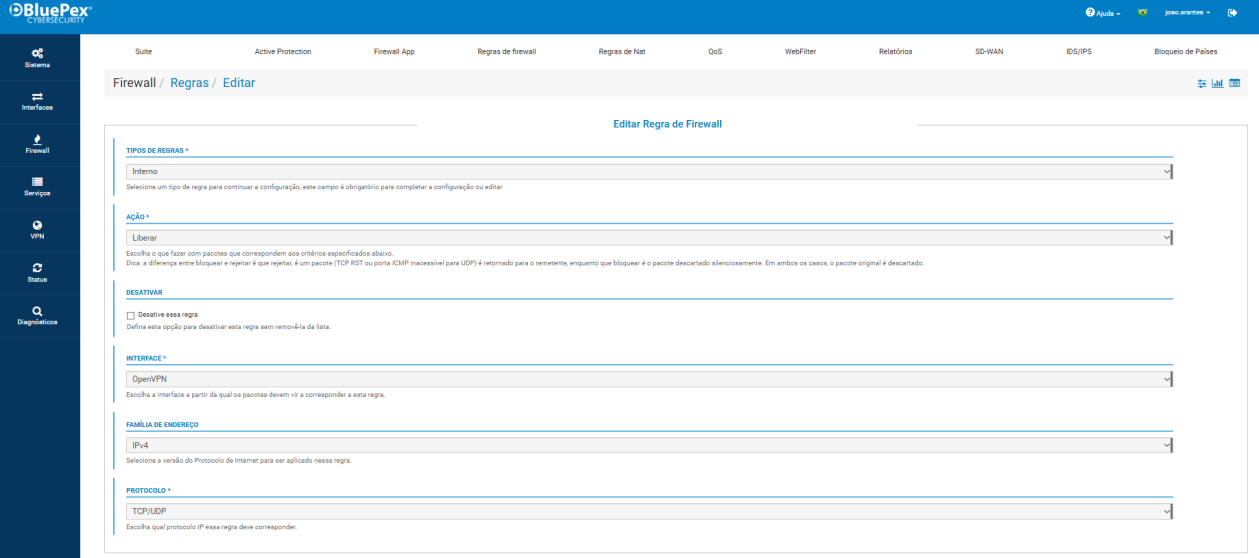


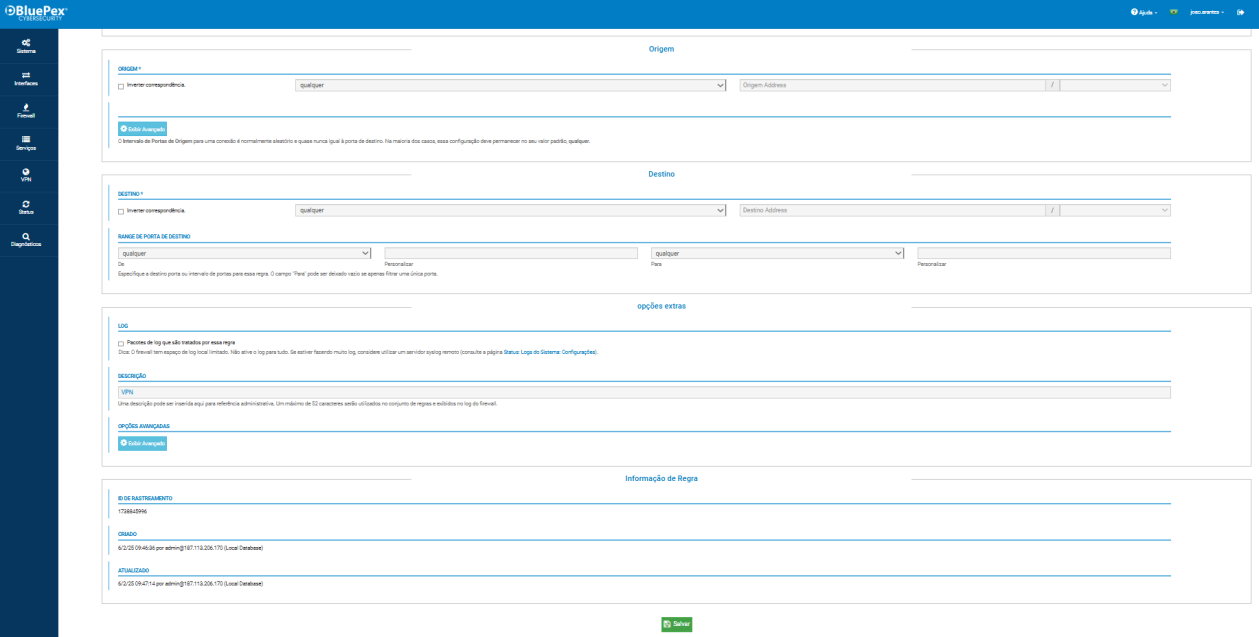
Fonte: BluePex Cloud Figura 31 – Regras da OpenVPN



Fonte: BluePex Cloud

* + Foi criado uma regra que autoriza que todo mundo que tenha acessado a VPN não tenha nenhuma restrição de acesso.

Figura 32 – Regras da OpenVPN

Fonte: BluePex Cloud Figura 33 – Regras da OpenVPN

Fonte: BluePex Cloud

## Servidor DHCP

Após a definição das regras de firewall para a rede, o próximo passo é a configuração do **servidor DHCP**, responsável por atribuir automaticamente endereços IP aos dispositivos conectados, tanto na rede interna quanto por conexões VPN. Nessa configuração, determinamos

os intervalos de IP válidos para cada tipo de conexão, assim como o gateway, máscara de sub- rede e demais parâmetros de rede.

A seguir, detalhamos como o DHCP foi configurado para cada interface da infraestrutura:

## Servidor DHCP LAN

Na interface LAN, foi habilitado o serviço de DHCP com a faixa de IP pertencente à rede 172.16.23.0/24. Os endereços atribuídos variam de 172.16.23.2 a 172.16.23.254, sendo reservada a primeira faixa para uso interno do gateway e serviços. O sistema define como DNS preferenciais os endereços 172.16.23.10, 8.8.8.8 e 1.1.1.1.

Além disso, a configuração conta com recursos adicionais como:

* + - * + Tempo padrão de concessão: 2 horas (7200 segundos);
        + Tempo máximo de concessão: 24 horas (86400 segundos);
        + Verificação de disponibilidade via ping antes da entrega do IP;
        + Mapeamento de estatísticas e suporte a ARP estático, permitindo restringir a comunicação apenas a dispositivos autorizados.

## Servidor DHCP WAN\_TIM\_1GBPS

Na interface de saída WAN\_TIM\_1GBPS, utilizada para conexões externas ou links de operadora, também foi ativado o DHCP. A rede atribuída é 192.168.2.0/24, com endereços disponíveis entre 192.168.2.1 e 192.168.2.254.

Essa configuração é recomendada para permitir a atribuição dinâmica de IPs a dispositivos de borda ou equipamentos temporários. Assim como na LAN, há suporte a:

* + - * + Limitação de tempo de concessão;
        + Gerenciamento remoto via OMAPI com autenticação segura (HMAC- SHA256);
        + Estatísticas de uso;
        + Controle de acesso por endereço MAC.

## Servidor DHCP VLAN

A interface VLAN foi configurada com a sub-rede 10.1.1.0/24, utilizando o intervalo de 10.1.1.100 a 10.1.1.200 para entrega de IPs. Essa separação é

estratégica para isolar redes de convidados ou setores específicos da organização, mantendo maior controle e segurança.

Os servidores DNS utilizados são os públicos: 8.8.8.8, 8.8.4.4 e 1.1.1.1. Também estão disponíveis as mesmas funcionalidades aplicadas às demais interfaces, como:

* + - * + Tempo de concessão configurável;
        + Suporte a failover via IP de tolerância (CARP);
        + Registro de estatísticas de uso e ativação de ARP estático.

## Serviços de DNS

O BluePex UTM oferece suporte completo a serviços de DNS, permitindo a configuração personalizada tanto do *DNS Resolver* quanto do *DNS Dinâmico*. Na seção de *DNS Resolver*, o administrador pode ajustar configurações gerais como ativação do serviço, escuta em interfaces específicas, suporte a IPv6, registro de logs e encaminhamento de requisições (*forwarders*), além de permitir a definição de domínios a serem resolvidos diretamente. Já nas configurações avançadas, é possível aplicar regras personalizadas, configurar acessos por ACLs (Listas de Controle de Acesso), realizar tunings de performance e definir bloqueios baseados em regras DNS.

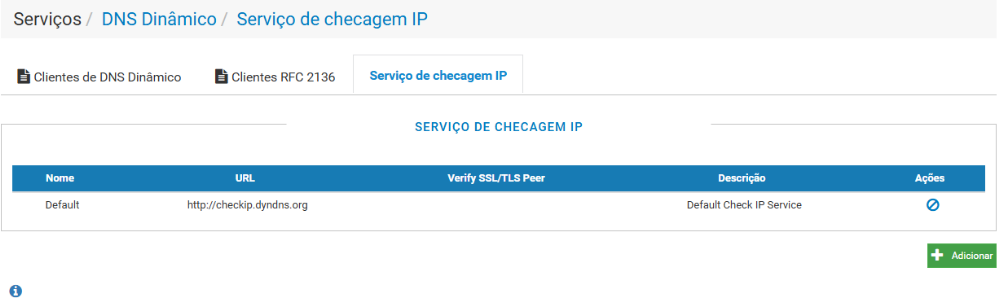
O serviço de *DNS Dinâmico* viabiliza a atualização automática de registros DNS associados a endereços IP dinâmicos. Entre as funcionalidades está a integração com provedores de DNS dinâmico, como o serviço de checagem de IP padrão (ex: [http://checkip.dyndns.org),](http://checkip.dyndns.org/) com possibilidade de verificar o par SSL/TLS e descrever o serviço. A interface permite ainda a adição de novos serviços personalizados conforme a necessidade da rede.

## DNS Dinâmico

O recurso de **DNS Dinâmico** no BluePex UTM permite manter o mapeamento de nomes de domínio atualizado mesmo quando o endereço IP público da conexão é alterado com frequência, como em links residenciais ou empresariais com IP dinâmico. Através dessa funcionalidade, o dispositivo pode informar automaticamente seu novo IP a um serviço de DNS dinâmico, garantindo que o nome de domínio configurado continue apontando corretamente para o ambiente de rede interno.

Na interface do sistema, é possível configurar provedores de DNS dinâmico já reconhecidos ou cadastrar serviços personalizados. Também é permitido definir intervalos de atualização, ativar verificações automáticas de IP via URLs externas (como [http://checkip.dyndns.org),](http://checkip.dyndns.org/) e habilitar conexões seguras com suporte a SSL/TLS. Esse recurso é essencial para acessos remotos, VPNs, e outros serviços que dependem de disponibilidade externa estável, mesmo sem um IP fixo.

Figura 34 – Serviço de checagem de IP do DNS Dinâmico



Fonte: BluePex Cloud

## Serviço NTP

O serviço NTP (Network Time Protocol) é responsável por sincronizar o relógio dos dispositivos em uma rede com servidores de horário de referência, garantindo que todos os sistemas compartilhem a mesma hora exata. Essa sincronização é essencial para o funcionamento correto de serviços de rede, registros de logs, autenticações e outras operações sensíveis ao tempo.

No BluePex UTM, o serviço NTP pode ser habilitado para funcionar como servidor de horário, sincronizando a hora com servidores externos confiáveis, como ***a.ntp.br***. O sistema permite configurar múltiplos servidores com diferentes prioridades e tipos (servidor único, par ou pool), recomendando-se a adição de ao menos quatro fontes para maior confiabilidade. Também é possível definir interfaces específicas para o serviço, ativar gráficos estatísticos, configurar intervalos de pesquisa e ativar o modo órfão, que permite ao dispositivo manter uma referência interna de tempo na ausência de servidores externos.

Complementarmente, o BluePex oferece a configuração de ACLs (listas de controle de acesso) no NTP para restringir operações como modificações de tempo, consultas de status e associação de pares. Essas restrições aumentam a segurança ao impedir, por exemplo, ataques baseados em consulta (como o uso malicioso do comando **ntpq**) ou a tentativa de associar o dispositivo com fontes de tempo não autorizadas.

## Web Filter

O **Web Filter** (ou filtro de conteúdo web) é um recurso essencial de segurança de rede que tem como objetivo controlar o acesso a conteúdos na internet com base em categorias, endereços URL, palavras-chave ou reputação de sites. Essa ferramenta atua como uma camada de proteção, bloqueando sites maliciosos, inadequados ou que possam representar riscos à produtividade e segurança da rede corporativa.

No contexto do BluePex UTM, o Web Filter é uma das funcionalidades integradas à suíte de proteção ativa. Ele permite a criação de políticas de filtragem personalizadas, nas quais

é possível permitir ou negar o acesso a determinados tipos de conteúdo, como redes sociais, sites de jogos, pornografia, notícias falsas, entre outros. O administrador pode aplicar essas políticas por grupo de usuários, horário ou faixa de IP, garantindo um controle mais granular sobre o uso da internet.

Além da proteção contra ameaças virtuais, como phishing e malware hospedado em páginas suspeitas, o Web Filter contribui para o bom uso dos recursos da empresa, evitando desperdício de banda e promovendo maior foco dos colaboradores em suas atividades. Com relatórios detalhados, também é possível monitorar o comportamento de navegação dos usuários, identificando possíveis abusos ou violações às políticas de uso da internet da organização.

Entretanto, neste projeto, optou-se por **não utilizar o serviço de Web Filter**, uma vez que **não foi identificada a necessidade da aplicação deste recurso**, considerando os demais serviços implementados, a estrutura organizacional e o planejamento operacional da empresa. A política de uso responsável da internet, aliada ao perfil das atividades desempenhadas, demonstrou ser suficiente para manter o controle e a segurança no ambiente digital corporativo, sem a necessidade de filtragem adicional.

# VPN

A **VPN (Virtual Private Network)** é uma tecnologia que permite a criação de uma conexão segura entre redes distintas através da internet pública. Essa conexão seja criptografada, garantindo a confidencialidade e integridade dos dados trafegados. O uso de VPNs é essencial em ambientes corporativos, especialmente para integrar filiais, permitir o acesso remoto seguro de colaboradores ou interligar servidores entre diferentes localidades geográficas.

No BluePex UTM, a configuração de VPN é feita por meio do protocolo **IPSec**, um dos mais utilizados para garantir segurança em comunicações IP. A solução permite criar túneis criptografados com diversas opções de algoritmos, modos e níveis de autenticação, proporcionando alta flexibilidade e segurança conforme a necessidade da organização.

## Túnel IPsec Configurado

A configuração da Fase 1 de um túnel IPsec na interface de gerenciamento do BluePex UTM é um passo crucial para o estabelecimento seguro de conexões VPN entre dois pontos de rede. Essa fase envolve principalmente a negociação de parâmetros criptográficos e autenticação mútua entre os peers (pontos finais da conexão).

O PDF demonstra a configuração do túnel nomeado EMPRESAX\_X\_EMPRESATI, utilizando o protocolo IKEv2, que é a versão mais moderna e segura do Internet Key Exchange, sendo compatível com a maioria dos

dispositivos e recomendada para novos projetos. O tráfego VPN é roteado pela interface WAN\_ALGAR\_300MBPS, conectando-se ao endereço IP remoto 45.191.207.251.

Para autenticação, o método selecionado é o PSK Mútuo (Pre-Shared Key), utilizando identificadores únicos (empresax\_empresati e empresati\_empresax) e uma chave forte de 64 caracteres hexadecimais. A robustez dessa chave é essencial para impedir ataques de força bruta ou comprometimento da conexão.

No que diz respeito à segurança dos dados, foram definidos os seguintes algoritmos criptográficos:

* Criptografia: AES com chave de 256 bits;
* Integridade: SHA256;
* Troca de chaves: Grupo DH 14 (2048 bits).

Estes parâmetros seguem boas práticas de segurança, evitando algoritmos obsoletos como 3DES, MD5 ou SHA1, citados no próprio sistema como opções fracas.

A política de expiração da associação de segurança (SA) também foi cuidadosamente configurada:

* Tempo de vida: 28.800 segundos (~8 horas),
* Rekeying: 25.920 segundos,
* Reautenticação: 300 segundos (valor relativamente baixo, indicando alta preocupação com segurança),
* Tempo aleatório: 2.880 segundos, o que evita a renegociação simultânea e colisões entre sessões.

Outras opções avançadas, como DPD (Dead Peer Detection), estão habilitadas, garantindo a resiliência da conexão. A configuração do DPD com atraso de 10 segundos e tolerância para até 5 falhas consecutivas assegura que o sistema rapidamente identifique peers inativos e restabeleça a conexão automaticamente.

Por fim, a configuração permite duplicações de gateway e conexões divididas, possibilitando maior flexibilidade e suporte a múltiplos túneis Fase 2 por um mesmo par Fase 1, o que é útil em cenários com múltiplas sub-redes ou necessidades de segmentação.

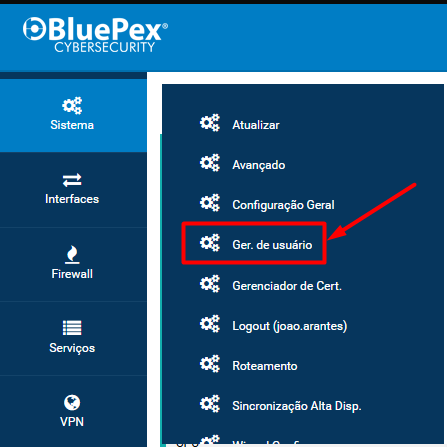
## Configuração VPN

Para a configuração da VPN, é necessário, inicialmente, realizar a criação de um perfil de usuário. Esse processo consiste no preenchimento de um formulário que contempla informações essenciais, como nome, senha, nível de acesso, permissões e, de forma destacada, a associação de um certificado digital sendo este o certificado VPN que garantirá a autenticação segura do usuário.

O formulário de criação de usuários pode ser acessado por meio do painel lateral da plataforma BluePex Cloud, na opção Sistema. Ao selecionar essa opção, são exibidas subcategorias, entre as quais se encontra Ger. de Usuários (Gerenciamento de Usuários). Nesta seção, é possível realizar o gerenciamento completo dos perfis, incluindo a filtragem de usuários existentes, bem como a criação de novos registros ou exclusão de contas previamente cadastradas.

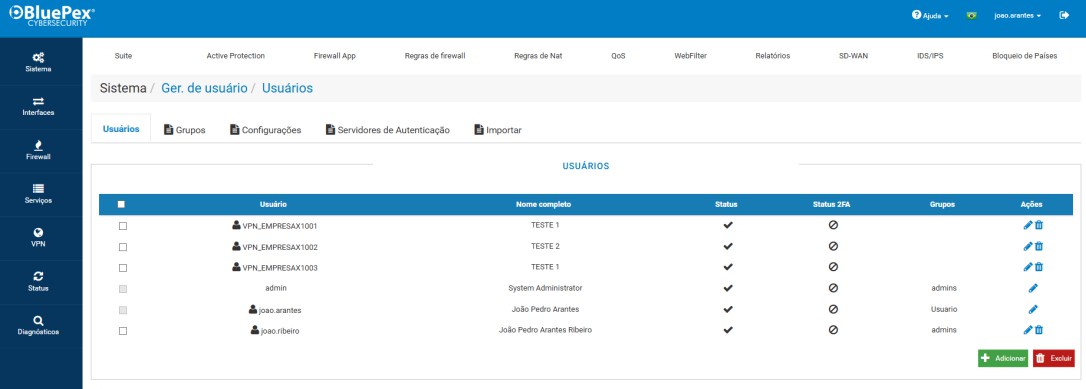
Essa etapa é fundamental para assegurar que apenas usuários autorizados tenham acesso à rede privada virtual, garantindo, assim, a integridade e a confidencialidade das informações trafegadas.

Figura 35 – Ger. de usuários 1



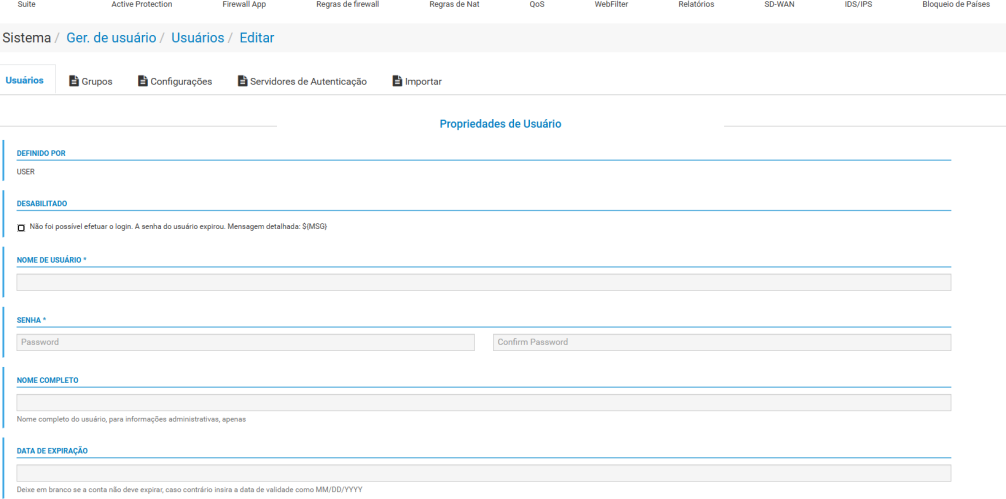
Fonte: BluePex Cloud

Figura 36 – Ger. de usuários 2

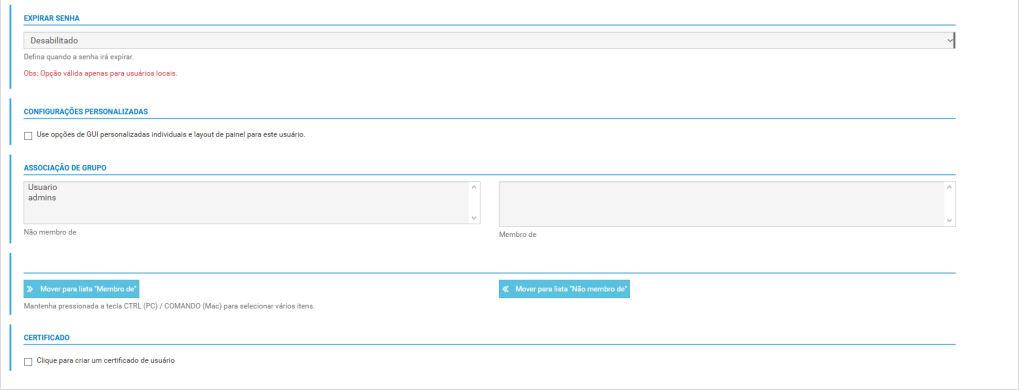


Fonte: BluePex Cloud

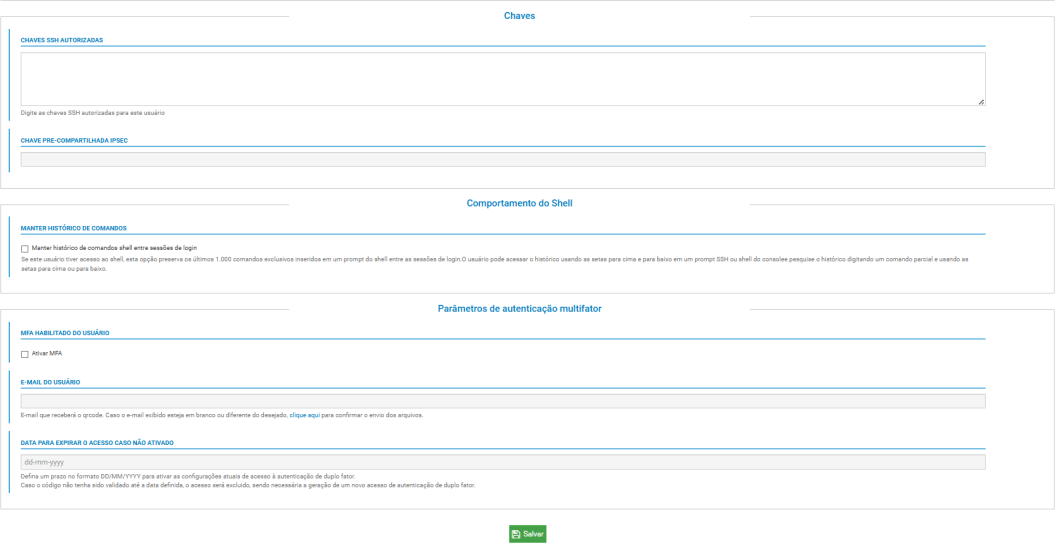
Figura 37 – Criação de Usuário 1



Fonte: BluePex Cloud Figura 38 – Criação de Usuário 2



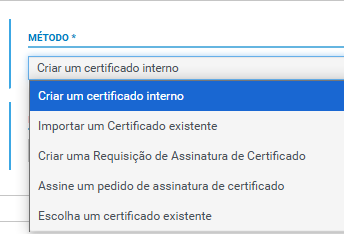
Fonte: BluePex Cloud Figura 39 – Criação de Usuário 3



Fonte: BluePex Cloud

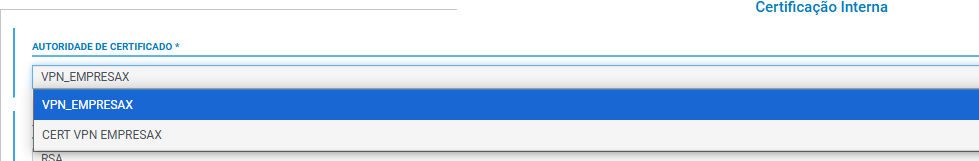
Aprofundando especificamente na etapa de seleção do certificado VPN para liberação do acesso do usuário, é fundamental atentar-se a dois elementos principais: o **método** e a **autoridade de certificado**.

Figura 40 – Método



Fonte: BluePex Cloud

Figura 41 – Autoridade de Certificado



Fonte: BluePex Cloud

Para a criação da Autoridade Certificadora, foi necessária a contratação de uma certificação VPN. Devido ao custo envolvido, optou-se pela utilização autorizada de uma estrutura pertencente a uma empresa terceirizada, cujos nomes foram omitidos para preservar aspectos legais. Realizou-se a simulação da configuração e conexão da VPN, a qual foi desfeita imediatamente após a elaboração deste trabalho, não gerando qualquer impacto nas atividades ou nos custos da empresa. Por esse motivo, a criação da Autoridade Certificadora não será apresentada neste documento, a fim de manter em sigilo os dados sensíveis envolvidos no processo.

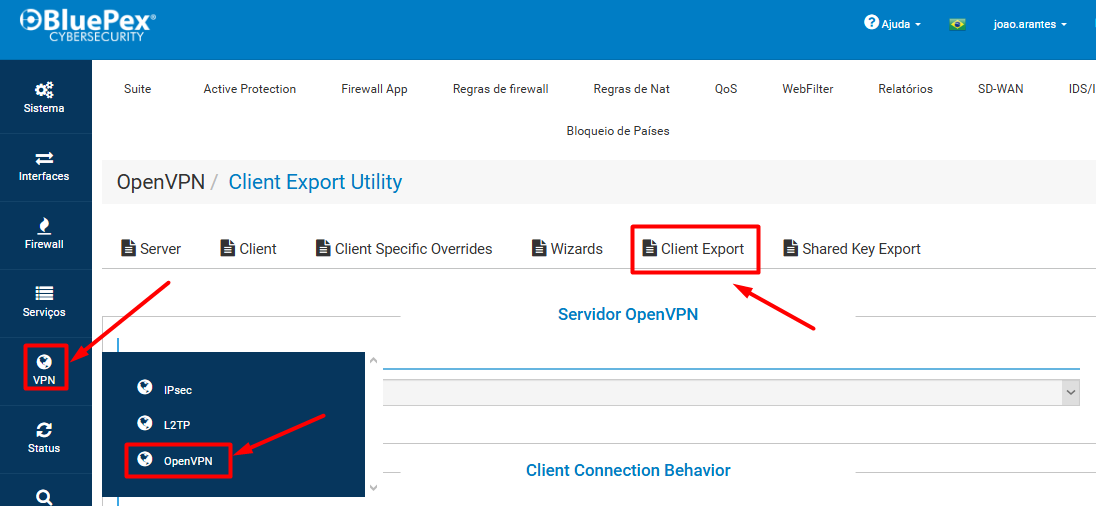
Com a criação do usuário concluída e o certificado digital devidamente atribuído, o próximo passo para finalizar a configuração da VPN consiste no acesso ao módulo de VPN dentro da plataforma. A partir desse ponto, deve-se navegar até as subcategorias previamente configuradas na seção **5.4.1 – Regras de Firewall**.

Dentro dessa estrutura, seleciona-se a opção **OpenVPN**, o que abrirá uma nova interface contendo diversas funcionalidades relacionadas à gestão da conexão VPN. Para os propósitos deste trabalho, é necessário acessar a subseção **Client Export**, cuja

função é permitir a exportação do certificado VPN correspondente ao usuário criado anteriormente.

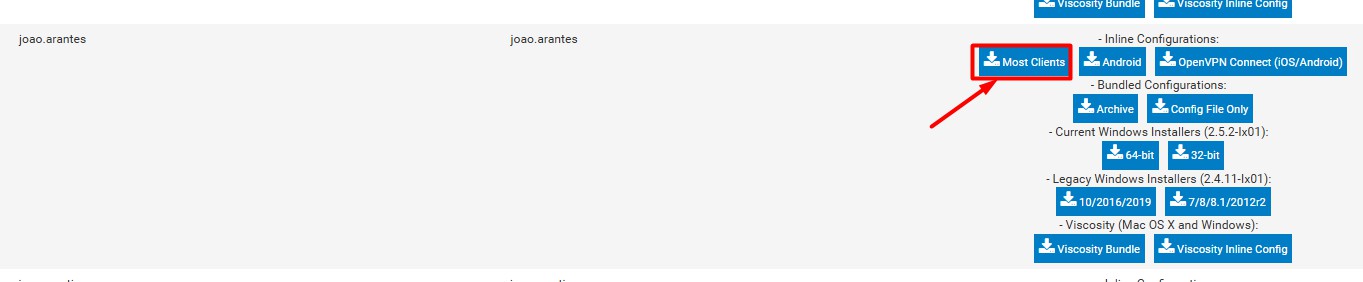
A exportação correta desse certificado é essencial para que o usuário consiga estabelecer a conexão com a rede privada virtual, utilizando as credenciais e configurações definidas previamente. Esse processo garante a autenticação segura e o controle de acesso aos recursos da rede.

Figura 41 – Certificação VPN



Fonte: BluePex Cloud

Figura 42 – Instalação do Certificado



Fonte: BluePex Cloud

Após a instalação do certificado digital e do aplicativo **OpenVPN Connect**, foi iniciado o procedimento de configuração da conexão. O primeiro passo consistiu em abrir o aplicativo e anexar o certificado previamente exportado. No entanto, ao realizar essa etapa, foi exibida uma mensagem de alerta informando que o arquivo possuía uma linha sem valor definido.

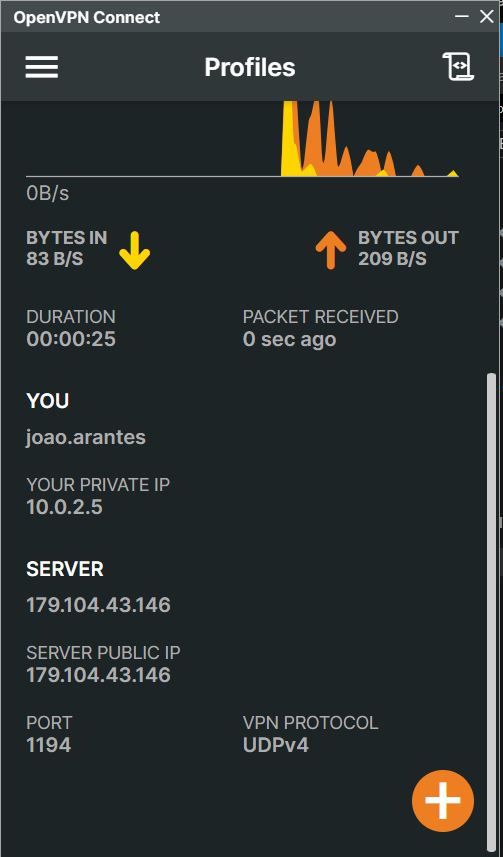
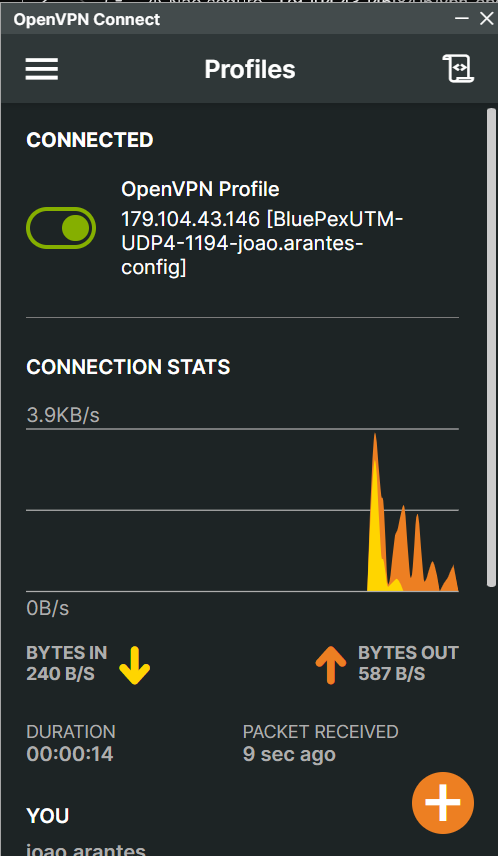
Para solucionar o problema, o certificado foi aberto com o editor de texto (Bloco de Notas), e a linha mencionada foi manualmente removida. Após a modificação, o arquivo foi salvo e novamente anexado ao aplicativo, que, desta vez, aceitou o certificado e prosseguiu para a solicitação das credenciais de autenticação (usuário e senha).

Contudo, ao tentar estabelecer a conexão, uma nova mensagem de alerta foi apresentada, indicando a presença de comandos obsoletos e outras linhas com

parâmetros não suportados no arquivo de configuração. Repetiu-se, então, o procedimento anterior: o arquivo foi reaberto como texto (.txt), as linhas incompatíveis foram removidas, e o conteúdo foi salvo.

Após essa última correção, a tentativa de conexão foi bem-sucedida, permitindo o estabelecimento de uma conexão VPN segura, validando, assim, todas as etapas de configuração e autenticação definidas no processo.

Figura 43 – Conexão VPN



Fonte: Tela do computador

# CONCLUSÃO

Chegando ao final deste trabalho, fica claro o quanto a segurança nas redes corporativas é um tema que não pode ser deixado de lado. Com a ajuda da plataforma BluePex, explorei como é possível proteger e gerenciar redes de forma prática e eficiente, especialmente em um mundo onde os ataques cibernéticos estão cada vez mais espertos e a digitalização não para de crescer. Esse estudo foi uma jornada para entender como ferramentas como firewalls e proteção de dispositivos podem fazer a diferença, garantindo que os dados de uma empresa estejam seguros, acessíveis e bem protegidos.

Misturando teoria, prática e um caso fictício, mergulhei nos quatro pilares da BluePex – segurança, controle, disponibilidade e conformidade – e vi como eles trabalham juntos para bloquear ameaças como ataques de negação de serviço, ransomwares e tentativas de phishing. No exemplo da Empresa X, configurei o BluePex 1500 e percebi na prática como ele organiza a rede, controla o tráfego, protege informações importantes e mantém tudo funcionando, mesmo com vários dispositivos e conexões de internet. Desde as regras de firewall até os serviços de

DHCP, DNS, NTP e VPN, a ferramenta mostrou ser uma aliada poderosa. E o melhor: ela ainda ajuda a cumprir leis como a LGPD e normas como a ISO/IEC 27001, com controles rigorosos e monitoramento constante.

Quando coloquei a BluePex lado a lado com outras soluções, como Splunk e SonicWall, ficou evidente que ela brilha pela simplicidade e pelo preço acessível, sendo perfeita para pequenas e médias empresas. Claro, o Splunk é incrível para grandes corporações que precisam de análises super detalhadas, mas a BluePex entrega um pacote completo, fácil de usar e com suporte em português, o que faz toda a diferença para quem não tem um time de TI gigante.

Esse trabalho reforça que investir em segurança cibernética não é só uma opção, mas uma necessidade. A BluePex não apenas protege contra riscos, mas também torna a gestão da rede mais tranquila, ajuda a seguir as leis e deixa a empresa mais preparada para os desafios do mundo digital. Espero que este estudo inspire outros profissionais a apostarem em soluções práticas e eficientes como essa. Quem sabe, no futuro, a gente possa explorar como a BluePex se sai em redes ainda mais complexas ou até com tecnologias novas, como inteligência artificial, para enfrentar as próximas gerações de ameaças cibernéticas. Por enquanto, fica a certeza: com as ferramentas certas, dá pra navegar no mundo digital com muito mais segurança!

# REFERÊNCIAS

COMER, D. E. *Computer Networks and Internets.* 6. ed. Pearson, 2014.

FOROUZAN, B. A. *Data Communications and Networking.* 5. ed. McGraw-Hill, 2012.

MINOLI, D. *Network Security: Private Communication in a Public World.* 2. ed. Wiley, 2002.

TANENBAUM, A. S. *Redes de Computadores.* 5. ed. Pearson, 2010.

KUROSE, J. F.; ROSS, K. W. *Computer Networking: A Top-Down Approach*. 7ª ed. Pearson, 2016.

STALLINGS, W. *Data and Computer Communications*. 10ª ed. Pearson, 2014.

CERT.br. **Cartilha de Segurança para Internet**. Disponível em: [https://cartilha.cert.br](https://cartilha.cert.br/). Acesso em: 19 nov. 2024.

BLUEPEX. **Universidade BluePex**. Disponível em: [https://universidade.bluepex.com](https://universidade.bluepex.com/). Acesso em: 19 nov. 2024.

BLUEPEX. **BluePex**. Disponível em: [https://bluepex.com.br](https://bluepex.com.br/). Acesso em: 19 nov. 2024.

SPLUNK. *Splunk Enterprise*. Disponível em: [https://www.splunk.com](https://www.splunk.com/). Acesso em: 19 nov. 2024.

MITRE ATT&CK. *Splunk: Applying Advanced Analytics for Threat Detection*. Disponível em: [https://www.mitre.org](https://www.mitre.org/). Acesso em: 19 nov. 2024.

SONICWALL. *SonicWall Next-Generation Firewalls*. Disponível em: [https://www.sonicwall.com](https://www.sonicwall.com/). Acesso em: 19 nov. 2024.

GARTNER. *Magic Quadrant for Network Firewalls 2024*. Disponível em: [https://www.gartner.com](https://www.gartner.com/). Acesso em: 19 nov. 2024.

CERT.BR. *Cartilha de Segurança para Internet*. Disponível em: [https://cartilha.cert.br](https://cartilha.cert.br/). Acesso em: 19 nov. 2024.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 21 abr. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC*

*27001:2022 – Tecnologia da informação – Segurança da informação, cibersegurança e proteção da privacidade – Sistemas de gestão da segurança da informação – Requisitos*. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC*

*27002:2023 – Tecnologia da informação – Segurança da informação, cibersegurança e proteção da privacidade – Controles de segurança da informação*. Rio de Janeiro: ABNT, 2023.

BRASIL. MINISTÉRIO DA DEFESA. *Empresas Estratégicas de Defesa – EED*. Brasília, DF: Ministério da Defesa, [s.d.]. Disponível em: [https://www.gov.br/defesa/pt-](https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/eed) [br/assuntos/industria-de-defesa/eed](https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/eed). Acesso em: 21 abr. 2025.

**OPENVPN.** OpenVPN Client. Disponível em: <https://openvpn.net/client/>. Acesso em: 8 maio 2025.

CHECK POINT. **Cyber Security Report 2024.** Disponível em: <https://www.checkpoint.com/cyber-security-report/>. Acesso em: 8 mai. 2025.

FORTINET. **FortiGate next-generation firewalls.** Disponível em: <https://www.fortinet.com/products/next-generation-firewall>. Acesso em: 8 mai. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC**

**27005:2022: Information security risk management.** Geneva: ISO, 2022.

NIST. **Framework for improving critical infrastructure cybersecurity.** Gaithersburg: National Institute of Standards and Technology, 2018. Disponível em: [https://www.nist.gov/cyberframework.](https://www.nist.gov/cyberframework) Acesso em: 8 mai. 2025.

OWASP. **OWASP Top Ten.** Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 8 mai. 2025.

ROSSI, L. D.; OLIVEIRA, A. L. **Cibersegurança no Brasil: desafios e oportunidades na era digital.** São Paulo: Elsevier, 2023.

SCHNEIER, B. **Click here to kill everybody: security and survival in a hyper- connected world.** New York: W.W. Norton & Company, 2018.