**RELATÓRIO FINAL**

UMA NOVA ABORDAGEM DE PROTEÇÃO DE RECURSOS DE REDE DE COMPUTADORES BASEADA EM PERÍMETRO DEFINIDO POR SOFTWARE.

Altair Olivo Santin

Curitiba

2022

JHONATAN FARIAS DE LIMA

Altair Olivo Santin

Tecnólogo em segurança da informação – ep

BOLSA CNPq

UMA NOVA ABORDAGEM DE PROTEÇÃO DE RECURSOS DE REDE DE COMPUTADORES BASEADA EM PERÍMETRO DEFINIDO POR SOFTWARE

Relatório Final apresentado ao Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico e Inovação (PIBITI), Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação da Pontifícia Universidade Católica do Paraná.

Orientador: Prof. Dr. Altair Olivo Santin.

curitiba

2022

resumo

**Introdução**: Um perímetro definido por software (SDP) tem como objetivo basear toda a proteção de um determinado perímetro de rede em software e sistemas lógicos, consistindo seu funcionamento basicamente em ocultar a infraestrutura de forma que somente quem tem os devidos acessos, passando por critérios de segurança como provedores de identidade e componentes lógicos do perímetro, pode visualizar e se conectar aos recursos da rede. **Objetivo:** Busca-se pela melhor maneira para aplicar de forma prática o conceito de um perímetro definido por software. **Materiais e Métodos**: A principal solução usada para testes durante o período do projeto foi a ofertada pela empresa Twingate, um recurso que permite fazer o gerenciamento de ativos de rede baseando sua segurança em perímetro definido por software. **Resultados**: Os resultados obtidos foram promissores, a solução escolhida é de fácil manuseio e permite a aplicação de uma forma pratica o conceito de SDP, possibilitando assim o gerenciamento de acessos aos recursos computacionais em redes de computadores. **Conclusão:** Este trabalho contribui para o desenvolvimento de ferramentas e métodos voltados a segurança computacional, principalmente ao que se diz respeito a segurança de recursos computacionais em redes de computadores.

**Palavras-chave**: *Perímetro definido por software, Segurança computacional, Recursos computacionais, Redes de computadores.*

Lista de figuras

FIGURA 1 - Modelo ilustrativo da arquitetura castelo e fosso...................................17

FIGURA 2 – Estrutura de funcionamento de uma rede ZTNA...................................22

FIGURA 3 - Modelo lógico de uma arquitetura SDP..................................................23

FIGURA 4 – Exemplo de perimetro Twingate............................................................25

FIGURA 5 - Exemplificação do perimetro criado para testes.....................................26

FIGURA 6 - Imagem da pagina web usada para testes no servidor local.................27

FIGURA 7 - Regras de entrada no servidor AWS......................................................27

FIGURA 8 - Imagem da pagina web usada para testes no servidor EC2 AWS.........28

FIGURA 9 - Restrição de protocolos de acesso aos recursos Twingate...................28

FIGURA 10 - Imagem da rede AWS configurada com o recurso Web......................29

FIGURA 11 - Imagem das permições de acesso a rede............................................29

FIGURA 12 – Soluções para implementação de Connectors....................................30

FIGURA 13 – Execução do processo do componete connector................................31

FIGURA 14 - Status do componente connector.........................................................31

FIGURA 15 - Provedores de identidade (IDP)...........................................................32

FIGURA 16 - Software cliente usado para conexão no perimetro Twingate.............33

FIGURA 17 - Cliente Twingate para dispositivos moveis..........................................33

Lista de abreviaturas OU siglas

SDP - Software Defined Perimeter

AWS - Amazon Web Services

VPN - Virtual Private Network

IDS - Sistema de Detecção de Intrusos

IPS - Intrusion Prevention System

ZT - Zero Trust

BYOD - Bring your own device

EC2 - Amazon Elastic Compute Cloud

ZTNA - Acesso de confiança zero à rede.

LAN - Local área network.

SUMÁRIO

1. INTRODUÇÃO....................................................................................................................16
   1. REVISÃO DE LITERATURA .......................................................................................17
      1. ARQUITETURA CASTELO E FOSSO............................................................17
      2. PERÍMETRO DEFINIDOS POR SOFTWARE E ZERO TRUST.....................18
      3. ZTNA X VPN....................................................................................................21
      4. CONEXÃO E DESENHO DA ARQUITETURA SDP........................................22
2. OBJETIVOS........................................................................................................................24
   1. OBJETIVO GERAL.......................................................................................................24
3. MATERIAIS E MÉTODO......................................................................................................24
4. RESULTADOS.....................................................................................................................26

### IMPLEMENTAÇÃO DO PERÍMETRO TWINGATE..................................26

* 1. ACESSO AO PERIMETRO TWINGATE.......................................................................32

1. DISSCUÇÃO........................................................................................................................34
2. CONSIDERAÇÕES FINAIS.................................................................................................35
3. OUTRAS ATIVIDADES REALIZADAS.................................................................................36
4. REFERENCIAS....................................................................................................................37

# INTRODUÇÃO

O termo "Zero Trust" foi cunhado por um analista da Forrester Research Inc. em 2010, quando o modelo para o conceito foi apresentado pela primeira vez. Alguns anos mais tarde, o Google anunciou que havia implementado a segurança Zero Trust em sua rede, o que levou a um interesse crescente pela adoção desse modelo dentro da comunidade tecnológica (CloudFlare - 2022).

A premissa de arquitetura de rede corporativa tradicional é criar uma rede interna separada do mundo externo por um perímetro fixo, que consiste em uma série de funções de firewall que bloqueiam usuários externos de entrar, mas permitir que usuários internos saiam. Os perímetros fixos tradicionais permitiam que serviços internos permaneçam protegidos de ameaças externas por vários anos devido às características poderosas, mas simples, de bloqueio a visibilidade e a acessibilidade de fora do perímetro para aplicativos internos e a infraestrutura. Mas o modelo de perímetro fixo tradicional está se tornando rapidamente obsoleto devido ao BYOD (Bring your own device) e aos ataques de Phishing que fornecem acesso não confiável dentro do perímetro e SaaS (Software as a Service) e IaaS (infrastructure as a service) alterando a localização do perímetro (CSA - 2013).

O surgimento desse contexto junto ao crescimento exponencial de novos usuários na internet e das novas tecnologias surgindo no mercado, como a computação em nuvem, rompeu a ideia de segurança para os ativos na rede e trouxeram com sigo grandes desafios e preocupações para a segurança e privacidade de recursos na internet. Com essa visão, em dezembro de 2013 a empresa Cloud Security Aliance (CSA) publicou um artigo intitulado: “Software Defined Perimeter”, introduzindo assim um modelo de segurança que prometia proteger ativos independente do lugar onde precisem ser armazenados ou acessados, para isso adotava medidas de Zero Trust tendo como principal filosofia o conceito de “nunca confie, sempre verifique”, atuando assim com fortes exigências na autenticação dos dispositivos e de usuários, além de sempre trabalhar com privilégios mínimos nos acessos. Essa então seria a evolução na forma de proteção de recursos computacionais em redes de computadores, resolvendo assim os problemas de acesso seguro a infraestrutura.

Por fim, após a difusão do conceito apresentado pela CSA, várias adaptações ao longo do tempo se aproveitaram da flexibilização na arquitetura inicialmente proposta para se adequar a realidade de cada situação de uso. Sendo assim, explorando diferentes maneiras para aplicação, o conceito de perímetros definidos por software vem sendo cada vez mais visado para proteção e gerenciamento de recursos computacionais.

## **REVISÃO DE LITERATURA**

### ARQUITETURA CASTELO E FOSSO:

O modelo de segurança de rede castelo e fosso é o método mais tradicionalmente usado para proteção de recursos computacionais. Seguindo a analogia, a definição do perímetro em questão seria o fosso em volta do castelo que o protege de invasões, e o castelo seria onde estariam todos os ativos a serem protegidos, seguindo assim a filosofia: “tudo dentro é amigo e tudo fora é inimigo”.

Para acessar a parte de dentro do castelo é preciso então usar uma ponte levadiça, no caso uma VPN (Virtual Private Network) trabalhando em conjunto com sistemas de barramento físicos (Exemplo: portas de acesso) e outros produtos de segurança usados para proteção do perímetro, só então o usuário finalmente tem acesso aos dispostos dentro da rede e pode acessar todos os dados e sistemas contidos nela.

Figura 1 – Modelo ilustrativo da arquitetura castelo e fosso.

Diagrama, Desenho técnico

Descrição gerada automaticamente

Fonte: Cloudflare, 2022 (adaptado).

Porém a algumas considerações sobre essa abordagem, uma delas é o fator humano, mais precisamente em ataques de Phishing por exemplo, já que a rede não confia no seu exterior, uma maneira de burlar a segurança seria recebendo um ‘convite’ do interior da rede, assim sendo possível entrar sem mesmo ter credenciais de acessos próprias, já que possui uma permissão de dentro da rede considerada então como segura, levando assim a maior falha dessa abordagem, como descrito pela empresa CloudFlare.

“A maior falha de segurança é que, se um invasor obtiver acesso à rede — se cruzar o "fosso" — também poderá acessar quaisquer dados e sistemas dentro dela. Eles podem violar a rede [roubando credenciais do usuário](https://www.cloudflare.com/learning/access-management/phishing-attack), explorando uma vulnerabilidade de segurança, introduzindo uma infecção de [malware](https://www.cloudflare.com/learning/ddos/glossary/malware/) ou realizando um [ataque de engenharia social](https://www.cloudflare.com/learning/security/threats/social-engineering-attack), entre outros métodos.”(CloudFlare2022).

Outro ponto sobre essa abordagem seria a atual descentralização dos recursos de redes de computadores, seguindo a rápida popularização do armazenamento em nuvem os perímetros antes centralizados agora estão distribuídos por toda a internet, dificultando essa abordagem tradicional de segurança, seguindo a analogia descrita pela empresa CloudFlare (2022)” [...] não faz sentido colocar todos os recursos na defesa do castelo se a rainha e sua corte estão espalhados pelo campo”.

### PERÍMETRO DEFINIDOS POR SOFTWARE E ZERO TRUST:

A arquitetura de perímetro definido por software, em forma abreviada SDP, foi baseada no modelo de segurança Zero Trust (ZT), sendo uma evolução dos métodos tradicionais de segurança de rede que surgiu para acompanhar as atuais mudanças físicas e logicas nos perímetros de rede, sendo assim uma resposta as tendencias de BYOD, migração dos ativos armazenados fisicamente em sistemas próprios para o armazenamento em nuvem e abrangendo também os acessos que ocorrem fora de um determinado perímetro físico, como por exemplo em casos de home office.

As Arquiteturas SDP e ZT, tem ambas como base o seu controle de acesso a solução de ZTNA, que é um modelo de segurança de ti que assume que as ameaças estão presentes dentro e fora do uma rede. Consequentemente, requerendo uma verificação estrita para cada usuário e cada dispositivo antes de autorizar sua comunicação e permanência dentro da rede. Além disso, para garantir a segurança da rede, o ZTNA trabalha de forma a ocultar todo seu perímetro, assim somente quem tem a devida permissão e conhecimento de tal ativo pode se conectar à rede.

Sendo assim, modelos que também trabalham independentemente da localização dos dispositivos, trazendo medidas de segurança bem mais rigorosas para acessos, baseando sua lógica de validação no usuário, no dispositivo e no recurso alvo do acesso, deixando de lado as tratativas de forma implícita da validação dos acessos aos ativos independentemente se o usuário já estiver dentro da rede, vigorando assim sua filosofia de “nunca confie sempre verifique”, baseando-se em seis princípios básicos que são aplicados não só no início da conexão, mas também durante toda a comunicação e permanência do dispositivo na rede:

* Monitoramento e validação contínua:

Mesmo após o acesso a rede, deve se levar em conta os privilégios de acesso previamente atribuídos ao usuário, porém ainda sim logins e conexões expiram periodicamente necessitando de uma nova autenticação do usuário, assim sendo continuamente validada sua identidade.

* Último privilégio:

Outro princípio seria o acesso com privilégios mínimos, isso quer disser dar acesso ao usuário somente a áreas necessárias para uso, minimizando assim a exposição da rede.

* Controle de acesso ao dispositivo:

Além de controlar o acesso de usuários na rede, o modelo de segurança zero verifica também os dispositivos, suas autorizações e ainda executa checagens de saúde, podendo colocá-lo em quarentena caso necessário, impedindo assim o acesso a rede por meio deste.

* Micro segmentação:

Esse princípio divide todos os perímetros da rede em pequenas zonas de segurança mantendo-as separadas, assim mesmo tendo acesso a uma

determinada área, ainda só será possível acessar uma segunda passando pelos processos de segurança e validação da rede novamente.

* Prevenção de movimentos laterais:

Após obter acesso a rede o atacante tentará se mover para outras áreas em busca de mais privilégios, o modelo de segurança zero é projetado para prevenir isso, pois como sendo a rede segmentada o atacante não poderá se mover lateralmente, uma vez que para isso, deverá passar pelos níveis de validação do segmento de acesso. Além disso, assim que identificado sua presença na rede na tentativa de movimentação lateral, medidas como a de quarenta do dispositivo e do usuário serão tomadas, impossibilitando assim o acesso posterior dos mesmos a rede.

* Autenticação multifator:

Exigir apenas uma evidência para autenticação dos usuários e dispositivos não é suficiente para o modelo de segurança zero, além de tudo é necessário alternativas como validação de códigos enviados por SMS (Tokens) e validação da localização (GPS) dos dispositivos por exemplo, para só então a autenticação deles na rede.

Por fim o modelo de perímetro definido por software requer uma rigorosa verificação de identidade para cada tentativa de acesso aos recursos de rede que ele abrange, independente da origem da tentativa estar fora ou dentro da rede já com acesso a alguns recursos.

**1.1.3 ZTNA x VPN:**

As redes baseadas no modelo ZTNA se diferenciam das convencionais VPNs em vários aspectos, tais como, o de permissões após o acesso na rede, uma vez que um usuário acessa um VPN, ele tem então acesso a todos os ativos dentro da rede. Já em redes baseadas em ZTNA, é apenas concedido acesso ao aplicativo específico solicitado e negado o acesso aos outros ativos dentro da rede por padrão, assim sempre considerando que um cibe ataque possa vir não só de fora da rede, mas de dentro dala também, como por exemplo em ataques de Insiders, ou seja uma pessoa que tem acesso as informações de dentro da rede e as usa de forma ilegal para vantagem pessoal.

Ademais existem também diferenças técnicas dentre as duas técnicas, sendo as principais que as VPNs comumente são executadas por meios do protocolo IPec, rodando assim na terceira camada, camada de rede no modelo OSI. Já em redes ZTNA normalmente operam em nível de aplicativo, assim sendo na sétima camada do modelo OSI, dessa maneira a rede ZTNA fornece criptografia de ponta nas conexões entre os dispositivos, ou seja, em um par, o que é diferente do protocolo IPsec que fornecera o acesso criptografado a toda uma LAN de uma só vez, dento assim o usuário acesso a todos os IPs da rede.

Além da disparidade de hardware, onde as VPNs geralmente exigem o uso de servidores locais e que os dispositivos sejam conectados a esses servidores, passando assim todas as conexão pelo [firewall](https://www.cloudflare.com/learning/security/what-is-a-firewall/) da organização, na rede ZTNA esse controle é feito em nuvem, não se limitando ao local de acesso na questão de performance da conexão e ainda exigindo bem menos poder computacional, já que todo o esforço que a rede precisa fazer é gerenciar as permissões de conexão e apontar o destino final para os dispositivos.

Por fim as VPNs são imprecisas e relaxadas na verificação interna na rede, trabalhando todos os usuários e dispositivos da mesma forma após a conexão, sem nenhum tipo de validação posterior a conexão que aja de forma preventiva.

Diagrama

Descrição gerada automaticamenteFigura 2 – Estrutura de funcionamento de uma rede ZTNA.

Fonte: CloudFlare(2022).

### 1.1.4 CONEXÃO E DESENHO DA ARQUITETURA SDP:

A arquitetura SDP possui dois principais componentes, o controlador que é responsável pela validação e autenticação do cliente por meio de provedores de identidade (IDP), tabelas IP e tabelas de endereços físicos dos dispositivos (MAC Adress), a verificação de infecções por malwares e softwares desatualizados nos dispositivos, além disso é nele que ficam armazenados as autorizações de acesso de cada usuário na rede. O segundo componente da rede é o Gateway, responsável por estabelecer de fato as conexões entre o cliente e o ativo almejado, usando para isso técnicas de criação de sub-redes e tunelamento com TLS mútuo entre as partes.

Figura 3 – Modelo lógico de uma arquitetura SDP.Diagrama

Descrição gerada automaticamente

*Fonte: O autor (2022).*

Para realizar a conexão entre um cliente e um ativo usando a arquitetura SDP alguns passos devem ser seguidos:

1) o cliente envia uma solicitação ao controlador, passando pelo provedor de identidade (IDP) para validação do usuário e pelos filtros de endereços IP e MAC para validar também o dispositivo de acesso que já deve estar cadastrado na base de dados;

2) em seguida é enviado ao usuário a localização do Gateway da rede junto a um token de acesso único contendo os dados do usuário e seus acessos permitidos dentro da rede;

3) após o gateway recebe o token do usuário, ele será o responsável por abrir ou não a conexão, para isso é requisitado e validado os certificados digitais tanto do cliente quanto da aplicação que ele pretende acessar;

4) somente após essa autenticação de TLS mútua é então estabelecido uma conexão em uma sub-rede usando tunelamento que será única e de acesso restrito entre o usuário e o recurso almejado, dessa forma as partes da conexão não ficam conectadas a uma rede maior e para mudar de ativo ou área dentro da rede o usuário precisa passar por todo o processo de autenticação novamente;

5) Por fim é estabelecido uma linha de comunicação entre controlador, gateway e o usuário da rede, onde acontecera as verificações de segurança e checagem da saúde da conexão durante o processo.

# OBJETIVOS

## **Objetivo geral**

Esse projeto possuirá como objetivo, buscar e encontrar pela melhor maneira para aplicar de forma prática o conceito de um perímetro definido por software (SDP), em testes que serão realizados no decorrer e estudos de casos reais de aplicações do conceito.

# MATERIAIS E MÉTODO

A principal solução usada para testes durante o período do projeto foi a disponibilizada pela empresa Twingate, um recurso de fácil manuseio que permite fazer o gerenciamento de ativos na rede usando os princípios de um perímetro definido por software.

Com isso foi possível montar um perímetro virtual que contenha todos os ativos necessários, mesmo eles estando em diferentes lugares de hospedagem, em nuvem ou em servidores locais por exemplo. Para isso é criado um perimetro Twingate, a adicionado todas as redes que contenhão os recursos computacionais protegidos.

Figura 4 – Exemplo de perimetro Twingate.

Interface gráfica do usuário, Diagrama, Aplicativo

Descrição gerada automaticamente

*Fonte: O autor (2021).*

Apesar de ser relativamente nova no mercado a Twingate foi fundada em 2019 com a premissa de garantir o acesso segura a recursos, e já se destaca nesse eixo com suas propostas de soluções, tendo apoio de grandes investidores por todo o globo como por exemplo a SignalFire, Green bay ventures (GBV) e a 8VC.

“Começamos a construir o Twingate em 2019 para resolver os desafios que todas as empresas enfrentam para garantir o acesso aos recursos. Apesar das grandes mudanças na forma como usamos a tecnologia nos últimos 30 anos, o modelo de controle de acesso no qual a maioria das empresas confia é frustrantemente arcaico”. (Twingate, 2022).

Desse modo, o acesso ao perimetro de rede Twingate segue com pequenas diferenças da forma inicialmente proposta pela CSA, para melhor adaptação da arquitetura nos cenarios de uso propostos pela solução, a principal mudança na estrutura é a junção do controlador e gateway do perimetro de rede em um único componente: Connector. Assim tudo começa apartir de um software cliente do lado do usuario, o qual faz a autenticação com um provedor de identidade (IDP) a escolha, e estabelece uma conecção inicial com o connector, depois disso é possivel ver os ativos dentro das redes que estão no perimetro e conectar-se a eles, seguindo as permições de conexão já determinadas pelo administrador do perimetro na plataforma, validando então se o dispositivo e usuarios podem acessar determinada área.

# RESULTADOS

Os resultados obtidos foram promissores, a solução escolhida é de fácil manuseio e permite a aplicação de uma forma pratica o conceito de um perímetro definido por software, possibilitando assim o gerenciamento de acessos aos recursos computacionais em redes de computadores.

## **Implementação do perímetro Twingate.**

O primeiro passo para implementação da solução foi criar um perimetro de rede geral no twingate, e em seguida adicionar as redes externas onde estão os recursos a serem protegidos, no caso dos testes foi usado um rede local, não exposta para internet, e uma instância EC2 da AWS, ambos com uma aplicação web rodando.

Figura 5 – Exemplificação do perimetro criado para testes.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

*Fonte: O autor (2021).*

Figura 6 – Imagem da pagina web usada para testes no servidor local.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

*Fonte: O autor (2021).*

Além disso, as regras de rede do servidor AWS, tanto de entrada como de saída de dados, devem ser configuradas de forma que sejam de acesso exclusivo do IP onde será implementado o Connector da rede Twingate, trazendo assim o conceito da rede oculta, onde só o Connector deve conhecer a rede e conseguir estabelecer a conexão com sucesso.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamenteFigura 7 – Regras de entrada no servidor AWS

*Fonte: O autor (2021).*

Figura 8 – Imagem da pagina web usada para testes no servidor EC2 AWS.

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

*Fonte: O autor (2021).*

Após adicionada as redes (AWS e Local) é possível especificar então os seus recursos, podendo também bloquear ou restringir o uso de alguns protocolos de rede na hora da conexão, restringindo assim o tipo de tráfego de rede aceitável pelo recurso.

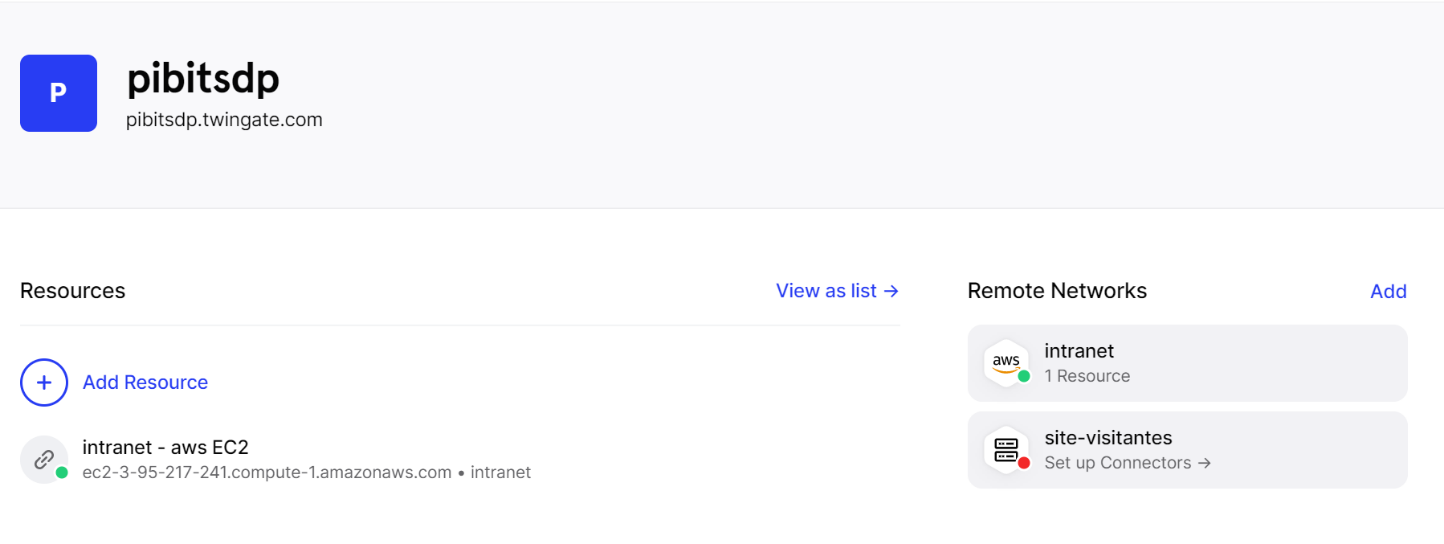
Figura 9 - Restrição de protocolos de acesso aos recursos Twingate.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

*Fonte: Twingate (2022)*

Figura 10 – Imagem da rede AWS configurada com o recurso Web.



*Fonte: Twingate (2022).*

Depois de adicionada ao perimetro, cada rede dentro do twingate tem seu proprio componente chamado de connector que exerce as funções do Controlador (Controller) e do Gateway (Relay) de uma arquitetura SDP, sendo assim responsavel pela validação, autenticação do usuario e do trafego de rede, alem de estabelecer a cominicação entre o usuario e o recurso desejado dentro da rede, levando em conta as permições de acesso do usuario concedidas e geranciadas na propria aplicação do Twingate.

Figura 11 – Imagem das permições de acesso a rede.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

*Fonte: Twingate (2022).*

A implementação do connector é possivel de varias maneira diferentes, desde soluções On primisse, Docker, em nuvem, etc. Alem da possibilidade das adições de vários conectores diferentes há rede, para que aja assim uma redundância no acesso aos recursos caso um conector venha falhar, ou se o volume das conexões for maior do que o esperado saturando assim o componente, levando a um balanceamento automático das conexões na rede.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamenteFigura 12 - Soluções para implementação de Connectors.

*Fonte: Twingate (2022).*

O componente connector deve ser aplicado e administrado pelo dono do perimetro, para isso é possivel ser aplicado em varios cenarios como no caso dos testes realizados, em uma maquina linux local. A instalação do Connector é bem simples e ocorre com um único comando (curl <https://binaries.twingate.com/>connect

or/setup.sh" | Sudo TWINGATE\_ACCESS\_TOKEN="..."TWINGATE\_REFRESH\_

TOKEN="..." TWINGATE\_URL="https:// <YOUR TWINGATE SUBDOMAIN>

.twingate.com" bash), e então o serviço começa rodar em Background na máquina. (Figuras 11 e 12).

Figura 13 – Execução do processo do componete connector.

Uma imagem contendo Calendário

Descrição gerada automaticamente

*Fonte: O autor (2022).*

Texto

Descrição gerada automaticamente com confiança médiaFigura 14 – Status do componente connector.

*Fonte: O autor (2022).*

Por padrão o Connector já é iniciado com a máquina e não necessita de configurações adicionais, sendo assim bastando estar a máquina ligada e com recursos de rede e processamento suficientes, que dependerão de cada caso específico de uso.

## **Acesso ao perimetro Twingate:**

Finalmente o acesso ao perimetro de rede do Twingate segue com pequenas diferenças da formar já citado no capitulo 3.3, para melhor adaptação da arquitetura nos cenarios de uso propostos pela solução, sendo a principal mudança a junção do controlador e gateway do perimetro de rede em um único componente (Connector).

Assim tudo começa apartir de um software cliente do lado do usuario, o qual faz a autenticação com um provedor de identidade (IDP) a escolha, e estabelece uma conecção inicial com o connector, depois disso é possivel ver os ativos dentro das redes que estão no perimetro e conectar-se a eles, seguindo as permições de conexão já determinadas pelo administrador do perimetro na plataforma, validando então se o dispositivo e usuarios podem acessar determinada área (Capitulo 5.1). (Figuras 13 e 14).

Figura 15 – Provedores de identidade (IDP).

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Fonte: Twingate (2022).

Figura 16 – Software cliente usado para conexão no perimetro Twingate.

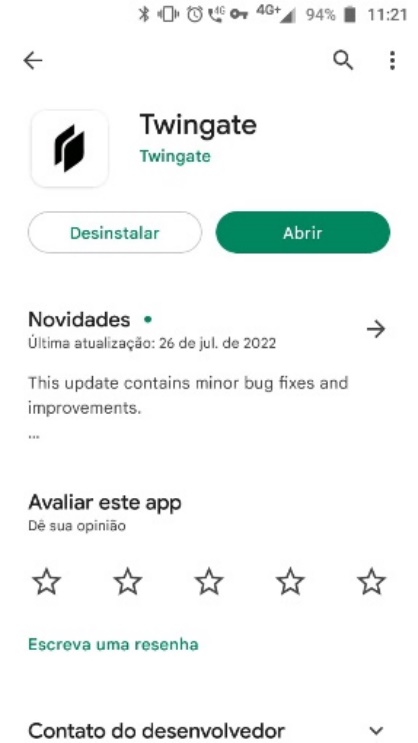
Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Fonte: O autor (2022)*.*

Alem disso, o Twingate tem grande suporte para dispositivos moveis como smartphones e tablets. Assim o perímetro criado pode ser acessado através do celular se limitações de recursos, apenas baixando o cliente Twingate na loja do dispositivo.

Figura 17 – Cliente Twingate para dispositivos moveis.

 Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Fonte: O autor (2022)*.*

# DISCUSSÃO

Os resultados obtidos com os testes e estudos realizados na plataforma Twingate durante o período da pesquisa, evidenciam o grande potencial da nova abordagem de proteção de recursos computacionais em redes de computadores baseada em perímetro definido por software, a qual diferente das mais comumente usadas até então, como a arquitetura de castelo e fosso, essa nova abordagem traz mais segurança em questões de BYOD, home office e para a computação em nuvem.

Além de deixar claro outros aspectos com a facilidade de uso da arquitetura, sua versatilidade para melhor adaptação a realidade aplicada, e a agilidade na proteção de recursos computacionais em sua migração para a nuvem, visando todos os quesitos de segurança necessários. Além da sua adaptação para dispositivos moveis como smartphones, expandindo os horizontes da tecnologia e mostrando que confiança pode e deve existir em todos os lugares.

# CONSIDERAÇÕES FINAIS

Pelo que os indícios apontam a abordagem de proteção de redes de computadores vai sofrer uma mudança muito em breve, adotando como principal técnica, a arquitetura de perímetro definido por software.

A Twingate é uma empresa relativamente nova no mercado, porém deixa bem claro todo o seu potencial, e evidência também todo o potencial da arquitetura de perímetro definido por software, que apesar de ter sido criada e discutida a algum tempo atras, vem se destacando cada vez mais no mercado com o crescimento da necessidade de as pessoas estarem conectadas.

# OUTRAS ATIVIDADES REALIZADAS

Reuniões nas quartas-feiras em um grupo fechado no Teams para os alunos dedicados ao PICBIC, como também mestrado e doutorado em conjuntos dos orientadores. Este era o momento para relatar o que foi realizado durante a semana, novas ideias eram sugeridas assim como novos objetivos a serem realizadas para o próximo encontro.

Além das reuniões semanais, eventualmente me reunia com o meu orientador para tirar algumas dúvidas e alinhar os objetivos do projeto.

# REFERÊNCIAS

CSA, CLOUD SECURITY ALIANCE. Introduction. **Software Defined Perimer**. p.5. Dec. 2013. Disponível em: <https://encurtador.com.br/bxFX3>. Acesso em: 19 Jan. 2022.

TWINGATE. **How Twingate Works**. Disponível em: <https://docs.twingate.com/docs>. Acesso em: 19 Jan. 2022.

CLOUDFLARE. **Mutual TLS**. Disponível em: <https://developers.cloudflare.com/cloudflare-one/identity/devices/mutual-tls-authentication>. Acesso em: 19 Jan. 2022.

CLOUDFLARE. **Segurança Zero Trust | O que é uma rede Zero Trust?**. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-zero-trust/>. Acesso em: 25 Jan. 2022.

CLOUDFLARE. **What is the castle-and-moat network security model?.**

Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/castle-and-moat-network-security/>. Acesso em: 25 Jan. 2022.