# Uso de Software-Defined Perimeter (SDP) e Virtual Desktop Infrastructure (VDI) como estratégias para aprimorar a segurança em atividades de home office[1]

*José Thiago Fredenhagem Filho*

Técnico do MPU em Tecnologia da Informação e Comunicações, lotado na PRM de Ribeirão Preto-SP. Especialista em Infraestrutura de TI pela Universidade Federal de São Carlos (UFSCar). Especialista em Gestão Pública pela UFSCar. MBA em Governança de TI pelo Centro Universitário Unieuro (DF). Bacharel em Sistemas de Informação.

**Resumo:** A adoção do sistema de trabalho remoto por diversas organizações tem suscitado discussões sobre a segurança do acesso às redes corporativas e seus recursos, bem como sobre o uso de dispositivos não gerenciados nesse processo. O presente artigo apresenta brevemente as tecnologias *virtual desktop infrastructure* e *software-defined perimeter* e avalia se, pelas suas características, a adoção de ambas pode mitigar os danos de segurança decorrentes do trabalho remoto. Os resultados demonstram que a adoção conjunta pode minimizar os danos de ataques, sobretudo porque, além de uma boa tecnologia, é necessário que haja uma estratégia de segurança e política adequada ao contexto.

**Palavras-chave:** perímetro definido por software; infraestrutura de desktop virtual; virtualização; segurança de rede.

movimentação lateral e varredura da rede causados por um invasor que acesse a rede por meio de uma VPN. 5 Conclusão.

## 1 Introdução

No ano de 2020, com a pandemia causada pelo novo coronavírus, chamado de covid-19, a Organização Mundial da Saúde (OMS) recomendou, como medida para evitar a sua propagação, que fossem feitos o distanciamento físico para as pessoas não infectadas e o isolamento para os casos sintomáticos ou positivos. Com isso, muitas organizações privadas e públicas adotaram o regime de trabalho remoto, ainda que não tivessem a estrutura de TI adequada para tal.

Por não terem tido o tempo necessário para se prepararem, não raro, essas empresas enfrentaram problemas de segurança, principalmente pelo fato de seus funcionários terem passado a usar computadores domésticos sem o devido gerenciamento de atualizações e *patches* de segurança, sem antivírus e com o uso de senhas fracas em suas redes wi-fi domésticas. Além de tudo, nem todas as organizações possuíam uma infraestrutura robusta para aceitar conexões remotas em grande escala com alta segurança (KASPERSKY, 2020b; MICROSOFT, 2020a).

Segundo levantamento feito pela Microsoft em 2020 com gestores de segurança da informação nos EUA, a maior preocupação nesse ano tem sido quanto ao uso que seus funcionários podem fazer com seus dispositivos pessoais que reduzem a segurança corporativa e o consequente fornecimento de segurança a esses dispositivos. Outros pontos também requerem cuidados, segundo eles: o aumento de *phishings*, roubo de credenciais e a mudança de foco para ataques a infraestruturas de rede e VPNs (MICROSOFT, 2020a).

De acordo com o estudo citado, era comum, antes da pandemia, que as empresas emprestassem notebooks aos seus funcionários para trabalhos remotos. Contando que os funcionários retornariam aos escritórios em pequeno intervalo de tempo, e, também, por terem VPNs não estruturadas para acessos simultâneos em grande escala, era frequente aplicarem políticas que impediam a atualização automática dos softwares nos equipamentos, seja através da conexão VPN,

evitando sobrecarga no acesso, seja pela própria internet, evitando atualizações não homologadas.

A Microsoft (2020a) constatou, também, que essa regra passou a ser flexibilizada, permitindo que atualizações fossem recebidas diretamente da internet. Contudo, essa abordagem é restrita aos equipamentos corporativos e gera o problema de permitir a instalação de *patches* e atualizações não homologadas.

Aliado a isso e devido à maior área de exploração disponível, foi relatado pela Kaspersky um aumento de 333% de ataques cibernéticos de força bruta no Brasil de fevereiro a abril de 2020, direcionados a serviços RDP (Remote Desktop Protocol), totalizando mais de 50 milhões de tentativas só em abril, sendo este tipo de ataque o mais comum contra empresas no ano de 2020 (KASPERSKY, 2020a, 2020b).

Assim, considerando as dificuldades apresentadas sobre as questões de segurança devido ao uso de dispositivos de terceiros desprotegidos ou supostamente comprometidos no acesso à rede corporativa, este artigo tem o propósito de estudar se soluções de *Virtual Desktop Infrastructure* (VDI) aliadas ao modelo de segurança *Software-Defined Perimeter* (SDP) podem auxiliar na mitigação das vulnerabilidades decorrentes do trabalho remoto.

As principais vulnerabilidades que serão consideradas são a varredura de endereços IPs e portas de serviços abertas, a movimentação lateral entre dispositivos e recursos, e o vazamento de dados decorrentes do acesso remoto.

Para tanto, este artigo apresenta brevemente, no item 2, o framework de segurança *Zero Trust* e seu derivado *Software-Defined Perimeter*. A tecnologia de *Virtual Desktop Infrastructure* é apresentada no item 3. Os resultados e discussões são expostos no item 4 e, no 5, há a conclusão.

## 2 Frameworks de segurança para redes modernas

O uso de VPN (*Virtual Private Network*), bastante comum na realização de trabalho remoto, garante que o tráfego de dados ocorra em um túnel privado protegido por criptografia. Embora proporcione

segurança quanto à interceptação de dados, não impede que uma ameaça acesse a rede corporativa caso a segurança do equipamento do usuário esteja comprometida. Vale dizer, ainda, que diversas vulnerabilidades relacionadas a VPNs foram divulgadas nos últimos dez anos e, mesmo havendo *patches* de segurança para as suas correções, ainda são encontrados muitos serviços vulneráveis na internet (SARVEPALLI, 2019).

Em vista disso, a VPN tornou-se um vetor de ataques muito desejado por crackers, principalmente neste momento de pandemia, tendo sido emitidos vários alertas por agências norte-americanas e europeias de cibersegurança sobre segurança em VPNs e respectivos ataques que vêm ocorrendo (CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, 2020b, 2020c; NATIONAL CYBER SECURITY CENTRE, 2019).

Entre os problemas mais relatados estão a exploração de vulnerabilidades de *bugs* em servidores VPN, com subsequente instalação de *backdoors* e/ou *ransomwares*; *VPN pivoting*, em que o atacante, depois de um acesso bem-sucedido, faz a movimentação lateral para outros equipamentos da rede corporativa. Esse acesso pode ter sido obtido por hacking direto ao servidor VPN ou através de uma conexão legítima realizada por funcionário da empresa em um dispositivo comprometido. Tendo acessado a rede, é bastante comum a realização de escaneamento dos endereços IPs e portas abertas. E, em todos os casos, a extração de dados relevantes (BYOS INC, 2020; CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, 2020b; MICROSOFT, 2020a).

Há também as ameaças internas, intencionais ou não, e que podem ser mais frequentes quando se tem a maioria dos funcionários em trabalho remoto. O roubo de propriedade intelectual e fraude para ganho financeiro, como consequência de alguma insatisfação com a organização ou alguma perda financeira, é uma delas. E o vazamento de dados não intencional também, por erro ou distração, geralmente como consequência de estresse pela mudança abrupta e não voluntária da rotina de trabalho (CARNEGIE MELLON UNIVERSITY, 2020; MICROSOFT, 2020a).

Desse modo, embora o uso da VPN para o trabalho remoto atenda a questões operacionais dos funcionários, fica evidente que não tem

atendido bem aos problemas de gerenciamento de atualizações e *patches* de segurança, a exploração da rede depois do seu acesso e o vazamento de dados (BYOS INC, 2020; MICROSOFT, 2020a).

Além das questões atinentes ao cenário da VPN, os modelos tradicionais de segurança também têm se mostrado inadequados para proteger as redes atuais de ataques, pois estas se diferem em vários pontos da infraestrutura tradicional. Atualmente, a adoção da computação em nuvem, com o uso crescente de dispositivos IoT e equipamentos não gerenciados, decorrentes, neste último caso, da adesão ao trabalho remoto e BYOD (*Bring Your Own Device*), mudaram os limites de perímetro das redes (MOUBAYED; REFAEY; SHAMI, 2019).

Novos modelos ou frameworks de segurança estão sendo propostos e adaptados, visando tratar as novas dificuldades surgidas. Entre eles, pode-se citar o *Zero Trust* (ZT) e o *Software-Defined Perimeters* (SDP), que serão apresentados brevemente a seguir.

## 2.1 Modelo de segurança *Zero Trust*

O framework de segurança denominado *Zero Trust* busca a proteção das pessoas, dispositivos, aplicativos e dados, independentemente do local onde estejam ou sejam acessados. Uma de suas premissas é que toda solicitação de sessão ou acesso parte de um meio não confiável, potencialmente já comprometido, mesmo que ocorra internamente, sendo, portanto, válida a regra de nunca confiar e sempre verificar (MICROSOFT, 2020b).

A infraestrutura de TI deve estar preparada de tal modo que, se um invasor obtiver acesso a um dispositivo ou credencial de usuário, tenha a capacidade de movimentação lateral ou de extração de dados inibida ou reduzida, oferecendo um plano de defesa em profundidade (UTTECHT, 2020).

Para isso, alguns princípios são definidos. Um deles é que todas as entidades da infraestrutura (identidades, dispositivos, aplicações, dados, infraestrutura e redes) devem ser submetidas à autenticação para as comunicações entre si, sejam elas externas ou não (UTTECHT, 2020).

Além disso, os recursos devem ser segmentados à mínima parte possível, de modo que todo o acesso permitido não possibilite visualizar todo o conjunto de dados críticos de uma só vez. Junto com esse princípio, há a atribuição de confiança mínima à entidade, restringindo os privilégios de acesso e direitos ao estritamente necessário para as suas atividades. Essa restrição vai além da função, indo também por quanto tempo possuir tal privilégio e onde puder ser usado ou acessado. Ainda, a avaliação de confiabilidade deve ser dinâmica, ou seja, avalia-se conforme o contexto da requisição (UTTECHT, 2020).

Esse contexto pode ser formado pelas informações da requisição de acesso, bem como com a identidade do usuário, o estado do seu dispositivo, os aplicativos em uso, a classificação dos dados, entre outros (MICROSOFT, 2020b).

A criptografia total também é um princípio desse modelo, no qual todos os dados em trânsito ou armazenados, na rede ou fora dela, deverão ser criptografados (UTTECHT, 2020).

Por fim, o monitoramento de todas as entidades é peça chave para a melhoria contínua das políticas de segurança e detecção de problemas e sua correção (UTTECHT, 2020).

Vale dizer que esses princípios se aplicam a seis elementos principais (MICROSOFT, 2020b):

- Identidades: representam pessoas, serviços e dispositivos. Em um nível ótimo de maturidade deste framework, a autenticação é realizada sem senha e conforme a análise do contexto.
- Dispositivos: são todos os equipamentos ligados à infraestrutura – IoT, smartphones, BYOD, dispositivos gerenciados por parceiros e servidores hospedados na nuvem.
- Aplicações: desde aplicações legadas e locais até as em nuvem e SaaS.
- Dados: devem ser classificados, rotulados, criptografados e rastreados.

- Infraestrutura: devem ser definidos controles de segurança aos ativos da infraestrutura, tais como servidores locais, VMs em nuvem, contêineres e microsserviços.
- Redes: controles de rede e microssegmentação, criptografia ponta a ponta, monitoramento e análise de tráfego.

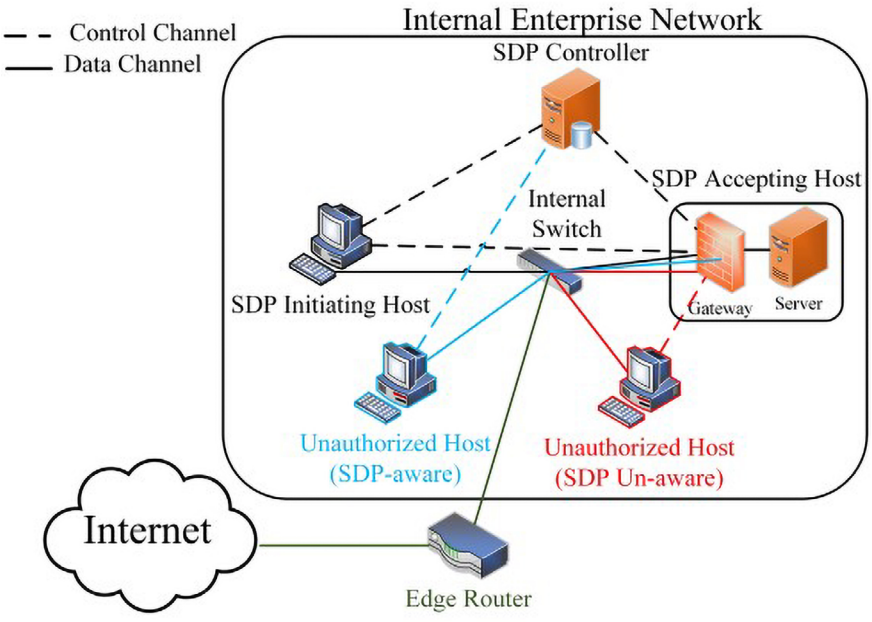
É importante ressaltar que esse framework é concebido para ser aplicado à organização como um todo, permeando as diretrizes, políticas e planos de segurança, todas as tecnologias envolvidas em todos os níveis, pessoas e cultura organizacional. Devem-se automatizar os processos de controle de segurança e utilizar a inteligência artificial para análise de anomalias e emissão de alertas, de modo que o tempo médio de resposta a incidentes seja reduzido (MICROSOFT, 2020b; UTTECHT, 2020).

## 2.2 *Software-Defined Perimeter* (SDP)

Este é um modelo de segurança derivado do *Zero Trust* que é mais genérico e abrangente e não define, necessariamente, de que modo a segurança deve ser feita. Já o SDP define que o perímetro deve ser protegido por mecanismos lógicos e também de forma dinâmica, em vez de se usar dispositivos físicos com regras estáticas. Essa segurança é feita por meio de um *gateway* lógico de acesso que protege os recursos da rede, autenticando e autorizando as identidades dos usuários e dispositivos antes de conceder visibilidade e acesso ao recurso solicitado. Todos os acessos são feitos por meio de conexões criptografadas em tempo real (MOUBAYED; REFAEY; SHAMI, 2019).

Dessa forma, o usuário não se conecta a uma infraestrutura completa ou, ainda, a uma parcialmente segmentada, mas somente ao recurso solicitado pelo tempo que durar a conexão. Essa conexão é criptografada por meio do protocolo TLS, tanto no cliente quanto no servidor. Se houver desconexão e for necessário novo acesso, todo o processo de verificação, validação do usuário e do dispositivo e criação do túnel é repetido (CLOUDFLARE, 2020).

**Figura 1 – Diagrama da arquitetura SDP**




**Fonte:** MOUBAYED; REFAEY; SHAMI, 2019.

Na Figura 1, pode-se observar um diagrama do modelo SDP, cujos elementos principais (*SDP Initiating Host*, *SDP Controller* e *SDP Accepting Host*) estão interligados por um canal de controle, necessário para as verificações e autorizações de acesso. Um *host* não autorizado (em azul), mas pertencente ao SDP, tentou uma comunicação com o *controller*, que foi recusada e não repassada ao *gateway*. Há também outro *host* (em vermelho) que não pertence ao SDP e que, por não ter conhecimento do *controller*, submeteu pacotes diretamente ao *gateway*, o que também foi rejeitado. Por fim, o *host* que possui permissão para acessar o *Server* teve uma conexão estabelecida com o *controller*, seguida por uma conexão ao *gateway*, que se comunicou com o *Server*, estabelecendo, assim, um túnel de comunicação.

A arquitetura deste modelo se baseia em cinco camadas de segurança e três elementos de funcionamento. As camadas, que são na realidade os princípios do funcionamento deste modelo, são:

- Autenticação de pacote único (SPA): é a base da autenticação do modelo. É usada para rejeitar o tráfego recebido de dispositivos não autorizados. O dispositivo cliente envia um pacote criptografado para o controlador SDP, que verifica e autoriza, se estiver tudo certo. Um segundo pacote é enviado pelo dispositivo, para que ajude a determinar o tráfego do dispositivo autorizado e rejeitar o restante.

- Segurança mútua de camada de transporte (mTLS): no SDP, o protocolo TLS é usado bidirecionalmente (cliente-servidor e servidor-cliente) para a autenticação de dispositivos, e não apenas servidor-cliente. Ou seja, a autenticação de tudo e todos. Um atacante precisaria das chaves SDP para falsificar um pacote SPA.

- Validação de dispositivo (DV): o mTLS prova apenas que a chave ainda é válida (não está expirada nem revogada), mas não que a chave foi roubada e que está sendo usada por dispositivo indevido. Desse modo, há uma camada extra de segurança que garante que a chave criptográfica usada seja mantida no dispositivo apropriado. Para isso, é feita a validação do dispositivo, verificando se pertence a um usuário autorizado e se o dispositivo é o mesmo que foi habilitado previamente no SDP.

- *Firewalls* dinâmicos: os *firewalls* tradicionais costumam ter muitas regras estáticas. Já os dinâmicos possuem apenas uma regra estática: negar todas as conexões. As liberações são feitas dinamicamente no *gateway*, sendo autorizadas ou recusadas conforme o contexto.

- Vinculação de aplicativos (AppB): é um processo de forçar que os aplicativos autorizados usem os túneis TLS criptografados criados pelo SDP. Isso acontece depois que o dispositivo e o usuário já estiverem autenticados e autorizados.

Quanto aos elementos, o SDP *Controller* é o responsável pela coordenação das mensagens de controle, sendo um agente de confiança entre os demais elementos. Determina quais serviços cada cliente está autorizado a acessar, autentica dispositivos, emite certificados TLS e ajuda nas demais configurações necessárias para o estabelecimento de túnel mútuo TLS entre as partes (MOUBAYED; REFAEY; SHAMI, 2019).

Quando o cliente deseja se conectar a um serviço, o *controller* recebe as informações de identificação e contexto do dispositivo e valida-as conforme uma base interna. Em Moubayed, Refaey e Shami (2019), foi montada uma estrutura em que os detalhes dos usuários, dispositivos, servidores autorizados e serviços eram armazenados em um banco de dados local. Esses dados são fornecidos ao *gateway* para a definição das regras dinâmicas de acesso.

O SDP *Initiating Host* (IH) é o *host* cliente previamente habilitado no *controller*. Inicialmente, o IH envia o pedido de conexão ao controlador com o seu certificado e dados do hardware e software instalados. Uma vez verificado e autorizado, é estabelecido um túnel mútuo com o *controller*. Só depois disso é que o IH informa qual o serviço que deseja acessar. Faz-se nova verificação para avaliar se esse acesso é permitido. Em caso positivo, o *controller* envia ao *gateway* os dados de conexão do cliente e certificado, que inicia novo processo de conexão com o cliente (MOUBAYED; REFAEY; SHAMI, 2019).

O SDP *Accepting Hosts* (AH), ou *gateway* SDP, é o dispositivo responsável pela segurança do serviço ou recurso, tal como um *firewall* lógico. De regra, todos os pacotes e solicitações de *hosts* clientes são rejeitados e há uma regra fixa de aceitar pacotes somente do *controller* e do serviço ou recurso que protege, mas cujas comunicações são feitas por um túnel TLS (MOUBAYED; REFAEY; SHAMI, 2019).

O estabelecimento de conexão com o cliente se dá após a informação do *controller* de que o cliente está validado, autorizado e possui permissão para determinado serviço. Aí sim é feito um túnel entre o *gateway* e o cliente, e a troca de dados entre este e o serviço de fato ocorrem (CLOUDFLARE, 2020).

Em uma implementação feita por Moubayed, Refaey e Shami (2019), o *gateway* foi implementado com o uso de um i*ptables* cujas regras eram dinamicamente atualizadas conforme as informações recebidas do *controller*.

## 3 *Virtual Desktop Infrastructure* (VDI)

As tecnologias de computação em nuvem, ou *cloud computing*, têm sido cada vez mais adotadas por instituições públicas e privadas, tendo em

vista as vantagens a elas inerentes, tais como o alto desempenho e disponibilidade fornecidos, redução de consumo de energia e gastos, escalabilidade de recursos, segurança e gerenciamento mais eficiente.

Com a computação em nuvem, recursos de processamento, armazenamento e redes passaram a ser oferecidos virtualmente e sob diferentes níveis de serviços ao usuário, sendo os principais IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) e SaaS (*Software as a Service*).

À medida que essa tecnologia amadureceu, outro serviço começou a ganhar espaço: a *Virtual Desktop Infrastructure* (VDI), trazendo também o conceito de DaaS (*Desktop as a Service*). Essa solução fornece ambientes de desktops virtuais, os quais são virtualizados em servidores e disponibilizados na forma de serviços sob demanda aos usuários. Além das vantagens herdadas da *cloud computing*, o acesso a um ambiente de trabalho computacional virtual possibilita um melhor aproveitamento de poder de processamento de hardware, diferentemente da solução tradicional, a qual fornece um computador pessoal completo para o usuário, que frequentemente fica subutilizado para a maioria dos perfis de usuários (NAKHAI; ANUAR, 2017).

Outro ponto é que essa tecnologia permite aos gestores de TI resolverem problemas de gerenciamento de *endpoints* (estações de trabalho e dispositivos móveis), facilitando a padronização de sistemas operacionais, atualizações e aplicações de *patches* de segurança, e até mesmo sendo uma solução viável para os problemas oriundos da adoção do BYOD (*Bring Your Own Device* – traga seu próprio aparelho, em tradução livre), fundamentais para o trabalho remoto (AMERICA, 2016).

## 3.1 Computação em nuvem e virtualização

A computação em nuvem é um modelo computacional que fornece aos seus usuários recursos de processamento, armazenamento e rede sob a forma de serviços descentralizados do local do usuário. Tais serviços são executados sobre uma plataforma física que fica encapsulada para os seus usuários, de modo que estes têm acesso apenas ao que está disponível em sua interface, não sendo necessário gerenciar nem saber exatamente como a estrutura física está composta, importando mais a qualidade, o custo e o gerenciamento dos recursos oferecidos (RIBEIRO, 2019).

Esse modelo depende essencialmente da virtualização, que possibilita a criação de uma máquina virtual – do inglês, *virtual machine* (VM) – para o usuário, ocultando o hardware real. A VM tem o seu funcionamento parecido com o de um equipamento físico, porém possibilita o melhor aproveitamento do poder computacional do hardware que a hospeda, visto que várias máquinas virtuais podem ser criadas e executadas ao mesmo tempo, reduzindo a possibilidade de hardware ocioso (YANG *et al.*, 2018).

## 3.2 Características principais

Com o avanço das tecnologias de computação em nuvem, surgiram soluções de desktops virtualizados (VDIs) em servidores instalados em estrutura própria ou em nuvens públicas e disponibilizados na forma de serviços sob demanda aos usuários por meio da rede ou da internet (NAKHAI; ANUAR, 2017).

Em um cenário em que as equipes de TI estão cada vez mais reduzidas, apesar da sua importância dentro das organizações, a adoção de VDI pode poupar tempo e esforço para a área técnica, visto que vários desktops virtuais (VDs) podem ser disponibilizados aos usuários em pouco tempo, pois são criados a partir de um *template*, chamado também de *golden image* ou imagem mestre. Essa imagem é previamente definida a partir de um determinado perfil de usuário, onde são instalados o sistema operacional e os demais aplicativos, configurações e atualizações necessárias, sendo feito isso apenas uma vez (AZZEDIN; YAHYA; MAHMOOD, 2019).

Desse modo, organizações podem fornecer aos seus funcionários uma área de trabalho remota completa, atualizada, gerenciada centralizadamente e isolada do equipamento do usuário, possibilitando uma redução de riscos de segurança, pois uma vez conectado ao desktop virtual, o acesso aos recursos internos da empresa passa a ser realizado a partir de um desktop homologado e controlado, e não por meio do seu próprio equipamento ligado diretamente à rede, sendo uma solução interessante para trabalhos remotos (AZZEDIN; YAHYA; MAHMOOD, 2019).

Aliado a isso, a solução pode oferecer níveis elevados de disponibilidade, se construída em um ambiente altamente disponível. E a flexibilidade

na forma de acesso também tende a ser outro ponto forte, pois o usuário tem a liberdade de acessar seu ambiente de trabalho a qualquer momento e a partir de qualquer equipamento, seja um computador pessoal (PC), um *thin client*, um smartphone, tablet, independentemente do sistema operacional executado (AZZEDIN; YAHYA; MAHMOOD, 2019).

Outra vantagem do VDI é a economia gerada pelo uso de dispositivos mais simples como terminais de acesso, ou seja, não é necessário investir tanto na aquisição de computadores pessoais, podendo ser usados *thin clients* ou até mesmo equipamentos antigos, o que dispensaria o gasto com novas compras. Nesse ponto, os *upgrades* nesses computadores tornam-se minimamente necessários e o consumo de energia elétrica também pode ser reduzido (SIGL; BERL, 2018).

Apesar das vantagens citadas, as desvantagens referem-se à alta dependência de conexão de rede para ser possível o uso de VDI e desempenho atrelado à largura de banda disponível. Outro problema é que, se houver alguma falha no servidor, o serviço será interrompido. Contudo, essa questão é facilmente resolvida com a redundância da infraestrutura, de modo que possibilite a migração de VD em execução de um servidor para outro (AZZEDIN, YAHYA; MAHMOOD, 2019).

## 3.3 Arquitetura básica de um VDI

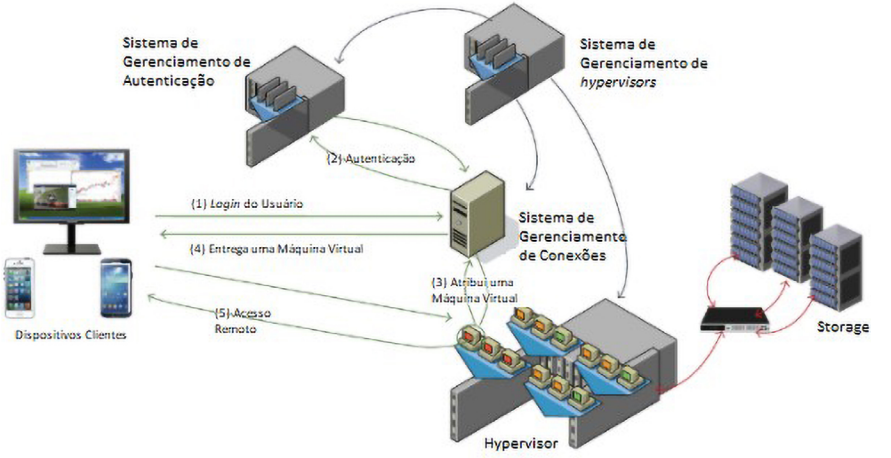
O processo de disponibilização de uma máquina virtual ao usuário inicia-se quando ele envia uma requisição de login de acesso para o sistema de gerenciamento de conexões (*connection management system* – CMS). Essa requisição é iniciada em seu dispositivo cliente, que pode ser um computador ou notebook, tablet, smartphone ou *thin client* (JEONG *et al*., 2015).

Dependendo da solução VDI utilizada, pode-se fazer a conexão e a visualização do desktop virtual por meio de um aplicativo instalado ou de um navegador com suporte a HTML5.

O sistema de gerenciamento de conexões (CMS), também chamado de *broker* de conexão, é o intermediário entre o cliente e o sistema de gerenciamento de autenticação (*authentication management system* – AMS), que é, na realidade, o serviço de diretório da rede, como o *Microsoft Active Directory*, por exemplo (JEONG *et al*., 2015).

Após o processo de autenticação ter sido concluído com sucesso, o CMS envia uma requisição ao sistema de gerenciamento de *hypervisors*, ou diretamente ao próprio *hypervisor*, para que seja alocado um desktop virtual ao solicitante. O desktop virtual é, então, instanciado e atribuído a ele. O CMS, por sua vez, faz a entrega ao usuário, atuando, nesse momento, como um gerenciador de visualização dos desktops virtuais disponibilizados (JEONG *et al.*, 2015).

**Figura 2 – Arquitetura básica de um VDI**




**Fonte:** JEONG *et al.*, 2015.

Na Figura 2, é mostrada uma requisição direta do CMS ao *hypervisor*, porém, em ambientes que requeiram alta disponibilidade e escalabilidade, adota-se uma estrutura com vários virtualizadores, sendo necessário um sistema de gerenciamento de *hypervisors* que possa definir qual deverá ser usado, realizando assim um balanceamento de cargas (GORDON, 2019).

O *hypervisor* é o responsável por criar máquinas virtuais (VMs). A criação de máquinas é feita a partir de uma imagem pré-definida, chamada de imagem mestre ou *golden image*. É boa prática criar variações de imagens mestre que atendam a diferentes perfis, prioridades e necessidades de uso, tendo uma variedade de arquiteturas de hardware com

memória, processador, sistema operacional, aplicativos e outros recursos diferentes entre si (UDS ENTERPRISE TEAM, 2016).

Outra estratégia é criar um *pool* de VMs, que é vinculado a uma imagem mestre e tem definido um número máximo de VMs daquele tipo. Ou seja, quando o usuário solicita um desktop virtual, após a autenticação, será verificado a qual tipo de máquina ele possui privilégio de acesso. Para esse tipo, instancia-se uma VM, se não tiver sido atingido o limite total de uso. Isso permite um melhor gerenciamento dos recursos do *hypervisor*, não permitindo que mais máquinas, além da quantidade ideal, sejam instanciadas e consumam todos os recursos (VMWARE INC, 2017).

Esse processo de instanciação ocorre por meio de clonagem total da imagem mestre ou de um *snapshot*, criando um clone vinculado. No primeiro caso, o processo de clonagem é mais demorado para ser feito e ocupa mais espaço de armazenamento, visto que uma nova máquina virtual totalmente independente é criada. Já no segundo modo, cria-se uma máquina vinculada à máquina virtual pai a partir de um *snapshot*, que dependerá de uma conexão permanente a ele e compartilhará os discos virtuais, o que também reduz o espaço de armazenamento consumido (VMWARE INC, 2017).

O uso de *pools* permite um melhor gerenciamento das VMs, visto que basta que a imagem mestre seja atualizada ou modificada para que as suas instâncias repliquem essas mudanças. Esta funcionalidade é bastante interessante para minimizar o problema de segurança referente ao controle de atualização dos softwares utilizados pelos usuários da organização (VMWARE INC, 2017).

Isso ocorre devido à instalação e aplicação de atualizações e *patches* do sistema operacional e de demais aplicativos se feitas de modo centralizado, com muita simplicidade, sendo distribuídas a inúmeras máquinas de modo automatizado e não individualizado.

Ainda quanto aos tipos de desktops virtuais, estes podem ser de dois tipos: desktops não persistentes e persistentes. A escolha do tipo adequado deve levar em consideração o orçamento disponível, a infraestrutura existente e o perfil de uso dos usuários.

Os desktops não persistentes são aqueles cujos dados armazenados na máquina virtual durante o seu uso são destruídos após o desligamento. É um modelo mais econômico, pois possui baixo custo de backup e armazenamento. O seu funcionamento pode ser baseado em *pool*, sendo atribuída aleatoriamente uma das máquinas ao solicitante. Uma variação possível é não atribuir aleatoriamente, mas, sim, estaticamente (VMWARE INC, 2017).

Já os desktops persistentes permitem o armazenamento das alterações feitas no desktop virtual, mantendo um disco virtual para o usuário. Nesse caso, após a realização do primeiro logon, é atribuída ao usuário uma máquina que ficará estaticamente vinculada ao seu perfil, de modo que somente ele poderá usá-la no futuro. Assim, todas as personalizações realizadas serão carregadas junto com a máquina virtual (VMWARE INC, 2017).

Uma variação híbrida desses modelos, que permite o uso e armazenamento dos documentos pessoais, mas não necessariamente os dados de aplicativos instalados pelo usuário e personalizações de área de trabalho, é através de perfis móveis, que ficam armazenados em algum *storage* e são carregados no momento que a máquina é atribuída ao usuário. Neste caso, somente os dados armazenados na unidade de rede montada serão mantidos (VMWARE INC, 2017).

Por fim, um recurso oferecido por soluções VDI do mercado é a proteção de cópia de conteúdo, que permite que o gestor habilite ou não a transferência de arquivos e dados da máquina virtual para o dispositivo cliente e vice-versa. Essa funcionalidade, embora não impeça de todo modo, mitiga o vazamento de documentos inteiros de uma só vez por meio de sua cópia ou transferência (VMWARE INC, 2017).

## 4 Resultados e discussões

Nesta seção, serão apresentados os resultados da presente pesquisa e suas discussões em relação aos problemas inicialmente destacados.

O trabalho remoto adotado pelas organizações já há algum tempo, mas principalmente no ano de 2020 devido à pandemia, tem suscitado discussões sobre a segurança dos dispositivos dos usuários e um

modo seguro de acessar os recursos da rede corporativa a partir de uma rede externa.

O artigo focou em descrever soluções e estratégias que poderiam minimizar três problemas de segurança relacionados ao cenário descrito.

## 4.1 Minimização dos riscos de segurança do acesso do usuário à rede corporativa por meio de um dispositivo desprotegido ou supostamente comprometido

O acesso à rede corporativa por dispositivos desprotegidos, mesmo que pela VPN, é um risco de segurança grave que deve ser evitado. O uso de dispositivos não gerenciados, embora comum, é de difícil controle. Porém, como se pode verificar neste artigo, o VDI proporciona a disponibilização de um desktop virtual ao usuário, isolado do computador que o acessa. O gerenciamento desse desktop é possível pela adoção de *pools* de VMs e gerenciamento de versões das imagens mestres, devido à replicação feita às VMs clones.

Embora essa tecnologia não possibilite o gerenciamento do equipamento particular, oferece ao usuário um canal de acesso e comunicação mais seguro e isolado do seu sistema de acesso, no qual os riscos de um malware e a interação de um atacante presente seriam mitigados, por acrescentar uma camada de interação.

## 4.2 Vazamento de dados causado pelo usuário que deseja salvar algum documento do ambiente corporativo em seu equipamento doméstico

Aqui, o uso de VDI e SDP são fundamentais para evitar que vazamentos de dados causados pelo usuário comprometam a segurança da organização. Isso pelo fato de as soluções VDI no mercado terem recursos que, se habilitados, impedem o download e o upload de arquivos da máquina virtual para o dispositivo cliente.

Já o SDP, também pela microssegmentação dos recursos, que podem e devem ser estendidos aos dados, e pela política de privilégios mínimos, mitiga o vazamento de dados, uma vez que, se

ocorrer, será de pequenas partes de informações, com o menor potencial possível de dano.

### 4.3 Mitigação dos riscos de movimentação lateral e varredura da rede causados por um invasor que acesse a rede por meio de uma VPN

O modelo de segurança SDP, que é baseado no *Zero Trust*, pode reduzir os riscos de segurança advindos de acesso à rede corporativa por meio de um dispositivo desprotegido ou de roubo de credenciais, visto que seus princípios propõem mecanismos que impedem a varredura de rede e a movimentação lateral. Dentre estes princípios, citam-se a segurança mútua de camada de transporte e a validação de dispositivo, que exigem que o atacante obtenha as chaves SDP e o conjunto de dados necessários do contexto para conseguir acessar algum determinado recurso. Como esses dados de contexto são variáveis, acrescentam um alto nível de dificuldade para a ação hacker.

Outro ponto benéfico é que a microssegmentação, aliada às permissões mínimas de acesso, protegem os recursos caso o atacante consiga, de fato, estabelecer conexão. Isso permitiria que ele acessasse alguma coisa; porém, pela sua granularidade, possivelmente não o suficiente para comprometer um sistema ou a confidencialidade de alguma informação.

Por esses motivos, a adoção do modelo SDP proporciona um incremento de segurança no que se refere ao problema citado.

## 5 Conclusão

Este artigo apresentou, sem esgotar o assunto, aspectos básicos da tecnologia VDI e o modelo de segurança SDP. Ambas as tecnologias apresentam pontos relevantes na mitigação de vulnerabilidades de segurança oriundas do trabalho remoto, principalmente se forem usadas em conjunto, montando-se uma arquitetura SDP aplicada a VDI.

Vale dizer que não basta o uso de uma tecnologia para que a segurança da informação seja provida; também é preciso pensar a estratégia de uso e a política de segurança adequada para o contexto.

## Referências


AMERICA, Computer Resources of. **VDI vs. DaaS**: exploring the benefits of hosted desktops. New York, USA. Disponível em: https://www.consultcra.com/wp-content/uploads/2020/04/Connect_White_Paper-Hosted_desktops.pdf. Acesso em: 22 jun. 2022.

AZZEDIN, Farag; YAHYA, Salah; MAHMOOD, Sajjad. Performance evaluation of VDI-based private cloud technology for education and research. **International Journal of Computer Science and Network Security**, v. 19, n. 9, p. 231-237, set. 2019. Disponível em: http://paper.ijcsns.org/07_book/201909/20190927.pdf. Acesso em: 22 jun. 2022.

BYOS INC. **The problem with VPNs**. 2020. Disponível em: https://byos.io/blog/the-problem-with-vpns. Acesso em: 21 nov. 2020.

CARNEGIE MELLON UNIVERSITY. Software Engineering Institute. **Insider threats in the time of covid-19**. 2020. Disponível em: https://www.sei.cmu.edu/news-events/news/article.cfm?assetId=638958. Acesso em: 21 nov. 2020.

CLOUDFLARE. **What is a software-defined perimeter?** SDP *vs.* VPN. 2020. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/software-defined-perimeter/. Acesso em: 24 nov. 2020.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **Critical Infrastructure Sectors**. 2020a. Disponível em: https://www.cisa.gov/critical-infrastructure-sectors. Acesso em: 21 nov. 2020.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **Iran-based threat actor exploits VPN vulnerabilities**. 2020b. Disponível em: https://us-cert.cisa.gov/ncas/alerts/aa20-259a. Acesso em: 21 nov. 2020.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **Enterprise VPN security**. 2020c. Disponível em: https://us-cert.cisa.gov/ncas/alerts/aa20-073a. Acesso em: 21 nov. 2020.

GORDON, Graeme. **Understanding horizon connections**. 2019. Disponível em: https://techzone.vmware.com/blog/understanding-horizon-connections. Acesso em: 1º out. 2020.

JEONG, Doowon *et al*. Investigation methodology of a virtual desktop infrastructure for IoT. **Journal of Applied Mathematics**, v. 2015, 10 p., mar. 2015. Hindawi Limited. Disponível em: http://dx.doi.org/10.1155/2015/689870. Acesso em: 22 jun. 2022.

KASPERSKY. **Empresas já são o principal alvo de ciberataques na América Latina, mostra relatório da Kaspersky**. 2020a. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_empresas-ja-sao-o-principal-alvo-de-ciberataques-na-america-latina-mostra-relatorio-da-kaspersky. Acesso em: 21 nov. 2020.

KASPERSKY. **Home office motiva aumento de mais de 330% em ataques usando sistemas de acesso remoto no Brasil**. 2020b. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_home-office-motiva-aumento-de-mais-de-330-em-ataques-usando-sistemas-de-acesso-remoto-no-brasil. Acesso em: 21 nov. 2020.

MICROSOFT (EUA). **Microsoft Digital Defense Report**. [Redmond]: Microsoft, 2020a. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf?culture=en-us&country=US. Acesso em: 6 jul. 2022.

MICROSOFT (EUA). **Zero Trust Maturity Model**. [Redmond]: Microsoft, 2020b. Disponível em: https://download.microsoft.com/download/f/9/2/f92129bc-0d6e-4b8e-a47b-288432bae68e/Zero_Trust_Vision_Paper_Final%2010.28.pdf. Acesso em: 23 nov. 2020.

MOUBAYED, Abdallah; REFAEY, Ahmed; SHAMI, Abdallah. Software-Defined Perimeter (SDP): state of the art secure solution for modern networks. **IEEE Network**, Nova Iorque, v. 33, n. 5, p. 226-233, set./out. 2019. Disponível em: https://ieeexplore.ieee.org/document/8863736. Acesso em: 22 nov. 2020.

NAKHAI, Pedram Hossein; ANUAR, Nor Badrul. Performance evaluation of virtual desktop operating systems in virtual desktop infrastructure. **2017 IEEE Conference on Application, Information and Network Security** (AINS), 2017, p. 105–110, 2017.

NATIONAL CYBER SECURITY CENTRE. **Vulnerabilities exploited in VPN products used worldwide**: APTs are exploiting vulnerabilities in several VPN products used worldwide. 2019. Disponível em: https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities. Acesso em: 23 nov. 2020.

RAHMAN, Hafiz Ur *et al.* Performance evaluation of VDI environment. **2016 6th International Conference on Innovative Computing Technology (INTECH)**, Dublin, IEEE, p. 104-109, 2016. Disponível em: https://ieeexplore.ieee.org/document/7845102. Acesso em: 1º out. 2020.

RIBEIRO, Carlos E. R. **Gerenciando Ambientes Multicloud**. 2019. Trabalho de Conclusão de Curso (Especialização em Infraestrutura de TI) – Departamento de Computação, Universidade Federal de São Carlos, São Carlos-SP, 2019.

SARVEPALLI, Vijay. **VPN**: a gateway for vulnerabilities. Software Engineering Institute, 2019. Disponível em: https://insights.sei.cmu.edu/cert/2019/11/vpn---a-gateway-for-vulnerabilities.html. Acesso em: 21 nov. 2020.

SIGL, Christina; BERL, Andreas. Benchmarking and user types in virtual desktop infrastructures. **2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing**, ICCP 2018, p. 47-54, 2018. DOI: 10.1109/ICCP.2018.8516634.

UDS ENTERPRISE TEAM. **Best practices for VDI golden images management**. 2016. Disponível em: https://www.udsenterprise.com/en/blog/2016/06/14/vdi-golden-images-best-practices/. Acesso em: 20 out. 2020.

UTTECHT, Karen D. **Zero trust (ZT) concepts for federal government architectures**. Technical Report 1253. Lexington: Massachusetts Institute of Technology, 2020. 58 p. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1106904.pdf. Acesso em: 23 nov. 2020.

VMWARE INC. Setting Up desktop and application pools in view: vmware horizon 7 7.0. **VMware Horizon 7 7.0.** 2017. Disponível em: https://docs.vmware.com/en/VMware-Horizon-7/7.0/view-70-setting-up-desktops.pdf. Acesso em: 30 nov. 2020.

YANG, Chao-Tung; LIU, Jung-Chun; LEE, Jheng-Yue; CHANG, Chih-Hung; LAI, Chuan-Lin; KUO, Chia-Chen. The implementation of a virtual desktop infrastructure with GPU accelerated on OpenStack. **15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN),** 2018, p. 366-370. DOI: 10.1109/I-SPAN.2018.00069.

## Nota

[1] Texto adaptado de artigo apresentado para fins de conclusão de Especialização em Infraestrutura de TI pela Universidade Federal de São Carlos (UFSCar) em 2021.