Software Defined Perimeter - SDP

Pedro Antunes
DCC
FCUP
Porto, Portugal
up201507254fc.up.pt

André Rodrigues
DCC
FCUP
Porto, Portugal
up201505639@fc.up.pt

Steve Rocha
DCC
FCUP
Porto, Portugal
up202009115@edu.fc.up.pt

***Abstract*—A tradicional defesa de perímetro recorre a dispositivos que atuam como firewalls. Nos tempos de hoje existe um vasto leque de ataques informáticos que deixou este conceito enfraquecido. Os níveis de segurança têm de ser aumentados para fazer com que a superfície e a exposição a ataques. Ocultando a infraestrutura de uma rede e incluindo um controlo de acessos resiliente entre cada utilizador e cada recurso, ficam assegurados os principais níveis de segurança (confidencialidade, integridade e disponibilidade). Neste artigo é abordada a metodologia SDP, os pontos positivos e negativos e é feita uma comparação com as arquiteturas de defesa de perímetro que têm sido implementadas na atualidade.**

I. Introdução

Antes de se começar a falar ou até mesmo de implementar o SDP, já existia um paradigma de segurança de redes que se baseava em criar um perimetro em torno da rede cujo o objetivo era bloquear utilizadores de poderem entrar na rede, mas deixar os utilizadores internos sairem para o mundo exterior. Era implementado recurrendo a hardware especializado como balanceadores de carga e software, como por exemplo as firewalls. Este tipo de perimetro tradicional serviu por muitos anos para proteger a rede de ameaças externas devido as caracteristicas de bloquear a visibildade e accessibilidade da infraestrutura da rede e das aplicações a correrem na rede para todos que se situassem na parte externa do perimetro. Só depois mais tarde com o aparecimento da tecnologia de redes virtuais (VPN) e a revelação que os protocolos tradicionais, como o TCP e o IP não visavam a segurança, é que levou a uma reformulação da arquitetura deste paradigma, onde a tecnologia VPN passou a ser a base da arquitetura e algo importante de resalvar é que na maior parte deixou-se de usar hardware, ou seja, a partir de agora o perimetro era implementado apenas por software. Contudo a evolução e consequentemente implementação de novas tecnologias, arquiteturas e novos tipos de ciberatques, nomeadamente devido à adopção do paradigma das "clouds" ou "Software as a Service" que altera a localização do perimetro, BYOD, "Internet of Things", ataques de "physhing" que proporciona que uma pessoa não autorizada tenha acesso ao conteúdo dentro do perimetro, entre outros problemas que desafiam o modelo do perimetro tradicional. Ou seja, estas novas tecnologias trouxeram novos desafios no que toca às àreas de segurança e privacidade, nomeadamente em relação à autenticação, controlo de acesso, privacidade da informação, integridade dos dados, etc. Portanto seguindo o trabalho produzido pela "Defense Information Systems Agency" (DISA) sob o "Black Core Initiative" em 2007 a organização "Cloud Secuirty Alliance"(CSA) propôs um novo modelo/framework em 2013, mantendo-se o paradigma do perimetro e mantendo a reformulação anterior de apenas usar software para implementar o perimetro. Este modelo segue a filosofia "need-to-know" onde a identidade de um dispositivo tem de ser primeiro identificada antes de lhe ser concedido acesso à infraestrutura da aplicação, essencialmente a infraestrutura fica "black", este termo significa que toda a infraestrutura: rede (servidores, routers, etc) e a aplicação fica escondida para qualquer pessoa sem autorização. De forma resumida, o SDP adereça as dificuldades citadas em cima fornecendo à organização uma forma de implementar um perimetro que retem a invisibilidade e a inacessivelidade do perimetro tradicional, mas agora tanto para as pessoas exteriores como interiores ao perimetro e com a vantagem de ser agnóstico à localização da infraestrutura. Neste artigo, iremos aprofundar os motivos que levaram ao aparecimento deste novo paradigma que é o SDP, bem como iremos olhar para a sua arquitetura e como as organizações a podem implementar consoante as suas necessidades. Iremos também fazer uma pequena comparação com o modelo antigo, que recorria às VPNs, de forma a clarificar o porque da adopção do SDP no conexto de segurança de redes atual. No final do artigo, iremos abordar os desafios que o SDP resolve e o trabalho que ainda é preciso fazer para tornar esta framework mais robusta.

II. Zero Trust Networks (ZTN)

"Zero Trust Networks" (ZTN) ou Redes Inseguras é um conceito que foi desenvolvido pelo Departamento de Defesa dos Estados Unidos no inicio dos anos 2000 e que ao longo do tempo estabeleceu-se como esta nova arquitetura ZTN/SDP de segurança de redes. Na sua essência, ZTN é centrado na ideia que que uma organização não deve confiar em algo automaticamente, não importa se esse algo seja externo ou interno ao perimetro, visando a proteção dos bens da organização.

Redes Inseguras possuem tres conceitos chave: [1]

- O conceito de confiança de uma rede, onde se torna natural garantir que todos os recursos estão devidamente assegurados, independentemente de qualquer carecteristica (remetente, localização, tipo, etc) do tráfego.

- O conceito de adoptar uma estratégia de privilégio minimo que aplica um controlo de acesso que elimine a possibilidade de aceder bens restritos.
- Monitoramento e análise permanente do tráfico com a finalidade de detectar atividade suspeita.

Como o SDP é agnostico à infraestructura baseada em IP e tem como objetivo oferecer segurança para todas as conexões parece que o SDP está alinhado com o conceito de redes inseguras, portanto parece lógico que a arquitetura do SDP seja a melhor forma para implementar o conceito das ZTN. Podemos olhar para ZTN como a filosofia por detrás da arquitetura do SDP.

III. Software Defined Perimeter (SDP)

Antes de entramos a fundo no assuntos em torno do SDP, convém esclarecer que o SDP em nada é similar ao paradigma do SDN. O modelo SDN permite melhorar a eficiencia da configuração de uma rede de forma a melhor a performance e o monitoramento da mesma, ou seja, o seu foco é na eficiencia do trafego, não em segurança ou privacidade. Embora o SDP possa ser integrado de forma a beneficiar da implementação do SDP na rede, não necessita de um. Podemos dividir os motivos que levaram à criação do SDP em três categorias: segurança, privacidade e disponibilidade. Nestas categorias existem o desafios relacionado com autenticação, controlo de acesso, integridade e privacidade dos dados e disponibilidade dos dados. O SDP é um conceito que tem como objetivo de dotar uma organização com o poder de aplicar a funcionlidade de um perimetro de forma a proteger os seus bens na rede. Isto é conseguido adoptado componentes lógicos (software) ao invés dos tradicionais dispositivos físicos. Estes componentes ficam a cargo da organização responsável por proteger os bens, normalmente a própria organização e servem como um mecanismo de proteção. Estes componentes irão implementar a filosofia de redes inseguras que designa-mos pela framework SDP, onde é concedido o acesso e a visibilidade dos serviços de um servidor após validar e autenticar a identidade do dispositivo, em comparação com os outros modelos anteriores, onde a autenticação acontece depois do utilizador se ligar ao sistema. A framework SDP também define uma separação, entre a componente que estabelece a validação e autenticação da componente responsável pela troca de dados entre o servidor e o dispositivo autenticado.

IV. Arquitetura SDP

As principais funcionalidades do SDP são a abilidade de autenticar dispositivos, autenticar e autorizar utilizadores e prover serviços de forma dinâmica. Para tal a arquitetura do SDP é composta e dependente de cinco protocolos de segurança. [2]

A. Single Packet Authentication (SPA)

SPA permite ao SDP rejeitar todo o tráfico originário de dispositivos não autenticados. Para isso ele exige que apenas um pacote seja enviado para o controlador para que ele possa autorizar o dispositivo que está a solicitar um serviço protegido pelo SDP.

B. Mutual Transport Layer Security (mTLS)

TLS foi projetado para fornecer autenticação de um dispositivo de forma segura. Foi projetado originalmente para desempenhar funções de autenticação mútua, contudo, na maioria dos casos, TLS é apenas usado para autenticar servidores a clientes, e não clientes a servidores. O SDP faz uso do TLS completo, ou seja, de autenticação mútua.

C. Device Validation (DV)

A autenticação mútua assegura que um dispositivo que solicita acesso a um serviço protegido pelo SDP possui uma chave privada válida, mas não prova se a não chave foi roubada. Portanto é a função do device validation provar que a chave usada é usada pelo dispositivo responsável por aquela chave. Outras funções do device validation sao, verificar se o dispositivo está a correr software de confiança e se está a ser usado pelo utilizador intencionado.

D. Dynamic Firewalls

Firewalls tradicionais usam configurações estáticas para limitar o tráfico, baseado nas componentes IP e porta do pacote e cada firewall possui um elevado número de regras. Já uma firewall dinâmica tem apenas uma regra: proibir tudo. Cada IP autorizado é introduzido na firewall de forma dinâmica, permitindo assim comunicações individuais entre dispositivos de forma dinâmica. Na prática o SDP cria um vinculo entre os utilizadores e os dispositivos, e depois de forma dinâmica permite a esses utilizadores acesseder recursos protegidos criando e apagando de forma dinâmica regras na firewall. Esta firewall dinâmica fica localizada nos gateways do SDP.

E. Application Binding (AppB)

Depois da autenticação e autorização de um dispositivo e do seu utilizador for concluída com sucesso, o SDP cria um túnel TLS (encriptado) entre o dispositivo e a aplicação protegida. Este vinculo entre ambos significa que a comunicação só pode acontecer entre estas duas entidades, ou seja, este túnel não pode ser usado por outras aplicações, bloqueando assim qualquer outra interação por parte do utilizador com outra aplicação. Para tal é criado um novo túnel caso o dispositivo e o utilizadores tenham credenciais para tal.

A arquitetura do SDP é constituida por dois componentes: SDP Hosts e SDP Controller(s). Os SDP Hosts podem iniciar conexões (IH de Initiating Host) ou aceitar conexões (AH de Accepting Hosts). As conexões dos SDP Hosts é controlado pelo SDP Controller, via uma conexão segura. É esta estrutura que permite separar a componente de controlo (autenticação e verificação) da componente de transmissão de dados. Isto tem a vantagem de permitir escalar o sistema, pois não terá o "overhead" associado ao controlo da comunicação durante todo o processo da mesma. O IH terá de correr o software do SDP de forma nativa. Os AH, normalmente servidores que providenciam serviços, normalmente situados normalmente na rede da organização, ou então na cloud de outra organização, aceitam conexões vindas do IH, conexões essas criadas pelo

SDP controller. Já o SDP controller deve ser configurado num gateway da organização e tem como função proporcionar a IHs autorizados a serviços do AH. O gateway pode também ser usado para monitoramento, logging, etc. Como forma de realizar as suas funções de controlador, o SDP controller pode recorrer a serviços como SAML, OpenID, Oauth, LDAP, Kerberos, geolocalização, autenticação de multi-fatores, entre outros.

Para compreender melhor o funcionamento do SDP iremos analisar o seu workflow: [2]

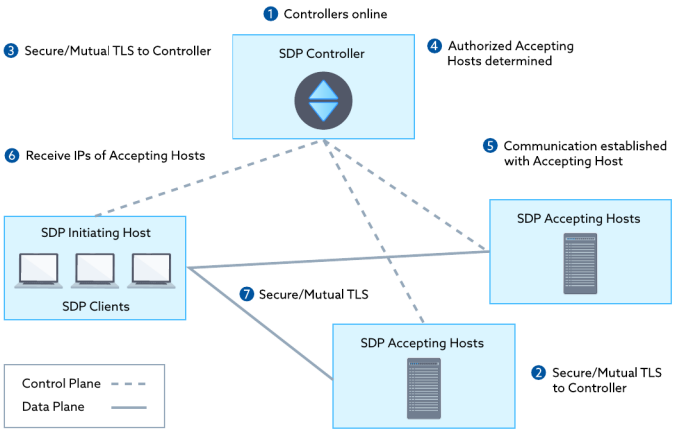

Fig. 1. Workflow do SDP

1) Um ou mais SDP Controllers online e conectados ao serviço de autenticação e autorização.

2) Um ou mais AH online. Estes hosts conectam-se ao SDP Controller. Nesta fase não podem estabelecer conexão com mais nenhum host.

3) Cada IH que pretenda se conectar a um AH, tem de primeiro enviar um SPA para o SDP Controller onde terá a possibilidade de se autenticar.

4) Depois do IH completar a sua autenticação, o SDP determina quais AH o IH tem autorização para se conectar.

5) O SDP Controller informa os AHs listados no passo quatro que podem aceitar comunicações com o respetivo IH, bem como as condições necessárias para estabelecer uma ligação segura.

6) O SDP Controller informa o IH sobre a lista de AH que ele têm autorização para se conectar, e tal como no passo anterior, as condições para estabelecer a ligação.

7) O IH cria uma conexão mTLS para cada AH requesitado e devidamente autorizado.

V. Modelos de Implementação

Os modelos de implementação SDP podem ser caracterizados pela maneira de como são organizadas as interações entre clientes, servidores, gateways e os seus diferentes métodos para prevenir futuros ataques. Os principais modelos são os seguintes:

A. Client-to-Gateway

O SDP usa um proxy que controla as conexões entre clientes e um conjunto de servidores protegidos. Um cliente se conecta a um gateway que, por sua vez, fornece acesso a hosts que fornecem serviços, este é o modelo mais comum. Existem duas maneiras de ser implementado dentro de uma rede para prevenir os seguintes ataques: ataques de movimento lateral, que incluem exploits, varredura de servidor e ataques man-in-the-middle entre outros.

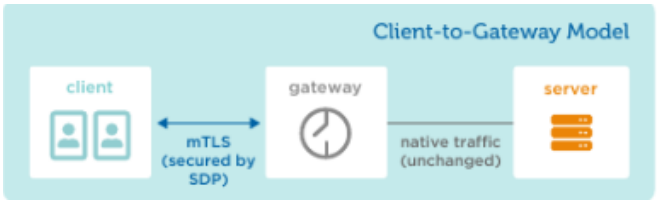

Fig. 2. Client-to-Gateway [3]

B. Client-to-Server

Este modelo tem características e benefícios semelhantes ao Client-to-Gateway , exceto na forma em que o servidor vai ser protegido pelo SDP , ele mesmo vai executar o software host de aceitação em vez do gateway, a escolha deste modelo é normalmente baseada no número de servidores protegidos, metodologia de balanceamento de carga e elasticidade dos servidores.

Fig. 3. Client-to-Server [3]

C. Server-to-Server

O seguinte modelo protege servidores que oferecem serviços de transferência de estado representacional (REST), serviços de protocolo de acesso a objeto simples (SOAP), uma chamada de procedimento remoto (RPC) ou qualquer tipo de interface de programação de aplicativo (API) . Este modelo vai prevenir dos ataques que foram citados no modelo Client-to-Gateway.

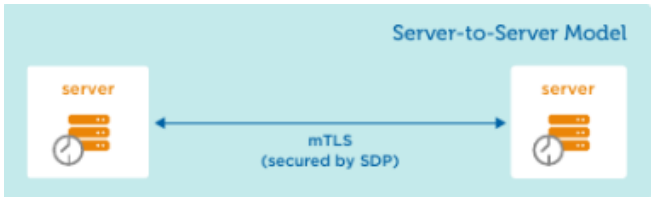

Fig. 4. Server-to-Server [3]

D. Client-to-Server-to-Client

Este modelo SDP permite a criação de uma rede ponto a ponto (P2P) na qual os clientes podem compartilhar seus recursos. Este modelo é mais adequado para organizações que usam aplicativos como chat, videoconferência e telefonia IP.

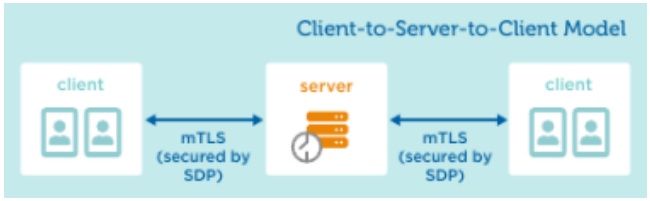

Fig. 5. Client-to-Server [3]

E. Client-to-Gateway-to-Client

Este modelo é uma variação do Client-to-Server-to-Client , oferece suporte a protocolos de rede ponto a ponto que exigem que os clientes se conectem diretamente uns aos outros com base nas políticas de acesso SDP.

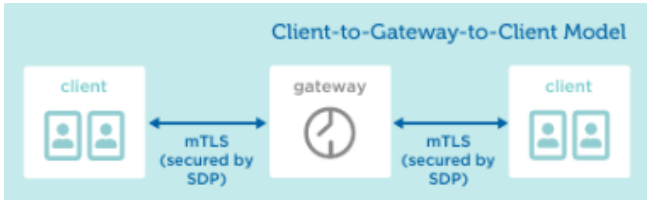

Fig. 6. Client-to-Gateway-to-Client [3]

F. Gateway-to-Gateway

Por último, neste modelo um ou mais servidores ou até mesmo clientes estão protegidos por um Gateway, é principalmente usado para dispositivos em rede e IoT nos quais clientes SDP não podem ser instalados. Como por exemplo impressoras, scanners e sensores inteligentes. Os gateways operam como firewalls e também potencialmente como um roteador ou proxy, dependendo da implementação.

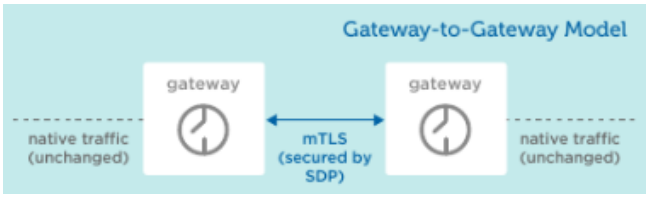

Fig. 7. Gateway-to-Gateway [3]

VI. SDP vs Modelo VPN

A. Como é o modelo VPN

A localização é tipicamente um desafio complexo de segurança e a solução, por hábito, passa pela utilização de uma VPN. Tecnicamente, as VPNs disponibilizam um túnel de comunicação seguro e utilizam cifras para o tráfego da rede entre um sistema do utilizador e a rede na nuvem. O acesso remoto seguro é proporcionado através de uma VPN gateway em cada extremo da ligação que queremos estabelecer. Por exemplo, quando queremos estabelecer uma ligação com a infraestrutura de uma organização e a rede na nuvem, ou então quando queremos estabelecer uma ligação direta de um dispositivo remoto do utilizador para a rede da organização. As VPNs fazem uso dos protocolos TLS (Transport Layer Security) ou IPSec (IP Security Protocol) para garantir a privacidade (aumentando a confiabilidade da comunicação) e a integridade das mensagens (conteúdo entregue no destinatário sem nenhuma alteração) [4]. Mesmo tendo um acesso remoto seguro é preciso monitorizar e controlar quais são os utilizadores que podem aceder à rede e que tipo de recursos da rede serão disponibilizados para esses utilizadores. Caso contrário, os utilizadores teriam permissões de acesso a toda a rede. Para obter um nível de segurança razoável, as VPNs requerem a ferramentas extra que atuam como Firewalls que utilizam os endereços IP da origem das ligações para controlarem o acesso aos servidores/serviços. Posto isto, em termos

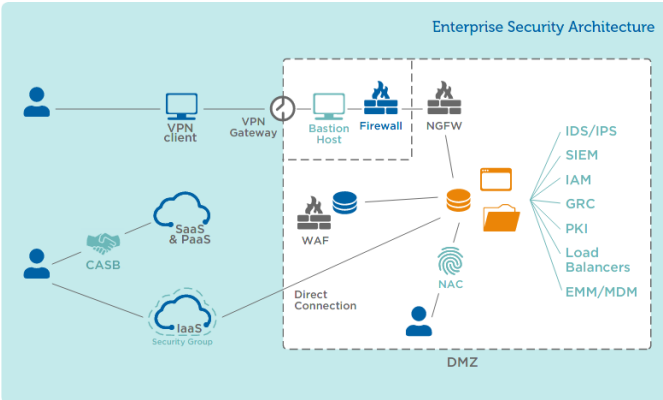

Fig. 8. Modelo com VPN [3]

de disponibilidade as VPNs acabam por ser uma boa solução já que acaba por tornar os recursos invisíveis publicamente e protege os recursos contra ataques do estilo de negação de serviço. Porém, existem algumas desvantagens:

- Pode haver latência nas ligações e custos para a largura de banda que é utilizada;
- O próprio servidor VPN é exposto na Internet;
- Na necessidade de acesso a vários locais remotos, as VPNs podem impedir a ligação e obrigarem o utilizador a terminar as ligações para poder criar uma ligação nova
- Numa circunstância de mudanças na infraestrutura de uma organização, como adotar uma tecnologia IaaS (Infrastruture as a Service) recorrendo a serviços cloud, as configurações VPN precisam de políticas de firewalls em vários locais e por isso estas configurações tornam-se complexas e difíceis de prevenirem o acesso indevido.

B. SDP vs VPN

As VPNs têm lacunas que as tornam inconvenientes para os tempos de hoje pelo facto de atribuírem um acesso à rede com toda ou nenhuma liberdade para um conjunto de servidores. Com a dinâmica do perimetro de hoje (IoT ; Software as a Service) [5] nos tempos de hoje, as VPNs não têm a agilidade necessária para se poderem moldar às possíveis mudanças na rede ou às mudanças dos conjuntos de servidores. Mesmo que este serviço fosse plausível para uma organização, as VPNs apenas iriam solucionar as questões de segurança para os utilizadores remotos. Ou seja, para os utilizadores locais teria de ser implementada uma nova estratégia de segurança para proteger e controlar o acesso. Ajustar as soluções de segurança consoante o caso de acesso torna as VPNs ineficientes. Elas acabam por ser o grande alvo para as organizações adotarem uma substituição para o SDP.

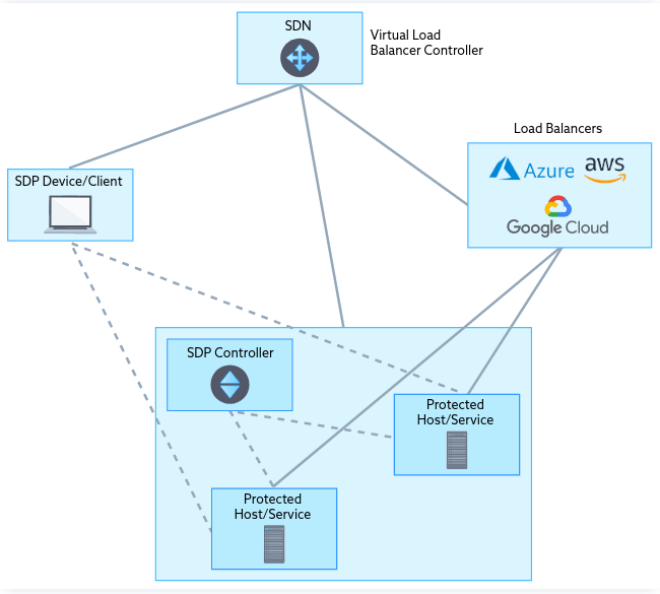

Fig. 9. Modelo com o SDP

Pontos positivos da substituição:

- Com o SDP, e tal como as VPNs é preciso haver um software "cliente" para os dispositivos dos utilizadores, contudo os problemas descritos em cima deixam de existir. Este paradigma fornece às organizações acesso remoto seguro e um único ponto de controlo de acessos dos utilizadores aos recursos.
- SDPs podem usar protocolos como Ipsec e TLS para criar VPNs [6] entre hosts, contudo SDPs não são o mesmo do que VPNs. No caso do SDP, com o Controlador SDP, a organização pode criar múltiplos servidores protegidos pelo SDP (via software), enquanto que os custos associados em configurar VPN gateways para cada servidor individual é bastante superior [7].
- A infraestrutura da aplicação de uma organização pode ser implementada na cloud que o SDP garante a segurança da mesma.
- SDP também protege contra ataques de "Denial of Service", enquanto que um gateway de uma VPN está vulnerável a estes ataques e não consegue garantir um acesso remoto com autenticação e validação do utilizador.
- Mesmo os SDPs expostos na internet, através dos SPAs e de firewalls dinâmicas, não fornecem nenhuma visibilidade de fora para dentro do perímetro de rede. Posto isto, com o SDP, autentica-se e verifica-se um dispositivo para cada sessão e apenas se concede privilégios mínimos. O que reforça a ideia de POLP (Principle of Least Privilege), que defende que seja criada uma camada de abstração sobre uma rede e que qualquer unidade interventiva na rede (um processo, um utilizador, um router, etc) só poderá ter acesso aos recursos e à informação enquadrada no propósito do assunto da unidade. Com isto, consegue-se mitigar os modelos de ameaças laterais que estão presentes em ambientes VPN.

VII. Deteção e Prevenção- Problemas versão atual do SDP e o que SDP resolve

Vantagens de um SDP: [5]

- Modelo de confiança zero: Nenhum dispositivo ou usuário é confiável até que seja identificado por um controlador SDP. A conexão entre usuários e recursos é dinâmica e criptografada.
- Não necessita de Firewall: Permite um novo perímetro definido por software e não mais por firewall.
- Acesso a determinados recursos. Um controlador SDP conecta usuários a um recurso apenas se eles tiverem permissões de acesso. É possível restringir o acesso para uma determinada função, grupo de usuários ou um único usuário.
- Ocultar recursos numa empresa. Um SDP pode ocultar qualquer informação de estranhos, incluindo os endereços de servidores DNS. Os usuários identificados podem se conectar apenas aos recursos aos quais têm acesso - todos os outros estão ocultos deles.
- Escalabilidade e flexibilidade. podemos adicionar um novo recurso (aplicativo, servidor, base de dados, etc.) é mais fácil dentro de um SDP porque pode simplesmente adicioná-lo a um Host. No modelo de segurança de perímetro tradicional, é preciso adicionar o recurso a todas as soluções de cibersegurança que implementar.

- Extensibilidade. Um SDP é construído em componentes baseados em padrões, como TLS mútuo e VPNs. Ele garante fácil integração com outros sistemas de segurança padrão.
- Suporte para uma variedade de dispositivos (incluindo IoT). O SDP protege conexões para qualquer tipo de dispositivo, usando um conjunto de dados como credenciais.
- Transferências de dados criptografadas. Todas as conexões entre hosts e controladores são criptografadas com TLS, SAML ou X.509.
- Superfície de ataque de rede reduzida. Um SDP restringe o amplo acesso à rede o que torna difícil os hackers usarem as suas ferramentas de ataque. É muito difícil para os hackers atacarem algo sobre o qual não sabem nada.

Desvantagens de um SDP [8]:

- Controlador: torna-se num alvo prioritário para futuras ataques.
- Vulnerabilidade do controlador: Em uma arquitetura SDP, os controladores têm uma função vital, pois conectam dispositivos a recursos protegidos. Se os controladores estiverem offline, é impossível estabelecer uma conexão com os recursos.
- Interrupção da rede durante a implantação do SDP. Um SDP difere muito dos controladores de segurança de rede tradicionais. Em grandes empresas, a integração de uma solução SDP pode causar interrupções na rede e na infraestrutura porque vai ser preciso reconfigurar todos os dispositivos e aplicativos.
- Atualizações de configuração para aplicativos. Os administradores de sistema levarão muito tempo para atualizar todos os aplicativos e recursos necessários para converter em SDP.
- Limitações do dispositivo. Apesar do suporte para muitos dispositivos modernos, pode ser um desafio conectar roteadores antigos ou dispositivos específicos do fornecedor ao software SDP.

VIII. Conclusão e Análises críticas

Este artigo descreveu o modelo SDP como uma solução para vários problemas associados a segurança de redes, tendo demonstrado sucesso em hackathons, no ramo militar e em múltiplas organizações, tendo algumas delas adotando um modelo similar, mas proprietário, como o caso da google com o BeyondCorp. Constatou-se que é necessário várias tecnologias e processos que ofereçam ocultação da infraestrutura, de aplicativos e controles de acesso, bem como prover conexão segura para proteger redes e servidores. Tudo isto permitiu criar segurança, devido às formas de controlo de identidade, ao nível da rede e não da aplicação. Contudo é obvio que o SDP não resolve todos os problemas e apesar de também ter uma aplicabilidade grande, devido ao facto da área da cibersegurança, ser uma área muito dinâmica faz com que o modelo do SDP ou qualquer outro modelo, não possa ser aplicado de forma bem sucedida em todas as situações possíveis. Embora o modelo do SDP tenha tentado criar um modelo que pudesse ser adotado pelo maior número de organizações possíveis e de forma acessível, com o intuito de diminuir os ataques que se tem registado. Posto isto nós acreditamos que o SDP é um modelo que veio para somar e ajudar a combater muitos problemas antigos que continuavam sem resposta como o DDoS, escalar privilégios, entre outros, e com a vantagem de poder lidar com desafios modernos associados com a cloud (software as a service) e Internet of Things. Assim como, de ser implementado sem exigir muitas alterações na parte aplicacional desses serviços. Contudo nova investigação continua a ser feita, explorando como integrar o SDP com outros paradigmas como o caso dos VPNs.

References

[1] Cloud Security Aliance (CSA) (2020) Software-Defined-Perimeter-and-Zero-Trust (PDF)

[2] Cloud Security Aliance (CSA) (2014) SDP Hackathon Whitepaper (PDF)

[3] Cloud Security Aliance (CSA) (2019) SDP Architecture Guide Web (PDF)

[4] Francesco Palmieri (2003) VPN scalability over high performance backbones evaluating MPLS VPN against traditional approaches (PDF)

[5] SDP Working Group - CSA (2016) Software Defined Perimeter for a Infrastructure as a Service (PDF)

[6] Everson L. Rosa Lucion, Raul Ceretta Nunes (2018) Software Defined Perimeter: improvements in the security of Single Packet Authorization and user authentication (PDF)

[7] Abdallah Moubayed, Ahmed Refaey, and Abdallah Shami (2019) Software-Defined Perimeter (SDP): State of the Art Secure Solution for Modern Networks (PDF)

[8] Waverley Labs LLC and Juanita Koilpillai – Warveley Labs LLC (2017) Software Defined Perimeter (SDP) A Primer for CIOs (PDF)