クラウド時代に求められる最新の認証方式

ソフトウェア・ディファインド・ペリメタ

(Software Defined Perimeter : SDP) の活用

CSA ジャパン　SDP ワーキンググループ

バージョン 1.0

本書の提供について

本書「**クラウド時代に求められる最新の認証方式　ソフトウェア・ディファインド・ペリメタ (Software Defined Perimeter ：SDP)の活用**」は、CSAジャパン SDPワーキンググループの以下のメンバーが作成し公開したものです（順不同、敬称略）。

生田隆由：　SDP ワーキンググループ　リーダー
塩田英二
斎藤知明
斉藤晃一
勝見勉
矢部沖比古
上田光一
橋本健太
諸角昌宏

また、本書は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2016 年 4 月 8 日	バージョン 1.0	

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能です。
http://cloudsecurityalliance.jp

2016 年 4 月 8 日

© 2016 一般社団法人　日本クラウドセキュリティアライアンス

コンテンツ

はじめに.....1
1. SDP の構成.....2
2. SDP の動作.....3
3. SDP の実例.....4
4. SDP とリモート VPN 接続の違い.....5
5. SDP の安全性.....5
おわりに.....6
参考文献.....6

はじめに

ソフトウェア・ディファインド・ペリメタ (Software Defined Perimeter ：SDP)は、 ネットワークを経由した様々な脅威からアプリケーションインフラや利用者の情報を守るための機能です。

従来、企業の外部と内部の間に境界としてファイアウォール等の物理的な装置を設置して内部へのアクセスまたは外部へのアクセスを制御してきました。これらの機能は、外部からの脅威をブロックして内部を守る単純な機能としては有効でした。しかし、昨今、BYOD 対応、内部に入り込んでのフィッシング攻撃対応、また、外部にある各種クラウドの利用が増えてくると従来の防御方法では対応が難しくなってきました。

SDP は、その名前に由来するように「境界線（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更して安全にデータを転送する」技術です。SDP は、常に動的に相手先のアドレスなどを決定するため、その通信経路を外部侵入者から発見されず、従って、攻撃やデータ漏洩・侵害を防ぐ仕組みを提供することができます。

また、SDP は、インターネット上、プライベート網の両方で利用でき、また、プライベートクラウド、パブリッククラウドとも非常に親和性が高い仕組みとなっています。更に、SDP は、PKI、 TLS、IPsec、SAML などの標準技術を利用しており、フェデレーション、デバイス認証、地域認証などの複数の標準化された認証の仕組みを合わせて構築するため、技術が進歩し新しいトレンドができたとしても、それらの最近のトレンドの技術を組み合わせてセキュリティ機能を高めていくことができます。

そのため、実際、暗号化や情報セキュリティを扱う RSA 会議や、国際的に活動を展開しているクラウドセキュリティアライアンス（CSA）の主催する会議において、多くの注目を集めています。

© 2016 一般社団法人　日本クラウドセキュリティアライアンス

1. SDP の構成

SDP は、2 つのコンポーネントで構成されます。SDP ホストおよび SDP コントローラとなります。SDP のホストは、接続の開始依頼を行う Initiating-SDP ホストと接続の相手先である Accepting-SDP ホストに分かれます。全てのやりとりは、SDP コントローラにて管理され、セキュリティで保護された制御チャネルを介して相互に 実施され、「制御する機能」と「データを管理する機能」は完全に分離されています。（図 1 参照）

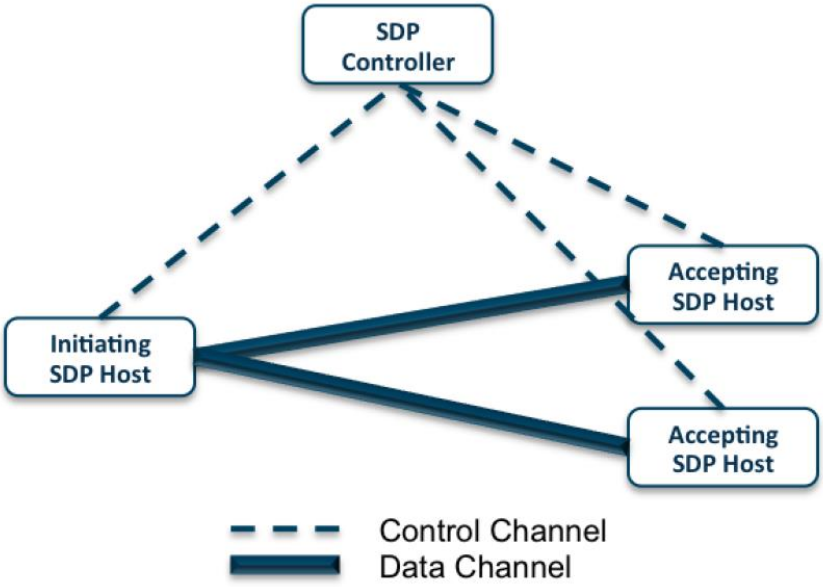

図 1: SDP の構成：SDP ホストと SDP コントローラ

1.1 SDP コントローラ

SDP コントローラは、認証局、地理認証、外部の認証サーバなどと情報連携を行い、利用者のデバイス認証と ID 認証を行い、どの SDP ホストと通信を行うかを管理します。

1.2 Initiating-SDP ホスト

Initiating-SDP ホストは、接続の依頼元であり、本人認証、デバイス認証のため、SDP コントローラに接続します。Initiating-SDP ホストは、ハードウェア、ソフトウェアの登録情報など登録されている情報を SDP コントローラに送り、ネットワーク上で識別が可能な IP アドレス等の情報が返信されることを待ちます。

1.3 Accepting-SDP ホスト

Accepting-SDP ホストは、SDP コントローラの要求においてのみ接続を許可し、その後、指定された Initiating-SDP ホストからの接続を待ちます。

© 2016 一般社団法人　日本クラウドセキュリティアライアンス

2. SDP の動作

SDP の動作の流れは以下の通りです。（図２参照）

1. SDP コントローラがオンラインとなります。
2. Accepting-SDP ホストは、SDP コントローラとセキュアな VPN 接続を確立します。
3. Initiating-SDP ホストは、SDP コントローラとセキュアな VPN 接続を確立します。
4. SDP コントローラにて、Initiating- SDP ホストから送られてきたデバイスと本人情報に基づいて認証を行い、接続依頼先に Accepting-SDP ホストが存在するかを確認します。
5. 接続依頼が正しい場合、SDP コントローラは、Accepting-SDP ホストに対して、Initiating-SDP ホストからの接続要求を送ります。
6. SDP コントローラは、Initiating-SDP ホストに対して、アクセスが可能な Accepting-SDP ホストのネットワーク情報を送ります。
7. Initiating- SDP ホストは、アクセスが許可された Accepting-SDP ホストに対して VPN 接続を依頼し、相互に Initiating- SDP ホストと Accepting-SDP ホストが通信を開始します。（一連の通信が終わり次第、当該の経路はなくなり、新たな接続要求によってのみ接続が再開されます。）

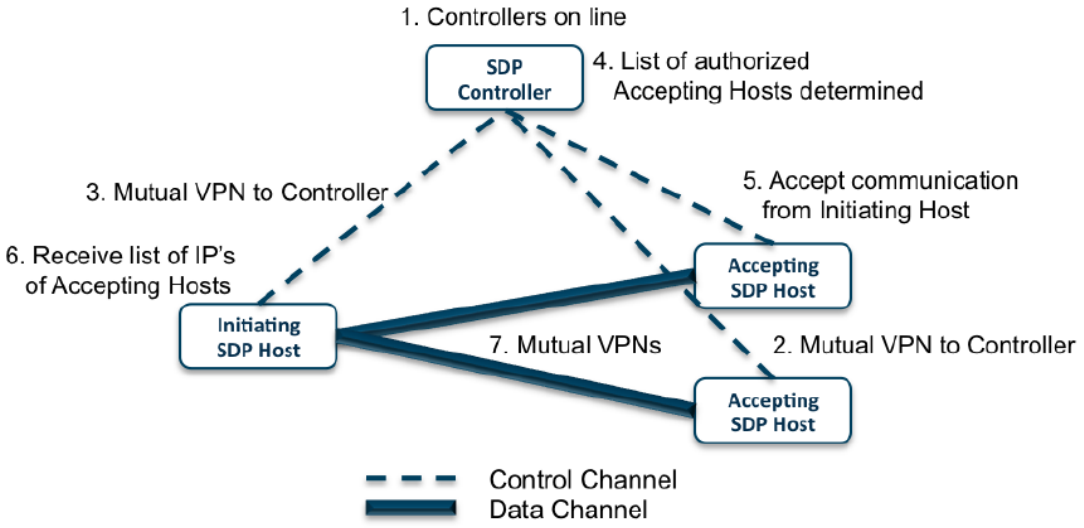

図 2: SDP の動作

© 2016 一般社団法人　日本クラウドセキュリティアライアンス

3. SDP の実例

SDP を利用した企業における実例を２つご紹介します。3.1 は企業が社内システムを安全に利用するため SDP 機能を利用するケースであり、3.2 は複数のクラウド利用を効果的に、かつ安全に利用するため SDP 機能を利用するケースです。

3.1 重要アプリケーションへのアクセス

社内、社外のどこからでも社内の重要アプリケーションへ安全なアクセスすることができます。例えば、経営者だけがアクセスできるサイトには、限定された役員のみがアクセスできます。つまり、権限のないユーザは保護されている企業のアプリケーションやデータを見つけることができず、攻撃者からの侵入を防止することができます。（図 3 参照）

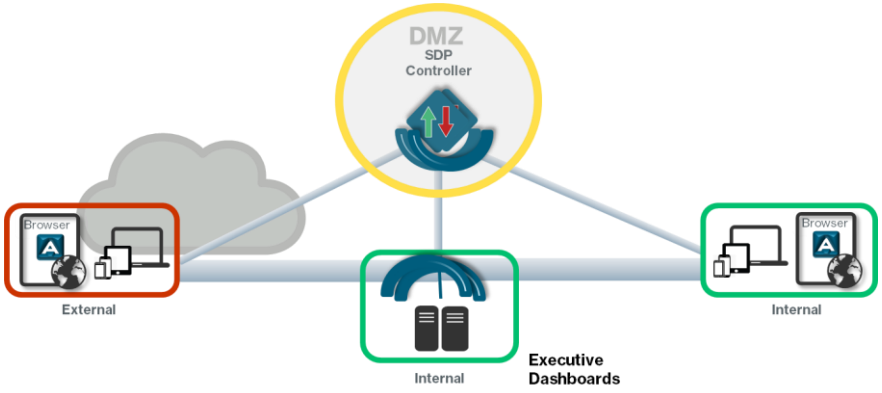

図 3: 重要アプリケーションへのアクセス

3.2 パブリッククラウドサービス

様々なパブリッククラウド（IaaS）を複数利用してサービスを構築します。SDP コントローラでは、接続する会社、ユーザ・端末を判断して、接続可能なパブリッククラウドを判定します。（図 4 参照）

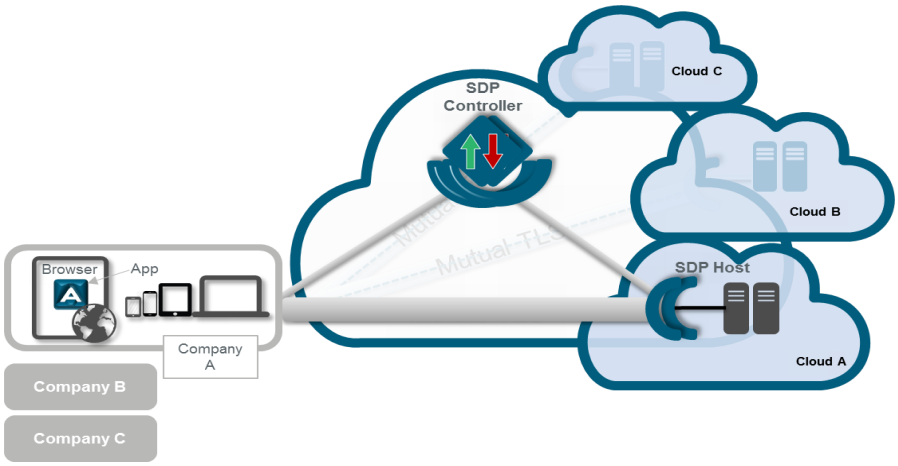

図 4: パブリッククラウドサービス

© 2016 一般社団法人　日本クラウドセキュリティアライアンス

クラウド利用には、他にも様々な利用ケースがあります。プライベートクラウドとハイブリッドクラウドの事例では、SDP をプライベートクラウドとパブリッククラウドの統合に利用しました。分離したパブリッククラウドのインスタンスを公開しないように保護するこができ、また、プライベートクラウドとパブリッククラウドのインスタンスを 1 つのクラウドクラスタのように取り扱うことができました。

4. SDP とリモート VPN 接続の違い

SDP は Initiating-SDP ホストと Accepting-SDP ホストの間で VPN を構築するため IKE プロトコルを利用した IPsec や TLS のようなセキュリティプロトコルを利用します。ただし、SDP と VPN は同じではありません。その主な違いは以下の通りです。

- SDP の場合、SDP コントローラを経由し、保護されたサーバと接続するため、アクセスしてくるユーザの接続許可を事前に識別します。
- 接続許可の識別は、端末認証、各ユーザ固有のディレクトリサービス等の複数の認証方式を組み合わせて実施するため、認証能力が非常に高くなります。
- 接続先となる Accepting-SDP ホスト（アプリケーションの実態があるホスト）のネットワーク情報は動的に個別に設定され、データは暗号化され、デバイス認証と連携して動作するため、このホスト自身が直接の攻撃を受けることがありません。
- SDP の仕組みはソフトウェアで制御されているため、クラウド環境とも非常に親和性が高くなっています。（主だったクラウドサービス事業者が本技術の検証に参加しています）

このように SDP を利用することで、簡易に、柔軟に、しかもセキュリティ機能を高めることができることとなります。

5. SDP の安全性

SDP の構成において、外部より SDP コントローラをネットワーク情報が識別することは可能であり、SDP コントローラに対する攻撃を心配する声がありました。しかし、SDP の構成と動作手順では、最初に、SPA(Single Packet Authorization)を利用し、認証されていない端末からのアクセスは全て破棄します。TCP ストリームは、この認証を通過したアクセスのみが対象となり、コントローラ側にかかる負荷は非常に小さく、テラバイト級の攻撃に耐えられることを証明しました。なお、2014 年より開始された Hackathons テストでは、これらの SDP コントローラの安全性、安定性をライブで紹介するものとなりました。（http://www.hacksdp.com）

© 2016 一般社団法人　日本クラウドセキュリティアライアンス

おわりに

2013 年より SDP は情報セキュリティを扱う RSA 会議や、クラウドセキュリティアライアンス（CSA）において審議され、現在、SDP を利用した各種サービスが商用サービスとして開始されました。また、SDP は、非常に負荷の少ないアクセスプロトコルを利用しているため、今後のモバイルアプリケーションサービスや IoT（Internet of Things）サービス向けのソリューションとして期待されています。CSA SDP ワーキンググループでは、今後とも、多くの事例を検証し、その活用方法について引き続き活動報告をさせていただきます。

参考文献

Software Defined Perimeter Working Group, Software Defined Perimeter

Editors
Brent Bilger, VP Solutions Architecture, Vidder
Contributors
Alan Boehme, Director CSA; Chief of Enterprise Architecture and Emerging Technologies, The Coca-Cola Company
Bob Flores, Former CTO, Central Intelligence Agency
Jeff Schweitzer, Chief Innovation Architect, Verizon
Junaid Islam, CTO, Vidder

© 2016 一般社団法人　日本クラウドセキュリティアライアンス