SDP による
真のゼロトラスト実装

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance®

The permanent and official location for Software Defined Perimeter Working Group is

https://cloudsecurityalliance.org/software-defined-perimeter/

Acknowledgments

Lead Authors:

Juanita Koilpillai

Nya Alison Murray

Contributors:

Michael Roza

Matt Conran

Junaid Islam

Aditya Bhelke

Eitan Bremier

Tino Hirschmann

Steve Swift

Sam Heuchert

John Markh

Roupe Sahans

Oscar Monge Espana

Gerardo Di Giacomo

Vladimir Klasnya

J. Lam

Clara Andress

Dan Mountstephan

Manoj Sharma

CSA Analysts:

Shamun Mahmud

CSA Global Staff:

AnnMarie Ulskey (Design)

日本語版提供に際しての告知及び注意事項

本書「SDP による真のゼロトラスト実装」は、Cloud Security Alliance (CSA)が公開している「Software Defined Perimeter (SDP) and Zero Trust」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。

翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。

この翻訳版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
2020 年 07 月 20 日	日本語版 1.0	初版発行

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1．　責任の限定

CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2．　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3．　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。

(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　原典がある場合の制限事項等

本書が Cloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「Software Defined Perimeter (SDP) and Zero Trust」の日本語訳は、CSA ジャパン SDP ワーキンググループの有志により行われました。

作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。

以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

小野　貴博

小池　泰治

髙岡　隆佳

諸角　昌宏

Table of Contents

はじめに

Software Defined Perimeter (以下 SDP)はネットワークセキュリティ・アーキテクチャの一つであり、ＯＳＩ参照モデルにおける層（レイヤー）１－７に対し、セキュリティを提供するものである。ＳＤＰ実装において資産（Asset）は隔離される。そして、端末からの単一のパケットを用いて、コントロールプレーンで信頼を確立し、データプレーンを経由して隔離された資産へのアクセスを確立する。ＳＤＰを活用したゼロトラストの実装により、企業ネットワークの境界を狙う、様々な新しい脅威に対し、組織を保護することが可能となる。より複雑化する攻撃面への対応が求められる企業において、ビジネス推進のためのセキュリティ対応力をＳＤＰの実装により向上できる。

元来、Zero Trust Network (ZTN) コンセプトは、米国 Department of Defense (DoD)の Netcentric Service Strategy の一部として、２０００年初頭に発表されたものである。なお、DoD が Global Information Grid (GIG) Network Operations (NetOps) Black Core ルーティングを定義し、アーキテクチャを確立したタイミングでもある。このコンセプトは DoD 内有識者コミュニティにより、現在のＺＴＮ/SDP フレームワーク[1]に発展した。米フォレスター・リサーチ社が、エンタープライズセキュリティチームに対し ZTN が有用であることを宣伝し始めたのもちょうどこの頃である。今日、ゼロトラストの定義は広く解釈されてきている。

フォレスター社のレポート"Zero-Trust-eXtended-ZTX-Ecosystem"において、ネットワーク境界の変化が意味するところについて言及している。それは、歴史的なゼロトラストアーキテクチャのコンテキストが「拠点間ネットワークおよびホストのセグメント化とセキュリティ徹底による保護モデル」から急速に脱却することである。現在の企業のセキュリティ戦略にあるような、「性善説に基づく信頼」を排除していく課題に対し、現行のモデルで対応できることをフォレスターは主張している。また、新しい様々なソフトウェアベースの手法も有用としている。しかしながら、"extended ecosystem framework."[2]への新しい方向性について指し示していない。

[1] https://www.secureworldexpo.com/industry-news/pentagon-zero-trust-security-framework

[2] https://www.em360tech.com/wp-content/uploads/2019/04/The-Forres- er-Wave%E2%84%A2_-Zero-Trust-eXtended-ZTX-Ecosystem-Providers-Q4-2018-1-1.pdf

本質的にゼロトラストはネットワークセキュリティのコンセプトであり、組織は、性善説に基づき境界内外のあらゆるものを信用するべきではない、とある。ゼロトラストの実装には、資産に接続するもの全てに対し、権限を与える前に検証し、接続が終了するまでの間、継続的にセッションを評価し続ける必要がある。これは図 1 にある通りで、アメリカ国立標準技術研究所 (NIST) が'trust boundaries'として表現している。

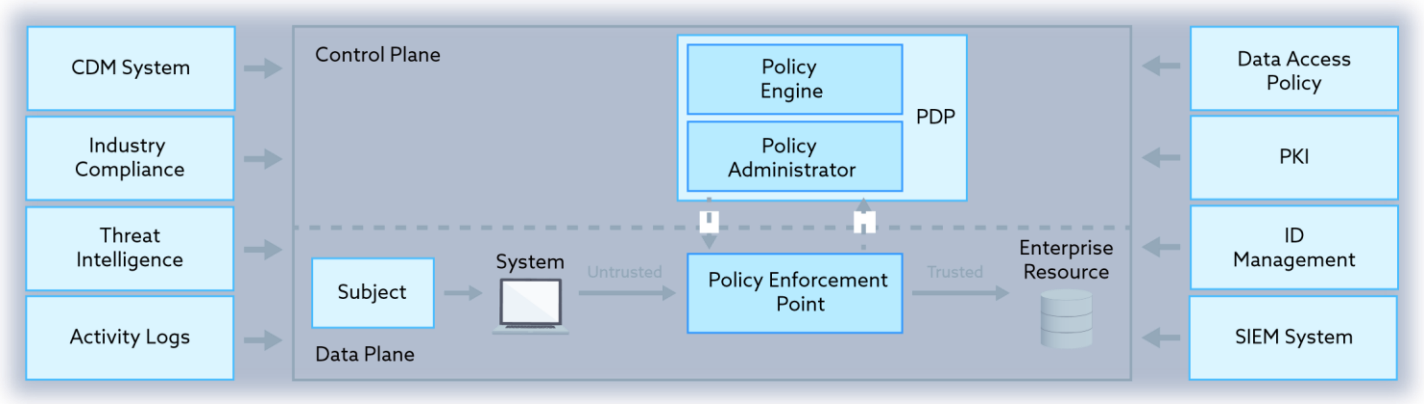

図 1: Source: NIST, 800-207, Zero Trust Architecture 2nd Draft https://csrc.nist.gov/publications/detail/sp/800-207/draft

では何がゼロトラストなのだろうか？フォレスターによれば、以下の 3 つの主なコンセプトがある:

- ネットワークへ信頼のコンセプトを導入、つまり場所やホスト種別、クラウド、オンプレまたは併設されたリソースであろうと、誰がどこから通信しようと、全てのリソースが安全にアクセスできることを保証。
- least privilege strategy (LPS)：最小権限の法則を適用することで、禁止されたリソースへアクセスされるリスクを排除し、アクセス制御を徹底。
- 疑わしい活動の兆候を検出するための、継続的なログ取得とユーザ通信の分析。

SDP とは何か? Software Defined Perimeter (SDP) はゼロトラスト戦略において最も高度な実装方式である。Cloud Security Alliance は下記のように、ネットワークアーキテクチャを定義することを提唱している:

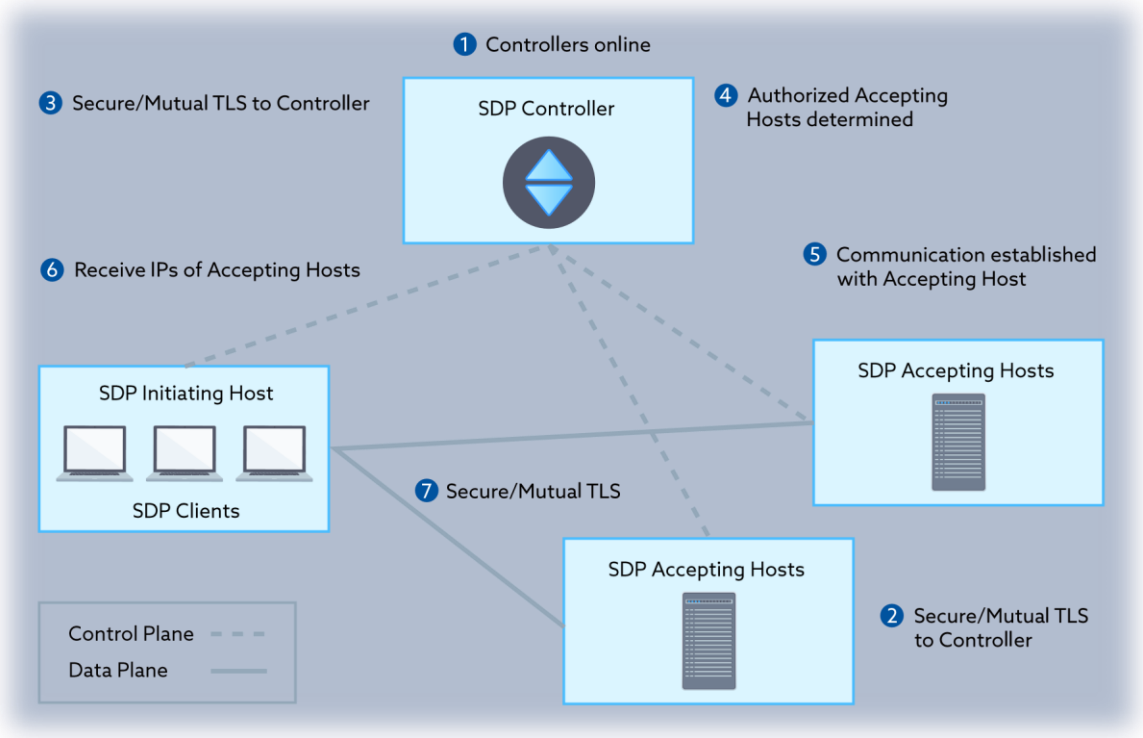

図 2: SDP Architecture (previously published by CSA in SDP Specification 1.0)

- 信頼確立を行うコントロールプレーンと、実際にデータ通信が行われるデータプレーンを分ける。
- 動的な deny-all(場合によっては例外設定を含む) firewall によりインフラを隠蔽し、認証されていないパケットは全てドロップされ、通信分析用にログ取得される。
- Single Packet Authorization(SPA) を利用し、ユーザの認証・認可を行い、サービスを保護するためにデバイスを検査する　– 言わずとも、この制御において最小権限は必須である。

SDP は IP ベースのインフラ下層に依存せず全ての通信をセキュアにし、また OSI 参照モデルのネットワーク層に適用できるため、ゼロトラスト戦略においてベストなアーキテクチャであると言えよう。これは、未知の T L S 脆弱性やセッション確立における TCP/IP SYN-ACK 攻撃などが起こりうるトランスポート層やセッション層にとって重要である。

下記テーブルは ISO Open Systems Interconnection (OSI) モデルと Internet Engineering Task Force (IETF) TCP/IP プロトコルとの関係を示している。

#	OSI 層	TCP/IP 層	プロトコルデータユニット	詳細
7	アプリケーション	アプリケーション	データ	アプリへのネットワークプロセス
6	プレゼンテーション		データ	データ表示と暗号化
5	セッション		データ	ホスト間通信
4	トランスポート	トランスポート	セグメント	エンドツーエンドの接続と信頼性
3	ネットワーク	インターネット	パケット	パスの決定とアドレス
2	データリンク	ネットワークアクセス	フレーム	物理的なアドレス
1	物理		ビット	メディア、信号とバイナリ処理

図 3: Source: https://www.iso.org/ics/35.100/x/ and https://tools.ietf.org/html/rfc1180

目的

SDP による ZTN 実装が、最も理想的なネットワーク接続性を提供できることについて解説する。

想定する読者

既に SDP アーキテクチャを理解した、セキュリティ専門家, CIO, CISO および、大規模な漏洩への施策としてゼロトラストに期待している経営層に向けて、このホワイトペーパーは書かれている。

Zero Trust Networking (ZTN) and SDP

セキュリティ業界では、既存の防御機構が完璧ではないことを認識している。SDP の実装は、TCP/IP および TLS 通信以前に適用されるため、これらまたは他の脆弱なプロトコルを攻撃者が悪用できる可能性を削減する。CSA SDP version1 仕様に沿った SDP 実装は、Open Web Application Security Project (OWASP)が公開している OWASP TOP10 における、DDoS やクレデンシャルの搾取などの攻撃手法を防ぐ実装となっている。SDP は企業の資産を隔離し、関連付けられた個人のアクセスを正しく認証および認可されるまでは、ゼロトラスト実装に基づきアクセスを認めない。

SDP アーキテクチャの概念の根幹にあるのは「ゼロトラスト」である。 SDP の基本的な方針は ABCD : “Assume nothing, Believe nobody, Check everything, Defeat threats.”「何も仮定しない、誰も信じない、すべてをチェックする、脅威を排除する」である。SDP は、OSI 参照モデルのネットワーク層で適用されることを前提としており、ハイブリッドクラウド環境を考慮して、最適なパフォーマンスを確保し、不要なサービス遅延を防ぐためにも、企業の境界に限りなく近くに ZTN を適用するように注意する必要がある。

Why Zero Trust

今日のネットワークセキュリティ実装は、犯罪者がドアの鍵を破り侵入するケースに例えられる。組織はセキュリティを「ドアのロック」に依存し、それが犯罪者によって破られないよう厳重に監視している。それよりも、資産をフェンスで囲い込み、侵入者を排除するために監視した方が良い手法と言える。誰がノックしているかを確認したい場合もあるが、ドアのロックにたどり着くチャンスを与えないことで、悪意のある行為を確実に防止することが望ましい。
これが、効果的なゼロトラスト展開が急務である理由の本質である。さらに、攻撃者の主な目的は、ネットワークに侵入し、ラテラルムーブメントを可能にし、特権アカウントを得てシステムにアクセスすることである。ゼロトラストは、許可されていないユーザの活動を防ぎ、許可されたユーザのアクセスを制限できる。

ただし、今日のネットワークセキュリティの実装においては、下記のような課題がある。

a) 境界の変更

ロードバランサーやファイアウォールなどのネットワークアプライアンスによって保護された、信頼できる内部ネットワークセグメントを持つという固定的なネットワーク境界のあり方は、仮想化ネットワークと、これまでのネットワークプロトコルは安全ではないと認識によって覆された。

実際、IPSec や SSL VPN など、現在の多くのネットワークプロトコルには既知の脆弱性が存在する。さらに、モバイルデバイスと IoT デバイスの大規模な展開は、従来の固定的なネットワーク境界に依存する企業にとって大きな課題となっている。

クラウドの導入により、環境は変化した。上記で言及してきたように、BYOD 要件、マシン間接続要件も加え、リモートアクセスやフィッシング攻撃の増加など、これまでのアプローチは常に困難に向き合わなければならない。

そこに様々な内部デバイスと様々な要件のユーザが存在する。一般的な例として、オンサイトの請負業者がオンプレミスとクラウド、両方のネットワークリソースにアクセスする必要がある場合だ。従業員が顧客やパートナーの場所に移動し、お客様環境で自社のクラウドを活用するといった、ハイブリッドの活用シーンがよく見られる。これらのシナリオにおいて企業の境界は、他の環境にまたがり再定義される必要がある。

[3] https://crypto.stanford.edu/cs155old/cs155-spring11/lectures/08-tcp-dns.pdf

b)IP アドレスの限界

OSI 参照モデル１－４層において、全ての信頼は IP アドレスが拠り所となっていることが問題である: ＩＰアドレスは、デバイスからの要求が正しいものか検査するための、ユーザの情報を何も持っていない。純粋に IP アドレスにユーザコンテキストを持たせることはできない。IP アドレスは単に接続情報を提供するが、エンドポイントまたはユーザの信頼性の指標を提供しない。
TCP はあくまで OSI 参照モデルにおけるトランスポート層の双方向プロトコルであり、内部の信頼できるホストと外部の信頼できないホスト間で、信頼できないメッセージの受信ができてしまう。

IP アドレスに対する変更は、複雑な設定を伴い、結果として設定エラーなどでネットワークセキュリティグループまたはネットワーク制御リストへつけ込む隙を与えてしまう。放置された内部ホストは、ICMP ネットワークサポートなどデフォルトの応答を提供することにより、ハッカーに侵入ポイントを与えてしまう。

最後に、IP アドレスをネットワーク場所の特定に使うべきではない。例えば、IP の動的な付与やユーザの移動に伴う IP 変更などがその理由だ。

c) 統合管理と制御における課題

ネットワーク接続の可視性において、ネットワークセキュリティとセキュリティツールの実装上の問題が残っている。現在、統合管理と制御は、SIEM または SOAR に複数のログを転送し、データを収集することによって実現される。

ネットワーク接続の信頼を、一点に絞ることはできない。ファイアウォールを経由する前に認証を実装することは、リソース負荷の高いタスクとなる。さらに、ほとんどの開発/運用/ネットワークチームにとって、セキュアコーディング手法、WAF、DDoS 対策の使用は、後付けの検討となる。

個々のアプリケーションにセキュリティを徹底する仕組みを提供することは、現在、大きな課題である。アプリケーションおよびコンテナプラットフォームにセキュリティを組み込むには、アクセスコントロール、ID 管理、トークン管理、ファイアウォール管理、コード、スクリプト、パ

イプライン、およびイメージスキャンの統合と、全体のオーケストレーションが必要となる。これは、ほとんどの組織において困難を極めるだろう。

ゼロトラストで解決できること

以下に記載した、今日のネットワークの構築方法における一般的な問題点から、セキュリティを前提としたネットワークの必要性が生じている。

a) 接続後認証- ほとんどのネットワークにおいて、認証前にアクセスできてしまう。暗号化されてようがされていまいが、認証、認可、トークンに基づくアクセス制御システムはいくつもの脆弱性を持つ可能性があるため、アクセス制御メカニズムをバイパスすることもできる。

今日、ネットワーク接続に使用されている主なプロトコルは、TCP である。このプロトコルによりネットワーク接続を確立する場合、接続後認証モデルで動作する。クライアントがアプリケーションへアクセスを求める際、まずネットワーク接続を確立し、次にクライアント認証を行う。一旦認証されれば、データのやりとりが可能となる。

このモデルにおいては、最初にクライアントはネットワークに接続することが許可される、これはつまり認証されないユーザがたどり着けてしまうことになる。クライアントは次に認証を受けるが、接続が許可された後の話だ。これは、認証されないユーザは接続後、不審な活動ができてしまうということを意味する。どのクライアントが健全であるか認証前には判断がつかないため、これらのユーザは、ID が要求されない場合は認証方法をバイパスできてしまう。

デバイスがインターネットに接続する際は IP アドレスを伴うため、組織は今まで下記 3 つについて検討してきた:

- 接続を試みる悪意あるユーザを拒否するために、脅威インテリジェンスを活用する。
- 端末をロックダウンする（例えば脆弱性対策、パッチや設定管理）。ただしこれらの徹底は難しい。
- 次世代ネットワークファイアウォール（NGFW）を実装する。(注: NGFW はユーザコンテキストやアプリケーションコンテキスト、セッションコンテキストを利用するものの、いまだ IP ベースであり、アプリケーション層に脆弱性がある点に注意が必要である。詳細については SDP アーキテクチャドキュメント参照のこと。).

SDP の視点：**これらの手法はどれも、攻撃を防ぐのに効果的ではない。ゼロトラストの実装には、ネットワーク、ホスティング、およびアプリケーションプラットフォームインフラストラクチャに対するあらゆる層の攻撃に対する耐性が必要である。**

b) **エンドポイントの監視はコンピューティング、ネットワーク、人的資源の負荷が高い-** AI を使用したエンドポイント監視では、未承認のアクセスを未だ正しく検出または防止することはできない。保護されたリソースの分離に関する幾つかの手法は、ID の詳細をキャプチャし、承認メカニズムを理解し、人、ロール、アプリケーションの認証資格情報を偽装することにより、時間の経過とともに侵害される可能性がある。

今日、人工知能モデルは、単純な行動モデルであり、ほとんどの場合、複数の線形回帰分析やエキスパートシステム、あるいはパターンを検出するようにトレーニングされたニューラルネットワークに基づいている。AI セキュリティ検出モデルは、十分な期間のデータがある場合は、時系列でのイベントに適応できる。 これらのモデルは発展途上であり、ほとんどが事後の侵入のパターンを検出することとなる。 AI は急速な発展の過程にあるため、熟練したセキュリティ専門家は、未知の脅威を検出および防止するための分析をしなければならない。十分にトレーニングされたモデルに大量のデータを分析させることで、既知の攻撃を検出できる可能性はある。

しかしながら、未知の侵入の手法を検出するには、パフォーマンスの監視、トランザクションデータのパターン分析、およびセキュリティ専門家による分析の組み合わせが必要となる。エンドポイントの監視だけに依存している場合、企業は検出できない攻撃に対して脆弱なままである。

SDP の観点：**機密性の高いデータを保護する最良の方法は、攻撃が発生する前に防止することである。SDP ゼロトラスト展開では、一つのパケット分析に基づいてリスクのあるトランザクションを拒否し、十分でない ID の利用を認識することができる。**

c) **パケット分析はユーザコンテキストを含まない**- ネットワークパケット分析は、その分析がアプリケーション層で起こることから、検出するのは侵入後になる。

接続を識別するネットワークの単一パケット検査は革新的であり、有用である。これらの方法は、TCP / IP および TLS プロトコルとアプリケーションコードと同じくらい安全である。

従来、パケット検査は、侵入検知システム（IDS）を備えたファイアウォール上またはその近くや、監視が必要な領域で行われる。従来のファイアウォールは、送信元ＩＰアドレスに基づきネットワークアクセスを制御する。パケットの検査における根本的な課題は、送信元 IP アドレスからユーザを識別できない点である。分析の手段は IP アドレスが基準となる。DDoS やマルウェアなどの一部の攻撃は既存の手法を使用して検出される可能性があるが、コードインジェクションや資格情報の盗難などの攻撃の大部分は、アプリケーション層で実行されるため、コンテキストの検出が必要となる。

SDP の視点: **逆に、SDP にはパケット検査のエンドユーザコンテキストがある。 SDP ゼロトラスト実装では、SDP ゲートウェイでドロップされたパケットを集め、オフラインで分析することができる。ネットワークデータと組み合わせると、侵入前にリスクプロファイルを検出可能となる。**

ゼロトラスト戦略の実装

ゼロトラストは、ユーザ、デバイス、または個々のパケットを十分に検査、認証、承認されるまでアクセスを保留する方法で、ネットワークセキュリティアーキテクチャを設計するための考え方である。さらに、アクセスの許可に基づき、必要最小限のアクセスのみが許可される。ゼロトラスト戦略を採用するには、次の構成要素が必要である。

a) アクセス前認証

VPN とファイアウォールを使用したゼロトラスト実装を検討してみる (例：メールサーバへのアクセス)。ファイアウォールにブラックリストを登録し、サービスを設定、許可または拒否する IP アドレスを決定する。VPN は、承認された VPN クライアントと適切なキー（証明書など）を持つネットワーク上のユーザのみを許可するように構成できる。一見、ゼロトラストが実装できているように見える。しかし、VPN クライアントのクローンを作成してキーをあるユーザが盗んだ場合、メールサーバにアクセスして他のユーザ名とパスワードを推測し、DDoS、資格情報の盗難などの悪意のある行為を実行することもできる。

一方で、権限のないユーザが既にネットワークにいる場合、他のサーバーへの横方向のアクセスが可能となる。認証前のアクセスにより、ユーザは、アクセス権以上のサービスにアクセスできてしまう。

アクセス前に認証を確実にするために、暗黙の要件がある: 認証のためのコントロールプレーンはデータプレーンから分離する。許容できるレスポンスを確保するには、即時認証のメカニズムも必要だ。

b) ネットワーク接続と露出を制限する

パブリック/プライベートクラウドはもちろんネットワークセキュリティ境界の設定が可能だ。これらは、セキュリティへの階層化アプローチを提供し、監視ツールにログをストリーミングし、洞察とハイブリッドサービスコントロールポリシーを提供する。ただし、これらの機能は、アクセス前に認証に挑戦するという問題には対応していない。

クラウドネイティブプラットフォームとアプリケーションサービスを強力にサポートする手段として、インバウンド/アウトバウンドのセキュリティ構成と企業ネットワークポリシー構成がある。強固な認証と認可のための業界標準の手法として双方向 TLS (two-way SSL) 証明書がある。より良いアプローチは、アクセスの前に認証を要求することだ。SDP ゼロトラスト展開に接続する SDN コントローラーによって提供される通信管理により、ネットワーク層でパケットをドロップまたは転送する。このアーキテクチャにより、S D N インフラは認証失敗時にネットワーク接続を切断できることとなる。

c) 柔軟な信頼認証メカニズム

ネットワークレイヤーVPN とファイアウォール、およびアプリケーションレイヤーファイアウォールと SSL VPN には、本来求められる粒度のアクセス制御は存在しない。ゼロトラストの導入には、暗黙的なポリシーベースの承認だけでなく、ネットワークマイクロセグメンテーションのコンテキストでの ID 認証と、ハイブリッドプライベート/パブリックマルチクラウドシナリオにわたる分散サービス接続と双方向接続が必要となる。

ネットワークレイヤーファイアウォールはその特有の設定がメリットとなる。静的な、ユーザグループは柔軟な信頼を与えるために利用される。同じ IP アドレスで同じサービスへのアクセスを必要とする、役割や部門の異なるユーザグループがあることは珍しいことではない。ファイアウォールのルールは静的で、ネットワーク情報に依存している。これはファイアウォールが動的なコンテキスト、例えばあるネットワーク上のある端末における信頼レベルなどに対応できないことを意味する。よくある例として、ユーザがインターネットカフェなどの危険なネットワークを通じてアクセスを要求する場合がある。 ローカルファイアウォールまたはウイルス対策ソフトウェアがマルウェアにより、または偶然に無効にされた場合、これは従来のファイアウォールでは検出されない。

IPSec VPN の場合は、アクセスを許可する前に認証用の ID 属性にアクセスしない場合がある。代わりに IPSec VPN は、傍受された可能性のあるトークンと資格情報に依存している。 SSL VPN には既知の脆弱性がある。

これらの制限に目を向けることで、きめ細かい信頼認証メカニズムとポリシーベースの承認によるネットワーク境界のゼロトラストアプローチは、より安全であることが分かる。

d) 疑わしい活動の監視

ID 属性認証に失敗した場合を考えてみよう。パケット検査に基づいて疑わしいアクティビティをエンドポイントのロギングおよびモニタリングサービスに転送する機能は、組織がさまざまなソース（主にセキュリティ情報やイベントから）から入力を取得できるようにする SOAR（セキュリティオーケストレーションと応答の自動化）テクノロジーへの非常に有用な情報を提供する。（多くの場合は SIEM（ログ管理システム）を経由。詳細については、SDP アーキテクチャガイドを参照）。SOAR による自動化とは、データを収集し、統合および調整するために開始されるワークフロープロセスを指し、運用インテリジェンスと視覚化グラフおよびダッシュボードを提供してくれる。ゼロトラストの実装は、SOAR AI モデルへのインプットに関する有用なインテリジェンスと疑わしいアクティビティの適切なモニタリングを転送できる。

SDP ゼロトラストの利点

SDP のゼロトラストソリューションは、CSA SDP アーキテクチャ仕様で定義されている次のセキュリティおよびビジネス上の利点がある。

セキュリティ上の利点

利点	詳細
攻撃面の削減	アクセスコントロールとデータプレーンを分離してそれぞれを隠蔽し、ネットワークベースの潜在的な攻撃をブロックすることで、重要な資産とインフラストラクチャを保護
重要な資産およびインフラの保護	隠蔽することでクラウドアプリケーションの保護を向上: • ビジネス・システム担当者に対し、集中制御を提供 • 全ての認証された通信に対し、「いつ、誰が、どこから、何に」を可視化 • 統合化された制御により可視化を提供
接続の拒否により資産を隠蔽	ユーザ/デバイスが認証され、資産へのアクセスが承認されるまで、“deny-all”ファイアウォールを有効化
所有コストの削減	エンドポイントの脅威防止/検出のコストを削減 インシデントレスポンスのコストを削減 統合化された制御における複雑さを軽減
コネクションベースのセキュリティアーキテクチャ	今日のクラウド環境における IP の急増と境界の喪失により、IP ベースのセキュリティが脆弱になっている。そこで、IP ベースではなく、コネクションベースでのセキュリティアーキテクチャを提供する。
統合化されたセキュリティアーキテクチャ	NAC やマルウェア対策などの既存のセキュリティポイント製品では実現が難しい統合化されたセキュリティアーキテクチャを提供できる。SDP は、次の個別のアーキテクチャ要素を統合する。: • ユーザと紐づいたアプリケーション利用

	• 利用者と紐づいたデバイス • ネットワークと紐づいたファイアウォールまたはゲートウェイ
SPA の利用	認証および認可のための統合された制御に基づき、接続を確立
接続の事前確認が必要	誰がどのデバイスから、どのサービス、インフラストラクチャ、その他のパラメータに接続できるかを事前に確認して、すべての接続を制御できる。
リソースへのアクセスを許可する前に認証	コントロールチャネルとデータチャネルを分離して実装 TLS / TCP ハンドシェイクの前に検証を有効 設計時に明示的に詳細なアクセス制御を提供 双方向の暗号化通信の実施が可能
オープンな仕様	コミュニティによる審査を許可 ハッカソンへの参加促進

ビジネス上の利点

利点	詳細
コストおよび労働力の削減	従来のネットワークセキュリティコンポーネントが SDP に置き換えられているため、ライセンスとサポートのコストが削減される。 SDP を使用したセキュリティポリシーの実装により、運用の複雑さと従来のセキュリティツールへの依存を軽減できる。 MPLS または専用回線の使用を最小化または置換することにより、コストを削減できる。組織は、プライベートバックボーンネットワークの使用を削減または排除できる。 組織に効率とシンプルさをもたらし、最終的に労働力を削減できる。
IT 運用の迅速化	IT プロセスは、時としてビジネスプロセスの妨げになることがある。一方、SDP 実装は、IT または IAM イベントによって自動駆動できる。これらの利点はビジネスとセキュリティの要求に応え、IT を加速させる。

GRC 上の利点	従来のアプローチと比較してリスクを低減できる SDP は、脅威を抑制し、攻撃面を減らし、ネットワークベースの攻撃とアプリケーションの脆弱性の悪用を防ぐ。SDP は、GRC システム（SIEM と統合する場合など）にフィードして応答し、システムとアプリケーションのコンプライアンス活動を合理化できる。
コンプライアンス上の利点	コンプライアンスデータの収集、レポート、および監査のプロセスは、登録済みデバイス上のユーザから特定のアプリケーション/サービスへの接続を集中制御を通じて SDP によって改善できる。SDP は、オンラインビジネスの接続のトレーサビリティをより高める。SDP によって提供されるネットワークマイクロセグメンテーションは、コンプライアンスの範囲を削減し、コンプライアンスレポートの取り組みに大きな影響を与える可能性がある。
安全なクラウドコンピューティングへの適用	パブリッククラウド、プライベートクラウド、データセンター、および混在環境でアプリケーションをサポートするために必要なセキュリティアーキテクチャのコストと複雑さを軽減することにより、企業がクラウドアーキテクチャを迅速、確実、かつ安全に採用できるよう支援する。新しいアプリケーションは、他のオプションと同等またはそれ以上にセキュアかつ迅速に展開できる。
ビジネスの俊敏性とイノベーション	ビジネスがプライオリティに従って迅速かつセキュアに実装できる。例として: • オンプレミスのコールセンターエージェントから在宅ベースのエージェントへの移行が可能 • コアビジネス以外の機能を、専門のサードパーティにアウトソーシングできるようにする • リモートのサードパーティネットワークおよびロケーションで顧客向けキオスクを可能にする • 顧客サイトへの企業資産の展開を可能にし、顧客とのより強力な連携を実現し、新しい収益を生み出す

ビジネス革新を促進	• セグメンテーションと権限管理を通じて IoT の採用を促進 • 既存のサービスに依存せずに、デジタル推進エンジニアとの作業が可能 • ブロックチェーンを組み合わせた次世代の安全なシステムを構築

SDP ゼロトラスト戦略的なアプローチと PoC

企業の大規模な侵害に焦点を当て、本質的なサービスとデータのプライバシー保護のために機微情報をセキュリティの高いネットワークに分離することは、重要な対策だ。CSA 2019 クラウドセキュリティ脅威レポートによる最近の分析では、クラウドマルウェアのインジェクションや DDoS インシデントに加えて、危険な人間の行動が情報漏えいの大部分を占め続けていることが示されている。

CSA の SDP プロトコルとして知られる、新しいネットワークアーキテクチャパラダイムは 2013 年に開発された。機密データにアクセスする前に、単一パケット検査からネットワーク接続を確実に識別するアーキテクチャを作成するように設計された。このアーキテクチャで明らかなのは、信頼を確立するコントロールプレーンが、実データを転送するデータプレーンから分離されていることである。これにより、TCP および TLS 終端に固有の脆弱性、および IP ネットワークアドレス変換（NAT）テーブルによるネットワークファイアウォールの複雑性が排除できる。

SDP は、クラウド上の企業セキュリティおよび法的なセキュリティを迂回することを防ぐ。 SDP 実装を採用すると、信頼を確立することとデータ転送の分離が強制される。ネットワークのセグメンテーションとマイクロネットワークの確立は、マルチクラウドの展開にとって非常に重要であり、ソフトウェア定義の境界型ゼロトラストアーキテクチャを採用することからも実現できる。

多要素認証、および改善されたアクセス制御/許可メカニズムを SDP に組み合わせすることで、組織はセキュリティの脆弱性と大規模な侵入に対処するための戦略的な道を歩むことができる。SDP は、実行時の検出と応答に加え、構成と展開時にセキュリティポリシーを適用する。

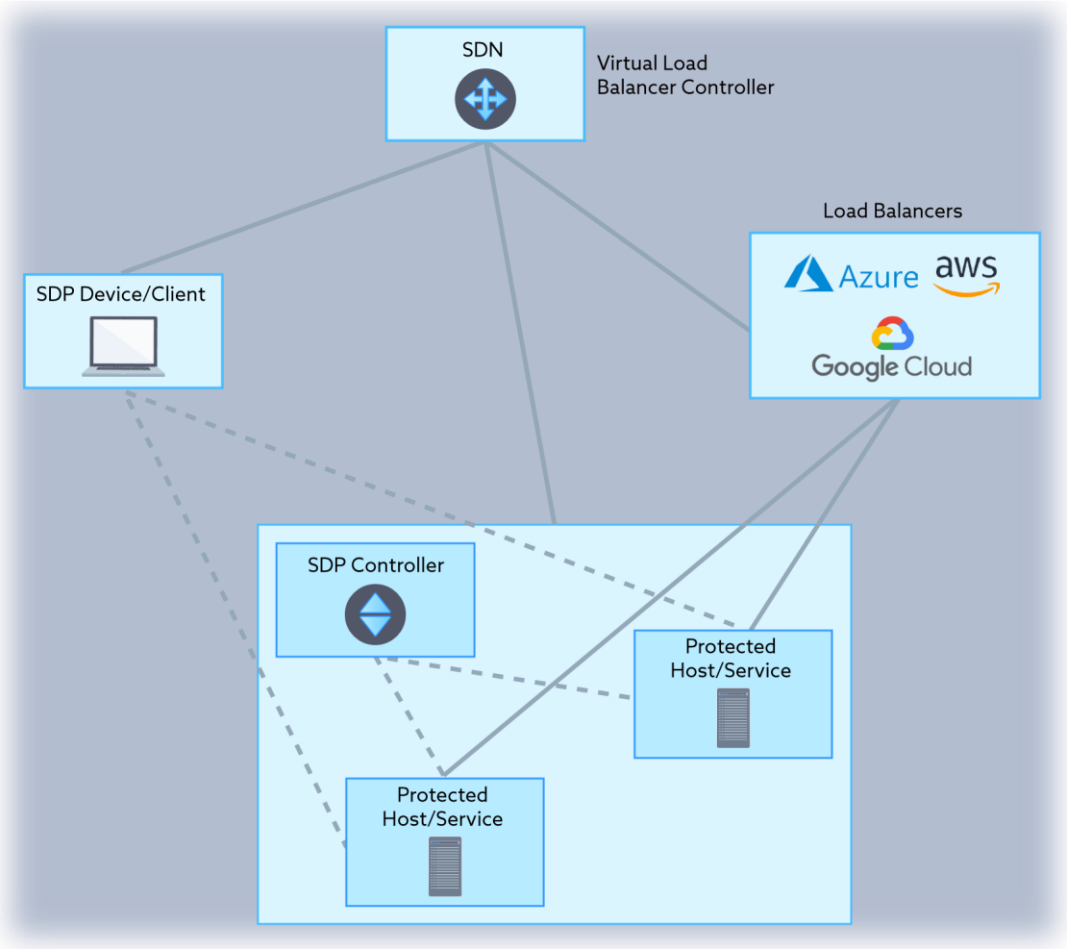

図 4: Hybrid Cloud Environment

SDP アーキテクチャの PoC 一上の例は、SDP がハイブリッドマルチクラウド環境におけるアプリケーション配信の課題への対処方法を示す。 具体的な PoC の内容は下記の通り。:

- 機密性が高いと分類されている通信は、SDP アプローチを使用して、ネットワーク層からアプリケーション層のセキュリティを実行する必要なしに、1 つの安全な環境から別の安全な環境まで、あらゆるタイプのネットワーク（インターネットを含む）でセキュリティ保護を実行できる。
- SDN の進歩により、個別のコントロールプレーンとデータプレーン、および deny-all / allow ファイアウォールをサポートすることで、SDP を実装できる。
- ハイブリッドマルチクラウド環境におけるネットワーク転送の SDP アプローチは、単一パケット検査に基づくゼロトラストネットワーキングの原則と完全に一致している。

ネットワーク層に適用された SDP の配備は、SDN コントローラーからのインターフェースを使用して、開始ホスト（Initiating Host）から SDP コントローラーに接続をルーティングすることだ。このル

ーティングを構成するための望ましいインターフェースは、セルフサービス構成を可能にする REST インターフェースだ。 このネットワーク層の SDP デモを提供する理由は、TLS 終端後にアプリケーション層でゼロトラストを適用することによって引き起こされる問題に対処することである。

既存の「ゼロトラスト」セキュリティ対策のほとんどは、TLS での終端後、ポリシーに基づく認証と、サービスによっては一部認可が実行される。 証明書の検証は複雑な検証プロセスであり、TLS 1.2、TLS 1.3、および双方向 TLS の既知の潜在的な脆弱性が存在する。
すべての主要なクラウドサービスプロバイダーから、ゼロトラストアプローチに取り組むための多くの取り組みがある。現在のところ、ネットワーク層だけでゼロトラストを適用することはできない。特に、ハイブリッドマルチクラウドの導入が関係している。この例では、「ハイブリッドクラウド」はプライベートクラウドからエンタープライズ、データセンターへの接続を指し、「マルチクラウド」は異なるパブリッククラウドとプライベートクラウド間のネットワーク接続を指す。業界筋は、ほとんどの企業がハイブリッドマルチクラウド戦略を現在持っているか、ハイブリッドへ移行する予定を示している。
PoC では、ネットワークの仮想化により、セキュリティ関連のアクションを SDP のコントロールプレーンで実行できる点を利用している。SDN への適用拡大と進化により、サービスプロバイダーはネットワーク管理を簡素化できるようになった。 ただし、SDN の採用は、API によるネットワークルーティングのオーケストレーションのために、適切な認証、アクセス制御、データプライバシー、およびデータの整合性を提供する方法において大きな課題をもたらしている。SDN では、効率的なデータ転送ときめ細かな制御サービスの両方をオンデマンドで仮想ネットワークに対しプロビジョニングできるが、現在のセキュリティプラクティスは、これらのソフトウェア定義インフラストラクチャの統合から生じる複雑さと課題に対応するようには設計されていない。ただし、SDN 環境では、SDN コントローラーがソフトウェア定義の境界サービスを呼び出し、接続を調整し、SDP が提供するリクエストされたＩD およびデバイス検証に基づいて、ネットワーク接続で許可/拒否アクションを実行できる[4]。次に、SDP コントローラーは、パケットを識別する属性が条件に満たない場合、接続を Accepting Host にルーティングするか、接続をドロップするように SDN に指示する。

[4] On the Security of SDN: A Completed Secure and Scalable Framework Using the Software-Defined Perimeter (http://sdpcenter.com/resources/research/)

PoC 構成要素

OSI Layer	Cloud Layer		
アプリケーション	アプリケーション	**エンドユーザ層**–アプリケーションとビジネス価値の提供	Apps, UIs
プレゼンテーション	サービス	**ミドルウェア**–アプリが利用する機能的な構成要素	SDP クライアント（SPA） SDP コントローラー – ユーザトークン、デバイス検証
セッション	イメージ	**OS**–仮想化を正しく管理する	SDP ゲートウェイ – ファイアウォールルール、ロードバランサー
トランスポート	ソフトウェア定義のデータセンター	**クラウド API**–仮想化されたリソースの作成	SDN – 通信制御、パケット分析
ネットワーク	ハイパバイザー	**仮想化**–コンピューティングやストレージの仮想化を提供	
データリンク	インフラ	**ハードウェア**–データセンタ内の物	
物理			

図 5: Proof of Concept SDP Components

技術要素とインフラ

次のサービスは、SDP 展開がエンタープライズにおける IT の脆弱性に対処できることを示すために必要だ。 このシナリオは、既存の SDP オープンソース展開に基づいて構築されている。 シナリオは公開される予定であり、オープンソースが不可能な場合、テクノロジーサプライヤーはコンポーネントの構成と展開に関する明確な説明を提供する予定である。

SDP コントロール&データプレーン技術要素

1. SDP クライアントとして配布されたＳＤＰエージェント
2. SDN 仮想ロードバランサー(VLB)にアクセスできる場所にホストされている SDP コントローラー

3. ゼロトラストの許可/拒否の判断に必要となるセキュリティ対策を講じた SDP ホストサービス（この PoC の目的で、これらのサーバーは、外部クラウドロードバランサーによってアクセス可能なパブリッククラウドにデプロイされた VM である場合がある）

4. インターネットからのネットワーク接続性

ネットワークロードバランサーおよびパブリッククラウド技術要素

1. SDP リクエストを、ID アクセス制御を処理するマイクロサービスにルーティングし、許可/拒否を応答する SDN 仮想ロードバランサー
2. SDP が許可するホスト/サービスにリクエストを転送する、クラウドに展開された VLB

技術的なリスクと問題

SDP/ゼロトラストを SDN と仮想ロードバランサーによりネットワーク層で実現する場合、リスクがある。 SDP による許可/拒否は、二者択一のネットワーク接続であるため、この実装は明らかに単一障害点を示唆している。 従って、データプレーンに統合されたアクセス制御メカニズムが十分なセキュリティを備えていることが重要である。 これにより、ID 識別に使用される属性が正しく計画、構築、実行されることが保証されることとなる。

PoC における前提

1. 既存のオープンソースベースの SDP 実装が、PoC のシナリオの基盤として使用される。
2. マイクロサービスを呼び出し、リクエストを一般的なクラウドおよびオンプレミスのロードバランサーに転送できる仮想ロードバランサーを選択する。
3. PoC のサプライヤーテクノロジーの導入は、独自の機能やプライベートな機能を含まない実装の詳細を含めて、公開可能にする必要がある。
4. マイクロセグメンテーション実装をしている仮想プライベートクラウドネットワーキングを、PoC 目的で利用できるようにする。
5. SDP Initiating Host/Server として機能するデバイスまたは VM を使用可能にする。
6. テスト環境には、リクエストパケットの ID 属性が ID サービスで一致する（接続が許可される）か、一致しない（接続がドロップされる）かを、テストケースで網羅する。

技術的な分析

ネットワーク層で本当のゼロトラストにおける許可/拒否接続を展開するためには、Accepting Host でネットワークプロトコルを適用する前に、新しい接続にアクセスする技術要素が必要となる。

PoC において、TLS 認証の終了前に、通信管理およびルーティング中に展開されるコンポーネントが必要であり、実際の Accepting Host を外部に晒す事はない。これには、証明書の脆弱性による侵入を防ぎ、DDoS パケットがターゲットに到達するのを防ぐという明らかな利点がある。

必要なテクノロジーは、仮想ロードバランサーから ID 属性に直接アクセスできるパケット検査サービスの導入である。接続は、ID 属性サービスに基づいて、接続をドロップするか、Accepting Host/Server への転送を許可するかを決定する SDP コントローラーサービスを介してルーティングできる。

マルチクラウド接続を必要とする現在のネットワーク環境を促進するために、SDP 実装に必要なテクノロジーは、クラウドサービスプロバイダーおよび企業のロードバランサーを連携できる仮想ロードバランサーである。

このテクノロジーは、SDP コントローラーをデプロイする VM に接続できること、および Initiating Host/Server からの SDP に関するリクエストをインターセプトできることも必要となる。

必要となる構成要素

SDP ゼロトラストの PoC シナリオを提供するために必要な構成要素は次のとおり。:

1. ネットワーク接続を開始する Initiating Host/Server
2. インターネット接続
3. パケット分析に基づき、転送前に REST をコールできる仮想ロードバランサー
4. マイクロサービスに配備された SDP コントローラー
5. ネットワーク接続を受け入れる Accepting Host/Server
6. Accepting Host/Server にリクエストを転送するための CSP /企業の外部ロードバランサー

要件	構成要素
接続前認証	ID 属性を検証するためのサービスが SDP コントローラーに配置される
検査済みの接続にのみ公開を制限する機能	SDP コントローラーによって検証されていない接続をドロップする仮想ロードバランサーコントローラー
ID およびアクセス管理の粒度の高い制御	実行時に各接続を認証するために SDP コントローラーに展開された VLB によって転送された各接続の SPA
疑わしい活動を監視システムに転送	疑わしい接続に関する情報を SIEM に転送する VLB コントローラー

鍵となる技術革新

SDN の進歩、特に REST サービス API を実行できる仮想ロードバランサーコントローラー、およびネットワーク接続をルーティングする機能により、この PoC が実行可能になる。

従って、仮想ロードバランサーコントロールプレーンサービスは、接続リクエストに含まれるネットワークパケットに基づいてインテリジェントな決定をする。 これは、ID 属性によるネットワーク層認証の実装が、REST を介して境界で保護されたサービスを呼び出すことによって実現できるようになったことを意味する。

展開への準備

SDP ゼロトラストの PoC シナリオを実装するには、次の準備が必要となる。:

1. 仮想プライベートクラウドネットワークと仮想マシンのセットアップ
2. エンドポイント間のインターネット接続の確立
3. ID 検証マイクロサービス
4. 仮想ロードバランサーのセットアップ、CSP 外部ロードバランサーのパブリック IP アドレスへのルーティング
5. SDP 接続を判別するためのパケット検査
6. 接続単一パケット検査からの ID 属性の抽出
7. アイデンティティ検証マイクロサービスへの REST サービス
8. VLB と SDP コントローラー間のネットワーク接続のルーティング

現在の状況

現在、多くのサプライヤーとベンダーが自社の製品とサービスの提供に対して「ゼロトラスト」機能を主張している。本来、以下の機能とアクティビティがゼロトラストネットワーク機能実現に必要となる。

- 境界ネットワークセキュリティの設定
- 監視ツールに知見を与えるログ
- ハイブリッドサービスを制御するポリシー設定
- インバウンド/アウトバンドファイアウォールのセキュリティ設定
- 企業ネットワークポリシーの設定
- 双方向ＴＬＳ証明書による認証
- SPA による認可

ほとんどの従来の製品とサービスはエンドポイントのアクセス前認証が提供できておらず、ネットワークレイヤーのゼロトラストを構成したとは言えない。

終わりに

SDP ゼロトラストのデモに参加することに関心のあるテクノロジーコンポーネントのサプライヤーは、クラウドセキュリティアライアンス SDP ワーキンググループに電子メールで連絡いただきたい。
smahmud@cloudsecurityalliance.org.

References

Cloud Security Alliance Initiatives:

- SDP Architecture Guide published May 2019
  https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/
- SDP as a DDoS Defense Mechanism published October 2019
  https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-as-a-ddosprevention-mechanism/
- Specification 2.0 in Jan 2020 - In progress

Market Awareness and Adoption Overview:

- Cloud Security Alliance The State of SDP Survey: A Summary

Open Source Reference Implementation (funded by DHS):

- http://sdpcenter.com/test-sdp/

Zero Trust Presentation to OMG (Object Management Group):

- https://cloudsecurityalliance.org/artifacts/sdp-the-most-advanced-zero-trust-architecture/

US Department of Defense Net-Centric Services Strategy:

- https://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf