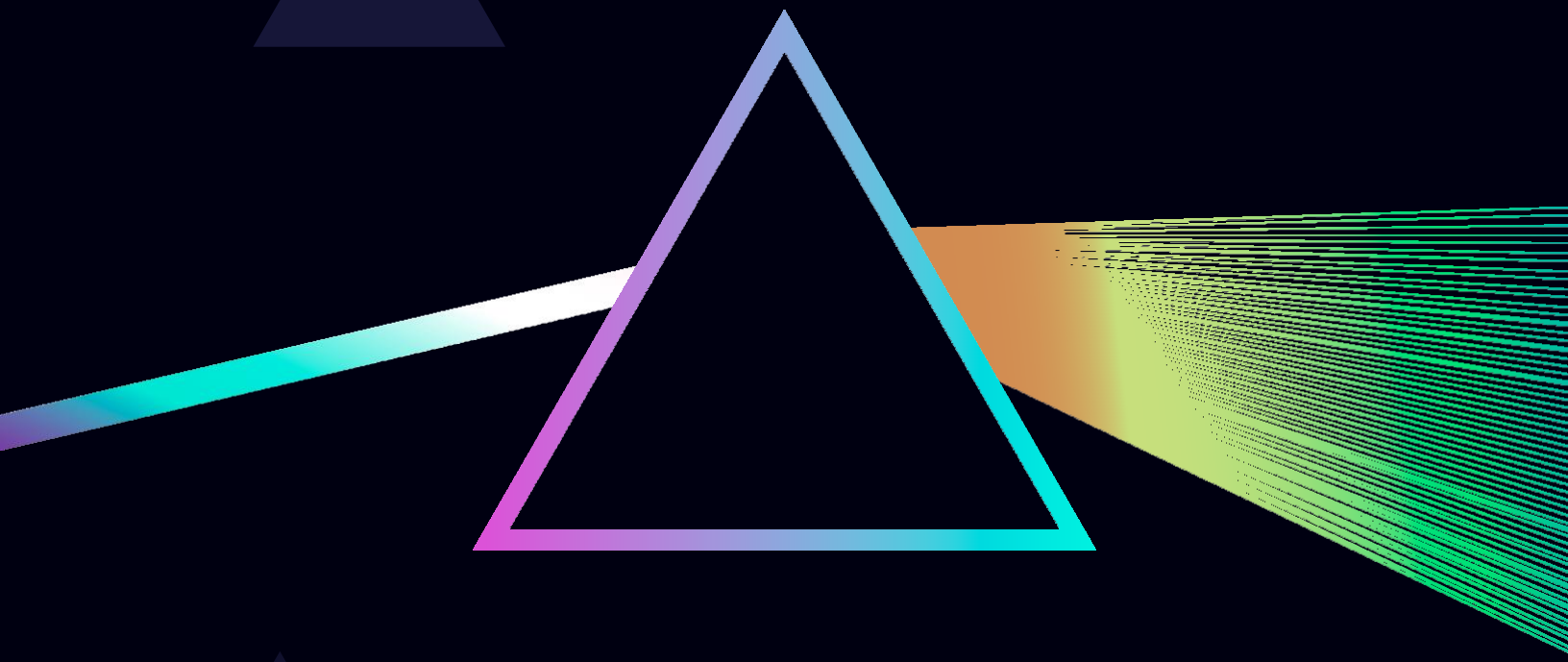
Software-Defined Perimeter

アーキテクチャガイド



cloud security alliance®

CSAJC cloud security alliance℠ Japan Chapter

ACKNOWLEDGMENTS

CSA thanks everyone who contributed and supported us throughout the development of this guide.

LEAD AUTHORS
Jason Garbis
Juanita Koilpillai

CONTRIBUTORS
Junaid Islam Nya
Murray Aaron Palermo
Preeta Raman
Michael Roza

CSA GLOBAL STAFF
Shamun Mahmud

日本語版提供に際しての告知及び注意事項

本書「Software-Defined Perimeter アーキテクチャガイド」は、Cloud Security Alliance (CSA)が公開している「Software-Defined Perimeter ARCHITECTURE GUIDE」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 03 月 10 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 アーキテクチャガイド」の日本語訳は、CSA ジャパン会員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）

石井　敏満
太田　拓也
小池　泰治
諸角　昌宏
矢部　沖比古

目次

はじめに

SDPは、技術コンポーネントとアーキテクチャを組み合わせて、ネットワークベースのアプリケーションとインフラストラクチャを従来のセキュリティツールよりも効率的かつ効果的に保護します。

今日のネットワークセキュリティアーキテクチャ、ツール、およびプラットフォームは、現在の脅威が示す課題を解決できていません。主なメディアの見出しを確認している、ネットワークの防衛に日々努めている、またはセキュリティベンダーとして活動しているかどうかにかかわらず、企業、政府組織、および重要インフラが、さまざまな攻撃者からの持続的な攻撃に対処できていないことは明らかです。

ネットワークスタックのすべてのレイヤを包含する最新のネットワークセキュリティである、Software-Defined Perimeter（SDP）を採用する時が来ています。SDPは、実績のある技術コンポーネントとアーキテクチャを組み合わせて、ネットワークベースのアプリケーションとインフラストラクチャを従来のセキュリティツールよりも効率的かつ効果的に保護します。***2014年4月に公開された***SDPの仕様(1.0)では以下のように述べています:

> “SDPの背景にある原則は、新しいものではありません。国防総省（DoD）およびインテリジェンスコミュニティ（IC）内の複数の組織は、ネットワークアクセス前の認証と認可に基づいて類似のネットワークアーキテクチャを実装しています。通常、機密として扱われるものや高セキュリティネットワーク（DoD定義による）におけるすべてのサーバーは、リモートアクセスゲートウェイの背後に隠され、ユーザーのネットワークへのアクセスやサービスの利用に関する認可の前に、認証を受ける必要があります。SDPはそれぞれのネットワークで用いられる論理モデルを活用し、標準ワークフローに組み込まれます。SDPでは、保護されているサーバーへのアクセスの前に、認証と認可を受ける必要があります。次に、接続元とアプリケーションインフラストラクチャ間で暗号化通信がリアルタイムに行われます。

目的

セキュリティ専門家、ソリューションプロバイダーのグループとして、私たちは情報セキュリティとサイバーセキュリティに情熱を傾けており、Software-Defined Perimeter (SDP)は、私たち全員が直面するセキュリティの脅威に対抗するための重要な新しいソリューションであると考えています。

SDP Specification：1.0の発行以来、ソフトウェアベンダー、システムおよびセキュリティアーキテクト、および企業を含む共同ワーキンググループとして、これらのガイドラインに従う多数のシステムを構築および配備してきました。一方で、SDPの実装について、特に元の仕様が欠けていた分野について多くのことを学びました。

このガイドでは、企業や専門家がSDPに関する情報を取得するのを支援します。これは、経済的および技術的利益を提供できることを示すとともに、ユーザーが組織にSDPを正常に実装できるように支援します。以下の目標が達成できるように、この文書を利用していただきたいと考えています：

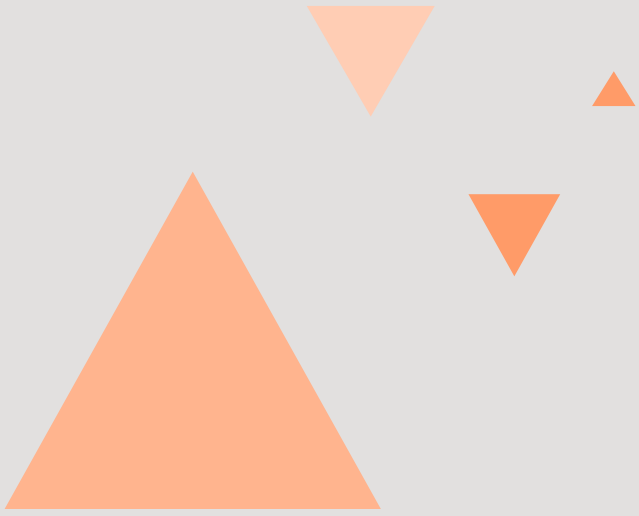
- 市場の認知度、信頼性の向上、およびSDPの企業での採用
- さまざまな環境でSDPを使用する方法についての理解の向上
- SDPを使用して企業の問題を解決するための動機付け
- SDPについて、内部関係者を教育するためにこの文書を使用
- 企業が、この文書のアーキテクチャの推奨事項に基づいて、SDPソリューションの配備を成功させます。

対象者

この文書に記載されている情報は、組織でSDPプロジェクトを検討している、または現在実装しているすべてのセキュリティチーム、アーキテクチャチーム、および技術ネットワークチームに役立ちます。

この文書の主な対象者は、情報セキュリティに関わる専門家、エンタープライズアーキテクト、セキュリティコンプライアンス担当者です。これらの方々は主に、SDPソリューションの評価、設計、配備、運用を担当します。

さらに、ソリューションプロバイダー、サービスプロバイダー、およびテクノロジーベンダーに従事する方々も、この文書を読むことでメリットを得ることが出来ます。



概要

Software Defined Perimeter (SDP)の概要

SDPは、データ暗号化など、実績のある標準ベースのコンポーネントを活用するように設計されています。それらは、リモート認証（ホストがリモートアクセスを認証する）；双方向トランスポート層セキュリティ（TLS;クライアント情報を暗号化を用いて検証する方法）；適切なアクセスを保護するために暗号化とデジタル署名を利用したSecurity Assertion Markup Language（SAML）；公開鍵を介したアクセスを検証したX.509証明書などの様々な標準ベースのテクノロジーを組み込むことでSDPを組織の既存のセキュリティシステムと統合することができます。

クラウドセキュリティアライアンス（CSA）が、Software Defined Perimeter（SDP）仕様を最初に公開して以来、CSAはSDPイノベーションの可視性と企業での採用を飛躍的に高めています。従来のネットワークセキュリティ手法が、全ての産業のIT、セキュリティチームを圧倒してきたように、SDPテクノロジーの使用と関心の増加に関連する例として、以下のものがあります：

- 5つのSDPワークグループは、IaaS向けSDP、Anti-DDoS、および自動車の安全な通信、を含む重点分野において大きな進歩を遂げました。
- 複数の商用SDPが複数のベンダーおよび複数の企業で利用されています。
- Anti-DDoSのユースケースではオープンソースのリファレンス実装が利用されています。
- 4つのSDPハッカソンにおいて、SDPテストインフラストラクチャに対する攻撃は成功しませんでした。
- 業界アナリストの調査とプレゼンテーションのレポートに、SDPの取り扱いが増えています。

SDPのセキュリティ上の利点

- SDPは、攻撃対象領域を減少させ、リスクを低減します。
- SDPはアクセス制御とデータプレーンを分離してこれを見えなくすることで、潜在的なネットワークベースの攻撃を防ぎ、重要な資産やインフラストラクチャを保護します。
- SDPは、既存のNACやアンチマルウエアのような個々のセキュリティ製品では達成が難しい統合セキュリティアーキテクチャを提供します:
  - 》 ユーザーが認識しているアプリケーション
  - 》 クライアントが認識しているデバイス
  - 》 ネットワークが認識しているファイアウォール/ゲートウェイ
- SDPは、IPベースの代わりにコネクションベースのセキュリティアーキテクチャを提供します。これは、今日のIPの爆発的増加とクラウド環境での境界の喪失により、IPベースのセキュリティが弱くなることに対応します。
- SDPはすべてのコネクションを制御できます。これは、接続できる人の事前審査、どのデバイスからか、どのサービス、インフラストラクチャおよびその他のパラメータに対してか、に基づきます。

SDPのビジネス上の利点

SDPは、上記のセクションで触れた多くのビジネス上の利点（下記参照）を提供します。今後の成果において、これらの利点のより詳細な定性的および定量的な検討を提供するためにSDPコミュニティと協力することを期待しています。

ビジネスエリア	SDPを実装した場合の利点
コストと省力化	従来のネットワークセキュリティコンポーネントを置き換えることで、ライセンスとサポートのコストが削減されます。 SDPを使用してセキュリティポリシーを実装および実施することで、運用上の複雑さと従来のセキュリティツールへの依存を軽減します。 SDPはMPLSまたは専用回線の使用率を削減または置き換えてコストを削減することもできます。これにより、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ます。
IT運用のアジリティの向上	ITプロセスはビジネスプロセスの障害と見なされます。一方、SDPの実装は、ITまたはIAMのイベントによって自動的に推進されます。これによりITが加速され、ビジネスとセキュリティの要求に対する応答性が向上します。
GRCの利点	SDPは、従来の方法と比較してリスクを軽減します。SDPは脅威を抑制し、攻撃対象を減らし、ネットワークベースの攻撃やアプリケーションの脆弱性の悪用を防ぎます。 SDPシステムは、システムおよびアプリケーションのコンプライアンス活動を合理化するために、（上記のSIEM統合シナリオと同様に）GRCシステムに取り込んだり対応したりすることができます。
コンプライアンス範囲とコスト削減	SDPは、登録済みデバイスのユーザーから特定のアプリケーション/サービスへの接続の制御を一元管理するため、コンプライアンスデータの収集、報告、および監査プロセスを改善できます。 SDPは、オンラインビジネスのための追加の接続の追跡性を提供することによって全体的なコンプライアンス活動を可能にします。 SDPが提供するネットワークの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縮小するために頻繁に使用されます。これは、コンプライアンス報告の取り組みに大きくプラスの影響を与える可能性があります。
セキュアクラウドコンピューティングの採用	SDPは、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、または混在環境の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で、企業が迅速かつ自信を持って安全にクラウドアーキテクチャを採用できるようにします。既存のオプションと比較して同等またはそれ以上のセキュリティ対策で新しいアプリケーションを迅速に配備できます。
ビジネスのアジリティとイノベーションを実現	SDPは、ビジネス上の優先事項を迅速かつ安全に実行できます。以下の例があります: • SDPは、 オンプレミスのコールセンターエージェントからホームベースのエージェントへの移行が避けられないビジネスを可能にします。 • SDPは、非中核的な業務機能を専門の第三者にアウトソーシングすることを可能にします。 • SDPは、リモートのサードパーティパートナーネットワークおよび場所に、顧客向けのキオスクを配備することを可能にします。 • SDPは、顧客サイトへの会社資産の配備を可能にし、顧客とのより強力な統合を実現し、新しい収益を生み出します。

SDPの主な機能

SDPは、少なくとも5つのセキュリティ層を含むように設計されています。（1）デバイスの認証と検証（2）ユーザーの認証と認可（3）双方向暗号化通信の確保（4）コネクションを動的にプロビジョニング（5）サービスへの接続を見えない状態で維持しつつ管理する。これらに加えて追加のコンポーネントもSDP実装に組み込まれています。

情報とインフラストラクチャの秘匿		
SPDアーキテクチャのコンポーネント	**セキュリティ脅威の低減、回避**	**追加の利点**
サーバーは”黒塗り”（見えない化）	全ての外部ネットワークからの攻撃及びクロスドメイン攻撃が低減されます。	SDPコンポーネント（コントローラ、ゲートウェイ）は、クライアントがSingle-Packet Authorization（SPA）などのプロトコルを使用して認証及び認可されるまで、接続要求に応答しません。
DoS攻撃を低減	帯域幅とサーバーのDoS攻撃（ただし、ISPによって提供されるアップストリームのAnti-DoSサービスと組み合わせる必要があることに注意してください。）	インターネットに面するサービスは、通常「deny-all」SDPゲートウェイ（ネットワークファイアウォールとして機能）の背後に配置されます。それにより、DoS攻撃に対し耐性を持ちます。SDPゲートウェイ自体は、SPAによりDoS攻撃から保護されています
不良パケット検出	全ての外部ネットワークおよびクロスドメイン攻撃は、すぐに検出されます。	受入れホスト（Accepting Host:AH）が他のホストから受け取る最初のパケットはSPAパケット（または同様のもの）です。AHがこれ以外のパケットを受信した場合、それは攻撃と見なされます。

双方向に暗号化された接続		
SPDアーキテクチャのコンポーネント	**セキュリティ脅威の低減、回避**	**追加の利点**
ユーザーおよびデバイスの認証	認証されていないまたは不正なデバイスからのコネクション	全てのホスト間の接続では、双方向認証を用いてユーザーとデバイスをSDPの承認されたメンバーとして検証する必要があります。
偽造された証明書の不許可	資格情報の盗難を目的とした攻撃	双方向認証スキームは、SDPによってルート管理（または信頼）されている既知の有効な証明書を固定します。
Man-in-the-middle attacks（中間者攻撃）の防止	中間者攻撃	双方向ハンドシェイクは、サーバー証明書が取り消される前にOCSP応答を悪用する中間者攻撃を防止します。

“Need to Know” アクセスモデル		
SPDアーキテクチャのコンポーネント	**セキュリティ脅威の低減、回避**	**追加の利点**
フォレンジックが容易	不良パケットとの不良接続。	全ての不良パケットを分析し、フォレンジックアクティビティを追跡
きめ細やかなアクセス制御	未知のデバイスを用いた外部ユーザーからのデータ盗難を低減します。	アクセスポリシーに基づいて、許可されたユーザーとデバイスのみがサーバーに接続できます。
デバイスの検証	不正なデバイスからの脅威と、資格情報の盗難のリスクが低減します。	デバイスの検証により、接続を要求するデバイスが適切な鍵を保持していることが証明されます。
侵害されたデバイスからシステムを保護	侵害されたデバイスからのラテラルムーブメントの脅威を低減します。	ユーザーは承認されたアプリケーションへのアクセスのみが許可されます。

動的なアクセスコントロール		
SPDアーキテクチャのコンポーネント	**セキュリティ脅威の低減、回避**	**追加の利点**
動的なメンバーシップベースのアクセス許可	ネットワークベースの攻撃	アクセスルールを動的に作成及び削除する事により、保護されたリソースへのアクセスを可能にします。（アウトバウンド、インバウンドの両方）

アプリケーションレイヤーのアクセス		
SPDアーキテクチャのコンポーネント	**セキュリティ脅威の低減、回避**	**追加の利点**
広範なネットワークアクセスを排除	攻撃対象を最小化：マルウェアまたは悪意あるユーザーによるポートスキャン、脆弱性スキャンを排除します。	デバイスは、ポリシーで許可されている特定のホストとサービスのみにアクセス出来ます。ネットワークセグメントやサブネットへのアクセスは出来なくなります。
アプリケーションとサービスのアクセス制限	攻撃対象領域を制限し、マルウェアまたは悪意あるユーザーがリソースに接続出来ないよう防ぎます。	SDPシステムは、指定されたサービスへのアクセスを許可するデバイス、アプリケーションを制御出来ます。

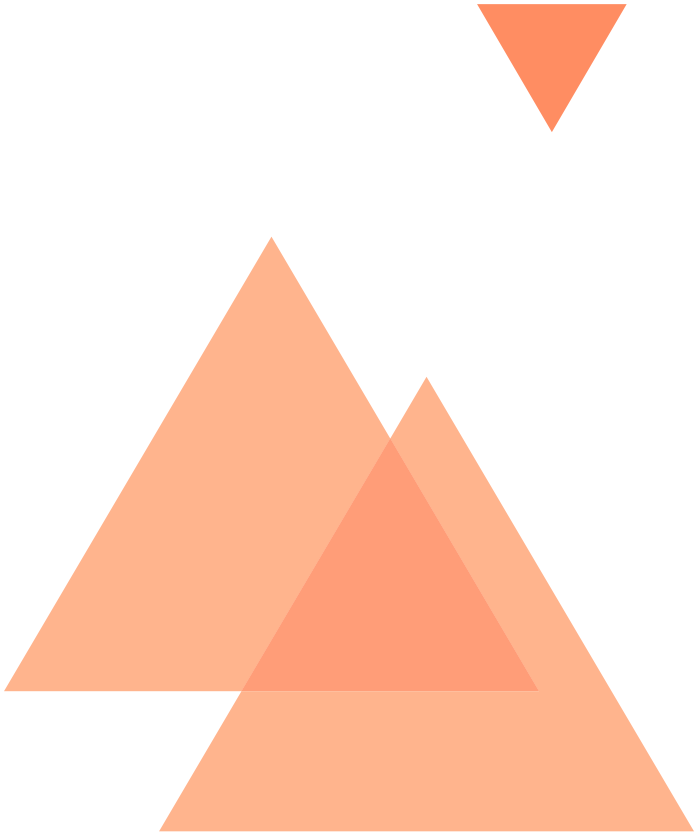
SDPの潜在的なユーザー

SDPはセキュリティアーキテクチャであるため、以下の表に示す様々なレベルで利点を提供しますが、古典的な「ユースケース」の狭い範囲にはうまく収まりません。もちろん、SDPを適用できる他のシナリオもあり、以下のリストは包括的なものではありません。以下の図は、SDP実装によって保護できるコネクションのタイプの考えられる例を示しています。

ネットワークシナリオ	既存の技術の限界	SDPに変更する利点
アイデンティティ主導のネットワークアクセス制御	従来のネットワークソリューションは、粗いネットワークセグメンテーションのみを提供し、IPアドレス中心となっています。SDNのような新しいプラットフォームでも、企業はタイムリーにアイデンティティに焦点を合わせた正確なユーザーアクセス制御を実施するのは困難です。	SDPを使用すると、ネットワークレベルで実施される組織に関連するアイデンティティ中心のアクセス制御を作成できます。例えば「財務管理システムへのWebアクセスには、企業が管理するデバイスを用いた財務ユーザーのみを許可する。ITユーザーにはSSHアクセスのみを許可する」というように。
ネットワークマイクロセグメンテーション	従来のネットワークセキュリティツールでは、マイクロセグメンテーションサービスによるネットワークセキュリティの強化は労働集約的になります。	SDPはユーザー定義のコントロールに基づいて、ネットワークのマイクロセグメンテーションを可能にします。サービスに対するきめ細やかなネットワークアクセス制御はSDPによって自動的に実行され、手動設定は不要です。
セキュアリモートアクセス（VPN　代替）	VPNはユーザーに安全なリモートアクセスを提供しますが、範囲と機能が制限されます。オンプレミスユーザーのセキュリティには一切対応しておらず、通常は粗いアクセスコントロールのみを提供し、ネットワークセグメントまたはサブネット全体へのアクセスを許可します。これは多くの場合、セキュリティとコンプライアンスのリスクを表しており、最小権限の原則に違反しています。	SDPはリモートユーザーとオンプレミスユーザーの両方を保護します。その結果、組織は全体的なソリューションとしてSDPを使用すると、VPNポイントソリューションを廃止できます。SDPソリューションはきめ細かいアクセス制御用にも設計されています。許可されていないリソースはユーザーからアクセスできず、最小権限の原則を満たしています。
サードパーティユーザーのアクセス	セキュリティチームは通常、VPN、NAC及びVLANの組み合わせを活用してサードパーティアクセスを制御しようとします。これらのソリューションは一般的にサイロ化されており、環境全体でのきめ細やかなアクセス制御、包括的なアクセス制御を提供できません。	安全なサードパーティアクセスにより、ビジネスの革新と適応を行う事ができます。例えば、ユーザーを企業オフィスから自宅オフィスに移行してコストを削減できます。特定の機能はサードパーティの専門家に安全に外部委託できます。サードパーティユーザーのオンプレミスアクセスを簡単に制御及び保護できます　。

ネットワークシナリオ	既存の技術の限界	SDPに変更する利点
特権ユーザーアクセスの保護	特権ユーザー（通常は管理者）アクセスには、高度なセキュリティ、監視、コンプライアンス監視が必要です。従来、特権アクセス管理（PAM）ソリューションは資格情報管理を通じてアクセスを管理しますが、ネットワークセキュリティ、リモートアクセス、または状況に応じたアクセス制御を提供しません。	特権サービスへのアクセスは許可されたユーザーに制限され、ネットワークレベルで保護されます。権限の無いユーザーから特権サービスは秘匿されるため、攻撃対象領域を制限する事が出来ます。SDPシステムはビジネス条件で許可されている場合（例えば定義されたメンテナンスウィンドウ中）にのみアクセスが許可され、コンプライアンスレポートのためにログに記録する事を保証できます。もしくは特定デバイスからのアクセスの場合にのみ許可されます。
高価値アプリケーションへのアクセス保護	現在、機密データを含む価値の高いアプリケーションに対するきめ細かい認可制御には、いくつかの機能的なレイヤに変更が必要になる場合があります。（例えば、アプリケーション、データ外部アクセス）	ユーザー/アイデンティティ認識、ネットワーク認識、およびデバイス認識を統合することにより、またネットワーク全体を公開しないことにより、さらにアクセス制御をアプリケーションまたはアプリケーションゲートウェイに依存することにより、アプリケーションへのアクセスを制限できます。SDPは、アプリケーションのアップグレード、テスト、および展開を促進し、DevOps CI/CDに必要なセキュリティフレームワークを提供することもできます。
管理対象サーバーへの安全なアクセス	MSSPまたは大規模なIT環境では、管理者は管理対象サーバーへの定期的なネットワークアクセスを必要とし、そのIPアドレスレンジは重複する可能性があります。 これは、従来のネットワーク及びセキュリティツールでは達成が難しく、面倒なコンプライアンスレポートが要求される可能性があります。	管理対象サーバーへのアクセスはビジネスプロセス（オープンサービスデスクチケットなど）で制御ができます。 SDPシステムは、複雑なネットワークレイヤをオーバーレイし、アクセスを簡素化及び合理化しながら、コンプライアンス要件を満たすためにユーザーアクティビティを記録できます。
ネットワーク統合の簡素化	組織は、M&Aや災害復旧のシナリオなどで、以前は別だったネットワークを迅速に統合する必要がある場合があります。	SDPを使用すると、大規模な変更を必要とせず、ネットワークを迅速かつ無停止で相互接続できます。
IaaSクラウド環境への安全な移行を可能にする	IaaSの採用は劇的に増加していますが、多くの組織は依然としてセキュリティを懸念事項として挙げています。例えば、IaaSアクセス制御は、企業から切断されクラウドプロバイダに限定されます。	IaaSセキュリティの改善。アプリケーションをデフォルト拒否ファイアウォールの背後に隠すことに加え、全てのトラフィックが暗号化され、また、異機種混在の企業全体でユーザーアクセスポリシーを一貫して定義できます。詳細については、CSAが2017年2月13日に公開した”***SDP for IaaS***”を参照してください。

ネットワークシナリオ	既存の技術の限界	SDPに変更する利点
認証スキームの強化	セキュリティまたはコンプライアンスの懸念により、既存の「レガシー」アプリケーションへ2FAの追加が必要になる場合があります。これは、Web以外のアプリ、または簡単に変更できないアプリでは実現が難しい場合があります。	SDPは、特定のアプリケーションへのアクセスを許可する前に、2FAを要求できます。 ユーザーエクスペリエンスを向上させるためにインプレースMFAシステムを使用でき、MFAを追加してレガシーアプリケーションのセキュリティを強化できます。
エンタープライズコンプライアンス管理とレポートの合理化	通常、コンプライアンスレポートは、セキュリティチームとITチームにとって好ましくない負担です。	SDPは、コンプライアンスの範囲を（マイクロセグメンテーションを介して）縮小し、コンプライアンスレポートタスクを自動化します（ID中心のログ記録とアクセスレポートを介して）。
DDoS 防止	従来のリモートアクセスソリューションは、インターネット上のホストとポートを公開するため、DDoS攻撃の対象となります。従来のDDoSセキュリティ制御は、正常なパケットがドロップされるだけでなく、低帯域幅のDDoS攻撃はバイパスされます。	SDPはデフォルト拒否のファイアウォールを利用しており、権限の無いユーザーには見えない状態で配備されます。これにより、正常なパケットのみ許可します。



SDPアーキテクチャ

SDPアーキテクチャの主要コンポーネントには、クライアント/接続を開始するホスト（Initiating Hosts:IH）、サービス/接続を受け入れるホスト（Accepting Hosts:AH）、およびAHとIHの両方が接続するSDPコントローラが含まれます。 SDPホストは、接続を開始する（ホストを開始する、またはIH）か、接続を受け入れる（ホストを受け入れる、またはAH）ことができます。IHおよびAH接続は、安全な制御チャネルを介したSDPコントローラとの通信によって管理されます。この構造により、完全にスケーラブルなセキュリティシステムを実現するために、コントロールプレーンをデータプレーンから分離したままにすることができます。さらに、すべてのコンポーネントは、拡張性または可用性の目的で冗長化できます。ここで概要を説明するワークフローに従うことにより、図1に概要を示した手法を使用して、これら3つのコンポーネント間の接続を保護できます。

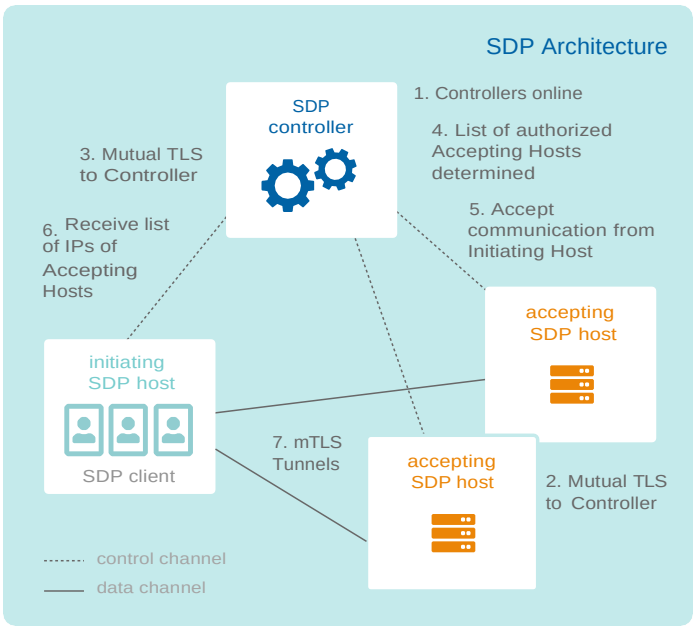


図1: SDP Specification 1.0でCSAが公開したSDPアーキテクチャ,

SDPの動作

IH上のSDPクライアントソフトウェアは、SDPへの接続を開始します。

ラップトップ、タブレット、スマートフォンなどのIHデバイスはユーザー向けです。つまり、SDPソフトウェアはデバイス自体で実行されます。ネットワークは、SDPを運用している企業の管理外にある可能性があります。

AHデバイスはIHからの接続を受け入れ、SDPによって安全に保護された一連のサービスを提供します。AHは通常、企業の管理下（あるいは直接代表するもの）にあるネットワークに存在します。

SDPゲートウェイは、許可されたユーザーとデバイスに対して保護されたプロセスとサービスへのアクセスを提供します。ゲートウェイは、これらの接続の監視、ロギング、およびレポートを実施することもできます。

IHおよびAHデバイスはSDPコントローラに接続します。SDPコントローラは、ユーザーの認証と認可、デバイスの検証、安全な通信の確立、ネットワーク上のユーザーと管理トラフィックの分離を保証することにより、分離サービスへのアクセスを保護するアプライアンスまたはプロセスです 。

コントローラとAHはsingle-packet authorization（SPA）で保護されており、許可されていないユーザーやデバイスからは見えず、アクセスもできません。SPAは、この文書全体および21ページで詳細に記述しています。

SDPのセキュリティは、以下で示すステップバイステップのワークフローになります:

1. 1つ以上のSDPコントローラがSDP内で追加およびアクティベートされ、AM、PKIサービス、デバイス認証、地理位置情報、SAML、OpenID、OAuth、LDAP、Kerberos、多要素認証、IDフェデレーション、およびその他の同様の認証および認可サービスなどに接続されます。
2. 1つ以上のAHがSDP内で追加およびアクティベーションされます。安全な方法でコントローラに接続して認証します。AHは他のホストからの通信を認識せず、あらかじめプロビジョニングされていない要求には応答しません。
3. 各IHは、SDP内で追加およびアクティベーションされ、SDPコントローラに接続して認証されます。
4. IHを認証した後、SDPコントローラは、IHが通信を認可されているAHのリストを決定します。
5. SDPコントローラは、IHからの通信を受け入れるようにAHに指示し、暗号化された通信に必要なオプションのポリシーを開始します。
6. SDPコントローラは、IHにAHのリストと、暗号化された通信に必要なオプションのポリシーを提供します。
7. IHは、許可された各AHに対してSPAを開始します。IHは、それらのAHへの双方向暗号化接続（双方向TLS、またはmTLSなど）を作成します。
8. IHは、AHを介して相互に暗号化されたデータチャネルを通してターゲットシステムと通信します（注：前のページの図1にはステップ8は示されていません）。

SDP配備モデル

CSAのSDP specification 1.0は、組織がSDPアーキテクチャを配備できる以下の潜在的な方法を紹介しました。:

- クライアント→ゲートウェイ
- クライアント→サーバー
- サーバー→サーバー
- クライアント→サーバー→クライアント
- クライアント→ゲートウェイ→クライアント
- ゲートウェイ→ゲートウェイ

クライアント→ゲートウェイ

1つまたは複数のサーバーをゲートウェイの背後で保護する必要がある場合、もとになるネットワークトポロジに関係なく、クライアント/IHとゲートウェイ間の接続が保護されます。ゲートウェイは同じ場所にある場合もあれば、世界中に分散している場合もあります。

クライアント/IHは、接続を終端するmTLSトンネルを介してゲートウェイに直接接続されます。サーバーへの接続を保護するには、追加の予防措置を講じる必要があります。SDPコントローラは、コントローラとサーバーが同じSDPゲートウェイを使用するように、保護されたサーバーの近くに配置できます。

図2では、サーバー（1つ以上の環境）は、AHとして機能するSDPゲートウェイの背後で保護されています。ゲートウェイを介したサーバーへの接続を保護するには、サーバー環境はSDPを運用している組織によって制御される必要があります。

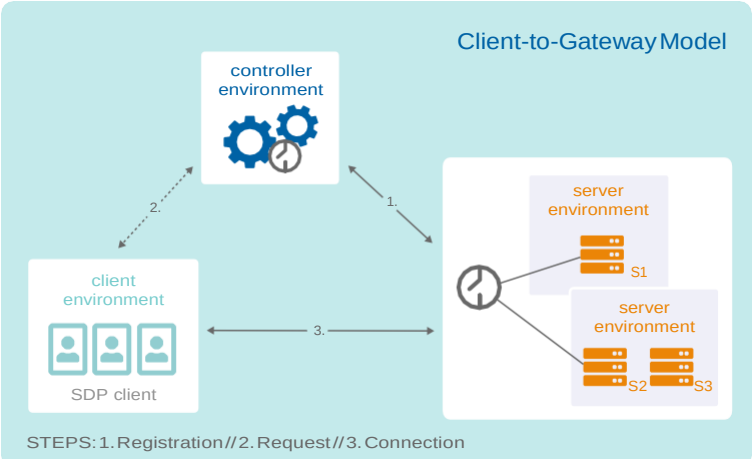


図2：クライアント→ゲートウェイモデル：1つ以上のサーバーがゲートウェイの背後で保護されています

保護されたサーバーは、”Deny-All”ファイアウォールとして動作するSPAで保護されているため、適切にオンボードされたクライアント/IHを除いて到達不能であり、ゲートウェイとコントローラは、攻撃者や不正ユーザーにはアクセスできません。

サーバーに変更を加えることなく、保護されたサーバーをSDPに含めることができます。それらが存在するネットワークは、保護されたサーバーへのインバウンド接続をゲートウェイからのみ許可するように構成する必要があります。これにより、許可されていないクライアントは、ゲートウェイをバイパスできません。

このモデルは、SDPゲートウェイと保護されたサーバーの間にそれらを展開することにより、組織がIDS/IPSなどの既存のネットワークセキュリティコンポーネントを使用することができます。トラフィックは、クライアントをゲートウェイに接続するmTLSトンネルから抽出された後に監視されます。

クライアント/IHは、デバイスでもサーバー自体でもかまいません。（16ページ「サーバー→サーバー」を参照）

クライアント→ゲートウェイモデルは、アプリケーションをクラウドに移行した時のクラウド環境に適しています。 サーバー環境の場所（クラウドまたはオンプレミス）に関係なく、組織はゲートウェイとアプリケーションの間でデータが保護されていることを保障できます。

また、このモデルは、IHへの変更を必要としないため、オンプレミスのレガシーアプリケーションの保護に適しています。

クライアント→サーバー

組織がアプリケーションをIaaSプロバイダーに移行し、エンドツーエンドで接続を保護する場合、このモデルはサーバーとゲートウェイを単一のホストに結合します。クライアント/IHは、サーバーと同じ場所に配置することも、分散させることもできます。いずれの場合も、クライアント/IHとサーバー間の接続はエンドツーエンドで保護されます。

このモデルは、サーバーとゲートウェイの組み合わせを必要に応じて複数のIaaSプロバイダー間で移動できるため、組織に大きな柔軟性を提供します。このモデルは、アップグレードできないオンプレミスのレガシーアプリケーションの保護にも適しています。

このモデルでは、クライアント/IHは、接続を終端するmTLSトンネルを介してサーバーに直接接続されます。SDPコントローラは、（コントローラとサーバーが同じSDPゲートウェイを使用するように）サーバーあるいはクラウドに配置できます。

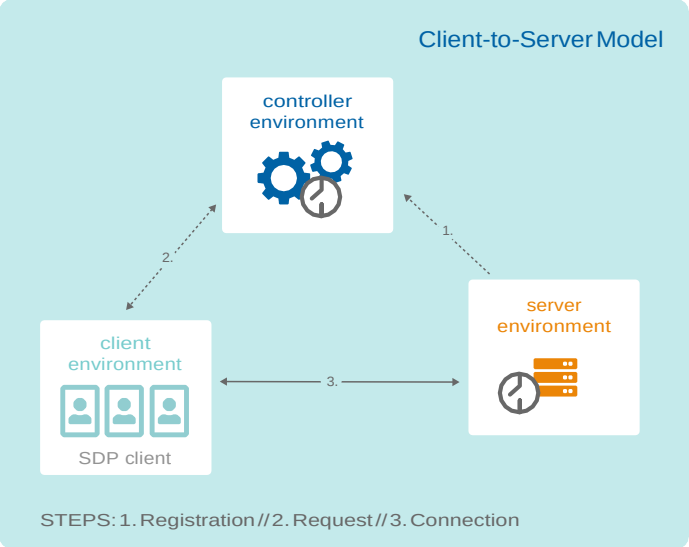


図3：クライアント→サーバーモデル：サーバーはゲートウェイソフトウェアをローカルで実行します

サーバーはSDPゲートウェイ（AHとして機能）の背後で保護されます。ゲートウェイからサーバー（サーバー環境において）への安全な接続は、サーバー上のアプリケーション/サービスの所有者の制御下にあり、所有者がこれらの接続を完全に制御できます。

保護されたサーバーは、”Deny-All”ファイアウォールとして動作するSPAで保護されているため、適切にオンボードされたクライアント/IHを除いては到達不能です。このことは、サーバーは内部/外部の攻撃者や不正ユーザーにはアクセスできず、インサイダーの脅威から最大限の保護を提供していることを意味します。

このモデルでは、保護されたサーバーにゲートウェイを実装する必要があります。サーバーが存在するネットワークは、保護されたサーバーへのインバウンド接続を許可するように構成する必要はありません。これらのサーバー上のゲートウェイは、SPAを使用して、許可されていない接続を防ぎます。

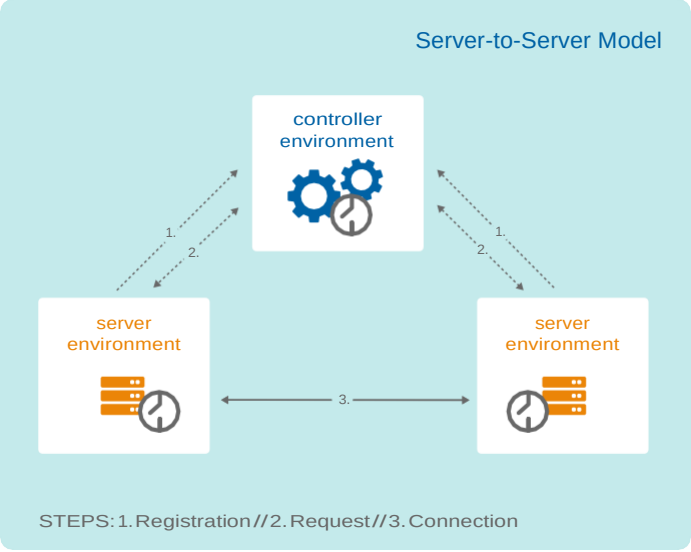
また、IDS/IPSやSIEMなどの既存のネットワークセキュリティコンポーネントを簡単に使用できます。トラフィックは、SDPゲートウェイ/保護されたサーバーからのこれらのドロップされたパケットを分析することによって監視でき、クライアント/IHとサーバー間のmTLS接続を保持します。（クライアント/IHは、ユーザーデバイスとして表されますが、それ自体がサーバーである場合があります。このモデルについては、以下のサーバー→サーバーモデルを参照）

クライアント→サーバーモデルは、アプリケーションをクラウドに移行する組織に適しています。サーバー環境の場所（クラウドまたはオンプレミス）に関係なく、組織はクラウド内のアプリケーションへの接続を完全に制御できます。

サーバー→サーバー

このモデルはIoTおよびVM環境に最適で、基盤となるネットワークまたはIPインフラストラクチャに関係なくサーバー間のすべての接続が暗号化されます。サーバー→サーバーモデルは、すべての通信がSDPホワイトリストポリシーによって明示的に許可されます。信頼できないネットワークを介したサーバー間の安全な通信を可能にし、軽量のSPAプロトコルを使用してサーバーをすべての不正接続から隠します。

このモデルは、前ページのクライアント→サーバーモデルに似ていますが、IH自体がサーバーであり、SDP AHとしても機能できるという違いがあります。クライアント→サーバーモデルと同様に、サーバー→サーバーモデルは、各サーバーにSDPゲートウェイあるいは同様の軽量の技術をインストールする必要があり、すべてのサーバー→サーバートラフィックを、セキュリティエコシステムおよび攻撃者の他の要素から見えなくします。ネットワークベースのIDS/IPSは、SDP外部のパケット検査の代わりに、SDPゲートウェイからドロップされたパケットを取得する必要があります。さらに、組織はホストベースのIDS/IPSシステムに依存する場合があります。



SDPコントローラは、コントローラとサーバーが同じSDPゲートウェイを使用するようにサーバーに配置できます。SDPコントローラはクラウドに存在する場合もあります。

サーバーは、AHとして機能するSDPゲートウェイの背後で保護されています。ゲートウェイはサーバー環境内にあり、ゲートウェイからの安全な接続は、サーバー上のアプリケーション/サービスの所有者の制御下にあり、所有者がこれらの接続を完全に制御できる場合があります。

保護されたサーバーは、”Deny-All”ファイアウォールとして動作するSPAで保護されているため、適切にホワイトリストに登録された他のサーバーを除き到達不能です。攻撃者や不正ユーザー（内部、外部の両方）にはアクセスできず、インサイダーの脅威から最大限の保護を提供します。

このモデルでは、保護されたサーバーにゲートウェイまたは軽量SPAプロトコルメカニズムを実装する必要があります。保護されたサーバーへのインバウンド接続を許可するように、サーバーが存在するネットワークを構成する必要はありません。これらのサーバーのゲートウェイは、SPAを使用して、内部および外部の不正接続を防止します。

また、IDS/IPSやSIEMなどの既存のネットワークセキュリティコンポーネントを簡単に使用できます。トラフィックは、SDPゲートウェイ/保護されたサーバーからのこれらのドロップされたパケットを分析することによって監視でき、クライアント/IHとサーバー間のmTLS接続を保持します。

このモデルは、組織がIoTまたはVM環境をクラウドに移行した時のすべてのクラウド環境に適しています。サーバー環境の場所（クラウドまたはオンプレミス）に関係なく、組織はクラウド内の環境への接続を完全に制御できます。

クライアント→サーバー→クライアント

場合によっては、ピアツーピアの関係になり、トラフィックが中間サーバーを通過する必要があるIP電話、チャット、ビデオ会議などのアプリケーションに使用できます。このような場合、SDPは接続クライアントのIPアドレスを難読化し、コンポーネント間のネットワーク接続を暗号化し、サーバー/AHをSPAによる不正なネットワーク接続から保護します。

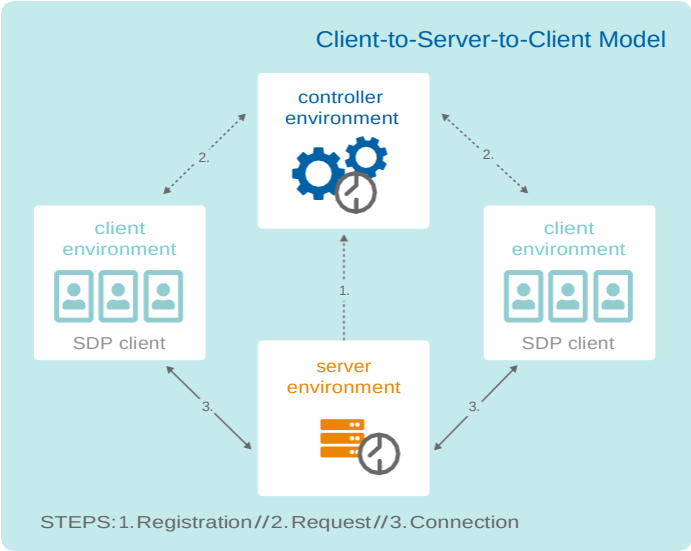


図5：クライアント→サーバー→クライアントモデル：IP電話やチャットなどのピアツーピアスタイルのサービスに使用されます。

SDPコントローラは、（コントローラとサーバーが同じSDPゲートウェイを使用する）サーバー上あるいはクラウドに配置することができます。SDPコントローラはクラウドに常駐することもできます。上記のように、サーバーはAHとして機能するSDPゲートウェイの背後で保護されています。ゲートウェイを経由するサーバーへの安全な接続は、デフォルトではサーバー上のアプリケーション/サービスの所有者の管理下にあります。

保護されたサーバーは、他の適切なオンボードクライアント以外から到達不能で、ゲートウェイとコントローラが”Deny-All”ファイアウォールとしてのsPAで保護されています。従ってサーバーは到達不能なため、攻撃者や不正ユーザー（内部と外部の両方）にはアクセスできず、インサイダーの脅威からの保護が強化されます。

このモデルでは、保護されたサーバーにゲートウェイまたは軽量SPAプロトコルメカニズムを装備する必要があります。サーバーが存在するネットワークは、保護対象サーバーへのインバウンド接続に制限するように構成する必要はありません。サーバー上のゲートウェイ（実施ポイント）はSPA を利用して、内部および外部の両方の無許可接続を防止します。

このモデルにより、IDS/IPSやSIEMなどのネットワークセキュリティコンポーネントを簡単に使用できます。SDPゲートウェイ/保護対象サーバーからドロップされたすべてのパケットを分析して、クライアントと保護対象サーバー間のmTLS接続を保護することで、トラフィックを監視できます。

このモデルは、組織がすべての環境のピアツーピアアプリケーションをクラウドに移行する場合に非常に適しています。サーバー環境がどこにあるか（クラウドまたはオンプレミス）にかかわらず、組織はクライアントへの接続を完全に制御できます。

クライアント→ゲートウェイ→クライアント

このモデルは上記のモデルの変化形です。このモデルには、SDPのアクセスポリシーを適用しながら、クライアントが互いに直接接続することが必要となるピアツーピア・ネットワークプロトコルをサポートする利点があります。

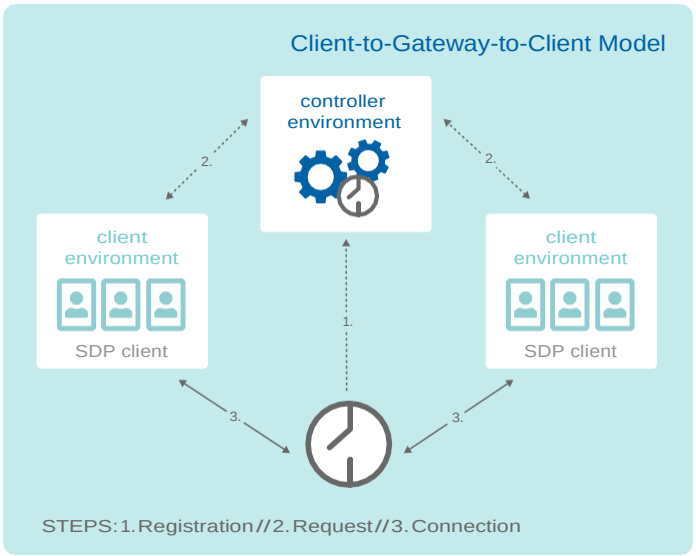


図6：クライアント→ゲートウェイ→クライアントモデル：クライアントからクライアントへの通信を保護するために使用されます。.

これにより、クライアント間で論理的な接続が確立されます（それぞれがアプリケーションプロトコルに応じてIH、AH、またはその両方として機能します）。アプリケーションプロトコルによって、クライアント同士の接続方法が決まることに注意してください。SDPゲートウェイは、それらの間で一般的なファイアウォールの役割を担います。

このモデルの詳細については、今後の出版物で追加される予定です。

ゲートウェイ→ゲートウェイ

ゲートウェイ→ゲートウェイモデルは、SDP Specification 1.0の最初の公開には含まれていませんでした。このモデルは、特定のIoT環境に適しています。このシナリオでは、1つ以上のサーバーがAHの背後にあり、AHがクライアントとサーバー間のゲートウェイとして機能します。同時に、IHがゲートウェイとしても機能するように、1つ以上のクライアントがIHの背後にあります。

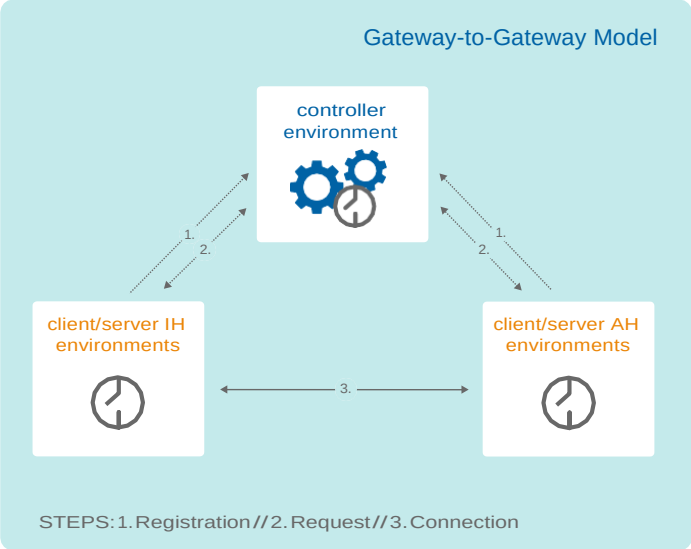


図7：ゲートウェイ→ゲートウェイモデル：1つ以上のサーバーまたはクライアントがゲートウェイの背後で保護されています

このモデルでは、クライアントデバイスはSDPクライアントソフトウェアを実行しません。実際に、プリンタ、スキャナ、センサー、IoTデバイスなどでは、SDPクライアントをインストールすることが望ましくないか不可能なデバイスタイプである可能性があります。このモデルでは、ゲートウェイはファイアウォールとして機能し、実装によってはルーターまたはプロキシーとして機能する可能性もあります。

SDP配備モデルと関連するシナリオ

以下の表は、どの配備モデルがどのSDPシナリオを利用できるかを示しています。配備の種類ごとに、異なる接続を保護する必要があります。

ネットワークシナリオ	クライアント →ゲートウェイ	クライアント→サーバー	サーバー → サーバー	クライアント → サーバー → クライアント	クライアント → ゲートウェイ → クライアント	ゲートウェイ →ゲートウェイ
アイデンティティ主導のネットワークアクセス制御	Y	Y*	Y	Y	Y	Y**
すべてのSDPモデルは、アイデンティティ主導のネットワークアクセス制御をサポートしています。 * このモデルは、ネットワークおよびサービスへの安全な接続を提供します。 **SDPがデバイスをどこまで識別できるかは、デバイスの識別と検証を実行する方法に依存します。 たとえば、MACアドレスは802.1xに基づく実装よりも弱いID検証を提供します。						
ネットワークマイクロセグメンテーション	Y*	Y **	Y ***	Y	Y	Y
すべてのSDPモデルは、個々の接続を保護することにより、ネットワークのマイクロセグメンテーションを提供します。 * このモデルは、クライアントとゲートウェイ間の接続を保護することでマイクロセグメンテーションを提供しますが、ゲートウェイの背後にあるサーバーへのマイクロセグメント接続は行いません。 **このモデルは、サーバーへのすべての接続を安全にすることによってネットワークマイクロセグメンテーションを提供します。さらに、ゲートウェイをホストするサーバーを隠します。 ***このモデルは、サーバーへのすべての接続を安全にすることによってネットワークマイクロセグメンテーションを提供します。さらに、ゲートウェイをホストするサーバーを隠します。						
セキュアリモートアクセス（VPN代替）	Y	Y	Y	Y	Y	Y
SDPモデルは、従来のVPNに代わるものです。すべての場合において、コントローラとゲートウェイ/AHは、リモートデバイスからアクセス可能である必要があり、SPAを使用して接続を開始できます。						
サードパーティユーザーアクセス	Y	Y	Y*	Y	Y	Y
SDPは、保護が必要な接続に応じて、すべてのシナリオでサードパーティアクセスをサポートします。 サードパーティは、リモートまたはオンプレミスである可能性があり、また、認証を受ける別のIDプロバイダーを持っている場合があります。 * SDPは、これらのモデルの内部アプリケーションにアクセスするすべてのサードパーティアプリケーションからの接続を保護し、サードパーティアプリケーションはクライアントとして機能します。						
特権ユーザーアクセス保護	Y	Y	N	Y	Y	N
SDPは、クライアントからの接続に対する特権ユーザーアクセスを保護します。通常、特権ユーザーアクセスはサーバーにアクセスするクライアントを対象としています。しかし、アプリケーションによっては他のモデルも適用可能です。						
価値の高いアプリケーションのアクセス保護	Y	Y	Y	Y	Y	N
ゲートウェイ→ゲートウェイモデルを除くすべてのモデルは、その特定のモデルによって保護された価値の高いアプリケーションに関連するすべての接続を保護します。.						
マネージドサーバーへのセキュアアクセス	Y	Y*	Y	Y	N	Y
このシナリオは、マネージドサーバーへのサービスプロバイダーアクセス用です。 サーバーは、ゲートウェイによって非表示にできます。 * このモデルでは、SDPゲートウェイソフトウェアがサーバーに配備されます。サーバーが非表示になり、MSSP /マネージドサービスへのサービス接続の検出および制御を許可します。						

ネットワーク統合の単純化	Y	Y*	Y*	Y	Y	Y
必要なセキュア接続のタイプに応じて、すべてのSDP配備モデルがこのシナリオをサポートします。 * これらのモデルの利点は、サーバー上のサービスをゲートウェイで非表示にできることです。						
IaaSクラウド環境へのセキュアな移行	Y	Y	Y	Y	Y	Y
このシナリオには、オンプレミスからIaaS環境へのサービスの移行を含みます。						
認証スキームの強化	Y	Y	Y*	Y	Y	Y
すべてのSDPモデルは、多くの場合ユーザーの多要素/ステップアップ認証を介して、認証を強化する機能を提供します。 *ユーザーのいないこのモデルは、ワンタイムパスワードの入力を要求できませんが、PKIやサーバーベースのHSMの使用など、多要素認証をサポートできます。 アイデンティティ管理システムは、人だけでなく、システムやデバイスにも使用すべきです。						
企業のコンプライアンスコントロールとレポートの合理化	Y	Y	Y	Y	Y	Y
すべてのSDPモデルは、コントロールを統合することにより、企業がコンプライアンスを合理化するのに役立ちます.						
DDoS攻撃対策	Y	Y	Y	Y	Y	Y
すべてのSDPモデルはゲートウェイ内でSPAを利用するため、DDoS攻撃への対応力が向上します。 “Deny-All” なゲートウェイを構成してない場合、インターネットに直接接続されたサービスは、内部でホストされているサービスと比較して、DDoSの影響を受けやすくなります。						

SDP接続セキュリティ

アーキテクチャとして、SDPはネットワークスタックのすべてのレイヤで安全に接続するためのプロトコルを提供します。図8は、各SDPの配備モデルによって保護されている接続について示しています。重要な場所にゲートウェイとコントローラを配置することで、実装者は最も重要な接続の保護に集中し、ネットワークベースおよびクロスドメイン攻撃から保護することができます。

Single-Packet Authorization (SPA)

SDPモデルの最も重要な要素の1つは、「接続前認証（authenticate-before connect）」モデルを必要としている（実施している）ことです。これは、TCP / IPの根本的にオープンな（そして安全でない）性質を補うものです。SDPは、Single Packet Authorization（SPA）を通してこれを実現しています。SPAは、デバイスまたはユーザの身元を検証し、追加のアクセス制御を実施する関連するシステムコンポーネント（コントローラまたはゲートウェイ）へのネットワークアクセスを許可するだけの軽量プロトコルです。

要求者のIPアドレスを含むこのリクエストに関する情報は、単一のネットワークメッセージの中で暗号化および認証が行われます。SPAの目的は、デフォルトドロップのファイアウォールを通してサービスを見えなくすることができることです。そしてそのサービスへのアクセスは、認証（そして暗黙の認可）が起こったときに一度だけ許可されます。SPA はSDP仕様の中核部分であり、クライアントからコントローラ、ゲートウェイからコントローラ、クライアントからゲートウェイのすべてで通信を開始するために使用されます。

SPAの実装方法は多少異なる場合がありますが、以下の共通の原則を共有する必要があります。:

1. SPAパケットは、暗号化されなければならないし、認証されなければならない。
2. SPAパケットは、必要な情報をすべて1パケットの中に含めなければならない。パケットヘッダーは信頼できると考えてはいけません。
3. SPAパケットは、生成および送信するために管理者またはルートレベルのアクセスに依存してはいけません。パケットそのものの操作はありません。
4. サーバーは、SPAパケットをできるだけ静かに受信して処理しなければならない。応答も検証も送信されません。

SPAの利点

SPAはSDPで大きな役割を果たします。SDPの目標の1つは、TCP/IPの基本的にオープンで安全でない特性を克服することです。これは、「接続してから認証する」モデルです。今日のサイバーセキュリティの脅威の状況を考えると、悪意のある攻撃者が企業のシステムをスキャンして接続することを許可することは受け入れられません。SPAとSDPの組み合わせは、2つの方法でこの脆弱性に対処します。

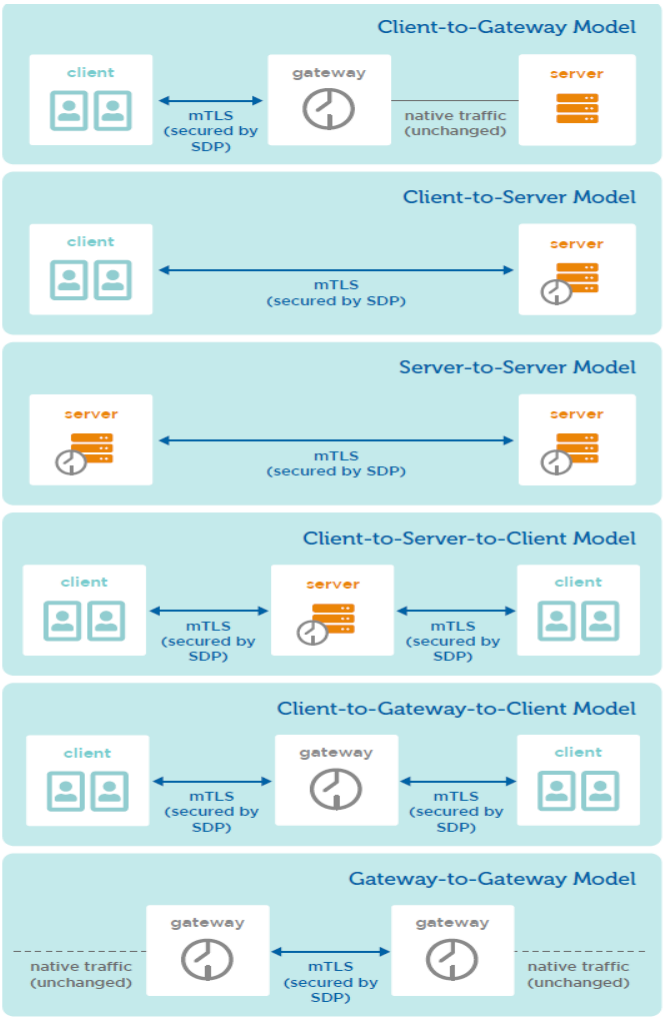


図8：各展開モデルで保護された接続

SDPアーキテクチャを使用するアプリケーションは、SDPゲートウェイ/AHの背後に隠されているため、許可されたユーザーのみがアクセスできます。さらに、SDPコンポーネント自体（コントローラーとゲートウェイ）は、SPAによって保護されています。これにより、インターネットに面した状況で安全に配備でき、正当なユーザーが生産的で信頼性の高いアクセスを確保し、許可されていないユーザーには見えなくなります。SPAは、サービスを見えなくするという重要な利点を提供します。”Deny-All”ファイアウォールのスタンスは、ポートスキャンおよび関連する偵察技術を軽減します。このタイプのファイアウォールは、SPAコンポーネントを許可されていないユーザーに見えなくし、SDP全体の攻撃対象領域を大幅に削減します。SPAは、多くの実装でポートが開いているなどの既知の脆弱性があるVPNよりも多くのセキュリティを提供します。

別の利点は、ゼロデイからの保護です。認証されたユーザーのみが目的のサービスにアクセスできるので、新たに発見された脆弱性はそれほど問題ではありません。

もう1つの利点はDDoSからの保護です。もし、HTTPSサービスが攻撃可能なパブリック・インターネットに公開されている場合、比較的少量のトラフィックでHTTPSサービスをオフラインにすることができます。SPAは、認証されたユーザーのみにそのサービスを見えるようにしているので、DDoS攻撃は、保護されているサービス自体ではなく、デフォルトドロップのファイアウォールによって処理されます。

SPAの制限

SPAはSDPの一部にすぎず、それだけでは完全ではありません。SPAの実装はリプレイ攻撃に対してレジリエントであるように設計されるべきですが、SPAは中間者攻撃（MITM）を受ける可能性があります。具体的には、MITMの攻撃者がSPAパケットをキャプチャまたは変更できる場合、攻撃者は認可されたクライアントに代わってコントローラ/AHへのTCP接続を確立できる可能性があります。しかしながら、この攻撃者はクライアントの証明書を持っていないため、mTLS接続を行うことができません。そのため、コントローラ/ AHは、この接続の試行を拒否し、TCP接続を閉じます。MITMシナリオにのみ適用されるこの制限を考慮しても、SPAは標準のTCPよりはるかに安全です。SPAの実装は、ベンダーによって若干異なる場合があります。オープンソースのSPA参照の実装は、Fwknopプロジェクト、あるいはは「FireWall KNock OPerator」で利用できます。SPAの詳細な技術情報については、38ページの「Appendix 2」を参照してください。その他の優れた参考資料は、Evan GilmanとDoug BarthによるZero Trust Networksの「Trusting the Traffic」の章です（O'Reilly Media、Inc.、2017）。

SDPとアクセス制御

新しいアーキテクチャとしてのSDPの価値は、情報資産とネットワークサービスを保護するために、ユーザーアクセス管理、ネットワークアクセス制御、システム認証制御を実装するための標準を設定するアクセス制御管理を強化することです。SDPには、許可されていないユーザーからのネットワークレベルのアクセス、あるいは、未検証のデバイスの使用を防止するアクセス制御を実施する機能があります。 SDPは”deny-all”ゲートウェイを配備するため、ネットワークパケットがIHとAHの間を流れるのをブロックまたは許可または防止します。SDPを使用すると、組織は、少なくとも、どのアイデンティティがネットワークサービスおよびどの検証済みデバイスからのアクセスを許可するかを決定するアクセスポリシーを定義および制御できます。

SDPは、既存のアイデンティティとアクセス管理のソリューションを置き換えようとしません。しかし、SDPはユーザー認証のみのアクセス制御を拡張します。SDPはユーザーの認証と認可を他のセキュリティコンポーネントと統合することで、攻撃対象領域を大幅に縮小します（ページ8「中心となるSDP コンセプト」を参照）。例として、私たちのお気に入りのユーザーJaneは、会社の稼働中の財務管理サーバーにサインインするための資格情報を持っていないとします。もしそれがネットワーク上のJaneのデバイスから見える場合、それはリスクになります。Janeの会社がSDPアーキテクチャを実装している場合、財務管理サーバーはJaneのデバイスから隠されています。そのため、攻撃者がJaneのマシンに足場を築いたとしても、SDPはJaneのデバイスからJaneが資格情報を持たない財務管理サーバーへの接続を拒否します。Janeが財務管理サーバーへのアクセスを許可する資格情報を持っていたとしても、SDPクライアントをデバイスにインストールすると、さらに保護が提供されます。攻撃者は多要素ユーザー認証と強力なデバイス検証を有効にして接続を確立するのは困難です。

補完的なアーキテクチャ

ゼロトラストとBeyondCorp

Software-Defined Perimeterに加えて、今日のセキュリティ環境には2つの新しいアプローチがあります。最初は業界アナリスト会社Forresterによって推進された「ゼロトラスト」コンセプトと、Google社内の「BeyondCorp」イニシアチブです。

Forresterゼロトラストモデル

Forresterのゼロトラストモデルは、過去数年間で範囲が拡大し、主に次の3つの原則に基づいています:

- すべてのリソースが場所に関係なく安全にアクセスされるようにする
- すべてのトラフィックを記録して検査する
- 最小特権の原則を実施する

これらの原則は、SDPが提供するものと明確に整合が取れています。実際、SDPアーキテクチャは、ゼロトラストの原則を実装する理想的な方法であると考えています。SDPはユーザーとデバイスを強力に認証し、ネットワーク接続を暗号化するため、ユーザーの場所に関係なく、すべてのリソースに安全にアクセスできます。また、SDPは通常、既存のネットワーク全体にオーバーレイとして配備されるため、リソースの場所（オンプレミス、クラウド、またはその他）に関係なく、すべてのリソースに安全にアクセスできることも保証します。ネットワーク接続はSDPによって制御されるため、どのID（人間またはマシン）がどのリソースにアクセスしているかを記録するための効果的かつ一元化された場所を提供します。ディープパケットインスペクションが必要な場合、SDPはネットワークトラフィックのインスペクションシステムと簡単に統合できます。最後に、おそらく最も重要なこととして、SDPは本質的かつ強力に最小権限の原則を実施します。SDPはデフォルトですべての通信を拒否するゲートウェイから始まり、アクセスはホワイトリストアクセスモデルに厳密に従うため、IDはSDPコントロールによって明示的に許可されている場合にのみネットワークアプリケーション（およびSDPシステム自体）にアクセスできます。これが最小権限の原則の本質です。

GoogleのBeyondCorpモデル

BeyondCorpは、従業員が内部リソースにアクセスできるように設計されたGoogleの内部ネットワークおよびアクセスセキュリティプラットフォームであり、企業発行のChromebookを管理するためのデバイス検証に重点を置いています。Googleチームによって文書化されており、すべてのアカウントで過去5年間にわたってGoogleで成功した内部プロジェクトとなっています。

BeyondCorpは、いくつかの点でSDPアーキテクチャと異なります。BeyondCorpは、http、https、およびsshプロトコルをサポートするWebプロキシベースのソリューションですが、SDPは通常、より多くの（一部の実装ではすべての）IPプロトコルをサポートします。SDPは、BeyondCorpよりもきめの細かいアクセス制御もサポートしています。BeyondCorpは、アプリケーションが割り当てられる少数の「信頼層」を持っています。SDPは、ユーザーおよびデバイスのコンテキストにより、よりきめ細かく個別化されたアクセス制御をサポートします。

GoogleのBeyondCorpは市販されていませんが、BeyondCorpプラットフォームの一部の要素をマイクロサービスを保護するためのistioプラットフォームに含めています。また、Googleは、Google Cloud Platform（GCP）ベースのリソースへのアクセスを制御するためのIdentity-Aware Proxy（IAP）と呼ばれる無料のコンポーネントを開始しました。IAPはSDPではありません（完全なBeyondCorpでもありません）が、Googleが述べているように、「クラウドIAPはBeyondCorpの構成要素です」。

ゼロトラストを検討する場合の結論として、アーキテクチャとしてSDPを評価する必要があります。BeyondCorpアプローチが望ましい場合でも、SDPを評価する必要があります。SDPは同様のメリットをもたらし、すべての環境でアクセスを保護する複数の市販ソリューションがあるためです。

要約すると、アーキテクチャとしてのSDPは、ゼロトラストの原則の実装を確実に成功させることができます。BeyondCorpの実装においては、自社のBYOD戦略にSDPアーキテクチャを組み込み、推進してく必要があります。

SDPとエンタープライズセキュリティアーキテクチャ

エンタープライズ情報セキュリティアーキテクチャは、組織全体に多数の利害関係者がいるため、複雑になる可能性があります。SDPは、基盤となるIPインフラストラクチャに関係なく、安全な接続を保証します。SDPは、以下の重要な概念を備えているため、エンタープライズセキュリティアーキテクチャの基盤になります:

1. 接続を許可する前にユーザーを認証し、デバイスを検証する
2. 双方向暗号化通信
3. deny-allファイウォールに基づいた動的制御およびサーバー隠蔽
4. アプリケーションコンテキストときめ細かいアクセス制御の統合

このセクションでは、アーキテクトが企業にSDPを配備する計画を立てる際に考慮すべき多くの質問を示します。質問は、アーキテクトが利用数、ネットワーク、サーバー環境、セキュリティおよびコンプライアンス要件など、セキュリティのさまざまな側面を検討するのに役立ちます。

SDPの配備は、既存のネットワークテクノロジにどのように適合しますか?

アーキテクトは、どのSDP配備モデルを使用するかを決定する必要があります。また、いくつかのモデルにおいては、ゲートウェイが追加のインラインネットワークコンポーネントになる可能性があることを理解してください。これは、保護されたサーバーを見えないようにし、SDPゲートウェイ経由でのみアクセス可能にするために、ファイアウォールやルーティングの変更を必要とするなど、ネットワークに影響を与える可能性があります。

SDPは、監視およびロギングシステムにどのように影響しますか？

SDPはIHとAHの間でmTLSを使用するため、このネットワークトラフィックは、セキュリティ、パフォーマンス、信頼性を監視する目的で配置されている可能性がある中間サービスに対して不透明になります。アーキテクトは、どのシステムが稼働しているのか、またネットワークトラフィックの変更がそれらにどのように影響するのかを理解する必要があります。反対に、SDPシステムは通常、より豊富なアイデンティティ中心のユーザーアクセスのログ記録を提供するため、既存の監視システムを強化するために使用されることがよくあります。さらに、SDPゲートウェイおよびコントローラでドロップされたパケットはすべて、より深く分析するためにSIEM に記録できます。誰が、いつ、何を、どこからという、すべての接続の情報を、SDPを用意することで簡単に収集できるようになります。

SDPは、APIの統合を含む、アプリケーションのリリース/DevOpsプロセスおよびツールセットにどのように影響しますか？

多くの組織がDevOpsやCI / CDなどの高速アプリケーションリリースプロセスを採用しています最小権限。これらのプロセス、およびそれをサポートする自動化フレームワークは、セキュリティシステムとの慎重な統合を必要とし、SDPも例外ではありません。SDPは、DevOpsの中で非常に効果的に使用され、認可されたユーザーが開発環境への接続を安全に行うことができます。SDPは、正当なユーザーから保護されたサーバーやアプリケーションへの接続を保護するために運用中にも使用できます。

セキュリティアーキテクトは選択したSDP配備モデルを理解し、組織のDevOpsメカニズムがSDPと相互連携し統合する方法を理解しなければなりません。API統合はDevOpsのツールセットとの統合が必要となることが多いため、セキュリティチームは、SDPの実装においてサポートされる一連のAPIを検討する必要があります。

SDPは、ユーザー、特にビジネスユーザーにどのような影響を与えますか？

セキュリティチームは、通常、ソリューションをユーザーに対してできるだけ透過的に機能させるように努めています。SDPはこれをサポートします。もし、最小権限の原則が達成されると、ユーザーは必要なものすべてにフルアクセスできるようになり、不要なアクセスが取り除かれたことに気付くことはありません。SDP配備モデルに応じて、ユーザーは自分のデバイスでSDPクライアントソフトウェアを実行します。セキュリティアーキテクトは、ITと協力して、ユーザーエクスペリエンス、クライアントソフトウェアの配布、デバイスのオンボードプロセスのモデル化と計画を立てる必要があります。

エンタープライズ情報セキュリティ アーキテクチャ要素

下の図9は、エンタープライズセキュリティアーキテクチャの主な要素を示しています。この図は、ハイブリッドエンタープライズを単純化したもので、プロトタイプのセキュリティインフラストラクチャの主要要素と要素間の論理的な関係を表しています。

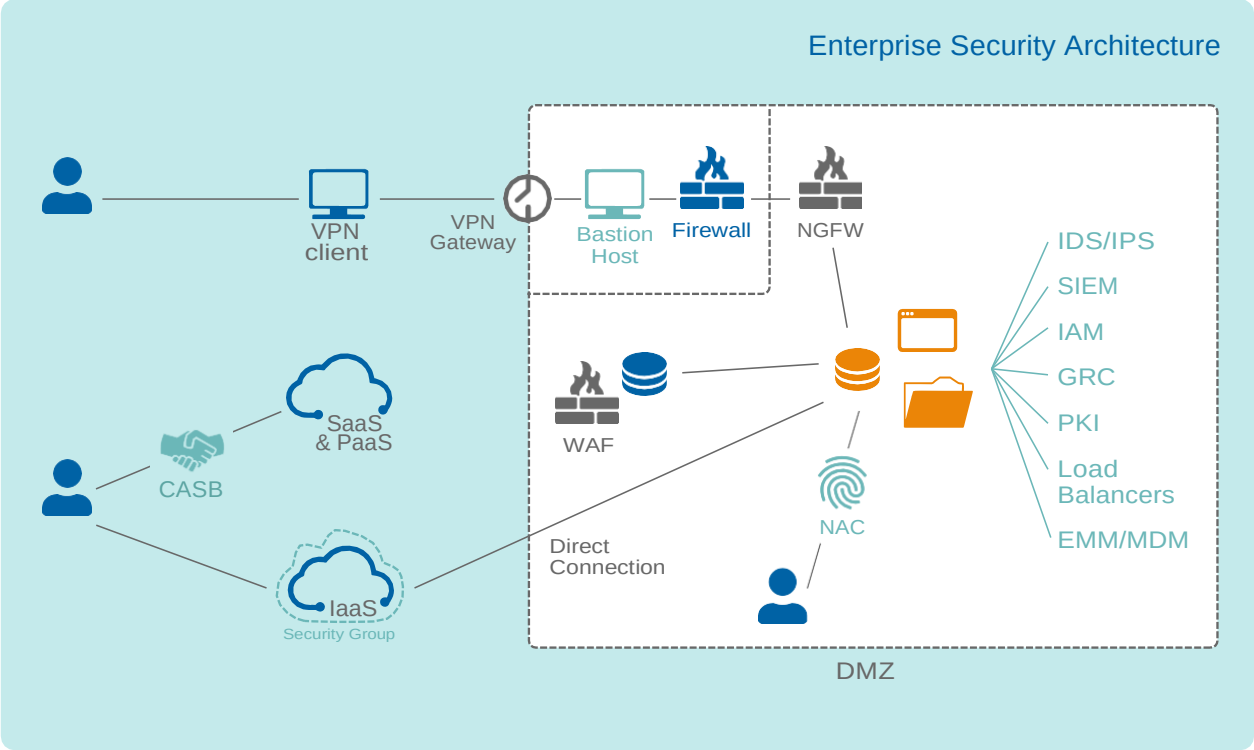


図9：エンタープライズセキュリティアーキテクチャの主な要素

このエンタープライズセキュリティアーキテクチャの例では、オンプレミスおよびクラウドベースのリソース（IaaSおよびSaaS/PaaS）で構成され、セキュリティ、IT、コンプライアンスコンポーネントの標準セットを備えています。これらの標準コンポーネントとSDPの統合方法については、次のページ以降で詳しく説明します。

Security Information and Event Management (SIEM)

SIEMシステムは、アプリケーションやネットワークコンポーネントから生成されたログ情報およびセキュリティ警告の分析を行います。SIEMは、ログの保存と解釈を一元化し、ほぼリアルタイムの分析を可能にし、セキュリティ担当者がより迅速に防御措置を取ることを可能にします。SIEMシステムは、また、コンプライアンス（規制、監査）に通常必要とされる自動化され一元化された報告を提供します。

SIEMシステムは、オンプレミスにでもクラウドにでもおかれ、ITおよびセキュリティ管理システムの主要な部分として設置されます。市販のSDPソリューションは、通常、内部でロギング機能を提供していますが、SDPログが複数のソースからの情報を集約するエンタープライズSIEMシステムに送信されると、その価値はさらに高まります。企業システムは、分散されたSDPコンポーネントから直接フィードを受けたり、複数の収集エージェントを階層的に配置したりすることがあります。SIEMは、SDP用に事前定義およびカスタマイズされたイベントを集中管理コンソールに転送するか、電子メールを介して指定された個人にアラートを送信することによって、検査を実行し、異常に対してフラグを立てます。

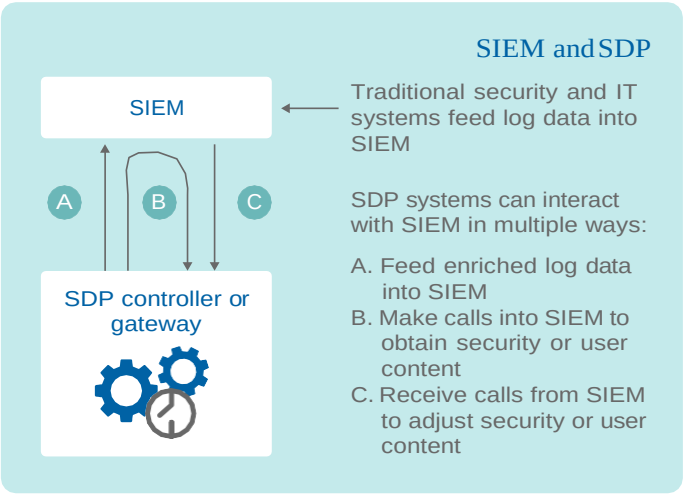


図10：SDPを用いたSIEM

SDPはアイデンティティとデバイスを検証することで接続の観点からアクセスを制御するため、通常のネットワークまたはアプリケーション監視ツールよりもはるかに豊富な情報をSIEMに提供します。SDPは、リアルタイムに、誰が、何を、どこからという、あらゆる接続に関する情報を提供することができ、それによってSIEMシステムの有効性と価値を高めることができます。SIEMは現在ロギングに使用されており、アナリストは複数のログから情報をまとめる必要があり、許可されていないユーザーはもちろん、許可されていないデバイスがどこへ接続しようとしているかも識別します。SDPは、特定のユーザーが特定のデバイスから特定のサービスに接続した接続情報について、SIEMに明確な情報を提供します。SDPクライアントがユーザーのデバイス上にある場合は、そのデバイスからより具体的な情報も収集できます。SDPゲートウェイからは、ドロップされたすべてのパケットを分析のために保存します。これは、潜在的なハッキングだけでなく攻撃者による偵察などの分析になります。
このレベルの記録は、従来のファイアウォールによって生成されたIPアドレスとポートのリストよりも優れています。

これは、（たとえば）従来のファイアウォールによって生成されたIPアドレスとポートのリストよりもはるかに優れた情報です。SDPは、複数のデバイスで発生するユーザーアクティビティを簡単に関連付けるSIEMの機能も強化します。SDPなしでは、特にBYODやモバイル機器の出現により、これを達成することは困難であるかエラーが発生しやすくなります。

SIEMをSDPの配備と統合すると、セキュリティ操作を事後対応型から予防型に移行するという目標を達成することができます。リスクを制御するには、SDPログ情報を含めることに加えて、既存のSIEMも重要な情報源と見なす必要があります。SIEMは、ユーザーの接続を切ったり、未検証のデバイスまたは特定のホストからの接続を拒否したり、疑わしい接続をドロップすることにより、リスクを制御するのに役立ちます。たとえば、SIEMが不正なユーザーアクティビティを示す通常よりも高いリスクレベルを示した場合、SDPは、追加の分析を実行できるようになるまで、ユーザーからのすべての接続をドロップします。SDPは、接続のアドレス指定と制御を数秒で行うことにより、SIEMを補完します。

ログ情報を生成するすべてのシステムと同様に、SDPログは企業にとってデータプライバシーの潜在的な懸念事項になります。ネットワーク接続（およびそのメタデータ）はログ内の特定のユーザーに関連付けられる可能性があるため、組織はこの問題に対処するためにSDPの配備中に予防策を講じる必要があります。

SDPは、さまざまな種類の攻撃を防止、検出、対応するためのSIEMシステムの機能を強化および向上させます。次のページに、軽減できる攻撃の種類の例をいくつか示します。（SDPとSIEMを統合することで防止される攻撃の網羅的なリストは、将来のCSAの出版物で予定されています）。

攻撃の種類	軽減	SDPのSIEMへの統合の仕方
ポートスキャン/ネットワーク偵察	ブロックと通知	SDPは不正なネットワークアクティビティをすべてブロックし、SIEM内で使用するためにすべての接続要求をログに記録できます。
DoS攻撃	ブロックと通知	SDPシステムはSPAによって保護されているため、DoS攻撃はほとんど効果がありません。SPAは、不良パケットをドロップします。これはSIEMに記録できます。
認可されたリソースの悪用	検出と対応	認可されたリソースへの認可されたユーザーのアクセスは、SDPによって許可されますが、SIEMは異常な行動についてユーザーのアクティビティを分析できます。また、SDPは更なる分析が行われるまでこの許可されたユーザーによるアクセスを許可しません。
盗まれたクレデンシャルの使用	ブロックと通知	通常、SDPは、デバイスの検証やオンボーディング（訳注： 新規デバイスが有線/無線のネットワークに初めてアクセスできるようにするプロセスのこと）など、接続前に複数の要素が必要です。これにより、盗まれたパスワードは攻撃者がアクセスするのに不十分になります。

従来のファイアウォール

従来のファイアウォールは、一連の規則に従ってネットワークトラフィックを監視および制御します。これらは、OSI（Open Systems Interconnection）モデルのレイヤ2から4（データリンクレイヤ、ネットワークレイヤ、トランスポートレイヤ）の情報を使用してネットワークパケットデータをフィルタリングします。従来のファイアウォールは、5タプルで表現された単純なルールモデルをサポートしています。ファイアウォールは、ネットワークアドレス変換（NAT）やポートアドレス変換（PAT）などの機能もサポートする場合がありますが、ここでは直接関係ありません。

ファイアウォールは何十年もの間、エンタープライズネットワークセキュリティの主力でしたが、5タプルの限られた世界の中でのみ動作しているため、多くの制限があります。特に、アイデンティティ情報に基づいてルールを表現する（または実施する）ことができず、通常は静的なルールセットを表現することができるだけです。したがって、セキュリティインフラストラクチャの一部にすぎません。

ファイアウォールを利用する（あるいは同等のネットワークトラフィック実施機能を実装する）SDPは、今日の企業のファイアウォールの使用方法を大幅に改善します（そしてある意味では誤用を招きます）。SDPは、今日組織がファイアウォールを使用しようとしているネットワークアクセス制御の実施の大部分を引き受けるでしょう。SDPを使用すると、企業はファイアウォールのルールセットを大幅に減らすことができます。5タプルの制約内でアイデンティティ中心のアクセス制御をモデル化することを試みる代わりに、SDPはそれらをSDPアクセス制御としてはるかに正確に表現し実施することを可能にします。これにより、複雑な環境でのファイアウォールルールの作成、テスト、デバッグ、配備に必要な作業が軽減されるだけでなく、はるかに正確で豊富なアクセス制御メカニズムも可能になります。

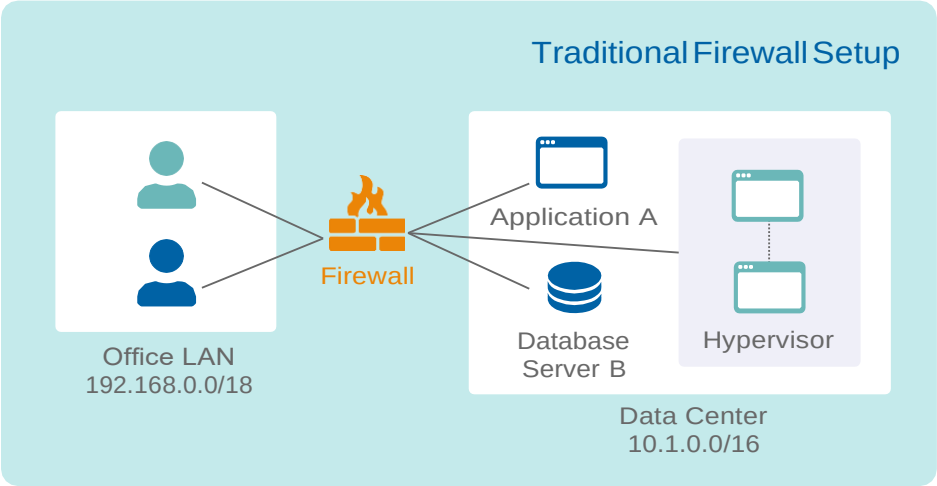


図11：従来のファイアウォール設定

*上の図11*は，ユーザーサブネット（192.168.100.0/24）からローカルデータセンターサブネットへのアクセスを制御するために、単一のファイアウォールを使用する従来のオフィスLAN環境を示しています。この図は単純ですが、静的なファイアウォールルールを使用してこのアクセスを保護しようとすることの難しさを示しています。

ファイアウォールはオフィスネットワーク上のユーザーを区別できません。IPアドレスのみ表示されるからです。さらに、多くのユーザーが、定期的に接続および切断するラップトップを使用しているため、ユーザーのIPアドレスは頻繁に変更します。

一般的なデータセンターネットワークには、テストシステムと本番システムの両方を含むさまざまなワークロードがあります。アプリケーションの中には長寿命で静的IPアドレスを持つものもありますが、別のアプリケーションでは定期的に作成および破棄される（したがって予測不可能なIPアドレスを持つ）仮想マシン上に構築されます。個々のユーザーがデータセンター内のすべてのサーバー（およびそれらのサーバー上のすべてのポート）にアクセスする必要はありませんが、この環境では、実質的にファイアウォールにオフィスLANのすべてのIPアドレスからデータセンターネットワーク内のすべてのIPアドレスへのアクセスを許可するルールセットを設定します。

SDPのクライアント→ゲートウェイモデルの簡略版を示す以下の図と比較してください（わかりやすくするためにコントローラを省略しています）。従来のファイアウォール設定と、下の図12を比較してください。図12は、SDPのクライアント→ゲートウェイモデルの簡略バージョンを示しています（わかりやすくするためにコントローラを省略しています）。他のSDP配備モデルにも同様に適用されることに注意してください。

この例では、ネットワークファイアウォールは、ファイアウォール機能を実行するSDPゲートウェイに置き換えられています。SDPはアイデンティティと使用しているデバイスに基づいてアクセスを制御するため、組織はデータセンターに対してきめ細かいアクセス制御を適用できます。大規模な攻撃対象となるオープンでフラットなネットワークは最小限に抑えられています。データセンター内のサーバーの近くまたは上にSDPゲートウェイを追加することで、特定のサービスへのよりきめ細かいアクセスを実現できます。（上記のクライアント→サーバーモデルを参照）

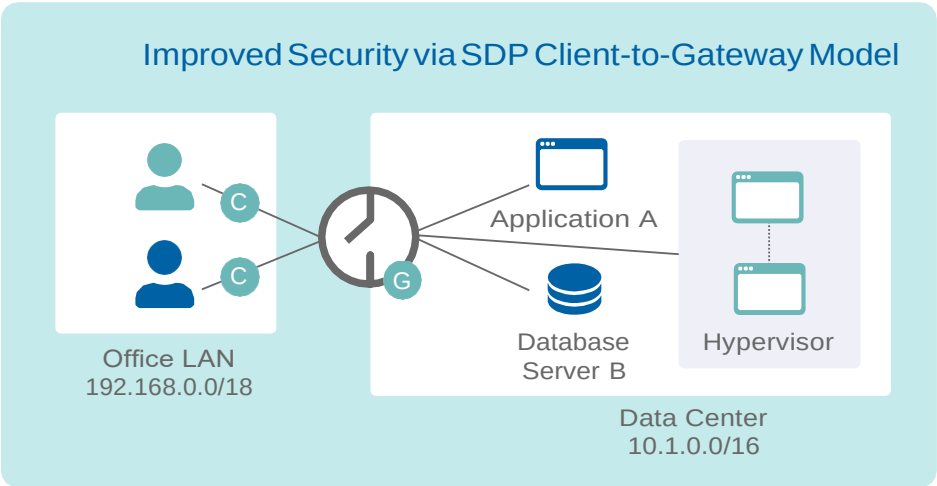


図12:SDPクライアント→ゲートウェイモデルを使用して改善されたセキュリティ

侵入検知/防止システム（IDS/IPS）

侵入検知および侵入防止システム（IDS/IPS） - ここでは同義的に扱います - 悪意のある活動やポリシー違反についてネットワークやシステムを監視するセキュリティコンポーネントです。これらは、ネットワーク型（トラフィックの検査）あるいはホスト型（アクティビティおよび潜在的にネットワークトラフィックの検査）があります。SDPはIDS/IPSシステムの導入にプラスの影響を与える可能性がありますが、コスト削減のためにIDS/IPSの必要性を排除しても、ネットワーク型のIDSの変更や小規模な運用（つまり単一ネットワークのリモートオフィス）には必要です。

さらに、SDPはクライアントとゲートウェイ間で双方向TLS（mutual TLS）暗号化を使用するため、ネットワークトラフィックはTLSインスペクションに基づくネットワークベースのIDSでは見えなくなります。IDSは通常、証明書をインポートしてTLSトラフィックのプロキシーになります。（これは攻撃対象を増大させる副作用があります）/これは双方向TLSに基づいており（通常は一時証明書を使用）、したがってIDSが果たすMITMの役割に耐性があるため、一般にSDPでは不可能です。

これらの論理接続のmTLSセグメント（紫色で表示）は、外部のシステムには不透明です。これらはSDPの資格情報を使用して暗号化されているため、このトラフィックを分析しようとするシステムにはアクセスできません。ある意味では、この変更はTLS 1.2から1.3への移行と同様に、中間のセキュリティやネットワーク監視システムに影響を与えることになります。ページ 21、SDP接続セキュリティを参照.）

SDPの展開にはIDSシステムの変更が必要になる場合がありますが、許可されていないネットワークトラフィックをすべてブロックすることにより、システムのノイズを削減するという利点をもたらします。この移行により、IDSとそれを運用しているチームは、許可されたアプリケーションへのネットワークトラフィックに集中し、内部の脅威の検出にリソースを移行できます。

さらに、SDPは「ハニーポット」システムの作成と有効性を単純化し、強化することができます。保護されたシステムは攻撃者には見えないため、悪意のある行為者がハニーポットを見つけて攻撃する可能性が高くなります。これは、承認されたユーザーまたは承認されていないユーザーにとって目に見えるシステムの割合が高いためです。これにより、ネットワーク上の悪意のあるアクティビティをより迅速に検出できます。

仮想プライベートネットワーク（VPN）

VPNは、信頼できないネットワーク間で安全なプライベートネットワーク接続を確立するために使用されます。VPNは、安全なリモートアクセス（従業員から企業サイトへ）、安全なサイト間通信（サイト間）、または異なる企業間（サイト間エクストラネット）でさえも一般的に使用されています。VPNは一般にTLSまたはIPSecを使用しますが、他の種類も存在します。

VPNはネットワークトラフィックのカプセル化と暗号化を提供しますが、SDPによって解決されるいくつかの制限もあります。SDPの展開にはIDSシステムの変更が必要になる場合がありますが、許可されていないネットワークトラフィックをすべてブロックすることにより、システムのノイズを削減するという利点をもたらします。この移行により、IDSとそれを運用しているチームは、許可されたアプリケーションへのネットワークトラフィックに集中し、内部の脅威の検出にリソースを移行できます。第一に、VPNは一般に広く、過度に寛容なネットワークアクセスを提供します。VPNは通常、基本的なアクセス制御制限のみを提供します（たとえば、サブネット範囲に基づく）。これは多くの組織におけるセキュリティとコンプライアンスのリスクを表します。第二に、分散環境では、VPNは企業のデータセンターを介してユーザートラフィックの不要なバックホールを必要とし、待ち時間と帯域幅のコストを追加する可能性があります。第三に、VPNサーバー自体は、定義上、インターネット上のサービスとして公開されています。VPNサーバーにはセキュリティの脆弱性が存在することがあります。これは攻撃者によって悪用される可能性があります。

さらに、VPNはユーザーにかなりの負担をかけ、弱いユーザーエクスペリエンスをもたらします。ユーザーは、どのアプリケーションがVPNの使用を必要としているか（およびどのアプリケーションがそうしていないか）を覚えており、手動で接続および切断する必要があります。複数の遠隔地にアクセスする必要があるユーザーの場合、VPNでは、両方の場所に同時に接続できないため、環境間での切り替えが必要になります。クラウドの移行が行われるたびに、VPN管理は複雑になり、IT管理者は複数の場所にまたがってVPNおよびファイアウォールポリシーを設定および同期することになります。これにより、不当なアクセスを排除することがさらに困難になります。

VPNは明らかにSDPによる置き換えの主なターゲットです。VPNと同様に、SDPもユーザーのデバイスにクライアントをインストールする必要があります。VPNの代わりにSDPを使用することで、組織は、リモートユーザーとオンプレミスユーザーの両方、およびモバイルデバイスユーザーにとって一貫性のある単一のアクセス制御プラットフォームを持つことができます。そして、特にインターネットにさらされている環境においてSDPはSPAとダイナミックなファイアウォールを使用してゼロ可視性を提供し、一般的なVPNサーバーよりも攻撃にかなり弾力性があります。

次世代ファイアウォール (NGFW)

一般に、次世代ファイアウォールは上記の伝統的なファイアウォールの特性と利点を持ち、追加の機能が含まれています（それが「次世代」なるものです）。特に、事前定義された規則に従ってアクセスを監視し、ネットワークパケットを検査し、OSI（Open Systems Interconnection model）の第2層から第4層（データリンク層、ネットワーク層、トランスポート層）の情報を使用してデータをフィルタリングします。さらに、第5層から第7層（セッション層、プレゼンテーション層、およびアプリケーション層）の情報を使用して追加機能を実行します。

ベンダーに応じて、以下の機能の一部または全部を提供する可能性があります:

- アプリケーション認識 - アプリケーションを認識して、どの攻撃を探すべきかを判断します。
- 侵入検知システム（IDS） - ネットワークのセキュリティステータスを監視します。
- 侵入防止システム（IPS）：セキュリティ問題を防ぐためにトラフィックを拒否します。
- アイデンティティ認識（ユーザおよびグループ制御） - ユーザーがアクセスできるリソースを制御します。
- Virtual Private Network（VPN;バーチャルプライベートネットワーク） - NGFWは、信頼できないネットワークを介したリモートユーザアクセスに対してこの機能を提供することがあります。

NGFWは、従来のファイアウォールや、個別のセキュリティデバイス/アプライアンスの調整に比べて大幅に改善されていますが、まだ制限があります:

- 他のIDS / IPSと同様に、特にファイル検査を実行している場合は、ネットワークトラフィックにレイテンシが増加します。
- スケーラビリティの問題 - 規模を拡大するためにはかなり充実したハードウェアが必要になる場合があります。
- ルールの複雑さ - 一部のNGFWベンダーは、ユーザーやグループの属性など、IDに関する機能を備えていますが、逸話的にこれらは実装が複雑になる傾向があります。

SDPは配備されたNGFWを自然に補完するものです - 企業はセキュアなユーザーアクセスポリシーのためにSDPを使用することができますが、コアのファイアウォール機能、IDS/IPSおよびトラフィック検査にNGFWを使用することができます。SDPをNGFWと統合することの利点は、可視性をゼロにし、それらをより動的にすることです（このセクションの後半で説明します）。ユーザーアクセスポリシーは、NGFWをIAMまたはADと統合することによって実現できます。しかし、真の安全な接続とそれらの制御を得るためには、SDPを使用してください。

ある意味で、NGFWアーキテクチャはSDPと競合し（そしてオーバーラップします）、これがここで議論するポイントです。過去10年ほどで、NGFWベンダーは市場で大成功を収めており、SDPと同じ問題のいくつかを革新し、解決しようとしてきました。具体的には、NGFWとVPN機能とユーザーおよびアプリケーションの認識を組み合わせることで、企業はある程度までSDPの目標の多くを達成できます。ただし、ここで説明する一般的なアーキテクチャ上の違いがいくつかあります。 NGFWシステムはIPベースであるのに対し、SDPはコネクションごとの制御であるため、許可された接続の制御が容易です。NGFWは、限られたアイデンティティとアプリケーション中心の機能を提供する傾向があります。それらのアクセスポリシーモデルは通常粗粒度であり、厳密に必要なものよりも広いネットワークアクセスをユーザーに提供します。それらはSDP よりもはるかに動的ではない傾向があります。SDPは多くの場合、外部システムをアクセス決定に含める機能をサポートしています。たとえば、承認された変更管理ウィンドウ中にのみ開発者がステージングサーバーにアクセスすることを許可します。SDPシステムは、ステップアップ認証を実施することもできます。これは通常、NGFWではサポートされていません。

NGFWは依然としてファイアウォールであり、ロケーション間のサイト間接続を伴う従来の境界中心のネットワークアーキテクチャを義務付けていることがよくあります。SDP配備は通常、より分散された柔軟なネットワークをサポートし、それによって柔軟なネットワークセグメンテーション機能を可能にします。SDPは基本的に「知る必要性」（ホワイトリスト）セキュリティモデルに基づいています。これは、設計上、すべての不正なサービスをユーザーから隠し、SPA と動的ファイアウォールを利用してSDPで保護された接続を隠します。NGFWは単純にこのように設計されていないため、通常はSDPよりも目に見える（したがってリスクが高い）環境になります。

アイデンティティとアクセス管理(IAM)

アイデンティティおよびアクセス管理（IAM）システムは、（認証を介して）自分のアイデンティティを検証し、それらのアイデンティティに関する管理された属性とグループメンバーシップを保存するためのメカニズムをユーザーとデバイスに提供します。SDP アーキテクチャは、ユーザー認証およびユーザー属性の取得のために、LDAP、Active Directory、SAMLなどの既存のエンタープライズIAMプロバイダーと統合するように設計されています。

SDPは、通常、接続を確立するために使用されているデバイスの属性とともに、IAM属性やグループメンバーシップなどの要素に基づいてアクセスを制御します。ユーザーとデバイスの承認基準を組み合わせることで、アクセスを許可または制限するためのきめ細かいアクセス規則を作成し、登録済みデバイス上のユーザーからの承認されたアクセスのみを許可されたアプリケーションに認めます。

SDPとIAMの統合は、初期ユーザー認証に使用されるだけでなく、OTPから機密システムへのアクセスを要求するなどのステップアップ認証や、特定の状況下（リモートアクセスとオンプレミスなど）にも使用されます。 IAMシステムは、アカウントの無効化、グループメンバーシップの変更、ユーザーからの接続の切断、ユーザーロールの変更などのIDライフサイクルアクションに応答して、API呼び出しを介してSDPと通信することもできます。

IAMはSDP内でユーザーを認証し、SDPが承認の決定を下すために使用する情報を提供し、登録済みデバイスからユーザーに付与されたすべてのアクセスに対して強化された監査ログを有効にするために使用されます。（ネットワークアクセスではなく）アプリケーションアクセスを（IPアドレスではなく）ユーザーに結び付けると、ログ記録に役立つ接続情報が得られ、セキュリティ上またはコンプライアンス上の理由から過去のアクセスを監査する際のITオーバーヘッドが大幅に削減されます。

IAMツールは通常、IDライフサイクルを維持するビジネスプロセスに重点を置き、リソースへのアクセスを制御するためにID情報を使用する方法を標準化します。たとえば、アクセスのためのユーザーの「プロビジョニング」のメカニズム。通常は手動プロセスと自動プロセスを組み合わせたものです。SDPはIAMによって管理されるID属性とグループメンバーシップに依存するため、SDPはこれらのIAMプロセスをサポートします。ユーザー属性またはグループメンバーシップが変わると、SDPはこれを自動的に検出し、IAMプロセスを変更せずにユーザーアクセスを変更します。

SDPはSAMLと統合します。SDP配備の中では、SAMLプロバイダーはユーザー属性のためのアイデンティティプロバイダーとして、そして/または認証プロバイダーとして（例えばMFAのために）機能するかもしれません。

SAMLに加えて、OAuth、OpenID Connect、W3C Web認証（WebAuthn）などの多くのオープン認証プロトコルがあります。また、FIDOアライアンスのClient-to-Authenticatorプロトコル（CTAP）は、今後のSDP関連の研究で検討される予定です。しかしながら、これらの調査はこの研究文書の範囲には含まれていません。

ネットワークアクセス制御（NAC）ソリューション

ネットワークアクセス制御（NAC）は通常、どのデバイスがネットワークに接続できるかを制御し、どのネットワークサブジェクトにアクセスできるかを管理します。これらのソリューションは、ネットワークへのアクセスを許可する前に、標準的なハードウェア（802.1X）とソフトウェアを使用してデバイスを検証するのが最も一般的で、OSI モデルのレイヤ2で動作します。

デバイスが最初にネットワークに表示されたときに、NACはデバイス検証を実行してから、デバイスをネットワークセグメント（VLAN）に割り当てます。実際には、NACは少数のネットワークにデバイスを非常に大まかに割り当てるために使用されます。ほとんどの組織には、Guest、Employee、Productionなどの少数のネットワークしかありません。NACはネットワークのレイヤ2で動作するため、特定のネットワーク機器を必要とし、クラウド環境では動作せず、リモートユーザーが使用することはできません。

SDPは、デバイスアクセスと組み合わせてユーザーを統合するためのNACに対する最新のソリューションです。ただし、NACの使用に意味がある環境には、プリンタ/コピー機、ハードフォン、防犯カメラなどのハードウェアデバイスがあります。これらのデバイスには802.1Xサポートが組み込まれていることが多く、通常はSDPクライアントのインストールをサポートしていません。これらのデバイスを保護し、それらへのユーザーアクセスを制御するためのゲートウェイ間モデルは、より優れた選択肢であり、今後のSDP調査のトピックとなります。

エンドポイント管理（EMM/MDM/UEM）

多くの企業では、エンタープライズモビリティ管理（EMM）、モバイルデバイス管理（MDM）、または統合エンドポイント管理(UEM)として分類されることが多いエンドポイント管理システムを利用しています。これらはエンタープライズITとセキュリティの重要な要素であり、それらの価値と重要性はSDPの配備によって強化されます。

まず、これらの管理システムを使用して、ユーザーデバイス間でのSDPクライアントの配布とインストールを自動化できます。これらのシステムはSDPと同じIAMシステムを使用することが多いため、これらの配備はユーザーエクスペリエンスを簡素化するために密接に調整することができます。そして第二に、これらの管理システムはしばしばデバイスの内観とプロファイル評価に関して機能的に豊富な機能を提供します。SDPは、特定のユーザーデバイスに関する情報を取得するためにデバイス管理プラットフォームにAPI呼び出しを行い、この情報に基づいて動的なアクセス決定を行うことができます。一般に、SDPはエンドポイント管理システムの価値と到達範囲を高めることができます。

あるいは、エンドポイント管理システムを持たない組織は、SDPによって提供されるデバイスの管理と制御を利用できます。

Webアプリケーションファイアウォール（WAF）

Webアプリケーションファイアウォール（WAF）は、Webアプリケーションとの間のWeb（HTTP（S））トラフィックをフィルタリング、監視、およびブロックするように設計されています。WAFは、SQLインジェクション、クロスサイトスクリプティング（XSS）、ファイルインクルード、セキュリティの誤設定など、Webアプリケーションのセキュリティ上の欠陥による攻撃を防ぐために、アプリケーションプロトコルトラフィックを分析します。**WAFはネットワークアクセス制御やネットワークセキュリティソリューションではありません。**

通常、IDS / IPSのようにユーザーとアプリケーションの間でネットワーク内でインラインで動作しています。一般に、これらは悪意のあるコンテンツを検出してブロックするためにHTTP（S）プロトコルトラフィックを調べるためだけに設計されています。WAFはSDPを補完するものです。たとえば、クライアント→ゲートウェイモデルでは、WAFはSDPゲートウェイの背後に配備され、SDP mTLSトンネルから抽出された後、ネイティブWebアプリケーショントラフィックを処理します。クライアント→サーバーモデルまたはサーバー→サーバーモデルでは、HTTP（S）トラフィック検査をより分散的に制御するために、WAFがサーバー上のSDPゲートウェイと統合されています。このトピックに関する今後の研究が計画されています。

ロードバランサ

ロードバランサは、多くの企業のネットワークおよびアプリケーションアーキテクチャの一部であるため、SDP配備において検討する必要があります。DNSやネットワークベースのソリューションを含むさまざまな種類のロードバランサがあり、設計者は、組織がそれらをどのように利用しているか、およびSDP配備が及ぼす可能性のある影響について明確に理解する必要があります。

例えば、ネットワークベースのロードバランサは通常、クライアントとサーバーの間のネットワーク上にインラインで配備され、上述のWAFの説明と同様に、SDPコンポーネント間のmTLS接続を検査できない場合があります。SDP配備とロードバランサのアプローチの詳細は、最大限の利益を得るためにSDPを配備できることを保証するために慎重な分析を必要とします。このトピックに関する将来のSDP研究が計画されています。

Cloud Access Security Brokers (CASB)

CASBはクラウドサービスユーザーとクラウドアプリケーションの間に位置し、セキュリティポリシーの実施を含むすべてのアクティビティを監視します。CASBは、ユーザーの行動の監視、潜在的に危険な行動に関する管理者への警告、セキュリティポリシーの遵守の実施、マルウェアの自動防止など、さまざまなサービスを提供できます。CASBは、ユーザーとクラウドサービスの間にインラインで配備するか、ベンダーによる実装とSaaSプラットフォーム内のAPIサポートのレベルに応じて、SaaS APIを利用してSaaSシステムの「内部」に配備することができます。

CASBの機能は通常SDPの機能と重複しませんが、SDPを使用することで、データ保護やユーザーの行動分析のためにアプリケーショントラフィックを内観するレイヤ7（アプリケーション層）で動作するため、操作が簡単になります。CASBは、一般的にネットワークセキュリティやアクセス制御機能を提供していないので、SDPを含めることでそれらの製品を強化することができます。詳細についてはSDPとSaaSに関する次のセクションを参照してください。

Infrastructure as a Service (IaaS)

IaaSのセキュリティは、責任共有モデルに基づいて構築されます。そこでは、クラウドプロバイダは一定の責任（クラウドのセキュリティ）を持ち、利用者はアプリケーションのセキュリティ（クラウド内のセキュリティ）に対して責任があります。IaaSの利用者は、ネットワークセキュリティグループを利用して、クラウドリソースへのアクセスを制御します。これらのネットワークセキュリティグループは、基本的なファイアウォールを構成し動作します。このように、ネットワークセキュリティグループはSDPによって効果的に利用することができます。
追加情報については、”SDP for IaaS research document”を参照してください。

Software as a Service (SaaS)

Salesforce.comやOffice 365などのSaaSアプリケーションは、マルチテナントであり、インターネット上で一般公開されています。したがって、権限のないユーザーによるネットワークレベルのアクセスを防止することは、現時点では難しいです。代わりに、組織は以下の理由でSaaSアプリケーションでSDPを使用することができます：

- 許可されたデバイス上の許可されたユーザーのみが、その特定の組織のテナントがSaaSにアクセスできるようにします。
- 管理対象の企業IAM認証情報が、SaaSアプリケーションへの認証に使用されるようにします。
- SaaSアプリケーションにアクセスするための多要素認証を実施します。
- SaaSアプリケーションへのすべてのユーザーアクセスがログに記録され追跡されるようにします。

増え続けるSaaSプロバイダーは、自社の利用者がこれらの利点を望んでいることを認識しており、これをサポートするための「ソースIPアドレスとデバイス制限」機能を追加しています。

この機能は、SDPまたは従来のVPNのどちらでも同じように機能し、SaaSの利用者が自分のドメイン（テナント）に対するユーザーアクセス（ログインと使用）を制限できるため、その利用者のテナントに対するすべてのアクセスは特定のIPアドレスから開始されます。SDPでは、そのソースIPは、ユーザートラフィックがルーティングされ、不正な接続が拒否されるシステム（SDPゲートウェイなど）の要素になります。

Platform as a Service (PaaS)

Platform-as-a-Serviceによって、企業は標準的なハードウェアやIaaSベースのシステムよりも少ないオーバーヘッドで、カスタムアプリケーションを構築および配備できます。IaaSおよびSaaS（どちらも上記）とは異なり、PaaSシステムへのネットワークアクセス制御（したがってSDPの関連する度合）は、提供される機能の種類、およびPaaSプロバイダが外部アクセス制御を有効にした方法によって異なります。

ただし、主要なPaaSプロバイダーは、IaaSと同じネットワークセキュリティモデルをPaaSプラットフォームに対してもサポートしています。たとえば、Microsoft Azure PaaSセキュリティモデル、Google Cloud Platform App EngineやAWS Elastic Beanstalkと同様に、Azureネットワークセキュリティグループによるソースアドレスの制限をサポートしています。PaaSアプリケーションがどのようなものであり、どの接続を保護するのが最善かに応じて、さまざまなSDPモデルを配備できます。

ガバナンス、リスク、およびコンプライアンス（GRC）

ガバナンス、リスク、コンプライアンスの原理は、企業全体の企業セキュリティフレームワークの一部であることが多く[36]「組織が確実に目的を達成し、不確実性に対処し、誠実に行動することを保証するのに役立ちます」。GRCシステムは、ITを含む多くの組織システムの周りで統制を定義し実施するのを助け、通常は標準やガイドライン（例：SOX、PCIなど）の順守を確実にします。

SDPは、GRCに必要なアクセス制御を実施および文書化することによって、GRCシステムと対話してGRCシステムをサポートできます。たとえば、GRCシステムでは、本番システムを非本番システムから分離し、稼働システムへのすべてのユーザーアクセスをログに記録することが必要になる場合があります。SDPはこのネットワークセグメンテーションを実施し、GRCシステムに監査ログを提供してこの制御が適切に機能していることを検証できます。このトピックに関するさらなる研究が計画されています。

Public Key Infrastructure (PKI)

公開鍵基盤（PKI）は、デジタル証明書を作成、管理、配布、使用、保存、失効させ、暗号化、復号化、ハッシュ、署名に使用される秘密鍵と公開鍵を管理するために必要なロール、ポリシー、手順のセットです。SDPは、TLS証明書の生成と安全な接続のためにPKIを使うこともできます。PKIインフラストラクチャが存在しない場合、SDPは安全な接続に使用するためのTLS証明書を提供できます。

既存のPKIは、SDP証明書の生成およびオプションでユーザー認証に使用できるため、SDPに自然に統合が可能です。

Software-Defined Networking (SDN)

SDNは、ITネットワークインフラストラクチャのAPI駆動型オーケストレーションであり、ITネットワーク内のネットワークルーティングのオーケストレーションを可能にするために使用されます。ネットワーク管理を容易にし、ネットワークのパフォーマンスと監視を改善するためにプログラム的で効率的なネットワーク構成を可能にします。SDNはネットワークトラフィックの効率的なフローに焦点を当てており、現在は、認証または認可を含む接続のセキュリティには対応していません。適切に運用されているSDNシステムは、信頼性が高く効率的で適応性のあるネットワーク帯域幅の提供を企業に提供します。

SDPは、基盤となるネットワークインフラストラクチャに関係なく、ネットワーク上のオブジェクト間の接続のオーケストレーションを提供します。SDPは、SDNの配備による恩恵を受けるように統合できますが、必須ではありません。たとえば、SDPとSDNコントローラの統合や、SDNが不透明で暗号化されたmTLS接続にネットワークQoSを提供する機能など、いくつかの興味深い統合ポイントがあります。この分野におけるさらなる研究が計画されています。

サーバーレスコンピューティングモデル

コンピューティングモデルが進化するにつれて、セキュリティツールとアーキテクチャもそれらと共に進化する必要があります。そのような進化の1つは、いわゆる「サーバーレス」コンピューティングモデルです[41]。ここでは、クラウドプロバイダは、カスタムコード（“function as a service”モデル）、または事前に構築されたコードセット（「サーバーレスデータベース」など）のいずれかを実行する機能を提供します。

“function as a service”モデルは、インターネット全体に共通のパブリックエンドポイントを公開し、認証と認可を制御するためにAPIキーを使用することがあります。

この場合、これらのやり取りは公開されるように設計されているため、SDPモデルは適用されません。

ただし、他のサービス（または他のクラウドプロバイダ）は、各利用者が“as a service”機能用の独自の専用アクセスポイントを持つという異なるセキュリティモデルを選択する場合があります。このモデルでは、SDPはこれらの接続を制御するために使用されるSDPゲートウェイによって保護されたプライベートアクセスポイントに適用できます。

アーキテクチャ上の考慮事項

ネットワークアクセスシナリオを十分広くカバーしていますが、SDPはすべてのセキュリティ問題を解決することを意図していません。一部の除外領域として以下があります:

- パブリックネットワークサービス（認証を必要としないウエブサイトなど）へのアクセスを保護または制御 - SDPはメンバーシップを基本としたサービスに、より適しています
- エンドポイントプロテクション
- サーバレスコンピューティングのような特定のコンピューティングモデル
- SDP配備モデルに応じた、ピアツーピアなどの特定のネットワーク接続トポロジ（ページ19、SDP配備モデルと関連シナリオを参照）

結論

情報セキュリティは今日の企業や政府機関にとって重大な課題であり、組織のデータ資産を保護するためにより効果的なアプローチを採用する必要があります。Software Defined Perimeterアプローチは、堅牢な開発、運用、セキュリティのために、組織が強力で適応性があり管理しやすい基盤を提供する方法を根本的に最新にすることができます。この文書は、セキュリティの専門家に、SDPアーキテクチャがどのように機能するのか、またどのように組織に効果的に配備できるのかについてのより深い理解を提供します。

しかしながら、私たちの仕事はまだ終わっていません。

今後の調査で取り上げるトピックは、SDP配備モデルやここに掲載されている統合ごとの詳細な論文、SDPのビジネス上の利点、SDP配備に基づくコンプライアンスコントロールマッピングなど、いろいろあります。最も重要なこととして、私たちはすべての答えを持っているわけではありません！私たちはあなたが私たちのワーキンググループに参加し、会話に参加し、そして貢献していただくことを勧めます。

最も重要なことは、私たちはすべての答えを持っていないことを認識していることです！SDPワーキンググループに参加して、会話に参加し、貢献してください。安全でオープンで利用可能なインターネットをサポートするセキュリティ専門家として、また倫理的に動機付けられた人間として、私たちはより良い未来を確保するために懸命に働いています。活動に。ご参加いただけることを期待します。詳細については、**https://cloudsecurityalliance.org/working-groups/software-defined-perimeter/**. を参照してください。

Appendix 1
補足資料

“Software-Defined Perimeter Working Group: SDP Specification 1.0,” by Brent Bilger, Alan Boehme, Bob Flores, Zvi Guterman, Mark Hoover, Michaela Iorga, Junaid Islam, Marc Kolenko, Juanita Koilpilla, Gabor Lengyel, Gram Ludlow, Ted Schroeder, and Jeff Schweitzer (CSA, April 2014).
SDP v1.0 Spec

“Software-Defined Perimeter for Infrastructure as a Service,” by Jason Garbis and Puneet Thapliyal (CSA, 2016).
SDP for IaaS

“Software-Defined Perimeter Working Group Glossary,” Cloud Security Alliance (CSA, 2018).
SDP Glossary

“Zero Trust Networks: Building Secure Systems in Untrusted Networks,” by Evan Gilman and Doug Barth (June 2017).
http://shop.oreilly.com/product/0636920052265.do

“fwknop: Single Packet Authorization > Port Knocking,” by Michael Rash (CipherDyne).
http://www.cipherdyne.org/fwknop/

“Open Source Software-Defined Perimeter,” Waverley Labs.
http://www.waverleylabs.com/open-source-sdp/

Appendix 2

SPAの詳細

SDP 1.0仕様で定義されているSPAパケットのフォーマットは次のとおりです。

CIPHERTEXT	Nonce	Prevents servicing outdated SPA packets
	Timestamp	**Most common: Service Access Request**
	Message Type	**Possibly deprecated: access request, NAT access request,** gateway command message
	Message String	Source IP address to allow, service ID(s) to open
	Optional Fields	**NOTE: Gateway knows which port to open as well as whether and where to forward the connection.**
	Digest	**NOTE: Might be used to request tunneling of service traffic.**
CLEARTEXT	HMAC	**Before encryption, this SHA256 hash is calculated over the ciphertext portion of the message and then used by the server to verify message integrity after a successful** message decrypt.

上記に対する改善案として、平文のクライアントIDを追加することが考えられます。これにより、着信パケットをより効率的に処理できます。RFC文書と同様にバイナリSPAフォーマットを設計するための取り組みが始められました。

SPAは、単一のUDPパケットとして送信された場合に最も効果的です。一部の使用例では、ネットワーク環境が一部またはすべての発信UDPパケットをブロックする可能性があるため、実用的ではありません。このような場合、SPAパケットはTCP接続を介して送信できます。これは技術的にSPAの「シングルパケット」の性質に反しますが、実際的な考慮事項として必要な場合があります。

SPAパケットは接続しているマシンから送信できますが、別のシナリオではパケットが別のデバイスから送信されます。この使用例は、デスクトップコンピュータの代わりにモバイルデバイスを使用してSPAパケットを送信する場合です。他のシナリオでは、UDPパケットをブロックする環境のための合理的な回避策になります。