Infrastructure as a Serviceのための Software Defined Perimeter

Presented by the SDP Working Group

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

The permanent and official location for *Cloud Security Alliance Sokware Defined Perimeter Working Group* is **https://cloudsecurityalliance.org/group/sohware-defined-perimeter/**.

© 2016 Cloud Security Alliance – All Rights Reserved All rights reserved.

You may download, store, display on your computer, view, print, and link to International Standardization Council Policies & Procedures Security at https://cloudsecurityalliance.org/download/international-standardization-council-policies-procedures, subject to the following: (a) the Report may be used solely for your personal, informational, non-commercial use; (b) the Report may not be modified or altered in any way; (c) the Report may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to International Standardization Council Policies & Procedures.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ACKNOWLEDGEMENTS

We'd like to offer our sincere thanks to all the people who have collaborated and helped us create this document. Your input, feedback, and different perspectives have made this document better and more meaningful than we could have done on our own.

Thank you!

Lead Authors:
Jason Garbis
Puneet Thapliyal

SDP Co-Chairs:
Bob Flores
Junaid Islam

Editor:
John Yeoh

Peer Reviewers:
Brent Bilger
Vince Campitelli
Matthew Carter
Aradhna Chetal
Gerald Greer
Kevin Fletcher
Jeff Huegel
Scott Kennedy
Juanita Koilpillai
Dan Logan
Nya Murray
Elamurian R
Vijay Rangayyan
John Reel
Reza Reza
Colin Robbins
Puneet Thapliyal
Yoshio Turner
Flavio Villanustre
Manish Yadav
Erkki Yli-Juuti
Xing Zhang

Design:
Stephen Lumpe (cover art)
Kendall Scoboria

© Copyright 2017, Cloud Security Alliance. All rights reserved.

日本語版提供に際しての告知及び注意事項

本書「Infrastructure as a Service のための Software Defined Perimeter」は、Cloud Security Alliance (CSA)が公開している「Software Defined Perimeter for Infrastructure as a Service」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 06 月 24 日	日本語版 1.0	初版発行

本翻訳の著作権は CSA ジャパンに帰属します。引用に際しては、出典を明記してください。無断転載を禁止します。転載および商用利用に際しては、事前に CSA ジャパンにご相談ください。
本翻訳の原著作物の著作権は、CSA または執筆者に帰属します。CSA ジャパンはこれら権利者を代理しません。原著作物における著作権表示と、利用に関する許容・制限事項の日本語訳は、前ページに記したとおりです。なお、本日本語訳は参考用であり、転載等の利用に際しては、原文の記載をご確認下さい。

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。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

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。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

日本語版作成に際しての謝辞

「Infrastructure as a Service のための Software Defined Perimeter」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
諸角　昌宏
矢部　沖比古

© Copyright 2017, Cloud Security Alliance. All rights reserved.

目次

ゴール 5
アプローチと範囲 6
エグゼクティブサマリー 7
SDPとCSA Treacherous 12（危険な12の落とし穴） 8
導入：IaaSセキュリティの概要 10
技術的基盤 11
IaaS参照アーキテクチャ 11
なぜIaaSのセキュリティが異なるのか？ 12
場所は属性の一つ 12
常に変化し続ける 12
IPアドレスに関わる難題 13
セキュリティ要件と従来のセキュリティツール 14
踏み台サーバー：飛びつく前に検討を 16
なぜVPNではなくSDPなのか? 16
仮想デスクトップインフラストラクチャ（VDI） 18
Software-Defined Perimeterではどのようにこれらの問題を解決するか 18
Software-Defined Perimeter とは？ 19
IPアドレスだけでなくユーザーに基づいたポリシー 20
SDPの利点 20
運用効率 20
コンプライアンスの簡素化 20
コストの削減 20
変化のきっかけとしてのSDP 21
SDPとID/アクセス管理 21
IAASユースケース 22
ユースケース：IaaS環境における開発者の安全なアクセス 22
SDPなしのアクセス 22
SDPありのアクセス 22
比較 24
まとめ 26
ユースケース：ビジネスユーザーによる社内アプリケーションへのアクセス 26
SDPなしのアクセス 26
SDPありのアクセス 27
まとめ 30
ユースケース：管理者によるインターネット公開サービスへのアクセス 31
ユースケース：新しいサーバーインスタンスが作成されたときのユーザーアクセスの更新 33
まとめ 35
ユースケース：サービスプロバイダーのハードウェア管理プレーンアクセス 37
まとめ 38
ユースケース：複数のエンタープライズアカウントにわたるアクセスの制御 39
まとめ 40
SDP仕様の強化に関する推奨事項 41
ハイブリッドおよびマルチクラウド環境 42

© Copyright 2017, Cloud Security Alliance. All rights reserved.

サイドバー: 代替のコンピュートモデルとSDP 43
サイドバー: コンテナとSDP.....44
結論と次のステップ 45

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ゴール

Software-Defined Perimeter（SDP）アーキテクチャの認知度と採用が急速に拡大しており[1]、その有効性が多くの企業とユースケースによって実証されています。組織が戦略的にInfrastructure as a Service（IaaS）を採用していく速さと、クラウドリソースへのアクセスを保護する差し迫った必要性を考慮すると、これらのリソースを守るためにSDPの利用を推進するべき時です。

この文書は、Software-Defined Perimeter（SDP）アーキテクチャを Infrastructure-as-a-Service 環境に適用する場合に、セキュリティ、コンプライアンス、および運用効率がどのように改善されるかを調査し、説明することを目的とします。読者は、IaaS のエンタープライズユーザーが直面するセキュリティの課題を明確に理解し（責任共有モデルを前提とします）、IaaS が提供するアクセス制御と従来のネットワークセキュリティツールの組み合わせによって生じる問題を理解し、様々なユースケースにおいて Software-Defined Perimeter がこれらの問題をどのように解決するかを学ぶことができます。この文書は様々な読者を対象とします。主に IaaS の顧客である組織を対象としますが、IaaS を提供するサービスプロバイダーにも関連します。サービスプロバイダーには、商用サービスプロバイダーの他、プライベート IaaS や共通サービス環境を提供する組織内の IT チームを含みます。

この活動は、IaaSに関連するセキュリティの課題を詳細に調査し、SDPがこれらの問題をどのように解決するかを示すために行っています。

1 Gartner predicts that by end 2017, enterprises using SDP to protect network services will increase from 1% to 10%, and by 2021, 60% of enterprises will have replaced VPNs with SDP solutions. (Gartner, It's Time to Isolate Your Services From the Internet Cesspool, 30 September 2016). Markets And Markets predicts a CAGR of 34% over the next 5 years (http://www.marketsandmarkets.com/PressReleases/software-defined-perimeter.asp). Other analysts such as ESG predict growth as well: http://www.networkworld.com/article/3141930/security/goodbye-nac-hello-software-defined-perimeter-sdp.html

© Copyright 2017, Cloud Security Alliance. All rights reserved.

アプローチと範囲

- この文書では、Amazon Web Services、Microsoft Azure、Google Compute Engine、Rackspace Public CloudなどのパブリッククラウドIaaSで使われる用語を主に使用します。ただし、ユースケースとアプローチは、VMwareやOpenStackなどを使ったオンプレミスのIaaSにも同じように適用できます。
- SDPの仕様を商用に実装しているベンダーは、完全な製品を提供するため、SDP v1の仕様の範囲以外のことにも対応しています。このような実装には、様々なアーキテクチャ、アプローチ、機能があります。この文書では、ベンダー中立であり、かつベンダー固有機能の説明を避けるようにしています。ベンダー間で機能に差がある場合は、*may*（場合がある）、*typically*（通常）、*often*（多くの場合）といった表現を使って、読みやすさを犠牲にすることなく、これらの違いを説明します。
- 現在、ほとんどのパブリックIaaSプロバイダーがIPv4のみをサポートしているため、ここではIPv4の機能や制限による影響や制約を前提として説明します。IPv6の採用による内容の変更は、この文書の今後の改訂で対応する予定です。
- SDPの仕様に沿って、ユーザー→サービスのアクセス制御通信（North-South）に焦点を当てます。サーバー→サーバーの通信（East-Westとも呼ばれます）はこの文書の範囲外とし、SDPの仕様とこの文書の今後の改訂において、市場での採用動向を反映しながら対応する予定です。[2] サーバー→サーバーモデルは、SDP v1の仕様で言及したサポート対象のモデルですが、ユーザー→サービスモデルほど採用が進んでいません。
- 高可用性と負荷分散に関する考慮事項の説明は、この文書の範囲外です。
- SDPポリシーモデルの説明は、この文書の範囲外です。
- ここで説明するSDPのユースケースとアプローチは、ネットワークアクセス制御のサポート状況や管理方法によっては、Platform-as-a-Serviceに適用できる場合があります。[3]

この文書を作成する間、「スコープが肥大化」しないように留意しました。検討し得る多くのトピックについて議論しましたが、最終的にそれらをv2の仕様に含める、もしくは関連のないものとして整理しました。私達が重要と考え、かつIaaSにより広く適用されるトピックについては、セクション「SDP仕様の強化に関する推奨事項」を参照してください。

いくつかのトピックを先送りしましたが、それでも目標のページ数を超えており、このような長文を純粋に楽しんでいただけると幸いです。そんな冗談はさておき、長さとスコープのバランスには、適切な判断をしたと信じています。お気づきの点があればご連絡ください。次の改訂を一緒に手伝っていただくことも歓迎します！

2 Note that in IaaS environments, it's actually in some ways easier to control E-W traffic compared to on-premises environments, since IaaS network security groups default to denying cross-server traffic, which has to be explicitly enabled.
3 For example, if the PaaS system supports source IP address restrictions, it can be configured to only accept traffic from the SDP Gateway, allowing SDP policies to control user access.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

エグゼクティブサマリー

ITやセキュリティのリーダーは、クラウドにおけるInfrastructure-as-a-Service（IaaS）では、企業とクラウドプロバイダーがセキュリティに対する責任を共有し、またユーザーアクセスやセキュリティに関する要件が従来のオンプレミスシステムとは異なる（ある意味でより困難な）ことを理解しています。しかし、従来のセキュリティツールとIaaSベンダーが提供するセキュリティ機能では、これらの要件を完全に充たすことができません。

例えば、組織はネットワーク上のリソースに対してユーザーアクセスを制限する必要がありますが、従来のネットワークアクセス制御（NAC）や仮想LAN（VLAN）といったソリューションは、マルチテナントかつ仮想化されたネットワークインフラストラクチャに基づくIaaS環境で使用することができません。別の例を挙げると、IaaS環境はすべてのユーザーに対してクラウドリソースへの「リモートアクセス」を要求しますが、従来のVPNは、最近のモバイルを使った働き方、組織間の共同作業、動的なクラウド環境などにあまり向いていません。IaaSのセキュリティ機能がこれらの一部に対応していますが、（皮肉なことに）ネットワークアクセス制御には、IPアドレスとポートによるアクセス管理を中心とする、非常に伝統的なネットワークファイアウォールの視点で提供しています。アイデンティティを中心に据えたセキュリティやアクセスモデルが増える中で、多くの組織がこのような機能の扱い方に苦労しています。

Software-Defined Perimeter（SDP）を使うことにより、ビジネスユーザーやITの生産性を妨げることなく、組織はIaaSリソースへのユーザーアクセスを安全に提供できます。実際、SDPを適切に展開すると、オンプレミスとクラウドを横断する企業全体のネットワークセキュリティを変革するきっかけになります。組織がSDPを使用すると、インフラストラクチャ全体（オンプレミスおよびクラウド）とすべてのユーザーを対象として、集中型かつポリシー主導のネットワークセキュリティプラットフォームを実現することができます。これは説得力のあるビジョンですが、SDPで現実的に実現可能なビジョンです。世界中の多くの組織がSDPを使用して、セキュリティに対する姿勢を高め、攻撃面の領域を減らし、ビジネスやITスタッフの生産性を高め、コンプライアンスにかかる負担を減らし、その一方でコストを削減しています。

この調査文書は、SDPをInfrastructure-as-a-Service環境に適用する方法に焦点を当て、以下のユースケースを扱います。

- 開発者によるIaaS環境への安全なアクセス
- ビジネスユーザーによる社内アプリケーションサービスへの安全なアクセス
- 管理者によるインターネット公開したサービスへの安全なアクセス
- 新しくサーバーインスタンスを作成した際のユーザーアクセスの更新
- サービスプロバイダーによるハードウェア管理プレーンへのアクセス
- 複数のエンタープライズアカウントを使ったアクセス制御

さらに、この調査では、ネットワークセキュリティへの従来のアプローチがIaaS環境に対して効果的でも効率的でもない理由を説明します。最後に、ハイブリッド環境でSDPがどのように役立つかを見ていきます。実際、従来のオンプレミス環境や仮想化環境でもSDPが非常に効果的に導入されています。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

SDPとCSA Treacherous 12（危険な12の落とし穴）

Cloud Security Allianceでは、クラウド導入戦略の中で知識に裏付けられたリスク管理の判断が行えるように、重要な脅威や懸念事項をリストにして公開しています。このレポートは、クラウドにおける最も重大なセキュリティ課題について、CSAコミュニティのセキュリティ専門家による最新の見解を反映しています。SDPは、この重大脅威レポートに記載された脅威、リスク、および脆弱性の多くを軽減または排除することにより、攻撃面となる領域を減らします。その結果、組織はリソースを他の領域に集中させることができます。

下表は、レポートに記載された12の重大脅威を示し、SDPがそれらに与える効果を分析します。

	脅威	SDPによる効果
1	データ侵害	SDPは、事前認証および事前認可の層を追加することにより、インターネットに公開したホストへの攻撃面を削減します。サーバーやネットワークにおける「最小権限アクセス」モデルを保証し、データ侵害に繋がる多くの攻撃ベクターを減らします。 残存リスク：フィッシング、設定不備、端末への脅威など、データ侵害に繋がるいくつかの攻撃ベクターは、SDPでは対応することができません。正規ユーザーによる認可されたリソースへの不正アクセスは、SDPでは直接防ぐことができません。
2	ID、認証情報、アクセス管理の不備	従来、VPNアクセスの認証情報が窃取されると、多くの組織でデータ侵害に繋がりました。一般的に、VPNはユーザーに対してネットワーク全体への幅広いアクセスを許可するため、認証情報の管理不備の中でも最も失敗しやすい弱点の一つでした。 これとは対照的に、SDPは幅広いネットワークアクセスを許可せず、明示的に許可されたホストへのアクセスのみに制限します。そのため、認証情報が窃取された場合でも、侵害の影響範囲が限定されます。その結果、ID、認証情報、アクセス管理の不備に対して、遥かにレジリエンスの優れたセキュリティアーキテクチャを実現することができます。SDPは、ユーザーがリソースにアクセスする前に、強力な認証を要求することもできます。 残存リスク：組織は、Joiner-Mover-Leaver（新規採用、異動、退職など）に対応した信頼できるIAMプロセスを用意し、アクセスポリシーが適切に定義されていることを確認する必要があります。アクセスポリシーが広すぎると、リスクが発生します。
3	インターフェースとAPIのセキュリティ欠陥	無認可のユーザーからユーザーインターフェースを保護することは、SDPの主要な機能です。SDPを使うことにより、無認可のユーザー（すなわち、攻撃者）はユーザーインターフェースにアクセスすることができず、脆弱性を悪用することができません。 ユーザーのデバイスで実行されているプロセスから呼び出される場合であれば、SDPがAPIを保護することができます。今のところSDPは、主にユーザー→サーバーのアクセスを保護するため導入されています。 サーバー→サーバーのアクセスは、これまでのところSDPの対象として認知されていませんが、近い将来、SDPの範囲に含まれてくることを予想しています。 残存リスク：サーバー→サーバーのAPI実行が、現時点では一般的なSDPのユースケースではないため、APIサービスがSDPシステムによって保護されない場合があります。
4	システムの脆弱性	SDPは、システムやアプリケーションの脆弱性を不正ユーザーから隠すことによって、攻撃面となる領域を大幅に減らします。 残存リスク：正規ユーザーは認可されたリソースにアクセスできますが、これらのリソースに対して攻撃を行う可能性があります。SIEMやIDSなど、他のセキュリティシステムを使って、リソースへのアクセスやネットワーク内の行動を監視する必要があります。（下記「悪意のある内部者」を参照）

© Copyright 2017, Cloud Security Alliance. All rights reserved.

5	アカウントハイジャック	セッションクッキーを悪用したアカウントハイジャックは、SDPによって完全に軽減することができます。アプリケーションサーバーは、事前認証と事前認可を経ておらず、正規のSPA（Single Packet Authorization）パケットを含まない、不正な端末からのリクエストを拒否します。そのため、ハイジャックしたセッションクッキーをリクエストに含めても、SDPゲートウェイを通過することができません。 残存リスク：フィッシングやパスワードの盗難は依然としてリスクですが、SDPは、強力な認証を実施し、地理情報などの属性を使ったアクセス制御ポリシーを設定することによって、これらを軽減することができます。
6	悪意のある内部者	SDPは、被害を発生させる悪意のある内部者の能力を制限します。適切に構成されたSDPシステムは、ユーザーのビジネス機能に必要なリソースのみに限定したアクセスポリシーを設定します。その結果、それ以外のリソースの存在に気付くことがありません。 残存リスク：SDPは、正規ユーザーによる認可されたリソースへの不正アクセスを防ぐことができません。
7	APT攻撃の脅威	APT攻撃は、本質的に高度で多面的であるため、単一のセキュリティで防ぐことができません。 SDPは、攻撃面を減らし、感染端末がネットワーク内を探索する能力を制限し、さらに多要素認証を組織全体に対して強制することにより、APT攻撃が発生する可能性と組織内での広がりを抑えることができます。 残存リスク：APT攻撃の防御と検知には、多層防御を行うため、複数のセキュリティシステムとプロセスを組み合わせる必要があります。
8	データの喪失	SDPは、最小権限の原則を適用し、不正ユーザーからネットワーク上のリソースを隠すことにより、データ喪失を起こりにくくします。SDPの他、適切なDLPソリューションを併用する必要があります。 残存リスク：SDPは、正規ユーザーによる認可されたリソースへの不正アクセスを防ぐことができません。
9	不十分なデューディリジェンス	SDPには関係しません。
10	クラウドサービスの悪用・乱用・不正利用	SDPには直接関係しません。クラウドサービスの使用を検知して通知する機能を、SDPのベンダー製品が持っている場合があります。
11	サービス妨害攻撃	SDPアーキテクチャのSingle Packet Authorization（SPA）スキームは、DoS攻撃を阻止することにより、SDPコントローラとSDPゲートウェイをよりレジリエンスのあるものにします。SPAの処理に必要なリソースは、通常のTCPハンドシェイクより大幅に少ないため、一方的に送り付けられるパケットをサーバーが大量に処理して破棄することを可能にします。UDPベースのSPAは、TCPベースのSPAよりさらにサーバーのレジリエンスを向上させます。[4] 残存リスク：SPAは、無効なSPAパケットの処理に必要なCPUの負荷を大幅に減らしていますが、それでもゼロではないため、インターネット公開されたSDPシステムが大規模なDDoS攻撃の影響を受ける可能性があります。
12	共用技術の脆弱性	管理者によるハードウェアや仮想化インフラストラクチャへのアクセスを保護するため、クラウドサービスプロバイダーがSDPを使用することができます。後述する「サービスプロバイダーによるハードウェア管理プレーンへのアクセス」のユースケースを参照してください。 残存リスク：クラウドサービスプロバイダーは、SDPに加えて、様々なセキュリティシステムやプロセスを併用する必要があります。

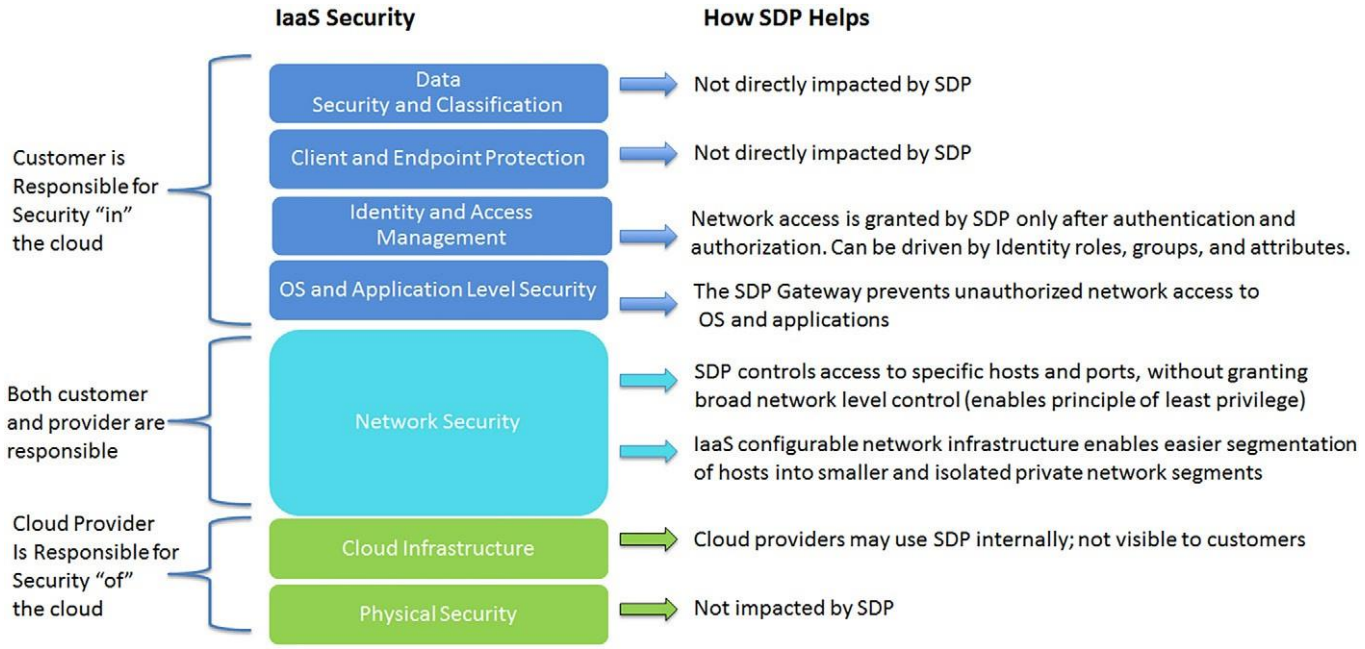
4 The anti-DDoS SDP group has some interesting research on this topic, and some in-progress performance metrics showing server load with traditional TCP connections vs. SPA. Note that UDP-based SPA is even more resilient than TCP-based SPA, as it consumes even fewer server resources, and would better withstand an invalid packet flood attack.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

導入：IaaSセキュリティの概要

クラウド内のアプリケーションのセキュリティについて、この業界には恐らく多くの誤解があります。クラウドを使ったアプリケーションと環境は、適切に展開されていれば、オンプレミスよりも安全にすることができることがよく知られています。課題はもちろん、クラウド環境のセキュリティが、従来のオンプレミスのセキュリティと異なるモデルに基づいていることで、これらの違いによって意図しないところでセキュリティが低下する可能性があります。[5] クラウドに移行するだけで、ワークロードが自動的に安全になるわけではありません。安全にするには、いくつかの考え方と作業が必要です。

一般的に、IaaSベンダーは、IaaSベンダーがクラウドのセキュリティに責任を負い、顧客（企業）自身がクラウド内のセキュリティに責任を負うことを宣言する「責任共有モデル」を作成して普及させてきました。下図は、いくつかの主要なIaaSプロバイダーのコンセプトを組み合わせて作成した、典型的な責任共有モデルです。[6]



クラウドセキュリティにおける責任共有は、特にIaaSプロバイダーが提供する一連のツールの使い方について、まだ多くの組織が理解を試みているところです。後述するIaaSセキュリティの課題でも説明しますが、これらのツールは、ユーザー（もしくはアイデンティティ）より、静的なIPアドレスをベースとする傾向にあります。このアプローチでは、顧客はクラウドリソースへのネットワークアクセスをユーザー単位で効果的に管理することができません。その結果、多くの場合、クラウドネットワーク全体を企業ネットワーク上の誰にでも開放し、アプリケーションまたはインスタンスレベルの認証によって、これらのリソースへのアクセスを保護しています。

これはセキュリティのリスクを伴います。リソースへのネットワークレベルのアクセスさえあれば、認証されていない攻撃者が非常に多くの脆弱性を探索できます。組織は、機密情報を扱う規制対象の環境において、「誰が何にアクセスできるか」を報告しなければならないことが多く、コンプライアンスの問題にもなります。

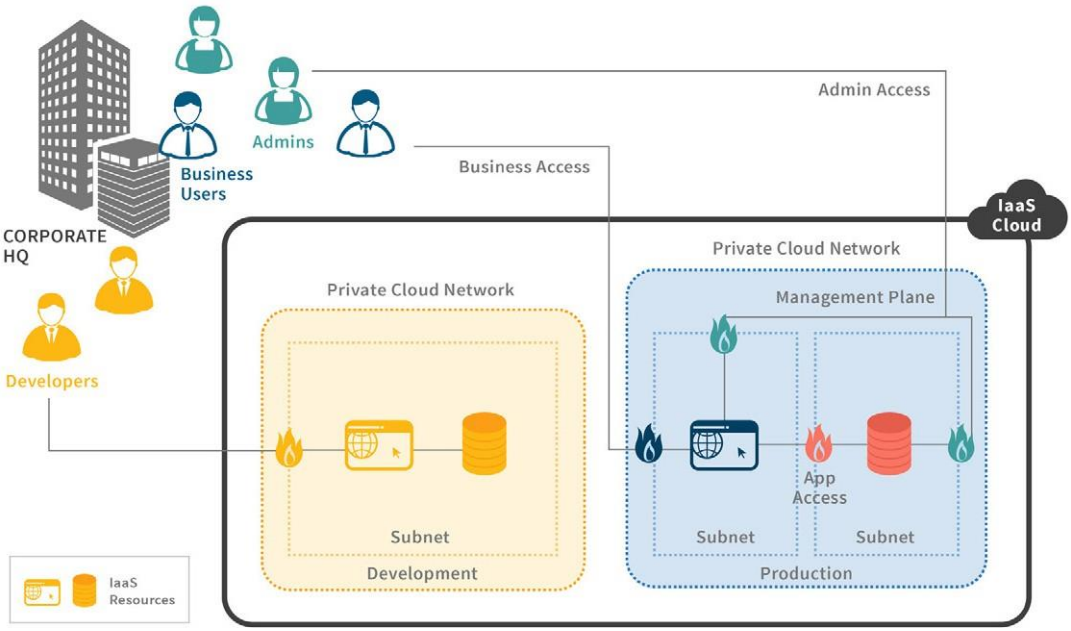
上図に示すように、SDPアーキテクチャは、IaaSベンダーとの責任共有モデルに大きな効果があります。クラウドの利用者は、SDPを使用することにより、共有しているセキュリティコントロールの担当部分を遥かに効果的な方法で実現することができます。

5 For example, the January 2017 ransom attacks on unsecured, publicly-exposed NoSQL databases, most of which were running in IaaS environments, is a good example of this.
6 In particular, these are drawn from the AWS model https://aws.amazon.com/compliance/shared-responsibility-model/ and the Mircosoft Azure model https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

© Copyright 2017, Cloud Security Alliance. All rights reserved.

IaaS参照アーキテクチャ

この文書の読者は、Infrastructure-as-a-Serviceのコンポーネントとアーキテクチャに馴染みがあるものとし、ここでは改めて説明しません。ただし、IaaSの概念をプロバイダー固有の用語ではなく、一般的な用語で説明するため、ここでは用語を定義します。下図は、IaaS環境を簡略化したアーキテクチャ図で、パブリッククラウドとプライベートクラウドのいずれにも当てはまります。



この図では、2つのグループのIaaSリソース（仮想マシン）を、2つのプライベートクラウドネットワークに分割したIaaSクラウド環境を表しています。これらのプライベートクラウドネットワークには、複数のアカウントを使ったり、クラウド環境内の複数のプライベート領域（例えばAWSのVirtual Private Cloud）を使ったりします。ネットワークアクセスの観点から最も重要な点は、これらのプライベートクラウドネットワークがクラウドファイアウォールで保護され、ネットワーク間を往来するアクセスが論理的に制御されていることです。プライベートクラウドネットワークに入っていく（またはプライベートネットワーク間の）ネットワークアクセスの制御はすぐに複雑になりやすく、またクラウドプロバイダー毎に異なるツールを提供しています。IaaSリソースへのユーザーアクセス管理に関する課題に集中するため、この文書では、ルーティングテーブル、ゲートウェイ、NACLなどの構成要素を意図的に省略しています。この文書は、クラウドネットワーク設定の入門書ではないですから！

この単純なモデルにより、プロバイダーに関係なく、クラウドのセキュリティやネットワークについて一貫した説明をすることができます。特に、この調査では次の用語を使用します：

© Copyright 2017, Cloud Security Alliance. All rights reserved.

用語	説明	例
クラウドファイアウォール	クラウド環境を出入りするネットワークトラフィックを制御するセキュリティ機能。サーバーインスタンスをクラウドファイアウォールのグループに割り当てることにより管理します。	AWS: Security Group Azure: Network Security Group
プライベートクラウドネットワーク	クラウド環境内の独立したネットワーク領域で、単一のアカウントに所属する。複数サブネットで構成される場合があり、また単一の組織に所属する多くのユーザーがアクセスする場合があります。	AWS: Virtual Private Cloud Azure: Virtual Network
タグ	IaaSシステムは、名前と値のペアをサーバーインスタンスに割り当てることができます。タグは、IaaSシステム内では意味を持ちませんが、SDPシステムがアクセスポリシーを判断するために利用することができます。	AWS Tags Azure Tags
ダイレクトコネクション	IaaSプロバイダーは、通信プロバイダーと協力して、オンプレミスネットワークからIaaS環境への専用ネットワーク接続を提供します。（多くの場合、MPLSを使用）信頼性や帯域幅の占有などの利点があり、通常、複数のVLANに分割することができます。	AWS Direct Connect Azure Express Route

なぜIaaSのセキュリティが異なるのか？

IaaSのネットワークアクセスには、重要なセキュリティ上の課題があります。ネットワークセキュリティは、クラウドの責任共有モデルの一部であり、間違いなく企業にも責任が発生します。プライベートなクラウドリソースをインターネットに公開することは、通常、許容できる選択肢ではなく、認証のみに依存した保護では、セキュリティやコンプライアンスの要件を明らかに充たせません。組織は、このセキュリティのギャップをネットワークレイヤーで解決する必要があります。

そして、いくつかの理由により、このギャップは複雑なセキュリティの課題を抱えています。

場所は属性の一つ

開発者は、席が隣同士であっても、必要なネットワークアクセスや必要なリソースが開発者毎に異なることがあります。例えば、データベース管理者のSallyは、すべてのプロジェクトに渡って、データベースを実行するすべてのサーバーのポート3306にアクセスする必要があります。Sallyの隣に座っているJoeは、プロジェクトPurpleのアプリケーションコードを管理しており、プロジェクトPurpleのアプリケーションサーバーだけにSSH接続する必要があります。チームと離れた場所で作業するChrisもプロジェクトPurpleのアプリケーション開発者で、数百マイル離れていますが、Joeと同じアクセス権限が必要です。

場所は、アクセスポリシーを構成する一つの属性になることがありますが、従来のコンピューティング環境のように、ネットワークアクセスのレベルを判断する主要な要素ではなくなっています。

常に変化し続ける

これは自明ですが、特にクラウド環境に当てはまります。まず、IaaS環境内のコンピュータリソースは非常に動的であり、サーバーインスタンスは継続的に作成と破棄が繰り返されます。[7] これらのリソースへのアクセスを手動で管理および追跡することは、ほぼ不可能です。また、開発者もまた動的（人格についてでは

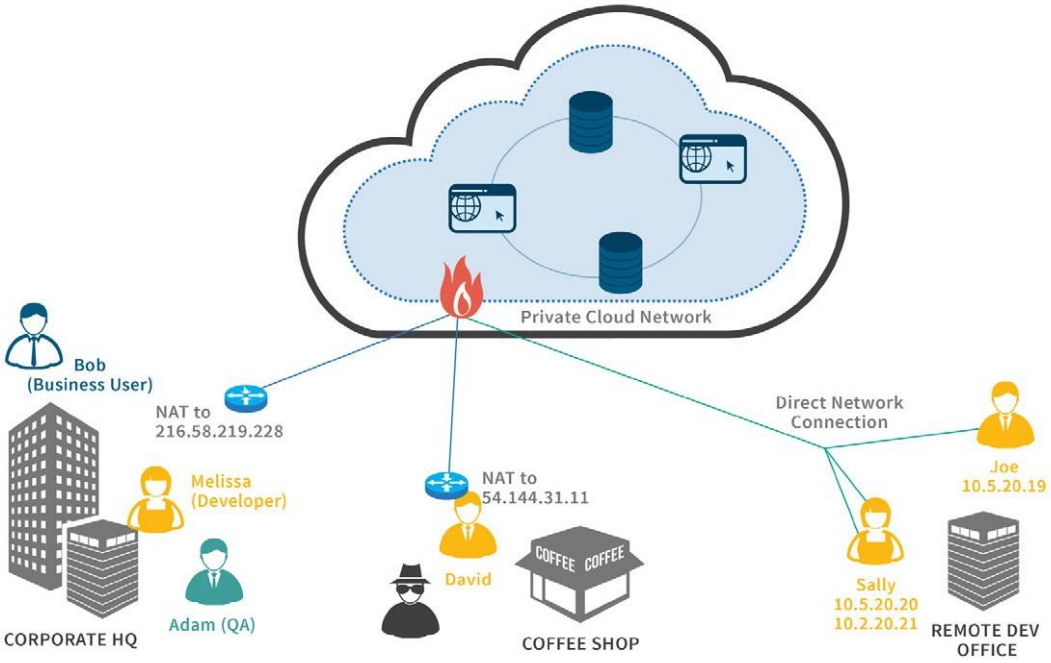
© Copyright 2017, Cloud Security Alliance. All rights reserved.

ありません）で、少なくとも複数プロジェクトで異なる役割を担う可能性があり、場合によってはそれらが同時に進行します。

これはDevOps環境で顕著になり、開発、品質管理、リリース、運用の役割がチーム間で混ざり合い、「本番」リソースへの必要なアクセス要件が急速に変化します。

IPアドレスに関わる難題

伝説的なネットワーク管理者であるシャーロック・ホームズ（CCIE#1）にはふさわしくないかもしれませんが、IPv4の世界には現実の課題があります。ユーザーのIPアドレスは定期的に変更されるだけでなく、ユーザーとIPアドレスの間には1対1の対応がありません。下図は、アクセスルールがIPアドレスのみに依存した場合に、どれだけ単純な環境であっても管理が複雑になることを示しています：



場所	ネットワーク設定	セキュリティへの影響
本社	すべてのユーザーを単一のIPアドレスにマッピングします。この拠点には、幅広いネットワークアクセスが必要なユーザーが多数います。	ネットワークセキュリティグループがユーザーを識別できないため、すべてのユーザーにすべてのリソースへのフルアクセスを許可する必要があります。これは、悪意のあるユーザー、攻撃者、マルウェアなどが、オンプレミスからクラウドネットワークに不自由なく移動できることを意味しています。
リモート開発拠点	ダイレクトコネクションのため、各ユーザーのIPアドレスが保持されます。	IPアドレスは動的に割り当てられ、毎日変更されます。ユーザーは、複数のデバイスを使ってクラウドにアクセスします。 セキュリティグループのルールをIT運用チームが継続的に更新する（ビジネスへの遅れが発生）か、このネットワークをクラウドに完全に開放する（上の行と同様にセキュリティが低下）かのいずれかが必要です。
コーヒーショップ	1人（またはごく少数）のユーザーが様々な場所からリモートアクセスを行い、高い確率でNATが適用されます。	これらの場所からのネットワークアクセスは、同じネットワーク上の悪意のあるユーザーにも繋がります。ネットワークアクセスを手動で調整し、ユーザーの場所やアクセス要件の変化に追従することは困難です。

7 Gartner: G00315586, "It's Time to Isolate Your Services From the Internet Cesspool", 30 September 2016.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

セキュリティ要件と従来のセキュリティツール

本質的に、取り組むべき課題が2つあります：

- 安全なリモートアクセス
- ユーザーアクセスの可視化と制御

一般的に、セキュリティの専門家は、機微なサービスをインターネットに公開するべきではないと考えており、上記の片方もしくは両方に取り組むことによって、このようなサービスを保護しようとします。

安全なリモートアクセス

まず、安全なリモートアクセスという課題について考えてみましょう。今のところ、開発者をクラウドにアップロードする方法がまだ発明されていないため、すべてのクラウドユーザーは「リモート」であり、その定義上、クラウドへの通信は、公開インターネットもしくはダイレクトコネクションによる専用接続を介して行われます。

通常、組織はこの課題の解決にVPNを採用しており、サイト間VPN（上図において、本社からクラウドに繋がる青い線）を設置したり、VPN接続をユーザーのデバイスからクラウド上のVPNコンセントレーターに直接収容したりします。他にも、ソリューションを組み合わせることによって、ユーザーのデバイスから企業ネットワークにVPN接続した後、企業ネットワークのサイト間VPN経由でクラウドにアクセスすることもできます。

VPNは、ユーザーのデバイスとクラウドネットワークの間に安全で暗号化されたトンネルを提供するため、上記の1つ目の課題（安全なリモートアクセス）を技術的に解決します。VPNにはいくつか欠点があり、特にすべてのユーザートラフィックを企業ネットワークに迂回させる場合、レイテンシが大きくなり、単一障害点が発生し、さらにネットワーク帯域やVPNライセンスに関するコストが増加します。ユーザーのデバイスからクラウドに直接VPN接続することによって、いくつかの課題に対処することができますが、例えば社内の開発リソースにアクセスする場合など、同時に企業ネットワークにもVPN接続する必要性が出てきた時に問題が発生する可能性があります。

一方、意外なことかもしれませんが、VPNトンネルを通過するアプリケーションプロトコルがHTTPSやSSHなどで、すでに暗号化が行われている場合、VPNを使ってもセキュリティの「機密性」や「完全性」がまったく向上しないことがあります。

VPNが貢献できるのはセキュリティの「可用性」であり、VPNの背後に保護するリソースは、インターネットに公開されることがないため、DDoSスタイルの攻撃を防ぐことができます。

次のセクションでは、VPNが対応できない、ユーザーアクセスの可視化と制御の必要性について議論します。

ユーザーアクセスの可視化と制御

ユーザーがどのようにIaaS環境の「入口」に到達したかに関わらず、VPN経由かにも関わらず、セキュリティチームは、どのユーザーが、IaaS環境内のどのリソースにアクセスすることができるかを制御（そして、監視やレポート）する必要があります。

IaaSプラットフォームは、これらを管理するためにツールを用意しています。AWSのSecurity GroupやAzureのNetwork Security Groupなど、本書でクラウドファイアウォールと定義したツールで、送信元IPアドレスによってサーバーへのアクセスを制御する単純なファイアウォールとして動作します。これは、アクセス保護に関する根本的な課題であり、組織が「ユーザーアクセス」の問題を解決しなければならない一方、用意されたツールは「IPアドレス」に基づいてアクセスを制御します。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

クラウドファイアウォールの例を見てみましょう:

Type	Protocol	Port Range	Source
HTTP	TCP	80	173.76.247.254/32
HTTP	TCP	80	50.255.155.113/32
HTTP	TCP	80	73.68.25.221/32
HTTP	TCP	80	98.217.113.192/32
HTTP	TCP	80	209.64.11.88/32
HTTP	TCP	80	172.85.50.162/32
HTTP	TCP	80	68.190.210.117/32
RDP	TCP	3389	173.76.247.254/32
RDP	TCP	3389	110.142.238.207/32
RDP	TCP	3389	50.255.155.113/32
RDP	TCP	3389	73.68.25.221/32
RDP	TCP	3389	98.217.113.192/32
RDP	TCP	3389	209.64.11.88/32

このファイアウォール設定の抜粋は、IaaSプラットフォームが提供する、IPアドレスを使った単純なルールによるアプローチを表しています。このクラウドファイアウォールのグループを割り当てたすべてのサーバーインスタンスに、これらの一連のルールが適用され、指定したポートへのネットワークアクセスが許可されます。IaaSのユーザーなら誰でも気づくように、このアプローチにはいくつかの問題があります：

- このクラウドファイアウォールに関連付けた「すべて」のサーバーに、粒度の粗いアクセスを提供します。
- IPアドレスがユーザーに紐づいていません。
- 「ポリシー」の概念がなく、送信元IPアドレスをリストに含めた「理由」の説明もありません。ユーザーアクセスポリシーに合わせて複雑な実装をすることは、非常に困難で労力がかかります。
- 静的なリストであり、ユーザーの場所や権限の変化に対応することができません。
- このアプローチでは、信頼の概念（認証の強度、デバイスプロファイル、クライアントの挙動など）を考慮して、アクセスを調整することができません。
- 設定変更には、IaaSアカウントの管理者アクセスが必要になります。
  》変更の集中管理によって生産性に遅延が発生する、もしくは、
  》IaaSアカウントの管理者アクセスを幅広いユーザーに許可することによって、セキュリティ、コンプライアンス、運用に問題が発生します。

IaaS環境において、安全なリモートアクセスは特殊なケースではありません。すべてのユーザーがクラウドから「リモート」であるため、セキュリティチームとネットワークチームは、一部のユーザーのみでなく、すべてのユーザーがどのようにリソースにアクセスするかを考慮する必要があります。すなわち、「安全なリモートアクセス」は、IaaSを採用するすべての企業にとって、主要な関心事として組織全体のセキュリティ戦略の中に位置付けられなければなりません。

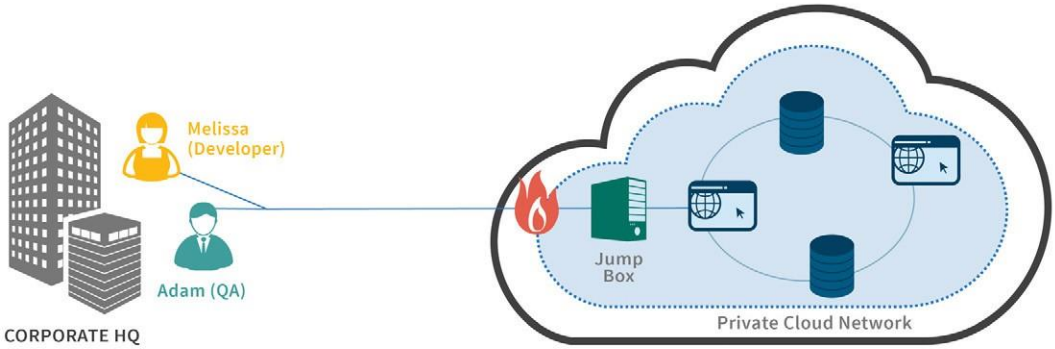
複数の送信元IPアドレスを1つのクラウドファイアウォールに登録する前述のアプローチの他、一部のプラットフォームでは、複数のクラウドファイアウォール（例えば、ユーザーのIPアドレス毎）を作成し、1台のサーバーインスタンスに複数のクラウドファイアウォールを関連付けるアプローチを取ることができます。このアプローチは、論理的に前述のアプローチと同様の効果があり、議論の余地はありますが、ファイアウォールに意味のある名前（「Sallyの家と職場」など）を付けられるため、前述のアプローチよりわずかに優れ

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ています。しかし、追加のオーバーヘッドが必要であり、また静的なソリューションであることに変わりはありません。

踏み台サーバー：飛びつく前に検討を

踏み台サーバーは、安全性の低いゾーンにいるユーザーに対して、より安全なゾーンにあるサーバーやサービスへのアクセスを提供するために設計されたサーバーです。本書では、踏み台サーバーを経由してクラウド環境内のサーバーにアクセスするシナリオを考えます。



上図に示す踏み台サーバーへのネットワークアクセスには、公開インターネット、ダイレクトコネクション経由の接続、VPN接続などが使われます。踏み台サーバーのデスクトップへのアクセスは、ユーザー認証（できれば多要素）によって制御されます。踏み台サーバーは、管理対象のサーバーへの単一のアクセスポイントを導入することにより、クラウドリソースへのアクセスを制御することができます。ただし、踏み台サーバーには多くの制限があるため、幅広いクラウドリソースへのアクセスに適していません：

- 通常、複数ユーザーによる利用ではなく、単独のユーザーが保護されたサーバーにアクセスすることを想定しています。
- 継続的なアクセスではなく、システム管理者などが必要時に限ってアクセスすることを想定しています。
- 踏み台サーバーの先にあるネットワーク上の全サーバーに対して、全部かゼロかのネットワークアクセスを提供します。
- 踏み台サーバー、もしくは踏み台サーバーにアクセスできるユーザーのデバイスを侵害すると、攻撃者はネットワーク全体にアクセスできるようになるため、攻撃面になりやすいです。
- コンプライアンスを目的としたユーザーアクセスの追跡を困難にします。

クラウドシステムへのユーザーアクセスに採用するソリューションとして、踏み台サーバーが相応しくないことは明らかです。

なぜVPNではなくSDPなのか?

言うまでもなく、VPNは、安全なリモートユーザーアクセスのために、幅広く展開されている一般的な技術です。なぜ、組織は、この実績ある技術を使い続けることができないのでしょうか。

VPNは、リモートユーザーが物理的に企業ネットワーク内にいるかのように、リモートユーザーにVLANやネットワークセグメントへの安全なアクセスを提供します。この技術は、特に多要素認証と組み合わせる場合、ユーザーやサーバーリソースが静的で、従来型の境界を採用する企業に適しています。Gartnerが述べるように、「DMZや旧来のVPNは、1990年代のネットワークのために設計されており、デジタルビジネスの保護に必要な俊敏性に欠けることから、時代遅れになってきています。」[8]

8 Gartner: G00315586, "It's Time to Isolate Your Services From the Internet Cesspool", 30 September 2016.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

VPNには、今日のニーズに合わない欠点が2つあり、他技術へのリプレースを待っています。第一に、VPNは、割り当てられたネットワークに対して、非常に大まかで、全部かゼロかのアクセスを提供します。VPNは、リモートユーザーがローカルネットワークにいるかのように振る舞うことを目的としており、すべてのユーザーにVLAN全体への完全なネットワークアクセスを提供します。VPNの設定によって、ユーザー単位で異なるアクセスレベルを提供することは、非現実的です。また、容易にネットワークやサーバーの変更に対応することもできません。単純に、VPNは今日のダイナミックな企業に追従できないのです。

第二に、VPNが提供する制御レベルに組織が満足したとしても、VPNはリモートユーザーのみを制御するサイロ化されたソリューションであり、オンプレミスユーザーの保護には何もできません。組織は、オンプレミスユーザーによるアクセスを制御するため、まったく異なる技術とポリシーを用意する必要があります。2つのソリューションを調整して整合性を取るには、2倍以上の労力が必要になります。また、組織がハイブリッドやクラウドベースのコンピューティングモデルを採用するにつれ、VPNを効果的に使用することがさらに困難になっていきます。

[9]

Gartnerも、次のようにVPNをSDPモデルに置き換える時期が来たとしています。「2016年の1%未満に対して、2021年までに60%の企業が、デジタルビジネスコミュニケーション用のネットワークVPNを段階的に廃止し、Software-Defined Perimeterを採用します。」[9]

9 Ibid.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

仮想デスクトップインフラストラクチャ（VDI）

仮想デスクトップインフラストラクチャ（VDI）は、組織が社内データセンターにある一元化されたサーバーが設置された施設上で多数のデスクトップOSインスタンスをホストすることを可能にする一連のテクノロジーです。 これらのインスタンスは、デスクトップOSの仮想化されたインスタンスの場合もあれば、多数のユーザーが同時にログインするデスクトップOSのマルチユーザーバージョンで構成されている場合もあります。VPNとともに、VDIは企業がネットワークやアプリケーションへの安全なリモートアクセスのために使用する優れたメカニズムです。

全体として、今日のクラウドとモバイルの世界には、VDIのいくつかの欠点があります。まず、デスクトップストリーミングにおけるユーザーエクスペリエンスは、小型の形状のモバイルデバイスでは悪くなる傾向があります。反応が悪く使用が非常に難しいため生産性が低下します。

第2に、多くのデスクトップベースのクライアント/サーバーアプリケーションはWebアプリケーションとして書き直されているため、VDIの価値が減少しています。3番目に、VDIのファームは、特にハードウェアベースの場合、調達費用が高くなる可能性があります。そしておそらく最も重要なことは、ワークロードがクラウドへ移行するにつれて、組織はVDIがリモートアプリケーションへのユーザーアクセスの問題を解決しないことを認識してきたということです。
実際、（通常はクライアントデバイスからVDIサーバーへのトラフィックを暗号化することによって、）VDIはリモートアクセスの問題の一部に役立ちますが、（特定のユーザーがどのネットワークリソースにアクセスできるかを制御するといった）ユーザーアクセスの根本的な問題の解決には役立ちません。状況によっては、VDIは、マルチユーザーオペレーティングシステムから発される一つのIPアドレスに対して複数のユーザーを表示することにより、この問題をさらに難しくすることがあります。この状況では、従来のネットワークセキュリティソリューションでは、ネットワークアクセス制御は事実上不可能です。

VDIには確かに特定の利点がありますが、クラウドネットワークおよびサーバーリソースへのユーザーアクセスを制御するようには設計されていないため、この問題がさらに難しくなる場合があります。

Software-Defined Perimeterではどのようにこれらの問題を解決するか

SDPは、前述のすべてのセキュリティ問題に対処でき、企業にIaaS環境への安全なリモートアクセスと、これらの環境へのユーザーアクセスのきめ細かい可視性と制御を提供します。

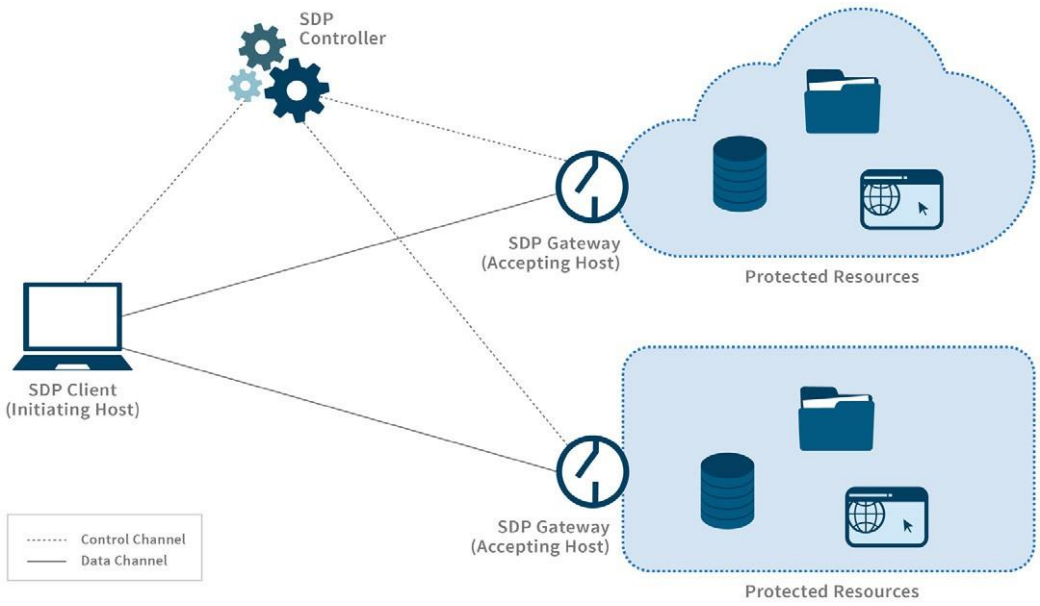
SDPを使用すると、組織は権限のないユーザーに対してクラウドリソースを完全に遮断できます。これにより、ブルートフォース攻撃、フラッディング攻撃、およびHeartbleedやPoodleなどのTLSの脆弱性を含む多くの攻撃ベクターが完全に排除されます。SDPは、サーバーの周りに「ダークネット」を構築することにより、組織がクラウド内部でのセキュリティの責任分担を適切に管理するのに役立ちます。

SDPは、2つの基本的な柱として事前認証と事前認可に依存しています。SDPは、例え1つのパケットがターゲットサーバーに到達する前であってもユーザーとデバイスを認証および認可することで、最小権限の原則をネットワーク層に適用し、攻撃面を大幅に削減します。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

Software-Defined Perimeter とは？

Software-Defined Perimeter[10]（SDP）アーキテクチャは、次に示す3つの主要コンポーネントで構成されています：



クライアント (Initiating Host)	各ユーザーのデバイスで実行されるクライアント
コントローラ	ユーザーを認証するコンポーネント（オプションでID管理システムへの統合を使用）、および各ユーザーに個別のネットワーク資格を付与する前にポリシーを評価するコンポーネント
ゲートウエイ (Accepting Host)	ゲートウェイは、保護されたリソースへのアクセスを仲介します。クライアントからのトラフィックは、暗号化されたトンネルを介して各ゲートウェイに送信され、そこで復号化されて適切なアプリケーション（保護されたリソース）に送信されます。 上の図に示すように、SDPアーキテクチャは複数の分散型ゲートウェイをサポートし、それぞれが一連のアプリケーションまたはシステムリソースを保護します。

SDPの用語を使用すると、クライアント（ユーザーデバイス）は*Initiating Host*であり、ゲートウェイは*Accepting Host*です。 コントローラによって認証された後、クライアントは各ゲートウェイへ暗号化されたトンネルを確立します（上の図は、1つのコントローラによって管理される2つの分散型ゲートウェイを示しており、それぞれが一連の個別のリソースを保護しています）。

SDP仕様の1つの重要な要素は、Single-Packet Authorization（SPA）です。この手法では、クライアントは共有秘密鍵（シード）に基づいてHMACベースのワンタイムパスワードを作成し、これを接続セットアップ中に送られる最初のネットワークパケットとしてSDPコントローラとゲートウェイに送信します。（これは、ゲートウェイとコントローラ間の接続設定にも使用されます）。

SDPコントローラとゲートウェイは（おそらく無認可のユーザーからの）無効なパケットを拒否するため、無認可のユーザーまたはデバイスからのTCP接続の確立を防ぐことができます。無効なクライアントは１つのパケットを分析することで区別できるため、SDPコントローラとゲートウェイによって発生するCPUの負荷は最小限に抑えられます[11]。これにより、DDoS攻撃の有効性は減少し、公衆ネットワークでのSDPサービスの安全で信頼性の高い展開が可能になります 。

10 The SDP version 1.0 specification is available here: https://cloudsecurityalliance.org/download/sdp-specification-v1-0/

11 The anti-DDoS SDP group has some interesting research on this topic, and some in-progress performance metrics showing server load with traditional TCP connections vs. SPA. Note that UDP-based SPA is even more resilient than TCP-based SPA, as it consumes even fewer server resources, and would better withstand an invalid packet flood attack.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

IPアドレスだけでなくユーザーに基づいたポリシー

SDPシステムはユーザーセントリックであるため（つまり、アクセスを許可する前にユーザーとデバイスを検証する）、組織がユーザー属性に基づいてアクセスポリシーを作成できるようにします。企業は、ディレクトリグループメンバーシップ、IAMが割り当てた属性、および役割などの側面を活用することで、ビジネス、セキュリティ、コンプライアンスチームにとって意味のある方法でクラウドリソースへのアクセスを定義および制御できます。これは、IPアドレスのみに基づきユーザーをまったく考慮しない従来のネットワークセキュリティシステムと比較して優れている点です。

SDPの利点

SDPを導入している組織は、この文書で明確に述べているセキュリティの改善の他、いくつかの側面でその恩恵を受けています。SDPの他の利点には、運用効率、コンプライアンスの簡素化、およびコストの削減が含まれます。 それぞれについて簡単に見ていきましょう。

運用効率

SDPによって実行される自動ポリシー適用には、特定のレベルのセキュリティを実現するために通常必要とされる手作業と比較して、運用上の大きなメリットがあります。これを別の観点から見ると、組織がSDPを使用して簡単に得られるセキュリティのレベルは、従来のセキュリティツールで達成することは事実上不可能ということです。

コンプライアンスの簡素化

ゲートウェイはすべてのクライアントネットワークトラフィックのログを取得し制御するため、SDPの実装は、通常、ユーザーごとのアクセス権限の付与とアクティビティの詳細な可視性を提供します。従って、SDPはこれらの詳細に基づいて自動化されたコンプライアンスレポートを提供できます。

また、SDPはユーザーアクセスのきめ細かい制御を可能にするため、企業は、ネットワークをより小さく、また十分に分離されたパーツにセグメント化することにより、コンプライアンス範囲を削減できるようになります。

コストの削減

SDPはいくつかの方法により企業がコストを削減するのに役立ちます。まず、アクセスポリシーの自動適用により、ユーザーまたはサーバーの変更に応じてファイアウォールルールを手動で更新およびテストする必要性が減少します。大規模な組織では、これは通常、IT部門の毎日のワークロードの一部であるため、ワークロードと人件費の両方を削減する機会を（特に外部委託モデルで）得ることができます。また、ビジネスおよび技術者の生産性を向上させます。これは、それだけで価値がある一方で、ハードコストを削減することもできます（特に時間給または外部委託された労働者の場合）。

次に、コンプライアンスの合理化により、監査の準備と実施に必要な時間と労力が削減されます。これらの活動は両方とも外部のコンサルタントを必要とすることが多く、節約された時間ごとに直接的なコスト削減になります。

最後に、SDPは、他のテクノロジーの代替として組織が費用を削減するのにも役立ちます。たとえば、NACによって必要となるネットワークスイッチのアップグレード要件を比較した後、従来のNACではなくSDPを選択し、設備投資だけで数十万ドルを削減した企業を見てきています。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

変化のきっかけとしてのSDP

特に興味深いのは、SDPが変化のきっかけになる可能性があるという考え方です。SDPはセキュリティアーキテクチャの大転換であり、近いうちにネットワークサービスを保護するために広く採用されるアプローチになると考えています。

組織は、セキュリティにアプローチする新しい方法としてより頻繁にSDPを取り入れ、またこれを、VPN、NAC、DMZなどの従来のセキュリティテクノロジーから、より効果的で、より動的で、よりセキュアな代替手段に置き換える機会としています。

SDPとID/アクセス管理

SDPとIdentity and Access Management（IAM）は、いくつかの点で相補的です。まず、SDPの実装は通常、SDPのロールアウトを加速するにあたり、すでに配備されているIAMシステムを認証に利用するように設計されます。この認証は、オンプレミスのLDAPサーバーまたはADサーバーへの接続を介して行われるか、SAMLなどの標準サービスを使用します。

第2に、SDPの実装は通常、ユーザーのIAM属性（ディレクトリグループメンバーシップ、ディレクトリ属性、ロールなど）をSDPポリシーの要素として使用します。たとえば、SDPポリシーには、「ディレクトリグループSalesのすべてのユーザーがポート443でサーバーSalesPortalにアクセスできる」と記載することができます。これは、SDPシステムが既存のIAM配備に付加価値を与える（そしてその能力を拡張する）方法の優れた例です。[12]

最後に、SDPシステムは、IAMシステムによって管理されるIDライフサイクルに含めることもできます。よく「Joiner, Mover, Leaver（新規採用、異動、退職）」と呼ばれますが、IAMシステムは、ユーザーアカウントとアクセスの変更に関連するビジネスプロセスと技術プロセスを管理します。SDPを導入する企業は、IAMプロビジョニングシステムにSDPが管理するネットワーク資格を含める必要があります。たとえば、IAMシステムがアプリケーションXにSally Smithの新しいアカウントを作成する場合、SDPシステムは対応するネットワーク資格を同時に作成する必要があります。

まとめると、この統合は、SDPシステムにアクセスするサードパーティのユーザーをサポートするために非常にうまく機能します。SDPコントローラは、認証とユーザーのIDライフサイクルの所有権の両方についてサードパーティのIAMシステムを信頼します。従って、あるサードパーティユーザーがIAMシステム上で無効化されると（これはユーザーのプロビジョニング無効化ビジネスプロセスのコアであるが）、ユーザーはフェデレーションを介して認証をできなくなるため、自動的にSDPで保護されたリソースにアクセスできなくなります。このフェデレーションは、サードパーティのアクセスに関する一般的な問題をうまく解決します。

SDPとIAMがどのように連携するかについてはまだ記載すべき多くのことがありますが、（これらのどちらも好きですが、）これらの分析はこの文書の範囲外となります。ただし、SDP v2仕様に含めることを検討中です。

12 This example is a realistic policy, but in some larger-scale environments may impose challenges. Vendors should consider policies that support parameterization, for example a policy that leverages identity and system attributes to effectively state "Only users in a {Department} may access their {Department portal} on port 443".

© Copyright 2017, Cloud Security Alliance. All rights reserved.

IAASユースケース

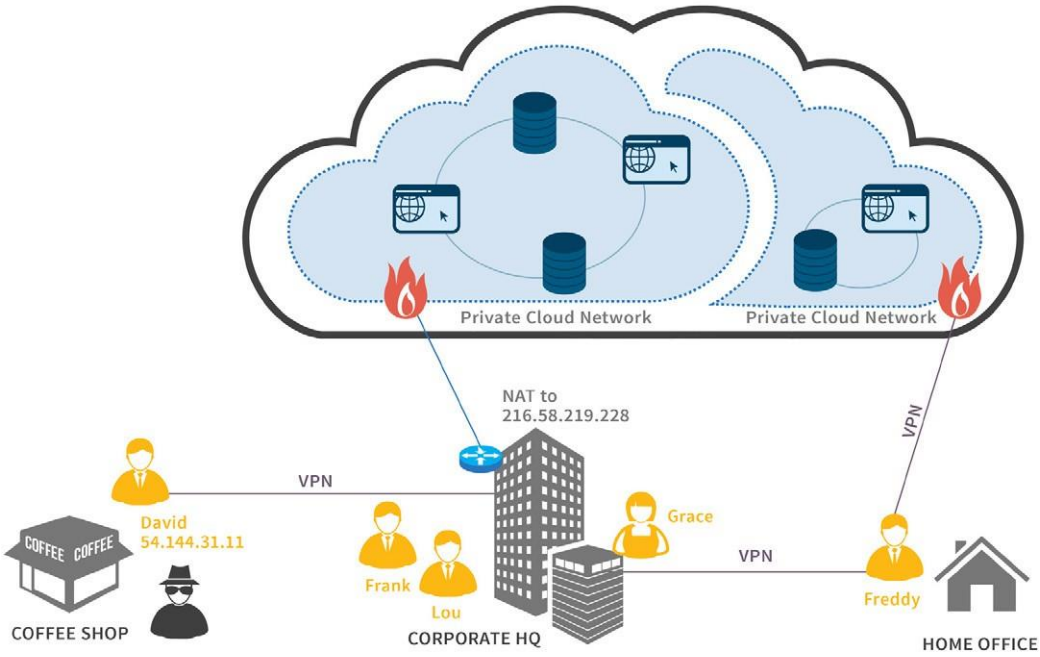
このセクションには、SDPが役立つIaaSアクセスのコア要件を表す6つのユースケースが含まれています。

ユースケース：IaaS環境における開発者の安全なアクセス

開発者は、開発、テスト、配備のためにIaaSリソースへの管理者権限によるアクセスを必要とします。これらのユーザーは、幅広いポートとプロトコルへのアクセス、および絶えず変化する一連のIaaSリソースへのアクセスを必要とします。

開発者は、機密データを扱う可能性があり、またDevOps環境では本番システムを扱います。その結果、組織は、システムへのアクセスの可視性と制御を必要とするセキュリティとコンプライアンスを必要とします。

SDPなしのアクセス



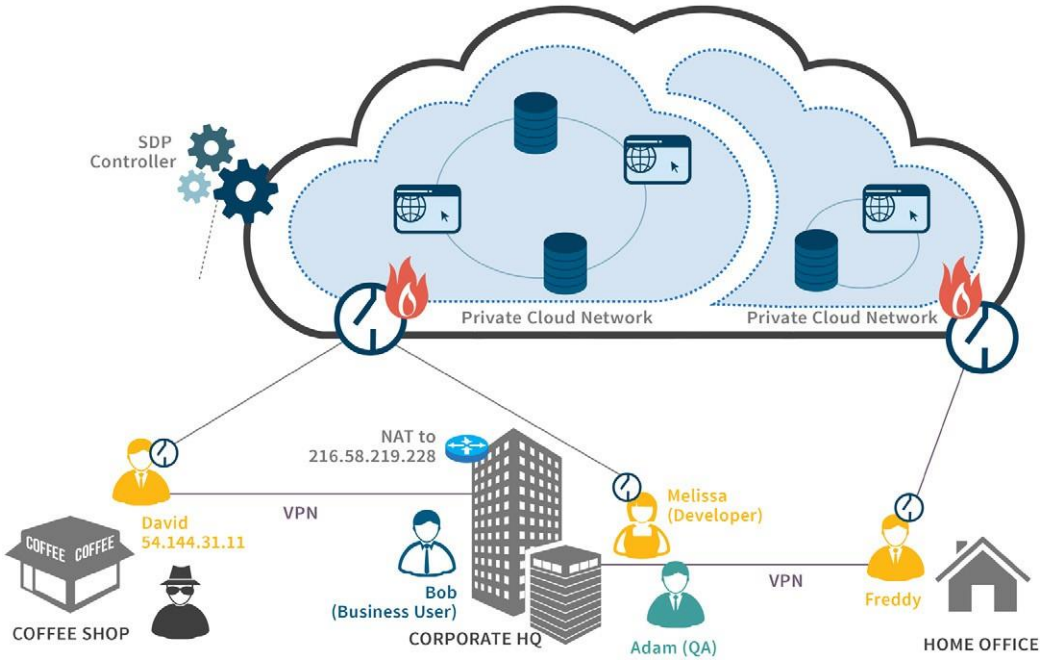
上の図では、さまざまな開発者の集まりが2つのプライベートクラウドネットワーク環境へのアクセスを必要としています。これらの開発者はアクセス要件が異なり、さまざまな場所にいます。クラウドファイアウォールはネットワークトラフィックの唯一の制御ポイントであり、基本的に許可された接続の単純なテーブルであり、ソースIPアドレスをターゲットサーバーとポートにマッピングします。

SDPありのアクセス

SDPは次のように展開されます。コントローラ（次のページの図に で示しています）は、すべてのユーザーがアクセスできる場所で動作しています（わかりやすくするため、接続は図に示されていません）。コントローラは、図のようにクラウドのエッジにあるパブリックにアクセス可能な場所で動作しているか、企業の本社のDMZで動作します。コントローラへのアクセスは、Single-Packet Authorizationによって保護されているため、インターネットに公開してもリスクは大幅に増加しません。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ユーザーは、コントローラによって適切に認証された後、ゲートウェイを介してプライベートクラウドネットワーク上のリソースにアクセスします。ゲートウェイもSPAで保護されており、すべてのユーザートラフィックは暗号化されたトンネルを介してインターネット経由で送信されます。ゲートウェイは、ユーザーごとにアクセスポリシーを適用し、最小権限の原則を実現します。ゲートウェイは、各プライベートクラウドネットワークのエントリポイントに配置され、すべての受信トラフィックを制御します。



© Copyright 2017, Cloud Security Alliance. All rights reserved.

比較

要件：Grace、Lou、Frankは本社で働いており、あるアプリケーションに対して共同作業を行う必要があり、複数のサーバーインスタンスのポート22（SSH）、443（HTTPS）、3306（MySQL）、3389（RDP）にアクセスする必要があります。

課題：本社のすべてのシステムは、単一のIPアドレス216.58.219.228にNAT変換されます。

SDPなし	SDPあり
アプローチ：216.58.219.228からプライベートクラウドネットワーク内のすべてのサーバー上のすべてのポートへのトラフィックを許可するようにクラウドファイアウォールを構成する必要があります。これらのサーバーには、パブリックにアクセス可能なIPアドレスが割り当てられている必要があります。	アプローチ：各ユーザーは、デバイス（Initiating Host）からゲートウェイ、次にクラウド内のターゲットリソースへの双方向認証されたトンネル接続を確立します。 クラウドファイアウォールの構成がはるかに簡単になります： • ゲートウェイは、インターネット全体からのすべてのトラフィックに開放されています。SPAを介してのみアクセスできるため、DoSおよびその他の攻撃に対してより耐性があります。[13] • 保護されたリソースは、ゲートウェイの背後のプライベートIPアドレスにあり、インターネットからはアクセスできません。クラウドファイアウォールは、ゲートウェイのIPアドレスからの接続のみを受け入れるように構成されます。
結果：企業ネットワーク上のすべてのユーザーとシステムは、プライベートクラウドネットワークへの完全なアクセス権を持っているため、最小権限の原則に違反し、攻撃面が増加します。このクラウドネットワークはスキャンすることが可能で、攻撃者は脆弱性を悪用できます。 サーバーアクセスは認証によってのみ保護され、ネットワークレベルでは保護されません。鍵管理は開発者にとって負担となります。 すべてのユーザーがすべてのシステムにネットワークアクセスできるため、コンプライアンスはさらに難しくなります。	結果：各ユーザーのゲートウェイへの接続は個別に確立され強力な認証が行われるため、送信元IPアドレスがNAT変換されているという事実は関係ありません。ゲートウェイは、ユーザーごとにきめ細かな方法でクラウドリソースへのアクセスを実施および制御できます。組織は、ユーザー、デバイス、および役割に関連付けられたポリシーを定義できます。

13 For more information, see the SDP research from the anti-DDoS group, as well as the annual SDP Hackathons sponsored by the CSA.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

要件：Davidはリモートで作業する開発者であり、コーヒーショップなどの安全でないネットワークからクラウドシステム内の複数のサーバーに定期的にアクセスする必要があります。また、本社のネットワーク上の開発リソースにアクセスする必要があります。これらのサービスは、複数のプロトコルとポート（22、443、3389）を使用します。

課題：コーヒーショップのネットワークは、単一のIPアドレス54.144.131.11にNAT変換されます。

SDPなし	SDPあり
アプローチ：クラウドファイアウォールをインターネット全体にオープンすることは受け入れられず、54.144.131.11からのすべてのトラフィックを許可することもセキュリティリスクが高すぎるため、Davidはまずオフィスネットワークに VPN接続し、企業LAN上にいるようにクラウドネットワークにアクセスします。	アプローチ：Davidのデバイスはコントローラで認証され、ゲートウェイによって保護されているリソースへのアクセスが許可されます。Davidは、オフィスネットワークにVPN接続する必要がなくなったため、ネットワークのパフォーマンスが向上し、ネットワーク帯域幅の使用とコストが削減されます。
結果：Davidは本社のネットワークへのVPN接続を必要とします（これは、オンプレミスのリソースにアクセスするためにもともと必要です）。 すべてのトラフィックを企業ネットワークに迂回させる必要があるため、レイテンシと帯域幅コストが増えます。 このソリューションによって、企業ネットワーク上のすべてのユーザーとデバイスがクラウドネットワークへのフルアクセスを持つということで、上記の要件を削除します。	結果：Davidのデバイスからゲートウェイへのトラフィックは暗号化されているため、Davidが公衆無線ネットワークや公衆インターネットを使用することによるリスクはありません。インターネットに開放されているクラウドファイアウォールの構成を変更する必要はありません（ただし、SPAによって保護されています）。そのため、Davidはどこにいても生産性を発揮でき、 セキュリティインフラは、場所に関係なく一貫して機能し続けます。

要件：Freddyは、ホームオフィスで働く開発者であり、チームの他のメンバーとは別のプライベートクラウドネットワークにアクセスする必要があります。この環境には機密で規制された機密情報が含まれているため、彼はそれにアクセスするためにVPNを設定しています。また、本社のネットワーク上の開発リソースへのアクセスも必要です。

課題：Freddyの場所は変わりませんが、クラウドと本社のリソースへの継続的なアクセスが必要です。セキュリティのため、安全なネットワーク接続が必要です。ただし、同じマシン上で2つのVPNを同時に実行することはできません。

SDPなし	SDPあり
アプローチ：Freddyは、開発マシンの別の環境を通じてこれらのリソースにアクセスします-彼はVMを介してクラウドにVPN接続し、ホストOSで実行されているVPNを介して本社のネットワークにアクセスします。	アプローチ：Freddyは、保護されたクラウドリソースにアクセスするために、ゲートウェイへの安全な接続を確立します。
結果：Freddyのツールと開発タスクのいくつかは、同じシステムから両方の環境にアクセスする必要があるため、このアプローチはFreddyに生産性の問題を引き起こします。 現在、この環境にアクセスしているのはFreddyだけなので、コンプライアンスと監査レポートに問題はありません。 しかし、数週間後に他のチームメンバーがこのプロジェクトに参加するときに、アクセスに関する追跡とレポート、およびこのアクセスの管理に問題が発生することを知っています。彼はこのアクセスをどのように有効にするかまだ知りません。彼はオフィスの中のすべての人にクラウドファイアウォールを開放する必要がありますか？リモート開発者はどうですか？彼は全員のVPNアクセスを管理する必要がありますか？	結果：SDP接続は、VPNではなくデスクトップOSの観点からは通常のネットワーク接続のように見えるため、競合や問題なしにオフィスネットワークへのVPN接続を同時に使用できます。したがって、Freddyはより生産的になります。 Freddyは、設計した一連のポリシーを通じて、これらのリソースへのアクセスを簡単に制御および報告できます。新しいユーザーへのアクセスのプロビジョニングは、ポリシーを編集するかユーザー属性を編集するだけの簡単なものであり、アクセスをきめ細かく制御できるようになります。そして彼にきめ細かい方法でアクセスを制御する能力を与えます。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

まとめ

このユースケースでは、SDPは組織に説得力のある利点を提供します：

- 場所に関係なく開発者のアクセスの安全化
- 各開発者がアクセスできるサービスの正確な制御-サービスおよびポートごと
- コンプライアンスレポートの簡素化
- セキュリティポリシー構成の簡素化
- 開発者の生産性の向上

ユースケース：ビジネスユーザーによる社内アプリケーションへのアクセス

ビジネスユーザーは、IaaS環境で実行されているエンタープライズアプリケーションに対して安全にアクセスする必要があります。ビジネスユーザーは、人事、財務、調達、経費、サプライチェーンなど、幅広いアプリケーションにアクセスする必要があります。アプリケーションには、ベンダー提供のパッケージアプリケーションや、社内開発者による自社開発アプリケーションがあります。

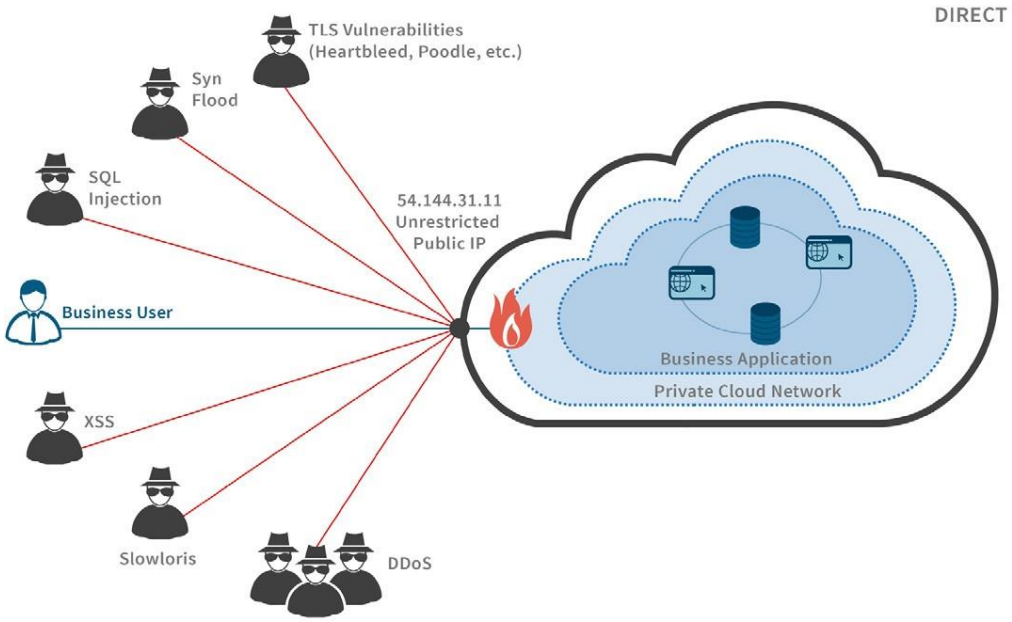
通常、ビジネスユーザーは、ネットワークやサーバーへの低レベルのアクセス（SSHやRDPなど）を必要としません。

アプリケーションは、本番環境やテスト／品質保証環境で動いている場合があります。

SDPなしのアクセス

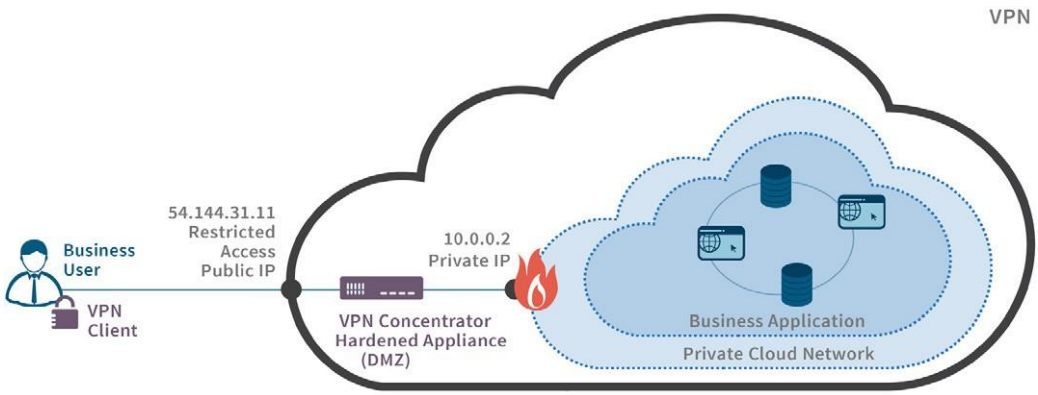
一般的に、ビジネスユーザーによるアプリケーションへの安全なアクセスには、1）直接、2）VPN、3）VDIといった3つの方法があります。

直接：直接アクセスの場合、通常、アクセス制限を行わずに、Webアプリケーションをインターネットに公開します。このような場合、ブルートフォース、DDoS、XSSといった攻撃や、HeartbleedやPoodleのようにTLSの脆弱性を悪用する攻撃など、アプリケーションがあらゆる種類の攻撃ベクターに晒されます。

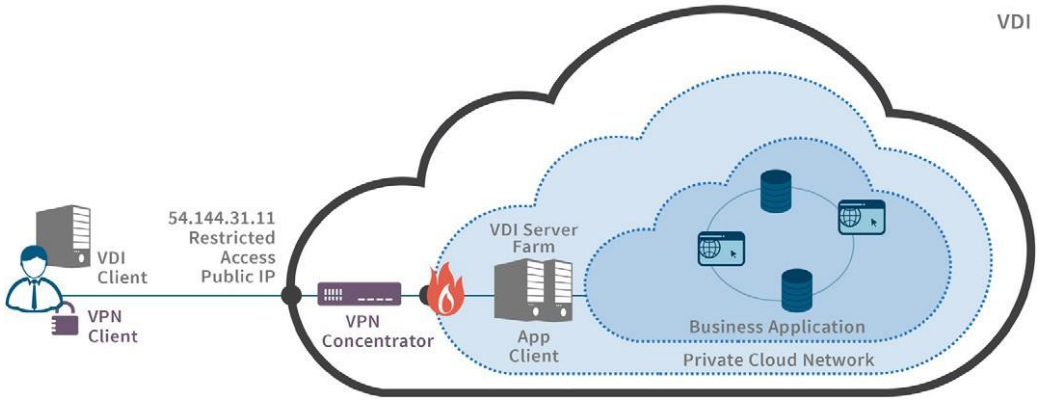


© Copyright 2017, Cloud Security Alliance. All rights reserved.

VPN：VPNを使用する場合、プライベートネットワークとともに、すべてのリソースがビジネスユーザーのデバイスからアクセスできるようになります。

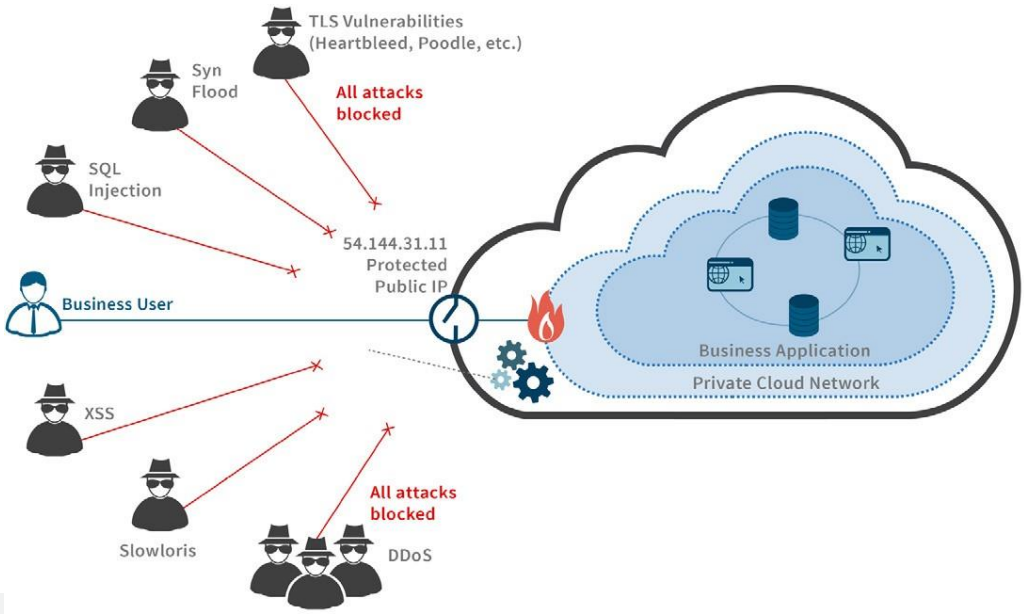


VDI：VDIを使用する場合、エンタープライズアプリケーションを起動するための仮想コンピューター（通常、Windows OS）がビジネスユーザーに提供されます。一般的に、ビジネスアプリケーションはクライアント／サーバー型で、Windowsのファットクライアントを使用します。



SDPありのアクセス

SDPソリューションを使う場合、許可されたユーザーのみがビジネスアプリケーションサービスにアクセスできます。実際、SDPゲートウェイがSingle-Packet Authorizationによって保護され、攻撃者には「見えない」ため、許可のないユーザーは、SDPゲートウェイにアクセスすることさえできません。

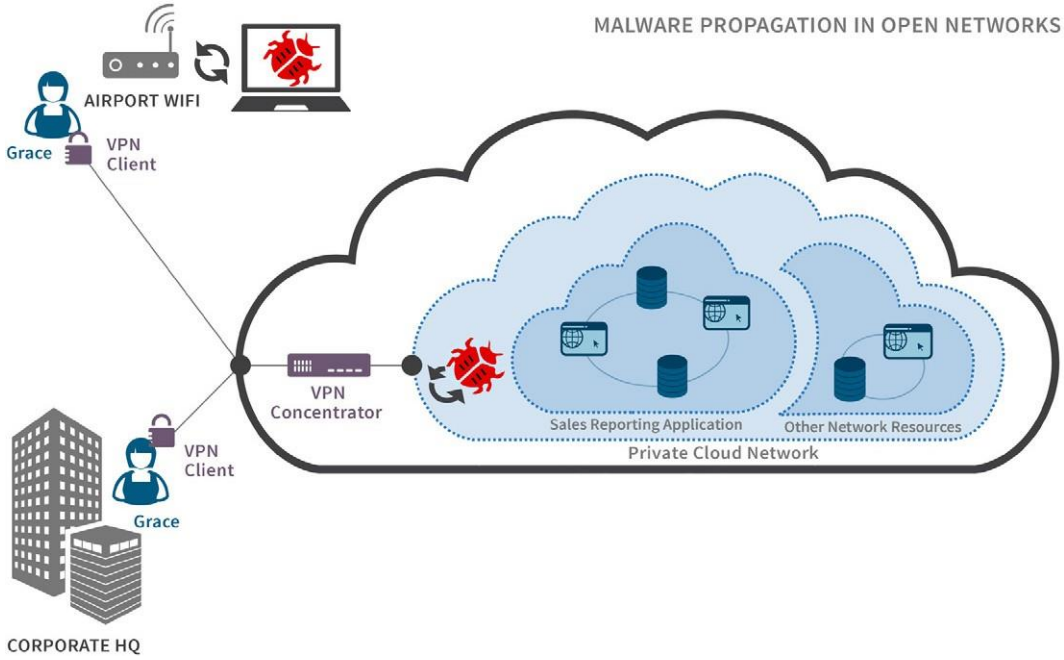


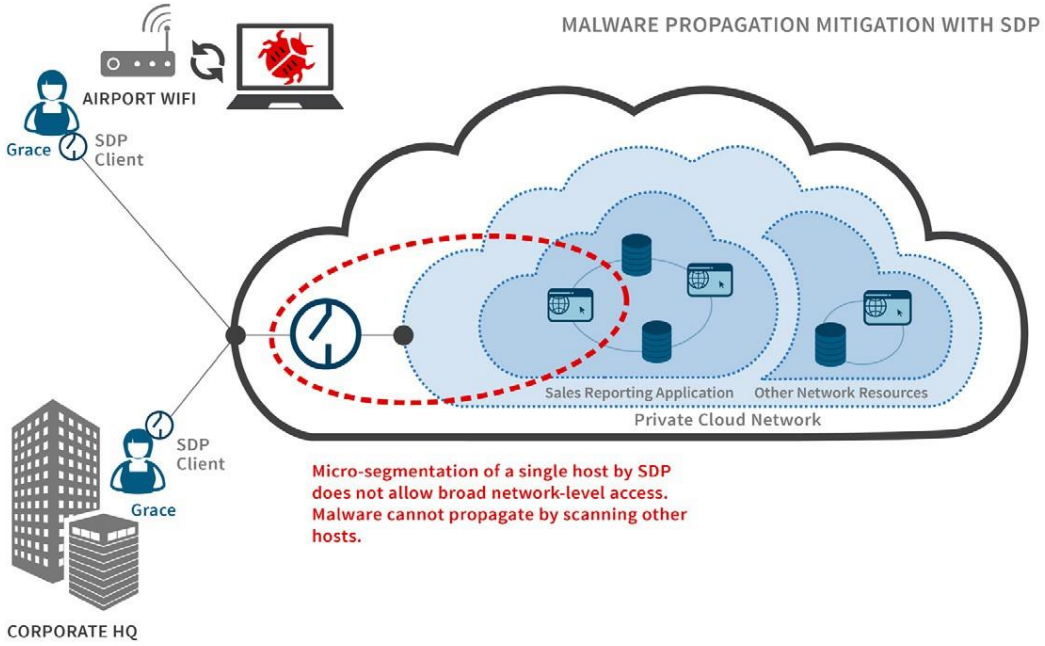
© Copyright 2017, Cloud Security Alliance. All rights reserved.

さまざまなユーザーのアクセス要件に対して、どのようにアクセスを管理するかを見ていきます。

要件：Graceは、本社の営業部門で働いています。彼女は、ITチームが新しく構築した営業報告アプリケーションを使って、上位顧客レポートにアクセスする必要があります。彼女は、複数の顧客先に出張するため、頻繁にリモートからレポートを実行する必要があります。このアプリケーションは、Amazon AWSで動作しています。

課題：Graceは出張中、業務のために空港やコーヒーショップのいくつかの無料ネットワークに接続します。過去にITセキュリティチームは、Graceが出張から戻ってきた後、彼女の端末からマルウェアを発見したことがありました。VPN経由で、もしくは本社に戻ってきた後、Graceが新しい上位顧客レポートにアクセスして、マルウェアがAWSインフラストラクチャに広がってしまうことを、ITセキュリティチームは懸念しています。（「Malware Monday」）





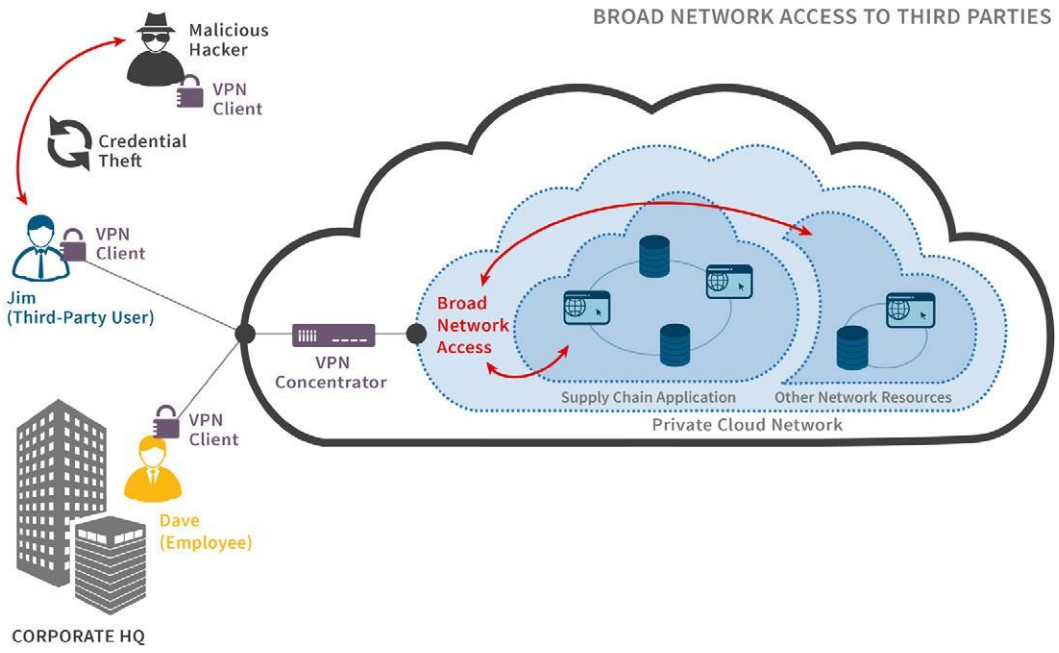
© Copyright 2017, Cloud Security Alliance. All rights reserved.

SDPなし	SDPあり
アプローチ：マルウェアをネットワーク内に拡散してはいけません。そのため、ITセキュリティチームは、ネットワークセグメンテーションを作成し、AWS上のアプリケーションサーバーを隔離します。	アプローチ：SDPには、ネットワーク全体ではなく、サーバー単位でネットワークを分離する利点があります。SDPは、Graceに安全なリモートアクセスを提供すると同時に、VPNのようなオープンネットワークアクセスに起因するマルウェアの拡散を防ぎます。[14]
結果：従来のネットワークツールによるマイクロセグメンテーションは複雑です。アプリケーションの数が増えるにつれ、ACLのレコード数が指数関数的に増える傾向にあります。[15] ネットワーク管理者は、何千ものACLを管理するため、すぐに過負荷に陥ります。新しいACLの追加には、分析と処理に何日もかかります。生産性が低下し、ITが俊敏性を失い、新しいアプリケーションの展開が遅くなります。	結果：ビジネスユーザーは、パブリッククラウドのネットワーク上にある社内アプリケーションに完全にアクセスできます。SDPは、ネットワークアクセスの制限を標準で提供します。従って、従来のVPNのように、最小権限の原則に違反することがありません。 ネットワーク管理者は、社内ネットワークが複雑に成長しても過負荷に陥ることがありません。オープンネットワークによるマルウェアの拡散は、既に防がれています。

要件：Daveは、IT部門でサプライチェーンアプリケーションを管理しています。新しいビジネスプロセスでは、商品が出荷されたらすぐに、サプライヤ—側の担当者であるJimがこのアプリケーションに出荷の詳細を入力する必要があります。

課題：サードパーティベンダーの担当者数名に対して、アプリケーションへのアクセスを許可する必要があります。これらのビジネスユーザー（Jimなど）は自社の従業員ではないため、彼らのセキュリティポリシーやトレーニングなどを、Daveがすべて管理することはできません。

Daveは、VPNを使って彼らに社内ネットワークへの広範なアクセスを許可することを望んでいません。ベンダー側で認証情報が盗まれた場合に、社内ネットワーク全体が侵害されることを懸念しています。侵害が起きた場合、影響範囲を制限する手段がありません。



14 Controlling East-West traffic with SDP will be substantively addressed in the v2 SDP spec. As noted elsewhere in this document, this is an easier problem to solve in IaaS environments versus on-premises.

15 Technically, O(n^2) in order to model application-to-application connections.

© Copyright 2017, Cloud Security Alliance. All rights reserved.

SDPなし	SDPあり
アプローチ：Daveは、このアプリケーションサーバー用にVLANを作成し、ネットワークの他の部分から隔離しました。しかし、サプライチェーンアプリケーションは非常に複雑で、ネットワーク内のいくつかのシステムと統合されています。VPC間接続、ファイアウォールルール、ネットワークレベルACLの整合性が必要です。複雑なネットワーク構成の維持は難しく、どこかのシステムでIPアドレスを1つ変更するだけで、サプライチェーンアプリケーション全体が停止する可能性があります。	アプローチ：SDPでは、ネットワーク全体ではなく、サーバー単位でネットワークを分離することができます。ベンダーがリモート接続しても、ネットワーク上の他のリソースにアクセスすることはできません。悪意のあるハッカーがネットワーク上の脆弱なリソースを探索することはできません。 Daveは、ベンダーの担当者に安全なリモートアクセスを提供するため、SDPを選択します。
結果：ネットワークセキュリティの観点から複雑でリスクが高いため、Daveはサードパーティに対するアプリケーションアクセスの提供を拒否します。 サプライチェーンアプリケーションのユーザーは、ベンダーからの入庫計画の改善を望んでいました。この結果、ビジネス部門がデータセンターで使う資材の入庫予定を確認できなくなり、発注誤りや出荷遅延に悩まされます。	結果：Daveがサードパーティのビジネスユーザーに対してセキュリティのベストプラクティスやトレーニングを強制することはできませんが、認証情報が窃取された場合の影響範囲をSDPによって限定することができます。サードパーティに対して、より安全にアクセスを許可することができます。このアプローチによって、サプライチェーンアプリケーションの効率を改善し、ビジネスの成長を維持することができます。

要件：Jimは、出張中であっても、ビジネス分析レポートを毎週実行します。このレポートは、Windows OS専用に作られた（Webアプリケーションではなく）クライアント／サーバー型のアプリケーションです。IT部門はJimのチームのためにVDIソリューションを導入しました。Jimは、VDI経由でリモートデスクトップにログインし、レポートアプリケーションを起動します。

課題：このクライアント／サーバー型のレポートアプリケーションは、大手ベンダーから購入したパッケージアプリケーションです。推奨される導入モデルは「オンプレミス」のみです。ベンダーは、安全でないため、アプリケーションサーバーをパブリックインターネット経由で使用しないことを推奨しています。すなわち、サーバーとクライアントが同じネットワーク上にある必要があります。

そのため、ITセキュリティチームは、リモートユーザーのためにVDIを使用することを決め、クライアントとサーバーが常に同じネットワーク内にとどまるようにしました。しかし、VDIサーバー環境の構築と維持にかかるコストが非常に高く、モバイルユーザーや出張者の増加にともない、さらにコストが増えています。

課題は、クライアント／サーバー型アプリケーションのサーバー部分を安全に公開して、ビジネスユーザーが自分のWindows端末で直接クライアントを実行できるようにすることです。

SDPなし	SDPあり
アプローチ：Jimは、VDI環境をサポートするため、インフラストラクチャを増強し続けます。	アプローチ：Jimは、SDPを使うことにより、許可されたビジネスユーザーが所有するデバイスに対してのみ、認証／認可を行った上で、サーバーのポートを安全に公開します。それ以外のユーザーやデバイスには、このサーバーは「見えません」。 Jimは、SDPを選択することによって、ビジネス分析を行うユーザーに、クライアント／サーバーアプリケーションへの安全なリモートアクセスを提供します。
結果：大規模なVDI環境を用意するには、ハードウェアのための設備投資と、VDIサーバーの維持管理をするための運用費用が増加します。 その結果、IT部門は他の重要プロジェクトの予算を削減する必要があり、VDI環境が予算を食いつぶします。	結果：SDPアプローチによって、VDIインフラストラクチャを維持する理由が薄れます。ビジネスユーザーは、アプリケーション実行前にリモートデスクトップ接続する必要がなくなるため、生産性が向上します。 VDI環境を廃止することができ、自由になるIT予算を他の活動に使うことができます。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

まとめ

このユースケースでは、組織にとって説得力のある利点があります：

- リモートビジネスユーザーによる社内アプリケーションへの安全なアクセス
- ユーザーがアクセスできるアプリケーションの正確な制御
- サードパーティとのビジネス統合の強化
- コンプライアンスレポートの簡素化
- VDIに関わるインフラストラクチャコストの削減
- セキュリティポリシー設定の簡素化
- ビジネスプロセスの生産性向上

© Copyright 2017, Cloud Security Alliance. All rights reserved.

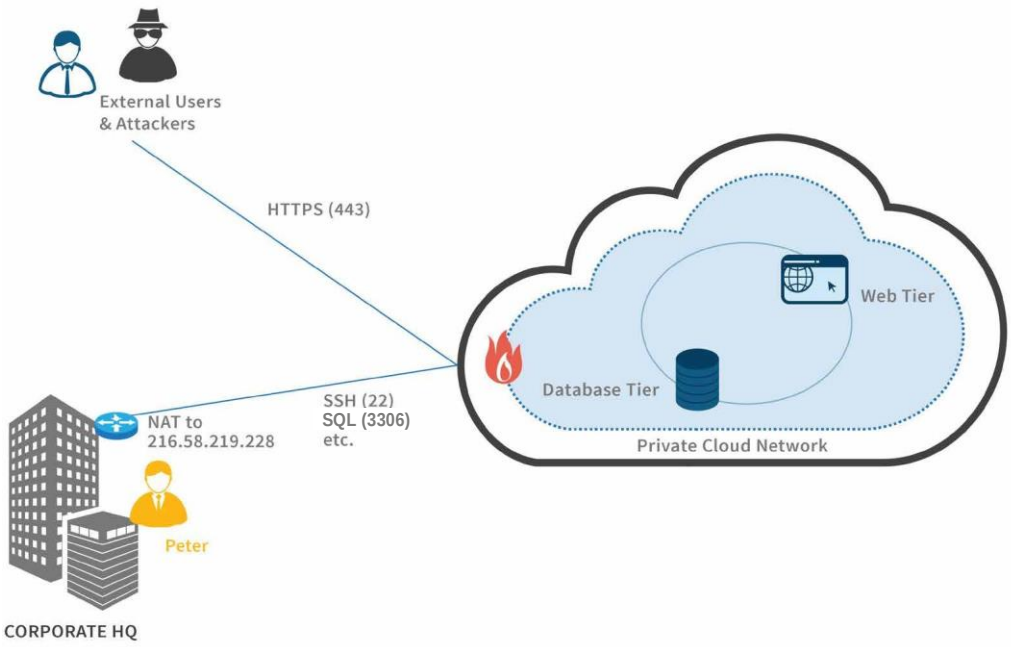
ユースケース：管理者によるインターネット公開サービスへのアクセス

アプリケーションをクラウドに配置すると、バックエンドサービスの多くに対して、システム管理者やDevOps担当者などのパワーユーザーが、リモートからアクセスする必要があります。これには、次のサービスを含みます：

- データベースへのSQLインターフェース（SQL Navigator for Oracle、PgAdmin for Postgresなど）
- サーバーへのSSHアクセス
- アプリケーションへの管理者アクセス（Wordpressブログの管理者など）
- HTTPS経由のデータベースツール（PhpMyAdmin for MySQLなど）

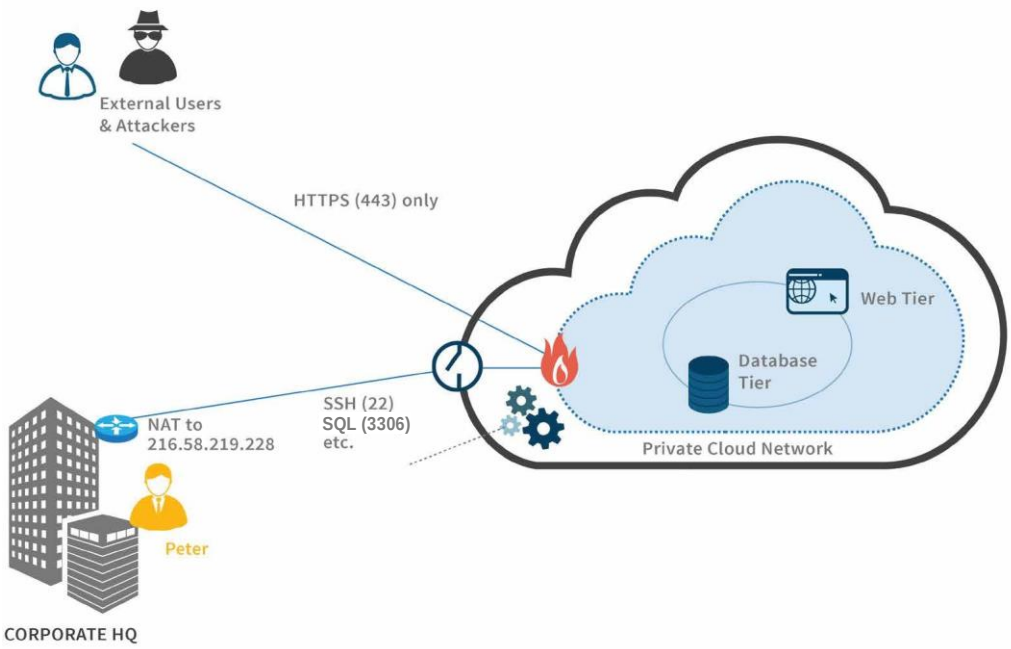
これらのサービスを、制限なくインターネットに公開することは賢明でありません。これらを公開することは、ブルートフォース、設定不備、ゼロデイなどによる攻撃機会の増加をともないます。

SDPを使わない場合、バックエンドサービスは、インターネットに公開するか、もしくは送信元IPアドレスによってアクセスを制限します。送信元IPアドレスによるアクセス制限は、クラウドファイアウォールを手動でメンテナンスする必要があり、また制限をかけても多くのユーザーに対してサービスが公開されています。



© Copyright 2017, Cloud Security Alliance. All rights reserved.

SDPソリューションを導入すると、公開を意図したサービスのみ（HTTPSなど）がインターネットに公開されます。他のサービスはSDPゲートウェイによって隠蔽され、ポリシーによってアクセスが制御されます。アクセスを分離するためにVPNを追加する必要はありません。



要件：Peterは、財務アプリケーションのデータベース管理者です。彼の会社は、インフラストラクチャを主要なIaaSプロバイダーに移行しました。Peterのタスクには、データベースSQLクエリのチューニングによる、アプリケーション性能の改善があります。Peterは、チューニングを行うため、ファイアウォールでデータベース接続ポートを開放し、SQL Navigatorを使ってデータベースに接続します。

課題：データベース接続ポートが世界中に公開されています。悪意のあるボットがすぐさまポートを発見し、管理者パスワードに対してブルートフォース攻撃を仕掛けます。数日で辞書攻撃に成功し、企業の重要財務データへのアクセスを奪われたり、デフォルトパスワードの使用が見つかったり、（パッチが適用されていない）データベースの既知の脆弱性を攻撃されたりする可能性があります。

SDPなし	SDPあり
アプローチ：Peterは、VPNを使ってクラウドネットワークに接続します。	アプローチ：SDPを使うことにより、データベース接続ポートをPeter以外に対してクローズします。悪意のあるハッカーは、データベースサービスが動作していることに気付くことができません。 データベース接続ポートへのアクセスは、Peterのデバイスに対してのみ、適切な認証および認可の上で許可されます。
結果：Peterは、自社データセンターのプライベートネットワーク以外にVPN接続する必要があります。Peterは、自分の端末に2つのVPNエンドポイントを設定し、ネットワークリソースにアクセスする度に、どちらのVPNに接続するかを選択する必要があります。 PeterはSQL開発者であり、IT管理者ではないため、VPNの設定を十分に理解していません。Peterは、VPNによって生産性が損なわれることを嫌っています。	結果：Peterは、複数の設定を切り替えたり、ネットワークセキュリティ設定したりすることなく、データベースに対して安全なプライベートアクセスを手に入れることができます。

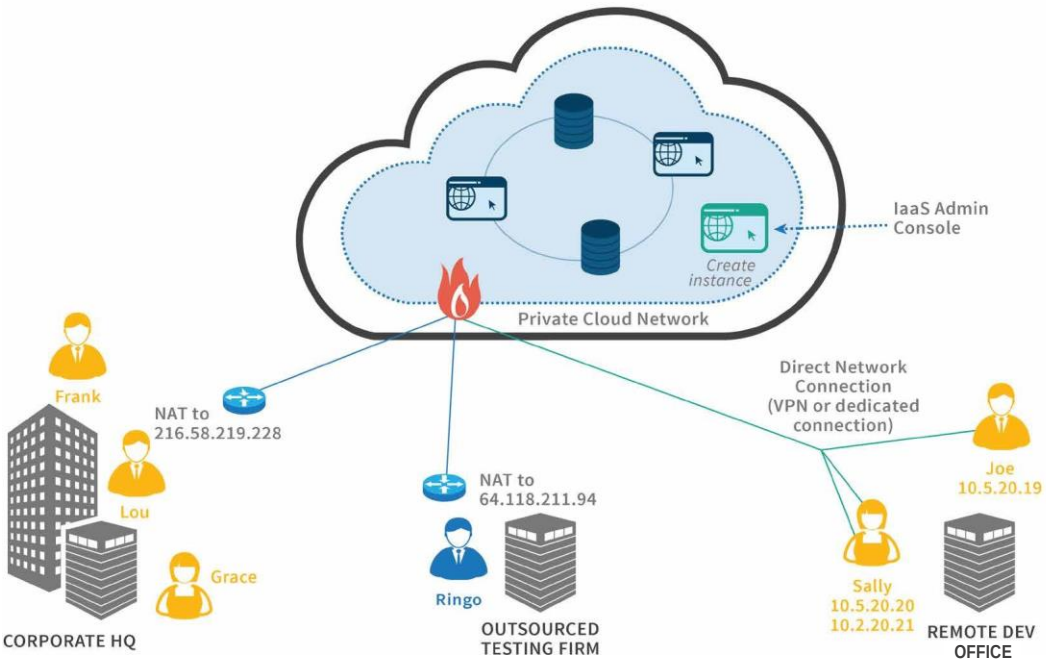
© Copyright 2017, Cloud Security Alliance. All rights reserved.

ユースケース：新しいサーバーインスタンスが作成されたときのユーザーアクセスの更新

クラウド環境は本質的に動的であり、ほとんどの組織がIaaSのこの側面を活用して、開発の速度と俊敏性を高めていると言っても過言ではありません。特に、IaaS環境では、サーバーインスタンスの作成と破棄がすばやく簡単にできるため、組織はこれを頻繁に（継続的ではないにせよ）実行します。[16]

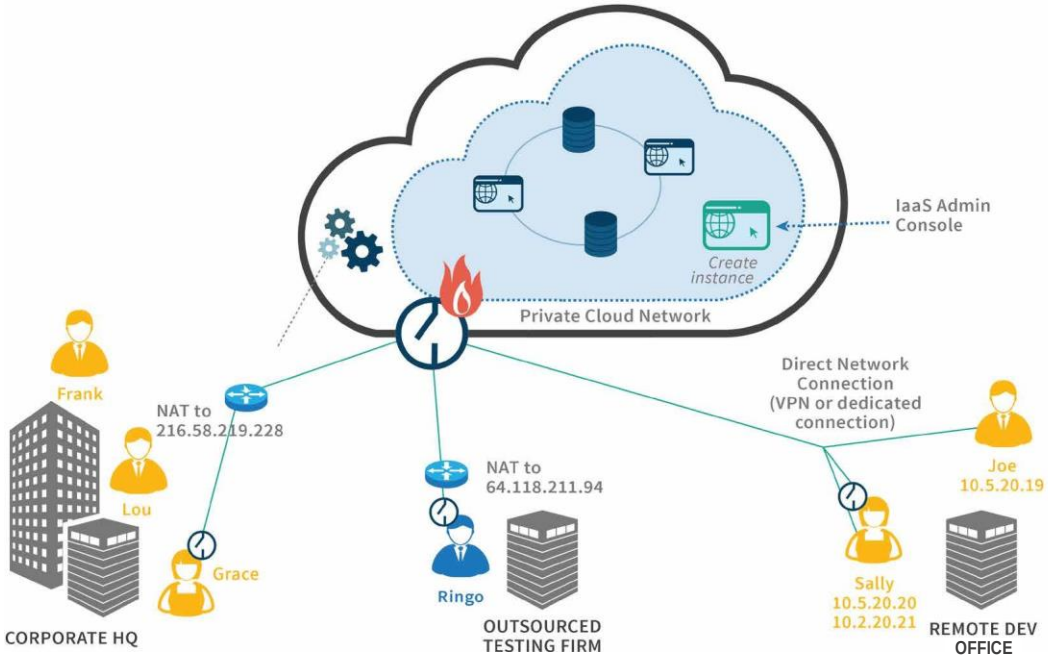
SDPなしのアクセス

次の図に示すように、IaaS管理コンソール（またはAPIコールを行うシステム）を使用しているユーザーが新しいサーバーインスタンスを作成します。必要なネットワークの変更は、場所、クラウド接続の種類、およびニーズによって異なります。これは、次のページの表で説明されています。



16 *Note 1:* For this use case, we're examining server instances that are manually launched by the IaaS admin console, or launched via IaaS API from a development or deployment script. Automated scaling of server instances (for example based on a CPU load threshold) by the IaaS infrastructure is not discussed here. Access to these instances is covered by existing use cases, since they're effectively clones of already-running resources that exist solely for load balancing and scale purposes. Access to them will be governed by the same access policies that control the core set of servers in the pool, which are covered in other use cases in this document. *Note 2:* Because network access is granted by assigning an instance to a Cloud Firewall group, no action is required to remove access when an instance is terminated. Cloud Firewalls control access to specific server IP addresses, and therefore there's no risk of access being mistakenly inherited through IP address reuse.

© Copyright 2017, Cloud Security Alliance. All rights reserved.



SDPありのアクセス

クラウドサーバーは、すべてSDPシステムによって保護され、ゲートウェイがプライベートクラウドネットワークへの唯一のネットワークエントリポイントとして機能します。新しいサーバーインスタンスにはメタデータ（タグ）があります。

要件：Graceは、インスタンスを起動し、SSHアクセスのみ（ポート22）アクセスできるようにします。

課題：Graceは、NAT変換されたIPアドレスからクラウドにアクセスするネットワーク上にいます。

SDPなし	SDPあり
アプローチ：このインスタンスにはパブリックIPアドレスを割り当てる必要があり、クラウドファイアウォールはNAT変換された IPアドレス216.58.219.228からこのインスタンスへのフルアクセス、またはインターネット全体（0.0.0.0）へのフルアクセスを許可する必要があります。	アプローチ：新しいサーバーインスタンスへのアクセスは、SDPゲートウェイを経由する必要があります。SDPゲートウェイは、パブリックにアクセス可能で、SPAによって保護されています。 SDPシステムはこの新しいサーバーインスタンスを検出し、そのメタデータ（タグ）に基づいて、Graceにポート22へのアクセスを自動的に許可します。
結果：クラウドファイアウォールをすぐに変更する必要はありませんが、このサーバーへのアクセスはすべてのユーザーに対して無制限になります。これは、重大なセキュリティリスクになります。 IPアドレスはNAT変換されているため、ネットワークアクセスを単一のユーザーまたは単一のポートだけに制限することは不可能です。代わりに、セキュリティチームはこれらのインスタンスへのSSHアクセスを別々の鍵によって制御する必要があります。これらの鍵ファイルの管理と追跡は、開発者にとって頭痛の種であり、セキュリティ上のリスクです。	結果：Graceには、手動による再構成やIT運用の関与なしに、生産性を高めるために必要最小限のアクセスレベルが自動的に付与されます。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

要件：Sallyはインスタンスを起動し、両方のデバイスからHTTPS、RDP、およびMySQLのポートにアクセスする必要があります。
課題：Sallyはオフィスからクラウドへの直接的なネットワーク接続を通してクラウドにアクセスします。これらのリソースは、ローカルネットワーク上にあるように見えます。

SDPなし	SDPあり
アプローチ：Sallyのみへのアクセスを制限することを目的とする場合は、クラウドファイアウォールを更新して、Sallyの現在のIPアドレスがこの特定の新しいサーバーインスタンスにアクセスできるようにする必要があります。遅延なくSallyにアクセスを許可することが目的である場合、ローカルネットワーク上のすべてのデバイスがすべてのポート上のこの新しいサーバーインスタンスにアクセスできるようにインスタンスを構成する必要があります。	アプローチ：SDPシステムはこの新しいサーバーインスタンスを検出し、そのメタデータ（タグ）に基づいて、適切なポートへのアクセスをSallyに自動的に許可します。
結果：クラウドファイアウォールに継続的な変更を要求することは、時間とコストを追加するため、ほとんどの組織が引き受けようとしない運用上の負担になります。ほとんどの組織は、オープンネットワークアクセスを許可し、認証のみに依存しています。	結果：Sallyには、手動による再構成やIT運用の関与なしに、生産性を高めるために必要最小限のアクセスレベルが自動的に付与されます。

要件：Ringoは外部委託のQAチームで作業しており、この新しいインスタンスをテストするにはWebアクセス（443）が必要です。

課題：Ringoのオフィスは単一のパブリックIPアドレスにNAT変換され、このパブリックIPアドレスは変更されません。Ringoは別のタイムゾーンにいるため、リアルタイムでチームと共同作業するために、自宅で仕事をする必要がある場合があります。

SDPなし	SDPあり
アプローチ：クラウドファイアウォールは、RingoのパブリックIPアドレスからのアクセスを許可する必要があります。 特定のサーバーのみをこのクラウドファイアウォールグループに割り当てることにより、これを特定のサーバーインスタンスに制限できます。ファイアウォールは、Ringoの（定期的に変更される）自宅のIPアドレスからのアクセスも許可する必要があります。	アプローチ：SDPシステムはこの新しいサーバーインスタンスを検出し、そのメタデータ（タグ）に基づいて、Ringoにポート443へのアクセスを自動的に許可します。
結果：この新しいサーバーインスタンスを起動するユーザーは、RingoのNAT変換されたIPアドレスからのアクセスを許可するセキュリティグループにインスタンスを割り当てる必要があります。Ringoを含むローカルネットワーク上のすべてのユーザーも、ポート443でこのインスタンスにネットワークアクセスできます。 Ringoの自宅のIPアドレスが変更されるたびに、クラウドファイアウォールの更新をITに要求する必要があります。これには最大24時間かかる場合があり、チーム全体の生産性に影響を与えます。	結果：Ringoには、手動による再構成やITオペレーションの関与なしに、生産性を高めるために必要な最小限のアクセスレベルが自動的に付与されます。 Ringoはユーザーとしてアクセスが許可されているため、IPアドレスに関連付けられていません。これは、Ringoがすぐに生産性を発揮し、どこから作業しているかに関係なく、同じレベルの安全なアクセスができることを意味します。

まとめ

この使用例では、SDPは組織に説得力のある利点を提供します。

- 新しいサーバーインスタンスの自動検出、およびインスタンスメタデータに基づくユーザーアクセスの

© Copyright 2017, Cloud Security Alliance. All rights reserved.

自動割り当て

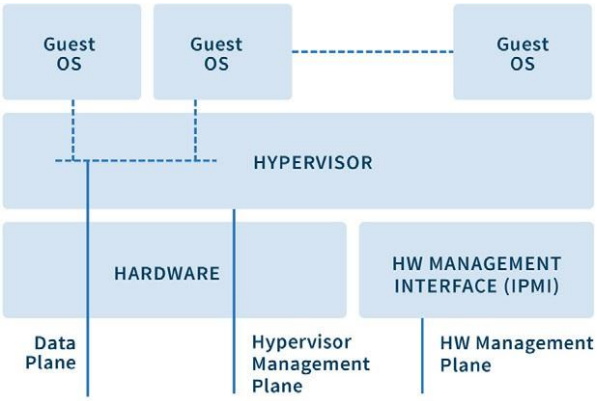
- 場所に関係ない安全な開発者のアクセス
- 十分なユーザー生産性-ネットワークアクセスの変更を待つための遅延なし
- アクセスはポリシーに基づき、クラウドファイアウォール構成に基づくものではない
- ITオペレーションの労力とコストの削減

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ユースケース：サービスプロバイダーのハードウェア管理プレーンアクセス

クラウドは、無限に拡張可能で完全に仮想化されたプラットフォームという抽象的な概念にも関わらず、実際にはネットワークおよびコンピュートハードウェア上のあるレベルで実行されます（つまり、仮想化された「下にずっと続く亀たち」（Turtles all the way down）」ではありません）（訳注： それぞれの亀を、他の（より大きな）亀が支えていくという考え方）。 そしてもちろん、このハードウェアは、プライベートクラウドプラットフォームを提供するオンプレミスのIT部門、マネージドホスティングまたはコロケーションプロバイダー、商用IaaSベンダーのいずれであっても、サービスプロバイダーによって管理される必要があります。

次の論理図は、管理対象のネットワークアクセスパスを示しています：



データプレーンは、ゲストOSインスタンスへのアクセスおよびゲストOSインスタンスからのアクセスに使用される標準ネットワークです。この文書全体の議論はすべて、このネットワークに集中しています。

ハードウェア管理プレーンは、多くのハードウェアプラットフォームに組み込まれているネットワークで、通常はIPMI（Intelligent Platform Management Interface）と呼ばれるIntel仕様に基づいて構築されています。これは、一般的にBMC（ベースボード管理コントローラ）と呼ばれることもあれば、非公式に「ライトアウトネットワーク（lights out network）」と呼ばれることもあります。ほとんどのサーバーメーカーは、Dellサーバーの場合はDRAC、HPサーバーの場合はILOと呼ばれる独自の物理ネットワーク接続を備えた組み込みハードウェアカードを介してこれをサポートしています。[17]

残念ながら、これらのIPMIサービスは、変更されないことが多いデフォルトの資格情報や単純な攻撃に対する脆弱性など、多くの脆弱性が存在することがよく知られています。[18]

ハイパーバイザー管理プレーン（Hypervisor Management Plane）は、管理者がGUIコンソールまたはAPIを介してハイパーバイザー管理機能にアクセスする方法です。ハイパーバイザーは一般にIPMIシステムよりも優れたアクセス制御を備えていますが、物理的に別のネットワークまたはVLAN上にある別のネットワークカードを介してのみアクセスできるように構成し、SDPで保護される必要があります。以下の説明は、IPMIに焦点を当てていますが、ハイパーバイザー管理プレーンにも適用できます。

要件：さまざまなポートのIPMIネットワークインターフェイスへの管理者アクセスを保護します。このアクセスには強力な認証が必要であり、セキュリティとコンプライアンスのレポートのためにログに記録する必要があります。理想的には、管理者はこのネットワークに24時間アクセスできますが、必要な場合のみです。ただし、ITがサーバーの停止に対応している可能性があるため、この必要に応じたアクセスは多くの場合、時間的な制約があります。アクセスを制御するには、要求や許可などのビジネスプロセスが必要です。アクセスが不要になったときにアクセスを確実に削除するための閉ループ制御のメカニズムが必要です。

課題：IPMIには、悪用可能な脆弱性から不十分な管理機能まで、多くの既知の弱点があります。
IPMIには、物理的に分離されているかVLANを介した別のネットワークが必要です。

17 See https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface for additional information.
18 See https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi

© Copyright 2017, Cloud Security Alliance. All rights reserved.

SDPなし	SDPあり
アプローチ：あまり推奨されないデフォルトのアプローチは、IPMIシステム内のデフォルトの資格情報に依存し、IPMIネットワークへのアクセスを許可されたユーザーのみに制限することです。 もう少し優れたアプローチは、かなりのオーバーヘッドが発生しますが、各サーバーのアクセス資格情報を個別に管理することです。 さらに優れたアプローチは、IPMI認証を企業のLDAP/RADIUSシステムに関連付けることです。	アプローチ：SDPを使用すると、IPMIサーバーをSDPゲートウェイで保護されたネットワークセグメントに簡単に配置できます。つまり、SDPポリシーで許可されない限り、ネットワークトラフィックはIPMIインターフェースに到達できません。 SDPシステムは、グループメンバーシップ、デバイスプロファイル、場所、時刻など、さまざまなユーザーおよびシステムの属性を活用できます。
結果：これらのソリューションはどれも強力ではありません。IPMIシステムをデフォルトの資格情報のままにしておくと問題が発生するだけです。たとえば、設定ミスなどにより、悪意のある人物がネットワークにアクセスするのは簡単です。 サーバーごとにユーザーアクセス資格情報を構成すると、セキュリティは向上しますが、様々なサイズの環境において機能するようにはできません。これを行うには、手作業と資格情報の追跡が多すぎるためです。 組織のLDAP / RADIUSシステムを認証に利用する方がはるかに優れていますが、ある時点でIPMIアクセスを必要とする可能性のあるすべてのユーザーが、常にIPMIネットワークに完全にアクセスできる必要があります。 ファイアウォールルールを使用してネットワークアクセスを制御することは技術的には可能ですが、プロセスのオーバーヘッドが大きすぎ、サーバーへの管理者のアクセスが遅れます。	結果：IPMIインターフェースへのユーザーアクセスは、ポリシーに基づき、即時の「知る必要性」に基づいて簡単かつ動的に行うことができます。たとえば、SDPシステムは、アクセスを許可する前に、特定のユーザーと特定のサーバーをリストするオープンのサービスデスクチケットの存在を検証できます。これにより、この機密の資格へのアクセスを要求および承認するビジネスプロセスが簡単にサポートされます。 また、SDPシステムは、オンプレミスの企業ネットワークからのアクセスのみを許可し、リモートの場所からのアクセスをブロックするなど、場所に基づいてアクセスルールを適用することができます。 SDPは、組織のIAMシステムと統合して、強力な認証を実施することもできます。

まとめ

このユースケースでは、SDPには次の利点があります：

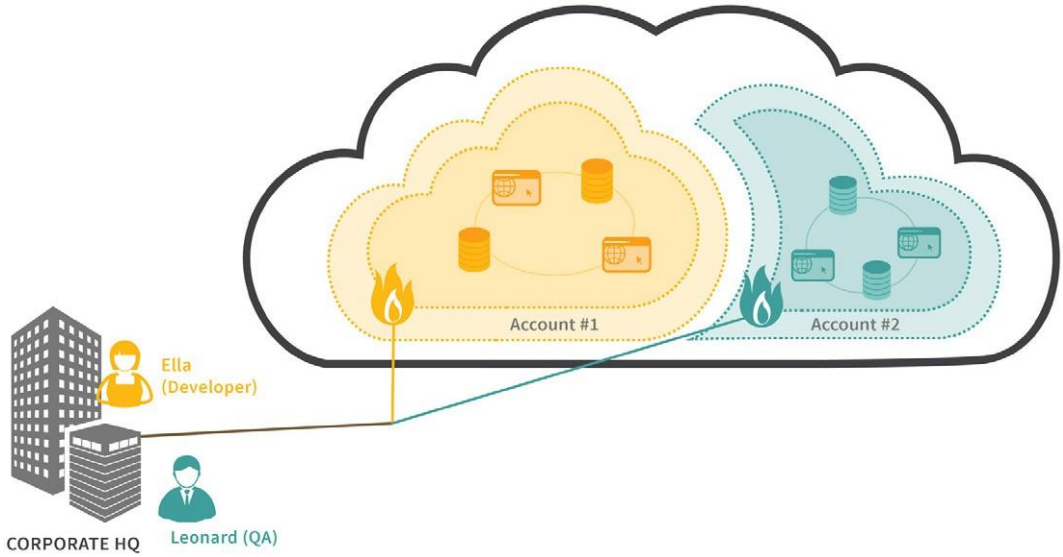
- リスクが高く脆弱なIPMIネットワークへの安全で制御されたアクセス
- どのユーザーがいつこれらのシステムにアクセスできるかをきめ細かく制御
- ユーザーセントリックのシンプルなポリシーによる制御
- IAMとの統合による強力な認証の実施
- セキュリティやコンプライアンスを犠牲にすることなく、緊急/サーバー停止状況への迅速なアクセスを実現
- コンプライアンスの目的で誰がどのシステムに（いつ）アクセスしたかについての包括的かつ詳細なログ
- データセンターの成長とダイナミクスに対応するソリューション

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ユースケース：複数のエンタープライズアカウントにわたるアクセスの制御

このシナリオでは、組織はIaaSプロバイダー内に複数の異なるアカウントを持っています。 これは、セキュリティまたはコンプライアンス上の理由から意図的なものであるか、あるいは異なるグループが個別にアカウントを設定しているために偶然発生した可能性もあります。下の図は2つのアカウントを示していますが、特にアプリケーションごとに1つのアカウントを利用している場合など、通常では組織にはさらに多くのアカウントが存在します。

企業からクラウドへの接続は、下の図に青緑色で示されていますが、共有のクラウド直接接続（事実上、専用のサイト-クラウド間VPN）またはインターネットを介してルーティングされます。 どちらの場合も、次の図に示すように、共通の課題があります。



要件：これらのアカウントによってどのユーザーがどのサービスに一貫して効率的にアクセスできるかを制御すること。

課題：個別のアカウントでは、統合された請求であったりクラウド管理コンソールへの共有IAMアクセスをもつ場合がありますが、クラウドファイアウォールは共有されません。

SDPなし	SDPあり
アプローチ：組織がリソースへのユーザーアクセスを厳しく制御しようとする場合、上記の使用例で指摘された問題が残り、実際にはアカウント数の増加によってひどくなります。クラウドAPIを使用して多くのセキュリティグループを更新することでこの一部を自動化しようとしても、最終的にはやはり、IPアドレスセントリックなクラウドファイアウォールモデルにおいてユーザーセントリックなセキュリティ制御を試みなければならないという問題に直面します。	ウドファイアウォールの前にSDPゲートウェイを配置することで、組織はセキュリティを即座に簡素化および改善できます。 各アカウントのクラウドファイアウォールにおいては、保護されたサービスへのトラフィックをSDPゲートウェイからのみ許可することによって、実質的に単純なルールへと減らすことができます。
結果：結果として、組織は実際にはネットワーク上のすべてのユーザーにすべてのクラウドリソースを開放し、認証を利用してそれらを保護します。 そしてこれは、上記で説明したように、強力なセキュリティやコンプライアンスのための対応ではありません。	結果：使用中のクラウドアカウントの数や種類に関係なく、SDPポリシーを一貫して適用できます。 これらのポリシーはコンプライアンスの完全なトラッキングを可能にし、企業のIAMシステムと一貫して統合されます。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

まとめ

このユースケースでは、SDPは次の利点を提供します：

- セキュリティを犠牲にすることなく、複数のクラウドプロバイダーアカウントが使用可能です。
- 手作業でのクラウドファイアウォールルールの管理を排除します。
- すべてのユーザーについて、すべてのアカウントに対する一貫したアクセスポリシーを適用します。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

SDP仕様の強化に関する推奨事項

この調査の過程において、SDPに関する専門家の視点を慎重に取り入れながら、利用可能なSDP実装とアーキテクチャによって一般的にサポートされている実際のユースケースを調べました。 必然的に、これらのユースケースと要件は、現在の（v1）SDP仕様を超えて拡張されました。

これまでの議論、会話、および執筆において、SDPの完全な実装に必要であると認識する部分に注意を払いました（SDPベンダー製品が解決した問題が示すとおり）。

これらのトピックの多くは、IaaSだけでなくSDP仕様全体の一部として必要でありこの文書の範囲外であると判断しましたが、現在進行中のSDP v2の仕様に含めるにはおそらく適しています。 私たちは是非その作成に参加し、次のトピックに関する議論をしたいと考えています：

- ネットワーク権限のポリシーモデル
- IAM統合
    - ポリシーモデルの一部としてのディレクトリ属性とSAMLアサーション
    - ステップアップ認証トリガー
- 高可用性と負荷分散のアプローチ
- HTTP以外の追加のネットワークプロトコル（SSH、UDPなど）のサポート
- ディープパケットインスペクションおよび/またはセッションプロキシ
- 既存のエンタープライズ環境への段階的な導入に関する考慮事項
- クラウドおよびオンプレミス環境のインスタンスメタデータと自動検出
- SDPコスト削減/ ROIモデル
- サーバー間トラフィック（東西トラフィック）のマイクロセグメンテーションの議論
- SDPシステムの残存リスクと潜在的な脆弱性（中間者攻撃、コントローラまたはゲートウェイの侵害など）

© Copyright 2017, Cloud Security Alliance. All rights reserved.

ハイブリッドおよびマルチクラウド環境

ほとんどの組織は、近い将来に複雑で異機種混在のIT環境を持つことになります。 セキュリティチームは、これを排除すべき問題と見なすのではなく、ビジネスの一環として、この豊富さ、およびそれに関連する複雑さを受け入れる必要があります。 ビジネスのさまざまな領域にはさまざまな要件があり、今日の企業のすべての部分に「1つのサイズですべてに適合する」ITインフラストラクチャが存在することはないと予測できます。

つまり、セキュリティチームは、これらの環境全体で一貫したセキュリティを提供する適切な種類のツールとテクノロジーを見つける必要があります。システム管理、自動化、エンドポイント管理などのプラットフォーム固有のツールは常に存在しますが、セキュリティの観点からすると、組織にとって重要なことは、ユーザーセントリックのポリシーとプロセスを確立し、それがプラットフォーム全体で一貫して機能することであると考えます。

たとえば、組織は、どのIDがどのシステムにアクセスできるかに関するポリシーとプロセスを定義および適用できる単一のプラットフォームを、明らかに必要としています。 このプラットフォームは、オンプレミスの物理的で、同じ場所に配置され、仮想化されたプライベートクラウドとパブリッククラウドのリソース全体で一貫して動作する必要があります。 そうしなければ組織の、複雑さ、リスク、および運用コストが増加されることになります。

SDPは、ユーザーセントリックであり基盤となるコンピューティングプラットフォームに依存しないため、またネットワークレベルで強力なアクセス制御を実施できるため、企業が今日の複雑な環境でセキュリティ目標を達成するための最適な方法であると確信しています。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

サイドバー: 代替のコンピュートモデルとSDP

いわゆる「サーバーレス」コンピューティングモデルの可用性と採用が着実に増加し、それによりクラウドプロバイダーは新しいタイプの Platform-as-a Service をサービスに追加しています。 これらは、リレーショナルデータベースやメッセージキューイングなどの従来の機能に対する「as-a-service」の発展から、より新しい「function as a service」（AWS Lambda、Azure Functions、GoogleのCloud Functionsなど）まで、さらにIoTを中心とした新しい製品に至るまで、さまざまです。

これらすべての共通点は、従来のOSをまったく顧客に公開しないことです。つまり、解決すべきネットワークアクセス制御の問題は、IaaSプラットフォームに関わる問題とは異なる可能性があります。

場合によっては、これらのサービスは、ここで説明したIaaSシナリオと完全に一致します。 たとえば、relational databases as a service は、まさにSDPによる防御の恩恵を受けるサービスのタイプです。 実際、多くのIaaSプロバイダーは、IaaSインスタンスと同じネットワークアクセスモデルを使用してリレーショナルインスタンスへのアクセスを制御しているため、ここで説明したSDPアプローチとまさしく関連しています。

他の場合では、これらのサービスのいくつかは他のセキュリティモデルを使用します。 たとえば、「function as a service」は、一般に公開されているURLまたは何らかのAPIゲートウェイを介してアクセスできる傾向があります。 これらのサービスは、クライアントゲートウェイサービスモデルが意味をなさないため、現在ではSDPアプローチと互換性がないかもしれません。これらのモデルはSDPと同様に進化し、これは今後の活動にとって興味深い領域になると考えています。

いずれの場合でも、組織がこれらの代替コンピューティングモデルの一部を使用（または検討）している場合は、あなたやセキュリティチームは、そのツールのセキュリティモデルと、それが他のセキュリティアーキテクチャとどのように適合するかを、開発者と相互に理解するようにしてください。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

サイドバー: コンテナとSDP

コンテナは、急速に成長しているもう1つのトレンドであり、多くの組織が、高速のDevOpsメソドロジー/ライフスタイルを可能にする基盤テクノロジーとして採用しています。 コンテナには、いくつかの興味深い新しいセキュリティとアクセスの課題があります。（もちろん）さまざまなコンテナおよびクラスター化テクノロジーのためのさまざまなネットワークアクセスモデルがありますが、極端に単純化すると、次のいずれかにマッピングされます：

- 各ポッド（単一のOSプロセス内のコンテナのグループ）は、コンテナによって共有されるパブリックIPを取得します（Kubernetesモデル）
- 各コンテナは、ポッドのパブリックIPにNAT変換されたプライベートIPを取得します。（Dockerモデル）。

どちらの場合でも、SDPを効果的に適用できます。 ポッドとそのコンテナは、SDPゲートウェイの背後に配置でき、SDPポリシーを定義してユーザーのサービスアクセスを制御します。保護されたサービスは、IaaS環境と同様に、IPアドレスまたはメタデータに紐づけられ、コンテナ環境内で動的に解決されます。また、ポートからコンテナへのポッド固有のマッピングは、SPDゲートウェイの背後で問題なく機能し、SDPの追加による影響はありません。

もちろん、コンテナ内のネットワーキングには別のアプローチもあります。そのため、チームが使用しているツールを注意深く確認してください。しかし、一般に、上記の主流のアプローチはSDPと互換性があり、実際にはSDPでうまく機能します。 これは、将来の研究と検証の恩恵を受ける別の領域です。

© Copyright 2017, Cloud Security Alliance. All rights reserved.

結論と次のステップ

企業、サービスプロバイダー、あるいは個々の専門家のいずれであっても、この研究があなたにとって有用であるとお判り頂けたのであれば幸いです。 理想としては、この文書が、あなたのIaaS環境に関連する特定のネットワークアクセスの課題の理解を深め、SDPがこれらの問題を解決する方法であると認識頂けたなら、と。
IaaSリソースを、オンプレミスネットワークの単なる拡張ではないものと考えて頂きたいと思います。 クラウドを採用することには多くの利点がありますが、多くの場合、最大限に活用するには多くの変更が必要です。-この研究報告がクラウドの考え方を変えるのに役立ち、ユーザーがこれらのリソースにアクセスする方法を、より安全で、より柔軟で、より効率的なものに変える機会になればと願っています。

私たちは、SDPがセキュリティにおいて非常に重要な進歩であると確信しています。SDPは、初めて動的にIDセントリックなセキュリティをネットワークレイヤーで適用できるようし、また、企業は今日のセキュリティとビジネスのニーズを満たすために、SDPを熱心に広く取り入れています。 ガートナーはこう述べています。

> *「接続性の複雑さにより、古いセキュリティへの妥協が持続不可能になり、複雑さ、トラフィック量、および柔軟性に対するデジタルビジネスのニーズを満たす一方で古いモデルに固有の脆弱性を回避する、新しいアプローチの必要性が高まっています。」*[19]

もちろん、SDPがすべてのセキュリティ問題を解決するわけではありません。単にSDPの対象外となる情報セキュリティの分野は多くあり、また、特定の製品に関連付けられたり、企業の特定の実装によって生じる可能性のある残存リスクもあります。

しかし、全般的に見れば、SDPは、Infrastructure-as-a-Service環境に特定の適用性を備えることでセキュリティを改善するための斬新で説得力のあるアプローチであると信じており、この文書によりあなたが同じく納得して頂けることを願っています。

19 Gartner: It's Time to Isolate Your Services From the Internet Cesspool, 30 September 2016.

© Copyright 2017, Cloud Security Alliance. All rights reserved.