Microsoft Azure の ネットワーク セキュリティ

要約

このドキュメントは、お客様が仮想インフラストラクチャ、データ、Microsoft Azure にデプロイされたアプリケーションをより適切な形で保護できるように、ネットワーク通信のセキュリティを強化する方法を示したガイドです。

このドキュメントは、次のユーザーを対象としています。

- Azure でのアプリケーションのデプロイメントに関心のある IT 担当者およびネットワーク管理者
- Azure で動作するアプリケーションの作成に関心のある開発者
- Azure で新規または既存のサービスのサポートを検討している技術意思決定者 (TDM)

注: このドキュメントで紹介されている推奨事項には、データ量、ネットワーク使用量、コンピューティング リソース消費の増大や、ライセンス コストまたはサブスクリプション コストの追加を伴うものがあります。

第 3 版、2015 年 2 月発行

目次

1 概要

Microsoft Azure (Azure) のネットワークは、Virtual Machines (VM) 間の安全な接続や、オンプレミスのデータセンターとクラウド間の接続に必要なインフラストラクチャを備えています。

Azure のネットワーク サービスは、柔軟性、可用性、回復性、セキュリティ、整合性を最大限に高める仕様となっています。このホワイト ペーパーでは、Azure のネットワーク機能の詳細について説明し、ネイティブのセキュリティ機能を利用して情報資産を保護するための情報を提供します。

2 Azure Virtual Machines を安全に利用するためのガイドライン

Azure は、共有インフラストラクチャを活用するマルチテナント プラットフォームとして、世界中の 80 以上のデータセンターの何百万というお客様を同時にサポートしています。Azure の共有インフラストラクチャでは何億ものアクティブな VM をホストしているため、ネットワーク トラフィックのセキュリティと機密性を保護することは非常に重要です。

Azure Virtual Network では、論理的分離、ファイアウォール、アクセス制御、認証、暗号化を組み合わせて、転送中のお客様のデータを保護します。マイクロソフトによる Azure データセンターの運用には、ISO 27001、SOC 1、SOC 2 といった業界標準のコントロール フレームワークに基づく、包括的な情報セキュリティ ポリシーとプロセスを導入しています。そのうえで、第三者監査機関より、Azure インフラストラクチャの物理的および仮想的側面について、マイクロソフトがこれらの標準に準拠しているとの認定を定期的に受けています。

従来のデータセンター モデルでは、企業の情報技術 (IT) 部門が、ネットワーク設備への物理的なアクセスを含むネットワーク システムの管理を行います。ネットワーク トポロジの物理的な変更、ルーター設定の変更、ファイアウォール デバイスのデプロイメントなど、デプロイメント、構成、管理に関する作業は、企業の従業員や請負業者が担当します。

クラウド サービス モデルでは、ネットワークの保護と管理に関する責任をクラウド プロバイダーとお客様で分担します。もちろん、お客様がクラウド プロバイダーのデータセンターに出向いてサーバー ラックの配線を変更するなど、物理的にアクセスできるわけではなく、ゲスト オペレーティング システム (OS) のファイアウォール、Virtual Network Gateway の構成、仮想プライベート ネットワークなどのツールを使用して、論理的にクラウド環境を保護、管理します。このように物理的な側面と論理的な側面で分担するため、Azure によって提供される基本的なセキュリティ機能は、お客様にとってインフラストラクチャを構築するうえで欠かせません。

2.1 プライベート ネットワーク

パブリック クラウド上のお客様のインフラストラクチャを論理的に分離することは、セキュリティを維持するうえで不可欠です。これを実現するために、Azure では主に分散型の仮想ファイアウォールを使用します。また、お客様は論理的に分離された複数のプライベート ネットワークをデプロイ

することが可能です。このように下位レベルで分割されたネットワークは通常、以下の 2 種類に分類されます。

- **デプロイメント ネットワーク**: それぞれのデプロイメントはネットワーク レベルで相互に分離されています。あるデプロイメントの中に存在する複数の VM は、プライベート IP アドレスを使用して相互に通信できます。
- **仮想ネットワーク**: それぞれの仮想ネットワークは相互に分離されています。同一の仮想ネットワークには、同一サブスクリプション内の複数のデプロイメントを割り当てることができます。この場合、各デプロイメントはプライベート IP アドレスを使用して相互に通信できます。

図 1 は、仮想ネットワーク トポロジの例です。

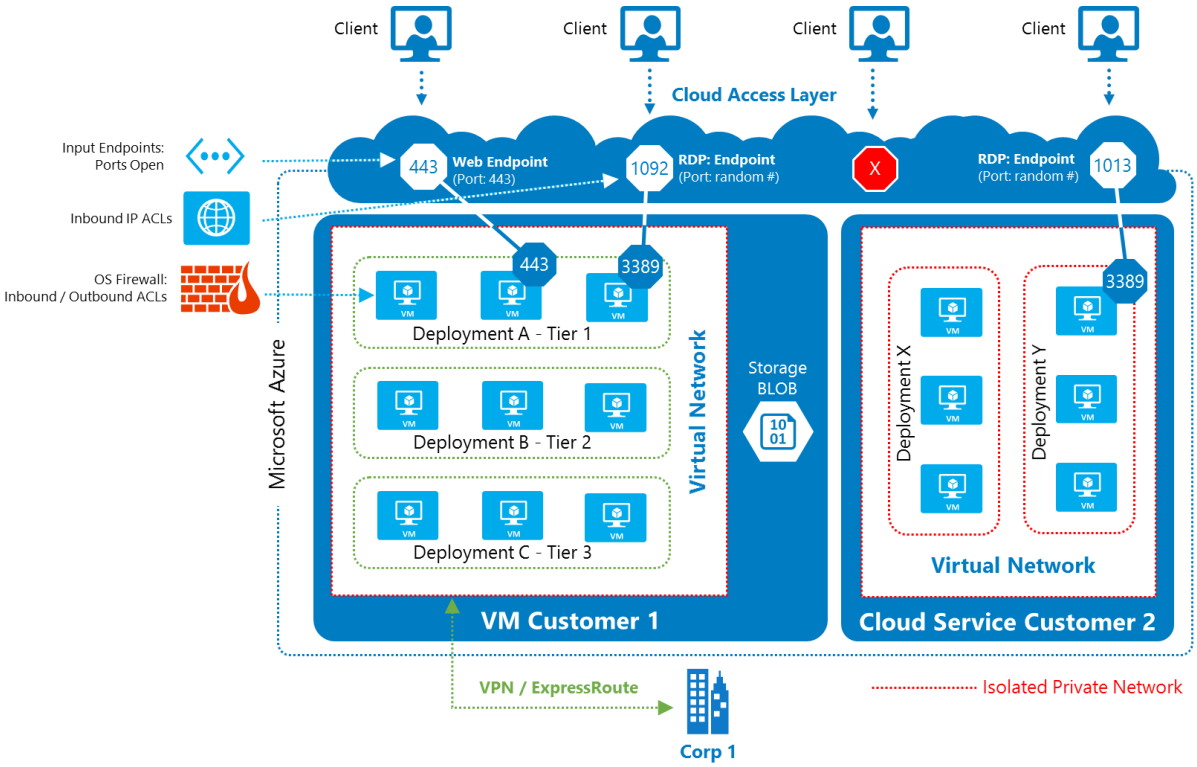

図 1: Azure でホストされている分離された多層 IaaS アプリケーションの例

ネットワーク管理者は、オンプレミスのプライベート ネットワークを管理する場合と同様の方法で、これらの分離されたプライベート ネットワークを管理できます。

Azure プライベート ネットワークのネットワーク セキュリティを管理するメカニズムは Azure Cloud Access Layer によって提供されます。このレイヤーは、インターネットに接続されている企業ネットワークの境界と同様の役割を果たします。Cloud Access Layer にはファイアウォール、ロード バランサー、ネットワーク アドレス変換 (NAT) 機能が含まれ、これらの機能の管理はお客様の管理者が行います。

2.1.1 インターネット通信の許可

既定では、プライベート ネットワーク内の VM はインターネットからのトラフィックを受信しません。管理者がインターネット通信を許可するには、以下の 3 種類の方法があります。

- 入力エンドポイントを定義することによって、デプロイメントの分離されたネットワークの外部からの受信トラフィックを許可する VM のポート マッピングを指定できます。ネットワークの外部とは、インターネットや、Azure 内に存在する他の VM を指します。
- さらにセキュリティを強化する場合は、Azure Security Groups を定義することによって、Virtual Network の外部からの受信トラフィックを許可する IP アドレスを指定できます。ただし、入力エンドポイントにはアクセス制御リスト (ACL) と Security Groups のいずれか一方しか定義できない点に注意してください。
- Virtual Machines にインスタンス レベルのパブリック IP アドレスを割り当てることができます。この場合、VM のすべてのポートにインターネットからのアクセスが許可されます。

注: このドキュメントで「受信トラフィック」と言った場合には、インターネット上のコンピューター、または Azure 内のお客様のプライベート ネットワークの外部に存在するコンピューターから送信されたトラフィックを指します。これは、「要請されていない受信トラフィック」とも呼ばれ、要求に対する応答としての受信トラフィック (「要請された受信トラフィック」) と区別されます。

2.1.2 通信の安全性確保

プライベート ネットワーク内の VM 間通信の安全性確保	デプロイメント ネットワーク内に配置された Virtual Machines は、プライベート IP アドレスを使用して内部的に通信できます。単一サブスクリプションの複数のデプロイメントに配置されている VM 間の通信は、Virtual Network によってセキュリティを強化することが可能です。 アプリケーションが VPN などの内部プライベート ネットワーク経由で機密データを送受信する場合、IPsec や SSL/TLS などのアプリケーション レベルの暗号化技術を使用してデータを暗号化できます。さまざまな業界規制および標準への準拠など、機密性の高い要件やプライバシーの要件に対応する必要があるお客様の場合は、リージョン内のプライベート ネットワークを介した VM 間のすべての通信を確実に暗号化することをお勧めします。 Virtual Network の暗号化の構成についての詳細は、Azure Virtual Network に関する MSDN ドキュメントを参照してください。

インターネットからの受信トラフィックに対する安全性確保	既定では、リモート管理ポートの通信を除き、Azure 管理ポータルで作成された VM に対するインターネットからの受信トラフィックはすべてブロックされます。 管理者は、インターネットからの受信トラフィックを許可する VM ポートおよび IP アドレスを指定できます。さらに、以下に挙げる複数の方法で構成を変更することで、インターネットから VM または VNET のポートへのリモート アクセスのセキュリティをネットワーク レベルで確保することができます。 • Cloud Access Layer に入力エンドポイントを定義することで、必要な場合にのみポートを開放する。入力エンドポイントに対してアクセス制御リスト (ACL) を指定し、VM がトラフィックを許可する送信元の IP アドレスを制御できます。 • Security Groups を定義することで、Virtual Network 内の特定の VM への受信トラフィックを制御する。ただし、入力エンドポイントには ACL と Security Groups のいずれか一方しか定義できません。 • VM 上でサードパーティ製のプロキシ ファイアウォール (Barracuda Web Application Firewall Vx や NG Firewall Vx 仮想アプライアンスなど) を実行し、他の VM へのトラフィックをフィルタリングする。VM を Virtual Network に追加し、プロキシ ファイアウォールのポートに対して入力エンドポイントを定義します。 • ゲスト OS VM 内のファイアウォールの内部で開放するポートを定義する。 入力エンドポイントまたは IP アドレスを公開する場合は、VM がインターネット上のオープンな環境で実行されている場合と同じセキュリティ モデルに従うことを推奨します。アプリケーションが入力エンドポイントに対して機密データを送受信する場合、すべての入力エンドポイントでサーバーおよびクライアントの認証を利用し、通信を暗号化することを推奨します。アプリケーションがパブリック ネットワーク経由で機密データを送受信する場合 (リージョン内のパブリック IP アドレスを使用する場合を含む) は、SSL による暗号化などのアプリケーション レベルの暗号化技術を使用して通信を暗号化することを推奨します。
サブスクリプション間の通信の安全性確保	複数のサブスクリプションを所有している場合や、異なるサブスクリプションに配置された VM 間で通信を行う必要がある場合は、通信に仮想パブリック IP アドレスを使用するように VM を構成できます。さらに、指定した VM 間でのみ接続の開始を許可するには、入力エンドポイントに対して IP ACL を構成する必要があります。

IP アドレスの ACL が変更されないように、仮想パブリック IP アドレスには予約済み IP アドレスを使用する必要があります。

IP アドレス ACL の構成の詳細については、「ネットワーク アクセス制御リスト (ACL) について」を参照してください。

オンプレミス ネットワークへの通信の安全性確保

ワークロードで Azure Virtual Network とオンプレミス システムの間でセキュアな通信が求められる場合、Virtual Network Gateway を使用して対象のチャネルを保護することが理想的です。これには、2 種類のデプロイ方法があります。

1. **内部型多層アプリケーション**: 多層アプリケーション (Web ベースの記録処理システムなど) を Azure にデプロイします。この場合、アプリケーションにはインターネットからの受信接続は不要ですが、図 2 に示すように、お客様のオンプレミス ネットワークのサーバーおよびアプリケーションとの接続が必要です。

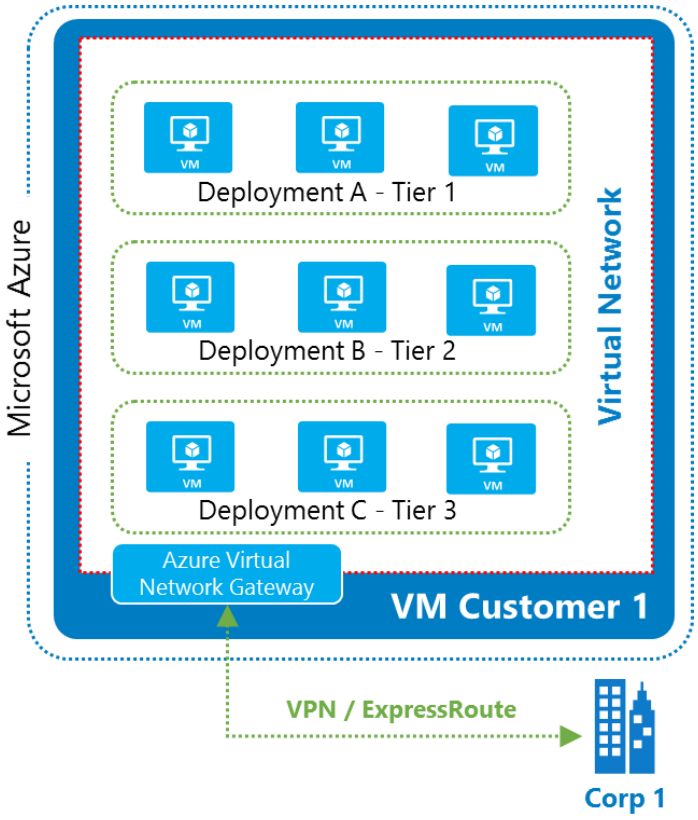

図 2: 企業ネットワークと Microsoft Azure 間の VPN 接続

VNET 間接続を構成する必要がある場合、Virtual Network を構築し、そこにアプリケーション層の VM を追加できます。ただし、入力エンドポイントを定義する必要はありません。加えて、以下を実行することを推奨します。

- 下記の「Virtual Network 内の VM の分離による多層防御」セクションの説明に従って、リモート管理入力エンドポイントを削除またはロック ダウンし、管理エンドポイントの安全性を確保する。
- 企業ネットワーク宛てのトラフィックが VPN 接続を経由して企業ネットワーク上の目的のサーバーまたはネットワーク デバイスへ流れるように Virtual Network Gateway または ExpressRoute を構成する。また、Site-to-Site VPN トンネルを使用する場合は、Forced Tunneling を利用することで、すべてのインターネットへの送信トラフィックが VPN トンネルを経由するように構成できます。

2. **外部公開型多層アプリケーション**: 多層アプリケーションを Azure にデプロイします。フロントエンド層にはインターネットからの受信接続 (SSL ポート 443 番を使用) が必要です。バックエンド層にはインターネットからの受信接続は不要ですが、図 3 に示すように、お客様の企業ネットワークとの接続が必要です。

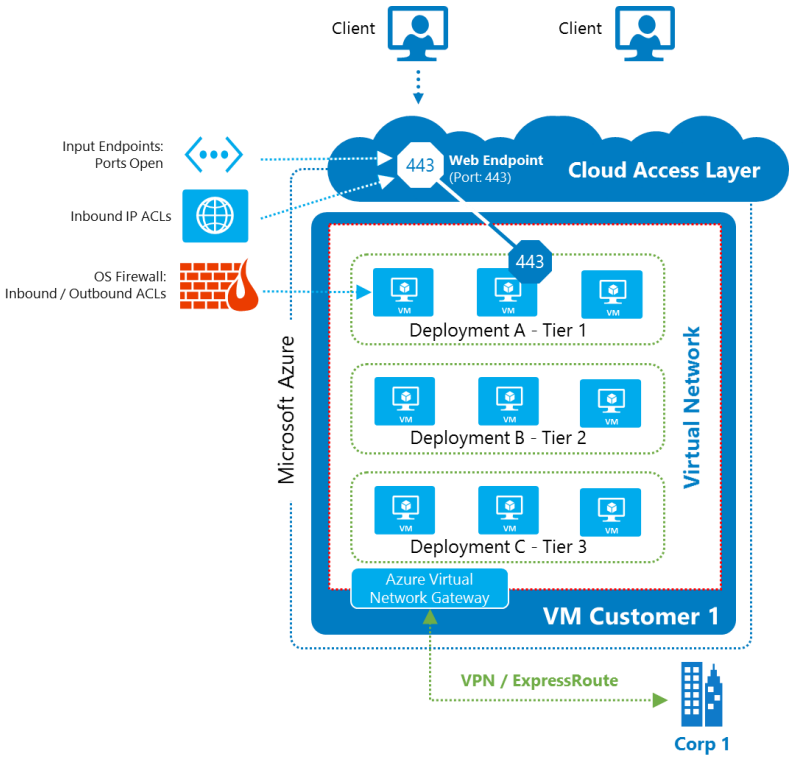

図 3: インターネットに接続されたエンドポイントの追加による、フロントエンド層のインターネット アクセス許可

この場合、以下を実行することを推奨します。

- 各アプリケーション層に適切な VM を配置した Virtual Network を構築する。
- フロントエンド層の VM に対するインターネットからの受信トラフィック用の入力エンドポイントを定義する。
- すべての VM のリモート管理入力エンドポイントを削除またはロック ダウンする。
- 企業ネットワーク宛てのトラフィックが VPN 接続を経由して企業ネットワークへ流れるように Virtual Network Gateway を構成する。

Virtual Network Gateway は、Virtual Network とお客様の VPN デバイス間に IPsec トンネルを確立し、トラフィックをルーティングします。この VPN には、ハードウェアの VPN デバイスまたはソフトウェア VPN (Windows Server 2012 のルーティングとリモート アクセス サービスなど) のいずれも使用できます。

Azure 内に仮想プライベート ネットワークを作成すると、オンプレミス ネットワークを Azure に安全に拡張できます。この接続には、Site-to-Site VPN と Point-to-Site VPN のいずれも使用できます。

Virtual Network Gateway を使用してリージョン内の VPN を企業ネットワークにインターネット経由で接続している場合、この通信の暗号化には、既定で AES-256 などの標準が使用されます。ただし、構成は企業ネットワークの Site-to-Site VPN ゲートウェイに依存します。

リージョン内の仮想プライベート ネットワークが Azure ExpressRoute などの直接接続テクノロジを使用して企業ネットワークに接続している場合、このトラフィックは MPLS ネットワーク上の ISP を経由するため、一般的に安全性がより高いと考えられます。追加のセキュリティ要件に対応する必要があるお客様の場合は、仮想ハード ディスク (VHD) ファイルを移動する際に、IPsec、TLS、または BitLocker などのその他のアプリケーション レベルの暗号化技術を使用して通信を暗号化することを推奨します。

Virtual Network Gateway の構成の詳細については、「管理ポータルでの Virtual Network Gateway の構成」を参照してください。

2.2 セキュリティ管理と脅威からの防御

Virtual Machines のリモート管理の安全性確保	管理者は、Azure 管理ポータルまたは Windows PowerShell のいずれかを使用して、VM を作成することができます。 Azure 管理ポータルを使用して VM を作成した場合、リモート デスクトップ プロトコル (RDP) およびリモート Windows PowerShell のポートが既定で開放されます。その後、パスワードへの辞書攻撃のリスクを減らすために、Azure 管理ポータルによって RDP およびリモート Windows PowerShell にランダムなポート番号が割り当てられます。 Windows PowerShell で VM を作成した場合は、RDP およびリモート Windows PowerShell のポートを明示的に開放する必要があります。 • RDP およびリモート Windows PowerShell のポートをインターネットに対して開放したままにすることは可能ですが、最低でも RDP およびリモート Windows PowerShell 接続の作成が許可されているアカウントを強力なパスワードで保護する必要があります。 • また、前述したように一般的なオプションを使用して、インターネットからの受信トラフィックの安全性を確保することを検討してください。
DDoS からの保護	Azure プラットフォーム サービスを保護するために、マイクロソフトは Azure の継続的な監視プロセスの一環として分散型サービス拒否 (DDoS) 攻撃に対する防御システムを提供し、侵入テストを実施することでさらなる改善を続けています。Azure の DDoS 防御システムは、外部からの攻撃に耐えるだけではなく、他の Azure テナントからの攻撃にも対応しています。 1. ネットワーク層への大容量攻撃: これは、ネットワークに膨大な量のパケットを送り込むことで、ネットワーク パイプやパケット処理機能を麻痺させる攻撃です。Azure の DDoS 防御テクノロジでは、お客様の環境がこれらの攻撃による影響を受けないように、SYN Cookies、レート制限、接続制限などの検出および緩和手法を提供しています。 2. アプリケーション層への攻撃: この攻撃は、お客様の VM に対して実行される可能性があります。Azure のインフラストラクチャでは、お客様のアプリケーションで想定される動作を判断できないため、対策を提供したり、個々のお客様のデプロイメントに影響を与えているネットワーク トラフィックを積極的にブロックしたりすることはありません。この場合には、オンプレミスのデプロイメントと同様に、以下の対策を講じることができます。 • 負荷分散されたパブリック IP アドレスの範囲内で複数の VM インスタンスを実行する。

	• Web アプリケーション ファイアウォール (WAF) などのファイアウォール プロキシ デバイスを使用して、VM 内で実行中のエンドポイントへのトラフィックを終了させて転送する。これにより、低レート攻撃、HTTP 攻撃といった幅広い DoS 攻撃やその他の脅威からアプリケーション層をある程度保護することができます。Barracuda Networks など、侵入の検知と防御の両方を実行する仮想化ソリューションも存在します。 • 特定の DoS 攻撃を防御する Web サーバー アドオンを使用する。 • 特定の IP アドレスから VM へのパケット送信を禁止するネットワーク ACL を使用する。 アプリケーションが攻撃を受けていることが判明したら、すぐに Azure カスタマー サポートに連絡し、支援を要請してください。このようなご要望には Azure カスタマー サポートの担当者が優先的に対応します。
内部 DNS を使用した内部 VM 名の安全性確保	Cloud Services 内に存在する VM に対して名前でアドレスを割り当てられるように、Azure では内部 DNS サービスを使用できます。VM 名は、Cloud Services 内でプライベート IP アドレスに名前解決されます。この際、Cloud Services 全体、さらには同一サブスクリプション内でプライバシーが保護されます。 プライベート IP アドレスは、Cloud Services のロールに割り当てられたものと Virtual Machines に割り当てられたもののどちらも、クラウド インフラストラクチャの修復中に変更される可能性があります。このため、Azure でホストされているサービス内のロール間での通信は、IP アドレスではなく DNS 名で解決する必要があります。ただし、カスタム IP アドレス空間に Virtual Network が使用されている場合は、このルールの例外となり、IP アドレスは静的アドレスになります。また、プライベート IP アドレスは変更される可能性があるため、クライアントでは DNS 応答の DNS TTL (Time-to-Live) 値を維持する必要があります。
Virtual Network 内の VM の分離による多層防御	Network Security Groups を使用すると、Virtual Network 内のネットワーク層のイントラネット トラフィックをセグメント化することができます。Network Security Groups は Virtual Network のサブネットにも適用できます。 図 4 は、多層アプリケーションのデプロイメントの例です。

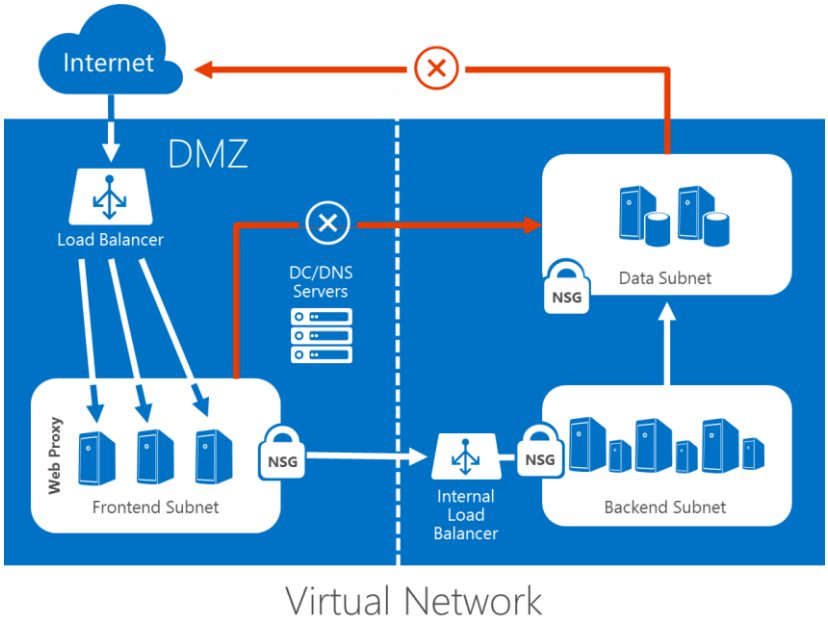

図 4: 多層アプリケーションの VNET に Network Security Groups を使用した例

さらに、Network Security Groups (NSG) は、イントラネット トラフィックのセグメント化だけでなく、インターネットとの間で送受信されるトラフィックの制御にも使用できます。

Network Security Groups は、VM またはサブネットのいずれか、また場合によってはその両方に対して適用できます。NSG には、以下のような重要な特徴があります。

- 図 5 に示すように、NSG のルールには 5 つのタプル (送信元 IP、送信元のポート番号、送信先 IP、送信先のポート番号、プロトコル) が含まれます。
- NSG のルールはステートフルです。つまり、特定のポートでのトラフィックを許可する受信ルールがある場合、同一ポートを流れるパケットに対して、これに対応するルールを送信側でも作成する必要はありません。
- NSG には、既定で Virtual Network 内の接続およびインターネットへの送信アクセスを許可するルールが含まれます。この既定のルールは、お客様の管理者が上書きすることができます。
- NSG では、優先度に従ってルールが処理されます。値が小さいルール (優先度高) は、値が大きいルール (優先度低) よりも先に処理されます。
- Azure では、パブリック IP アドレス空間を参照する既定のタグ (INTERNET や VIRTUAL_NETWORK など) が用意されています。このタグは、Virtual Network 外部、またはお客様のネットワーク全体のアドレス空間の外部に存在するアドレス空間を参照し、アクセス制御ルールの一部として使用できます。

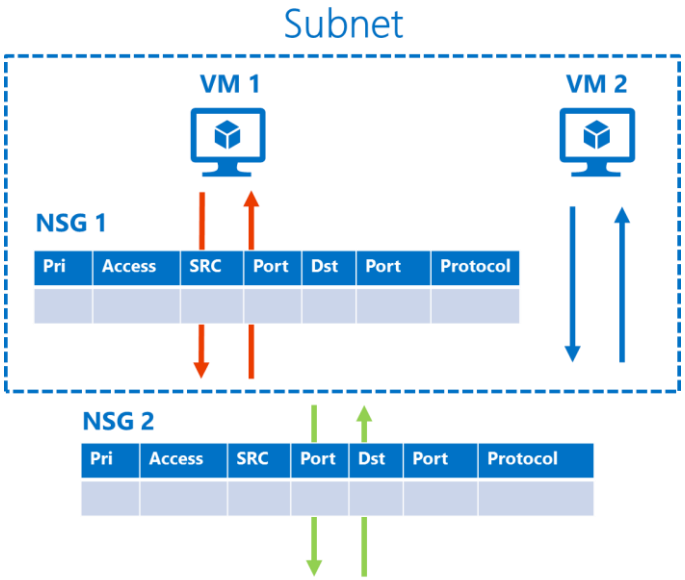

図 5: Virtual Network で処理される 5 つのタプルを含むルール

VM から Microsoft Azure SQL Database への通信の安全性確保

Microsoft Azure SQL Database には、受信トラフィックをフィルタリングするファイアウォールが組み込まれています。既定では、SQL Database との通信はすべてブロックされます。データベースと通信できるようにするには、Azure 内の VM のパブリック IP アドレスとデータ ソースの通信を許可するように、Azure SQL Database でファイアウォール ルールを定義する必要があります。

それに加えて、仮想パブリック アドレスが変更されるたびに IP アドレスの ACL を更新する必要があります。その結果、サービスで障害が発生する可能性があり、管理者の負担は増えます。また、仮想パブリック IP アドレスは、VM がシャットダウンされてコンピューティング リソースの割り当てが解除されたり、デプロイメントが削除されたりした場合に変更されることがあります。

ただし、インプレース アップグレードを使用すると、VM のパブリック IP アドレスを変更せずに新バージョンのサービスをデプロイできます。

IP ACL の構成の詳細については、「ネットワーク アクセス制御リスト (ACL) について」を参照してください。SQL Database のファイアウォールを構成してサーバー レベルとデータベース レベルの両方でルールを指定する方法については、次の記事を参照してください。

- Microsoft Azure SQL Database ファイアウォール
- sp_set_firewall_rule (Microsoft Azure SQL Database) (英語)

3 Azure Cloud Services を安全に利用するためのガイドライン

上記の Azure VM および VNET 向けのガイドラインは、Azure Cloud Services の Web ロールと Worker ロールにも適用されます。

VM と同様に、Azure 管理ポータルで作成された Cloud Services の各ロールでは、インターネットおよびリモート管理ポートからの受信トラフィック フローが既定でブロックされます。リモート デスクトップ サーバーのロールを有効にすると、RDP のポートが開放されます。RDP のポート番号には、一般的なスキャニングやパスワード辞書攻撃のリスクを減らすために、ランダムな数字が割り当てられます (図 6 を参照)。

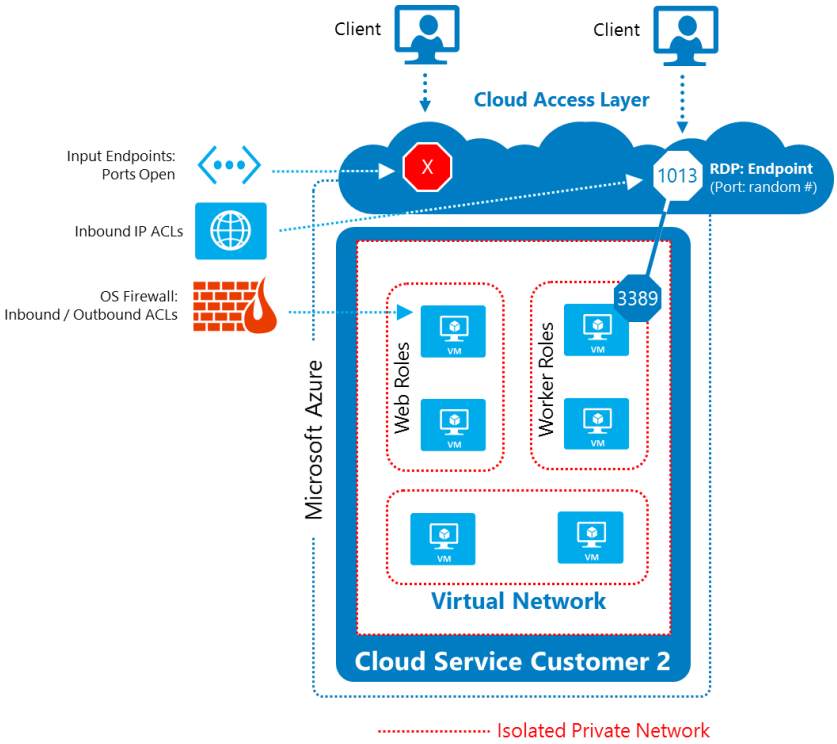

図 6: Azure Cloud Services の Virtual Network のトポロジ

RDP のポートをインターネットに対して開放したままにすることは可能ですが、最低でもロールを強力なパスワードを使用するアカウントで保護する必要があります。RDP を使用する場合には Azure 管理ポータルから RDP のポートを有効化しますが、使用後はこのポートを無効化してください。

同様に、他のポートを開放する場合には、必ずサービス定義ファイル (.csdef) で WebRole スキーマまたは WorkerRole スキーマの Endpoints 要素を定義してください。詳細については、MSDN の「WebRole スキーマ」および「WorkerRole スキーマ」のガイダンスを参照してください。

4 まとめ

以下の表に、Azure Virtual Network を構成してセキュリティを向上させる方法に関する詳細情報へのリンクを紹介します。

機能	テクノロジ	推奨事項	詳細情報
暗号化	SSL/TLS	インターネットから VM への受信トラフィックの安全性を確保する	http://azure.microsoft.com/ja-jp/documentation/articles/cloud-services-configure-ssl-certificate/
	IPsec	VPN を構成して安全なクロスプレミス接続を確立する	http://msdn.microsoft.com/ja-jp/library/azure/dn133798.aspx
ホストのファイアウォール	IP アドレスの ACL	入力エンドポイントを作成して VM へのトラフィック フローを制御する	http://msdn.microsoft.com/ja-jp/library/azure/dn376541.aspx
分離	ExpressRoute	専用のファイバー リンクを使用してリモート ネットワークのトラフィックを保護する	http://azure.microsoft.com/ja-jp/services/expressroute/
	Network Security Groups		http://blogs.msdn.com/b/windowsazurej/archive/2014/11/19/blog-network-security-groups.aspx
	インスタンス レベルのパブリック IP アドレス		http://blogs.msdn.com/b/windowsazurej/archive/2014/11/06/blog-instance-level-public-ip-address.aspx
ゲストのファイアウォール	Windows ファイアウォール	VM にファイアウォールを構成して必要なエンドポイントのみを許可する	http://azure.microsoft.com/ja-jp/documentation/articles/virtual-machines-set-up-endpoints/
	アプリケーション ファイアウォール	サードパーティ製の Web アプリケーション ファイアウォールを使用して IDS/IPS および DDoS からの保護を強化する	http://azure.microsoft.com/ja-jp/marketplace/partners/barracuda/barracudawebapplicationfirewallwaf78/ (英語)
複数の NIC	複数の NIC およびネットワーク仮想アプライアンス		http://blogs.msdn.com/b/windowsazurej/archive/2014/11/14/blog-multiple-vm-nics-and-network-virtual-appliances-in-azure.aspx

5 参考資料

Azure や関連するマイクロソフトのサービス、本ドキュメントで言及した特定の項目に関する一般的な情報は、以下のリソースを参照してください。

- Azure ホーム – Azure の一般的な情報と各種リンク
  - http://azure.microsoft.com/ja-jp/
- Azure ドキュメント センター – 開発者向けのガイダンスと情報
  - http://azure.microsoft.com/ja-jp/documentation/
- Azure トラスト センター
  - http://azure.microsoft.com/ja-jp/support/trust-center/
- Microsoft Security Response Center (Azure を始めとするマイクロソフト製品のセキュリティ脆弱性について報告できます)
  - http://www.microsoft.com/ja-jp/security/msrc/default.aspx
  - または、secure@microsoft.com
- Azure のネットワーク サービス
  - http://msdn.microsoft.com/ja-jp/library/azure/gg433091
- ホワイト ペーパー「Microsoft Azure のネットワーク セキュリティ」の補足ビデオ
  - http://channel9.msdn.com/Blogs/Windows-Azure/Companion-video-for-the-Windows-Azure-Network-Security-white-paper?format=html5 (英語)

6 付録: Azure のネットワーク セキュリティの内部構造

このセクションでは、Azure のネットワーク セキュリティの内部構造について、技術的な詳細を説明します。同時に、Azure に組み込まれているサービスの安全性確保についても説明します。

6.1 複数の保護層

図 7 は、Azure のネットワークを保護するさまざまな層を示しています。

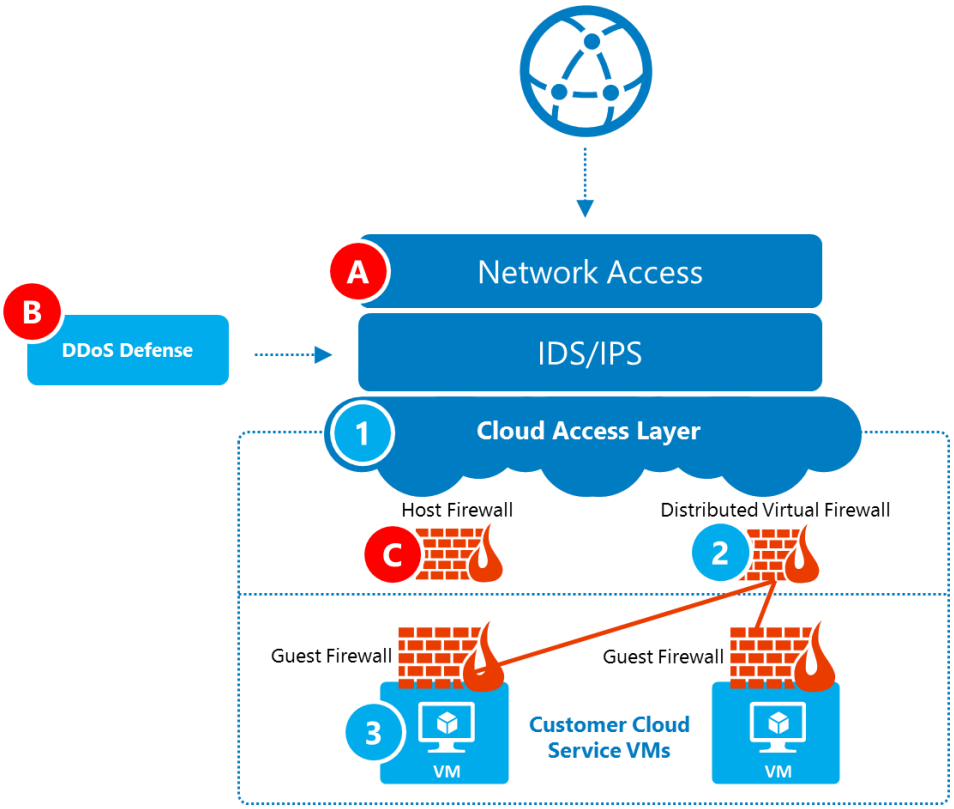

図 7. お客様と Azure インフラストラクチャを保護する複数の防御層

保護は、インフラストラクチャの保護とお客様の保護という 2 種類に分類されます。

1. Azure プラットフォーム サービスのインフラストラクチャの保護
    a. A 層: Network Access Layer により、Azure のプライベート ネットワークをインターネットから分離します。
    b. B 層: Azure の DDoS/DOS/IDS Layer では、オンプレミスのデプロイメントとは異なる手法とテクノロジを使用して、同様のセキュリティ目標を達成します。
    c. C 層: ホストのファイアウォールによってすべてのホストを保護し、VLAN によって重要な資産の保護を強化します。
    d. D 層: オペレーターに対する 2 要素認証などを採用し、セキュリティとプライバシーの要件に準拠します。
2. お客様の保護

a. 1 ～ 2 層: 分散型ファイアウォールにより、ネットワーク レベルでお客様のデプロイメントを他のデプロイメントから分離します。Virtual Network 内には複数のデプロイメントを配置することが可能で、それぞれの Virtual Network は相互に分離されます。Cloud Access Layer は、インターネットからこの分離されたネットワークへのゲートウェイの役割を果たします。また、負荷分散、NAT、ファイアウォール機能が含まれ、これらの機能はお客様の管理者が構成することができます。
b. 3 層: Virtual Network は、オンプレミスのプライベート ネットワークと同様に管理できます。
    i. VM の内部: VM のゲスト OS にはファイアウォール、IDS、DoS ソリューションをデプロイできます。
    ii. 仮想ネットワーク アプライアンス: VM では、プロキシベースのデバイス (WAF など) を実行して、エンドポイント宛てのトラフィックの処理をいったん終了させてから転送できます。これにより、DoS 攻撃やその他の攻撃 (低レート攻撃、HTTP 攻撃、アプリケーション層への攻撃など) に対して、より広範な防御を実現できます。ブリッジ モードのセキュリティ アプライアンスを使用する必要がある場合は、Azure Virtual Network を (VPN 経由などで) オンプレミス ネットワークに接続し、企業内のデバイスを使用してトラフィックを送信することができます。

6.2 分離

Azure では、各デプロイメントのネットワークを分離しています。お客様は、入力エンドポイントを使用して、インターネットからのアクセスに使用するポートを決定できます。

- VM 間のトラフィックは、常に信頼済みのパケット フィルターを経由します。
    a. アドレス解決プロトコル (ARP) や動的ホスト構成プロトコル (DHCP) といったプロトコルや、VM からのその他の OSI 第 2 層のトラフィックは、レート制限およびスプーフィング対策の保護を使用して制御されます。
    b. VM は、自身に宛てられた以外のネットワーク上のトラフィックを検知することはできません。
- お客様の VM では、Azure のプライベート インターフェイス、他のお客様の VM、Azure のインフラストラクチャ サービス自体にトラフィックを送信することはできません。お客様自身が所有または制御する他の VM、またはパブリック通信用の Azure インフラストラクチャのサービス エンドポイントとのみ通信することができます。
- VM を仮想プライベート ネットワーク上に配置した場合、VM が保有するアドレス空間は完全に不可視となります。このため、パブリック IP アドレスを使用して可視となるように構成しない限り、デプロイメントまたは Virtual Network の外部の VM からアクセスすることはできません。お客様の環境は、パブリック アクセスを許可するように指定したポートのみを通じて解放されます。VM にパブリック IP アドレスを使用した場合は、すべてのポートにパブリック アクセスが許可されます。