DirectAccess

Technical Overview

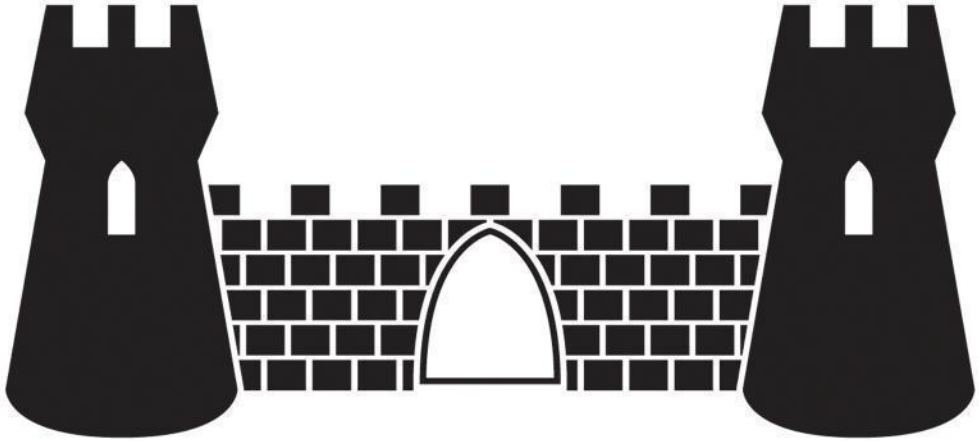
マイクロソフト（株）
チーフセキュリティアドバイザー
高橋　正和

DirectAccessの概要

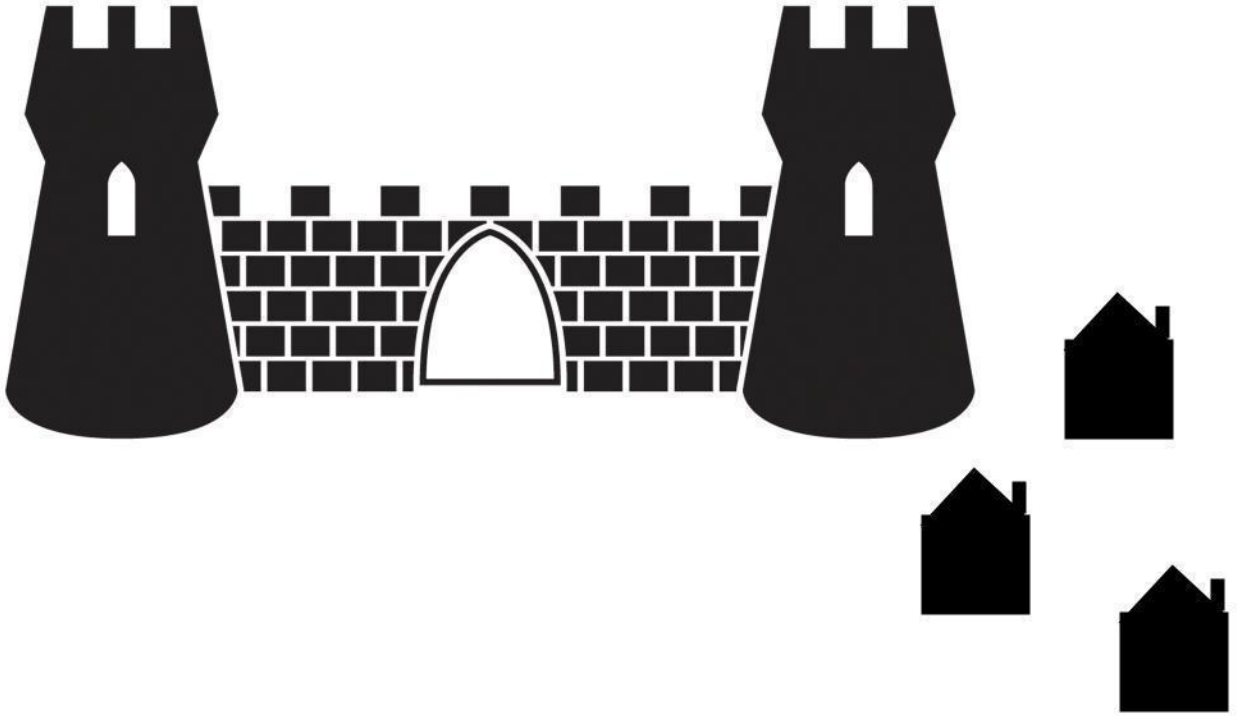
- DirectAccessは、オフィスの外にいる場合でも、オフィスと同等の利用環境を提供する
  - どこにいても、イントラネットのファイルにアクセスし、社内アプリケーションを利用する
  - インターネットに接続されていれば、常に双方向の通信を可能にする
    - 自分がどこで作業をしているのかを、意識せずに利用できるようになる
    - 社外のPCについても、IT管理者が管理をできるようになる。
- DirectAccessは、IPv6の技術を利用する
  - IPsecを利用した、サーバー・クライアント相互認証による接続
  - トネリング技術を使った、IPv4環境での利用

モバイルの必要性とVPNの課題

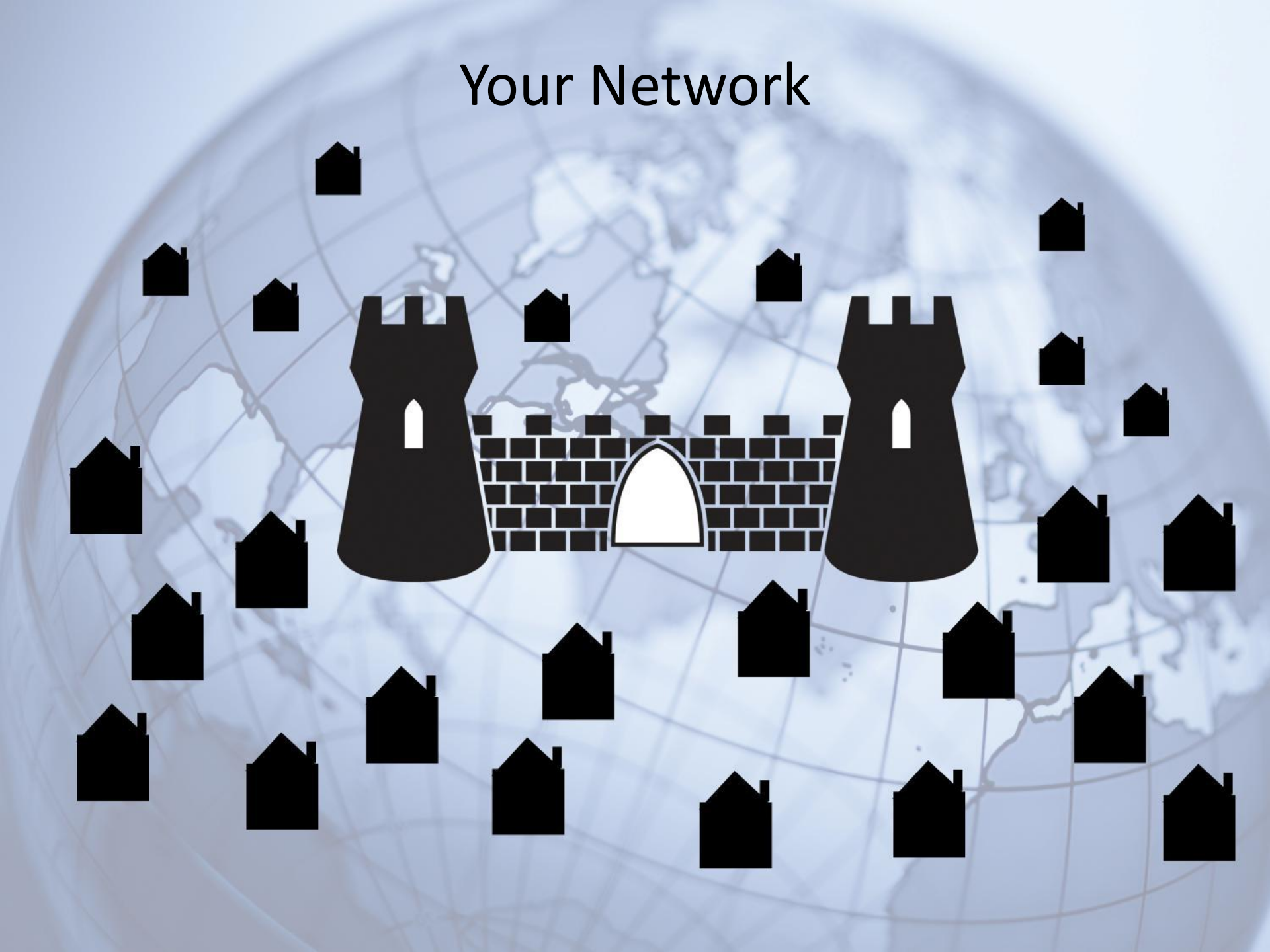
Your Network



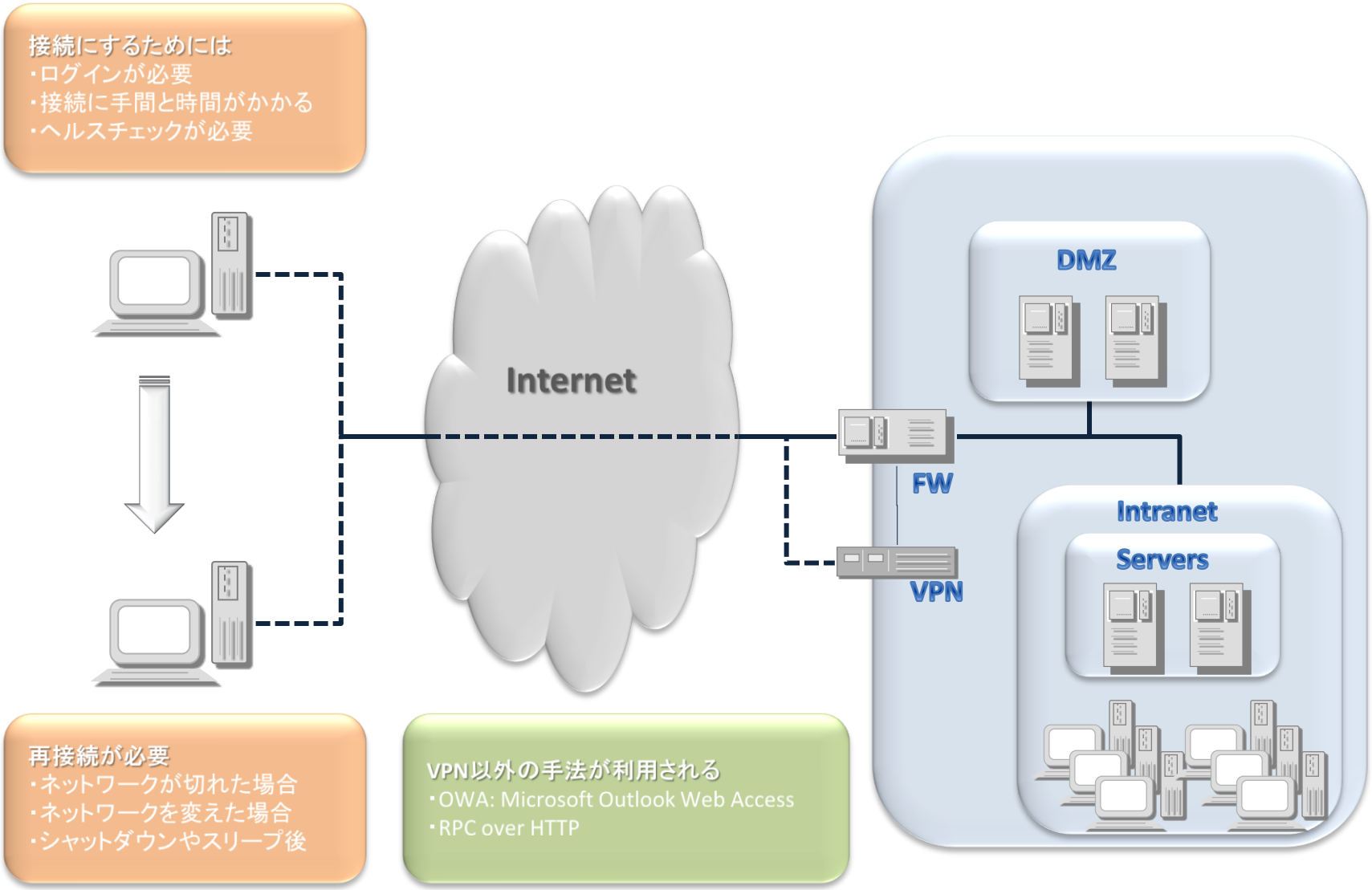
Your Network



Your Network

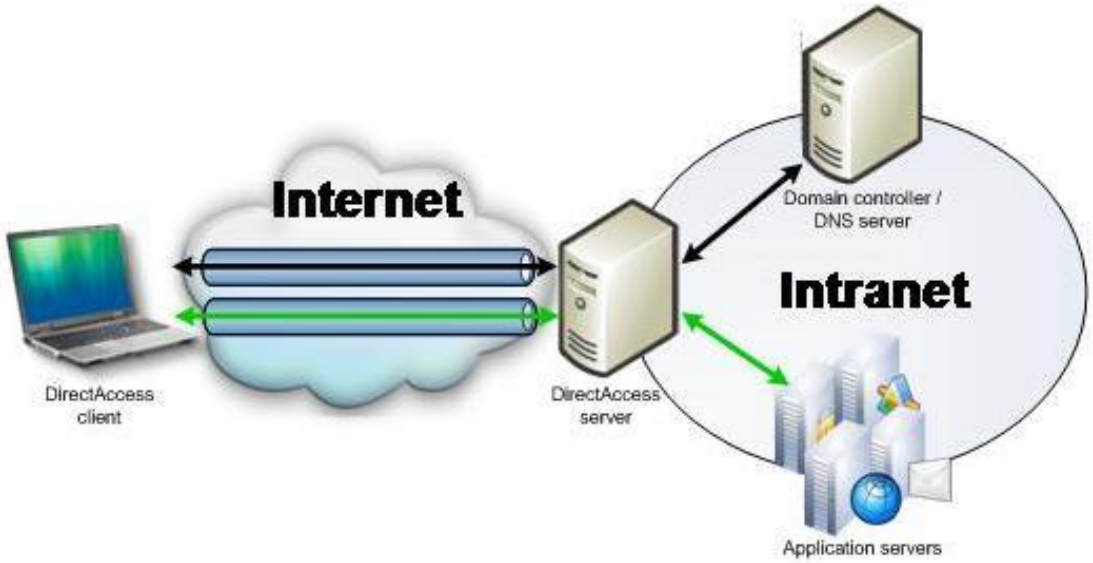


VPNの課題


接続にするためには
・ログインが必要
・接続に手間と時間がかかる
・ヘルスチェックが必要
Internet
DMZ
FW
VPN
Intranet
Servers
再接続が必要
・ネットワークが切れた場合
・ネットワークを変えた場合
・シャットダウンやスリープ後
VPN以外の手法が利用される
・OWA: Microsoft Outlook Web Access
・RPC over HTTP

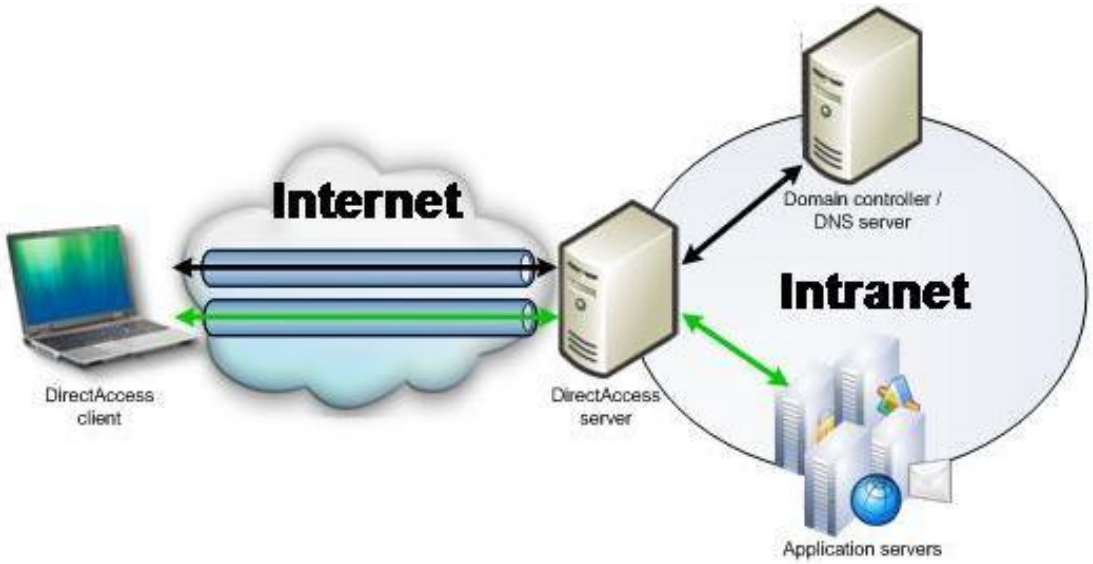
DirectAccess による接続-1

- VPNの課題を解決するための技術としてのDirectAccess
  - クライアントと社内ネットワークを自動的かつ、双方向に接続する
  - IPv6 / IPsecを使って構築
    - クライアントとユーザーの認証にIPsecを利用
      - スマートカードを利用することも可能
    - 通信の暗号化にもIPsecを利用
    - クライアントとDirectAccessサーバー間をIPv6で接続



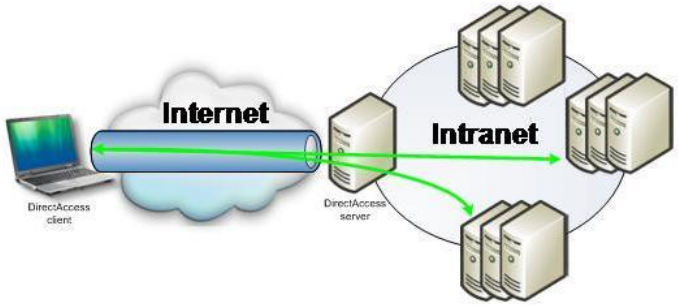
DirectAccess による接続-2

- 二つのIPsecトネルを利用
  - コンピュータ認証のためのIPsec ESP(Encapsulating Security Payload)
    - DNSサーバへのアクセス、
    - ドメインコントローラへのアクセス
      - グループポリシーのダウンロードと、ユーザー認証に利用
  - コンピューターとユーザー認証のためのESP
    - ユーザー認証と、イントラネットリソースやアプリケーションサーバーへのアクセスを提供

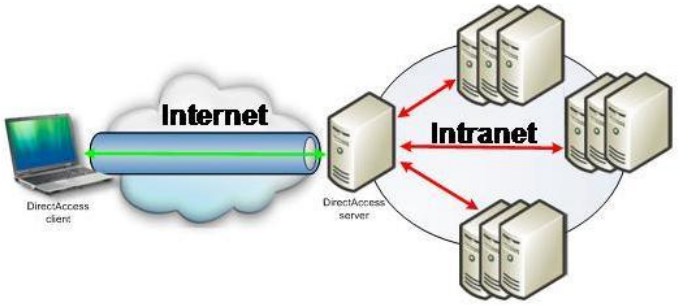


二つの構成

- End-to-end Protection
  - クライアントは、DirectAccessサーバーを経由して、アプリケーションサーバーとIPsecで接続する
  - この形態は、DirectAccessサーバーによて、全ての通信を制御できるため、高いセキュリティレベルを得ることができる
  - アプリケーションサーバーが、Windows Server 2008/2008R2で構成され、IPv6とIPsecをサポートしている必要がある



- End-to-edge protection
  - クライアントは、IPsec GWとIPsecセッションを確立(DirectAccessサーバでもよい）
  - IPsec GWは暗号化されていないトラフィックをイントラネット上のアプリケーションサーバーに送信する
  - サーバーにIPv6やIPsecを要求しない。

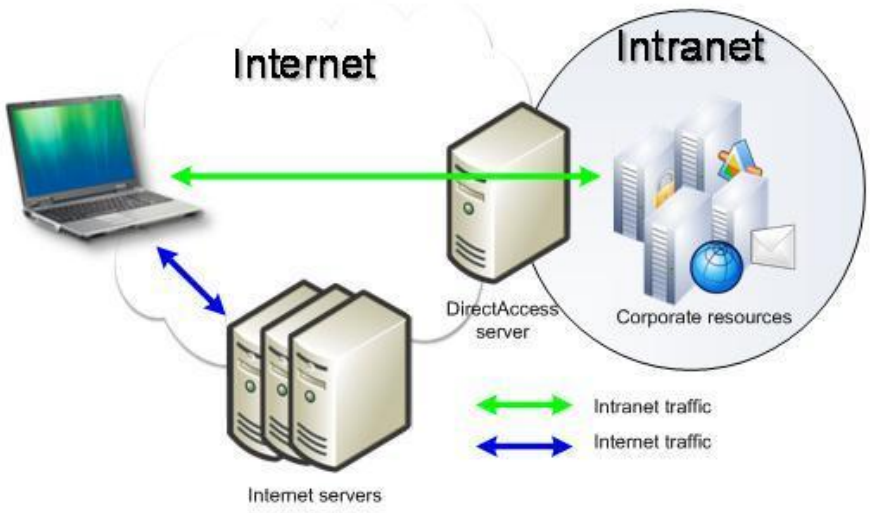


The DirectAccess Connection Process

1. Windows 7で稼動するDirectAccessクライアントがネットワーク接続を検知
2. 事前に設定されたイントラネットのWebにアクセスを試みる
   - アクセスができれば、すでにイントラネットに接続されていると判断し活動を停止
   - アクセスできない場合、インターネットに接続し、以下のプロセスを行う
3. IPv6とIPsecを使って、DirectAccessサーバーへ接続
   - ネットワークがIPv6ネットワークでない場合
     - 6to4かTeredoを使ったIPv6-over-IPv4トンネルによる接続を行う
   - ファイアウォールやProxyが6to4かTeredoを許可しない場合
     - IP-HTTPSを使って接続を行う
4. IPsecセッションの一部として、相互のマシン認証
   - クライアント・サーバーの相互マシン認証
5. Active Directoryによるコンピューターとユーザーの認証
6. NAPによるヘルスチェックが必要な場合
   - DirectAccessクライアントは、Health Registration Authority (HRA)を使って承認を得ることができる
7. DirectAccessサーバーは、クライアントのトラフィックを、ユーザーが利用可能なイントラネットにフォワードを始める

インターネットとイントラネットのトラフィックの分離

- インターネットトラフィックとイントラネットトラフィック
  - 多くのVPNでは、全てのトラフィックがいったんイントラネットに送信されるため、通信が遅い場合がある。
- DirectAccessでは、クライアントレベルで分離することができる
  - 全てのトラフィックをDirectAccessサーバーを経由させることもできる
- 詳細なアクセス制御
  - Windows Firewallの高度なセキュリティと組み合わせることで、IT管理者は、どのアプリケーションが、どのサブネットに通信ができるかを、制御することができる。
  - 例：イントラネットへの接続を…
    - 1サブネットだけへの接続を許可
    - IEは許可、他のアプリケーションは拒否
    - 特定のサーバーだけを許可



DirectAccessの認証方式

- ユーザーがログインする前に、コンピューターを認証する
  - 一般的には、この段階はドメインコントローラーとDNSにだけアクセスを許可し、ユーザー認証が済んだところで、他のリソースへのアクセスができるようになる。
  - ユーザ認証は、標準的なユーザー名とパスワードによる認証と、より高いセキュリティのためには、スマートカードを使った二要素認証が利用できる

- スマートカードによる認証
  - ユーザー認証
    - 特定のユーザーに、利用するコンピューターにかかわらずスマートカード認証を要求することができる
  - コンピューター認証
    - 特定のコンピューターに、利用者にかかわrずスマートカード認証を要求することができる
  - ゲートウェイ認証
    - IPsecゲートウェイは、接続を許可する前にスマートカード認証を要求することができる
      - この場合、ユーザーはインターネットへのアクセスは自由にできるが、イントラネットへのアクセスを行う場合にスマートカード認証を要求される
    - ゲートウェイ認証と、ユーザー認証、コンピューター認証を組み合わせることもできる。

IPv6とNAPの利用について

- IPv6の利用
  - すでにIPv6環境を利用している場合
    - DirectAccessは、シームレスに導入ができる
  - IPv6環境がない場合
    - 6to4 と Terado IPv6トンネルの利用
    - ISATAP IPv6の利用
    - NAT-PTの利用

- DirectAccessにおけるNAPの利用
  - NAPを使うことで、クライアントを規定に沿った健全な状態に保つことができる。
  - たとえば、DirectAccessサーバーへの接続を、最新のセキュリティパッチ、安置マルウエア、その他のセキュリティ設定が適切に適用されている場合に限り、接続を許すことができる
  - DirectAccessとNAPを併用する場合、DirectAccessサーバーと接続を開始する際に、クライアントの状態を認証するためNAP-enabled DirectAccessクライアントを必要とする。

DirectAccess requirement

- DirectAccess サーバー（複数設置が可能）
  - Windows Server 2008 R2で稼動する、
  - 二つのネットワークアダプター
  - インターネット側に連続した二つのIPv4グローバルアドレス
- DirectAccessクライアント
  - Windows 7で稼動するDirectAccessクライアント
- ドメインコントローラーとDNS
  - Windows Server 2008 SP2または、Windows Server 2008 R2
- PKI
  - コンピューターの認証、スマートカード認証、NAPのヘルス認証に必要
- IPsecポリシー
  - どのようにトラフィックを守るかを明確にする
- IPv6移行技術
  - ISATAP, Terado, 6to4
- NAP-PTデバイス（オプション）
  - IPv6をサポートしないリソースにアクセスするために必要

Summary

- シームレスコネクション
  - 利用者が、どこにいても、イントラネットリソースへのシームレスなアクセスを提供する（旅行、コーヒーショップ、自宅など）
- リモートマネージメント
  - IT管理者は、DirectAccessクライアントに接続し、ログインしていない場合でも、モニター、管理、アップデートの適用を行うことができる。
  - リモートコンピューターを最新に保ち、適切な設定の変更を行うためのコストを軽減することができる。
- セキュリティの向上
  - 認証と暗号にIpsecを利用するほか、スマートカード認証も利用できる
  - NAPと組み合わせることで、DirectAccessサーバー接続前に、接続条件を満たすことを要求できる
  - DirectAccessサーバーは、利用者、アプリケーションごとにアクセス許可を定義できる

- 統合的なサーチ（フェデレートサーチ）
  - イントラネットナイト同様に、総合的なサーチを利用することができる
- フォルダーリダイレクション
  - 複数のコンピューターを、ネットワークをまたいで、自動的にフォルダーを同期することができる。
- 取替え可能なコンピューター
  - アプリケーション、ドキュメント、セッティングがネットワークに保存され、どのコンピューターからも利用できる場合
  - コンピューターが壊れたり、失くした場合でも、代替機は、ユーザーごとの設定を行う必要がない。

References

技術要素	URL
Active Directory	http://go.microsoft.com/fwlink/?LinkID=147288
DirectAccess	http://go.microsoft.com/fwlink/?LinkId=147011
DNS	http://go.microsoft.com/fwlink/?LinkId=147013
Group Policy	http://go.microsoft.com/fwlink/?LinkId=100760
IPv6	http://go.microsoft.com/fwlink/?LinkId=17074
IPsec	http://go.microsoft.com/fwlink/?LinkId=50170
NAP	http://go.microsoft.com/fwlink/?LinkId=56443
PKI	http://go.microsoft.com/fwlink/?LinkId=83694