

Office365 ネットワーク・セキュリティソリューション

**Microsoft Office 365 導入に伴う
ネットワークの課題をSD-WAN機能で解決!**

1. 拠点での課題

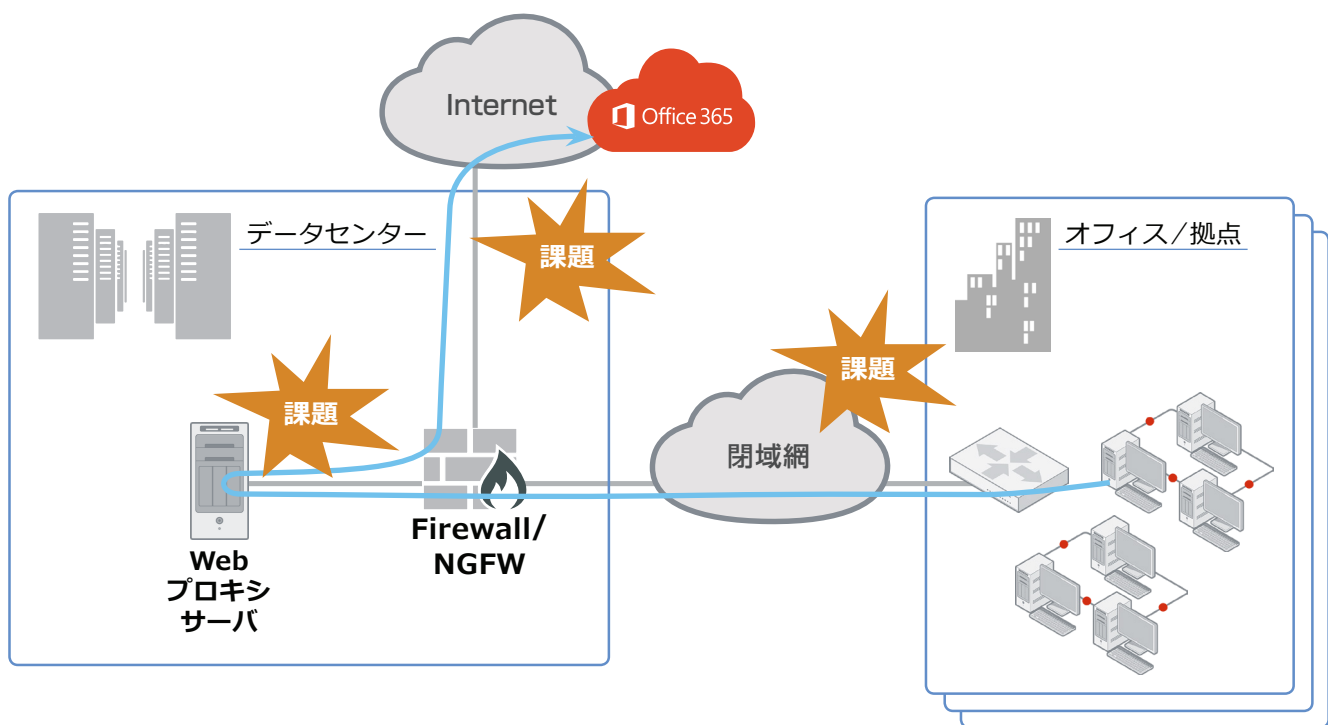
拠点からセンター向けの閉域網経由のインターネットトラフィックが増加

- Office365利用により拠点からのインターネット向けトラフィックが増加
- 拠点からセンター向けの閉域網経由のトラフィックも増加し回線費用が上昇

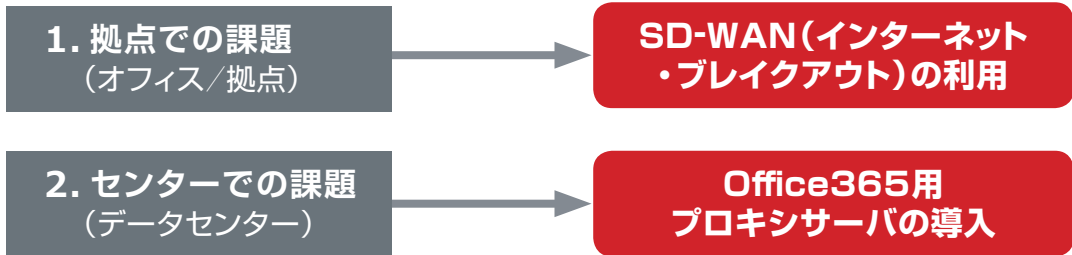
2. センターでの課題

セッション数増加によるプロキシサーバの負荷増大

- Office365は1ユーザに対し多くのセッションを同時利用するため既存プロキシではパフォーマンスが不足
- インターネット向けトラフィックの増加で回線への負荷も増加

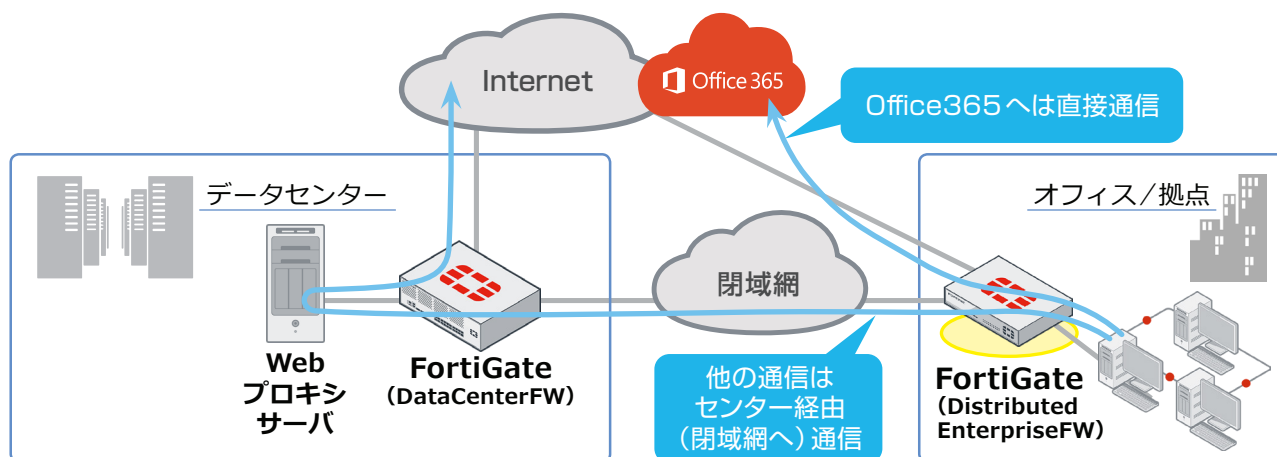


フォーティネットのご提案



1. 拠点:SD-WAN(インターネット・ブレイクアウト)の利用

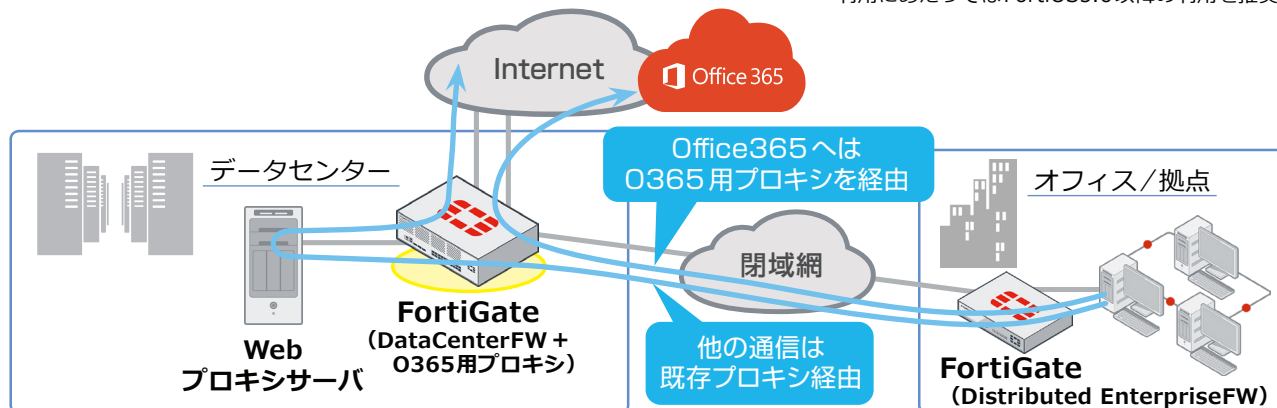
- ソリューション
 - FortiGateのSD-WAN機能で、Office365への通信とそれ以外の通信とで使用する回線を分離(インターネット・ブレイクアウト)
 - 閉域網へのトラフィック量は変わらず、安価なインターネット回線の利用で回線費用も最適化
- フォーティネットの優位性
 - FortiGateの標準機能でSD-WAN機能を利用可能
 - Office365を始めとするクラウドサービスが使用するIPアドレス情報を自動更新(ISDB*)
 - レイヤ7(アプリケーションレベル)ではなく、ポリシルーティング処理により高速に動作



2. センター:Office365用プロキシサーバの導入

- ソリューション
 - FortiGateのプロキシ機能とSD-WAN機能でOffice365への通信はインターネットへ直接転送
 - その他の通信のみ既存プロキシへ転送するため、既存プロキシに負荷を与えない
 - インターネット回線を増設し、SD-WAN機能で回線を有効活用(マルチホーミング)
- フォーティネットの優位性
 - ネットワークセキュリティ機能とプロキシ機能の利用で柔軟なネットワークデザインが可能(2つの機能をFortiGateに統合も可能)
 - Office365が使用するIPアドレス情報を自動更新(ISDB*)
 - Microsoft Azure上にプロキシ(FortiGate-VM)を構築し、閉域網からExpressRoute接続時もプロキシを利用可能(クラウド環境で完結可能)
 - SSLインスペクションを利用してテナントアクセス制限も可能

*ISDB:Internet Service Databaseの略。利用にあたってはFortiOS5.6以降の利用を推奨。



FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

HCNET エイチ・シー・ネットワークス株式会社
〒111-0053 東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル4F <https://www.hcnet.co.jp>