ファイヤーウォール・UTM・VPN
SonicWall

DELL Technologies

SonicWallのUTM

ネットワーク機器としての機能

- ファイアウォール
- WAN冗長 ロードバランス
- ルーティング NAT VLAN
- VPN
- SSLインスペクション (DPI-SSL)
- ハードウェア冗長

サイバーセキュリティ対策機能

- ゲートウェイ アンチウィルス
- 不正侵入 検知/防御
- アンチスパイウェア
- アプリケーション制御 /可視化
- Webフィルタ コンテンツフィルタ
- ボットネットフィルタ 地域IPフィルタ
- マルチエンジンサンドボックス
- キャプチャ脅威評価レポート
- エンドポイントセキュリティ連携

その他

- セキュアワイアレスAP (SonicWave)
- スイッチング (Dell Xシリーズ スイッチ)
- 管理 レポーティング

クラウド管理
ゼロタッチ
レポーティング
脅威解析
リスク計測

(Capture Security Center)

様々な機能をすべてのモデルに実装

TZ Series

NSa Series

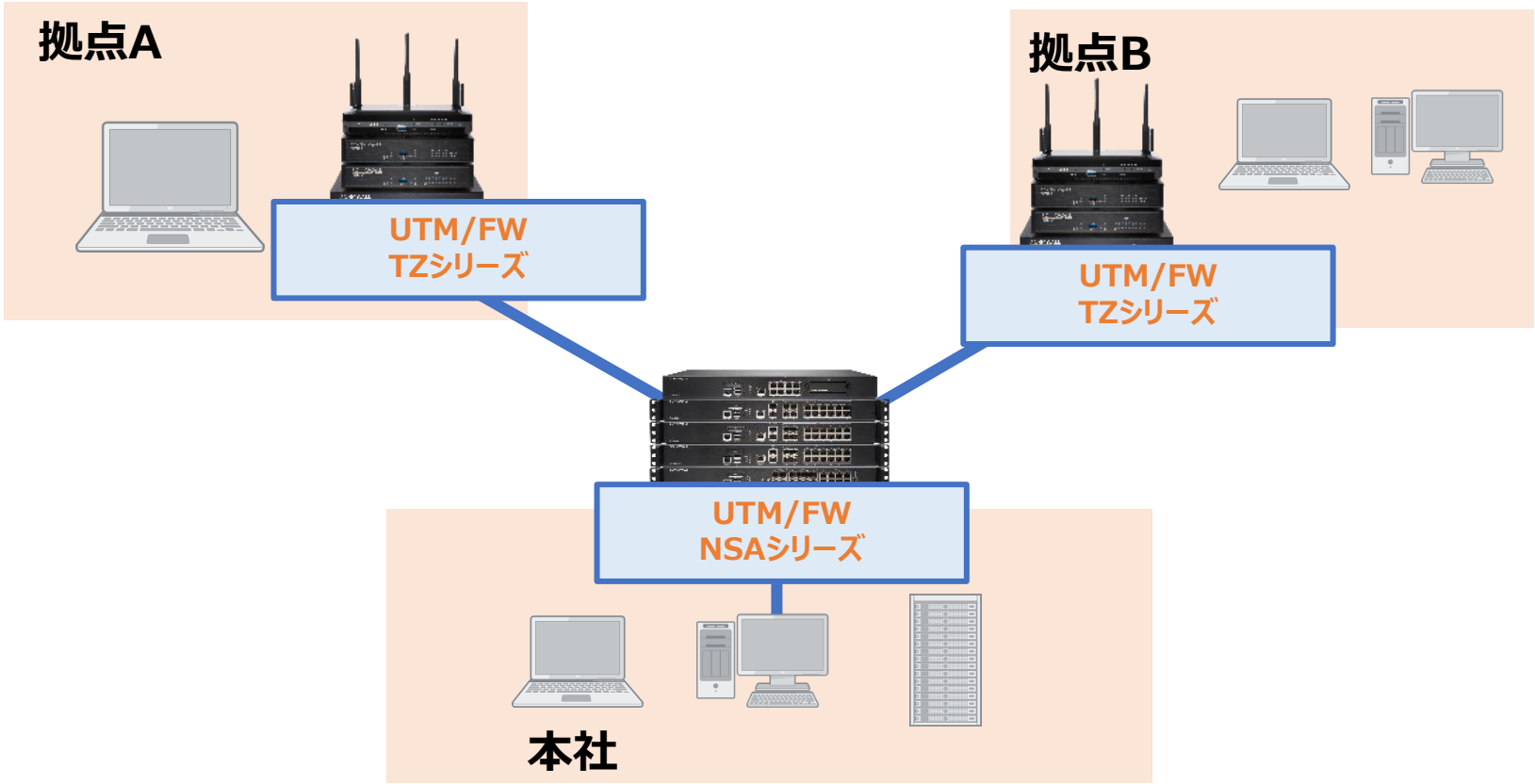
NSa 9000 Series

(*1) GVC(IPSec VPN Client)・SSLVPN Client は、同時接続数を拡張するためにオプションライセンスの購入が必要な場合があります
(*2) モデルによって、一部利用できない機能や制限があります

Internal Use - Confidential

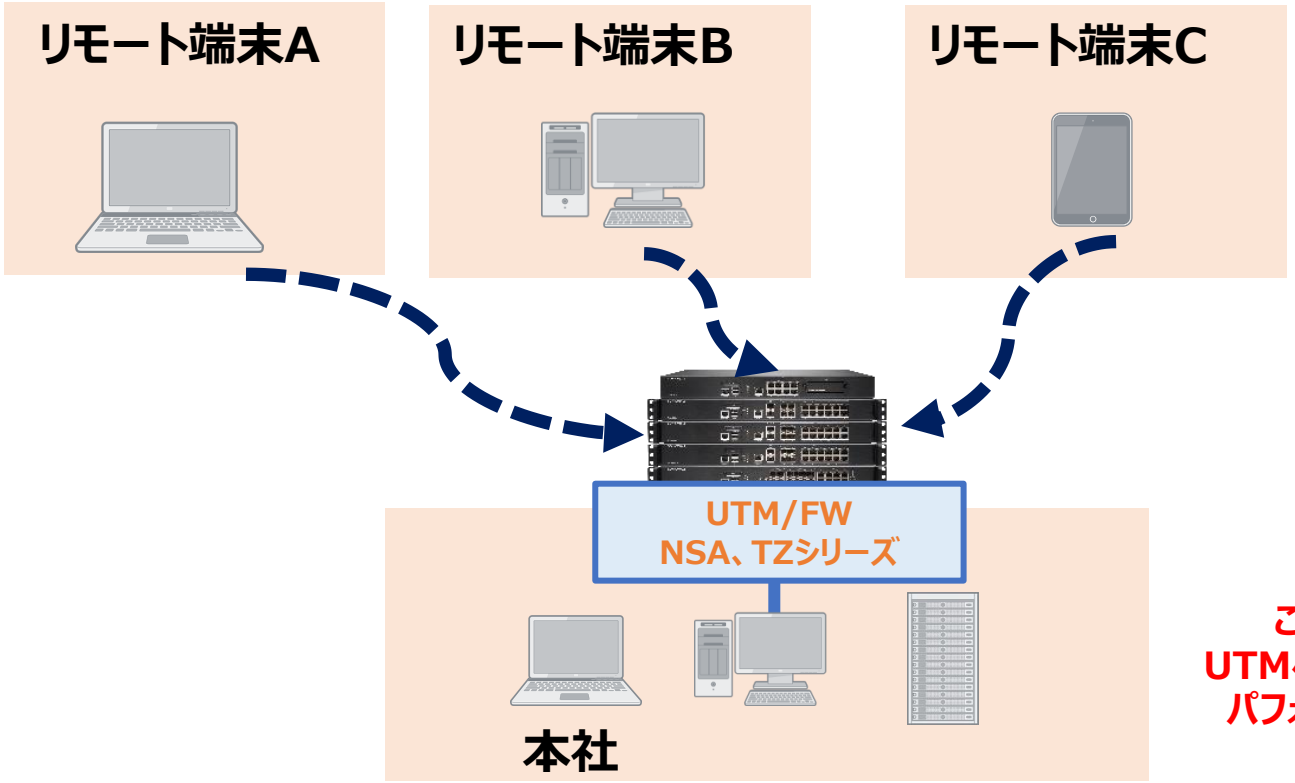
© Copyright 2021 Dell Inc.

拠点間VPN通信



© Copyright 2021 Dell Inc.

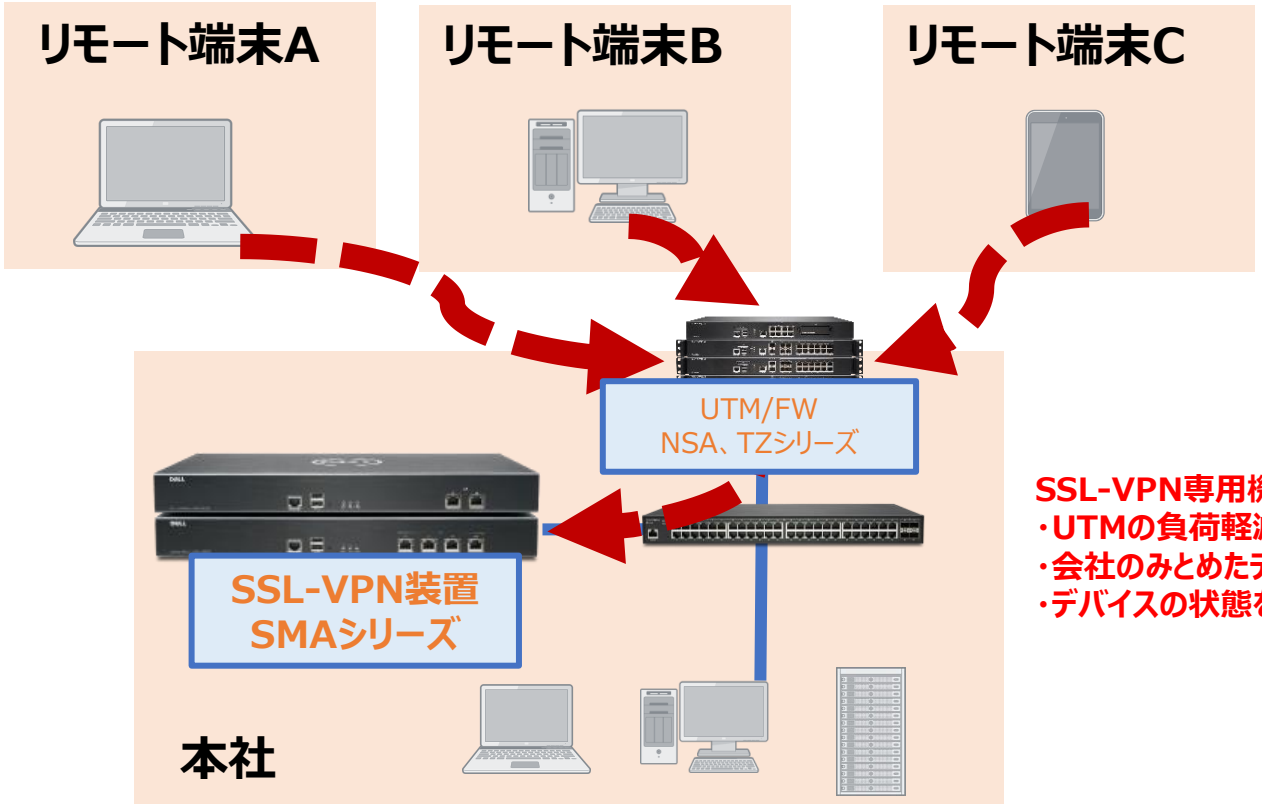
リモートVPN（UTMで）



※注意※
このパターンは
UTMへの負荷が大きい
パフォーマンスに課題

© Copyright 2021 Dell Inc.

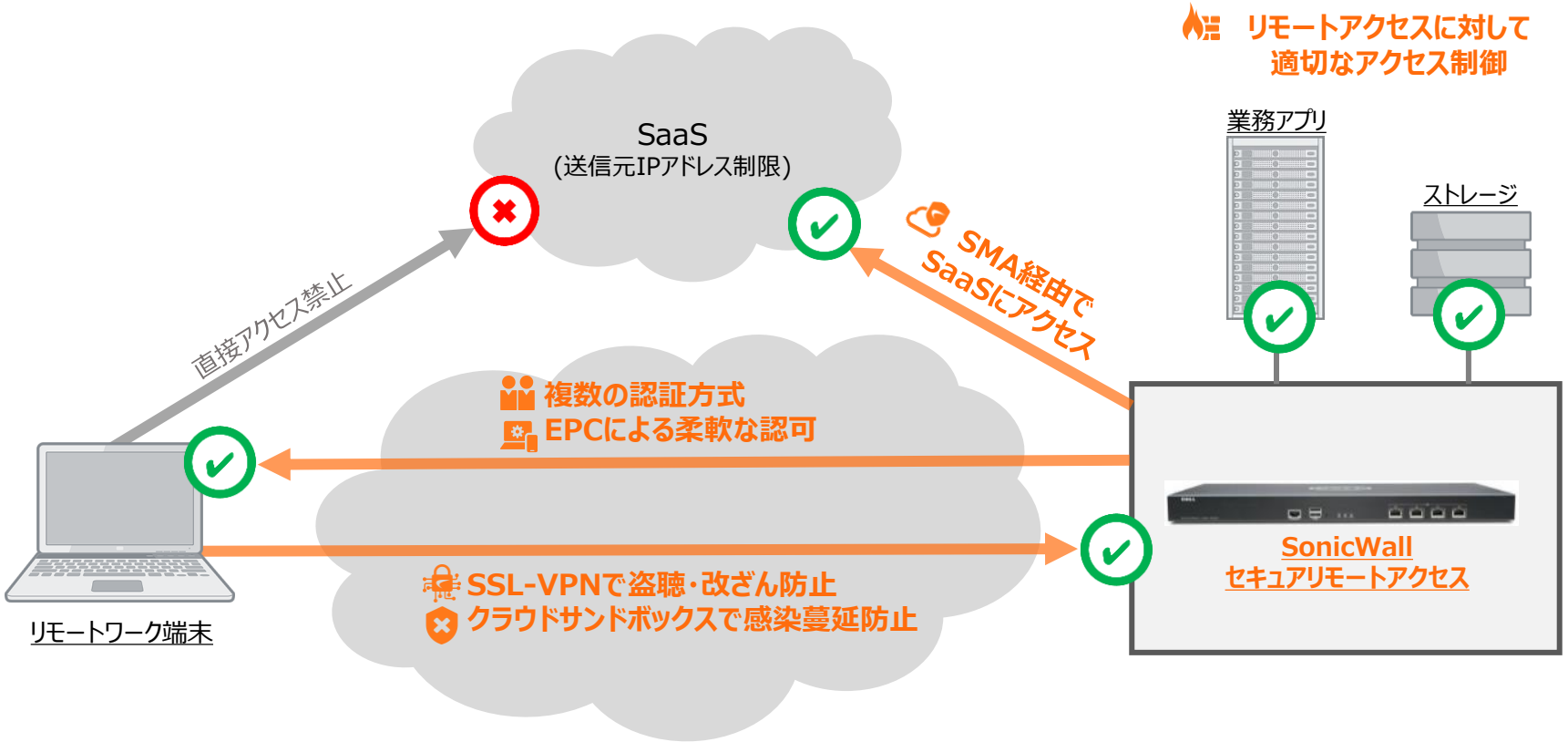
リモートVPN（SSL-VPN専用機SMAで）



SSL-VPN専用機のため、
・UTMの負荷軽減
・会社のみとめたデバイスのみ接続可能
・デバイスの状態をみて接続の可否が可能

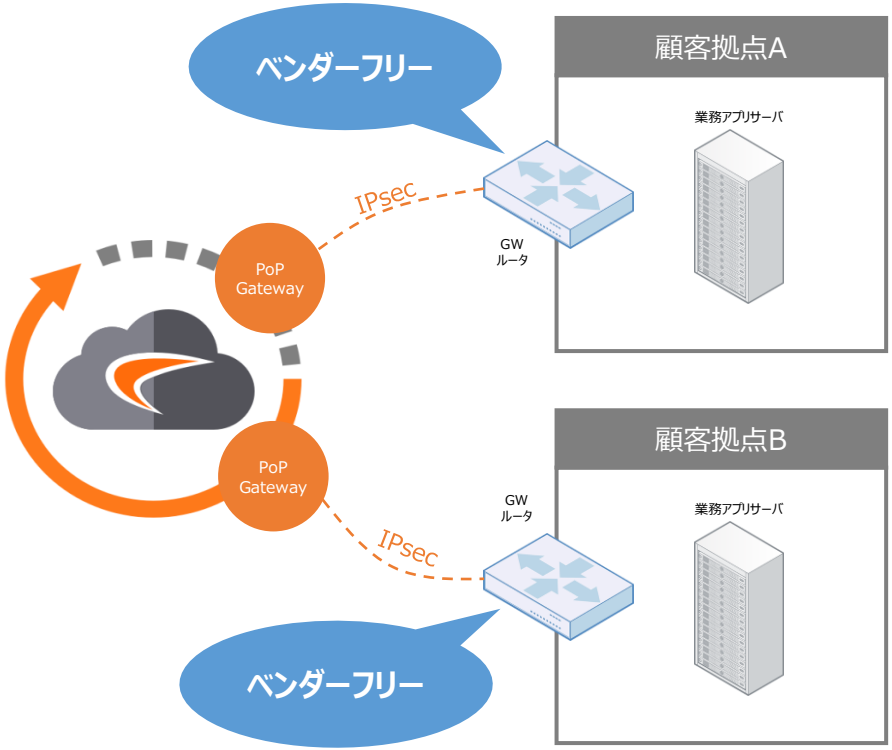
© Copyright 2021 Dell Inc.

SonicWallセキュアモバイルアクセス（SMA）



© Copyright 2021 Dell Inc.

容易な導入方式で既存システムへの影響がないCloudEdge



CloudEdgeの対向ルータはベンダーフリー

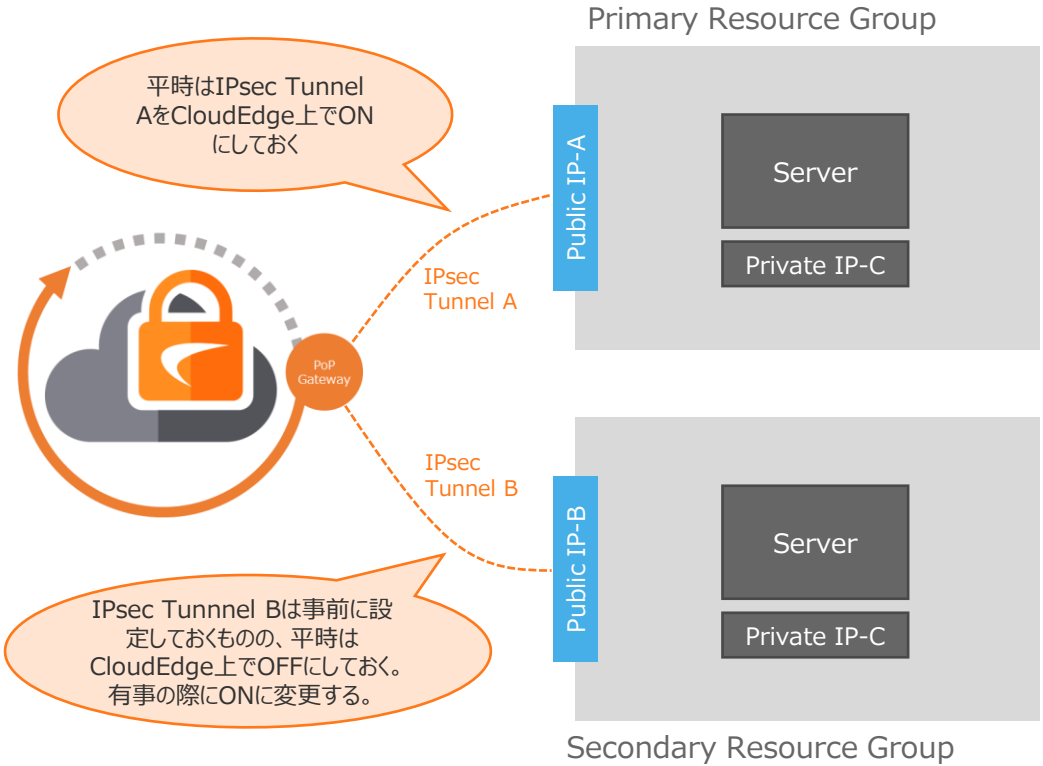
CloudEdgeを利用するためには、PoPGatewayとお客様拠点にあるルータとの間でIPsecを設定いただきますが、CloudEdgeではそのルータに制約はありません。いかなるベンダーのルータでもIPsecさえ設定可能であればCloudEdgeをご利用いただくことが可能です。

同業他社製品では、業務アプリサーバに専用のエージェントをインストールする必要があったり、専用アプライアンスを設置したりと、導入へのハードルが高いケースが見受けられます。

CloudEdgeは既存ルータへのIPsec設定追加のみで導入できるため、他社製品に比べ手間や影響を限りなく抑えることができます。

© Copyright 2021 Dell Inc.

Azureリージョンペアをご利用の場合にCloudEdgeを導入するためには



前提として、リージョンペアは異なるパブリックIPで、プライベートIPは同一とします。

CloudEdgeではそれぞれのリージョンのルータとPoPGatewayの間でIPsecを設定します。このときPoPGatewayは一つで構いません。

IPsecを設定することで、CloudEdgeから顧客サーバに対してプライベートIPアドレスによるルーティングが可能になるのですが、リージョンペアではサーバのプライベートIPアドレスは同一であるため、CloudEdgeは正しくルーティングができなくなってしまいます。

この問題を解消するためには、平時の際はプライマリーリソースサイトとのIPsecをCloudEdge上でONにしておき、有事が起きた際にセカンダリリソースサイトとのIPsecをONにします。こうすることでIPアドレスの重複を抑えてルーティングが可能になります。

このオペレーションは現在手動で行う必要がありますが、現在CloudEdgeはAPIの実装を進めておりますので、Azure上で自動化できる見込みです。

© Copyright 2021 Dell Inc.


DELL Technologies