

Zscalerで実現可能なゼロトラストセキュリティ

Zscaler Internet Access (ZIA)

Zscaler Private Access (ZPA)

① アクセス制御、脅威保護、データ保護、管理機能

| | |
|------------|---------------|
| SSL復号 | URL Filtering |
| AV/Sandbox | NGFW/IPS |
| CASB | DLP |
| SSPM | RBI |
| Logging | Reporting |

② 限界の無いスケーラビリティ

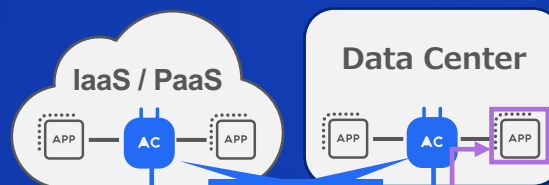
③ セキュアなローカルブレイクアウトアーキテクチャ

④ ユーザ識別、デバイスポスチャ



拠点内 / リモート
ユーザ

⑧ 場所にとらわれないセキュリティポリシー



⑦ 攻撃表面の削除

- 許可する? (セッション毎のポリシー)
- リスクは? (適応型)
- どこ行くの? (アプリアクセス)
- 誰? (ID)

⑥ マイクロセグメンテーションへ

⑤ リモートアクセス

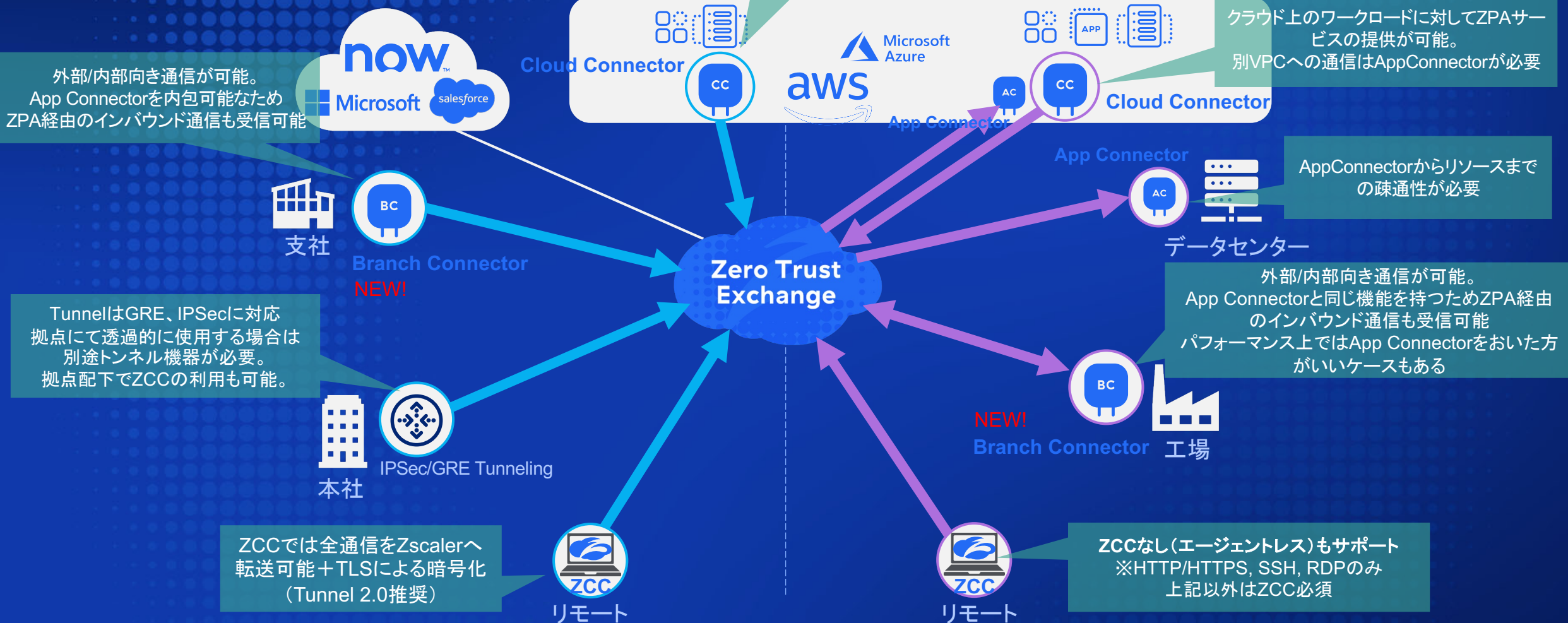


拠点内 / リモート
ユーザ

ZIAとZPAへの接続方式

Internet / SaaS

IaaS



外部/内部向き通信が可能。
App Connectorを内包可能なため
ZPA経由のインバウンド通信も受信可能

クラウド上のワークロードに対して
ZIAサービスの提供が可能

クラウド上のワークロードに対してZPAサー
ビスの提供が可能。
別VPCへの通信はAppConnectorが必要

AppConnectorからリソースまで
の疎通性が必要

TunnelはGRE、IPSecに対応
拠点にて透過的に使用する場合は
別途トンネル機器が必要。
拠点配下でZCCの利用も可能。

外部/内部向き通信が可能。
App Connectorと同じ機能を持つためZPA経由
のインバウンド通信も受信可能
パフォーマンス上ではApp Connectorをおいた方
がいいケースもある

ZCCでは全通信をZscalerへ
転送可能+TLSによる暗号化
(Tunnel 2.0推奨)

ZCCなし(エージェントレス)もサポート
※HTTP/HTTPS, SSH, RDPのみ
上記以外はZCC必須

ZIA(外部向け: Internet/SaaS)

ZPA(内部向け: Private/IaaS)

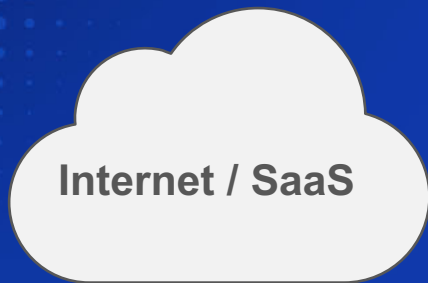
Zscalerアーキテクチャーにおけるコンポーネント

IDaaS : ユーザ管理/認証

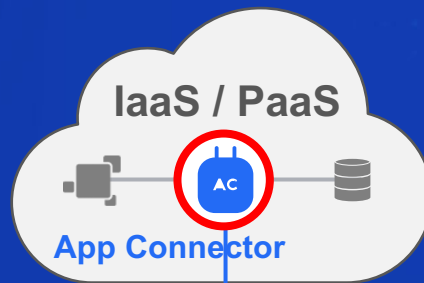
- ✓ ZPAではSAML認証が必須 (ZIAは推奨)
- ✓ SAML2.0に対応していればIdPとして連携が可能
- ✓ AzureAD, Okta, HENNGE等



IDaaS



Internet / SaaS



IaaS / PaaS

App Connector

App Connector : ZTNAゲートウェイ

- ✓ ZPAからプライベートリソースまで経路提供
- ✓ 仮想アプライアンス
- ✓ VMWare, AWS, Azure, Dockerなど



データセンタ

App Connector



Zero Trust Exchange

ZIA / ZPA

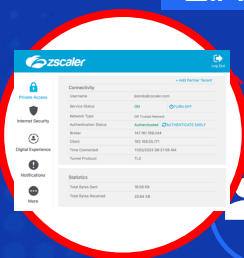
ZIA

ZIA / ZPA

Zscaler Client Connector (ZCC)

ZCC : エージェント

- ✓ ZIAとZPA利用 (ZDXでも必要)
- ✓ Zscaler推奨構成
- ✓ Windows, MacOS, Linux, ChromeOS, Android, iOS



拠点内/リモート
ユーザ



GRE / IPsec

拠点



拠点内 / リモート
ユーザ

GRE / IPsec : トンネリング方式

- ✓ ZIA利用
- ✓ ZCCがインストールできない端末トラフィックをZIAへ転送可能

管理ポータル(ブラウザ)

