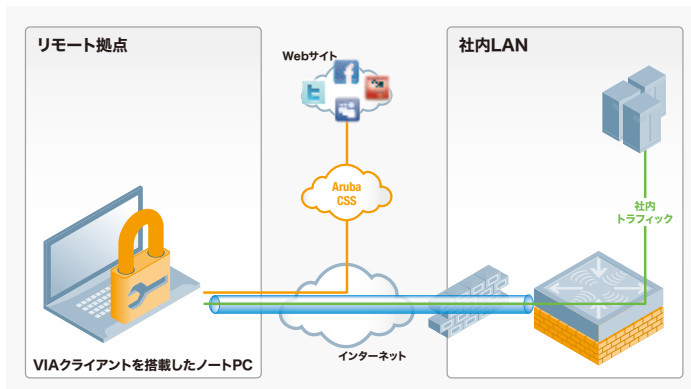




Virtual Intranet Access エージェント

Aruba Virtual Intranet Access™ (VIA™) エージェントは、リモート拠点のWindowsノートPCとApple MacBookを社内ネットワークに安全に接続します。VIAは、Aruba Virtual Branch Network™ (VBN™) ソリューションのカギとなるコンポーネントであり、Arubaモビリティ・コントローラーとともにライセンスが供与されます。

VIAはIPsec/SSLのハイブリッド型VPNソリューションです。ネットワーク接続をスキャンし、必要に応じて社内ネットワークへの最適な接続を自動的に選択します。従来のVPNソフトウェアと異なり、VIAでは、ノートPCでのWLAN設定をゼロタッチで行うことができます。



セキュリティ強化のため、VIAはクラウドベースのAruba

Content Security Service (CSS)をサポートし、インターネット上の脅威や攻撃を幅広く回避します。さらに、オプションのArubaOS Advanced Cryptography (ACR) モジュールをインストールすると、ミリタリーグレードのSuite B暗号も導入できます。その結果、管理が必要な公開情報、機密情報、非公開情報を処理するネットワークにユーザーのモバイル機器を安全に接続できます。

統合ソリューション

VIAは、Policy Enforcement Firewall (PEF) ライセンスを通して注文でき、モビリティ・コントローラーから直接ダウンロードすることも、既存のソフトウェア管理プラットフォームからプッシュすることもできます。追加のハードウェアがなくても、モビリティ・コントローラーに接続し、ソフトウェア更新と設定更新を直接受信することができます。

自動的なIPsec接続

外出先のビジネス・ユーザーは、一般に、ホテル、空港、カフェ、3Gセラー・ネットワークを経由して社内リソースに接続しますが、そのためには社内リソースとの間で安全なリンクを確立する必要があります。一般的な従来型VPNでは、別のソフトウェアを起動し、複雑なログイン・プロセスを実行しなければなりません。

VIAは、ネットワーク接続を自動的に検出し、それが社内ネットワークの接続かどうかを判別します。社内ネットワークの接続でない場合、VIAはデータ・センターとの間でIPsec接続を開始し、ユーザーの場所に関係なく、シームレスにネットワーク・アクセスを確立します。

SSLフォールバックでカプセル化できるIPsec

VIAは、VIA対応デバイスとデータ・センター内のArubaモビリティ・コントローラーとの間で通信の安全性を確保するために、標準的なIPsecプロトコル・スイートを使用します。そのため、クライアントがネイティブIPsecで実現できる最高速度で接続を行うことができます。IPsecによる直接接続がファイアウォールでブロックされる場合、VIAはIPsecパケットをSSLヘッダー内にラップするため、社内ファイアウォール経由で安全な接続を確立することができます。

シングル・サインオンの活用

無線LAN (WLAN) のユーザーを認証するときと同じWindows資格情報を使用してVIAユーザーを認証することができます。VIAは、これらの資格情報を使用することで、ユーザー名とパスワードを確認することなくバックグラウンドのユーザーを自動的に接続します。

この自動接続機能により、ユーザーの作業習慣を変えることなく、常に同じ方法で接続と認証を行うことができます。認証方式を追加する必要がある場合、ユーザー名とパスワードまたはトークンによる従来の方式を採用することもできます。

ユーザー・ロールのサポート

VIAエージェントは、ローカルとリモートのどちらのネットワーク・アクセスにも、ロール・ベースが同じのステートフル・ファイアウォール・ポリシーを適用します。そのため、エンドユーザーはどこからでも同じようにネットワークにアクセスできます。また、同じエンド・ポイントでも、ネットワークにログインす

る場所によって別々のアクセス・ロールとポリシーを使用するように設定することもできます。

幅広いトラブルシューティング方法のサポート

VIAに標準装備されたロギング/診断機能により、複雑なツール類を操作することなく、接続に関する問題をリモート環境からトラブルシューティングできます。

必要な場合、クライアント・ログをサポート・チームに電子メールで送信し、詳細を調べてもらうことができます。診断ツールには、接続ログ、システム情報、検出されたWLANネットワークのリスト、詳細な接続テストが含まれています。

Windows Zero Configurationのサポート

VIAには、Windows Zero Configuration (WZC) サプリカントでWLAN設定を構成できるオプション機能があります。ネットワーク管理者は、マシン操作や他のツールの管理を行わなくても、使用したいWLAN設定をクライアントに動的にプッシュすることができます。

幅広いセキュリティ

VIAは、モバイル・ワーカーのセキュリティを強化するために、インターネット宛でのトラフィックをAruba CSSに送信します。CSSは、世界各地にあるクラウドベースのセキュリティ・センターから、拡張URLフィルタリング、ピアツーピア・コントロール、ウイルス/マルウェア対策、ボットネット検出、データ・ロス防止 (DLP) などの保護機能全般を提供します。

VIAとCSSが高スループットと低遅延を同時に実現するため、モバイル・ワーカーがどこにいても、クラウドベースの安全なネットワークを提供できます。

社内、ホーム・オフィス、外出先からのアクセス

VIAは、ArubaOS™オペレーティング・システムの一部としてライセンス供与され、Aruba 600シリーズ、3000シリーズ、6000モビリティ・コントローラーから入手できます。VPNヘッドエンドのサーバーやアプライアンスを追加する必要はありません。

VIAが導入されると、ユーザーは本社や支社のネットワークに接続するときと同じ感覚でネットワークに接続できます。ローカル、リモートのどちらからでも、ネットワーク・リソースにシームレスにアクセスできます。

Virtual Intranet Access エージェント

対応セキュリティ・プロトコル

- 暗号化: AES-GCM-128、AES-GCM-256、AES256、AES192、AES128、3DES、DES
- ハッシュ: SHA-256、SHA-384、SHA、MD5
- 認証: ★★事前共有キー、RSA、RSA、ECDSA、スマート・カード★★
☆☆事前共有キー、RSA、RSA、ECDSA、スマート・カード☆☆
- Diffie-Hellmanグループ:
★★Group 1、Group 2、ECDH Group 19、ECDH Group 20★★
☆☆Group 1、Group 2、ECDH Group 19、ECDH Group 20☆☆
- IPsec IKEv2

認証オプション

- ユーザー名/パスワードと証明書による多要素認証
- スマート・カード

フォワーディング・モード

- トンネル・モード
- スプリットトンネル・モード

対応クライアント・オペレーティング・システム

- Windows 7 (32ビットおよび64ビット)
- Windows Vista (32ビットおよび64ビット)
- Windows XP Service Pack 2以降
- Mac OS X
- ★★ オプション構成として、Windows® WLANクライアント構成を提供★★
☆☆ オプション構成として、Windows® WLANクライアント構成を提供☆☆

対応Arubaモビリティ・コントローラー

- 600シリーズ
- M3コントローラー・モジュール搭載の6000モビリティ・コントローラー
- 3000シリーズ

VIAのSuite B暗号サポート

非公開または極秘のネットワークを展開するために、VIAが強化されました。VIAは、RFC 4869 (IPsec用Suite B暗号スイート) とbSec (安全なワイヤレス接続を実現するためにIEEE 802.11i用に強化されたSuite B) をサポートします。VIAのSuite B機能を有効にするには、オプションのArubaOS ACRモジュールを使用します。Suite B機能は、Windows Vista/7デバイスのほか、一般的なスマートフォン*やタブレット*のオペレーティング・システムでも使用できます。

* ロードマップ項目



© 2011 Aruba Networks, Inc. All rights reserved. Aruba Networksは、Aruba Networks, Inc.の商標です。その他の商標または登録商標は各社の所有物です。仕様については、予告なく変更されることがあります。

2011.10.0000.v1

■ 開発元

■ お問い合わせ

アルバネットワークス株式会社

〒105-0004 東京都港区新橋5-27-1 パークプレイス3F
TEL. 03-6809-1540 (代表) FAX. 03-6809-1541
<http://www.arubanetworks.co.jp>