

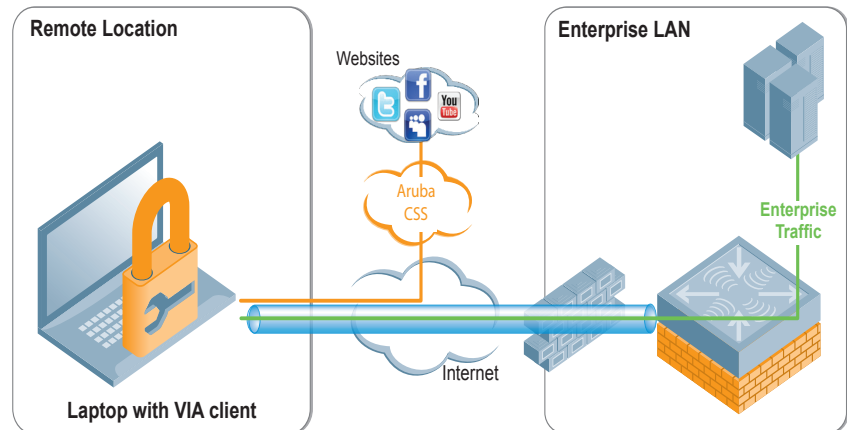


VIRTUAL INTRANET ACCESS-AGENT

Der Virtual Intranet Access™-Agent (VIA™) von Aruba bietet sichere Netzwerk-Remote-Verbindung für Windows- und Apple MacBook-Laptops in Außenstellen. Als Schlüsselkomponente der Virtual Branch Network™-Lösung (VBN™) von Aruba ist VIA als lizenzierte Option in Verbindung mit Aruba Mobility Controllern verfügbar.

VIA ist eine IPsec-/SSL VPN-Mischlösung, die Netzwerkverbindungen überprüft und im Bedarfsfall automatisch die beste und sicherste Verbindung mit dem Unternehmensnetzwerk auswählt. Im Gegensatz zu herkömmlicher VPN-Software entsteht dem Endbenutzer mit VIA kein Mehraufwand. Es können mit VIA sogar die WLAN-Einstellungen an Laptops konfiguriert werden.

Für höhere Sicherheit unterstützt VIA den Cloud-gestützten Content Security Service (CSS) von Aruba, um einen umfassenden Schutz vor Bedrohungen und Angriffen aus dem Internet zu bieten.



INTEGRIERTE LÖSUNG

VIA kann über die Policy Enforcement Firewall-Lizenz (PEF) von Aruba bestellt und direkt vom Mobility Controller heruntergeladen werden. Auch das verteilen über eine vorhandene Softwareverwaltungsplattform ist möglich. VIA verbindet sich mit dem Mobility Controller und empfängt direkt von diesem sowohl Software- als auch Konfigurationsaktualisierungen, ohne dass zusätzliche Hardware erforderlich wäre.

AUTOMATISCHE IPSEC-VERBINDUNG

Geschäftsreisende, die häufig unterwegs sind, wählen sich oft über 3G-Mobilfunknetze von Hotels, an Flughäfen, in Cafés in ihr Unternehmensnetzwerk ein um auf interne Ressourcen zuzugreifen. Diese Verbindungen müssen sicher sein. Bei herkömmlichen VPNs müssen die Benutzer nicht selten zusätzliche Software starten und einen komplexen Anmeldeprozess durchlaufen.

VIA hingegen erkennt die Netzwerkverbindung automatisch und ermittelt, ob sich diese im eigenen Unternehmensnetzwerk befindet. Wenn dies nicht der Fall ist, erstellt VIA eine IPsec-Verbindung zum Rechenzentrum, wodurch der Netzwerkzugriff für Benutzer unabhängig von seinem Standort gesichert erfolgt.

IPSEC MIT SSL-FALLBACK VERSCHLÜSSELUNG

Bei VIA wird das IPsec-Standardprotokoll verwendet, um die Kommunikation zwischen VIA-fähigen Geräten und einem Aruba Mobility Controller im Datenzentrum zu sichern. Somit wird die schnellstmögliche Verbindung gewährleistet, wo Clients über IPsec eine Verbindung herstellen können. Wenn direkte IPsec-Verbindungen von einer Firewall blockiert werden, können IPsec-Pakete von VIA in einen SSL-Header verpackt werden, um eine sichere Konnektivität mittels der Unternehmens Firewalls sicherzustellen.

NUTZUNG VON SINGLE SIGN-ON

Die gleichen Windows-Anmeldeinformationen, mit denen Benutzer bei drahtlosen Netzwerken authentifiziert werden, können auch zum Authentifizieren von VIA-Benutzern verwendet werden. Durch die Nutzung dieser Anmeldeinformationen stellt VIA im Hintergrund automatisch

eine Verbindung für den User her, ohne dass diese zur Eingabe von Benutzername oder Kennwort aufgefordert wird.

Beim anmelden an das Unternehmensnetzwerk mittels der automatischen Verbindungsfunktion kommen die Benutzer in den Genuss einer kontinuierlichen Anbindung und Authentifizierung, bei welcher keine gewohnten Arbeitsabläufe geändert werden müssen. Organisationen, bei denen zusätzliche Authentifizierungsmethoden erforderlich sind, können herkömmliche Systeme mit Benutzername und Kennwort bzw. Tokens verwenden.

UNTERSTÜTZUNG VON BENUTZERROLLEN

Beim VIA-Agenten werden rollenbasierte Richtlinien und Regeln von Firewalls beim lokalen und entfernten Netzwerkzugriff eingesetzt, um für Endbenutzer unabhängig vom Standort eine gewohnte, gleichbleibende Vorgehensweise zu gewährleisten. Die Lösung kann ferner so konfiguriert werden, dass beim gleichen Arbeitsgerät separate Zugriffsrollen und Richtlinien möglich sind, die davon abhängen, an welchem Standort sich der Benutzer am Netzwerk anmeldet.

UMFASSENDE UNTERSTÜTZUNG FÜR DIE FEHLERSUCHE

Die integrierten Protokollier- und Diagnosefunktionen von VIA ermöglichen eine Remote Fehlersuche und Behebung von Verbindungsproblemen, ohne dass Benutzer eine komplexe Anzahl an zusätzlicher Hard- oder Software einsetzen muss. Dadurch wird der administrative Vorgang verkürzt sowie der Benutzerreparaturprozess vereinfacht.

Im Bedarfsfall können Protokollaufzeichnungen (Log Files) per E-Mail an die Supportabteilung gesendet werden, um eine detailliertere Fehlerbehebung zu ermöglichen. Zu den Diagnosetools zählen Verbindungsprotokolle, Systeminformationen, erkannte WLAN-Netzwerke und detaillierte Konnektivitätstests.

WINDOWS ZERO CONFIGURATION-UNTERSTÜTZUNG

Optional können mit VIA WLAN-Einstellungen mit dem Windows Zero Configuration-Suppliment (WZC) konfiguriert werden. Dadurch können Netzwerkadministratoren bevorzugte WLAN-Einstellungen dynamisch an Benutzer übermitteln, ohne dass sie sich dazu an deren Computer begeben oder zusätzliche Tools verwenden müssen.

VIRTUAL INTRANET ACCESS-AGENT

UMFASSENDE SICHERHEIT

VIA kann Internetdatenverkehr für die erhöhte Sicherheit mobiler Mitarbeiter an Aruba CSS weiterleiten. Über Cloud-gestützte Sicherheitszentren auf der ganzen Welt sorgt CSS für einen umfassenden Schutz, unter anderem durch Technologien wie erweiterte URL-Filterung, P2P-Kontrolle, Anti-Virus, Anti-Malware, Botnet-Erkennung und Data Loss Prevention (DLP).

VIA und CSS kombinieren hohen Durchsatz und niedrige Latenz zur Bereitstellung sicherer, Cloud-gestützter Netzwerke für mobile Mitarbeiter, unabhängig von deren Arbeitsplatz und Standort.

ZUGRIFF IM UNTERNEHMEN, AM HEIMARBEITSPLATZ UND UNTERWEGS

VIA ist als Teil des ArubaOS™-Betriebssystems lizenziert und auf den Aruba-Serien 600 und 3000 sowie den Mobility Controllern 6000 verfügbar. Es sind keine weiteren VPN-server oder -Anwendungen erforderlich.

Mit VIA verbinden sich die Benutzer wie mit dem Netzwerk in der Firmenzentrale oder in Zweigstellen. Egal ob lokaler oder entfernter Zugriff, der Benutzer muss seine gewohnte Arbeitsweise nicht umstellen.

UNTERSTÜTZTE SICHERHEITSPROTOKOLLE

- Verschlüsselung: AES-GCM-128, AES-GCM-256, AES256, AES192, AES128, 3DES, DES
- Hash: SHA-256, SHA-384, SHA, MD5
- Authentifizierung: Preshared key, RSA, RSA und ECDSA, Smartcard
- Diffie-Hellman Group: Group 1, Group 2, ECDH Group 19, ECDH Group 20
- IPsec IKEv2

AUTHENTIFIZIERUNGSOPTIONEN

- Benutzername/Kennwort und mehrstufige Authentifizierung per Zertifikat
- Smartcard

FORWARDING MODES

- Tunnelmodus
- Split Tunnel Mode

UNTERSTÜTZTE CLIENT-BETRIEBSSYSTEME

- Windows® 7 (32 und 64 Bit)
- Windows Vista (32 und 64 Bit)
- Windows XP, Service Pack 2 oder höher
- Mac OS X
- Möglichkeit der optionalen Konfiguration einer Windows-WLAN-Client-Konfiguration

UNTERSTÜTZTE ARUBA MOBILITY CONTROLLER

- Mobility Controller 6000 mit M3-Controllermodul
- Mobility Controller der Serie 3000
- Mobility Controller der Serie 600

BESTELLINFORMATIONEN

TEILENUMMER	BESCHREIBUNG
LIC-620-PEFV	Policy Enforcement Firewall for Aruba 620 controller VIA agent
LIC-650-PEFV	Policy Enforcement Firewall for Aruba 650 controller VIA agent Policy
LIC-651-PEFV	Policy Enforcement Firewall for Aruba 651 controller VIA agent
LIC-3200-PEFV	Policy Enforcement Firewall for Aruba 3200 controller VIA agent
LIC-3400-PEFV	Policy Enforcement Firewall for Aruba 3400 controller VIA agent
LIC-3600-PEFV	Policy Enforcement Firewall for Aruba 3600 controller VIA agent
LIC-M3-PEFV	Policy Enforcement Firewall for Aruba M3 module VIA agent



WWW.ARUBANETWORKS.COM | 1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel.: +1 408.227.4500 | Fax: +1 408.227.4550 | info@arubanetworks.com