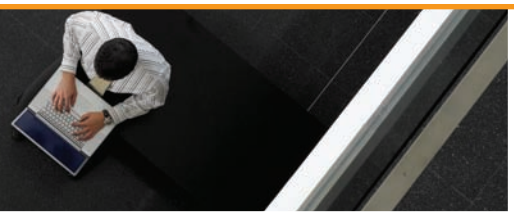
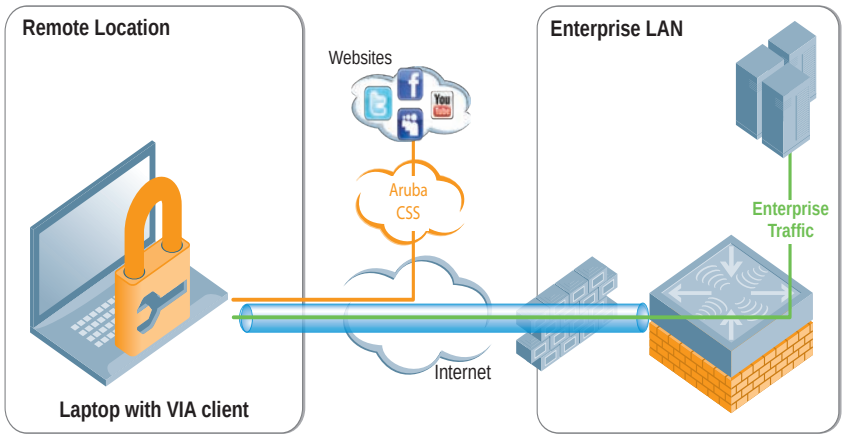


产品介绍
虚拟企业内网接入客户端软件

虚拟企业内网接入代理

Aruba 虚拟企业内网接入Virtual Intranet Access™(VIA™)客户端软件可为Windows和AppleMacBook笔记本电脑提供安全的远程网络连接。VIA是Aruba Virtual Branch Network™虚拟分支机构网络(VBN™)解决方案中的一个重要组件，可作为Aruba移动控制器的一个软件许可选件。



VIA是一套整合了IPsec/SSLVPN的解决方案，VIA可对网络连接进行扫描，并可根据网络环境和需要自动选择最佳的连接方式（IPsec或SSLVPN）接入企业网络。与传统的VPN软件不同，VIA不仅可以为用户提供“零配置”体验，还可以通过VIA配置笔记本电脑上的WLAN设置。

为了获得更高的安全性，VIA支持基于云的Aruba内容安全服务(CSS)，能够对终端设备提供全面防护，屏蔽来自互联网的各类威胁和攻击。

集成解决方案

如果订购了Aruba策略执行防火墙(PEF)软件许可，VIA可从移动控制器直接下载，或从现有的软件管理平台分离出来。VIA可直接连接移动控制器，并可进行软件和配置更新，不需要其他额外的VPN硬件。

IPSEC自动连接

那些经常出差的员工会通过宾馆、机场、咖啡馆和3G进行网络接入，这样就需要安全的链路来访问企业内部资源。传统的VPN通常要求用户启动额外的软件，并且经历一个复杂而痛苦的配置和登录过程。

但是，VIA可以自动检测网络连接，并可判别该连接是否在企业内部网络。如果不是内网连接，则VIA将建立一个连接数据中心的IPsec安全连接，因此无论用户身在何处，都可以进行无缝的企业内部网络接入。

可通过SSL封装的IPSEC连接

VIA使用标准的IPsec协议来保护安装VIA的终端设备与位于数据中心的Aruba移动控制器之间的通信。当客户端通过本地IPsec进行连接时，可以确保获得最快最安全的连接。如果防火墙阻止了IPsec直接连接，VIA还可以将IPsec包封装在SSL报文中，这样就可以透过防火墙进行安全连接。

便捷的单次登录

那些用于验证用户接入无线局域网(WLAN)的Windows证书也可以用于验证VIA用户。VIA可以利用这些证书，自动在后台建立连接，而不需要用户额外的输入用户名和密码。

通过使用VIA的自动连接功能，用户将会获得一致性的连接和认证体验，不需要改变他们的现有工作习惯。那些需要其它认证方式的企业也可以使用传统的用户名和密码或Token 令牌来认证。

基于用户的状态防火墙支持

对于本地和远程网络接入，VIA客户端都使用相同的基于用户的状态防火墙策略，以确保无论最终用户身在何处，都能获得一致的网络访问体验。此外，经过配置后，根据用户从不同的地方接入网络，VIA还可以在相同的终端设备上使用不同的安全接入策略。

强大的故障排除支持

VIA中内置的日志和诊断功能支持远程对VIA连接问题进行故障排除，不需要用户本地使用一系列复杂的工具。这样可以缩短解决问题的时间，简化了管理和最终用户的维修过程。

如果需要，用户可以将客户端日志以电子邮件的方式发送到IT支持中心，以便进行更详细的故障排除。VIA诊断工具包括连接日志、系统信息、检测到的WLAN网络和详细的连接测试等。

WINDOWS ZERO CONFIGURATION功能支持

此外，VIA还能够使用Windows Zero Configuration (WZC) Supplicant来配置WLAN设置。这样可以帮助网络管理员将首选的WLAN设置动态推送到客户端，而不需要接触到用户的终端，也不需要管理额外的工具软件。

虚拟企业内网接入客户端软件

全面的安全性

VIA可以将互联网流量定向到基于云的Aruba内容安全服务 (CSS)，提高移动员工的信息安全性。Aruba内容安全服务 (CSS) 可以从全球基于云的安全性中心提供全面的防护，包括高级URL过滤、端到端控制、防病毒/防恶意软件、僵尸网络 (Botnet) 检测和数据丢失防护 (DLP)。

对于移动员工来说，无论他们身在何处，通过基于云架构的网络，VIA和CSS将为用户提供高吞吐量和低延迟性能的网络安全防护。

企业、家庭办公室和远程接入

VIA是作为ArubaOS™操作系统的一部分，在Aruba 600系列、3000系列和6000移动控制器上都提供这一组件，可通过软件许可的方式获得，不需要额外的VPN服务器或设备。

通过VIA在用户接入总部或分支机构网络，进行本地或远程数据访问时，都将获得相同的无缝连接的体验。

支持的安全协议

- 加密：AES-GCM-128,AES-GCM-256,AES256,AES192, AES128, 3DES, DES
- Hash：SHA-256, SHA-384, SHA, MD5
- 认证：Preshared key, RSA, RSA and ECDSA, Smart card
- Diffie-HellmanGroup：Group1, Group2, ECDHGroup 19, ECDH Group 20
- IPsec IKEv2

认证选项

- 用户名/密码和证书多因素认证
- Smart card

转发方式

- 隧道方式
- 分离隧道方式

支持的客户端操作系统

- Windows® 7 (32位和64位)
- Windows Vista (32位和64位)
- Windows XP, Service Pack 2或以上版本
- Mac OS X
- 提供可选的用于Windows WLAN客户端的配置

支持的ARUBA移动控制器

- 带M3控制器模块的6000移动控制器
- 3000系列移动控制器
- 600系列移动控制器

订购信息

产品编号	描述
LIC-620-PEFV	Aruba 620控制器VIA客户端的策略执行防火墙模块软件许可
LIC-650-PEFV	Aruba 650控制器VIA客户端的策略执行防火墙模块软件许可
LIC-651-PEFV	Aruba 651控制器VIA客户端的策略执行防火墙模块软件许可
LIC-3200-PEFV	Aruba 3200控制器VIA客户端的策略执行防火墙模块软件许可
LIC-3400-PEFV	Aruba 3400控制器VIA客户端的策略执行防火墙模块软件许可
LIC-3600-PEFV	Aruba 3600控制器VIA客户端的策略执行防火墙模块软件许可
LIC-M3-PEFV	Aruba M3模块VIA客户端的策略执行防火墙模块软件许可

ARUBA® networks
安移通科技（中国）有限公司
北京市朝阳区朝外大街18号丰联广场A座2101
电话：010-65805588 传真：010-65805566 www.arubanetworks.com.cn