Ivanti Connect Secure：面向零信任网络的下一代安全访问解决方

概述

自带设备（BYOD）和云业务的扩张，增加了随时随地从设备——包括个人生产力设备（笔记本电脑、智能手机、智能平板）或IP设备（打印机、摄像头、电话）——对传统数据中心或云数据或应用的访问需求。

Ivanti Connect Secure为远程和移动用户提供了一个无缝的化、高效益的SSL VPN解决方案，供他们从任何具有网络功能的设备访问企业资源，并且随时随地皆可。

产品描述

企业和服务提供商面临严峻挑战。他们需要提 供无关地点和设备类型的网络连接能力，并且这种 连接必须是安全的，能够控制仅授权用户能访 问资源。数据泄露和威胁继续呈急剧上升态势，越来越多的员工和用户希望使用他们自己的个 人生产力解决方案。Ivanti Connect Secure为 远程和移动用户提供安全的验证访问，供他们 从任何支持网络的设备访问企业资源——并且 随时随地皆可。它是部署最广泛的SSL VPN，适用于各主要行业中任何规模的组织。

Ivanti Connect Secure包括Secure Clients和 AppConnect SDK。Ivanti Clients是用于移动和 个人计算设备的动态、多服务网络客户端。Ivanti Clients部署简单，使用户能够从任何设备、任何地方“一触即连“。

AppConnect SDK为iOS和Android客户端提供单应用 SSL VPN连接能力，使IT部门能够为其用户创造更加透明和安全的移动应用体验。

基本架构和关键组件

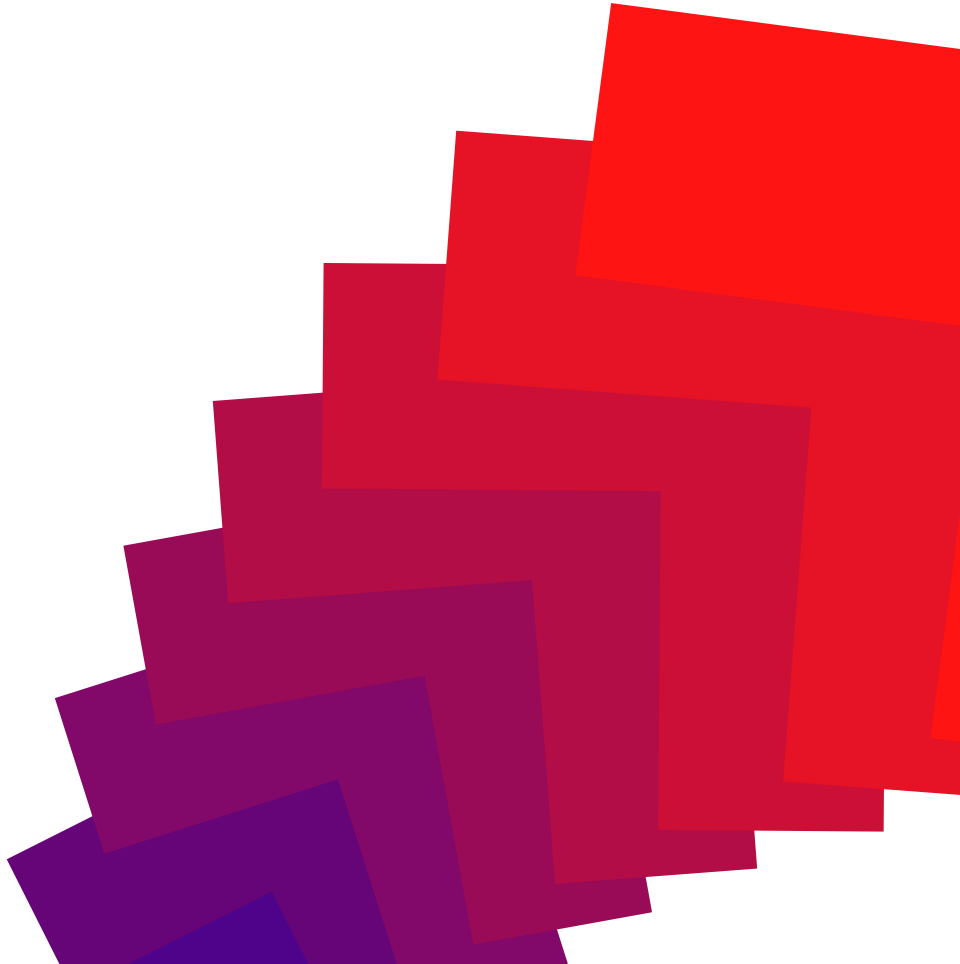
Ivanti Connect Secure在Ivanti Appliance Family中以硬件（PSA系列）或虚拟器件（PSA-V系列）的形式提供，具体如下所示：

- PSA3000：固定配置，机架式，适合中小企业，最多同时支持200并发SSL VPN并发用户。
- PSA5000：固定配置，适合可扩展的中型企业，最多同时支持2,500并发SSL VPN并发用户。
- PSA7000：固定配置，适合满足大型企业最高扩展性需求，最多同时支持25,000并发SSL VPN并发用户。
- 虚拟器件（PSA-V系列）：ESXi、KVM、Hyper-V、Microsoft Azure、Amazon AWS、OpenStack Fabric和Alibaba Cloud器件，可实现SSL VPN服务的可扩展灵活部署. 虚拟器件（PSA-V系列）包括：
  - PSA3000-V：支持2个vCPU核心和最多200并发用户。上或需要启用什么服务。有了Ivanti，连接就能正
  - PSA5000-V：支持4个vCPU核心和最多2500并发用户。
  - PSA7000-V：支持8个vCPU核心和最多10,000 并发用户。

Secure Clients

Secure Clients在用户与网络（包括数据中心和云）之间实现安全连接。Ivanti Clients用户体验极佳，它可以在用户端点上动态启用适当的网络和安全服务。用户可以专注自己的工作，不必分心去弄清他们在什么网络上或需要启用什么服务。有了Ivanti，连接就能 常态化，帮助实现移动设备的生产力。Ivanti Client提供动态访问控制，可在Microsoft Windows设备的远程（SSL VPN）和本地（NAC）访问控制服务之间无缝切换。Ivanti Client还能对移动和桌面计算设备执行全面的端点安全态势评估，并在必要时进行隔离和修复。

数字世界继续创造着BYOD不可企及的劳动生产力。更多企业正在结合不同应用，并跨越多个数据中心和云资源，以满足不断增长的需求和生产力。这样做的结果是一套混用私有和公共IT架构的混合方案。了解如何利用Ivanti Cloud Secure拥抱Hybrid IT，以及如何能够将 云和数据中心访问融合为无缝化用户体验供你的下一代员工队伍享用。



ivanti

功能和优点

功能	说明
Layer 3 SSL VPN	■ 双路传输（SSL + 封装安全有效载荷）完整Layer 3 VPN 连接，提供细化访问控制。 ■ “VPN始终在线及锁定模式”和“仅VPN访问”模式，以遵守合规要求（VPN连接根据用户的位置自动连接/断开）。
应用VPN	■ 客户端/服务器代理应用，将流量从特定应用通过隧道传输至特定目的地（仅适用于Windows设备）。 ■ “按需VPN”和“单应用VPN”，可实现无缝、安全的终端用户体验。
Layer 7 Web单点登录（SSO）（基于SAML）	■ 允许终端用户通过Layer 3隧道经身份验证接入网络，同时允许用户经由SAML SSO支持功能通过其浏览器以SSO方式访问Web应用。
条件访问	■ 按照一套自动策略对设备和用户加以验证和确认，以保护网络和数据。每个访问尝试都经动态评估，并根据现行策略加以实时控制。实现对应用访问的细化控制和零信任执行。
优化终端用户体验	■ 在远程访问与本地局域网访问之间平滑切换（Ivanti Policy Secure）。 ■ 单点登录（SSO）功能可实现从远程或现场位置快速、安全地访问（通过集成Ivanti Cloud Secure和Ivanti Policy Secure）。
端点完整性和安全评估	■ 通过简单的策略定义，在身份验证前对终端用户设备进行评估和修复。 ■ Windows 10（桌面及移动）Mac OS X、Apple iOS和Android。
灵活的启动选项（独立客户端、基于浏览器的启动）	■ 用户可以通过他们的网络浏览器轻松启动SSL VPN，或直接从他们的桌面启动。 ■ Auto Connect功能允许设备自动连接到VPN，这可以在机器启动时也可以在用户登录时执行。 ■ 当一个经批准的应用需要访问企业资源时，VPN按需启用功能会利用操作系统功能在后台无缝地自动触发VPN。
支持Cloud Secure解决方案	■ 将云和数据中心访问融合为一套无缝化用户体验供员工享用下一代远程访问体验。 ■ 能够为混合型DC访问添加合规性规则。
预配置选项（仅Windows和Mac）	■ 管理员可以为某个部署任务预配置一系列网关供终端用户从中选择。

功能和优点（续）

身份验证选项	■ 使用多个用户属性的动态多因素自适应验证方法。 ■ 管理员可以部署Ivanti对远程用户执行身份验证，可使用各种验证机制，包括Windows Hello for Business支持下的生物特征识别验证、硬件令牌、智能卡、软令牌、Google Authenticator、一次性密码和证书验证。 ■ 管理员可以选择通过所需接口（内部/外部/管理）发送AAA流量，以便将用户身份验证任务委托给身份提供程序。
RDP/Telnet/SSH会话，使用HTML5	■ 100%无客户端访问，使用HTML5浏览器。
VMware Horizon和Citrix XenApp/ XenDesktop VPN	■ Ivanti支持最新版的Vmware和Citrix。
细化SSL密码配置	■ 使管理员能够选择特定密码而不是那些预配置密码，以实现高度安全合规。
REST API	■ 一个全面的基于REST的API，用于对设备进行程序化访问。

端到端分层安全保护

功能	说明	优点
端点状态合规检查	■ 在远程访问会话之前和期间，比如要求安装/运行端点安全应用（防病毒、个人防火墙等）时，对端点设备进行检查，以确认可接受的设备安全态势；以及检查符合 IT 要求的操作系统版本、补丁级别、浏览器类型和许多其他要求。 ■ 支持为客户特殊要求而定制的检查。 ■ 不合规的端点可能被隔离、拒绝访问或允许访问，具体取决于管理员定义的策略。 ■ 只要有可能，Host Checker就会通过更新不符合企业安全策略的软件应用，自动修复不合规的端点。	■ 确保端点设备在符合企业安全策略条件后才会被授予网络访问权限。 ■ 必要时修复设备并隔离用户。 ■ 能够确保终端设备上不会留下任何潜在的敏感数据。
Host Checker中的可信网络连接（TNC）支持功能	■ 允许与不同的端点安全解决方案（从防病毒到补丁管理到合规性管理解决方案）进行互操作。	■ 使客户能够在采用第三方供应商提供的端点安全解决方案的同时充分利用现有投资。
VPN始终在线	■ 确保所有来自端点的流量都通过隧道发送；检测到互联网连接时会自动建立隧道。	■ 使企业能够对来自端点的所有流量掌握其安全性、合规性和可见性，即使它们并非本地端点。

易于管理

功能	说明	优点
移动设备管理（MDM）集成	■ 启用综合报告和仪表板以简化管理。 ■ 利用MDM属性实现更智能化和集中化的策略创建。 ■ 便于以基于MDM的透明“零接触“方式将Ivanti Clients部署到iOS和Android设备上。	■ 扩展MDM投资以获得全面端点可见性并支持其他移动用例。
安全浏览器	■ 该移动浏览器可安全访问企业网络应用，无需安装/管理/启动VPN客户端。	■ IT部门不必担心在移动设备上部署和管理VPN。终端用户则不必担心启动VPN的问题。实现无缝的终端用户体验，用户照常启动浏览器就能访问其资源。
安全访问SAP 应用	■ 将Ivanti Per-App VPN SDK嵌入SAP的Fiori移动应用之中。	■ 通过现有的Ivanti VPN器件为SAP服务提供透明、安全的数据中心连接。
与强大的身份验证和识别及访问管理（IAM）平台集成	■ 有能力支持SecurID、安全声明标记语言（SAML），包括支持基于标准的SAML v2.0，以及公钥基础设施（PKI）/数字证书。	■ 利用现有的企业身份认证方法来简化管理。
桥证书认证机构（BCA）支持	■ 以客户端证书验证方式支持联盟式PKI部署。桥证书认证机构是一个 PKI扩展（如RFC 5280所规定），用于交叉认证由不同信任锚（根 CA）签发的客户端证书。 ■ 同时，使客户能够在管理UI中配置策略扩展，用于在证书验证期间强制执行。	■ 让使用高级PKI部署的客户得以部署Ivanti，以执行符合严格标准的证书验证——然后才允许数据和应用在组织和用户之间共享。
支持多主机名	■ 能够从一台设备中托管不同的虚拟外网网站。	■ 节省了增加服务器的成本。 ■ 减轻管理开销。 ■ 通过差异化条目URL提供透明的用户体验。
支持多主机名	■ 从一个控制台查看和控制企业对数据中心和云的访问。	■ 快速访问动态信息和报告。 ■ 经由拖放功能实现可定制布局。
可定制用户界面	■ 创建完全定制化的登录页面。	■ 为特定角色提供个性化外观，简化用户体验。
应用程序启动器（AL）	■ 增强对不是基于JAVA的浏览器的支持。	■ 支持不支持Java和Active X的最新一代浏览器（Apple、Microsoft、Google、Firefox,等）。

丰富的访问权限管理功能

功能	说明	优点
使用自定义表达式的动态角色映射	■ 结合网络、设备和会话属性来决定允许哪些类型的访问。 ■ 可以在每个会话基础上使用动态属性组合来做出角色映射决策。	■ 使管理员能够为每个独特会话按目的进行配置。
SSL VPN与NAC联合（Ivanti Policy Secure）	■ 登录时将SSL VPN用户会话无缝配置为NAC会话。 ■ 由于会话数据是在Ivanti面向SSL VPN的控制器和面向NAC的控制器之间共享的，因此在这类环境中，用户只需要验证一次就可以获得访问权限。	■ 为无论远程还是本地用户提供无缝访问功能，只需一次登录即可访问受访问控制策略保护的企业资源。 ■ 简化终端用户体验。
支持RSA身份验证管理器	■ RSA身份验证管理器8.1能实现基于风险的身份验证。	■ 经由电子邮件账户提供其他身份验证层选项。
基于标准的内置式一次性动态密码（TOTP）	■ 可使用智能手机执行多因素验证。	■ 利用无处不在的智能手机，推出低成本自助式双因素验证机制，其中一次性密码由移动应用生成。基于RFC6238实现。
每用户多个会话	■ 允许远程用户发起多个远程访问会话。	■ 使远程用户能够同时打开多个已验证会话，例如从笔记本电脑和智能手机同时访问VPN时。
用户记录同步	■ 支持不同Ivanti控制器之间的用户记录（如用户书签）同步。	■ 确保那些经常往来不同地区之间并因此需要连接到不同Ivanti控制器运行Ivanti Connect Secure服务的用户能够获得一致的体验。
移动友好型SSL VPN登录页面	■ 提供为移动设备定制的预定义HTML页面，包括Apple iPhone及iPad、Google Android和Nokia Symbian设备。	■ 为移动设备用户提供更简单、更流畅的用户体验，以及为其设备类型定制的网页。

灵活的单点登录（SSO）能力

功能	说明	优点
针对云和网页应用访问的SAML单点登录	■ 经由基于SAML 2.0的SSO功能登录各种网页应用，包括许多当前最流行的软件即服（SaaS）应用，例如Salesforce.com和Google Apps。 ■ 包含SSO功能，即使是通过Ivanti Connect Secure Layer 3 VPN隧道连接也一样，这在业界也是独一无二的。 ■ Ivanti Connect Secure既支持以SAML Identity Provider（IdP）也支持以SAML Service Provider（SP）身份进行部署。	■ 单点登录到用户基于网络和云的应用，简化了用户的连接体验。
Kerberos Constrained Delegation	■ 支持Kerberos Constrained Delegation协议。 ■ 当用户使用无法代理到后端服务器的凭证登录Ivanti Connect Secure时，网关将代表用户从活动目录基础设施中调取一个Kerberos票证。 ■ 该票证将在整个会话期间被缓存在Ivanti Connect Secure上。 ■ 当用户访问受Kerberos保护的应用时，器件将使用缓存的Kerberos凭证将用户登录到应用，而不提示输入密码。	■ 消除了公司管理静态密码的需要，从而减少了管理时间和成本。
支持Kerberos SSO和NT LAN Manager（NTLMv2）	■ Ivanti Connect Secure将通过Kerberos或NTLMv2使用用户凭证自动验证远程用户。	■ 通过消除用户为访问不同的应用多次输入凭证的需要，简化了用户体验。
密码管理集成	■ 基于标准的接口，可与目录存储（LDAP、AD及其他）中的密码策略广泛集成。	■ 利用现有服务器验证用户身份。 ■ 用户可以直接通过Ivanti Connect Secure界面管理其密码。
基于网络的 SSO基本验证和NTLM	■ 允许用户访问受另一个访问管理系统保护的其他应用或资源，无需重新输入登录凭证。	■ ■ 减轻了用户为访问网络应用和Microsoft应用输入和维护多组凭证的需要。
基于网络的SSO 基于表单、基于 标头变量、基于SAML	■ 能够将用户名、凭证和其他客户定义属性传递给其他产品的验证表单并作为标头变量。	■ ■ 提高用户的生产力，并提供定制化体验。

按目的配置

功能	说明	优点
安全客户端	■ 单一集成式远程访问客户端，还可以为远程用户提供LAN访问控制和动态VPN功能。	■ Ivanti Client取代了为不同功能（如VPN和LAN访问控制）部署和维护多个独立客户端的需要。终端用户能够“一触即连”。
无客户端核心网络访问	■ 安全访问许多不同类型的基于网络的应用，包括许多当今最常见的网络应用，如Outlook Web Access、SharePoint及许多其他应用。 ■ Ivanti Connect Secure中的远程桌面协议（RDP）访问能够以HTML5、经由第三方RDP、通过WebSockets转换器（如Ericom）提供。	■ 提供最方便的可访问表单供用户从各种终端用户设备访问应用和资源，并且具有极其详细的安全控制选项。完全不用客户端，仅使用Web浏览器。
面向移动设备的 IPsec/IKEv2支持功能	■ 允许远程用户从任何支持互联网密钥交换（IKEv2）VPN连接功能的移动设备接入。 ■ 管理员可以对经由IPsec/IKEv2的访问启用严格的证书或用户名/密码验证方法。	■ 对支持IKEv2但尚未有客户端可用的新设备提供全面的L3 VPN支持。
虚拟桌面基础架构（VDI）支持功能	■ 允许与VMware View Manager互操作，使管理员能够通过Ivanti Connect Secure部署虚拟桌面。	■ 让远程用户能无缝访问其托管在VMware服务器上的虚拟桌面。 ■ 提供VMware View客户端的动态传递，包括动态客户端回退选项，以使用户能够连接到他们的虚拟桌面。
零接触配置	■ 使用OpenStack集中式编排部署PCS ■ 从本地DHCP服务器获取初始配置，无需手动输入数据 ■ 经由REST API配置和管理	■ 使客户能够允许大量的用户（包括雇员、合同工和合作伙伴）通过移动电话经由ActiveSync访问企业资源。
ActiveSync代理	■ 提供经由代理从移动设备（如iOS或Android设备）到Exchange Server的安全访问连接（强加密+证书验证），无需安装客户端软件。可实现多达5,000个同步会话。	■ 提高用户生产力，并提供定制化体验。
安全应用管理器（SAM）	■ 一个轻量化、基于Java或Windows的下载功能，能够访问客户端/服务器应用。	■ 只需使用Web浏览器就能访问客户端/服务器应用。还提供对终端服务器应用的本地访问，无需预先安装客户端。

关于Ivanti

Ivanti让无处不在的工作空间成为可能。在“无处不在的工作空间”，员工使用各种各样的设备访问IT网络、应用和数据，以便能随时随地保持工作效率。Ivanti自动化平台连接业界领先的统一端点管理、零信任安全和企业服务管理解决方案，通过单一管理界面让企业实现设备的自我修复和 自我保护，让终端用户实现自我服务。已有超 过40,000家客户，包括78家财富百强企业，选择了Ivanti来为他们发现、管理、保护和服务从云端到边缘的IT资产，并为员工提供卓越的终端用户体验，无论他们在哪里、以什么方式工作。更多信息请访问 www.ivanti.com.cn

ivanti

www.ivanti.com.cn
8610 85412999
Contactchina@ivanti.com