

利用Cisco ASA 5500系列建立VPN连接思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E5_88_A9_E7_94_A8Cisc_c101_644207.htm Cisco? ASA 5500 系列自适应安全设备是专为中小企业（SMB）和大型企业应用开发的平台，将最高安全性与VPN服务有机地结合在一起。Cisco ASA 5500 系列自适应威胁防御解决方案基于防火墙、入侵防御系统（IPS）和网络防病毒功能。作为专用VPN平台，该解决方案可以独立使用，也可以与其它解决方案配合使用。对于VPN服务，由于Cisco ASA 5500 系列提供灵活的技术，因而能根据远程接入和站点到站点连接要求，提供定制的解决方案。Cisco ASA 5500 系列提供易于管理的IP Security（IPsec）和安全套接字层（SSL）VPN远程和网络敏感型站点到站点VPN连接，使企业能够通过公共网络为移动用户、远程站点和业务合作伙伴创建安全连接。利用Cisco ASA 5500 系列，各机构不需要降低公司安全策略的完整性，就能够获得互联网的连接和成本优势。Cisco ASA 5500 系列将VPN服务与全面威胁消除服务有机地结合在一起，提供安全的VPN连接和通信。集成式自适应威胁防御功能提供统一保护，保证VPN部署不会成为网络攻击的导体，例如蠕虫、病毒、坏件或黑客等。不仅如此，还可以为VPN流量应用详细的应用和访问控制策略，使个人和用户组能够访问到他们有权访问的应用、网络服务和资源（见图1）。图1针对任意部署方案的VPN服务：带有威胁防御的增强型IPsec和SSL VPN服务 远程接入 Cisco ASA 5500 系列提供支持多种连接方式的完整远程接入VPN解决方案，包括WebVPN（SSL VPN）、Cisco VPN

Client (IPsec VPN) 以及从Windows 移动设备建立的Nokia Symbian 移动无线和无客户端接入。利用思科的远程接入技术，各企业只需部署一个集成式平台，就能广泛支持各种核心企业应用，简化管理，并提高部署灵活性。安全的远程连接可以通过SSL 型Web浏览器或VPN客户端建立，因此，不需要部署和管理独立的设备就能够获得最高的灵活性和应用接入。利用Cisco ASA 5500 系列安全设备，各企业可以为每个用户组选用最适当的技术，而不需要同时部署多种解决方案。利用安全远程接入，由于企业不再需要同时为SSL和IPsec VPN 分别建立独立的平台，因而提高了效率，降低了成本。基于IPsec的远程接入 利用IPsec 提供远程接入能够建立最增强型的可定制连接。利用IPsec，用户几乎可以访问任何应用，就好像自己与总部局域网建立了实际连接一样。思科IPsec 远程接入具有高度可定制性，利用提供的API，管理员可以编写执行程序及其它定制程序。Cisco ASA 5500 系列是思科系统? 公司提供的功能最丰富的基于IPsec 的远程接入解决方案。对于IPsec 部署，由于ASA 5500 系列充分利用了Cisco VPN 3000 系列集中器平台的特性和功能，因而能提供几乎相同的功能，但每用户吞吐量更高。不仅如此，ASA 5500 系列还能无缝地与现有VPN 3000集中器集群集成在一起，使两个平台同时为相同的用户群服务。另外，Cisco ASA 5500 系列还提供其它思科安全解决方案也提供的新型Cisco Easy VPN远程接入功能，例如Cisco PIX? 安全设备、Cisco IOS? 路由器和Cisco VPN 3000系列集中器。Cisco Easy VPN 提供可以扩展、经济高效、易于管理的独特远程接入VPN架构，并能够降低传统VPN解决方案维护远程设备配置所需要的运作成本。Cisco ASA 5500

系列设备能够将最新的VPN安全策略动态推广到远程VPN设备和客户端，以保证这些远程端点在建立连接之前先实施最新策略，从而实现最高的灵活性、可扩展性和易于使用性。Cisco ASA 5500 系列安全设备支持VPN客户端安全策略实施，在试图建立VPN连接时执行安全检查，包括安全策略执行情况、版本号以及公司管理的主机安全产品（例如Cisco Security Agent 或个人防火墙软件），然后再允许远程用户接入公司网络。另外，Cisco VPN Client 还可以根据客户端的类型、安装的操作系统以及Cisco VPN Client 软件的版本限制网络连接，以防非法VPN客户端接入公司网络。Cisco VPN Client 和 Cisco VPN 3002 Hardware Client 可以自动执行软件更新，即能够在建立VPN连接时触发更新，或者根据需要更新当前连接的VPN客户端。这种方法使企业能够轻松地更新远程用户的客户端软件。远程接入用户可以依据设备本身的内部用户数据库进行认证，也可以利用RADIUS或TACACS 通过外部源完成认证。由于与主流认证服务，包括Microsoft Active Directory、Microsoft Windows Domains、Kerberos、轻量目录访问协议（LDAP）和RSA SecurID，集成在一起，因此，不需要通过独立的RADIUS/TACACS 服务器就能完成用户认证。SSL VPN Cisco ASA 5500 系列能够同时为无客户端和完全网络接入部署提供核心SSL VPN功能。无客户端接入适用于非公司管理的桌面，例如外部网系统和公共接入点。完全网络接入适用于需要一致"局域网型"用户体验，并需要访问所有应用或网络资源的远程接入用户。基于SSL的完全网络接入通过Cisco SSL VPN Client for WebVPN提供，这种网络接入与IPSec VPN客户端相似，但不需要预装VPN Client 软件。

SSL VPN 只使用Web浏览器及其本地SSL加密，不需要预装VPN 客户端软件就几乎能够从可以接入互联网的任何位置远程访问网络资源。利用Cisco ASA 5500 系列上支持的WebVPN，能够容易地访问多种企业应用，包括Web资源、Web型应用、NT/Active Directory 文件共享（Web型）、电子邮件以及基于TCP的其它应用，例如来自与互联网相连、可以到达HTTP互联网站点的任何计算机的Telnet 或 Windows 终端服务。WebVPN 使用SSL及其后续产品Transport Layer Security（TLS）在远程用户与中央站点的特殊内部资源之间建立安全连接。使用WebVPN建立安全连接之后，不需要安装其它桌面软件就可以从任何系统接入网络。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com