

At-A-Glance

Why Should I Care About Remote-Access Virtual Private Networks (VPNs)?

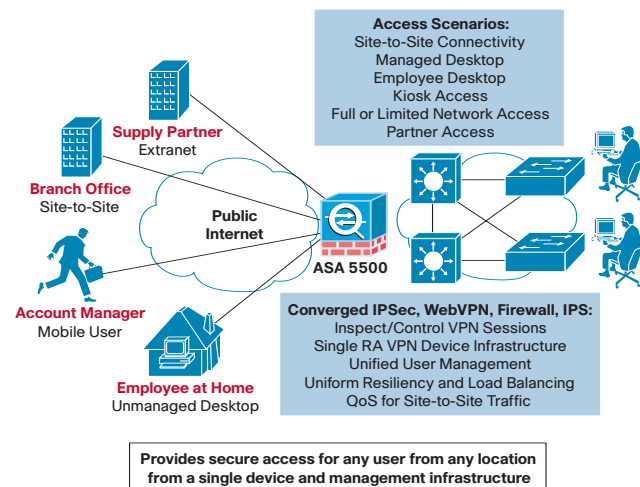
Remote-access VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet using a broadband (cable, DSL) or ISP dial connection. The ubiquity of the Internet, combined with today's VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to anyone, anyplace, at any time.

To fully realize the benefits of remote-access VPNs, corporations must deploy a robust, highly available, full-featured solution that supports a diverse user community with different connectivity and access requirements.

Cisco ASA 5500 Series Security Appliances for Remote Access

The Cisco® ASA 5500 Series provides easy-to-manage IPSec and SSL VPN-based remote-access connectivity, enabling businesses to create secure connections across public networks to mobile users, remote sites, and business partners. The Cisco ASA 5500 Series enables organizations to gain the connectivity and cost benefits of the Internet, without compromising the integrity of the corporate security policy. By converging VPN services with comprehensive threat mitigation services, the Cisco ASA 5500 Series provides secure VPN connectivity and communications. Integrated threat protection capabilities help ensure that the VPN deployment does not become a conduit for network attacks such as worms, viruses, malware, or hacking. Furthermore, detailed application and access control policy can be applied to VPN traffic, so individuals and groups of users have access to the applications, network services, and resources to which they are entitled (Figure 1).

Figure 1. VPN Services for Any Deployment Scenario: Robust IPSec and SSL VPN Services with Threat Prevention



The Cisco ASA 5500 Series provides a complete remote-access VPN solution that supports numerous connectivity options, including WebVPN (SSL VPN), Cisco VPN Client (IPSec VPN), and connectivity for Nokia Symbian mobile wireless and PDA clients. Taking advantage of Cisco's remote-access expertise, enterprises can deploy a single integrated platform with broad support for core enterprise applications, ease of management, and deployment flexibility.

Secure, remote connections can be established from either an SSL-capable Web browser or a VPN client, allowing for maximum flexibility and application access without the need to deploy and manage separate devices. With Cisco ASA 5500 Series security appliances, enterprises can choose the most appropriate technology—IPSec or SSL VPN—for each user segment without deploying parallel solutions. The inefficiency and added cost of having separate, distinct platforms for both SSL and IPSec VPNs is eliminated.

Broad Application Support for SSL VPN

The Cisco ASA 5500 Series offers extensive application support through its dynamically downloaded SSL VPN client, enabling network-layer connectivity to virtually any application. Citrix application access is provided in a truly clientless manner, allowing a seamless, low-overhead extension of the network resources to VPN users through a standard Web browser. Pure clientless and thin-client port forwarding options may be deployed for environments with limited application access requirements, such as extranets.

With any VPN session, authentication of both the user and the endpoint device is extremely important. The Cisco ASA 5500 Series offers the ultimate in endpoint security—Cisco Secure Desktop. This functionality delivered as part of Cisco ASA 5500 Series Software Release 7.1, provides a consistent and reliable means of eliminating all traces of sensitive data by providing a single secured location for session activity and removal on the client system. In addition, Cisco Secure Desktop can define different policies and profiles based on identification of specific network locations and the types of network devices (home PC, Internet kiosk, or corporate laptop), helping ensure that all confidential data is protected without impacting user productivity. Whether users are accessing the network from a corporate-managed PC, personal home computer, or public terminal, the Cisco Secure Desktop helps ensure complete data protection before, during, and after the SSL VPN session.

For IPSec deployments, the Cisco ASA 5500 Series leverages features and functionality from the Cisco VPN 3000 Series Concentrator platform, thereby delivering nearly identical capabilities but with great per-user throughput. Furthermore, the Cisco ASA 5500 Series integrates seamlessly with existing Cisco VPN 3000 Series Concentrator clusters, enabling both platforms to serve the same user population. Innovative features include support of Cisco Easy VPN remote-access capabilities for a uniquely scalable and easy to manage VPN architecture, and Cisco VPN Client security posture

enforcement and automated software updates. These features offer the ultimate flexibility, scalability, and ease of use for VPN deployments.

Threat Protection for VPN Connections

Worms, viruses, application-embedded attacks, and application abuse are considered among the greatest security challenges in today's networks. All too often, VPNs are often deployed without proper inspection and threat mitigation applied at the tunnel termination point at the corporate location, thereby allowing malware from remote users to infiltrate the network and spread.

With the Cisco ASA 5500 Series, proper inspection and threat mitigation can be designed as part of the VPN solution without any additional cost or design, deployment, or operational complexity. With the converged threat mitigation capabilities of the Cisco ASA 5500 Series, customers can detect malware and stop it before it enters the network interior and spreads. For application-embedded attacks, such as spyware or adware spread via file-sharing peer-to-peer networks, the Cisco ASA 5500 Series deeply examines application traffic to identify dangerous payload and drop its contents before it reaches its target and causes damage.

Application-aware inspection engines provide rich stateful inspection services, tracking the state of all authorized network communications and preventing unauthorized network access. These integrated capabilities create a strong multilayered defense for today's ever-changing network environments. Detailed security policy is applied to VPN traffic, so individuals and groups of users have access to the services and resources to which they are entitled. All VPN traffic is decrypted and inspected to ensure that only appropriate content is allowed through the device.

The Cisco ASA 5500 Series enables a network administrator to define a single policy that incorporates both security and connectivity for remote offices and workers. This single policy provides unparalleled security, while maintaining an accessible network environment. Cisco ASA 5500 Series security appliances provide an integrated approach to security that enables organizations to gain the connectivity and cost benefits of the Internet, without compromising the integrity of the corporate security policy.

Integrated Management

The integrated Cisco Adaptive Security Device Manager provides a world-class Web-based management interface that greatly simplifies the deployment, ongoing configuration, and monitoring of a single Cisco ASA 5500 Series security appliance. VPN and intelligent setup wizards provide easy integration into any network environment, while informative monitoring features, including a dashboard and real-time syslog viewer, provide vital device/network health status and event monitoring at a glance. Full management of all threat mitigation features is provided, offering a single console to configure and secure all aspects of VPN connectivity.

At-A-Glance

User Authentication Flexibility

The Cisco ASA 5500 Series supports multiple authentication mechanisms, allowing a company to choose the method most appropriate for their environment. Remote-access users can be authenticated against the internal user database on the appliance itself, or via an external source using RADIUS or TACACS+. Native integration with popular authentication services, including Microsoft Active Directory, Microsoft Windows Domains, Kerberos, Lightweight Directory Access Protocol (LDAP), and RSA SecurID, allows for authentication of users without requiring a separate RADIUS/TACACS+ server to act as an intermediary.

Summary

The Cisco ASA 5500 Series provides a flexible, full-featured platform for VPN deployments. Secure, remote-access sessions can be established from either an SSL-capable Web browser or a VPN client, allowing for maximum flexibility and application access.

With the Cisco ASA 5500 Series, proper access control, application inspection, and threat mitigation can be designed as part of the VPN solution without any additional cost or design, deployment, or operational complexity. Administrators can define a single network policy to provide unparalleled security, while maintaining an accessible network environment.

By taking advantage of Cisco's depth of VPN expertise, enterprises can deploy a single integrated platform with broad support for core enterprise applications, ease of management, and deployment flexibility.