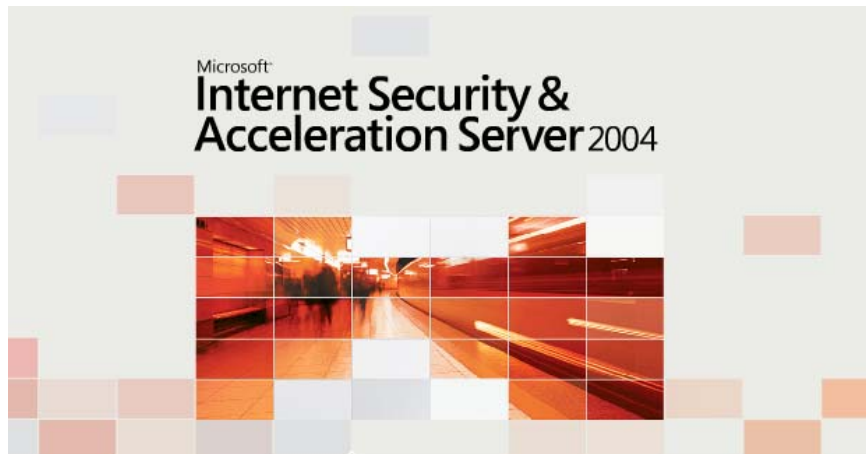


What Is ISA Server 2004?



© 2006 Adjigol.com All Rights Reserved

Microsoft Internet Security and Acceleration (ISA) Server 2004 is the advanced stateful packet and application-layer inspection firewall, virtual private network (VPN), and Web cache solution that enables enterprise customers to easily maximize existing information technology (IT) investments by improving network security and performance. ISA Server 2004 is available in two versions: standard edition and enterprise edition. Information included in this product overview includes features and capabilities in both versions, unless otherwise specified.

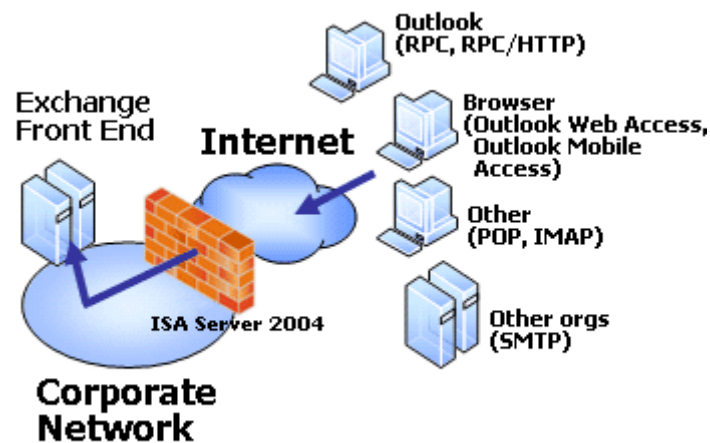
ISA Server 2004 provides advanced protection, ease of use, and fast, secure access for all types of networks. ISA Server is particularly well suited for protecting large enterprise network configurations requiring multiple firewall arrays in disparate locations that are running Microsoft client and server applications, such as Microsoft Office, Office Outlook Web Access 2003, Office SharePoint Portal Server 2003, Internet Information Services (IIS), Routing and Remote Access, Active Directory directory service, and many other Microsoft applications, servers, and services.

ISA Server contains a full featured, application-layer aware firewall that helps protect organizations of all sizes from attack by both external and internal threats. ISA Server performs deep inspection of Internet protocols such as Hypertext Transfer Protocol (HTTP), which enables it to detect many threats that traditional firewalls cannot detect. The integrated firewall and VPN architecture of ISA Server support stateful filtering and inspection of all VPN traffic. The firewall also provides VPN client inspection for Microsoft Windows Server 2003-based quarantine solutions, helping to protect networks from

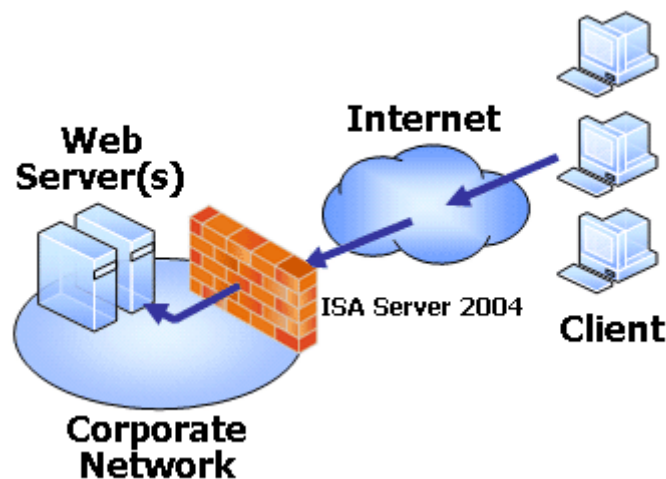
attacks that enter through a VPN connection. In addition, a completely new user interface, wizards, templates, and a host of management tools help administrators avoid common security configuration errors.

Common usage scenarios for ISA Server 2004 include:

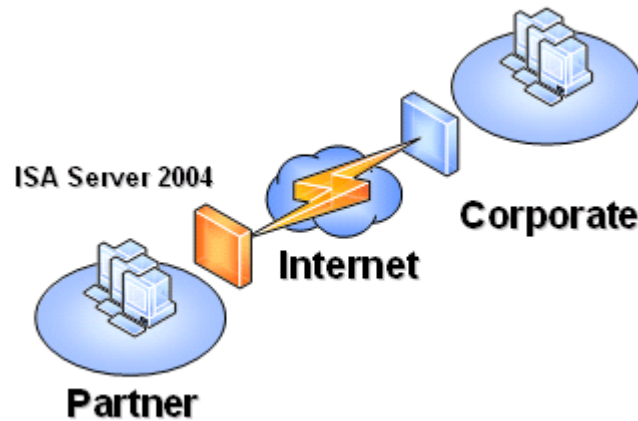
•**E-mail Access for Mobile Employees.** Provide secure e-mail access to employees outside your corporate network, including Microsoft Exchange Server 2003 and other mail servers.



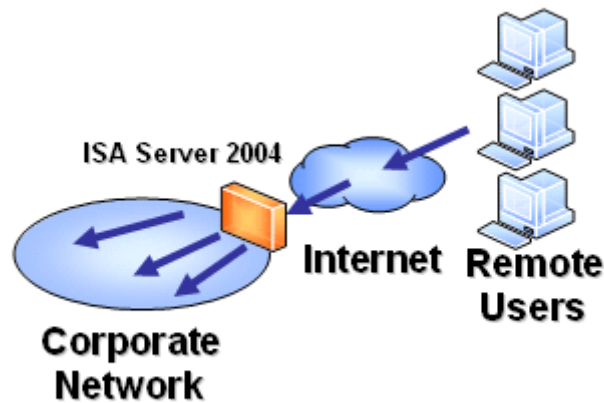
•**Establish a VPN for Remote Users.** Provide secure access to intranet information for remote users, including access to corporate resources hosted on servers running IIS and other Web servers.



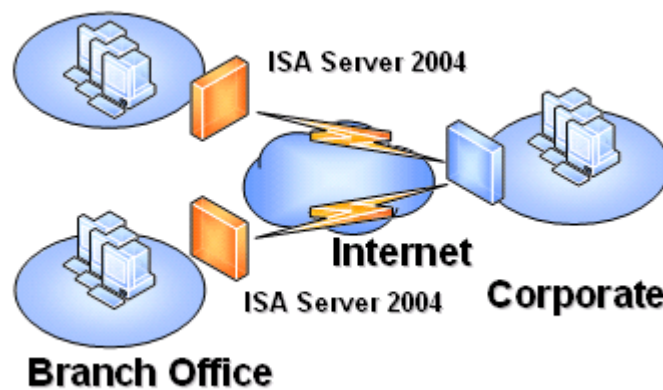
•**Create Encrypted Tunnels with Partners.** Enable secure access to corporate network information for partners, including remote access and site-to-site extranet VPNs.



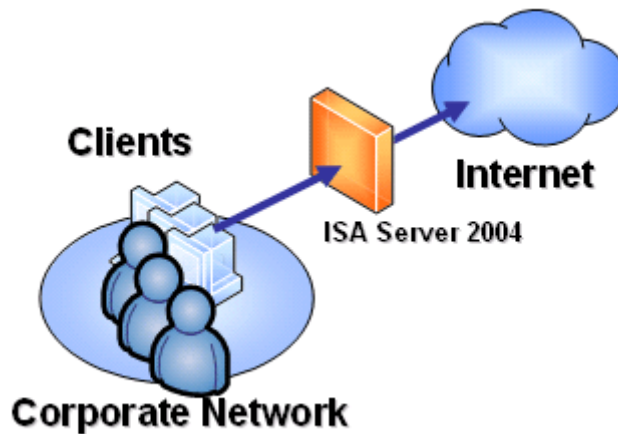
•**Remote Access for Mobile Employees.** Provide employees secure remote access to only the corporate network resources they require.



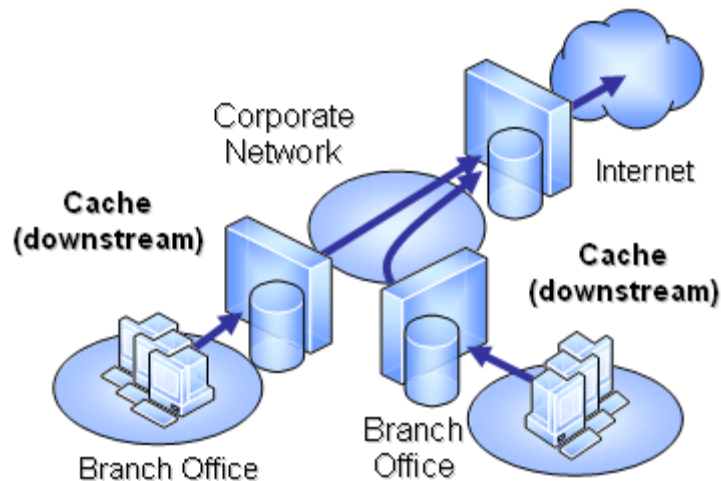
•**Link Branch Offices Together.** Enable branch offices to communicate securely with the main office over the Internet using highly secure site-to-site VPN connections.



•**Control and Protect from Malicious Traffic.** Control corporate users' Internet access and protect clients from malicious Internet traffic.



•**Cache Content for Performance.** Ensure fast access to your most frequently used Web content, thereby reducing corporate bandwidth usage costs and speeding up Web connections for corporate network users.



Benefits

Key benefits that set ISA Server 2004 apart from other firewall solutions include its advanced application-layer inspection and protection capabilities, ease of use, ability to provide fast and secure Internet access, centralized management capabilities for distributed firewall infrastructures, and its easy integration with current firewall and VPN infrastructures.

Enterprise Firewall Security	
Feature	Description
Multilayered firewall security	<p>Organizations can maximize security with packet, circuit, and application-level traffic filtering:</p> <ul style="list-style-type: none"> • Stateful packet filtering (stateful packet inspection) determines which packets will be allowed to pass through to the secured network circuit and application-layer proxy services. Stateful filtering opens ports automatically only as needed and then closes the ports when the communication ends. • Circuit filtering provides application-transparent circuit gateways for multiplatform access to Telnet, RealAudio, Windows Media technologies, Internet Relay Chat (IRC), and many other Internet protocols and services. Unlike other circuit-layer proxies, ISA Server circuit-layer security works together with dynamic packet filtering for enhanced security and ease of use. • Application filtering and stateful inspection processes commands within client computer application protocols (such as HTTP, FTP, and Gopher). ISA Server 2004 acts on behalf of the client computer, hiding the network topology and IP addresses from the outside network.
Stateful inspection	<p>ISA Server 2004 dynamically and intelligently performs stateful packet filtering (stateful packet inspection) and stateful application-layer inspection of traffic crossing the firewall. This ensures integrity of communications and prevents security breaches by intruders, hackers, worms, viruses, and suspicious command strings. Stateful inspection is done in the context of both the application-layer protocol and the state of the connection.</p>
Smart	<p>ISA Server 2004 goes beyond basic application</p>

Enterprise Firewall Security	
Feature	Description
application filtering	filtering by controlling application-specific traffic with application, command, and data-aware filters. Through intelligent filtering of VPN, HTTP, FTP, SMTP, POP3, DNS, H.323 conferencing, streaming media, and RPC traffic, ISA Server can accept, reject, redirect, and modify traffic based on its contents.
Secure server publishing	Secure server publishing helps protect Web servers, e-mail servers, and e-commerce applications from external attacks. ISA Server 2004 adds a layer of security by impersonating the published server. Web publishing rules protect internal Web servers by allowing you to specify which computers can be accessed. Server publishing rules protect internal servers from unwarranted access by external users. Intelligent application filtering protects all published servers from external attack.
Intrusion detection and intrusion prevention	Using integrated intrusion detection capabilities based on technology from Internet security systems, ISA Server 2004 generates an alert and executes an action if it detects a network intrusion attempt (such as port scanning, WinNuke, or ping of death).
Integrated virtual private networking	By integrating its services with the VPN services of Windows Server 2003 and Windows 2000 Server, ISA Server 2004 enables you to provide standards-based secure remote access to connect branch offices and remote users to corporate networks. You can apply the ISA Server firewall policy to VPN connections to gain fine-tuned control over the resources and protocols that VPN users can access.
Firewall transparency	SecureNAT provides transparent firewall access through the ISA Server computer and protection for all IP clients on ISA Server-protected networks, with no client software or configuration necessary, by

Enterprise Firewall Security	
Feature	Description
	substituting a globally valid IP address for an internal IP address. Sophisticated application-layer filters provide complex protocol support for SecureNAT clients.
Strong user authentication	ISA Server 2004 supports strong user authentication with integrated Windows authentication (Windows NT/LAN Manager and Kerberos) for its firewall and Web proxy clients. For Web proxy clients, the product supports client certificates as well as digest, basic, forms-based, and anonymous Web authentication. ISA Server 2004 Enterprise Edition can authenticate users against the local user database on the firewall in Active Directory, or it can use RADIUS to authenticate against any RADIUS-compliant directory.
SSL-to-SSL bridging	For Web servers that require authenticated and encrypted client access, ISA Server 2004 provides end-to-end security and application-layer filtering using SSL-to-SSL bridging. Unlike most firewalls, ISA Server 2004 inspects encrypted data before it reaches the Web server. The firewall decrypts the SSL stream, performs stateful inspection, and then re-encrypts the data and forwards it to the published Web server.
High availability (Enterprise Edition only)	You can use ISA Server integrated Windows NLB to configure and manage high availability for your ISA Server arrays. NLB allows online array members to transparently take over for disabled members of the array. Integrated NLB provides for NLB service health monitoring and supports all protocols with its built-in bidirectional affinity feature. ISA Server integrated bidirectional affinity supports multiple networks connected to, or through, the array.
Web Caching Server	
Feature	Description

Web Caching Server	
Feature	Description
High-performance Web caching	ISA Server 2004 uses fast random access memory (RAM) caching and an optimized disk cache to accelerate Web performance, both for ISA Server-protected network clients accessing Internet Web servers and for Internet users accessing content on a corporate Web server.
Scheduled caching	You can preload the cache with entire Web sites on a defined schedule. Scheduled downloads ensure up-to-date cache content for every user while also making content on offline Web servers available to your users.
Increased Web performance with CARP (Enterprise Edition only)	ISA Server supports the Cache Array Routing Protocol (CARP). CARP enhances Web performance by providing both load balancing and transparent failover for Web proxy browser connections. CARP efficiently manages the storage and retrieval of caching information for an array of Web caching servers through a sophisticated caching algorithm. Autoconfiguration of Web browsers ensures that IT personnel will not need to reconfigure Web browsers to support CARP.
Intuitive Firewall Management	
Feature	Description
Centralized firewall management	You can manage all ISA Server computers from a single, centralized management console. The ISA Server management console allows you to configure and manage hundreds of ISA Server computers and Web caching servers from a single location.
Enforcement of enterprise-wide firewall policy (Enterprise Edition only)	You can create a standardized set of enterprise firewall policies and automatically apply them to all ISA Server computers and Web caching servers in an array. From a single location, you can deploy enterprise policy to hundreds of firewalls belonging to multiple firewall arrays. An ISA Server enterprise administrator has fine

Intuitive Firewall Management	
Feature	Description
Edition only)	tuned, granular control over firewall policy throughout the enterprise. The high level of control includes the level of policy access authority granted to firewall array administrators.
Centralized storage of firewall policy (Enterprise Edition only)	ISA Server uses ADAM for firewall policy storage. ADAM storage allows you to place policy storage containers anywhere in the organization, allowing enhanced flexibility and availability for firewall policy redundancy and facilitated access.
Policy-based access control	You can control inbound and outbound access according to user, group, application, source, destination, content, and schedule. ISA Server firewall policy wizards specify which sites and content are accessible, whether a particular protocol is accessible for both inbound and outbound communication, and whether communication between specified IP addresses, using specified protocols and ports, should be allowed or denied.
Simplified management	ISA Server 2004 enables you to copy your entire firewall configuration to an .xml file. This .xml file can be copied to removable media or sent through secure e-mail to other firewall administrators. You can easily create a standardized firewall configuration throughout your organization or deploy it using these configuration files. You can also copy selected elements, such as VPN configuration or firewall policy rules, to an .xml file and import them.
Active Directory integration	ISA Server can leverage the user database stored in Active Directory to authenticate both inbound and outbound access through the firewall. Active Directory integration is available even when the ISA Server computer is not a member of an Active Directory

Intuitive Firewall Management	
Feature	Description
	domain.
Graphical taskpads and configuration wizards	Graphical taskpads and configuration wizards help you simplify configuration of common firewall tasks. For example, wizards can publish Exchange Server-based servers on the network behind the ISA Server 2004 computer, configure the computer to be a remote access VPN server or gateway, or create a new firewall rule.
Remote management	You can manage ISA Server 2004 remotely through a Microsoft Management Console (MMC), Windows Server 2003 Remote Desktop, Windows 2000 Terminal Services, and command-line scripts.
Centralized monitoring	You can monitor servers in all arrays from a single location with the ISA Server centralized monitoring feature. Any firewall administrator with the proper credentials can monitor all servers in any array from a centralized management console environment.
Logging, reporting, and alerting	ISA Server 2004 provides detailed security and access logs in standard data formats, such as delimited text files, Microsoft SQL Server databases, or SQL Server 2000 Desktop Engine (MSDE) databases. You can run scheduled built-in reports on Web usage, application usage, network traffic patterns, and security, and you can automatically publish these reports to a local folder or a remote file share. Event-driven alerts can trigger e-mail messages to administrators, start and stop firewall services, and take automated action based on alert criteria.
User-level management	For ISA Server 2004 Web proxy and firewall clients, you can restrict access through the firewall based not only on IP addresses but also on user names. This group-based and user-based access control provides

Intuitive Firewall Management	
Feature	Description
	you with granular control over inbound and outbound access for all protocols.
Extensible Platform	
Feature	Description
Broad application support	ISA Server 2004 supports many Internet protocols, including HTTP/SSL, FTP, RDP, Telnet, RealAudio, RealVideo, IRC, H.323, Windows Media streaming, e-mail and news, in addition to over a hundred more Internet and intranet protocols.
Broad vendor support	Independent vendors offer products that build on and integrate with ISA Server 2004, including virus detection software, management tools, and content filtering and reporting software. For example, you can use third-party filters to prevent the latest viruses, Java scripts, or ActiveX controls from being downloaded on to your secured networks.
Extensive SDK	ISA Server 2004 includes a comprehensive SDK for developing tools that build on the ISA Server firewall, caching, and management features. The SDK provides full application programming interfaces (API) documentation and step-by-step samples for building additional Web filters, application filters, MMC snap-ins, reporting tools, scriptable commands, alert management, and more.