
Secure enterprise networks with directory-enabled firewall

Directory-enabled firewalls provides secure, fast, and manageable Internet connectivity. These firewalls integrates an extensible, multilayer enterprise firewall and a scalable high-performance Web cache. Drill into the features below for more information about how directory-enabled firewalls provides secure Internet connectivity, fast Web access, and unified management.

Security policies vary from organization to organization. Traffic volume and content formats also pose unique concerns. A firewall enhances security using various methods, including packet filtering, circuit-level filtering, and application filtering. Advanced enterprise firewalls, such as Internet Security and Acceleration (ISA) Server 2000, combine several methods to provide protection at multiple network layers.

Packet Filtering

Packet filtering allows you to control the flow of Internet Protocol (IP) packets to and from ISA Server. When packet filtering is enabled, all packets on the external interface are dropped unless they are explicitly allowed, either statically by IP packet filters, or dynamically by access policy or publishing rules. With IP packet filtering, your system intercepts and evaluates packets, before they are passed to higher levels in the firewall engine, or to an application filter.

If you configure IP packet filters to have only specified packet filters pass through the ISA Server, you create a high level of security for your network. IP packet filtering also allows you to block packets originating from specific Internet hosts, and reject packets associated with many common attacks. With IP packet filtering, you also have the ability to block packets destined to any service on your internal network, including the Web Proxy, Web server, or a Simple Mail Transfer Protocol (SMTP) server.

IP packet filters filter packets based on service type, port number, source computer name, and destination computer name. IP packets filters are static-communication through a specific port, and are always either allowed or blocked. Allow filters allow the traffic through, unconditionally, at the specified port. Block filters always prevent the packets from passing through the ISA Server computer.

Dynamic Packet Filtering

ISA Server supports dynamic packet filtering. At the packet level, Internet Security and Application (ISA) Server inspects the source and destination of the traffic indicated in the Internet Protocol (IP) header, and the port in the Terminal Control Protocol (TCP) or User Datagram Protocol (UDP) header identifying the network service or application used.

Dynamic packet filters enable opening a port only in response to a user's request and only for the duration required to satisfy that request, reducing the vulnerability associated with open ports. ISA Server lets you dynamically determine which packets can be passed through to the internal network's circuit and application layer services. Configure access policy rules that open ports automatically only as allowed, and then close the ports when the communication ends. This process is known as dynamic IP packet filtering.

With dynamic packet filtering, ports open automatically only as required for communications, and ports close when the communication ends. This approach minimizes the number of exposed ports, in either direction, and provides a high level of hassle-free security for your network. ISA Server supports inbound and outbound IP packet filtering. You can also block fragments, and detect packet-level attacks against the firewall.

This approach minimizes the number of exposed ports in either direction and provides a high level of problem-free security for your network. For many application protocols, such as media streaming, dynamic IP packet filtering provides the most secure method to handle dynamically allocated ports. At the application level, smart application filters allow you to analyze a data stream for a particular application and to provide application-specific processing that includes inspecting, screening or blocking, redirecting, or even modifying the data as it passes through the firewall.

Internet Security and Acceleration (ISA) Server application filters go beyond the packet filtering of most firewalls.

While packet filtering examines the source, destination, and type of traffic, application filters provide a more sophisticated level of security by inspecting the actual contents of traffic passing through the firewall. An application filter allows you to analyze, block, redirect, or even modify the actual data stream, by knowing the specifics of the application protocol and data structures. This capability allows application filters to perform application-specific tasks such as transparent access to secondary

connections, security enhancements such as blocking potentially harmful commands, or content tasks like virus detection.

Circuit-Level Filtering

At the circuit level, the ISA Server Firewall service works with virtually all Internet applications and protocols, such as Telnet, mail, news, Microsoft Windows Media™, RealAudio, Internet Relay Chat (IRC), and other client applications. The Firewall service makes these applications perform as if they were directly connected to the Internet. Circuit level filtering is offered for both firewall and secure address network translation (SecureNAT) clients.

Winsock application programming interface (API) calls communicate with an application running on an Internet-based host. The Firewall service redirects the necessary functions to ISA Server, thus establishing a communication path from the internal application to the Internet application. This eliminates the need for a specific gateway for each protocol, such as Network News Transfer Protocol (NNTP), SMTP, Telnet, or File Transfer Protocol (FTP). Even if you have applications without built-in support for a proxy, or no knowledge of the firewall, firewall service still provides its benefits.

Circuit-level filtering enables support for virtually all standard and custom Internet applications on the Microsoft Windows® platform. These applications communicate on the network, using Winsock, and can be supported unmodified on client machines—client machines that have the Firewall Client software installed.

Circuit-level filtering lets you inspect sessions, as opposed to connections or packets. A session can include multiple connections, providing a number of important benefits for Windows-based clients running the Firewall Client software. First, like dynamic packet filtering, sessions are established only in response to a user request, improving your security. Second, circuit-level filtering provides built-in support for protocols with secondary connections, such as FTP and streaming media. Also available is the ability to define the protocol's primary and secondary connection in the user interface, without any programming or third-party tools, by specifying the port number or range, protocol type, TCP or UDP, and inbound or outbound direction.

For clients without Firewall Client software, circuit-level filtering happens with a Windows Sockets (SOCKS) filter. The SOCKS filter forwards requests from SOCKS 4.3 applications to the ISA Firewall service. The access policy rules determine if the SOCKS client application communicates with the Internet. Unlike Winsock, SOCKS can support any client platform including Unix, Macintosh, and non-computer devices. However, SOCKS also requires that client applications be specifically modified to support the SOCKS protocol.

Application Filters

The most sophisticated level of firewall traffic inspection is the application-level security. Good application filters allow you to analyze a data stream for a particular application and provide application-specific processing including inspecting, screening or blocking, redirecting, or modifying the data as it passes through the firewall. This mechanism is used to protect against things like unsafe SMTP commands or attacks against internal Domain Name Servers (DNS). Third-party tools for content screening, including virus detection, lexical analysis, and site categorization, apply application and Web filters to build into your firewall.

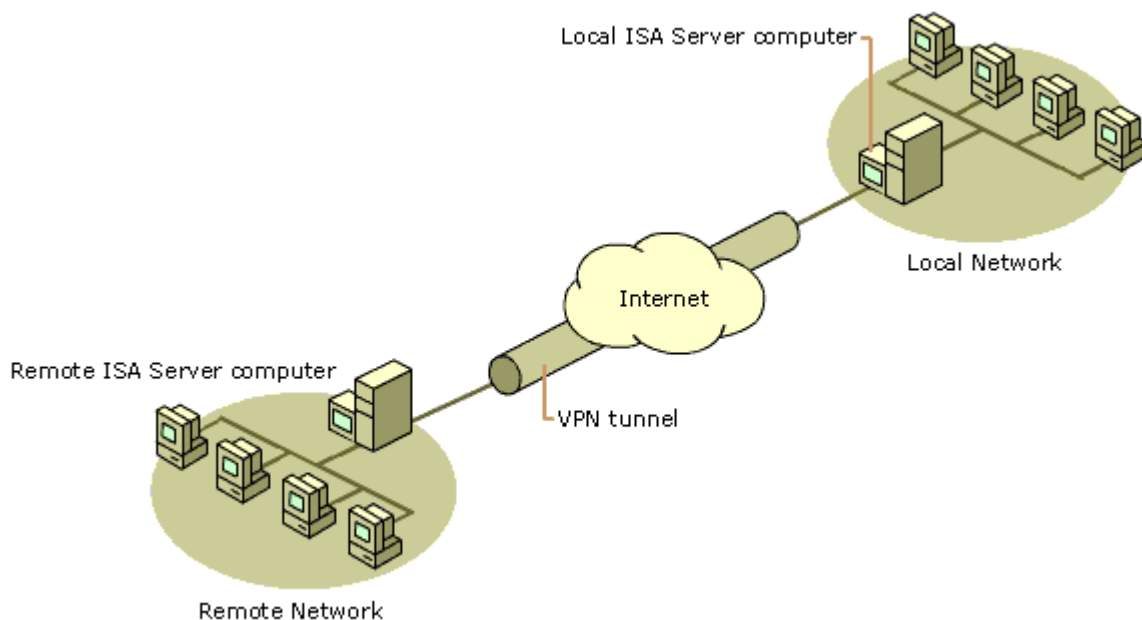
ISA Server includes the following built-in application filters:

- ?? HTTP Filter. The Hypertext Transfer Protocol (HTTP) filter forwards HTTP requests from the firewall to the Web Proxy service. This creates transparent caching for clients that do not have their browser configured to direct to the Web Proxy.
- ?? FTP Filter. The File Transfer Protocol (FTP) filter intercepts and checks FTP data. A kernel-mode data pump gives you high-performance data transfer for approved traffic. The filter also allows optional filtering-out, write requests, providing read-only, FTP access.
- ?? SMTP Filter. The Simple Mail Transfer Protocol (SMTP) filter intercepts and checks your SMTP e-mail traffic, protecting mail servers from attack. The filter recognizes unsafe commands and can screen e-mail messages for content or size, rejecting unapproved e-mail before it ever reaches the mail server.
- ?? SOCKS Filter. The SOCKS filter supports the SOCKS 4.3a standard, transparently routing client traffic from applications, with SOCKS, through the Firewall Service.
- ?? RPC Filter. The RPC filter allows sophisticated filtering of Remote Procedure Call (RPC) requests based on specific interfaces. You select RPC interfaces to expose.

- ?? H.323 Filter. The H.323 filter directs H.323 packets used for multimedia communications and teleconferencing. It provides call control, including the ability to handle incoming calls and to connect to a specific H.323 gatekeeper.
- ?? Streaming Media Filter. The streaming media filter supports industry-standard media protocols, including Microsoft Windows Media™ Technologies, RealAudio/RealVideo PNM, and RTSP—used by RealNetworks and Apple QuickTime. It also offers the ability to split live Windows Media streams, saving bandwidth.
- ?? POP and DNS Intrusion Detection Filters. Two filters recognize and block attacks against internal servers, including Domain Name System (DNS) Host Name Overflow, DNS Zone Transfer, and Post Office Protocol (POP) Buffer Overflow.

Integrated Virtual Private Networking

Internet Security and Acceleration (ISA) Server helps you set up and secure a virtual private network (VPN). A VPN is an extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public intranet in a manner that emulates the properties of a point-to-point private link. ISA Server can be configured as a VPN server to support secure, gateway-to-gateway communication or client-to-gateway remote access communication over the Internet.



The local VPN wizard runs on ISA Server on the local network. The local ISA VPN computer connects to its Internet Service Provider (ISP). The remote VPN wizard runs on the ISA Server on the remote network. The remote ISA Server VPN computer connects to its ISP. When a computer on the local network communicates with a computer on the remote network, data is encapsulated and sent through the VPN tunnel. Microsoft Windows® 2000 standards-based VPN supports PPTP and L2TP/IPSec tunneling technology. A tunneling protocol, such as PPTP or L2TP, is used to manage tunnels and encapsulate private data. Data that is tunneled must also be encrypted to be a VPN connection.

Integrated Intrusion Detection

Internet Security and Acceleration (ISA) Server features an integrated intrusion detection mechanism. This identifies when an attack is attempted against your network. The firewall administrator can set alerts to trigger when an intrusion is detected. You can also specify, with alerts, what action the system should take when the attack is recognized. You can read more about alerts on the Extensible Alerts page. This may include sending an e-mail message or a page to the administrator, stopping the

Firewall service, writing to the system event log, or running any program or script. ISA Server implements intrusion detection at both the packet filter and the application filter level.

Packet Filter Intrusions

At the packet filter level, ISA Server detects the following attacks:

- ?? All Ports Scan Attack. This happens when an attempt was made to access more than the pre-configured number of ports. The administrator specifies a threshold, indicating the number of ports that can be accessed.
- ?? Enumerated Port Scan Attack. An attempt was made to count the services running on a computer by probing each port for a response.
- ?? IP Half Scan Attack. Repeated attempts were made to connect to a destination computer, and no corresponding connection was established. This is an indication that an attacker is probing for open ports, while evading logging by the system.
- ?? Land Attack. A land attack involves a Transmission Control Protocol (TCP) connection that was requested by a spoofed source Internet Protocol (IP) address, and port number, that matches the destination IP address and port. If the attack is successfully mounted, it can cause some TCP implementation to go into a loop that crashes the computer.
- ?? Ping of Death Attack. A large amount of information was appended to an Internet Control Message Protocol (ICMP) echo request/ping, packet. If the attack is successfully mounted, a kernel buffer overflows when the computer attempts to respond, and crashes the computer.
- ?? UDP Bomb Attack. This is an attempt to send an illegal User Datagram Protocol (UDP) packet. A UDP packet that is constructed with illegal values in certain fields causes some older operating systems to crash when the packet is received.
- ?? Windows Out of Band Attack. This means an out-of-band, denial-of-service attack is attempted against a computer protected by ISA Server. If mounted successfully, this attack causes the computer to crash or causes a loss of network connectivity on vulnerable computers.

POP and DNS Application Filters

ISA Server also includes Post Office Protocol (POP) and Domain Name System (DNS) application filters that analyze all incoming traffic for specific intrusions against the corresponding servers. To read more about application filters, see the Multi-Layer Firewall page. The DNS intrusion detection filter helps you to intercept and analyze DNS traffic destined for the internal network. The POP intrusion detection filter intercepts and analyzes POP traffic destined for the internal network. The administrator can configure the filters to check for the following intrusion attempts:

- ?? DNS Hostname Overflow. A DNS hostname overflow occurs when a DNS response for a host name exceeds a certain fixed length. Applications that do not check the length of the host names may return overflow internal buffers when copying this host name, allowing a remote attacker to execute arbitrary commands on a targeted computer.
- ?? DNS Length Overflow. DNS responses for IP addresses contain a length field, which should be four bytes. By formatting a DNS response with a larger value, some applications executing DNS lookups will overflow internal buffers, allowing a remote attacker to execute arbitrary commands on a targeted computer.
- ?? DNS Zone Transfer from Privileged Ports (1-1024). A DNS zone transfer, from privileged ports (1-1024), occurs when a client system uses a DNS client application to transfer zones from an internal DNS server. The source port number is a privileged port number (between 1 and 1024), indicating a client process.
- ?? DNS Zone Transfer from High Ports (above 1024). A DNS zone transfer from high ports (above 1024) occurs when a client system uses a DNS client application to transfer zones from an internal DNS server. The source port number is a privileged port number (between 1 and 1024), indicating a client process.
- ?? POP Buffer Overflow. A POP buffer overflow attack occurs when a remote attacker attempts to gain root access of a POP server by overflowing an internal buffer on the server.

Note: ISA Server intrusion detection is based on technology licensed from Internet Security Systems (ISS) <http://www.iss.net/>

Advanced Authentication

In Internet Security and Acceleration (ISA) Server, access policy and publishing rules can be configured to allow or deny a set of computers (client address sets) or a group of users from accessing

specific servers. If the rule applies specifically to users, then ISA Server checks the Web request properties for listeners on the array to determine how the user should be authenticated. You can configure incoming and outgoing Web request settings so that users must always be authenticated before processing rules. This ensures that requests are allowed only if the user making the request is authenticated. You can also configure which authentication method to use, using different authentication methods for incoming Web requests and outgoing Web requests.

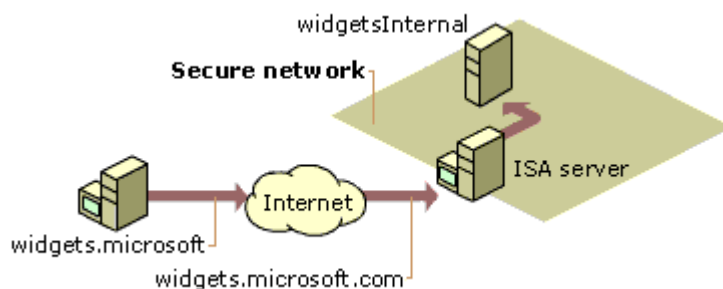
ISA Server supports the following authentication methods for the Web Proxy Service:

- ?? Basic, plain text, authentication.
- ?? Digest authentication, in a Microsoft Windows® 2000 domain.
- ?? Integrated Windows Authentication, NTLM, and Kerberos V5 protocol.
- ?? Configuring Client certificate and server certificate.

ISA Server supports NTLM pass-through authentication—the ability to pass a client's authentication information to the destination server—for both outgoing and incoming Web requests.

Secure Publishing

Internet Security and Acceleration (ISA) Server allows you to publish services to the Internet—without compromising the security of your internal network. You can configure Web publishing and server publishing rules that determine which requests should be sent to a server on your local network, providing an increased layer of security for your internal servers. For example, when Microsoft Exchange Server is used with ISA Server, create server-publishing rules that allow the e-mail server to be published to the Internet. The ISA Server computer intercepts incoming e-mail to the Exchange server. This gives the appearance of an e-mail server to clients. With ISA Server, you filter the traffic, and forward it on to the Exchange server. Your Exchange server is never exposed directly to external users and sits in its secure environment, maintaining access to other internal network services.



This figure illustrates how you can use ISA Server in a similar way to publish securely to Web servers. When a client on the Internet requests an object from a Web server, the request is actually sent to an Internet Protocol (IP) address on the ISA Server. Web publishing rules configured on the ISA Server forward the request as applicable to the internal Web server.

eMail content screening

Prevent unauthorized access to mail servers and stop unacceptable e-mail at the gateway.

Policy-based Access Control

At your fingertips with Internet Security and Acceleration (ISA) Server, is the ability to define and enforce Internet usage policy for an organization. Many companies have usage policy statements, outlined in an employee handbook or a guidelines document, defining what uses, and users, are allowed, restricted, or prohibited. ISA Server ensures that employees and external users comply with these policies by inspecting all incoming and outgoing requests and applying access rules. ISA Server rules use predefined, customizable, extensible, and reusable policy elements, including the following:

- ?? Client address sets: Internet Protocol (IP) addresses or, with Microsoft Active Directory™, authenticated users and groups.
- ?? Destination sets: URLs.
- ?? Protocols.
- ?? Content groups, for Hypertext Transfer Protocol (HTTP) and tunneled File Transfer Protocol (FTP) traffic: multipurpose Internet mail extensions (MIME) types, and file extensions.
- ?? Schedules.
- ?? Bandwidth priorities.

Once these elements have been defined, you utilize them to create an access policy—one that consists of protocol, site, and content rules. Protocol rules define which protocols can be used for communication, between the local network and the Internet. For example, a protocol rule might allow clients to use the HTTP protocol. Site and content rules define what content on which clients behind the ISA Server computer can access Internet sites. For example, a site and content rule might allow clients to access any destination on the Internet. Both protocol rules, and site and content rules, are processed at the application level.

Access rules are not ordered. However, rules that deny access are processed before rules that allow it. Access rules apply to content stored in the ISA Server cache and to content crossing the firewall. This unified access control ensures you apply the corporate usage policy consistently. This includes content that has been cached inside the network. User authorization is required to access any content, regardless of its location on the network. Wizards provide step-by-step assistance for creating new policy elements and rules, simplifying the task and ensuring that all the required information is included. Access policy rules apply to all types of clients: firewall, secure network address translation (SecureNAT) clients, and Web Proxy.

In addition to Internet access policy, you can configure a publishing policy for incoming requests. This consists of server and Web publishing rules. Server publishing rules filter all incoming requests and map incoming requests to the appropriate servers behind the ISA Server computer. Web publishing rules map incoming requests to the appropriate Web servers behind the ISA Server computer.

With ISA Server, you have support for two levels of policy: array-level and enterprise-level. Array-level access policy, or local policy, is used for stand-alone servers and arrays. As an enterprise administrator, you define enterprise-level policy elements and enterprise-level rules. You select a centralized enterprise policy that applies to all arrays in the enterprise, or a more flexible policy where each array administrator defines a local policy. The enterprise policy can be applied to any array, and can be augmented by the array policy.

Tiered Policy

Internet Security and Acceleration (ISA) Server can be installed as a stand-alone server, or as an array member. Array members share the same configuration. Management and administration are then easier. When you modify the array configuration, all the ISA Server computers in the array are also modified, including all the access policies and cache policies.

The centralized administration also means greater security. Perform all administrative tasks from one computer, and the configuration is applied to all—ensuring that servers have the same access policies configured. This is particularly useful in large organizations, where arrays include many ISA Server computers.

Array Policy

You can create site and content rules, protocol rules, Internet Protocol (IP) packet filters, Web publishing rules, and server publishing rules at the array level. Together, these rules compose an array policy. The array policy determines how your clients communicate with the Internet, and what communication is permitted. As the name implies, the array policy applies only to the ISA Server computers in the array.

Enterprise Policy

The enterprise takes your centralized management one step further, allowing you to implement one or more enterprise policies. These include site, content, and protocol rules. You can apply an enterprise policy to any array, while also augmenting it by the array policy. This enforces enterprise policies at branch and departmental levels, while allowing local administrators to further restrict access.

You can determine how array administrators use the enterprise policy. You might decide on a very restrictive policy. In this case, no array policies are configurable. You might also decide on a very

liberal policy, allowing the array administrators to define any rules. In this case, no enterprise policy is applied to the array. A mixed approach might be to allow array policies while still applying an enterprise policy. In this scenario, the array administrator defines array policy rules. Enterprise policy rules are then restricted.

At the enterprise level, you can configure all the arrays in the enterprise to use the enterprise policy. You also have the capability to allow some arrays to restrict access policy. At the enterprise level, you can also decide which arrays are allowed to publish servers. By allowing both enterprise and array policies, you ensure that a corporate policy is implemented throughout the organization. At the same time, you are able to allow nuances at the department or branch level, creating additional rules as necessary. For example, an enterprise policy might only allow access to Hypertext Transfer Protocol (HTTP) addresses and deny communication using all other protocol definitions. An array that uses this enterprise policy allows you to add a rule that limits who can use the HTTP protocol. The array policy cannot overwrite the enterprise policy and allow communication using other protocols.

Built-in reporting

Create graphical summary reports showing application usage, security events, and network activity.

Monitoring and alerting

Track real-time session and performance monitoring data. Define alerts to notify an administrator, stop a service, or execute a script in response to important system events.

Bandwidth priorities

Set bandwidth priorities to optimize resource allocation, prioritizing bandwidth by user, group, application, destination site, or content type.

Conclusion

Scaling Up and Scaling Out for the Enterprise

Directory-enabled firewalls are built for the enterprise. The tiered policies provide a scalable management model. This model makes it simple to extend the number of managed clients and servers. Performance also scales to meet the growing needs of large organizations with technologies such as symmetric multiprocessing (SMP), network load balancing (NLB), and Caching Array Routing Protocol (CARP).

- ?? **Tiered Policy Management.** Directory-enabled firewalls provides tiered policies that allow servers to have local array policies while inheriting enterprise-wide policies. Administrators can also delegate various levels of firewall administration in distributed deployments.
- ?? **Scale Up Performance.** Directory-enabled firewalls were designed to scale up with multiple processors by optimizing for OS SMP. Unlike many other products, these firewalls utilizes the extra processing power to boost performance.
- ?? **Scale Out Performance.** Directory-enabled firewalls uses the NLB Services and CARP to provide fault-tolerance, high availability, efficiency, and performance through clustering of multiple firewall machines.

Lower Cost of Ownership

Secure networks with directory-enabled firewalls lowers cost of ownership for firewall and Web caching by providing integrated services, familiar management tools, and an open platform for product extensions. Customers benefit from integrated robust features and an extensible investment.

- ?? **Integrated Services.** Unlike other vendors that require separate purchases, directory-enabled firewalls integrates services such as firewall, Web cache, basic intrusion detection, reporting, VPN, and bandwidth management into a single solution.

- ?? **Works with What You Have.** Directory-enabled firewalls can operate in a mixed environment. They provide transparent services to clients and servers, allowing administrators to work with their existing computing platforms.
- ?? **Extensible Open Platform.** With an extensive software development kit (SDK) and application programming interfaces (APIs), Windows based directory-enabled firewalls have industry-wide, third-party, vendor support to provide value-added security, management, and caching applications. They provide an open platform that ensures customers get scalable security, performance, and management.

*Thomas K.H. Bittner
Senior Consultant, Online GmbH
Microsoft Servers and Windows 2000 MVP
Microsoft Windows 2000 Certified Professional*