Learn about the ISA Firewall Client (Part 1)

Client firewall software (Firewall client) is a software installed on Windows operating systems to provide enhanced security and access.

Client firewall software (Firewall client) is a software installed on Windows operating systems to provide enhanced security and access. This software provides the following advanced features for Windows clients :

• Allows authentication based on user groups or a single user for all Winsock applications using TCP and UDP protocols

• Allow users and application information to be recorded in the log file of the ISA firewall

• Provides advanced support for network applications including complex protocols that require secondary connectivity

• Provide 'proxy' DNS support for computer firewalls

• Allows you to present servers that require complex protocols without the need of application filters

• Network routing infrastructure is transparent to the client firewall

• Allows user-based or user-based authentication for Winsock applications using TCP and UDP protocols.

Firewall client software sends user information transparently to the ISA firewall. This allows you to create access rules to apply to individual groups or users, restrict or allow access to protocols, pages, or content based on user accounts or group membership. Access control comes out of individual groups or users. Not all users require the same access levels and users should only be allowed to access the protocol, page and content they require to perform their work.

Note

The concept allows users to access only the protocols, pages and content they require based on the principle of least privilege. The minimum privilege principle applies to both access and output. With the access scenario, Server and Web Publishing principles allow traffic from machines to expand to Internet resources in a highly controlled and controlled manner. Such things are also true for access out. In traditional network environments, access is often limited while users are allowed to access any resource they desire. This weak access control method not only poses a risk to the collaborative network but also for other networks because the Internet worm can penetrate the firewall without restricting access.

The Firewall client automatically sends user credentials (name and password) to the ISA firewall. Users must be logged in with the user account in either the Windows Active Directory domain or NT, or the user account must be reflected to the ISA firewall. For example, if you have an Active Directory domain, the user must log on to the domain, the ISA firewall must be a member of the domain. The ISA firewall can authenticate users and allow or restrict access based on user domain credentials.

Without a Windows domain, you can still use the Firewall client software to control access based on a single group or user. In this case, you must reflect the accounts that users log into their workstations with user accounts stored in the internal Security Account Manager (SAM) or on the ISA firewall.

For example, a small business does not use Active Directory, but they want to control good access based on group members and users. Users log on to their computers with an internal user account. You can enter the same username and password in the ISA firewall. The ISA firewall will be able to authenticate users based on the same account information used when users log on to local computers.

Windows 9x clients can be configured according to domain credentials if they have installed Active Directory software.

Allow user and application information to be recorded in the log files of ISA 2004 Firewall

The big advantage in using Firewall Client is that when the username is sent to the ISA Firewall, that name is contained in the ISA Firewall log files. This allows you to easily query log files to obtain user names and get accurate information about the user's Internet activities.

In this context, the Firewall client not only provides a high level of security by allowing you to control access based on user accounts and group accounts, but also provides a high level of accountability. Users will be less likely to share their account information with other users when they know that their Internet activity is being monitored based on their account name and they are responsible for that action.

Provides enhanced support for network applications including complex protocols that require secondary connectivity

Unlike the SecureNAT client that requires an application filter to support complex protocols that require secondary connectivity, Firewall client can support virtual Winsock applications using TCP and UDP protocols without concern. Consider the main or secondary connection number, no application filters are required.

The ISA Firewall allows you to easily configure Protocol Definition that reflects primary or secondary connections, and then create access rules based on this protocol definition. This provides a significant advantage in terms of the total cost of the investor (TCO), you do not need to spend a lot of time and money in creating custom application filters to support the application. use 'off-label' Internet.

Provides 'Proxy' DNS support for Firewall Client

In contrast to the SecureNAT client, the Firewall client does not need to configure the DNS server related to Internet host name. The ISA Firewall can perform the 'proxy' DNS function for Firewall clients.

For example, when a Firewall client sends a connection request to ftp://ftp.microsoft.com, the request is sent directly to the ISA Firewall. The ISA firewall processes the name of the Firewall client based on DNS settings

on the ISA firewall's network interface card. The ISA firewall returns the IP address to the Firewall client machine, and the Firewall client computer sends an FTP request to the IP address for the ftp.microsoft.com FTP site.

The ISA firewall also stores the DNS query results it performs for the Firewall client. Unlike ISA Server 2000, storing information in a default cycle of 6 hours, the ISA firewall stores the entire period specified by the TTL on the DNS record. This has increased the number of names for Firewall client connections to the following for the same site. Figure 1 shows the name string for the Firewall client.

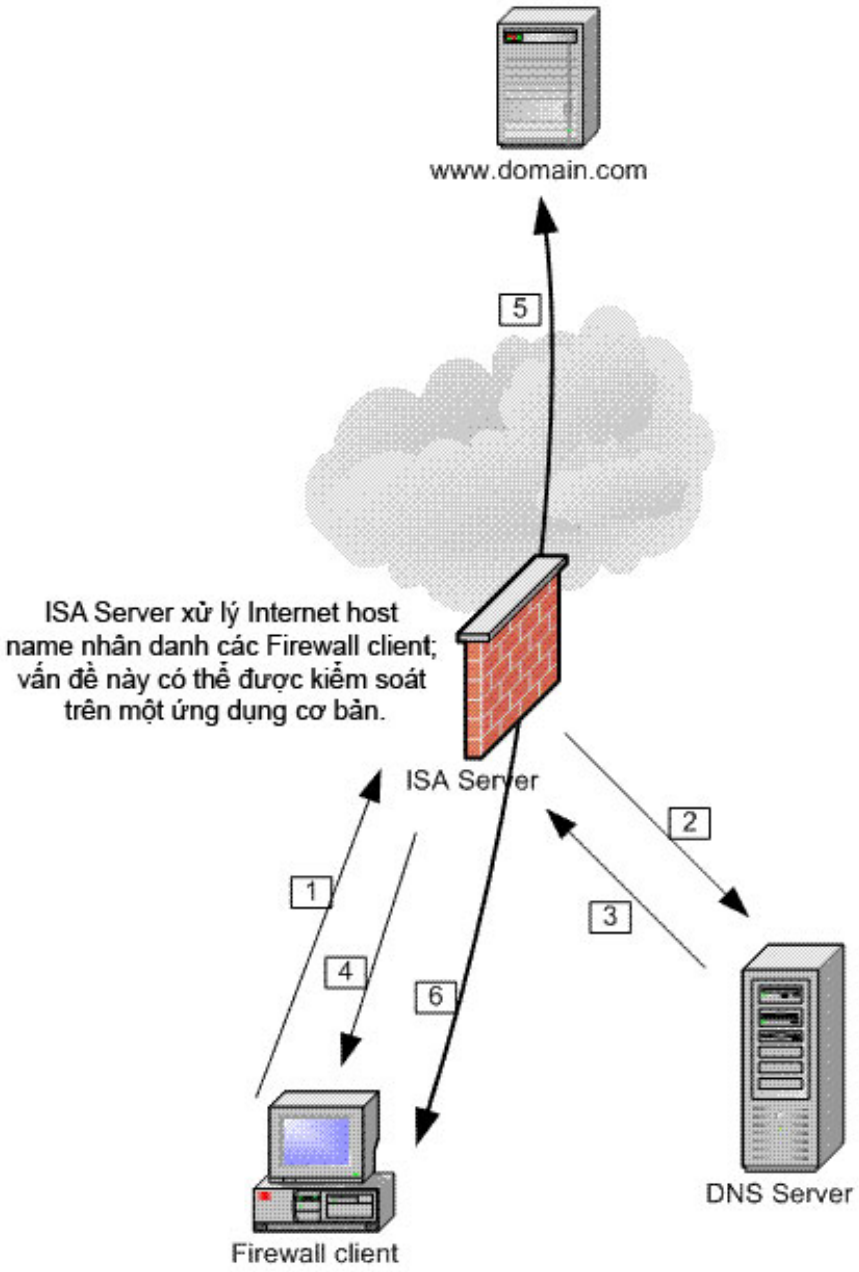

Figure 1 : String name Firewall

1. Firewall client sends a request to ftp.microsoft.com.

2. The ISA firewall sends a DNS query to the internal DNS server.

3. The DNS server processes ftp.microsoft.com with its IP address and returns the results to the ISA firewall.

4. The ISA firewall returns the IP address of ftp.microsoft.com for the Firewall client to create the request.

5. The Firewall client sends a request to the IP address ftp.microsoft.com and the connection is completed

6. The Internet server returns the required information to the Firewall client via the Firewall client connection that is made with the ISA firewall.

Transparent network routing infrastructure for Firewall Client

The final advantage of the Firewall client is its transparent virtual routing infrastructure for the Firewall client. In contrast to the SecureNAT client, depending on its default gateway and router settings on the router through the collaborative network, the Firewall client computer only needs to know the IP address routing on the internal interface of the ISA 2004 firewall. . Firewall client machine 'remotely' or requests sent directly to the ISA firewall's IP address. Used routers are used to implement all the routes in the collaborative network, so there is no need to make changes to the routing infrastructure to support Firewall client connections to the Internet. Figure 2 shows the 'remote' nature of the connections directly to the ISA firewall. Table 1 provides a summary of the advantages of the Firewall client application.

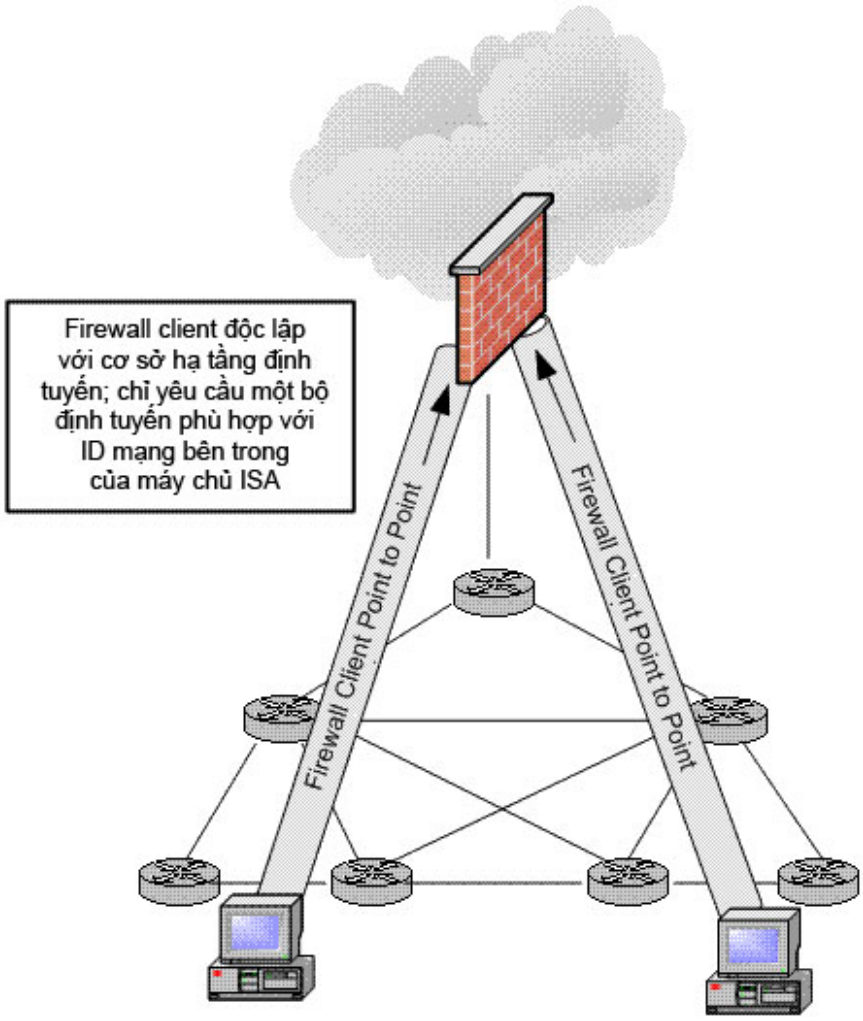

Figure 2: Firewall client connections to the ISA 2004 Firewall are completely independent with default port configurations on routers.

Advantages of Firewall client Meaning Good authentication based on users or groups for good Winsock TCP and UDP protocolsbased on user or group for applications using TCP and UDP allows you to control Strictly access goes out and can implement the minimum privilege principle to protect not only your network and also protect the network of other companies.User name and application information stored in the ISA 2004 firewall record.Strong user and group access controls increase the security of the firewall for your network, the user name and application name information. saved in the logs of the ISA 2004 firewall increases accountability and allows you to easily study which pages, protocols and applications users are accessing the Firewall client software to be accessed.Advanced support for network applications and protocolsFirewall clients have virtual access to any TCP and UDP-based protocols, even those using complex protocols require multiple primary connections and secondary.In contrast, the SecureNAT client requires an application filter on the ISA 2004 firewall to support complex protocols.Overall the Firewall client reduces TCO compared to ISA 2004 firewall solutionProxy support DNS for Firewall clientISA 2004 firewall can handle names on behalf of Firewall clients.This eliminated the responsibility of handling Internet host names for the Firewall client computer and allowed the ISA 2004 firewall to keep DNS storage for recent name processing requests.This DNS proxy feature also enhances the security configuration for the Firewall client because it eliminates the requirement that the Firewall client is configured to use a public DNS server to handle Internet host names.Allows publishing servers

that require complex network protocolsWeb and Server Publishing principles support a simple protocol, in addition to an application installed on the ISA 2004 firewall as an FTP Access application filter.You can install Firewall client software on a public server to support complex protocols that may be required if you want to run a game server on the network.In the future Microsoft also officially supports this configuration and they remind you that you need to have a C ++ program to support your application.Network routing infrastructure is completely transparent to firewall clientsUnlike the SecureNAT client, which relies on the organization's routing infrastructure to use the ISA 2004 firewall as an Internet access firewall, the Firewall client only needs to know Routing for the IP address on the internal interface of the ISA 2004 firewall.This reduces the requirement management requirements to support Firewall client versus SecureNAT client.

Table 1 : Advantages of Firewall client configuration

How the Firewall Client works

Details of how the Firewall client works are not fully documented in Microsoft documents. In fact, if you track the Firewall client media using Microsoft Network Monitor, you can see that Network Monitoring is unable to decode the Firewall client communication; however, Ethereal has a primitive Firewall client filter that you can use.

What we know is that the ISA 2004/6 Firewall client, unlike previous versions, only uses TCP 1745 for the Firewall client *Control Channel* . On this control channel, the Firewall client communicates directly with the ISA firewall service to perform specific application control names and commands (such as those used by FTP and Telnet). The firewall service uses information amplified through the control channel and establishes a connection between the Firewall client and the destination server on the Internet. The ISA firewall proxies the connection between the Firewall client and the destination server.

Note

The Firewall client only establishes a control channel connection when connecting to a resource that is not located on the internal network. In ISA Server 2000, the internal network is defined by Local Address Table (LAT). The ISA 2004/6 firewall does not use LAT because of its advanced multi-network connectivity capabilities. However, the Firewall client must have some alternative mechanism to determine which communications will be sent to the firewall service on the ISA firewall and which communications are sent directly to the destination that the Firewall client wants.

The firewall client solves the problem by using the addresses defined by the **ISA Firewall Network** on the existing client. The ISA Firewall Network for specific Firewall clients has all possible addresses from the network interface connected to the Firewall client's own ISA Firewall Network. This situation makes an interesting part of the ISA firewall, many families have multiple ISA Firewall Networks associated with other network adapters. In general, all hosts placed inside the same network adapter (regardless of network ID) are considered as part of the same ISA Firewall Network and all communications between hosts on the ISA Firewall Network must be via Firewall client.

Addresses for the ISA Firewall Network are defined during the installation of the ISA firewall software, but you can create other networks after the installation is completed. Typically, after installation, only the internal ISA Firewall Network is created for you and you need to manually create another ISA Firewall Network if there are more than 2 NICs on your ISA Firewall.

ISA FIREWALL security warning

You can have multiple interfaces on the same ISA firewall. However, only a single network can have an **Internal** name (inside). The internal network has a group of computers that have absolute reliability (at least trust enough not to require network firewalls for communication between them). You can also have multiple internal networks, but these additional internal networks can be placed in the internal address range of another internal network. Carefully review the ISA Firewall System Policy after installation is completed to limit communication between the default ISA Firewall and the Internal Network only for communications required for your script.

However, the centralized configuration of the Firewall client can be done on the ISA Firewall Network; so you can control the Firewall client settings for each basic network name. This allows you to take a measure of how the Firewall client configuration settings are managed on each network. Although this solution does not help in network scenarios in the network, where there are multiple network IDs located behind the same network interface card.

In the network scenario in the network, you can use the internal LAT locallat.txt file to override the central internal network settings if it is necessary. In general, network scripts in the network do not create significant problems for the Firewall client. The most significant improvement that ISA 2004/6 Firewall client has over previous versions (Winsock Proxy Client 2.0 and ISA Server 2000 Firewall Client) is that you have the option to use an encrypted channel between the Firewall client and ISA firewall.

Remember, the Firewall client sends transparent user credentials to the ISA firewall. The ISA Firewall client encrypts the channel to keep it secret. Note that you can optionally configure the ISA firewall to allow communications that are not secure and secure.

Note :

If Internet Protocol security (IPSec) transfer mode is enabled for a network so that the Firewall client machine uses this mode to connect to the ISA firewall, you may feel abnormal or connection problems. anticipated. If Firewall client in the network does not perform as expected, disable **IP routing** at the ISA firewall's user interface. In that interface, open the server, expand **Configuration** , click the **General** button. In the details window, click **Define IP Preferences** . On the **IP Routing** tab, verify that the **Enable IP Routing** check box is not **ticked** . Note that disabling IP Routing can significantly reduce SecureNAT clients' performance, requiring access to secondary connections.

Conclude

In this article we have introduced you to the ISA firewall's Firewall client software. The Firewall client performs as a Winsock proxy client application that the remote control network's Winsock application calls to the ISA Firewall. The ISA Firewall firewall service then delegates connections to the destination requested by the client. The Firewall client supports protocols that have multiple primary and secondary connections and do not require specific protocol definitions if an 'open all' access rule is created. Most importantly, the Firewall client can send computer name information and use it to the ISA Firewall and this information is stored in logs and reports so you can get detailed information about what users are doing. Existing with Internet connection, for most applications and protocols, things that cannot be done with a computer are configured as Web proxies or SecureNET clients. In addition, the Firewall client sends the application image name to the ISA Firewall so that you can easily decide whether the prohibited application is being used by the user.

on tips and guides. Thank you for reading and for following us regularly.