Installing, configuring and administering ISA Server 2004 Firewall

Among the current firewall products on the market, Microsoft's ISA Server 2004 is loved by many people due to its strong system protection and flexible management mechanisms. ISA Server 2004 Firewall has two Standard and Enterprise versions for different environments.

Among the current firewall products on the market, Microsoft's ISA Server 2004 is loved by many people due to its strong system protection and flexible management mechanisms.ISA Server 2004 Firewall has two Standard and Enterprise versions for different environments.

ISA Server 2004 Standard meets the need to protect and share bandwidth for medium sized companies. With this version we can build a firewall to control the flow of data in and out of the intranet system of the company, control the access process of users according to protocol, time and content to prevent blocking connections to websites with inappropriate content. In addition, we can deploy Site to Site or Remote Access VPN systems to support remote access, or data exchange between branch offices. For companies with important server systems such as Mail Server and Web Server that need to be strictly protected in a separate environment, ISA 2004 allows deploying DMZ zones (terminology for demilitarized zone) preventing direct interaction between people inside and outside the system. In addition to the information security features above, ISA 2004 also has a buffer system (cache) to help connect to the Internet faster because the website information can be stored on RAM or hard disk, significantly saving system bandwidth. system. For this reason, this firewall product is called Internet Security & Aceleration.

ISA Server 2004 Enterprise is used in large network models, meeting many of the access requirements of internal and external users. In addition to the features already available on ISA Server 2004 Standard, the Enterprise edition also allows the establishment of an array of ISA Servers using a policy, which makes it easy to manage and provide Load Balancing features (load balancing).).

This article presents how to deploy ISA Server (Standar and Enterprise) systems to a company with more than 50 employees. To provide Internet sharing services, the company uses an ADSL line and ISA Server 2004 Firewall system. With an ADSL modem address of **1.1.1.2** , the system has two main network layers, Internal including computers of employees with a range of private IP addresses of **192.168.1.1** - **192.168.1.255/24** and DMZ for servers (Like Exchange Server, Web Server) uses the **172.16.1.0/24** network address. The server used to install ISA Server running Windows Server 2003 SP1 has 3 NICs (network interfaces) with the following IP addresses:

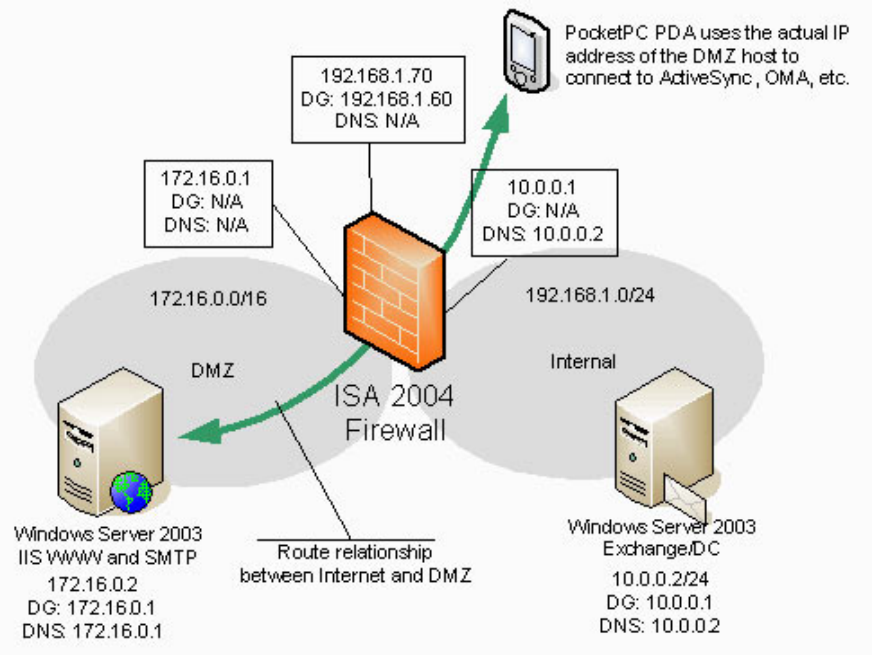
- Outside Interface: IP 1.1.1.1, Subnet Mask 255.255.255 and Default Gateway 1.1.1.2 (ADSL modem).

- Inside Interface: IP 192.168.1.10, Subnet Mask 255.255.255.0 and DNS 192.168.1.11 (DNS Server and Domain Controler of the system)

- DMZ Interface: IP 172.16.1.1, Subnet Mask 255.255.255.0

To ensure the safety of the system and firewall, on the Network interface Outside select Disable Netbios Over TCP IP, uncheck the Register this connections address in DNS and Enable LMHOST lookup as shown below:

Note : The function Disable NetBIOS over TCP / IP makes the computer become "invisible" on the network, the software scans the system error like Retina, Nmap will not find the name of the computer, limiting detection cases password of brute force accounts. Internet-based servers like firewalls often choose this function, but for computers on the internal network we should not use it because it will prevent other computers from accessing shared resources on the computer such as Printer , Folder Share. Some security applications (such as PC Security) when installed will default to Disable NetBIOS over TCP / IP.



Install ISA Server

After you have set up all the necessary information, we will install ISA Server 2004 Standard on a firewall computer. We can choose one of the following 3 installation modes:

- Typical: In this mode, only a minimal number of services are installed, no Cache service.

- Complete: all services will be installed as Firewall used for access control; Message Screener allows to prevent spam and attachments (IIS 6.0 SMTP is required before installing Message Screener); Firewall Client Installation Share.

- Custom: allows you to select which components to install from ISA Server 2004.

Here we will use the Custom installation mode, by default only two Firewall Services and ISA Server Management services, please select the Firewall Client Installation Share.

Next, the installation process will ask you to specify the network interface with the internal network (Internal Network), in the Internal Network window click Add and Select Network Adapter. Check Inside on the Select

Network Adapter page.

Next, we need to provide an array of IP addresses containing computers on the local network (From, To). Note, this address range must contain the IP of the Inside network interface.

In the Firewall Client Connection Settings window, check Allow nonencrypted Firewall client connections and Allow Firewall clients running versions of the Firewall client software to connect to ISA Server, click Next in the next steps to complete the installation process.

For the Standard version we should install SP1 ISA2004-KB891024-X86-ENU.msp (can be downloaded from www.microsoft.com or www.security365.org/downloads/software) to ensure the system works. Dynamic stability.

ISA Server Connection With Internet And Configuring The ISA Client

ISA Server 2004 Firewall has three types of security policies: system policy, access rules and publishing rules.

- System policy is usually hidden and is used for interaction between a firewall and other network services such as ICMP, RDP . System policy is processed before the access rule is applied. After installing the default system policies, ISA Server will allow you to use system services such as DHCP, RDP, Ping .

- Access Rule: is a collection of Internet access rules or email. Pay special attention to the order of access rules because the firewall's processing flow will terminate when it encounters a policy of "blocking" again. To understand this mechanism, we see an example with 5 access rules with the following order:

1. Deny HTTP (not allowed to use HTTP protocol)

2. Allow HTTP (for HTTP protocol use)

3. Allow FTP (allow FTP use)

4. Deny FTP (no FTP allowed)

5. Deny All (default policy)

In case we assume that the user object is the same, when a user uses the HTTP protocol to browse the web, he will be denied access because the first access rule does not allow the use of this protocol. . But if the user downloads the file via FTP, he will be allowed because the third access rule allows FTP, and the firewall will ignore the remaining access rules.

- Publishing Rule: used to provide services such as Web Server, Mail Server on Internal network or DMZ layer to allow users on Internet access.

When the ISA Server 2004 installation is complete, we connect ISA Server to the Internet and configure the ISA clients to access the Internet through the ISA Server Firewall. By default ISA Server has only one access rule after installing Deny All, denying all I / O access through the ISA firewall, so we need to create rules that match the organization needs or apply the Sample rules (Predefine Template) for ISA Server. You can configure the ISA Firewall Policy through the ISA Management Console interface on ISA Server itself or install the ISA Management Console management tool on another computer and connect to ISA Server to perform remote

administration tasks. The management interface of ISA Server Management console has 3 main parts:

- Left frame to browse main functions such as Server name, Monitoring, Firewall Policy, Cache .

- The middle pane shows details of the main components that we choose such as System Policy, Access Rule .

- The right pane called Tasks Pane contains special tasks such as Publishing Server, Enable VPN Server .
ISA Server Management console

1. Create Access Rule On ISA

Open the ISA Management Server management interface by selecting Start -> All Programs -> Microsoft ISA Server -> ISA Server Management. Right-click the Firewall Policy and select Create New Access Rule or select from the Task Pane of the management screen. Name the access rule to create as Permit any traffic from internal network or the name that matches your system and select Next. In the Rule Action section we select Allow, as this is an access rule that allows clients to use protocols and applications through the firewall.

Determine which protocols the user is using, such as HTTP or FTP . In the Protocols window, select All outbond trafic, if you want to change you just need to select in the list as Selected Protocol to select some protocols or in Inbound trafic for the case of providing external connections.

The system needs to know the object using the protocols in the access rule, in which case the clients are users in the intranet so we choose Add on the Access Rule Source and select Internal. For User, we select All User (in case of necessity you can define the appropriate Group or User of the system such as Group Domain User, Administrator ., when Firewall is not part of the Domain, please use local account of Firewall in Local Users And Groups).

Click Apply to enable the newly created firewall policy. Now we have 2 acess rules as the Default Rule (with the Deny All function, note that the Default Rule cannot be deleted) and Permit Any Traffic from internal network allows users to Intranet is allowed to use all protocols on the Internet.

2. ISA Client configuration:

To use ISA Server, the network clients must configure one of the following three types: SecureNAT, Firewall Client, Web Proxy Client or all three.

* ***SecureNAT Client*** :

This is the simplest method, computers only need to configure Default Gateway which is the internal network card address of ISA Server (in this case 192.168.1.10), or we can allocate it via DHCP server with option 006 for Router. The advantage of this method is that the client does not need to install anything else, and can use non-Microsoft operating systems such as Linux, Unix and still use the protocols and applications on the Internet through ISA. However, one disadvantage is that the SecureNAT clients do not send authentication information including usernames and passwords to the firewall, so if you deploy access control services according to domain users, a username and password are required. The SecureNAT client is not applicable. In addition, we cannot log the access process for this type of client.
SecureNAT client configuration

* ***Firewall Client*** :

So if we want a more stringent control mechanism, for example, how do users log in to the domain to access the Internet? The solution is that we will install the Firewall Client for these computers. Normally when installing ISA Server you will install Firewall Client Installation Share service, then on ISA Server open system policy to allow access to shared resources and client computers only need to connect to ISA Server by internal IP address with a valid account to run the Firewall Client installation file.

If you do not want to install Firewall Client Installation Share on each client computer, you can choose to install this service on any computer such as file server or domain controller as follows: select Setup Type of Custom type and select This feature, and all subfeatures, will be installed on the local hard drive in the Firewall Client Installation Share section.

Then on the client computers install Firewall Client by opening Start -> Run and running the 192.168.1.10mspclntsetup command.

In case the system has multiple workstations, it is difficult to install on each machine, the solution to deploy the program automatically by SMS Server 2003 or Assign through Group Policy is most effective (you can refer to Refer to the automatic installation method via Group Policy on the website www.security365.org). With Firewall Client, you can take advantage of the most powerful capabilities of ISA Server such as user authentication based on Domain User and Group, allowing logging of visits . However the main disadvantage of the school This is the computer that wants to install Firewall Client must use Windows operating system.

* ***Web Proxy Client*** :

As we know, besides the security function, ISA Server 2004 Firewall also has a Cache function to store websites that are normally accessed on RAM or on hard disk to save bandwidth. However, Web Proxy Client only uses HTTP / HTTPS, FTP protocols, which means users will not be able to access email with Outlook or use other applications. To use Web Proxy, the client computers must configure in the web browser by opening Internet Explorer, selecting Tools -> Internet Options, selecting Connections -> LAN Settings tab and entering the address of Proxy server.

So the fastest way to allow computers on the network to access the Internet via ISA Server is the SecureNAT client configuration based on the system that allocates dynamic IP addresses or static IP configurations and points the default gateway to the internal network address. of ISA Server. In addition to the smooth IP address resolution process, clients need to configure both internal and ISP DNS server addresses such as 210.245.31.10 or 203.162.4.191.

Set Up Private Policies

Although the system is connected to the Internet, some companies have specific system policy requirements such as not allowing chat with AOL or MSN Messenger, allowing downloading of files via FTP. In addition, for browsing purposes, the HTTP protocol is allowed to be used, but it is prohibited to download executable files on Windows systems via HTTP to prevent virus infection. To do this, you need to re-edit your firewall policy.

1. Creating access rules does not allow the use of AOL and MSN Mesenger

Right-click Firewall Policy, select Create new Access Rule and name it deny MSN and AIM, click Next. In the Rule Action window, select Deny and click Next.

In this This rule applies section select Selected Protocols. Click Add. Then open Protocols of Instant Messaging

and double-click AOL Instant Messenger and MSN Messenger. Click Close.

Next, select Internal and External in the Network section, apply to All users and Apply to apply this policy to the system.

2. Create an access rule that allows the client to use FTP to download and upload

In case you want to allow users to use FTP for downloading and uploading, proceed as follows: Create a new access rule through Create a New Access Rule, named the FTP permit with Rule Action is Allow, applicable to All User and Internal Network.

After clicking Apply, the User on the intranet system can download via FTP using FTP Client programs such as FileZilla. However, in order for them to upload FTP servers, we need to uncheck Read Only for FTP access rules by right-clicking on the Access Rule permit FTP and selecting Configure FTP.
In the Configure FTP protocol policy window, select Read Only to allow uploading to Ftp server.

3. Create an access rule that allows use of HTTP but does not allow downloading of executable files on Windows systems.

Create a new access rule named HTTP permit deny executables that allows users on the Internal network class to use the HTTP protocol.

Right-click the HTTP permit deny executables and select the HTTP configure. Check the Block responses box containing Windows executable content as shown below:

Using WPAD Support ISA Client Automatically Detects Firewall and Web Proxy

When the system uses DHCP to allocate dynamic IP address, we need to support clients to automatically detect Web Proxy Server and Firewall via CNAME WPAD record on DNS Server or configure Predefine option as wpad on DHCP server (refer to Refer to the demo file http://www.security365.org/downloads/demo/ISA2004.rar).
Note: Configuring WPAD on DHCP is only available if the DHCP Server is a Windows OS service, and when using other companies' DHCP Servers, we must use DNS to do this.

1. First we need to enable Auto Discovery support on ISA Server. Open the ISA Management Console, in the Network section, double-click the Internal Network, select the AutoDiscovery tab, and check the Publish automatic discovery information box, in the box Use this port for automatic discovery request enter 80.

2. Create a CNAME record in the DNS server named WPAD: Open the DNS Management Console window, right-click on Domain Zone and select New Alias ??(CNAME). Enter WPAD in the Alias ??name section and the full name of WPAD.SECURITY365.ORG in the box Full qualified domain name.

Click OK to finish. Please use any Firewall Client or Web Proxy Client to check again. Select Automatically detect ISA Server in the client firewall and uncheck Use proxy server, instead Automatically detec settings in the web browser to automatically detect Web Proxy.

Select Detect Now, after a short time the ISA Server name on your system will appear

So we installed and configured ISA Server to support Internet access, download and upload documents via FTP,

support automatic detection of Firewall and Web Proxy for clients with WPAD record in DNS Server. However, you notice that some clients still chat with MSN Messenger or use P2P programs to search for documents. This is because these applications can use HTTP, port 80 to communicate via the web proxy server. This can be prevented by editing the HTTP policy permit as follows:

Right-click the HTTP Access Rule permit and select Configure HTTP. In the Signature tab enter the parameters as shown below and click OK, then click Apply to apply to the system.

Saving Bandwidth With Cache Features And Content Download Job

There is a very useful feature of ISA Server, but the default is blocked by web caching for http and ftp requests. With ISA we can implement two caching mechanisms:

- Forward caching: with this mechanism, the content of frequently accessed web pages will be downloaded and stored in the cache of ISA server, so when users reopen these sites, the content will be paid for. cache instead of having to connect directly to the web server on the Internet.

- Reverse caching: in contrast to forward caching, when businesses or organizations have web servers that allow external users to access, reserver caching saves bandwidth by storing web content on proxy servers to meet , reduce the load for the web server. So on some reverse cache documents, this is also called a cache gateway.

In terms of organization, we can build cache systems on ISA according to different models depending on the number of users and the network architecture of each business.

- Distributed Caching: ISA Servers will be distributed evenly across the network, improving the responsiveness for users.

- Hierarchical caching: different from the above model, in this case ISA Server will be distributed at each level, the requests will be handled by the internal ISA Server first, so the response time is higher.

- Hybrid caching: is a combination of both models.

So, when the Web Cache function is turned on, frequently visited web pages will automatically download that can be stored on RAM or hard disk of ISA Server (cache), and users when accessing this site again. will be returned content from the cache, not downloaded from the Internet. However, some search sites should not store cached content because the search results will not be updated, so when setting up Web Caching you should set Caching Rule to not keep the pages Web like www.google.com. In addition, some websites are frequently accessed by users to read news, refer to market prices, news about security . we can schedule Web services Proxy Server to download before working hours. through Content Download Job function.

1. Enable Web Caching :

Open the ISA Management Console, select the Cache entry in the Configuration section and click Define Cache Drivers (enable caching).

Specify the NTFS partition for storing web page content (cache size), for example 20 MB, press Set to set and click OK.

After clicking Apply to apply the Web Cache function, there will be a dialog box that says Restart Firewall

Services or just save and not Restart, select Save the changes and restart the services and click OK.

2. Create a Cache Rule that does not store Web content from www.google.com :

On the Task Pane pane, choose Create a Cache Rule.

Name it No Google Cache in the New Cache Rule Wizard pane.

In the destination rule cache, we need to specify the site without storage by selecting Add, clicking New and on the menu that appears, select the URL Set, enter the name Google and then select New and enter the http:/// address. www.google.com.

Click OK to return to the Add New Network Entities window, open the URL Sets section and select Google.

Click Next to continue, on the next screen, accept the default value, then click Next and select Never, no content will ever be cached. Finally click Finish to finish the setup process.

Thus, ISA Server 2004 has enabled Web Caching to save bandwidth, while preventing the storage of content of search sites like Google. Now we can verify the new policy created on the management interface and click Apply to apply.

3. Content Download Job configuration :

Suppose users on the system often visit www.security365.org to see new information about viruses or security errors, so we configure ISA Server to automatically download this site first. certain date and time of the week to improve operational efficiency.

Click Content Download Job, on the Tasks Pane pane, select Schedule a Content Download Job. We will see the message as shown below.

Select Yes and then name Content Download Job as SecureSolution, click Next to continue defining the schedule for the process.

Click Next and enter the website address to download in the Download content from this URL box, in this case we enter www.security365.org . Please select the default value in the next steps to complete.

Backup and restore ISA Server 2004 Firewall configuration information

For large systems with many departments and employees, each department requires its own access policies to make the policy number very much and difficult to manage. So in order to ensure that the system is working properly, we need to make backups of policies fully to restore when problems occur. We can back up the entire ISA Server or just some of the firewall policies.

The following operation will perform a full backup of the ISA Server. Open the ISA Management Console, select server name (ISA) and click Backup the ISA Server Configuration on the Tasks Pane pane.

Next we set the name of the backup file (should be in the form of X-XX-XXXX as the backup date-to-date to make it easier to carry out the recovery), select the storage location and click the Backup button. A dialog box asking for a password for the backup file appears, enter the password and click OK.

After the backup process is complete. To test, you can delete some or all firewall policies on your system, then select Restore this ISA Server Configuration on the Tasks Pane pane, locate the backup file, select Restore and enter the password set. for this file. After the recovery process is complete we can verify that the previous policies of the system have been fully restored.

In case of only backing up a certain firewall policy, we will do the same with the Export Firewall Policy function on the Task Pane pane.

Setting up DMZ Region and Publish Server Through ISA

One of the most popular security terms is DMZ (Demilitarized Zone), which refers to the "Demilitarized" zone in the real world, and in the computer environment, the DMZ is reserved for servers. "external" (like web server) allows external users (Internet) to access. Because the DMZ is completely separate from the Internal system, so when Internet users access these servers, it will not affect and endanger the computers and internal data. In addition, servers located in the DMZ prevent direct interaction between internal users and external users. In the traditional sense of the DMZ, the requests of internal users to "external" servers have to go through the DMZ first and then to the internal firewall, but today the DMZ includes both human situations. Internal use connects to the firewall / router and then requests will be transferred to servers in the DMZ based on Firewall Policy as the case that we apply later on ISA Server to build a DMZ containing mail and web server.

1. Create DMZ :

In the Network section, select Create a New Network, name it DMZ and select Next, select Perimeter Nework (we can create as many network layers as we like on ISA 2000 with only 3 classes, this is an improvement of ISA Server 2004).

Sau khi nh?n Next c?a s? Network Address xu?t hi?n, hãy ch?n Add Adapter ?? l?a ch?n card m?ng cho vùng DMZ.

Nh?n OK và ??a ch? m?ng cho vùng DMZ s? xu?t hi?n nh? hình d??i (b?n có th? thay ??i theo yêu c?u h? th?ng c?a mình), ti?p theo ch?n Next và Finish ?? hoàn t?t.

Sau khi nh?n Apply ?? áp d?ng cho h? th?ng, trong ph?n Network chúng ta s? th?y m?t l?p m?ng là DMZ tách bi ?t v?i h? th?ng Internal, b?n có th? ??t Exchange Mail Server hay Apche Web Server trong l?p m?ng này.

2. Publish Exchange Server trong DMZ :

L?y ví d?, công ty có m?t Exchange Server có ??a ch? là 172.16.1.10 ??t trong DMZ. ?? ng??i dùng bên ngoài Internet có th? truy c?p ??n mail server ?? g?i và nh?n mail chúng ta c?n ph?i "publish" (cho phép truy c?p t? Internet) chúng thông qua ISA Firewall c?a mình. M? ISA Management Console, ch?n Firewall Policy, trên khung Task Pane hãy nh?n vào Publish a Mail Server ?? hi?n th? New Mail Server Publishing Rule Wizard. ??t tên cho Publishing Rule này và ch?n Next.
Trong c?a s? Select Server Type chúng ta ch?n Server-to-server Communications: SMTP, NNTP.

Ch?n Next, trên khung Select Services hãy ?ánh d?u ch?n ô SMTP.

Trong c?a s? ti?p theo chúng ta nh?p vào ??a ch? c?a Mail Server trong DMZ, ? ?ây là 172.16.1.10.

Cu?i cùng là xác ??nh l?p m?ng ???c phép k?t n?i v?i Mail Server, trong tr??ng h?p này ng??i dùng ? bên ngoài

Internet nên chúng ta ch?n l?p m?ng là External và nh?n Next, sau ?ó ch?n Finish ?? hoàn t?t quá trình publish mail server.

C?n l?u ý là ?? có th? truy c?p email thì ph?i có thêm nh?ng protocol khác nh? DNS, POP hay RPC. Vì v?y có th ? chúng ta c?n cho phép các yêu c?u v? DNS t? Mail Server v?i Domain Controler (có cài tích h?p DNS) trong l? p m?ng Internal hay v?i các ISP DNS.

C?u Hình Remote Access VPN Trên ISA Server

Ngoài ch?c n?ng qu?n lý truy c?p Internet, Publish Web/Mail server và Caching, chúng ta có th? dùng ISA Server làm VPN Server cung c?p các k?t n?i remote access cho ng??i dùng bên trong ?? có th? truy c?p tài nguyên trên m?ng n?i b?. Ví d? công ty có m?t s? nhân viên kinh doanh s? d?ng máy tính xách tay và h? c?n truy c?p vào h? th?ng m?ng LAN thông qua VPN Server ?? ki?m tra mail, ch?y nh?ng ch??ng trình qu?n lý khách hàng hay c?p nh?t các báo cáo. Sau ?ây là các b??c c?u hình Remote Access VPN trên ISA 2004.

M? ISA Management Console ch?n m?c Virtual Private Network (VPN), sau ?ó ch?n Verify that VPN Client Access is Enable. ?ánh d?u ch?n Enable VPN client access và ??t giá tr? Maximum number of VPN clients allowed b?ng 9 (s? l??ng VPN client t?i ?a có th? k?t n?i cùng lúc) r?i nh?n OK và Apply chính sách m?i cho firewall.

?? các VPN client có th? k?t n?i thành công hãy t?o group VPN trên domain controler và gán quy?n Allow access cho thu?c tính Dial-in ??i v?i nh?ng user thu?c group VPN. Hãy ??ng nh?p vào Domain Controler c?a h? th?ng và ch?n *Start -> Administrative Tools -> Active Directory Users and Computers* . Nh?n chu?t ph?i trên *User container* , ch?n *New -> Group* .

Thêm nh?ng user thu?c b? ph?n kinh doanh (nh?ng ng??i c?n truy c?p qua VPN) vào VPN Group, ví d? Joe Franks. Trên thanh thu?c tính c?a Joe Franks ch?n tab Dial-in và ?ánh d?u ch?n Allow access.

Hãy tr? l?i màn hình qu?n lý ISA Server trên ISA1 mà chúng ta ?ang m? và ch?n Specify Windows Users trên danh sách VPN Client, nh?n Add và ch?n group VPN User chúng ta ?ã t?o.

Vi?c ti?p theo c?n làm ?? cho phép VPN client k?t n?i là c?u hình ??a ch? IP cho các VPN client, có hai cách là s ? d?ng DHCP ?? c?p phát IP ??ng cho các client ho?c dùng m?t static pool ?? gán IP cho chúng nh? sau:

Trên khung Tasks Pane nh?n vào m?c Define Address Assignment, ch?n Static address pool và nh?p vào dãy ??a ch? sau:

Nh?n OK, xác nh?n thêm m?t l?n n?a và kh?i ??ng l?i máy tính.

Cu?i cùng, hãy t?o access rule cho phép các VPN client có th? truy c?p ??n các tài nguyên n?i b? sau khi k?t n?i thành công ??n VPN server. Hãy ch?n Firewall Policy và ch?n Create New Access Rule ??t tên là VPN Client full access to Internal.

Nh?n Next và ch?n Allow, trên c?a s? ti?p theo ch?n All outbound trafic. Do access rule cho phép VPN client truy c?p tài nguyên n?i b? nên hãy xác ??nh source trafic là VPN Clients trong ph?n Network. Ng??c l?i ? khung destination hãy ch?n Internal trong ph?n Network, và ch?n các giá tr? m?c ??nh cho nh?ng b??c ti?p theo ?? hoàn t?t.

Bây gi? ISA Server ?ã s?n sàng cho các k?t n?i VPN, b?n ch? c?n t?o các VPN Connection ??n ??a ch? Outside

c?a firewall và th?c hi?n k?t n?i và truy c?p vào tài nguyên h? th?ng n?i b?.

B?n có th? tham kh?o file trình di?n cài ??t ISA Server t?i v? t?i http://www.security365.org/downloads/demo/ISA2004.rar.

Hi?n ?ã có phiên b?n th? nghi?m ISA Server 2006, b?n có th? t?i v? t?i http://www.microsoft.com/isaserver/2006/beta.mspx.

Nguyen Tran Tuong Vinh
Leader@Security365.Org
www.security365.org