

IIS 5, FTP, Different access permissions for different users

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-03/1199.html>

From: David Elliott (david.elliott@lifeway.com)

Date: 03/25/03

From: "David Elliott" <david.elliott@lifeway.com>

Date: Tue, 25 Mar 2003 09:43:21 -0800

Thanks for answering so quickly.

In answer to your statement "didn't quite get you" let me explain again:

My objective is to have internal users (IPs on 172.16.0.0 subnet) login as intFTP ("internal FTP user") to write to outgoing folder and read from incoming folder, and allow anonymous users (from anywhere) to read from outgoing folder and write-only to incoming folder.

I first tried one FTP site (Default FTP) Home directory E:\inetpub\ftproot containing outgoing and incoming folders (permissions set at NTFS level --- seems to work) with the virtual directory "intFTP" with Directory Security configured to deny access to all except 172.16.0.0 submask 255.255.0.0 also pointing to same path. Result: Anonymous users get correct permissions. IntFTP users get correct permissions.

Problem is that if you type:

<ftp://intFTP:password@ftp.domain.com> in IE,

it allows intFTP access regardless of your IP address --- like the 172.16.0.0 restriction is ignored.

I tried making two FTP sites with different IPs on same machine, pointing to same home directory: one for Anonymous and other userids and one site just for intFTP with the intFTP Virtual Directory deleted from original default FTP site and created under the new intFTP FTP site.

Result: Can still login to default FTP site by typing

<ftp://intFTP:password@ftp.domain.com> in IE (even from internet with client IP outside 172.16.0.0 range).

I was surprized that I could login to Default FTP site as intFTP and get access to the incoming and outgoing folders since the intFTP virtual directory only existed on the other FTP site.

Any ideas why it works this way?

>-----Original Message-----

>I am trying to allow anonymous users to our FTP site to
>Read-only from Outgoing folder and Write-only to Incoming
>folder.

>

>I want internal users (IP addresses 172.16.0.0) to be
able

>to logon using a userid and account to Read from Incoming
>folder and write to outgoing folder.

>

>I set NTFS permissions on the folders to give desired
>access and that works.

>

>My problem is in enforcing the IP restriction.

>

>ATTEMPT #1

>I created a Virtual directory pointing to same path as
>anonymous site E:\inetpub\ftproot and named it intFTP (so
>users could login as "intFTP") and set the Directory
>Security tab to deny all except IPs in 172.16.0.0 subnet.
>>>That didn't work. Internet users who log in as intftp
>still have access to the folders I only want internal
>users to have.

>

>ATTEMPT #2

>I created an additional Virtual site. Default FTP site
>supports anonymous access and other authenticated users
>who access other folders not in the inetpub\ftproot path
>and new Virtual site with different IP address for my
>internal (announced on internal DNS only). I deleted the
>intFTP virtual directory from default FTP site and
>created intFtp virtual directory in the new FTP site
(with

>same IP restrictions).

>>>> I was surprized to find that I could login to Default
>FTP site using intFTP userid eventhough the intFTP
virtual

>directory had been deleted from Default FTP Site and now
>only existed under new FTP site (different IP address).

>

>How can I ensure that users can only login to the new FTP
>site with the intFTP user account since both FTP sites
are

>on same machine? NOTE: The FTP server is configured to

microsoft.public.inetserver.iis.security: IIS 5, FTP, Different access permissions for different users

>use domain authentication (msftpsvc/DefaultLogonDomain =
>domainname) rather than local accounts.
>
>