

RE: Understanding ISA Server System Policy

Source:

<http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.configuration/2007-04/msg00053.html>

- *From:* Mohammad Ghavidel <[MohammadGhavidel@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto: MohammadGhavidel@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
 - *Date:* Mon, 23 Apr 2007 02:20:03 -0700
-

for dhcp and dns the system policies do able isa to be dhcp and dns CLIENT
not a server.

I show you required protocols and hope that you will be able to create
required access rule and properly configure them.
Microsoft CIFS (TCP 445)

- DNS
- Kerberos-Adm(UDP)
- Kerberos-Sec(TCP)
- Kerberos-Sec(UDP)
- LDAP (TCP)
- LDAP (UDP)
- LDAP GC (Global Catalog)
- RPC (all interfaces)
- NTP
- Ping

then you will be able to successfully join clients to your AD domain.

--
Mohammad Ghavidel MCSE 2000 & 2003

"Andy" wrote:

I am running ISA 2006 Standard on a Windows 2003 Enterprise R2 Server which
is a DC with DHCP and DNS roles.

I know it is best having ISA on another server but that is what the primary
school that I work at wanted after our LEA ICT support people said that is
all we needed. It saved the school some money and I had to go along with it.

The server has 2 NIC's for internal and external (internet) traffic.

- External
- 10.210.10.10
- Subnet Mask 255.255.255.0
- Gateway 10.210.10.1

RE: Understanding ISA Server System Policy

TCP/IP only

Internal

10.200.10.10

Subnet Mask 255.255.255.0

Gateway Blank

Client for Microsoft Windows, QoS, File and Printer sharing, TCP/IP.

The Internal card is above the external card in the advanced options in network connections.

At http://www.microsoft.com/technet/isa/2006/system_policy.msp it mentions that default system policies are applied after a default install for required network services: Active Directory, DHCP, DNS etc

Initially my workstations couldn't get an IP address through DHCP.

I created my own access rule for DHCP Requests and Replies, DNS, LDAP and PING, the workstations could get an IP address and the DNS server was from the internal card. I could then ping the server through IP address and by name.

I still cannot get the workstation to join the domain. It asks me for the username and password, which I enter the correct user details to perform the task. After a while I get a network path not found error.

My questions are:

1. Why did I have to create my own access rules when there are default system policies for these?
2. If I do have to create rules, what have I missed to enable the workstations to join the domain?

Thanks in advance for any help you can offer.

Andy