Knowledge Base

How to Configure a Firewall for Domains and Trusts

PSS ID Number: 179442

Article Last Modified on 8/5/2004

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional
- Microsoft Windows NT Server 4.0

This article was previously published under Q179442

SUMMARY

This article describes how to configure a firewall for domains and trusts.

MORE INFORMATION

To establish a domain trust or a security channel across a firewall, the following ports must be opened. Note that there may be hosts functioning with both client and server roles on both sides of the firewall. Because of this, ports rules may need to be mirrored.

Windows NT

Client Port(s)	Server Port	Service
1024-65535/TCP	135/TCP	RPC *
137/UDP	137/UDP	NetBIOS Name
138/UDP	138/UDP	NetBIOS Netlogon and Browsing
1024-65535/TCP	139/TCP	NetBIOS Session
1024-65535/TCP	42/TCP	WINS Replication

Windows 2000

For a mixed-mode domain with either Windows NT domain controllers or legacy clients or trust relationship between two windows 2000 domain controllers that are not in the same forest, all of the preceding ports for Windows NT may need to be opened in addition to the following ports:

Client Port(s)	Server Port	Service
1024-65535/TCP	135/TCP	RPC *
1024-65535/TCP/UDP	389/TCP/UDP	LDAP
1024-65535/TCP	636/TCP	LDAP SSL
1024-65535/TCP	3268/TCP	LDAP GC
1024-65535/TCP	3269/TCP	LDAP GC SSL
53,1024-65535/TCP/UDP	53/TCP/UDP	DNS
1024-65535/TCP/UDP	88/TCP/UDP	Kerberos
1024-65535/TCP	445/TCP	SMB

For Active Directory to function correctly through a firewall, the Internet Control Message Protocol (ICMP) protocol must be allowed through the firewall from the clients to the domain controllers so that the clients can receive Group Policy information. ICMP is used to determine whether the link is a slow link or a fast link. ICMP

is a legitimate protocol that Active Directory uses for Group Policy detection and for Maximum Transfer Unit (MTU) detection. ICMP does not have a port number, unlike the TCP protocol layer and the UDP protocol layer, because it is directly hosted by the IP layer.

Note There are specific requirements for RPC communication beyond what is listed in this table. For additional information about how to configure RPC communications for a firewall, click the following article number to view the article in the Microsoft Knowledge Base:

154596 How to configure RPC dynamic port allocation to work with firewall

By default, Windows 2000 DNS servers use ephemeral client-side ports when they query other DNS servers. However, this behavior may be modified with a specific registry setting that is described in the following article in the Microsoft Knowledge Base:

260186 The SendPort DNS registry key does not work as expected

Alternatively, you can establish a trust through the Point-to-Point Tunneling Protocol (PPTP) compulsory tunnel, and this will limit the number of ports that the firewall will need to open. For PPTP, the following ports must be enabled:

Client Ports	Server Port	Protocol
1024-65535/TCP	1723/TCP	PPTP

In addition, you would need to enable IP PROTOCOL 47 (GRE).

Note When you add permissions to a resource on a trusting domain for users in a trusted domain, there are some differences between the Windows 2000 and Windows NT 4.0 behavior. If the computer is not able to bring up a list of the remote domain's users:

- Windows NT 4.0 tries to resolve manually-typed names by contacting the PDC for the remote user's domain (UDP 138). If that communication fails, a Windows NT 4.0-based computer contacts its own PDC, and then asks for resolution of the name.
- Windows 2000 also tries to contact the remote user's PDC for resolution over UDP 138, but does not fall back on using its own PDC. Make sure that all Windows 2000-based member servers that will be granting access to resources have UDP 138 connectivity to the remote PDC.

Additional query words: tcpip

Keywords: kbenv kbhowto kbnetwork KB179442
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinNT400search kbWinNTS400 kbWinNTS400search kbWinNTsearch kbWinNTSsearch

---