Knowledge Base

How to Enable IPSec Traffic Through a Firewall

PSS ID Number: 233256

Article Last Modified on 11/21/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Datacenter Server

This article was previously published under Q233256

SUMMARY

IP Security (IPSec) is used to securely transmit data between computers. It is implemented at the Networking layer (Layer 3) of the Open Systems Interconnection (OSI) model. This provides protection for all IP and upper-layer protocols in the TCP/IP protocol suite. The primary benefit of securing information at Layer 3 is that all programs and services using IP for data transport can be protected.

MORE INFORMATION

IPSec does not disturb the original IP header and can be routed as normal IP traffic. Routers and switches in the data path between the communicating hosts simply forward the packets to their destination. However, when there is a firewall or gateway in the data path, IP forwarding must be enabled at the firewall for the following IP protocols and UDP ports:

- IP Protocol ID 50:
  For both inbound and outbound filters. Should be set to allow Encapsulating Security Protocol (ESP) traffic to be forwarded.
- IP Protocol ID 51:
  For both inbound and outbound filters. Should be set to allow Authentication Header (AH) traffic to be forwarded.
- UDP Port 500:
  For both inbound and outbound filters. Should be set to allow ISAKMP traffic to be forwarded.

L2TP/IPSec traffic looks just like IPSec traffic on the wire. The firewall just has to allow IKE (UDP 500) and IPSec ESP formatted packets (IP protocol = 50).

It may be necessary to allow Kerberos traffic through the firewall, if so then UDP port 88 and TCP port 88 would also need to be forwarded. For additional information, click the article numbers below to view the articles in the Microsoft Knowledge Base:

253169 Traffic That Can--and Cannot--Be Secured by IPSec

254949 Client-to-Domain Controller and Domain Controller-to-Domain Controller IPSec Support

254728 IPSec Does Not Secure Kerberos Traffic Between Domain Controllers

Keywords: kbenv kbinfo kbnetwork KB233256
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch