Windows Insider
34,000 Subscribers Worldwide
July 17, 2002
Issue #101

Feature

IPSec Troubleshooting Tips and Tricks

to top

Windows 2000 IPSec allows you to secure communications end-to-end. This end-to-end security protects the data from source to destination. This type of security is quite different from what you might see with a

traditional VPN connection, where the data is secure from client to gateway but "in the open" after leaving the gateway.

But, you also have to take the bad things along with the good things IPSec has to offer. There are times when IPSec or connections between two IPSec-enabled computers just don't work. In some cases, what appears to be a connectivity problem may in fact be a matter of misconfigured security policies, thus it is important that you be familiar with how IPSec and other security features work, and keep this information in mind when troubleshooting network connectivity in IPSec-enabled environments.

Failure of RAS Secured Communications

When secured communications fail but unsecured communications go through without problems on remote access connections, you should check the authentication method selected for the RAS connection. Another possibility is that the RAS server with which you are attempting to communicate does not support the security method. It's very common for a Server to require 128-bit encryption while the client doesn't support high encryption. All the client needs is an upgrade to the high encryption pack for its operating system.

Failure of Internal (LAN) Secured Communications

When you are unable to connect to another computer on your internal network (intranet), and you have verified that the computer is not offline, check your IP filter settings and ascertain that the list of acceptable security methods is correct.

Restarting the IPSec policy agent will clear old security associations that could be causing conflicts. To restart the policy agent, from the System Service Management console, double-click the IPSec Policy Agent in the results pane and click Restart (this will restart the IPSec driver as well).

Broken Policy Links

When more than one administrator is editing IPSec policies, links between the policy components could become broken due to the fact that the Active Directory assumes that whatever information is saved last is the current information. This is rare, but could occur if two administrators create rules that both use the same filter and then save the changes at the same time. This is only a problem when you're using IPSec Policies deployed via Windows 2000 Group Policy.

Windows 2000 protects against this problem by providing a way to check the integrity of the IPSec policies. To do so, from the IP Security Management console, click on the Action menu, select Task, and then click Policy integrity check. This will verify the validity of filters and settings and display an error message if any are found to be invalid.

Using the IPSec Monitor

Windows 2000 includes the IPSec monitoring tool, which displays active security associations on local or remote systems. This will help you to recognize patterns and trends of failed security associations or failed authentications or other indicators of bad policy settings.

To use the IPSec monitor, open the Run command and in the Open text box type:

```
ipsecmon <computername>
```

You should see an entry for every security association that is active, showing the policy name, the filter action, and the IP filter details. The tunnel endpoint will be shown if applicable. Other statistical information that can be provided by IPSec Mon includes:

* Number of active security associations
* Types of active security associations
* Number of master and session keys generated
* Number of ESP or AH bytes sent and received

By default, the IPSec monitor's information will be updated every 15 seconds. You can change the refresh rate using the Options button.

Using the IPSec monitor, you can determine whether your secured communications were transmitted successfully.

Using Event Viewer to Troubleshoot IPSec Problems

The Windows 2000 Event Viewer can be used in troubleshooting IPSec, since the IPSec policy agent writes to the System Log in several instances. For example, you can see in the Event Viewer whether local or Active Directory policy is being used, since the policy source is entered in the Event log.

You can also view the Security Log for entries pertaining to failures of secured communications or informational messages pertaining to the Oakley protocol. The Application Log may also contain messages from ISAKMP/Oakley.

Using Network Monitor to Troubleshoot IPSec Problems

The Network Monitor included with Windows 2000 (or the enhanced version that comes with System Management Server) can be used to view the AH and ESP transmissions. AH-secured packets will be indicated as TCP, UDP, or ICMP packets, but you will not see the AH header when you open the packet. ESP packets are easier to spot, as they are marked as ESP packets. Because it is encrypted, however, you won't be able to read the data itself when you open the ESP packet.

IPSec Files Missing

IPSec is installed as part of the installation of TCP/IP. If problems occur due to files that are needed for IPSec being deleted or corrupted, you reinstall IPSec by removing and then reinstalling the TCP/IP protocol.

Problems with Multihomed Computers

If a computer has multiple default routes, as is likely to be the case with a multihomed system, this can cause problems with secured communications. To correct the problem, open a command prompt and type route print and press the [ENTER] key. You will see a list of routes that make up the computer's routing table. If one has a destination 0.0.0.0, or if there is more than one with a metric of 1 (or the lowest metric if none are shown as 1), take one of the following actions:

1) Delete one of the default routes.
2) Ensure that one of the default routes has a lower metric value than all of the rest.

Performance Slowdown When Using IPSec

You should also be aware of the fact that implementing IPSec data encryption may slow down the network; this is to be expected due to the overhead involved in processing the encryption algorithms. There are ways to alleviate this; for instance, NDIS 5.0 allows for offloading of tasks. This means the encryption duties could be offloaded to the hardware so that the NIC would handle that task. Of course, offloading requires a NIC that is designed to support IPSec hardware offloading. There are a few NICs that can do this, such as the 3Com 10/100 Secure NIC.

Summary

IPSec is quite reliable and its unlikely you'll have many problems using it. However, the time may come when a small glitch causes a snafu in your IPSec Policies or connectivity. If you do run into problems, check out the things mentioned in this article and chances are good you'll be up and running in no time.

This week's feature article by
Deb Shinder
MCSE, etc.
Guest Contributor

Ask Uncle Bill

Q and A's

to top

Question:

Hi, Uncle Bill.
I am getting a persistant error on my Win2K GC. The error is:

"9999 - The DNS server has encountered numerous run-time events. These are usually caused by the reception of bad or unexpected packets, or from problems with or excessive replication traffic. The data is the number of suppressed events encountered in the last 15 minute interval. [14]"

The Microsoft knowledgebase is not really any help in this case. The error is occurring on the local Global Catalog server, which is connected to the rest of the WAN using relatively fast links. Any help appreciated. Cheers, Damian

Uncle Bill says:

Yo Damian! You're asking one of those questions for which there may be no answer. "What is the meaning of the DNS 9999 error?" "Does the falling tree in the woods make a sound when there is no one to hear?" Some people have posited that you see the DNS 9999 when the machine that is configured to use its own adapter to register isn't in DNS. That could be so, because I see my own GCs exhibit the same behavior when I configure them that way. You can check out Q198757 and Q199792 for what Microsoft has to say about this problem. But as you've pointed out, they're not too helpful when it comes to this error.

Question:

Hi, Uncle Bill
When I was allocating some IP address to one of our office machines I received the IP conflict error. I have open the Event Viewer and found the following error message: "The system detected an address conflict for IP address 203.199.178.194 with the system having network address 00:50:BA:32:31:D1. The local interface has been disabled". Now I want to know from which machine I was receiving the above error. I can find the MAC Address in Event Viewer. How to find now IP Address of the machine which is getting conflict. I have typed the command "arp -a" but I could not find the answer. Is there any tool to find the IP Address if we know MAC Address of the machine. I would be appreciate if any one could help me for this.
--Ramprasady

Uncle Bill says:

Hey, does that question look familiar? It should! It was in last week's newsletter. I wanted to run it again because we got another good answer from one of our readers. Braunyaur says:

"This is in regard to Ramprasady's issue with finding an IP Conflict in today's Windows Insider (issue #100). I run GETMAC from the W2K Resource Kit in a batch file, and run it every 30 days (or when a MAC Addres is added or changed).

<Syntax>GETMAC \\Servername

This data is copied to a .txt file (no, I haven't piped it, yet:)), and whenever I see an IP Address Conflict, I can search for the offending unit and resolve it quickly. I also use the LanGuard programs, and swear by them, but for just MAC Addresses, I find this to be quicker."

Thanks!

Security Advisories

Cumulative Patch for SQL Server

to top

This is a cumulative patch that includes the functionality of all previously released patches for SQL Server 2000. In addition, it eliminates three newly discovered vulnerabilities affecting SQL Server 2000 and MSDE 2000 (but not any previous versions of SQL Server or MSDE). Check the site for details. SEVERITY: *Moderate*

Read more...

SQL Server Install Process May Leave Passwords on System

to top

Another SQL Server problem. This time, its related to passwords that might be exposed during and after the installation process. If you run SQL 7 or 2000, check out the site to see if you're affected. Check the site for details. SEVERITY: *Moderate*

Read more...

News Headlines and Resources

Keeping Windows Current - Part One

to top

I pine for the days when you could download a service pack every few months and feel like you're up to date. Back in the day, you didn't worry about Internet scum and network criminals trying to ruin your network. You worried about making things work right. Those days are over, and you need to know how to update your OS whenever one is offered to you. Check out the article by Joern Wettern and get a true expert's advice.

Read more...

Configuring Exchange RPC Publishing in a Back-to-Back ISA Server Environment

to top

You've discovered the joys of Exchange RPC publishing and how happy it makes your users. Now you need to go to the next level: allow Exchange RPC through your back-to-back ISA Server configuration. Can you do it? Yes – check out the story here.

Read more...

Exchange 2000 Server Operations Guide

to top

Are you the one responsible for keeping your company's Exchange 2000 Server running? If so, you need to read this guide! Microsoft has done a great job in putting together this Exchange 2000 Server Operations guide. It covers backup, support, capacity planning and more!

Read more...

Next version of Exchange "Titanium" Unveiled

to top

Ready for the next version of Microsoft Exchange? Ready or not it's coming at you. Code named "Titanium", the next version of Exchange

will have some cool features that you've been waiting for. Check the link to find out what they are!

Read more...

Terminal Services Community Center

to top

Do you use Terminal Servers and clients? If so, you want to check out the Microsoft Terminal Services Community Center. There's a ton of good info here that should help you find the answer to just about any Terminal Services problem.

Read more...

Windows 2000 Service Pack 3 is Coming...When?

to top

Windows 2000 Service Pack 3 is late! How late? Really late! There are some problems with the Microsoft installer that might create havoc when the SP installation. So, no SP for you until they get the glitch in the MSI fixed.

Read more...

What Happened to Windows Corporate Update?

to top

What happened to the Corporate Update site? You know, the one you used to securely download files just like you used to without having to install some sort of Spyware/Scumware just to get a fix. Its gone, dead, caput. It wasn't up for long! Check out its premature demise at the old link.

Read more...

Walmart Helps Prepare You for a Windows-less Future

to top

I never thought Microsoft would lose its preeminent position as the consumer operating system of choice. But if you moisten your index finger and stick it in the air, you'll feel those winds 'o change blowing away from the Microsoft machine. The draconian licensing scheme is turning the Microsoft profit machine to the Microsoft "shoot yourself in the foot" machine. Who will win over the inevitable converts? Mac or Linux? Walmart is betting you'll check out Linux as a low cost, wormless alternative.

Read more...

Support WebCast: Microsoft Exchange 2000 Server Service Pack 3 Overview

to top

In this Support WebCast session, you'll be introduced to Exchange 2000 Server Service Pack 3. You'll hear about the various fixes included in SP3, and why it will benefit you to apply this service pack. You will also be introduced to the Active Directory updates included in Microsoft Windows 2000 SP3, and how they affect Exchange 2000 SP3.

Read more...

Download of the Week

Research-Desk 3.0

to top

Research Desk is a pretty simple application that can really help simplify your project management duties. Within a single integrated desktop environment you can view and edit your Microsoft Office docs, save a collection of open Office documents as a group, save Web pages with the group of Office docs, open and track files in the integrated file manager, and use integrated zip and unzip. We've started using this handy tool and I think it will even help me become more organized! Check out the 30-day trial before you buy.

Read more...