Using IPSec in Windows 2000 and XP, Part 2

Chris Weber 2001-12-20

This is the second part of a three-part series devoted to discussing the technical details of using Internet Protocol Security (IPSec) in a Windows 2000 and XP environment. The first installment of this series offered a brief overview of IPSec, as well as a look at the structure and interface for IPSec in Windows and a look at the two different modes of IPSec authentication methods for IKE in Windows. This article will discuss Security Associations, main mode authentication and IKE, Quick Mode Authentication Headers and ESP. We will also discuss some of the tools available in 2000 and XP.

Security Associations – How Connections are Managed

Security Associations, or SAs, are fundamental to IPSec. The SA is the negotiated set of protocols and parameters that the two computers will use to communicate. Actually, SAs are unidirectional. That is, if two computers have established a secured communications channel, they will at least have one SA each to manage that channel. They do not share an SA.

IKE negotiations actually consist of two phases, described more in the next sections. The first phase takes care of secure authentication, while the second phase sets up the security protocols such as ESP or AH to be used for the secure channel.

Let's illustrate this a little. Client1 is communicating with HR Server using transport mode IPSec. Client1 initiates the communications, and they first go through the process of authenticating with each other and proving their identities using ISAKMP/IKE. This first phase produces what can be called an IKE SA. Next, IKE begins negotiation of the security protocols that will be used to set up the secure communications channel between the two computers. Client1 may offer ESP using 3DES-CBC encryption and AH using HMAC-SHA1 as the two options it will accept. The HR Server may only wish to use ESP with 3DES-CBC encryption so it will respond with only that option. At that point there is agreement and IKE sets up the secure channel using 3DES-CBC and passes this second SA off to the IPSec Driver for processing.

Before we leave our talk of SAs there is a very important piece to mention. Consider the fields that make up an ESP and AH packet, per RFC 2406 and 2402 respectively. Each packet contains a 32-bit value known as the **Security Parameters Index** (SPI), immediately followed by a 32-bit Sequence Number value. The SPI is critical to determining the integrity of datagrams. Its value is set for each SA, and uniquely identifies the Security Association for a particular datagram. If a computer suddenly gets a datagram with a bad SPI value, it will discard the packet. The Sequence Number value is used to keep session state, as a monotonically increasing value.

IKE Phase I – Main Mode Authentication and IKE

Main Mode is the initial form of IKE negotiation. This is where master key material is generated, and the computer identities are authenticated, using the authentication method you have chosen. Main Mode must successfully complete before moving on to Phase II – Quick Mode.

Computer identities are protected during Main Mode for Certificate and Preshared Key authentication. Encryption takes place before this information is sent out. However, identity privacy is not maintained when using Kerberos, where the computer identity is sent unencrypted.

The completion of Main Mode negotiations results in an ISAKMP SA, also known as a Main Mode SA. The default Windows settings will make the Main Mode SA last for 8 hours (480 minutes), at

which point, if data is being actively transmitted, a new Main Mode SA will automatically be renegotiated. This lifetime setting can be adjusted through the IP Security Policy snap-in – click the **Key Exchange Advanced** button on the **General** tab for the properties of an IPSec policy.

Clicking the **Methods** button will take you to the place where you can configure the encryption and hashing algorithms that IKE will use for SA negotiations, the preference order for negotiations, and the key strengths of the Diffie-Hellman Group that it will accept.

The Main Mode SA is not visible in the ipsecmon.exe utility described later; however, it is viewable with netdiag and the IP Security Monitor snap-in of Windows XP.

IKE Phase II – Quick Mode Authentication Headers and ESP

IKE has a lot of responsibility. Phase II is where its job comes to a close. Quick Mode negotiations determine the security protocols and lifetimes that will be used for the secure communications channel. Your selections are determined in the IPSec policy you created, and can consist of either Authentication Headers, Encapsulating Security Payload, or a combination of both.

AH provides connectionless integrity, data origin authentication, and anti-replay protection for IP datagrams. It does not provide encryption. AH protects the entire packet by signing everything from the beginning of the IP Header to the end of the payload (refer to **Figure 4** from the first article in this series). The packet is signed using an HMAC-SHA1 or HMAC-MD5 hashing algorithm, configurable by the administrator through the IP Security Policy snap-in – policy properties, rule, filter actions tab.

ESP may provide encryption and limited traffic-flow confidentiality. It may also provide connectionless integrity, data origin authentication, and anti-replay protection. ESP uses the same hashing algorithms – SHA1 or MD5. The encryption algorithms you may choose from include DES and 3DES. The configurations for ESP protection are also configurable by the

administrator through the IP Security Policy snap-in – policy properties, rule, filter actions tab.

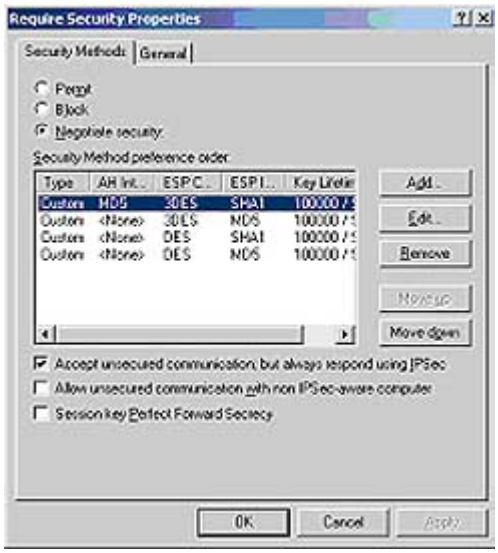
The main difference between AH and ESP, aside from encryption, is that AH protection starts at the beginning of the IP datagram, whereas ESP protection starts after the IP header (refer to **Figure 3** from earlier).

Lifetimes for Quick Mode SAs are configurable and default to either 5 minutes or 100 MB of traffic. At this point, new Quick Mode SAs would be automatically renegotiated.

There are a couple of options to be aware of when configuring your Security settings:

1. Accept unsecured communication, but always respond using IPSec
2. Allow unsecured communication with non IPSec-aware computers

Checking either of these two options could jeopardize security by allowing for fallback to unsecured communications if a client requests it. However they may be necessary in your environment.



Once IKE has finished setting up the Phase II SA, it passes the SA and the shared encryption key off to the IPSec Driver and communications begin.

Interface - Get Your Tools Ready

Several tools are available to help manage and monitor IPSec in Windows. There are some differences between Windows 2000 and XP. Let's look at each tool:

IPSec Security Policies snap-in for the MMC (Windows 2000 and XP)

This is the primary GUI for setting up IPSec policy on either the local or a remote machine. This snap-in is already added to the **Local Security Policy** MMC, so start it either through the Administrative Tools menu, or from Start, Run, **secpol.msc.** The policy, its rules, and all filters can be created by navigating through the myriad of windows in this GUI. At first, the amount of options may seem overwhelming, but going through all layers of this interface will give you a better understanding of what is configurable.

From here, policies can be created, verified, exported to, or imported from a file. There is also an option to Manage IP Filter Lists and Filter Actions, which gives you a central place to define

all your filters. This can make applying filters easier – for each rule you only have to check the filters you want to enforce, rather than creating new filters on the fly.

Of course almost every other option is configurable here, including:

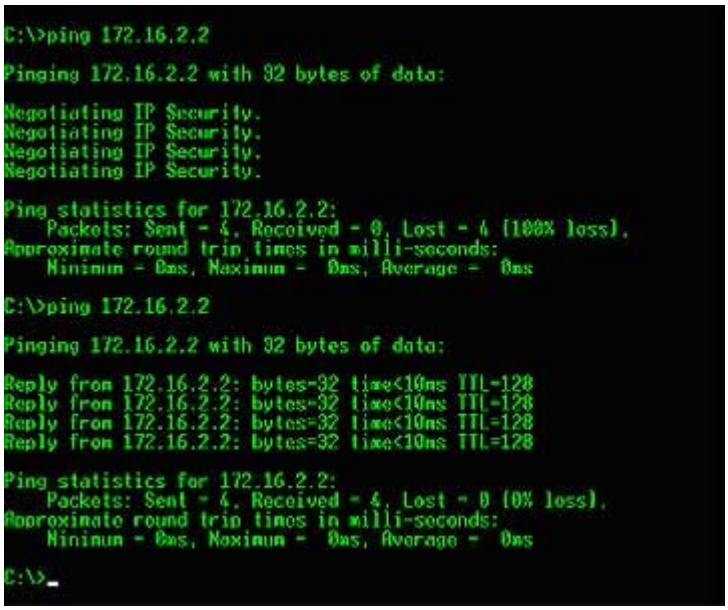
- comments and names (for general policy, rules, and filters)
- Key Exchange Settings for Main Mode (under policy properties, General tab, Advanced)
- IP Filters (under policy properties, Rules, edit, IP Filter List tab)
    - This is where you setup IP filters. Much like a firewall rule, these filters define packets based on IP headers.
- Packet security settings (under policy properties, Rules, edit, Filter Action)
    - These are the security settings associated with the IP Filters you have set up. This is where you define whether a packet is to be Permitted, Blocked, or Negotiated for security settings such as AH and ESP. These include granular settings for Integrity and Encryption algorithms as well as key lifetimes.
- Authentication Methods (under policy properties, Rules, edit, Authentication Methods tab)
    - Defines how the packets you defined in IP Filters will be authenticated, using either Kerberos, Certificates, or preshared keys.

IPSecpol.exe (Windows 2000 and XP) The command line tool for creating IPSec policies is called **ipsecpol.exe**, and is available from Microsoft's download page. A nice function of ipsecpol.exe is that it has two modes – Dynamic and Static. Dynamic mode defines policy that will be loaded and enforced for the duration of the Policy Agent. That is, upon Policy Agent restart, or computer reboot, the policy and its filters are forgotten. Dynamic filters currently cannot be set under Windows XP. Static mode is the common mode of defining a policy for indefinite use.

Type `ipsecpol -h` from the command line (once it is in your environment path) to get detailed usage information. This is a good tool because it can be used in dynamic scripts or logon scripts to suit your needs.

ping.exe (Windows 2000 and XP)

If ICMP traffic is allowed in your policies, then the ever-useful ping program will initiate an IKE negotiation (if an SA is not already established). As shown in the screenshot, you will see four "Negotiating IP Security" messages the first time around. With a successful SA negotiation, the next four ICMP echo requests generated by ping.exe will do their normal thing, and elicit four ICMP echo replies.



Netdiag.exe (installed from the Windows 2000 or XP installation CD, \Support directory) Netdiag is a useful utility for any network administrator or support professional. It provides detailed information on an enormous amount of networking components, as well as runs diagnostic tests to help isolate networking problems. Type `netdiag –h` from the command line once it is installed, to see all of your options.

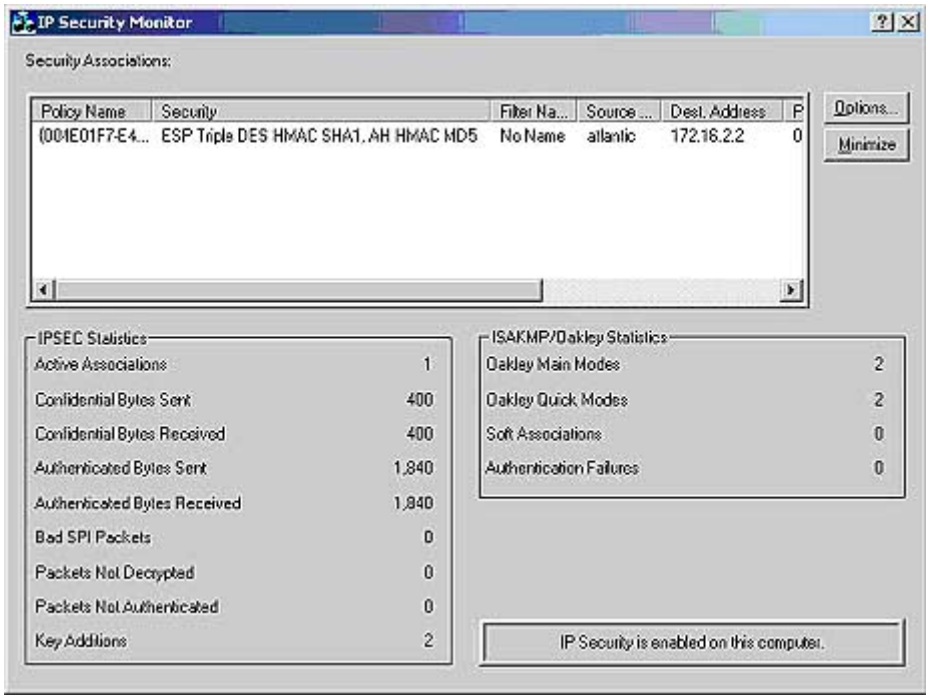
Caution: Netdiag requires that the Remote Registry service be running (even locally!). See Microsoft Article ID: Q287735 for details.

To run a test of IPSec type `netdiag /test:ipsec /debug` from the command line. This will return valuable IPSec policy information including rule and filter details, and preshared keys in clear text! This command will also return both the active Main Mode SAs and Quick Mode SAs.

Note: In order to run the /debug option on a computer with domain IPSec policy assigned, you must be logged in as a domain admin.

IPSecmon.exe (only in Windows 2000)

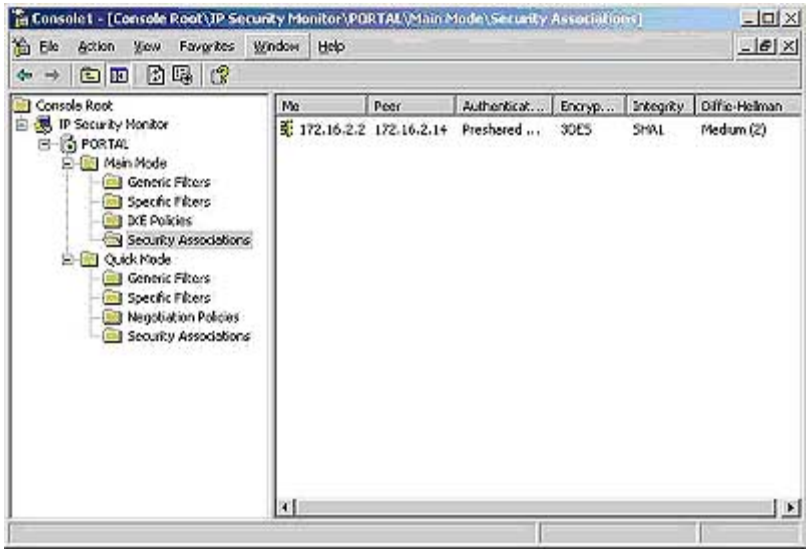
Type `ipsecmon` from a command line, or from `Start, Run`. The IPSec Monitor displays active Quick Mode SAs on your computer, as well as valuable ISAKMP/Oakley and IPSec statistics. This tool is great for troubleshooting connections, take a look at Authentication Failures, under the ISAKMP/Oakley statistics section, and you know that you probably have inconsistent authentication configurations between your two hosts.



Note: While Quick Mode establishes two SAs (one per computer), only the outbound SA for your computer is displayed.

IP Security Monitor snap-in (Windows XP only)

This tool is the equivalent of ipsecmon.exe in Windows 2000. However, Microsoft beefed it up a bit to provide even more information. You can now view Main Mode and Quick Mode SAs separately, and you can even add remote computers to the MMC. There is no default shortcut for this tool, you have to start the MMC (Start, Run, MMC) and add the snap-in for it.



Event Viewer (Windows 2000 and XP)

The Event Viewer is used to view the following IPSec events:

- Policy Agent and IPSec Driver events (System Log)
- Oakley events (Application Log)
- ISAKMP and SA details (Security Log – requires that logon auditing be enabled)

With auditing enabled for logon events, policy changes, and object access, useful IPSec events can be gathered. As an example, you should see event ID 541 in the Security Log, which denotes the establishment of an IPSec Security Association.

ipseccmd.exe (only Windows XP)

IPSeccmd is a very useful command line tool for displaying IPSec policy information, including filters and preshared keys, and many usage statistics. Type `ipseccmd show all` to display IKE SAs, IPSec filters, and IPSec usage statistics. It is similar to netdiag in some regards, but more focused on IPSec in that it returns more information, especially related to usage statistics, that netdiag does not.

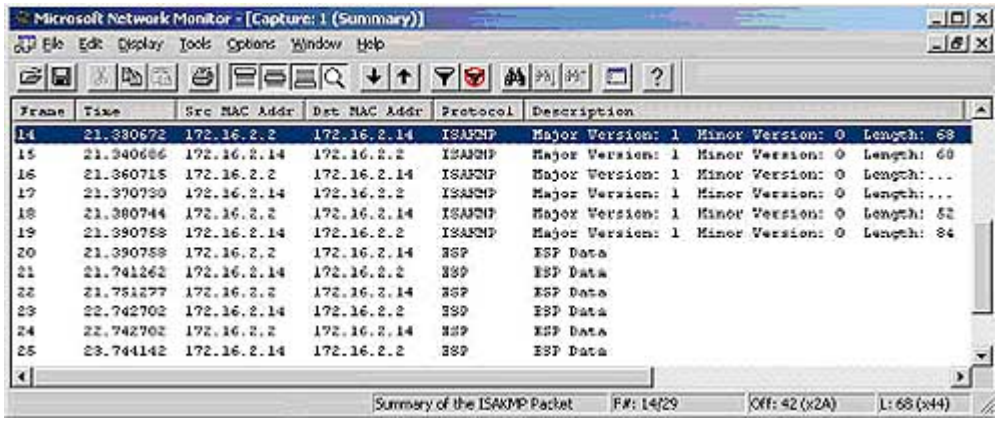
Network Monitor (Windows 2000 and XP)

Netmon is Microsoft's packet capture tool. It is a good general-purpose packet decoder, and will break down protocols such as ESP and AH for you.

Netmon can be installed from the SMS 2.0 CD (this version allows promiscuous mode capture) or as a component install under 2000 or XP. To install as a built-in component, navigate to the Control Panel, open Add/Remove Programs, click Add/Remove Windows Components, click Management and Monitoring Tools, then click Details - you will see the option for Network Monitor Tools.

Network Monitor v2.0 includes parsers for ISAKMP, AH, and ESP traffic. AH traffic will actually be parsed into upper layer protocols such as TCP and UDP, thus will not be displayed as AH. ESP traffic cannot be parsed this way because the upper layer protocols are encrypted.

The following screenshot illustrates the traffic generated from the ping example. First is a series of ISAKMP negotiations, followed by ESP encrypted ICMP packets.



Registry Settings for Advanced Logging

So you want more information dumped to the Event Viewer. Well the following registry value will give you the details you crave, but only in Windows XP. Most of these dump events to the System Log.

`HKLM\System\CCS\Services\IPSEC\EnableDiagnostics`

You will have to add EnableDiagnostics as a `DWORD` value of 1 through 7, where: 0 = no logging 1 = get aggregated driver logs, bad SPI value, unauthenticated hash, except "clear text received when should have been secured" 2 = no aggregated driver logs, get inbound-only per packet

drop events, including “clear text received when should have been secured” 3 = both level 1 and 2 logging turned on 4 = no aggregated driver logs, get outbound-only per packet drop events 5 = both level 1 and 4 logging turned on 6 = both level 2 and 4 logging turned on 7 = all logging enabled

More advanced logging can be achieved for the Oakley logs with this value (not set by default):

```
HKLM\System\CurrentControlSet \Services\PolicyAgent\Oakley\EnableLogging
```

Setting this key as a `DWORD` value of 1 will enable Oakley logging. The log files will be stored in SystemRoot\Debug. Once enabled, all ISAKMP Main Mode and Quick Mode negotiations are logged to a file. This file is overwritten when the Policy Agent is restarted.

Conclusion

That concludes the second article in this three-part series on IPSec for Win2K and XP. Join us next time as we conclude this series with a look at the integration of IPSec policies into Active Directory, attacks on IPSec and other security concerns, as well as a few properties of IPSec.

Relevant Links

Using IPSec in Windows 2000 and XP, Part One
Chris Weber, SecurityFocus

How to Configure IPSec Tunneling in Windows 2000
Microsoft Product Support Services

IETF home page for the IP Security Protocol

RFC 2401 – Security Architecture for the Internet Protocol

RFC 2402 – IP Authentication Header

RFC 2406 – IP Encapsulating Security Protocol

RFC 2408 – Internet Security Association and Key Management Protocol (ISAKMP)

RFC 2409 – The Internet Key Exchange (IKE)

Client-to-Domain Controller and Domain Controller-to-Domain Controller IPSec
Microsoft Product Support Services

Traffic That Can--and Cannot--Be Secured by IPSec
Microsoft Product Support Services

Step-by-Step Guide to Internet Protocol Security (IPSec)
Microsoft TechNet

Configuring IPSec to Handle Trusted and Untrusted Domain Authentication
Microsoft Product Support Services

How to Enable IPSec Traffic Through a Firewall
Microsoft Product Support Services