Using IPSec in Windows 2000 and XP, Part 3

Chris Weber 2002-01-03

This is the third and final installment in a series devoted to exploring IPSec in Win2K and XP. 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. The second installment discussed Security Associations, main mode authentication and IKE, Quick Mode Authentication Headers and ESP, and some of the tools available in 2000 and XP. This article will 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.

Active Directory Integration

The intention from the start was that IPSec policies could be integrated into the Active Directory. This means that your 2000 and XP domains can store and distribute IPSec configurations through Group Policy. From this point on, the rules of Group Policy take over. This means that applying IPSec policies to domains, organizational units, or individual machines and users, depends on what your needs are and how Group Policy is used in your organization.

So you can set up IPSec policies for Organizational Units that you have defined in your Active Directory database, by using the **Active Directory Users and Computers** snap-in for the MMC. Simply right-click on the OU you want to create policy for and select properties. Then navigate to the Group Policy tab and click the Add button. Navigate to **Computer Configuration\Windows Settings\Security Settings\IP Security Policies**, where you can create and modify IPSec policies for your OU. You can also use the Group Policy snap-in to troubleshoot policy precedence issues that might arise from Group Policy inheritance.

Attacks on IPSec and Other Security Concerns

There are some important security considerations to keep in mind about IPSec in Windows:

1. preshared keys are stored clear text in the registry, accessible by administrators
2. Active Directory stores IPSec configuration policies, and preshared keys in the clear, with relaxed access controls
3. Exemptions allow certain traffic to pass unprotected
4. DoS attacks
5. lower layers still vulnerable
6. upper layers still vulnerable

We will touch briefly on each of these. **Preshared Keys** are displayed in clear text through the GUI, and stored clear text in the registry, both accessible by administrators. Check the subkeys of the following registry key for details:

```
HKLM\Software\Policies\Microsoft\Windows\IPSec\Policy
```

Important note: Microsoft has been publicly telling people all along NOT to use preshared keys in production Microsoft IPSec environments. The preshared key functionality is only included to meet RFC compliance, and for testing purposes.

The **Active Directory** stores IPSec configuration policies in a central container. All comments, preshared keys, and other configuration information is stored here, in a combination of clear text and hex, which can be deciphered with minimal time. The following container defaults to allowing all “Authenticated Users” read access to this information. While this may be necessary for deploying Group Policy, you may want to fine-tune these directory permissions to fit your needs.

```
LDAP://abc.forest.com/CN=IP Security,CN=System,DC=forest,DC=com
```

Default Exemptions will be the biggest section here, because they deserve some of the highest concerns. By default, certain traffic is not protected by IPSec filters in Windows 2000. These unprotected traffic types are known as the default exemptions, and, (minus Broadcast and Multicast) apply only to IPSec transport mode filters:

A. **Broadcast** – Broadcast traffic is considered to be traffic going from one sender to many receivers on the same subnet. Windows uses broadcast traffic for many functions, including NetBIOS name queries and announcements. As an example, a class C subnet using 172.16.2.0 and subnet mask 255.255.255.0 (class C) has a broadcast address of 172.16.2.255. This exemption can be disabled in Windows XP.
B. **Multicast** – Similar to Broadcast traffic, multicast traffic is when a sender sends an IP packet to multiple receivers in the address range 224.0.0.0 to 239.255.255.255. This exemption can be disabled in Windows XP.
C. **Resource Reservation Protocol (RSVP)** – RSVP traffic is IP protocol 46, and is used for Quality of Service (QoS) of IP traffic. This exemption is required for QoS to work with Windows 2000. This exemption can be disabled in Windows 2000 and XP.
D. **Internet Key Exchange (IKE)** – IKE uses source and destination UDP port 500. It is paramount to remember this as you may need to configure a firewall to let this traffic through for IKE negotiations to take place.
E. **Kerberos** – Kerberos is the core authentication protocol used in Windows 2000 and XP. Kerberos traffic uses a TCP and UDP source and destination port 88. It is important to keep in mind that the IPSec exemption for Kerberos traffic is as simple as: if a packet is TCP or UDP, and has a source or destination port equal to 88, then permit the packet unprotected. This exemption can be disabled in Windows 2000 and XP.

Only Unicast traffic can be protected by IPSec in Windows 2000 and XP. Broadcast and Multicast traffic filtering is not supported, and therefore not protected by IPSec.

IPSec tunnel mode filters also cannot process multicast and broadcast traffic. However RSVP, IKE, and Kerberos traffic can be secured by an IPSec tunnel.

The thing to keep in mind about the exemptions is that just because you set a rule saying that all IP traffic is to be protected, doesn’t mean it will. These are the only exemptions listed above, so keep these in mind. Also remember that the IPSec driver does not do content filtering, but only filters on IP headers.

Important note: Microsoft has provided a means for removing these default exemptions. There is a registry value you can set, check it out:

```
HKLM\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt
```

This key needs to be added to the registry as a DWORD value. It can be set to 0 or 1 in Windows 2000, or 0,1, or 2 in Windows XP:

```
0 = default exemptions are still active
1 = disable the exemption for RSVP and Kerberos
2 = disable the exemption for broadcast and multicast (Windows XP only!)
```

An attacker could potentially use these exemptions to force unauthorized traffic through your

IPSec filters.

IPSec was built with defense against **Denial of Service** attacks in mind. However, IKE still has some known vulnerabilities to DoS attacks – scour the web for references and you will see. Basically, flooding the computer with IKE exchange initiations will fill up the IKE state table, and consume CPU cycles and memory space. While established connections will remain connected, new connections will be prevented. This is not specific to the Microsoft IPSec implementation, but a natural shortcoming of the IPSec architecture.

Lower layer attacks are still possible. ARP cache poisoning and other layer 2 attacks still take place before IPSec even wakes up. This is not specific to the Microsoft IPSec implementation, but a natural shortcoming of the IPSec architecture.

Upper layer attacks have been the focus of widespread mayhem in the recent past. While IPSec will protect who can talk to who, and encryption of the communication, it cannot protect a buggy application that is vulnerable to a buffer overflow. So, if your DMZ web server is using IPSec to secure communications with the backend SQL database, an allowed web surfer can still use SQL query poisoning to exploit the SQL server. See the CNET article Sequel to SQL oversights by Chris Prosise and Saumil Shah for more details.

The facts of IPSec in Windows

- The implementation is based on IETF standards for interoperability and security of communications.
- IPSec can be used with the Clustering and Network Load Balancing (NLB) services of Windows 2000 Advanced Server. However there will be a temporary connectivity loss during failover as stateful connections must be re-established.
- Certificate-based authentication is supported for certificates that meet certain criteria. This criterion includes such things as RSA (not DSA), key size of 512 bits or larger, and a digital signature included in the certificate.
- IPSec policy requires administrative privileges to manage and operate. If you do not want end users having access to manage and control IPSec policies, then do not give them administrative rights.
- There are currently no API's in place for the management and connection-oriented functions of IPSec. IPSec is provided solely as an administrative interface. This may change in the future as Microsoft extends the functionality to third party developers.
- RFCs 2401 and 2409 are important, be sure to read them.
- IPSec protected traffic will not work with Network Address Translation (NAT). NAT needs to modify packets in transit, but IPSec is designed to be tamper resistant, preventing packet modification. The IETF is currently working toward specifying a NAT and IPSec interoperability standard.
- Tunnel mode in IPSec only works for gateway-to-gateway, server-to-gateway, or server-to-server communications. By itself, IPsec is not a solution for client VPN remote access.
- So you want a secure VPN remote access solution for the travelers eh? The only way that is possible under Windows 2000 and XP (or most other implementations of IPSec) is to use IPSec and L2TP together. Clicking the tunnel mode button in the IPSec policy is not what you want to do here. You need to use IPSec transport mode to secure the L2TP flow. That's right, it's L2TP inside of and protected by IPSec.

Relevant Links

Using IPSec in Windows 2000 and XP, Part One

Using IPSec in Windows and XP, Part Two

How to Configure IPSec Tunneling in Windows 2000

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

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

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

Configuring IPSec to Handle Trusted and Untrusted Domain Authentication

How to Enable IPSec Traffic Through a Firewall

Privacy Statement