

Using Microsoft Windows 2000 IPsec as a workstation firewall

Marc DeBonis
VTmig
V1.1 - 020911

Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPSec is based on standards developed by the Internet Engineering Task Force (IETF) IPSec working group.

IPSec is supported by the Windows .NET Server, Windows XP, and Windows 2000 operating systems and is integrated with the Active Directory directory service. IPSec policies can be assigned through Group Policy configuration of Active Directory domains and organizational units. This allows the IPSec policy to be assigned at the domain, site, or organizational unit level, simplifying IPSec deployment.

For more information about IPSec, please see:

<http://www.microsoft.com/windows2000/technologies/communications/ipsec/default.asp>

<http://vtntug.w2k.vt.edu> (see presentations)

Included in this document are directions on enabling a firewall_base local IPSec policy for your workstation. Once enabled, you can determine for yourself how IPSec functions as a firewall. As defined, this firewall configuration should only be considered a base (basic) level policy. In accordance with proper firewall configuration, this policy is based on a DENY ALL default. With the proper experimentation, “holes” are opened in the policy to allow certain ip address, protocols, and ports to and from the local system. In this way, with careful design, the system can be strongly secured, while still maintaining a high level of usability. For differing ip ranges (say NOVA), or for other services such as LPR printing, DHCP address leasing, and video conferencing, the application\service must be examined and fully understood and new “holes” written into the policy to achieve proper functionality.

To test this policy, all applications as stated in the documentation were tested for functionality. Once these were determined to work, Doug Edmonds and I used nmap and GFI Languard to scan the system from VT and non-VT addresses. The only ports the scans from the VT address detected were the ones we deliberately opened and the non-VT address didn't even see a system at that ip address! Mitigating this success is the fact that IPSec does not do stateful inspection, so if a port scan is conducted from a port that is allowed into the system, it would succeed.

In summary, I think IPSec can be used, in some limited cases, both for a standalone workstation and as part of a pushed secure group policy in the VT AD. If group policies are not used, customization of the policy should be designated to the local administrator who is aware of additional requirements for the systems. I strongly suggest that people familiar with ZoneAlarm or BlackIce Defender try this setup to acclimate themselves to how it works and what functionality they are gaining and losing by using this built in functionality of Windows 2000.

Marc DeBonis
VTmig - Systems Architect

IPsec can also be installed and run on a standalone workstation. The following instruction will show you how to install, enable and disable the base firewall configuration on any Windows 2000 system.

1. Log in as the local administrator of the system
2. Point a web browser to <http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp>
3. Download the file http://download.microsoft.com/download/win2000platform/ipsecpol/1.00.0.0/nt5/en-us/ipsecpol_setup.exe
4. Execute the file to install
5. Use notepad to create a empty file in the same directory you installed the ipsecpol files to (be sure there is no .txt suffix on the file!)
6. Cut and paste the text of section A into the file (you may need to make sure the lines do not wrap in notepad)
7. Save the file as enable_firewall.bat
8. Use notepad to create a empty file in the same directory you installed the ipsecpol files to
9. Cut and paste the test of section B into the file
10. Save the file as disable_firewall.bat
11. Open a MSDOS command prompt
12. Change to the directory you installed the ipsecpol files to
13. To enable the base firewall, type “enable_firewall.bat” (no quotes)
14. Test to insure you can still do:
 - a. DNS lookups
 - b. Network mapping to/from the machine
 - c. Remote Desktop to machines
 - d. Web browsing and secure web browsing
 - e. Outlook XP/Exchange 2000 mail/calendaring
 - f. POP/SMTP mail
 - g. Ping machines local to the VT ip space
15. To disable the base firewall, type “disable_firewall.bat” (no quotes)

Section A

```
REM
REM Base ipsec firewall for VT central campus systems
REM by Marc DeBonis, Mike Moyer, and Zeb Bowden
REM version 1.1 - 020830
REM
REM Read and learn, edit and burn...
REM
REM Stop firewall_base
REM
ipsecpol -w REG -p "firewall_base" -y
REM
REM Delete firewall_base
REM
ipsecpol -w REG -p "firewall_base" -o
REM
REM Deny All by default
REM
ipsecpol -w REG -p "firewall_base" -r "blockall_raw" -f *+0::RAW -n BLOCK
ipsecpol -w REG -p "firewall_base" -r "blockall_udp" -f *+0::UDP -n BLOCK
ipsecpol -w REG -p "firewall_base" -r "blockall_tcp" -f *+0::TCP -n BLOCK
ipsecpol -w REG -p "firewall_base" -r "blockall_icmp" -f *+0::ICMP -n BLOCK
REM
REM Allow ping locally
REM
ipsecpol -w REG -p "firewall_base" -r "ping_a" -f 128.173.*+0::ICMP -n PASS
ipsecpol -w REG -p "firewall_base" -r "ping_b" -f 198.82.*+0::ICMP -n PASS
REM
REM Allow access to DNS (allow remote to port 53)
REM
ipsecpol -w REG -p "firewall_base" -r "DNS_tcp" -f 198.82.247.34:53+0::TCP -f 198.82.247.98:53+0::TCP -n
PASS
ipsecpol -w REG -p "firewall_base" -r "DNS_udp" -f 198.82.247.34:53+0::UDP -f 198.82.247.98:53+0::UDP -
n PASS
REM
REM Allow local netbios traffic in and out (allow local to ports 135,137,138,139)
REM
ipsecpol -w REG -p "firewall_base" -r "local_netbios_a_in" -f 128.173.*+0:135:TCP -f 128.173.*+0:135:UDP -
f 128.173.*+0:137:UDP -f 128.173.*+0:138:UDP -f 128.173.*+0:139:TCP -f 128.173.*+0:445:TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "local_netbios_b_in" -f 198.82.*+0:135:TCP -f 198.82.*+0:135:UDP -f
198.82.*+0:137:UDP -f 198.82.*+0:138:UDP -f 198.82.*+0:139:TCP -f 198.82.*+0:445:TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "local_netbios_a_out" -f 128.173.*:135+0::TCP -f
128.173.*:135+0::UDP -f 128.173.*:137+0::UDP -f 128.173.*:138+0::UDP -f 128.173.*:139+0::TCP -f
128.173.*:445+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "local_netbios_b_out" -f 198.82.*:135+0::TCP -f 198.82.*:135+0::UDP
-f 198.82.*:137+0::UDP -f 198.82.*:138+0::UDP -f 198.82.*:139+0::TCP -f 198.82.*:445+0::TCP -n PASS
REM
REM Allow traffic to terminal Servers (allow remote to port 3389)
REM
```

```
ipsecpol -w REG -p "firewall_base" -r "term_serv_a" -f 128.173.*.*:3389+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "term_serv_b" -f 198.82.*.*:3389+0::TCP -n PASS
REM
REM Allow connections to web servers (allow remote to port 80,443)
REM
ipsecpol -w REG -p "firewall_base" -r "web" -f *:80+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "secureweb" -f *:443+0::TCP -n PASS
REM
REM Allow connections to Exchange (allow 1026 to frodo.cc.vt.edu, allow 1712, 1097, 1701, 1066 to
fangorn.cc.vt.edu)
REM
ipsecpol -w REG -p "firewall_base" -r "exchange_a" -f 198.82.160.13:1026+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "exchange_b" -f 198.82.160.35:1712+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "exchange_c" -f 198.82.160.35:1097+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "exchange_d" -f 198.82.160.35:1701+0::TCP -n PASS
ipsecpol -w REG -p "firewall_base" -r "exchange_e" -f 198.82.160.35:1066+0::TCP -n PASS
REM
REM Allow connections to other mail server (allow 25, 110,995 to mail.vt.edu)
REM
ipsecpol -w REG -p "firewall_base" -r "popmail" -f 198.82.161.8:25+::TCP -f 198.82.161.8:110+0::TCP -f
198.82.161.8:995+0::TCP -n PASS
REM
REM Start firewall_base
REM
ipsecpol -w REG -p "firewall_base" -x
```

Section B

```
REM
REM Base ipsec firewall for VT central campus systems
REM by Marc DeBonis, Mike Moyer, and Zeb Bowden
REM version 1.1 - 020830
REM
REM Read and learn, edit and burn...
REM
REM Stop firewall_base
REM
ipsecpol -w REG -p "firewall_base" -y
REM
REM Delete firewall_base
REM
ipsecpol -w REG -p "firewall_base" -o
```