

# Anatomy of IPSec Policies in Windows 2000

## IPSec Policies

(There are three default policies, more can be created, but only one can be assigned at a time)

### Status: (Assigned, or Unassigned)

Unassigned	<b>Client (Respond Only)</b>
Unassigned	<b>Server (Request Security)</b>
Unassigned	<b>Secure Server (Require Security)</b>

**Assigned**      **Custom Policy 1**

**Key Exchange Settings:**

Master Key Perfect Forward Secrecy

Authenticate and generate a new key after every  minutes

Authenticate and generate a new key after every  sessions

Protect Identities with these security **methods**:

Security method preference order:

Type	Encryption	Integrity	Diffie-Hellman Group
IKE	▼ 3DES	▼ SHA1	▼ Medium (2)
IKE	▼ 3DES	▼ MD5	▼ Medium (2)
IKE	▼ DES	▼ SHA1	▼ Low (1)
IKE	▼ DES	▼ MD5	▼ Low (1)

### IP Security Rules (one or more Rules can be active *per policy*, notice the Checkboxes)

**Rule 1**

**IP Filter List TAB** (more than one filter list can exist, but only one filter list can be active *per Rule*)  
(Filter lists can contain combinations of Source/Destination IP addresses, Source Destination Subnets, and various *Protocols* [ICMP, TCP, UDP, RDP, EGP and others] at various *Ports*, and DNS names)

- Filter List 1 (Multiple entries can exist in the Filter List)  
i.e., TCP Port 25 Traffic from 130.156.16.0  
i.e., Any inbound traffic from subnet 209.69.7.0
- Filter List 2
- Filter List 3

**Authentication Preferences TAB**

Kerberos (Authentication Preference 1)      Authentication Preference Order (I can have >1 preference, but each preference can have only one Authentication method)

- Windows 2000 Default Kerberos V5
- Use a Certificate from this CA
- Use this string (Preshared Key)

Authentication Preference 2 (IF more than one Authentication Preference exists)

- Windows 2000 Default Kerberos V5
- Use a Certificate from this CA
- Use this string (Preshared Key)

Authentication Preference 2 (IF more than two Authentication Preferences exist)

- Windows 2000 Default Kerberos V5
- Use a Certificate from this CA
- Use this string (Preshared Key)

**Tunnel Setting TAB**

- This rule does not specify an IPSec Tunnel
- The tunnel endpoint is specified by this IP Address (w.x.y.z)

**Connection Type TAB**

- All network connections
- Local area network (LAN)
- Remote access

**Filter Action TAB** (Three Authentication Preferences exist by default)

- Permit
- Request Security (Optional)
- Require Security

(When a New Filter Action is made, the Radio Button Choices are:

- Permit
- Block
- Negotiate

(When Negotiate is chosen, one of three Radio Button choices must be made:

- High (ESP)
- Medium (AH)
- Custom (Several Custom options available)

Data and address integrity without encryption (AH)

- ▼ Integrity Algorithm (Pick one)
  - SHA1
  - MD5
- Data Integrity and Encryption (ESP) Algorithm
  - ▼ Integrity Algorithm (Pick one)
    - <None>
    - SHA1
    - MD5
  - ▼ Encryption Algorithm (Pick one)
    - <None>
    - 3DES
    - DES

Generate a new key every "x" Kbytes

Generate a new key every "x" seconds

**Rule 2**

**Rule 3**