

An Introduction to IPsec

Paul Asadoorian

IPsec: Friend or Foe?

"We strongly discourage the use of IPsec in its current form for protection of any kind of valuable information, and hope that future iterations of the design will be improved. However, we even more strongly discourage any current alternatives, and recommend IPsec when the alternative is an insecure network. Such are the realities of the world."

- Niels Ferguson and Bruce Schneier
Counterpane Internet Security, Inc.

Outline

- IPsec overview (Alphabet soup being served...)
- Security Associations (SA) & SPI's
- Authentication Header (AH) protocol
- Encapsulating Security Payload (ESP) protocol
- Internet Key Exchange (IKE)
- IPsec pitfalls
- IPsec vs tunneling (PPTP, L2TP)

VPN (Virtual Private Network)

- Secure communications between two hosts or networks
- VPN, the buzzword that solves all your problems
- Still a new technology
- IPsec is one of the more popular VPN technology's

Network Computing, Sept. 1999

- 37% were using it production environments
- 25% were in planning/testing phase
- 18% did not have any plans for IPsec

What can IPSEC do for me?

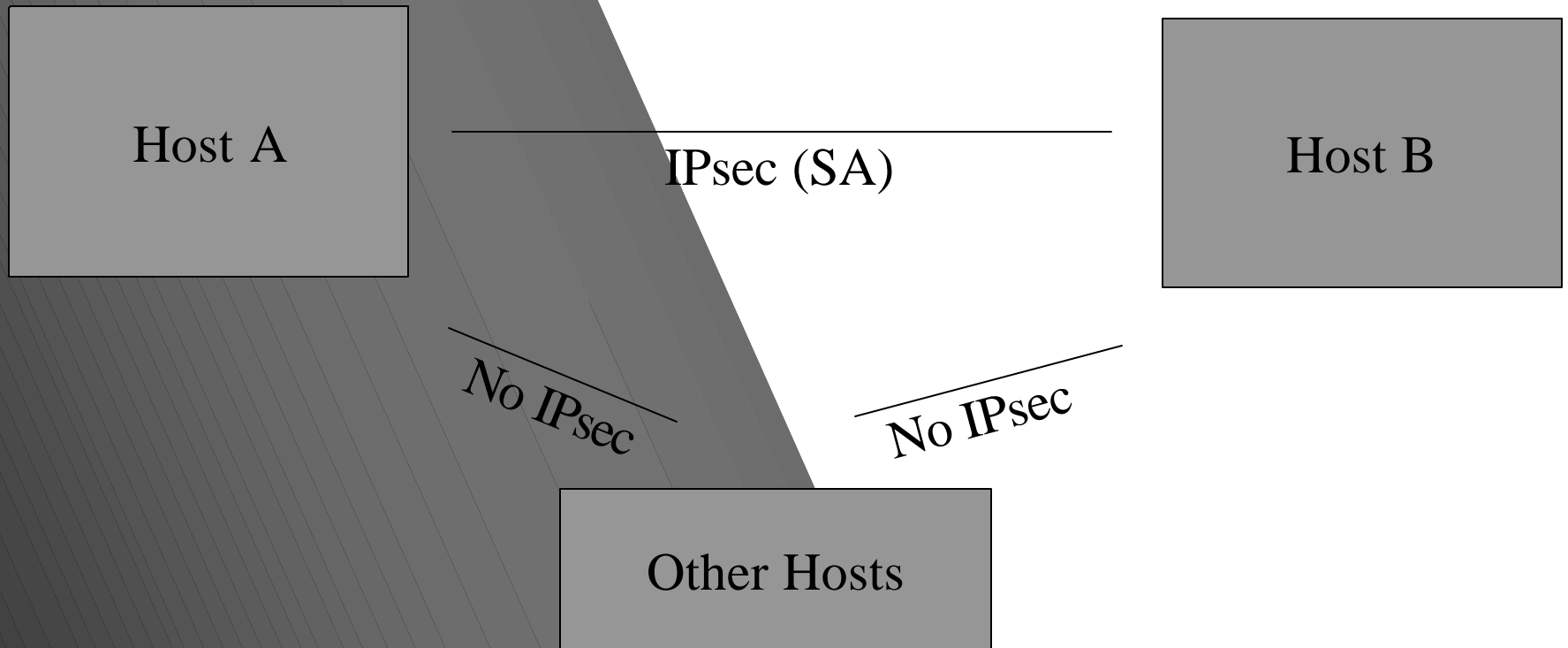
- Authentication
- Integrity
- Access control
- Confidentiality
- Replay protection (Partial)

Types of communications

- Host To Host
- Host To Security Gateway
- Security Gateway To Security Gateway
 - Security Gateway = Firewall
 - Also referred to as Network (i.e. Network To Network)

How does IPSEC work?

- Host To Host



Security Associations

- Stored in the SPD (Security Policy Database)
- Uniquely Identify IPsec sessions by:
 - SPI – Security Parameter Index, a unique number that identifies the session
 - The destination IP address
 - A security protocol (AH or ESP)

Security Associations

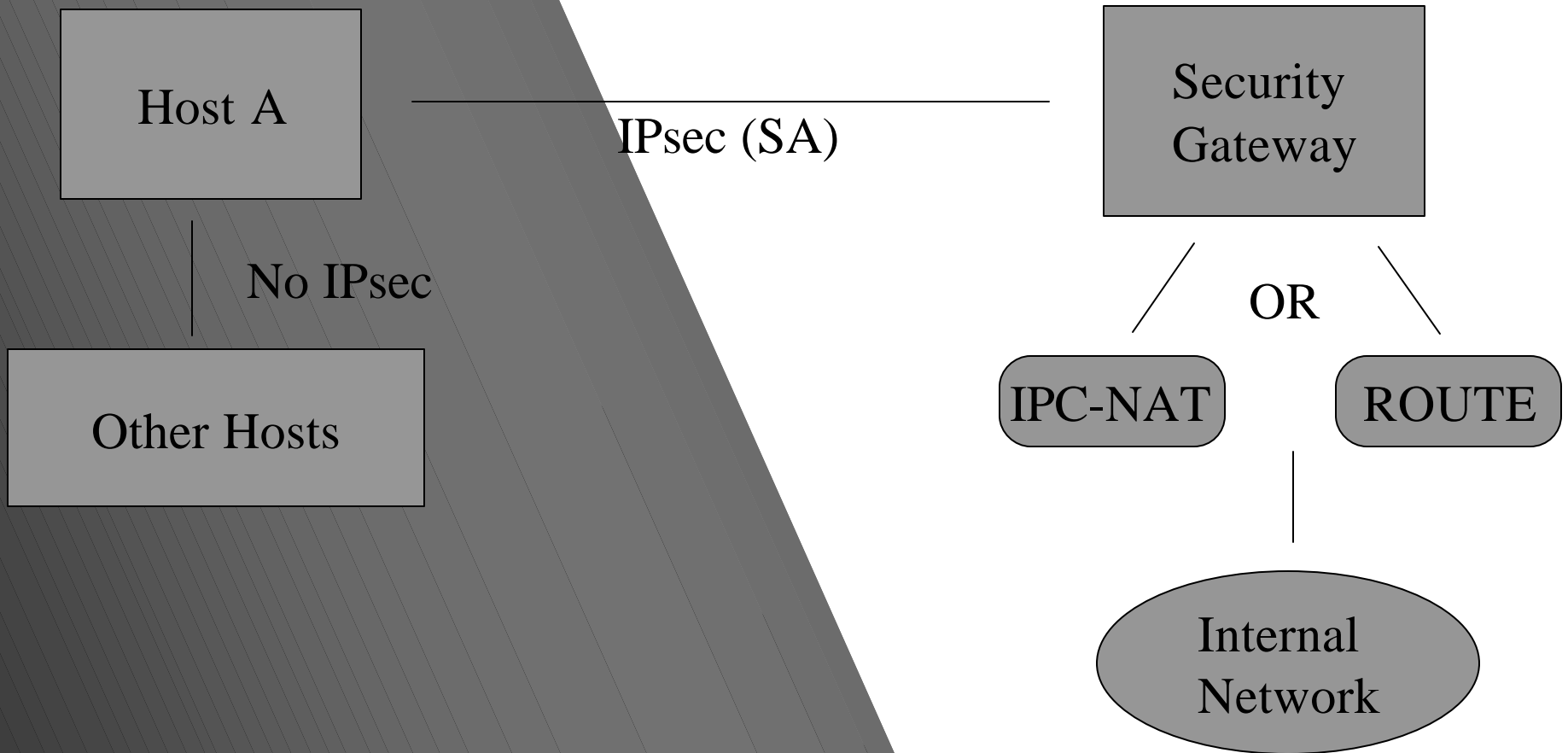
- **Host A Security Association:**

```
# ipsecadm new esp -spi 1000 -src HostA \  
-dst HostB -forcetunnel -enc 3des -auth sha1 \  
-key 7762d8707255d974168cbb1d274f8bed4cbd3364 \  
-authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

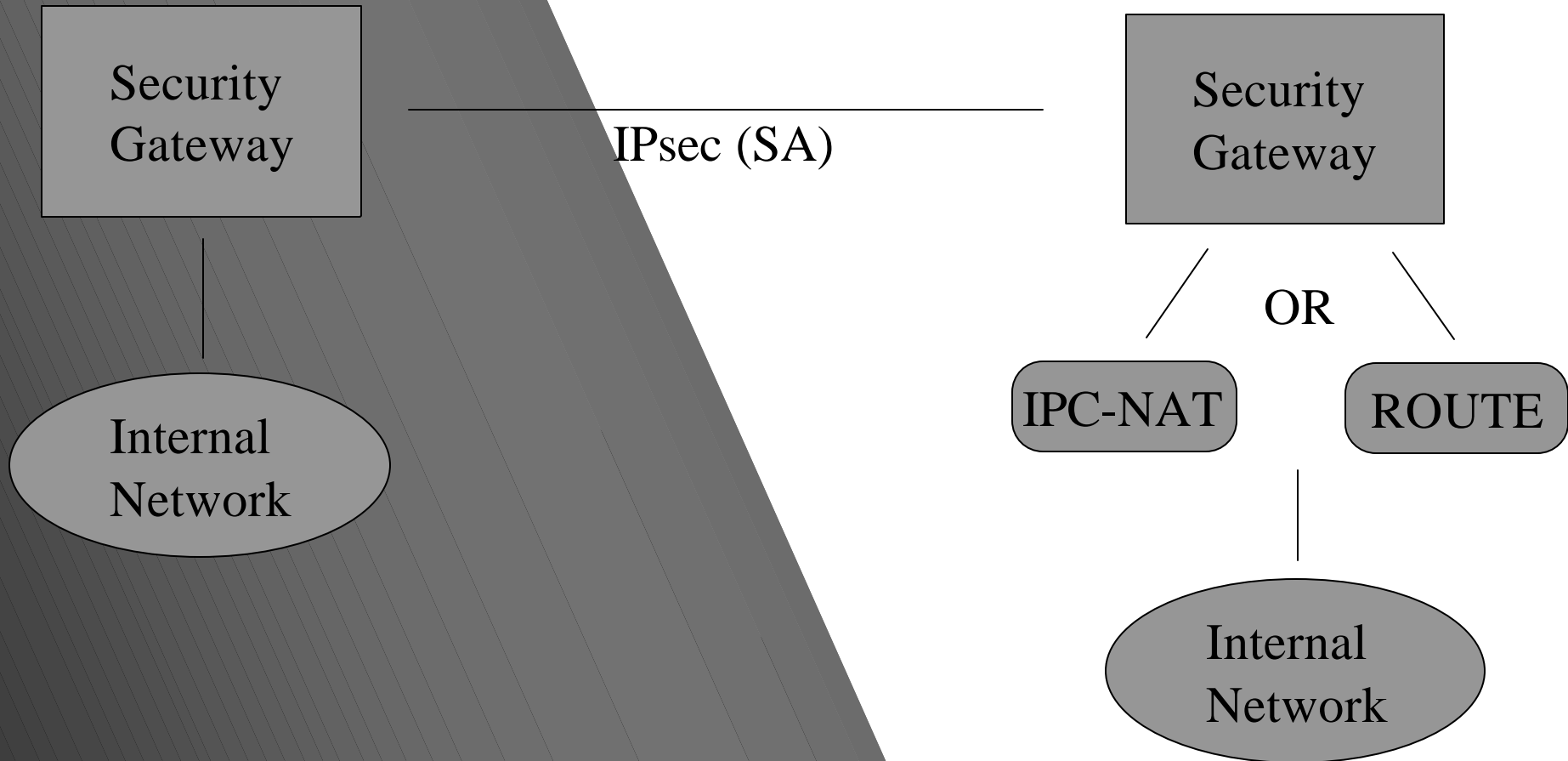
- **Host B Security Association:**

```
# ipsecadm new esp -spi 1001 -src HostB \  
-dst HostA -forcetunnel -enc 3des -auth sha1 \  
-key 7762d8707255d974168cbb1d274f8bed4cbd3364 \  
-authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

Host To Security Gateway



Security Gateway to Security Gateway



Types of IPSEC Connections

- Transport Mode
 - Does not encrypt the entire packet
 - Uses original IP Header
 - Faster
 - Counterpane recommends getting rid of it
- Tunnel Mode
 - Encrypts entire packet including IP Header (ESP)
 - Creates a new IP header
 - Slower

Normal TCP/IP Packet

Application Layers (5-7) / Data

TCP/UDP Header (Layer 4)

IP Header (Layer 3)

Frame Header (Layer 2)

OR

Frame Hdr

IP Hdr

TCP/UDP

Data

AH (Authentication Header)

- IP Protocol 51
- Provides authentication of packets
- Does not encrypt the payload

Transport Mode



Tunnel Mode



ESP (Encapsulating Security Payload)

- IP Protocol 50
- Encrypts the Payload
- Provides Encryption and Authentication

Transport Mode



Tunnel Mode



IKE (Internet Key Exchange)

- UDP port 500
- Negotiates connection parameters
- ISAKMP (Internet Security Association and Key Management Protocol)
- Oakley (Diffie-Helmen key exchange)

IKE Negotiation

- Two phases
 - Phase 1 – Negotiate two way SA's
 - Uses certificates or Pre-Shared Secrets
 - Main Mode or Aggressive Mode
 - Phase 2 – Negotiate IPSEC (AH, ESP, Tunnel, Transport)
 - How shall I encrypt you data today?
 - Always Uses Quick mode because we are already authenticated

IKE Negotiation

- Negotiates the following parameters:
 - SA lifetime
 - Encryption Algorithm (NEVER USE DES, USE 3DES)
 - Authentication Algorithm (MD5, SHA, SHA-1)
 - Type of Key Exchange

Remember:

```
# ipsecadm new esp -spi 1000 -src HostA \  
-dst HostB -forcetunnel -enc 3des -auth sha1 \  
-key 7762d8707255d974168cbb1d274f8bed4cbd3364 \  
-authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

IPSec Example

- ESP Only (demo only)
- Two hosts on the same network:
 - Jerry 192.168.0.11 - OpenBSD 2.8
 - Tom 192.168.0.17 – OpenBSD 2.7
- Why OpenBSD?
 - Good implementation and documentation

Jerry Configuration (192.168.0.11)

```
ipsecadm new esp -spi 1000 -src 192.168.0.11 -dst 192.168.0.17 -forcetunnel \  
enc blf -auth sha1 -key b4bc9f7f37d09332ac95dd32223e685fe6aaa026 \  
authkey d041653ae78a9fa5ca795df2a051102ec30b33aa
```

```
ipsecadm new esp -spi 1001 -src 192.168.0.11 -dst 192.168.0.17 -forcetunnel \  
enc blf -auth sha1 -key b4bc9f7f37d09332ac95dd32223e685fe6aaa026 \  
authkey d041653ae78a9fa5ca795df2a051102ec30b33aa
```

```
ipsecadm flow -proto esp -dst 192.168.0.17 -addr 192.168.0.11 255.255.255.255 \  
192.168.0.17 255.255.255.255 -proto esp -acquire
```

Encap:

Source	Port	Destination	Port	Proto	SA(Addr/Proto/Type/Direction)
192.168.0.11/32	0	192.168.0.17/32	0	0	192.168.0.17/50/acquire/out

Tom Configuration

(192.168.0.17)

```
ipsecadm new esp -spi 1001 -src 192.168.0.17 -dst 192.168.0.11 -forcetunnel \  
-enc blf -auth sha1 -key b4bc9f7f37d09332ac95dd32223e685fe6aaa026 \  
-authkey d041653ae78a9fa5ca795df2a051102ec30b33aa
```

```
ipsecadm new esp -spi 1000 -src 192.168.0.17 -dst 192.168.0.11 -forcetunnel \  
-enc blf -auth sha1 -key b4bc9f7f37d09332ac95dd32223e685fe6aaa026 \  
-authkey d041653ae78a9fa5ca795df2a051102ec30b33aa
```

```
ipsecadm flow -proto esp -dst 192.168.0.11 -spi 1001 -addr 192.168.0.17  
255.255.255.255 192.168.0.11 255.255.255.255
```

Encap:

Source	Port	Destination	Port	Proto	SA(Address/SPI/Proto)
192.168.0.17/32	0	192.168.0.11/32	0	0	192.168.0.11/00001001/50

Packets Before

ICMP

```
12:46:21.545929 192.168.0.11 > 192.168.0.17: icmp: echo request (ttl 255, id 29731)
0000: 4500 0054 7423 0000 ff01 c618 c0a8 000b E..Tt#.....
0010: c0a8 0011 0800 09d8 9d66 0000 3b6d 104f .....f.;m.O
0020: 0008 19fa 0809 0a0b 0c0d 0e0f 1011 1213 .....
0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 ..... !"#
0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0050: 3435                                     45
```

FTP

```
12:47:42.431056 192.168.0.11.42261 > 192.168.0.17.21: P [tcp sum ok] 13:28(15) ack 98
win 17232 <nop,nop,timestamp 9663 9697> [tos 0x10] (ttl 64, id 44333)
0000: 4510 0043 ad2d 0000 4006 4c0b c0a8 000b E..C-..@.L.....
0010: c0a8 0011 a515 0015 5062 b4c2 5d0f 41e7 .....Pb..].A.
0020: 8018 4350 a693 0000 0101 080a 0000 25bf ..CP.....%.
0030: 0000 25e1 5041 5353 2070 6173 7377 6f72 ..%.PASS passwor
0040: 640d 0a                                     d..
```

Packets After

MP

```
:51:58.736930 esp 192.168.0.11 > 192.168.0.17 spi 0x00001001 seq 1 len 116 (ttl 64, id 16933)
0000: 4500 0088 4225 0000 4032 b6b2 c0a8 000b  E...B%..@2.....
0010: c0a8 0011 0000 1001 0000 0001 b5c1 1de8  .....
0020: 9e67 4463 cab1 f496 2970 e7d9 267c 0cef  .gDc....)p..&|..
0030: 6bfc a5d6 6f6a 9f51 0e95 20fe c930 0e77  k...oj.Q.. ..0.w
0040: 2918 6c92 d7ac 6c13 f9f1 de8b 1674 fd42  ).l...l.....t.B
0050: be98 4a40 29e8 9ecb 6759 cfbe 993d 1001  ..J@)...gY...=..
0060: 0f11 0b8b 5e93 8852 dc28 786b 2479 465d  ....^..R.(xk$yF]
0070: 5a67 d503 6b51 ff0b 074c 0076 6d03 a1ec  Zg..kQ...L.vm...
0080: 5b14 765f cb06 51f8                               [.v_..Q.
```

TP

```
:52:29.730868 esp 192.168.0.11 > 192.168.0.17 spi 0x00001001 seq 2 len 100 (ttl 64, id 28675)
0000: 4500 0078 7003 0000 4032 88e4 c0a8 000b  E..xp...@2.....
0010: c0a8 0011 0000 1001 0000 0002 6b51 ff0b  .....kQ..
0020: 074c 0076 30fa 28c7 ef53 592a 7b13 a068  .L.v0(..SY*{.h
0030: 06bf 071d 81a0 98de ddd8 0174 b637 2b9a  .....t.7+.
0040: f1d2 a36e d83a 08ec 59bf 5341 a4b3 7ae5  ...n:...Y.SA..z.
0050: bbc3 000b d2b1 e93c e086 cf69 71d6 dcf5  .....<...iq...
0060: 8498 13d7 8930 2451 f43b b6fc 4abc da2c  ....0$Q.;..J.,
0070: 77c5 01dd cb2a bc11                               W
```

IPsec Pitfalls

- Too complicated, many different ways to configure
- Can be configured insecurely
- Client security is an issue
- Performance in IPv4 implementation (Especially a BITS)

Advantages of IPSec over SSL/TLS

- Encrypts the entire packet, including IP Header (not just layer 4 and higher)
- Can Encrypt any protocol
- No Impact on users when using SG to SG
- Acts independent of IP address

IPsec Guidelines

- Always use:
 - 3des or blowfish
 - SHA1 over SHA and MD5
 - NEVER USE DES
 - Tunnel Mode
 - Main Mode
 - AH and ESP together
 - Certificates for production environments

OS Support for IPsec

- OpenBSD, FreeBSD, NetBSD
- Linux
- Solaris
- Windows 2000 (Native)
- Windows NT/95/98/Me (Add-on)
- Cisco IOS (PIX and Routers)
- Others as well....

Links

<http://www.openbsd.org/faq/faq13.html> – OpenBSD Doc

<http://www.freeswan.org/> – Linux IPsec Support

<http://www.ietf.org/html.charters/ipsec-charter.html> – All RFC's & Drafts

<http://www.cisco.com/warp/public/105/IPSECpart1.html> – Intro from Cisco

<http://www.counterpane.com/ipsec.pdf> – An eval of IPsec