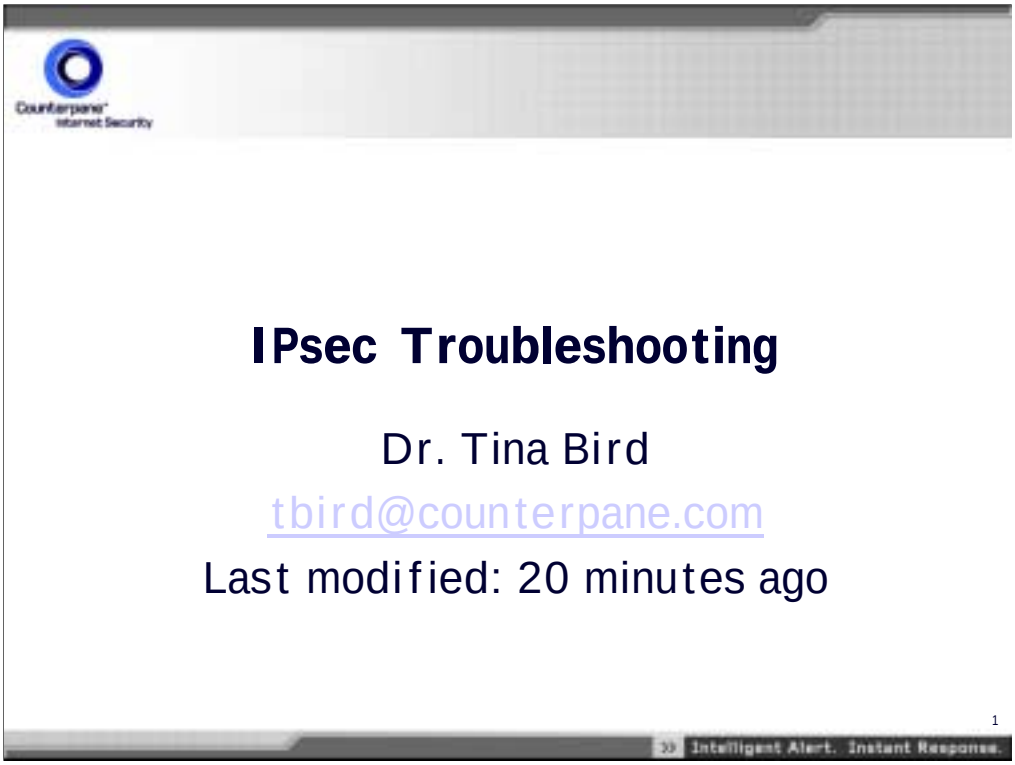

Counterpane
Internet Security
IPsec Troubleshooting
Dr. Tina Bird
tbird@counterpane.com
Last modified: 20 minutes ago
1
Intelligent Alert. Instant Response.

Agenda

- Building an IPsec Connection
- Troubleshooting
- Known Issues

Building a VPN connection

- Initial connection request between remote and local machine
- Authentication process -- may include Diffie-Hellman exchange, strong user authentication, certificate verification
- Negotiation of session keys and other network characteristics

Building a VPN connection cont.

- Establishment of encrypted connection between local and remote machines
- Data transport between local and remote machines or networks -- HTTP, FTP, *telnet,* NFS, SMB, etc.

Building an IPsec Connection

- Initial connection request (IKE Phase One, Main Mode or Aggressive Mode): verifies machine identities, user authentication if required, keys for Phase Two if required

Building an IPsec Connection cont.

- Initial connection request between remote and local machine – IKE Phase 1

192.168.30.57.500 > 192.168.167.40.500: udp 990 (ttl 128, id 37896)

192.168.30.57.500 > 192.168.167.40.500: udp 92 (ttl 128, id 38152)

Building an IPsec Connection cont.

- Authentication process – LDAP certificate exchange

192.168.30.57.1038 > 192.168.174.40.389: s 395784:395784(0) win …..

192.168.174.40.389 > 192.168.30.57.1038: s 1757781809:1757781809(0) ack 395785 win…..

Building an IPsec Connection cont.

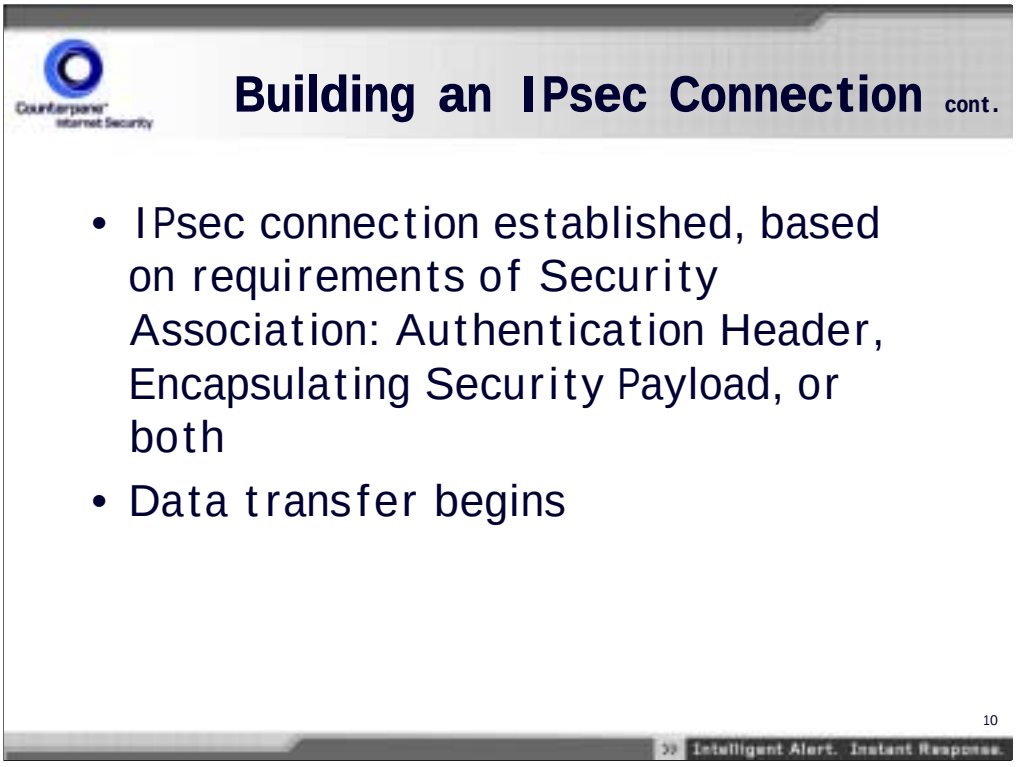
- IKE Phase Two, Quick Mode: establishes *Security Association*, including
  - IPsec protocol
  - encryption & packet authentication algorithms
  - keys for bulk data transfer
  - session lifetime

Building an IPsec Connection cont.

- Negotiation of session keys and other network characteristics – IKE Phase 2

192.168.30.57.500 > 192.168.167.40.500: udp 990 (ttl 128, id 39323)

192.168.30.57.500 > 192.168.167.40.500: udp 92 (ttl 128, id 3958)


Counterpane Internet Security
Building an IPsec Connection cont.
• IPsec connection established, based on requirements of Security Association: Authentication Header, Encapsulating Security Payload, or both
• Data transfer begins
10
Intelligent Alert. Instant Response.

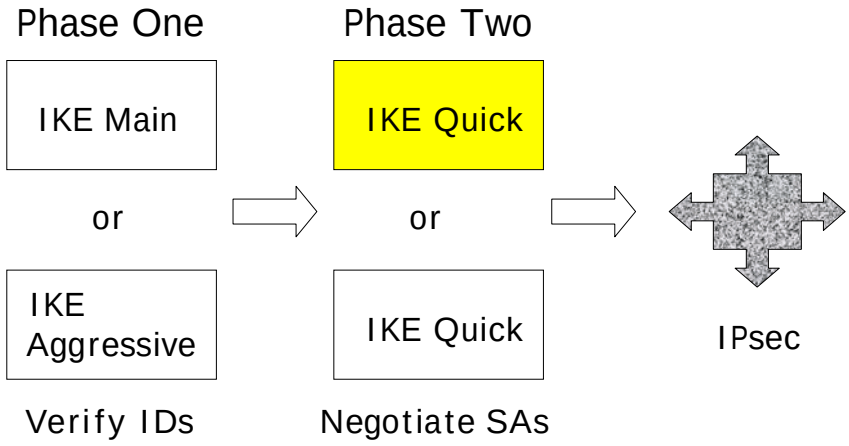
Building an IPsec Connection cont.

- Data transport between local and remote machines or networks

192.168.30.57 > 192.168.167.40: ip-proto-50 132 (ttl 128, id 32522)

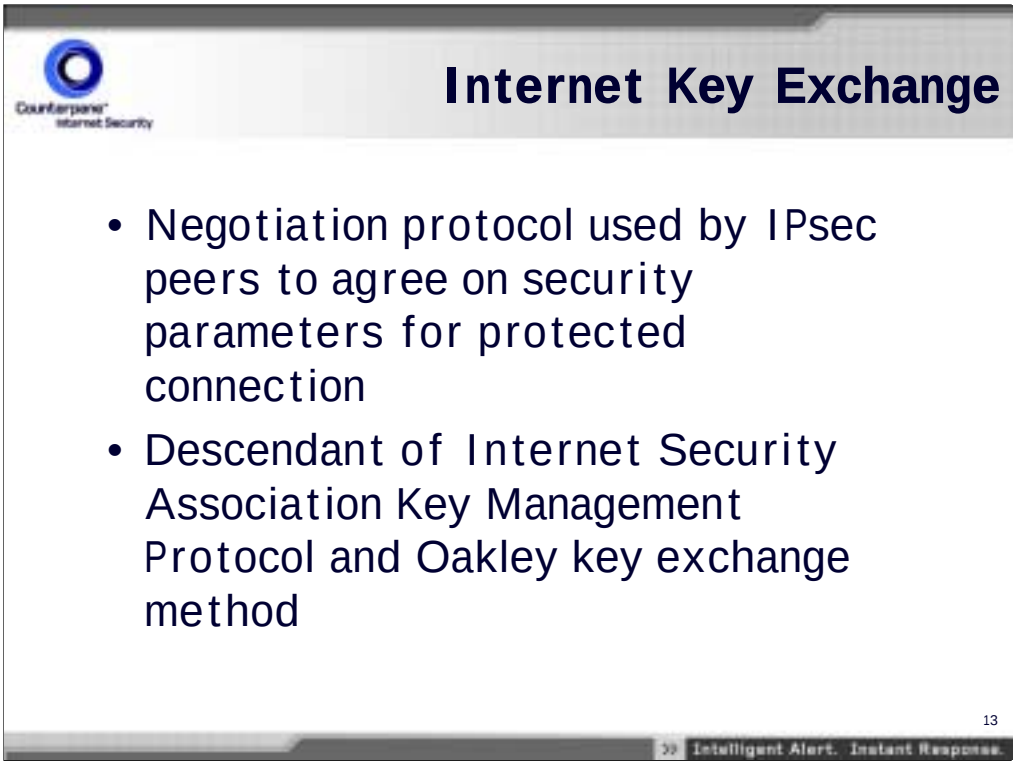
192.168.30.57 > 192.168.167.40: ip-proto-50 132 (ttl 128, id 32778)

IPsec Connection



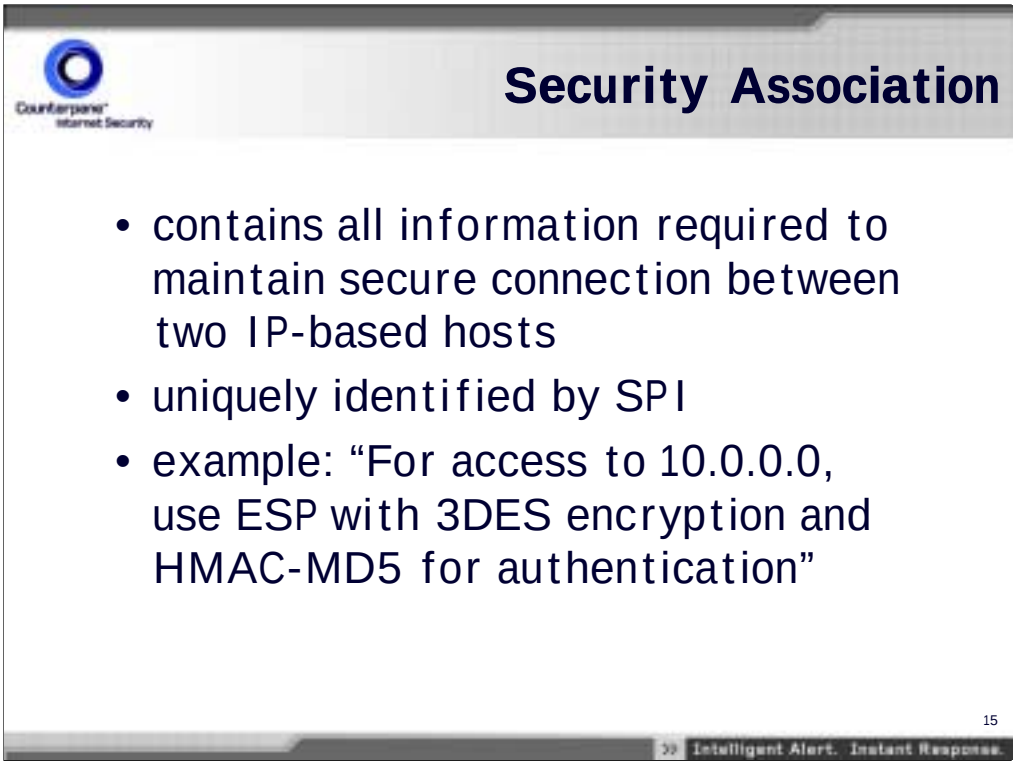
12

Intelligent Alert. Instant Response.


Internet Key Exchange
Negotiation protocol used by IPsec peers to agree on security parameters for protected connection
Descendant of Internet Security Association Key Management Protocol and Oakley key exchange method
13
Intelligent Alert. Instant Response.

Internet Key Exchange cont.

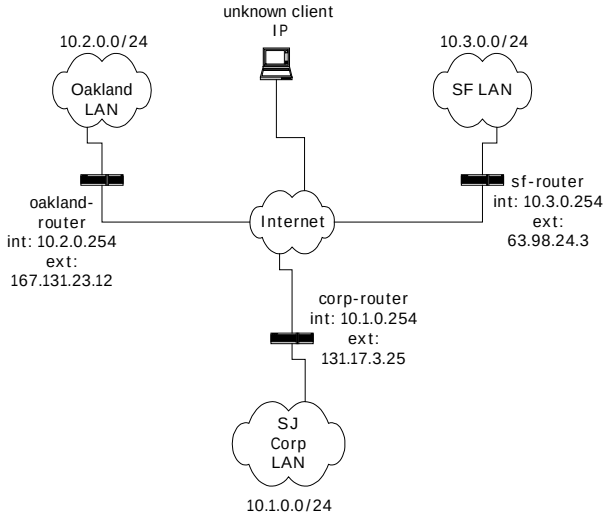
- IKE uses UDP/500.
- Phase One – authenticates sources and destination and establishes a secure channel (if required) to perform SA negotiations
- Phase Two -- negotiates SA


Counterpane
Internet Security
Security Association
• contains all information required to maintain secure connection between two IP-based hosts
• uniquely identified by SPI
• example: “For access to 10.0.0.0, use ESP with 3DES encryption and HMAC-MD5 for authentication”
15
Intelligent Alert. Instant Response.

Security Association cont.

- Two SAs required for each network connection, one per IPsec peer (or one inbound, one outbound)
- Active SAs stored in *Security Association Database* on each peer

Cisco-based VPN



17

Cisco-based VPN cont.

- Determine IPsec parameters
  - Security parameters
  - Gateway addresses
  - Pre-shared secrets (host authentication)
  - Access control lists (control routing)
- Configure security policy on routers
- Apply crypto policy to appropriate interfaces on routers

Cisco-based VPN cont.

- IPsec parameters
  - ESP only, tunnel mode for LAN-to-LAN connections
  - 3DES encryption, SHA for hash
- sj-router is endpoint of all connections (star configuration)

Cisco-based VPN cont.

Define ISAKMP policy for each set of connections:

```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key secretkey
   address 167.131.23.12
```

Cisco-based VPN cont.

Establish IPsec security parameters:

```
crypto ipsec transform-set
   config esp-3des esp-sha-
hmac
```

Cisco-based VPN cont.

Create crypto map entries on all routers:

- Determine which traffic needs IPsec
- Determine local and remote VPN endpoints
- etc.

Cisco-based VPN cont.

Create a static crypto map between sj-router and the gateways at the remote offices:

```
crypto map sj-oakland 1 ipsec-isakmp
set peer 167.131.23.12
set transform-set config
match address 100
```

Cisco-based VPN cont.

Symmetric map on oakland-router:

```
crypto map oakland-sj 1 ipsec-
  isakmp
  set peer 131.17.3.25
  set transform-set config
  match address 100
```

Cisco-based VPN cont.

VPN Access Control Lists determine which traffic is routed over the IPsec connection:

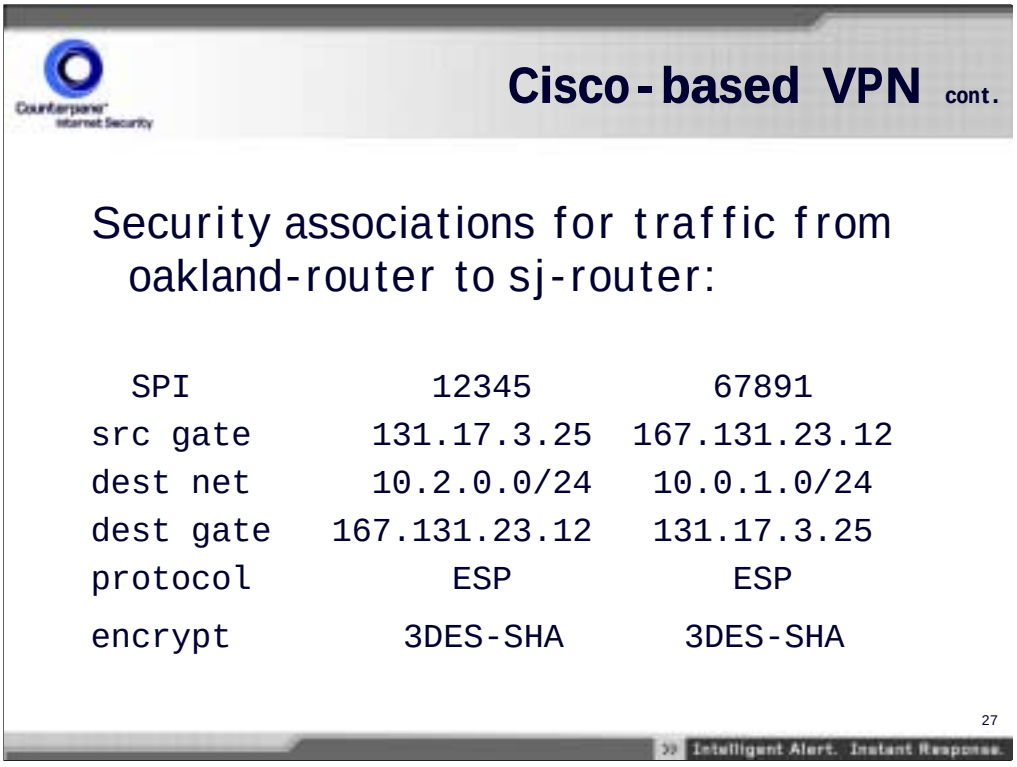
```
access-list 100 permit ip 10.1.0.0
  0.0.255.255 10.2.0.0 0.0.255.255
```

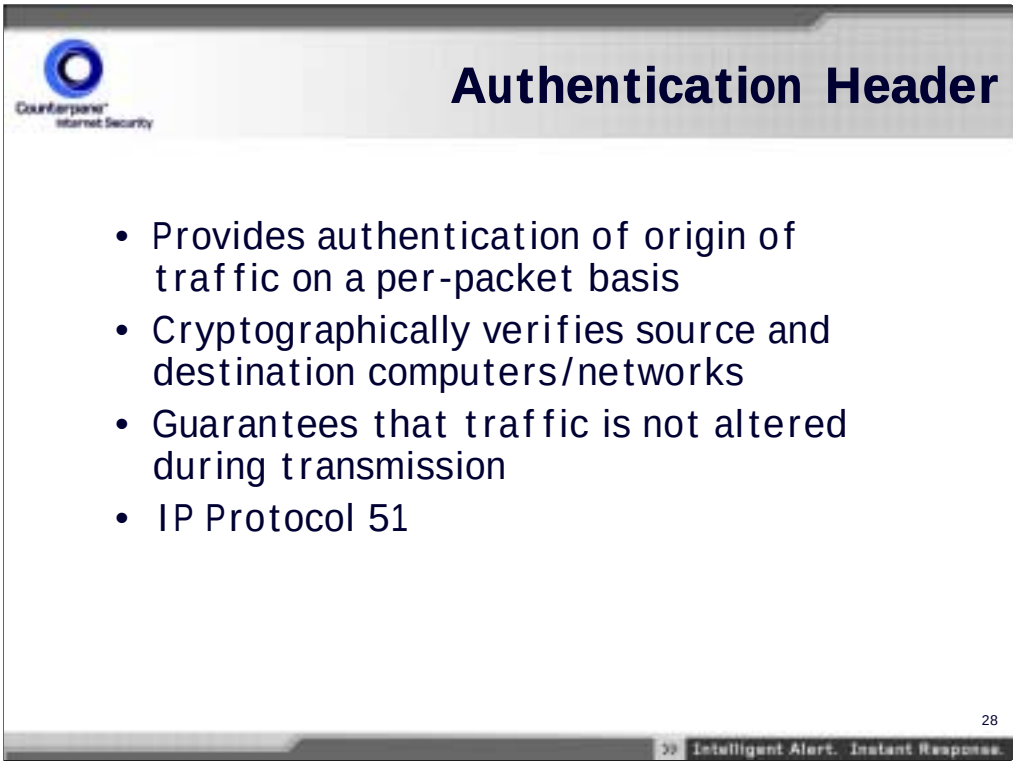
for SJ-to-Oakland traffic.

Cisco-based VPN cont.

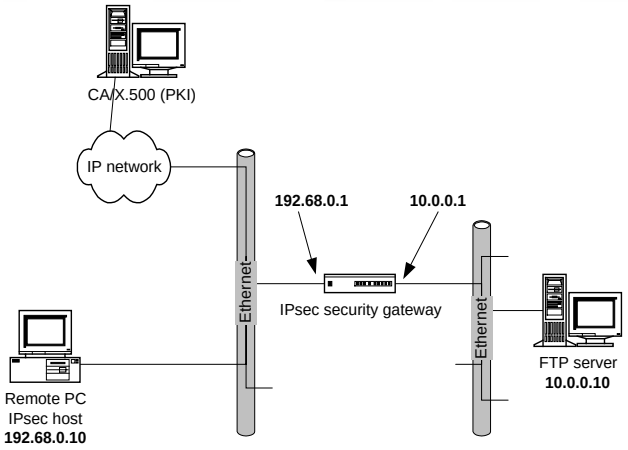
Security associations for traffic from sj-router to oakland-router:

SPI	12345	67891
src gate	131.17.3.25	167.131.23.12
dest net	10.2.0.0/24	10.0.1.0/24
dest gate	167.131.23.12	131.17.3.25
protocol	ESP	ESP
encrypt	3DES-SHA	3DES-SHA


Counterpane Internet Security
Cisco-based VPN cont.
Security associations for traffic from oakland-router to sj-router:
SPI 12345 67891
src gate 131.17.3.25 167.131.23.12
dest net 10.2.0.0/24 10.0.1.0/24
dest gate 167.131.23.12 131.17.3.25
protocol ESP ESP
encrypt 3DES-SHA 3DES-SHA
27
Intelligent Alert. Instant Response.

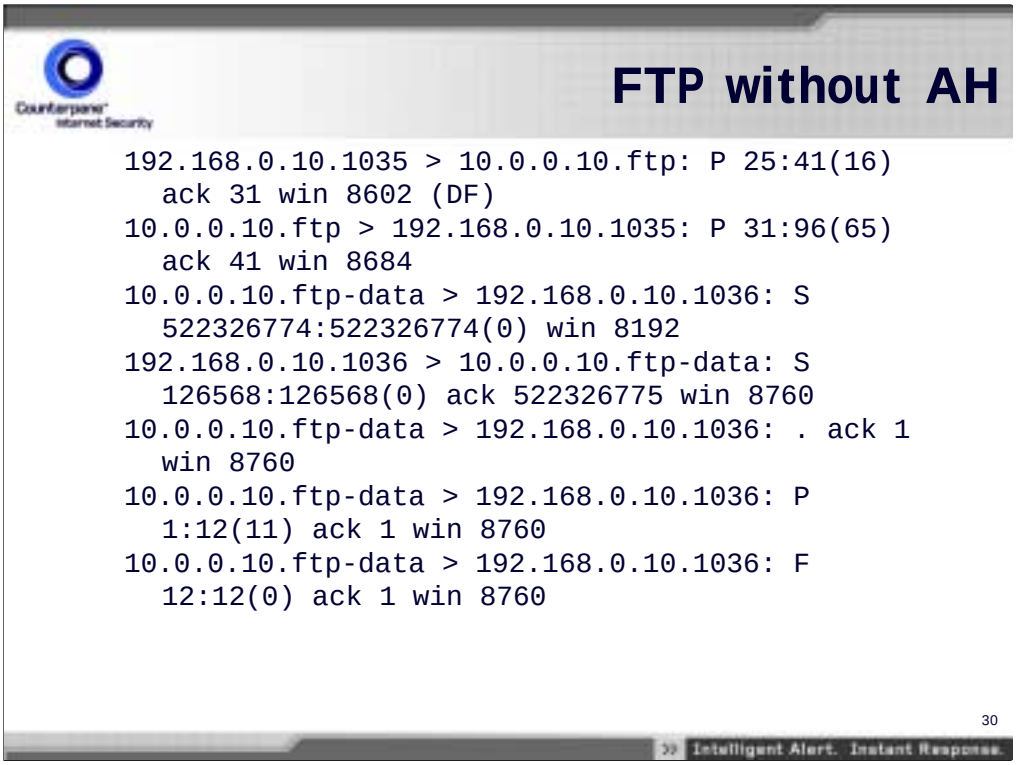

Counterpane Internet Security
Authentication Header
• Provides authentication of origin of traffic on a per-packet basis
• Cryptographically verifies source and destination computers/networks
• Guarantees that traffic is not altered during transmission
• IP Protocol 51
28
Intelligent Alert. Instant Response.

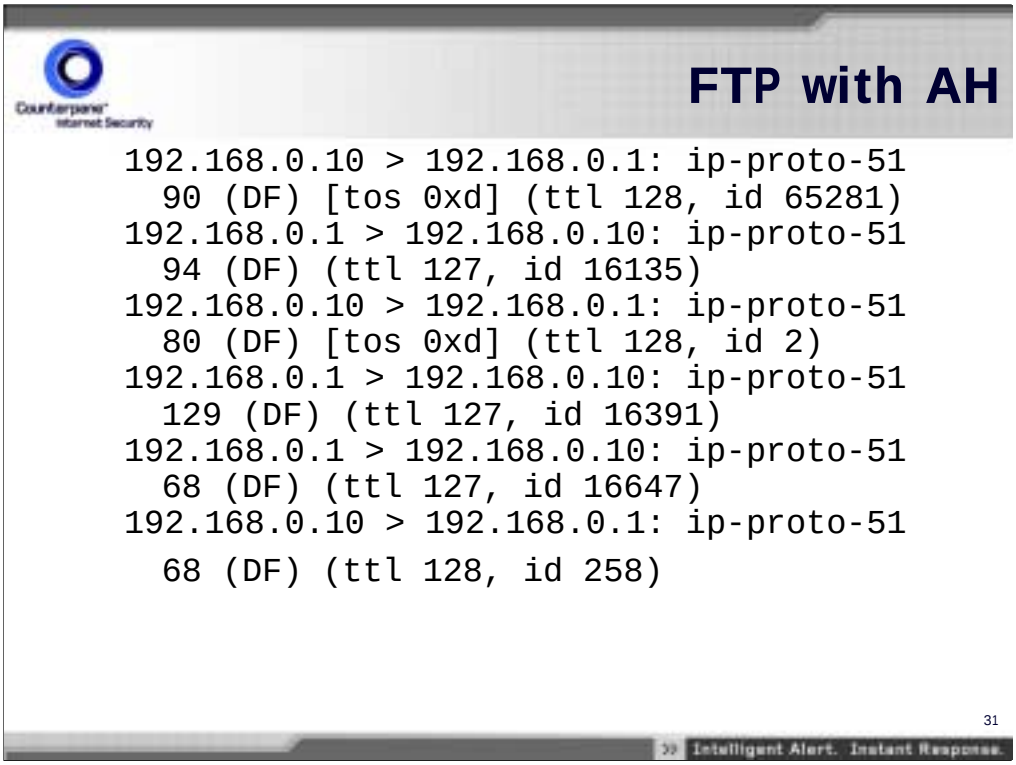
IPsec Sample Configuration

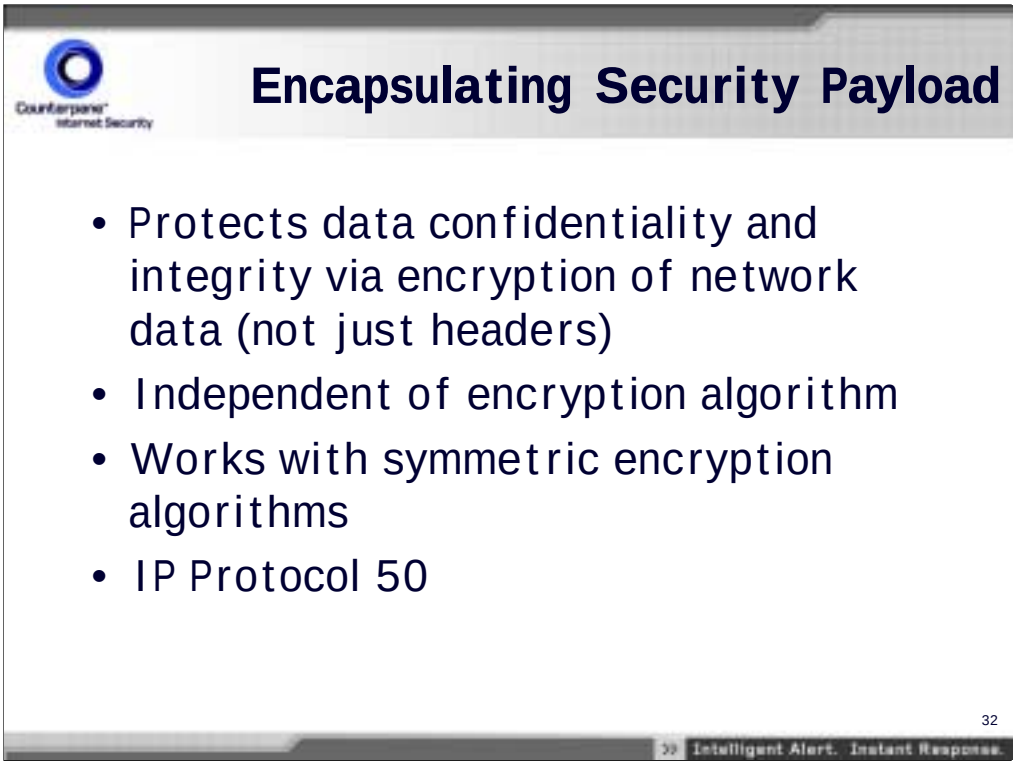


29

Intelligent Alert. Instant Response.


Counterpane
Internet Security
FTP without AH
192.168.0.10.1035 > 10.0.0.10.ftp: P 25:41(16)
ack 31 win 8602 (DF)
10.0.0.10.ftp > 192.168.0.10.1035: P 31:96(65)
ack 41 win 8684
10.0.0.10.ftp-data > 192.168.0.10.1036: S
522326774:522326774(0) win 8192
192.168.0.10.1036 > 10.0.0.10.ftp-data: S
126568:126568(0) ack 522326775 win 8760
10.0.0.10.ftp-data > 192.168.0.10.1036: . ack 1
win 8760
10.0.0.10.ftp-data > 192.168.0.10.1036: P
1:12(11) ack 1 win 8760
10.0.0.10.ftp-data > 192.168.0.10.1036: F
12:12(0) ack 1 win 8760
30
Intelligent Alert. Instant Response.


FTP with AH
192.168.0.10 > 192.168.0.1: ip-proto-51
90 (DF) [tos 0xd] (ttl 128, id 65281)
192.168.0.1 > 192.168.0.10: ip-proto-51
94 (DF) (ttl 127, id 16135)
192.168.0.10 > 192.168.0.1: ip-proto-51
80 (DF) [tos 0xd] (ttl 128, id 2)
192.168.0.1 > 192.168.0.10: ip-proto-51
129 (DF) (ttl 127, id 16391)
192.168.0.1 > 192.168.0.10: ip-proto-51
68 (DF) (ttl 127, id 16647)
192.168.0.10 > 192.168.0.1: ip-proto-51
68 (DF) (ttl 128, id 258)
31
Intelligent Alert. Instant Response.


Encapsulating Security Payload
• Protects data confidentiality and integrity via encryption of network data (not just headers)
• Independent of encryption algorithm
• Works with symmetric encryption algorithms
• IP Protocol 50
32
Intelligent Alert. Instant Response.

FTP with ESP

```
192.168.0.10 > 192.168.0.1: ip-proto-50
  88 (DF) [tos 0xd] (ttl 128, id 52740)
192.168.0.1 > 192.168.0.10: ip-proto-50
  88 (DF) (ttl 127, id 37383)
192.168.0.10 > 192.168.0.1: ip-proto-50
  80 (DF) [tos 0xd] (ttl 128, id 52996)
192.168.0.1 > 192.168.0.10: ip-proto-50
  128 (DF) (ttl 127, id 37639)
192.168.0.1 > 192.168.0.10: ip-proto-50
  64 (DF) (ttl 127, id 37895)
192.168.0.10 > 192.168.0.1: ip-proto-50
  64 (DF) (ttl 128, id 53252)
```

IPsec Troubleshooting

Be sure that each segment functions individually before testing complete IPsec system

IPsec Troubleshooting cont.

- Verify connectivity between remote machine and local VPN gateway
- Verify connectivity between local gateway and local network
  - Do you have to configure VPN server as a router explicitly?
- *ping, traceroute, netstat* to check connectivity

IPsec Troubleshooting cont.

Key negotiation failures

- Verify connectivity to Internet Key Exchange server (IKE)
- UDP/500
- Verify that remote machine is sending IKE traffic on *source port 500*
- NAT, port translation at perimeter problematic

IPsec Troubleshooting cont.

- Both IPsec gateways must be able to agree on security parameters
- Compare Security Policy Databases on both ends to be sure encryption/hash algorithms, authentication mechanisms, lifetimes compatible
- NO_PROPOSAL_CHOSEN

IPsec Troubleshooting cont.

- ISAKMP error: no common policy --

*Mar 1 00:34:06.187: ISAKMP (17): SA not acceptable!

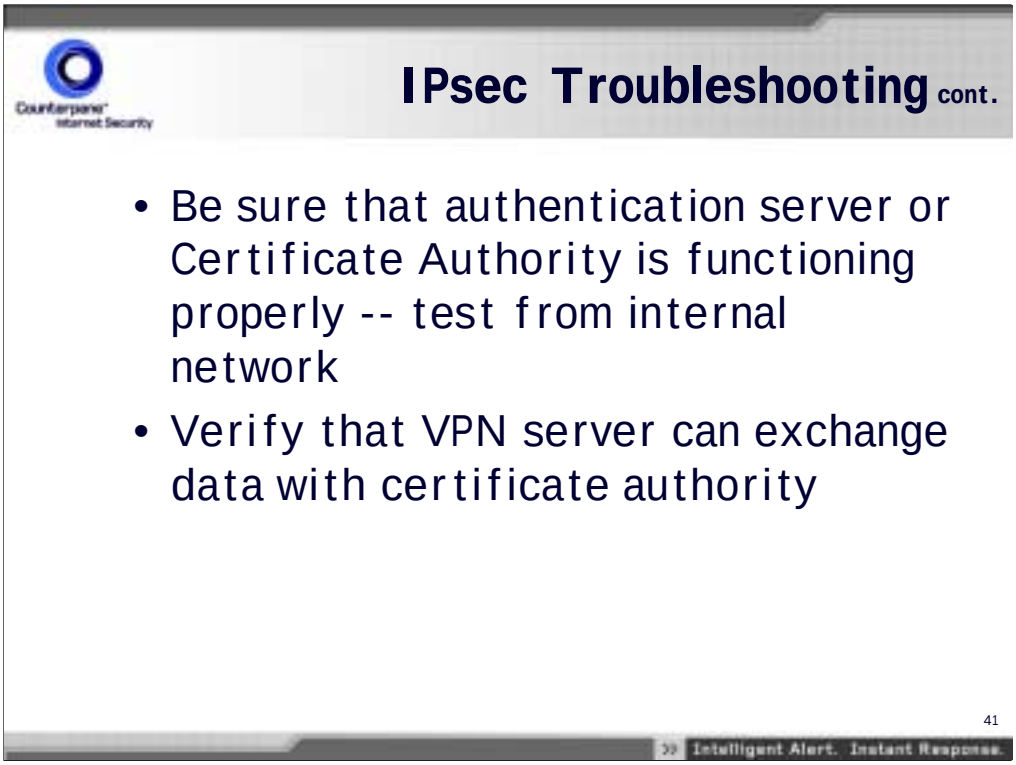
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed with peer at 20.20.20.20

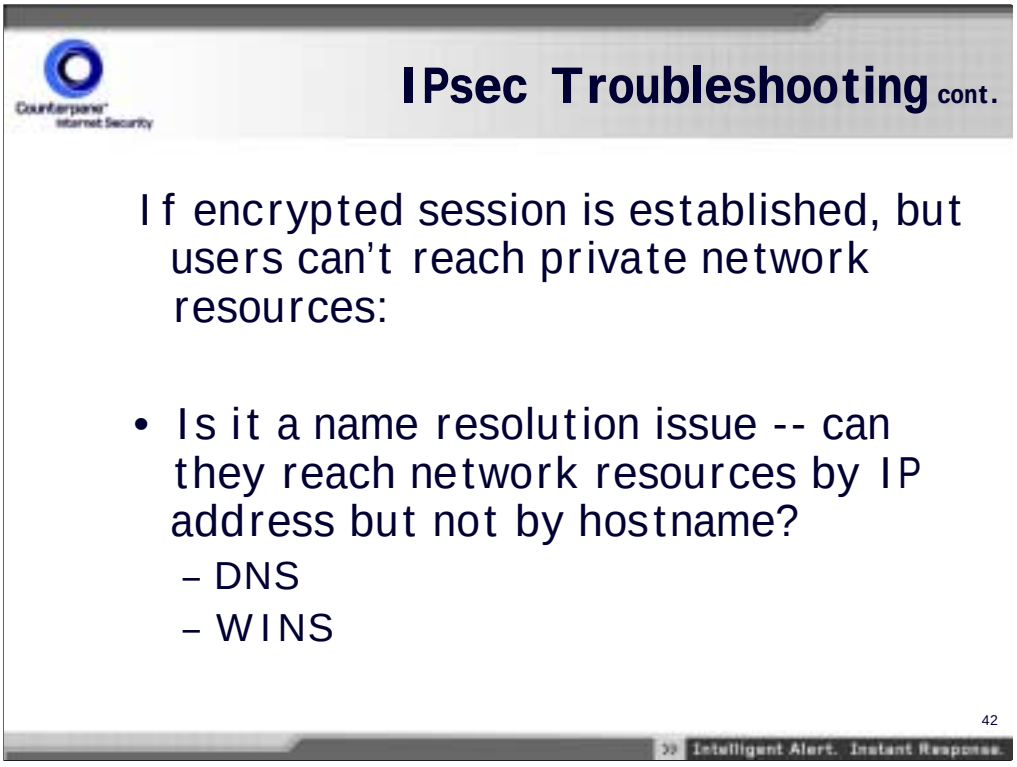
IPsec Troubleshooting cont.

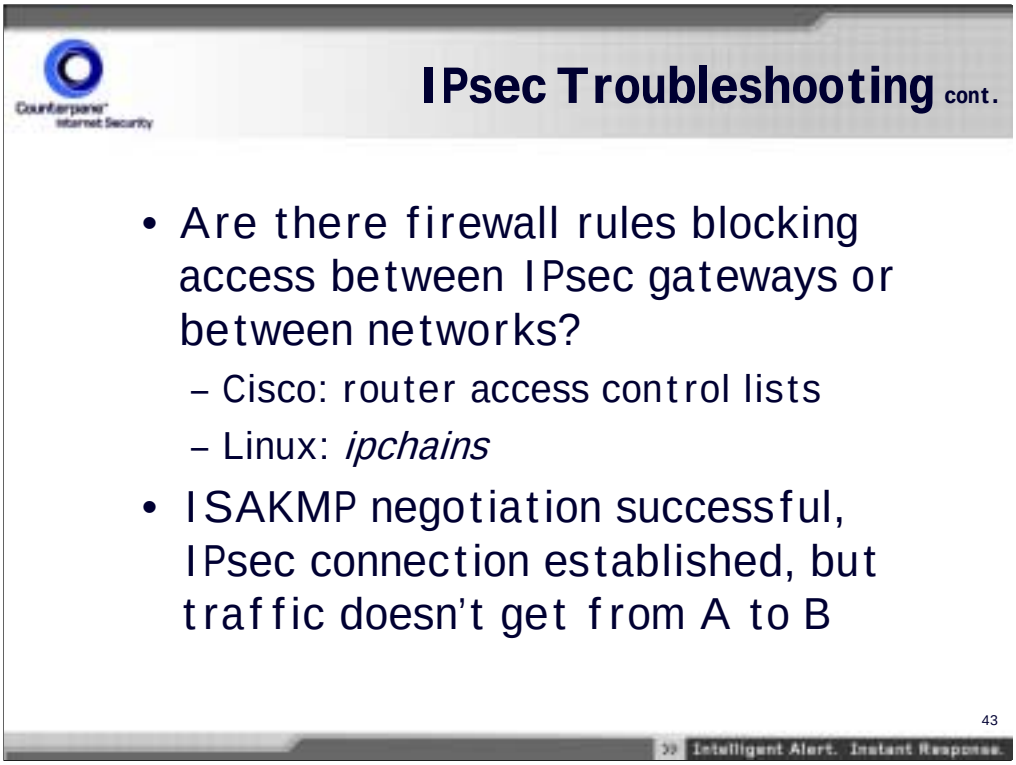
- ISAKMP error: CERT-TYPE-UNSUPPORTED
- IPsec gateway cannot understand encoding of certificate received from remote peer

IPsec Troubleshooting cont.

- ISAKMP error: AUTHENTICATION-FAILED
- IPsec gateway failed to verify the identity of a remote peer
- Check that auth server is includes both IPsec gateways in authentication database, have valid certs, or pre-shared secrets are the same


IPsec Troubleshooting cont.
• Be sure that authentication server or Certificate Authority is functioning properly -- test from internal network
• Verify that VPN server can exchange data with certificate authority
41
Intelligent Alert. Instant Response.


Counterpane Internet Security
IPsec Troubleshooting cont.
If encrypted session is established, but users can't reach private network resources:
• Is it a name resolution issue -- can they reach network resources by IP address but not by hostname?
– DNS
– WINS
42
Intelligent Alert. Instant Response.


IPsec Troubleshooting cont.
• Are there firewall rules blocking access between IPsec gateways or between networks?
– Cisco: router access control lists
– Linux: *ipchains*
• ISAKMP negotiation successful, IPsec connection established, but traffic doesn't get from A to B
43
Intelligent Alert. Instant Response.

IPsec Troubleshooting cont.

If encrypted session is established, but times out after a predictable period of time (3600 sec):

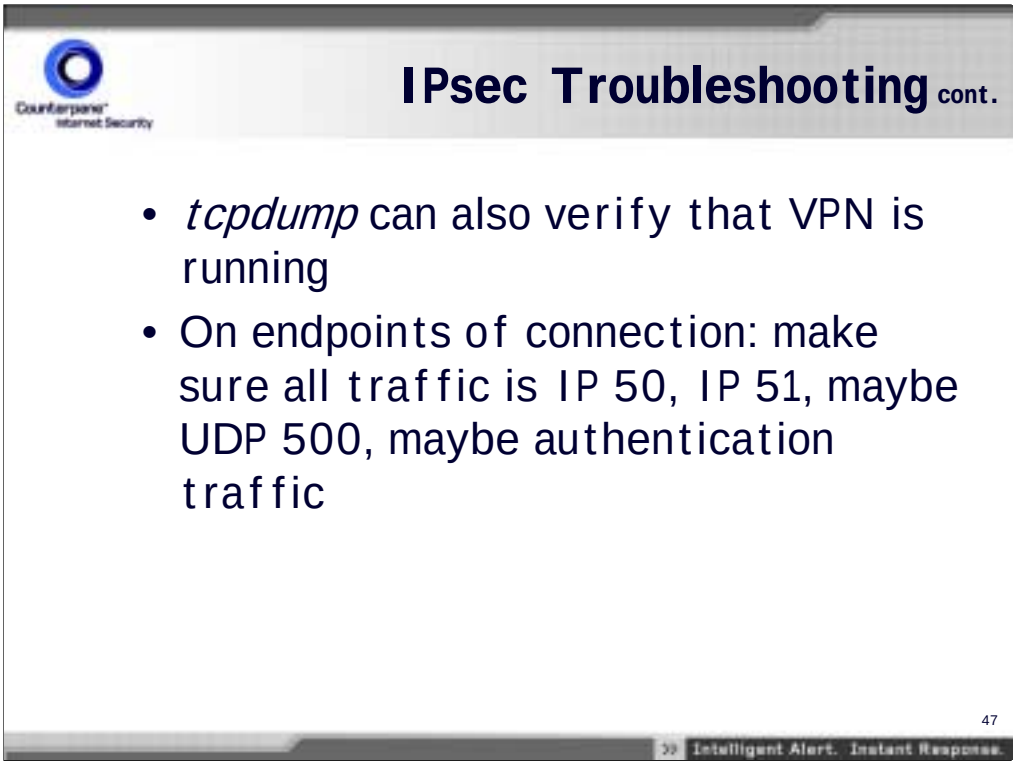
- verify that all systems have the same lifetimes set for SAs, keys
- deliberate session disconnect due to inactivity?
- interoperability issues?

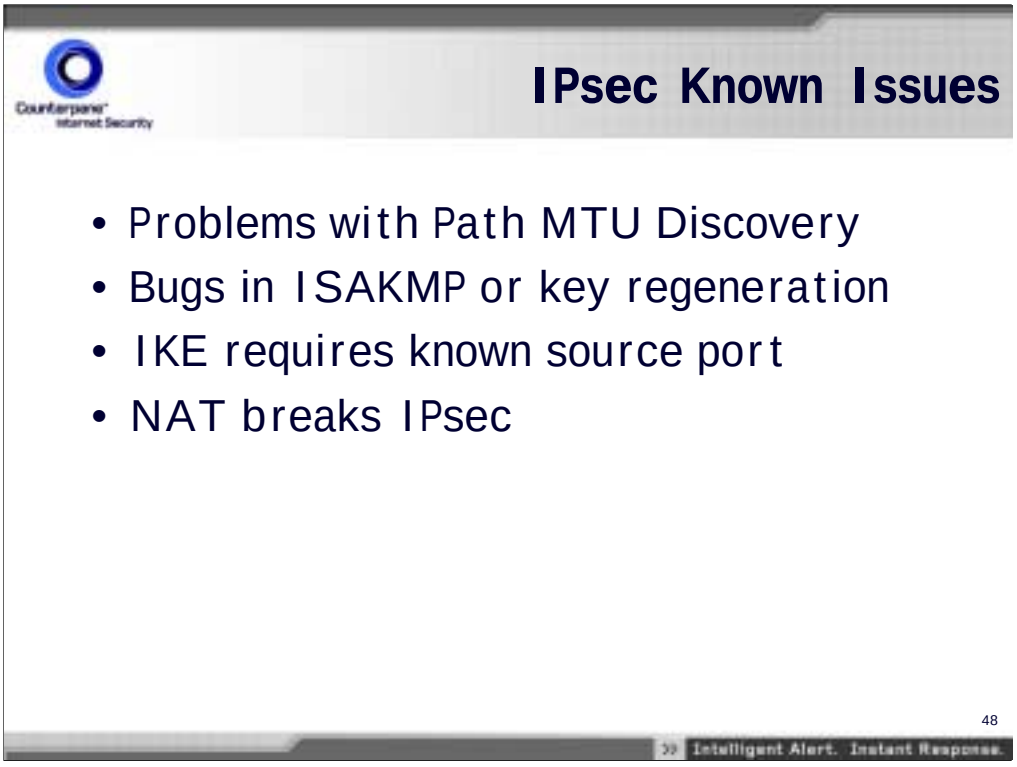
IPsec Troubleshooting cont.

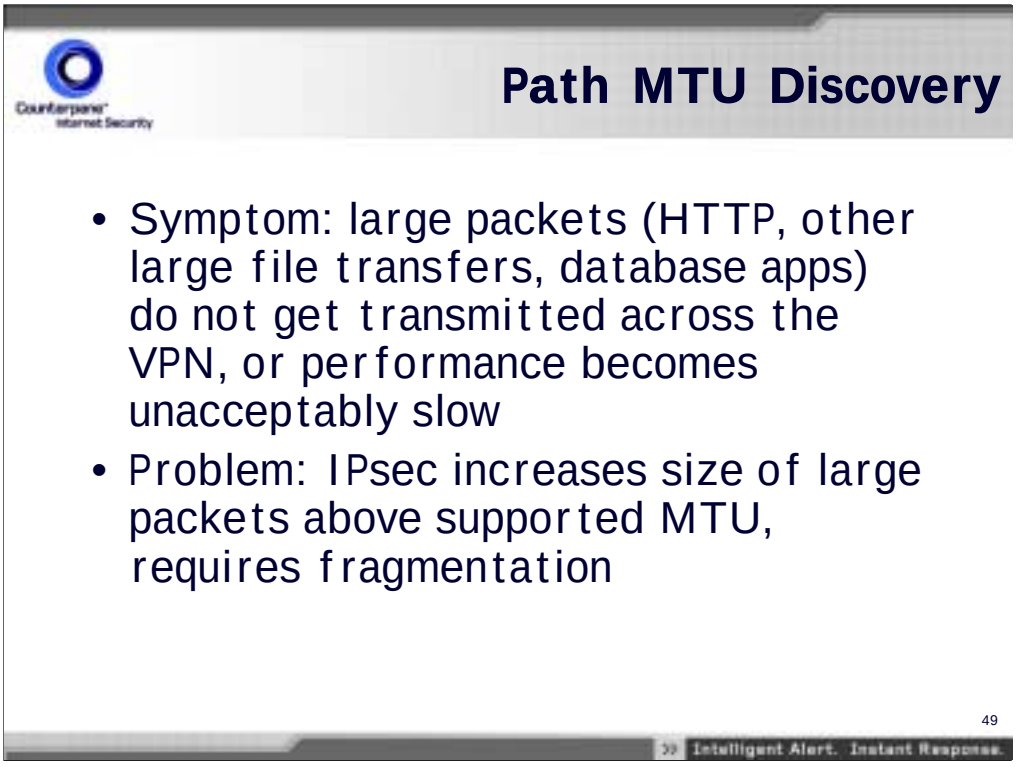
- If encrypted session is established and network resources are visible, but not accessible to the user, verify that NT Domain controls aren't blocking them.

IPsec Troubleshooting cont.

- *tcpdump*, a UNIX-based packet sniffing tool, can be used to monitor the progress of a VPN connection being established.
  - Look for successful key negotiation, user authentication, correct routing
  - Be sure all required servers are responding

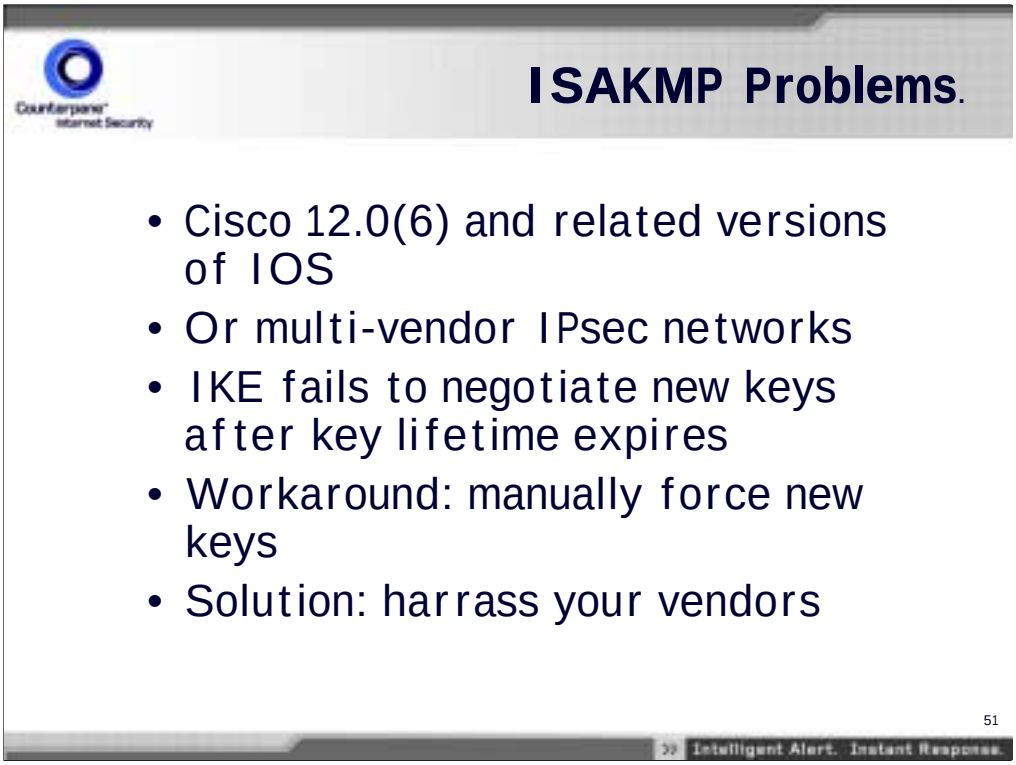

IPsec Troubleshooting cont.
• tcpdump can also verify that VPN is running
• On endpoints of connection: make sure all traffic is IP 50, IP 51, maybe UDP 500, maybe authentication traffic
47
Intelligent Alert. Instant Response.

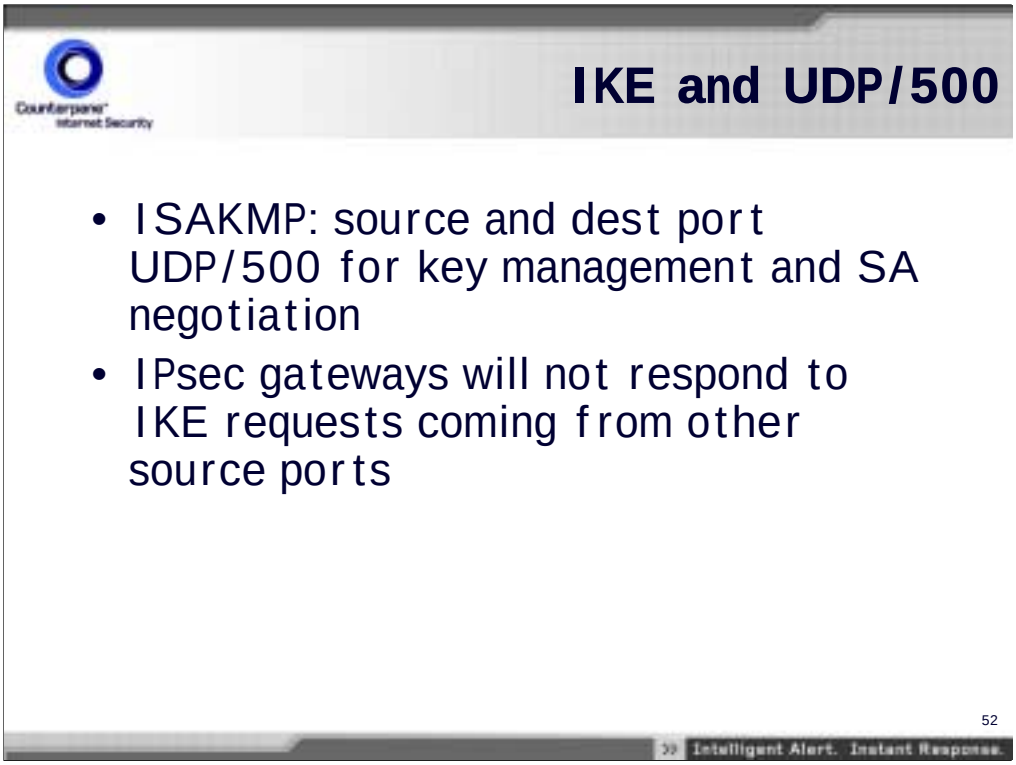

Counterpane
Internet Security
IPsec Known Issues
• Problems with Path MTU Discovery
• Bugs in ISAKMP or key regeneration
• IKE requires known source port
• NAT breaks IPsec
48
Intelligent Alert. Instant Response.

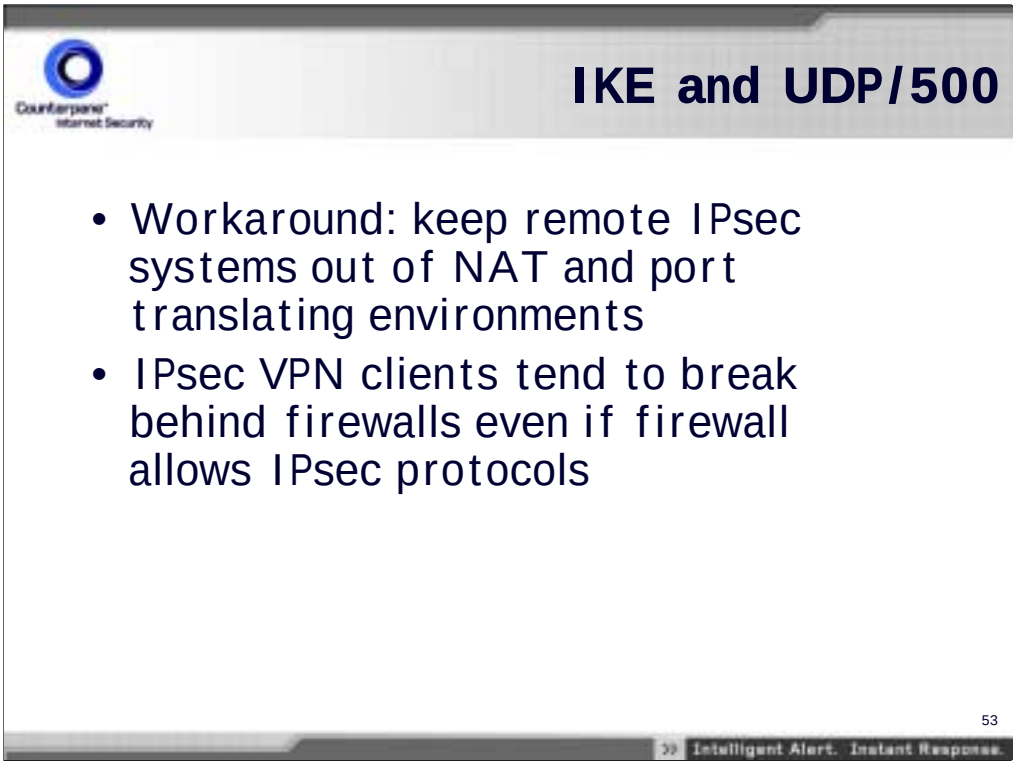

Counterpane
Internet Security
Path MTU Discovery
• Symptom: large packets (HTTP, other large file transfers, database apps) do not get transmitted across the VPN, or performance becomes unacceptably slow
• Problem: IPsec increases size of large packets above supported MTU, requires fragmentation
49
Intelligent Alert. Instant Response.

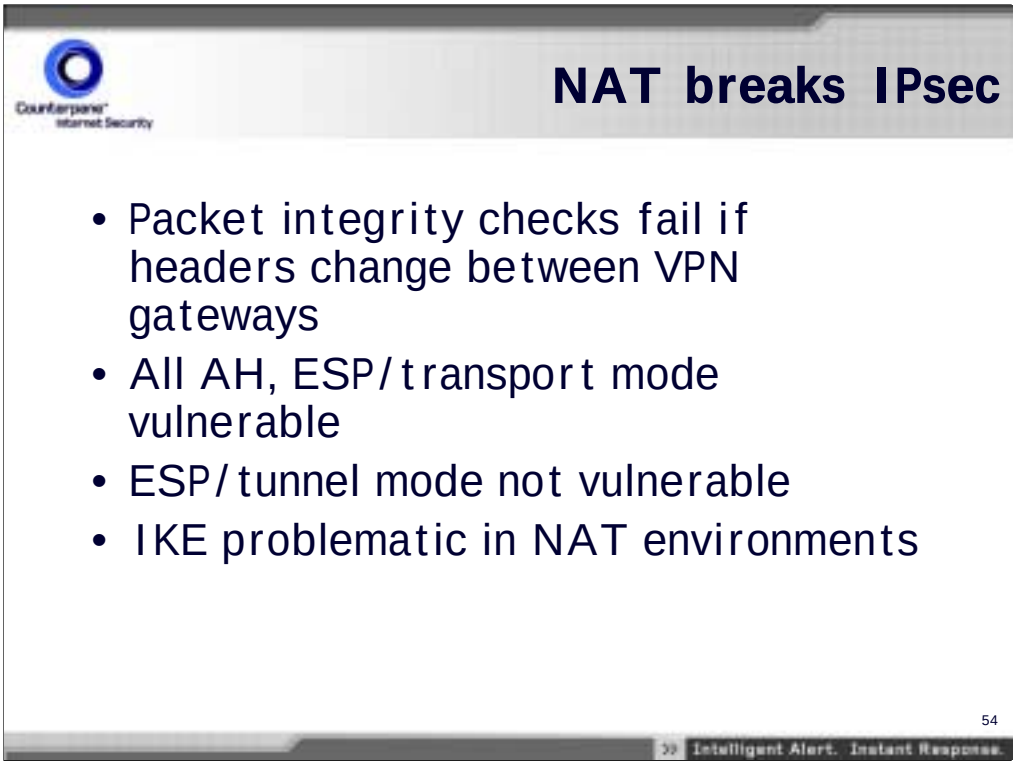
Path MTU Discovery cont.

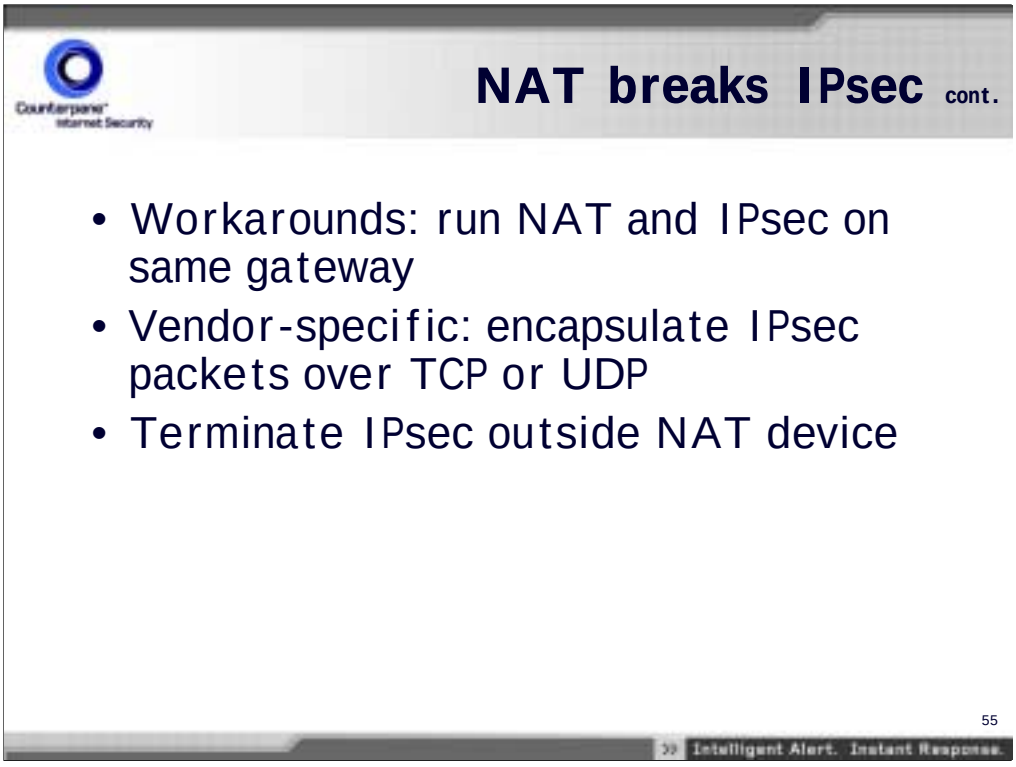
- Work-around: force smaller packets!
- Manually configure servers (behind IPsec gateways) for a lower MTU
- Want size of (data + IPsec) to be below max MTU of gateways


ISAKMP Problems.
• Cisco 12.0(6) and related versions of IOS
• Or multi-vendor IPsec networks
• IKE fails to negotiate new keys after key lifetime expires
• Workaround: manually force new keys
• Solution: harrass your vendors
51
Intelligent Alert. Instant Response.


Counterpane Internet Security
IKE and UDP/500
• ISAKMP: source and dest port UDP/500 for key management and SA negotiation
• IPsec gateways will not respond to IKE requests coming from other source ports
52
Intelligent Alert. Instant Response.


Counterpane Internet Security
IKE and UDP/500
• Workaround: keep remote IPsec systems out of NAT and port translating environments
• IPsec VPN clients tend to break behind firewalls even if firewall allows IPsec protocols
53
Intelligent Alert. Instant Response.

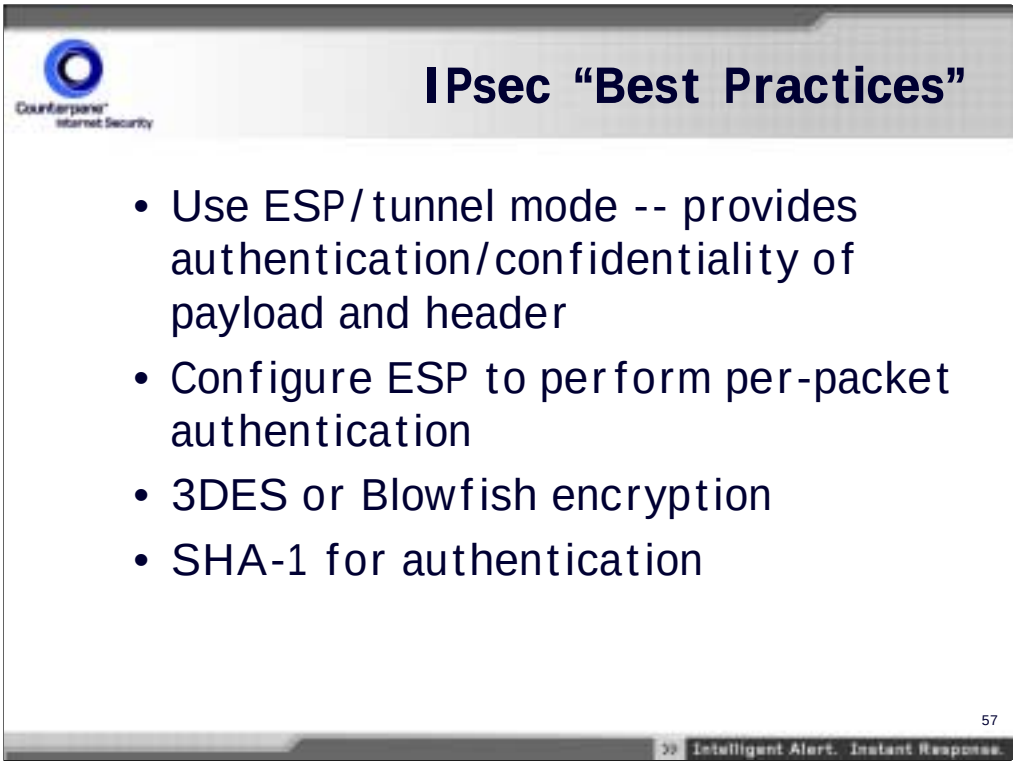

Counterpane Internet Security
NAT breaks IPsec
• Packet integrity checks fail if headers change between VPN gateways
• All AH, ESP/transport mode vulnerable
• ESP/tunnel mode not vulnerable
• IKE problematic in NAT environments
54
Intelligent Alert. Instant Response.

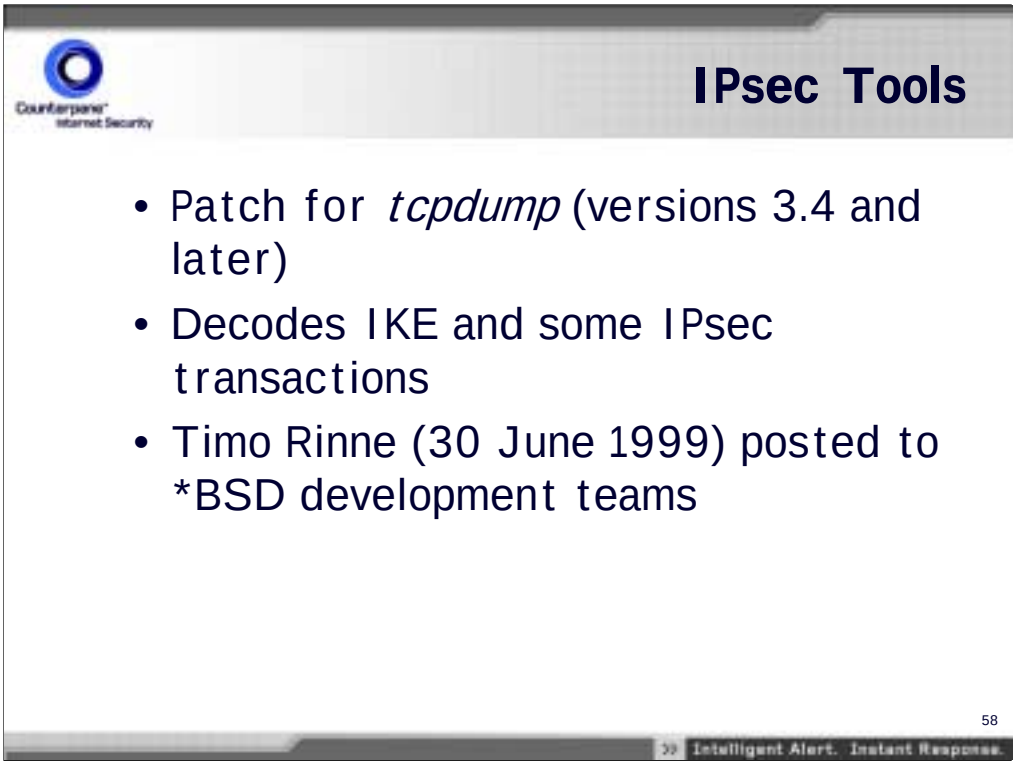

Counterpane Internet Security
NAT breaks IPsec cont.
• Workarounds: run NAT and IPsec on same gateway
• Vendor-specific: encapsulate IPsec packets over TCP or UDP
• Terminate IPsec outside NAT device
55
Intelligent Alert. Instant Response.

NAT breaks IPsec cont.

Dan Harkins, co-author of IKE:

"NAT is the kind of attack IPsec was designed to detect."


IPsec “Best Practices”
• Use ESP/tunnel mode -- provides authentication/confidentiality of payload and header
• Configure ESP to perform per-packet authentication
• 3DES or Blowfish encryption
• SHA-1 for authentication
57
Intelligent Alert. Instant Response.

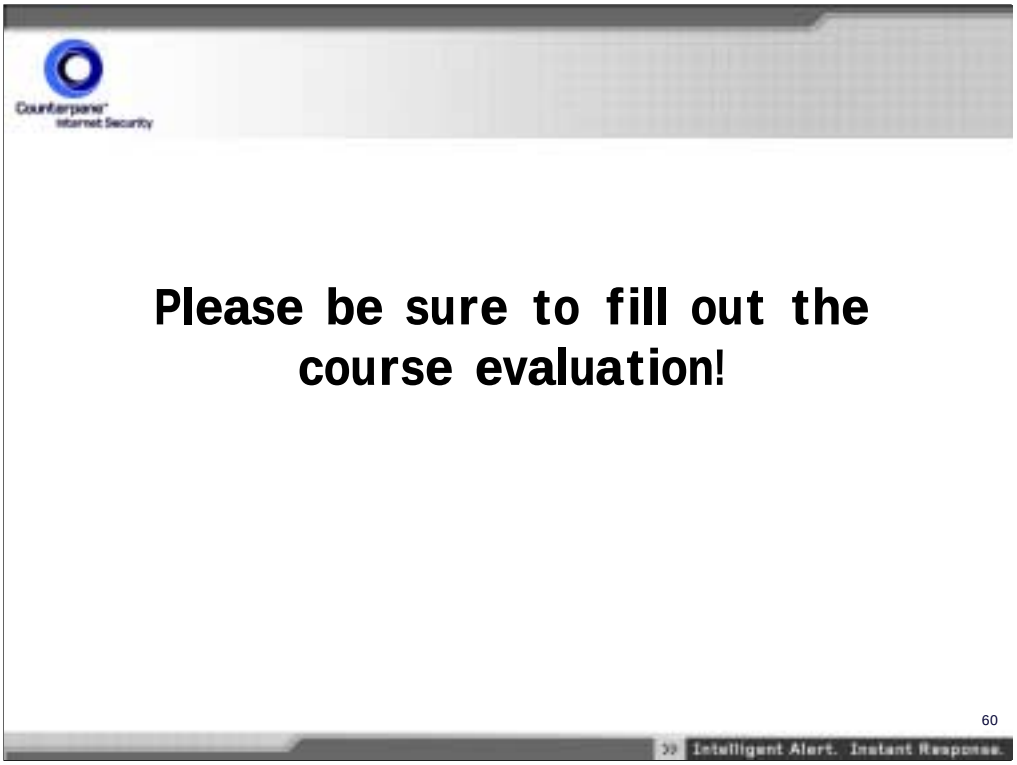

IPsec Tools
• Patch for *tcpdump* (versions 3.4 and later)
• Decodes IKE and some IPsec transactions
• Timo Rinne (30 June 1999) posted to *BSD development teams
58
Intelligent Alert. Instant Response.

For more info:

VPN Resources on the World Wide Web:

http://kubarb.phsx.ukans.edu/~tbird/vpn.html

VPN Mailing list:
vpn@securityfocus.com


Counterpane
Internet Security
Please be sure to fill out the course evaluation!
60
Intelligent Alert. Instant Response.