Hacking into Bank

priv8 Network

y3dips@echo.or.id | y3dips.echo.or.id


PARENTAL
ADVISORY
XTREME CONTENT

Private Network

- Old time: Infrastructure Deploy by banks
- Present time: Public infrastructure usage - VPN


PRIVATE
PROPERTY
NO TRESPASSING
THE HILLMAN GROUP
Made in U.S.A.
840147
03-6182-045

VPN

- Just like a Phone call between 2 node over public phone infrastructure
- Priv8 network service delivered over a public network infrastructure

VPN

- a Virtual Private Network
- l2tp, pptp, ipsec, ssl vpn, ssh based vpn (oepn vpn)

VPN


Laptop
PDA
Encrypted "tunnel" direct
from client to VPN server
Internet
Secure
VPN
server

Why Using VPN

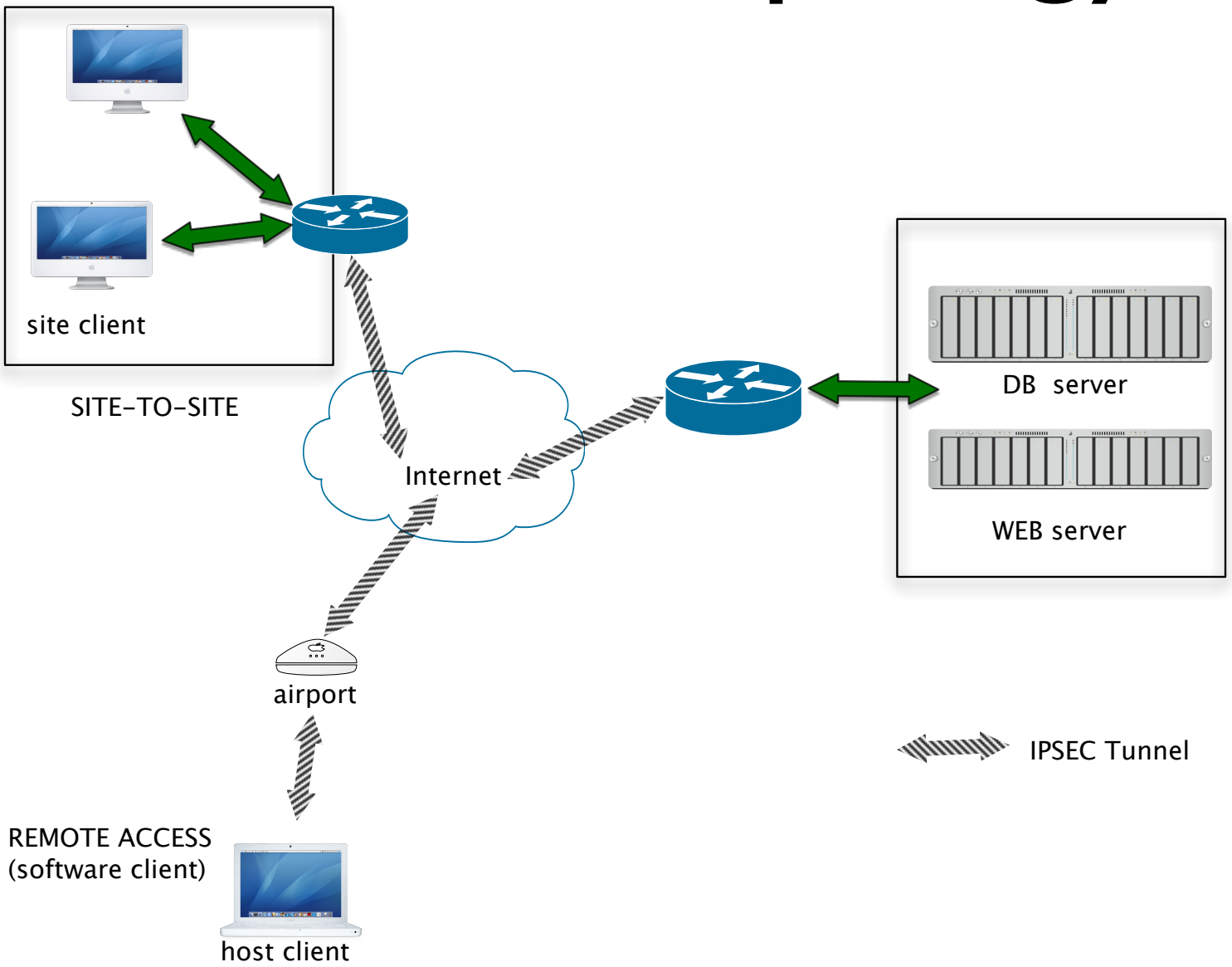
- Bank eagerly needed a private line!
- Reducing Cost.
- “It should be” Secure.

Why Attacking VPN

- Yes, Its Private.
- Is it Secure? (relatively).
- The Most Dangerous place are the safest place.
- Rely on the security product.

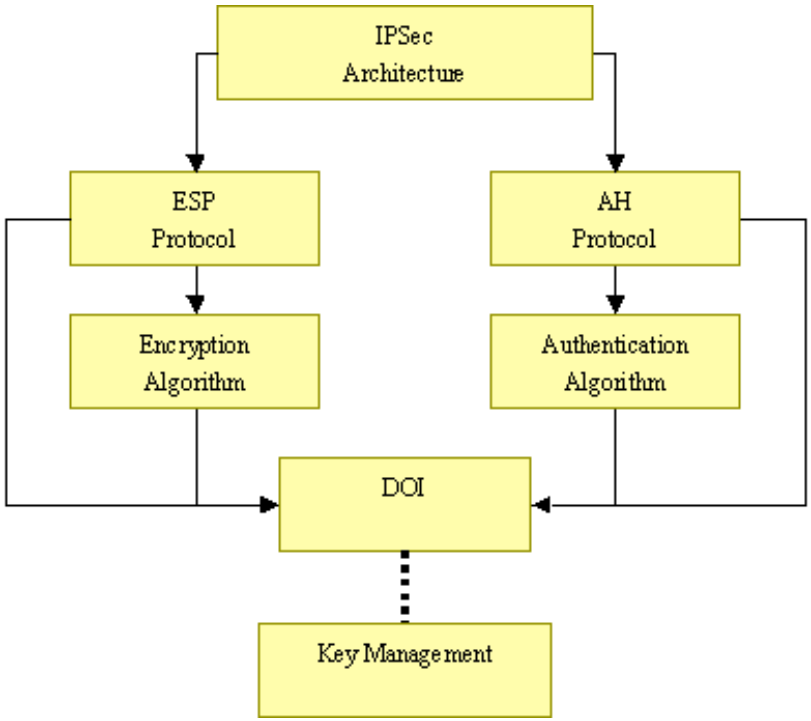
Hacking
The IPSECs VPN

The VPN Topology



The IPSECs

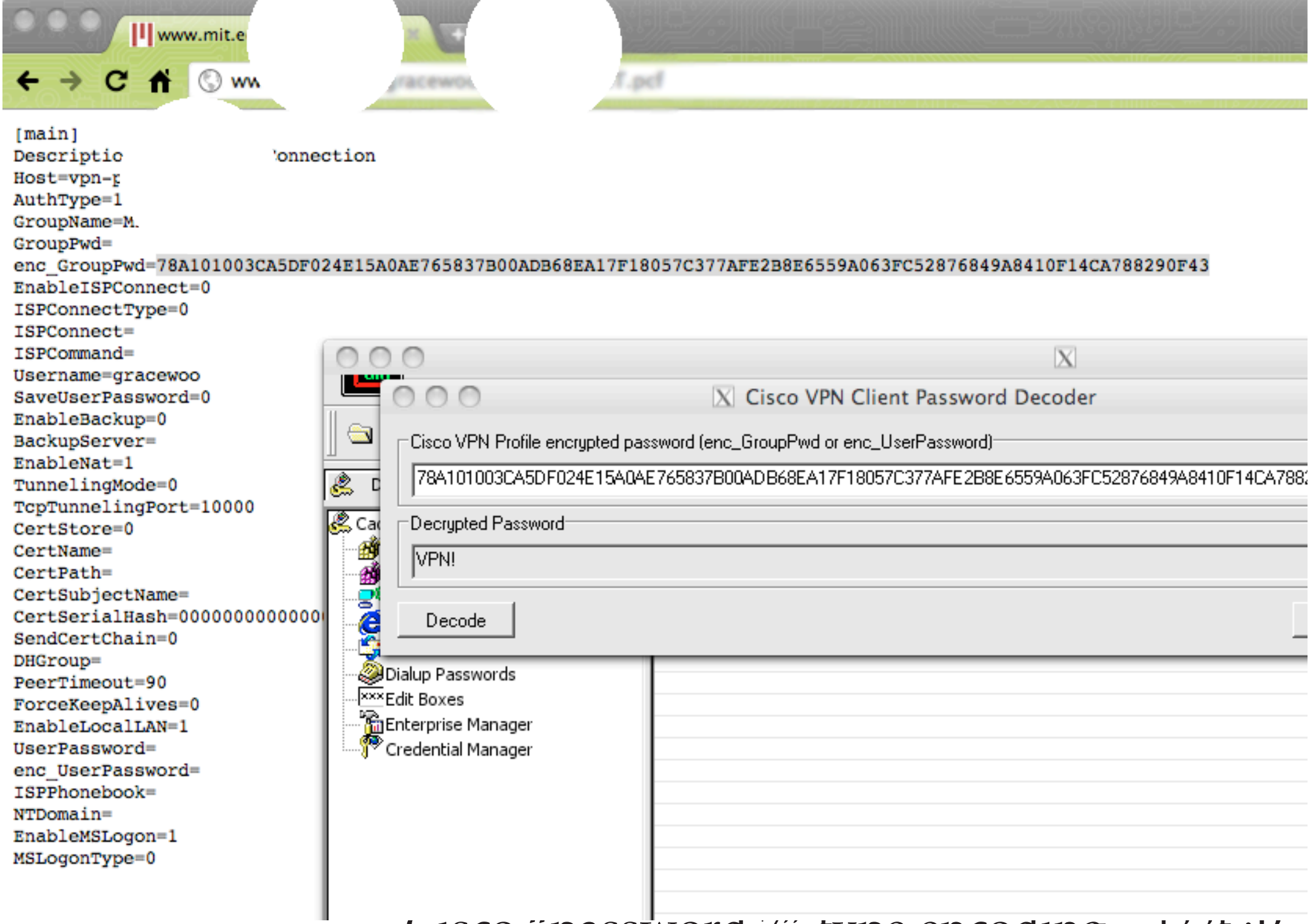
IPSEC


IPSec
Architecture
ESP
Protocol
AH
Protocol
Encryption
Algorithm
Authentication
Algorithm
DOI
Key Management

IPSEC

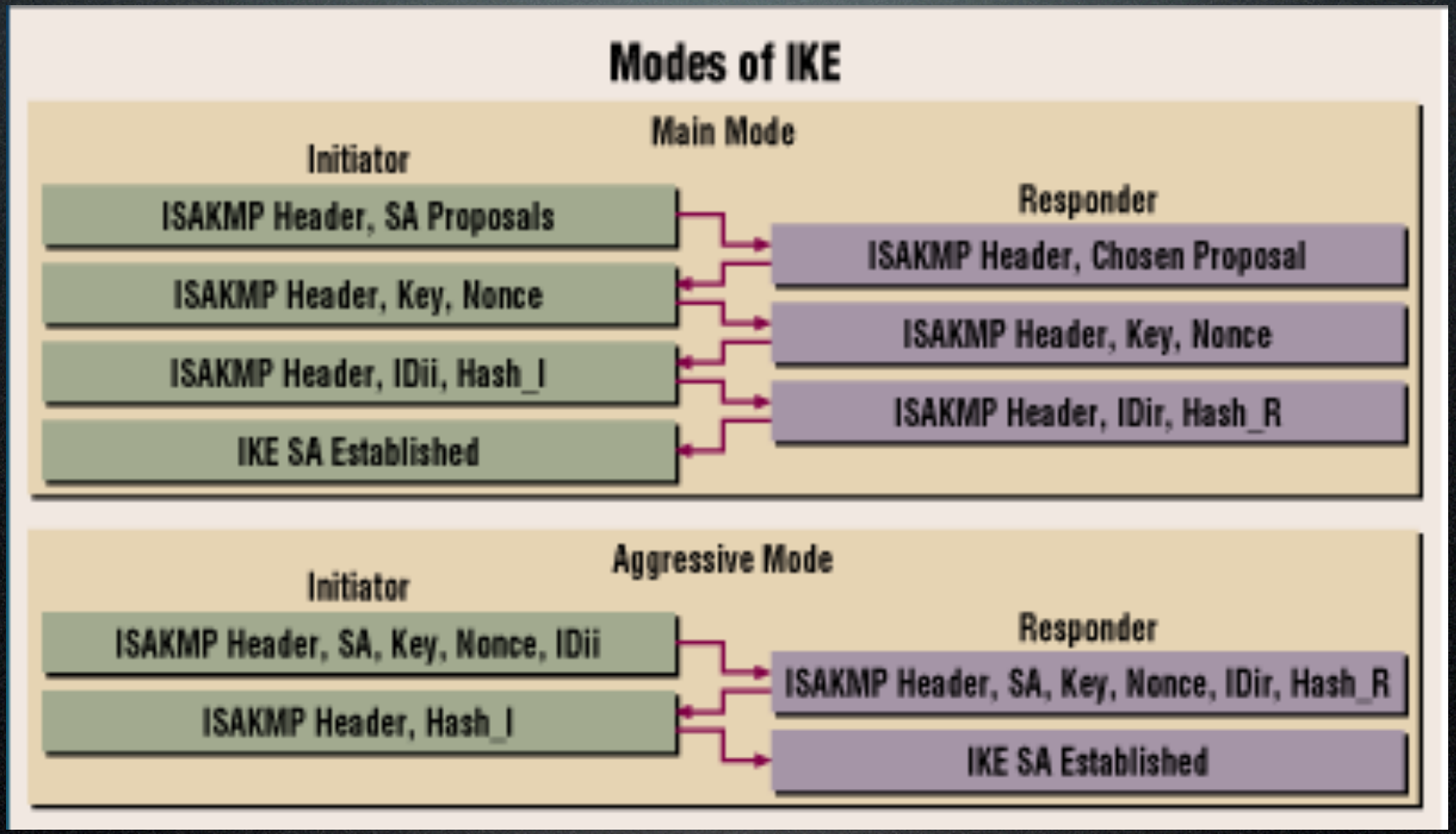
- Set of Protocols.
- AH, ESP, IKE, Encryption.
- Layer 3, Network
- udp 500, 4500, IP 50,51

Famous Issue with The IPSECs VPN



Cisco "password 7" type encoding = 133t :P

Core Issue !



supportforums.cisco.com

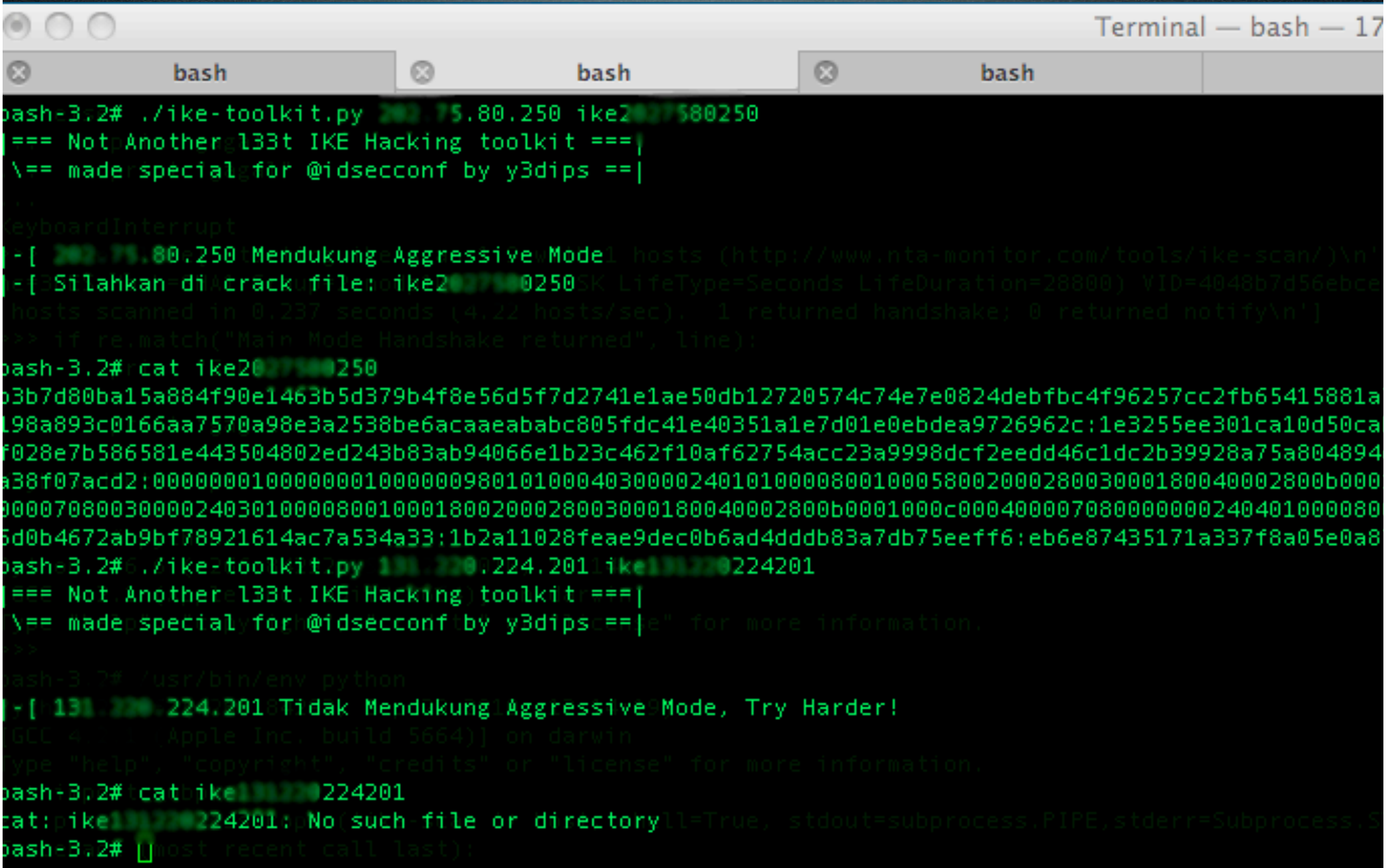
Aggressive Mode Issue

- Quick Handshake.
- Hash in Plaintext.
- Dedicated IP not a mandatory.
- User (ID) not a mandatory.

Well Known Tools

- Ike-Scan
- Ike-probe
- IKEprober
- ikecrack-snarf

Custom Tools?

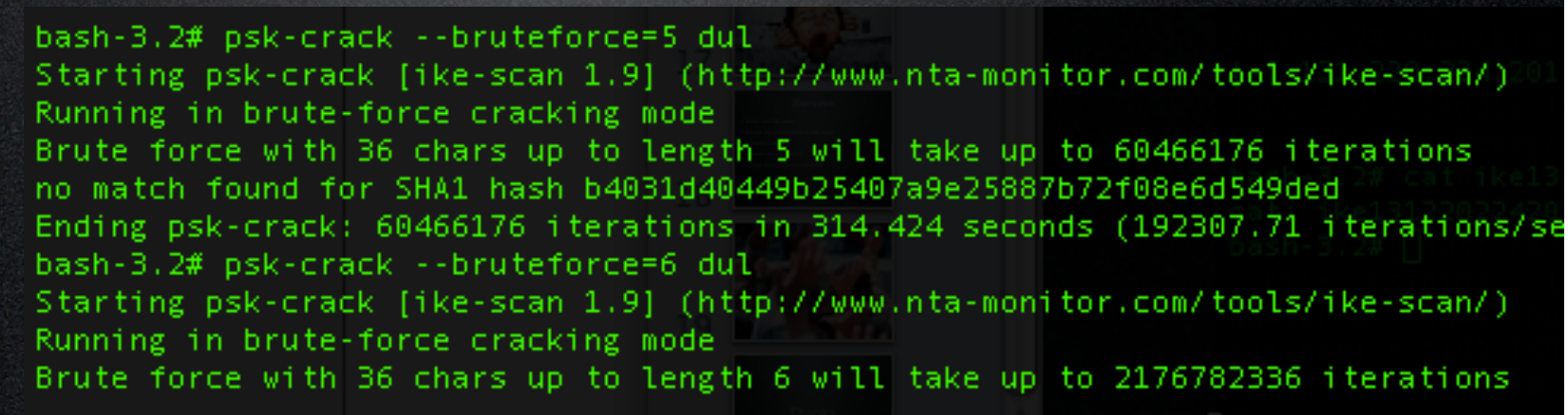


How it works

```
        [Good: True]
        [Bad : False]
    Source: 192.168.1.4 (192.168.1.4)
    Destination: 202.75.80.250 (202.75.80.250)
▽ User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
    Source port: isakmp (500)
    Destination port: isakmp (500)
    Length: 644
  ▷ Checksum: 0x0c43 [validation disabled]
▽ Internet Security Association and Key Management Protocol
    Initiator cookie: 1FADFBC43B73FA4B
    Responder cookie: 0000000000000000
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Aggressive (4)
  ▽ Flags: 0x00
        .... ...0 = Not encrypted
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 636
  ▽ Security Association payload
        Next payload: Key Exchange (4)
```

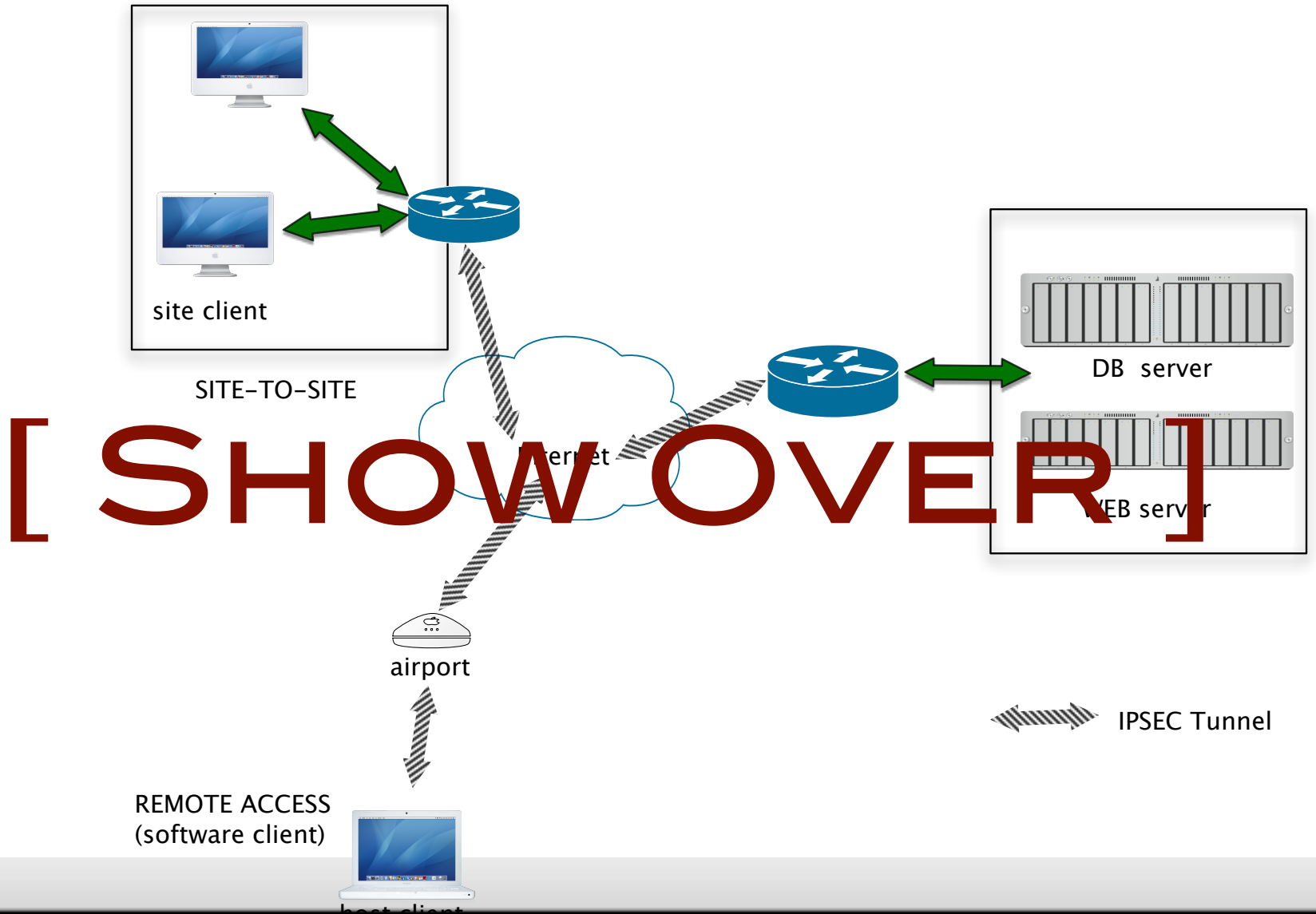
What Next?

- Crack the PSK with known Tools
  - psk-crack
- Build Your Own Cracker (not so hard but not done :P)



Other Issue

- Vendor Issue with the device/protocl implementation (!google)
- Configuration Issue
  - Split tunneling
  - Transform Mode
- Credential storing
  - Un-encrypted
  - Not Secure



[SHOW OVER]

```
bash-3.2# psk-crack --bruteforce=8 dul
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in brute-force cracking mode
Brute force with 36 chars up to length 8 will take up to 2821109907456 iterations
key "woodpack" matches SHA1 hash 323e4df348e32dd5fc8e93ac4686a12d8d5ec930
```


RAMI MEIRI 06

Survive

- “Eliminate transport mode and the AH protocol, and fold authentication of the ciphertext into the ESP protocol, leaving only ESP in tunnel mode.”

http://www.schneier.com/paper-ipsec.html

Survive

- Dont Use PSK please :)
- Disable Aggresive Mode in the device
- Network Filtering
  - Never use Dynamic IP
  - Filter IP to connect to Gateway

Reference

- PSK Cracking using IKE Aggressive Mode - Michael Thumann
- IPSec VPN Design - Vijay Bollapragada, Mohamed Khalid, Scott Wainner
- Great Old “google” also for “most of the” images.

Thanks

@y3dips