Computador 1 computador 2

ISAKMP (opções de segurança)

AES 128 Bits

SHA=1

MODP – p

ISAKMP (opções de segurança Escolhida)

AES 128 Bits

SHA=1

MODP – p

a=4(nunca troco com ninguém)

p=33

g=15 ISAKMP(g, A)

= 3 b = 18(nunca troca

Com ninguém)

p = 33

g = 15

ISAKMP(g, B) = 9

AES # AES

chave chave confirma

Quick Mode

ESP