



## ADVANCED IPSEC ALGORITHMS AND PROTOCOLS SESSION SEC-4011

SEC-4011  
9831\_05\_2004\_X2

© 2004 Cisco Systems, Inc. All rights reserved.

1

## Agenda

Cisco.com

- **Analysis of Baseline IPSec Functionality**
  - IKE: IPSec Negotiation Protocol Flow
  - PKI: IPSec Authentication Architecture
  - SHA and MD5: IPSec Hashing Mechanisms
  - DES and AES: IPSec Encryption Techniques
- **Analysis of the Enhancements in IPSec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPSec Negotiation Protocol Flow
  - Multicast IPSec
  - Major IPSec Enhancements in the works

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

2

# Agenda

Cisco.com

- **Analysis of Baseline IPsec Functionality**
  - IKE: IPsec Negotiation Protocol Flow**
  - PKI: IPsec Authentication Architecture**
  - SHA and MD5: IPsec Hashing Mechanisms**
  - DES and AES: IPsec Encryption Techniques**
- **Analysis of the Enhancements in IPsec**
  - Remote Access Features, NAT Traversal, DPD**
  - IKE v2: New IPsec Negotiation Protocol Flow**
  - Multicast IPsec**
  - Major IPsec Enhancements in the works**

SEC-4011  
9831\_05\_2004\_X2

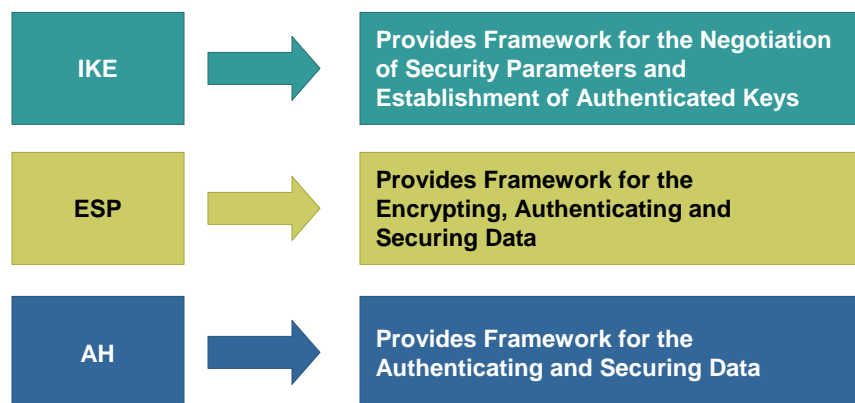
© 2004, Cisco Systems, Inc. All rights reserved.

3

# IPsec Composition

Cisco.com

## IPsec Combines Three Main Protocols into a Cohesive Security Framework



SEC-4011  
9831\_05\_2004\_X2

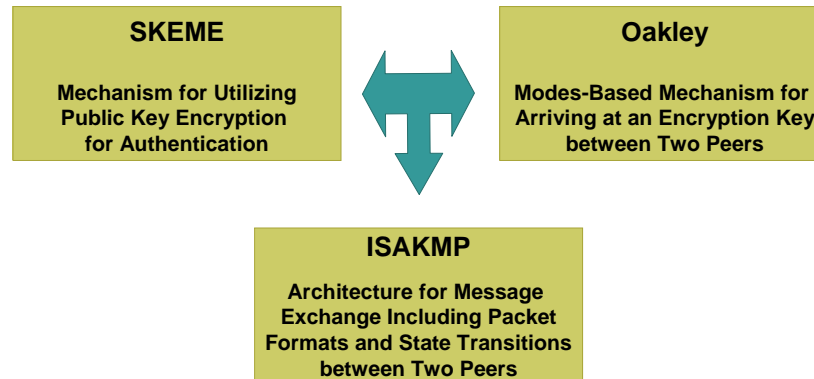
© 2004, Cisco Systems, Inc. All rights reserved.

4

## What Is IKE?

Cisco.com

### IKE (Internet Key Exchange) (RFC 2409) Is a Hybrid Protocol



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

5

## Why IKE?

Cisco.com

- **IKE solves the problems of manual and unscalable implementation of IPSec by automating the entire key exchange process**
  - Negotiation of SA characteristics**
  - Automatic key generation**
  - Automatic key refresh**
  - Manageable manual configuration**

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

6

# How Does IKE Work?

Cisco.com

## IKE Is a TWO Phase Protocol

### Phase 1 Exchange

Peers Negotiate a Secure, Authenticated Channel with which to Communicate 'Main Mode' or 'Aggressive Mode' Accomplish a Phase I Exchange



### Phase 2 Exchange

Security Associations Are Negotiated on Behalf of IPSec Services; 'Quick Mode' Accomplishes a Phase II Exchange

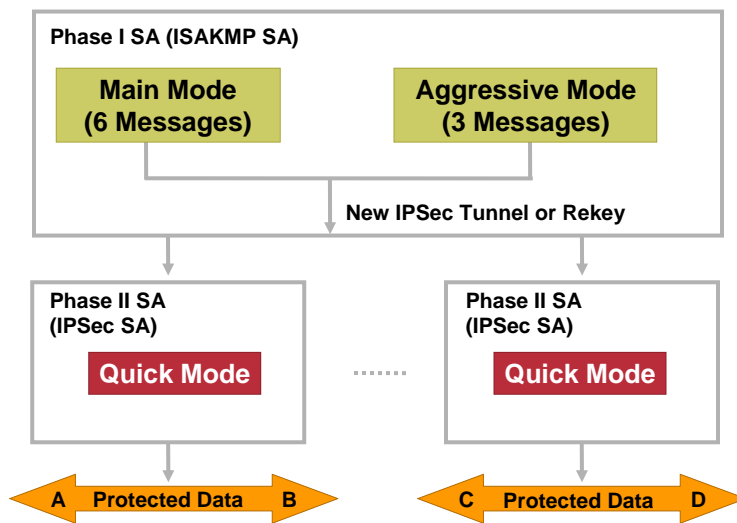
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

7

# How Does IKE Work?

Cisco.com



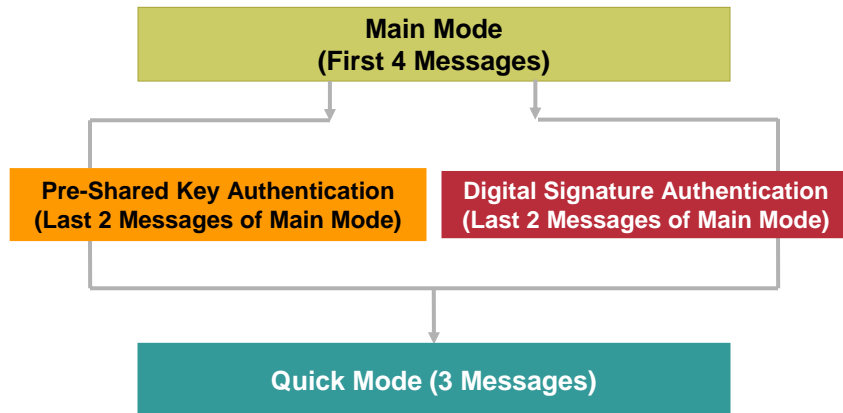
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

8

## Presentation Flow

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

9

## IKE Phase 1 (Main Mode): Preparation for Sending 'Message 1 and 2'

Cisco.com

### Goal: Negotiation of IKE SA Parameters

#### Generation of Initiator Cookie

A 8 Byte Pseudo-Random Number Used for Anti-Clogging

$CKY-I = md5\{\{src\_ip, dest\_ip\}, Random\ Number\}$

#### Generation of Responder Cookie

A 8 Byte Pseudo-Random Number Used for Anti-Clogging

$CKY-R = md5\{\{src\_ip, dest\_ip\}, Random\ Number\}$

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

10

# IKE Phase 1 (Main Mode): Sending 'Message 1'

Cisco.com

The Initiator Proposes a Set of Attributes to Base the SA on

Initiator → Responder

Initiator Cookie (Calculated and Inserted Here)			
Responder Cookie (Left 0 for Now)			
SA	Version	Exchange	Flags
Message ID			
Total Message Length			
Next Payload	1	SA Payload	Length
SA Payload (Includes DOI and Situation)			
Next Payload	1	Proposal Payload	Length
Proposal Payload			
Next Payload	1	Transform Payload	Length
Transform Payload			
Next Payload	1	Proposal Payload	Length
Proposal Payload			
0	1	Transform Payload	Length
Transform Payload			

DOI Identifies the Exchange To Be Occurring to Setup IPsec

SPI = 0 For All Phase 1 Messages  
Includes Proposal #, Protocol ID, SPI Size, # of Transforms, SPI (Two Proposals Shown Here)

Includes Transform #, Transform ID, SA Attributes, For Example, DES, MD5, DH 1, Pre Share, Timeout (Two Transform Sets Shown Here)

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

11

# IKE Phase 1 (Main Mode): Sending 'Message 2'

Cisco.com

The Responder Sends Back the One Set of Attributes Acceptable to It

Responder ← Initiator

Initiator Cookie (Same as Before)			
Responder Cookie (Calculated and Inserted Here)			
SA	Version	Exchange	Flags
Message ID			
Total Message Length			
Next Payload	1	SA Payload	Length
SA Payload (Includes DOI and Situation)			
Next Payload	1	Proposal Payload	Length
Proposal Payload (Includes Proposal #, Protocol ID, SPI Size, # of Transforms, SPI)			
0	1	Transform Payload	Length
Transform Payload (Includes Transform #, Transform ID, SA Attributes)			

DOI Identifies the Exchange To Be Occurring to Setup IPsec

PROTO\_ISAKMP, SPI = 0 for All Phase 1 Messages

KEY\_OAKLEY = type DES, MD5, DH 1 Pre-Share

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

12

## IKE Phase 1 (Main Mode): Preparation for Sending 'Message 3 and 4'

Cisco.com

### Goal: Exchange of Information Required for Key Generation Using DH Exchange

#### Generation of DH Public Value by Initiator

$$\text{DH Public Value} = X_a$$

$$X_a = g^a \text{ mod } p$$

Where  $g$  Is the Generator and  $p$  a Large Prime Number and  $a$  Is a Private Secret Known Only to the Initiator

#### Generation of DH Public Value by Responder

$$\text{DH Public Value} = X_b$$

$$X_b = g^b \text{ mod } p$$

Where  $g$  Is the Generator and  $p$  a Large Prime Number and  $b$  Is a Private Secret Known Only to the Responder

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

13

## IKE Phase 1 (Main Mode): Preparation for Sending 'Message 3 and 4'

Cisco.com

#### Generation of a Nonce by Initiator

Nonce Is a Very Large Random Number

$$\text{Initiator Nonce} = N_i$$

#### Generation of a Nonce by Responder

Nonce Is a Very Large Random Number

$$\text{Responder Nonce} = N_r$$

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

14



## IKE Phase 1 (Main Mode): Preparation for Sending 'Message 5 and 6'

Cisco.com

**Goal: Exchange of Authentication Information Using DH**

**Calculation of the Shared DH Secret by Initiator**

Shared Secret =  $(X_b)^a \bmod p$

$$\begin{aligned} (X_b)^a \bmod p &= \\ (X_a)^b \bmod p &= \\ &= g^{ab} \end{aligned}$$

**Calculation of the Shared DH Secret by Responder**

Shared Secret =  $(X_a)^b \bmod p$

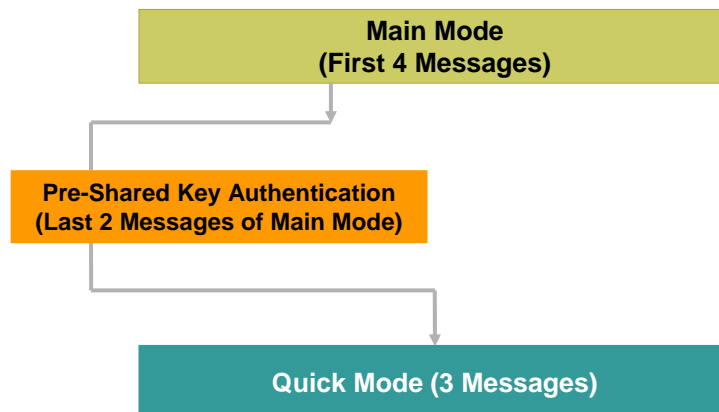
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

17

## Presentation Flow

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

18

## IKE Phase 1 (Main Mode): (Pre-Shared Keys) Preparation for Sending 'Message 5 and 6'

Cisco.com

### Calculation of Three Keys (Initiator)

SKEYID\_d—Used to Calculate Subsequent IPSec Keying Material

SKEYID\_a—Used to Provide Data integrity and Authentication to IKE Messages

SKEYID\_e—Used to Encrypt IKE Messages

$$\text{SKEYID} = \text{PRF}(\text{Pre-Shared Key}, N_i | N_r)$$

PRF = A Pseudo Random Function Based on the Negotiated Hash

$$\text{SKEYID}_d = \text{PRF}(\text{SKEYID}, g^{ab} | \text{CKY-I} | \text{CKY-R} | 0)$$

$$\text{SKEYID}_a = \text{PRF}(\text{SKEYID}, \text{SKEYID}_d | g^{ab} | \text{CKY-I} | \text{CKY-R} | 1)$$

$$\text{SKEYID}_e = \text{PRF}(\text{SKEYID}, \text{SKEYID}_a | g^{ab} | \text{CKY-I} | \text{CKY-R} | 2)$$

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

19

## IKE Phase 1 (Main Mode): (Pre-Shared Keys) Preparation for Sending 'Message 5 and 6'

Cisco.com

### Calculation of Three Keys (Responder)

SKEYID\_d—Used to Calculate Subsequent IPSec Keying Material

SKEYID\_a—Used to Provide Data integrity and Authentication to IKE Messages

SKEYID\_e—Used to Encrypt IKE Messages

$$\text{SKEYID} = \text{PRF}(\text{Pre-Shared Key}, N_i | N_r)$$

$$\text{SKEYID}_d = \text{PRF}(\text{SKEYID}, g^{ab} | \text{CKY-I} | \text{CKY-R} | 0)$$

$$\text{SKEYID}_a = \text{PRF}(\text{SKEYID}, \text{SKEYID}_d | g^{ab} | \text{CKY-I} | \text{CKY-R} | 1)$$

$$\text{SKEYID}_e = \text{PRF}(\text{SKEYID}, \text{SKEYID}_a | g^{ab} | \text{CKY-I} | \text{CKY-R} | 2)$$

SEC-4011  
9831\_05\_2004\_X2

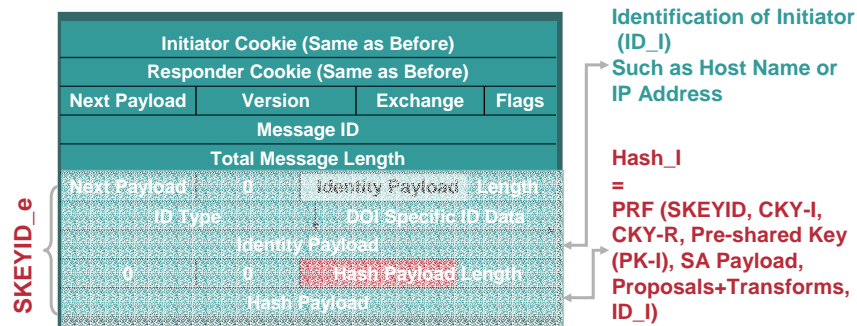
© 2004, Cisco Systems, Inc. All rights reserved.

20

# IKE Phase 1 (Main Mode): (Pre-Shared Keys) Sending 'Message 5'

Cisco.com

The Initiator Sends Its Authentication Material and ID



SEC-4011  
9831\_05\_2004\_X2

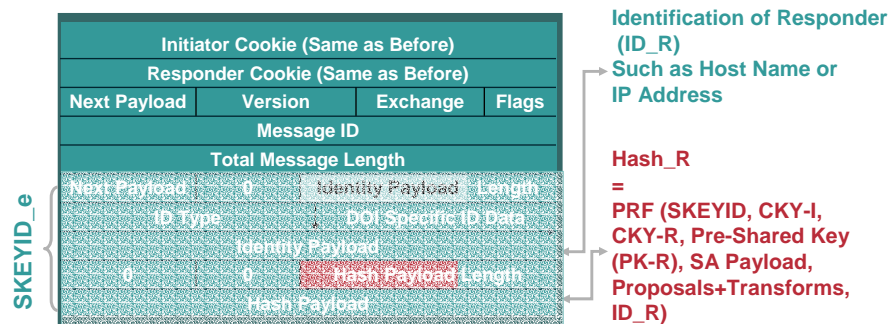
© 2004, Cisco Systems, Inc. All rights reserved.

21

# IKE Phase 1 (Main Mode): (Pre-Shared Keys) Sending 'Message 6'

Cisco.com

The Responder Sends Its Authentication Material and ID



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

22

## IKE Phase 1 (Main Mode): Completion of Phase 1

Cisco.com

### Initiator Authenticates the Responder

1. Decrypt message using SKEYID\_E
2. Find configured PK-R using ID\_R
3. Calculate Hash\_R on it's own
4. If received Hash\_R = self-generated Hash\_R then authentication = successful!!

### Responder Authenticates the Initiator

1. Decrypt message using SKEYID\_E
2. Find configured PK-I using ID\_I
3. Calculate Hash\_I on it's own
4. If received Hash\_I = self-generated Hash\_I then authentication = successful!!

ISAKMP SA  
Established!

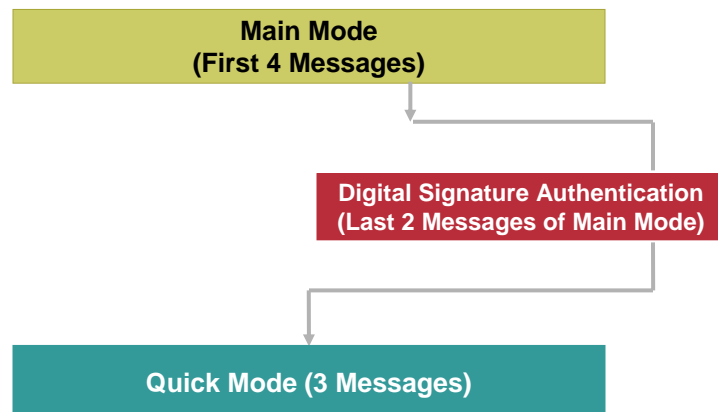
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

23

## Presentation Flow

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

24

## IKE Phase 1 (Main Mode): (Digital Signatures) Preparation for Sending 'Message 5 and 6'

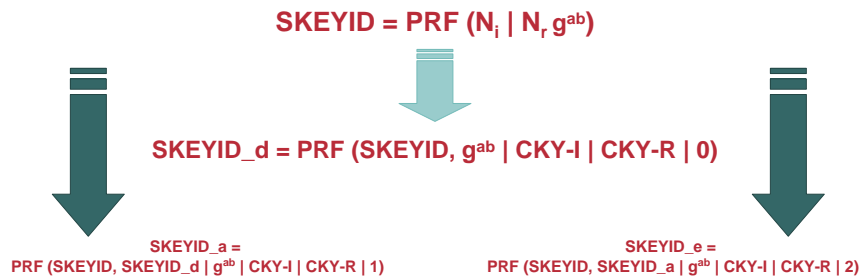
Cisco.com

### Calculation of Three Keys (Initiator)

SKEYID\_d—Used to Calculate Subsequent IPSec Keying Material

SKEYID\_a—Used to Provide Data Integrity and Authentication  
to IKE Messages

SKEYID\_e—Used to Encrypt IKE Messages



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

25

## IKE Phase 1 (Main Mode): (Digital Signatures) Preparation for Sending 'Message 5 and 6'

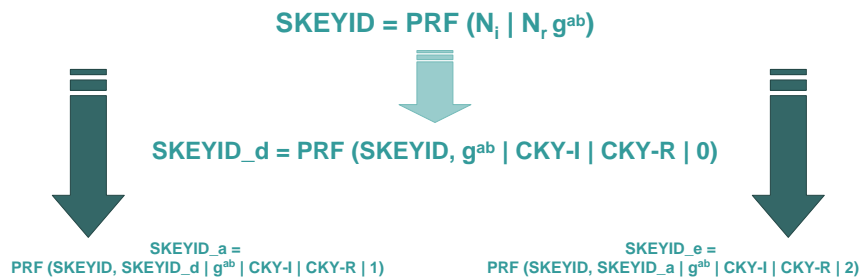
Cisco.com

### Calculation of Three Keys (Responder)

SKEYID\_d—Used to Calculate Subsequent IPSec Keying Material

SKEYID\_a—Used to Provide Data Integrity and Authentication  
to IKE Messages

SKEYID\_e—Used to Encrypt IKE Messages



SEC-4011  
9831\_05\_2004\_X2

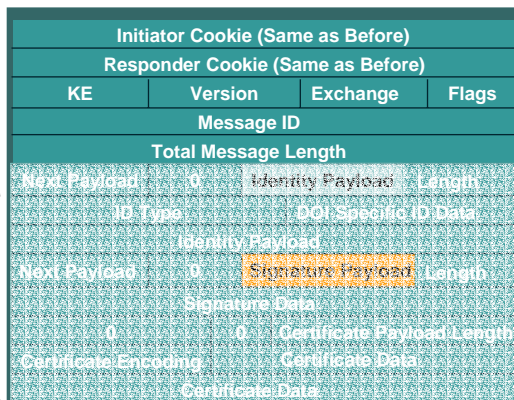
© 2004, Cisco Systems, Inc. All rights reserved.

26

# IKE Phase 1 (Main Mode): (Digital Signatures) Sending 'Message 5'

Cisco.com

The Initiator Sends Its Authentication Material and ID



SKEYID\_e

Identification of Responder (ID\_I)  
Such as Host Name or IP Address

Signature  
= Hash\_I Encrypted with Priv\_I  
= Priv\_I {PRF (SKEYID, CKY-I, CKY-R, SA Payload, Proposals+Transforms, ID\_I)}

SEC-4011  
9831\_05\_2004\_X2

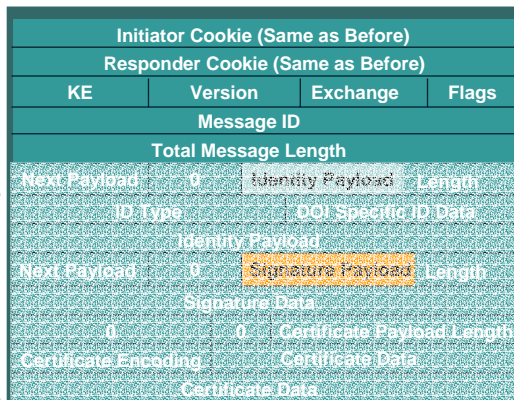
© 2004, Cisco Systems, Inc. All rights reserved.

27

# IKE Phase 1 (Main Mode): (Digital Signatures) Sending 'Message 6'

Cisco.com

The Responder Sends Its Authentication Material and ID



SKEYID\_e

Identification of Responder (ID\_I)  
Such as Host Name or IP Address

Signature  
= Hash\_I Encrypted with Priv\_I  
= Priv\_I {PRF (SKEYID, CKY-I, CKY-R, SA Payload, Proposals+Transforms, ID\_I)}

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

28

## IKE Phase 1 (Main Mode): (Digital Signatures) Completion of Phase 1

Cisco.com

### Initiator Authenticates the Responder

1. Decrypt message using SKEYID\_E
2. Decrypt Hash\_R using Pub\_R
3. Calculate Hash\_R on its own
4. If received Hash\_R = self-generated Hash\_R then authentication = successful!!

### Responder Authenticates the Initiator

1. Decrypt message using SKEYID\_E
2. Decrypt Hash\_I using Pub\_I
3. Calculate Hash\_I on its own
4. If received Hash\_I = self-generated Hash\_I then authentication = successful!!



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

29

## IKE Phase 1 (Quick Mode): Preparation for Sending 'Message 1 and 2'

Cisco.com

### Goal: Negotiation of IPSec SA

#### Execution of DH by Initiator Again to Ensure PFS

New Nonce Generated: Ni'  
New DH Public Value = X<sub>a</sub>'  
 $X_a' = g^a \text{ mod } p$

Where g Is the Generator and p a Large Prime Number  
and a Is a Private Secret Known Only to the Initiator

#### Execution of DH by Responder Again to Ensure PFS

New Nonce Generated: Nr'  
New DH Public Value = X<sub>b</sub>'  
 $X_b' = g^b \text{ mod } p$

Where g Is the Generator and p a Large Prime Number  
and b Is a Private Secret Known Only to the Responder

SEC-4011  
9831\_05\_2004\_X2

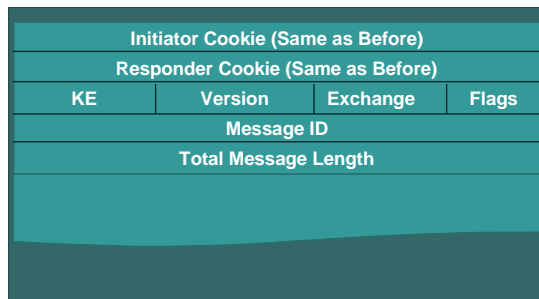
© 2004, Cisco Systems, Inc. All rights reserved.

30

## IKE Phase 2 (Quick Mode): Sending 'Message 1'

Cisco.com

The Initiator Sends Authentication/keying Material and Proposes a Set of Attributes to Base the SA on



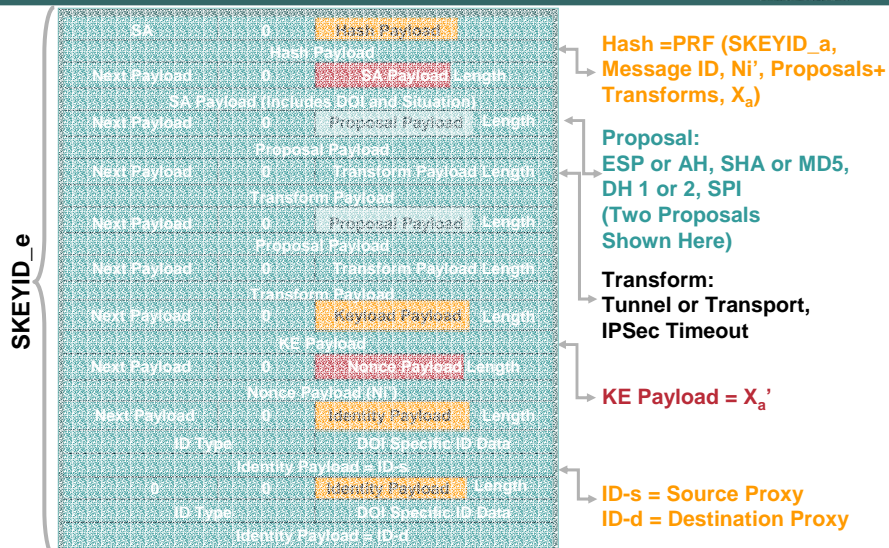
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

31

## IKE Phase 2 (Quick Mode): Sending 'Message 1'

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

32



## IKE Phase 2 (Quick Mode): Completion of Phase 2

Cisco.com

### Initiator Generates IPsec Keying Material

1. Generate new DH shared sSecret =  $(X_b')^a \text{ mod } p$
2. IPsec session key =  
PRF (SKEYID\_d, protocol (ISAKMP),  
new DH shared secret, SPI\_i, N\_i', N\_r')

### Responder Generates IPsec Keying Material

1. Generate new DH shared secret =  $(X_a')^b \text{ mod } p$
2. IPsec session key =  
PRF (SKEYID\_d, protocol (ISAKMP),  
new DH shared secret, SPI\_i, N\_i', N\_r')

SEC-4011  
9831\_05\_2004\_X2

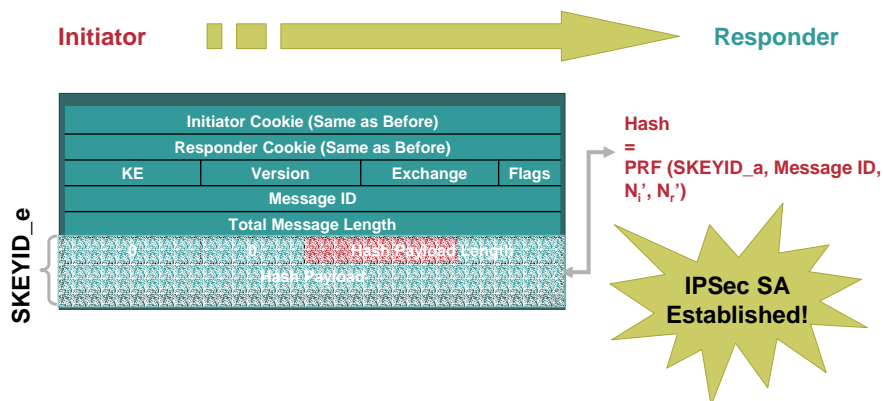
© 2004, Cisco Systems, Inc. All rights reserved.

35

## IKE Phase 2 (Quick Mode): Sending 'Message 3'

Cisco.com

### The Initiator Sends across a Proof of Liveness



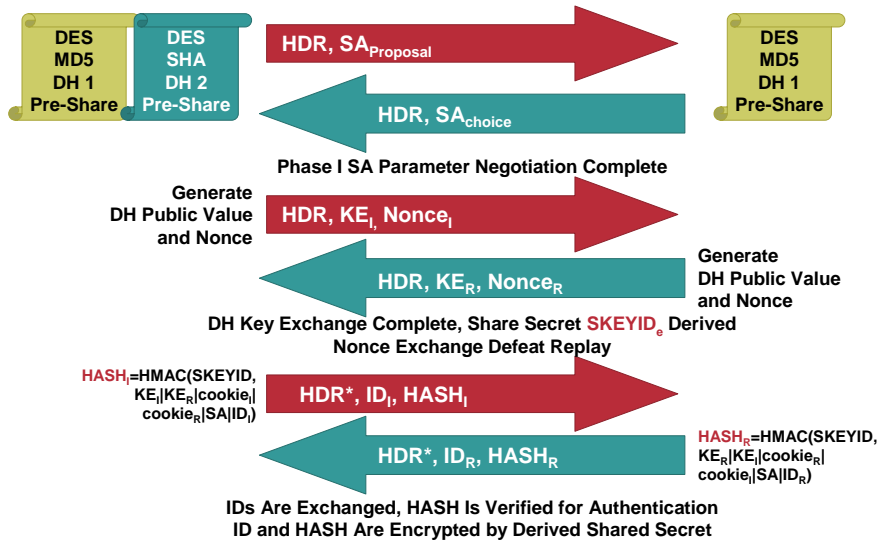
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

36

# One Page Summary: Pre-Shared Main Mode

Cisco.com



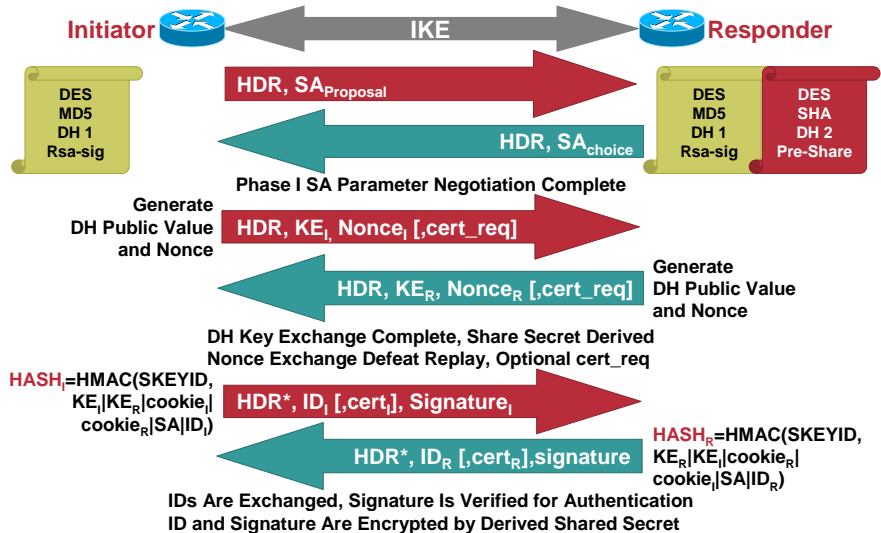
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

37

# One Page Summary: Signatures Main Mode

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

38

## One Page Summary: Quick Mode

Cisco.com

Initiator   $\longleftrightarrow$  IPsec  $\longleftrightarrow$   Responder



SEC-4011  
9831\_05\_2004\_X2

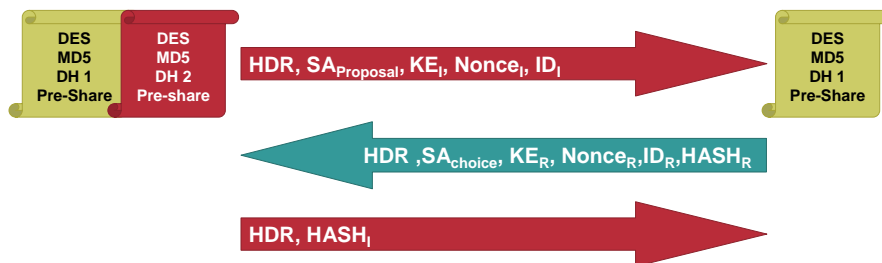
© 2004, Cisco Systems, Inc. All rights reserved.

39

## Aggressive Mode Using Pre-Shared Key: A Quick Overview

Cisco.com

Initiator   $\longleftrightarrow$  IKE  $\longleftrightarrow$   Responder



- Three messages compared to the 6 messages in main mode
- Group pre-shared key lookup possible for remote access applications
- ID is not protected (except RSA encryption)

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

40

# Agenda

Cisco.com

- **Analysis of Baseline IPSec Functionality**
  - IKE: IPSec Negotiation Protocol Flow**
  - PKI: IPSec Authentication Architecture**
  - SHA and MD5: IPSec Hashing Mechanisms**
  - DES and AES: IPSec Encryption Techniques**
- **Analysis of the Enhancements in IPSec**
  - Remote Access Features, NAT Traversal, DPD**
  - IKE v2: New IPSec Negotiation Protocol Flow**
  - Multicast IPSec**
  - Major IPSec Enhancements in the works**

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

41

# PKI: IKE Authentication Architecture

Cisco.com

- **PKI**
- **Digital signatures and certificates**
- **X509, PKIX, PKCS**
- **CA and RA**
- **SCEP**

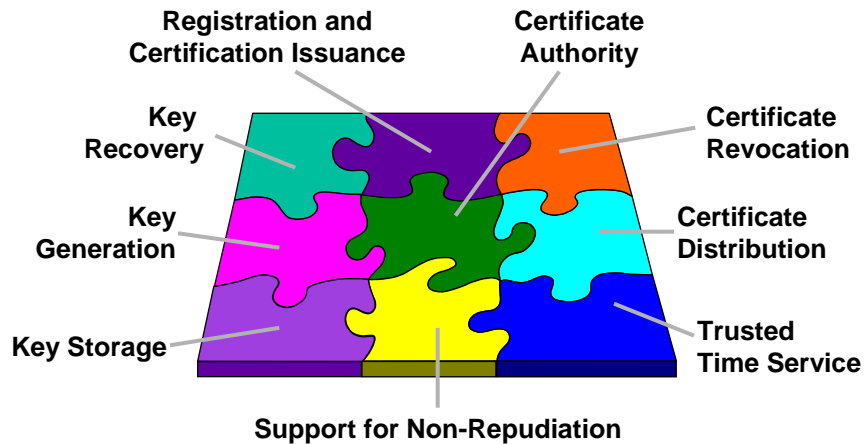
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

42

## PKI: IKE Authentication Architecture

Cisco.com



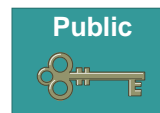
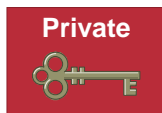
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

43

## Digital Signatures

Cisco.com



- Entity authentication
- Data origin authentication
- Integrity
- Non-repudiation

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

44

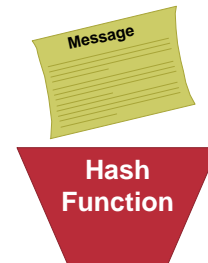
# Digital Signatures

Cisco.com

- One-way function; easy to produce hash from message, “impossible” to produce message from hash



Hash of Message



s74hr7sh7040236fw

Sign Hash with Private Key

7sr7ewq7ytoj56o457  
*Alice*

Signature = “Encrypted”  
Hash of Message

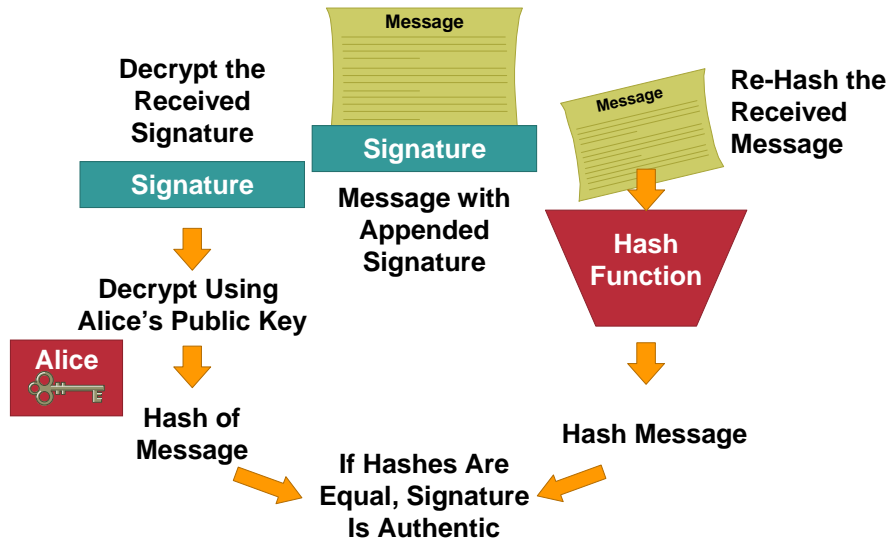
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

45

# Signature Verification

Cisco.com




SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

46

# Certificate Authority

Cisco.com

- The trust basis of a PKI system 
- Verify user identity, issues certificates by binding user's identity to a public key with a digital certificate
- Revokes certificates and publish Certificate Revocation List (CRL)
- In-house implementation or outsourcing

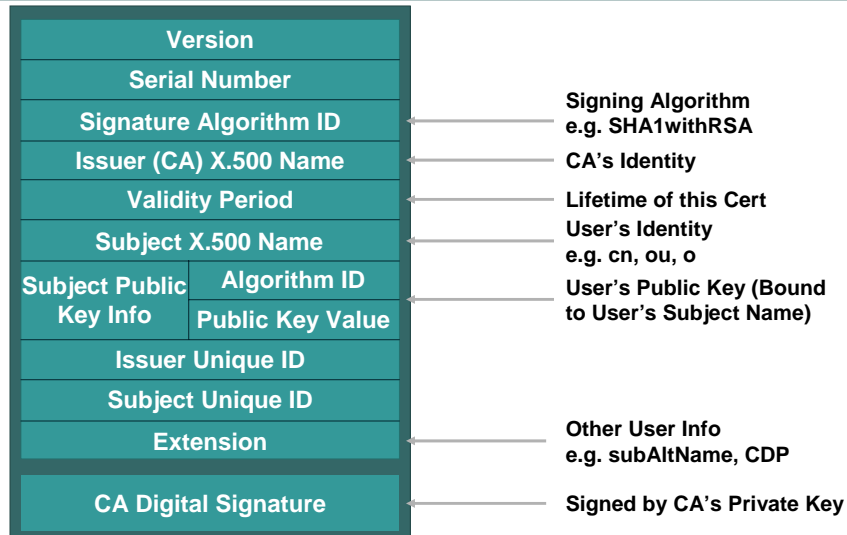
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

47

# X.509 v3 Certificate

Cisco.com



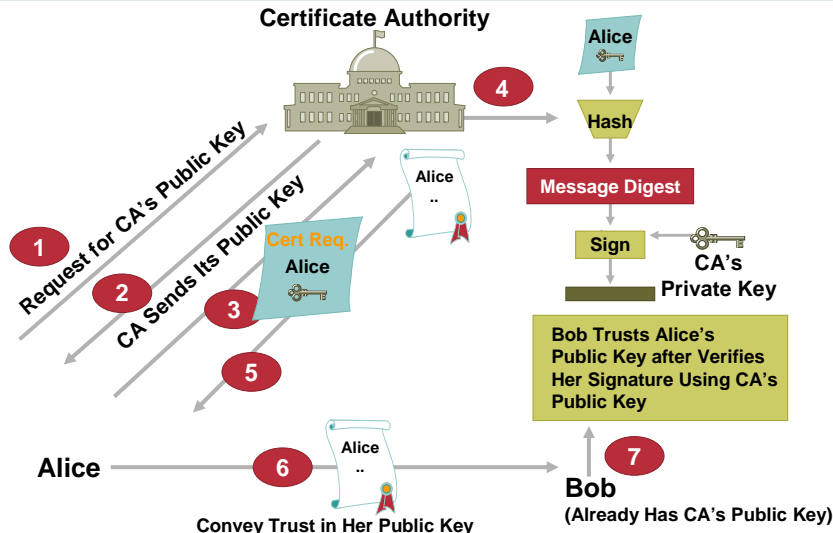
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

48

# Digital Certification

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

49

# Simple Certificate Enrollment Protocol (SCEP)

Cisco.com

- A PKI communication protocol that supports secure issuance certificates to network device in a scalable manner
- Use existing PKCS standards:
  - PKCS #1, RSA algorithms
  - PKCS #7, digital signature, digital envelop
  - PKCS #10, certificate request syntax
- Uses HTTP as transport for certificate enrollment, access
- Uses LDAP or HTTP for CRL support

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

50

# Agenda

Cisco.com

- **Analysis of Baseline IPSec Functionality**
  - IKE: IPSec Negotiation Protocol Flow
  - PKI: IPSec Authentication Architecture
  - SHA and MD5: IPSec Hashing Mechanisms**
  - DES and AES: IPSec Encryption Techniques
- **Analysis of the Enhancements in IPSec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPSec Negotiation Protocol Flow
  - Multicast IPSec
  - Major IPSec Enhancements in the works

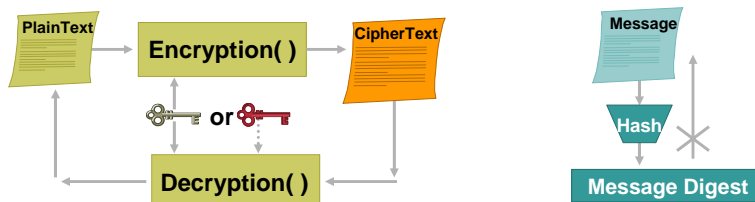
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

51

# Encryption vs. Hashing

Cisco.com



- Encryption keeps communications private
- Private
- Encryption and decryption can use same or different keys
- Achieved by various algorithms, e.g. DES, CAST
- Need key management

- Hash transforms message into fixed-size string
- One-way hash function
- Strongly collision-free hash
- Message digest can be viewed as “digital fingerprint”
- Used for message integrity check and digital certificates
- Hash is generally faster than encryption

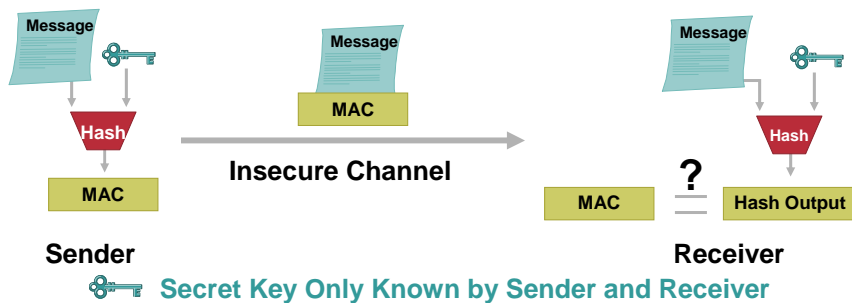
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

52

# Message Authentication and Integrity Check Using Hash

Cisco.com



- MAC (Message Authentication Code): cryptographic checksum generated by passing data thru a message authentication algorithm
- MAC is often used for message authentication and integrity check
- HMAC—keyed hashed-based MAC

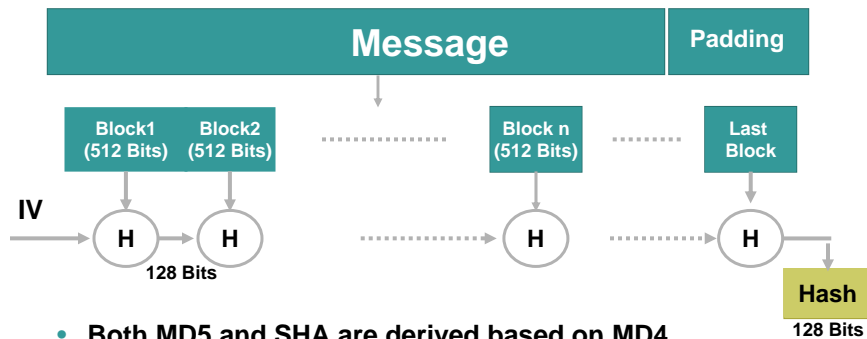
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

53

# Commonly Used Hash Functions (MD5 and SHA)

Cisco.com



- Both MD5 and SHA are derived based on MD4
- MD5 provides 128-bit output, SHA provide 160-bit output; (only first 96 bits used in IPSec)
- Both of MD5 and SHA are considered **one-way strongly collision-free** hash functions
- SHA is computationally slower than MD5, but more secure

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

54

# Agenda

Cisco.com

- **Analysis of Baseline IPsec Functionality**
  - IKE: IPsec Negotiation Protocol Flow
  - PKI: IPsec Authentication Architecture
  - SHA and MD5: IPsec Hashing Mechanisms
  - DES and AES: IPsec Encryption Techniques**
- **Analysis of the Enhancements in IPsec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPsec Negotiation Protocol Flow
  - Multicast IPsec
  - Major IPsec Enhancements in the works

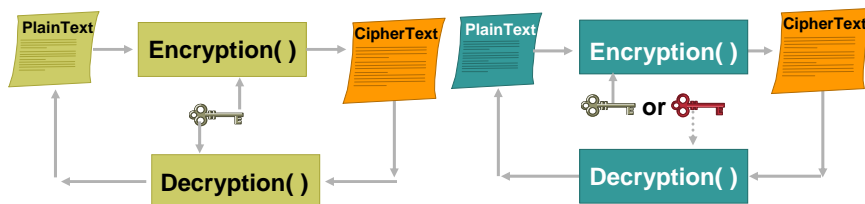
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

55

# Symmetric vs. Asymmetric Encryption Algorithms

Cisco.com



- Secret-key cryptography
- Encryption and decryption use the same key
- Typically used to encrypt the content of a message
- Examples: DES

- Public-key cryptography
- Encryption and decryption use different keys
- Typically used in digital certification and key management
- Examples: Diffie-Hellman, RSA

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

56

# Data Encryption Standard (DES)

Cisco.com

- **Symmetric key encryption algorithm**
- **Block cipher: works on 64-bit data block, use 56-bit key (last bit of each byte used for parity)**
- **Mode of operation: how to apply DES to encrypt blocks of data**

Electronic Code Book (ECB)

Cipher Block Chaining (CBC)

K-bit Cipher FeedBack (CFB)

K-bit Output FeedBack (OFB)

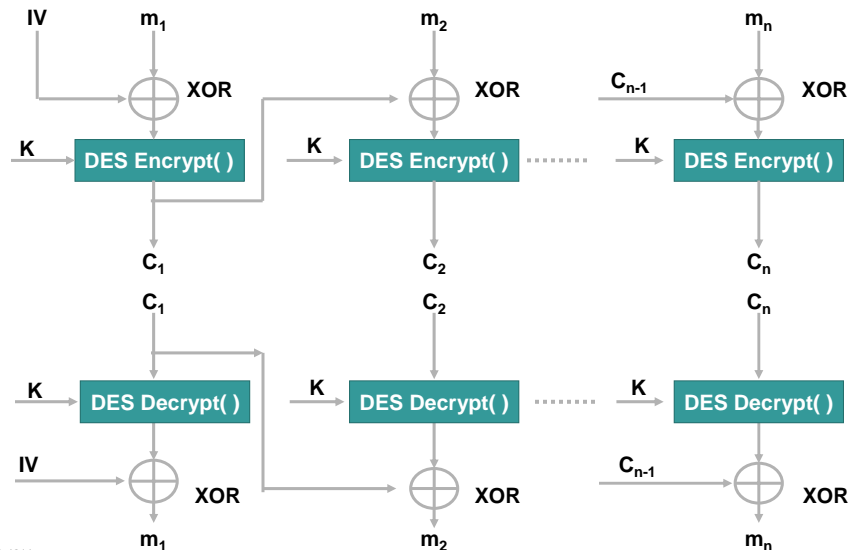
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

57

# DES CBC Mode

Cisco.com



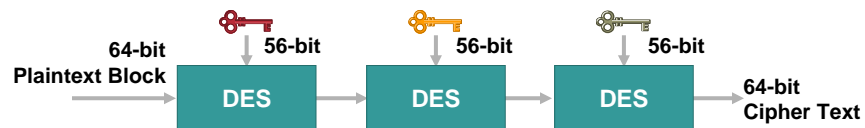
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

58

## Triple-DES

Cisco.com



- 168-bit total key length
- Mode of operation decides how to process DES three times
- Normally: encrypt, decrypt, encrypt
- More secure than DES but slower
- **So is 3DES optimally the fastest, the easiest to implement and the securest algorithm out there?**

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

59

## AES: the New Encryption Standard

Cisco.com

- 'Advanced Encryption Standard' formerly known as 'Rijndael'
- Successor to DES and 3DES
- Will ultimately become the default ESP cipher
- Symmetric key block cipher
- Strong encryption with long expected life
- AES can support 128, 192 and 256 keys strengths but 128 is considered safe
- HMAC-SHA-1 and HMAC-MD5 can serve as the IKE generators of the 128 bit AES keys

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

60

## AES: Pseudo Code

Cisco.com

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w[0, Nb-1])
  for round = 1 step 1 to Nr-1
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
  end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
  out = state
end
```

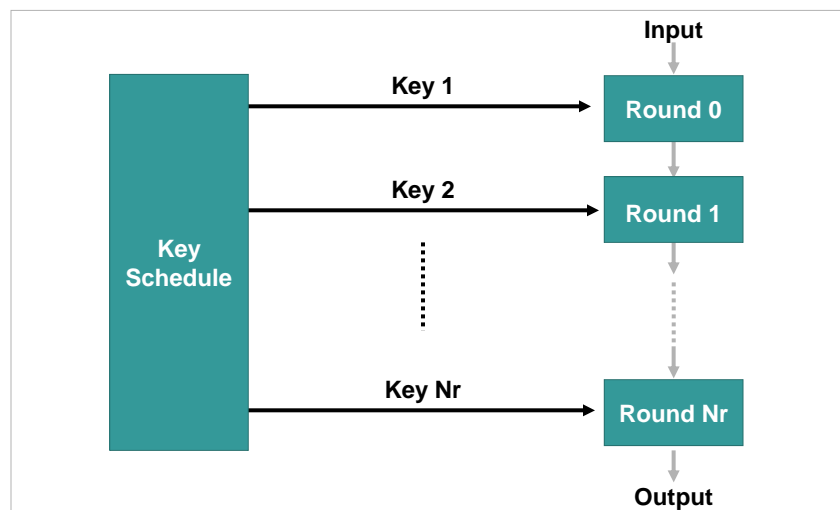
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

61

## AES: The Complete Cipher

Cisco.com



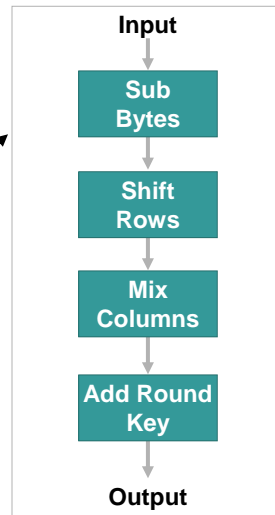
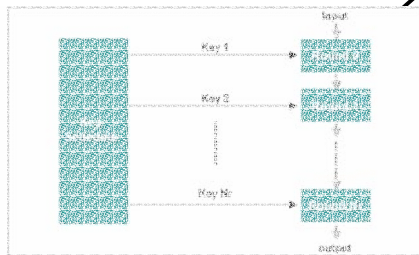
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

62

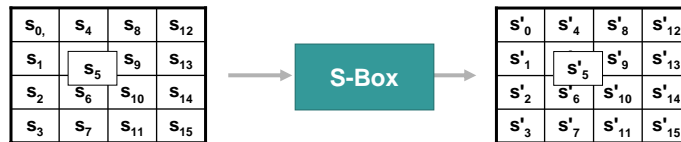
# AES: Individual Rounds

Note: Last Round Is Slightly Different from the Rest of the Rounds



# AES Functions: SubBytes and ShiftRows

## SubBytes



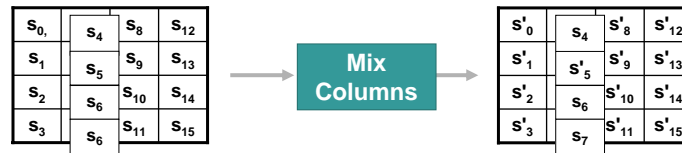
## ShiftRows



# AES Functions: MixColumns and AddRoundKey

Cisco.com

## MixColumns



## AddRoundKey



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

65

# Agenda

Cisco.com

- **Analysis of Baseline IPsec Functionality**
  - IKE: IPsec Negotiation Protocol Flow
  - PKI: IPsec Authentication Architecture
  - SHA and MD5: IPsec Hashing Mechanisms
  - DES and AES: IPsec Encryption Techniques
- **Analysis of the Enhancements in IPsec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPsec Negotiation Protocol Flow
  - Multicast IPsec
  - Major IPsec Enhancements in the works

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

66

# Remote Access Features

Cisco.com

- Mode config
- Extended authentication

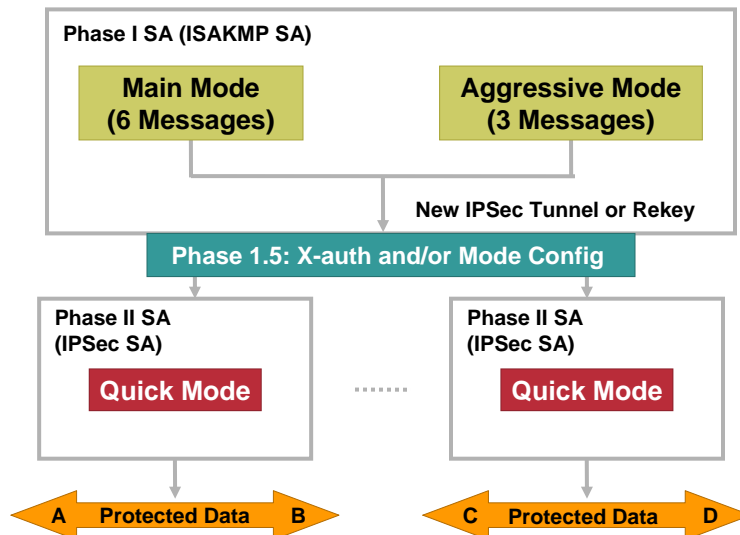
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

67

# Placement of Mode Config and X-auth in IKE

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

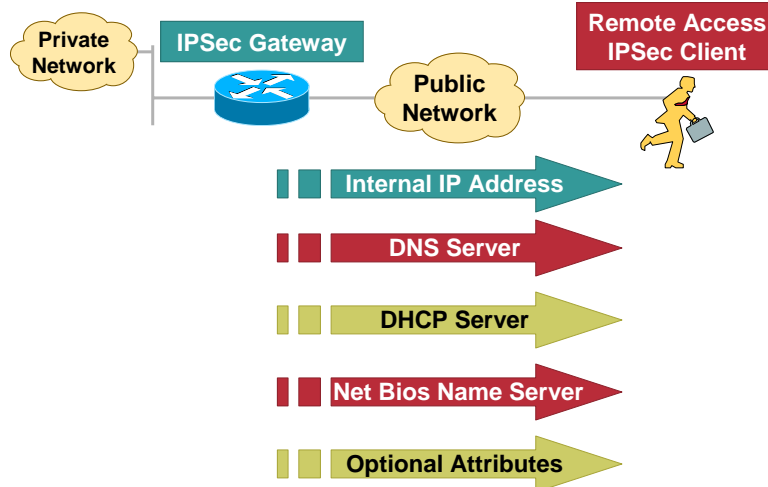
© 2004, Cisco Systems, Inc. All rights reserved.

68

# Mode Config

Cisco.com

## Mechanism Used to Push Attributes to Remote Access IPsec Clients



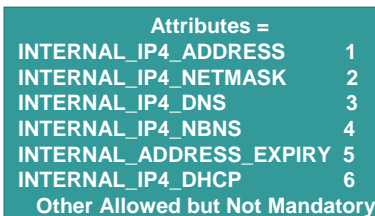
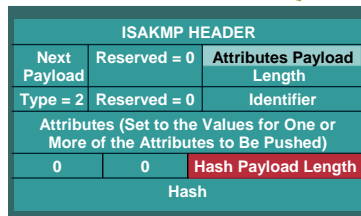
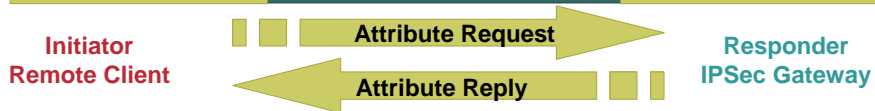
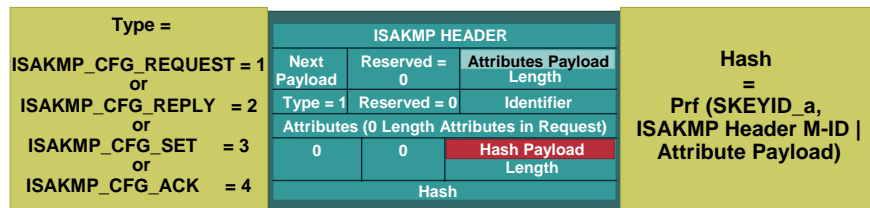
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

69

# Mode Config Protocol Specifications

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

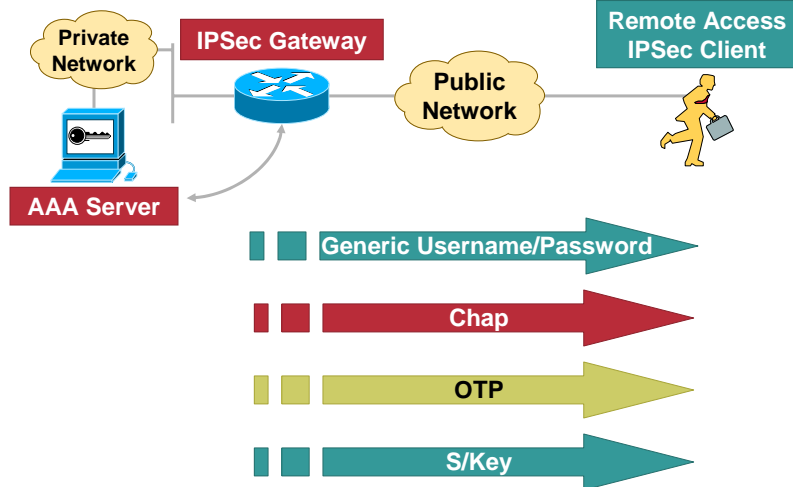
© 2004, Cisco Systems, Inc. All rights reserved.

70

# X-auth

Cisco.com

## Mechanism Used to Perform Per User Authentication for RA Clients



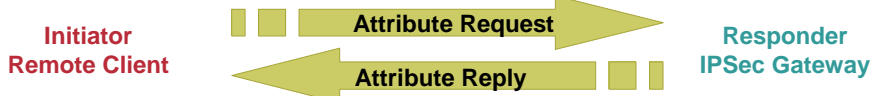
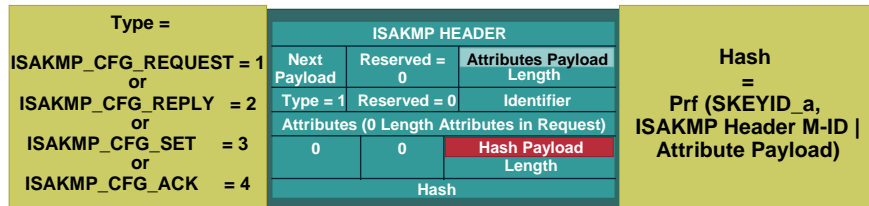
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

71

# X-auth Protocol Specifications

Cisco.com



ISAKMP HEADER			Attributes =	
Next Payload	Reserved = 0	Attributes Payload Length	XAUTH_TYPE	16520
Type = 2	Reserved = 0	Identifier	XAUTH_USER_NAME	16521
Attributes (Set to the Values for One or More of the Attributes to Be Pushed)			XAUTH_USER_PASSWORD	16522
0	0	Hash Payload Length	XAUTH_PASSCODE	16523
Hash			XAUTH_MESSAGE	16524
			XAUTH_CHALLENGE	16525
			XAUTH_DOMAIN	16526
			XAUTH_STATUS	16527

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

72

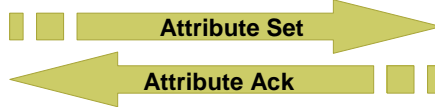
# X-auth Protocol Specifications

Cisco.com

Type =  
 ISAKMP\_CFG\_REQUEST = 1  
 or  
 ISAKMP\_CFG\_REPLY = 2  
 or  
 ISAKMP\_CFG\_SET = 3  
 or  
 ISAKMP\_CFG\_ACK = 4

ISAKMP HEADER		
Hash	Reserved = 0	Attributes Payload Length
Type = 3	Reserved = 0	Identifier
Attributes (X-auth Status = OK or FAIL)		
0	0	Hash Payload Length
Hash		

Initiator  
IPSec Gateway



Responder  
IPSec Client

ISAKMP HEADER		
Hash	Reserved = 0	Attributes Payload Length
Type = 4	Reserved = 0	Identifier
Attributes (None Included)		
0	0	Hash Payload Length
Hash		

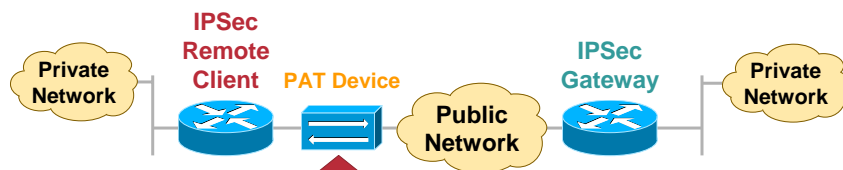
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

73

# IPSec and NAT: The Problem

Cisco.com



Port Address Translation Fails since in ESP Packets L4 Port Info Is Encrypted

SEC-4011  
9831\_05\_2004\_X2

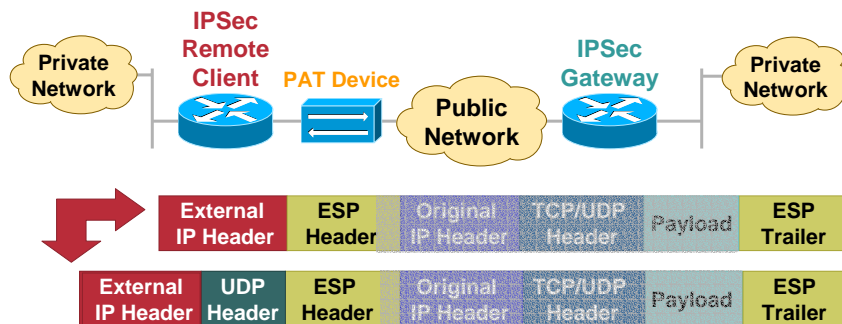
© 2004, Cisco Systems, Inc. All rights reserved.

74

# Need Based NAT Traversal with IPSec over TCP or UDP

Cisco.com

- **Step 1:** Detect support for bi-directional NAT Traversal
- **Step 2:** Discover existence of NAT in IPSec path
- **Step 3:** Negotiate NAT traversal encapsulation
- **Step 4:** Begin encapsulation of packets



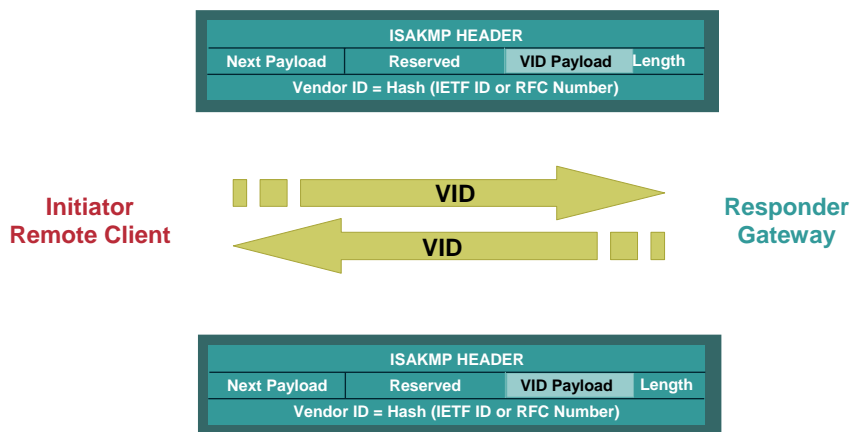
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

75

# Step 1: Detect Support for Bi-Directional NAT Traversal

Cisco.com



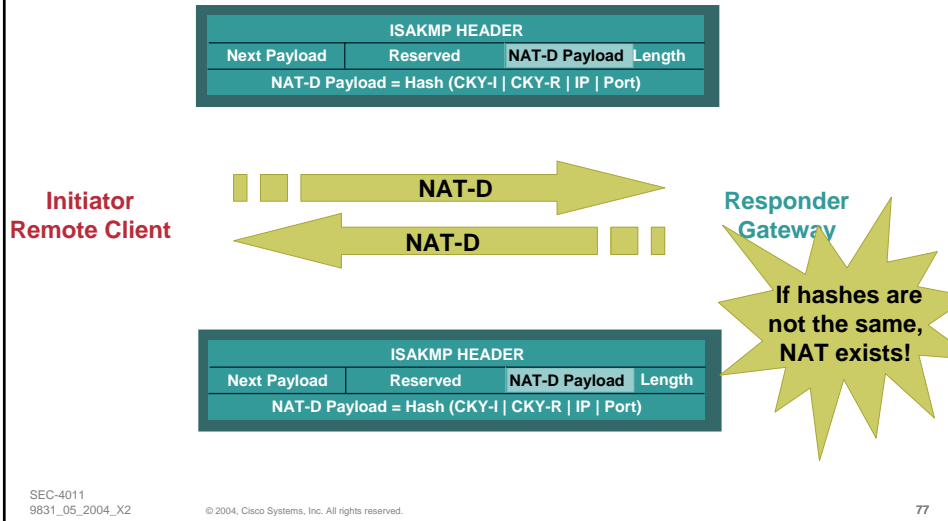
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

76

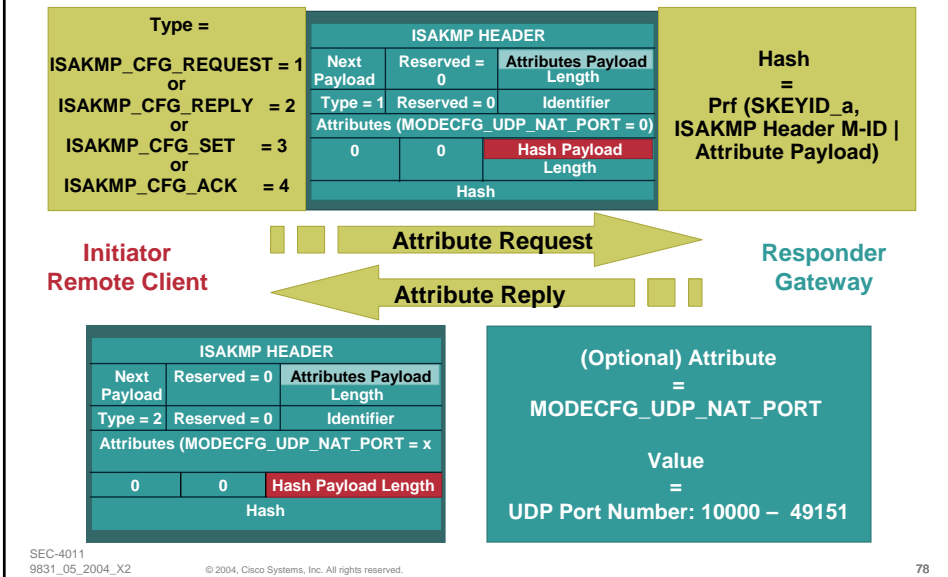
## Step 2: Discover Existence of NAT in IPsec path

Cisco.com



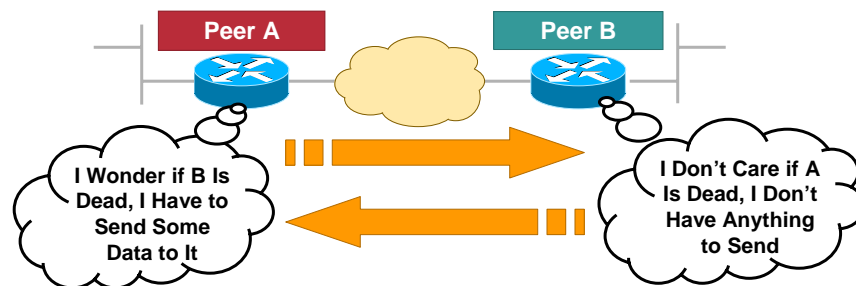
## Step 3: Negotiate NAT Traversal Encapsulation (shown here for UDP)

Cisco.com



## Dead Peer Discovery

Cisco.com



Passage of IPsec Traffic Is Proof of Liveliness

DPD Is Asynchronous

Each Peer Sets Its Own WORRY METRIC

Check on Peer Only if there Is a Need to Do So

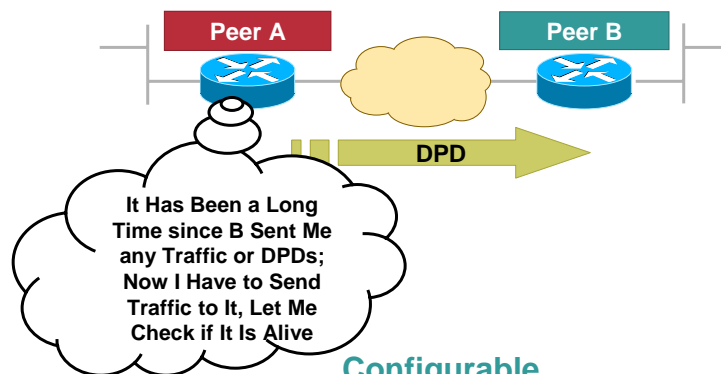
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

79

## Cisco's DPD Worry Metric

Cisco.com



Configurable

Idle Time between Data and DPD Traffic before which No DPDs Sent

DPD Only Used when there Is Data to Send

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

80

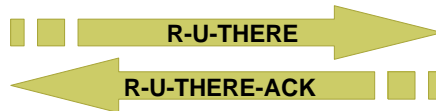
# DPD Protocol Specifications

Cisco.com

Vendor ID Payload Is Exchanged in IKE Negotiation Beforehand

ISAKMP HEADER			
Next Payload	Reserved	Notify Payload	Length
DOI = IPsec DOI			
Protocol ID = ISAKMP	SPI SIZE	Notify Message Type = R-U-THERE	
SPI = CKY-I   CKY-R			
Notification Data = Sequence Number			

Initiator



Responder

ISAKMP HEADER			
Next Payload	Reserved	Notify Payload	Length
DOI = IPsec DOI			
Protocol ID = ISAKMP	SPI SIZE	Notify Message Type = R-U-THERE	
SPI = CKY-I   CKY-R			
Notification Data = Sequence Number			

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

81

# Agenda

Cisco.com

- **Analysis of Baseline IPsec Functionality**
  - IKE: IPsec Negotiation Protocol Flow
  - PKI: IPsec Authentication Architecture
  - SHA and MD5: IPsec Hashing Mechanisms
  - DES and AES: IPsec Encryption Techniques
- **Analysis of the Enhancements in IPsec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPsec Negotiation Protocol Flow**
  - Multicast IPsec
  - Major IPsec Enhancements in the works

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

82

## IKE v2: Replacement for Current IKE Specification

Cisco.com

- **Feature preservation**

Most of the features and characteristics of the baseline parent IKE v1 protocol are being preserved in v2

- **Compilation of features and extensions**

Quite a few features that were added on top of the baseline IKE protocol functionality in v1 are being reconciled into the mainline v2 framework

- **New features**

A few new mechanisms and features are being introduced in the IKE v2 protocol as well

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

83

## IKE v2: What Is Not Changing

Cisco.com

- **Features in v1 that have been debated but are ultimately being preserved in v2**

Most payloads reused

Use of nonces to ensure uniqueness of keys

- **v1 extensions and enhancements being merged into mainline v2 specification**

Use of a 'configuration payload' similar to MODECFG for address assignment

'X-auth' type functionality retained through EAP

Use of NAT Discovery and NAT Traversal techniques

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

84

## IKE v2: What Is Changing

Cisco.com

- **Significant changes being made to the baseline functionality of IKE**

Use of suites for algorithm negotiation

EAP adopted as the method to provide legacy authentication integration with IKE

Public Signature keys and pre-shared keys, the only methods of IKE authentication

Use of 'stateless cookie' to avoid certain types of DOS attacks on IK

Continuous phase of negotiation

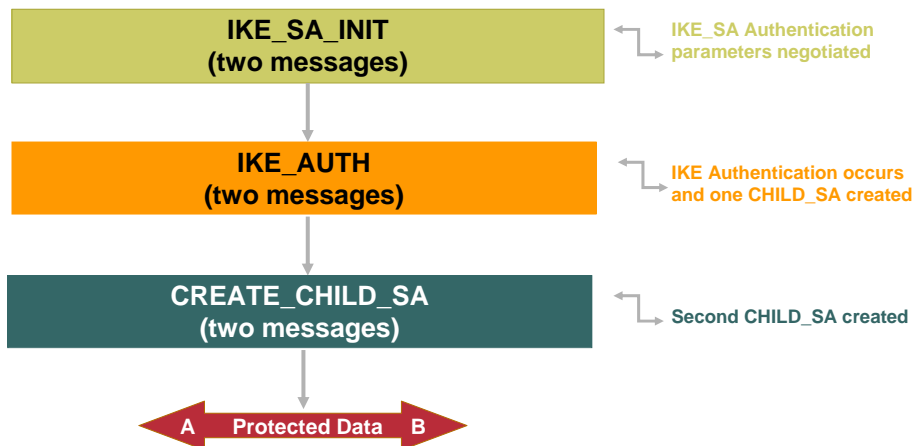
SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

85

## How Does IKE v2 Work?

Cisco.com



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

86

# IKE\_SA\_INIT: 'Message 1'

Cisco.com

The Initiator Proposes basic SA attributes along with authentication material



Initiator SPI				
Responder SPI (Left 0 for Now)				
Next Payload	Version	Exchange	Flags	
Message ID				
Total Message Length				
Next Payload	C	0	SA Payload	Length
SA Payload (Includes Proposal and Transform info)				
Next Payload	C	0	KE Payload	Length
Key Exchange Payload (Incls. DH Public Value)				
Next Payload	C	0	Nonce Payload	Length
Nonce				

Critical Bit: Request rejection of entire message if this payload not understood

DH Public value is guessed

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

87

# IKE\_SA\_INIT: 'Message 2'

Cisco.com

The Responder Sends Back the One Set of Attributes Acceptable to It along with authentication material



Initiator SPI (Same as Before)				
Responder SPI (Calculated and Inserted Here)				
Next Payload	Version	Exchange	Flags	
Message ID				
Total Message Length				
Next Payload	C	0	SA Payload	Length
SA Payload (Includes Proposal and Transform info)				
Next Payload	C	0	KE Payload	Length
Key Exchange Payload (Incls. DH Public Value)				
0	C	0	Nonce Payload	Length
Nonce				

Includes accepted transforms and proposals

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

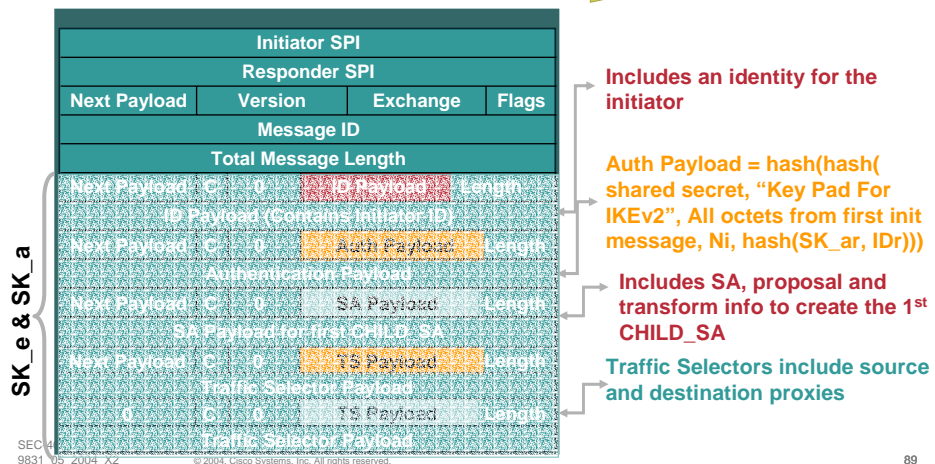
88

# IKE\_AUTH: 'Message 3'

Cisco.com

Authentication material along with CHILD\_SA info sent

Initiator → Responder



SEC-9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

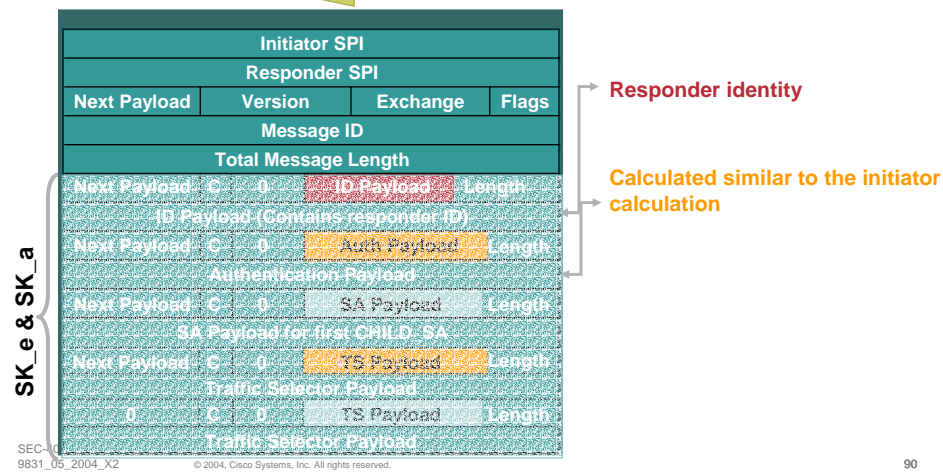
89

# IKE\_AUTH: 'Message 4'

Cisco.com

Authentication material along with CHILD\_SA info sent

Responder ← Initiator



SEC-9831\_05\_2004\_X2

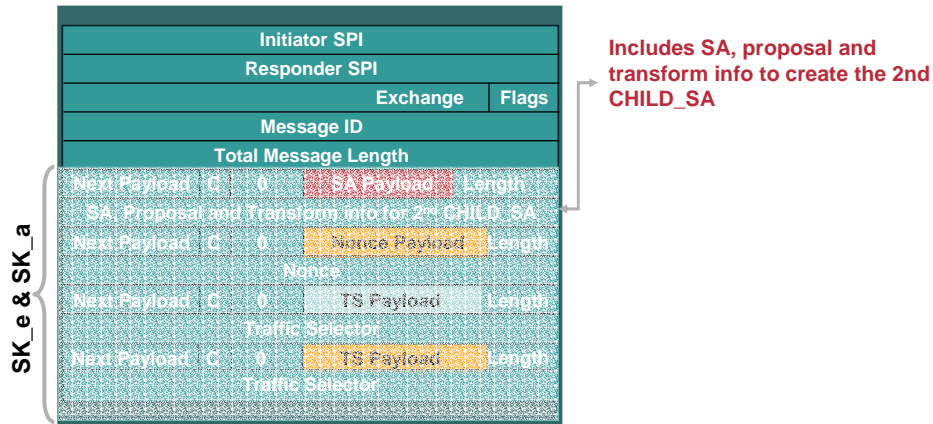
© 2004, Cisco Systems, Inc. All rights reserved.

90

# CREATE\_CHILD\_SA: 'Message 5'

Cisco.com

The Initiator Sends Its Authentication Material and ID



SEC-4011  
9831\_05\_2004\_X2

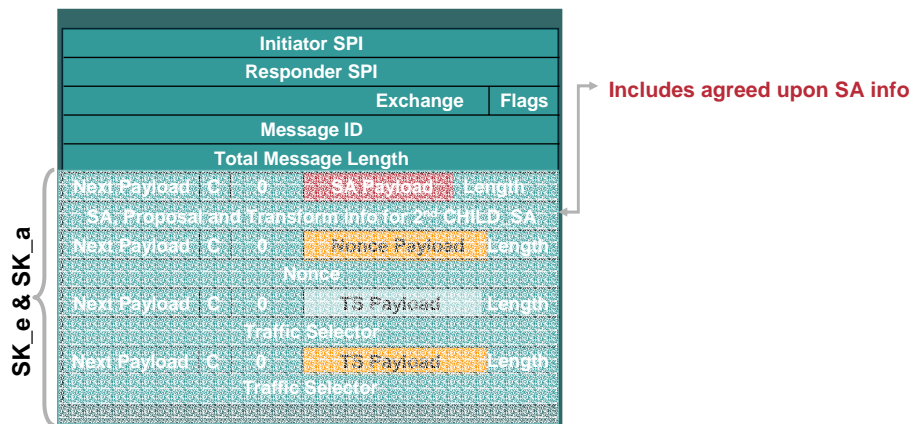
© 2004, Cisco Systems, Inc. All rights reserved.

91

# CREATE\_CHILD\_SA: 'Message 6'

Cisco.com

The responder Sends Its Authentication Material and ID



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

92

## Agenda

Cisco.com

- **Analysis of Baseline IPSec Functionality**
  - IKE: IPSec Negotiation Protocol Flow
  - PKI: IPSec Authentication Architecture
  - SHA and MD5: IPSec Hashing Mechanisms
  - DES and AES: IPSec Encryption Techniques
- **Analysis of the Enhancements in IPSec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPSec Negotiation Protocol Flow
  - Multicast IPSec**
  - Major IPSec Enhancements in the works

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

93

## What Is a Multicast Group?

Cisco.com

- **Two or more parties who send and receive the same data transmitted over a network**
- **Packet delivery can be multicast, or unicast (where identical data is directed to each group member)**
- **Group members can be routers, PCs, telephones, any IP device**
- **There are many different examples of group topologies**

SEC-4011  
9831\_05\_2004\_X2

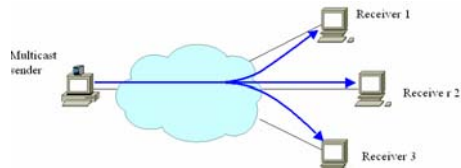
© 2004, Cisco Systems, Inc. All rights reserved.

94

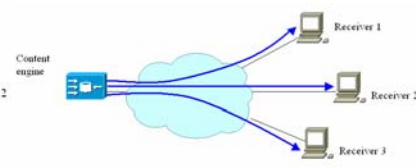
# Multicasting

Cisco.com

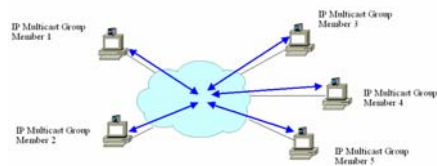
## Single-Source Multicast



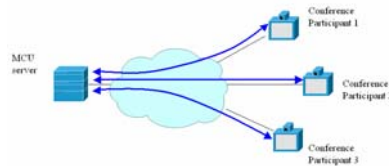
## Publish-Subscribe



## Multiple-Source Multicast



## Multipoint Control Unit



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

95

# Securing Multicast Groups

Cisco.com

## What Is Needed to Secure Group Traffic?

- **Policy distribution**

Distribution of the knowledge that group traffic is protected, and what is needed to participate in the group

- **Protect the data in transit**

Only group members should be able to participate in the group

Non-group members should not be able to spoof or disrupt group communication

- **Deliver keys to all group members**

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

96

## Solution: GDOI and Key Server

Cisco.com

- **Group Domain of Interpretation (GDOI)**
  - Re-uses IKE protocols and definitions
  - IETF MSEC Internet Draft stage
- **Key server method**
  - A key server (known as group controller/key server or GCKS) unilaterally chooses the keys
  - Group members join by registering with the key server
  - The key server replaces keys when a group member leaves
  - Can scale to very large groups by using multiple collaborating key servers

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

97

## GDOI Overview

Cisco.com

- **Distributes keys and policy for groups**
  - Security associations and keys
- **Can efficiently re-key the group when needed**
  - When a member joins/leaves the group
  - When an existing SA is about to expire
- **Quickly and efficiently eject a group member**

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

98

## GDOI Protocol Flow

Cisco.com

- **Two phases**

IKE phase 1 protocol

GROUPKEY-PULL protocol



- **Security protections**

IKE phase 1 provides authentication, confidentiality, and integrity

GROUPKEY-PULL protocol provides authorization and replay protection

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

99

## GDOI Phase 2 Protocol

Cisco.com

Member Requests to Join Group Using an ID Payload



Key Server Returns Policy in SA Payload



Group Member

Member Agrees to Policy

GCKS

Key Server Returns Keys Using a KD Payload

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

100

## GDOI Rekey GROUPKEY-PUSH Message

Cisco.com

- **One message exchange**
  - Sent from key server to all group members
  - IP multicast message is the most efficient distribution
- **Security protections**
  - Authentication/integrity provided by a digital signature on the message
  - Confidentiality provided using keys distributed during GDOI registration
  - Replay protection through use of a message sequence number



SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

101

## Agenda

Cisco.com

- **Analysis of Baseline IPsec Functionality**
  - IKE: IPsec Negotiation Protocol Flow
  - PKI: IPsec Authentication Architecture
  - SHA and MD5: IPsec Hashing Mechanisms
  - DES and AES: IPsec Encryption Techniques
- **Analysis of the Enhancements in IPsec**
  - Remote Access Features, NAT Traversal, DPD
  - IKE v2: New IPsec Negotiation Protocol Flow
  - Multicast IPsec
  - Major IPsec Enhancements in the works**

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

102

## Major IPSec Enhancements in the Works

Cisco.com

- **Sequence Number Extensions**

Increased range of sequence numbers

Overcomes the issue of sequence number exhaustion when large quantities of data are processed

Need to rekey SA to refresh sequence numbers eliminated

Security risk: Less rekeying contains inherent risk and needs to be controlled through other restraints

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

103

## Major IPSec Enhancements in the Works

Cisco.com

- **IPSec Cryptographic Suites**

Commonly used combinations of IKE and IPSec algorithms combined into standardized and named suites

Example: 'VPN-A'

**IPsec:**

Protocol	ESP [RFC2406]
ESP encryption	TripleDES in CBC mode [RFC2451]
ESP integrity	HMAC-SHA1-96 [RFC2404]

**IKE and IKEv2:**

Encryption	TripleDES in CBC mode [RFC2451]
Pseudo-random function	HMAC-SHA1 [RFC2104]
Integrity	HMAC-SHA1-96 [RFC2404]
Diffie-Hellman group	1024-bit MODP [RFC2409]

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

104

## Major IPSec Enhancements in the Works

Cisco.com

- **IPSec Cryptographic Suites**

Commonly used combinations of IKE and IPSec algorithms combined into standardized and named suites

Example: 'VPN-A'

**IPsec:**

Protocol	ESP [RFC2406]
ESP encryption	TripleDES in CBC mode [RFC2451]
ESP integrity	HMAC-SHA1-96 [RFC2404]

**IKE and IKEv2:**

Encryption	TripleDES in CBC mode [RFC2451]
Pseudo-random function	HMAC-SHA1 [RFC2104]
Integrity	HMAC-SHA1-96 [RFC2404]
Diffie-Hellman group	1024-bit MODP [RFC2409]

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

105

## Agenda

Cisco.com

- **Analysis of Baseline IPSec Functionality**

IKE: IPSec Negotiation Protocol Flow

PKI: IPSec Authentication Architecture

SHA and MD5: IPSec Hashing Mechanisms

DES and AES: IPSec Encryption Techniques

- **Analysis of the Enhancements in IPSec**

Remote Access Features, NAT Traversal, DPD

IKE v2: New IPSec Negotiation Protocol Flow

Multicast IPSec

Major IPSec Enhancements in the works

SEC-4011  
9831\_05\_2004\_X2

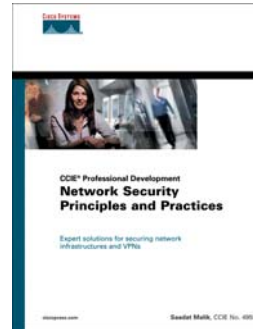
© 2004, Cisco Systems, Inc. All rights reserved.

106

## Recommended Reading

Cisco.com

- Continue your Networkers learning experience with further reading for this session from Cisco Press.
- Check the Recommended Reading flyer for suggested books.



Available on-site at the Cisco Company Store

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

107

## Complete Your Online Session Evaluation!

Cisco.com

- WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing
- WHY:** Win fabulous prizes! Give us your feedback!
- WHERE:** Go to the Internet stations located throughout the Convention Center
- HOW:** Winners will be posted on the onsite Networkers Website; four winners per day

SEC-4011  
9831\_05\_2004\_X2

© 2004, Cisco Systems, Inc. All rights reserved.

108

**CISCO SYSTEMS**

