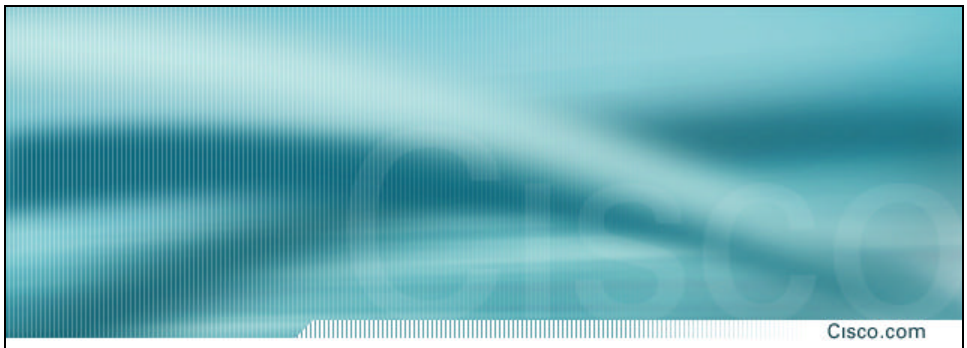
NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.



Advanced IPSec Algorithms and Protocols

Session SEC-4010

Saadat Malik

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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

Agenda

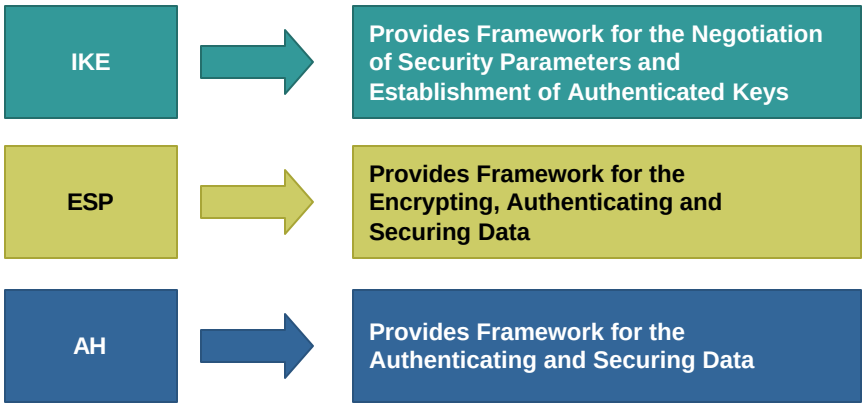
Cisco.com

- 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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

IPSec Composition

Cisco.com

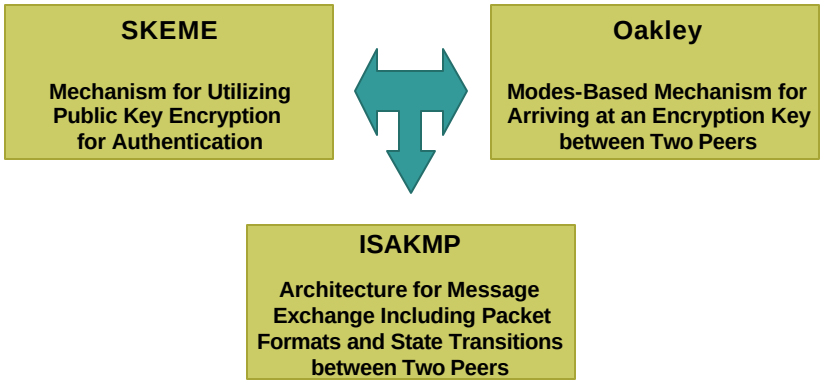
IPSec Combines Three Main Protocols into a Cohesive Security Framework



What Is IKE?

Cisco.com

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



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**

How Does IKE Work?

Cisco.com

IKE Is a TWO Phase Protocol

Phase 1 Exchange

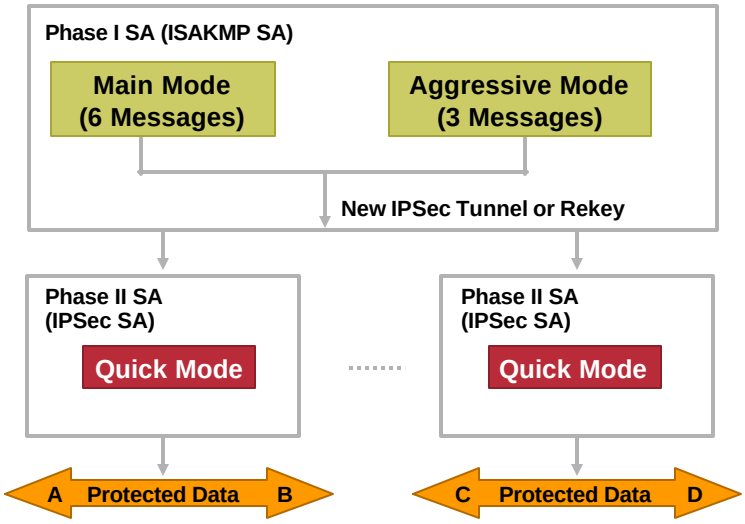
Peers Negotiate a Secure, Authenticated Channel with which to Communicate 'Main Mode'
or 'Aggressive Mode' Accomplish a Phase I Exchange

Phase 2 Exchange

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

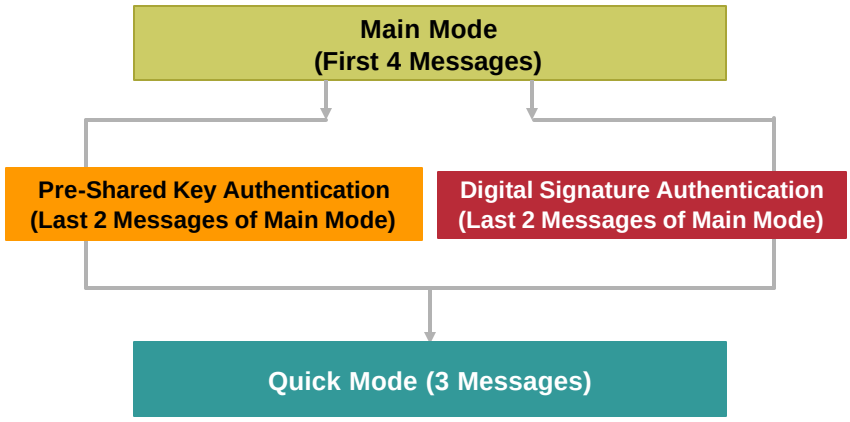
How Does IKE Work?

Cisco.com



Presentation Flow

Cisco.com



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

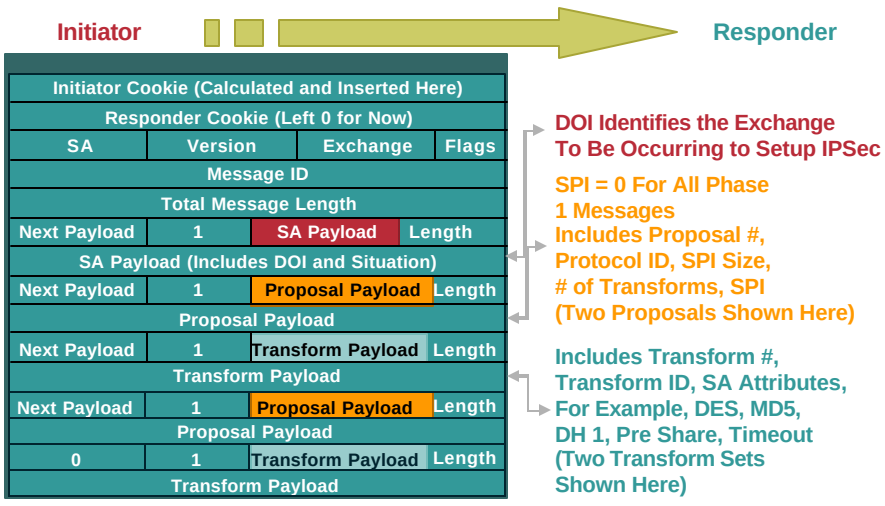
A 8 Byte Pseudo-Random Number Used for Anti-Clogging

CKY-R = md5{(src_ip, dest_ip), Random Number}

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

Cisco.com

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



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

Cisco.com

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

Initiator ← Responder

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

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

DH Public Value = X_a

$X_a = g^a \bmod p$

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

DH Public Value = X_b

$X_b = g^b \bmod p$

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

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
Initiator Nonce = N_i

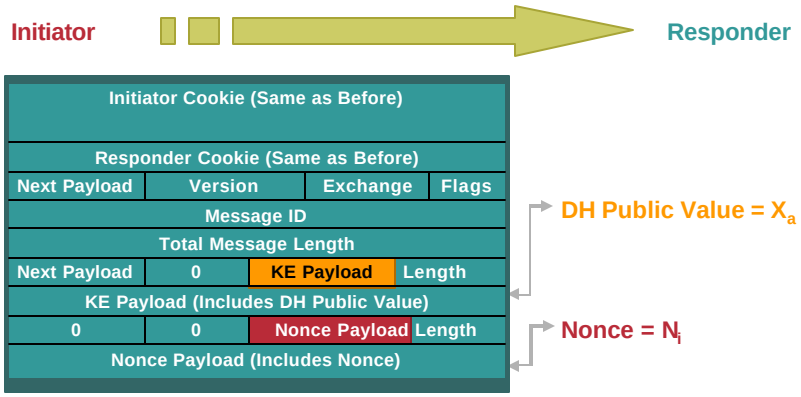
Generation of a Nonce by Responder

Nonce Is a Very Large Random Number
Responder Nonce = N_r

IKE Phase 1 (Main Mode): Sending 'Message 3'

Cisco.com

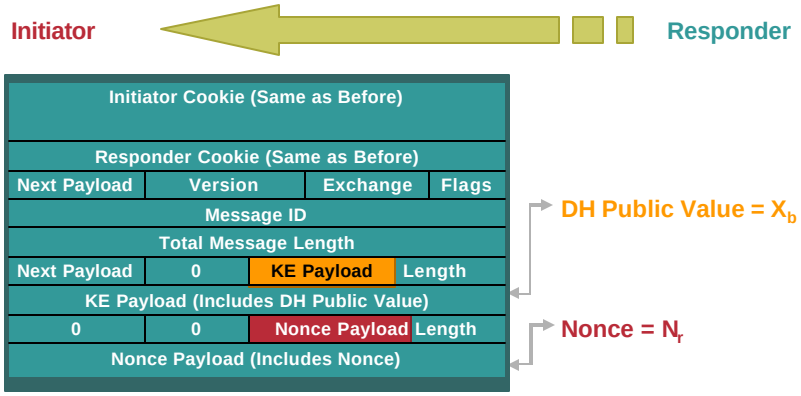
The Initiator Sends Its DH Public Value X_a and Nonce N_i



IKE Phase 1 (Main Mode): Sending 'Message 4'

Cisco.com

The Responder Sends Its DH Public Value X_b and Nonce N_r



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 = $(X_b)^a \bmod p$

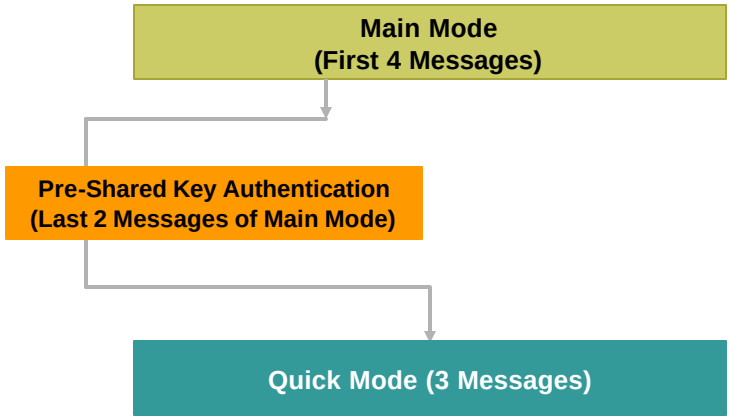
$(X_b)^a \bmod p = (X_a)^b \bmod p = g^{ab}$

Calculation of the Shared DH Secret by Responder

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

Presentation Flow

Cisco.com



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

PRF = A Pseudo Random Function Based on the Negotiated Hash

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

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

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

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

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

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

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

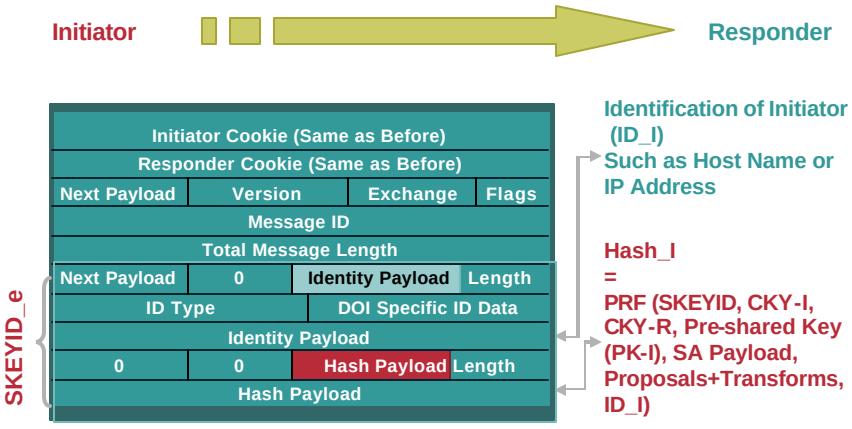
$SKEYID\_a = PRF (SKEYID, SKEYID\_d \mid g^{ab} \mid CKY\text{-}I \mid CKY\text{-}R \mid 1)$

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

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

Cisco.com

The Initiator Sends Its Authentication Material and ID

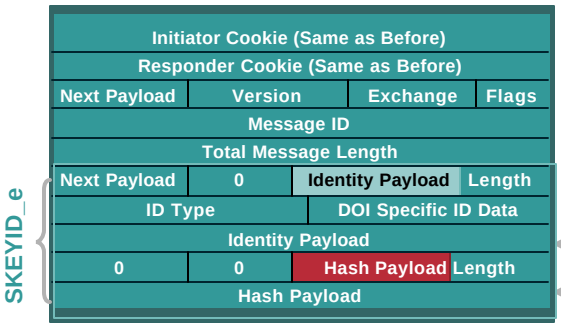


IKE Phase 1 (Main Mode): (Pre-Shared Keys) Sending 'Message 6'

Cisco.com

The Responder Sends Its Authentication Material and ID

Initiator ⟵ Responder



Identification of Responder (ID_R)
Such as Host Name or IP Address

Hash_R
=
PRF (SKEYID, CKY-I, CKY-R, Pre-Shared Key (PK-R), SA Payload, Proposals+Transforms, ID_R)

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!!

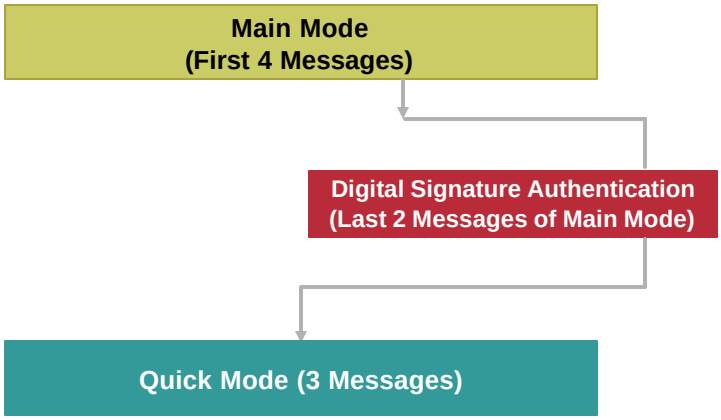
ISAKMP SA Established!

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!!

Presentation Flow

Cisco.com



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

$SKEYID = PRF (N_i \mid N_r, g^{ab})$

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

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

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

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

$SKEYID = PRF(N_i \mid N_r, g^{ab})$

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

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

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

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

Cisco.com

The Initiator Sends Its Authentication Material and ID

Initiator → Responder

Initiator Cookie (Same as Before)			
Responder Cookie (Same as Before)			
KE	Version	Exchange	Flags
Message ID			
Total Message Length			
Next Payload	0	Identity Payload	Length
ID Type		DOI Specific ID Data	
Identity Payload			
Next Payload	0	Signature Payload	Length
Signature Data			
0	0	Certificate Payload Length	
Certificate Encoding	Certificate Data		
Certificate Data			

SKEYID_e

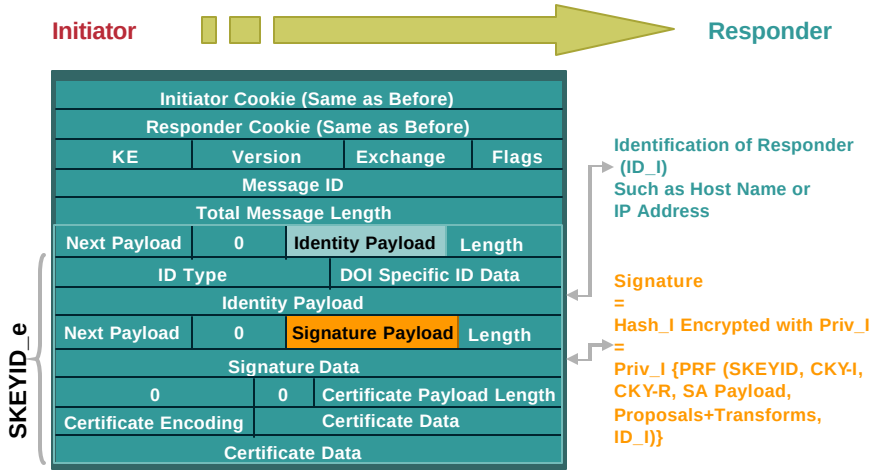
Identification of Responder (ID_I) Such as Host Name or IP Address

Signature = Hash_I Encrypted with Priv_I = Priv_I {PRF (SKEYID, CKY-I, CKY-R, SA Payload, Proposals+Transforms, ID_I)}

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

Cisco.com

The Responder Sends Its Authentication Material and ID



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!!

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_a'
$X_a' = g^a \bmod p$
Where g Is the Generator and p a Large Prime Number and a Is a Private Secret Known Only to the Initiator

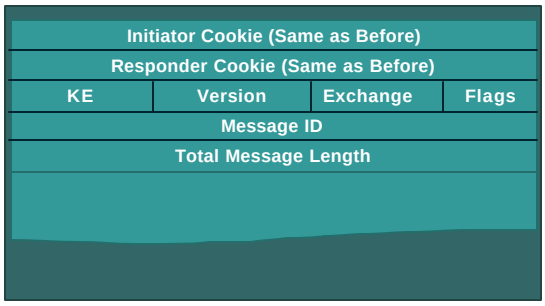
Execution of DH by Responder Again to Ensure PFS

New Nonce Generated: Nr'
New DH Public Value = X_b'
$X_b' = g^b \bmod p$
Where g Is the Generator and p a Large Prime Number and b Is a Private Secret Known Only to the Responder

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

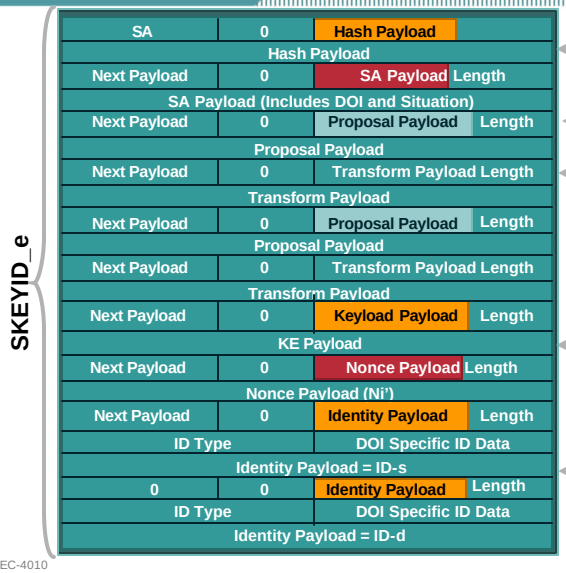
Cisco.com

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



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

Cisco.com



Hash =PRF (SKEYID_a, Message ID, Ni', Proposals+ Transforms, X_a)

Proposal: ESP or AH, SHA or MD5, DH 1 or 2, SPI (Two Proposals Shown Here)

Transform: Tunnel or Transport, IPSec Timeout

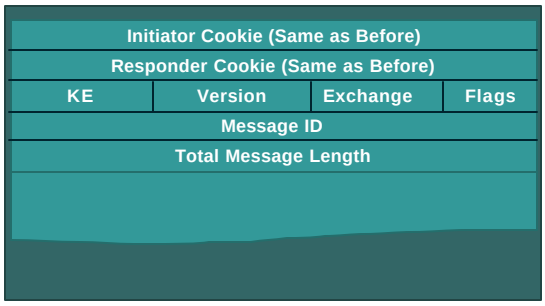
KE Payload = X_a'

ID-s = Source Proxy
ID-d = Destination Proxy

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

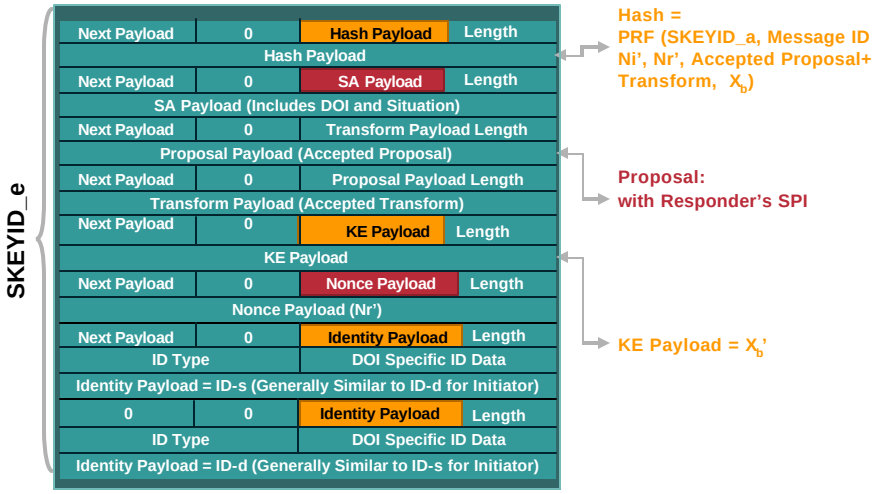
Cisco.com

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



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

Cisco.com



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

Cisco.com

Initiator Generates IPSec Keying Material

1. Generate new DH shared sSecret = $(X_b')^a \bmod p$
2. IPSec session key = PRF (SKEYID_d, protocol (ISAKMP), new DH shared secret, SPI_r, N_i', N_r')

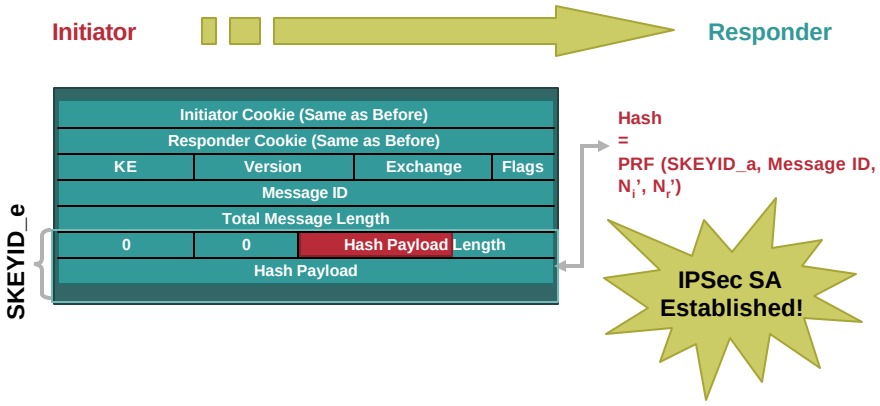
Responder Generates IPSec Keying Material

1. Generate new DH shared secret = $(X_a')^b \bmod p$
2. IPSec session key = PRF (SKEYID_d, protocol (ISAKMP), new DH shared secret, SPI_i, N_i', N_r')

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

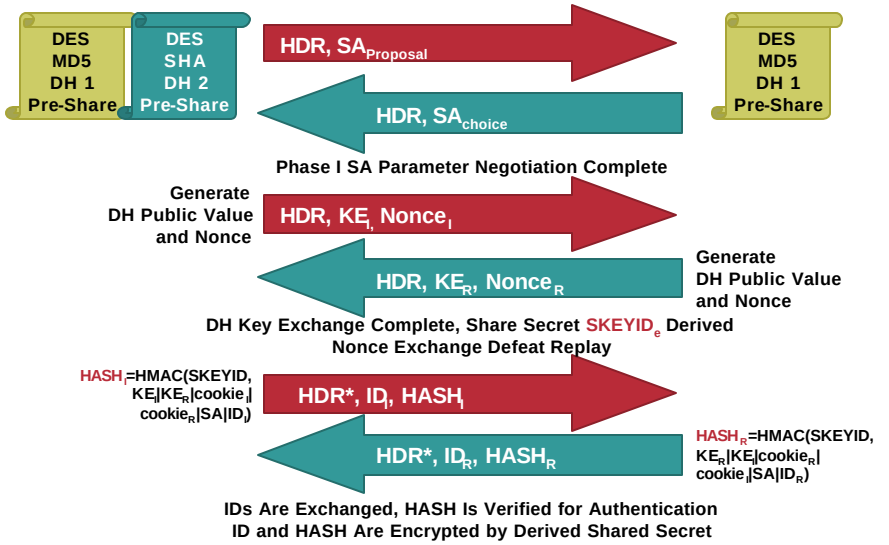
Cisco.com

The Initiator Sends across a Proof of Liveness

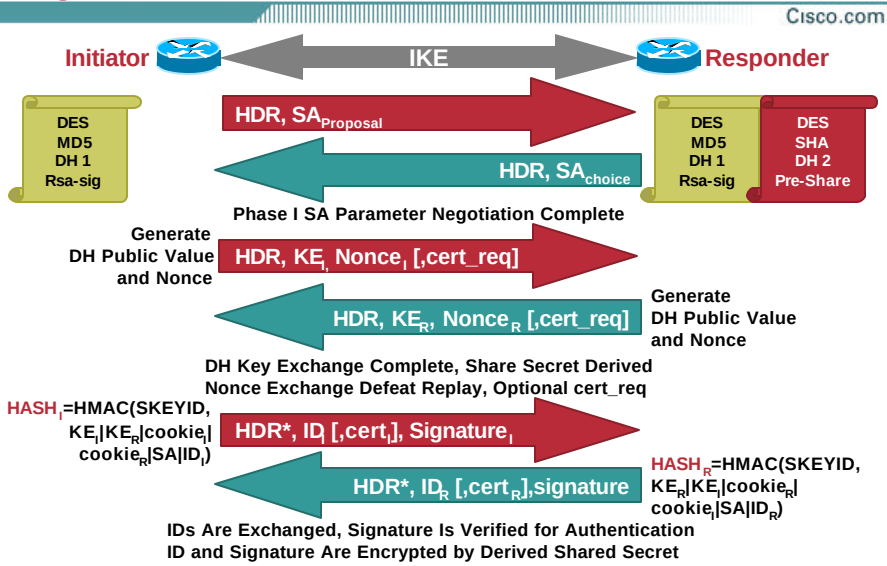


One Page Summary: Pre-Shared Main Mode

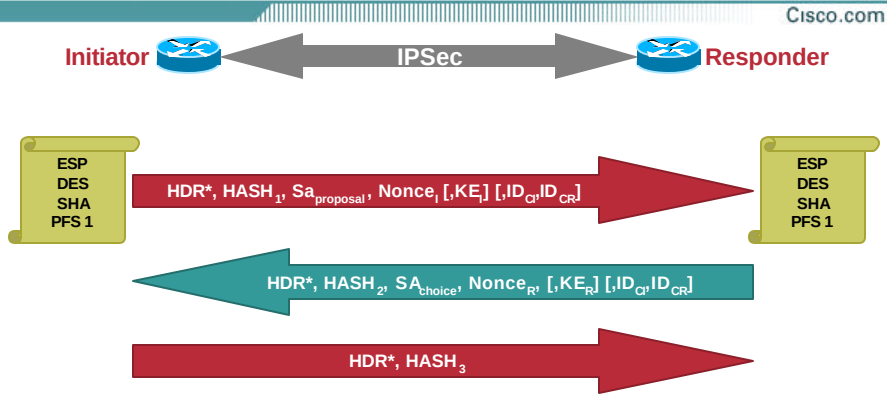
Cisco.com



One Page Summary: Signatures Main Mode

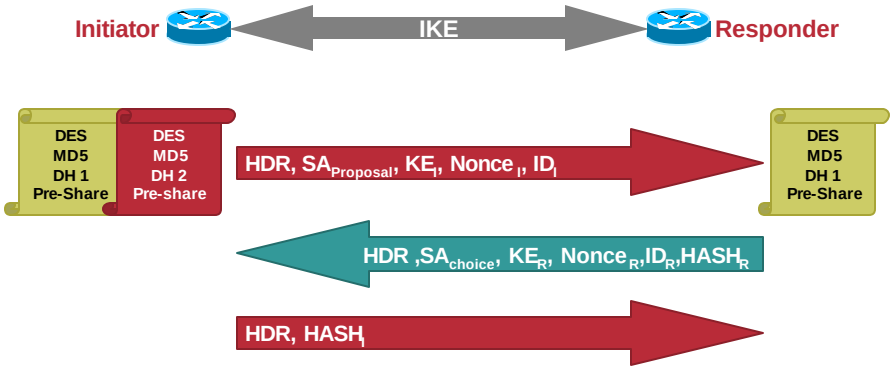


One Page Summary: Quick Mode



Aggressive Mode Using Pre-Shared Key: A Quick Overview

Cisco.com



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

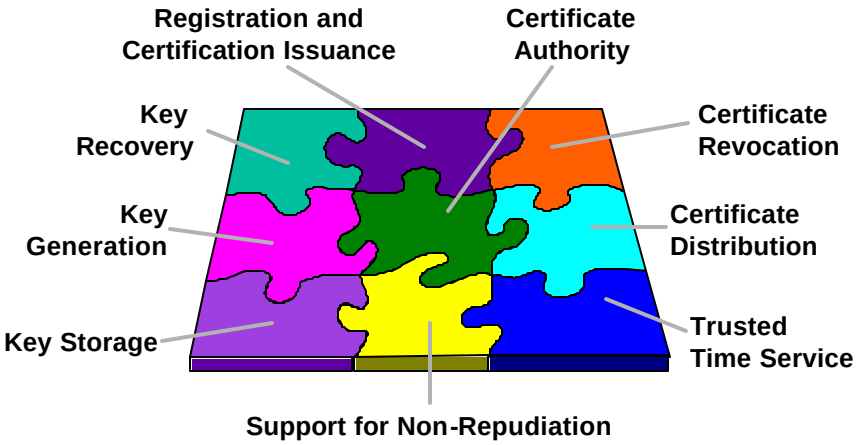
Agenda

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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

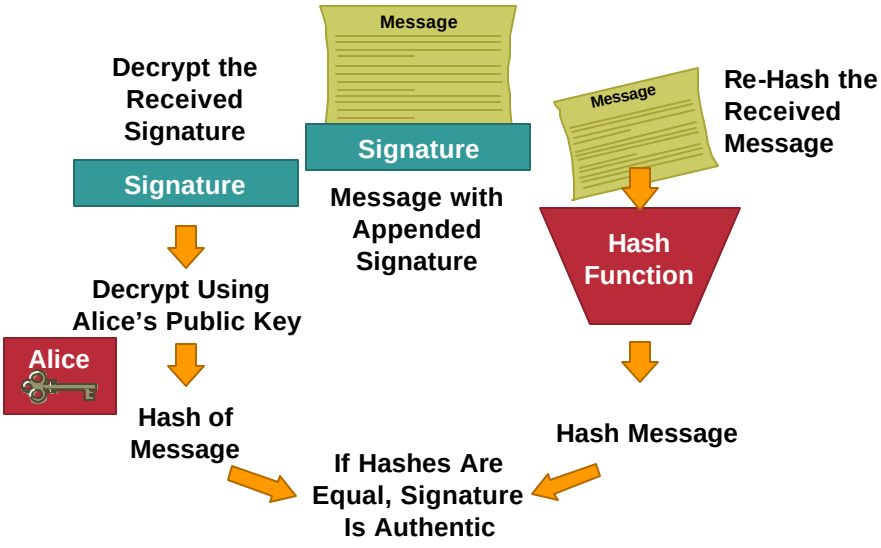
PKI: IKE Authentication Architecture

Cisco.com

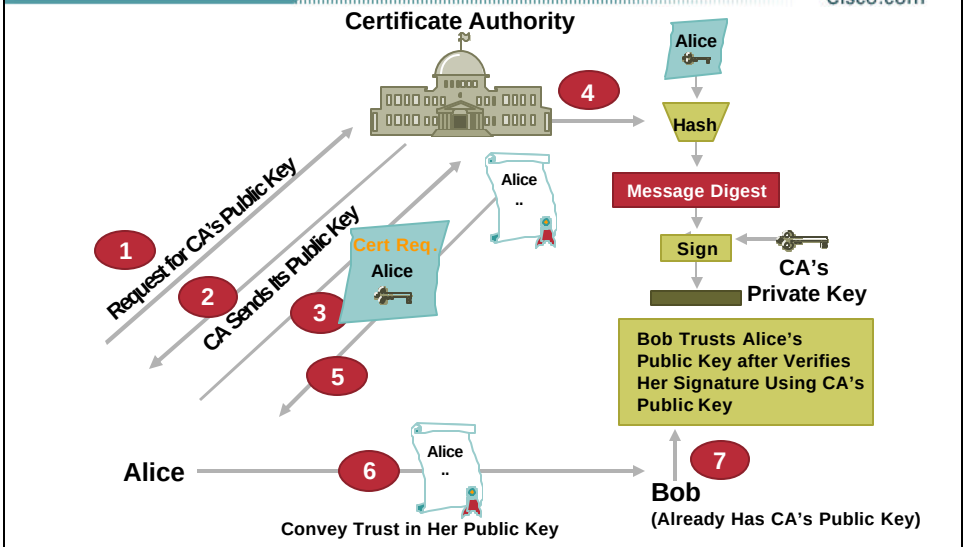


Signature Verification

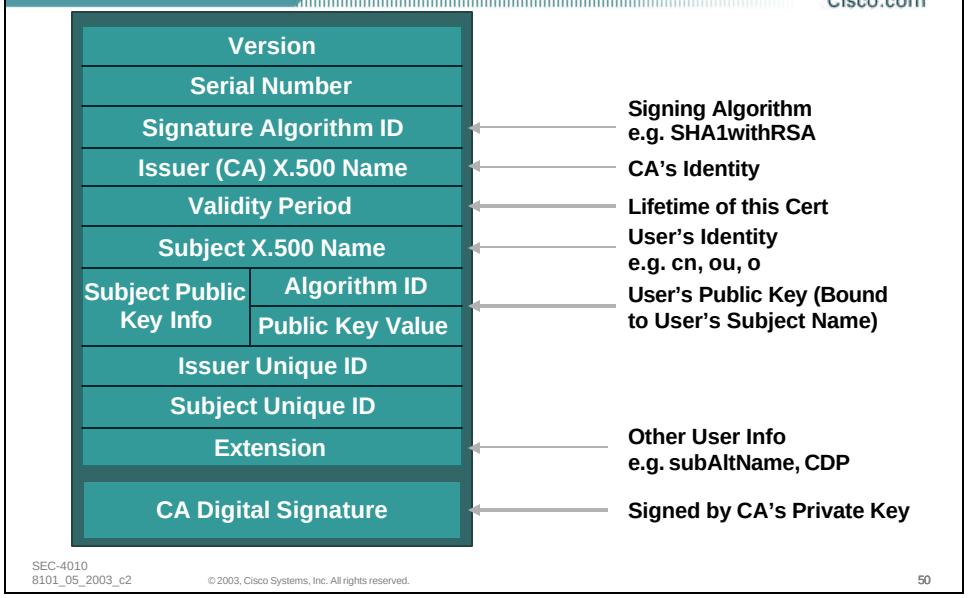
Cisco.com



Digital Certification



X.509 v3 Certificate



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

SCEP Overview—Getting CA's Certificate

Cisco.com

Get CA/RA Cert: HTTP Request Message

Send CA/RA Cert: HTTP Response Message

Compute Fingerprint and Call CA Operator ⟷ Operator Check Fingerprint

SCEP Overview—Enrollment

Cisco.com

PKCSReq: PKI Cert. Enrollment Message

CertRep: pkistatus = PENDING

Compute Fingerprint and Call CA Operator

Operator Check Fingerprint

CetCertInitial: Polling Message

CertRep: pkistatus = GRANTED
Certificate Attached

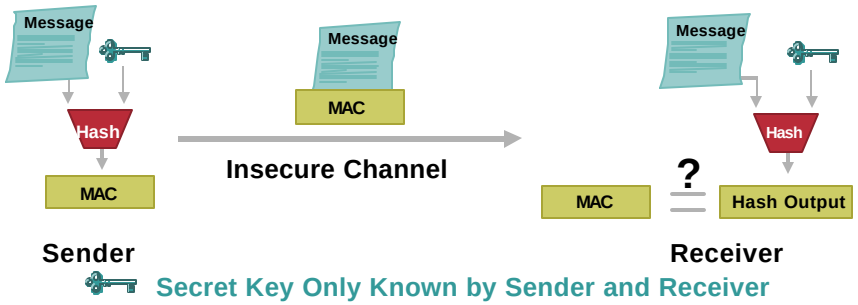
Agenda

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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

Message Authentication and Integrity Check Using Hash

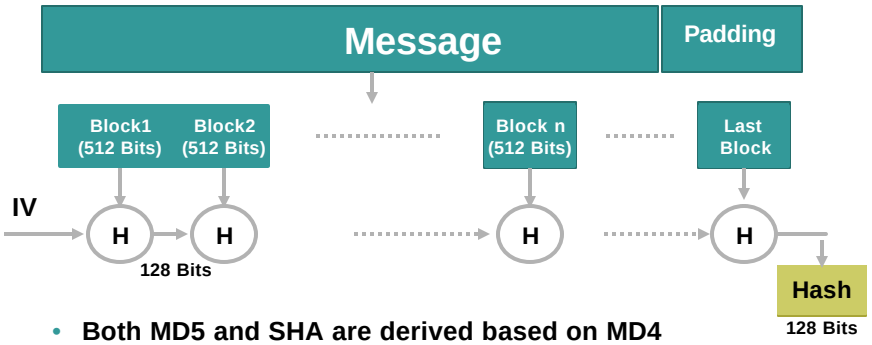
Cisco.com



- 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

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

Agenda

Cisco.com

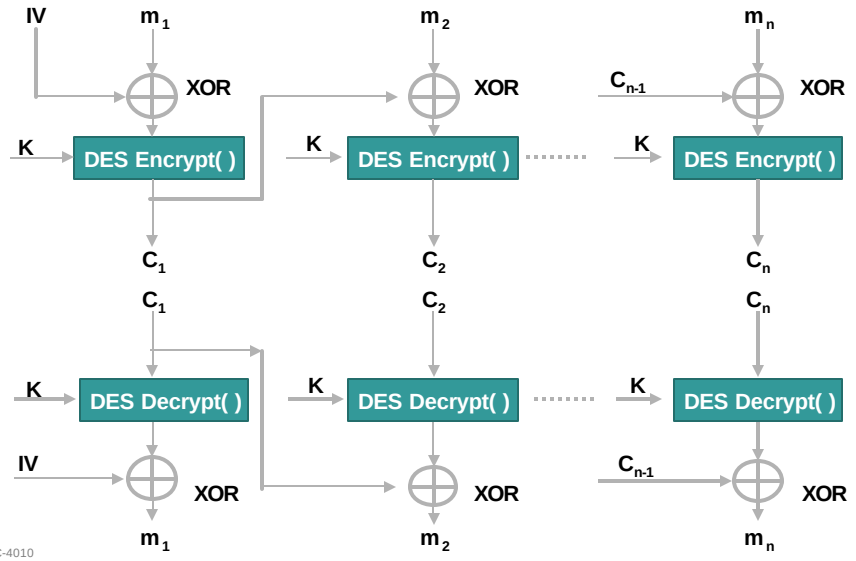
- **Analysis of Baseline IPSec Functionality**
  - IKE: IPSec Negotiation Protocol Flow
  - PKI: IPSec Authentication Architecture
  - SHA and MD5: IPSec Hashing Mechanisms
  - DES and AES: IPSec Encryption Techniques
- **Analysis of the Enhancements in IPSec**
  - Remote Access Features
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

Data Encryption Standard (DES)

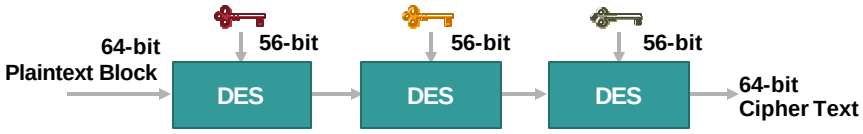
Cisco.com

- 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)

DES CBC Mode



Triple-DES



- 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?

‘Rijndael…the chief drawback to this cipher is the difficulty Americans have pronouncing it…The designers, Vincent Rijmen and Joan Daemen, know what they are doing.’

Bruce Schneier

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

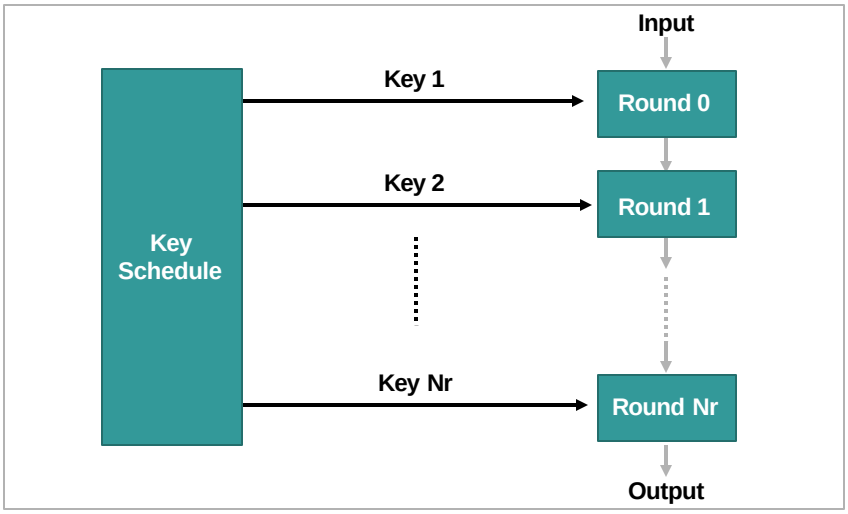
AES: Pseudo Code

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
```


AES: The Complete Cipher

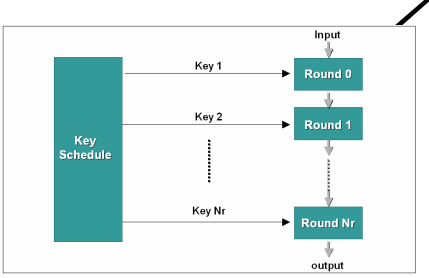
Cisco.com

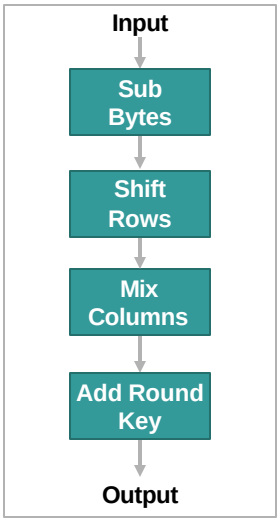


AES: Individual Rounds

Cisco.com

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

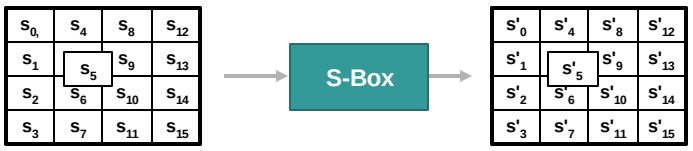




AES Functions: SubBytes and ShiftRows

Cisco.com

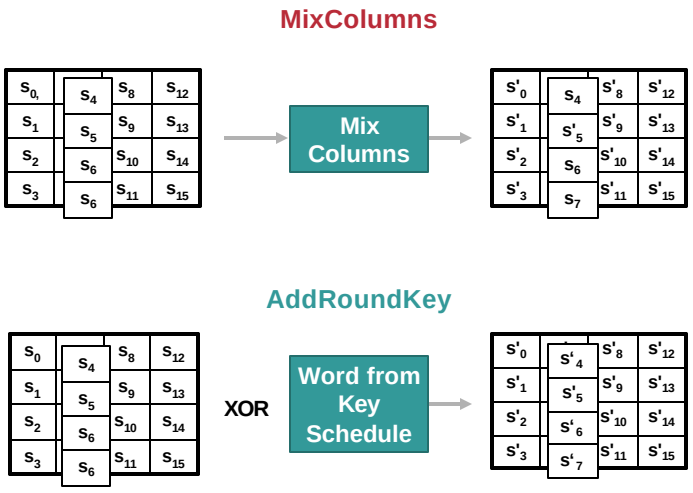
SubBytes



ShiftRows

AES Functions: MixColumns and AddRoundKey

Cisco.com



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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

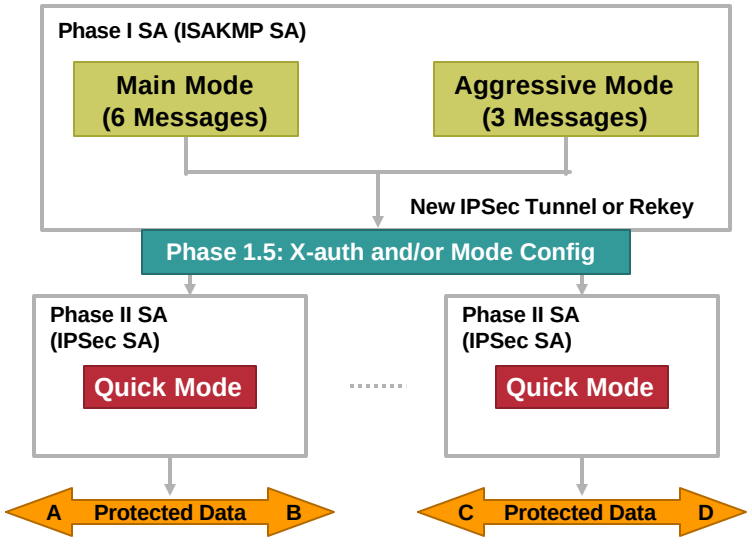
Remote Access Features

Cisco.com

- Mode config
- Extended authentication

Placement of Mode Config and X-auth in IKE

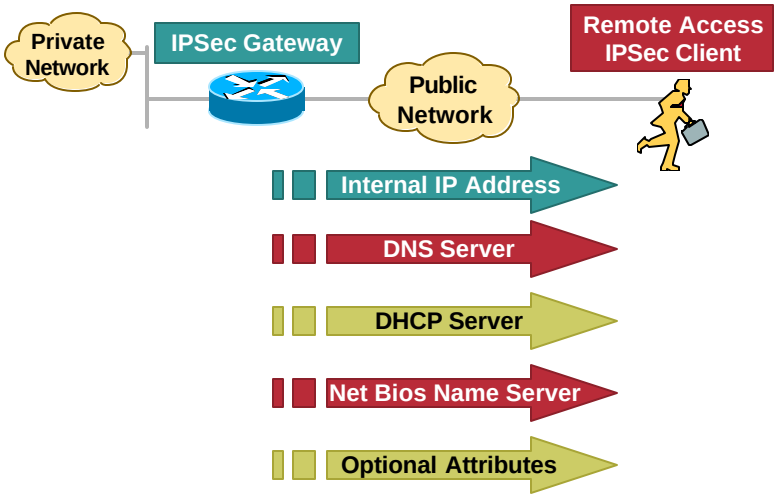
Cisco.com



Mode Config

Cisco.com

Mechanism Used to Push Attributes to Remote Access IPSec Clients



Mode Config 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		
Next Payload	Reserved = 0	Attributes Payload Length
Type = 1	Reserved = 0	Identifier
Attributes (0 Length Attributes in Request)		
0	0	Hash Payload Length
Hash		

Hash
=
Prf (SKEYID_a,
ISAKMP Header M-ID |
Attribute Payload)

Initiator
Remote Client

Attribute Request

Attribute Reply

Responder
IPSec Gateway

ISAKMP HEADER		
Next Payload	Reserved = 0	Attributes Payload Length
Type = 2	Reserved = 0	Identifier
Attributes (Set to the Values for One or More of the Attributes to Be Pushed)		
0	0	Hash Payload Length
Hash		

Attributes =

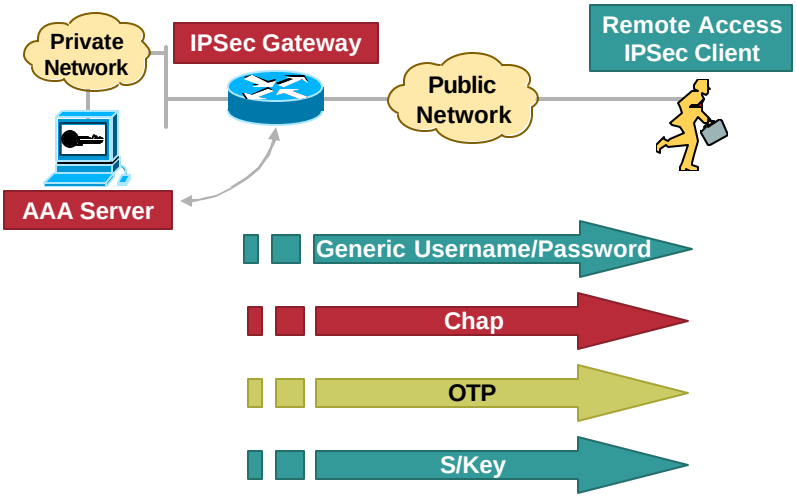
INTERNAL_IP4_ADDRESS	1
INTERNAL_IP4_NETMASK	2
INTERNAL_IP4_DNS	3
INTERNAL_IP4_NBNS	4
INTERNAL_ADDRESS_EXPIRY	5
INTERNAL_IP4_DHCP	6

Other Allowed but Not Mandatory

X-auth

Cisco.com

Mechanism Used to Perform Per User Authentication for RA Clients



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		
Next Payload	Reserved = 0	Attributes Payload Length
Type = 1	Reserved = 0	Identifier
Attributes (0 Length Attributes in Request)		
0	0	Hash Payload Length
Hash		

Hash
=
Prf (SKEYID_a, ISAKMP Header M-ID | Attribute Payload)

Initiator
IPSec Gateway

Attribute Request

Attribute Reply

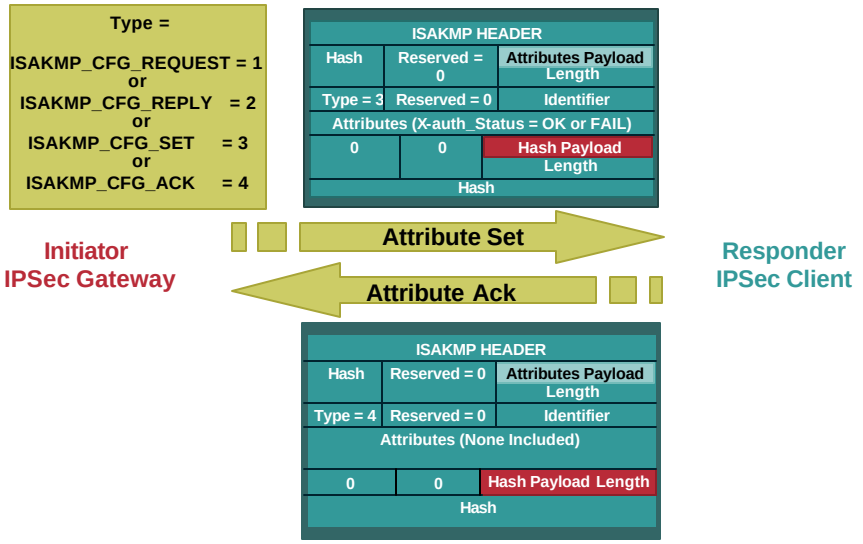
Responder
IPSec Client

ISAKMP HEADER		
Next Payload	Reserved = 0	Attributes Payload Length
Type = 2	Reserved = 0	Identifier
Attributes (Set to the Values for One or More of the Attributes to Be Pushed)		
0	0	Hash Payload Length
Hash		

Attributes =	
XAUTH_TYPE	16520
XAUTH_USER_NAME	16521
XAUTH_USER_PASSWORD	16522
XAUTH_PASSCODE	16523
XAUTH_MESSAGE	16524
XAUTH_CHALLENGE	16525
XAUTH_DOMAIN	16526
XAUTH_STATUS	16527

X-auth Protocol Specifications

Cisco.com



Agenda

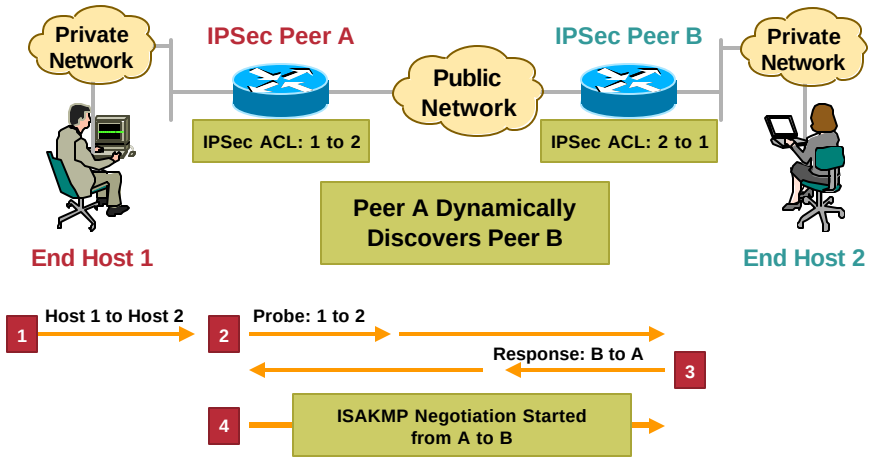
Cisco.com

- 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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

TED (Tunnel Endpoint Discovery)

Cisco.com

Mechanism Used to Dynamically Discover Peer and Negotiate Proxies



TED Protocol Specifications

Cisco.com

Initiator Proxy = Configured Source Address For IPSec Interesting Traffic

ISAKMP HEADER			
NP	Reserved = 0	Vendor Payload	Length
Cisco's Vendor ID Along with Capability Flags			
NP	Reserved = 0	ID Payload	Length
ID = Initiator's ID Encoded as IP Address			
NP	Reserved =	ID Payload	Length
ID = Initiator's Proxy			
0	Reserved = 0	Vendor Payload	Length
Special Vendor ID Payload			

Special Vendor Payload = Hash of Special String +TED Version Number (3) +IPVersion+Src IP and Port+ IP and Port

Initiator IPSec Gateway

TED Probe

TED Response

Responder IPSec Client

ISAKMP HEADER			
NP	Reserved = 0	Vendor Payload	Length
Cisco's Vendor ID Along with Capability Flags			
NP	Reserved = 0	ID Payload	Length
ID = Responder's ID Encoded as IP Address			
NP	Reserved = 0	Private Payload	Length
TED Response Payload			

TED Response Payload = Protocol Version+ Matched Proxies

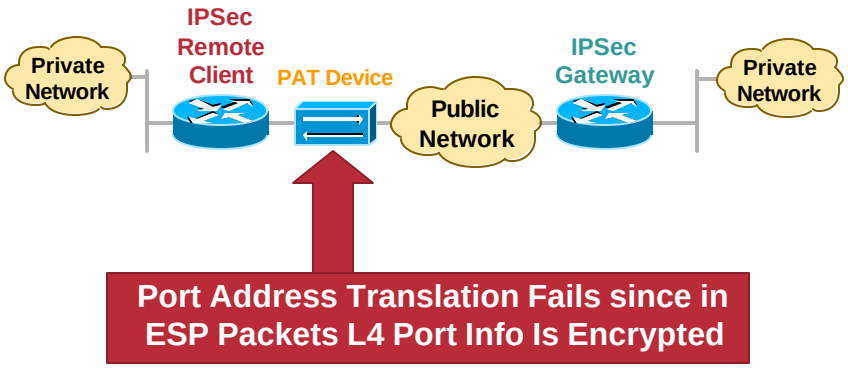
Agenda

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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

IPSec and NAT: The Problem

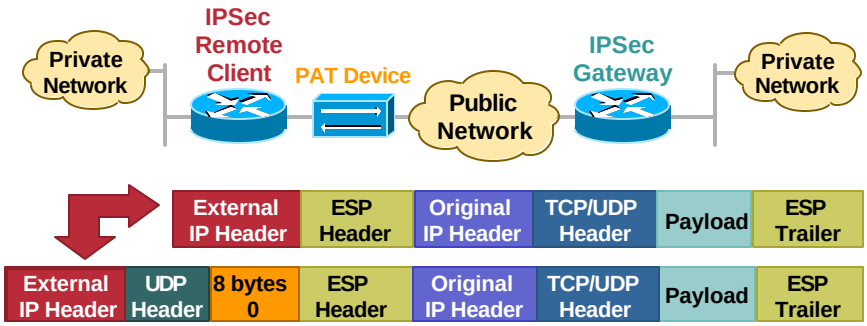
Cisco.com



IPSec and NAT: Three Solutions

Cisco.com

- Always on IPSec over UDP (most deployed)
- Always on IPSec over TCP (an alternate solution)
- Need based IPSec NAT traversal (in the works)



Always on IPSec over UDP: Part of Mode Config

Cisco.com

Type =

ISAKMP_CFG_REQUEST = 1
or
ISAKMP_CFG_REPLY = 2
or
ISAKMP_CFG_SET = 3
or
ISAKMP_CFG_ACK = 4

ISAKMP HEADER		
Next Payload	Reserved = 0	Attributes Payload Length
Type = 1	Reserved = 0	Identifier
Attributes (MODECFG_UDP_NAT_PORT = 0)		
0	0	Hash Payload Length
Hash		

Hash
=
Prf (SKEYID_a, ISAKMP Header M-ID | Attribute Payload)

Initiator
Remote Client

Attribute Request

Attribute Reply

Responder
IPSec Client

ISAKMP HEADER		
Next Payload	Reserved = 0	Attributes Payload Length
Type = 2	Reserved = 0	Identifier
Attributes (MODECFG_UDP_NAT_PORT = x		
0	0	Hash Payload Length
Hash		

(Optional) Attribute
=
MODECFG_UDP_NAT_PORT

Value
=
UDP Port Number: 10000 – 49151

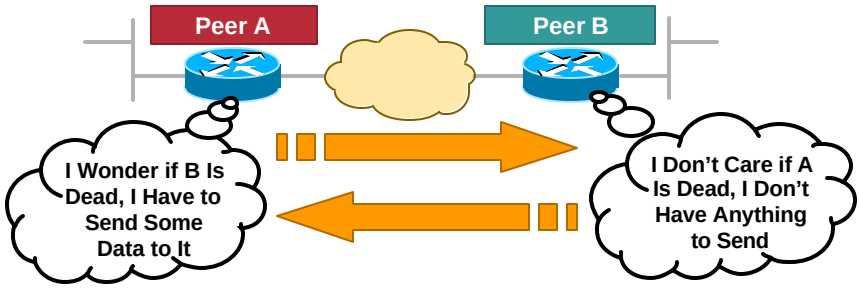
Agenda

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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

DPD Rules

Cisco.com



Passage of IPSec Traffic Is Proof of Liveliness

DPD Is Asynchronous

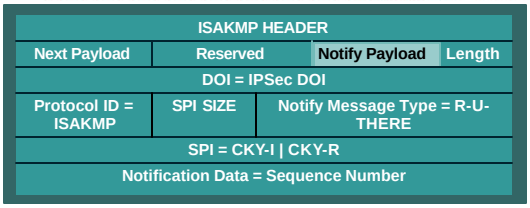
Each Peer Sets Its Own WORRY METRIC

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

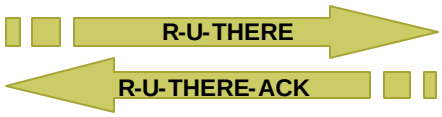
DPD Protocol Specifications

Cisco.com

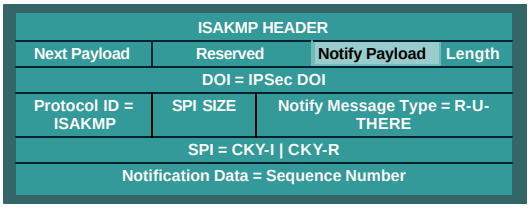
Vendor ID Payload Is Exchanged in IKE Negotiation Beforehand



Initiator



Responder



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
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

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

(Please Note that This Information Is Current as of February 2003; Finalization of the Specifications of the IKE V2 Protocol Is Still a Work in Progress)

IKE v2: What Is Not Changing

Cisco.com

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

  Two phases of negotiation

  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

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**

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**
  - **Tunnel End Point Discovery (TED)**
  - **IPSec NAT Traversal**
  - **Dead Peer Discovery (DPD)**
  - **IPSec Work in Progress: IKE v2, Multicast IPSec**

What Is a Multicast Group?

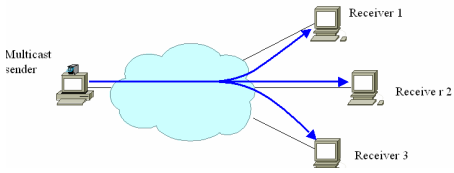
Cisco.com

- 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

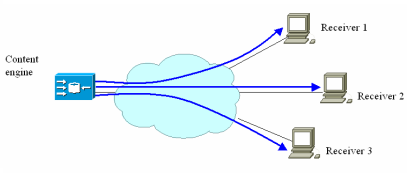
Types of Multicast Groups

Cisco.com

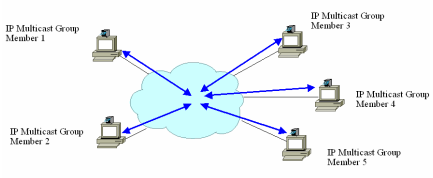
Single-Source Multicast



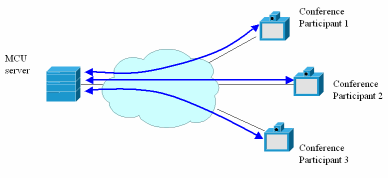
Publish-Subscribe



Multiple-Source Multicast



Multipoint Control Unit



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**

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 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

(Please Note that This Information Is Current as of the Beginning of 2003; GDOI Is Still a Work in Progress)

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**

GDOI Protocol Flow

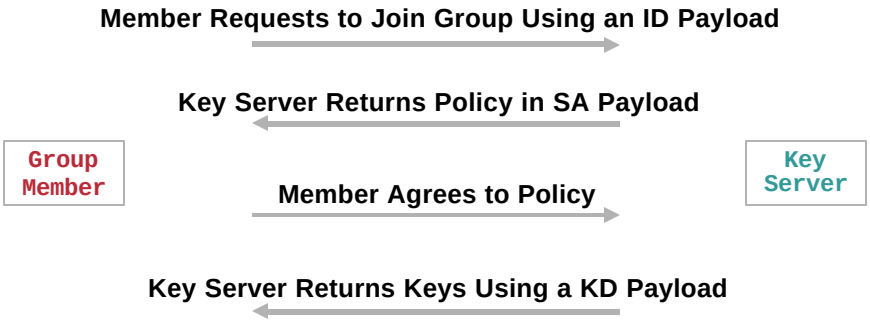
Cisco.com

- **Two phases**
  - IKE phase 1 protocol
  - GDOI registration protocol

- **Security protections**
  - IKE phase 1 provides authentication, confidentiality, and integrity
  - GDOI registration provides authorization and replay protection

GDOI Registration Protocol

Cisco.com



GDOI Registration Results

Cisco.com

- When registration is complete a group member has:
  - Data security SAs and keys
  - GDOI Rekey SA and keys (if defined to be part of the group policy)

GDOI Rekey 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

GDOI Rekey Results

Cisco.com

- **When rekey is complete a group member has one or more of the following:**
  - New data security SAs and keys
  - New GDOI Rekey SA and keys

Agenda

Cisco.com

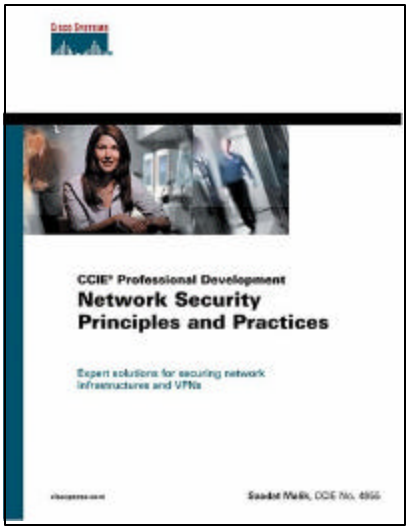
- **Analysis of Baseline IPSec Functionality**
  - IKE: IPSec Negotiation Protocol Flow
  - PKI: IPSec Authentication Architecture
  - SHA and MD5: IPSec Hashing Mechanisms
  - DES and AES: IPSec Encryption Techniques
- **Analysis of the Enhancements in IPSec**
  - Remote Access Features
  - Tunnel End Point Discovery (TED)
  - IPSec NAT Traversal
  - Dead Peer Discovery (DPD)
  - IPSec Work in Progress: IKE v2, Multicast IPSec

So, Where Can I Read in Detail about All This?

Cisco.com

'Network Security Principles and Practices'

by Saadat Malik



Also Available at the Networkers CiscoPress Booth

NETWORKERS 2003
THE POWER TO TRANSFORM BUSINESS. now.

Please Complete Your Evaluation Form

Session SEC-4010