CISCO SYSTEMS

Cisco.com

IPsec Deployment

Franjo Majstor
EMEA Consulting Engineer
Cisco Systems, Inc
fmajstor@cisco.com

Agenda

Cisco.com

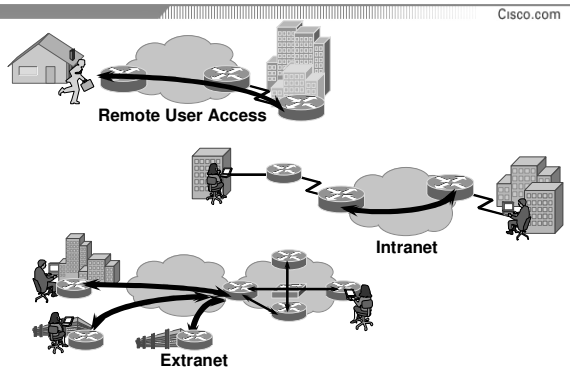
- IPsec deployment
  - Cisco VPN Portfolio
  - IPsec Remote Access VPNs
  - IOS and IPsec
  - Deployment topologies
  - Scalable Authentication with IOS PKI Enhancements
  - IPsec and QoS, VoIP
- Wrap up and Q&A

Cisco.com

Cisco VPN Portfolio

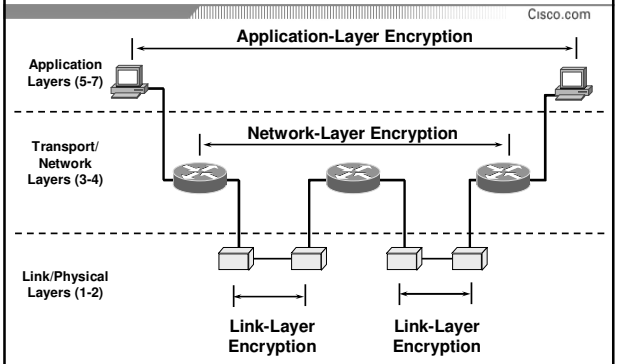
Applications of IPsec

Cisco.com



IPsec Alternatives

Cisco.com



VPN Types and Applications

Cisco.com

Type	Application	Alternative To	Benefits
Remote Access VPN	Remote Dial Connectivity	Direct Dial ISDN	Ubiquitous Access Lower Cost
Site-to-Site VPN	Branch Office Connectivity	Leased Line Frame Relay ATM	Extend Connectivity Increased Bandwidth Lower Cost
Extranet VPN	Biz-to-Biz Connectivity	Fax EDI Mail	Timing Lower Cost

Evolution away from Dial

Next generation of WAN infrastructure

Enables E-commerce efficiencies

Cisco VPN Portfolio

Cisco.com

Cisco Provides the Industry's Broadest VPN Solution Set!

VPN Application	Large Enterprise	Medium Enterprise	Small Biz/Branch	SOHO
Remote Access Cisco VPN 3000	VPN 3080 VPN 3060 Concentrators	VPN 3030 Concentrator	VPN 3015 VPN 3005 Concentrators	VPN 3002 Hardware Client VPN 3000 Software Client
Site-to-Site IOS Routers	7600 7400 7200 7100	3700 3600	3700 3600 2600 1700	900 800
Firewall-Based VPN Pix Firewall	Pix 535 Pix 525	Pix 525 Pix 515E	Pix 515E Pix 506E	Pix 506E Pix 501

Voice and Video Enabled VPN - V^{3}PN

New

Cisco.com

V^{3}PN delivers integrated IP Telephony and Video over IPsec VPNs, thus enabling:

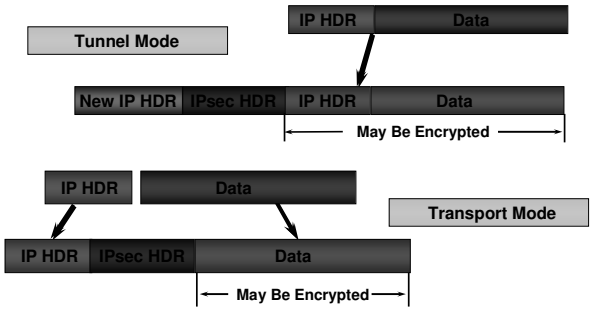
- **Fully functional, cost-effective remote working environments**
  - **Securely extend the corporate PBX to home offices for full-featured teleworker solutions**
  - **Deliver secure IP Video for video conferencing and training**
- **Enhanced security for voice and video traffic over the WAN**
  - **Encryption of voice/video streams, authentication of gateways**
- **IP Telephony + VPNs = Greater cost savings**
  - **Combining IP Telephony & Video with VPNs reduces bandwidth and telephony expenses**
  - **Extending converged communications to remote sites/users increases productivity**

Cisco.com

IPsec Remote Access VPNs

IPsec Modes

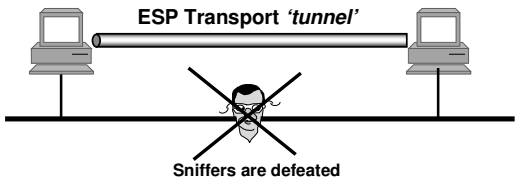
Cisco.com



IPsec Transport Mode

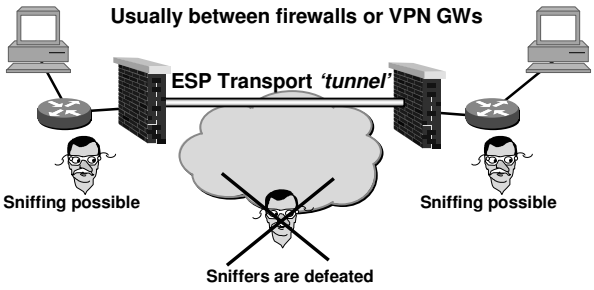
Cisco.com

Can be used end to end, between host



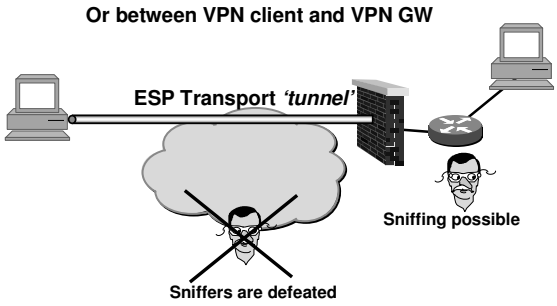
IPsec Tunnel Mode

Cisco.com



IPsec Tunnel Mode

Cisco.com



Weakening IKE (Wildcard Pre-Shared Keys)

Cisco.com

RFC 2409 requires a unique IP address associated to pre-shared key

- this is for good security
- but prevents the use of dynamic IP address
- hence no dial client (where IP address given dynamically by ISP)

Weakening IKE (Wildcard Pre-Shared Keys)

Cisco.com

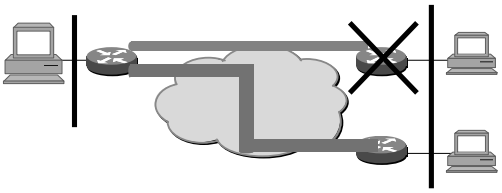
- RFC 2409 was strictly implemented in IOS
- CSCdm59913 (IOS 12.0(5)XE 12.0(6)T) optional extension

```
crypto isakmp key <key> address <ip-address>
[<subnet>]
crypto isakmp key foobar address 0.0.0.0 0.0.0.0
```


IPsec and Keepalives

Cisco.com

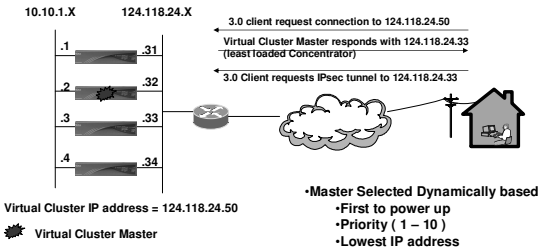
Specific configuration of IPsec/IKE peer to allow resilience/load balancing



Plain IKE can detect failed peer during Main Mode
IKE Keep Alive detects failed peer at any time

Advanced Features Load balancing

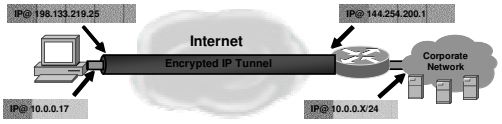
Cisco.com



Based on IETF draft "A Traffic-Based Method of Detecting Dead IKE Peers"
www.ietf.org/internet-drafts/draft-ietf-ipsec-dpd-01.txt

Remote Access VPN

Cisco.com

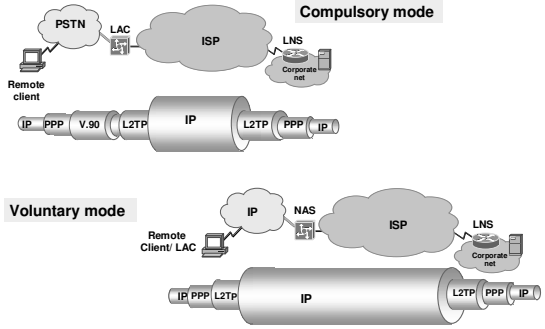


Encapsulate original (green) packet in a new packet (red), traverse shared backbone and require:

- Per packet encryption and authentication
- Private address assignment
- Private services assignment (DNS, WINS, domain,..)
- End point authentication (user, device)
- NAT traversal support

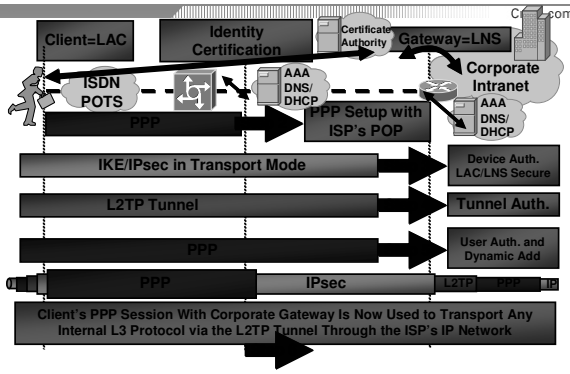
VPN RA Alternatives - L2TP

Cisco.com



L2TP/IPsec Remote Access VPN

Cisco.com



VPN RA Alternative - L2TP and IPsec

Cisco.com

L2TP is used for:

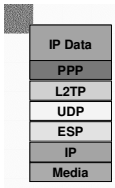
- user authentication (PAP,CHAP, EAP)
- IPCP: IP address, DNS/WINS server config
  (centrally managed via RADIUS server)
- multi-protocol support (IP, IPX, AT,…)
- multicast

IPsec transport mode is used for:

- per packet confidentiality, integrity, authentication and anti-replay protection

Problems:

- overhead, independent protocols (fixed with RFC 3193), lack of clients

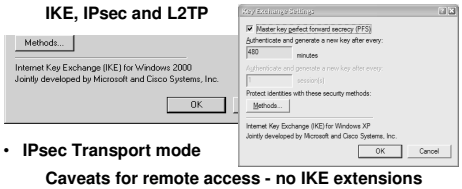


LT2P/IPsec Stack

Windows 2000/XP VPN Client

Cisco.com

- **Cisco and Microsoft Co-development**
  IKE, IPsec and L2TP



- **IPsec Transport mode**
  Caveats for remote access - no IKE extensions

IKE Configuration Method (IKE mode-cfg)

Cisco.com

www.ietf.org/internet-drafts/draft-dukes-ike-mode-cfg-03.txt

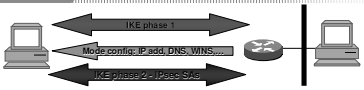
• IETF draft to allow the dynamic allocation of IP parameters to an IPsec client (a la DHCP or IPCP of PPP).

• Just after IKE phase I (main or aggressive mode)

Goal: easy configuration of IPsec client

VPN RA Alternatives - IKE Mode Config

Cisco.com



Attribute	Value	Type	Length
INTERNAL_IP4_ADDRESS	1	Variable	0 or 4 octets
INTERNAL_IP4_NETMASK	2	Variable	0 or 4 octets
INTERNAL_IP4_DNS	3	Variable	0 or 4 octets
INTERNAL_IP4_NBNS	4	Variable	0 or 4 octets
INTERNAL_ADDRESS_EXPIRY	5	Variable	0 or 4 octets
INTERNAL_IP4_DHCP	6	Variable	0 or 4 octets
APPLICATION_VERSION	7	Variable	0 or more
INTERNAL_IP4_SUBNET	13	Variable	0 or 8 octets
...	...		
Reserved for future use	16-16383		
Reserved for private use	16384-32767		

draft-dukes-ike-mode-cfg-03.txt

IKE Extended Authentication (Xauth)

Cisco.com

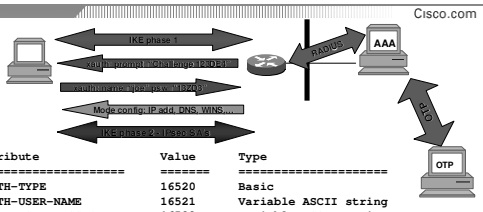
www.ietf.org/internet-drafts/draft-beaulieu-ike-xauth-03.txt

- **IETF draft to authenticate the USER using a remote IPsec client**
- **Just after IKE phase I (main or aggressive mode) and after configuration mode**

Goal: re-use existing AAA infrastructure (RADIUS, TACAS+, OTP,…) with IPsec based VPN clients

VPN RA Alternatives - IKE Xauth

Cisco.com

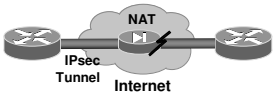


Attribute	Value	Type
XAUTH-TYPE	16520	Basic
XAUTH-USER-NAME	16521	Variable ASCII string
XAUTH-USER-PASSWORD	16522	Variable ASCII string
XAUTH-PASSCODE	16523	Variable ASCII string
XAUTH-MESSAGE	16524	Variable ASCII string
XAUTH-CHALLENGE	16525	Variable ASCII string
XAUTH-DOMAIN	16526	Variable ASCII string
XAUTH-STATUS	16527	Basic
XAUTH-NEXT-PIN	16528	Variable
XAUTH-ANSWER	16529	Variable ASCII string

draft-beaulieu-ike-xauth-03.txt

Network Address Translation and IPsec

Cisco.com

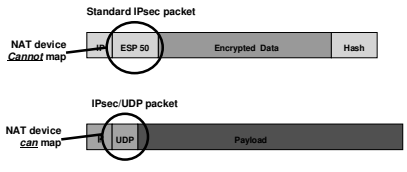


- **PAT breaks IPsec**
- **NAT works with ESP and tunnel mode**
- **NAT with AH breaks IPsec**
- **Fixing this in remote access: one further encapsulations (TCP or UDP)**

IPsec VPN and NAT/PAT Transparency

Cisco.com

- **IPsec/UDP**
  - Allows clients to operate behind a NAT device
  - Provides the security of IPsec/ESP
  - Requires no user intervention



IPsec over NAT

Cisco.com

- **IPsec UDP encapsulation:**
  - **defines methods to encapsulate and decapsulate ESP packets inside UDP packets for the purpose of traversing NATs.**

  www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-04.txt

- **IPsec NAT-T:**
  - **describes how to detect one or more NATs between IPsec hosts, and how to negotiate the use of UDP encapsulation of the IPsec packets through the NAT boxes in IKE**

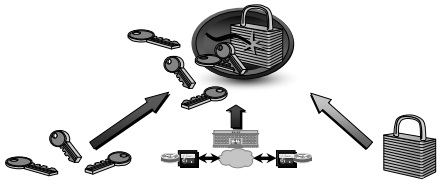
  www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-04.txt

Cisco.com

IOS and IPsec

End-to-End Secured VPN

Cisco.com

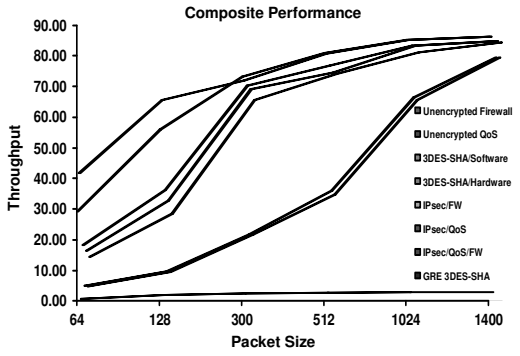


Cisco VPN Solutions Utilize Standards-Based Security

Tunneling	Encryption	Authentication	Integrity
IPsec	DES	RSA digital certificates	HMAC-MD5
GRE/IPinIP	3DES		HMAC-SHA1
L2TP/PPTP	AES	RADIUS	

Performance Vs. Features

Cisco.com



Branch Throughput Results

Cisco.com

- **Based on 60–65% CPU utilization target**
- **NOTE: Throughput numbers are valid for specific design configuration; Other designs may produce different results**

Branch Platform	HW Encryption	SW Encryption
Cisco 800	2.0Mb	200kb
Cisco 1750	2.6Mb	560kb
Cisco 2611	2.0Mb	380kb
Cisco 2621	2.4Mb	520kb
Cisco 2651	2.8Mb	960kb
Cisco 3620	1.8Mb	480kb
Cisco 3640	3.5Mb	900kb
Cisco 3660	16.0Mb	2.4Mb

New Cisco Dual Ethernet VPN Platforms

Cisco.com

Cisco SOHO 90 Series

SOHO 91: Dual Ethernet

New Model

New Features
- 4 port 10/100 Switch
- IP/FW/3DES Cisco IOS Image
- Console port for out-of-band management only
- Easy VPN Remote

Cisco 830 Series

831: Dual Ethernet

New Model

New Features
- 4 port 10/100 Switch
- Hardware-Assisted Crypto
- Advanced QoS
- Security enhancements*
- Virtual Aux via console port
- dial backup & out-of-band management
- Easy VPN Remote

* Q1CY2003

IPsec VPN Services Module

Cisco.com

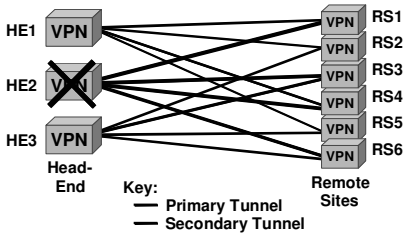
- **Initial Release (FCS-ed)**
  - **July, 2002**
- **FCS IOS Release: 12.2(9)YO**
  - **Special off of early 12.2S**
- **Part #: WS-SVC-IPSEC-1**
- **Speeds & Feeds:**
  - **1.9 Gbps 3DES (Maximum)**
  - **1.6 Gbps 3DES (300 byte packet)**
  - **8,000 tunnels**
  - **60 tunnels/second**

Fabric Enabled

Load Dispersion on Failure

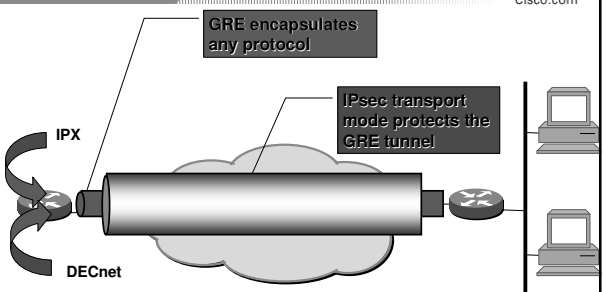
Cisco.com

- When a head-end tunnel termination device fails, its load should be equally shared among the other remaining head-end devices
  - Aids in the resiliency and scalability of the head-end
  - Adds to the configuration complexity



Generic Routing Encapsulation

Cisco.com



GRE RFC 2784 encapsulates any protocol in IP

GRE (Cont.)

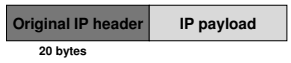
Cisco.com

- GRE is RFC2784
- Standards Track by Cisco, Procket and Juniper
- Uses protocol 47
- Works for several IP protocols: IP, OSI, DECnet, IPv6, …
- Works for multicast traffic
- Overhead: 24 bytes

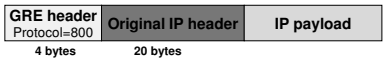
Generic Routing Encapsulation

Cisco.com

Original IP datagram *(before forwarding)*



GRE encapsulation *(after forwarding to a GRE tunnel)*



GRE packet with new IP header: protocol 47 *(forwarded using new IP dst)*

GRE: IOS Configuration

Cisco.com

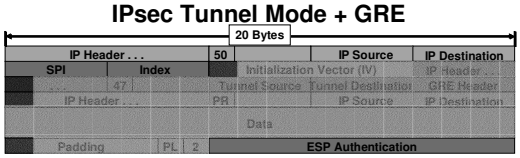
```
interface Tunnel0
 ip address 192.168.100.1 255.255.255.252
 tunnel source 193.193.193.1
 tunnel destination 194.194.194.1
 tunnel mode gre ip
```

GRE is the default tunnel mode, so, this line will not appear in a show running-config

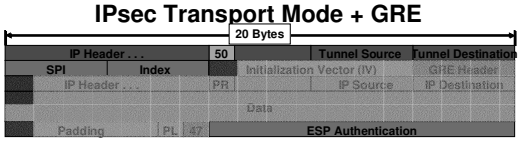
IPsec + GRE Packets

Cisco.com

IPsec Tunnel Mode + GRE



IPsec Transport Mode + GRE



IPsec/GRE with Dynamic IP Addresses

Cisco.com

```
VPN_GW_hub#
interface Tunnel0
   ip unnumbered Ethernet0
   tunnel source Ethernet1
   tunnel destination 1.1.1.1   <---  fake IP@ with only local significance

VPN_GW_spoke#
interface Tunnel0
 ip address 1.1.1.1 255.255.255.252 <-- fake IP@  force the tunnelling
 tunnel destination 20.20.20.51     <----- real head-end IP@
…
ip route 1.0.0.0 255.0.0.0 Ethernet1  <-- tunnel traffic over IPsec
```

Caveats:

- **Doable with config tricks**
- **Must use the IPsec in tunnel mode (overhead)**
- **Loose RRI functionality - Must use static routes**

What is IP in IP tunneling

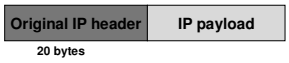
Cisco.com

- **IPinIP is RFC2003**
- **Standards Track by IBM**
- **Uses protocol 4**
- **Only works for IP**
- **Used by IPsec tunnel mode**
- **Overhead: 20 bytes**

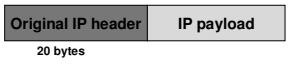
IP in IP Encapsulation

Cisco.com

Original IP datagram *(before forwarding)*



IPinIP encapsulation *(after forwarding to a IPinIP tunnel)*



IPinIP packet with new IP header: protocol 4 *(forwarded using new IP dst)*

IP in IP: IOS configuration

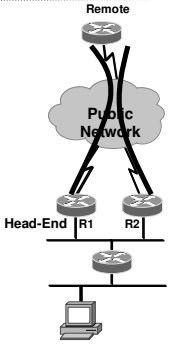
Cisco.com

```
interface Tunnel0
 ip address 192.168.100.1 255.255.255.252
 tunnel source 193.193.193.1
 tunnel destination 194.194.194.1
 tunnel mode ipip
```


IPsec VPN Site-to-Site High-Availability

Cisco.com

- **Options for IPsec HA:**
  - **GRE tunnels + dynamic routing**
  - **IKE keepalives**
  - **HSRP - Hot Standby Router Protocol**
  - **RRI - Reverse Route Injection**

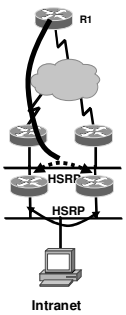


HSRP and VPNs for 12.1(9)E

Cisco.com

- **HSRP can now be used on the VPN interface**
  - **crypto can attach to virtual interfaces on 12.1(E)9**

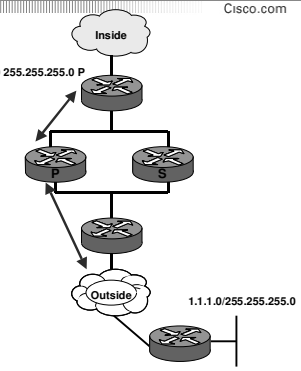
```
interface FastEthernet 0/0
ip address 192.168.0.2…
  … 255.255.255.0
standby name group1
standby ip 192.168.0.3
crypto map mymap redundancy group1
```

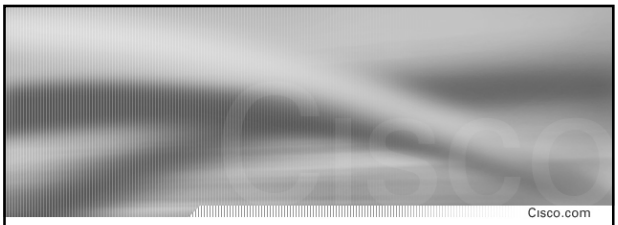


Reverse Route Injection Example

Cisco.com

- Remote connects to HSRP VIP, attaches to Primary P.
- After QM success, route to 1.1.1.0/24created by RRI and advertised to inside router.
- Returning traffic (from inside) destined for 1.1.1.0 is sent via the correct router.



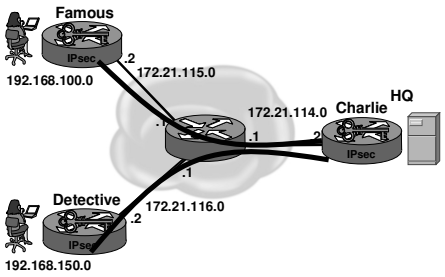


Cisco.com

Deployment topologies

A Star Topology

Cisco.com



Star Topology Central Site Router - Cfg 1

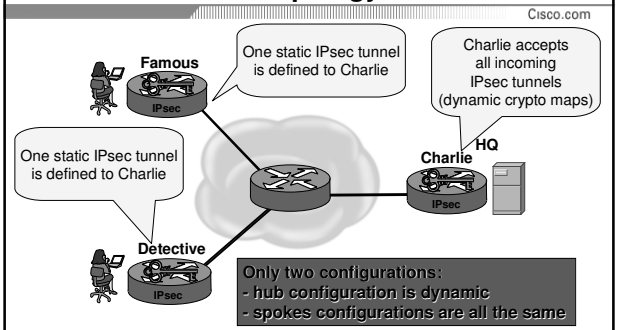
Cisco.com

```
! Let's be courageous and let's define
! One crypto map entry per remote peer
! ...
crypto map HQ 10 ipsec-isakmp
 set peer 172.21.115.2
 set transform-set encrypt-des
 match address 101

crypto map HQ 20 ipsec-isakmp
 set peer 172.21.116.2
 set transform-set encrypt-des
 match address 102
```


Smart IPsec Star Topology

Cisco.com



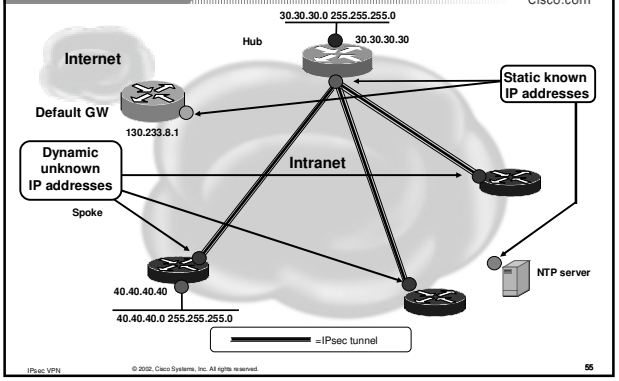
Star Topology Central Site Router - Cfg 2

Cisco.com

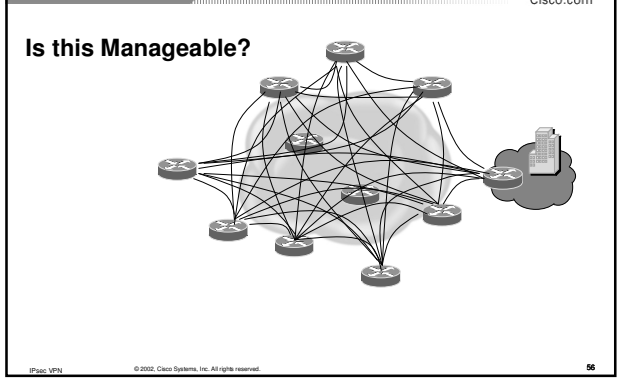
```
! Let's be smart and let's define a single
! Dynamic crypto map
!
crypto map DYNAMIC 10 ipsec-isakmp dynamic TEMPLATE

! Template used to define: transforms, lifetime,
! Identities, ...
crypto dynamic-map TEMPLATE 10
     set transform-set ...
```

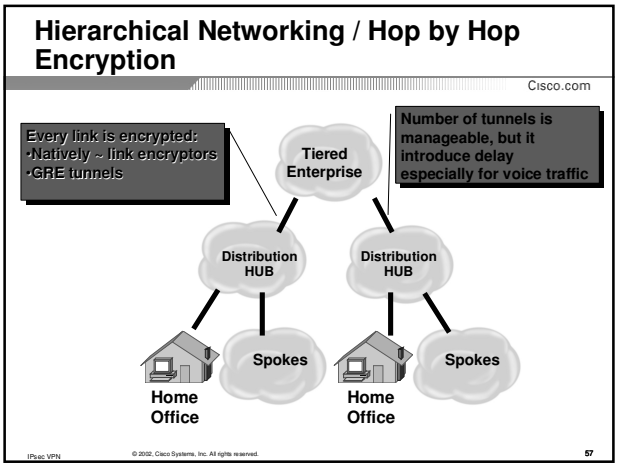
Hub-and-spoke IPsec VPN



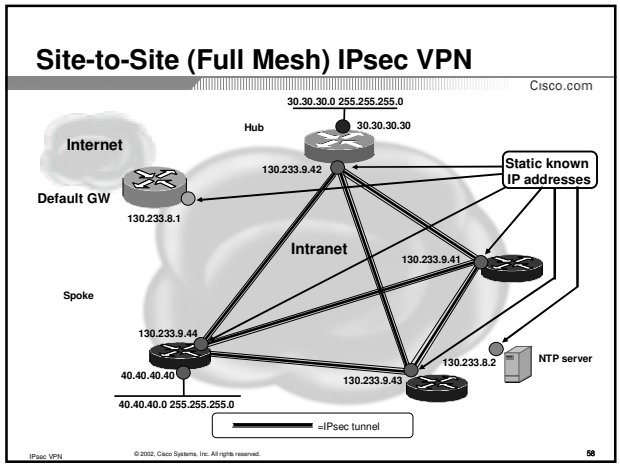
Large Networks : n(n-1)/2 issue



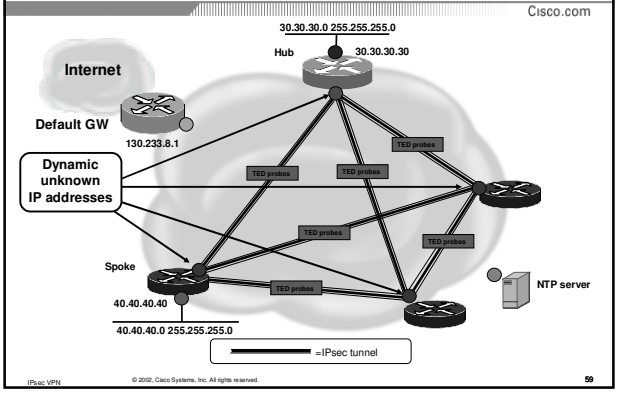
Hierarchical Networking / Hop by Hop Encryption



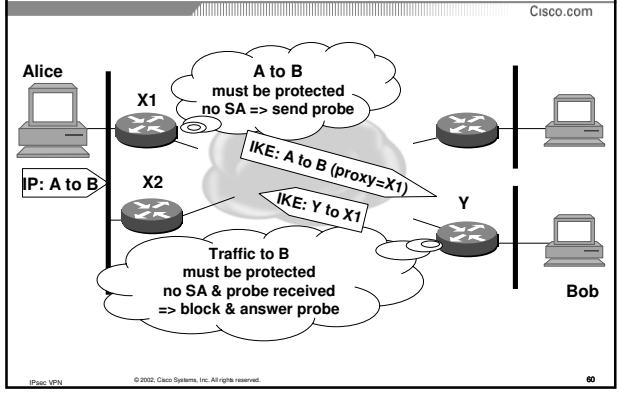
Site-to-Site (Full Mesh) IPsec VPN



Full Mesh with TED IPsec VPN



Fully Meshed - Tunnel Endpoint Discovery



Caveats of TED

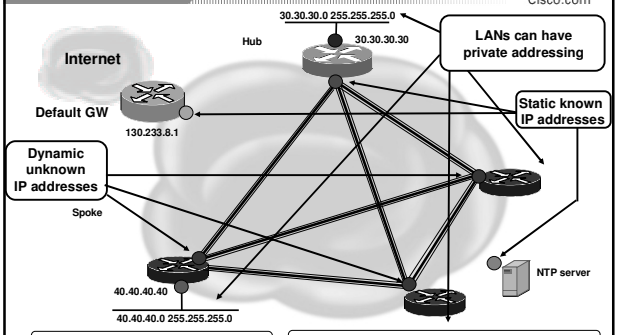
Cisco.com

- **Addressing**
  - As the probe uses the protected entities address (A, B) these address MUST be routable
  - TED is thus not applicable for VPN over Internet
- **Deployment**
  - All IPsec routers must have TED enabled
  - deployment on ALL routers SIMULTANEOUSLY...

www.ietf.org/internet-drafts/draft-fluhrer-ted-01.txt

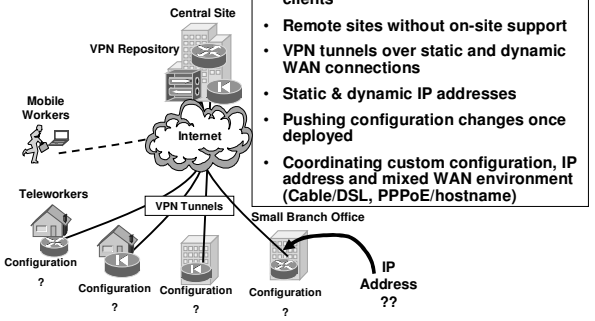
Dynamic Multipoint VPN - IOS 12.2(13)T

Cisco.com



VPN Deployment & Management Challenges

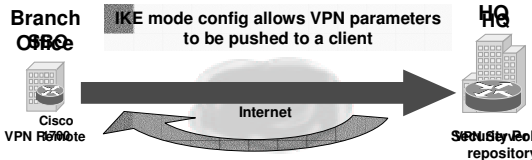
Cisco.com



- Heterogeneous CPE devices and clients
- Remote sites without on-site support
- VPN tunnels over static and dynamic WAN connections
- Static & dynamic IP addresses
- Pushing configuration changes once deployed
- Coordinating custom configuration, IP address and mixed WAN environment (Cable/DSL, PPPoE/hostname)

Easy VPN Client Implementation

Cisco.com



Dynamically updated:
- central services and security policy
- offload VPN function from local devices
- Client and Network Extension mode

- Internal IP Address
- Internal Network Mask
- Internal DNS Server
- Internal WINS Server
- Split tunneling
- IPsec Transforms

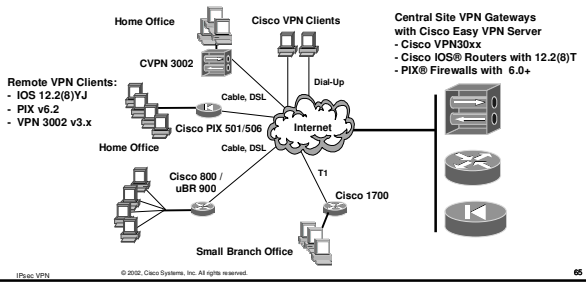
Centralized control:
- configuration and security policy pushed at the time of the VPN tunnel establishment

Cisco Easy VPN Remote and Server

Cisco.com

Cisco Easy VPN Remote
Eliminates complex remote-side configuration simplifying VPN deployments

Cisco Easy VPN Server
Accepts VPN connection from Cisco VPN clients and Cisco Easy VPN Remote devices



Cisco Easy VPN HW Family

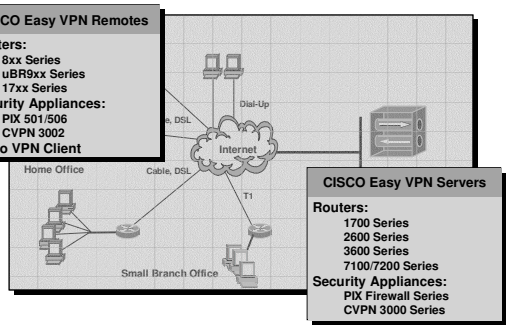
Cisco.com

CISCO Easy VPN Remotes

Routers:
- 8xx Series
- uBR9xx Series
- 17xx Series

Security Appliances:
- PIX 501/506
- CVPN 3002

Cisco VPN Client



CISCO Easy VPN Servers

Routers:
- 1700 Series
- 2600 Series
- 3600 Series
- 7100/7200 Series

Security Appliances:
- PIX Firewall Series
- CVPN 3000 Series

Easy VPN Remote IOS commands

Cisco.com

- crypto ipsec client ezvpn {profile_name}
  - group <group-name> key <group-key>
  - mode {[client] | network-extension}
  - peer {<ip-address> | <hostname*>}
  - local-interface {<ip-address> | <hostname>}
  - connect {auto | manual}
- interface <interface-name>
  - crypto ipsec client ezvpn <profile_name>
  - crypto ipsec client ezvpn default <inside | outside >

** Does DNS resolution at tunnel initiation*

Cisco Router Web Setup (CRWS) v3.1

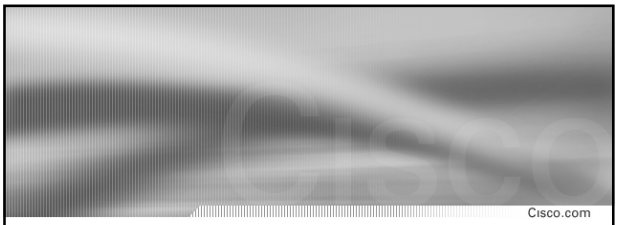
Cisco.com

Cisco Router Web Setup 3.1 configuration for:
- NAT/PAT, DHCP Server/Relay
- Firewall, Voice-over IP dial plans
- Easy VPN configuration and tunnel login

Where to use what

Cisco.com

	IPsec	IPsec/GRE
Dynamic addresses	Yes	Yes - DMVPN
Full mesh	Yes (TED)	Partial mesh
Easy VPN	Yes	No
HSRP/RRI	Yes	IPsec only
	IP only	Multiprotocol, multicast

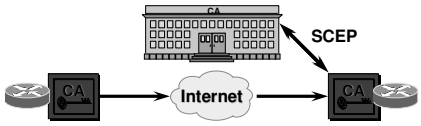


Cisco.com

Scalable Authentication with IOS PKI Enhancements

Public Key Infrastructure

Cisco.com



- Certificate Authority (CA) verifies identity
- Certificate equivalent to an ID card
- Interoperability delivered through industry standards - Simple Certificate Enrollment Protocol (SCEP)

PKI and Cisco

Cisco.com

- Build open PKI aligned with PKIX

  http://www.ietf.org/internet-drafts/draft-nourse-scep-06.txt
- Support of leading CA vendors
  - ✓ Verisign summer 98
  - ✓ Entrust summer 98
  - ✓ Netscape CMS 3.1 end 99
  - ✓ Microsoft Windows 2000 February 00 *requires Windows Resource Kit*
  - – Baltimore Technologies 00
  - – RSA Keon, XCert,…

PKI Features in Cisco IOS 12.2T

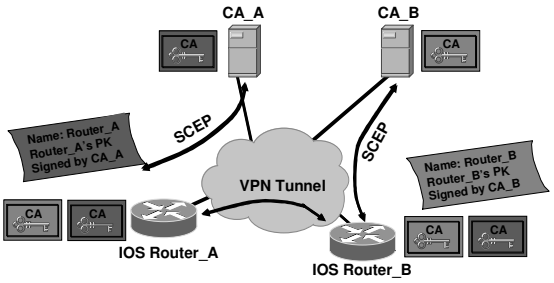
Cisco.com

- 12.1(5)T 2-Tiered Certificate Chaining
- 12.2(2)T Multiple Certificates per Router (one key pair)
- 12.2(4)T Distinguished Name (DN) Based Crypto Maps
- 12.2(8)T Separate Key-Pair per Identity
- 12.2(8)T Multi-Certs per Router (multiple key pair)
- 12.2(8)T Certificate Auto-Enrollment

Existing PKI Features…

Cisco.com

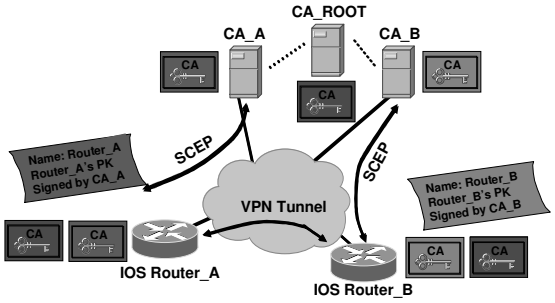
12.1(4)/12.1(1)T Multi Root Support



Existing PKI Features…

Cisco.com

12.1(5)T 2-Tiered Certificate Chaining



12.2(2)T Multiple Certificates per Router

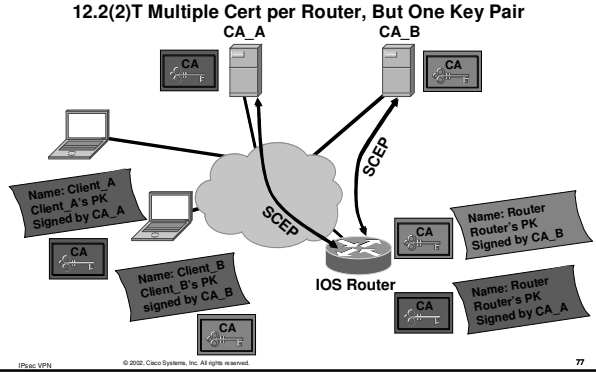
Cisco.com

- Multiple certificates is an essential feature for a PKI environment
- Adds flexibility to terminate tunnels initiated by devices enrolled with different CA's

Existing PKI Features…

Cisco.com

12.2(2)T Multiple Cert per Router, But One Key Pair



12.2(8)T Separate Key-Pair per Identity

Cisco.com

crypto key generate rsa [<keypairlabel>]

! FQDN still default value for generation

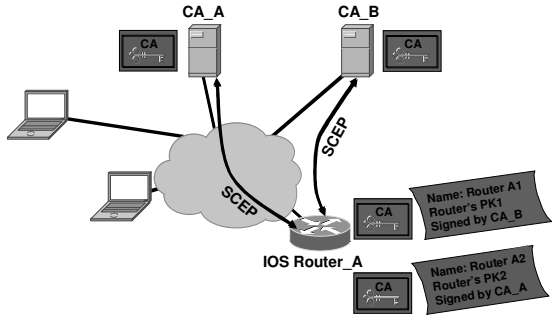
Additional '**crypto ca trustpoint**' CLI command:

rsakeypair <keypairlabel>

- Current Key-Pair is labeled with the routers FQDN
- Feature gives ability to tie keys to different Key-Pair labels and specify label under Trustpoint
- Changing label requires re-enrollment with CA
- Enables variable key lengths for different identities where security policy so requires.

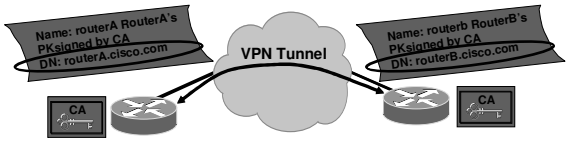
12.2(8)T Separate Key-Pair per Identity

Cisco.com



12.2(4)T Distinguished Name (DN) Crypto Maps

Cisco.com



- **Customer wants to restrict access to selected encrypted interfaces to peers with specific certificates, and in particular, certificates with particular DNs**

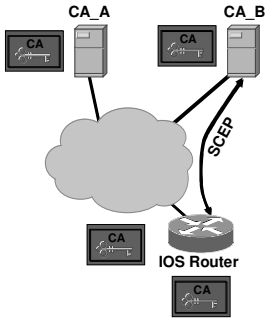
12.2(4)T Distinguished Name (DN) Crypto Maps

Cisco.com

- **Allow user to set restrictions in the router configuration**
  - **Add the function to the existing static and dynamic crypto maps and a tighter control on access is achieved**

12.2(8)T Certificate Auto-Enrollment

Cisco.com




```
crypto ca trustpoint lab.cisco.com
enrollment mode ra
enrollment url
http://CA1/certsrv/mscep/mscep.dll
password 7 104D000A0618
subject-name OU=Lab1
auto-enroll 90 regenerate
```

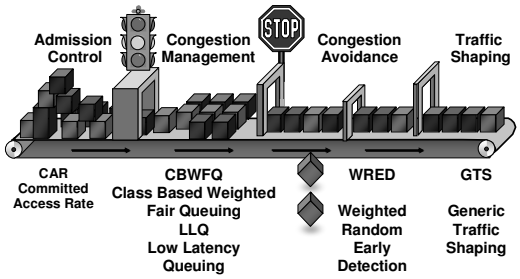
At start and when certificate lifetime % expires router starts SCEP to re-enroll aautomatically

Cisco.com

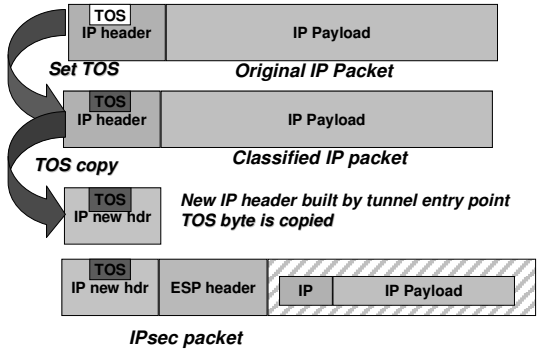
IPsec and QoS

QoS Policy Enforcement

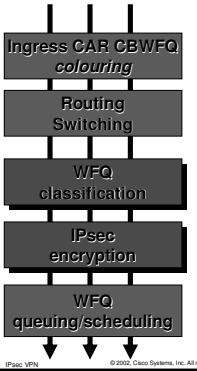
Cisco.com



Tunnels IPsec & QoS



WFQ and IPsec



- If

```
crypto map …
    qos pre-classify
```

IOS 12.2
IOS 12.1(5)T

- WFQ

  classification based on IP addresses, protocols, (L4 ports) of clear text packets

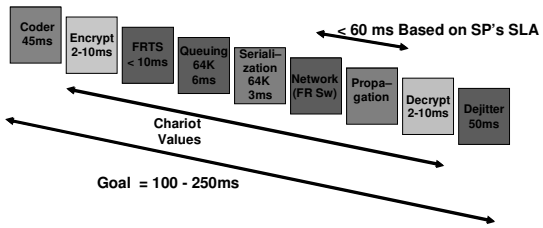
  weight based on IP precedence

  => multiple queues are used

IPsec and VoIP

Delay Budget

Expect IPsec Encryption to add 2-10ms…
…not your largest delay worry



VoIP & RTP

	IP	UDP	RTP	Voice
Length (bytes)	20	8	12	20

Payload (voice): 20 bytes
Overhead: 40 bytes
Total packet: 60 bytes

If codec = 8 kbps, actual line utilization is 24 kbps !

VoIP & Compressed RTP *RFC 2508*

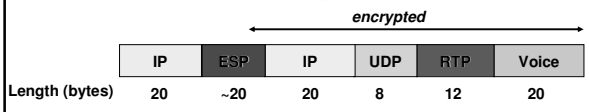
	cRTP	Voice
Length (bytes)	~3	20

Payload (voice): 20 bytes
Overhead: ~3 bytes
Total packet: ~23 bytes

If codec = 8 kbps, actual line utilization is 9 kbps
cRTP compress IP+UDP+RTP only
cRTP works only link-by-link over PPP, …

VoIP & RTP & IPsec = Adding Headers

Cisco.com

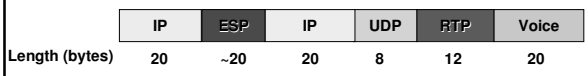


Payload: 20 bytes
Overhead: 80 bytes
Total packet: 100 bytes

If codec = 8 kbps, actual line utilization is 40 kbps !

IPsec and cRTP ?

Cisco.com



- **cRTP does not work because IP+ESP != IP+UDP+RTP**
- **Two bad effects:**
  - **Serialization time increased**
  - **Line utilization increased**
- **The worst effect seen in reality**
- **IETF work on *Robust Header Compression (RFC3095)***

Summary

Cisco.com

- **IPsec deployment**
  - **Cisco VPN Portfolio**
  - **IPsec Remote Access VPNs**
  - **IOS and IPsec**
  - **Deployment topologies**
  - **Scalable Authentication with IOS PKI Enhancements**
  - **IPsec and QoS, VoIP**
- **Wrap up and Q&A**

Wrap up and Q&A

Cisco.com

Information Resources

Cisco.com

IPsec The New Security Standard for Internet, Intranets, and Virtual Private Networks; *Harkins Dan, Doraswamy Naganand*
Prentice Hall PTR; 1999

Demystifying the IPsec Puzzle; *Frankel Sheila*, Artech House; April 2001

www.ietf.org RFC 2401-… or www.vpnc.org for VPN draft collection

IETF IPsec mailing list: *ipsec@lists.tislabs.com*

Archives at *www.vpnc.org/ietf-ipsec* **or** *www.ietf.org/internet-drafts*

Cisco VPN resource pointers:

Cisco.com/go/evpn and Cisco.com/go/v3pn

List of Acronyms

Cisco.com

AES - Advanced Encryption Standard
AH - Authentication Header
CA - Certificate Authority
CRL - Certificate Revocation List
DES - Data Encryption Standard
3DES - Triple Data Encryption Standard
DSA - Digital Signature Algorithm
ESP - Encapsulating Security Protocol
HMAC - Hash-Based Message Authentication Code
IDEA - International Data Encryption Algorithm
IKE - Internet Key Exchange
IPsec - IP Security Protocol
MD5 - Message Digest 5
PKI - Public Key Infrastructure
RC2/4 - Rivest Cypher 2/4
RSA - Rivest, Shamir, Adelman
SADB - Security Association Database
SCEP - Simple Certificate Enrollment Protocol
SHA - Secure Hash Algorithm

Thank you!

Cisco.com

IPsec Deployment

fmajstor@cisco.com

www.cisco.com
98