IPsec VPN Technologies & Trends

Franjo Majstor

World Trade Center Bucharest, 7-8 May 2003

Agenda

- **IPsec VPN Technologies & Trends**
  - **Introduction**
  - **IPsec Technology Deployment**
  - **IOS and IPsec**
  - **Deployment topologies**
  - **Scalable Authentication with IOS PKI Enhancements**
  - **Reference Case**
  - **The Future**
- **Q&A**

Introduction

Brief History of IPsec & IETF

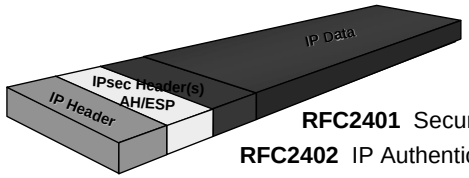
Cisco.com

- **July 1991: An idea was born (21st IETF)**
- **March 1992: IPsec BoF (23rd IETF)**
- **November 1992: (25th IETF) IPsec working group formed**
- **By 1995 multiple interoperable implementations**
- **November 1998 RFC standards**

And the work is still not done…

IPsec Framework

Cisco.com



November 1998 Set of Standards

RFC2401 Security Architecture for the Internet Protocol
RFC2402 IP Authentication Header (AH)
RFC2403 Use of HMAC-MD5-96 within ESP and AH
RFC2404 Use of HMAC-SHA-1-96 within ESP and AH
RFC2405 ESP DES-CBC Cipher Algorithm With Explicit IV
RFC2406 IP Encapsulating Security Payload (ESP)
RFC2407 Internet IP Security Domain of Interpretation for ISAKMP
RFC2408 Internet Security Association and Key Management Protocol (ISAKMP)
RFC2409 Internet Key Exchange (IKE)
RFC2410 NULL Encryption Algorithm and Its Use With IPsec
RFC2411 IP Security Document Roadmap
RFC2412 OAKLEY Key Determination Protocol

IPsec Technology Deployment

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**

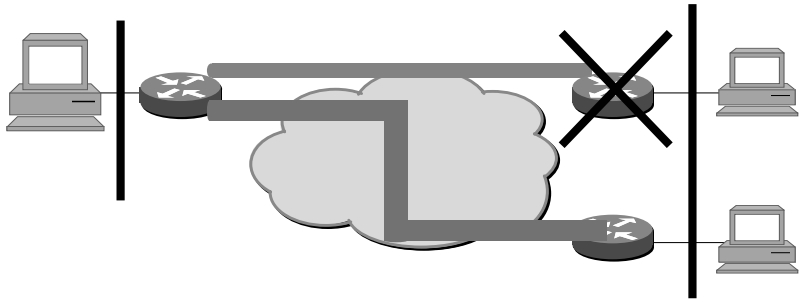
draft-dukes-ike-mode-cfg-03.txt ***draft-beaulieu-ike-xauth-03.txt***

www.vpnc.org/temp-draft-lebovitz-ipsec-scalable-ikev2cp-00.txt

IPsec and Keepalives

Cisco.com

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



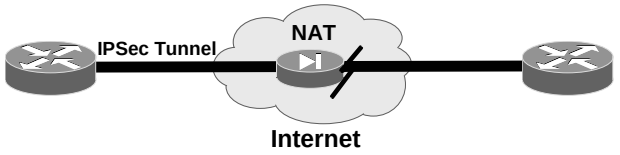
Based on IETF draft "A Traffic-Based Method of Detecting Dead IKE Peers"

www.ietf.org/internet-drafts/draft-ietf-ipsec-dpd-02.txt

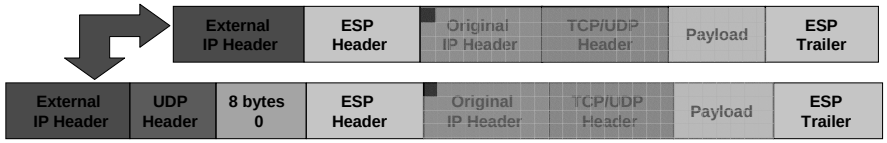
IPSec NAT Transparency

Cisco.com

- **NAT/PAT devices are deployed everywhere, by default don't allow IPSec traffic to pass**



- **IPSec NAT transparency allows IPSec to traverse NAT/PAT devices by wrapping IPSec within UDP**
- **Simplifies VPN design and deployment**



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-06.txt

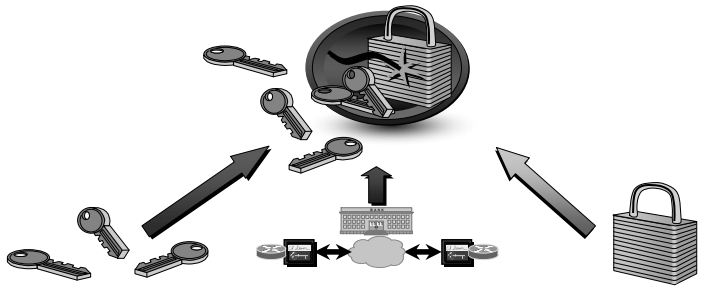
- **IPsec NAT-T:**

  -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-05.txt

IOS and IPsec

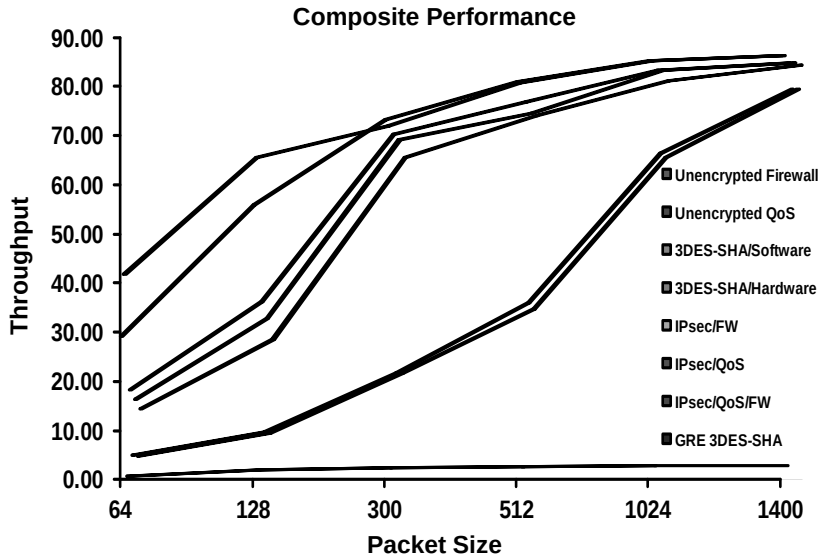
End-to-End Secured VPN



Cisco VPN Solutions Utilize Standards-Based Security

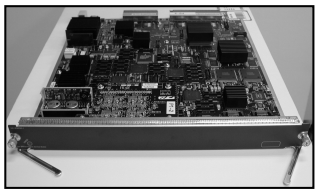
Tunneling	Encryption	Authentication	Integrity
IPsec	DES	RSA digital certificates	HMAC-MD5
GRE/IPinIP	3DES	RADIUS	HMAC-SHA1
L2TP/PPTP	AES		

Performance Vs. Features



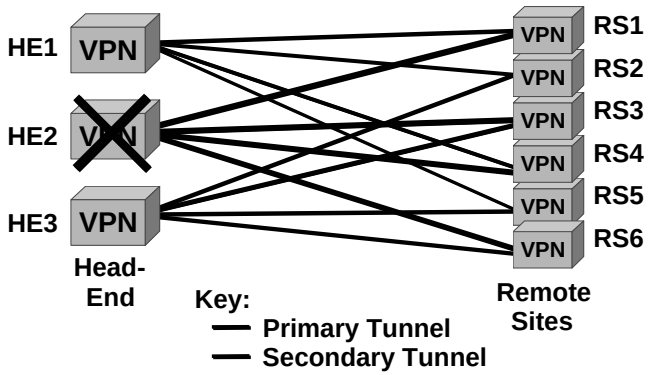
IPsec VPN Services Module

- **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**



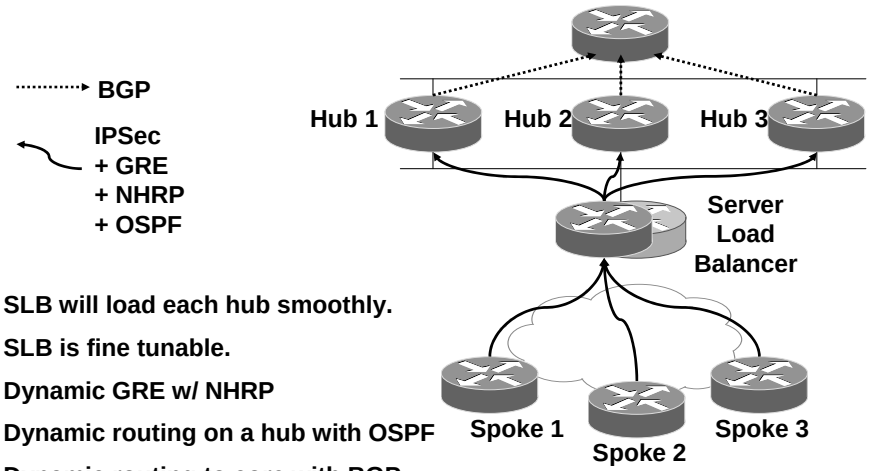
Load Dispersion on Failure

- **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**



High available load based concentration design

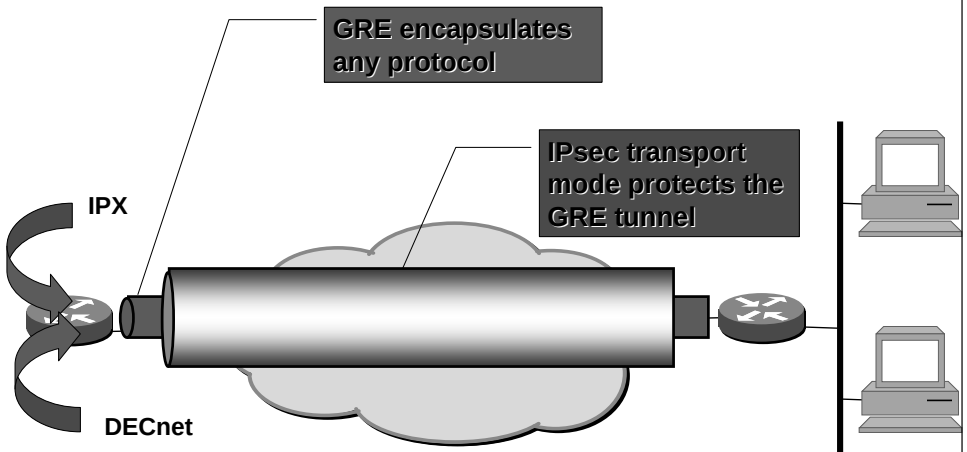
Cisco.com



- SLB will load each hub smoothly.
- SLB is fine tunable.
- Dynamic GRE w/ NHRP
- Dynamic routing on a hub with OSPF
- Dynamic routing to core with BGP

Generic Routing Encapsulation

Cisco.com

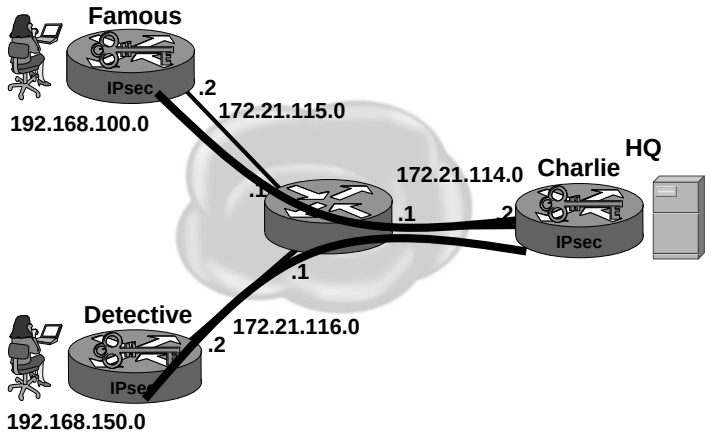


GRE RFC 2784 encapsulates any protocol in IP

Deployment Topologies

A Star Topology

Cisco.com



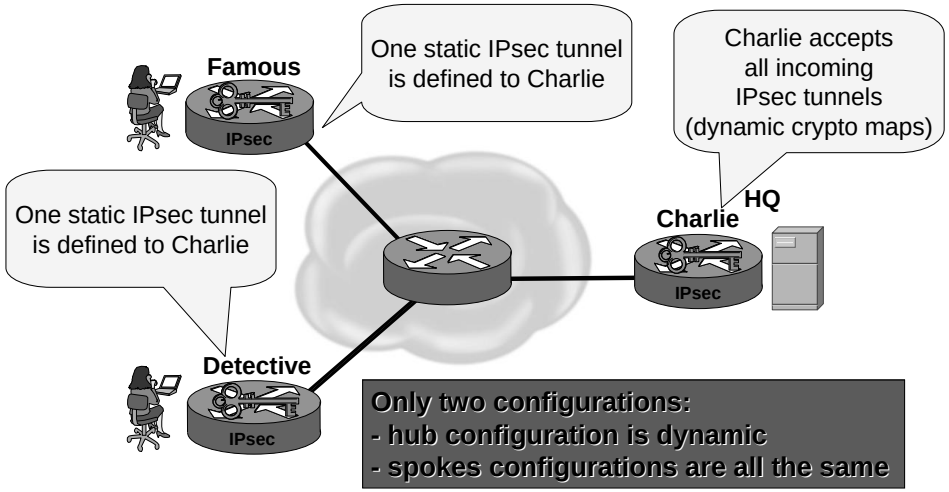
Star Topology Central Site Router - Cfg 1

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



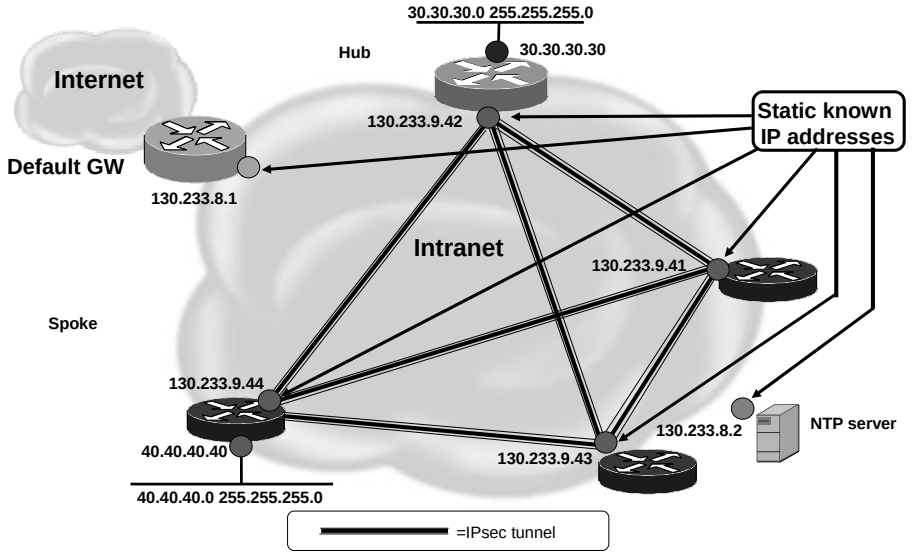
Star Topology Central Site Router - Cfg 2

Cisco.com

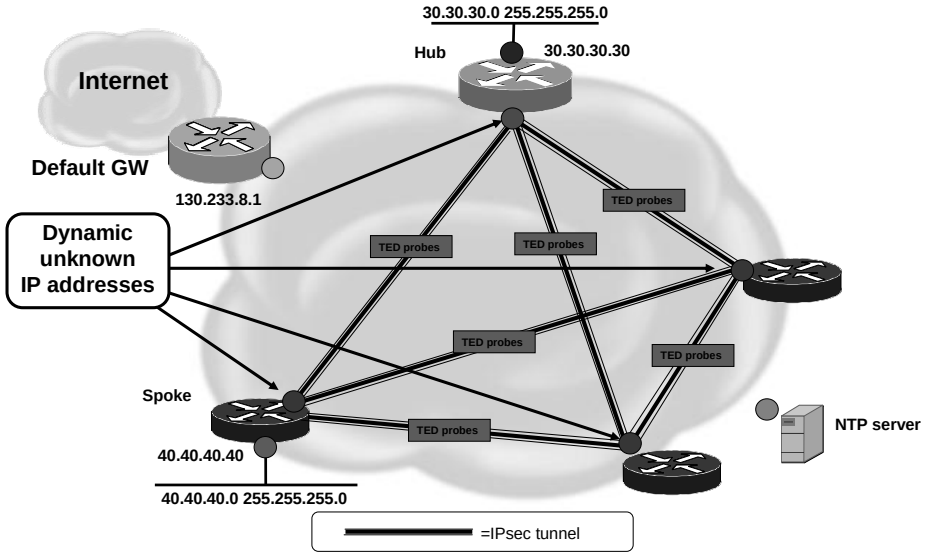
```
! Let's be smart and let's define a single
! Dynamic crypto map
!
crypto map DYNAMIC 10 ipsec-isakmp dynamic TEMPLATE

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


Site-to-Site (Full Mesh) IPsec VPN

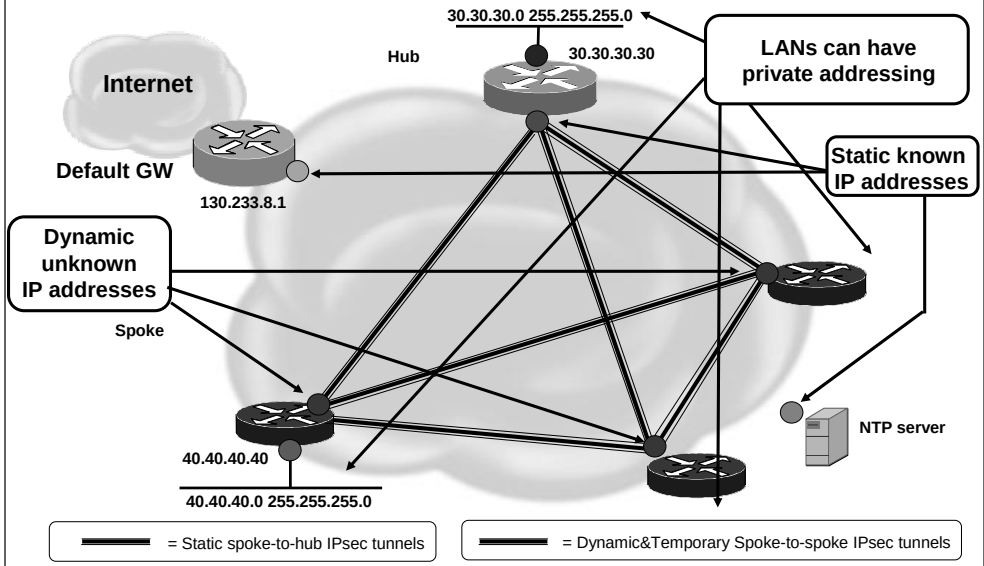
Cisco.com



Full Mesh with TED IPsec VPN



Dynamic Multipoint VPN - IOS 12.2(13)T



Configuration Examples – Hub

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto IPsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
```


Configuration Examples – Hub – Cont.

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

Configuration Size Reduction Example - Hub Router in 300-Spoke Network

Cisco.com

- **Typical Hub Configuration Size**
  - **13 lines per spoke = 3,900 lines**
- **DMVPN Hub Configuration Size**
  - **16 lines**

➢ **Savings: 3,884 lines!**

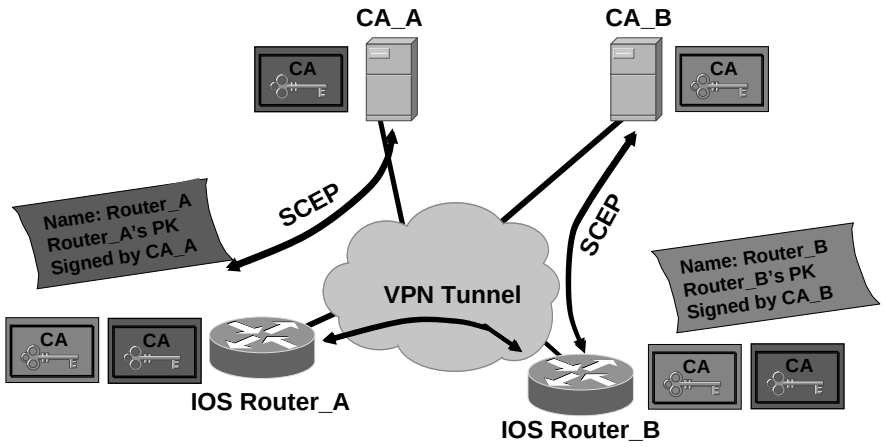
- **(This is the hub configuration related to the spokes, not the entire configuration on the hub router.)**

Scalable Authentication with IOS PKI Enhancements

Existing PKI Features…

Cisco.com

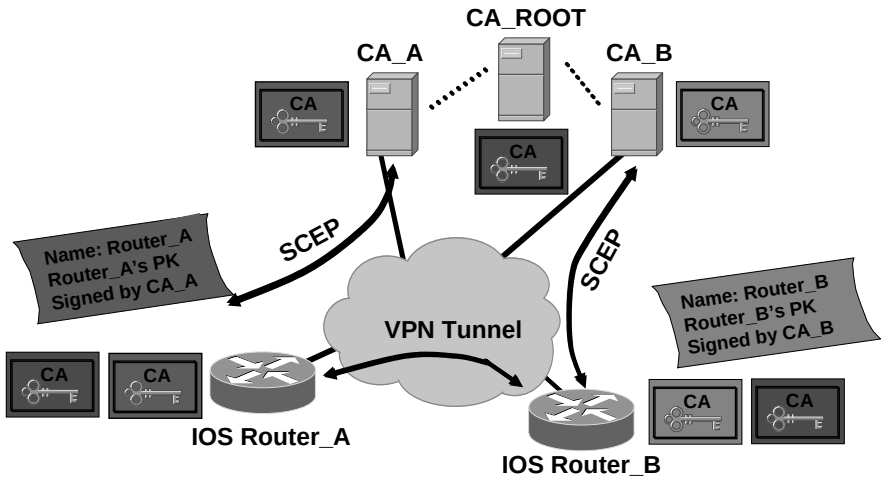
12.1(4)/12.1(1)T Multi Root Support



Existing PKI Features…

Cisco.com

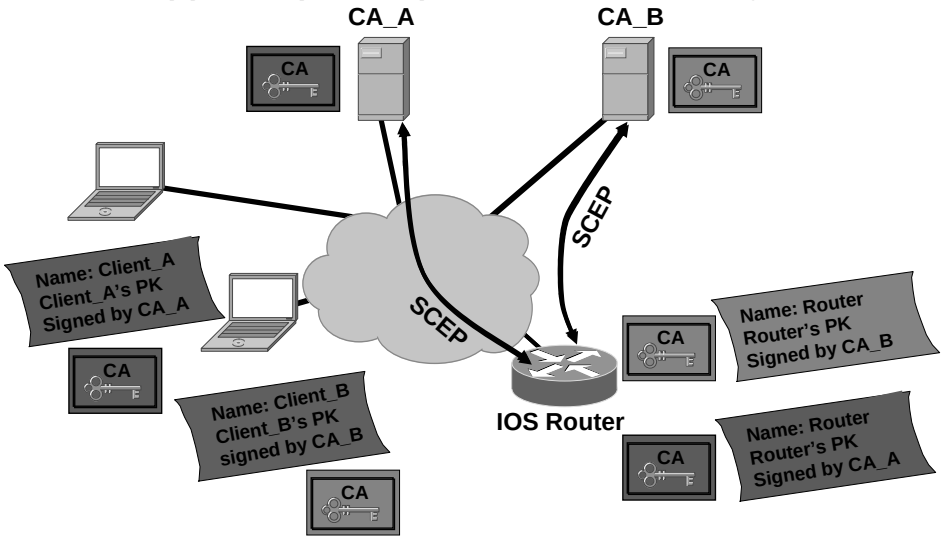
12.1(5)T 2-Tiered Certificate Chaining



Existing PKI Features…

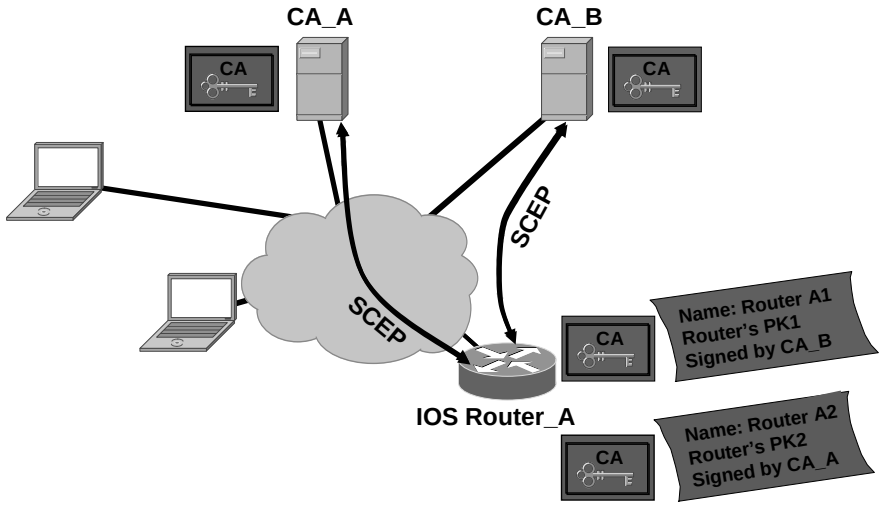
Cisco.com

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



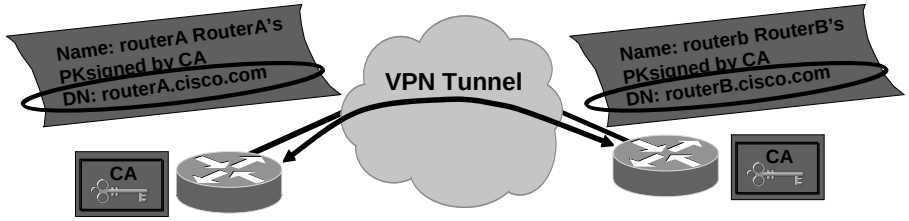
12.2(8)T Separate Key-Pair per Identity

Cisco.com



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

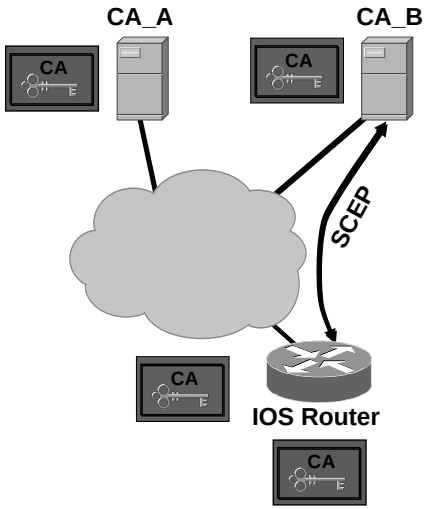
Cisco.com



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

12.2(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

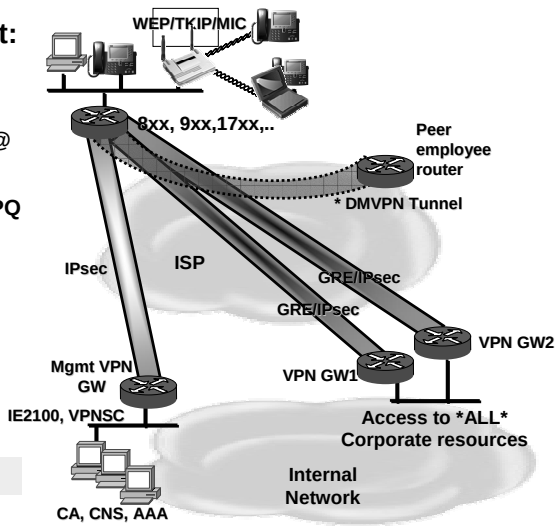
Reference Case

Cisco Internal VPN Deployment Pilot

Cisco Internal Deployment:

- IKE/IPsec with PKI
- IOS Firewall
- GRE for static and dynamic IP@
- NAT Overload [PAT]
- QoS-MQC based CBFWQ and PQ
- Split tunneling
- Multicast [IP/TV]
- MGRE + NHRP
- Nat traversal
- Pre-provisioning
- IP Telephony

> 600 sites in USA and Europe



Cisco.com/warp/public/cc/pd/iosw/prodlit/stlvp_cg.htm

The Future

Quo Vadis IPsec?

- Reduce complexity of existing framework
- Standardize method of IPsec traversing firewalls and NAT boxes
- Standardize method for peer detection
- New algorithms support (AES, EC,...)
- New protocols support (SCTP,iSCSI,…)
- New Key Exchange protocol

Mutiple proposals (IKEv2, JFK, SigMA,…) now merged into one:

- IKEv2

Quick Comparison of IKEv1 vs IKEv2

Cisco.com

	IKEv1	IKEv2
UDP port	500	500, **4500**
Phases	2	2
DPD	No	**Yes**
Pre-shared keys	Yes	Yes
UDP/NAT	No	**Yes**
SA Negotiation	Yes	Yes
Number of msgs	6-9	**4-6**
EAP/CP	No	**Yes**

www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-07.txt

Summary

Cisco.com

- **IPsec VPN Technologies & Trends**
  - **Introduction**
  - **IPsec Technology Deployment**
  - **IOS and IPsec**
  - **Deployment topologies**
  - **Scalable Authentication with IOS PKI Enhancements**
  - **Reference Case**
  - **The Future**
- **Q&A**

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 IPsec VPN resource pointers:

Cisco.com/go/security *and* ***Cisco.com/go/v3pn***

Thank you!

Cisco.com

IPsec VPN Technologies & Trends

fmajstor@cisco.com

Empowering the Internet Generation℠