CISCO SYSTEMS

© 2002, Cisco Systems, Inc. All rights reserved. 1

Cisco.com

IPsec VPN Technologies & Topologies

EXPO 2002 Athens

December 13th 2002

Franjo Majstor

EMEA Consulting Engineer

Cisco Systems, Inc

fmajstor@cisco.com

© 2002, Cisco Systems, Inc. All rights reserved. 2

Agenda

Cisco.com

- IPsec VPN Tehnologies & Topologies
  - Cisco VPN Portfolio
  - IPsec Remote Access VPNs
  - IOS and IPsec
  - Deployment topologies
  - Scalable Authentication with IOS PKI Enhancements
  - Reference case
- Q&A

 © 2002, Cisco Systems, Inc. All rights reserved.

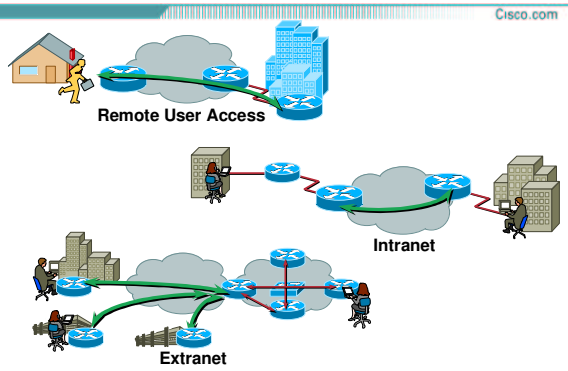
Cisco.com

Cisco VPN Portfolio

© 2002, Cisco Systems, Inc. All rights reserved. 4

Applications of IPsec

Cisco.com



 © 2002, Cisco Systems, Inc. All rights reserved.

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

 © 2002, Cisco Systems, Inc. All rights reserved.

 Copyright © 2002, Cisco Systems, Inc. All rights reserved.

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

 © 2002, Cisco Systems, Inc. All rights reserved.

Voice and Video Enabled VPN - V³PN

New

Cisco.com

V³PN 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

© 2002, Cisco Systems, Inc. All rights reserved.

Remote Access VPN

Cisco.com

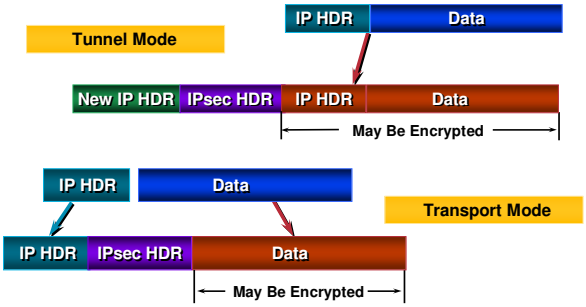
Encapsulate original (green) packet in a new packet (red), traverse shared backbone and require:

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

 © 2002, Cisco Systems, Inc. All rights reserved.

IPsec Modes

Cisco.com

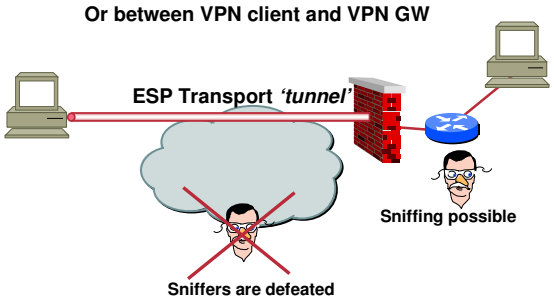


 © 2002, Cisco Systems, Inc. All rights reserved.

IPsec Tunnel Mode

Cisco.com

Or between VPN client and VPN GW



 © 2002, Cisco Systems, Inc. All rights reserved.

 Copyright © 2002, Cisco Systems, Inc. All rights reserved.

IPsec and Keepalives

Cisco.com

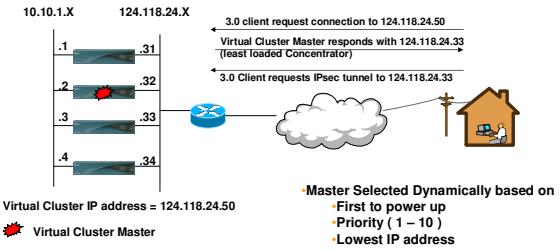
Specific configuration of IPsec/IKE peer to allow resilience/load balancing

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

 © 2002, Cisco Systems, Inc. All rights reserved.

Advanced Features - Load balancing

Cisco.com



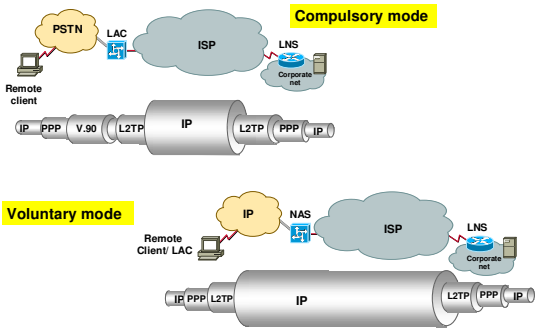
- Master Selected Dynamically based on
  - First to power up
  - Priority (1 – 10)
  - Lowest IP address

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

 © 2002, Cisco Systems, Inc. All rights reserved.

VPN RA Alternatives - L2TP

Cisco.com



 © 2002, Cisco Systems, Inc. All rights reserved.

VPN RA Alternative - L2TP and IPsec

Cisco.com

L2TP is used for:

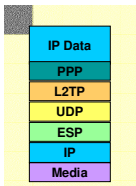
- user authentication (PAP,CHAP, EAP)
- IPCP: IP address, DNS/WINS server config
  (centrally managed via RADIUS server)
- multi-protocol support (IP, IPX, AT,…)
- multicast

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



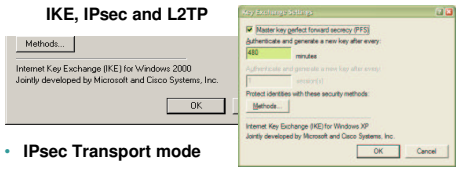
LT2P/IPsec Stack

 © 2002, Cisco Systems, Inc. All rights reserved.

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

 © 2002, Cisco Systems, Inc. All rights reserved.

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)**

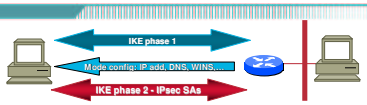
Goal: easy configuration of IPsec client

 © 2002, Cisco Systems, Inc. All rights reserved.

 Copyright © 2002, Cisco Systems, Inc. All rights reserved.

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

 © 2002, Cisco Systems, Inc. All rights reserved.

IKE Extended Authentication (Xauth)

Cisco.com

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

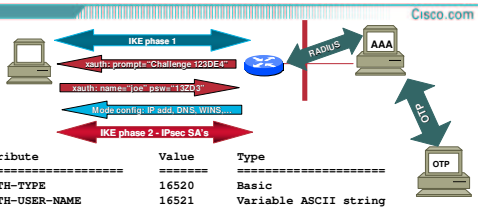
- IETF draft to authenticate the USER using a remote IPsec client
- Just after IKE phase I (main or aggressive mode) and after configuration mode

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

 © 2002, Cisco Systems, Inc. All rights reserved.

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

 © 2002, Cisco Systems, Inc. All rights reserved.

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)

 © 2002, Cisco Systems, Inc. All rights reserved.

IPsec VPN and NAT/PAT Transparency

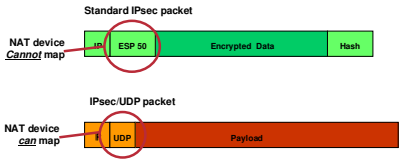
Cisco.com

- IPsec/UDP

  Allows clients to operate behind a NAT device

  Provides the security of IPsec/ESP

  Requires no user intervention



 © 2002, Cisco Systems, Inc. All rights reserved.

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

 © 2002, Cisco Systems, Inc. All rights reserved.

fmajstor@cisco.com, IPsec VPNs , Copyright © 2002, Cisco Systems, Inc. All rights reserved.

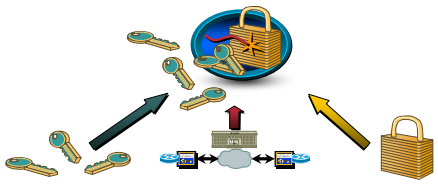
Cisco.com

IOS and IPsec

© 2002, Cisco Systems, Inc. All rights reserved. 25

End-to-End Secured VPN

Cisco.com



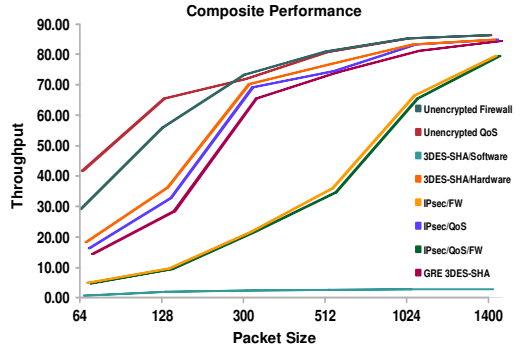
Cisco VPN Solutions Utilize Standards-Based Security

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

 © 2002, Cisco Systems, Inc. All rights reserved. 26

Performance Vs. Features

Cisco.com



 © 2002, Cisco Systems, Inc. All rights reserved. 27

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

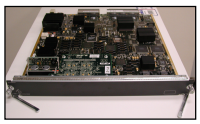
 © 2002, Cisco Systems, Inc. All rights reserved. 28

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

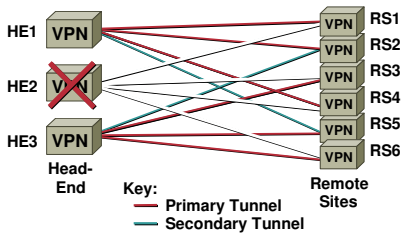


 © 2002, Cisco Systems, Inc. All rights reserved. 29

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



 © 2002, Cisco Systems, Inc. All rights reserved. 30

 Copyright © 2002, Cisco Systems, Inc. All rights reserved.