Cisco.com

IPsec VPN Made Easy

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

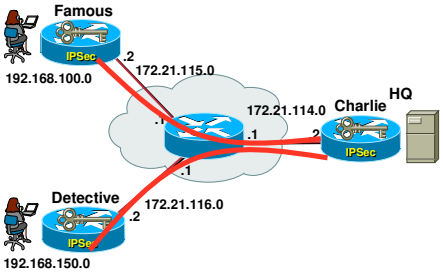
Agenda

Cisco.com

- VPN Deployment & Management Challenges
- Technology background
- Cisco Easy VPN Solution
- Q&A

A Star Topology IPsec VPN

Cisco.com



Star Topology Central Site Router

Cisco.com

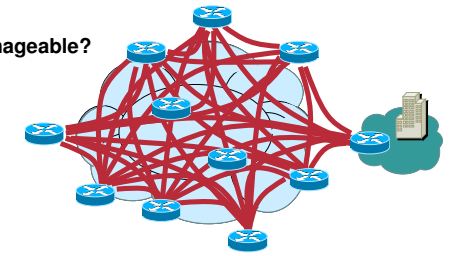
```
! Let's be courageous and let's define
! One crypto map entry per remote peer
! ...
crypto map HQ 10 ipsec-isakmp
 set peer 172.21.115.2
 set transform-set encrypt-des
 match address 101

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


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

Cisco.com

Is this Manageable?

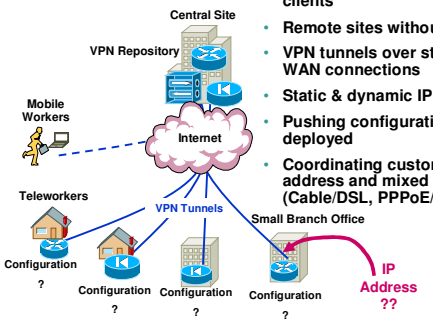


Copyright © 2002, Cisco Systems, Inc. All rights reserved.

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)



VPN Technology Requirements

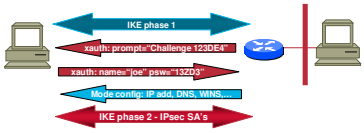
Cisco.com

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)
- Network Address Translation

Technology background - IKE Xauth/Mode-cfg

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		

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

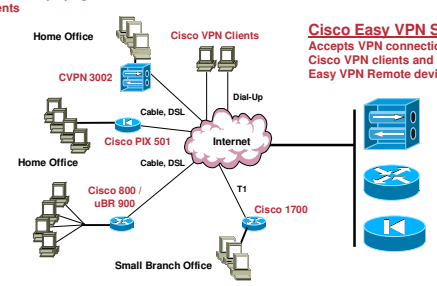
draft-beaulieu-ike-xauth-03.txt

Cisco Easy VPN Solutions Leverages Cisco Unified VPN Client Framework

Cisco.com

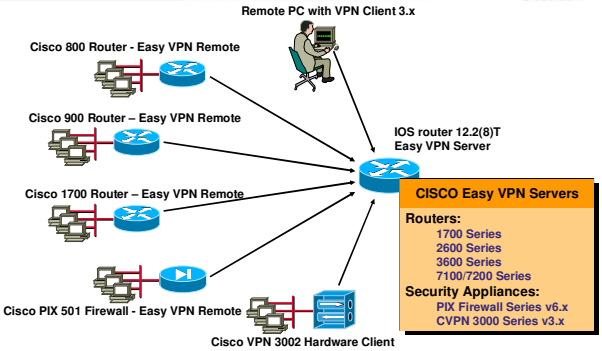
Cisco Easy VPN Remote
Eliminates complex remote-side configuration simplifying VPN deployments

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



Remote Access Using Cisco Easy VPN

Cisco.com



CISCO Easy VPN Servers

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

Security Appliances:
- PIX Firewall Series v6.x
- CVPN 3000 Series v3.x

Easy VPN Feature Support

Cisco.com

- Mode configuration version 6 support
- Xauth version 6 support
- IKE Dead Peer Detection (DPD)
- Split tunneling control
- Dynamic NAT/PAT configuration
- Proxy DNS
- Group-based policy control

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

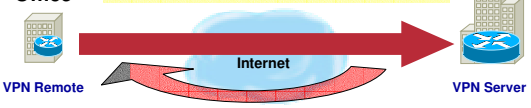
Push VPN Policy with Cisco Easy VPN

Cisco.com

Branch Office

IKE mode config allows VPN parameters to be pushed to a client

HQ



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

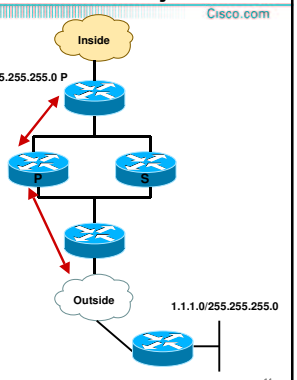
Centralized control:

- Configuration and security policy pushed at the time of the VPN tunnel establishment

Easy VPN server - Reverse Route Injection

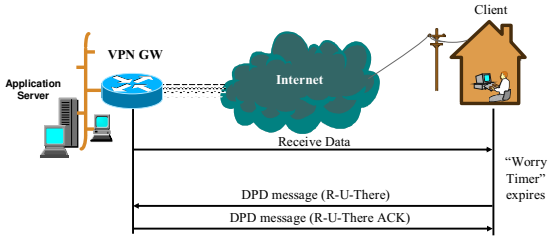
Cisco.com

- 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.



IKE Keepalives - Dead Peer Detection (DPD)

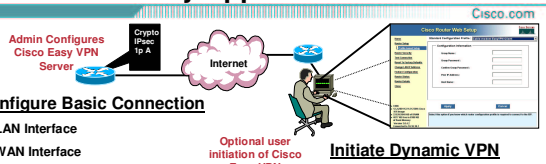
Cisco.com



www.ietf.org/internet-drafts/draft-ietf-ipsec-dpd-01.txt

Cisco Easy VPN Remote Initiation on Cisco Routers & Security Appliances

Cisco.com



1. Configure Basic Connection
   - LAN Interface
   - WAN Interface
   - DNS Address
   - DHCP Address
   - NAT / PAT Configuration (optional)
2. Configure Cisco Easy VPN Specifics
   - Mode (client or network ext.)
   - Peer address
   - VPN tunnel interface
   - Group name and password
   - User name and password

Initiate Dynamic VPN

100% pre-configured and automated initiation

Optional: admin final set up with Web, CLI, Telnet or console

Optional: user final set up (Cisco 800 & uBR900, CVPN 3002 and Cisco PIX 501 FW only)

- Group Name, Group Password, Peer IP Address, Host Name

•Optional: dynamic/ongoing device authentication

Simple with GUI - Example Cisco 800 Series

Cisco.com

Setting up Cisco Easy VPN Remote

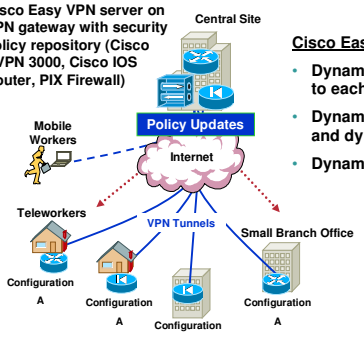
- Non-technical users can enable Easy VPN with simple login information provided by IT
- No pre-configuration required, standard router configuration can be used

Cisco Easy VPN Remote GUI support on Cisco 800, 900, Cisco PIX Firewalls, and CVPN 3002

Scalable VPN Deployment & Management

Cisco.com

Cisco Easy VPN server on VPN gateway with security policy repository (Cisco CVPN 3000, Cisco IOS Router, PIX Firewall)



Cisco Easy VPN Remote and Server

- Dynamic policy updates, pushed to each CPE and clients
- Dynamic VPN tunnels over static and dynamic WAN connections
- Dynamic & static IP addresses

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

Summary - Cisco Easy VPN Benefits

Cisco.com

- Streamlines VPN deployments for remote offices and teleworkers
- Simplifies on-going VPN management
- Ensures and applies up-to-date policies before connections are established
- Removes complex remote-side administration burden
- Provides a consistent policy, key management and system management approach for all Cisco VPN CPE devices - routers, security appliances and software clients

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

Questions?

Cisco.com

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

Thank you!

Cisco.com

IPsec VPN Made Easy

fmajstor@cisco.com

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

© 2002, Cisco Systems, Inc. www.cisco.com

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