Cisco Easy VPN on Cisco IOS Routers

April 2008

Cisco.com/go/easyvpn

Agenda

- Cisco® Easy VPN Overview
- Enhanced Easy VPN Architecture
- Feature Details
  - Network Integration
  - Centralized Provisioning and Management
  - Authentication Services
  - High Availability
- Platform Support Table

Cisco IOS Secure Connectivity Overview

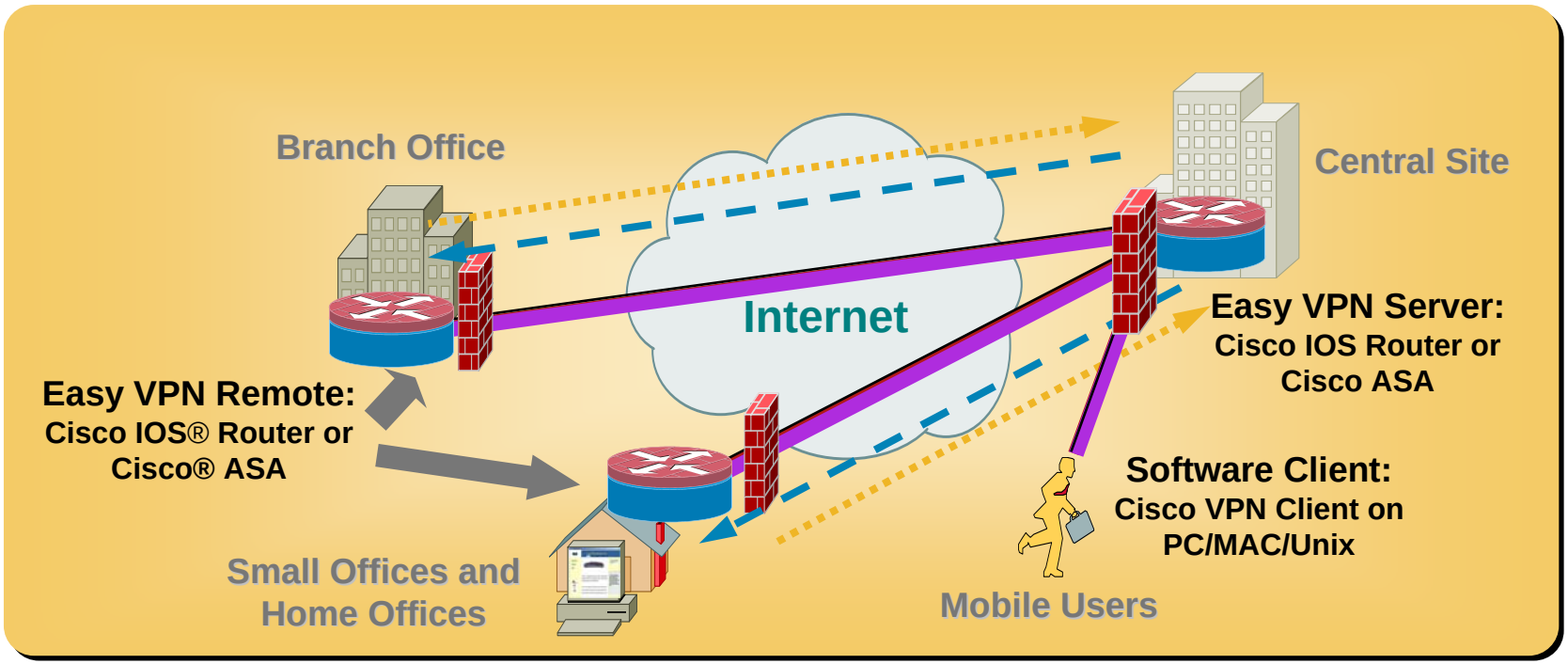
Industry-Leading VPN Solutions

Solution	Key Technologies
Standard IPsec	▪ Full standards compliance for interoperability with other vendors
Advanced Site-to-Site VPN	▪ Hub-and-Spoke VPN: **Enhanced Easy VPN – Dynamic Virtual Tunnel Interfaces, Reverse Route Injection (RRI), dynamic policy push and high scalability** **Routed IPsec + Generic Routing Encapsulation (GRE) or Dynamic Multipoint VPN (DMVPN) with dynamic routing** ▪ Spoke-to-Spoke VPN: DMVPN – On-demand VPNs (partial mesh) ▪ Any-to-Any VPN: Group-Encrypted Transport (GET) VPN – No point-to-point tunnels
Advanced Remote Access VPN	▪ Easy VPN (IPsec): Cisco® dynamic policy push and included VPN Clients for Windows, Linux, Solaris and Mac platforms ▪ SSL VPN: No client pre-installation required and provides endpoint security through Cisco Secure Desktop

Cisco IOS VPN Key Differentiators

First to Market	**Cisco® is the first to support innovative VPN solutions like Easy VPN, DMVPN, GET VPN on an integrated services access router**
Platform Support	**Cisco has comprehensive VPN platform offerings including support for Cisco 800-3800 Series, Cisco 7200 Series, Cisco 7301 routers, Cisco 7600 Series, and Cisco Catalyst® 6500 Series**
Integration	**Cisco VPN solutions have advanced network integration capabilities such as QOS, multicast, voice and video**
Feature Performance	**Rich integration of VPN with several routing protocols such as OSPF, EIGRP, BGP, RIPV2 without degrading performance to enable scalable services**
Enhanced Management	**Cisco has comprehensive management suite for provisioning and maintenance of VPN networks**

Cisco Easy VPN Overview



1. **Cisco Easy VPN Unity® Framework**: Remote/branch device can be Cisco IOS router, ASA or PC/Mac/Unix computer running VPN Client software.
2. **Call Home/Authentication:** Remote device contacts central-site router/concentrator, and provides authentication credentials.
3. **Centralized Policy Push:** Central-site checks credentials and "pushes" configuration securely to the remote device.
4. **VPN is established.**

Easy VPN Highlights

Network Integration

- Virtual Tunnel Interface integration provides advanced QoS, IP Multicast and Network Address Translation (NAT) policies
- Advanced VRF integration enables scalable managed services

Ease of Provisioning and Management

- Centralized policy push for dynamic configuration and change management of remote devices from central server

Authentication

- Group and user-based authentication including AAA, RADIUS, Digital Certificates, Xauth, etc.

High Availability

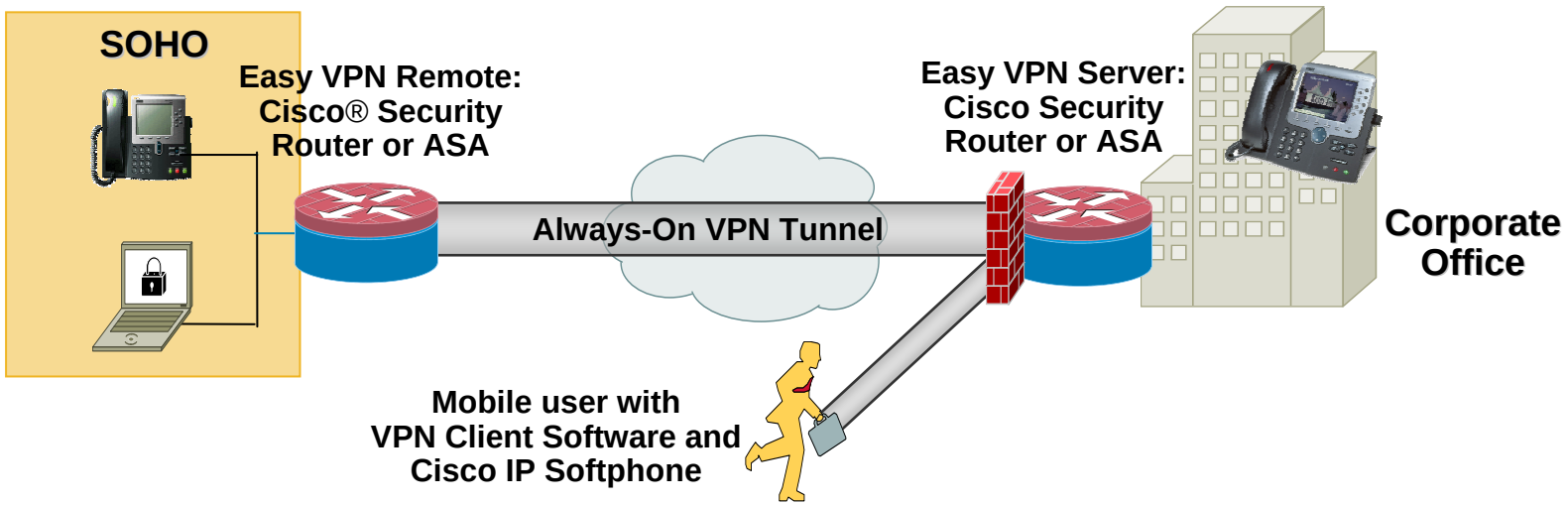
- Several advanced mechanisms such as IPsec stateful failover, Dead Peer Detection (DPD) and Remote Dual Tunnel, provide resiliency required for high scalability

Cisco Easy VPN Use Cases

Easy VPN is suitable for the following customer profiles:

- Requires interoperability between Cisco IOS® routers, Cisco® ASA and PC-based software VPN clients
- Requires per-tunnel QoS/firewall/ACL/NAT policies
- Requires large scale i.e. thousands of remote devices
- Does not require support for non-IP traffic
- Does not require dynamic routing protocol updates through the VPN link

Enterprise Network Designs



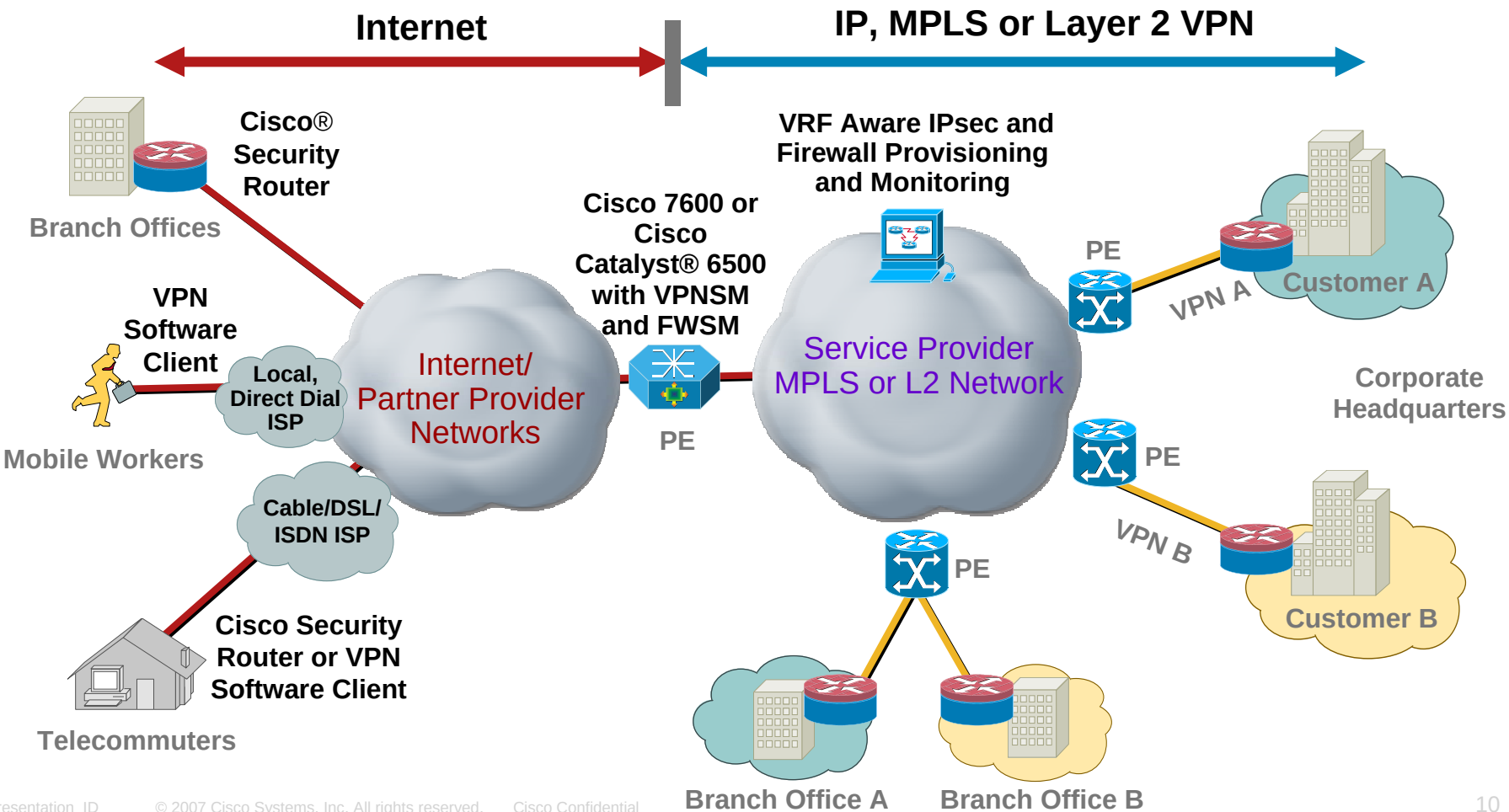
- Easy VPN extends employee access to home or offsite locations
- Mobile users with software VPN client and Cisco IP Softphone
- Enterprise Class Teleworker (ECT) designs for employees working out of home–supports voice (IP phone) and data

Enterprise Network Design: Highlights

- QoS policies to protect voice, video, data traffic
- Allows private IP addressing and NAT on the spokes
- TCP-based Firewall Traversal allows IPsec traffic pass through NAT device and third party firewall in between
- Centralized policy push: Secure, automated configuration and change management of endpoints– including DNS, banner, DHCP, split ACL, etc.
- Extended authentication (Xauth) bypass for IP phones
- Save password on the remote to provide always-on VPN tunnel
- RRI to simplify routing
- Multiple peers, dialup backup for high availability purposes

Service Provider Network Design 1:
VRF Aware IPsec and Firewall with MPLS

- VRF Aware IPsec at the hub segregates customer traffic, introduces IPsec tunnel mapping to MPLS VPNs



Service Provider Network Design 1: Highlights

Highly scalable

- Aggregates a large number of spokes–no dynamic routing, therefore not limited by scale of routing protocols

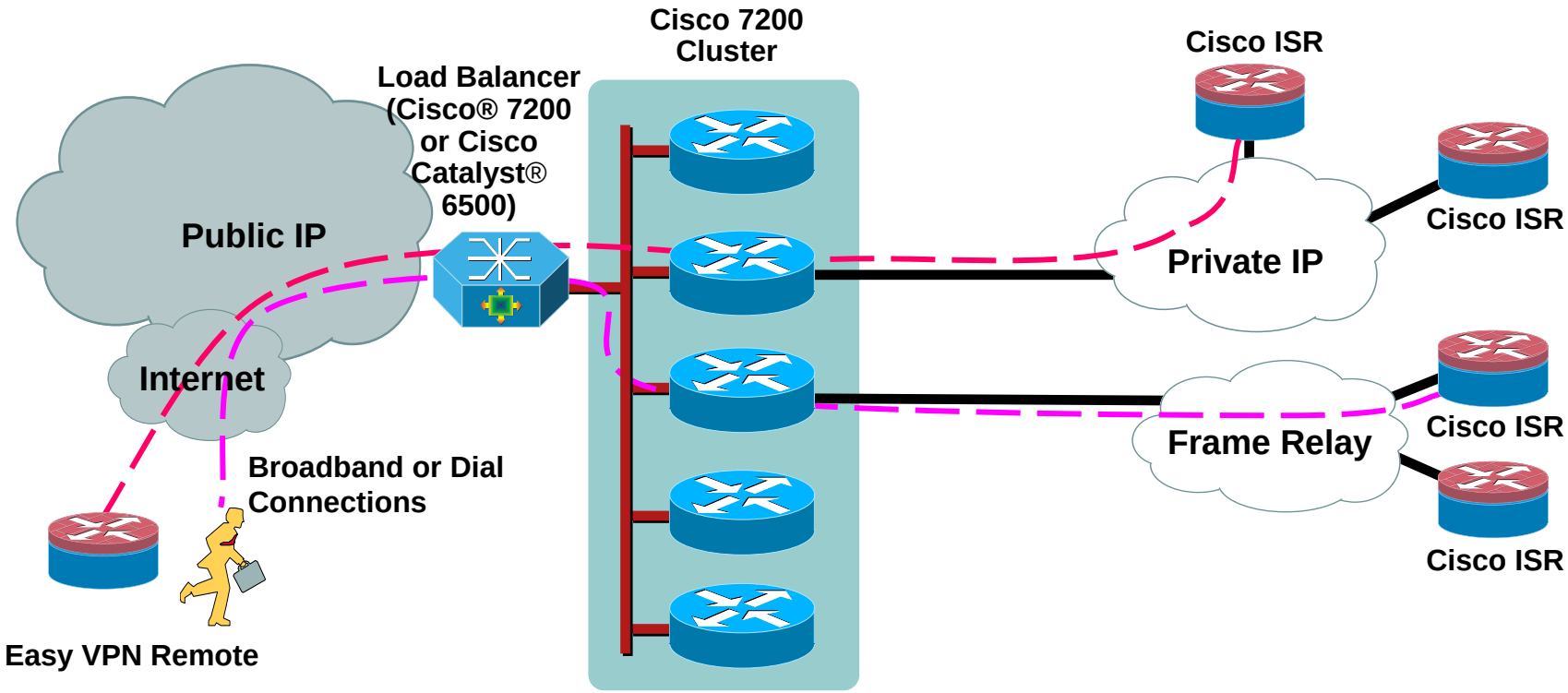
Easy to provision and manage

- Centralized policy push simplifies management for large numbers of clients
- RRI simplifies routing
- NAT integration allows for split tunneling and identical remote IP addressing
- Allows flexibility in the form of enhanced Easy VPN split tunneling and/or multiple routed subnet scenarios

Highly available

- Multiple peers, dialup backup, dual-tunnels

Service Provider Network Design 2:
Server Load Balancing



- Very large scale hub-and-spoke designs – thousands of spokes
- Tunnels load balanced automatically over available hubs
- N+1 hub redundancy
- Multiply performance by number of identical hubs e.g. creation rate, speed, maximum number of Security Associations (SAs)

Enhanced Easy VPN Architecture

Enhanced Easy VPN Architecture

Extends Easy VPN and IP Services Integration

Problem Statement

- Certain deployments require the ability to treat VPN (encrypted) and non-VPN (plain text) traffic as distinct entities within the router, and apply separate IP services such as QoS, multicast and NAT
- Traditional Easy VPN architecture had limitations in this respect

Solution

- Enhanced Easy VPN defines a logical interface (a virtual interface) in which packets are encapsulated with IPsec
- Each interface has the capability to tie several services such as QoS, multicast and NAT to Easy VPN

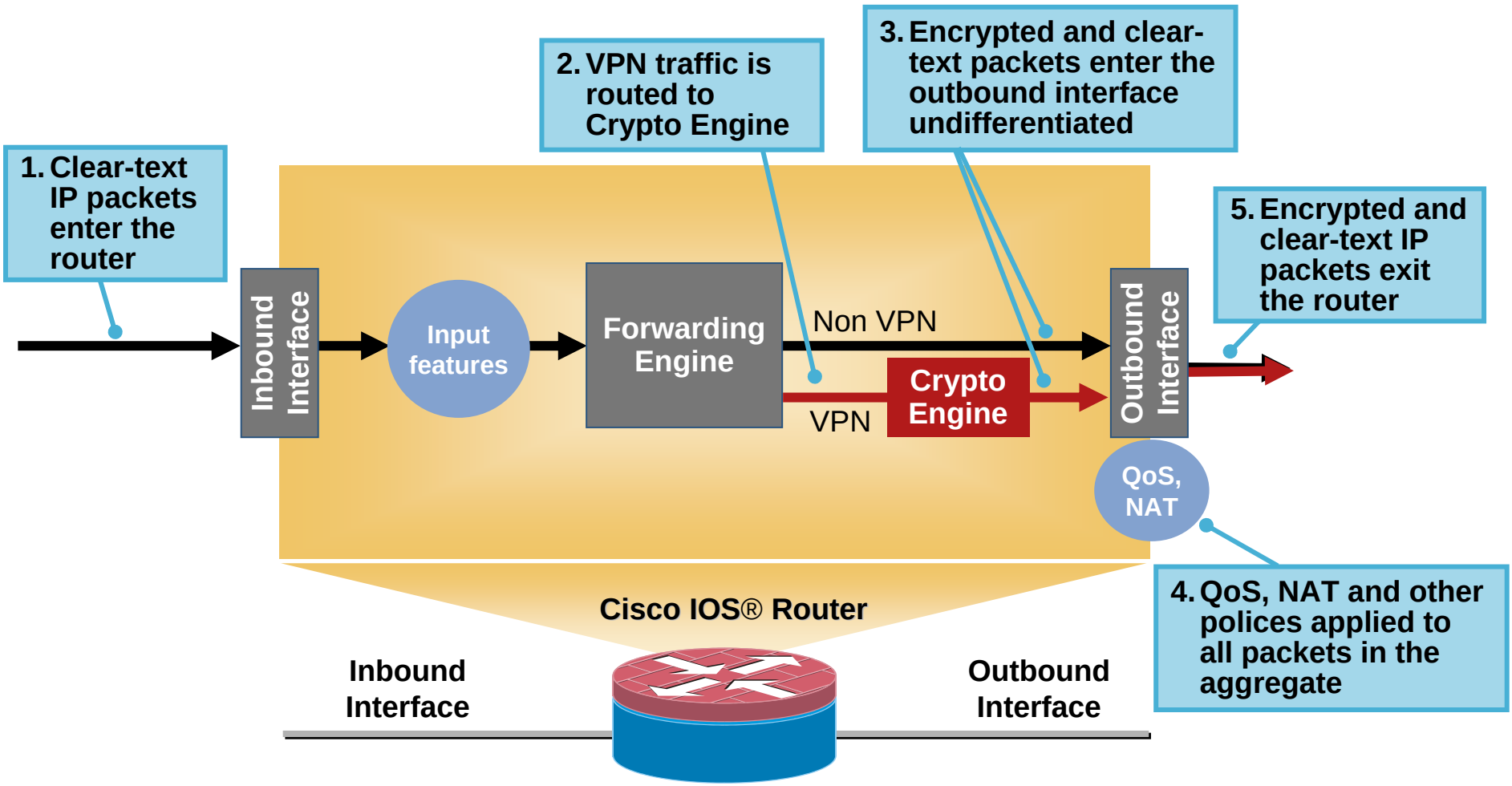
Enhanced Easy VPN

- Administrator defines a virtual template containing Cisco IOS® commands applicable for all users

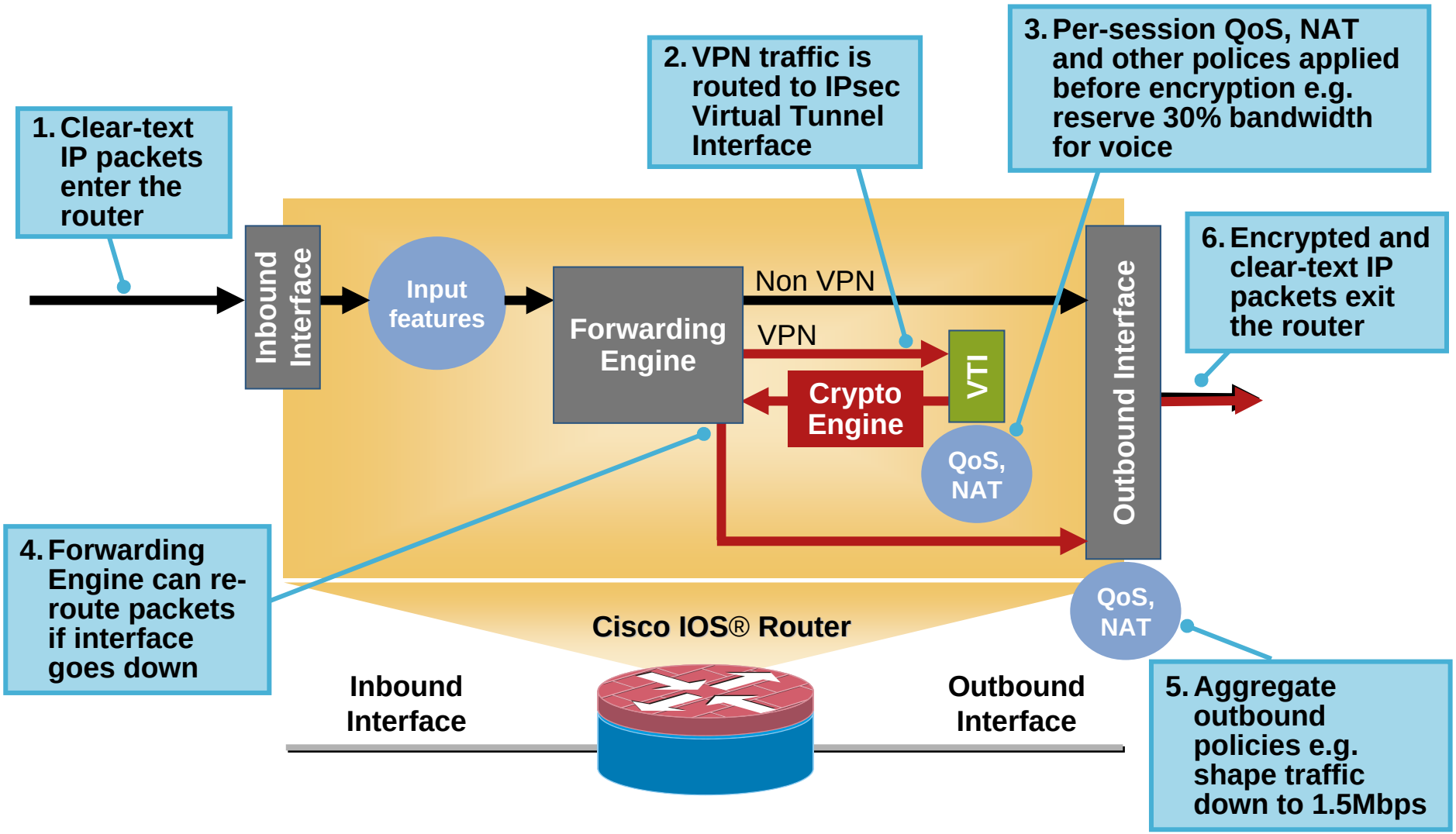
  Easy VPN Remote (hardware client) has a separate interface context allowing tunnel specific features to be applied e.g., ACL, NAT and QoS

- As each new user seeks to gain VPN access, a virtual access interface is cloned automatically based on the virtual template
- Per-user attributes allow individual users to be treated preferentially for QoS, ACLs, etc.

Standard Easy VPN



Enhanced Easy VPN



Virtual Templates for Easy VPN Server

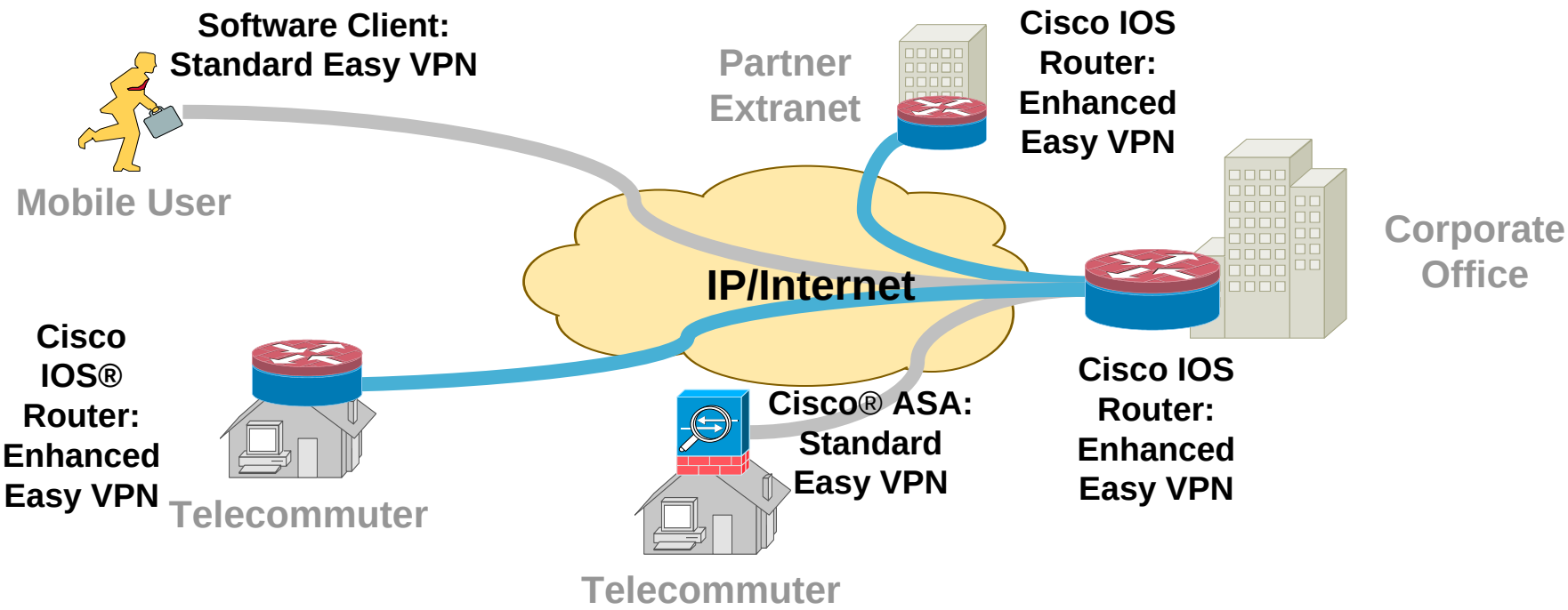
- Use the specified virtual template interface for creating and cloning the virtual access interface
- Dynamic IPsec interface is required
- The IPsec profile is applied on the virtual template
- IPsec profiles define the phase 2 policy

```
Interface Virtual-template1 tunnel
  ip unnumbered Lo0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROFILE
 …
!
Crypto isakmp profile FOO
 virtual-template 1
 …
!
```

Enhanced Easy VPN Features and Benefits

Enhanced Easy VPN Features	Customer Benefits
Voice and Video Integration	▪ Separate interface context to apply pre- and post- interface features ▪ Each remote router has a separate interface context, allowing tunnel-specific features to be applied, e.g. per-user QoS, IP Multicast, NAT and ACL ▪ Enables the network administrator to set proactive policies and deliver the performance required by voice and video applications
VRF Integration	▪ Multiple VRFs can be terminated in multiple interfaces (one VRF per VTI Interface) ▪ Simplifies large scale service provider/enterprise MPLS deployments
Single Security Association (SA)	▪ Single SA for client, network extension (NEM) and network extension plus (NEM+) modes; works for both split or no-split tunneling ▪ Provides enhanced scalability and ease of troubleshooting

Enhanced Easy VPN Connectivity Scenarios



- Enhanced Easy VPN supported between Cisco 800-3800 Series routers, Cisco 7200 Series and Cisco 7301 routers
- Standard Easy VPN for connectivity to software clients, Cisco ASA, Cisco 7600 Series and Cisco Catalyst® 6500 Series switches
- Both can be operational at the same time on the same device

Easy VPN
Network Integration

Network Integration

- Three modes of connection
- QoS support on DVTI
- VRF integration
- TCP-based firewall traversal
- NAT integration
- SafeNet client

Easy VPN Remote Connection Modes

Easy VPN Remote feature supports three modes of operation

- Client Mode

  Server pushes down an IP address to the client and all traffic from the client is internally translated to this address before being encrypted and sent into the tunnel

  NAT or PAT is performed at the remote end of the VPN tunnel, forming a private network and protecting the remote hosts behind the router

- Network Extension

  Remote subnet IP addresses are fully routable and reachable by the server side network over the tunnel

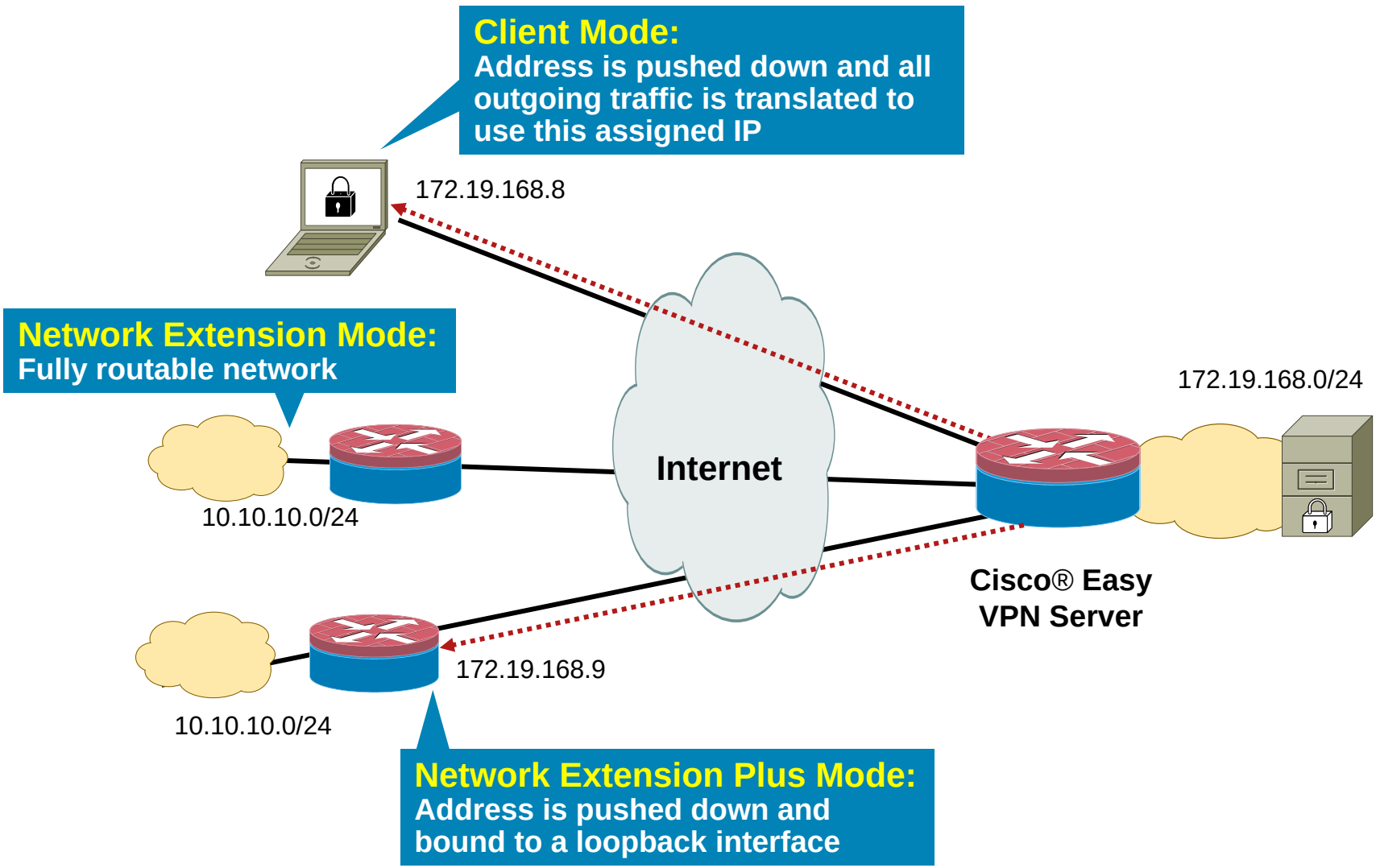
- Network Extension Plus

  Typically used for management purposes.

  Identical to network extension mode with one addition:

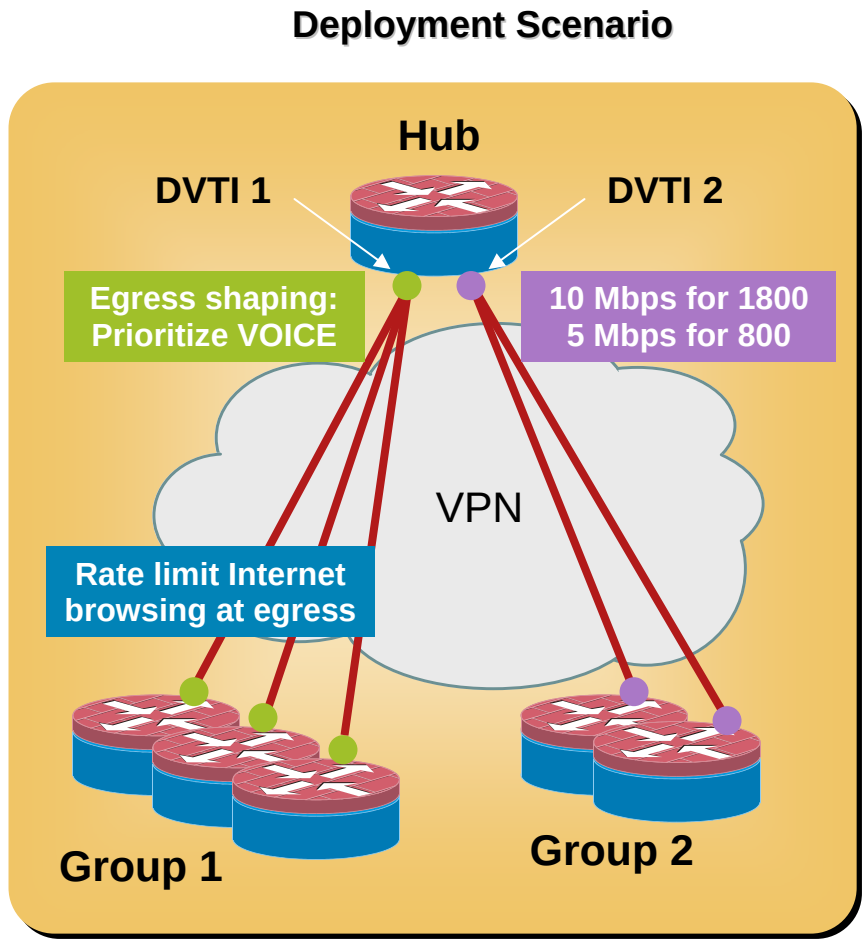
  Remote requests an IP address through Mode-Config from the Server, and ties it to an available loopback interface.

Easy VPN Remote Connection Modes



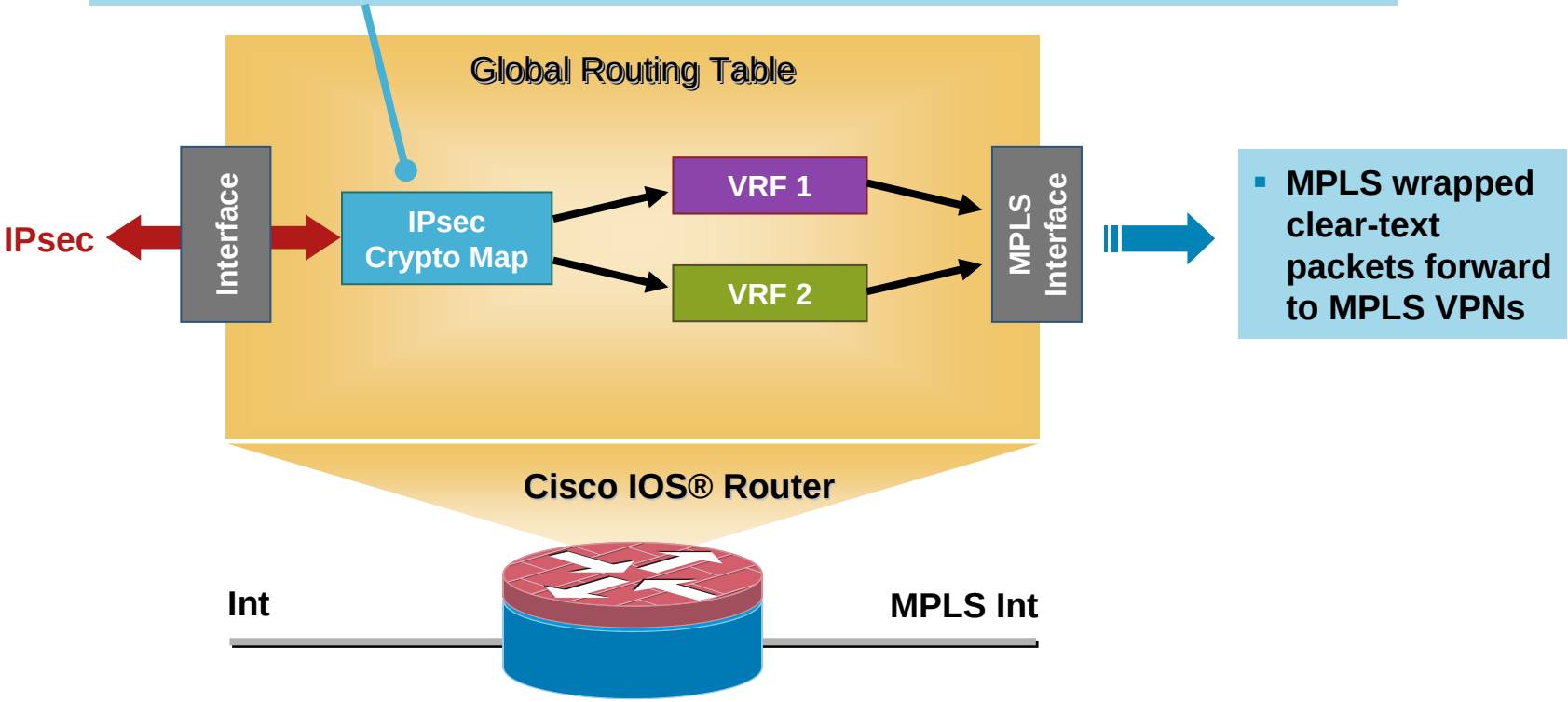
Network Integration
Advanced QoS Integration with VTI

- Enhanced Easy VPN (or DVTI) provides a routable interface with native IPsec tunneling: Eliminates crypto maps, ACLs and GRE
- Per Tunnel QoS: Individual QoS policies per SA.
- Granular policies: Separate ingress and egress policies per spoke or hub.
- Cookie-cutter policies: Use virtual templates to group spokes together. Can be centralized into a AAA server.
- Dynamic instantiation: New instances of the template are cloned only when the SA is formed and torn down after use, conserving system resources.



Network Integration
VRF Aware IKE/IPsec

- IPsec tunnel directly associated with the VRF based on IKE authentication
- AAA passes the VRF ID for the tunnel to the router
- Decrypted clear-text packets forwarded directly to correct VRF



- Works for site-to-site and remote access IPsec VPNs
- Single interface/public IP address for all the VPNs

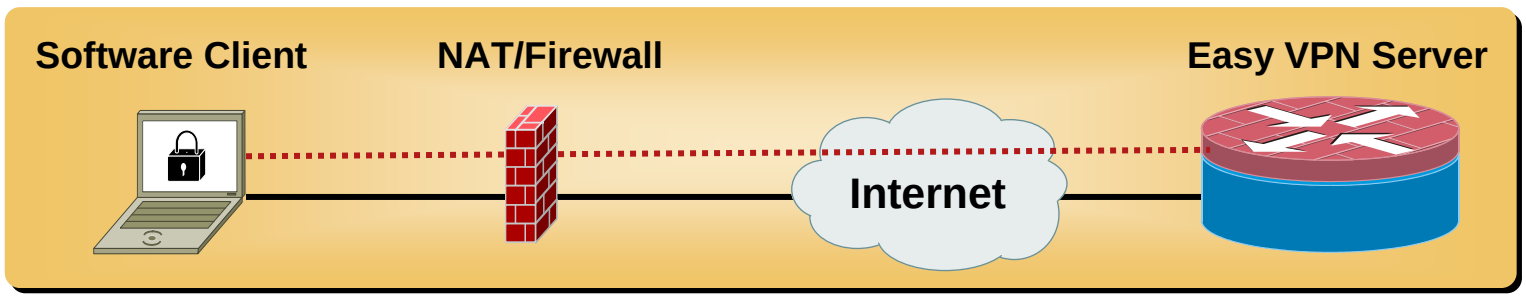
Network Integration
TCP-based Firewall Traversal

Problem Statement

- Mobile users operating out of hotel rooms and airports often see their IPsec traffic blocked by third party firewall/NAT devices
- Original NAT Traversal specifications (NAT-T, rfc3947 and rfc3948) do not consider this

Solution: Cisco® Tunneling Control Protocol (cTCP)

- IPsec traffic tunneled inside TCP, traverses firewall and NAT



- Note: Cisco IOS® Easy VPN Server currently supports cTCP for VPN software clients and Cisco ASA 5505

Network Integration

cTCP Commands

- New CLI introduced to enable the Easy VPN server's support of cTCP globally

```
crypto ctcp port <port#>
```

- Show crypto has a new sub-option to show details of one or more cTCP sessions

```
show crypto ctcp
```

- Relevant show commands are modified to indicate the new encapsulation information

```
Show crypto isakmp peers
Show crypto isakmp sa
Show crypto session
```

NAT Integration: Overlapping Addresses

Problem Statement

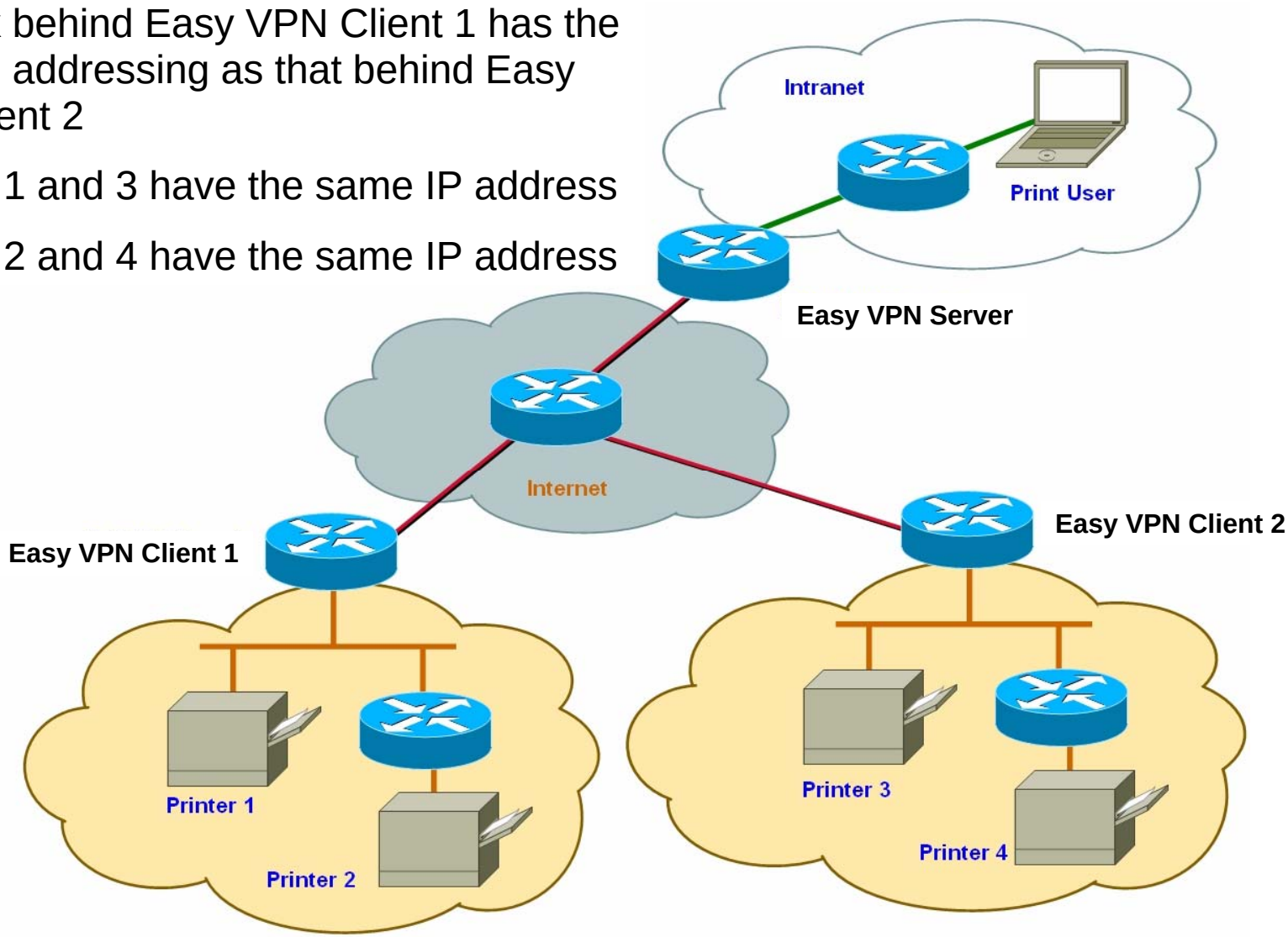
- Internal IP addresses at a branch or remote location may overlap with other locations; especially true during acquisitions and mergers
- Locating and renumbering IP addresses on all devices can be an administrative nightmare

Solution

- Easy VPN Remote Identical Addressing integrates NAT with Easy VPN to allow remote locations with overlapping internal IP addresses
- Printers and servers hosted at remote locations are reachable from the hub as well as other spoke locations

Network Integration
NAT Integration: Overlapping Addresses

- Network behind Easy VPN Client 1 has the same IP addressing as that behind Easy VPN Client 2
- Printers 1 and 3 have the same IP address
- Printers 2 and 4 have the same IP address



NAT Integration: Overlapping Addresses

- Two new sub-commands under

```
crypto ipsec client ezvpn <name>
```

- Allow NAT to be integrated with EzVPN:

```
nat allow
```

- Enable Split-Tunneling for the traffic permitted by the Access-list:

```
nat acl <ACL_Name | ACL_number>
```

NAT Integration: Overlapping Addresses

Configuration steps

1. Define Easy VPN Remote in network-extension mode.
2. Apply Easy VPN Outside on the desired Outside interface. Do not apply Easy VPN Inside on any physical interface of the Client router.
3. Create a loopback interface and apply Easy VPN Inside on that loopback interface.
4. Configure one-to-one static NAT translation for each host that needs to be accessible from Easy VPN server side network or from other client locations.
5. Configure dynamic overloaded NAT (PAT) using an Access list, for all the desired VPN traffic. Map all the Dynamic NAT traffic to the Easy VPN Inside Interface IP address.
6. If Split-Tunnel is required, then use the command

```
nat acl <ACL_Name | ACL_Number>
```

This ACL is the same as that used by NAT mapping created in step 5.

Network Integration

Interoperability: SafeNet Client Support

Problem Statement

- SafeNet clients do not support the Cisco® Unity® spec, but support Xauth and mode configuration. SafeNet Clients should interoperate with Cisco IOS® Easy VPN server using group pre-shared key authentication.

Solution

- SafeNet clients bind to a client configuration group by using a specific isakmp local address.
- Crypto keyrings are enhanced to allow a more granular attachment to a particular address.
- Dynamic Virtual IPsec interfaces are used for terminating the SafeNet Clients.
- SafeNet clients on Cisco 7600 platform will be supported using crypto maps.

Interoperability: SafeNet Client Support

- CLI Configuration
- ISAKMP Profile

```
crypto isakmp profile <name>
  local-address <interface> | <ip address>
```

- ISAKMP Keyring

```
crypto  keyring <name>
  local-address <interface> | <ip address>
```

Easy VPN: Provisioning and Management

Centralized Policy Push and Change Management

- Policies are pushed centrally from Easy VPN Server
- Automates policy updates and image upgrades on remote Easy VPN hardware devices that are hard to access or support
- Also automates policy updates to Easy VPN software clients
- Ideal for Enterprise and Service Providers with large number of remote clients

Centralized Policy Push

- Browser proxy configuration
- Include-local-lan
- Login banner (for hardware clients)
- Auto upgrade (for software clients)
- Auto configuration update
- Integrated client firewall
- DHCP client proxy and distributed DNS
- Split tunneling
- Split DNS support

Centralized Policy Push

Browser Proxy Configuration

- Easy VPN server is configured so that an Easy VPN remote device can use Web proxy on the corporate network.
- Using this feature, the user does not have to manually modify the proxy settings of his or her Web browser when connecting to the corporate network.
- With Cisco IOS® VPN Client or manually revert the proxy settings upon disconnecting.

```
crypto isakmp client configuration browser-proxy bproxy1
 proxy auto-detect
!
crypto isakmp client configuration browser-proxy bproxy2
 proxy none
!
crypto isakmp client configuration browser-proxy bproxy
  proxy server 10.1.1.1:2000
  proxy exception-list 10.2.2.*,www.*org
!
crypto isakmp client configuration group EZVPN
browser-proxy bproxy
```

Centralized Policy Push

Include-local-lan

- This is a pushed attribute that allows a non split-tunneling connection to access to the local subnet at the same time that is the subnet the client is directly attached to.

  Not extensible to other networks on the remote side as it is with the VPN 3000 concentrator.

- CLI

```
crypto isakmp client configuration group <group>
  include-local-lan
```

- RADIUS: Add the AV pair

```
ipsec:include-local-lan=1
```

Centralized Policy Push

Login Banner Push

- Easy VPN server pushes a banner to the Easy VPN remote device.
- Easy VPN remote device can use the banner during Xauth and Web-based activation.
- Easy VPN remote device displays the banner the first time that the Easy VPN tunnel is brought up.
- The banner is configured under group configuration on the Easy VPN server.

```
Router(config)#crypto isakmp client configuration group
EZVPN

Router (config-isakmp-group)# banner @ The quick brown
fox jumped over the lazy dog @
```

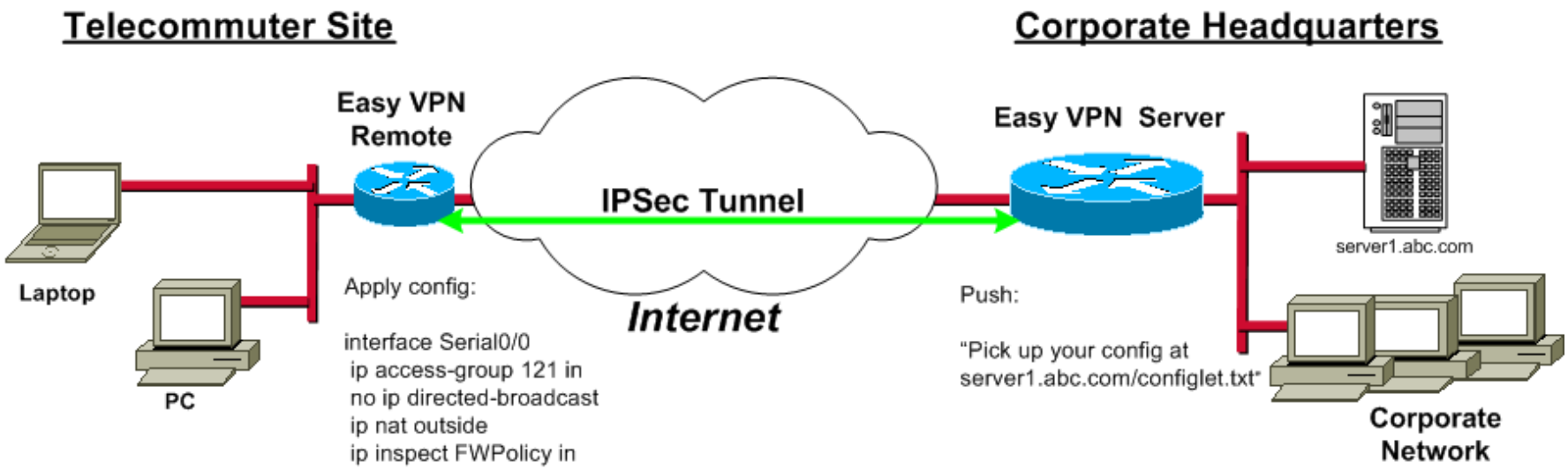
Centralized Policy Push

Auto Upgrade for Software Clients

- An Easy VPN server can be configured to provide an automated mechanism for software upgrades on an Easy VPN software client.

```
crypto isakmp client configuration group {group-name}

  auto-update client Win2000 url
http:www.ourcompanysite.com/newclient rev 3.0.1(Rel),
3.1(Rel)

auto-update client {type-of-system} {url url} {rev
review-version}
```

Centralized Policy Push
Auto Configuration Update



- Allows any configuration change to be pushed to any number of Cisco IOS® Easy VPN hardware clients (e.g. Cisco® 871 router)
- Provisioning of any feature including voice and routing
- Could be used to stop worms or attacks on the fly by enabling ACLs, firewall, IPS and QoS. Easy VPN client cannot join the VPN unless it applies the configuration change!

Centralized Policy Push

Auto Configuration Update

Server Configuration

- AAA configuration for management update

```
aaa authentication login listless local
aaa authorization network listful local
aaa accounting update newinfo
aaa accounting network arshad start-stop broadcast group
radius
```

- Group “Store” configuration

```
crypto isakmp client configuration group store
 key storekey
 domain cisco.com
 pool storepool
 save-password
 configuration url tftp://172.16.30.2/store.cfg
 configuration version 2
```

Centralized Policy Push

Auto Configuration Update

Server Configuration

```
crypto isakmp client configuration group branch
 key cisco
 domain branch.com
 pool dynpool
 acl 150
 configuration url tftp://10.0.149.203/branch.cfg
 configuration version 21
```

- Remote router: no change

Centralized Policy Push
Auto Configuration Update

Branch Configuration

```
interface Virtual-Template1 type tunnel
exit
!
crypto ipsec client ezvpn ez2
 connect auto
 group cisco key cisco
 local-address FastEthernet1/0
 mode client
 peer 10.0.149.221
 virtual-interface 1
 xauth userid mode interactive
exit
!
interface VLAN1
crypto ipsec client ezvpn ez2 inside
!
interface FastEthernet4
 crypto ipsec client ezvpn ez2
```

Centralized Policy Push
Auto Configuration Update

Branch Configuration

```
c7200-3(config)#crypto isakmp client configuration group branch
c7200-3(config-isakmp-group)#configuration url ?
  cns:        URL the client will use to fetch configuration
  flash:      URL the client will use to fetch configuration
  http:       URL the client will use to fetch configuration
  https:      URL the client will use to fetch configuration
  nvram:      URL the client will use to fetch configuration
  rcp:        URL the client will use to fetch configuration
  scp:        URL the client will use to fetch configuration
  tftp:       URL the client will use to fetch configuration
..
..
< Others removed>
```

Centralized Policy Push

Auto Configuration Update

Server Monitoring

- Once the configuration is updated Easy VPN Remote will send management updates to Easy VPN Server and AAA Server (if accounting is enabled)

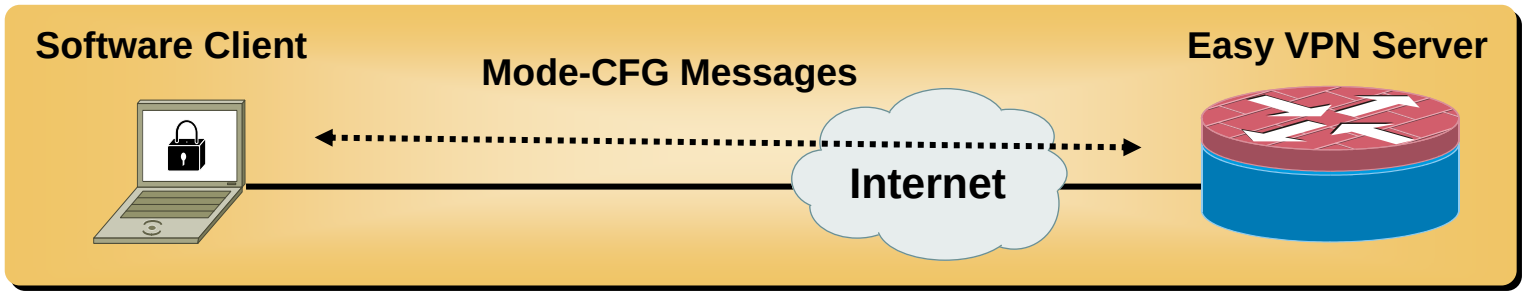
```
c7200-3#sh cry isakmp peers config | in 231

Client-Public-Addr=10.0.149.231:500; Client-Assigned-
  Addr=30.30.30.23; Client-Group=branch; Client-User=;
  Client-Hostname=c3845-31.yourdomain.com; Client-
  Platform=Cisco 3845; Client-Serial=FHK0848F19B; Client-
  Config-Version=21; Client-Flash=63885312; Client-
  Available-Flash=16400384; Client-Memory=226492416;
  Client-Free-Memory=138466564; Client-Image=flash:c3845-
  advsecurityk9-mz.124-4.7.T;
```

Allows network administrator to easily get the status of any or all the spokes.

Centralized Policy Push

Integrated Client Firewall

- Centralized Policy Push enables administrators to push policies that enforce security at the client devices
- The server can be set up to allow/deny the tunnel, e.g. if client does not have a required firewall



Centralized Policy Push

Integrated Client Firewall

Easy VPN Server Configuration

- policy_name: Can be associated with a client group config on the server or on the AAA
- required: Tunnel will be terminated if the client doesn't confirm to the defined policy.
- optional: Tunnel setup will continue even if the client doesn't confirm to the defined policy.
- firewall_type includes Cisco-Integrated-Firewall, Cisco-Security-Agent, Zonelabs-Zonealarm, Zonelabs-ZonealarmPro

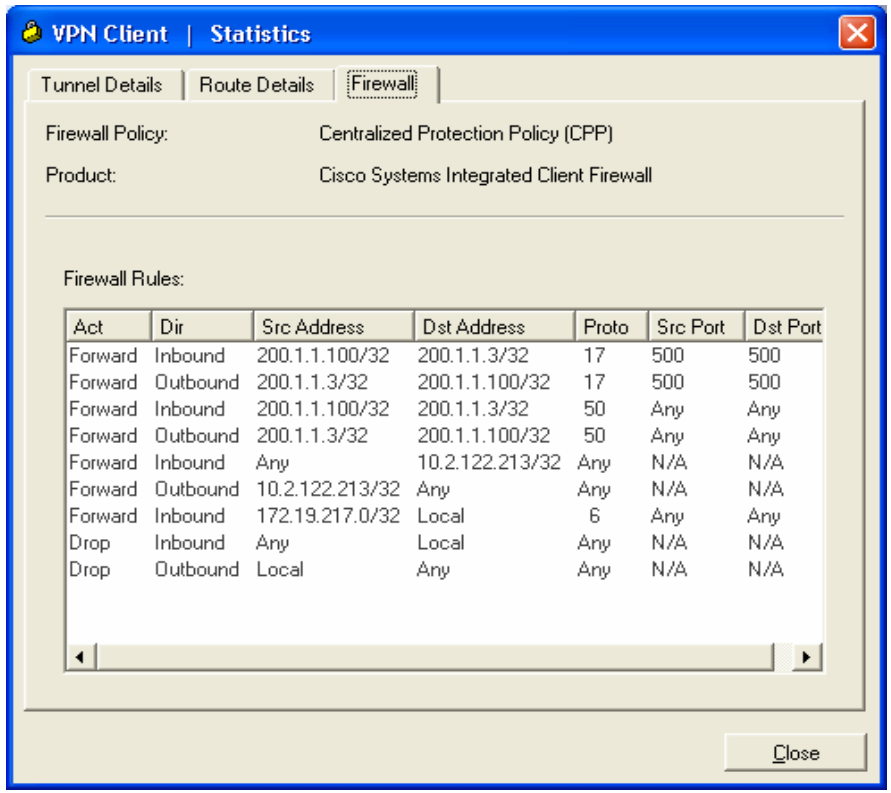
```
crypto isakmp client configuration group <group-name>
       policy <policy-name>]

crypto isakmp client firewall <policy_name> required|optional
<firewall_type>
       policy central-policy-push|check-presence access-list
in|out <acl-name/no>
```

Centralized Policy Push

Integrated Client Firewall

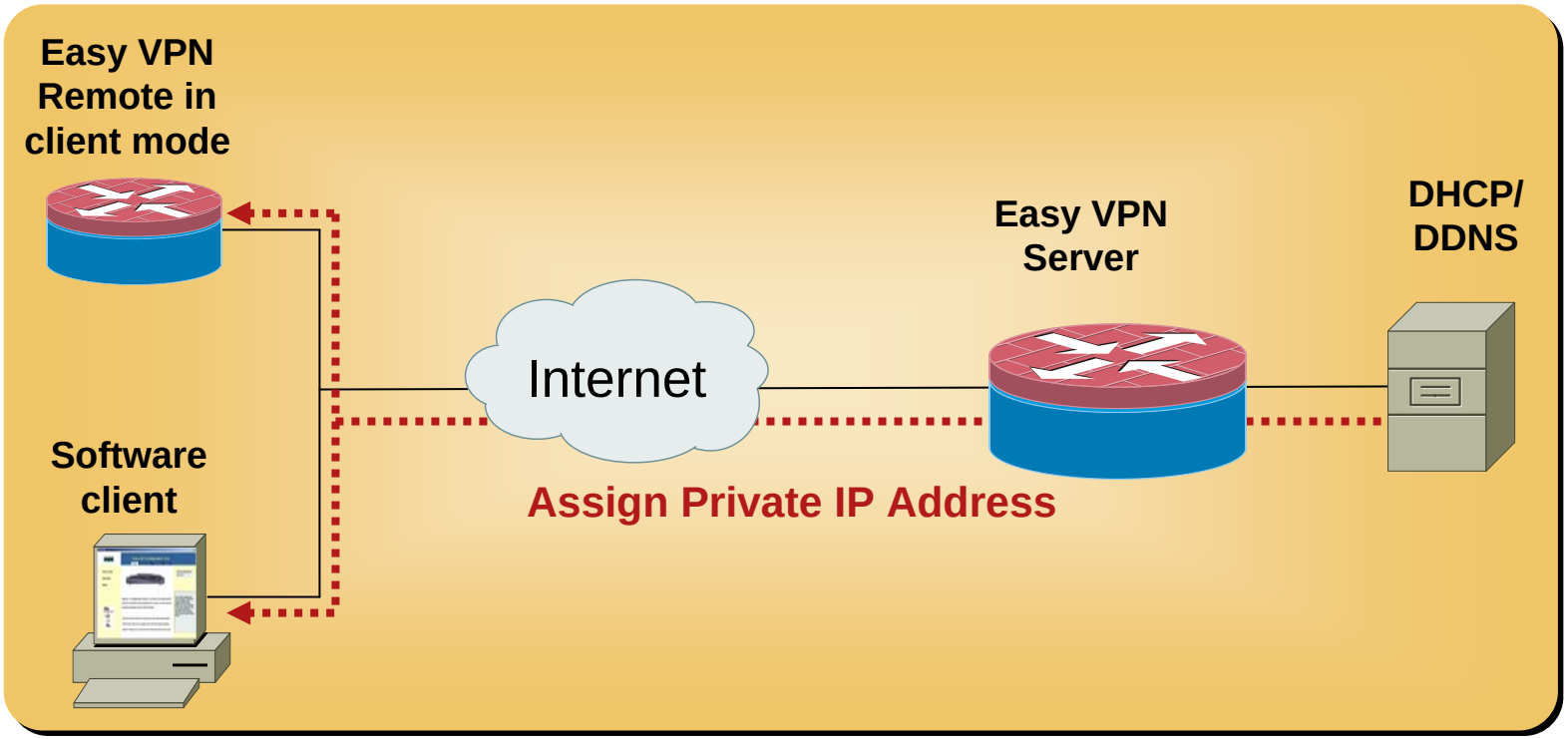
Verify the CPP On the Client

- The access list configured on the server is enforced on the client
- Check the pushed down firewall policy in VPN Client | Statistics | Firewall tab



Centralized Policy Push

DHCP Client Proxy and Distributed DNS



- Centralized management of IP address
- Less network administration work

Centralized Policy Push

DHCP Client Proxy and Distributed DNS

System Flow

1. The client talks to the server, sends over its hostname and requests a private IP address
2. The server forwards the request along with the hostname to the DHCP server
3. DHCP server assigns an IP address from its pool and sends an update request to the DDNS Server
4. DDNS Server updates its records and registers this hostname with the new IP address
5. Everybody in the LAN behind the server can reach the client by its hostname now

Centralized Policy Push

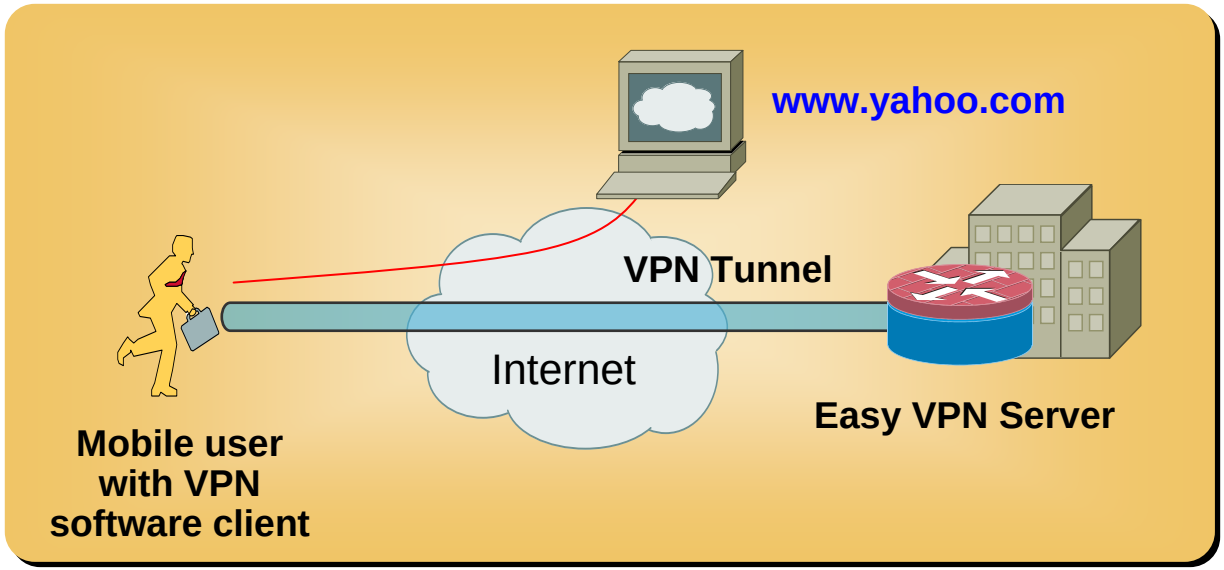
DHCP Client Proxy and Distributed DNS

Address Assignment on Easy VPN Server

The following order of precedence is followed in selecting a method for address assignment:

1. Framed IP configured on RADIUS
2. Local pool
3. Global IKE address pool
4. DHCP

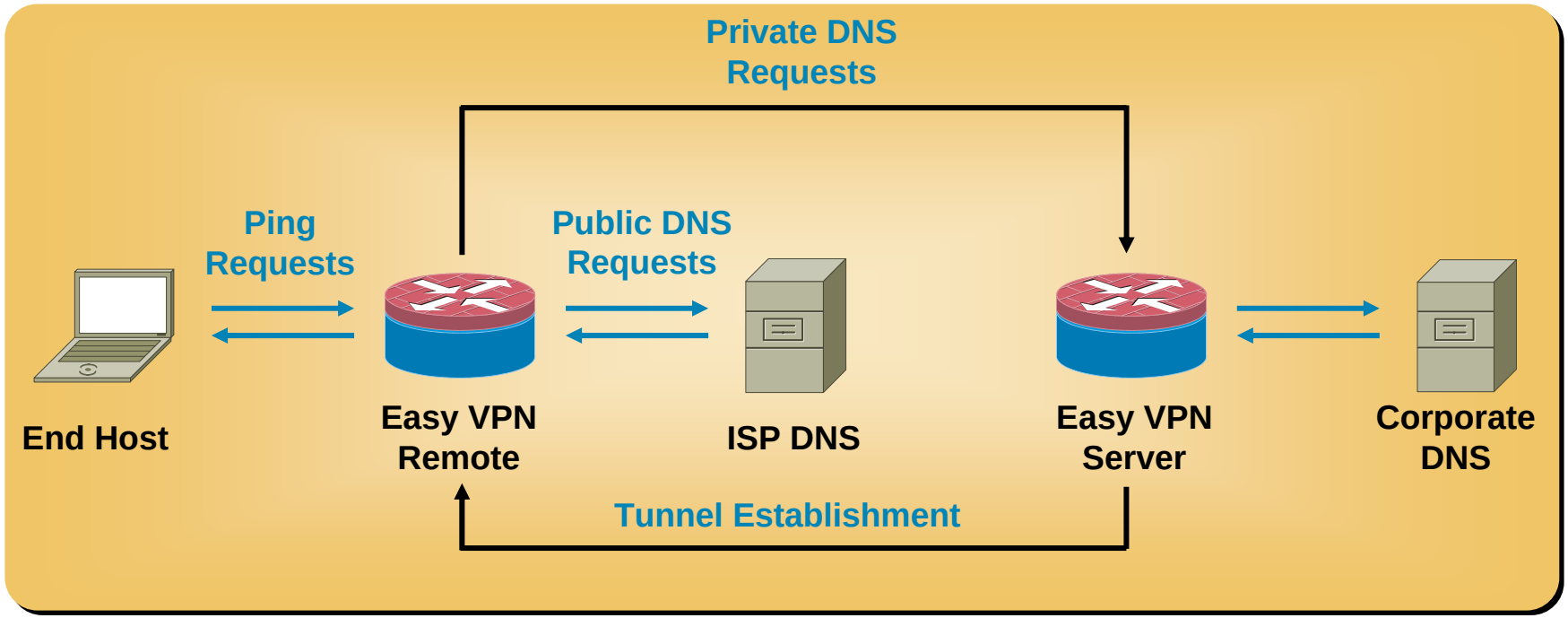
Centralized Policy Push
Split Tunneling



- Traffic goes directly to the Internet without forwarding it over the encrypted tunnel
- Less traffic over the tunnel saves bandwidth of the Easy VPN server and internal resources

```
crypto isakmp client configuration group <group>
   acl <acl_num>
```

Centralized Policy Push
Split DNS



- Reduced workload for internal DNS server
- Faster DNS resolve for Internet URLs
- Used in conjunction with split tunneling

Centralized Policy Push

Split DNS

- Easy VPN Server configuration

```
crypto isakmp client configuration group 831server
  key abcd
  dns 64.104.128.248      ← Internal DNS Server
  acl 150                 ← Split Tunnel
  split-dns wwwin.cisco.com
  split-dns wwwin-release.cisco.com
```

- Easy VPN Client configuration

```
ip name-server 200.1.1.202     ← ISP DNS Server
ip dns server  ← Enable client as DNS forwarder
ip domain-lookup
```

Centralized Policy Push
Split DNS

Show messages on the client:

```
c871#sh ip dns view
DNS View ezvpn-internal-view
parameters:
Logging is off
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name:
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    64.104.128.248 ← Corporate
DNS Server settings:
  Forwarding of queries is
enabled
  Forwarder addresses:
```

```
DNS View default parameters:
Logging is off
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name:
internet.com
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    200.1.1.202 ← ISP
DNS Server settings:
  Forwarding of queries is
enabled
  Forwarder addresses:
```

Easy VPN: Authentication

Authentication

- Two-Stage Authentication

  Group Level: Through preshared keys or digital certificates

  User Level (Xauth): The remote side submits a username and password. Four ways to activate: automatic, traffic-triggered, Web-intercept, and console.

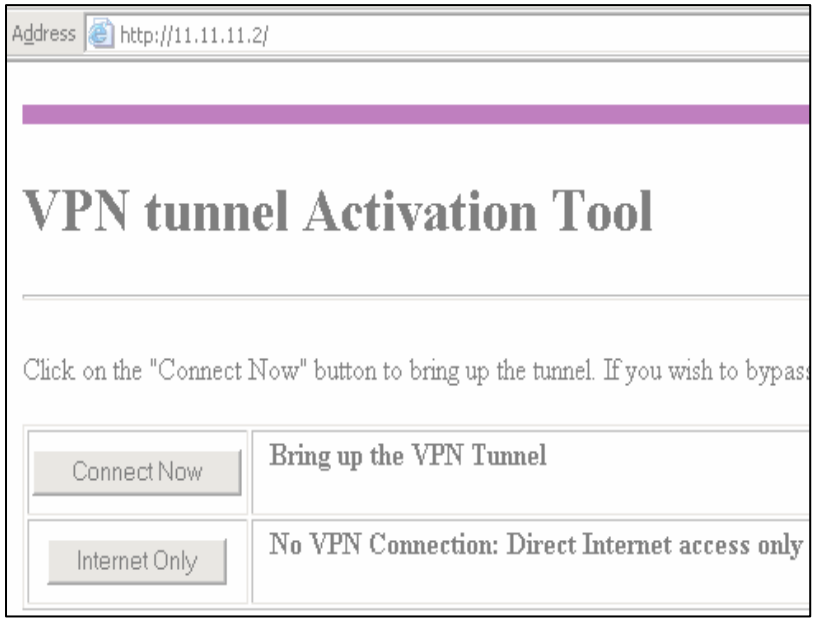
- RADIUS and AAA
- IPsec accounting
- Encrypted secrets
- Save password
- Password expiry via AAA

Authentication

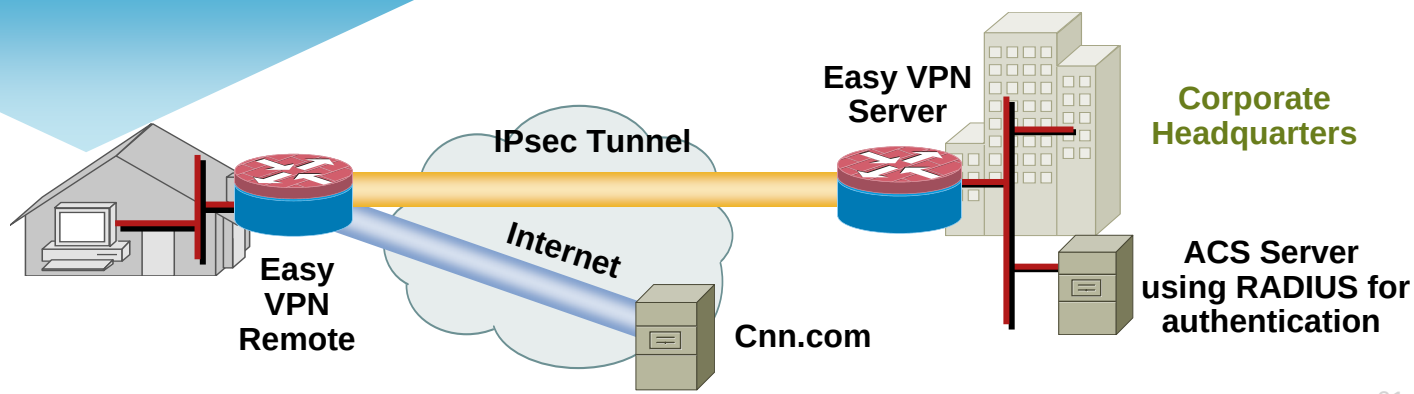
User Level Authentication (RADIUS)

- Automatic and traffic-triggered activation
  - Typically Used by the router shared between several PCs
  - Automatic: Keeps the VPN tunnel up all the time
  - Traffic-triggered: Brings up the tunnel when there is data to be sent
  - Xauth username and password stored on the router
- Web-intercept activation
  - RADIUS username and password input via Web page
  - Not stored on the router
- Console activation
  - Xauth username and password entered manually via CLI
  - Useful for network administrators during troubleshooting

Authentication
RADIUS Web-Intercept Activation



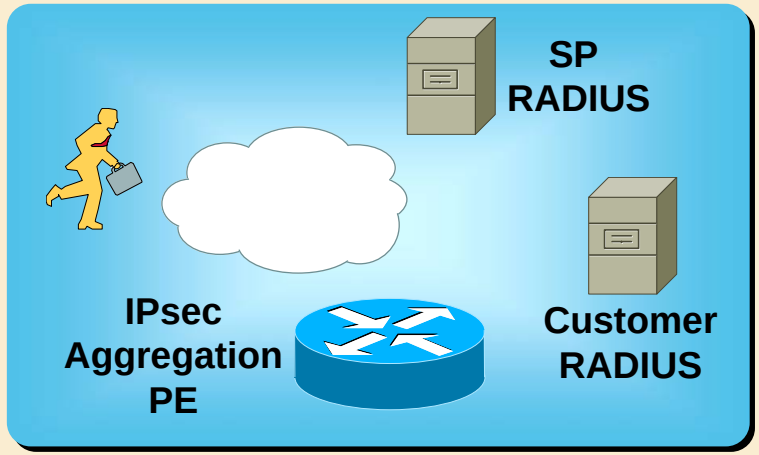
- User-driven authentication of the client router
  - HTTP interface for entering Xauth user/password to Cisco IOS® hardware client
  - Allows the user to authenticate the entire device, not just a single port
  - Eliminates the need for logging in via CLI
- Useful in teleworker applications
  - Provides an option to "bypass" the tunnel (direct Internet access for spouse and kids)
  - Can use “Code 401” username/password screen instead of HTML login page*



Authentication
RADIUS and AAA

Authentication

- After IKE has been successful (device authentication complete), move to Xauth
- Client prompted for credentials. Response handed to RADIUS and to SDI Server
- Challenge/Next Pin message to client if required
- Username is user@domain where domain matches group policy domain
- Once RADIUS complete, retrieve user specific attributes (framed IP address) from RADIUS



Authorization

- Client initiates IKE (AG Pre-shared, MM certs), ID_KEY_ID (group name) identifies group profile on RADIUS server
- Authorization occurs on receipt of AG1, retrieve Profile for client (including pre-shared key) from RADIUS
- Authorization occurs on a per VRF basis and must present a matching identity
- Once RADIUS is passed, MODECFG will pass the retrieved attributes to the client

Accounting

- After IKE, RADIUS and MODECFG succeed, remote initiates QM, this triggers accounting-start to RADIUS for the remote peer
- Accounting session tied to IPsec SAs

Authentication

IPsec Accounting

- RADIUS accounting starts after initializing Quick Mode (QM). This ensures all intermediate modes are finished.
- RADIUS accounting stops after all IPsec SAs to a peer are deleted.
- RADIUS accounting updates are supported. Packet and octet counts are shown in the updates.
- New accounting records are not generated during a rekeying.
- Accounting records can be used for auditing or billing purpose

Authentication

Encrypted Secrets

- Type 6: Encryption scheme to hide passwords in the Cisco IOS® configuration using a strong cipher like AES.

  The '6' derives from the single digit '6' that will precede passwords encrypted under this scheme.

- Encryption key and a symmetric cipher
- Store encryption key in private-nvram
- Symmetric cipher AES to encrypt the keys. The password encryption method used is ICM (Integer Counter Mode).

Authentication

Encrypted Secrets

Configuration

- Encryption of keys does not happen until the user configures a master encryption key using the following command (enables type 6):

```
(config)# password encryption aes
```

- The master encryption key can be removed, however this renders all the existing type 6 keys invalid.

Authentication

Encrypted Secrets

Configuration

- An encryption key is stored in private-nvram using the command:

```
(config)# key config-key password-encryption
<\r> or <text>
```

- If there is a key configured already, the above command will ask for the old key before allowing you to enter the new key.

```
(config)# key config-key password-encryption
   Old key:
   New key:
   Confirm key:
```

- Changing config-key will result in the re-encryption of all type 6 passwords under the new key.

Authentication

Encrypted Secrets

Configuration

- The user can delete the master encryption key with the following command. The user is prompted for confirmation before deletion.

```
(config)# no key config-key password-encryption
   WARNING: All type 6 encrypted keys will become unusable
   Continue with master key deletion ? [yes/no]:
```

- The following command gives debugs of type 6 password operation. This can be used to debug type 6 password problems.

```
(config)#  password logging
```

Authentication

Encrypted Secrets

Key Protection

- crypto isakmp keys:

```
crypto isakmp key 6 RHZE`]ACMUI\bcbTdELISAAB
address 11.1.0.1
```

- crypto keyring keys:

```
crypto keyring test
  pre-shared-key address 1.1.1.5 key 6
WgMad[FXGN[cJOdXRLZVFeJ^AAB
```

- isakmp aggressive mode keys:

```
crypto isakmp peer address 11.1.0.2
 set aggressive-mode password 6
DV`P[aTVWWbcgKU]T\QhZAAB
 set aggressive-mode client-endpoint ipv4-
address 11.1.0.1
```

Authentication

Encrypted Secrets

Key Protection

- Easy VPN Client keys:

```
crypto ipsec client ezvpn easy
 group ez key 6 dGIS[GEOHPhROiBA\OgCi

 username fred password 6 HJGR/P\123
 mode client
 connect manual
```

- ISAKMP client group policy keys:

```
crypto isakmp client configuration group test
 key 6 JK_\JHZPeJV_XFZTKCQFYAAB
 pool dynpool
```

Authentication
Save Password

- Easy VPN Remote: If this attribute is received, the RADIUS username/password is automatically inserted into the RADIUS request. No OTPs!
- Easy VPN Server: Allows the user to save their RADIUS password locally on the PC such that once the user enters the password initially, the attribute is pushed down. On a subsequent authentication, the user may activate the save-password tick box on the software client or add the username and password to the Cisco IOS® hardware client profile. The setting remains until the save-password attribute is removed from the server group profile.

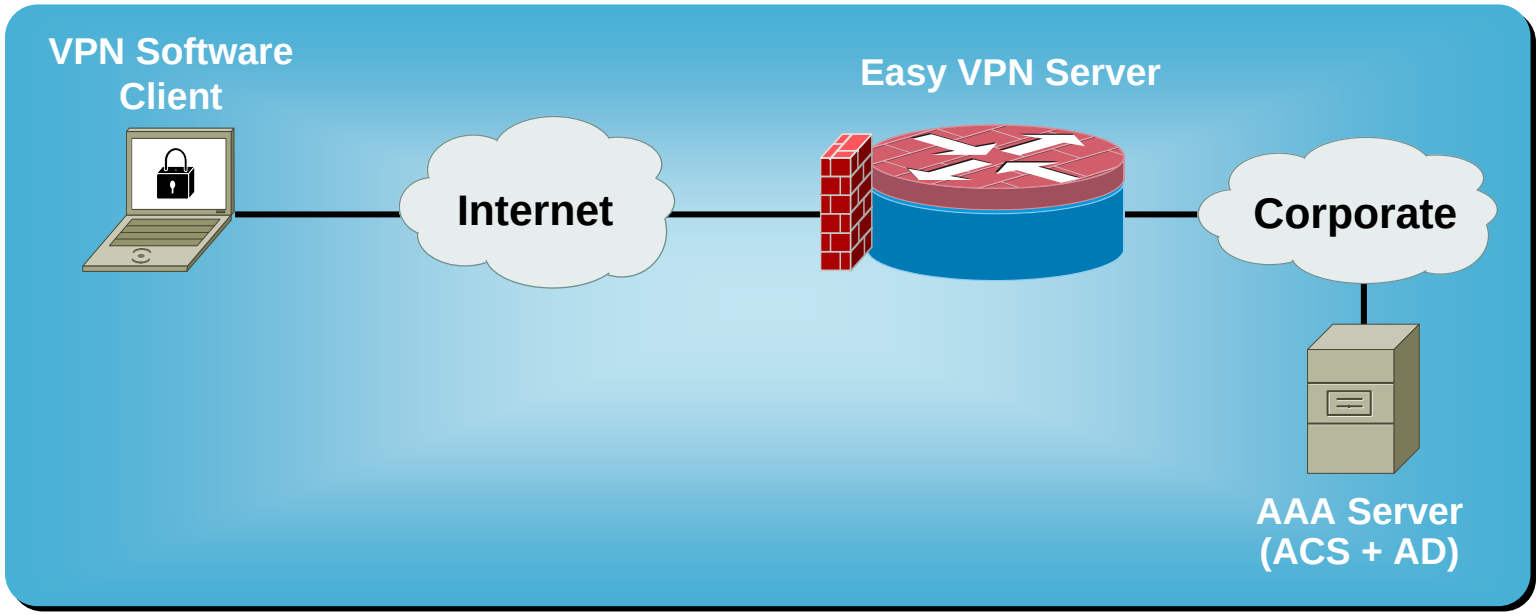
CLI

```
crypto isakmp client configuration group <group>
  save-password
```

RADIUS: Add the AV pair

```
ipsec:save-password=1
```

Authentication
Password Expiry via AAA



- Provides a chance for VPN software client users to enter a new password when the old one expires

Authentication

Password Expiry via AAA

Configuration Example

```
C2821(config)# aaa authentication login USERAUTH passwd-
  expiry group test-server-group
C2821(config)# aaa authorization network branch local
C2821(config)# aaa group server radius test-server-group
C2821(config-sg-radius)#server 172.19.220.149 auth-port 1645
  acct-port 1646
C2821(config)# crypto map dynmap client authentication list
  USERAUTH
```

```
C2821(config)# aaa authentication login USERAUTH passwd-
  expiry group radius
C2821(config)# aaa authorization network branch local
C2821(config)# radius-server host 172.19.220.149 auth-port
  1645 acct-port 1646 key cisco
C2821(config)# radius-server vsa send authentication
C2821(config)# crypto map dynmap client authentication list
  USERAUTH
```

Easy VPN:
High Availability

High Availability

- Reverse Route Injection (RRI)
- Dead Peer Detection (DPD) and IKE keepalives
- Stateless failover with Hot Standby Router Protocol (HSRP)
- IPsec stateful failover
- Invalid SPI recovery
- Multiple backup peers
- Dial backup and primary peer reactivation
- Remote dual tunnels
- Server load balancing

High Availability

Reverse Route Injection

- RRI allows static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.
- Easy VPN uses RRI to simplify network design when there is a requirement for redundancy and routing.
- RRI works with both dynamic/static crypto maps and DVTI.

RRI Distance Metric Enhancement

- Allows the user to define a distance metric for each static route created by RRI.
- Supported on ipsec-profiles and crypto maps.

```
crypto ipsec profile fred
          set reverse-route distance 20
```

```
crypto map fred 1 ipsec-isakmp
          set reverse-route distance 20
```

- Allows the dynamically learned route on a router to take precedence over a locally configured static route.

High Availability

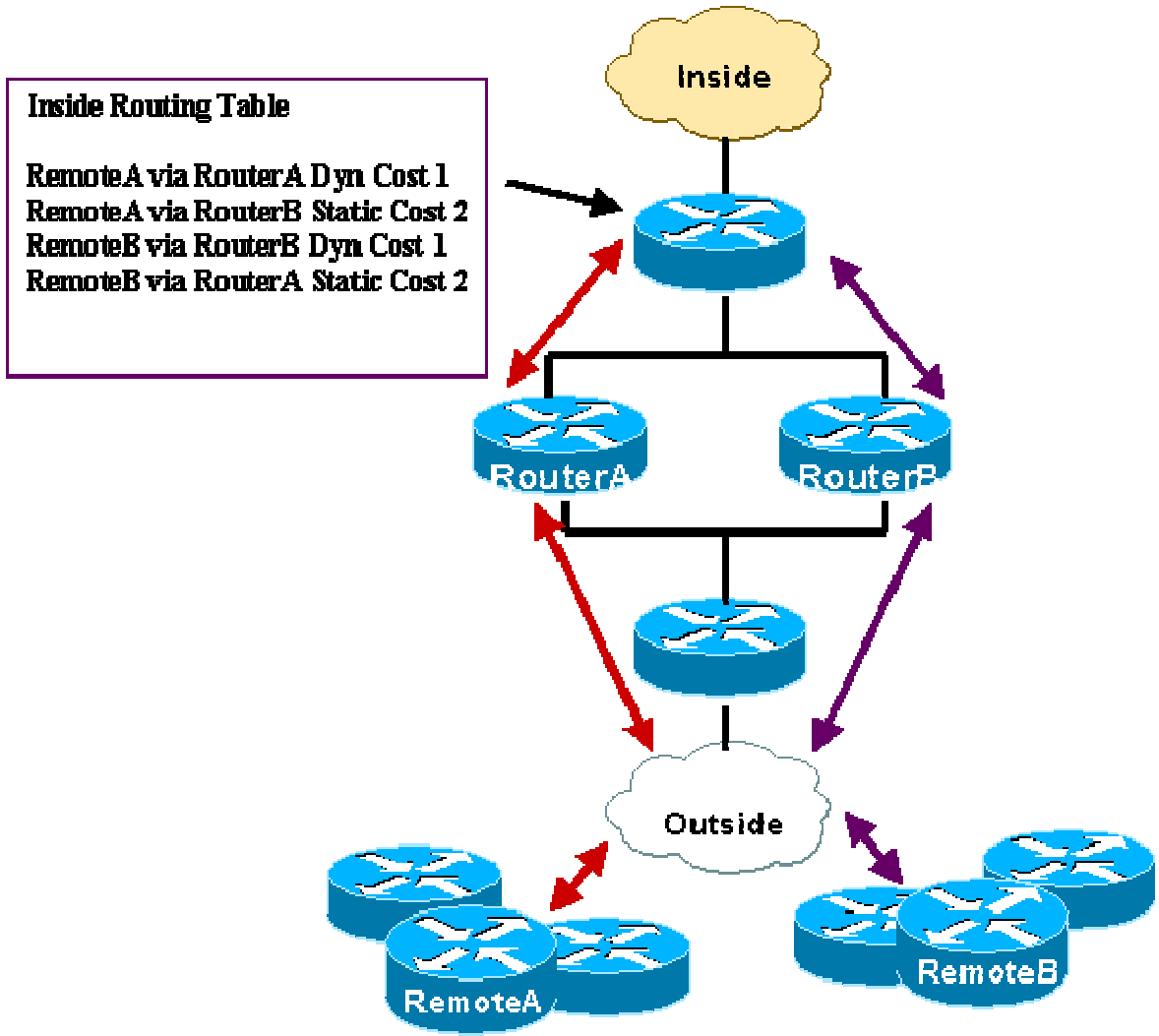
Dead Peer Detection and IKE Keepalives

- DPD is required for environments in which customers want failover between concentrators on different subnets.
- Router queries the liveliness of its IKE peer at regular intervals.
- DPD is a replacement of IKE keepalives
  - IKE keepalives are periodic and bidirectional, which add to the processing overhead and reduce the data encryption throughput performance.
  - DPDs are sent only if there is outbound traffic, but there has not been any inbound traffic for the DPD interval.

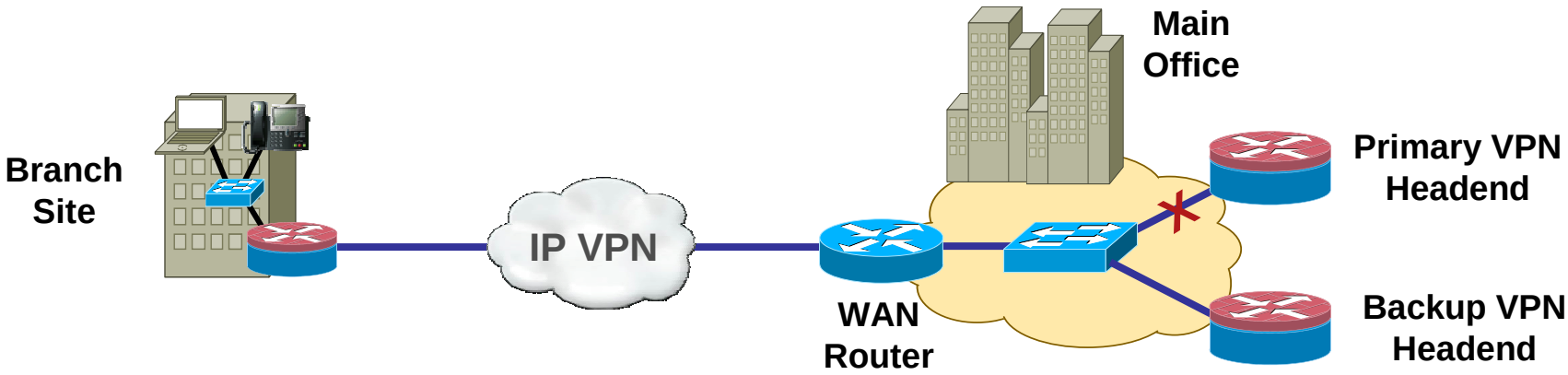
```
crypto isakmp keepalive <idle_interval> <cr>
crypto isakmp keepalive <idle_interval>
<retransmit_interval> <cr>
```

High Availability
Stateless Failover with HSRP

- Provides primary to secondary cutover
- Allows the active and standby VPN gateways to share a common virtual IP address
- Detects that the primary has gone down and then completely re-establishes IKE and IPsec with the standby gateway
- Nontransparent cutover and typically results in lost application layer sessions
- A complete failover takes between 20 and 45 seconds



High Availability
IPsec Stateful Failover



- IPsec stateful failover* delivers sub-second VPN failover for thousands of remote sites
- No service disruption—protects mission-critical applications
- IPsec state information shared with standby device

*** Requires Standard Easy VPN**

High Availability
IPsec Stateful Failover

Enabling stateful failover for IPsec

```
interface <interface-name>
  crypto map <map-name> redundancy <standby-group-name> stateful
```

- Binds the crypto map in use on this interface to the redundancy group. The virtual IP address is taken from the group named by standby-group-name.

Enabling stateful failover for tunnel protection

```
crypto ipsec profile <profile-name>
       set transform-set <ipsec-trans>
       redundancy <standby-group-name> stateful

interface tunnel <tunnel-number>
tunnel protection ipsec <profile-name>
```

- The redundancy configuration for the tunnels is done in the IPsec profile.

High Availability

Invalid SPI Recovery

- Enabled via CLI

```
crypto isakmp invalid-spi-recovery
```

- Can lead to DoS attack susceptibility
- Used to help resync peers after a failover (for devices that do NOT support keepalives or DPD)
- Receipt of invalid-spi messages will trigger receiver to initiate new IKE

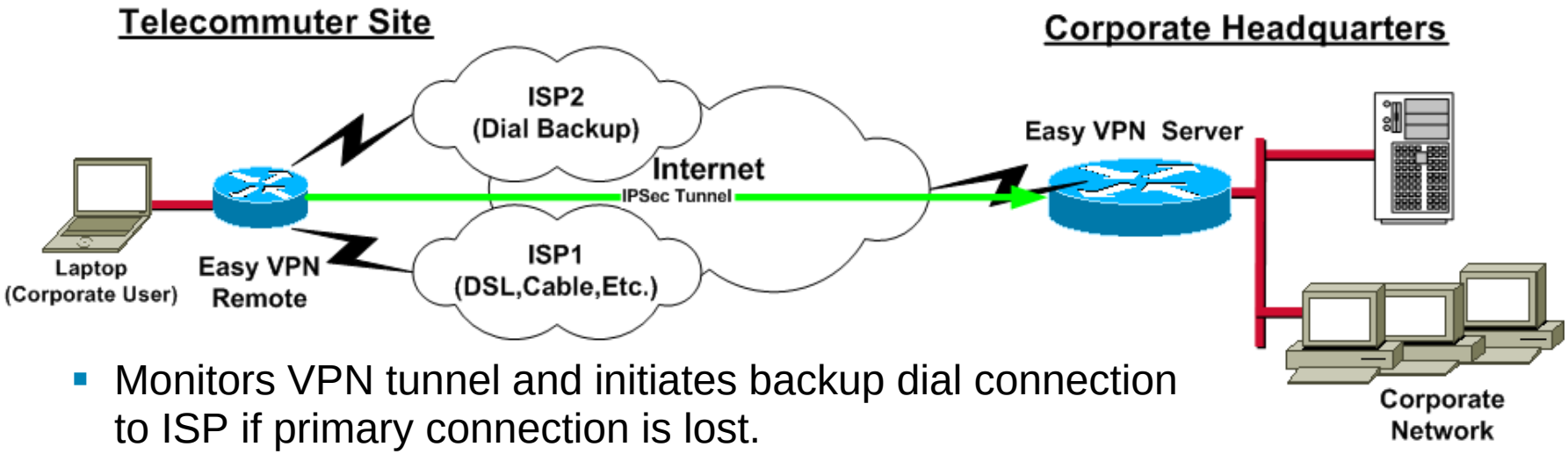
High Availability

Multiple Backup Peers

- Uses peer statements as per traditional Easy VPN
- DPD will help facilitate the failover

```
crypto ipsec client ezvpn <name>
peer <ip-addr>
peer <hostname>*
*crypto isakmp identity host (on server)
```

High Availability
Dial Backup and Reactivate Primary Peer



- Monitors VPN tunnel and initiates backup dial connection to ISP if primary connection is lost.
- Easy VPN client continues the IKE SA setup attempt with primary server even after failover.
- Once primary becomes available connection is re-established and secondary is dropped.
- Does not require use of dynamic routing protocol.

```
Router (config)# crypto ipsec client ezvpn ez1
Router (config-crypto-ezvpn)# peer 10.2.2.2 default
Router (config-crypto-ezvpn)# peer 10.2.2.1
Router (config-crypto-ezvpn)# idle-time 60
```

High Availability

Dial Backup and Reactivate Primary Peer

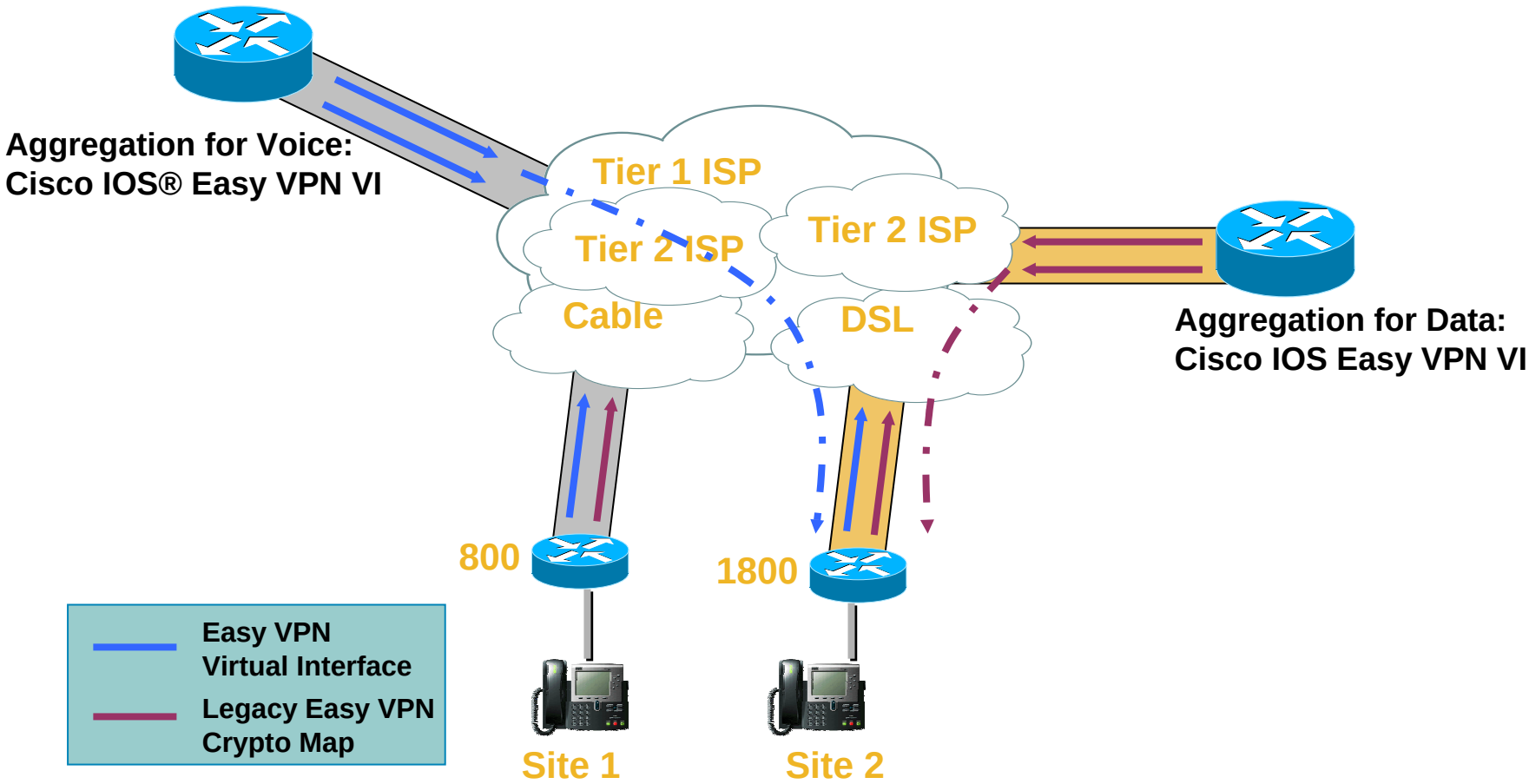
- CLI

```
crypto ipsec client ezvpn <name>
  peer <hostname> | <ip addr> [default]
  idle-timer [seconds]
```

- Only one peer in an Easy VPN configuration can be designated as “default”

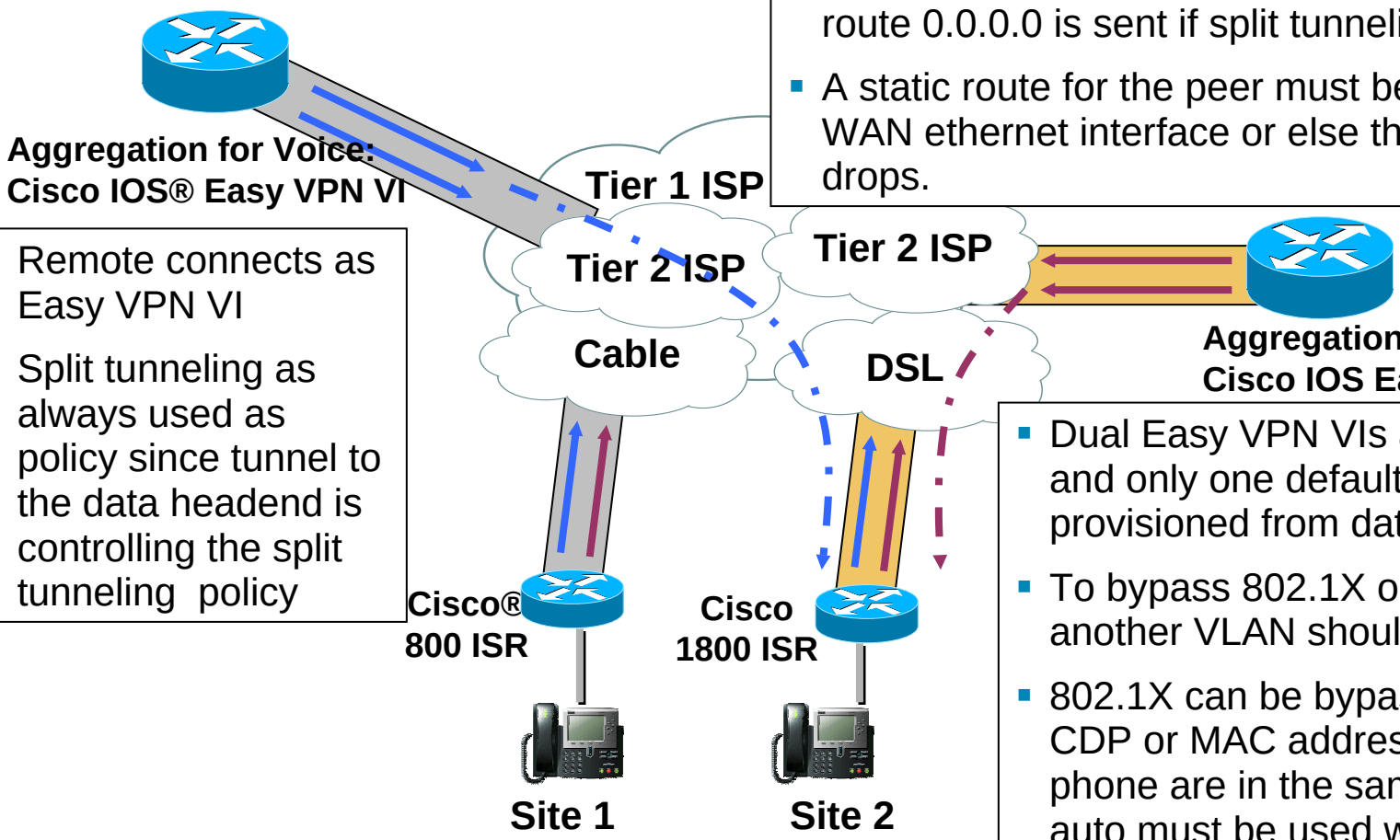
High Availability
Remote Dual Tunnel Support

- Configure multiple Easy VPN tunnels that share common inside and outside interfaces to connect two peers to two different VPN servers simultaneously



High Availability
Remote Dual Tunnel Support

- Remote connects as Easy VPN VI and split tunneling policy may or not be enabled. A default route 0.0.0.0 is sent if split tunneling is disabled.
- A static route for the peer must be enabled out the WAN ethernet interface or else the IKE tunnel drops.



- Remote connects as Easy VPN VI
- Split tunneling as always used as policy since tunnel to the data headend is controlling the split tunneling policy

- Dual Easy VPN VIs are supported and only one default route as provisioned from data headend.
- To bypass 802.1X or Web Intercept another VLAN should be used.
- 802.1X can be bypassed by using CDP or MAC address if PCs and the phone are in the same LAN. Connect auto must be used with 802.1X for access to the data tunnel i.e. the data tunnel must be up.

High Availability

Remote Dual Tunnel Support

Usage Guidelines (1 of 2)

Dual Tunnel Combinations	Headends Supported	Configuration and Usage Considerations on the Easy VPN Remote Device and Headend
Two legacy Easy VPN tunnels	Cisco IOS® Security Routers, Cisco® ASA, and VPN 3000	• Two tunnels cannot share a common outside interface. • Two tunnels cannot share a common inside interface. • The two tunnels should use separate inside and outside interfaces. • Traffic from an inside interface that belongs to one Easy VPN tunnel cannot be pushed into another tunnel.
One legacy Easy VPN tunnel and one crypto map	Cisco IOS Security Routers, Cisco ASA, and VPN 3000	The crypto map can share the same outside interface as the legacy Easy VPN client configuration. However, the behavior of the two remote devices depends on the mode of Easy VPN as well as the IPsec selectors of the crypto map and the Easy VPN remote device. This is not a recommended combination.
One legacy Easy VPN tunnel and one static virtual interface	Cisco IOS Security Routers	Both tunnels cannot terminate on the same headend. The static virtual interface remote device tunnel has to be terminated on a static virtual interface on the headend router. The legacy Easy VPN remote device tunnel can terminate on the virtual tunnel interface or crypto map that is configured on the headend.

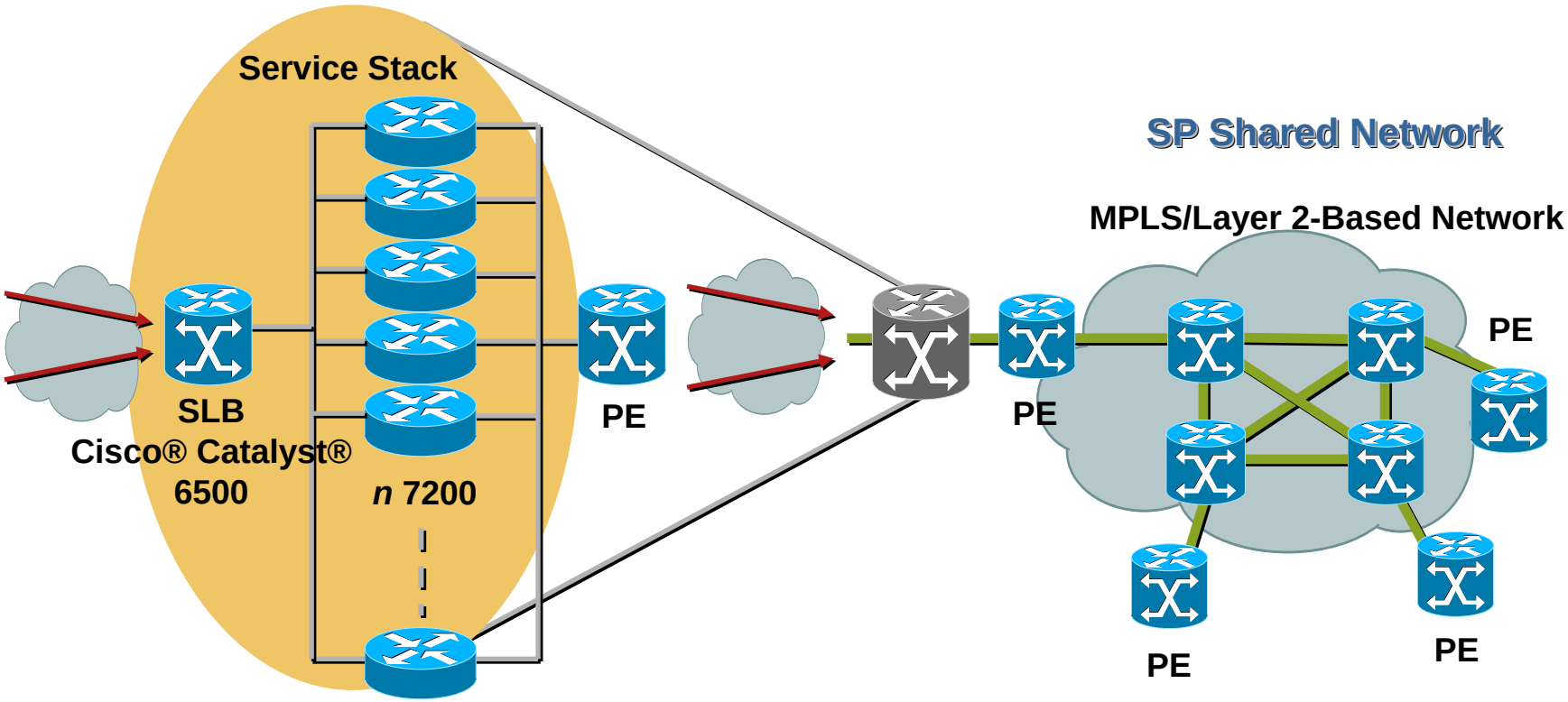
High Availability

Remote Dual Tunnel Support

Usage Guidelines (2 of 2)

Dual Tunnel Combinations	Headends Supported	Configuration and Usage Considerations on the Easy VPN Remote Device and Headend
One legacy Easy VPN tunnel and one Easy VPN virtual interface	Cisco IOS® Security Routers, Cisco® ASA, and VPN 3000	Both tunnels cannot terminate on the same headend. • The legacy Easy VPN tunnel and the Easy VPN virtual interface can share a common inside and outside interface. • An Easy VPN virtual interface should be used only with split tunneling. • Legacy Easy VPN can use a split tunnel or no split tunnel. • Web-based Activation cannot be applied on both Easy VPN tunnels. • Using two Easy VPN virtual interfaces is preferable to using this combination.
One Easy VPN virtual interface and one static virtual interface	Cisco IOS Security Routers	Both tunnels cannot terminate on the same peer. The static virtual interface and the Easy VPN virtual interface can use the same outside interface. • The Easy VPN virtual interface should use split tunneling.
Two Easy VPN virtual interfaces	Cisco IOS Security Routers, Cisco ASA, and VPN 3000	Both tunnels cannot terminate on the same peer. • At least one of the tunnels should use split tunneling. • Web-Based Activation cannot be applied to both Easy VPN tunnels.

High Availability
Server Load Balancing



- Cisco Catalyst 6500 SLB used to load balance between n IPsec aggregators
- Users connect to a single IP address—SLB takes care of rest
- Supported for remote access VPN clients and dynamic cryptos only

Summary

Easy VPN Major Features Availability

Feature	Standard Easy VPN	Enhanced Easy VPN
Stateful failover	Y	N
VRF-aware IPsec	Y	Y
NAC integration	Y	Y
Dynamic routing	N	N
Auto config update	Y	Y
Dial backup–reactivate primary peer	Y	Y
Secure multicast	N	Y
QoS per tunnel	N	Y
Remote dual tunnel	Y	Y
Remote identical IP addressing	N	Y
RRI distance metric enhancement	Y	Y

Hardware Platform Support Table

Cisco Router Platform	Maximum IPsec Tunnels
Cisco® 800 Series	10
Cisco 181x Series	50
Cisco 184x with AIM-VPN/SSL-1	800
Cisco 2800 Series with AIM-VPN/SSL-2	1,500
Cisco 382x with AIM-VPN/SSL-3	2,000
Cisco 384x with AIM-VPN/SSL-3	2,500
Cisco 7200 Series with VAM2+	5,000
Cisco 7200VXR NPE-G2 with VSA	5,000
Cisco 7301 Series with VAM2+	5,000
Cisco 7600 Series with IPsec VPN SPA	16,000
Cisco Catalyst® 6500 Series with IPsec VPN SPA	16,000

Enhanced Easy VPN and DMVPN Comparison

Feature	Enhanced Easy VPN	Dynamic Multipoint VPN
Scalability per hub	Large number of spokes per hub	Varies with routing protocol chosen
Identical configuration for all spokes	Y	N
Cross-platform support	Y	N
Support for software client	Y	N
IPsec stateful failover	N (Standard Easy VPN only)	N (Depends on routing protocol for recovery)
Stateless failover	Y	Y
Always-up tunnel to hub	Not required	Y
IP Multicast support	Y	Y
Direct spoke-to-spoke communication	N	Y
QoS support	Y	Y
Supports routing protocols	N	Y
Digital certificates support	Y	Y

Summary

- **Increases productivity** — Provides remote users with LAN-like access to corporate applications and unified communications
- **Provides deployment flexibility** — Enables large-scale deployments with rapid user provisioning
- **Is easy to use and maintain** — Allows dynamic configuration of end-user policy, requiring less manual configuration by end users and field technicians, thus reducing errors and further service calls
- **Enhances interoperability** — Reduces interoperability issues between different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications

Cisco.com/go/easyvpn