Configuring Tunnel Default Gateway on Cisco IOS EasyVPN/DMVPN Server to Route Tunneled Traffic

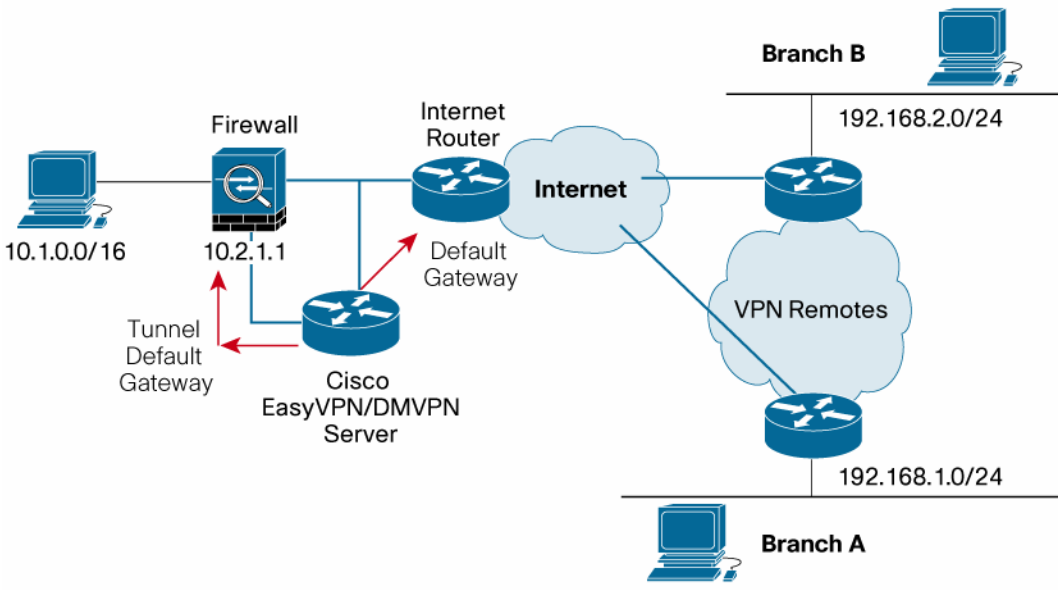
Introduction

This document discusses Cisco® tunnel default gateway implementations that are available as part of a Cisco EasyVPN/DMVPN solution. Currently, there is no easy way for customers to have traffic that terminates on VPN tunnels go through one default gateway, while all other traffic (Internet Key Exchange [IKE], for example) uses a different default gateway. This requirement is common and this paper discusses the best ways to implement this on most Cisco IP Security (IPsec) VPN devices, primarily routers.

Problem Description

The tunnel default gateway is needed to let the internal firewall and router handle the routing for all decrypted IPsec packets. Today, after a Cisco IOS® EasyVPN Client connects to a Cisco IOS EasyVPN Server, there is no simple way for the client to send the tunnel traffic to the internal corporate network (other than to have the entire routing table on the IPsec gateway). In this type of implementation, the Cisco IOS routers use the default gateway to route all packets toward the Internet that do not have a more specific route. The tunnel default gateway gives customers the flexibility to control how they handle IPsec tunneled traffic. Once traffic coming in from a remote site is decrypted and ready to go out to the Internet, that traffic would first need to go through the internal firewall/corporate router for Network Address Translation (NAT) and firewall inspection. This is shown in Figure 1.

Figure 1. Topology



Cisco IOS Solution

Cisco IOS Software offers two solutions to provide tunnel default gateway capability: policy-based routing and virtual routing and forwarding.

Policy-Based Routing

Policy-based routing (PBR) works in a simple way. If we can define the traffic with an access control list (ACL), we can create a PBR route map, which sends traffic matched by the ACL to the specified next hop. The PBR route map should apply to the interface where “interesting” traffic enters the router. This is a simpler implementation and is recommended for small and medium-sized customers. As PBR now uses Cisco Express Forwarding switching, the impact on the router CPU should be minimal. Following is a configuration that implements a tunnel default gateway using PBR

Configuration

In this configuration example, all the remote subnets are in the 192.168.0.0/16 range (i.e. 192.168.1.0/24, 192.168.2.0/24). We can define PBR route maps for traffic sourcing from 192.168.0.0/16 headed to anywhere and set the next hop to 10.2.1.1, which is our inside corporate firewall interface. Make sure you have the appropriate route inside statements on your firewalls to return traffic appropriately.

```
access-list 100 remark TUNNEL DEFAULT GATEWAY TRAFFIC
access-list 100 permit ip 192.168.0.0 0.0.255.255 any

route-map VPN-INTERNET permit 10
 match ip address 100
 set ip next-hop 10.2.1.1 (toward the firewall)

interface FastEthernet1/1
 description PUBLIC PHYSICAL INTERFACE TO ISP
 ip address 1.1.1.1 255.255.255.224
 no ip redirects
 duplex full
 speed 100
 crypto map MY-VPN
 ip policy route-map VPN-INTERNET

interface Vlan1
 description PUBLIC VIRTUAL INTERFACE TO ISP
 ip address 2.2.2.2 255.255.255.240
 no ip redirects
 crypto map MY-VPN
 ip policy route-map VPN-INTERNET
```

Traffic that terminates on either F1/1 or Vlan1 (the interfaces where the crypto map is applied) will show a source address representative of the remote site’s internal networks (i.e. 192.168.1.0/16 and 192.168.2.0/16) and would get forwarded to the firewall after decryption.

Virtual Routing and Forwarding

Using virtual routing and forwarding (VRF) instances, the customer would still have a default route in the global routing table so that the IKE and IPsec signature authorities can be built. The first

step is to create a “dummy” VRF and then define a default gateway within the VRF. Once the decrypted packets are mapped into the VRF instance, there is another default route that points toward the corporate firewall side. Reverse route injects a static route in the VRF routing table, which can be redistributed by the routing protocol running between this box and the corporate network as a host route or an aggregate summary of the pool. The configuration needed to achieve this is complex, and is best suited for enterprise and service provider customers. This solution has worked well in the service provider space due to the familiarity with VRFs in general, but customers without VRF knowledge can still use this configuration -- no Multiprotocol Label Switching (MPLS) knowledge is required.

Configuration

Here, we configure the dummy VRFs on the Cisco IOS routers to route the tunneled traffic toward the inside corporate firewall/router.

Create a dummy VRF

```
ip vrf coke
rd 100:1
```

Define ISAKMP profile and associate the specific dummy VRF to it

```
crypto isakmp profile coke-ra
    match identity group coke
    vrf coke  (associate the dummy vrf within the isakmp profile)
    client authentication list authenlist
    isakmp authorization list authorlist
    client configuration address respond
    accounting coke
```

Define the dynamic crypto map and bind it to the overall crypto map

```
crypto dynamic-map dynamic-coke 1
 set transform-set transform-coke
  set isakmp-profile coke-ra
  reverse-route remote-peer 57.0.0.1
crypto map vpn 11 ipsec-isakmp dynamic dynamic-coke
ip local pool coke 10.3.10.1 10.3.10.253
```

Apply the crypto map to the Internet-facing outside interface

```
interface FastEthernet1/1
    ip address 1.1.1.1 255.255.255.224
    crypto map vpn
```

Set Default route in the global table pointing toward the Internet gateway for IKE and IPsec SAs to be built

```
ip route 0.0.0.0 0.0.0.0 1.1.1.2
```

Configure **corporate-facing inside interface**

```
interface FastEthernet1/0
 ip vrf forwarding coke
```

```
 ip address 10.2.1.2 255.255.255.240
crypto map vpn
```

Set default route in the VRF pointing toward the inside corporate gateway for other traffic

```
ip route vrf coke 0.0.0.0 0.0.0.0 10.2.1.1
```

Cisco VPN 3000 Series and Cisco ASA 5500 Series Configuration

This section addresses the Cisco VPN 3000 Series and Cisco ASA 5500 Series configuration for the tunnel default gateway feature, which completes the implementation for all Cisco Easy VPN servers.

Cisco VPN 3000 Series Solution

Configure the default gateways for your system.

Table 1. Configuring the Default Gateways

Feature	Configuration	Description
Default Gateway	172.16.172.1	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router (Internet-facing).
Metric	1	Enter the metric, from 1 to 16.
Tunnel Default Gateway	10.10.0.2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router (corporate-facing).

Cisco ASA 5500 Series Solution

Users can enter static routes in the same format as Cisco PIX® to configure routes. Users will have the option to configure two default gateways, one with a “tunneled” option and one without. All traffic that arrives at the **appliance** and cannot be routed using learned routes or static routes will be routed through default gateways. If the traffic was encrypted when it initially arrived at the **appliance**, it will be routed through Default Tunnel Gateway (DTGW); otherwise, it will be routed through Default Gateway (DGW). A set of default gateways can be installed for each virtual context.

The IP routing subsystem routes data packets first using learned routes, then static routes, then the default gateway. If a default gateway is not configured, packets that cannot be routed to another host will be dropped. Also, a tunnel default gateway is specified, which is a separate default gateway for tunneled traffic only. A switch to let the default gateways learned through routing protocols override the configured default gateways is provided through the usage of floating metric. If a static route needs to be overridden by a route found by a routing protocol, it is specified with a maximum possible metric. In that case, when a route is found by Routing Information Protocol (RIP) or Open Shortest Path First (OSPF), it overrides the statically configured route.

Modification to existing CLI command when using Cisco ASA:

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway> [<metric>] [tunneled]
```

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Printed in USA

C07-396193-00 3/07