

## Using VPN with Zone-Based Policy Firewall

Recent enhancements to IP Security (IPsec) VPN simplify firewall policy configuration for VPN connectivity. Dynamic Multipoint VPN (DMVPN), IPsec Virtual Tunnel Interface (VTI), and site-to-site VTI allow the confinement of VPN site-to-site and client connections to a specific security zone by placing the tunnel interfaces in a specified security zone. Connections may be isolated in a VPN DMZ if connectivity must be limited by a specific policy; if VPN connectivity is implicitly trusted, VPN connectivity may be placed in the same security zone as the trusted inside network.

This document offers basic configuration guidelines for the relevant portions of IPsec VPN configuration. If a detailed configuration reference is required for IPsec VPN configuration, please browse to the IPsec configuration references included in each of the configuration examples.

### Zone-Based Firewall and IPsec VPN

Cisco IOS<sup>®</sup> Software-based routers offering both Zone-Based Policy Firewall and IPsec VPN connectivity provide improved security and more intuitive configuration if IPsec connections use one of the interface-based VPN options, such as site-to-site VTI, DMVPN, or IPsec VTI for site-to-site and Easy VPN client connections.

If non-VTI IPsec is employed, you must exercise caution when you configure the firewall policy for VPN. The zone policy must specifically allow access by IP address to protected hosts for remote VPN sites' hosts or clients if they are in a different zone than the VPN traffic's ingress interface, where encrypted traffic will be sent to and received from remote VPN sites or clients. Access policy must be configured by including an access control list (ACL) enumerating the source addresses of the VPN clients and the destination addresses of the hosts the VPN clients will be allowed to reach. If the access policy is not properly configured, the policy could expose vulnerable hosts to hostile traffic.

### DMVPN

DMVPN employs a virtual interface (interface tunnel **[number]**) for IPsec VPN connectivity. When the DMVPN interface is assigned to a security zone, traffic routing to and from other interfaces in the router are subjected to zone-to-zone firewall policy.

If the DMVPN interface is assigned to the same security zone as another interface (for example, Gigabit Ethernet 0/0), traffic moving between hosts on the DMVPN and hosts connected to Gigabit Ethernet 0/0 will freely pass with no policy application.

This basic example illustrates a DMVPN interface in the "VPN" zone, the FastEthernet 0/1 interface in the "safe" zone, and the FastEthernet 0/0 interface in the "hostile" zone. Policy is applied according to the following matrix:

Source v	Destination >	Safe	VPN	Hostile
Safe		N/A	smtp, http	dns, http, https, ftp
VPN		Citrix	N/A	Deny
Hostile		Deny	Deny	N/A

For more information on Dynamic Multipoint VPN, please see:

<http://www.cisco.com/en/US/products/ps6658/index.html>

For additional details on Zone-Based Policy Firewall, please see:

[http://www.cisco.com/en/US/products/sw/secursw/ps1018/products\\_tech\\_note09186a00808bc994.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml)

### DMVPN with Zone-Based Policy Firewall Configuration

```

class-map type inspect match-any safe-vpn-cmap
  match protocol http
  match protocol smtp
class-map type inspect match-any vpn-safe-cmap
  match protocol citrix
class-map type inspect match-any safe-hostile-cmap
  match protocol dns
  match protocol http
  match protocol https
  match protocol ftp
!
!
policy-map type inspect safe-hostile-pmap
  class type inspect safe-hostile-cmap
  inspect
  class class-default
policy-map type inspect safe-vpn-pmap
  class type inspect priv-vpn-cmap
  inspect
  class class-default
policy-map type inspect vpn-safe-pmap
  class type inspect vpn-priv-cmap
  inspect
  class class-default
!
zone security hostile
zone security safe
zone security vpn
zone-pair security safe-vpn source safe destination vpn
  service-policy type inspect safe-vpn-pmap
zone-pair security vpn-safe source vpn destination safe
  service-policy type inspect vpn-safe-pmap
zone-pair security safe-hostile source safe destination hostile
  service-policy type inspect safe-hostile-pmap
!
!
crypto isakmp policy 10
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
!
```

```
crypto ipsec transform-set md5-des esp-des esp-md5-hmac
!
crypto ipsec profile cry-profile-1
  set transform-set md5-des
!
!
!
!
!
!
interface Tunnel0
  ip address 172.18.1.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication DMVPN_NW
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 360
  ip nhrp cache non-authoritative
  zone-member security vpn
  delay 1000
  tunnel source GigabitEthernet0/0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile cry-profile-1
!
interface GigabitEthernet0/0
  ip address 172.16.107.10 255.255.255.0
  ip virtual-reassembly
  zone-member security hostile
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.107.10 255.255.255.0
  ip virtual-reassembly
  zone-member security safe
  duplex auto
  speed auto
```

## Site-to-Site VTI

Similar to DMVPN, site-to-site VTI employs a virtual interface (interface tunnel [number]) for IPsec VPN connectivity. When the site-to-site VTI interface is assigned to a security zone, traffic routing to and from other interfaces in the router are subjected to zone-to-zone firewall policy. If the site-to-site VTI interface is assigned to the same security zone as another interface (for example, Gigabit Ethernet 0/0), traffic moving between hosts on the site-to-site VTI connection and hosts connected to Gigabit Ethernet 0/0 will freely pass with no policy application.

This basic example illustrates a site-to-site VTI interface in the “VPN” zone, the FastEthernet 0/1 interface in the “safe” zone, and the FastEthernet 0/0 interface in the “hostile” zone. Policy is applied according to the following matrix:

Source v	Destination >	Safe	VPN	Hostile
Safe		N/A	smtp, http	dns, http, https, ftp
VPN		citrix	N/A	Deny
Hostile		Deny	Deny	N/A

For more information on site-to-site VTI configuration, please see:

[http://www.cisco.com/en/US/products/ps6635/products\\_white\\_paper0900aecd8029d629.shtml](http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd8029d629.shtml)

For a conceptual discussion of Zone-Based Policy Firewall, please see:

[http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a008060f6dd.html](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html)

### Site-to-Site VTI with Zone-Based Policy Firewall Configuration

```

class-map type inspect match-any safe-vpn-cmap
  match protocol http
  match protocol smtp
class-map type inspect match-any vpn-safe-cmap
  match protocol citrix
class-map type inspect match-any safe-hostile-cmap
  match protocol dns
  match protocol http
  match protocol https
  match protocol ftp
!
!
policy-map type inspect safe-hostile-pmap
  class type inspect safe-hostile-cmap
  inspect
  class class-default
policy-map type inspect safe-vpn-pmap
  class type inspect priv-vpn-cmap
  inspect
  class class-default
policy-map type inspect vpn-safe-pmap
  class type inspect vpn-priv-cmap
  inspect
  class class-default
!

```

```
zone security hostile
zone security safe
zone security vpn
zone-pair security safe-vpn source safe destination vpn
  service-policy type inspect safe-vpn-pmap
zone-pair security vpn-safe source vpn destination safe
  service-policy type inspect vpn-safe-pmap
zone-pair security safe-hostile source safe destination hostile
  service-policy type inspect safe-hostile-pmap
!
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile VTI
  set transform-set TSET
!
!
interface Tunnel0
  ip address 192.168.10.2 255.255.255.0
  zone-member security vpn
  tunnel source 10.0.149.220
  tunnel destination 10.0.149.221
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile VTI
!
interface FastEthernet0/0
  ip address 10.0.149.220 255.255.255.0
  zone-member security hostile
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.20.1 255.255.255.0
  zone-member security safe
  duplex auto
  speed auto
```

### Easy VPN with IPsec VTI

Easy VPN VTI differs from DMVPN and site-to-site VTI in that instead of using an “interface tunnel **[number]**” configuration, an “interface virtual-template type tunnel **[number]**” configuration is used to apply IP attributes for IPsec Easy VPN clients. Network Address Translation (NAT), quality of

service (QoS), intrusion prevention, and other IP policy applications may be applied to the virtual-template interface, as well as classic or Zone-Based Policy Firewall.

This basic example illustrates an Easy VPN-VTI interface in the “VPN” zone, the FastEthernet 0/1 interface in the “safe” zone, and the FastEthernet 0/0 interface in the “hostile” zone. Policy is applied according to the following matrix:

Source v	Destination >	Safe	VPN	Hostile
Safe		N/A	smtp, http	dns, http, https, ftp
VPN		citrix	N/A	Deny
Hostile		Deny	Deny	N/A

For more information for Easy VPN with IPsec VTI, please see:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/prod\\_white\\_paper0900aecd803645b5.shtml](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/prod_white_paper0900aecd803645b5.shtml)

For a conceptual discussion of Zone-Based Policy Firewall, please see:

[http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a008060f6dd.html](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html)

### Easy VPN-VTI with Zone-Based Policy Firewall Configuration

```

class-map type inspect match-any safe-vpn-cmap
  match protocol http
  match protocol smtp
class-map type inspect match-any vpn-safe-cmap
  match protocol citrix
class-map type inspect match-any safe-hostile-cmap
  match protocol dns
  match protocol http
  match protocol https
  match protocol ftp
!
!
policy-map type inspect safe-hostile-pmap
  class type inspect safe-hostile-cmap
  inspect
  class class-default
policy-map type inspect safe-vpn-pmap
  class type inspect priv-vpn-cmap
  inspect
  class class-default
policy-map type inspect vpn-safe-pmap
  class type inspect vpn-priv-cmap
  inspect
  class class-default
!
zone security hostile
zone security safe
zone security vpn
zone-pair security safe-vpn source safe destination vpn
  service-policy type inspect safe-vpn-pmap

```

```

zone-pair security vpn-safe source vpn destination safe
  service-policy type inspect vpn-safe-pmap
zone-pair security safe-hostile source safe destination hostile
  service-policy type inspect safe-hostile-pmap
!
!
aaa new-model
!
aaa authentication login default local
aaa authorization network default local
!
aaa session-id common
!
!
username cisco privilege 15 password 0 cisco
!
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
  crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
  key cisco
  dns 6.0.0.2
  wins 7.0.0.1
  domain cisco.com
  pool dpool
  acl 101
  crypto isakmp profile vi
    match identity group cisco
    isakmp authorization list default
    client configuration address respond
    virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
  set transform-set set
  set isakmp-profile vi
!
interface FastEthernet0/0
  ip address 10.0.149.221 255.255.255.0
  zone-member security hostile
  duplex auto

```

```

speed auto
!
interface FastEthernet0/1
ip address 192.168.20.21 255.255.255.0
zone-member security safe
duplex auto
speed 100
!
!
interface Virtual-Template1 type tunnel
ip unnumbered FastEthernet0/1
zone-member security vpn
tunnel source FastEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile vi
service-policy output FOO
!
ip local pool dpool 5.0.0.1 5.0.0.3
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.149.207
!
access-list 101 permit ip 192.168.20.0 0.0.0.255 any

```

### Zone-Based Policy Firewall with non-interface-based IPsec VPN

Some types of IPsec VPN differ from tunnel-interface- (VTI-)based VPN in that instead of using an “interface tunnel [number]” or “interface virtual-template type tunnel [number]” configuration, a crypto map is applied to one or more interfaces in a router, and traffic passing the interface is checked to see if it matches the cryptographic policy. Traffic matching the policy is encrypted and sent over the IPsec VPN connection. IPsec VPN features such as classic site-to-site connections, classic EasyVPN, and GET VPN all apply this type of configuration. Non-interface-based IPsec VPN generally requires more complex configuration than VTI-based VPN features for application of features such as network address translation (NAT), quality of service (QoS), intrusion prevention, as the traffic must be specifically selected from all traffic flowing through clear-text interfaces, and may require feature application on multiple interfaces to catch all cleartext traffic that will enter or leave a router through an IPsec tunnel.

This basic example illustrates an IPsec crypto map applied to the FastEthernet 0/0 interface in the “Hostile” zone, and connection to the protected network on the FastEthernet 0/1 interface in the “safe” zone. Policy is applied according to the following matrix:

Source >	Destination >	Safe	Hostile
Safe		N/A	All dns, http, https, ftp traffic SMTP connections from 192.168.20.0/24 to 192.168.21.0/24
Hostile		Deny, except for Citrix connections from 192.168.21.0/24 to 192.168.20.0/24	N/A

For a conceptual discussion of Zone-Based Policy Firewall, please see:

[http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a008060f6dd.html](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html)

## Zone-Based Policy Firewall with Classic IPSec Configuration

```

class-map type inspect match-all safe-vpn-mail-cmap
  match protocol smtp
  match access-group 112
class-map type inspect match-all vpn-safe-citrix-cmap
  match protocol citrix
  match access-group 111
class-map type inspect match-any safe-hostile-cmap
  match protocol dns
  match protocol http
  match protocol https
  match protocol ftp
!
!
policy-map type inspect safe-hostile-pmap
  class type inspect safe-hostile-cmap
    inspect
  class type inspect safe-vpn-mail-cmap
    inspect
  class class-default
policy-map type inspect hostile-safe-pmap
  class type inspect vpn-safe-citrix-cmap
    inspect
  class class-default
!
zone security hostile
zone security safe
zone-pair security hostile-safe source hostile destination safe
  service-policy type inspect hostile-safe-pmap
zone-pair security safe-hostile source safe destination hostile
  service-policy type inspect safe-hostile-pmap
!
!
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set 3des-sha-set esp-3des esp-sha-hmac
!
crypto map vpn-map 10 ipsec-isakmp
  match address 101
  set peer 10.0.150.221
  set transform-set 3des-sha-set
!
interface GigabitEthernet0/0
ip address 10.0.149.221 255.255.255.0

```

```
zone-member security hostile
duplex auto
speed auto
crypto map vpn-map
!
interface GigabitEthernet0/1
ip address 192.168.20.21 255.255.255.0
zone-member security safe
duplex auto
speed 100
!
!
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.21.0
0.0.0.255
access-list 111 permit ip 192.168.21.0 0.0.0.255 192.168.20.0
0.0.0.255
access-list 112 permit ip 192.168.20.0 0.0.0.255 192.168.21.0
0.0.0.255
```



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCI, CCNA, CCNP, CCSF, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)