SECURITY

IPSec VPN Design

The definitive design and deployment guide for secure virtual private networks

Vijay Bollapragada, CCIE® No. 1606
Mohamed Khalid, CCIE No. 2435
Scott Wainner

ciscopress.com

IPSec VPN Design

Vijay Bollapragada
Mohamed Khalid
Scott Wainner

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

The configuration of the EzVPN server is shown in Example 4-5.

Example 4-5 *EzVPN Server-side Configuration*

```
vpn-gw1-east#
!
hostname vpn-gw1-east
!
username ezvpn password 0 east
username ezvpn1@vpngroup password 0 ezvpn1east
username ezvpn2@vpngroup password 0 ezvpn2east
aaa new-model
!
aaa authentication login vpn local
aaa authorization network vpn local
aaa session-id common
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10 10
!
crypto isakmp client configuration group vpngroup
 key ciscoezvpn
 dns 10.1.1.10
 wins 10.1.1.11
 pool vpnpool
 include-local-lan
 backup-gateway 9.1.1.36
!
!
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
!
crypto dynamic-map dynamic 1
 set transform-set vpn
 reverse-route remote-peer 9.1.1.33
!
!
crypto map vpn client authentication list vpn
crypto map vpn isakmp authorization list vpn
crypto map vpn client configuration address respond
crypto map vpn 3 ipsec-isakmp dynamic dynamic
!
!
interface Loopback0
 ip address 9.2.1.100 255.255.255.255
!
interface FastEthernet0/0
 ip address 9.1.1.35 255.255.255.248
 duplex full
 crypto map vpn
!
```

Example 4-5 *EzVPN Server-side Configuration (Continued)*

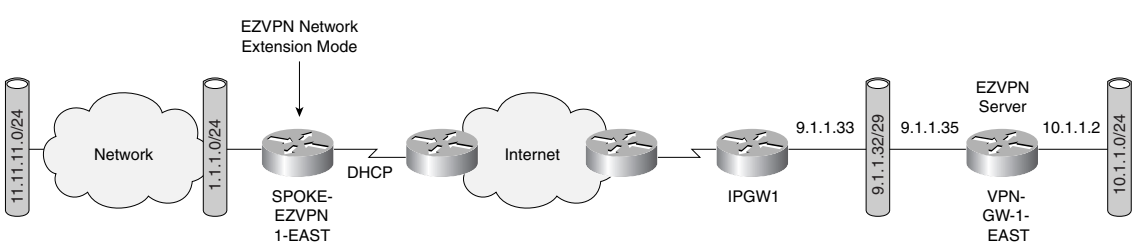
```
interface FastEthernet2/0
 ip address 100.1.1.147 255.255.255.0
 duplex full
!
interface FastEthernet4/0
 ip address 10.1.1.1 255.255.255.0
 duplex full
!
router ospf 1
 log-adjacency-changes
 redistribute static subnets
 network 10.1.1.0 0.0.0.255 area 0
!
ip local pool vpnpool 10.0.68.1 10.0.68.100
ip classless
ip route 0.0.0.0 0.0.0.0 9.1.1.33
!
radius-server host 100.1.1.4 auth-port 1645 acct-port 1646
radius-server key cisco
end
```

The IOS command **crypto isakmp client configuration group vpngroup** defines the attributes for the VPN group that was assigned to the EzVPN client.

Network Extension Mode

Figure 4-3 shows an EzVPN client in Network Extension Mode. This mode allows the EzVPN client to present a full, routable network to the tunneled network.

Figure 4-3 *EzVPN IPSec Network Extension Mode Connection*



IPSec encapsulates all traffic from the EzVPN client's private network, which is marked as 'inside' to networks behind the IPSec gateway. Therefore, devices behind the gateway have direct access to devices on the EzVPN client's private network via the tunnel and vice versa without the need for NAT or PAT. As there is no reason for NAT or PAT, the EzVPN server does not push down an IP address for tunneled traffic, but all other attributes like ACLs, DNS, and

WINS, can be pushed down. Example 4-6 shows the configuration of Network Extension Mode on the EzVPN client shown in Figure 4-3.

Example 4-6 *EzVPN Client Configuration for Network Extension Mode*

```
spoke-ezvpn1-east#
!
hostname spoke-ezvpn1-east
!
crypto ipsec client ezvpn vpn
 connect auto
 group vpngroup key ciscoezvpn
 local-address Ethernet0
 mode network-extension
 acl 100
 peer 9.1.1.35
 username ezvpn1@vpngroup password  ezvpn1east
!
interface Ethernet0
 ip address dhcp
 load-interval 30
 half-duplex
 crypto ipsec client ezvpn vpn outside
!
interface FastEthernet0
 ip address 1.1.1.1 255.255.255.0
 load-interval 30
 speed 100
 full-duplex
 no keepalive
 crypto ipsec client ezvpn vpn inside
!
access-list 100 permit 11.1.1.0 0.0.0.255 any
ip route 0.0.0.0 0.0.0.0 dhcp
```

Note the ACL 100 under the mode network-extension in the configuration. The ACL 100 permits networks behind the "inside" network (11.1.1.0/24) and allows traffic to and from these subnets to be encrypted. Without the access list, only traffic to and from the "inside" subnet (1.1.1.0/24) is encrypted.

NOTE The EzVPN server configuration is the same for both Client Extension Mode and Network Extension Mode. The client configuration determines which mode is being used.

Redundancy is always an integral part of any IPSec design and, in the case of EzVPN dead peer detection along with backup peer list, makes such a design possible. Example 4-7 shows the client configuration with multiple EzVPN server peer addresses manually configured on the

client. An alternate mechanism to provide EzVPN server redundancy is to push the backup server's address list down to the client as an attribute. Dead peer detection is on by default on the EzVPN clients.

Example 4-7 *EzVPN Server Redundancy*

```
spoke-ezvpn1-east#
!
hostname spoke-ezvpn1-east
!
crypto ipsec client ezvpn vpn
 connect auto
 group vpngroup key ciscoezvpn
 local-address Ethernet0
 mode network-extension
 peer 9.1.1.35
 peer 9.1.1.45
 username ezvpn1@vpngroup password  ezvpn1east
```

EzVPN can be combined with XAUTH and MODECFG to provide extended authentication and thereby push all MODECFG attributes to the client. The attributes to be pushed can be defined locally on the EzVPN server or defined on a AAA server and defined either on a per-group or per-user basis. Example 4-8 shows the policies configured on a AAA server on a group basis.

Example 4-8 *Per-Group–based Policy Configuration on a AAA Server*

```
vpngroup Password = "cisco", Service-Type = Outbound
 cisco-avpair = "ipsec:tunnel-type=ESP"
 cisco-avpair = "ipsec:key-exchange=ike"
 cisco-avpair = "ipsec:tunnel-password=ciscoezvpn"
 cisco-avpair = "ipsec:addr-pool=vpnpool"
 cisco-avpair = "ipsec:default-domain=cisco"
 cisco-avpair = "ipsec:inacl=101"
 cisco-avpair = "ipsec:access-restrict=fastethernet 0/0"
 cisco-avpair = "ipsec:group-lock=1"
cisco-avpair = "ipsec:backup-server=9.1.1.35"

 cisco-avpair = "ipsec:dns-servers=10.1.1.10"
 cisco-avpair = "ipsec:firewall=1"
 cisco-avpair = "ipsec:include-local-lan=1"
 cisco-avpair = "ipsec:save-password=1"
 cisco-avpair = "ipsec:wins-servers=10.1.1.11"
 cisco-avpair = "ipsec:max-users = 100"
 cisco-avpair = "ipsec:max-logins = 2"
```

NOTE When AAA is used for pushing the attributes, AAA between EzVPN server and the AAA server requires a hard-coded password of **cisco**. Therefore, notice the use of the string **cisco** as the vpngroup password. This is a requirement of the Cisco AAA implementation.

Example 4-9 shows the configuration of the policy attributes locally on the EzVPN server on a per-group basis.

Example 4-9 *Per-Group EzVPN Policy Attributes Configured Locally on an EzVPN Server*

```
crypto isakmp client configuration group vpngroup
 key ciscoezvpn
 dns 10.1.1.10
 wins 10.1.1.11
 domain cisco.com
 pool vpnpool
 group-lock
 save-password
 include-local-lan
 pfs
 backup-gateway 9.1.1.36
 max-users 100
 max-logins 2
 access-restrict fastEthernet 0/0
```

You've already seen described some attributes such as IP address, WINS, DNS, and backup server in the previous section. For a complete list of attributes and their description, refer to Cisco IOS EzVPN documentation. A couple of very useful attributes for telecommuter scenarios are max-logins and include-local-lan. The max-logins attribute allows the administrator to restrict the number of simultaneous IPSec connections from the same user to the gateway. The include-local-lan attribute is very useful in scenarios in which the telecommuter's LAN has resources, such as printers, attached to the LAN and access to these resources is required when the VPN tunnel is up.

The attributes may also be applied on a per-user basis. A user attribute overrides a group attribute value. These attributes are retrieved at the time user authentication occurs using XAUTH, and are then combined with group attributes and applied during Mode-Configuration. User-based attributes are available only if RADIUS is used as the database. Example 4-10 shows the RADIUS attributes that must be configured on a per-user basis.

Example 4-10 *User-Based Policy Control Using AAA*

```
ezvpn1@vpngroup Password = "ezvpn1east"
framed-Ip-Address=10.0.68.1
ipsec:user-save-password=1
ipsec:user-include-local-lan=1
ipsec:user-vpn-group=cisco
```

Note that EzVPN using the Cisco Unity protocol is not an IETF standard. The Cisco proprietary Unity protocol is supported by Cisco IOS devices, VPN 3000, and PIX devices for interoperability across Cisco devices.

Digital Certificates for IPSec VPNs

You have learned from Chapter 2, "IPSec Overview," that pre-shared keys and digital certificates are two primary authentication methods in IKE that can be used in the context of IPSec VPN deployments. You also saw that pre-shared keys with IKE Main Mode cannot be used for remote access scenarios in which the responder does not know the source IP address of the initiator in advance. Although Aggressive Mode can alleviate this issue, given that Aggressive Mode does not offer any form of ID protection, such a solution may not be acceptable. You also saw XAUTH provide an additional level of authentication for Aggressive Mode with pre-shared keys. Another solution for such a scenario is the use of digital certificates instead of pre-shared keys.

In addition to solving the authentication issue for remote access users, digital certificate–based authentication is also becoming increasingly popular for large IPSec VPN site-to-site deployments because it is more scalable than pre-shared keys. Without digital signatures, users must either manually exchange public keys or secrets between each pair of devices that use IPSec to protect communications. This is cumbersome because when a new device is added to the network, users are required to make configuration changes on every other device it securely communicates with. By using digital certificates, users simply enroll each new device with a Certificate Authority, and none of the other devices need modification. When the new device attempts an IPSec connection, IKE automatically exchanges certificates with the peer and the devices authenticate each other, thus making a large-scale IPSec VPN deployment very scalable using digital certificates. An entire book can be written on digital certificates and PKI. You will be introduced to some of the components of PKI in the remainder of this chapter.

Digital Certificates

Digital certificates provide a means to digitally authenticate devices and individual users. These certificates act kind of like an online passport—they are tamper proof and cannot be forged. An individual that wishes to send encrypted data obtains a digital certificate from a *Certificate Authority (CA)*. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available. The recipient of the encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA, and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. Public key infrastructure (PKI) is the enabler for managing digital certificates for IPSec VPN deployment. The most widely used format for digital certificates is X.509, which is supported by Cisco IOS.