

VPN Gateway Router Configuration Using Transform Sets

Michael J. Martin

Implementing IPsec VPN gateways on Cisco routers involves a number of different configuration elements. In addition to the ISAKMP and IKE configuration covered in previous articles in this series, transform set definitions and crypto maps are part of configuring gateways that will support Cisco software VPN client connections.

IPsec/ISAKMP utilizes a two-phase negotiating process. The first phase authenticates the peers, and the second phase negotiates the algorithms (i.e., DES/3DES) and protocols (ESP/AH) the peers will use to protect data communications. Cisco IOS devices use transform set definitions to create IPsec security protocol/algorithm sets. These definition sets are then assigned to crypto map sequence entries. The VPN gateway (router) then provides these definition sets during the Phase 2 security association (SA) negotiation. If, however, the two peers cannot find a mutually acceptable set of security protocols to utilize, the SA negotiation will fail and the IPsec connection will not be established.

A transform set has three configuration elements: data encryption, data authentication, and encapsulation mode. The data encryption and authentication definitions are created with the configuration command `<crypto ipsec transform-set {transform set name} {data encrypt} {data auth} comp-lzs>`. The last option, "comp-lzs," enables IP compression. Once the transform set is created, you are dropped into a sub-configuration mode that allows you to define the encapsulation mode to be either tunnel mode, the default, which encrypts the whole IP packet, or transport mode, which encrypts only the data portion of the packet. The sub-configuration command is `<mode {transport | tunnel}>`. Here are the various encryption options available for IPsec ESP transform sets:

Data Encryption	Data Authentication	Security Service
esp-3des	esp-md5-hmac/esp-sha-hmac	168-Bit Encryption/Authentication
esp-null	esp-md5-hmac/esp-sha-hmac	No Encryption/Authentication
esp-3des	esp-md5-hmac/esp-sha-hmac	56-Bit Encryption/Authentication
esp-aes 128	esp-md5-hmac/esp-sha-hmac	128-Bit Encryption/Authentication
esp-aes 192	esp-md5-hmac/esp-sha-hmac	192-Bit Encryption/Authentication
esp-aes 256	esp-md5-hmac/esp-sha-hmac	256-Bit Encryption/Authentication

Here is a transform set configuration example:

```
outlan-rt02(config)#crypto ipsec transform-set AES-192-SHA-COMZ esp-aes 192  
esp-sha-hmac comp-lzs
```

```
outlan-rt02(cfg-crypto-trans)#mode transport  
outlan-rt02(cfg-crypto-trans)#exit  
outlan-rt02(config)#
```

Once you have built a transform set, you may need to make adjustments. Changes to transform sets that have been associated with a crypto map (and are being actively used to protect traffic) will only apply to post-change SAs. Any active SAs will re-negotiate to use the new set definition. To force a re-negotiation, a given SA can be cleared using `<clear crypto sa>`. To see the transform sets

VPN Gateway Router Configuration Using Transform Sets

Michael J. Martin

configured on the router, use <show crypto ipsec transform-set> You can see which transform set has been selected by looking at the IPsec SA. Use <show crypto ipsec sa peer x.x.x.x>:

inbound esp sas:

```
spi: 0x26886B9F(646474655)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2157, flow_id: FPGA:157, crypto map: no-nat-crypto
sa timing: remaining key lifetime (k/sec): (4530308/3529)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```