.:Books:::IPSec VPNDesign :.

Print

Links

[/.]
[tr]
[wired]
[bbc]
[fark]
[salon]
[gn]
[sb]
[jmro]
[g&m]
[sm]
[nyt]
[ud]
[cbc]
[istop]
[th]
[oc]

Chapter3.Enhanced IPSec Features

Previous Top Next

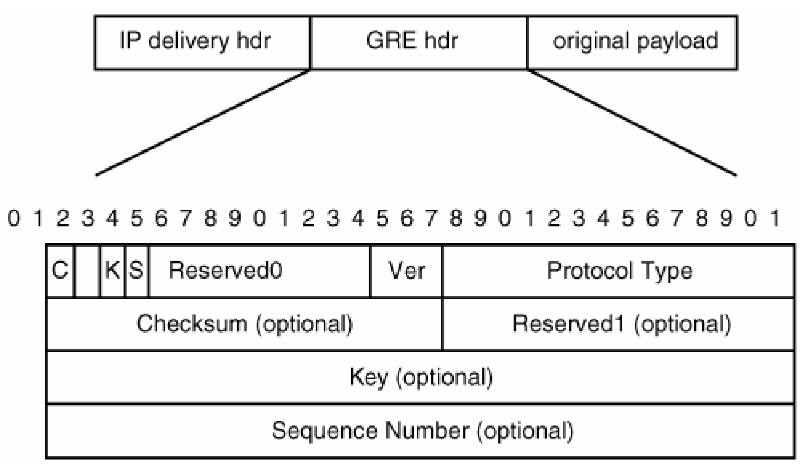
GRE and IPSec

DesigningaVPNusing IPSec forconnectivitybetweenpeershasinherent limitations.Theseare:

- **IPSec canencrypt/decryptonlyIPtraffic.**
- **IPtrafficdestinedtoamulticastorbroadcastIPaddresscannotbehandledby IPSec, whichmeansthatIPmulticasttrafficcannottraversethe IPSec tunnel. Also,manyroutingprotocols(suchasEIGRP,OSPF,andRIPv2)useamulticast orabroadcastaddress;therefore,dynamicroutingusingtheserouting protocolscannotbeconfiguredbetween IPSec peers.**

TheselimitationscanbeovercomebyconfiguringanIP-encapsulated GRE tunnel betweenthepeersandapplying IPSec protectiononthe GRE/IP tunnel. RFC2784 covers GRE indetail.Itessentially GRE-encapsulatesanypayloadinanIPunicast packetdestinedtothe GRE endpoint.A GRE-encapsulatedpacketisshownin Figure 3-7.

Figure3-7. GRE-EncapsulatedPacket



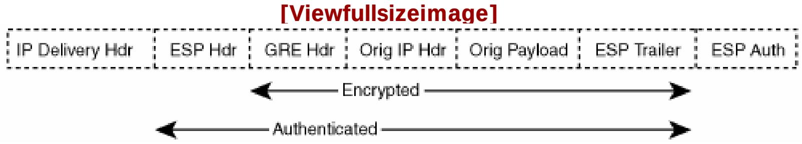
When GRE isusedinconjunctionwith IPSec, either tunnel modeortransportmode canbeused. Tunnel modeaddsan IPSec IPheadertothe GRE packetwhereas IPSec transportmodeusestheoriginal GRE packet'sIPheader. Figures3-8 and 3-9 show GRE with IPSec in tunnel modeandtransportmode,respectively.

Figure3-8. GRE-EncapsulatedPacketin IPSec Tunnel Mode

[Viewfullsizeimage]

Figure3-9. GRE-EncapsulatedPacketin IPSec TransportMode

[Viewfullsizeimage]



IPSec transportmodeisthemostefficientwaytocombine GRE and IPSec together because GRE encapsulationalreadyplacesanewIPheaderonthepayload.Theuse of IPSec transportmode,however,requiresthatthe GRE encapsulationuseanIP sourceanddestinationaddressthatisreachableviatheIPpathtoitspeer. GRE adds24bytesofoverheadtotheoriginalIPpacket.Inconjunctionwith IPSec transportmode, GRE encapsulationadds4bytesofextraoverheadincomparisonto the20bytesofoverheadaddedby IPSec tunnel mode.Althoughtheadditional overheadandextraprocessingfor GRE encapsulationreducetheoverallthroughput andmayimpactthelatencyoftheconnection,thebenefitsofusing GRE with IPSec faroutweightheimpact.

Useof GRE with IPSec alsohastheusefulsideeffectofmaking IPSec VPN configurationsimpler.Traditional IPSec configurationbetweenpeersrequires IPSec policyconfigurationtospecifytheprotectedsubnetssothattrafficdestinedtothe protectedsubnetsisencryptedordecrypted.Everytimeanewprotectedsubnetis addedordeleted,the IPSec policyconfigurationneedstobeupdatedonbothpeers. Also,thesecuritypolicydatabase(SPD)andsecurityassociationdatabase(SADB) sizecangetquitelargedependingonthe IPSec SAbundlesnegotiatedand installed.Thisusuallyhasanimpactontheoverallperformanceandscalabilityof thesecuritygateway.Using GRE with IPSec significantlyreducestheconfiguration complexity,asthepolicyintheSPDneedstomatchthetrafficonlytothe GRE endpointaddresses.Theadditionordeletionoftheprotectedsubnetsrequiresno changeintheconfigurationofthe IPSec SPDpeers.Theprotectedsubnettrafficis directedtobeencryptedbybeingroutedoutthe GRE tunnel interface(everything thatgoesthroughthe GRE tunnel willbeencrypted).Thisdoesmeanthatthe granularityforwhatgetsencryptedisnowattheIPaddresslevelratherthanthe portlevelinthetransportheader.Ingeneral,thisisnotanissuebecauseusuallyall trafficforhostsonprotectedsubnetsistobeencrypted.

The GRE encapsulationdoesincreasethesizeofthepacketandpotentiallycauses fragmentationissues.PacketfragmentationcanbeavoidedbyensuringthatPMTUD isenabled.ToensurethatPMTUDworksasexpected,ICMPcode3type4messages mustbeallowedthroughthenetwork.IfICMPcode3type4messagesarenot supportedinthenetwork,settingalowerMTUsizeonthe tunnel interfacewill causefragmentationbeforeencryptiontohappen,achievingthesameeffectasLook AheadFragmentation.IftheendhostssupportPMTUD,thentheywillmatchthe packetsizetotheconfiguredMTU.Boththe IPSec and GRE specificationssupport PathMTUDiscoverybyallowingthecopyoftheDFbitoftheoriginalIPheaderinto thenewlybuiltIPheader.Thisisusuallyaconfigurationoptionofthedevices.

IftheendhostdoesnotsupportPMTUDandtheDFbitisnotset,thepacketwillbe fragmentedandsentoverthe GRE-encrypted tunnel. Onebenefittoreducingthe MTUonthe GRE tunnel isthatpacketfragmentationoccursbeforeithitsthe encryptionprocess;therefore,thereassemblyisdoneontheendhostandnoton thepeer IPSec gateway.

Example3-10 showstheconfigurationof GRE tunnelsprotectedby IPSec onSPOKE-1-EAST.Notethe tunnelprotection ipsecprofile gre commandunderthe GRE tunnel interfaceconfiguration,whichisanewwayofprotecting GRE tunnelsusing IPSec whereinthephysicalinterfacethatthe GRE tunnel traversesdoesnotneed thecryptomapconfiguration.Comparethisconfigurationwith Example3-11 ,which showstheoldwayof IPSec-protected GRE inIOS.

Example3-10. GRE and IPSec Using Tunnel ProtectionCLI

```
spoke-1-east

!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 9.1.1.35
crypto isakmp keepalive 60 2

!
crypto ipsec transform-set test esp-3des esp-sha-hmac
!
crypto ipsec profile gre
 set transform-set test
!
int tu0
 ip address 192.168.1.1 255.255.255.0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source s0/0
 tunnel destination 9.1.1.35
 tunnel path-mtu-discovery
 tunnel protection ipsec profile gre

!
interface Serial0/0
 ip address 9.1.1.146 255.255.255.252
 crypto map vpn
!
interface Ethernet0/1
 ip address 10.0.68.1 255.255.255.0
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 9.1.1.145
ip route 10.0.1.0 0.0.0.255 tu0
```

Example3-11. GRE Tunnel Keepalive

```
spoke-1-east

!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 9.1.1.35
crypto isakmp keepalive 60 2
```

```
!
crypto ipsec transform-set test esp-3des esp-sha-hmac
mode transport
!
crypto map vpn 1 ipsec-isakmp
 set peer 9.1.1.35
 set transform-set test
 match address 100

!
int tunnel0
ip address 192.168.1.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel source s0/0
tunnel destination 9.1.1.35
keepalive 20 3

!
interface Serial0/0
 ip address 9.1.1.146 255.255.255.252
 crypto map vpn

!
interface Ethernet0/1
 ip address 10.0.68.1 255.255.255.0
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 9.1.1.145
ip route 10.0.1.0 0.0.0.255 tu0
!
access-list 100 permit gre host 9.1.1.146 host 9.1.1.35


spoke-1-east#show cry isa sa
dst             src             state          conn-id    slot
9.1.1.35        9.1.1.146       QM_IDLE             82       0

spoke-1-east#show int tu0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Ethernet0/1 (10.0.68.1)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (20 sec), retries 3

  Tunnel source 9.1.1.146 (Serial0/0), destination 9.1.1.35
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:14
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     483 packets input, 36396 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     168 packets output, 8596 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out

Tunnel0: sending keepalive, 9.1.1.35->9.1.1.146 (len=24 ttl=255),
counter=1
Tunnel0: GRE/IP encapsulated 9.1.1.146->9.1.1.35 (linktype=7, len=48)
IP: s=9.1.1.146 (Tunnel0), d=9.1.1.35 (Serial0/0), len 48, sending,
proto =47
IP: s=9.1.1.35 (Serial0/0), d=9.1.1.146 (Serial0/0), len 24, rcvd 3,
proto=47
Tunnel0: GRE/IP to decaps 9.1.1.35->9.1.1.146 (len=24 ttl=253)
Tunnel0: keepalive received, 9.1.1.35->9.1.1.146 (len=24 ttl=253),
reset
```

TheprimarymotivationforusingGRE with IPSec isitsabilitytorundynamic routingprotocolssuchasOSPForEIGRPbetweensitesforadvertisingtheprotected subnets.Dynamicroutingalsoimplicitlyhelpsinfailoversituations.Ontheother hand,ifstaticroutesareusedforthereachabilityoftheprotectedsubnetswith GRE, thenthereisnowayforthe IPSec peerstoknowthattheprotectedsubnets arenotreachablewhenthe GRE tunnel endpointsarenotreachableanymore.To facilitateknowledgeofthe tunnel status, GRE keepalivemessagescanbe configuredonthe GRE peers. Example3-11 showsconfigurationof GRE keepalive underthe tunnel interface. GRE tunnel comesupassoonasitseesthedefault routeintheroutingtableonSPOKE-1-EAST.Now,ifVPN-GW1-EASTgoesdown,you wantthe tunnel interfaceonSPOKE-1-EASTtogodown—thisisfacilitatedby GRE keepalives.

Note

GRE keepalivesarenotsupportedwiththe tunnelprotection IPsec configurationsyntax.Therefore,for GRE keepalivefunctionality,youneedto usetheold-stylecryptomapconfiguration.

Figure3-10 showstheformatofa GRE keepalivepacketfromSPOKE-1-EAST's perspective.

Figure3-10. GRE KeepalivePacket

NoticethatthedestinationIPaddressintheinnerIPheaderisSPOKE-1-EAST's tunnel sourceaddress(9.1.1.146)andthesourceIPaddressintheinnerIPheader isthatofthe tunnel destinationaddressofVPN-GW1-EAST(9.1.1.35).Theprotocol type(PT)intheinnerheaderissetto0.Thispayloadissentina GRE tunnel witha protocoltypeofIPintheouterheaderwithsourceanddestinationaddressesas configuredonthe tunnel interfaceshownin Example3-11 .The tunnel keepalive counterisincrementedbyoneasshowninthedebugsnapshotsin Example3-11 .As the GRE tunnel isprotectedviathecryptomap,thiskeepalivepacketwillbe encryptedwhenitleavesSPOKE-1-EAST.Thepacketwillreachthefarend tunnel endpointpeer(VPN-GW1-EAST)vianormalrouting.UponarrivalonVPN-GW1-EAST, thepacketwillgetdecryptedandthendecapsulated;theresultingpacketwillhavea sourceIPaddressofVPNGW1-EASTandadestinationIPaddressofSPOKE-1-EAST. ThispacketwillnowmakeitswaybacktoSPOKE-1-EASTthroughthe GRE tunnel,

whichisagainencrypted.Thepacket,onreachingSPOKE-1-EASTafterdecryption and GRE decapsulation,willresultinaPTof0,whichwillsignifythatthisisa keepalivepacketthatitoriginallyconstructed.Thereceiptofthispacketsignifiesthe GRE tunnel isup.The tunnel keepalivecounterwillberesetto0andthepacket willbediscarded.Thisprocessisrepeatedperiodicallybyeach GRE peer.

WhenVPN-GW1-EASTbecomesunreachablefromSPOKE-1-EASTforwhatever reason,SPOKE-1-EASTwillcontinuetoconstructandsendthekeepalivepacketsas wellasnormaltraffic.Becausethekeepalivesdonotcomeback,the tunnel line protocolwillstayupaslongasthe tunnel keepalivecounterislessthanthe configuredretryvalue.Whenthenumberofretriesexceedstheconfiguredvalue, thelineprotocolwillbebroughtdownonthe tunnel interfaceonVPN-SPOKE1-EAST.

Intheup/downstate,the tunnel willnotforwardorprocessanytrafficapartfrom thekeepalivepackets.ThereceptionofakeepalivepacketfromVPN-GW1-EAST wouldimplythatthe tunnel endpointisagainreachable;whenthishappens,the tunnel keepalivecounterwillberesetto0andthelineprotocolwillchangestate backtoup,resumingdatatraffic.

Onethingworthmentioningisthat GRE keepalivepacketsaresentoutwiththeTOS bitsetto5sothattheroutersprocessthosepacketswithhigherpriority,even duringcongestion.

◂ Previous | Top ▴ | Next ▸