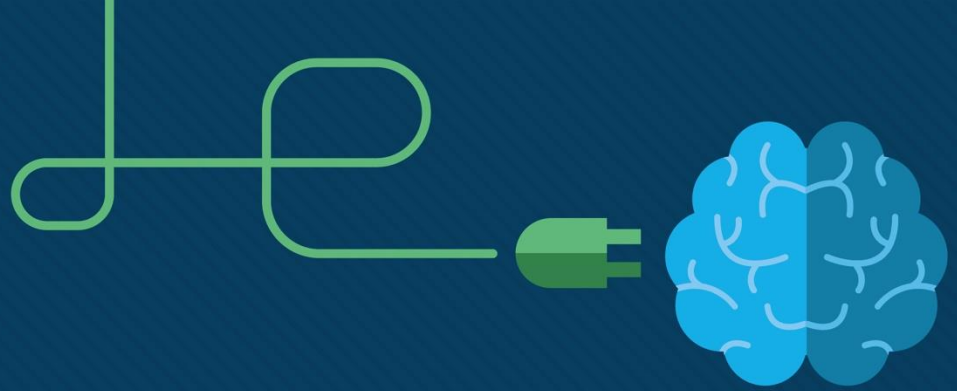
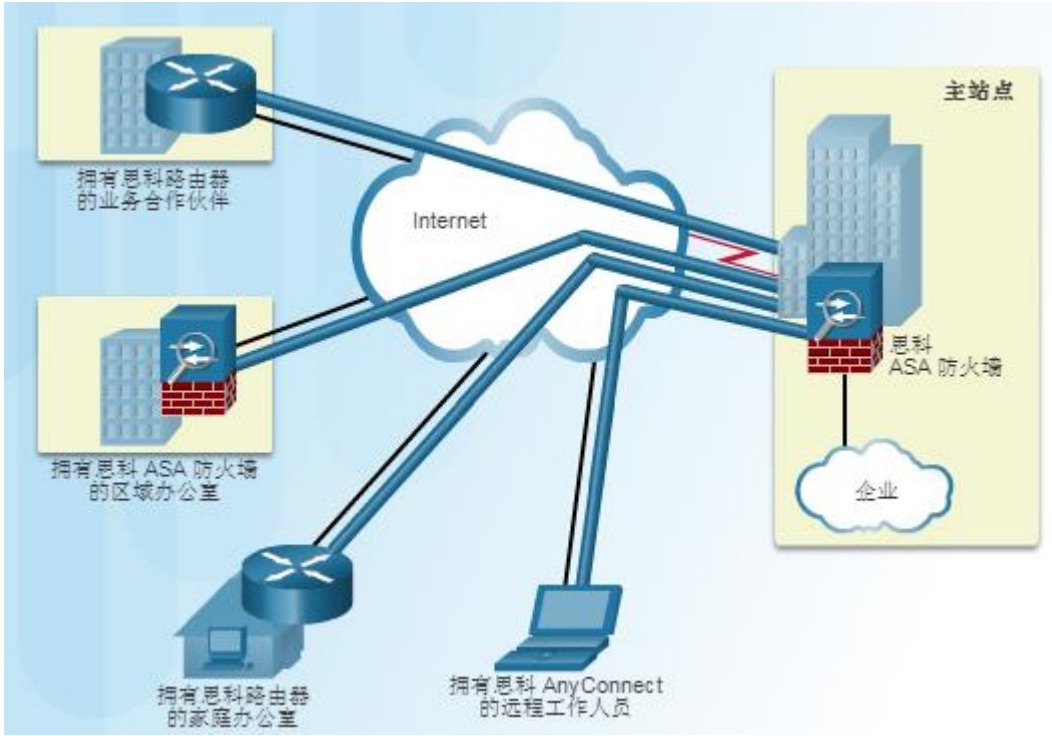


25 VPN 和 IPSec 概念

25.1 VPN Technology
VPN技术

VPN技术
Virtual Private Networks

- 组织使用 VPN 通过第三方网络（例如 Internet）来创建端到端专用网络连接。
- 目前，加密 VPN（例如 IPsec VPN）的安全实施通常通过虚拟专用网络来实现。
- 要实施 VPN，必须使用 VPN 网关。VPN 网关可以是路由器、防火墙或思科自适应安全设备 (ASA)。

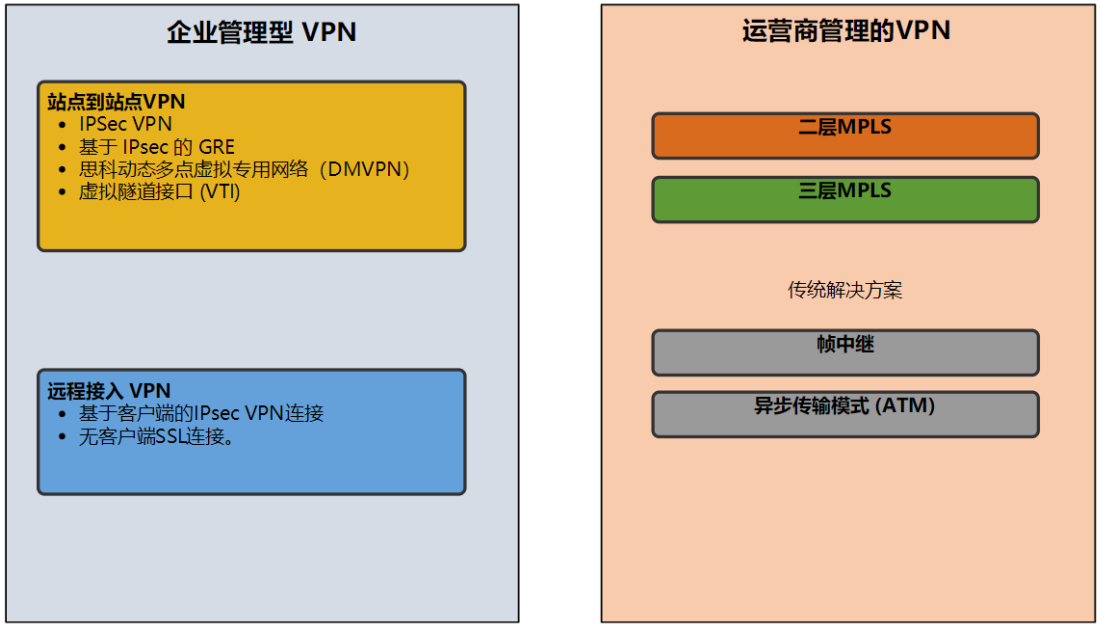


VPN 优点

- 节省成本 - VPN 使组织能够使用经济有效的第三方 Internet 传输将远程办公室和远程用户连接到主站点；因而无需使用昂贵的专用 WAN 链路和大量调制解调器。
- 可扩展性 - VPN 使组织能够在 ISP 和设备内使用 Internet 基础设施，从而轻松添加新用户。因此，组织可以在不增加重大基础设施的情况下增添大量功能。
- 与宽带技术的兼容性 - VPN 允许移动员工和远程工作人员使用高速宽带连接（例如 DSL 和电缆）来访问其组织的网络。宽带连接可同时提供灵活性和效率。高速宽带连接还可为连接远程办公室提供经济有效的解决方案。
- 安全性 - 通过使用高级加密和身份验证协议，VPN 可以保护数据免遭未授权访问，从而加入可提供最高级别安全性的安全机制。

企业和ISP VPNs

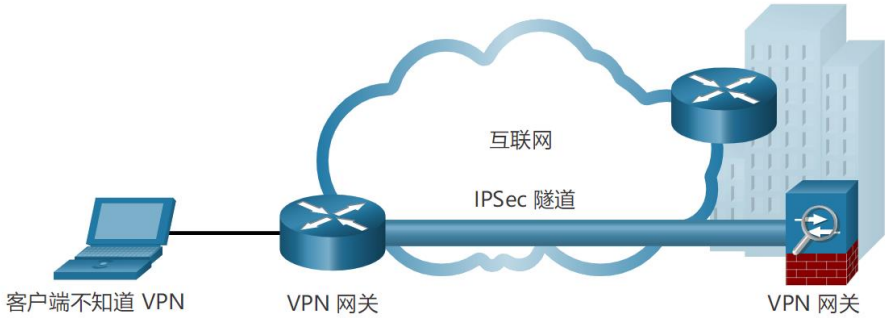
- **Enterprise VPNs** -用于保Internet上的企业通信安全的通用解决方案。站点到站点和远程访问VPN由企业使用IPsec和SSL VPN创建和管理。.
- **Service Provider VPNs** -由运营商创建和管理。提供商在第2层或第3层使用多协议标签交换（MPLS）在企业站点之间创建安全通道，有效地将流量与其他客户流量隔离。



VPN类型

Site-to-Site IPsec VPNs

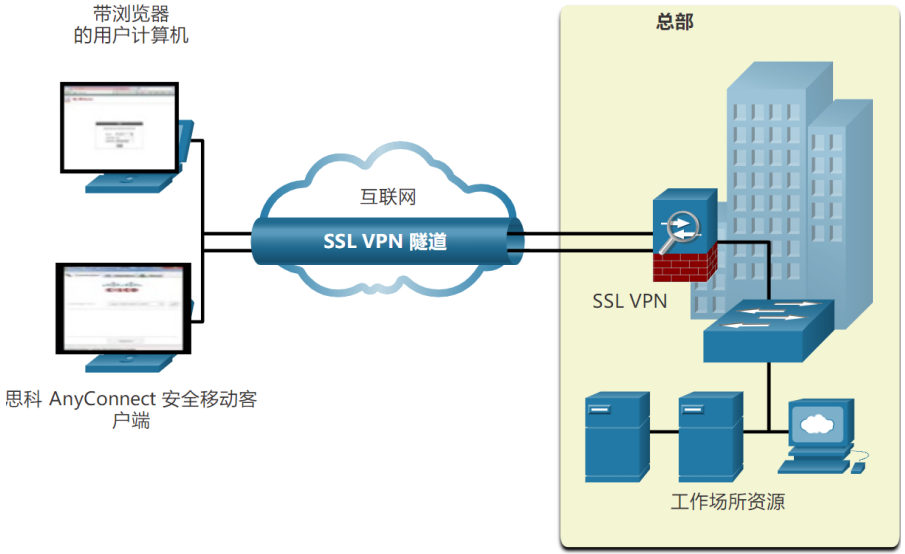
- 站点到站点VPN通过不受信任的网络（如Internet）连接网络。
- 终端主机通过VPN网关发送和接收正常的未加密TCP/IP通信。
- VPN网关封装并加密来自站点的出站流量，并通过VPN隧道将流量发送到目标站点的VPN网关。
- 接收VPN网关剥离报头，解密内容，并将数据包转发到其专用网络内的目标主机。



VPN类型

Remote-Access VPNs

- 远程访问VPN允许远程和移动用户安全地连接到企业。
- 远程访问VPN通常由用户在需要时动态启用，可以使用IPsec或SSL创建.
  - **Clientless VPN connection** -使用web浏览器SSL连接实现安全.
  - **Client-based VPN connection** -必须在远程用户的终端设备上安装VPN客户端软件，如Cisco AnyConnect安全移动客户端.



VPN类型

SSL VPNs

当客户端与 VPN 网关协商 SSL VPN 连接时，实际上它会使用 TLS（传输层安全）进行连接。TLS 是 SSL 的较新版本，有时表示为 SSL/TLS。

SSL使用公钥基础设施和数字证书来验证对等方。SSL根据用户的访问需求和组织的IT流程来实现的。

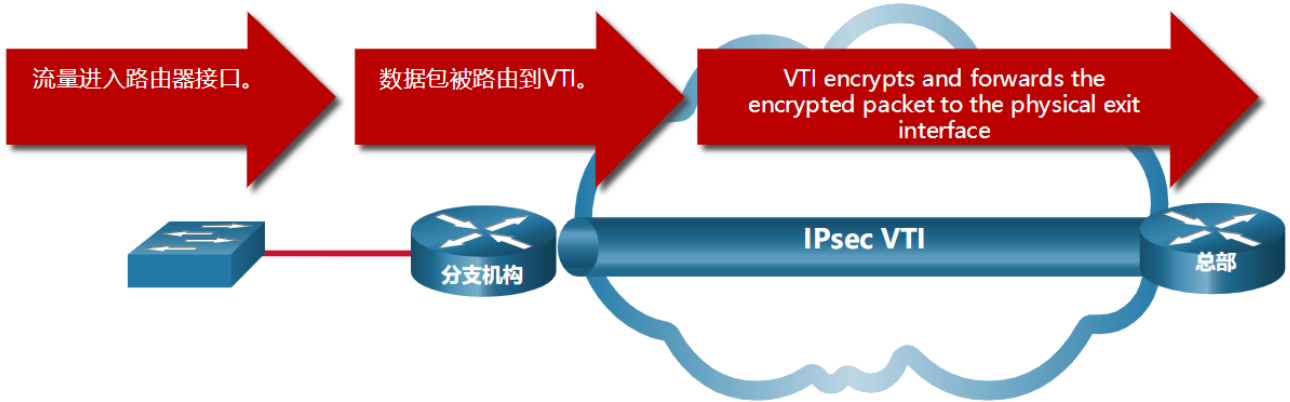
特性	IPSec	SSL
支持的应用	**广泛** - 支持基于所有 IP 的应用。	**有限** - 仅支持基于 Web 的应用和文件共享。 支持共享
认证强度	**强** - 进行双向认证，且使用共享密钥或数字证书。	**中** - 单向或双向认证。
加密强度	**强** - 密钥长度为 56 位到 256 位。	**中到强** - 密钥长度为 40 位到 256 位。
连接复杂性	**中** - 因为需要把 VPN 客户端 预安装在主机上。	**低** - 只需要主机上具有 Web 浏览器。
连接选项	**有限** - 只有拥有特定设备且拥有特殊配置才可以连接。	**广泛** - 任何拥有 Web 浏览器的设备均可以 进行连接。

VPN类型

IPsec Virtual Tunnel Interface虚拟隧道接口

IPsec虚拟隧道接口(VTI)简化了支持多个站点和远程访问所需的配置过程.

- IPsec VTI配置应用于虚拟接口，而不是将IPsec会话静态映射到物理接口。
- IPsec VTI能够发送和接收IP单播和多播加密流量。因此，自动支持路由协议，而无需配置GRE隧道。
- 可以在站点之间或在中心和分支拓扑中配置IPsec VTI。

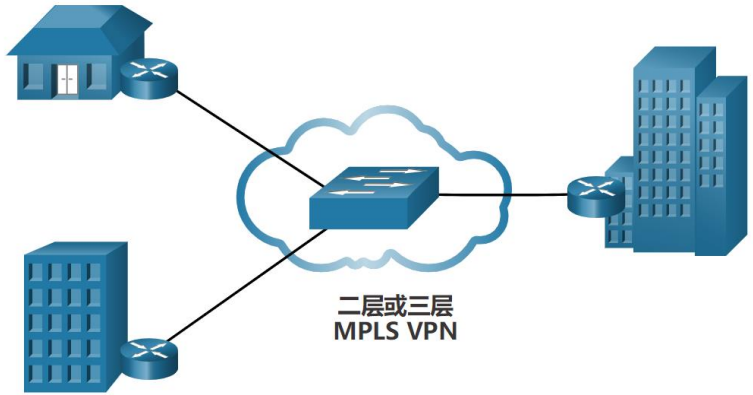


VPN类型

Service Provider MPLS VPNs

服务提供商在其核心网络中使用MPLS。流量使用标签通过MPLS骨干网转发。因服务提供商隔离客户的流量而使得数据传输是安全的。

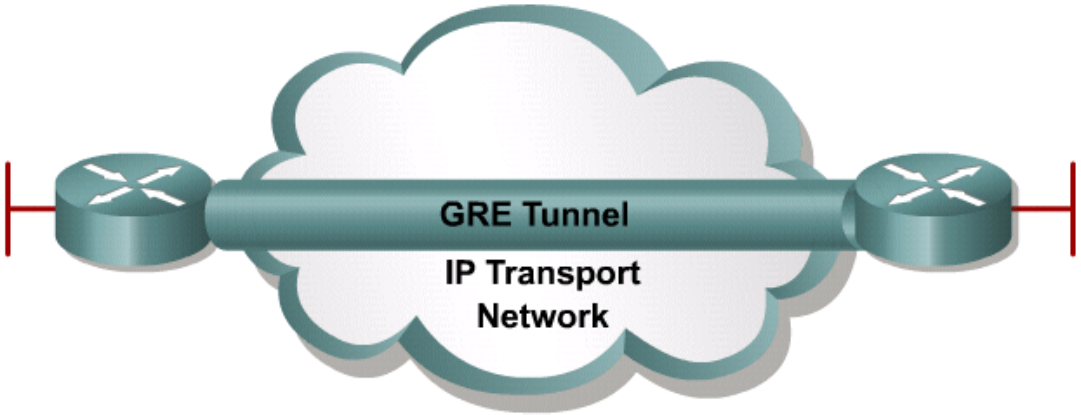
- 保护客户端站点之间的通信是服务提供商的责任.
  - **Layer 3 MPLS VPN** -服务提供商通过在客户的路由器和提供商的路由器之间运行路由协议来传递客户的路由。
  - **Layer 2 MPLS VPN** -服务提供商不参与客户路由。提供商部署一个虚拟专用局域网服务（VPLS）来模拟MPLS网络上的以太网段。由于不涉及路由，所以用户的路由器实际上属于同一个多路访问网络。



25.2 GRE VPNs

VPN类型

GRE over IPsec

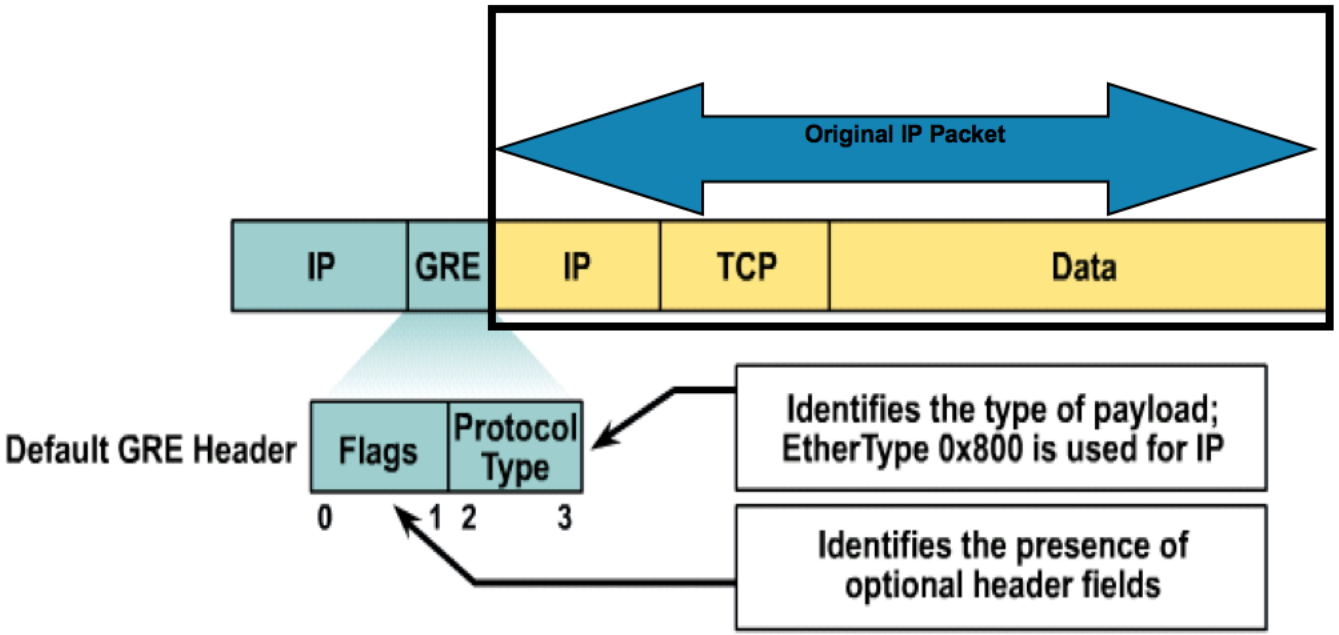


- GRE被定义为**IETF标准**。
- IP用**协议号47**来标识GRE数据包。
- GRE**支持任何**OSI**第3层协议**的封装。
- GRE协议本身是**无状态**的，它默认情况下不包括任何流量控制机制。
- GRE**没有**任何有力的**安全机制**来保护其有效载荷
- GRE报头和隧道IP报头一起，为隧道数据包添加了至少**24个字节**的**额外开销**。

VPN类型

GRE over IPsec

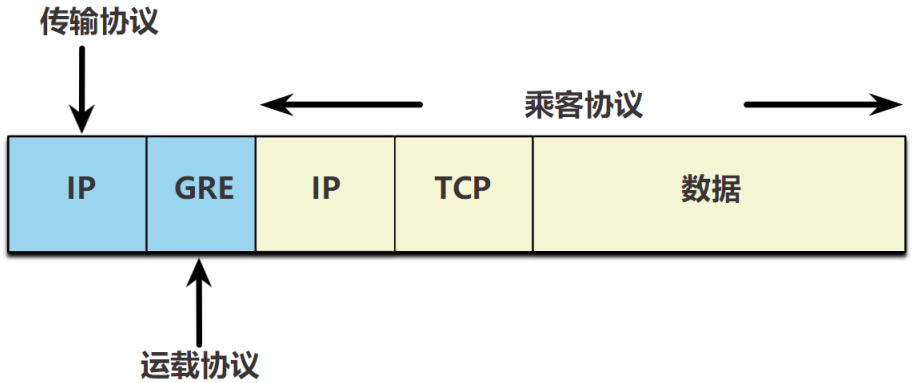
- 通用路由封装 (GRE) 用于管理两个或多个站点之间（可能只有 IP 连接）多协议和 IP 组播流量的传输。
- 使用 GRE 的 IP 隧道允许跨单协议主干环境扩展网络。



GRE over IPsec (Cont.)

隧道接口支持以下各项的报头：

- 被封装的协议（或乘客协议），例如 IPv4、IPv6
- 封装协议（或运载协议），例如 GRE
- 传输交付协议（例如 IP），该协议用于传输经过封装的协议

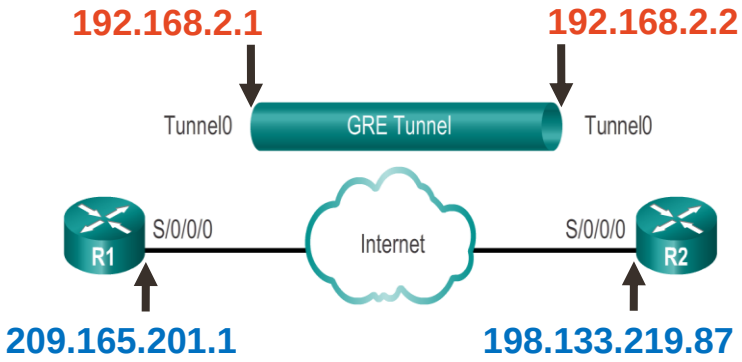


GRE over IPsec (Cont.)

- **第 1 步：**使用 **interface tunnel number** 命令创建隧道接口。
- **第 2 步：**配置隧道接口的 IP 地址。这通常是私有 IP 地址。
- **第 3 步：**指定隧道源 IP 地址。
- **第 4 步：**指定隧道目标 IP 地址。
- **第 5 步：**（可选）将 GRE 隧道模式指定为隧道接口模式。

命令	说明
`tunnel mode gre ip`	指定隧道接口模式为基于 IP 的 GRE。
`tunnel source` *ip_address*	指定隧道源地址。
`tunnel destination` *ip address*	指定隧道目的地址。
`ip address` *ip address mask*	指定隧道接口的 IP 地址。

GRE over IPsec (Cont.)




```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

GRE over IPsec (Cont.)

验证 GRE

- 要确定隧道接口已启用还是关闭，可使用 **show ip interface brief** 命令。
- 要验证 GRE 隧道的状态，可使用 **show interface tunnel** 命令。
- 使用 **show ip ospf neighbor** 命令验证已通过隧道接口建立了 OSPF 邻接关系。

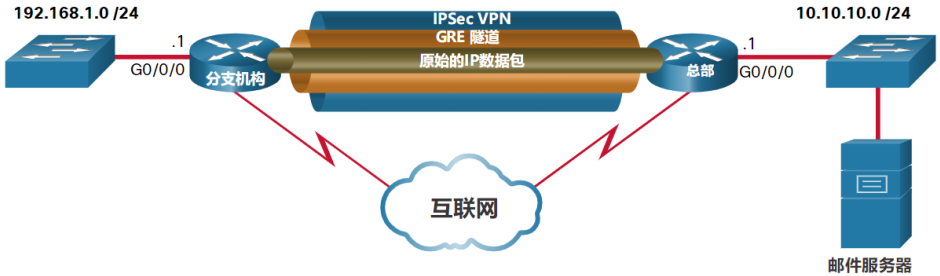
GRE 故障排除

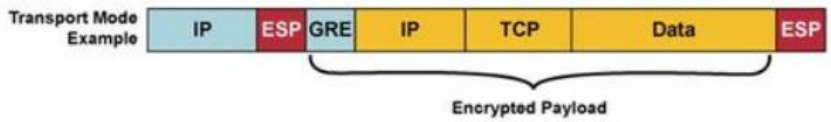
- 同时在两台路由器上使用 **show ip interface brief** 命令，以验证隧道接口已启用，并且已使用物理接口和隧道接口的正确 IP 地址进行了配置。
- 使用 **show ip ospf neighbor** 命令验证邻接关系。
- 使用 **show ip route** 验证网络在两台路由器之间传输

GRE over IPsec (Cont.)

标准的 IPsec VPN（非 GRE）只可以为单播流量创建安全隧道。因此路由协议无法通过 IPsec VPN 来交换路由信息。 为了解决这个问题，我们可以使用 GRE 包来封装路由协议流量，然后将这个 GRE 包封装到 IPsec 包中，并将其安全地转发到目的地 VPN 网关。

分支和总部需要通过IPsec VPN交换OSPF路由信息。GRE over IPsec用于支持IPsec VPN上的路由协议流量。具体地说，OSPF分组（即乘客协议）将被GRE（即运营协议）封装并随后封装在IPsec VPN隧道中。





25.3 IPsec

IPsec 技术

IPsec是IETF标准，它定义了如何用VPN保护IP网络上的通信。IPsec保护和认证源和目标之间的IP包，并提供这些基本的安全功能:

- 机密性（Confidentiality）：用加密算法进行数据加密
- 数据完整性（Data Integrity）:检验在传输中数据是不是被改变，如果检测到篡改，则数据包被丢弃。
- 验证（Authentication）：检验发送数据源的身份，确保连接是由希望的通信伙伴发起的。
- 抗重放保护：检测和拒绝重放的数据包，并有助于防止欺骗（跟踪数据包序列号）。
- Diffie-Hellman:安全的key交换

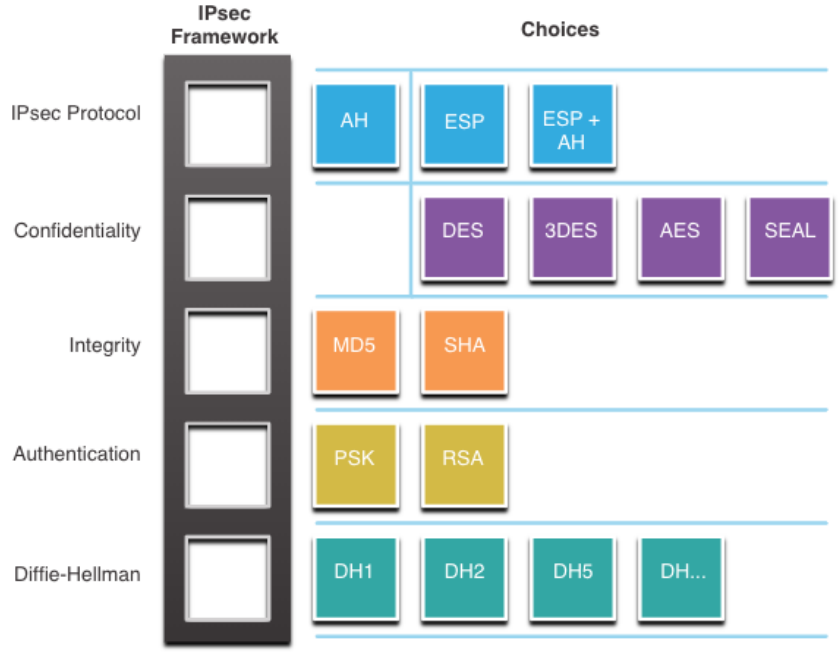
Confidentiality

Data Integrity

Authentication

IPsec Technologies (Cont.)

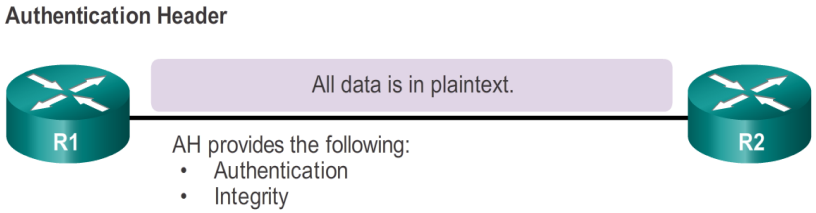
- IPsec未绑定到实现安全通信的任何特定规则。
- IPsec可以很容易地集成新的安全技术，而无需更新现有的IPsec标准。
- IPsec框架中可以填充可用的任何选项来创建唯一安全关联（SA）。



IPsec 封装协议

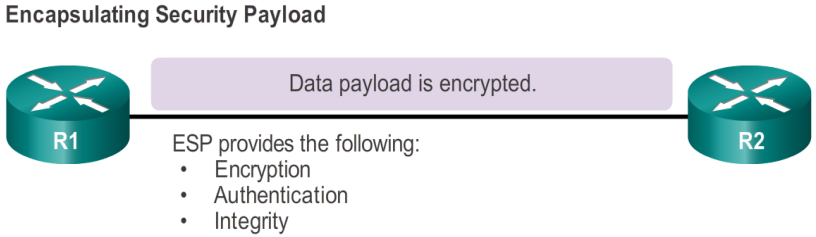
认证头 (AH) - Authentication Header

- 在不需要或不允许加密的情况下可以适合的协议。
- 提供两个系统间的IP数据包头的验证和完整性。
- 不提供数据包的数据机密性（加密）。



封装安全载荷 (ESP) - Encapsulating Security Payload

- 通过加密IP数据包提供机密性和验证的安全协议。
- 验证内部IP数据包和ESP头。
- 在ESP中加密和验证都是可选的，但是最少要选一个。



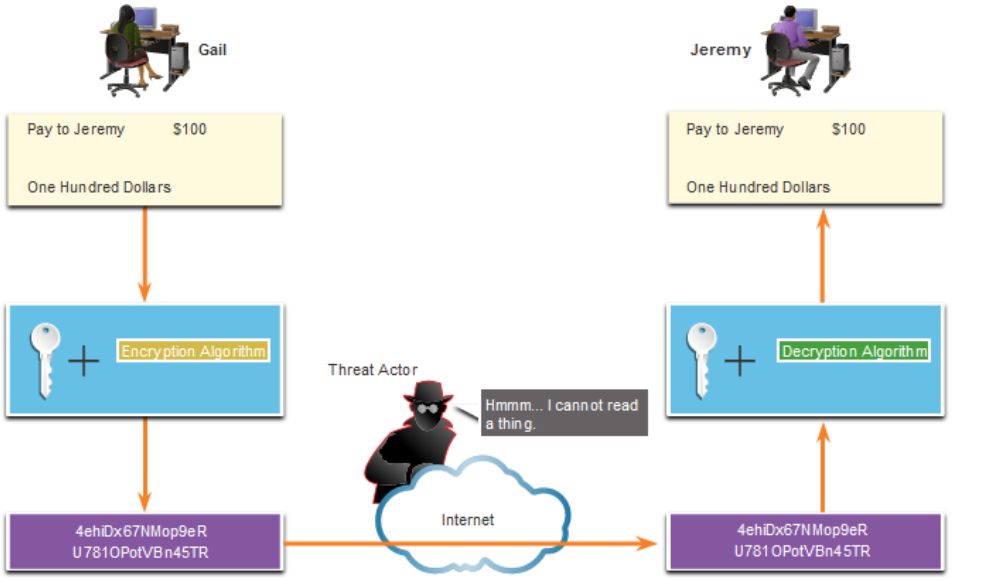
IPSec

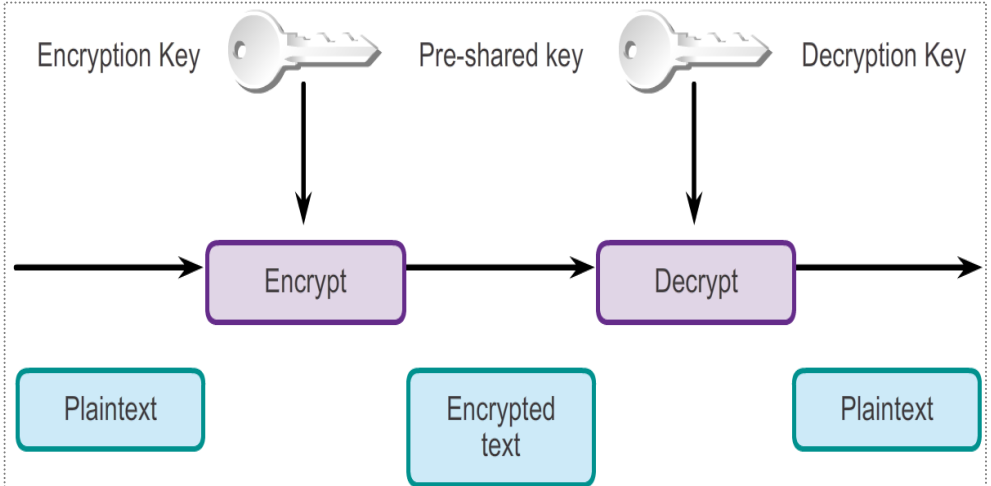
加密

保密程度取决于加密算法和加密算法中使用的密钥长度。钥匙越短就越容易被破解。

对称加密：

- 加密和解密使用**相同的秘钥**。
- 两个网络设备都要知道秘钥来解码信息。
- **通常**用于对**消息的内容**进行加密。（很少使用非对称加密来加密用户信息）
- 代表算法： **DES** (不再被认为是安全的)
  - **3DES** (不再被认为是安全的)
  - **AES** (IPsec 加密时推荐使用256比特）
  - SEAL（流加密）



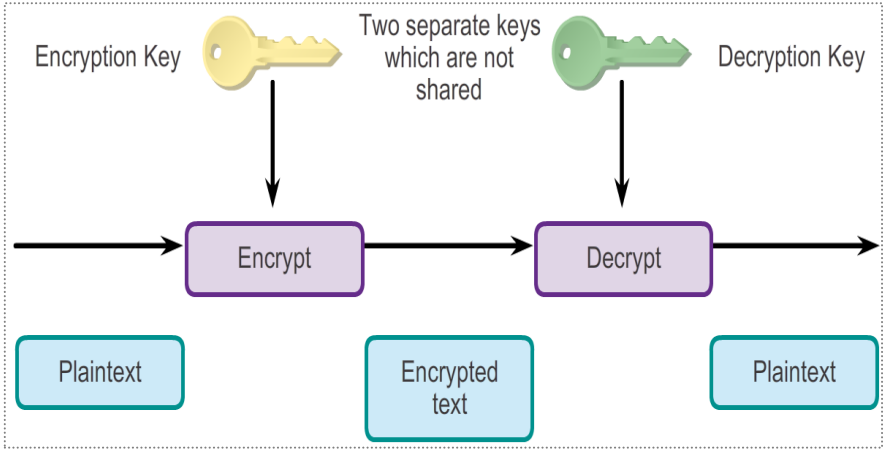


IPSec

加密

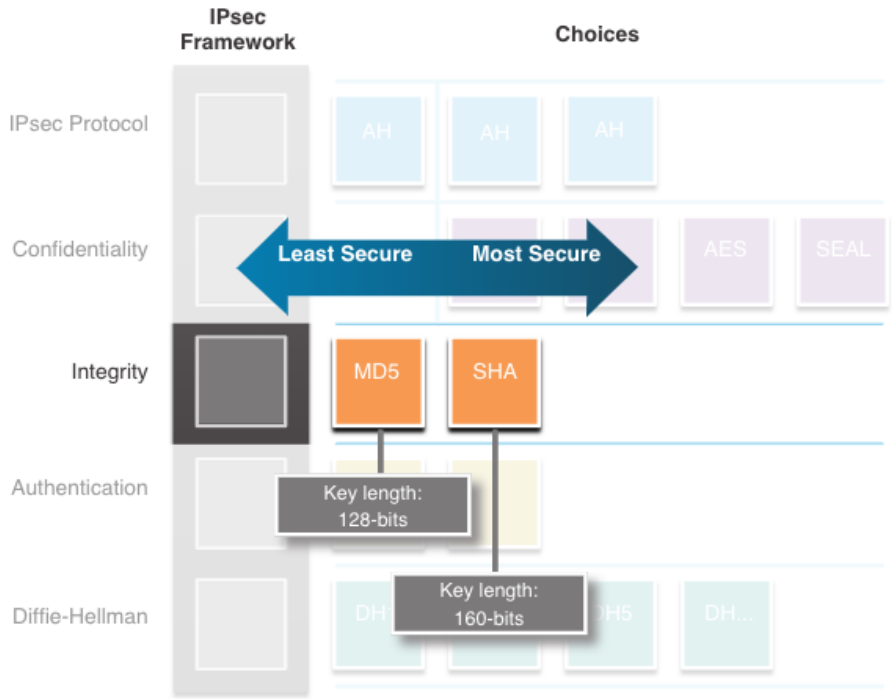
非对称加密：

- 加密和解密使用**不同的秘钥**。
- 知道一个秘钥不能破解第二个秘钥也不能解码信息。
- **一个秘钥加密**的信息，只有**第二个秘钥可以解密**。
- 公开秘钥加密是非对称加密的一种变体，它使用**私有秘钥**（private key ）和**公开秘钥**（public key）的一对组合。
- 典型的应用是**数字签名**和**秘钥管理**。
- 代表算法： **RSA**

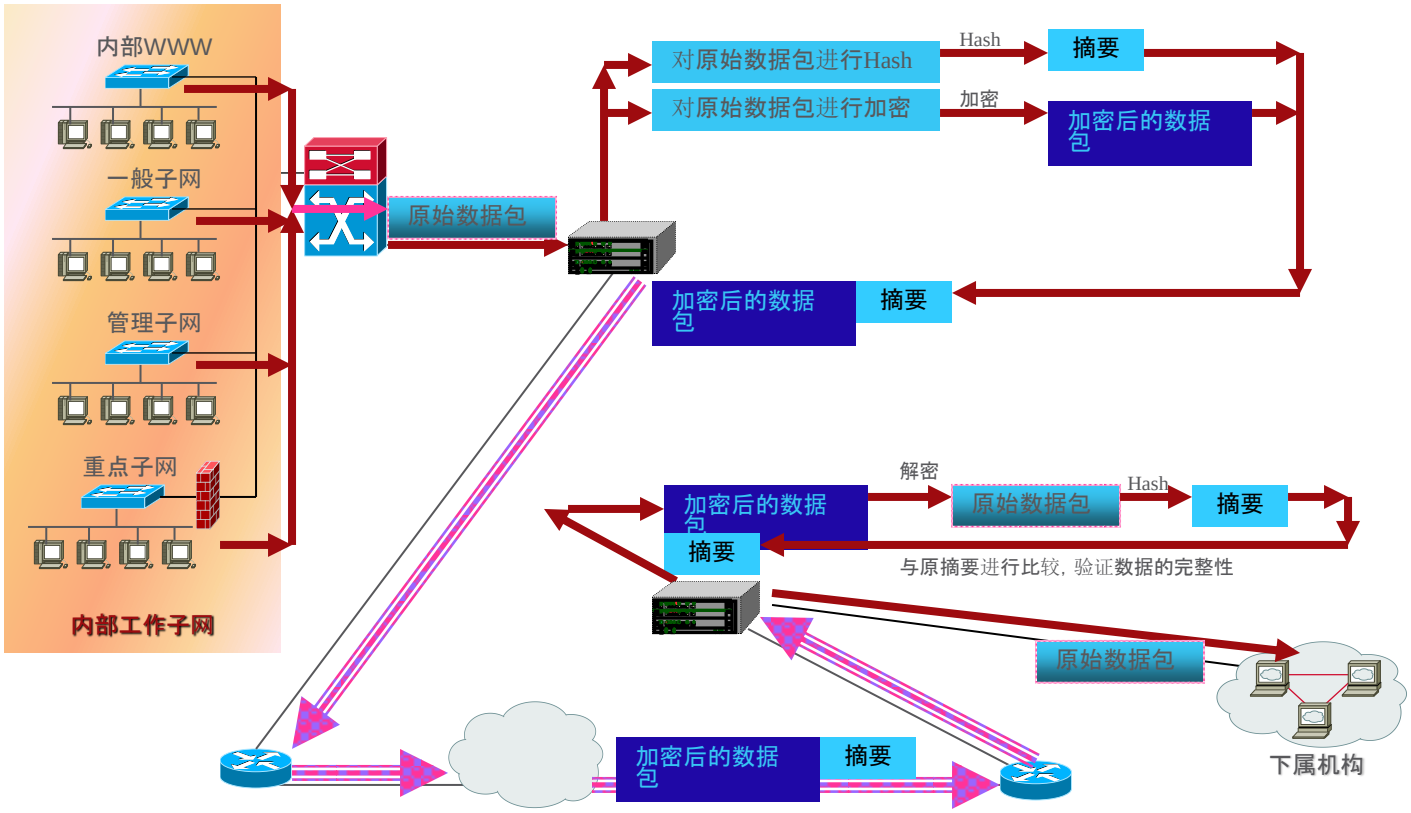


IPSec
Integrity

- 数据完整性意味着数据在传输过程中没有变化。
- 需要一种证明数据完整性的方法。
- 哈希消息身份验证代码(HMAC)是一种数据完整性算法，它使用哈希值保证消息的完整性。
- 消息摘要5(MD5)使用128位共享密钥。安全哈希算法(SHA)使用160位密钥。
- SHA2:SHA-256、SHA-384和SHA-512



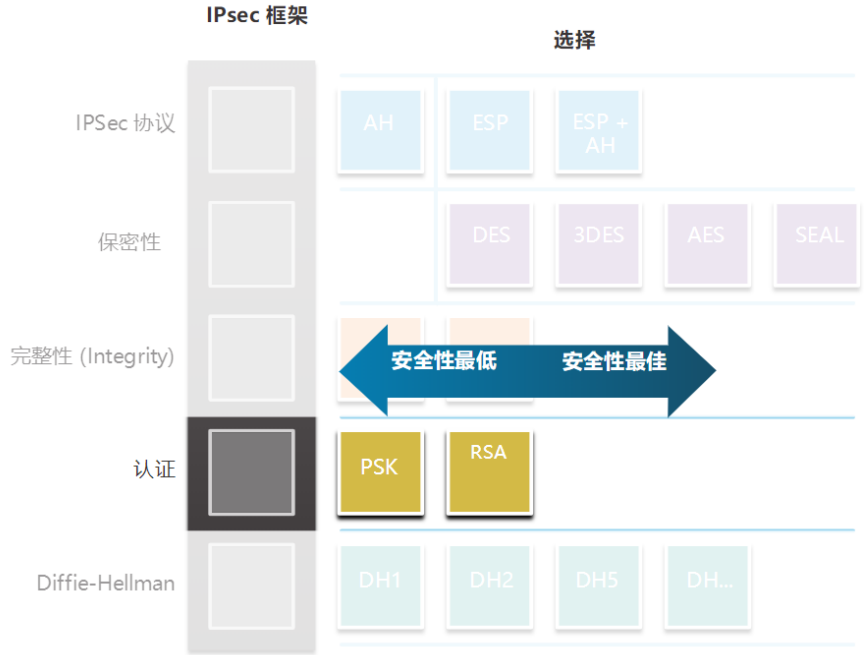
IPSec
Integrity



IPSec
Authentication

有两个对等身份验证的方法：

- **PSK - 在使用安全通道前，双方需要共享一个私有秘钥。**
- **RSA signatures - 交换数字证书来验证对方。**



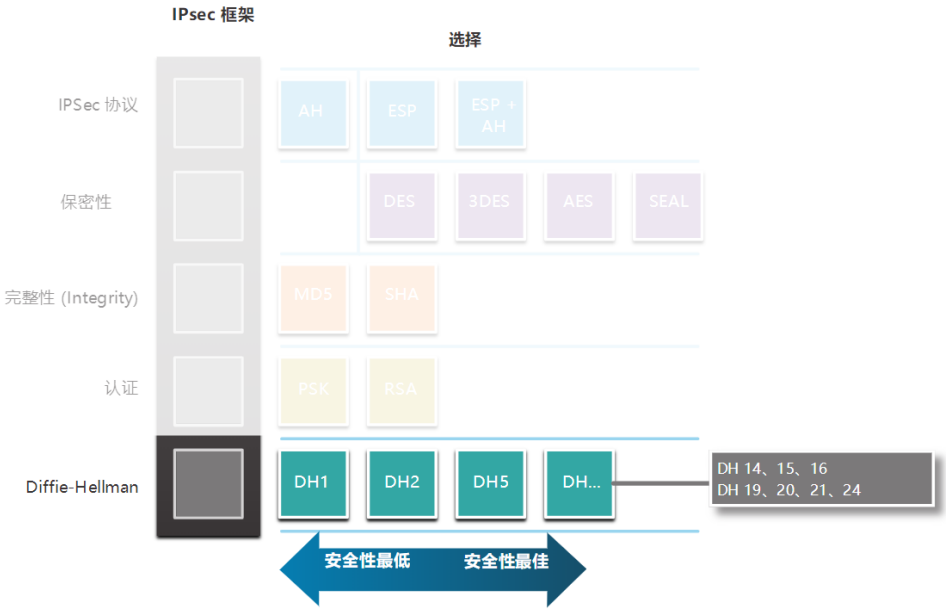
Secure Key Exchange with Diffie - Hellman

DH不是一个加密机制，一般不用来加密数据。

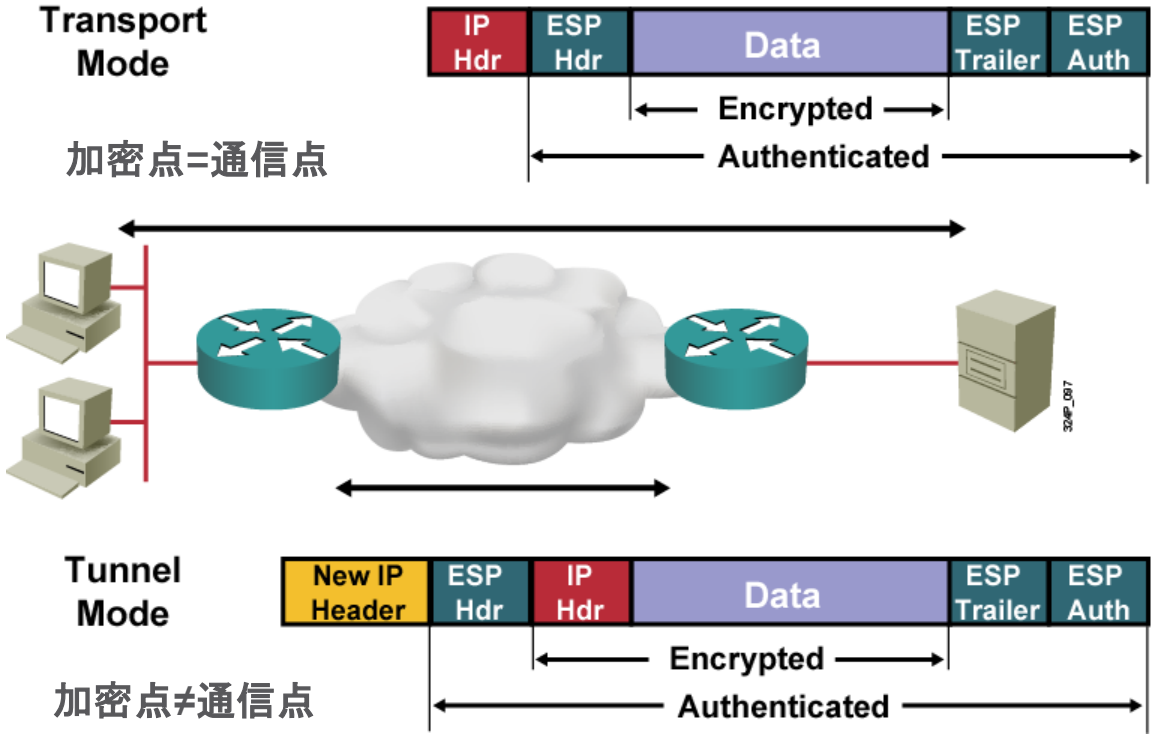
DH主要是用来在不安全的通道上安全的交换加密数据的共享秘钥。

DH groups:

- 不应再使用DH组1、2和5。
- DH组14、15和16分别使用2048位、3072位和4096位的较长密钥。
- DH组19、20、21和24各自的密钥大小分别为256位、384位、521位和2048位，它们支持椭圆曲线加密（ECC），这减少了生成密钥所需的时间。

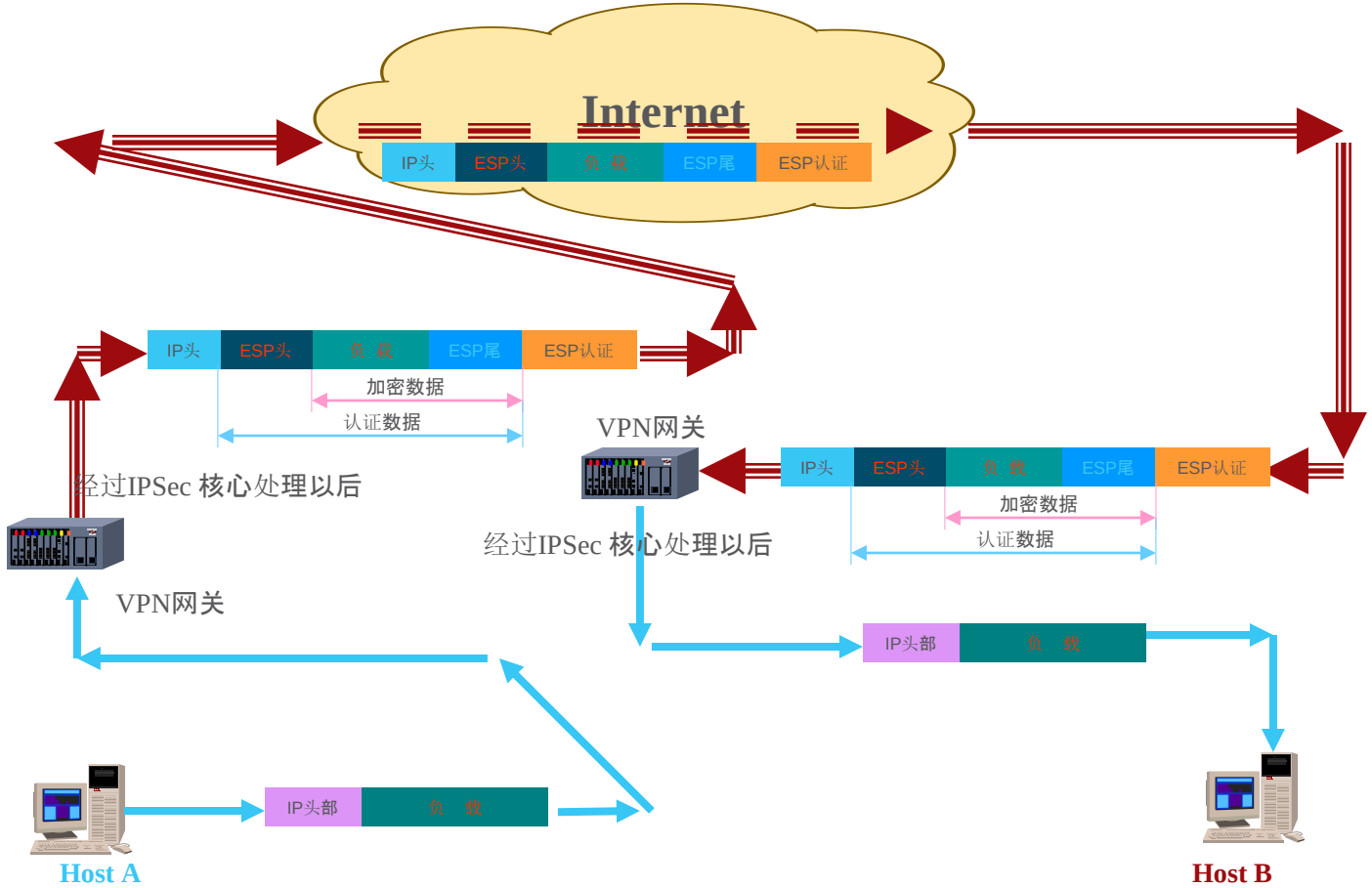


IPsec 工作模式

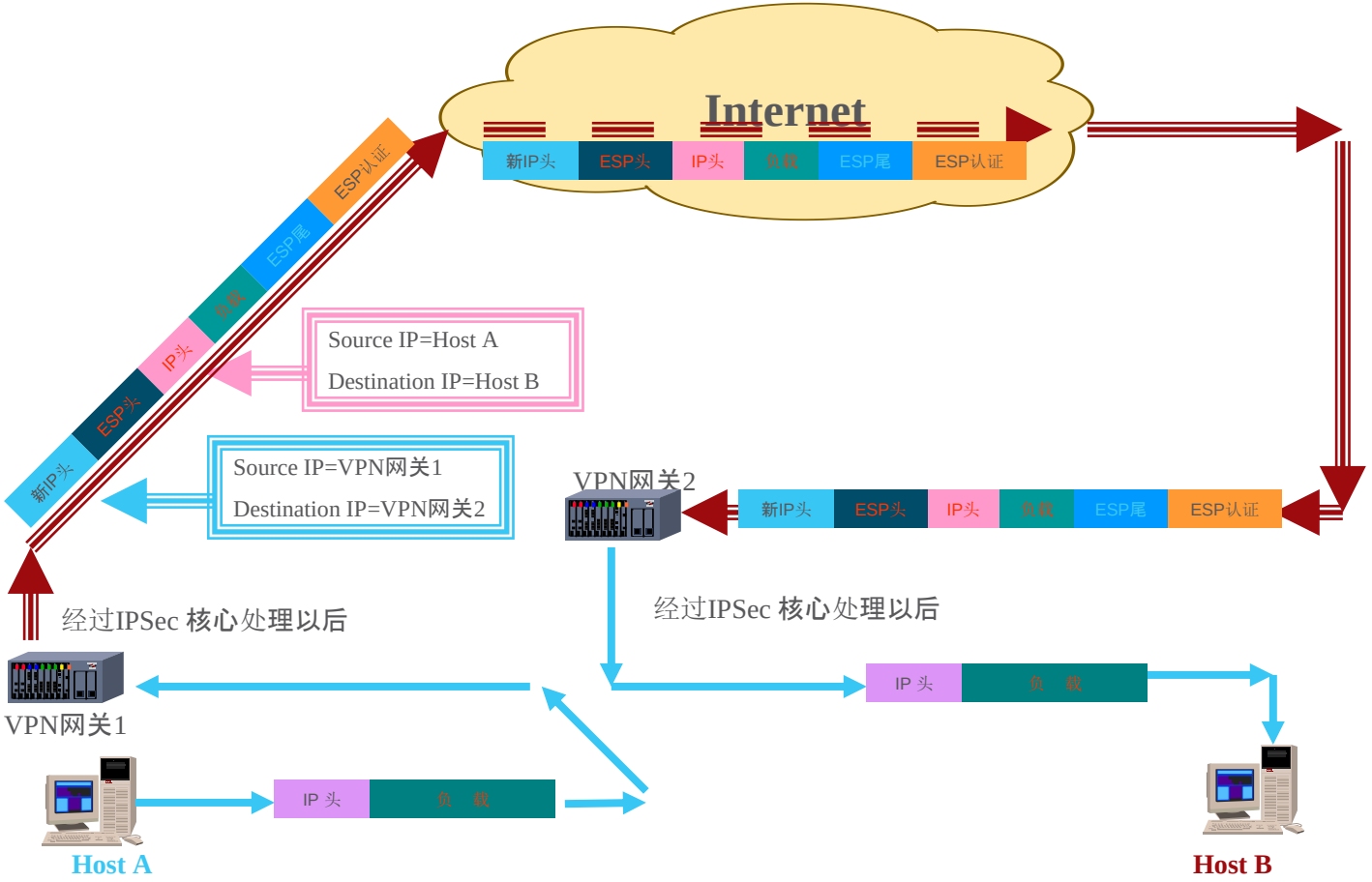

Transport Mode
IP Hdr
ESP Hdr
Data
ESP Trailer
ESP Auth
Encrypted
Authenticated
加密点=通信点
32#P_097
Tunnel Mode
New IP Header
ESP Hdr
IP Hdr
Data
ESP Trailer
ESP Auth
Encrypted
Authenticated
加密点≠通信点

IPsec

传输模式下的ESP认证工作原理



隧道模式下的ESP认证工作原理



IPsec 操作5步

1. Host A sends interesting traffic to Host B.

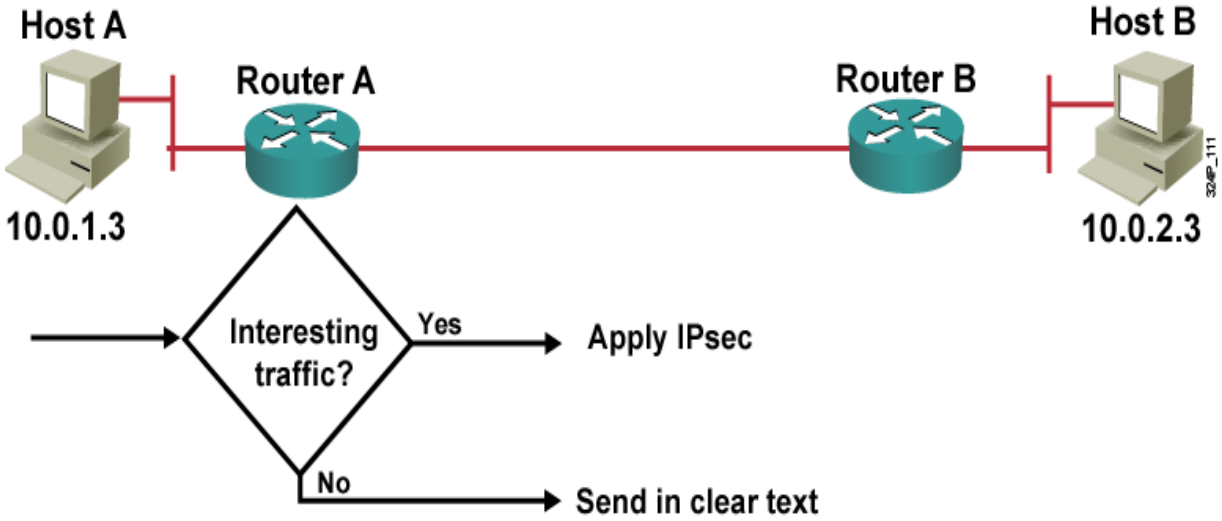
2. Routers A and B negotiate an IKE Phase 1 session.

3. Routers A and B negotiate an IKE Phase 2 session.

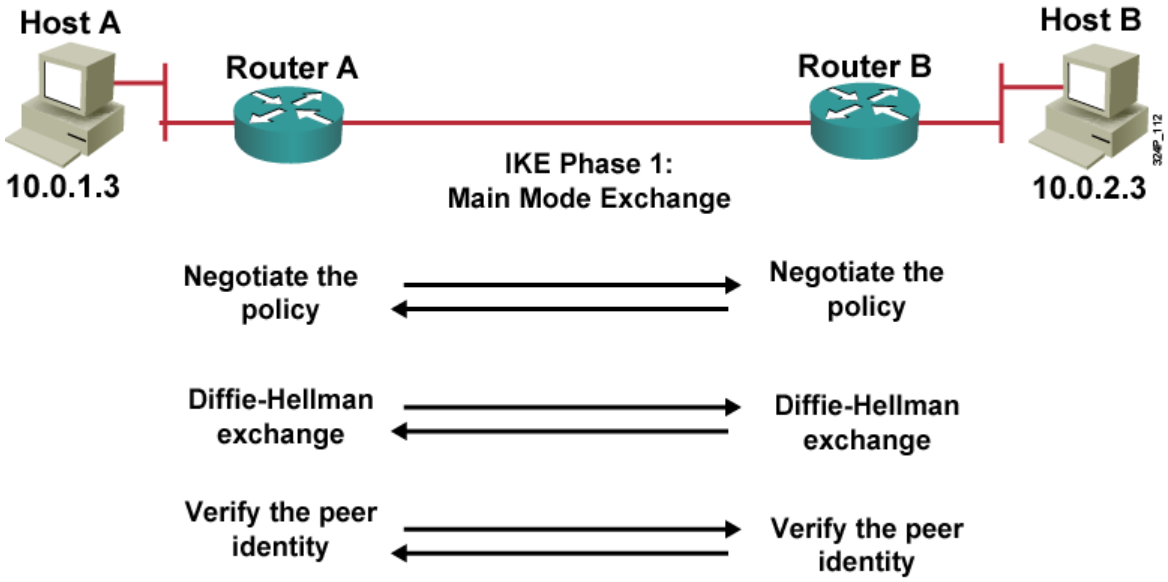
4. Information is exchanged via the IPsec tunnel.

5. The IPsec tunnel is terminated.

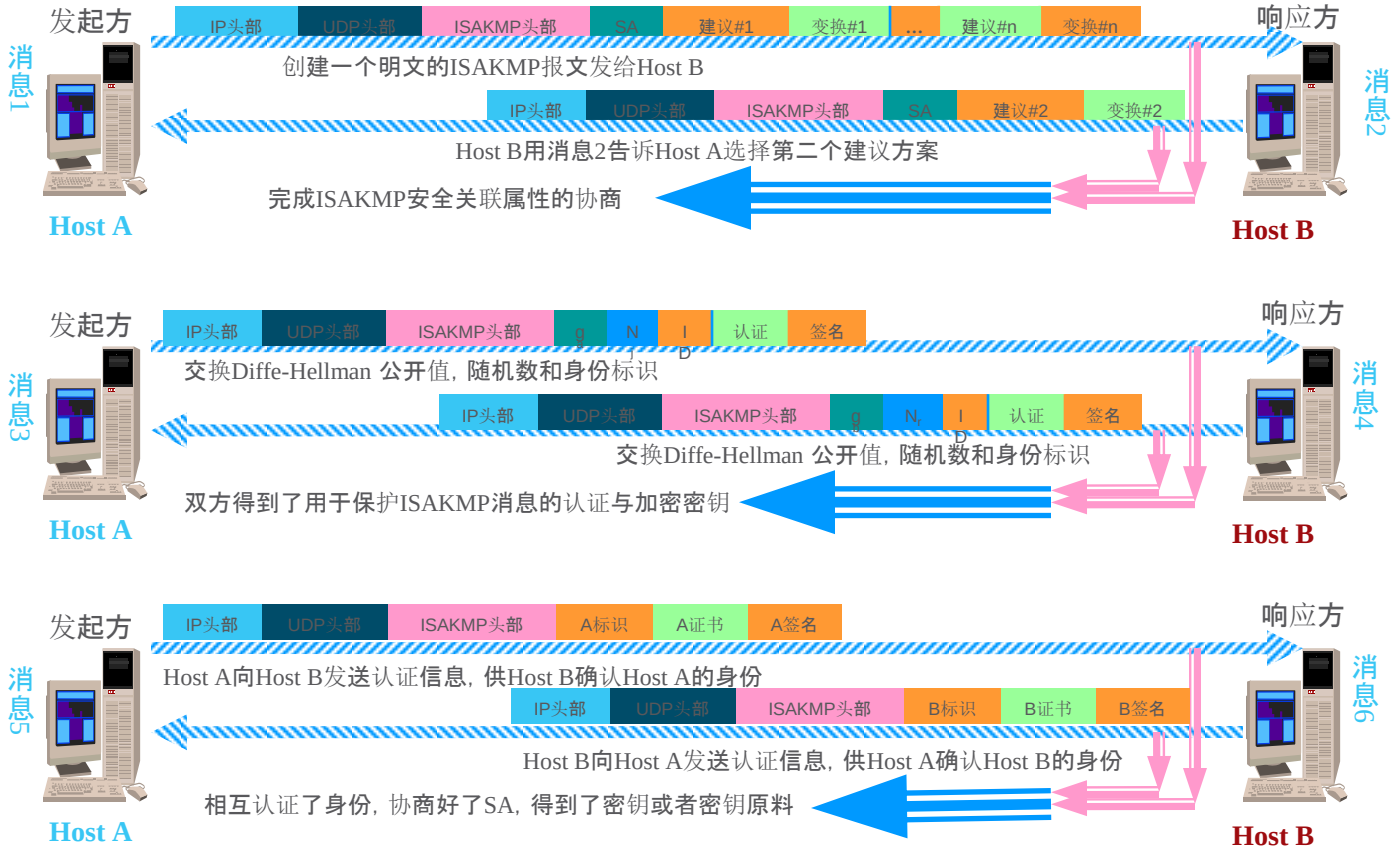
IPsec 操作1：定义感兴趣流量



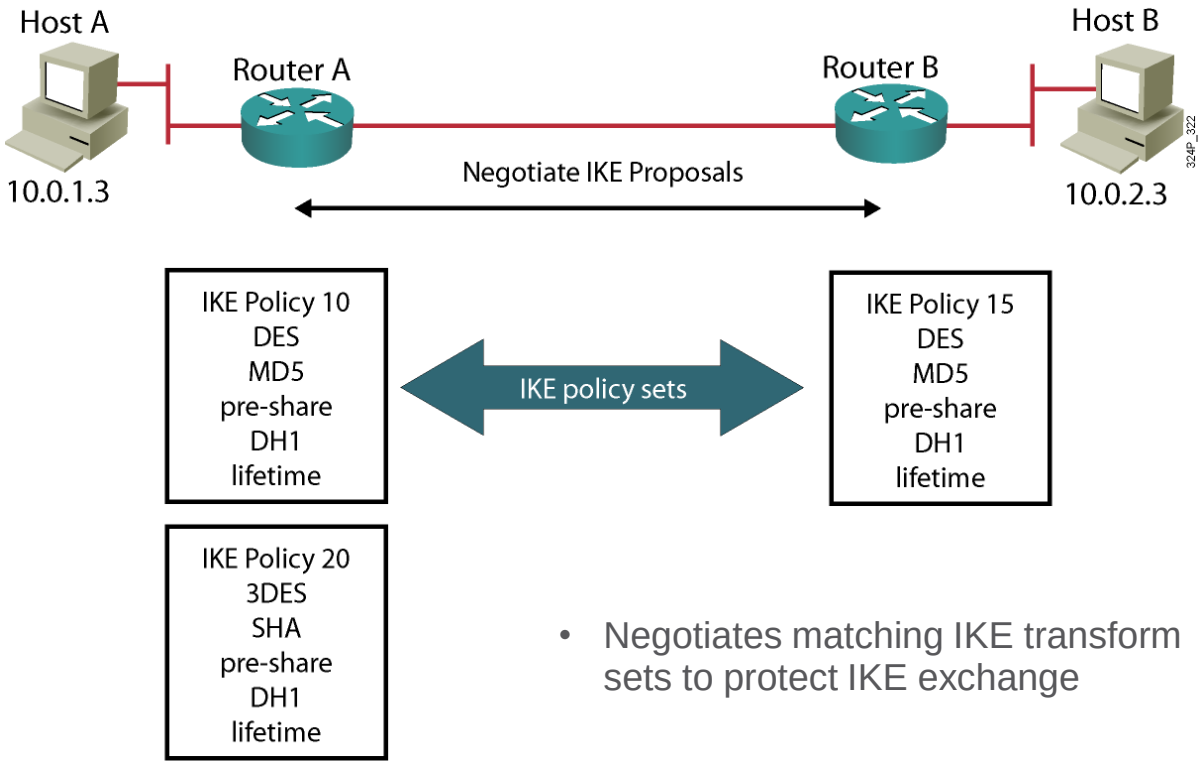
IPsec 操作2：IKE阶段1



IPsec 操作2：IKE阶段1工作过程



IPsec 操作2：IKE阶段1-IKE策略协商

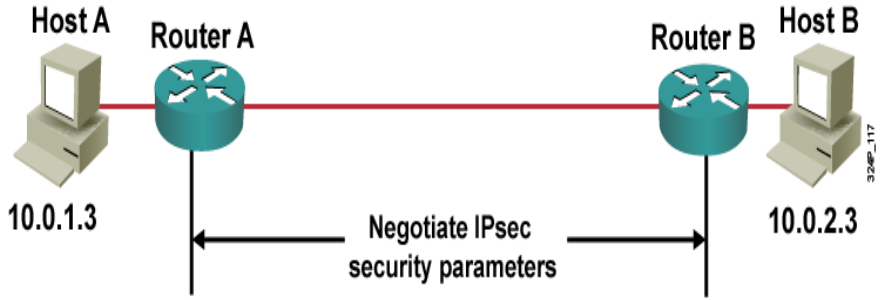


- Negotiates matching IKE transform sets to protect IKE exchange

IPsec 操作2：IKE阶段1-验证对端

- 对端验证**方法**:
  - Preshared keys：预**共享秘**钥
  - RSA signatures：RSA数字签名
  - RSA encrypted nonces：RSA加密随机数

IPsec 操作3：IKE阶段2



- 协商IPsec安全参数、IPsec转换集、建立IPsec SA、定期重新协商IPsec SA以确保安全，作为可选，执行额外的DH交换

IKE第二阶段：建立IPsec SA 协商的是以下信息：

1、双方使用哪种封装技术，AH还是ESP

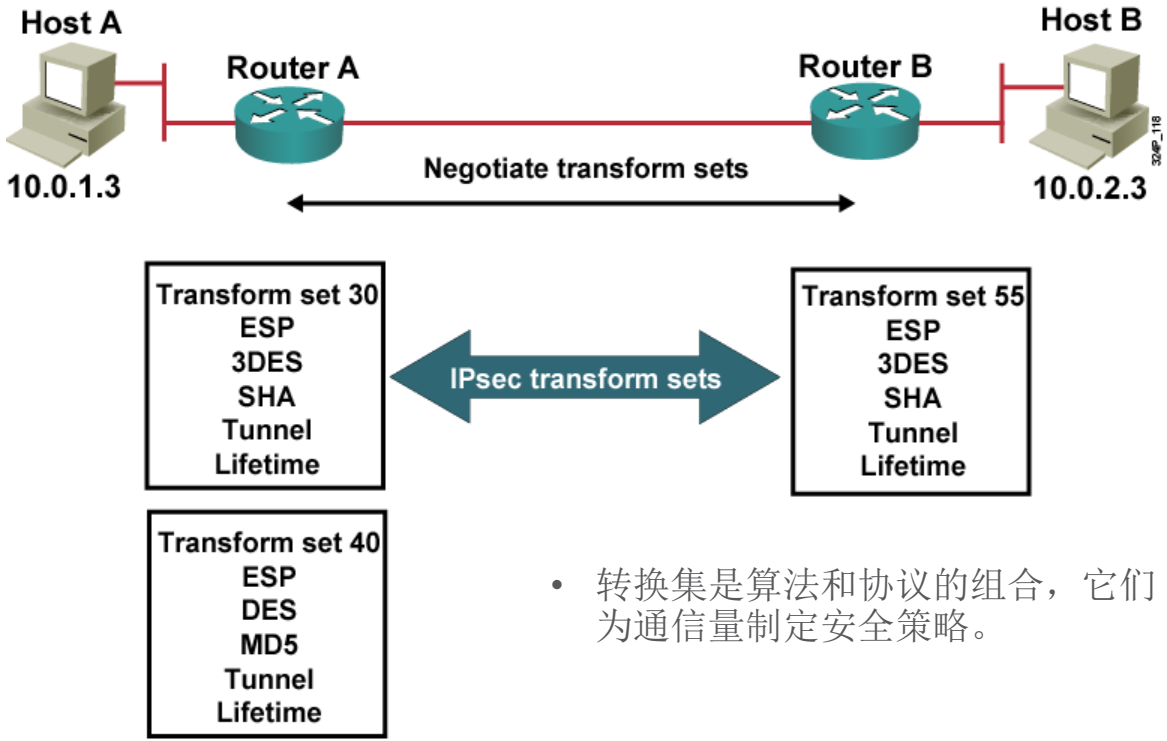
2、双方使用哪种加密算法

3、双方使用哪种HMAC方式，是MD5还是SHA

4、使用哪种传输模式，是隧道模式还是传输模式

5、还要协商SA的生存期

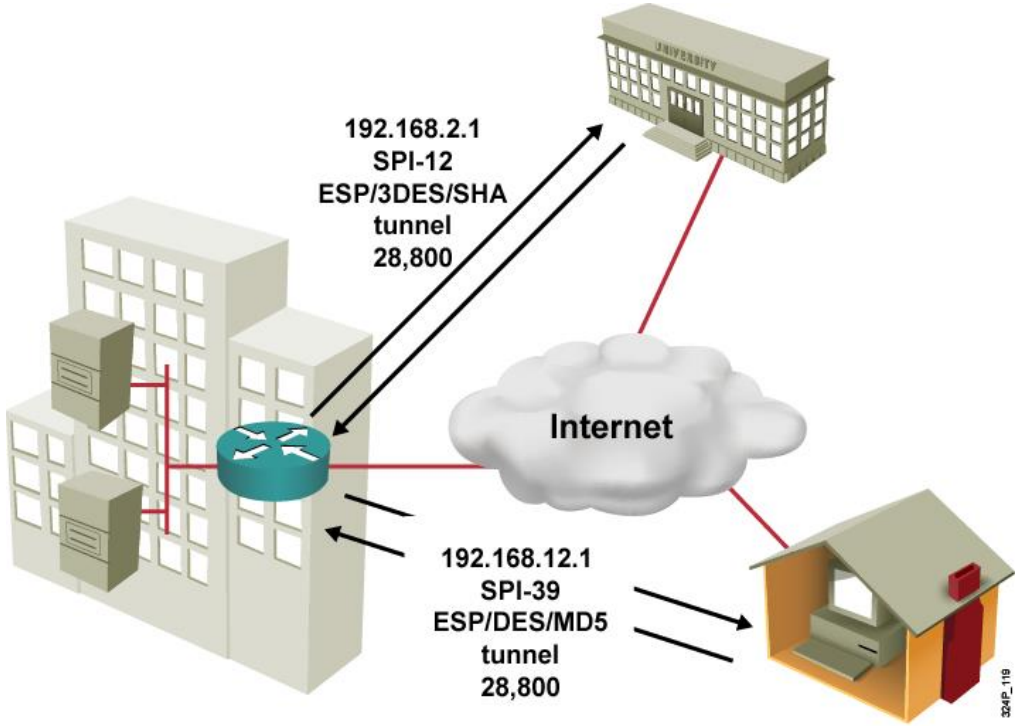
IPsec 操作3：IPSec转换集



- 转换集是算法和协议的组合，它们为通信量制定安全策略。

IPsec 操作3：Security Associations（安全关联）

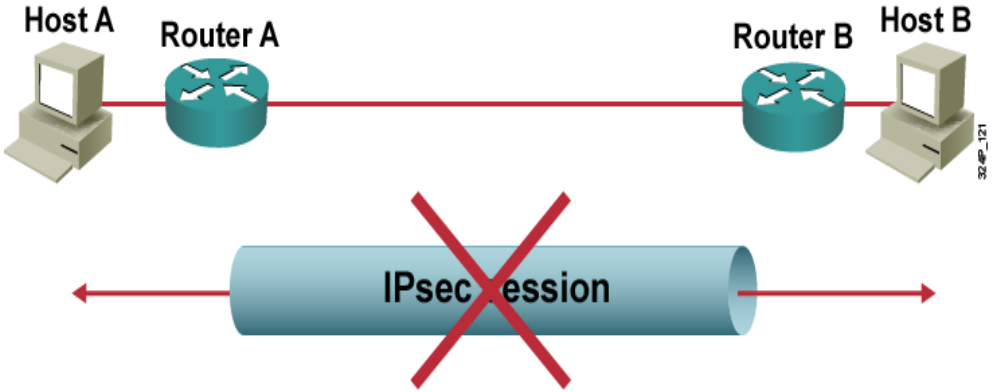
- SA database:
  - Destination IP address
  - SPI
  - Protocol (ESP or AH)
- Security policy database:
  - Encryption algorithm
  - Authentication algorithm
  - Key lifetime



IPsec 操作4： Ipsec会话

- SA在对等体之间交换，协商的安全服务应用于通信流量。

IPsec 操作5： IPSec隧道终止



- IPSec隧道由下列之一终止：
  - 通过SA生命周期超时
  - 超过了允许的数据包数量
  - IPSec隧道终止时IPsec SA被删除

Data transmitted-based

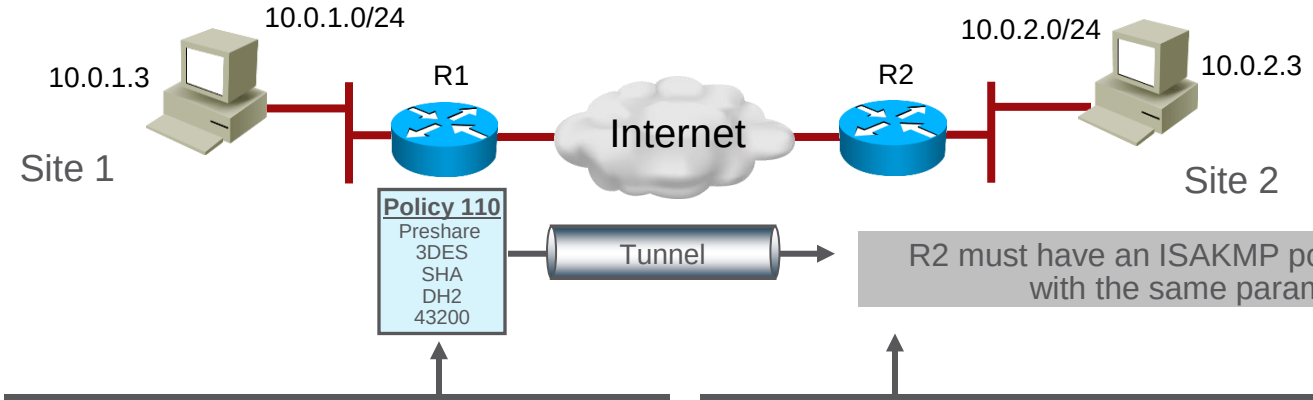
Time-based

IPsec VPN配置步骤

1. Establish ISAKMP policy
2. Configure IPsec transform set
3. Configure crypto ACL(Interesting Traffic)
4. Configure crypto map
5. Apply crypto map to the interface
6. Configure interface ACL

Task 1 Policy Negotiations

R1 attempts to establish a VPN tunnel with R2 and sends its IKE policy parameters



R2 must have an ISAKMP policy configured with the same parameters.

```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
```

```
R2(config)# crypto isakmp policy 100
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
```

ISAKMP Parameters

Parameter	Keyword	Accepted Values	Default Value	Description

`encryption`	`des`
	`3des`
	`aes`
	`aes 192`
	`aes 256`
		56-bit Data Encryption Standard
		Triple DES
		128-bit AES
		192-bit AES
		256-bit AES
			des	Message encryption algorithm

`hash`	`sha` `md5`	SHA-1 (HMAC variant) MD5 (HMAC variant)	**sha**	Message integrity (Hash) algorithm

`authentication`	`pre-share`
	`rsa-encr`
	`rsa-sig`
		preshared keys
		RSA encrypted nonces
		RSA signatures
			rsa-sig	Peer authentication method

`group`	`1`
	`2`
	`5`
		768-bit Diffie-Hellman (DH)
		1024-bit DH
		1536-bit DH
			1	Key exchange parameters (DH group identifier)

`lifetime`	*seconds*	Can specify any number of seconds	86,400 sec (one day)	ISAKMP-established SA lifetime

Multiple Policies

R1(config)#

```
crypto isakmp policy 100
        hash md5
 authentication pre-share
        !
crypto isakmp policy 200
        hash sha
  authentication rsa-sig
        !
crypto isakmp policy 300
        hash md5
 authentication pre-share
```

R2(config)#

```
crypto isakmp policy 100
        hash md5
 authentication pre-share
        !
crypto isakmp policy 200
        hash sha
  authentication rsa-sig
        !
crypto isakmp policy 300
        hash md5
  authentication rsa-sig
```

Task 2 Crypto ISAKMP Key

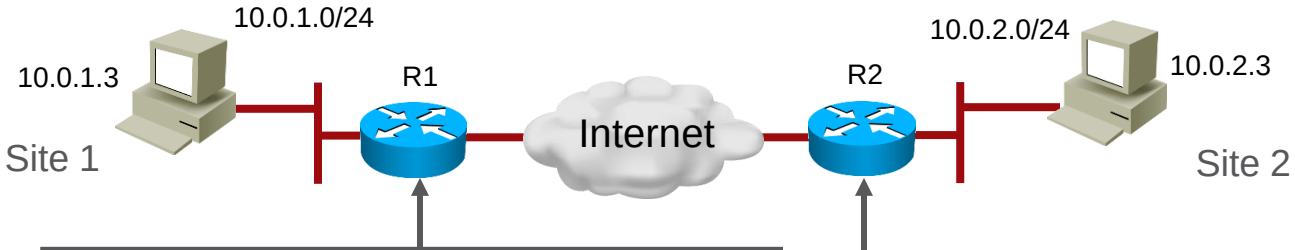
```
router(config)#
crypto isakmp key keystring address peer-address
```

```
router(config)#
crypto isakmp key keystring hostname hostname
```

Parameter	Description
keystring	This parameter specifies the PSK. Use any combination of alphanumeric characters up to 128 bytes. This PSK must be identical on both peers.
peer-address	This parameter specifies the IP address of the remote peer.
hostname	This parameter specifies the hostname of the remote peer. This is the peer hostname concatenated with its domain name (for example, myhost.domain.com).

- The *peer-address* or *peer-hostname* can be used, but must be used consistently between peers.
- If the *peer-hostname* is used, then the **crypto isakmp identity hostname** command must also be configured.

Sample Configuration




```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)#
```

```
R2(config)# crypto isakmp policy 110
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)#
```

Note:

- The keystring **cisco123** matches.
- The address identity method is specified.
- The ISAKMP policies are compatible.
- Default values do not have to be configured.

Task 3 Configure the Transform Set

- Overview
- Transform Sets
- Sample Configuration

Sample Configuration

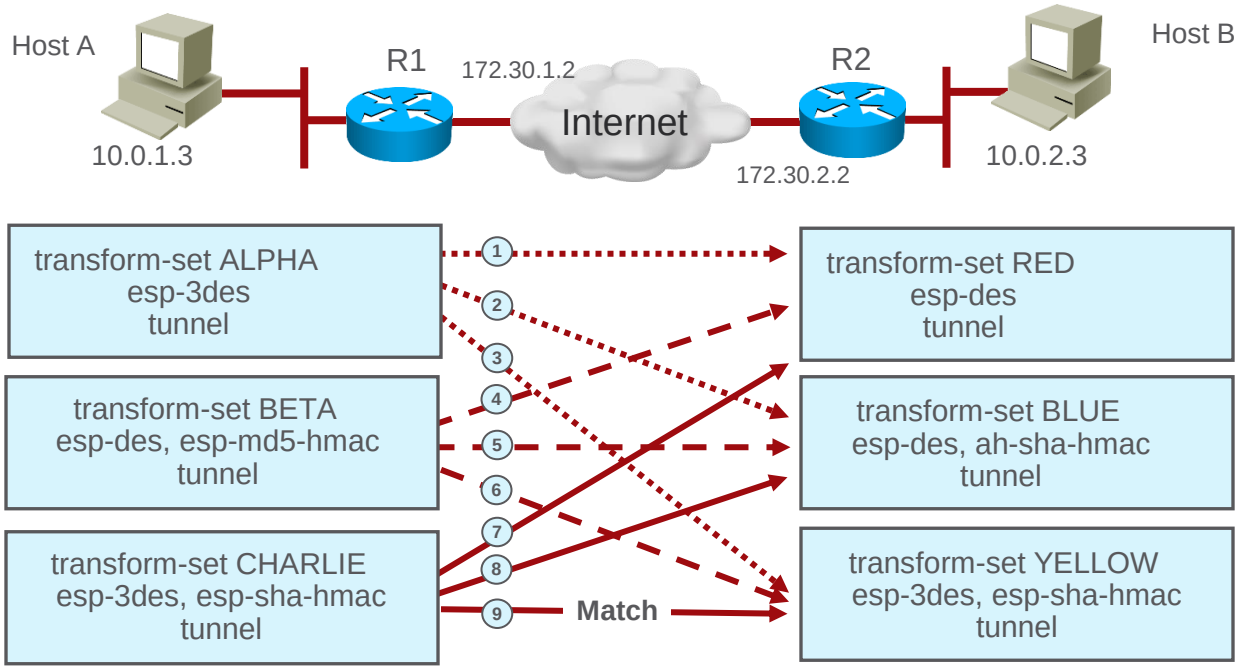

```
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)# crypto ipsec transform-set MYSET esp-aes 128
R1(cfg-crypto-trans)# exit
R1(config)#
```

```
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)#crypto ipsec transform-set OTHERSET esp-aes 128
R2(cfg-crypto-trans)# exit
```

Note:

- Peers must share the same transform set settings.
- Names are only locally significant.

Transform Sets

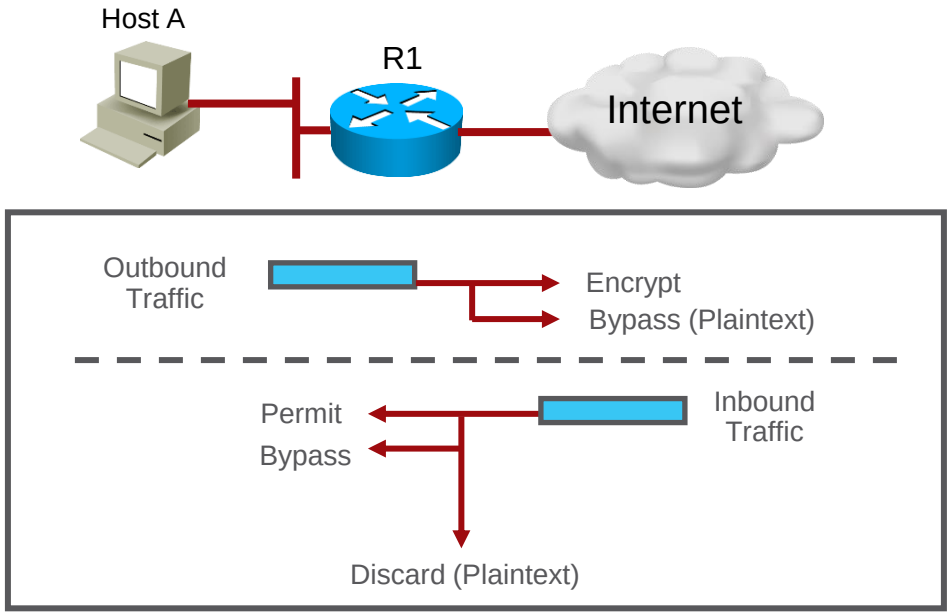


- Transform sets are negotiated during IKE Phase 2.
- The 9th attempt found matching transform sets (CHARLIE - YELLOW).

Task 4 Configure the Crypto ACLs

- Overview
- Command Syntax
- Symmetric Crypto ACLs

Overview



- Outbound indicates the data flow to be protected by IPsec.
- Inbound filters and discards traffic that should have been protected by IPsec.

Symmetric Crypto ACLs


```
Applied to R1 S0/0/0 outbound traffic:
R1(config)# access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255

(when evaluating inbound traffic- source: 10.0.2.0, destination: 10.0.1.0)
```

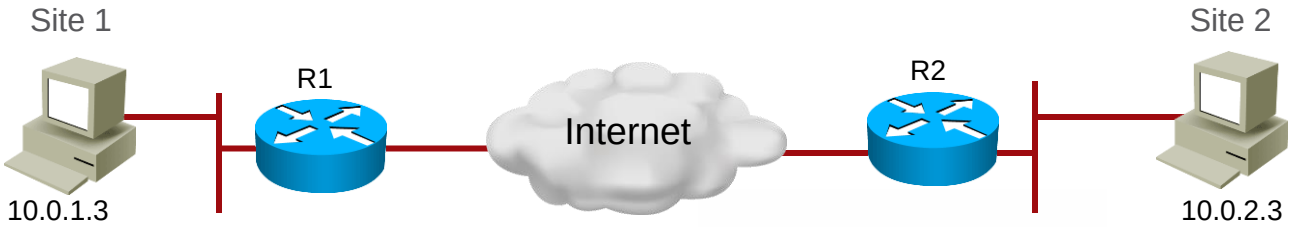
```
Applied to R2 S0/0/0 outbound traffic:
R2(config)# access-list 101 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255

(when evaluating inbound traffic- source: 10.0.1.0, destination: 10.0.2.0)
```

Task 5 Apply the Crypto Map

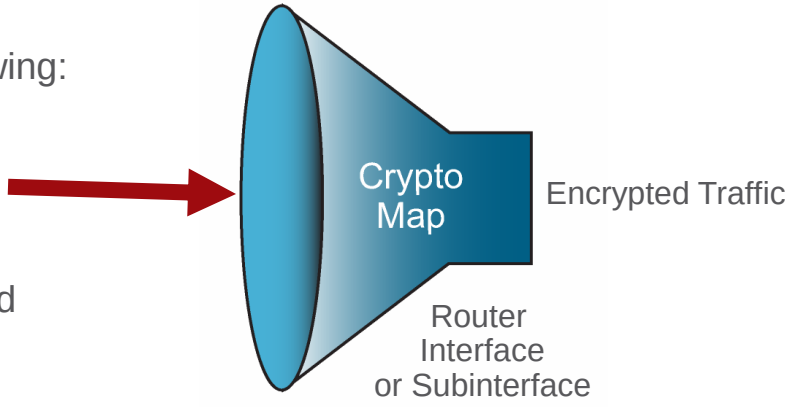
- Overview
- Crypto Map Command
- Crypto Map Configuration Mode Commands
- Sample Configuration
- Assign the Crypto Map Set

Overview

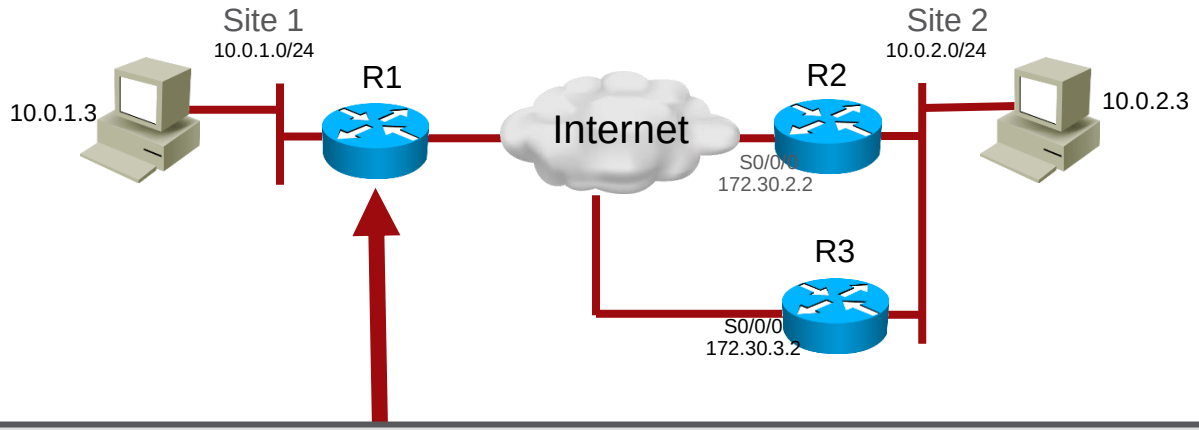


Crypto maps define the following:

- ACL to be used
- Remote VPN peers
- Transform set to be used
- Key management method
- SA lifetimes



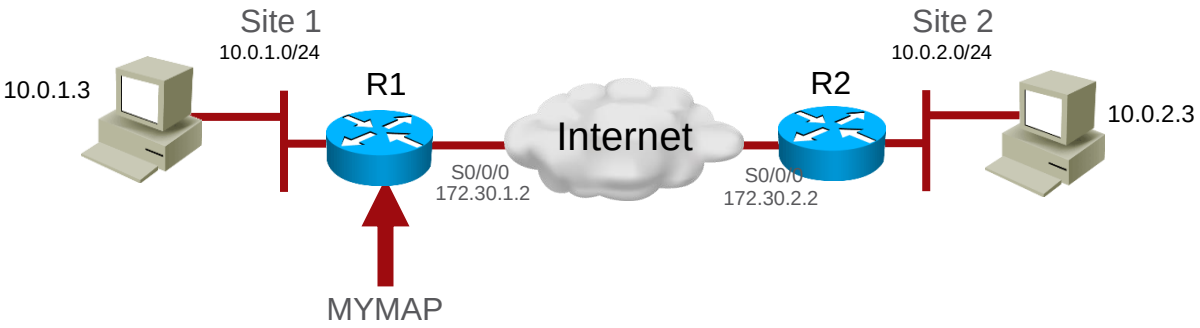
Sample Configuration




```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set mine
R1(config-crypto-map)# set security-association lifetime seconds 86400
```

Multiple peers can be specified for redundancy.

Assign the Crypto Map Set



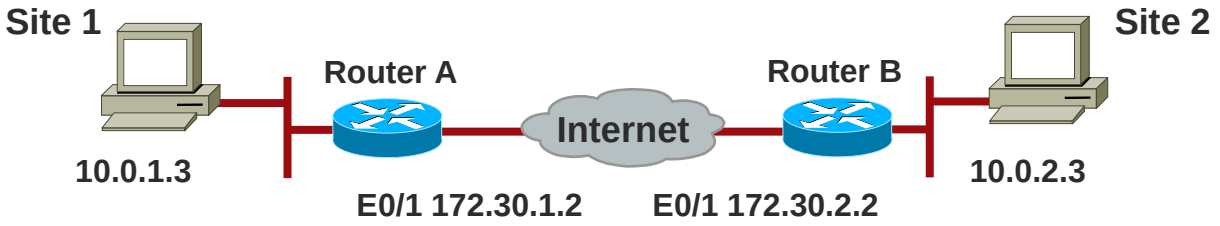
router(config-if)#

```
crypto map map-name
```

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map MYMAP
```

- Applies the crypto map to outgoing interface
- Activates the IPsec policy

配置实例




```
RouterA# show running config
crypto ipsec transform-set MINE esp-
des esp-md5-hmac
!
crypto map MYMAP 10 ipsec-isakmp
set peer 172.30.2.2
set transform-set MINE
match address 110
!
interface Ethernet 0/1
ip address 172.30.1.2 255.255.255.0
no ip directed-broadcast
crypto map MYMAP
!
access-list 110 permit tcp 10.0.1.0
0.0.0.255 10.0.2.0 0.0.0.255
```

```
RouterB# show running config
crypto ipsec transform-set MINE esp-
des esp-md5-hmac
!
crypto map MYMAP 10 ipsec-isakmp
set peer 172.30.1.2
set transform-set MINE
match address 101
!
interface Ethernet 0/1
ip address 172.30.2.2 255.255.255.0
no ip directed-broadcast
crypto map MYMAP
!
access-list 101 permit tcp 10.0.2.0
0.0.0.255 10.0.1.0 0.0.0.255
```

测试和验证IPSec

- Display your configured ISAKMP policies.

  show crypto isakmp policy

- Display your configured transform sets.

  show crypto ipsec transform-set

- Display the current state of your IPSec SAs.

  show crypto ipsec sa

  - Display your configured crypto maps.

    show crypto map

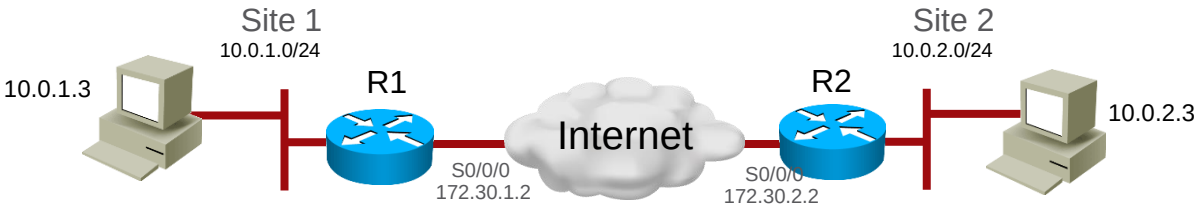
  - Enable debug output for IPSec events.

    debug crypto ipsec

  - Enable debug output for ISAKMP events.

    debug crypto isakmp

show crypto map



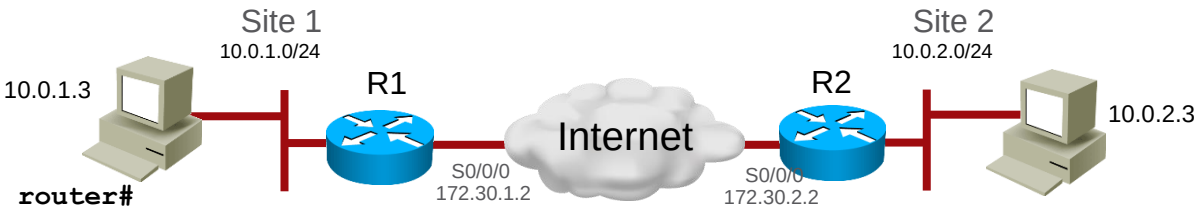

```
router#
```

```
show crypto map
```

Displays the currently configured crypto maps

```
R1# show crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
              Peer = 172.30.2.2
              Extended IP access list 110
                   access-list 102 permit ip host 10.0.1.3 host 10.0.2.3
              Current peer: 172.30.2.2
              Security association lifetime: 4608000 kilobytes/3600 seconds
              PFS (Y/N): N
              Transform sets={ MYSET, }
```

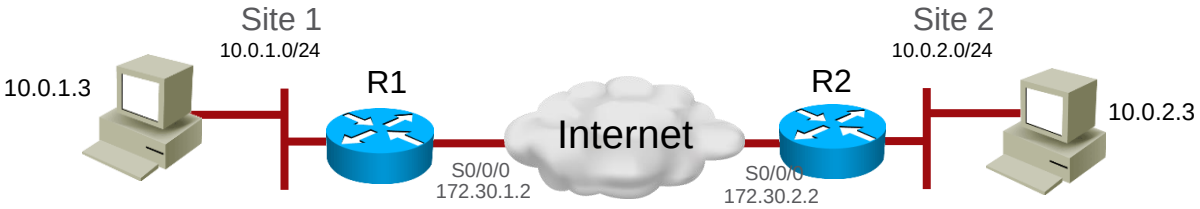
show crypto isakmp policy




```
show crypto isakmp policy
```

```
R1# show crypto isakmp policy
Protection suite of priority 110
      encryption algorithm:   3DES - Data Encryption Standard (168 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  preshared
      Diffie-Hellman group:   #2 (1024 bit)
      lifetime:               86400 seconds, no volume limit
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
```

show crypto ipsec transform-set




```
show crypto ipsec transform-set
```

Displays the currently defined transform sets

```
R1# show crypto ipsec transform-set
Transform set AES_SHA: { esp-128-aes esp-sha-hmac }
        will negotiate = { Tunnel,  },
```


CISCO