



智能业务平台

大型企业

无边界网络

GET VPN部署指南

● ● ● IBA智能业务平台

修订版：2012年上半年

前言

本指南是一份思科®智能业务平台（IBA）指南。

本指南的目标受众

本指南主要面向在企业中承担以下职务的人员：

- 需要解决方案标准实施规程的系统工程师
- 需要获取参考资料以撰写思科IBA实施项目工作说明书的项目经理
- 需要借助产品指南销售新技术或撰写自己的实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说，您也可以将思科IBA指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，或利用它更好地规划项目成本预算和项目工作范围。

版本系列

思科每年对IBA指南进行两次更新和修订。在发布思科IBA指南系列之前，我们将在IBA实验室对其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性，您应使用同一IBA系列中的设计指南文档。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。指南系列的命名方式如下：

- 年2月指南系列
- 年8月指南系列

其中的年表示发布该指南系列的公历年度。

您可以在以下网址查看最新的思科IBA指南系列：

客户登录：<http://www.cisco.com/go/cn/iba>

合作伙伴登录：<http://www.cisco.com/go/cn/iba>

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤，这些设备运行着Cisco IOS、Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系统命令的指定规则，您需要按照这些规则来输入命令。

在CLI中输入的命令如下所示：

```
configure terminal
```

为某个变量指定一个值的命令如下所示：

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示：

```
class-map [highest class name]
```

以交互示例形式显示的命令（如脚本和包含提示的命令）如下所示：

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入：

```
wrr-queue random-detect max-threshold 1 100 100 100 100  
100 100 100
```

问题和评论

如需要了解更多有关思科IBA智能业务平台的信息，请访问

<http://www.cisco.com/go/cn/iba>

如需要注册快速报价工具（QPT），请访问

<http://www.cisco.com/go/qpt>

目录

本IBA指南的内容	1	部署详情	5
关于IBA	1	密钥服务器的部署详情	5
关于本指南	1	部署密钥服务器	5
成功部署路线图	1	组成员的部署详情	16
		部署组成员	16
简介	2	附录A: GET VPN产品列表	18
业务概述	2	附录B: 设备配置文件	19
技术概述	2	GET VPN密钥服务器	19
		GET VPN组成员	22

本手册中的所有设计、规格、陈述、信息和建议（统称为“设计”）均按“原样”提供，可能包含错误信息。思科及其供应商不提供任何保证，包括但不限于适销性、适合特定用途和非侵权保证，或与交易过程、使用或贸易惯例相关的保证。在任何情况下，思科及其供应商对任何间接的、特殊的、继发的或偶然性的损害均不承担责任，包括但不限于由于使用或未能使用本手册所造成的利润损失或数据丢失或损害，即使思科或其供应商已被告知存在此类损害的可能性。这些设计如有更改，恕不另行通知。用户对于这些设计的使用负有全部责任。这些设计不属于思科、供应商或合作伙伴的技术建议或其它专业建议。用户在采用这些设计之前应咨询他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

文中使用的任何互联网协议（IP）地址均非真实地址。文中的任何举例、命令显示输出和图示仅供说明之用。在图示中使用任何真实IP地址均属无意和巧合。

© 2011思科系统公司。保留所有权利。

本IBA指南的内容

关于IBA

思科IBA能帮助您设计和快速部署一个全服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

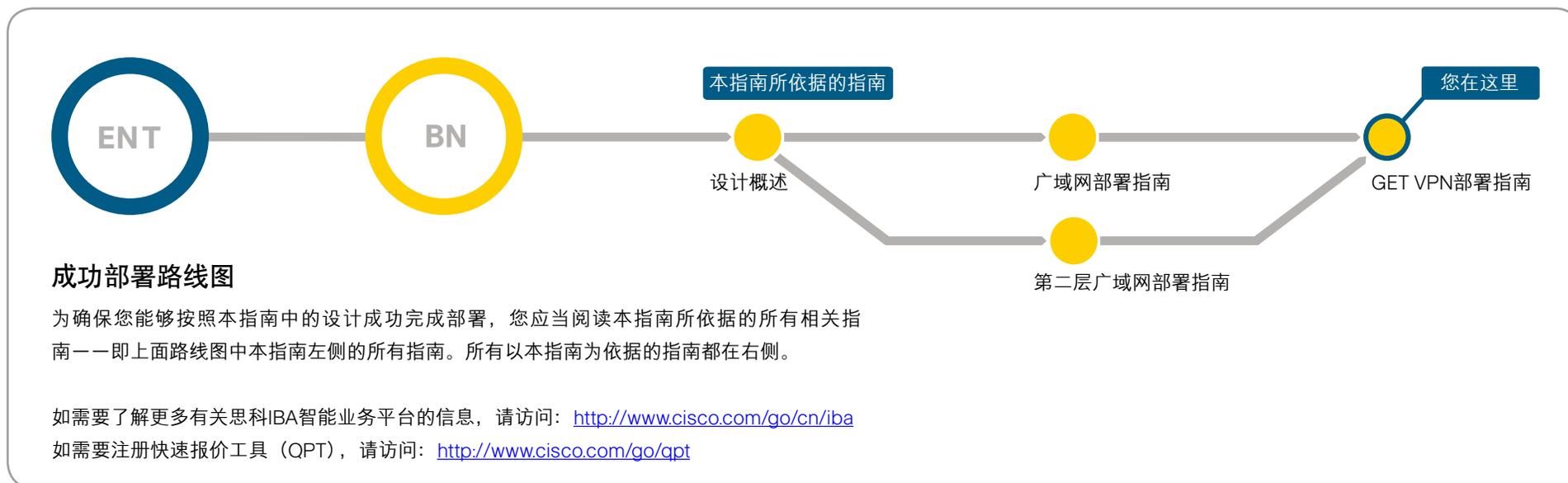
思科IBA在一个综合解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能够实现无缝协作。IBA采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足企业需求的解决方案，而不必担心技术复杂性方面的问题。

关于本指南

本指南是一份附加设计概述，包含如下内容：

- 针对一项可以添加到IBA基础部署项目中的思科IBA设计的介绍
- 阐明该设计所涉及的各项要求
- 描述该附加设计将为您的组织带来的优势

在成功部署路线图上，附加设计概述总是紧随基础设计概述之后，如下所示。



简介

本指南介绍了如何部署Cisco? 群组加密传输VPN(GET VPN)技术, 以在主站点与多达500个远程站点之间建立安全的广域网与城域网(MAN)连接。

业务概述

各企事业单位均极为关注对电子资产的保护, 以使其免遭外部攻击。目前, 一种重要的发展趋势日益显现: IT服务逐渐向云服务迁移。

随着企业逐渐向基于云的IT服务和云计算迁移, 他们越来越需要为传输中的数据提供保护, 以保证数据的机密性、完整性与可用性。同时, 政府法规与业界安全标准的出台也进一步推动了这种需求, 例如健康保险便携性与责任法案 (HIPAA)、联邦信息安全管理法案(FISMA)、萨班斯-奥克斯利法案和支付卡行业数据安全标准(PCI DSS)详细说明了这一需求并为经由网络传输的数据进行加密设立了标准。

此外, 语音与视频也逐渐在整个网络流量中占据主导地位。企业希望通过充分利用技术(如富媒体协作工具和交互式视频解决方案)减少差旅次数, 进而降低运营成本, 减少碳排放。语音与交互式视频应用的分布式特性迫切要求实现即时的远程站点间通信。与此同时, 面对当前的广域网技术, 企业不得不在为这些实时应用提供QoS和保证网络传输的安全之间做出权衡。

为解决这些挑战, 思科推出了下一代广域网加密技术Cisco GET VPN, 该技术在满足安全要求的同时提供了实时应用所需的即时性远程站点间通信支持。Cisco GET VPN 使用户无需再在专用广域网环境中在网络智能与数据私密性之间进行折中处理。该技术引入了一种全新类型的VPN, 它无需隧道, 同时提供了符合联邦信息处理标准(FIPS) 140系列的强大加密特性。

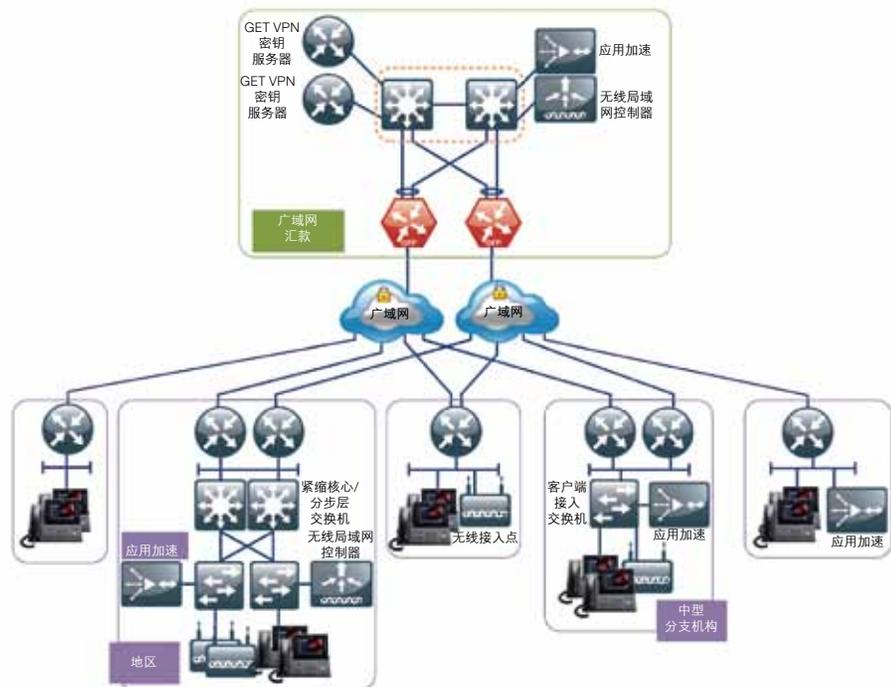
技术概述

GET VPN是一种基于IETF标准(RFC 3547)的无隧道VPN技术。该技术为网络基础设施提供了端到端的数据加密, 同时能保持站点间的任意点到任意点通信。您可以将其部署在各种广域网核心传输网络中, 如IP或多协议标签交换 (MPLS) 网络等。GET VPN可充分利用群组解释域(GDOI)协议, 在网络设备之间建立一个安全的通信域。

GET VPN的优势包括:

- 高度可扩展的VPN技术, 提供了任意点到任意点的网状拓扑结构, 而无需进行复杂的对等安全关联
- 在站点间直接传输流量, 可有效减少延迟和抖动
- 使用密钥服务器 (KS) 集中管理加密策略与成员
- 通过充分利用本机路由基础设施, 简化了网络设计 (无需重叠路由协议)
- 通过支持基于组播的网络核心, 可高效利用带宽
- 提供了出色网络智能特性, 如本机路由路径、网络拓扑和QoS等

图1. 面向大型企业的无边安全广域网

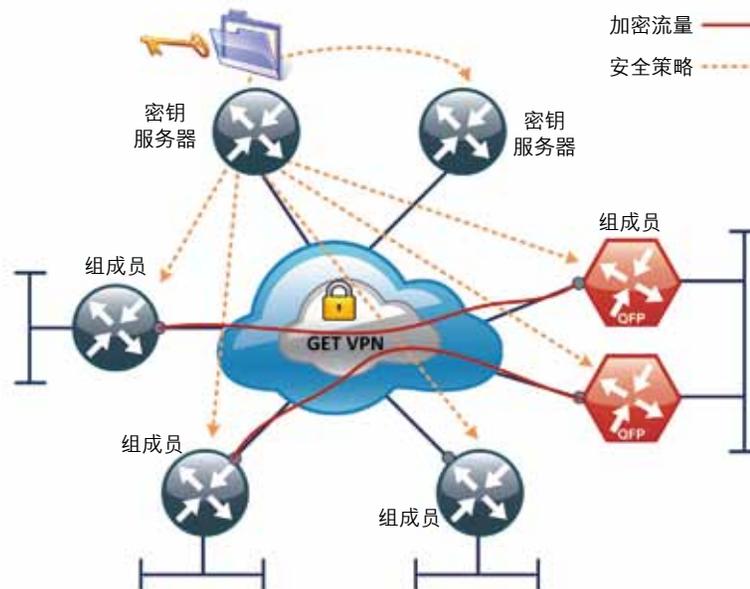


GET VPN的 组件

组成员(GM)是Cisco IOS路由器，专门用于对数据流量进行加密和解密。GM在密钥服务器(KS)上注册，以获取对流经设备的数据流进行加密和解密所需的加密密钥。GM还负责在安全与不安全的域之间执行路由。最后，GM还参与网络中已建立的组播通信。

KS是GET VPN的中枢系统，负责验证GM。KS还负责管理安全策略，决定应该对哪些流量进行加密。KS通过GDOI协议将用于流量加密的会话密钥和安全策略分发给GM。KS发给GM的密钥有两种：密钥加密密钥(KEK)及流量加密密钥(TEK)。KS利用KEK来保护KS与GM之间的通信。GM利用TEK对GM之间传输的流量进行批量数据加密。

图2. GET VPN的组件

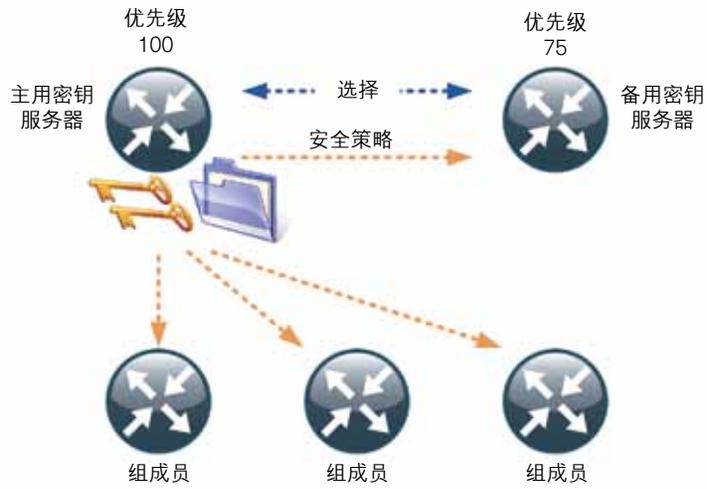


KS将按照需要发出密钥重置信息，其中包含了旧的IPSec安全关联(IPSec SA)到期以后应该使用的新加密策略和加密密钥。密钥重置信息将在SA到期之前发出，以便所有GM都能获得新密钥。

KS是GET VPN部署中的一个重要组件。如果KS不可用，新的GM将无法注册和参与安全通信，而且现有的GM在当前的安全关联到期时也将收不到新的密钥和安全策略。

为保证GET VPN网络的高可用性和永续性，冗余的KS以协作模式运行。协作密钥服务器(COOP KS)将共同管理群组的GDOI注册工作，共担GM注册负载。COOP KS在启动时会进入一个选择流程，优先级最高的KS将成为主用设备，其它KS将作为备用设备。主用KS负责创建并向GM重新发送安全策略和密钥，同时与备用KS进行同步。

图3. COOP KS同步 workflow



备注

部署详情

本部分包括以下内容：

- 密钥服务器的部署详情
- 组成员的部署详情

密钥服务器的部署详情

这一部分描述了GET VPN KS的配置流程，其中只说明了核心相关特性。

流程

部署密钥服务器

1. 应用路由器通用配置
2. 连接至分布层交换机
3. 为KS配置分布层交换机
4. 生成和导出RSA密钥
5. 配置KS策略
6. 在主用KS上配置冗余特性
7. 配置备用KS

表 1. 密钥服务器参数

主机名	端口通道 编号	IP地址	子网掩码	缺省网关	KS KS角色	优先级
KS-2951-1	21	10.4.32.151	255.255.255.192	10.4.32.129	主用	100
KS-2951-2	22	10.4.32.152	255.255.255.192	10.4.32.129	备用	75

程序 1

应用路由器通用配置

您首先需要为KS路由器应用通用配置。

步骤1：配置设备主机名。

```
hostname KS-2951-1
```

步骤2：配置设备管理协议。

安全HTTP (HTTPS)和安全外壳 (SSH) 是HTTP和Telnet协议的安全替代品。它们使用安全套接字层(SSL)和传输层安全(TLS)提供了设备身份验证和数据加密功能。

通过使用SSH和HTTPS协议，能对局域网设备进行安全的管理。这两个协议均进行了加密，可提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

```
ip domain-name cisco.local  
ip ssh version 2  
no ip http server  
ip http secure-server  
line vty 0 15  
transport input ssh
```

启用简单网络管理协议(SNMP)后，能够通过网络管理系统 (NMS) 对网络基础设施设备进行配置。SNMPv2c针对只读和读写团体字符串进行了配置。

```
snmp-server community cisco RO  
snmp-server community cisco123 RW
```

步骤3: 配置安全用户身份验证。

启用身份验证、授权与记账 (AAA) 来支持访问控制。所有针对网络基础设施设备的管理访问 (SSH和HTTPS) 均受到AAA的控制。



读者提示

本架构中使用的AAA服务器是思科身份验证控制系统。如需了解有关ACS配置的详细信息, 请参阅《面向大型企业的思科IBA智能业务平台——无边界网络网络设备身份验证与授权部署指南》。

TACACS+是在基础设施设备上向AAA服务器验证管理登录所采用的主要协议。此外, 系统还在每个网络基础设施设备上定义了一个本地AAA用户数据库, 用于在中央TACACS+服务器不可用时, 提供备用身份认证源。

```
enable secret clisco123
service password-encryption
!
username admin password clisco123
aaa new-model
!
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

步骤4: 配置同步时钟。

网络时间协议(NTP)用于同步网络设备。NTP网络通常从权威时间源, 如与时间服务器相连的无线电时钟或原子钟那里获取时间信息, 然后在企业网络中分发此信息。

您应将网络设备设定为与网络中的本地NTP服务器保持同步。本地NTP服务器通常会参考来自外部来源的更准确的时钟信息。通过对控制台消息、日志和调试报告进行配置, 在输出时添加时间戳, 从而实现对网络中事件的交叉参考。

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time  PDT  recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```



技术提示

配置网络时间协议(NTP)来实现所有设备的同步是一种最佳实践。但是, GET VPN并不依靠NTP来提供基于时间的反回放 (TBAR) 功能。GET VPN使用KS上的一个伪时钟来管理时间, 不需要NTP。

当启用同步记录未请求信息和调试报告时, 在显示或打印交互式CLI输出结果后, 控制台日志信息将在控制台上显示。借助这一命令, 您可以在启用调试流程时, 继续在设备控制台上输入信息。

```
line con 0
  logging synchronous
```

程序2

连接至分布层交换机

第三层端口通道接口连接到广域网分布层交换机。以下配置用于在路由器和交换机之间创建一个EtherChannel链路，并设定两个通道组(channel-group)成员。

步骤1: 配置端口通道接口并分配IP地址

作为一种最佳实践，请尽可能在链路两端使用相同的通道编号。

```
interface Port-channel [number]
  ip address [IP address] [netmask]
```

步骤2: 启用端口通道组成员并指定相应的通道组。

并非所有的路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface [interface type] [number]
  no ip address
  channel-group [number]
  no shutdown
```

步骤3: 配置缺省路由器。

提供可达性信息，使KS利用缺省路由到达GM。

```
ip route 0.0.0.0 0.0.0.0 [Gateway IP address]
```

示例

```
interface Port-channel21
  ip address 10.4.32.151 255.255.255.192
!
interface GigabitEthernet0/0
  no ip address
  channel-group 21
  no shutdown
!
interface GigabitEthernet0/1
  no ip address
  channel-group 21
```

```
no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.4.32.129
```

程序3

为KS配置分布层交换机

WAN分布层交换机是物理连接位于WAN汇聚站点的设备（如GET VPN KS）的相应位置。该类型设备需要一种具有弹性的连接，但不需要路由协议。这种连接可以使用第二层EtherChannel链路。

本指南假定已经配置了分布层交换机，文中仅包括完成交换机与KS连接所需的程序。如需了解有关分布层交换机配置的更多信息，请参阅《面向大型企业的IBA智能业务平台——无边界网络局域网部署指南》。

您必须为此设备以及具有相似连接需求的其它设备创建一个VLAN和SVI。该VLAN被称为广域网服务网络。

步骤1: 配置第二层

采用星型设计，可以避免生成树环路或链路被拦截；但仍需启用快速PVST，以防止意外环路的出现。

创建VLAN并将分布层交换机设置成VLAN的生成树根（如有必要）。

```
vlan 350
  name WAN_Service_Net
spanning-tree vlan 350 root primary
```

步骤2: 配置EtherChannel成员接口。

使用EtherChannel时，成员接口应位于堆叠中的不同交换机上，或模块化交换机中的不同模块上，才能实现最高永续性。

在配置逻辑端口通道接口前，先配置属于第二层EtherChannel成员的物理接口。按此顺序进行配置能够最大限度减少所需操作，因为大多数输入端口通道接口的命令会复制到其成员接口，而无需人工复制。

当与路由器等不支持LACP的网络基础设施设备相连时，使用以下命令。

此外，采用在平台配置程序中定义的出口QoS宏，以确保正确地划分流量优先级。

```
interface GigabitEthernet 1/0/9
  description KS-2951-1 Gig0/0
interface GigabitEthernet 2/0/9
  description KS-2951-1 Gig0/1
!
interface range GigabitEthernet 1/0/9, GigabitEthernet 2/0/9
  switchport
  macro apply EgressQoS
  channel-group 21 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

步骤3: 端口通道接口配置

处于接入模式的端口通道接口用于连接至这一上游设备，该设备允许端口通道接口提供到单一VLAN的访问功能。当使用EtherChannel时接口类型为端口通道，而且编号必须和上一步中配置的通道组相匹配。

```
interface Port-channel 21
  description KS-2951-1
  switchport mode access
  switchport access vlan 350
  logging event link-status
  no shutdown
```

步骤4: 配置第三层（如有必要）。

配置VLAN接口（SVI），以便VLAN中的设备能与网络其余部分通信。

```
interface Vlan350
  ip address 10.4.32.129 255.255.255.192
  ip pim sparse-mode
  no shutdown
```

程序4 生成和导出RSA密钥

本程序仅适用于主用KS。

在开始KS配置之前，先生成在密钥重置过程中将使用的可导出RSA密钥。

步骤1: 生成在密钥重置过程中将使用的RSA密钥。

```
crypto key generate rsa label GETVPN-REKEY-RSA modulus 2048
exportable
```



技术提示

在主用KS上生成RSA密钥对。确保在生成RSA密钥时使用“可导出”选项。这样，您便可以将密钥对导出并安装到其它将在网络中以COOP KS模式运行的密钥服务器上。

示例

```
KS-2951-1(config)# crypto key generate rsa label GETVPN-REKEY-RSA
modulus 2048 exportable
```

```
The name for the keys will be: GETVPN-REKEY-RSA
```

```
% The key modulus size is 2048 bits
```

```
% Generating 2048 bit RSA keys, keys will be exportable...[OK]
```

步骤2: 从主用KS导出RSA密钥。

```
crypto key export rsa GETVPN-REKEY-RSA pem terminal 3des
clsco123
```

技术提示

在本例中，您将RSA密钥对从主用KS导出为一种增强保密邮件(PEM)格式。我们建议您通过复制粘贴将密钥对从KS控制台导出到文件中，并将文件保存在安全的环境中。以后您可利用此密钥对构建备用KS，或在必要时重新构建主用KS。

示例

```
KS-2951-1(config)#crypto key export rsa GETVPN-REKEY-RSA pem
terminal 3des c1sco123
% Key name: GETVPN-REKEY-RSA
  Usage: General Purpose Key
  Key data:
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtX3Cr8QUpSmgTpmLkyYG
CySAYlPTnoy06umGRMmxXu/XB4ls64BpfHnrmuCqhtNajr1OxKO9TYh6r7kUSSKO
EpFqmtk3bEJq/MF+hUvCXxz6Qe8S+YC0dHUem1039/mZJdK9RBwjC7KlFbP4io6D
h9Wm1L9R8mvTms1CEfdu4ameRaR+8dt6Tbm9SGwamKA8U2I8q5BPXDXfJMHCE/4y
Kijo+5gSy1hy+1SEXW9MiNtV4Htckb5K1H+vhtkxDIzhXT2m8/wUQz3t+9LXfRgU
OWFS09XjTqbMDCmpAGSNnhFsqHW6+DYqup1wJGypfRK1TFr5cQ8nQx0q6pwzA+5
fwIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, B0EA38C0B90569C9
2BADU1kcBZQo3aY/C+lgT3jVQxbawIoidGi50ZtqpczzHX5KwkjN/o36t1Wa7ka
TtPh3XZ6UZJ1YCiAW/fzyuKD3ITx6eS/npaHQu2pKl0ToDUEman0ptdKklRv50DV7
AQEMyW127Uy16cbbOdTkX4y1y5VmzCz3oLWqcygEiYWe2pHaBldP7TEHnKmrp3H
ztRJlWlWJc682EI0K2IuhhNb05XAt3xXO241wNSvgE5zAtE9p2Z81GSevcWjfmoi
Pp58T7EWL9hWoCmpUA6+S60b/OVTV+MG7tGENGiL0alquMKQnGRf/eK28KaLwg7x
<key data deleted>
-----END RSA PRIVATE KEY-----
```

程序5

配置KS策略

面向GET VPN的ISAKMP策略使用如下标准：

- 基于256位密钥的高级加密标准(AES)
- 安全哈希标准 (SHA)
- Diffie-Hellman组: 5 (用于KS)
- Diffie-Hellman组: 2 (用于GM)
- IKE使用期限: 86400 (缺省——用于KS)
- IKE使用期限: 1200 (用于GM)

步骤1: 为COOP KS定义ISAKMP策略。

```
crypto isakmp policy 10
  encr aes 256
  group 5
```

步骤2: 为GM定义ISAKMP策略。

```
crypto isakmp policy 15
  encr aes 256
  group 2
  lifetime 1200
```

尽管多数ISAKMP策略参数都必须在KS和GM之间进行相同的配置，但IKE使用期限将在KS和GM之间进行协商，使用配置的最低值。在KS上，将IKE使用期限从缺省的86400秒更改为1200秒，以集中设置GM的IKE使用期限。

步骤3: 利用预共享密钥(PSK)配置互联网密钥交换(IKE)身份验证方法。

```
crypto isakmp policy 10
  authentication pre-share
!
crypto isakmp policy 15
  authentication pre-share
```

缺省的身份验证方法是使用公共密钥基础设施(PKI) (authentication rsa-sig)。为方便部署，本示例使用PSK身份验证方法。

步骤4: 配置PSK。要成功完成IKE身份验证，远程对等设备的PSK必须与本地对等设备的PSK相匹配。您可以在每个对等设备的基础上进行独特的PSK配置，也可以使用通配符PSK，让一组身份验证水平相当的远程设备共用一个IKE PSK。

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```

步骤5: 配置IPSec加密配置文件。

```
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac  
!  
crypto ipsec profile GETVPN-PROFILE  
set security-association lifetime seconds 7200  
set transform-set AES256/SHA
```

本示例定义了数据加密算法以及流量加密密钥(TEK)的使用期限。使用AES-256加密算法能实现更强大的安全性。TEK的使用期限被设置为两个小时（7200秒）。



技术提示

TEK的使用期限不能低于3600秒的缺省值。较短的TEK使用期限会导致更多的加密策略更替（rollover），并且必须要从KS同步到所有的GM。将TEK使用期限设定得过短可能导致GET VPN网络运行不稳定。

步骤6: 配置GET VPN GDOI组参数。KS上配置的每个GDOI组都需要一个独特的组ID。

```
crypto gdoi group GETVPN-GROUP  
identity number 65511
```

步骤7: 将设备命名为GDOI KS，并定义将在密钥重置过程中使用的参数。

```
server local  
rekey algorithm aes 256  
rekey retransmit 40 number 3  
rekey authentication mypubkey rsa GETVPN-REKEY-RSA
```

```
rekey transport unicast  
address ipv4 10.4.32.151
```

缺省的密钥重置传输机制是组播，但此处使用了单播密钥重置传输机制，两次重新传输之间的间隔为40秒。密钥重置算法使用AES-256定义，并使用RSA签名进行密钥重置身份验证。

步骤8: 配置用于定义应加密的流量的IPSec配置文件和安全策略，以及TBAR窗口尺寸。

```
sa ipsec 10  
profile GETVPN-PROFILE  
match address ipv4 GETVPN-POLICY-ACL  
replay time window-size 5
```

步骤9: 配置安全策略访问控制列表 (ACL)。

利用扩展的IP访问列表定义密钥服务器上的安全策略。您应只使用访问列表中的五元组（即source_ip_address、destination_ip_address、protocol、source_port和destination_port）来决定对哪些流量进行加密。ACL中的允许项定义了需要加密的流量，而拒绝项定义了不需要GET VPN加密的流量。您需对ACL中的拒绝项进行配置，以排除已经加密的路由协议和流量，如SSH、TACACS+、GDOI和ISAKMP等。如先前步骤所示，ACL将应用于GET VPN配置。

```
ip access-list extended GETVPN-POLICY-ACL  
remark >> exclude transient encrypted traffic (ESP, ISAKMP,  
GDOI)  
deny esp any any  
deny udp any eq isakmp any eq isakmp  
deny udp any eq 848 any eq 848  
remark >> exclude encrypted in-band management traffic (SSH,  
TACACS+)  
deny tcp any any eq 22  
deny tcp any eq 22 any  
deny tcp any any eq 49  
deny tcp any eq 49 any  
remark >> exclude routing protocol with MPLS provider  
deny tcp any any eq bgp  
deny tcp any eq bgp any
```

```

remark >> exclude routing protocol used for Layer 2 WAN
deny  eigrp any any
remark >> exclude other protocols as necessary (multiple
lines)
deny  [protocol] [source] [destination]
remark >> Require all other traffic to be encrypted
permit ip any any

```



技术提示

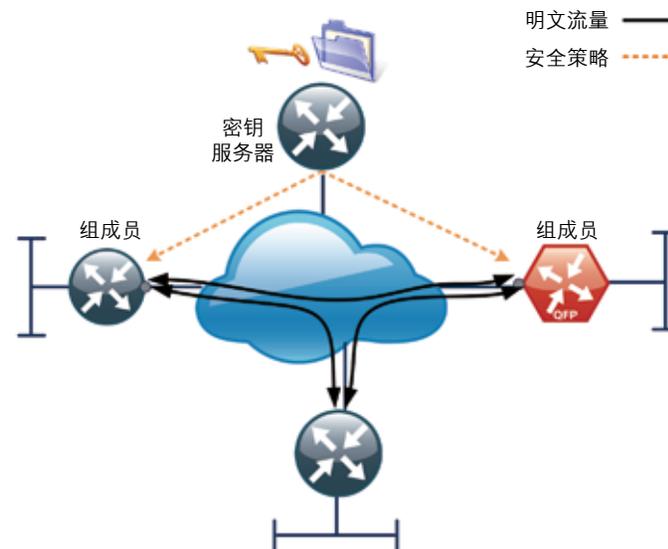
通过从未加密网络向GET VPN迁移，您可以在转换到GET VPN GM的过程中使用仅接收SA（receive-only SA）。仅接收SA允许GM注册到一个KS并开始接收安全策略和用于加密的密钥；但是，GM将继续以明文方式转发流量。仅接收SA为GET VPN建立控制平面时不需要使用数据计划，从而能够在已经迁移到GET VPN网络的站点和等待迁移的站点之间实现互操作性。以下命令用于在KS上启用仅接收SA功能。

```

crypto gdoi group GETVPN-GROUP
server local
sa receive-only

```

图4. 仅接收模式



在您的网络完全迁移到GET VPN，而且经检验控制平面已经完全投入运行之后，您可以通过禁用KS上的仅接收SA模式，为群组中的所有GM启用加密功能。

```

crypto gdoi group GETVPN-GROUP
server local
no sa receive-only

```

图5: 稳定状态运行



示例一主用密钥服务器

```
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp policy 15
  encr aes 256
  authentication pre-share
  group 2
  lifetime 1200
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
!
```

```
crypto ipsec profile GETVPN-PROFILE
  set security-association lifetime seconds 7200
  set transform-set AES256/SHA
!
crypto gdoi group GETVPN-GROUP identity number 65511
  server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
  rekey transport unicast
  sa ipsec 10
  profile GETVPN-PROFILE
  match address ipv4 GETVPN-POLICY-ACL
  replay time window-size 5
  address ipv4 10.4.32.151
!
ip access-list extended GETVPN-POLICY-ACL
  remark >> exclude transient encrypted traffic (ESP, ISAKMP,
  GDOI)
  deny esp any any
  deny udp any eq isakmp any eq isakmp
  deny udp any eq 848 any eq 848
  remark >> exclude encrypted in-band management traffic (SSH,
  TACACS+)
  deny tcp any any eq 22
  deny tcp any eq 22 any
  deny tcp any any eq 49
  deny tcp any eq 49 any
  remark >> exclude routing protocol with MPLS provider
  deny tcp any any eq bgp
  deny tcp any eq bgp any
  remark >> exclude routing protocol used for Layer 2 WAN
  deny eigrp any any
  remark >> exclude PIM protocol
  deny pim any host 224.0.0.13
  remark >> exclude IGMP with MPLS provider
  deny igmp any host 224.0.0.1
```

```
deny igmp host 224.0.0.1 any
deny igmp any host 224.0.1.40
deny igmp host 224.0.1.40 any
remark >> exclude icmp traffic destined to SP address
deny icmp any 192.168.3.0 0.0.0.255
deny icmp 192.168.3.0 0.0.0.255 any
deny icmp any 192.168.4.0 0.0.0.255
deny icmp 192.168.4.0 0.0.0.255 any
remark >> Require all other traffic to be encrypted
permit ip any any
```

程序6

在主用KS上配置冗余特性

为实现GET VPN网络的冗余性和高可用性，思科建议至少让两个KS以COOP KS模式运行。COOP KS能确保组安全策略、加密密钥和注册的GM信息在KS之间共享和同步。从以COOP模式运行的所有KS中确定主用KS时，首先要看优先级是否最高，然后选择用于密钥重置的最大IP地址。

主用KS负责建立并重新分发组策略，同时还负责向其它KS发送组信息更新，以保持备用KS的同步。如果主用KS不可用，一个备用KS在没有检测到其它优先级更高的KS时可以宣布自己成为主用KS，承担起主用KS的角色。

步骤1: 在主用KS上配置KS冗余特性，将KS的优先级设为100。

```
crypto gdoi group GETVPN-GROUP
server local
redundancy
local priority 100
peer address ipv4 10.4.32.152
```

步骤2: 在以COOP KS模式运行的主用KS上配置定期失效对等体保护，以便备用KS能够跟踪主用KS的状态。

```
crypto isakmp keepalive 15 periodic
```

示例一具备冗余特性的主用密钥服务器

```
crypto isakmp keepalive 15 periodic
crypto gdoi group GETVPN-GROUP
identity number 65511
server local
redundancy
local priority 100
peer address ipv4 10.4.32.152
```

程序7

配置备用KS

本程序仅适用于备用KS。

备用KS的配置方法与主用KS类似。首先完成程序1、程序2和程序3。然后完成以下步骤。在主用和备用KS之间必须配置相同的策略。这样可以保证在备用KS成为主用KS时，重新分发给GM的规则与以前相同。

步骤1: 从在先前程序中创建的KS导入RSA密钥。此步骤需要PEM格式的密钥，导入操作通过从终端剪切粘贴到新的KS路由器来完成。您需要分别粘贴公共密钥和私有密钥。

```
crypto key import rsa GETVPN-REKEY-RSA exportable terminal
clscc123
```

示例

```
KS-2951-2(config)# crypto key import rsa GETVPN-REKEY-RSA
exportable terminal c1sco123
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtX3Cr8QUpSmgTpmLkyYG
CySAYlPTnoy06umGRMmxXu/XB4ls64BpfHnrMuCqhtNajrloXKO9TYh6r7kUSSKO
EpFqmtk3bEJq/MF+hUvCXxz6Qe8S+YC0dHUem1039/mZJdK9RBwjC7KlFbP4io6D
h9WmLL9R8mvTmslCEfdu4ameRaR+8dt6Tbm9SGwamKA8U2I8q5BPXDXfJMHCe/4y
Kijo+5gSylhy+1SEXW9MiNtV4Htckb5KlH+vhtkxDIzhXT2m8/wUQz3t+9LXfRgU
OWFS09XjTqbMDcMpAGSNnhFsqHW6+DYqup1wJGypfRk1TFr5cQ8nCQx0q6pwzA+5
fwIDAQAB
-----END PUBLIC KEY-----
quit
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, B0EA38C0B90569C9
2BADU1kcBZQo3aY/C+lgT3jVQxbawIoidGi5OZtqpczzHX5KwkGjN/o36t1Wa7ka
TtPh3XZ6UZJ1YCiAW/fzyuKD3ITx6eS/npaHQu2pKl0ToDUEman0ptdKklRv5ODV
AQEMYwI27Uy16cbbOdTkX4y1y5VmzCz3oLWqcygEiyWe2pHaB1dP7TEHnKmnrp3H
ztRJIwLWJc682EI0K2IuhhNb05XAt3xXO241wNSvgE5zAtE9p2Z81GSevcWjfmoi
Pp58T7EWL9hWoCmpUA6+S60b/OVTV+MG7tGENGiL0alquMKQnGRf/eK28KaLwg7x
<key data deleted>
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.
```

技术提示

所有以COOP KS模式运行的KS上的RSA密钥对必须完全相同。如果KS被添加到群组时没有RSA密钥，它将无法生成策略。这将导致注册到此KS的GM处于故障关闭状态，无法与群组中的其它GM传输流量。

步骤2: 针对备用KS完成程序5（所有步骤）

步骤3: 在所有以COOP KS模式运行的备用KS上配置定期失效对等体保护，以便主用KS能够跟踪备用KS的状态。

```
crypto isakmp keepalive 15 periodic
```

步骤4: 通过在备用KS上启用协作KS功能并将此KS的优先级设为75（此优先级低于主用KS的优先级（100））来配置KS冗余。

```
crypto gdoi group GETVPN-GROUP
server local
redundancy
local priority 75
peer address ipv4 10.4.32.151
```

技术提示

在将一个新的KS设置为COOP KS模式时，为最大限度地减少对现有KS的中断，我们建议首先在备用KS上进行配置更改，最后再在主用KS上完成更改。

示例—备用密钥服务器

```
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp policy 15
  encr aes 256
  authentication pre-share
  group 2
  lifetime 1200
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN-PROFILE
  set security-association lifetime seconds 7200
  set transform-set AES256/SHA
!
crypto gdoi group GETVPN-GROUP identity number 65511
  server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
  rekey transport unicast
  sa ipsec 10
  profile GETVPN-PROFILE
  match address ipv4 GETVPN-POLICY
  replay time window-size 5
  address ipv4 10.4.32.152
  redundancy
  local priority 75
  peer address ipv4 10.4.32.151
!
ip access-list extended GETVPN-POLICY-ACL
```

```
  remark >> exclude transient encrypted traffic (ESP, ISAKMP,
GDOI)
  deny esp any any
  deny udp any eq isakmp any eq isakmp
  deny udp any eq 848 any eq 848
  remark >> exclude encrypted in-band management traffic (SSH,
TACACS+)
  deny tcp any any eq 22
  deny tcp any eq 22 any
  deny tcp any any eq 49
  deny tcp any eq 49 any
  remark >> exclude routing protocol with MPLS provider
  deny tcp any any eq bgp
  deny tcp any eq bgp any
  remark >> exclude routing protocol used for Layer 2 WAN
  deny eigrp any any
  remark >> exclude PIM protocol
  deny pim any host 224.0.0.13
  remark >> exclude IGMP with MPLS provider
  deny igmp any host 224.0.0.1
  deny igmp host 224.0.0.1 any
  deny igmp any host 224.0.1.40
  deny igmp host 224.0.1.40 any
  remark >> exclude icmp traffic destined to SP address
  deny icmp any 192.168.3.0 0.0.0.255
  deny icmp 192.168.3.0 0.0.0.255 any
  deny icmp any 192.168.4.0 0.0.0.255
  deny icmp 192.168.4.0 0.0.0.255 any
  remark >> Permit all other traffic to be encrypted
  permit ip any any
```

组成员的部署详情

这一流程将为一个已经配置完毕的广域网路由器添加GM功能。其中仅包含了启用GM功能所需要的额外步骤。

流程

部署组成员

1. 配置GM

程序 1

配置GM

GM将注册到KS，以获取IPSec SA和对流量进行加密所需的加密密钥。在注册过程中，GM将向KS提供一个组ID，以获得该组的策略和密钥。由于多数智能特性位于KS上，GM上的配置相对比较简单，所有GM的配置几乎完全相同。

这一程序假定所有基本连接配置（如缺省路由、路由协议等）均已设置完毕。

步骤1：配置ISAKMP策略。

面向GET VPN的ISAKMP策略使用如下标准：

- 基于256位密钥的高级加密标准(AES)
- 安全哈希标准 (SHA)
- Diffie-Hellman Group 2
- 预共享密钥身份验证

```
crypto isakmp policy 15
  encr aes 256
  authentication pre-share
  group 2
```

步骤2：为KS配置PSK。

```
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
```

要成功完成IKE身份验证，远程对等设备的PSK必须与本地对等设备的PSK相匹配。您仅需要指明KS的PSK即可。

步骤3：配置GDOI组信息。

```
crypto gdoi group GETVPN-GROUP
  identity number 65511
  server address ipv4 10.4.32.151
  server address ipv4 10.4.32.152
```

在GM上无需设置IPSec转换集和配置文件。在GM成功注册到KS时，这些参数将从KS下载。GM只需定义GDOI组身份及KS的地址即可。

步骤4：定义GDOI选项的加密映射表(crypto map)并连接到在上一步骤中建立的GDOI组。

```
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP [Sequence number] gdoi
  set group GETVPN-GROUP
```

步骤5：在GM上激活GET VPN配置。



技术提示

与多个WAN传输网络相连的路由器（如双MPLS）必须将加密映射表应用到每个面向WAN的接口上。

```
interface [type] [number]
  crypto map GETVPN-MAP
```

步骤6：在广域网接口上执行ip tcp adjust-mss 1360命令，以支持IPSec开销。执行这一命令将降低穿过接口的TCP流量的报文段最大长度(MSS)，以避免IPSec报头造成的开销。该命令只适用于TCP流量，不能用于UDP流量。

```
interface [type] [number]
  ip tcp adjust-mss 1360
```

示例

```
crypto isakmp policy 15
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 10.4.32.151
crypto isakmp key cisco123 address 10.4.32.152
!
crypto gdoi group GETVPN-GROUP
  identity number 65511
  server address ipv4 10.4.32.151
  server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
  set group BN-WAN
!
interface GigabitEthernet0/0/3
  description WAN Interface
  ip tcp adjust-mss 1360
  crypto map GETVPN-MAP
```

备注

附录A: GET VPN产品列表

以下产品和软件版本已经过验证，可用于思科智能业务平台：

功能区域	产品	产品编号	软件版本
GET VPN密钥服务器			
WAN汇聚	Cisco2951	CISCO2951-SEC/K9	15.1(4)M2
GET VPN组成员			
WAN汇聚	ASR1002	ASR1002-5G-VPN/K9 ASR1002-PWR-AC	IOS-XE 15.1(3)S0a
WAN汇聚	ASR1001	ASR1001-2.5G-VPNK9 ASR1001-PWR-AC	IOS-XE 15.1(3)S0a
WAN远程站点路由器	Cisco1941	C1941-WAASX-SEC/K9 SL-19-DATA-K9	15.1(4)M2
WAN远程站点路由器	Cisco2911	C2911-VSEC/K9 SL-29-DATA-K9	15.1(4)M2
WAN远程站点路由器	Cisco2921	C2921-VSEC/K9 SL-29-DATA-K9	15.1(4)M2
WAN远程站点路由器	Cisco3925	C3925-VSEC/K9 SL-39-DATA-K9	15.1(4)M2
WAN远程站点路由器	Cisco3945	C3945-VSEC/K9 SL-39-DATA-K9	15.1(4)M2

附录B: 设备配置文件

GET VPN密钥服务器

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname KS-2951-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 *****
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
```

```
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-2801167241
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2801167241
  revocation-check none
  rsakeypair TP-self-signed-2801167241
!
!
crypto pki certificate chain TP-self-signed-2801167241
  certificate self-signed 01
    30820251 308201BA A0030201 02020101 300D0609 2A864886 F70D0101
    04050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
    43657274
    69666963 6174652D 32383031 31363732 3431301E 170D3131 30393133
    31363037
    33315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
    03132649
    4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32
    38303131
    36373234 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030
    81890281
    8100F09B 5205AE4A 514C90F8 64A5CA95 BDC94D50 92A3335A D1145BA2
    D37932A8
    1FFD373A F4EEF599 EF556203 12046D35 178F79DF 1B67C9E3 B44739D3
    F1AF9894
    4847E43A AAC4B9C4 865FE74D FA380D8A B796CD81 C653F1B4 0987651E
    A44155E6
    5C02B416 77489A24 A2AB0680 8A3246D9 9ED473CB DFA09653 81BD9970
    8529877A
    23DD0203 010001A3 79307730 0F060355 1D130101 FF040530 030101FF
    30240603
    551D1104 1D301B82 1957414E 5356432D 32393531 2D312E63 6973636F
    2E6C6F63
```

```

616C301F 0603551D 23041830 16801485 37C8FE88 641B64B5 C8CD2EFB
4982BAFB
3E34B830 1D060355 1D0E0416 04148537 C8FE8864 1B64B5C8 CD2EFB49
82BAFB3E
34B8300D 06092A86 4886F70D 01010405 00038181 009ECB89 3AD10D49
4830FF94
5B8ACD6B 9B7AD7EB 00DBB16A D865341E CB020CAB 2710F841 E8E7B54A
DF8ABA50
D36D9454 ECF88C68 14ED4426 5654F2D4 F4555BE8 37164AED 9218D46F
46A5EA73
2EE58953 8AD1ED76 435E2A8A 8A6FBFD7 BCE549ED CD0C8999 3CEC3DAC
D86047CD
45834775 601F40A2 A1369F35 A83E0DB6 F19F7DAA 17
quit
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
ip source-route
ip cef
!
!
!
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!

```

```

!
!
!
license udi pid CISCO2951/K9 sn *****
license boot module c2951 technology-package securityk9
hw-module pvdm 0/0
!
!
!
username admin password 7 *****
!
redundancy
!
!
!
!
ip ssh version 2
!
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp policy 15
  encr aes 256
  authentication pre-share
  group 2
  lifetime 1200
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN-PROFILE
  set security-association lifetime seconds 7200

```

```

set transform-set AES256/SHA
!
crypto gdoi group GETVPN-GROUP
identity number 65511
server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
  rekey transport unicast
sa ipsec 10
  profile GETVPN-PROFILE
  match address ipv4 GETVPN-POLICY-ACL
  replay time window-size 5
address ipv4 10.4.32.151
redundancy
  local priority 100
  peer address ipv4 10.4.32.152
!
!
!
!
!
interface Port-channel21
ip address 10.4.32.151 255.255.255.192
hold-queue 150 in
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
channel-group 21
!
interface GigabitEthernet0/1

```

```

no ip address
duplex auto
speed auto
channel-group 21
!
interface GigabitEthernet0/2
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.4.32.129
!
ip access-list extended GETVPN-POLICY-ACL
  remark >> exclude transient encrypted traffic (ESP, ISAKMP,
  GDOI)
  deny    esp any any
  deny    udp any eq isakmp any eq isakmp
  deny    udp any eq 848 any eq 848
  remark >> exclude encrypted in-band management traffic (SSH,
  TACACS+)
  deny    tcp any any eq 22
  deny    tcp any eq 22 any
  deny    tcp any any eq tacacs
  deny    tcp any eq tacacs any
  remark >> exclude routing protocol with MPLS provider
  deny    tcp any any eq bgp
  deny    tcp any eq bgp any
  remark >> exclude routing protocol used for Layer 2 WAN
  deny    eigrp any any
  remark >> exclude PIM protocol
  deny    pim any host 224.0.0.13

```

```

remark >> exclude IGMP with MPLS provider
deny igmp any host 224.0.0.1
deny igmp host 224.0.0.1 any
deny igmp any host 224.0.1.40
deny igmp host 224.0.1.40 any
remark >> exclude icmp traffic destined to SP address
deny icmp any 192.168.3.0 0.0.0.255
deny icmp 192.168.3.0 0.0.0.255 any
deny icmp any 192.168.4.0 0.0.0.255
deny icmp 192.168.4.0 0.0.0.255 any
remark >> Require all other traffic to be encrypted
permit ip any any
!
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 113A1C0605171F270133
!
!

```

```

!
!
gatekeeper
shutdown
!
!
!
line con 0
logging synchronous
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.4.48.17
end

```

GET VPN组成员

```

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname CE-ASR1002-1
!

```

```

boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
enable secret 4 *****
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
!
ip domain name cisco.local

```

```

ip multicast-routing distributed
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-4113326676
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4113326676
revocation-check none
rsa-keypair TP-self-signed-4113326676
!
!
crypto pki certificate chain TP-self-signed-4113326676
certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
  05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
  43657274
  69666963 6174652D 34313133 33323636 3736301E 170D3131 30393132
  30393430
  34365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
  03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34
  31313333
  32363637 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281

```

```

8100B0B7 95D8339F FD32AC21 1DDBBE64 C1823A93 2DBFD418 3884B579
D09323CA
808956FB 90946F69 BD84F663 34D6A211 0FDAA566 E2ECABF6 724CB7E0
4988785A
7FAAC219 B47BCA29 5B3CDE7C 70EB82F5 20748635 9FED08FC 79E09452
2A439EE2
A2EDF999 237FCF92 1FE1E7DF 9775C319 A0151975 8979CC04 FB0857F9
B363C956
BD250203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
551D2304 18301680 14755619 84805049 9491980C BDB86DED 8F18B643
EA301D06
03551D0E 04160414 75561984 80504994 91980CBD B86DED8F 18B643EA
300D0609
2A864886 F70D0101 05050003 81810001 CE3585E9 A38C275F 47189D1E
1E3C5320
3526EBDD 41491D0C 9D58D5CA ECFBA606 34E6B2BC CA8D3C3F 395DB3C7
769EA897
47870E62 D01D33E9 A9D48F98 D8E9ECD8 9C8AABF6 F5E9DC0A F7BD3A93
9BC263D7
6986441D D1C8D548 9D8BC222 B2AB99F1 DDE04E81 5F77C841 D0246154
78DAC605
41EA9130 F343DEB7 3124D143 20A236
quit
!
username admin password 7 *****
!
redundancy
mode none
!
!
!
!
!
ip tftp source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2

```

```

!
!
!
crypto isakmp policy 15
encr aes 256
authentication pre-share
group 2
crypto isakmp key cisco123 address 10.4.32.151
crypto isakmp key cisco123 address 10.4.32.152
!
!
crypto gdoi group GETVPN-GROUP
identity number 65511
server address ipv4 10.4.32.151
server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
set group BN-WAN
!
!
!
!
!
interface Loopback0
ip address 10.4.32.241 255.255.255.255
ip pim sparse-mode
!
interface Port-channel1
ip address 10.4.32.2 255.255.255.252
ip pim sparse-mode
no negotiation auto
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto

```

```

channel-group 1 mode active
!
interface GigabitEthernet0/0/1
no ip address
negotiation auto
channel-group 1 mode active
!
interface GigabitEthernet0/0/2
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/3
description WAN Interface
bandwidth 300000
ip address 192.168.3.1 255.255.255.252
ip tcp adjust-mss 1360
negotiation auto
crypto map GETVPN-MAP
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
!
!
router eigrp 100
distribute-list route-map BLOCK-TAGGED-ROUTES in
default-metric 100000 100 255 1 1500
network 10.4.0.0 0.1.255.255
redistribute bgp 65511
passive-interface default
no passive-interface Port-channell
eigrp router-id 10.4.32.241
!
router bgp 65511

```

```

bgp router-id 10.4.32.241
bgp log-neighbor-changes
network 0.0.0.0
network 192.168.3.0 mask 255.255.255.252
redistribute eigrp 100
neighbor 10.4.32.242 remote-as 65511
neighbor 10.4.32.242 update-source Loopback0
neighbor 10.4.32.242 next-hop-self
neighbor 192.168.3.2 remote-as 65401
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip pim autorp listener
ip tacacs source-interface Loopback0
!
!
route-map BLOCK-TAGGED-ROUTES deny 10
match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 113A1C0605171F270133
!
!
control-plane
!
!
!

```

```
!  
!  
line con 0  
  logging synchronous  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  transport input ssh  
line vty 5 15  
  transport input ssh  
!  
ntp source Loopback0  
ntp server 10.4.48.17  
end
```

备注



智能业务平台



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

B-0000121-1 12/11