

IPSec VPN 基本配置指南

（适用）运行AlliedWare™的交换机和路由器（部分）

ATC-TS1007

V1.1

2005-11-29

目 录

1. 概述	3
2. 实施需求	3
3. 配置实例实现环境	3
4. 配置说明	4
4.1 点到点 VPN（LAN to LAN VPN）配置实例一	5
4.2 点到点 VPN（LAN to LAN VPN）配置实例二	10
5. 验证和排错	18

1. 概述

本文介绍如何配置安奈特设备的 IPSec 模块。

2. 实施需求

要求至少一个合法静态 Internet 公网 IP 地址。

安奈特设备作为 IPSec VPN 网关，需要安装相应的加密卡 EMAC (Encryption Mini Accelerator Card)或 EPAC (Encryption PCI Accelerator Card)

所有带有“S”的路由器已经内置加密卡和防火墙 Feature license，无需额外购买。

下列安奈特产品可以作为 IPSec VPN 网关，但需要增加相应的加密卡，启用防火墙模块需要有相应 Feature License。

- AR300 系列；
- AR400 系列
- AR700 系列；
- AT-Rapier24i/Rapier16fi/8800 系列交换机；

所有产品中，如果使用 3DES 或 AES 加密，需要购买相应的 Feature License。DES 在安装加密卡后已经有效。

为了获得更好的性能，推荐使用 AR450S/AR750S 路由器作为 IPSec VPN 网关。

3. 配置实例实现环境

- AR450S ， Software release 2.6.1-06

4. 配置说明

IPSec VPN 配置是比较复杂的，如果希望一次就能正确配置成功，尽量减少配置错误，必须在开始配置每一台路由器之前预先做好规划，应该根据整个网络的安全策略来定义 IPSec VPN 策略，下面是规划的步骤：

步骤一：了解/制定网络拓扑结构。

步骤二：根据网络安全的需求，确定 IPSec 对等体感兴趣的数据流（确定我们所希望保护的主机和网络）。

步骤三：根据上面已经确定的 IPSec 对等体的数量和位置，来确定他们之间的关系。比如：是点对点的 VPN；点对多点的 VPN；还是移动用户的 VPN；或者是多种情况的混和使用。

步骤四：确定各 IPSec 对等体的详细资料，包括 IP 地址、选择的安全协议、选择的加密方式（确定安全的加密密钥）、选择认证方式（确定认证密码）等。

步骤五：检查当前的配置。保证现有网络在没有使用 IPSec 加密的情况下能正常工作—确认在配置 IPSec 之前，IPSec 各对等体之间存在基本的连接，实现所有的 IP 服务（根据实际的应用可能包含 Firewall 和 NAT 等功能）。可以使用“Ping”命令来检查基本的连通性。

规划完成后，进行 ISAKMP 和 IPSec 的配置。以下是配置步骤：

步骤一：创建安全用户，创建密钥

步骤二：使用 ISAKMP 进行密钥管理。需要在两个 IPSec 端点之间建立 ISAKMP 对等体（ISAKMP SA）。创建对等体间共享的密钥

步骤三：配置 IPSec 变换集（Bundle），为 IPSec 对等体创建所有可能的组合。包括：IPSec 的隧道模式、安全协议、加密方式、认证方式

步骤四：根据计划步骤中得到的资料来制定 IPSec 策略，过滤 IPSec 对等体之间感兴趣的数据流。注意某些特定的数据流的过滤（在后面的配置实例中详细介绍）

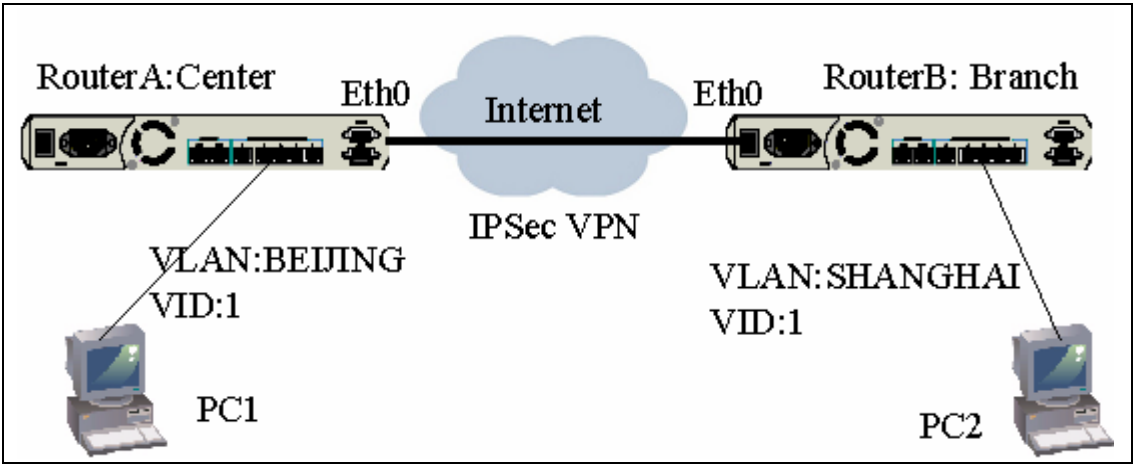
步骤五：测试和验证 IPSec。初始化 IPSec 的连接，验证 IPSec 对等体之间的连通性。

4.1 点到点 VPN（LAN to LAN VPN）配置实例一

该实例是点对点的 IPSec VPN，适合公司各分支与总部相连接的情况。要求各分支与总部都有固定的 IP 地址。没有使用 Firewall 和 NAT 等功能。

■ 网络拓扑：

图 1



■ IP地址表

名称	RouerA	RouterB
	Center	Branch
WAN	Eth0: 200.200.200.1/24	Eth0: 200.200.200.2/24
LAN	VLAN1: 192.168.10.1/24	VLAN1: 192.168.20.1/24
PC	PC1: 192.168.10.159/24	PC2: 192.168.20.87/24

■ IPSec 策略：

	RouterA	RouterB
路由器间认证方式	Pre-shared Key	Pre-shared Key
Pre-shared Key	123456	123456
安全协议	ESP	ESP
认证方式	SHA1	SHA1
加密方式	DES	DES

IPSec SA 模式	隧道模式	隧道模式
对等体 (Peer) IP	200.200.200.2	200.200.200.1
对等体主机名	Branch	Center
被加密的数据	192.168.10.0/24	192.168.20.0/24

■ IPSec VPN 配置:

步骤一: 配置基本网络:

Router A:

```
set system name=center
```

```
enable ip
```

```
add ip int=vlan1 ip=192.168.10.1 mask=255.255.255.0
```

```
add ip int=eth0 ip=200.200.200.1 mask=255.255.255.0
```

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.200.200.2
```

Router B:

```
set system name=branch
```

```
enable ip
```

```
add ip int=vlan1 ip=192.168.20.1 mask=255.255.255.0
```

```
add ip int=eth0 ip=200.200.200.2 mask=255.255.255.0
```

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.200.200.1
```

完成基本配置后, 先确保这个网络的连通性:

保证 PC1 可以 Ping 通 PC2

保证 PC2 可以 Ping 通 PC1

步骤二：创建安全用户，启用安全模式

RouterA:

```
add user=secoff pass=secoff priv=security
```

```
set user securedelay=600
```

```
enable system security
```

RouterB:

```
add user=secoff pass=secoff priv=security
```

```
set user securedelay=600
```

```
enable system security
```

在两台路由器上创建名为 **secoff** 的安全级别用户，启用安全模式后，需要使用该用户登陆才能对 IPSec 进行配置。

```
login secoff
```

输入该用户的登录密码 **secoff**。

步骤三：创建 Pre-shared Key

RouterA:

```
create enco key=1 type=gen val=123456
```

RouterB:

```
create enco key=1 type=gen val=123456
```

创建完成后使用 `sh enco key=1` 命令查看两边路由器上配置的 KEY 是否相同。

注意： 两端 *pre-shared key*（预共享密钥）必须完全相同。

在开始下一步配置之前，请确认 **AR450S** 工作在安全模式，而且使用安全用户登陆。取消安全模式，会删除所生成的 **KEY**，**IPSec** 将不能正常工作。

步骤四：配置 ISAKMP

RouterA:

```
create isakmp policy=centerkey peer=200.200.200.2 key=1
```

```
set isakmp policy=centerkey sendd=true setc=true
```

在路由器 A 上创建名为 **centerkey** 的 ISAKMP 策略，使用先前创建的密钥 **Key=1**（参考步骤三）。

RouterB:

```
create isakmp policy=branchkey peer=200.200.200.1 key=1
```

```
set isakmp policy=branchkey sendd=true setc=true
```

在路由器 B 上创建名为 **branchkey** 的 ISAKMP 策略，使用先前创建的密钥 **Key=1**（参考步骤三）。

步骤五：配置 IPSec 变换集（Bundle）

RouterA:

```
create ipsec sas=1 key=isakmp prot=esp enc=des hasha=sha
```

```
create ipsec bund=1 key=isakmp string="1"
```

RouterB:

```
create ipsec sas=1 key=isakmp prot=esp enc=des hasha=sha
```

```
create ipsec bund=1 key=isakmp string="1"
```

在两台路由器上配置的安全协议是 ESP，加密方式是 DES，认证方式是 SHA。

步骤六：配置 IPSec 策略

RouterA:

```
create ipsec pol="isakmp" int=eth0 ac=permit
```

```
set ipsec pol="isakmp" lp=500 rp=500
```

```
create ipsec pol="lan2lan" int=eth0 ac=ipsec key=isakmp bund=1 peer=200.200.200.2
```

```
set ipsec pol="lan2lan" lad=192.168.10.0 lma=255.255.255.0 rad=192.168.20.0
```

```
rma=255.255.255.0
```

```
create ipsec pol="internet" int=eth0 ac=permit
```

策略 isakmp 允许端口号为 500 的 isakmp 数据通过；

策略 lan2lan 制定了需要加密的数据；

策略 internet 指定其他的数据不经过 IPSec 加密。在 RouterA（Center）上只有源（本地）地址为 192.168.10.0/24、目的（远端）地址为 192.168.20.0/24 的数据进行 IPSec 的加密，而其他的数据不进行加密，由策略 internet 定义，正常转发。

RouterB:

```
create ipsec pol="isakmp" int=eth0 ac=permit
```

```
set ipsec pol="isakmp" lp=500 rp=500
```

```
create ipsec pol="lan2lan" int=eth0 ac=ipsec key=isakmp bund=1 peer=200.200.200.1
```

```
set ipsec pol="lan2lan" lad=192.168.20.0 lma=255.255.255.0 rad=192.168.10.0  
rma=255.255.255.0
```

```
create ipsec pol="internet" int=eth0 ac=permit
```

在 RouterB（Branch）上只有源地址为 192.168.20.0/24、目的地址为 192.168.10.0/24 的数据进行 IPSec 的加密。

注意：上述配置中，黑斜体部分是两台路由器上配置不同的地方。

配置完成后，使用 `create config=ipsec.cfg` 命令保存配置。

步骤七：启用 IPSec 和 ISAKMP，保存配置

在两台路由器上，使用 `enable isakmp` 和 `enable ipsec` 命令来启用 IPSec VPN。

全部配置完成后，使用 `create config=ipsec.cfg` 命令保存配置。

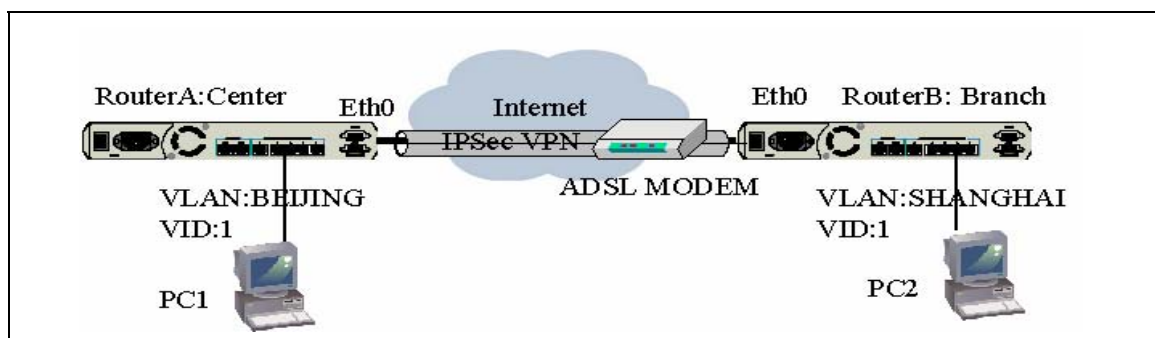
使用 `set config=ipsec.cfg` 来指定启动配置文件。

4.2 点到点 VPN（LAN to LAN VPN）配置实例二

该实例中，中心站点使用固定的 IP 地址；分支站点使用 ADSL 动态分配 IP 地址。在两个站点上都启用了 Firewall 和 NAT。

■ 网络拓扑：

图二



■ IP 地址表:

名称	RouerA	RouterB
	Center	Branch
WAN	Eth0: 200.200.200.1/24	Eth0: Dynamic
LAN	VLAN1: 192.168.10.1/24	VLAN1: 192.168.20.1/24
PC	PC1: 192.168.10.159/24	PC2: 192.168.20.87/24

■ IPSec 策略:

	RouterA	RouterB
路由器间认证方式	Pre-shared Key	Pre-shared Key
Pre-shared Key	123456	123456
安全协议	ESP	ESP
认证方式	SHA1	SHA1
加密方式	DES	DES
IPSec SA 模式	隧道模式	隧道模式
对等体 (Peer) IP	Any	200.200.200.1
对等体主机名	Branch	Center
被加密的数据	192.168.10.0/24	192.168.20.0/24

■ IPSec VPN 配置 (配置步骤与上例相同, 这里给出具体的配置文件和配置命令的说明):

Router A (中心路由器)

```
set system name=center
```

#设置系统的名称

```
add user=secoff pass=secoff priv=security
```

```
set user securedelay=600
```

```
enable sys sec
```

#创建安全用户, 启用安全模式

```
Login user=secoff
```

```
# 使用安全用户登陆，登录后配置 pre-shared KEY

create enco key=1 type=gen val=123456

#设置 pre-shared KEY 值，该配置在 sh conf dyn 命令中是不会显示出来的，使用 sh enco
key=1 命令查看

enable ip

#启用 IP 模块

add ip int=vlan1 ip=192.168.10.1 mask=255.255.255.0

#设置接口 VLAN1 的 IP 地址

add ip int=eth0 ip=200.200.200.1 mask=255.255.255.0

#设置接口 ETH0 的 IP 地址

add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=0.0.0.0

#添加一条默认路由

enable firewall

#启用防火墙功能

create firewall policy=main

#创建一条防火墙的策略，名为 main

enable firewall policy=main icmp_f=all

#允许对防火墙接口进行 PING，建议在配置完成后删除此命令
```

```
add firewall policy=main int=eth0 type=public

add firewall policy=main int=vlan1 type=private

#设置防火墙策略 main 中的 public 接口和 private 接口

add firewall poli=main nat=enhanced int=vlan1 gblin=eth0

# Firewall NAT 的配置，将来自 VLAN1 的私有地址都转换为 ETH0 的 IP 地址

add firewall poli=main ru=1 ac=allo int=eth0 prot=udp po=500 ip=200.200.200.1
gblip=200.200.200.1 gblp=500

# 添加防火墙规则 1，允许 IKE 的数据包通过防火墙，ISAKMP 使用的是 UDP 端口 500

add firewall poli=main ru=3 ac=non int=eth0 prot=ALL
ip=192.168.10.1-192.168.10.254 enc=ips

# 防火墙规则 3，设定从外部端口进入访问 192.168.10.0/24 网段的 IPSec 加密流量不
执行 NAT 功能

add firewall poli=main ru=10 ac=non int=vlan1 prot=ALL
ip=192.168.10.1-192.168.10.254

set firewall poli=main ru=10 rem=192.168.20.1-192.168.20.254

# 指定了从 192.168.10.0/24 网段到 192.168.20.0/24 网段的数据流量不执行 NAT 功能

create isakmp policy=centerkey peer=any key=1

# 创建名为 centerkey 的策略，由于对端路由器 Branch 为动态获得 IP 地址，所以 peer
参数为 any；使用 Pre-shared KEY1

set isakmp policy=centerkey sendd=true setc=true
```

#设置这条策略的一些参数

```
create ipsec sas=1 key=isakmp prot=esp enc=des hasha=sha
```

#配置的安全协议是 ESP，加密方式是 DES，认证方式是 SHA，使用 isakmp 进行密钥管理

```
create ipsec bund=1 key=isakmp string="1"
```

```
create ipsec pol="isakmp" int=eth0 ac=permit
```

```
set ipsec pol="isakmp" lp=500 rp=500 tra=udp
```

#创建一条名为 isakmp 的 IPSec 策略，action 为 permit，设置策略 isakmp 的参数，这里 lp 和 rp 都是 500，因为 isakmp 使用的是 UDP 端口 500。

```
create ipsec pol="lan2lan" int=eth0 ac=ipsec key=isakmp bund=1 peer=dynamic
```

#创建名为 lan2lan 的策略，进行 IPSec 加密。由于对端路由器 Branch 动态获得 IP 地址，所以 peer 参数为 dynamic

```
set ipsec pol="lan2lan" lad=192.168.10.0 lma=255.255.255.0 rad=192.168.20.0  
rma=255.255.255.0
```

#设置策略 lan2lan 的需要进行 IPSec 加密的数据

```
create ipsec pol="internet" int=eth0 ac=permit
```

#配置策略 internet，允许其他经过 eth0，不符合 IPSec 加密策略的数据通过

```
enable isakmp
```

#启用 isakmp

```
enable ipsec
```

```
#启用 ipsec
```

Router B（分支路由器）

```
set system name=branch
```

```
add user=secoff pass=secoff priv=security
```

```
set user securedelay=600
```

```
enable sys sec
```

```
# 创建安全用户，启用安全模式
```

```
login user=secoff
```

```
# 使用安全用户身份登录路由器，进行 IPSec VPN 的配置
```

```
create enco key=1 type=gen val=123456
```

```
# 设置 pre-shared KEY 值，该配置在 sh conf dyn 命令中是不会显示出来的，使用 sh  
enco key=1 命令查看
```

```
create ppp=0 over=eth1-any
```

```
set ppp=0 bap=off iprequest=on username=tester password=test
```

```
set ppp=0 over=eth1-any lqr=off echo=10 idle=on
```

```
# 创建一个 pppoe 的拨号连接，用于 ADSL 拨号连接，该 ADSL 将会由流量自动触发拨  
号
```

```
enable ip

enable ip remote

add ip int=vlan1 ip=192.168.20.1 mask=255.255.255.0

add ip int=ppp0 ip=0.0.0.0

add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

# PPP 接口地址从 ISP 端获得

enable firewall

create firewall policy=main

enable firewall policy=main icmp_f=all

add firewall policy=main int=ppp0 type=public

add firewall policy=main int=vlan1 type=private

add firewall poli=main nat=enhanced int=vlan1 gblin=ppp0

add firewall poli=main ru=3 ac=non int=ppp0 prot=ALL
ip=192.168.20.1-192.168.20.254 enc=ips

add firewall poli=main ru=10 ac=non int=vlan1 prot=ALL
ip=192.168.20.1-192.168.20.254

set firewall poli=main ru=10 rem=192.168.10.1-192.168.10.254

#以上为防火墙的配置，配置命令的讲解同 Router1，注意正确设置策略中的本地地址和
远端地址
```

```
create isakmp policy=centerkey peer=200.200.200.1 key=1

# 由于对端为固定 IP 地址，所以这里一定要正确的配置对端 IP 地址 200.200.200.1

set isakmp policy=centerkey sendd=true setc=true

# 以上为 isakmp 的配置

create ipsec sas=1 key=isakmp prot=esp enc=des hash=sha

create ipsec bund=1 key=isakmp string="1"

create ipsec pol="isakmp" int=ppp0 ac=permit

set ipsec pol="isakmp" lp=500 rp=500 tra=udp

# 允许 isakmp 的数据通过，isakmp 使用的是 UDP 端口 500

create ipsec pol="lan2lan" int=ppp0 ac=ipsec key=isakmp bund=1
peer=200.200.200.1

set ipsec pol="lan2lan" lad=192.168.20.0 lma=255.255.255.0 rad=192.168.10.0
rma=255.255.255.0

# 配置策略 lan2lan，对端为固定 IP 地址 200.200.200.1，设置本地和对端需要加密的
网段

create ipsec pol="internet" int=ppp0 ac=permit

enable isakmp

enable ipsec
```

5. 验证和排错

从 Branch 的局域网中(192.168.20.0/24)的一台主机 PC2 Ping Center (192.168.10.0/24)中的一台主机（必须为匹配 IPSec 策略中制定的需要 IPSEec 加密源和目的地址的数据，才可以建立 ISAKMP 和 IPSec 的连接）。

连接建立后使用下面的命令来查看建立的 ISAKMP 和 IPSec 的 SA:

show isakmp sa

```
SecOff > sh isa sa
```

SA Id	PeerAddress	EncA.	HashA.	Bytes	Seconds

1	200.200.200.2	DES	SHA	-/-	86400/75600/2806

show ipsec sa

```
SecOff > sh ips sa
```

SA Id	Policy	Bundle	State	Protocol	OutSPI	InSPI

1	lan2lan	1	Valid	ESP	661560017	3206031938

如果没有看到上述成功建立的 IPSec SA，可以考虑如下排错：

- 在开始前，最好再仔细检查一遍当然运行的配置，使用 **sh config dyn** 命令。
- “IP local” 参数最好保持缺省值，否则可能会影响 ISAKMP 的协商。可以使用 **sh ip inter** 命令查看，使用 **set ip local** 命令修改。
- 要确定流量是否被加密，最好先使用 **sh log** 命令检查系统日志中的 ISAKMP 协商相关条目。ISAKMP 协商是分几个阶段的，可以在 Log 中看到过程以及成功完成的记录。如果没有看到相关记录或者只有协商初始记录没有一个完成的协商阶段，那么很有可能是配置错误或者是 ISAKMP 的协商信息对端节点没有接收。如果配置正确，使用 **sh fire event** 命令

检查对端节点发送过来的流量记录。另外，也可以使用 **sh isakmp sa** 和 **sh ipsec sa** 命令来确认 ISAKMP 和 IPSEC。

- 可以检查计数器来检查流量是否被加密。如前面例子中的配置，ping 对端节点，检查命令 **sh ipsec poli=to_hq count** 的输出，重点查看 “outProcessDone” 和 “inProcessDone”。
- 可以使用 debug 模式来检查。由于 debug 信息较多，推荐一步步的使用。首先可以使用 **ena isakmp debug=state**，接下来使用 **ena isakmp debug=trace**。

关于安奈特（Allied Telesyn）

安奈特（Allied Telesyn）作为全球知名的网络产品和解决方案供应商，拥有遍布世界各地的 200 多个公司和分支机构。自 1987 年成立以来，安奈特专注于为用户提供高安全性、高可靠性、易于管理、易于维护、易于升级的网络系统解决方案。

公司在世界各地设立了十余个强大的研发机构，时刻跟踪最新的科技进步成果，了解客户的需求，及时推出性能优异、契合需求的全系列产品，包括从接入、汇聚、核心到传输的以太网交换机、路由器、电信综合接入平台、介质转换器、VoIP 产品以及高性能操作系统和网络管理平台。安奈特自成立以来一直保持稳定的高增长态势，成为全球发展最快的高科技公司之一。

1999 年，安奈特在北京成立了安奈特（中国）网络有限公司。2002 年在东莞设立了全资工厂，还在全国各大区增设了办事处，并进一步完善了技术服务体系、认证培训体系和渠道运营体系，以便更好地为中国客户服务，满足不同行业和领域客户需求。

欲知详情，请致电安奈特公司及其各分支机构，或访问 www.alliedtelesyn.com.cn

北京（中国总部及北方区办事处）

负责地区：东北三省、北京、内蒙古、天津、河北、山西、山东、河南、陕西、甘肃、青海

地址：北京市朝阳区朝外大街 16 号中国人寿大厦 1007-1009 室

邮编：100020 电话：(010)85252299 传真：(010)85252298

上海（华东区办事处）

负责地区：上海、江苏、安徽、浙江、湖北、江西

地址：上海市南京西路 1168 号中信泰富广场 3405 室

邮编：200041 电话：(021)52984245/46/47 传真：(021)52984239

广州（华南区办事处）

负责地区：广东、广西、海南、福建、湖南

地址：广州市天河北路 233 号中信广场 1102 室

邮编：510613 电话：(020)38911922 传真：(020)38911303

成都（华西区办事处）

负责地区：四川、重庆、贵州、云南、西藏、新疆、宁夏

地址：四川省成都市顺城大街 308 号冠城广场 19 层 H 座

邮编：610017 电话：(028)86527190 传真：(028)86527193

香港（安奈特北亚区总部）

负责地区：香港、澳门、台湾、韩国

地址：香港官塘官塘道 418 号创纪之城 5 期东亚银行中心 18 楼 1812-1816 室

电话：(00852)22636566 传真：(00852) 27568130 / 23180720

USA Headquarters:

19800 North Creek Pkwy, Suite 200, Bothell, WA 98011, USA

Tel: 800.424.4284 Fax: 425.481.3895

European Headquarters: Via Motta 24, 6830 Chiasso, Switzerland

(Corporate) Tel: (+41) 91 697.69.00 Fax: (+41) 91 697.69.11

(European Sales) Tel: (+39) 02 414.112.1 Fax: (+39) 02 414.112.61