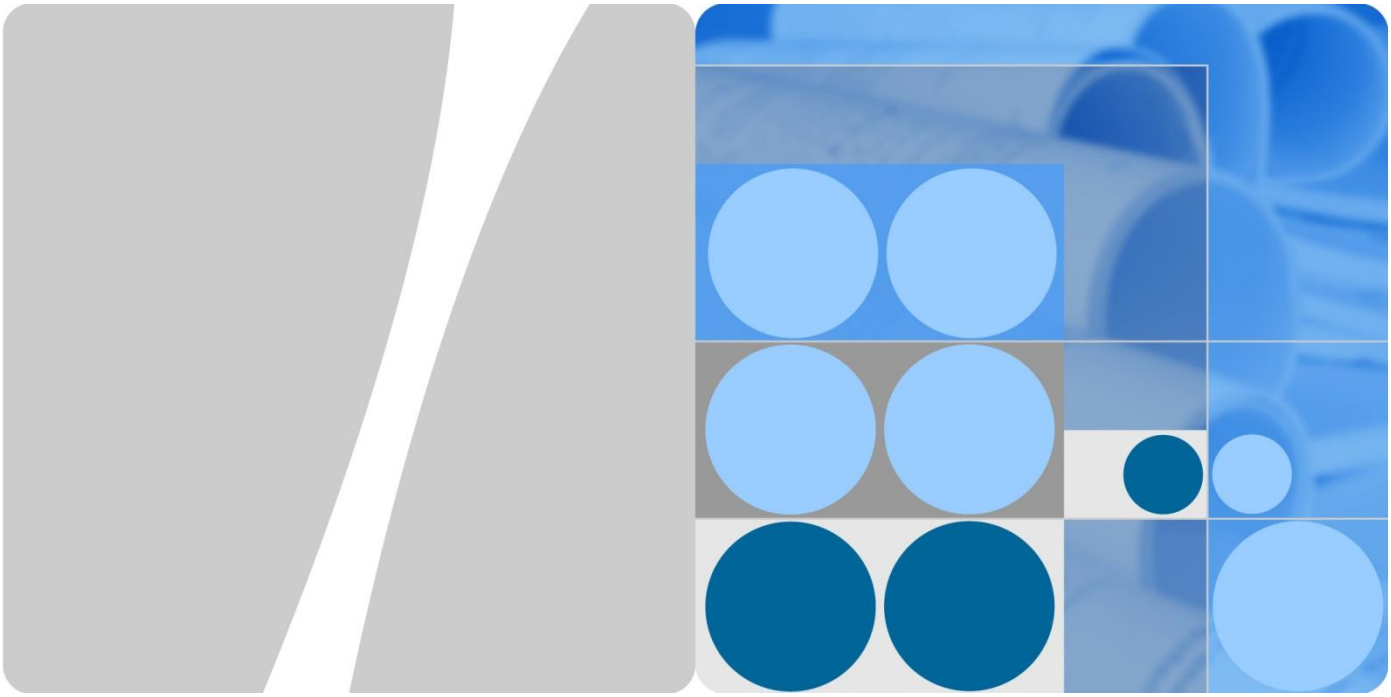


eSight

V300R001C10

IPSec VPN 特性技术白皮书

文档版本 01

发布日期 2013-12-10

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

前 言

概述

本文档通过对 eSight IPSec VPN 的解决方案和应用场景等方面的描述，帮助用户了解 IPSec VPN 的使用场景与使用方法。

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
 说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2013-12-10)

第一次正式发布。

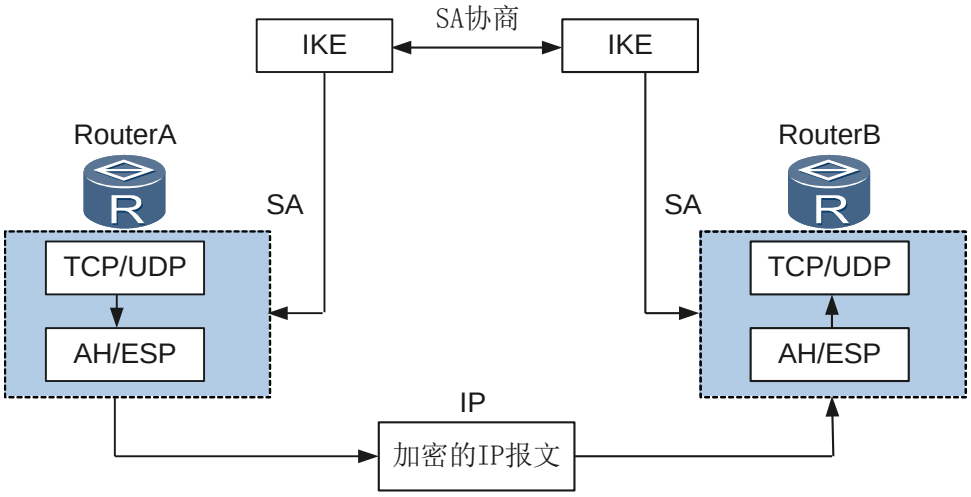
目 录

1 执行摘要

IPSec（Internet Protocol Security）协议族是 IETF（Internet Engineering Task Force）制定的一系列协议，它为 IP 数据包提供了高质量的、基于密码学的安全传输特性。特定的通信双方在 IP 层通过加密与数据源认证等方式，保证 IP 数据报在网络上传输的私有性、完整性和防重放。

- 私有性（Confidentiality）指对用户数据进行加密保护，用密文的形式传送。
- 完整性（Data integrity）指对接收的数据进行认证，以判定报文是否被篡改。
- 防重放（Anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

图1-1 IPSec 的 SA 协商图



IPSec 协议族示意框架说明如上图所示，IPSec 通过认证头 AH（Authentication Header）和封装安全载荷 ESP（Encapsulating Security Payload）这两个安全协议来实现 IP 数据包的安全传送；因特网密钥交换协议 IKE（Internet Key Exchange）提供密钥协商、建立和维护安全联盟的服务，以简化 IPSec 的部署和使用。

- AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。发送端对 IP 头的不变部分和 IP 净荷进行离散运算，生成一个摘要字段；接收端根据接收的 IP 报文，对报文重新计算摘要字段，通过摘要字段的比较，判别报文在网络传输期间是否被篡改。AH 认证头协议没有对 IP 净荷提供加密操作。
- ESP 封装安全载荷协议：除提供 AH 认证头协议的所有功能之外，还可对 IP 报文净荷进行加密。ESP 协议允许对 IP 报文净荷进行加密和认证、只加密或者只认证，ESP 没有对 IP 头的内容进行保护。
- IKE 因特网密钥交换协议：完成 IPSec 通信对等体间的安全联盟 SA(Security Association)协商，协商出对等体间数据安全传输需要的认证算法、加密算法和对应的密钥。

说明

- AH 和 ESP 可以单独使用，也可以同时使用。AH 和 ESP 同时使用时，报文在 IPSec 安全转换时，先进行 ESP 封装，再进行 AH 封装；IPSec 解封装时，先进行 AH 解封装，再进行 ESP 解封装。
- IKE 密钥交换协商并不是必须的，IPSec 所使用的策略和算法等也可以手工配置。

1.4 目的

在 IP 网络的传输中，绝大部分数据的内容都是明文传输的，这样就会存在很多潜在的危险，比如：密码、银行账户的信息被窃取；用户的身份被冒充等。网络中部署 IPSec 后，可对传输的 IP 数据进行保护处理，降低信息泄漏的风险。

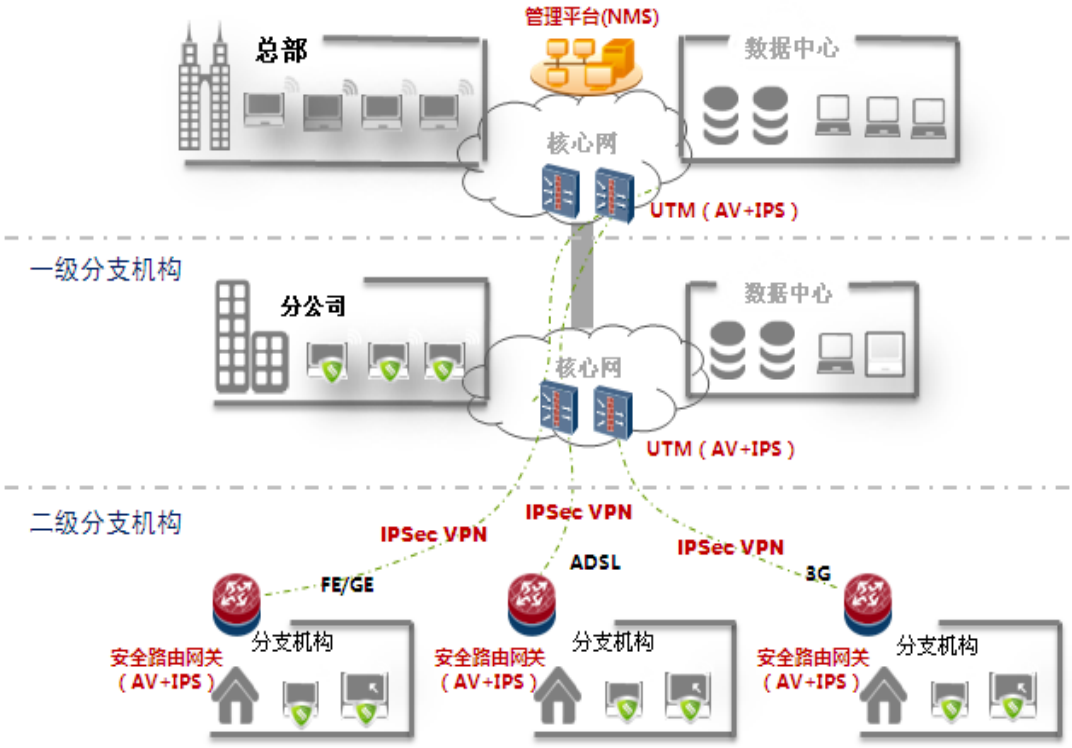
1.5 受益

- 用户业务数据在 IP 网络传输时，减少了泄漏和被窃听的风险，保障了用户业务传输的安全。
- 减少用户在各级应用层自部署 TLS 等安全特性的开销，节约用户业务部署成本。

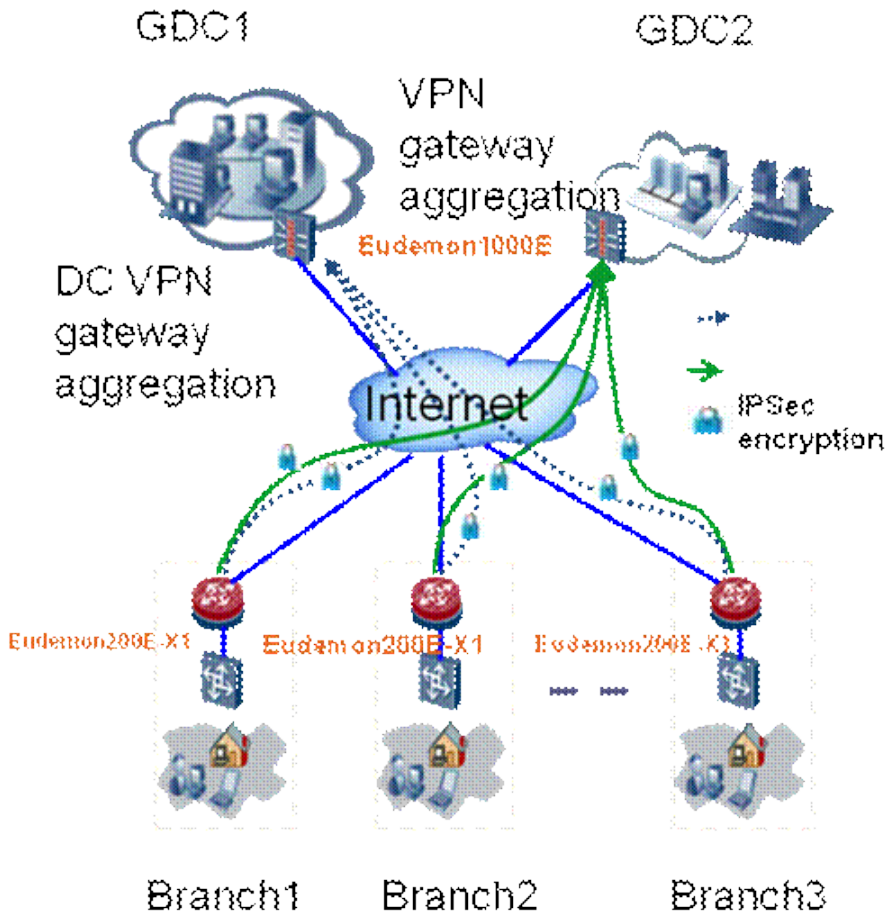
1.6 组网场景

1.6.1 安全纵向网

华为针对企业生产，办公，营销业务信息化发展，为企业客户提出了基于业务的纵向 VPN 安全互联的解决方案。通过在总部，以及各级分支纵向网络中部署安全网关，实现多级分支机构之间，分支机构与总部之间 VPN 安全互联。彻底解决一直困扰业务发展的通信链路可靠性、安全性问题，保障关键业务数据传输都采用专业 VPN 加密。下图为安全纵向网场景，分支机构与上层机构星型组网，使用 IPSec VPN 进行安全保护。



下图为方案设计，总部使用两台 Eudemong1000E 作为 IPSec 中心端，各分支节点部署 Eudemon200E-X1 与总部进行 Site-Site IPSec VPN 连接，使用 PKI 进行认证。同时通过安装 IPSec VPN 管理组件帮助用户实现 VPN 管理。



2 简介

IPSec VPN 组件直观友好、简单易用的图形管理界面，简化了管理员的维护操作。支持自动发现和构建 VPN 拓扑，直观查看 VPN 通道状态、通道流量情况、VPN 设备的运行情况等。能够快速定位网络故障，为解决问题赢得时间。

3 解决方案

3.1 IPSec VPN 管理客户痛点问题

IPSec VPN 专业技术学习难度大，业务容易出现故障，IPSec VPN 配置参数繁多、命令多，人工进行排障很困难，因而导致维护人员难以承担其日常维护，而依赖于厂家技术支持工程师。

客户使用 IPSec VPN 网络承载了业务数据，保证了数据的安全，但无法保证业务稳定与畅通。网络设备断电、IPSec VPN 配置参数有误、路由不通等，导致业务中断后，事后由业务部门感知到业务不能办理时，才汇报故障情况到网络维护部门后才得知可能是网络的原因。维护人员不能第一时间感知由网络原因而导致的业务中断，业务中断时间越长，对客户的损失越大。

痛点给客户带来了强烈冲突：网络部门提供网络维护服务质量低但难以自行完成；客户的业务部门因业务中断后的恢复时间长而痛苦、抱怨。

3.2 产品亮点

维护人员快速上手，轻松维护 IPSec VPN 网络，为承载在 IPSec VPN 上的关键业务的稳定运行保驾护航，只需简单的两步，就可以看到想要的操作结果：

1 一次性快速发现全网业务。

2 打开 IPSec VPN 业务监控拓扑图或 IPSec VPN 业务监控管理列表，即可开始监控全网 IPSec VPN 业务。

告警实时通知拓扑图、列表颜色动态变化，声音、短信、邮件传递到网络维护工程师，他只需完成诊断操作，根据诊断结果即可以排除网络故障。

呈现 VPN 流量趋势情况，掌握业务丢包等质量信息。

3.3 解决方案整体介绍

为了提高用户对 VPN 业务的监控效率，及时发现并定位故障，详细的方案如下：

1 用户在通过命令行或者智能配置工具在网络中部署业务。

2 用户通过 eSight 网管将网络中部署的业务发现到网管，进行监控。

3 用户通过网管监控业务的告警、运行状态、业务性能。

4 用户通过概览信息页面帮助用户掌握 IPSec VPN 整体运维情况。

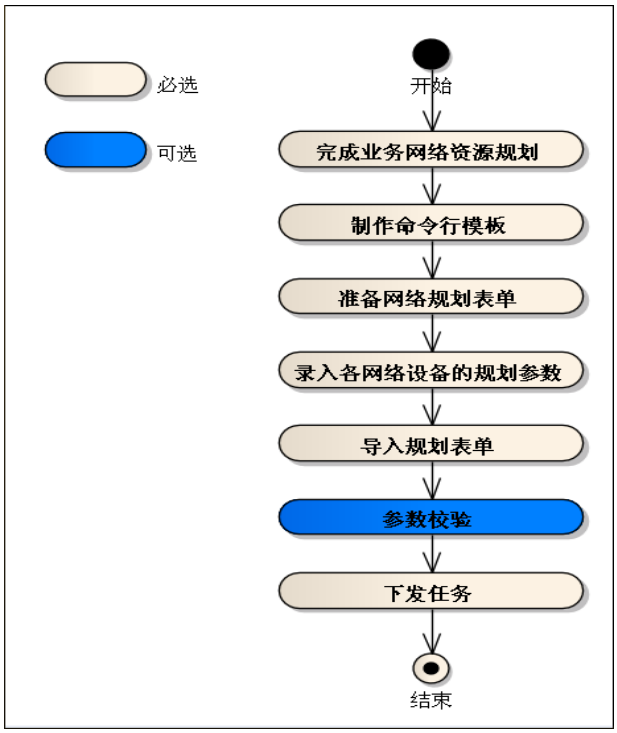
5 用户通过上述手段对业务进行监控，如果发现业务有故障，可通过快速诊断定位业务的故障原因和故障点。

3.4 关键技术点介绍

3.4.1 通过智能工具部署业务

在企业网中，对于 IPSec 业务的部署涉及到大量的策略下发，而很多设备的配置基本是类似的，因此可以通过 eSight 网管提供的具有批量部署功能的智能工具下发业务。

通过智能配置工具完成业务部署操作流程如下：



图表 1 利用智能配置工具部署业务流程图

每个步骤的工作如下：

Step1：完成网络资源规划。用户根据实际业务规划，完成对设备 IP 地址、接口 IP 地址、IPSec 策略、IKE 提议、IKE peer、IPSec 提议、ACL 规划。

Step2：制作命令行模板。根据局点实际组网，制作 IPSec 策略、IKE 提议、IKE peer、IPSec 提议、ACL 模板。

Step3：准备网络规划表单。用户根据当前网络设备支持的设备类型和要部署的命令，准备规划表单。

Step4：录入各网络设备的规划参数。将第一步规划网络资源的数据作为参数录入相应的规划表单，作为命令行参数对应的值。

Step5：导入规划表单。导入上一步已经录入参数的规划表单。

Step6：参数校验（可选）。将规划表单的命令行下发设备，校验参数的合法性。

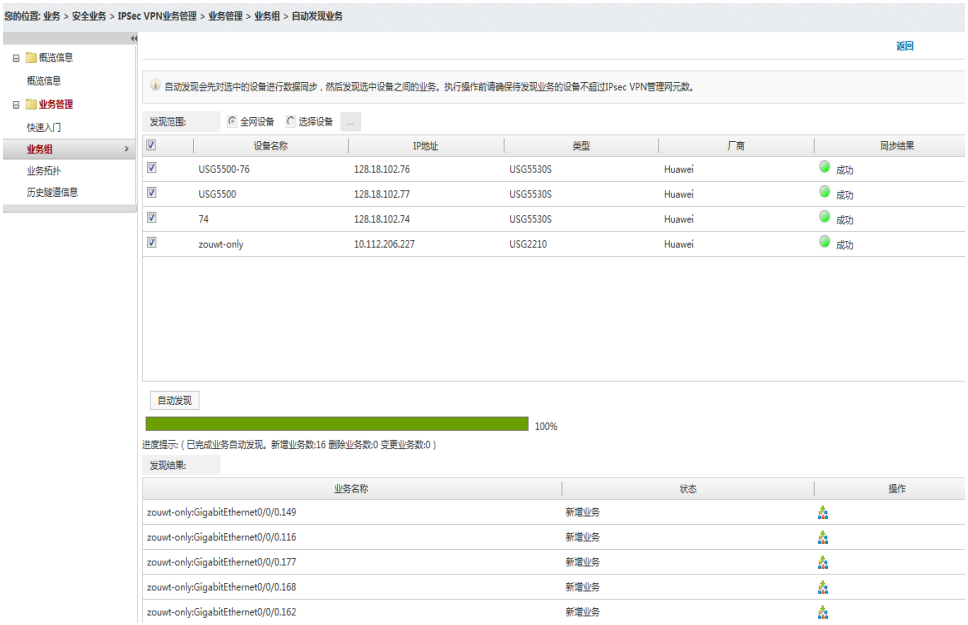
Step7：下发任务。下发规划表单配置完成的命令行参数，完成业务的部署。

3.4.2 业务自动发现

eSight 提供 IPSec 业务自动发现功能，可以将现网中已经存在的 IPSec 业务发现到网管。

如下为 IPSec 业务管理自动发现界面，提供对业务发现设备范围的选择。用户可根据不同的组网场景选择不同的设备范围来发现。

图3-1 业务自动发现界面



发现功能分为两个步骤：

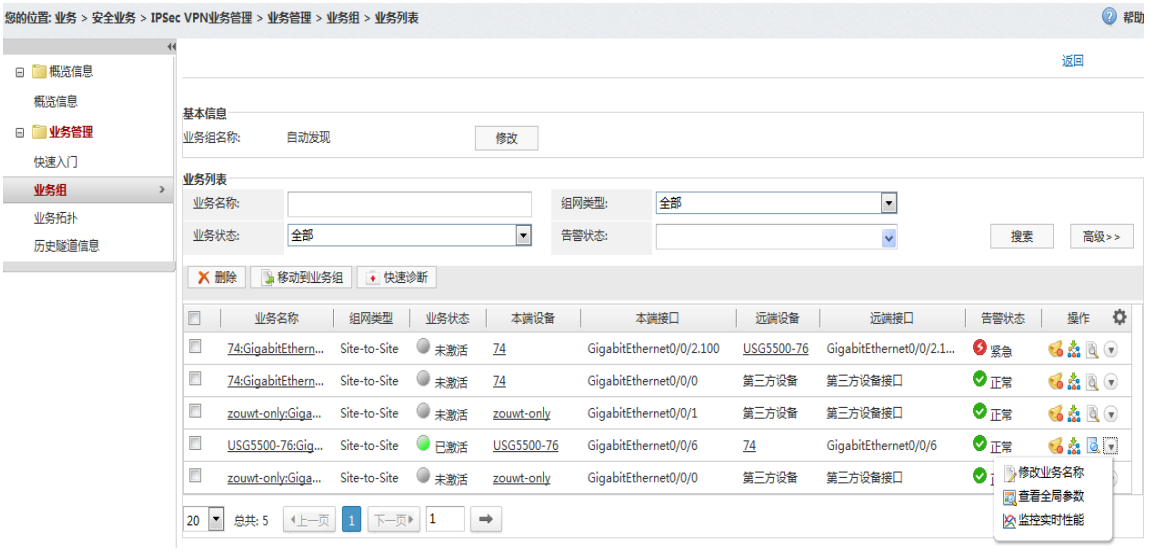
第一，设备同步，通过 telnet 命令登录到设备，获取设备上 IPSec 配置，此时要保证网管配置 telnet 参数。

第二，发现业务，通过配置比对将现网中存在的 IPSec 业务发现到网管上。此时要保证 license 充足，否则无法还原。

还原过程将网络上设备已经绑定在接口的 policy 信息进行配对，当发现设备 B 接口上绑定的 policy 中 peer 指向另一设备 A，并且设备 A 接口绑定的 policy 中 peer 指向设备 B，将其还原至网管。发现过程中不匹配 propose、ACL 信息。

3.4.3 业务列表展示

图3-2 IPSec 业务展示



展示当前可管理的 IPSec 业务列表，列表字段解释如下，

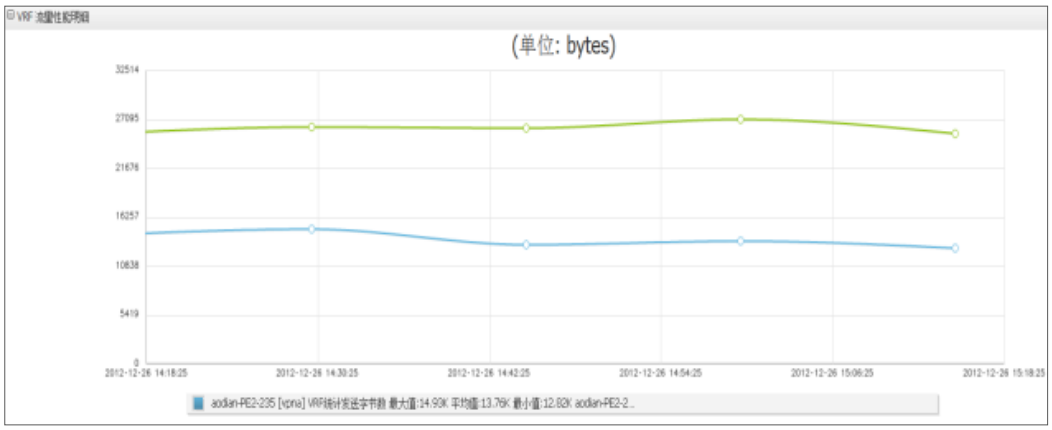
业务状态：已激活表示存在 IPSec 业务流量，未激活表示业务上没有流量。

告警状态：展示当前与业务相关的告警最高级别。当前统计的告警有，link-up/down 告警、设备离线、性能阈值告警。

功能操作解释如下，

查看性能指标：查看已存在业务性能指标，主要监控 IPSec 隧道出入方向流量/速率、丢包数等信息。

图3-3 IPSec 性能展示



查看业务配置：可以查看单条 IPSec 业务配置信息。

查看业务全局参数：查看业务两端设备全局参数。

修改名称：发现至网管的业务名称为业务两端设备名称加端口名称的组合，可以通过手工修改的方式将业务名称修改得更直观。

查看隧道信息：查看隧道两端 IPSec SA 信息。

3.4.4 快速诊断

提供从不同的方面对业务的故障进行定位的功能，如果业务出现故障，通过诊断功能，可以检查配置完整性、接口运行状态、业务绑定状态、加密数据流匹配情况、路由可达情况、业务协商情况。

诊断功能由网管向设备发下 IPSec 业务诊断命令，诊断命令如下：

根据对端地址进行 IPSec 协商诊断；

diagnose ipsec peer *[peer-address]*

设备通过各种维度进行 IPSec 协商分析，最终提供协商结果。

图3-4 IPSec VPN 快速诊断

3.4.5 历史隧道信息

通过历史隧道信息，可以查看已管理 IPSec 隧道建立、删除、中断记录。

图3-5 历史隧道信息

在监控业务过程中发现某条业务是未激活的，可在历史隧道信息中查看该业务是否曾被激活过，若从未激活过，则建议通过诊断功能查看该业务配置是否正常。

业务中断也可以查看业务历史记录，查找业务中断规律。

图3-6 历史隧道详细信息

3.4.6 查看隧道信息

查看隧道信息可以查看已激活 IPSec 业务隧道 SA 详细信息，包括协商方式、加密方式、入出方向流量信息，以及数据流加密等信息。

图3-7 查看隧道信息

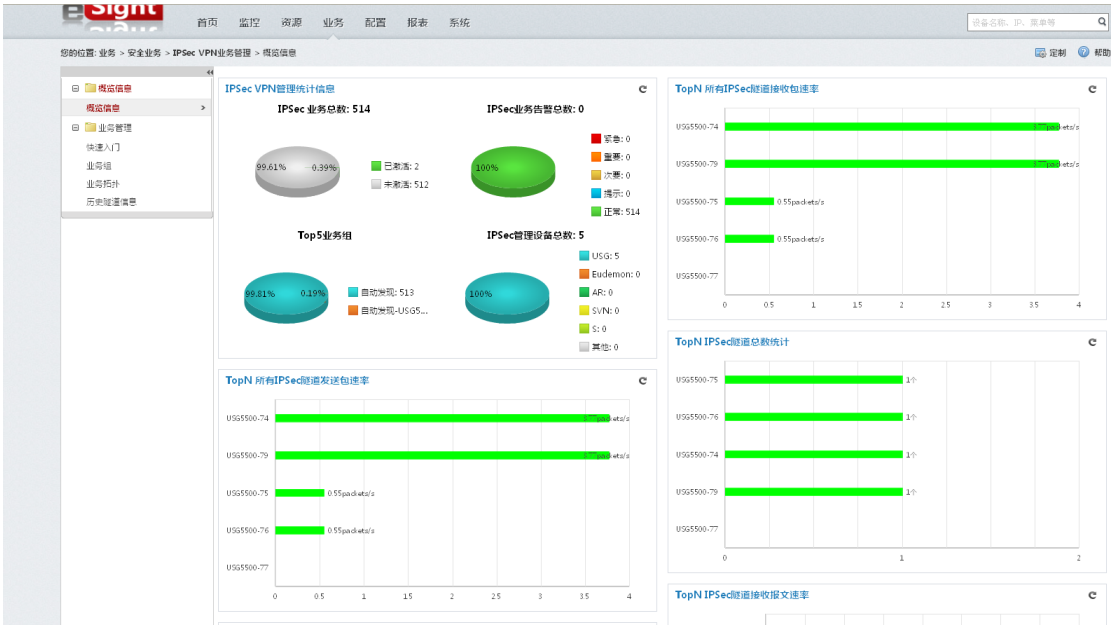
3.4.7 性能采集

在业务自动发现之后，激活的 IPSec 业务可以进行业务性能采集，对 IPSec 隧道接收、发送报文数、速率，接收、发送丢包数进行统计。统计用户使用业务特征，为网络优化、扩容提供准确信息。

3.4.8 概览信息

通过 IPSecVPN 概览信息可以全局监控 IPSecVPN 业务的整体情况，包括：IPSec 隧道总数、设备全局与 IPSec 隧道的接收与发送包速率/报文速率/丢包率、IPSec 隧道远程接入用户数、业务告警列表等监控信息。

图3-8 IPSec VPN 概览信息



3.4.9 功能约束

3.4.9.1 适用设备类型约束

设备	设备类型	设备版本
交换机	S9700	V200R001C00/V200R002C00
AR	AR1200	V200R001C00/V2R3C00/V2R3C01
	AR2200	V200R001C00/V2R3C00/V2R3C01
	AR3200	V200R001C00/V2R3C00/V2R3C01
	AR150	V200R002C00/V2R3C00/V2R3C01
	AR200	V200R002C00/V2R3C00/V2R3C01
Eudemon	Eudemon200E-B	V300R001C00/V100R005C00/V100R002C00
	Eudemon200E-BW	V300R001C00/V100R005C00
	Eudemon200E-X2 Eudemon200E-X2W Eudemon200E-X1 Eudemon200E-X1AW Eudemon200E-X1AGW-W Eudemon200E-X1AGW-C	V300R001C00
	Eudemon200E-X1W Eudemon200E-X3	V100R005C00 V300R001C00

设备	设备类型	设备版本
	Eudemon200E-X5 Eudemon200E-X5DC Eudemon200E-X6 Eudemon200E-X6DC Eudemon200E-X7	
USG	USG2160 USG2160W USG2130 USG2130W	V300R001C00 V100R005C00 V100R003C01 V100R002C01
	USG2160BSR USG2160BSR-W USG2130BSR USG2130BSR-W USG2120BSR	V300R001C00 V100R005C00 V100R003C01
	USG2160HSR-W USG2160HSR USG2130HSR USG2130HSR-W	V300R001C00 V100R005C00
	USG2110-F USG2110-F-W USG2110-A-W USG2110-A-GW-W USG2110-A-GW-C	V100R003C03 V100R005C00 V300R001
SVN	SVN3000	V100R002C02
	SVN2230 SVN2260 SVN5530 SVN5560	V200R001C00 V200R001C01 V200R002C00
	SVN5300	V200R001C00
	SVN5530-C1 SVN5530-C3	V200R001C01 V200R002C00

3.5 典型应用

3.5.1 业务自动发现

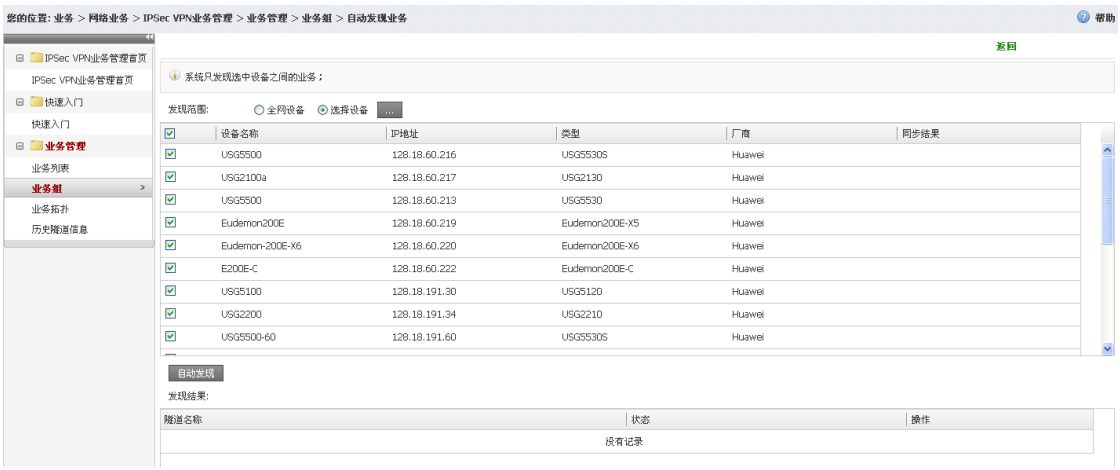
将网络上部署的业务发现到网管，网管对发现上来的业务进行监控。

例如 HUB-Spoke 组网，用户选择 HUB-Spoke 组网中所有设备（包括中心、分支机构设备），用户点击“自动发现”按钮，系统进行自动发现操作。业务自动发现操作包括如下两个过程：

1 设备同步：系统将设备上的和 VPN 业务有关的配置信息同步到网管。

2 业务发现：系统根据同步到网管的设备配置信息发现业务，根据发现的结果将业务分为新增业务（自动发现操作新发现的业务）以及删除业务（业务在设备中不存在，系统根据此判断将此业务从网管删除）

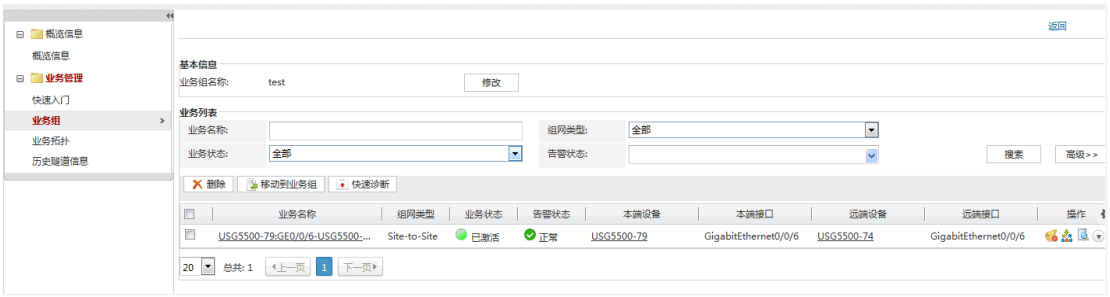
图3-9 业务自动发现



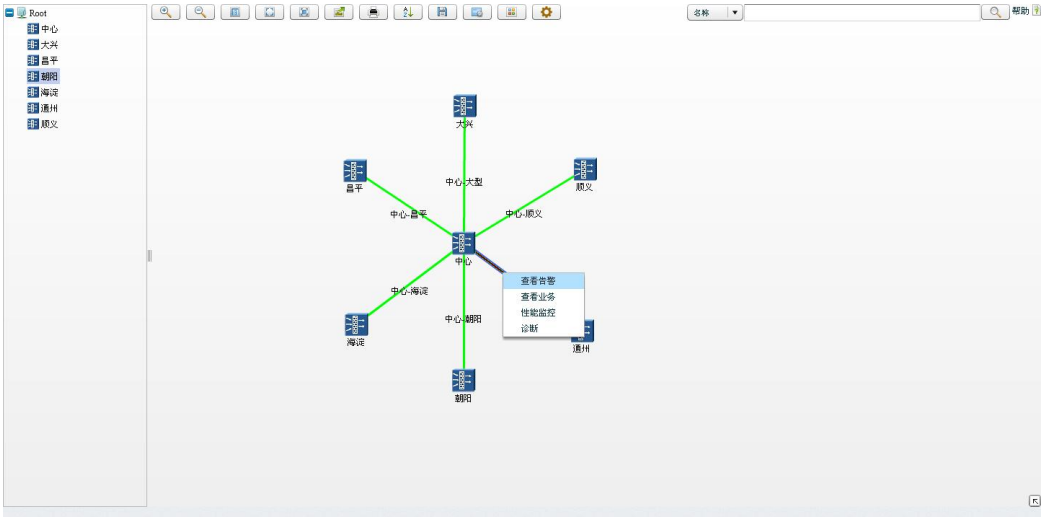
3.5.2 告警监控和运行状态监控

用户可以方便的通过业务列表和业务拓扑能够看到当前业务的告警的最高级别，业务拓扑中能够看到当前业务的告警发生在哪台设备上，并能够看到 IPSec VPN 运行状态。

图3-10 业务拓扑



图表 2 业务列表



用户从业务列表可以直接跳转到当前告警的界面，查看与当前业务有关设备的具体的告警信息。

图3-11 告警列表

3.5.3 快速诊断

发现业务无法激活、VPN 故障，可以通过快速诊断查看具体业务不能正常使用详细原因。下图为故障诊断的流程图，“失败”表示测试结果为不连通。

图3-12 快速诊断

4 结论

eSight Secure Center 支持对华为网络安全设备的集中策略管理，可以满足访问控制策略、内容安全策略、上网行为控制集中管理等多种应用场景。

通过部署 eSight Secure Center，可以降低 IT 系统的维护成本，增强对华为安全设备集中配置和统一管理的能力。

5 缩略语表

表5-1 缩略语清单

英文缩写	英文全称	中文全称
UTM	Unified Threat Management	统一威胁管理