文章编号:1671-4598(2024)11-0080-07 DOI:10.16526/j.cnki.11-4762/tp.2024.11.011 中图分类号:TP206+.1 文献标识码:A

IPsec 产品自动化测试系统设计

罗 晋,骆 超,赵 祺,周华明
(中国电子科集团公司 第30研究所,成都 610041)

摘要:在向着IP化发展的通信网络中,IPsec产品作为确保IP业务机密性、完整性的重要手段,其自身的可靠性尤为重要;传统的IPsec产品测试方法往往带来可观的人力、物力、时间成本,且难以避免人工执行引入的误差;为了在降低投入的同时,提高IPsec产品的可靠性和稳定性,研发了一种IPsec产品自动化测试系统,采用分层架构将物理环境动态抽象为软件功能,通过集成测试工具、测试仪表,并结合自动化执行技术、测试用例组合技术,提高系统的测试能力、测试效率、扩展能力,具备高效、高可靠、高准确的特点,具备较高实用价值。

关键词:IPsec产品;自动化测试;用例库;测试脚本;执行机

Design of Automatic Testing System for IPsec Products

LUO Jin, LUO Chao, ZHAO Qi, ZHOU Huaming
(The 30th Institute of CETC, Chengdu 610041, China)

Abstract: In the development of internet protocol (IP) based communication networks, internet protocol security (IPsec) products are taken as an important means to ensure the confidentiality and integrity of IP services, which is of particular importance to the reliability of IPsec products themselves. Traditional testing methods for IPsec products often have the shortages of huge human, material, and time costs, and it is difficult to avoid errors introduced by manual operation. In order to improve the reliability and stability of IPsec products while reducing investment, an IPsec product automation testing system is developed. The physical environment is dynamically abstracted into software functions by using a layered architecture. By integrating testing tools and instruments, and combining automation technology and test case combination technology, the system improves the testing capability, efficiency, and scalability, with the characteristics of high efficiency, reliability, accuracy, and practical value.

Keywords: IPsec products; automatic testing; testing case library; test script; execution machine

0 引言

互联网协议安全(IPsec, internet protocol security)[1]是一种通过对IP协议的分组进行加密和认证来保护IP协议的网络传输协议簇。IPsec提供一种点对多点的IP数据加密认证服务,当其服务可靠时,能够确保用户IP业务的机密性、完整性、认证性等;反之,当其服务不可靠时,不仅不能起到对用户IP业务的保护作用,甚至可能影响到用户的基本通信,因此,IPsec设计实现的可靠性尤为重要。IPsec产品是一种实施了IPsec的网关/终端类产品,通过对进出其保护子网的IP业务实施加解密,确保用户敏感数据在公共IP网络上传输的机密性、完整性、认证性。由于其承担了其内网侧整个保护子网/宿主终端的加密认证服务,相应的,对其可靠性则提出了更高的要求。

IPsec产品服务可靠性的提高,设计保证固然重要,但IPsec产品应用于复杂多样的网络环境中,要确保其在各类网络环境中均能够高效可靠的运行,必然也需要经历一个反复测试,反复迭代的过程。

为了提高IPsec产品在网络中运行的可靠性,必然需要对IPsec产品的功能/性能做出严格和全面的测试,而传统的测试方法无法满足海量业务测试点的测试效率,且大量的重复性操作在带来可观的人力成本、物力成本、时间成本之外,也增加了因人工执行引入误差的概率。因此,设计一套针对IPsec产品的自动化测试系统,需求尤为迫切。

基于以上需求,本文提出一种IPsec产品自动化测试系统,实现对IPsec产品服务全面、高效、高可靠性、高准确性的功能、性能测试,对提高IPsec产品的质量具有重要的意义。

1 IPsec产品测试现状

1.1 当前测试方法局限性分析

当前针对IPsec产品执行的功能、性能测试主要通过人工操作方式执行测试用例,并通过目检的方式判断用例执行结果的正确性。首先,在参数配置方面,针对IPsec产品的测试,除网络环境搭建、基础网络参数配置外,还涉及大量直接影响互通正确性的安全策略配置,若完全通过人工配置,难免出现因参数配置错误而带来的通信异常;其次,在用例执行方面,部分测试用例需通过多次执行以验

收稿日期:2024-04-21; **修回日期**:2024-05-29。
基金项目:四川省科技计划项目(2022YFG0172)。
作者简介:罗 晋(1981-),男,硕士,网络安全高级工程师。
引用格式:罗 晋,骆 超,赵 祺,等.IPsec产品自动化测试系统设计[J].计算机测量与控制,2024,32(11):80-86,94.

证功能性能的一致性，人工反复执行重复操作可能在操作层面即引入偏差；再者，在测试持续性方面，人工执行不能达到全天候不间断的时间利用，对于海量用例的多轮迭代，显然无法使测试效率得到最极致的提高。

综上，无论在测试执行的准确率还是效率方面，人工执行均存在较大的局限性，亟需引入自动化测试以改善现状。

1.2　IPsec 产品测试需求分析

IPsec 产品应用于 IP 网络中，其 IPsec 服务作用于所有以 IP 承载的业务。因此，对 IPsec 产品进行测试，不应局限于与其有直接协议处理关系的 2～4 层协议，对于承载其上的各类应用协议，也应进行覆盖，以避免 IPsec 服务的引入对用户业务带来适配性影响。此外，由于 IPsec 的实施会引入协议封装及处理开销，所以对于 IPsec 产品引入的吞吐率及时延开销，也需得到重点关注。业界对于网络协议、网络性能的测试已具备多种成熟的三方工具、测试仪表[2]，因此，对于 IPsec 产品的测试，需将通用的自动化测试与成熟工具、仪表充分结合，设计出一套具有针对性的自动化测试系统。

2　系统方案

2.1　系统设计思路

为更好地保障 IPsec 产品功能、性能测试的完整性和有效性，本文提出的自动化测试系统具备以下五大特性。

1）通用性：可根据被测设备特点及具体测试需求灵活制定单次测试任务的用例集合[3]，适用于多种 IPsec 产品乃至同类网关类产品。

2）扩展性：可在应用过程中不断扩展，支持制定、修改、完善测试用例，对三方工具、测试仪表的集成联动，以全面覆盖设备在各种工况和实网应用场景下的功能、性能测试。

3）高效性：可根据预设参数，在无人值守的情况下准确、快速、高并发、不间断地执行测试用例。

4）追溯性：可自动生成详实的测试日志和测试报告，实现测试过程可追溯。

5）易用性：充分考虑测试人员的使用体验，简化操作，直观呈现，降低使用门槛。

2.2　系统设计难点

IPsec 产品型号多样，虽然其核心功能均是为 IP 业务提供加密认证服务，但不同的 IPsec 产品基于不同的承载平台，不同的产品形态呈现，在速率等级、协商交互流程、协议封装方式，以及对通用网络协议的处理等方面，又各有特点。因此，针对不同 IPsec 产品的特点进行通用性和扩展性设计，是自动化测试系统设计的一大重点和难点。

为了迅速完成大规模的测试任务，IPsec 产品自动化测试系统需支持多任务并行。因此，对多任务的集中规划、调度和监控，降低多任务并行过程中的测试资源冲突风险，是自动化测试系统设计的另一大难点。

2.3　系统架构设计

为适应不同型号的 IPsec 产品测试，提高自动化测试系统通用性和扩展性，将自动化测试系统整体架构进行抽象分层[4]，分为设备层、设备控制层、测试执行层、测试管理层，降低层次间功能耦合，各层次仅关注其特定职责。IPsec 产品自动化测试系统架构如图 1 所示。

1）设备层：

设备层由被测设备、数通网络设备、数据流产生装置等物理设备组成。通过将被测设备、陪试数通网络设备固化形成测试工装，数据流产生装置通过以太网接入测试工装和被测设备构成完整的物理测试环境。

设备层中的物理设备均具备控制接口，设备控制层可通过以太网接口或 RS232 接口对设备层中的物理设备进行控制。

2）设备控制层：

设备控制层是将设备层中的设备以及陪试网络环境抽象[5]为逻辑软件环境。由被测设备管理软件、密码设备配置接口、陪试网络配置接口、数据流产生装置控制接口组成。

设备控制层对上为测试脚本提供控制被测设备和陪试设备的接口，对下实现对被测设备的控制。设备控制层通过调用被测设备配置接口实现对被测设备的控制，通过陪试设备配置接口对陪试设备状态进行查询和配置，同时实现对陪试环境状态的感知。设备控制层还将数据流产生装置的功能封装软件接口，实现对数据流产生装置的数据读取和控制。

3）测试执行层：

测试执行层由测试脚本组成，测试脚本开发人员依据测试用例完成测试脚本开发后在该层部署并执行。该层主要实现测试用例脚本执行，测试用例脚本通过调用设备控制层的被测设备管理软件、数据流产生装置控制接口、陪试网络数通设备配置接口支撑测试用例执行，接收并存储设备控制层上报的执行信息[6]。

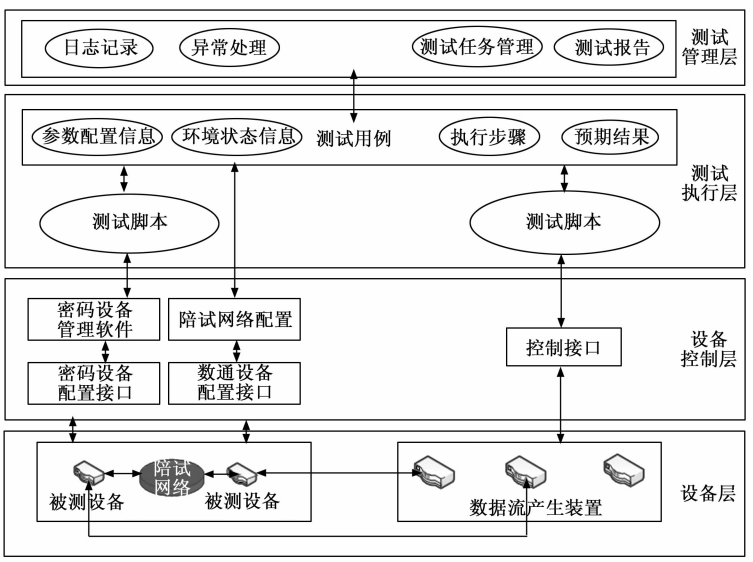

图 1　系统架构示意图

4）测试管理层：

测试管理层是测试执行人员操作的人机接口，主要包含测试用例管理模块、日志模块、测试任务配置模块、测试任务调度模块、测试过程监控模块、测试报告生成模块等功能模块组成。

测试用例管理模块，完成测试用用例的增、删、改、查。

测试任务配置模块，测试执行人员通过该模块创建测试任务，选择需要执行的测试脚本或测试用例，创建测试任务，系统自动将任务分配到当前空闲的各个执行机上执行。

测试过程监控模块，完成对测试任务执行过程的监控，检测测试任务执行情况，保存测试过程中的执行日志，同时监测测试执行进程运行状态。

日志模块收集测试执行层上报的测试脚本日志以及被测设备控制接口调用结果日志，收集陪试网络环境状态信息。

测试报告生成模块将每条测试用例执行结果按照测试报告模板生成测试报告。测试报告分为两类，一类是被测设备检测报告，一类是用例执行 log，用例执行 log 与用例操作步骤强关联，以便测试执行人员定位被测设备故障原因。

3 系统设计与实现

为实现上述通用性、扩展性、高效性、追溯性、易用性等五大特性，本方案结合分层架构展开设计。

IPsec 产品自动化测试系统的核心主要包含两大软件：测试管理层的自动化测试管理软件（简称“ATMS”），该软件部署于测试服务器上，以高度集成的方式实现了测试活动的全面规划、执行监控与结果的深度分析；测试执行层的自动化测试执行软件（简称“ATES”）该软件部署于测试执行机上集成实现测试用例高效执行以及与上下层次间交互。

3.1 设备控制层设计

设备控制层作为 IPsec 产品自动化测试系统中对硬件资源进行逻辑抽象的一层，通过集成 RS232 协议、I^2C 协议、RS485 协议、以太网协议对下层测试设备层的被测设备和配测设备进行控制调度。

集成 RS232[7]接口通信协议，通过该协议与被测设备资源注入接口进行交互，注入被测设备提供服务所需要的密码资源。RS232 作为一种标准通信接口，可通过修改或增加接口交互协议方便快捷地扩展交互功能。

集成 RS485[8]自定义通信协议，进行被测产品的电源控制以及对瞬时功耗、瞬时电流、瞬时电压等数据的读取。同样，RS485 作为一种标准通信接口，也可通过修改或增加接口交互协议实现更多交互功能的快捷扩展。

集成以太网协议对测试仪器和陪测设备进行控制和配置。通过以太网协议与测试仪器建立连接进行业务流量创建、修改、流量统计等功能调用，后续可通过协议扩展进一步扩展功能、性能测试能力。

集成陪测设备控制相关以太网协议，实现下发和读取陪试设备配置参数实现对测试环境的动态感知。

集成 webdriver[9]工具和 request 库，通过本地以太网实现对被测设备身份认证、网络参数配置、安全策略配置等配置管理功能以及日志查询功能。

3.2 测试执行层设计

测试执行层在测试执行机上实现，主要包含测试用例库以及 ATES。

3.2.1 用例库设计

为灵活适应不同 IPsec 产品的测试需求，实现自动化测试用例的通用性和扩展性，对用例库进行了分层分类设计和组合化设计。

用例库将测试用例类型划分为功能测试用例、性能测试用例、稳定性测试用例[10]3 个类别。在功能测试用例中，主要包含配置管理身份验证、网络配置、策略配置、传输模式业务、隧道模式业务等测试用例；性能测试用例中，主要包含吞吐率测试、隧道协商性能、密钥同步性能等；稳定性测试用例中，主要包含加解密稳定性、协商稳定性、管理通道稳定性等。测试用例库[11]结构如图 2 所示。

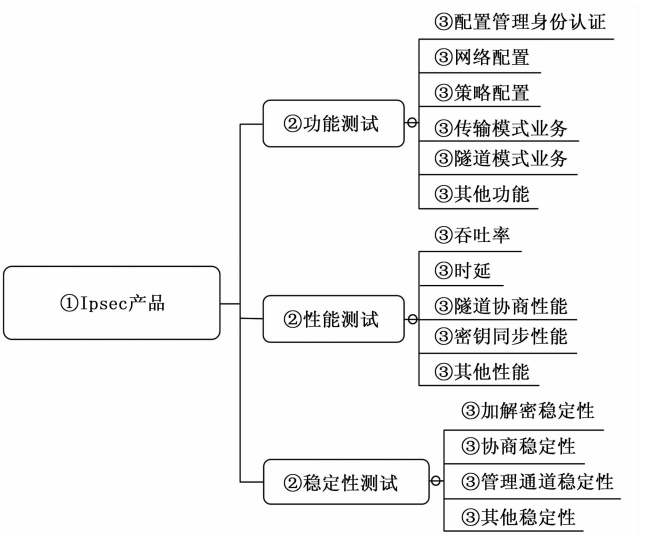

图 2 用例库结构图

在功能测试用例设计方面，不同 IPsec 产品存在业务类功能趋同，管理类功能各异的特点。因此，本系统将功能测试用例进一步划分为业务类功能测试用例和管理类功能测试用例。其中，业务类功能测试用例遵循 RFC 中相关 IP 标准协议进行设计，具备良好的通用性。为实现管理类功能测试用例的复用，则将其进行拆分细化，并为细化后的功能模块提炼“关键字”[12]，以“关键字”驱动[13]相应自动化测试脚本。如此，当需要将测试用例转换为自动化测试脚本时，只需按“搭积木”方式将多个“关键字”对应的自动化测试脚本进行组合，即可完成特定管理类功能测试用例的自动化，而无需重复编写自动化脚本，从而达到自动化测试脚本组合复用的效果[14]。

测试用例组合过程如图 3 所示。

在性能测试用例设计方面，不同 IPsec 产品的性能测试

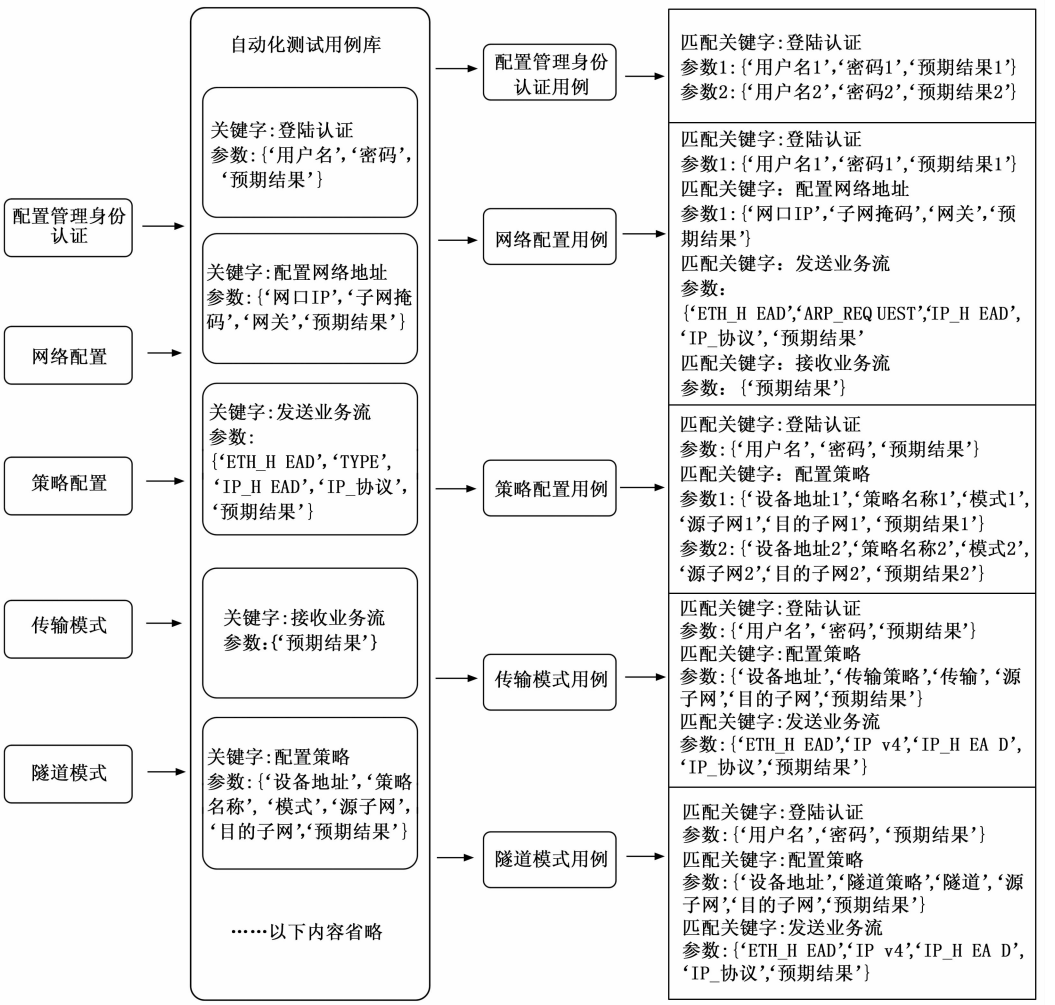

图 3　用例组合过程图

用例测试方法也大都遵循 RFC 标准，主要差异仅在于性能指标数据不同。因此，本方案将测试脚本中产品性能指标数据如包长、测试时长、测试方法、初始速率、最高速率参数化[15]，针对不同 IPsec 产品的测试，仅需将产品型号和性能指标按照特定格式以配置参数的形式传入测试脚本，即可实现产品性能测试用例脚本的高度复用。

在稳定性测试用例设计方面，主要考虑 IPsec 产品在不同应用场景下，一段时间区间内工作的稳定性。通过对 IPsec 产品的应用场景进行分析，本方案将稳定性考核场景主要设定为二层网络场景、三层网络场景、多路协同网络场景等。测试时，只需要将不同型号的产品接入固化好的测试网络场景，并执行相应的稳定性测试用例脚本。二层网络场景稳定性测试拓扑图如图 4 所示，三层网络场景稳定性测试拓扑如图 5 所示，多路协同网络场景稳定性测试拓扑如图 6 所示。

3.2.2　ATES 设计

ATES 主要由指令执行引擎和用例脚本执行引擎组成[16]。

1）指令执行引擎设计：

ATES 与上层测试管理层的 ATMS 之间通过建立 RPC

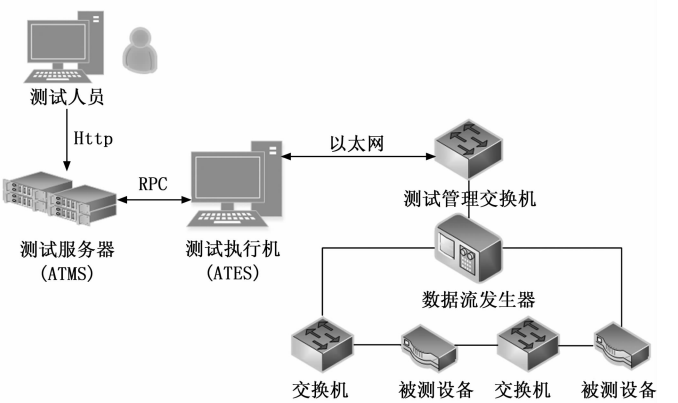

图 4　二层网络场景稳定性测试典型拓扑图

连接进行双向交互，一方面接收 ATMS 下发的任务和控制指令，一方面上报测试执行机状态、上报用例执行日志、上报测试用例执行结果等。

（1）指令接收：

ATES 在接收到 ATMS 下发的指令后，按照一定的机制进行指令接收以及执行，ATES 接收到指令后，首先对指令进行解析，获取数据详细信息如执行测试用例、执行

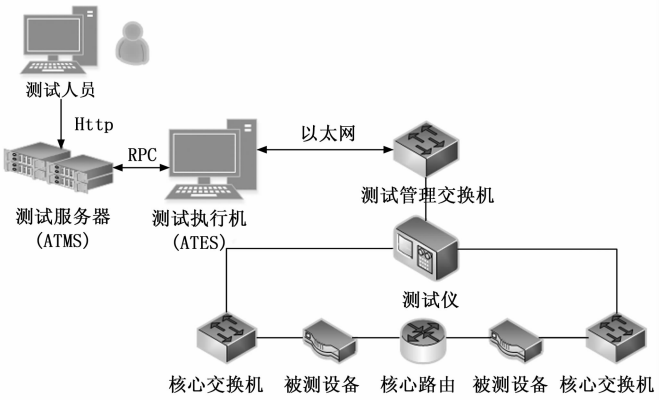

图 5 三层网络场景稳定性测试典型拓扑图

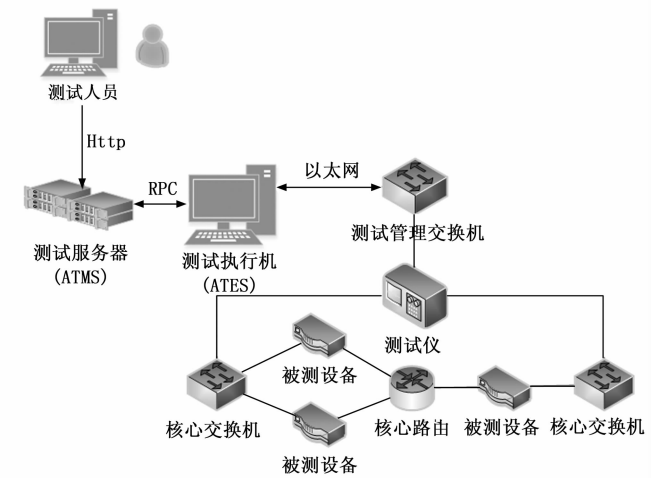

图 6 多路协同网络场景稳定性测试典型拓扑图

测试任务、暂停测试任务、任务状态查询、用例执行结果查询等。同时，在接收到指令后进行指令合法性验证，确保指令符合预设的规则和要求。

（2）指令执行：

ATES 在指令解析和验证通过后，开始执行指令，主要包括加载测试用例、配置测试环境并记录测试过程中的相关信息。

（3）数据上报：

ATES 在调度执行测试用例过程中，按照预设的时间间隔或事件触发的方式向 ATMS 上报测试状态。同时，当每条测试用例执行完毕后 ATES 将执行结果上报给测试管理组件。除基本的测试状态和结果上报外，ATES 还可根据需求进行扩展，支持上报更多数据如当前网络状态、执行机使用状态。

为了提高上报效率，数据上报采用异步上报方式，即 ATES 在收集到一定量的状态或结果信息后在进行批量上报。上报过程中支持对上报数据进行压缩和加密。

2）用例脚本执行引擎设计：

ATES 集成测试用例脚本执行环境（如 Python[17]、Java 等）和测试用例脚本执行引擎。

测试用例脚本开发人员按照模块化原则将每个用例脚本化，将每个用例步骤划分为 1 个模块或函数，每个模块返回相应的测试结果。

集成测试用例脚本执行引擎，用于解析和执行测试测试用例脚本。执行引擎负责读取测试用例脚本，按照其中的指令执行操作，并返回执行结果。

脚本解析：解析测试用例脚本中的语法和指令，确保脚本的正确性。

脚本执行：按照测试脚本中的指令，执行测试操作，如下发/读取被测设备配置、读取测试仪表流量信息、控制测试仪表等。

收集结果：收集测试过程中的日志、用例脚本执行结果以便 ATES 上报这些数据。

3.3 测试管理层设计

测试管理层的核心是 ATMS，ATMS 设计采用前后端分离设计，前端为测试人员提供 UI 接口，后端与所有 ATES 建立并发 RPC 连接实现 ATMS 和 ATES 间数据交互。

3.3.1 ATMS 前端设计

良好的人机界面设计是解决测试工程师实施自动化测试学习成本的关键，系统通过基于 B/S 架构[18]的 ATMS 提供人机界面，界面设计采用 CSS 加 HTML 技术，测试人员通过 web 界面管理测试任务，无需安装相关软件，提高 ATMS 的易用性和跨平台性。人机界面主要包含：测试任务管理界面、测试用例管理界面、执行过程查询界面、执行结果查询界面以及测试报告查阅界面。

如图 7 所示，测试任务管理界面采用图形化方式进行分类统计，能够直观展示待测设备总数、测试完成设备数量、异常设备数量等统计信息。

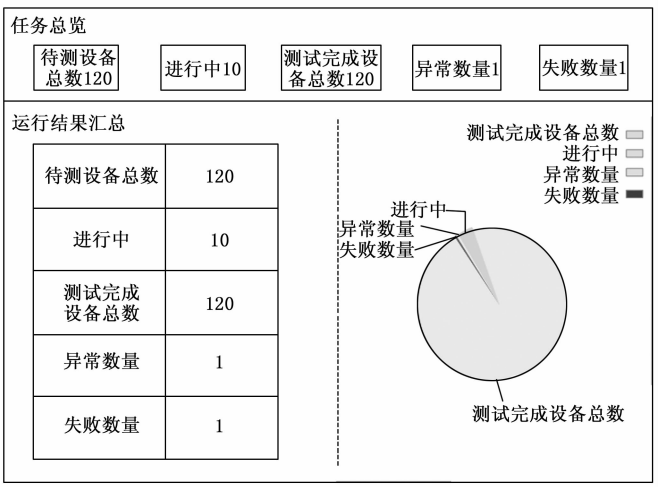

图 7 测试任务管理界面设计

ATMS 中内置了用例库，覆盖 IPsec 产品功能、性能、稳定性等各方面测试需求，并持续根据产品研制、实网应用信息不断迭代、完善。针对特定 IPsec 产品的批量生产，根据验收测试大纲建立了典型测试用例集，可在创建测试任务时快速选择。此外，也可针对其它测试任务从用例库

中灵活选择适用的测试用例。

ATMS 可清晰呈现测试任务的执行过程，供测试人员精确监控测试任务中每一台被测设备的用例执行情况。

测试完成后，系统对执行完成的测试任务中每一台被测设备分别生成规范、详实的电子测试报告，对测试情况进行记录、总结，也可用于支撑检验任务的报告出具。

ATMS 提供良好的人机界面有效缩短用户学习使用系统所需的时间，使得测试工程师能够更快地配置测试场景、执行测试并分析结果，进一步简化复杂的测试流程，提升整个测试生命周期的管理效率和质量控制水平。

3.3.2　ATMS 后端设计

ATMS 作为测试管理的核心，通过集成测试执行机管理功能，监控和调度测试执行层中所有的测试执行机资源，实现对测试任务的统一配置、调度和监控[19]，进而达到降低多任务并行过程中测试资源冲突风险的目的。ATMS 对测试执行机资源的调度包括测试套件的组织、测试用例的分配、测试策略的调整等，并可根据测试任务的优先级调整测试任务对测试执行机资源的配比，从而保障关键测试任务得到优先处理。

ATMS 集成结果聚合与分析功能，收集从各执行机上报的测试结果和日志，进行整合分析，如通过率统计、性能指标评估、缺陷趋势分析等。测试报告中不仅包含测试通过/失败信息，还包括性能测试数据、资源消耗情况以及可能的故障定位分析，支持以图表、摘要、日志等形式，定制化输出为 PDF、HTML、Excel 等格式的目标文件，确保测试结果的透明度和可追溯性[20]。

ATMS 集成动态管理测试执行机资源的功能，可根据测试需求的波动，自动或手动增加或减少执行机数量，确保测试能力始终与项目需求保持同步。

3.4　典型测试任务执行过程

IPsec 产品自动化测试系统通过测试管理层的 ATMS 建立相关测试任务。

一次典型的自动化测试过程如图 8 所示。

1）测试人员根据测试任务需求在设备层搭建被测设备测试执行环境；

2）通过 ATMS 创建测试任务，录入该批次待测设备信息，选择需要执行的测试用例集，完成测试任务创建；

3）ATMS 配置测试执行机并将选择的测试用例集发送到测试执行机；

4）由测试执行机执行测试任务，测试执行机根据用例脚本调用被测设备控制接口或流量发生器控制执行测试用例，在执行用例过程将测试执行过程日志和执行结果上报给 ATMS。

5）ATMS 根据执行上报的执行结果生成测试报告。

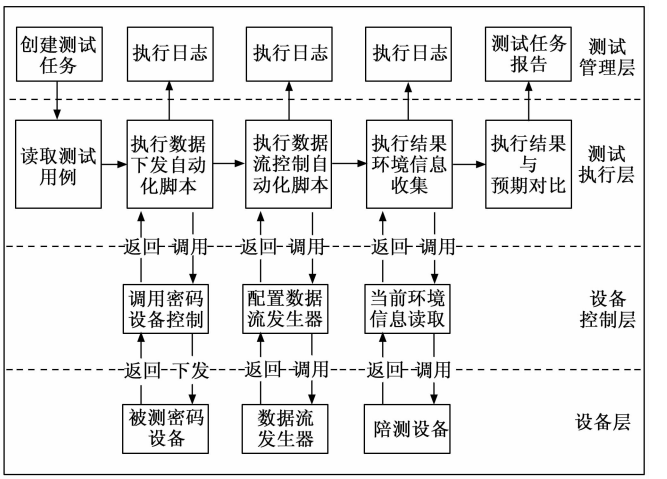

图 8　典型测试任务执行过程示意图

3.5　IPsec 产品典型测试方案设计

IPsec 产品核心旨在确保 IP 业务在传输过程中的机密性、完整性以及高效性。本章节基于 IPsec 产品自动化测试系统对 IPsec 产品加密测试方案进行设计，IPsec 加密测试网络拓扑如图 10 所示。

IPsec 产品加密测试主要包含以下内容。

1）IPsec 产品参数设置：

测试人员通过 ATMS 导入测试用例及用例对应的自动化测试脚本并通过 ATMS 创建测试任务，ATMS 将自动化测试脚本下发测试执行机并控制测试执行机执行自动化测试脚本。

ATES 接收自动化测试脚本并执行，通过调用 RS232 接口下发 IPSec 策略配置，配置加密算法、哈希算法、密钥协商协议。下发完成后通过 RS232 接口读取配置与下发的配置进行比对，将比对结果返回 ATMS。

ATES 继续执行自动化测试脚本，控制测试仪表抓包端口在交换机上抓取被测设备发出的密钥协商报文并进行协议格式比对。通过比对密钥协商报文验证双方是否能够

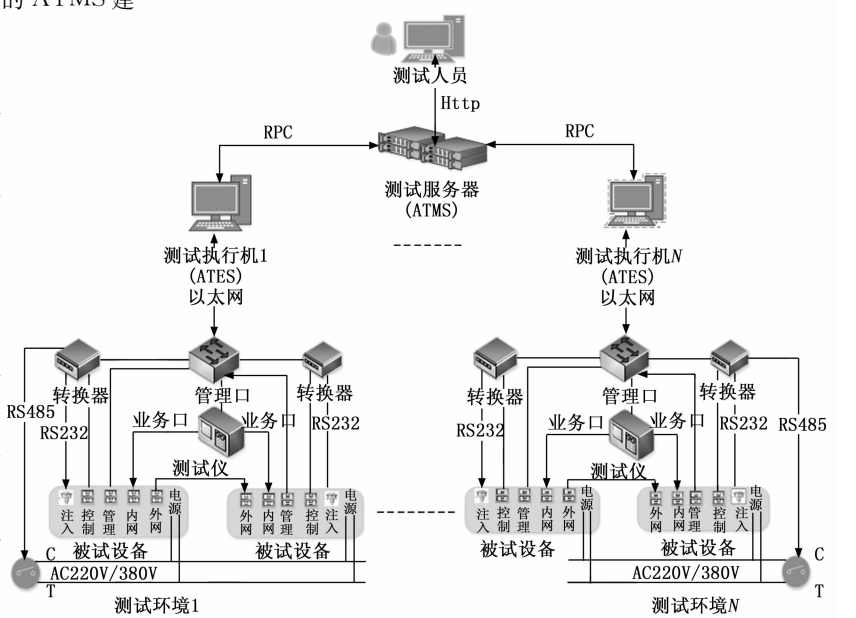

图 9　系统连接拓扑示意图

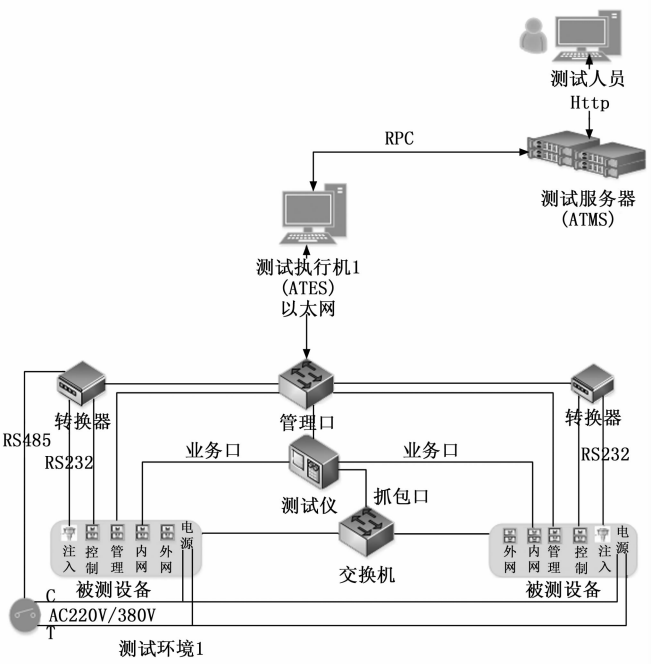

图 10 IPsec 产品典型测试拓扑图

正确建立 SA（Security Association），将比对结果上报给 ATMS。

2）加密有效性验证：

ATES 创建 IP 流量明文并将该明文数据下发给测试仪表，ATES 通过控制测试仪表明文数据发送端口发送明文数据并控制测试仪表抓包端口在被测设备外网口交换机上抓取密文数据，ATES 将抓取到的密文数据和明文数据进行对比，检查封装安全载荷（ESP，encapsulate security payload）封装的数据包是否符合预期，验证加密算法的实际执行效果将结果上报给 ATMS。

ATES 控制测试仪表抓包端口在密钥轮换周期前抓取指定的密钥协商报文，并进行协议格式比对，验证 SA 是否发生变化；另一方面 ATES 控制测试仪表发送明文数据并抓取密文数据对明文和密文进行比对以及密文格式比对验证密钥轮换机制是否按预期工作。

3）认证与完整性验证：

数据包完整性检查测试：ATES 将测试仪表抓取到的 ESP 数据包，依次修改 ESP 头部信息、数据包密文内容，认证码等字段；ATES 控制测试仪表抓包口将篡改后的数据发送给交换机通过交换机转发给被测设备。同时，ATES 监控测试仪表业务口接收到的明文包数量验证篡改包是否被丢弃，从而验证被测设备是否对数据包进行完整性检查，并将结果上报给 ATMS。

4）实时性验证：

ATES 通过控制测试仪表业务口采用二分法按照 RFC2544 发送不同包长度、不同速率的明文数据经过被测设备加解密后的吞吐率和时延数据，验证被测设备加解密的实时性，并将吞吐率和时延数据上报给 ATMS。

4 系统应用效果

基于本方案设计的 IPsec 产品自动化测试系统，使用 10 套 IPsec 产品搭建测试环境，创建并执行 IPSec 产品典型测试任务，覆盖网络地址配置、五元组包过滤、IPv4 传输模式业务互通、IPv4 隧道模式业务互通、IPv6 传输模式业务互通、IPv6 隧道模式业务互通等 6 项功能测试用例，开机进入工作状态时间、IPv4 传输模式加密吞吐率、IPv4 隧道模式加密吞吐率、IPv6 传输模式加密吞吐率、IPv6 隧道模式加密吞吐率等 5 项性能测试用例。

将被测 IPsec 产品两两组成一组，采用 IPsec 产品自动化测试原型系统并行执行典型测试任务，总计耗时约 8 小时。为验证该系统的执行效率，通过人工手动方式执行相同测试任务以作对比，耗时约 22 小时。用例执行时间如表 1 所示。

表 1 测试用例执行事件对比

序号	用例执行方式	时间/人时	执行结果
1	人工手动	22	通过
2	自动化执行	8	通过

通过以上对比验证，使用 IPsec 产品自动化测试系统比人工手动方式节约 14 人时，提升效率（22－8）/22×100%≈64%，测试效率明显高于传统人工执行，且执行过程和结果与传统人工执行一致，符合系统设计预期。

5 结束语

本文所提出的 IPsec 产品自动化测试系统，可全天候不间断运行测试，与人工测试对比测试效率提高 64%。IPsec 产品自动化测试系统可实现对不同种类 IPsec 产品的功能性能测试，并能模拟不同实网环境与各种工况，系统操作简便，可实现高效可靠地验证设备是否完成设计需求达到设计目的，给测试工作带来极大助力。

自动化测试是一个全面、需要持续优化的过程，涉及到测试用例的设计、测试脚本的扩展、测试结果的分析等多个环节。随着人工智能、机器学习等技术的成熟，如何将其与本系统结合，以更好地适应和服务复杂多变的产品测试需求，为产品提供更好更高效的测试服务，将是我们下一步研究的核心。

参考文献：

[1] KENT S, SEO K. Security architecture for the internet protocol: RFC4301 [S]. IETF, 2005: 6－10.

[2] 赵 靖. 局域网系统验收测试中网络测试仪的选择 [J]. 山西电子技术, 2015 (2): 61－62.

[3] 蒲卿路, 王月波, 刘 涛, 等. 基于模型的测试用例生成方法 [J]. 计算机测量与控制, 2021, 29 (12): 22－32.

[4] 高 虎. 机载设备驱动软件自动化测试环境框架设计 [J]. 计算机工程与设计, 2018 (4): 992－993.

[5] 骆 超. 一种网络层通信终端设备业务测试自动化实现方法 [P]. 中国: 201911224372. 1, 2019-12-04.

（下转第 94 页）