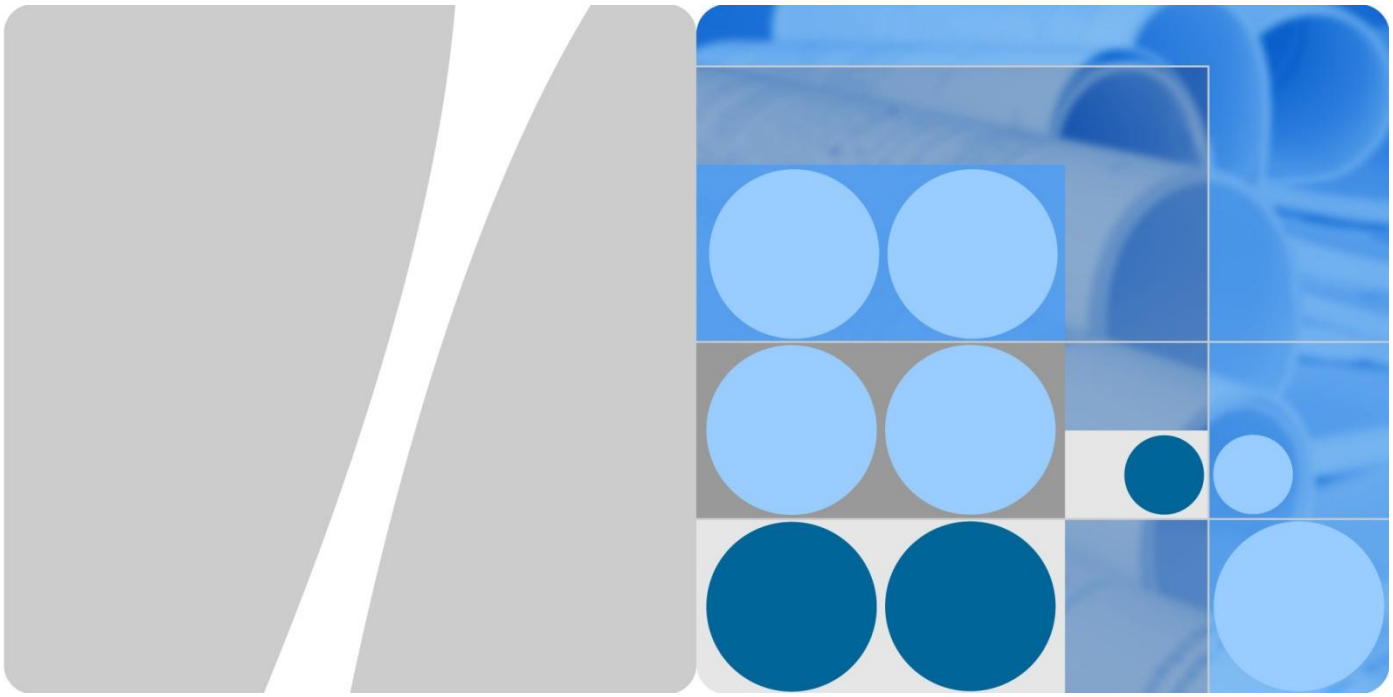


eSight
V300R001C10

Secure Center 特性技术白皮书

文档版本 01

发布日期 2013-12-26

华为技术有限公司

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 Secure Center 的解决方案和应用场景等方面的描述，帮助用户了解 Secure Center 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。
	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。

修改记录

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(2013-12-26)

第一次正式发布。

目 录

1 执行摘要

Secure Center 是对华为安全和网络设备进行集中策略管理的软件系统，主要用于集中管理防火墙、交换机和路由器等设备的安全策略，包括防火墙安全策略配置、入侵防御策略配置、反病毒策略配置、安全策略分析和接入认证策略配置等。

本文档从技术角度上介绍 Secure Center 的功能和解决方案。

2 简介

Secure Center 支持对华为防火墙、交换机和路由器等设备的集中安全策略管理，包括策略配置、策略部署、策略发现、策略分析和策略一致性审计等。在大规模部署华为网络和安全设备的应用场景中，能有效提高策略运维的效率，降低策略运维的成本。

3 解决方案

关于本章

3.1 解决方案整体介绍

Secure Center 能有效管理大规模华为防火墙、交换机和路由器部署环境中设备的安全策略，主要功能包括：

1、 安全策略分析

- 支持对防火墙的安全策略进行冗余分析、风险分析、命中分析和综合分析。

2、 防火墙策略管理

- 支持防火墙安全策略、入侵防御策略和反病毒策略的批量配置和部署；
- 支持集中配置地址集、时间段、服务等公共对象
- 支持虚拟防火墙的管理和基于虚拟防火墙的安全策略配置

3、 交换机策略管理

- 支持交换机接入认证策略批量配置和部署
- 支持集中配置用户组、Radius 服务器组和接入策略模板。
- 支持接入认证策略的一致性审计

4、 AR 策略管理

- 支持域间安全策略的集中配置和批量部署

3.2 关键技术点介绍

3.2.1 策略冗余分析

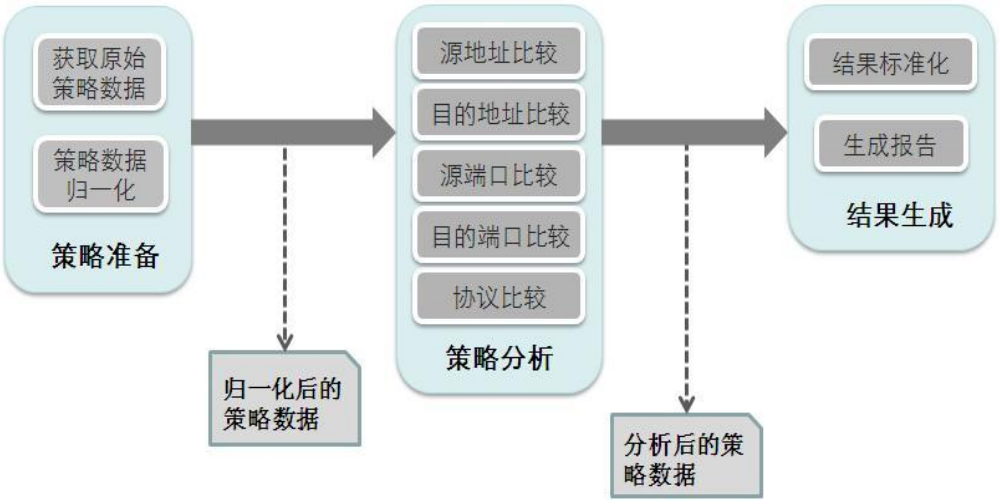
策略冗余分析用于分析防火墙安全策略的冗余情况， 从而帮助管理员发现垃圾策略和无效策略。

策略冗余分析支持从防火墙设备或从系统数据库获取安全策略，从防火墙获取安全策略支持 Telnet/SSH 两种通信方式。

策略数据在冗余分析前需要进行归一化处理，归一化的过程包含了策略对象的扁平化及策略数据标准化。策略数据标准化时，将进行数据值合并，例如将多个 IP 地址范围进行合并。

策略冗余分析按域间对防火墙安全策略进行分组，对每一分组的策略数据两两比较生成策略的冗余关系。

图3-1 策略冗余分析原理



3.2.2 策略风险分析

策略风险分析根据系统预定义或者用户自定义的风险规则对防火墙安全策略进行分析，发现存在风险和不符合企业规定的策略。

策略风险规则支持对于 IP 地址、服务、端口和协议的指定值或数量限制进行定义，用户可以根据企业的需要定义符合企业的风险规则。

图3-2 定义风险规则

策略风险分析时对防火墙所有策略数据采用规则匹配的方式进行分析，策略的风险级别由匹配的风险规则中的最高风险级别决定。

3.3 功能约束

3.3.1 适用设备类型约束

表3-1 设备支持列表

设备分类	设备类型	设备版本
USG 系列		
	USG2110	V300R001C00
	USG2110-F	V300R001C00
	USG2110-F-W	V300R001C00
	USG2110-A-W	V300R001C00
	USG2110-A-GW-W	V300R001C00
	USG2110-A-GW-C	V300R001C00
	USG2110-A-GW-T	V300R001C00
	USG2120BSR	V300R001C00
	USG2130	V300R001C00
	USG2130BSR	V300R001C00
	USG2130HSR	V300R001C00
	USG2130W	V300R001C00
	USG2130BSR-W	V300R001C00

	USG2130HSR-W	V300R001C00
	USG2160	V300R001C00
	USG2160BSR	V300R001C00
	USG2160HSR	V300R001C00
	USG2160W	V300R001C00
	USG2160BSR-W	V300R001C00
	USG2160HSR-W	V300R001C00
	USG2210	V300R001C00
	USG2205BSR	V300R001C00
	USG2205HSR	V300R001C00
	USG2220	V300R001C00
	USG2220BSR	V300R001C00
	USG2220BSR-D	V300R001C00
	USG2220HSR	V300R001C00
	USG2220HSR-D	V300R001C00
	USG2220TSM	V300R001C00
	USG2230	V300R001C00
	USG2250	V300R001C00
	USG2250-D	V300R001C00
	USG2250TSM	V300R001C00
	USG2260	V300R001C00
	USG5120	V300R001C00
	USG5120BSR	V300R001C00
	USG5120BSR-D	V300R001C00
	USG5120-D	V300R001C00
	USG5120HSR	V300R001C00
	USG5150	V300R001C00
	USG5150BSR	V300R001C00
	USG5150HSR	V300R001C00
	USG5160	V300R001C00
	USG5520S	V300R001C00
	USG5530	V300R001C00
	USG5530S	V300R001C00
	USG5550	V300R001C00
	USG5560	V300R001C00
	USG9520	V300R001C00

	USG9560	V300R001C00
	USG9580	V300R001C00
	USG9520	V300R001C01
	USG9560	V300R001C01
	USG9580	V300R001C01
Eudemon 系列		
	Eudemon1000E-X2	V300R001C00
	Eudemon1000E-X2-D	V300R001C00
	Eudemon1000E-X3	V300R001C00
	Eudemon1000E-X5	V300R001C00
	Eudemon1000E-X6	V300R001C00
	Eudemon1000E-X7	V300R001C00
	Eudemon1000E-X7-D	V300R001C00
	Eudemon1000E-X8	V300R001C00
	Eudemon1000E-X8-D	V300R001C00
	Eudemon200E-X1	V100R005C00
	Eudemon200E-X1	V300R001C00
	Eudemon200E-X1W	V300R001C00
	Eudemon200E-X1AW	V300R001C00
	Eudemon200E-X1AGW-W	V300R001C00
	Eudemon200E-X1AGW-C	V300R001C00
	Eudemon200E-X2	V100R005C00
	Eudemon200E-X2	V300R001C00
	Eudemon200E-X2W	V300R001C00
	Eudemon200E-X2NEW	V300R001C00
	Eudemon200E-X2WNEW	V300R001C00
	Eudemon200E-X3	V100R005C00
	Eudemon200E-X3	V300R001C00
	Eudemon200E-X5	V100R005C00
	Eudemon200E-X5	V300R001C00
	Eudemon200E-X5DC	V300R001C00
	Eudemon200E-X6	V100R005C00
	Eudemon200E-X6	V300R001C00
	Eudemon200E-X6DC	V300R001C00
	Eudemon200E-X7	V100R005C00
	Eudemon200E-X7	V300R001C00

	Eudemon200E-B	V300R001C00
	Eudemon200E-BW	V300R001C00
	Eudemon200E-C	V300R001C00
	Eudemon200E-F	V300R001C00
	Eudemon200E-F-D	V300R001C00
	Eudemon8000E-X3	V300R001C00
	Eudemon8000E-X8	V300R001C00
	Eudemon8000E-X16	V300R001C00
	Eudemon8000E-X3	V300R001C01
	Eudemon8000E-X8	V300R001C01
	Eudemon8000E-X16	V300R001C01
AR 路由器		
	AR1220V	V200R005C00
	AR1220L-S	V200R003C01
	AR1220L	V200R003C01
	AR2220	V200R003C01
交换机		
	S5710-28C-EI	V200R003C00SPC300sph0002
	S5710-52C-EI	V200R003C00SPC300sph0002
	S5710-28C-PWR-EI-AC	V200R003C00SPC300sph0002
	S5710-52C-PWR-EI-AC	V200R003C00SPC300sph0002
	S5710-52C-PWR-EI	V200R003C00SPC300sph0002

3.4 典型场景应用

3.4.1 安全策略精简和调优

运维痛点：

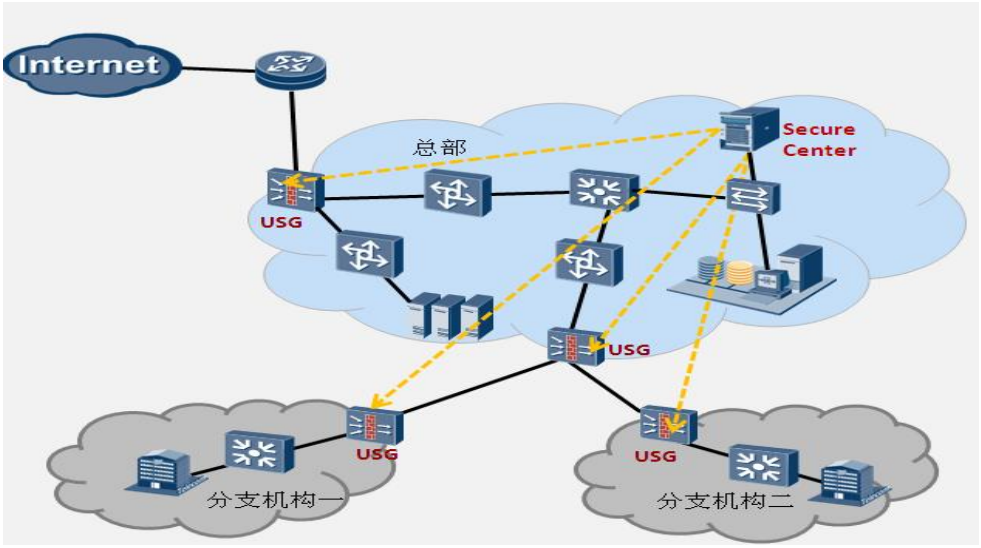
企业网络中部署多台防火墙，防火墙策略比较多，变更频繁，维护困难，易出错。

防火墙策略垃圾策略/无效策略多，影响防火墙效率。

解决方案：

企业网络部署 eSight Secure Center 安全策略管理组件，对于华为防火墙的安全策略进行冗余分析和命中分析，识别出现网中的垃圾冗余策略和低命中策略，提高防火墙策略的合理性，并提高网络运维效率，简化运维工作。

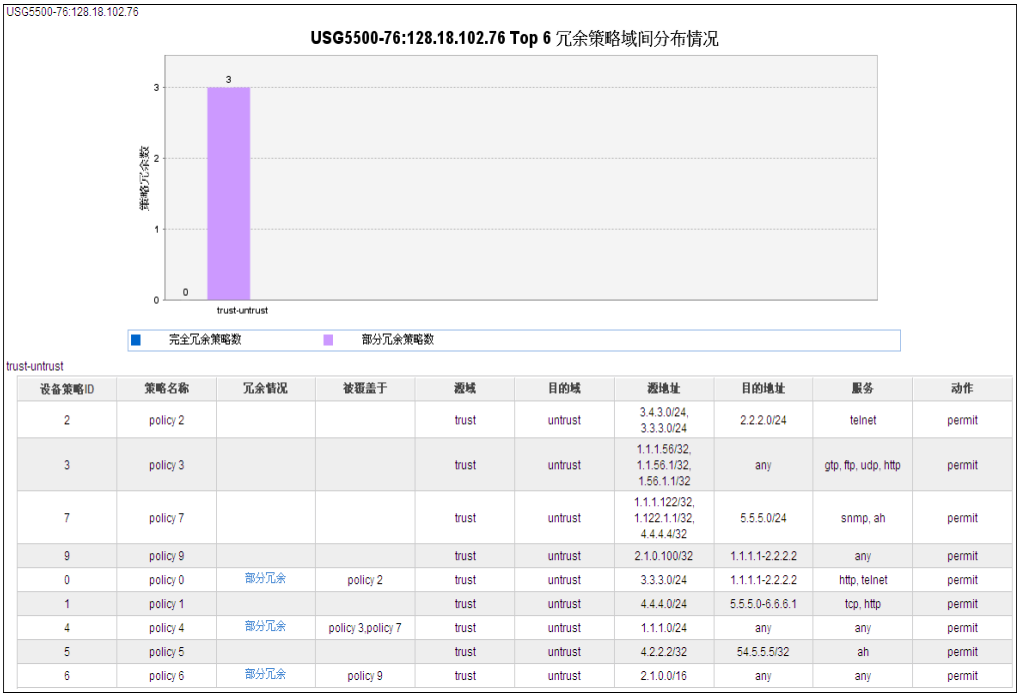
图3-3 安全策略精简和调优



安全管理员通过 eSight Secure Center 配置冗余分析和命中分析任务，手工或者定时触发系统执行分析任务。

通过策略冗余分析，可以识别防火墙设备中的垃圾策略和无效策略；通过策略命中分析，可以识别防火墙未命中的策略。根据冗余分析和命中分析的结果对安全策略进行精简，删除完全冗余和无用策略，避免人为分析出错而导致误删除策略。

图3-4 策略冗余分析结果



trust-untrust

设备策略ID	策略名称	冗余情况	被覆盖于	源域	目的域	源地址	目的地址	服务	动作
2	policy 2			trust	untrust	3.4.3.0/24, 3.3.3.0/24	2.2.2.0/24	telnet	permit
3	policy 3			trust	untrust	1.1.1.56/32, 1.1.56.1/32, 1.56.1.1/32	any	gtp, ftp, udp, http	permit
7	policy 7			trust	untrust	1.1.1.122/32, 1.122.1.1/32, 4.4.4.4/32	5.5.5.0/24	snmp, ah	permit
9	policy 9			trust	untrust	2.1.0.100/32	1.1.1.1-2.2.2.2	any	permit
0	policy 0	部分冗余	policy 2	trust	untrust	3.3.3.0/24	1.1.1.1-2.2.2.2	http, telnet	permit
1	policy 1			trust	untrust	4.4.4.0/24	5.5.5.0-6.6.6.1	tcp, http	permit
4	policy 4	部分冗余	policy 3,policy 7	trust	untrust	1.1.1.0/24	any	any	permit
5	policy 5			trust	untrust	4.2.2.2/32	54.5.5.5/32	ah	permit
6	policy 6	部分冗余	policy 9	trust	untrust	2.1.0.0/16	any	any	permit

通过命中分析，可以识别高命中策略和低命中策略，根据业务和策略命中次数调整策略的优先级顺序，提高防火墙安全策略匹配效率。

图3-5 策略命中分析结果

3.4.2 安全策略风险分析

运维痛点：

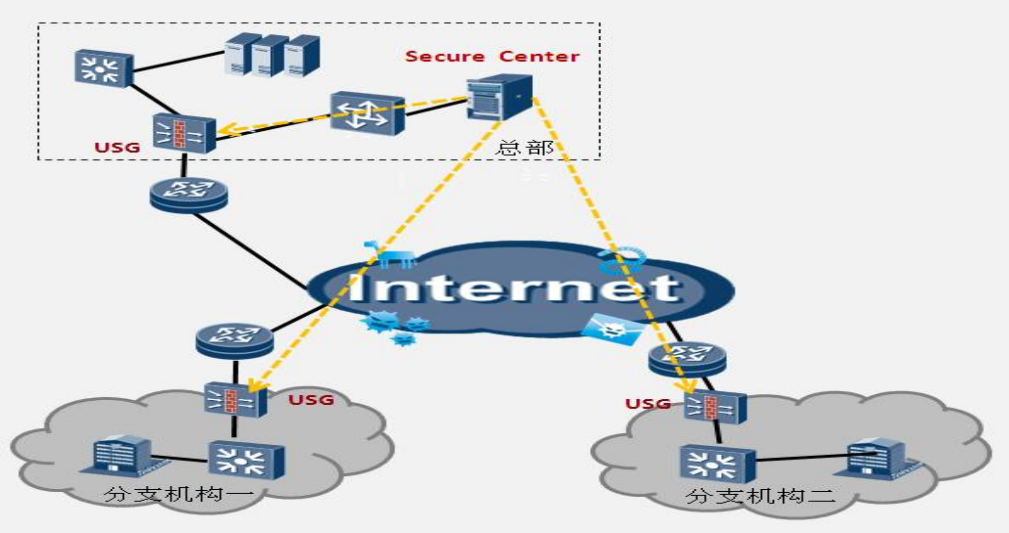
客户对防火墙策略的管理有一定的规范和要求，但无法自动检查不符合要求（例如开了不该开启的端口，网段被放大等）和存在风险的策略 。

出现蠕虫和病毒爆发的情况时，不能快速及时发现有安全漏洞（例如开了蠕虫传播的端口等）的策略。

解决方案：

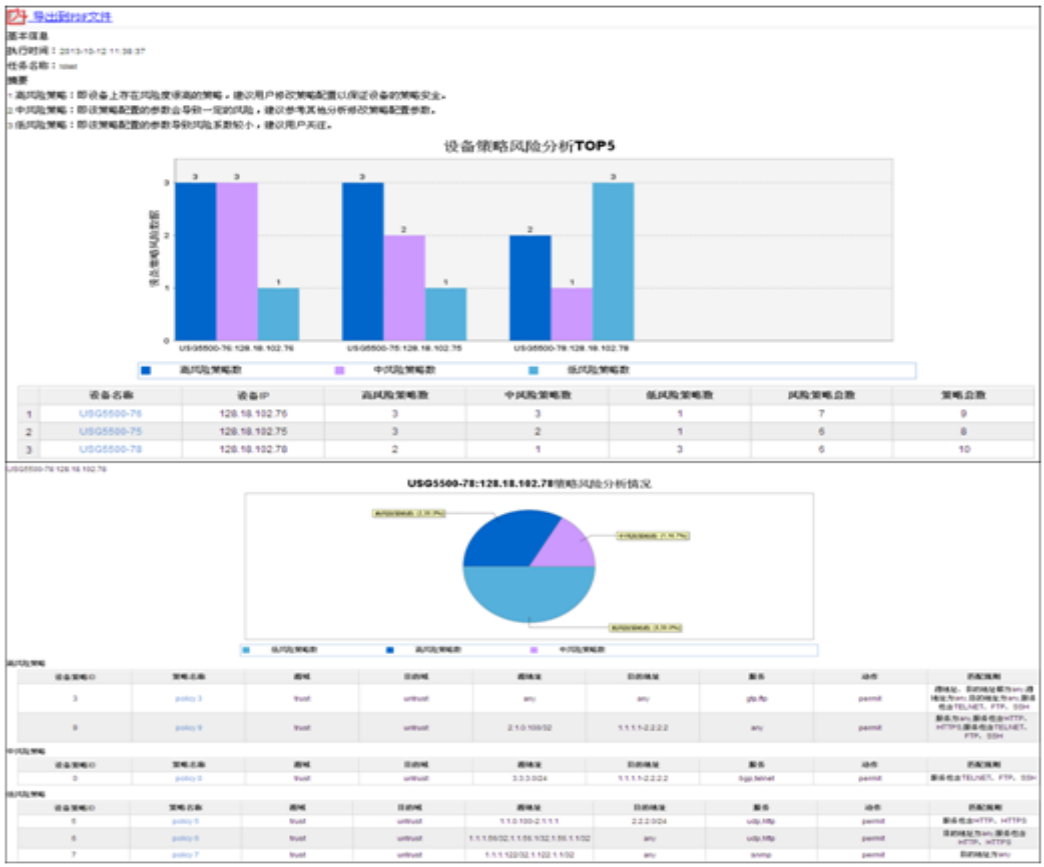
企业网络部署 eSight Secure Center 安全策略管理组件，对于防火墙安全策略进行风险分析，识别防火墙设备上存在问题的风险策略，让用户从策略维度及时了解企业网络安全风险。

图3-6 安全策略风险分析



安全管理员可以根据企业的业务和规范通过 eSight Secure Center 定义风险规则和检查基线，并创建定时执行或者手工执行的风险分析任务。

图3-7 策略风险分析结果



根据用户选择的风险规则，通过风险分析算法，可以分析出防火墙的高、中、低风险策略。安全管理员可以通过分析的结果，结合企业的情况和业务需要，对防火墙的安

全策略进行调整，降低由于安全策略配置不合理而导致的风险，帮助企业规范防火墙安全策略的配置。

3.4.3 安全策略综合分析

运维痛点：

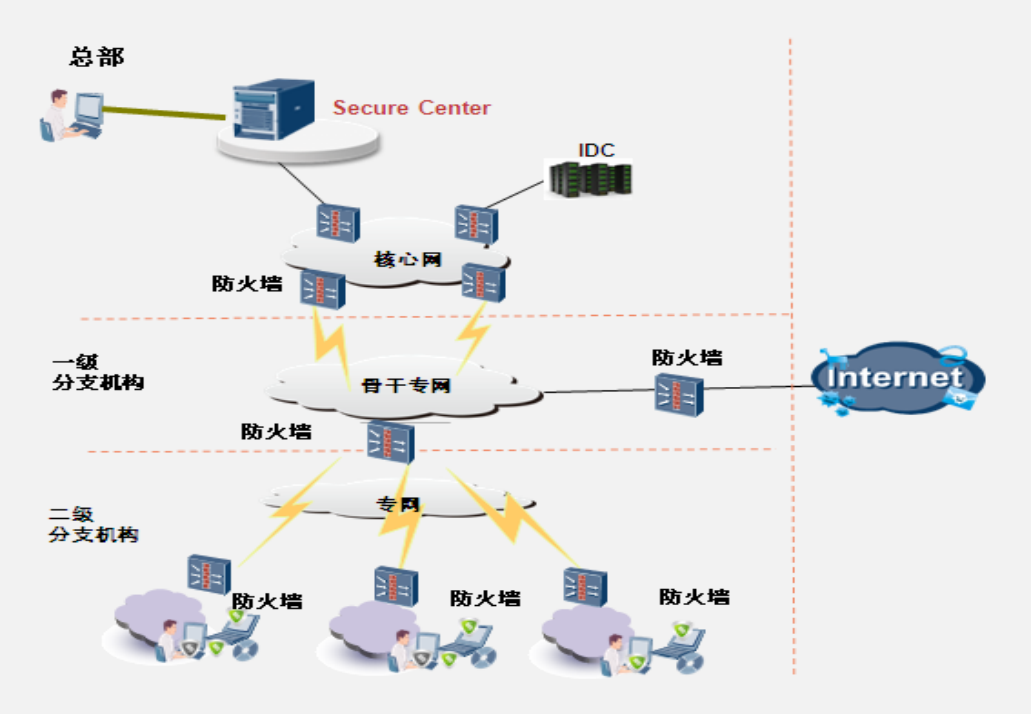
企业现网中防火墙的安全策略很多，无法直观、有效评估防火墙策略运维的情况。

对于防火墙安全策略运维工作的成效，无法进行量化的指标考核。

解决方案：

企业网络部署 eSight Secure Center 安全策略管理组件，对于防火墙安全策略进行综合分析，直观并明确给出防火墙安全策略的健康度状况，便于企业客户全面了解防火墙安全策略运维情况。

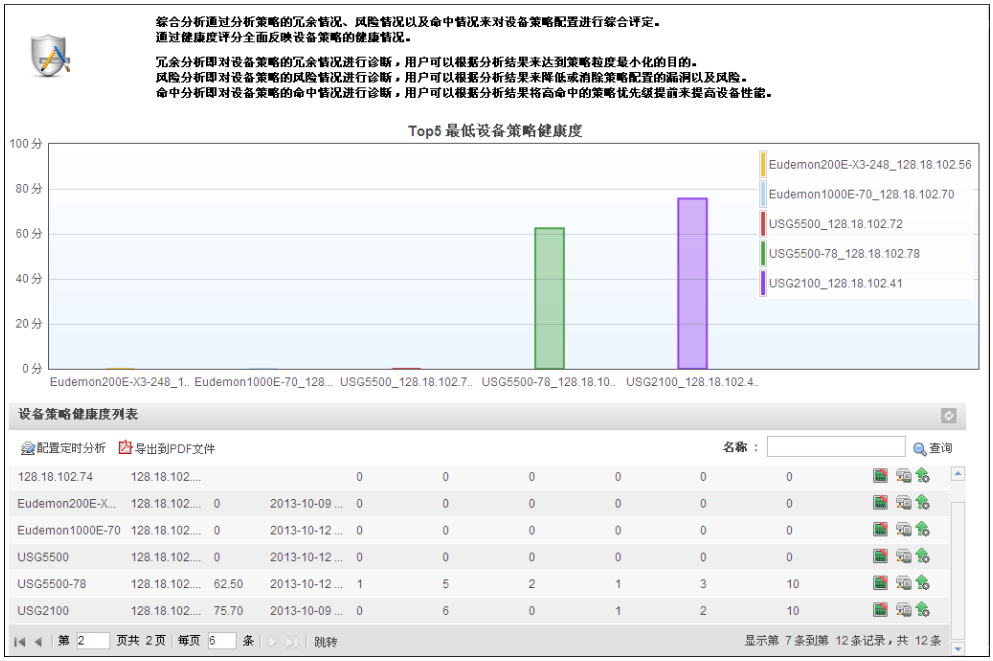
图3-8 安全策略综合分析



安全管理员通过 eSight Secure Center 手工或者定时运行策略综合分析，策略综合分析包含了冗余分析、命中分析和风险分析等处理。

根据防火墙策略综合分析的结果（冗余策略数、风险策略数和未命中策略数），利用健康度算法对防火墙设备策略给出一个直观的分值，帮助管理员了解防火墙策略的整体运维情况。

图3-9 策略综合分析结果



在对防火墙策略进行优化调整后，通过分析结果展示策略运维的效果，为策略运维工作的评估和考核提供量化的指标。

3.4.4 访问控制策略集中管理

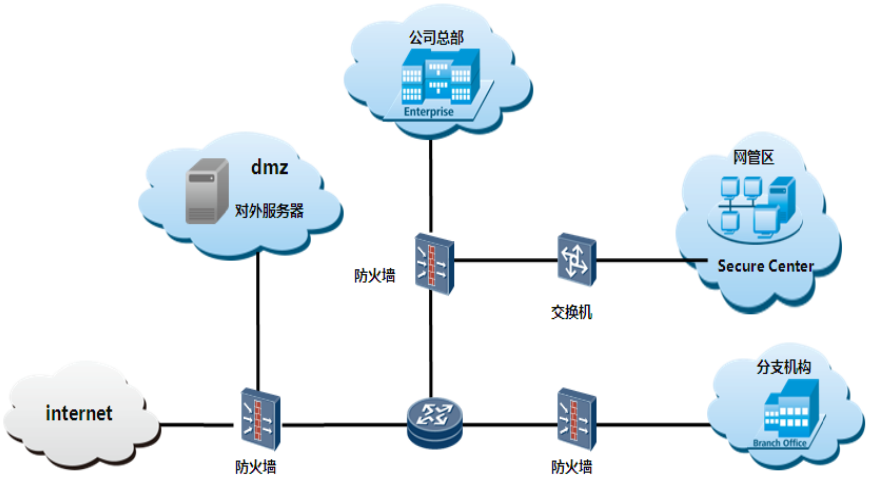
运维痛点：

企业网络中部署多台防火墙设备，客户需要集中配置管理企业不同安全域间的访问控制策略。传统安全管理基于单台设备的维护方式，会导致维护方式不统一，策略配置不一致等问题。

解决方案：

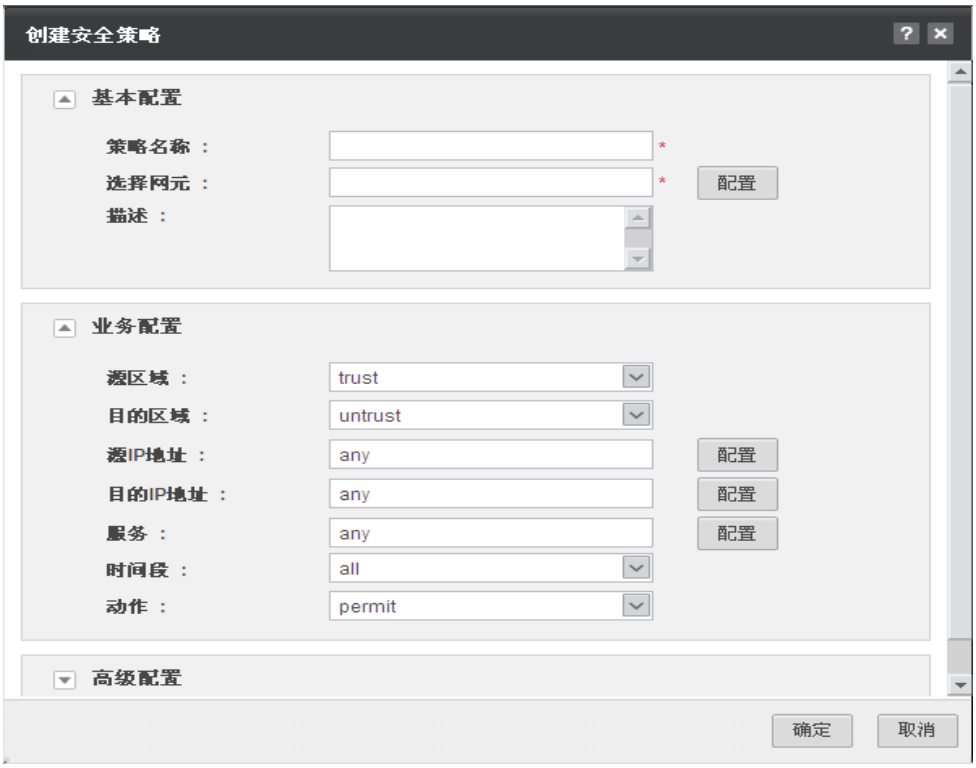
eSight Secure Center 提供访问控制策略集中管理能力，针对华为防火墙设备，提供简单、有效的安全策略管理功能。简化了企业日常访问控制策略维护工作量，节约人力成本。

图3-10 集中管理访问控制策略



通过 eSight Secure Center 集中配置企业网络中访问控制策略，实现安全域内以及域间各种数据流量的最基本的转发控制，并提供基于地址集、时间段和服务等公共对象的配置。

图3-11 创建访问控制策略



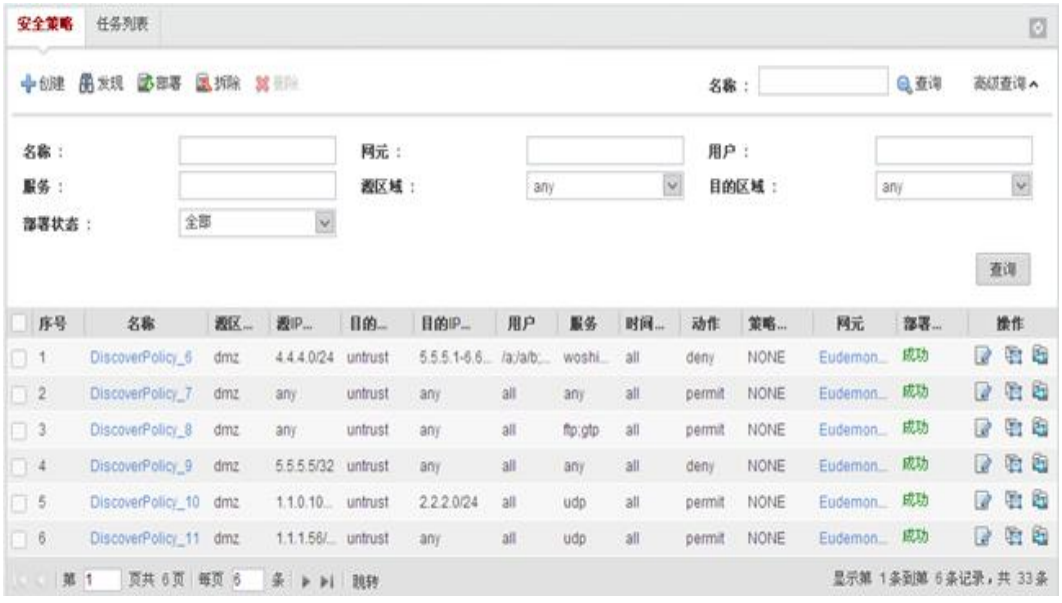
可以对多个物理防火墙/虚拟防火墙进行策略的批量部署，简化操作，提高效率。

提供策略部署成功、失败，以及失败原因，便于检查具体设备的失败原因，精确定位问题。

图3-12 部署结果查看

提供多维度的策略查询视图，保证管理员从设备、安全域等角度检查安全策略。

图3-13 策略高级查询



在不影响现有业务的前提下，可以将现有设备安全策略配置发现到网管侧进行集中管理，实现运维的平滑过渡。

3.4.5 内容安全策略集中管理

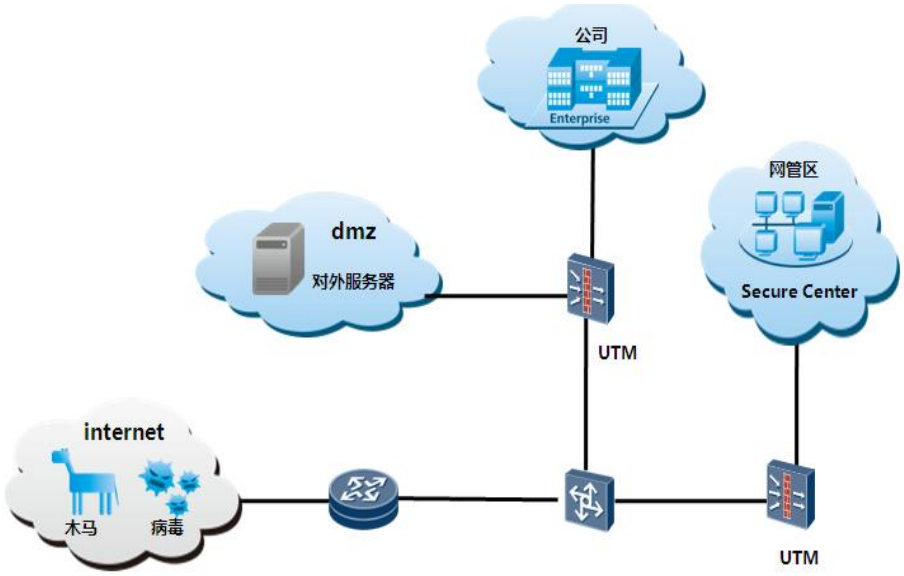
运维痛点：

企业网络中部署多台安全设备，需要配置内容安全策略（入侵防御/反病毒）避免企业受到黑客和病毒的攻击。传统安全管理基于单台设备的维护方式，不便于对多个防火墙进行统一的内容安全策略控制，容易出现安全纰漏或者隐患。

解决方案：

eSight Secure Center 提供内容安全策略集中管理能力，针对华为防火墙设备，提供简单、有效、全面的入侵防御和反病毒策略管理功能。简化了企业日常内容安全策略维护工作量，节约人力成本。

图3-14 集中管理内容安全



安全管理员通过 eSight Secure Center 集中配置入侵防御/反病毒策略，实现对于不同安全区域的内容安全控制，避免黑客入侵和病毒传播，保证企业网络的安全。

图3-15 创建内容安全策略

对于入侵防御策略，提供默认的策略模板，并支持自定义签名，为客户提供了更加方便和灵活的管理方式。

图3-16 入侵防御策略模板

对于反病毒策略，提供基于 HTTP、FTP、SMTP 和 POP3 的细粒度策略配置。

图3-17 反病毒策略配置

3.4.6 接入认证策略集中管理

运维痛点：

现网交换机数量多，无法进行统一接入认证策略管理，运维效率低

交换机 802.1x 策略配置命令复杂，不便于维护

解决方案：

企业网络部署 eSight Secure Center 安全策略管理组件，基于设备组进行接入认证策略集中管理和批量部署，通过一致性审计有效检查设备策略与管理软件策略的差异，可以简化策略配置和一致性检查，提高运维效率。

图3-18 集中管理接入认证策略

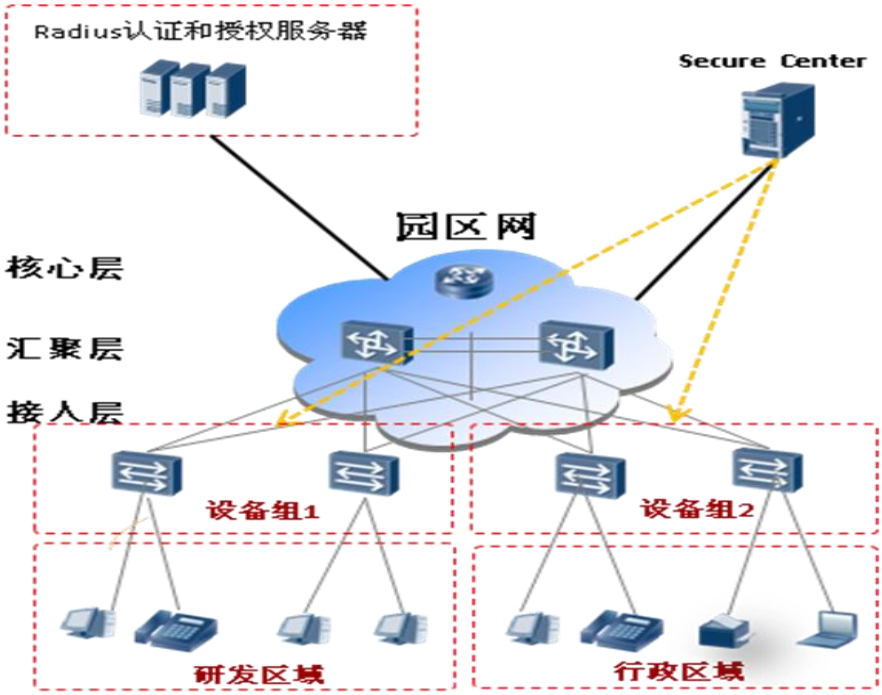
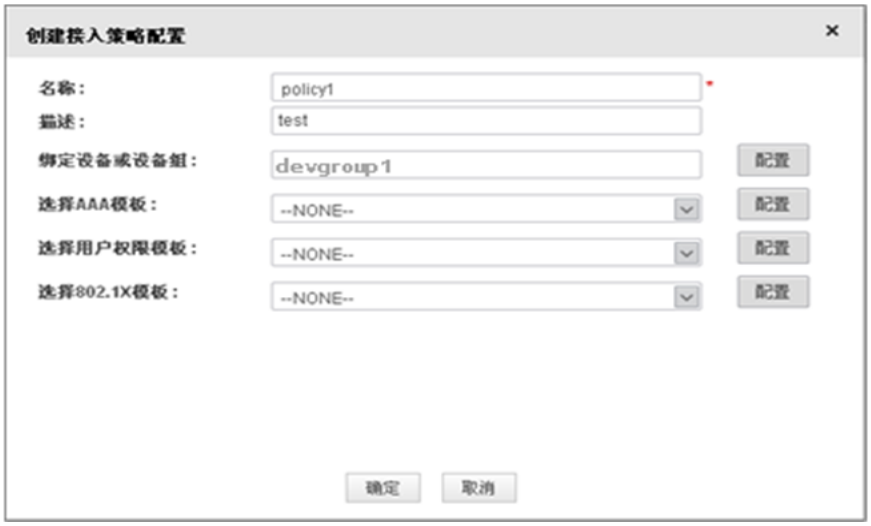
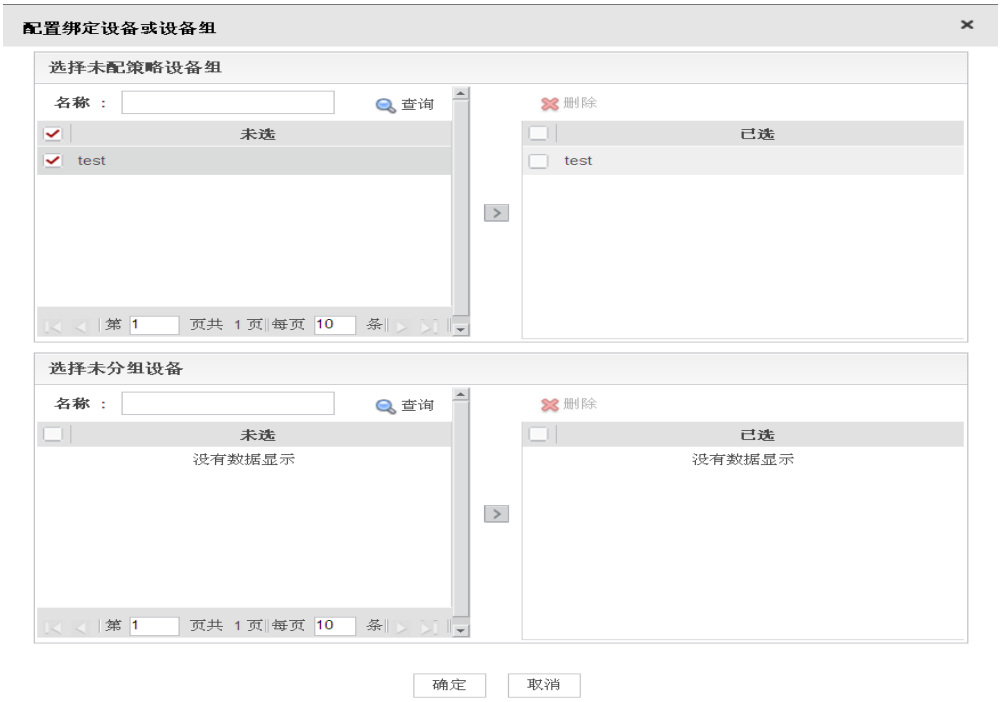


图3-19 创建接入认证策略



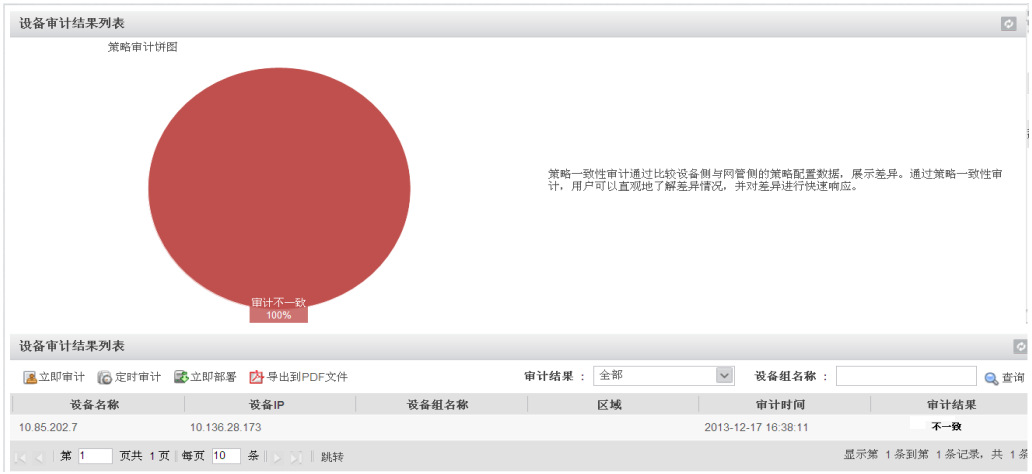
在创建接入认证策略时，需要选择 AAA 模板、用户权限模板和 802.1x 模板，同时需要选择绑定的设备或设备组。

图3-20 绑定设备或设备组



部署策略时，根据策略绑定的设备或者设备组将策略下发到相应的交换机设备上。

图3-21 策略一致性审计



支持手工和定时对交换机设备的接入认证策略进行一致性审计，审计结果支持导出报表，并可以查看一致性比较详细结果。

3.4.7 AR 安全策略集中管理

运维痛点：

用户现网部署了很多 AR 设备，无法统一对安全策略进行集中配置和批量下发，策略管理不方便，运维成本高而且效率低。

解决方案：

企业网络部署 eSight Secure Center 安全策略管理组件，提供统一的策略配置入口，集中管理网络中 AR 设备的安全策略，可以对 AR 设备的安全策略进行批量配置和部署，简化策略运维，提高运维效率。

图3-22 集中管理 AR 安全策略

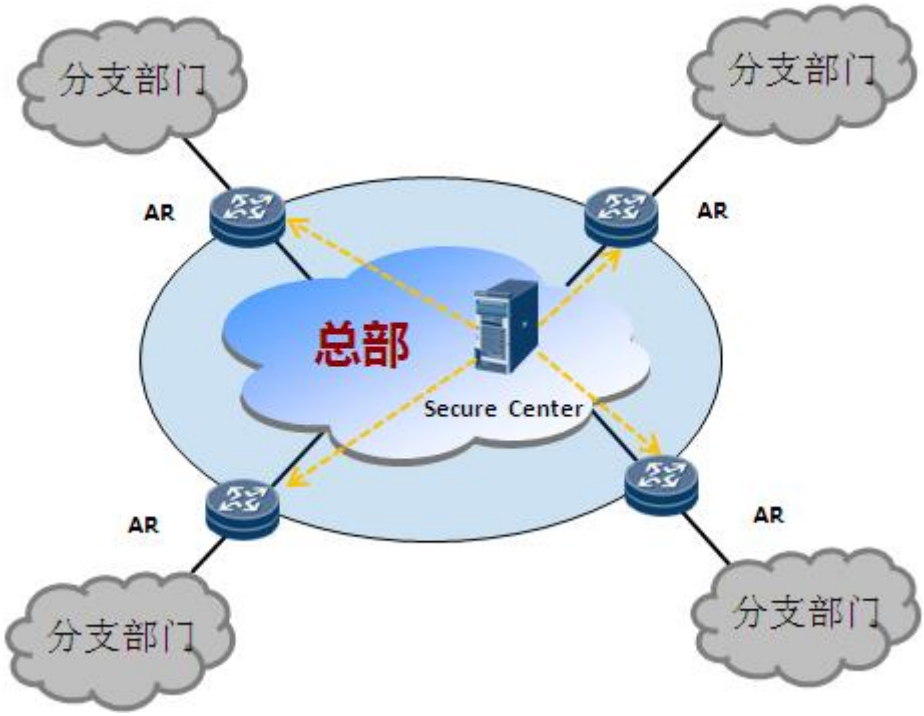


图3-23 创建高级 ACL

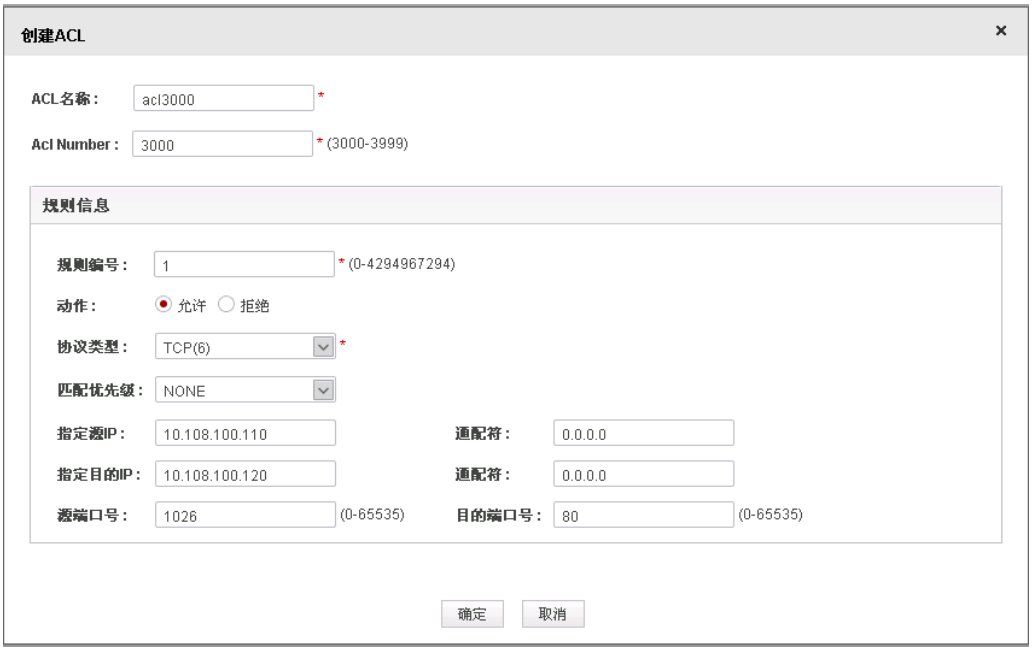
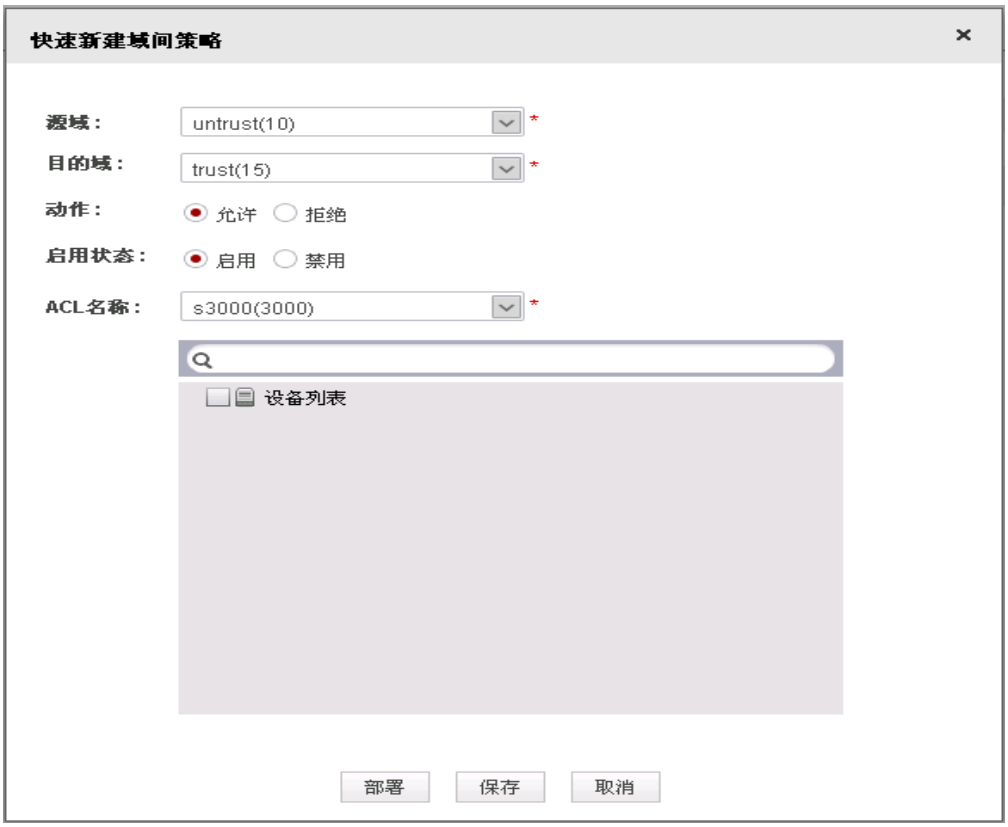
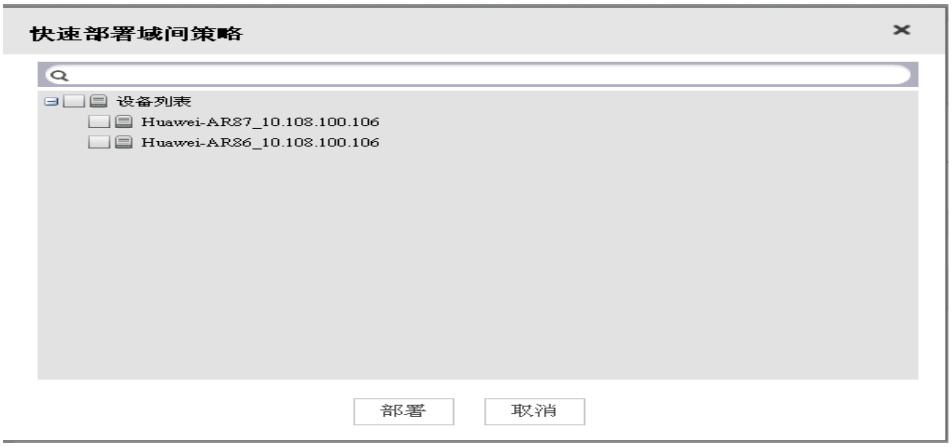


图3-24 创建 AR 域间策略



在创建域间策略时，可以使用快速创建的方式将新建的域间策略直接部署到多个 AR 设备上，也可以在创建策略后选择策略进行批量策略部署。

图3-25 快速部署 AR 域间策略



4 结论

eSight Secure Center 支持对华为网络和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、接入认证策略集中管理等多种应用场景。

eSight Secure Center 支持对华为防火墙安全策略的冗余分析、命中分析、风险分析和综合分析，可以为安全策略的精细化和高效运维提供有效的帮助。

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

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
SSH	Secure Shell	安全外壳协议
HTTP	Hyper Text Transfer Protocol	超文本传输协议
FTP	File Transfer Protocol	文件传输协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
POP3	Post Office Protocol 3	邮局协议的第 3 个版本