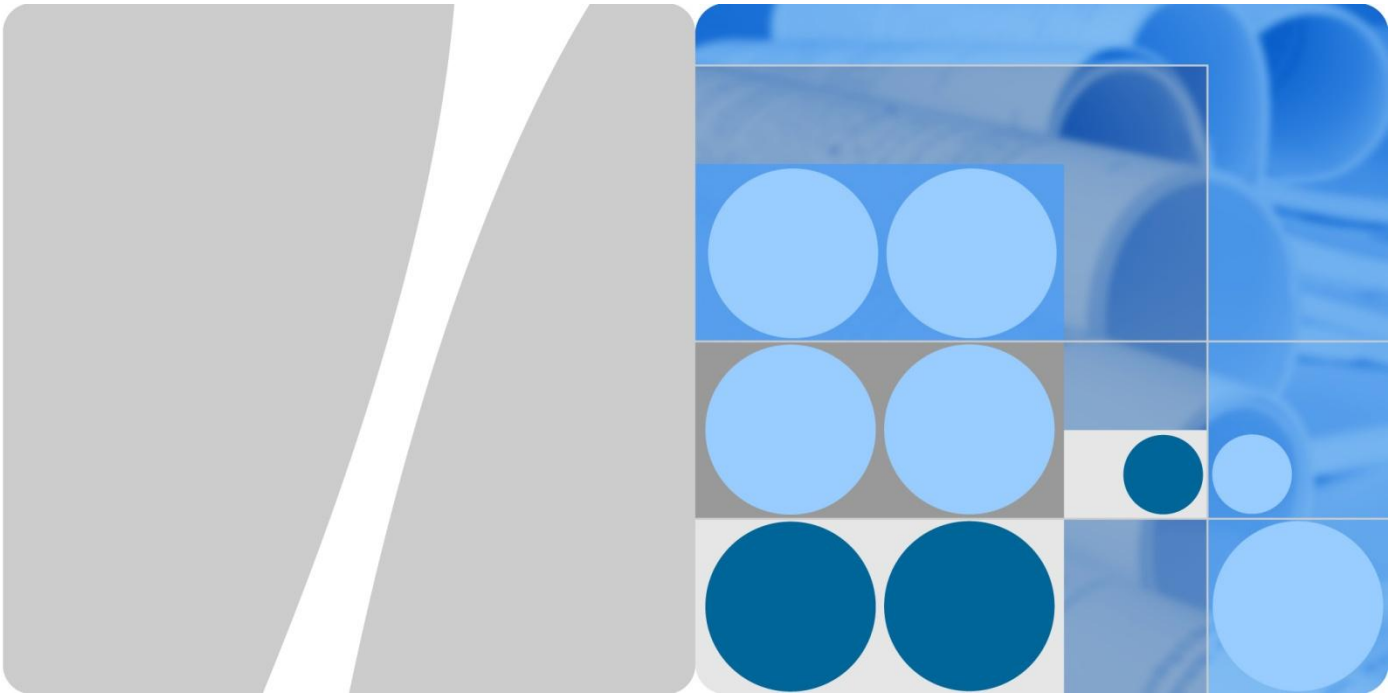


eSight
V300R001C10

LogCenter 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

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 LogCenter 的解决方案、关键技术点以及典型场景等方面的描述，帮助用户了解 LogCenter 的关键能力、使用场景与使用方法。

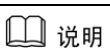
读者对象

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

LogCenter 是华为面向安全业务管理的 B/S 架构管理平台。LogCenter 充分融合了华为安全设备的业务管理、业务分析等功能，具有高集成度、高可靠性等特点。

LogCenter 支持对全系列华为安全网元等的管理，具有完善的安全设备日志采集和业务分析功能。LogCenter 满足网元集中管理、日志统一管理和分析、上网 NAT 追踪、企业员工上网行为分析等多种应用场景。

本文档从技术角度上介绍 LogCenter 系统的功能和解决方案。

2 简介

LogCenter 提供华为全系列安全设备管理。通过采集安全网元的日志并进行细粒度分析，使用户通过日志的业务分析报表能及时了解网络安全现状，及时了解网络用户的行为，迅速识别并消除安全威胁，提高企业办公效率。

3 解决方案

3.3 LogCenter 系统

3.3.1 系统功能介绍

LogCenter 系统支持针对华为安全设备的安全业务分析功能和基础网元管理功能。满足安全管理的基本功能需求。

- 安全业务分析功能

  LogCenter 通过高效地采集网元的日志，用户能及时了解华为安全网元的业务情况，跟踪网络用户的行为，迅速识别并消除安全威胁。

  通过对华为防火墙设备、MA5200G、NE40/80 和 ME60 网元的海量 NAT 会话日志的存储及查询功能，帮助用户进行快速精确的 NAT 追踪。

  通过对华为防火墙设备 Syslog 日志的实时分析和统计，当发生攻击事件或异常流量时能实时进行告警响应，帮助用户迅速识别并消除安全威胁。

  通过对华为防火墙设备等网络网元的会话日志和安全日志进行采集和分析，从而追踪上网行为（如使用 P2P、email、HTTP、MSN、QQ 等业务），分析上网行为，分析应用时长和流量，对上网行为进行管理。

  针对华为防火墙等设备提供丰富的报表功能，方便用户了解设备的实时和历史安全信息以及网络攻击状况。

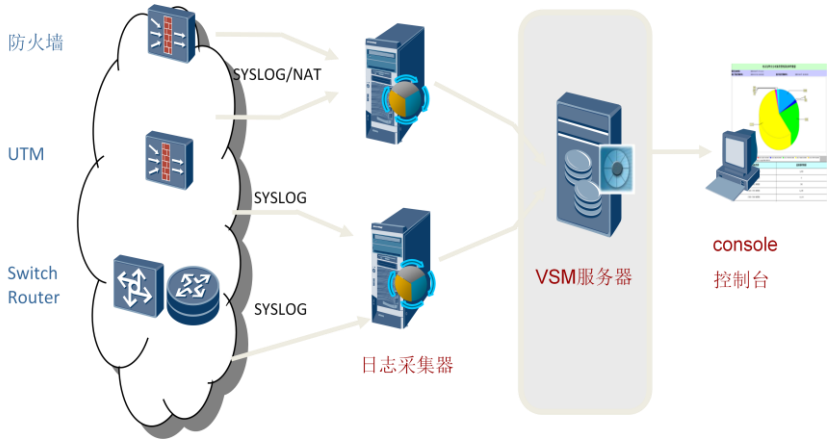
- 基础网元管理

  LogCenter 可管理设备覆盖全系列华为安全网元。支持网元自动发现，网元信息批量同步等功能，方便用户对网元的管理。

3.3.2 系统组成介绍

下图是 LogCenter 系统组成示例图：

图3-1 LogCenter 系统组成图



在该图中，各组件功能如下表所示：

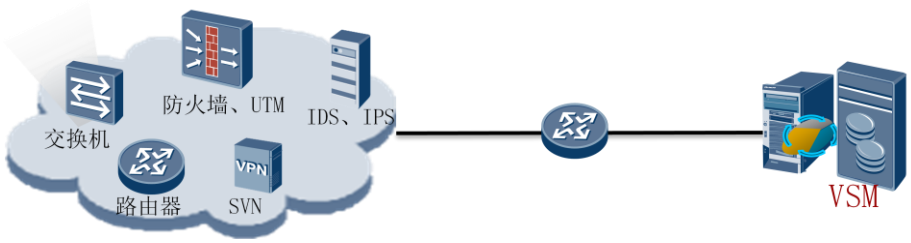
表3-1 各组件的功能与接口

组件	功能	对外接口
控制台	通过 WEB 界面提供统一的系统管理界面；提供统一的日志、告警和报表查询界面；提供统一的策略设置界面	HTTP/HTTPS
LogCenter 服务器	提供日志查询、日志二次统计分析、各种统计报表，以及安全策略管理、用户管理等功能	
日志采集器	负责安全设备的日志采集、分类、过滤、归并和统计	

3.4 典型组网

3.4.1 集中式组网

图3-2 LogCenter 服务器与采集器集中式部署组网图



集中式组网方案适用于网元较少、物理地域部署相对集中、会话日志量小于160,000EPS（Events Per Second）或文本日志量小于 8,000EPS（Events Per Second）的网络环境。此时，将 LogCenter 服务器和采集器部署在同一台机器上。

集中式部署成本较低，适用于网元集中的小规模网络，具体组网请参见组网。选择该组网方式需要考虑以下因素：

- 所管理网元的组网情况

  集中式组网时，建议所管理的网元部署在相同的局域网，如果网元部署在广域网，集中式部署会导致大量的日志信息占用广域网的带宽，影响正常的业务。

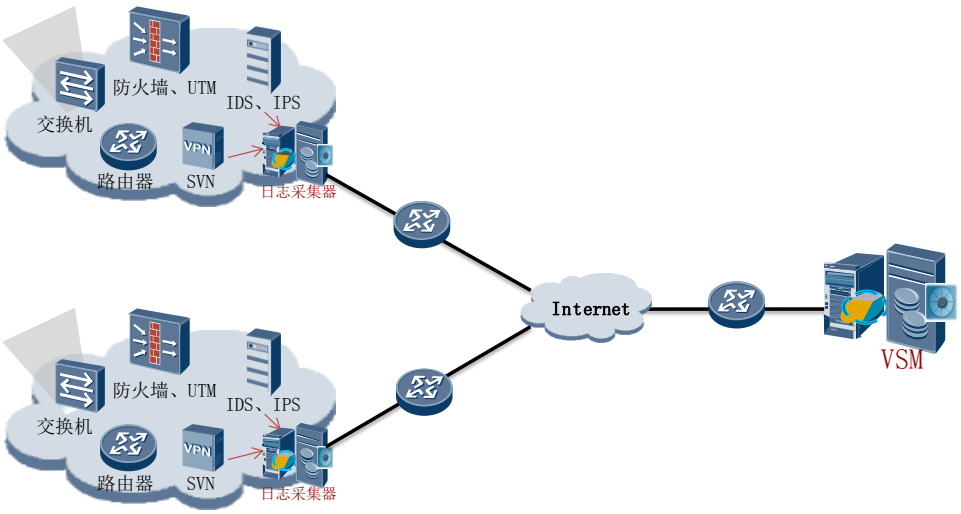
- 日志量

  集中式组网时，建议日志量不要超过一台采集器的处理能力。如果现网的日志量超过了一台日志采集器的处理能力，应该考虑使用分布式部署。

  一台日志采集器可以处理 160000EPS（Events Per Second）的会话日志，或 8000EPS 的文本日志（包括 Syslog、FTP/SFTP），或 20000EPS 的二进制 Dataflow 日志。

3.4.2 分布式组网

图3-3 LogCenter 服务器与日志采集器分布式部署组网图



分布式组网方案适用于网元多且分部分散，日志量在 160,000EPS 以上的大规模网络环境。网络管理员可配置 1 台 LogCenter 服务器和最多 15 台日志采集器，每添加 1 台日志采集器，可多处理 160,000EPS 的日志量。

分布式部署适合大中规模网络，具体组网请参见组网。选择该组网方式需要考虑以下因素：

- 所管理网元的组网情况

  网元分布在多个区域，区域间需要通过广域网连接。每个区域部署一台日志采集器，可以避免大量的日志信息占用带宽，节约租用带宽的成本。

- 日志量

当现网的日志量超过了一台日志采集器的处理能力，需要使用分布式部署。

一台日志采集器可以处理 160000EPS 的会话日志，或 8000EPS 的文本日志（包括 Syslog、FTP/SFTP），或 20000EPS 的二进制 Dataflow 日志。

- 节约磁盘柜的配置

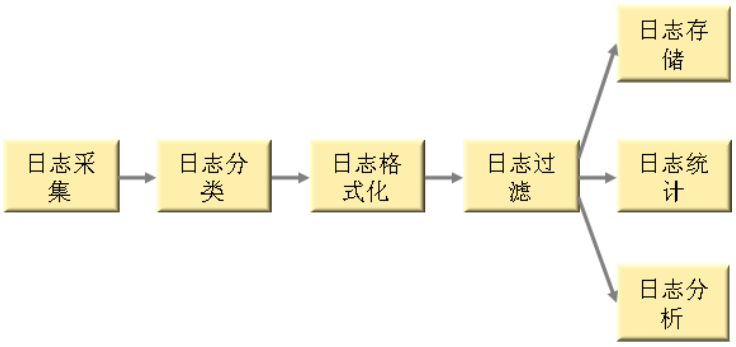
  服务器的存储成本比磁盘柜低，可以通过配置多台日志采集器以增加服务器的存储空间，避免或减少配置磁盘柜。

3.5 关键技术原理

3.5.1 日志归一化管理

日志信息来自不同类型的华为安全设备，日志格式差异性很大，需要对日志进行归一化处理。

图3-4 日志处理流程



如上图所示，日志需要经过一下的处理步骤：

- 日志采集

  通过多种途径接收和采集设备和应用系统产生的日志。LogCenter 可以支持无代理的日志采集方式。可以支持通过 Syslog、NAT，FTP/SFTP 的采集方式，可以对设备日志和文本日志进行采集；

- 日志分类

  LogCenter 根据对设备和应用系统日志的长期积累经验，提供了一套简洁而有效的日志统一分类。相同分类的日志具有相同的日志结构，可以方便的进行查询和分析；

- 日志格式化

  LogCenter 使用自有的专利技术对日志进行格式化，格式化的规则支持快速升级。通过日志格式化，可以将异构的日志转换为统一的日志格式；

- 日志过滤

  LogCenter 提供日志过滤功能，根据用户设置的过滤策略对日志进行过滤。丢弃无用的噪音信息，节省磁盘空间和提供日志分析的性能；

- 日志存储

针对日志管理系统的存储特点，LogCenter 将日志保持在文件数据库。相对于关系数据库，文件数据库具有吞吐量大，资源占用率低的特点，能够很好的满足日志管理系统 存储海量数据的要求；

- 日志统计

  日志管理系统需要输出大量的日志分析报表，满足用户的巡检要求和法规遵从性要求。LogCenter 通过对格式化后的日志数据进行统计分析，将分析结果记录在数据库中，可以支持快速的日志报表输出；

- 日志分析

  快速的从海量的日志中发现安全事件是日志管理系统提供的一个主要功能。LogCenter 提供基于策略的实施日志关联分析。对于符合策略的一条或多条日志可以通过各种方式（Email、短信告警(SMS)、声音告警）向管理员发出告警；

3.5.2 日志存储方案

为了满足海量日志的存储和节约磁盘空间，LogCenter 系统采用三级日志存储方案，既保证日志数据能够长时间的保存，又节省了用户用于日志数据的存储成本。

根据日志数据文件根据不同的生命周期，可以将 LogCenter 的日志文件分为在线日志、转储日志和备份日志：

- 在线日志

  日志数据不经过压缩，可以提供快速的日志查询能力，占用的磁盘空间大。适合新产生的日志，可以根据用户的查询习惯设置在线日志的存储天数。

- 转储日志

  在线日志达到设定的阈值（在线空间使用率或存储天数），系统会自动将在线日志进行压缩并自动转储到制定的转储目录。转储日志经过压缩，对于一般的日志数据，压缩比可以达到 4:1。

- 备份日志

  对于有长期数据保留的需求的用户，可以将日志保存到成本更加低廉的存储设备上。系统可以支持备份的日志重新导入查询。

日志文件的转换过程如下图所示：

图3-5 三级存储方案

4 推广

4.1 应用场景

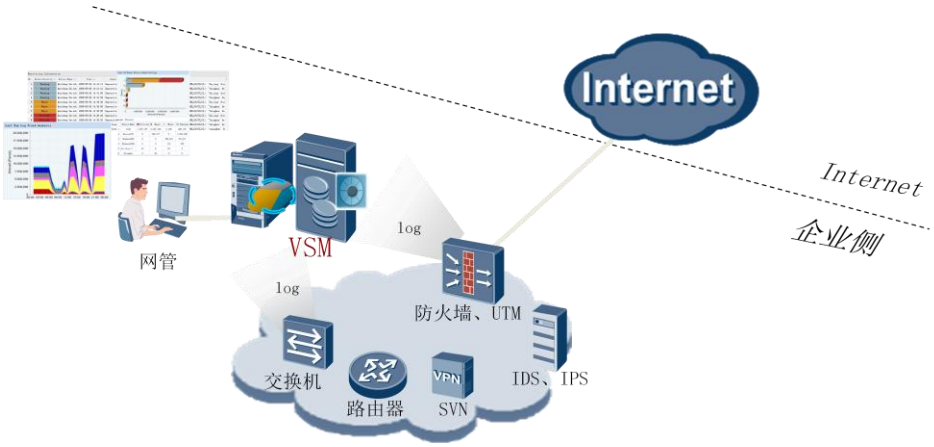
4.1.1 日志统一管理

企业内部部署了大量的路由器、交换机、防火墙等网络网元，由于存在网元日志格式不统一、可读性差、海量日志存储困难、日志难于统一管理等问题，网管很难及时从日志中发现重大安全隐患。

LogCenter 能够实现日志统一管理，支持 SYSLOG、NAT 日志、SFTP、FTP 静态文件、FTP 动态文件多种日志采集方式。LogCenter 能够采集、分类、过滤、归并、分析、存储和监控网元上报的日志，帮助用户对海量日志进行管理，使用户能及时了解安全网元和网络网元的运行情况，跟踪网络用户行为，迅速识别并消除安全威胁。

LogCenter 在日志管理的基础上，提供日志的实时告警响应功能，能够对日志进行实时的分析，并实时产生告警。

图4-1 安全事件管理场景图



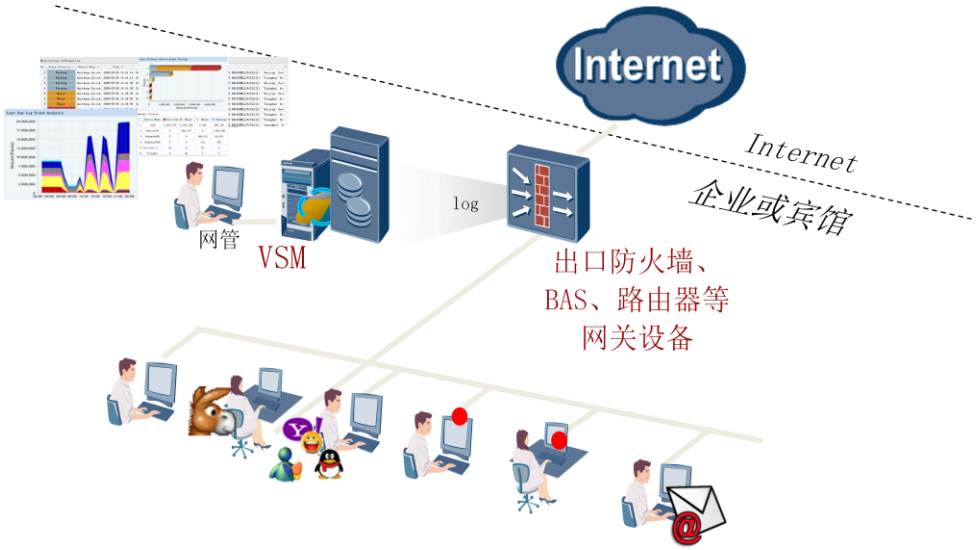
4.1.2 NAT 溯源

网络地址转换(NAT, Network Address Translation)被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

NAT 在解决了 IP 地址资源的同时带来了一个问题，由于企业组织内部使用相同的 IP 地址，无法追究企业内部的人员在网上的违法行为。

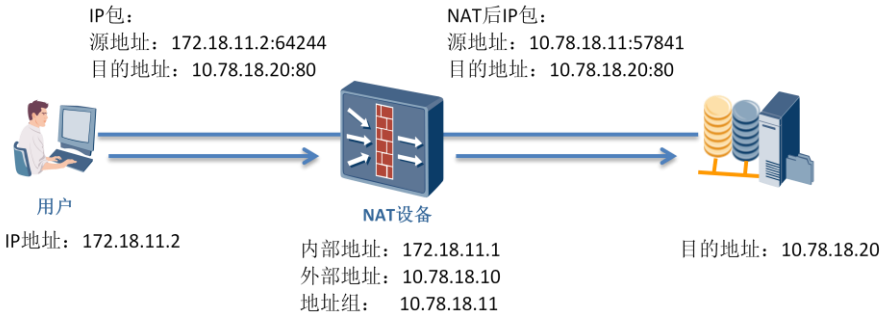
在上网行为追踪的场景下，LogCenter 系统对 Eudemon/USG、MA5200G、NE40/80、ME60 等网关设备的会话日志进行采集和分析，获取 NAT 信息（包括目的 IP 地址、目的端口、NAT 前源 IP 地址和协议等），结合流量日志，从而追踪企业内部用户的上网行为。

图4-2 上网 NAT 追踪场景图



NAT 追踪涉及到多个 IP 地址端口（源 IP、源端口、目的 IP、目的端口、NAT 后源 IP、NAT 后源端口、NAT 后目的 IP、NAT 后目的端口），下面的例子说明 PAT 方式下，各个字段的含义：

图4-3 上网 NAT 追踪 IP 地址转换示例



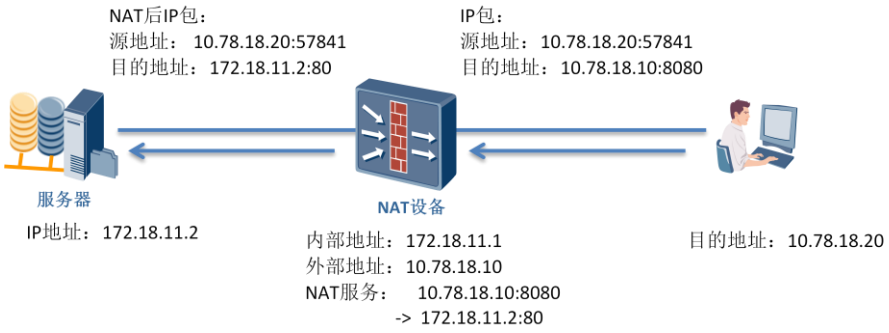
如图所示，内网用户 172.18.11.2 访问外网的服务器 10.78.18.20 的 HTTP 服务，中间通过 NAT 转换。这个会话的各个地址如下：

源 IP/源端口： 172.18.11.2:64244

目的 IP/目的端口： 10.78.18.20:80

NAT 后源 IP/NAT 后源端口： 10.78.18.11:57841

图4-4 NAT Server 方式 IP 地址转换示例



如图所示，外网用户 10.78.18.20 访问出于内网的服务器 172.18.11.2 的 HTTP 服务，NAT 设备上已经将内部服务器的 HTTP 服务做了映射。这个会话的各个地址如下：

源 IP/源端口： 10.78.18.20:57841

目的 IP/目的端口： 10.78.18.11:8080

NAT 后目的 IP/NAT 后目的端口： 172.18.11.2:80

说明

NAT 的实现方式有三种，即静态转换 Static NAT、动态转换 Dynamic NAT 和 端口多路复用 OverLoad。

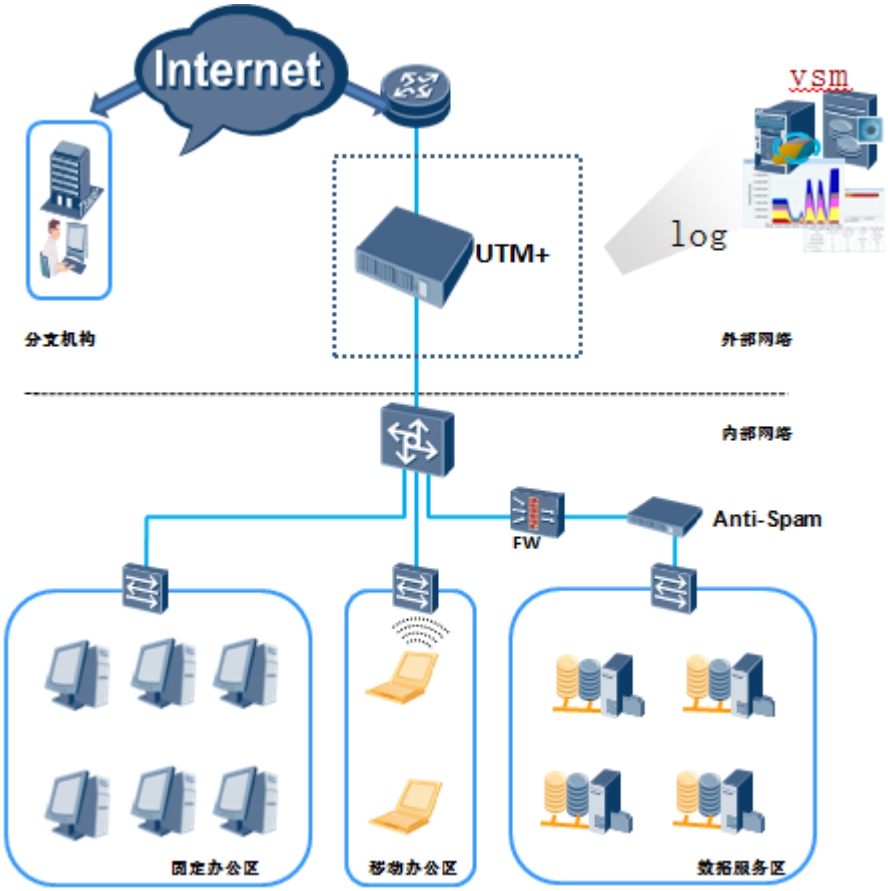
- 静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。
- 动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对是不确定的，而是随机的，所有被授权访问上 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。
- 端口多路复用(Port address Translation,PAT)是指改变外出数据包的源端口并进行端口转换。内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

4.1.3 上网行为管理

在企业员工上网行为管理的应用场景下，LogCenter 对防火墙等网络网元的会话日志和安全日志进行采集和分析，从而追踪企业员工的上网行为（上网流量 TopN，上网时长 TopN，WEB 访问分析，邮件分析等），分析企业员工上网行为。

LogCenter 可以进行按用户的上网流量、上网时长、上网关键字、Web 访问、邮件收发、上网应用、网络威胁、文件外发等的分析和查询，管理人员可以根据分析结果对用户上网行为进行管理。

图4-5 企业员工上网行为管理场景图



4.1.4 基础网元管理

如果购买了多台华为安全设备，在此种场景下，考虑在公司中心机房搭建一套 LogCenter 基础组件，可实现对全网所有安全网元集中监控。网络管理员的日常管理可仅通过 LogCenter 进行。

LogCenter 网元集中管理的应用使网络管理效率大幅提高，管理员可以节约出更多的时间与精力考虑如何更好的优化网络，使得公司网络更加稳定。

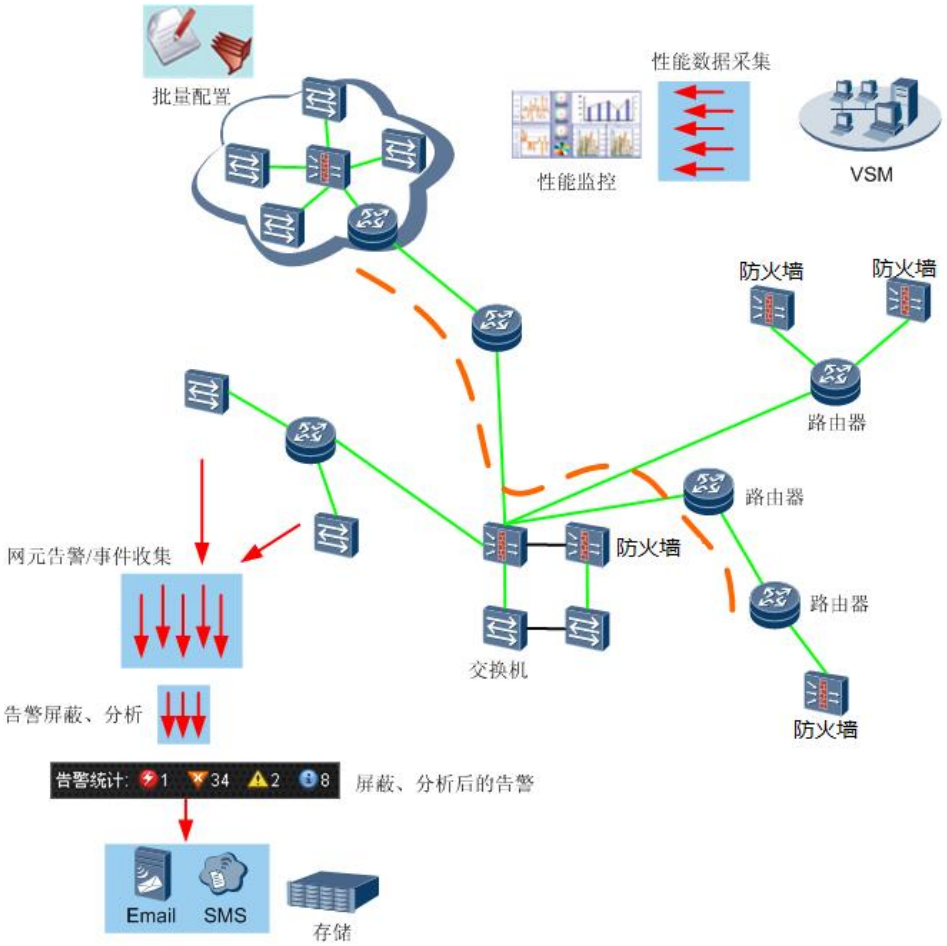
1. 拓扑集中管理
   - 系统支持网元自动发现功能，新发现网元自动在拓扑图中呈现。
   - 直观的集中展现全网拓扑，通过拓扑子图可支持拓扑分层管理，对大型的网络的拓扑呈现也非常清晰。
   - 提供了日常操作入口，网络管理日常操作可以通过拓扑作为入口进行，使得网管操作易于上手。
   - 告警在拓扑图中呈现，网络管理员可以直接利用拓扑进行故障定位。
2. 集中管理全网所有告警
   - 设置告警过滤功能，管理员可只关注重大故障告警，例如：网元离线告警、业务端口 down 告警。

– 可设置告警通知，使用短信或邮件发送告警，而不必在机房 7*24 小时值守。

3. 性能监控

可以实时监控接口数据包，可以设置阈值告警，进行网络故障提前预防。

图4-6 网元集中管理应用场景图



4.2 性能指标

表4-1 LogCenter 技术规格

项目	子项目	描述
网管性能指标	管理的最大容量	• 2000 个等效网元（典型配置）
	最大在线管理员数	16 个
日志性能	日志处理性能	• 二进制会话日志：均值 160,000EPS(Events

项目	子项目	描述
指标		per second)。 • 文本日志：均值 7,000EPS。 • 二进制 Dataflow 日志：均值 20,000EPS。 系统支持通过增加硬件设施提高处理性能，每增加一台标准配置日志采集器，二进制日志处理性能最高可提高 160,000EPS，文本日志处理能力最高可以提高 7000EPS。
	实时分析告警时间	• 对于采集的日志（FTP/SFTP）实时分析告警时间延误不超过 300 秒。

5 结论

LogCenter 支持对全系列华为安全网元等的管理，具有完善的安全设备日志采集和业务分析功能。LogCenter 可以满足日志统一管理和分析、上网 NAT 追踪、企业员工上网行为管理等多种应用场景。

通过部署 LogCenter 系统，一方面可以降低 IT 系统的维护成本，增强对华为安全设备系统故障和安全事件的及时响应能力；一方面帮助企业应对法规的顺应性检查，增强 IT 系统的可审计性。

6 缩略语表

表6-1 缩略语清单

英文缩写	英文全称	中文全称
EPS	Event per second	每秒事件量
NAT	Network Address Translation	网络地址转换
FTP	File Transfer Protocol	文件传输协议
SFTP	Secure File Transfer Protocol	安全文件传送协议
SOAP	Simple Object Access Protocol	简单对象访问协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	基于安全传输层的超文本传输协议