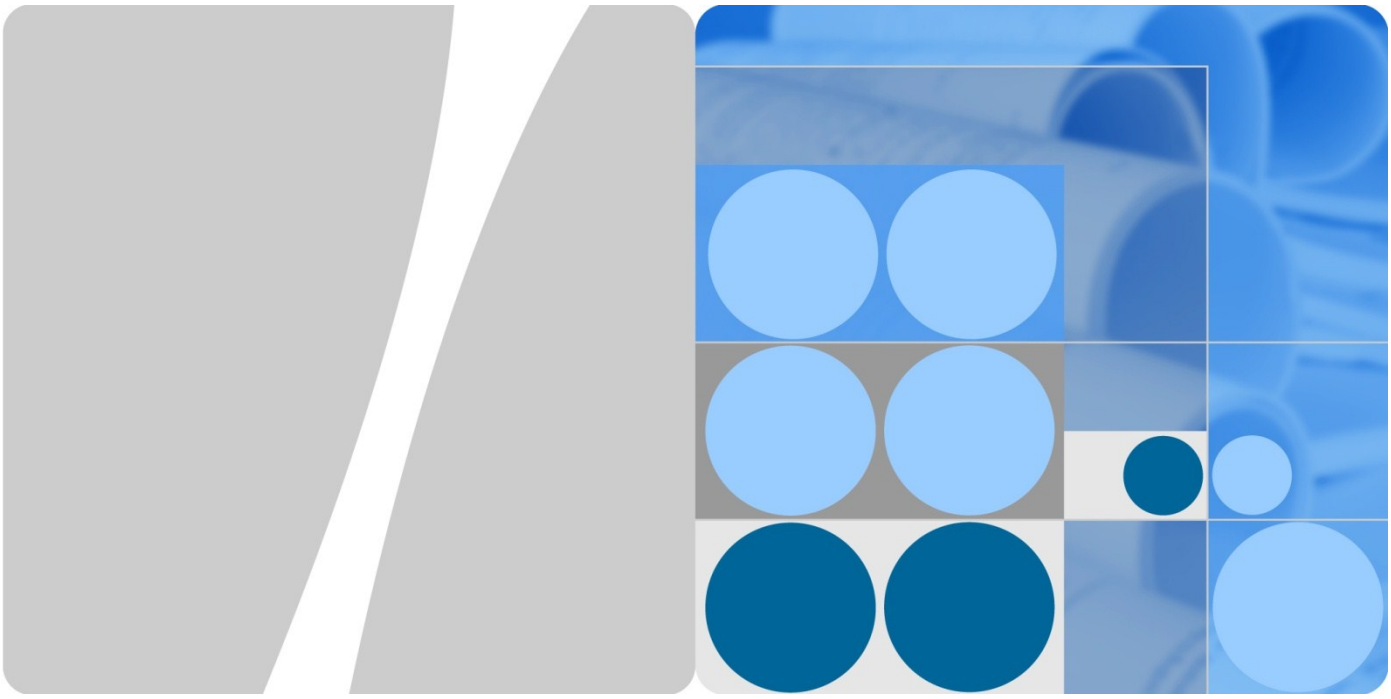

华为 TSM 终端安全管理系统
配置原则

华为技术有限公司

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://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

关 键 词：安全策略、资产管理、准入控制、补丁管理、软件分发、安全接入控制网关、安全代理、可消融客户端、WEB认证客户端。

1 TSM 总体介绍

随着网络技术的应用与发展，人们对信息网络的应用需求不断提升，对网络的依赖越来越强，伴随而来的信息安全威胁也在不断增加。网络安全已经超过对网络可靠性、交换能力和服务质量的需求，成为企业用户最关心的问题，网络安全基础设施也日渐成为企业网建设的重中之重。在企业网中，新的安全威胁不断涌现，它们对网络的破坏程度和范围持续扩大，经常引起系统崩溃、网络瘫痪，使企业蒙受严重损失。在企业网络中，任何一台终端的安全状态都将直接影响到整个网络的安全，这些问题极大地困扰着企业高层管理人员和IT部门。

TSM终端安全管理系统是华为公司推出安全解决方案，通过把准入控制与终端的安全状态相结合，对于不符合安全策略的终端进行隔离修复，强制终端用户实施企业的安全策略。控制接入网络的终端用户网络访问权限，实现最小授权访问控制，保障企业内网的安全。

TSM系统支持如下功能：

1. 身份认证功能：

身份认证是TSM系统的基础，通过认证，确定终端用户的身份，进而确定终端的安全策略和准入控制策略。支持多级的组织结构，支持本地数据源和外部数据源，支持基于USB Key双因素等高强度的身份认证。

2. 终端安全检查功能：

TSM系统提供多种终端安全检查功能，包括防病毒软件、补丁、共享文件和冗余账号等检查功能。当检查到终端的配置与企业的安全策略不符合的时候，能够提醒终端用户，并且协助终端用户完成安全漏洞修复。

3. 安全接入控制功能：

TSM系统支持多种准入控制手段，包括安全准入控制网关SACG、802.1X交换机，以及基于终端主机防火墙的软件准入控制。C06版本新增基于ARP准入控制功能（测试特性，不对市场发布）。把准入控制与终端的安全状态相结合，对于不符合安全策略的终端进行隔离修复，强制终端用户实施企业的安全策略。控制接入网络的终端用户网络访问权限，实现最小授权网络访问。

4. 补丁管理功能：

TSM系统能够从微软网站下载补丁，检查终端补丁安装情况，当终端存在安全漏洞的时

候，根据管理员配置的安全策略，协助终端用户手工或者自动安装补丁。TSM终端安全管理系统能够与WSUS补丁管理系统联动，通过微软提供的API，利用WSUS服务器，与补丁检查策略配合，检查终端补丁的安装情况，对不按管理员要求进行补丁升级的用户进行自动强制升级。对于没有AD的网络环境，通过给TSM安全代理下发WSUS参数，协助管理员在终端部署WSUS服务。

5. 用户行为监控功能：

提供终端设备的管理功能，管理终端PC的接口设备，根据策略打开或者关闭特定的设备，在一定程度上防范信息泄漏。能够控制终端的网络行为，管理终端的外联事件，当探测到终端非法访问互联网的时候，可以根据需要，阻断终端的所有网络访问，并且记录终端访问互联网的事件。提供WEB访问监控功能，记录终端用户的WEB网站访问信息，以及控制网络应用程序对网络的访问。

6. 资产管理功能：

TSM系统提供资产采集功能，采集终端的软硬件信息，为企业的管理者提供一个全局的视图，了解企业终端当前配置的状况，为企业更新终端PC配置提供统计数据。TSM系统能够跟踪资产变更的情况，记录资产变更的详细信息，并且提供资产变更告警功能。

7. 软件分发功能

能够协助IT管理人员，分发软件，提高软件部署的效率。TSM系统的软件分发功能支持局域网范围内的P2P下载，能够大大减少对网络带宽的占用。

8. 设备发现功能

提供设备发现功能，通过扫描的方式，能够发现网络中的IP设备。在部署阶段能够协助实施人员了解网络的基本状态，判断实施的进展。

9. U盘注册管理功能

企业可以根据自己的管理要求，对企业内部U盘和企业外部U盘区别管理。TSM系统提供U盘注册功能，注册后的U盘将作为企业内部U盘，进行管理。通过与USB设备管理策略功能配合，对于注册U盘和非注册U盘，能够定义不同的安全策略，实现精细化管理。

1.1 系统网络逻辑结构及接口关系

1.1.1 网络实体组成

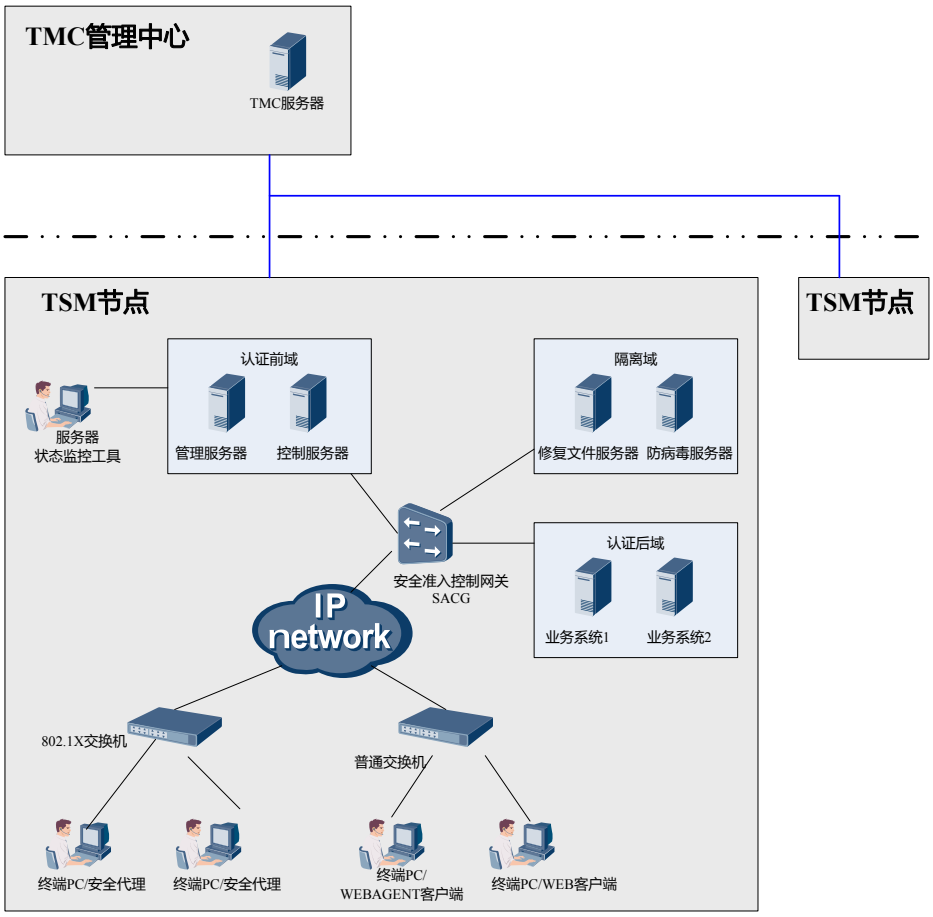

图1 TSM终端安全管理系统网络实体组成

1. TSM管理服务器SM

TSM管理服务器SM采用B/S架构，系统管理员通过WEB管理界面，可以完成终端用户管理、安全策略配置等业务管理工作。通过该操作界面，可以查询终端的安全状态和违规记录报表。

作为管理服务器，将管理其下的各个TSM控制服务器的连接状态，向已经连接的各个控制服务器发送实时指令，通知TSM控制服务器SC执行各种业务。

2. TSM控制服务器SC

控制服务器SC主要负责执行如下几项业务：

- 与802.1X联动，当身份认证通过后，根据终端的安装状态，通知802.1X交换机开放

网络端口或者切换VLAN。

- 与SACG联动，当身份认证通过后，通过扩展的COPS协议，根据终端的安全状态，对于安全检查不通过的终端，通知SACG切换到隔离域。对于安全检查通过的终端，通知SACG切换到认证后域。
- 作为与TSM安全代理SA的交互控制点，完成身份认证、安全策略下发、数据上报等任务。
- 实施ARP准入控制（测试特性，谨慎使用）的时候，SC负责在一个VLAN范围内挑选若干台终端，充当ARP干扰源，由这些ARP干扰源负责对非法终端实施干扰。

3. 网络准入控制设备

有四种可选的网络准入：

1）安全准入控制网关SACG

2）802.1X交换机

3）基于Windows IPSEC组件的软件准入控制

4）ARP准入控制—测试特性，谨慎使用

通过准入控制设备，把企业的网络资源划分为一个认证前域，若干个隔离域，以及若干个认证后域。终端在身份认证前，只能访问认证前域；当终端通过身份认证，没有通过安全认证的时候（某些检查项违规级别=严重），只能访问该终端用户所属的隔离域；当终端通过身份认证，并且通过安全认证，根据终端用户的身份，切换到该用户对应的认证后域，实现最小授权网络访问控制。

4. TSM安全代理SA

安全代理是一个安装在终端PC（运行Windows操作系统）上的应用程序，当终端PC启动后，终端用户输入用户名+口令（不同的认证方式会有所不同），执行身份认证和安全检查操作，并且把检查的结果（安全认证结果）作为开通网络访问权限的依据。在代理执行的过程中，监控终端的行为，包括监视和控制两个部分，如禁止使用USB接口以及监视用户所有网络访问的WEB URL，并且把审计的结果上报服务器，用于事后审计。

当启用ARP准入控制功能时，某些TSM安全代理将被选举成为干扰源（为了降低对网络的影响，每个VLAN选举3个干扰源），对接入网络的非法终端实施干扰，阻止其使用网络或者是阻止其正常使用网络。

此外，安全代理提供补丁管理、软件分发、资产管理、公告下发，以及远程协助等桌面管理功能。

5. 基于ActiveX技术的WEBAGENT客户端

TSM系统提供无需在终端安装代理软件的安全解决方案，通过基于ActiveX技术的WEBAGENT客户端，提供身份认证和安全检查操作，并且把检查的结果作为开通网络访问权限的依据。

6. 服务器状态监控工具

TSM系统提供一个工具，该工具可以部署在管理员的PC上，协助管理员监控各个TSM服务器的状态。当服务器发生故障的时候，管理员能够及时了解状态，及时修复，降低服务器故障对业务的影响。此外，状态监控工具还支持使用短信猫（调制解调器，需要另外配置）的方式发送短信进行告警，当发生验证的设备故障的时候，可以选择使用短信告警，提高问题的响应速度。

7. TMC管理中心

对于超大规模的网络，例如某个电信运营商的集团公司，可以考虑采用分布式部署方案，这时候可以在各个省公司部署一套TSM系统，然后在集团公司部署一套TMC管理中心。TMC管理中心提供如下几个业务：

1）定义并且下发安全策略；

2）提供统一的补丁下载途径；

3）定义并且下发补丁管理策略；

4）远程登录TSM节点。

8. 设备扫描器

设备扫描器是TSM系统的一个独立部件，通过发送探测报文的方式，发现网络终端的IP设备，对于探测到的IP设备，尝试识别设备的类型，如交换机/路由器/PC/服务器/IP PHONE/打印机等，对于PC设备，还能识别该设备是否部署了TSM安全代理。

9. 远程日志采集工具

远程日志采集工具是TSM系统的一个辅助程序，用于简化管理员/技术支持人员采集问题终端的日志。当某个终端出现故障的时候，管理员/技术支持人员不需要到终端所在的位置，可以通过该工具，远程获得终端的日志。

10. 服务器状态监控工具

服务器状态监控工具是TSM系统的一个辅助程序，用于监控TSM服务器的运行状态。当TSM服务器发生异常事件，或者系统运行异常，服务器状态监控工具能够快速检测到发生的问题，并且向管理员告警。

当系统发生严重故障的时候，管理员可以与网络割接辅助工具配合，在SACG设备（FW）上开启逃生通道。

1.1.2 主要的网络接口与协议说明

TSM系统与外部设备/系统的接口如图所示：

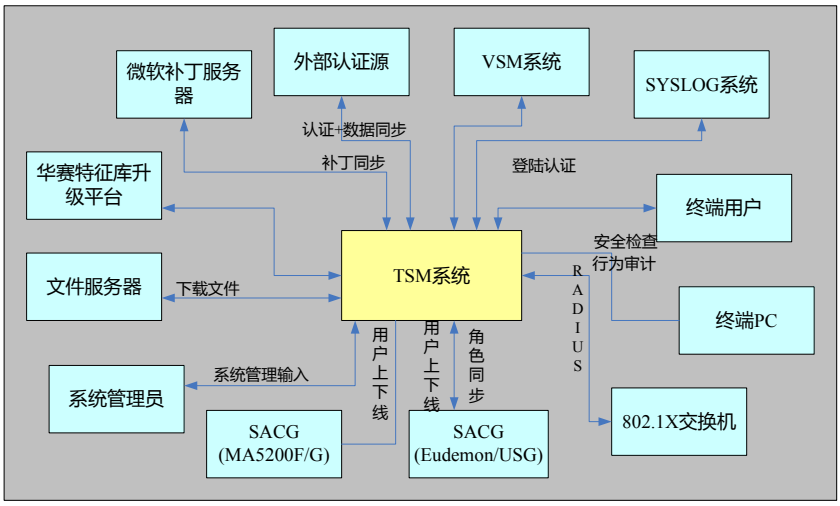

图2 TSM终端安全管理系统与外部设备之间的接口

与微软补丁服务器的通信协议：HTTP

与外部认证源的通信协议：LDAP V3、Kerberos

与外部文件服务器之间的通信协议：HTTP、FTP、文件共享

与802.1X交换机之间的通信协议：EAP、RADIUS

与MA5200F/G之间的通信协议：PORTAL 2.0

与SACG之间的通信协议：COPS、RADIUS-PAP

与华为交换机之间的通信协议：PORTAL 2.0、CHAP

与华为特征库升级平台之间的通信协议：暂无，现阶段没有实现自动升级功能

与外部SYSLOG系统之间的通信协议：SYSLOG

与VSM系统之间的通信协议：HTTP远程调用

TSM系统内部通信接口协议：

终端安全代理SA与控制服务器SC之间的通信协议：SSL

采用的密码算法：

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA，其中3DES使用168位的密钥

控制服务器SC与管理服务器SM之间的通信协议：HTTP

终端之间采用互访控制通信协议：IPSEC

控制服务器/管理服务器与数据库之间的通信协议：JDBC

控制服务器/管理服务器与文件服务器之间的通信协议：FTP

FTP镜像工具之间的通信协议：TCP+UDP

1.2 组网方式和配置原则介绍

1.2.1 端口重定向/策略路由原理

侧挂的情况下，需要在交换机或者路由器上进行配置，有两种方式：

- 端口重定向
- 策略路由

一般来说，端口重定向和策略路由实现相同的功能，只是起的名字不一样，从目前了解的情况看，只有H3C把该功能定义为端口重定向，其他厂商通常把该功能命名为策略路由。端口重定向/策略路由的数据流图如图所示：

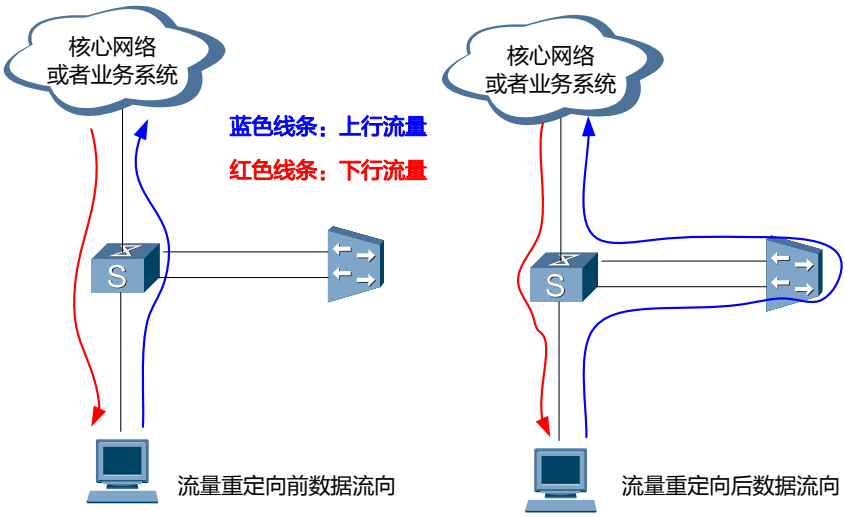

图3 端口重定向/策略路由数据流图

下面以端口重定向为例说明：

交换机上可以配置来自某个接口的报文直接重定向到另一个接口上；例如公司的3528可以进行如下的配置：

[Quidway]acl number 3000

[Quidway-acl-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255

[Quidway]interface Ethernet 0/20

Quidway-Ethernet0/20]traffic-redirect inbound ip-group 3000 next-hop 10.1.6.1 10.1.1.240

简单说明：在3528上配置一个ACL 3000；

对入口方向匹配IP-GROUP 3000的报文，进行报文重定向，重定向的时候有两跳：10.1.6.1 和 10.1.1.240

其中10.1.6.1的优先级高，当10.1.6.1接口出现故障的时候，选择10.1.1.240

1.2.2 ARP 准入控制原理

当启用ARP准入控制功能，在部署了TSM安全代理的网络区域，会选举出若干个干扰源。当发现网络中有非法终端存在的时候，这些干扰源将对非法终端发送ARP干扰报文，干扰其正常使用网络。发现网络中存在非法终端主要有两种方式：

1）设备扫描器周期对指定的网络实施扫描，发现网络中存在的非法终端；

2）干扰源对网络中的ARP报文进行探测，当发现IP设备新接入网络（ARP广播），主动探测该设备是否合法终端。

一旦确认网络中存在非法终端，干扰源将对非法终端发送ARP干扰报文，发送干扰报文的类型和原理如下：

1）仿冒网关欺骗：仿冒网关给被干扰终端发送ARP报文，使得被干扰终端学习到错误的网关MAC地址。终端学习到错误的网关MAC地址，将无法通过网关访问外部设备。（被干扰终端可以访问同一个VLAN的其他设备，如果被干扰终端安装了ARP防护软件，则该方式失效）

2）构造IP地址冲突：给被干扰终端发送ARP欺骗报文，使得被干扰终端提示IP冲突，通常情况下，IP冲突后，Windows PC无法正常使用网络。（如果被干扰终端的操作系统是Windows 7，该方式不生效；如果被干扰终端安装了ARP防护软件，则该方式失效）

3）交换机端口飘移：伪造被干扰终端发送一个ARP报文，欺骗局域网范围的交换机，使得交换机学习错误的端口信息，误以为被干扰终端位于发起攻击的PC到网关的路径上。（如果交换机开启了ARP防护功能，交换机端口飘移方式失效，建议管理员在交换机上修改配置，关闭ARP防护功能。）

可以指定ARP干扰的范围，只有指定范围的外来终端，才会被干扰。对于无法部署TSM安全代理的IP设备，可以通过添加例外设备的方式，避免被干扰。

ARP准入控制功能局限性：

1）对于被干扰终端，如果被干扰终端安装了ARP防护软件，则仿冒网关欺骗和构造IP地址冲突方式失效，只有交换机端口飘移能够对被干扰终端其到干扰作用；

2）如果交换机开启了ARP防护功能，则交换机端口飘移的干扰方式失效，只能使用仿冒网关欺骗和构造IP地址冲突两种方式对非法终端实施干扰。如果要启用ARP准入控制功能，建议关闭交换机的ARP防护功能；

3）如果被干扰终端部署了主机防护功能（如SEP 11.0），会产生一些告警提示，告知网络中存在ARP攻击；

4）对于干扰源（安装了TSM AGENT的终端），如果干扰源安装了一些主机防护软件，可能会阻止TSM AGENT发送干扰ARP报文，导致干扰功能失效（目前尚未发现这样的主机

防护软件，但是存在这样的风险）。并且可能提示终端正在发起ARP攻击，让客户误以为TSM AGENT是病毒；

5）使用ARP准入控制，只能阻止或者部分阻止被干扰终端访问网络，无法实现认证前域、隔离域和认证后域的功能；

6）由于ARP报文只能在二层网络中转发，如果某个VLAN中计划实施ARP准入控制功能，那么该VLAN中必须有已经部署了TSM安全代理的终端，而且TSM安全代理安全认证通过。

1.2.3 TSM 服务器的组网和配置原则

1. 单服务器集中组网方案

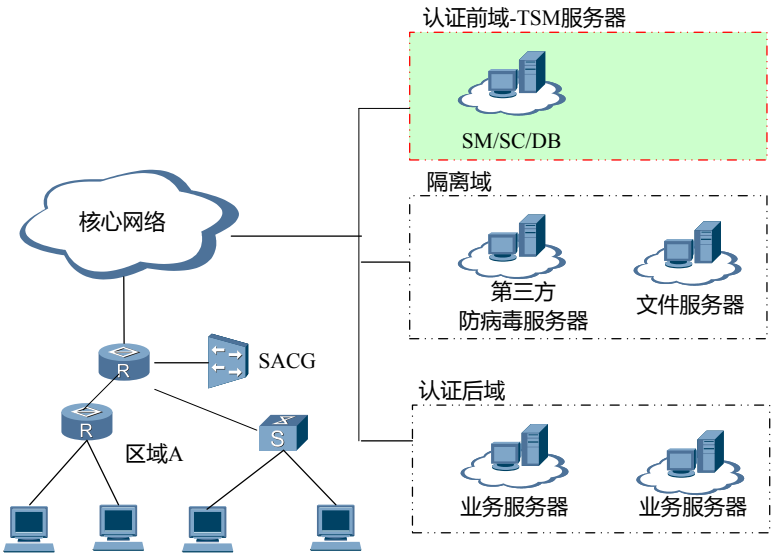

图4 单服务器集中组网方案

1）组网方式：

说明：使用一台服务器，安装全部软件模块，包括数据库，管理服务器以及控制服务器，适合较小型网络，以及不需要数据库备份的局点。

服务器数量：1台

服务器1安装组件：数据库，管理服务器SM，控制服务器SC

2）选择该方案，需要满足如下条件：

- 终端数量：

  建议单服务器集中组网时，被管理终端的数量小于2000。

  当终端数量大于2000终端时，网络的规模已经比较大，对可靠性的要求会更高，虽然一个控制服务器SC能够管理1万终端，但是从可靠性的角度考虑，不推荐使用该方案。

- 网络环境：

  A）适用于网络相对集中，网络之间的带宽比较大的网络，例如典型的园区网。

  B）适用于小型多分支机构的网络，并且分支机构到总部之间的带宽比较小，典型的如金融行业的网络，分支机构到总部的带宽是2Mbps。能够容忍因为分支机构到总部链路故障，导致无法提供有效的准入控制访问。

  小型多分支机构的定义：

  分支机构到总部的带宽=2Mbps，分支机构的终端数量<=100

  分支机构到总部的带宽=10Mbps，分支机构的终端数量<=500

  评估模型：

  需要计算终端对带宽的需求，需要保证在一般情况下（包括认证阶段，以及平时的业务阶段对带宽的占用率<1%，认证阶段<5%）

  假设分支机构到总部的带宽=2Mbps

  5%的带宽=2000Kbps*5%=100Kbps

  1%待带宽=2000Kbps*1%=20Kbps

  查询下表的数据，400终端可以满足认证阶段对带宽的需求，考虑到其他的如补丁/软件分发等文件下载业务，终端数<=100。

- 该方案的优点和局限性：

  单服务器集中组网方案，由于只有一台服务器，只能安装一个数据库，无法提供数据库热备功能，当数据库发生故障的时候，会影响如下业务：

  A）管理员无法通过操作界面管理相关业务；

  B）控制服务器SC不重启的情况下，虽然能够提供基本的准入控制业务，但是终端的违规信息无法上报服务器并且写入数据库，需要等到数据库恢复正常后才能上报；

C）当控制服务器SC重启的情况下，控制服务器SC无法提供任何服务；

单服务器集中组网方案，由于只有一台服务器，只能部署一个控制服务器SC，无法提供控制服务器失效转移功能，当控制服务器SC发生故障的时候，无法提供终端的身份认证和准入控制等基本服务。

2. 双服务器集中组网方案

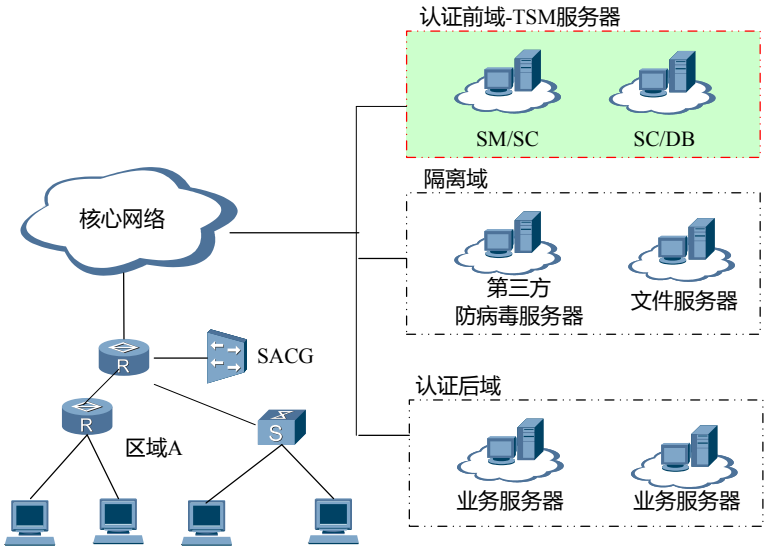

图5 双服务器集中组网方案

1）组网方式

说明：使用两台服务器，集中部署。安装两个控制服务器SC，提供资源池模式的负载均衡和失效转移方案，允许一个控制服务器发生故障的时候，另一个控制服务器能够继续工作。

服务器数量：2台

服务器1安装组件：管理服务器SM、控制服务器SC

服务器2安装组件：控制服务器SC、数据库DB

2）选择该方案，需要满足如下条件：

- 终端数量：

  建议双服务器集中组网时，被管理终端的数量小于10000。

当终端数量大于10000终端时，网络的规模已经非常大，对可靠性的要求会更高，虽然一个控制服务器SC能够管理1万终端，两个服务器能够支撑20000终端，但是从可靠性的角度考虑，1万终端以上的网络不建议使用该方案。

- 网络环境：

  适用于网络相对集中，网络之间的带宽比较大的网络，例如典型的园区网。

  适用于小型多分支机构的网络，并且分支机构到总部之间的带宽比较小，典型的如金融行业的网络，分支机构到总部的带宽是2Mbps。能够容忍因为分支机构到总部链路故障，导致无法提供有效的准入控制访问。

  小型多分支机构的定义参见单服务器集中组网方案的说明。

- 该方案的优点和局限性：

  双服务器集中组网方案，由于只有两台服务器，无法部署数据库镜像方案，无法提供数据库热备功能，当数据库发生故障的时候，会影响如下业务：

  A）管理员无法通过管理界面登录管理界面管理相关业务；

  B）控制服务器SC不重启的情况下，虽然能够提供基本的准入控制业务，但是终端的违规信息无法上报服务器并且写入数据库，需要等到数据库恢复正常后才能上报；

  C）当控制服务器SC重启的情况下，控制服务器SC无法提供任何服务；

3. 三服务器集中组网方案

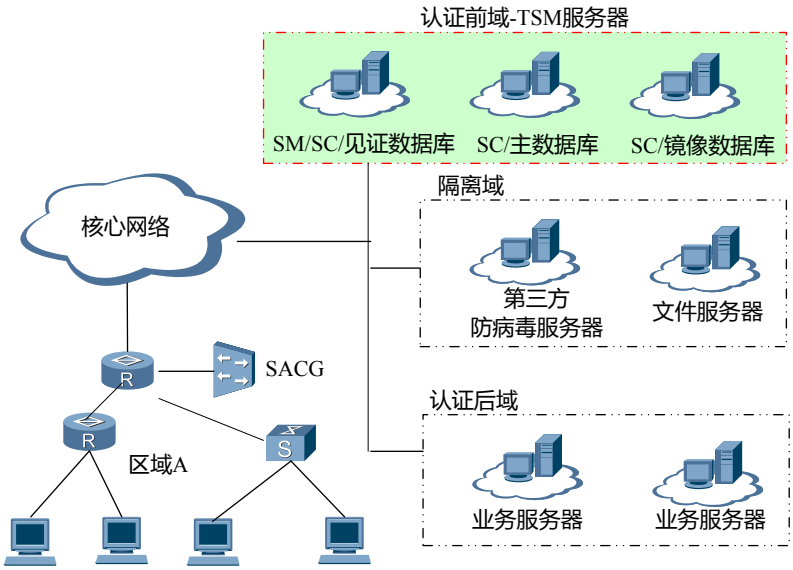

图6 三服务器集中组网方案

1）组网方式

说明：使用三台服务器，集中部署。安装三台SQL SERVER 2005数据库，该数据库组成数据库镜像，提供数据库备份方案。安装三个控制服务器SC，提供资源池模式的负载均衡和失效转移方案，允许一个控制服务器发生故障的时候，另两个控制服务器能够继续工作。

服务器数量：3台

服务器1安装组件：管理服务器SM、控制服务器SC、见证数据库

服务器2安装组件：控制服务器SC、主数据库

服务器3安装组件：控制服务器SC、镜像数据库

2）选择该方案，需要满足如下条件：

- 终端数量：

  建议三服务器集中组网时，被管理终端的数量小于20000。

  当终端数大于20000终端时，没有现成的方案，需要市场技术与研发一同评估后提供。

- 网络环境：

  适用于网络相对集中，网络之间的带宽比较大的网络，例如典型的园区网。

  适用于小型多分支机构的网络，并且分支机构到总部之间的带宽比较小，典型的如金融行业的网络，分支机构到总部的带宽是2Mbps。能够容忍因为分支机构到总部链路故障，导致无法提供有效的准入控制访问。

  小型多分支机构的定义参见单服务器集中组网方案的说明。

- 该方案的优点和局限性：

  数据库提供了热备功能，当一个数据库发生故障的时候，业务不中断。

  系统提供了控制服务器失效转移功能，当单个控制服务器发生故障，不能提供服务的时候，终端能够从另一个控制服务器获得准入控制等服务，业务不中断。

  如果客户的审计数据(违规信息)量比较大，需要引入更多的数据库存储违规信息。按照TSM V100R002版本的设计，如果一种类型的违规信息的数据量一个月的数据大于2千万条记录的时候，存储在一个数据库中，将使得数据库性能急剧下降。因此，当一种类型的违规信息的数据量一个月大于2千万条记录的时候，需要部署多个数据库，分

担数据存储方面的压力。这时候可以在见证数据库上部署一个扩展数据源，分担违规信息存储压力。

具体实施的时候，可以在分阶段上线过程中，观察违规信息数据量增长的情况，决定是否需要引入扩展数据库，存储违规信息。

4. 多服务器集中组网方案

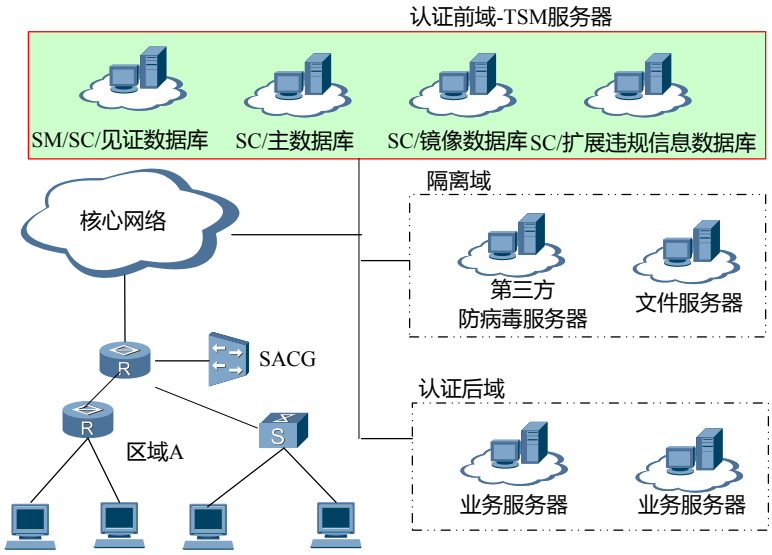

图7 多服务器集中组网方案

1）组网说明

当终端的数量超过2万，则需要使用更多的控制服务器SC，分担业务压力。

2）组网方式

说明：使用四台服务器，集中部署。安装四台SQL SERVER 2005数据库，其中三台数据库组成数据库镜像，提供数据库备份方案，另外一个数据库用于作为违规信息的扩展数据源。安装四个控制服务器SC，提供资源池模式的负载均衡和失效转移方案，允许一个控制服务器发生故障的时候，另三个控制服务器能够继续工作。

服务器数量：4台

服务器1安装组件：管理服务器SM、控制服务器SC、见证数据库、扩展违规信息数据库

服务器2安装组件：控制服务器SC、主数据库

服务器3安装组件：控制服务器SC、镜像数据库

服务器4…N安装组件：控制服务器SC、扩展违规信息数据库

5. 控制服务器SC分布式组网方案：

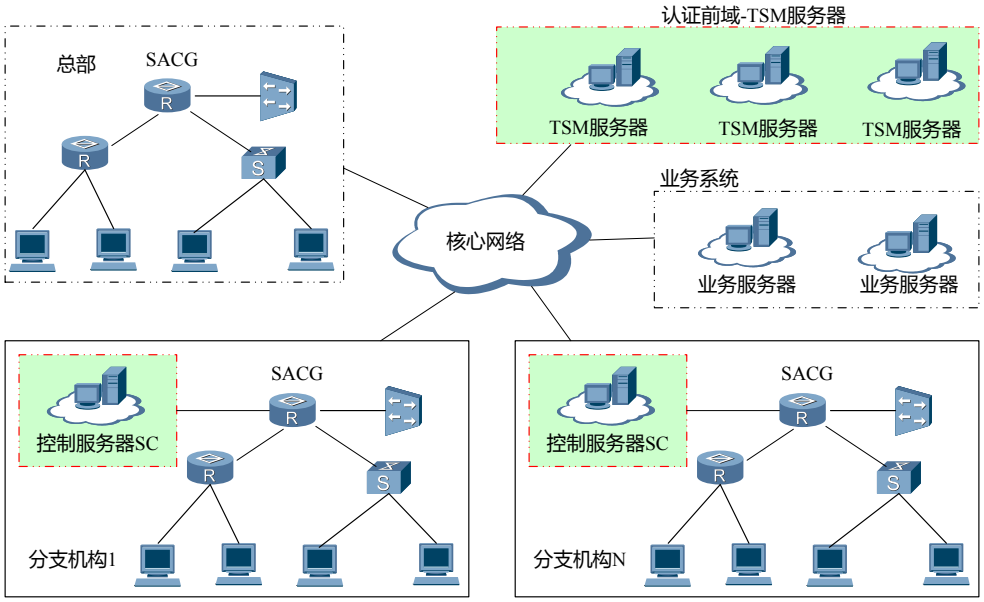

图8 控制服务器分布式组网方案

1）组网方式

说明：对于企业存在多个分支机构，分支机构的终端规模比较大，并且分支机构之间的网络带宽比较小的情况，可以使用分布式组网方案。首先需要识别总部和分支机构，对于每个分支机构，配置1~2个控制服务器SC（根据客户是否需要在分支机构实现控制服务器备份决定）。总部不单独配置控制服务器SC，直接使用数据中心的TSM服务器作为控制服务器SC（假设总部与数据中心在一个区域）。

服务器数量：

- 分支机构：可以选择不提供失效转移功能，部署1台控制服务器；可以选择使用总部的控制服务器提供失效转移功能，部署1台控制服务器；可以选择分支机构本地提供失效转移功能，部署2台控制服务器。
- 总部：参照集中组网方案，如果分支机构选择总部的控制服务器提供失效转移功能，配置服务器的时候，终端数量=总部终端数量+最大分支机构的终端数量。

服务器安装组件：

- 分支结构：只安装控制服务器SC
- 总部：参照集中组网方案

2）选择该方案，需要满足如下条件：

- 终端数量：

  整个企业（包括总部和所有分支机构）被管理终端数量的范围：1--20000终端

- 网络环境：

  存在多个分支结构，分支机构是典型的园区网，或者是银行的市级分行；

  分支机构到总部的网络带宽有限，评估采用集中组网，可能会占用大量分支机构之间的网络带宽；

  分支机构到总部之间的网络质量难以保障，总部和分支机构之间的网络可能中断，使得分支机构的终端无法连接总部数据中心。

- 方案的风险以及可靠性：

  方案的鞲小以及可靠性参照集中组网方案。

3）分布式部署环境下数据同步对带宽的需求

假设系统中存在10万账号，按照这样的规模计算，一个账号的数据量<200字节，总量<=20M字节，加上安全策略等各种缓存数据，估计数据量<=30M字节。

假设分支机构到总部之间的网络带宽是2Mbps，控制服务器SC从总部区所有的缓存数据，假设占用全部带宽，所需要的时间=30M*8bit/2Mbps=120秒。所需要的时间约等于2分钟。

控制服务器SC每四个小时从总部同步一次数据，因此数据同步部分对分支机构到总部之间的网络占用=2/(4*60)*100%=0.83%

6. 分级部署方案：

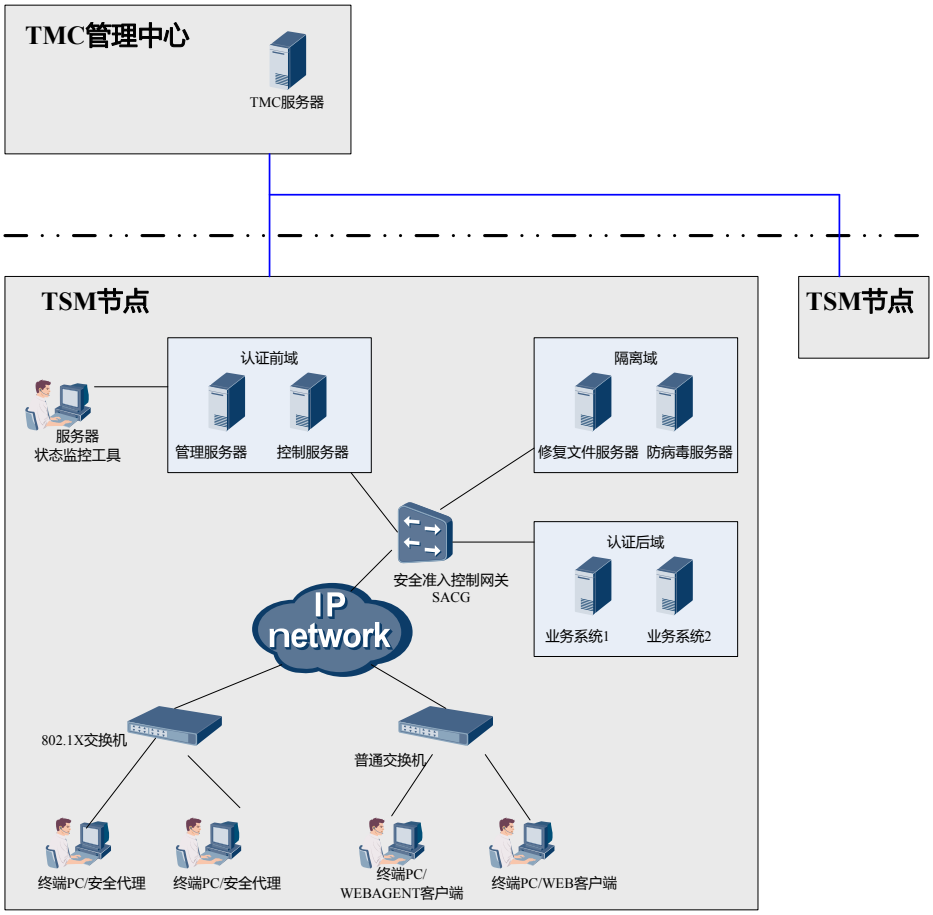

图9 分级部署方案

1）组网方式

对于超大规模的网络，如全国性的集团公司，各个省/分公司独立管理和运维自身的IT系统，在业务上接受集团公司的指导。这种情况下，可以推荐使用分级部署方案，各个省公司/分公司部署TSM节点，在集团公司部署TMC管理中心，通过TMC管理中心进行业务监控。

服务器数量：

- TSM节点：参见TSM节点的部署方案以及配置；
- TMC管理中心：当前TMC管理中心只提供单机功能，只需要一台服务器。

服务器安装组件：

- TSM节点：参见TSM部署方案
- TMC管理中心：TMC管理中心组件

2）选择该方案，需要满足如下条件：

- 对组织管理模式的要求：

对于TSM系统运维来说，要求各个分公司自行管理和运维TSM系统，总公司只需要对各个分公司实施的情况进行监控。

- 对网络的要求：

总公司和分公司之间的网络是可以互联互通的，可以是内网层面的互联互通，也可以通过互联网，使其互联互通。

3）单个TSM节点与TMC之间的带宽需求

TSM和TMC之间的通信包括两个部分的内容：

- 配置数据同步相关流量

TMC与TSM之间的配置数据总量，取决于在TMC上配置以及下发给某个TSM节点的策略模板数量，一个策略模板的大小约几十到几百K，以1M字节计算，假设TMC给TSM下发10个策略模板/补丁模板。

TMC给TSM下发的数据总量=10*1M字节=10M字节；

TMC与TSM之间每天进行一次数据同步，所需的平均带宽

=10*1000K*8/(3600*24)=0.9Kbps

TMC与TSM之间用于配置同步对带宽的需求可以忽略不计。

- 补丁文件下载流量

初次补丁同步的时候，补丁的规模比较大，如下数据可以作为一个参考：

操作系统类型：XP、2003、VISTA、Win 7

语言：中英文

补丁级别：各种级别的补丁，包含SP补丁

这样一个补丁的集合大约是4G字节左右。

后续微软会持续的发布补丁，发布频率为1周到2周发布一次，每次发布几个补丁，假设这些补丁的大小的总和<100M字节。由于微软后续发布是一个常态，因此以后续发布补丁作为评估TMC/TSM之间带宽需求的标准。假设TSM/TMC之间的同步时间限制4小时，

TSM/TMC之间的带宽需求=100*8*1000K/(4*3600)=55Kbps。

初次补丁同步的时间可能会长一些，为了降低对网络的影响，可以通过在TMC上的FTP

服务器上配置限制传输的速率，降低网络带宽占用。

1.2.4 硬件 SACG 准入控制的组网和配置原则

1. SACG直挂路由模式

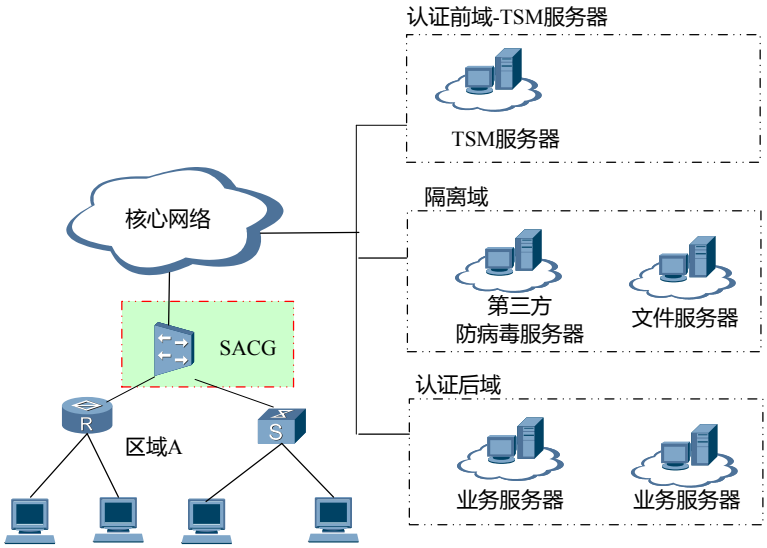

图10 SACG直挂路由模式部署方案

1）组网方式：

SACG直挂路由模式如图所示，SACG设备在这种组网模式下，通常充当两种类型的角色，第一是网关，要么是接入终端的网关/服务器设备的接入网关，另一种是互联网出口网关。根据部署的位置，如果作为终端的接入网关，可以控制终端访问网关范围外的网络资源；如果作为服务器设备的接入网关，可以控制终端PC对服务器设备的访问；如果作为企业的互联网出口网关，可以控制终端PC对互联网的访问。

这样的部署方式，如果是现成的网络，则需要使用SACG设备替换网关，当网络的规模比较大的时候，可能需要替换比较多的网关，成本较高。如果是新建的网络，则需要购买比较多的SACG设备，作为网关，性价比不高。除了部署在互联网出口位置，作为出口网关外，一般不推荐使用这种部署方案。

2. SACG侧挂路由模式

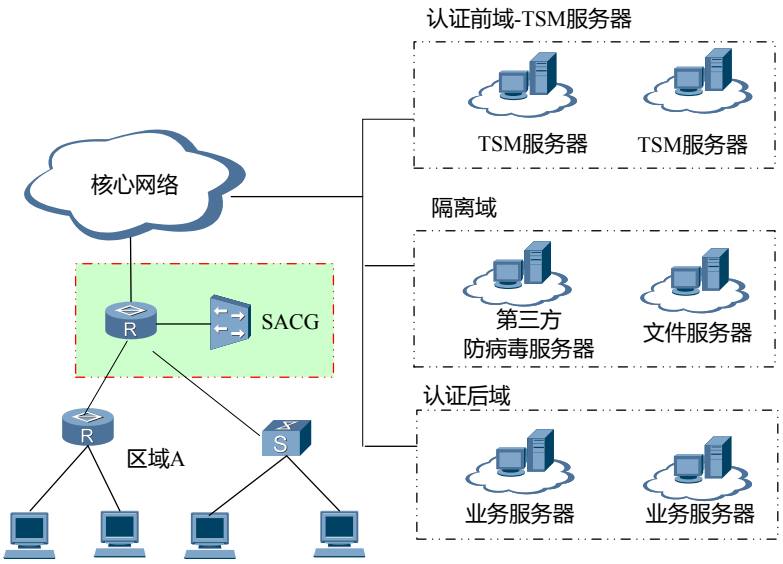

图11 SACG侧挂路由模式部署方案

1）组网方式：

SACG侧挂路由单机模式的组网如图所示，SACG设备侧挂在三层交换机或者路由器上。一般来说，通过在交换机上配置报文重定向，或者在路由器上配置策略路由，把来自终端PC的上行流量重定向到SACG设备，通过SACG设备过滤后，再回到交换机/路由器上执行正常的路由转发。对于来自业务系统，发到终端PC的数据报文，出于对性能的考虑，一般不走SACG，直接通过交换机/路由器发送到合适的设备/终端上。

出于成本的考虑，会根据客户的网络环境，把SACG设备侧挂在能够控制终端PC访问业务系统的关键网络设备上，如园区网的核心交换机/路由器，或者数据中心前的交换机/路由器。具体部署的位置，需要根据客户网络的情况，以及客户的业务目标，折中考虑。

2）配置原则：

满足如下条件，可以考虑采用侧挂路由模式部署方案：

- 对终端之间的互相访问控制要求不严格，需要重点保护企业的业务系统；
- 终端到业务系统之间的数据流量有比较集中的控制点；
- 允许对网络的配置进行少量的调整；

3）双机方案建议

如果客户的网络是双平面的网络，通常能够找到两个对称的侧挂点，使用两个SACG设备，侧挂在两个对称的侧挂点上。如果客户的网络本身没有提供双平面方案，不建议在同一

个设备上部署两个SACG设备。通过配置，可以使得当一个SACG设备发生故障的时候，流量走正常路由，也不会导致网络中断，不会影响该网络的可靠性。

3. SACG透明/混合模式

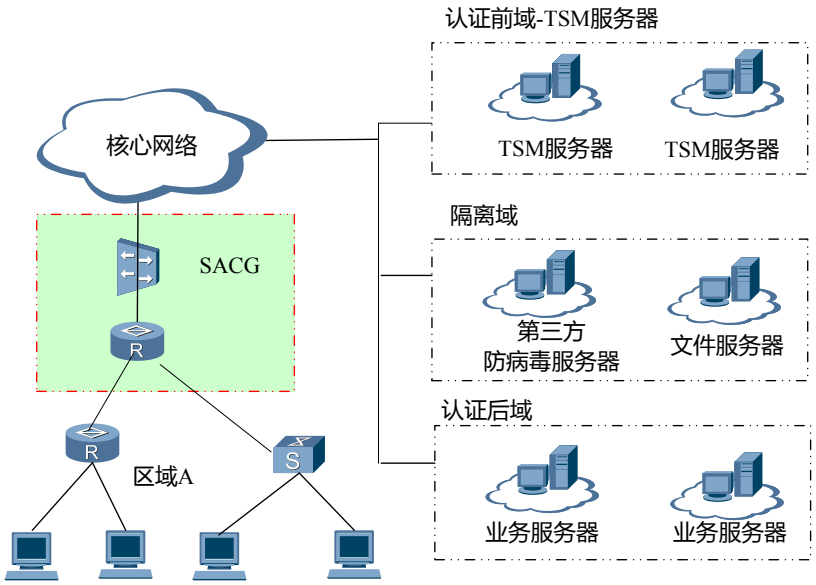

图12 SACG透明/混合模式部署方案

1）组网方式

SACG透明/混合模式组网比较简单，在网络中找到一个控制点，然后把SACG设备直接串接在网络中，如图所示。所有通过SACG的流量，都会受到控制。

这样的组网方式简单，而且不需要改变现网的网络拓扑结构，而且部署和实施简单。

2）配置原则：

当满足下列条件，可以考虑采用透明/混合模式的组网方案：

- 对终端之间的互相访问控制要求不严格，重点保护企业的业务系统；
- 不希望对网络的拓扑和配置进行调整；
- 链路的端口是GE口或者FE口(目前各个型号的SACG设备,没有支持10GE的接口)；

3）透明模式/混合模式双机方案建议

如果客户的网络支持双平面，则可以通过在两个链路上分别部署SACG设备，实现双平面的需求。

4）透明模式/混合模式组网局限性

吞吐能力局限性：

透明模式/混合模式组网的情况下，由于SACG设备串接在两个网络设备之间，网络的吞吐能力的扩展性首先与SACG设备的处理能力。以USG5300系列为例，USG5360产品最大处理能力标称值等于6G，USG5360提供了四个可以做聚合的端口，假设四个可以聚合的端口分为两组，两两聚合成一个2G的端口，分别连接两个网络设备，这样USG5360的最大处理能力为2G。后续如果处理能力不足，将很难通过扩容的方式，提高设备的处理能力。

接口数量局限性：

SACG设备的接口数量有限，以USG5300系列为例，USG5300设备有6个GE接口，如果客户的网络环境比较复杂，例如没有一个可以串接在两个设备之间的链路用于准入控制，那么SACG设备可能需要连接多个网络设备，SACG设备的接口比较有限，在这种网络环境下，需要比较多的SACG设备。

可靠性：

由于原来的Eudemon 300/500/1000系列SACG设备已经停产，替换的USG系列产品没有提供BYPASS功能，在透明模式/混合模式下，当SACG设备异常掉电后，网络将会中断。

4. 如何选择SACG设备

选择SACG设备的时候，需要考察两个指标：

第一：需要考察SACG设备的在线用户数，这可以通过SACG上标称支持的在线用户数进行选择。

第二：需要考察SACG设备的处理能力，不同的组网方式，对SACG设备的处理能力要求不同，对SACG设备处理能力的要求：

在侧挂路由模式组网的时候，由于只有上行流量会经过SACG设备，因此需要评估侧挂设备的数据流量。如果只控制终端对侧挂设备上行口的访问，那么SACG设备的处理能力应该是上行流量的1/10。例如，如果上行口是10G的链路，则要求SACG设备的处理能力至少是1G。

注意：在做SACG设备选型的时候，除了关注SACG设备的处理能力外，还需要关注如下两个问题：

1）SACG设备是否支持端口聚合（聚合后可以看做一个网口，提供更大的处理能力），以及交换机/路由器上的端口是否支持端口聚合；

2）交换机/路由器上是否有足够的端口，根据带宽的需求，每G的带宽需要1端口。需要注意交换机/路由器上采用的接口类型（光口/电口），避免SACG设备在现场无法与交换机/路由器上的端口对接。

假如侧挂设备是核心交换机，或者汇聚交换机（该交换机支持策略路由或者端口重定向功能），如果需要控制终端上行的业务流量，以及控制终端之间的业务流量（通过核心交换终端之间的业务流量），如图所示：

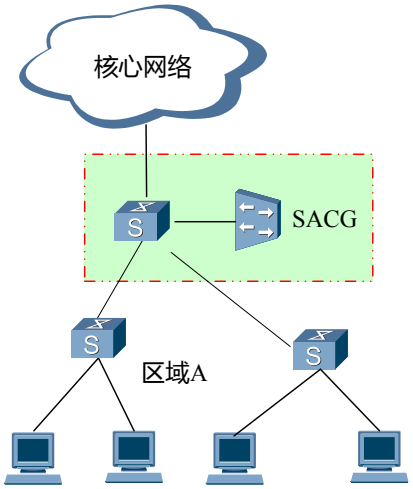

图13 SACG侧挂侧挂核心交换机示意图

这时候需要评估两个部分的流量：

- 通过核心交换机上行的流量；
- 通过核心交换机到其他终端的双向业务流量；

对SACG设备处理能力的要求：(通过核心交换机上行的流量/10) + 通过核心交换机到其他终端的双向业务流量。

1.2.5 802.1X 准入控制的组网和配置原则

1. 在接入层交换机上实施802.1X

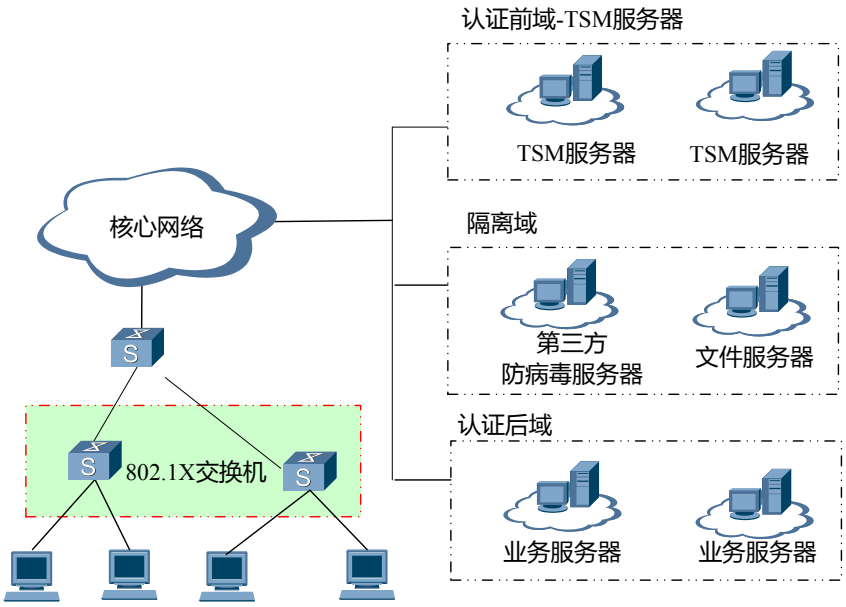

图14 在接入层交换机上实施802.1X

1）方案说明：

在最靠近终端的交换机上启用802.1X，终端正常接入网络前，需要先部署安全代理（一般情况下，不支持Windows自带的安全代理，除非在服务器端进行特殊的配置）。

该部署方案能够达到的控制效果，与交换机的特性有关，一般来说可以区分两种类型的交换机：

- 只支持端口关闭的802.1X交换机

只支持端口关闭的交换机，有两种选择：

第一种是身份认证通过后，开通交换机端口，而不管安全检查的结果是否满足企业的安全策略（可以选择使用其他的准入控制设备配合实现隔离和控制）。

第二种是只有身份认证和安全认证通过后开通交换机端口，其余情况均关闭交换机端口。这时候，终端无法通过网络实施修复，例如没有安装杀毒软件，被隔离的时候，只能通过光盘/U盘的方式，在终端安装杀毒软件，并且想办法更新病毒库。

- 支持GUEST VLAN和动态VLAN的802.1X交换机

支持GUEST VLAN和动态VLAN的交换机，通过配置，可以使得没有部署安全代理的终端能够访问GUEST VLAN，通过GUEST VLAN部署TSM安全代理。在认证过程中，根据安全检查的结果，给交换机下发隔离域VLAN或者认证后域VLAN，实现对问题终端的隔离。

2）配置原则：

当满足如下条件，可以使用在接入层交换机上实施802.1X：

- 客户要求终端在接入前，不允许访问任何网络资源，包括邻居的终端；
- 客户具备实施和管理802.1X的能力，包括部署TSM安全代理的能力；
- 客户的所有接入层交换机都支持802.1X，不存在使用HUB的情况；

3）其他局限性：

对于只支持端口关闭的802.1X交换机，部署TSM安全代理比较困难，目前主要有两种方式：

第一种：通过U盘/光盘等物理介质的方式，手工在终端PC上安装TSM安全代理；

第二种：由专门的部门负责安装软件，例如在一个受控的区域内，交换机不启用802.1X，使得终端在没有部署TSM安全代理的时候也能够接入网络，通过网络下载并且安装TSM安全代理，或者使用克隆工具重新安装系统。

2. 在汇聚层交换机上实施802.1X

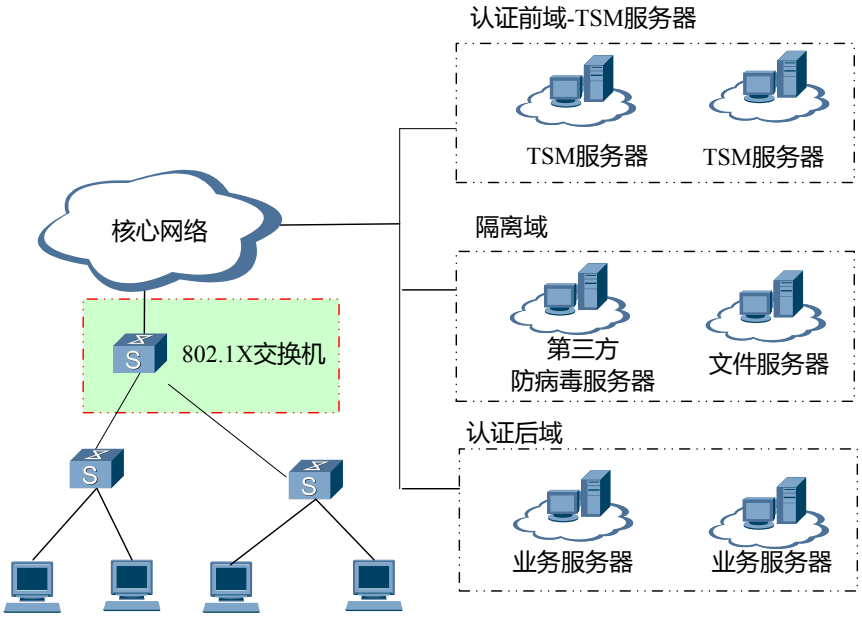

图15 在汇聚层交换机上实施802.1X

1）方案说明：

在汇聚层交换机上实施802.1X（一般来说，汇聚层交换机都能够支持802.1X），这时候，下层交换机之间的终端在没有认证前可以互相访问。在汇聚层交换机上实施802.1X，

可以减少802.1X的控制点，降低实施的复杂性。

2）配置原则：

当满足如下条件，可以使用在汇聚层交换机上实施802.1X：

- 客户允许终端在认证前，可以访问接入交换机之间的终端；
- 客户具备实施和管理802.1X的能力，包括部署TSM安全代理的能力；
- 接入层的交换机/HUB等设备，包括无线AP等，必须支持802.1X组播报文透传；

3）其他限制和局限性：

为了在汇聚层交换机实施802.1X，要求该交换机支持MACBASED的802.1X。从目前获得的资料来看，只有国内厂商的交换机才支持该特性。CISCO交换机没有发现能够支持该特性，海外其他厂商的交换机不清楚能否支持MAC BASE的802.1X特性。

3. 接入层/汇聚层混合实施802.1X

当客户的网络比较复杂的时候，如果强烈要求实施802.1X，也可以采用在接入层/汇聚层混合的方式，方案与配置原则与前面章节一致，这时候802.1X的管理会比较复杂。

4. TSM系统支持交换机列表

厂商	型号	备注
CISCO	Crystal 2950/2960	支持VLAN下发 支持根据终端安全检查结果下发不同的VLAN 其中2950交换机需要特定的软件版本才能支持VLAN下发 2960交换机没有测试验证
CISCO	Crystal 3550/3560	支持VLAN下发 支持根据终端安全检查结果下发不同的VLAN 3550交换机没有测试验证
华为	Quidway S3526	支持VLAN下发 支持根据终端安全检查结果下发不同的VLAN
华为3COM	H3C S3600	支持VLAN下发

		支持根据终端安全检查结果下发不同的VLAN

由于实验室的设备有限，能够进行验证的设备很少。当在组网遇到不在上述列表中的设备的时候，建议如下：

1. 找交换机厂商确认该交换机是否支持标准的802.1X功能，以及支持的协议版本

2. 如果该交换机支持标准的802.1X，并且协议版本是V1版本或者V2版本，需要询问厂商是否对1X有特殊的限制，如果没有特殊的限制，原则上TSM能够与该设备对接

3. 对于没有验证过的厂商的交换机，只有通过测试，才能确定是否能够根据终端安全检查结果下发不同的VLAN

1.2.6 基于主机防火墙准入控制/互访控制的组网和配置原则

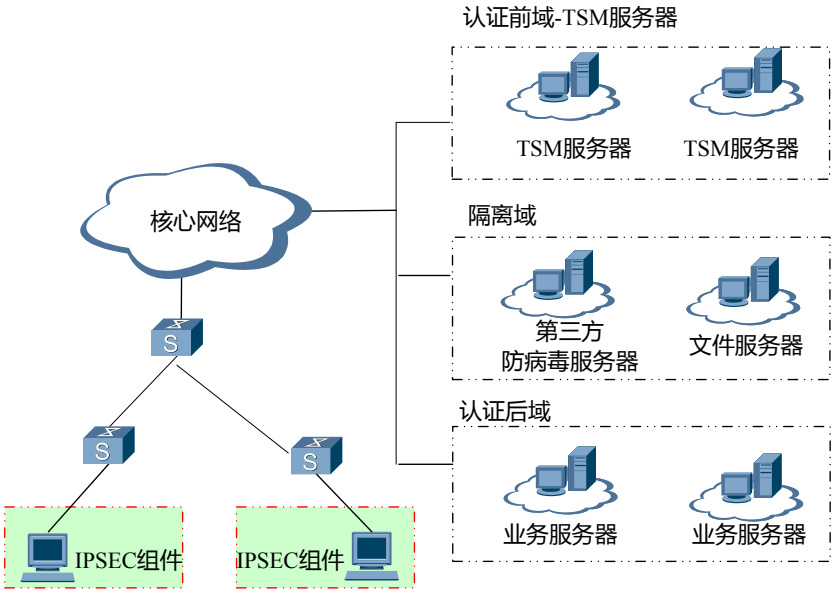

图16 通过主机IPSEC组件实施终端准入和互访控制

1）方案说明

该方案的前提是终端安装安全代理。安装代理通常有两种强制方式：

- 通过管理手段强制安装安全代理，并且定期/不定期检查代理安装情况；
- 在业务系统前部署其他强制手段，如硬件SACG，协助强制部署安全代理；

准入控制功能：

终端PC安装了安全代理后，在没有通过身份认证前，通过主机软件控制只能访问定义的认证前域。当通过身份认证，但是安全检查不通过，则通过主机软件控制只能访问隔离域。当安全检查通过的时候，可以访问特定的认证后域。

终端互访控制：

终端PC安装了安全代理，并且启用了互访控制功能，对于没有安装安全代理的终端，不管是否合法终端（添加到例外列表的终端除外），之间不能正常执行TCP/IP通信（能够PING通，但是不能做TCP/UDP等业务）。对于两个安装了安全代理的终端，如果这两个终端属于同一个可信域，那么这两个终端可以正常通信。如果两个安装了安全代理的终端属于不同的可信域，则无法正常通信。终端之间互访控制，可以支持NAT穿越（支持NAT穿越的局限性参见版本发布材料中产品固有缺陷说明）。

启用终端互访控制功能的时候，按照操作指导书的要求，分阶段实施。

2）配置原则

当满足如下条件，可以推荐使用软件准入控制：

- 准入控制的粒度控制比较粗，不需要配置特别多的准入控制规则（详细情况参见软件准入控制的产品规格）；
- 不需要使用VPN的方式接入内网，或者在使用VPN接入的时候，允许软件准入控制功能失效；

当满足如下条件，可以使用软件互访控制：

- 不需要使用VPN的方式接入内网，或者在使用VPN接入的时候，允许终端互访控制功能失效；
- 具备较强的管理能力，能够识别并且管理例外设备；

3）其他限制和局限性：

启用逃生通道的局限性：

终端终端代理检测到控制服务器SC连接失败，将启用逃生通道，启用逃生通道将直接关闭终端互访控制功能，会带来如下问题：

- 无法阻止外来终端对该设备的访问；
- 在比较短暂的时间内（4分钟左右），可能无法与邻居的可信终端通信，原因是不

同终端检测到控制服务器SC连接失败的时间会有一定的差异；

- 如果该设备因为故障等原因无法连接控制服务器SC，而不是因为控制服务器故障，该终端无法与邻居终端正常通信；

1.2.7 ARP 准入控制配置原则

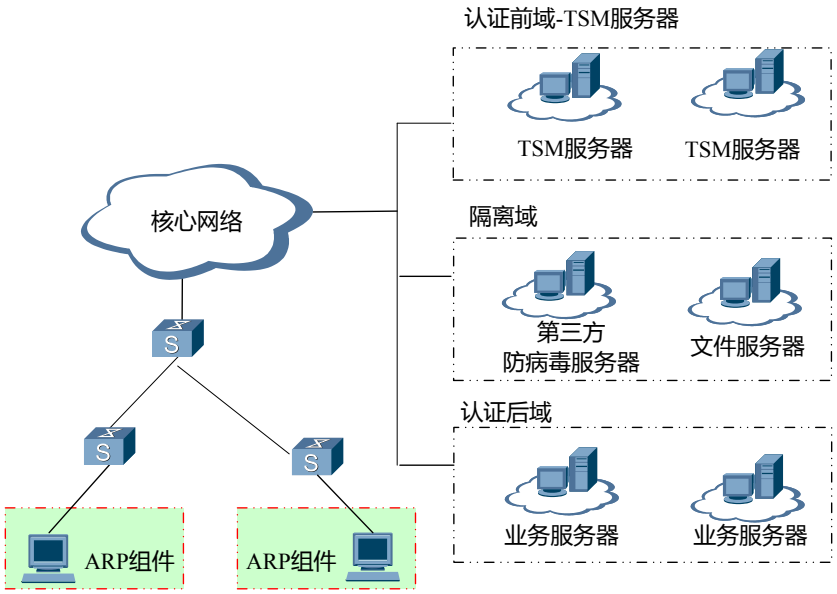

图17 通过ARP实施终端准入控制

1）方案说明

ARP准入控制功能：

当实施ARP准入控制的时候，可以通过干扰的方式，阻止非法终端访问网络。也可以通过干扰的方式，让终端断断续续使用网络，并且能够在间歇期间下载并且安装TSM安全代理。

2）配置原则

当满足如下条件，可以实施ARP准入控制：

在计划实施ARP准入控制的VLAN中（二层网络），已经部署了TSM安全代理，并且有TSM安全代理通过认证；

3）其他限制和局限性：

限制和局限性参见ARP准入控制原理部分，关于局限性的描述。

1.2.8 服务器状态监控工具组网和配置原则

TSM系统提供一个工具，协助监控各个TSM服务器的状态，当服务器发生故障的时候，管理员能够及时发现问题，及时修复，降低故障的影响。状态监控工具是一个部署在服务器之外的应用程序，可以部署在管理员的终端PC上。状态监控工具可以发送邮件告警，短信告警。如果要发送短信告警，要求使用短信猫（调制解调器），并且该短信猫需要部署在可以接入GSM的环境中（不要部署在机房，机房的电磁屏蔽很可能导致短信猫无法接入GSM网络）。短信猫是选配件，需要在报价的时候选择是否购买。服务器状态监控工具的部署结构如图所示：

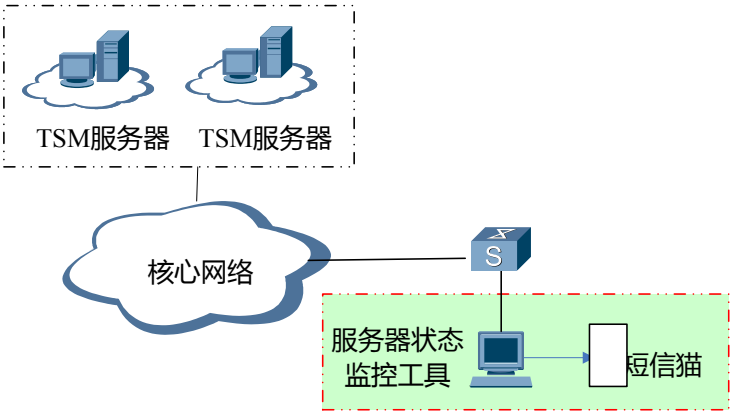

图18 服务器状态监控工具部署示意图

1.2.9 设备扫描器的组网和配置原则

1. 设备扫描器的性能：

1）扫描各种设备所需的时间：

- 发现一个交换机设备，并且从该设备提取信息所需的时间=24秒；

- 发现一个PC设备，并且从该PC提取信息所需的时间=22秒；
- 发现一个已经部署了代理的PC设备，并且从该PC设备提取信息所需的时间=6秒；
- 发现一个IP PHONE/打印机设备，并且从该设备提取信息所需的时间=20秒；
- 探测一个IP地址（不应答任何报文），所需的时间=24秒；

2）设备扫描器的并发处理能力

- 设备扫描器能够并发200个扫描任务

2. ARP方式设备发现性能评估：

网络模型：

假设每个网关设备下带100个IP设备，在这100个IP设备当中，IP PHONE/打印机设备量=5%

对该网关下的设备进行扫描耗时：

(1*24(交换机)+95*22(PC)+5*20(IP PHONE/打印机))/200并发=11秒

假设每次扫描的时间=2小时，那么一个扫描器可以扫描的IP设备的数量=65000

3. IP段方式设备发现性能评估：

通过实际测试发现：按照IP地址段扫描一个B类网段，耗时2.5小时。

部署方式：独立找一台PC计算机部署设备扫描器程序

适用场景：

1）TSM节点采用集中式组网；

2）设备扫描器与被扫描的设备之间没有部署NAT；

3）终端的规模小于65000个终端（使用ARP方式），或者终端的网络地址小于等于一个B类地址段；

部署方式：独立找多台PC计算机部署设备扫描器程序

适用场景1：

1）TSM节点采用集中式部署；

2）终端的规模大于65000个终端（使用ARP方式），或者终端的网络地址大于一个B类地址段；

由于一个扫描器每2.5小时只能扫描完成1个B类网段，因此如果被扫描的网络范围大于等于一个B类网段，建议部署更多的设备扫描器进行扫描，或者降低扫描的频率，增加扫描的时间间隔实现。

需要注意：尽可能确保不同扫描器之间设备扫描的范围不重叠

适用场景2：

1）TSM节点采用分布式部署

在分布式部署的环境下，设备扫描器不适合跨网络区域进行设备扫描，因此需要在各个分支机构的控制服务器SC中挑选一台部署设备扫描器。

部署方式：设备扫描器部署在独立的计算机上（可能是PC）

适用场景：

客户的网络中存在NAT，通过集中部署的设备扫描器无法发现NAT内的PC设备，这时候可以通过在NAT内找一台计算机，在其上部署设备扫描器，实现对NAT内设备的扫描。

特别说明：

需要静态配置NAT映射，使得管理服务器SM能够直接与设备扫描器进行通信。

1.2.10 自定义策略编辑器配置原则

不同的企业在管理上差异较大，产品自身提供的安全策略，往往难以满足企业的一些特殊的需求。TSM系统提供用户自定义安全策略功能，对于一些特殊的安全检查，客户可以利用TSM产品提供的工具，自行开发出安全策略，对终端进行检查和管理。

TSM系统的自定义安全策略，支持对注册表、文件、进程等进行各种组合检查。针对

检查发现的问题，可以定义多种修复措施，包括给终端用户修复建议，或者下载一个文件或者脚本，对终端执行修复操作。

该自定义策略编辑程序，可以根据需要，部署在管理员的PC上。不建议部署在TSM服务器上。

2 产品基本配置说明

2.1 配置说明

第一步：需要收集如下信息：

1. 客户网络中，计划实施终端安全管理的终端数量
2. 客户的网络环境，如果存在分支机构，需要进一步收集如下数据：
   a) 分支机构的数量；
   b) 各个分支机构计划实施TSM的终端数量；
   c) 各个分支机构到总部之间的通信带宽；
3. 数据库是否需要做备份；
4. 估算违规信息的数量级;

第二步. 判断是否需要使用分布式部署方案：

1）如果存在分支机构，在分支机构到总部之间的链路断裂的情况下，如果要求分支机构的认证和准入控制不受影响，则需要采用分布式部署方案，在分支机构部署控制服务器SC；

2）如果存在分支机构，在分支机构到总部之间的链路断裂的情况下，允许分支机构的认证和准入控制受一定的影响，则需要评估分支机构到总部之间的链路带宽，确定是否需要在分支机构部署控制服务器SC：

- 某个分支机构到总部的带宽>=2Mbps，并且分支机构的终端数量<=100，该分支机构可以选择不部署控制服务器SC，分支机构的终端使用总部的控制服务器SC获得准入控制服务；

- 某个分支机构到总部的带宽>=10Mbps，并且分支机构的终端数量<=500，该分支机构可以选择不部署控制服务器SC，分支机构的终端使用总部的控制服务器SC获得准入控制服务；
- 如果某个分支机构不满足上述两个条件时，包括带宽不满足，或者该分支机构终端数量>500，该分支机构需要采用分布式部署方案，在该分支机构部署控制服务器SC。

第三步. 根据集中式组网/分布式组网方案，以及终端规模，评估设备的数量：

1）集中组网推荐配置表

表1　集中组网推荐配置表

可靠性需求	适用终端数量	数据库 0224G030/0224G014	无数据库服务器 0224G037/0224G038
不要求数据库备份 不要求控制服务器SC备份	1-2000 大于2000终端的网络,从可靠性的角度不推荐使用该配置	1PCS	0PCS
不要求数据库备份 要求提供控制服务器SC备份	1-10000 大于10000终端的网络，从可靠性的角度不推荐使用该配置	1PCS	1PCS
要求数据库备份 要求提供控制服务器SC备份	1-20000 大于20000终端的网络，不提供通用配置方案，联系研发和市场技术单独提供	3PCS	0PCS

2）分布式组网推荐配置表

总部的推荐配置参照集中组网推荐配置表。

对于每个分支机构，使用如下配置建议：

表2　分布式组网分支机构推荐配置表

分支机构可靠性需求	适用分支结构终端数量	数据库 0224G030/0224G014	无数据库服务器 0224G037/0224G038
分支机构不要求提供控制服务器SC备份	1-10000 如果某个分支机构的终端数大于10000终端，不提供通用配置方案，联系研发和市场技术单独提供	0PCS	1PCS

分支机构要求提供控制服务器SC备份，使用总部的控制服务器提供备份	1-10000 如果某个分支机构的终端数大于10000终端，不提供通用配置方案，联系研发和市场技术单独提供	0PCS	1PCS
分支机构独立提供控制服务器SC备份	1-10000 如果某个分支机构的终端数大于10000终端，不提供通用配置方案，联系研发和市场技术单独提供	0PCS	2PCS

说明：分布式组网的情况下，需要根据总部和各个分支机构的终端数，选择总部和各个分支结构需要部署的服务器的个数，然后在进行汇总。

第四步：根据评估违规信息的数据量，判断是否需要引入扩展违规信息数据库（使用EXCEL表提供的公式进行计算）

由计算公式得出的扩展数据源数	数据库配置 0224G030/ 0224G014
N	N PCS

在采用分布式部署的情况下，扩展违规信息数据库需要部署在总部。

3）TMC推荐配置表

TMC 推荐软件和数据库部署在同一台服务器上，使用该编码配置：0224G030/0224G014（根据国内/海外分别选择）。

2.2 服务器物理尺寸

表3 服务器物理尺寸表

设备	高（mm）	宽（mm）	深（mm）
IBM X3650M3 机架式服务器	86（2U）	444	698

2.3 TSM 系统配置清单及配置说明

2.3.1 产品配置说明

项目编码：01270009

项目描述：安全产品-Secospace -Secospace Suite

表4 01270009配置清单

序号	BOM 编码	项目描述	备注
1	02236464	组件丨附件-TSM-软件	选配
2	80010082	Package of license-Secospace Suite-Secospace Suite License	必配
3	0223G238	组件丨附件-TSM-业务整机配置方案	选配
4	02234267	组件丨附件-Numen-配套设备	选配
5	04000407	外部成套电缆-世界各国交流电源线-I类设备用带C13连接器-HS	交流电源线成套编码，根据情况选择不能选择该编码的全部

表5 01270009配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	02236464	组件丨附件-TSM-软件	否	PTO编码，见“TSM-软件”配置说明
2	80010082	Package of license-Secospace Suite-Secospace Suite License	否	PTO编码，见“License”配置说明
3	0223G238	组件丨附件-TSM-业务整机配置方案	否	PTO编码，见“TSM-业务整机”配置说明
4	02234267	组件丨附件-Numen-配套设备	否	PTO编码，见“Numen-配套设备”配置说明
5	04000407	外部成套电缆-世界各国交流电源线-I类设备用带C13连接器-HS	否	见“外部成套电缆”配置说明

2.3.2 TSM-软件配置说明

项目编码：02236464

项目描述：组件丨附件-TSM-软件

表6 02236464配置清单

序号	BOM 编码	项目描述	备注
1	0511G080	终端物理软件-Secoway TSM-AF2TSM01-终端安全管理V1R2-含HS 终端安全管理系统软件-安装光盘	选配
2	0511G081	终端物理软件-Secospace TSM-AF2TSM02-终端安全管理V1R2-含HS 终端安全管理系统软件-安装光盘	选配
3	0511G15A	终端物理软件-Secoway TSM&DSM&PSM-AF2DEV01-终端软件新增功能A1-华为-含HS终端安全管理系统软件-软件	选配
4	0511G15B	终端物理软件-Secoway TSM&DSM&PSM-AF2DEV02-终端软件新增功能B1-华为-含HS终端安全管理系统软件-软件	选配
5	0511G15C	终端物理软件-Secoway TSM&DSM&PSM-AF2DEV03-终端软件新增功能C1-华为-含HS终端安全管理系统软件-软件	选配

表7 02236464配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	0511G080	终端物理软件-Secoway TSM-AF2TSM01-终端安全管理V1R2-含HS 终端安全管理系统软件-安装光盘	是	选配
2	0511G081	终端物理软件-Secospace TSM-AF2TSM02-终端安全管理V1R2-含HS 终端安全管理系统软件-安装光盘	是	选配
3	0511G15A	终端物理软件-Secoway TSM&DSM&PSM-AF2DEV01-终端软件新增功能A1-华为-含HS终端安全管理系统软件-软件	是	选配
4	0511G15B	终端物理软件-Secoway TSM&DSM&PSM-AF2DEV02-终端软件新增功能B1-华为-含HS终端安全管理系统软件-软件	是	选配
5	0511G15C	终端物理软件-Secoway TSM&DSM&PSM-AF2DEV03-终端软件新增功能C1-华为-含HS终端安全管理系统软件-软件	是	选配

2.3.3 TSM-业务整机配置说明

项目编码：0223G238

项目描述：组件丨附件-TSM-业务整机配置方案

表8 0223G238配置清单

序号	BOM 编码	项目描述	备注

1	0224G014	计算机终端-TSM&DSM&PSM-AF1TFSVR-数据库配置方案-海外版	选配
2	0224G030	计算机终端-TSM&DSM&PSM-AF1TLSVR-数据库配置方案-国内版	选配
3	0224G037	计算机终端-TSM&DSM&PSM-AF1T1DOCSVR-无数据库服务器配置方案-国内版	选配
4	0224G038	计算机终端-TSM&DSM&PSM-AF1T2DOCSVR-无数据库服务器配置方案-海外版	选配

表9 0223G238配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	0224G014	计算机终端-TSM&DSM&PSM-AF1TFSVR-数据库配置方案-海外版	是	选配
2	0224G030	计算机终端-TSM&DSM&PSM-AF1TLSVR-数据库配置方案-国内版	是	选配
3	0224G037	计算机终端-TSM&DSM&PSM-AF1T1DOCSVR-无数据库服务器配置方案-国内版	是	选配
4	0224G038	计算机终端-TSM&DSM&PSM-AF1T2DOCSVR-无数据库服务器配置方案-海外版	是	选配

2.3.4 License 配置说明

项目编码：80010082

项目描述：Package of license-Secospace Suite-Secospace Suite License

表10 80010082配置清单

序号	BOM 编码	项目描述	备注
1	80020142	Feature-Secospace-SecospaceFE-Secospace Suite	选配
2	8002G045	Feature-Secospace Suite-TSMHSFE1-终端安全管理服务	选配
3	8002G1JR	Feature-Secospace Suite-TSMUPG01-升级功能控制	选配
4	8002G17S	Feature-Secospace Suite-PSMF1-移动存储介质管理服务	选配
5	31070026	Huawei License授权证书-(HW)	选配

表11 80010082配置说明

序号	BOM 编码	项目描述	是否报价	说明

1	31070026	Huawei License授权证书-(HW)	否	当客户报有License的功能项和控制项时配发1PCS

SecospaceFE特性配置说明

项目编码：80020142

项目描述：Feature-Secospace-SecospaceFE-Secospace Suite

表12 80020142配置清单

序号	BOM 编码	项目描述	备注
1	81800045	Function-Secospace-LSS1FSERV01-接入控制服务-含HS 终端安全管理系统软件	选配
2	81800048	Function-Secospace-LSS1FSERV04-安全策略管理服务-含HS 终端安全管理系统软件	选配
3	81800049	Function-Secospace-LSS1FSERV05-资产管理服务-含HS 终端安全管理系统软件	选配
4	81800050	Function-Secospace-LSS1FSERV06-软件分发服务-含HS 终端安全管理系统软件	选配
5	81800051	Function-Secospace-LSS1FSERV07-补丁管理服务-含HS 终端安全管理系统软件	选配
6	81800052	Function-Secospace-LSS1FSERV08-员工行为管理服务-含HS 终端安全管理系统软件	选配
7	82800034	Resource-Secospace-LSS1RTERA01-接入控制服务终端数-1终端-含HS 终端安全管理系统软件	选配
8	8280G002	Resource-Secospace-LAF1RTERA02-安全策略管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
9	8280G003	Resource-Secospace-LAF1RTERA03-资产管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
10	8280G004	Resource-Secospace-LAF1RTERA04-软件分发服务终端数-1终端-含HS 终端安全管理系统软件	选配
11	8280G005	Resource-Secospace-LAF1RTERA05-补丁管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
12	8280G006	Resource-Secospace-LAF1RTERA06-员工行为管理服务终端数-1终端-含HS 终端安全管理系统软件	选配

表13 80020142配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	81800045	Function-Secospace-LSS1FSERV01-接入控制服务-含	是	选配

		HS 终端安全管理系统软件		
2	81800048	Function-Secospace-LSS1FSERV04-安全策略管理服务-含HS 终端安全管理系统软件	是	选配
3	81800049	Function-Secospace-LSS1FSERV05-资产管理服务-含HS 终端安全管理系统软件	是	选配
4	81800050	Function-Secospace-LSS1FSERV06-软件分发服务-含HS 终端安全管理系统软件	是	选配
5	81800051	Function-Secospace-LSS1FSERV07-补丁管理服务-含HS 终端安全管理系统软件	是	选配
6	81800052	Function-Secospace-LSS1FSERV08-员工行为管理服务-含HS 终端安全管理系统软件	是	选配
7	82800034	Resource-Secospace-LSS1RTERA01-接入控制服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
8	8280G002	Resource-Secospace-LAF1RTERA02-安全策略管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
9	8280G003	Resource-Secospace-LAF1RTERA03-资产管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
10	8280G004	Resource-Secospace-LAF1RTERA04-软件分发服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
11	8280G005	Resource-Secospace-LAF1RTERA05-补丁管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
12	8280G006	Resource-Secospace-LAF1RTERA06-员工行为管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配

TSMHSFE1特性配置说明

项目编码：8002G045

项目描述：Feature-Secospace Suite-TSMHSFE1-终端安全管理服务

表14 8002G045配置清单

序号	BOM 编码	项目描述	备注
1	8180G003	Function-TSM-LSS2FSERV01-接入控制服务-含HS 终端安全管理系统软件	选配
2	8180G004	Function-TSM-LSS2FSERV02-安全策略管理服务-含HS 终端安全管理系统软件	选配
3	8180G005	Function-TSM-LSS2FSERV03-资产管理服务-含HS 终端安全管理系统软件	选配
4	8180G006	Function-TSM-LSS2FSERV04-软件分发服务-含HS 终端安全管理系统软件	选配
5	8180G007	Function-TSM-LSS2FSERV05-补丁管理服务-含HS 终端安全管理系统软件	选配

6	8180G008	Function-TSM-LSS2FSERV06-员工行为管理服务-含HS 终端安全管理系统软件	选配
7	8280G010	Resource-TSM-LAF2RTERA01-接入控制服务终端数-1终端-含HS 终端安全管理系统软件	选配
8	8280G011	Resource-TSM-LAF2RTERA02-安全策略管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
9	8280G012	Resource-TSM-LAF2RTERA03-资产管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
10	8280G013	Resource-TSM-LAF2RTERA04-软件分发服务终端数-1终端-含HS 终端安全管理系统软件	选配
11	8280G014	Resource-TSM-LAF2RTERA05-补丁管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
12	8280G015	Resource-TSM-LAF2RTERA06-员工行为管理服务终端数-1终端-含HS 终端安全管理系统软件	选配
13	8280G025	Resource-Secospace-LAF1DEVR01-定制开发-人天	选配
14	8280G027	Resource-Secospace Suite-LAF1DEVR02-Secospace suite通用软件定制开发费-人天	选配

表15 8002G045配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	8180G003	Function-TSM-LSS2FSERV01-接入控制服务-含HS 终端安全管理系统软件	是	选配
2	8180G004	Function-TSM-LSS2FSERV02-安全策略管理服务-含HS 终端安全管理系统软件	是	选配
3	8180G005	Function-TSM-LSS2FSERV03-资产管理服务-含HS 终端安全管理系统软件	是	选配
4	8180G006	Function-TSM-LSS2FSERV04-软件分发服务-含HS 终端安全管理系统软件	是	选配
5	8180G007	Function-TSM-LSS2FSERV05-补丁管理服务-含HS 终端安全管理系统软件	是	选配
6	8180G008	Function-TSM-LSS2FSERV06-员工行为管理服务-含HS 终端安全管理系统软件	是	选配
7	8280G010	Resource-TSM-LAF2RTERA01-接入控制服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
8	8280G011	Resource-TSM-LAF2RTERA02-安全策略管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
9	8280G012	Resource-TSM-LAF2RTERA03-资产管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
10	8280G013	Resource-TSM-LAF2RTERA04-软件分发服务终端数	是	选配

		-1终端-含HS 终端安全管理系统软件		
11	8280G014	Resource-TSM-LAF2RTERA05-补丁管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
12	8280G015	Resource-TSM-LAF2RTERA06-员工行为管理服务终端数-1终端-含HS 终端安全管理系统软件	是	选配
13	8280G025	Resource-Secospace-LAF1DEVR01-定制开发-人天	是	选配
14	8280G027	Resource-Secospace Suite-LAF1DEVR02-Secospace suite通用软件定制开发费-人天	是	选配

TSMUPG01特性配置说明

项目编码：8002G1JR

项目描述：Feature-Secospace Suite-TSMUPG01-升级功能控制

表16 8002G1JR配置清单

序号	BOM 编码	项目描述	备注
1	8280G029	Resource-TSM-LAF2PLCUP01-策略升级服务(1年)-含HS 终端安全管理系统软件	选配
2	8280G02A	Resource-TSM-LAF2RPTUP01-报表升级服务(1年)-含HS 终端安全管理系统软件	选配

表17 8002G1JR配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	8280G029	Resource-TSM-LAF2PLCUP01-策略升级服务(1年)-含HS 终端安全管理系统软件	是	选配
2	8280G02A	Resource-TSM-LAF2RPTUP01-报表升级服务(1年)-含HS 终端安全管理系统软件	是	选配

PSMF1特性配置说明

项目编码：8002G17S

项目描述：Feature-Secospace Suite-PSMF1-移动存储介质管理服务

表18 8002G17S配置清单

序号	BOM 编码	项目描述	备注
1	8180G009	Function-Secospace Suite-LAF2PSMF01-移动存储介质管理服务-含HS Secospace 终端安全管理系统软件	选配
2	8280G016	Resource-Secospace Suite-LAF2PSMR01-移动存储介质管理用户数	选配

		-1用户-含HS Secospace 终端安全管理系统软件	
3	8280G028	Resource-PSM-LAF2PSMR02-移动存储介质管理终端数-TSM配套销售专用-1终端-含HS 终端安全管理系统软件	选配

表19 8002G17S配置说明

序号	BOM 编码	项目描述	是否报价	说明
1	8180G009	Function-Secospace Suite-LAF2PSMF01-移动存储介质管理服务-含HS Secospace 终端安全管理系统软件	是	选配
2	8280G016	Resource-Secospace Suite-LAF2PSMR01-移动存储介质管理用户数-1用户-含HS Secospace 终端安全管理系统软件	是	选配
3	8280G028	Resource-PSM-LAF2PSMR02-移动存储介质管理终端数-TSM配套销售专用-1终端-含HS 终端安全管理系统软件	是	选配

2.3.5 外部成套电缆配置说明

项目编码：04000407

项目描述：外部成套电缆-世界各国交流电源线-I类设备用带C13连接器-HS

外部电缆仅用于海外局点用，国内使用时无需配置外部电缆，需配置数量：

每台0224G038 计算机终端-TSM&DSM&PSM-AF1T2DOCSVR-无数据库服务器配置方案-海外版

配2PCS

每台0224G014 计算机终端-TSM&DSM&PSM-AF1TFSVR-数据库配置方案-海外版

配2PCS

每台06040109 KVM设备-KVM四合一-1U高-17" TFT LCD-8路KVM接口-鼠标键盘-八根USB直头线缆/带机架安装配件-英文资料-100~240V AC-黑色

配1PCS

3 资料配置

TSM系统的配套资料随安装光盘提供，不单独配套发货。

资料包括：

- TSM 安装指南
- TSM 操作指南
- TSM Installation Guide
- TSM Operation Guide

中文资料仅限国内发布，英文资料仅限海外发布。

4 部分配件说明

4.1 市场建议

如果选购

50030084 调制解调器-无线GPRS-48Kbps-无线接口-外置式-100~240VAC转DC12V电源适配器-适配器插头规格:5.5x2.1mm-中英文资料-RS232标准串型接口

当海外局点选配该GSM Modem时，需要在当地采购电源适配器。

4.2 用户自备硬件说明

所有硬件(SACG、服务器、联网设备等)原则上应由华为公司提供。若用户一定要自备，则应对用户提出设备的型号及配置要求，当用户要求在建议范围之外时，尽快与安全产品管理部联系，以免出现安全产品管理部还没有实现方案就向局方轻易承诺，或者是把高价的设备按照低价报给局方的情况。

4.3 合同预审要求

a）局方技术要求或技术规范书

b）技术方案

c）详细组网图

d）技术协议书

e）配置清单

5 扩容和升级改造方法与配置说明

5.1 扩容方法与配置说明

5.1.1 扩容的方法与原则

5.1.2 扩容设备的清单

见2.2.1和2.2.4。

5.1.3 可扩容部分的说明

TSM系统在扩容方面包括2个方面：

（1）用户规模增大。

在这种情况下，首先考虑扩容后的用户规模的License是否超过用户所购买的License，如果还在所购买的License范围之内，则无需在购买License；如果超过所购买的License，则需要再增加购买License。

例如：某个地区的网络规模为400个License，用户购买了500个TSM License。

如果网络扩容，扩容后的网络规模为500个License以内，则无需再购买License。如果扩容后的网络规模超过500个License（比如为600个License），则用户还需要购买100个License或更多（为了以后的再扩容）。

如果需要新增License，可能需要购买如下内容：

如果新增用户超过当前硬件的处理能力，需要购买新的服务器和存储设备；具体服务器购买的数量，参见配置原则。

（2）网络规模增大，需要部署新的SACG设备。

这种情况下需要根据SACG设备的处理能力，购买新的SACG，并根据相应增加的用户数购买更多的License。

5.1.4 扩容所涉及的机柜、母板插框、单板等的配置原则

纯软件产品，不涉及。

5.1.5 扩容中需特别注意的问题

无。