



CNSEC Netwrok

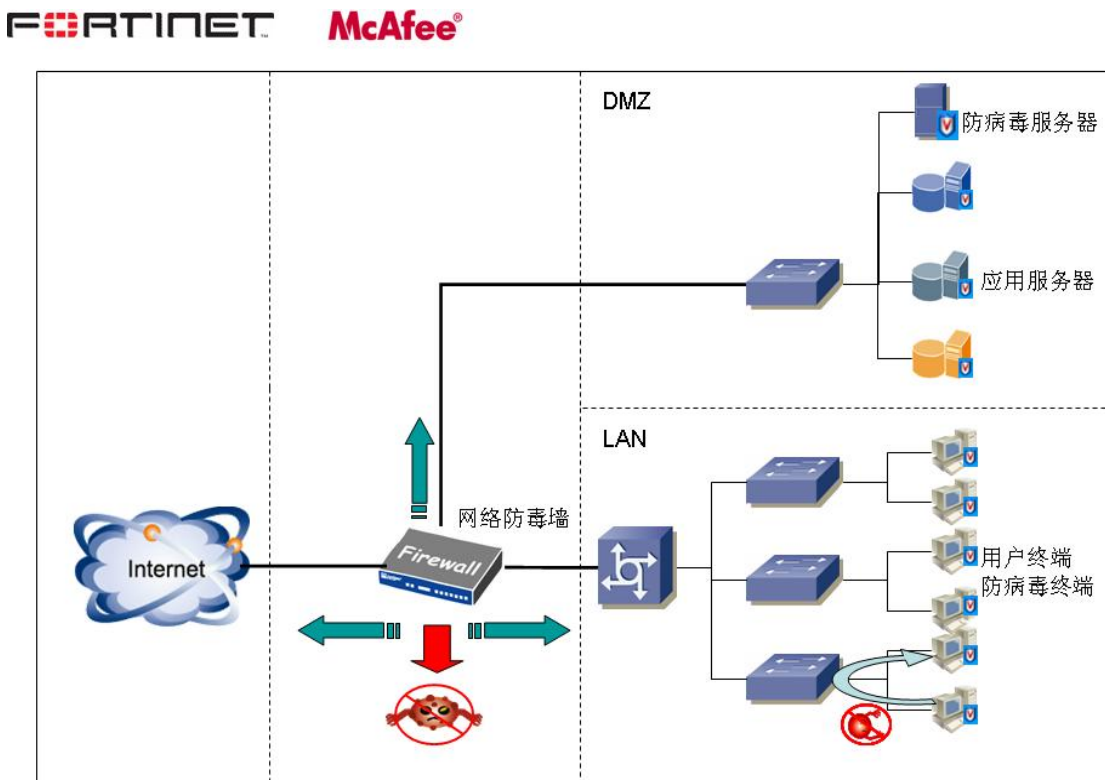
通用解决方案汇编

1、问题：网络中总有病毒杀不干净怎么办？

现有情况描述

某企业网络中有大量病毒、间谍软件、木马程序、流氓软件...等有害程序传播，导致用户计算机运行速度缓慢，影响网络中员工的正常工作。在用户没有任何防护措施下窃取或破坏员工计算机上的重要数据。

实施后网络拓扑结构



解决方案描述

病毒一般是由于用户手动或自动运行了感染病毒的文件，病毒最重要的是要做到防范，针对企业目前存在的问题，并结合病毒的传播途径，我们采用网关防毒墙+网络版杀毒软件解决方案。

1) 在网络接入处部署 Fortinet 防毒墙（自动更新病毒库），当企业员工访问网页或接收邮件过程中，网关防毒墙将会过滤进出网络数据流，如果发现数据中包含病毒将在网关处直接查杀，拦截来自外网的病毒，使病毒无法传播到用户端。

2) 在企业内部安装 McAfee 网络版杀毒软件，查杀企业内部计算机感染的病毒，同时还可以查杀通过优盘拷贝或其它途径传播到客户端的病毒。

总结

网关防病毒与网络版防病毒相结合，防毒墙经过过滤后，网络版杀毒软件主要针对内网传播的病毒进行查杀，保证了企业用户计算机免受病毒威胁。同时，McAfee 网络版杀毒软件具有对客户端计算机进行统计、自定义防护策略及策略分发、统一病毒库更新等优势，方便网络管理员管理企业内部计算机，查看内部计算机杀毒软件的安装及执行情况，使管理员对网络安全现状有了全面的管理及监控能力。

2、问题：如何对桌面终端进行安全有效的管理？

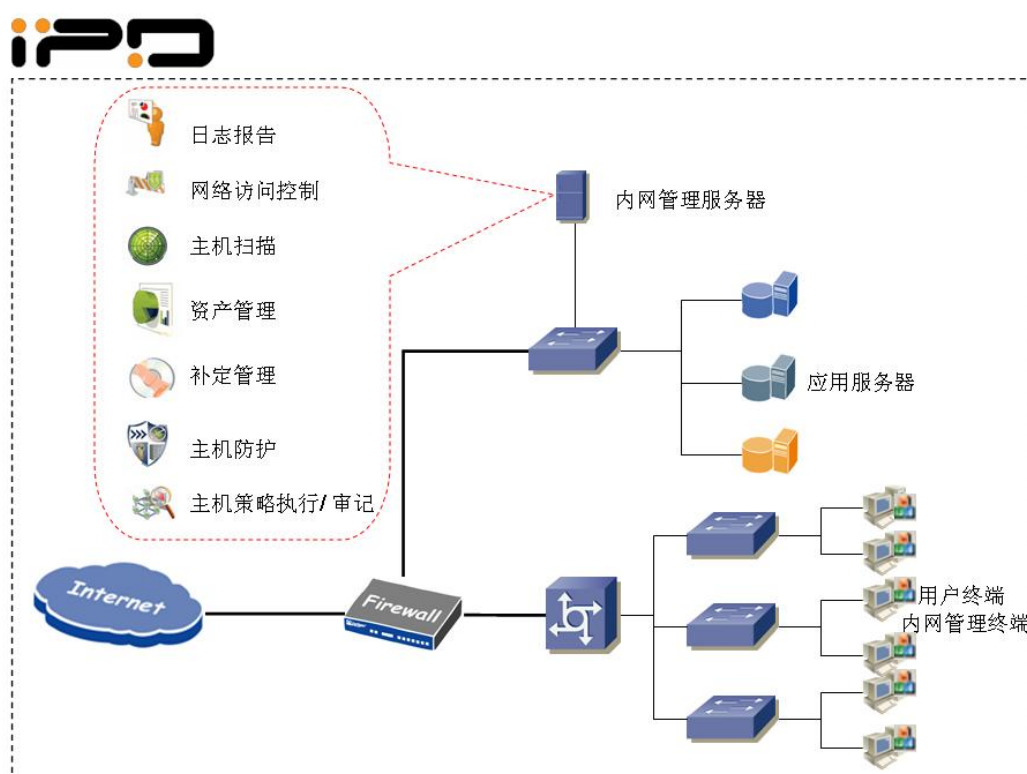
问题：想对单位的每台电脑进行统一管理，补丁分发，有什么有效的方法？

现有情况描述

某企业 IT 管理人员反映，计算机不断更新，数量不断增多，人员流动大，很难完成统计计算机配置情况、软件安装情况、操作系统的使用情况、补丁安装情况。

内部计算机还经常由于没有及时安装操作系统漏洞补丁，导致由于操作系统漏洞而感染计算机病毒，从而影响网络中其它计算机。我们都清楚，反病毒厂商只能做到事后的救急和处理，而不能从源头上解决问题，无法防范由于系统漏洞造成的网络攻击或病毒攻击，“冲击波”、“熊猫烧香”等蠕虫病毒让企业网管及计算机使用者得到深刻“教训”。解决由于操作系统漏洞引发的安全问题，统一管理和自动分发补丁程序逐渐被计算机使用者重视。

实施后网络拓扑结构



解决方案描述

针对目前大部分企业面临的问题，我们将提出内网管理及补丁分发解决方案，在一台服务器上安装 IPD 服务器端，可以设置服务器端自动或手动安装 IPD 客户端程序到用户计算机，这样就可以对企业内部计算机的硬件资源、软件安装情况及计算机运行的进程管理等，并可以实现由 IPD 服务器自动下发操作系统最新补丁程序到客户端，及时安装系统最新的补丁。网络管理员还可以通过登陆管理 IPD 服务器实现对网络中所有计算机的统一管理，提高了 IT 管理的工作效率。

总结

IPD 系统管理套件，是针对局域网 PC 集中运维管理的全面解决方案，其核心目标是提供高效率的管理手段和措施，协助 IT 主管应对日益增长的 PC 运营维护和安全管理需求。

IPD 内网管理系统采用模块化的产品架构，用户可以按照实际管理需求，灵活组合运用不同模块，有针对性地部署和实施。IPD 内网管理系统包括 PC 资产管理、应用程序进程管

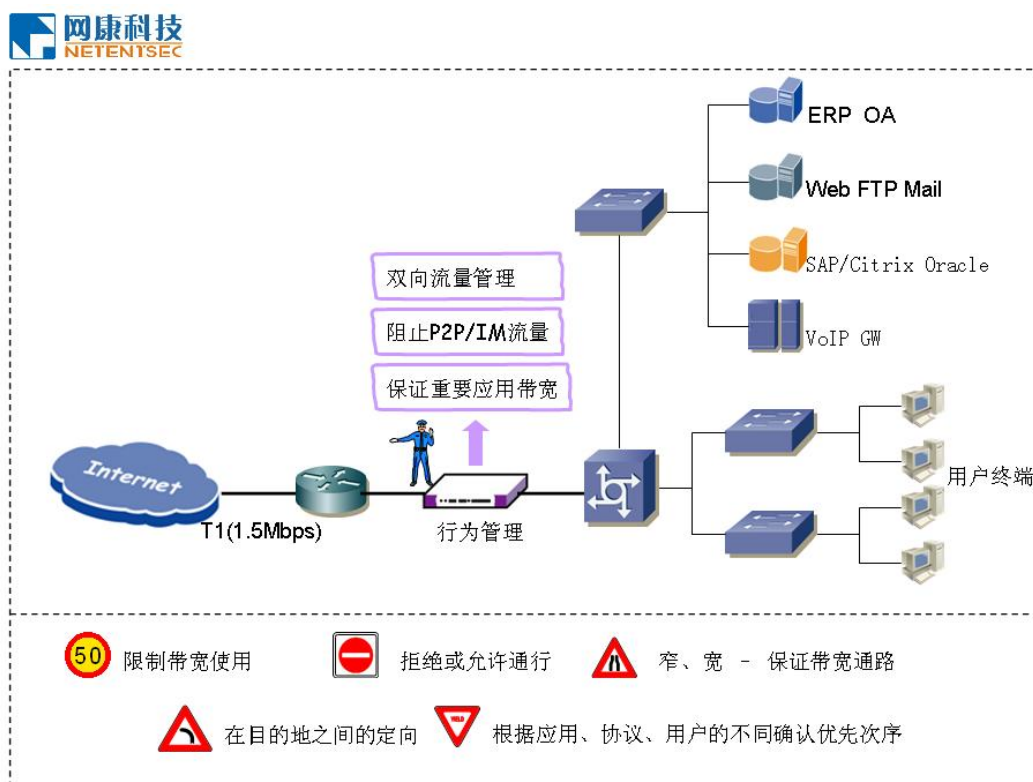
理、补丁与分发、网络访问管理、接入安全控制、远程桌面管理、外设管理、桌面设置、系统预警、互联网访问日志、文件访问日志等管理模块。IPD 内网管理系统将全方面的解决企业内部计算机的管理问题。

3、问题：要阻止员工在上班时间使用 QQ,MSN,BT 等工具，应如何实现？

现有情况描述

某企业管理人员反映员工经常在上班时间使用 QQ、MSN 等聊天工具，某些员工还使用 BT 等工具下载电影，严重浪费公司宝贵的带宽资源，降低公司整体工作效率，同时 IM 实时聊天工具还会增加病毒的感染机率，如何在上班时间阻止员工使用与工作无关的软件成为企业关注的紧迫问题。

实施后网络拓扑结构



解决方案描述

在路由器与交换机之间部署网康上网行为管理设备，可以对员工上网行为进行访问控制，当发现员工使用 QQ、MSN 或 BT 等与工作无关的软件时，自动阻止相关软件网络流量，保证了网络带宽的合理使用，提高企业的整体工作效率。并且网康产品支持网页过滤功能，包含色情、反动、娱乐、新闻、体育、病毒、黑客等分类库，可以对员工访问的网站类别进行分时段控制。

总结

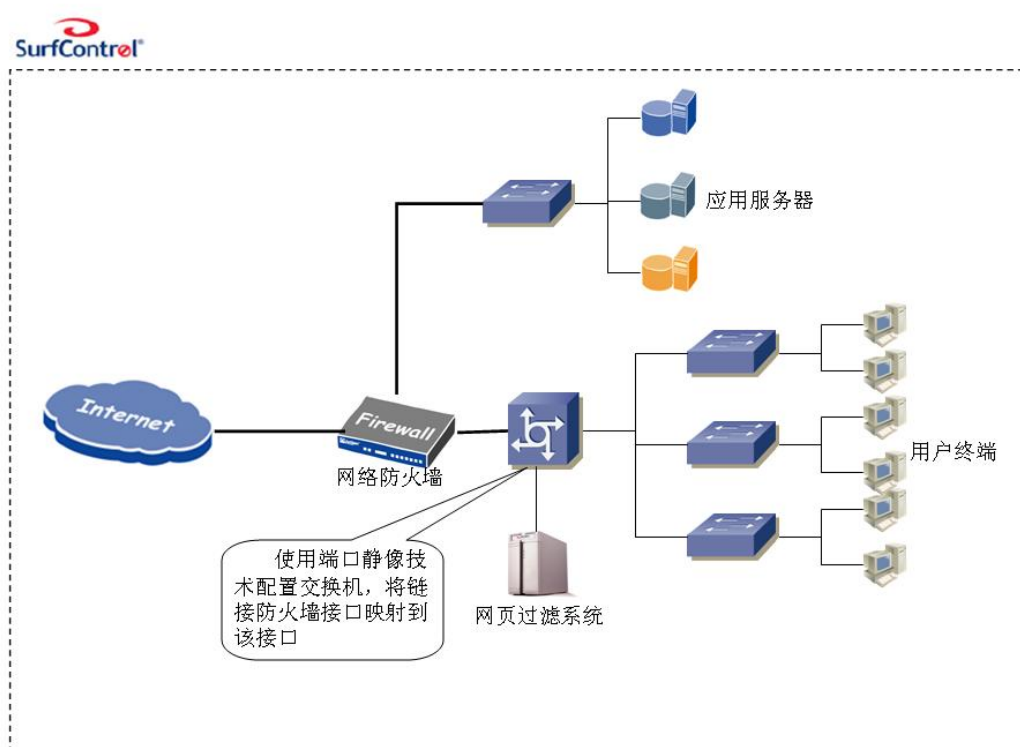
网康上网行为管理系统通过制定细粒度的访问策略，实现对互联网使用者的上网行为、访问内容、外发信息、带宽流量等进行有效的控制和管理，从控制和管理角度帮助企业制定并落实互联网使用规定，防止访问高风险、非法和不健康的互联网内容，防止外发信息泄密，从而帮助企业用户提高工作生产效率、提高设备和网络带宽的利用率、避免法律纠纷，为企业建立了更加安全、更加完善的网络环境。

4、怎样限制员工在上班时间访问与工作无关，甚至色情，反动的网站？

现有情况描述

某企业网管反映公司员工在上班时间访问与公司业务无关的网站，例如：新闻、体育、娱乐等网站，甚至还有和色情、反动有关。不仅浪费了公司的宝贵的带宽资源，而且也给公司带来了许多风险，因为色情的网站会经常带有一些病毒、木马、间谍软件，从而给公司内网带来一定隐患。虽然公司也拟定了一些相关规定，但是这种情况仍然是屡禁不止。

实施后网络拓扑结构



解决方案描述

根据用户需求我们采用了 Surfcontrol Web Filter 网页过滤系统，此系统提供了一套完整的网页过滤机制，可以根据企业自身的业务需求及互连网使用情况灵活的定制过滤机制。同时强大的报告与分析工具能让网络管理人员详细了解网络中网站访问情况及网络中带宽使用情况。而且 Web Filter 系统可以分时段配置不同的访问规则，如在工作时段不允许访问体育、娱乐类网站，而下班和午餐时间允许访问。

总结

Surfcontrol WebFilter 目录是行业内规模最大且最精确的内容数据库，收集了超过 1700 万条网址及 30 亿个网页，200 个国家的 70 种语言，它可以每日按计划自动更新。而且它可以配置在任何的网络环境中，无论是在防火墙，代理服务器，还是在使用特殊的网络设备平台都可以兼容使用，这意味着您可以对管理好互联网的使用充满信心。

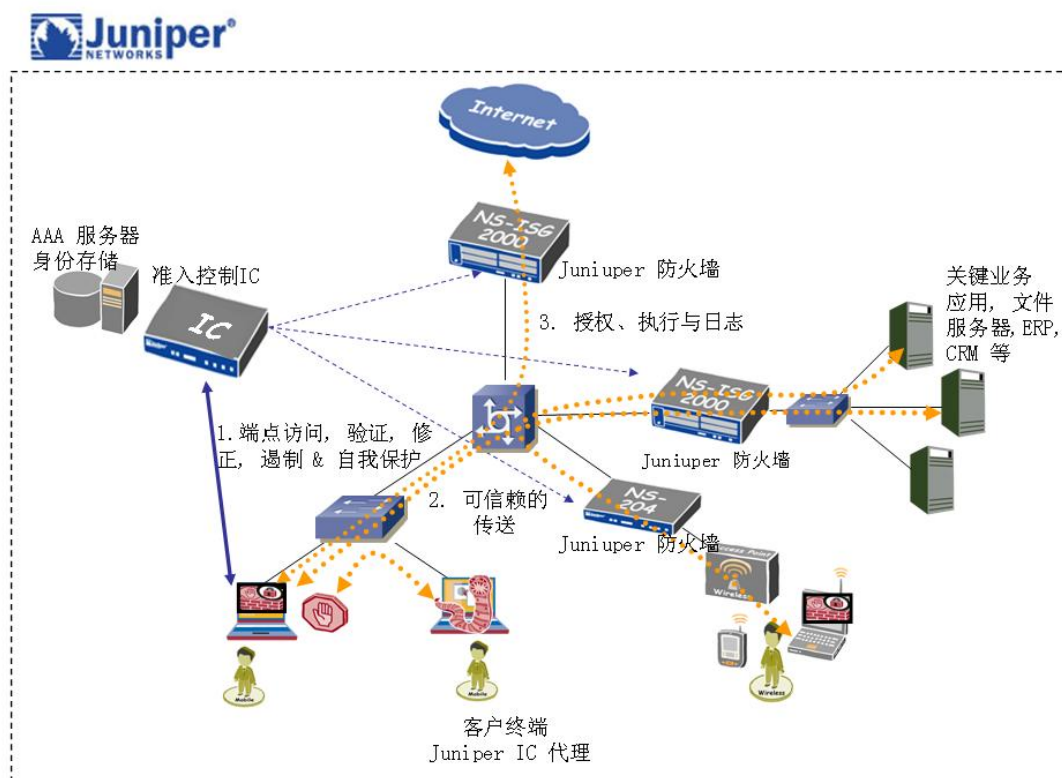
5、问题：怎样才能对企业内部关键应用服务器进行细粒度访问控制？

问题：怎样防止没有打补丁或未升级病毒库的机器进入内网？

现有情况描述

企业网络必须为更为多样化的用户（如访客、承包商和移动员工）提供接入服务，他们中的某些人会使用自己的设备接入网络。用户可能在无意中下载一些受感染的文件，并使用这些受感染的设备直接连接到您的网络。或者他们只是从您的局域网中接入互联网而得不到适当的安全保护，从而将您的网络暴露于大量威胁之中。

实施后网络拓扑结构



解决方案描述

在内网核心交换机上部署 Juniper IC 统一接入控制设备，对内部非法接入的用户进行验证，检测计算机是否安装杀毒软件、病毒库是否是升级为新版本，可根据检测的内容决定是否限制用户访问互联网或访问公司内部服务器资源，防止企业重要资源泄漏，保证了网络的安全性。

总结

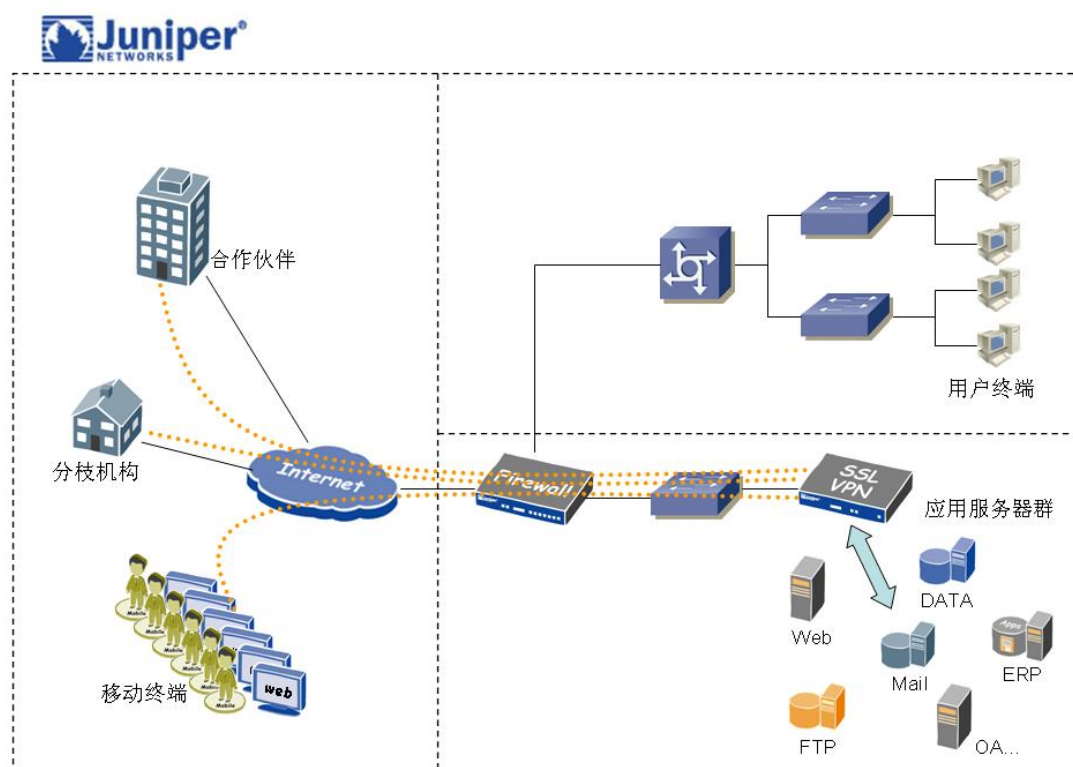
Juniper IC 能够与 Juniper 防火墙及支持 802.1X 标准的网络设备联动，可以向 Juniper 防火墙或支持 802.1X 网络设备（如交换机）下发命令，从而对非法用户访问 Internet 及内网服务器等重要资源进行策略控制，减少了企业面临的威胁。

6、大量分散的远程接入用户通过互联网连接企业内部重要应用服务器资源，如何提供数据传输的安全性以及访问权限控制细粒度？

现有情况描述

某企业在外移动办公人员较多，每天都要通过互联网访问公司总部资源,例如上传，下载资料，可是方便快捷的同时也给公司带来了一定的隐患。比如上传文件时把带有病毒的资料传到了公司的服务器，导致服务器瘫痪。同时对访问者的权限也无法精确控制，如果这个用户可以访问到服务器，那么他将在这台服务器的所有开放端口都具有访问权限，从而也带来了诸多安全问题。

实施后网络拓扑结构



解决方案描述

根据用户需求，针对该企业移动办公用户较多的特点，我们采用 JuniperSSL VPN 系列产品，SSL VPN 使用标准的 Web 浏览器。使用 SSL 技术，使客户无需部署客户端软件、无需更改内部网络配置，也无需提供长期维护服务。通过 SSL VPN 细粒度的访问控制，及审计和日志记录功能，可以对不同用户进行具体的访问权限设置，可以根据用户组或角色、网络、设备及会话属性来规定基于用户身份的接入，从而对外网用户做到安全、精细的访问控制。

总结

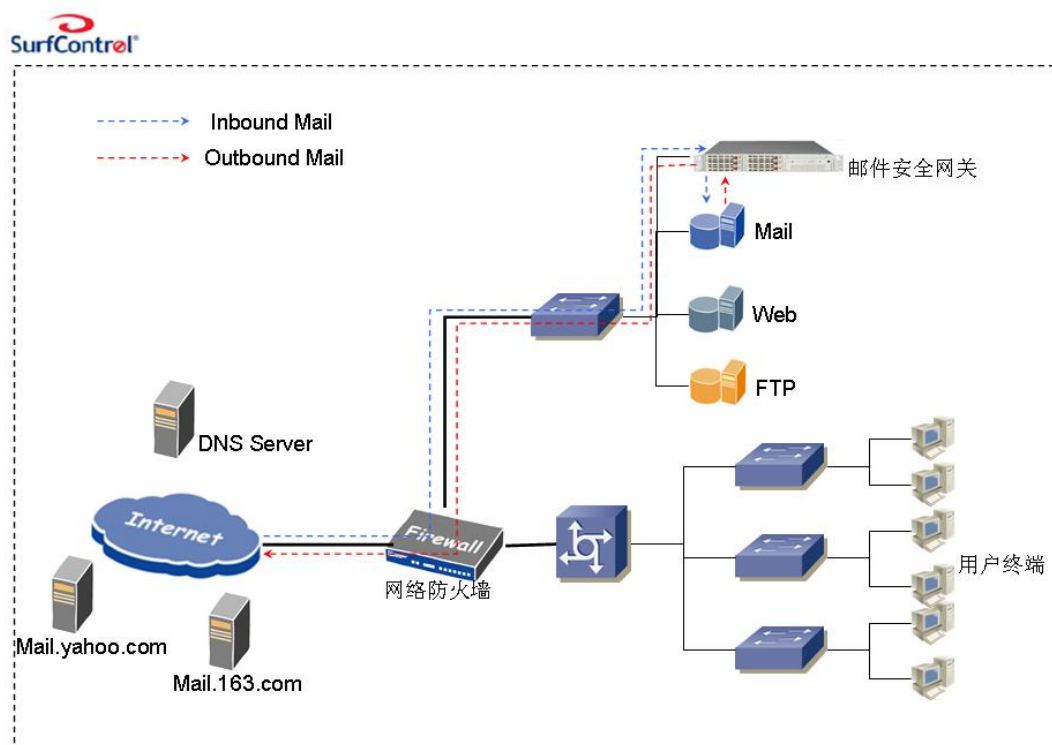
Juniper 的 Secure Access 产品拥有各种机型和特性，可以满足各种企业所需的远程/移动员工的接入访问，与传统的 IPSec 客户端解决方案相比，SSL VPN 安全接入产品可提供更低的总成本和独特的端到端安全特性。增强的接入方式使企业可以根据需要，安心的提供适当的访问权限。如果环境需要，软件许可还能提供各种数据进行压缩的功能，以及 SSL 加速。

7、大量垃圾、病毒邮件充斥着企业邮箱，如何最大程度提高企业员工的工作效率？

现有情况描述

据某企业网管反映公司的内部邮件服务器每天都有大量垃圾邮件，每天早上员工上班收取邮件时可能会有上百封邮件，而垃圾邮件却占到了 80%-90%，员工则需要手动进行查找出有用的邮件，然后删除垃圾邮件。为了避免误删正确邮件需要每封邮件都进行排查，从而浪费了大量的时间。

实施后网络拓扑结构



解决方案描述

由于该企业垃圾邮件繁多，我们采用了 Surfcontrol 的 Riskfilter 产品，强大的 ASA 垃圾邮件数字指纹数据库识别垃圾邮件的准确率最高可达 99.2%，基于行为识别和内容分析的垃圾邮件过滤技术极大的降低了误报率。垃圾、病毒库全球自动更新，实施后基本不需要人工管理，可以根据实际需求，定制用户发件人邮件地址黑名单和白名单。而且系统每天自动产生垃圾邮件摘要信息，用户可以直接处理垃圾邮件，彻底解决了误报的问题。

总结

Surfcontrol RiskFilter 邮件网关操作简单，在内容判断方面具有强大的推理技术，多层面的防垃圾邮件体系及防病毒技术，可根据内容词典预先定义关键字词典，支持多种格式文件的过滤，避免恶意文件占用您的网络带宽，RiskFilter 提供完善的防攻击体系，有效地防范针对邮件系统地各类攻击，例如：字典算法攻击，目录攻击，多线程攻击等等。同时结合大量的统计与分析报告，旨在电子邮件过滤需求上，带给您最完善的解决方案。

8、怎样提高 Intranet 内部南北互通访问速度？

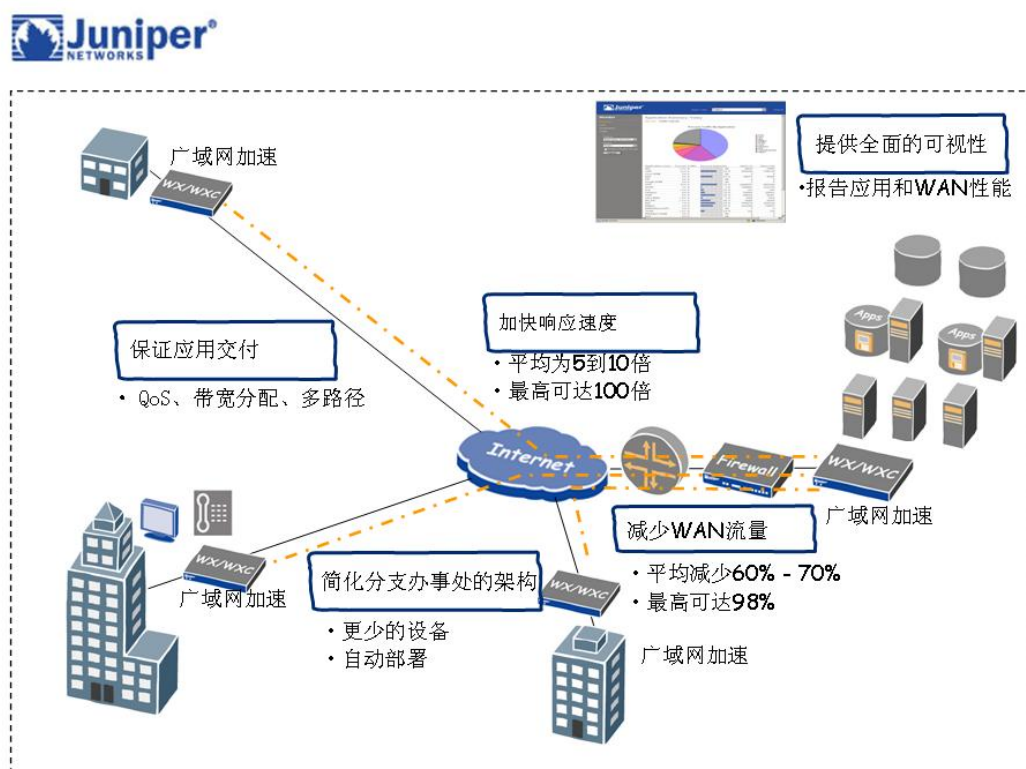
现有状况描述

根据某企业现状分析，总部与分部存在大量数据交互，网络接入分别为电信、网通，由于我国南北互连一直存在如下问题：

- 广域网传输延迟较大，严重影响了应用的响应时间
- 带宽紧张，而带宽资源费用较高

上述问题严重影响着企业内部应用访问速度，如何提高分布式企业数据交互效率已经成为高级 IT 管理人员迫在眉睫的问题。

实施后网络拓扑结构



解决方案描述

根据客户需求我们选用 Juniper WX 系列产品来解决南北访问速度问题。WX 应用加速平台为分布式企业提供经济高效的方法，通过分子序列压缩技术实现压缩，用于加速 WAN 上数据流，提高生产访问效率。WX 平台基于独特的 WX Framework，可帮助企业提高应用响应速度、优化 WAN 投资、控制主要应用并为它们分配优先级，QoS 引擎紧密集成到压缩和序列缓存技术中，允许 QoS 策略即刻检测出有效 WAN 规模的变化，并据此对资源分配优先级进行相应调整，从而保证企业重要数据的传输。

总结

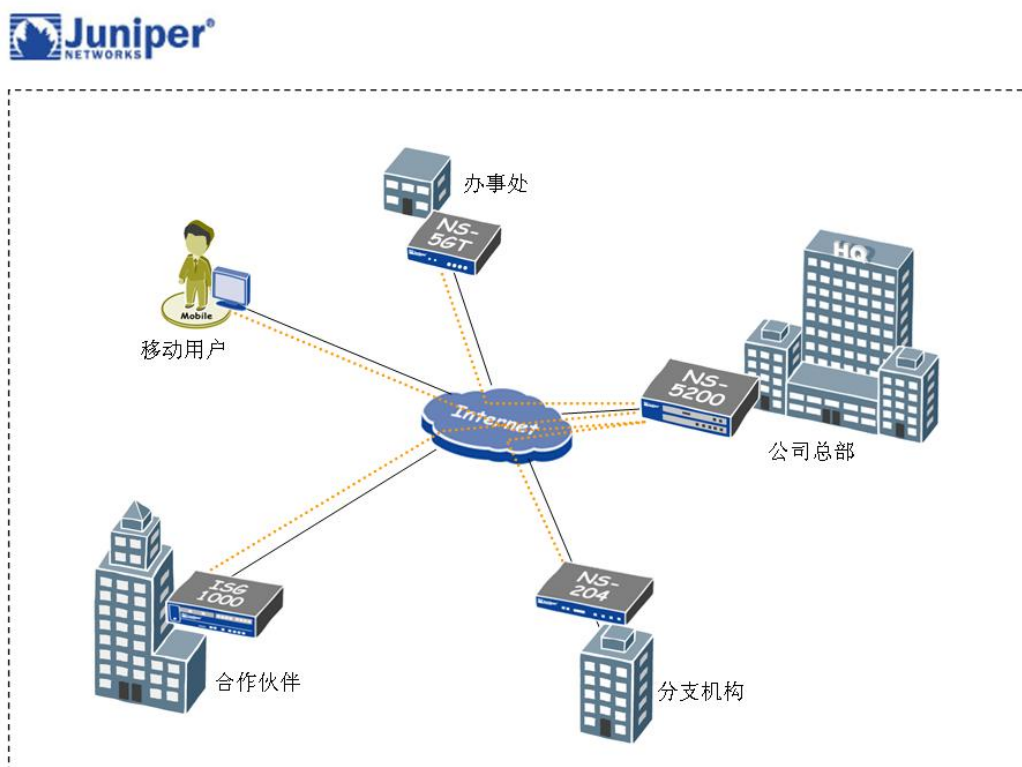
Juniper WX 用户管理界面友好，可通过基于 web 的安全向导，在 10 分钟内完成部署与配置。经济高效的解决方案，用于加速 WAN 上的应用，帮助企业缩短应用响应时间，优化 WAN 数据传输，求在降低成本的同时增加网络流量。通过 WX 平台，您可加速应用并整合服务器，使 IT 部门和用户都达成满意。

9、有多家分支机构分布在全国各地，如何连接更经济，安全？

现有情况描述

某企业在全国各地分布大量的办事处，办事处与总部之间每天都有数据访问与交互。出于安全考虑，该企业准备在分之机构与总部之间搭建 VPN 进行数据传输，并且在保证安全的同时也想节约成本。

实施后网络拓扑结构



解决方案描述

根据该企业目前状况，我们采用了 Juniper 系列防火墙搭建 IPsec VPN。总部作为中心点采用高端的型号，分部则采用低端与总部进行互连。Juniper IPsec VPN 采用 DES、3DES 和 AES 加密，自动或手动的 IKE 密钥交互手段保证传输数据的安全性。该设备并可以控制 IPsec 的数据访问，及带宽保证，限制未授权用户接入与攻击、简化 VPN 管理。

总结

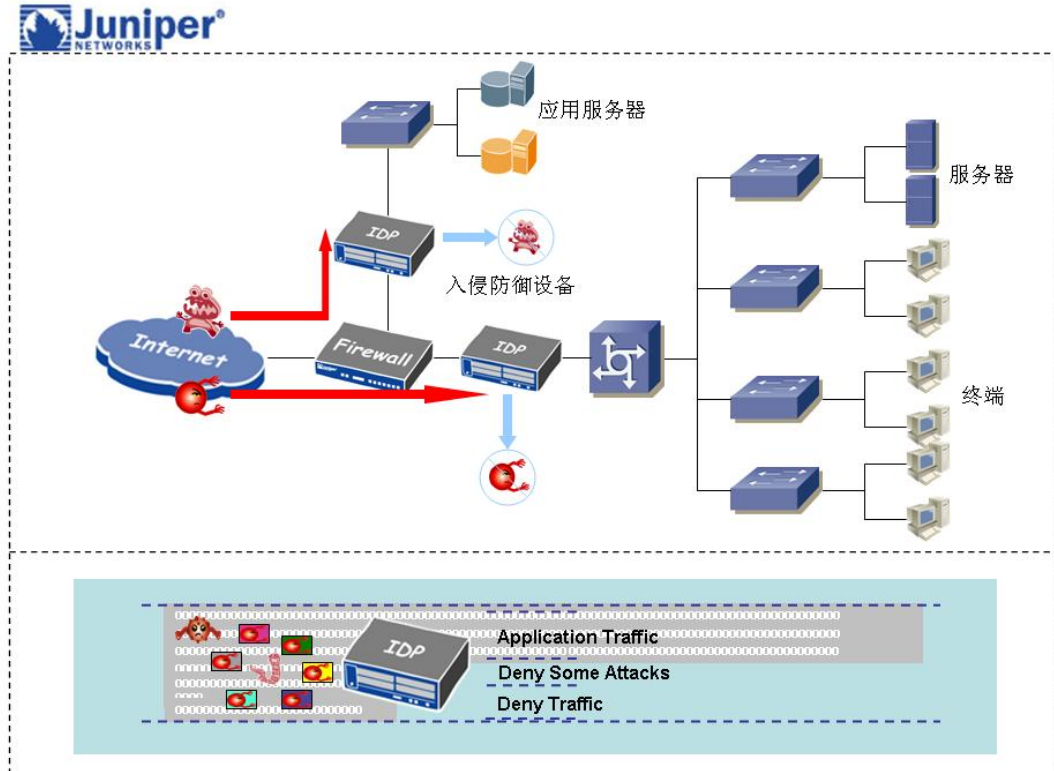
Juniper 些列产品同时支持网状式(mesh)及集中星型(hub and spoke)的VPN网络，可按 VPN 部署的需求，配置用其一或整合两种网络拓扑。支持 VPN 冗余，可以实施基于策略的 VPN 和基于路由的 VPN。同时提供一组统一威胁管理 (UTM) 安全特性，包括状态防火墙、IPS、防病毒、防垃圾邮件和 Web 过滤等，Juniper 集成防火墙/IPsec VPN 安全产品是专用安全解决方案，保护网络免遭攻击，同时最大限度地提高性能，为安全可靠的联网奠定坚实基础，是保护网络安全的理想选择。

10、问题：如何保护企业内部网络及资源免受外部黑客攻击及窃取？

现有情况描述

某企业网络中心人员反映，网络中正面临多种攻击，前端防火墙针对外界的服务做了严格的限制，但是黑客还是通过一些攻击手段窃取了服务器上的重要资源，大量的应用层攻击使服务器无法提供的正常访问服务，网关防火墙无法针对所有攻击行为进行拦截处理。

实施后网络拓扑结构



解决方案描述

传统的防火墙只能防御或处理来自 2—4 层攻击，但目前网络中已经不仅仅是来自 2—4 层的攻击行为，更多的来自应用层的攻击行为，通过针对应用程序的漏洞，以及防火墙开放的正常的服务端口对服务器进行攻击。我们通过部署 Juniper 集成安全网关（ISG）添加入侵检测与防护功能（IDP）模块或 Juniper 入侵检测与防护功能（IDP）设备，检测来自应用层的攻击行为，从而弥补了由于操作系统或应用程序漏洞导致服务器被黑客攻击。

总结

Juniper ISG 系列可通过添加安全模块来支持集成入侵检测与防护功能（IDP），从而针对现有和新型威胁提供强劲的网络层和应用层防护功能。ISG 系列利用与 Juniper 网络公司 IDP 平台相同的软件，但将其集成到了 ScreenOS 中，在单一解决方案中提供最佳防火墙、VPN 和 IDP 的组合。此外，产品还通过名为安全模块的专用处理模块提供专用处理能力，以确保数千兆位的防火墙、VPN 和 IDP 性能。通过无与伦比的安全处理能力以及网络分段特性，ISG 系列产品可部署用于保护网络周边设备或内部网络安全性。

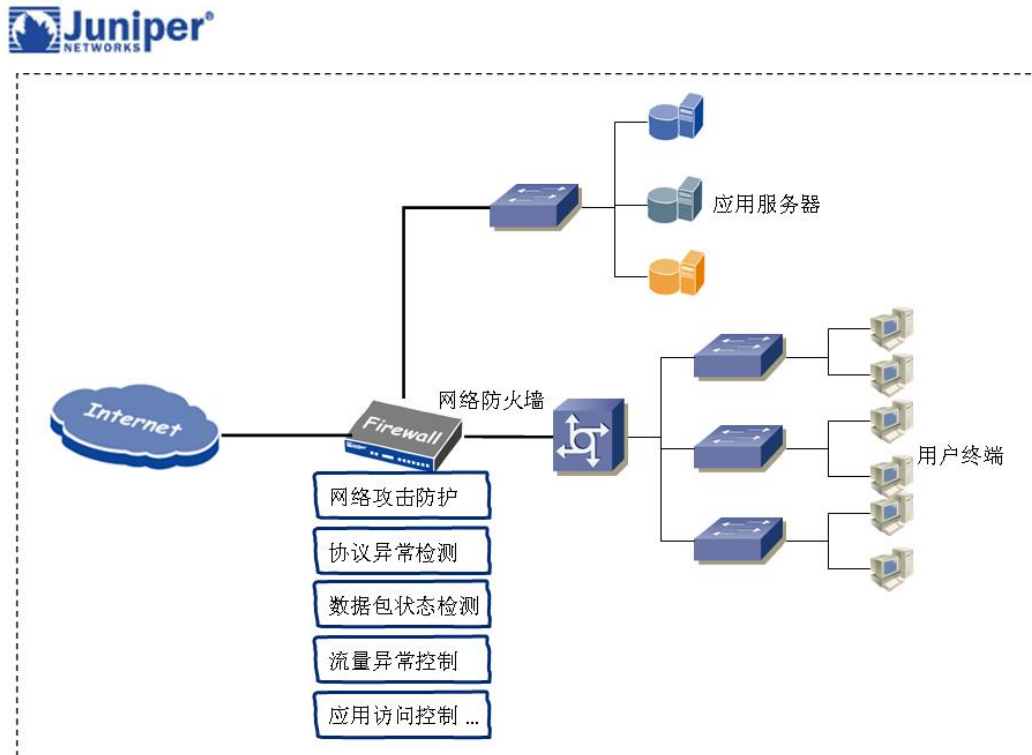
Juniper IDP 使用业界公认的状态检测与防护技术，能够提供 Zero-Day 防护，以抵御针对蠕虫、特洛伊木马、间谍软件、键盘记录和其他恶意软件，防止它们穿过网络或通过已被感染的用户扩散到其他用户。Juniper 网络公司 IDP 不仅帮助抵御网络攻击，还能提供关于擅自添加到网络中的流氓服务器和应用的信息。

11、企业网络上 Internet 前最基本的安全防护措施是什么？

现有情况描述

某企业网管反映他们公司内部服务器经常遭受到黑客攻击，导致数据丢失甚至服务器瘫痪。偶尔网络访问速度特别慢，怀疑是黑客在对企业进行 DOS 拒绝服务攻击，互联网的种种威胁时刻会影响企业正常办公。

实施后网络拓扑结构



解决方案描述

公网上每时每刻都充满了大量的威胁与攻击，针对该公司目前情况，我们采用了 Juniper SSG 系列防火墙，内网用户与服务器分离开，服务器单独放在 DMZ 区。SSG 系列是新型的专用安全设备，将高性能、安全性和局域网/广域网连接性完美地结合起来。产品提供一套全面的统一威胁管理（UTM）安全特性，包括状态防火墙、IPSec VPN、DI、防病毒（包括防间谍软件、防广告软件、防网页仿冒）、防垃圾邮件和 Web 过滤等，可防止出入企业的流量免遭蠕虫、间谍软件、特洛伊木马和恶意软件等攻击。从而安全有效的保护了内部网络以及内部的服务器。

总结

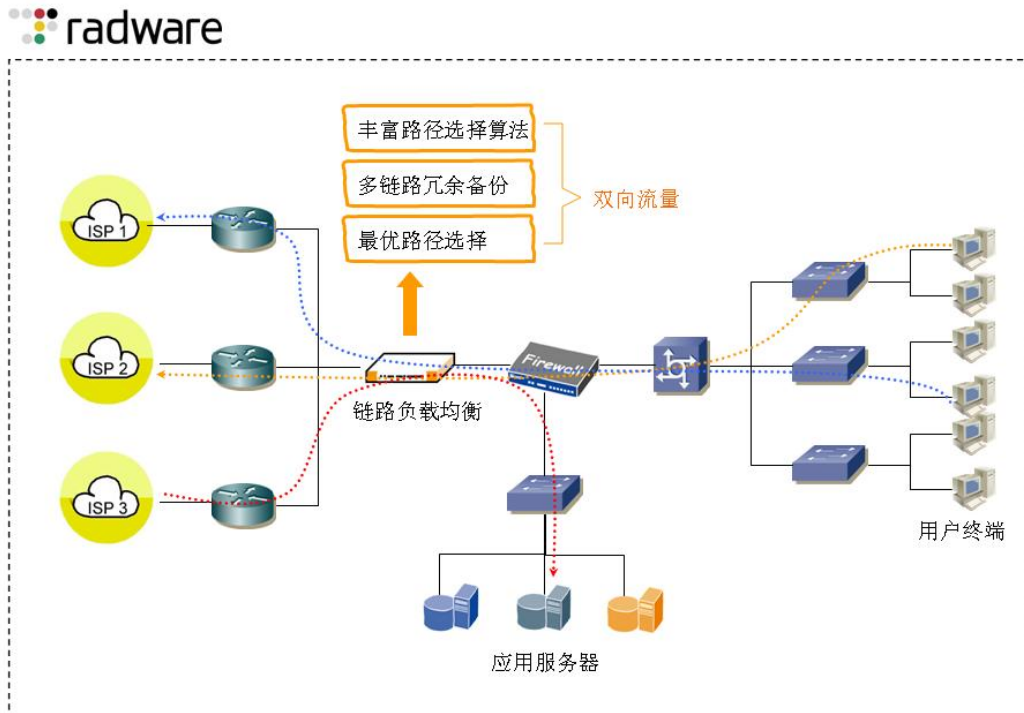
Juniper SSG 系列防火墙将安全和局域网/广域网路由功能组合在一起，可以提供合并设备并降低 IT 成本的能力，全面的局域网和广域网接口，支持串行、T1/E1、DS3 等广域网接口，并且通过图形 Web UI、CLI 或 NetScreen-Security Manager 可集中对系统进行管理，如果您希望拥有一个平台，即能保证内网安全，又要稳定可靠，那么，SSG 系列是您理想的选择。

12、问题：如何保证多链路带宽合理使用并实现最优链路选择？

现有情况描述

某企业为了提高用户访问 Internet 速度，以及广域网用户访问本部服务器速度，申请多条专线接入，但是用户访问的整体速度并没有得到预期的提升，如何加快用户的访问速度，合理使用多条专线带宽，将用户的请求定向到最优的链路，并实现多链路的冗余备份。

实施后网络拓扑结构



解决方案描述

针对用户多链路问题，我们采用 Radware 链路负载设备，Radware 可以实现链路冗余、链路负载选择及最优链路选择。当企业用户访问互联网时，通过 Radware 强大的算法会判断访问的目的地通过哪条链路最优，迅速做出路径选择。

总结

Radware LinkProof 的专利技术：就近性，能够根据用户访问的目的 IP、各条链路的负载等情况来综合考虑，计算出内部用户访问 Internet 的最佳路径，以保证用户能够得到最快和最高效的服务和响应。

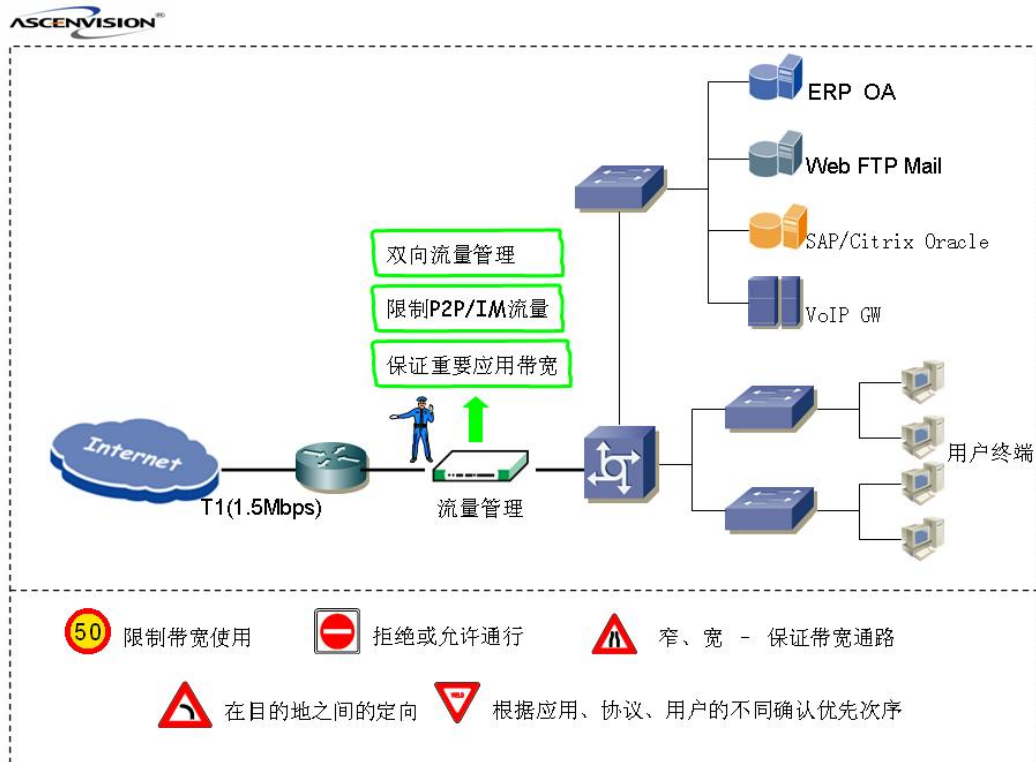
13、问题：如何监控和管理网络流量？限制网络 BT,网络视频等带宽？

问题：如何保障企业网上关键应用的带宽流量？

现有情况描述

某企业由于带宽使用不当，经常造成网络堵塞，无法监控及分析网络流量日志，影响网络中 ERP、OA 等重要应用服务，降低了企业的整体工作效率。

实施后网络拓扑结构



解决方案描述

在网络中部署 AscenVision 的 AscenFlow 设备，对企业重要的应用分配保证带宽，还可以对服务内容赋予相应的优先级，对个别人员使用 BT、网络电视等占用高带宽程序阻止或限速，使网络带宽得到了合理的分配，提高带宽的利用率。

总结

AscenVision 的 AscenFlow 是针对网络带宽控制及流量监控分析的所开发的解决方案。它能提供管理者设定各项服务的基本带宽/最大带宽，并能分析网络性能及流量计费、异常流量监控、异常流量警告等功能。

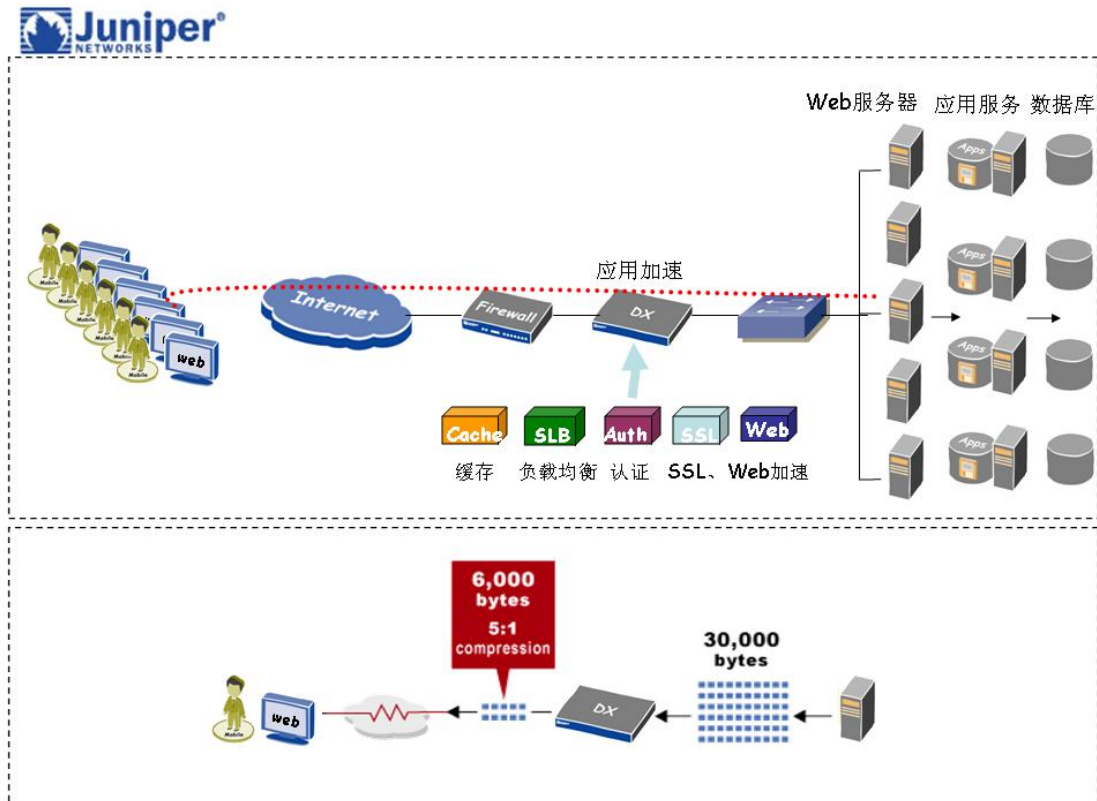
AscenFlow 可确保网络服务质量具有良好的可靠性及性能，能协助管理人员迅速查觉各种网络异常情况，快速而正确地将问题解决，让资源分配恰当及弹性化，帮助企业：带宽投资与管理费用两方面获利，是企业最佳的网络流量监控与决策分析系统

14、如何提高 WEB 服务器的被访问速度，优化服务器资源？

现有情况描述

在某企业的 IDC 机房部署大量的 Web 服务器群对外提供服务，由于每日访问量过大，部分 WEB 服务器负载较大，回应速度较慢，因此影响了终端用户访问网站的速度，打开页面时间缓慢，甚至无法打开而面，导致用户选择了其他同类型的门户网站，从而影响了该企业的业务拓展。

实施后网络拓扑结构



解决方案描述

针对该企业反映的情况我们选择了 Juniper DX 应用加速平台系列产品，利用 DX 应用加速平台，通常可使访问业务关键应用的时间缩短一半，极大地提高应用可用性，尤其对远程和分支机构用户更为有效。DX 平台可实时优化并压缩所有发出的 Web 数据，而且时延几乎可以忽略不计，用户可以快速加载页面，不受位置和网络连接的影响。而且 DX 应用加速平台提供了完全的第 4 层至第 7 层服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群的部署。

总结

DX 系列应用加速平台加速 Web 应用同时缩短用户访问网站所需的时间，减少带宽消耗，并提高应用可扩展性。同时 DX 平台具有验证用户、保护数据和连接安全、保护服务器免受 DOS 和 SYN 泛滥攻击的功能。DX 应用加速平台结合了关键安全功能，在易用管理的灵活产品中提供前所未有的 Web 性能和应用可用性，是新型数据中心公认的基石产品。