飞塔公司教育行业解决方案介绍

2008年9月

FORTINET

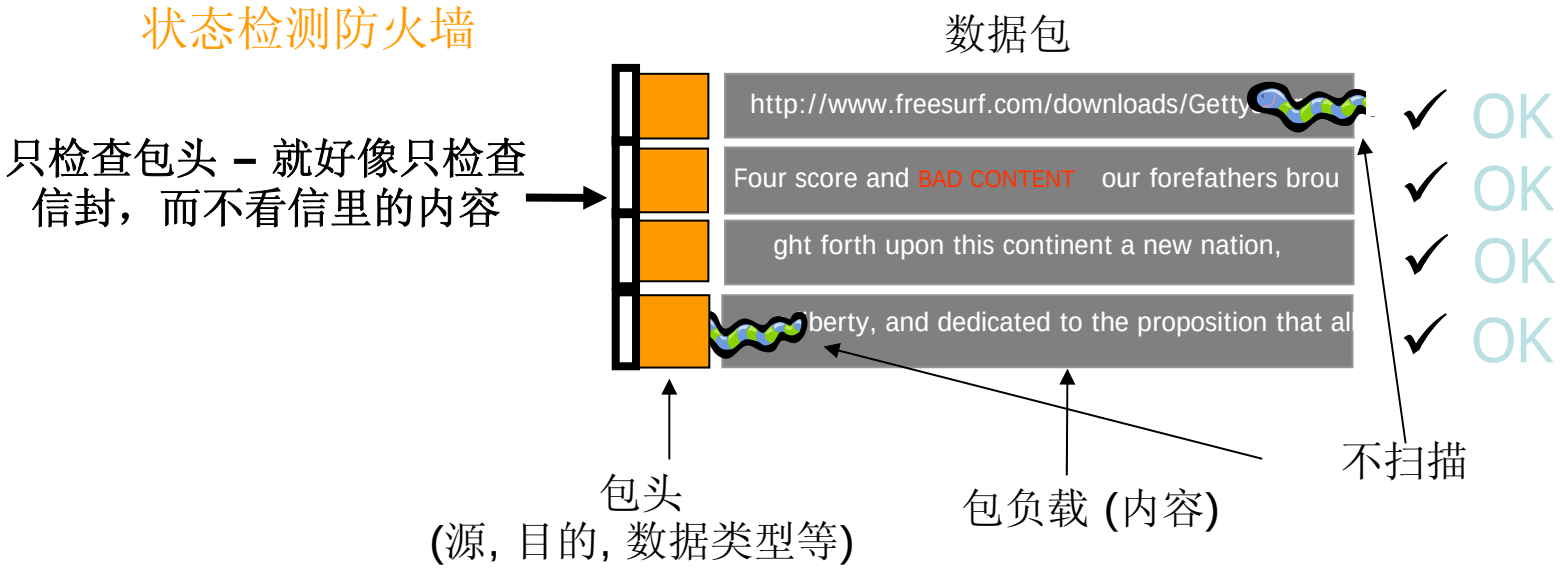
议程

1	教育安全解决方案（1） — 防御多种安全威胁
2	教育安全解决方案（2） — 高性能及高可靠性
3	教育安全解决方案（3） — 有效的管理
4	Fortinet公司介绍

高校A校园网安全现状

- 学生进行Internet访问时带入大量病毒、木马、蠕虫、间谍软件（通过浏览网页、Email、聊天、下载等多种方式）
- 大量蠕虫病毒在校园网各区域之间泛滥，形成DDoS攻击，导致网络拥塞，主机性能低下
- 校园网内服务器面临各种网络攻击和入侵
- 学生访问Internet上的不良内容（如反动、色情的内容等）
- 垃圾邮件降低效率，占用网络资源

防火墙无法实现多层次安全防御



传统防火墙弱点如下：

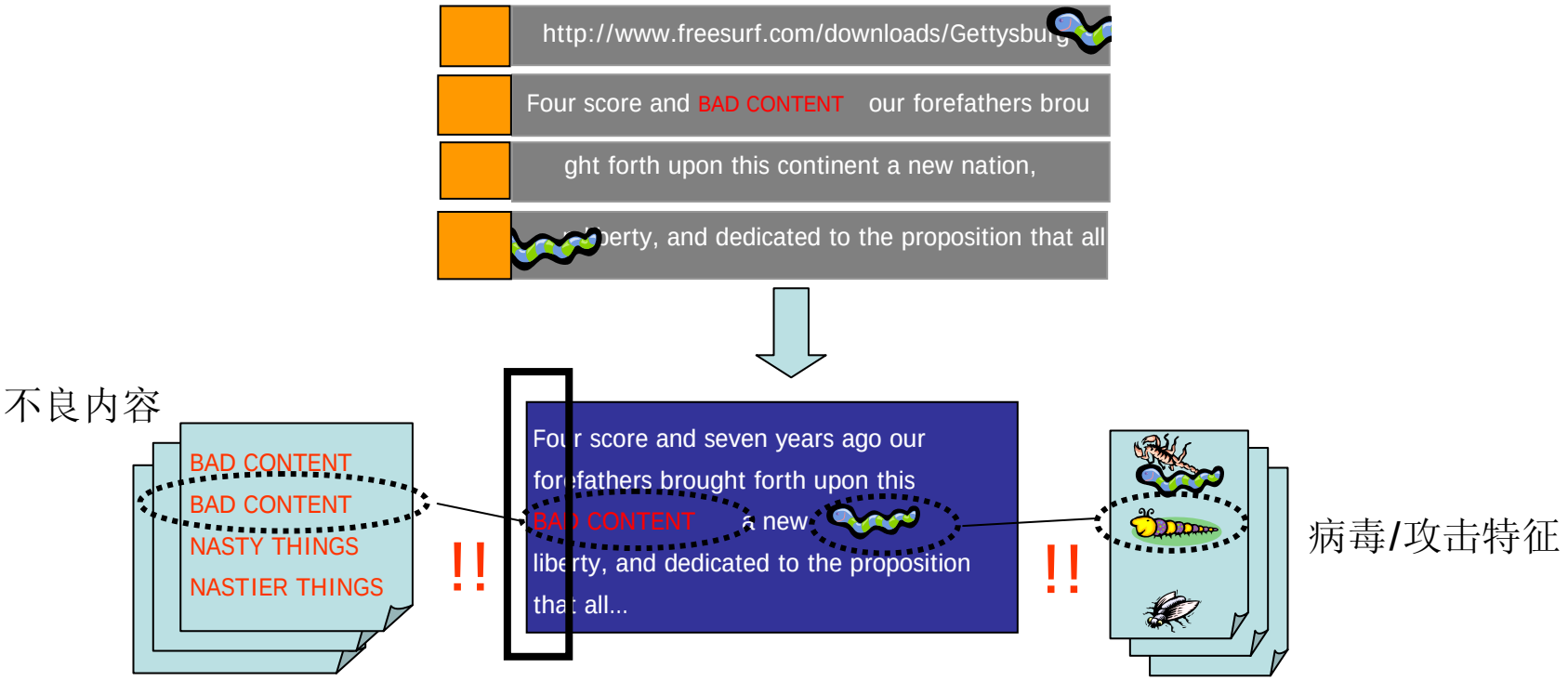
- 没有深度包检测来发现恶意代码
- 每包的转发方式，不能进行包重组
- 恶意程序可以通过信任端口建立隧道穿过去
- 传统的部署方法仅仅是网络边缘，不能防御内部攻击

FORTINET

完全内容检测机制

完全内容检测

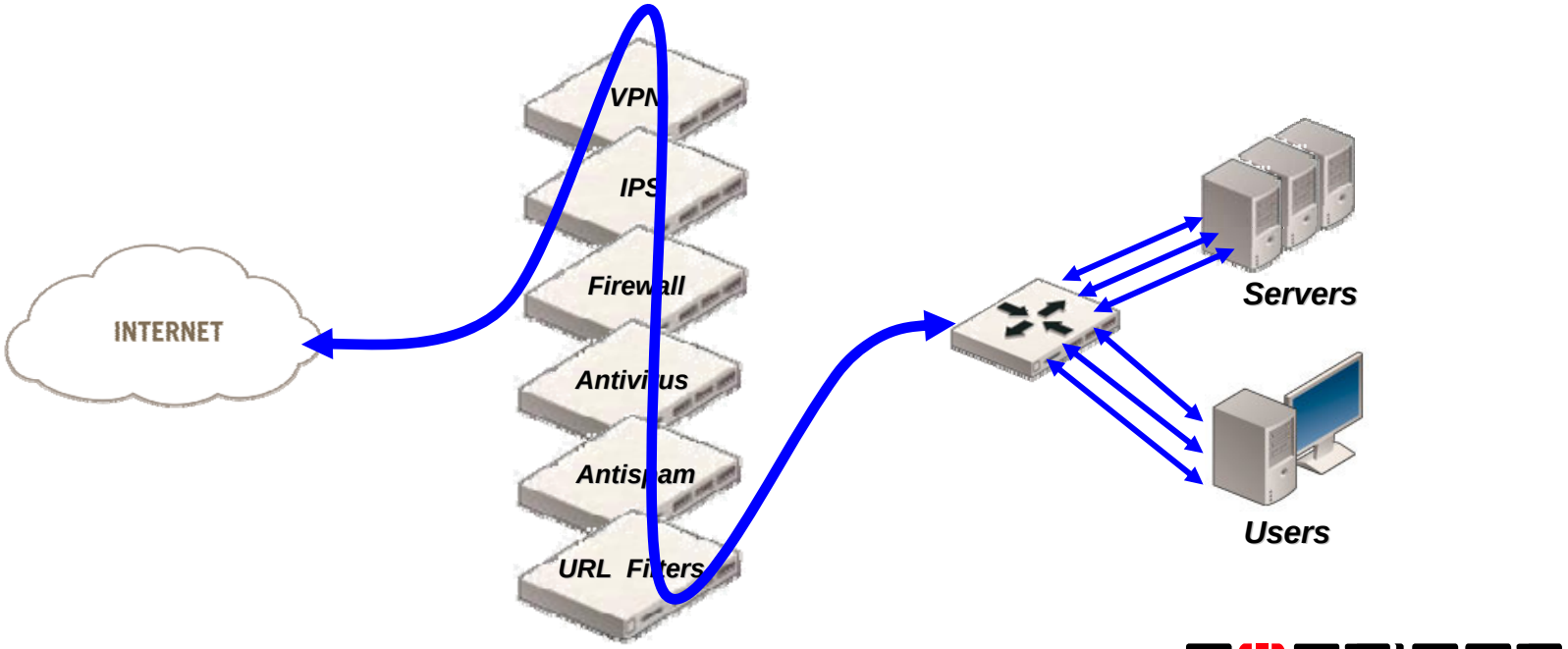
1. 重新组装数据包



2. 完整比较攻击特征库和蠕虫样本库

多产品方案的局限性

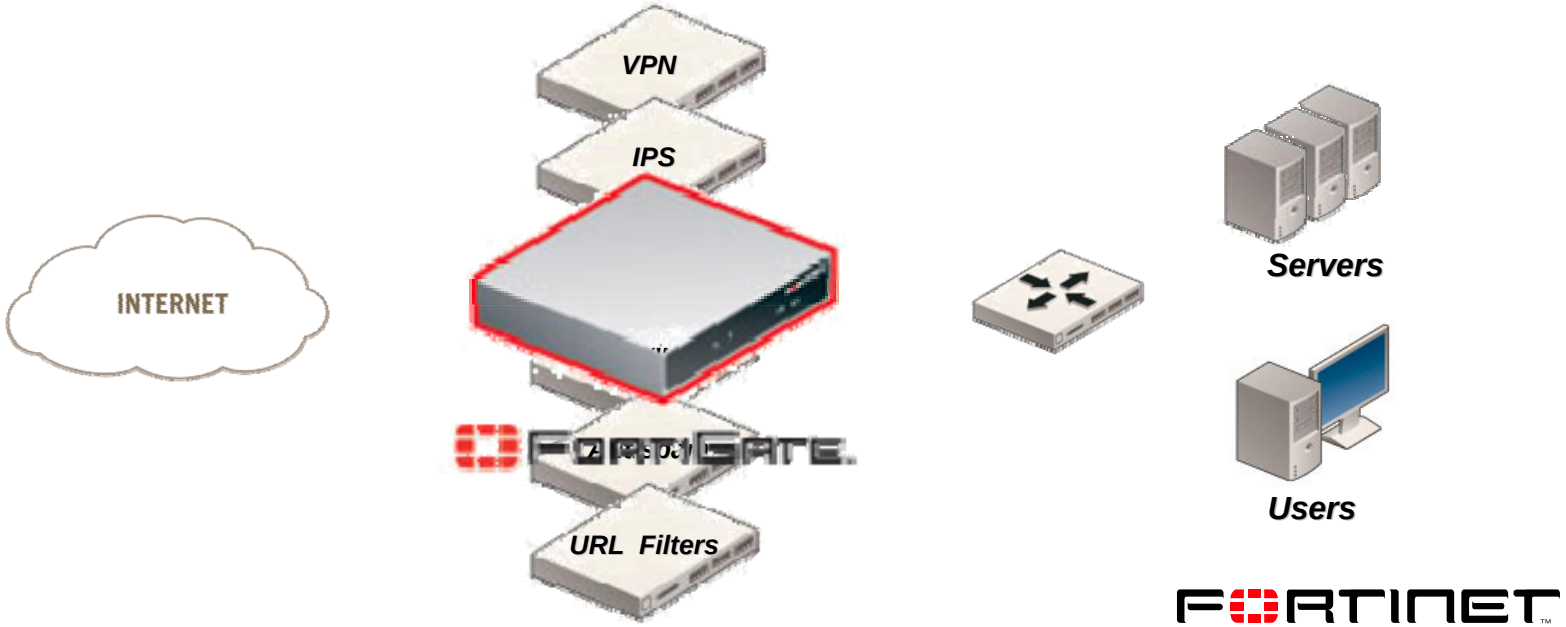
- 假设的优势
  - 全面的安全
  - 对个人攻击能够迅速地反应
- 真实的缺点
  - 需要部署不能相互通讯的多种产品
  - 提高了网络的复杂性和操作成本
  - 不是最佳的安全部署方法



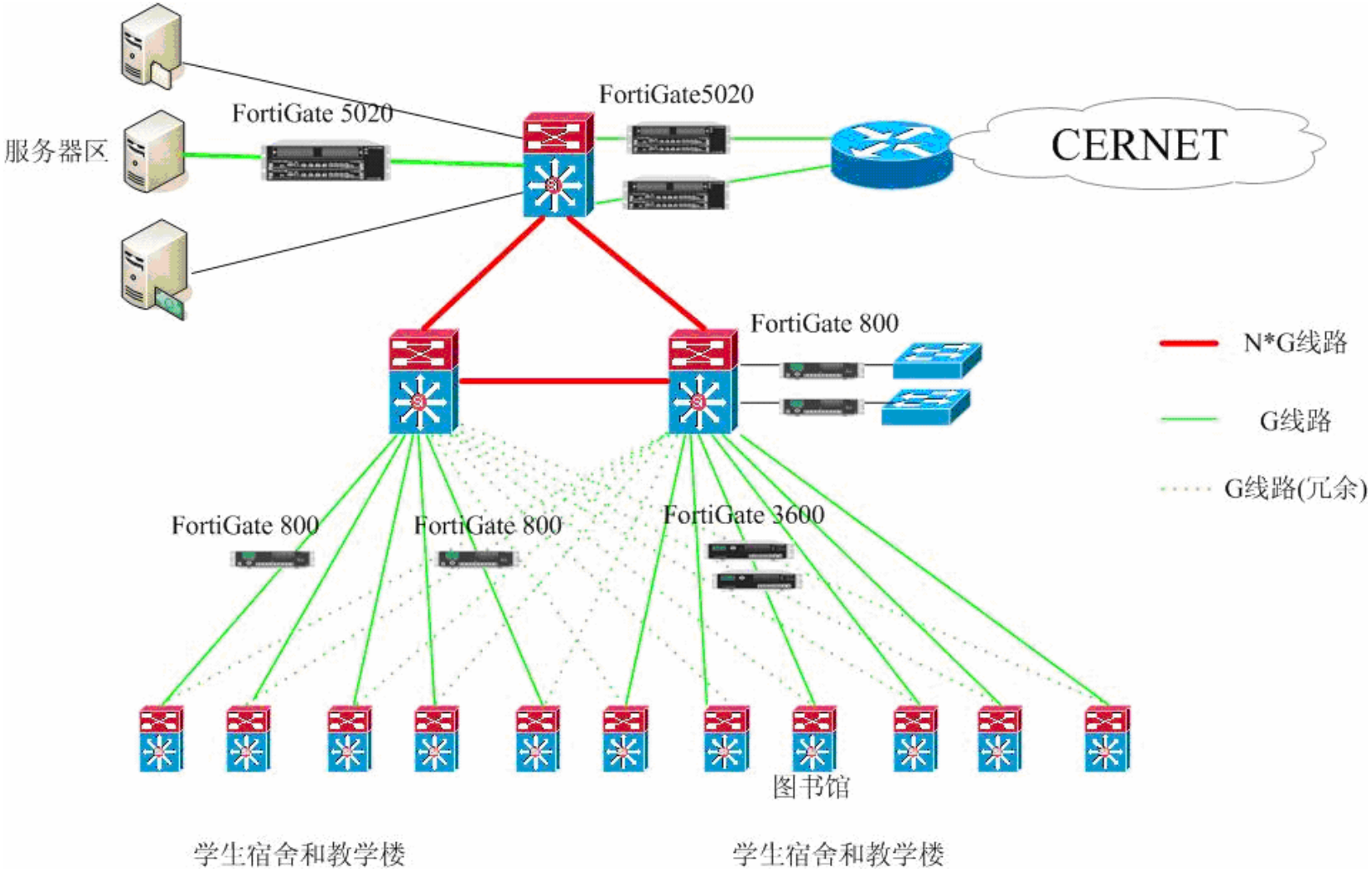
FORTINET

Fortinet的解决之道

- Fortinet优势
  - 全面的安全
  - 最大化地减少了攻击导致的宕机时间
  - 减少了厂商和设备的数量
  - 简化了安全管理
  - 相应的安全报警、日志和报表
  - 提高检测能力

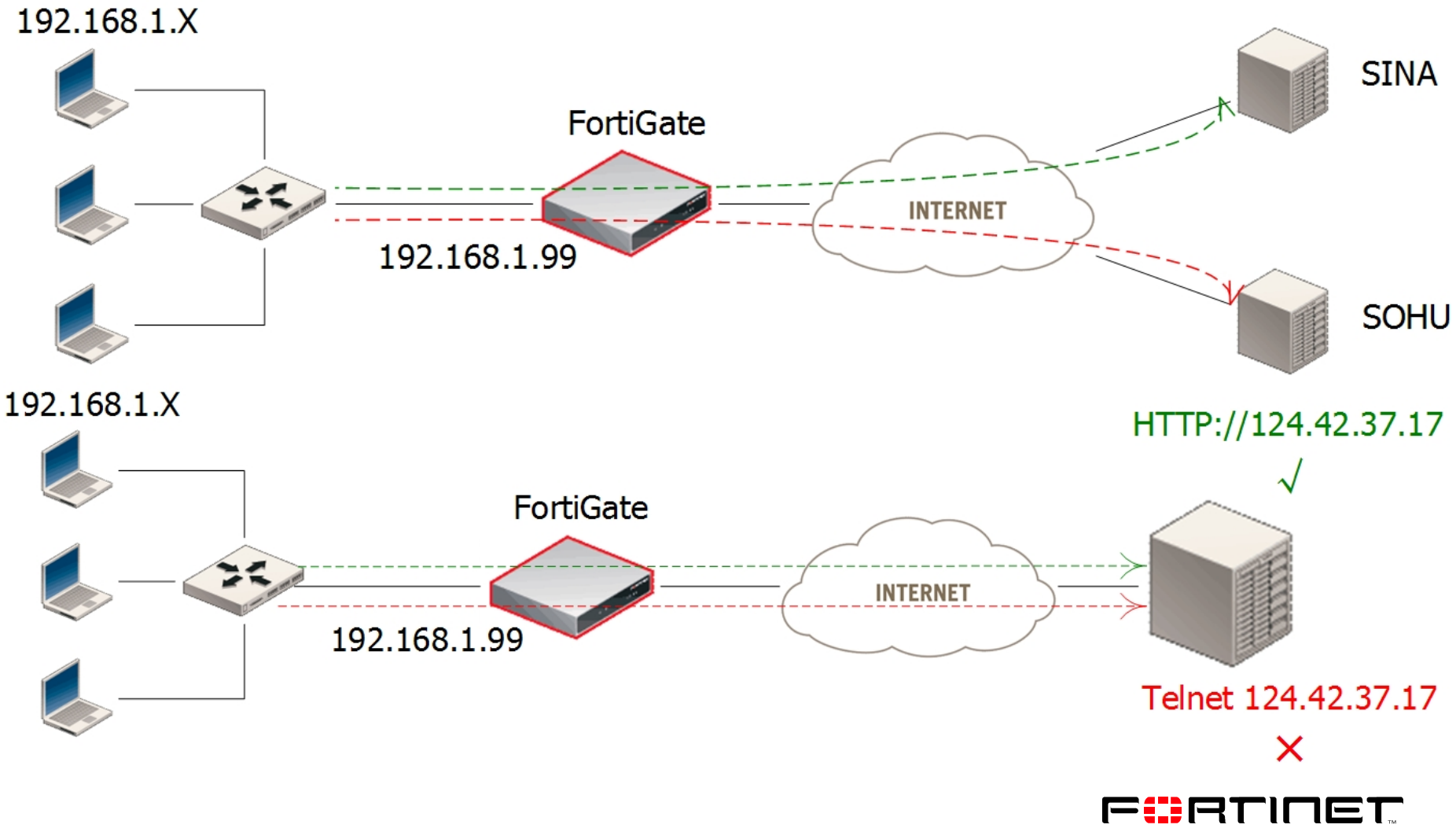


FortiGate在高校A的部署



FORTINET

防火墙 - 安全区域之间的访问控制



IPS与防病毒的结合

Exploit.MyDoom-net	服务器	TCP	Windows	Other		通过	worm
LSASS.Bind.0090.139	服务器	TCP, NBSS	Windows	Other	✓	丢弃	worm
Trojan.Storm.Worm.HTTP.DoS	服务器	TCP, HTTP	Windows	Other		通过	worm
Trojan.Storm.Worm.Krackin.Detection	用户端, 服务器	UDP	All	All		通过	worm
Virus.Massacre.POP3	用户端	TCP, POP3	Windows	Other		通过	worm
Virus.SDBot.Command.PRIVMSG	用户端, 服务器	TCP	Windows	Other	✓	通过	worm
W32/Bropia.A-tr.MSNFTP	用户端, 服务器	TCP	Windows	Other		通过	worm
W32/Bropia.D-net.MSNP2P	用户端, 服务器	TCP	Windows	Other		通过	worm
W32/Bropia.E-net.MSNFTP	用户端, 服务器	TCP	Windows	Other		通过	worm
W32/Bropia.F-net.MSNFTP	用户端, 服务器	TCP	Windows	Other		通过	worm
Worm.Beagle.AA.SMTP	服务器	TCP, SMTP	Windows	Other		通过	worm
Worm.Blaster.POP3	用户端	TCP, POP3	Windows	Other	✓	通过	worm
Worm.Loveletter.VBS.POP3	用户端	TCP, POP3	Windows	MS_Office		通过	worm
Worm.Lupper	用户端, 服务器	TCP, HTTP	All	PHP_app, CGI_app	✓	通过	worm
Worm.Netsky	服务器	TCP, SMTP	Windows	Other		通过	worm
Worm.Netsky.Z.POP3	用户端	TCP, POP3	Windows	Other		通过	worm
Worm.W32.Nyxem	用户端, 服务器	TCP, DCERPC, NBSS, SMTP, HTTP	Windows	Other		通过	worm
Worm.W32.Sasser	服务器	TCP	Windows	Other	✓	丢弃	worm

- 通过IPS方式阻挡蠕虫病毒在校园网内的传播，保护骨干网的安全

FORTINET

在Internet出口过滤不良网页内容

- FortiGuard动态过滤
  - 76个类别
  - 超过2850万个网站
  - 数十亿个网页
  - 实时更新数据库
- URL过滤
  - 黑白名单
- 关键字过滤
  - 支持多种语言
- 安全过滤
  - ActiveX
  - Java Applet
  - Cookies

FORTINET

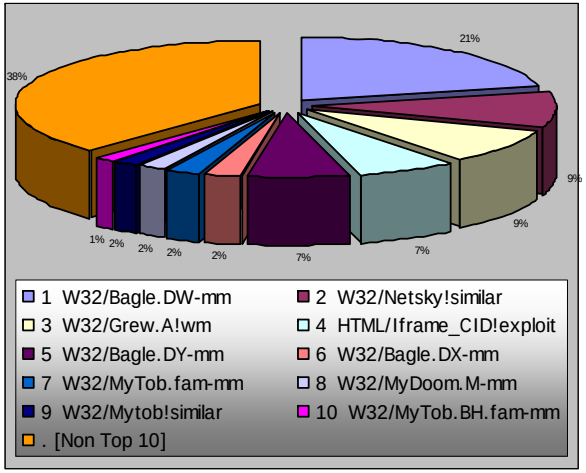
反垃圾邮件

- 使用FortiGate或FortiMail保护邮件服务器、过滤垃圾邮件
  - 降低感染病毒及网络欺诈的风险
  - 减少带宽占用、降低服务器负载
  - 提高学习工作效率
  - 防止学校公网IP被其它邮件服务商列入黑名单

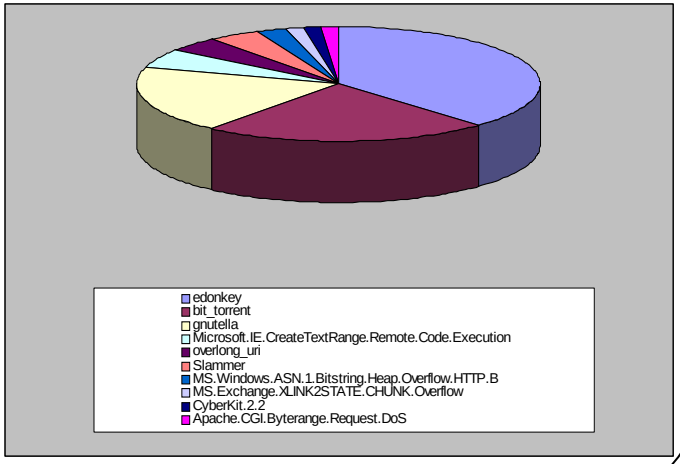
FORTINET

各项UTM功能均实时更新特征库

防病毒
(包括防间谍软件)



入侵防御系统
(IPS)



FDS MALAYSIA

Web 内容过滤

- **76**个以上有害或危险的类别
- 业界最佳的精度和覆盖率**!**

SLA 响应时间 **< 2 hrs.**

反垃圾邮件

- 超过**97.4%**的垃圾邮件捕获率
- 低于**0.18%**的误报率

24x7 全球威胁响应实验室

FORTINET

高校A部署FortiGate产品的效果

- 病毒数量大幅度减少，校园网因病毒泛滥而陷入瘫痪的情况不再发生。
- 校园网各区域（骨干网、网络中心、各院系、图书馆、学生宿舍等）之间通过防火墙、防病毒、IPS等功能实现了有效隔离，某个学院或宿舍楼的病毒或攻击不会扩散到校园网的其它区域。
- 服务器被内外网入侵的危险性降至最低限度。
- 学生无法访问不被允许的网站。
- 垃圾邮件数量减少了95%以上，邮件服务器的负载得以减轻。
- 防病毒、IPS、Web过滤、反垃圾邮件功能自动在线更新，新的安全威胁在第一时间即可防御。

FORTINET

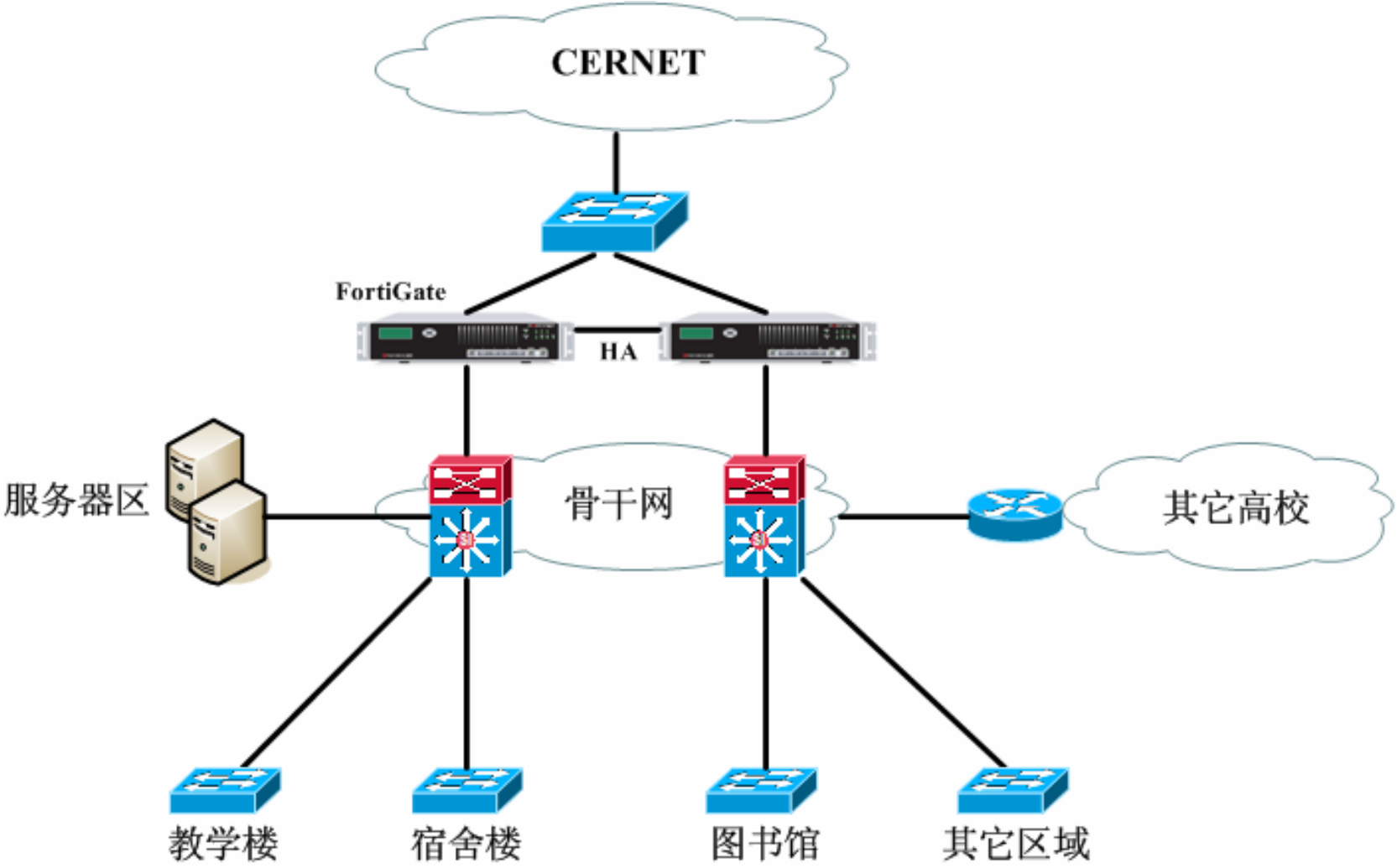
议程

1	教育安全解决方案（1） — 防御多种安全威胁
2	教育安全解决方案（2） — 高性能及高可靠性
3	教育安全解决方案（3） — 有效的管理
4	Fortinet公司介绍

高校B网络现状及需求

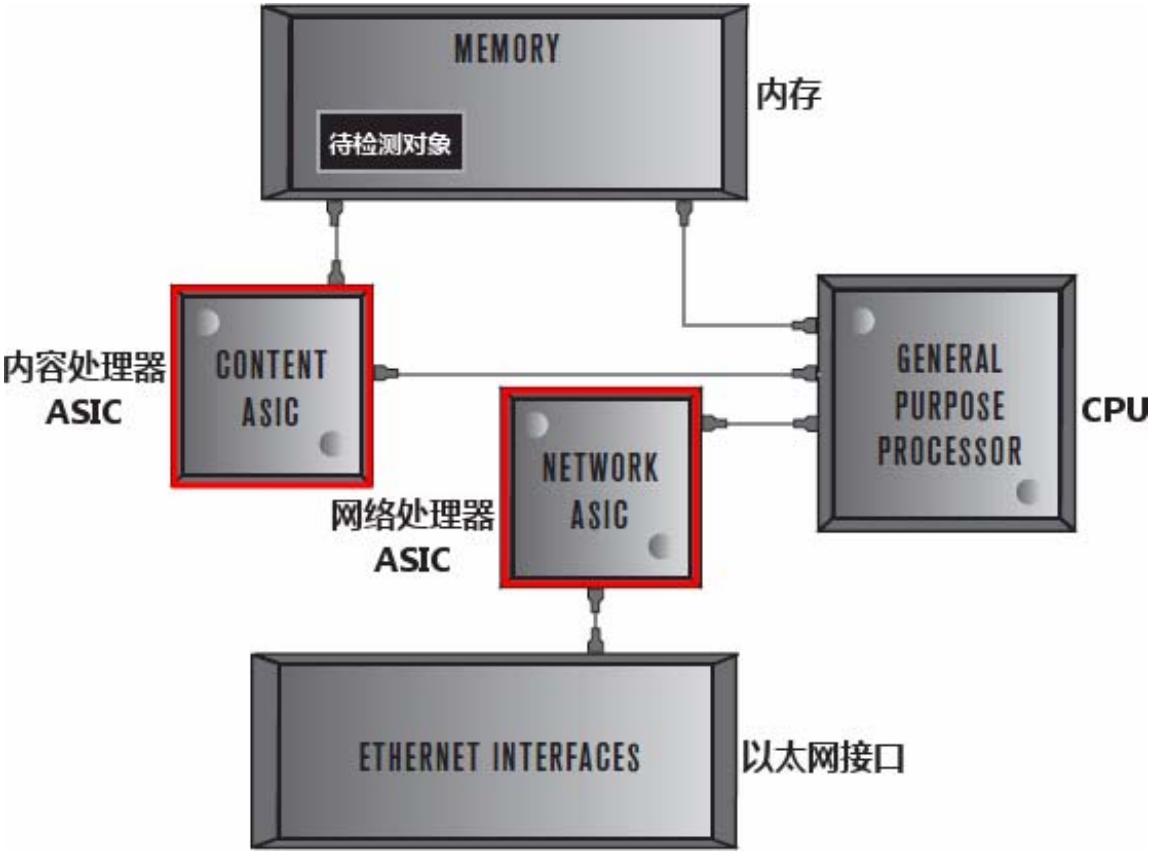
- 高校B拥有教职工、学生共数万人，且是数十所高校的CERNET接入节点，粗略估计有30万以上用户使用高校B的CERNET出口。
- 根据网管软件的监控结果，出口实时网络进出流量超过2Gbps，并发会话数超过100万。
- 之前使用的防火墙不堪重负，对于网络访问产生较高延迟，影响了网络服务质量。丢包现象也时有发生，严重时还会导致网络中断。
- 由于高校B网络出口的重要性，因此对网关防火墙的可靠性要求也非常高。

FortiGate在高校B的部署



独特的双ASIC芯片加速

- **FortiASIC-CP (内容处理器)**
  - 特征匹配
    - 防病毒
    - IPS
    - 内容过滤
  - 加密解密
    - VPN协商
    - 密钥维护
- **FortiASIC-NP (网络处理器)**
  - 高速包转发
    - 线速防火墙
    - IPSec VPN
    - NAT
    - 防DoS攻击
    - 流量整形



部分产品性能测试结果 - 吞吐量

- NAT模式，UDP防火墙双向吞吐量（单位：Mbps）

型号	接口	64	512	1518
FGT-310B	Port1-Port2	2000.00	2000.00	2000.00
FGT-3016B-FB4 Ports	amc-sw1/1-amc-sw1/2	2000.00	2000.00	2000.00
FGT-3600A-FB4 Ports	amc-sw1/1-amc-sw1/2	2000.00	2000.00	2000.00
FGT-3810A-FB4 Ports	amc-sw1/1-amc-sw1/2	2000.00	2000.00	2000.00
FGT-5001A-FB8	amc-dw1/1-amc-dw1/2	2000.00	2000.00	2000.00

高校B部署FortiGate产品的效果

- FortiGate 3000及5000系列在高达数Gbps的网络流量，百万级并发会话的情况下，仍能实现各种大小包的线速转发，网络延迟保持在微秒级别。防火墙不再成为高校B CERNET出口的性能瓶颈。

- FortiGate自身的可靠性设计（专用ASIC、NP芯片及专用安全操作系统，冗余电源风扇），配合优秀的HA保护机制，为高校B的网络运行提供365×24的全天候保障。部署3年多以来，设备一直稳定运行，从未发生网络中断故障。

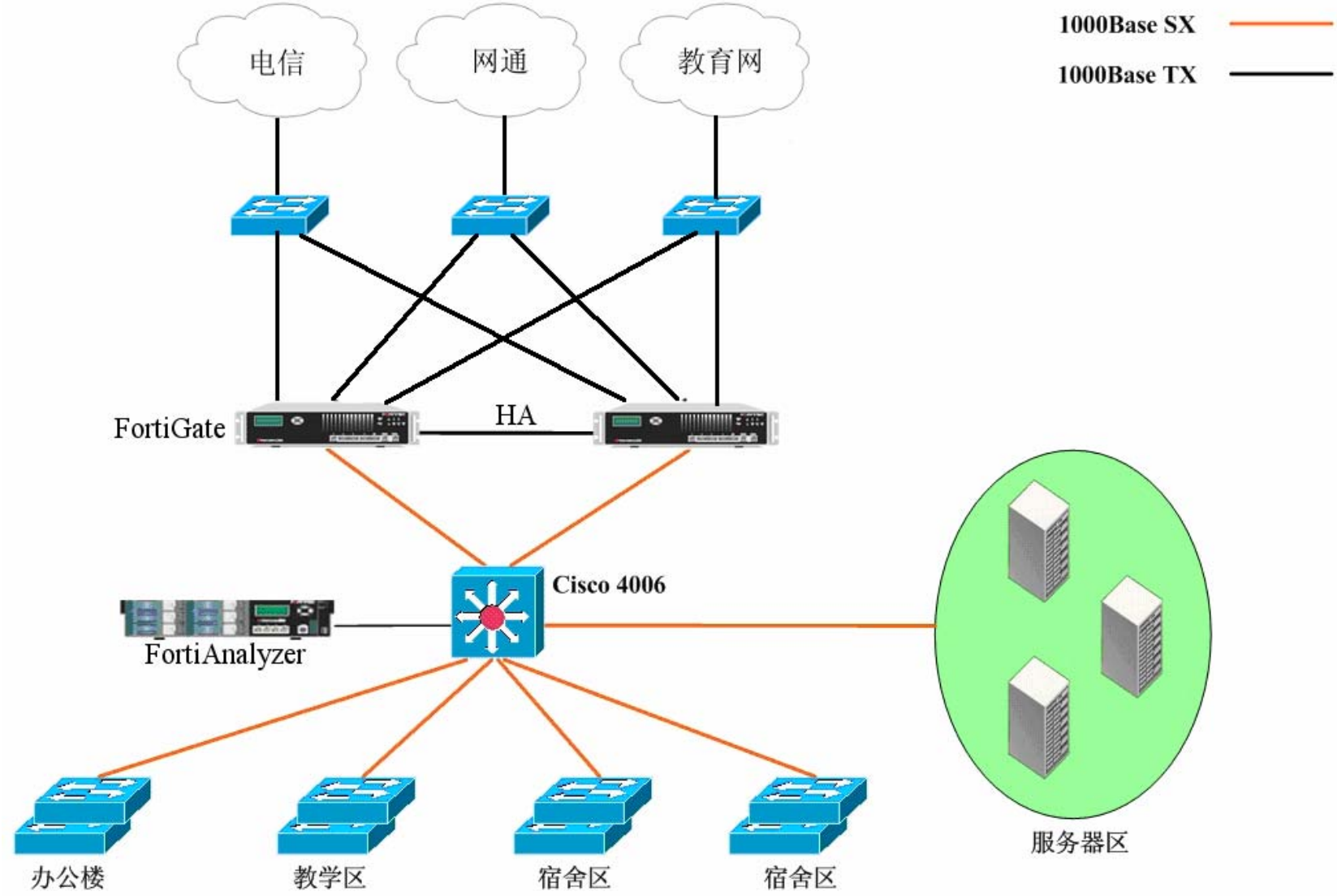
议程

1	教育安全解决方案（1） — 防御多种安全威胁
2	教育安全解决方案（2） — 高性能及高可靠性
3	教育安全解决方案（3） — 有效的管理
4	Fortinet公司介绍

高校C网络现状及需求

- 高校C具有一万多在校学生，加上教职工及家属，学院网络用户总数上万人。
- 学校共有3个网络出口：电信、网通、教育网出口。其中教育网出口的国际流量是按流量大小计费的，所以对教育网的国际流量很敏感，要求出国流量全部走电信或网通出口。同时要求电信及网通出口进行流量优化，实现链路冗余及负载分担。
- 流量的管理：校园网用户数量众多，应用五花八门，流量组成很复杂，下载和P2P（BT、电驴等）、P2SP（迅雷等）类的流量占据了大部分的带宽，需要实现对带宽的控制。
- 该学校是一个管理相对松散的机构，网络中心对各院系部门没有很强的约束力，只能对各种非正常访问和网络滥用进行记录分析，呈交给上级主管部门。因此要求能对网络故障、异常要能迅速定位并形成可读性强的报表。

Fortinet产品在高校C的应用



多链路管理

静态路由 | 策略路由

新建

#	流入接口	流出接口	源地址	目的地址
131	port8	port2	121.33.253.214 / 255.255.255.255	192.168.0.0 / 255.255.0.0
128	port1	port7	0.0.0.0 / 0.0.0.0	61.144.43.224 / 255.255.255.240
127	port1	port8	0.0.0.0 / 0.0.0.0	121.33.253.208 / 255.255.255.240
117	port2	port3	0.0.0.0 / 0.0.0.0	210.38.112.0 / 255.255.255.0
6	port2	port5	0.0.0.0 / 0.0.0.0	202.113.0.0 / 255.255.0.0
7	port2	port5	0.0.0.0 / 0.0.0.0	202.204.0.0 / 255.252.0.0
8	port2	port5	0.0.0.0 / 0.0.0.0	210.31.0.0 / 255.255.0.0
9	port2	port5	0.0.0.0 / 0.0.0.0	211.68.0.0 / 255.255.0.0
10	port2	port5	0.0.0.0 / 0.0.0.0	211.71.0.0 / 255.255.0.0

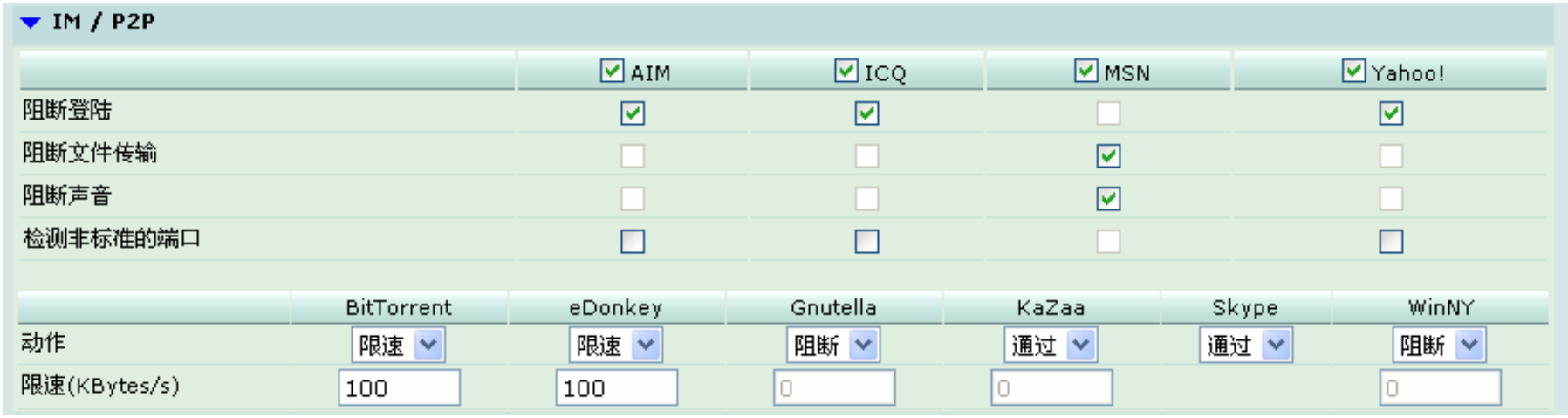
- 利用静态路由实现分流，访问教育网内资源时使用教育网链路，访问其它国内及所有国外资源使用电信或网通出口。
- 可以通过静态路由、策略路由、等值路由等多种方式实现电信和网通出口的链路负载分担，实现带宽最优化分配。
- 利用端口检测、ping服务器检测等方式探测链路健康状况，如果电信、网通中的任意一个出口发生故障，都可以自动迅速将流量切换到另一条链路。出于费用角度考虑，教育网链路不参与出口冗余设计。

注：FortiGate还支持RIP、OSPF、BGP等动态路由协议，并支持IPv6网络，可以很好的融入各种各种校园网环境。

FORTINET

带宽管理

- 虽然高校C的出口资源比较丰富（3个Internet出口，总出口带宽超过1G），但由于上网人数众多，因此网络资源仍然比较紧张。需要进行优化管理。
- 首先，利用FortiGate的P2P管理及IPS功能，对公共上网区（如各教学楼、图书馆等）禁用P2P、迅雷等下载工具，保证网络访问速度。

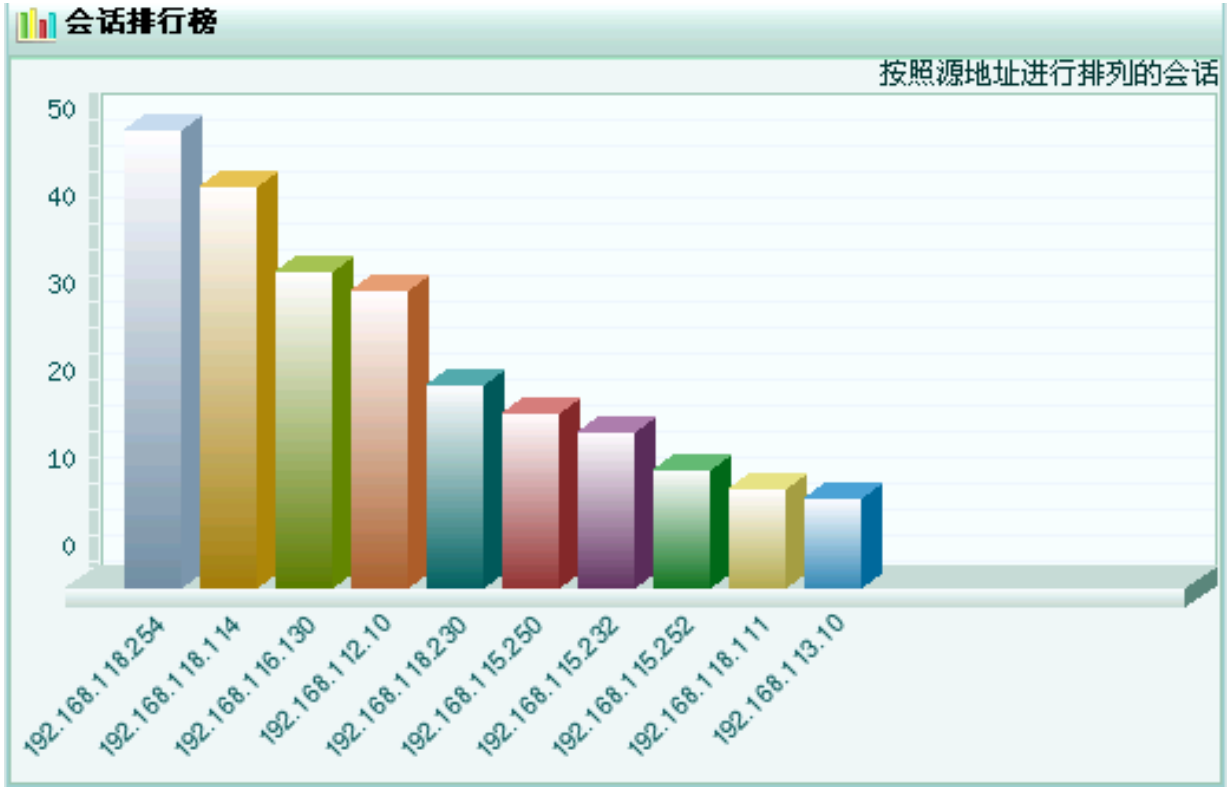


带宽管理

- 宿舍楼、家属楼内用户均为付费用户，不能简单的禁止所有P2P、P2SP等下载行为，因此采用带宽限制、会话数限制等方式降低P2P、 P2SP等行为对网络资源的占用。

异常行为管理及网络监控

- 利用FortiGate的会话管理功能，可以很容易的掌握全网的会话情况，并可列出实时IP地址会话排名，帮助及时发现网络中的异常（如蠕虫病毒、DoS攻击、超常的P2P行为等）。
- 并可直接中止会话。



用户管理及访问记录

- 教师、学生等上网均需要进行身份认证，FortiGate支持Radius、LDAP、Windows AD、TACACS+等多种认证协议，直接使用高校C原有的LDAP认证服务器，无需重新建立用户数据库。
- 使用FortiAnalyzer日志审计设备，将病毒、入侵、不良内容、垃圾邮件、P2P下载等行为进行记录，并保留足够长的时间（如2个月）。用户访问行为也可进行记录，并将IP地址与用户名、用户组相对应。

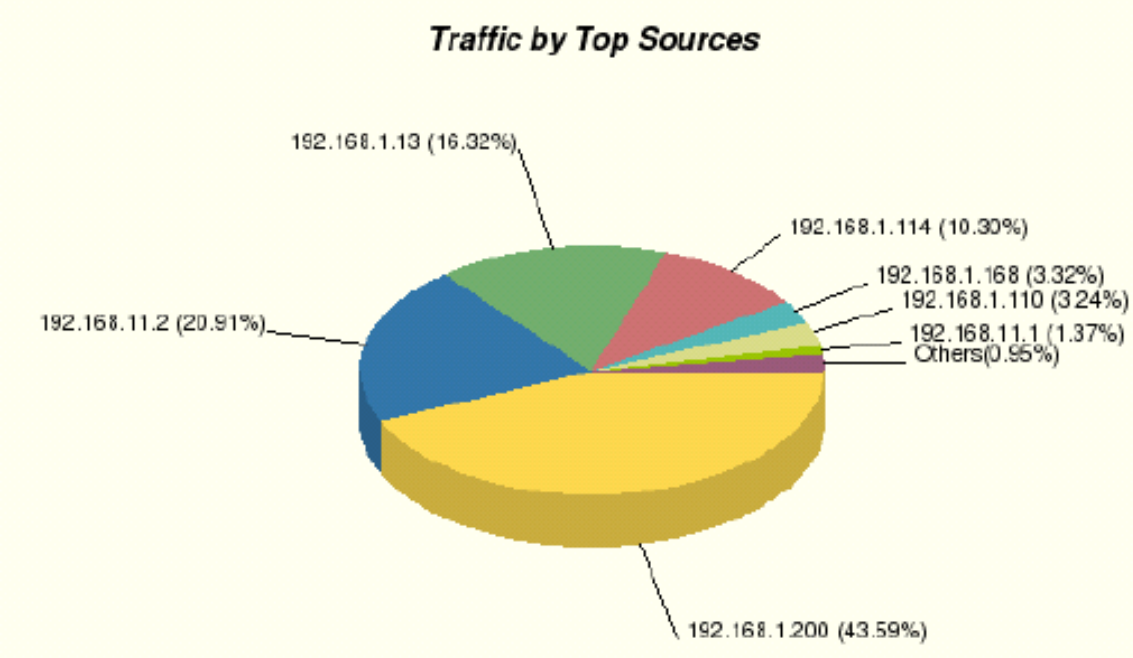
1	2007-03-05	17:23:46	192.168.118.2	210.51.190.99	ftp	EICAR_TEST_FILE	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
2	2007-03-05	17:22:52	192.168.118.2	210.51.190.99	ftp	EICAR_TEST_FILE	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE

43	2007-03-06	15:36:40	192.168.115.52	60.209.36.110	1812/udp	radius_decoder: RADIUS.Malformed.Packet	http://www.fortinet
44	2007-03-06	15:36:40	192.168.115.52	60.209.36.110	1812/udp	radius_decoder: RADIUS.Invalid.Message.Length	http://www.fortinet
45	2007-03-06	15:36:35	192.168.115.52	60.209.36.110	1812/udp	radius_decoder: RADIUS.Malformed.Packet	http://www.fortinet

1	2007-03-06	15:37:29	Skype	block	192.168.115.52	60.21.80.27
2	2007-03-06	15:36:59	eDonkey	limit	192.168.115.52	221.11.2.81

网络访问报表

- 利用FortiAnalyzer记录日志，并产生各种报表（超过300种），直观反映网络中的各种事件。如
  - 协议分布
  - 流量排名
  - 病毒、攻击、不良内容、垃圾邮件统计等



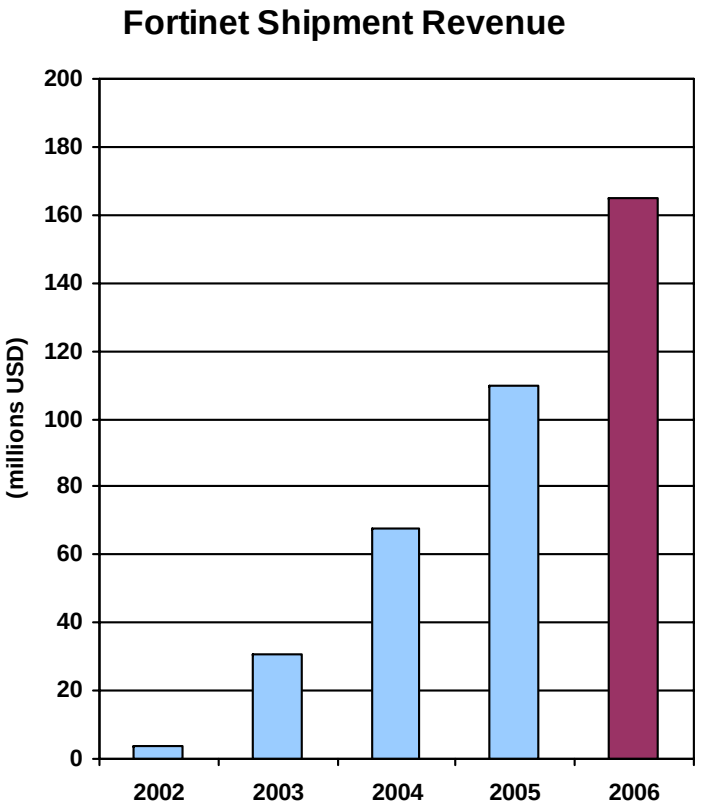
按最大来源统计流量		
源地址	流量 (kB)	% of Total
192.168.1.200	489563	43.59
192.168.11.2	234870	20.91
192.168.1.13	183320	16.32
192.168.1.114	115714	10.30
192.168.1.168	37242	3.32
192.168.1.110	36370	3.24
192.168.11.1	15394	1.37
10.0.1.129	10525	0.94
192.168.11.33	95	0.01
192.168.1.123	44	0.00
Other	6	0.00
Total	1123150	100

议程

1	教育安全解决方案（1） — 防御多种安全威胁
2	教育安全解决方案（2） — 高性能及高可靠性
3	教育安全解决方案（3） — 有效的管理
4	Fortinet公司介绍

Fortinet公司概况

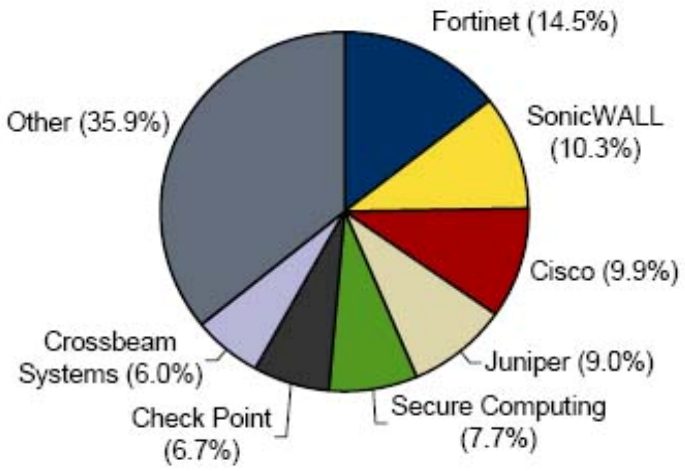
- 第一个基于ASIC技术的多层安全平台提供者
- 专业网络安全厂商
  - 1000+名员工 / 500+名技术人员
  - 超过300,000台FortiGate设备在全球使用
  - 2000年成立
  - 最大的私营安全公司
  - 全球化的公司(U.S., EMEA & Asia Pac)
- 大量的认证
  - 7项ICSA认证(全球唯一)
  - 政府认证 (FIPS-2, Common Criteria EAL4+)
  - 50+ 行业认证
  - VB 100 和 NSS认证



FORTINET

全球UTM销量冠军

Worldwide UTM Revenue Share by Vendor, 2007



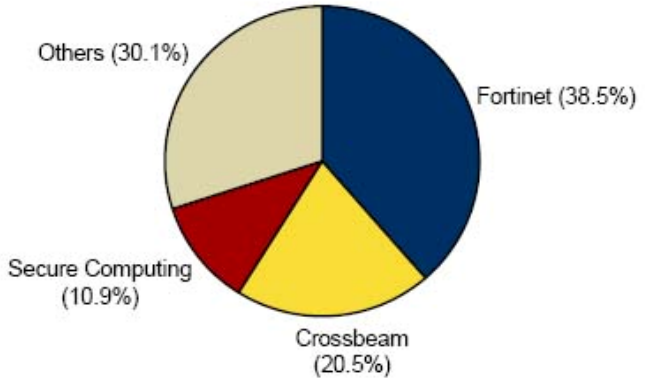
Total = $1.216B

Note: Market shares are based on IDC's Quarterly Security Appliance Tracker.

Source: IDC, March 2008

"Fortinet 引导着UTM技术的发展方向"

Worldwide UTM Revenue Share for the $50,000–99,999 Price Band by Top 3 Vendor, 2007



Total = $64.5M

Note: Market shares are based on IDC's Quarterly Security Appliance Tracker.

Source: IDC, March 2008

"Fortinet UTM 产品系列在全球占有率第一"

FORTINET

Fortinet国内教育行业用户

- 北京大学
- 清华大学
- 北京师范大学
- 北京科技大学
- 西安交通大学
- 国防大学
- 南京航空航天大学
- 中山大学
- 华南师范大学
- 广州外国语大学
- 上海外国语大学
- 惠州大学
- 北京信息工程学院
- 河北经贸大学
- 华北工学院
- 新疆大学
- 天津工业大学
- 广西财经学院
- 天津北方教育网
- 教育部科技发展中心
- 厦门市教育局
- ……

FORTINET

谢谢!

更多信息请访问
http://www.fortinet.com