Huawei Enterprise A Better Way

更专注，更专业

--华为 NIP 产品族汇报

www.huawei.com

HUAWEI

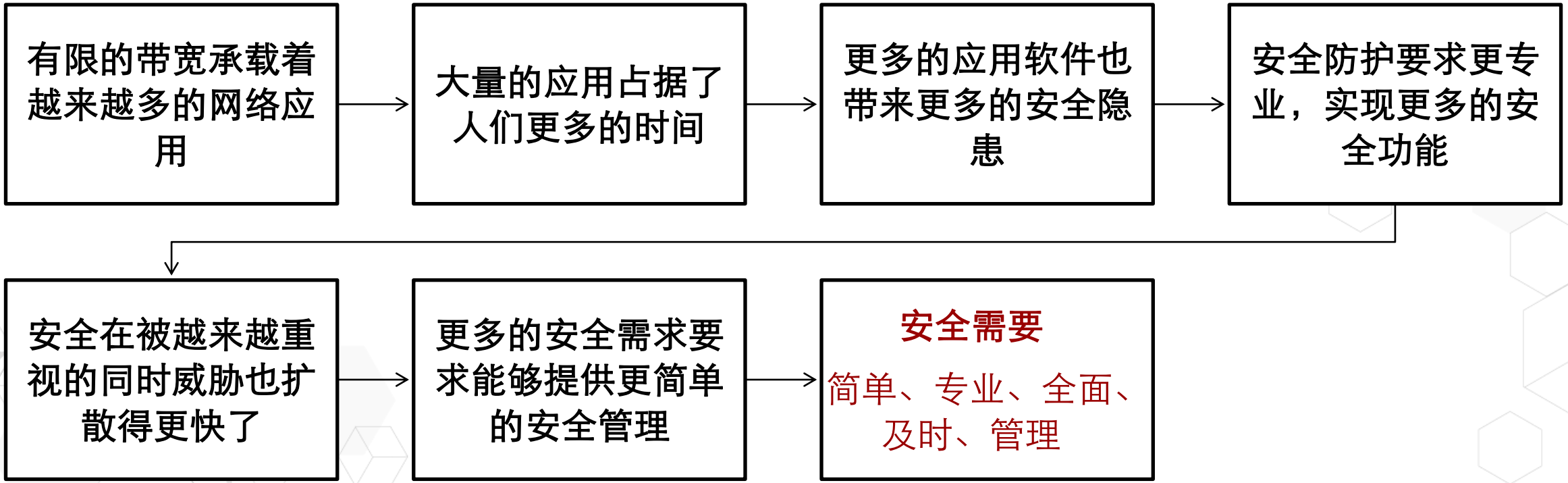
目录

针对客户端的安全威胁日趋严重

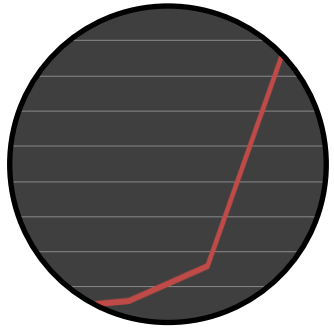
- 赛门铁克发布《第十七期互联网安全威胁报告》
  - 漏洞总数减少了20%，但2011年总的恶意攻击数量猛增了81%;
  - 特殊恶意软件变种数量增加至4.03亿个;
  - 每日被阻止的网页攻击数量也同比增加了36%;
  - 究其原因，赛门铁克方面认为是由于攻击者针对现有漏洞的攻击加强了;

- 漏洞指可被者利用来进行超出应用系统设计者没有预想到的一些操作。
- 攻击威胁指某个针对某个漏洞发起攻击入侵的执行代码或动作

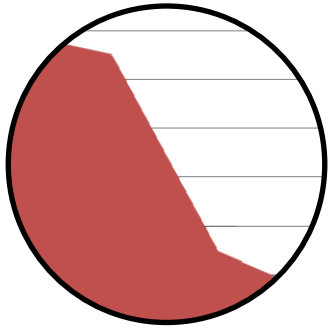
网络安全挑战越来越大


有限的带宽承载着越来越多的网络应用
大量的应用占据了人们更多的时间
更多的应用软件也带来更多的安全隐患
安全防护要求更专业，实现更多的安全功能
安全在被越来越重视的同时威胁也扩散得更快了
更多的安全需求要求能够提供更简单的安全管理
安全需要
简单、专业、全面、及时、管理

IP 网络高速发展



网络带宽不断提高

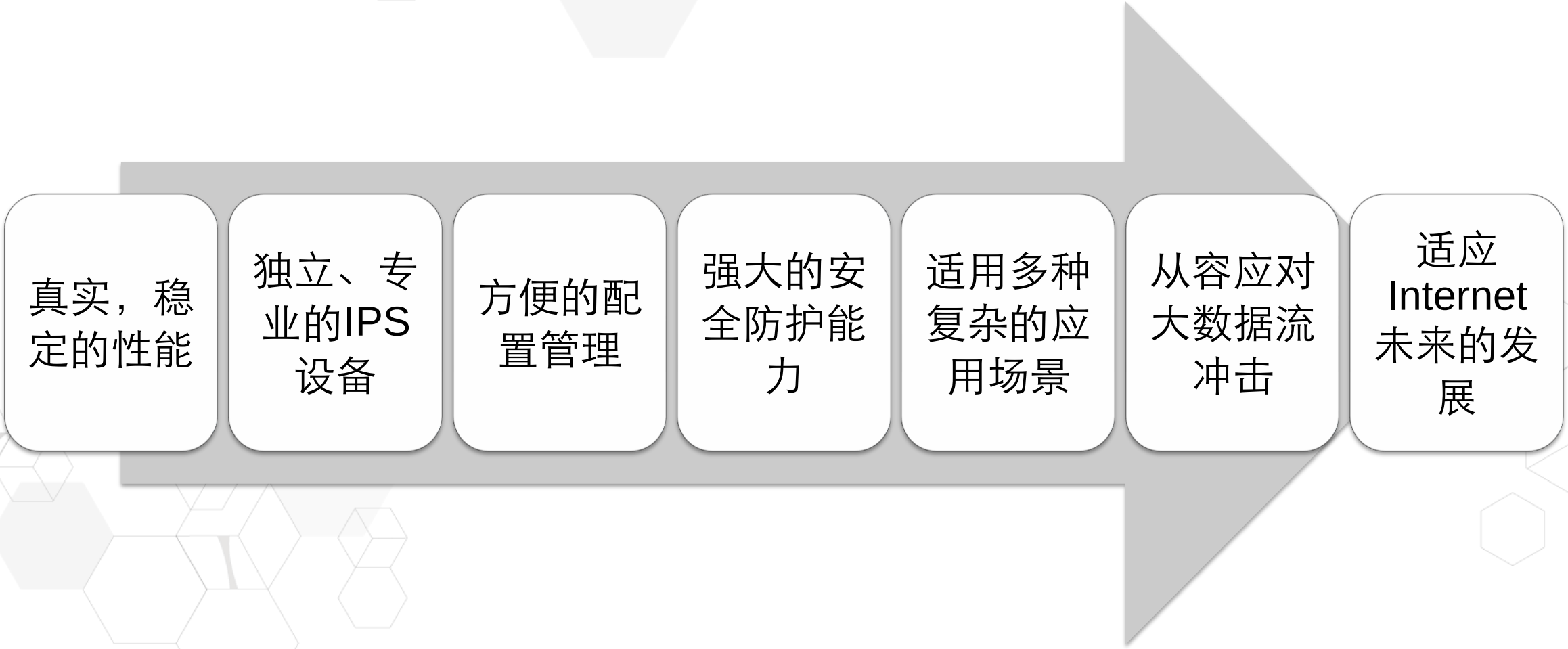


IPv4地址面临枯竭

虚拟化及云趋势

目录

华为 NIP 的定位及设计理念



华为 NIP 领先的硬件架构

多核处理器

- 实现对网络报文的通用预处理；协议智能识别；DDoS攻击防护

FPGA 转发加速

- 实现对安全流量的快速转发

ESP 应用层加速

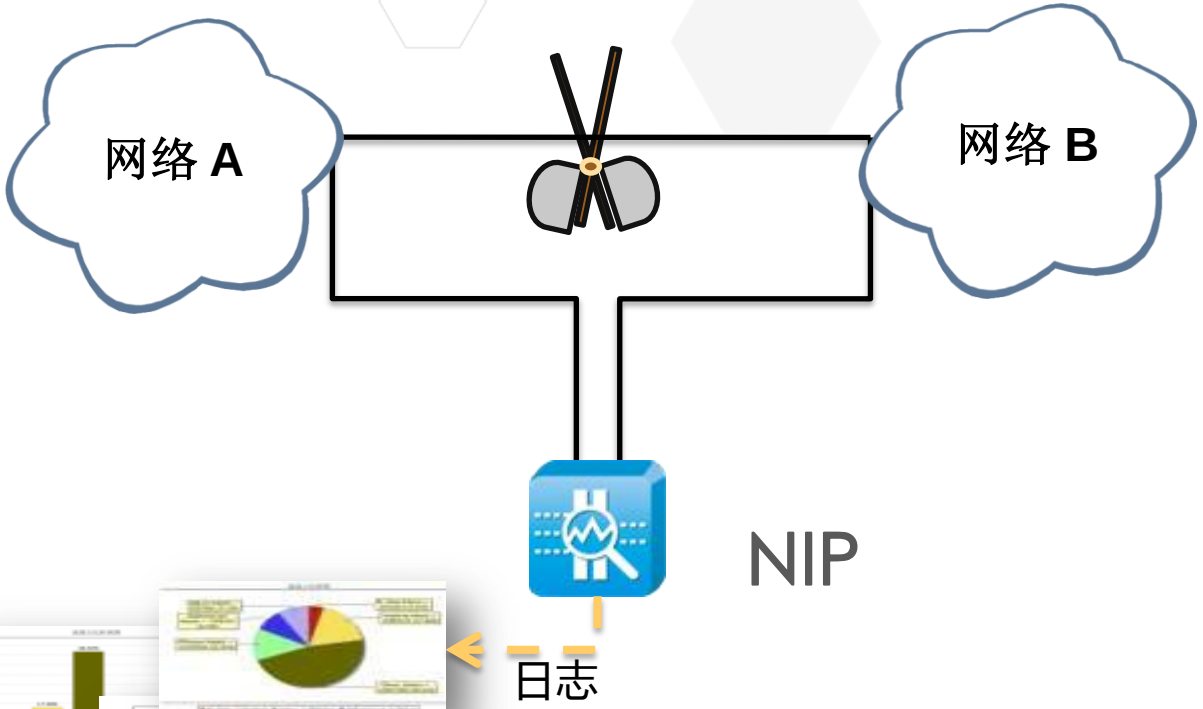
- 实现对应用层威胁的加速检测及响应处理

8 核网络报文处理器，实现会话的快速连接及网络报文预处理

ESP加速板卡实现应用层报文的灵活，快速处理

FPGA卡实现报文的快速转发，最大限度的降低网络时延

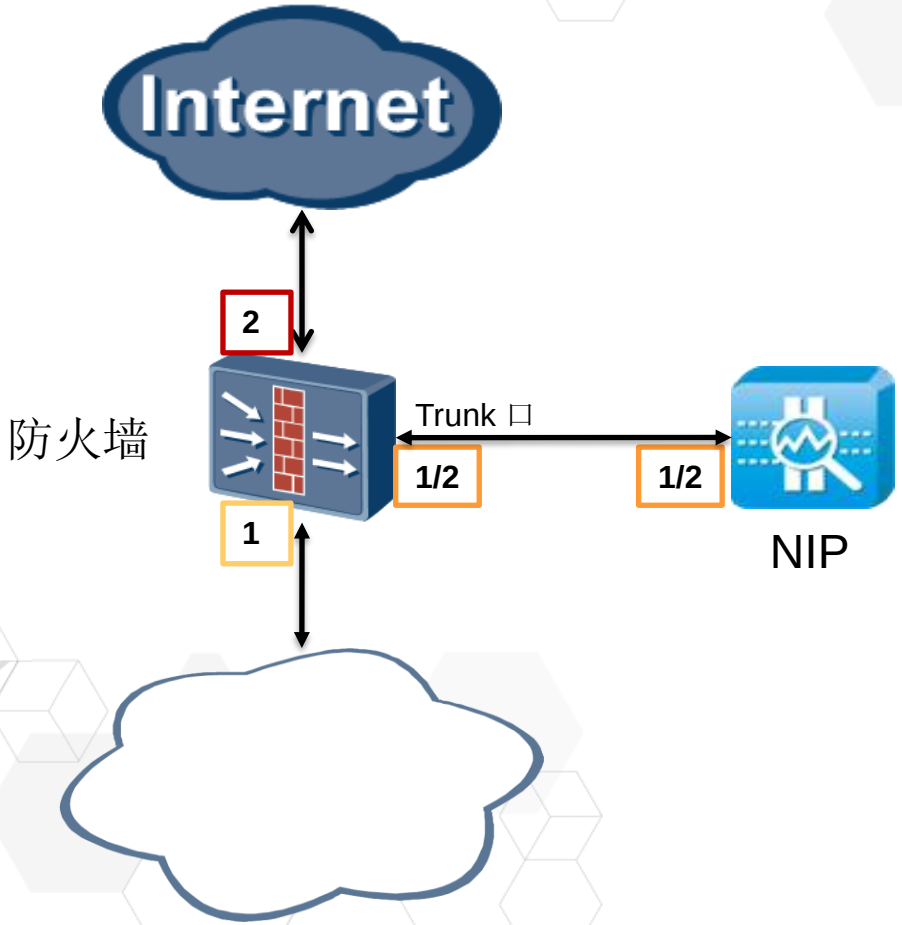
IPS 直路部署



- 自动阻断攻击
- 生成日志与报表

- 漏洞攻击签名默认开启，智能阻断
- 零配置上线
- 零设置网络参数
- 即插即用

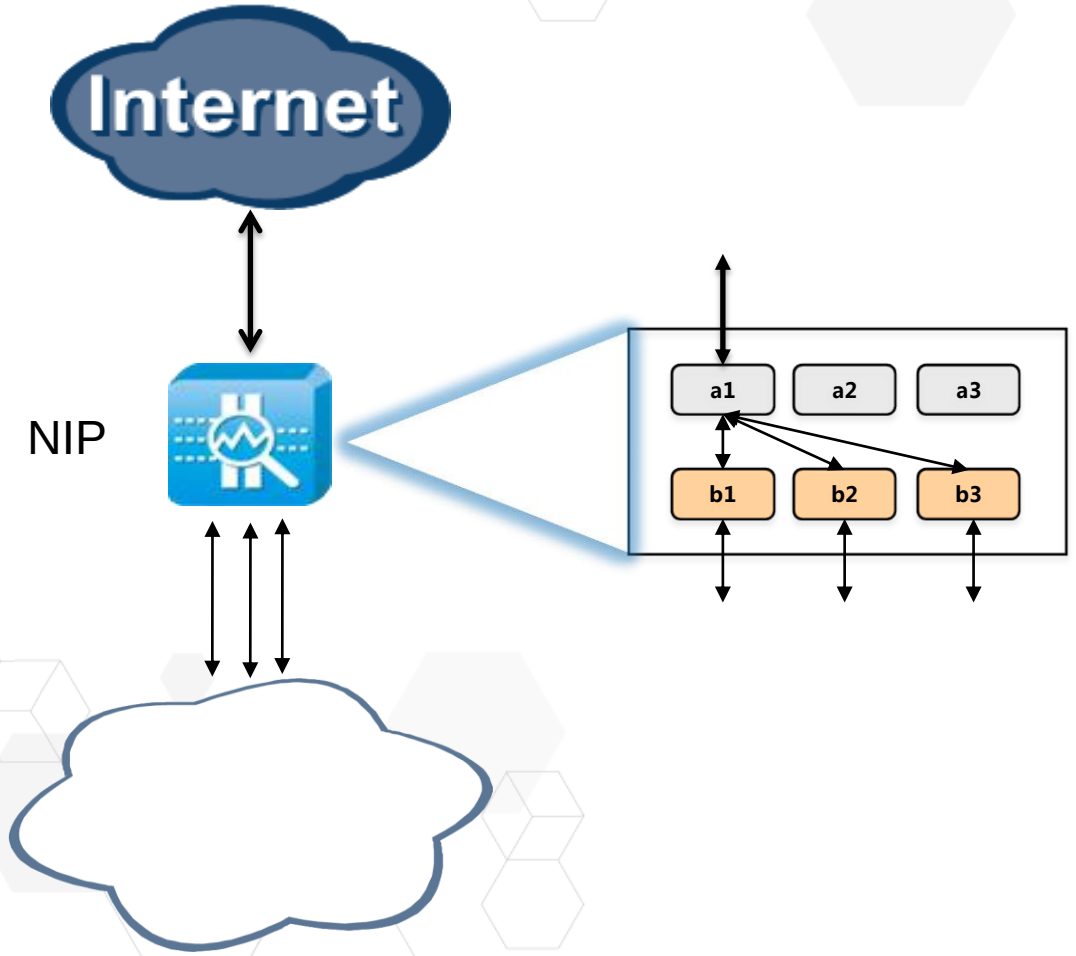
IPS 旁挂部署



VLAN 旁挂组网

- 防火墙设置两个VLAN ， VLAN1 和 VLAN2
- NIP 上通过一个物理接口，设置VLAN转换对：VLAN1 与 VLAN2 标签互换
- 通过防火墙VLAN 1接口上行的流量会由右侧Trunk口发给NIP ， NIP完成入侵检测后把VLAN1的标签换成VLAN2标签返回给防火墙，再发到Internet。
- Internet 返回的流量路则路径相反
- NIP 支持基于VLAN配置安全策略及记录日志信息

接口对基于MAC地址的报文交换

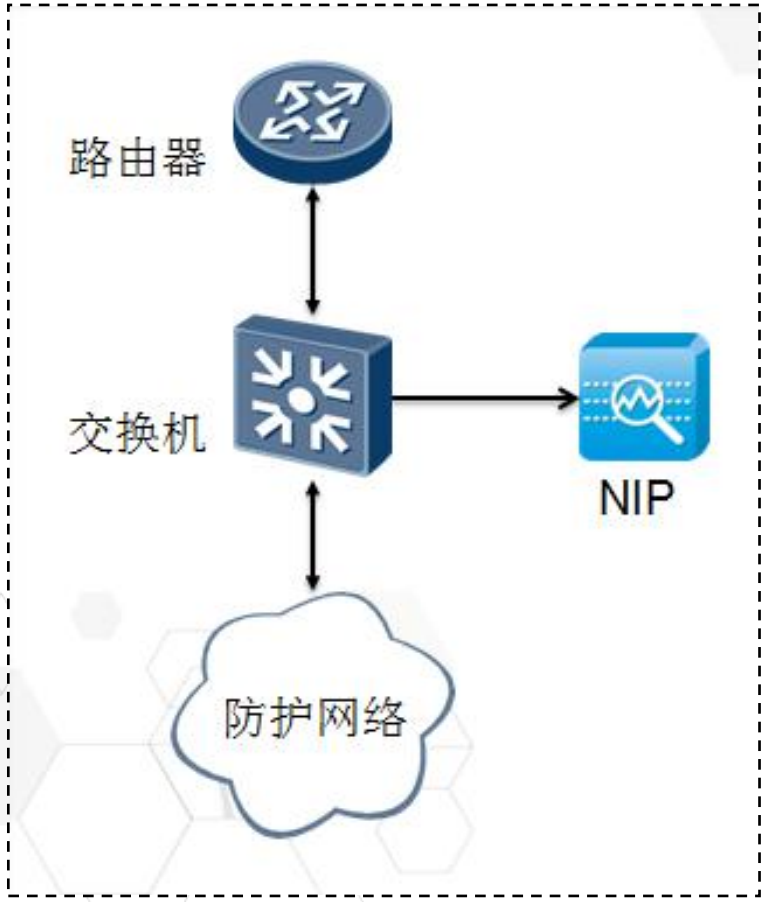


一对多报文转发

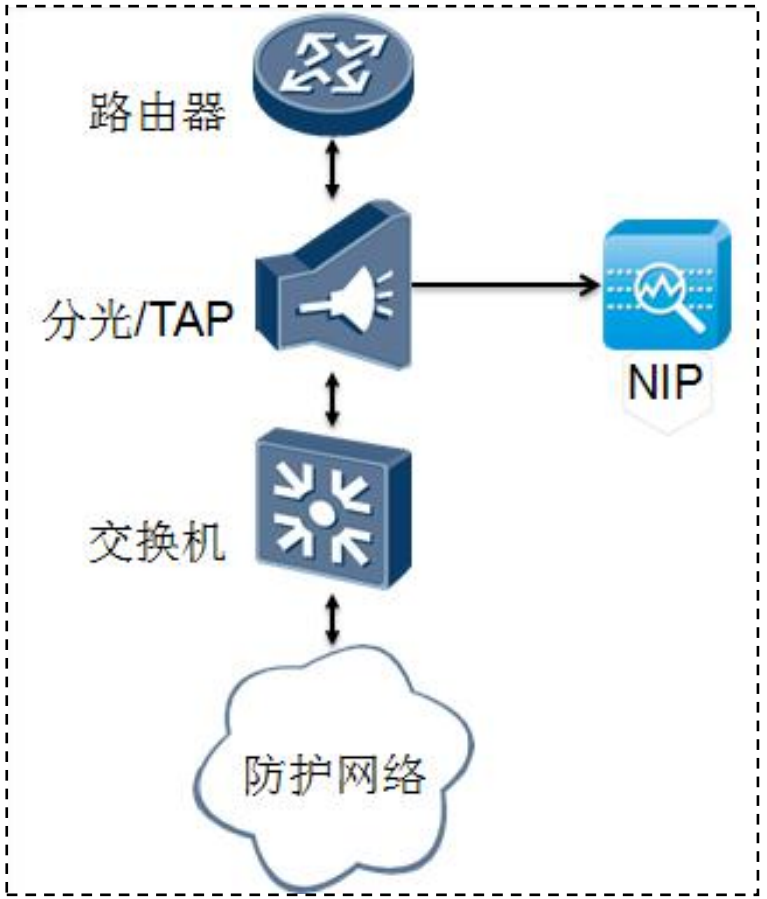
- 把接口对a1b1, a2b2, a3b3接口对绑定为一个逻辑接口对，NIP支持报文从物理接口a1进来的流量基于MAC地址学习自动选路从b1, b2或者b3物理接口转发出去；实现一个物理接口对应多个物理接口的报文转发功能
- 系统默认a1和b1为接口对，a2和b2为接口对，其他接口以此类推

IDS 旁路部署

SPAN 接口镜像流量



分光器或TAP设备拷贝分流



NIP产品价值

保护客户端

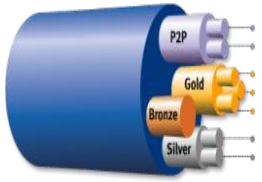
- 客户端应用防护
- 恶意软件防护

保护服务器

- 服务器漏洞防护
- Web应用防护
- 恶意软件防护
- DDOS防护

IPS
核心价值

保护带宽性能



- 应用带宽管理

保护基础架构

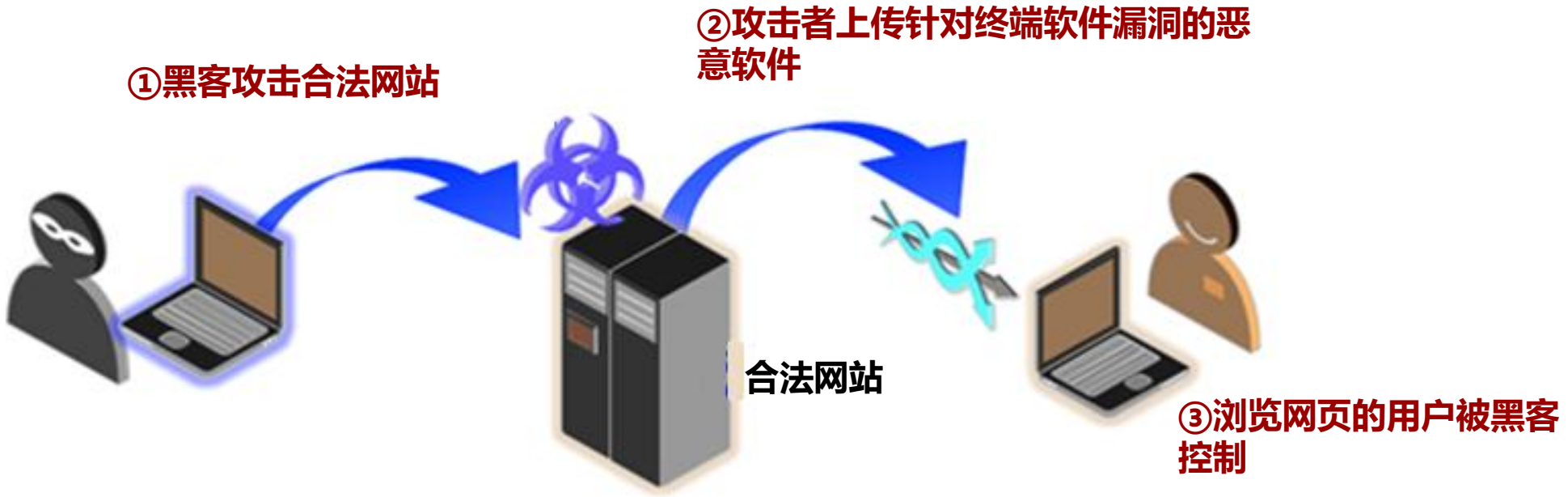
- DNS、交换路由设备漏洞防护
- DDOS防护

服务器漏洞防护 | **客户端应用防护** | **WEB应用防护** | **带宽管理** | **恶意软件防护** | **DDOS防护**

保护服务器

攻击前期	• 网络扫描 • 漏洞扫描	→	• 基于网络异常发现网络扫描 • 基于行为特征发现漏扫工具	
攻击中期	• 漏洞攻击 • Web应用攻击 • DOS攻击 • 暴力破解	→	• 虚拟补丁技术检测漏洞攻击 • Web应用防护 • 完整的DOS防御 • 基于行为检测发现暴力破解	
攻击后期	• 种植恶意软件 • 操控被攻击设备	→	• 检测恶意软件并阻断 • 检测控制、外传流量	← • 外传数据信息 • 成为傀儡主机

保护客户端



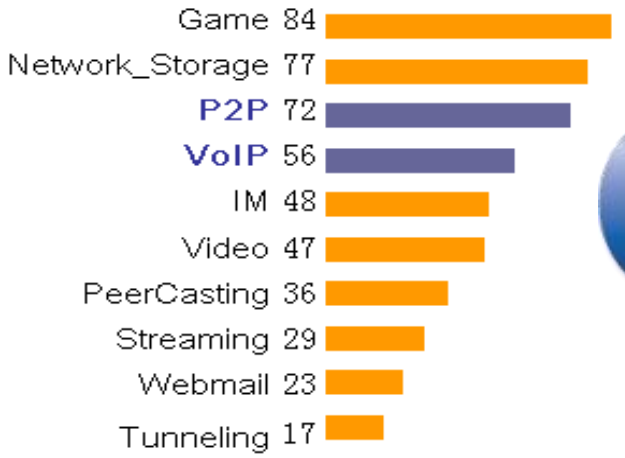
- 浏览器及其插件（Java、ActiveX等）的安全防护；
- PDF、Word、Flash、AVI等文件层的攻击防护；
- 木马、蠕虫及对操作系统的攻击防护；
- URL 关键字过滤

保护基础设施

- 基于虚拟补丁技术，对基础网络设备的漏洞进行防护；
- 综合7种流量检测技术，对各种网络DOS、应用DOS（针对DNS、HTTP、SIP的基础服务）提供整体防护；
- 提供流量自学习功能，保障对各种异常流量攻击的准确检测；

保护带宽性能

- **支持协议1200+**
- **支持热门加密P2P协议**
- **定制化需求的快速响应能力**



有效保障业务带宽，提高企业IT治理水平：

- 对P2P、流媒体等应用带宽控制，保障网络资源有效使用；
- 限制使用IM、游戏、股票等应用，保障工作效率；
- Web Mail、在线存储以及隧道传输等控制，防止机构内部文件非法外传；
- 基于IP地址的限流

威胁防护全面

服务器攻击检测

- 防止对HTTP、FTP、DNS、Mail等服务器的各种攻击：缓冲去溢出、系统或服务漏洞攻击、暴力破解等
- 文件型病毒扫描检测

客户端攻击检测

- 针对客户日常应用，如：Office文档、PDF ,多媒体以及浏览器提供深度检测，避免客户端免成为Botnet或网马的受害者
- 文件型病毒扫描检测

Web攻击检测

- 检测Web应用相关攻击，包括Web2.0及后台数据库； 对注入攻击、跨站脚本、目录穿越等提供重点防护

网络滥用检测

- 检测P2P、视频应用，保障业务带宽
- IM、在线存储、web邮箱、网络隧道证券及游戏的访问，影响员工效率
- 基于 IP 地址带宽限流

恶意软件检测

- 蠕虫、木马、间谍软件
- 僵尸网络
- 广告软件等
- 文件型病毒扫描检测

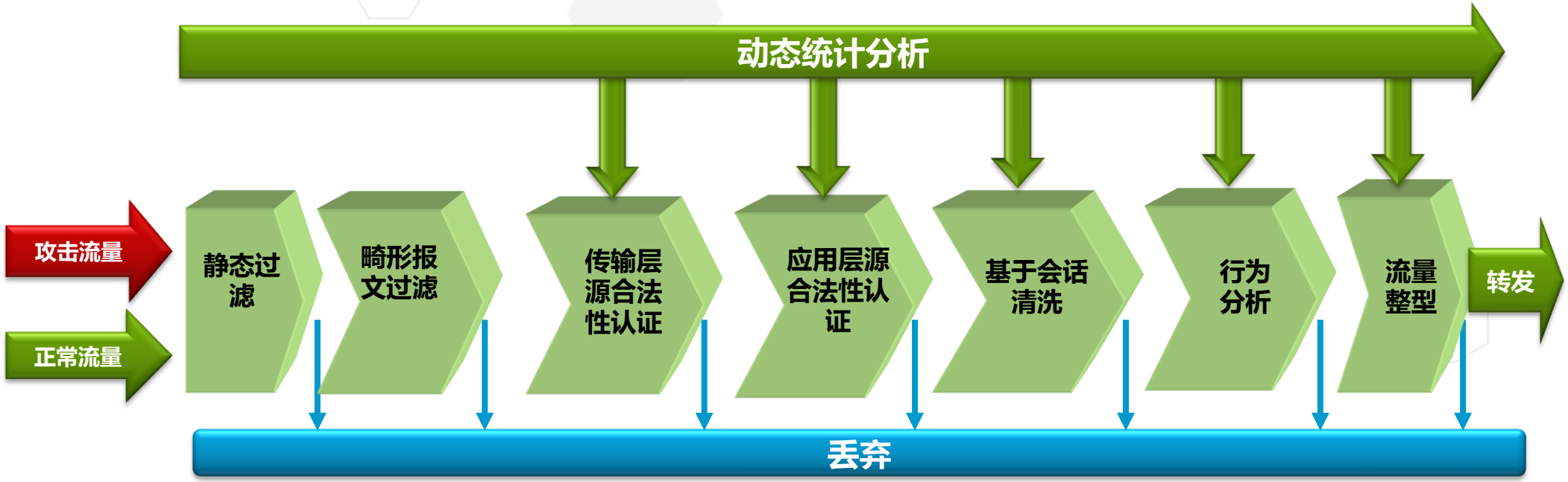
DDOS检测

- 针对网络流量的DoS
- 针对应用服务的DoS
- 针对操作系统的DoS
- 扫描探测

检测技术全面

检测技术	用户价值
协议智能识别	保障对非标准端口应用的检测
数据包及流重组、高级逃避检测	防止逃避技术造成的漏报
应用协议还原及文件还原	覆盖到文件级别的恶意威胁
攻击特征检测	对已知攻击方式或软件的检测
基于漏洞的检测	对已知漏洞及对应不同工具的检测
基于攻击原理的启发式检测	对未知漏洞和攻击的检测
网络行为/应用协议异常检测	对DoS、未知漏洞、滥用的检测

L2-L7层DDOS 全方位抵御



- 流量自学习能力；
- 抵御应用层DDOS：Web、DNS、VoIP等；

网络流量自学习

通过网络流量基线学习，精确的得到正常业务的流量阈值，防止人工配置流量异常参数引起的错误

IPv6 入侵检测

应用场景

- 校园网及运营商，适应未来网络的发展

安全策略

- 支持基于IPv6 地址设置安全检测策略

检测特性

- 支持IPv6 报文检测，IPv4 over IPv6隧道及IPv6 over IPv4隧道报文检测

日志报表

- 支持记录IPv6地址，对于隧道协议的入侵检测结果，记录内层报文的有效IP地址

性能指标

- 对IPv6报文的检测性能大概是IPv4报文检测性能的80%

IPv6管理

- 当前版本不支持通过IPv6地址对设备进行管理

NIP 版本演变及规划

V1R1C01 (在售)

IPS/IDS

应用识别

Anti-DDoS

V1R2C00 (13年4月)

万兆检测能力

IPv6报文及相关隧道检测

基于IP地址的限流

反病毒及URL关键字过滤

基于VLAN安全策略等

V1R2C10 (13年9月)

加强虚拟化特性

适应更多应用场景

V2R1 (14年7月)

感知能力：应用、漏洞、用户、Geo

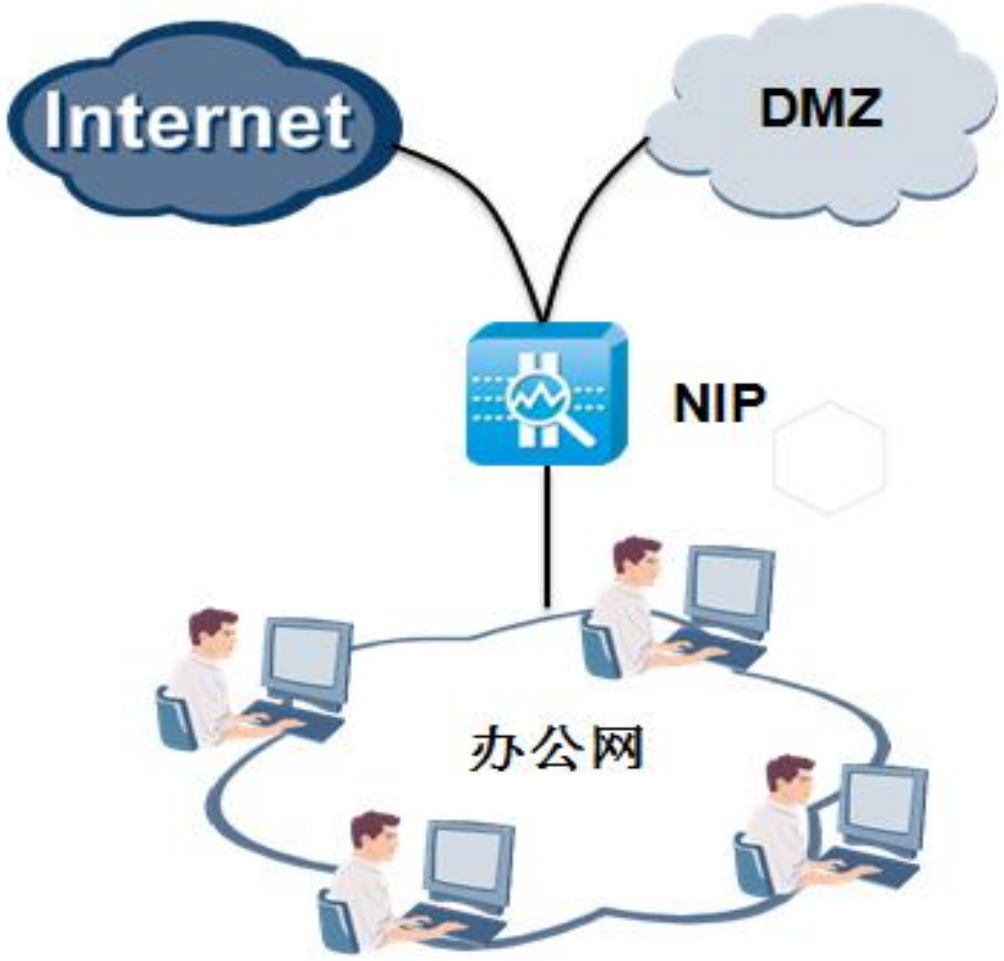
Web应用防护

目录

应用场景介绍


企业办公网出口
客户端安全防护及管理
企业 DMZ 区域出口
服务器安全及DDoS攻击防护
企业内网安全监控
安全事件记录及审计
运营商 IDC 出口
高流量场景，服务器安全防护、检测及审计
运营商 BOSS 网络出口
网管网及相关服务器系统安全检测及审计

企业办公网 Internet 出口



连接网络

- 连接 Internet，连接DMZ

主要业务

- Web访问、邮件、IM通信、文件传输等

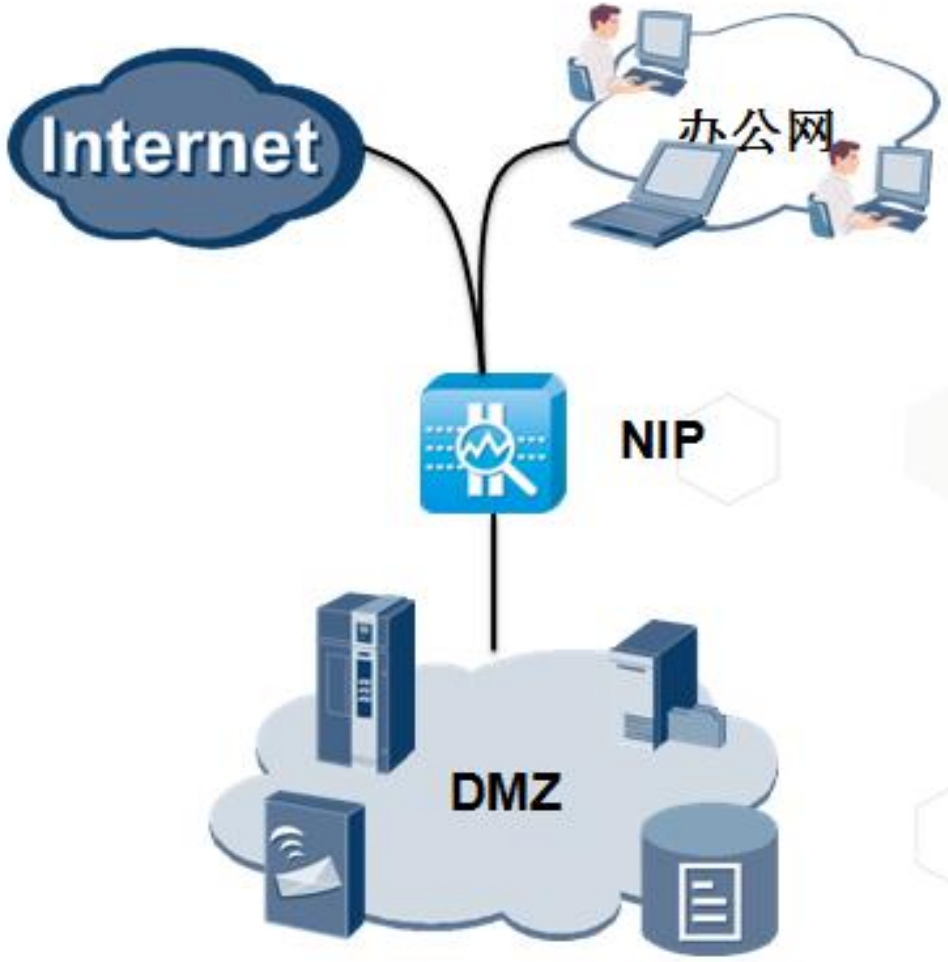
安全关注点

- 来自 Internet 的威胁传播、阻止对DMZ发起的威胁攻击
- 限制与业务无关的应用及URL过滤

办公网出口威胁防护重点

安全威胁	防护重点	安全策略
• 普通办公网用户访问Internet，直接面对 Internet上的各种威胁，中间缺少应用层的安全防护； • 终端主机应用种类繁多，版本也多，难免存在各种安全漏洞； • 一般普通用户网络安全知识有限，主机容易被远程入侵并控制，成为攻击跳板，对企业构成信誉风险；	• 应用层威胁的全面检测及实时阻断，并生成日志记录； • 基于企业网络访问策略，基于时间段针对非核心业务流量采取限流或限制使用；	• 应用系统默认的通用安全策略，避免用户因没能及时升级软件版本或安装补丁而导致的入侵； • 防止已遭入侵的用户成为攻击的跳板（僵尸主机）； • 通过合理的网络应用策略，优化企业整体办公环境，提高办公效率；

企业 DMZ 区域出口



连接网络

- 连接 Internet，连接内部网络

主要业务

- 企业业务服务器、web服务器、邮件服务器、文件服务器等

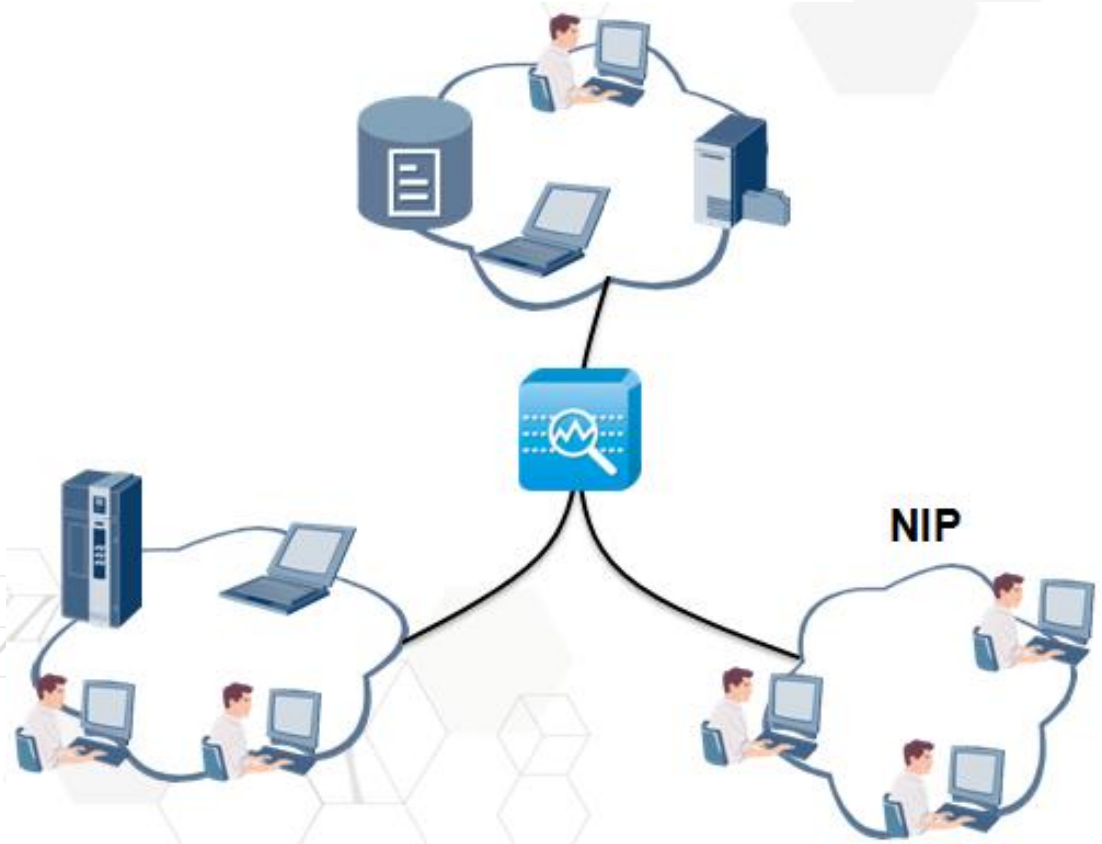
安全关注点

- 来自 Internet 的威胁传播、来自内网的安全威胁
- 文件上传限制

企业 DMZ 区域出口威胁防护重点

安全威胁	防护重点	安全策略
• DMZ 接收来自 Internet 用户及内网用户的访问，面临 Internet 的各种入侵威胁，同时内网用户对DMZ有一定的了解，可能还面对内网有针对性的入侵； • DMZ 向 Internet 提供访问接口，可能遭受 DDoS 攻击； • 如果存在文件上传操作，还会面临文件型病毒的传播	• 保护 DMZ 区域服务器免遭入侵； • 开启 Anti-DDoS 功能保护有限的网络带宽及服务器能力； • 基于业务情况确定是否开启 Anti-Virus 功能；	• 根据业务类型优化入侵防护规则策略，删除不必要的检测签名规则； • 开启 Anti-DDoS 自学习模式，实现对 DDoS 攻击的智能防护； • 如果提供文件上传业务，可以考虑开启 Anti-Virus 功能，但对设备性能有一定影响

企业内网安全监控



连接网络

- 内部网络不同网段间的互联

主要业务

- 不同内部网络区域间的业务访问及数据传输

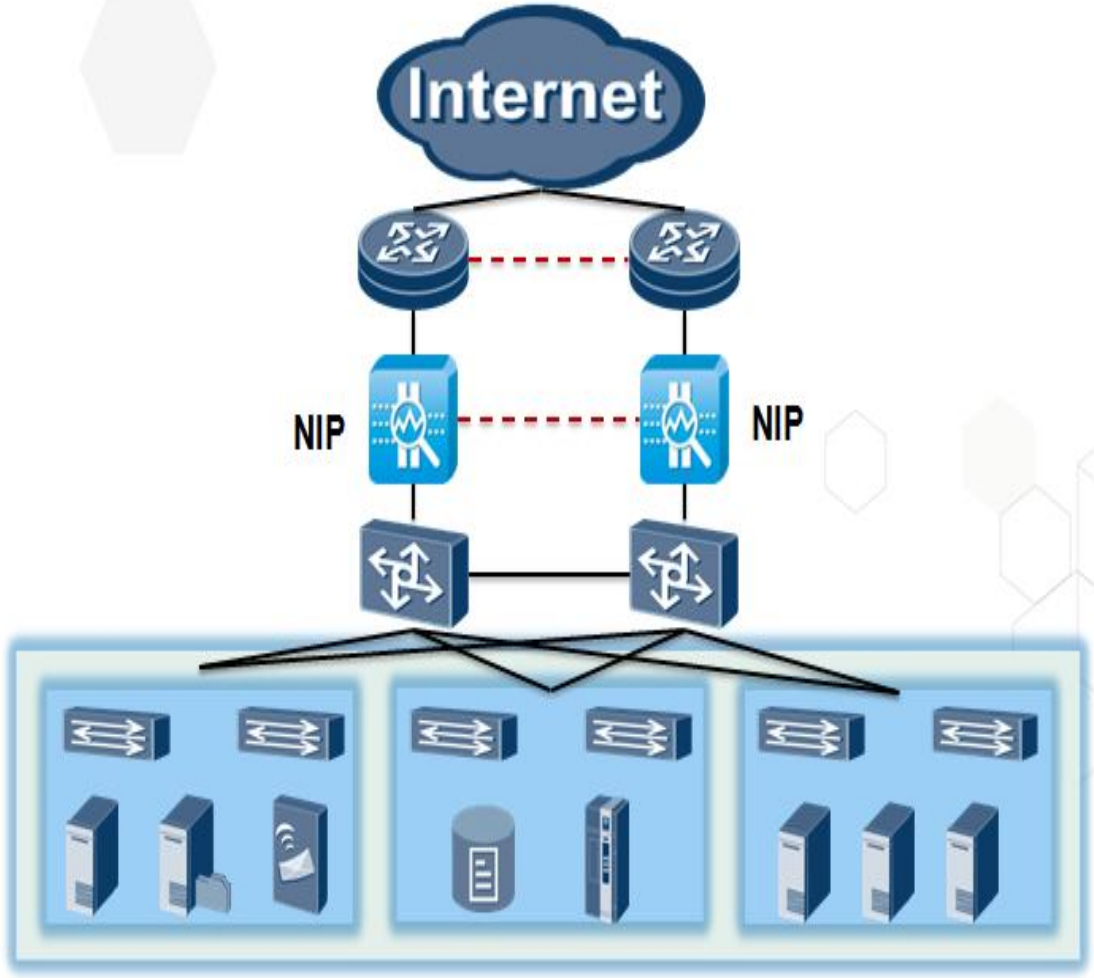
安全关注点

- 威胁在内网的扩散及不合规行为
- 基于IP地址限流

企业内网安全监控重点

安全威胁	防护重点	安全策略
• 大企业内部一般都划分为多个业务区域，不同区域间的业务不同，用户权限不同，安全级别也有所区别，个区域间的直接互联可能导致威胁在各个网络间的扩散，如蠕虫； • 已被入侵主机可能主动攻击其他系统，甚至成为外网的傀儡主机窃取内部数据；	• 有效隔离网络威胁，如蠕虫等在内网中扩散； • 实现对个网络区域的安全监控，生成详细的安全检测日志报表； • 限制与企业业务无关的流量占用内部带宽，影响正常业务的进展； • 对不同网段间的文件传输实行反病毒检测；	• 最大化入侵检测安全策略，实现内网安全的全面监控； • 定时生成详细的日志报表，实现内网安全监控并及时调整安全策略，隔离高威胁级别主机； • 对可能的文件传输业务实行反病毒检测；

运营商 IDC 出口



连接网络

- 运营商网络及Internet

主要业务

- 运营商自身及企业等用户租用的各类应用服务器

安全关注点

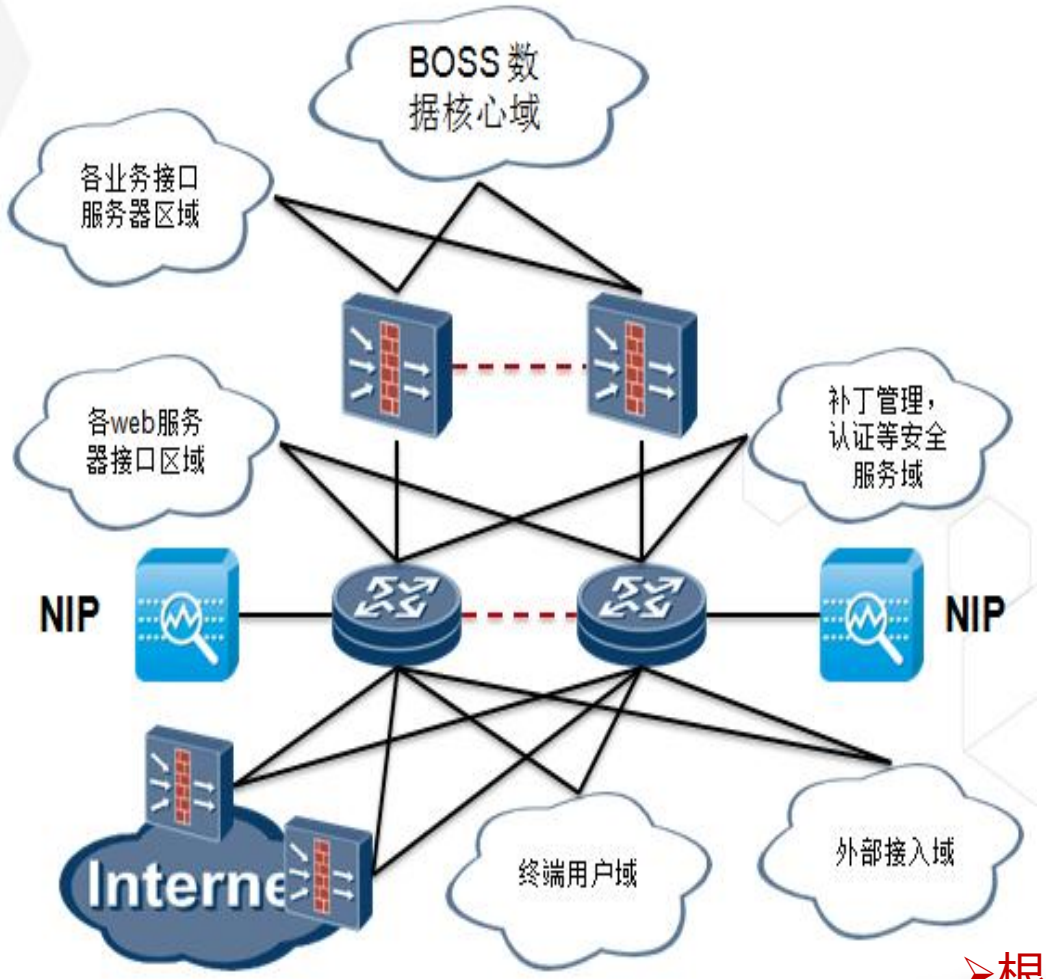
- 服务器的安全及业务的高可靠性
- 基于单IP的流量限流

➢可考虑作为IDS设备旁挂在核心交换机上

运营商 IDC 出口防护重点

安全威胁	防护重点	安全策略
• IDC 的访问用户复杂，IDC 内服务器多而杂，系统漏洞几乎无法感知，用户访问意图无从知晓； • Internet 连接带来直接的网络安全威胁，如蠕虫的扩散，病毒的自行传播； • 网络带宽出口大，容易发起大流量的DDoS攻击； • IDC 租用服务器安全能力各异，可能成为傀儡主机对外发起攻击；	• 全面检测防护来自 Internet 的网络应用层威胁，组织非法用户入侵服务器； • 基于系统漏洞提供入侵威胁保护，阻止蠕虫、网络病毒类威胁传播到IDC 内部； • 实时监控网络流量，实现 DDoS 攻击防护； • 发现 IDC 内部傀儡主机，及时阻断远程控制威胁；	• 优化安全检测策略，专注服务器端的安全防护； • 开启DDoS攻击防护及自学习功能，实现DDoS的智能防护； • 详细记录入侵检测日志，定时生成安全报告，协助管理员调整安全策略；

运营商 BOSS 网络出口



连接网络

- 运营商内部业务网络

主要业务

- 各类计费及网络系统

安全关注点

- 服务器的安全及业务的高可靠性
- 识别分析网络内流量模型

➢根据实际需求，可考虑作为IPS串联在核心交换机下方的组网

运营商 BOSS 网络出口防护重点

安全威胁	防护重点	安全策略
• BOSS 网络业务多而且都是关键业务，内网的网络病毒、蠕虫传播将对业务系统造成巨大的影响； • 业务系统中存储许多关键数据，一旦被入侵修改或损毁影响巨大； • BOSS 网络内不应用有非业务数据在运行，从而影响业务的正常访问；	• 实现 BOSS 网络的全面威胁监控并记录详细日志； • 发现高威胁级别主机及时进行告警并清除； • 识别及限制网络内非关键业务流量，如IM, P2P等；	• 开启全方位的入侵检测策略，及时进行告警或阻断非法连接； • 全面记录检测日志，定时生成日志安全报告以便后续的审计； • 实时分析识别内网流量类型，限制非关键业务流量；

哪些场景与您目前的情况类似？或者那些场景是您目前碰到的主要需求？

接下来你最希望对哪种应用场景进一步了解呢？

您对今天交流的哪些内容感兴趣? 还想要了解什么内容?

Q & A

目录

华为 NIP 产品 IPS 系列

高端百兆系列

NIP2050

NIP2100

分销型号

NIP2130

NIP2150

NIP2200

基础千兆

NIP5100

中端千兆

NIP5200

高端千兆

NIP5500

基础万兆

型号	NIP2050	NIP2100	NIP2130	NIP2150	NIP2200	NIP5100	NIP5200	NIP5500
吞吐量	600M	800M	800M	1.2G	1.5G	3G	6G	20G

华为 NIP 产品 IDS 系列

高端百兆系列

NIP2050D

NIP2100D

分销型号

NIP2130D

NIP2150D

NIP2200D

基础千兆

NIP5100D

中端千兆

NIP5200D

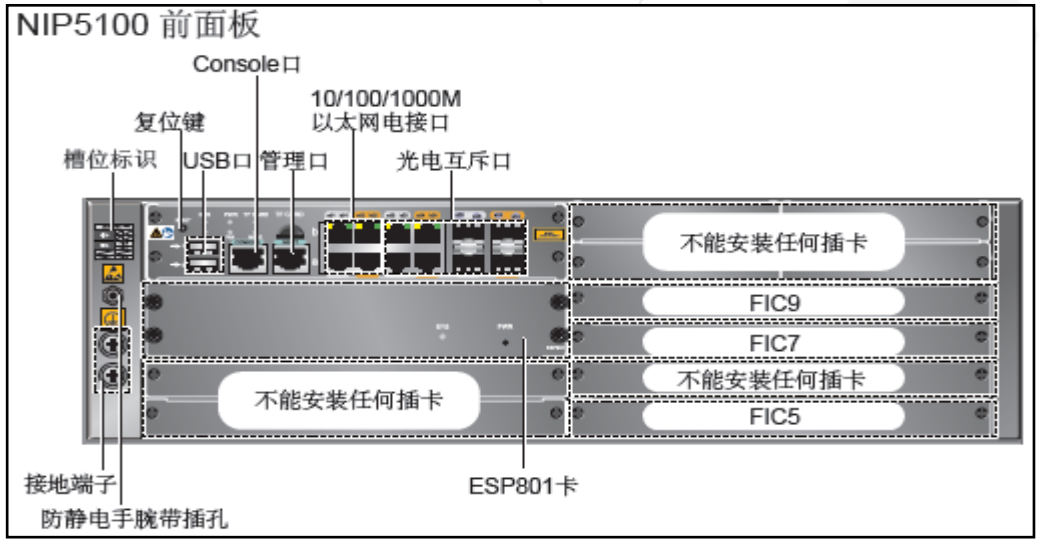
高端千兆

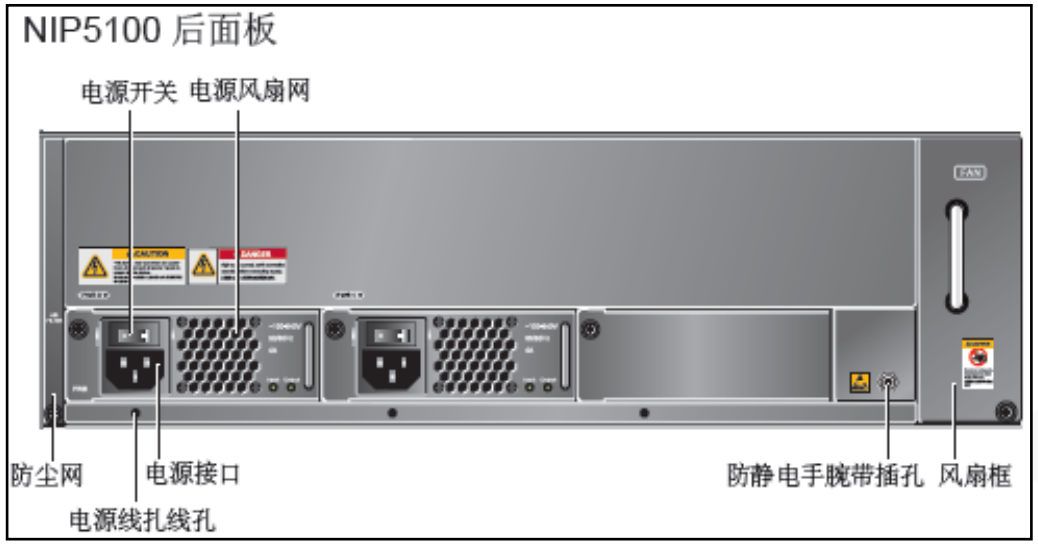
NIP5500D

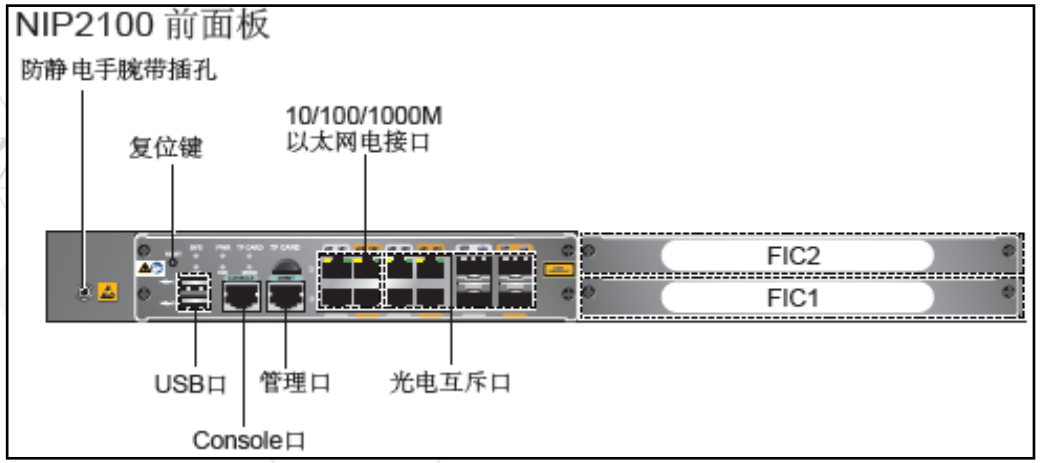
基础万兆

型号	NIP2050D	NIP2100D	NIP2130D	NIP2150D	NIP2200D	NIP5100D	NIP5200D	NIP5500D
吞吐量	600M	800M	800M	1.2G	1.5G	3G	6G	20G

设备外观

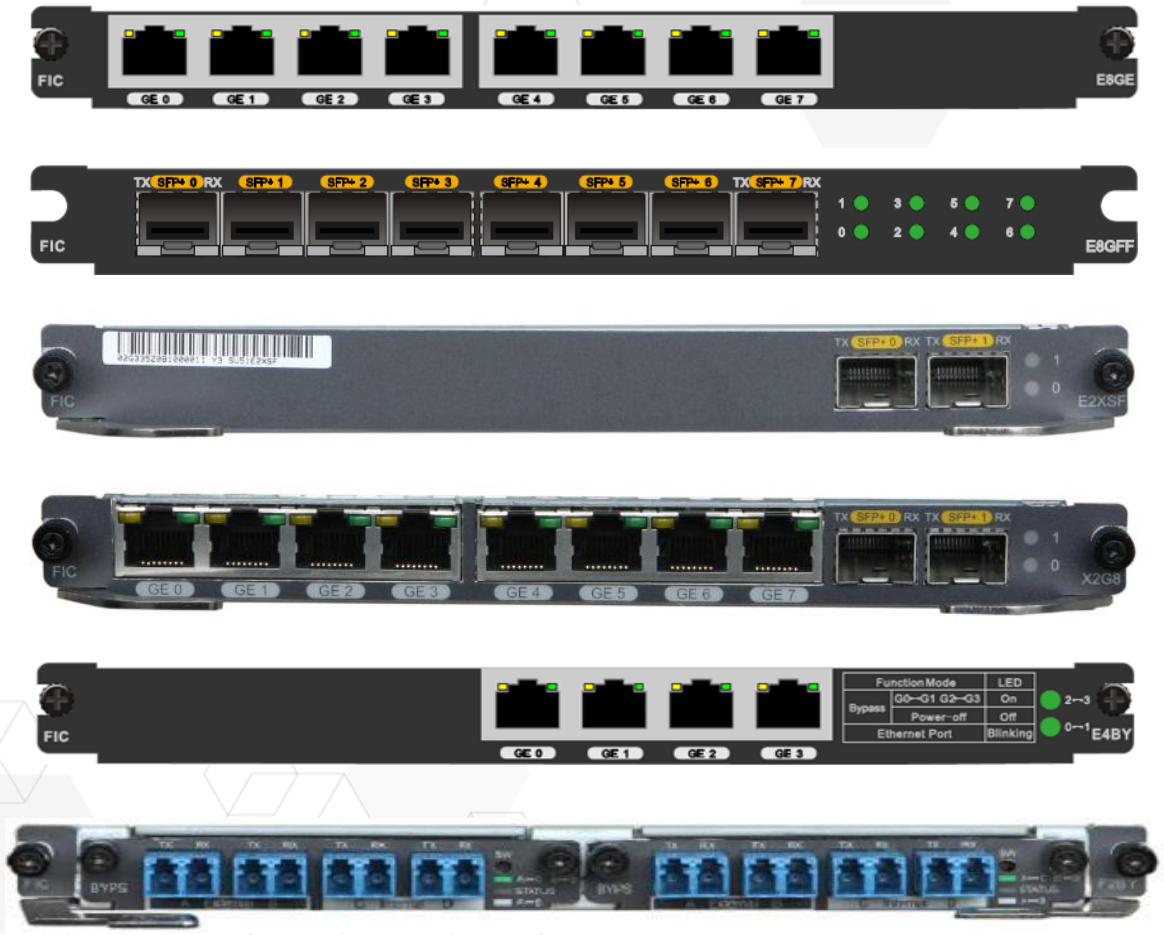






说明：
- ESP 卡用于业务加速处理，出厂时默认固定安装在设备插槽上，不允许插拔
- NIP 暂不支持位于管理口上边的Micro-SD 卡接口
- 每个光电互斥接口由一个光接口和一个电接口组成，同一时刻只能使用一种接口，缺省电接口生效。

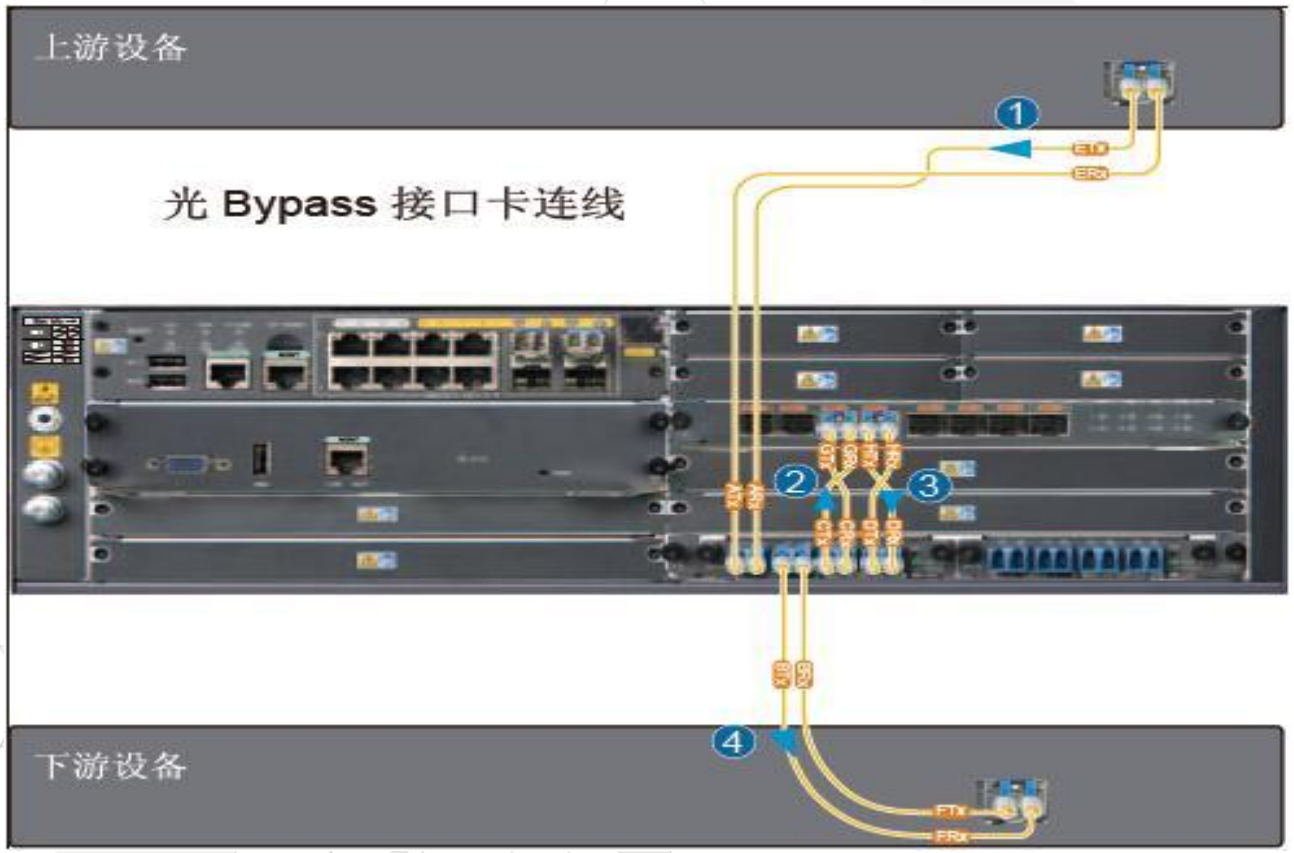
扩展接口板

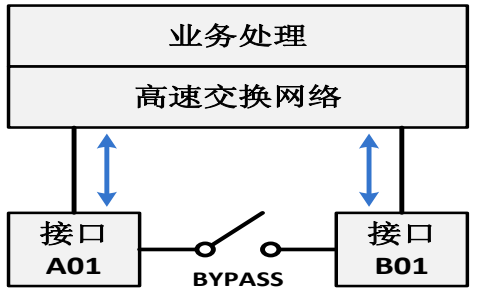


- 8*GE电接口扩展卡
- 8*GE光接口扩展卡
- 2*10GE接口扩展卡
- 8*GE+2*10GE接口扩展卡 （NIP5500不支持）
- 4*GE电接口bypass接口卡
- 两路光接口bypass接口卡

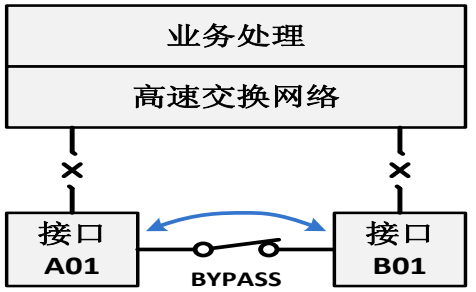
注：万兆口接口卡只有NIP5100/5200型号支持

光bypass卡的配置





正常工作中



系统异常触发 BYPASS

- 光bypass卡需另外配置
- 4 接口的光bypass卡保护一路数据
- 正常数据流向: **1 - 2 - 3 - 4**
- 数据bypass流向: **1 - 4**

异常情况包括：主机软件系统异常，系统硬件故障，设备掉电等

NIP 亮点

独立的IPS设备

- 聚焦核心功能，而不是一款防火墙设备的二次开发来集成IPS特性
- 真实高效的入侵威胁检测能力，而不是网路吞吐能力

开创性的软硬件架构

- 基于网络分层的软件分离式处理
- 针对特定处理流程的硬件加速

高效的检测及防护能力

- 支持强大的客户端及服务器端安全防护，支持带宽管理及保障

强大的安全研发能力，提供及时的安全升级支持

- 实时跟踪、分析现网安全威胁，应用漏洞，发布签名包；设备支持多种升级方式

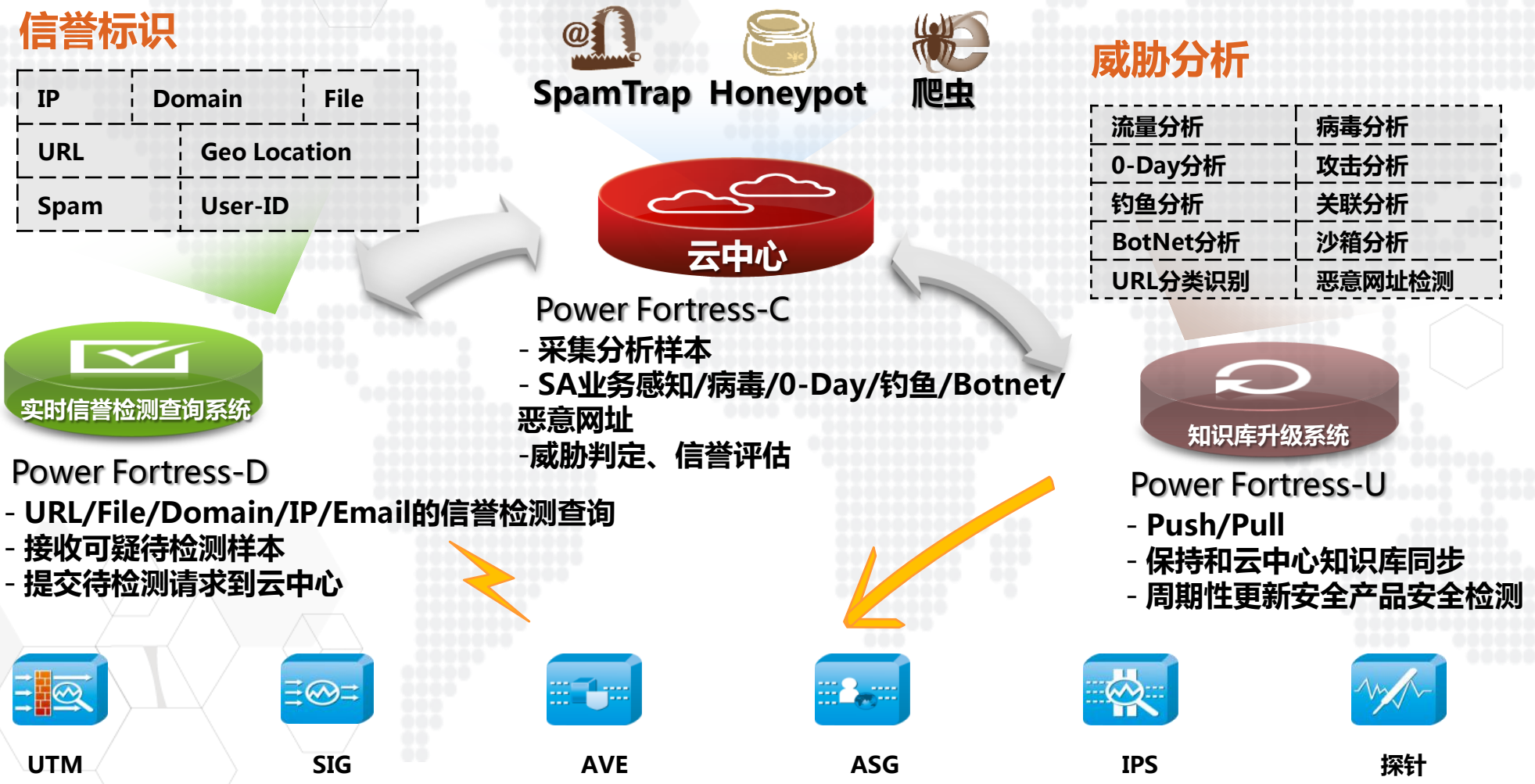
灵活的部署及配置，满足各种应用场景

- 直路部署、旁路部署、混合部署、旁挂部署

支持IPv4/IPv6 双栈协议，紧跟Internet 发展的脚步

- 支持IPv6报文、隧道解析的应用层报文检测

华为云安全系统—Power Fortress Cloud



Huawei Enterprise A Better Way