目录

1. 企业网络的安全威胁来源

【 外部威胁 】

DDoS 攻击

病毒、木马、蠕虫（不需要寄生，即不需要触发条件）等网络入侵

网络扫描

垃圾邮件，钓鱼邮件

针对 Web 服务器的攻击

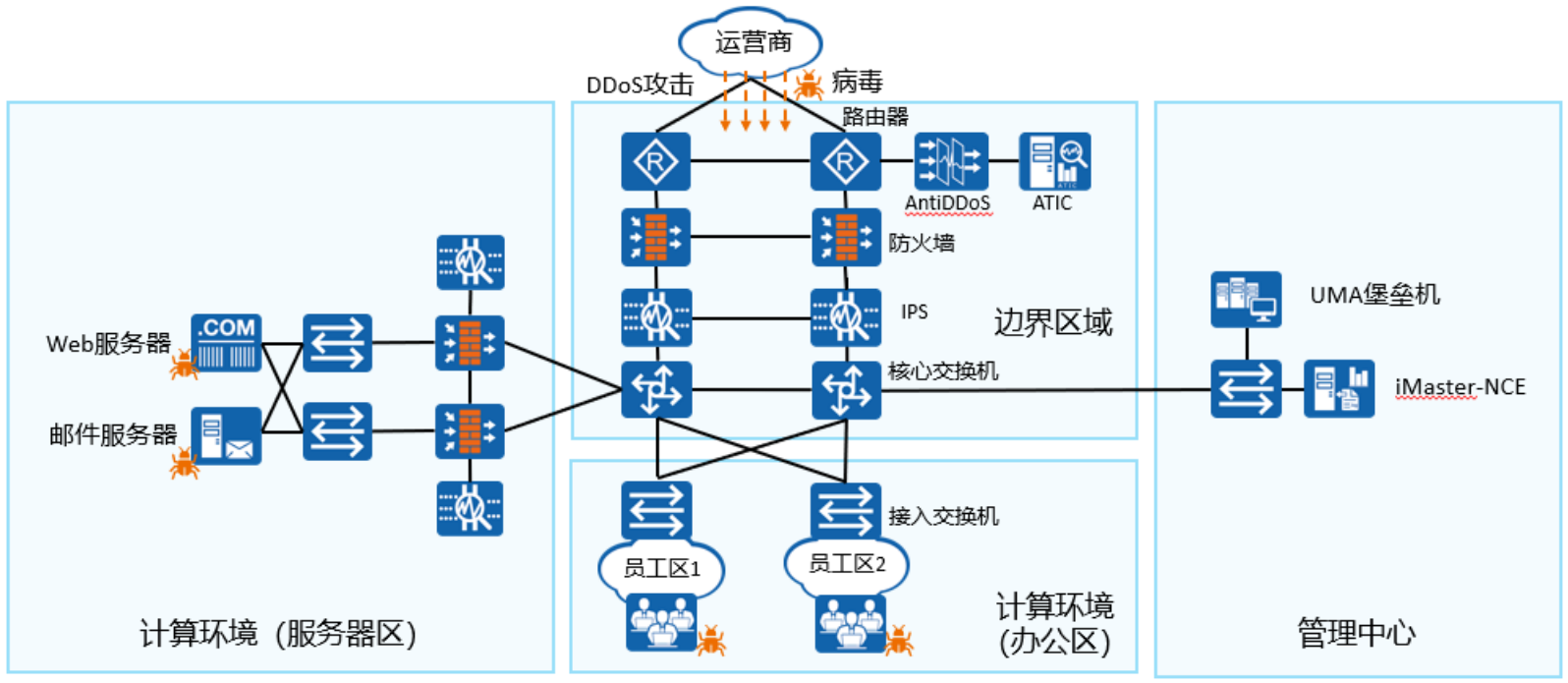
【 内部威胁 】

网络结构不可靠，网络未隔离，终端存在漏洞

员工行为不受控，信息安全违规操作，信息泄露，恶意员工，权限管理混乱，非法接入

2. 企业网络安全威胁概览

【 典型企业网络架构图 】



【 企业对安全威胁的规避措施 】

[管理方面]

制定各类安全制度、运维要求、应急流程，**以提升员工的安全意识**

定期开展安全意识培训、明确安全制度与规则

安全意识是一切防御手段的基础

比如：

培训学习

奖惩制度、将制度落实到每个人（谁负责、谁组织、谁操作）

生产例会（总结半年或每季度的安全生产事件，事情的概述、原因、教训、总结、巩固强化、启发等）

最终目的：让员工对安全制度形成肌肉记忆！

[技术方面]

针对性防范企业网络安全威胁，企业工程师会根据威胁来源，将网络划分为不同区域

{ 通信网络架构 }

具备高可靠性　　//保障业务的正常运行

部署 VPN　　//保障数据传输的机密性与完整性

{ 边界区域 }

部署 AntiDDoS 方案　　//应对 DDoS 攻击

部署防火墙设备　　//网络隔离、流量控制

部署 IPS 设备　　//防范外网的病毒、入侵

{ 计算环境 }

终端安全加固　　//防范漏洞带来的威胁

部署 IPS 设备　　//应对外网的入侵行为

部署终端 IPS 或杀毒软件　　//应对病毒入侵

{ 管理中心 }

通过堡垒机管控管理员的权限　　//降低恶意操作带来的影响，监控运维操作，做到运维过程可回溯

iMaster-NCE 管控员工权限　　//降低信息泄露的风险，同时防范非法接入

【 安全设备 】

[IPS 设备]

专业的入侵防御设备

通常部署在出口区域防火墙的后端

用于防范去往内网的安全威胁，在中大型企业中较为常见

[AntiDDoS]

专业的 DDoS 防御设备，价格昂贵

部署在防火墙之前

主要用于大型企业，如银行、互联网公司等 DDoS 重灾区

[UMA 堡垒机]

专业的运维审计设备

企业通常根据需要部署

主要用于管控管理员的操作权限及监控操作过程

[iMaster-NCE]

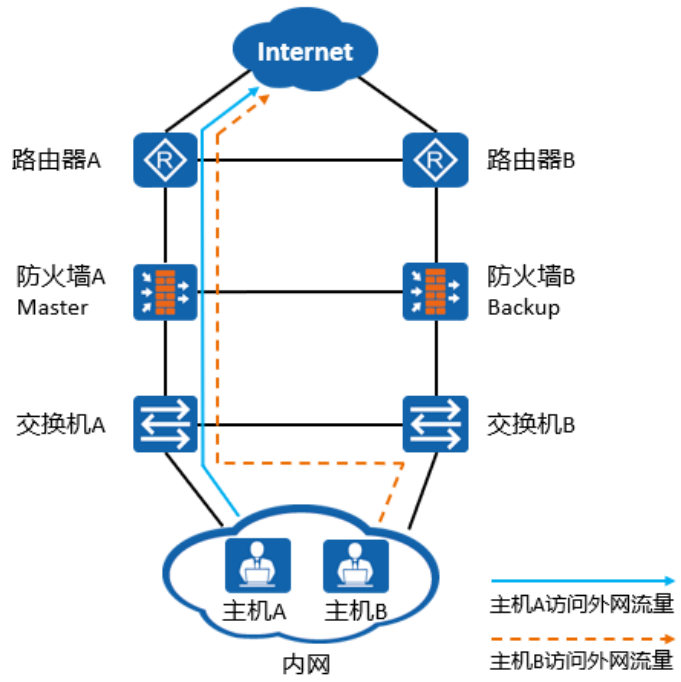
企业中常见的准入控制设备

常与交换机/防火墙组成准入控制方案

对员工进行身份认证、授权访问资源及审计上网行为

3. 通信网络架构安全需求与方案 1：网络架构可靠性

【 图示 】



【 等保要求 】

第三级等级保护（监督保护级）开始，安全通信网络部分中，网络架构要求：

提供通信线路、关键网络设备、关键计算设备的硬件冗余

【 解决方案 】

汇聚层、核心层必须考虑可靠性

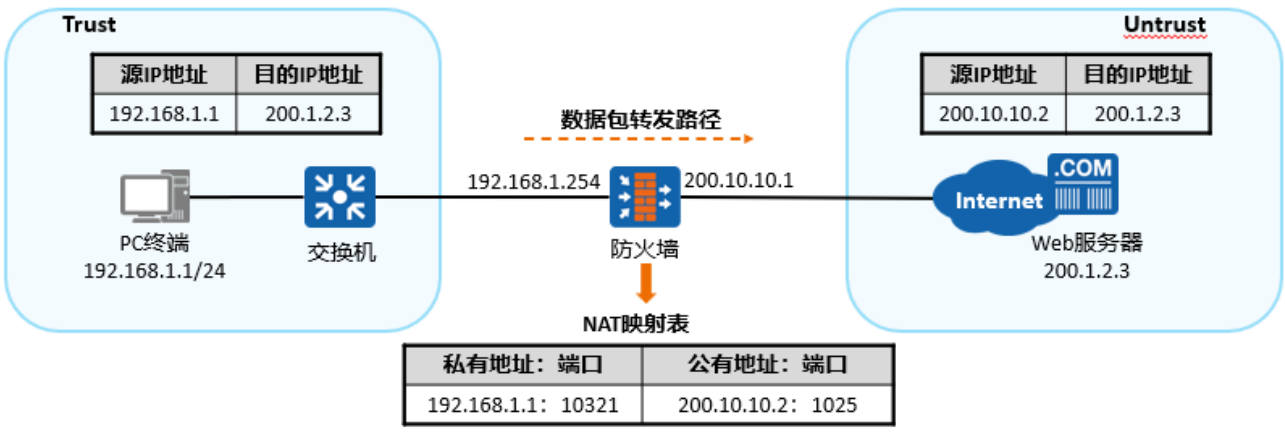
盒式设备可以通过堆叠、链路聚合，实现可靠性的需求

框式设备可以通过两块相同功能的板卡实现设备自身的可靠性（重要的板卡两块，一主一备），框式设备也可以通过 CSS、链路聚合实现可靠性，从而实现**“多级冗余”**

防火墙设备可以配置双机热备

4. 通信网络架构安全需求与方案 2：区域隔离

【 图示 】



【 解决方案 】

[背景]

企业网络资源不能直接暴露在公网中

互联网中的不法份子可能通过 IP 地址扫描或其他方式探测企业网络，便于进行下一步的攻击（**探测和扫描是攻击的前置步骤**）

[安全区域]

防火墙的基本机制，不同安全区域不能直接通信，以此起到**隔离网络**的作用

[NAT]

通过在防火墙上部署**地址转换技术，可以在一定程度上隐藏内网 IP 地址，保护内部网络**

5. 通信网络架构安全需求与方案 3：信息保密性

【 背景 】

出差员工和企业总部，企业分支和企业总部之间在不安全的 Internet 上进行数据传输时，可能存在数据被窃取或篡改的风险

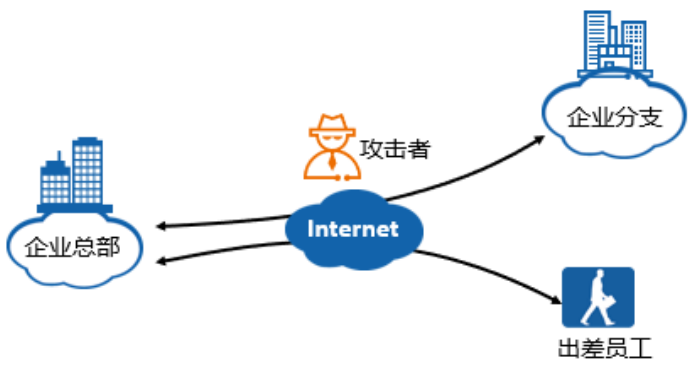
原因在于：

（1）企业数据传输本身未加密或加密程度不够

（2）中间人攻击

【 中间人攻击 】

[图示]



[简述]

指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据

使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制

在中间人攻击中，攻击者可以拦截通讯双方的通话并插入新的内容

【 解决方案 】

[VPN]

使用 VPN 技术在 Internet 上构建安全可靠的传输隧道

对于有经济实力和有高安全高可靠性要求的企业，还可以向运营商购买专线

[出差员工]

对于出差员工，可以使用 **L2TP over IPSec，SSL VPN** 等方式安全地接入公司网络

6. 区域边界安全威胁 1：DDoS 攻击

【 概念 】

指攻击者通过**控制大量僵尸主机**

向攻击目标**发送大量攻击报文**

导致被攻击目标所在的网络的**链路拥塞，系统资源耗尽**，从而无法向正常用户提供服务

【 场景 】

有些恶意竞争对手会使用 DDoS 攻击，对正常合法企业造成较大经济损失

如在购物节期间对网上购物平台发动的 DDoS 攻击

【 分类 】

[TCP Flood]

利用 TCP 协议发起的 DDoS 攻击

常见的攻击有 SYN Flood，SYN+ACK Flood，ACK Flood，FIN/RST Flood 等

[UDP Flood]

使用 UDP 协议发起的攻击

常见攻击有 UDP Flood，UDP 分片攻击等

[ICMP Flood]

利用 ICMP 协议在短时间内发送大量的 ICMP 报文导致网络瘫痪

或采用超大报文攻击导致网络链路拥塞

[HTTP Flood]

利用 HTTP 协议交互，发动 HTTP Flood，或者 HTTP 慢速攻击等

[GRE Flood]

利用 GRE 报文发动的 DDoS 攻击，利用 GRE 报文的解封装消耗攻击目标的计算资源

7. 区域边界安全威胁 2：单包攻击

【 概念 】

单包攻击不像 DDoS 攻击，通过使网络拥塞或者消耗系统资源的方式进行攻击

而是通过发送有缺陷的报文，使主机或服务器在处理报文时系统崩溃，或发送特殊控制报文、扫描类报文探测网络结构

【 分类 】

[扫描型攻击]

一种潜在的攻击行为，不具备直接的破坏行为

{ 地址扫描 }

攻击者运用 ICMP 报文探测目标地址，以确定哪些目标系统确实存活，并连接在目标网络上

{ 端口扫描 }

攻击者对端口进行扫描探测，探寻被攻击对象目前开放的端口，从而确定攻击方式

[畸形报文攻击]

攻击者通过发送大量有缺陷的报文，从而造成主机或服务器再处理这类报文时系统崩溃

[特殊报文控制类攻击]

一种潜在的攻击行为，不具备直接的破坏行为

攻击者通过发送特殊控制报文探测网络结构，为后续发起真正的攻击做准备

8. 区域边界安全威胁 3：用户行为不受控

【 概述 】

70%的信息安全事件，是由于内部员工误操作或安全意识不够引起的

【 解决方案 】

[1]

加强员工安全意识

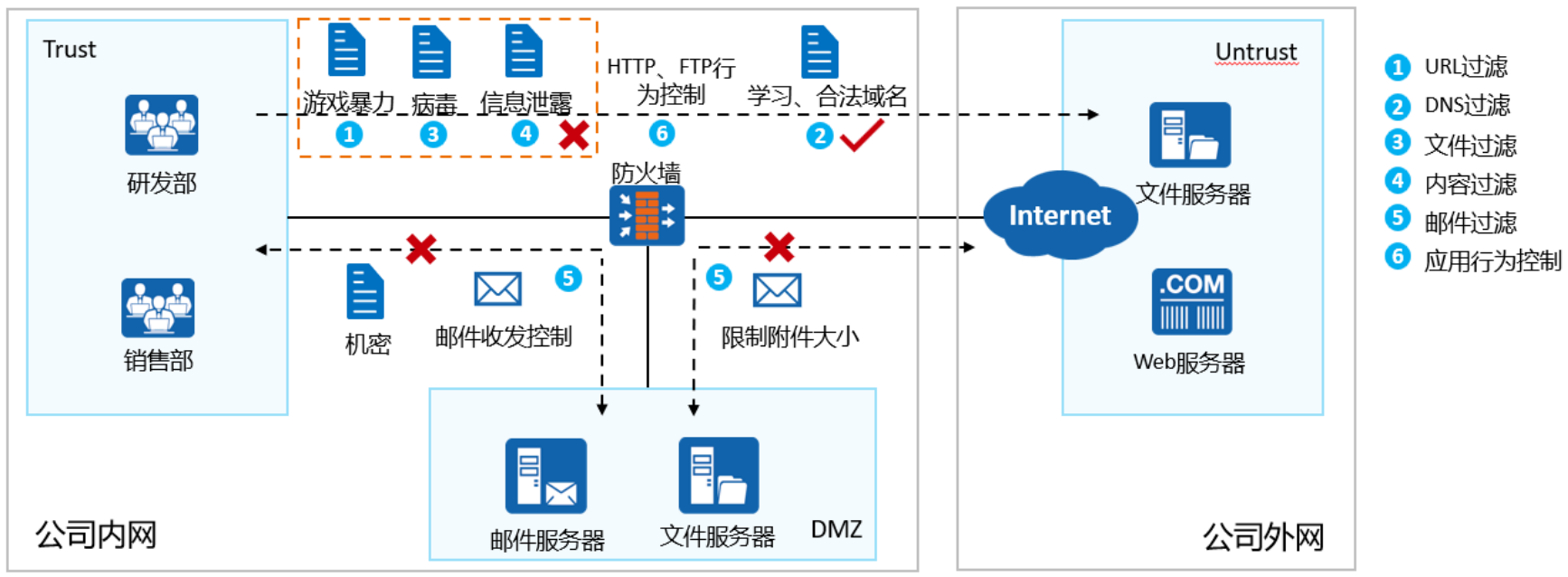
[2]

企业需要在技术层面管控员工访问外网的行为

权限——通过 **iMaster-NCE** 管控用户的访问权限

上网行为——通过防火墙的**内容过滤功能**管控用户的上网行为

【 图示 】



9. 区域边界安全威胁 4：外部网络入侵行为

【 入侵类型 1——病毒 】

可感染或附着在应用程序或文件中的恶意代码

一般通过**邮件或文件共享等协议**进行传播，威胁用户主机和网络的安全

病毒能够**自我复制，但需要通过打开受感染的文件，启用宏等手动操作才能激活**

【 入侵类型 2——SQL 注入 】

通过构建特殊的输入作为参数传入 Web 应用程序，而这些输入大都是 SQL 语法里的一些组合

通过**破坏 SQL 语句的原始逻辑**，进而执行攻击者所希望的操作

SQL 注入漏洞属于高危型 Web 漏洞

【 入侵类型 3——DDoS 攻击 】

通过发出海量数据包，造成目标设备负载过高

最终导致网络带宽或是设备资源耗尽

【 解决方案——入侵防御安全防范 】

对所有通过的报文进行检测分析，并实时决定允许通过或阻断

FW/IPS 上具备入侵防御功能模块，**该模块通过将流经 FW/IP 设备的流量与加载的签名库做对比，并根据危险程度进行相应处理**

如果流量和签名库匹配，就认为是某种攻击

签名库是签名的集合