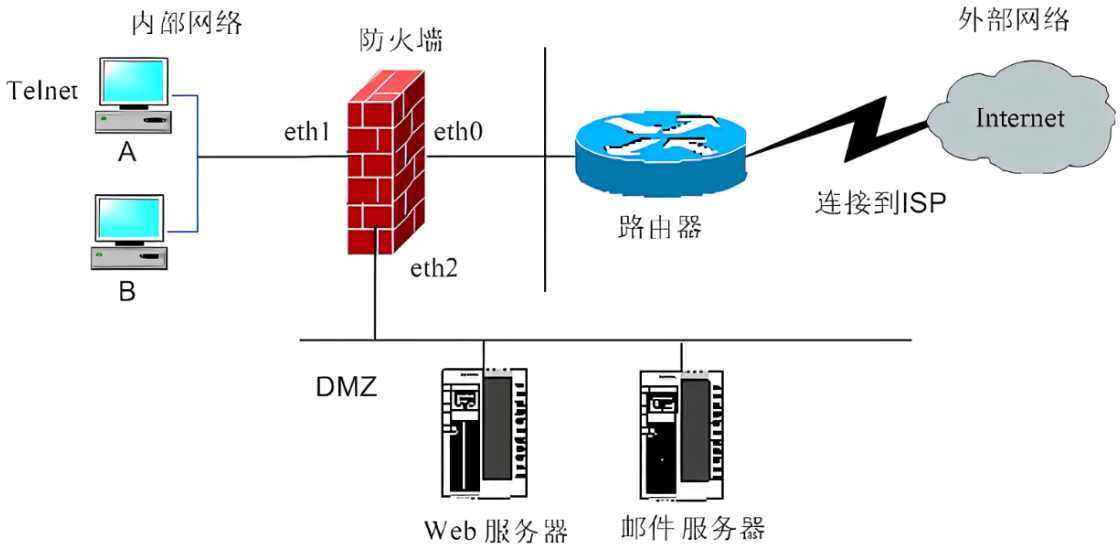
一、防火墙

1、介绍

```
# 简介
    防火墙（Firewall）是一组用于监控入站和出站网络流量的网络安全设备，可基于一组定义的安全规则来决定是允许还是阻止特定流量。
```

```
# 局限
    1、不能解决来自内部网络的攻击和安全问题。
    2、不能防止策略配置不当或错误配置引起的安全威胁。
    3、不能防止受病毒感染的文件的传输。
    4、不能防止数据驱动式的攻击。
```

2、拓扑图



3、常见品牌

```
    1、华为
    2、网域
    3、H3C
    4、深信服
    5、飞塔
    6、天融信
    7、山石网科
    8、思科
    9、绿盟科技
    10、锐捷网络
```

4、历史漏洞

```
    CVE-2022-30525：Zyxel 防火墙远程命令注入
```

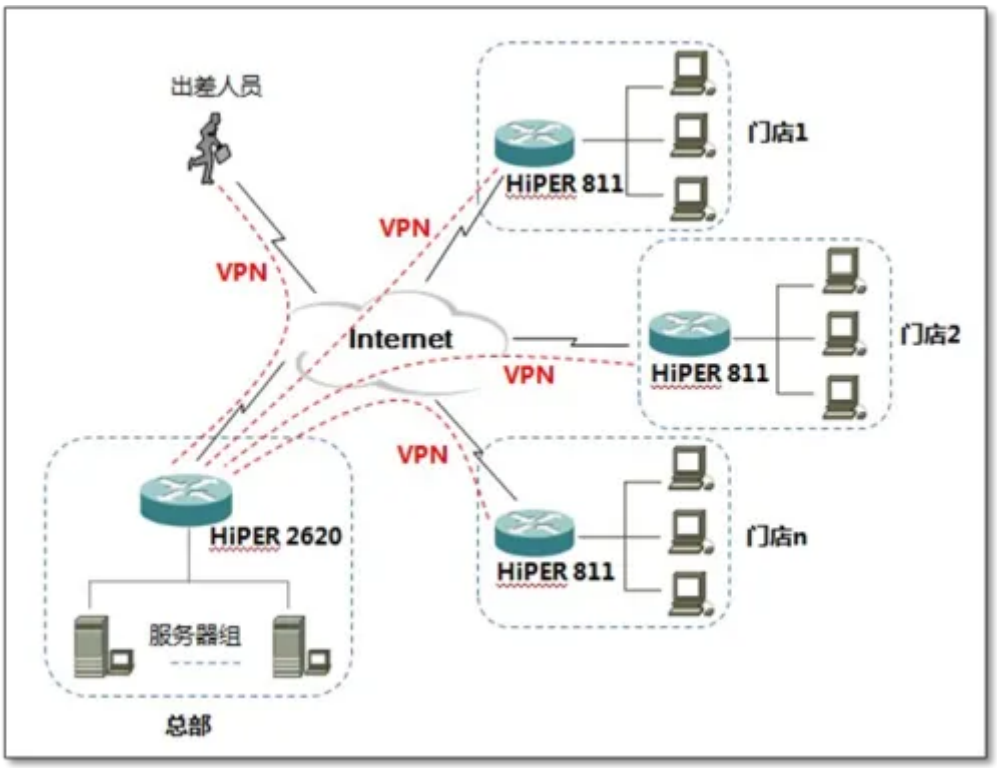
二、VPN

1、介绍

```
# 简介
    VPN，全称Virtual Private Network，虚拟专用网，就是利用开放的公众网络，建立专用数据传输的通道，将远程的分支机构、移动办公人员等连接起来。
```

```
# 局限
    1、企业不能直接控制基于互联网的VPN的可靠性和性能
    2、企业创建和部署VPN线路并不容易
    3、不同厂商的VPN产品和解决方案总是不兼容的
    4、当使用无线设备时，VPN有安全风险
```

2、拓扑图



3、常见品牌

```
1、深信服
2、天融信
3、锐捷网络
4、华为
5、启博
6、迪普科技
7、中科网威
8、Juniper
9、SonicWALL
10、锐见
```

4、历史漏洞

```
CVE-2021-35523：Securepoint SSL VPN 本地权限提升
CVE-2016-6329：OpenVPN
CVE-2021-1609：Cisco Small Business VPN路由器任意代码执行
```

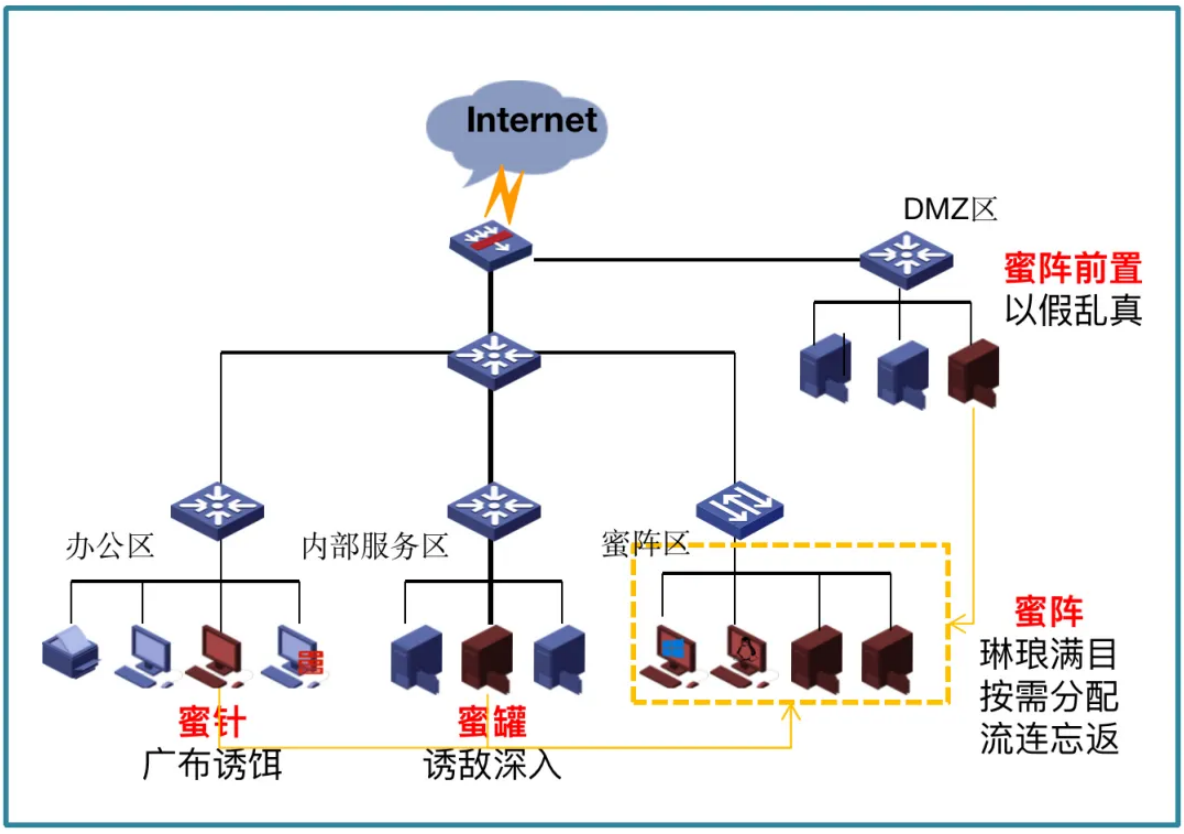
三、蜜罐

1、介绍

```
# 简介
    蜜罐是一种安全威胁的主动防御技术，它通过模拟一个或多个易受攻击的主机或服务来吸引攻击者，捕获攻击流量与样本，发现网络威胁、提取威胁特征。蜜罐的价值在于被探测、攻陷。
```

```
# 局限
    1、需要较多的事件和精力投入
    2、蜜罐技术只能对针对蜜罐的攻击行为进行监视和分析，其视图较为有限，不像入侵检测那样，能够通过旁路侦听等技术对整个网站进行监控。
```

2、拓扑图



3、常见品牌

```
1、知道创宇-创宇蜜罐
2、长亭科技-谛听
3、默安科技-幻阵
4、锦行科技-幻云
```

4、识别蜜罐

```
1、配置失真
2、JS文件大量请求其他网站
```

四、HIDS

1、介绍

```
# 简介
    HIDS，全称Host-based Intrusion Detection System，基于主机型入侵检测系统。作为计算系统的监视器和分析器，并不作用于外部接口，而是专注于系统内部，监视系统全部或部分的动态的行为以及整个计算机系统的状态。
```

2、拓扑图

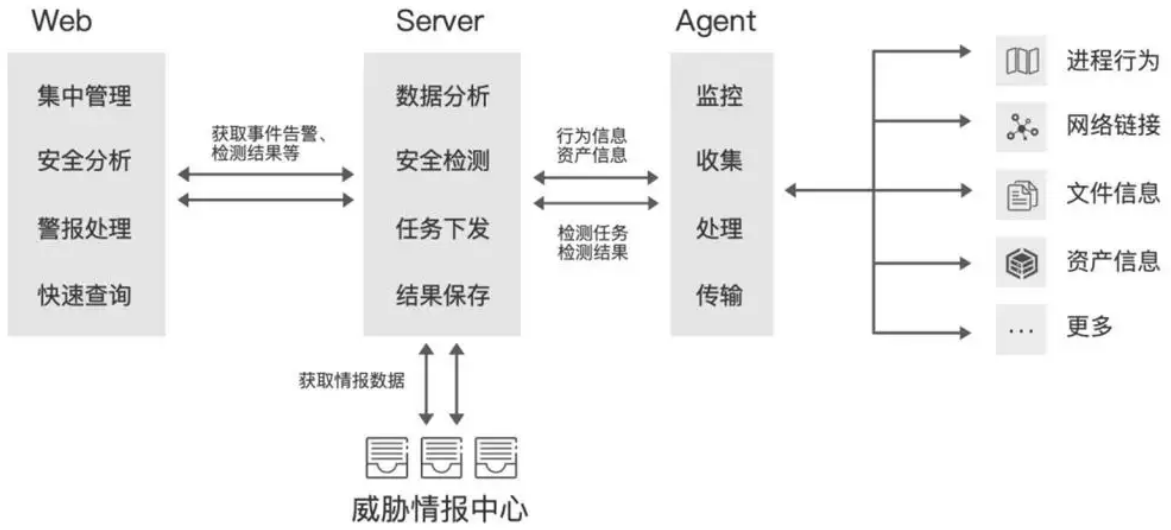


图1 基于HIDS的威胁情报架构

3、常见品牌

```
1、绿盟科技-绿盟工控安全入侵检测系统IDS-ICS
2、启明星辰-入侵检测IDS
3、天融信-入侵检测系统
4、华为云-企业主机安全 HSS
5、腾讯云-T-Sec 主机安全
6、网御星云-网御入侵检测产品（IDS）
7、浪潮云-主机安全 HSS 网络入侵检测 木马检测
8、奇安信-入侵检测系统
9、安全狗-云眼
10、UCloud优刻得-主机入侵检测
```

4、历史漏洞

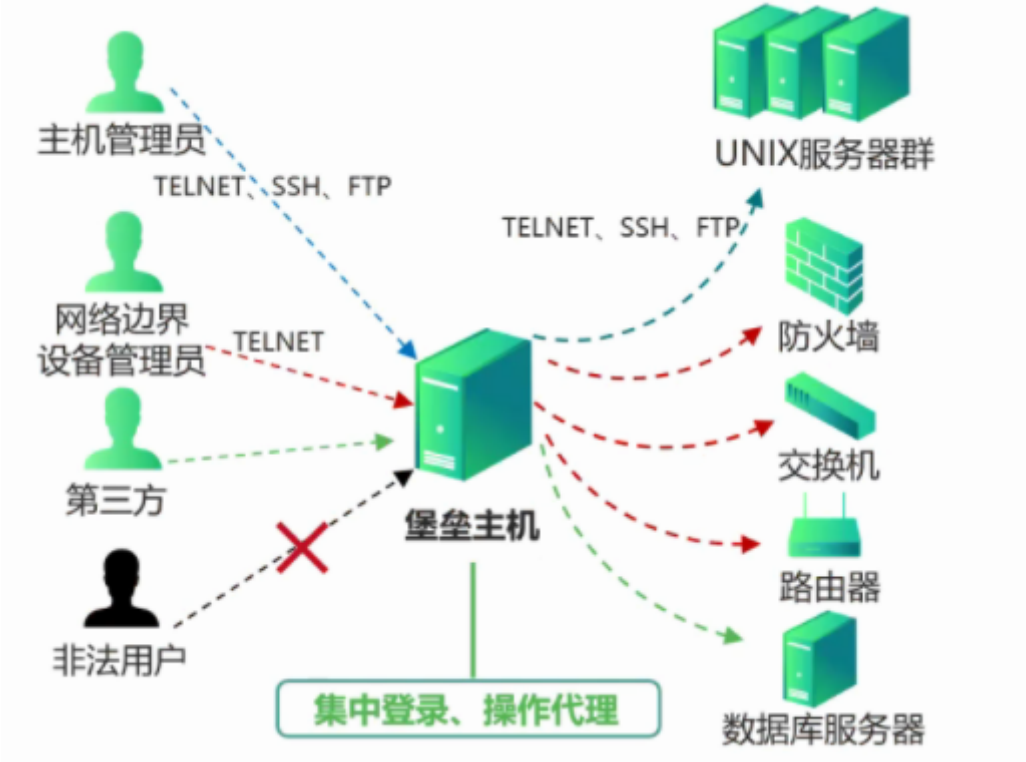
```
CNVD-2020-04123：OSSEC-HIDS服务器组件缓冲区溢出
```

五、堡垒机

1、介绍

```
# 简介
    堡垒机，即在一个特定的网络环境下，为了保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实现收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动，以便集中报警、及时处理及审计定责。
```

2、拓扑图



3、常见品牌

```
1、阿里云-堡垒机
2、腾讯云-T-Sec 堡垒机
3、华为云-云堡垒机 CBH
4、齐治科技-RIS-ACA 齐治访问控制审计系统
5、UCloud优刻得-堡垒机
6、绿盟科技-绿盟运维安全管理系统 OSMS
7、浪潮云-堡垒机 HAS 运维堡垒机 云堡垒机
8、天融信-运维安全审计系统
9、启明星辰-堡垒机 运维堡垒机
10、行云管家-行云管家堡垒机
```

4、历史漏洞

```
CNVD-2019-20835：齐治堡垒机前台远程命令执行
```

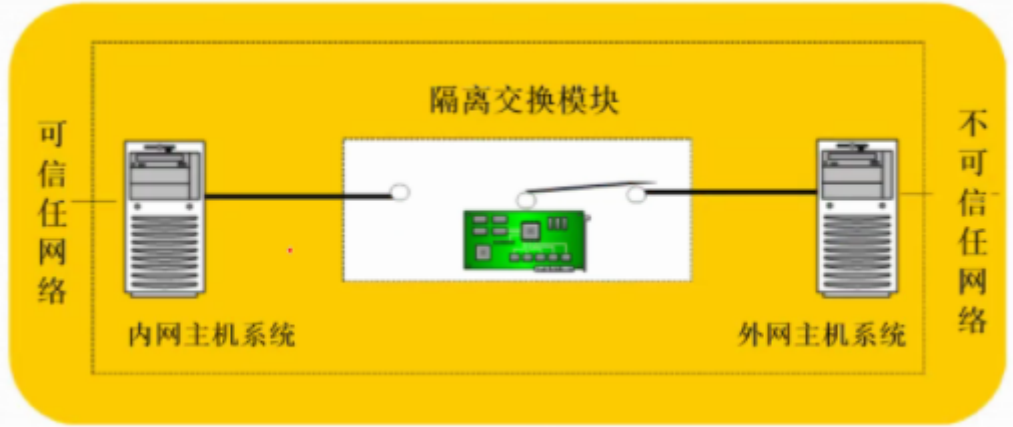
六、网闸

1、介绍

```
# 简介
    网闸，又称安全隔离网闸、物理隔离网闸，用以实现不同安全级别网络之间的安全隔离，不基于通信，用于存储和读写，类似于可移动硬盘。
```

```
# 局限
    1、只支持静态数据交换，不支持交互式访问
    2、适用范围窄
    3、结构复杂，成本较高
    4、技术不成熟，没有形成体系化
```

2、拓扑图



3、常见品牌

1、天融信
2、启明星辰
3、利谱
4、绿盟科技
5、伟思
6、宇宙盾
7、中孚
8、迪普科技
9、北信源
10、华烽泰特

4、历史漏洞

暂无