

**{{title}}**

设备编号：3334443

统计周期：2022-06-29至2022-07-05

生成时间：2022-07-05 11:38:47

**版权说明**

本文件中出现的全部内容，除另有特别注明，版权均属**中国电信宁夏公司**所有，以下简称（**“宁夏电信”**）。任何个人、机构未经**中国电信宁夏公司**书面授权许可，不得以任何方式复制或引用文件的任何片段。

**保密申明**

本文件包含了来自**中国电信宁夏公司**的可靠、权威的信息，以及被检测单位信息系统的敏感信息，接受这份文件表示同意对其内容保密并且未经**中国电信宁夏公司**书面请求和书面认可，不得复制，泄露或散布这份文件。如果你不是有意接受者，请注意对这份文件内容的任何形式的泄露、复制或散布都是被禁止的。

**目录**

[一、安全运营总览 1](#_Toc583649453)

[二、安全事件详情 2](#_Toc1838540722)

[2.1 病毒防御分析 2](#_Toc211717971)

[2.2入侵防御分析 2](#_Toc2111019165)

[2.3DDoS防护分析 3](#_Toc1321774068)

[2.4WEB防护分析 4](#_Toc1485916308)

[三、网络情况分析 6](#_Toc708057593)

[四、安全网关运行情况分析 8](#_Toc1117077524)

[五、安全加固建议 9](#_Toc1419903794)

[5.1网络安全加固 9](#_Toc1484780294)

[5.2主机安全加固 9](#_Toc942423118)

[5.3应用安全加固 9](#_Toc1613447601)

[5.4管理加固 9](#_Toc937819338)

一、安全运营总览

**尊敬的XXX公司，您好！**

**感谢您使用中国电信天翼安全大脑服务。**

**天翼安全大脑****KB038484566已持续守护您的网络53天。**

天翼安全大脑在2022-07-15至2022-07-21服务期间，安全防护功能中病毒防御已开启、IPS防御已开启、DDoS防护已开启、WEB防护未开启。

**病毒防御情况：**2022-07-15至2022-07-21期间，发现病毒防御告警总数：29,834，其中高危告警：0，已拦截：29,934，拦截率：90.32%。

**IPS防御情况**：2022-07-15至2022-07-21期间，发现IPS告警总数：29,834，其中高危告警：0，已拦截：29,934，拦截率：100%。

**DDoS防护情况：**2022-07-15至2022-07-21期间，发现DDoS告警总数：29,834，其中高危告警：0，已拦截：29,934，拦截率：100%。

**WEB防护情况**：2022-07-15至2022-07-21期间，发现WEB防护告警总数：29,834，其中高危告警：0，已拦截：29,934，拦截率：100%。

**安全网关运行情况**：2022-07-15至2022-07-21期间，天翼安全大脑安全网关运行正常，24小时不间断持续正常防护您的网络。

**网络情况**：总流量峰值：12323Mbps，总流量平均速度：234Mbps，总流量：33,345Gbps。

二、安全事件详情

**2.1 病毒防御分析**

病毒防御是一种检测恶意传输行为的安全机制，可以保护企业终端或服务器免受病毒、木马、勒索、挖矿等恶意程序感染。

病毒防御情况分析：2022-07-15至2022-07-21期间，共检测到34,885次恶意程序传输行为，拦截数：0，低风险放行数：34,885，拦截率：0%。

病毒事件TOP5

|  |  |  |  |
| --- | --- | --- | --- |
| 病毒名称 | 最新发现时间 | 次数 | 受影响IP地址 |
|  | 2022-09-01 12:12:23 | 23,874 | 172.168.3.2等 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**2.2入侵防御分析**

入侵防御是一种通过分析流经设备的网络流量来实时分析漏洞利用、暴力破解、数据泄露等入侵行为，实现保护企业终端及服务器免遭攻击的目的。

入侵防御情况分析：2022-07-15至2022-07-21期间，共检测到入侵威胁8774次，其中高风险4次，已拦截4次；中低风险8770次，低风险放行数：8770，拦截率：0.2%。

入侵防御类型TOP5

|  |  |
| --- | --- |
| 攻击类型 | 攻击次数 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

攻击目标IP TOP5

|  |  |
| --- | --- |
| 攻击目标IP | 受攻击次数 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

攻击源IP TOP5

|  |  |  |  |
| --- | --- | --- | --- |
| 攻击源IP | 攻击类型 | 攻击次数 | IP归属地 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：有8870次低风险入侵放行，可根据实际需求调整安全策略，减少上报次数。

**2.3DDoS防护分析**

DoS攻击/DDoS 攻击（拒绝服务攻击/分布式拒绝服务攻击），通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。

DoS/DDoS防护可以防止外网对内网的 DoS 攻击。

DDoS防护情况分析：2022-07-15至2022-07-21期间，共检测到DDoS攻击8774次，拦截数：4，低风险放行数：8770，拦截率：0.2%。

DDoS攻击类型TOP5

|  |  |
| --- | --- |
| 攻击类型 | 攻击次数 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

攻击目标IP TOP5

|  |  |
| --- | --- |
| 攻击目标IP | 受攻击次数 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

攻击源IP TOP5

|  |  |  |  |
| --- | --- | --- | --- |
| 攻击源IP | 攻击类型 | 攻击次数 | IP归属地 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**2.4WEB防护分析**

WEB防护专门用于保护内网的WEB服务器，可以有效防止跨站请求伪造、SQL 注入、XSS 攻击、会话劫持、目录遍历等各种针对 WEB 应用的攻击行为。

WEB防护情况分析：2022-07-15至2022-07-21期间，共检测到攻击8774次，其中高风险4次，已拦截 34次；中低风险8770次，放行数：8770。拦截率：0.2%。

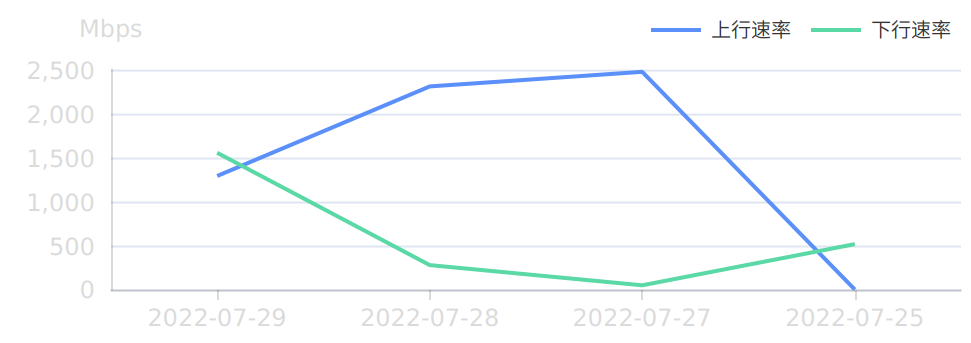
攻击源IP TOP5

|  |  |  |
| --- | --- | --- |
| 攻击源IP | 攻击次数 | IP归属地 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

注：有8870次低风险入侵放行，可根据实际需求调整安全策略，减少上报次数。

三、网络情况分析

通过对出口带宽流量进行统计分析，可以识别带宽的异常情况。



|  |  |  |  |
| --- | --- | --- | --- |
|  | 总流量 | 上行流量 | 下行流量 |
| 总流量（Byte） | 102.3G | 50.8G | 51.5G |
| 平均速率（bps） | 9.91M | 4.83M | 5.3M |
| 峰值速率（bps） | 19.3M | 10.2M | 9.1M |

用户总流量TOP5

|  |  |  |  |
| --- | --- | --- | --- |
| 用户 | 总流量 | 上行流量 | 下行流量 |
| 192.168.3.2 | 102.3G | 50.8G | 51.5G |
| 192.168.2.3 | 9.91M | 4.83M | 5.3M |
| 192.168.32.3 | 19.3M | 10.2M | 9.1M |
|  |  |  |  |
|  |  |  |  |

网站总流量TOP5

|  |  |  |  |
| --- | --- | --- | --- |
| URL | 总流量 | 上行流量 | 下行流量 |
| qq.com | 102.3G | 50.8G | 51.5G |
| Baidu.com | 9.91M | 4.83M | 5.3M |
| Docker.com | 19.3M | 10.2M | 9.1M |
|  |  |  |  |
|  |  |  |  |

服务总流量TOP5

|  |  |  |  |
| --- | --- | --- | --- |
| 服务名称 | 总流量 | 上行流量 | 下行流量 |
| BGP | 102.3G | 50.8G | 51.5G |
| IMAP | 9.91M | 4.83M | 5.3M |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

四、安全网关运行情况分析

安全网关运行情况分析对安全网关设备在线数量、离线数量、CPU、内存使用率进行统计，监控安全网关运行异常情况。

安全网关设备编号：393884394。

安全网关情况分析：CPU平均使用率34%，内存平均使用率21.32%，硬盘使用率32%，安全网关运行正常，将持续为您的网络提供安全防护。

CPU平均使用率：33%

CPU使用率超过90%的次数：9

内存平均使用率：23.12%

内存使用率超过90%的次数：12

五、安全加固建议

**5.1网络安全加固**

1. 使用VLAN技术对各个业务区域进行逻辑隔离，为不同用户和业务分配不同的IP地址段。

2.内部网络建议部署安全管家服务，全面检测内部网络安全威胁，并通过云端安全能力和安全专家服务预警网络安全事件，并通过天翼安全大脑安全网关及时处置。可为不同安全级别的系统划分安全域，对外业务部署DMZ区域，内部业务部署数据中心区域，用户接入为用户区域，视情况部署远程接入区域，并在这些不同的安全域之间部署访问控制策略，当有安全事件发生的时候，可以将安全事件（例如：勒索病毒永恒之蓝攻击）抑制在有限的区域内，不会面向全网进行传播，控制风险传播范围，降低损失。

3.建议部署相应的安全产品提供安全审计，如日志审计系统、堡垒机（运维审计系统）等。

**5.2主机安全加固**

1. 对操作系统和业务系统的弱口令进行整改，修改掉已有的弱口令，并启用密码策略，对密码的长度和复杂度进行强制性要求，并定期进行更换。

2. 对操作系统的补丁进行检查，并对尚未更新的系统进行补丁更新。

3. 部署终端检测与响应软件，实时对系统的安全状态进行评估，并且在有安全事件发生的时候进行响应，消除影响。

**5.3应用安全加固**

1.使用HTTPS提供安全的访问，并对存在的管理员弱密码进行修改。

2.修改WEB系统的页面源码，修复XSS漏洞，或部署WAF进行防御。

3.避免用户敏感信息在数据库明文存储。

**5.4数据安全加固**

1.定期对重要数据进行备份，可根据数据安全级别进行定时或实时备份。

2.对重要数据库进行安全防护或安全审计，可根据需要部署数据库防火墙或数据库审计系统。

3.对数据防泄露要求高的环境，可考虑部署数据加密或数据防泄露工具。

**5.5管理加固**

1. 建立网络安全管理制度，对日志保存时间、补丁管理升级与管理，口令定期更新周期等方面做出规定。

2. 补丁管理制度，安全补丁根据其对应漏洞的严重程度分为三个级别：紧急补丁、重要补丁和一般补丁；紧急补丁必须在15天内完成安装，重要补丁必须在一个月内完成安装，一般补丁要求六个月内完成安装。

3. 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证系统中不存在弱口令等风险，并按季度对密码进行更新；更改默认的系统管理员帐号和口令，管理员帐号应采用实名制。

4. 建立突发安全事件应急响应预案，并定期对预案进行演练，评估自身应对突发安全事件对响应和处理能力，并持续提升。