2022 年 8.9 日更新

HFish

威胁诱捕与诱骗系统

实施部署说明

目录

一、文档说明

本文档提供 Hfish 蜜罐产品相关介绍，帮助安全人员快速了解 HFish 功能、部署、使用等相关信息。

二、HFish 产品介绍

1、基础介绍

HFish 是一款蜜罐工具，侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个场景出发，为用户提供可独立操作且实用的功能，通过安全、敏捷、可靠的中低交互蜜罐增加用户在失陷感知和威胁情报领域的能力。

HFish 具有超过 40 种蜜罐环境、提供云蜜网、可高度自定义的蜜饵能力、一键部署、跨平台多架构、国产操作系统和 CPU 支持、极低的性能要求、邮件/syslog/webhook/企业微信/钉钉/飞书告警等多项特性，帮助用户降低运维成本，提升运营效率。

2、安全性介绍

从蜜罐的部署角度来讲，目前对蜜罐的网络策略有严格限制，端口打开情况有严格限制。目前，HFish 节点端与管理端之间单向通信，节点端单向访问服务端。服务端被动接受节点端传递来的攻击信息。

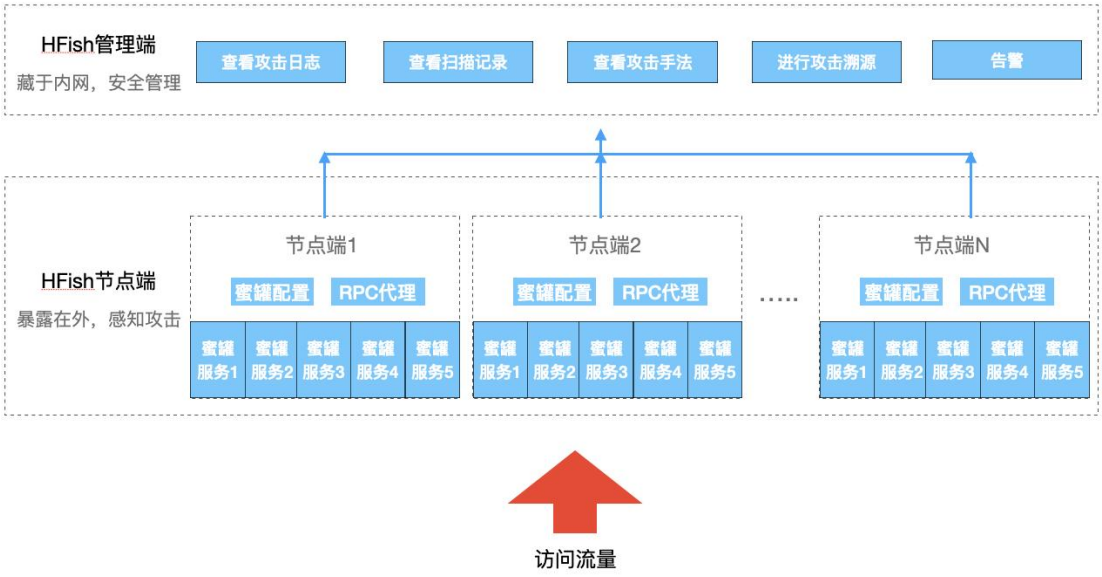
从蜜罐交互上来讲，HFish 是基于本地低交互和云端高交互的蜜罐产品，本地蜜罐全部为低交互蜜罐，其只有少量命令响应，可以保证蜜罐的安全性。云端高交互蜜罐的所有攻击交互发生在微步在线的云端，用户本地无任何失陷风险。

最后，在本身逻辑隔离的网络内，都会单独部署一套蜜罐。防止扰乱正常的网络隔离逻辑。

三、HFish 软件架构

1. 系统架构

HFish 采用经典 C/S 架构组成。管理端（Server）用于管理节点端，接收存储和分析节点端回传攻击日志和流量数据，最终形成实时威胁列表页面、威胁画像，协助客户了解当前网络威胁态势和捕捉攻击者信息。节点端（Client）用于接收管理端配置指令，实时构建多个虚拟环境，支持高低交互蜜罐，支持基础远程管理服务模拟、数据库服务模拟、网络传输服务模拟、邮件 Web 登录页面模拟、网络及 IoT 设备模拟、常见 Web 服务模拟、常见安全漏洞模拟等多种模拟服务，并内置多种行业环境模板。



3、主机环境

为保证蜜罐业务稳定性，HFish 管理端应部署在以下操作系统环境内：

- CentOS 7.x 及以上版本 64 位
- Redhat 7.x 及以上版本 64 位

HFish 节点端支持 Linux、Windows、ARM 等各类架构和操作系统部署环境，

具体包括：

- Windows 7 及以上版本的 32 和 64 位
- Windows 10 及以上版本的 32 和 64 位
- Windows Server 2008 及以上版本的 32 和 64 位
- CentOS 7.x 及以上版本的 32 和 64 位
- Redhat 7.x 及以上版本的 32 和 64 位
- Ubuntu 12.x 及以上版本的 32 和 64 位 (*)
- 基于 ARM 32 和 64 位架构的树莓派操作系统

四、溯源能力介绍

1、溯源版本简介

HFish 作为蜜罐软件，提供被攻击时候的正常防卫需求。当攻击者扫描、攻击或者恶意连接 HFish 的蜜罐时，HFish 提供包括但不限于： 通过现有攻击工具漏洞，在合理范围内对攻击者进行信息提取、溯源等必要的攻击防御信息收集手段。

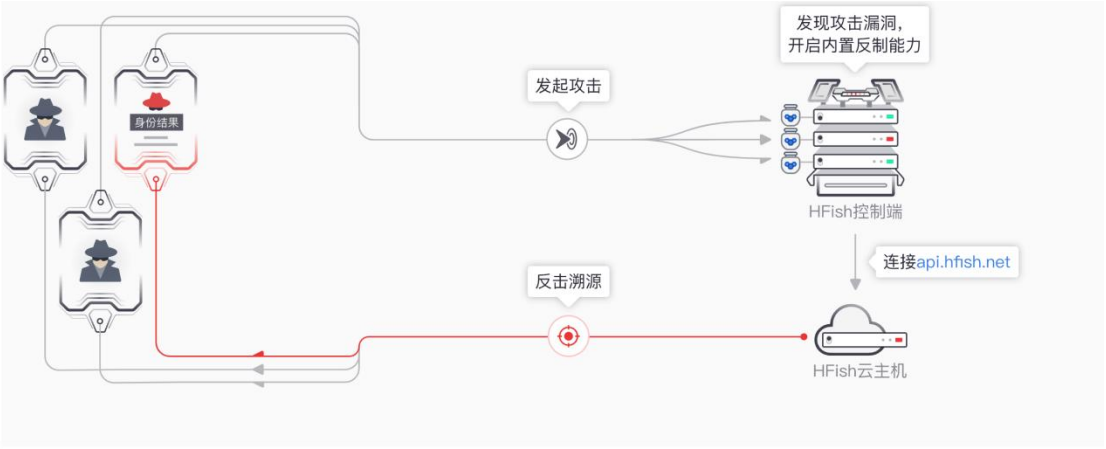


图-HFish 溯源流程介绍

HFish 溯源功能主要分为对 Web 类蜜罐的反制及对 Mysql 蜜罐的反制。其主要共功能简介如下：

反制类型	反制工具	反制触发条件
Web 类蜜罐反制	针对包括 Goby、蚁剑在内的 7 种攻击者常见工具的反制。	当攻击者使用攻击、在运行工具的电脑攻击 HFish web 蜜罐时，HFish 蜜罐进行反制。 反制过程需要按照第七章，开启对应的网络访问权限。 反制后可以获得攻击者使用机器的权限，从而自动获得攻击者的微信、QQ、history、whoami、qq 音乐用户名、百度网盘用户名、浏览器记录等信息。 （该功能只在被攻击时启动自动溯源，如需要做一对一反制，请联系微步销售）
Mysql 蜜罐反制	针对 8.0 以下的 Mysql 客户端连接 HFish	8.0 以下的 Mysql 客户端连接 HFish Mysql 蜜罐时候，可以拿到攻击者电脑任意路径的文件。 该具体的拿取路径，可以在节点管理-MySql 蜜罐中进行修改。

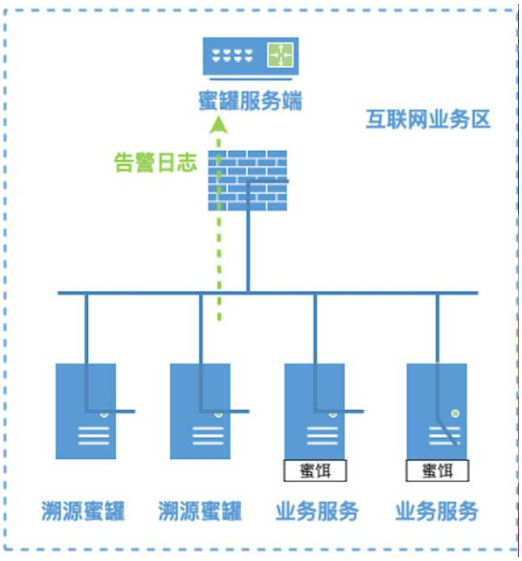
2、溯源版本环境需求

需求内容	需求版本
产品版本	更新至 3.1.0
网络情况	节点需要可联通 106.75.5.50:22220 与 106.65.15.34:2220。 管理端需要可连接 api.hfish.net

产品内配置需求	进入【系统配置】-【溯源配置】中确认用户协议，开启功能即可。 

五、部署环境

1、互联网区域部署图



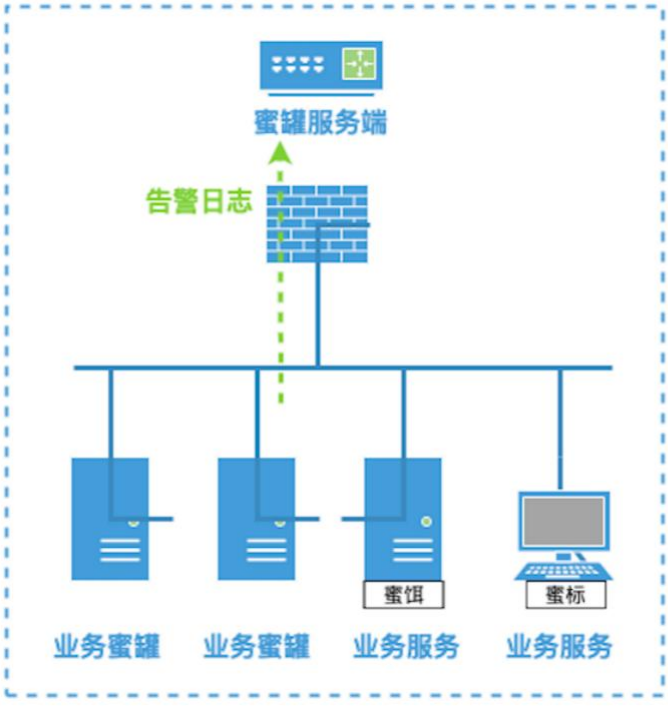
管理端需要如下部署环境

	最低配置	建议配置
CPU	2 核	4 核
内存	4G	8G
硬盘	50G	200G

内网节点端需要如下部署环境

	最低配置	建议配置
CPU	1 核	1 核
内存	1 G	2G
硬盘	20G	50G

2、内网区域部署图



内网管理端需要如下部署环境

	最低配置	建议配置
CPU	2 核	4 核
内存	4G	8G

硬盘	50G	100G

外网节点端需要如下部署环境

	最低配置	**建议配置**
CPU	1 核	1 核
内存	1 G	2G
硬盘	20G	50G

3、部署说明

（1）部署所需权限

●管理端对 root 权限的需求：

如果使用官网推荐的 install.sh 脚本安装，需要 root 权限，安装目录会位于 opt 目录下；

如果下载安装包手动安装，在默认使用 SQLite 数据库情况下，管理端的部署和使用不需要 root 权限，但如果要替换 SQLite 改为 MySQL 数据，则 MySQL 安装和配置需要 root 权限。

●节点端对 root 权限的需求：

节点端安装和运行需要 root 权限。非 root 权限运行的节点无法监听低于 tcp/1024 的端口。

4、部署范围

我们建议蜜罐的部署情况如下

环境	基础部署方案	最佳部署方案
内网	1. 每个网段内，在网段头和网段尾部署两个节点 2. 其他业务与办公机器根据架构，灵活	1. 每个网段内，能覆盖 20%～50%的 IP 提供给蜜罐。 2. 其他业务与办公机器根据架构，根据

	部署蜜饵或蜜标，覆盖程度越高，失陷感知越好。	业务蜜饵或蜜标进行部署，覆盖程度越高，失陷感知越好。 3. 每个网段按照网段内的应用，自定义 1-2 个业务蜜罐进行失陷感知。
外网	1. 关键服务器相邻 IP 部署蜜罐 2. 外网业务部署蜜饵、蜜标，引流至蜜罐	1. 关键服务器相邻 IP 部署蜜罐 2. 主域名下的三级子域名提供给蜜罐页面 3. 业务不过重的情况下，将业务的 404 页面重定向至自定义蜜罐页面。

如有攻击者触发了蜜罐的告警，告警会被发送到蜜罐服务器，各区域蜜罐服务器可以将告警发送到日志服务器进行汇总。

六、主要功能说明

1、蜜罐可生成的相关模板

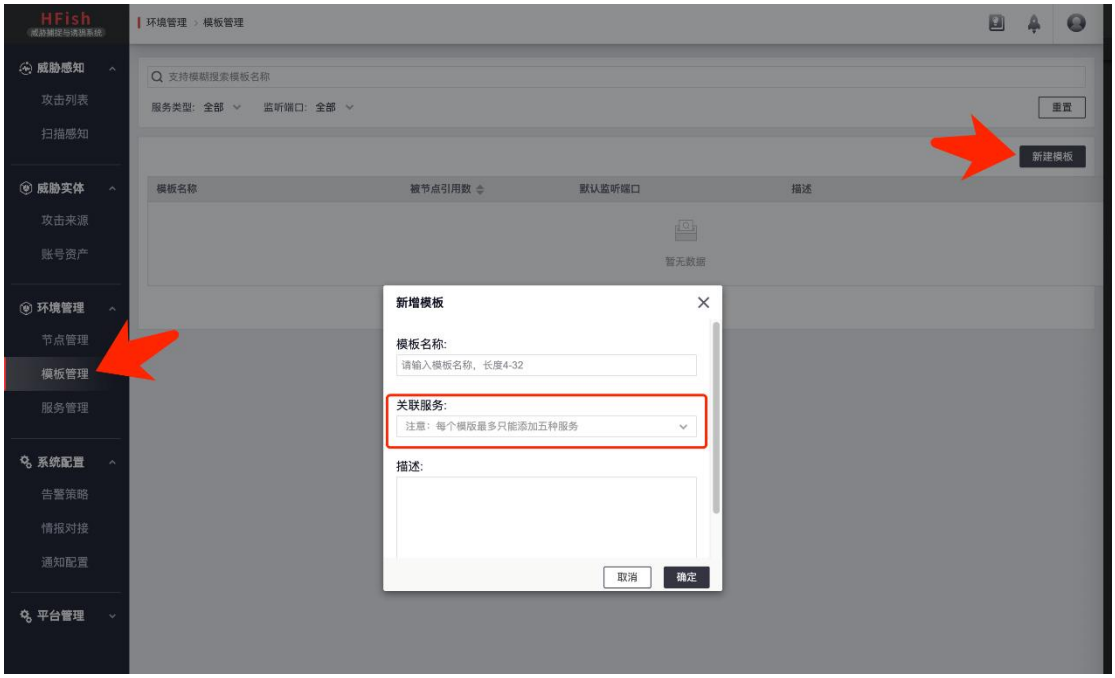
(1) 模板管理

模板管理用于展示现有模板及其被引用情况，安全人员可自行定制经常被重复使用或有批量修改需求的一组蜜罐服务模板。界面配置如下：

(2) 制作服务模板

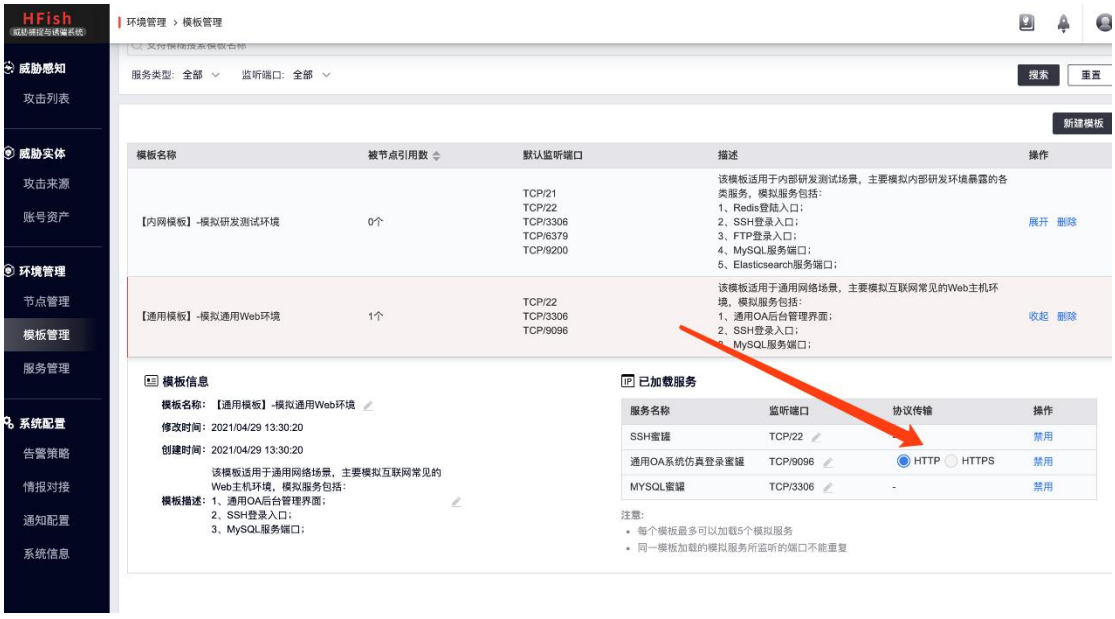
在【模板管理】页面，自定义模板名称、最多 10 个蜜罐服务，并添加一段

描述完成模板制作。



（3）调整传输协议

点击上一步制作好的模板，可以对某个服务的传输协议进行调整。针对 Web 应用仿真、网络设备服务、安全设备服务以及 IOT 服务，根据安全人员自身业务场景和网络情况，选择其具体的传输协议（HTTP 或者 HTTPS），从而让蜜罐更符合当前网络结构，更好吸引攻击者视线。



最后，在【节点管理】页面，展开某个节点，可以通过右侧下拉菜单选择需要的模板。一个模板可以被无限的节点使用，修改模板时，所有引用该模板的节

点蜜罐服务都会被实时更新，用户可以利用该特性批量修改节点上的蜜罐服务。

2、触发告警的判断机制

（1）告警配置

对于蜜罐捕获到的信息，根据安全人员的安全运营流程，第一时间将该信息通知至其他安全设备或者相关安全运营人员。界面配置如下：

【告警配置】页面分为两个标签页，分别是【告警策略】和【通知配置】。

【告警策略】用于配置发送告警的内容和告警方式(syslog、邮件或 webhook)，目前支持威胁告警和系统通知两种类型，其中威胁告警是系统感知攻击时的告警，系统通知是系统自身运行状态的告警；

【通知配置】用于配置使用 syslog、邮件或 webhook 发送告警时所需的参数；

（2）告警策略

添加一个新的策略

设置名称、类型和通知方式

（3）通知配置

●syslog 服务器配置

支持使用 TCP 或 UDP 两种协议外发告警策略，HFish 支持同时外发 5 路 syslog 进行通知。

●邮件服务器配置

设置 SMTP 主机、协议、端口、SMTP 账号、密码、发件人名称后、收件人地址后，外发告警。

●Webhook 配置

Webhook 是一种 API 概念，即当事件发生时，事件产生方使用 HTTP(s)的方式调用某个 Web API 接口，该接口可以灵活的进行后续工作。

HFish 支持四种 Webhook 通知，分别是：钉钉、飞书、企业微信和自定义方式。

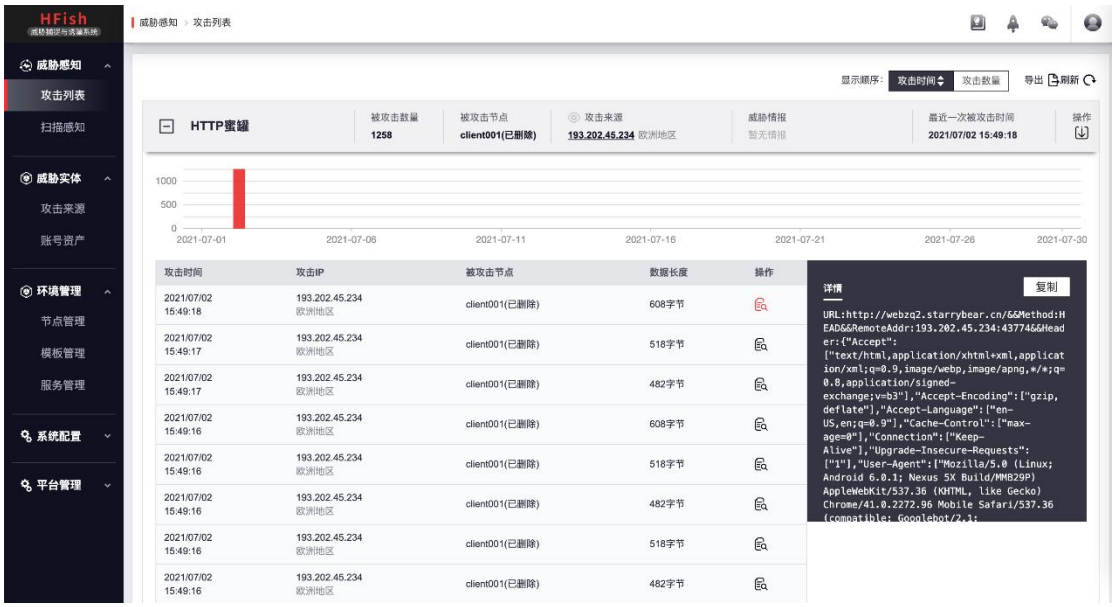
5、Hfish 内网推荐功能

（1）支持自定义 word 和 excel 类型的蜜标，蜜标支持便捷播撒到正常业务机器上，打开即报警。

（2）攻击列表：可以查看所有蜜罐被攻击的记录。

攻击列表本身有一定的聚合能力，会把一段时间内，针对同一 IP、同一蜜罐的同一攻击者行为聚合在一起。

支持按照攻击来源 IP 地址、蜜罐场景、蜜罐类型、被攻击节点名称、数据长度、攻击来源地理位置名称、情报标签和是否标记进行搜索，支持按照攻击时间或数量排序，支持导出所有攻击数据或导出某个聚合事件到 CSV 文件。



(3) 扫描感知

即使节点相关端口没有开放，HFish 仍能记录下扫描行为，此外，HFish 还会记录节点主机本身外联行为。

(4) 失陷感知

利用已经播撒的蜜饵实现主机失陷感知威胁，用户可以在该页面生成蜜饵，并观测蜜饵被触碰状态。

使用场景：HFish 的蜜饵在牵引攻击者的功能上增加了精确定位失陷能力，即每个蜜饵都是唯一的，攻击者入侵用户主机后，如果盗取蜜饵文件中的数据并从任意主机发起攻击，防守者仍能知道失陷源头在哪里。

HFish 提供完整的蜜饵定制，可以通过在「失陷感知」-「失陷感知」中定制新增自己的业务蜜饵。

七、安全特性

HFish 管理端默认安装无需 root 权限，但如果客户设置的监听端口小于 TCP/1024 端口会需要 root 权限，不建议客户修改监听端口小于 TCP/1024。

1、端口开放需求

HFish 管理端默认开放端口列表:

端口	服务类型	服务说明
TCP/22	SSH	用于管理端远程管理，该端口仅应被堡垒机、跳板机等运维平台或授权人员访问
TCP/4433	Web	默认的 Web 管理页面端口，该端口仅应被堡垒机、跳板机等运维平台或授权人员访问
TCP/4434	Web	默认的节点数据回传端口

HFish 节点端默认开放端口列表：

端口	服务类型	服务说明
TCP/22122	SSH	原 TCP/22 端口，HFish 节点端部署成功后，会被改到 TCP/22122 端口，以避免和模拟的虚假 SSH 端口冲突，该端口用于管理端远程管理，该端口仅应被堡垒机、跳板机等运维平台或授权人员访问

注意：

- HFish 节点端负责构建欺骗服务，因此该主机上实际开放的端口受用户指定的虚假服务特性决定；
- 应保证 HFish 节点端上被启用的欺骗服务可被内网或外网访问到，特别注意排查节点端本机防火墙是否做了限制；

2、网络访问需求

HFish 支持 IPv4 和 IPv6 地址环境，可以在完全隔离互联网的内部网络工作，但为了最大限度感知真实威胁和对接云端接口消费威胁情报，以及接受自动化升级服务，微步在线强烈建议客户允许 HFish 管理端访问互联网，为兼顾安全性和服务可用性，推荐用户仅允许 HFish 管理端主动访问如下网络域名、地址和端口：

开放地址	开放端口	访问目的
api.hfish.net（禁 ping，需要 telnet 端口）	TCP/443	用于官网升级功能，建议开启

106.75.5.50、106.65.15.34（禁 ping，需要 telnet 端口）	TCP/22220（高交互 ssh 端口） TCP/22222（高交互 ssh 端口）、 TCP/22224(高交互 MySql 端口)	用于与云端高交互蜜罐进行通信，建议开启
api.hfish.net	TCP/443	用于攻击数据拉取，建议开启
hfish.cn-bj.ufileos.com	TCP/443	用于分发安装和升级包
api.threatbook.cn	TCP/443	用于威胁情报查询，如果未启用该功能，无需开放
open.feishu.cn	TCP/443	用于飞书告警功能，如果未使用该功能，无需开放
oapi.dingtalk.com	TCP/443	用于钉钉告警功能，如果未使用该功能，无需开放
qyapi.weixin.qq.com	TCP/443	用于企业微信告警功能，如果未使用该功能，无需开放

注意：

- HFish 管理端仅需要通过 NAT 模式访问互联网，基于安全考虑，微步在线不建议用户将 HFish 管理端管理接口暴露在互联网。

3、正常体验需求

为保证客户可以正常访问 HFish 系统 Web 管理页面，强烈建议客户使用以下版本浏览器：

浏览器	架构	版本信息
Google Chrome	32 或 64 位	版本大于 70 或更高
Firefox	32 或 64 位	版本大于 52 或更高
Microsoft Edge	32 或 64 位	版本大于 58 或更高

基于 Chromium 内核浏览器	32 或 64 位	内核版本大于 65 或更高
Microsoft IE	32 或 64 位	版本大于 11 或更高
Safari	32 或 64 位	版本大于 14 或更高