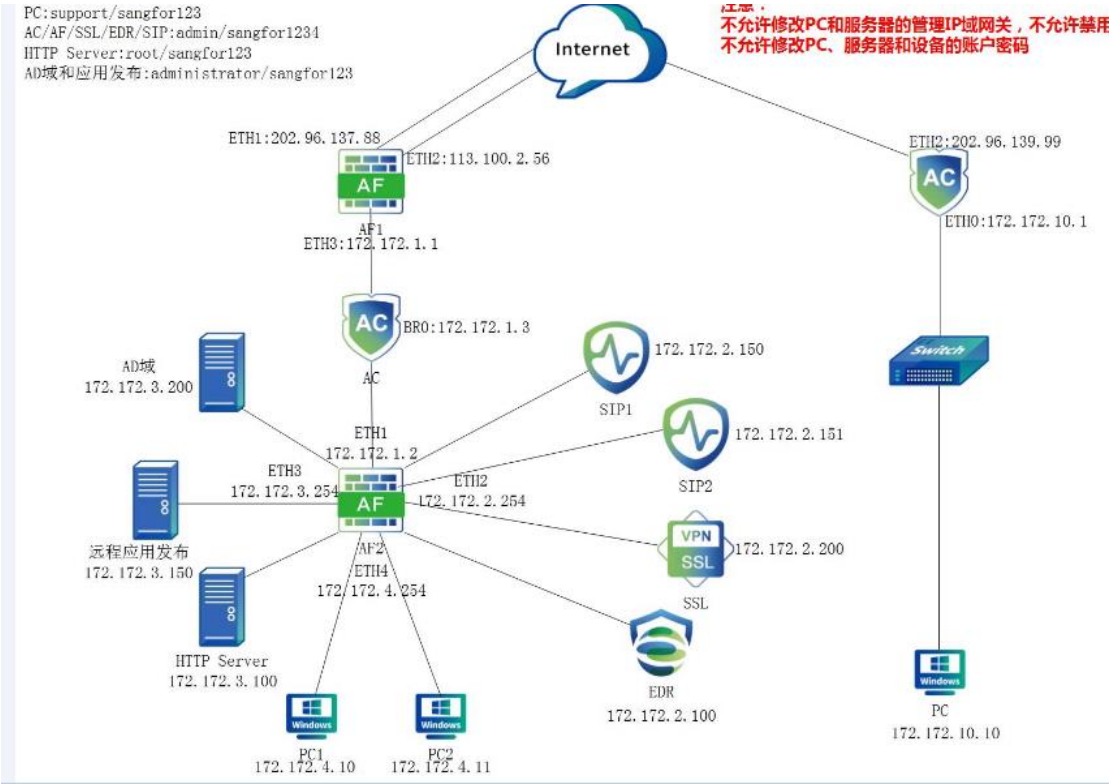
SSLVPN 配置实验

一、 实验环境如图：



二、 实现要求：

1、SVPN 中泛域名 WEB 访问，允许访问 https://www.baidu.com,但不允许访问 tieba.baidu.com 不允许访问。

2、SVPN 中尝试什么情况下直接输入内网地址进行访问。

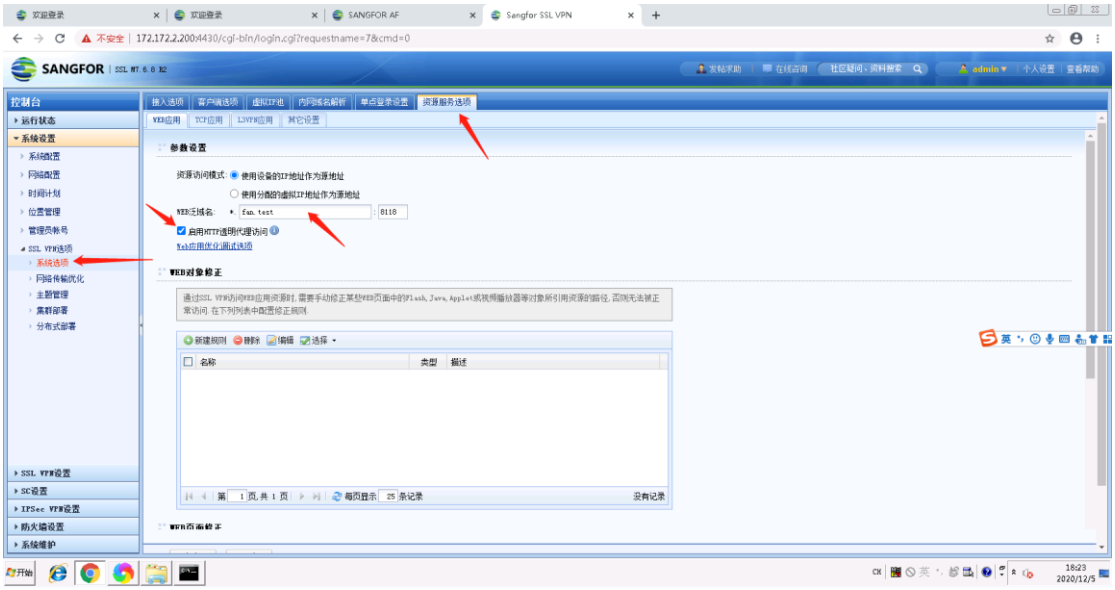
3、EDR 对接 AF,AC,SIP,抓取恶意流量，观察 rdp 或 ssh 或 smb 或 ftp 暴破情况。

4、EDR 自动监测系统漏洞，并报告结果，不需要自动打补丁；定期进行基线检查并报告结果。

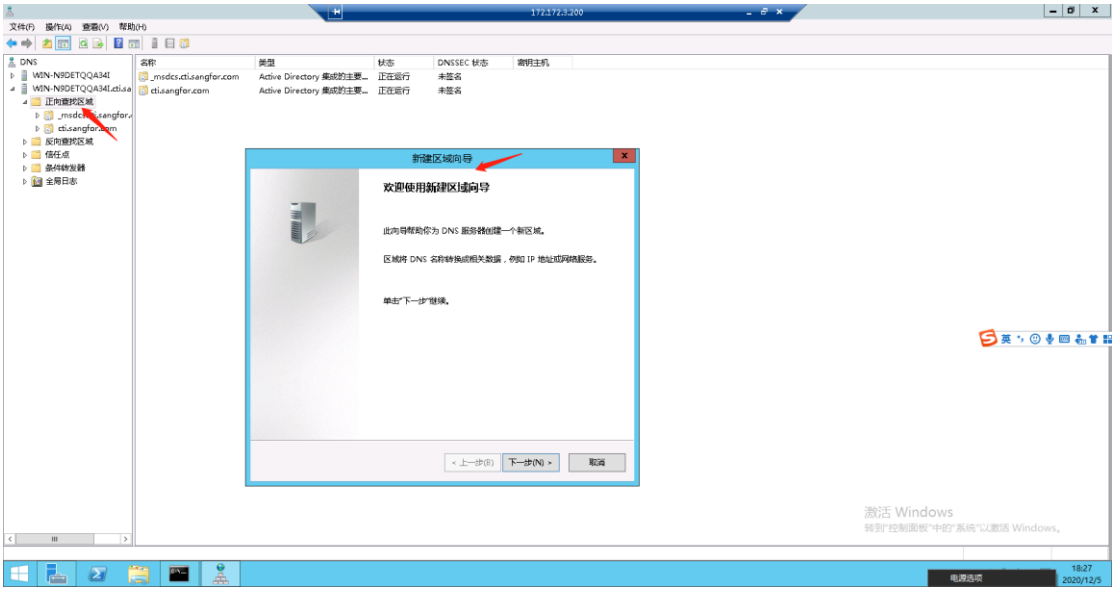
三、 实现步骤：

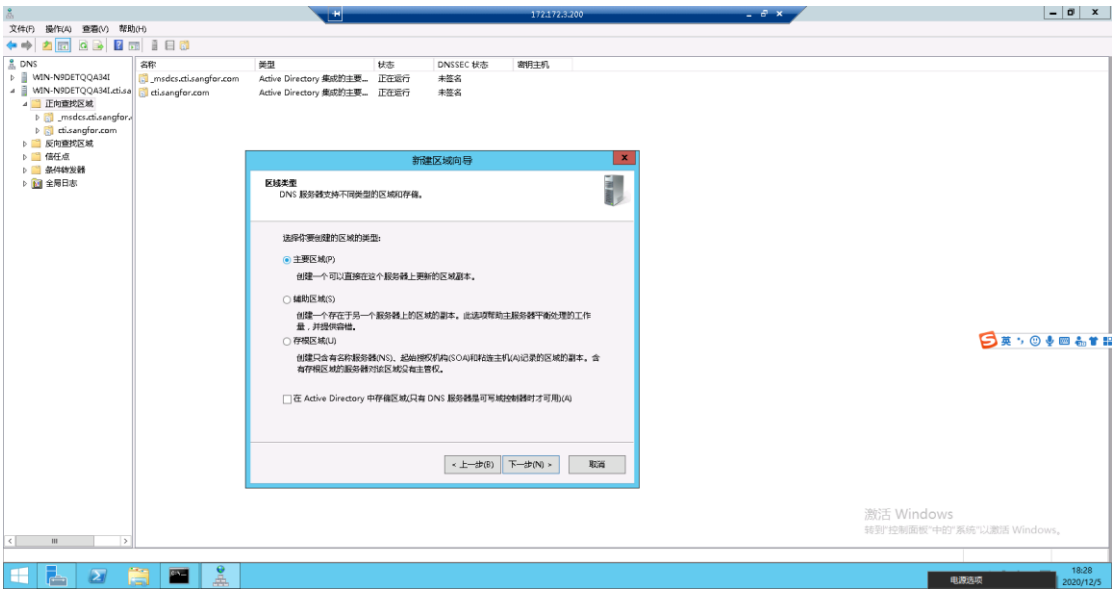
实验 1 步骤如下：

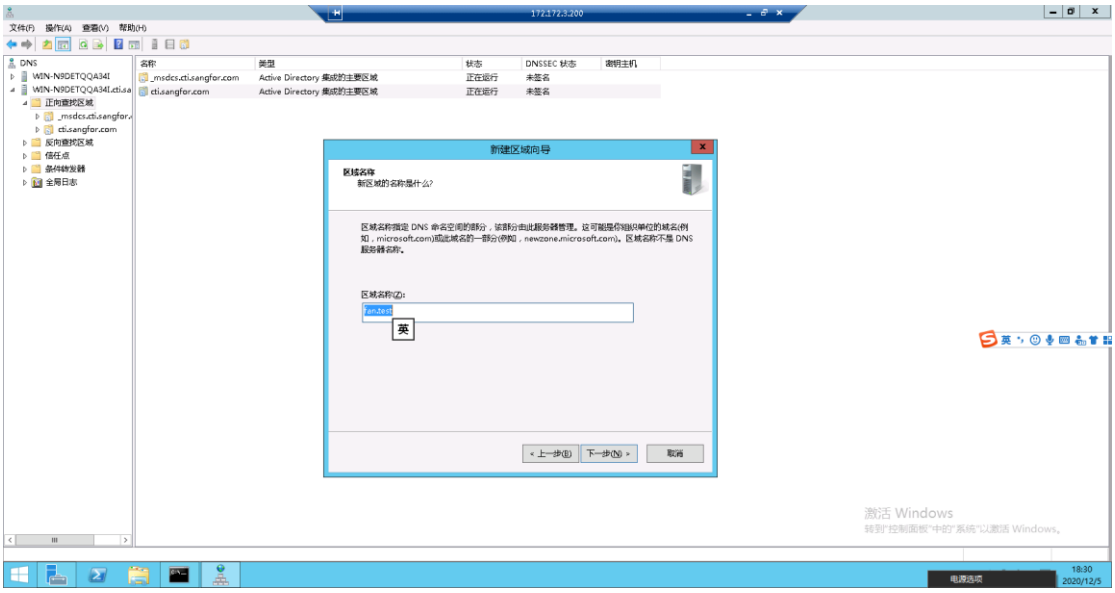
1、 登录 vpn 配置泛域名

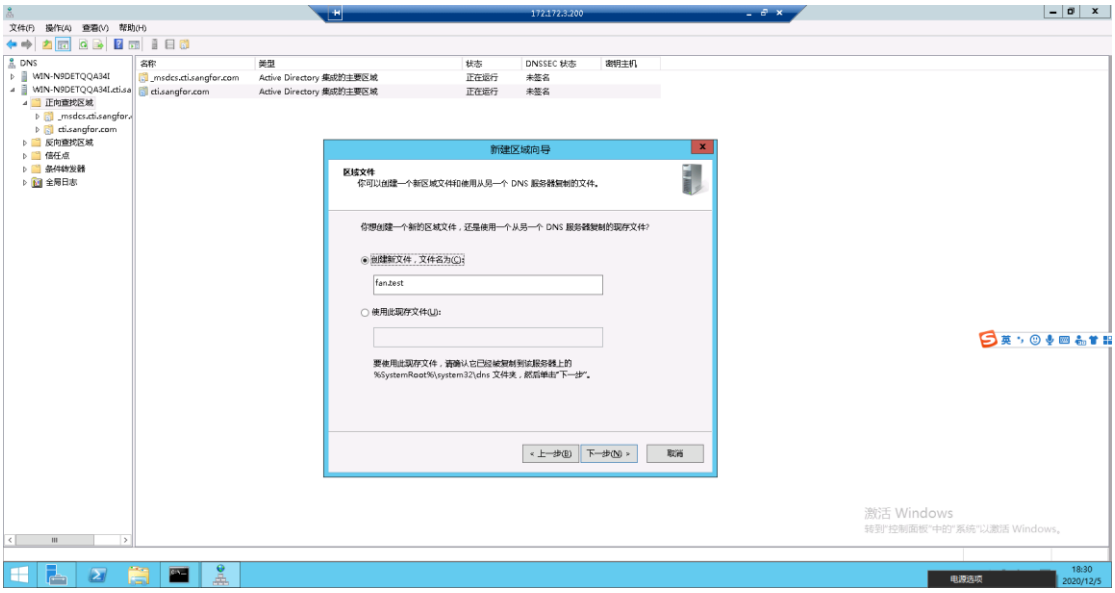


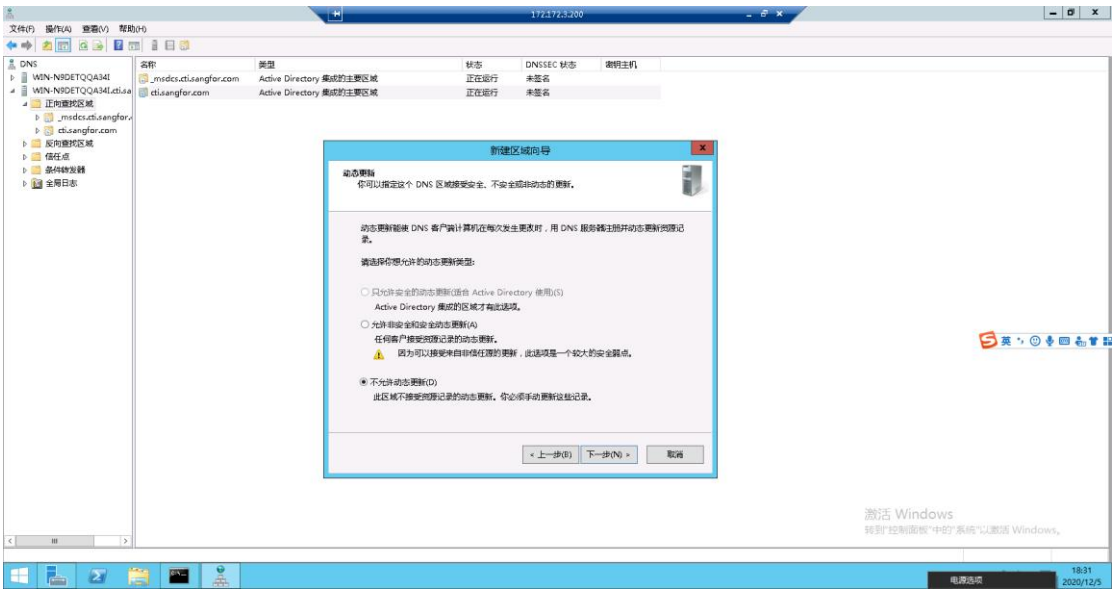
2、 登录 ad 配置 dns

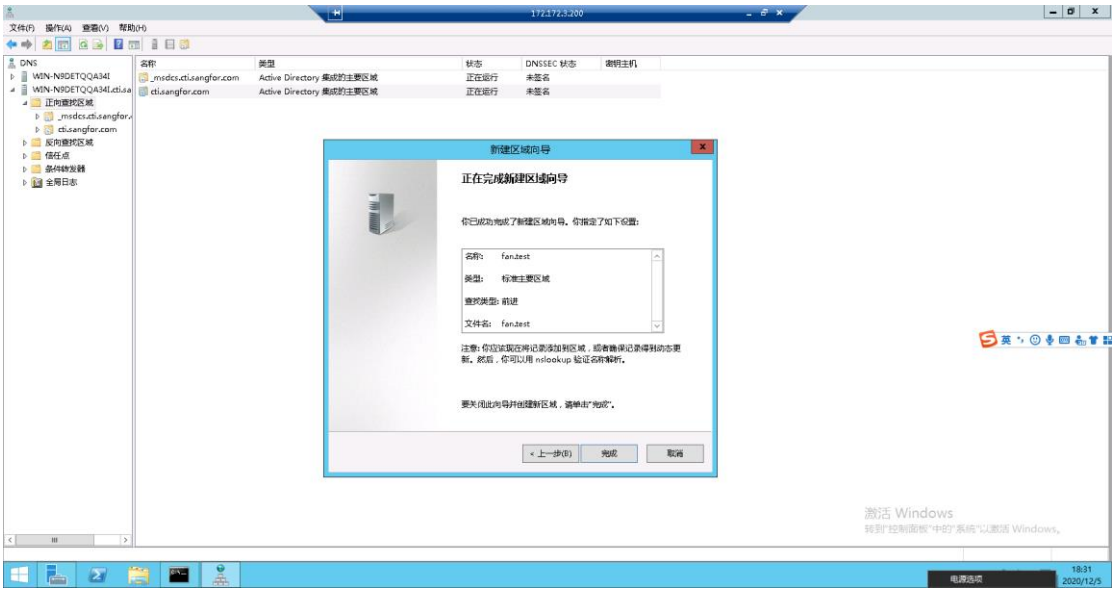


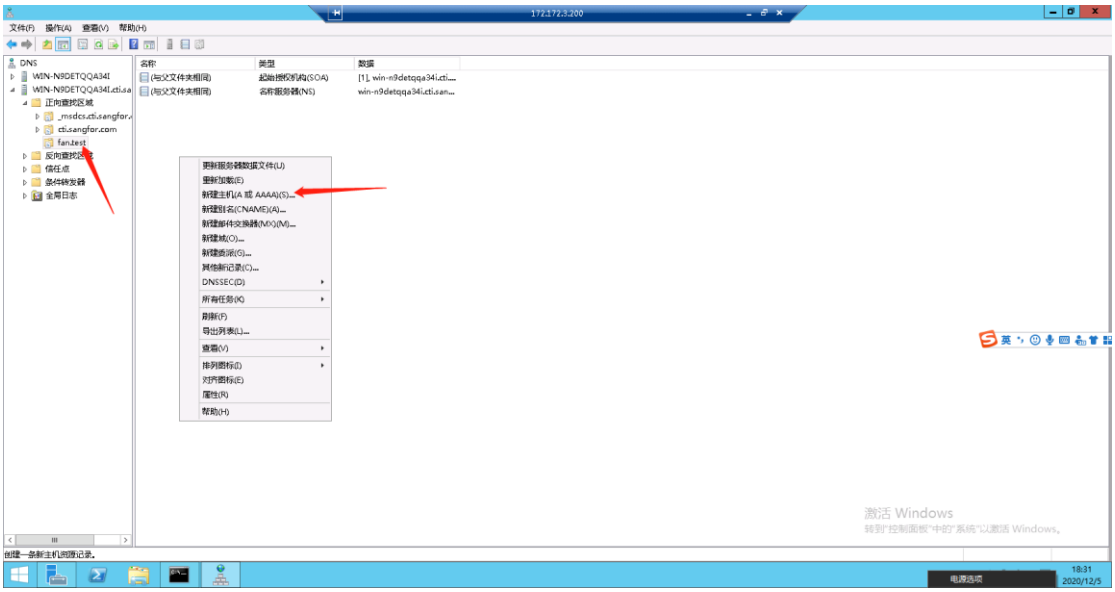

新建区域向导
区域类型
DNS 服务器支持不同类型的区域和存储。
选择你要创建的区域的类型：
主要区域(P)
创建一个可以直接在这个服务器上更新的区域副本。
辅助区域(S)
创建一个存在于另一个服务器上的区域的副本。此选项帮助主服务器平衡处理的工作量，并提供容错。
存根区域(U)
创建只含有名称服务器(NS)、起始授权机构(SOA)和A连主机(A)记录的区域的副本。含有存根区域的服务器对此区域没有主管权。
在 Active Directory 中存储区域(只有 DNS 服务器是可写域控制器时才可用)(A)
< 上一步(B)
下一步(N) >
取消

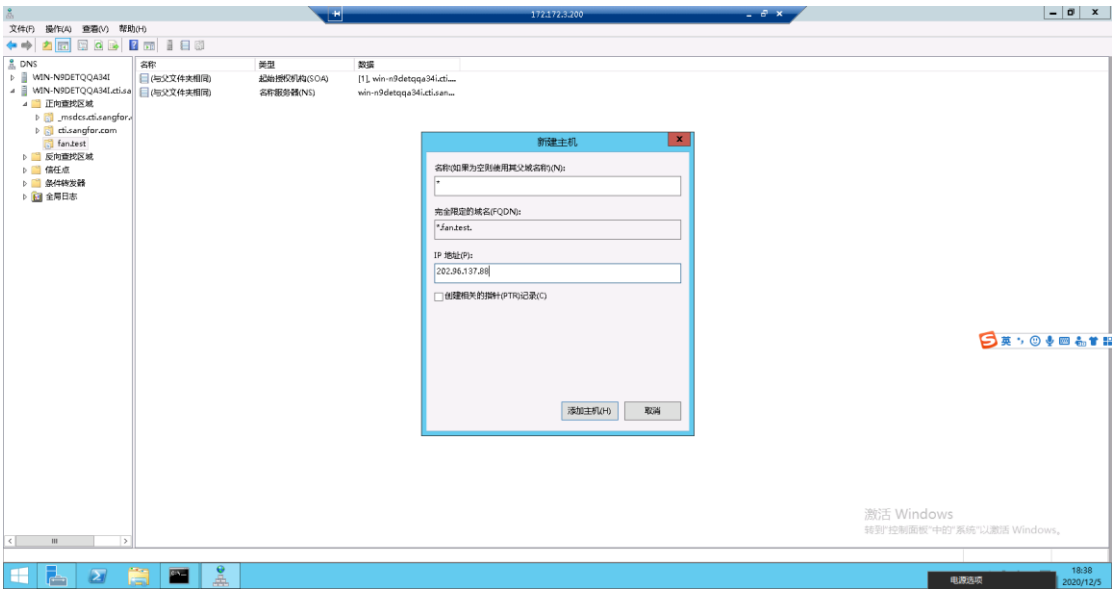

新建区域向导
区域名称
新区域的名称是什么?
区域名称指定 DNS 命名空间的部分，该部分由此服务器管理。这可能是你组织单位的域名(例如，microsoft.com)或此域名的一部分(例如，newzone.microsoft.com)。区域名称不是 DNS 服务器名称。
区域名称(Z):
fan.test
英
< 上一步(B)
下一步(N) >
取消


新建区域向导
区域文件
你可以创建一个新区域文件和使用从另一个 DNS 服务器复制的文件。
你想创建一个新的区域文件，还是使用一个从另一个 DNS 服务器复制的现存文件?
创建新文件，文件名为(C):
fan.test
使用此现存文件(U):
要使用此现存文件，请确认它已经被复制到该服务器上的 %SystemRoot%\system32\dns 文件夹，然后单击"下一步"。
< 上一步(B)
下一步(N) >
取消

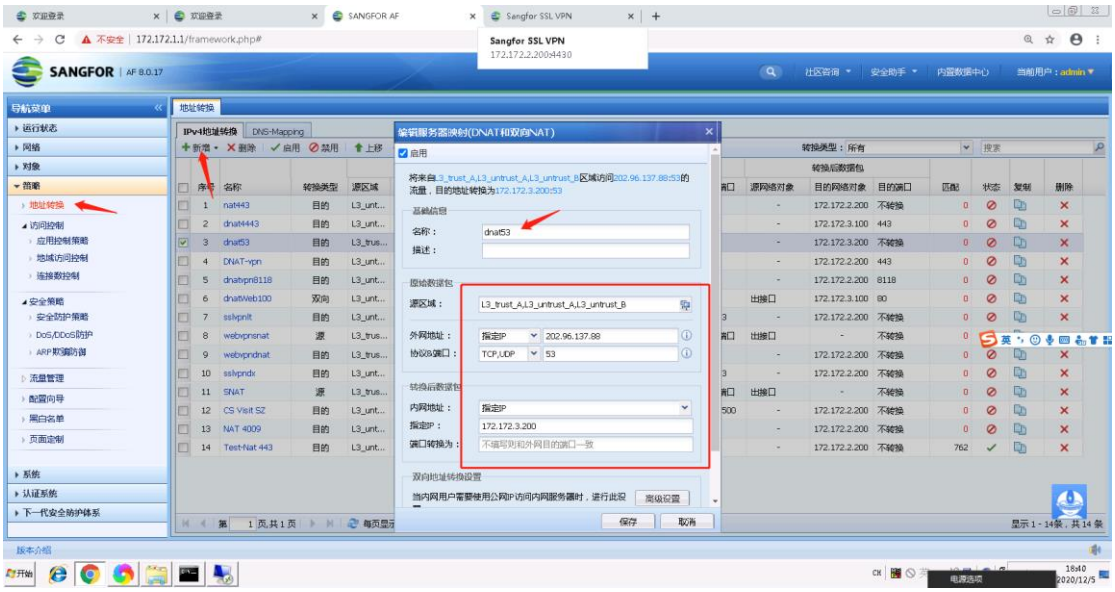

新建区域向导
动态更新
你可以指定这个 DNS 区域接受安全、不安全或非动态的更新。
动态更新能使 DNS 客户端计算机在每次发生更改时，用 DNS 服务器注册并动态更新资源记录。
请选择你要允许的动态更新类型：
只允许安全的动态更新(适合 Active Directory 使用)(S)
Active Directory 集成的区域才有此选项。
允许非安全和安全动态更新(A)
任何客户接受资源记录的动态更新。
因为可以接受来自非信任源的更新，此选项是一个较大的安全弱点。
不允许动态更新(D)
此区域不接受资源记录的动态更新。你必须手动更新这些记录。
< 上一步(B)
下一步(N) >
取消

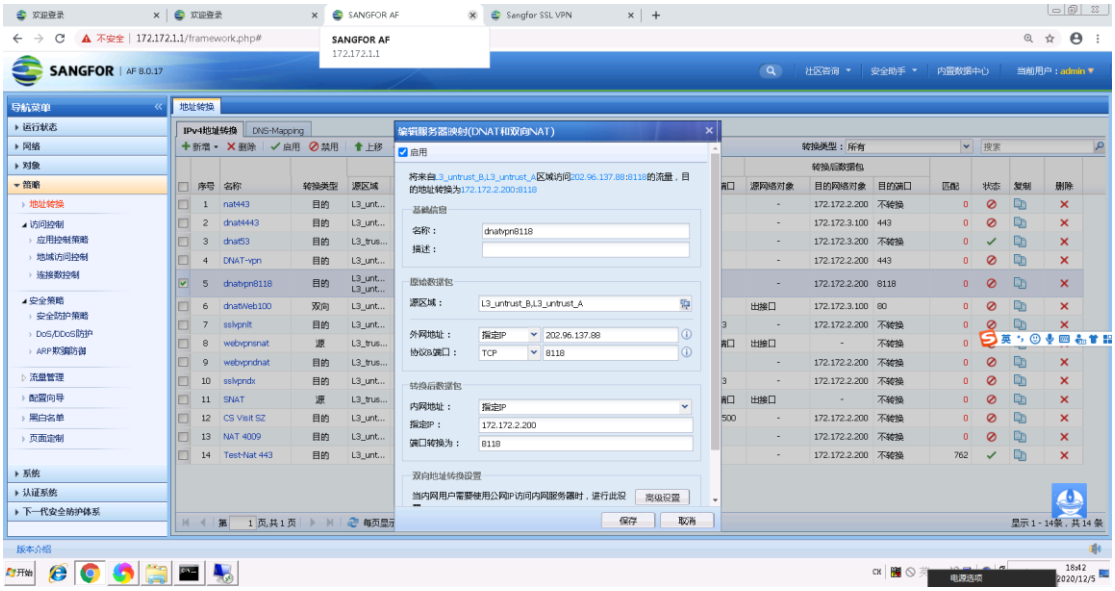

新建区域向导
正在完成新建区域向导
你已成功完成了新建区域向导。你指定了如下设置：
名称: fan.test
类型: 标准主要区域
查找类型: 前进
文件名: fan.test
注意：你应该现在将记录添加到区域，或者确保记录得到动态更新。然后，你可以用 nslookup 验证名称解析。
要关闭此向导并创建新区域，请单击"完成"。
< 上一步(B)
完成
取消


更新服务器数据文件(U)
重新加载(E)
新建主机(A 或 AAAA)(S)...
新建别名(CNAME)(A)...
新建邮件交换器(MX)(M)...
新建域(O)...
新建委派(G)...
其他新记录(C)...
DNSSEC(D)
所有任务(K)
刷新(F)
导出列表(L)...
查看(V)
排列图标(I)
对齐图标(E)
属性(R)
帮助(H)

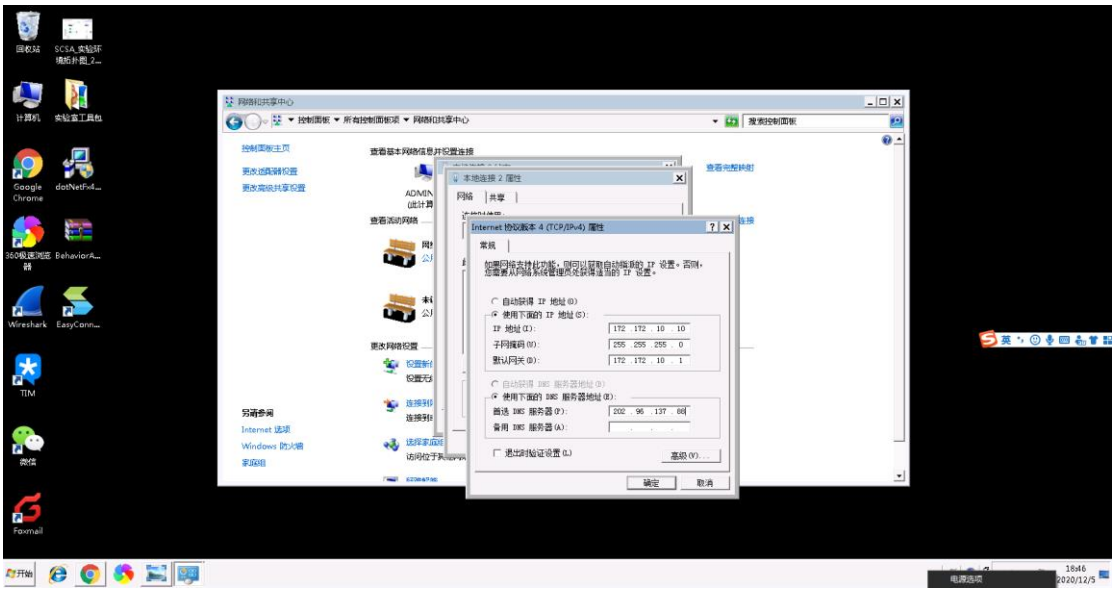

新建主机
名称(如果为空则使用其父域名称)(N):
完全限定的域名(FQDN):
*.fan.test.
IP 地址(P):
202.96.137.88
创建相关的指针(PTR)记录(C)
添加主机(H)
取消

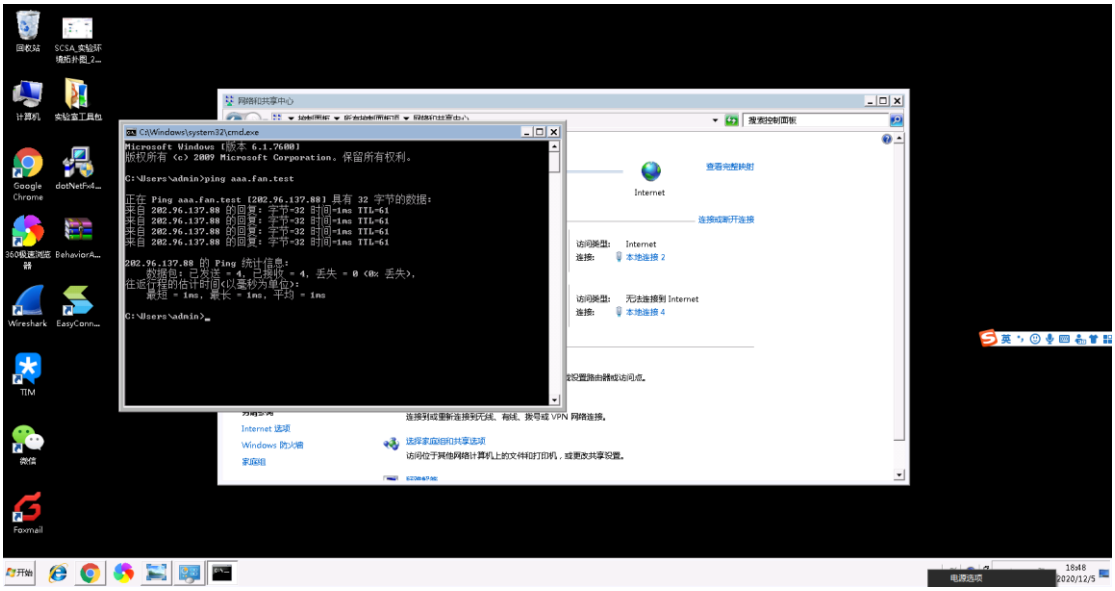
3、 登录 af 配置


SANGFOR AF 8.0.17
Sangfor SSL VPN
172.172.2.200:4430
导航菜单
地址转换
IPv4地址转换
DNS-Mapping
编辑服务器映射(DNAT和双向NAT)
名称：
dnat53
描述：
源区域：
外网地址：
协议&端口：
内网地址：
指定IP：
172.172.3.200
保存
取消

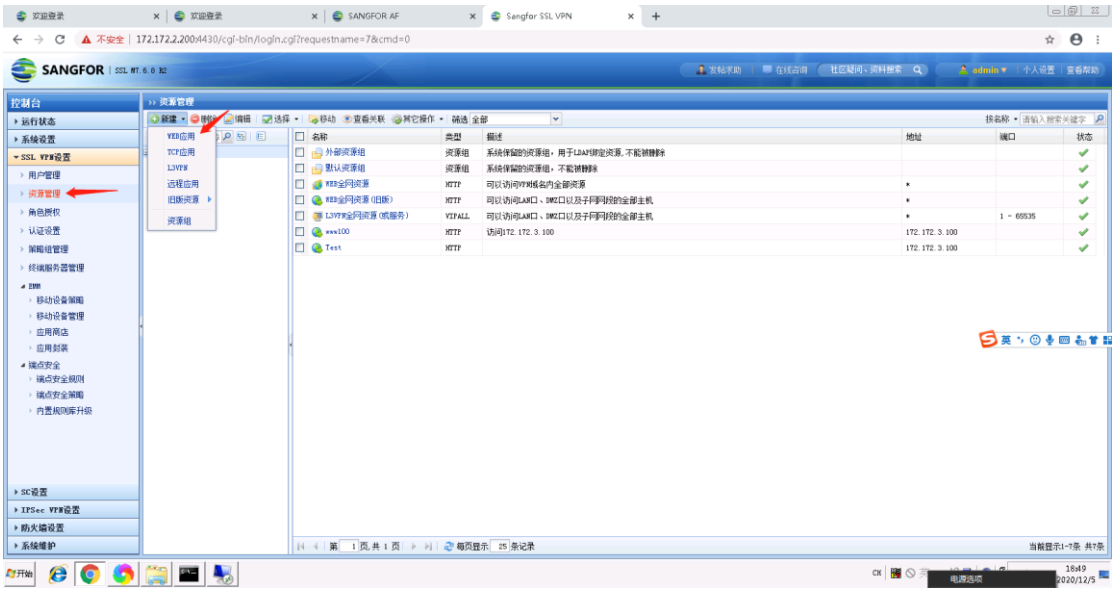

SANGFOR AF
172.172.1.1
SANGFOR | AF 8.0.17
编辑服务器映射(DNAT和双向NAT)

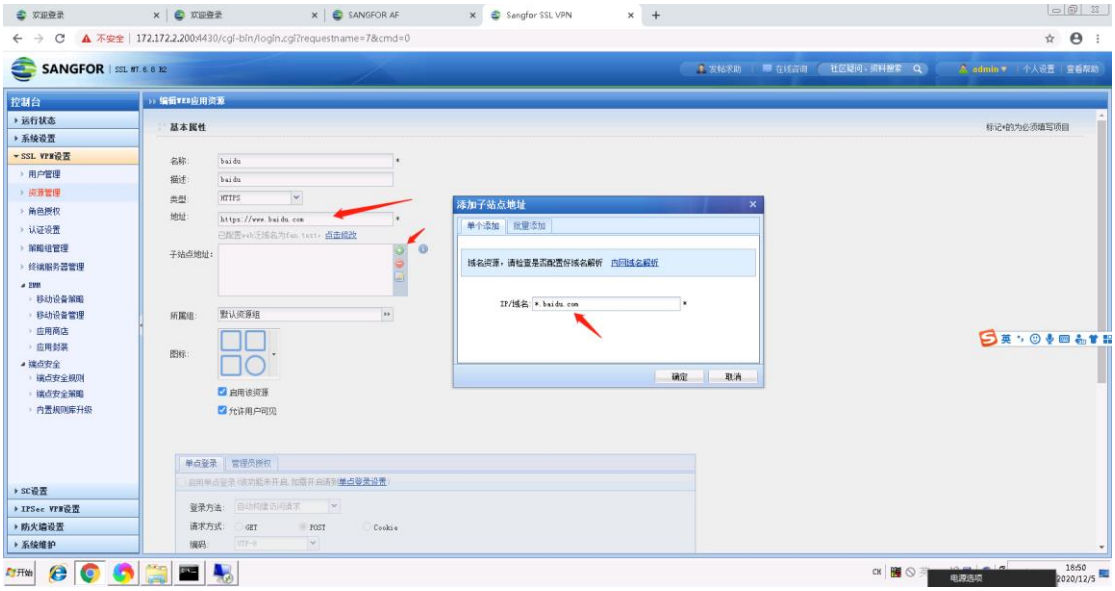
4、 登录长沙，修改 dns


Internet 协议版本 4 (TCP/IPv4) 属性


C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\admin>ping aaa.fan.test
正在 Ping aaa.fan.test [202.96.137.88] 具有 32 字节的数据:
来自 202.96.137.88 的回复: 字节=32 时间=1ms TTL=61
来自 202.96.137.88 的回复: 字节=32 时间=1ms TTL=61
来自 202.96.137.88 的回复: 字节=32 时间=1ms TTL=61
来自 202.96.137.88 的回复: 字节=32 时间=1ms TTL=61
202.96.137.88 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 1ms, 最长 = 1ms, 平均 = 1ms
C:\Users\admin>
网络和共享中心
Internet
本地连接 2
本地连接 4
Internet 选项
Windows 防火墙
家庭组

5、 登录 vpn 新增应用


SANGFOR
172.172.2.200:4430/cgi-bin/loginl.cgi?requestname=7&cmd=0
控制台
运行状态
系统设置
SSL VPN设置
用户管理
资源管理
角色授权
认证设置
策略组管理
终端服务器管理
EMM
移动设备策略
移动设备管理
应用商店
应用封装
端点安全
端点安全规则
端点安全策略
内置规则库升级
SC设置
IPSec VPN设置
防火墙设置
系统维护
资源管理
新建
编辑
选择
移动
查看关联
其它操作
筛选 全部
WEB应用
TCP应用
L3VPN
远程应用
旧版资源
资源组
名称
类型
描述
地址
端口
状态
外部资源组
默认资源组
WEB全网资源
WEB全网资源 (旧版)
L3VPN全网资源 (或服务)
www100
Test

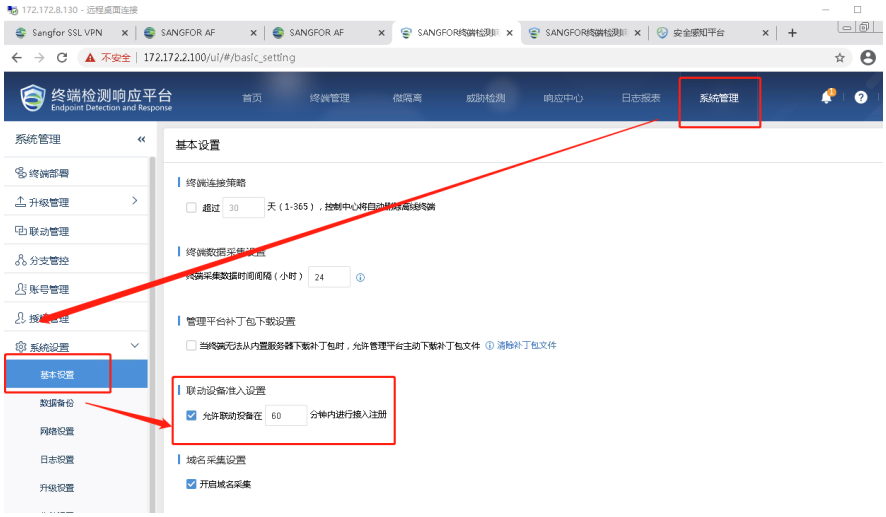

SANGFOR
控制台
运行状态
系统设置
SSL VPN设置
用户管理
资源管理
角色授权
认证设置
策略组管理
终端服务器管理
EMM
移动设备策略
移动设备管理
应用商店
应用封装
端点安全
端点安全规则
端点安全策略
内置规则库升级
SC设置
IPSec VPN设置
防火墙设置
系统维护
编辑WEB应用资源
基本属性
标记*的为必须填写项目
名称:
描述:
类型:
地址:
子站点地址:
所属组:
图标:
启用该资源
允许用户可见
单点登录
管理员授权
登录方法:
请求方式:
编码:
添加子站点地址
单个添加
批量添加
域名资源，请检查是否配置好域名解析
IP/域名:
确定
取消

实验 3 需求如下：

EDR 对接 AF,AC,SIP,抓取恶意流量，观察 rdp 或 ssh 或 smb 或 ftp 暴破情况。

实验 3 步骤如下：

1. EDR 开启联动设置



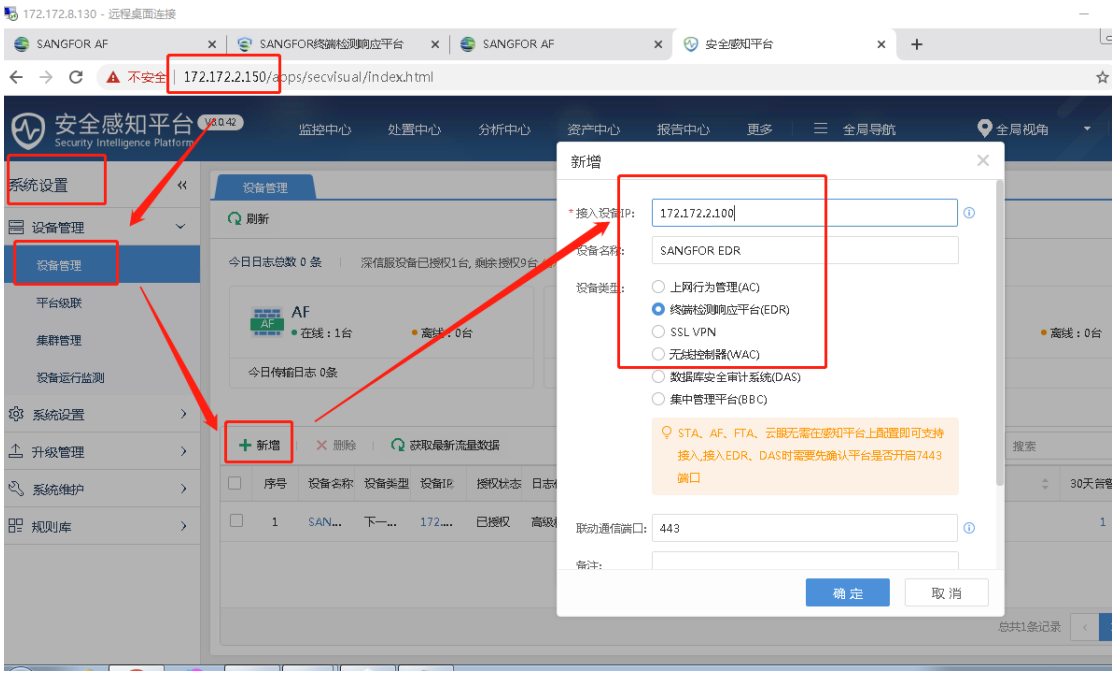
2. EDR 联动 AC

在 AC 上连接 EDR

连接成功

3. EDR 联动 SIP

在 SIP 上操作

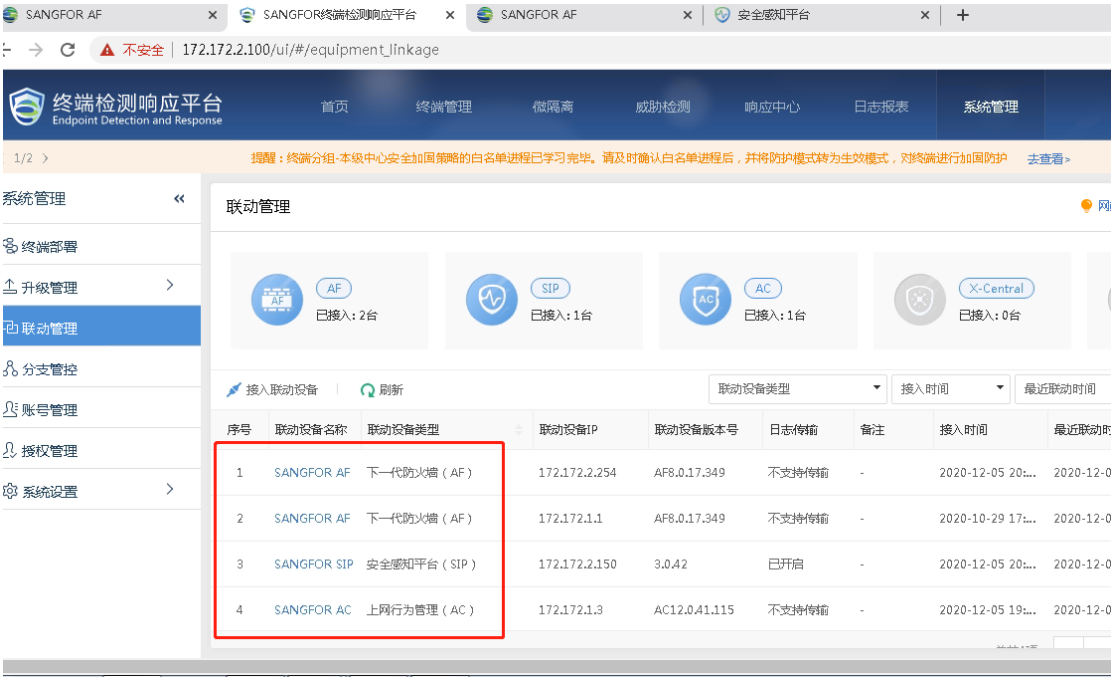



今日日志总数 0 条
深信服设备已授权2台, 剩余授权8台（探针、云眼、文件威胁分析系统不占用授权）
EDR
在线：1台
离线：0台
今日传输日志 0条
AF
在线：1台
离线：0台
今日传输日志 0条
STA
在线：0台
今日传输日志 0条
新增
删除
获取最新流量数据
序号
设备名称
设备类型
设备IP
授权状态
日志传输模式
今日传输
传输日志
今日日志
最近同步时间
设备状态
1
SAN...
下一...
172....
已授权
高级模式
0B
0B
0
2020-12-05 20:13:08
正常
2
SAN...
终端...
172....
已授权
高级模式
0B
0B
-
-
正常

4. EDR 联动 AF

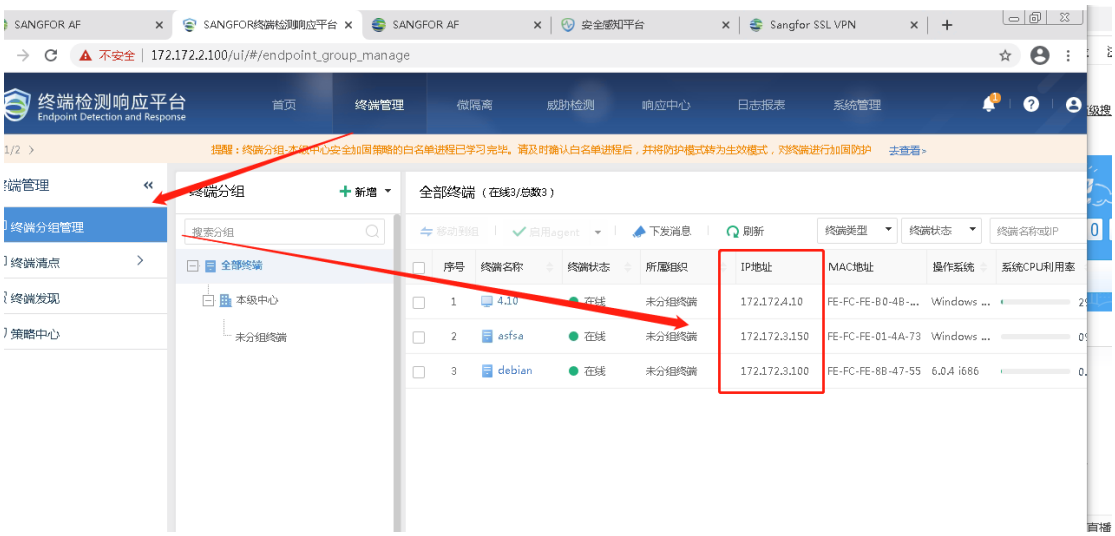

SANGFOR AF
172.172.4.254/framework.php
SANGFOR
网端接入
网端联动安全方案
关联分析
AF
防护更全面
响应更快速
检测更准确
联动处置
网络入侵证据
终端异常线索
EDR
EDR
前往EDR官网
EDR接入设置
如何接入？ 如何购买？
接入方式：
本地EDR管控平台接入
云端EDR管控平台接入
172.172.2.100
立即接入
服务亮点
人工智能，精准识别
协同联动，快速响应

5. EDR 上查看联动状态



6. 观察 rdp 或 ssh 或 smb 或 ftp 暴破情况

现将 edr 终端软件包安装在 172.150.3.150　172.172.3.100 上



cmd 进入爆破工具目录 C:\hydra-8.1-windows

使用命令　hydra.exe -t 4 -V -l administrator -P Passwd.txt rdp://172.172.3.150

hydra.exe -t 4 -V -l root -P Passwd.txt ssh://172.172.3.100

对两个 ip 进行爆破