

网站安全管理中

如何玩好Nginx



河北大学信息技术中心 张彬

CCIE Security 27948



内容提要

- ◆ 不断升级的网站安全管理需求
- ◆ Nginx在校园网的灵活应用
- ◆ 基于Nginx的IPv6网站发布
- ◆ Nginx在安全拓扑的适宜位置

新时代高校数据中心的Web管理需求

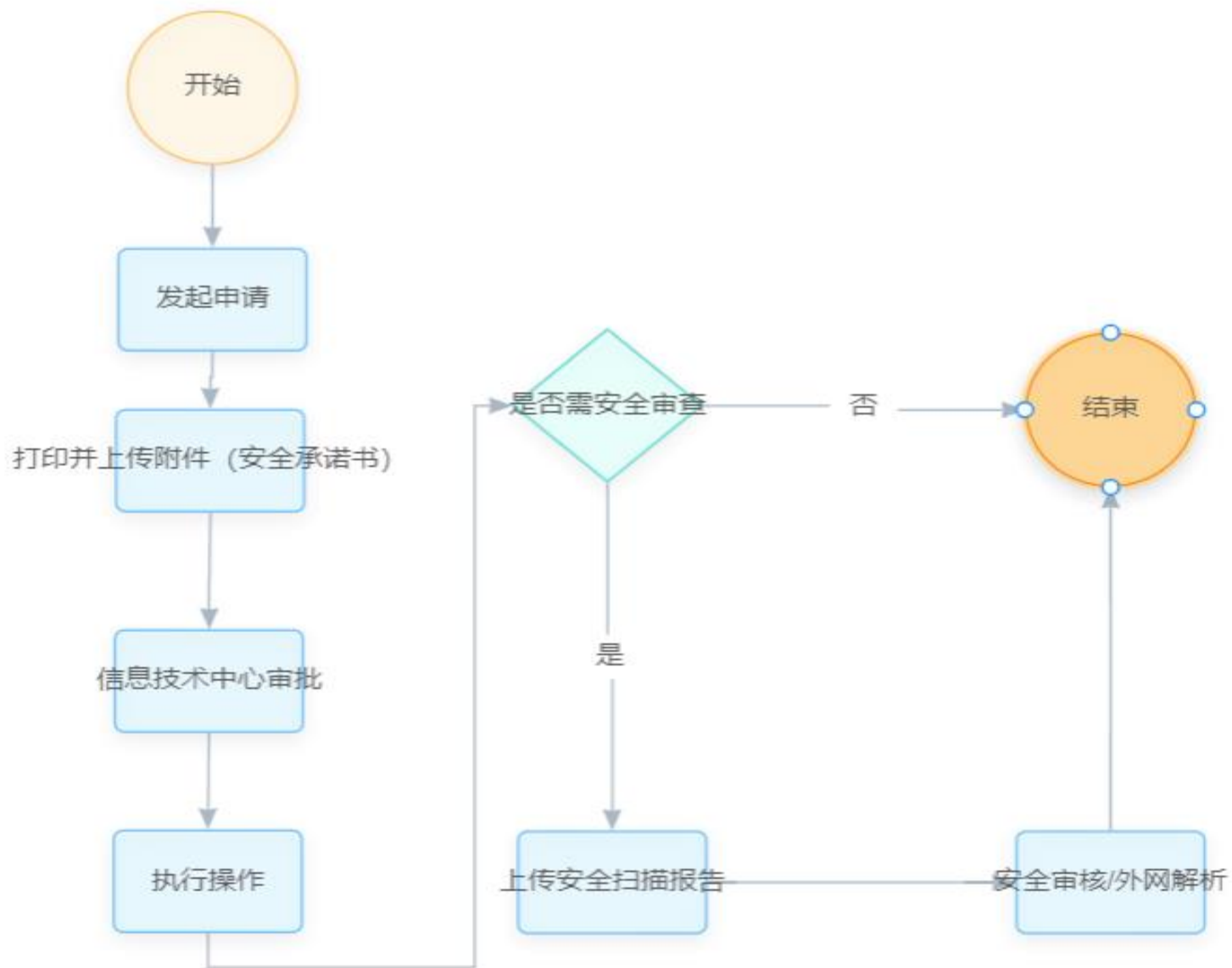
- Web站点发布时不浪费有限的公网地址资源
- 重点时期站点分级分时段开放站点
- 切换出口运营商灵活轻量部署
- 发布外网站点最简化的配置步骤
- 内部站点故障后能够自动切换
- IPv6站点发布不调整网络结构
- 没有发布站点的授权数限制

lǎn

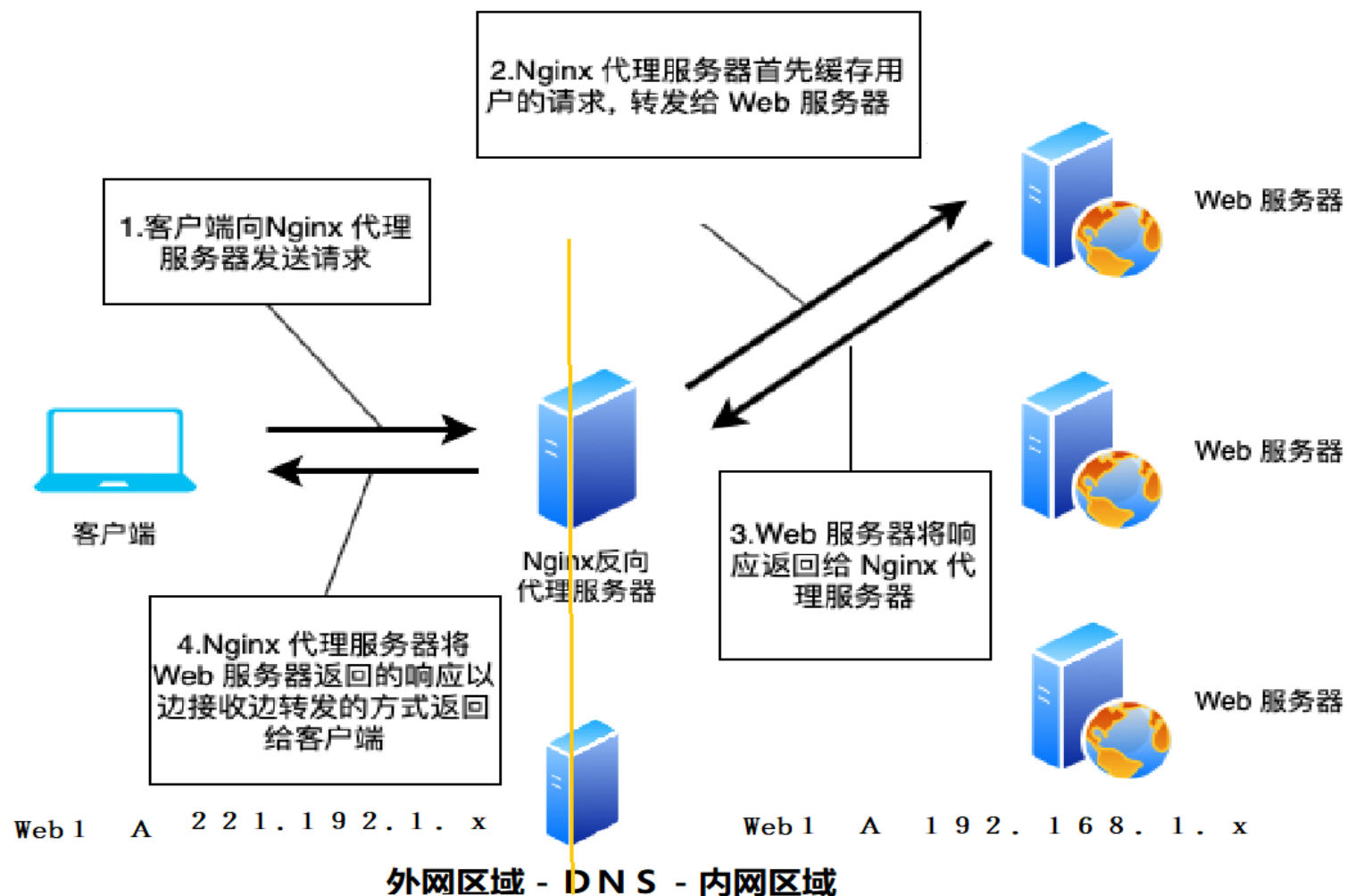
精益求精



网站外网发布流程



Nginx工作机制



传统工作模式的负载均衡与故障监测



```
upstream cluster1 {  
    # simple round-robin  
    server 192.168.0.1:80;  
    server 192.168.0.2:80;  
  
    check interval=3000 rise=2 fall=5 timeout=1000 type=http;  
    check_http_send "HEAD / HTTP/1.0\r\n\r\n";  
    check_http_expect_alive http_2xx http_3xx;  
}  
location /status {  
    check_status;  
    allow SOME.IP.ADD.RESS;  
    deny all;  
}
```

Nginx http upstream check status

Check upstream server number: 3, generation: 7

Index	Upstream	Name	Status	Rise counts	Fall counts	Check type	Check port
0	web_app	.1.114:8080	up	24417	0	http	0
1	web_app	.1.116:8080	up	13787	0	http	0
2	web_app	.1.117:8080	down	0	8	http	0



Nginx分支版本：

Tengine-淘宝网(tengine.taobao.org)



文档

Tengine完全兼容Nginx，因此可以参照Nginx的方式来配置Tengine。

我们在此只列出Tengine中值得注意的功能。

关于详细的Tengine的相对于Nginx的差别，可以访问[变更列表](#)。

Nginx官方文档中文版（不断翻译中）

[Nginx文档](#)

使用

[编译和安装](#)

[命令行参数](#)

模块文档

[主功能](#)

[HTTP核心模块](#)

[动态加载模块功能\(已废弃\)](#)

[Dyups模块](#)

[SPDY模块功能\(已废弃\)](#)

[独立进程模块功能](#)

[backtrace模块功能](#)

[concat模块功能](#)

[其他模块功能](#)

基于Nginx的WEB站点的极简发布

---添加域名的CNANE解析/外网解析 Over。



配置信息

* 类型

☐ A ☐ AAAA ☒ CNAME ☐ CNAME4 ☐ CNAME6 ☐ NS ☐ MX ☐ CAA ☐ SRV ☐ TXT ☐ 显性URL解析 ☐ 隐性URL解析 ☐ 其他

* 记录名称

liuyan

.hbu.edu.cn.

域名解析

线路

线路-默认公网

记录值

cdn

提示: 如CNAME指向外域, 则写完整域名加上后缀".",如"www.baidu.com."

TTL

7200 秒(继承域配置)

多值解析

生命周期设置

长期有效

ON

* 停用时间

请选择生命周期

自动停用

ON

* 开启此选项, 当天早晨0点记录当自动停用

开启到期提醒

OFF

* 开启此选项, 记录到期两周前会发送提醒邮

申请人信息

申请人

信息技术中心

单位

信息技术中心

用途

网上留言板

申请时间

2022-04-27

联系方式

请输入联系方式

☐	名称	类型	值	使用状态	应用线路	创建时间
☐	app	CNAME	cdn(线路-默认公网)	使用中	线路-默认公网	2022-03-22
☐	ks	CNAME	cdn(线路-默认公网)	使用中	线路-默认公网	2022-04-14
☐	liuyan	CNAME	cdn(线路-默认公网)	使用中	线路-默认公网	2022-04-27

IPv4网站的Easy转发

```
server {  
    resolver 202.206.1.31 202.206.1.32 202.206.1.1 202.206.1.2 ipv6=off; --DNS解析内网地址  
    resolver_timeout 60s;  
    listen      80;  
  
    location / {  
        proxy_pass $scheme://$host$request_uri; --直接放通  
        proxy_set_header Host $http_host;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
        proxy_buffers 256 4k;  
        proxy_max_temp_file_size 0;  
        proxy_connect_timeout 60;  
        proxy_cache_valid 200 302 10m;  
        proxy_cache_valid 301 1h;  
        proxy_cache_valid any 1m;  
        allow all;  
    }  
}
```

域名发布安全控制：站点的放通与禁止清单

#hbsite ok 反代内网地址名单放行规则

#只允许特定的域名后缀通过

```
if ($host ~* (hbu.cn|hbu.edu.cn|hicc.cn))
{
    set $flag "ok";
}
```

#some inside site deny 禁止对外发布的域名及IP

```
if ($host ~* (kj.hbu|office.hbu|cwc-query.hbu|10.186.|202.206. ....))
{
    set $flag "deny";
}
```

#禁止名单的返回401错误

```
if ($flag != "ok" ){
    return 401;
}
```

← ↻ ↶ 🏠 | ✓ http://202.206.0.109:9080/

★收藏 ▾ 📁系统管理 📁科研 📁党员学习 📁SSL证书 📁InternetTo 📁技术资料 📁资源 📁MD5 📁python 📁舆情 📁行为感知系 📁Neo4j

401 Authorization Required

This server could not verify that you are authorized to access the document requested. Sorry for the inconvenience. Please report this message and include the following information to us.
Thank you very much!

URL: http://202.206.0.109/
Server: cdn-nginx-20-244
Date: 2022/08/19 23:49:44

Powered by Tengine


```
access_log syslog:server=10.10.0.150,facility=local7,tag=hbu115,severity=info;
```

DPtech

资产

搜索...

Q

当前事件速率(153eps)
当前事件速率(153eps)

系统管理

安全概览

安全监控

事件分析

日志列表

关联事件

审计事件

导出任务管理

报表管理

策略管理

资产管理

日志列表

友情提示: 请尽量输入精确查询条件,查询时系统将返回前10,000条记录。

普通模式

专家模式

查询条件

请选择

时间段类型: 自定义

日期范围: 2022-08-22 00:00:00 - 2022-08-22 23:59:59

采集器: 请选择

名称:

严重级别: 请选择

设备IP: 10.191.20.244

源IP:

目的IP:

设备类型: 请选择

执行动作帐号:

动作对象名称:

动作对象类型:

相关文件名:

高级查询

类型: 请选择

子类: 请选择

标准事件编号:

源主机名:

源端口:

源用户名:

目的主机名:

目的端口:

目的用户名:

其它地址:

其它端口:

结果:

源城市:

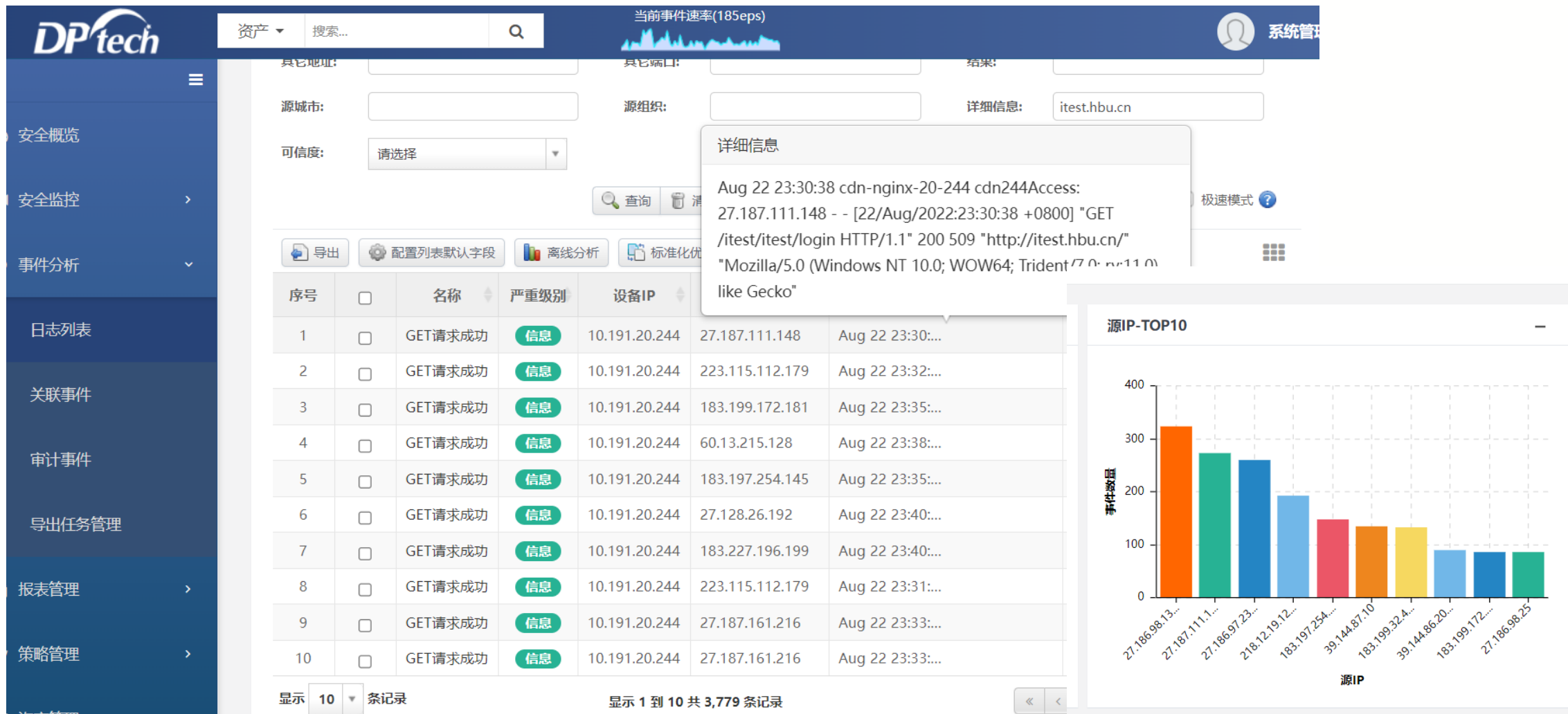
源组织:

详细信息: itest.hbu.cn

第三方日志审计：审计查询、后端分析

#发送访问日志到第三方日志审计设备

```
access_log syslog:server=10.10.0.150,facility=local7,tag=hbu115,severity=info;
```



IPv4站点的Easy IPv6发布

IPv6版本Nginx编译安装

DNS域名解析

(AAAA、CNAME、CNAME6)

或 泛域名AAAA

```
server {  
    listen    80;  
    #IPv6的网络侦听, 以提供IPv6反代  
    listen [::]:80;  
  
    #内网主机为IPv4域名的反代, 注意规避访问IPv6地址, 防止造成回环  
    resolver 202.206.1.31 202.206.1.32 202.206.1.1 202.206.1.2  
    ipv6=off;  
  
    location / {  
        proxy_pass $scheme://$host$request_uri; --直接放通  
        proxy_set_header Host $http_host;  
        proxy_set_header X-Forwarded-For  
        $proxy_add_x_forwarded_for;  
  
        ....  
    }  
}
```

Https->Http的快速部署（内网非https）

```
server{
    listen    443;           --IPv4
    listen [::]:443;        --IPv6
    server_name www.news.hbu.cn news.hbu.cn *.hbu.cn;    --内网不支持https的域名清单
    ssl on;                 --开启SSL
    ssl_certificate /usr/local/nginx/conf/cert/hbu.pem;    --证书
    ssl_certificate_key /usr/local/nginx/conf/cert/hbu.key; --证书
    ....
    location / {
        proxy_pass http://$host$request_uri;            --指向内网http主机头
        proxy_set_header Host $http_host;

        proxy_set_header X-Real-IP $remote_addr;        --真实IP
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    ....
    }

}
```

Https->Http的快速部署（内网非https）

```
server{
    listen    443;           --IPv4
    listen [::]:443;        --IPv6
    server_name www.hbu.cn cxcy.hbu.cn; --内网已支持https的域名清单
    ssl on;                 --开启SSL
    ssl_certificate /usr/local/nginx/conf/cert/hbu.pem; --证书
    ssl_certificate_key /usr/local/nginx/conf/cert/hbu.key; --证书
    ....
    location / {
        proxy_pass https://$host$request_uri; --指向内网http主机头
        proxy_set_header Host $http_host;

        proxy_set_header X-Real-IP $remote_addr; --真实IP
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    ....
    }
}
```

WEB应用 获取真实IP

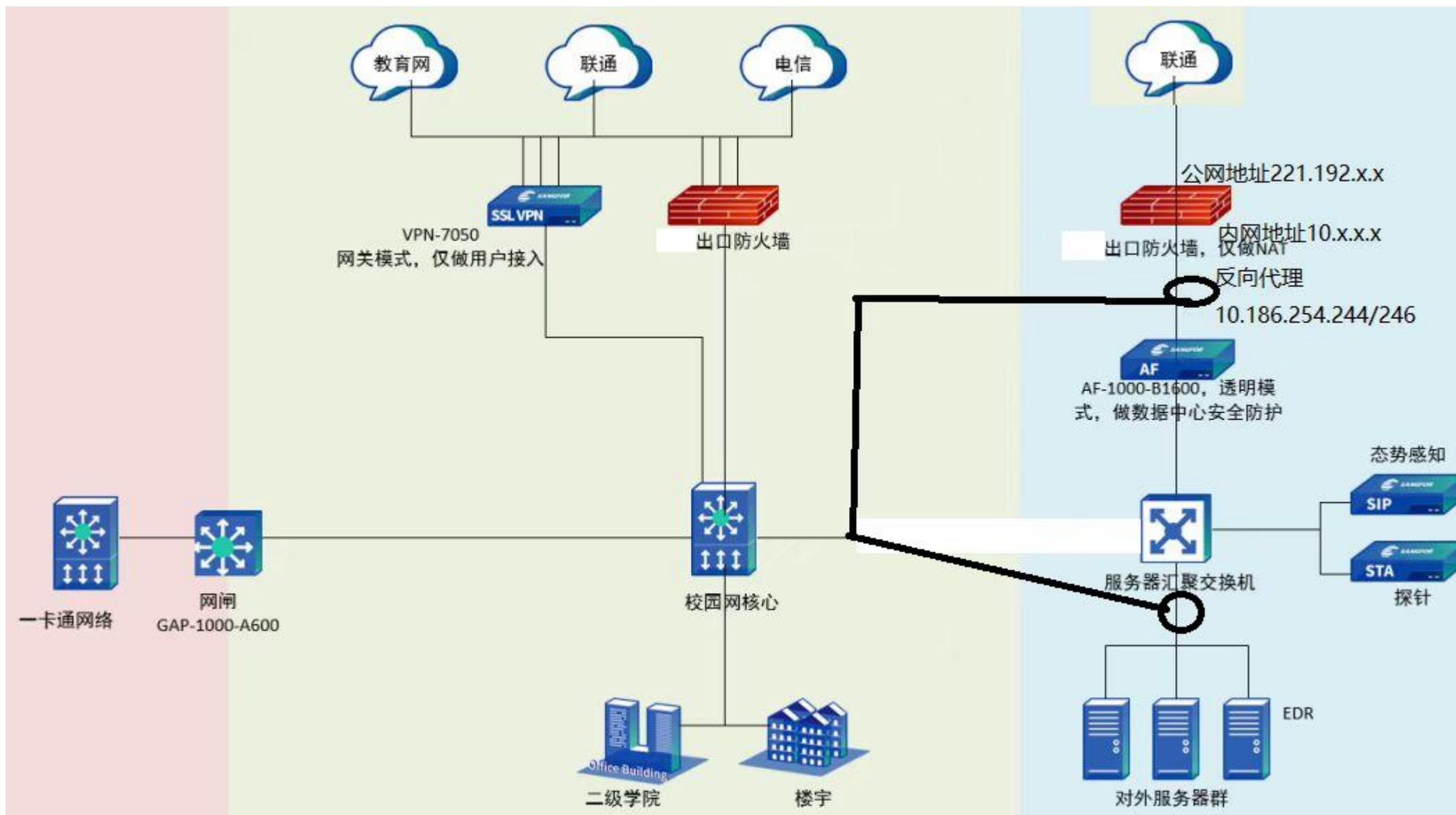
XForward IP:

IPv4
IPv6

审核详情	
河北大学智慧校园头像照片更新	
人员类型	学生
相似度	77.91%
照片库当前照片 本次申请更新的照片 一卡通或身份证	
申请时间	2022-08-22 22:02
申请IP地址	XForward -IPv4源地址 (申请者) 27.186.129.254
审核状态	审核通过
审核人	刘劲松
审核时间	2022-08-22 22:09
审核IP地址	XForward -IPv6源地址 (审核者) 240e:440:5300:1f61:35da:689e:92f0:f6f9

河北大学智慧校园头像照片更新	
人员类型	学生
相似度	77.84%
照片库当前照片 本次申请更新的照片 一卡通或身份证	
申请时间	2022-08-22 19:52
申请IP地址	X-Forwarded-For \$proxy_add x forwarder 2409:8904:5380:d669:2589:caed:3fa8:f866
审核状态	审核通过
审核人	张彬
审核时间	2022-08-22 21:29
审核IP地址	2408:841e:5300:64ec:9d97:e483:919e:4289

Nginx在网络安全防御中的合理位置





**请各位专家
批评指正**

