电子科技大学
WEB资源安全运营

刘仁婷 2022.8.25

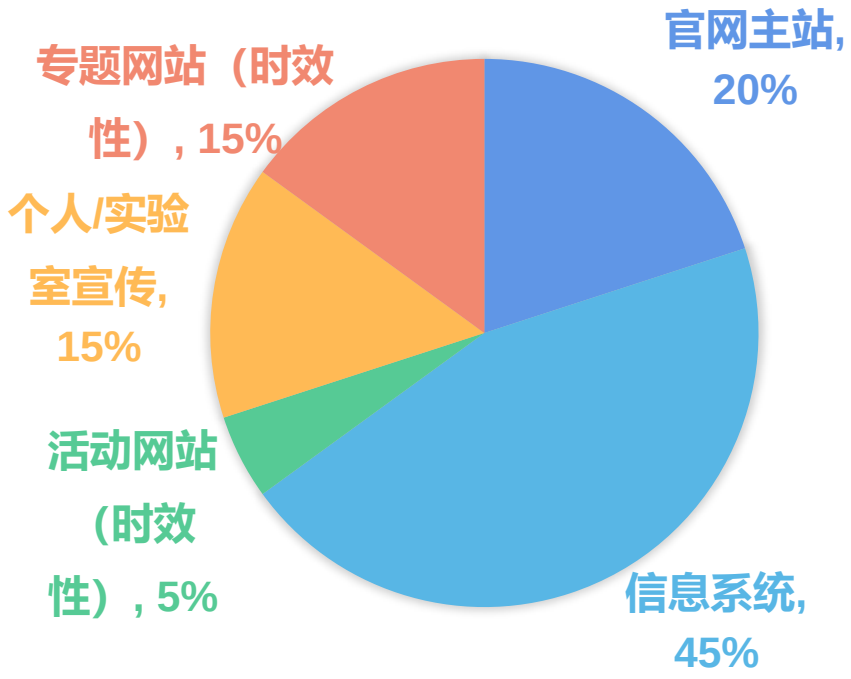
目录

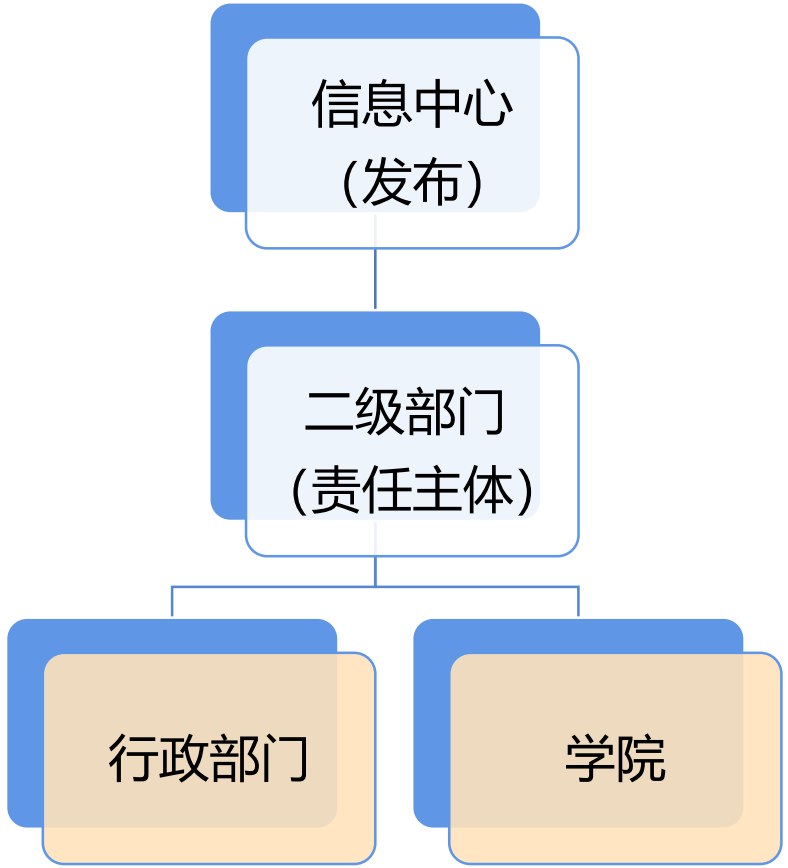
一

电子科技大学WEB资源概况

1 WEB资源概况

- 网站责任归属各二级部门，信息中心负责审核备案、IP&域名分配、审核发布
- 鼓励站群部署，有单独服务器部署；
- 数据中心机房托管/实验室自建；





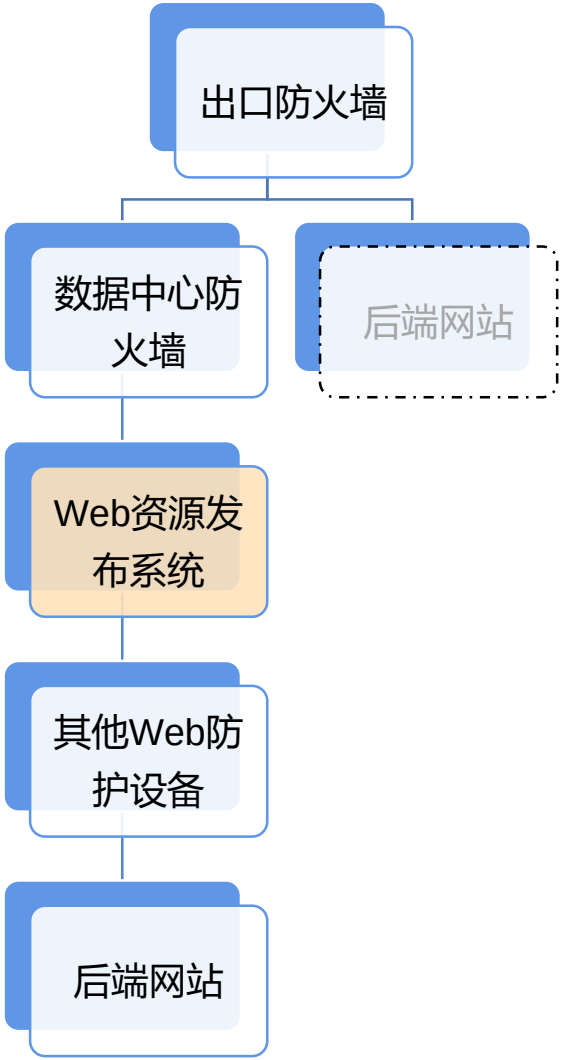
WEB资源日常运营所面临的问题：

- 控制难：实际网站部署散落在校园各处，控制依赖校园网出口访问控制，频繁配置调整存在风险；
- 管理难：网站白名单变动，需要两级双校区防火墙管理员的配合；
- 升级难：网站HTTPS/IPv6升级全部需要在网站所属服务器完成，涉及改造面大，还需要网站维护单位积极配合，管理部门缺少主动权；我校存在www.xx.uestc.edu.cn/xx.uestc.edu.cn此类域名同时生效的情况，四级域名无法使用泛域名证书；
- 安全管理难：网站访问量、可用性、日志等情况未知，难以管控，存在僵尸网站，用户侧部署（数据中心外）的网站缺乏安全防护手段；

二

WEB资源安全运营实践

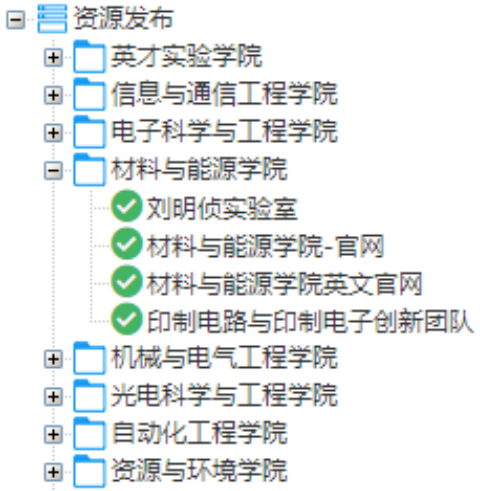
部署架构



- Web资源发布系统部署在数据中心，域名代理模式，物理旁挂，逻辑串联，双机主备
- 用户访问网站的请求均先经过Web资源发布系统到后端网站
- 在Web资源发布系统进行网站白名单控制，防火墙只开放资源发布系统业务IP及端口

2 WEB安全运营实践

400+网站按照所属二级部门分组，统一通过Web资源发布系统发布；
网站访问日志统一查询；



超过80%的网站域名指向Web资源发布系统，未指向网站包括：

- 带宽占用大：视频直播类（在线课堂）、提供本地大文件下载类（正版软件）
- 网站源代码不规范，路径/端口写死： 需要反复调试， “http://XXX” 变换https需要手动找到源代码中链接再进行内容替换更正
- 其他：端口号过多、通报定位到Web资源发布系统IP，但未定位域名、虚仿类

- 为每个网站分类，制定发布策略
  - 是否站群
  - 是否官网
  - 是否白名单
- 白名单分类
  - 重保白名单
  - 常态化白名单
  - 专项白名单
- 白名单网站后台管理路径：限制校内访问

策略名称	生效网站	操作
限校内	共 个	编辑 删除
站群-官网	共 个	编辑 删除
站群-非官网	共 个	编辑 删除
非站群-官网	共 个	编辑 删除
非站群-非官网	共 个	编辑 删除
废弃-待回收	共 个	编辑 删除
禁VPN	共 个	编辑 删除
重保白名单-非官网	共 个	编辑 删除
常态化白名单	共 个	编辑 删除
限信息中心内部	共 个	编辑 删除
2022专项白名单	共 个	编辑 删除

cwcx.uestc.edu.cn

很抱歉，您没有权限访问该网站，可能是您不在校园网内,没有使用VPN或者资源路径错误

- 您(IP：118.112.138.1)，没有权限访问相应的资源(https://cwcx.uestc.edu.cn/)，请通过校园网或者VPN获取相应的访问权限
- 您所访问的资源(https://cwcx.uestc.edu.cn/)，可能存在配置时路径错误，请联系管理员修改相关配置

(错误代码：403)

网站活跃度监测

☐	紧急	（网站）[redacted]图书馆公共服务部巡检系统	无法正常访问，原因：被代理后端URL无法从工作节点访问	2022-08-07 20:31:01	未确认已恢复，恢复时间: 2022-08-07 21:00:39
☐	紧急	（网站）[redacted]图书馆统一应用管理平台	无法正常访问，原因：被代理后端URL无法从工作节点访问	2022-08-07 20:31:01	未确认已恢复，恢复时间: 2022-08-07 21:00:39
☐	紧急	（网站）[redacted]图书馆-微信	无法正常访问，原因：被代理后端URL无法从工作节点访问	2022-08-07 20:31:00	未确认已恢复，恢复时间: 2022-08-07 21:00:35
☐	紧急	（网站）[redacted]自助借还相关接口服务	无法正常访问，原因：被代理后端URL无法从工作节点访问	2022-08-07 20:31:00	未确认已恢复，恢复时间: 2022-08-07 21:00:37
☐	紧急	（网站）[redacted]万方镜像（含医学库）、万方视频	无法正常访问，原因：被代理后端URL无法从工作节点访问	2022-08-07 20:31:00	未确认已恢复，恢复时间: 2022-08-07 21:00:37

	告警等级	告警对象	告警内容	触发时间
☐	警告	（网站）[redacted]电子科技大学可视化校园	检测到该网站已经连续192天处于不活跃状态，请酌情处理。	2022-07-27 08:40:16
☐	警告	（网站）[redacted]电子校友卡	检测到该网站已经连续211天处于不活跃状态，请酌情处理。	2022-07-08 09:07:57
☐	警告	（网站）[redacted]电子科技大学终身学习平台	检测到该网站已经连续216天处于不活跃状态，请酌情处理。	2022-07-03 09:15:46
☐	警告	（网站）[redacted]—代码托管	检测到该网站已经连续216天处于不活跃状态，请酌情处理。	2022-07-03 09:12:25
☐	警告	（网站）[redacted]电子科技大学学生事务中心	检测到该网站已经连续216天处于不活跃状态，请酌情处理。	2022-07-03 08:22:03

- 自动监控网站可达性；
- 筛查不活跃网站，定义僵尸网站为连续180天不活跃状态，定期停止发布僵尸网站；

日志溯源，与态势感知配合（XFF）

时间	网站名	IP	用户名	状态码	请求方式	访问路径	终端	后端地址	后端响应时长	反代处理时长
2022-08-08 14:09:16	财务处缴费平台	202.115.1.244	-	304	GET	/payment/jquery/ui.dialog.min.js	Chrome 104.0.5112/Windows 10	[redacted]	0.006s	0.006s
2022-08-08 14:09:16	电子科技大学就业网	125.36.119.9(天津市)	-	200	GET	/career/images/top.png	Chrome 104.0.0/Windows 10	[redacted]	0.001s	0.000s
2022-08-08 14:09:16	财务处缴费平台	202.115.1.244	-	304	GET	/payment/style/theme/ui.slider.css	Chrome 104.0.5112/Windows 10	[redacted]	0.005s	0.001s
2022-08-08 14:09:16	电子科技大学就业网	125.36.119.9(天津市)	-	200	GET	/career/images/online.png	Chrome 104.0.0/Windows 10	[redacted]	0.001s	0.000s
2022-08-08 14:09:16	本科招生网-别名	182.111.159.62(江西-...	-	200	GET	/static/wap/js/weui.min.js	Chrome Mobile 89.0.4389/Android	[redacted]	0.001s	0.001s

网站：访问最多网站 更多

网站	次数
财务处缴费平台	528668
财务综合信息门户	375526
研究生系统（老系统）	359227
教师主页	244088
科研财务管理系统	230613
研究生招生网	216582
精准思政	164525
网上预约系统	164255

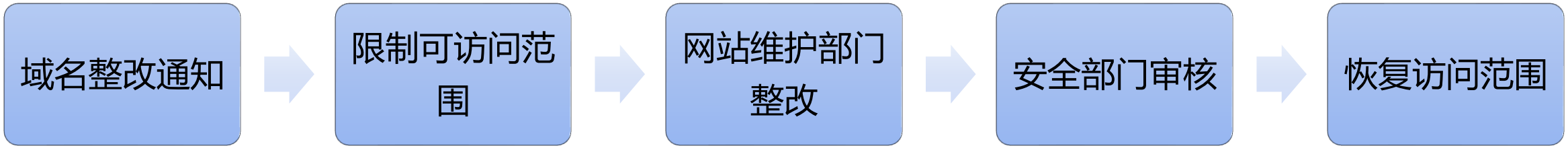
网站：访问最多IP 更多

IP	次数
125.69.68.106(四川省-成都)	271129
202.112.14.6	79127
223.101.45.195(辽宁-沈阳)	51437
8.136.14.245	43260
222.197.166.48	35437
202.115.1.244	14607
113.54.157.156(四川省-成都)	13861
113.54.152.151(四川省-成都)	13022

网站上线管理

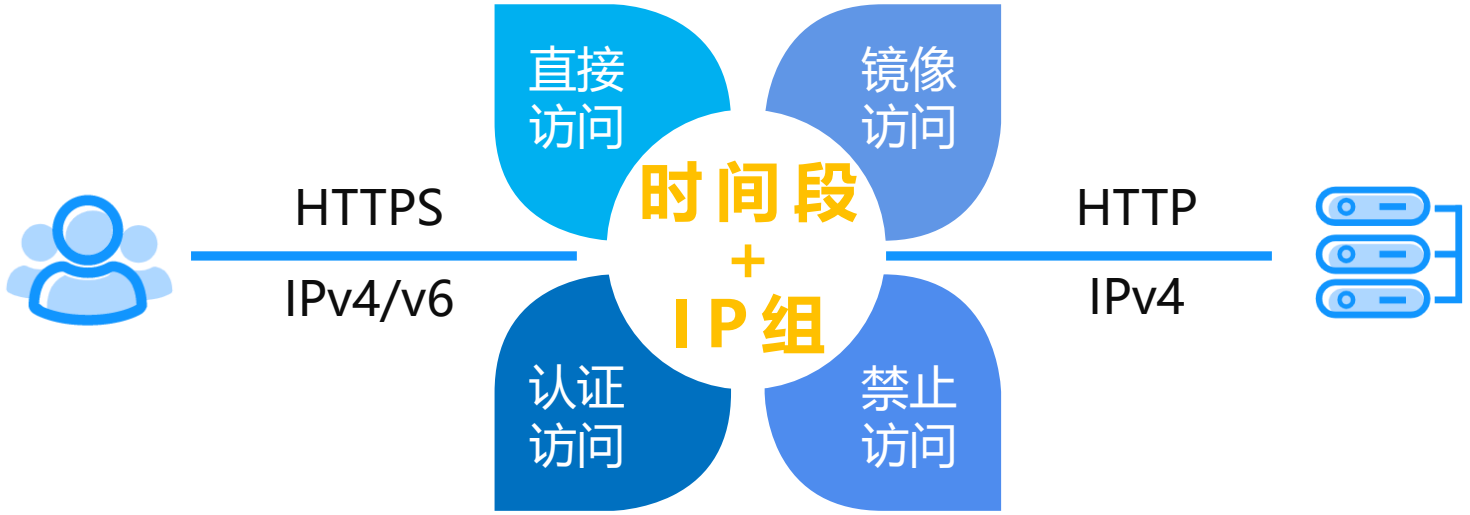
- 用户申请新域名，DNS新增域名均指向Web资源发布系统，通过Web资源发布系统进行发布配置、备案、访问策略；
- 提出管理需求：通过反代和DNS两系统联动，在反代系统添加资源的同时，同步信息至DNS系统，完成A/AAAA记录添加，简化工作流程

网站安全通报管理



- 网站被通知整改，先通过反代将其限制为仅校内可以访问，网站整改完成审核后，再重新恢复公网访问
- 一键断网：反代后台/微信公众号/微信小程序

访问策略、时间段控制、 https&Ipv6一键升级



- HTTPS支持：通过反代进行HTTPS升级改造，避免了各个服务器单独改动的巨大工作量；反代提供www.xx.uestc.edu.cn等四级域名证书申请和自动续期，弥补泛域名证书支持度不全的问题。
- IPv6升级：通过反代进行IPv6升级，后端网站服务器不变，简化IPv6升级改造工作。

发布策略

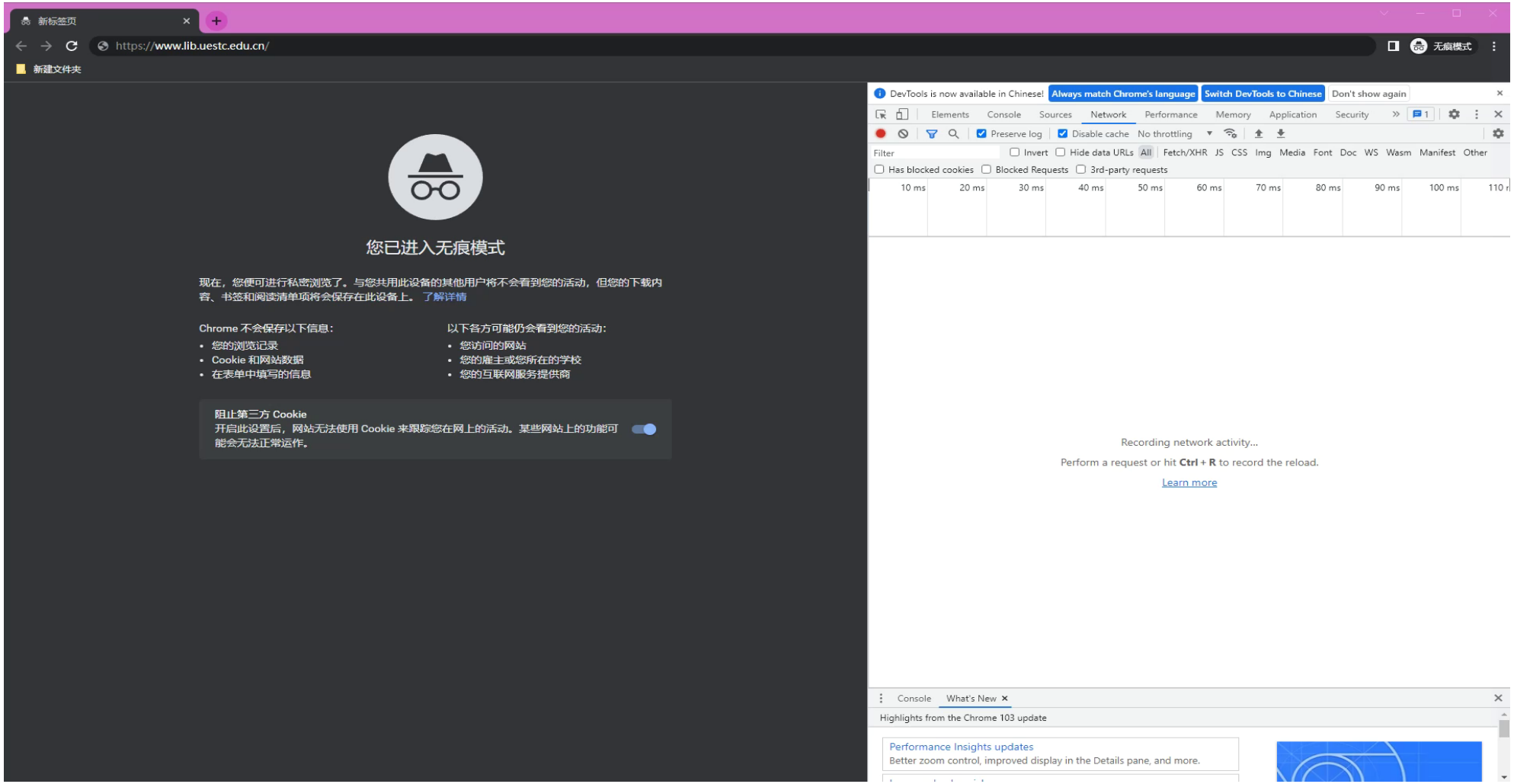
时间段 每日 7:00 – 18:00

IP组 国内校外IP

访问方式

- ○ 直接访问
- ◉ 认证访问 —— 选择用户组
- ○ 禁止访问
- ○ 镜像访问

IPv6支持


新标签页
https://www.lib.uestc.edu.cn/
无痕模式
新建文件夹
您已进入无痕模式
现在，您便可进行私密浏览了。与您共用此设备的其他用户将不会看到您的活动，但您的下载内容、书签和阅读清单项将会保存在此设备上。 了解详情
Chrome 不会保存以下信息：
• 您的浏览记录
• Cookie 和网站数据
• 在表单中填写的信息
以下各方可能仍会看到您的活动：
• 您访问的网站
• 您的雇主或您所在的学校
• 您的互联网服务提供商
阻止第三方 Cookie
开启此设置后，网站无法使用 Cookie 来跟踪您在网上的活动。某些网站上的功能可能会无法正常运作。
DevTools is now available in Chinese!
Always match Chrome's language
Switch DevTools to Chinese
Don't show again
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
All
Fetch/XHR
JS
CSS
Img
Media
Font
Doc
WS
Wasm
Manifest
Other
Has blocked cookies
Blocked Requests
3rd-party requests
10 ms
20 ms
30 ms
40 ms
50 ms
60 ms
70 ms
80 ms
90 ms
100 ms
Recording network activity...
Perform a request or hit Ctrl + R to record the reload.
Learn more
Console
What's New
Highlights from the Chrome 103 update
Performance Insights updates
Better zoom control, improved display in the Details pane, and more.

- 内链IPv6支持度：
  - 二级链接：96.48%
  - 三级链接：94.71%
  - 评分：96.48

省市	学校名称	门户网站	可解析	可访问	二级内链支持度	三级内链支持度	IPv6支持度评分	活跃用户数	入流量平均带宽(Mbps)	出流量平均带宽(Mbps)
四川	电子科技大学	www.uestc.edu.cn	是	是	96.48%	93.47%	95.98	42,430	364.39	69.67

《电子科技大学校内域名管理办法（试行）》

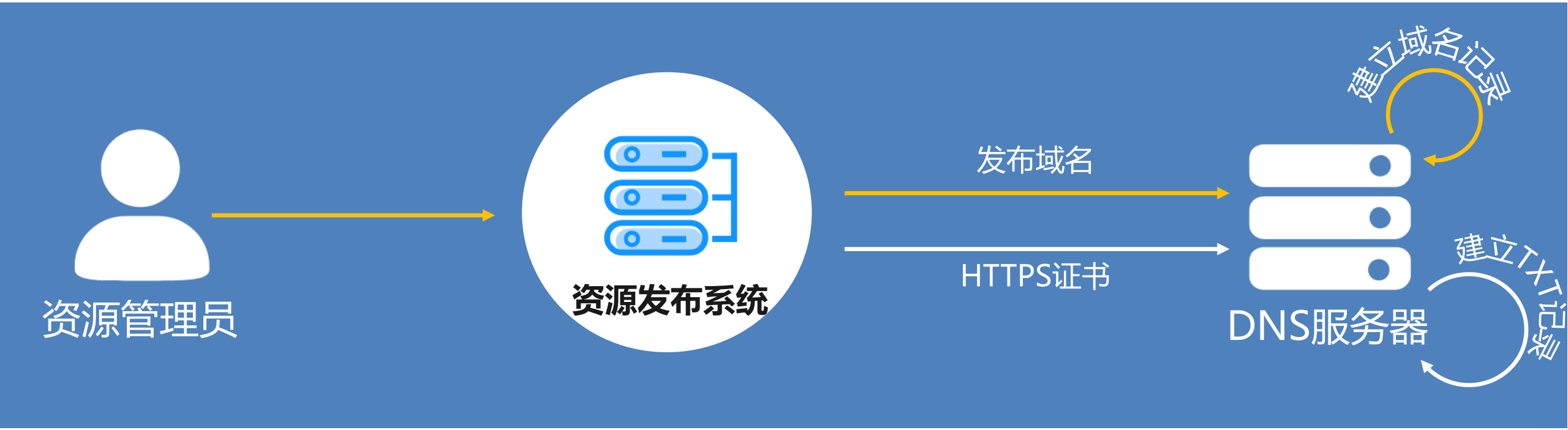
第四条 原则上所有校内域名都由信息中心维护的反向代理统一对校外发布，对校外发布的端口原则上仅支持80、443和8080。信息中心将依据反向代理对域名的活跃和维护情况进行评估，暂停发布6个月内无访问记录或被代理后端无法正常访问的域名。

第五条 所有校内域名都要求加载SSL证书。信息中心统一提供二级域名的SSL证书，暂不支持三级域名的SSL证书。

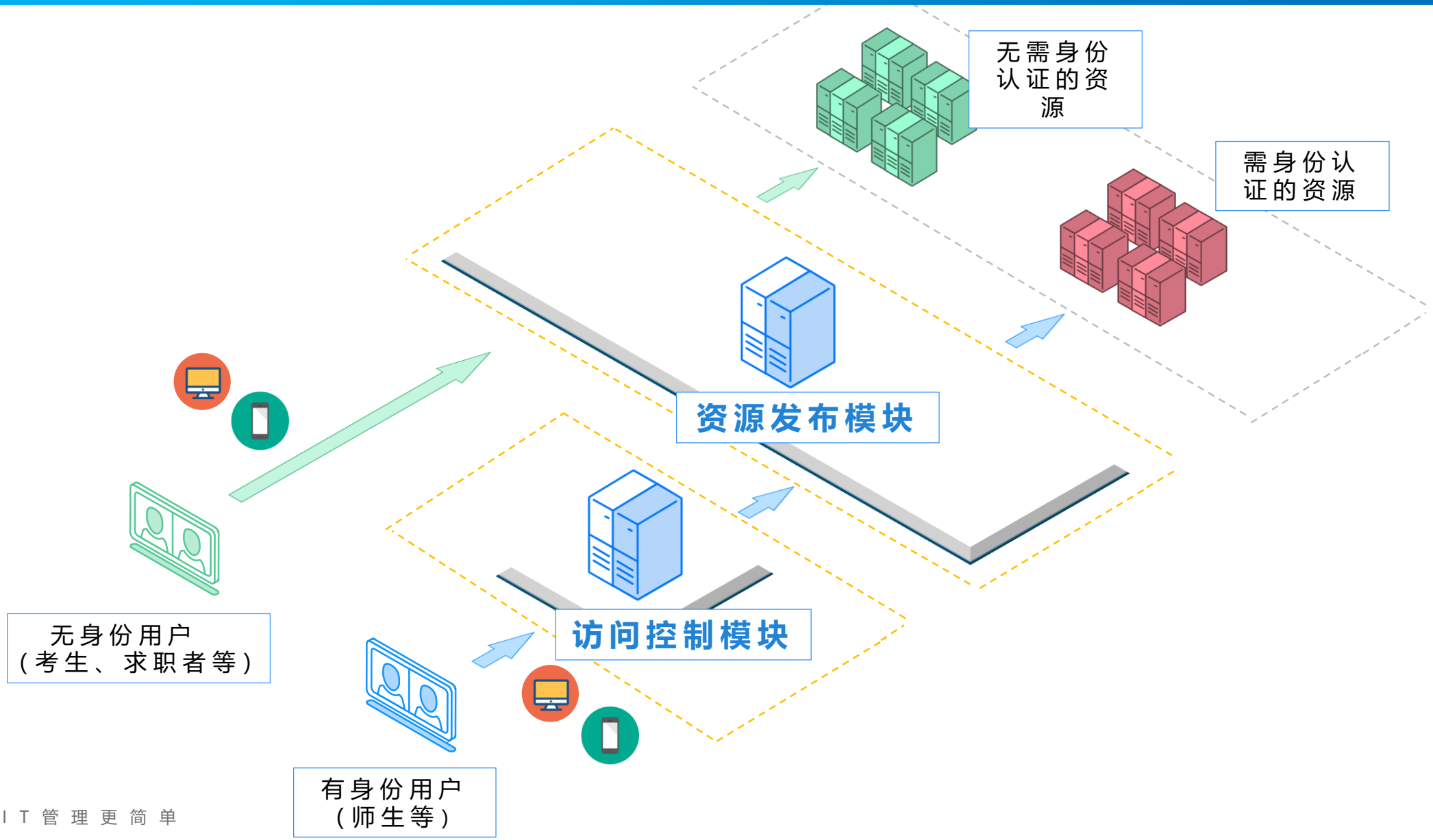
三

WEB资源安全运营展望和扩展

3 网站发布过程尽可能自动化



3 网站发布安全性与便利性的平衡



谢 谢！