ArcGIS Server 10.1 服务安全设计策略

Esri中国北京有限公司

行业技术部　程 杰

esri China BEIJING
分 享 地 理 价 值

内容

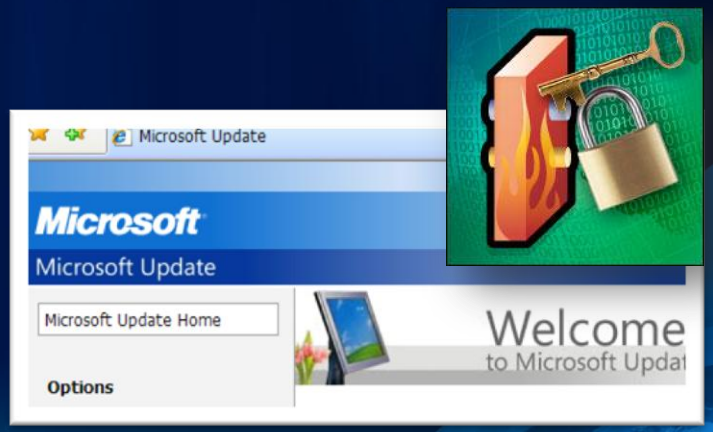
- 企业级GIS安全概述
- ArcGIS Server安全配置
  - 用户与角色
  - 服务安全
  - 保护缓存目录
  - Token验证
  - HTTP验证
  - 防火墙
  - 集成安全 ***

esri China BEIJING
分 享 地 理 价 值

企业级GIS安全概述

安全性概述

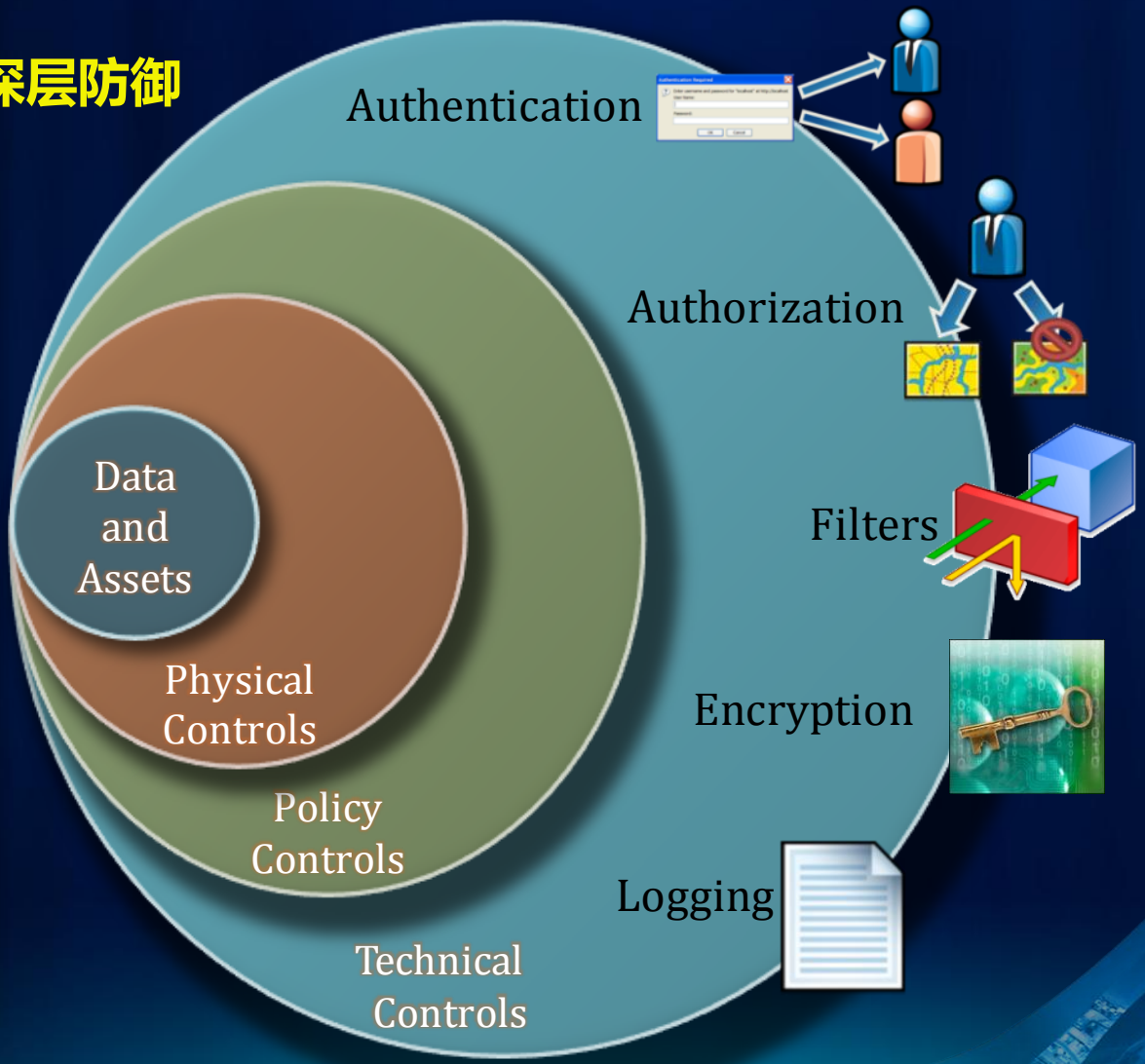
- 访问安全
  - 只有经过授权的合法用户才能访问特定的资源
    - 合法的用户
    - 经过授权
- 传输安全
  - 对敏感信息在传输过程中的加密
- 其他：
  - 操作系统-升级、防病毒
  - 代码-SQL注入
  - 用户培训
  - 网络钓鱼
  - ……



esri China BEIJING
分 享 地 理 价 值

ESRI的安全策略

- 深层防御



esri China BEIJING
分 享 地 理 价 值

ArcGIS Server 一般的安全模型

请求资源 → 身份证明 → 角色映射 → 角色评估和授权

Browser/Desktop Applications

Web

认证\验证

Principal Store (Users & Roles)

Web server

Web service handler

Token service

Web applications

认证\验证

查看/配置

授权

cluster

Permission Store (for services)

GIS Services

Manager

配置

esri China BEIJING
分 享 地 理 价 值

GIS安全模式

- **安全模式的选择**

- 基本模式
  - 不敏感的数据– 公共信息
  - 所有架构层都可以部署在一个服务器上
- 标准模式
  - 数据丢失或者完整性破坏会有一定的影响
  - 架构层部署到多个单独的系统
  - 可能需要联合服务
- 高级模式
  - 敏感的数据
  - 所有组件采用冗余配置以保证高可用性
  - 使用第三方企业安全性组件

esri China BEIJING
分 享 地 理 价 值

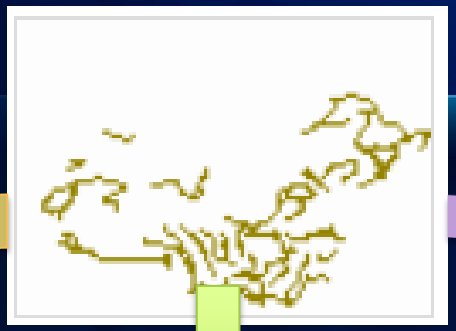
ArcGIS Server安全配置

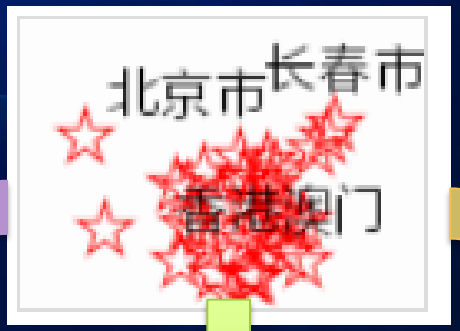
用户与角色
服务安全
保护缓存目录
Token验证
HTTP验证
防火墙
集成安全性

用户和角色

- 角色：控制访问服务资源
- 用户：通过控制拥有某个角色的权限，从而控制访问服务资源的权限

esri China BEIJING
分 享 地 理 价 值





admin
ROLE1
user1

admin
ROLE2
user2

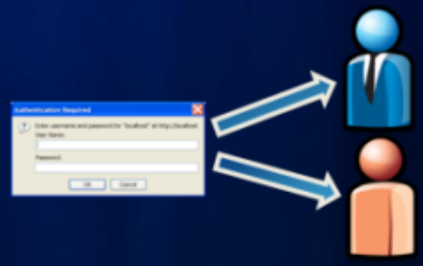
user1

admin

user2

esri China BEIJING
分 享 地 理 价 值

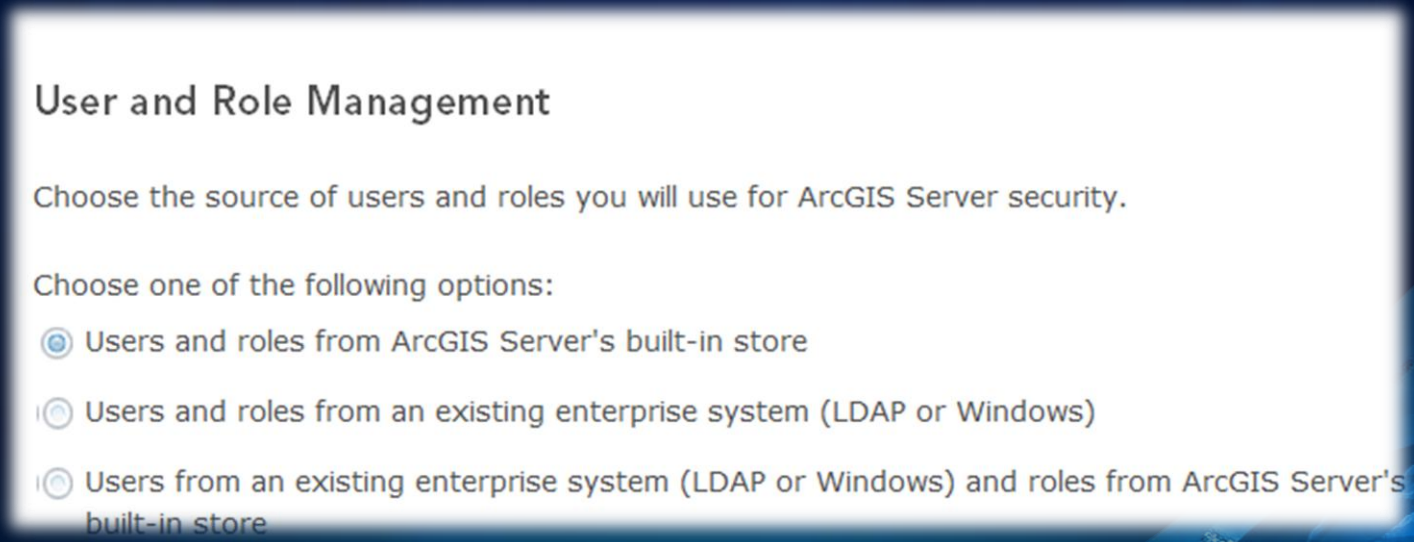
用户和角色存储



ArcGIS Server内嵌存贮

Lightweight Directory Access Protocol(LDAP) 或者 Windows用户和组

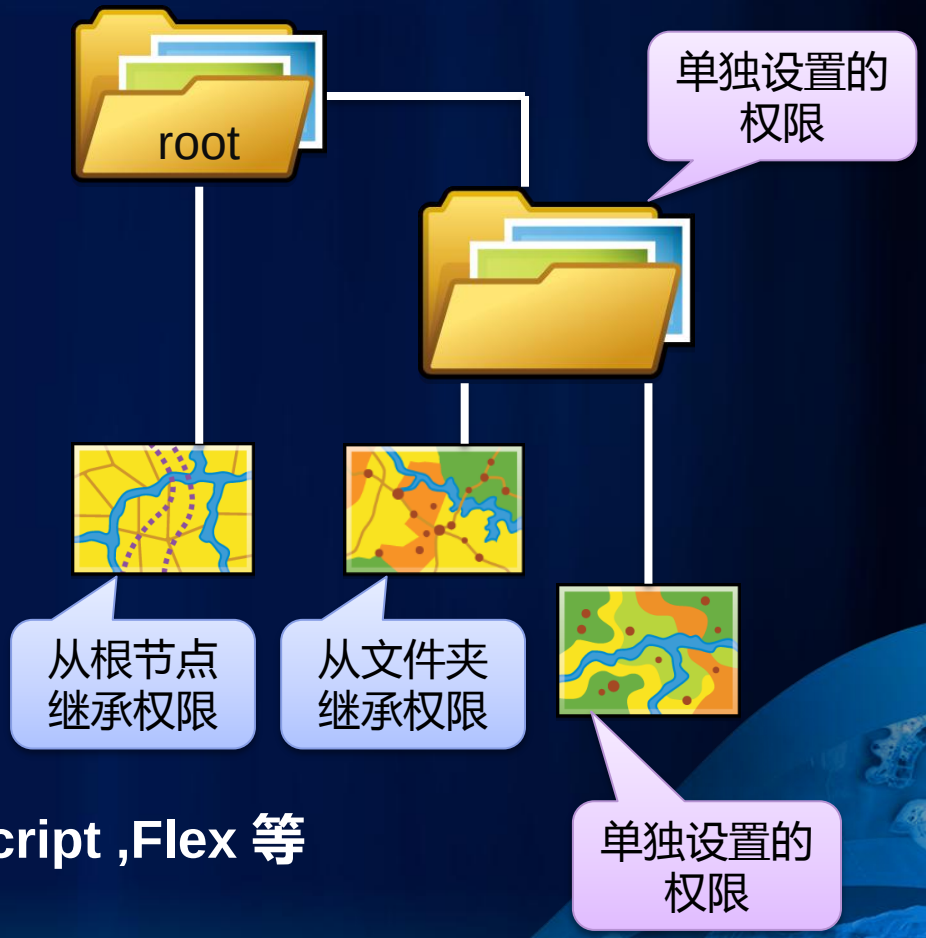
用户和角色分开存贮



esri China BEIJING
分 享 地 理 价 值

GIS Web 服务安全

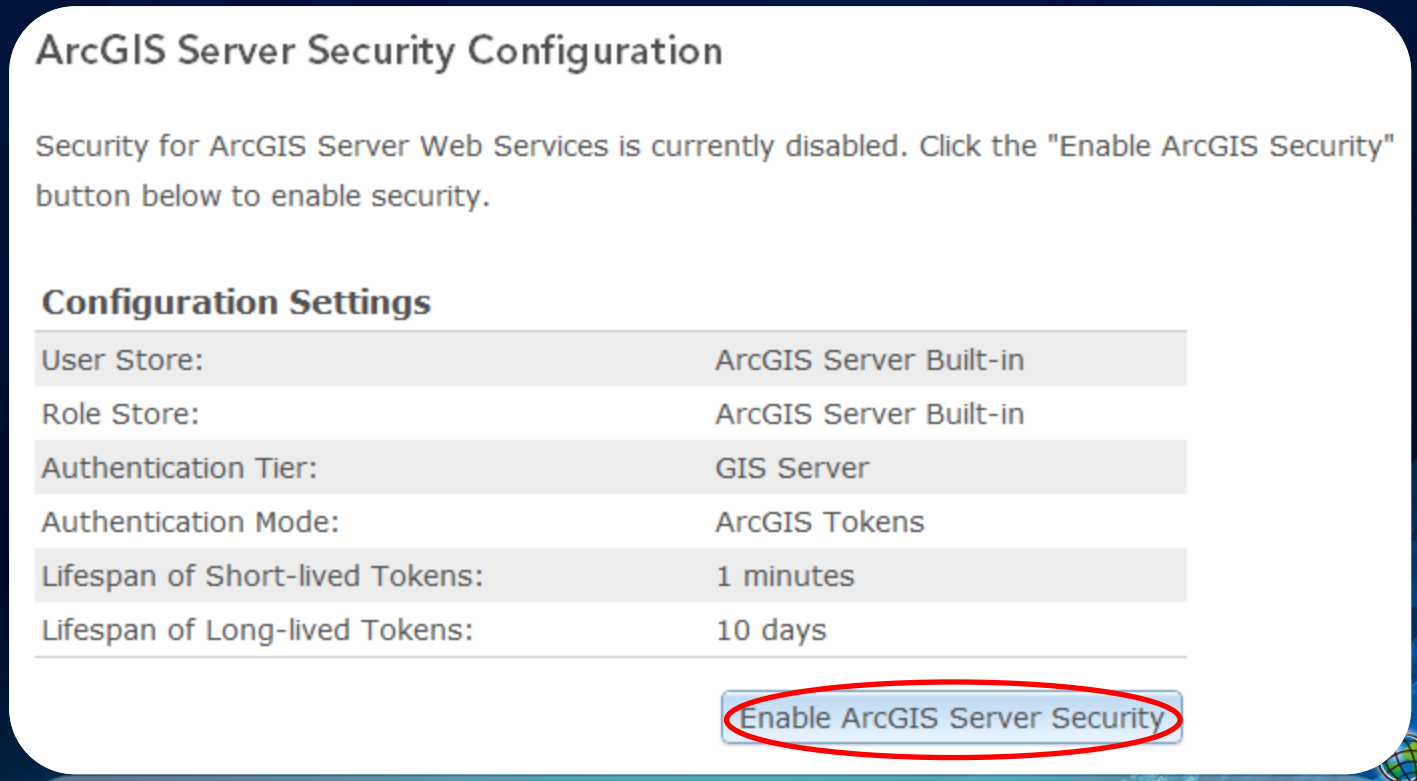
- 基于角色模型的安全控制
  - 目录和服务都可设置权限
  - 权限向下继承
- 适用于服务所有的Web接口
  - SOAP, REST, OGC, KML
- 支持Desktop, Web ADF ,JavaScript ,Flex 等
- 功能和服务具有相同的安全性



esri China BEIJING
分 享 地 理 价 值

ArcGIS Server：从开放到安全

- 启用安全和权限设置互相独立
- 如果没有启用安全，任何人都可以访问所有服务
- 启用安全后，如果没有设置访问权限，所有服务都不能被访问



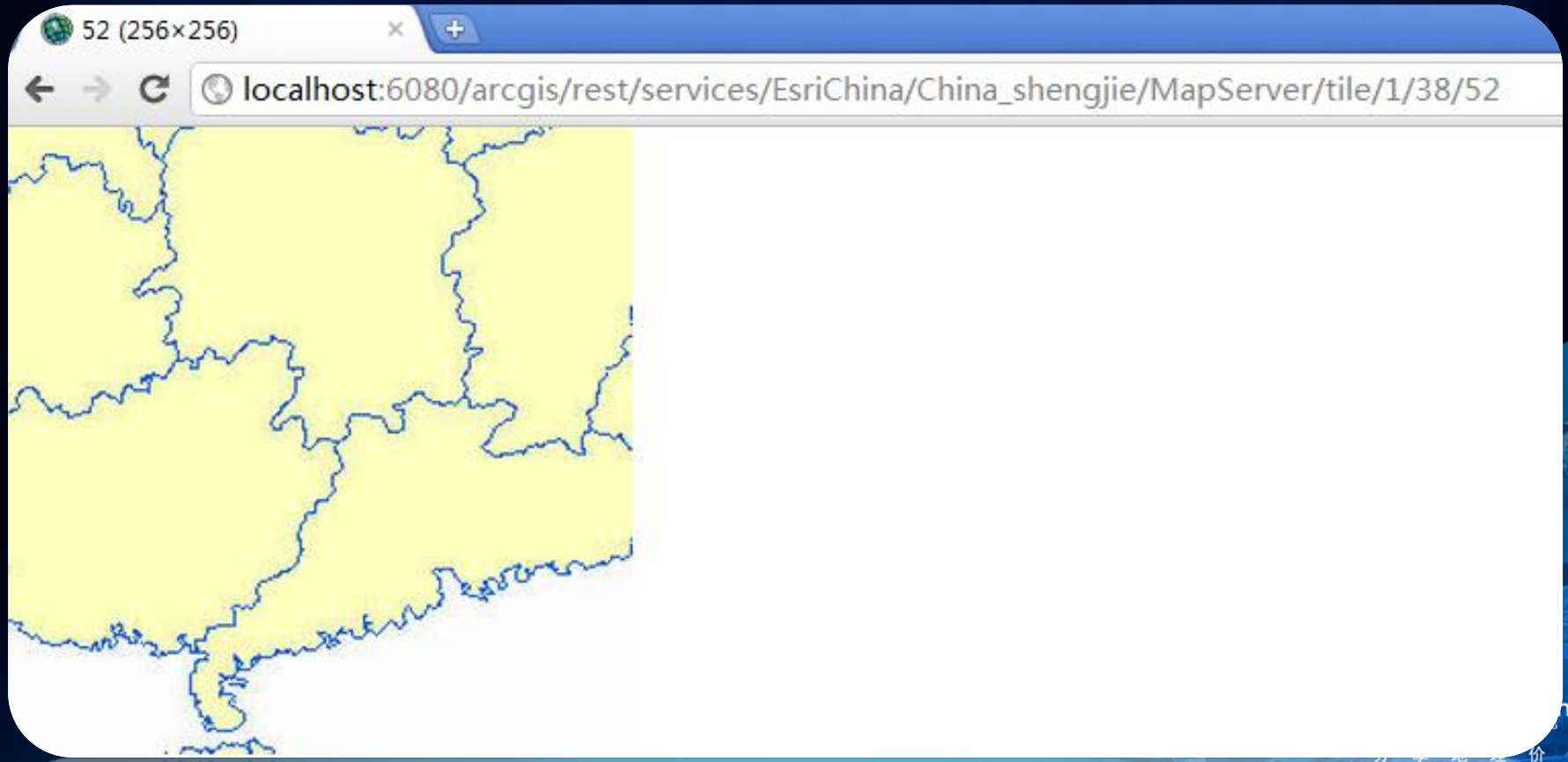
esri China BEIJING
分 享 地 理 价 值

Demo1 ：ArcGIS Server安全设置

esri China BEIJING
分 享 地 理 价 值

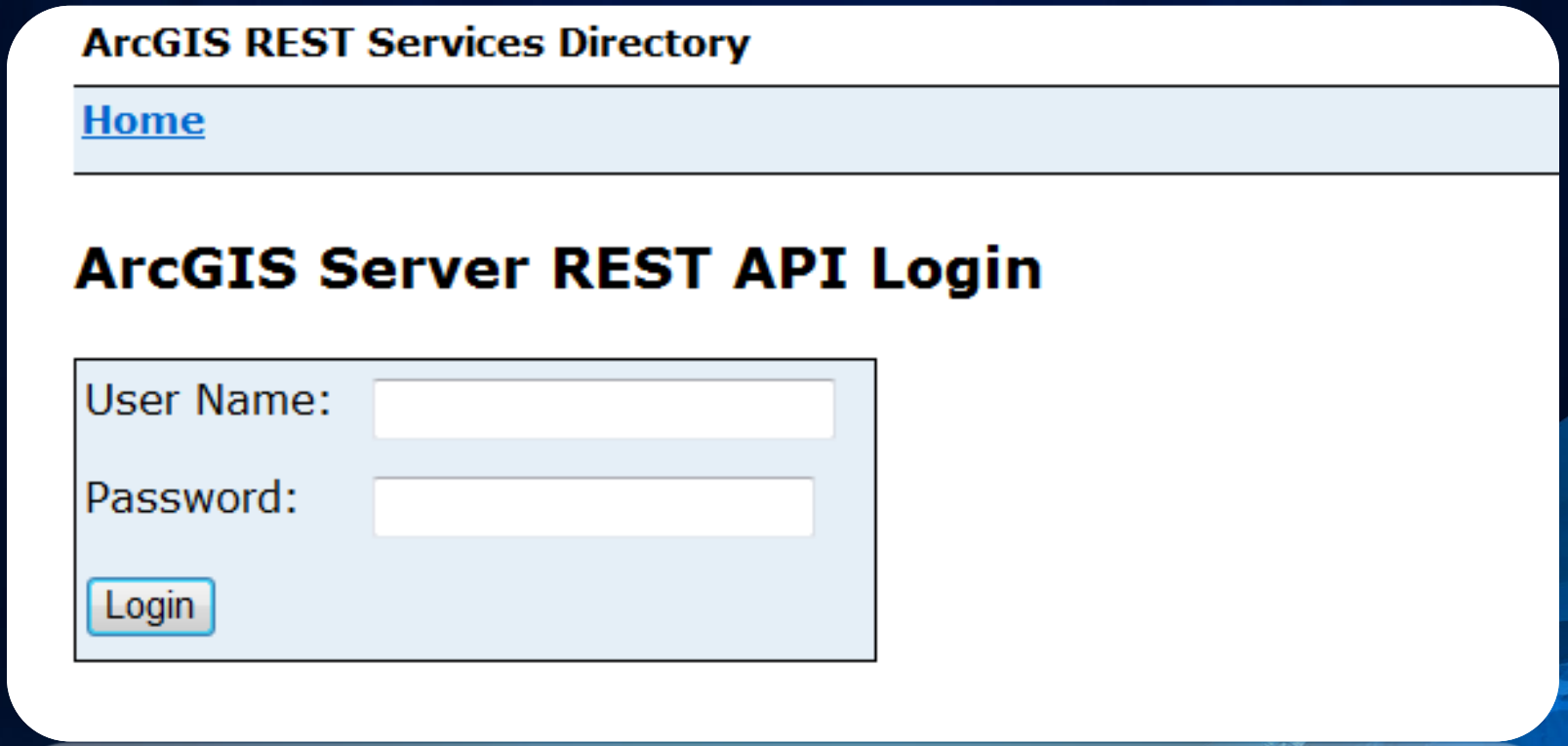
保护缓存目录

- 目标：
  - 阻止直接通过REST URL访问缓存图片



保护缓存目录

- 方法：
- 使用Token



esri China BEIJING
分 享 地 理 价 值

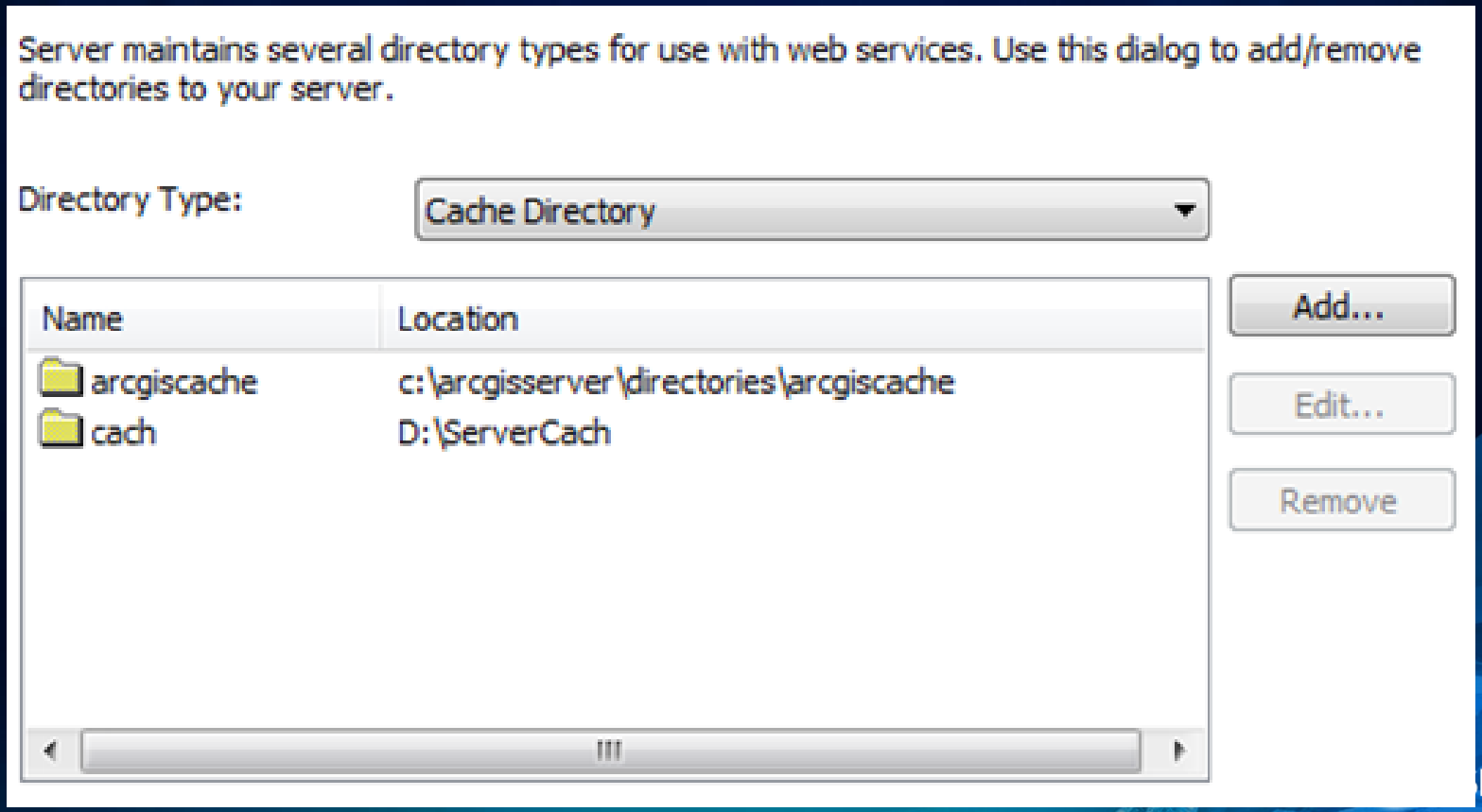
保护缓存目录

- 目标
- 阻止直接通过Cache虚拟路径访问图片

esri China BEIJING
分 享 地 理 价 值

保护缓存目录

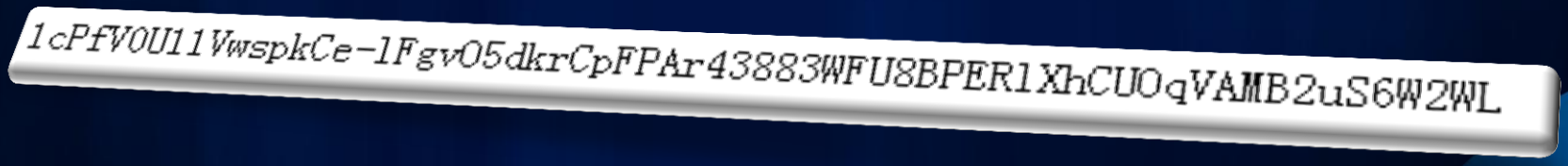
- 方法
  - 新建cach目录



China BEIJING
分 享 地 理 价 值

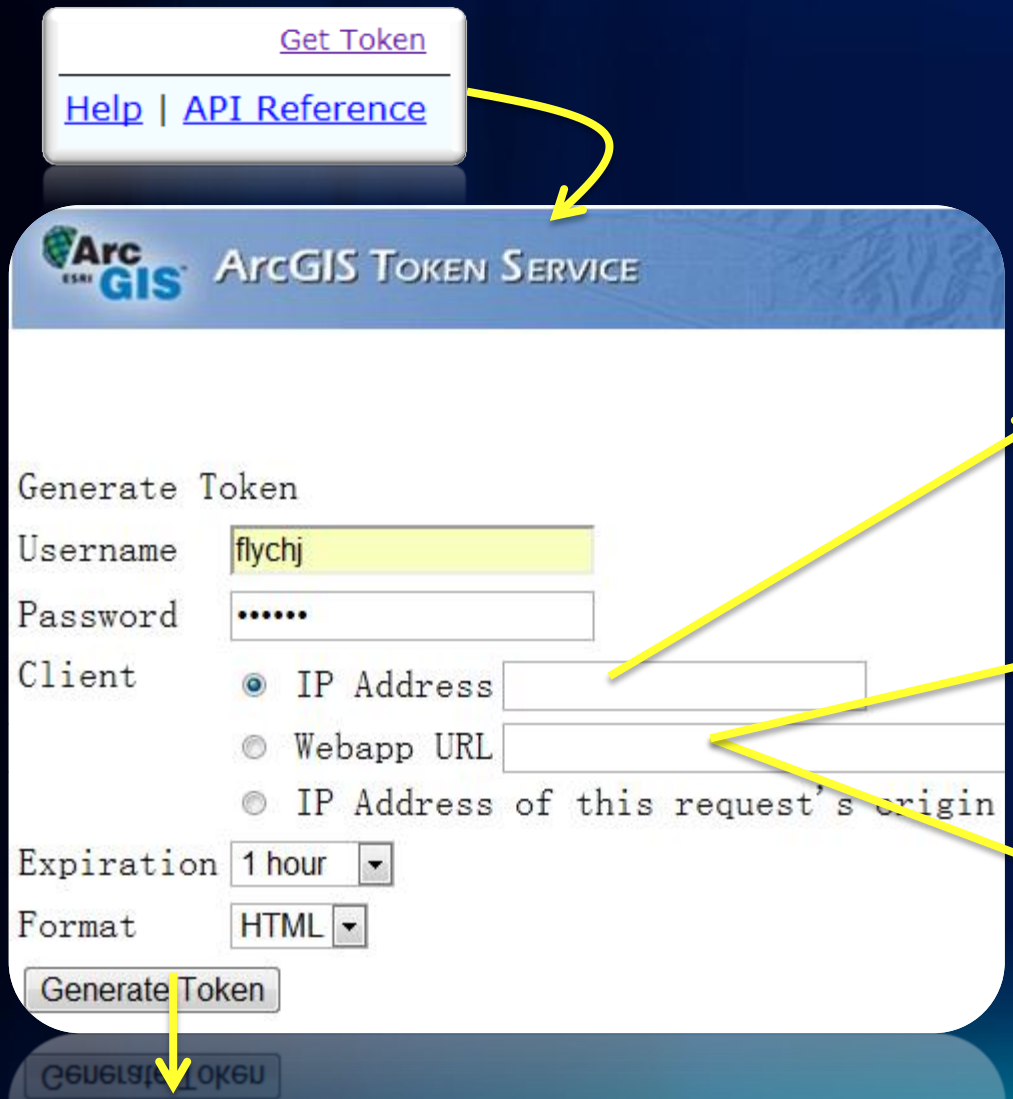
Token是什么？

- Token是一个加密的字符串，包含以下信息
  - 用户名
  - 过期时间
  - 客户端ID
  - IP地址或URL



esri China BEIJING
分 享 地 理 价 值

从页面获取token



用IP和代理页组合

http://myWebappHost/myApp

- 程序必须通过HTTP访问

myWebappHost/myApp

- 程序可以通过HTTP或HTTPS访问

WlKIV-rRW5MewDVSq_kiXy9SArD3dvKMUPr8CxsqBXpWHC90YRc4nHGFNycuefyO

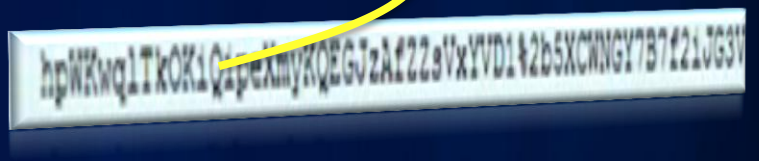
Token服务常见使用方法

开发人员

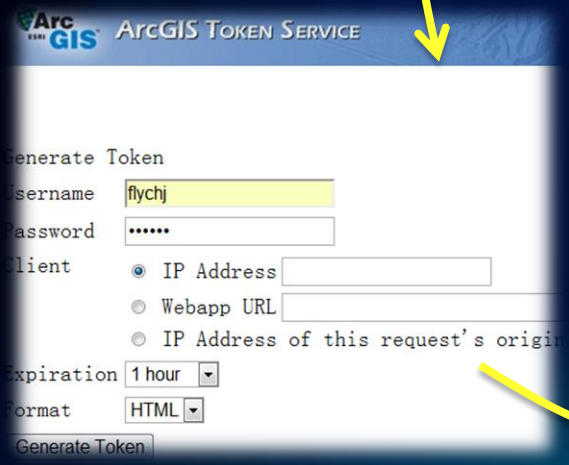
7、把token复制到程序代码

1、开发人员访问token服务页面

6、返回token



2、输入必要的信息



Web服务器

Token服务

4、身份验证

用户和角色存储位置

5、通过验证

3、客户端请求token

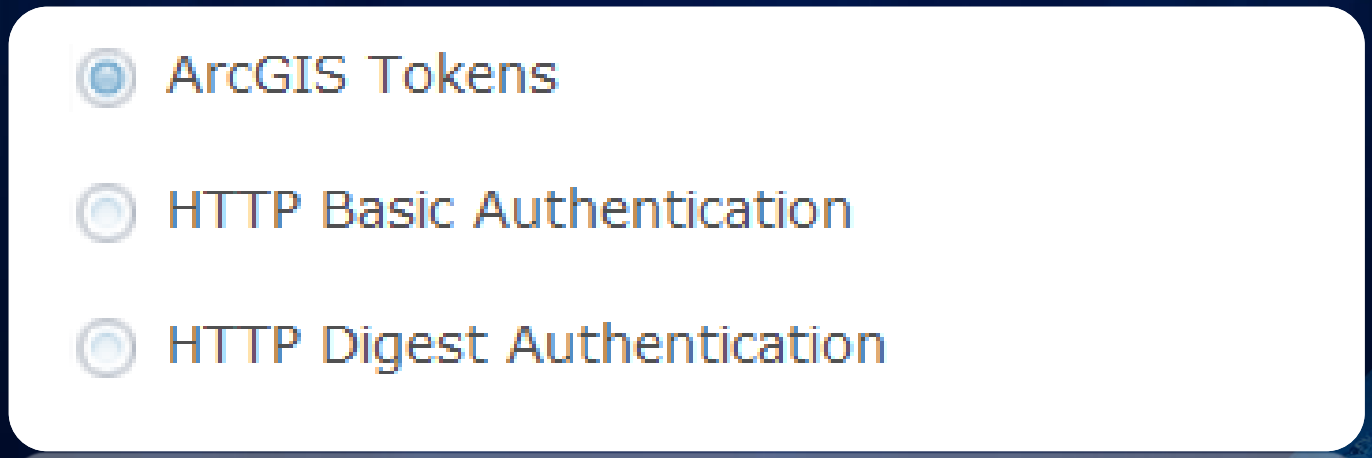
esri China BEIJING
分 享 地 理 价 值

Demo2 ：Token的使用

esri China BEIJING
分 享 地 理 价 值

HTTP 身份验证

- HTTP Basic Authentication（ArcGIS 10.1 new）
- HTTP Digest Authentication（ArcGIS 10.1 new）



esri China BEIJING
分 享 地 理 价 值

HTTP Basic Authentication

- 基本认证是一种用来允许Web浏览器，或其他客户端程序在请求时提供以用户名和口令形式的凭证。

- 用户输入了用户名和口令后，客户端在原先的请求上添加了认证消息头（值是base64encode(username+":"+password)），然后重新发送。

esri China BEIJING
分 享 地 理 价 值

HTTP基本认证优缺点

- **优点：**

  所有流行的网页浏览器都支持基本认证

- **缺点：**

  以明文传输的密钥和口令很容易被拦截

  没有对服务器返回的信息提供保护

  现存的浏览器保存认证信息直到标签页或浏览器被关闭，或者用户清除历史记录

  服务端其没有一种有效的方法来登出，而无需关闭浏览器

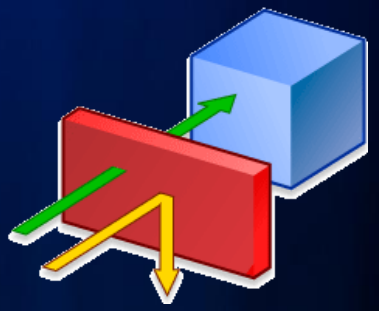
esri China BEIJING
分 享 地 理 价 值

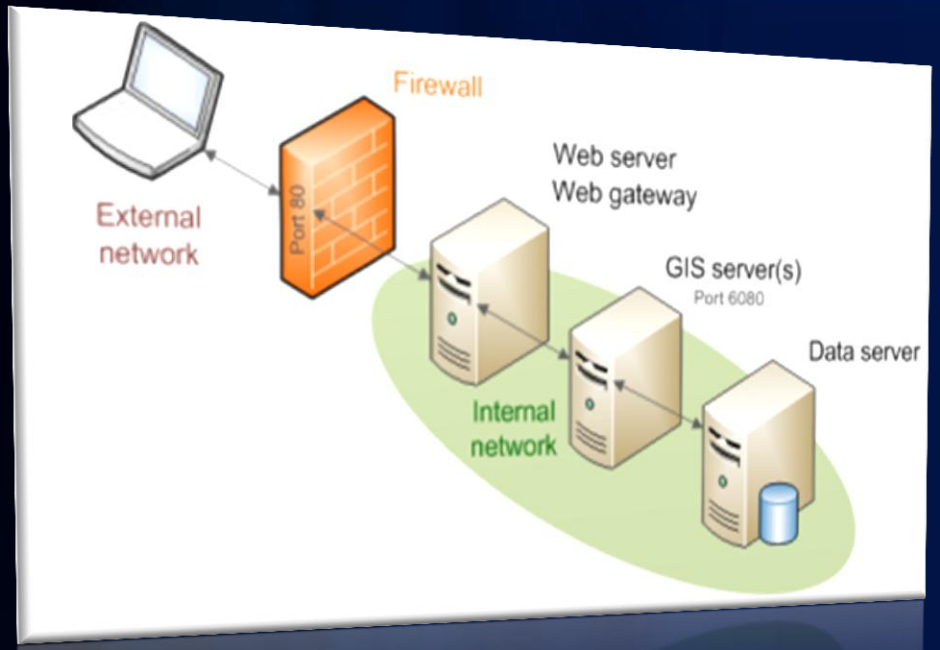
HTTP Digest Authentication

- 在客户发送请求后，收到一个401（未授权）消息，包含一个Challenge，消息里面有一个唯一的字符串。每次请求返回都不一样。
- 客户将用户名密码以及返回的Challenge一起加密后传给服务器。
- 为了防止重放攻击，采用摘要访问认证。

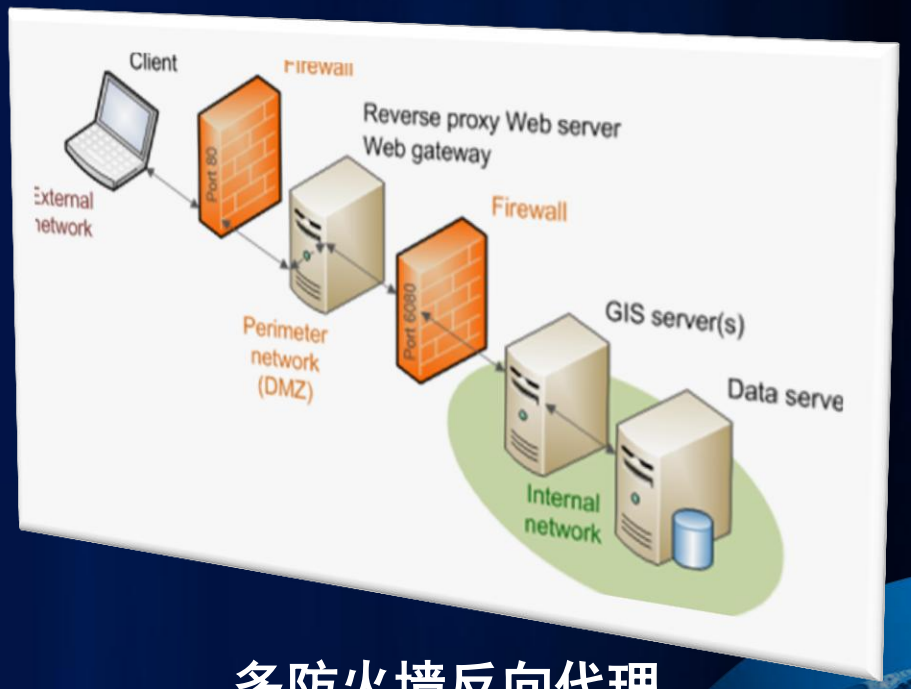
esri China BEIJING
分 享 地 理 价 值

防火墙





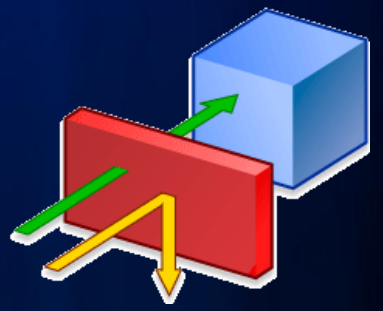
单一防火墙场景
Single firewall scenario



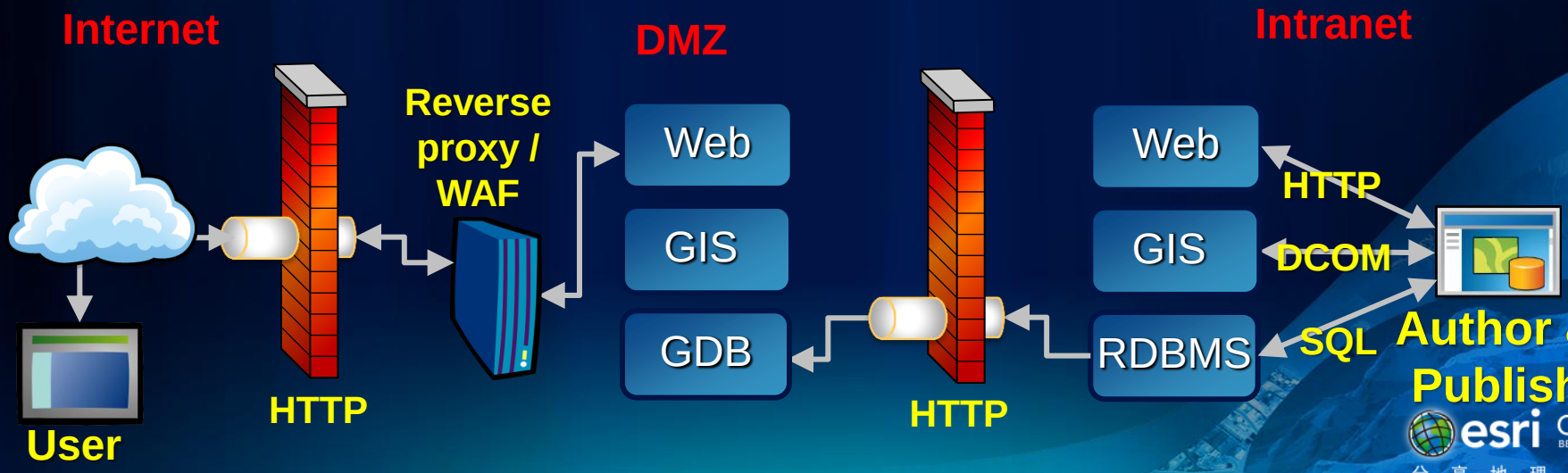
多防火墙反向代理
Multiple firewall scenario with reverse proxy Web server

esri China BEIJING
分 享 地 理 价 值

反向代理



- 反向代理隐蔽内部系统
  - 添加 Web Application Firewall (WAF)
  - 代理服务器和Web服务器之间的通信可以是任何端口
- Geodatabase in DMZ(demilitarized zone)
  - 通过HTTP单向复制（One-way replication via HTTP）
  - 每个Web服务器上都需要部署防火墙
  - 互联网用户只能访问到整个地理数据库的子集



esri China BEIJING
分 享 地 理 价 值

ArcGIS Server集成的安全

- ArcGIS Server 10引入的一种新的安全模型
- 发出请求的用户身份在系统的各个层都可以得到，每个层都可以根据用户身份进行访问控制
  - 仅限于以Internet方式访问ArcGIS Web Service的应用程序
  - 通过Web Service Handler把用户信息传递给SOM和SOC
- 如果数据来自ArcSDE for Oracle，用户信息还可以传递给Oracle数据库
  - 该功能目前只支持Oracle

esri China BEIJING
分 享 地 理 价 值

客户端1
SOAP/REST

Token
User_two

shengjie
heliu

mxd
shengjie
shenghui
heliu

发布

ArcGIS Server
服务

chengj
shengjie
shenghui
heliu

User_one

User_two

Token
User_one

shengjie
shenghui

客户端2
SOAP/REST

esri China BEIJING
分 享 地 理 价 值

Demo 3：集成安全性

esri China BEIJING
分 享 地 理 价 值

1、创建一个编辑地图的用户

```
CREATE USER map IDENTIFIED BY map
DEFAULT TABLESPACE sde
TEMPORARY TABLESPACE temp;
GRANT CONNECT, RESOURCE TO map;
```

- 也可以用已有的sde用户或者新建一个数据库用户

esri China BEIJING
分 享 地 理 价 值

2、创建访问web service的数据库用户

```
CREATE USER user_one IDENTIFIED by user_one;

GRANT CONNECT,RESOURCE to user_one;


CREATE USER user_two IDENTIFIED by user_two;

GRANT CONNECT,RESOURCE to user_two;
```

esri China BEIJING
分 享 地 理 价 值

3、设置web service账号的访问权限

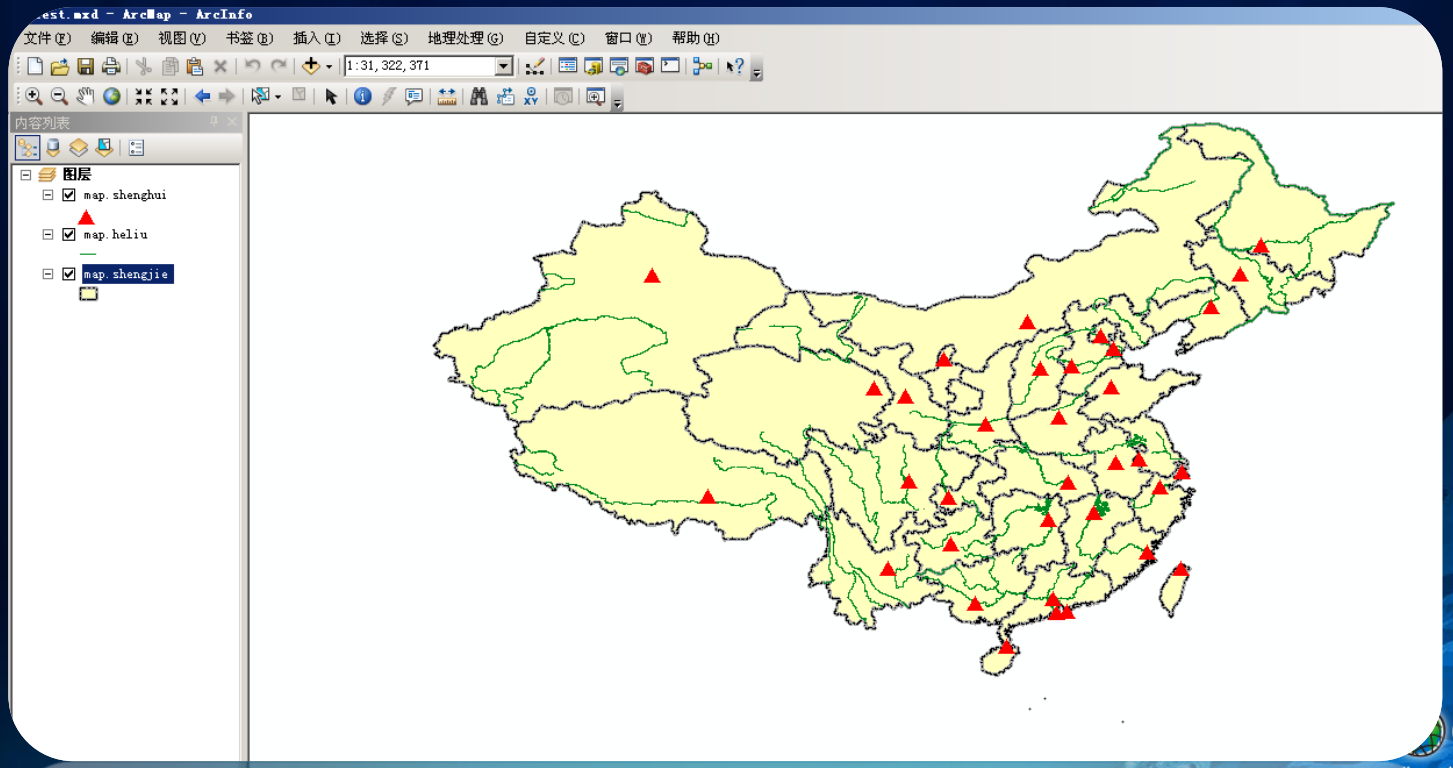
```
CREATE ROLE sel_shenghui NOT IDENTIFIED;
GRANT SELECT ON map.shengjie TO sel_shenghui;
GRANT SELECT ON map.shenghui TO sel_shenghui;
GRANT sel_shenghui to user_one;

CREATE ROLE sel_heliu NOT IDENTIFIED;
GRANT SELECT ON map.shengjie TO sel_heliu;
GRANT SELECT ON map.heliu TO sel_heliu;
GRANT sel_heliu to user_two;
```

esri China BEIJING
分 享 地 理 价 值

4、创建地图文档并发布

- 用**map**用户连接SDE，作为数据源
- 配图完成以后发布成地图服务
- 地图服务的功能，比如WMS，KML的访问控制和标准的ArcGIS Web Service是一致的（SOAP/REST）



esri China BEIJING
分 享 地 理 价 值

5、修改ArcGIS Server的配置文件

- 修改<ArcGIS InstallationDirectory>\server\system\Server.dat文件

- 重启ArcGIS Server

```
<Properties>
  <PushIdentityToDatabase>true</PushIdentityToDatabase>
  ...
</Properties>
```

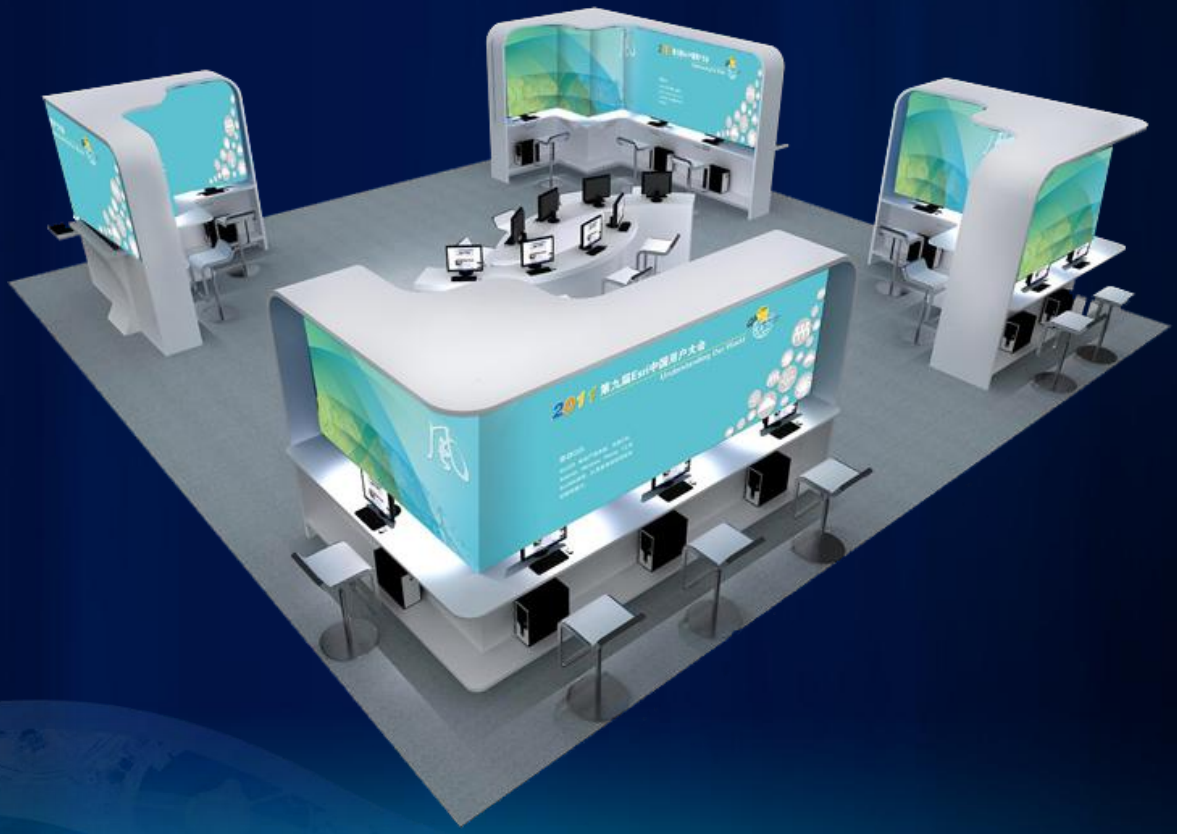
esri China BEIJING
分 享 地 理 价 值

ArcGIS在线体验中心(原群英萃)

在线体验
视频中心
地图长廊
资源下载
知识中心
虚拟课堂

http://tm.esrichina-bj.cn

欢迎移步到体验区 体验炫彩GIS世界



esri China BEIJING
分 享 地 理 价 值

esri China
BEIJING
分 享 地 理 价 值