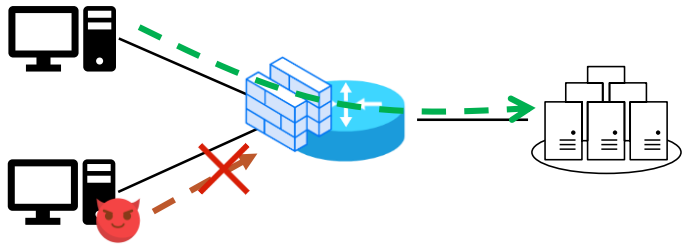
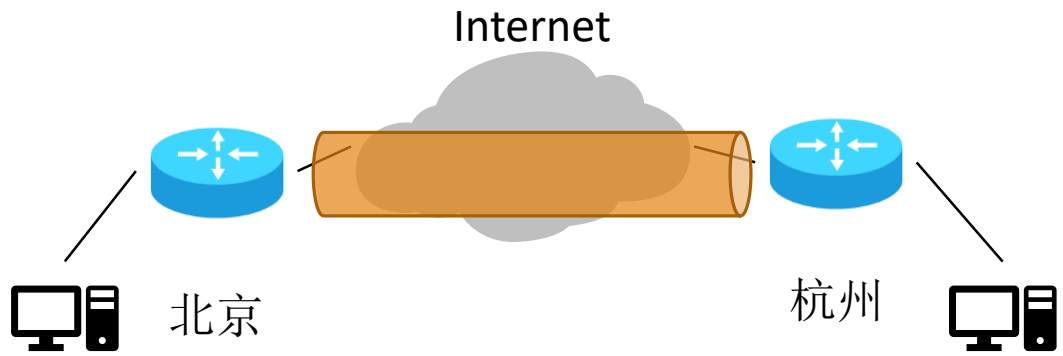
计算机网络安全技术实验课
(2020年秋季学期)

陈蔚瀚

如何用更安全的方式管理网络?



ACL (CBAC)



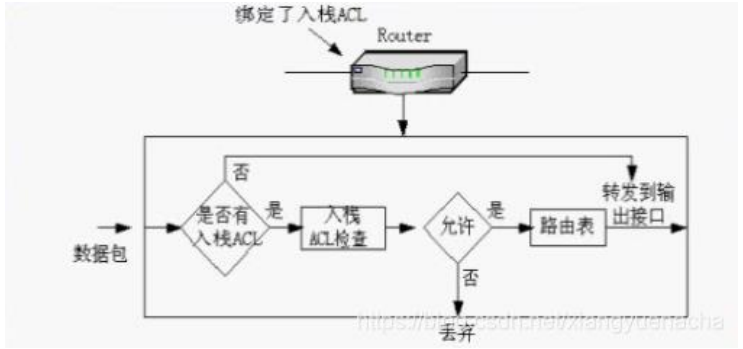
VPN

如何提升网络的安全性

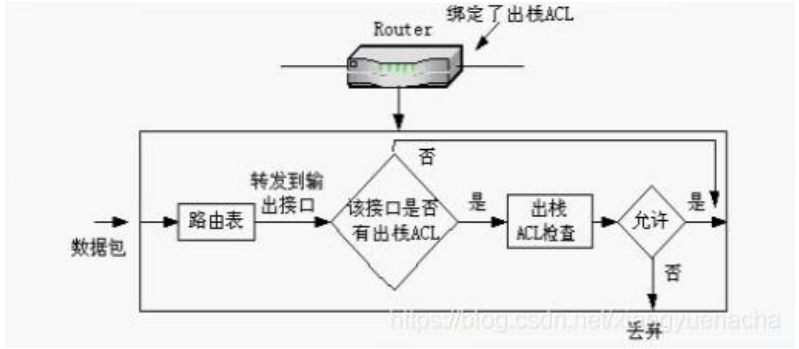
- 访问权限
  - 白名单，黑名单
  - 原则: “Someone goes, someone leaves”
- 消息认证
  - 签名(signature)，日志(logs)
  - 原则: “That is you! That is what you do”
- 信息加密
  - !#@?*&^%$($&*%^!*
  - 原则: “You know, he don’t know”

Access Control List (ACL)

- 什么是ACL?
  - 一个授权和拒绝条件的序列表
  - 基于地址或协议对流量进行过滤
  - 明确哪些用户可以访问，哪些操作可以被允许
- 分类
  - 按出入栈不同分类
    - 入栈ACL、出栈ACL
  - 其他分类
    - 标准ACL (Standard ACL)：#1~99
    - 扩展ACL (Extended ACL)：#100~199
    - 命名ACL (Named ACL)



入栈ACL



出栈ACL

标准ACL

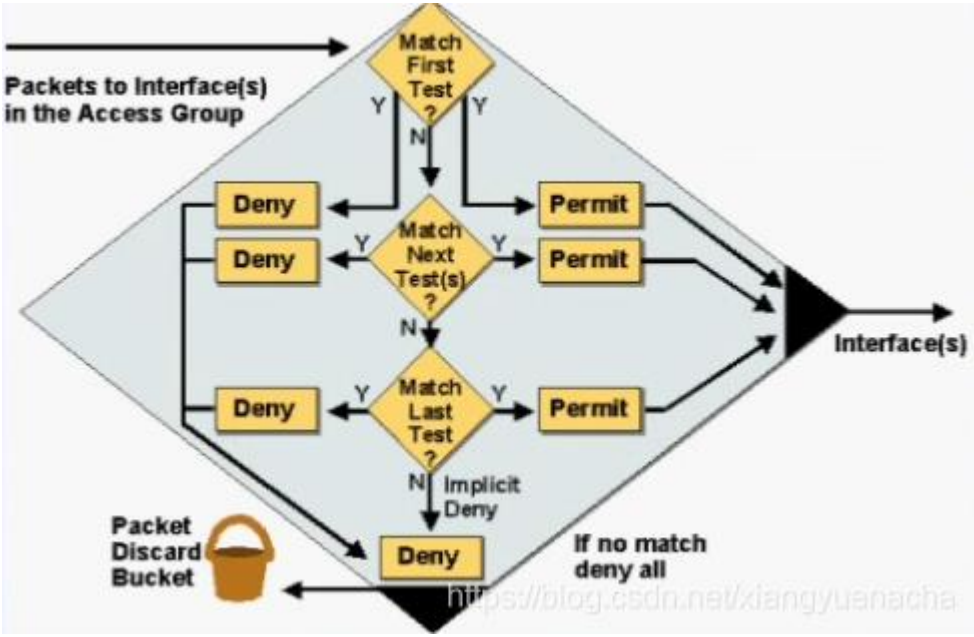
- (config)# access-list [access-list number 1-99] [permit/deny] [source IP] [ACL mask]
  - 具备相同group number的允许语句被视为一条ACL命令
  - ACL mask：0 refers to check，1 refers not
    - 与子网掩码相反
- Example
  - (config)# access-list 1 permit 192.168.1.0 0.0.0.255
  - (config)# access-list 1 permit host 10.0.0.1
  - (config)# access-list 1 deny any
- 删除语句：(config)# no access-list [access-list number]

ACL绑定

- (config-if)# ip access-group [access-list number] [in/out]
  - 标准ACL，扩展ACL，命名ACL均需要此步骤
- 取消接口上的ACL规则：
  - (config-if)# no ip access-group [access-list number] [in/out]
- 查看ACL配置
  - 在特权模式下，使用show access-lists查看

ACL工作规则

- 每个路由器的每个接口上，每个方向（in/out）只能设置一条ACL命令
- 从上至下的匹配规则
  - 如果数据包与某条ACL语句匹配，则其他语句会被忽略；
  - 如果当前ACL语句不匹配，则继续检查下一跳ACL语句；
  - 如果所有语句都不匹配，数据包会被丢弃；
  - 如果从未定义过任何ACL语句，则所有数据包都可以转发；



ACL 实例

- 例 1
  - access-list 1 deny 172.30.16.5 0.0.0.0
  - access-list 1 permit 172.30.16.0 0.0.0.255
  - 从172.30.16.4,172.30.16.5,172.30.15.2来的数据包，会如何转发?
  - 对语句顺序调整之后，转发情况是否有所改变?

ACL 实例

- 例 2
  - access-list 2 deny 172.30.16.5 0.0.0.0
  - access-list 2 permit 172.30.16.0 0.0.0.255
  - access-list 2 permit 192.168.1.0 0.0.0.255
  - 是否存在冗余的允许语句?
  - 在最后一行前添加“access-list 2 deny 192.168.3.1 0.0.0.0”后，是否存在冗余?

扩展ACL

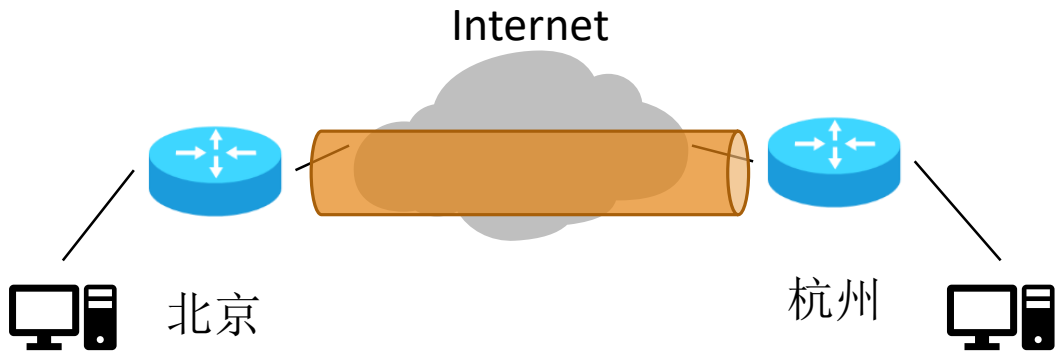
- (config)# access-list [access-list number 100-199] [permit/deny] [protocol] [source IP] [ACL mask] [destination IP] [ACL mask] [protocol option]
- Example:
  - access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
  - access-list 101 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.100 eq 21 (ftp)
  - access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq telnet

Context-Based Access Control (CBAC)

- 什么是CBAC?
  - 通过检查经过防火墙流量的会话状态信息，为防火墙访问列表创建临时通道（预留后门，放行指定流量）
  - 支持的协议不止网络层(ICMP)和传输层(TCP/UDP)，还支持应用层的协议(FTP, HTTP, POP3,SMTP, …)
  - 通常与扩展ACL配合使用
- (config)# ip inspect name [name] [protocol] [protocol option]
- (config-if)# ip inspect [name] [in/out]

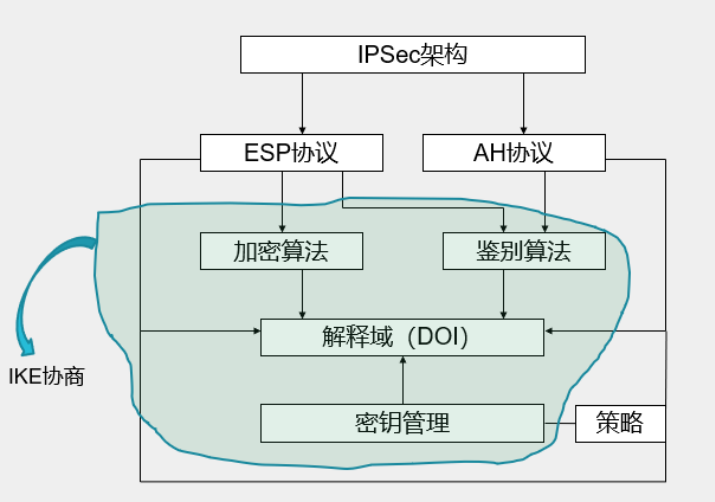
Virtual Private Network (VPN)

- 什么是VPN?
  - 建立在公共网络上的层叠网络（专用网络）
  - 一个点到点的虚拟连接
- 优势
  - 安全性
  - 便于管理



IPSec VPN

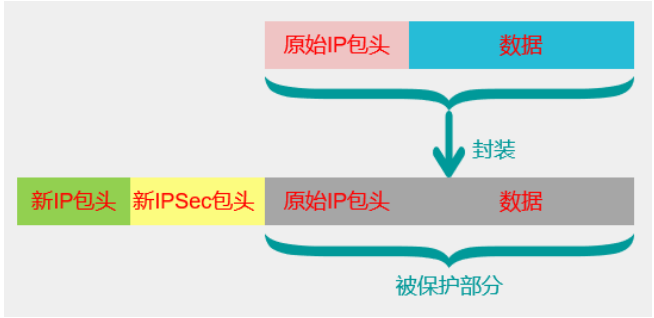
- IPSec架构
  - 数据认证及加密：AH/ESP
    - AH (Authentication Header): 报文头验证协议，对数据源和数据完整性进行验证，防止报文重放
    - ESP (Encapsulating Security Payload): 封装安全载荷协议，提供AH协议验证功能外，还支持对报文进行加密
  - 秘钥管理：IKE (ISAKMP+Oakley+SKEME)
    - 自动协商交换秘钥，建立和维护安全联盟的服务



IPSec VPN

- IPSec工作模式
  - 传输模式（Transport mode）
    - 在IP报头和高层协议报头之间插入IPSec报头
    - 应用场景：主机和主机之间通信的数据保护
  - 隧道模式（Tunnel mode）
    - 原始IP报文被封装成负荷，在其前面插入IPSec报头和新的IP报头
    - 应用场景：私网和私网间通过公网通信，建立安全的VPN通道

传输模式



隧道模式

ISAKMP配置

- (config) # crypto isakmp policy [isakmp index]
- (config-isakmp) # encryption [method: aes/3des/des]
- (config-isakmp) # hash [method: sha/md5]
- (config-isakmp) # authentication pre-share
- (config-isakmp) # group [method] (1/2/5)
- (config) # crypto isakmp key [key value] address [ip]

IPSec配置

- 使用ACL对流量进行过滤
  - （config）# access-list [group 100-199] [permit/deny] [protocol] [source ip] [acl mask] [destination ip] [acl mask] [protocol option]
- 创建transform-set
  - （config）# crypto ipsec transform-set [name] [esp/ah method]

IPSec配置

- 创建MAP映射表
  - （config）# crypto map [name] [map index] ipsec-isakmp
  - （config-crypto-map）# set peer [ip]
  - （config-crypto-map）# match address [acl group]
  - （config-crypto-map）# set transform-set [name]
- 端口绑定
  - （config）# int fX/X（外网端口）
  - （config-if）# crypto map [name]

IPSec配置查看

- show crypto isakmp sa
  - 查看isakmp配置状态
- show crypto isakmp policy
  - 查看isakmp策略配置集
- show crypto ipsec sa
  - 查看ipsec配置状态
- show crypto ipsec transform-set
  - 查看ipsec传输模式

IPSec VPN配置Tips

- 通常isakmp-ip与map-peer-ip相同
- 同一个VPN的MAP name应该一致
- 同一个pair的MAP index应该一致
- 需要在边界路由器上配置相应的路由转发规则，保证经过VPN隧道的报文能得到正常转发
- 搜索 cisco packet tracer ipsec vpn获取更多内容

作业提交注意事项

- 在网络学堂上提交后，检查作业是否上传成功
- 注意提交的实验报告是否完整