



# 【CSC公开课】第十八期——思科 AnyConnect 安全接入

高阳

# 今天的网络安全形势

- 安全公司等提供的安全分析报告
- 对自己的VPS评估
  1. 加固前，3天被破解
  2. 加固后，目前2个多月还未被破解



# 一个星期 尝试登陆破解的失败次数

写脚本,封掉登陆尝试失败10次以上的IP地址,并发邮件通知

```
Jan 23 01:43:54 vps sshd[5418]: Connection closed by 220.113.7.98
Jan 23 02:21:02 vps sshd[7280]: Invalid user jose from 220.113.7.98
Jan 23 02:21:02 vps sshd[7281]: input_userauth_request: invalid user jose
Jan 23 02:21:02 vps sshd[7280]: pam_unix(sshd:auth): check pass; user unknown
Jan 23 02:21:02 vps sshd[7280]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=220.113.7.98
Jan 23 02:21:02 vps sshd[7280]: pam_succeed_if(sshd:auth): error retrieving information about user
  jose
Jan 23 02:21:04 vps sshd[7281]: Connection closed by 220.113.7.98
Jan 23 02:21:04 vps sshd[7280]: Failed password for invalid user jose from 220.113.7.98 port 19500
  ssh2
Jan 23 02:33:05 vps saslauthd[1236]: pam_unix(smtp:auth): authentication failure; logname= uid=0 e
uid=0 tty= ruser= rhost= user=root
Jan 23 02:58:46 vps sshd[9146]: Invalid user joseph from 220.113.7.98
Jan 23 02:58:46 vps sshd[9147]: input_userauth_request: invalid user joseph
Jan 23 02:58:46 vps sshd[9146]: pam_unix(sshd:auth): check pass; user unknown
Jan 23 02:58:46 vps sshd[9146]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=220.113.7.98
Jan 23 02:58:46 vps sshd[9146]: pam_succeed_if(sshd:auth): error retrieving information about user
  joseph
Jan 23 02:58:48 vps sshd[9146]: Failed password for invalid user joseph from 220.113.7.98 port 358
  57 ssh2
Jan 23 02:58:49 vps sshd[9147]: Connection closed by 220.113.7.98
Jan 23 03:35:34 vps saslauthd[1238]: pam_unix(smtp:auth): check pass; user unknown
Jan 23 03:35:34 vps saslauthd[1238]: pam_unix(smtp:auth): authentication failure; logname= uid=0 e
uid=0 tty= ruser= rhost=
Jan 23 03:35:34 vps saslauthd[1238]: pam_succeed_if(smtp:auth): error retrieving information about
  user temp
Jan 23 03:46:06 vps sshd[11524]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=
0 tty=ssh ruser= rhost=183.3.202.107 user=root
Jan 23 03:46:08 vps sshd[11524]: Failed password for root from 183.3.202.107 port 44643 ssh2
Jan 23 03:46:10 vps sshd[11524]: Failed password for root from 183.3.202.107 port 44643 ssh2
Jan 23 03:46:12 vps sshd[11524]: Failed password for root from 183.3.202.107 port 44643 ssh2
Jan 23 03:46:12 vps sshd[11525]: Received disconnect from 183.3.202.107: 11:
Jan 23 03:46:12 vps sshd[11524]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
  ruser= rhost=183.3.202.107 user=root
```

```
[root@vps log]# grep 'Failed password' secure-20160124 | wc -l
28634
```

# 一个多月 被隔离到/tmp目录下的垃圾邮件的数量

绝大部分  
都是relay  
的mail,导  
致你的域  
名被加入  
黑名单

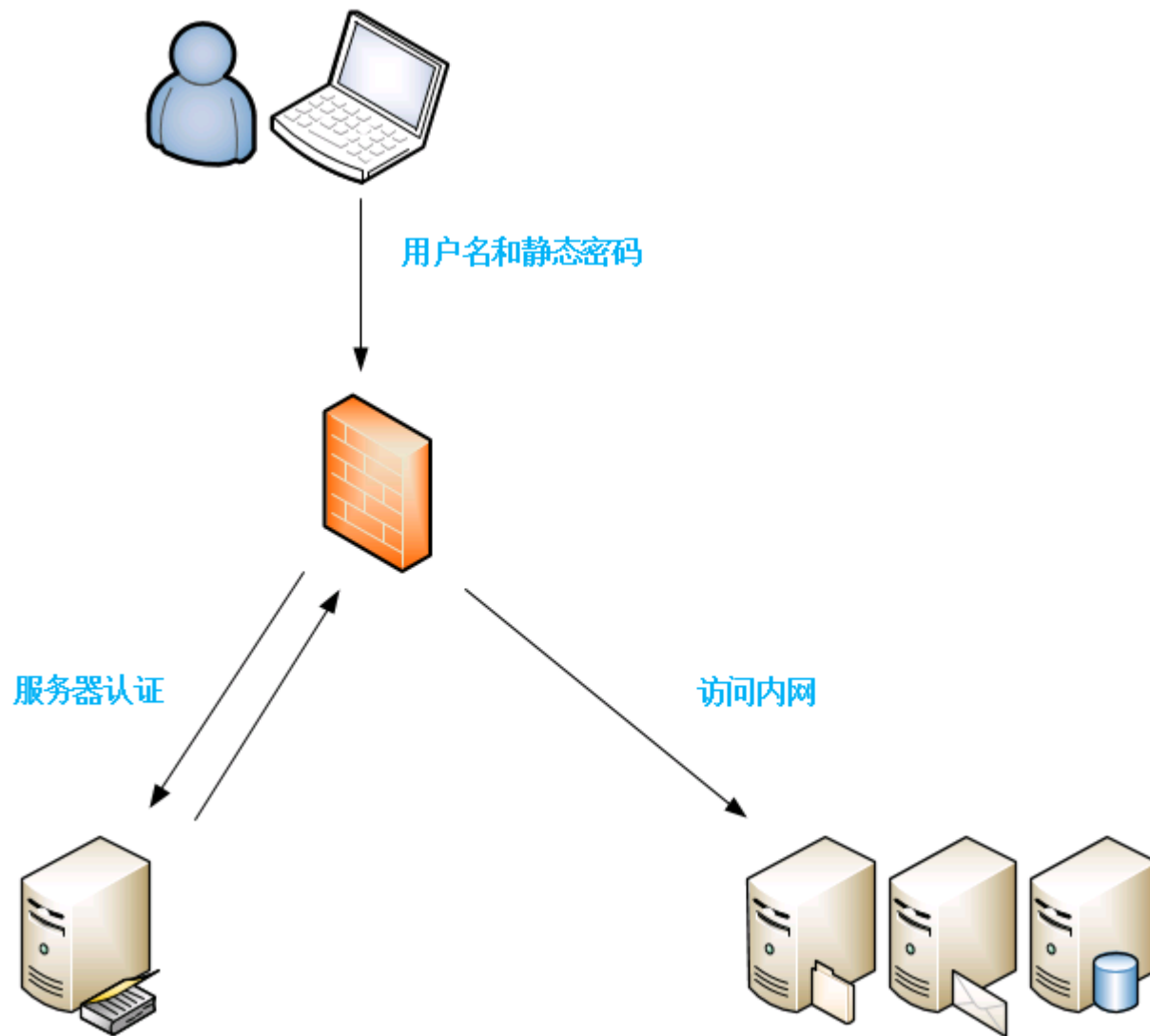
```
spam-zw2IFaY94Hcj.gz  
spam-ZW_2NB0yHNcj.gz  
spam-zW_3iffoyncO.gz  
spam-Zw6mKqmuBFLO.gz  
spam-zw7daviD_5mU.gz  
spam-zWaMOFkgvo4J.gz  
spam-ZWBqc2RlWG7b.gz  
spam-zwDbWT8qURlI.gz  
spam-zwee-Q7oP6XO.gz  
spam-zWfMdk9h4nDm.gz  
spam-zWfojQ7goORZ.gz  
spam-ZwGjenAtb4uw.gz  
spam-Z-wgJv04t-e0.gz  
spam-zwKjG3pZfB6K.gz  
spam-zWKRSSOm-xIM.gz  
spam-ZWmURwsWDfvE.gz  
spam-ZwnK3HYm2c8V.gz  
spam-ZWQUeCMcOUzQ.gz  
spam-zwstHxpUTATa.gz  
spam-zwwTLVAF4ORt.gz  
spam-zwxq4fh4geWQ.gz  
spam-ZWXRUb-AGIgs.gz  
spam-zwyBgjJTFLpp.gz  
spam-z-WzT9-1cGvN.gz  
spam-Zx2KOYohhfpX.gz  
spam-Zx3OscOSL8PJ.gz  
spam-zx5lCJoxw5mC.gz  
spam-zx7v73Qr2IPb.gz  
spam-Zx8T1p9Z-1Zf.gz  
spam-zXAXGRL8D3md.gz  
spam-zxA_ZY6rBdUR.gz  
spam-zXBuYdZv07Fa.gz  
spam-zxcIuhzTRq53.gz  
spam-zXEGQJrFonty.gz  
spam-zXeThnlSwh-R.gz  
spam-zxgj6uJlth73.gz  
spam-ZXj9c61-UT7I.gz
```

```
[root@vps tmp]# ls | grep spam | wc -l  
28470
```

结论:

只要开放端口和服务,就一定会被攻击,并且有被破解的可能

# 大多数公司的访问策略



# 为什么这种VPN访问安全比较低

- 用户名容易被别人得到
- 密码容易被破解,  
非IT员工密码都很简单,不会设置复杂密码

# 如何加固VPN访问的安全

对VPN的各个因素进行评估

1. 是不是需要VPN
2. 是不是所有人都需要VPN
3. 公司的笔记本带出去安全么
4. ASA本身有没有漏洞
5. 认证策略安全么



# 方案：对笔记本进行加固

- 普通用户 无管理员权限
- 组策略
- 系统补丁
- 杀毒软件
- HIPS
- 硬盘加密
- 等等

# 方案: 对ASA进行加固

- 不要在Internet接口 开启SSH和ASDM
- Syslog和SNMP， 并经常关注
- 使用实时流量分析工具 例： Ntopng
- 经常关注IT安全信息,注意Cisco发布的安全通告
- 及时更新系统（带\*号） 代表已知的问题基本都修复了
  - 对内部设备的升级观念
  - 对外部设备的升级观念

# 方案:对用户的识别

1.使用证书认证+静态密码

2.使用动态密码+静态密码

这个token最好是一个单独的设备,硬件token或手机集成token

防止笔记本丢失. 必须人+笔记本+token 三个要素才能连接

957696



Primary Token (gaoyang)

# 方案: 连接VPN的时候是否需要同时访问Internet

- 如果不必需, 可以不给Internet访问
- Tunnel-Split的坏处
- U-Turn的优点
  - 结合其他内部安全防护如IPS, WSA等
  - 缺点:速度问题,可能需要QoS限速

# 思考：有了以下四点是否就足够安全

- 1. 笔记本加固
- 2. ASA加固
- 3. 用户的证书或动态密码 + 静态密码
- 4. VPN同时控制Internet访问

# 不确定性

用户一定会用公司的笔记本连接VPN么？

个人的电脑，网吧电脑，酒店电脑等  
可能有病毒，木马，已被控制了等等

通过VPN直接危害到外部用户和内部网络

# 如何确定用户就是使用公司发的笔记本登陆VPN?

- 公司的笔记本有什么特征
  1. windows 7 sp1
  2. 有某些组策略
  3. 有某杀毒软件
  4. 有某软件
  5. 有某文件
  6. 加入域了
  7. 等等

# AnyConnect的机器识别 HostScan

- 能够支持的系统
  1. Windows
  2. Mac
  3. Linux



# HostScan的授权

Advanced Endpoint Assessment : Enabled perpetual

# 实验说明

- 客户机为Windows 7 SP1
- 有McAfee 8.8，最后一次病毒更新小于10天
- 有windows 防火墙并且开启
- 已经加入MS AD域
- 其他条件,这里不演示了

# ASA基本配置

webvpn

enable outside

no anyconnect-essentials

anyconnect image disk0:/anyconnect-win-4.2.01035-k9.pkg 1

anyconnect enable

tunnel-group-list enable

# ASA基本配置

```
aaa-server ACS protocol radius
```

```
aaa-server ACS (inside) host 10.0.10.101
```

```
key *****
```

```
aaa-server OTP protocol radius
```

```
aaa-server OTP (inside) host 10.0.10.103
```

```
key *****
```

## ASA基本配置

```
ip local pool SSLPool 10.0.100.1-10.0.100.254 mask 255.255.255.0
```

```
group-policy GroupPolicy1 internal
```

```
group-policy GroupPolicy1 attributes
```

```
wins-server value 10.0.10.2
```

```
dns-server value 10.0.10.2
```

```
vpn-tunnel-protocol ssl-client
```

```
default-domain value gaojack.com
```

```
address-pools value SSLPool
```

# ASA基本配置

```
tunnel-group TunnelGroup1 type remote-access
```

```
tunnel-group TunnelGroup1 general-attributes
```

```
address-pool SSLPool
```

```
authentication-server-group ACS
```

```
secondary-authentication-server-group OTP use-primary-username
```

```
default-group-policy GroupPolicy1
```

```
tunnel-group TunnelGroup1 webvpn-attributes
```

```
group-alias AnyConnect enable
```

# 导入 Host Scan Image

The screenshot shows the Cisco ASDM configuration interface. At the top, there is a navigation bar with tabs for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. Below this is a breadcrumb trail: Configuration > Remote Access VPN > Host Scan Image. On the left, a 'Device List' sidebar shows a tree view of configuration options, with 'Host Scan Image' selected and highlighted in blue. The main content area contains the following text and controls:

Use this panel to install Host Scan. The Host Scan image can come from a stand-alone package, or included as part of the AnyConnect 3.0 and 3.1 for Windows OS or the Cisco Secure Desktop packages.

Host Scan configuration can be performed by going to Secure Desktop Manager/Host Scan. If 'Host Scan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Location:

Enable Host Scan/CSD

# 配置 Host Scan --- configure

The screenshot shows a management console interface for configuring Host Scan. On the left is a navigation tree with categories like Introduction, Network (Client) Access, AAA/Local Users, Host Scan Image, Secure Desktop Manager, Setup, Certificate Management, Language Localization, Load Balancing, DHCP Server, DNS, and Advanced. The 'Host Scan' item under 'Setup' is selected. The main area is titled 'Host Scan' and contains a descriptive paragraph: 'Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under [Dynamic Access Policies](#)'. Below this is a section for 'Basic Host Scan' with a table that has columns for 'Type', 'ID', and 'Info'. To the right of the table are buttons for 'Add', 'Edit...', and 'Delete'. Below the table is a section for 'Host Scan Extensions' with a list of two items: 'Advanced Endpoint Assessment ver 3.6.10294.2' and 'Endpoint Assessment ver 3.6.10294.2', both with checked checkboxes. A 'Configure...' button is located to the right of this list. At the bottom left, there is a secondary navigation bar with items: Device Setup, Firewall, Remote Access VPN (highlighted), Site-to-Site VPN, and Device Management.

**Host Scan**

Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under [Dynamic Access Policies](#)

Basic Host Scan

Type	ID	Info
------	----	------

Host Scan Extensions

- Advanced Endpoint Assessment ver 3.6.10294.2
- Endpoint Assessment ver 3.6.10294.2

Navigation Tree:

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Setup
  - Global Settings
  - Host Scan**
- Certificate Management
- Language Localization
- Load Balancing
- DHCP Server
- DNS
- Advanced

Bottom Navigation Bar:

- Device Setup
- Firewall
- Remote Access VPN**
- Site-to-Site VPN
- Device Management



# 配置Host Scan 杀毒软件 防火墙的策略

Advanced Endpoint Assessment

Windows Mac OS Linux

### AntiVirus

Vendor	Product	Note
McAfee, Inc.	McAfee VirusScan Enterprise 8.8.x	Supports virus definition update and fi...

Force File System Protection

Force Virus Definitions Update

if not updated in last  days

### Personal Firewall

Vendor	Product	Note
Microsoft Corp.	Microsoft Windows Firewall 7	Supports firewall rules

Firewall Action:

Rules

**The action and rules remain effective on client device even after VPN session ends, please use them with discretion.**

### AntiSpyware

Vendor	Product	Note
--------	---------	------

Force Spyware Definitions Update

if not updated in last  days

# 如何在VPN客户端进入内网以前判断客户端是否加域了

## Computer name, domain, and workgroup settings

---

Computer name: YANGGA2-GLB3N  
Full computer name: YANGGA2-GLB3N.cisco.com  
Computer description: Build Date: Monday, September 21, 2015 [OSD 2015-02-22 (GA)]  
Domain: cisco.com

 [Change settings](#)

## Windows activation

---

Windows is activated  
Product ID: 00392-918-5000002-85974 [Change product key](#)



[Learn more online...](#)

# 通过注册表扫描，判断是否加入域了

SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History\  
MachineDomain

**Host Scan**

Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under [Dynamic Access Policies](#)

Basic Host Scan

Type	ID	Info
Registry	Domain	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Poli...

**Edit Registry Scan**

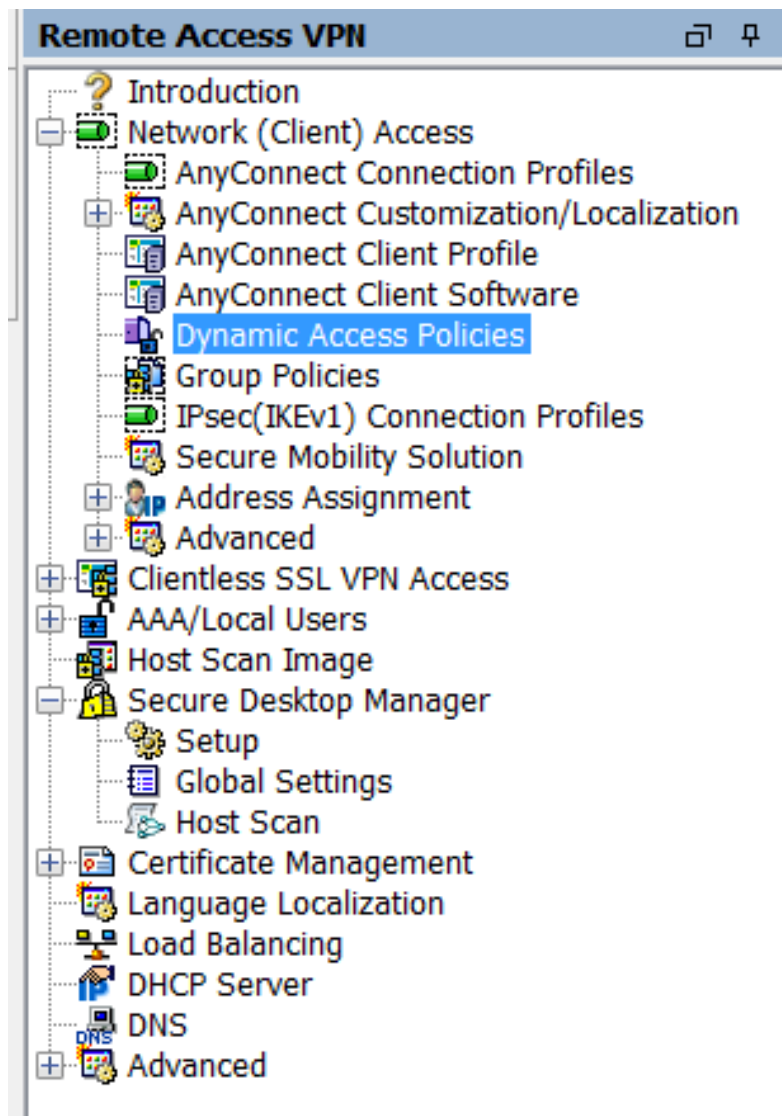
Endpoint ID:

Entry Path:

Host Scan Extensions

<input checked="" type="checkbox"/> Advanced Endpoint Assessment ver 3.6.10294.2	<input type="button" value="Configure..."/>
<input checked="" type="checkbox"/> Endpoint Assessment ver 3.6.10294.2	

# 配置Dynamic Access Policies



# 修改默认的DAP策略为Terminate并给出相应的提示

[Configuration](#) > [Remote Access VPN](#) > [Network \(Client\) Access](#) > [Dynamic Access Policies](#)

Configure Dynamic Access Policies

For IPsec, AnyConnect Client, Clientless SSL VPN, and Cut-Through-Proxy sessions, you can configure dynamic access policies (DAP) that define which network resources a user is authorized to access. All policies are enforced during session establishment. When none of the DAP policies are matched, the ASA will enforce the DfltAccessPolicy.

ACL Priority	Name	Network ACL List	Webtype ACL List	Description
-	DfltAccessPolicy			

**Edit Dynamic Access Policy**

Policy Name: DfltAccessPolicy

Description:

**Access/Authorization Policy Attributes**

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Functions	Port Forwarding Lists	Bookmarks	Access Method	AnyConnect
Action	Network ACL Filters (client)		Webtype ACL Filters (clientless)	

Action:  Continue  Quarantine  Terminate [?](#)

Specify the message that will be displayed when this record is selected.

User Message:

# 查看ASA支持的识别方式

The screenshot displays the 'Add Dynamic Access Policy' configuration window. The main window includes fields for 'Policy Name', 'Description', and 'ACL Priority'. It features two main sections: 'Selection Criteria' and 'Access/Authorization Policy Attributes'. The 'Selection Criteria' section includes a table for 'AAA Attribute' and 'Operation/Value', and an 'Advanced' section. The 'Access/Authorization Policy Attributes' section includes 'Action' (Continue, Quarantine, Terminate) and 'User Message'.

The 'Operator For Endpoint Category' dialog box is open, showing a list of endpoint categories with radio buttons for 'Match Any' and 'Match All'. The categories listed are:

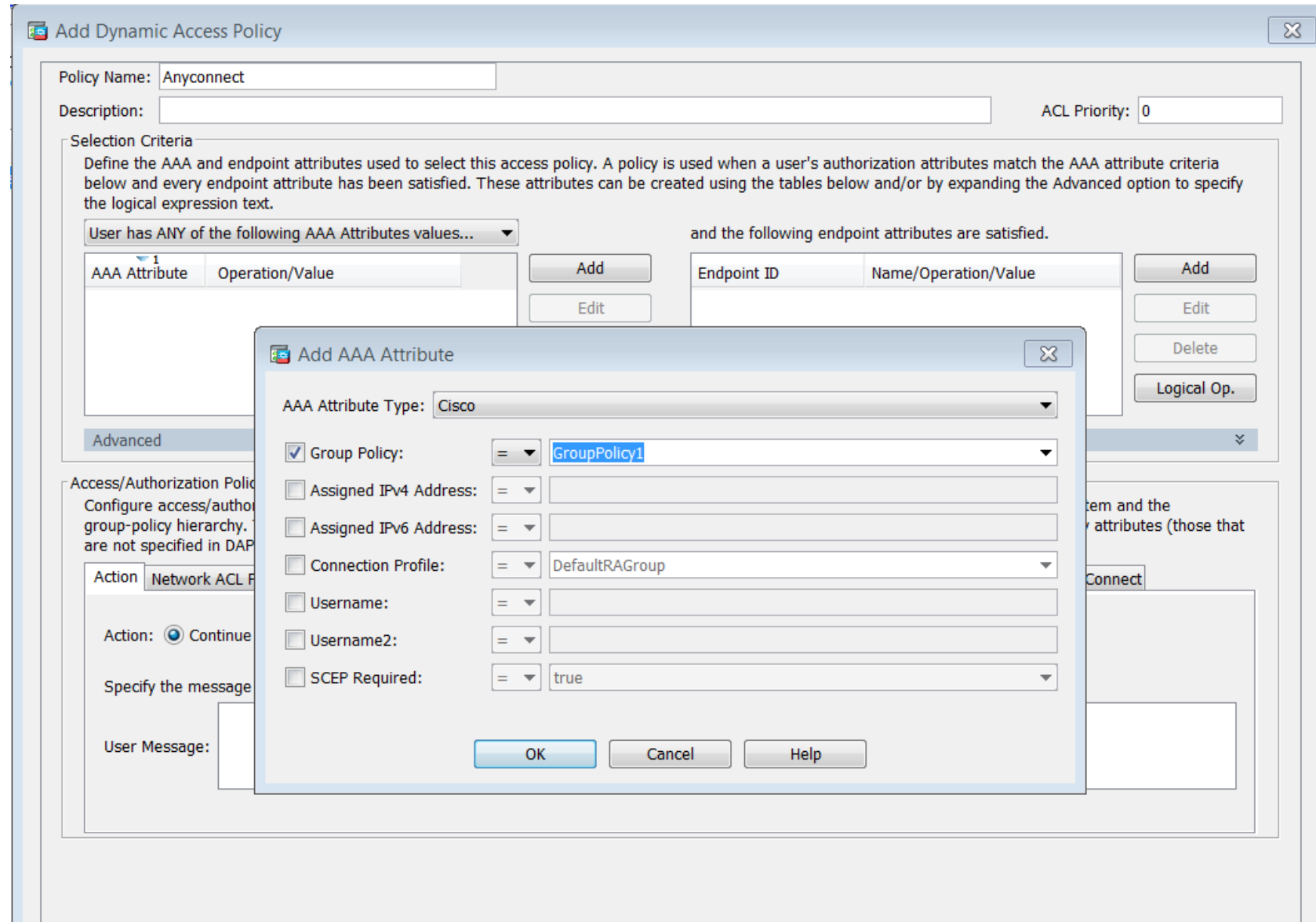
- AnyConnect:  Match Any  Match All
- Anti-Spyware:  Match Any  Match All
- Anti-Virus:  Match Any  Match All
- Application:  Match Any  Match All
- File:  Match Any  Match All
- Device:  Match Any  Match All
- NAC:  Match Any  Match All
- OS:  Match Any  Match All
- Policy:  Match Any  Match All
- Personal Firewall:  Match Any  Match All
- Process:  Match Any  Match All
- Registry:  Match Any  Match All

A note at the bottom of the dialog states: 'Note: The security appliance performs a logical AND operation on all configured endpoint categories.' Buttons for 'OK', 'Cancel', and 'Help' are visible at the bottom of the dialog.

The background window shows a table with columns for 'Access Method' and 'AnyConnect', and buttons for 'Add', 'Edit', and 'Delete'.



# 新建Policy 设置AAA Attribute并关联到对应的GroupPolicy 上



# 新建Endpoint Attribute, 设置操作系统的版本

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add

**Add Endpoint Attribute**

Endpoint Attribute Type:

OS Version: =

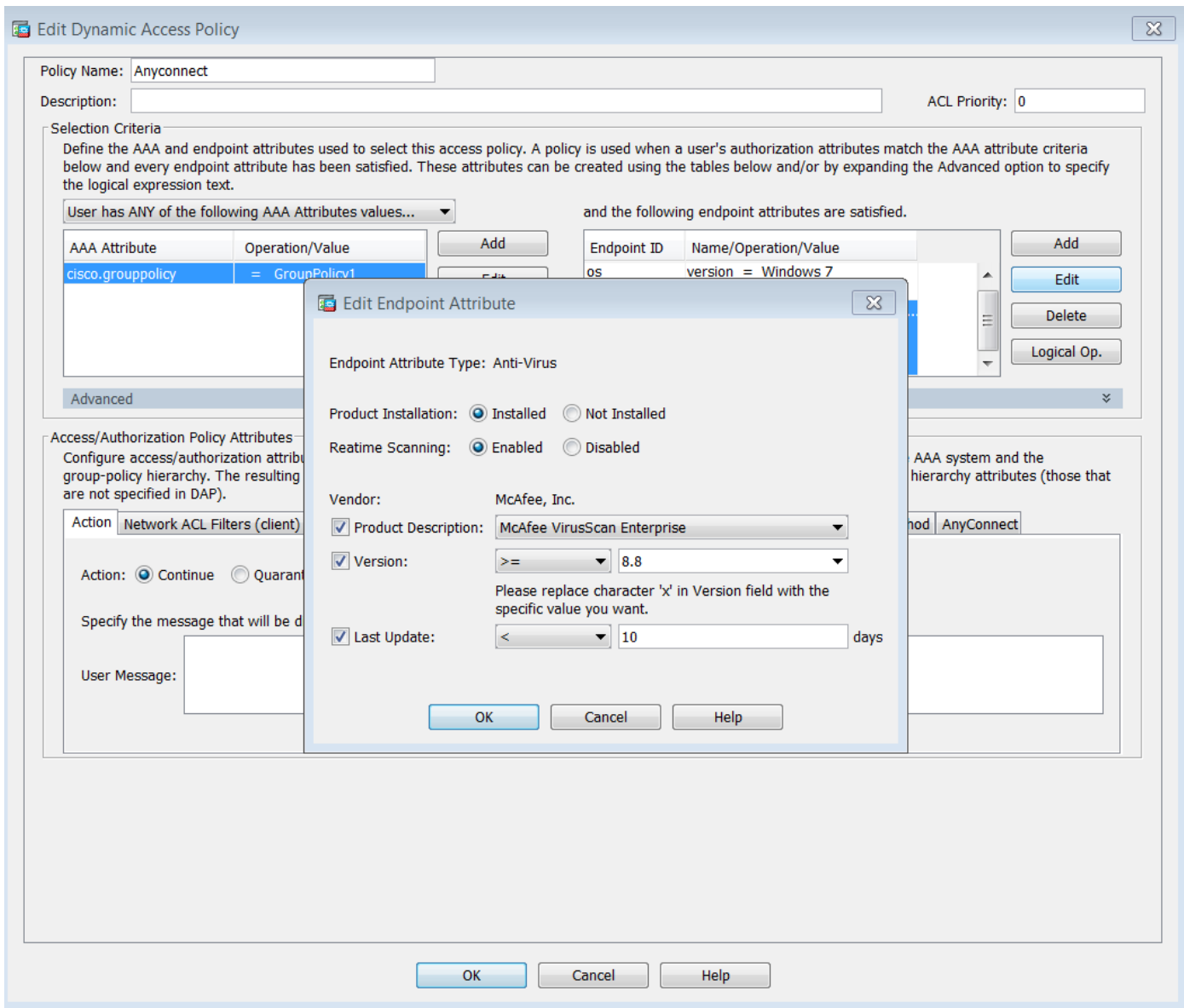
Service Pack: =

Hot Fix: =

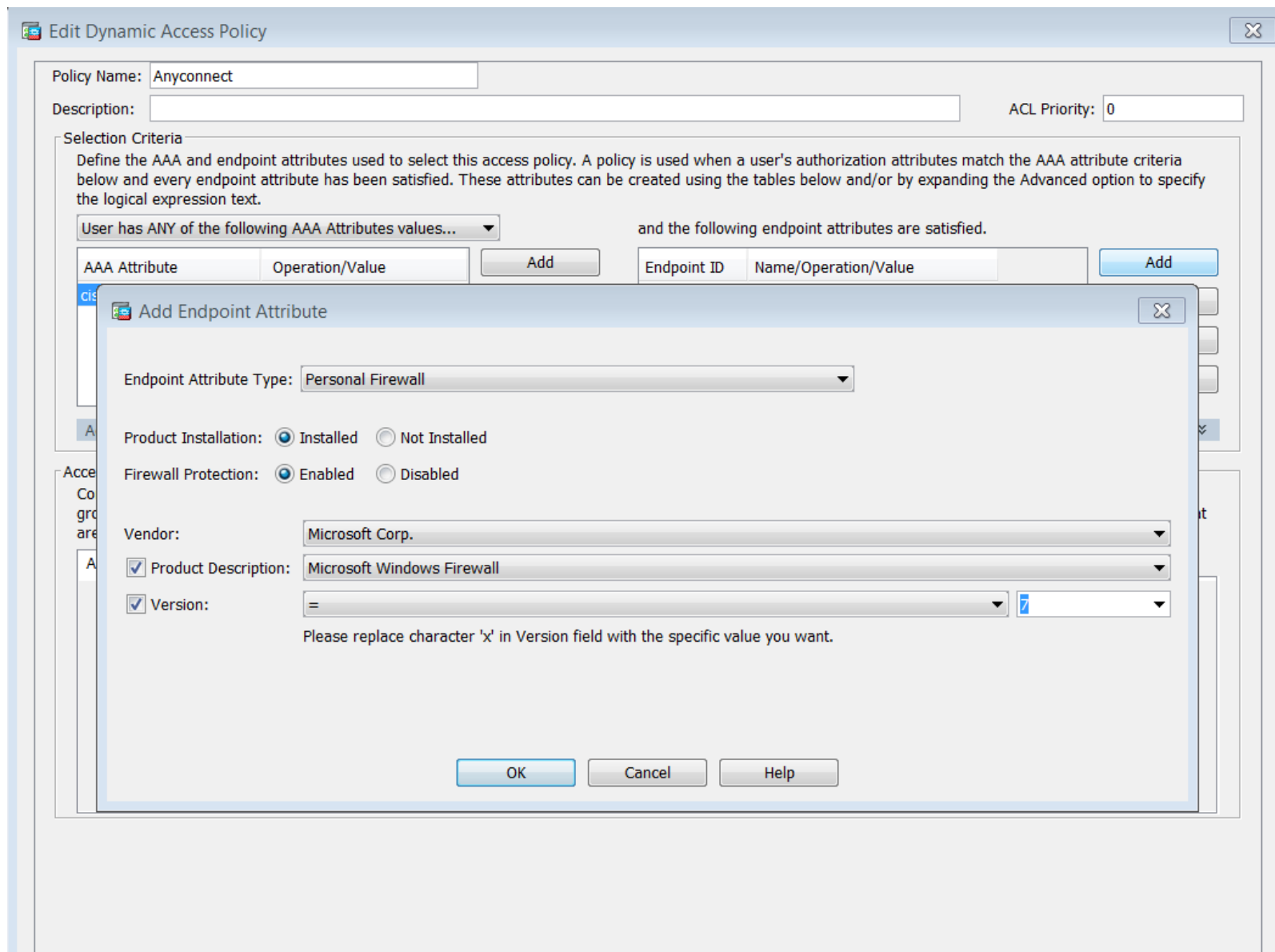
OK Cancel Help



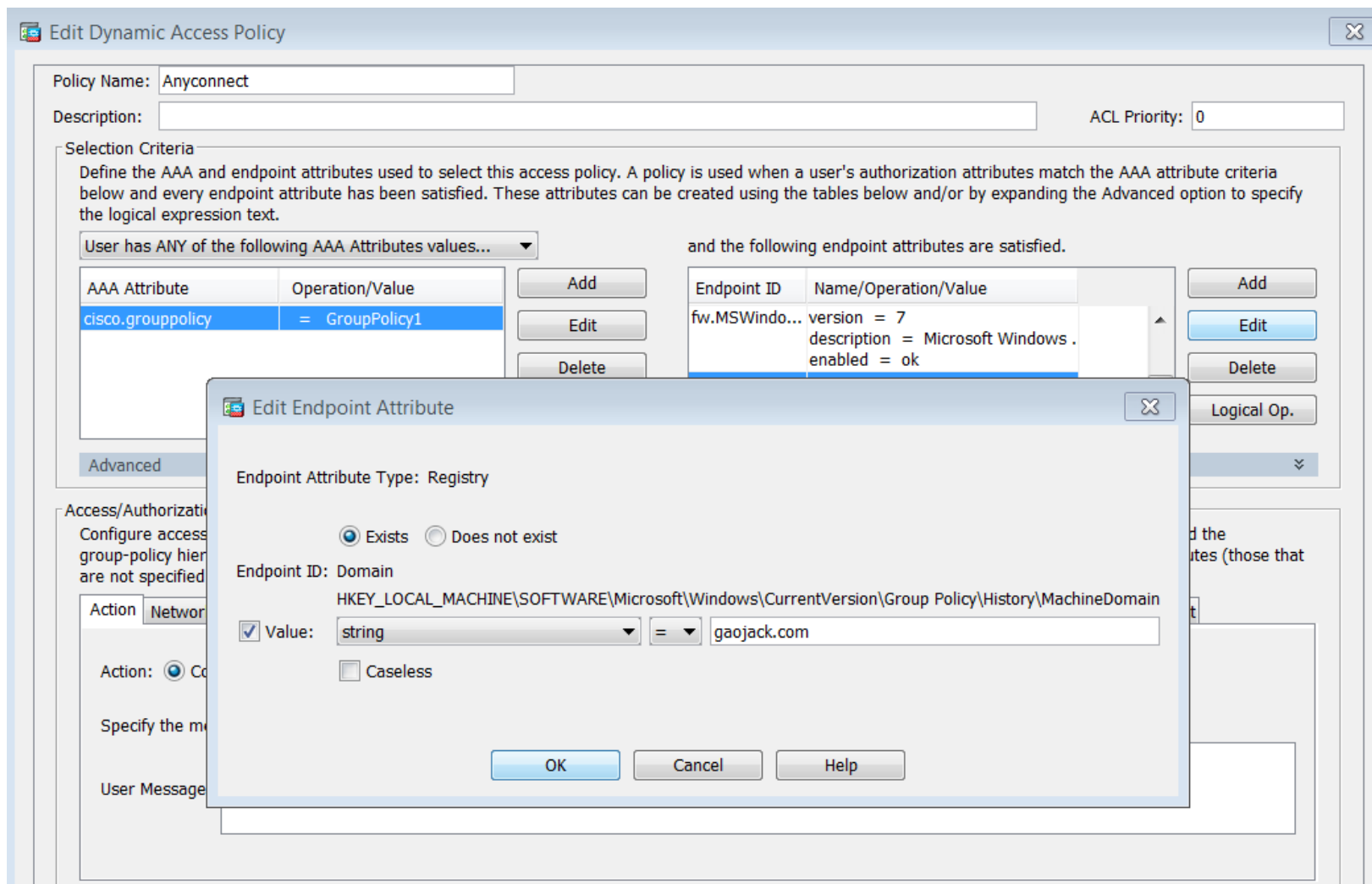
# 新建Endpoint Attribute, 设置扫描杀毒软件检测



# 新建Endpoint Attribute, 设置系统防火墙检测



# 新建Endpoint Attribute, 设置域识别



# 所有Endpoint Attribute是逻辑“与”关系，设置Action为Continue

Policy Name: Anyconnect  
Description:   
ACL Priority: 0

**Selection Criteria**  
Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
cisco.grouppolicy	= GroupPolicy1

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
os	version = Windows 7 servicepack = 1
av.McAfeeAV	description = McAfee VirusScan ... version >= 8.8 lastupdate < 864000 activescan = ok

Advanced

**Access/Authorization Policy Attributes**  
Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action: Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions | Port Forwarding Lists | Bookmarks | Access Method | AnyConnect

Action:  Continue  Quarantine  Terminate

Specify the message that will be displayed when this record is selected.

User Message:

OK Cancel Help

# 确保自定义策略在默认策略之上

The screenshot displays the Cisco ASA configuration interface for Remote Access VPN. The left sidebar shows a tree view of configuration options, with 'Dynamic Access Policies' selected under 'Network (Client) Access'. The main content area shows the configuration page for Dynamic Access Policies, including a table of existing policies.

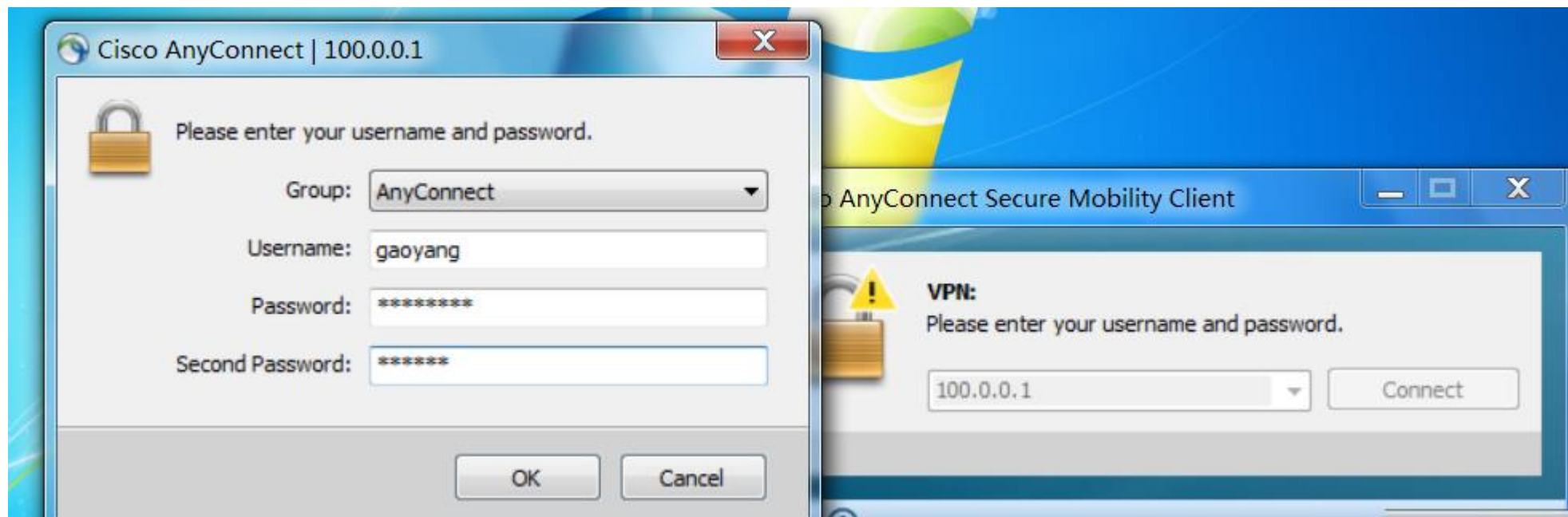
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

Configure Dynamic Access Policies

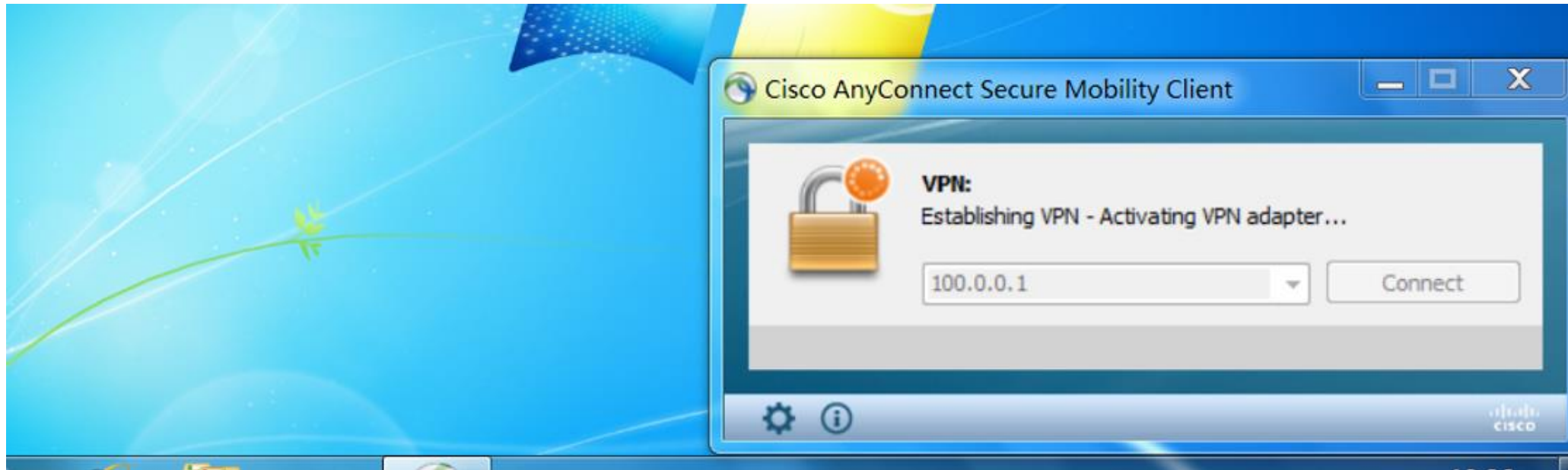
For IPsec, AnyConnect Client, Clientless SSL VPN, and Cut-Through-Proxy sessions, you can configure dynamic access policies (DAP) that define establishment. When none of the DAP policies are matched, the ASA will enforce the DfltAccessPolicy.

ACL Priority	Name	Network ACL List	Webtype ACL List	Description
0	Anyconnect			
-	DfltAccessPolicy			

# Anyconnect登陆系统




# 客户端连接VPN



# ACS和Token分别认证通过

注意:是先认证,后机器扫描

RADIUS Status	NAS Failure	Details	User Name	MAC/IP Address	Access Service	Authentication Method	Network Device Name	NAS IP
<input checked="" type="checkbox"/>			All <input type="text" value="All"/>	All <input type="text" value="All"/>	All <input type="text" value="All"/>	All <input type="text" value="All"/>	All <input type="text" value="All"/>	All <input type="text" value="All"/>
			gaoyang	100.0.0.100	Anyconnect	PAP_ASCII	ASA	10.0.10.1

<input type="radio"/> Client	<input type="radio"/> User DN	<input type="radio"/> Source	Session	Details
<a href="#">10.0.10.1</a>	<a href="#">cn=gaoyang,o=Root</a>	[NA]	<a href="#">CF451FCB</a>	Authentication success (TOKEN)



# ASA上 debug dap trace

```
DAP_TRACE: endpoint.registry["Domain"] = {}
DAP_TRACE: endpoint.registry["Domain"].exists = "true"
DAP_TRACE: endpoint.registry["Domain"].path = "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Group Policy\\History\\MachineDomain"
DAP_TRACE: endpoint.registry["Domain"].type = "string"
DAP_TRACE: endpoint.registry["Domain"].value = "gaojack.com"
DAP_TRACE: endpoint.device.protection_extension = "3.6.10294.2"
DAP_TRACE: endpoint.enforce = "success"
DAP_TRACE: endpoint.fw["MSWindowsFW"] = {}
DAP_TRACE: endpoint.fw["MSWindowsFW"].exists = "true"
DAP_TRACE: endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall"
DAP_TRACE: endpoint.fw["MSWindowsFW"].version = "7"
DAP_TRACE: endpoint.fw["MSWindowsFW"].enabled = "ok"
DAP_TRACE: endpoint.av["McAfeeAV"] = {}
DAP_TRACE: endpoint.av["McAfeeAV"].exists = "true"
DAP_TRACE: endpoint.av["McAfeeAV"].description = "McAfee VirusScan Enterprise"
DAP_TRACE: endpoint.av["McAfeeAV"].version = "8.8.0.777"
DAP_TRACE: endpoint.av["McAfeeAV"].activescan = "ok"
DAP_TRACE: endpoint.av["McAfeeAV"].lastupdate = "310555"
DAP_TRACE: endpoint.av["McAfeeAV"].timestamp = "1454774400"
DAP_TRACE: endpoint.as["McAfeeAV"] = {}
DAP_TRACE: endpoint.as["McAfeeAV"].exists = "true"
DAP_TRACE: endpoint.as["McAfeeAV"].description = "McAfee VirusScan Enterprise"
DAP_TRACE: endpoint.as["McAfeeAV"].version = "8.8.0.777"
DAP_TRACE: endpoint.as["McAfeeAV"].activescan = "ok"
DAP_TRACE: endpoint.as["McAfeeAV"].lastupdate = "310555"
DAP_TRACE: endpoint.as["McAfeeAV"].timestamp = "1454774400"
DAP_TRACE: endpoint.as["MicrosoftAS"] = {}
DAP_TRACE: endpoint.as["MicrosoftAS"].exists = "true"
DAP_TRACE: endpoint.as["MicrosoftAS"].description = "Windows Defender"
DAP_TRACE: endpoint.as["MicrosoftAS"].version = "6.1.7600.16385"
DAP_TRACE: endpoint.as["MicrosoftAS"].activescan = "ok"
DAP_TRACE: endpoint.as["MicrosoftAS"].lastupdate = "164957431"
DAP_TRACE: endpoint.as["MicrosoftAS"].timestamp = "1290127524"
DAP_TRACE: endpoint.anyconnect.clientversion = "4.2.01035"
DAP_TRACE: endpoint.anyconnect.platform = "win"
DAP_TRACE: endpoint.anyconnect.devicetype = "VMware, Inc. VMware Virtual Platform"
DAP_TRACE: endpoint.anyconnect.platformversion = "6.1.7601 Service Pack 1"
DAP_TRACE: endpoint.anyconnect.deviceuniqueid = "B025068EB4504962387F52C71902CBEC83E41D368CE7A1FCA30AEC6A6D524CB5"
DAP_TRACE: endpoint.anyconnect.macaddress["0"] = "00-0c-29-ed-88-84"
DAP_TRACE: Username: gaoyang, Selected DAPs: ,Anyconnect
DAP_TRACE: dap_process_selected daps: selected 1 records
DAP_TRACE: Username: gaoyang, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: gaoyang, DAP_close: 7FFFDD957080
```

# 测试1: 卸载杀毒软件

控制面板主页

查看已安装的更新

打开或关闭 Windows 功能

从网络安装程序

## 卸载或更改程序

若要卸载程序，请从列表中将其中选中，然后单击“卸载”、“更改”或“修复”。

组织 卸载

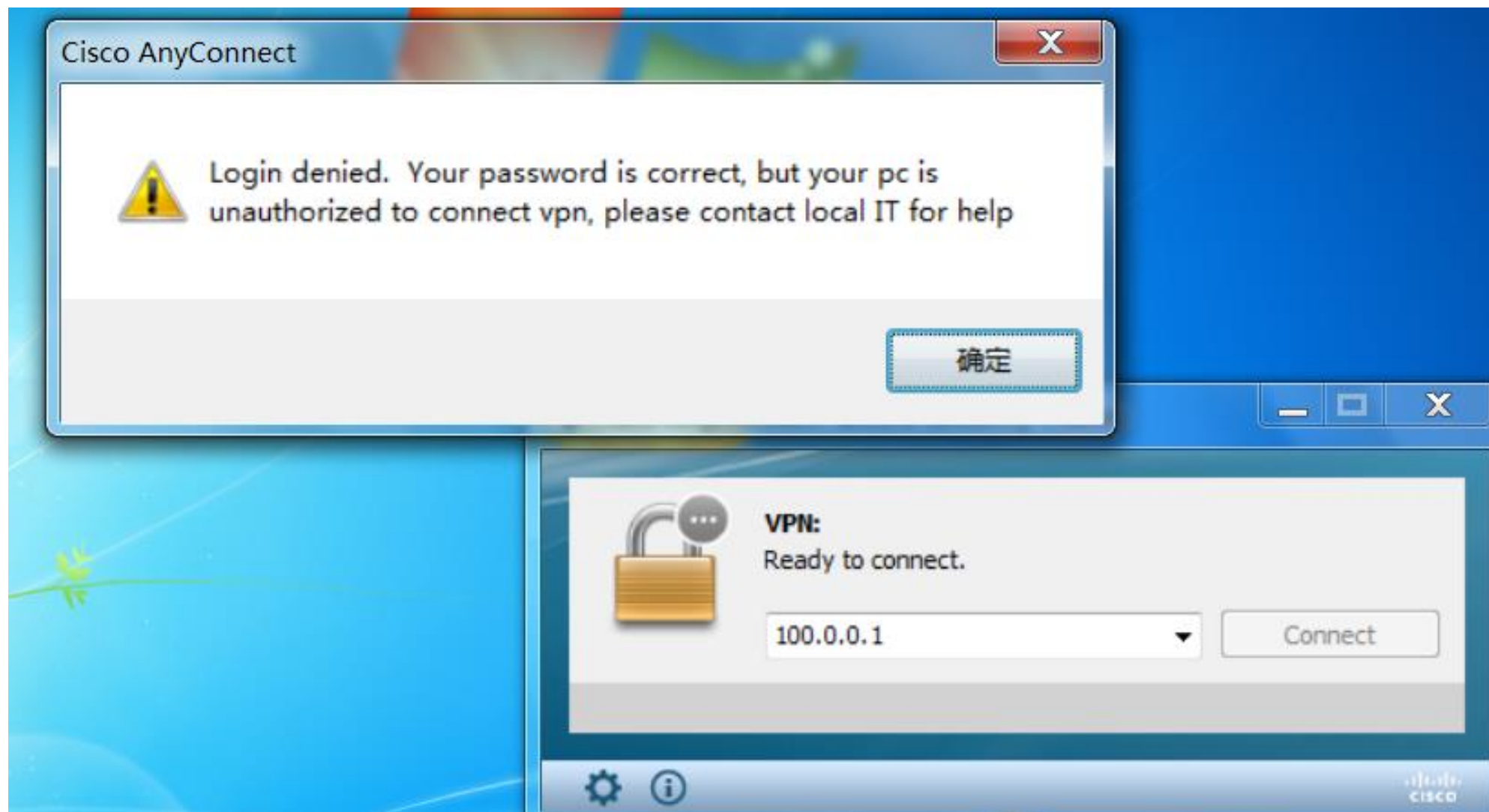
名称	发布者
Cisco AnyConnect Secure Mobility Client	Cisco Systems, Inc.
McAfee Agent	McAfee, Inc.
McAfee VirusScan Enterprise	McAfee, Inc.
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation
VMware Workstation	VMware, Inc.
Windows Live Mail	Microsoft Corporation

Windows Installer

正在准备删除...

取消

# 拒绝用户了在这台机器上登录 给出明确提示的必要性



## 测试2：机器没加域或退域

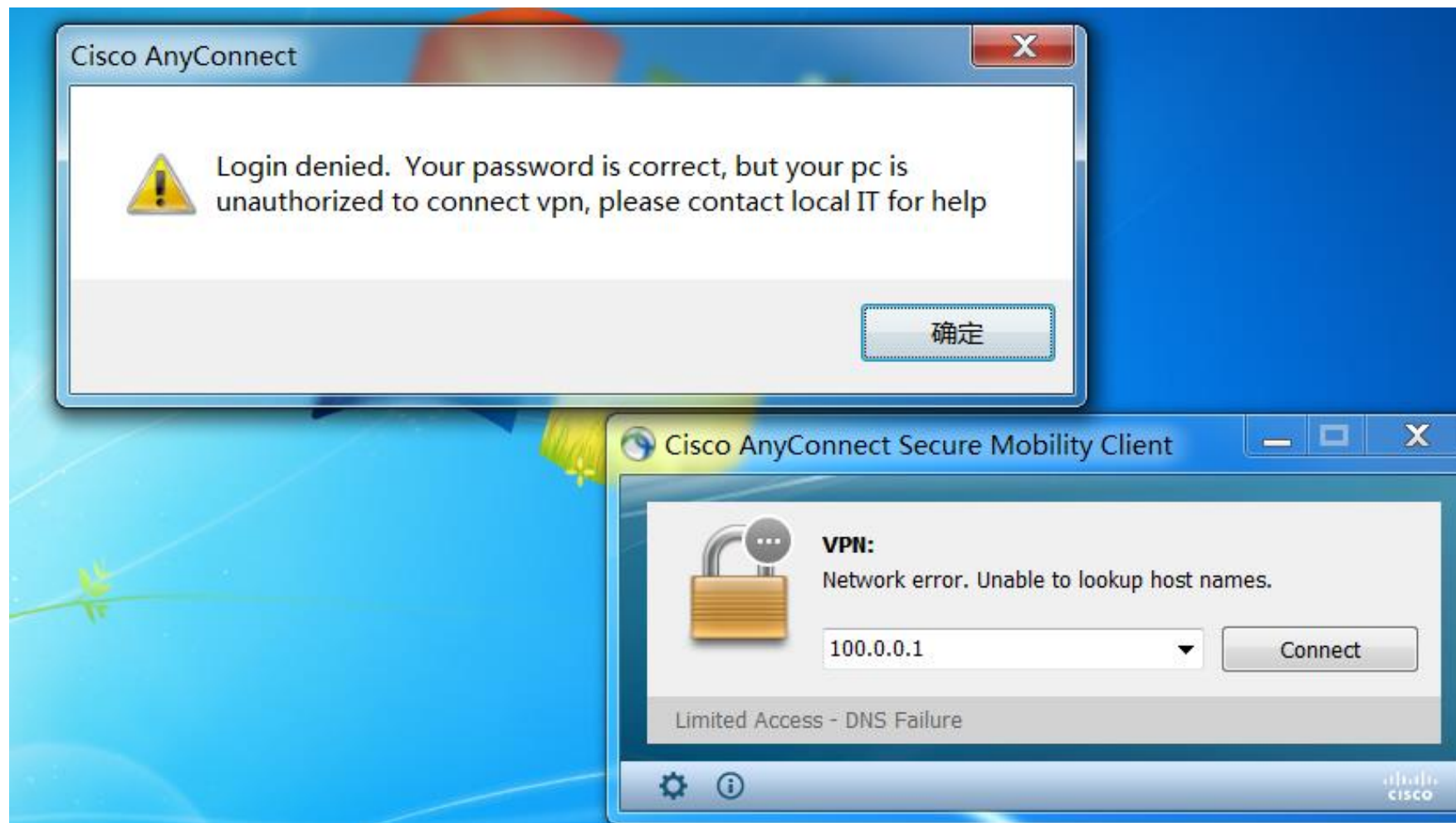
计算机名称、域和工作组设置

---

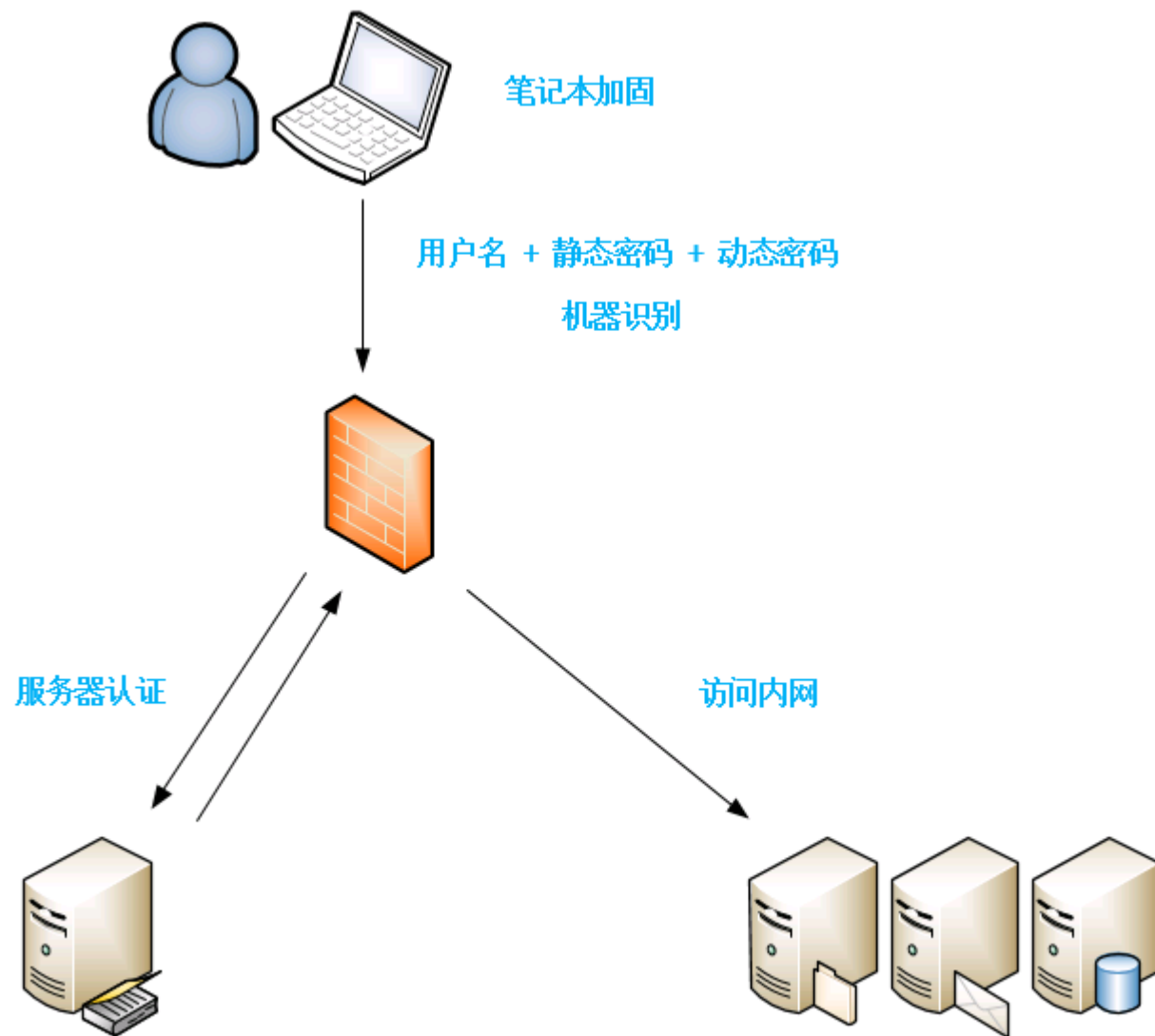
计算机名: csc-win7  
计算机全名: csc-win7  
计算机描述:  
工作组: WORKGROUP

 更改设置

# 拒绝用户了在这台机器上登录 给出明确提示的必要性



# 经过安全加固后的VPN架构



思考：有了以上的所有策略是否就足够安全

如果之前的所有策略都被攻破了怎么办？  
或者合法用户远程上来搞破坏怎么办？

用户能够直接通过Anyconnect访问内部网络



# 用户连接VPN以后的策略

- 访问非关键服务，如mail等可以直接访问
- 访问关键服务，如服务器，网络设备等必须经过堡垒机

# 通过ACS的Download ACL让VPN用户只能访问非关键服务器的端口和堡垒机的端口

The screenshot displays the Cisco ACS web interface for configuring a Downloadable ACL. The left sidebar shows the navigation menu with 'Policy Elements' expanded to 'Downloadable ACLs'. The main content area shows the configuration for 'Anyconnect-DACL'.

Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs > Edit: "Anyconnect-DACL"

**General**

- Name:
- Description:

**Downloadable ACL Content**

```
permit TCP any host 10.0.10.20 eq 465
permit TCP any host 10.0.10.20 eq 993
permit TCP any host 10.0.10.30 eq 443
deny ip any any
```

= Required fields

# 新建Authorization profile

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

**General** | Common Tasks | RADIUS Attributes

⚙ Name:

Description:

⚙ = Required fields

- My Workspace
- Network Resources
- Users and Identity Stores
- Policy Elements**
  - Session Conditions
    - Date and Time
    - Custom
  - Network Conditions
  - Authorization and Permissions
    - Network Access**
      - Authorization Profiles**
      - Security Groups
    - Device Administration
      - Shell Profiles
      - Command Sets
    - Named Permission Objects
      - Downloadable ACLs
      - Security Group ACLs
- Access Policies
- Monitoring and Reports
- System Administration

# 调用DACL

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General Common Tasks RADIUS Attributes

**ACLS**

Downloadable ACL Name: Static Value Anyconnect-DACL

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

**Voice VLAN**

Permission to Join: Not in Use

**VLAN**

VLAN ID/Name: Not in Use

**Reauthentication**

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

**QOS**

Input Policy Map: Not in Use

Output Policy Map: Not in Use

**802.1X-REV**

LinkSec Security Policy: Not in Use

**URL Redirect**

When a URL is defined for Redirect an ACL must also be defined

URL for Redirect: Not in Use

URL Redirect ACL: Not in Use

\* = Required fields

# 调用这个authorization profile到anyconnect访问策略上

The screenshot displays a network management interface. On the left is a navigation tree with the following structure:

- My Workspace
- Network Resources
- Users and Identity Stores
- Policy Elements
- Access Policies**
  - Access Services
    - Service Selection Rules
    - Anyconnect
      - Identity
      - Authorization**
      - Default Device Admin
  - Max User Session Policy
    - Max Session User Settings
    - Max Session Group Settings
  - Max Login Failed Attempts Policy
    - Max Login Failed Attempts Group
  - Security Group Access (SGA)
    - Egress Policy
  - Network Device Access
- Monitoring and Reports
- System Administration

The main content area shows the breadcrumb path: **Access Policies > Access Services > Anyconnect > Authorization**. Below this, there are tabs for **Standard Policy** and **Exception Policy**. The **Network Access Authorization Policy** section includes a filter bar with the following settings:

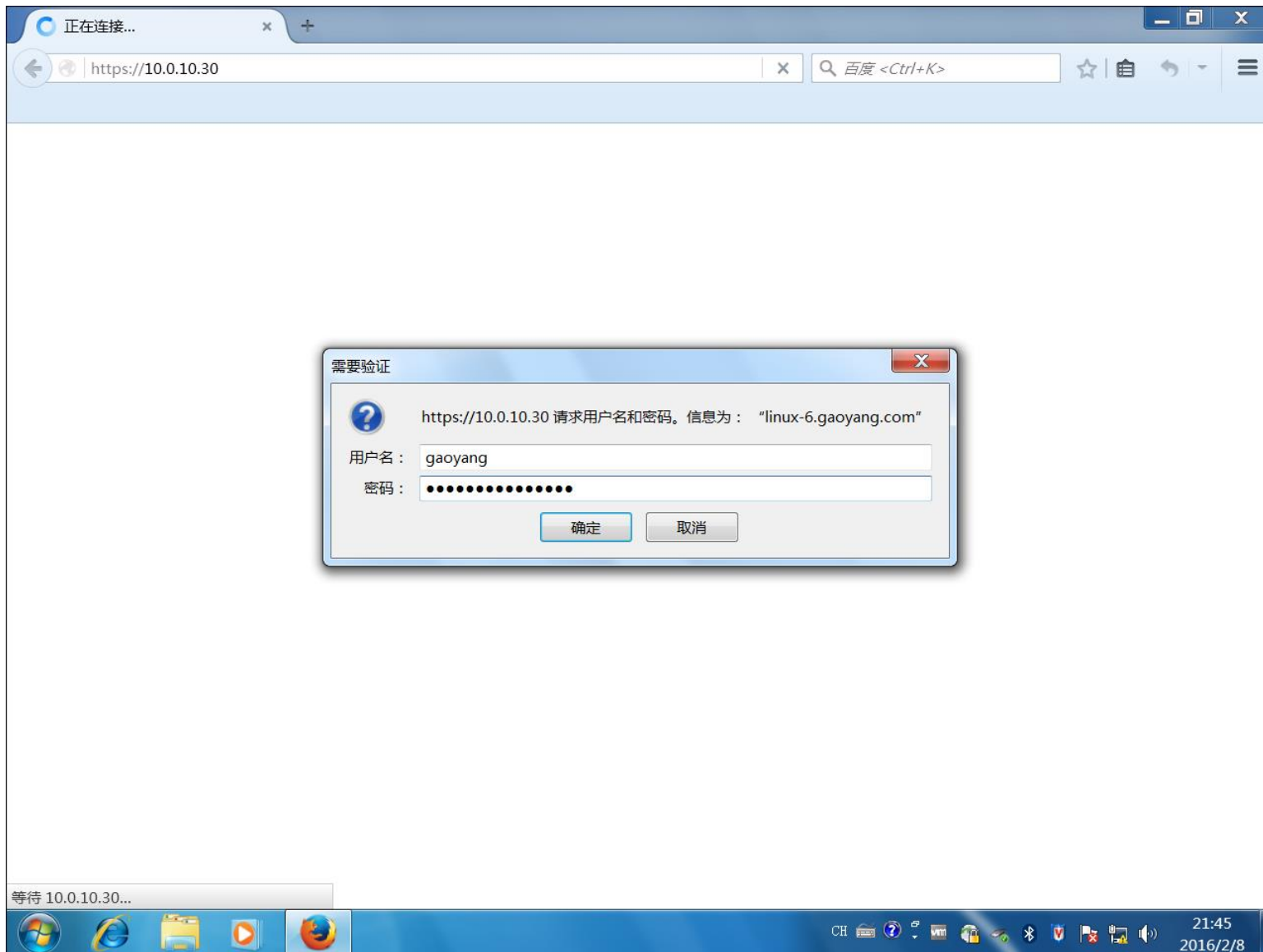
Filter: Status (dropdown) Match if: Equals (dropdown) [Clear Filter] [Go]

	<input type="checkbox"/>	Status	Name	Conditions			Results	Hit Count
				AD1:ExternalGroups	Device Filter	Protocol	Authorization Profiles	
1	<input type="checkbox"/>	●	<a href="#">Rule-1</a>	-ANY-	match ASA	match Radius	Anyconnect	58

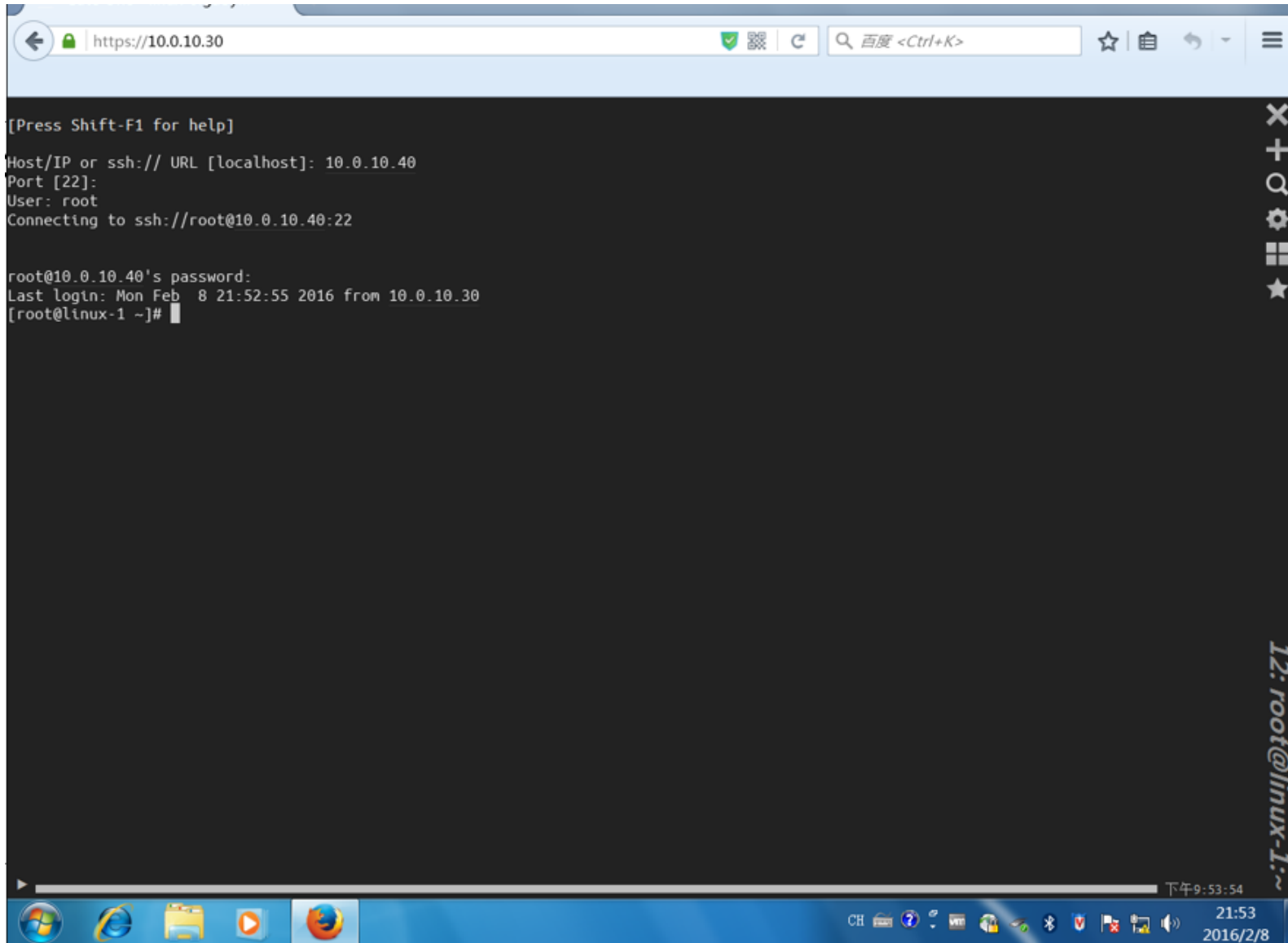
## VPN连接后，在ASA上查看DACL

```
ciscoasa#
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list #ACSACL#-IP-Anyconnect-DACL-56b88b83; 4 elements; name hash: 0xae67e892 (dynamic)
access-list #ACSACL#-IP-Anyconnect-DACL-56b88b83 line 1 extended permit tcp any4 host 10.0.10.20 eq 465 (hitcnt=0) 0xa539e671
access-list #ACSACL#-IP-Anyconnect-DACL-56b88b83 line 2 extended permit tcp any4 host 10.0.10.20 eq 993 (hitcnt=0) 0x27f13021
access-list #ACSACL#-IP-Anyconnect-DACL-56b88b83 line 3 extended permit tcp any4 host 10.0.10.30 eq https (hitcnt=0) 0xaa16d101
access-list #ACSACL#-IP-Anyconnect-DACL-56b88b83 line 4 extended deny ip any4 any4 (hitcnt=26) 0xb736807a
ciscoasa#
```

# VPN客户端只能通过堡垒机访问内部关键服务器，登陆堡垒机还需要额外验证

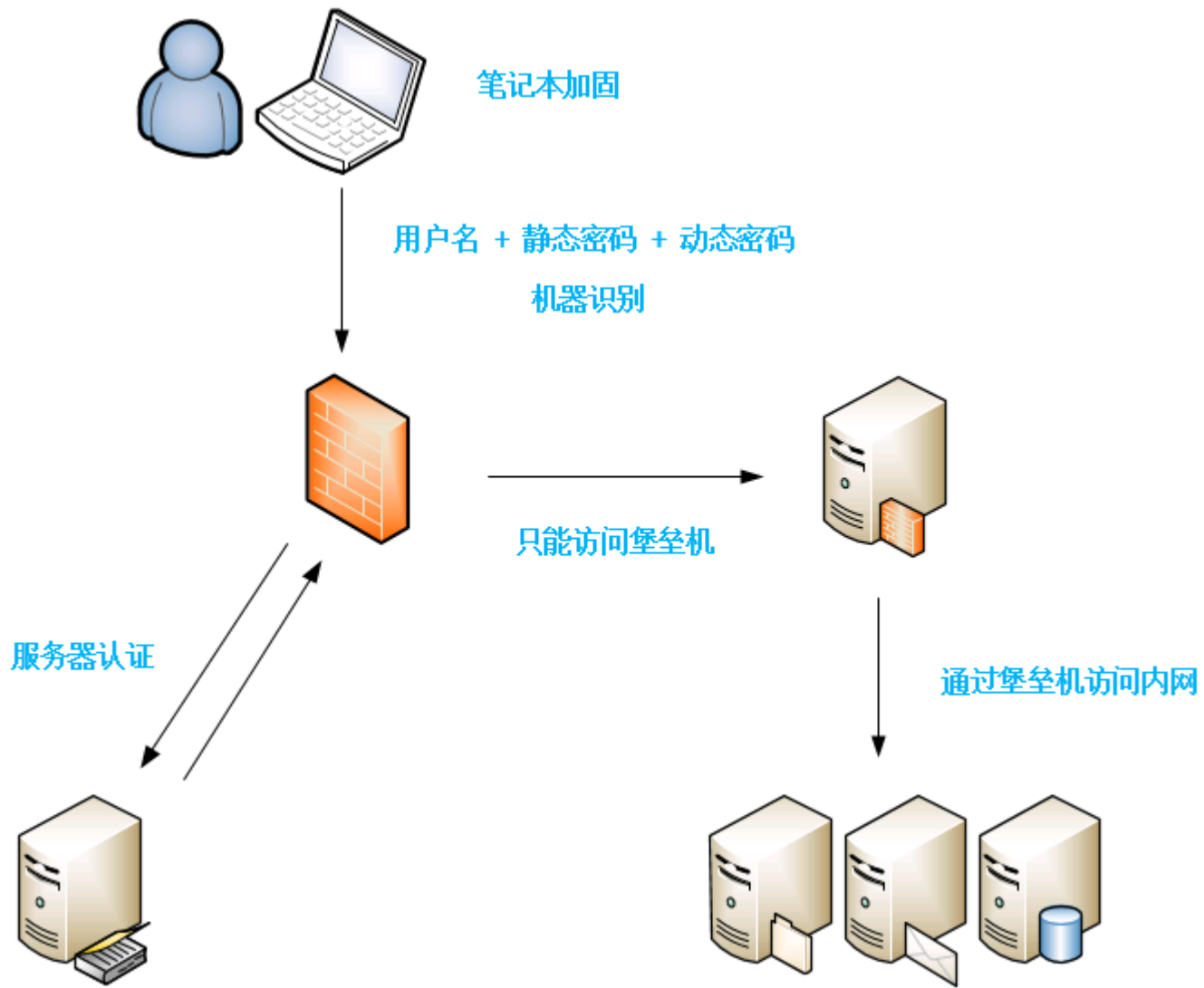


# VPN客户端通过堡垒机访问内部服务器 堡垒机演示





# 带有内部审计的VPN架构



谢谢

**Q & A**