# ASA远程访问VPN IKE/SSL -密码终止和崔凡吉莱RADIUS、TACACS和IDAP配置示例的

## 目录


简介
先决条件
要求
使用的组件
配置
与本地认证的ASA
ACS和本地用户
ACS和活动目录用户
与ACS的ASA通过RADIUS
与ACS的ASA通过TACACS+
与LDAP的ASA
SSL的Microsoft LDAP
LDAP和亚里桑在有效期前
ASA和L2TP
ASA SSL VPN客户端
ASA SSL Web门户
ACS用户崔凡吉莱密码
验证
故障排除
相关信息


## 简介

本文描述在思科可适应安全工具终止的远程访问VPN通道的密码终止和密码更改功能(ASA)。本文包括：

- 不同的客户端：Cisco VPN Client和思科AnyConnect安全移动性
- 不同的协议：TACACS、RADIUS和轻量级目录访问协议(LDAP)
- 思科安全访问控制系统的(ACS)不同的存储：本地和激活目录(AD)

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- ASA配置知识通过命令行界面(CLI)
- VPN配置基础知识在ASA的
- Cisco Secure ACS的基础知识

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco可适应安全工具，版本8.4和以上
- Microsoft Windows服务器2003 SP1
- 思科安全访问控制系统，版本5.4或以上
- Cisco AnyConnect安全移动性，版本3.1
- Cisco VPN Client，版本5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

> 注意：
>
> 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。
>
> 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

### 与本地认证的ASA

与本地定义的用户的ASA不允许使用密码到期或密码更改功能。一个外部服务器，例如RADIUS，TACACS、LDAP或者Windows NT，要求。

### ACS和本地用户

ACS支持密码终止和密码更改本地定义的用户的。例如，您能迫使新建立的用户更改他们的密码在他们的下登录，或者您能禁用在一个特定日期的一个帐户：

您能配置所有用户的一项密码策略。例如，在密码超时后，您能禁用用户帐户(块它没有能力登陆)，或者您能提供选项更改密码：

使用物精确的设置优先于全局设置。

ACS保留从未超时用户标识的一个内部属性。

此属性由用户启用，并且可以使用为了禁用全局帐户终止设置。使用此设置，帐户没有禁用，即使全局策略指示应该是：

## ACS和活动目录用户

ACS可以配置检查AD数据库的用户。支持密码终止和更改，当使用微软询问握手认证协议版本2 (MSCHAPv2)时;请参阅用户指南关于思科安全访问控制系统5.4 ：在ACS 5.4的验证：认证协议和标识存储兼容性关于详细信息。

在ASA，您能使用密码管理功能，正如下一部分所描述，为了强制ASA使用MSCHAPv2。

ACS使用通用网络文件系统(CIFS)分布式计算环境/远程程序调用(DCE/RPC)呼叫，当与域控制器(DC)时目录联系为了更改密码：

ASA能使用RADIUS和TACACS+协议为了接触与AD密码更改的ACS。

## 与ACS的ASA通过RADIUS

RADIUS协议不本地支持密码终止或密码更改。一般，密码认证协议使用RADIUS。ASA发送在纯文本的用户名和密码，并且密码通过使用RADIUS共享的机密然后加密。

在典型方案，当用户密码超时时， ACS返回RADIUS拒绝消息对ASA。ACS注意那：

对于ASA，它是一个简单RADIUS拒绝消息，并且验证发生故障。

要解决此问题， ASA允许使用管理命令在组配置下：

```
tunnel-group RA general-attributes
 authentication-server-group ACS
 password-management
```

管理命令更改行为，以便ASA被迫使用MSCHAPv2，而不是PAP，在RADIUS请求。

MSCHAPv2协议支持密码终止和密码更改。因此，如果在Xauth相位期间， VPN用户在该特定隧道群中登陆了，从ASA的RADIUS请求当前包括MS CHAP挑战：

如果ACS注意用户需要更改密码，返回与MSCHAPv2错误648的RADIUS拒绝消息。

ASA了解该消息并且使用MODE_CFG为了请求从Cisco VPN Client的新密码：

```
Oct 02 06:22:26 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received Password Expiration from Auth server!
```

Cisco VPN Client提交该的对话框提示输入新密码：

ASA发送与MS-CHAP-CPW和MS CHAP NT Enc PW有效负载(新密码)的另一个RADIUS请求：

ACS确认请求并且返回与MS-CHAP2-Success的一RADIUS接受：

这在ACS可以验证，报告'24204密码更改的successfully ：

ASA然后报告成功认证并且继续快速模式进程：

```
Oct 02 06:22:28 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

## 与ACS的ASA通过TACACS+

同样地， TACACS+可以用于密码终止和更改。因为ASA以ASCII认证类型仍然使用TACACS+而不是MSCHAPv2，管理功能不是需要的。

多个信息包被交换，并且ACS请求新密码：

Cisco VPN Client提交与RADIUS使用的对话有所不同)该的对话框(提示输入新密码：

ACS新密码的请求确认：

Cisco VPN Client存在确认方框：

如果确认正确， ACS报告成功认证：

ACS然后记录事件密码顺利地更改：

ASA调试显示交换和成功认证整个过程：

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
   Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

密码更改为ASA是完全透明。它有点更加长TACACS+会话用更多请求和应答数据包，由VPN客户端解析并且被提交给用户更改密码。

## 与LDAP的ASA

Microsoft AD和Sun LDAP服务器模式充分地支持密码终止和更改。

对于密码更改，服务器返回‘bindresponse = invalidCredentials’与‘error= 773.'此错误表明用户必须重置密码。典型的错误代码算入：

| 错误代码 | 错误 |
| --- | --- |
| 525 | 找不到用户 |
| 52e | 凭据无效 |
| 530 | 没允许此时登录 |
| 531 | 没允许在此工作站登录 |
| 532 | 超时的密码 |
| 533 | 禁用的帐户 |
| 701 | 超时的帐户 |
| 773 | 用户必须重置口令 |
| 775 | 锁定的用户帐户 |

配置LDAP服务器：

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
   Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

请使用该配置隧道群和管理功能：

```
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group LDAP
 default-group-policy MY
 password-management
```

配置AD用户，因此密码更改要求：

当用户设法使用Cisco VPN Client时， ASA报告一个无效密码：

```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[111] Session Start
[111] New request Session, context 0xbd835c10, reqType = Authentication
[111] Fiber started
[111] Creating LDAP context with uri=ldap://10.48.66.128:389
[111] Connect to LDAP server: ldap://10.48.66.128:389, status = Successful
[111] supportedLDAPVersion: value = 3
[111] supportedLDAPVersion: value = 2
[111] Binding as Administrator
[111] Performing Simple authentication for Administrator to 10.48.66.128
[111] LDAP Search:
       Base DN = [CN=USers,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[111] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[111] Talking to Active Directory server 10.48.66.128
[111] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[111] Read bad password count 2
[111] Binding as cisco-test
[111] Performing Simple authentication for cisco-test to 10.48.66.128
[111] Simple authentication for cisco-test returned code (49) Invalid
credentials
[111] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 773, vece
[111] Invalid password for cisco-test
```

如果凭证无效， 52e错误出现：

```
[110] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 52e, vece
```

Cisco VPN Client然后请求密码更改：

因为显示策略，此对话框与TACACS或RADIUS使用的对话有所不同。在本例中，策略是七个字符最小密码长度。

一旦用户更改密码， ASA也许从LDAP服务器收到此故障消息：

```
[113] Modify Password for cisco-test successfully converted password to unicode
[113] modify failed, no SSL enabled on connection
```

Microsoft策略要求使用密码修改的安全套接字协议层(SSL)。更改配置：

```
aaa-server LDAP (outside) host 10.48.66.128
 ldap-over-ssl enable
```

## SSL的Microsoft LDAP

默认情况下，在SSL的Microsoft LDAP不工作。为了启用此功能，您必须安装计算机帐户的证书与正确关键分机。欲了解更详细的信息请参阅如何启用在SSL的LDAP与一第三方证书颁发机构。

因为ASA不验证LDAP证书，证书可以均等是自签名证书。请参阅Cisco Bug ID CSCui40212，“允许ASA验证从LDAP服务器的证书”，一个相关增强请求的。

> **注意**：ACS验证在版本5.5和以上的LDAP证书。

要安装证书，请打开mmc控制台，选择**添加/删除管理单元**，添加证书，并且选择**计算机帐户**：

选择**本地计算机**，导入证书到个人存储，并且搬到相关的Certificate Authority (CA)证书委托存储。验证证书委托：

有在ASA版本8.4.2的一bug，此错误也许返回，当您尝试使用在SSL时的LDAP ：

```
ASA(config)# debug ldap 255

[142] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[142] supportedLDAPVersion: value = 3
[142] supportedLDAPVersion: value = 2
[142] Binding as Administrator
[142] Performing Simple authentication for Administrator to 10.48.66.128
[142] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=Administrator]
       Scope   = [SUBTREE]
[142] Request for Administrator returned code (-1) Can't contact LDAP server
```

ASA版本9.1.3正确地与相同的配置一起使用。有两LDAP会话。而第二会话使用密码更改，第一会话归还有代码的773 (超时的密码一失败) ：

```
[53] Session Start
[53] New request Session, context 0xadebe3d4, reqType = Modify Password
[53] Fiber started
[53] Creating LDAP context with uri=ldaps://10.48.66.128:636
[53] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] Binding as Administrator
[53] Performing Simple authentication for Administrator to 10.48.66.128
[53] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[53] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[53] Talking to Active Directory server 10.48.66.128
[53] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
```

```
DC=test-cisco,DC=com
[53] Read bad password count 0
[53] Change Password for cisco-test successfully converted old password to
unicode
[53] Change Password for cisco-test successfully converted new password to
unicode
[53] Password for cisco-test successfully changed
[53] Retrieved User Attributes:

<....most attributes details ommitted for clarity>
accountExpires: value = 130256568000000000 <----- 100ns intervals since
January 1, 1601 (UTC)
```

要验证密码更改，请查看数据包。LDAP服务器的专用密钥可以由Wireshark用于为了解密SSL流量：

在ASA的Internet Key Exchange (IKE) /Authentication，授权和核算(AAA)调试非常类似于在RADIUS验证方案提交的那些。

### LDAP和亚里桑在有效期前

对于LDAP，您能使用发出警告的功能，在密码超时前。ASA在与此设置的密码到期前警告用户90天：

```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```

此处密码在42天超时，并且用户设法登录：

```
ASA# debug ldap 255
<some outputs removed for clarity>

[84] Binding as test-cisco
[84] Performing Simple authentication for test-cisco to 10.48.66.128
[84] Processing LDAP response for user test-cisco
[84] Message (test-cisco):
[84] Checking password policy
[84] Authentication successful for test-cisco to 10.48.66.128
[84] now: Fri, 04 Oct 2013 09:41:55 GMT, lastset: Fri, 04 Oct 2013 09:07:23
GMT, delta=2072, maxage=1244139139 secs
[84] expire in: 3708780 secs, 42 days
[84] Password expires Sat, 16 Nov 2013 07:54:55 GMT
[84] Password expiring in 42 day(s),threshold 90 days
```

ASA发出警告并且提供密码更改的选项：

如果用户选择更改密码，有一提示输入新密码，并且正常密码更改步骤开始。

## ASA和L2TP

前面的示例提交了IKE版本1 (IKEv1)和IPSec VPN。

对于第2层隧道协议和IPSec， PPP使用作为传输验证。MSCHAPv2要求而不是一密码更改的PAP对工作：

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

对于在L2TP的扩展认证在PPP会话里面， MSCHAPv2协商：

当用户密码超时时，有代码的648一失败返回：

密码更改然后必要。进程的其余非常类似于RADIUS的方案与MSCHAPv2。

请参阅在Windows 2000/XP PC和PIX/ASA 7.2之间的IPSec上的L2TP使用预先共享密钥配置示例关于关于怎样的其他详细信息配置L2TP。

## ASA SSL VPN客户端

前面的示例是指IKEv1和Cisco VPN Client，是到期(EOL)。

远程访问VPN的推荐的解决方案是思科AnyConnect安全移动性，使用IKE版本2 (IKEv2)和SSL协议。密码更改和终止功能工作同一为作为他们为Cisco VPN Client执行的思科AnyConnect。

对于IKEv1，密码更改和终止数据交换在ASA和VPN客户端之间相位的1.5 (Xauth/模式配置)。

对于IKEv2，它是类似的;配置模式使用CFG_REQUEST/CFG_REPLY数据包。

对于SSL，数据在控制数据报传输传送层安全(DTL)会话上。

配置是相同的为ASA。

这是与思科AnyConnect和SSL协议的一配置示例用在SSL的一个LDAP服务器：

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

一旦超时)的正确密码(提供，思科AnyConnect设法连接并且请求新密码：

日志表明用户凭证两次被输入了：

更多详细的日志是可用的在诊断AnyConnect报告工具(箭)。

## ASA SSL Web门户

同一登录过程在Web门户发生：

同一个密码到期和更改过程发生：

## ACS用户崔凡吉莱密码

如果更改在VPN的密码是不可能的，您能使用ACS用户崔凡吉莱密码(UCP)专用的网站服务。请参阅软件开发商的指南关于思科安全访问控制系统5.4 ：使用UCP网站服务。

# 验证

当前没有可用于此配置的验证过程。

## 故障排除

目前没有针对此配置的故障排除信息。

## 相关信息

- Cisco ASA 5500系列配置指南使用CLI，8.4和8.6 ：配置安全工具用户授权的一个外部服务器
- 技术支持和文档 - Cisco Systems