VPN de acceso remoto IKE/SSL ASA - Vencimiento y cambio de la contraseña para el RADIUS, el TACACS, y el ejemplo de la Configuración LDAP

Contenido

Introducción

Este documento describe las características del cambio del vencimiento de la contraseña y de la contraseña en un túnel del VPN de acceso remoto terminadas en un dispositivo de seguridad adaptante de Cisco (ASA). Los documentos abarca:

- Diversos clientes: Cliente Cisco VPN y movilidad segura de Cisco AnyConnect
- Diversos protocolos: TACACS, RADIUS, y Lightweight Directory Access Protocol (LDAP)
- Diversos almacenes en el Cisco Secure Access Control System (ACS): local y Active Directory (AD)

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la configuración ASA a través del comando line interface(cli)
- Conocimiento básico de la configuración VPN en un ASA
- Conocimiento básico del Cisco Secure ACS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad adaptante de Cisco, versión 8.4 y posterior
- Microsoft Windows server 2003 SP1
- Cisco Secure Access Control System, versión 5.4 o posterior
- Movilidad segura de Cisco AnyConnect, versión 3.1
- Cliente Cisco VPN, versión 5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

> Notas:
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

ASA con la autenticación local

Un ASA con los usuarios localmente definidos no permite el uso de las características del cambio del vencimiento de contraseña o de la contraseña. Requieren a un servidor externo, tal como RADIUS, TACACS, LDAP, o Windows NT.

ACS y usuarios locales

El ACS soporta el vencimiento de la contraseña y el cambio de la contraseña para los usuarios

localmente definidos. Por ejemplo, usted puede forzar a los usuarios creados recientemente a cambiar su contraseña en su login siguiente, o usted puede inhabilitar una cuenta una fecha específica:

Usted puede configurar una política de contraseña para todos los usuarios. Por ejemplo, después de que expire una contraseña, usted puede inhabilitar la cuenta de usuario (bloque él sin la capacidad de iniciar sesión), o usted puede ofrecer la opción para cambiar la contraseña:

Las configuraciones específicas del usuario toman la precedencia sobre las configuraciones globales.

ACS-RESERVADo-nunca-Expirar es un atributo interno para la Identificación del usuario.

Este atributo es habilitado por el usuario y se puede utilizar para inhabilitar las configuraciones globales del vencimiento de la cuenta. Con esta configuración, una cuenta no se inhabilita incluso si la política global indica que debe ser:

ACS y usuarios de Active Directory

El ACS se puede configurar para marcar a los usuarios en una base de datos AD. Se soporta el vencimiento y el cambio de la contraseña cuando el protocolo microsoft challenge handshake authentication versión 2 (MSCHAPv2) se utiliza; vea el guía del usuario para el Cisco Secure Access Control System 5.4: Autenticación en ACS 5.4: Compatibilidad del almacén del protocolo de autenticación y de la identidad para los detalles.

En un ASA, usted puede utilizar la característica de la administración de contraseñas, según lo descrito en la siguiente sección, para forzar el ASA para utilizar el MSCHAPv2.

El ACS utiliza la llamada del Distributed Computing Environment/de la llamada a procedimiento remoto del Common Internet File System (CIFS) (DCE/RPC) cuando entra en contacto el directorio del controlador de dominio (DC) para cambiar la contraseña:

El ASA puede utilizar los protocolos RADIUS y TACACS+ para entrar en contacto con el ACS para un cambio de la contraseña AD.

ASA con el ACS vía el RADIUS

El protocolo RADIUS no soporta nativo el cambio del vencimiento de la contraseña o de la contraseña. Típicamente, el protocolo password authentication (PAP) se utiliza para el RADIUS. El ASA envía el nombre de usuario y contraseña en el sólo texto, y la contraseña entonces se cifra con el uso del secreto compartido RADIUS.

En un escenario típico cuando ha expirado la contraseña del usuario, el ACS vuelve un mensaje del Radio-rechazo al ASA. El ACS nota eso:

Para el ASA, es un mensaje simple del Radio-rechazo, y la autenticación falla.

Para solucionar este problema, el ASA permite el uso del comando de la **administración de contraseñas** bajo configuración del grupo de túnel:

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

El comando de la **administración de contraseñas** cambia el comportamiento para forzar el ASA para utilizar el MSCHAPv2, bastante que el PAP, en el pedido de RADIUS.

El vencimiento de la contraseña de los soportes a protocolo del MSCHAPv2 y la contraseña cambian. Así pues, si un usuario de VPN ha aterrizado en que el grupo de túnel específico durante la fase del Xauth, el pedido de RADIUS del ASA ahora incluye un MS-GRIETA-desafío:

Si el ACS nota que el usuario necesita cambiar la contraseña, vuelve un mensaje del Radio-rechazo con el error 648 del MSCHAPv2.

El ASA entiende ese mensaje y utiliza MODE_CFG para pedir la nueva contraseña del Cliente Cisco VPN:

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

El Cliente Cisco VPN presenta un cuadro de diálogo que indique para una nueva contraseña:

El ASA envía otro pedido de RADIUS con el payload un MS-CHAP-CPW y MS-GRIETA-NT-Enc-picovatio (la nueva contraseña):

El ACS confirma la petición y vuelve un Radio-validar con MS-CHAP2-Success:

Esto se puede verificar en el ACS, que señala un successfully cambiado contraseña '24204:

El ASA después señala la autenticación satisfactoria y continúa con el proceso del quick mode (QM):

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

ASA con el ACS vía el TACACS+

Semejantemente, el TACACS+ se puede utilizar para el vencimiento y el cambio de la contraseña. La característica de la administración de contraseñas no es necesaria, porque el ASA todavía utiliza el TACACS+ con un tipo de autenticación de ASCII en vez del MSCHAPv2.

Se intercambian los paquetes múltiples, y el ACS pide una nueva contraseña:

El Cliente Cisco VPN presenta a cuadro de diálogo (que diferencia del diálogo usado por el RADIUS) ese los prompts para una nueva contraseña:

El ACS pide la confirmación de la nueva contraseña:

El presente del Cliente Cisco VPN un cuadro de la confirmación:

Si la confirmación está correcta, el ACS señala una autenticación satisfactoria:

El ACS entonces registra un evento que la contraseña se ha cambiado con éxito:

Los debugs ASA muestran todo el proceso del intercambio y de la autenticación satisfactoria:

```
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.
```

Que el cambio de la contraseña es totalmente transparente para el ASA. Es apenas un bit más de largo la sesión TACACS+ con más petición y paquetes de respuesta, que son analizados por el cliente VPN y presentados al usuario que está cambiando la contraseña.

ASA con el LDAP

El vencimiento y el cambio de la contraseña son soportados completamente por Microsoft AD y el esquema del servidor LDAP de Sun.

Para un cambio de la contraseña, el “bindresponse = los invalidCredentials” de la vuelta de los servidores con el 'error = este error 773.' indica que el usuario debe reajustar la contraseña. Los códigos de error frecuente incluyen:

Código de error	Error
525	Usuario no encontrado
52e	Invalid credentiales (Credencial no válida)
530	No permitido para abrir una sesión ahora
531	No permitido para abrir una sesión en este puesto de trabajo
532	La contraseña expiró
533	Cuenta inhabilitada
701	La cuenta expiró
773	El usuario debe reajustar la contraseña
775	Cuenta de usuario bloqueada

Configure al servidor LDAP:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.48.66.128
 ldap-base-dn CN=USers,DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
 server-type microsoft
```

Utilice esa configuración para el grupo de túnel y la característica de la administración de contraseñas:

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

Configure al usuario AD así que se requiere un cambio de la contraseña:

Cuando el usuario intenta utilizar al Cliente Cisco VPN, el ASA señala una contraseña no válida:

```
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
```

Si las credenciales son inválidas, el error 52e aparece:

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

El Cliente Cisco VPN entonces pide un cambio de la contraseña:

Este cuadro de diálogo diferencia del diálogo usado por el TACACS o el RADIUS porque visualiza la directiva. En este ejemplo, la directiva es una longitud de contraseña mínima de siete caracteres.

Una vez que el usuario cambia la contraseña, el ASA pudo conseguir este mensaje de error del servidor LDAP:

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

La directiva de Microsoft requiere el uso de Secure Sockets Layer (SSL) para la modificación de la contraseña. Cambie la configuración:

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

Microsoft LDAP para el SSL

Por abandono, Microsoft LDAP sobre el SSL no trabaja. Para habilitar esta función, usted debe instalar el certificado para la cuenta del ordenador con la extensión dominante correcta. Vea cómo habilitar el LDAP sobre el SSL con las autoridades de certificación de tercera persona para más

detalles.

El certificado puede incluso ser un certificado autofirmado porque el ASA no verifica el certificado LDAP. Vea el Id. de bug Cisco CSCui40212, “permiten que el ASA valide el certificado del servidor LDAPS,” para un pedido de mejora relacionado.

> Nota: El ACS verifica el certificado LDAP en la versión 5.5 y posterior.

Para instalar el certificado, abra la consola mmc, selecta **agregue/quite Broche-en**, agregue el certificado, y elija la **cuenta de la Computadora**:

Seleccione la **computadora local**, importe el certificado al almacén personal, y mueva el certificado asociado del Certificate Authority (CA) al almacén de confianza. Verifique que el certificado esté confiado en:

Hay un bug en la Versión de ASA 8.4.2, donde este error pudo ser vuelto cuando usted está intentando utilizar el LDAP sobre el SSL:

```
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
```

Trabajos de la Versión de ASA 9.1.3 correctamente con la misma configuración. Hay dos sesiones LDAP. La primera sesión vuelve un error con el código 773 (la contraseña expiró), mientras que la segunda sesión se utiliza para el cambio de la contraseña:

```
[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)
```

Para verificar el cambio de la contraseña, mire los paquetes. La clave privada del servidor LDAP se puede utilizar por Wireshark para desencriptar el tráfico SSL:

Los debugs del Internet Key Exchange (IKE) /Authentication, de la autorización, y de las estadísticas (AAA) en el ASA son muy similares a ésos presentados en el escenario de la autenticación de RADIUS.

LDAP y advertencia antes de la expiración

Para el LDAP, usted puede utilizar una característica que envíe una advertencia antes de que expire una contraseña. El ASA advierte al usuario 90 días antes del vencimiento de contraseña con esta configuración:

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

Aquí la contraseña está expirando en 42 días, y el usuario intenta iniciar sesión:

```
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
```

El ASA envía una advertencia y ofrece la opción para un cambio de la contraseña:

Si el usuario elige cambiar la contraseña, hay un prompt para una nueva contraseña, y el procedimiento normal del cambio de la contraseña comienza.

ASA y L2TP

Los ejemplos anteriores presentaron la versión 1 (IKEv1) IKE y un IPSec VPN.

Para el protocolo Layer 2 Tunneling Protocol (L2TP) y el IPSec, el PPP se utiliza como transporte para la autenticación. El MSCHAPv2 se requiere en vez del PAP para un cambio de la contraseña al trabajo:

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

Para la autenticación ampliada en el L2TP dentro de la sesión PPP, se negocia el MSCHAPv2:

Cuando ha expirado la contraseña del usuario, vuelven a un error con el código 648:

Un cambio de la contraseña entonces se necesita. El resto del proceso es muy similar al escenario para el RADIUS con el MSCHAPv2.

Vea el L2TP sobre el IPSec entre Windows 2000/XP PC y PIX/ASA 7.2 usando el ejemplo de configuración de la clave previamente compartida para los detalles adicionales en cómo configurar el L2TP.

Cliente VPN ASA SSL

Los ejemplos anteriores refirieron a IKEv1 y al Cliente Cisco VPN, que es el fin de vida (EOL).

La solución recomendada para un VPN de acceso remoto es la movilidad segura de Cisco AnyConnect, que utiliza el IKE versión 2 (IKEv2) y los Protocolos SSL. El cambio y las funciones de vencimiento de la contraseña trabajan exactamente lo mismo para Cisco AnyConnect que hicieron para el Cliente Cisco VPN.

Para IKEv1, los datos del cambio de la contraseña y del vencimiento fueron intercambiados entre el ASA y el cliente VPN en la fase 1.5 (Xauth/configuración de modo).

Para IKEv2, son similares; el modo de configuración utiliza los paquetes CFG_REQUEST/CFG_REPLY.

Para el SSL, los datos están en la sesión de la Seguridad de la capa de transporte de datagrama del control (DTL).

La configuración es lo mismo para el ASA.

Esto es un ejemplo de configuración con Cisco AnyConnect y el Protocolo SSL con un servidor LDAP sobre el SSL:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host win2003-mga.test-cisco.com
 ldap-base-dn CN=Users,DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
 ldap-over-ssl enable
 server-type microsoft

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

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

```
tunnel-group RA webvpn-attributes
 group-alias RA enable
 without-csd

ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0
```

La contraseña correcta (que ha expirado) se proporciona una vez, Cisco AnyConnect intenta conectar y pide una nueva contraseña:

Los registros indican que los credenciales de usuario fueron ingresados dos veces:

Registros más detallados están disponibles en la herramienta de informe de diagnóstico de AnyConnect (DARDO).

Portal web ASA SSL

El mismo proceso de ingreso ocurre en el portal web:

El mismo vencimiento de contraseña y proceso de cambio ocurre:

Contraseña del cambio del usuario de ACS

Si no es posible cambiar la contraseña sobre el VPN, usted puede utilizar el servicio web dedicado de la contraseña del cambio del usuario de ACS (UCP). Vea la guía del desarrollar de software para el Cisco Secure Access Control System 5.4: Usando los servicios web UCP.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6: Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad
- Soporte Técnico y Documentación - Cisco Systems