Configure la red inalámbrica unificada para la autenticación contra la base de datos eDirectory del Novell's

Contenido

Introducción

En el espacio de la educación K-12, ha habido una necesidad cada vez mayor de autenticar a los usuarios de red inalámbrica vía las cuentas creadas dentro del Novell's eDirectory. Debido a la naturaleza distribuida del entorno K-12, las escuelas individuales no pudieron tener los recursos para colocar a un servidor de RADIUS en cada sitio ni hacen ellas desean los gastos indirectos adicionales de configurar a estos servidores de RADIUS. La única forma de lograr esto está usando el LDAP a comunicar entre el regulador del Wireless LAN (WLC) y un servidor LDAP. Los controladores LAN de la tecnología inalámbrica de Cisco soportan la autenticación EAP local contra las bases de datos de LDAP externas tales como Microsoft Active Directory. Este informe oficial ofrece información sobre un Cisco WLC que se haya configurado para la autenticación EAP local frente a un eDirectory de Novell habilitado como servidor LDAP con plenas funciones. Una advertencia a observar – los clientes probados utilizaban la utilidad de escritorio del Cisco Aironet para realizar la autenticación del 802.1x. El Novell no soporta actualmente el 802.1x con su cliente ahora. Como consecuencia, dependiendo del cliente, un proceso de ingreso de dos etapas podía ocurrir. Observe estas referencias:

Declaración del 802.1x del Novell

“Actualmente, deben iniciar sesión dos veces. Cuando el cliente Novell está instalado, un usuario debe iniciar sesión usando la casilla de verificación del puesto de trabajo solamente en el diálogo de la conexión con el sistema inicial para permitir la autenticación de usuario del 802.1x cuando se inicializa el escritorio, y entonces deben iniciar sesión a la red Novell usando la utilidad del login “N roja”. Esto se refiere como login de dos etapas.”

Una alternativa al “login del puesto de trabajo solamente” es configurar al cliente Novell para

utilizar el “Novell inicial Login=Off” en las configuraciones avanzadas del login (el valor por defecto es “Novell inicial Login=On”). Para más información, refiera a la autenticación del 802.1x y al cliente Novell para Windows .

Los clientes del otro vendedor tales como cliente de Meetinghouse Aeigs (Cisco Secure Services Client) un partner de tecnología del Novell pueden no requerir un login doble. Para más información, refiera a la TUTELA SecureConnect .

Otra solución alternativa viable para el cliente Novell es tener la máquina (o el usuario) autentica (802.1x) a la red inalámbrica (WLAN) antes del Novell GINA que es ejecutada.

La prueba de una solución para la sola muestra encendido con el cliente Novell y el 802.1x está fuera del alcance de este White Paper.

Topología probada

Solución probada

- Controlador LAN de la tecnología inalámbrica de Cisco con el software de 6.0.188.0
- LWAPP AP 1242AG del Cisco Aironet
- Windows XP con la utilidad de escritorio 4.4 del Cisco Aironet
- Servidor Windows 2003 con el Novell 8.8,5 eDirectory
- Novell ConsoleOne 1.3.6h (utilidad de administración eDirectory)

Topología de red

Figura 1

Dispositivo	DIRECCIÓN IP	Máscara de subnet	Gateway predeterminado
Novell eDirectory	192.168.3.3	255.255.255.0	192.168.3.254
Switch de la capa 3	192.168.3.254	255.255.255.0	-
AP	Asignado vía el DHCP del Switch L3	255.255.255.0	192.168.3.254
Interfaz del administrador del WLC AP de la interfaz de administración del WLC	192.168.3.253 192.168.3.252	255.255.255.0	192.168.3.254

Configuración

Configuración eDirectory del Novell

La instalación eDirectory y la configuración del Novell lleno está fuera del alcance de este White Paper. El Novell eDirectory debe ser instalado así como los componentes correspondientes LDAP.

Los parámetros de la configuración dominantes requeridos son que la contraseña sencilla se deba habilitar para las cuentas de usuario y el LDAP autenticado debe ser configurado. Usando TLS para el LDAP fue soportado en las versiones anteriores del código del WLC (4.2); sin embargo, el LDAP seguro se soporta no más en el software del controlador de WLAN de Cisco.

1. Al configurar la porción del servidor LDAP de eDirectory, aseegurese que los puertos NON-cifrados LDAP (389) están habilitados. Véase el cuadro 2 de la aplicación del iManager del Novell.**Figura 2**
2. Durante la instalación eDirectory, le pedirá la estructura de árbol o el Domain Name, etc. Si es eDirectory está instalado ya, Novell's ConsoleOne (el cuadro 3) es una herramienta fácil por la cual ver la estructura eDirectory. Es crítico encontrar cuáles son los esquemas apropiados al intentar establecer la comunicación al WLC. Usted debe también hacer una cuenta crear que permita que el WLC realice un lazo autenticado al servidor LDAP. Para la simplicidad, en este caso, la cuenta de administración eDirecotry del Novell se utiliza para el lazo autenticado.**Figura 3**
3. Utilice ConsoleOne para verificar que el grupo LDAP permite las **contraseñas de texto sin cifrar**.**'Figura 4'**
4. Verifique eso bajo el OU, los ajustes de seguridad que la **contraseña sencilla** esté habilitada.**Figura 5**

Otra herramienta útil por la cual ver la estructura eDirectory del Novell es el navegador incluyó con la instalación predeterminada.

'Figura 6'

Configuración del WLC

Refiera al cuadro 1 para la topología física de la red de prueba. El WLC usado en esta prueba fue configurado según la práctica estándar con el AP manager y las interfaces de administración en la misma subred y untagged de una perspectiva del VLA N.

Figura 7

1. Autenticación EAP local de la configuración: **Seguridad > local EAP > general**.Los valores por defecto estándar no fueron cambiados.**Figura 8**
2. Cree un nuevo perfil del Local EAP: **Seguridad > local EAP > perfiles**.Para este caso de prueba, el nombre del perfil local EAP elegido era eDirectory. Los métodos de autentificación elegidos eran SALTO, EAP-FAST y PEAP; sin embargo, solamente el PEAP fue probado en este documento.**Figura 9** Cuando usted configura la autenticación EAP local para el PEAP, usted debe tener un certificado instalado en el WLC. En este caso, para comprobar, el certificado instalado en fábrica de Cisco fue utilizado; sin embargo, un certificado del aprovisionado del cliente puede también ser instalado. Los certificados de lado del cliente no se requieren para el uso del PEAP-GTC, sino que pueden ser habilitados para el método interno PEAP si procede.**Figura 10**
3. Establezca la prioridad de la autenticación para el LDAP: **Seguridad > local EAP > prioridad de la autenticación**.**Figura 11**
4. Agregue al servidor LDAP al WLC: **Seguridad** >AAA > **LDAP**.**Figura 12**
5. Configure el WLC para utilizar eDirecotry nuevo (véase el cuadro 13):Elija **autenticado** para

el método bind simple.Ingrese el nombre de usuario del lazo. Ésta es la cuenta que fue creada dentro a eDirectory que será utilizada para que el WLC ate a eDirectory.**Nota:** Aseegurese que usted ingresa los atributos del directorio correcto para el nombre de usuario. Para este caso de prueba, el “cn=Admin, o=ZION” fue utilizado.Ingrese la contraseña del lazo. Ésta es la contraseña para la cuenta de usuario del lazo.Ingrese la Base del usuario DN. Éste es el Domain Name donde se localizan las cuentas de usuario de red inalámbrica. En el caso de prueba, los usuarios fueron situados en la raíz del DN (o=Zion). Si los jerarquizan dentro de otros grupos/organizaciones, encadénelas así como una coma (por ejemplo, “o=ZION, o=WLCUser”).Ingrese el atributo de usuario. Éste es el Common Name (CN) (véase el cuadro 6).Tipo de objeto de usuario – Esto se fija al *usuario*.**Figura 13**

6. Cree la red inalámbrica (WLAN) que usted quisiera que los clientes eDirectory del Novell utilizaran. Para este caso de prueba, el nombre del perfil de la red inalámbrica (WLAN) es *eDirectory* y el SSID es *Novell* (véase el cuadro 14).**Figura 14**
7. Habilite la red inalámbrica (WLAN) y aplique la directiva de radio apropiada e interconecte. Para este caso de prueba, el Novell SSID fue habilitado solamente para la red del 802.11a y atado a la interfaz de administración.**Figura 15**
8. Configure los ajustes de seguridad apropiados de la capa 2. Para este caso de prueba, la Seguridad WPA+WPA2, la directiva WPA2, la encripción AES, y el 802.1x para la administración de claves fueron seleccionados.**Figura 16**
9. Para completar la configuración local de la autenticación EAP, configure la red inalámbrica (WLAN) para la autenticación EAP local usando el servidor LDAP:Elija la **autenticación EAP local habilitada** y aplique el perfil creado EAP (**eDirectory**).Bajo los servidores LDAP, elija la dirección IP del servidor eDirectory configurado (**192.168.3.3**).**‘Figura 17’**

Configuración del Cliente

El PEAP-GTC es los Requisitos de autenticación actuales para la mayoría de las escuelas K-12. El WLC no soporta el MSCHAPv2 para la autenticación EAP local. Como consecuencia, usted debe elegir el GTC para el tipo de la autenticación EAP en el cliente.

Las figuras siguientes son un recorrido de la configuración de la utilidad de escritorio del Cisco Aironet para que el PEAP-GTC conecte con el Novell de la red inalámbrica (WLAN) SSID. Las configuraciones similares se alcanzan con el cliente Microsoft nativo con el soporte PEAP-GTC.

1. Configure el nombre del perfil y el SSID (Novell) del cliente.**Figura 18**
2. Elija **WPA/WPA2/CCKM** para la Seguridad y **PEAP (EAP-GTC)** para el tipo EAP.**Figura 19**
3. Configuración PEAP-GTC:Elija **validan la identidad** y la **contraseña estática del servidor**.Ingrese el nombre de usuario y contraseña para la cuenta o el supplicant indicará para las credenciales en la conexión a la comunicación.No ingrese en el Esquema del directorio del Novell **<ANY>**, como esto no se requiere.**Figura 20**
4. Una vez que se completa el perfil, actívelo y el proceso de autenticación debe comenzar.**Figura 21**

El cuadro 22 representa una asociación y una autenticación acertadas vía el PEAP-GTC.

Figura 22

Depuraciones

Para verificar que usted pueda realizar un LAZO autenticado así como la autenticación de usuario, habilita estas opciones de la traza para eDirectory:

- Autenticación
- LDAP
- NMAS

Figura 23

Tal y como se muestra en del debug, una respuesta acertada de la autenticación ldap se entrega al regulador del Wireless LAN en 192.168.3.253:

```
LDAP   : (192.168.3.253:36802)(0x0020:0x63) DoSearch on connection
    0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
Auth   : Starting SEV calculation for conn 23, entry .sorr.ZION.ZION..
Auth   : 1 GlobalGetSEV.
Auth   : 4 GlobalGetSEV succeeded.
Auth   : SEV calculation complete for conn 23, (0:0 s:ms).
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) DoSearch on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) DoBind on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Bind name:cn=sorr,o=ZION, version:3,
    authentication:simple
Auth   : [0000804d] <.sorr.ZION.ZION.> LocalLoginRequest. Error success, conn:
    22.
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Sending operation result 0:"":"" to
    connection 0x34367d0
Auth   : UpdateLoginAttributesThread page 1 processed 1 login in 0 milliseconds
```

Nota: Algunas de las líneas en la salida de los debugs han sido envuelto debido a los apremios del espacio.

Para asegurarse de que el WLC esté haciendo una petición de la autenticación satisfactoria al servidor eDirectory, publique estos comandos debug en el WLC:

```
debug aaa ldap enable

debug aaa local-auth eap method events enable

debug aaa local-auth db enable
```

Salida de muestra de una autenticación satisfactoria:

```
*Dec 23 16:57:04.267: LOCAL_AUTH: (EAP) Sending password verify request profile
    'sorr' to LDAP
*Dec 23 16:57:04.267: AuthenticationRequest: 0xcdb6d54
*Dec 23 16:57:04.267:   Callback.....................................0x84cab60
*Dec 23 16:57:04.267:   protocolType.................................0x00100002
*Dec 23 16:57:04.267:   proxyState.....................................
    00:40:96:A6:D6:CB-00:00
*Dec 23 16:57:04.267:   Packet contains 3 AVPs (not shown)
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from method
*Dec 23 16:57:04.267: ldapTask [1] received msg 'REQUEST' (2) in state
    'CONNECTED' (3)
*Dec 23 16:57:04.267: disabled LDAP_OPT_REFERRALS
*Dec 23 16:57:04.267: LDAP_CLIENT: UID Search (base=o=ZION,
    pattern=(&(objectclass=user)(cn=sorr)))
*Dec 23 16:57:04.269: LDAP_CLIENT: ldap_search_ext_s returns 0 85
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned 2 msgs including 0 references
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 1 type 0x64
*Dec 23 16:57:04.269: LDAP_CLIENT: Received 1 attributes in search entry msg
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 2 type 0x65
*Dec 23 16:57:04.269: LDAP_CLIENT : No matched DN
*Dec 23 16:57:04.269: LDAP_CLIENT : Check result error 0 rc 1013
*Dec 23 16:57:04.269: LDAP_CLIENT: Received no referrals in search result msg
*Dec 23 16:57:04.269: ldapAuthRequest [1] called lcapi_query base="o=ZION"
    type="user" attr="cn" user="sorr" (rc = 0 - Success)
*Dec 23 16:57:04.269: Attempting user bind with username cn=sorr,o=ZION
*Dec 23 16:57:04.273: LDAP ATTR> dn = cn=sorr,o=ZION (size 14)
*Dec 23 16:57:04.273: Handling LDAP response Success
*Dec 23 16:57:04.274: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.274: LOCAL_AUTH: (EAP:448) Password verify credential callback
    invoked
*Dec 23 16:57:04.274: eap_gtc.c-TX-AUTH-PAK:
*Dec 23 16:57:04.274: eap_core.c:1484: Code:SUCCESS  ID:0x 8  Length:0x0004
    Type:GTC
*Dec 23 16:57:04.274: EAP-EVENT: Received event 'EAP_METHOD_REPLY' on handle
    0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: Handling asynchronous method response for
    context 0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method state: Done
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method decision: Unconditional Success
*Dec 23 16:57:04.274: EAP-EVENT: Sending method directive 'Free Context' on
    handle 0xBB000075
*Dec 23 16:57:04.274: eap_gtc.c-EVENT: Free context
*Dec 23 16:57:04.274: id_manager.c-AUTH-SM: Entry deleted fine id 68000002 -
    id_delete
*Dec 23 16:57:04.274: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xBB000075
*Dec 23 16:57:04.274: peap_inner_method.c-AUTH-EVENT: EAP_SUCCESS from inner
    method GTC
*Dec 23 16:57:04.278: LOCAL_AUTH: EAP: Received an auth request
*Dec 23 16:57:04.278: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.278: LOCAL_AUTH: (EAP:448) Sending the Rxd EAP packet (id 9) to
    EAP subsys
*Dec 23 16:57:04.280: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) ---> [KEY AVAIL] send_len 64,
    recv_len 64
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) received keys waiting for success
*Dec 23 16:57:04.280: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xEE000074
*Dec 23 16:57:04.281: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Received success event
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Processing keys success
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] AAA response 'Success'
```

```
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] Returning AAA response
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb AAA Message 'Success' received for
    mobile 00:40:96:a6:d6:cb
```

Nota: Algunas de las líneas en la salida han sido envuelto debido a los apremios del espacio.

Pues más escuelas K-12 adoptan la arquitectura de WLAN de Cisco, habrá una necesidad cada vez mayor de soportar la autenticación de usuario de red inalámbrica al Novell's eDirectory. Este papel ha verificado que un WLC de Cisco puede autenticar a los usuarios contra la base de datos de LDAP eDirectory del Novell's cuando está configurado para la autenticación EAP local. Una configuración similar se puede también hacer con el Cisco Secure ACS que autentica a los usuarios al Novell's eDirectory. La investigación adicional debe ser hecha para la sola muestra encendido con otros clientes WLAN tales como configuración cero del Cisco Secure Services Client y de Microsoft Windows.

Información Relacionada

- Autenticación EAP local en el regulador del Wireless LAN con el ejemplo de configuración del EAP-FAST y del servidor LDAP
- Ejemplo de configuración del servidor local unificado de la red inalámbrica EAP
- Autenticación del EAP-FAST con el ejemplo de configuración de los reguladores y del servidor RADIUS externo del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems