Ejemplo fuera de banda de la configuración de red inalámbrica del NAC (OOB)

Contenido

Introducción

Este documento proporciona una guía para el diseño para el despliegue de seguridad de punto final para dispositivos Cisco Network Admission Control (NAC) Out of Band (OOB) en una implementación de Cisco Unified Wireless Network. Estas recomendaciones de la mejor práctica asumen que una red del Cisco Unified Wireless se ha desplegado de acuerdo con las guías de consulta proporcionadas en el 3.0 de la guía de diseño de la movilidad de la empresa.

El diseño recomendado es el gateway virtual (modo Bridge) y del despliegue solución central OOB con el RADIUS solo Muestra-en. El regulador del Wireless LAN (WLC) debe ser L2 colocado adyacente al servidor del NAC. El cliente se asocia al WLC, y el WLC autentica al usuario. Una vez que se completa la autenticación, el tráfico de usuarios pasa con el VLA N de la cuarentena del WLC al servidor del NAC. El proceso de la evaluación y de la corrección de la postura ocurre.

Una vez que certifican al usuario, el VLAN de usuario cambia de la cuarentena para acceder el VLA N en el WLC. El tráfico desvía el servidor del NAC cuando está movido para acceder el VLA N.

prerrequisitos

Requisitos

Esta configuración del documento es específica a la versión del NAC 4.5 y del WLC 5.1

Componentes Utilizados

Este documento es t restringido a las versiones de software y hardware específicas.

- Servidor 3350 4.5 del NAC
- Administrador 3350 del NAC 4.5
- WLC 2106 5.1

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Descripción del NAC de Cisco

El NAC de Cisco utiliza la infraestructura de red para aplicar la conformidad de la política de seguridad en todos los dispositivos que busquen a los recursos de computación de la red de acceso. Con el dispositivo NAC de Cisco, los administradores de la red pueden autenticar, autorizan, evalúan, y remediate atado con alambre, Tecnología inalámbrica, y los usuarios remotos y sus máquinas antes del acceso a la red. El dispositivo NAC de Cisco identifica si los dispositivos conectados a la red tales como laptopes, Teléfonos IP, o videoconsolas son obedientes con las políticas de seguridad de la red, y repara cualquier vulnerabilidad antes de que permita el acceso a la red.

La terminología del diseño recomendado se discute:

Modo de gateway virtual (modo Bridge)

Cuando el dispositivo NAC se configura como gateway virtual, actúa como Bridge entre los usuarios finales y el default gateway (router) para la subred cliente se maneja que. Para un VLA N dado del cliente, el dispositivo NAC interliga el tráfico de su interfaz no confiable a su interfaz confiada en. Cuando actúa como Bridge del lado untrusted al lado confiado en de la aplicación, se

utilizan dos VLA N. Por ejemplo, el VLA N 110 del cliente se define entre el regulador del Wireless LAN (WLC) y la interfaz no confiable del dispositivo NAC. No hay interfaz ruteada o el Switched Virtual Interface (SVI) asociado al VLA N 110 en el switch de distribución. El VLAN10 se configura entre la interfaz de confianza del dispositivo NAC y el Next Hop Router interface/SVI para la subred cliente. Una regla de la asignación se hace en el dispositivo NAC que adelante los paquetes que llegan en el VLA N 110 hacia fuera VLAN10 cuando intercambia la información de la etiqueta del VLA N tal y como se muestra en del higo 1-1. El proceso se invierte para los paquetes que vuelven al cliente. Observe que, en este modo, los BPDU no están pasados de los VLA N del untrusted-lado a sus contrapartes de confianza-lado. La opción de la asignación del VLA N se elige generalmente cuando el dispositivo NAC se coloca lógicamente en línea entre los clientes y las redes se protegen que. Esta opción del bridging debe ser utilizada si se va el dispositivo NAC a ser desplegado en el modo de gateway virtual con un despliegue inalámbrico unificado. Porque el servidor del NAC es consciente de los *protocolos de la capa superiores*, por abandono permite explícitamente los protocolos que lo requieren conectar con la red en el papel autenticado, por ejemplo, el DNS y el DHCP.

Cuadro gateway virtual de 1-1 con la asignación del VLA N

Modo fuera de banda

Las implementaciones fuera de banda requieren el tráfico de usuarios atravesar a través del dispositivo NAC solamente dentro de la autenticación, de la evaluación de la postura, y de la corrección. Cuando autentican y pasa a un usuario todos los controles de la directiva, el tráfico se conmuta normalmente a través de la red y desvía el servidor del NAC. Para más información, refiera al capítulo 4 de la instalación y de la guía de administración Dispositivo-limpias del Access Manager del NAC de Cisco.

Cuando el dispositivo NAC se configura de este modo, el WLC es un dispositivo administrado en el administrador del NAC de la misma forma que eso un switch Cisco es manejada por el administrador del NAC. Después de que autentiquen y pase al usuario la evaluación de la postura, el administrador del NAC da instrucciones el WLC para marcar el tráfico de usuarios con etiqueta del VLA N del NAC para acceder el VLA N que ofrece los privilegios de acceso.

Cuadro dispositivo NAC de 1-2 en el modo fuera de banda con el modo de gateway virtual

Inicio de Sesión Único

Escoja muestra-en (SSO) es una opción que no requiere la intervención del usuario y es relativamente directo implementar. Hace uso de la capacidad VPN SSO de la solución del NAC, juntada con el software agente limpio del acceso que se ejecuta en PC del cliente. El VPN SSO utiliza los registros de contabilidad RADIUS para notificar el dispositivo NAC sobre los usuarios de acceso remoto autenticados que conectan con la red. De la misma manera, esta característica se puede utilizar conjuntamente con el controlador de WLAN para informar automáticamente al servidor del NAC sobre los clientes de red inalámbrica autenticados que conectan con la red.

Véase los cuadros 1-3 a 1-6 por ejemplos de un cliente de red inalámbrica que realice la autenticación SSO, la evaluación de la postura, la corrección, y el acceso a la red a través del dispositivo NAC.

Esta secuencia se muestra en el cuadro 1-3:

1. El usuario de red inalámbrica realiza la autenticación 802.1x/EAP a través del controlador de

WLAN a un servidor de AAA por aguas arriba.
2. El cliente obtiene una dirección IP del AAA o de un servidor DHCP.
3. Después de que el cliente reciba una dirección IP, el WLC adelante un expediente de las estadísticas RADIUS (comienzo) al dispositivo NAC, que incluye la dirección IP del cliente de red inalámbrica.**Nota:** El regulador del WLC utiliza un solo registro de contabilidad RADIUS (comienzo) para la autenticación de cliente del 802.1x y la asignación de la dirección IP, mientras que el Switches del Cisco Catalyst envía dos registros de contabilidad: un comienzo de las estadísticas se envía después de la autenticación de cliente del 802.1x, y se envía una actualización interina después de que asignen el cliente una dirección IP.
4. Después de que detecte la conectividad de red, el agente del NAC intenta conectar con el CAM (con el protocolo SWISS). El tráfico es interceptado por el servidor del NAC, que, a su vez, pregunta al administrador del NAC para determinar si el usuario está en la lista de usuario en línea. Solamente los clientes se autentican que están en la lista de usuario en línea, que es el caso en el ejemplo anterior como resultado de la actualización RADIUS en el paso 3.
5. El agente del NAC realiza una evaluación local de la postura de la Seguridad/del riesgo de la máquina del cliente y adelante la evaluación al servidor del NAC para la determinación de la admisión de la red.**Cuadro proceso de autenticación de cliente de 1-3 y evaluación de la postura**

Esta secuencia ocurre en el cuadro 1-4:

1. El dispositivo NAC adelante la evaluación del agente al administrador del dispositivo NAC (CAM).
2. En este ejemplo, el CAM determina que el cliente no está en la conformidad y da instrucciones el dispositivo NAC para poner al usuario en un papel de la cuarentena.
3. El dispositivo NAC entonces envía la información de la corrección al agente del cliente.**Cuadro información de la evaluación de la postura de 1-4 de CAS al CAM**

Esta secuencia ocurre en el cuadro 1-5:

1. El agente del cliente visualiza el tiempo que sigue habiendo lograr la corrección.
2. El agente dirige al usuario paso a paso con el proceso de la corrección; por ejemplo, en la actualización del archivo de definición del contra virus.
3. Después de la realización de la corrección, el agente pone al día el servidor del NAC.
4. El CAM visualiza una declaración del Acceptable Use Policy (AUP) al usuario.**Cuadro proceso de la corrección del cliente de 1-5 con CAS como el dispositivo de imposición**

Esta secuencia ocurre en el cuadro 1-6:

1. Después de que valide el AUP, el dispositivo NAC conmuta al usuario a un papel (autorizado) en línea.
2. Las funciones SSO pueblan la lista de usuario en línea con el dirección IP del cliente. Después de la corrección, una entrada para el host se agrega a la lista certificada. Ambas tablas (así como la tabla descubierta de los clientes) son mantenidas por el CAM (administrador del dispositivo NAC).
3. El administrador del NAC envía un SNMP escribe la notificación al WLC para cambiar el VLAN de usuario de la cuarentena para acceder el VLA N.
4. El tráfico de usuarios comienza a dejar el WLC con la etiqueta del VLA N del acceso. El servidor del NAC está no más en la trayectoria para este tráfico del usuario determinado.**El cuadro 1-6 certificó puente del cliente CAS conmutando encima para acceder el VLA N**

El método más transparente para facilitar la autenticación de usuario de red inalámbrica es habilitar la autenticación VPN-SSO en el servidor del NAC y configurar el WLCs para remitir el RADIUS que considera al servidor del NAC. En caso que los registros de contabilidad necesiten ser remitidos a una conexión en sentido ascendente del servidor de RADIUS en la red, el servidor del NAC se puede configurar para remitir el paquete de las estadísticas al servidor de RADIUS.

Nota: Si la autenticación VPN-SSO se habilita sin el agente limpio del acceso instalado en PC del cliente, todavía autentican al usuario automáticamente. Sin embargo, no están conectados automáticamente a través del dispositivo NAC hasta que abran a su buscador Web y se hace un intento de conexión. En este caso, cuando el usuario abre a su buscador Web, se reorientan momentáneamente (sin un mensaje de conexión a la comunicación) dentro de la fase del “agente-menos”. Cuando el proceso SSO es completo, están conectados con su URL originalmente pedido.

De la configuración del NAC solución de red inalámbrica OOB

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

En el WLC de la implementación del NAC de la corriente integra con el dispositivo NAC de Cisco en el modo de la en-banda solamente, donde el dispositivo NAC tiene que permanecer en el trayecto de datos incluso después certifican al usuario. Una vez que el dispositivo NAC completa su validación de la postura, el empleado/el invitado recibe el acceso de la red basada en su papel.

Con la versión del NAC 4.5 y del WLC 5.1, del NAC de la solución de los soportes la integración inalámbrica OOB con el dispositivo NAC. Cuando el cliente asocia y completa L2Auth, se marca si la interfaz de la cuarentena está asociada al WLAN/SSID. Si sí, el tráfico inicial se envía en la interfaz de la cuarentena. Los flujos de tráfico del cliente en el VLA N de la cuarentena, que es trunked al dispositivo NAC. Una vez que se hace la validación de la postura, el administrador del NAC envía un SNMP el mensaje determinado que pone al día el acceso VLAN ID; el regulador se pone al día con el acceso VLAN ID, y el tráfico de datos comienza a conmutar del regulador directamente a la red sin el servidor del NAC.

Cuadro ejemplo de 2-1 de CAS independiente en el modo Bridge conectado con el WLC a través del Switch

En el cuadro 2-1, el WLC está conectado con un puerto troncal que lleve el VLA N de la cuarentena y el VLA N del acceso (176 y 175). En el Switch, el tráfico VLAN de la cuarentena es trunked al dispositivo NAC, y el tráfico VLAN del acceso es trunked directamente al Switch Layer3. Trafique que alcanza el VLA N de la cuarentena en el dispositivo NAC se asocia para acceder el VLA N basado en la configuración de la correlación estática. Cuando los socios del cliente completan el auth L2, marca si la interfaz de la cuarentena es asociada; si sí, los datos se envían en la interfaz de la cuarentena. Los flujos de tráfico del cliente en el VLA N de la cuarentena, que es trunked al dispositivo NAC. Una vez que se hace la validación de la postura, el servidor del NAC (CAS) envía un SNMP el mensaje determinado que pone al día el acceso VLAN ID al regulador, y el comienzo del tráfico de datos para conmutar del WLC directamente a la red sin el servidor del NAC.

Restricciones

- Ningún perfil del puerto asociado
- Ningún VLAN ID especificado en el administrador del NAC: definido en el WLC
- El soporte del filtro MAC no puede utilizar el VLAN ID de las configuraciones del papel
- Soporte virtual fuera de banda del modo de servidor del NAC del gateway solamente
- Asociación de la capa 2 entre el servidor del WLC y del NAC
- El NAC ISR y el WLC NM no se pueden configurar para hacer el NAC de la Tecnología inalámbrica OOB

Nota: Refiera a la asignación del VLA N en la sección de los modos de gateway virtual del dispositivo NAC de Cisco - la guía de configuración del Access Server limpia, libera 4.8(1) para más información sobre cómo configurar con seguridad los VLA N en los modos de gateway virtual.

Configuración del switch Catalyst

```
interface GigabitEthernet2/21
 description NAC SERVER UNTRUSTED INTERFACE switchport switchport trunk native vlan 998
switchport trunk allowed vlan 176 switchport mode trunk no ip address ! interface
GigabitEthernet2/22 description NAC SERVER TRUSTED INTERFACE switchport switchport trunk native
vlan 999 switchport trunk allowed vlan 11,175 switchport mode trunk no ip address ! interface
GigabitEthernet2/23 description NAC MANAGER INTERFACE switchport switchport access vlan 10 no ip
address spanning-tree portfast ! interface GigabitEthernet2/1 description WLC switchport
switchport trunk allowed vlan 75,175,176 switchport trunk native vlan 75 switchport mode trunk
no ip address ! interface Vlan75 Description WLC Management VLAN ip address 10.10.75.1
255.255.255.0 ! interface Vlan175 Description Client Subnet Access VLAN ip address 10.10.175.1
255.255.255.0 end
```

Pasos para configurar el NAC OOB en el administrador del WLC y del NAC

Siga los siguientes pasos para configurar el NAC OOB en el administrador del WLC y del NAC:

1. Habilite el modo del v2 SNMP en el regulador.
2. Cree un perfil para el WLC en el administrador CAM. Haga clic **OOB el perfil > el dispositivo de la Administración > nuevo**.
3. Una vez que el perfil se crea en el CAM, agregue el WLC en el perfil; vaya **OOB a la Administración > a los dispositivos > nuevo** y ingrese el IP Address de administración del WLC.Ahora el regulador se agrega en el administrador CAM.
4. Agregue el CAM como el receptor de trampa SNMP del WLC. Utilice el nombre exacto del receptor de trampa en el CAM como el receptor SNMP.
5. Configure al receptor de trampa SNMP en el CAM con el mismo nombre, que se especifica en el regulador; haga clic los perfiles bajo **OOB la Administración > el receptor SNMP**.En esta etapa, el WLC y el CAM pueden hablar el uno al otro para las actualizaciones del estado de la validación y del acceso/de la cuarentena de la postura del cliente.
6. En el regulador, cree una interfaz dinámica con el VLA N del acceso y de la cuarentena.
7. Cree la red inalámbrica (WLAN), y asocíela a la interfaz dinámica.
8. Finalmente, NAC del permiso en la red inalámbrica (WLAN).
9. Agregue la subred cliente en el servidor de CAS como la subred manejada; haga clic el **server> CAS seleccionan su server> IP Address inusitado >Advanced > manejado Manage CAS de las subredes del >Add de la subred cliente** y ponen el VLA N de la cuarentena (VLA N untrusted) para la subred manejada.
10. Cree las asignaciones del VLA N en CAS. Elija el **server> de CAS seleccionan su server> de CAS manejan > avanzó > asignación del VLA N**. Agregue el VLA N del acceso como

VLA N confiado en y de la cuarentena como untrusted.

El configurar solo Muestra-en (SSO) con OOB la solución de red inalámbrica

Éstos son los requisitos de habilitar la Tecnología inalámbrica SSO:

1. Autenticación del permiso VPN en el servidor del NAC — el WLC se define como “concentrador VPN” en el dispositivo NAC.
2. Habilite las estadísticas RADIUS en el WLC — el regulador que se define en el dispositivo NAC se debe configurar para enviar los registros de contabilidad RADIUS al dispositivo NAC para cada red inalámbrica (WLAN) 802.1x/EAP que sea una subred manejada en el NAC.

Pasos para configurar el SSO en el administrador del NAC

Siga los siguientes pasos para configurar el SSO en el administrador del NAC:

1. Del menú izquierdo CAM, bajo Administración de dispositivos, elija **CCA el servidor**, y después haga clic el link del **servidor del NAC**.
2. De la página del estado del servidor, elija la lengueta de la **autenticación** y entonces el submenú del **auth VPN**. Véase el cuadro 3-1.**Cuadro 3-1 habilitando el solo Muestra-en el servidor del NAC**
3. Elija los **concentradores VPN que fijan** (cuadro 3-2) para agregar una nueva entrada del WLC. Pueble los campos de entrada para el IP Address de administración y el secreto compartido del WLC que usted quiere utilizar entre el servidor del WLC y del NAC.**El cuadro 3-2 agrega el WLC como cliente RADIUS bajo sección del concentrador VPN**
4. Para la asignación del papel, agregue al nuevo servidor de autenticación con el **sso del vpn del** tipo bajo **User Management (Administración de usuario) > los servidores de autenticación**.
5. Haga clic el icono de la **asignación** y después agregue la **regla de la asignación**. La asignación varía al dependiente sobre el valor del atributo de clase 25 que el WLC envía en el paquete de las estadísticas. Este valor de atributo se configura en el servidor de RADIUS y varía basado sobre la autorización de usuario. En este ejemplo, el valor de atributo es **ALLOWALL**, y se pone en el papel **AllowAll**.

Pasos para configurar el SSO en el regulador del Wireless LAN

Las estadísticas RADIUS necesitan ser configuradas en el WLC para alcanzar solo Muestra-en la capacidad con el servidor del NAC.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Comandos CLI del WLC de CISCO para la verificación

```
(Cisco Controller) >show interface summary

Interface Name    Port Vlan Id    IP Address      Type    Ap Mgr Guest
------------------------------------------------ ---- -------- ------
ap-manager        1    untagged   10.10.75.3      Static  Yes    No
management        1    untagged   10.10.75.2      Static  No     No
nac-vlan          1    175        10.10.175.2     Dynamic No     No
service-port      N/A  N/A        192.168.1.1     Static  No     No
virtual           N/A  N/A        1.1.1.1         Static  No     No


(Cisco Controller) >show interface detailed management

Interface Name..................................... management
MAC Address........................................ 00:18:73:34:b2:60
IP Address......................................... 10.10.75.2
IP Netmask......................................... 255.255.255.0
IP Gateway......................................... 10.10.75.1
VLAN............................................... untagged
Quarantine-vlan.................................... 0
Active Physical Port............................... 1
Primary Physical Port.............................. 1
Backup Physical Port............................... Unconfigured
Primary DHCP Server................................ 10.10.75.1
Secondary DHCP Server.............................. Unconfigured
DHCP Option 82..................................... Disabled
ACL................................................ Unconfigured
AP Manager......................................... No
Guest Interface.................................... No

(Cisco Controller) >show interface detailed nac-vlan

Interface Name..................................... nac-vlan
MAC Address........................................ 00:18:73:34:b2:63
IP Address......................................... 10.10.175.2
IP Netmask......................................... 255.255.255.0
IP Gateway......................................... 10.10.175.1
VLAN............................................... 175 Quarantine-
vlan.................................. 176 Active Physical Port........................... 1
Primary Physical Port.............................. 1 Backup Physical
Port............................... Unconfigured Primary DHCP Server.............................
10.10.175.1 Secondary DHCP Server............................ Unconfigured DHCP Option
82................................. Disabled ACL.........................................
Unconfigured AP Manager..................................... No Guest
Interface................................. No
```

Verificación del estado del cliente del WLC GUI

La corriente está inicialmente en un estado de la cuarentena hasta que el análisis de la postura se haga en el dispositivo NAC.

El estado del NAC del cliente debe ser **acceso** después de que se complete el análisis de la postura.

Verificación de solo Muestra-en el servidor del NAC con el WLC

Bajo el auth VPN, vaya a la subdivisión del **cliente activo** a verificar si el paquete de inicio de contabilidad ha llegado del WLC. Esta entrada aparece con CCA el agente instalado en la máquina del cliente.

Usted necesita abrir a un navegador para completar el solo Muestra-en el proceso sin un agente.

Cuando el usuario abre al navegador, el proceso SSO ocurre, y el usuario aparece en la lista de usuario en línea (OUL). Con el paquete de finalización de contabilidad RADIUS, quitan al usuario de la lista del cliente activo.

Troubleshooting

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

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Información Relacionada

- Remote Authentication Dial-In User Service (RADIUS)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems