Capa 3 del NAC de Cisco OOB con los ACL

Contenido

Introducción

Cisco Network Admission Control (NAC) exige las políticas de seguridad de la red de una organización en todos los dispositivos que buscan el acceso a la red. El NAC de Cisco permite los solamente dispositivos de punto final obedientes y de confianza, tales como PC, los servidores, y los PDA, sobre la red. El acceso es restricto para los dispositivos no obedientes, que limita el daño potencial de las amenazas de seguridad y de los riesgos emergentes. El NAC de Cisco da a organizaciones un método potente, papel-basado a prevenir el acceso no autorizado y mejora la flexibilidad de la red.

La solución del NAC de Cisco proporciona a los beneficios comerciales siguientes:

- **Conformidad de la política de seguridad**: Se asegura de que los puntos finales se ajusten a la política de seguridad; protege la infraestructura y la productividad del empleado; asegura los activos manejados y unmanaged; entornos internos y acceso de invitado de los soportes; adapta las directivas a su Nivel de riesgo.
- **Protege las inversiones existentes**: Es compatible con las aplicaciones de administración de terceros; las Opciones de instrumentación flexibles minimizan la necesidad de las actualizaciones de la infraestructura.
- **Atenúa los riesgos de los virus, de los gusanos, y del acceso no autorizado**: Los controles y reducen las interrupciones en grande de la infraestructura; reduce los gastos de explotación haciendo los movimientos, agrega, y cambia dinámico y automatizado, que habilita una eficacia más alta TIC; integra con otros componentes de la red Auto-Defensiva de Cisco para entregar la protección de Seguridad completa.

Descripción de la solución

Esta sección introduce abreviadamente la capa 3 fuera de banda (OOB) usando los métodos del Access Control List (ACL) para implementar una arquitectura del Cisco Network Admission Control (NAC).

Descripción de la solución

El NAC de Cisco se utiliza en la infraestructura de red para aplicar la conformidad de la política de seguridad en todos los dispositivos que busquen el acceso a los recursos de red. El NAC de Cisco permite que los administradores de la red autentiquen y que autoricen los usuarios y que los evalúen y el remediate sus máquinas asociadas antes de que se concedan el acceso a la red. Hay varios métodos de configuración que usted puede utilizar para lograr esta tarea, pero acoda 3 fuera de banda (OOB) tiene rápidamente convertido de las metodologías más populares del despliegue para el NAC. Esta rotación en el renombre se basa en varias dinámicas, incluyendo una mejor utilización de los Recursos de hardware.

Por el NAC de Cisco que despliega en una metodología de la capa 3 OOB, un solo dispositivo NAC de Cisco (servidor del NAC del administrador o de Cisco del NAC de Cisco) puede escalar para acomodar a más usuarios. También permite que los dispositivos NAC centralmente sean situados bastante que distribuido a través del campus o de la organización. Así, las implementaciones de la capa 3 OOB son mucho más rentables ambos de un punto de vista del capital y del gasto operativo.

Esta guía describe una implementación ACL-basada del NAC de Cisco en un despliegue de la capa 3 OOB.

Arquitectura de la solución

La arquitectura de la solución (véase que el cuadro 1) identifica los componentes de solución y las puntas dominantes de la integración.

Figura 1: Colocación del dispositivo NAC de Cisco en un entorno de campus típico

Las secciones siguientes describen la capa de acceso, la capa de distribución, la capa del núcleo, y las puntas de la integración de los servicios del centro de datos que componen una arquitectura típica del campus.

Capa de acceso

La solución del NAC de la capa 3 de Cisco OOB es aplicable a un diseño para oficinas centrales ruteado del acceso. En el modo de acceso ruteado, acode 3 interfaces virtuales conmutadas (SVI) se configuran en el switch de acceso, y hay un link de la capa 3 entre el acceso y los switches de distribución.

Nota: El término “switch de acceso” y “Edge Switch” se utiliza alternativamente en este documento.

Como se ve en el cuadro 2, el VLA N del acceso de la capa 3 (por ejemplo, VLAN14) se configura en el Edge Switch, acoda 3 que la encaminamiento se soporta del Switch al switch de distribución o al router por aguas arriba, y el administrador del NAC de Cisco maneja los puertos en el switch de acceso.

Figura 2: Switches de acceso con la capa 3 al borde

Capa de distribución

La capa de distribución es responsable de la encaminamiento de la capa 3. A diferencia de una solución de la capa 2, el servidor del NAC de Cisco no necesita ser situado en la capa de distribución. En lugar, se coloca centralmente en el bloque del servicio del centro de datos.

Capa del núcleo

La capa del núcleo utiliza al Routers basado en IOS de Cisco. La capa del núcleo es reservada para la encaminamiento de alta velocidad, sin ningunos servicios. Los servicios pueden ser puestos en un Switch del servicio en el centro de datos.

El centro de datos mantiene la capa

El centro de datos mantiene el Routers basado en IOS y el Switches de Cisco de las aplicaciones de la capa. El servidor del NAC de Cisco del NAC del administrador y de Cisco centralmente está situado en el bloque del servicio del centro de datos.

Componentes de solución

Esta sección describe los componentes de la solución del dispositivo NAC de Cisco.

Administrador del NAC de Cisco

El administrador del NAC de Cisco es el servidor de la administración y la base de datos que centraliza la configuración y la supervisión de todos los servidores, usuarios, y directivas del NAC de Cisco en un despliegue del dispositivo NAC de Cisco. Para OOB un despliegue del NAC, el administrador proporciona OOB la Administración para agregar y el Switches de control en el dominio del administrador y para configurar los puertos del switch.

Servidor del NAC de Cisco

El servidor del NAC de Cisco es la punta de la aplicación entre la red (manejada) untrusted y la red (interna) confiada en. El servidor aplica limpia definido en el administrador del NAC de Cisco, y los puntos finales comunican con el servidor durante la autenticación. En este diseño, el servidor no se coloca lógicamente o físicamente “en línea” para separar el untrusted y la red de confianza. Este concepto se dirige más detalladamente más adelante en la sección “(OOB) del modo fuera de banda”.

Agente del NAC de Cisco

El agente del NAC de Cisco es un componente opcional de la solución del NAC de Cisco. Cuando el agente se habilita para su despliegue del NAC de Cisco, el agente se asegura de que los ordenadores que acceden su reunión de la red los requisitos de la postura del sistema usted especifiquen. El agente del NAC de Cisco es un solo lectura, fácil de usar, el programa de la pequeño-huella que reside en las máquinas del usuario. Cuando un usuario intenta acceder la red, el agente marca el sistema del cliente para el software que usted requiere, y los usuarios de las ayudas adquieren cualesquiera actualizaciones o software que falta.

(OOB) modo fuera de banda

En de Cisco del dispositivo NAC el despliegue OOB, el servidor del NAC de Cisco comunica con el host extremo solamente durante el proceso de autenticación, posture la evaluación, y la corrección. Después de que se certifique, el host extremo no comunica con el servidor. En OOB el modo, el administrador del NAC de Cisco utiliza el Simple Network Management Protocol (SNMP) al Switches de control y a las asignaciones VLAN del conjunto para los puertos. Cuando configuran al Cisco NAC Manager and Server para OOB, el administrador puede controlar los puertos del switch de Switches soportado. Para una lista de Switches soportado, vaya a:

http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017.

La demostración próxima de los diagramas cómo el administrador del NAC de Cisco utiliza OOB para controlar cómo un usuario consigue el acceso a la red. La secuencia es como sigue:

1. Un PC está conectado físicamente con un Switch en la red (véase el cuadro 3).
2. El Switch envía la dirección MAC usando el SNMP al administrador del NAC de Cisco (véase el cuadro 3).
3. El administrador del NAC de Cisco verifica independientemente de si el PC “esté certificado.”Si el PC no se certifica, el administrador del NAC de Cisco da instrucciones el Switch para asignar el puerto del switch PC a un VLA N de la autenticación (véase el cuadro

4). Continúe con el paso 4 al paso 6.Si se certifica el PC, vaya al paso 5.
4. El PC comunica con el servidor del NAC de Cisco y pasa con la autenticación, la evaluación de la postura, y la corrección (véase el cuadro 4).
5. El servidor del NAC de Cisco informa al administrador del NAC de Cisco que el PC “está certificado” (véase el cuadro 5).
6. El PC está conectado con la red como dispositivo confiable.

Figura 3: OOB comunicación SNMP (1 de 3) Figura 4: OOB comunicación SNMP (2 de 3) Figura 5: OOB comunicación SNMP (3 de 3)

Aspectos del diseño

Cuando usted considera un despliegue del NAC de la capa 3 OOB, usted debe revisar varios aspectos del diseño. Estas consideraciones son mencionadas discutidas en las subdivisiones siguientes, y una explicación abreviada de su importancia es incluida.

Clasificación de la punto final

Varios factores contribuyen a la clasificación del punto final, incluyendo los tipos de dispositivo y los rol del usuario. El tipo de dispositivo y el rol del usuario afectan el papel del punto final.

Tipos de dispositivo posibles

- Dispositivos corporativos
- dispositivos NON-corporativos
- Dispositivos NON-PC

Rol del usuario posibles

- Empleado
- Contratista
- Invitados

Inicialmente, todos los puntos finales se asignan al VLA N del unauthenticated. El acceso a los otros papeles se permite después de la identidad y el proceso de la postura es completo.

Papeles del punto final

El papel de cada tipo de punto final debe ser determinado inicialmente. Un despliegue típico del campus incluye varios papeles, tales como empleados, los invitados, y los contratistas, y otros puntos finales, tales como impresoras, untos de acceso de red inalámbrica, y cámaras IP. Los papeles se asocian a los VLA N del Edge Switch.

Nota: La función no autenticada asocia inicialmente a todos los usuarios a un VLA N del unauthenticated para la autenticación por primera vez.

Aislamiento del papel

Es vital aislar los papeles del punto final cuando usted implementa la solución del NAC de Cisco. Seleccione un mecanismo de aplicación apropiado para proporcionar el tráfico y el aislamiento de la trayectoria para todo el tráfico que origina del unauthenticated y de los ordenadores centrales de host no autorizado. En un entorno de la capa 3 OOB, el Edge Switch de la capa 3 (usando los

ACL) actúa como la punta de la aplicación que asegura la segregación entre las redes “limpia” y del “unauthenticated”.

Flujo de tráfico

El proceso del NAC comienza cuando un punto final conecta con un Switch NAC-manejado. El tráfico clasificado como “unauthenticated” es restringido por los ACL aplicados en el VLA N del unauthenticated. El punto final se permite comunicar a la interfaz “untrusted” del servidor del NAC de Cisco para continuar con el proceso de la evaluación y de la corrección de la postura (hay varios métodos para realizar la evaluación y la corrección de la postura que se discuten más adelante en las “directivas de la actualización del cisco.com en el administrador del NAC de Cisco.” sección). Después de la autenticación, el punto final se mueve al VLA N de confianza.

Modo de servidor del NAC de Cisco

Un servidor del NAC de Cisco se puede desplegar en el modo virtual del gateway (Bridge) o el modo (ruteado) del gateway real-IP.

Modo virtual del gateway (Bridge)

El modo virtual del gateway (Bridge) se utiliza típicamente cuando el servidor del NAC de Cisco es la capa 2 adyacente a los puntos finales. En este modo, el servidor actúa como Bridge y no está implicado en la decisión de ruteo del tráfico de la red.

Nota: El modo virtual del gateway (Bridge) es no corresponde para el diseño de la capa 3 OOB ACL.

Modo (ruteado) del gateway Real-IP

El modo (ruteado) del gateway real-IP es aplicable cuando el servidor del NAC de Cisco es saltos múltiples lejos del punto final. Cuando usted utiliza el servidor como gateway real-IP, especifique los IP Addresses de sus dos interfaces: un IP Address para el lado confiado en (prever la Administración del administrador del NAC de Cisco) y un IP Address para el lado untrusted. Los formatos de dos direcciones deben estar en diversas subredes. El IP Address de la interfaz no confiable se utiliza para comunicar con el punto final en la subred untrusted. Un despliegue de la capa 3 OOB usando los ACL requiere el punto final comunicar con la interfaz no confiable para los propósitos de la autenticación y autorización. Porque el modo real-IP utiliza un IP Address válido para la interfaz no confiable, el servidor del NAC de Cisco se debe configurar para funcionar en el modo del gateway real-IP.

Scalability

Un servidor estándar del NAC de Cisco puede manejar a hasta 5000 usuarios finales simultáneos. El diseño de la capa 3 OOB ACL se adapta para un sitio que sirve a no más que 5000 usuarios. Si usted tiene sitios múltiples, usted puede tener servidores adicionales por el sitio. Si usted tiene un solo sitio que necesite servir a más de 5000 usuarios, usted puede utilizar las técnicas externas del Equilibrio de carga (por ejemplo, balanceador de la carga del motor del control de la aplicación (ACE)) para escalar a más de 5000 usuarios para el solo sitio.

Nota: ACE carga la discusión del balanceador está fuera del alcance de este documento.

Host de la detección

El host de la detección es el IP Address del Nombre de dominio totalmente calificado (FQDN) (FQDN) o de la interfaz no confiable usado por el agente del NAC de Cisco para descubrir los saltos múltiples localizados servidor del NAC de Cisco lejos en la red. El agente inicia el proceso de detección enviando los paquetes UDP a la dirección de host conocida de la detección. Los paquetes de detección deben alcanzar la interfaz no confiable del servidor del NAC para recibir una respuesta. En el caso de un despliegue de la capa 3 OOB, el servidor no está en la trayectoria del tráfico de datos en el VLA N de la autenticación. Por lo tanto, la configuración del host de la detección se debe configurar para ser el IP Address de la interfaz no confiable del servidor del NAC de Cisco de modo que el agente pueda enviar los paquetes de detección directamente al servidor.

Experiencia del usuario (con el agente del NAC de Cisco)

Típicamente, los administradores de red corporativa instalan el agente del NAC de Cisco en las máquinas del cliente antes de publicar esas máquinas a los usuarios. El IP Address del host de la detección o el nombre resolvable en el agente del NAC de Cisco acciona los paquetes de detección que se enviarán a la interfaz no confiable del servidor del NAC, que dirige automáticamente la máquina del cliente con el proceso del NAC.

Experiencia del usuario (sin el agente del NAC de Cisco)

Los puntos finales sin un agente del NAC de Cisco (invitados más probable, contratistas, y activos NON-corporativos) pueden no continuar automáticamente con el proceso del NAC. Los métodos manuales y dirigidos existen para ayudar a los puntos finales que no tienen el agente. Para más detalle, vea “punto final la sección a la comunicación del servidor del NAC de Cisco”.

Nota: Para la mejor experiencia del usuario final posible, Certificados del uso que son confiados en por el navegador del usuario final. Usando los Certificados uno mismo-generados en el servidor del NAC de Cisco no se recomienda para un entorno de producción.

Flujos del proceso del NAC de Cisco

Esta sección explica el flujo de proceso básico para una solución del NAC OOB. Los escenarios son ambos descritos con y sin un agente del NAC de Cisco instalado en la máquina del cliente. Esta sección muestra cómo el administrador del NAC de Cisco controla los puertos del switch usando el SNMP como el media del control. Estos flujos del proceso son macroanáliticos en la naturaleza y contienen solamente los pasos funcionales de la decisión. Los flujos del proceso no incluyen cada opción ni caminan que ocurra y no incluyen las decisiones de autorización que se basan en los criterios de evaluación del punto final.

Refiera al diagrama del flujo del proceso mostrado en el cuadro 7 para los pasos circundados mostrados en el cuadro 6.

Figura 6: Flujo del proceso del NAC para la solución fuera de banda del NAC de la capa 3 Figura 7: Diagrama del flujo del proceso

Implementación de solución del NAC de Cisco

En un diseño del NAC de la capa 3 OOB que utilice los ACL, la autenticación de los Guías del servidor del NAC de Cisco funciona, pero el servidor no es la punta de la aplicación de políticas en la red. El Edge Switch actúa como punta de la aplicación durante la autenticación, la cuarentena, y las etapas del acceso. De acuerdo con esta rotación, algunos cambios adicionales se requieren en el Edge Switch.

Aislamiento del papel

Para un despliegue acertado del NAC, el aislamiento de los puntos finales es crítico. Después de que se determine el diseño de la clasificación del punto final, los permisos entre las clases deben ser determinados. Un enfoque recomendado sigue, sobre la base del cuadro 8.

Figura 8: Acercamiento del aislamiento del papel en de Cisco del NAC la solución OOB

Nota: La interfaz del administrador del NAC de Cisco y la interfaz confiada en de Cisco del servidor del NAC se ilustran arriba en diversos VLA N. Sin embargo, estas dos interfaces pueden ser en el mismo VLA N si el servidor se despliega en el modo del gateway real-IP.

El VLA N del unauthenticated requiere el acceso a estos recursos:

- Servicios de la infraestructura tales como DHCP y DNS
- Servidores de autenticación, típicamente el controlador de dominio para el login del Dominio de Windows antes de la validación del NAC
- La interfaz no confiable del servidor del NAC
- Servidores de la corrección (opcionales)

El VLA N del empleado tiene típicamente acceso sin restricciones a todos los recursos, el VLA N del contratista ha limitado típicamente el acceso a un subconjunto de recursos, y el VLA N del invitado tiene típicamente solamente acceso a Internet.

Técnica de la lista de acceso

Una lista de acceso (ACL) se utiliza para especificar el tráfico de la red. Después de que usted especifique el tráfico con un ACL, usted puede hacer una variedad de cosas con el tráfico. Por ejemplo, usted puede permitirlo, negarlo, limitarlo, o utilizarlo para restringir las actualizaciones de ruteo.

En la técnica ACL, un conjunto de los ACL se aplica a cada nueva interfaz VLAN que usted crea basado en sus requisitos. Los comandos CLI dados en las subdivisiones siguientes muestran los comandos required de configurar aislamiento de la trayectoria confiado en y de red no confiable usando el VLA N ACL. Siga el procedimiento abajo para implementar los ACL.

Nota: La adición de VLA N para el aislamiento del papel y de ACL el configurar en esos VLA N se debe realizar en cada Edge Switch. Este trabajo debe ser disposición del despliegue del NAC de la parte de.

1. Antes de implementar el NAC, examine la configuración del VLAN existente.Los comandos CLI mostrados en el texto siguiente muestran cómo el VLA N de los empleados se configura típicamente antes de que se implemente el NAC.!

```
int vlan
200description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
```

2. VLA N adicionales de la configuración.La planificación del NAC del PRE-despliegue requiere configurar los VLA N adicionales y los ACL relevantes aplicados a las interfaces VLAN. Como un ejemplo, el texto siguiente CLI muestra cómo agregar un nuevo VLA N de la capa 3 para cada uno del unauthenticated, de los empleados, de los contratistas, y de los roles de invitado.!

```
int vlan
100description UNAUTHENTICATED_Vlan
ip address 172.16.1.1 255.255.255.0
!
int vlan
200description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int VLAN
210description CONTRACTORS_Vlan
ip address 10.120.1.1 255.255.255.0
!
int vlan
300description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```

3. Implemente las restricciones en el papel del unauthenticated.Los dispositivos del unauthenticated en el papel del unauthenticated requieren típicamente el acceso a los recursos en la red limpia, tal como DNS, DHCP, Active Directory, y servidores de la corrección. También requieren el acceso a la interfaz no confiable del servidor del NAC de Cisco, en la configuración de muestra abajo, el papel del unauthenticated tienen acceso a los recursos en 10.10.10.0/24 redes y la interfaz no confiable de Cisco del servidor del NAC.!

```
! this access-list permits traffic destined to devices on 10.10.10.x
! this should be a consistent ACL that can be applied across all L3
switches
!
ip host NAC_SERVER_UNTRUSTED_INTERFACE <IP_Address>
access-list 100 permit ip any host NAC_SERVER_UNTRUSTED_INTERFACE
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! then apply this access-list to the UNAUTHENTICATED_Vlan
!
int vlan100
description UNAUTHENTICATED_Vlan
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int vlan200
description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int vlan300
description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```

4. Implemente las restricciones en el VLA N de los invitados.Típicamente, el rol de invitado tiene acceso a Internet solamente. Todo el acceso a los recursos innecesarios, tales como todas las redes internas, debe ser negado explícitamente. La única excepción puede ser servidor DNS interno.!

```
! ACL 100 permits traffic destined to devices on 10.10.10.0 / 24
! this should be a consistent ACL that can be applied across all L3
```

```
switches
!
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! ACL 101 for Guests should deny access to all internal networks
! while DNS is permitted
!
access-list 101 permit udp any host GUEST_DNS_SERVER eq 53
access-list 101 deny ip any 10.0.0.0 255.0.0.0
access-list 101 deny ip any 192.168.0.0 255.255.0.0
access-list 101 deny ip any 172.16.0.0 255.240.0.0
access-list 101 permit ip any any
!
int VLAN100
description UNAUTHENTICATED_VLAN
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int VLAN200
description EMPLOYEES_VLAN
ip address 10.100.1.1 255.255.255.0
!
!
int VLAN300
description GUESTS_VLAN
ip address 192.168.1.1 255.255.255.0
ip access-group 101 in
!
```

Punto final a la comunicación del servidor del NAC de Cisco

El servidor del NAC de Cisco consigue la información MAC del agente del NAC de Cisco o de una página de registro de la red habilitada para ActiveX o la Java Applet para determinar el MAC Address del dispositivo y para señalarlo de nuevo al administrador del NAC de Cisco.

Agente del NAC de Cisco

El agente del NAC de Cisco necesita comunicar con la interfaz no confiable del servidor del NAC para iniciar el proceso de ingreso. Los intentos del agente para descubrir el servidor basado en el valor sabido del host de la detección. Tal y como se muestra en del cuadro 9, el valor del host de la detección en el Agente Cisco (nacs.nac.local) señala a la interfaz no confiable (172.23.117.57) en el servidor del NAC. El cuadro 9 muestra una combinación de tres pantallas.

Vea el “login del agente.” sección para más detalles en la apertura de sesión a través del agente del NAC de Cisco.

Figura 9: Host de la detección que señala a la interfaz no confiable del servidor del NAC

Nota: El agente del NAC de Cisco no aparece si el agente no puede recibir ninguna parte posterior de la respuesta del servidor del NAC de Cisco.

Login de la red

El login de la red se requiere típicamente para las sesiones de conexión al sistema del invitado. Cuando se utiliza la técnica del aislamiento ACL, la interfaz no confiable del servidor del NAC no está directamente en la trayectoria del tráfico de datos. Por lo tanto, no reorientan al usuario

automáticamente a la página de registro cuando abren al navegador primero. Dos opciones pueden permitir al host extremo para conseguir la página de registro.

Opción 1

- Cree un login URL del invitado sabido a los usuarios (por ejemplo, guest.cisco.com).
- El invitado debe después abrir un hojeador y ingresar ese URL, que causa una reorientación a la página de registro.

Opción 2

- Cree a un servidor DNS simulado para el Subred de usuario del unauthenticated.
- Este servidor DNS simulado resuelve cada URL a la interfaz no confiable del servidor del NAC de Cisco.
- Cuando el invitado abre a un navegador, sin importar cuyo URL él está intentando alcanzar, lo reorientan a la página de registro.
- Cuando entonces mueven al usuario al VLA N apropiado para su papel, él consigue una nueva asignación de dirección de DNS al realizar la versión IP o renueva en una registración satisfactoria.

En un diseño de la capa 3 OOB, usuarios que inician sesión usando una descarga de la página web y ejecutan un control ActiveX (para los buscadores Internet Explorer) o los subprogramas java (para los navegadores NON-IE). El control ActiveX (o las Javas) debe ejecutarse para realizar el siguiente:

- Recoja la dirección MAC del host, que está señalado al servidor del NAC de Cisco y al administrador del NAC de Cisco para proporcionar la asignación de la dirección IP y de la dirección MAC.
- Realice la versión IP y renueve del cliente del punto final.

Nota: La decisión para permitir que los invitados utilicen interno o el externo DNS es una decisión de políticas que cada organización debe tomar. Usando un DNS público-basado mantenga las actitudes el menos riesgo potencial en este acercamiento.

Vea el login de la red, para más detalles en la apertura de sesión a través de una página web.

Ejemplo de la configuración ACL de la capa 3 del NAC OOB

Para desplegar con éxito una solución del NAC OOB, los componentes del NAC necesitan ser configurados para hacer juego la arquitectura deseada. El cuadro 10 muestra un diagrama de red lógica del NAC de la capa 3 OOB que se utilice en esta sección para ilustrar la configuración pertinente servidor del NAC del administrador, de Cisco del NAC de Cisco, y un Edge Switch para el despliegue de la capa 3 del NAC OOB usando los ACL.

Figura 10: Diagrama de la topología lógica de la capa 3 del NAC OOB

Para configurar un despliegue del NAC REAL-IP de la capa 3 OOB, siga los siguientes pasos:

1. Configure el Edge Switch para la aplicación.Primero, cree tres VLA N adicionales (UNAUTHENTICATED, CONTRATISTAS, e INVITADOS) en el Edge Switch. El VLA N existente de la producción será utilizado para los empleados.Configure y aplique los ACL en cada VLA N para restringir el acceso a la red basada en la función asignada.Función no autenticada: Nombre del VLA N 17 y ACL: UNAUTH_ACL`! Create SVI for Un-auth VLAN`

```
Edge Switch(config)#interface vlan 17
Edge Switch (config)#ip address 192.168.7.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10
! 192.168.3.10 is the dhcp server (see Figure 10)

! Configure ACL for Un-auth Role
Edge Switch(conf)#ip access-list extended UNAUTH_ACL
   remark Allow Discovery packets from Agent to NAC Server
   permit udp any host 192.168.8.10 eq 8906
   remark Allow Discovery packets from Agent to NAC Server for ADSSO
   permit udp any host 192.168.8.10 eq 8910
   remark Allow Web traffic from PC to NAC Server
   permit tcp any host 192.168.8.10 eq www
   remark Allow SSL traffic from PC to NAC Server
   permit tcp any host 192.168.8.10 eq 443
   remark Allow DHCP permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark Allow Web traffic to the Remediation Server
   permit tcp any host 192.168.3.10 eq www

! Apply ACL for Un-auth VLAN Interface

Edge Switch(config)#interface vlan 17
Edge Switch(config)# ip access-group UNAUTH_ACL in
```

Papel del contratista: Nombre del VLA N 77 y ACL: CONTRACTOR_ACL

```
! Create SVI for Contractor VLAN

Edge Switch(config)#interface vlan 77
Edge Switch (config)#ip address 192.168.77.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL for Contractor Role

Edge Switch(conf)#ip access-list extended CONTRACTOR_ACL
   remark Allow DHCP permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark Allow traffic to DMZ Subnet
   permit ip any 192.168.3.0 0.0.0.255
   remark deny rest of the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for Contractor VLAN Interface

Edge Switch(config)#interface vlan 77
Edge Switch(config)# ip access-group CONTRACTOR_ACL in
```

Rol de invitado: Nombre del VLA N 78 y ACL: GUEST_ACL

```
! Create SVI for GUEST VLAN

Edge Switch(config)#interface vlan 78
Edge Switch (config)#ip address 192.168.78.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL for Guest Role

Edge Switch(conf)#ip access-list extended GUEST_ACL
```

```
   remark Allow DHCP
   permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark deny access to the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for GUEST VLAN Interface

Edge Switch(config)#interface vlan 78
Edge Switch(config)# ip access-group GUEST_ACL in
```

Papel del empleado: VLAN14 y ACL: Production_ACLEl VLA N existente de la producción se puede utilizar para mover al empleado desde el VLA N del unauthenticated al VLA N del empleado. Después de que muevan al cliente del extremo a este VLA N, el agente del NAC de Cisco todavía intenta descubrir el servidor del NAC de Cisco. Diseñan al agente para comportarse esta manera. Si el agente puede alcanzar el servidor, el agente surge e intenta realizar el proceso de ingreso otra vez, aunque la máquina ha concedido ya el acceso. Obviamente, esto es un comportamiento indeseado y los administradores deben asegurarse de que los paquetes de detección UDP 8906 que originan del agente estén caídos. Employee_ACL se configura para caer estos paquetes de detección.

```
! Use Existing Production Layer 3 VLAN for Employees

Edge Switch(config)#interface vlan 14
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL to prevent discovery packets from reaching the
untrusted interface on the NAC Server

Edge Switch(conf)#ip access-list extended Employee_ACL
   remark Deny Discovery packets from Agent to NAC Server
   deny udp any host 192.168.8.10 eq 8906
   permit ip any any

! Apply ACL for Employee VLAN Interface

Edge Switch(config)#interface vlan 14
Edge Switch(config)# ip access-group Employee_ACL in
```

2. Realice la configuración inicial del Cisco NAC Manager and Server.La instalación del Cisco NAC Manager and Server se realiza con el acceso a la consola. El instalar utilitario le dirige con la configuración inicial para el administrador y el servidor. Para realizar la configuración inicial, vaya a:http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html
3. Aplique la licencia al administrador del NAC de Cisco.Después de que usted realice la configuración inicial a través de la consola, acceda al administrador GUI del NAC de Cisco para continuar configurando al Cisco NAC Manager and Server. Primero cargue el administrador y las licencias del servidor que vinieron con los dispositivos. Para más detalle en cargar las licencias, vaya a:http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html#wp1113597**Nota:** Todas las licencias del Cisco NAC Manager and Server se basan en la dirección MAC del eth0 del administrador. En una configuración de la

Conmutación por falla, las licencias se basan en la dirección MAC del eth0 de los administradores primarios y secundarios del NAC de Cisco.

4. Ponga al día las directivas del cisco.com en el administrador del NAC de Cisco.El administrador del NAC de Cisco debe ser configurado para extraer las actualizaciones periódicas del servidor de actualización central situado en Cisco. La lista soportada dispositivo NAC del producto de Cisco AV/AS es un archivo XML versioned distribuido de un servidor de actualización centralizado que proporcione la matriz más actual de los vendedores soportados del antivirus y del antispyware y las versiones del producto usadas para configurar las reglas del antivirus o del antispyware y los requisitos de la actualización de la definición del antivirus o del antispyware para la evaluación y la corrección de la postura. Esta lista se pone al día regularmente para el antivirus y los Productos y las versiones del antispyware soportados en cada agente del NAC de Cisco liberan e incluyen los productos nuevos para las nuevas versiones agente. Observe que la lista proporciona la información de la versión solamente. Cuando el administrador del NAC de Cisco descarga la lista soportada del producto del antivirus y del antispyware, está descargando la información sobre cuáles son las últimas versiones para los Productos del antivirus y del antispyware; no está descargando los archivos de parche o los archivos de definición de virus reales. De acuerdo con esta información, el agente puede entonces accionar la aplicación nativa del antivirus o del antispyware para realizar las actualizaciones. Para más información sobre cómo se extraen las actualizaciones, vaya a:http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html#wp1351880
5. Instale los Certificados de un Certificate Authority (CA) de tercera persona.Durante la instalación, el script de la utilidad de configuración para servidor del NAC de Cisco del NAC del administrador y de Cisco le requiere generar un certificado temporal SSL. Para el ambiente de laboratorio, usted puede continuar utilizando los certificados autofirmados; sin embargo, no se recomiendan para una red de producción.Para más información sobre instalar los Certificados en el administrador del NAC de Cisco de CA de tercera persona, vaya a:http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_admin.html#wp1078189Para más información sobre instalar los Certificados en el servidor del NAC de Cisco de CA de tercera persona, vaya a:http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_admin.html#wp1040111**Nota:** Si usted está utilizando los Certificados de la uno mismo-muestra en el servidor del NAC del ambiente de laboratorio, del administrador y de Cisco del NAC de Cisco cada necesidad de confiar en el certificado del otro, bajo las cuales le requiere cargar los Certificados para ambos como Certificate Authority de confianza SSL > las autoridades del certificado confiable.
6. Agregue el servidor del NAC de Cisco al administrador del NAC de Cisco.Para agregar el servidor del NAC al administrador del NAC, siga los siguientes pasos:Haga clic **CCA los servidores** bajo el cristal de la Administración de dispositivos (véase el cuadro 11).Haga clic la **nueva** lengueta del **servidor**.Utilice el cuadro del *dirección IP del servidor* para agregar la dirección IP de la interfaz confiada en del servidor del NAC.En el rectángulo de la *ubicación del servidor*, ingrese **OOB el servidor del NAC** como la ubicación del servidor.Elija el Real-IP-**gateway fuera de banda de la** lista desplegable del *tipo de servidor*.El tecleo **agrega el servidor de acceso limpio**.**Cuadro 11: Agregar el servidor del NAC de Cisco al administrador del NAC de Cisco** Después de que usted agregue el servidor del NAC de Cisco, aparece en la lista conforme a la lista de lengueta de los servidores (véase el cuadro 12).**Nota:** El

servidor del NAC de Cisco del NAC del administrador y de Cisco tiene que confiar en el Certificate Authority (CA) de cada uno para que el administrador agregue con éxito el servidor.

7. Configure el servidor del NAC de Cisco.Tal y como se muestra en del cuadro 12, haga clic la **lista de** lengueta de los **servidores**.Haga clic el icono del **manejo** (circundado) para que el servidor del NAC de Cisco continúe la configuración.**Cuadro 12: Servidor del NAC de Cisco manejado por el administrador del NAC de Cisco** Después de que usted haga clic el icono del manejo, la pantalla mostrada en el cuadro 13 aparece.
8. Soporte de la capa 3 del permiso.Haga clic la lengueta de la **red** (cuadro 13).Marque el checkbox del **soporte del permiso L3**.Marque el **modo estricto del permiso L3 para bloquear los dispositivos NAT con el** checkbox **limpio del agente del acceso**.Haga clic en **Update** (Actualizar).Reinicie el servidor del NAC de Cisco según lo dado instrucciones.**Cuadro 13: Detalles de la red de servidores del NAC de Cisco Nota:** Genere siempre el certificado para el servidor del NAC de Cisco con el IP Address de su interfaz no confiable. Para el certificado nombre-basado, el nombre debe resolver al IP Address de la interfaz no confiable. Cuando el punto final comunica con la interfaz no confiable del servidor para comenzar el proceso del NAC, el servidor reorientará al usuario al nombre de host del certificado o al IP. Si no funcionan las puntas del certificado a la interfaz de confianza, el proceso de ingreso correctamente.En el cuadro 13 antedicho, usted ve que los dos default gatewayes están presentes. Solamente el default gateway configurado en la interfaz de confianza es aplicable. El valor en la interfaz no confiable no se utiliza para remitir el tráfico. El tráfico que se remite de la interfaz no confiable es dependiente en la Static ruta cubierta en el siguiente paso.
9. Static rutas de la configuración.Después de que las reinicializaciones del servidor del NAC de Cisco, vuelvan al servidor y continúen con la configuración.El servidor debe utilizar la interfaz no confiable para comunicar con los puntos finales en el VLA N del unauthenticated.Van a **avanzado > las Static rutas** (véase el cuadro 14) para agregar las rutas al VLA N del unauthenticated.Complete las subredes apropiadas para los VLA N del unauthenticated.El tecleo **agrega la ruta**.Seleccione la **interfaz no confiable [eth1]** para estas rutas.**Figura 14: Agregar la Static ruta para alcanzar el Subred de usuario del unauthenticated**
10. Perfiles de la configuración para el Switches en el administrador del NAC de Cisco.Seleccione **OOB la Administración > los perfiles > el dispositivo > editan** (véase el cuadro 15).Complete la información de perfil del dispositivo, usando el ejemplo como guía.Cada Switch será asociado a un perfil. Agregue un perfil para cada tipo de Edge Switch que el administrador del NAC de Cisco manejará. El administrador soporta el SNMPv1, el SNMPv2C, y el SNMPv3. Este ejemplo cubre el SNMPv1 solamente. Usted puede querer configurar SNMPv2 o SNMPv3c para una comunicación más segura SNMP entre el administrador y el Switch.**Figura 15: Perfil SNMP usado para manejar el Switch**Configure la configuración del switch para el SNMP.El Edge Switch se debe configurar para las mismas cadenas de comunidad de lectura/grabación SNMP que ésos configurados en el administrador del NAC de Cisco. Vea los comandos CLI abajo.`3560-remote(config)#snmp-server community cisco123 RO`
`3560-remote(config)#snmp-server community cisco321 RW`Seleccione **OOB la Administración > los perfiles > el puerto > nuevo** (véase el cuadro 16).Para el control del puerto individual, configure un perfil del puerto bajo **OOB la Administración > los perfiles > el puerto** que incluye el VLA N predeterminado del unauthenticated y el VLA N del acceso del valor por defecto. En la sección del VLA N del acceso, especifique el rol del usuario del VLA N

usando el **VLA N del acceso** dropdown. El administrador del NAC de Cisco cambia el VLA N del unauthenticated al VLA N del acceso basado en el VLA N definido en el papel donde pertenece el usuario.Defina el perfil del puerto para controlar el VLA N del puerto basado sobre los rol del usuario y los VLA N implementados.El VLA N del auth es el VLA N del UNAUTHENTICATED (VLA N 17) al cual los dispositivos del unauthenticated se asignan inicialmente.El VLA N predeterminado del acceso es el VLA N de los EMPLEADOS (VLAN14). Se utiliza este VLA N si el usuario autenticado no hace un VLA N papel-basado definir.El VLA N del acceso puede reemplazar el VLAN predeterminado a un rol del usuario del VLA N, que se define bajo rol del usuario (para más información sobre configurar los rol del usuario, vea los “rol del usuario de la configuración.” sección). Las sincronizaciones LDAP se pueden utilizar para asociar los rol del usuario en el NAC a los grupos LDAP. Para más información, vaya a:http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080846d7a.shtml**Figura 16: Perfil del puerto para manejar el puerto del switch Nota:** Usted puede también definir los nombres del VLA N en vez de los ID. Si usted define los nombres del VLA N, usted puede tener diversas identificaciones de VLAN en diverso Switches a través del campus, pero el mismo nombre del VLA N asociado a un rol específico.Las opciones adcionales están disponibles bajo perfil del puerto para la versión IP y renuevan las opciones. Navegue hacia abajo la página mostrada en el cuadro 16 para ver estas opciones.Si el usuario está detrás de un teléfono del IP, desmarque la despedida el puerto después de que el VLA N sea el checkbox cambiado (véase el cuadro 17), que, si estuvo marcado, pudo reiniciar el teléfono del IP cuando se despide el puerto.**Figura 17: Perfil inferior disponible del puerto de las diversas opciones**

11. Configuraciones del receptor de la configuración SNMP.Además de configurar la cadena de comunidad SNMP para leído o escriba, usted debe también configurar al administrador del NAC de Cisco para recibir el SNMP traps del Switch. Se envían estos desvíos cuando el usuario conecta y las desconexiones del puerto. Cuando el servidor del NAC de Cisco envía la información de la dirección IP MAC/de un punto final específico al administrador, el administrador construye una tabla de correspondencia internamente para el MAC/IP y el puerto del switch.**Nota:** Usted debe configurar todo el Switches para enviar los desvíos o informa al NAC de Cisco al administrador que usa las cadenas de comunidad definidas en el cuadro 18.Seleccione **OOB la Administración > los perfiles > el receptor SNMP** (véase el cuadro 18).Configure las configuraciones del SNMP trap usando la pantalla en el cuadro 18 como guía.**Figura 18: La configuración del receptor del administrador SNMP del NAC para recoger el SNMP traps e informa**Para configurar las configuraciones del switch para el SNMP traps, aumente el temporizador limpio del rubor del Access Manager del switch predeterminado (CAM) a 1 hora (3600 en el cuadro CLI abajo) por las recomendaciones de la mejor práctica de Cisco para el NAC OOB. La muestra CLI muestra el parámetro configurado del tiempo de envejecimiento del mac-address-table a 3600.La determinación del temporizador a 1 hora reduce la frecuencia de las notificaciones MAC enviadas ya de los dispositivos conectados al administrador del NAC de Cisco. Utilice el comando trap de la fuente de especificar a la dirección de origen que se utiliza para enviar los desvíos.`snmp-server enable traps mac-notification`
`snmp-server host 192.168.2.33 informs NacTraps`
`snmp-server trap-source Vlan 2`
`mac-address-table aging-time 3600`Opcionalmente, conexión de la configuración y trampas de interrupción de link para enviar al NAC de Cisco al administrador (no mostrado en la muestra CLI). Estos desvíos se utilizan solamente en un escenario de instrumentación

donde los host extremos no están conectados detrás de un teléfono del IP.**Nota:** Se recomienda el SNMP informa porque son más confiables que el SNMP traps. También, considere QoS para el SNMP en un entorno de red del mucho tráfico.

12. Agregue el Switches como dispositivos en el administrador del NAC de Cisco.Seleccione **OOB la Administración > los dispositivos > los dispositivos > nuevo** (véase el cuadro 19).El perfil del Switch creado en el paso 10 será utilizado para agregar el Switch.Bajo perfil del dispositivo, utilice el perfil que usted creó, pero no cambie el valor del perfil del puerto predeterminado cuando usted agrega el Switch.**Nota:** Para el perfil del puerto predeterminado, seleccione siempre “incontrolado,” porque usted nunca maneja todos los puertos del switch de acceso. Un mínimo de un puerto de link ascendente debe ser incontrolado. Por lo tanto, usted debe agregar el Switch con un perfil incontrolado del puerto y después seleccionar los puertos que necesite ser manejado.**Figura 19: Agregar un Edge Switch en el administrador del NAC de Cisco para controlar usando el SNMP**Después de que el Switch se agregue al administrador del NAC de Cisco, seleccione los puertos que usted quiere manejar.
13. Configure los puertos del switch para que los dispositivos sean manejados por el NAC.Seleccione **OOB el Switch de la Administración > de dispositivos [IP address] > vira hacia el lado de babor > lista** para ver los puertos del switch disponibles que usted puede manejar (véase el cuadro 20).**Figura 20: Selección del control del puerto disponible para un Switch manejado**Seleccione **OOB el Switch de la Administración > de dispositivos [IP address] > los puertos > manejan** manejar varios puertos inmediatamente (véase el cuadro 21).**Cuadro 21: Los manejos de los puertos múltiples con se unen a la opción**
14. Rol del usuario de la configuración.En este ejemplo, se crean tres papeles adicionales. Los VLA N creados ya en el borde que cada uno corresponde a un papel.Seleccione **User Management (Administración de usuario) > los rol del usuario > editan el papel** y crean un papel del empleado usando el cuadro 22 como guía.**Cuadro 22: Crear el papel del empleado y el asociar a la producción VLAN14**Seleccione **User Management (Administración de usuario) > los rol del usuario > editan el papel** y crean un papel del contratista usando el cuadro 23 como guía.**Figura 23: Creando el papel y asociarlo del contratista al VLA N limitado 77 del acceso**Seleccione **User Management (Administración de usuario) > los rol del usuario > editan el papel** y crean un rol de invitado usando el cuadro 24 como guía.**Figura 24: Creando el rol de invitado y asociarlo al VLA N de Internet solamente** En el total, usted debe ver seis papeles creados en esta sección (tres papeles predeterminados y tres nuevos papeles), tal y como se muestra en del cuadro 25.**Cuadro 25: Agregar los papeles en el administrador del NAC**
15. Agregue a los usuarios y asígnelos para apropiarse del rol del usuario.En un entorno de campus, usted integrará con un servidor de autenticación externa y asociará al usuario a un rol específico mediante el atributo LDAP. Este ejemplo utiliza un usuario local y a los socios ese usuario local con un papel.
16. Personalice la página del ingreso del usuario al sistema para el login de la red.Una página de registro predeterminada se crea ya en el administrador del NAC de Cisco. Usted puede personalizar opcionalmente la página de registro para cambiar el aspecto del portal web. Para una solución de la capa 3 del NAC OOB, el ActiveX o el componente Java debe ser al final cliente descargado para realizar las tareas siguientes:Traiga la dirección MAC de la máquina del cliente.Realice la versión de la dirección IP y renueve.**La administración > páginas del usuario** selectas (véase el cuadro 26).Edite la página para hacer permiso las opciones mostradas en el cuadro 26.**Cuadro 26: Paginaciones del usuario para el login de la red**

17. Personalice el agente del NAC de Cisco para los rol del usuario.Seleccione la **Administración de dispositivos > acceso limpio > configuración > login generales del agente** (véase el cuadro 27).El administrador del NAC de Cisco puede ser configurado para hacer el agente obligatorio para cualquier rol del usuario. En este ejemplo, el agente es obligatorio para el papel del empleado. El contratista y los roles de invitado deben utilizar el login de la red.Marque el **uso del requerir del** checkbox del **agente**.**Figura 27: Login del agente requerido para el papel del empleado**
18. Distribuya el host de la detección para el agente del NAC de Cisco.La distribución de software agente del NAC de Cisco, la instalación, y la configuración se cubren en el apéndice en el “que configura dispositivo NAC de Cisco para la sección del login del agente y de la evaluación de la postura del cliente”. Este ejemplo configura el host de la detección en el administrador del NAC de Cisco.**Administración de dispositivos** selecta **> acceso limpio > agente > instalación limpios del acceso** (véase el cuadro 28).**Cuadro 28: Host de la detección para el agente del NAC de Cisco** El campo del host de la detección PRE-se puebla tal y como se muestra en del cuadro 28 si el agente del NAC de Cisco se descarga del servidor del NAC de Cisco.
19. Login de la red.Conecte la máquina del cliente usando uno de los puertos de borde controlados por el administrador del NAC de Cisco.La máquina del cliente se coloca en el VLA N del unauthenticated. La máquina debe conseguir una dirección IP de la subred del VLA N del unauthenticated.Abra al navegador para realizar el login.La suposición es que esta máquina del cliente no tiene un agente del NAC de Cisco instalado ya. Si todas las entradas DNS se están reorientando a la interfaz no confiable del servidor del NAC de Cisco, el hojeador se debe reorientar a una página de registro automáticamente. Si no, vaya a un URL específico (por ejemplo, guest.nac.local) a realizar el login (cuadro 29).**Figura 29: Página de registro de la red**
20. Login del agente.El agente del NAC de Cisco se puede distribuir apenas como cualquier aplicación del otro software a los usuarios finales o puede ser forzado usando el servidor del NAC de Cisco.**Nota:** Más información detallada en el Agent Distribution y la instalación está disponible en el *dispositivo NAC de Cisco - guía de configuración limpia del Access Manager*.Cuando se activa el agente, la pantalla mostrada en el cuadro 30 aparece.**Figura 30: Login del agente** Seleccione el servidor de la lista desplegable del **servidor**.Ingrese el **nombre de usuario**.Ingrese la **contraseña**.Haga clic en Login (Conexión).La pantalla en el cuadro 31 aparece, seguido pronto por el cuadro 32.**Cuadro 31: El agente del NAC de Cisco que realiza la versión IP y renueva Figura 32: El agente del NAC de Cisco que indica el acceso a la red completo después del IP restaura**Haga clic en OK.

Verifique la asignación VLAN

El puerto manejado por este ejemplo es 0/7. Después de que usted complete con éxito el proceso de ingreso, el VLA N se cambia del unauthenticated VLAN14 al VLA N 17 del empleado. Usted puede confirmar qué puerto está funcionando con la configuración publicando el siguiente comando:

```
3560-remote#show run interface fast 0/7
Building configuration…

Current configuration : 153 bytes
!
interface FastEthernet0/7
```

```
 switchport access VLAN 14
 switchport mode access
 snmp trap mac-notification change added
 spanning-tree portfast
end
```

Solución de la capa 3 OOB ACL del NAC para la Tecnología inalámbrica

La solución de red inalámbrica existente del NAC OOB se limita actualmente a una solución de la capa 2 OOB con el servidor del NAC de Cisco en el modo de gateway virtual. La limitación de esa solución es que el regulador del Wireless LAN (WLC) debe ser la capa 2 adyacente con el servidor del NAC de Cisco. Para más información sobre el despliegue OOB inalámbrico de la capa 2, vaya a:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml

Nota: Actualmente, Cisco está trabajando en una solución de la capa 3 OOB ACL del NAC para las implementaciones inalámbricas.

Apéndice

Alta disponibilidad

Cada uno los servidores del NAC de Cisco del NAC de los administradores individuales y de Cisco en la solución se puede configurar en el modo de gran disponibilidad, significando que hay dos dispositivos que actúan en una configuración activo-espera.

Administrador del NAC

El administrador del NAC de Cisco puede ser configurado en el modo de gran disponibilidad donde hay dos administradores del NAC que actúan en una configuración activo-espera. La configuración completa en un administrador se salva en una base de datos. El administrador espera sincroniza su base de datos con la base de datos en el administrador activo. Cualquier cambio de configuración realizado al administrador activo se avanza inmediatamente al administrador espera. Los puntos claves siguientes proporcionan un resumen de alto nivel de operación de gran disponibilidad del administrador:

- El modo de gran disponibilidad del administrador del NAC de Cisco es una configuración activa o pasiva del dos-servidor en la cual un administrador espera actúa como respaldo a un administrador activo.
- El administrador activo del NAC de Cisco realiza todas las tareas para el sistema. El administrador espera monitorea al administrador activo y mantiene su base de datos sincronizada con la base de datos del administrador activo.
- Ambos administradores del NAC de Cisco comparten un IP virtual del servicio para la interfaz confiada en eth0. El IP del servicio se debe utilizar para el certificado SSL.
- Los administradores primarios y secundarios del NAC de Cisco intercambian los paquetes de latidos UDP cada 2 segundos. Si expira el temporizador Heartbeat (de latido), la falla de estado ocurre.

- Para asegurar a un administrador activo del NAC de Cisco está siempre disponible, su interfaz de confianza (eth0) debe estar para arriba. La situación se debe evitar donde está activo un administrador pero no es directa accesible su interfaz de confianza. Esta condición ocurre si el administrador espera recibe los paquetes de latidos del administrador activo, pero la interfaz del eth0 del administrador activo falla). El mecanismo de la link-detección permite que el administrador espera sepa cuando la interfaz del eth0 del administrador activo llega a ser inasequible.
- Usted puede elegir “configura automáticamente” la interfaz del eth1 en la administración > CCA página del administrador > de la Conmutación por falla. Sin embargo, usted debe configurar manualmente otras (Eth2 o Eth3) interfaces de gran disponibilidad con una dirección IP y el netmask antes de que usted configure la Alta disponibilidad en el administrador del NAC de Cisco.
- El eth0, el eth1, y las interfaces Eth2/Eth3 se pueden utilizar para los paquetes de latidos y la sincronización de la base de datos. Además, cualquier interfaz serial disponible (COM) se puede también utilizar para los paquetes de latidos. Si usted está utilizando más de uno de estas interfaces, la Conmutación por falla ocurre solamente si todas las interfaces del latido del corazón fallan.

Nota: Los pares de gran disponibilidad del administrador del NAC de Cisco no se pueden separar por un link de la capa 3.

Para más detalles, refiera a la documentación del administrador del NAC de Cisco en:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

Servidor del NAC de Cisco

Para proporcionar la protección contra un solo punto de falla, el servidor del NAC de Cisco se puede configurar en el modo de gran disponibilidad. El modo de gran disponibilidad para el servidor del NAC de Cisco es similar al del administrador del NAC de Cisco y también utiliza una configuración activo-espera. Los servidores del NAC de Cisco todavía comparten a una dirección IP virtual (llamada un IP del servicio), pero no comparten las direcciones MAC virtuales.

Los puntos claves siguientes proporcionan una descripción general de alto nivel de la operación de servidor de gran disponibilidad del NAC de Cisco:

- El modo de gran disponibilidad del servidor del NAC de Cisco es una configuración activo-pasiva del dos-servidor en la cual una máquina servidor espera del NAC de Cisco actúa como respaldo a un servidor activo del NAC de Cisco.
- El servidor activo del NAC de Cisco realiza todas las tareas para el sistema. Porque la mayor parte de la Configuración del servidor se salva en el administrador del NAC de Cisco, cuando ocurre la Conmutación por falla del servidor, el administrador avanza la configuración al servidor nuevo-activo.
- El servidor espera del NAC de Cisco no remite ninguna paquetes entre sus interfaces.
- El servidor espera del NAC de Cisco monitorea la salud del servidor activo a través de una interfaz del latido del corazón (serial y una o más interfaces UDP). Los paquetes de latidos se pueden enviar en la interfaz serial, la interfaz dedicada Eth2, la interfaz dedicada Eth3, o la interfaz Eth0/Eth1 (si no hay interfaz Eth2 o Eth3 disponible).
- Los servidores primarios y secundarios del NAC de Cisco intercambian los paquetes de

latidos UDP cada dos segundos. Si expira el temporizador Heartbeat (de latido), la falla de estado ocurre.
- Además de la Conmutación por falla latido del corazón-basada, el servidor del NAC de Cisco también proporciona la Conmutación por falla link-basada basada en la falla de link del eth0 o del eth1. El servidor envía los paquetes del ping de ICMP a un IP Address externo a través de la interfaz del eth0 y/o del eth1. La Conmutación por falla ocurre solamente si un servidor del NAC de Cisco puede hacer ping a las direcciones externas.

Para más detalles, refiera a la documentación del servidor del NAC de Cisco en:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

Active Directory SingleSignOn (Active Directory SSO)

El Active Directory SSO de Windows es la capacidad para un dispositivo NAC de Cisco automáticamente a los usuarios que ingresa al sistema autenticada ya a un controlador de dominio backend del Kerberos (servidor Active Directory). Esta capacidad elimina la necesidad de registrar en el NAC de Cisco el servidor después de que le registren ya en el dominio. Para más detalles sobre configurar el Active Directory SSO en un dispositivo NAC de Cisco, vaya a:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_adsso.html

Consideraciones del entorno del Dominio de Windows

Con objeto de un despliegue del NAC, los cambios a la directiva del script del login pueden ser requeridos. Los scripts del login de Windows pueden ser clasificados como lanzamiento o apagar y abrir una sesión o terminar una sesión los scripts. Windows funciona con el lanzamiento y apaga los scripts en un “contexto de la máquina.” Funcionar con los scripts funciona solamente si el dispositivo NAC de Cisco abre a los recursos de red apropiados requeridos por el script para el rol específico cuando estos scripts se ejecutan en el inicio PC para arriba o apagan, que es típicamente el papel del unauthenticated. Los scripts del inicio y del cierre de sesión se ejecutan en un “contexto del usuario,” que significa que la secuencia de comandos de inicio ejecuta después de que el usuario haya abierto una sesión con Windows GINA. La secuencia de comandos de inicio puede no poder ejecutar si la autenticación o la evaluación de la postura de la máquina del cliente no completa y el acceso a la red no se concede a tiempo. Estos scripts se pueden también interrumpir por la dirección IP restauran iniciado por el agente del NAC de Cisco después OOB de un evento de inicio de sesión. Para más información con respecto a los cambios necesarios a los scripts del login, vaya a:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a70c18.shtml

Configurar el dispositivo NAC de Cisco para el login del agente y la evaluación de la postura del cliente

El agente de la red del NAC de Cisco del NAC del agente y de Cisco proporciona la evaluación y la corrección locales de la postura para las máquinas del cliente. Los usuarios descargan y instalan el agente de la red del NAC de Cisco del NAC del agente o de Cisco (software de cliente solo lectura), que puede marcar el registro, los procesos, las aplicaciones, y los servicios del host. Para más detalles sobre el agente y la evaluación y la corrección de la postura, vaya a:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems