Capa 3 del NAC de Cisco OOB usando VRF-Lite para el aislamiento de tráfico

Contenido

Introducción

Esta guía describe una implementación de Cisco Network Admission Control (NAC) en una implementación de Out-of-Band (OOB) de Capa 3 basado en reenvío de ruta virtual (VRF)-Lite.

Descripción de la solución

Esta sección da una introducción abreviada para acodar 3 OOB usando los métodos de VRF-Lite para implementar una arquitectura del NAC.

Documento de síntesis

El NAC de Cisco aplica las políticas de seguridad de la red de una organización en todos los dispositivos que busquen 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 NAC de Cisco restringe el acceso de los dispositivos noncompliant, 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 para prevenir el acceso no autorizado y mejorar la flexibilidad de la red.

La solución del NAC de Cisco proporciona a estos beneficios comerciales:

- **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 de los controles de acceso desautorizados** y reduce las interrupciones en grande de la infraestructura; reduce los gastos de explotación haciendo los movimientos, agrega, y cambia dinámico y automatizado, así habilitando 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

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. Usted puede utilizar varios métodos de configuración para lograr esta tarea. Este documento se centra específicamente en la implementación VRF-basada del NAC de Cisco en un despliegue de la capa 3 OOB donde el servidor del NAC de Cisco (servidor de acceso limpio de Cisco) se configura en el modo (ruteado) real del gateway IP.

La capa 3 OOB es una de las metodologías más populares del despliegue para el NAC. Esta rotación en el renombre se basa en varias dinámicas que incluyan 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 puede escalar para acomodar a más usuarios. También permite que los dispositivos NAC de Cisco centralmente sean situados bastante que distribuido a través del campus o de la organización. Por lo tanto, las implementaciones de la capa 3 OOB son más rentables ambos de un punto de vista del capital y del gasto operativo.

Esta guía describe una implementación del NAC de Cisco en un despliegue de la capa 3 OOB que se base en VRF-Lite.

Definición simple del VRF

Una manera de mirar la virtualización del dispositivo VRF es compararla al advenimiento de los VLA N. Los VLA N crearon los switches virtuales fuera de un solo Switch físico. Los VRF amplían esa virtualización más allá del límite de la capa 2, y permiten la creación de los routeres virtuales. Los routeres virtuales preven las redes lleno-virtualizadas de punta a punta.

Otra manera de mirar el diseño VRF es que cada VRF actúa apenas como un VPN o un túnel. El tráfico que se pone en un VRF no puede comunicar fuera del VRF (túnel) hasta que el tráfico pase a través del dispositivo que termina el túnel (el VPN Router del destino).

Nota: Estas definiciones se significan para ayudar a introducir un concepto nuevo. Estas definiciones no son representaciones o definiciones oficiales exactas del VRF.

El cuadro 1 muestra un ejemplo de la virtualización del dispositivo con los VRF. Cada capa coloreada en el diagrama representa un diverso router virtual, o el VRF. La metodología VRF proporciona el avión y los datos del control aislamiento plano de la trayectoria, junto con la

capacidad de tener aviones aislados múltiplo de los datos. Es decir proporciona la posibilidad de un router virtual separado o la red para cada tipo de tráfico que se espere en un entorno que utilice el NAC de Cisco. Los tipos de tráfico típicos son:

- Tráfico de usuarios del unauthenticated
- Tráfico del usuario autenticado
- Tráfico del contratista
- Tráfico del invitado

Cuadro 1 – *Virtualización del dispositivo*

Arquitectura de la solución

Los servidores del NAC de Cisco fueron diseñados inicialmente para ser dispositivos de la en-banda. El uso de los dispositivos NAC de Cisco en una infraestructura de red de Cisco permite que usted tome un dispositivo que fue diseñado para ser en-banda a todo el tráfico de la red, y lo despliega con OOB una metodología.

La arquitectura de la solución (véase que el cuadro 2) identifica los componentes de solución y la punta dominantes de la integración del servidor del NAC de Cisco.

Nota: En este documento, los términos “Edge Switch” y “switch de acceso” se utilizan alternativamente.

Cuadro 2 – *Arquitectura de la solución*

Las siguientes secciones describen el acceso, la distribución, la base, y las capas del centro de datos que componen una arquitectura típica del campus.

Capa de acceso

La solución del NAC de Cisco de la capa 3 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. Como cuadro 3 muestra, el VLA N del acceso de la capa 3 (por ejemplo, VLAN 100) 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.

Cuadro 3 – *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 y de la agregación de los switches de capa de acceso. Mientras que usted puede colocar los servidores del NAC de Cisco en esta capa en un diseño de la capa 2 OOB, usted no los localiza aquí en un diseño de la capa 3 OOB. En lugar, coloque los servidores del NAC de Cisco centralmente en el bloque del servicio del centro de datos, como la arquitectura de la solución muestra (el cuadro 2).

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. Ponga los servicios 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 en la red de oficinas centrales. 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 en este diseño de la capa 3 OOB.

Componentes de solución

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 de Cisco, el administrador del NAC de Cisco proporciona OOB la Administración para agregar y el Switches de control en el dominio del administrador del NAC de Cisco y 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 separa lógicamente el untrusted y las redes de confianza, y sirve como la punta centralizada de la aplicación para todas las Listas de acceso (ACL) y las restricciones de ancho de banda para los dispositivos en la red no confiable. Vea OOB la sección de modo para más información.

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, se asegura de que los ordenadores que acceden su reunión de la red los requisitos de la postura del sistema usted especifiquen. El agente 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 le ayuda a adquirir cualesquiera actualizaciones o software que falta. Vea el paso 6: Ponga al día las directivas del cisco.com en el administrador del NAC de Cisco para más información.

Aspectos del diseño

Cuando usted considera un despliegue del NAC de la capa 3 OOB, revise varios aspectos del diseño. Estas consideraciones se enumeran en estas subdivisiones, junto con una explicación abreviada de su importancia.

OOB modo

En de Cisco del dispositivo NAC el despliegue OOB, el servidor del NAC 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 Switches de control del Simple Network Management Protocol (SNMP) para y 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. El control de los puertos del switch se conoce como el avión del control SNMP. Para una lista de modelos de switches soportados, refiera a la sección *OOB soportada del Switches del* soporte del Switch para el dispositivo NAC de Cisco.

OOB el modo se utiliza sobre todo para las implementaciones atadas con alambre. Cuando el método VRF de la capa 3 OOB se utiliza, todo el tráfico de los VLA N (sucios) untrusted, incluyendo el tráfico del agente, alcanza el servidor centralizado del NAC de Cisco donde ocurre toda la aplicación. La aplicación del tráfico en el servidor es un diferenciador de claves entre el método VRF y el método ACL de la capa 3 OOB.

Nota: El servidor del NAC de Cisco fue dirigido originalmente para ser un dispositivo de la en-banda. Es decir el servidor fue diseñado para hacer todo el tráfico lo atraviese, que permitiría que el servidor fuera el punto de control. Cuando usted utiliza el método VRF de la capa 3 OOB, todo el tráfico de usuarios del unauthenticated atraviesa el servidor exactamente como si fuera un despliegue de la en-banda. Este flujo de tráfico permite un entorno constante, fiable.

Clasificación del punto final

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

Éstos son los tipos de dispositivo posibles:

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

Éstos son los 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, invitados, 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: Un papel adicional se requiere para la autenticación a la cual todos los puntos finales pertenecen inicialmente. Este papel asocia al unauthenticated un VLA N “sucio”.

Aislamiento del papel

Para este tipo de diseño del NAC, el tráfico clasificado como “sucio” debe fluir en el lado “untrusted” del servidor del NAC de Cisco. Tenga este principio presente mientras que usted diseña una implementación del NAC de Cisco. Además, no permita “limpian” y las redes “sucias” para comunicar directamente con uno a.

El cuadro 4 muestra que cuando un diseño de la capa 3 OOB utiliza los VRF, el VRF se asegura de que los restos del tráfico del unauthenticated aislados en su propia red virtual. El servidor del NAC de Cisco actúa como la punta de la aplicación o el regulador que asegura la segregación y la comunicación segura entre “limpia” y las redes “sucias”.

Cuadro 4 – *El servidor del NAC de Cisco conecta con los lados sucios y limpios*

Flujo de tráfico

El proceso del NAC comienza cuando un punto final está conectado con un switchport NAC-manejado. El tráfico clasificado como “sucio” o “unauthenticated” se aísla del resto de las redes mientras que está en el VRF “sucio”. Este tráfico se aísla y se envía a la interfaz no confiable en el servidor del NAC de Cisco. Vea la figura 4.

Nota: El dispositivo NAC de Cisco es olvidadizo a cómo el tráfico se presenta él. Es decir el dispositivo sí mismo no tiene ninguna preferencia si el tráfico llega a través de un túnel del Generic Routing Encapsulation (GRE) o está reorientado con una configuración del Policy-Based Routing, VRF-ruteada, u otros métodos de redireccionamiento.

Modo de servidor del NAC de Cisco

Usted puede desplegar un servidor del NAC de Cisco en uno de estos dos modos:

- Modo virtual del gateway (Bridge)
- Modo (ruteado) real del gateway 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: Este modo es no corresponde para este diseño determinado ACL.

Modo (ruteado) del gateway Real-IP

El modo (ruteado) del gateway real-IP es más aplicable en un diseño donde está saltos el servidor del NAC de Cisco de la capa múltiple 3 lejos del punto final, tal como capa 3 OOB. Cuando usted utiliza el servidor como gateway real-IP, especifique los IP Addresses de sus dos interfaces: uno para el lado confiado en (Administración del servidor) y uno para el lado (sucio) untrusted. Los formatos de dos direcciones deben estar en diversas subredes. El IP de la interfaz no confiable se utiliza para comunicar con el punto final en la subred untrusted. El modo que esta guía utiliza es el gateway real-IP.

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

Típicamente, las entidades corporativas tienen los clientes al final por adelantado desplegados agente del NAC de Cisco. La configuración del host de la detección en el agente acciona los paquetes de detección que se enviarán a la interfaz no confiable del servidor del NAC de Cisco, que continúa automáticamente el punto final con el proceso del NAC.

En una capa 3 OOB con el modelo VRF, el host de la detección se fija típicamente para ser el nombre DNS o la dirección IP del administrador del NAC de Cisco. El administrador existe en la red limpia. Porque todo el tráfico de las redes “sucias” se rutea por abandono a través del servidor del NAC de Cisco, los paquetes de detección atraviesan automáticamente el servidor. El flujo de tráfico descrito aquí es una de las ventajas al método VRF. Este flujo de tráfico prevé una experiencia constante, fiable. Vea los flujos del proceso del NAC de Cisco para más información.

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

La capacidad de actuar sin un agente del NAC de Cisco es otra ventaja del modelo VRF. Todo el tráfico de las redes “sucias” se rutea naturalmente a través del servidor del NAC de Cisco. Esto significa que un usuario en una máquina sin un agente del NAC de Cisco tiene que abrir solamente a un buscador Web y hojear a cualquier sitio web válido. El tráfico del navegador intenta pasar a través del servidor, que a su vez captura a la sesión del buscador y la reorienta a un portal del cautivo. Vea los flujos del proceso del NAC de Cisco para más información.

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

Nota: Genere siempre el certificado para el servidor del NAC de Cisco con el IP Address de su interfaz no confiable.

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 en el cuadro 6 para los pasos circundados que están en el cuadro 5.

Cuadro 5 – *Flujo del proceso del NAC para la solución del NAC de Cisco de la capa 3 OOB*
Cuadro 6 – *Diagrama de bloque del flujo del proceso del NAC de Cisco*

Implementación de solución del NAC de Cisco

Esta sección describe cómo implementar una solución del NAC de Cisco.

Topología

El cuadro 7 muestra la topología usada para la creación de esta guía. La red interna, que consiste en los VLA N 200 y 210, se rutea usando la tabla de Global Routing. La red interna no tiene ningún VRF asociado a ella.

El VRF sucio contiene solamente el VLA N SUCIO y el asociados transitan las redes que son necesarias para crear una sola red virtual para que todo el tráfico sucio fluya al lado sucio del servidor centralizado del NAC de Cisco.

El invitado VRF contiene el VLA N de los INVITADOS y asociado transite las redes que son necesarias para terminar todos los datos con origen del VLA N de los INVITADOS en una sub-interfaz separada en el Firewall. Cada uno de las tres redes virtuales (SUCIAS, los INVITADOS, y GLOBAL) se lleva en la misma Infraestructura física y proporciona el aislamiento completo del tráfico y de la trayectoria.

Cuadro 7 – *Topología usada en esta guía*

Orden de funcionamiento

La orden de funcionamiento para el despliegue de una solución del NAC de Cisco está fácilmente para arriba para el debate. ¿Usted configura la porción del NAC de la solución antes de que se prepare la red? ¿O, usted prepara la red antes de que usted configure los dispositivos del NAC de Cisco?

Con objeto de la organización, esta guía se centra en la configuración de red primero. Esto se asegura de que la red esté lista para el NAC, entonces la configuración de los Productos del NAC de Cisco.

Configuración de red

Esta guía se centra en VRF-Lite de punta a punta para el aislamiento de la trayectoria. Es importante observar que usted puede utilizar los VRF con un túnel GRE para permitir el aislamiento de la trayectoria a través de una distribución y de una capa del núcleo existentes, sin requerir ninguna configuración en esos dispositivos. Para más información sobre cuando y por qué utilizar los túneles GRE comparados a un VRF de punta a punta diseñe, vea que el extender que un VRF entre dos dispositivos secciona. Usted puede también referir a la capa 3 del NAC fuera de la guía de diseño de la banda que utiliza VRF-Lite para el aislamiento de tráfico.

Este documento es guía de diseño completa centrada en el VRF-Lite con el método GRE.

Además, el Tag Switching completo se puede utilizar en lugar de VRF-Lite en caso pertinente. El Tag Switching se considera hacia fuera-de-alcance con el propósito de este documento.

Consideraciones importantes para VRF-Lite

Nota: VRF-Lite es una característica que le permite para soportar dos o más redes virtuales. VRF-Lite también permite los IP Addresses que solapan entre las redes virtuales. Sin embargo, la coincidencia de la dirección IP no se recomienda para una implementación del NAC, porque mientras que la infraestructura sí mismo apoya a las direcciones superpuestas, puede crear las complejidades del troubleshooting y la información incorrecta.

Los detalles dados en los pasos proporcionados en esta sección delinean los pasos necesarios para configurar su red para el aislamiento de la trayectoria usando VRF-Lite. La configuración

requerida para insertar el dispositivo NAC de Cisco en su red como gateway real-IP de la capa 3 OOB también se proporciona.

Las interfaces de entrada de las aplicaciones de VRF-Lite para distinguir las rutas para las diversas redes virtuales y formas separan las tablas de ruteo virtual asociando uno o más las interfaces de la capa 3 con cada VRF. Las interfaces en un VRF pueden ser o comprobación, tal como accesos de Ethernet, o pueden ser o lógico, por ejemplo los subinterfaces, las interfaces del túnel, o las interfaces virtuales del Switch del VLA N (SVI).

Nota: Una interfaz de la capa 3 no puede pertenecer a más de un en un momento VRF.

Observe estas consideraciones de VRF-Lite:

- VRF-Lite está localmente - significativo solamente al Switch donde se define, y a la Pertenencia a VRF es determinado por la interfaz de entrada. No se realiza ninguna manipulación del encabezado de paquete o del payload.
- Un Switch con VRF-Lite es compartido por las redes virtuales múltiples (dominios de seguridad), y todos los dominios de seguridad tienen sus propias tablas de ruteo únicas.
- Todos los dominios de seguridad deben tener sus propios VLA N.
- VRF-Lite no soporta todo el Multiprotocol Label Switching (MPLS) - Las funciones VRF tales como intercambio de la escritura de la etiqueta, la adyacencia del Protocolo de distribución de etiquetas (LDP), o los paquetes etiquetados que están también saben como Tag Switching).
- El recurso del Ternary Content Addressable Memory de la capa 3 (TCAM) se comparte entre todos los VRF. Para asegurarse de que cualquier un VRF tenga suficiente espacio de contenido direccionable de la memoria (CAM), utilice el **comando maximum routes**.
- Un switch de Catalyst que utiliza VRF-Lite puede soportar una red global y hasta 64 VRF. El número total de rutas soportadas es limitado por el tamaño del TCAM.
- Usted puede utilizar la mayoría de los Routing Protocol tales como Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), y Static Routing entre los dispositivos que ejecutan VRF-Lite.
- En la mayoría de los casos, no hay necesidad de ejecutar el BGP con VRF-Lite.
- VRF-Lite no afecta a la tarifa de conmutación de conjunto de bits.
- Usted no puede configurar el Multicast y VRF-Lite en lo mismo interfaz de la capa 3 al mismo tiempo.
- Utilice el submandato de VRF-**lite de la capacidad** bajo el router OSPF cuando usted configura el OSPF como el Routing Protocol entre los dispositivos de red.

Defina un VRF

En este ejemplo de diseño, el aislamiento de la trayectoria se debe proporcionar para el unauthenticated o los usuarios y los invitados sucios. El resto del tráfico se permite para utilizar la red interna. Usted debe definir dos VRF mientras que esta configuración muestra:

Ejemplo de la configuración de VRF

```
!--- This command creates a VRF for the DIRTY virtual
network: ! ip vrf DIRTY ! !--- This command names the
VRF and places you into VRF configuration mode: !
description DIRTY_VRF_FOR_NAC ! !--- Gives the VRF a
```

```
user friendly description field for documentation ! rd
100:3 ! !--- Creates a VRF table by specifying a route
distinguisher. !--- Enter either an AS number and an
arbitrary number (xxx:y) or an IP !--- address and
arbitrary number (A.B.C.D:y). ! !--- This document uses
the Autonomous System number and a unique router-id in
that AS. !--- This example signifies AS 100:Router-ID 3
!
```

Nota: El Route Distinguisher no es una configuración necesaria para VRF-Lite. Sin embargo, se considera una mejor práctica de configurar el Route Distinguisher para el futuro, de modo que trabaje el seamlessly con el Tag Switching.

```
! -- Here we create a VRF for the GUEST Virtual Network: ! ip vrf GUESTSdescription
GUESTS_VRF_FOR_VISITORSrd 600:3 !
```

Asocie un VLA N o interconecte con un VRF

Después de que el VRF se defina en el switch de la capa 3 o el router, usted debe asociar las interfaces que van a participar en la configuración de VRF-Lite con el VRF donde pertenecen. Usted puede asociar la comprobación o las interfaces virtuales con un VRF. Esta sección proporciona los ejemplos de una interfaz física, una interfaz sub, un Switched Virtual Interface, y una interfaz del túnel que todos se asocian a un VRF.

Nota: Los ejemplos son muestras solamente, y no fueron utilizados en la topología de este documento.

Ejemplo de la configuración de interfaz física

```
interface FastEthernet0/1
ip vrf forwarding GUESTS
!--- Associates the interface with the appropriate VRF
defined in Step 1. ip address 192.168.39.1
255.255.255.252
```

Ejemplo de configuración de la Sub-interfaz

```
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
```

Ejemplo de configuración del Switched Virtual Interface

```
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
```

Ejemplo de configuración de la interfaz del túnel

```
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.254.1
```

Amplíe un dispositivo VRF entre dos dispositivos

Hay varias metodologías aceptables que usted puede utilizar para ampliar un VRF entre dos pedazos de infraestructura. Aseegurese que el método que usted elige está basado en estos criterios:

- Considere las capacidades de la plataforma. Todo el soporte actual VRF-Lite de la transferencia y de plataformas de ruteo de la empresa de la capa 3-capable de Cisco. Estas Plataformas incluyen, pero no se limitan a, 4500, 3750, y 3560 las Plataformas del Catalyst 6500.
- Una plataforma de ruteo debe ejecutar el IOS apropiado. Las Plataformas incluyen, pero no se limitan a, los 7600, los 3900, la 3800, 2900, 2800, 1900, 1800, y el Routers de los Servicios integrados de las 800 Series (ISR).
- Considere el número de saltos de la capa 3 entre los pedazos relevantes de infraestructura. Para determinar el número de saltos de la capa 3, mantenga el despliegue tan simple como sea posible. Por ejemplo, si cinco saltos de la capa 3 existen entre la infraestructura que recibe los dispositivos del Señalización asociada al canal (CAS) y a los clientes, puede crear el consumo de recursos gasto administrativo.

Con la solución incorrecta:

- El enlace de la capa 2 crea una topología muy subóptima de la capa 2.
- Los subinterfaces de la capa 3 crean muchas interfaces adicionales para configurar. Más interfaces a configurar pueden crear los problemas adicionales del IP Addressing de la tara de administración y del potencial. Con la suposición que no hay Redundancia en la infraestructura, cada capa de la red tiene un ingreso y interfaz física de la salida. El cómputo para el número de subi-nterfaces es entonces (2 * número de gradas en la red * número de VRF). Nuestro ejemplo tiene dos VRF, así que la fórmula es (2 *5 * 2) o 20 subinterfaces. Después de que se agregue la Redundancia, este número más que dobla. Compare esto a la extensión GRE, donde solamente cuatro interfaces se requieren con el mismo resultado final. Esta comparación ilustra cómo el GRE reduce el impacto de la configuración.

Enlace de la capa 2

El enlace de la capa 2 se prefiere en los escenarios donde los dispositivos de la capa de acceso no soportan los subinterfaces. Las 4500 Plataformas del Catalyst 3560, 3750, y no soportan los subinterfaces.

En un acceso de la capa 3 modelo que conecta con una plataforma que no soporte los subinterfaces a una plataforma que lo haga, sólo enlace de la capa 2 del uso en un lado y subinterfaces del uso en el otro lado. Esta configuración mantiene todas las ventajas de una arquitectura del armario de la capa 3 y todavía supera la limitación de ningún soporte de la sub-interfaz en algunas Plataformas.

Una de las ventajas primarias de configurar el enlace de la capa 2 en solamente un lado del link es que el Spanning-tree no está introducido nuevamente dentro del entorno de la capa 3. Vea el ejemplo de 3750 configuraciones pertinentes donde un switch de acceso 3750. cuál no soporta el GRE o los subinterfaces, está conectado con un switch de distribución 6500. El switch de distribución 6500 soporta el GRE y los subinterfaces.

Configuración pertinente 3750

En esta configuración, la configuración predeterminada para el VLAN NATIVO es VLAN1 en el FastEthernet 1/0/1. Esta configuración no se ha cambiado. Sin embargo, el VLAN1 no se permite ser trunked a través del link. Los VLA N permitidos se limitan solamente a los VLA N se marcan con etiqueta que.

No hay necesidad de la negociación de tronco del switch a switch o del tráfico del VLAN Trunk

Protocol (VTP) en este Layer 3 Topology. Por lo tanto, no hay tampoco necesidad de ningún tráfico sin Tags de ser transmitido en este link. Esta configuración aumenta la postura de seguridad de la arquitectura porque no abre a las brechas en la seguridad innecesarias de la capa 2.

Ejemplo de 3750 configuraciones pertinentes

```
!--- 3750 Switch configuration, related to connecting it
to a !--- sub-interface capable switch (Catalyst 6500):
! ip vrf DIRTY rd 100:1 ! ip vrf GUEST rd 600:1 !
interface GigabitEthernet1/0/48 description Uplink to
Cat6k switchport trunk encapsulation dot1q switchport
trunk allowed vlan 901-903,906 switchport mode trunk
spanning-tree portfast trunk ! !--- Since the 3750 does
not support sub-interfaces, !--- you must configure one
SVI per transit network: ! interface Vlan901 description
DIRTY_TRANSIT ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 ! interface Vlan902
description GLOBAL_TRANSIT ip address 172.26.120.6
255.255.255.252 ! interface Vlan906 description
GUEST_TRANSIT ip vrf forwarding GUEST ip address
172.26.120.14 255.255.255.252 ! !--- This configuration
uses EIGRP as the routing protocol !--- of choice in
this document. !--- Each VRF is defined as a separate !-
-- Autonomous System under the Global AS. ! router eigrp
26 ! address-family ipv4 vrf DIRTY network 172.26.120.0
0.0.0.255 autonomous-system 100 no auto-summary exit-
address-family ! address-family ipv4 vrf GUEST
redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family network 172.26.0.0
```

Configuración pertinente 6500

En esta configuración, la encapsulación del dot1q se utiliza para marcar las tramas con etiqueta con el VLA N 901, 902, y 906. Cuando usted selecciona el VLA N marca con etiqueta para utilizar en una sub-interfaz, usted no puede utilizar un número VLAN que se defina ya localmente en la base de datos de VLAN en el Switch.

Ejemplo de 6500 configuraciones pertinentes

```
!--- 6500 Switch configuration, related to connecting it
!--- to a non-sub-interface capable switch (Catalyst
3750): ! ip vrf DIRTY rd 100:26 ! ip vrf GUEST rd 600:26
! interface FastEthernet1/34 description NAC LAB - 3750
no ip address ! interface FastEthernet1/34.901
encapsulation dot1Q 901 ip vrf forwarding DIRTY ip
address 172.26.120.1 255.255.255.252 ! interface
FastEthernet1/34.902 encapsulation dot1Q 902 ip address
172.26.120.5 255.255.255.252 ! interface
FastEthernet1/34.906 encapsulation dot1Q 906 ip vrf
forwarding GUEST ip address 172.26.120.13
255.255.255.252 ! !--- EIGRP is the routing protocol of
choice in this document. !--- Each VRF is defined as a
!--- separate Autonomous System under the Global AS. !--
- See Configure Routing for the VRF for more
information. ! router eigrp 26 network 172.26.0.0
0.0.255.255 no auto-summary passive-interface Vlan1
redistribute static ! address-family ipv4 vrf DIRTY
autonomous-system 100 network 172.26.120.0 0.0.0.3
```

```
network 172.26.160.0 0.0.0.255 no auto-summary no
default-information out redistribute static route-map
gw-route exit-address-family ! address-family ipv4 vrf
GUEST redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family !
```

Encaminamiento de la configuración para el VRF

Según lo discutido anterior en las consideraciones importantes para la sección de VRF-Lite que usa, VRF-Lite soporta el BGP, el OSPF, y el EIGRP. En este ejemplo de configuración, se selecciona el EIGRP porque es el Routing Protocol que Cisco recomienda para la implementación en las redes de oficinas centrales dónde se requiere la convergencia rápida.

Nota: Trabajos OSPF igualmente bien con VRF-Lite, al igual que BGP.

Nota: Se requiere el BGP si el diseño requiere que el tráfico “esté escapado” entre los VRF.

Encaminamiento para un VRF con el ejemplo de configuración de EIGRP

```
!
!--- This base routing protocol configuration handles
the routing !--- for the Global Routing Table. ! router
eigrp 26 network 172.26.50.0 0.0.0.255 network
172.26.51.0 0.0.0.255 network 172.26.52.0 0.0.0.255
network 172.26.55.0 0.0.0.255 network 172.26.60.0
0.0.0.255 network 172.26.61.0 0.0.0.255 network
172.26.62.0 0.0.0.255 network 172.26.120.4 0.0.0.3
network 172.26.176.0 0.0.0.255 network 172.26.254.1
0.0.0.0 no auto-summary passive-interface Vlan1
redistribute static ! !--- You must define an address
family for each VRF !--- that is to be routing using the
routing protocol. !--- Routing protocol options such as
auto-summarization, !--- AS number, and router id are
all configured under the !--- address family. EIGRP does
not form a neighbor !--- relationship without the AS
specified under the address family. !--- Also, this AS
number needs to be unique for !--- each VRF and cannot
be the same as the global AS number. ! address-family
ipv4 vrf DIRTY autonomous-system 100 network
172.26.120.0 0.0.0.3 network 172.26.160.0 0.0.0.255 no
auto-summary no default-information out redistribute
static route-map gw-route exit-address-family ! address-
family ipv4 vrf GUEST redistribute static network
172.26.120.0 0.0.0.255 autonomous-system 600 no auto-
summary exit-address-family !
```

Tráfico de la ruta entre la tabla de Global Routing y el VRF sucio

Dependiendo de los requisitos del despliegue del NAC, puede ser necesario pasar el tráfico del lado untrusted o sucio de la red al haber confiado en o limpiar el lado de la red. Por ejemplo, los servicios de la corrección pueden potencialmente vivo en el lado de confianza del dispositivo NAC de Cisco. En el caso del Active Directory solo muestra-en las implementaciones, es necesario pasar un subconjunto de tráfico al Active Directory para permitir el intercambio del boleto del Kerberos de los inicios de sesión interactivos, y así sucesivamente.

En cualquier caso, es muy importante que la tabla de Global Routing sabe alcanzar el VRF sucio,

y que el VRF sucio sabe alcanzar la tabla de Global Routing si algunos datos necesitan pasar entre los dos. Esto es dirigida típicamente por la metodología en el cuadro 8.

El VRF sucio omite la interfaz untrusted o sucia del dispositivo NAC de Cisco. El global tiene Static rutas solamente a las subredes que se consideran los VLA N sucios. Esas Static rutas señalan a la interfaz (de confianza) limpia del servidor del NAC de Cisco como el salto siguiente.

Cuadro 8 – ***Rutear los flujos***

El primer salto de la capa 3 en el lado untrusted o sucio del dispositivo NAC de Cisco redistribuye una ruta predeterminado en un proceso de ruteo esas puntas al dispositivo NAC de Cisco. El primer salto de la capa 3 en el lado de confianza o limpio del dispositivo NAC de Cisco redistribuye una Static ruta para las subredes que pertenecen a los VLA N sucios en la capa de acceso (en este caso 172.26.123.0/26).

Nota: El primer salto de la capa 3 en los lados opuestos del dispositivo NAC de Cisco puede estar en el mismo dispositivo físico, pero en diversos VRF.

Nota: En la topología usada para este documento, sigue habiendo el lado untrusted o sucio del servidor del NAC de Cisco está en un VRF, mientras que haber confiado en o limpia el lado del dispositivo NAC de Cisco en la tabla de Global Routing. Sin embargo, ambas interfaces están conectadas con el mismo Switch de centro de datos.

Ejemplo de configuración de VRF-Lite de la capa 3 del NAC de Cisco OOB

Para desplegar con éxito una solución del NAC de Cisco OOB, usted necesita configurar los componentes del NAC para hacer juego la arquitectura deseada. El cuadro 9 es un diagrama de red lógica del NAC de Cisco de la capa 3 OOB que se utiliza en esta sección para mostrar la configuración pertinente servidor del NAC de Cisco del NAC del administrador, de Cisco, y Edge Switch para una capa 3 del NAC OOB con el despliegue de VRF-Lite.

Cuadro 9 – ***Topología lógica de la capa 3 del NAC de Cisco OOB***

Complete los pasos en estas secciones para configurar un despliegue del NAC real-IP OOB VRF Cisco de la capa 3:

Paso 1: Configure el Edge Switch

Como estos ejemplos de configuración muestran, cree dos más VLA N (SUCIOS e INVITADO) en el Edge Switch.

El VLA N existente de la producción (VLA N 200) se utiliza para todos los sistemas corporativos. Este ejemplo crea los VLA N, sus asociados transitan las redes, y asignan ambos a los VRF correctos. La aplicación ocurre en el servidor del NAC de Cisco, así que usted no necesita aplicar los ACL a cada VLA N en el Switch.

Función no autenticada: VLAN 100, ejemplo sucio de la configuración de VRF
`!--- Define the DIRTY VRF.` ip vrf DIRTY rd 100:3 `!--- Create the SVI for the DIRTY VLAN.` interface Vlan100 ip vrf forwarding DIRTY ip address 172.26.123.1

```
255.255.255.224 ip helper-address vrf DIRTY 172.26.51.11
!--- Create the SVI for the DIRTY_TRANSIT_NETWORK.
interface Vlan301 ip vrf forwarding DIRTY ip address
172.26.120.50 255.255.255.252 !--- Set the allowed VLAN
on the trunk. interface FastEthernet1/0/48 switchport
trunk allowed vlan add 301 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf DIRTY
network 172.26.0.0 autonomous-system 100 no auto-summary
exit-address-family
```

Rol de invitado: VLA N 600, ejemplo de la configuración de VRF del INVITADO

```
!--- Define the GUEST VRF. ip vrf GUEST rd 600:3 !---
Create the SVI for the GUEST VLAN. interface Vlan600 ip
vrf forwarding GUEST ip address 172.26.123.193
255.255.255.224 !--- Create the SVI for the
DIRTY_TRANSIT_NETWORK. interface Vlan306 ip vrf
forwarding GUEST ip address 172.26.120.62
255.255.255.252 !--- Set the allowed VLAN on the trunk.
interface FastEthernet1/0/48 switchport trunk allowed
vlan add 306 !--- Set up the routing for the VRF. router
eigrp 26 address-family ipv4 vrf GUEST network
172.26.0.0 autonomous-system 600 no auto-summary exit-
address-family
```

Paso 2: Configure el switch del núcleo

Los ejemplos de configuración en esta sección muestran la simulación de un Núcleo colapsado con un Catalyst 3750-E Switch. En la mayoría de los entornos, esto no es un Switch de la borde-clase. Sin embargo, el Switch fue construido en el ambiente de laboratorio usado para este documento.

Cree cuatro más VLA N para transitan las redes, dos para el VLA N SUCIO y dos para el VLA N del INVITADO. Véase el cuadro 10.

- VLA N SUCIOVLA N 301 SUCIO del borde a quitar el corazónVLA N 901 SUCIO de la base al centro de datos
- VLA N DEL INVITADOINVITADO del VLA N 306 del borde a quitar el corazónINVITADO del VLA N 906 de la base al centro de datos

Un transit network se está construyendo a partir del borde a la base, y de un segundo para la base al centro de datos. Las redes del transitar se deben completar para que el SUCIO y el INVITADO VRF. Si el Tag Switching se habilita en vez de VRF-Lite, esto no es necesario.

Nota: Este documento se centra en VRF-Lite, y el Tag Switching se considera hacia fuera-de-alcance.

Cuadro 10 – *Transite las redes*

:

VLA N 301 SUCIO del borde a quitar el corazón; VLA N 901 SUCIO de la base al ejemplo de configuración del centro de datos

```
!--- This is the core switch. !--- Define the DIRTY VRF.
ip vrf DIRTY rd 100:1 !--- Create the SVI for the DIRTY
```

```
VLANs. interface Vlan301 desc This is the Transit
Network between the Edge & Core ip vrf forwarding DIRTY
ip address 172.26.120.49 255.255.255.252 interface
Vlan901 desc This is the Transit Network between the
Core and the DC ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 !--- Set the allowed VLAN
on the trunks. interface GigabitEthernet1/0/3 switchport
trunk allowed vlan add 301 interface
GigabitEthernet1/0/48 switchport trunk allowed vlan add
901 !--- Set up the routing for the VRF. router eigrp 26
address-family ipv4 vrf DIRTY network 172.26.0.0
autonomous-system 100 no auto-summary exit-address-
family exit-address-family
```

INVITADO del VLA N 306 del borde a quitar el corazón; INVITADO del VLA N 906 de la base al ejemplo de configuración del centro de datos

```
!--- This is the core switch. ! !--- Define the GUEST
VRF. ip vrf GUEST rd 600:1 !--- Create the SVI for the
GUEST VLANS. interface Vlan306 desc This is the transit
network between the Edge & Core ip vrf forwarding GUEST
ip address 172.26.120.61 255.255.255.252 interface
Vlan906 description Transit Network between Core & DC ip
vrf forwarding GUEST ip address 172.26.120.14
255.255.255.252 !--- Set the allowed VLAN on the trunks.
interface GigabitEthernet1/0/3 switchport trunk allowed
vlan add 306 interface GigabitEthernet1/0/48 switchport
trunk allowed vlan add 906 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf GUEST
network 172.26.0.0 autonomous-system 600 no auto-summary
exit-address-family
```

Paso 3: Configure el Switch de centro de datos

Mientras que el ejemplo de configuración muestra, el servidor del NAC de Cisco tiene ambas interfaces conectadas con el mismo Switch de centro de datos 6500. La interfaz confiada en está en el VLA N 60, y la interfaz no confiable está en el VLA N 160, que está en el VRF SUCIO.

1. Cree cuatro más VLA N para la conexión a la base:Un VLA N sucio (160)Un VLA N limpio (60)Un transit network sucio (901)Un transit network limpio (906)Agregue el VLA N SUCIO al VRF SUCIO.Termine al INVITADO VRF en un INVITADO DMZ (999) ese las aplicaciones un Firewall de Cisco ASA (fuera del alcance para este documento) para conectar a los Usuarios invitados con Internet y realizar las funciones del Network Address Translation (NAT).
2. Cree el SUCIO y el INVITADO transita los subinterfaces.Los comandos mostrados en el ejemplo de la configuración del switch del centro de datos realizan estas tareas:Defina el SUCIO y al INVITADO VRF.Cree las redes SUCIAS y LIMPIAS para el servidor del NAC de Cisco.

Ejemplo de la configuración del switch del centro de datos

```
!--- Define the DIRTY and GUEST VRFs. ip vrf DIRTY rd
100:26 ip vrf GUEST rd 600:26 !--- Create the sub-
interface and switched virtual interface (SVI) !--- for
the DIRTY and GUEST VLANs. interface
FastEthernet1/34.901 desc Transit Network from Core to
```

```
DC for DIRTY traffic encapsulation dot1Q 901 ip vrf
forwarding DIRTY ip address 172.26.120.1 255.255.255.252
interface FastEthernet1/34.906 desc Transit Network from
Core to DC for GUEST traffic encapsulation dot1Q 906 ip
vrf forwarding GUEST ip address 172.26.120.13
255.255.255.252 interface Vlan60 desc Trusted (CLEAN)
side of the NAC Server ip address 172.26.60.1
255.255.255.0 interface Vlan160 desc Untrusted (DIRTY)
side of the NAC Server ip vrf forwarding DIRTY ip
address 172.26.160.1 255.255.255.0 interface Vlan999
description GUEST VLAN SVI ip vrf forwarding GUEST ip
address 192.168.26.254 255.255.255.0 !--- Set up the
routing for the VRFs. router eigrp 26 network
172.26.60.0 0.0.0.255 no auto-summary redistribute
static address-family ipv4 vrf DIRTY autonomous-system
100 network 172.26.120.0 0.0.0.3 network 172.26.160.0
0.0.0.255 no auto-summary redistribute static exit-
address-family address-family ipv4 vrf GUEST network
172.26.0.0 network 192.168.26.0 autonomous-system 600 no
auto-summary redistribute static exit-address-family !--
- Set up the static routes for redistribution for the
VRFs. ip route 172.26.123.0 255.255.255.192 172.26.60.2
ip route vrf DIRTY 0.0.0.0 0.0.0.0 172.26.160.2 ip route
vrf GUEST 0.0.0.0 0.0.0.0 192.168.26.1
```

Paso 4: 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. Vaya a instalar el Access Manager limpio y el servidor de acceso limpio para realizar la configuración inicial.

Paso 5: Aplique una 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 información sobre cómo cargar las licencias, vaya al *acceso la* sección de la *consola Web CAM de* instalar el Access Manager limpio y limpie el servidor de acceso.

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.

Paso 6: Directivas de la actualización 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. 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 al *login del agente del requerir para la* sección de las *máquinas del cliente de* configurar el dispositivo NAC de Cisco para el login del agente y la evaluación de la postura del cliente.

Paso 7: 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 al *Tiempo del sistema del conjunto* y *limpie las* secciones *de acceso directo de la consola Web del servidor de acceso de* administrar el CAM.

Nota: Si usted utiliza 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. Esto requiere que usted cargue los Certificados para ambos como Certificate Authority de confianza bajo **SSL >** las **autoridades del certificado confiable**.

Paso 8: Configuración de servidor del NAC de Cisco del estudio

La mayoría del asunto importante a recordar para un diseño acertado del NAC es que el tráfico clasificado como flujo sucio de la necesidad en el lado untrusted del servidor del NAC, como cuadro 11 muestra:

Cuadro 11 – ***Instrumentación del servidor del NAC de Cisco***

Paso 9: Agregue el servidor del NAC de Cisco al administrador del NAC de Cisco

Complete estos pasos para agregar el servidor del NAC de Cisco al administrador del NAC de Cisco:

1. Haga clic **CCA los servidores** bajo el cristal de la Administración de dispositivos. Véase el cuadro 12.
2. Haga clic la nueva lengueta del servidor.
3. Utilice el cuadro del dirección IP del servidor para agregar la dirección IP de la interfaz confiada en de Cisco del servidor del NAC.
4. En el rectángulo de la ubicación del servidor, ingrese **OOB el servidor del NAC de Cisco** como la ubicación del servidor.
5. Elija el Real-IP-**gateway fuera de banda de la** lista desplegable del tipo de servidor.
6. El tecleo **agrega el servidor de acceso limpio**.

Cuadro 12 – ***Agregar el servidor del NAC de Cisco al administrador del NAC de Cisco***

Nota: El servidor del NAC de Cisco del NAC del administrador y de Cisco tiene que confiar en CA de cada uno para que el administrador agregue con éxito el servidor.

Después de que usted agregue el servidor del NAC de Cisco, aparece en la lista conforme a la lista de lengueta de los servidores. Ver Figura 13.

Paso 10: Configure el servidor del NAC de Cisco

Complete estos pasos para configurar el servidor del NAC de Cisco:

1. Haga clic la lista de lengueta de los servidores.
2. Haga clic el icono del manejo para el servidor del NAC de Cisco para continuar la configuración.

Cuadro 13 – ***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 14 aparece.

Paso 11: Soporte de la capa 3 del permiso

Complete estos pasos para habilitar el soporte de la capa 3:

1. Seleccione la lengueta de la red.
2. Marque el checkbox del **soporte del permiso L3**.
3. Marque el **modo estricto del permiso L3 para bloquear los dispositivos NAT con el** checkbox del **agente del NAC**.
4. Haga clic en **Update** (Actualizar).
5. Reinicie el servidor del NAC de Cisco según lo dado instrucciones.

Cuadro 14 – ***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 un certificado nombre-basado, el nombre necesita resolver al IP Address de la interfaz no confiable. Cuando el punto extremo comunica con la interfaz no confiable del servidor para comenzar el proceso del NAC, el servidor reorienta 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.

Paso 12: Static rutas de la configuración

Complete estos pasos para configurar las Static rutas:

1. Después de que las reinicializaciones del servidor del NAC de Cisco, vuelvan al servidor y continúen con la configuración.El servidor del NAC de Cisco debe utilizar la interfaz no confiable para comunicar con los puntos extremos en el VLA N del unauthenticated.
2. **Avanzado** selecto > **Static rutas** para agregar las rutas al VLA N del unauthenticated.
3. Complete las subredes apropiadas para los VLA N del unauthenticated.
4. El tecleo **agrega la ruta**.
5. Seleccione la **interfaz no confiable [eth1]** para estas rutas.

Cuadro 15 – ***Agregue una Static ruta para alcanzar el Subred de usuario O.N.U-autenticado***

Paso 13: Perfiles de la configuración para el Switches en el administrador del NAC de Cisco

Complete estos pasos para configurar los perfiles para el Switches en el administrador del NAC de Cisco:

1. Seleccione **OOB la Administración** > los **perfiles** > el **dispositivo** > **editan**.
2. Complete la información de perfil del dispositivo. Utilice el cuadro 16 como guía.Cada Switch se asocia a un perfil. Agregue un perfil para cada tipo de Edge Switch que el administrador del NAC de Cisco manejará. En este ejemplo, se maneja un 3750 Switch.**Cuadro 16 – *Perfil SNMP usado para manejar el Switch***
3. Configure la configuración del switch para el SNMP.Configure el Edge Switch para las mismas cadenas de comunidad de lectura/grabación SNMP que se configuran en el administrador del NAC de Cisco.
```
snmp-server community Cisco123 RO
snmp-server community Cisco1234 RW
```
4. Seleccione **OOB la Administración** > los **perfiles** > el **puerto** > **nuevo**. Véase el cuadro 17.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 el paso 17: Configure los rol del usuario. Las sincronizaciones LDAP se pueden utilizar para asociar los rol del usuario en el NAC a los grupos LDAP. Para más información, refiera a NAC(CCA) 4.x: Asocie a los usuarios a ciertos papeles usando el ejemplo de la Configuración LDAP.**Cuadro 17 – *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 identificaciones de VLAN en diverso Switches a través del campus. Sin embargo, el mismo nombre del VLA N se asocia 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 adentro 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** checkbox **cambiado**. Si se marca esto, puede reiniciar posiblemente el teléfono del IP cuando se despide el puerto.**Cuadro 18 – *Perfil inferior disponible del puerto de las diversas opciones***

Paso 14: Configuraciones del receptor de la configuración SNMP

Además de configurar la cadena de comunidad SNMP para el Read/Write, usted también necesita 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 extremo determinado al

administrador, el administrador puede construir una tabla de correspondencia internamente para el MAC/IP y el puerto del switch.

1. Seleccione **OOB la Administración** > los **perfiles** > el **receptor SNMP**.
2. Configure las configuraciones del SNMP trap como esta figura muestra:**Cuadro 19 – *La configuración del receptor del administrador SNMP del NAC de Cisco para recoger el SNMP traps e informa***
3. 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 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** para especificar a la dirección de origen que se utiliza para enviar los desvíos.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 el Calidad de Servicio (QoS) para el SNMP en un entorno de red del mucho tráfico.

Paso 15: Agregue el Switches como dispositivos en el administrador del NAC de Cisco

Complete estos pasos para agregar el Switches como dispositivos en el administrador del NAC de Cisco:

1. Seleccione **OOB la Administración** > los **dispositivos** > los **dispositivos** > **nuevo**.Utilice el perfil del Switch creado en el paso 13 para agregar el Switch.
2. Bajo perfil del dispositivo, utilice el perfil que usted creó. No cambie el valor del perfil del puerto predeterminado cuando usted agrega el Switch.**Cuadro 20 – *Agregue el Edge Switch en el administrador del NAC de Cisco para controlar vía el SNMP***
3. Después de que el Switch se agregue al administrador del NAC de Cisco, usted puede seleccionar los puertos que usted quiere manejar.

Paso 16: Configure los puertos del switch para que los dispositivos sean manejados por el NAC

Complete estos pasos para configurar los puertos del switch para que los dispositivos sean manejados por el NAC.

1. 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.**Cuadro 21 – *Selección del control del puerto disponible para un Switch manejado***
Nota: No deje el perfil predeterminado como “incontrolado” hasta que usted pueda marcar las interfaces apropiadas estáticamente como “incontrolado”. Después de los puertos de link ascendente, y de cualquier otro puerto encendido-apagado que necesite seguir siendo incontrolado se fijan; entonces cambie el valor por defecto a su perfil controlado del puerto.

El error hacer tan en esta orden puede dar lugar a los resultados menos que deseables.
2. Seleccione **OOB el Switch de la Administración** > de **dispositivos [IP address]** > los **puertos** > **manejan** para manejar varios puertos inmediatamente.

Cuadro 22 – *Maneje los puertos múltiples con la opción del unido*

Paso 17: Rol del usuario de la configuración

En este ejemplo, los VLA N que corresponden a cada papel se crean ya en el Edge Switch.

1. Seleccione **User Management (Administración de usuario)** > los **rol del usuario** > **editan el papel** y crean un papel del empleado como esta figura muestra:**Cuadro 23 – *Cree un papel del empleado y asocie el VLAN DE DATO***
2. Seleccione **User Management (Administración de usuario)** > los **rol del usuario** > **editan el papel** y crean un rol de invitado como esta figura muestra:**Cuadro 24 – *Cree un rol de invitado y asocie el VLA N del INVITADO***

Paso 18: 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.

Paso 19: 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, usted debe descargar al cliente de ActiveX o del componente Java al final para realizar estas tareas:

- Traiga la dirección MAC de la máquina del cliente.
- Realice la versión de la dirección IP y renueve.

1. Seleccione la **administración** > las **páginas del usuario**.
2. Edite la página para habilitar las opciones como esta figura muestra:

Cuadro 25 – *Paginaciones del usuario para el login de la red*

Paso 20: Personalice el agente del NAC de Cisco para los rol del usuario

Complete estos pasos para personalizar el agente del NAC de Cisco para los rol del usuario:

1. Seleccione la **Administración de dispositivos** > **acceso limpio** > **configuración** > **login generales del agente**.Usted puede configurar al administrador del NAC de Cisco 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.
2. Marque el **uso del requerir del** checkbox del **agente**.

Cuadro 26 – *Login del agente requerido para el papel del empleado*

Paso 21: 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 configuración el dispositivo NAC de Cisco para el login del agente y la evaluación de la postura del cliente. Este ejemplo configura el host de la detección en el administrador del NAC de Cisco.

Seleccione la **Administración de dispositivos > limpian el acceso > limpian el agente >** la **instalación del acceso**:

Cuadro 27 – ***Descubra el host para un agente del NAC de Cisco***
PRE-se puebla el campo del host de la detección si el agente del NAC de Cisco se descarga del servidor del NAC de Cisco. Consulte la figura 27.

Nota: En una capa 3 OOB con el modelo VRF, el host de la detección se fija típicamente para ser el nombre DNS o la dirección IP del administrador del NAC de Cisco, que existe en la red limpia. Porque todo el tráfico de las redes “sucias” se rutea por abandono a través del servidor del NAC de Cisco, los paquetes de detección atraviesan automáticamente el servidor. El flujo de tráfico descrito aquí es una de las ventajas al método VRF. Preve una experiencia constante, fiable. Vea los flujos del proceso del NAC de Cisco para más información.

Paso 22: Login de la red

Complete estos pasos para iniciar sesión con la red:

1. 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. Aseegurese que la máquina recibe una dirección IP de la subred del VLA N del unauthenticated.
2. 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 reorientan a la interfaz no confiable del servidor del NAC de Cisco, el hojeador reorienta automáticamente a una página de registro. Si no lo hace, ir a un URL específico tal como guest.nac.local para realizar el login:

Cuadro 28 – ***Página de registro de la red***

Paso 23: Login del agente

Usted puede distribuir el agente del NAC de Cisco apenas como cualquier aplicación del otro software a los usuarios finales o usted puede forzarla 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.

Esta figura muestra la pantalla que aparece cuando se activa el agente:

Cuadro 29 – ***Login del agente***

1. Seleccione el servidor de la lista desplegable del servidor.
2. Ingrese el nombre de usuario.
3. Ingrese la contraseña.
4. Haga clic en Login (Conexión).Los cuadros 30 y 31 muestran las pantallas que

aparecen:.**Cuadro 30 –** ***El agente del NAC de Cisco que realiza la versión IP o renueva*** **Cuadro 31 –** ***El agente del NAC de Cisco que indica el acceso a la red completo después del IP restaura***

5. Haga clic en OK.

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

Usted puede configurar al administrador del NAC de Cisco 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. Estos puntos claves 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. Utilice este IP del servicio 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. Usted debe evitar la situación donde está activo un administrador pero no es directo 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 configurar la Alta disponibilidad.

Servidor del NAC de Cisco

Para proporcionar la protección contra un solo punto de falla, usted puede configurar el servidor del NAC de Cisco 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.

Estos puntos claves 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 configurar la Alta disponibilidad.

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 configurar el Active Directory solo Muestra-en.

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 el canal 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, va la Interoperabilidad al NAC de los scripts y de Cisco de Windows GPO.

El dispositivo NAC de Cisco de la configuración para el login del agente y el cliente Posture la evaluación

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

Información Relacionada

- Página de soporte del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems