Capa 3 del NAC fuera de la guía de diseño de la banda que utiliza VRF-Lite para el aislamiento de tráfico

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Configurar
Configuración de la infraestructura
Topología
Flujos del proceso
Configuración
Configuración de NAC para la capa 3 OOB
Configuración de CAS
Verificación
Apéndice A: Configuraciones del switch
Troubleshooting
Información Relacionada

Introducción

Nota: La información de este documento puede cambiar sin previo aviso. Confirme todas las recomendaciones si es posible.

El propósito de este documento es describir una implementación basada VRF-Lite del NAC en una capa 3 fuera del despliegue de la banda (OOB) donde el servidor del NAC (CAS) se configura en el modo (ruteado) real del gateway IP. La capa 3 fuera de la banda tiene rápidamente convertido de las metodologías más populares del despliegue para el NAC. Esta rotación en el renombre se basa en varias dinámicas. El primer es una mejor utilización de los Recursos de hardware. Por el despliegue del NAC en una metodología de la capa 3 OOB, un solo dispositivo NAC se puede hacer para 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. Hay dos acercamientos ampliamente utilizados para desplegar el NAC en una arquitectura de la capa 3 OOB.

1. Acercamiento basado Detección-host — Utiliza la capacidad inherente dentro del agente del NAC para alcanzar el servidor del NAC (CAS). ACL aplicados en la aplicación del tráfico de

control del switch de acceso en la red sucia. Refiera a conectar con el NAC el servidor (CAS) usando el protocolo SWISS para más información.

2. El VRF basó el acercamiento — Aplicaciones VRF de rutear el tráfico del unauthenticated a CAS. Las políticas de tráfico configuradas en el servidor del NAC (CAS) se utilizan para la aplicación en la red sucia. Este acercamiento tiene dos sub-acercamientos. En el primer acercamiento, los VRF son penetrantes en la infraestructura, en este caso todos acodan 3 dispositivos participan en el Tag Switching. El segundo acercamiento utiliza VRF-Lite y los túneles GRE para hacer un túnel los VRF a través de los dispositivos de la capa 3 que no entienden el Tag Switching. La ventaja al segundo acercamiento es que los cambios de configuración mínima están requeridos a su infraestructura esencial.

Nota: Mientras que la capa 3 OOB es una de la mayoría de las metodologías de la instalación común, no puede siempre ser la solución óptima para cada entorno. Hay otras opciones de elegir de eso puede ser un más grado óptimo cabido para sus requerimientos particulares. Refiera a planear su despliegue para más información en estas otras opciones del diseño del NAC.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Una comprensión básica operación y configuración de la infraestructura de la capa 2 y de la capa 3
- Una comprensión básica del dispositivo NAC de Cisco, y las diferencias entre las diversas metodologías de la implementación que se asocian a él
- Todas las implementaciones y diseños del NAC se deben basar en los requisitos comerciales claros. Éstas son las suposiciones del requisito comercial para esta Configuración de prueba:Los usuarios deben ser autenticados antes de ser concedida el acceso a la red at large.Su acceso es limitado basado en quién son los usuarios. Estos privilegios se asocian a la membresía del grupo en el Active Directory. Los grupos son invitados, contratistas, y empleados.De acuerdo con la membresía del grupo AD, colocan a los usuarios en un VLA N que tenga privilegios de acceso a la red que sean apropiados para cada grupo.El tráfico del Usuario invitado continúa siendo aislado del resto de la red incluso después la autenticación.Después de que admitan al usuario a la red, el dispositivo NAC debe no más estar en el trayecto del tráfico. Esto evita el dispositivo NAC se convierta en un embotellamiento y permite que la red sea utilizada a su potencial completo por los usuarios validados.
- El NAC tiene muchas capacidades que no sean cubiertas por este documento. El propósito de esta guía es explorar y documentar las pautas de diseño y la configuración requeridas para una capa basada 3 de VRF-Lite fuera del despliegue del NAC de la banda. Esta guía no se centra en la evaluación o la corrección de la postura. Más información sobre el dispositivo NAC y sus capacidades totales se pueden encontrar en www.cisco.com/go/nac (clientes registrados solamente).

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de

hardware.

Convenciones

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

Configurar

Configuración de la infraestructura

Introducción:

Cuando en vista de un VRF-Lite basado el despliegue del NAC de la capa 3 OOB, allí es varios principios de diseño que son muy importantes considerar. Estos principios se enumeran aquí, y una explicación abreviada de su importancia es incluida.

1. **Clasificación de tráfico e ingeniería** — Un concepto fundamental a realizar y a recordar para este tipo de diseño del NAC es que tráfico clasificado como flujo sucio de la *necesidad* en el lado untrusted del servidor del NAC (CAS). Guarde siempre este top del principio de la mente durante el diseño de una implementación del NAC. Además, las redes limpias y sucias no se deben permitir comunicar directamente con uno a. En un diseño de la capa 3 OOB con los VRF, el servidor del NAC (CAS) actúa como la punta o el regulador de la aplicación que asegura la segregación y la comunicación segura entre las redes limpias y sucias.
2. **Aislamiento de tráfico** — Es importante estar seguro que un mecanismo de aplicación apropiado está seleccionado para proporcionar el tráfico y el aislamiento de la trayectoria para todos tráfico originado de los host NON-autenticados y NON-autorizados. VRF-Lite se utiliza aquí para alcanzar el aislamiento completo de los datos y de la controle de plano (VRF).
3. **Aplicación centralizada** — Porque la metodología de VRF-Lite sigue la selección de trayecto natural creada ruteando: los cambios de la topología, los requisitos del control de acceso, y/o los cambios de dirección no crean la necesidad de manipular los ACL a través de la infraestructura. Si usted utiliza un túnel GRE conjuntamente con VRF-Lite, éste le da la flexibilidad para caer la derecha sucia del tráfico delante del servidor del NAC sin la necesidad de configurar los saltos múltiples. VRF-Lite conjuntamente con el GRE requiere solamente la configuración en los dispositivos de la capa 3 del borde. Esto reduce dramáticamente el número de dispositivos que se deban tocar para proporcionar el requisito del aislamiento de la trayectoria.
4. **Dificultad** — Dificultad de la implementación así como del mantenimiento continuo. Cuando usted determina el acercamiento que usted es probable utilizar para la capa 3 del NAC OOB en su red, es importante considerar la facilidad de la implementación y costo de funcionamiento y complejidad en curso de implementar esa tecnología, determinado en un entorno dinámico.

Nota: El dispositivo NAC 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 GRE, ni fue reorientado con la configuración de ruteo basada directiva, VRF ruteado y así sucesivamente.

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

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

Un ejemplo de la virtualización del dispositivo con los VRF se puede considerar aquí. Esta metodología proporciona el avión del control y los datos acepillan para el aislamiento de la trayectoria.

Topología

Este diagrama es representante de la topología usada para la creación de este papel. La red interna está ruteando a través de la tabla de Global Routing y no tiene ningún VRF asociado a ella. El VRF SUCIO contiene solamente el Dirty_VLAN y el asociados transitan las redes que se requieren para forzar todos los datos con origen del DIRTY_VLAN para atravesar el lado sucio de los dispositivos NAC. El invitado VRF contiene el GUEST_VLAN y asociado transite las redes requeridas para terminar todos los datos con origen del GUEST_VLAN en una Sub-interfaz separada en el Firewall. Cada uno de las tres redes virtuales se lleva en la misma Infraestructura física y proporciona el aislamiento completo del tráfico y de la trayectoria respectivamente.

Flujos del proceso

Esta sección muestra el flujo de proceso básico con de lo que se requiere para tener el acceso a la red ambos, y sin un agente instalado. Estos flujos del proceso son macroanáliticos en la naturaleza y contienen solamente los pasos funcionales de la decisión. 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.

Configuración

La información de la configuración detalla los pasos requeridos configurar su red para el aislamiento de la trayectoria usando VRF-Lite/GRE y la configuración requerida para la inserción del dispositivo NAC en su red como gateway IP OOB real de la capa 3.

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. Pero, 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.

VRF-lite utiliza las interfaces de entrada para distinguir las rutas para diversas redes virtuales y las tablas virtuales del reenvío de paquete de las formas asociando uno o más acodan 3 interfaces con cada VRF. Las interfaces en un VRF pueden ser cualquiera física, por ejemplo los accesos de Ethernet; o lógico, por ejemplo los subinterfaces, las interfaces del túnel o el VLA N SVI. Observe por favor una interfaz de la capa 3 no puede pertenecer a más de un VRF en cualquier momento.

Consideraciones importantes para VRF-Lite

- VRF-Lite está solamente localmente - significativo 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 los dominios de seguridad múltiples, y todos los dominios de seguridad tienen sus propias tablas de ruteo únicas.
- VRF-Lite deja los dominios de seguridad múltiples compartir el mismo vículo físico entre los dispositivos de red. Los puertos troncales con los VLAN múltiples o los túneles GRE proporcionan el aislamiento de tráfico que separa los paquetes de cada diverso dominio de seguridad.
- Todos los dominios de seguridad deben tener sus propios VLA N.
- VRF-lite no soporta todas las funciones MPLS-VRF: etiquete el intercambio, la adyacencia LDP, o los paquetes etiquetados.
- Comparten al Recurso TCAM de la capa 3 entre todos los VRF. Para asegurarse de que cualquier un VRF tenga suficiente espacio CAM, utilice el **comando maximum routes**.
- Un switch de Catalyst usando VRF-Lite puede soportar una red global y hasta 64 VRF. El número total de rutas soportadas es limitado por el tamaño del TCAM.
- La mayoría de los Routing Protocol (BGP, OSPF, EIGRP, RIP y Static Routing) se pueden utilizar entre los dispositivos que ejecutan VRF-Lite.
- No hay necesidad de ejecutar el BGP con VRF-Lite a menos que usted necesite escaparse las rutas entre los VRF.
- VRF-Lite no afecta a la tarifa de conmutación de conjunto de bits.
- El Multicast y VRF-Lite no se pueden configurar en la misma interfaz de la capa 3 al mismo tiempo.
- El submandato de VRF-**lite de la capacidad** bajo el **OSPF del router** debe ser utilizado cuando usted configura el OSPF como el Routing Protocol entre los dispositivos de red.

Definición de A VRF

En el ejemplo de diseño, los requisitos proporcionan el aislamiento de la trayectoria para el unauthenticated o los usuarios así como los INVITADOS SUCIOS. El resto del tráfico se permite para utilizar la red interna. Esto requiere la definición de dos VRF. Ésta es la configuración:

```
!
ip vrf DIRTY
!--- 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
10:1 !--- 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). ! ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS rd 30:1 !
```

Asocie un VLA N o interconecte con un VRF

Después de que el VRF se haya definido en el switch de la capa 3 o el router, las interfaces que participan en la configuración de VRF-Lite se deben asociar al VRF al cual pertenecen. Según lo mencionado anterior, la comprobación o las interfaces virtuales se puede asociar a un VRF. Incluidos son los ejemplos de una interfaz física, de un Switched Virtual Interface, de una sub-interfaz y de una interfaz del túnel que se asocian a un VRF.

```
!
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
!
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
!
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 VRF entre dos dispositivos

Hay varias metodologías aceptables para el extenion de un VRF entre dos pedazos de infraestructura. El método que usted elige se debe basar en este los criterios:

1. Capacidades de la plataforma — Con respecto a las capacidades de la plataforma, a todo el de Cisco 3 actuales soportes capaces VRF-Lite de la transferencia y de plataformas de ruteo de la empresa de la capa. Esto incluye pero no se limita 4500, 3750, y 3560 a las Plataformas del Catalyst 6500.
2. Cualquier plataforma de ruteo que ejecute el ® apropiado del Cisco IOS, que incluyen pero no se limitan a los 7600, 3800, 2800, 1800, y 800 Series ISR.
3. El número de la capa 3 salta entre los pedazos relevantes de infraestructura — determinar el número de saltos de la capa 3 es crítico mantener el despliegue tan simple como sea posible. Por ejemplo, si había cinco saltos de la capa 3 entre la infraestructura que reciben los dispositivos de CAS y a los clientes, puede crear el consumo de recursos gasto administrativo.

Con la solución incorrecta:

1. El enlace de la capa 2 crea una topología muy subóptima de la capa 2.
2. Los subinterfaces de la capa 3 crean muchas interfaces adicionales para configurar. Como consecuencia esto puede crear los problemas adicionales del IP Addressing de la tara de administración y del potencial. Esto se ilustra en el diagrama. Si usted asume que no hay Redundancia en la infraestructura, cada capa de la red mostrada tiene un ingreso y interfaz física de la salida. El cómputo para el número de subinterfaces es entonces (2 * número de gradas en la red * (número de VRF)). En este ejemplo hay dos VRF así que la fórmula es ((2*5)*2) o 20 subinterfaces. Una vez que la Redundancia se agrega este número más que dobla. Compare esto a la extensión GRE, donde solamente cuatro interfaces se requieren con el mismo resultado final. Esto ilustra llano cómo el GRE reduce dramáticamente el impacto de la configuración.

Enlace de la capa 2

El enlace de la capa 2 se prefiere en los escenarios donde los armarios de la capa 3 no se despliegan o donde los dispositivos de red no soportan el GRE o los subinterfaces. Debe ser observado que las 4500 Plataformas del Catalyst 3560, 3750 y no soportan los subinterfaces. El Catalyst 3560, y 3750 también no soportan el GRE. El Catalyst 4500 soporta el GRE en el software, y el Catalyst 6500 soporta el GRE en hardware.

En un armario de la capa 3 modelo donde usted conecta una plataforma que no soporte los subinterfaces o el GRE a una plataforma que lo haga, él se prefiere para utilizar solamente el enlace de la capa 2 en un lado, y para utilizar los subinterfaces en el otro lado. Esto permite que usted mantenga todas las ventajas de una arquitectura del armario de la capa 3, y todavía que supere la limitación de ningún GRE o soporte de la Sub-interfaz en algunas Plataformas. Una de las ventajas primarias de la configuración de un enlace de la capa 2 solamente en un lado del link es que el Spanning-tree no está introducido nuevamente dentro del entorno de la capa 3. Vea el ejemplo donde un switch de acceso 3750 (ningún soporte GRE o de la Sub-interfaz) está conectado con un switch de distribución 6500, que soporta el GRE y los subinterfaces.

Configuración pertinente 3750:

En esta configuración, observe que en el FastEthernet 1/0/1 de la configuración predeterminada para el VLAN NATIVO es VLAN1. Esta configuración no se ha cambiado. Usted también nota, sin embargo, que el VLAN1 no está permitido ser trunked a través del link. Los VLA N permitidos se limitan solamente al VLANS se marcan con etiqueta que. Porque en este Layer 3 Topology no hay necesidad de la negociación de tronco, o tráfico VTP de ir del Switch a conmutar, no hay tampoco necesidad del tráfico unencapsulated de transitar este link. Esta configuración aumenta la postura de seguridad de la arquitectura puesto que él doesn para no abrir a las brechas en la seguridad innecesarias de la capa 2.

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
!
interface FastEthernet1/0/1
description CONNECTION_TO_DISTRIBUTION_6504
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport mode trunk
speed 100
duplex full
!
!
interface Vlan10
description DIRTY_VRF_TRANSIT
ip vrf forwarding DIRTY
ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
description CLEAN_TRANSIT
ip address 192.168.20.2 255.255.255.252
!
```

```
interface Vlan30
description GUESTS_VRF_TRANSIT
ip vrf forwarding GUESTS
ip address 192.168.30.2 255.255.255.252
!
```

Configuración pertinente 6500:

En esta configuración, observe que la encapsulación del dot1q está utilizada y las tramas con el VLAN10, 20 y 30 se marcan con etiqueta. Cuando usted elige el VLA N marca con etiqueta para utilizar, usted no puede utilizar un número VLAN que se defina ya localmente en la base de datos de VLAN en el Switch.

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface FastEthernet3/1.20
description CLEAN_TRANSIT
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
description GUESTS_VRF_TRANSIT
encapsulation dot1Q 30
ip vrf forwarding GUESTS
ip address 192.168.30.1 255.255.255.252
!
```

Subinterfaces de la capa 3

Los subinterfaces de la capa 3 son una buena opción cuando usted necesita solamente ampliar el VRF sobre un salto de la capa 3 en la red. El GRE o los subinterfaces se puede elegir basó en su nivel de comodidad con cada configuración. Esto es una configuración de muestra para una Sub-interfaz de la capa 3:

```
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
```

```
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
```

Túneles GRE

Los túneles GRE son el método preferido para extender un VRF-Lite VRF cuando hay saltos de la capa múltiple 3 entre los clientes que necesitan acceder el VRF. Este tipo de diseño es más común con el NAC de la sucursal remota donde los clientes remotos quieren acceder un servidor centralmente localizado del NAC. Por ejemplo, en una base típica, la distribución, los clientes del modelo de red de acceso no está conectada directamente con las distribuciones o con la base. Por lo tanto, no hay necesidad de agregar la complejidad de la definición VRF en la distribución o los dispositivos del núcleo. El GRE se puede utilizar para transportar simplemente el tráfico que necesita ser aislado a la punta en la red donde los servidores del NAC están conectados. Éste es un ejemplo de una interfaz de túnel GRE.

```
!
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
!
```

Configurar la encaminamiento para el VRF

Según lo discutido anterior en el documento, VRF-Lite soporta el BGP, el OSPF, y el EIGRP. En este ejemplo de configuración, se elige el EIGRP porque es el Cisco recomendó típicamente el Routing Protocol implementado en las redes de oficinas centrales en donde se requiere la convergencia rápida.

Debe ser observado, los trabajos ese OSPF igualmente bien con VRF-Lite, al igual que BGP.

Debe también ser observado que si el diseño requiere que el tráfico sea escapado entre los VRF, después se requiere el BGP.

Éste es un ejemplo de la configuración de la encaminamiento para un VRF con el EIGRP.

```
!
!--- As with any configuration this is base routing
protocol !--- configuration which handles the routing
for the Global Routing Table. router eigrp 1 network
192.168.20.0 0.0.0.3 network 192.168.21.0 network
192.168.22.0 network 192.168.28.0 0.0.0.3 network
192.168.29.0 0.0.0.3 network 192.168.254.1 0.0.0.0 no
auto-summary ! !--- An Address Family must be defined
for each VRF !--- that is to be routing through the
routing protocol. !--- Routing Protocol options such as
auto-summarization, !--- autonomous system number,
router id, and so forth are all !--- configured under
```

```
the address family. Note that EIGRP does not !---
neighbor without the autonomous system specified under
!--- the address family. Also note, that this autonomous
system !--- number should be unique for each VRF and
should not be !--- the same as the Global AS number. !
address-family ipv4 vrf GUESTS network 192.168.30.0
0.0.0.3 network 192.168.38.0 0.0.0.3 no auto-summary
autonomous-system 30 exit-address-family ! address-
family ipv4 vrf DIRTY network 192.168.10.0 0.0.0.3
network 192.168.11.0 no auto-summary autonomous-system
10 exit-address-family !
```

Rutear el tráfico entre la tabla de Global Routing y el VRF sucio

Depende de los requisitos del despliegue del NAC si 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. En el caso de la sola muestra del Active Directory en las implementaciones, es necesario pasar un subconjunto de tráfico al Active Directory para permitir los inicios de sesión interactivos, intercambio del boleto del Kerberos, 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 esta metodología.

El VRF sucio omite la interfaz untrusted o sucia del dispositivo NAC. El global tiene Static rutas *solamente a las* subredes que se consideran el VLA N SUCIO.

Considere este gráfico.

El primer salto de la capa 3 en el lado untrusted o sucio del dispositivo NAC redistribuye una ruta predeterminado en el proceso de ruteo esas puntas al dispositivo NAC. El primer salto de la capa 3 en el lado de confianza o limpio del dispositivo NAC redistribuye una Static ruta para la subred que pertenece al VLAN 100, que en este caso es 192.168.100.0/24.

Nota: El primer salto de la capa 3 en los lados opuestos del dispositivo NAC puede estar en el mismo dispositivo físico, pero en diversos VRF. En el próximo ejemplo, sigue habiendo el lado untrusted o sucio del servidor del NAC está en un VRF, mientras que haber confiado en o limpia el lado del dispositivo NAC en la tabla de Global Routing.

La configuración es la siguiente:

```
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
```

```
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
ip classless
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
!!
```

Configuración de NAC para la capa 3 OOB

Configuración de CAS

Recuerde nuestro principio del número uno de la sección de la introducción: El truco a un diseño acertado del NAC es recordar siempre que tráfico clasificado como flujo sucio de la *necesidad* en el lado untrusted del servidor del NAC (CAS).

En la primera captura de pantalla, atención de la paga a la configuración de la red de servidores del NAC. Usted nota que el servidor está desplegado como gateway fuera de banda Real-IP. Observe que la ruta predeterminado del servidor del NAC está señalada al lado DE CONFIANZA.

El servidor necesita ser configurado con las Static rutas para cada uno del VLANS SUCIO que existen en el lado UNTRUSTED. Vea a la segunda captura de pantalla.

Verificación

Encuentre el proceso documentado del registro del NAC-`empleado del` usuario en nuestra red. Cisco ha capturado la actividad del switch de acceso, el puesto de trabajo, y muestra la información de las tablas de ruteo de los switches de distribución.

Use esta sección para confirmar que su configuración funciona correctamente.

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

Etapa 1 — Usted no ha conectado con la red todavía, y el switchport en el switch de acceso está abajo.

```
! – Catalyst 3750 Access Switch
!--- Note: Client mahcine is off the network at this
point. ! 3750-Access#show int status | i Fa1/0/13
Fa1/0/13 CLIENT_CONNECTION notconnect 100 auto auto
10/100BaseTX ! ! 3750-Access#!Notice it is in the
"notconnect" state. !
```

Etapa 2 — El cliente de Windows conecta en la red, y el VLA N inicial en el Switch es VLAN 100

(el VLA N sucio). Una dirección IP se asigna al host, como usted puede ver en esta captura de pantalla.

```
! – Catalyst 3750 Access Switch
!--- Note: Client just connected to the network. 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100,
changed state to up 2w5d: %LINK-3-UPDOWN: Interface
FastEthernet1/0/13, changed state to up 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/13, changed state to up ! ! 3750-
Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 100 a-full a-100
10/100BaseTX !
```

Etapa 3 — Dentro de algunos segundos, el agente del NAC comienza su proceso del inicio. En este ejemplo, el Active Directory Solo-Muestra-en se configura, así que le no indican para un nombre de usuario y contraseña. En lugar, usted ve que ocurre una ventana emergente que describe eso Solo-Muestra-en.

Después de la autenticación y de la postura se ha completado la evaluación, se visualiza un Mensaje de éxito, el switchport se mueve desde el VLA N sucio al VLA N del empleado y a los refreshs del agente del NAC la dirección IP del PC.

```
! – Catalyst 3750 Access Switch
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan100, changed state to down
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan200, changed state to up
!
!--- Note: As you can tell from the previous messages,
!--- the switchport was just moved from VLAN 100 to VLAN
200. ! 3750-Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 200 a-full a-100
10/100BaseTX ! !
```

Esta captura de pantalla muestra la dirección IP final, que está en el VLA N del empleado (VLA N 200).

Esta captura de pantalla muestra el dispositivo del usuario del NAC-empleado como se lista en la lista de dispositivos certificada. El papel se asigna a los *EMPLEADOS* y el VLA N es 200.

Esta captura de pantalla muestra la lista de usuarios en línea en el administrador del NAC.

Éste es el registro de acontecimientos del administrador del NAC, que muestra la registración satisfactoria del usuario fuera de banda.

En esta sección, las tablas de ruteo de la tabla de ruta global y el VRF SUCIO se examinan. En la primera captura de pantalla, observe el **comando show ip route**. Esto indica que usted ve la tabla de ruteo para las rutas globales.

```
6504-DISTRIBUTION#show ip route Codes: C - connected, S
- static, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1
- OSPF external type 1, E2 - OSPF external type 2 i -
IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-
IS level-2 ia - IS-IS inter area, * - candidate default,
```

```
U - per-user static route o - ODR, P - periodic
downloaded static route Gateway of last resort is
192.168.28.2 to network 0.0.0.0 192.168.29.0/30 is
subnetted, 1 subnets D 192.168.29.0 [90/30720] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.28.0/30 is
subnetted, 1 subnets C 192.168.28.0 is directly
connected, FastEthernet3/48 D EX 192.168.31.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 D
EX 192.168.30.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D 192.168.200.0/24 [90/28416] via
192.168.20.2, 6d19h, FastEthernet3/1.20 D EX
192.168.38.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 C 192.168.21.0/24 is directly
connected, Vlan21 D EX 192.168.39.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.20.0/30 is
subnetted, 1 subnets C 192.168.20.0 is directly
connected, FastEthernet3/1.20 D EX 192.168.36.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.22.0/24 is directly connected, Vlan22 D EX
192.168.37.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.34.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.254.0/32 is
subnetted, 3 subnets D 192.168.254.2 [90/156160] via
192.168.20.2, 2w5d, FastEthernet3/1.20 D 192.168.254.3
[90/156160] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.254.1 is directly connected, Loopback0 D EX
192.168.35.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.32.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 S 192.168.100.0/24
[1/0] via 192.168.21.10 D EX 192.168.33.0/24 [170/30976]
via 192.168.28.2, 2w5d, FastEthernet3/48 D*EX 0.0.0.0/0
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48
```

Nota: La red 192.168.100.0/24 (la red sucia) está en la tabla de ruteo como Static ruta, con el Next-Hop siendo la interfaz de confianza del servidor del NAC.

Observe el comando **SUCIO del vrf de la ruta de IP de la demostración**. Esto indica que usted ve la tabla de ruteo para la red virtual SUCIA solamente.

```
6504-DISTRIBUTION#show ip route vrf DIRTY Routing Table:
DIRTY Codes: C - connected, S - static, R - RIP, M -
mobile, B - BGP D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area N1 - OSPF NSSA external type
1, N2 - OSPF NSSA external type 2 E1 - OSPF external
type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS
summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-
IS inter area, * - candidate default, U - per-user
static route o - ODR, P - periodic downloaded static
route Gateway of last resort is 192.168.11.2 to network
0.0.0.0 192.168.10.0/30 is subnetted, 1 subnets C
192.168.10.0 is directly connected, FastEthernet3/1.10 C
192.168.11.0/24 is directly connected, Vlan11 D
192.168.100.0/24 [90/28416] via 192.168.10.2, 01:03:19,
FastEthernet3/1.10 S* 0.0.0.0/0 [1/0] via 192.168.11.2
```

Nota: Observe el VLA N sucio del acceso (192.168.100.0/24) se aprende en la distribución con el EIGRP del switch de acceso 3750, solamente en la tabla de ruteo SUCIA VRF. Esta ruta no existe en la tabla global.

Apéndice A: Configuraciones del switch

Configuración corriente del switch de acceso

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3750-Access
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
!
!
crypto pki trustpoint TP-self-signed-819048320
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-819048320
 revocation-check none
 rsakeypair TP-self-signed-819048320
!
!
crypto ca certificate chain TP-self-signed-819048320
 certificate self-signed 01
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Loopback0
 ip address 192.168.254.2 255.255.255.255
!

!
interface FastEthernet1/0/1
 description CONNECTION_TO_DISTRIBUTION_6504
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 speed 100
 duplex full
!
interface range FastEthernet1/0/2 - 24
 description CLIENT_CONNECTION
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
!- SNIP -
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description DIRTY_VRF_TRANSMIT
 ip vrf forwarding DIRTY
 ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
 description CLEAN_TRANSIT
 ip address 192.168.20.2 255.255.255.252
!
interface Vlan30
 description GUESTS_TRANSIT
 ip vrf forwarding GUESTS
 ip address 192.168.30.2 255.255.255.252
!
interface Vlan100
 description DIRTY_VLAN
 ip vrf forwarding DIRTY
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan200
 description EMPLOYEES_VLAN
 ip address 192.168.200.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan210
 description CONTRACTORS_VLAN
 ip address 192.168.210.1 255.255.255.0
 ip helper-address 192.168.22.11
!

!
interface Vlan300
 description GUESTS
 ip vrf forwarding GUESTS
 ip address 192.168.31.1 255.255.255.0
!
router eigrp 1
 network 192.168.20.0 0.0.0.3
 network 192.168.200.0
 network 192.168.254.2 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
 network 192.168.30.0 0.0.0.3
 network 192.168.31.0
 no auto-summary
 autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
 network 192.168.10.0 0.0.0.3
 network 192.168.100.0
 no auto-summary
 autonomous-system 10
 exit-address-family
!
```

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip http server
ip http secure-server
!
!
snmp-server community NIC-NAC-PADDYWHACK RW
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v1
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v2c
snmp-server trap-source Loopback0
snmp-server host 192.168.22.5 version 2c NIC-NAC-
PADDYWHACK
!
!- SNIP
!
ntp clock-period 36028450
ntp source Loopback0
ntp server 192.168.254.1 version 2 prefer
end
```

Configuración corriente del switch de distribución

```
!– SNIP -
!
hostname 6504-DISTRIBUTION
!
boot-start-marker
boot system disk0:s72033-advipservicesk9_wan-mz.122-
33.SXH2a.bin
boot-end-marker
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
!
!- SNIP -
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
ipv6 mfib hardware-switching replication-mode ingress
vtp domain cmpd
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
no mls flow ip
no mls flow ipv6
```

```
mls cef error action freeze
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!

!
vlan 11
 name CAS_DIRTY
!
vlan 21
 name CAS_CLEAN
!
vlan 22
 name SERVER_VLAN
!
interface Tunnel0
 ip vrf forwarding GUESTS
 ip address 192.168.38.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 192.168.254.3
!
interface Loopback0
 ip address 192.168.254.1 255.255.255.255
!
!- SNIP -
!
interface FastEthernet3/1
 description CONNECTION_TO_3750_ACCESS
 no ip address
 speed 100
 duplex full
!
interface FastEthernet3/1.10
 description DIRTY_VRF_TRANSIT
 encapsulation dot1Q 10
 ip vrf forwarding DIRTY
 ip address 192.168.10.1 255.255.255.252
 ip verify unicast source reachable-via rx allow-default
!
interface FastEthernet3/1.20
 description CLEAN_TRANSIT
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
 description GUESTS_TRANSIT
 encapsulation dot1Q 30
 ip vrf forwarding GUESTS
 ip address 192.168.30.1 255.255.255.252
```

```
!
!
!
!

!
interface FastEthernet3/2
 description CAS1_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/3
 description CAS2_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/4
 description CAS1_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/5
 description CAS2_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/6
 description CAM
 switchport
 switchport access vlan 22
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!
!- SNIP -
!
!

!
interface FastEthernet3/48
 description CONNECTION_TO_THE_WORLD
```

```
 ip address 192.168.28.1 255.255.255.252
 speed 100
 duplex full
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan11
 description NAC_DIRTY
 ip vrf forwarding DIRTY
 ip address 192.168.11.1 255.255.255.0
!
interface Vlan21
 description NAC_CLEAN
 ip address 192.168.21.1 255.255.255.0
!
interface Vlan22
 description SERVER_VLAN
 ip address 192.168.22.1 255.255.255.0
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
!
!
!
!

!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
```

```
!
!
!- SNIP -
!
ntp source Loopback0
ntp master 2
!
end
```

Troubleshooting

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems