Configurar el registro integrado URL y la información del tráfico del invitado en una red de Cisco

Contenido

Introducción

Este documento describe cómo integrar un NAC Guest Server (NGS) con Controladores de LAN Inalámbricos (WLC) y un Adaptive Security Appliance (ASA) para proporcionar el registro de URL e información del tráfico del invitado. Muchas compañías necesitan monitorear el tráfico del invitado y este documento provee información sobre cómo configurar los componentes de Cisco para cumplir ese requisito.

Observe que hay soluciones de Cisco múltiples para configurar el acceso de invitado en una red de Cisco. Este artículo se centra en el método que utiliza el WLC como la tecnología que habilita. El WLC tiene la capacidad única al tráfico de túnel del borde de la red a Internet con EoIP. Esta característica elimina la necesidad de desplegar los VPN o los ACL dentro de la infraestructura de red para restringir el tráfico del invitado de escaparse en la red interna de la compañía.

El bulto de este artículo cubre “integró el registro y la información URL” en una red del

“Tecnología inalámbrica-invitado”, pero esta característica se puede configurar en una red del “atar con alambre-invitado”, también. El Apéndice A proporciona los detalles para una red del “atar con alambre-invitado”.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- ASA que funciona con la versión 8.0.4.24 o posterior
- Dos reguladores de la serie del WLC-4400 que funcionan con la versión 4.2.130 o posterior
- Servidor del invitado del NAC que funciona con la versión 2.0 o posterior

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA que funcionamientos 8.0.4.26
- Dos reguladores del WLC-44xx que funcionan con el código 4.2.130
- Servidor del invitado del NAC que funciona con el código 2.0.0
- Catalyst 6500

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

El acceso de invitado inalámbrico proporciona a los beneficios comerciales significativos a los clientes. Estas ventajas incluyen los costos de funcionamiento reducidos, productividad mejorada, y Administración y aprovisionamiento simplificados del acceso de invitado. Además, el servidor del invitado del NAC permite a los clientes para visualizar su Acceptable Use Policy y para requerir la aceptación de esta directiva antes de conceder el acceso a Internet. Ahora, con la adición del registro integrado URL y de la información, los clientes pueden registrar el uso del invitado y la conformidad de la pista contra su Acceptable Use Policy.

Configurar

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

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Topología de laboratorio del Tecnología inalámbrica-invitado

El Catalyst 6500 se utiliza para simular la red para empresas. El invitado SSID, mostrado en el rojo, asocia al VLAN nativo en el ASA, también mostrado en el rojo. Flujos de tráfico del invitado del PC en el Punto de acceso, a través del túnel del LWAPP al regulador no nativo del WLC, y entonces a través del túnel de EoIP al regulador del ancla del WLC. El regulador del ancla proporciona el DHCP y los servicios de autenticación para la red del invitado. El servicio del DHCP proporciona al invitado con una dirección IP, un default gateway, y un servidor DNS. El default gateway es el ASA, y el servidor DNS es un servidor público situado en Internet. El servicio de autenticación en el regulador del ancla comunica con los NG con el RADIUS para autenticar a los usuarios contra la base de datos de Usuario invitado en los NG. Se inicia el inicio del invitado cuando el invitado abre a un buscador Web, y el regulador del ancla reorienta el tráfico a la página de la autenticación. Todo el tráfico dentro y fuera de la subred del invitado se filtra con el ASA para el control de políticas y auditoría.

Registro integrado URL del ASA a los NG

Se activa el registro integrado URL cuando usted habilita éstos:

- Estadísticas RADIUS del regulador del ancla del WLC a los NG
- Registro de las peticiones get HTTP en el ASA
- Envío de los mensajes de Syslog del ASA a los NG

Las estadísticas RADIUS proporcionan los NG con una asignación entre la dirección IP del invitado y la identificación del usuario del invitado por un período específico. El registro de las peticiones get HTTP proporciona los NG con un registro de qué URL fue visitado por la dirección IP del invitado a que hora. Los NG pueden entonces correlacionar esta información para producir un informe que muestre los URL visitados por un invitado determinado por un período de tiempo determinado.

Observe que el tiempo preciso está requerido para que esta correlación trabaje correctamente. Por este motivo, la configuración de los servidores NTP se recomienda altamente en el ASA, el WLC, y los NG.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración ASA
- Configuración del WLC
- Configuración NG

Configuración ASA

Las tareas de configuración dominantes en el ASA incluyen éstos:

- NTP
- Examen HTTP
- Syslog

El NTP es requerido para asegurar la correlación apropiada de los mensajes por los NG. El examen HTTP habilita el registro URL. El Syslog es el método usado para enviar los registros URL a los NG.

En este ejemplo, se utiliza este comando de habilitar el NTP en el ASA:

```
ntp server 192.168.215.62
```

El examen HTTP permite al ASA para registrar los URL. Específicamente, el comando **HTTP de la inspección** habilita o inhabilita el registro de la petición get con el mensaje de Syslog 304001.

El comando **HTTP de la inspección** se pone bajo un clase-mapa dentro de un directiva-mapa. Cuando está habilitado con el **comando service-policy**, peticiones get de los registros de examen HTTP con el mensaje de Syslog 304001. El código se requiere 8.0.4.24 ASA o más adelante para el mensaje de Syslog 304001 para mostrar el nombre de host como parte del URL.

En este ejemplo, éstos son los comandos relevant:

```
policy-map global_policy
 class inspection_default
  inspect http
!
service-policy global_policy global
```

El Syslog es el método usado para comunicar el URL que registra a los NG. En esta configuración, solamente el mensaje de Syslog 304001 se envía a los NG con esta configuración:

```
logging enable
logging timestamp
logging list WebLogging message 304001
logging trap WebLogging
logging facility 21
logging host inside 192.168.215.16
```

Configuración del WLC

Los pasos para la configuración dominantes para los reguladores del Wireless LAN incluyen éstos:

- Acceso de invitado básico
- NTP
- Contabilización RADIUS

La configuración básica del acceso del invitado implica la configuración de un regulador no nativo del regulador del WLC y del ancla del WLC de modo que el tráfico del invitado sea tunneled a través de la red para empresas al Internet DMZ. La configuración del acceso de invitado básico se cubre en la documentación separada. Los ejemplos que muestran la configuración para la configuración se cubren en el apéndice.

Agregan a los servidores NTP en la pantalla Controller/NTP.

Configuración del NTP en el WLC

Requieren a un servidor de contabilidad RADIUS de modo que el servidor NG pueda asociar la dirección IP de origen recibida en los mensajes de Syslog ASA al invitado que utiliza ese direccionamiento en ese tiempo determinado.

Estas dos pantallas muestran la configuración de la autenticación de RADIUS y de las estadísticas RADIUS en el regulador del ancla del WLC. La configuración de RADIUS no se requiere en el regulador no nativo.

Autenticación RADIUS Estadísticas RADIUS

Configuración NG

- NTP
- Clientes RADIUS
- Syslog

El servidor NG se configura de la página web de https://(ip_address)/admin. El nombre de usuario/contraseña predeterminado es admin/admin.

Agregan a los servidores NTP en la pantalla del servidor/de las Fecha-Tiempo-configuraciones. Se recomienda que el timezone del sistema esté fijado al timezone donde el servidor se localiza físicamente. Cuando se sincroniza el NTP, usted ve un mensaje en la parte inferior de esta pantalla que diga, “estatus: Servidores NTP activos” junto con la dirección IP que muestra “la fuente de la hora actual.”

Configuración del NTP NG

El servidor NG necesita ser configurado con la dirección IP del regulador del ancla como cliente RADIUS. Esta pantalla está situada en la página Devices/RADIUS-Clients. Aseegurese que el secreto compartido es lo mismo que fue ingresado en el regulador del ancla. Haga clic el **botón Restart Button** después de que usted realice los cambios para recomenzar el servicio RADIUS en el servidor NG.

Clientes RADIUS

Por abandono, el servidor NG valida los mensajes de Syslog de cualquier dirección IP. Como consecuencia, no hay pasos adicionales requeridos para recibir los mensajes de Syslog del ASA.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

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

Siga los siguientes pasos para verificar que el registro URL trabaja correctamente.

1. Del PC del cliente, conecte con la red del invitado inalámbrica. El PC recibe una dirección IP, un default gateway, y a un servidor DNS del servidor DHCP en el regulador del ancla.
2. Abra a un buscador Web. Le reorientan a una pantalla de inicio de sesión. Ingrese un nombre de usuario y contraseña del invitado. Sobre la autenticación satisfactoria, le reorientan a una página predeterminada en Internet.
3. Hojee a las diversas páginas web en Internet.
4. Conecte una Administración PC con los NG en https://(ip_address) y inicie sesión como

patrocinador.

5. Haga clic la **administración de cuentas**. Usted ve una lista de cuentas de invitado. (Si su cuenta de invitado no aparece, haga clic el botón de la **búsqueda avanzada** y borre el filtro que especifica que este patrocinador puede ver solamente las cuentas que crearon.)
6. Encuentre la cuenta de Usuario invitado de la lista. Navegue a la derecha hasta que usted vea el icono de los detalles. Haga clic el icono de los **detalles**.
7. Haga clic la lengueta del **registro de actividad**. Usted ve una lista de los URL que el invitado visitó.**Informe del registro URL para el usuario**

El informe muestra que el Usuario invitado visitó http://www.cisco.com el 1 de abril de 2009 en 2:51 PM. La dirección del dispositivo de 192.168.59.49 es la dirección IP del ASA que envió el mensaje de Syslog que contenía el registro URL. La dirección IP de origen para los Usuarios invitados es 192.168.0.10. La dirección destino es 192.168.219.25 para http://www.cisco.com.

Apéndices

Apéndice A – Opción del Atar con alambre-invitado

Hasta esta punta, este artículo ha cubierto “registro integrado URL e información del tráfico del invitado” para el uso en una red del “Tecnología inalámbrica-invitado”. Esta sección proporciona los detalles para configurar a un “atar con alambre-invitado,” también. los Atar con alambre-invitados y los Tecnología inalámbrica-invitados pueden ser habilitados en el mismo regulador no nativo del WLC.

Éste es el diagrama de la red para el laboratorio de la red del Atar con alambre-invitado.

Topología de laboratorio del Atar con alambre-invitado

La Topología de laboratorio del atar con alambre-invitado es similar a la Topología de laboratorio del Tecnología inalámbrica-invitado, mostrada anterior, a excepción de la adición de un VLA N del atar con alambre-invitado. El VLA N del atar con alambre-invitado, mostrado en el rojo, es una conexión de la capa 2 entre el atar con alambre-invitado PC y el regulador no nativo del WLC. El tráfico del atar con alambre-invitado es recibido por el regulador no nativo del WLC y enviado por EoIP al regulador del ancla del WLC. El regulador del ancla del WLC proporciona el DHCP y los servicios de autenticación para el usuario del atar con alambre-invitado proporcionó de la misma manera estos servicios para el usuario del Tecnología inalámbrica-invitado. El default gateway es el ASA, y el servidor DNS es un servidor público en Internet. Lógicamente, todo el tráfico dentro y fuera de la subred es protegido por el ASA.

Se recomienda para no configurar una interfaz de la capa 3 en el VLA N del Atar con alambre-invitado puesto que éste puede permitir a una punta del saltar para que el tráfico se escape el VLA N del atar con alambre-invitado de los en la red corporativa.

Apéndice B – Configuraciones detalladas para el WLCs

Regulador del ancla del WLC

Interfaces del regulador del ancla

La configuración de las interfaces en el regulador del ancla se muestra:

El ap-administrador y las interfaces de administración están en el VLAN nativo del puerto físico 1

del WLC. El puerto 1 conecta con el switch de Catalyst y recibe el tráfico de la red del cliente. El tráfico del invitado se recibe a través del túnel de EoIP del regulador no nativo y termina a través de este puerto.

La interfaz del invitado está en el VLAN nativo del puerto 2, y la interfaz atada con alambre está en el VLA N 9 del puerto 2 del puerto 2. conecta con el ASA y se utiliza para mandar el tráfico a Internet.

Grupos de movilidad del regulador del ancla

Por este ejemplo, configuran a un grupo de la movilidad para el regulador no nativo (atado con alambre) y un grupo separado de la movilidad para el regulador del ancla (ancla). La configuración en el regulador del ancla se muestra.

Regulador WLAN del ancla

Regulador del ancla - Fije el ancla para la red inalámbrica (WLAN) del invitado

Para configurar o mostrar las anclas de la movilidad para una red inalámbrica (WLAN), mueva su ratón a la flecha desplegable en la derecha, y elija las **anclas de la movilidad**, como se muestra.

Regulador del ancla - Fije el ancla a sí mismo Regulador del ancla - red inalámbrica (WLAN) para los usuarios del Tecnología inalámbrica-invitado Regulador del ancla - red inalámbrica (WLAN) para los usuarios del atar con alambre-invitado (opcionales) Regulador del ancla - Alcances de DHCP Regulador del ancla - Alcance de DHCP para los Tecnología inalámbrica-invitados: Regulador del ancla - DHCP para los Atar con alambre-invitados (opcionales):

Regulador no nativo del WLC

Interfaces

La configuración de las interfaces en el regulador no nativo se muestra.

El ap-administrador y las interfaces de administración están en el VLAN nativo del puerto físico 1 del WLC.

La interfaz atada con alambre es *opcional* y se requiere solamente si usted quiere proporcionar el acceso del atar con alambre-invitado. La interfaz atada con alambre está en el VLA N 8 del puerto físico 1. Esta interfaz recibe el tráfico del VLA N del invitado del switch de Catalyst y le manda el túnel de EoIP, con el VLAN nativo, al regulador del ancla.

Regulador no nativo - Grupos de movilidad

La configuración en el regulador no nativo se muestra.

Regulador no nativo - WLAN

Para configurar o mostrar las anclas de la movilidad para una red inalámbrica (WLAN), mueven su ratón sobre la flecha desplegable en la derecha y eligen las **anclas de la movilidad**, como se muestra.

Ancla de la movilidad fijada para asegurar el regulador Regulador no nativo - red inalámbrica (WLAN) del invitado para los usuarios del Tecnología inalámbrica-invitado

s

Regulador no nativo - red inalámbrica (WLAN) para los usuarios del Atar con alambre-invitado (opcionales) – continuado

C del apéndice – Configuración ASA

```
ASA-5520# show run
:
ASA Version 8.0(4)26
!
hostname ASA-5520
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.59.49 255.255.255.240
!
interface GigabitEthernet0/2
   <- Guest traffic enters this interface
 nameif wireless_guest
 security-level 50
 ip address 192.168.0.254 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.99.1 255.255.255.0
 management-only
!
boot system disk0:/asa804-26-k8.bin
clock timezone CST -6
clock summer-time CDT recurring
logging enable
logging timestamp
   <- provide a timestamp in each syslog message
logging list WebLogging message 304001
   <- list includes URL Log message (304001)
logging console errors
logging buffered notifications
logging trap WebLogging
   <- Send this list of Log messages to syslog servers
logging asdm informational
logging facility 21
logging host inside 192.168.215.16
   <- NGS is the syslog server
asdm image disk0:/asdm-61551.bin
route inside 10.10.10.0 255.255.255.0 192.168.59.62 1
route inside 192.168.215.0 255.255.255.0 192.168.59.62 1
route inside 198.168.1.15 255.255.255.255 192.168.59.62 1
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.99.0 255.255.255.0 management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 198.168.1.15 <- Configure ntp server
!
class-map inspection_default
```

```
 match default-inspection-traffic
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect http
   <- Enable http inspection on the global policy
!
service-policy global_policy global
   <- Apply the policy
prompt hostname context
Cryptochecksum:b43ff809eacf50f0c9ef0ae2a9abbc1d
: end
```

Información Relacionada

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