Depuración del Flujo de Llamada de un Gateway de Internet SSG configurado con DHCP Secure ARP, SSG Port-Bundle Host Key, SSG TCP Redirect, SESM y SSG/DHCP Awareness

Contenido

Introducción

El foco de este documento es una gateway de Internet IOS que ejecuta SSG y DHCP con SESM para los servicios del portal.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Descripción general de la tecnología y las funciones

Gateway de selección de servicio (SSG)

Service Selection Gateway (SSG) es una solución de switching para proveedores de servicios que ofrecen conexiones de intranet, extranet e Internet a suscriptores con tecnología de acceso de banda ancha, como líneas de suscriptor digital (DSL), cablemódems o inalámbricas para permitir el acceso simultáneo a los servicios de red.

SSG funciona junto con Cisco Subscriber Edge Services Manager (SESM). Junto con el SESM, SSG proporciona autenticación de suscriptores, selección de servicios y capacidades de conexión de servicio a los suscriptores de servicios de Internet. Los suscriptores interactúan con una aplicación web SESM utilizando un navegador de Internet estándar.

El SESM funciona en dos modos:

- Modo RADIUS: este modo obtiene la información del suscriptor y del servicio de un servidor RADIUS. SESM en modo RADIUS es similar a SSD.
- Modo LDAP: el modo LDAP (protocolo ligero de acceso a directorios) proporciona acceso a un directorio compatible con LDAP para información de perfil de servicio y suscriptor. Este modo también cuenta con funcionalidad mejorada para las aplicaciones web SESM y utiliza un modelo de control de acceso basado en roles (RBAC) para gestionar el acceso de los suscriptores.

SSG Port Bundle Host Key

La función SSG Port-Bundle Host Key mejora la comunicación y funcionalidad entre SSG y SESM con un mecanismo que utiliza la dirección IP de origen del host y el puerto de origen para identificar y monitorear suscriptores.

Con la función SSG Port-Bundle Host Key, SSG realiza la traducción de direcciones de puerto (PAT) y la traducción de direcciones de red (NAT) en el tráfico HTTP entre el suscriptor y el servidor SESM. Cuando un suscriptor envía un paquete HTTP al servidor SESM, SSG crea un mapa de puerto que cambia la dirección IP de origen a una dirección IP de origen SSG configurada y cambia el puerto TCP de origen a un puerto asignado por SSG. SSG asigna un paquete de puertos a cada suscriptor porque un suscriptor puede tener varias sesiones TCP simultáneas cuando accede a una página web. La clave de host asignada, o combinación de conjunto de puertos y dirección IP de origen SSG, identifica de forma exclusiva a cada suscriptor. La clave de host se transporta en paquetes RADIUS enviados entre el servidor SESM y SSG en el atributo específico del proveedor de IP del suscriptor (VSA). Cuando el servidor SESM envía una respuesta al suscriptor, SSG traduce la dirección IP de destino y el puerto TCP de destino de acuerdo con el mapa de puerto.

Redirección TCP SSG para usuarios no autenticados

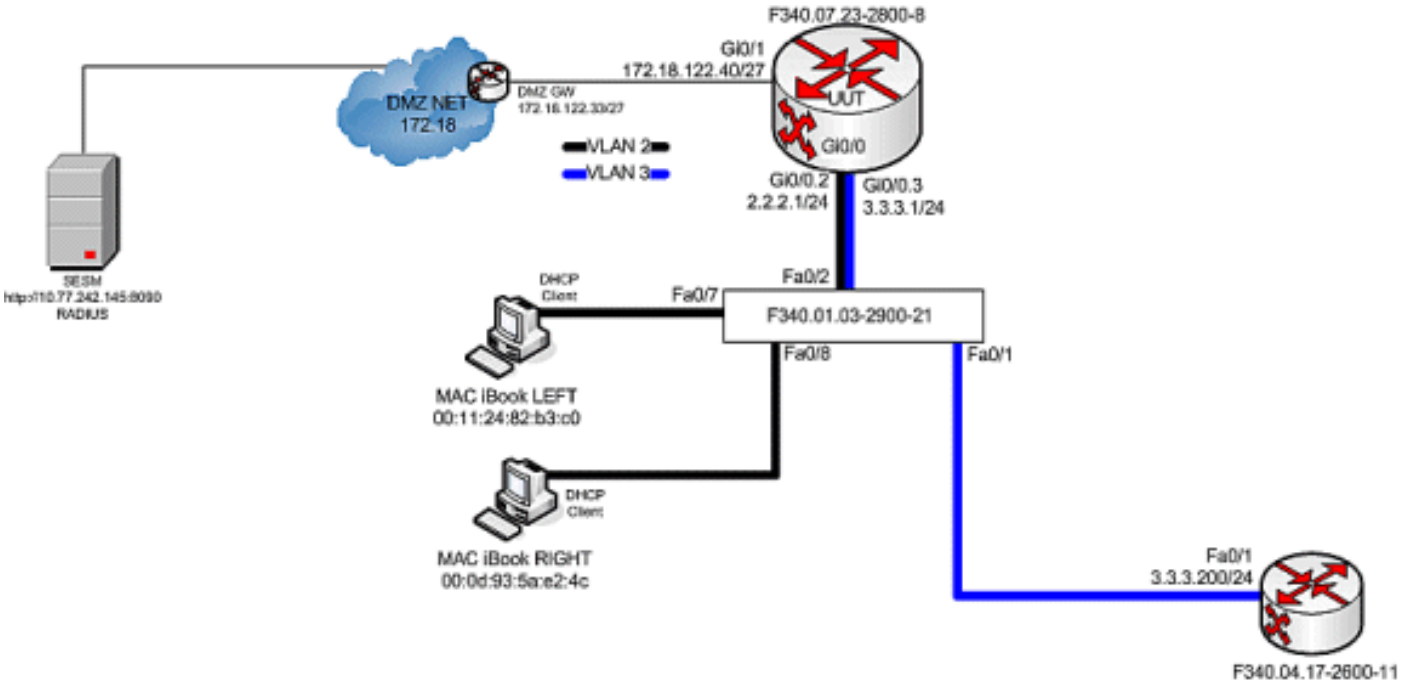
La redirección para usuarios no autenticados redirige los paquetes de un usuario si éste no ha autorizado con el proveedor de servicios. Cuando un suscriptor no autorizado intenta conectarse a un servicio en un puerto TCP (por ejemplo, a www.cisco.com), SSG TCP Redirect redirige el paquete al portal cautivo (SESM o un grupo de dispositivos SESM). SESM emite una redirección al explorador para mostrar la página de inicio de sesión. El suscriptor inicia sesión en SESM y se

autentica y autoriza. A continuación, SESM presenta al suscriptor una página de inicio personalizada, la página de inicio del proveedor de servicios o la URL original.

DHCP Secured IP Address Assignment

La función DHCP Secure IP Address Assignment introduce la capacidad de proteger las entradas de la tabla ARP a los arrendamientos de protocolo de configuración dinámica de host (DHCP) en la base de datos DHCP. Esta función protege y sincroniza la dirección MAC del cliente con el enlace DHCP, impidiendo que clientes no autorizados o hackers suplanten el servidor DHCP y se apropien de un arrendamiento DHCP de un cliente autorizado. Cuando se habilita esta función y el servidor DHCP asigna una dirección IP al cliente DHCP, el servidor DHCP agrega una entrada ARP segura a la tabla ARP con la dirección IP asignada y la dirección MAC del cliente. Esta entrada ARP no puede ser actualizada por ningún otro paquete ARP dinámico, y esta entrada ARP existe en la tabla ARP para el tiempo de arrendamiento configurado o mientras el arrendamiento esté activo. La entrada ARP segura sólo se puede eliminar mediante un mensaje de terminación explícito del cliente DHCP o del servidor DHCP cuando vence el enlace DHCP. Esta función se puede configurar para una nueva red DHCP o se puede utilizar para actualizar la seguridad de una red actual. La configuración de esta función no interrumpe el servicio y no es visible para el cliente DHCP.

Diagrama probado



Depuración de flujo de llamada

Complete estos pasos:

1. Cuando MAC iBook LEFT conecta por primera vez el cable Ethernet a esta red, alquila la dirección IP 2.2.2.5/29 del servidor DHCP del IOS que se ejecuta en "F340.07.23-2800-8".

```
debug ip dhcp server packet
debug ssg dhcp events

*Oct 13 20:24:04.073: SSG-DHCP-EVN: DHCP-DISCOVER event received.
```

```
   SSG-dhcp awareness feature enabled
*Oct 13 20:24:04.073: DHCPD: DHCPDISCOVER received from client
   0100.1124.82b3.c0 on interface GigabitEthernet0/0.2.
*Oct 13 20:24:04.073: SSG-DHCP-EVN: Get pool name called for
   0011.2482.b3c0. No hostobject
*Oct 13 20:24:04.073: SSG-DHCP-EVN: Get pool class called,
   class name = Oct 13 20:24:04.073: DHCPD: Sending DHCPOFFER
   to client 0100.1124.82b3.c0 (2.2.2.5).
*Oct 13 20:24:04.073: DHCPD: creating ARP entry
   (2.2.2.5, 0011.2482.b3c0).
*Oct 13 20:24:04.073: DHCPD: unicasting BOOTREPLY to client
   0011.2482.b3c0 (2.2.2.5).
*Oct 13 20:24:05.073:
   DHCPD: DHCPREQUEST received from client 0100.1124.82b3.c0.
*Oct 13 20:24:05.073:
   SSG-DHCP-EVN:2.2.2.5: IP address notification received.
*Oct 13 20:24:05.073:
   SSG-DHCP-EVN:2.2.2.5: HostObject not present
*Oct 13 20:24:05.073:
   DHCPD: Can't find any hostname to update
*Oct 13 20:24:05.073:
   DHCPD: Sending DHCPACK to client 0100.1124.82b3.c0 (2.2.2.5).
*Oct 13 20:24:05.073:
   DHCPD: creating ARP entry (2.2.2.5, 0011.2482.b3c0).
*Oct 13 20:24:05.073:
   DHCPD: unicasting BOOTREPLY to client 0011.2482.b3c0 (2.2.2.5).

F340.07.23-2800-8#show ip dhcp binding
 Bindings from all pools not associated with VRF:
  IP address Client-ID/          Lease expiration        Type
             Hardware address/
             User name
 2.2.2.5     0100.1124.82b3.c0  Oct 13 2008 08:37 PM    Automatic
```

2. Después de arrendar correctamente la dirección IP 2.2.2.5, MAC iBook LEFT abre un navegador web y lo señala a **http://3.3.3.200**, que se utiliza para simular recursos protegidos vinculados a "distlearn" del servicio SSG. El servicio SSG "distlearn" se define localmente en el router SSG "F340.07.23-2800-8":

```
local-profile distlearn
  attribute 26 9 251 "R3.3.3.200;255.255.255.255"
```

   En realidad, **http://3.3.3.200** es un router Cisco IOS configurado para "ip http server" y escucha en TCP 80, por lo que es básicamente un servidor web.Después de que el MAC iBook LEFT intente navegar a **http://3.3.3.200**, ya que esta conexión está ingresando en una interfaz configurada con "ssg direction downlink", el router SSG primero verifica la existencia de un SSG Host Object activo para la dirección IP de origen de la solicitud HTTP. Debido a que esta es la primera solicitud de este tipo desde la dirección IP 2.2.2.5, no existe un objeto host SSG y se crea una instancia de una redirección TCP hacia SESM para el host 2.2.2.5 a través de esta configuración:

```
ssg tcp-redirect
 port-list ports
  port 80
  port 8080
  port 8090
  port 443
All hosts with destination requests on these TCP Ports are candidates for redirection.
 server-group ssg_tr_unauth
```

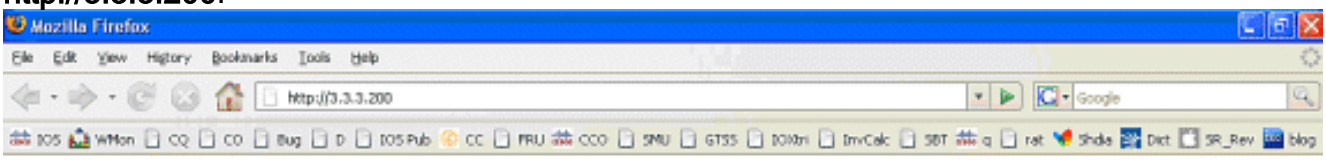
server 10.77.242.145 8090
10.77.242.145 is the SESM server and it's listening for HTTP on TCP 8090. "server" MUST be in default network or open-garden. **redirect port-list ports to ssg_tr_unauth**
redirect unauthenticated-user to ssg_tr_unauth
If an SSG router receives a packets on an interface with "ssg direction downlink" configured, it first compares the Source IP address of the packet with the SSG Host Object Table. If an Active SSG Host Object matching the Source IP address of this packet is not found, AND the destination TCP Port of the packet matches "port-list ports", and the destination IP address is NOT included as a part of "ssg default-network" OR SSG Open Garden, then the user will be redirected because his is unauthenticated [no Host Object] and his packet is destined for a TCP port in the "port-list ports". The user will then be captivated until an SSG Host Object is created, or until a timeout which is configurable via "redirect captivate initial default group". **debug ssg tcp redirect**
debug ssg ctrl-event

```
*Oct 13 20:24:36.833: SSG-TCP-REDIR:-Up:
   created new remap entry for unauthorised user at 2.2.2.5
*Oct 13 20:24:36.833: Redirect server set to 10.77.242.145,8090
*Oct 13 20:24:36.833: Initial src/dest port mapping 49273<->80

F340.07.23-2800-8#show ssg tcp-redirect mappings
 Authenticated hosts:
  No TCP redirect mappings for authenticated users

 Unauthenticated hosts:

  Downlink Interface: GigabitEthernet0/0.2
  TCP remapping Host:2.2.2.5 to server:10.77.242.145 on port:8090
```

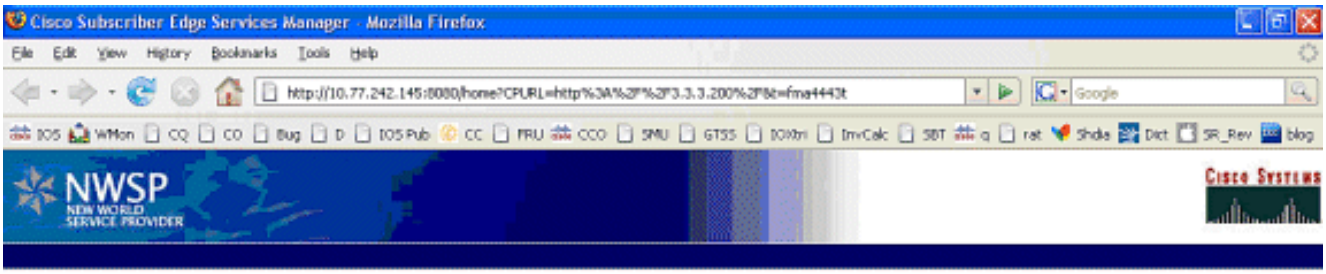
The initial HTTP request from 2.2.2.5 had a source TCP Port of 49273 and a destination IP address of 3.3.3.200 and TCP port of 80. Because of the SSG TCP Redirect, the destination IP header is overwritten with the socket of the SESM server 10.77.242.145:8090. If Port Bundle Host Key were NOT configured, the Source socket of 2.2.2.5:49273 would remain unchanged. However, in this case, Port Bundle Host Key is configured therefore the source address of this packet is ALSO changed based on this configuration: ssg port-map destination range 80 to 8100 ip 10.77.242.145 source ip 172.18.122.40 *Any packets destined to SESM on TCP ports 80-8100 are subject to PBHK source NAT to IP socket 172.18.122.40, starting with a port of 64.* *Oct 13 20:24:36.833: group:ssg_tr_unauth, web-proxy:0 *Oct 13 20:24:37.417: SSG-REDIR-EVT: -Down: TCP-FIN Rxd for user at 2.2.2.5, port 49273 *Oct 13 20:24:37.421: SSG-REDIR-EVT: -Up: TCP-FIN Rxd from user at 2.2.2.5, src port 49273 *As a part of this SSG TCP Redirect, the original URL is preserved http://3.3.3.200 but the destination IP socket is rewritten to 10.77.242.145:8090. So, when the SESM receives this URL of http://3.3.3.200 on TCP port 8090, it sends an HTTP redirect back toward the client's browser directing the client to the SESM login page, which is http://10.77.242.145:8080/home?CPURL=http%3A%2F%2F3.3.3. 200%2F&t=fma4443t. Notice the Browser Redirect points the Client Browser to TCP 8080 for captive portal. As such, the TCP session for the initial IOS SSG Redirect to 10.77.242.145:8090 is terminated. Also, notice SESM has captured the original URL of http://3.3.3.200 in the Redirect.* *Oct 13 20:24:38.049: SSG-CTL-EVN: Received cmd (4,&) from Host-Key 172.18.122.40:64 *Oct 13 20:24:38.049: SSG-CTL-EVN: Add cmd=4 from Host-Key 172.18.122.40:64 into SSG control cmd queue. *Oct 13 20:24:38.049: SSG-CTL-EVN: Dequeue cmd_ctx from the cmdQ and pass it to cmd handler *Oct 13 20:24:38.049: SSG-CTL-EVN: Handling account status query for Host-Key 172.18.122.40:64 *Oct 13 20:24:38.049: SSG-CTL-EVN: No active HostObject for Host-Key 172.18.122.40:64, Ack the query with Complete ID. *Oct 13 20:24:38.049: SSG-CTL-EVN: Send cmd 4 to host S172.18.122.40:64. dst=10.77.242.145:51806 *Oct 13 20:24:38.049: SSG-CTL-EVN: Deleting SSGCommandContext ::~SSGCommandContext *With Port Bundle Host Key configured, all HTTP communications between Client and SESM are subject to Port Bundling, which is effectively Source NAT for the TCP socket. Above, the "SSG-CTL-EVN" messages debug the communication between the SESM and the IOS SSG Router using a proprietary RADIUS-based protocol. When using Port Bundle Host Key, SESM always uses the Port Bundle to identify the host, which in this case is 172.18.122.40:64. You'll see when SESM sends the HTTP redirect resulting in the Web browser connecting to 10.77.242.145:8090, SESM also queries SSG on the Control Channel for existence of Host Object for 172.18.122.40:64, which the SSG Router knows is actually 2.2.2.5. Since no Host Object is present, the SSG Router sends the SESM "No active HostObject for Host-Key 172.18.122.40:64"* This can be confirmed at this point

```
like this: F340.07.23-2800-8#show ssg host
 ### Total HostObject Count: 0
```

En este punto, el navegador en MAC iBook Left se ve así cuando se ingresa **http://3.3.3.200**:



Después de que IOS SSG TCP y SESM HTTP redirijan, la pantalla se muestra de la siguiente
manera:



3. Después de la redirección TCP SSG al SESM y la subsiguiente redirección HTTP enviada por SESM al navegador de MAC iBook Left, MAC iBook Left ingresa **user1** como nombre de usuario y **cisco** como
contraseña:

4. Después de que se presione el botón **OK**, el SESM envía al router SSG estas credenciales a través de un protocolo basado en RADIUS propietario.

```
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Received cmd (1,user1) from Host-Key
   172.18.122.40:64
```

```
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Add cmd=1 from Host-Key 172.18.122.40:64
   into SSG control cmd queue.
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Dequeue cmd_ctx from the cmdQ
   and pass it to cmd handler
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Handling account logon for host
   172.18.122.40:64
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   No auto-domain selected for user user1
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Authenticating user user1.
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   ssg_aaa_nasport_fixup function
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   slot=0, adapter=0, port=0, vlan-id=2,
   dot1q-tunnel-id=0, vpi=0, vci=0, type=10
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Deleting SSGCommandContext
   ::~SSGCommandContext
```

5. A su vez, el router SSG construye un paquete de solicitud de acceso RADIUS y lo envía a RADIUS para autenticar al **usuario1**:

```
*Oct 13 20:25:01.785: RADIUS(00000008):
   Send Access-Request to
   10.77.242.145:1812 id 1645/11, len 88
*Oct 13 20:25:01.785: RADIUS:
   authenticator F0 56 DD E6 7E
   28 3D EF - BC B1 97 6A A9 4F F2 A6
*Oct 13 20:25:01.785: RADIUS:  User-Name
   [1]   7   "user1"
*Oct 13 20:25:01.785: RADIUS:  User-Password
   [2]   18  *
*Oct 13 20:25:01.785: RADIUS:  Calling-Station-Id
   [31]  16  "0011.2482.b3c0"
*Oct 13 20:25:01.785: RADIUS:  NAS-Port-Type
   [61]  6   Ethernet      [15]
*Oct 13 20:25:01.785: RADIUS:  NAS-Port
   [5]   6   0
*Oct 13 20:25:01.785: RADIUS:  NAS-Port-Id
   [87]  9   "0/0/0/2"
*Oct 13 20:25:01.785: RADIUS:  NAS-IP-Address
   [4]   6   172.18.122.40
```

6. RADIUS responde con Access-Accept para **user1**, y se crea un Objeto Host SSG en "F340.07.23-2800-8":

```
*Oct 13 20:25:02.081: RADIUS:
   Received from id 1645/11 10.77.242.145:1812,
   Access-Accept, len 273
*Oct 13 20:25:02.081: RADIUS:
   authenticator 52 7B 50 D7 F2 43 E6 FC -
   7E 3B 22 A4 22 A7 8F A6
*Oct 13 20:25:02.081: RADIUS:  Service-Type
   [6]   6   Framed         [2]
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  23
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 17  "NInternet-Basic"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  13
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
```

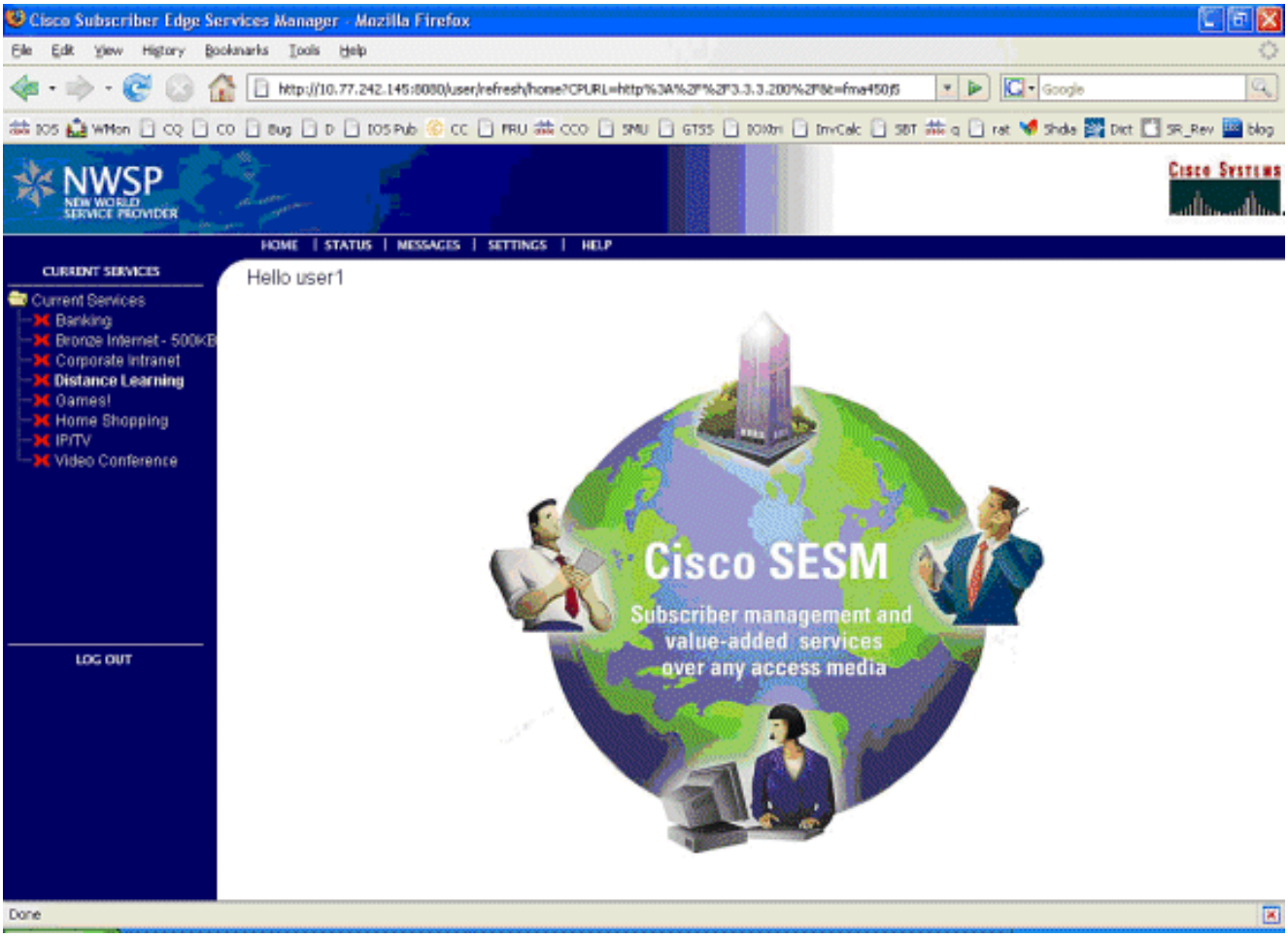
```
   [250] 7   "Niptv"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  14
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 8   "Ngames"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  18
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 12  "Ndistlearn"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  18
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 12  "Ncorporate"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  22
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 16  "Nhome_shopping"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  16
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 10  "Nbanking"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  16
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 10  "Nvidconf"
*Oct 13 20:25:02.081: RADIUS:  User-Name
   [1]   7   "user1"
*Oct 13 20:25:02.081: RADIUS:  Calling-Station-Id
   [31]  16  "0011.2482.b3c0"
*Oct 13 20:25:02.081: RADIUS:  NAS-Port-Type
   [61]  6   Ethernet       [15]
*Oct 13 20:25:02.081: RADIUS:  NAS-Port
   [5]   6   0
*Oct 13 20:25:02.081: RADIUS:  NAS-Port-Id
   [87]  9   "0/0/0/2"
*Oct 13 20:25:02.081: RADIUS:  NAS-IP-Address
   [4]   6   172.18.122.40
*Oct 13 20:25:02.081: RADIUS(00000008):
   eceived from id 1645/11
*Oct 13 20:25:02.081: RADIUS:  NAS-Port
   [5]   4   0
*Oct 13 20:25:02.081: SSG-CTL-EVN:
   Creating radius packet
*Oct 13 20:25:02.081: SSG-CTL-EVN:
   Response is good
*Oct 13 20:25:02.081: SSG-CTL-EVN:
   Creating HostObject for Host-Key
   172.18.122.40:64
*Oct 13 20:25:02.081: SSG-EVN:
   HostObject::HostObject: size = 616
*Oct 13 20:25:02.081: SSG-CTL-EVN:
   HostObject::Reset
*Oct 13 20:25:02.081: SSG-CTL-EVN:
   HostObject::InsertServiceList NInternet-Basic
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   HostObject::InsertServiceList Niptv
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   HostObject::InsertServiceList Ngames
*Oct 13 20:25:02.085: SSG-CTL-EVN:
  HostObject::InsertServiceList Ndistlearn
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   HostObject::InsertServiceList Ncorporate
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   HostObject::InsertServiceList Nhome_shopping
```

```
*Oct 13 20:25:02.085: SSG-CTL-EVN:
  HostObject::InsertServiceList Nbanking
*Oct 13 20:25:02.085: SSG-CTL-EVN:
  HostObject::InsertServiceList Nvidconf
*Oct 13 20:25:02.085: SSG-CTL-EVN:
  DoAccountLogon: ProfileCache is Enabled
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   Account logon is accepted
   [Host-Key 172.18.122.40:64, user1]
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   Send cmd 1 to host S172.18.122.40:64.
   dst=10.77.242.145:51806
*Oct 13 20:25:02.085: SSG-CTL-EVN:
  Activating HostObject for
   Host-Key 172.18.122.40:64
*Oct 13 20:25:02.085: SSG-CTL-EVN:
   Activating HostObject for host 2.2.2.5
```

Finally, our SSG Host Object is created for 2.2.2.5. Notice that "user1" RADIUS profile is configured with many ssg-account-info VSA with "N" Attribute, which is an SSG code for Service to which the user is subscribed. Please note, this doesn't mean "user1" has any Active services at this point, which can be confirmed with:

```
F340.07.23-2800-8#show ssg host
  1: 2.2.2.5  [Host-Key 172.18.122.40:64]

   ### Active HostObject Count: 1

 F340.07.23-2800-8#show ssg host 2.2.2.5

------------------------ HostObject Content ---
Activated: TRUE
Interface: GigabitEthernet0/0.2
User Name: user1
Host IP: 2.2.2.5
Host mac-address: 0011.2482.b3c0
Port Bundle: 172.18.122.40:64
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Host DHCP pool  :
Maximum Session Timeout: 64800 seconds
Action on session timeout: Terminate
Host Idle Timeout: 0 seconds
User policing disabled
User logged on since:
   *20:37:05.000 UTC Mon Oct 13 2008
User last activity at:
   *20:37:09.000 UTC Mon Oct 13 2008
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: NONE
AutoService: Internet-Basic;
Subscribed Services: Internet-Basic;
   iptv; games; distlearn;
   corporate; home_shopping; banking; vidconf;
Subscribed Service Groups: NONE
```

7. En este punto, **user1** se define como un objeto host SSG pero todavía no tiene acceso a ningún servicio SSG. MAC iBook Left se presenta con la pantalla Selección de servicio y hace clic en **Aprendizaje a distancia**:



8. Después de hacer clic en **Aprendizaje a distancia**, el cuadro SESM se comunica con el router SSG con el canal de control:

```
debug ssg ctrl-events

*Oct 13 20:25:38.029: SSG-CTL-EVN:
   Received cmd (11,distlearn) from
   Host-Key 172.18.122.40:64
```

SSG Router is receiving control channel command that SSG User 172.18.122.40:64 [maps to 2.2.2.5] wants to activate SSG Service 'distlearn'. *Oct 13 20:25:38.029: SSG-CTL-EVN: Add cmd=11 from Host-Key 172.18.122.40:64 into SSG control cmd queue. *Oct 13 20:25:38.029: SSG-CTL-EVN: Dequeue cmd_ctx from the cmdQ and pass it to cmd handler *Oct 13 20:25:38.029: SSG-CTL-EVN: Handling service logon for Host-Key 172.18.122.40:64 *Oct 13 20:25:38.029: SSG-CTL-EVN: Locating the HostObject for Host-Key 172.18.122.40:64 *Oct 13 20:25:38.029: SSG-CTL-EVN: Creating pseudo ServiceInfo for service: distlearn *Oct 13 20:25:38.029: SSG-EVN: ServiceInfo::ServiceInfo: size = 416 *Oct 13 20:25:38.029: SSG-CTL-EVN: ServiceInfo: Init servQ and start new process for distlearn *Oct 13 20:25:38.029: SSG-CTL-EVN: Service(distlearn)::AddRef(): ref after = 1 *Oct 13 20:25:38.029: SSG-CTL-EVN: **Got profile for distlearn locally**

Since "distlearn" is available from local configuration: local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255" *...we don't need to make a AAA call to download SSG Service Information. However, please note that in most real-world SSG implementations, SSG Services are defined on the RADIUS AAA Server.* *Oct 13 20:25:38.029: SSG-CTL-EVN: Create a new service table for distlearn *Oct 13 20:25:38.029: SSG-CTL-EVN: Service bound on this interface are : distlearn *Oct 13 20:25:38.029: SSG-CTL-EVN: Service distlearn bound to interface GigabitEthernet0/0.3 firsthop 0.0.0.0 *Oct 13 20:25:38.029: Service Address List : *Oct 13 20:25:38.033: Addr:3.3.3.200 mask:255.255.255.255 *Oct 13 20:25:38.033: SSG-CTL-EVN: Add a new service distlearn to an existing table *Here the SSG creates a Service Table for distlearn and binds it to an "ssg direction uplink" interface complete with the R attribute for the Service.* *Oct 13 20:25:38.033: SSG-CTL-EVN: Locating the HostObject for Host-Key 172.18.122.40:64 *Oct 13 20:25:38.033: SSG-CTL-EVN: Checking connection activation for 172.18.122.40:64 to distlearn. *Oct 13 20:25:38.033: SSG-CTL-EVN: Creating

ConnectionObject (172.18.122.40:64, distlearn) *Oct 13 20:25:38.033: SSG-EVN: ConnectionObject::ConnectionObject: size = 304 *Oct 13 20:25:38.033: SSG-CTL-EVN: Service(distlearn)::AddRef(): ref after = 2 *Oct 13 20:25:38.033: SSG-CTL-EVN: Checking maximum service count. *Oct 13 20:25:38.033: SSG-EVN: Opening connection for user user1 *Oct 13 20:25:38.033: SSG-EVN: Connection opened *Oct 13 20:25:38.033: **SSG-CTL-EVN: Service logon is accepted.**
*Oct 13 20:25:38.033: SSG-CTL-EVN:
Activating the ConnectionObject.

Once the Service is verified locally, SSG needs to build a "Connection" where a "Connection" is a tuple with: A. SSG Host Object B. SSG Service Name and Attributes C. SSG Downlink interface D. SSG Upstream interface A-D are used to create a pseudo hidden VRF service table for which traffic from this host can transit. See here: F340.07.23-2800-8#**show ssg connection 2.2.2.5 distlearn**

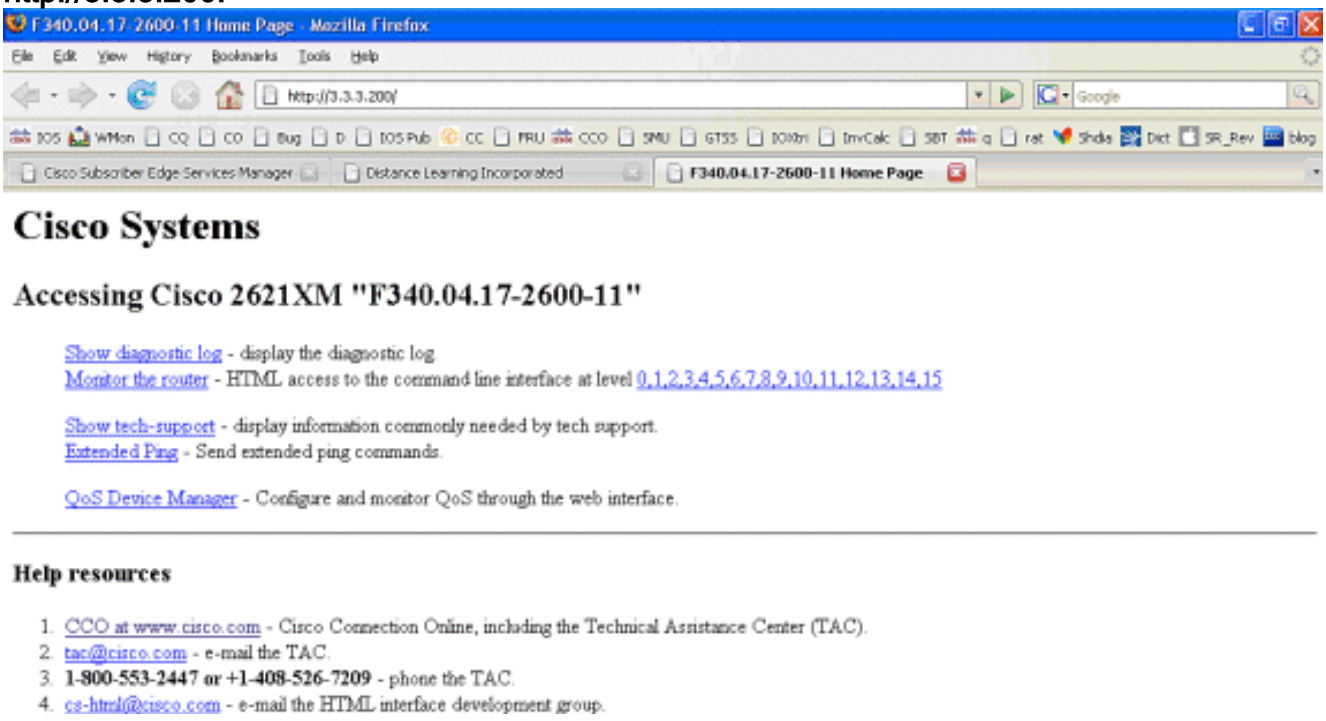
----------ConnectionObject Content ----
User Name: user1
Owner Host: 2.2.2.5
Associated Service: distlearn
Calling station id: 0011.2482.b3c0
Connection State: 0 (UP)
Connection Started since:
*20:40:21.000 UTC Mon Oct 13 2008

User last activity at:
*20:41:04.000 UTC Mon Oct 13 2008
Connection Traffic Statistics:
Input Bytes = 420, Input packets = 5
Output Bytes = 420, Output packets = 5
Session policing disabled

F340.07.23-2800-8#**show ssg host 2.2.2.5**

---------- HostObject Content -----------
Activated: TRUE
Interface: GigabitEthernet0/0.2
User Name: user1
Host IP: 2.2.2.5
Host mac-address: 0011.2482.b3c0
Port Bundle: 172.18.122.40:64
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Host DHCP pool :
Maximum Session Timeout: 64800 seconds
Action on session timeout: Terminate
Host Idle Timeout: 0 seconds
User policing disabled
User logged on since:
*20:37:05.000 UTC Mon Oct 13 2008
User last activity at:
*20:40:23.000 UTC Mon Oct 13 2008
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: distlearn;
AutoService: Internet-Basic;
Subscribed Services: Internet-Basic;
iptv; games; distlearn; corporate;
home_shopping; banking; vidconf;
Subscribed Service Groups: NONE

9. La conexión SSG está activa y el flujo de llamada ha finalizado. MAC iBook Left puede navegar con éxito a **http://3.3.3.200:**



Explicación de la configuración del router SSG con documentos de funciones

```
version 12.4
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname F340.07.23-2800-8
!
boot-start-marker
boot system flash flash:
   c2800nm-adventerprisek9-mz.124-21.15
boot-end-marker
!
logging buffered 1024000 debugging
!
aaa new-model
!
aaa authorization network default group radius
!
aaa session-id common
no ip source-route
!
ip cef
ip dhcp relay information trust-all
ip dhcp use vrf connected
ip dhcp excluded-address 2.2.2.1
```

ip dhcp excluded-address 2.2.2.2
ip dhcp excluded-address 2.2.2.3
ip dhcp excluded-address 2.2.2.4
ip dhcp excluded-address 2.2.2.6
ip dhcp excluded-address 2.2.2.7

We are excluding 2.2.2.1-4 and 2.2.2.6-7 to ensure the only DHCP address that will be leased is 2.2.2.5/29. Configuring the Cisco IOS DHCP Server ip dhcp pool dhcp_guest_v3501 network 2.2.2.0 255.255.255.248 default-router 2.2.2.1 dns-server 172.18.108.34 lease 0 4 update arp *If an interface on this router is configured with an address in the 2.2.2.0/29 range, it will field DHCP request from host on that network and assign IP address 2.2.2.5, GW 2.2.2.1, and DNS Server 172.18.108.24. The lease time on the IP address will be 4 hours. Also, "update arp" will ensure ARP entries for IP addresses leased via DHCP will match the MAC entry in the DHCP Binding table. This will prevent SSG session hijacking in the event a static user re-uses a DHCP [or is given] leased address.* Configuring the Cisco IOS DHCP Server Configuring DHCP Services for Accounting and Security ! no ip domain lookup ip auth-proxy max-nodata-conns 3 ip admission max-nodata-conns 3 ! voice-card 0 no dspfarm ! ssg enable *Enables SSG subsystem.* Implementing SSG: Initial Tasks ssg intercept dhcp *Enables SSG/DHCP Awareness. In our example, this will result in an SSG Host object being destroyed when either of these occur: A. A DHCPRELEASE message is received for an IP address matching a currently Active SSG Host Object. B. A DHCP Lease expires for an IP address matching a currently Active SSG Host Object.* Configuring SSG for On-Demand IP Address Renewal ssg default-network 10.77.242.145 255.255.255.255 *All packets ingress to "ssg direction downlink" interfaces can access the "ssg default-network" regardless as to whether a Host or Connection Object exists. SSG allows all users, even unauthenticated users, to access the default network. Typically, SESM belongs to the default network. However, other types of servers, such as DNS/DHCP servers or TCP-Redirect servers, can also be part of the default network.* Implementing SSG: Initial Tasks ssg service-password cisco *If an SSG Service is not defined locally and we therefore need to make a RADIUS call when a user subscribes to an SSG Service, the password "cisco" is used in the RADIUS Access-Request for the Service.* ssg radius-helper auth-port 1812 acct-port 1813 ssg radius-helper key cisco *Used to communicate with SESM on SSG Control Channel. SESM must also maintain a similar static configuration for each SSG Router it serves.* Implementing SSG: Initial Tasks ssg auto-logoff arp match-mac-address interval 30 *In the absence of user traffic, SSG will send an ARP Ping for all Active Host Objects and will invoke an AutoLogoff if either the host fails to reply or the MAC address of the host has changed.* Configuring SSG to Log Off Subscribers ssg bind service distlearn GigabitEthernet0/0.3 *SSG traffic is not routed using the Global routing table. Instead it's routed from "ssg direction downstream" interface using the information in the mini-VRF seen in "show ssg connection", which includes a manual binding of Service<-->"ssg direction uplink" interface. Hence, it is a requirement of SSG to manually bind services to interfaces or next-hop IP addresses.* Configuring SSG for Subscriber Services ssg timeouts session 64800 *Absolute timeout for SSG Host Object is 64800 seconds.* Configuring SSG to Log Off Subscribers ssg port-map destination range 80 to 8100 ip 10.77.242.145 source ip 172.18.122.40 *Port Bundle Host Key configuration. All traffic destined to 10.77.242.145 in the range of TCP 80 to 8100 will be Source NATed to 172.18.122.40.* Implementing SSG: Initial Tasks ssg tcp-redirect *Enters SSG redirect sub-config.* Configuring SSG to Authenticate Web Logon Subscribers port-list ports port 80 port 8080 port 8090 port 443 *Defines a list of destination TCP ports which are candidates for TCP redirection.* Configuring SSG to Authenticate Web Logon Subscribers server-group ssg_tr_unauth server 10.77.242.145 8090 *Defines a redirect server list and defines the TCP port on which they're listening for redirects.* Configuring SSG to Authenticate Web Logon Subscribers redirect port-list ports to ssg_tr_unauth redirect unauthenticated-user to ssg_tr_unauth *If a Host Object does NOT exist and the traffic is ingress to an "ssg direction downlink" interface AND its destination port is in port-list ports, THEN redirect this traffic to "server-group ssg_tr_unauth".* Configuring SSG to Authenticate Web Logon Subscribers ssg service-search-order local remote *Look for SSG Service defined in a local-profile in IOS configuration before making a AAA call to download Service information.* Configuring SSG for Subscriber Services local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255" *Local definition of SSG Service "distlearn" 26 9 251 is Vendor Specific, Cisco, SSG Service Info Attributes defined herein: R: Destination Network, Specifies IP routes belonging to this Service* Configuring SSG for Subscriber Services RADIUS Profiles and Attributes for SSG interface GigabitEthernet0/0 no ip address duplex auto speed auto ! interface GigabitEthernet0/0.2 description Guest Wireless Vlan encapsulation dot1Q 2 ip address 2.2.2.1 255.255.255.248 no ip redirects no ip unreachables no ip mroute-cache ssg direction downlink *All SSG Host Objects should be located on downlink direction.* Implementing SSG: Initial Tasks interface GigabitEthernet0/0.3 description Routed connection back to Blue encapsulation dot1Q 3 ip address 3.3.3.1 255.255.255.0 ssg direction

```
uplink All SSG Services should be located on uplink direction. Implementing SSG: Initial Tasks
interface GigabitEthernet0/1 ip address 172.18.122.40 255.255.255.224 duplex auto speed auto !
ip forward-protocol nd ip route 10.77.242.144 255.255.255.255 172.18.122.33 ip route
10.77.242.145 255.255.255.255 172.18.122.33 ip route 157.157.157.0 255.255.255.0 3.3.3.5 ip
route 172.18.108.34 255.255.255.255 172.18.122.33 ip route 172.18.124.101 255.255.255.255
172.18.122.33 ! no ip http server no ip http secure-server ! ip radius source-interface
GigabitEthernet0/1 ! radius-server host 10.77.242.145 auth-port 1812 acct-port 1813 timeout 5
retransmit 3 key 7 070C285F4D06 ! control-plane ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 ! scheduler allocate 20000 1000 ! end
```

Consideraciones sobre la seguridad y la reutilización de sesiones

Cuando utiliza SSG y DHCP juntos, estos escenarios pueden permitir a los usuarios malintencionados reutilizar un objeto host SSG autenticado que permita el acceso no autenticado a los recursos seguros:

- Si el reconocimiento de SSG/DHCP no se configura con "ssg intercept dhcp", un nuevo usuario DHCP puede ceder una dirección IP previamente arrendada para la cual todavía existe un objeto host SSG. Dado que la primera solicitud TCP de este nuevo usuario tiene un objeto host SSG coincidente, aunque obsoleto, que coincide con la dirección IP de origen, se concede a este usuario un uso no autenticado de los recursos protegidos. Esto se puede prevenir con "ssg intercept dhcp", que da como resultado la eliminación de un objeto host SSG cuando se produce alguno de los siguientes:DHCPRELEASE se recibe para una dirección IP que coincide con un objeto host activo.El arrendamiento DHCP vence para una dirección IP que coincide con un objeto host activo.
- Si un usuario DHCP socializa la dirección IP arrendada a un usuario malintencionado antes de un logout DHCP no elegante, que es un logout DHCP para el cual no se envía un DHCPRELEASE, el usuario malintencionado puede configurar estáticamente la máquina con esta dirección IP y reutilizar el objeto Host SSG si se configura o no "ssg intercept dhcp". Esto se puede prevenir con una combinación de "ssg intercept dhcp" y "update arp" configurados debajo del conjunto DHCP de IOS. El "arp de actualización" asegura que el único subsistema del IOS capaz de agregar o quitar entradas ARP sea el subsistema del servidor DHCP. Con "actualizar arp", el enlace DHCP de IP a MAC siempre coincide con el enlace de IP a MAC en la tabla ARP. Aunque el usuario malintencionado tiene una dirección IP configurada estáticamente que coincide con el objeto Host SSG, no se permite que el tráfico ingrese al router SSG. Debido a que la dirección MAC no coincide con la dirección MAC del enlace DHCP actual, el servidor DHCP de IOS evita la creación de una entrada ARP.
- Cuando SSG y DHCP se configuran juntos, "ssg intercept dhcp" y "update arp" impiden la reutilización de la sesión. El último desafío no relacionado con la seguridad es liberar el arriendo DHCP y la entrada ARP cuando un host DHCP realiza un logout no fluido. La configuración de "arp autorizado" en la interfaz "ssg direction downlink" da como resultado solicitudes ARP periódicas enviadas a todos los hosts para asegurarse de que siguen activos. Si no se recibe respuesta de estos mensajes ARP periódicos, se libera el enlace DHCP y el subsistema DHCP del IOS purga la entrada ARP.

  ```
  interface FastEthernet0/0
  ip address 10.0.0.1 255.255.255.0
  arp authorized
  arp probe interval 5 count 15
  ```

  En este ejemplo, se envía periódicamente una solicitud ARP para actualizar todas las entradas ARP conocidas en Fa0/0 cada 5 s. Después de 15 fallas, se libera el enlace DHCP y el subsistema DHCP de IOS purga la entrada ARP.En el contexto de SSG sin "arp

autorizado", si un host DHCP realiza un logout no fluido, el arrendamiento DHCP y su objeto host SSG asociado permanecen activos hasta que caduque el arrendamiento para esta dirección DHCP, pero no se produce una reutilización de la sesión mientras "ssg intercept dhcp" esté configurado globalmente.

El "ARP autorizado" desactiva el aprendizaje ARP dinámico en la interfaz en la que está configurado. Las únicas entradas ARP en la interfaz en cuestión son las agregadas por el servidor DHCP del IOS después de iniciar una concesión. Estas entradas ARP son purgadas luego por el servidor DHCP del IOS una vez que la concesión ha terminado, ya sea por la recepción de una VERSIÓN DHCP, una expiración de la concesión o una falla de sonda ARP debido a un cierre de sesión DHCP no elegante.

Notas de implementación:

- Los métodos "ssg auto-logoff arp" y "ssg auto-logoff icmp" son métodos no deseados para evitar la reutilización de la sesión o los problemas de seguridad resultantes. Las variantes "arp" e "icmp" de "ssg auto-logoff" sólo envían un PING ARP o IMCP cuando no se ve tráfico en la conexión SSG dentro del "intervalo" configurado, el más bajo de los cuales es de 30 segundos. Si DHCP arrienda una dirección IP utilizada anteriormente en 30 segundos o un usuario malintencionado configura estáticamente una dirección DHCP enlazada actualmente en 30 segundos, la sesión se reutiliza porque SSG ve tráfico en el objeto de conexión y "ssg auto-logoff" no invoca.
- En todos los casos prácticos, la reutilización de la sesión no se impide si un host malintencionado realiza una suplantación de dirección MAC.

Tabla 1: Consideraciones de Reutilización de Sesión y Seguridad en Implementaciones SSG/DHCP

Comando	Función	Implicaciones de seguridad
ssg auto-logoff arp [match-mac-address] [intervalo *segundos*] **ssg auto-logoff icmp [timeout milisecond s] [número de paquetes] [intervalo *segundos*]**	Quita el objeto host SSG después de una falla de ARP o ICMP PING, que sólo se envían después de no ver tráfico en la conexión SSG dentro del "intervalo".	Reutiliza la sesión si DHCP arrienda una dirección IP utilizada anteriormente en 30 segundos, o un usuario malintencionado configura estáticamente una dirección DHCP enlazada actualmente en 30 segundos porque SSG ve tráfico en el objeto de conexión y "ssg auto-logoff" no invoca.
ssg intercept dhcp	Crea un reconocimiento SSG/DHCP que permite la eliminación del objeto host SSG	Evita que los usuarios DHCP reutilicen las sesiones SSG, pero no impide que los

	dentro de estos eventos: Se recibe un DHCPRELEASE para una dirección IP que coincide con un objeto host activo. B El arrendamiento DHCP vence para una dirección IP que coincide con un objeto host activo.	usuarios estáticos suplanten direcciones DHCP o la reutilización de sesiones SSG.
ip dhcp pool TEST update arp	Se asegura de que el único subsistema del IOS capaz de agregar o eliminar entradas ARP sea el subsistema del servidor DHCP.	Evita la reutilización de todas las sesiones cuando se configura con "ssg intercept dhcp". Cuando se configura sin "ssg intercept dhcp", si DHCP arrienda una dirección IP previamente utilizada, la reutilización de la sesión sigue siendo posible.
interfaz FastEthernet0/0 arp autorizada	Envía solicitudes ARP periódicas a todos los hosts para asegurarse de que siguen activos. Desactiva el aprendizaje ARP dinámico.	Permite el enlace DHCP y la eliminación de entradas ARP cuando un usuario DHCP realiza un logout no correcto.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems