# Débogage de flux d'appel sur une passerelle Internet SSG configurée avec DHCP Secure ARP, SSG Port-Bundle Host Key, SSG TCP Redirect, SESM, et SSG/DHCP Awareness

## Contenu


Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
**Informations générales**
Technologie et vue d'ensemble des fonctionnalités
Diagramme de banc d'essai
Debug d'écoulement d'appel
Explication de configuration de routeur SSG avec des documents de caractéristique
Considérations de réutilisation de Sécurité et de session
**Informations connexes**


## Introduction

Le centre de ce document est une passerelle internet IOS qui exécute SSG et DHCP avec SESM pour des services portaiux.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

# Informations générales

## Technologie et vue d'ensemble des fonctionnalités

### Passerelle de sélection de services (SSG)

Le Passerelle de sélection de services (SSG) est une solution de commutation pour les fournisseurs de services qui offrent l'intranet, l'extranet, et les connexions Internet aux abonnés avec la technologie d'accès haut débit, telle que les lignes d'abonné numérique (DSL), les Modems câble, ou la radio pour permettre l'accès simultané aux services réseau.

Travaux SSG en même temps que le Cisco Subscriber Edge Services Manager (SESM). En même temps que le SESM, SSG fournit l'authentification d'abonné, entretient la sélection, et les capacités de connexion de service aux abonnés des services Internet. Les abonnés interagissent avec une application Web SESM utilisant un navigateur Internet standard.

Le SESM fonctionne en deux modes :

- Mode de RAYON — Ce mode obtient l'abonné et l'information d'un serveur de RAYON. SESM en mode de RAYON est semblable au disque transistorisé.
- Mode de LDAP — Le mode de Protocole LDAP (Lightweight Directory Access Protocol) permet d'accéder à un répertoire LDAP-conforme pour l'abonné et les informations de service profile. Ce mode également a la fonctionnalité améliorée pour des applications Web SESM et emploie un modèle basé sur rôle du contrôle d'accès (RBAC) pour gérer le subscriber access.

### Clé de hôte de paquet de port SSG

La caractéristique de SSG Port-Bundle Host Key améliore la transmission et la fonctionnalité entre SSG et SESM avec un mécanisme qui emploie l'adresse IP source d'hôte et le port de source pour identifier et surveiller des abonnés.

Avec la configuration de SSG Port-Bundle Host Key, SSG exécute la translation d'adresses (PAT) et le Traduction d'adresses de réseau (NAT) sur le trafic http entre l'abonné et le serveur SESM. Quand un abonné envoie un paquet de HTTP au serveur SESM, SSG crée une carte de port qui change l'adresse IP source à une adresse IP source configurée SSG et change le port TCP de source à un port alloué par SSG. SSG assigne un paquet de ports à chaque abonné parce qu'un abonné peut avoir plusieurs sessions TCP simultanées quand il accède à une page Web. La clé de hôte assignée, ou la combinaison du port-paquet et de l'adresse IP source SSG, identifie seulement chaque abonné. La clé de hôte est dedans portés les paquets RADIUS envoyés entre le serveur SESM et le SSG dans l'attribut de constructeur-particularité IP d'abonné (le VSA). Quand le serveur SESM envoie une réponse à l'abonné, SSG traduit l'adresse IP de destination et le port TCP de destination selon la carte de port.

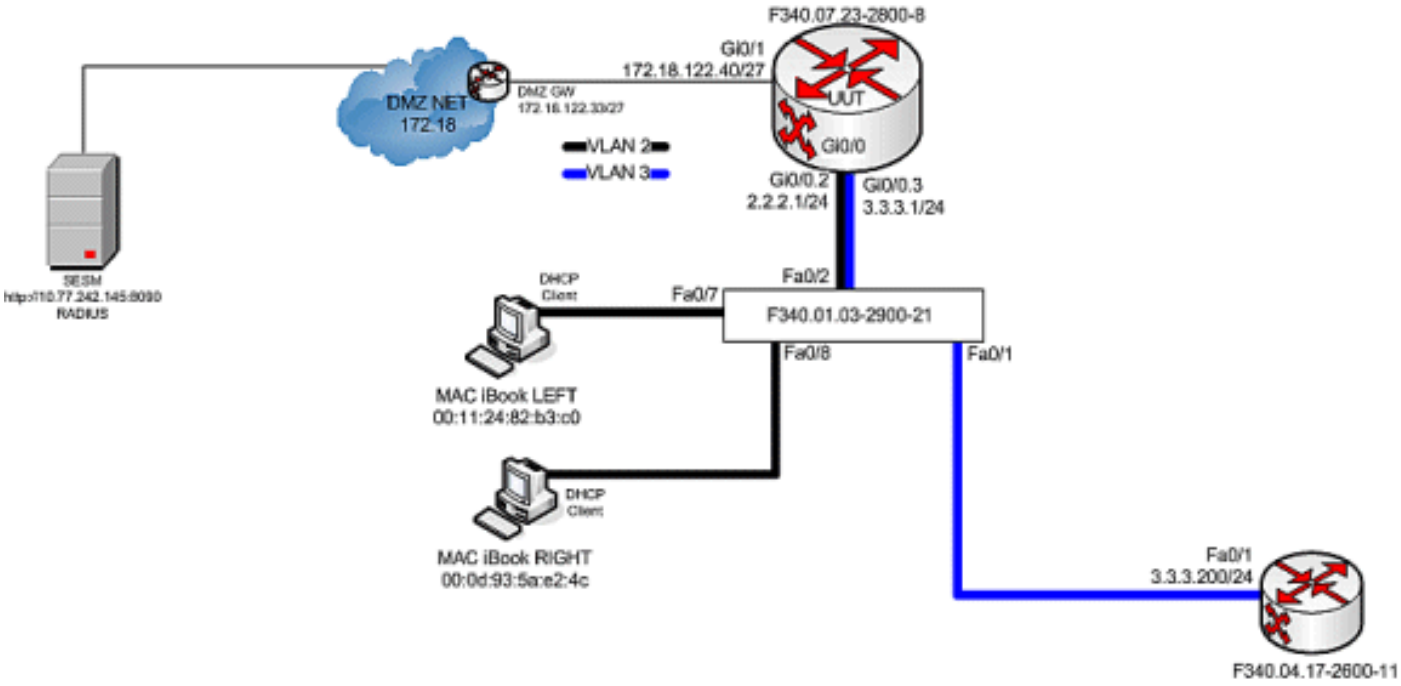
### Redirection de TCP SSG pour les utilisateurs Unauthenticated

La redirection pour les utilisateurs unauthenticated réoriente des paquets d'un utilisateur si l'utilisateur n'a pas autorisé avec le fournisseur de services. Quand les tentatives non autorisées d'un abonné de se connecter à un service sur un port TCP (par exemple, à www.cisco.com), SSG TCP Redirect réoriente le paquet au portail captif (SESM ou un groupe des périphériques SESM). SESM émet un redirect to le navigateur pour afficher la page de connexion. L'abonné ouvre une session à SESM et est authentifié et autorisé. SESM présente alors l'abonné avec une page d'accueil personnalisée, la page d'accueil de fournisseur de services, ou l'URL d'original.

### Le DHCP a sécurisé l'affectation d'adresse IP

La caractéristique sécurisée d'affectation d'adresse IP DHCP introduit la capacité pour sécuriser des entrées de la table ARP aux baux du protocole DHCP (DHCP) dans la base de données DHCP. Cette caractéristique sécurise et synchronise l'adresse MAC du client à la liaison DHCP, empêchant les clients ou les pirates informatiques non autorisés de charrier le serveur DHCP et d'assurer un bail DHCP d'un client autorisé. Quand cette caractéristique est activée, et le serveur DHCP assigne une adresse IP au DHCP Client, le serveur DHCP ajoute une entrée sécurisée d'ARP à la table ARP avec l'adresse IP assignée et l'adresse MAC du client. Cette entrée d'ARP ne peut pas n'être mise à jour par aucun autre paquet dynamique d'ARP, et cette entrée d'ARP existe dans la table ARP pour la durée de bail configurée ou tant que le bail est en activité. L'entrée sécurisée d'ARP peut être supprimée seulement par un message d'arrêt explicite du DHCP Client ou du serveur DHCP quand la liaison DHCP expire. Cette caractéristique peut être configurée pour un nouveau réseau DHCP ou être utilisée pour améliorer la Sécurité d'un réseau en cours. La configuration de cette caractéristique n'interrompt pas le service et n'est pas visible au DHCP Client.

## Diagramme de banc d'essai




## Debug d'écoulement d'appel

Procédez comme suit :

1. Quand l'iBook de MAC LAISSÉ d'abord connecte le câble Ethernet à ce réseau, il loue l'adresse IP 2.2.2.5/29 du serveur DHCP IOS qui fonctionne sur « 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-
```

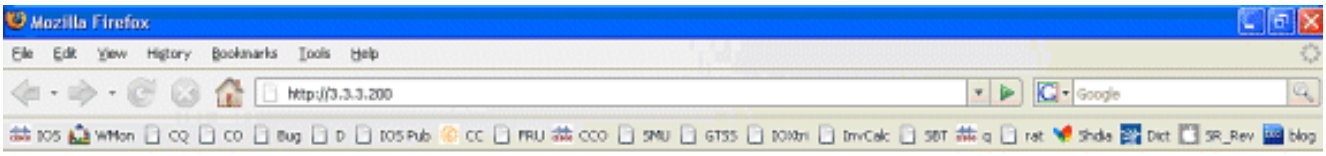
EVN:2.2.2.5: IP address notification received. *Oct 13 20:24:05.073: SSG-DHCP-EVN:2.2.2.5: HostObject not present *Oct 13 20:24:05.073: DHCPD: Can't find any hostname to update *Oct 13 20:24:05.073: DHCPD: Sending DHCPACK to client 0100.1124.82b3.c0 (2.2.2.5). *Oct 13 20:24:05.073: DHCPD: creating ARP 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. Après qu'il loue avec succès l'adresse IP 2.2.2.5, la GAUCHE d'iBook de MAC ouvre un navigateur Web et l'indique **http://3.3.3.200**, qui est utilisé pour simuler les ressources protégées attachées au service « distlearn SSG. » Le service « distlearn » SSG est localement défini dans le routeur « F340.07.23-2800-8 » SSG :

   **local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255"** En réalité, **http://3.3.3.200** est un routeur Cisco IOS configuré pour le « ip http server » et écoute sur le TCP 80, ainsi c'est fondamentalement un web server.Après que les tentatives de GAUCHE d'iBook de MAC de parcourir à **http://3.3.3.200**, puisque cette connexion est d'entrée sur une interface configurée avec la « liaison descendante de ssg direction, » le routeur SSG vérifie d'abord l'existence d'un objet actif d'hôte SSG pour l'adresse IP source de la demande de HTTP. Puisque ceci le premier une telle demande de l'adresse IP 2.2.2.5, un objet d'hôte SSG n'existe pas, et un TCP réorientent vers SESM est instancié pour l'hôte 2.2.2.5 par cette configuration :

   **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*

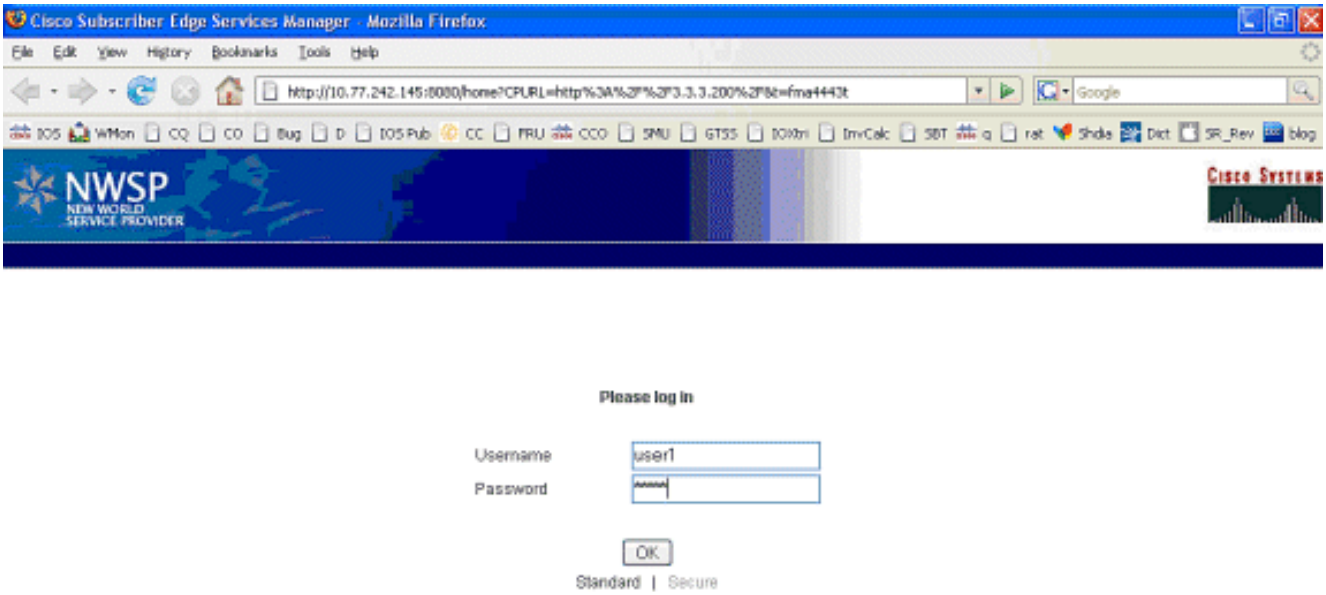
*http://3.3.3.200 in the Redirect.* *Oct 13 20:24:38.049: SSG-CTL-EVN: Received cmd (4,&) from Host-Key 172.18.122.40:64 *Oct 13 20:24:38.049: SSG-CTL-EVN: Add cmd=4 from Host-Key 172.18.122.40:64 into SSG control cmd queue. *Oct 13 20:24:38.049: SSG-CTL-EVN: Dequeue cmd_ctx from the cmdQ and pass it 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 ce moment, le navigateur sur la gauche d'iBook de MAC ressemble à ceci quand **http://3.3.3.200** est entré :




Après IOS SSG le TCP et le HTTP SESM réoriente, l'écran ressemble à ceci :



3. Après le redirect to SESM de TCP SSG et le HTTP ultérieur réorientez envoyé par SESM de nouveau au navigateur de l'iBook de MAC laissé, la gauche d'iBook de MAC entre dans **user1** comme nom d'utilisateur et **Cisco** comme mot de passe :



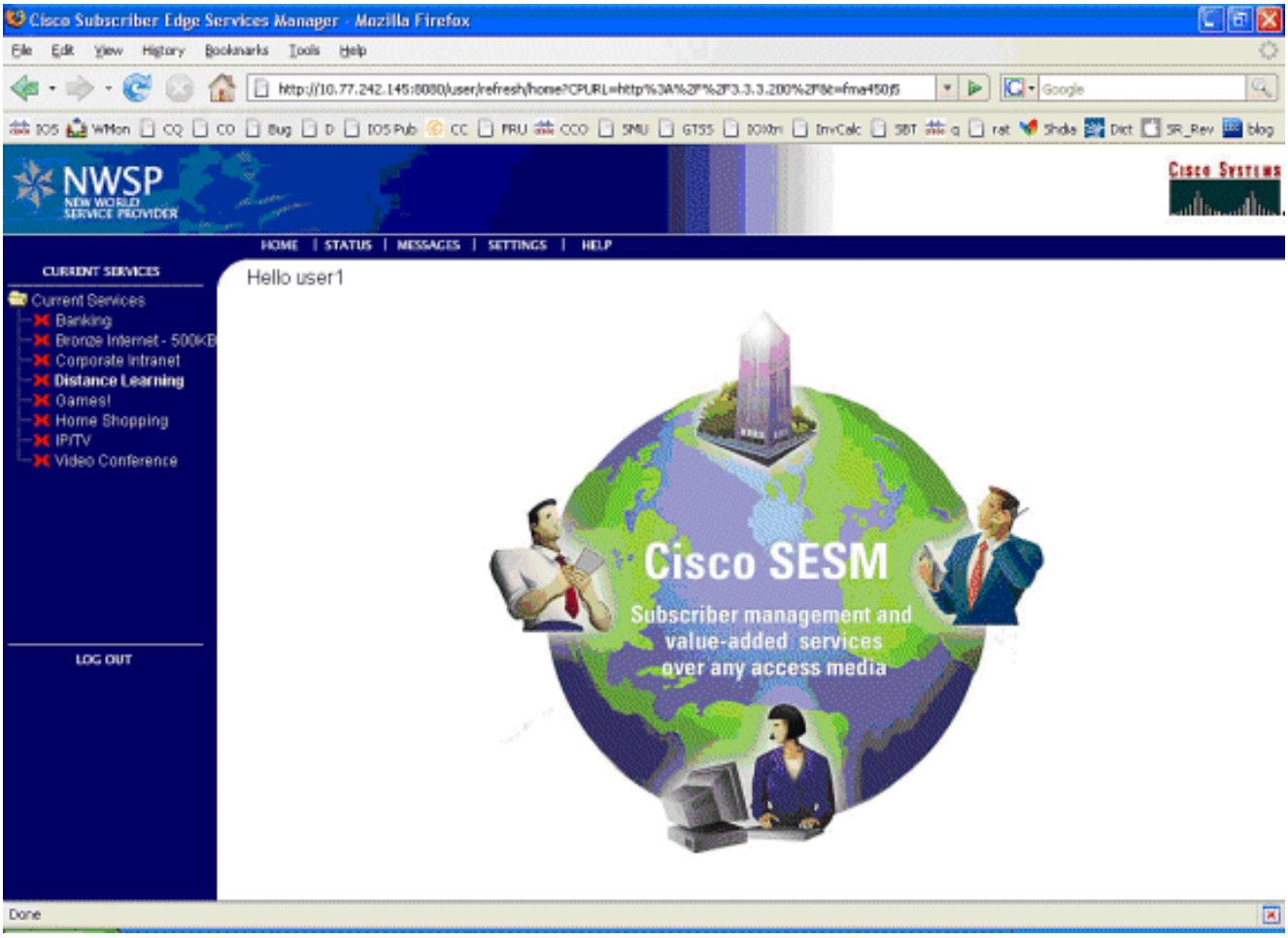

4. Après que le bouton **CORRECT** soit poussé, le SESM envoie au routeur SSG ces qualifications par un protocole basé sur rayon de propriété industrielle.
```
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Received cmd (1,user1) from Host-Key
   172.18.122.40:64
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Add cmd=1 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. Consécutivement, le routeur SSG construit un paquet de demande d'accès de RAYON et l'envoie au RAYON pour authentifier **user1** :
```
*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. Le RAYON répond avec un Access-recevoir pour **user1**, et un objet d'hôte SSG est créé dans « 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 ce moment, **user1** est défini comme objet d'hôte SSG mais n'a pas encore accès à aucun services SSG. La gauche d'iBook de MAC est présentée avec l'écran de sélection de service et clique sur l'**Apprentissage en ligne**
   :



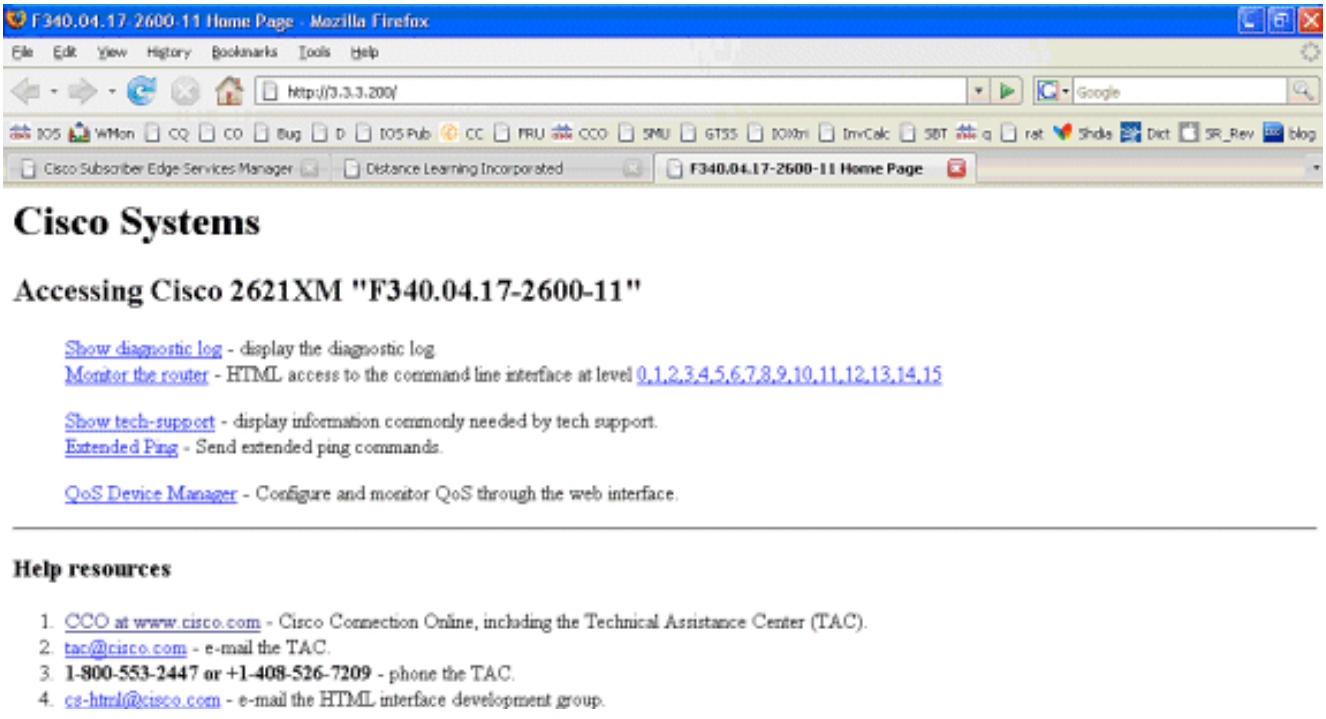

8. Après que l'**Apprentissage en ligne** soit cliqué sur, la case SESM communique au routeur SSG avec le canal de contrôle :`debug ssg ctrl-events`

```
*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 connexion SSG est en hausse, et l'écoulement d'appel est terminé. La gauche d'iBook de MAC peut avec succès parcourir à **http://3.3.3.200**
:




## Explication de configuration de routeur SSG avec des documents de caractéristique

```
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

## Considérations de réutilisation de Sécurité et de session

Quand vous utilisez SSG et DHCP ensemble, ces scénarios peuvent permettre aux utilisateurs malveillants pour réutiliser un objet authentifié d'hôte SSG qui permettent l'accès unauthenticated pour sécuriser des ressources :

- Si la connaissance SSG/DHCP n'est pas configurée avec le « ssg intercept dhcp, » un nouvel utilisateur DHCP peut louer une adresse IP précédent-louée pour laquelle un objet d'hôte SSG existe toujours. Puisque la première demande de TCP de ce nouvel utilisateur a apparier, bien qu'éventée, l'objet d'hôte SSG qu'apparie l'adresse IP source, on accorde cet utilisateur l'utilisation unauthenticated des ressources protégées. Ceci peut être empêché avec le « ssg intercept dhcp, » que les résultats dans la suppression d'un hôte SSG objectent quand l'un ou l'autre se produit :DHCPRELEASE est reçu pour une adresse IP qui apparie un objet actif d'hôte.Le bail DHCP expire pour une adresse IP qui apparie un objet actif d'hôte.
- Si un utilisateur DHCP socialise l'adresse IP louée à un utilisateur malveillant avant une déconnexion non-gracieuse DHCP, qui est une déconnexion DHCP pour laquelle un DHCPRELEASE n'est pas envoyé, l'utilisateur malveillant peut statiquement configurer l'ordinateur avec cette adresse IP et réutiliser l'objet d'hôte SSG si le « ssg intercept dhcp » est configuré. Ceci peut être empêché avec une combinaison de « ssg intercept dhcp » et de « update arp » configuré sous le pool DHCP IOS. Le « update arp » s'assure que le seul sous-système IOS capable ajouter ou retirer des entrées d'ARP est le sous-système de serveur DHCP. Avec le « update arp, » la liaison DHCP d'IP-à-MAC apparie toujours l'IP-à-MAC liant dans la table ARP. Quoique l'utilisateur malveillant ait une adresse IP statiquement configurée qui apparie l'objet d'hôte SSG, on ne permet pas au le trafic pour présenter le routeur SSG. Puisque l'adresse MAC n'apparie pas l'adresse MAC de la liaison DHCP en

cours, le serveur DHCP IOS empêche la création d'une entrée d'ARP.

- Quand SSG et DHCP sont configurés ensemble, le « ssg intercept dhcp » et le « update arp » empêchent la réutilisation de session. Le défi associé parSécurité finale est de libérer l'entrée de bail et d'ARP DHCP quand un hôte DHCP exécute une déconnexion non-gracieuse. La configuration « ARP autorisé » sur des résultats d'interface « de liaison descendante de ssg direction » dans des demandes périodiques d'ARP envoyées à tous les hôtes pour s'assurer les sont encore en activité. Si aucune réponse n'est reçue de ces messages périodiques d'ARP, la liaison DHCP est libérée, et le sous-système DHCP IOS purge l'entrée d'ARP.`interface FastEthernet0/0`
  `ip address 10.0.0.1 255.255.255.0`
  `arp authorized`
  `arp probe interval 5 count 15`
  Dans cet exemple, une demande d'ARP est envoyée périodiquement de régénérer toutes les entrées connues d'ARP sur Fa0/0 chaque 5s. Après 15 pannes, la liaison DHCP est libérée, et le sous-système DHCP IOS purge l'entrée d'ARP.Dans le cadre de SSG sans « a autorisé l'ARP, » si un hôte DHCP exécute une déconnexion non-gracieuse, le bail DHCP et son objet associé d'hôte SSG demeurent actif jusqu'à ce que le bail pour cette adresse DHCP expire, mais aucune réutilisation de session ne se produit tant que le « ssg intercept dhcp » est configuré globalement.

« L'ARP autorisé » arrête l'ARP dynamique apprenant sur l'interface sur laquelle il est configuré. Les seules entrées d'ARP sur l'interface en question sont ceux ajoutées par le serveur DHCP IOS après qu'un bail soit commencé. Ces entrées d'ARP sont alors purgées par le serveur DHCP IOS une fois que le bail s'est terminé, en raison de la réception d'une RELEASE DHCP, d'une expiration de bail, ou d'une panne de sonde d'ARP en raison d'une déconnexion non-gracieuse DHCP.

### Notes en implémentation :

- Le « ssg auto-logoff arp » et le « ssg auto-logoff icmp » sont des méthodes indésirables pour empêcher la réutilisation de session ou les problèmes de sécurité résultants. Le « ARP » et le « ICMP » variantes de la « automatique-déconnexion de ssg » envoient seulement un ARP ou le PING IMCP quand le trafic n'est pas vu sur la connexion SSG dans le « intervalle configuré, » le plus bas dont est 30 secondes. Si le DHCP loue une adresse IP précédemment utilisée dans 30 secondes, ou un utilisateur malveillant configure statiquement une adresse DHCP d'actuellement-limite dans 30 secondes, la session est réutilisée parce que SSG voit le trafic sur l'objet connexion, et la « automatique-déconnexion de ssg » n'appelle pas.
- Dans des tous les cas d'utilisation, la réutilisation de session n'est pas empêchée si un hôte malveillant exécute une adresse MAC charrient.

### Tableau 1 – Réutilisation et considérations liées à la sécurité de session dans des déploiements SSG/DHCP

| Commande | Fonction | Implications en matière de sécurité |
|---|---|---|
| **ssg auto-logoff icmp** de **ssg auto-logoff arp** **[correspondance-MAC-adresse]** [*secondes* | Enlève l'objet d'hôte SSG après panne de | Réutilise la session si le DHCP loue une adresse IP précédemment utilisée dans 30 secondes, ou un utilisateur malveillant |

| | | |
|---|---|---|
| **d'intervalle] [millisecondes de délai d'attente] [nombre de paquets] [*secondes d'*intervalle]** | PING d'ARP ou d'ICMP, qui est seulement envoyé après qu'aucun trafic ne soit vu sur la connexion SSG dans le « intervalle. » | configure statiquement une adresse DHCP d'actuellement-limite dans 30 secondes parce que SSG voit le trafic sur l'objet connexion, et la « automatique-déconnexion de ssg » n'appelle pas. |
| **ssg intercept dhcp** | Crée le SSG/DHCP Awareness qui permet la suppression de l'objet d'hôte SSG dans ces événements : Un DHCPRELEASE est reçu pour une adresse IP qui apparie un objet actif d'hôte. B. Le bail DHCP expire pour une adresse IP qui apparie un objet actif d'hôte. | Empêche des utilisateurs DHCP de la réutilisation des sessions SSG mais n'empêche pas les utilisateurs statiques de charrier des adresses DHCP ou la réutilisation des sessions SSG. |
| **update arp de TEST d'ip dhcp pool** | S'assure que le | Empêche toute la réutilisation de session |

| | | |
|---|---|---|
| | seul sous-système IOS capable de l'ajout ou de la suppression des entrées d'ARP est le sous-système de serveur DHCP. | une fois configuré avec le « ssg intercept dhcp. » Une fois configurée sans « ssg intercept dhcp, » si le DHCP loue une adresse IP précédemment utilisée, la réutilisation de session est encore possible. |
| **interface FastEthernet0/0 arp authorized** | Envoie des demandes périodiques d'ARP à tous les hôtes de s'assurer qu'elles sont encore en activité. Arrête apprendre dynamique d'ARP. | Permet la suppression de liaison DHCP et d'entrée d'ARP quand un utilisateur DHCP exécute une déconnexion non-gracieuse. |

## Informations connexes

- Support et documentation techniques - Cisco Systems