配置有DHCP安全的ARP， SSG端口套件主机密钥、SSG TCP重定向， SESM和SSG/DHCP感知的SSG互联网网关的呼叫流调试

目录

简介

本文焦点是运行SSG和DHCP以门户服务的SESM的IOS互联网网关。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

技术和功能概述

服务选择网关(SSG)

服务选择网关(SSG)是提供内联网、外联网和互联网连接对用户有宽带接入技术的，例如数字用户线路的服务提供商的一个交换解决方案(DSL)，电缆调制解调器或者无线允许同时存取对网络服务。

与Cisco Subscriber Edge Services Manager (SESM)一道的SSG工作。与SESM一起， SSG提供用户身份验证，服务选择和服务连接功能给网络服务的用户。使用一标准的Internet浏览器，用户与SESM Web应用程序呼应。

SESM在两个模式运行：

- RADIUS模式—此模式从RADIUS服务器得到用户和服务信息。在RADIUS模式的SESM类似于SSD。
- LDAP模式—对一个LDAP兼容目录的轻量级目录访问协议(LDAP)模式提供访问对于用户和服务档案信息。此模式也有SESM Web应用程序的高级功能并且使用一个基于任务的访问控制(RBAC)型号管理用户访问。

SSG波尔特套件主机密钥

SSG波尔特套件主机密钥关键功能提高通信和功能在SSG和SESM之间用使用主机源IP地址和源端口识别和监控用户的机制。

使用SSG波尔特套件主机密钥关键功能， SSG执行端口地址转换(PAT)和网络地址转换(NAT)在HTTP数据流在用户和SESM服务器之间。当用户发送HTTP数据包到SESM服务器时， SSG创建更改源IP地址对一已配置的SSG源IP地址并且更改来源TCP端口对SSG分配的端口的端口地图。SSG分配套件端口到每个用户，因为一个用户能有几同时TCP会话，当访问网页时。已分配波尔特套件和SSG源IP地址的主机密钥或者组合，独特识别每个用户。主机密钥是被传送的RADIUS信息包被发送在SESM服务器和SSG之间在用户IP供应商专用属性(VSA)。当SESM服务器发送对用户时的一回复， SSG翻译目的IP地址和目的地TCP端口符合端口映射。

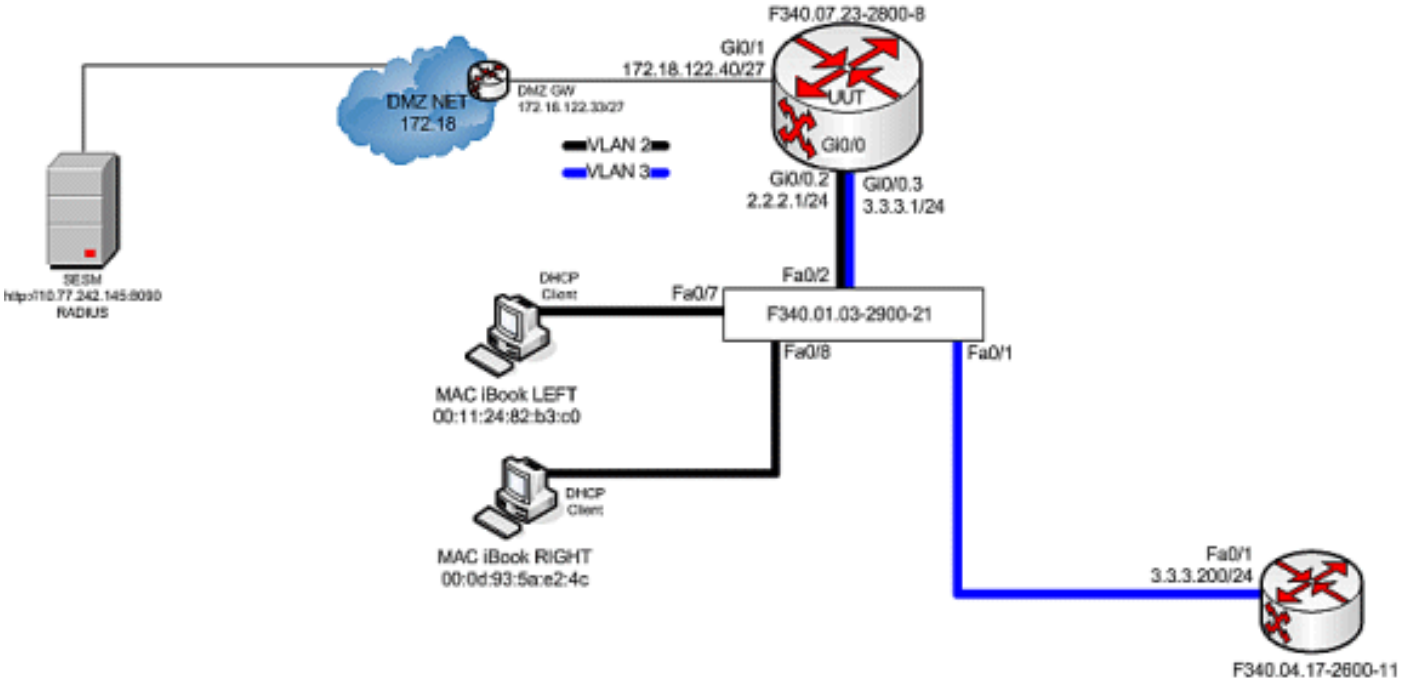
未认证的用户的SSG TCP重定向

如果用户未授权与服务提供商，未认证的用户的重定向重定向从用户的数据包。当一个未授权的用户尝试连接到在TCP端口的一服务(例如，对www.cisco.com)， SSG TCP重定向重定向数据包到俘虏门户(SESM或一组SESM设备)。SESM问题重定向对显示登录页的浏览器。用户登陆对SESM和验证并且授权。SESM然后提交有个性化的主页、服务提供商主页或者原始URL的用户。

DHCP 安全 IP 地址分配

DHCP安全IP地址分配功能引入功能绑ARP表条目到在DHCP数据库的动态主机配置协议(DHCP)租期上。此功能获取并且同步客户端的MAC地址对DHCP绑定，防止未授权的客户端或黑客伪装DHCP服务器和接管一个已授权客户端的DHCP租用。当此功能启用时，并且DHCP服务器分配IP地址到DHCP客户端， DHCP服务器添加安全ARP条目到与指定的IP地址和客户端的MAC地址的ARP表。此ARP条目不可能由任何其他动态ARP数据包更新，并且此ARP条目在已配置的租用时间的ARP表里存在或，只要租期是活跃的。当DHCP绑定超时时，被巩固的ARP条目可以由从DHCP客户端或DHCP服务器的一个明确终端消息仅删除。此功能可以为新的DHCP网络配置或用于升级当前网络的安全。此功能的配置不中断服务并且不是可视对DHCP客户端。

试验床图表



呼叫流调试

完成这些步骤：

1. 当首先被留下的MAC iBook连接以太网电缆对此网络时，租用在“F340.07.23-2800-8运行从IOS DHCP服务器的IP地址2.2.2.5/29”。

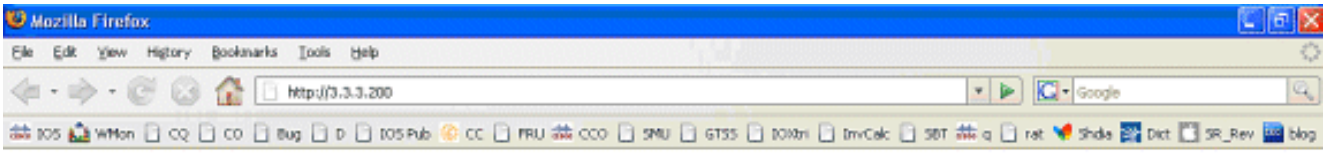
   debug ip dhcp server packet debug ssg dhcp events *Oct 13 20:24:04.073: SSG-DHCP-EVN: DHCP-DISCOVER event received. SSG-dhcp awareness feature enabled *Oct 13 20:24:04.073: DHCPD: DHCPDISCOVER received from client 0100.1124.82b3.c0 on interface GigabitEthernet0/0.2. *Oct 13 20:24:04.073: SSG-DHCP-EVN: 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. 在它顺利地租用IP地址2.2.2.5后， MAC iBook左打开Web浏览器并且指向它**http://3.3.3.200**，用于模拟已保护资源附加对SSG服务“distlearn”。SSG服务“distlearn”本地在SSG路由器“F340.07.23-2800-8”定义：

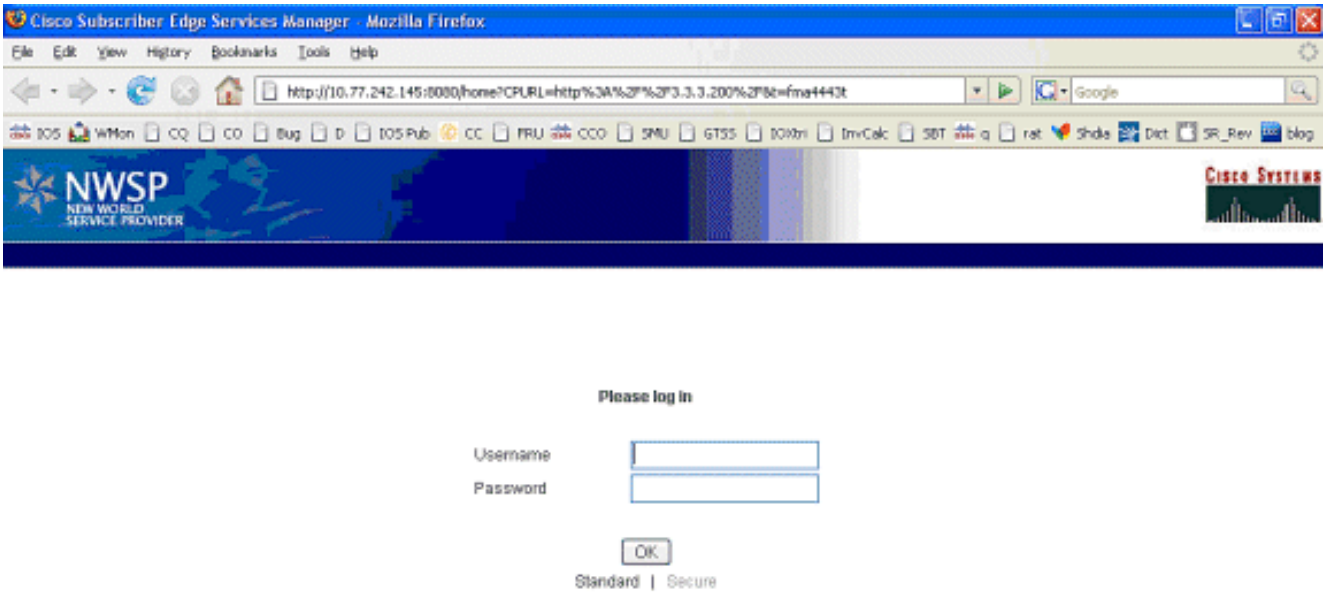
   local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255" 实际上，**http://3.3.3.200**是为“ip http server”配置的Cisco IOS路由器并且侦听在TCP 80，因此它基本上是Web服务器。在MAC iBook离开尝试浏览到**http://3.3.3.200后**，因为此连接是在接口的入口配置与“SSG方向下行”， SSG路由器首先检查一个活动SSG主机对象的存在HTTP请求的源IP地址的。由于这第一从IP地址2.2.2.5的这样请求， SSG主机对象不存在和往SESM的TCP重定向为主机2.2.2.5是例示的通过此配置：

   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-**

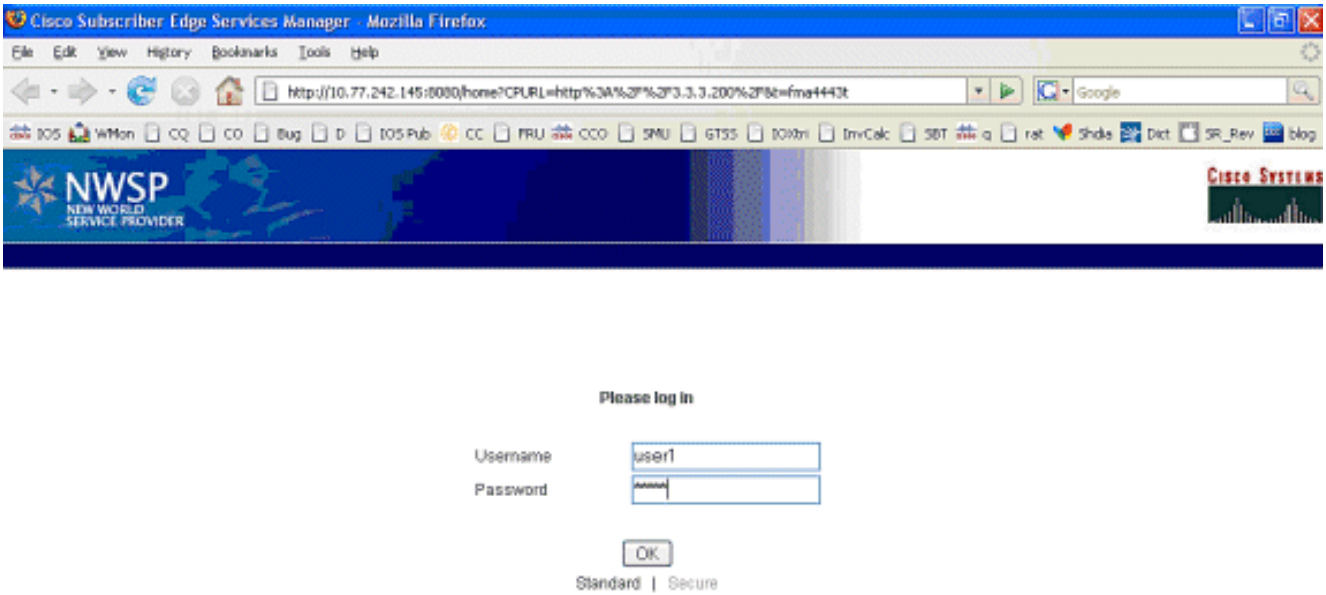
list ports to ssg_tr_unauth redirect unauthenticated-user to ssg_tr_unauth *If an SSG router receives a packets on an interface with "ssg direction downlink" configured, it first compares the Source IP address of the packet with the SSG Host Object Table. If an Active SSG Host Object matching the Source 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 这时，当http://3.3.3.200被输入时，在MAC iBook左岸堤防的浏览器看上去象这个：



在IOS SSG TCP和SESM HTTP重定向以后，屏幕如下所示：



3. 在对SESM的SSG TCP重定向和随后的HTTP重定向由SESM送回到被留下后的MAC iBook浏览器， MAC iBook左岸堤防进入**user1**作为用户名和**cisco**作为密码：



4. 在**OK按钮**被按后， SESM通过一份所有权基于RADIUS的协议发送SSG路由器这些凭证。

```
*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. 反过来， SSG路由器构件RADIUS访问请求信息包并且发送它对RADIUS验证**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. RADIUS回应**user1的**一Access-Accept，并且SSG主机对象在“F340.07.23-2800-8”创建：*Oct 13 20:25:02.081: RADIUS:

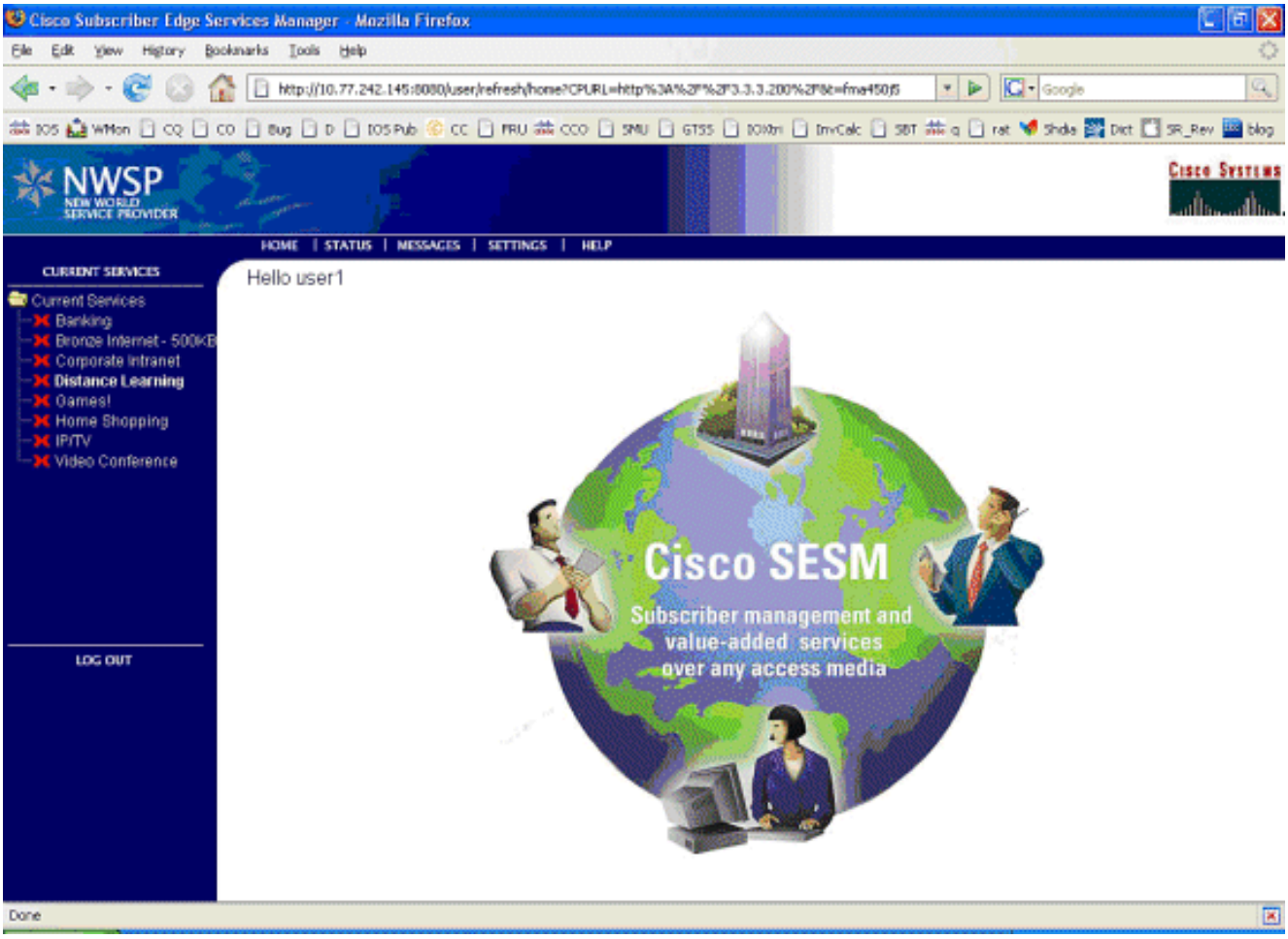
```
   Received from id 1645/11 10.77.242.145:1812,
   Access-Accept, len 273
*Oct 13 20:25:02.081: RADIUS:
   authenticator 52 7B 50 D7 F2 43 E6 FC -
   7E 3B 22 A4 22 A7 8F A6
*Oct 13 20:25:02.081: RADIUS:  Service-Type
   [6]   6   Framed         [2]
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [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. 这时， **user1**定义作为SSG主机对象，但是不访问任何SSG服务。MAC iBook左岸堤防提交与服务选择屏幕并且点击**远程教育**：



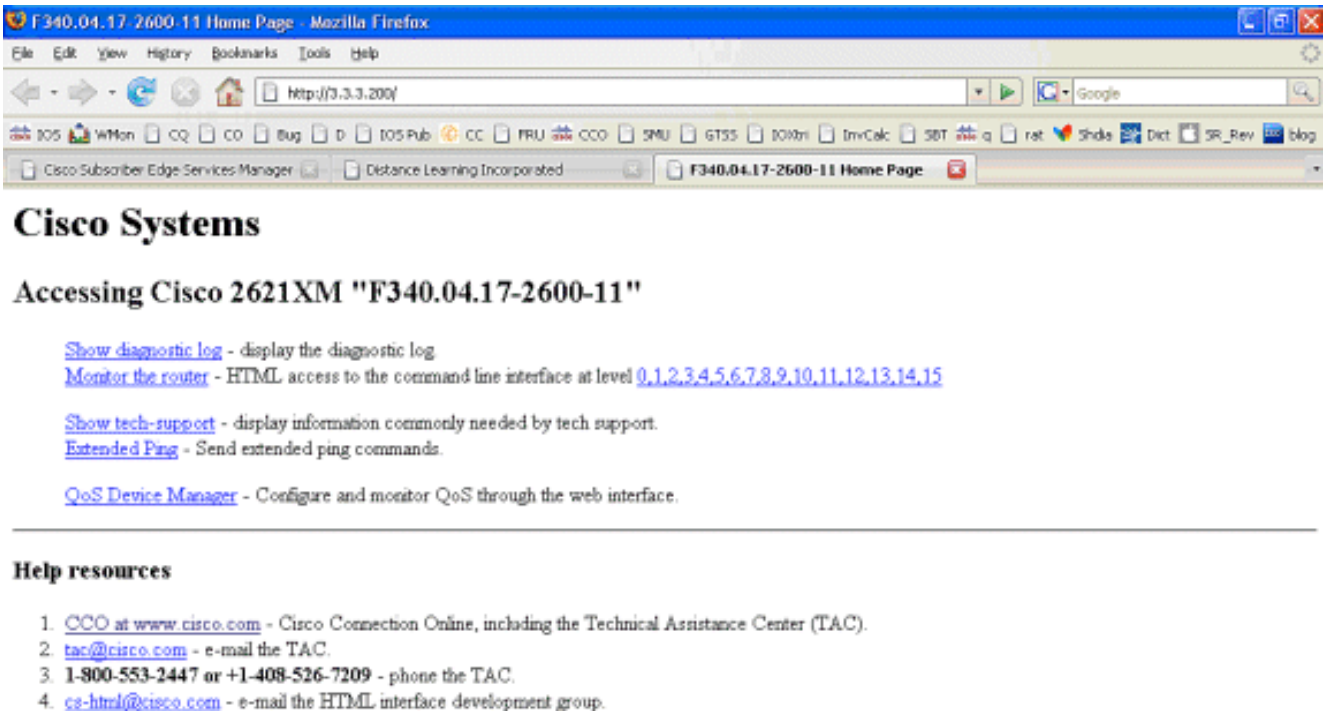
8. 在**远程教育**点击后， SESM方框通信到SSG路由器用控制通道：`debug ssg ctrl-events`

```
*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. SSG连接是UP，并且呼叫流完成。MAC iBook左岸堤防能顺利地浏览到**http://3.3.3.200**：



SSG与功能文档的路由器配置说明

```
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

安全和会话重新使用考虑事项

当您并用SSG和DHCP时，这些方案能允许允许未认证的访问巩固资源的有恶意的用户重新使用一个已验证SSG主机对象：

- 如果SSG/DHCP感知没有配置与"SSG截取dhcp"，一个新的DHCP用户能租用SSG主机对象仍然存在的一个早先租用的IP地址。因为从此新用户的第一TCP请求有一匹配，虽然过时，SSG匹配源IP地址的主机对象，此用户授权未经鉴定的使用已保护资源。这可以防止与"SSG截取dhcp"，导致SSG主机对象的删除，当二者之一发生时：DHCPRELEASE为匹配激活主机对象的IP地址接收。DHCP租用为匹配激活主机对象的IP地址超时。
- 如果DHCP用户交往租用的IP地址对恶意用户在一非优美的DHCP注销前，是DHCP注销DHCPRELEASE没有发送，恶意用户能静态配置计算机用此IP地址和重新使用SSG主机对象"SSG截取dhcp"是否配置。这可以防止与"SSG截取dhcp"和"在IOS DHCP池下"配置的更新arp的组合。"更新arp"保证唯一的IOS子系统能添加或删除ARP条目是DHCP服务器子系统。使用"更新arp"， IP对MAC DHCP绑定总是匹配在ARP表里绑定的IP对MAC。即使恶意用户静态有匹配SSG主机对象的一个配置的IP地址，流量没有允许输入SSG路由器。由于MAC地址不匹配当前DHCP绑定的MAC地址， IOS DHCP服务器防止ARP条目的创建。
- 当SSG和DHCP一起时配置， "SSG截取dhcp"和"更新arp"防止会话重新使用。当DHCP主机执行一非优美的注销时，最终非安全涉及的挑战是释放DHCP租用和ARP条目。"授权arp"在

“SSG方向下行”接口的配置导致定期ARP请求发送对所有主机确保他们是活跃的。如果无响应从这些定期ARP消息接收， DHCP绑定发布，并且IOS DHCP子系统清除ARP条目。
```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
arp authorized
arp probe interval 5 count 15
```
在本例中， ARP请求周期地发送刷新在Fa0/0的所有已知ARP条目每个5s。在15失败以后， DHCP绑定发布，并且IOS DHCP子系统清除ARP条目。在SSG中没有“授权arp”，如果DHCP主机执行一非优美的注销， DHCP租用，并且其相关的SSG主机对象依然是活动，直到此DHCP地址的租期超时，但是会话重新使用不发生，只要“SSG截取dhcp”配置全局。

“授权arp”关闭学习在配置的接口的动态ARP。在租期开始后，在有问题的接口的唯一的ARP条目是IOS DHCP服务器添加的那些。一旦租期终止，由于DHCP版本、租期有效期或者ARP探测器失败的收据由于一非优美的DHCP注销，这些ARP条目由IOS DHCP服务器然后清除。

实施注释：

- “SSG自动注销arp”和“ssg auto-logoff icmp”是防止会话重新使用或产生的安全问题的不理想的方法。“arp”和“icmp” “SSG仅自动注销”发送变形ARP或IMCP PING，当流量在已配置的“间隔内的SSG连接看不到”，最低是30秒。如果DHCP租约一个以前使用的IP地址在30秒以内或者恶意用户在30秒以内静态配置一个当前区域DHCP地址，重新使用会话，因为SSG看到在连接对象的流量，并且“SSG自动注销”不调用。
- 在所有使用案件中，如果一台有恶意的主机执行MAC地址欺骗，会话重新使用没有被防止。

表1 –会话重新使用和安全考虑在SSG/DHCP部署

命令	功能	安全影响
ssg自动注销arp [match-mac-address] [interval seconds] ssg auto-logoff icm	在ARP或ICMP PING的失败以后取消SSG主机对象，只被发送，在流量在“间隔内后的SSG连接没有被看到”。	重新使用会话，如果DHCP租约一个以前使用的IP地址在30秒以内或者恶意用户在30秒以内静态配置一个当前区域DHCP地址，因为SSG看到在连接对象的流量，并且“SSG自动注销”不调用。

p [timeout milliseconds] [packets number] [interval seconds]		
SSG截取dhcp	引起允许SSG主机对象删除在这些事件内的SSG/DHCP注意：DHCPRELEASE为匹配激活主机对象的IP地址接收。B.DHCP租用为匹配激活主机对象的IP地址超时。	防止DHCP用户SSG会话重新使用，但是不防止静态用户伪装DHCP地址或SSG会话重新使用。
ip dhcp pool TEST更新arp	保证唯一的IOS子系统有能力在ARP条目上新增内容或删除是DHCP服务器子系统。	防止所有会话重新使用，当配置与“SSG截取dhcp”。当配置，不用“SSG截取dhcp”，如果DHCP租约一个以前使用的IP地址，会话重新使用是可能的。
arp authorized接口的FastEthernet 0/0	对所有主机的发送定期ARP请求确保他们是活跃的。关闭动态ARP学习。	当DHCP用户执行一非优美的注销时，允许DHCP绑定和ARP条目删除。

相关信息

- 技术支持和文档 - Cisco Systems