

配置了DHCP安全ARP、SSG埠捆綁主機金鑰、SSG TCP重定向、SESM和SSG/DHCP感知的SSG網際網路網關的呼叫流調試

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[技術和功能概述](#)

[測試床圖](#)

[呼叫流調試](#)

[SSG路由器配置說明和功能文檔](#)

[安全性和會話重複使用注意事項](#)

[相關資訊](#)

簡介

本文檔重點介紹為門戶服務運行SSG和DHCP的IOS Internet網關。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

背景資訊

技術和功能概述

服務選取閘道 (SSG)

服務選擇閘道(SSG)是一種適用於使用寬頻存取技術(例如數位使用者線路(DSL)、纜線資料機或無線)為使用者提供Intranet、Extranet和網際網路連線以允許同時存取網路服務的服務提供者的交換解決方案。

SSG搭配Cisco Subscriber Edge Services Manager(ESM)使用。SSG搭配ESM共同使用，可以為網際網路服務的使用者提供使用者身分驗證、服務選取和服務連線功能。使用者使用標準的Internet瀏覽器與ESM Web應用程式互動。

ESM有兩種工作模式：

- RADIUS模式 — 此模式從RADIUS伺服器獲取使用者和服務資訊。RADIUS模式下的ESM與SSD類似。
- LDAP模式 — 輕量級目錄訪問協定(LDAP)模式提供對LDAP相容目錄的訪問，以獲取訂戶和服務配置檔案資訊。此模式還具有ESM Web應用的增強功能，並使用基於角色的訪問控制(RBAC)模型來管理使用者訪問。

SSG連線埠套件主機金鑰

SSG埠捆綁包主機金鑰功能使用主機源IP地址和源埠來識別和監控訂戶的機制，增強SSG和ESM之間的通訊和功能。

藉由SSG連線埠套件組合主機金鑰功能，SSG會在使用者和ESM伺服器之間的HTTP流量上執行連線埠位址轉譯(PAT)和網路位址轉譯(NAT)。當使用者向ESM伺服器傳送HTTP資料包時，SSG會建立一個埠對映，將源IP地址更改為已配置的SSG源IP地址，並將源TCP埠更改為SSG分配的埠。SSG將連線埠套件組合分配給每個使用者，因為一個使用者存取網頁時可以有多個同時的TCP作業階段。分配的主機金鑰或埠捆綁包和SSG源IP地址的組合可唯一標識每個使用者。主機金鑰是在ESM伺服器和SSG之間以訂戶IP廠商專用屬性(VSA)傳送的RADIUS封包中承載。當ESM伺服器向使用者傳送回覆時，SSG將根據埠對映轉換目標IP地址和目標TCP埠。

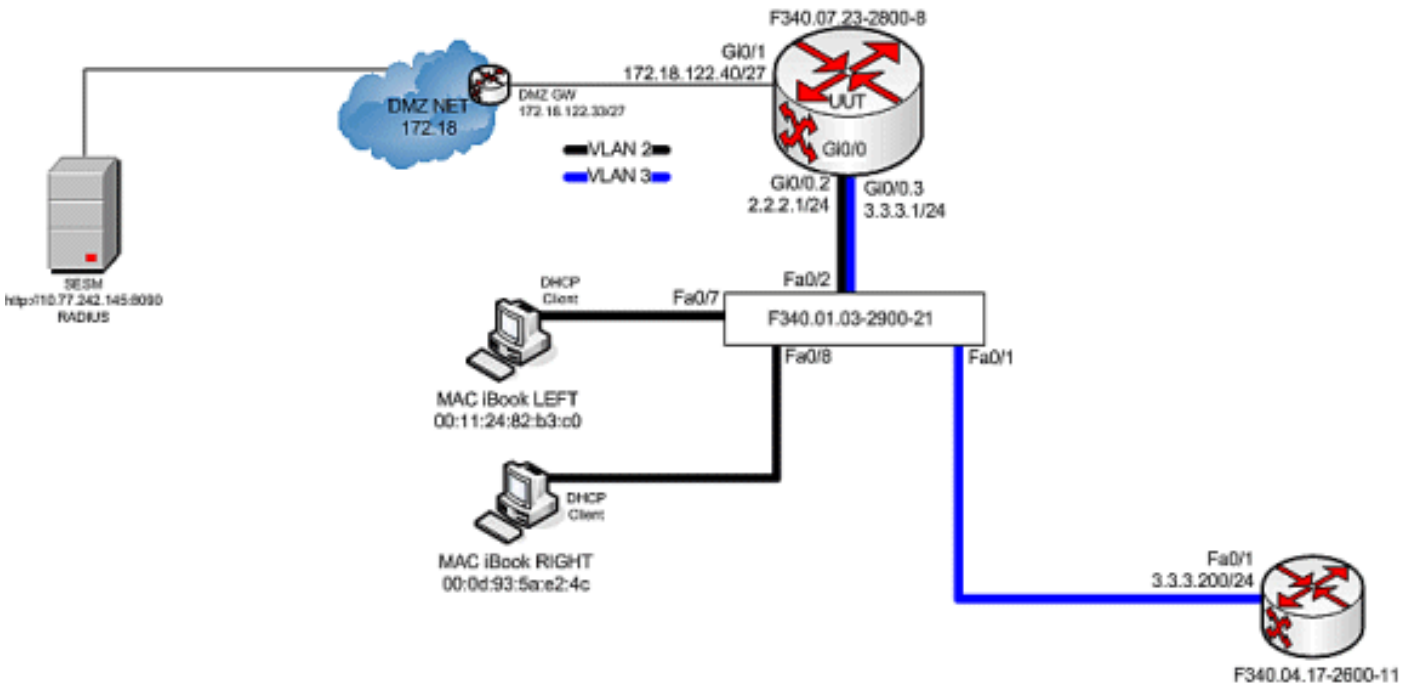
適用於未驗證使用者的SSG TCP重新導向

如果使用者未獲得服務提供商授權，則未經身份驗證的使用者的重定向會重定向來自該使用者的資料包。當未經授權的使用者嘗試連線到TCP埠上的服務時(例如連線到www.cisco.com)，SSG TCP重定向會將資料包重定向到強制網路門戶 (ESM或一組ESM裝置)。ESM會發出重新導向至瀏覽器以顯示登入頁面。使用者登入到ESM並經過驗證和授權。然後，ESM會為使用者呈現個人化首頁、服務提供者首頁或原始URL。

DHCP安全IP地址分配

DHCP安全IP地址分配功能引入了將ARP表條目安全到DHCP資料庫中動態主機配置協定(DHCP)租約的功能。此功能可將客戶端的MAC地址保護並同步到DHCP繫結，防止未經授權的客戶端或駭客欺騙DHCP伺服器並接管授權客戶端的DHCP租用。啟用此功能後，DHCP伺服器為DHCP客戶端分配IP地址時，DHCP伺服器會向ARP表中新增一個安全的ARP條目，其中包含分配的IP地址和客戶端的MAC地址。此ARP條目無法由任何其他動態ARP資料包更新，此ARP條目在配置的租用時間內，或者只要租用處於活動狀態，就會存在於ARP表中。只有在DHCP繫結到期時，從DHCP客戶端或DHCP伺服器發出顯式終止消息才能刪除受保護的ARP條目。此功能可配置用於新的DHCP網路或用於升級當前網路的安全性。此功能的配置不會中斷服務，對DHCP客戶端不可見。

測試床圖



呼叫流調試

請完成以下步驟：

1. 當MAC iBook LEFT首次將乙太網電纜連線到此網路時，它從運行在「F340.07.23-2800-8」上的IOS DHCP伺服器租用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 DHCP OFFER
  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. 成功租用IP地址2.2.2.5後，MAC iBook LEFT會開啟一個Web瀏覽器，並將其指向 <http://3.3.3.200>，該瀏覽器用於模擬與SSG服務「distlearn」繫結的受保護資源。SSG服務「distlearn」在SSG路由器「F340.07.23-2800-8」中本地定義：

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

實際上，<http://3.3.3.200>是為「ip http server」配置並偵聽TCP 80的Cisco IOS路由器，因此它基本上是Web伺服器。在MAC iBook LEFT嘗試瀏覽<http://3.3.3.200>後，由於此連線是配置了「ssg direction downlink」的介面上的輸入，因此SSG路由器首先檢查是否存在活動SSG主機對象以獲取HTTP請求的源IP地址。由於這是來自IP位址2.2.2.5的第一個此類要求，因此SSG主機物件不存在，且針對主機2.2.2.5的TCP重新導向透過以下設定進行例項化：

```
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
```

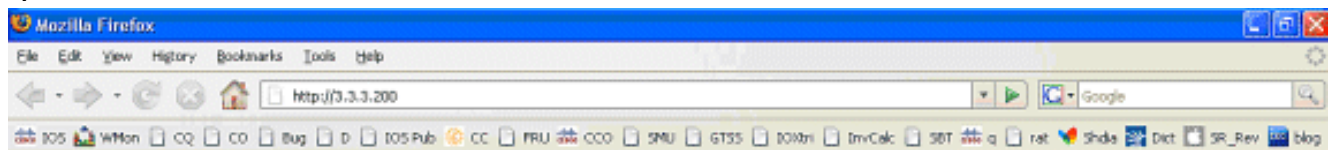
The initial HTTP request from 2.2.2.5 had a source TCP Port of 49273 and a destination IP

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
```

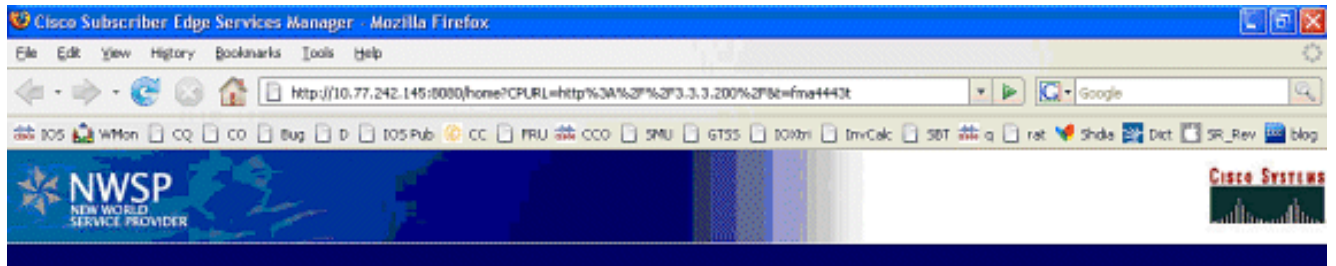
此時，輸入http://3.3.3.200時，MAC iBook Left上的瀏覽器將如下所示

:



IOS SSG TCP和SESM HTTP重新導向後，畫面如下所示

:



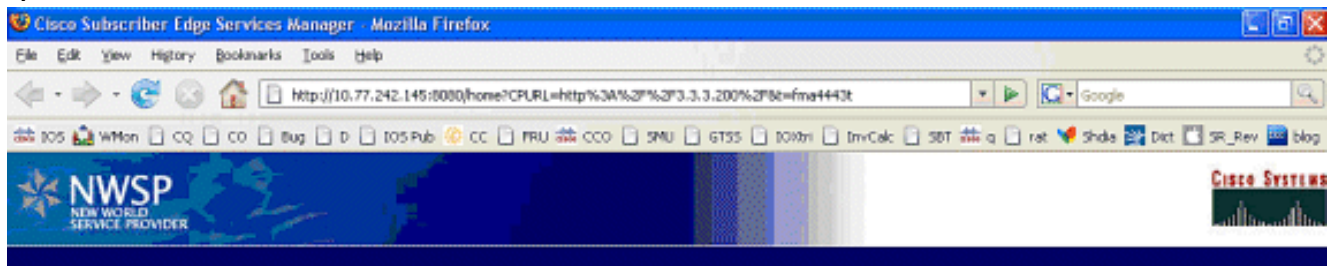
Please log in

Username
Password

OK

Standard | Secure

3. SSG TCP重新導向至SESM以及隨後SESM傳送回MAC iBook Left瀏覽器的HTTP重新導向後，MAC iBook Left會輸入user1作為使用者名稱，cisco作為密碼
:



Please log in

Username
Password

OK

Standard | Secure

4. 按下OK按鈕後，SESM會通過基於RADIUS的專有協定向SSG路由器傳送這些憑證。

```
*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. 反過來，SSG路由器建立RADIUS存取要求封包並將其傳送到RADIUS以驗證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使用user1的Access-Accept進行響應，並在「F340.07.23-2800-8」中建立SSG主機對象：

```
*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

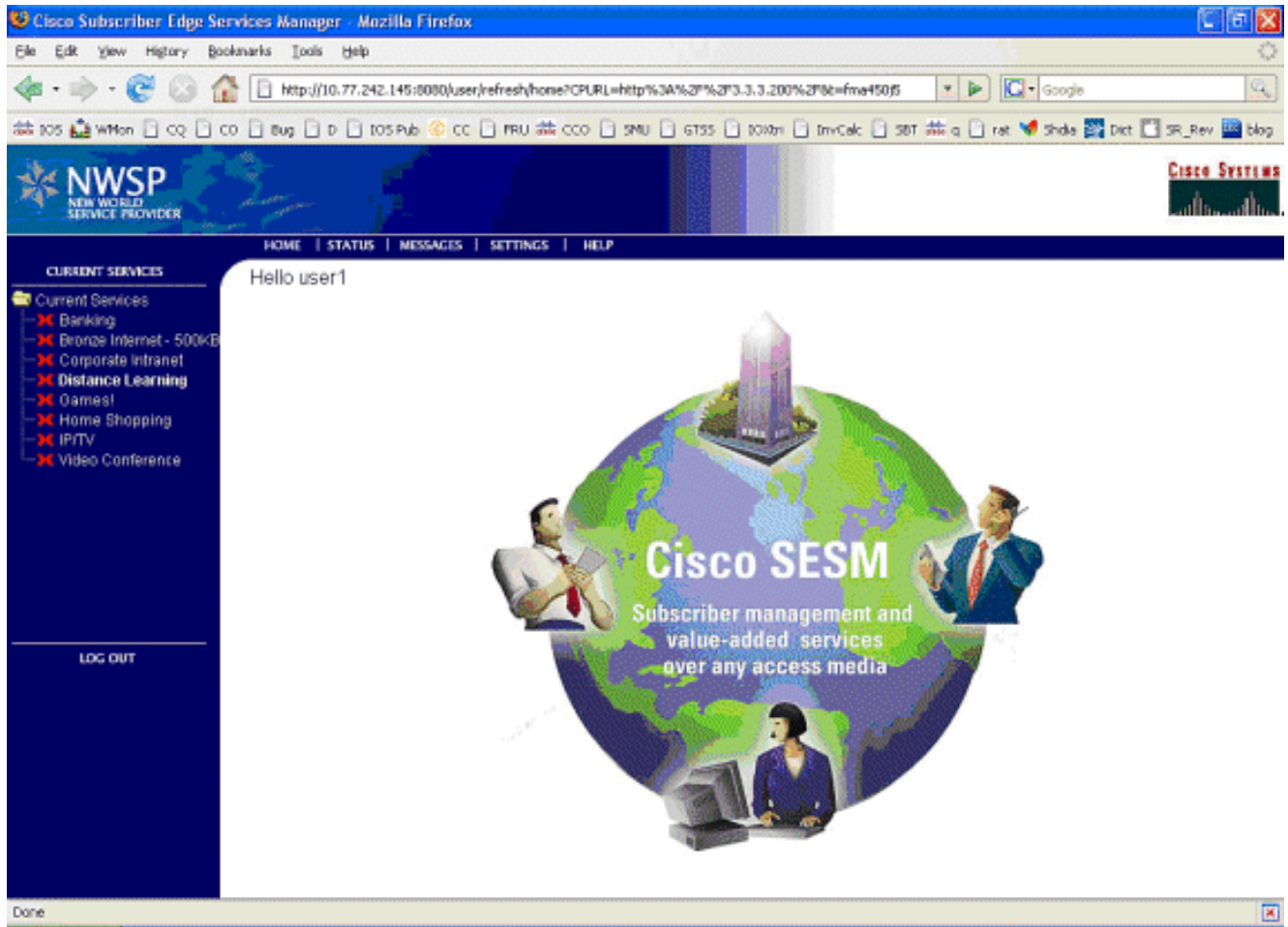
F340.07.23-2800-8#**show ssg host 2.2.2.5**

----- 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. 此時，**user1**被定義為SSG主機對象，但尚未訪問任何SSG服務。MAC iBook Left顯示服務選擇螢幕，並點選**Distance**

Learning:



8. 按一下Distance Learning後，SESM框會與控制通道與SSG路由器通訊：

```
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連線已啟動，呼叫流程已完成。MAC iBook Left可以成功瀏覽

<http://3.3.3.200/>:



Cisco Systems

Accessing Cisco 2621XM "F340.04.17-2600-11"

[Show diagnostic log](#) - display the diagnostic log

[Monitor the router](#) - HTML access to the command line interface at level [0](#),[1](#),[2](#),[3](#),[4](#),[5](#),[6](#),[7](#),[8](#),[9](#),[10](#),[11](#),[12](#),[13](#),[14](#),[15](#)

[Show tech-support](#) - display information commonly needed by tech support.

[Extended Ping](#) - Send extended ping commands.

[QoS Device Manager](#) - Configure and monitor QoS through the web interface.

Help resources

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447** or **+1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

SSG路由器配置說明和功能文檔

```
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 unreachable 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
```

安全性和會話重複使用注意事項

當您同時使用SSG和DHCP時，以下情況允許惡意使用者重複使用允許未經身份驗證訪問安全資源的已驗證SSG主機對象：

- 如果未使用「`ssg intercept dhcp`」配置SSG/DHCP感知，則新的DHCP使用者可以租用先前租用的IP地址，該IP地址仍存在SSG主機對象。由於來自此新使用者的第一個TCP請求具有與源IP地址匹配的（儘管已過期）SSG主機對象，因此授予此使用者未經身份驗證的使用受保護資源的許可權。可以使用「`ssg intercept dhcp`」阻止這種情況，這樣會在發生以下兩種情況時刪除SSG主機對象：收到與活動主機對象匹配的IP地址的DHCPRELEASE。與活動主機對象匹配的IP地址的DHCP租約到期。
- 如果DHCP使用者在未正常的DHCP註銷（即未傳送DHCPRELEASE的DHCP註銷）之前將租用IP地址關聯到惡意使用者，則無論是否配置了「`ssg intercept dhcp`」，惡意使用者可以使用此IP地址靜態配置電腦並重複使用SSG主機對象。在IOS DHCP池下配置了「`ssg intercept dhcp`」和「`update arp`」組合，可防止出現這種情況。「`update arp`」可確保唯一能夠新增或刪除ARP條目的IOS子系統是DHCP伺服器子系統。使用「更新arp」時，IP到MAC DHCP繫結始終與ARP表中的IP到MAC繫結匹配。即使惡意使用者具有與SSG主機對象匹配的靜態配置的IP地址，也不允許流量進入SSG路由器。由於MAC地址與當前的DHCP繫結的MAC地址不匹配，因此IOS DHCP伺服器會阻止建立ARP條目。
- 同時配置SSG和DHCP時，「`ssg intercept dhcp`」和「`update arp`」可防止會話重複使用。最後一個與安全性無關的挑戰是在DHCP主機執行非平穩註銷時釋放DHCP租用和ARP條目。在「`ssg`方向下行鏈路」介面上配置「`授權arp`」會導致定期向所有主機傳送的ARP請求，以確保它們仍然處於活動狀態。如果沒有收到這些定期ARP消息的響應，則釋放DHCP繫結，IOS DHCP子系統清除該ARP條目。

```
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，每5秒定期傳送一個ARP請求，以刷新Fa0/0上的所有已知ARP條目。15次故障後，DHCP繫結被釋放，IOS DHCP子系統清除該ARP條目。在沒有「`授權arp`」的SSG環境中，如果DHCP主機執行非優雅註銷，則DHCP租用及其關聯的SSG主機對象將保持活動狀態，直到此DHCP地址的租用到期，但只要全域性配置「`ssg intercept dhcp`」，會話不會重複使用。

「`授權的arp`」會關閉配置它的介面上的動態ARP學習。該介面上唯一的ARP條目是IOS DHCP伺服器在租用啟動後新增的條目。一旦租約終止，這些ARP條目會被IOS DHCP伺服器清除，原因可能是收到DHCP釋放、租約到期或由於不正常的DHCP註銷而導致ARP探測失敗。

實施說明：

- 「`ssg auto-logoff arp`」和「`ssg auto-logoff icmp`」是不理想的方法，用於防止會話重複使用或導致安全問題。「`ssg auto-logoff`」的「`arp`」和「`icmp`」變體僅當SSG連線上在配置的「時間間隔」內看不到流量時傳送ARP或IMCP PING，其中最小的為30秒。如果DHCP在30秒內租用以前使用的IP地址，或者惡意使用者在30秒內靜態配置當前繫結的DHCP地址，會話將被重複使用，因為SSG看到連線對象上的流量，並且「`ssg auto-logoff`」不會呼叫。

- 在所有使用情況下，如果惡意主機執行MAC地址欺騙，則不會阻止會話重複使用。

表1 - SSG/DHCP部署中的會話重複使用和安全注意事項

指令	功能	安全影響
s s g a u t o - l o g o f f a r p [m a t c h - m a c - a d d r e s s] i n t e r v a l s e c o n d s] s s g a u t o - l o g o f	<p>在ARP或ICMP PING失敗後刪除SSG主機對象，後者僅在「間隔」內SSG連線上未出現流量時傳送。</p>	<p>如果DHCP在30秒內租用以前使用的IP地址，或者惡意使用者在30秒內靜態配置當前繫結的DHCP地址（因為SSG看到連線對象上的流量），並且不呼叫「ssg自動註銷」，則重新使用會話。</p>

<p>f i c m p [t i m e o u t m illi s e c o n d s] [p a c k e t s n u m b e r] [i n t e r v a l s e c o n d s]</p>		
<p>s s g i n t e r c e p t d h c</p>	<p>建立SSG/DHCP感知，允許在這些事件中刪除SSG主機對象：收到與活動主機對象匹配的IP地址的DHCPRELEASE。 B.與活動主機對象匹配的IP地址的DHCP租約到期。</p>	<p>防止DHCP使用者重複使用SSG會話，但並不防止靜態使用者偽裝DHCP地址或重複使用SSG會話。</p>

p		
ip d h c p p o l T E S T u p d a t e a r p	<p>確保DHCP伺服器子系統是唯一能夠新增或刪除ARP條目的IOS子系統。</p>	<p>使用「<code>ssg intercept dhcp</code>」配置時防止所有會話重新使用。如果配置時沒有「<code>ssg intercept dhcp</code>」，則如果DHCP租用以前使用的IP地址，仍可以重複使用會話。</p>
in te r f a c e F a s t E t h e r n e t 0/ 0 a r p a u t h o r i z e d	<p>定期向所有主機傳送ARP請求，以確保它們仍然處於活動狀態。關閉動態ARP學習。</p>	<p>允許在DHCP使用者執行非平穩註銷時刪除DHCP繫結和ARP條目。</p>

[相關資訊](#)

- [技術支援與文件 - Cisco Systems](#)