

DHCP Secure ARP, SSG Port-Bundle 호스트 키, SSG TCP 리디렉션, SESM 및 SSG/DHCP 인식 기능을 사용하여 구성된 SSG 인터넷 게이트웨이의 통화 흐름 디버깅

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[기술 및 기능 개요](#)

[테스트베드 다이어그램](#)

[통화 흐름 디버그](#)

[SSG 라우터 구성 설명\(기능 문서 포함\)](#)

[보안 및 세션 재사용 고려 사항](#)

[관련 정보](#)

소개

이 문서의 핵심은 포털 서비스를 위해 SSG 및 DHCP와 SESM을 함께 실행하는 IOS 인터넷 게이트웨이입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

배경 정보

기술 및 기능 개요

SSG(Service Selection Gateway)

SSG(Service Selection Gateway)는 DSL(Digital Subscriber Lines), 케이블 모뎀 또는 무선과 같은 광대역 액세스 기술을 사용하는 가입자에게 인트라넷, 엑스트라넷 및 인터넷 연결을 제공하는 통신 사업자를 위한 스위칭 솔루션입니다.

SSG는 Cisco SESM(Subscriber Edge Services Manager)과 함께 작동합니다. SSG는 SESM과 함께 인터넷 서비스 가입자에게 가입자 인증, 서비스 선택 및 서비스 연결 기능을 제공합니다. 가입자는 표준 인터넷 브라우저를 사용하여 SESM 웹 애플리케이션과 상호 작용합니다.

SESM은 두 가지 모드로 작동합니다.

- RADIUS 모드 - 이 모드는 RADIUS 서버에서 가입자 및 서비스 정보를 가져옵니다. RADIUS 모드의 SESM은 SSD와 유사합니다.
- LDAP 모드—LDAP(Lightweight Directory Access Protocol) 모드는 가입자 및 서비스 프로필 정보를 위한 LDAP 호환 디렉토리에 대한 액세스를 제공합니다. 또한 이 모드는 SESM 웹 애플리케이션에 대한 향상된 기능을 제공하며 RBAC(Role-Based Access Control) 모델을 사용하여 가입자 액세스를 관리합니다.

SSG 포트 번들 호스트 키

SSG Port-Bundle Host Key 기능은 호스트 소스 IP 주소와 소스 포트를 사용하여 가입자를 식별하고 모니터링하는 메커니즘을 통해 SSG와 SESM 간의 통신 및 기능을 향상시킵니다.

SSG는 SSG Port-Bundle Host Key 기능을 사용하여 가입자와 SESM 서버 간의 HTTP 트래픽에서 PAT(port-address translation) 및 NAT(network-address translation)를 수행합니다. 가입자가 SESM 서버로 HTTP 패킷을 전송하면 SSG는 소스 IP 주소를 구성된 SSG 소스 IP 주소로 변경하고 소스 TCP 포트를 SSG에서 할당된 포트 번호로 변경하는 포트 맵을 만듭니다. SSG는 웹 페이지에 액세스할 때 한 가입자가 여러 개의 동시 TCP 세션을 가질 수 있으므로 각 가입자에 포트 번들을 할당합니다. 할당된 호스트 키 또는 포트 번들 및 SSG 소스 IP 주소의 조합은 각 가입자를 고유하게 식별합니다. 호스트 키는 SESM 서버와 SSG 간에 전송되는 RADIUS 패킷에서 VSA(Subscriber IP vendor-specific attribute) 로 전달됩니다. SESM 서버가 가입자에게 응답을 보낼 때 SSG는 포트 맵에 따라 대상 IP 주소 및 대상 TCP 포트를 변환합니다.

인증되지 않은 사용자를 위한 SSG TCP 리디렉션

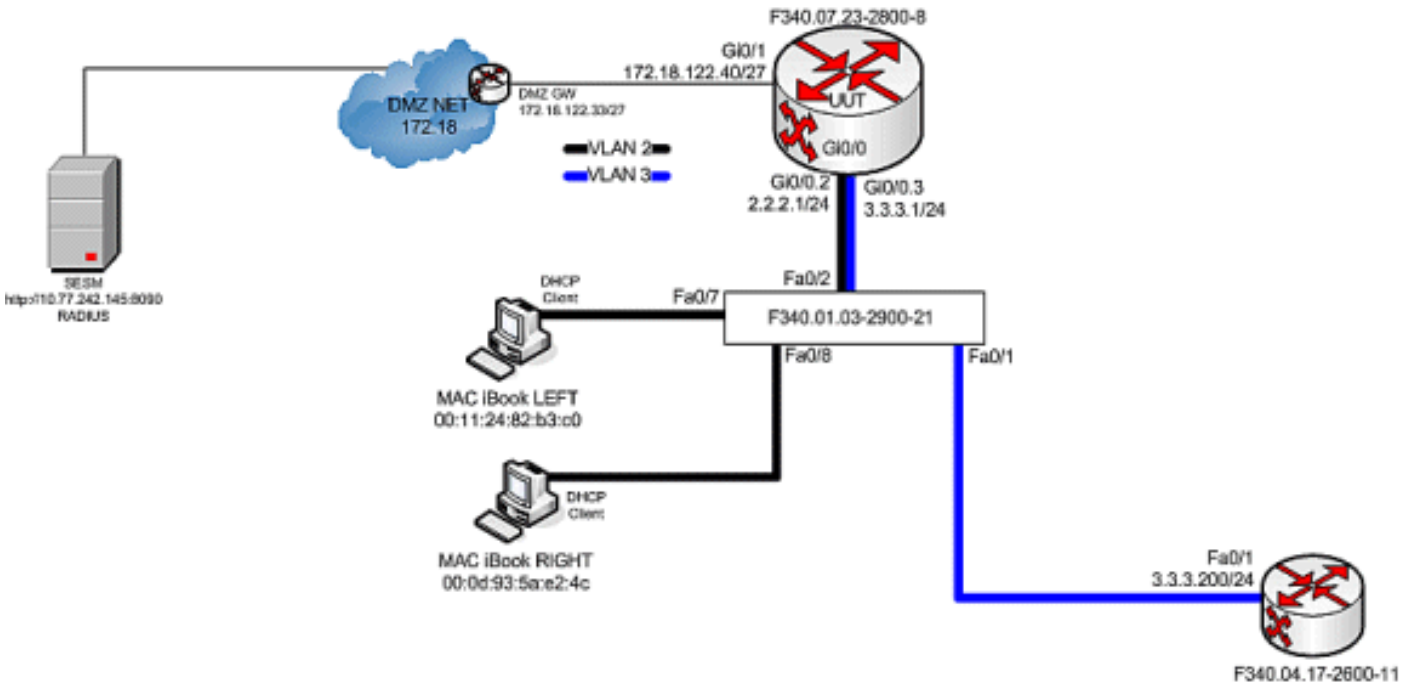
인증되지 않은 사용자에게 대한 리디렉션은 사용자가 서비스 제공자에게 권한을 부여하지 않은 경우 사용자로부터 패킷을 리디렉션합니다. 인증되지 않은 가입자가 TCP 포트의 서비스에 연결하려고 시도하면(예: www.cisco.com) SSG TCP 리디렉션은 패킷을 종속 포털(SESM 또는 SESM 디바이스 그룹)으로 리디렉션합니다. SESM은 로그인 페이지를 표시하기 위해 브라우저에 리디렉션을 발급합니다. 가입자가 SESM에 로그인하고 인증되고 인증됩니다. 그런 다음 SESM은 가입자에게 개인 설정된 홈 페이지, 서비스 제공자 홈 페이지 또는 원래 URL을 표시합니다.

DHCP 보안 IP 주소 할당

DHCP Secure IP Address Assignment 기능은 DHCP 데이터베이스의 DHCP(Dynamic Host Configuration Protocol) 임대 테이블 항목을 보호하는 기능을 제공합니다. 이 기능은 클라이언트의 MAC 주소를 DHCP 바인딩에 보호 및 동기화하여 권한이 없는 클라이언트 또는 해커가

DHCP 서버를 스푸핑하고 권한이 있는 클라이언트의 DHCP 임대를 인수하는 것을 방지합니다. 이 기능이 활성화되고 DHCP 서버가 DHCP 클라이언트에 IP 주소를 할당하면 DHCP 서버는 지정된 IP 주소와 클라이언트의 MAC 주소를 가진 ARP 테이블에 보안 ARP 항목을 추가합니다. 이 ARP 항목은 다른 동적 ARP 패킷으로 업데이트할 수 없으며, 구성된 리스 시간 또는 임대가 활성 상태인 경우 ARP 테이블에 이 ARP 항목이 있습니다. DHCP 바인딩이 만료될 때 DHCP 클라이언트 또는 DHCP 서버의 명시적 종료 메시지만 보안 ARP 항목을 삭제할 수 있습니다. 이 기능은 새 DHCP 네트워크에 대해 구성하거나 현재 네트워크의 보안을 업그레이드하는 데 사용할 수 있습니다. 이 기능의 컨피그레이션은 서비스를 중단하지 않으며 DHCP 클라이언트에 표시되지 않습니다.

테스트베드 다이어그램



통화 흐름 디버그

다음 단계를 완료하십시오.

1. MAC iBook LEFT가 먼저 이더넷 케이블을 이 네트워크에 연결할 때 "F340.07.23-2800-8"에서 실행되는 IOS DHCP 서버에서 IP 주소 2.2.2.5/29를 임대합니다.

```
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:
```

```

DHCPCD: 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:
  DHCPCD: Can't find any hostname to update
*Oct 13 20:24:05.073:
  DHCPCD: Sending DHCPACK to client 0100.1124.82b3.c0 (2.2.2.5).
*Oct 13 20:24:05.073:
  DHCPCD: creating ARP entry (2.2.2.5, 0011.2482.b3c0).
*Oct 13 20:24:05.073:
  DHCPCD: 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/ Hardware address/ User name	Lease expiration	Type
2.2.2.5	0100.1124.82b3.c0	Oct 13 2008 08:37 PM	Automatic

2. IP 주소 2.2.2.5을 성공적으로 임대한 후 MAC iBook LEFT는 웹 브라우저를 열고 <http://3.3.3.200>에 가리키며, 이는 SSG 서비스 "distlearn"에 연결된 보호된 리소스를 시뮬레이션하는 데 사용됩니다. SSG 서비스 "distlearn"은 SSG 라우터 "F340.07.23-2800-8"에서 로컬로 정의됩니다.

```
local-profile distlearn
```

```
attribute 26 9 251 "R3.3.3.200;255.255.255.255"
```

실제로 <http://3.3.3.200>는 "ip http server"로 구성되어 TCP 80에서 수신 대기하는 Cisco IOS 라우터이므로 기본적으로 웹 서버입니다. MAC iBook LEFT가 <http://3.3.3.200>로 찾아보기를 시도한 후, 이 연결이 "ssg direction downlink"로 구성된 인터페이스에서 인그레스(ingress)이므로 SSG 라우터는 먼저 HTTP 요청의 소스 IP 주소에 대해 활성 SSG 호스트 개체가 있는지 확인합니다. 이는 IP 주소 2.2.2.5의 첫 번째 요청이므로 SSG 호스트 개체가 없으며 SESM에 대한 TCP 리디렉션이 이 구성을 통해 호스트 2.2.2.5에 대해 인스턴스화됩니다.

```
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:
```

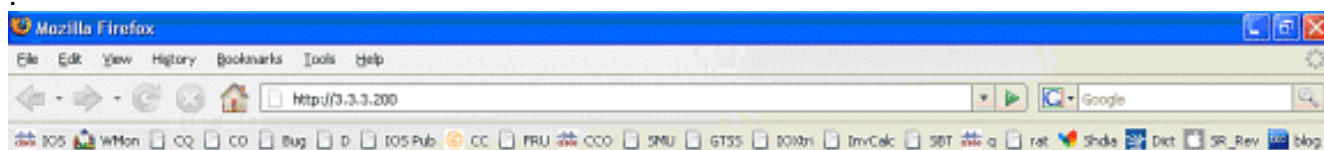
```
Downlink Interface: GigabitEthernet0/0.2
```

```
TCP remapping Host:2.2.2.5 to server:10.77.242.145 on port:8090
```

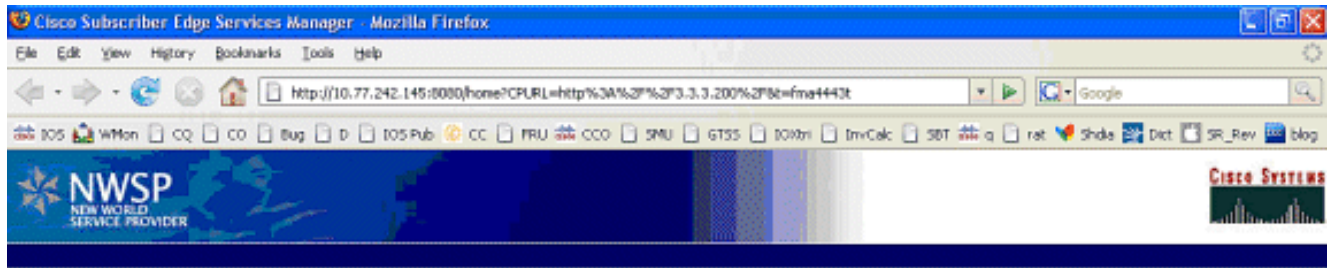
```
The initial HTTP request from 2.2.2.5 had a source TCP Port of 49273 and a destination IP address of 3.3.3.200 and TCP port of 80. Because of the SSG TCP Redirect, the destination IP header is overwritten with the socket of the SESM server 10.77.242.145:8090. If Port Bundle Host Key were NOT configured, 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
```

이 시점에서 MAC iBook Left의 브라우저는 http://3.3.3.200을 입력할 때 다음과 같습니다



IOS SSG TCP 및 SESM HTTP가 리디렉션되면 화면이 다음과 같이 표시됩니다



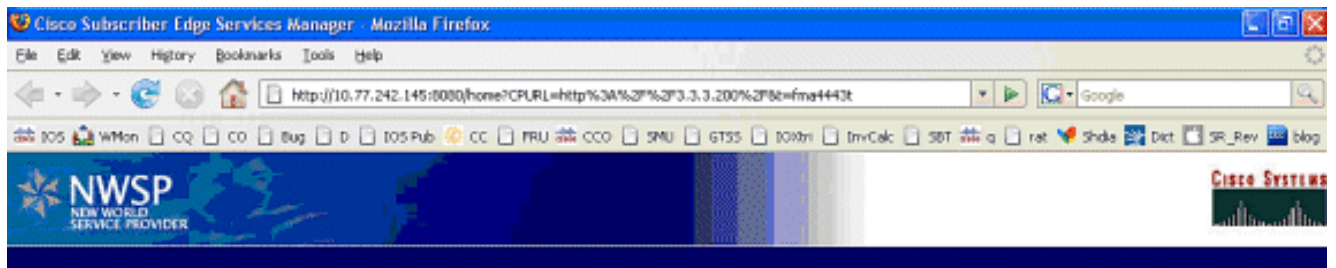
Please log in

Username
 Password

OK

Standard | Secure

3. SSG TCP가 SESM으로 리디렉션되고 SESM이 MAC iBook Left의 브라우저에 다시 보낸 후속 HTTP 리디렉션이 발생하면 MAC iBook Left는 **user1**을 사용자 이름으로 입력하고 **cisco**를 비밀번호로 입력합니다



Please log in

Username
 Password

OK

Standard | Secure

4. OK 버튼이 푸시되면 SESM은 독점적 RADIUS 기반 프로토콜을 통해 이러한 자격 증명을 SSG 라우터로 전송합니다.

```
*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. SSG 라우터는 RADIUS Access-Request Packet을 작성하여 RADIUS에 보내 user1을 인증합니다.

```
*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. RADIUS는 user1에 대한 액세스-수락으로 응답하며 SSG 호스트 개체는 "F340.07.23-2800-8"에서 생성됩니다.

```
*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. 이때 **user1**은 SSG 호스트 개체로 정의되지만 아직 SSG 서비스에 액세스할 수 없습니다. MAC iBook Left에는 Service Selection(서비스 선택) 화면이 표시되며 Distance Learning(원격 학습)을 클릭합니다


```
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
```

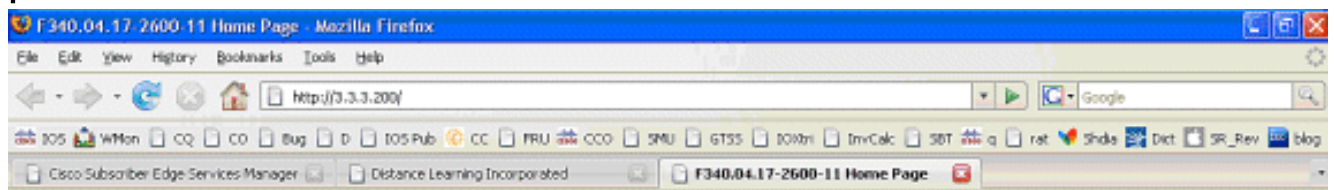
```
User last activity at:
    *20:41:04.000 UTC Mon Oct 13 2008
Connection Traffic Statistics:
    Input Bytes = 420, Input packets = 5
    Output Bytes = 420, Output packets = 5
Session policing disabled
```

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 연결이 작동되고 통화 흐름이 완료되었습니다. MAC iBook Left는 http://3.3.3.200으로 이
동합니다



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. cg-html@cisco.com - e-mail the HTML interface development group.

SSG 라우터 구성 설명(기능 문서 포함)

```
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
```

보안 및 세션 재사용 고려 사항

SSG와 DHCP를 함께 사용하는 경우, 이러한 시나리오를 통해 악의적인 사용자가 인증되지 않은 액세스를 통해 안전한 리소스에 대한 액세스를 허용하는 인증된 SSG 호스트 객체를 재사용할 수 있습니다.

- SSG/DHCP 인식이 "ssg intercept dhcp"로 구성되지 않은 경우, 새 DHCP 사용자는 SSG 호스트 객체가 여전히 존재하는 전에 임대한 IP 주소를 임대해 줄 수 있습니다. 이 새 사용자의 첫 번째 TCP 요청에 일치하는 항목이 있지만, 소스 IP 주소와 일치하는 SSG 호스트 객체가 오래되어 이 사용자에게 보호된 리소스의 인증되지 않은 사용이 허가됩니다. "ssg intercept dhcp"를 사용하면 이러한 작업을 방지할 수 있습니다. 그러면 다음 중 하나가 발생할 때 SSG 호스트 객체가 제거됩니다. 활성 호스트 객체와 일치하는 IP 주소에 대해 DHCPRELEASE가 수신됩니다. DHCP 리스는 활성 호스트 객체와 일치하는 IP 주소에 대해 만료됩니다.
- DHCP 사용자가 DHCP 로그아웃(DHCPRELEASE가 전송되지 않는 DHCP 로그아웃)이 되기 전에 임대한 IP 주소를 악의적인 사용자에게 연계하는 경우, 악의적인 사용자는 이 IP 주소로 시스템을 정적으로 구성하고 "ssg intercept dhcp"가 구성되었는지 여부에 관계없이 SSG 호스트 객체를 재사용할 수 있습니다. 이는 IOS DHCP 풀 아래에 구성된 "ssg intercept dhcp" 및 "update arp"의 조합으로 방지할 수 있습니다. "update arp"는 ARP 엔트리를 추가하거나 제거할 수 있는 유일한 IOS 하위 시스템이 DHCP 서버 하위 시스템을 보장합니다. "update arp"를 사용하면 IP-to-MAC DHCP 바인딩은 항상 ARP 테이블의 IP-MAC 바인딩과 일치합니다. 악의적인 사용자에게 SSG 호스트 객체와 일치하는 정적으로 구성된 IP 주소가 있지만 트래픽은 SSG 라우터에 들어갈 수 없습니다. MAC 주소가 현재 DHCP 바인딩의 MAC 주소와 일치하지 않기 때문에 IOS DHCP 서버는 ARP 항목을 생성할 수 없습니다.
- SSG와 DHCP를 함께 구성할 때 "ssg intercept dhcp" 및 "update arp"는 세션 재사용을 방지합니다. 마지막으로 비보안 관련 문제는 DHCP 호스트가 비정상 로그아웃을 수행할 때 DHCP 리스 및 ARP 항목을 해제하는 것입니다. "ssg direction downlink" 인터페이스에서 "authorized arp"를 구성하면 모든 호스트에 정기적인 ARP 요청이 전송되어 해당 요청이 계속 활성 상태인지 확인합니다. 이러한 주기적인 ARP 메시지에서 응답이 수신되지 않으면 DHCP 바인딩이 해제되고 IOS DHCP 하위 시스템이 ARP 항목을 삭제합니다.

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

이 예에서 ARP 요청은 5분마다 Fa0/0에서 알려진 모든 ARP 항목을 새로 고치도록 주기적으로 전송됩니다. 15개의 장애가 발생하면 DHCP 바인딩이 해제되고 IOS DHCP 하위 시스템이 ARP 항목을 삭제합니다. "authorized arp"가 없는 SSG의 컨텍스트에서 DHCP 호스트가 비정상 로그아웃을 수행하는 경우, 이 DHCP 주소에 대한 리스가 만료될 때까지 DHCP 리스 및 관련 SSG 호스트 객체가 활성 상태로 유지되지만 "ssg intercept dhcp"가 전역으로 구성된 경우 세션 재사용은 발생하지 않습니다.

"authorized arp"는 구성된 인터페이스에서 동적 ARP 학습을 해제합니다. 해당 인터페이스의 유일한 ARP 항목은 임대가 시작된 후 IOS DHCP 서버에서 추가한 항목입니다. 그런 다음 DHCP 릴리스의 수신, 리스 만료 또는 비정상 DHCP 로그아웃 때문에 ARP 프로브 실패 때문에 임대가 종료되

면 IOS DHCP 서버에서 이러한 ARP 항목을 삭제합니다.

구현 참고 사항:

- "ssg auto-logoff arp" 및 "ssg auto-logoff icmp"는 세션 재사용 또는 결과 보안 문제를 방지하기 위한 바람직하지 않은 방법입니다. "ssg auto-logoff"의 "arp" 및 "icmp" 변형은 구성된 "interval" 내에 SSG 연결에서 트래픽이 표시되지 않는 경우에만 ARP 또는 ICMP PING을 전송합니다. 이 중 가장 낮은 값은 30초입니다. DHCP가 이전에 사용한 IP 주소를 30초 이내에 임대하거나 악의적인 사용자가 30초 이내에 현재 바인딩된 DHCP 주소를 정적으로 구성한 경우 SSG는 연결 개체의 트래픽을 확인하고 "ssg auto-logoff"는 호출하지 않으므로 세션이 재사용됩니다.
- 모든 활용 사례에서 악성 호스트가 MAC 주소 스푸핑을 수행하는 경우 세션 재사용이 방지되지 않습니다.

표 1 - SSG/DHCP 구축의 세션 재사용 및 보안 고려 사항

명령을 사용합니다	합수	보안에 미치는 영향
ssg auto-logoff arp [match-mac-address] [interval seconds] ssg auto-logoff icmp [timeout millisecond s] [packets number] [interval seconds]	ARP 또는 ICMP PING에 실패한 후 SSG 호스트 객체를 제거합니다. 이는 "interval" 내에 SSG 연결에서 트래픽이 표시되지 않은 후에만 전송됩니다.	DHCP가 이전에 사용한 IP 주소를 30초 이내에 임대하거나, 악의적인 사용자가 SSG에서 연결 개체의 트래픽을 확인하고 "ssg auto-logoff"가 호출하지 않기 때문에 30초 이내에 현재 바인딩된 DHCP 주소를 정적으로 구성하는 경우 세션을 재사용합니다.
ssg 인터셉트 dhcp	다음 이벤트 내에서 SSG 호스트 객체를 삭제할 수 있는 SSG/DHCP 인식을 생성합니다. 활성 호스트 개체와 일치하는 IP 주소에 대해 DHCPRELEASE가 수신됩니다. B. DHCP 임대가 활성 호스트 개체와 일치하는 IP 주소에 대해 만료됩니다.	DHCP 사용자가 SSG 세션을 재사용하는 것을 방지하지만 고정 사용자가 DHCP 주소를 스푸핑하거나 SSG 세션을 재사용하는 것을 방지하지 않습니다.
ip dhcp pool TEST 업데이트 arp	ARP 항목을 추가하거나 제거할 수 있는 유일한 IOS 하위 시스템이 DHCP 서버 하위 시스템인지 확인합니다.	"ssg intercept dhcp"로 구성된 경우 모든 세션 재사용을 방지합니다. "ssg intercept dhcp"를 사용하지 않고 구성된 경우, DHCP가 이전에

		사용한 IP 주소를 임대하는 경우 세션 재사용이 가능합니다.
인터페이스 FastEthernet0/0 arp 인증	모든 호스트에 주기적인 ARP 요청을 보내 해당 요청이 계속 활성 상태인지 확인합니다. 동적 ARP 학습을 해제합니다.	DHCP 사용자가 비정상 로그아웃을 수행할 때 DHCP 바인딩 및 ARP 항목 삭제를 허용합니다.

관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)