Debug del flusso di chiamata di un gateway Internet SSG configurato con DHCP Secure ARP, SSG Port-Bundle Host Key, SSG TCP Redirect, SESM e consapevolezza SSG/DHCP

Sommario

Introduzione

Questo documento ha per oggetto un gateway Internet di IOS che esegue SSG e DHCP con SESM per i servizi del portale.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Panoramica delle tecnologie e delle caratteristiche

Service Selection Gateway (SSG)

SSG (Service Selection Gateway) è una soluzione di switching per i provider di servizi che offrono connessioni Intranet, Extranet e Internet agli utenti con tecnologia di accesso a banda larga, come DSL (Digital Subscriber Line), modem via cavo o wireless per consentire l'accesso simultaneo ai servizi di rete.

SSG lavora in abbinamento a Cisco Subscriber Edge Services Manager (SESM). Isieme al SESM, SSG fornisce l'autenticazione degli utenti, la selezione dei servizi e le funzionalità di connessione ai servizi Internet. Gli abbonati interagiscono con un'applicazione Web SESM utilizzando un browser Internet standard.

Il SESM funziona in due modalità:

- Modalità RADIUS: questa modalità consente di ottenere informazioni sul sottoscrittore e sul servizio da un server RADIUS. Il SESM in modalità RADIUS è simile all'SSD.
- Modalità LDAP - La modalità LDAP (Lightweight Directory Access Protocol) fornisce l'accesso a una directory conforme a LDAP per le informazioni sul profilo del sottoscrittore e del servizio. Questa modalità offre inoltre funzionalità avanzate per le applicazioni Web SESM e utilizza un modello di controllo di accesso basato sui ruoli (RBAC, role-based access control) per gestire l'accesso degli utenti.

Chiave host pacchetto porta SSG

La funzione SSG Port-Bundle Host Key migliora la comunicazione e la funzionalità tra SSG e SESM con un meccanismo che utilizza l'indirizzo IP di origine dell'host e la porta di origine per identificare e monitorare gli utenti.

Con la funzione SSG Port-Bundle Host Key, SSG esegue la conversione degli indirizzi delle porte (PAT) e la conversione degli indirizzi della rete (NAT) sul traffico HTTP tra il sottoscrittore e il server SESM. Quando un sottoscrittore invia un pacchetto HTTP al server SESM, SSG crea una mappa delle porte che cambia l'indirizzo IP di origine in un indirizzo IP di origine SSG configurato e cambia la porta TCP di origine in una porta allocata da SSG. SSG assegna un bundle di porte a ciascun sottoscrittore perché un sottoscrittore può avere più sessioni TCP simultanee quando accede a una pagina Web. La chiave host assegnata, o combinazione di porta-bundle e indirizzo IP di origine SSG, identifica in modo univoco ciascun sottoscrittore. La chiave host viene trasportata nei pacchetti RADIUS inviati tra il server SESM e SSG nell'attributo specifico del fornitore (VSA) dell'IP del sottoscrittore. Quando il server SESM invia una risposta al sottoscrittore, SSG converte l'indirizzo IP di destinazione e la porta TCP di destinazione in base alla mappa della porta.

Reindirizzamento TCP SSG per utenti non autenticati

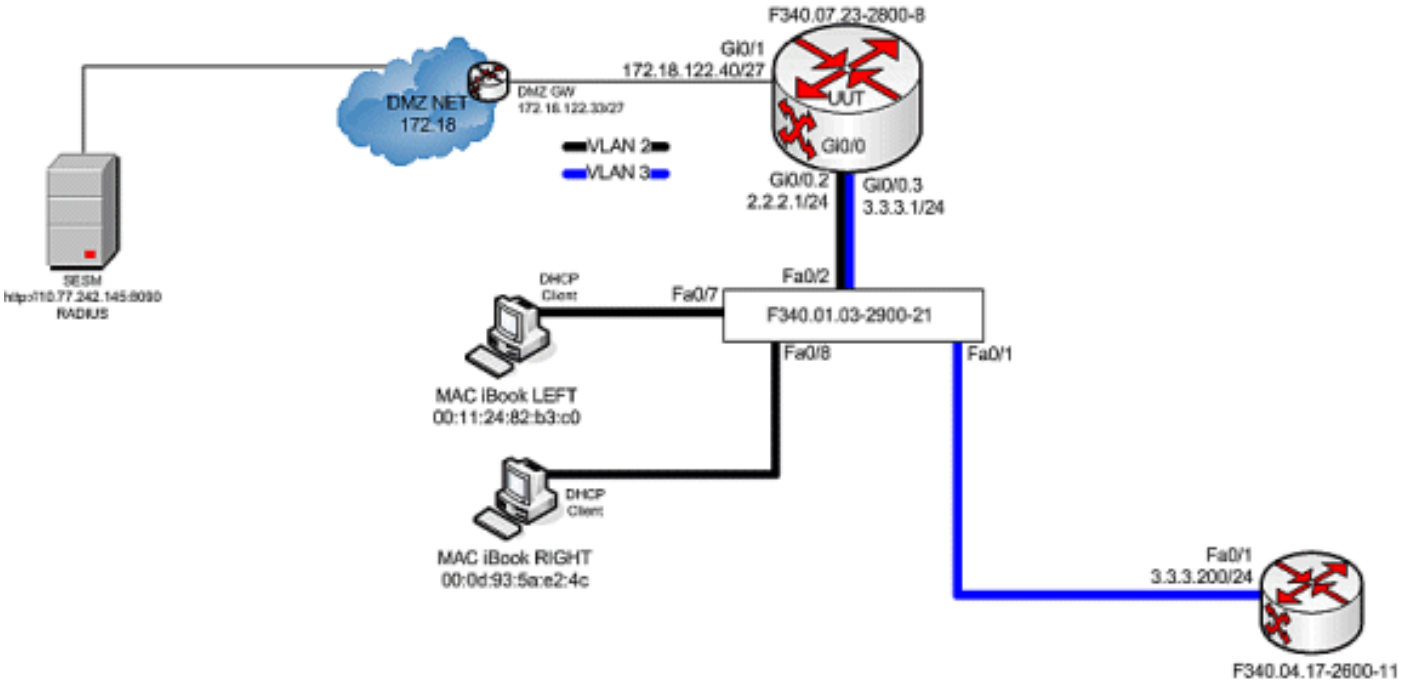
Il reindirizzamento per gli utenti non autenticati reindirizza i pacchetti da un utente se l'utente non ha ricevuto l'autorizzazione dal provider di servizi. Quando un sottoscrittore non autorizzato tenta di connettersi a un servizio su una porta TCP (ad esempio, verso www.cisco.com), SSG TCP Redirect reindirizza il pacchetto al portale captive (SESM o un gruppo di dispositivi SESM). SESM esegue un reindirizzamento al browser per visualizzare la pagina di accesso. Il sottoscrittore

accede a SESM ed è autenticato e autorizzato. Il modulo SESM quindi presenta al destinatario una home page personalizzata, la home page del provider di servizi o l'URL originale.

Assegnazione indirizzo IP protetto DHCP

La funzionalità di assegnazione degli indirizzi IP protetti di DHCP introduce la funzionalità di protezione delle voci della tabella ARP nei lease DHCP (Dynamic Host Configuration Protocol) nel database DHCP. Questa funzionalità protegge e sincronizza l'indirizzo MAC del client sul binding DHCP, impedendo a client non autorizzati o hacker di falsificare il server DHCP e di acquisire un lease DHCP di un client autorizzato. Quando questa funzione è abilitata e il server DHCP assegna un indirizzo IP al client DHCP, il server DHCP aggiunge una voce ARP sicura alla tabella ARP con l'indirizzo IP assegnato e l'indirizzo MAC del client. Questa voce ARP non può essere aggiornata da altri pacchetti ARP dinamici e esiste nella tabella ARP per la durata del lease configurata o finché il lease è attivo. La voce ARP protetta può essere eliminata solo da un messaggio di terminazione esplicito del client DHCP o del server DHCP alla scadenza del binding DHCP. Questa funzionalità può essere configurata per una nuova rete DHCP o utilizzata per aggiornare la sicurezza di una rete corrente. La configurazione di questa funzionalità non interrompe il servizio e non è visibile al client DHCP.

Diagramma testbed



Debug flusso di chiamata

Attenersi alla seguente procedura:

1. Quando MAC iBook LEFT connette per la prima volta il cavo Ethernet a questa rete, assegna in lease l'indirizzo IP 2.2.2.5/29 dal server DHCP IOS in esecuzione su "F340.07.23-2800-8".

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

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

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

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

2. Dopo aver assegnato correttamente in lease l'indirizzo IP 2.2.2.5, MAC iBook LEFT apre un browser Web e lo punta a **http://3.3.3.200**, che viene utilizzato per simulare le risorse protette legate a SSG Service "distlearn". Il valore "distlearn" del servizio SSG è definito localmente nel router SSG "F340.07.23-2800-8":

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

   In realtà, **http://3.3.3.200** è un router Cisco IOS configurato per "ip http server" e in ascolto su TCP 80, quindi è fondamentalmente un server Web.Dopo che MAC iBook LEFT ha tentato di raggiungere il sito **http://3.3.3.200**, poiché la connessione è in entrata su un'interfaccia configurata con "ssg direction downlink", il router SSG controlla prima l'esistenza di un oggetto host SSG attivo per l'indirizzo IP di origine della richiesta HTTP. Poiché questa è la prima richiesta di questo tipo dall'indirizzo IP 2.2.2.5, non esiste un oggetto host SSG e viene creata un'istanza di reindirizzamento TCP verso SESM per l'host 2.2.2.5 tramite questa configurazione:

```
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
```

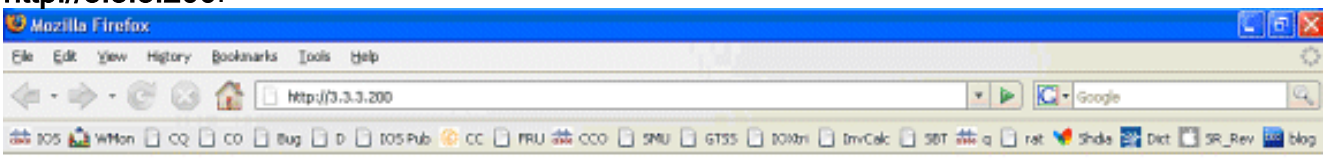
10.77.242.145 is the SESM server and it's listening for HTTP on TCP 8090. "server" MUST be in default network or open-garden. **redirect port-list ports to ssg_tr_unauth**
redirect unauthenticated-user to ssg_tr_unauth
If an SSG router receives a packets on an interface with "ssg direction downlink" 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
```

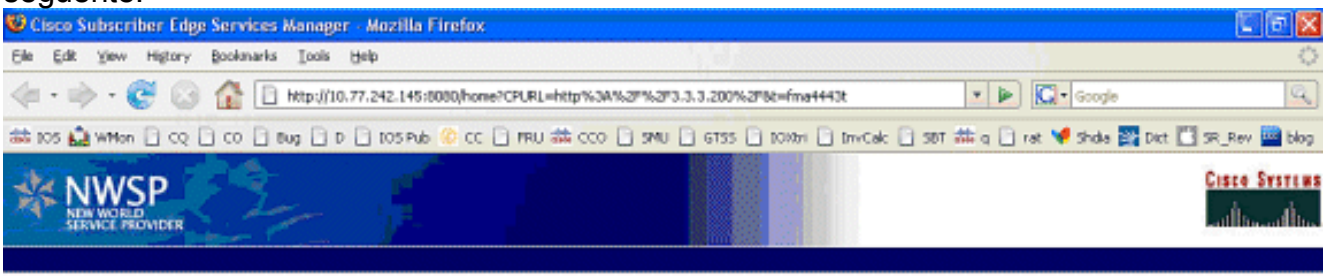
The initial HTTP request from 2.2.2.5 had a source TCP Port of 49273 and a destination IP address of 3.3.3.200 and TCP port of 80. Because of the SSG TCP Redirect, the destination IP header is overwritten with the socket of the SESM server 10.77.242.145:8090. If Port Bundle Host Key were NOT configured,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

A questo punto, il browser su MAC iBook Left appare così quando si immette **http://3.3.3.200**:



Dopo i reindirizzamenti IOS SSG TCP e SESM HTTP, la schermata sarà simile alla seguente:



3. Dopo il reindirizzamento TCP SSG al SESM e il successivo reindirizzamento HTTP inviato dal SESM al browser di MAC iBook Left, MAC iBook Left immette **user1** come nome utente e **cisco** come password:

4. Dopo aver premuto il pulsante **OK**, il SESM invia al router SSG queste credenziali tramite un protocollo proprietario basato su RADIUS.

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

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

5. A sua volta, il router SSG crea un pacchetto di richiesta di accesso RADIUS e lo invia a RADIUS per autenticare l'**utente 1**:

```
*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 risponde con un'autorizzazione di accesso per **user1**, e un oggetto host SSG viene creato in "F340.07.23-2800-8":

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

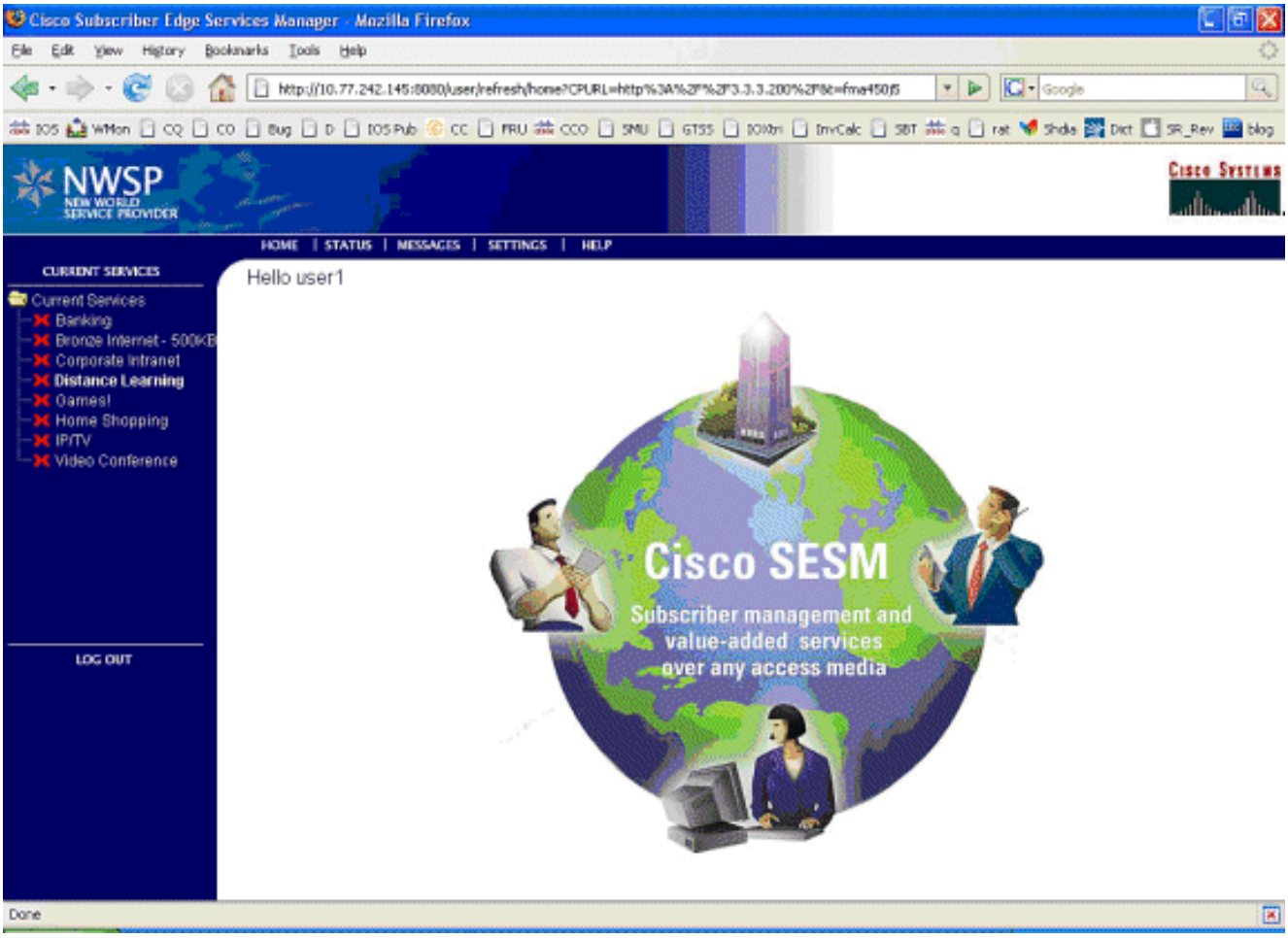
```
   [26]  14
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 8   "Ngames"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  18
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 12  "Ndistlearn"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  18
*Oct 13 20:25:02.081: RADIUS: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

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

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

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

   ### Active HostObject Count: 1

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

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

7. A questo punto, l'**utente 1** è definito come un oggetto host SSG, ma non ha ancora accesso ad alcun servizio SSG. MAC iBook Left viene presentato con la schermata di selezione dei servizi e fa clic su **Distance Learning**:



8. Dopo aver fatto clic su **Distance Learning**, la casella SESM comunica con il canale di controllo al router SSG:

```
debug ssg ctrl-events

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

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

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

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

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

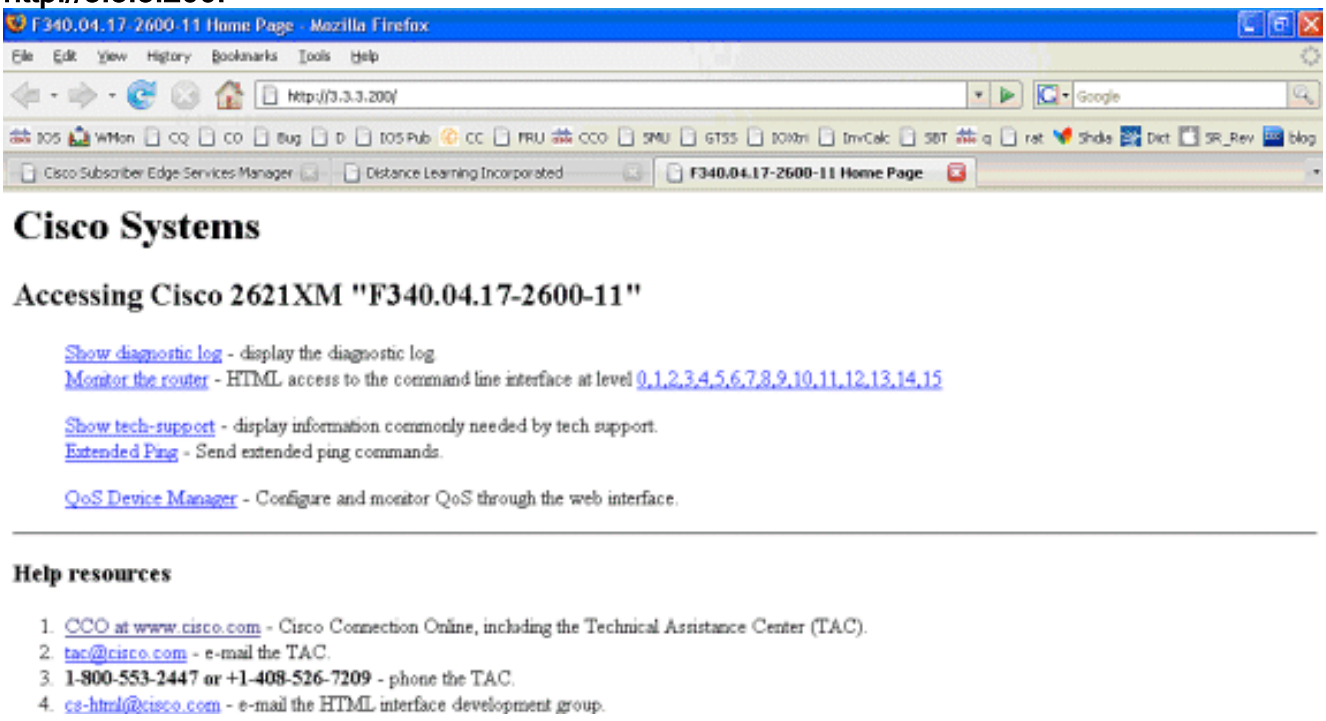
----------ConnectionObject Content ----
User Name: user1
Owner Host: 2.2.2.5
Associated Service: distlearn
Calling station id: 0011.2482.b3c0
Connection State: 0 (UP)
Connection Started since:
*20:40:21.000 UTC Mon Oct 13 2008

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

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

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

9. La connessione SSG è attiva e il flusso di chiamata è completato. MAC iBook Left può passare a
http://3.3.3.200:



Spiegazione della configurazione del router SSG con documenti sulle funzionalità

```
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
```

Considerazioni sulla sicurezza e sul riutilizzo delle sessioni

Quando si utilizzano SSG e DHCP insieme, questi scenari possono consentire a utenti malintenzionati di riutilizzare un oggetto host SSG autenticato che consente l'accesso non autenticato alle risorse protette:

- Se il riconoscimento SSG/DHCP non è configurato con "ssg intercept dhcp", un nuovo utente DHCP può concedere in lease un indirizzo IP precedentemente concesso in lease per cui esiste ancora un oggetto host SSG. Poiché la prima richiesta TCP di questo nuovo utente ha un oggetto host SSG corrispondente, anche se non aggiornato, all'indirizzo IP di origine, a questo utente viene concesso l'utilizzo non autenticato delle risorse protette. Per evitare questo problema, è possibile usare il comando "ssg intercept dhcp", che determina la rimozione di un oggetto host SSG quando si verifica una delle due situazioni:DHCPRELEASE ricevuto per un indirizzo IP corrispondente a un oggetto host attivo.Il lease DHCP scade per un indirizzo IP corrispondente a un oggetto host attivo.
- Se un utente DHCP socializza l'indirizzo IP in lease con un utente malintenzionato prima di una disconnessione DHCP non regolare, ovvero una disconnessione DHCP per la quale non viene inviato DHCPRELEASE, l'utente malintenzionato può configurare staticamente il computer con questo indirizzo IP e riutilizzare l'oggetto host SSG indipendentemente dal fatto che sia configurata o meno la funzione "ssg intercept dhcp". Per evitare questo problema, è possibile usare la combinazione di "ssg intercept dhcp" e "update arp" configurata sotto il pool DHCP IOS. L'opzione "update arp" (aggiorna arp) garantisce che l'unico sottosistema IOS in grado di aggiungere o rimuovere voci ARP sia il sottosistema server DHCP. Con "update arp", il binding DHCP IP-MAC corrisponde sempre al binding IP-MAC nella tabella ARP. Anche se l'utente malintenzionato ha un indirizzo IP configurato staticamente che corrisponde all'oggetto host SSG, il traffico non è autorizzato ad accedere al router SSG. Poiché l'indirizzo MAC non corrisponde all'indirizzo MAC del binding DHCP corrente, il server DHCP IOS impedisce la creazione di una voce ARP.
- Quando SSG e DHCP sono configurati insieme, "ssg intercept dhcp" e "update arp" impediscono il riutilizzo della sessione. L'ultimo problema non relativo alla sicurezza è liberare la voce DHCP Lease e ARP quando un host DHCP esegue una disconnessione non regolare. La configurazione di "arp autorizzato" sull'interfaccia "ssg direction downlink" determina l'invio periodico di richieste ARP a tutti gli host per essere certi che siano ancora attivi. Se non si riceve alcuna risposta da questi messaggi ARP periodici, il binding DHCP viene rilasciato e il sottosistema DHCP IOS rimuove la voce ARP.

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

In questo esempio, viene inviata periodicamente una richiesta ARP per aggiornare tutte le voci ARP conosciute su Fa0/0 ogni 5. Dopo 15 errori, il binding DHCP viene rilasciato e il

sottosistema DHCP IOS rimuove la voce ARP.Nel contesto di SSG senza "arp autorizzato", se un host DHCP esegue una disconnessione non autorizzata, il lease DHCP e l'oggetto host SSG associato rimangono attivi fino alla scadenza del lease per questo indirizzo DHCP, ma non si verifica alcun riutilizzo della sessione finché "ssg intercept dhcp" è configurato globalmente.

L'"arp autorizzato" disattiva l'apprendimento ARP dinamico sull'interfaccia su cui è configurato. Le uniche voci ARP sull'interfaccia in questione sono quelle aggiunte dal server DHCP IOS dopo l'avvio di un lease. Queste voci ARP vengono quindi eliminate dal server DHCP IOS una volta terminato il lease, a causa della ricezione di una versione DHCP, di una scadenza del lease o di un errore del probe ARP causato da una disconnessione DHCP non corretta.

Note sull'implementazione:

- Il "ssg auto-logoff arp" e il "ssg auto-logoff icmp" sono metodi indesiderati per impedire il riutilizzo della sessione o problemi di sicurezza risultanti. Le varianti "arp" e "icmp" di "disconnessione automatica SSG" inviano un PING ARP o IMCP solo quando il traffico sulla connessione SSG non viene rilevato entro l'"intervallo" configurato, il più basso dei quali è 30 secondi. Se DHCP concede in lease un indirizzo IP usato in precedenza entro 30 secondi o un utente malintenzionato configura staticamente un indirizzo DHCP attualmente associato entro 30 secondi, la sessione viene riutilizzata perché SSG rileva il traffico sull'oggetto connessione e "ssg auto-logoff" non richiama.
- In tutti i casi di utilizzo, il riutilizzo delle sessioni non viene impedito se un host dannoso esegue lo spoof dell'indirizzo MAC.

Tabella 1 - Considerazioni sul riutilizzo delle sessioni e sulla sicurezza nelle distribuzioni SSG/DHCP

Comando	Funzione	Implicazioni per la sicurezza
ssg auto-logoff arp [match-mac-address] [intervallo *secondi*] ssg auto-logoff icmp [timeout milliseconds] [numero pacchetti] [intervallo *secondi*]	Rimuove l'oggetto host SSG dopo un errore di ARP o PING ICMP, inviati solo dopo che non è stato rilevato alcun traffico sulla connessione SSG nell'intervallo.	Riutilizza la sessione se DHCP concede in lease un indirizzo IP usato in precedenza entro 30 secondi o se un utente malintenzionato configura staticamente un indirizzo DHCP attualmente associato entro 30 secondi, in quanto SSG rileva il traffico sull'oggetto connessione e "ssg auto-logoff" non

		richiama.
ssg intercept dhcp	Crea una consapevolezza SSG/DHCP che consente l'eliminazione dell'oggetto host SSG all'interno di questi eventi: DHCPRELEASE ricevuto per un indirizzo IP corrispondente a un oggetto host attivo. B. Il lease DHCP scade per un indirizzo IP corrispondente a un oggetto host attivo.	Impedisce agli utenti DHCP di riutilizzare le sessioni SSG ma non impedisce agli utenti statici di falsificare gli indirizzi DHCP o di riutilizzare le sessioni SSG.
arp ip dhcp pool TEST update	Assicura che l'unico sottosistema IOS in grado di aggiungere o rimuovere voci ARP sia il sottosistema server DHCP.	Impedisce il riutilizzo di tutte le sessioni se configurate con "ssg intercept dhcp". Se il protocollo DHCP non supporta la funzione "ssg intercept dhcp" e il protocollo DHCP assegna in lease un indirizzo IP precedentemente utilizzato, è comunque possibile riutilizzare la sessione.
interface Fast Ethernet0/0 arp autorizzata	Invia richieste ARP periodiche a tutti gli host per assicurarsi che siano ancora attivi. Disattiva l'apprendimento ARP dinamico.	Consente il binding DHCP e l'eliminazione della voce ARP quando un utente DHCP esegue una disconnessione non regolare.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems