Call Flow Debugging eines SSG Internet Gateway konfiguriert mit DHCP Secure ARP, SSG Port-Bundle Host Key, SSG TCP Redirect, SESM und SSG/DHCP Awareness

Inhalt

Einführung

Im Mittelpunkt dieses Dokuments steht ein IOS Internet Gateway, das SSG und DHCP mit SESM für Portaldienste ausführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Technologie und Funktionen im Überblick

Service Selection Gateway (SSG)

Das Service Selection Gateway (SSG) ist eine Switching-Lösung für Service Provider, die ihren Kunden Intranet-, Extranet- und Internetverbindungen über Breitbandtechnologie anbieten, z. B. digitale Teilnehmeranschlüsse (DSL), Kabelmodems oder Wireless-Netzwerke, um den gleichzeitigen Zugriff auf Netzwerkdienste zu ermöglichen.

Die SSG arbeitet mit dem Cisco Subscriber Edge Services Manager (SESM) zusammen. Zusammen mit dem SESM stellt die SSG Teilnehmer-Authentifizierung, Serviceauswahl und Dienstverbindungsfunktionen für Internetdienste bereit. Abonnenten interagieren mit einer SESM-Webanwendung über einen Standard-Internetbrowser.

Das SESM wird in zwei Modi betrieben:

- RADIUS mode (RADIUS-Modus): Dieser Modus ruft Teilnehmer- und Dienstinformationen von einem RADIUS-Server ab. SESM im RADIUS-Modus ähnelt der SSD.
- LDAP-Modus - Der Lightweight Directory Access Protocol (LDAP)-Modus ermöglicht den Zugriff auf ein LDAP-kompatibles Verzeichnis für Abonnenten- und Serviceprofildaten. Dieser Modus bietet außerdem erweiterte Funktionen für SESM-Webanwendungen und verwendet ein rollenbasiertes Zugriffssteuerungsmodell (RBAC) zur Verwaltung des Teilnehmerzugriffs.

SSG-Portpaket - Host-Schlüssel

Die Funktion "SSG Port-Bundle Host Key" (Hostschlüssel für SSG-Ports) verbessert die Kommunikation und Funktionalität zwischen SSG und SESM mit einem Mechanismus, der die IP-Adresse der Hostquelle und den Quellport zum Identifizieren und Überwachen von Teilnehmern verwendet.

Mit der SSG Port-Bundle Host Key-Funktion führt SSG die Port-Address Translation (PAT) und Network Address Translation (NAT) für den HTTP-Datenverkehr zwischen dem Teilnehmer und dem SESM-Server durch. Wenn ein Teilnehmer ein HTTP-Paket an den SESM-Server sendet, erstellt die SSG eine Port-Zuordnung, die die Quell-IP-Adresse in eine konfigurierte SSG-Quell-IP-Adresse ändert und den Quell-TCP-Port in einen von der SSG zugewiesenen Port ändert. SSG weist jedem Teilnehmer ein Portpaket zu, da ein Teilnehmer mehrere gleichzeitige TCP-Sitzungen abhalten kann, wenn er auf eine Webseite zugreift. Der zugewiesene Hostschlüssel oder die Kombination aus Port-Bündel und SSG-Quell-IP-Adresse identifiziert jeden Teilnehmer eindeutig. Der Hostschlüssel wird in RADIUS-Paketen übertragen, die zwischen dem SESM-Server und dem SSG im anbieterspezifischen Attribut (VSA) des Subscriber IP gesendet werden. Wenn der SESM-Server eine Antwort an den Abonnenten sendet, übersetzt SSG die Ziel-IP-Adresse und den Ziel-TCP-Port gemäß der Port-Zuordnung.

SSG-TCP-Umleitung für nicht authentifizierte Benutzer

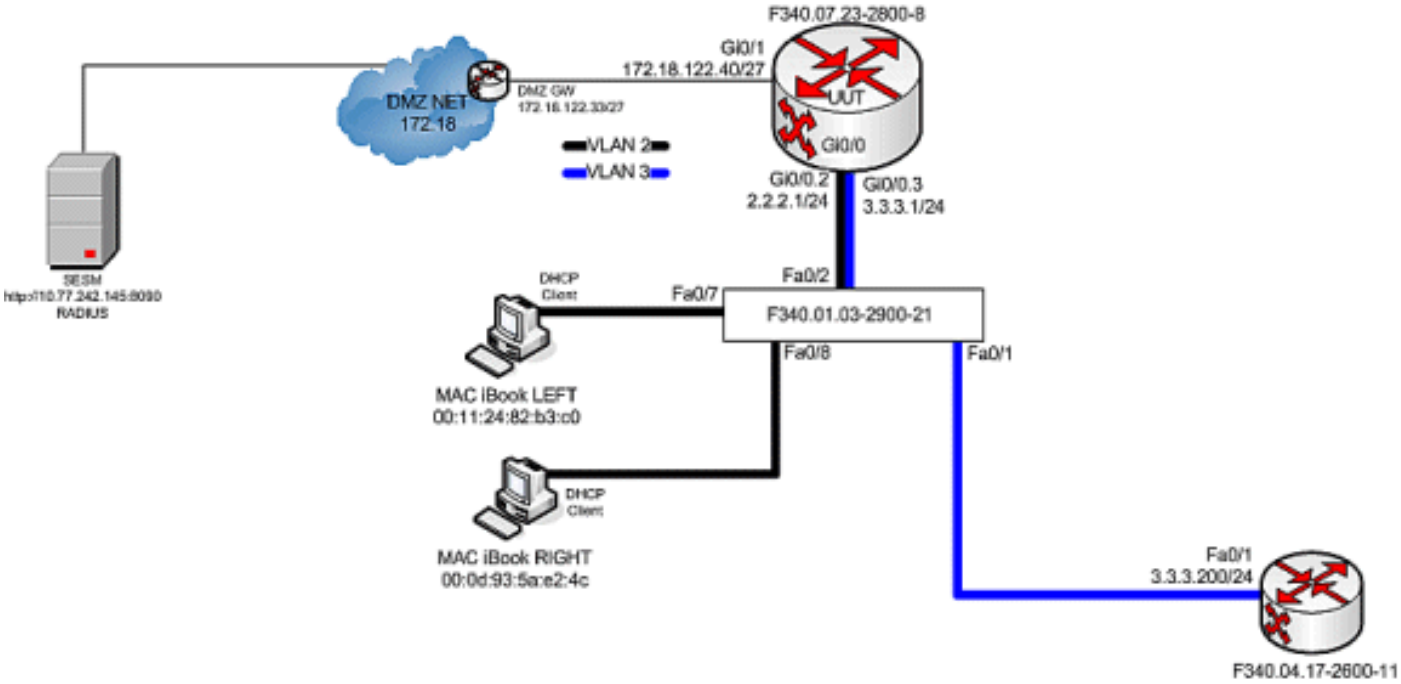
Umleitung für nicht authentifizierte Benutzer leitet Pakete von einem Benutzer um, wenn der Benutzer nicht beim Dienstanbieter autorisiert ist. Wenn ein nicht autorisierter Teilnehmer versucht, eine Verbindung zu einem Dienst an einem TCP-Port herzustellen (z. B. zu www.cisco.com), leitet SSG TCP Redirect das Paket an das Captive Portal (SESM oder eine Gruppe von SESM-Geräten) um. SESM gibt eine Umleitung zum Browser aus, um die

Anmeldeseite anzuzeigen. Der Teilnehmer meldet sich bei SESM an und wird authentifiziert und autorisiert. SESM stellt dem Teilnehmer dann eine personalisierte Startseite, die Startseite des Dienstanbieters oder die ursprüngliche URL zur Verfügung.

Gesicherte DHCP-IP-Adressenzuweisung

Die Funktion für die Zuweisung sicherer DHCP-IP-Adressen bietet die Möglichkeit, Einträge der ARP-Tabelle in DHCP-Leases (Dynamic Host Configuration Protocol) der DHCP-Datenbank zu sichern. Diese Funktion sichert und synchronisiert die MAC-Adresse des Clients mit der DHCP-Bindung, wodurch nicht autorisierte Clients oder Hacker daran gehindert werden, den DHCP-Server zu imitieren und einen DHCP-Lease eines autorisierten Clients zu übernehmen. Wenn diese Funktion aktiviert ist und der DHCP-Server dem DHCP-Client eine IP-Adresse zuweist, fügt der DHCP-Server der ARP-Tabelle einen sicheren ARP-Eintrag mit der zugewiesenen IP-Adresse und der MAC-Adresse des Clients hinzu. Dieser ARP-Eintrag kann nicht von anderen dynamischen ARP-Paketen aktualisiert werden. Dieser ARP-Eintrag existiert für die konfigurierte Leasedauer in der ARP-Tabelle, oder solange der Lease aktiv ist. Der gesicherte ARP-Eintrag kann nur durch eine explizite Terminierungsmeldung vom DHCP-Client oder DHCP-Server gelöscht werden, wenn die DHCP-Bindung abläuft. Diese Funktion kann für ein neues DHCP-Netzwerk konfiguriert oder zur Aktualisierung der Sicherheit eines aktuellen Netzwerks verwendet werden. Die Konfiguration dieser Funktion unterbricht den Dienst nicht und ist für den DHCP-Client nicht sichtbar.

Testdiagramm



Anruffluss-Debug

Gehen Sie wie folgt vor:

1. Wenn MAC iBook LINFT das Ethernetkabel zuerst mit diesem Netzwerk verbindet, wird die IP-Adresse 2.2.2.5/29 vom IOS DHCP-Server geleast, der auf "F340.07.23-2800-8" ausgeführt wird.

```
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. Nachdem die IP-Adresse 2.2.2.5 erfolgreich geleast wurde, öffnet MAC iBook LINFT einen Webbrowser und zeigt ihn auf **http://3.3.3.200**, die zur Simulation von geschützten Ressourcen verwendet wird, die an SSG Service "distlearn" gebunden sind. Der SSG-Service "distlearn" wird lokal im SSG-Router "F340.07.23-2800-8" definiert:

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

Tatsächlich ist **http://3.3.3.200** ein Cisco IOS-Router, der für "ip http server" konfiguriert ist und TCP 80 abhört, sodass es sich im Grunde um einen Webserver handelt.Nachdem die MAC iBook LEFT versucht hat, zu **http://3.3.3.200** zu navigieren, da diese Verbindung auf einer mit "ssg direction downlink" konfigurierten Schnittstelle eingeht, prüft der SSG-Router zunächst, ob ein aktives SSG-Host-Objekt für die Quell-IP-Adresse der HTTP-Anfrage vorhanden ist. Da dies die erste derartige Anforderung von der IP-Adresse 2.2.2.5 ist, existiert kein SSG-Hostobjekt, und eine TCP-Umleitung zu SESM wird für Host 2.2.2.5 mithilfe dieser Konfiguration instanziiert:

```
ssg tcp-redirect
 port-list ports
  port 80
  port 8080
```

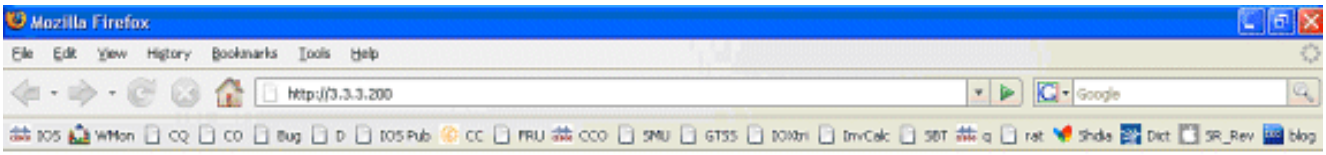
port 8090
port 443
All hosts with destination requests on these TCP Ports are candidates for redirection.
server-group ssg_tr_unauth
server 10.77.242.145 8090
10.77.242.145 is the SESM server and it's listening for HTTP on TCP 8090. "server" MUST be in default network or open-garden. **redirect port-list 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
```

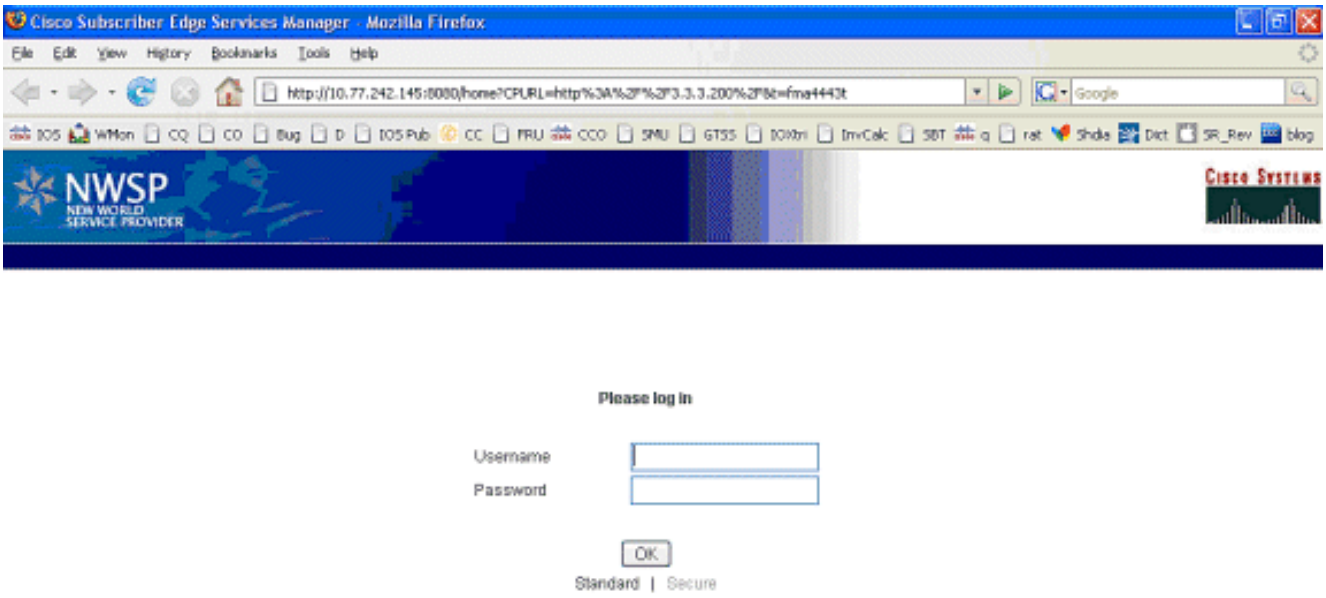
The initial HTTP request from 2.2.2.5 had a source TCP Port of 49273 and a destination IP address of 3.3.3.200 and TCP port of 80. Because of the SSG TCP Redirect, the destination IP header is overwritten with the socket of the SESM server 10.77.242.145:8090. If Port Bundle Host Key were NOT configured,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

An diesem Punkt sieht der Browser in der MAC iBook Left-Anzeige wie folgt aus, wenn **http://3.3.3.200** eingegeben wird:



Nach der Umleitung von IOS SSG TCP und SESM HTTP sieht der Bildschirm wie folgt aus:



3. Nach der Umleitung des SSG-TCP an SESM und der anschließenden HTTP-Umleitung, die von SESM zurück an den Browser des MAC iBook Left gesendet wurde, gibt die MAC iBook Left **user1** als Benutzernamen und **cisco** als Kennwort ein:

4. Nachdem die **OK**-Taste gedrückt wurde, sendet das SESM dem SSG-Router diese

Anmeldeinformationen über ein proprietäres RADIUS-basiertes Protokoll.

```
*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. Der SSG-Router wiederum erstellt ein RADIUS Access-Request-Paket und sendet es an RADIUS, um den **Benutzer** zu authentifizieren**.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 antwortet mit einem Access-Accept für **user1**, und ein SSG-Hostobjekt wird in "F340.07.23-2800-8" erstellt:

```
*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**

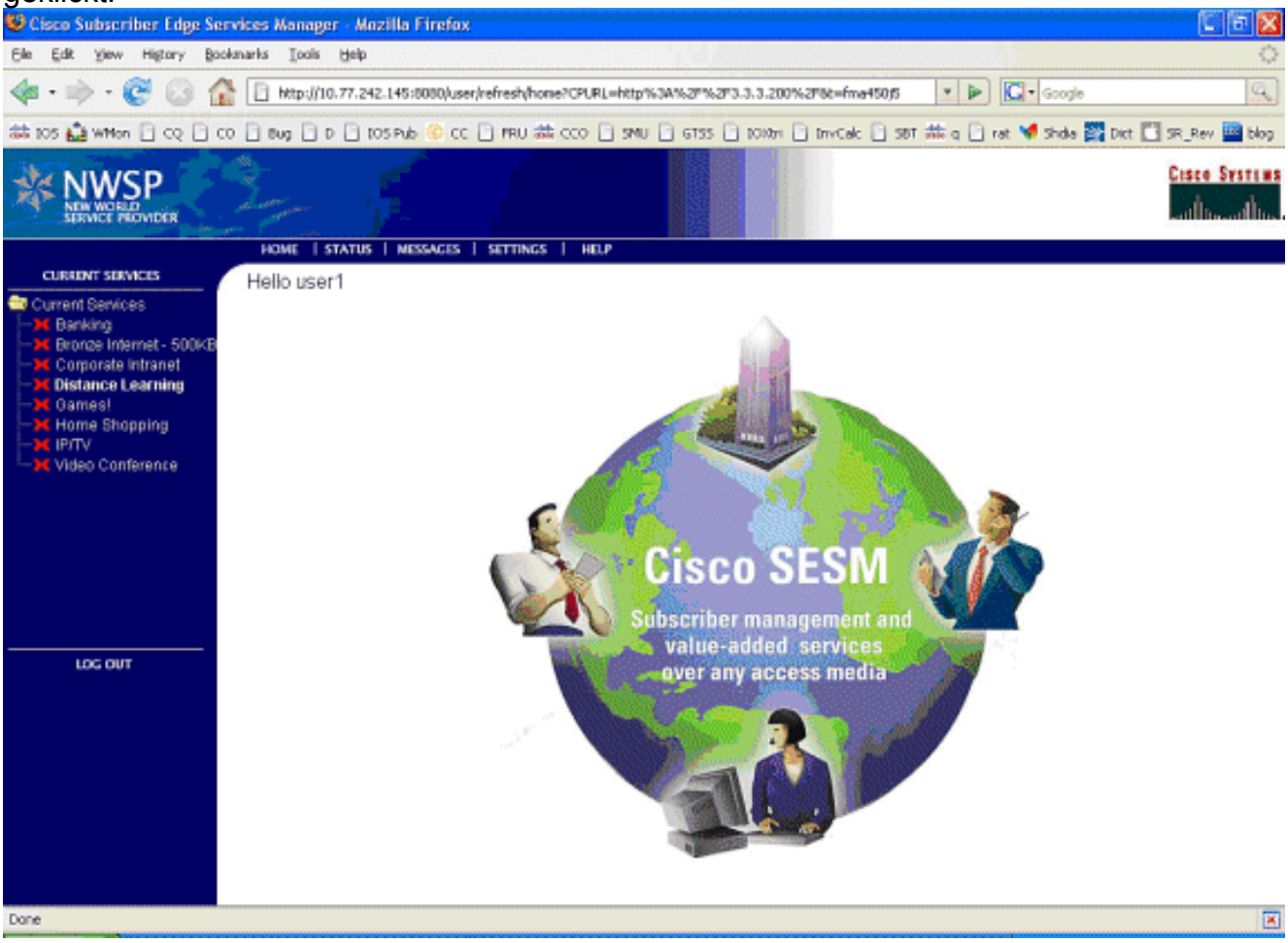
```
  1: 2.2.2.5  [Host-Key 172.18.122.40:64]

   ### 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. Zu diesem Zeitpunkt ist **user1** als SSG-Hostobjekt definiert, hat jedoch noch keinen Zugriff

auf SSG-Dienste. Das MAC-iBook "Links" wird mit dem Bildschirm "Service Selection" (Serviceauswahl) angezeigt, und es wird auf **Distance Learning (Entfernungslernen)** geklickt:



8. Nach dem Klicken auf **Distance Learning** kommuniziert das SESM-Feld mit dem Steuerungskanal an den SSG-Router:

```
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**

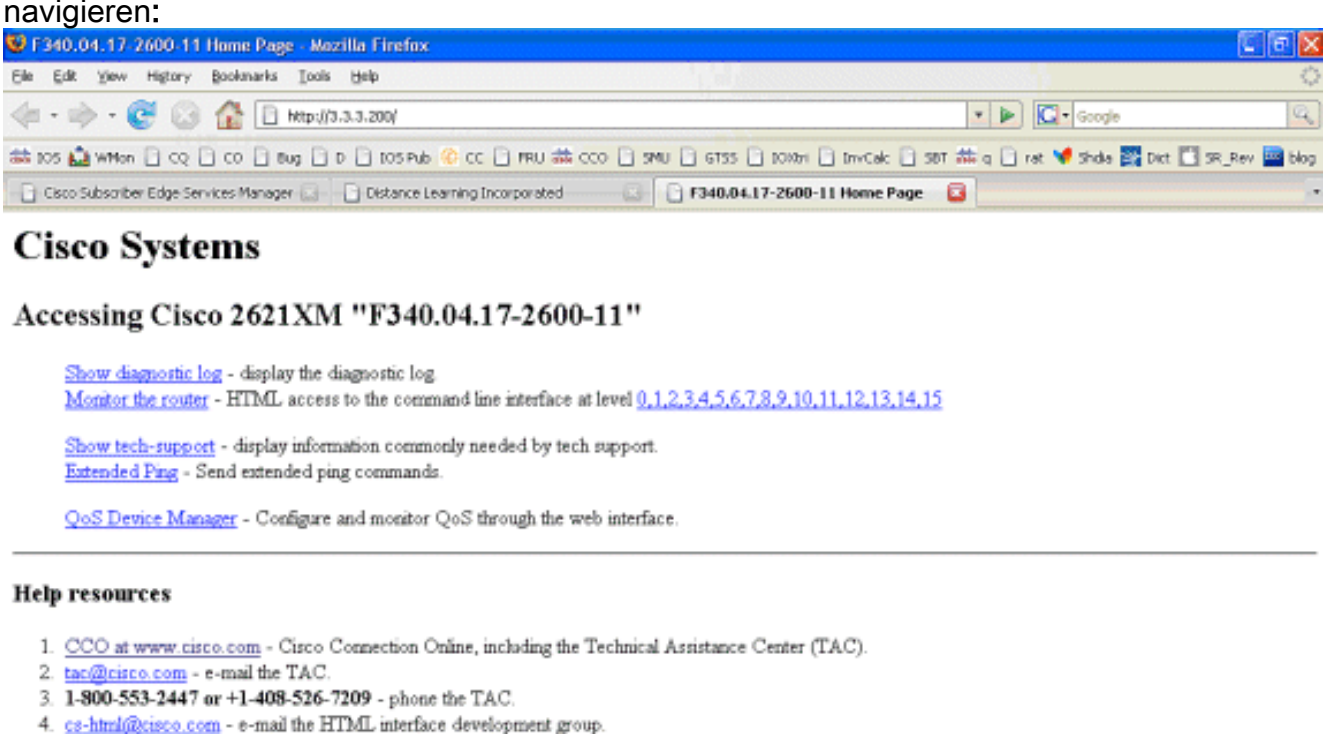
```
-----------------------ConnectionObject Content ----
User Name: user1
Owner Host: 2.2.2.5
Associated Service: distlearn
Calling station id: 0011.2482.b3c0
Connection State: 0 (UP)
Connection Started since:
   *20:40:21.000 UTC Mon Oct 13 2008

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. Die SSG-Verbindung ist aktiv, und der Anruffluss ist abgeschlossen. MAC iBook Left kann erfolgreich zu **http://3.3.3.200** navigieren:



Erläuterung der Konfiguration des SSG-Routers mit Funktionsdokumenten

```
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
```

Überlegungen zur Sicherheit und Sitzungswiederverwendung

Wenn Sie SSG und DHCP zusammen verwenden, können diese Szenarien böswilligen Benutzern die Wiederverwendung eines authentifizierten SSG-Host-Objekts ermöglichen, das nicht authentifizierten Zugriff auf sichere Ressourcen ermöglicht:

- Wenn die SSG/DHCP-Erkennung nicht mit "ssg intercept dhcp" konfiguriert ist, kann ein neuer DHCP-Benutzer eine zuvor geleaste IP-Adresse leasen, für die noch ein SSG-Host-Objekt vorhanden ist. Da die erste TCP-Anfrage von diesem neuen Benutzer ein übereinstimmendes, wenn auch veraltetes SSG-Hostobjekt enthält, das der Quell-IP-Adresse entspricht, wird diesem Benutzer die nicht authentifizierte Verwendung geschützter Ressourcen gewährt. Dies kann mithilfe von "ssg intercept dhcp" verhindert werden, was zur Entfernung eines SSG-Hostobjekts führt, wenn eines der folgenden Ereignisse eintritt:DHCPRELEASE wird für eine IP-Adresse empfangen, die mit einem Active Host-Objekt übereinstimmt.Der DHCP-Lease läuft für eine IP-Adresse ab, die mit einem Active Host-Objekt übereinstimmt.
- Wenn ein DHCP-Benutzer die geleaste IP-Adresse einem böswilligen Benutzer vor einer nicht ordnungsgemäßen DHCP-Abmeldung zuweist, d. h. einem DHCP-Abmelden, für das kein DHCPRELEASE gesendet wird, kann der böswillige Benutzer den Computer statisch mit dieser IP-Adresse konfigurieren und das SSG-Host-Objekt wiederverwenden, unabhängig davon, ob "ssg intercept dhcp" konfiguriert ist oder nicht. Dies kann durch eine Kombination aus "ssg intercept dhcp" und "update arp" verhindert werden, die unter dem IOS DHCP-Pool konfiguriert ist. Der "update arp" stellt sicher, dass das einzige IOS-Subsystem, das ARP-Einträge hinzufügen oder entfernen kann, das DHCP-Server-Subsystem ist. Mit "update arp" entspricht die IP-MAC-DHCP-Bindung immer der IP-MAC-Bindung in der ARP-Tabelle. Obwohl der böswillige Benutzer über eine statisch konfigurierte IP-Adresse verfügt, die mit dem SSG-Host-Objekt übereinstimmt, darf der Datenverkehr nicht in den SSG-Router gelangen. Da die MAC-Adresse nicht mit der MAC-Adresse der aktuellen DHCP-Bindung übereinstimmt, verhindert der IOS DHCP-Server die Erstellung eines ARP-Eintrags.
- Wenn SSG und DHCP zusammen konfiguriert werden, verhindern "ssg intercept dhcp" und "update arp" die Wiederverwendung von Sitzungen. Die letzte nicht sicherheitsbezogene Herausforderung besteht darin, den DHCP-Lease- und ARP-Eintrag freizugeben, wenn ein DHCP-Host einen nicht ordnungsgemäßen Abmelden durchführt. Die Konfiguration von "authorized arp" auf der "ssg direction downlink"-Schnittstelle führt dazu, dass periodische ARP-Anfragen an alle Hosts gesendet werden, um sicherzustellen, dass sie weiterhin aktiv sind. Wenn aus diesen periodischen ARP-Nachrichten keine Antwort empfangen wird, wird die DHCP-Bindung freigegeben, und das IOS DHCP-Subsystem entfernt den ARP-Eintrag.

```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
arp authorized
```

```
arp probe interval 5 count 15
```

In diesem Beispiel wird in regelmäßigen Abständen eine ARP-Anfrage gesendet, um alle bekannten ARP-Einträge auf Fa0/0 alle fünf Sekunden zu aktualisieren. Nach 15 Fehlern wird die DHCP-Bindung freigegeben, und das IOS DHCP-Subsystem löscht den ARP-Eintrag.Wenn ein DHCP-Host im Kontext von SSG ohne "authorized arp" einen nicht ordnungsgemäßen Abmeldevorgang durchführt, bleiben die DHCP-Lease und das zugehörige SSG-Host-Objekt aktiv, bis die Lease für diese DHCP-Adresse abläuft. Es erfolgt jedoch keine Sitzungswiederverwendung, solange "ssg intercept dhcp" global konfiguriert ist.

Der "authorized arp" deaktiviert dynamisches ARP-Lernen auf der Schnittstelle, auf der es konfiguriert ist. Die einzigen ARP-Einträge auf der betreffenden Schnittstelle sind die Einträge, die der IOS DHCP-Server nach dem Leasing-Start hinzugefügt hat. Diese ARP-Einträge werden dann vom IOS DHCP-Server gelöscht, sobald der Lease beendet wurde. Dies geschieht entweder aufgrund des Eingangs einer DHCP-RELEASE, eines Lease-Ablaufs oder eines ARP-Probe-Fehlers aufgrund eines nicht ordnungsgemäßen DHCP-Abmelds.

Implementierungshinweise:

- Die "ssg auto-logoff arp" und "ssg auto-logoff icmp" sind unerwünschte Methoden, um die Wiederverwendung von Sitzungen oder daraus resultierende Sicherheitsprobleme zu verhindern. Die Varianten "arp" und "icmp" von "ssg auto-logoff" senden nur dann einen ARP- oder IMCP-PING, wenn der Datenverkehr innerhalb des konfigurierten "interval" nicht auf der SSG-Verbindung sichtbar ist. Der niedrigste Wert beträgt 30 Sekunden. Wenn DHCP eine zuvor verwendete IP-Adresse innerhalb von 30 Sekunden leasen oder ein böswilliger Benutzer innerhalb von 30 Sekunden statisch eine aktuell gebundene DHCP-Adresse konfiguriert, wird die Sitzung wiederverwendet, da SSG den Datenverkehr im Verbindungsobjekt erkennt und "ssg auto-logoff" nicht aufgerufen wird.
- In allen Anwendungsfällen wird die Wiederverwendung von Sitzungen nicht verhindert, wenn ein böswilliger Host einen MAC-Adressen-Spoof ausführt.

Tabelle 1: Überlegungen zur Wiederverwendung und Sicherheit von Sitzungen bei SSG-/DHCP-Bereitstellungen

Befehl	Funktion	Sicherheitsimplikationen
ssg auto-logoff arp [match-mac-address] [Intervallsekunden] ssg auto-logoff icmp [timeout Millisekunden] [Paketnummer] [Intervall-*Sekunden*]	Entfernt das SSG-Hostobjekt nach einem Ausfall von ARP oder ICMP PING, die nur gesendet werden, wenn innerhalb des "Intervalls" kein Datenverkehr in der SSG-Verbindung sichtbar ist.	Verwendet die Sitzung wieder, wenn DHCP innerhalb von 30 Sekunden eine zuvor verwendete IP-Adresse leasing oder ein böswilliger Benutzer innerhalb von 30 Sekunden statisch eine aktuell gebundene DHCP-Adresse konfiguriert, da SSG den Datenverkehr im Verbindungsobjekt erkennt und "ssg auto-logoff" nicht aufruft.
ssg DHCP	Erstellt	Verhindert, dass DHCP-

abfangen	SSG/DHCP Awareness, das das Löschen des SSG-Hostobjekts innerhalb dieser Ereignisse ermöglicht: Eine DHCPRELEASE wird für eine IP-Adresse empfangen, die mit einem Active Host-Objekt übereinstimmt. B. Der DHCP-Lease läuft für eine IP-Adresse ab, die mit einem Active Host-Objekt übereinstimmt.	Benutzer SSG-Sitzungen wiederverwenden, hindert statische Benutzer jedoch nicht daran, DHCP-Adressen zu imitieren oder SSG-Sitzungen wiederzuverwenden.
ip dhcp pool TEST update arp	Stellt sicher, dass das einzige IOS-Subsystem, das ARP-Einträge hinzufügen oder entfernen kann, das DHCP-Server-Subsystem ist.	Verhindert die Wiederverwendung aller Sitzungen, wenn sie mit "ssg intercept dhcp" konfiguriert werden. Wenn DHCP ohne "ssg intercept dhcp" konfiguriert wird und eine zuvor verwendete IP-Adresse leasen soll, ist eine Sitzungswiederverwendung weiterhin möglich.
interface FastEthernet0/0 arp authorized	Sendet periodische ARP-Anfragen an alle Hosts, um sicherzustellen, dass sie noch aktiv sind. Deaktiviert dynamisches ARP-Lernen.	Ermöglicht das Löschen von DHCP-Bindungen und ARP-Einträgen, wenn ein DHCP-Benutzer einen nicht-ordnungsgemäßen Abmelden durchführt.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems