Depuração de fluxo de chamada de um gateway de Internet SSG configurado com DHCP Secure ARP, chave de host do pacote de porta SSG, redirecionamento TCP SSG, SESM e consciência SSG/DHCP

Contents

Introduction

O foco deste documento é um IOS Internet Gateway que executa SSG e DHCP com SESM para serviços de portal.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

Informações de Apoio

Visão geral da tecnologia e dos recursos

Gateway de seleção de serviço (SSG)

O Service Selection Gateway (SSG) é uma solução de comutação para provedores de serviços que oferecem intranet, extranet e conexões de Internet a assinantes com tecnologia de acesso de banda larga, como DSL (Digital Subscriber Line), modems a cabo ou sem fio para permitir acesso simultâneo a serviços de rede.

O SSG trabalha em conjunto com o Cisco Subscriber Edge Services Manager (SESM). Junto com o SESM, o SSG fornece autenticação de assinantes, seleção de serviços e recursos de conexão de serviços para assinantes de serviços de Internet. Os assinantes interagem com um aplicativo da Web SESM usando um navegador da Internet padrão.

O SESM opera em dois modos:

- Modo RADIUS—Este modo obtém informações de assinante e serviço de um servidor RADIUS. O SESM no modo RADIUS é semelhante ao SSD.
- Modo LDAP—O modo LDAP (Lightweight Diretory Access Protocol) fornece acesso a um diretório compatível com LDAP para informações de perfil de assinante e serviço. Esse modo também tem funcionalidade aprimorada para aplicativos da Web do SESM e usa um modelo RBAC (controle de acesso baseado em função) para gerenciar o acesso do assinante.

Chave de host do pacote de porta SSG

O recurso Chave de host do pacote de portas SSG melhora a comunicação e a funcionalidade entre SSG e SESM com um mecanismo que usa o endereço IP origem do host e a porta origem para identificar e monitorar assinantes.

Com o recurso SSG Port-Bundle Host Key, o SSG executa a conversão de endereço de porta (PAT - Port-Bundle Host Key) e a conversão de endereço de rede (NAT - Network-Address Translation) no tráfego HTTP entre o assinante e o servidor SESM. Quando um assinante envia um pacote HTTP ao servidor SESM, o SSG cria um mapa de portas que altera o endereço IP origem para um endereço IP de origem SSG configurado e altera a porta TCP de origem para uma porta alocada pelo SSG. O SSG atribui um pacote de portas a cada assinante porque um assinante pode ter várias sessões TCP simultâneas quando acessa uma página da Web. A chave de host atribuída, ou combinação de pacote de porta e endereço IP de origem SSG, identifica exclusivamente cada assinante. A chave do host é transportada em pacotes RADIUS enviados entre o servidor SESM e o SSG no atributo específico do fornecedor (VSA) do IP do assinante. Quando o servidor SESM envia uma resposta ao assinante, o SSG converte o endereço IP destino e a porta TCP destino de acordo com o mapa de portas.

Redirecionamento TCP SSG para usuários não autenticados

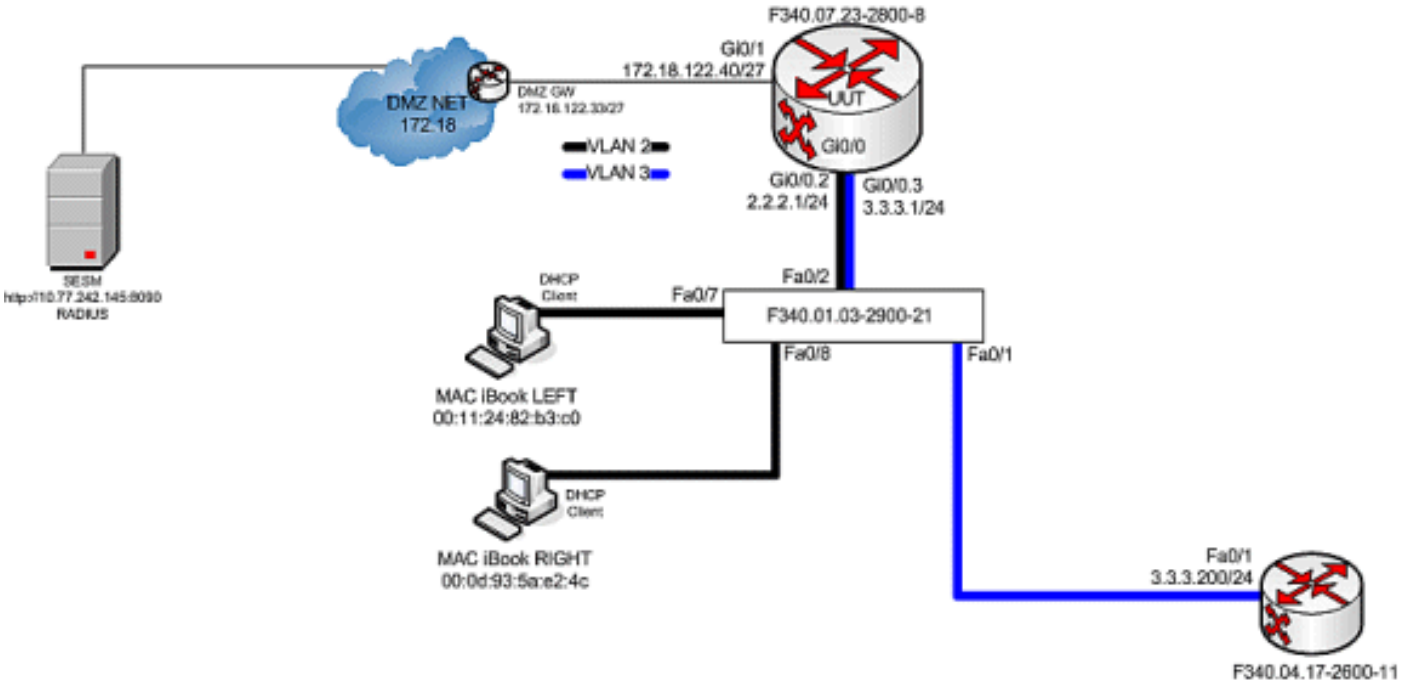
O redirecionamento para usuários não autenticados redireciona pacotes de um usuário se o usuário não tiver autorizado com o provedor de serviços. Quando um assinante não autorizado tenta se conectar a um serviço em uma porta TCP (por exemplo, a www.cisco.com), o SSG TCP Redirect redireciona o pacote para o portal cativo (SESM ou um grupo de dispositivos SESM). O

SESM emite um redirecionamento para o navegador para exibir a página de logon. O assinante faz login no SESM e é autenticado e autorizado. Em seguida, o SESM apresenta ao assinante uma página inicial personalizada, a página inicial do provedor de serviços ou o URL original.

Atribuição de endereço IP seguro de DHCP

O recurso DHCP Secure IP Address Assignment introduz a capacidade de proteger entradas da tabela ARP para locações do Dynamic Host Configuration Protocol (DHCP) no banco de dados DHCP. Esse recurso protege e sincroniza o endereço MAC do cliente com a associação DHCP, impedindo que clientes não autorizados ou hackers falsifiquem o servidor DHCP e assumam um aluguel de DHCP de um cliente autorizado. Quando esse recurso é ativado e o servidor DHCP atribui um endereço IP ao cliente DHCP, o servidor DHCP adiciona uma entrada ARP segura à tabela ARP com o endereço IP atribuído e o endereço MAC do cliente. Essa entrada ARP não pode ser atualizada por nenhum outro pacote ARP dinâmico, e essa entrada ARP existe na tabela ARP para o tempo de concessão configurado ou enquanto o leasing estiver ativo. A entrada ARP segura pode ser excluída somente por uma mensagem de terminação explícita do cliente DHCP ou do servidor DHCP quando a associação DHCP expira. Esse recurso pode ser configurado para uma nova rede DHCP ou usado para atualizar a segurança de uma rede atual. A configuração desse recurso não interrompe o serviço e não é visível para o cliente DHCP.

Diagrama testado



Depuração de fluxo de chamada

Conclua estes passos:

1. Quando o MAC iBook LEFT conecta pela primeira vez o cabo Ethernet a essa rede, ele aluga o endereço IP 2.2.2.5/29 do servidor DHCP do IOS executado em "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. Depois de alugar com êxito o endereço IP 2.2.2.5, o MAC iBook LEFT abre um navegador da Web e o aponta para **http://3.3.3.200**, que é usado para simular recursos protegidos vinculados ao SSG Service "distlearning". O SSG Service "distlearning" está definido localmente no roteador SSG "F340.07.23-2800-8":

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

   Na realidade, **http://3.3.3.200** é um roteador Cisco IOS configurado para "ip http server" e ouve no TCP 80, portanto, é basicamente um servidor web.Depois que o MAC iBook LEFT tenta navegar até **http://3.3.3.200**, já que essa conexão está entrando em uma interface configurada com "ssg direction downlink", o roteador SSG primeiro verifica a existência de um SSG Host Object ativo para o endereço IP origem da solicitação HTTP. Como esta é a primeira solicitação do endereço IP 2.2.2.5, um Objeto Host SSG não existe e um redirecionamento TCP para o SESM é instanciado para o host 2.2.2.5 através desta configuração:

```
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.
```

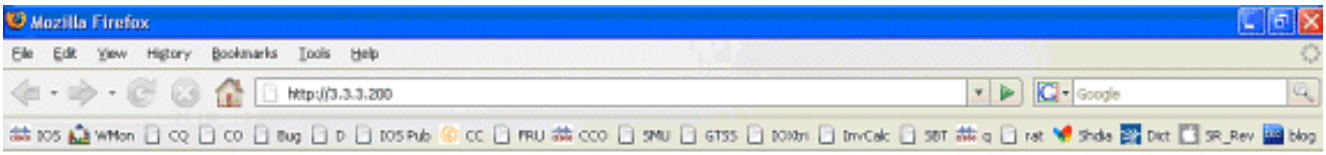
server-group ssg_tr_unauth
server 10.77.242.145 8090
10.77.242.145 is the SESM server and it's listening for HTTP on TCP 8090. "server" MUST be in default network or open-garden. **redirect port-list ports to ssg_tr_unauth**
redirect unauthenticated-user to ssg_tr_unauth
If an SSG router receives a packets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

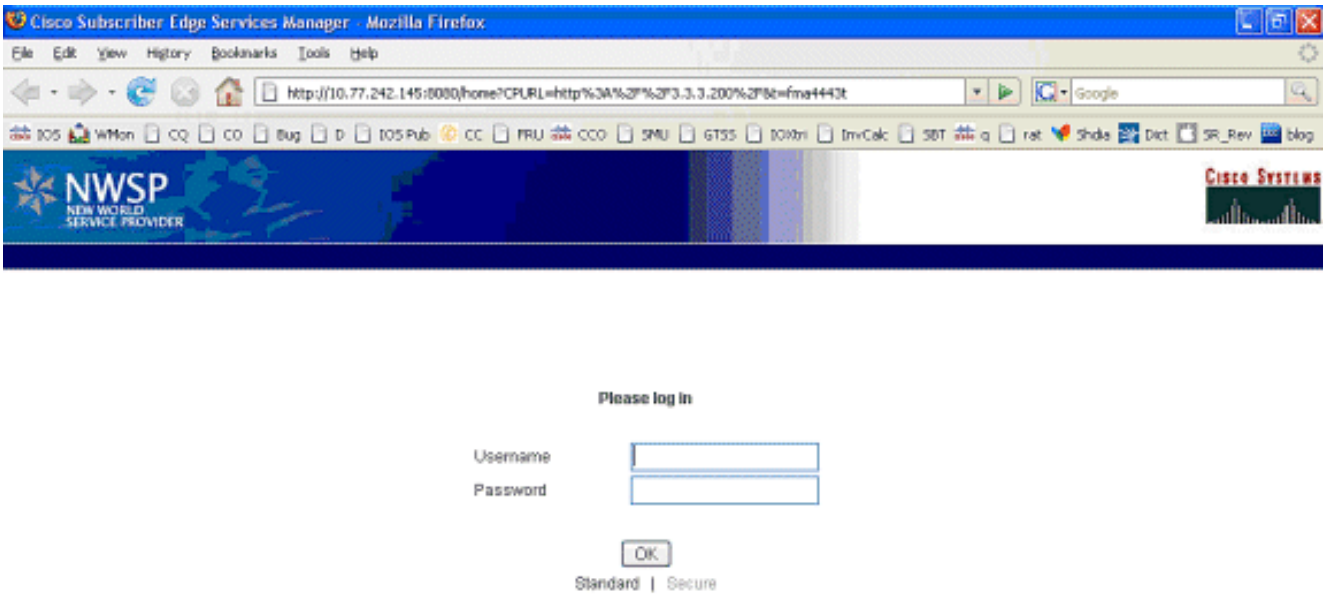
The initial HTTP request from 2.2.2.5 had a source TCP Port of 49273 and a destination IP address of 3.3.3.200 and TCP port of 80. Because of the SSG TCP Redirect, the destination IP header is overwritten with the socket of the SESM server 10.77.242.145:8090. If Port Bundle Host Key were NOT configured,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

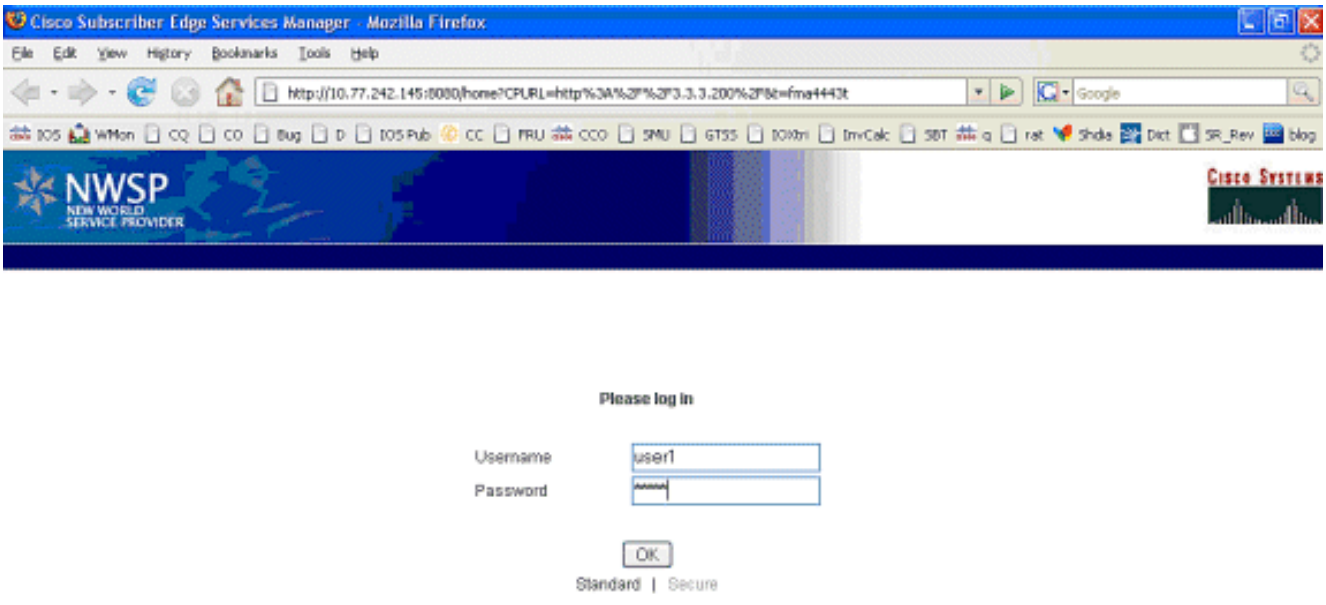
Neste ponto, o navegador no MAC iBook Left fica assim quando **http://3.3.3.200** é inserido:



Depois que o IOS SSG TCP e o SESM HTTP são redirecionados, a tela se parece com isto:



3. Depois que o SSG TCP redirecionar para o SESM e o redirecionamento HTTP subsequente enviado por SESM de volta ao navegador do MAC iBook Left, o MAC iBook Left insere **user1** como o nome de usuário e **cisco** como a senha:



4. Depois que o botão **OK** for pressionado, o SESM enviará essas credenciais ao roteador SSG por meio de um protocolo baseado em RADIUS proprietário.

```
*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. Por sua vez, o roteador SSG cria um pacote de solicitação de acesso RADIUS e o envia ao RADIUS para autenticar o **usuário1**:

```
*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 responde com um Access-Accept para **user1**, e um SSG Host Object é criado em "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
```

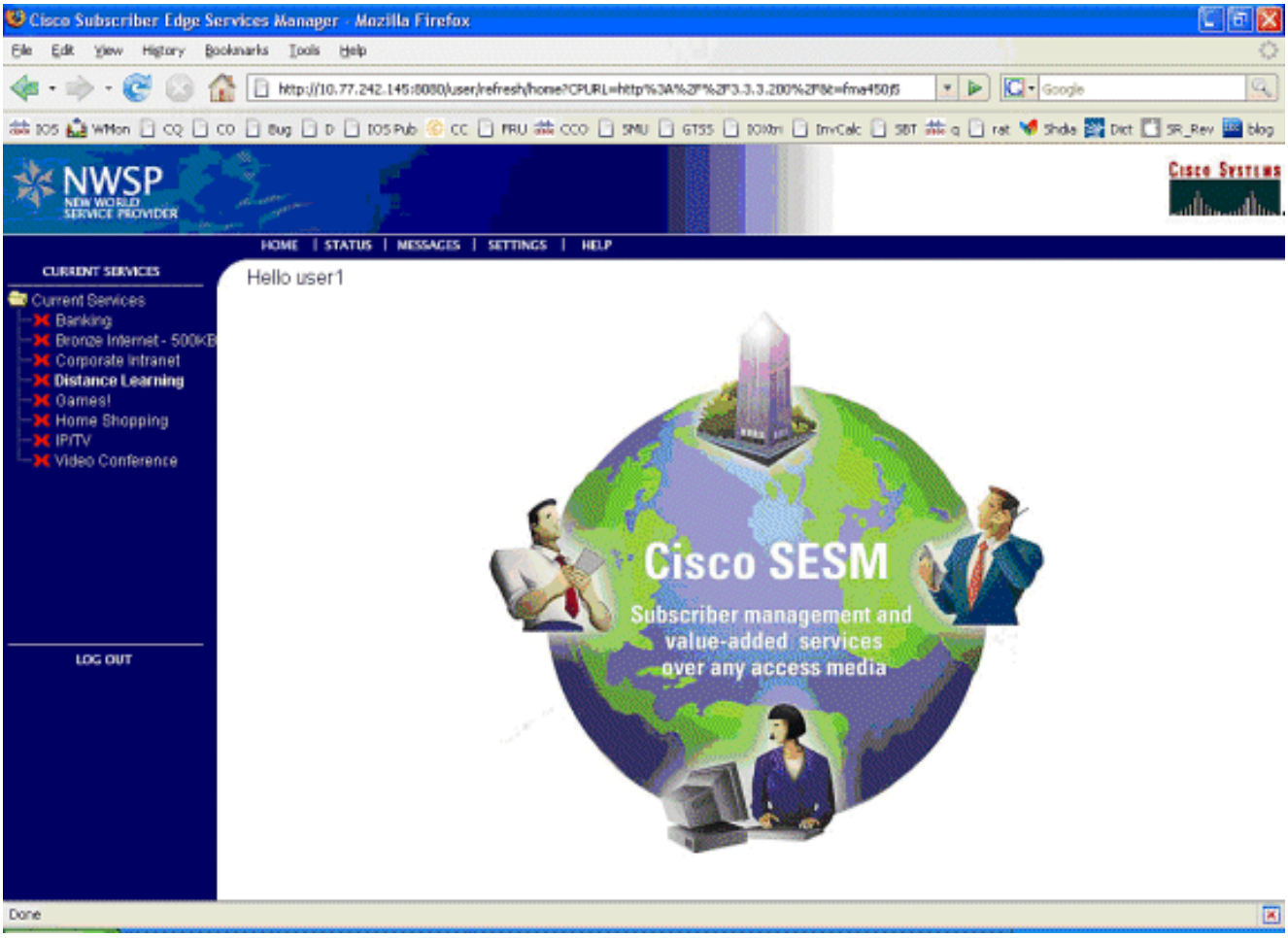
```
   [250] 7   "Niptv"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  14
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 8   "Ngames"
*Oct 13 20:25:02.081: RADIUS:  Vendor, Cisco
   [26]  18
*Oct 13 20:25:02.081: RADIUS:   ssg-account-info
   [250] 12  "Ndistlearn"
*Oct 13 20:25:02.081: 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. Neste ponto, **user1** é definido como um Objeto de Host SSG, mas ainda não tem acesso a nenhum Serviço SSG. MAC iBook Left (O MAC iBook Left) é apresentado com a tela Service Selection (Seleção de serviço) e clica em **Distance Learning (Aprendizado à distância)**:



8. Depois que o **Distance Learning** é clicado, a caixa SESM se comunica com o roteador SSG com o canal de controle:

```
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**

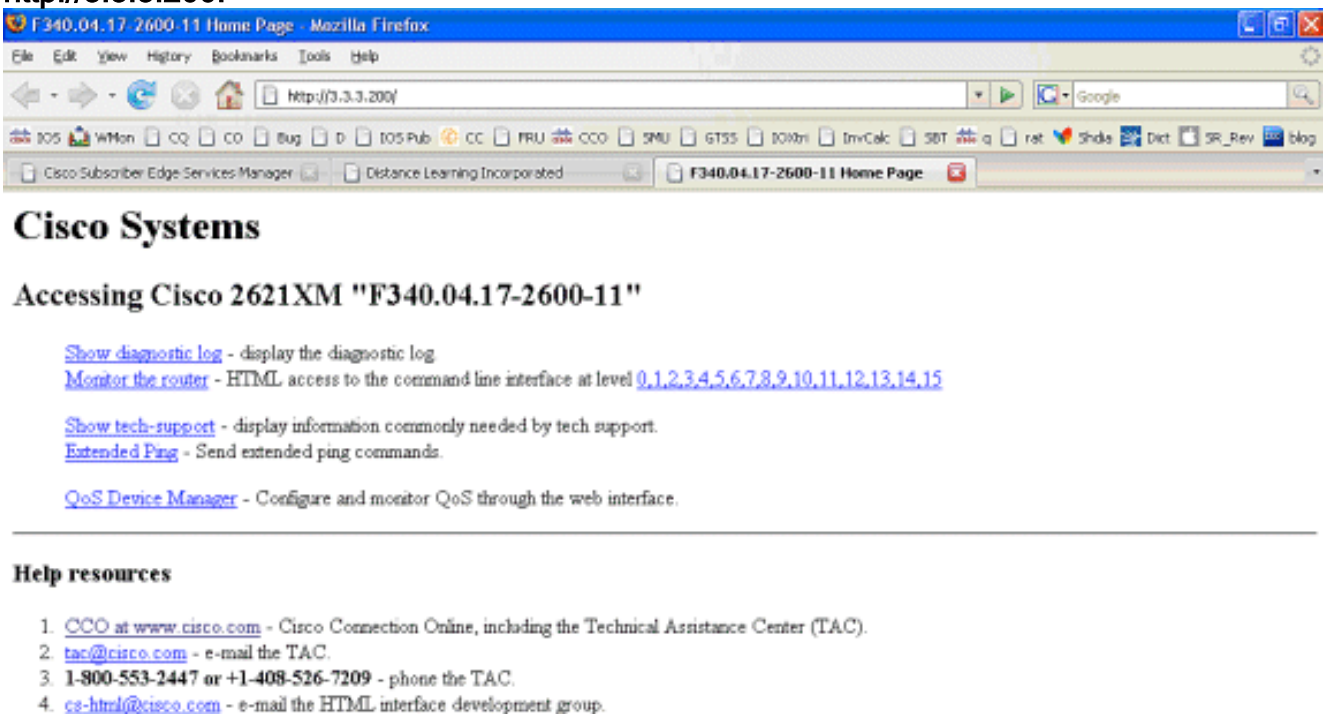
----------ConnectionObject Content ----
User Name: user1
Owner Host: 2.2.2.5
Associated Service: distlearn
Calling station id: 0011.2482.b3c0
Connection State: 0 (UP)
Connection Started since:
*20:40:21.000 UTC Mon Oct 13 2008

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. A conexão SSG está ativa e o fluxo de chamada está concluído. O MAC iBook Left pode navegar com êxito até
http://3.3.3.200:



Explicação de configuração do roteador SSG com documentos de recursos

```
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
```

Considerações sobre reutilização de sessão e segurança

Quando você usa SSG e DHCP juntos, esses cenários podem permitir que usuários mal-intencionados reutilizem um Objeto Host SSG autenticado que permita acesso não autenticado a recursos seguros:

- Se o reconhecimento de SSG/DHCP não estiver configurado com "ssg intercept dhcp", um novo usuário de DHCP poderá alugar um endereço IP anteriormente alugado para o qual ainda existe um objeto de host SSG. Como a primeira solicitação de TCP desse novo usuário tem um objeto de host SSG compatível, embora obsoleto, com o endereço IP de origem, esse usuário recebe o uso não autenticado de recursos protegidos. Isso pode ser evitado com "ssg intercept dhcp", o que resulta na remoção de um Objeto Host SSG quando:DHCPRELEASE é recebido para um endereço IP que corresponde a um Objeto de Host Ativo.O aluguel de DHCP expira para um endereço IP que corresponde a um Objeto de host ativo.
- Se um usuário DHCP socializar o endereço IP alugado a um usuário mal-intencionado antes de um logout DHCP não gracioso, que é um logout DHCP para o qual um DHCPRELEASE não é enviado, o usuário mal-intencionado pode configurar estaticamente a máquina com esse endereço IP e reutilizar o objeto Host SSG, seja configurado "ssg intercept dhcp". Isso pode ser evitado com uma combinação de "ssg intercept dhcp" e "update arp" configurados abaixo do pool de DHCP do IOS. A "arp de atualização" garante que o único subsistema IOS capaz de adicionar ou remover entradas ARP seja o subsistema do servidor DHCP. Com o "arp de atualização", a associação de DHCP IP para MAC sempre corresponde à associação IP para MAC na tabela ARP. Embora o usuário mal-intencionado tenha um endereço IP configurado estaticamente que corresponda ao objeto Host SSG, o tráfego não tem permissão para entrar no roteador SSG. Como o endereço MAC não corresponde ao endereço MAC da associação DHCP atual, o servidor DHCP do IOS impede a criação de uma entrada ARP.
- Quando o SSG e o DHCP são configurados juntos, "ssg intercept dhcp" e "update arp" impedem a reutilização da sessão. O desafio final não relacionado à segurança é liberar o aluguel de DHCP e a entrada ARP quando um host DHCP executa um logoff não gracioso. A configuração de "arp autorizado" na interface "ssg direction downlink" resulta em solicitações ARP periódicas enviadas a todos os hosts para garantir que eles ainda estejam ativos. Se nenhuma resposta for recebida dessas mensagens ARP periódicas, a associação DHCP será liberada e o subsistema DHCP do IOS eliminará a entrada ARP.

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

Neste exemplo, uma solicitação ARP é enviada periodicamente para atualizar todas as entradas ARP conhecidas em Fa0/0 a cada 5s. Após 15 falhas, a associação DHCP é

liberada e o subsistema DHCP do IOS elimina a entrada ARP.No contexto do SSG sem "arp autorizado", se um host DHCP executar um logoff não gracioso, o aluguel de DHCP e seu objeto host SSG associado permanecem ativos até que o aluguel desse endereço DHCP expire, mas nenhuma reutilização de sessão ocorre enquanto "ssg intercept dhcp" estiver configurado globalmente.

O "arp autorizado" desativa o aprendizado ARP dinâmico na interface em que está configurado. As únicas entradas ARP na interface em questão são aquelas adicionadas pelo servidor DHCP do IOS após um aluguel ser iniciado. Essas entradas ARP são limpas pelo servidor DHCP do IOS depois que a concessão é encerrada, seja por causa do recebimento de uma VERSÃO DHCP, uma expiração da concessão ou uma falha na prova ARP devido a um logoff DHCP não gracioso.

Notas de implementação:

- O "ssg autologoff arp" e o "ssg autologoff icmp" são métodos indesejáveis para evitar a reutilização da sessão ou problemas de segurança resultantes. As variantes "arp" e "icmp" de "logoff automático de ssg" somente enviam um PING ARP ou IMCP quando o tráfego não é visto na conexão SSG dentro do "intervalo" configurado, sendo que o mais baixo é de 30 segundos. Se o DHCP aluga um endereço IP usado anteriormente em 30 segundos, ou um usuário mal-intencionado configura estaticamente um endereço DHCP vinculado atualmente em 30 segundos, a sessão é reutilizada porque o SSG vê o tráfego no objeto de conexão, e o "logoff automático ssg" não é chamado.
- Em todos os casos de uso, a reutilização da sessão não é impedida se um host mal-intencionado executa uma falsificação de endereço MAC.

Tabela 1 - Considerações sobre reutilização de sessão e segurança em implantações de SSG/DHCP

Comando	Função	Implicações de segurança
ssg autologoff arp [match-mac-address] [intervalo *segundos*] **ssg autologoff icmp [timeout milliseconds] [número de pacotes] [intervalo *segundos*]**	Remove o Objeto Host SSG após falha do ARP ou do ICMP PING, que são enviados somente depois que não é visto nenhum tráfego na conexão SSG dentro do "intervalo".	Reutiliza a sessão se o DHCP aluga um endereço IP usado anteriormente em 30 segundos, ou se um usuário mal-intencionado configura estaticamente um endereço DHCP vinculado no momento em 30 segundos, porque o SSG vê o tráfego no objeto de conexão e o "logoff

		automático ssg" não chama.
ssg intercept dhcp	Cria a conscientização de SSG/DHCP que permite a exclusão do objeto de host SSG nesses eventos: Um DHCPRELEASE é recebido para um endereço IP que corresponde a um Objeto de Host Ativo. B. O aluguel de DHCP expira para um endereço IP que corresponde a um Objeto de host ativo.	Impede que os usuários DHCP reutilizem sessões SSG, mas não impede que os usuários estáticos falsifiquem endereços DHCP ou reutilizem sessões SSG.
ip dhcp pool TEST update arp	Garante que o único subsistema IOS capaz de adicionar ou remover entradas ARP é o subsistema do servidor DHCP.	Impede a reutilização de todas as sessões quando configurado com "ssg intercept dhcp". Quando configurado sem "ssg intercept dhcp", se o DHCP aluga um endereço IP usado anteriormente, a reutilização da sessão ainda é possível.
interface FastEthernet 0/0 arp autorizada	Envia solicitações ARP periódicas a todos os hosts para garantir que eles ainda estejam ativos. Desativa o aprendizado ARP dinâmico.	Permite associação de DHCP e exclusão de entrada ARP quando um usuário DHCP executa um logoff não gracioso.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems