A eliminação de erros do fluxo de chamadas de um Gateway de Internet SSG configurado com DHCP ARP seguro, chave Host do Porta-pacote SSG, SSG TCP reorienta, conscientização SES, e SSG/DHCP

Índice

Introdução

O foco deste documento é um Gateway de Internet IO que execute o SSG e o DHCP com o SES para serviços portais.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

convenções de documentos.

Informações de Apoio

Tecnologia e visão geral de características

Gateway de seleção de serviço (SSG)

O Service Selection Gateway (SSG) é uma solução de switching para os provedores de serviços que oferecem o intranet, o extranet, e as conexões com o Internet aos assinantes com tecnologia do acesso à banda larga, tal como digitais subscribers line (DSL), Modems a cabo, ou Sem fio permitir o acesso simultâneo aos serviços de rede.

O SSG trabalha conjuntamente com o Cisco Subscriber Edge Services Manager (SES). Junto com o SES, o SSG fornece a autenticação do subscritor, presta serviços de manutenção à seleção, e às capacidades da conexão do serviço aos assinantes dos serviços de Internet. Os assinantes interagem com um aplicativo de web SES usando um navegador de Internet padrão.

O SES opera-se em dois modos:

- Modo do RAIO — Este modo obtém o subscritor e a informação do serviço de um servidor Radius. O SES no modo do RAIO é similar ao SSD.
- Modo LDAP — O modo do Lightweight Directory Access Protocol (LDAP) fornece o acesso a um diretório LDAP-complacente para o subscritor e a informação do perfil do serviço. Este modo igualmente tem a funcionalidade aprimorada para aplicativos de web SES e usa um modelo papel-baseado do controle de acesso (RBAC) para controlar o acesso de assinante.

Chave Host do pacote da porta SSG

A característica de chave Host do Porta-pacote SSG aumenta uma comunicação e a funcionalidade entre o SSG e o SES com um mecanismo que use o endereço IP de origem e a porta de origem do host para identificar e monitorar assinantes.

Com a característica de chave Host do Porta-pacote SSG, o SSG executa a tradução de endereço de porta (PAT) e o Network Address Translation (NAT) no tráfego de HTTP entre o subscritor e o server SES. Quando um subscritor envia um pacote de HTTP ao server SES, o SSG cria um mapa de portas que mude o endereço IP de origem a um endereço IP de origem configurado SSG e mude a porta TCP da fonte a uma porta atribuída pelo SSG. O SSG atribui um pacote de portas a cada subscritor porque um subscritor pode ter diversas sessões de TCP simultâneas quando alcança um página da web. A chave Host atribuída, ou a combinação de porta-pacote e de endereço IP de origem SSG, identificam excepcionalmente cada subscritor. A chave Host é pacotes de informação de RADIUS dentro levados enviados entre o server SES e o SSG no atributo específico de fornecedor (VSA) IP do subscritor. Quando o server SES envia uma resposta ao subscritor, o SSG traduz a porta do endereço IP de destino e do TCP destino de acordo com o mapa de portas.

Reorientação SSG TCP para usuários não-autenticados

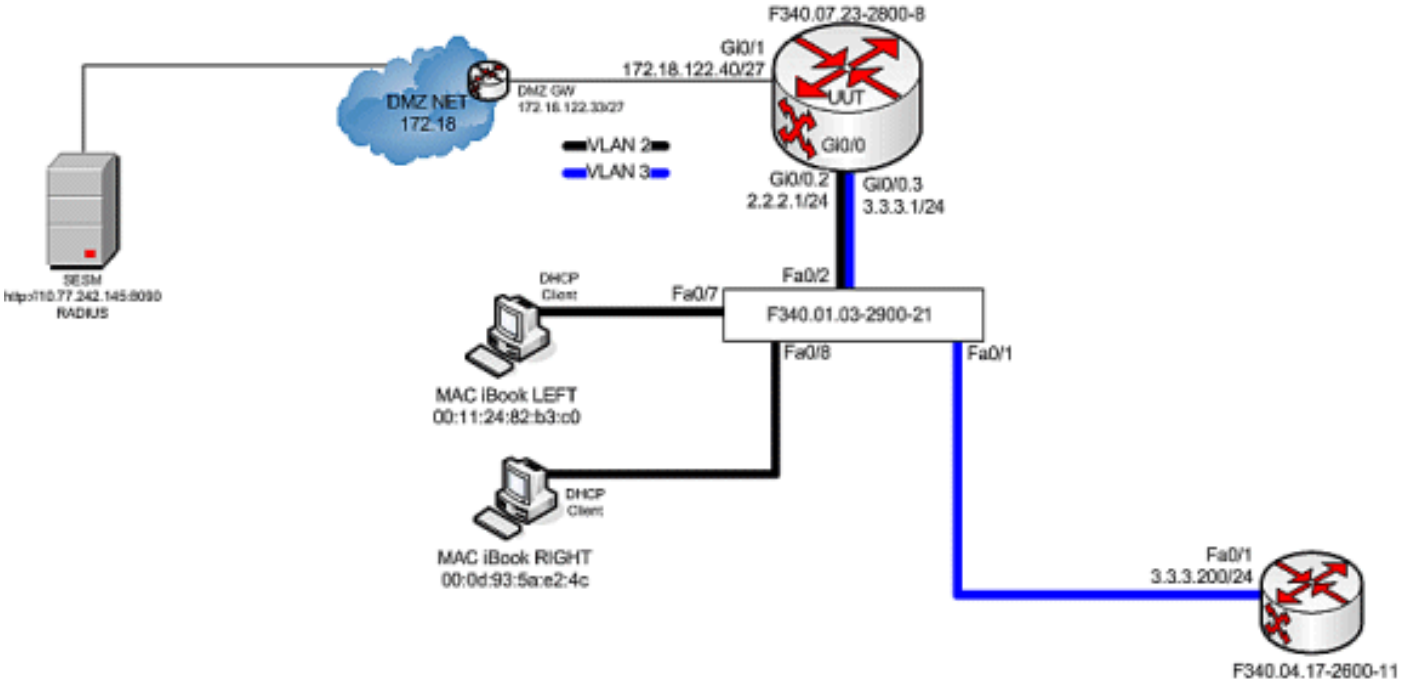
A reorientação para usuários não-autenticados reorienta pacotes de um usuário se o usuário não autorizou com o provedor de serviços. Quando um subscritor desautorizado tentar conectar a um serviço em uma porta TCP (por exemplo, a www.cisco.com), o SSG TCP reorienta reorienta o pacote ao portal prisioneiro (SES ou um grupo de dispositivos SES). O SES emite uma

reorientação ao navegador para indicar a página do fazer logon. O subscritor entra ao SES e é autenticado e autorizado. O SES apresenta então o subscritor com um Home Page personalizado, o Home Page do provedor de serviços, ou a URL original.

Atribuição fixada DHCP do endereço IP de Um ou Mais Servidores Cisco ICM NT

A característica segura da atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT DHCP introduz a capacidade de fixar registros de tabela ARP aos alugueres do protocolo de configuração dinâmica host (DHCP) no base de dados DHCP. Esta característica fixa e sincroniza o MAC address do cliente ao emperramento DHCP, impedindo clientes ou hacker desautorizados da falsificação o servidor DHCP e tomando sobre um aluguel de DHCP de um cliente autorizado. Quando esta característica está permitida, e o servidor DHCP atribui um endereço IP de Um ou Mais Servidores Cisco ICM NT ao DHCP Client, o servidor DHCP adiciona uma entrada de ARP segura à tabela ARP com o endereço IP atribuído e o MAC address do cliente. Esta entrada de ARP não pode ser atualizada por nenhuns outros pacotes ARP dinâmicos, e esta entrada de ARP existe na tabela ARP para o Lease Time configurado ou enquanto o aluguer é ativo. A entrada de ARP fixada pode ser suprimida somente por uma mensagem de terminação explícita do DHCP Client ou do servidor DHCP quando o emperramento DHCP expira. Esta característica pode ser configurada para uma rede nova DHCP ou ser usada para promover a Segurança de uma rede atual. A configuração desta característica não interrompe o serviço e não é visível ao DHCP Client.

Diagrama do Testbed



O fluxo de chamadas debuga

Conclua estes passos:

1. Quando o iBook MAC DEIXADO primeiramente conecta o cabo do Ethernet a esta rede, aluga o endereço IP de Um ou Mais Servidores Cisco ICM NT 2.2.2.5/29 do servidor DHCP IO que é 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 que aluga com sucesso o endereço IP 2.2.2.5, o iBook MAC DEIXADO abre um navegador da Web e aponta-o a **http://3.3.3.200**, que é usado para simular os recursos protegidos amarrados ao serviço “distlearn SSG.” O serviço “distlearn” SSG é definido localmente no roteador “F340.07.23-2800-8” SSG:

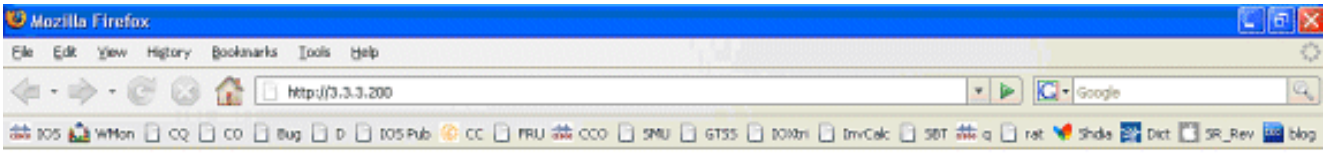
   local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255" Na realidade, **http://3.3.3.200** é um roteador do Cisco IOS configurado para do “o server HTTP de IP” e escuta em TCP 80, assim que é basicamente um servidor de Web.Depois que o iBook MAC SAIU de tentativas de consultar a **http://3.3.3.200**, desde que esta conexão é ingresso em uma relação configurada com do “downlink do sentido ssg,” as primeiras verificações do roteador SSG para a existência de um objeto ativo do host SSG para o endereço IP de origem do pedido do HTTP. Porque isto o primeiro tal pedido do endereço IP 2.2.2.5, um objeto do host SSG não existe, e um TCP reorienta para o SES instantiated para o host 2.2.2.5 com esta 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:

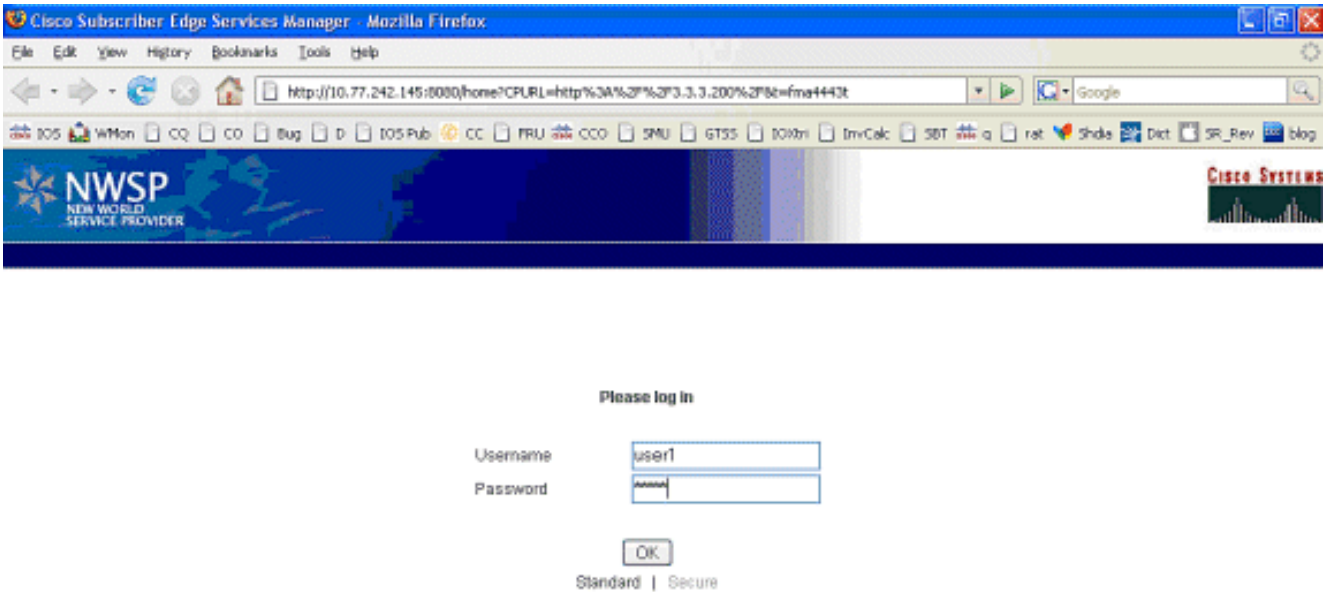
```
F340.07.23-2800-8#show ssg host ### Total HostObject Count: 0
```

Neste momento, o navegador no iBook MAC deixou olhares como este quando **http://3.3.3.200** é entrado:



Após os IO SSG TCP e SES O HTTP reorienta, os olhares da tela como esta:

3. Depois que o SSG TCP reorienta ao SES e o HTTP subsequente reorienta enviado pelo SES de volta ao navegador do iBook MAC à esquerda, o iBook MAC deixado entra no **usuário1** como o username e o **Cisco** como a senha:



4. Depois que o **botão OK** é empurrado, o SES envia ao roteador SSG estas credenciais com um protocolo Raio-baseado 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 constrói um pacote de solicitação de acesso do RAIO e envia-o ao RAIO 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
```

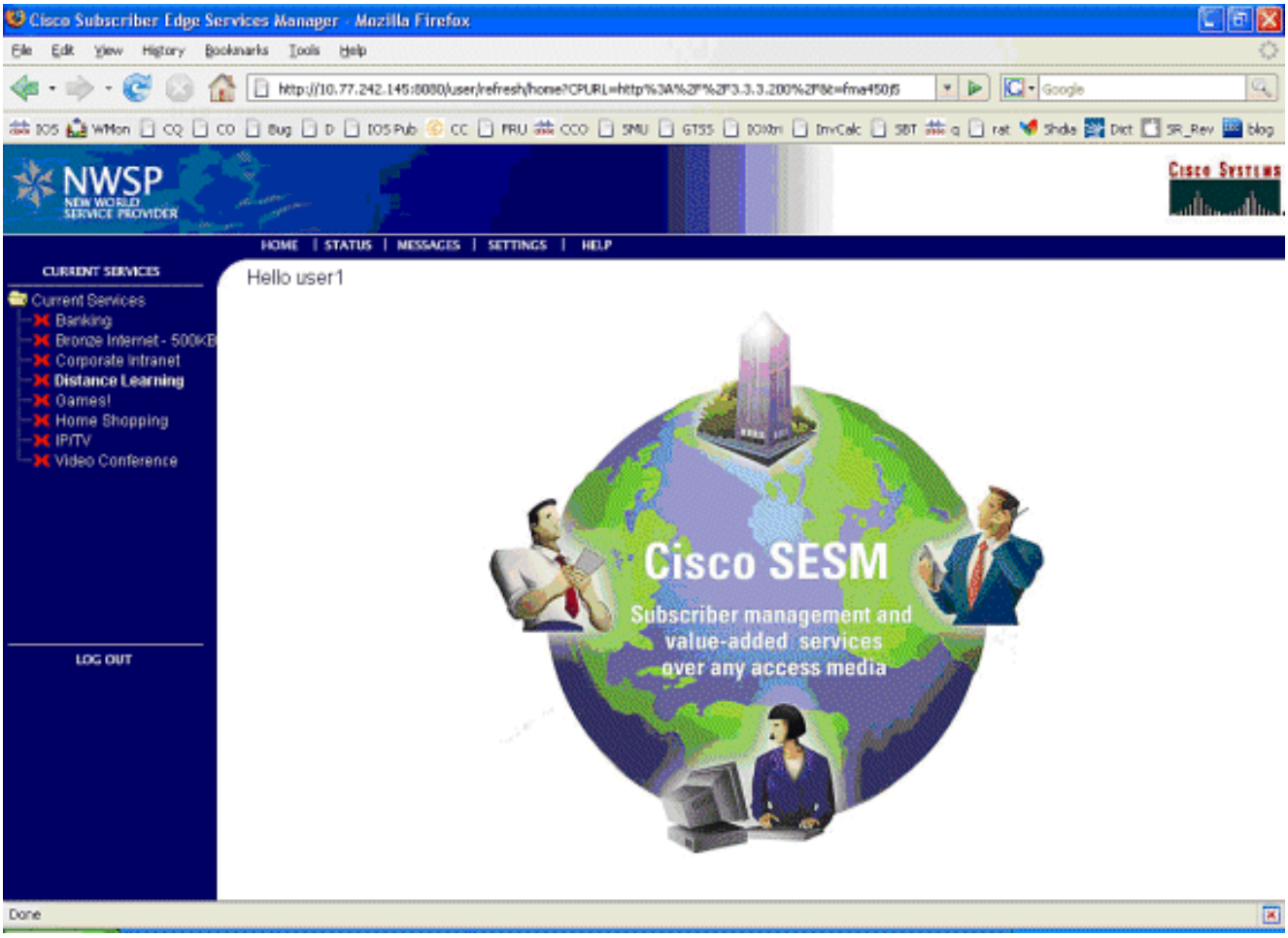
```
   [87]  9   "0/0/0/2"
*Oct 13 20:25:01.785: RADIUS:  NAS-IP-Address
   [4]   6   172.18.122.40
```

6. O RAIO responde com uma aceitação de acesso para o **usuário1**, e um objeto do host SSG 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 momento, o **usuário1** é definido como um objeto do host SSG mas não tem ainda o acesso a nenhuns serviços SSG. O iBook MAC deixado é presentado com a tela da seleção do serviço e clica o **Ensino à distância**:



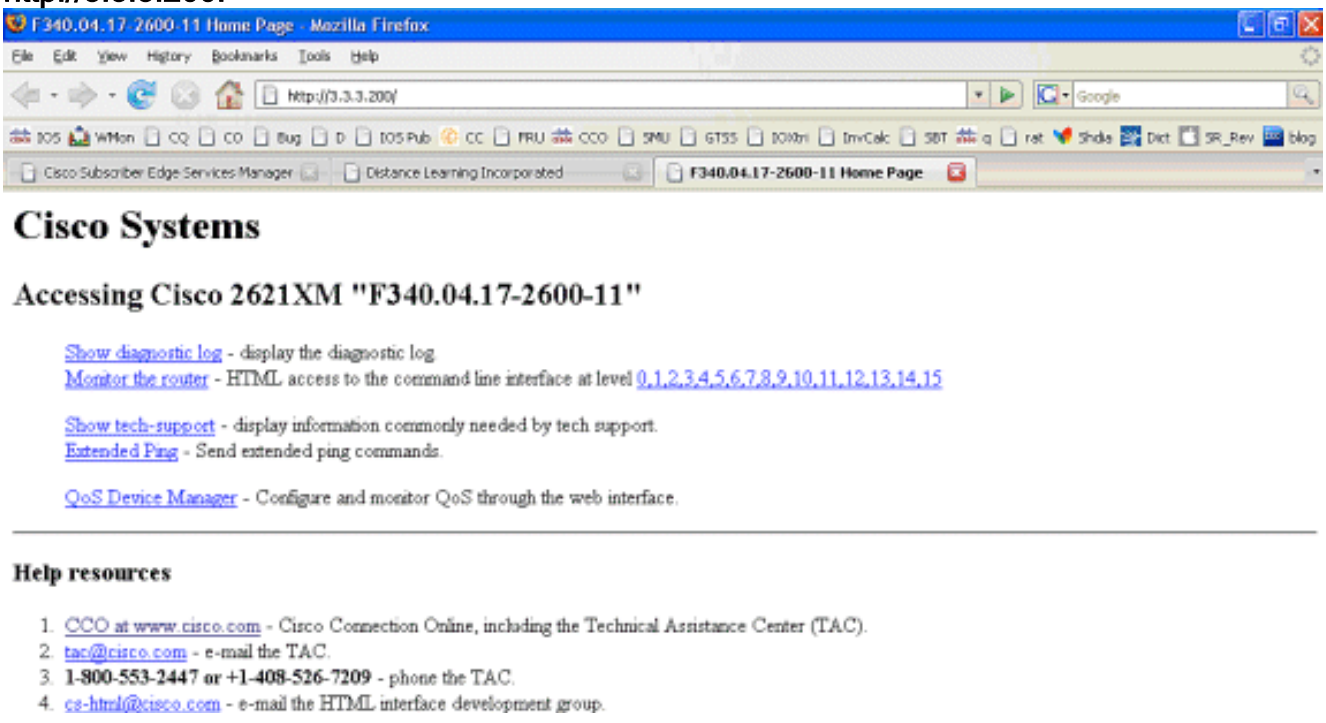
8. Depois que o **Ensino à distância** é clicado, a caixa SES comunica-se ao roteador SSG com o canal de controle:`debug ssg ctrl-events`

```
*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 acima, e o fluxo de chamadas é terminado. O iBook MAC deixado pode com sucesso consultar a http://3.3.3.200:



Explicação da configuração de roteador SSG com documentos da característica

```
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 da reutilização da Segurança e da sessão

Quando você usa o SSG e o DHCP junto, estas encenações podem permitir os usuários maliciosos reutilizem um objeto autenticado do host SSG que permitem que o acesso não-autenticado fixe recursos:

- Se a conscientização SSG/DHCP não é configurada com do "DHCP da intercepção ssg," um usuário novo DHCP pode alugar um endereço IP de Um ou Mais Servidores Cisco ICM NT precedente-alugado para que um objeto do host SSG ainda existe. Desde que o primeiro pedido TCP deste novo usuário tem uma harmonização, embora velho, do objeto do host SSG que combina o endereço IP de origem, este usuário é concedido o uso não-autenticado de recursos protegidos. Isto pode ser impedido com do "DHCP da intercepção ssg," que os resultados na remoção de um SSG hospedam o objeto quando qualquer um ocorre:DHCPRELEASE é recebido para um endereço IP de Um ou Mais Servidores Cisco ICM NT que combine um objeto do host ativo.O aluguel de DHCP expira para um endereço IP de Um ou Mais Servidores Cisco ICM NT que combine um objeto do host ativo.
- Se um usuário DHCP socializa o endereço IP de Um ou Mais Servidores Cisco ICM NT alugado a um usuário malicioso antes de uma saída NON-graciosa DHCP, que seja uma saída DHCP para que um DHCPRELEASE não é enviado, o usuário malicioso pode estaticamente configurar a máquina com este endereço IP de Um ou Mais Servidores Cisco ICM NT e reutilizar o objeto do host SSG mesmo se do "o DHCP da intercepção ssg" está configurado. Isto pode ser impedido com uma combinação do "de DHCP da intercepção ssg" e de "atualização arp" configurada debaixo do conjunto de DHCP IO. A "atualização arp" assegura-se de que o único subsistema IO capaz de adicionar ou remover entradas de ARP seja o subsistema do servidor DHCP. Com "atualização arp," o IP-à-MAC DHCP que liga

combina sempre o IP-à-MAC que liga na tabela ARP. Mesmo que o usuário malicioso tenha estaticamente um endereço IP configurado que combine o objeto do host SSG, o tráfego não é permitido inscrever o roteador SSG. Porque o MAC address não combina o MAC address do emperramento atual DHCP, o servidor DHCP IO impede a criação de uma entrada de ARP.

- Quando o SSG e o DHCP são configurados junto, do “o DHCP da intercepção ssg” e a “atualização arp” impedem a reutilização da sessão. NON-Segurança final o desafio relativo está livrar o aluguel de DHCP e a entrada de ARP quando um host DHCP executa uma saída NON-graciosa. A configuração “autorizou o arp” do “nos resultados da relação do downlink do sentido ssg” nas requisições ARP periódicas enviadas a todos os anfitriões para certificar-se que são ainda ativos. Se nenhuma resposta é recebida destes mensagens ARP periódicos, o emperramento DHCP está liberado, e o subsistema IO DHCP remove a entrada de 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 requisição ARP é enviada periodicamente refrescar todas as entradas de ARP conhecidas em Fa0/0 cada 5s. Após 15 falhas, o emperramento DHCP é liberado, e o subsistema IO DHCP remove a entrada de ARP.No contexto do SSG sem “autorizou o arp,” se um host DHCP executa uma saída NON-graciosa, o aluguel de DHCP e seu objeto associado do host SSG permanece ativo até que o aluguer para este endereço de DHCP expire, mas nenhuma reutilização da sessão ocorre enquanto do “o DHCP da intercepção ssg” está configurado globalmente.

“Autorizou o arp” desliga o ARP dinâmico que aprende na relação em que é configurada. As únicas entradas de ARP na relação na pergunta são aquelas adicionadas pelo servidor DHCP IO depois que um aluguer é começado. Estas entradas de ARP estão removidas então pelo servidor DHCP IO uma vez que o aluguer terminou, devido ao recibo de uma LIBERAÇÃO DHCP, de uma expiração do aluguer, ou de uma falha da ponta de prova ARP devido a uma saída NON-graciosa DHCP.

Notas da aplicação:

- Do “o auto-fazer logoff arp ssg” e do “o ICMP do auto-fazer logoff ssg” são métodos indesejáveis para impedir a reutilização da sessão ou questões de segurança resultantes. O “arp” e o “ICMP” variações do “do auto-fazer logoff ssg” enviam somente um ARP ou um IMCP PING quando o tráfego não é considerado na conexão SSG dentro do “intervalo configurado,” o mais baixo de que são 30 segundos. Se os aluguéis de DHCP um endereço IP de Um ou Mais Servidores Cisco ICM NT previamente usado dentro de 30 segundos, ou um usuário malicioso configuram estaticamente um endereço de DHCP do atual-limite dentro de 30 segundos, a sessão está reutilizada porque o SSG vê o tráfego no objeto de conexão, e do “o auto-fazer logoff ssg” não invoca.
- Em todos os casos do uso, a reutilização da sessão não é impedida se um host malicioso executa um spoof do MAC address.

Tabela 1 – Reutilização e considerações de segurança da sessão em disposições SSG/DHCP

Comando	Função	Implicações de segurança
[interval seconds] do [packets	Remove o objeto do host SSG após a	Reutiliza a sessão se os aluguéis de DHCP um endereço IP de Um ou

number] do [timeout milliseconds] ICMP do auto-fazer logoff do ssg do [interval seconds] do [match-mac-address] arp do auto-fazer logoff do ssg	falha do ARP ou do PING ICMP, que são enviados somente depois que o sem tráfego é considerado na conexão SSG dentro do "intervalo."	Mais Servidores Cisco ICM NT previamente usado dentro de 30 segundos, ou um usuário malicioso configuram estaticamente um endereço de DHCP do atual-limite dentro de 30 segundos porque o SSG vê o tráfego no objeto de conexão, e do "o auto-fazer logoff ssg" não invoca.
DHCP da intercepção do ssg	Cria a conscientizaçã o SSG/DHCP que permite o supressão do objeto do host SSG dentro destes eventos: Um DHCPRELEAS E é recebido para um endereço IP de Um ou Mais Servidores Cisco ICM NT que combine um objeto do host ativo. B. O aluguel de DHCP expira para um endereço IP de Um ou Mais Servidores Cisco ICM NT que combine um objeto do host ativo.	Impede usuários DHCP da reutilização de sessões SSG mas não impede usuários estáticos dos endereços de DHCP da falsificação ou da reutilização de sessões SSG.
atualização arp do TESTE do pool DHCP IP	Assegura-se de que o único subsistema IO capaz da adição ou da remoção das entradas de ARP seja o subsistema do servidor DHCP.	Impede toda a reutilização da sessão quando configurado com do "DHCP da intercepção ssg." Quando configurado sem do "DHCP da intercepção ssg," se os aluguéis de DHCP um endereço IP de Um ou Mais Servidores Cisco

		ICM NT previamente usado, reutilização da sessão são ainda possíveis.
FastEthernet 0/0 arp da relação autorizado	Envia requisições ARP periódicas a todos os anfitriões certificar-se que são ainda ativas. Desliga o ARP dinâmico que aprende.	Permite o emperramento DHCP e o supressão da entrada de ARP quando um usuário DHCP executa uma saída NON-graciosa.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems