El debugging del flujo de llamada de un gateway de Internet SSG configurado con el DHCP ARP seguro, clave de host del Puerto-conjunto SSG, SSG TCP reorienta, conciencia SES, y SSG/DHCP

Contenido

Introducción

El foco de este documento es un gateway de Internet IOS que ejecuta el SSG y el DHCP con el SES para los servicios porta.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Tecnología y descripción general de características

Gateway de selección de servicio (SSG)

El Service Selection Gateway (SSG) es un Switching Solution para los proveedores de servicio que ofrecen el intranet, el extranet, y las conexiones de Internet a los suscriptores con la tecnología del acceso por banda ancha, tal como Digital Subscriber Line (DSL), Cable módems, o Tecnología inalámbrica para permitir el acceso simultáneo a los servicios de red.

El SSG trabaja conjuntamente con el Cisco Subscriber Edge Services Manager (SES). Así como el SES, el SSG proporciona la autenticación del suscriptor, mantiene la selección, y las capacidades de la conexión del servicio a los suscriptores de los servicios de Internet. Los suscriptores obran recíprocamente con una aplicación de Web SES usando un buscador de Internet estándar.

El SES actúa en dos modos:

- Modo RADIUS — Este modo obtiene el suscriptor y la información de servicios de un servidor de RADIUS. El SES en el modo RADIUS es similar al SSD.
- Modo LDAP — El modo del Lightweight Directory Access Protocol (LDAP) proporciona el acceso a un directorio LDAP-obediente para el suscriptor y la información del perfil del servicio. Este modo también tiene funcionalidad mejorada para las aplicaciones de Web SES y utiliza un modelo papel-basado del control de acceso (RBAC) para manejar el acceso del suscriptor.

Clave de host del conjunto del puerto SSG

La característica de clave de host del Puerto-conjunto SSG aumenta la comunicación y las funciones entre el SSG y el SES con un mecanismo que utilice la dirección IP de origen y el puerto de origen del host para identificar y para monitorear a los suscriptores.

Con la característica de clave de host del Puerto-conjunto SSG, el SSG realiza el Port Address Translation (PAT) y el Network Address Translation (NAT) en el tráfico HTTP entre el suscriptor y el servidor SES. Cuando un suscriptor envía un paquete HTTP al servidor SES, el SSG crea un mapa del puerto que cambie la dirección IP de origen a una dirección IP de origen configurada SSG y cambie el puerto TCP de la fuente a un puerto afectado un aparato por el SSG. El SSG asigna a un conjunto de puertos a cada suscriptor porque un suscriptor puede tener varias sesiones TCP simultáneas cuando accede una página web. La clave de host asignada, o la combinación de puerto-conjunto y de dirección IP de origen SSG, identifica únicamente a cada suscriptor. La clave de host es adentro llevados paquetes RADIUS enviados entre el servidor SES y el SSG en el Atributo específico del proveedor (VSA) IP del suscriptor. Cuando el servidor SES envía una contestación al suscriptor, el SSG traduce el puerto del IP Address de destino y del TCP de destino de acuerdo con el mapa del puerto.

Cambio de dirección SSG TCP para los usuarios de unauthenticated

El cambio de dirección para los usuarios de unauthenticated reorienta los paquetes de un usuario

si el usuario no ha autorizado con el proveedor de servicio. Cuando un suscriptor desautorizado intenta conectar con un servicio en un puerto TCP (por ejemplo, a www.cisco.com), el SSG TCP reorienta reorienta el paquete al portal prisionero (SES o un grupo de los dispositivos SES). El SES publica una reorientación al navegador para visualizar la página del inicio. El suscriptor abre una sesión al SES y se autentica y se autoriza. El SES entonces presenta al suscriptor con un Home Page personalizado, el Home Page del proveedor de servicio, o el URL original.

DHCP Secured IP Address Assignment

La característica segura de la asignación de la dirección IP del DHCP introduce la capacidad para asegurar las entradas de tabla ARP a los arriendos del Protocolo de configuración dinámica de host (DHCP) en la base de datos del DHCP. Esta característica asegura y sincroniza el MAC address del cliente al DHCP que ata, previniendo los clientes o a los hackers desautorizados del spoofing el servidor DHCP y asumiendo el control un arriendo del DHCP de un cliente autorizado. Cuando se habilita esta característica, y el servidor DHCP asigna una dirección IP al Cliente de DHCP, el servidor DHCP agrega una entrada ARP segura a la tabla ARP con el IP Address asignado y la dirección MAC del cliente. Esta entrada ARP no se puede poner al día por ninguna otra paquetes ARP dinámica, y esta entrada ARP existe en la tabla ARP por el Tiempo de validez configurado o mientras el arriendo sea activo. La entrada ARP asegurada se puede borrar solamente por un mensaje de terminación explícito del Cliente de DHCP o del servidor DHCP cuando expira el atar del DHCP. Esta característica se puede configurar para una nueva red del DHCP o utilizar para actualizar la Seguridad de una red actual. La configuración de esta característica no interrumpe el servicio y no es visible al Cliente de DHCP.

Diagrama del banco de pruebas

Debug del flujo de llamada

Complete estos pasos:

1. Cuando el iBook MAC DEJADO primero conecta el cable Ethernet con esta red, arrienda la dirección IP 2.2.2.5/29 del servidor DHCP IOS que se ejecuta en “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. Después de que arriende con éxito a la dirección IP 2.2.2.5, el iBook MAC DEJADO abre a un buscador Web y lo señala a **http://3.3.3.200**, que se utiliza para simular los recursos protegidos atados al servicio “distlearn SSG.” El servicio “distlearn” SSG localmente se define en el router “F340.07.23-2800-8” SSG:

local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255" En la realidad, **http://3.3.3.200** es un router del Cisco IOS configurado para “ip http el servidor” y escucha en TCP 80, así que es básicamente servidor Web.Después de que el iBook MAC SALIERA de las tentativas de hojear a **http://3.3.3.200**, puesto que esta conexión es ingreso en una interfaz configurada con “el link descendente de la dirección del ssg,” las en primer lugar controles del router SSG para la existencia de un objeto activo del host SSG para la dirección IP de origen del pedido de HTTP. Porque no existe esto el primer tal petición de la dirección IP 2.2.2.5, un objeto del host SSG, y un TCP reorienta hacia el SES se ejemplifica para el host 2.2.2.5 con esta configuración:

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` En este momento, el hojeador en el iBook MAC salió de los parecer esto cuando se ingresa **http://3.3.3.200**:Después del IOS SSG TCP y SES EL HTTP reorienta, los parecer de la pantalla esto:

3. Después de que el SSG TCP reoriente al SES y el HTTP subsiguiente reorienta enviado por el SES de nuevo al hojeador del iBook MAC a la izquierda, el iBook MAC dejado ingresa el **user1** como el nombre de usuario y **Cisco** como la contraseña:
4. Después de que se avance el **botón OK**, el SES envía el router SSG estas credenciales con un protocolo basado en RADIUS propietario.
```
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Received cmd (1,user1) from Host-Key
   172.18.122.40:64
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Add cmd=1 from Host-Key 172.18.122.40:64
   into SSG control cmd queue.
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Dequeue cmd_ctx from the cmdQ
   and pass it to cmd handler
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Handling account logon for host
   172.18.122.40:64
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   No auto-domain selected for user user1
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Authenticating user user1.
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   ssg_aaa_nasport_fixup function
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   slot=0, adapter=0, port=0, vlan-id=2,
   dot1q-tunnel-id=0, vpi=0, vci=0, type=10
*Oct 13 20:25:01.781: SSG-CTL-EVN:
   Deleting SSGCommandContext
   ::~SSGCommandContext
```
5. A su vez, el router SSG construye un paquete access-request RADIUS y lo envía al RADIUS para autenticar el **user1**:
```
*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. El RADIUS responde con un access-accept para el **user1**, y un objeto del host SSG se crea en "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. En este momento, el **user1** se define como objeto del host SSG pero todavía no tiene acceso a ningunos servicios SSG. El iBook MAC dejado se presenta con la pantalla de la selección del servicio y hace clic el **Aprendizaje a distancia**:
8. Después de que se haga clic el **Aprendizaje a distancia**, el cuadro SES comunica al router SSG con el canal de control:`debug ssg ctrl-events`

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

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

Init servQ and start new process for distlearn *Oct 13 20:25:38.029: SSG-CTL-EVN: Service(distlearn)::AddRef(): ref after = 1 *Oct 13 20:25:38.029: SSG-CTL-EVN: **Got profile for distlearn locally** *Since "distlearn" is available from local configuration:* local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255" *...we don't need to make a AAA call to download SSG Service Information. However, please note that in most real-world SSG implementations, SSG Services are defined on the RADIUS AAA Server.* *Oct 13 20:25:38.029: SSG-CTL-EVN: Create a new service table for distlearn *Oct 13 20:25:38.029: SSG-CTL-EVN: Service bound on this interface are : distlearn *Oct 13 20:25:38.029: SSG-CTL-EVN: Service distlearn bound to interface GigabitEthernet0/0.3 firsthop 0.0.0.0 *Oct 13 20:25:38.029: Service Address List : *Oct 13 20:25:38.033: Addr:3.3.3.200 mask:255.255.255.255 *Oct 13 20:25:38.033: SSG-CTL-EVN: Add a new service distlearn to an existing table *Here the SSG creates a Service Table for distlearn and binds it to an "ssg direction uplink" interface complete with the R attribute for the Service.* *Oct 13 20:25:38.033: SSG-CTL-EVN: Locating the HostObject for Host-Key 172.18.122.40:64 *Oct 13 20:25:38.033: SSG-CTL-EVN: Checking connection activation for 172.18.122.40:64 to distlearn. *Oct 13 20:25:38.033: SSG-CTL-EVN: Creating ConnectionObject (172.18.122.40:64, distlearn) *Oct 13 20:25:38.033: SSG-EVN: ConnectionObject::ConnectionObject: size = 304 *Oct 13 20:25:38.033: SSG-CTL-EVN: Service(distlearn)::AddRef(): ref after = 2 *Oct 13 20:25:38.033: SSG-CTL-EVN: Checking maximum service count. *Oct 13 20:25:38.033: SSG-EVN: Opening connection for user user1 *Oct 13 20:25:38.033: SSG-EVN: Connection opened *Oct 13 20:25:38.033: **SSG-CTL-EVN: Service logon is accepted.** *Oct 13 20:25:38.033: SSG-CTL-EVN: **Activating the ConnectionObject.** *Once the Service is verified locally, SSG needs to build a "Connection" where a "Connection" is a tuple with: A. SSG Host Object B. SSG Service Name and Attributes C. SSG Downlink interface D. SSG Upstream interface* A-D are used to create a pseudo hidden VRF service table for which traffic from this host can transit. See here: F340.07.23-2800-8#**show ssg connection 2.2.2.5 distlearn** ---------- ConnectionObject Content ---- User Name: user1 Owner Host: 2.2.2.5 Associated Service: distlearn Calling station id: 0011.2482.b3c0 Connection State: 0 (UP) Connection Started since: *20:40:21.000 UTC Mon Oct 13 2008 User last activity at: *20:41:04.000 UTC Mon Oct 13 2008 Connection Traffic Statistics: Input Bytes = 420, Input packets = 5 Output Bytes = 420, Output packets = 5 Session policing disabled F340.07.23-2800-8#**show ssg host 2.2.2.5** ---------- HostObject Content ---------- Activated: TRUE Interface: GigabitEthernet0/0.2 User Name: user1 Host IP: 2.2.2.5 Host mac-address: 0011.2482.b3c0 Port Bundle: 172.18.122.40:64 Msg IP: 0.0.0.0 (0) Host DNS IP: 0.0.0.0 Host DHCP pool : Maximum Session Timeout: 64800 seconds Action on session timeout: Terminate Host Idle Timeout: 0 seconds User policing disabled User logged on since: *20:37:05.000 UTC Mon Oct 13 2008 User last activity at: *20:40:23.000 UTC Mon Oct 13 2008 SMTP Forwarding: NO Initial TCP captivate: NO TCP Advertisement captivate: NO Default Service: NONE DNS Default Service: NONE **Active Services: distlearn;** AutoService: Internet-Basic; Subscribed Services: Internet-Basic; iptv; games; distlearn; corporate; home_shopping; banking; vidconf; Subscribed Service Groups: NONE

9. La conexión SSG está para arriba, y se completa el flujo de llamada. El iBook MAC dejado puede hojear con éxito a **http://3.3.3.200:**

Explicación de la configuración del router SSG con los documentos de la 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

Consideraciones de la reutilización de la Seguridad y de la sesión

Cuando usted utiliza el SSG y el DHCP junto, estos escenarios pueden permitir los usuarios malintencionados reutilicen un objeto autenticado del host SSG que permiten que el acceso del unauthenticated asegure los recursos:

- Si la conciencia SSG/DHCP no se configura con "el DHCP de la interceptación del ssg," un nuevo usuario del DHCP puede arrendar una dirección IP anterior-arrendada para la cual un objeto del host SSG todavía exista. Puesto que la primera solicitud TCP de este usuario nuevo tiene corresponder con, aunque sea añeja, el objeto del host SSG que hace juego la dirección IP de origen, conceden este usuario el uso del unauthenticated de los recursos protegidos. Esto se puede prevenir con "el DHCP de la interceptación del ssg," que los resultados en el retiro de un SSG reciben el objeto cuando ocurre cualquiera:DHCPRELEASE se recibe para una dirección IP que haga juego un objeto del host activo.El arriendo del DHCP expira para una dirección IP que haga juego un objeto del host activo.
- Si un usuario del DHCP socializa la dirección IP arrendada a un usuario malintencionado antes de un logout NON-agraciado del DHCP, que es un logout del DHCP para el cual un DHCPRELEASE no se envía, el usuario malintencionado puede configurar estáticamente la máquina con esta dirección IP y reutilizar el objeto del host SSG independientemente de si "el DHCP de la interceptación del ssg" está configurado. Esto se puede prevenir con una combinación "de DHCP de la interceptación del ssg" y de la "actualización arp" configurada por debajo el agrupamiento DHCP IOS. La "actualización arp" se asegura de que el único subsistema IOS capaz de agregar o de quitar las entradas ARP sea el subsistema del servidor DHCP. Con la "actualización arp," el DHCP IP-A-MAC que ata hace juego siempre el IP-a-MAC que ata en la tabla ARP. Aunque el usuario malévolo tiene estáticamente un IP Address configurado que corresponda con el objeto del host SSG, el tráfico no se permite ingresar al router SSG. Porque la dirección MAC no hace juego la dirección MAC del DHCP

actual que ata, el servidor DHCP IOS previene la creación de una entrada ARP.

- Cuando se configuran juntos el SSG y el DHCP, “el DHCP de la interceptación del ssg” y la “actualización arp” previenen la reutilización de la sesión. El desafío relacionado NON-Seguridad final está liberar el arriendo y la entrada ARP del DHCP cuando un host del DHCP realiza un logout NON-agraciado. La configuración “arp autorizado” en “de la interfaz del link descendente de la dirección del ssg” da lugar a los pedidos ARP periódicos enviados a todos los host para aseegurarse los es todavía activa. Si no se recibe ninguna respuesta de estos mensajes ARP periódicos, se libera el atar del DHCP, y el subsistema del DHCP IOS purga la entrada ARP.
```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
arp authorized
arp probe interval 5 count 15
```
En este ejemplo, un pedido ARP se envía periódicamente de restaurar todas las entradas ARP conocidas en Fa0/0 cada 5s. Después de 15 errores, se libera el atar del DHCP, y el subsistema del DHCP IOS purga la entrada ARP.En el contexto del SSG sin “autorizó el arp,” si un host del DHCP realiza un logout NON-agraciado, el arriendo del DHCP y su objeto asociado del host SSG sigue siendo activo hasta que expire el arriendo para este DHCP Address, pero ocurre ninguna reutilización de la sesión mientras “el DHCP de la interceptación del ssg” se configure global.

“Autorizó el arp” apaga el ARP dinámico que aprendía en la interfaz en la cual se configura. Las únicas entradas ARP en la interfaz en la pregunta son ésas agregadas por el servidor DHCP IOS después de que se comience un arriendo. Estas entradas ARP entonces son purgadas por el servidor DHCP IOS una vez que el arriendo ha terminado, debido al recibo de una VERSIÓN del DHCP, de una expiración del arriendo, o de un error de la sonda ARP debido a un logout NON-agraciado del DHCP.

Notas de la implementación:

- El “auto-cierre de sesión arp del ssg” y “el ICMP del auto-cierre de sesión del ssg” son métodos indeseables para prevenir la reutilización de la sesión o los problemas de seguridad resultantes. El “arp” y el “ICMP” variantes del “auto-cierre de sesión del ssg” envían solamente un PING ARP o IMCP cuando el tráfico no se considera en la conexión SSG dentro del “intervalo configurado,” el más bajo cuyo son 30 segundos. Si el DHCP arrienda una dirección IP previamente usada en el plazo de 30 segundos, o un usuario malintencionado configura estáticamente un DHCP Address del actual-límite en el plazo de 30 segundos, se reutiliza la sesión porque el SSG ve el tráfico en el objeto de conexión, y el “auto-cierre de sesión del ssg” no invoca.
- En todos los casos del uso, la reutilización de la sesión no se previene si un host malévolo realiza un spoof de la dirección MAC.

Cuadro 1 – Reutilización y observaciones de seguridad de la sesión en las implementaciones SSG/DHCP

Comando	Función	Consecuencias en la seguridad
[interval seconds] del [packets number] del [timeout milliseconds	Quita el objeto del host SSG después del error de ARP o de PING DE ICMP, que se envían solamente después	Reutiliza la sesión si el DHCP arrienda una dirección IP previamente usada en el plazo de 30 segundos, o un

] ICMP del auto-cierre de sesión del ssg del [interval seconds] del [match-mac-address] arp del auto-cierre de sesión del ssg	de que no se considere ningún tráfico en la conexión SSG dentro del "intervalo."	usuario malintencionado configura estáticamente un DHCP Address del actual-límite en el plazo de 30 segundos porque el SSG ve el tráfico en el objeto de conexión, y el "auto-cierre de sesión del ssg" no invoca.
DHCP de la interceptación del ssg	Crea la conciencia SSG/DHCP que permite la cancelacíon del objeto del host SSG dentro de estos eventos: Un DHCPRELEASE se recibe para una dirección IP que haga juego un objeto del host activo. B El arriendo del DHCP expira para una dirección IP que haga juego un objeto del host activo.	Previene a los usuarios del DHCP de la reutilización de las sesiones SSG pero no previene a los usuarios estáticos de los DHCP Address del spoofing o de la reutilización de las sesiones SSG.
actualización arp de la PRUEBA del pool DHCP del IP	Se asegura de que el único subsistema IOS capaz de la adición o del retiro de las entradas ARP sea el subsistema del servidor DHCP.	Previene toda la reutilización de la sesión cuando está configurado con "el DHCP de la interceptación del ssg." Cuando está configurada sin "el DHCP de la interceptación del ssg," si el DHCP arrienda una dirección IP previamente usada, la reutilización de la sesión es todavía posible.
FastEthernet0/0 arp de la interfaz autorizado	Envía los pedidos ARP periódicos a todos los host de aseegurarse los son	Permite atar del DHCP y la cancelacíon de la entrada ARP cuando

	todavía activo. Apaga el aprendizaje dinámico ARP.	un usuario del DHCP realiza un logout NON-agraciado.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems