Отладка потоков вызовов интернет-шлюза SSG настроенного с DHCP Secure ARP, SSG Port-Bundle Host Key, SSG TCP Redirect, SESM и SSG/DHCP Awareness

Содержание

Введение

Фокусом этого документа является интернет-шлюз IOS, который выполняет SSG и DHCP с SESM для портала сервисов.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Технология и обзор характеристик

Шлюз выбора службы (SSG)

Шлюз выбора сервиса является коммутационным решением для поставщиков услуг, которые предлагают интранет, экстрасеть и Интернет-соединения абонентам с технологией широкополосного доступа, таким как цифровые абонентские линии (DSL), кабельные модемы или радио для разрешения синхронного доступа сетевым сервисам.

SSG работает в сочетании с Cisco Subscriber Edge Services Manager (SESM). Вместе с SESM, SSG предоставляет аутентификацию абонентов, сервисный выбор и возможности соединения услуг абонентам интернет-сервисов. Абоненты взаимодействуют с web - приложением SESM с помощью стандартного интернет-браузера.

SESM работает в двух режимах:

- Режим RADIUS — Этот режим получает абонента и служебную информацию от сервера RADIUS. SESM в режиме RADIUS подобен SSD.
- Режим LDAP — режим Протокола LDAP предоставляет доступ к совместимому LDAP каталогу для получения информации о профиле сервиса и абонента. Этот режим также имеет расширенную функциональность для web - приложений SESM и использует модель основанного на роли управления доступом (RBAC) для управления абонентским доступом.

Ключ хоста Бандла порта SSG

Функция Ключа хоста Бандла порта SSG улучшает связь и функциональность между SSG и SESM с механизмом, который использует IP - адрес источника хоста и исходный порт, чтобы определить и контролировать абонентов.

С функцией Ключа хоста Бандла порта SSG SSG выполняет преобразование адресов портов (PAT) и технологию NAT на трафике HTTP между абонентом и сервером SESM. Когда абонент передает пакет HTTP к серверу SESM, SSG создает схему порта, которая изменяет IP - адрес источника на настроенный IP - адрес источника SSG и изменяет исходный порт TCP на порт, выделенный SSG. SSG назначает связку (bundle) портов каждому абоненту, потому что у одного абонента может быть несколько одновременных сеансов TCP, когда он обращается к веб-странице. Назначенный ключ хоста или комбинация связки (bundle) порта и IP - адреса источника SSG, однозначно определяет каждого абонента. Ключ хоста несут в Пакетах RADIUS, передаваемых между сервером SESM и SSG в определяемом поставщиком атрибуте (VSA) IP Абонента. Когда сервер SESM передает ответ абоненту, SSG преобразовывает IP - адрес назначения и порт TCP - получателя в соответствии со схемой порта.

Перенаправление TCP SSG для не прошедших поверку подлинности пользователей

Если пользователь не авторизовал с поставщиком услуг, перенаправление для не прошедших поверку подлинности пользователей перенаправляет пакеты от пользователя. Когда неавторизованный абонент пытается соединиться с сервисом на порте TCP (например, к www. cisco . com), Перенаправление TCP SSG перенаправляет пакет к присоединенному порталу (SESM или группа устройств SESM). SESM выполняет

перенаправление к браузеру для отображения страницы регистрации. Абонент входит к SESM и аутентифицируется и авторизуется. SESM тогда предоставляет абоненту персонализированную домашнюю страницу, домашнюю страницу поставщика услуг или исходный URL.

DHCP защищенное присвоение IP-адреса

DHCP Безопасная функция Присвоения IP-адреса представляет возможность защитить записи таблицы ARP к арендным договорам Протокола DHCP (динамического конфигурирования узла) в базе данных DHCP. Эта функция защищает и синхронизирует MAC-адрес клиента к привязке DHCP, препятствованию неавторизованным клиентам или хакерам имитировать сервер DHCP и занять аренду DHCP уполномоченного клиента. Когда эта опция активирована, и сервер DHCP назначает IP-адрес на клиента DHCP, сервер DHCP добавляет безопасную Запись ARP к таблице ARP с назначенным IP - адресом и MAC-адресом клиента. Эта Запись ARP не может быть обновлена никакими другими динамическими пакетами ARP, и эта Запись ARP существует в таблице ARP в течение настроенного времени аренды или, пока арендный договор активен. Когда привязка DHCP истекает, защищенная Запись ARP может быть удалена только явным сообщением завершения от клиента DHCP или сервера DHCP. Эта функция может быть настроена для новой сети DHCP или использована для обновления безопасности текущей сети. Конфигурация этой функции не прерывает сервис и не видима клиенту DHCP.

Схема испытательного стенда

Отладка потока вызовов

Выполните следующие действия:

1. Когда iBook LEFT MAC сначала подключает Кабель Ethernet с этой сетью, это арендует IP-адрес 2.2.2.5/29 от Сервера DHCP IOS, который работает на “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. После того, как это успешно арендует IP-адрес 2.2.2.5, iBook LEFT MAC открывает web-браузер и указывает его к **http://3.3.3.200**, который используется для моделирования защищенных ресурсов, связанных к Сервису SSG “distlearn”. Сервис SSG “distlearn” локально определен в маршрутизаторе “F340.07.23-2800-8” SSG: **local-profile distlearn attribute 26 9 251 "R3.3.3.200;255.255.255.255"** В действительности, **http://3.3.3.200** маршрутизатор Cisco IOS, настроенный для “ip http

server", и слушает на TCP 80, таким образом, это - в основном Web-сервер.После того, как iBook LEFT MAC пытается перейти к **http://3.3.3.200**, так как это соединение является входом на интерфейсе, настроенном с "нисходящей линией ssg direction", первыми проверками маршрутизатора SSG для существования активного Объекта хоста SSG для IP - адреса источника запроса HTTP. Поскольку это первое, такой запрос от IP-адреса 2.2.2.5, Объект хоста SSG не существует, и перенаправление TCP к SESM, инстанцируют для хоста 2.2.2.5 через эту конфигурацию:

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
```

На этом этапе, когда **http://3.3.3.200** введен, браузер на iBook Left MAC похож на это:После TCP SSG IOS и перенаправлений HTTP SESM, экран похож на это:

3. После перенаправления TCP SSG к SESM и последующего перенаправления HTTP, передаваемого SESM назад к браузеру iBook Left MAC, iBook Left MAC вводит **user1** как имя пользователя и **Cisco** как пароль:
4. После того, как **кнопка OK** выдвинута, SESM передает маршрутизатору SSG эти учетные данные через составляющий собственность основанный на RADIUS протокол.

```
*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. В свою очередь маршрутизатор SSG создает Пакет запроса доступа RADIUS и передает его к RADIUS для аутентификации **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. RADIUS отвечает Access-Accept для **user1**, и Объект хоста SSG создан в "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. На этом этапе **user1** определен как Объект хоста SSG, но еще не имеет доступа ни к какой SSG Services. iBook Left MAC предоставляют Сервисный Экран выбора и нажимает **Distance Learning**:
8. После того, как **Дистанционное обучение** нажато, коробка SESM связывается с маршрутизатором SSG с управляющим канал:`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. Соединение SSG подключено, и поток вызовов завершен. iBook Left MAC может успешно перейти к **http://3.3.3.200:**

Пояснение конфигурации маршрутизатора SSG с документами функции

```
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.* DHCP Cisco IOS DHCP ! 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* SSG RADIUS 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

Безопасность и факторы повторного использования сеанса

При использовании SSG и DHCP вместе эти сценарии могут позволить злонамеренным пользователям снова использовать аутентифицируемый Объект хоста SSG, которые предоставляют не прошедший поверку подлинности доступ для обеспечения ресурсов:

- Если осведомленность SSG/DHCP не настроена с “ssg intercept dhcp”, новый пользователь DHCP может арендовать ранее арендованный IP-адрес, для которого все еще существует Объект хоста SSG. Так как первый запрос TCP от этого нового пользователя имеет соответствие, невзирая на то, что устаревший, Объект хоста SSG, который совпадает с IP - адресом источника, этому пользователю предоставляют не прошедшее поверку подлинности использование защищенных ресурсов. Это может быть предотвращено с “ssg intercept dhcp”, который приводит к удалению Объекта хоста SSG, когда любой происходит:DHCPRELEASE получен для IP-адреса, который совпадает с Объектом Активного узла.Аренда DHCP истекает для IP-адреса, который совпадает с Объектом Активного узла.
- Если пользователь DHCP социализирует арендованный IP-адрес злонамеренному пользователю перед непостепенным выходом из системы DHCP, который является выходом из системы DHCP, за которым не передается DHCPRELEASE, злонамеренный пользователь может статически настроить машину с этим IP-адресом и снова использовать Объект хоста SSG, настроен ли “ssg intercept dhcp”. Это может быть предотвращено с комбинацией “ssg intercept dhcp” и “update arp”, настроенного под ПУЛОМ DHCP IOS. “update arp” гарантирует, что единственная подсистема IOS, которая в состоянии добавить или удалить Записи ARP, является подсистемой сервера DHCP. С “update arp” DHCP IP К MAC, связывающий всегда, совпадает с привязкой IP К MAC в таблице ARP. Даже при том, что злонамеренный пользователь имеет статически настроенный IP - адрес, который совпадает с Объектом хоста SSG, трафику не позволяют ввести маршрутизатор SSG. Поскольку MAC-адрес не совпадает с MAC-адресом текущей привязки DHCP, сервер DHCP IOS предотвращает создание Записи ARP.

- Когда SSG и DHCP настроены вместе, “ssg intercept dhcp” и “update arp” предотвращают повторное использование сеанса. Когда Хост DHCP выполняет непостепенный выход из системы, связанный вызов заключительной небезопасности состоит в том, чтобы освободить Аренду DHCP и Запись ARP. Конфигурация “санкционированного arp” на “ssg direction передает в нисходящем направлении” интерфейсные результаты в периодических запросах ARP, передаваемых всем хостам, чтобы удостовериться, что они все еще активны. Если никакой ответ не получен от этих периодических сообщений ARP, привязка DHCP освобождена, и подсистема DHCP IOS удаляет Запись ARP.
```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
arp authorized
arp probe interval 5 count 15
```
В данном примере запрос ARP передается периодически для обновления всех известных Записей ARP на Fa0/0 каждые 5 с. После 15 сбоев освобождена привязка DHCP, и подсистема DHCP IOS удаляет Запись ARP.В контексте SSG без “санкционированного arp”, если хост DHCP выполняет непостепенный выход из системы, Аренда DHCP и ее связанный Объект хоста SSG остаются активными, пока арендный договор для этого адреса DHCP не истекает, но никакое повторное использование сеанса не происходит, пока “ssg intercept dhcp” настроен глобально.

“Санкционированный arp” выключает динамический ARP, учащийся на интерфейсе, на котором это настроено. Единственные Записи ARP на рассматриваемом интерфейсе - добавленные сервером DHCP IOS после того, как будет запущен арендный договор. Эти Записи ARP тогда очищены Сервером DHCP IOS, как только арендный договор завершился, или из-за получения ВЫПУСКА DHCP, истечения арендного договора, или из-за сбоя Зонда ARP из-за непостепенного выхода из системы DHCP.

Примечания реализации:

- “ssg auto-logoff arp” и “ssg auto-logoff icmp” являются нежелательными методами для предотвращения повторного использования сеанса или результирующих проблем безопасности. Варианты “arp” и “icmp” “ssg автовыход из системы” только передают ARP или PING IMCP, когда трафик не замечен на соединении SSG в настроенном “интервале”, самым низким из которых составляют 30 секунд. Если аренда DHCP, ранее используемый IP-адрес в течение 30 секунд или злонамеренный пользователь статически настраивает в настоящее время ограниченный адрес DHCP в течение 30 секунд, сеанс, снова использована, потому что SSG видит, что трафик на объекте подключения, и “ssg автовыход из системы” не вызывает.
- Если злонамеренный хост выполняет спуфинг MAC-адреса, во всех вариантах использования не предотвращено повторное использование сеанса.

Таблица 1 – открывает сеанс повторное использование и учитываемые факторы безопасности в развертываниях SSG/DHCP

Команда	Функция	Последствия для системы безопасности
ssg auto-logoff arp [mac-address соответствия]	Удаляет Объект хоста SSG после сбоя ARP или ФУНКЦИИ ПРОВЕРКИ СВЯЗНОСТИ	Повторные использования открывают сеанс, если аренда DHCP, ранее используемый IP-адрес в течение 30

[*секунды* интервала] ssg auto-logoff icmp [миллисекунды таймаута] [пакетный номер] [*секунды* интервала]	ICMP PING, которые только передаются после того, как "no traffic" (нет трафика) замечен на соединении SSG в “интервале”.	секунд или злонамеренный пользователь статически настраивает в настоящее время ограниченный адрес DHCP в течение 30 секунд, потому что SSG видит трафик на объекте подключения, и “ssg автовыход из системы”, не вызывает.
ssg intercept dhcp	Создает Осведомленность SSG/DHCP, которая позволяет удаление Объекта хоста SSG в этих событиях: DHCPRELEASE получен для IP-адреса, который совпадает с Объектом Активного узла. B. Аренда DHCP истекает для IP-адреса, который совпадает с Объектом Активного узла.	Предотвращает пользователей DHCP от повторного использования сеансов SSG, но не препятствует тому, чтобы статические пользователи имитировали адреса DHCP или повторное использование сеансов SSG.
ТЕСТОВЫЙ update arp ip dhcp pool	Гарантирует, что единственная подсистема IOS, способная к добавлению или удалению Записей ARP, является подсистемой Сервера DHCP.	Предотвращает все повторное использование сеанса, когда настроено с “ssg intercept dhcp”. Когда настроено без “ssg intercept dhcp”, если аренда DHCP ранее используемый IP-адрес, повторное использование сеанса все еще возможно.
arp authorized interface FastEthernet0/0	Передает периодические запросы ARP ко всем хостам, чтобы удостовериться,	Когда пользователь DHCP выполняет непостепенный выход из системы, позволяет удаление привязки и Записи ARP DHCP.

	что они все еще активны. Выключает динамическое обучение ARP.	

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация