配置在Cisco网络中访客流量的URL记录和报告集成

目录

简介

本文描述如何集成一个美洲台访客服务器(NGS)用无线局域网控制器(WLCs)和可适应安全工具(ASA)提供记录和报告访客流量的URL。许多公司有一个需求监控访客流量和关于如何的本文提供信息配置思科组件符合该要求。

注意有配置多的Cisco解决方案在Cisco网络的访客访问。此条款着重使用WLC作为启用的技术的方法。WLC有独特的能力对从网络边缘的隧道流量到有EoIP的互联网。此功能排除需要部署VPN或ACL在网络基础设施内限制访客流量从漏到公司的内部网络。

大多数此条款包括“集成记录和报告”在“无线访客”网络的URL，但是此功能在“有线的访客”网络可以配置。附录A为“有线的访客”网络提供细节。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 运行版本8.0.4.24或以上的ASA
- 两个WLC-4400系列控制器运行4.2.130或以上
- NAC运行版本2.0或以上的访客服务器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA运行8.0.4.26
- 运行4.2.130代码的两个WLC-44xx控制器
- 美洲台运行2.0.0代码的访客服务器
- Catalyst 6500

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

无线对客户的访客访问提供重大的商业效益。这些好处包括减少的运作成本、改善的生产率和访客访问简化的管理和供应。另外，美洲台访客服务器使客户显示他们的合格用者政策和在授权对互联网的访问之前要求此策略接受。现在，增加报告集成的URL记录和，客户能记录访客使用情况和跟踪标准他们的合格用者政策。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

无线访客实验室拓扑结构

Catalyst 6500用于模拟企业网络。访客SSID，显示为红色，对本地VLAN的地图在ASA，也显示为红色。从PC的访客通信流到接入点里，通过LWAPP通道对WLC外国控制器，然后通过EoIP通道对WLC锚点控制器。锚点控制器为访客网络提供DHCP和验证服务。DHCP服务提供访客IP地址、默认网关和DNS服务器。默认网关是ASA，并且DNS服务器是在互联网查找的公共服务器。在锚点控制器的验证服务通信与NGS通过RADIUS利用在NGS的来宾用户数据库验证用户。访客登录启动，当访客打开Web浏览器时，并且锚点控制器重定向流量对验证页。进出访客子网的所有流量过滤

策略控制和审计的ASA。

记录从ASA的集成URL到NGS

当您启用这些时，集成URL记录激活：

- 认为从WLC锚点控制器的RADIUS到NGS
- HTTP GET请求记录日志在ASA的
- 发送从ASA的系统消息到NGS

RADIUS认为提供NGS访客IP地址和访客用户ID之间的一映射特定的时间。HTTP GET记录日志请求提供与什么URL日志的NGS什么时候由访客IP地址访问。NGS能然后关联此信息提供显示一特定的访客访问的URL一个特定的时间的报道。

注意准确的时间要求此相关性的能适当地工作。为此， NTP服务器的配置是高度推荐的在ASA、WLC和NGS。

配置

本文档使用以下配置：

- ASA 配置
- WLC 配置
- NGS配置

ASA 配置

在ASA的关键配置任务包括这些：

- NTP
- HTTP检查
- Syslog

NTP由NGS要求确保消息的适当的相关性。HTTP检查enable (event) URL记录。Syslog是使用的方法发送URL日志到NGS。

在本例中，此命令用于启用在ASA的NTP ：

```
ntp server 192.168.215.62
```

HTTP检查使ASA记录URL。特别地， **Inspect http**命令启用或禁用GET请求的记录日志与系统消息304001的。

Inspect http命令被放置在策略映射内的类映射下。当启用用**service-policy命令**， http检查记录簿与系统消息304001的获得请求。作为URL一部分， ASA代码8.0.4.24或以后为系统消息304001要求显示主机名。

在本例中，这些是相关命令：

```
policy-map global_policy
 class inspection_default
  inspect http
!
service-policy global_policy global
```

Syslog是使用的方法传达记录对NGS的URL。在此配置中，仅系统消息304001传送对与此配置的NGS ：

```
logging enable
logging timestamp
logging list WebLogging message 304001
logging trap WebLogging
logging facility 21
logging host inside 192.168.215.16
```

WLC 配置

无线局域网控制器的关键配置步骤包括这些：

- 基本访客访问
- NTP
- RADIUS 记帐

基本访客访问配置介入WLC外国控制器和WLC锚点控制器的配置，以便访客流量通过对互联网DMZ的企业网络被以隧道传输。基本访客访问的配置在分开的文档报道。显示设置的配置的图示在附录报道。

NTP服务器被添加在Controller/NTP屏幕。

在WLC的NTP配置

RADIUS记帐服务器要求，以便NGS服务器能映射在ASA系统消息接收的源IP地址对使用该地址在该特定时间的访客。

这两个屏幕显示认为在WLC锚点控制器的RADIUS验证和RADIUS的配置。RADIUS配置在外国控制器没有要求。

RADIUS 身份验证 RADIUS 记帐

NGS配置

- NTP
- RADIUS客户端
- Syslog

NGS服务器从https://(ip_address)/admin网页配置。默认用户名/密码是admin/admin。

NTP服务器在服务器/DATE时间设置屏幕被添加。推荐系统时区设置为服务器物理的查找的时区。当NTP同步时，您在说的底部的此屏幕看到消息，“状态：活动NTP服务器”与显示“当前时间来源的IP地址一起”。

NGS NTP配置

NGS服务器需要配置用锚点控制器的IP地址作为RADIUS客户端。此屏幕查找在Devices/RADIUS客户端页。确保共享机密是相同的象在锚点控制器被输入了。在您做变动重新启动在NGS服务器后的RADIUS服务请点击**Restart按钮**。

RADIUS客户端

默认情况下，NGS服务器接受从所有IP地址的系统消息。结果，没有要求的额外步骤收到从ASA的系统消息。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

遵从这些步骤验证适当地记录工作的URL。

1. 从客户端PC，请连接对无线访客网络。PC接收一个IP地址、默认网关和DNS服务器从DHCP服务器在锚点控制器。
2. 打开 Web 浏览器。您重定向到登录画面。输入访客用户名和密码。在成功认证，您重定向对在互联网的一个默认页面。
3. 浏览对在互联网的多种网页。
4. 连接管理PC对NGS在https://(ip_address)并且登陆作为赞助商。
5. 点击**帐户管理**。您看到访客帐户列表。(如果您的访客帐户没出现，点击**高级搜索**按钮并且清除指定的过滤器此赞助商能只看到该的帐户他们创建。)
6. 查找从列表的来宾用户用户帐号。请移动在右边，直到您看到Details图标。点击**Details图标**。
7. 点击**活动Log选项**。您看到访客访问URL的列表。**记录用户的URL报告**

报告显示来宾用户访问了在April 1的http://www.cisco.com， 2009年在下午2:51。192.168.59.49设备地址是传送包含URL日志的系统消息ASA的IP地址。来宾用户的源IP地址是192.168.0.10。目的地址是http://www.cisco.com的192.168.219.25。

附录

附录A –有线的访客选项

至此点，此条款包括“记录和报告访客流量的集成的URL”用于“无线访客”网络。此部分提供细节配置“有线的访客”。有线的访客和无线访客在同一个WLC外国控制器可以启用。

这是有线的访客网络实验室的网络图。

有线的访客实验室拓扑结构

有线的访客实验室拓扑结构类似于无线访客实验室拓扑结构，显示前，除了有线的访客VLAN的新增内容。有线的访客VLAN，显示为红色，是在有线的访客PC和WLC外国控制器之间的一第2层连接。从有线的访客的流量由WLC外国控制器接收并且由EoIP发送到WLC锚点控制器。WLC锚点控制器提供DHCP和验证服务有线的访客用户的它为无线访客用户相似地提供了这些服务。默认网关是ASA，并且DNS服务器是在互联网的一个公共服务器。逻辑上，进出子网的所有流量由ASA保护。

因为这能使流量的跳离点能漏在有线的访客VLAN外面到公司网络，推荐不配置在有线的访客VLAN的一个第3层接口。

附录B – WLCs的详细配置

WLC锚点控制器

锚点控制器接口

接口的配置在锚点控制器的显示：

ap-manager和管理接口在本地VLAN WLC的物理端口1。Port1连接到Catalyst交换机并且收到从客户网络的流量。访客流量通过从外国控制器的EoIP通道接收并且通过此端口终止。

访客接口在端口2本地VLAN，并且有线的接口在端口2.端口2 VLAN9连接对ASA和使用传送流量到互联网。

锚点控制器移动组

对于此示例，一移动组为外国控制器(有线)和锚点控制器的(锚点)一分开的移动组配置。在锚点控制器的配置显示。

锚点控制器WLAN
锚点控制器-设置访客WLAN的锚点

为了配置或WLAN的show mobility anchor，移动您的鼠标向下拉箭头在权利，并且选择**移动性锚点**，如显示。

锚点控制器-设置锚点对本身 锚点控制器-无线访客用户的WLAN 锚点控制器-有线的访客用户的WLAN (可选) 锚点控制器- DHCP范围 锚点控制器-无线访客的DHCP范围： 锚点控制器-有线的访客的DHCP (可选) ：

WLC外国控制器

接口

接口的配置在外国控制器的显示。

ap-manager和管理接口在本地VLAN WLC的物理端口1。

如果要提供有线的访客访问，有线的接口 *可选*和只要求。有线的接口在VLAN8物理端口1。此接口收到从Catalyst交换机的访客VLAN的流量并且通过本地VLAN传送它EoIP通道，到锚点控制器。

外国控制器-移动组

在外国控制器的配置显示。

外国控制器- WLAN
为了配置或WLAN的show mobility anchor，移动您的在下拉箭头的鼠标在权利并且选择**移动性锚点**，如显示。

设置的移动性锚点停住控制器 外国控制器-无线访客用户的访客WLAN
s

外国控制器-有线的访客用户的WLAN (可选) –继续

附录C – ASA配置

```
ASA-5520# show run
:
ASA Version 8.0(4)26
!
hostname ASA-5520
```

```
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.59.49 255.255.255.240
!
interface GigabitEthernet0/2
   <- Guest traffic enters this interface
 nameif wireless_guest
 security-level 50
 ip address 192.168.0.254 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.99.1 255.255.255.0
 management-only
!
boot system disk0:/asa804-26-k8.bin
clock timezone CST -6
clock summer-time CDT recurring
logging enable
logging timestamp
   <- provide a timestamp in each syslog message
logging list WebLogging message 304001
   <- list includes URL Log message (304001)
logging console errors
logging buffered notifications
logging trap WebLogging
   <- Send this list of Log messages to syslog servers
logging asdm informational
logging facility 21
logging host inside 192.168.215.16
   <- NGS is the syslog server
asdm image disk0:/asdm-61551.bin
route inside 10.10.10.0 255.255.255.0 192.168.59.62 1
route inside 192.168.215.0 255.255.255.0 192.168.59.62 1
route inside 198.168.1.15 255.255.255.255 192.168.59.62 1
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.99.0 255.255.255.0 management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 198.168.1.15 <- Configure ntp server
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect http
   <- Enable http inspection on the global policy
!
service-policy global_policy global
   <- Apply the policy
prompt hostname context
Cryptochecksum:b43ff809eacf50f0c9ef0ae2a9abbc1d
: end
```

相关信息

- 远程用户拨入认证系统(RADIUS)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems