ISR IP接纳和LDAP Web重定向的对ScanSafe/Cloud Web安全配置示例

目录

简介

本文描述如何配置Cisco G2系列集成服务路由器(ISR)。当Ip admission和轻量级目录访问协议(LDAP)配置可以使用在ISR时的认证代理，与思科Cloud Web安全(CWS)重定向功能一道典型地使用。同样地，本文打算是参考为了补充CWS重定向配置和故障排除文档在ISR。

先决条件

要求

思科建议您的系统满足这些需求，在您尝试在本文描述的配置前：

- ISR必须运行代码版本15.2(1)T1或以上。
- 您的系统必须有是可用的在Cisco IOS与安全功能设置的(SEC)许可证的镜像(通用)。
- 激活目录(AD)域的客户端工作站必须有功能通过Web浏览器执行活动验证。
- 您必须有CWS订阅。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Internet Explorer，谷歌镀铬物， Mozilla Firefox (要求透明NT LAN Manager (NTLM)验证的更多的配置)
- Cisco G2 800， 1900， 2900和3900系列ISR。
- Microsoft Windows AD域控制器(ADDC)

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。

> **注意**：不支持Cisco G1 1800， 2800和3800系列路由器。

背景信息

安装Cisco G2系列ISR没有Cisco可适应安全工具的许多管理员(ASA)在他们的网络选择使用ISR CWS (以前ScanSafe)重定向功能为了利用Web过滤的CWS解决方案。作为该解决方案一部分，多数管理员在CWS门户也要使用当前AD基础设施为了发送用户身份信息到CWS塔为Web过滤策略的用户或基于组的策略执行的目的。

整体概念类似于在ASA和上下文目录代理(CDA)之间的集成，与一些差异。最值得注意的差异是ISR实际上不维护被动用户对IP映射数据库，因此用户必须穿过某种验证为了传输ISR和发送用户或组信息到CWS门户。

> **提示**：参考本文的**认证方法**部分关于是可用的多种认证方法之间的差异的更多信息。

当在本文时描述配置的CWS重定向部分是相对直接的，一些管理员也许遇到与尝试的困难配置验证部分。此部分与**ip admission**命令一起使用参考必须也配置的LDAP服务器和验证、授权和统计(AAA)认证语句。本文目的将提供网络操作员全面的参考源为了配置或排除故障IP接纳和此配置的LDAP部分在Cisco G2系列ISR的。

配置

请使用在此部分描述为了配置Cisco ISR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

配置LDAP

完成这些步骤为了配置AAA服务器的LDAP属性：

1. 配置LDAP属性地图为了强制由用户输入匹配在AD的**sAMAccountName**属性的用户名：
   ```
   C-881(config)#ldap attribute-map ldap-username-map map type sAMAccountName
    username
   C-881(config-attr-map)#map type sAMAccountName username
   ```
   注意：此配置要求，因为**sAMAccountName**属性是在AD的一一个唯一值，不同于共同名称(CN)属性，默认情况下否则用于为了配比。 例如，可以有*John Smith*多个实例在AD的，但是可以只有有*jsmith* **sAMAccountName的**一个用户，也是用户帐户登录。其他*John Smith*帐户有**sAMAccountNames**例如*jsmith1*或*jsmith2*。
   show ldap属性命令可能也用于为了查看LDAP属性和相关的AAA属性的列表。

2. 配置LDAP服务器组：
   ```
   C-881(config)#aaa group server ldap LDAP_GROUP
   C-881(config-ldap-sg)#server DC01
   ```
3. 配置LDAP服务器：
   ```
   C-881(config)#ldap server DC01
   C-881(config-ldap-server)# ipv4 10.10.10.150
   ```

```
C-881(config-ldap-server)#attribute map ldap-username-map
C-881(config-ldap-server)# bind authenticate root-dn CN=Csco_Service,CN=Users,
DC=lab,DC=cisco,DC=com password Cisco12345!

C-881(config-ldap-server)#base-dn DC=lab,DC=cisco,DC=com
C-881(config-ldap-server)#search-filter user-object-type top
C-881(config-ldap-server)#authentication bind-first
```

除非有需要实现一个自定义搜索过滤器，此配置通常不要求修改。是精通的在LDAP并且会适当地输入此信息只有的管理员应该使用自定义搜索过滤器。如果是不定的关于应该使用的搜索过滤器，请使用描述的过滤器;它找出正常AD环境的用户。

也要求仔细的注意选派lDAP配置的另一个部分是在BIND验证根**DN**和BASE **DN**命令要求的辨别名称(Dns)。必须正确地输入这些，当他们在LDAP服务器出现，或者LDAP查询发生故障。另外，BASE **DN**命令必须是LDAP树的低部，所有用户验证驻留。

考虑BASE **DN** in命令先前配置被修改例如此的方案：

```
base-dn OU=TestCompany,DC=lab,DC=cisco,DC=com
```

在这种情况下，在**Cn=users**包括的用户的查询， **DC=lab， Dc=cisco， Dc=com不**返回结果，因为LDAP服务器只搜索TestCompany组织单位(OU)和儿童对象在它里面。结果，验证为那些用户总是失效，直到他们搬入TestCompany OU或其子树，或者，如果BASE **DN**命令在查询被修改为了包括它。

> **提示**：关于如何确定基础的适当的Dns和根源命令的详情，参考**确定在AD的DN对象- ADSI编辑**本文的部分。

配置AAA

即然LDAP服务器配置，您必须参考他们由Ip admission进程使用的对应的AAA语句：

```
C-881(config)#aaa authentication login SCANSAFE_AUTH group LDAP_GROUP
C-881(config)#aaa authorization network SCANSAFE_AUTH group LDAP_GROUP
```

> **注意**：如果这些命令不是可用的，则**aaa new-model命令**威力需要被输入为了启用此AAA功能默认情况下，因为没有启用。

配置Ip admission

在配置里定义的Ip admission部分触发提示验证的用户的进程(或执行透明验证)然后执行根据用户凭证的LDAP查询和AAA服务器。如果用户顺利地验证，用户身份信息由内容扫描进程然后拉并且被派出对CWS塔，与重定向的流一起。Ip admission进程没有被启动，直到***name命令的***Ip admission在路由器的入口接口被输入。所以，配置的此部分可以实现，不用任何流量影响。

```
C-881(config)#ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm
C-881(config)#ip admission name SCANSAFE_ADMISSION method-list authentication
 SCANSAFE_AUTH authorization SCANSAFE_AUTH
```

Enable (event) Ip admission

这是使用为了启用Ip admission的配置：

注意：这迫使用户验证，导致通信流中断，如果验证发生故障。

```
C-881(config)#int vlan301 (internal LAN-facing interface)
C-881(config-if)#ip admission SCANSAFE_ADMISSION
```

从验证的豁免内部主机

一些管理员也许希望由于多种原因豁免从认证过程的一些内部主机。例如，它也许是不理想的为不IP接纳进程的或基本认证上将影响的有能力在NTLM的内部服务器或设备。在这些实例，访问控制表(ACL)可以应用到Ip admission配置为了防止特定主机IP或子网触发Ip admission。

在本例中，而验证为其他主机，仍然要求内部主机10.10.10.150从验证的需求是豁免：

```
C-881(config)#ip access-list extended NO_ADMISSION
C-881(config-ext-nacl)#deny ip host 10.10.10.150 any
C-881(config-ext-nacl)#permit ip any any
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm list NO_ADMISSION
```

启用在ISR的HTTP服务器

要求您使HTTP服务器为了拦截HTTP会话和开始认证过程：

```
Ip http server
Ip http secure-server
```

注意：如果对HTTPS的重定向验证的要求， **IP HTTP安全服务器**只是需要的。

配置CWS重定向

这是CWS重定向的一基本概略的配置：

```
Ip http server
Ip http secure-server
```

完整配置示例

此部分为前面部分提供完整配置示例。

LDAP

```
Ip http server
Ip http secure-server
```

AAA

```
Ip http server
Ip http secure-server
```

Ip admission

```
Ip http server
Ip http secure-server
```

HTTP 服务器

```
Ip http server
Ip http secure-server
```

内容扫描和CWS

```
Ip http server
Ip http secure-server
```

确定在AD的DN对象- ADSI编辑

若需要，浏览AD结构为了查寻Dns为了用在用户或组搜索库上是可能的。 管理员能使用呼叫被构件到AD域控制器的*ADSI的*工具*编辑*。为了打开ADSI请编辑，选择在AD域控制器的**Start > Run**并且输入**adsiedit.msc**。

一旦ADSI Edit是开放的，请用鼠标右键单击所有对象，例如OU，组或者用户，并且选择**属性**为了查看该对象DN。DN字符串可能容易地然后复制和插入到路由器配置为了避免所有印刷错误。此镜像说明进程：

认证方法

有使用Ip admission的四不同种类的认证方法联机，并且他们经常被误会，透明和被动NTLM之间的特别是差异。以下部分描述验证之间的这些类型的差异。

活动NTLM

验证的激活NTLM认证方法提示用户，当透明NTLM验证发生故障。这通常归结于事实客户端浏览器不支持集成Microsoft Windows验证或，因为用户登录有本地(非域)凭证的工作站。活动NTLM验证执行LDAP查询到域控制器为了保证提供的凭证正确。

> **注意**：使用NTLM验证的所有类型，凭证没有通过明文通过。然而， NTLM版本1 (NTLMv1)有有大量文件证明的漏洞。ISR是NTLMv2-capable，虽然默认情况下， Microsoft Windows更旧的版本也许通过NTLMv1协商。此行为取决于AD验证策略。

透明NTLM

透明NTLM验证出现，当用户登录有域凭证的时工作站，并且那些凭证由对IOS路由器的浏览器通过透明地。IOS路由器然后执行一LDAP查询为了验证用户凭证。这通常是此功能的最希望的认证形式。

基本认证(通过在明文的HTTP)

当NTLM验证发生故障或为客户端不是可能的例如麦金塔、基于linux的设备或者移动设备时，此认证形式典型地使用作为回退机制。使用此方法，如果HTTP安全服务器没有启用，然后这些凭证通过在明文的HTTP通过(非常不安全)。

被动NTLM

从用户的被动NTLM认证请求凭证，但是不利用域控制器实际上验证用户。当这能避免查询失效域控制器的LDAP相关问题时，也显示环境的用户在安全风险。 如果透明验证发生故障或不是可能的，则提示用户输入凭证。然而，用户能输入他们选择，通过对CWS塔的所有凭证。结果，策略也许不应用适当地。

默认情况下例如，用户A能使用(不允许透明NTLM没有更多的配置)的Firefox和用所有密码输入用户B用户名，并且用户的B策略应用给用户A。风险风险可以被减轻，如果用户全部被迫使使用支持透明NTLM验证的浏览器，但是，使用被动验证没有推荐在大多数情况下。

活动NTLM验证的消息序列

这是活动NTLM认证方法的全部的消息顺序：

```
Browser -->  ISR : GET / google.com
Browser <--  ISR : 302 Page moved http://1.1.1.1/login.html
Browser -->  ISR : GET /login.html 1.1.1.1
Browser <--  ISR : 401 Unauthorized..Authenticate using NTLM
Browser -->  ISR : GET /login.html + NTLM Type-1 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-1 msg
```

ISR复制从HTTP的类型1消息到LDAP，逐字节，不用任何数据变更。

```
ISR     <--  AD  : LDAP Bind Response + NTLM Type-2 msg
Browser <--  ISR : 401 Unauthorized + NTLM Type-2 msg
```

类型2消息从LDAP也复制逐字节到HTTP。因此，在PCAP，看起来起源于1.1.1.1，但是实际内容是从AD。

```
Browser -->  ISR : GET /login.html + NTLM Type-3 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-3 msg
ISR     <--  AD  : LDAP Bind response - Success
Browser <--  ISR : 200OK + redirect to google.com
```

当活动NTLM配置时，在NTLM交换期间， ISR不干涉。然而，如果被动NTLM配置，然后ISR生成其自己的类型2消息。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

显示命令

> **注意**：命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

您能使用这些**显示**命令为了排除故障您的配置：

- **显示ip admission缓存**
- **显示ip admission状态**
- **显示ip admission统计信息**
- **show ldap server全部**

debug 命令

> **注意**：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

这是您能使用为了排除故障您的配置的一些有用的调试指令：

- **全调试的ldap**此命令可以用于为了发现原因验证发生故障。
- **debug ip接纳详细信息**-此命令非常冗长和CPU密集型。思科建议您以触发Ip admission的单个测试客户端仅使用它。
- **debug ip接纳ntlm** -此命令可以用于为了发现原因Ip admission进程被触发。
- **debug ip接纳httpd**
- **debug ip http transaction**
- **debug aaa authentication debug aaa authorization**

常见问题

此部分描述遇到与在本文描述的配置的一些常见问题。

Ip admission不拦截HTTP请求

当您查看**显示ip admission statistics命令**输出时，此问题变得明显。输出不显示任何HTTP请求的拦截：

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

可能的解决方案

有两个可能的解决方案对此问题。第一是验证**ip http server**启用。

如果ISR的HTTP服务器没有启用，则Ip admission触发，但是从未实际上拦截HTTP会话。所以，它提示输入验证。在这种情况下，没有**cache命令显示的ip admission的**输出，但是这些线路许多循环在**detail命令debug ip的接纳的**输出中被看到：

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

对此问题的第二解决方案将验证用户IP地址从ACL不是豁免在Ip admission配置里。

用户收到*404 Not Found*错误

此问题被观察，当用户为验证时重定向，并且**404 Not Found**错误在浏览器出现。

可能的解决方案

保证在**ip admission虚拟IP 1.1.1.1虚拟主机ISR_PROXY的**名称能用客户端域名系统(DNS)服务器成功地解决。在这种情况下，客户端执行**ISR_PROXY.lab.cisco.com的**一DNS查询，因为**lab.cisco.com**是工作站加入域的完全合格的域名(FQDN)。如果DNS查询发生故障，客户端发送链路本地组播名字解析(LLMNR)查询，跟随由广播对本地子网的NETBIOS查询。

如果所有这些解决方法尝试发生故障，则**404 Not Found**或**Internet Explorer**在浏览器不**能显示网页**错误显示。

用户认证发生故障，当提示

这可以由多种原因造成，但是与在ISR的ISR和LDAP服务器之间的IDAP配置或者通信通常涉及。在ISR，症状通常被观察，当用户在**初始状态时**被滞留Ip admission一次被触发：

```
C-881(config)#do show ip admi cac
Authentication Proxy Cache
Client Name N/A, Client IP 10.10.10.152, Port 56674, timeout 60,
 Time Remaining 2, state INIT
```

常见原因

这些是此问题的常见原因：

- 一个无效用户名和密码由活动验证的用户输入。
- 一个无效BASE **DN**用于IDAP配置，导致搜索不返回结果。
- 一个无效捆绑验证根**DN**为用户名或密码配置，造成LDAP捆绑发生故障。

- ISR和LDAP服务器之间的通信发生故障。验证LDAP服务器在LDAP通信的指定的TCP端口侦听，并且在两个之间的所有防火墙允许流量。

- 一个无效搜索过滤器不导致LDAP搜索的结果。

排除故障LDAP

确定原因的最佳方法验证发生故障是使用LDAP调试on命令ISR。记住调试在ISR可以是昂贵和危险运行，如果有过量输出，并且他们能造成路由器暂停和要求一硬重新通电。这是准确无误的对低端的平台。

为了排除故障，思科建议您应用ACL对Ip admission规则为了对验证服从网络的仅单个测验工作站。这样，调试可以启用与负面影响最小风险对于路由器的能力通过流量。

> **提示**：参考**从**本文的**Authentication部分的豁免内部主机**关于ACL的应用程序的更多信息对IP接纳配置。

当您排除故障LDAP相关问题时，了解LDAP处理从ISR的请求的步骤是有用的。

LDAP认证的高层次步骤

这是LDAP认证的高层次步骤：

1. 打开对LDAP服务器的连接在指定的端口。默认端口是**TCP 389**。

2. 对LDAP服务器的捆绑有捆绑的验证根**DN**用户和密码。

3. 执行LDAP搜索，与在IDAP配置里定义的使用BASE **DN**和搜索过滤器，该的用户的尝试验证。

4. 请从LDAP服务器得到LDAP结果并且创建用户的Ip admission凭证的缓存条目，如果验证是成功的，在认证失败情形下，或者reprompt。

LDAP Debug输出分析

这些进程在**all命令调试的ldap的**输出中可以查看。此部分为验证提供发生故障由于一个无效BASE **DN** LDAP debug输出的示例。 查看debug输出和相关的注释，描述输出的部分显示上述步骤也许遇到失败的地方。

```
*Jan 30 20:51:50.818: LDAP: LDAP: Queuing AAA request 23 for processing
*Jan 30 20:51:50.818: LDAP: Received queue event, new AAA request
*Jan 30 20:51:50.818: LDAP: LDAP authentication request
*Jan 30 20:51:50.818: LDAP: Username sanity check failed
*Jan 30 20:51:50.818: LDAP: Invalid hash index 512, nothing to remove
*Jan 30 20:51:50.818: LDAP: New LDAP request
*Jan 30 20:51:50.818: LDAP: Attempting first next available LDAP server
*Jan 30 20:51:50.818: LDAP: Got next LDAP server :DC01
*Jan 30 20:51:50.818: LDAP: Free connection not available. Open a new one.
*Jan 30 20:51:50.818: LDAP: Opening ldap connection
( 10.10.10.150, 389 )ldap_open
```

在粗体显示的输出的部分表明这不是网络层问题，因为成功打开连接。

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

捆绑验证DN是正确在此输出中。如果配置为此是不正确，则捆绑失败看到。

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

在粗体显示的输出的部分表明所有捆绑操作是成功的，并且继续搜索实际用户。

```
*Jan 30 20:51:51.854: LDAP: SASL NTLM authentication done..Execute search
*Jan 30 20:51:51.854: LDAP: Next Task: Send search req
*Jan 30 20:51:51.854: LDAP: Transaction context removed from list[ldap reqid=15]
*Jan 30 20:51:51.854: LDAP: Dynamic map configured
*Jan 30 20:51:51.854: LDAP: Dynamic map found for aaa type=username
*Jan 30 20:51:51.854: LDAP: Ldap Search Req sent
ld 2293572544
base dn     dc=lab1,dc=cisco,dc=comscope       2
filter (&(objectclass=top)(sAMAccountName=testuser5))
ldap_req_encode
put_filter "(&(objectclass=top)(sAMAccountName=testuser5))"
put_filter: AND
put_filter_list "(objectclass=top)(sAMAccountName=testuser5)"
put_filter "(objectclass=top)"
put_filter: simple
put_filter "(sAMAccountName=testuser5)"
put_filter: simple
Doing socket write
*Jan 30 20:51:51.854: LDAP: lctx conn index = 2
```

第一行(显示在粗体)表明LDAP搜索debug输出开始。并且，请注意应该为**实验室**配置BASE **DN**域控制器，不是**lab1**。

```
*Jan 30 20:51:52.374: LDAP: LDAP Messages to be processed: 1
*Jan 30 20:51:52.374: LDAP: LDAP Message type: 101
*Jan 30 20:51:52.374: LDAP: Got ldap transaction context from reqid
16ldap_parse_result
*Jan 30 20:51:52.374: LDAP: resultCode: 10 (Referral)
*Jan 30 20:51:52.374: LDAP: Received Search Response resultldap_parse_result
ldap_err2string
*Jan 30 20:51:52.374: LDAP: Ldap Result Msg: FAILED:Referral, Result code =10
*Jan 30 20:51:52.374: LDAP: LDAP Search operation result : failedldap_msgfree
*Jan 30 20:51:52.374: LDAP: Closing transaction and reporting error to AAA
*Jan 30 20:51:52.374: LDAP: Transaction context removed from list
[ldap reqid=16]
*Jan 30 20:51:52.374: LDAP: Notifying AAA: REQUEST FAILED
```

在粗体显示的输出的部分表明搜索没有返回结果，在这种情况下归结于一个无效BASE **DN**。

RFC 4511

RFC 4511 (**轻量级目录访问协议(LDAP) ：协议**)为LDAP提供关于结果代码消息的信息和其他LDAP协议相关的信息，可以被参考列在IETF网站。