改进在CSS 11000和CSS11500上的安全

目录

简介

本文提供关于能改进在Cisco内容服务交换机的Cisco配置设置的信息(CSS) 11000或CSS11500的安全。本文描述是几乎普遍可适用的在IP网络的基本配置设置并且包括您一定知道的一些个意外的项目。

本文不提交这些项目详尽列表，亦不在本文可能信息用知识被替代在网络管理员部分。本文担当有时被忘记项目的提醒。

本文提及是重要在IP网络仅的命令。您在CSS能启用的许多服务需要仔细的安全配置。然而，本文着重默认情况下启用或由用户几乎总是启用，并且能要求不合格或重新配置的服务的信息。

某些默认设置在Cisco WebNS软件方面因历史上的原因存在。这些设置是可适用的，当他们选择，但是很可能不同的，如果新的默认是选定的今天。其他默认为多数系统是可适用的，但是能创建安全风险，如果这些默认用于构成网络周边防护的部分的设备。仍然其他默认由标准实际上要求，但是从安全角度讲总是不是理想。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

密码管理

密码和相似的所有权信息，例如简单网络管理协议(SNMP)社区字符串，是主要防御未经授权的访问对您的CSS。处理大多数密码的最佳方式是在TACACS+或RADIUS验证服务器上保存密码。然而，几乎每个CSS仍然有特许访问的一本地配置的口令。CSS在配置文件能也包括其他密码信息。在明文配置的所有密码在配置里出现加密与数据加密标准(DES)。

本地用户用户配置文件

此列表描述本地用户用户配置文件：

- *管理员*—管理员配置文件包括这些权限：对脱机诊断显示器菜单的访问对line命令的完全权限全双工目录访问这些设置可以从line命令或脱机诊断显示器菜单配置。
- *技术人员*—技术人员配置文件包括这些权限：对line命令的完全权限全双工目录访问这些设置可以配置与使用line命令。请勿使用技术人员配置文件CSS管理目的。
- *超级用户*—超级用户配置文件包括这些权限：对line命令的完全权限能力保存目录访问限制这些设置可以配置与使用line命令。
- *用户*—用户配置文件不能做配置更改并且包括目录访问限制。这些设置可以配置与使用line命令。

当您发出**restrict user-database命令时**，您强制执行在每个用户的目录访问限制。只有管理员和技术人员用户级可进行这些操作：

- 删除**restrict user-database命令**。
- 更改**local user-database命令**。
- 发出**clear running-config命令**。

交互式访问控制

能登陆到CSS的所有用户能显示公众不一定需要查看的信息。有时，能登陆到CSS的用户能使用CSS作为中继更深层网络攻击。获得对CSS的特许访问的用户能重新配置CSS。为了防止不适当的访问，您需要控制交互式登录到CSS。

默认情况下虽然多数交互式访问禁用，有例外。最明显的例外直接地是从连接的异步终端的对以太网管理端口的交互式会话，例如控制台终端和访问。

参考配置CSS远程访问存取方法关于如何控制对CSS的交互式访问的更多信息。

控制台端口

记住的一个重要项目是Cisco设备的控制台端口有特殊权限。特别是，请假设某人发送ESC (转码)字符到控制台端口，当POST诊断运行时。在重新启动，此人能容易地使用密码恢复流程为了控制系统后。能中断电源或导致系统崩溃，并且访问控制台端口到硬连线终端、调制解调器、终端服务器，或者一些其他网络设备的攻击者，能控制系统。这些攻击者能采取控制，即使他们不访问物理访问系统或能力通常登陆到系统。

所以，提供对Cisco控制台端口的访问的所有调制解调器或网络设备必须绑到与安全是可比较的使用对CSS的特许访问的标准上。最少，所有控制台调制解调器必须能要求拨号用户供应访问的一个密码的是类型，并且必须仔细管理调制解调器密码。

一般交互式访问

比用户有更多方式获得对CSS的交互式连接可能认识到。您能使用这些方法为了管理CSS ：

- Telnet
- Secure Shell主机(SSH)
- SNMP
- 控制台
- FTP
- XML
- Web管理

发出**restrict命令**为了启用或禁用。CSS在特定端口仍然侦听，但是断开连接。因此数据包不押这些端口，请配置访问控制表(ACL)子句丢弃数据包。

肯定的是困难的访问所有可能的模式阻塞。在大多数情况下，管理员必须使用某类认证机制为了确保，在所有线路的登录被控制。管理员必须保证登录是被控制的在应该是不可访问的从不受信任网络的机器。

控制台访问控制

默认情况下，控制台验证本地配置的用户配置文件。为了激活TACACS+或RADIUS验证，请发出**控制台验证**global命令和相关的选项。

VTY控制

默认情况下， VTY验证本地配置的用户配置文件。为了激活TACACS+或RADIUS验证，请发出**虚拟验证**global命令和相关的选项。

SSH 支持

如果您的软件支持加密的访问访问协议例如SSH，思科建议您启用仅该协议，并且请禁用Telnet访问，当您要使用SSH服务器时。为了启用SSH守护程序(SSHD)，您需要SSHD服务器许可证，启用在CSS软件英文虎报和增强版的SSHD功能。发出**sshd**命令。参考配置CSS网络协议欲知更多信息。

注意： SSH版本1支持在4.01开始的。SSH版本2支持在5.20开始的。

RADIUS

自版本5.00和以上，您能配置CSS使用RADIUS用户认证。为了配置RADIUS验证的CSS，参考配置用户配置文件和CSS参数。

注意： 用户/组配置文件只要求互联网工程任务组(IETF) RADIUS属性， [006]服务类型=管理。

此列表识别调试消息代码：

```
PW_ACCESS_REQUEST       1
PW_ACCESS_ACCEPT        2
PW_ACCESS_REJECT        3
PW_ACCOUNTING_REQUEST   4
PW_ACCOUNTING_RESPONSE  5
PW_ACCOUNTING_STATUS    6
PW_ACCESS_CHALLENGE     11
```

为了查看关联与RADIUS登录的调试，发出这些命令：

```
logging subsystem radius level debug-7 logging subsystem security level debug-7 logging
subsystem netman level debug-7
```

这是成功认证调试的示例：

```
JUL 23 02:30:41 7/1 165 SECURITY-7: SECMGR:SecurityAuth:Request from 0x30204b10
JUL 23 02:30:41 7/1 166 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
JUL 23 02:30:41 7/1 167 RADIUS-7: Auth Primary
JUL 23 02:30:41 7/1 168 RADIUS-7: The id is 1
```

```
JUL 23 02:30:41 7/1 169 RADIUS-7: Return Auth Primary
JUL 23 02:30:41 7/1 170 RADIUS-7: RADIUS attribute 0 received with bad length -2
JUL 23 02:30:41 7/1 171 SECURITY-7: Security Manager sending success 5 reply to
 caller 30201c00
JUL 23 02:30:41 7/1 172 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x30204b10
JUL 23 02:30:41 7/1 173 NETMAN-6: CLM: Login user1@172.16.20.200
JUL 23 02:30:45 7/1 174 NETMAN-6: CLM: Logout user1@172.16.20.200
```

这是失败由于不正确的用户名或密码验证的示例：

```
JUL 23 02:31:36 7/1 177 SECURITY-7: SECMGR:SecurityAuth:Request from 0x30204b11
JUL 23 02:31:36 7/1 178 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
JUL 23 02:31:36 7/1 179 RADIUS-7: Auth Primary
JUL 23 02:31:36 7/1 180 RADIUS-7: The id is 2
JUL 23 02:31:36 7/1 181 RADIUS-7: Return Auth Primary
JUL 23 02:31:36 7/1 182 SECURITY-7: Security Manager sending error 7 reply to
 caller 30201c00
JUL 23 02:31:36 7/1 183 SECURITY-7: SECMGR:SecurityMgrProc:Try Secondary
JUL 23 02:31:36 7/1 184 SECURITY-7: Security Manager sending error 7 reply to
 caller 30201c00
JUL 23 02:31:36 7/1 185 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x30204b11
```

这是失败验证的示例，因为用户配置文件RADIUS属性006服务类型没有配置：

```
JUL 23 02:36:33 7/1 195 SECURITY-7: SECMGR:SecurityAuth:Request from 0x30204b13
JUL 23 02:36:33 7/1 196 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
JUL 23 02:36:33 7/1 197 RADIUS-7: Auth Primary
JUL 23 02:36:33 7/1 198 RADIUS-7: The id is 4
JUL 23 02:36:33 7/1 199 RADIUS-7: Return Auth Primary
JUL 23 02:36:33 7/1 200 RADIUS-7: RADIUS attribute 0 received with bad length -2
JUL 23 02:36:33 7/1 201 SECURITY-7: Security Manager sending success 5 reply to
 caller 30201c00
JUL 23 02:36:33 7/1 202 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x30204b13
JUL 23 02:36:33 7/1 203 NETMAN-6: CLM: Login user1@172.16.20.200
```

TACACS+

在版本5.03和以上，您能配置CSS使用TACACS+用户认证。为了配置TACACS+认证的CSS，参考Cisco CSS 11000系列的版本注释。

为了查看关联与TACACS+登录的调试，发出这些命令：

```
logging subsystem security level debug-7 logging subsystem netman level debug-7
```

这是成功认证调试的示例：

```
JUL 23 01:53:32 7/1 89 SECURITY-7: SECMGR:SecurityAuth:Request from 0x30204b08
JUL 23 01:53:32 7/1 90 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
JUL 23 01:53:33 7/1 91 NETMAN-7: TACACS:tac_Authen:Final <Authen OK->
JUL 23 01:53:33 7/1 92 NETMAN-7: TACACS:tac_Authorize:Final <Author OK->
JUL 23 01:53:33 7/1 93 NETMAN-7: TACACS:tacacs_AuthorizeCommands <user1:vty1> Rsp:
 <Author OK> from10.66.79.241:49
JUL 23 01:53:33 7/1 94 NETMAN-7: TACACS:TACACS_AuthAgent:Rqst <user1:vty1:-2132790672>
 Rsp <Author OK:> <PRIV_ADMIN>
JUL 23 01:53:33 7/1 95 SECURITY-7: Security Manager sending success 0 reply to
 caller 30201c00
JUL 23 01:53:33 7/1 96 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x30204b08
JUL 23 01:53:33 7/1 97 NETMAN-6: CLM: Login user1@172.16.20.200
JUL 23 01:54:11 7/1 98 NETMAN-6: CLM: Logout user1@172.16.20.200
```

这是失败的认证的示例由于不正确的用户名或密码：

```
JUL 23 01:54:41 7/1 109 SECURITY-7: SECMGR:SecurityAuth:Request from 0x30204b0a
```

```
JUL 23 01:54:41 7/1 110 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
JUL 23 01:54:41 7/1 111 NETMAN-7: TACACS:tac_Authen:Final <Authen Rejected->
JUL 23 01:54:41 7/1 112 NETMAN-7: TACACS:TACACS_AuthAgent:Rqst <user1:vty1:-2132790672>
 Rsp <Authen Rejected:> <PRIV_DENIED>
JUL 23 01:54:41 7/1 113 SECURITY-7: Security Manager sending success 0 reply to
 caller 30201c00
JUL 23 01:54:41 7/1 114 SECURITY-7: SECMGR:SecurityMgrProc:Try Secondary
JUL 23 01:54:41 7/1 115 SECURITY-7: Security Manager sending error 7 reply to
 caller 30201c00
JUL 23 01:54:41 7/1 116 SECURITY-7: SECMGR:SecurityMgrProc:Try Tertiary
JUL 23 01:54:41 7/1 117 SECURITY-7: Security Manager sending error 7 reply to
 caller 30201c00
JUL 23 01:54:41 7/1 118 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x30204b0a
```

警告标志

在一些权限，您能大大缓和进入您的系统解密高手的进程民用并且/或者刑事诉讼，如果提供通知未经授权的用户的一标语他们的使用未授权的。除非采取步骤通知您的目的用户如此，执行其他权限禁止均等未经授权的用户的活动的监视器。一种方式提供此通知将放它到标志消息。您能配置与**set banner命令的**CSS的一个标志消息。此命令在5.03介绍。

合法通知需求复杂并且变化在每个权限和情况。在权限内，合法意见变化。与您的法律顾问讨论此问题。在与建议合作下，请考虑哪些通知放到您的标语：

- 公告或许特别地仅状态经授权的人员将登陆对或使用系统和信息关于谁能授权使用。
- 公告系统的所有未经许可使用是不合法的，并且可以是受民用并且/或者犯罪处罚支配。
- 公告任何使用系统可能不另行通知被记录或监控，并且产生的日志可能法庭上使用作为证据。
- 由本地法律要求的特定通知。

对于安全(而不是法律)原因，请勿包括在您的登录标识关于您的CSS的此信息：

- 名称
- 型号
- 运行的软件
- 所有者

通常配置的管理服务

除交互式远程登录之外，许多用户管理他们的与使用的网络协议。最普通的协议为此是SNMP和HTTP。多数安全选项不是启用这些协议。然而，如果启用其中一份协议，请获取它，此部分描述。

SNMP

SNMP是非常用途广泛为监控的网络设备，并且，频繁地，为配置更改。SNMP有两个主要标准的版本、SNMPv1和SNMPv2。您的CSS支持SNMP版本2C (SNMPv2C)，叫作基于属性的SNMP。CSS形成在SNMPv1格式的陷阱。

为了控制对CSS的SNMP访问，请发出**no restrict snmp命令**和**restrict snmp命令**。默认情况下访问通过SNMP启用。如果通过SNMP禁用访问， CSS在特定端口1仍然侦听，但是断开连接。配置ACL子句丢弃数据包，以便数据包不押SNMP端口。

不幸地， SNMPv1和SNMPv2C使用根据社区字符串的一个弱验证机制。验证共计在网络传送，不用加密的固定密码。如果必须使用SNMPv2C，小心选择无名的社区字符串，例如， (和请勿使用公

共或私有)。如果在所有可能，请避免使用所有网络设备的同样社区字符串。将不同字符串或字符串用于每个设备，或者至少用于网络的每个区域。请勿做只读字符串同读写字符串一样。若可能，请执行轮询与只读属性字段的定期SNMPv2C。使用仅读写字符串实际的写入操作。

SNMPv2C不是适当在公共互联网间使用对于这些原因：

- SNMPv2C用途明文验证字符串。
- SNMPv2C是容易地被伪装的基于数据报的事务处理协议。
- 作为定期轮询的一部分，大多数 SNMP 实现会反复发送这些字符串。

在您使用在公共互联网间前的SNMPv2C请认真考虑暗示。

在多数网络中，合法SNMP消息只来自某些管理站。如果合法SNMP消息只来自您的网络的某些管理站，请考虑应用对电路VLAN为了拒绝不需要的SNMP消息的使用ACL。

SNMP管理站经常有认证信息大数据库，例如社区字符串。此信息能提供存取对于许多CSSs和其他网络设备。此信息的集中度做SNMP管理站攻击的一个自然目标。相应地巩固SNMP管理站。

HTTP

CSS通过与使用的HTTP协议支持远程配置可扩展标记语言(XML)文档。在WebNS版本，如果浏览对TCP端口8081， 4.10中或前，您能到达对WebNS设备管理用户界面的访问在明文。一般来说，HTTP访问与对CSS的交互式访问是等同的。使用HTTP的认证协议与一明文密码的发送是等同的在间网络的。不幸地，没有在HTTP的有效提供向基于质询的或一次性密码。所以， HTTP是一相对危险的选择为在公共互联网间的使用。

如果选择使用HTTP管理，请限制对适当的IP地址的访问与应用对电路VLAN的使用ACL。为了控制对CSS的HTTP XML访问，请发出**no restrict xml命令**和**restrict xml命令**。在WebNS中最新版本，命令更改到**web-mgt状态***[禁用|enable (event)]*。默认情况下访问通过HTTP XML禁用。为了控制HTTP WebNS设备管理用户访问，请发出**no restrict web-mgmt命令**和**restrict web-mgmt命令**。默认情况下WebNS设备管理用户界面禁用。您必须配置**no restrict xml命令**和**no restrict web-mgmt命令**为了浏览到在端口8081的CSS。

在版本5.00和以上，如果对电路地址的HTTP-browse在端口8081，浏览器重定向使用HTTPS和连接到同一个电路地址。

HTTPS

CSS支持远程配置通过HTTP安全(HTTPS)协议。此安全套接字层SSL保护能包括密码)的数据传输(在WebNS设备管理用户界面和您的Web浏览器之间。

为了控制HTTPS WebNS设备管理用户访问，请发出**no restrict web-mgmt命令**和**restrict web-mgmt命令**。默认情况下WebNS设备管理用户界面禁用。如果它禁用， CSS在特定端口继续侦听，但是断开连接。因此数据包不押SSL TCP端口443，请配置ACL子句丢弃数据包。

在互联网(和其他不受信任的网络的)管理和交互式访问

许多用户远程管理他们的CSSs，并且有时这在互联网是实现的。所有未加密远程访问具有一定风险，但是在公共网络（如互联网）上传输特别危险。所有远程管理机制，包括交互式访问、HTTP和SNMP，易受攻击。

此部分讨论的攻击是相对复杂那些，但是他们不是在范围外今天解密高手。采取适当的安全措施的公共网络提供商能经常反对这些攻击者。评估您的在所有供应商运载您的管理数据流使用的安全措施的信任级别。即使您委托您的供应商，请采取至少一些步骤从这些供应商也许犯所有错误的结果保护。

在此部分的所有小心适用于一样主机至于CSS。当本文讨论如何保护时CSS登录会话，也调查使用类似的机制为了保护您的主机，如果远程管理那些主机。远程互联网管理是有用的，但是它要求对安全的仔细的注意。

包嗅探器

骇客频繁地进入网络服务提供商拥有的计算机，或者在其他大型网络的计算机。解密高手安装包嗅探器程序，监控流量穿过网络。这些包嗅探器程序偷走数据，例如密码和SNMP团体字符串。网络操作员开始改进他们的安全，使此盗窃更加困难。然而，此盗窃是比较普遍的。除从外部骇客的风险之外，恶意的ISP人员能也安装嗅探器。在未加密的信道被发送的所有密码是危险的危险，包括登录和特权密码您的CSSs的。

如果能，避免登录您的与使用的CSS在任何不受信任网络的任何未加密的协议。如果您的CSS软件软件支持它，使用一个加密的登录协议例如SSH。

如果不访问一个已加密远程访问协议，另一种可能性是使用一个一次性密码系统例如S/KEY或OPIE，与TACACS+或RADIUS服务器一起，为了控制交互式登录和特许访问对您的CSS。优点是窃取的密码是没有用途的。窃取的密码由窃取的会话设。在会话上传送，并且与密码没涉及请保持可用对窃听者的数据，但是许多嗅探器程序设置集中密码。

如果必须发送在明文远程登录会话的密码，频繁地请更改您的密码。并且请注意密切注意您的会话横贯的路径。

其他 互联网 访问 威胁

除包嗅探器之外， CSS的远程互联网管理提交这些安全风险：

- 为了管理在互联网的CSS，您必须允许至少一些互联网主机访问CSS。这些主机可以被攻陷，或者他们的地址可以被伪装。当您允许从互联网时的交互式访问，您独自地使您的安全从属，不仅反欺骗测量，但是于是包含的服务提供商的反欺骗测量。如果进行这些操作，您可以减少这些危险：确保允许登陆到您的CSS的所有主机在您自己的控制下。以强认证使用加密的登录协议。
- 有时，对一未加密TCP连接的访问(例如远程登录会话)是可能获取。获得对此种会话的访问的人能实际上采取远离登陆的用户的控制。这样攻击不是接近一样普通象探测的简单信息包并且可以是复杂装载。然而，这样攻击是可能和特别地有您的网络在头脑里的攻击者，当目标能使用他们。对会话盗窃问题的唯一的真正的解决方案将使用一个严格已验证，已加密管理协议。
- 拒绝服务攻击是比较普遍的在互联网。如果您的网络受到DOS攻击，您可以无法到达您的CSS为了收集信息或采取防御行动。在别人的网络的一攻击能削弱对您自己的网络的管理访问。虽然您能采取步骤使您的网络抗性对DOS攻击，此风险的唯一的真正防御是有分开，带外管理信道(例如拨号调制解调器)用于紧急状态。

记录

思科CSSs能关于各种各样的事件的记录信息，许多有安全重要性。日志可以是无价的为表征和答复

对安全事件。您能发出**logging subsystem命令**为了启用注册CSS。级的默认日志是所有子系统的warning-4。

发出登陆命令的子系统的这些命令收集此信息：

- 用户登录
- 注销
- RADIUS 身份验证
- TACACS+ 身份验证

```
logging subsystem radius level debug-7 logging subsystem security level debug-7 logging subsystem netman level debug-7
```

注意： netman subsystem命令盖板TACACS+调试。

从安全角度讲，最重要的事件系统日志记录通常包括这些事件：

- 接口状态变化
- 对系统配置的更改
- ACL匹配

```
logging subsystem netman level info-6 !--- Note that the default logging level is warning-4, which does !--- not appear in the configuration. logging commands enable logging subsystem acl level debug-7
```

远程监控(RMON)允许您远程监控并且分解数据包的活动在CSS以太网端口的。RMON也允许报警配置MIB对象监视器并且允许事件配置通知您这些告警条件。RMON事件是发生的操作，当一相关的RMON报警被触发时。您能配置报警事件这样，当报警事件发生时，生成一个或这两个项目：

- 日志事件
- 对SNMP网络管理站的一个陷阱

保存日志信息

默认情况下， CSS保存引导程序和子系统事件日志消息到在硬或闪存盘的日志文件。这些文件的内容在ASCII文本被记录。您能也配置CSS传送日志消息到激活CSS会话、电子邮件地址，或者另一个主机系统。

本地日志文件的最大大小是硬磁盘的系统和10 MB的50 MB闪存磁盘的系统的。

子系统日志消息是在CSS的操作时发生的子系统事件。CSS保存在sys.log文件的这些消息。CSS创建此文件，当必须记录的第一个子系统事件发生时。CSS确定记录的哪些子系统消息由其已配置的日志级别。

多数较大规模的安装有系统日志服务器。您能发出**logging host命令**为了发送记录信息到在主机系统的一个syslog demon。即使您有一个系统日志服务器，您应该仍然启用本地记录到磁盘。

所有日志用月标记时间，天，并且计时对第二。如果配置一相同的时间参考来源例如您的日志的Simple Network Time Protocol (SNTP)，您能更加容易地跟踪已登录事件顺序。为了配置在CSS的Sntp server，请发出**sntp命令**。SNTP介绍用5.00代码。

记录访问列表侵害

如果使用ACL对访问电路地址或内容规则Virtual IP (VIP)地址的过滤数据流，您能选择记录违犯您的过滤器标准的数据包。为了启用注册ACL条款，请发出**clause - log enable命令**。并且，请发出**logging subsystem acl level debug-7命令**。CSS记录此信息：

- 协议
- 源端口
- 目的端口
- 源 IP 地址
- 目的 IP 地址

设法避免记录日志的配置匹配非常很大数量的数据包的ACL条目的。此配置造成日志文件增长庞大，并且能剪切成系统性能。

您能也使用ACL记录分析关联与网络攻击的流量。在这种情况下，您配置ACL记录记录可疑数据流。您在CSS的Internet端的Cisco路由器能分析为了制作ACL。参考的分析和跟踪数据包泛洪使用Cisco路由器欲知更多信息。

注意： CSS ACL在入站数据包只应用。ACL不检查从接口是出站的数据包。

获取IP路由

此部分讨论与方式关连路由器转发IP信息包的一些基本安全测量。参考的Cisco ISP基本要素-每个ISP应该考察关于这些问题的更多信息的重要IOS功能。

默认情况下， CSS的配置：

- 限制去VIP在CSS前记录它作为DOS攻击SYN数据包的数量**注意：** 此行为不可能禁用。
- 拒绝定向广播
- 丢弃有同样源和目的地IP地址的数据包
- 拒绝组播源IP地址
- 丢弃源或目的地端口0数据包

反欺骗

许多网络攻击依靠弄虚的攻击者，或者欺骗， IP数据包源地址。一些攻击依靠伪装为了攻击能工作。如果攻击者能使用别人的地址而不是他们自己的地址，其他攻击是更难跟踪。所以，防止伪装，无论哪里可行为网络管理员有价值。

应该执行反欺骗在是实用的网络的每个点。但是反欺骗通常是最容易执行和最有效在边界在大地址块之间或在网络管理之间域。在每个路由器的反欺骗在网络通常是不切实际的，因为源地址能合法地出现在所有指定接口的确定是困难。

如果是互联网服务提供商，您可以发现有效反欺骗，与其他有效安全措施一起，导致昂贵，采取他们的事务的问题用户对其他供应商。如果是ISP，特别小心在拨号池和其他最终用户连接点实行反欺骗控制。

注意： 参考的RFC 2267 。

企业防火墙管理员或有时周边路由器安装反欺骗测量，以便互联网的主机不能假设内部主机地址。然而，内部主机能仍然假设在互联网的主机地址。设法防止伪装在两个方向。有至少三个有说服力的理由安装在两个方向的反欺骗在组织防火墙：

- 如果他们尝试，内部用户被诱惑设法发起网络攻击和不太可能成功。
- 偶然地被不正确配置的内部主机是不太可能导致远程站点的麻烦。所以，他们是不太可能生成客户不满情绪。
- 外部骇客经常进入网络作为启动深层攻击的填充。这些解密高手可能是对与流出的电子伪装保护的网络感兴趣。

与ACL的反欺骗

不幸地，列出提供的命令适当的欺骗保护不是实用的。ACL配置太多取决于独立网络。基本目标是丢弃在接口到达不是从那些数据包推测的源地址的可行的路径的数据包。例如，在双电路CSS，在连接服务器站到互联网的互联网电路到达的您要丢弃所有数据包，但是有声称的源地址域来自在服务器站的一计算机。

同样地，在接口到达连接到服务器站，但是有一源地址域声称的您要丢弃所有数据包来自一计算机服务器站外。如果CPU资源准许，请应用在确定的所有电路的反欺骗什么流量能合法地到达可行。

运载中转流量的ISP能限制了机会配置反欺骗ACL，但是这样ISP能通常过滤声称在该ISP内地址空间产生的外部流量。

一般来说，必须用输入ACL建立反欺骗过滤器。必须过滤数据包在数据包到达的电路。CSS能只适用于ACL入站数据包。

当反欺骗ACL存在时，他们应该总是拒绝与广播或组播源地址的数据包。默认情况下， CSS拒绝这些数据包。反欺骗ACL应该也拒绝有保留环回地址作为源地址的数据包。另外，不管源或目的地址，您应该通常安排反欺骗ACL过滤所有互联网控制消息协议(ICMP)重定向。CSS ACL不允许您指定ICMP类型拒绝。反而，请发出**no redirects命令**为了配置所有电路IP地址不接受ICMP重定向。这些是命令：

```
clause # deny any 127.0.0.0 255.0.0.0 destination any clause # deny any 0.0.0.0 0.0.0.0 destination any
```

注意： 条款#拒绝任何命令过滤从许多Bootstrap协议的**所有0.0.0.0 0.0.0.0目的地**(BOOTP)/DHCP客户端的数据包。所以，命令不是适当的在所有环境。

定向广播控制

十分普遍和普遍的smurf DOS攻击和一些相关攻击，使用IP定向广播。默认情况下， CSS用**no ip subnet-broadcast命令**配置，拒绝定向广播。

IP 定向广播是要发送到某个子网的广播地址且未直接连接发送方机器的数据报。定向广播通过网络路由作为单播信息包，直到定向广播到达在目标子网。在子网，定向广播转换到链路层广播。由于IP寻址体系结构的本质，仅最后路由器或第3层网络设备在一系列能确实地识别定向广播。此设备是连接直接地对目标子网的那个。定向广播偶尔用于一些正当用途，但在金融服务行业之外的使用较为少见。

在 smurf 攻击中，攻击者从伪造的源地址向定向广播地址发送 ICMP Echo 请求。结果，目标子网发送的所有主机回复伪造的来源。当攻击者发送这种请求的连续流时，攻击者能创建更更加大量的回复流，能完全淹没主机地址弄虚。

参考最新信息在拒绝服务攻击：“最小化策略的作用的Smurfing” 说明和信息能拦截在(的Smurf攻击取决于网络设计)的一些防火墙路由器。本文在Smurf攻击也提供一般信息。

路径完整性

许多攻击取决于能力影响数据包通过网络采取的路径。如果解密高手控制路由，有机会他们能伪装另一个用户计算机的地址和有回程数据流发送对他们。有时，解密高手能拦截和读供别人使用的数据。路由可能为DoS目的纯粹地也被打乱。

IP 源路由

IP协议支持允许IP数据包发送方控制路由数据包上往最终目的地，和通常，路由所有回复上的源路由选项。这些选项在实际网络用于合法目的很少使用。更加一些老的IP实施不适当地处理源路由信息包。某人能发送与源路由选项的数据包，并且，可能，失败运行这些实施的机器。

默认情况下CSS用**no ip source-route set命令**配置。CSS从未转发运载一个源路由选项的IP数据包。请留下default命令已配置的，除非知道您的网络需要源路由。

ICMP 重定向

ICMP重定向消息指示端节点使用一个特定路由器作为路径到特定目的地。在正常运行的IP网络，路由器发送仅重定向到在路由器的本地子网的主机。端节点从未发送重定向，并且重定向从未横断超过一网络跳。然而，攻击者能违反这些规则，并且一些攻击根据这些规则。过滤流入的ICMP重定向在管理域之间的一个边界位于所有路由器的输入接口。另外，在Cisco路由器接口输入端应用过滤所有ICMP重定向的您能有所有ACL。此过滤的正确地配置的网络不导致操作影响。

此种过滤防止远端攻击者发起仅的重定向攻击。另外，攻击者能使用重定向导致重大的麻烦，如果攻击者主机直接地连接对分段和受到攻击的主机一样。

默认情况下，CSS配置接受在配置的每个电路IP地址的重定向。发出**no redirect命令**在电路IP地址下为了关闭此功能。

路由协议过滤和验证

如果使用支持验证的一个动态路由协议，请启用该验证。验证防止在路由结构的一些恶意攻击，并且可也帮助防止在网络的不正确的配置的恶意设备能造成的损伤。

对于同样原因，服务提供商和大型网络的其他操作员能考虑使用路由过滤。使用路由过滤，网络路由器不接受明显错误的路由信息。对于路由过滤，请使用**distribute-list**参数在命令。路由过滤使用过度能毁坏动态路由优点。但是有选择性的使用经常帮助防止坏结果。例如，如果使用一个动态路由协议为了与残余部分客户网络联络，请勿接受从该客户的任何路由除路由之外对您实际上委派了给客户的地址空间。

CSS不能过滤路由。反而，请配置CSS的路由对等体与此功能的。

本文在路由验证和路由过滤的配置不提供更多的指导信息。这样文档是在Cisco.com和在别处可用的。您能参考本文Cisco ISP基本要素-每个ISP应该考察的重要IOS功能。由于复杂性，请征求有经验的建议，如果是新手，在您配置在重要网络前的这些功能。

泛洪管理

许多DOS攻击依靠无用信息包溢出。这些充斥拥塞网络链路，减速主机，并且能超载路由器。仔细的路由器配置可以减少扩散的影响。

溢出管理的重要部分是性能瓶颈能发生的感知。如果充斥超载一条T1线路，请过滤在路由器的充斥在线路的发起端。如果在这种情况下，过滤在目的地端有很少或没有效果。如果路由器是多数超载网络组件，您能使事态更坏，如果过滤在路由器放置重大需求的保护。当您考虑建议的实施在此部分时的请记住此。

转接泛洪

您能使用在上行Cisco IOS路由器的思科QoS功能为了保护CSS、主机和链路以防止充斥。不幸地，本文不提供泛洪管理这一类一般处理。并且，保护非常取决于攻击。唯一的简单，通常可适用的建议是使用加权公平排队(WFQ)，无论哪里CPU资源可以支持WFQ。WFQ是低速串行线路的默认在Cisco IOS软件最新版本。其它特性可能的利益包括：

- 承诺接入速率(CAR)
- 通用流量整形(GTS)
- 自定义队列

有时，您能配置这些功能，当在主动攻击下。

CSS可以减少SYN溢出攻击影响在VIP和真实服务器的。默认情况下， CSS限制SYN和不完整三方握手数量并且记录他们作为DOS攻击。

参考的安全参考信息欲知更多信息。

可能不必要的服务

通常，请禁用在从潜在敌对的网络是可及的任何路由器的所有多余服务。服务此部分列出是有时有用的。如果他们不是在活动使用，但是请禁用这些服务。

SNTP

SNTP不是特别危险的，但是所有多余服务能提交渗透的一个路径。如果实际上使用SNTP，请务必明确配置委托时间源。SNTP不使用验证。扫描的损坏是推翻某些安全协议的好办法。佳方法是使用是内部和不太可能被伪装的来源。

Cisco 发现协议

思科设备发现协议(CDP)，在WebNS 5.10介绍，使用一些网络管理功能。因为在一直接地连接的分段的所有系统可进行这些操作， CDP是危险的：

- 学习路由器是Cisco设备
- 确定型号和运行的软件版本

攻击者能使用此信息为了设计攻击CSS。CDP信息直接地是仅可访问对连接的系统。CSS只发布CDP信息。CSS不侦听。您能发出**no cdp run**全局配置命令为了禁用CDP协议。您不能禁用在CSS的CDP在单个交换面基础上。

最新的逗留

类似所有软件， Cisco WebNS软件有Bug。其中一些Bug有安全影响。另外，新建的攻击继续被发明。并且被认为正确的行为，当软件块写入能有不良影响，当故意地利用时行为。

如果在Cisco产品中新发现重要的安全弱点，Cisco通常会公布有关安全弱点的建议通告。参考安全漏洞策略关于这些通知发出的进程的信息。通知的参考的安全建议。

几乎任何软件块所有意外行为能创建安全风险某处。建议有系统安全的直接暗示仅的提及Bug。如果保持您的软件最新状态，在没有任何安全建议时，您能增强您的安全。

一些安全问题不是软件Bug结果，并且网络管理员一定坚持意识在攻击的趋势。有于这些趋势有关的一定数量的网站、互联网邮件列表和用户网新闻团体。

相关信息

- RFC 2267
- 安全性建议
- 安全漏洞政策
- 安全参考信息
- 配置CSS网络协议
- 配置CSS远程访问存取方法
- 配置用户配置文件和CSS参数
- 版本说明
- 使用 Cisco 路由器确定数据包泛洪的特征并加以跟踪
- Cisco ISP基本要素-每个ISP应该考察的重要IOS功能
- 拒绝服务攻击的最新信息：“Smurfing”介绍及使危害最小化的信息
- 技术支持和文档 - Cisco Systems