如何在思科网络安全设备（运行 5.2.0 及更高版本）上将网页手动添加到白名单中，以便绕过 WBRS、Webroot 或 McAfee 扫描？

文档编号：117932

作者：Simon Putz 和 Siddharth Rajpathak，Cisco TAC 工程师。

2014 年 7 月 14 日

目录

问题：

如何在思科网络安全设备（运行 5.2.0 及更高版本）上将网页手动添加到白名单中，以便绕过 WBRS、Webroot 或 McAfee 扫描？

症状：

用户尝试访问合法站点，但是因低 WBRS 分数（受到病毒感染的 Web 服务器、通过 Web 服务器 IP 发送的垃圾邮件等）或由于在该页面上触发一个防恶意软件引擎而受到阻止。

如果用户是因为低 WBRS 分数而受到阻止，则会看到 MALWARE_GENERAL 阻止消息。 accesslog 将在阻止阈值（默认值为 −6.0）下显示 WBRS 分数。

要获得永久解决方案，请与 Cisco TAC 联系。这样一来，您便可以查看页面，以便调整 WBRS 或者向防病毒和防恶意软件供应商报告误报情况。

您也可以联系 Cisco TAC 来收集有关站点受阻原因的更多信息，以便网站的技术联系人或管理员可以收到通知并采取必要步骤。
联系 Cisco TAC 时，请确保提供相关阻止代码和 accesslog 行

绕过 WBRS 的步骤：

1. 创建包含您不希望受到阻止的所有站点的自定义 URL 类别（GUI −>“网络安全管理器”[Web Security Manager] −>“自定义 URL 类别”[Custom URL Categories]）。
2. 创建新的身份并添加新的自定义 URL 类别作为成员。 (GUI −> “网络安全管理器”[Web Security Manager] −>“身份”[Identities])
   根据您的设置，您必须选择“需要执行身份验证”(Authentication Required) 以及相应的组/用户成

员身份设置或者“无身份验证”(No Authentication)。

3. 创建新的网络访问策略（GUI ->“网络安全管理器”[Web Security Manager] ->“网络访问策略”[Web Access Policies]），将新身份与“策略成员定义”(Policy Member Definition) 中的访问策略相关联。

4. 点击您新创建的网络访问策略（到现在为止应显示为“全局策略”[global policy]）的“网络信誉和防恶意软件过滤”(Web Reputation and Anti−Malware Filtering) 列中的链接。
5. 选择“定义网络信誉和防恶意软件自定义设置”(Define Web Reputation and Anti−Malware Custom Settings)。
6. 将 WBRS 扫描设置为禁用状态，并/或根据需要调整其他恶意软件扫描参数。
7. 提交并确认更改。

*注意：*如果您在“URL 类别”(URL Category) 中将操作设置为“允许”(Allow)，则将绕过防恶意软件/防病毒扫描。

绕过 WBRS 和防恶意软件扫描的步骤：

注意：禁用防恶意软件扫描（Webroot 和/或 McAfee）可能导致潜在的安全风险。 只应该针对不含恶意软件的可信任站点执行此操作。

1. 创建包含您不希望受到阻止的所有站点的自定义 URL 类别（GUI −>“网络安全管理器”[Web Security Manager] −>“自定义 URL 类别”[Custom URL Categories]）。
2. 创建新的身份并添加新的自定义 URL 类别作为成员。 (GUI −> “网络安全管理器”[Web Security Manager] −>“身份”[Identities])
3. 创建新的网络访问策略（GUI −>“网络安全管理器”[Web Security Manager] −>“网络访问策略”[Web Access Policies]），将新身份与“策略成员定义”(Policy Member Definition) 中的访问策略相关联。
4. 在您希望完全绕过 WBRS 和防恶意软件扫描的新网络访问策略中，点击“URL 类别”(URL Categories) 列中的链接。
5. 对于您之前创建的自定义 URL 类别，请选择“允许”(Allow) 操作。
6. 提交并确认更改。

更新日期：2014 年 7 月 14 日　　文档编号：117932