802.1X在AireOS WLC的客户端排除

文档ID117714

已更新：钧窑03， 2014

贡献用亚伦伦纳德和尚卡尔Ramanathan， Cisco TAC工程师。

下载 pdf文档
打印
反馈

相关产品

- 无线， LAN (WLAN)

目录

简介

本文描述AireOS无线局域网控制器的(WLC) 802.1X客户端Exlusion。802.1X客户端排除是一个重要选项有在一1X验证器类似WLC。这是为了由不正确地是活动过度或功能的可扩展的认证协议(EAP)客户端防止认证服务器基础设施的超载。

请使用案件

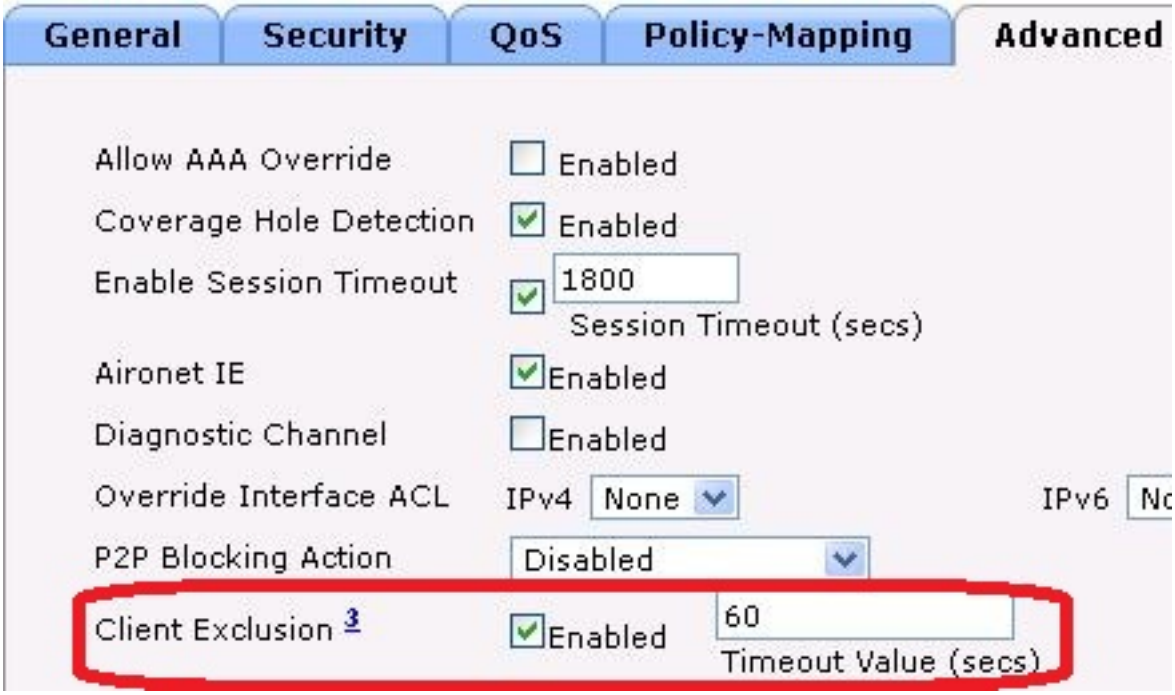
示例使用案件包括：

- EAP请求方可能配置与不正确凭证。多数恳求者，例如EAP恳求者，在一些个连续故障以后停止认证尝试。然而，一些EAP恳求者继续尝试重新鉴别在失败，可能许多次每秒。一些客户端超载RADIUS服务器并且导致整个网络的拒绝服务。
- 在主要网络故障切换以后，数百或千位EAP客户端也许同时尝试验证。 结果，也许超载认证服务器和提供一慢作用。如果客户端或验证器时间，在慢作用处理前，则恶性循环能发生认证尝试继续，然后的地方计时设法再处理答复。

注意：准入控制机制要求为了允许认证尝试成功。

802.1X排除防止触发超载30秒对几分钟在失败以后，允许正常认证成功的客户端。AireOS WLC名义上有802.1X客户端排除globablly启用在安全下>无线保护策略默认情况下。请参阅显示的策略此处。

客户端排除也许启用或禁用的根据每个WLAN基本类型。默认情况下它启用与60秒超时。



然而，由于默认EAP超时和重新传输设置， 802.1X排除从未生效。

WLC客户端没被排除，当802.1X排除启用

当802.1X排除在WLAN时，启用WLC客户端没有被排除。这归结于导致一个客户端行为不端从未点击足够的连续故障触发排除30秒的长默认EAP超时。配置更短的EAP超时用重新传输数量增长的允许802.1X排除生效。参见超时示例此处。

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
```

```
config advanced eap request-timeout 3
config advanced eap request-retries 10
```
确保RADIUS服务器从超载保护由于不正确地作用的无线客户端并且验证这些设置有效：

- “额外的802.1X认证失败”在WLC's全局客户端排除策略选择。
- 客户端排除在无线局域网的提前的设置启用。
- 客户端排除超时设置为60到300秒。

  注意：值高于300秒提供更加好的防护，但是也许触发用户投诉。

  警告：一些恳求者比其他需要更加长的超时。例如，如果使用一次性密码， EAP标识请求超时周期也许需要45秒为了允许用户输入New PIN。某慢可扩展Authetication灵活协议验证通过安全协议(EAP-FAST)恳求者也许要求20秒一更短的超时为了适应已保护访问控制(PAC)供应。

相关信息

- Cisco Bug ID CSCsq16858
- 技术支持和文档 - Cisco Systems

相关的思科支持社区讨论

已更新：钧窑03， 2014
文档ID117714