

使用外部CA将ISE 3.3与Stealthwatch 7.5.1集成

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[配置](#)

[A 部分：安全网络分析\(Stealthwatch\)证书配置](#)

[第I部分 — 为安全网络分析pxGrid客户端证书生成CSR](#)

[第II部分 — 使用外部CA创建安全网络分析pxGrid客户端证书](#)

[第III部分 — 将安全网络分析pxGrid客户端证书添加到管理器](#)

[第IV部分 — 将CA根证书导入到Manager信任库中](#)

[B 部分：思科身份服务引擎3.3证书配置](#)

[第I部分 — 生成ISE服务器pxGrid证书](#)

[第II部分 — 使用外部CA创建ISE服务器pxGrid证书](#)

[第III部分 — 将CA根证书导入ISE信任存储](#)

[第4部分 — 将ISE证书绑定到证书签名请求\(CSR\)](#)

[集成](#)

[验证](#)

[故障排除](#)

[DNS解析问题](#)

[解决方案](#)

[未知CA错误或缺少受信任证书](#)

[解决方案](#)

[已知缺陷](#)

简介

本文档介绍使用pxGrid连接将ISE 3.3与安全网络分析(Stealthwatch)集成的过程。

先决条件

思科建议了解以下主题：

- 身份服务引擎
- 平台交换网格(pxGrid)
- 安全网络分析(Stealthwatch)
- TLS/SSL证书。
- Windows Server 2016上的PKI

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE)版本3.3补丁4
- 安全网络分析(Stealthwatch)7.5.1
- Windows server 2016作为外部证书颁发机构(CA)服务器。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

A 部分：安全网络分析(Stealthwatch)证书配置

第1部分 — 为安全网络分析pxGrid客户端证书生成CSR

1.登录到Stealthwatch管理控制台(SMC)。

2.从主菜单中选择配置>全局>集中管理。



Risk



Monitor



Investigate



Report



Configure

Configure

X

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management

Manager

UDP Director

External Lookup

System

思科漏洞ID 18119	ISE选择不支持的密码ITLS服务器Hello数据包
思科漏洞ID 01634	无法使用EPS条件隔离设备

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。