思科快速遏制威胁 v1

最后更新日期：2016 年 2 月 4 日

关于本解决方案

恶意软件更加复杂、更加隐秘并且速度更快。少保护的 IoT（物联网）终端激增正在扩大攻击面。这些条件在攻击前、攻击中和攻击后对安全团队发出降低风险的挑战。

许多组织已经能够检测异常，导致攻击者开发恶意软件以避开检测并且快速移动以窃取有价值的数据。因此，检测和停止威胁对于 IT、安全和事件响应团队而言已成为当务之急。

作为一种思科安全解决方案，思科快速威胁遏制方案采用一系列紧密集成并由供应商支持的检测、可视性和实施技术，检测并自动遏制恶意软件。本解决方案利用思科 FireSIGHT 管理中心 (FMC) 和思科身份服务引擎 (ISE) 的功能。

当检测到严重的威胁或者危害表现时，思科 FireSIGHT 管理中心向身份服务引擎发出警报以遏制遭受侵害的终端。然后，ISE 将实施说明自动推送到路由器、交换机、防火墙和无线控制器。

思科快速威胁遏制过程遵循此基本时间线：

- 企业用户下载文件，而不知道此文件实际上是恶意软件。
- 思科安全传感器扫描用户活动和已下载文件，且 FireSIGHT 管理中心整合和关联传感器数据。
- FireSIGHT 管理中心公然标识可疑文件和警告 ISE，这会将用户或设备访问策略更改为可疑状态。
- 根据新策略信息，网络执行器自动限制访问
- 隔离设备以便减灾或规避，并根据安全策略拒绝访问。

关于本演示

本演示包括显示如何使用思科快速威胁遏制的场景，其中包括：

- 场景 1：威胁遏制和补救

要求

本演示无需终端路由器。

表 1. 要求

必备	可选
• 笔记本电脑	• Cisco AnyConnect

拓扑

此内容包含预配置的用户和组件，旨在说明解决方案脚本场景和功能。大多数组件都能通过预定义管理用户帐户进行完整的配置。要查看用于访问组件的 IP 地址和用户帐户凭证，可点击活动会话的 **Topology（拓扑）**菜单中的组件图标，也可点击需要使用这些凭证的场景步骤中的组件图标。

图 1. 逻辑拓扑

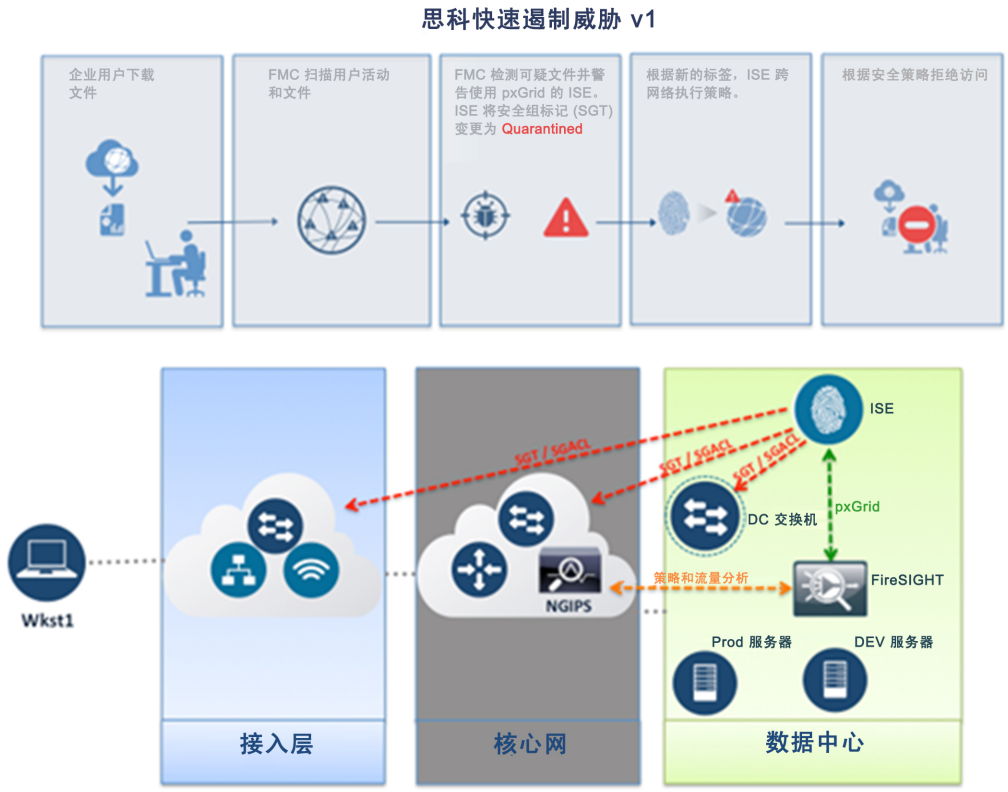
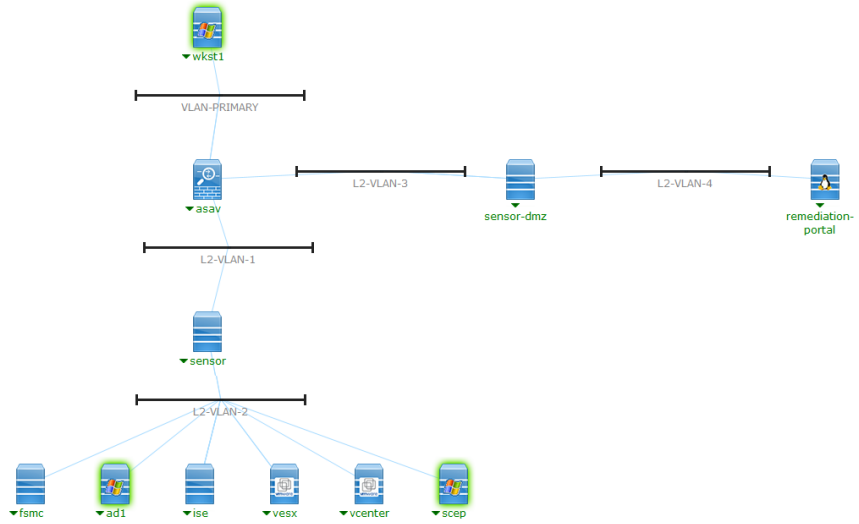


图 2. 物理拓扑



开始演示

演示前的准备

在向现场观众进行演示之前，我们强烈建议您浏览本文档的内容，并使用活动会话进行实操。这有助于您熟悉文档和内容结构。

准备是成功演示的关键。

执行以下步骤安排内容会话并配置演示环境。

1. 浏览至 dcloud.cisco.com，选择最接近您的位置，然后利用 Cisco.com 凭证登录。
2. 如果这是您首次将路由器与 dCloud 结合使用，则注册并配置路由器。[显示操作方法]
3. 安排会话。[显示操作方法]
4. 测试连接。[显示操作方法]
5. 在 **My Dashboard（我的控制面板）> My Sessions（我的会话）**中检查会话状态是否为 **Active（活动）**。

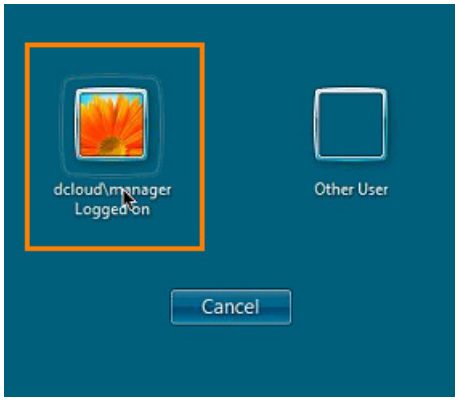
备注：会话可能最多需要 10 分钟才能变为活动状态。

6. 点击 **View（查看）**打开活动会话。
7. 为获取最佳性能，利用 **Cisco AnyConnect VPN** [显示操作方法] 和**笔记本电脑上的本地 RDP 客户端** [显示操作方法] 连接至工作站。
    - 工作站 1：**198.18.133.36**，用户名：**dcloud\manager**，密码：**C1sco12345**

备注：您也可以使用 Cisco dCloud 远程桌面客户端 [显示操作方法] 连接到工作站。dCloud 远程桌面客户端最适合用于访问交互最少的活动会话。然而，许多用户使用此方法遭遇连接和性能问题。

8. 如果登录期间提示，则在提示时选择 **dcloud\manager** 用户并输入密码 **C1sco12345**。

图 3. Dcloud\manager 用户

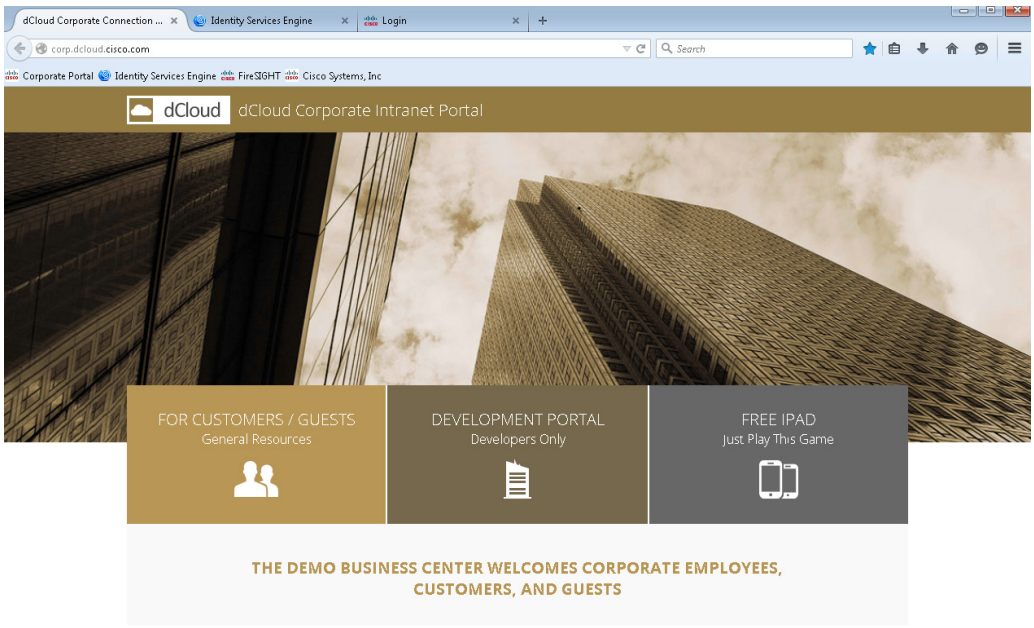


场景1.　威胁遏制和补救

步骤

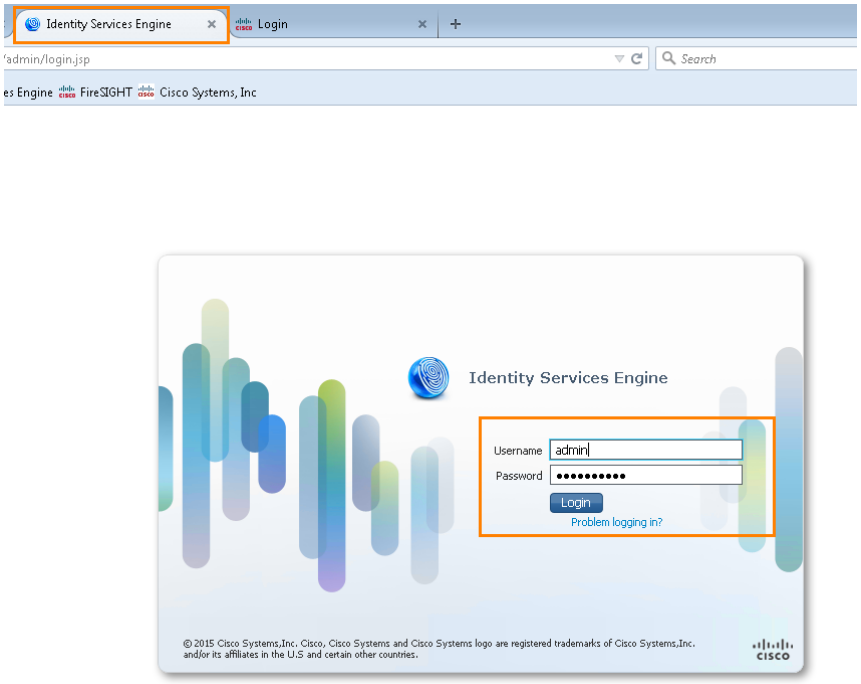
1. 从工作站打开 Firefox 浏览器。dCloud 企业内联网门户显示三个选项卡。

图 4.　dCloud 企业内联网门户



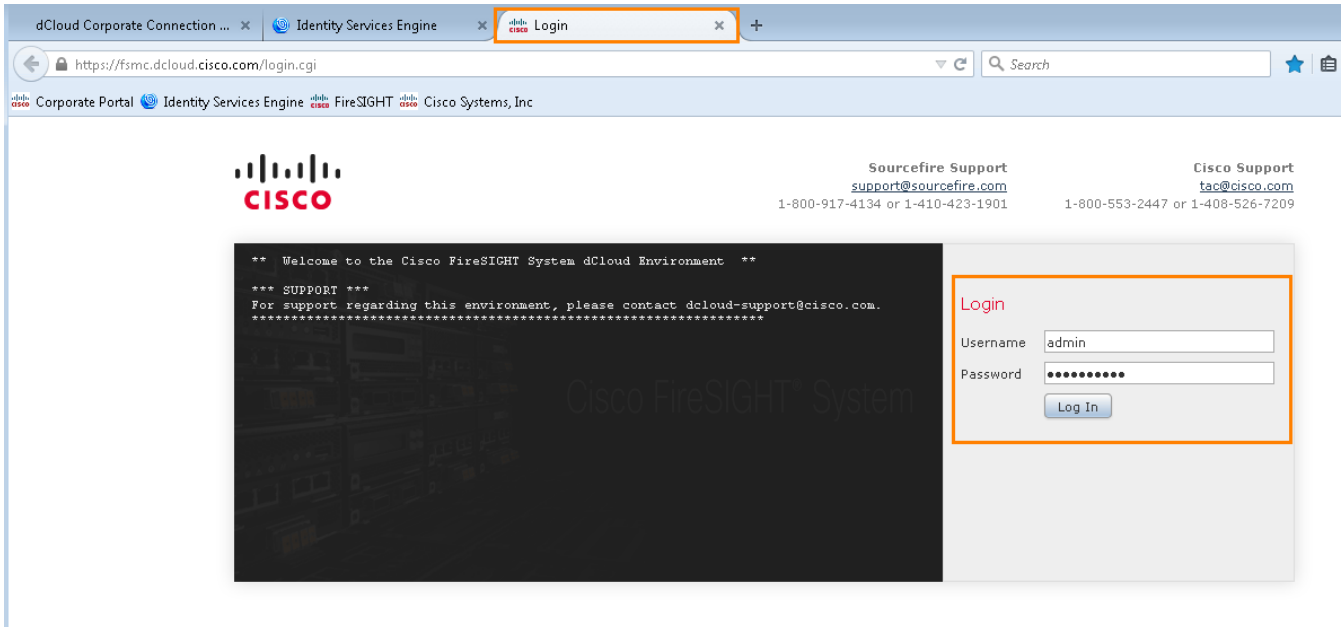
2. 点击 **Identity Services Engine (ISE)（身份服务引擎 (ISE)）**选项卡。使用 **userid admin** 和已保存的密码 (C1sco12345) 登录。

图 5.　ISE



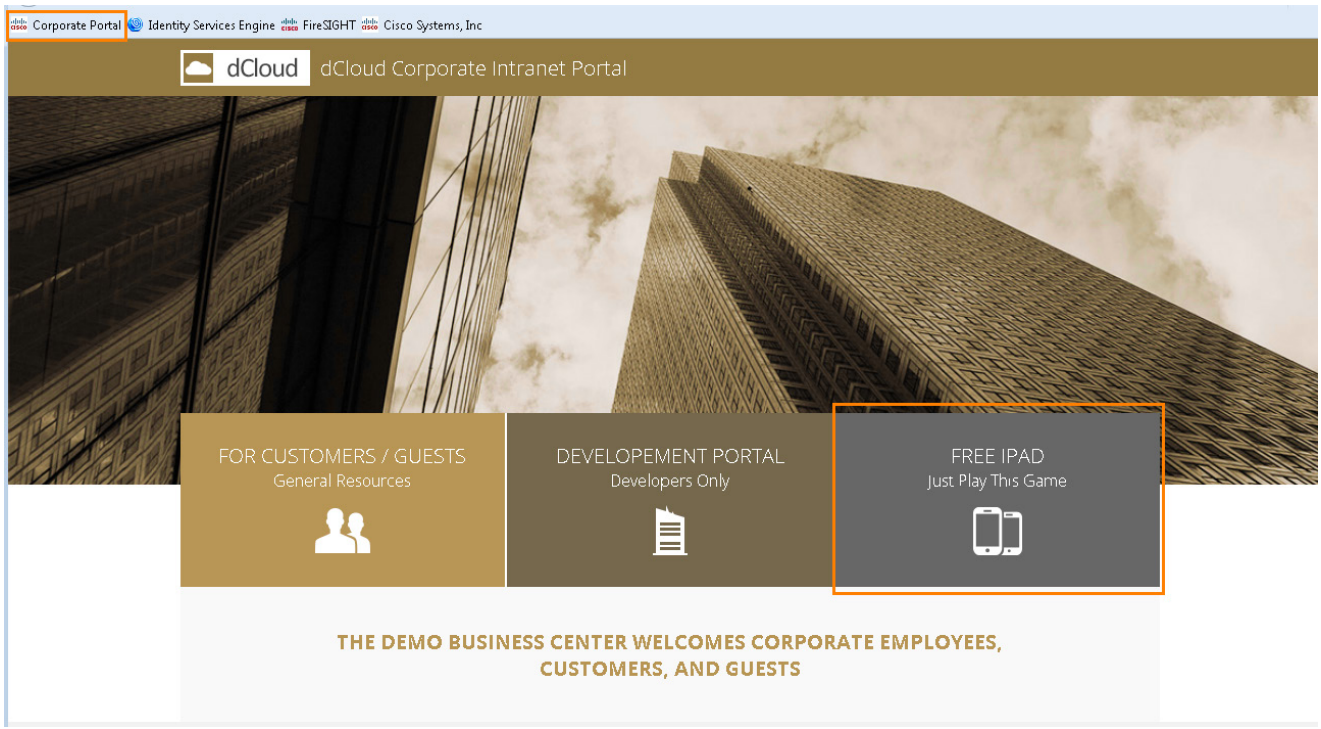
3. 点击 **FireSIGHT Management System（FireSIGHT 管理系统）**选项卡。使用 **userid admin** 和已保存的密码 (C1sco12345) 登录。

图 6. FireSIGHT 管理系统



4. 返回“dCloud Corporate Connection”（dCloud 企业连接）选项卡，选择 **Free iPad（免费 iPad）**。

图 7. 免费 iPad



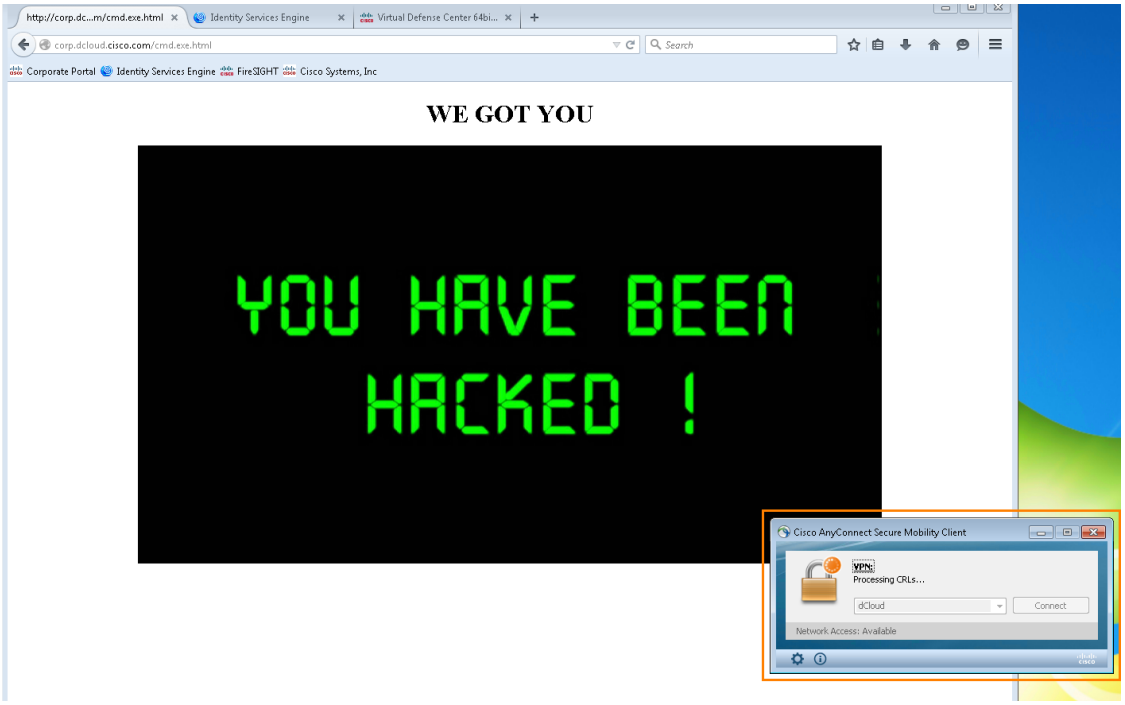
5. 点击链接导致恶意软件利用工作站上的安全性漏洞危害工作站。

备注：发生的顺序如下：

- 思科下一代 IPS (NGIPS) 传感器立即识别发生的事件，并查看 FireSIGHT 中的入侵事件。
- 入侵事件被绑定到 FireSIGHT 管理中心 (FSMC) 的相关事件上，FireSIGHT 管理中心指示 FireSIGHT 通过 pxGrid 与 ISE 进行通信，传达应隔离此特定工作站。
- 从 FireSIGHT 收到此信息后，ISE 将授权更改 (CoA) 发送至用户所连接的接入层设备，立即采取行动。
- 然后，ISE 从网络动态断开用户的连接。系统自动重新连接用户。
- ISE 动态更新此特定主机的安全策略，并通过将新的隔离安全组标记 (SGT) 推送至用于此特定用户会话的接入层设备，以强制执行此安全策略。
- SGT 用于允许或拒绝整个网络基础设施上的所有支持 TrustSEC 的设备上的流量。

备注：AnyConnect 偶尔不会自动重新连接。如果出现这种情况，请手动重新连接。

图 8. 重置连接



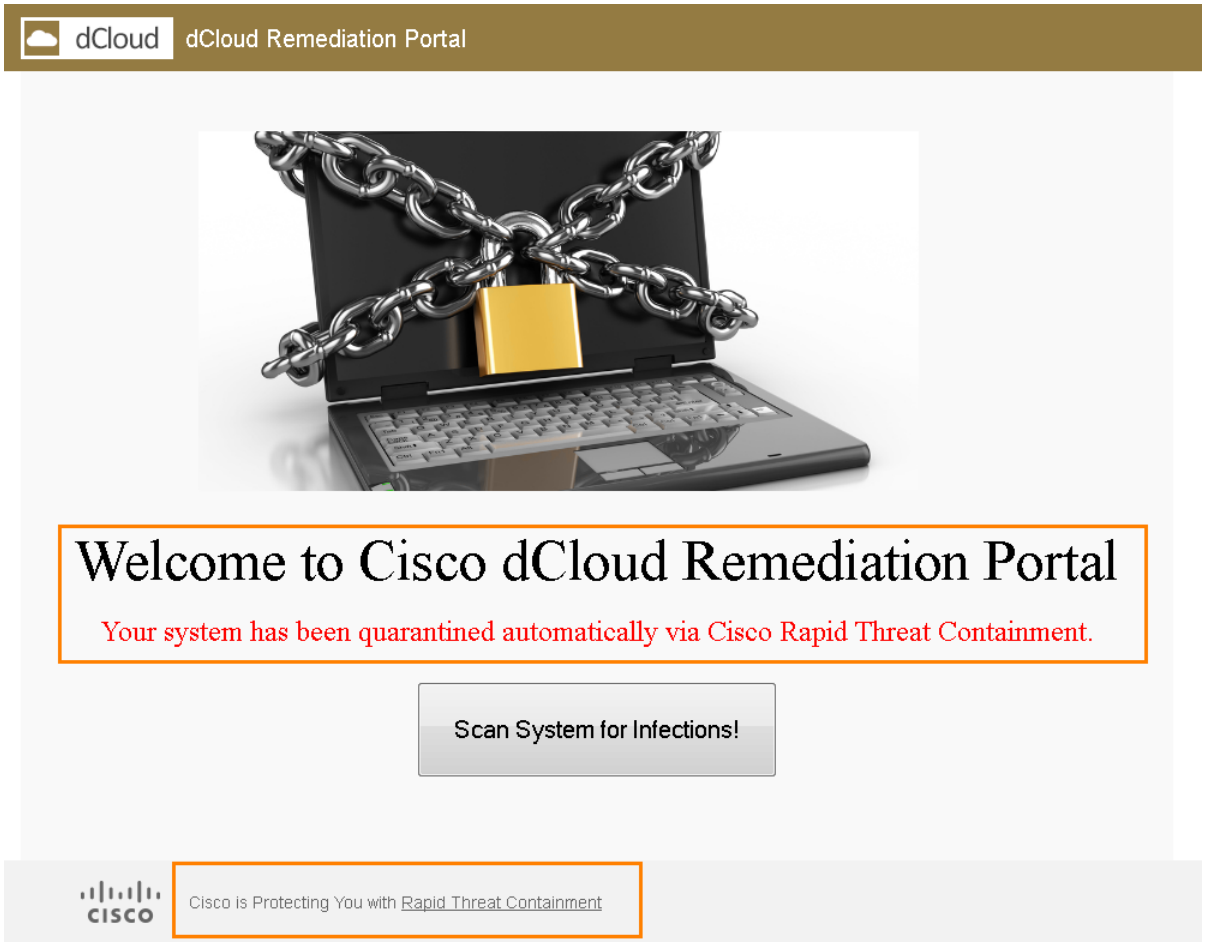
6. 重新连接后，系统会显示 Cisco dCloud 补救门户。

备注：ISE 动态更改工作站的安全策略后，此工作站就对网络资源具有非常有限的访问权限。在这种情况下，安全策略规定，应仅允许隔离系统访问企业补救门户。任何其他尝试通过的网络流量均将导致用户被重定向回补救门户。

此外，出于演示目的，我们已授权工作站访问权限，可以登录 ISE 和 FireSIGHT。最终，由组织强制执行安全策略，但在每种特殊情况下会有所不同。

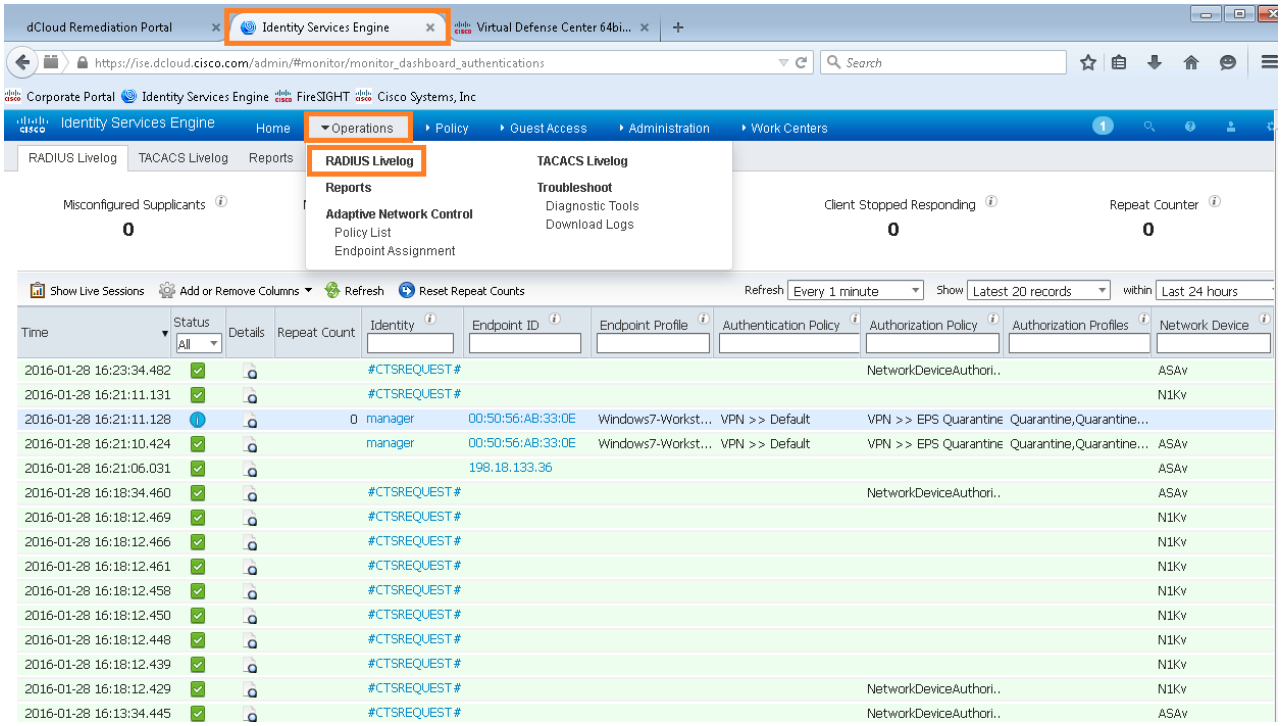
安全并不会一尘不变。安全策略会根据每个不同客户的独特需求而强制执行。

图 9. Cisco dCloud 补救门户



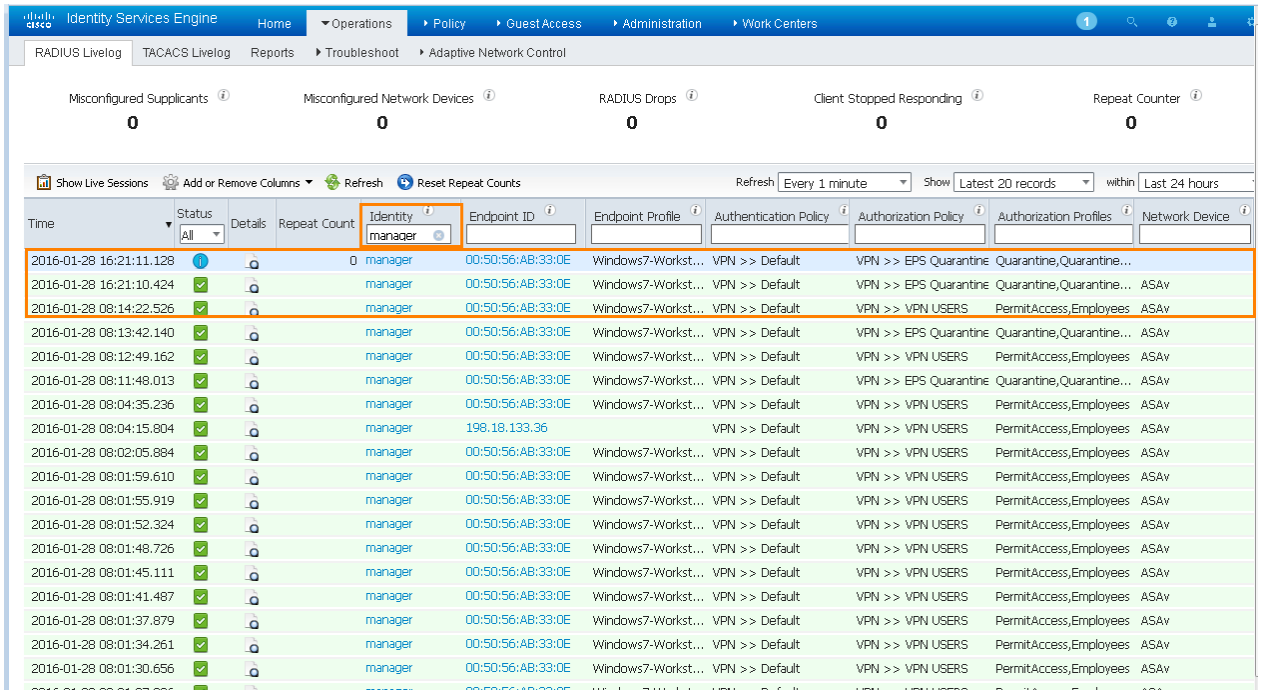
7. 转至 **ISE** 选项卡，然后依次选择 **Operations（操作）> Radius Livelog**。系统将显示连接历史记录。

图 10. ISE > Radius Livelog



8. 在“Identity Filter”（身份过滤器）中输入 **manager**，然后按 **Enter** 键。指出您被授予员工访问权限。检测到恶意软件后，则会断开您的连接，并在隔离区下重新登录。

图 11. 过滤结果

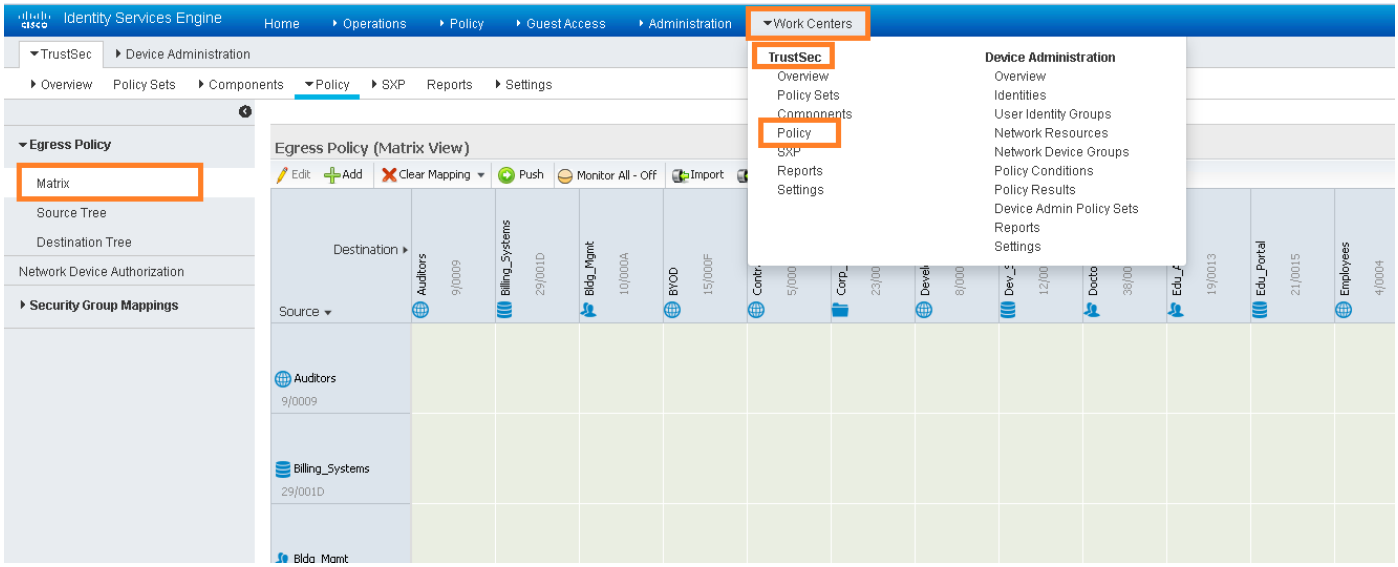


9. 依次选择 **Work Centers（工作中心）> TrustSec > Policy（策略）**。此时会显示出口策略矩阵。

备注：支持 Cisco TrustSec 的网络允许您从单一界面进行访问，从而轻松管理整个网络的安全策略。通过使用出口策略矩阵在 ISE 中轻松配置 TrustSec 策略。

配置矩阵时，使用源和目标安全组标记 (SCG) 的简单组合，可确定网络上存在的接入设备。然后，可以将 TrustSec 安全策略从 ISE 推送至支持此功能的网络中的所有支持 TrustSEC 的设备。

图 12. 出口策略矩阵



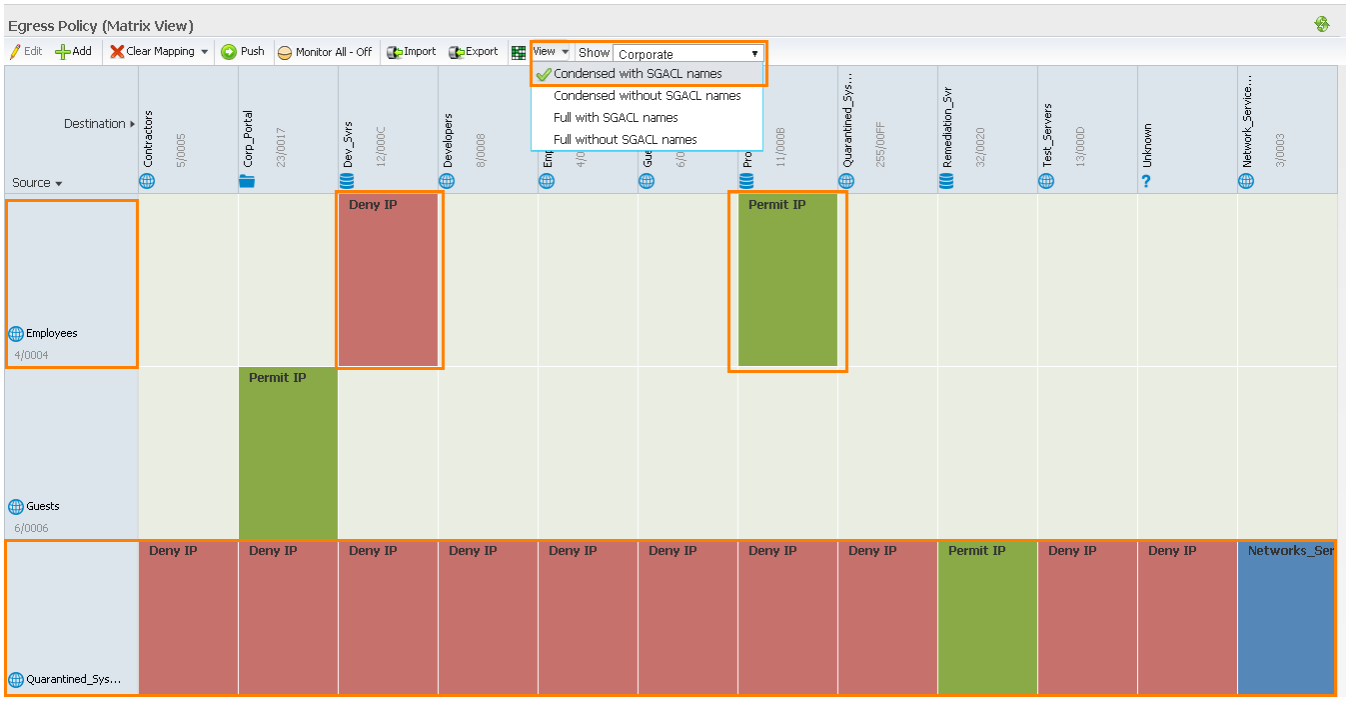
10. 在“Show”（显示）下拉菜单中，选择 **Corporate（企业）**。

11. 在“View”（视图）下拉菜单中，选择 **Condensed with SGACL names（压缩 SGACL 名称）**。

12. 系统会显示网络安全策略矩阵。指出在现行政策下，员工不得访问 Dev 服务器，但可访问生产服务器。此外，指出拒绝隔离系统访问任何内容，但补救服务器自身和某些基本网络服务除外。

备注：安全策略可以如同拒绝/允许特定源/目标 SGT 对的所有 IP 流量那样简单，或如同将各 SGT 对捆绑至特定的更为复杂的访问控制列表 (SGACL) 那样复杂。然后，SGACL 可被推送至受支持的 TrustSec 网络设备。

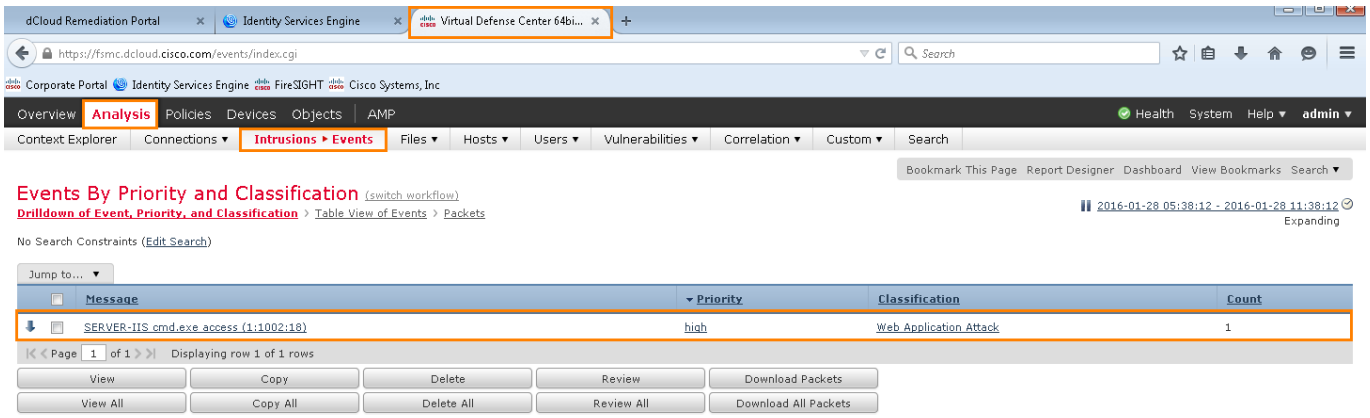
图 13. 安全策略矩阵



13. 点击 **FireSIGHT** 选项卡，然后依次选择 **Analysis（分析）> Intrusions（入侵）> Events（事件）**。此列表显示检测到的入侵威胁。

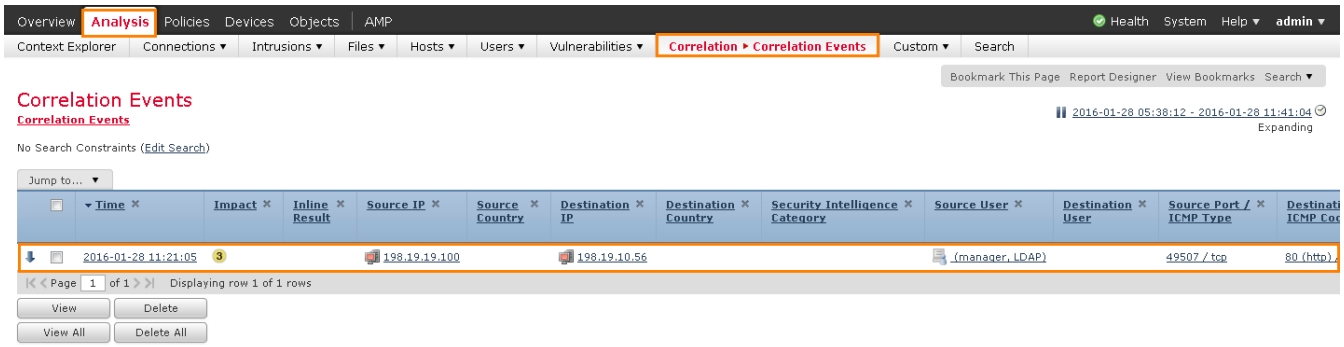
备注：入侵事件显示，FireSIGHT 检测到漏洞。然后，入侵事件用信号传递相关事件，最终导致 FireSIGHT 通过 pxGrid 向 ISE 传达应隔离工作站。

图 14. Analysis（分析）> Intrusions（入侵）> Events（事件）



14. 选择 **Analysis（分析）> Correlation（相关）> Correlation Events（相关事件）**。这会显示此文件被识别为恶意文件。触发入侵后，相关性会告知 FireSIGHT 向 ISE 发出信号以隔离用户，并将此用户从网络断开连接。

图 15. 相关事件

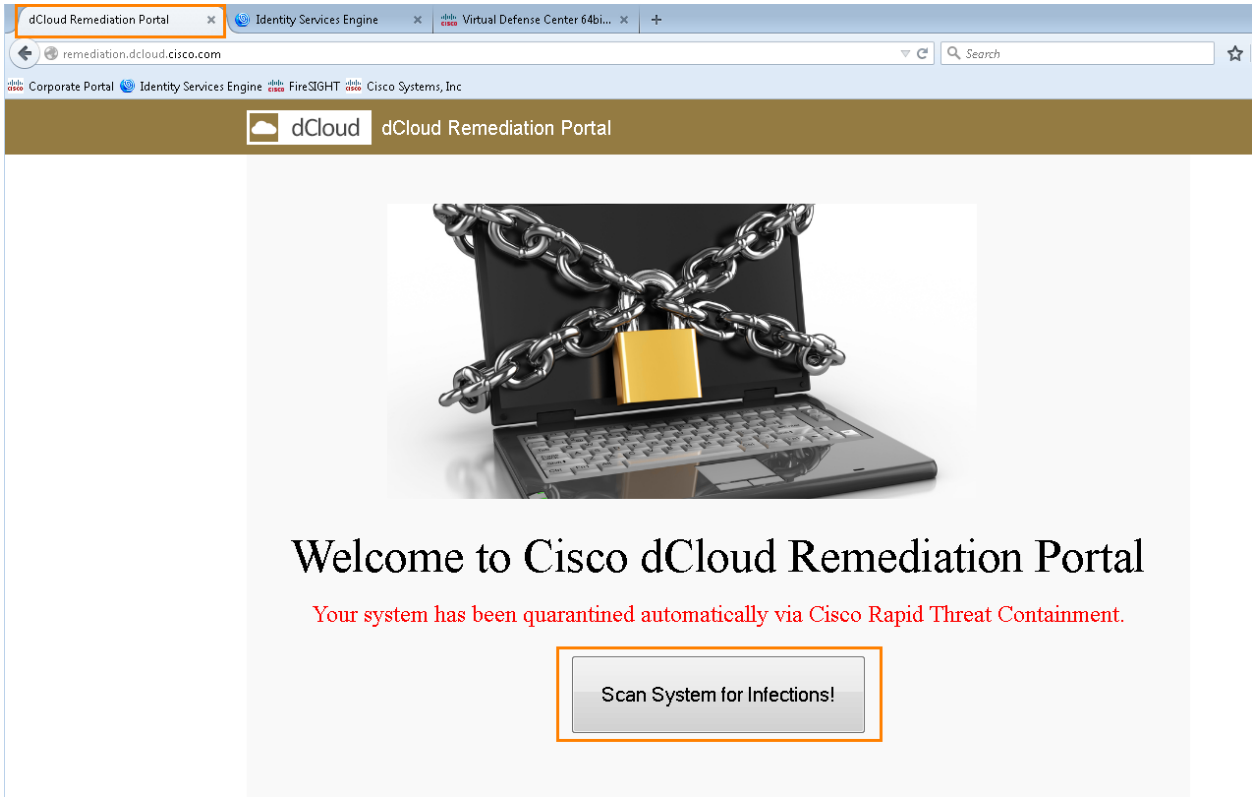


15. 向右滚动查看触发的规则。

图 16. 触发的规则

16. 返回 dCloud 补救门户，然后点击 **Scan System for Infections!（扫描系统是否被感染！）**。

图 17. 扫描系统是否被感染



17. 系统扫描以及断开和重新连接网络。

备注：正确扫描和清理系统后，则允许再次访问企业生产网络。当扫描结果显示为清洁时，对安全策略进行另一动态更改以允许用户再次访问网络。FireSIGHT 再次通过 pxGrid 向 ISE 发出采取行动的信号。在这种情况下，FireSIGHT 指示 ISE 取消隔离用户。因此，ISE 将另一授权更改 (CoA) 发送至网络接入设备。此外，更新分配用于此会话的安全组标记 (SGT)，允许员工访问。

备注：AnyConnect 偶尔不会自动重新连接。如果出现这种情况，请手动重新连接。

图 18. 系统扫描

18. 系统解决感染，并将您重定向至 dCloud 企业内联网门户。

图 19. 系统感染已解决

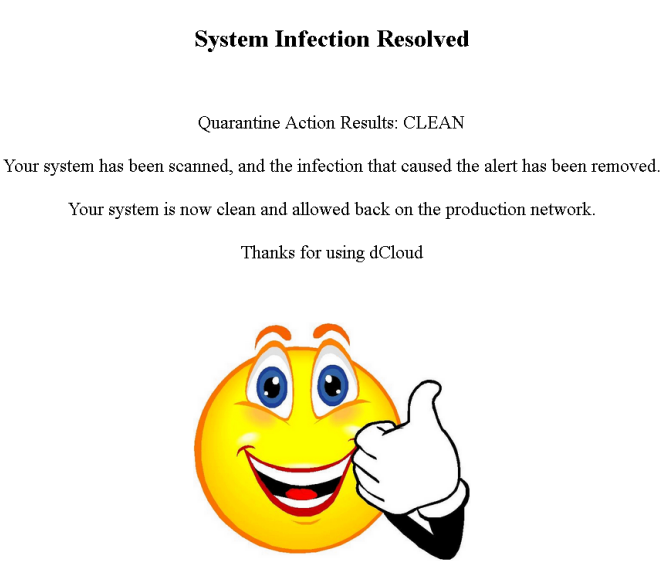
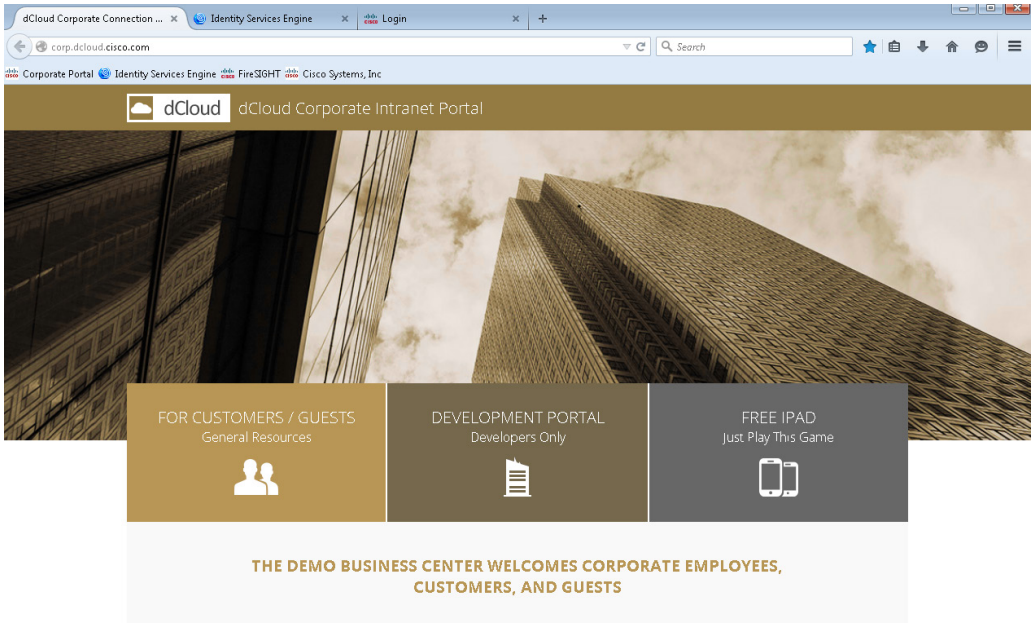
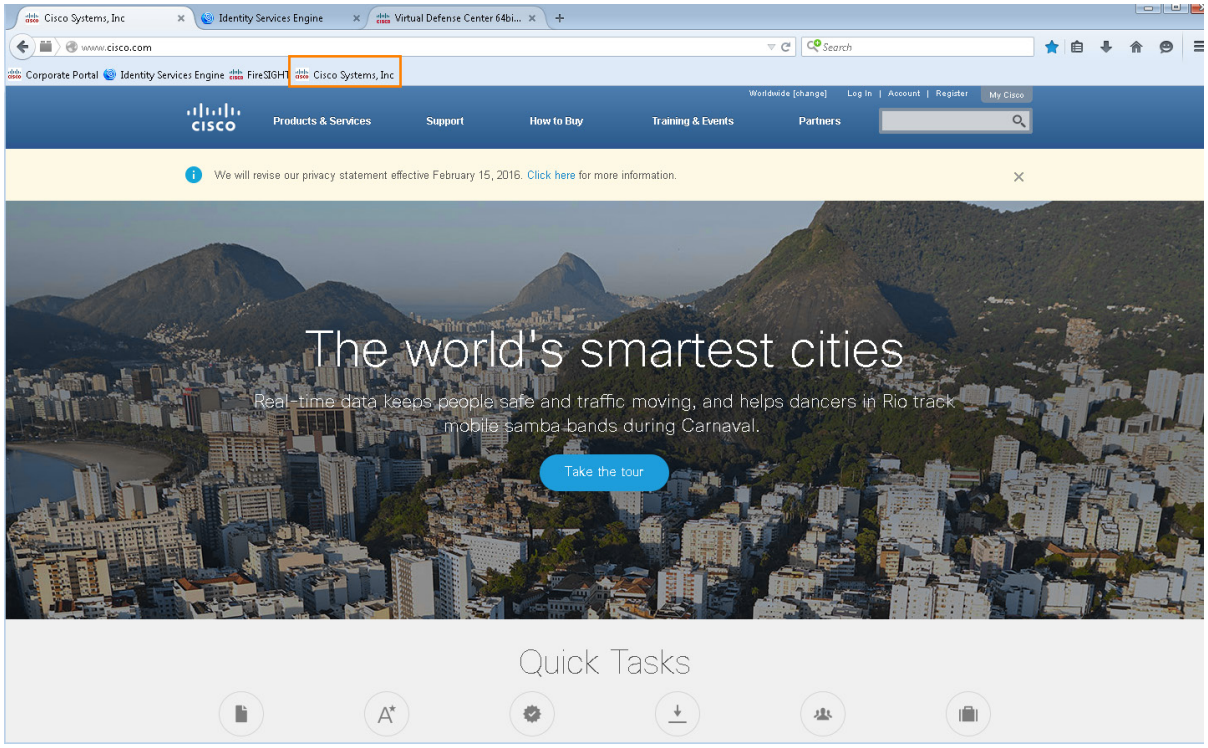


图 20. dCloud 企业内联网门户



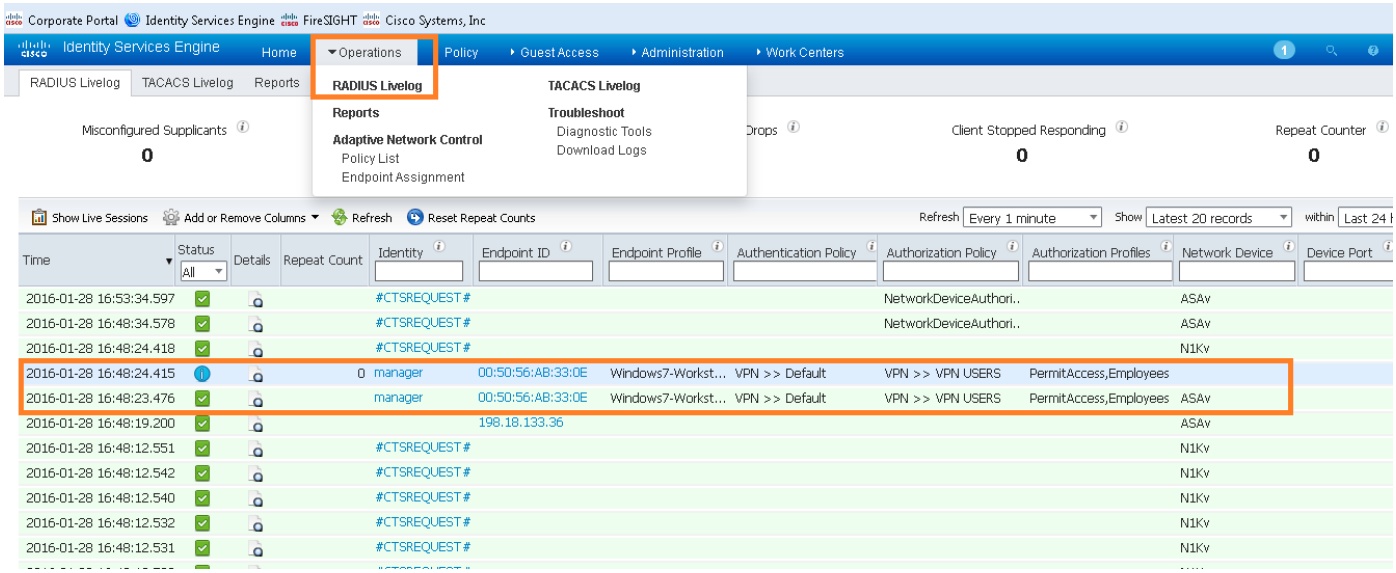
19. 选择 Cisco Systems Inc. 书签，显示目前已访问互联网。

图 21. Cisco Systems Inc.



20. 转至 **ISE** 选项卡，然后依次选择 **Operations（操作）> Radius Livelog**。系统将显示连接历史记录。指出已重新授予员工访问权限。

图 22. Operations（操作）> Radius Livelog



附录 A. 常见问题故障排除

问题

隔离或取消隔离过程中，断开了我与 AnyConnect 的连接，但不会自动重新连接。

解决方案：此故障偶发。只需点击 AnyConnect 中的连接按钮，即可手动重新连接网络。

从工作站注销后，我尝试再次作为经理登录，但在本演示的隔离和取消隔离部分遇到问题。

解决方案：AnyConnect 客户端存在异常，在某些情况下，身份验证过程中未将终端 MAC 地址正确发送至 ISE。在两种情况下，您可能会遇到此问题

- 您已登录工作站，但未完成所述场景。您已从工作站注销，并稍后重新登录以完成此场景
- 您已一次性成功地完成此场景。您已从工作站注销，并稍后重新登录以再次浏览流程。

这两种场景的最简单解决方案是实际上不从工作站注销。要从计算机断开连接，则使用 Windows 中的断开连接选项，方法为：点击“Start”（开始）按钮，然后选择“Disconnect”（断开连接）。

如果已从工作站注销，则从 Wkst 1 上的 Anyconnect 断开连接，并在尝试浏览流程前手动重新连接。这会使得 MAC 地址被正确发送至 ISE。

解决此问题的另一种方法是使用以下步骤强制将 Wkst 1 从 ASA 断开：

1. 使用 admin/C1sco12345 的用户 ID/密码组合登录位于 198.18.133.254 的 ASA。
2. 输入启用模式 (C1sco12345) 。
3. 发出命令 ***vpn-session logoff all***，然后按 **Enter** 键。
4. 确认您是否想要断开所有 VPN 用户的连接。

工作站 1 将会立即断开，并尝试自动重新连接网络。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。