思科安全防火墙/防火墙管理中心/自适应安全设备指南 — 紧急情况下不信任根证书颁发机构和中间证书颁发机构

目录

目的

下面是有关思科安全防火墙威胁防御(FTD)、思科安全防火墙管理中心(FMC)和自适应安全设备(ASA)的指南，用于应对穆德拉根和中间证书颁发机构的紧急不信任。

FMC本地思科服务证书捆绑包更新

FMC和FTD可以自动更新用于从设备到思科服务的TLS连接的本地CA捆绑包，包括智能许可和软件、VDB、SRU和地理位置更新。系统在系统定义的时间每天进行检查。从FMC/FTD 7.0.5、7.1.0.3、7.2.4和7.3.0+开始提供思科文档功能。这些是功能阈值，不是推荐的升级目标；使用确切的平台、源版本、兼容性要求和当前思科版本指南选择升级目标。[3、4]

在支持的FMC或FTD CLI上，`show cert-update`报告自动更新状态、每日时间表和捆绑的上次修改时间。`configure cert-update test`将检查本地捆绑包是否最新以及更新连接是否准备就绪。[4、5 和 6]

此思科服务捆绑包与FTD配置的可信CA对象/组（用于SSL解密）以及设备信任点（用于身份或VPN证书）分开。您将需要验证这些证书是否均未手动添加到配置中。[5、6]

ASA CA trustpool automatic import

在ASA上，CA信任池和命名信任点是独立的证书管理功能。信任池保存CA证书；信任点是用于证书身份和CA注册的命名配置。ASA trustpool auto-import也独立于上述FMC/FTD思科服务捆绑更新。[8、9]

对于只读检查，请运行`show crypto ca trustpool policy`以查看trustpool证书计数、导入状态和结果、下一次计划尝试以及有效策略详细信息。运行`show run crypto ca trustpool policy`以查看配置的信任池策略行。默认情况下，Cisco文档自动导入为关闭。如果未覆盖启用，记录的计划是每24小时22:00尝试一次，并且使用默认思科URL;配置的时间或URL可以更改这些值。检查实际的ASA输

出，而不是假设已启用自动导入或使用默认计划。[8、9]

这些检查显示策略和导入状态；它们不提供逐个证书的资产，也不确定任何已命名的Mudhra证书已安装、删除或不信任。不要从FMC/FTD `cert-update`推断ASA行为，并且不要将信任池状态视为有关在特定信任点或其他应用信任存储下配置的证书的证据。在决定是否需要任何产品特定操作之前，请确认确切的ASA版本和证书相关服务。[8、9]

使用FTD保护未打补丁设备的潜在解决方法

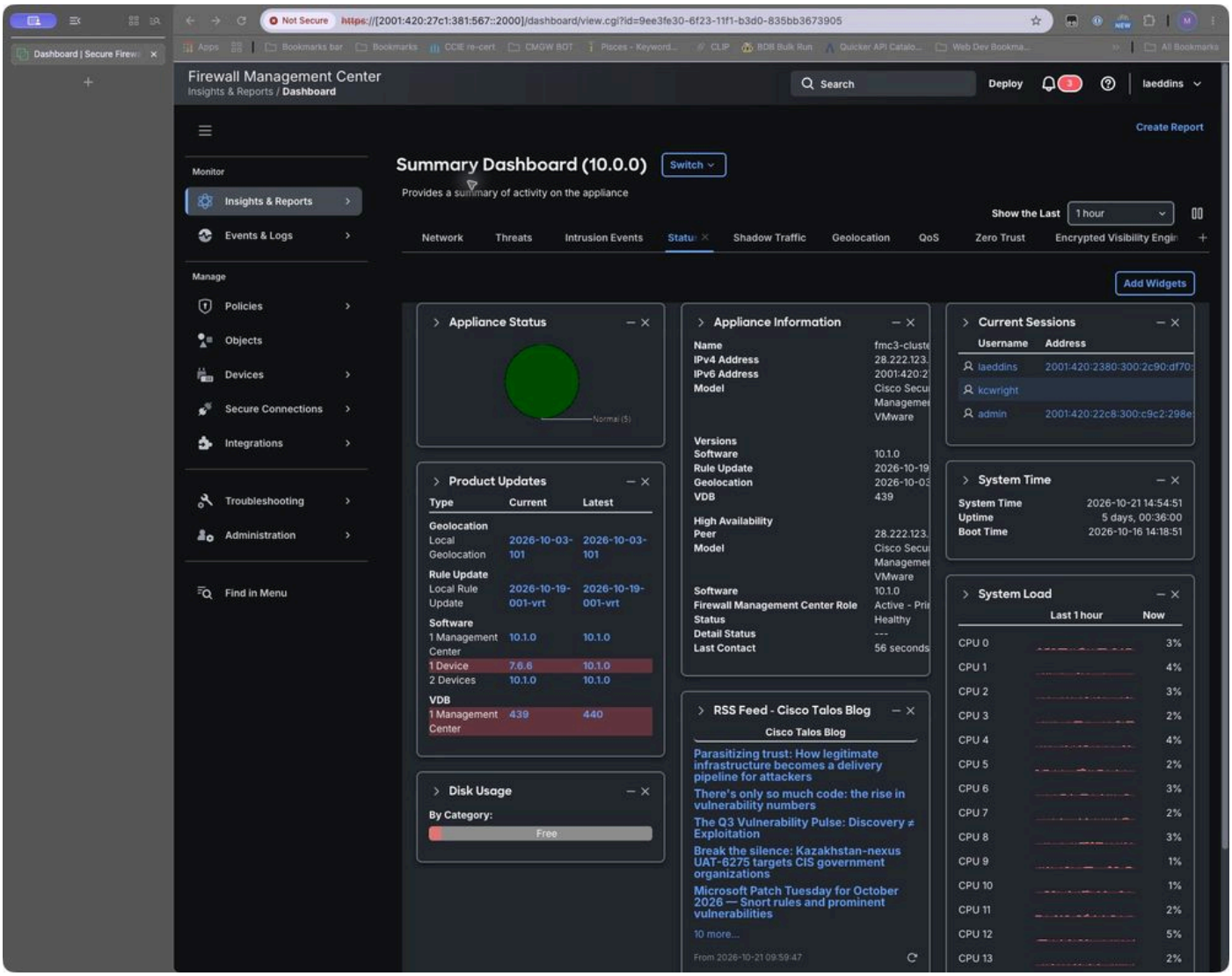
目的

使用Cisco安全防火墙管理中心(FMC)配置TLS策略规则，以阻止具有已知受影响的Mudhra颁发者名称的服务器证书。此控制可降低无外设客户端和服务器的风险，这些客户端和服务器的应用信任库尚未收到所需的更新，但它不会在所有情况下阻止连接。 继续信任存储补救和证书替换。请勿将受感染的CA导入此过程的受信任CA。

先决条件

本文中的配置屏幕是在FMC 10.1.0上捕获的。控制面板列出了10.0.0上的两个受管设备和7.6.6上的一个受管设备。未执行流量测试。在实施验证之前，请记录目标FTD版本、Snort引擎、实施模式、访问控制策略和TLS策略。确认受影响的出站流量达到预期策略。

图1. FMC 10.1.0和受管设备软件清单。



配置颁发者匹配

思科记录颁发者DN条件，以匹配颁发服务器证书的CA。在规则编辑器中添加DN对象并添加到颁发者。可用导航和标签取决于版本。[1、2]

1创建对象

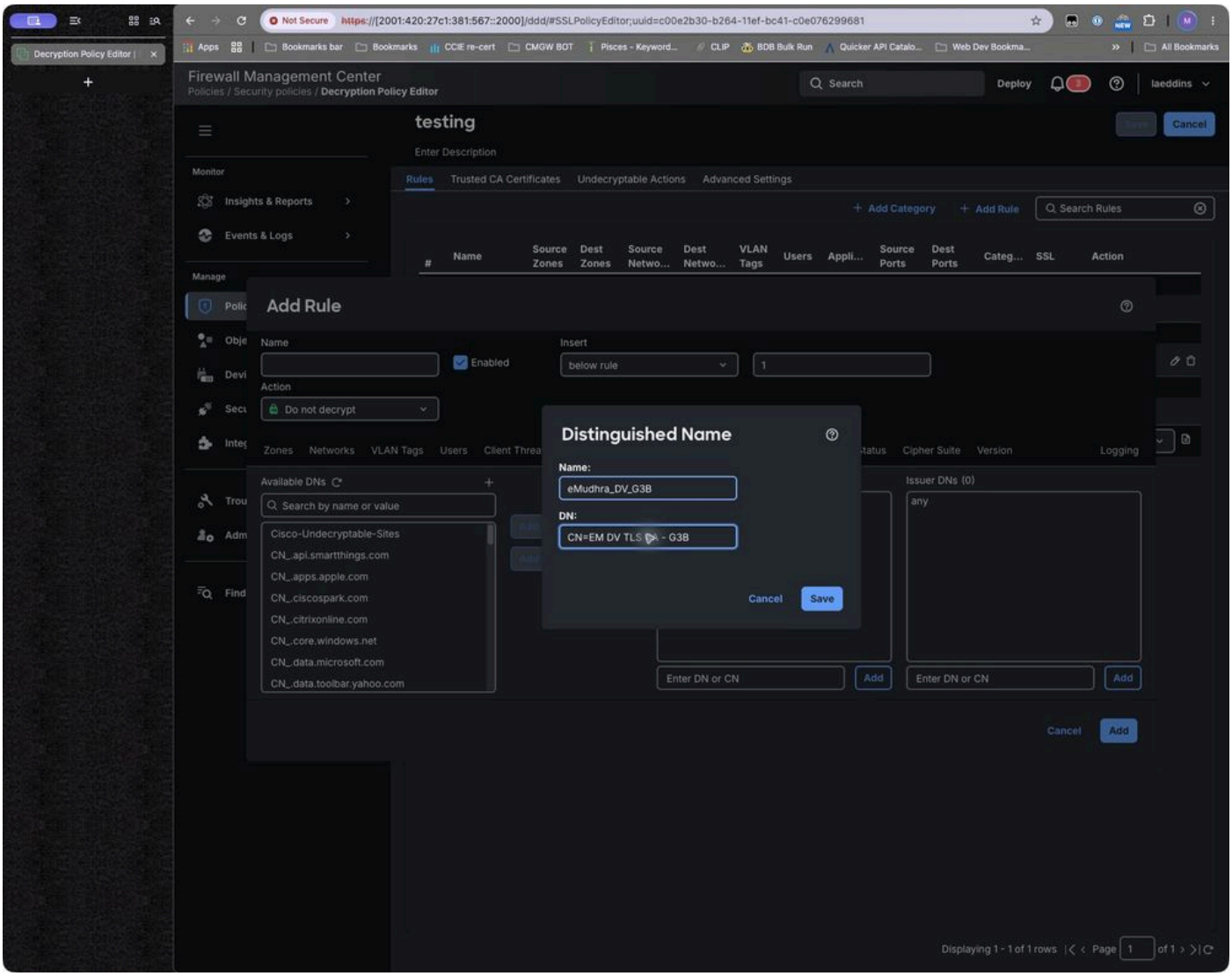
对象表

DN	建议的DN对象名称
CN=EM DV TLS CA - G3B	eMudhra_DV_G3B

DN	建议的DN对象名称
CN=EM DV TLS CA - G3C	eMudhra_DV_G3C
CN=EM EV TLS CA - G3B	eMudhra_EV_G3B
CN=EM EV TLS CA - G3C	eMudhra_EV_G3C
CN=EM OVER TLS CA - G3B	eMudhra_OV_G3B
CN=EM OVER TLS CA - G3C	eMudhra_OV_G3C

为上表中的每个对象创建一个缩小范围的DN对象。

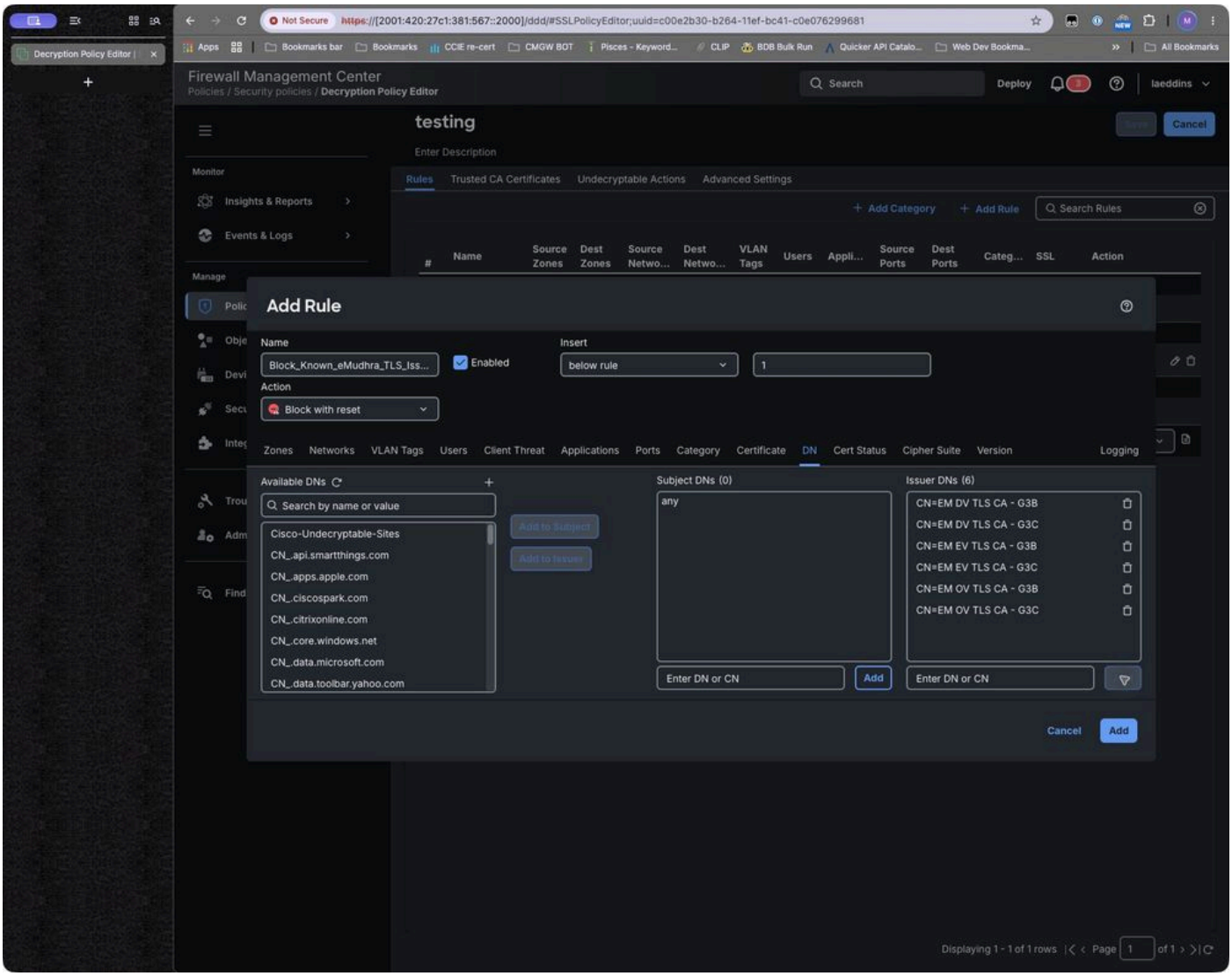
图2.显示“名称”和“DN”字段的“可分辨名称”表单。输入示例值进行说明；完成后点击Save。



2创建阻止规则

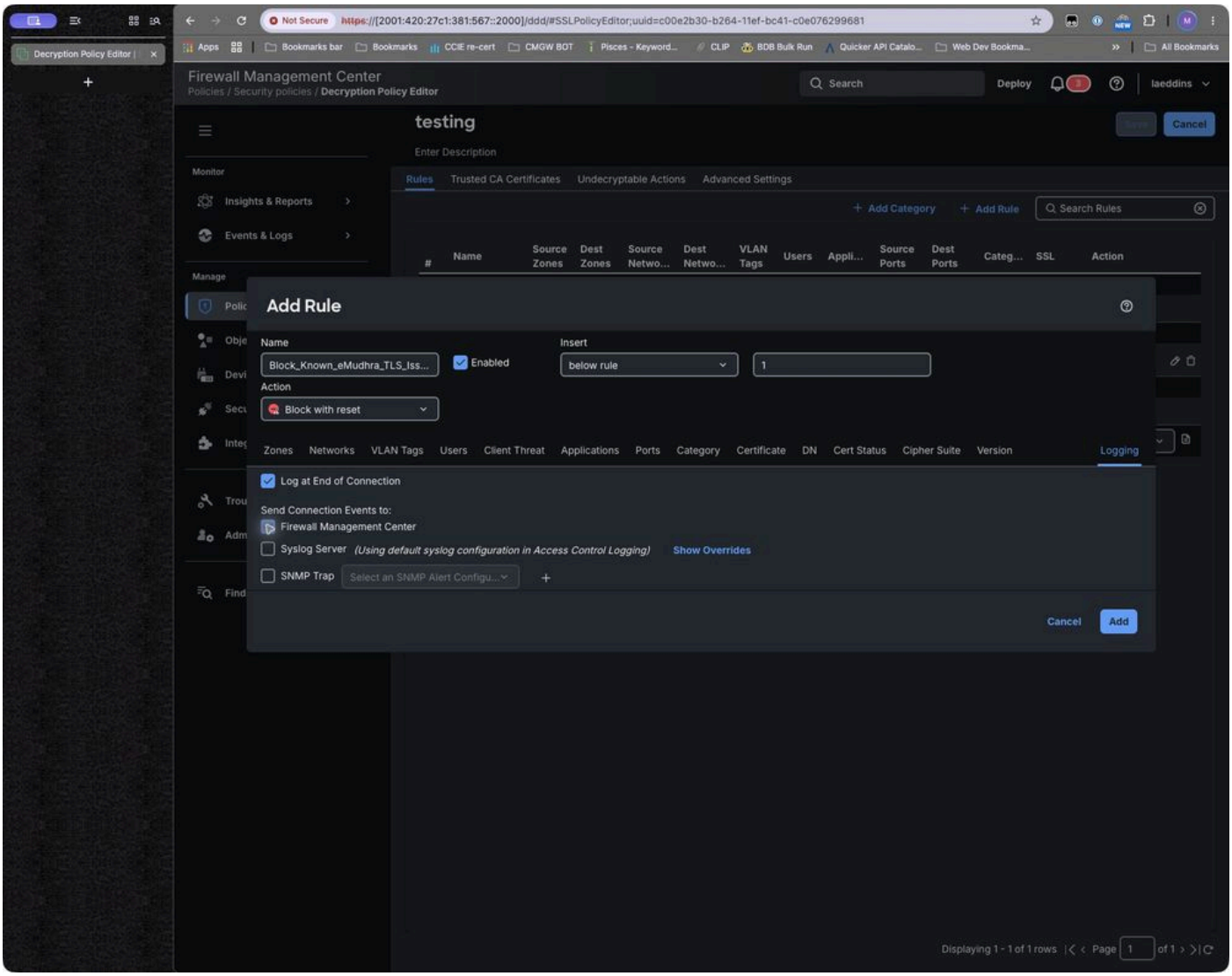
在FMC 10.1.0中，选择Policies > Security policies > Decryption，打开适用的策略，然后点击Add Rule。将规则命名为Block_Known_Mudhra_TLS_Issuers。打开DN选项卡。使用Add to Issuer添加验证对象，或在标记为Enter DN or CN的Issuer DNs字段中输入DN，然后点击Add按钮。确认名称显示在颁发者DN中，而不是主题DN中。

图3.显示阻止并重置、DN选项卡、六个颁发者DN和无主题DN限制的规则。完成后点击Add。



选择Block或Block with reset。将源区域或网络限制在约定的范围内。如果需要，在Logging选项卡上，选择Log at End of Connection，并验证已选择Firewall Management Center。请勿添加“有效=是”要求：目标颁发者块不得依赖于通过信任验证的证书。

图4.显示已选择“Log at End of Connection”和“Firewall Management Center”的规则。完成后点击Add



3检查规则顺序和策略关联

将规则置于可先处理相同流量的更广泛规则之前。确认TLS策略与分配给目标设备的访问控制策略的关联。在测试之前检查预过滤器和其他旁路路径。

图5.现有测试策略规则表。此处仅显示订购界面。

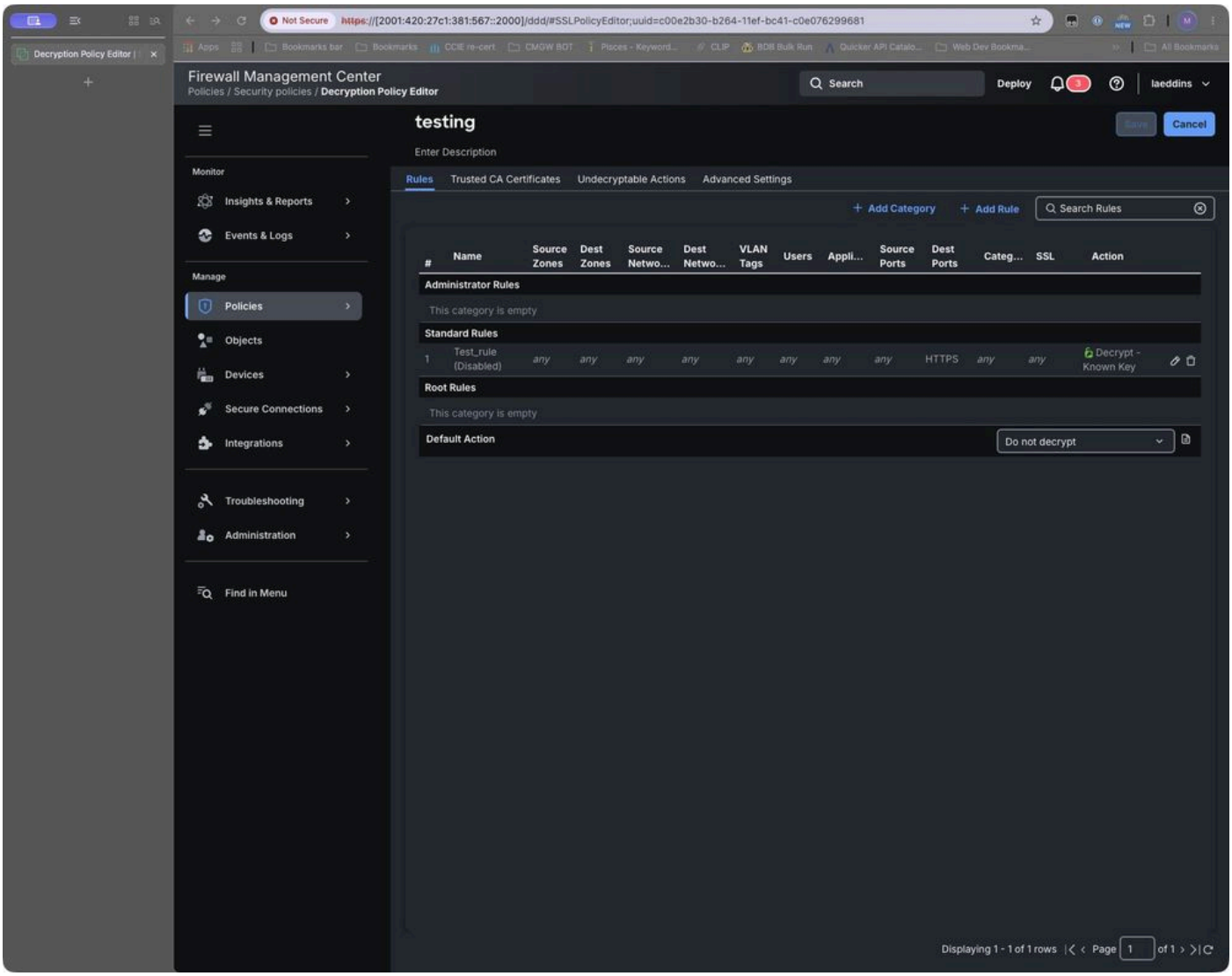
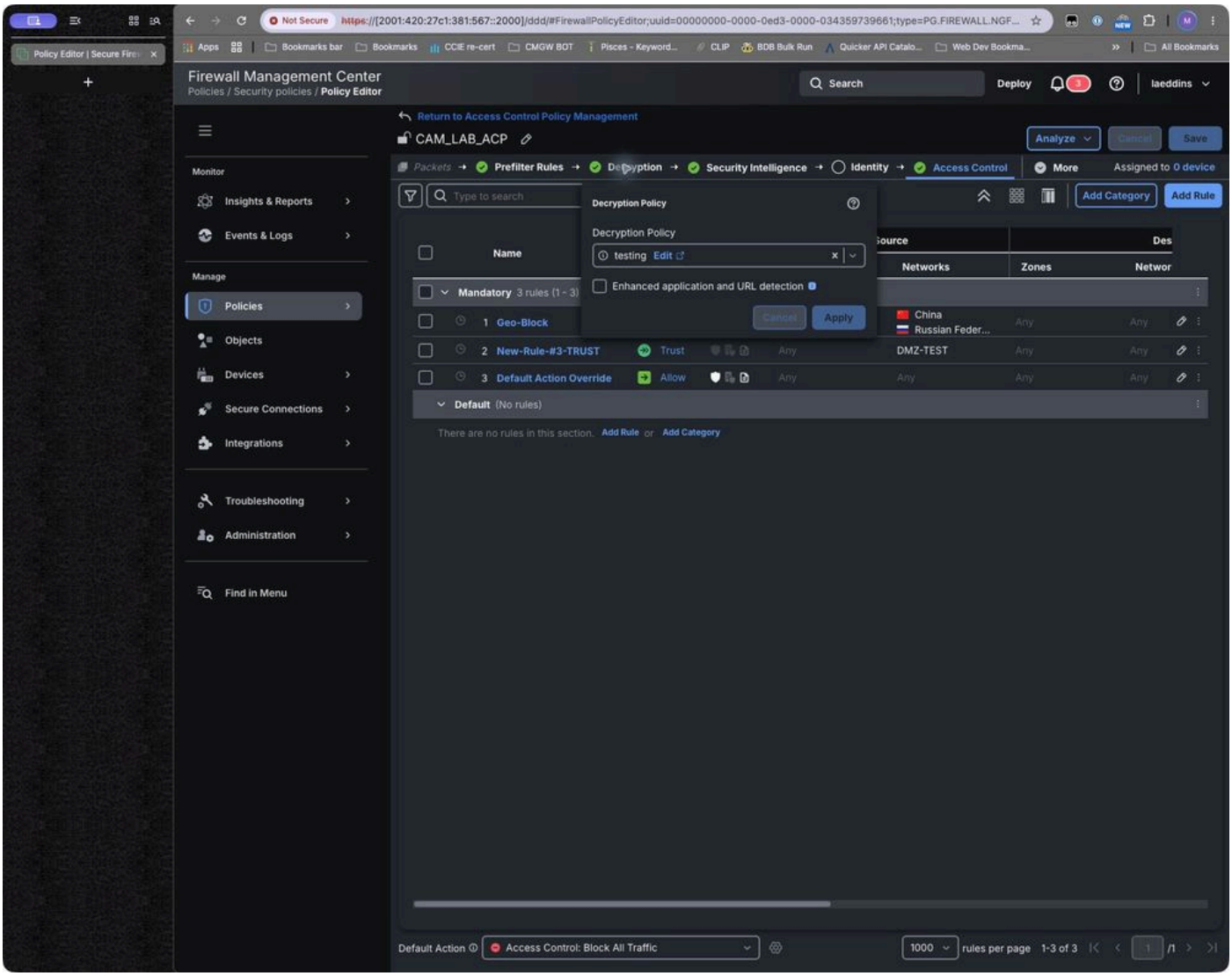


图 5b.现有CAM_LAB_ACP策略引用测试解密策略。



部署和验证

将更改部署到有问题的设备。如果可用，请使用您知道正在使用有问题的CA之一颁发的证书的网站进行测试。

排除意外结果故障

如果流量通过，请检查部署状态、流量范围、策略关联、规则顺序、颁发者拼写和字段编码，以及设备是否具有证书信息。确定其他规则或旁路路径是否处理了流。在申请同等覆盖范围之前，请查看测试版本的TLS 1.3可见性。

其他TLS 1.3验证：在FMC 7.6上，TLS 1.3解密是单独的解密策略高级设置；如果禁用该功能，则解密规则仅适用于TLS 1.2或更低版本。启用TLS 1.3解密启用自适应服务器身份探测，并且颁发者DN条件可以在证书未缓存时触发探测。相关访问控制策略的TLS 1.3服务器身份发现设置优先。思

科表示，这些高级设置在7.1之前或运行Snort 2的设备上会被忽略，并且部署到AWS的FTDv不支持自适应身份发现。在申请TLS 1.3覆盖范围之前验证目标软件/平台和证书可视性。规则的TLS版本选择器本身列出了SSL 3.0到TLS 1.2;不要依赖该选择器进行TLS 1.3。[7]

如果不相关的流量发生故障，请确定实际的匹配规则和颁发者。根据需要缩小DN或流量范围，然后重复受影响和未受影响的测试。请勿禁用证书验证作为解决方法。

覆盖范围和操作限制

此解决方案不会阻止每个场景，也不会取代更新其他服务的需要。

回滚和规则报废

如果规则导致不可接受的影响，请通过正常的更改流程禁用新规则并重新部署。保存事件并测试证据。在停用之前，请确认受影响的工作负载强制执行当前信任策略，重复否定证书验证测试，并获得更改所有者的批准以删除临时限制。

参考

[1] FMC 7.2解密规则

[2] FMC 10.x基于规则的解密规则

[3]安全防火墙管理中心新功能（按版本）

[4]为FMC和FDM配置自动更新CA包

[5] FMC 7.6证书

[6] FDM 7.6证书

[7] FMC 7.6解密策略和TLS 1.3指南

[8] Cisco Secure Firewall ASA 9.22常规操作CLI配置指南 — 数字证书

[9] Cisco Secure Firewall ASA Series Command Reference — crypto ca trustpool policy

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）。