**基于Citrix ADC Gateway Smart Access功能**

**实现Citrix远程桌面&应用的用户访问控制**

Citrix ADC是一款7层性能强大的应用交付产品，对于自家的明星产品Citrix CVAD更是拥有独特的Gateway功能提供了软硬结合的桌面云整体解决方案。

Citrix Gateway使用户能够利用任何设备，在任何地点任何时间通过单一URL安全地访问后端需要的应用及桌面。Citrix Gateway自带丰富的用户身份及管理功能，如：单点登录，多因素认证，联合身份认证，OTP等。除此之外还可以和CVAD通过集成的方式提供更加灵活的用户接入管理。

在此介绍Citrix Gateway独特的Smart Access功能，通过在DDC中调用Gateway上设置的访问策略来灵活设定不同桌面和应用交付组对终端用户的接入权限。

Smart Access的工作原理如下：

1. 当用户通过Web 浏览器访问虚拟服务器的 Web 地址时，您配置的任何预身份验证策略都会首先下载到用户设备。
2. Citrix Gateway 将预身份验证和会话策略名称作为筛选器发送到 Web Interface。如果策略条件设置为 true，则始终以筛选器名称发送策略。如果未满足策略条件，则不会发送筛选器名称。这样，您就可以根据端点分析的结果区分已发布的应用程序和桌面列表以及运行 Citrix Virtual Apps and Desktops 的计算机上的有效策略。
3. Web Interface 与 Citrix Virtual Apps and Desktops 服务器联系，并将已发布的资源列表返回给用户。除非满足筛选条件，否则应用过滤器的任何资源都不会显示在用户列表中。

详细通讯流程请参考KB：<https://support.citrix.com/article/CTX227054 中2.3>节部分

下面以一个实际客户需求为例，介绍Smart Access的配置实现。

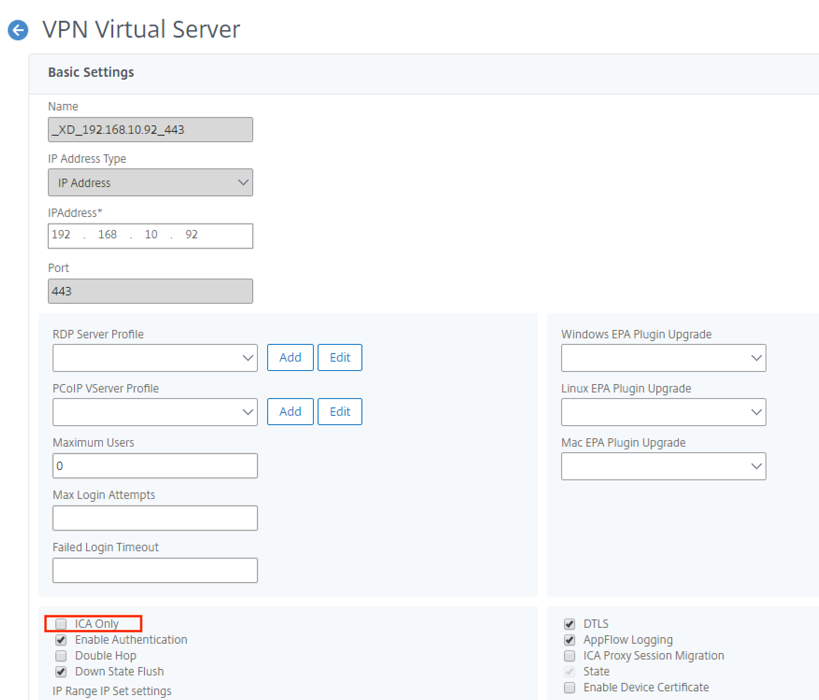
**客户需求**：针对DDC中不同交付组Delivery Group（DG），以DG为颗粒度设置访问用户ip地址白名单，只有ip地址在白名单网段内的用户可以获得桌面和应用资源清单，其他ip地址的用户无法获取。

**思路：**启用Smart Access功能，在Gateway上配置预身份验证策略，匹配客户端ip地址是否在白名单中，DDC针对特定DG开启Smart Access验证，为白名单中的用户展示资源清单，拒绝其他用户的资源访问。

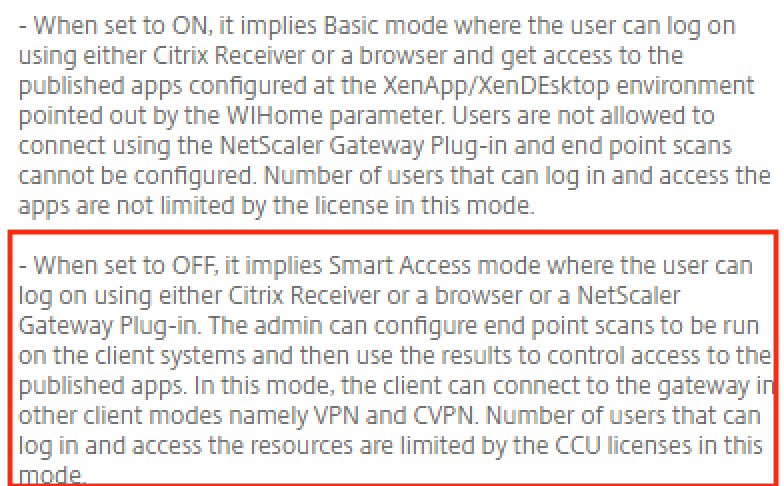
**配置：**

**前提** - Gateway Virtual Server正常配置，与StoreFront，DDC等完成集成，ADC有足够Gateway Universal License。

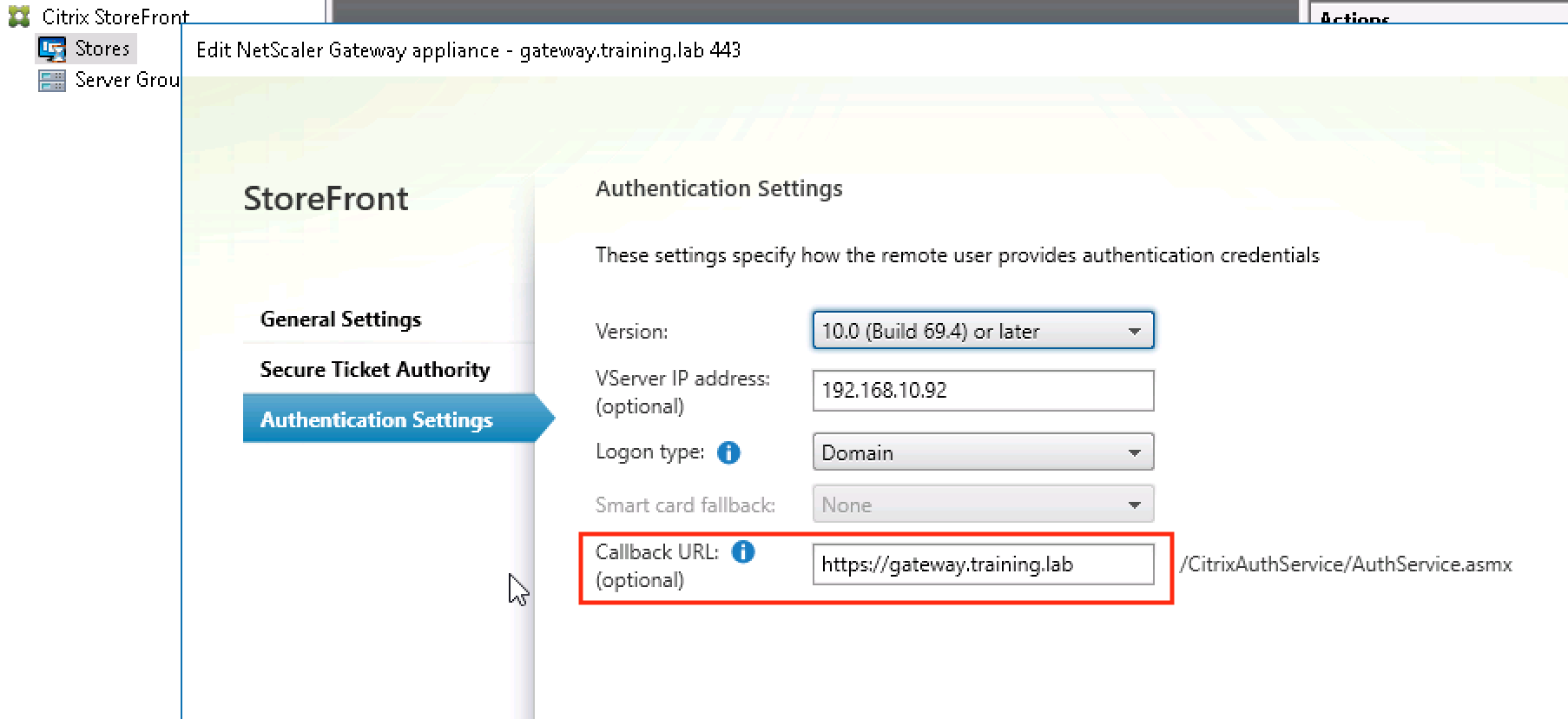
1. NetScaler Gateway/NetScaler Gateway Virtual Server编辑Gateway VS，在Basic Settings中点击more，确认“ICA Only”不被勾选（意味着该VS上开启Smart Access功能）



相关说明如下：



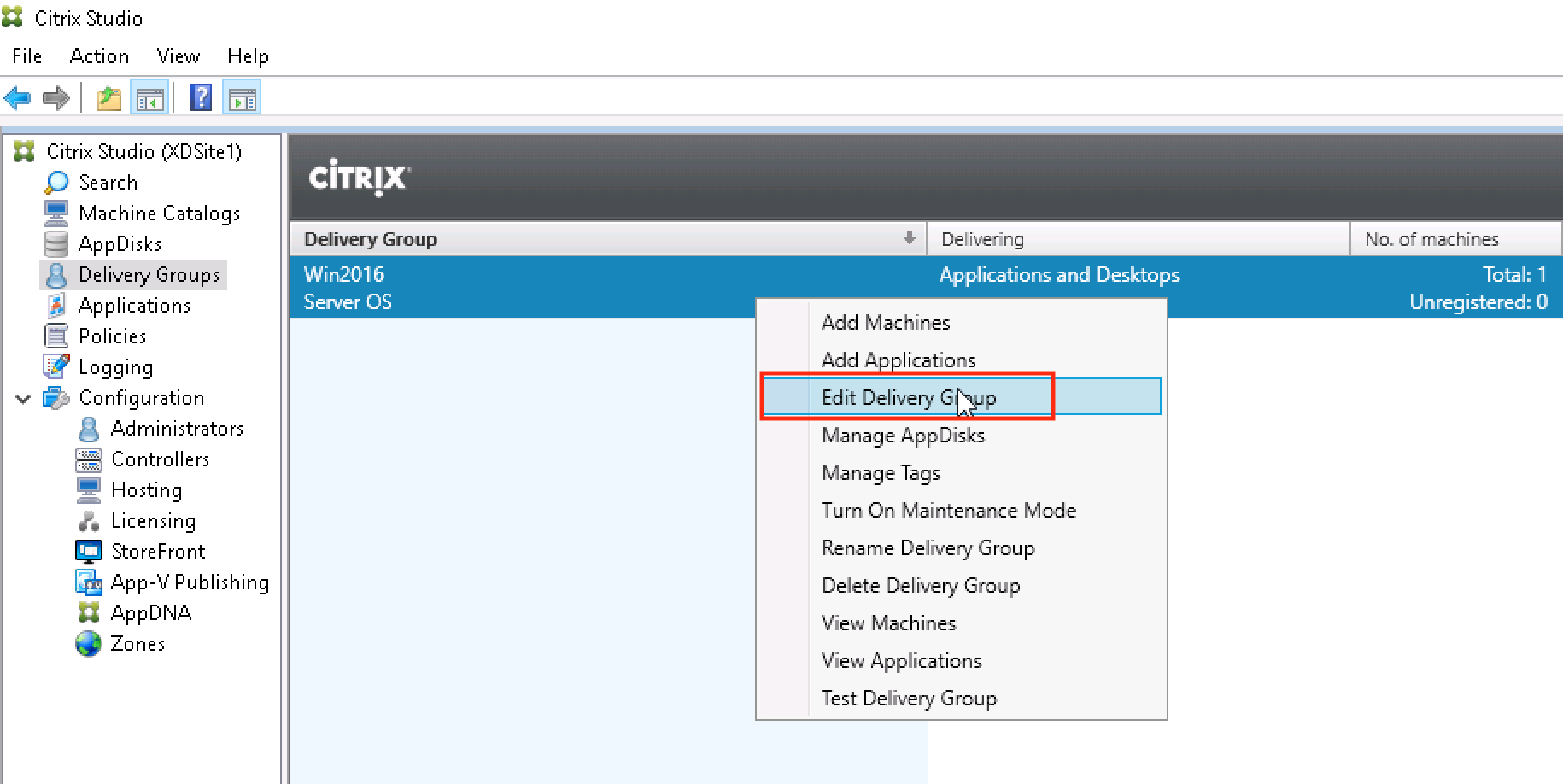
1. 登录StoreFront 在Stores中选择“Manage Netscaler Gateways”配置Callback URL。在Gateway与CVAD后端通信过程中，当StoreFront收到Gateway转发过来的用户信息后，StoreFront将会通过设置的Callback链接从Gateway获取更多的策略信息（VS的名称，关联的策略）。



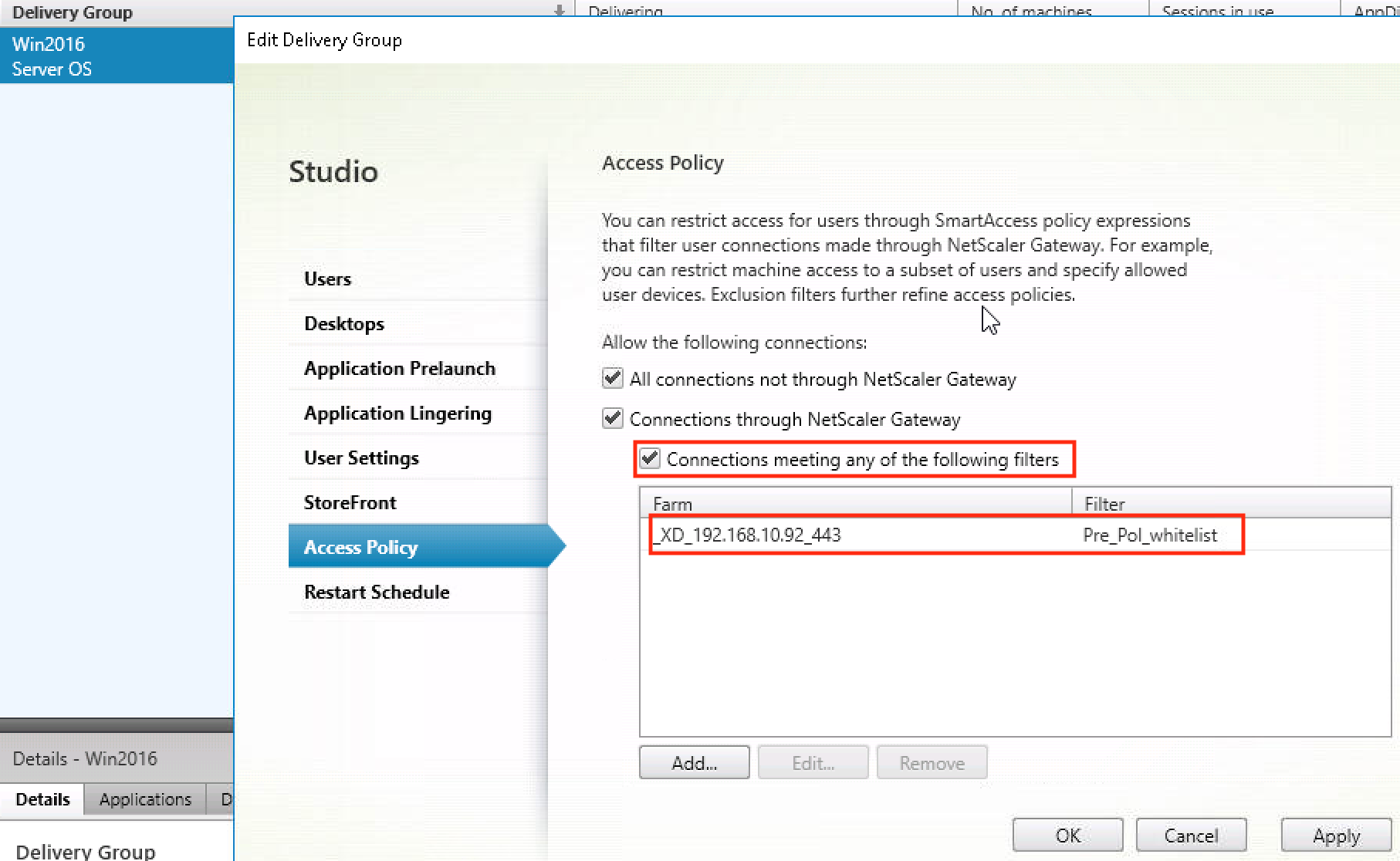
1. 登录DDC，DDC控制最终用户访问资源权限的生效。打开DDC上的Powershell，开启Trust XML



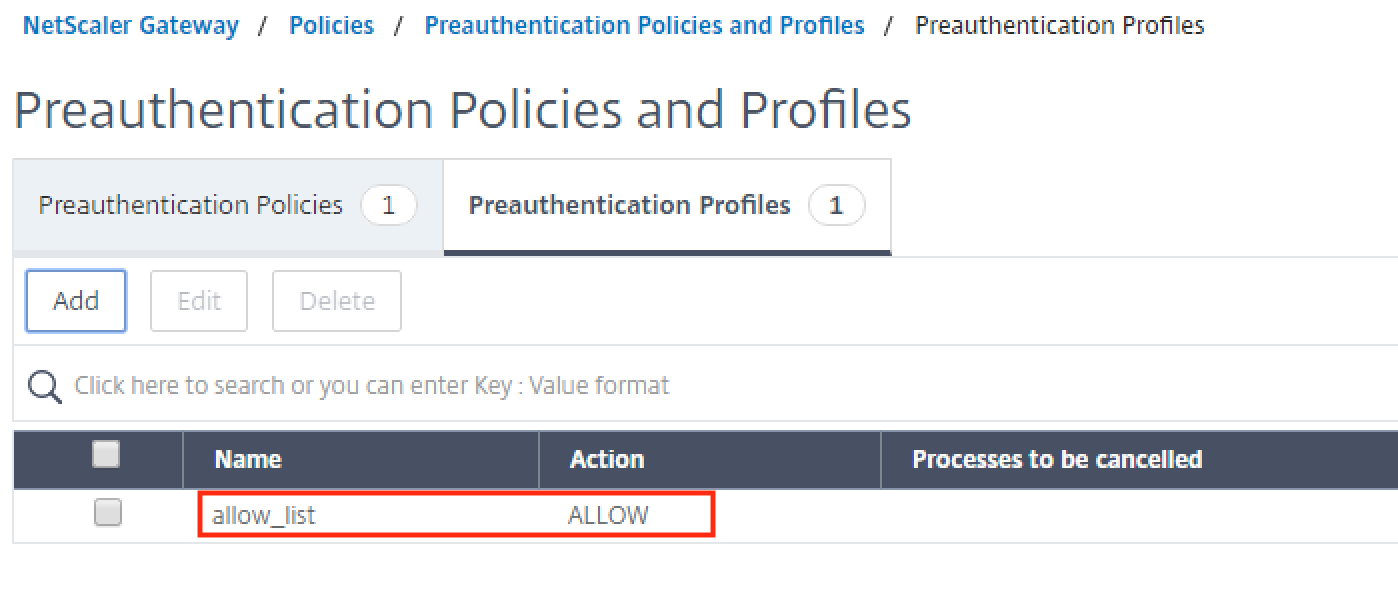
1. 选择需要启用Smart Access策略的Delivery Group（DG），右键点击“Edit Delivery Group”



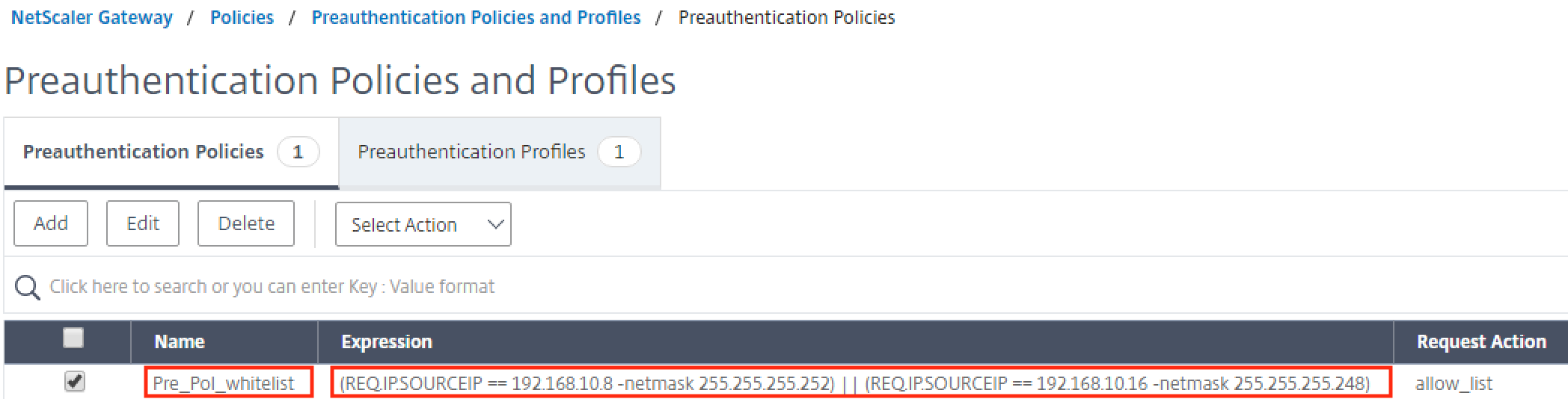
1. 在Access Policy中启用Smart Access，勾选”Connections through NetScaler Gateway”和”Connections meeting any of the following filters”，在Farm-Filter中点击Add，增加访问策略。其中，“Farm”对应值为Gateway VS名称，Filter为Gateway设置的策略名称（见下一步）



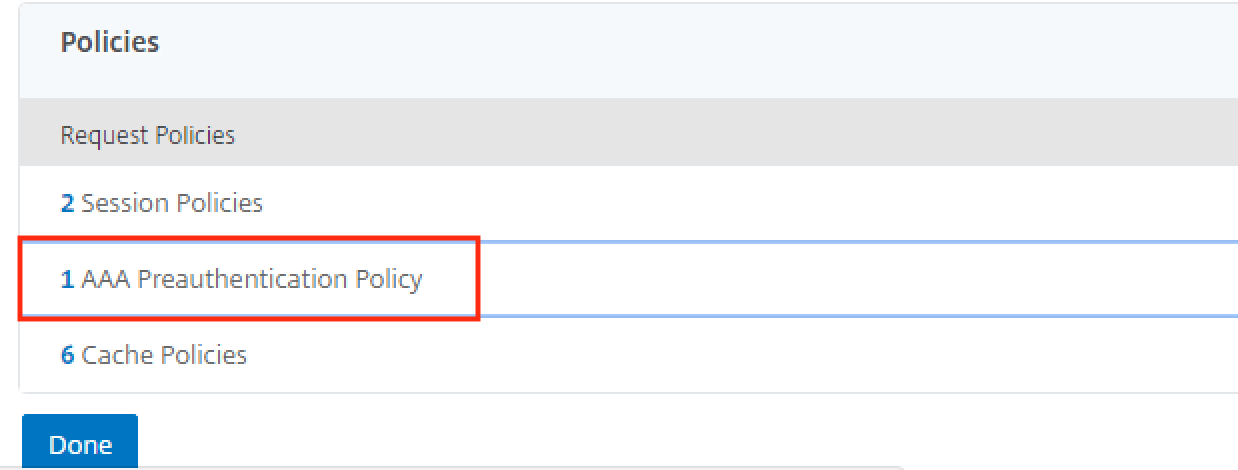
1. 配置Preauthentication策略，首先在NetScaler Gateway/Policies/Preauthentication Policies and Profiles/Preauthentication Profiles配置Action动作”allow\_list”，允许策略匹配特定用户终端

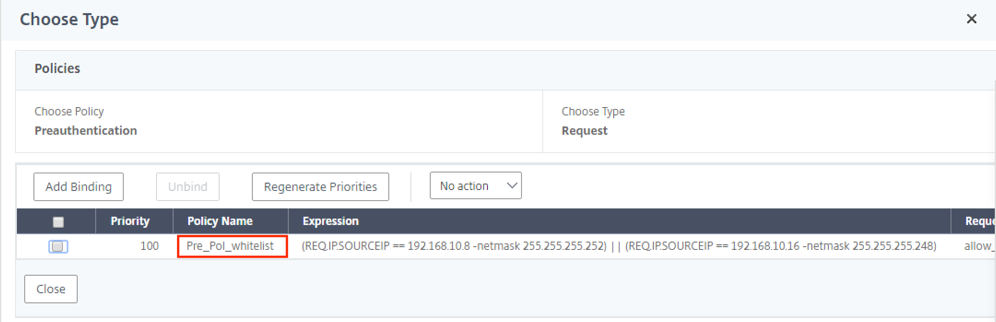
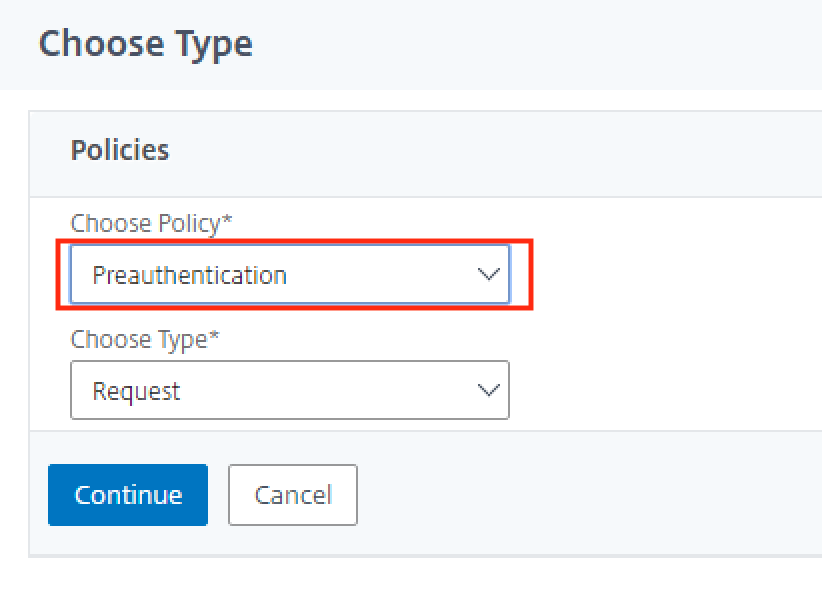


1. 之后在NetScaler Gateway/Policies/Preauthentication Policies and Profiles/Preauthentication Policies中设定匹配策略”Pre\_Pol\_whitelist”设定用户终端ip地址的白名单，Request Action为“allow\_list”具体表达式如下图（此处举例匹配了192.168.10/30和192.168.10.16/29网段，在这两个网段内用户ip可以获取CVAD资源，其他ip用户无法获取）：

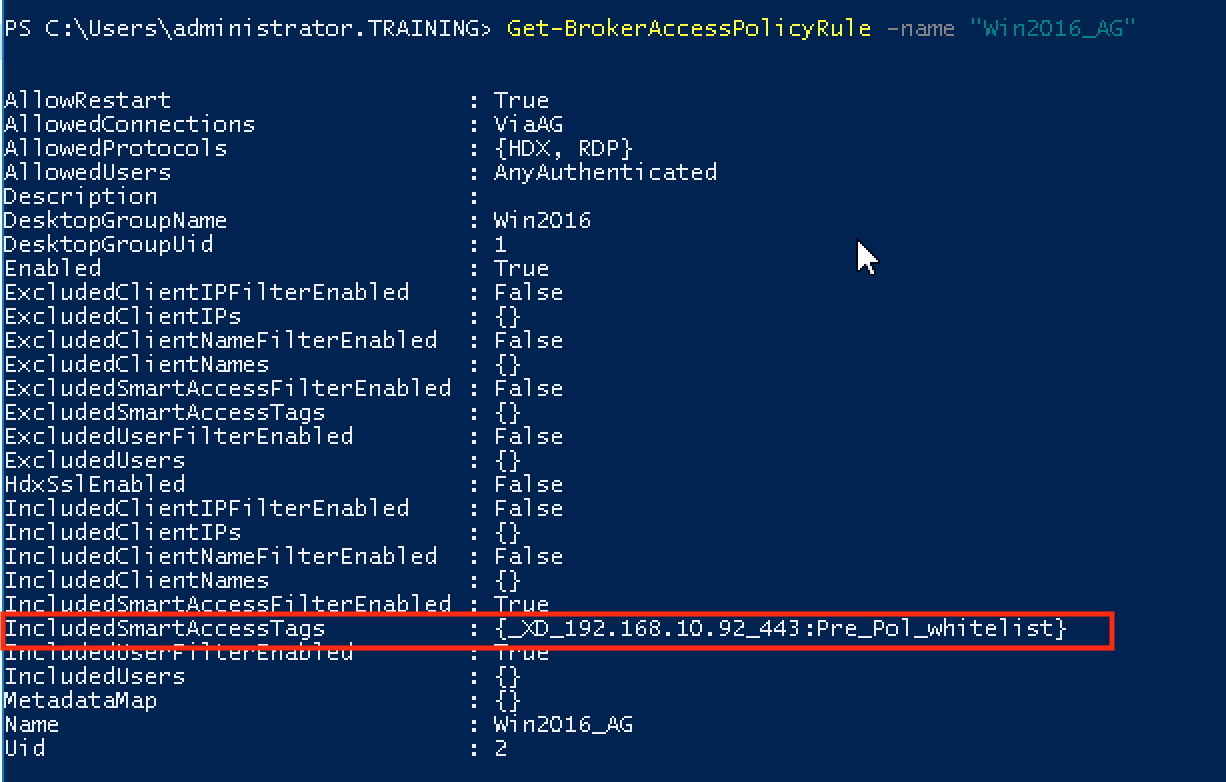


1. NetScaler Gateway/NetScaler Gateway Virtual Server将Preauthentication策略关联至VS。Policies添加Preauthentication Policy捆绑已建立的” Pre\_Pol\_whitelist”

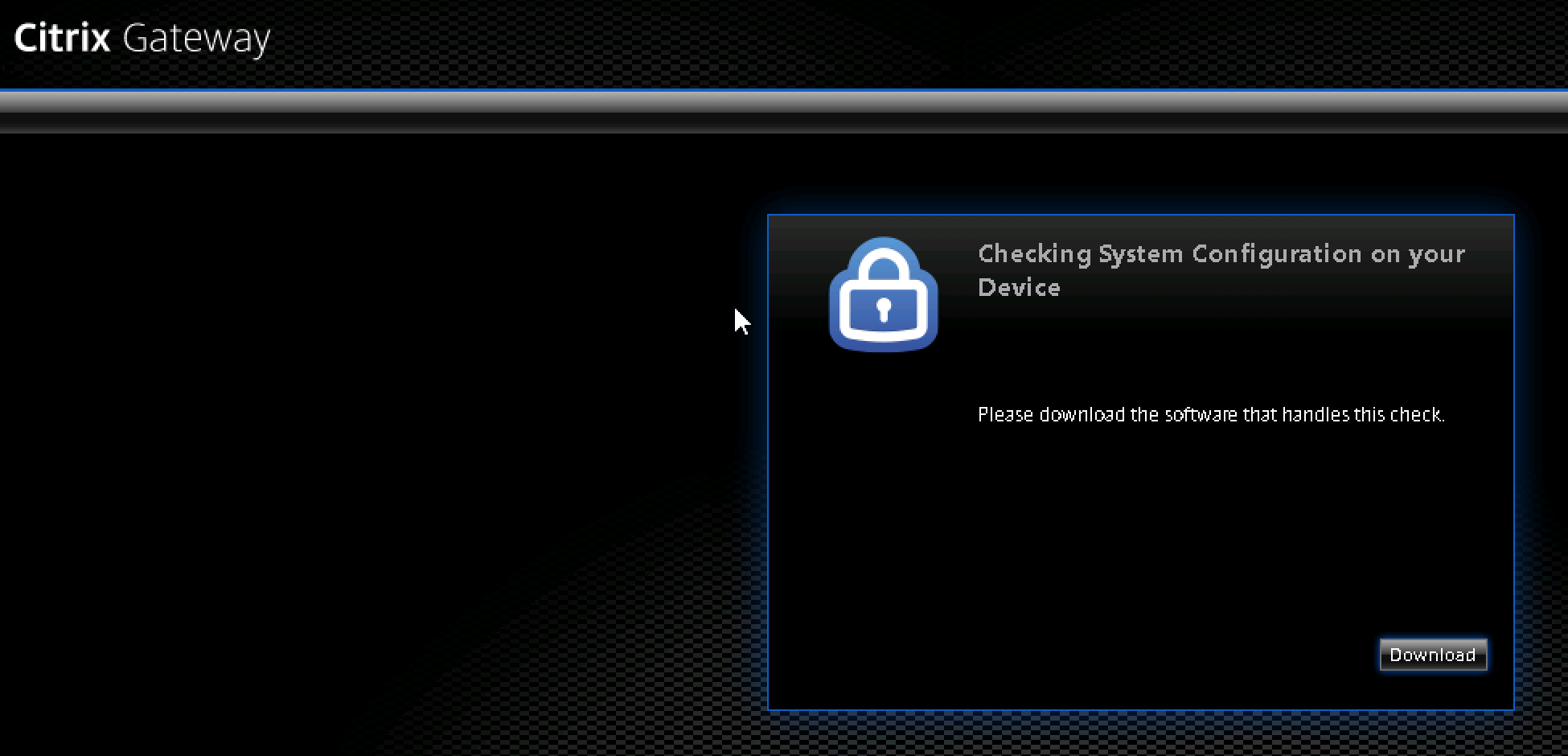


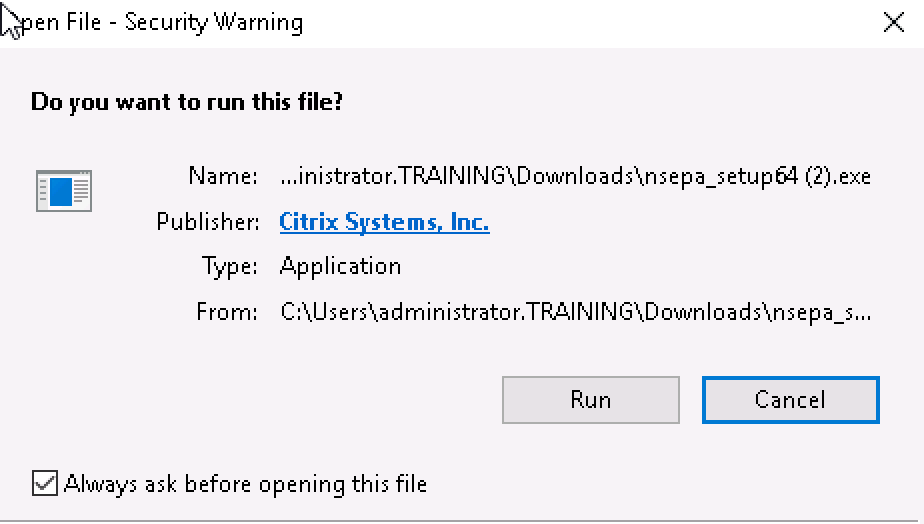


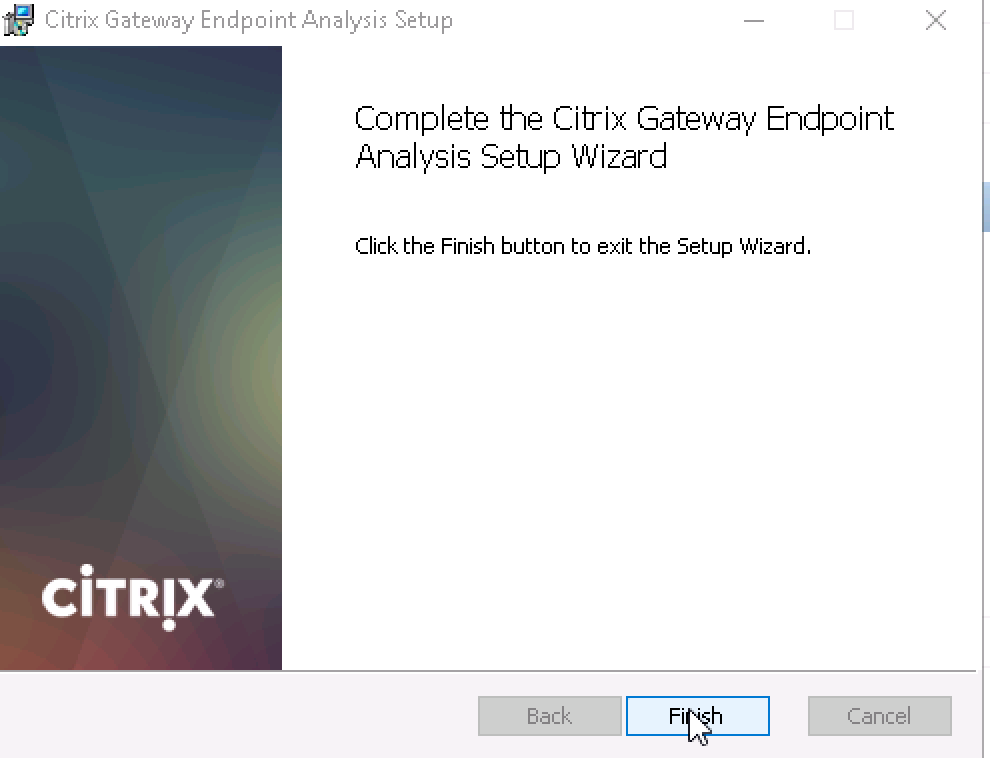
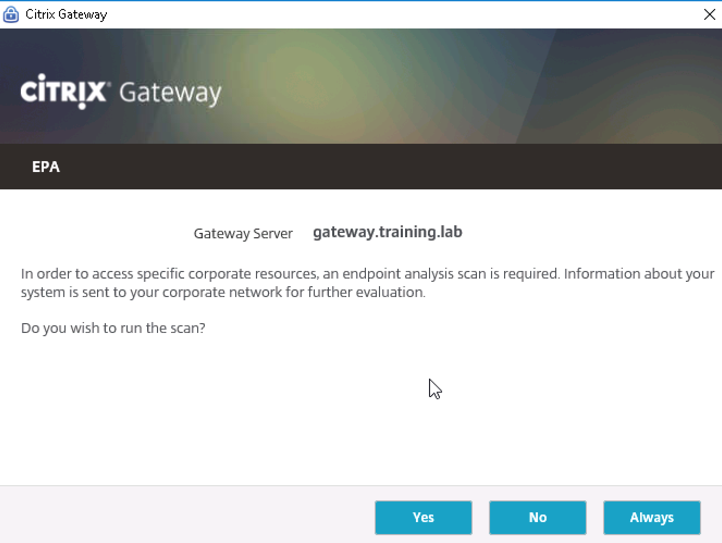
1. 返回DDC，在Powershell中输入如下命令确认策略绑定（IncludedSmartAccessTags中显示VS名称和Policy名称）



1. 验证
2. 首次用户登录Gateway需要下载插件EPA检验终端

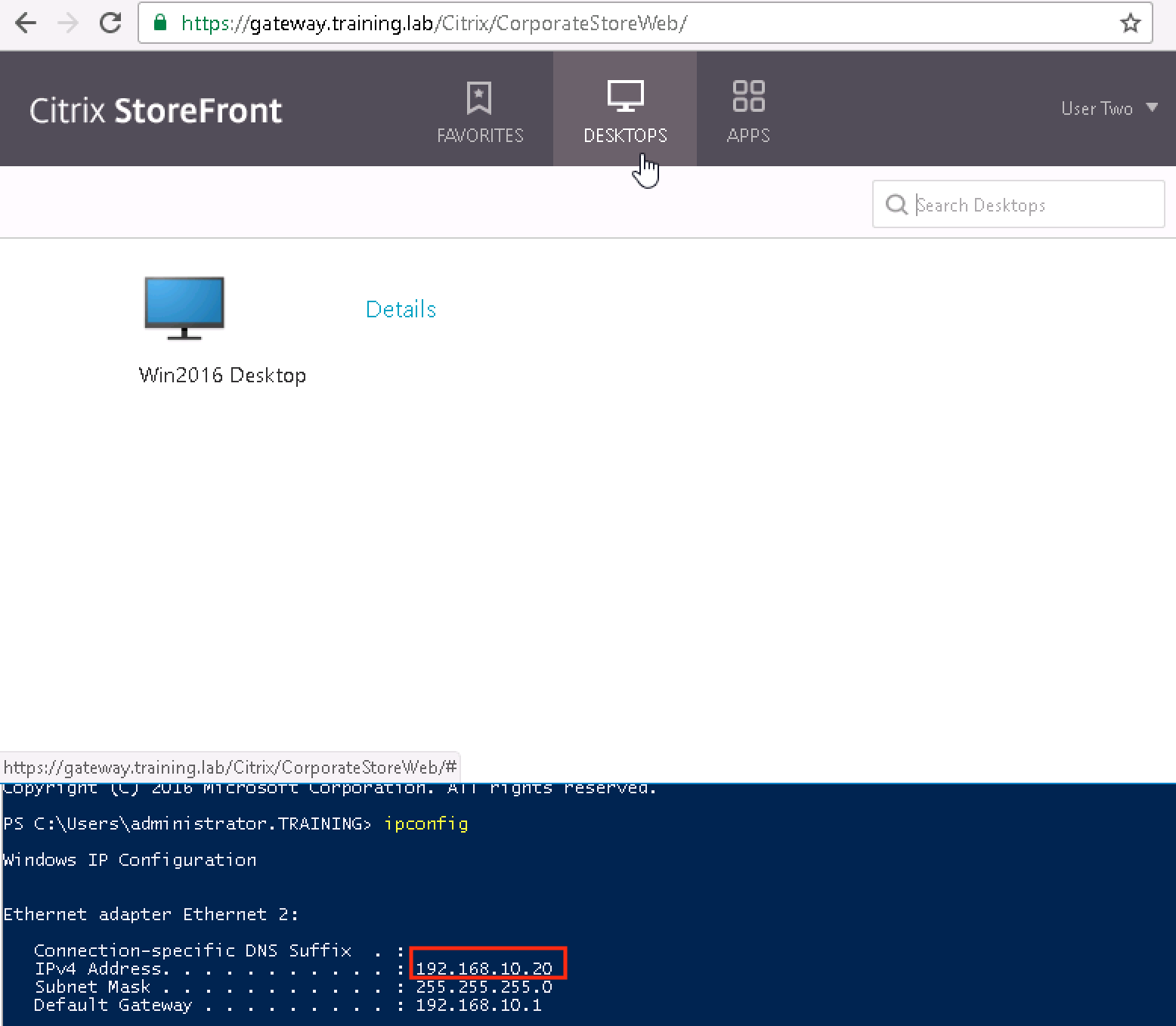
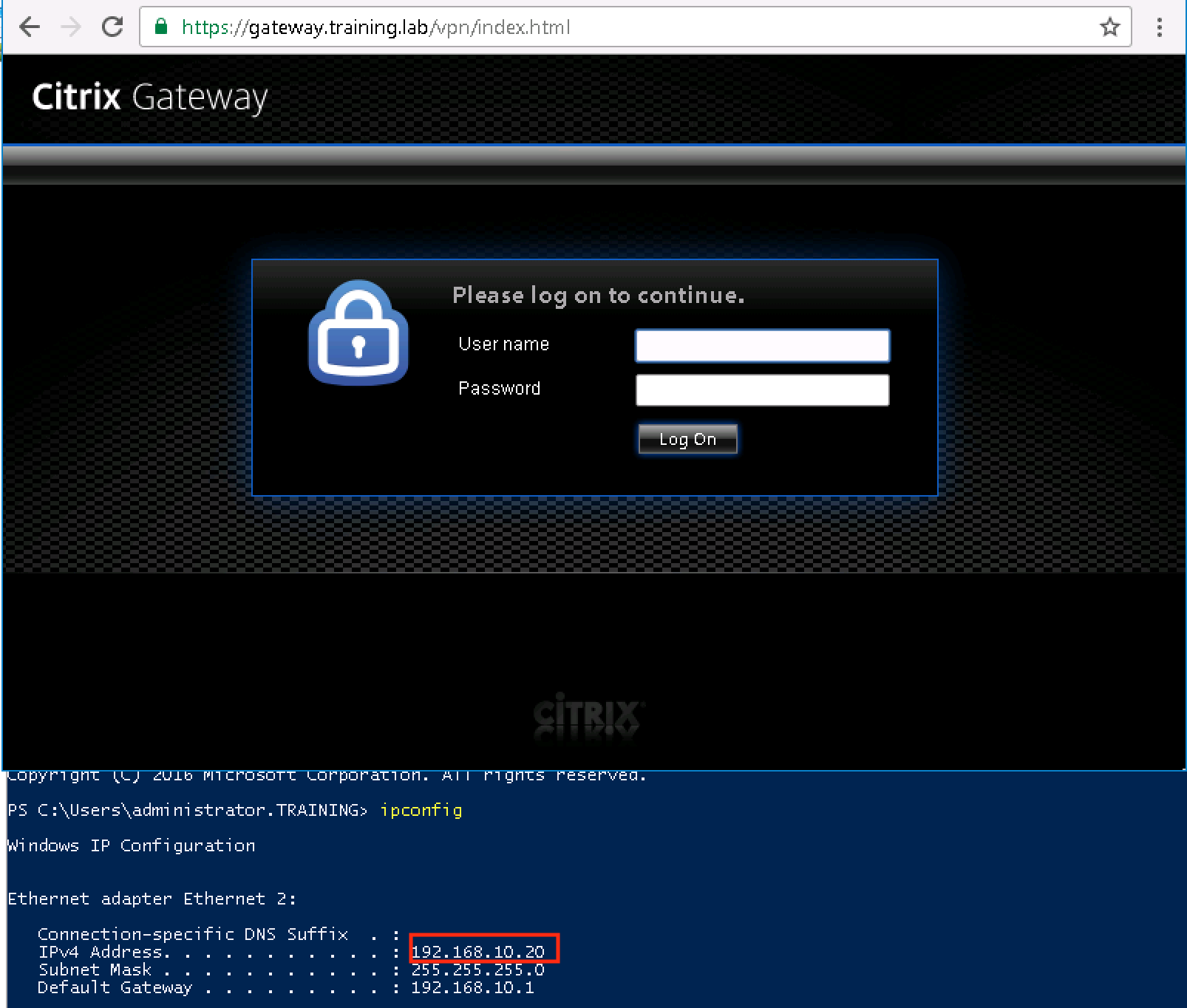




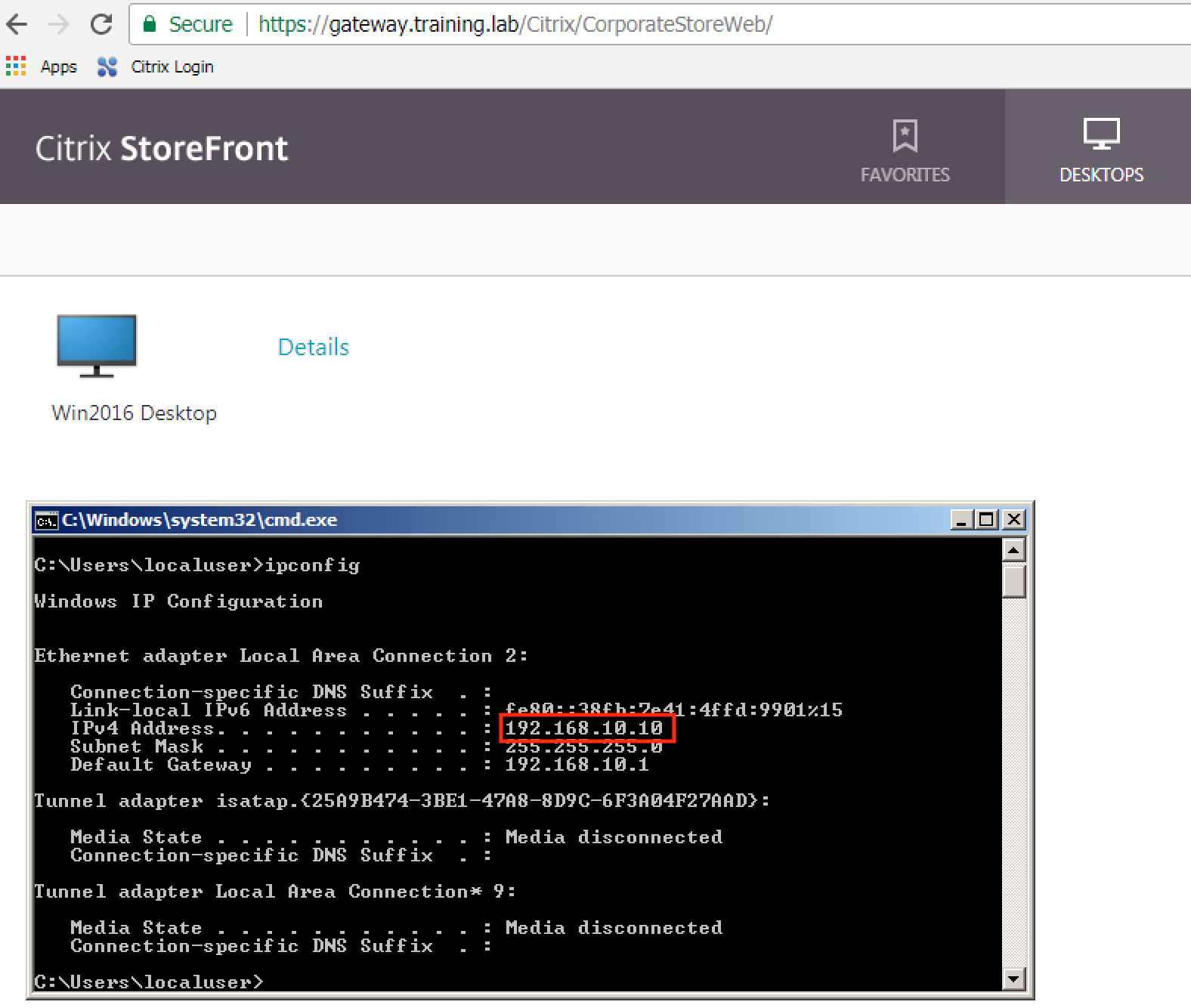


1. 白名单内用户访问：

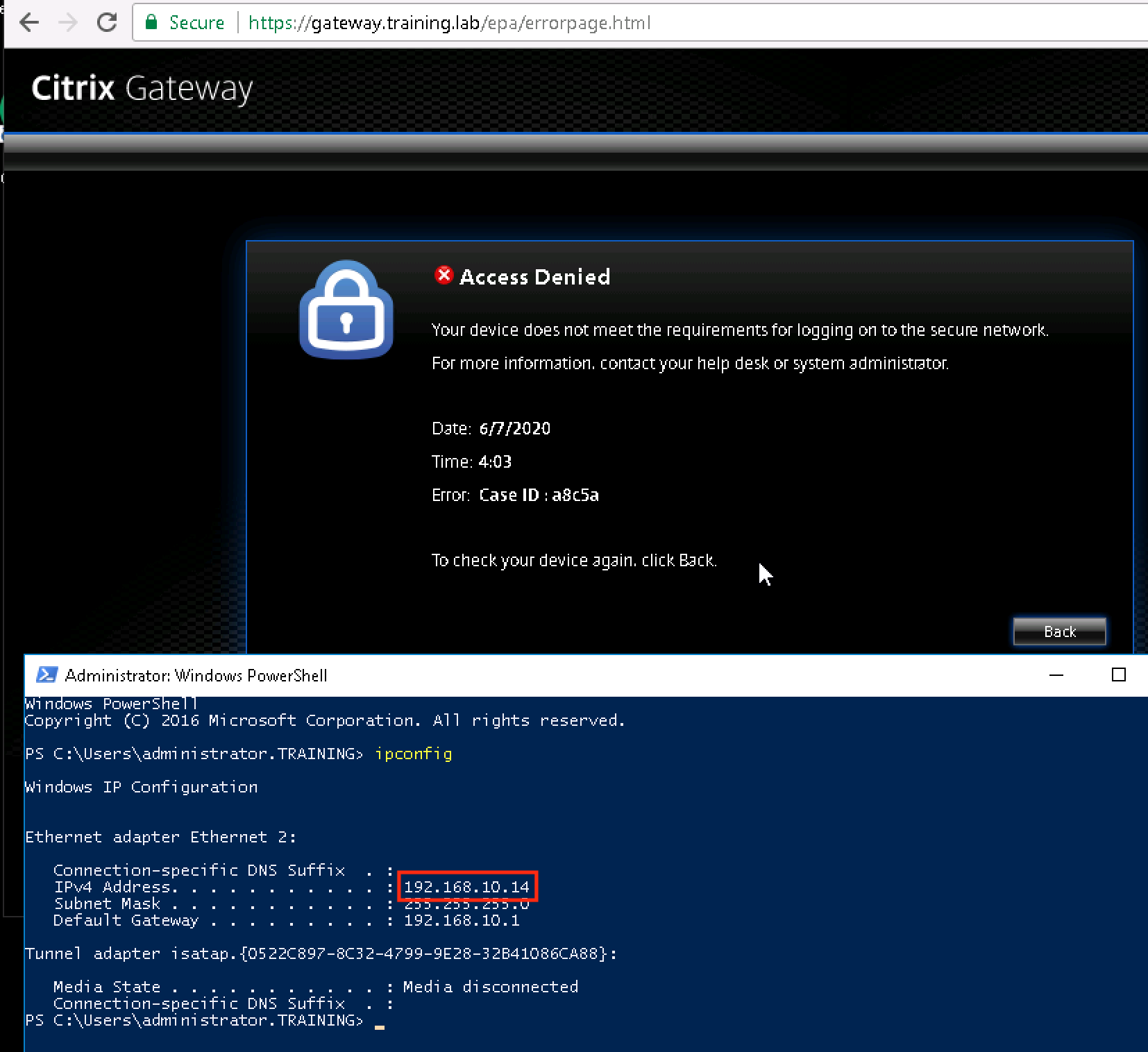
用户1，IP地址：192.168.10.20, 白名单内



用户2，IP地址：192.168.10.10, 白名单内



用户3，IP地址：192.168.10.14, 白名单外



结语：通过本次实测验证，证明通过Citrix ADC Gateway与CVAD进行集成后使用Smart Access功能，可以灵活便捷的基于Delivery Group实现对于远程桌面和应用接入终端的访问控制。本例中验证了基于用户ip地址白名单的访问策略控制，除此之外还可实现基于用户端操作系统，杀毒软件安全情况等多种因素条件组合对用户进行多维度的接入控制，大大提高系统架构安全性和管理灵活性。