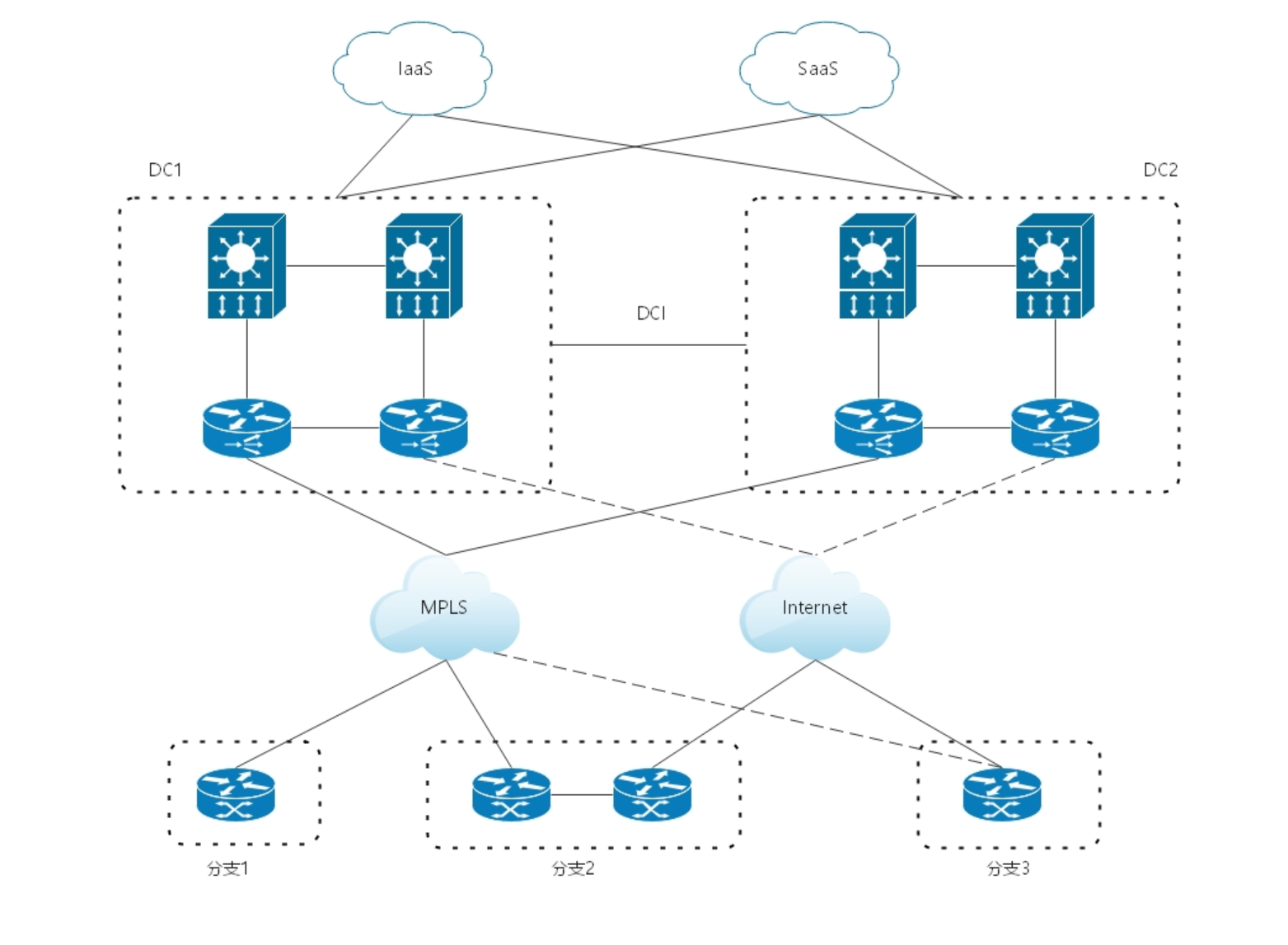
**搭建SDWAN环境，实际了解SDWAN**

1. 什么是SDWAN
2. SDWAN产生的背景

广域网（WAN）主要用于解决企业远程互联以及访问互联网（总部与分支、分支与分支、总部与互联网等）的需求，传统广域网技术主要有MPLS-VPN专线、数据专线、企业宽带等。传统广域网架构如下图所示：



传统广域网存在部署复杂、控制和数据平面集中、本地化管理、扩展性差、不支持多种传输方式、路由协议N平方问题、运维黑盒、链路优化困难、无法支持企业灵活上云，以及建设成本高等一系列挑战。

为解决上述传统广域网面临的一系列挑战和问题，SDWAN应运而生。SDWAN是软件定义广域网的简称，是将SDN技术应用到了广域网领域，以软件的方式去管理WAN，实现对广域网的集中控制，大大简化广域网WAN的运营。SDWAN是SDN技术的一部分，SDN是集中化的网络管理方法，将网络的控制平面和数据转发面分离，可以实现更多的网络自动化和智能化，简化网络配置，同时能够实现网络智能监控与故障自愈。

1. SDWAN的优势

相对传统广域网部署复杂、运维黑盒、链路优化困难、成本高等问题，SDWAN具有如下方面的优势：

1. 部署简单，即插即用，做到零配置上线，配置自动下发
2. 成本低廉，性价比高，采用开放的接入设备，节省设备投资费用
3. 接入灵活，支持多种接入方式，包括MPLS、Internet、4\5G等多种网络接入，灵活方便
4. 可视化，支持全局可视化模板配置以及可视化策略下发等，方便网络管理人员配置与监控网络
5. 业务感知，应用加速，自动进行最优链路选择，提高关键业务的QoS保障
6. 常见的SDWAN提供商

SDWAN技术应用越来越广，市场上提供SDWAN服务的厂商主要有如下四类：

（1）、传统设备厂商，代表有思科、华为等厂家，他们通过在自家路由器等设备上集成SDWAN功能来提供SDWAN服务

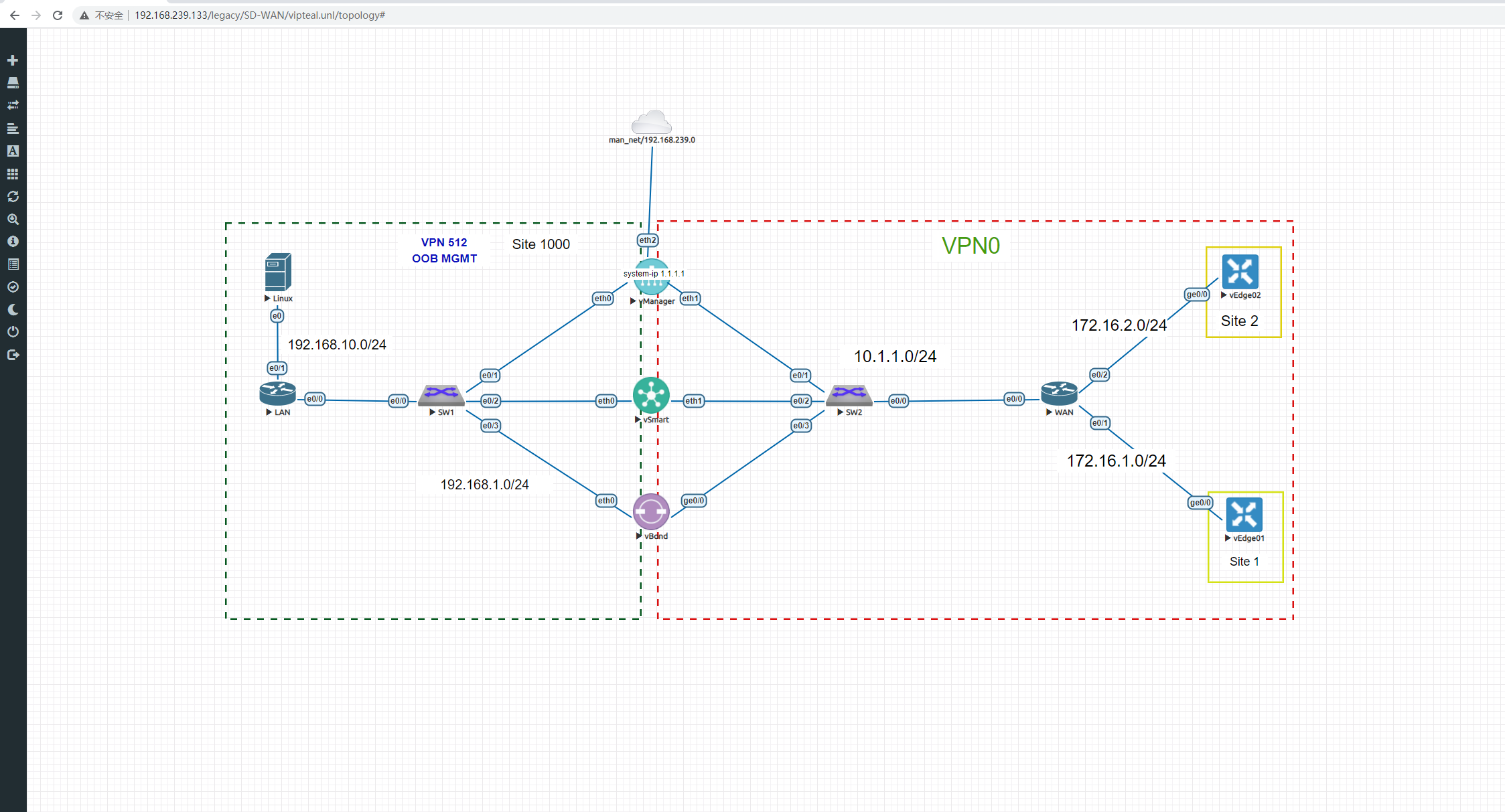
（2）、专门提供广域网解决方案的公司，这类公司租用三家运营商的网络，利用自己的技术构建overlay的SDWAN为企业提供广域网服务

（3）、运营商，运营商有丰富的网络资源，通过购买厂家的SDWAN软硬件来为客户提供SDWAN服务

（4）、云厂商，代表有阿里巴巴、腾讯等，他们围绕企业上云通过云原生的方式来构建以云为中心的SDWAN解决方案，帮助企业实现灵活快速上云

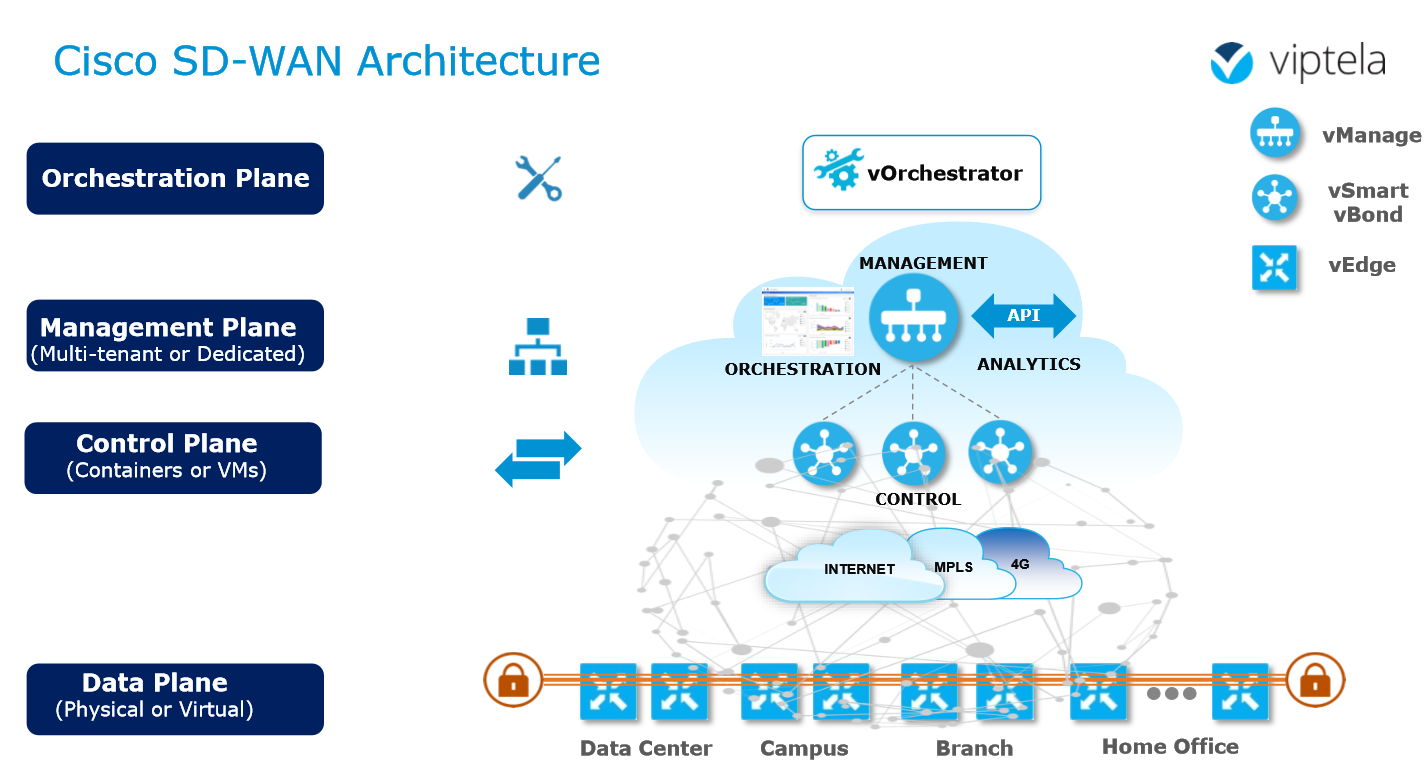
1. 搭建SDWAN环境，

前面说了SDWAN的概念以及优势，但是SDWAN到底是什么估计不少人还是云里雾里，接下来就通过实际搭建一套SDWAN的控制平面来给大家看看真实的SDWAN是什么样的。本次实验在EVE模拟环境中进行搭建。EVE是一款非常优秀的模拟器，类似华为的eNSP、思科的GNS3，但是EVE不仅仅可以模拟网络设备，而且可以运行一切虚拟机，感兴趣的可以去它的官网一探究竟www.eve-ng.net。本次实验基于思科的SDWAN组件进行搭建，网络拓扑如下图所示：



在本次实验中，构建了两个网络环境，分别是VPN512的管理网络和VPN0的业务网络。VPN512管理网络是专门用于管理SDWAN各组件的，VPN0是真正的业务网络，用于SDWAN的各组件之间通信。

在正式搭建之前，先介绍下思科SDWAN的架构。思科SDWAN主要由vManage、vBond、vSmart、vEdge组件构成。其中vManage、vBond、vSmart组成控制平面，vEdge组成数据平面。vManage是SDWAN的管理平面，可以看成是我们传统网络的OMC，是网络中单一的管理入口，通过GUI界面进行配置、管理和监控网络；vBond是orchestration编排平面，它知道网络的构建方式，在其他组件之间共享信息，所有要加入SDWAN的设备都必须先找到vBond,由vBond进行统一认证；vSmart是控制平面，可以看做SDN中的控制器，主要用于进行overlay层面的路由学习和发布；vEdge是数据平面，可以看做ovs中的vSwitch，接收vSmart下发的路由，根据路由进行数据包的转发与交换。



（此图片来自思科官网）

要搭建思科SDWAN，首先需要到思科官网注册账号，然后下载官方的组件镜像，再将镜像制作成EVE能够识别的格式导入到EVE环境中后，就可以在EVE环境中构建图中的网络拓扑，启动设备并且进行配置。详细的各网络设备的配置如下：

1、管理网络LAN配置

!

ip dhcp excluded-address 192.168.10.254

!

ip dhcp pool Ubuntu

network 192.168.10.0 255.255.255.0

default-router 192.168.10.254

!

!

interface Ethernet0/0

ip address 192.168.1.254 255.255.255.0

duplex auto

no cdp enable

!

interface Ethernet0/1

ip address 192.168.10.254 255.255.255.0

duplex auto

no cdp enable

no mop enabled

!

2、模拟互联网的WAN设备配置

!

interface Ethernet0/0

ip address 10.1.1.254 255.255.255.0

duplex auto

!

interface Ethernet0/1

ip address 172.16.1.254 255.255.255.0

duplex auto

!

interface Ethernet0/2

ip address 172.16.2.254 255.255.255.0

duplex auto

!

3、vManage的配置

system

host-name vmanage

system-ip 1.1.1.1

site-id 1000

admin-tech-on-failure

sp-organization-name mystacktrace

organization-name mystacktrace

vbond 10.1.1.2

!

vpn 0

interface eth1

ip address 10.1.1.1/24

tunnel-interface

allow-service dhcp

allow-service dns

allow-service icmp

no allow-service sshd

no allow-service netconf

no allow-service ntp

no allow-service stun

allow-service https

!

no shutdown

!

ip route 0.0.0.0/0 10.1.1.254

!

vpn 512

interface eth0

ip address 192.168.1.1/24

no shutdown

!

interface eth2

ip address 192.168.239.138/24

no shutdown

!

ip route 0.0.0.0/0 192.168.1.254

!

4、vBond配置

system

host-name vBond

system-ip 1.1.1.2

site-id 1000

admin-tech-on-failure

no route-consistency-check

organization-name mystacktrace

vbond 10.1.1.2 local vbond-only

vpn 0

interface ge0/0

ip address 10.1.1.2/24

tunnel-interface

encapsulation ipsec

no allow-service bgp

allow-service dhcp

allow-service dns

allow-service icmp

no allow-service sshd

no allow-service netconf

no allow-service ntp

no allow-service ospf

no allow-service stun

allow-service https

!

no shutdown

!

ip route 0.0.0.0/0 10.1.1.254

!

vpn 512

interface eth0

ip address 192.168.1.2/24

no shutdown

!

ip route 0.0.0.0/0 192.168.1.254

!

5、vSmart配置

system

host-name vsmart

system-ip 1.1.1.3

site-id 1000

admin-tech-on-failure

organization-name mystacktrace

vbond 10.1.1.2

vpn 0

interface eth1

ip address 10.1.1.3/24

tunnel-interface

allow-service dhcp

allow-service dns

allow-service icmp

no allow-service sshd

no allow-service netconf

no allow-service ntp

no allow-service stun

!

no shutdown

!

ip route 0.0.0.0/0 10.1.1.254

!

vpn 512

interface eth0

ip address 192.168.1.3/24

no shutdown

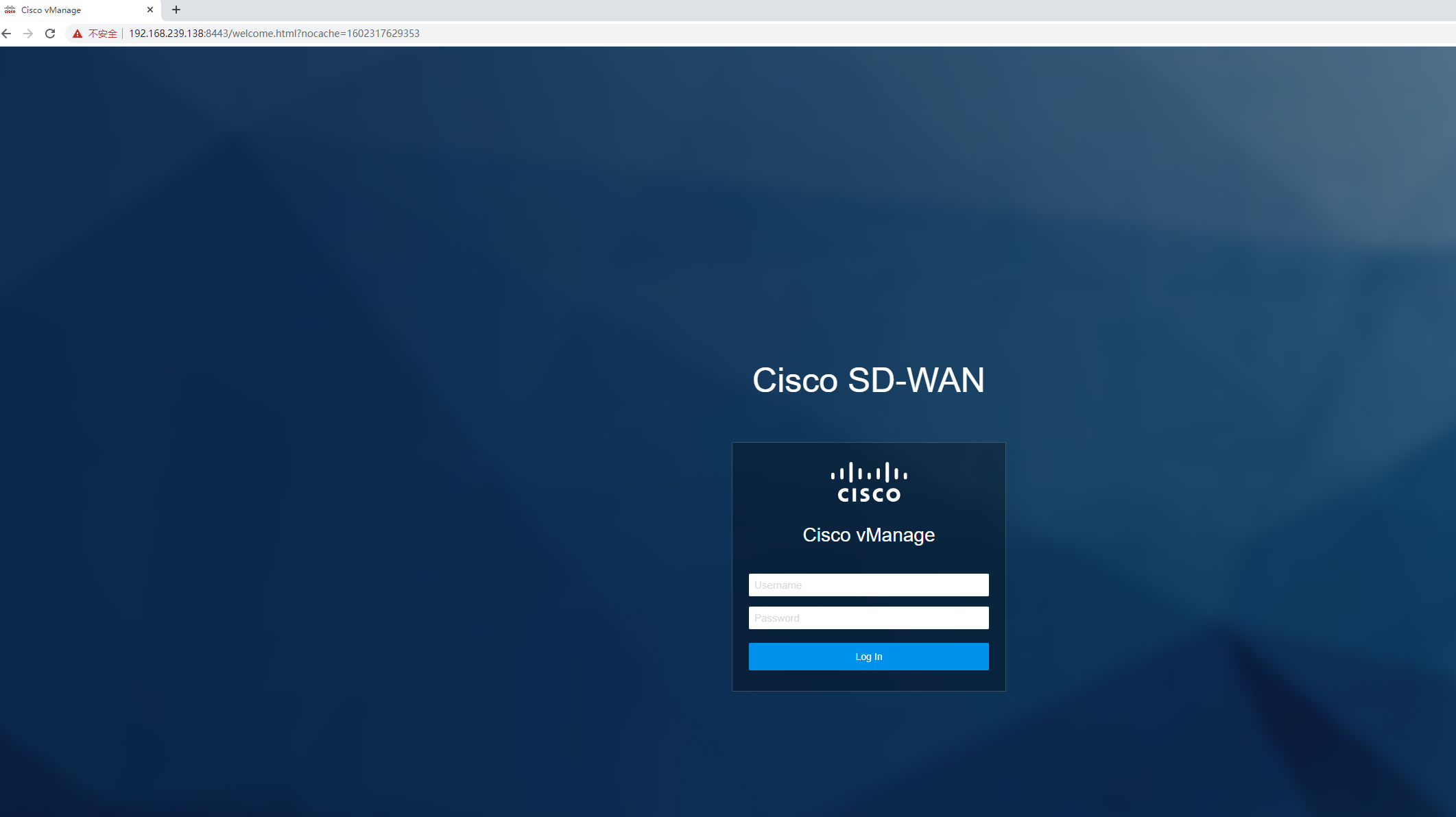
!

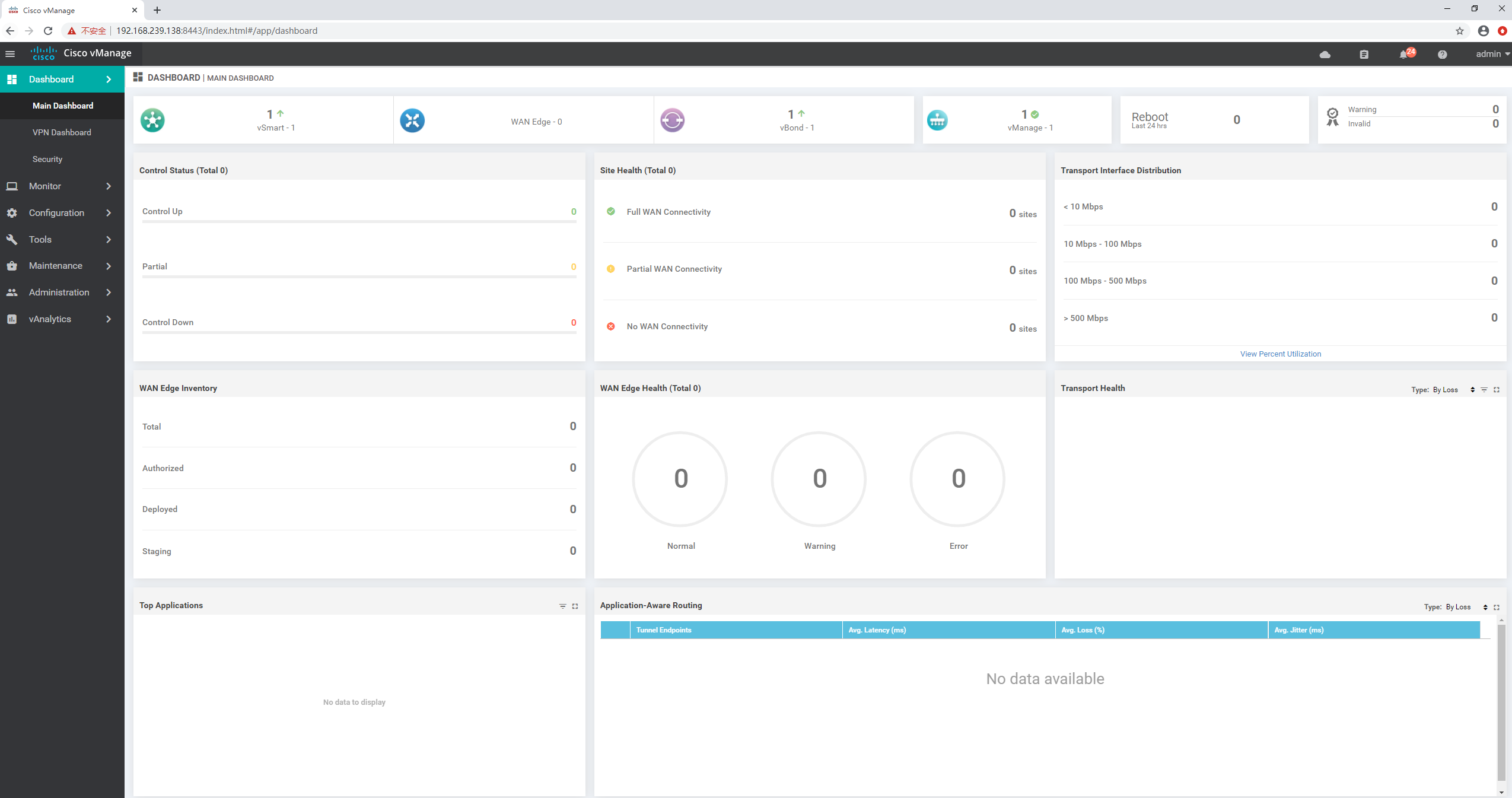
ip route 0.0.0.0/0 192.168.1.254

!

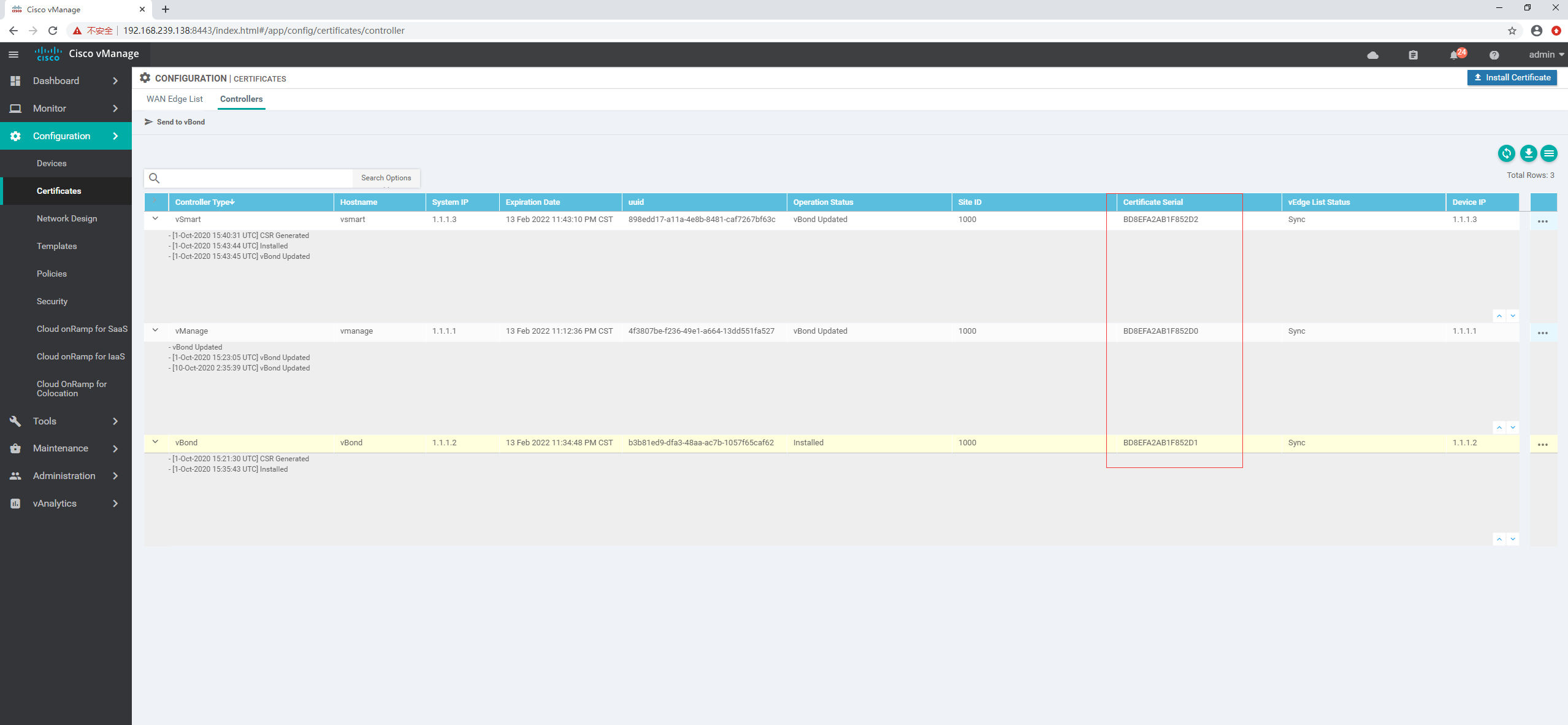
Tips:确保所有vManage、vBond、vSmart、vEdge组件的VPN 0域互通 VPN 0通常连接公网，用于控制流量通道。

6、上面的配置完成之后，我们就可以登录到vManage的GUI上，登录界面如下，默认用户名和密码admin/admin

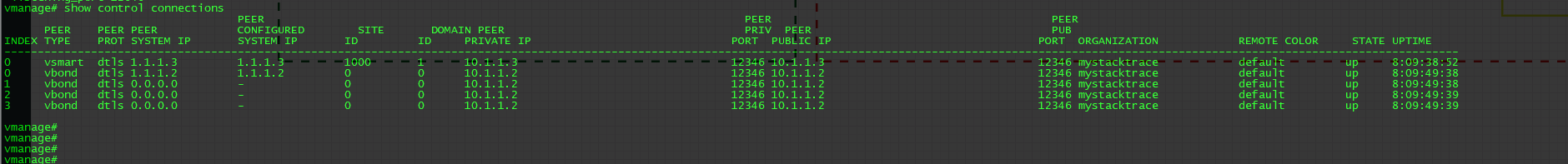




7、安装证书，实现组件之间的授权，因为思科viptela的各个组件vManage、vBond、vSmart、vEdge之间需要通过证书进行认证才能够相互注册交互，以免控制系统被黑客攻破。完成认证后的各个组件如下图所示：



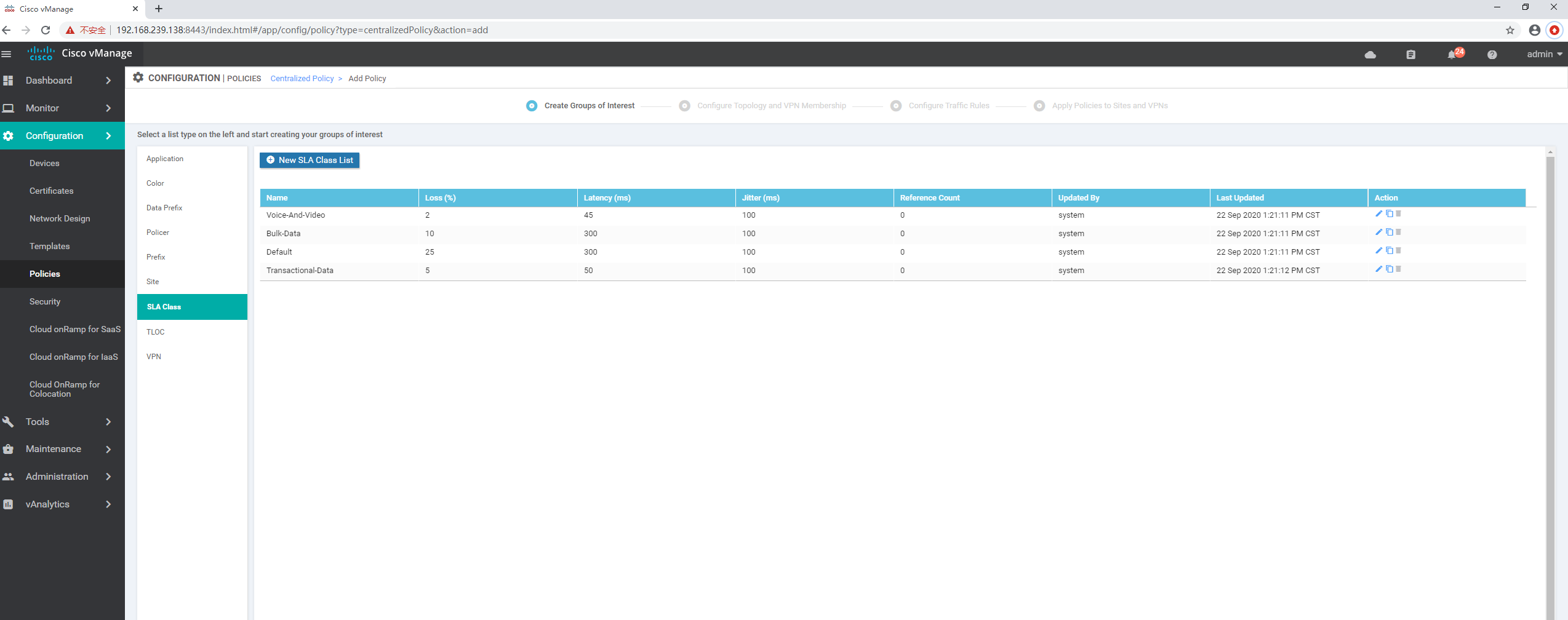
8、上面各组件完成配置以及认证之后，整个SDWAN的控制平面就算搭建完成，可以登录到设备运行下面的命令查看设备之间的连接是否建立起来。只要控制面连接建立起来，后续客户侧的CPE设备vEdge就可以通过ZTP的方式注册到SDWAN网络中来为企业提供服务了。



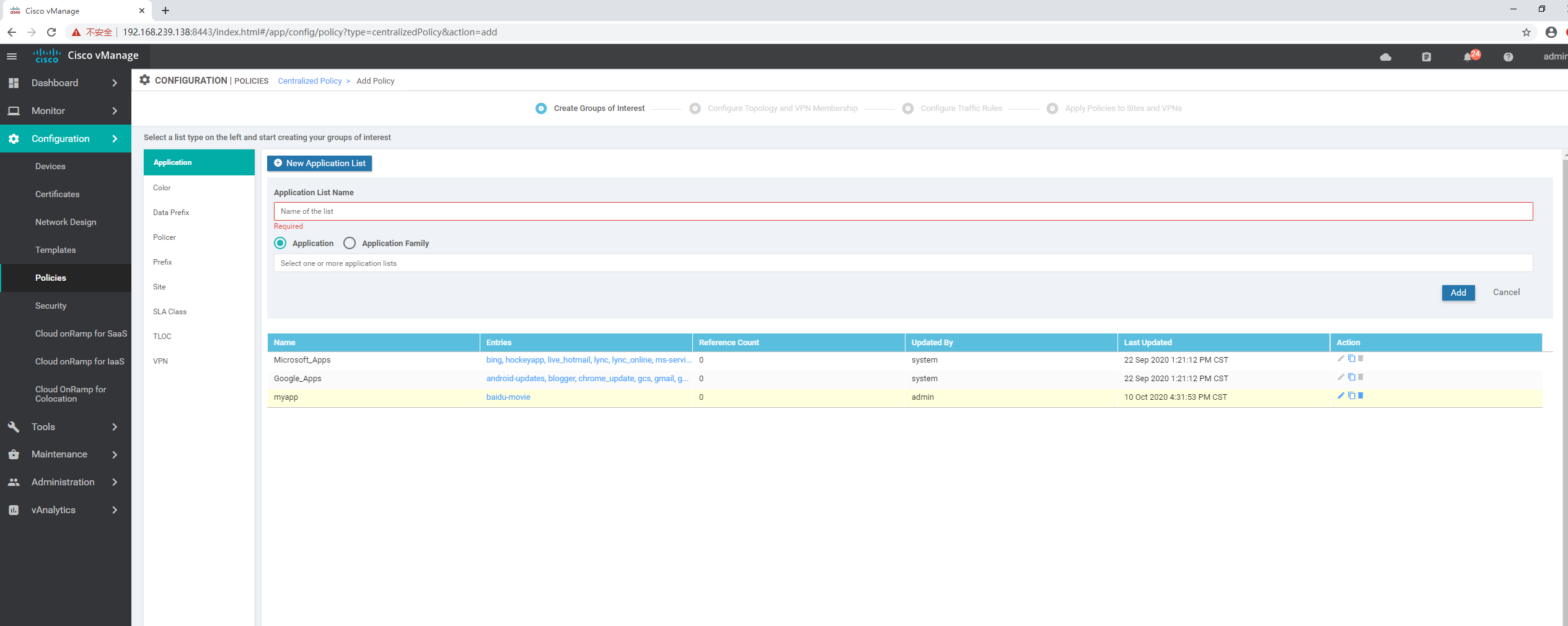
控制平面之间的DTLS连接

9、SDWAN的各种软技能列举：

SLA配置：



应用识别加速：



告警监控：

