

快速入门指南- Catalyst SD-WAN简化配置和策略

目录

[简介](#)

[背景信息](#)

[摘要](#)

[新部署](#)

[现有部署](#)

[增强用户体验和简化运营](#)

[定义网络层次结构和系统结构](#)

[网络层次结构](#)

[系统结构](#)

[工作流程](#)

[配置组](#)

[配置组部署示例](#)

[使用案例1：政府客户](#)

[使用案例2：零售客户](#)

[关联](#)

[部署](#)

[可重用性](#)

[应用目录](#)

[策略组](#)

[应用优先级和SLA](#)

[简单模式](#)

[高级模式](#)

[服务质量](#)

[应用感知路由](#)

[流量策略](#)

[嵌入式安全](#)

[安全互联网网关/安全服务边缘](#)

[DNS安全](#)

[利益集团](#)

[关联和部署](#)

[本地化策略](#)

[拓扑](#)

[拓扑和VPN](#)

[映射到多个VPN ID的VPN名称](#)

[映射到同一VPN ID的多个VPN名称](#)

[自注册](#)

[标记](#)

[添加标记](#)

[标记配置组中的规则](#)

[插图](#)

[现有部署](#)

[配置组](#)

[策略组](#)

[拓扑](#)

[转换工具](#)

[范围](#)

[访问详细信息](#)

[操作方法](#)

[前提条件](#)

[转换工具 workflow](#)

[转换后](#)

[考虑事项](#)

[20.12 考虑事项](#)

[相关信息](#)

简介

本文档介绍 Catalyst SD-WAN 的简化配置和策略。

背景信息

摘要

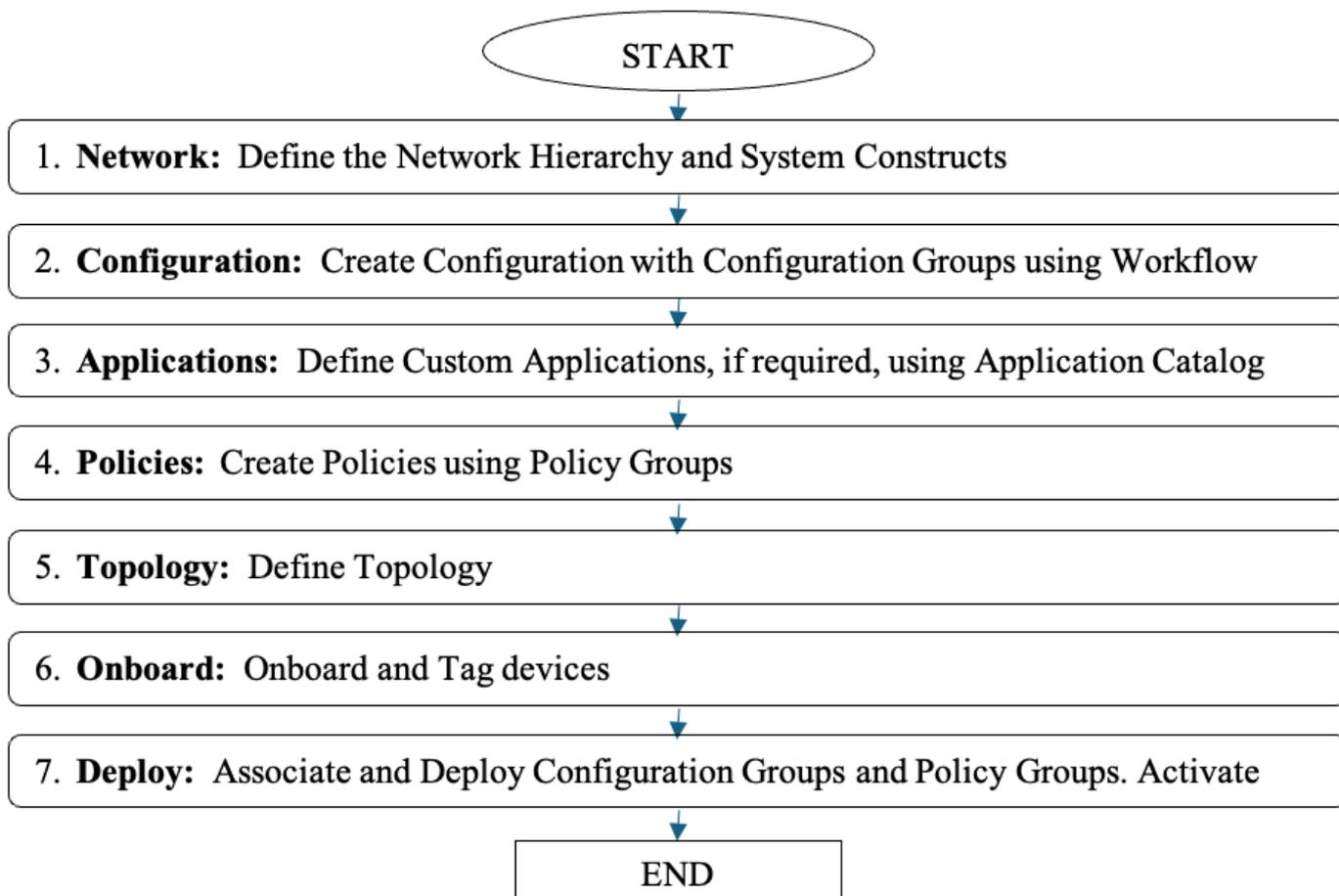
对于 Cisco Catalyst SD-WAN 软件版本 20.12/17.12，建议用户开始从基于设备和功能模板的传统配置迁移到基于配置组和策略组的新配置方法。本文档介绍了新配置方法的重要详细信息。

本文档的主要目的是作为指南，帮助您开始使用 20.12 金牌版本中的配置、策略和自行激活的新结构。本文档不介绍各个功能。

新部署

要成功利用新的配置方法，您需要执行以下步骤：

1. 网络：定义网络层次结构和系统结构
2. 配置：使用工作流程创建具有配置组的配置
3. 应用：如果需要，使用应用目录定义自定义应用
4. 策略：使用策略组创建策略
5. 拓扑：定义拓扑
6. 板载：板载和标记设备
7. 部署：关联和部署配置组和策略组。激活拓扑。



新部署的流程图

现有部署

1. 执行[现有部署](#)部分提到的步骤
2. 使用[Conversion tool](#)将现有配置/策略转换为新配置/策略

增强用户体验和简化运营

Cisco Catalyst SD-WAN提供增强的用户体验并简化操作。

- **通用UI**：在Catalyst SD-WAN Manager和其他思科产品中引入了一个新的UX框架，以实现用户体验的一致性并提供跨产品的通用外观和效果。
- **配置**：通过直观的基于意图的工作流程和思科建议的智能默认设置简化配置、策略创建和部署。
- **监控**：通过新构件和可定制且增强的控制面板，提供对网络和应用性能及运行状况的丰富见解。
- **故障排除**：动态站点和网络拓扑视图、基于情景的故障排除工具访问、定期的网络和应用性能报告。

好处

简单易用	直观、有指导的工作流程
------	-------------

配置无计划扩张	减少无计划扩张 (与模型无关、重复使用、结构化)
配置创建	使用智能默认值更快速、更轻松
配置修改	现在修改，以后有选择性地部署
可视性	新控制面板、应用/站点性能监控
故障排除指南	站点拓扑、故障排除工具指南

定义网络层次结构和系统结构

网络层次结构

为网络提供“层次结构”的概念，即站点、区域和区域。您可以根据网络创建此项。

示例：



Search



Global (15 of 15 nodes)



AMER



BR1_SanJose



BR2_NewYork



BR6_Dallas



APJC



BR3_Mumbai



BR4_Singapore

链路的蜂窝网接口（包括静态路由）必须在 workflows 后通过手动编辑配置组进行配置。

LAN 配置文件

LAN Profile

2 VPNs

2 SVIs

2 Wireless SSIDs

2 Access switch ports

DIA static route

示例 Use Case 1 - LAN 配置文件 2

使用 workflows，可以生成此使用案例的某些 LAN 配置文件配置。2 个 VPN、DIA 静态路由。

在将配置组部署到设备时，可以使用实际值指定实体，例如实际的 Dot1Q 子接口和标记为特定于设备的任何其他实体。

NOTE:

必须在工作流程后通过手动编辑配置组配置SVI、无线SSID、接入交换机端口等。

系统配置文件

System Profile

Default features - AAA, NTP, OMP etc.

Application Performance monitoring

使用实例1 -系统配置文件2

使用工作流程，可以生成此使用案例的大多数系统配置文件配置- OMP、AAA、NTP、日志记录等。

NOTE:

必须在工作流程后通过手动编辑配置组来配置高级配置（如应用性能监控）。

CLI配置文件

CLI Profile NBAR enable

示例Use Case 1 - CLI配置文件2

通过GUI不支持的功能（如应用/流可视性[NBAR]启用）可以使用CLI配置文件进行配置。

应用/流可视性

要启用应用可视性和流可视性，请使用CLI配置文件/包。

(在20.13及更高版本中，可在Policy Group中的Advanced Settings下使用)

但是，在20.12中，如果配置了AAR策略，则会启用应用/流可视性。并且不需要使用CLI配置文件/包配置此功能。

配置组SiteType2

执行创建配置组工作流程。

WAN配置文件

WAN Profile

1 Internet link

1 LTE link

DHCP

Static Route for Cellular link (AD=1)

示例1 - WAN配置文件3

使用工作流程，可以生成此使用案例的大多数WAN配置文件配置。Internet的以太网接口。DHCP。

NOTE:

LTE链路的蜂窝网接口（包括静态路由）必须在工作流程后通过手动编辑配置组进行配置。

LAN 配置文件

LAN Profile

1 VPN

1 SVI

1 Access switch port

DIA Static route

示例1 - LAN配置文件3

使用工作流程，可以生成此使用案例的某些LAN配置文件配置。1 VPN、DIA静态路由。

在将配置组部署到设备时，可以使用实际值指定实体，例如实际的Dot1Q子接口和标记为特定于设备的任何其他实体。

NOTE:

必须在工作流程后通过手动编辑配置组配置SVI、接入交换机端口等。

系统配置文件

与配置组SiteType1相同

CLI配置文件

与配置组SiteType1相同

配置组SiteType3

执行创建配置组工作流程。

WAN配置文件

与配置组SiteType2相同

LAN 配置文件

LAN Profile

1 VPN

1 SVI

1 Wireless SSID

1 Access switch port

DIA Static route

使用工作流程，可以生成此使用案例的某些LAN配置文件配置。1 VPN、DIA静态路由。

在将配置组部署到设备时，可以使用实际值指定实体，例如实际的Dot1Q子接口和标记为特定于设备的任何其他实体。

NOTE:

必须在工作流程后通过手动编辑配置组配置SVI、无线SSID、接入交换机端口等。

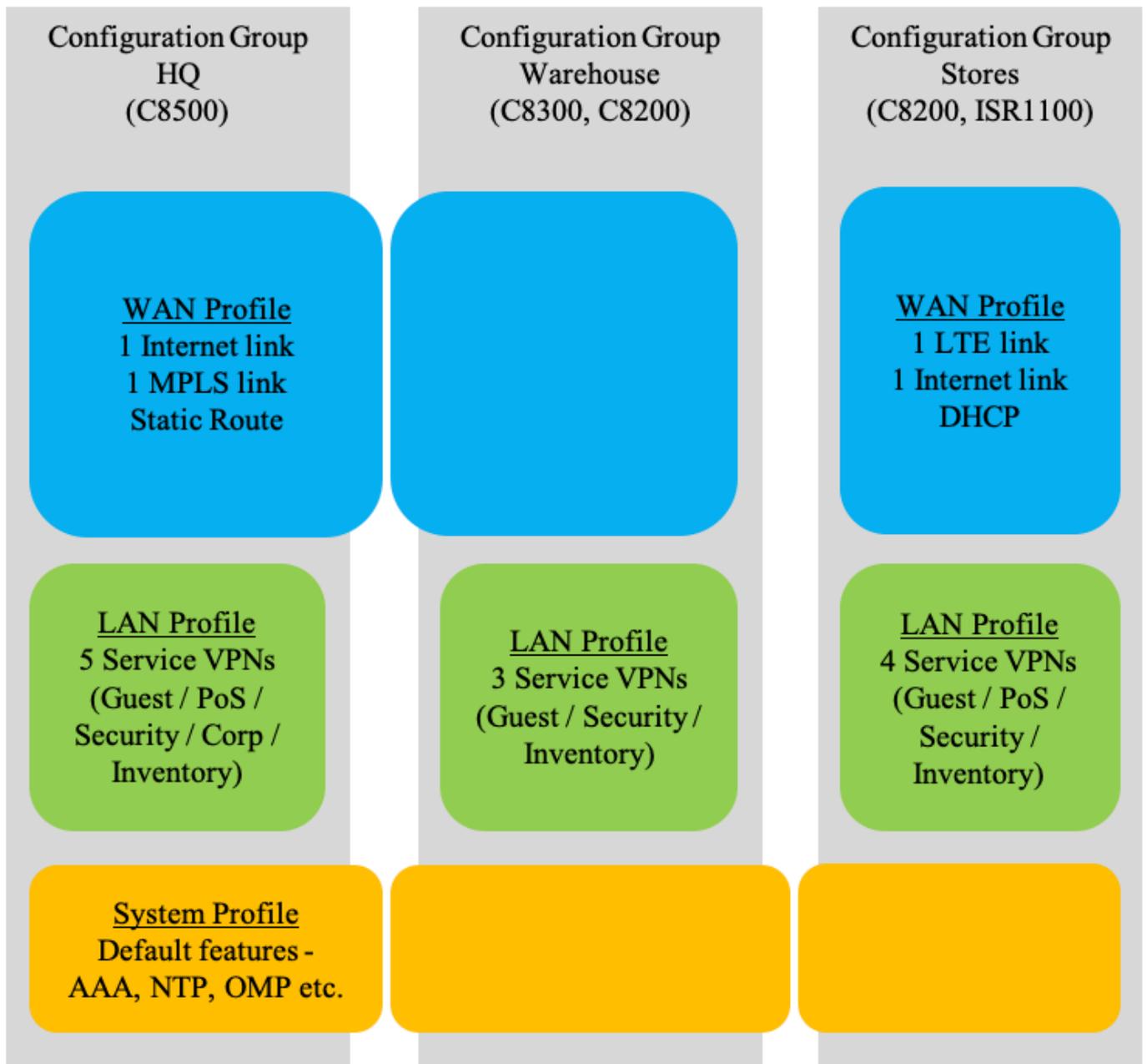
系统配置文件

与配置组SiteType1相同

CLI配置文件

与配置组SiteType1相同

使用案例2：零售客户



示例UseCase 2 -配置组

配置组HQ和仓库

执行创建配置组工作流程。

WAN配置文件

使用工作流程，可以生成此使用案例的所有WAN配置文件配置。

LAN 配置文件

使用工作流程，可以生成此使用案例的所有LAN配置文件配置。

在将配置组部署到设备时，可以使用实际值指定实体，例如实际的Dot1Q子接口和标记为特定于设备的任何其他实体。

系统配置文件

使用工作流程，可以生成此用例的所有系统配置文件配置。

NOTE:

如果需要进行任何更改或需要应用性能监控等高级配置，则必须在工作流程后通过手动编辑配置组对其进行配置。

配置组存储

执行创建配置组工作流程。

WAN配置文件

使用工作流程，可以生成此使用案例的大多数WAN配置文件配置。

NOTE:

LTE链路的蜂窝网接口（包括路由）必须在工作流程后通过手动编辑配置组进行配置。

LAN 配置文件

使用工作流程，可以生成此使用案例的所有LAN配置文件配置。

在将配置组部署到设备时，可以使用实际值指定实体，例如实际的Dot1Q子接口和标记为特定于设备的任何其他实体。

系统配置文件

与配置组HQ和仓库一样。

关联

在Configuration Group编辑页面(Configuration -> Configuration Groups)中，您可以将设备与配置组关联。

单击Associate Devices 并完成 workflow 中的步骤。

[Go Back to Configuration Group list](#)

US-WEST-SITES [Edit](#)

Description: US-WEST-SITES

DEVICE SOLUTION: [sdwan](#) | MODIFIED BY: [Chhalaji](#) | LAST UPDATED: [Dec 14, 2023 06:27:32](#)

[Feature Profiles](#) | [Associated Devices](#)

Global

SITE_1

SITE_3

Devices (2) [Export](#)

0 selected | [Associate Devices](#) | [Remove Devices](#) | [Add and Edit Rules](#) | [Change Device Values](#) | [Deploy](#) As of: Jul 15, 2024 10:23 AM

Chassis Numbers	Site Name	Hostname	Tags	Config Locked	System IP	Site ID	Device Status	Added by Rule	Last Configured	Up To Date
<input type="checkbox"/> CBK-A51EAB60-5D3D-35C1-0051-A1D4416C1202	SITE_1	Site1-Edge	-	Yes	1.1.1.1	1	In Sync	false	Dec 14, 2023, 6:27:32 AM	True
<input type="checkbox"/> CBK-01DE1D37-0F1B-F8DF-E71A-9D58D665FD1D	SITE_3	Site3-Edge	-	Yes	3.3.3.1	3	In Sync	false	Dec 14, 2023, 6:27:32 AM	True

关联设备-配置组

部署

执行部署配置组工作流程。



Deploy Configuration Group

Push configuration to devices in your WAN

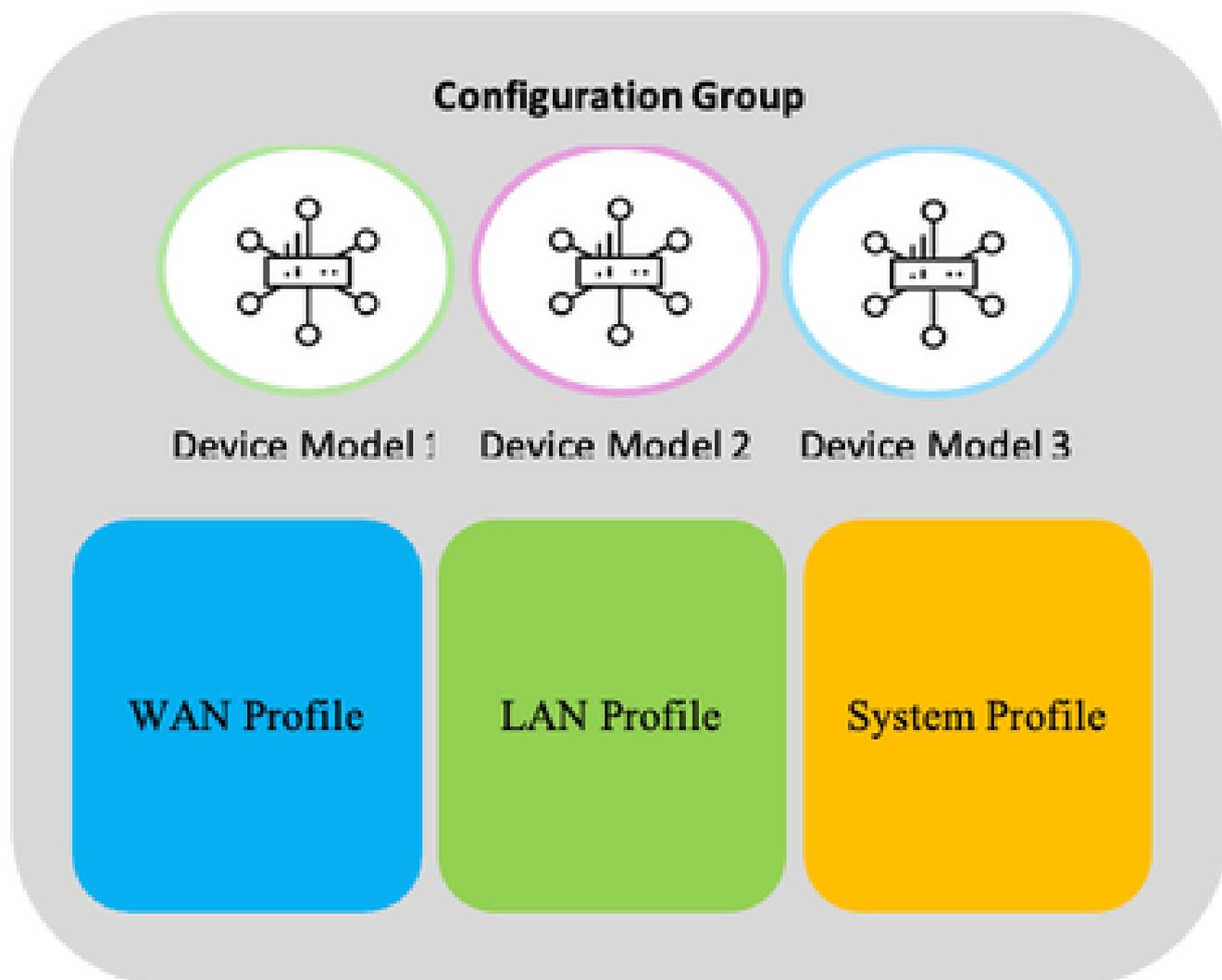
部署配置组工作流程

NOTE:

- 在配置组中，更改设备值仅更改Manager数据库中的值，不会向设备推送任何更改。如果您希望更改立即生效，则需要部署更改。
- 导出设备变量值（作为CSV文件）可以在添加/审核设备配置步骤的“部署”工作流程中完成。

可重用性

1. 配置组与设备型号无关。



配置组-与设备型号无关

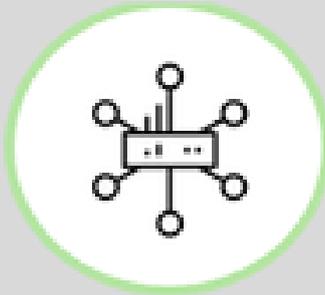
NOTE:

如果设备型号不支持特定配置，则不会执行相应的功能包推送，并且会在部署任务中显示相应的消息。

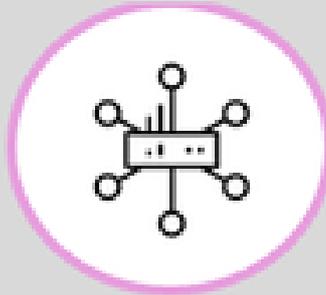
示例：设备不支持Wi-Fi，但配置组包含Wi-Fi包。在部署时，Wi-Fi包配置会被跳过，并且部署任务消息会通知已跳过Wi-Fi配置推送。

2. 使用配置变量-特定于设备的值

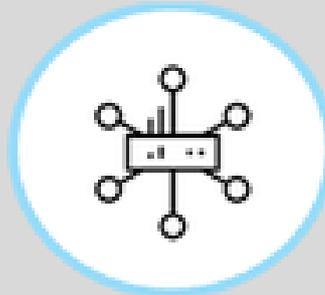
Configuration Group



Device Model 1



Device Model 2



Device Model 3

WAN Profile

LAN Profile

System Profile

Variable 1

Variable 2

Variable 3

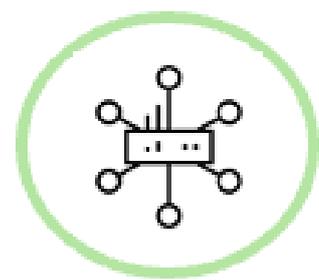
配置组-设备特定变量

功能配置文件可以将某些配置定义为特定于设备，类似于模板变量。

示例：接口IP地址、端口号、接口名称等。

这些设备特定值可在部署时提供。并且不同设备可以不同。

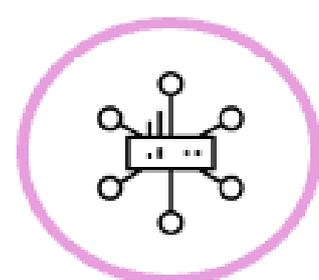
System Profile
Variable 1 = A
Variable 2 = B
Variable 3 = C



Device 1

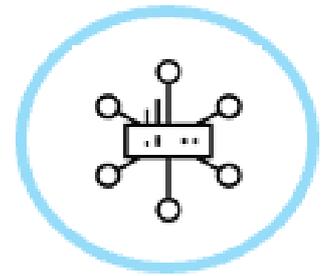
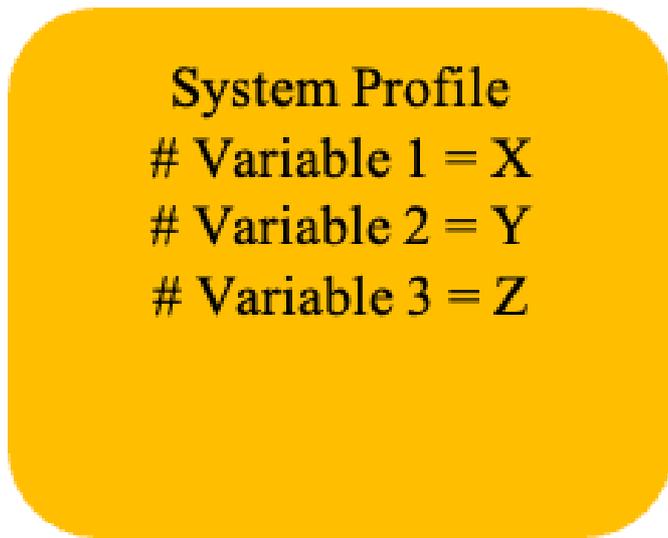
配置组-设备特定变量示例1

System Profile
Variable 1 = D
Variable 2 = E
Variable 3 = F



Device 2

配置组-设备特定变量示例2



Device 3

配置组-设备特定变量示例3

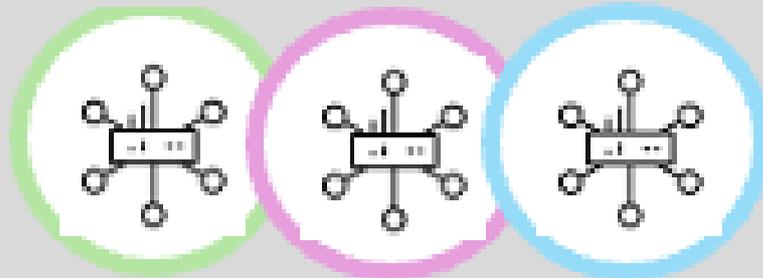
3. 重复使用功能配置文件

功能配置文件可在配置组中重复使用。

插图：

对于多台设备，如果WAN和系统配置相同，并且仅在LAN配置中不同（例如，如果WAN和系统配置文件的配置不同），则可以在其配置组间重复使用WAN和系统配置文件，同时每个配置组中具有不同的LAN配置文件。

Configuration Group



**WAN
Profile
1**

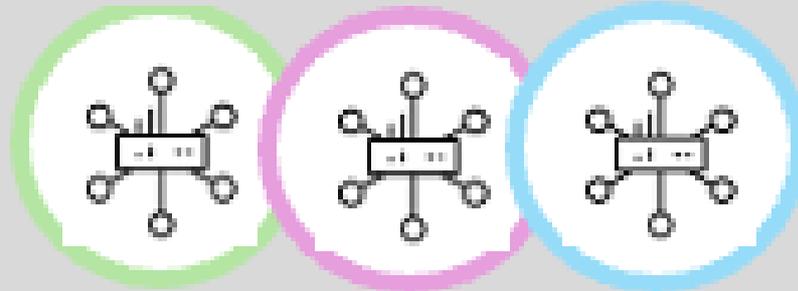
**LAN
Profile
1**

**System
Profile
1**

重复使用功能配置文件- 1

LAN配置文件1

Configuration Group



WAN
Profile
1

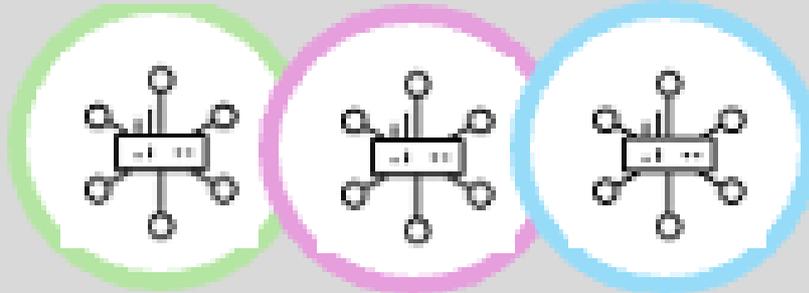
LAN
Profile
2

System
Profile
1

重复使用功能配置文件- 2

LAN配置文件2

Configuration Group



**WAN
Profile**

1

**LAN
Profile**

3

**System
Profile**

1

重复使用功能配置文件- 3

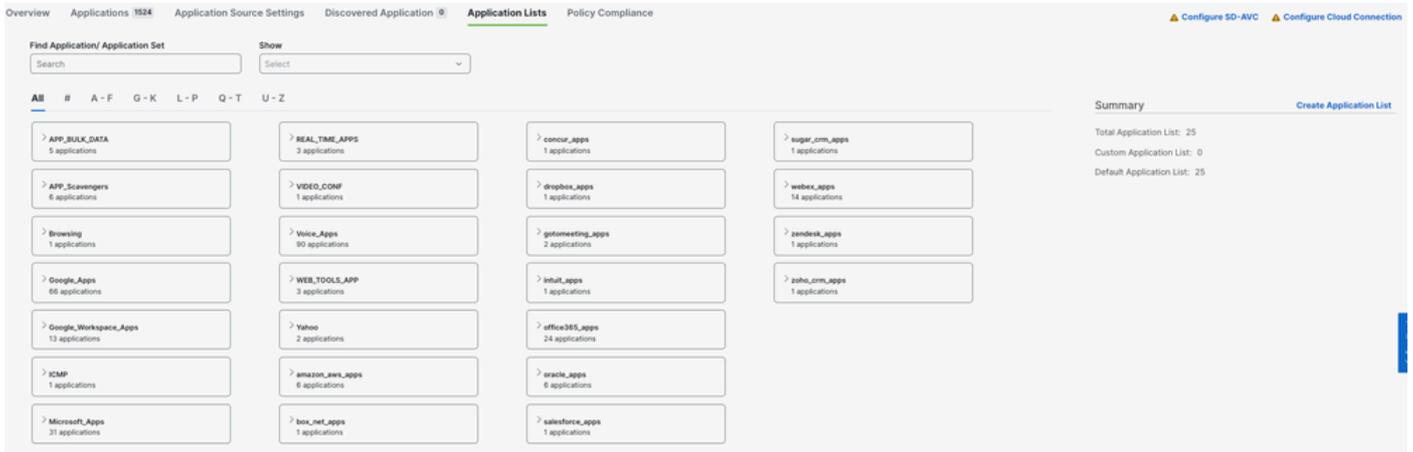
LAN配置文件3

应用目录

传统设备可以通过源和/或目标IP地址、源/目标端口和协议的条件匹配来控制流量。 由于越来越多的应用依赖于DNS或嵌入到HTTP中，因此很难在应用级别准确识别网络流量。

思科的网络应用识别(NBAR)引擎能够对1500多个应用进行分类，使网络工程师能够更精细地分类和操作流量。 思科的Catalyst SD-WAN Manager能够连接到思科应用存储库，应用签名可以在其中快速更新；这对于云提供商更改托管位置或流量模式具有重要意义。

应用程序目录允许根据服务器名称、IP地址、端口或协议的匹配创建自定义应用程序。 然后，该应用被定义为特定应用系列、应用组、流量类和业务相关性。



应用目录

可以将应用拖放到相应的业务相关性和/或流量分类中。保存更改后，即会在数据库中更新定义。

注意：应用分类是全球性的，应用目录中的更改会影响所有设备分类。

策略组

与配置组类似，策略组是部署至与策略组关联的设备的一组策略。

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Policy-Groups/policy-groups/m-policy-groups.html>

策略组根据意图处理策略创建和部署。简化的UI和 workflows 使创建策略、分组策略以及部署到设备成为一项轻松的任务。

前提条件：

将配置组关联并部署到设备是向该设备部署策略组的先决条件。

Cisco Catalyst SD-WAN Select Resource Group Configuration · Policy Group of Interest

Policy Group 3 Application Priority & SLA 7 Embedded Security 6 Secure Internet Gateway 4 DNS Security 1

As of: 12 August 2024 at 10:24

Search

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
US-West-Policy	US-West-Policy						

US-West-Policy

Policy Group Name: US-West-Policy Description: US-West-Policy

Policy

Application Priority: App-Visibility Embedded Security: US-West-Security

Secure Internet Gateway: Please Select one DNS Security: Please Select one

Deployment

Associated to: 2 Device(s)

Save Deploy

策略组

应用优先级和SLA

使用此策略意图，可以指定：

- 应用感知路由和SLA策略
- QoS策略
- 流量数据策略
- DIA策略
- SIG策略

提供了两种模式。

简单模式

这是默认模式。

SDWAN Fabric Traffic Policy

Priority	Preferred Path	When SLA not met	Backup Path
Gold Business Relevant	Select Preferred Path	Default to Best Path	Not Applicable
Silver Default	Select Preferred Path	Default to Best Path	Not Applicable
Bronze Business Irrelevant	Select Preferred Path	Default to Best Path	Not Applicable

Internet Offload Traffic

Policy	Application List	Fallback to Routing
Secure Internet Gateway	Select Application List	<input type="checkbox"/>
Direct Internet Access	Select Application List	<input type="checkbox"/>

Apply Policy

Target

Direction: Enter Direction | VPN: Select VPN | Interface: Enter Interfaces

[View](#) [Variable](#)

简单模式

这样可以快速、轻松地定义网络的应用优先级和SLA。

NOTE:

1. 默认策略操作为DROP
2. 匹配条件可以是应用程序。如果您需要前缀，请使用高级模式

高级模式

这是一种完整而灵活的模式。

BH_DIA_traffic (3) [Edit Policy](#) [Delete Policy](#) [Add Rules](#) [Delete All Rules](#)

VPN: Employee Direction: service

Search Rule by Name or Order

NAME	MATCH	ACTION
1 DNS	Destination Port - 53	Count - DNS_Counter Nat Use Vpn - true
2 traffic	App List - O365	Count - O365_Counter Nat Fallback - true Nat Use Vpn - true
3 Allow_All		Count - SIG_Counter Secure Internet Gateway - true

Rules per page: 10 < 1 > Go to: 1 / 1

SLA Class **QoS Queue**

No SLA Class added, add your first SLA Class in Traffic Policy

高级模式

NOTE:

1. 默认策略操作为DROP

2. “应用列表”和“流量类”实际上是“应用”列表。

其中任何一个都可用于匹配应用列表。可以在应用目录中完成应用到流量类的映射。

Simple模式使用其中任意一项或两项生成规则，而Advanced模式仅提供Application List。

服务质量

在QoS Queue选项中，您可以添加QoS策略：

Advanced Layout



SLA Class

QoS Queue

[⊕ Add QoS Policy](#)

No Qos Class added, add your first Qos Class in Traffic Policy

Queueing Model

4 Queues ^

Policy Name *
Enter Policy Name

Target Interface *
Enter Interfaces

Value Variable

Queue	Forwarding Class	Bandwidth %	Drops	Scheduling Type
0	Select one	%	Tail	Low Latency Queuing (LLQ)
1	Select one	40 %	Random Early	Weighted Round Robin (WRR)
2 (default)	Select one	20 %	Random Early	Weighted Round Robin (WRR)
3	Select one	30 %	Random Early	Weighted Round Robin (WRR)

Q0 10%
Q1 40%
Q2 20%
Q3 30%

Bandwidth

排队模型

接下来，您可以定义流量数据策略(添加流量策略)。

添加规则以匹配所需流量并重定向到适当的转发类。

Policies > Application Priority & SLA

Basic_4Queue_QoS_Policy (Total Traffic Policy: 1)

Additional Settings Advanced Layout

VPN: CORP,PARTNER Direction: Service Default Action: Accept

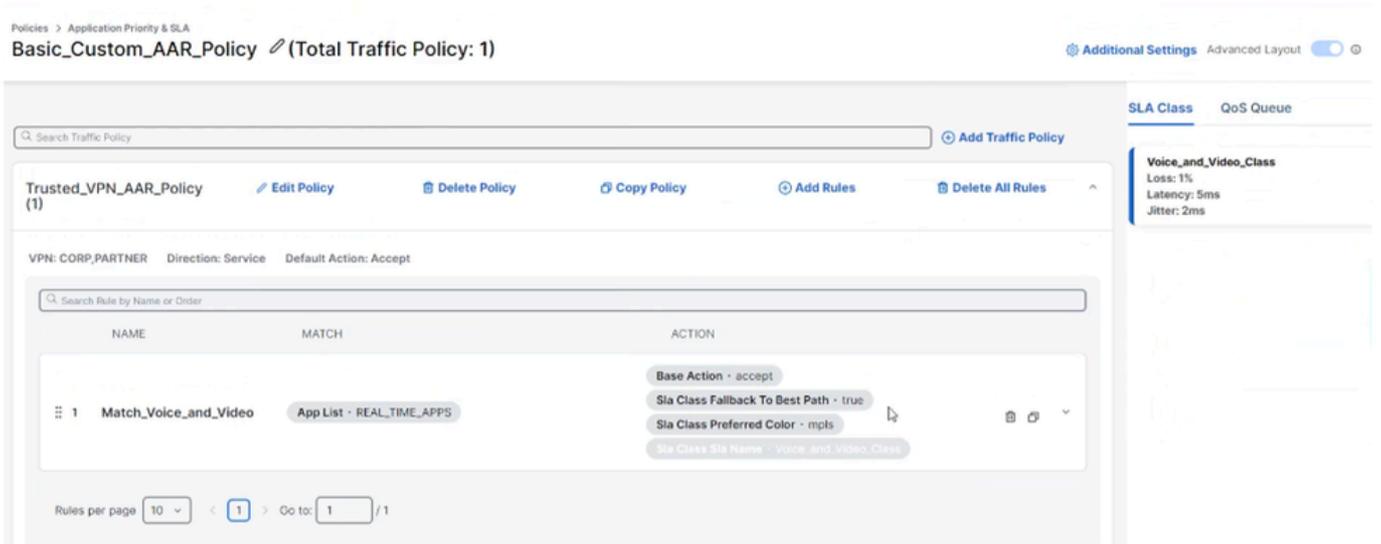
NAME	MATCH	ACTION
1 Match_Voice_Traffic	Dscp - 46	Base Action - accept Count - voice Forwarding Class - VOICE Log - true
2 Match_Critical_Apps	App List - Microsoft_Apps	Base Action - accept Count - critical_apps Forwarding Class - CRITICAL_DATA Log - true
3 Match_Bulk_Data_Traffic	Destination Data Prefix List - DC.File_Servers Destination Port - 21	Base Action - accept Count - bulk_data Forwarding Class - BULK_DATA Log - true
4 Match_All_Other		Base Action - accept Forwarding Class - DEFAULT

VOICE bandwidth 10%
CRITICAL_DATA bandwidth 40%
BULK_DATA bandwidth 20%
DEFAULT bandwidth 30%

QoS策略2

应用感知路由

您可以定义SLA类并在流量策略中使用它们来实现AAR策略的意图。



AAR策略

应用/流可视性

要启用应用可视性和流可视性，请使用配置组中的CLI配置文件/包。

(在20.13及更高版本中，可在Policy Group中的Advanced Settings下使用)

但是，在20.12中，如果配置了AAR策略，则会启用应用/流可视性。并且不需要使用CLI配置文件/包配置此功能。

流量策略

流量策略还可用于创建DIA策略、SIG重定向等。根据需要添加规则。

⊕ Add Traffic Policy

MyTrafficPolicy (1) [Edit Policy](#) [Delete Policy](#) [Add Rules](#) [Delete All Rules](#)

VPN: Corporate_Users,Local_Internet_for_Guests,Physical_Security_Devices Direction: all

NAME	MATCH	ACTION
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ⌵ 1 Rule1 </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 30%;"> <p>Sequence</p> <input style="width: 90%; border: 1px solid #ccc;" type="text" value="1"/> </div> <div style="width: 40%;"> <p>Name</p> <input style="width: 95%; border: 1px solid #ccc;" type="text" value="Rule1"/> </div> <div style="width: 30%;"> <p>Protocol</p> <input style="width: 90%; border: 1px solid #ccc;" type="text" value="IPv4"/> </div> </div> <div style="margin-top: 5px;"> <p>Match Add Match ⌵</p> <p>Action Add Action ⌵</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Base Action</p> <p><input type="radio"/> Accept <input checked="" type="radio"/> Drop</p> </div> </div>		

Cancel
Save Match and Actions

流量策略

NOTE:

如果在简单模式下创建应用优先级和SLA策略，然后切换到“高级”模式，则无法选择某些“匹配”选项。示例：目标数据前缀将灰显。

要使这些选项可用，请根据需要将Protocol从BOTH更改为IPv4或IPv6。

嵌入式安全

定义机载NGFW、IPS、恶意软件和内容过滤的安全策略

安全互联网网关/安全服务边缘

定义建立到基于云的内容和安全实体（如思科安全访问）的隧道所需的设置。

NOTE:

使用传统配置方法时，可作为功能模板使用。

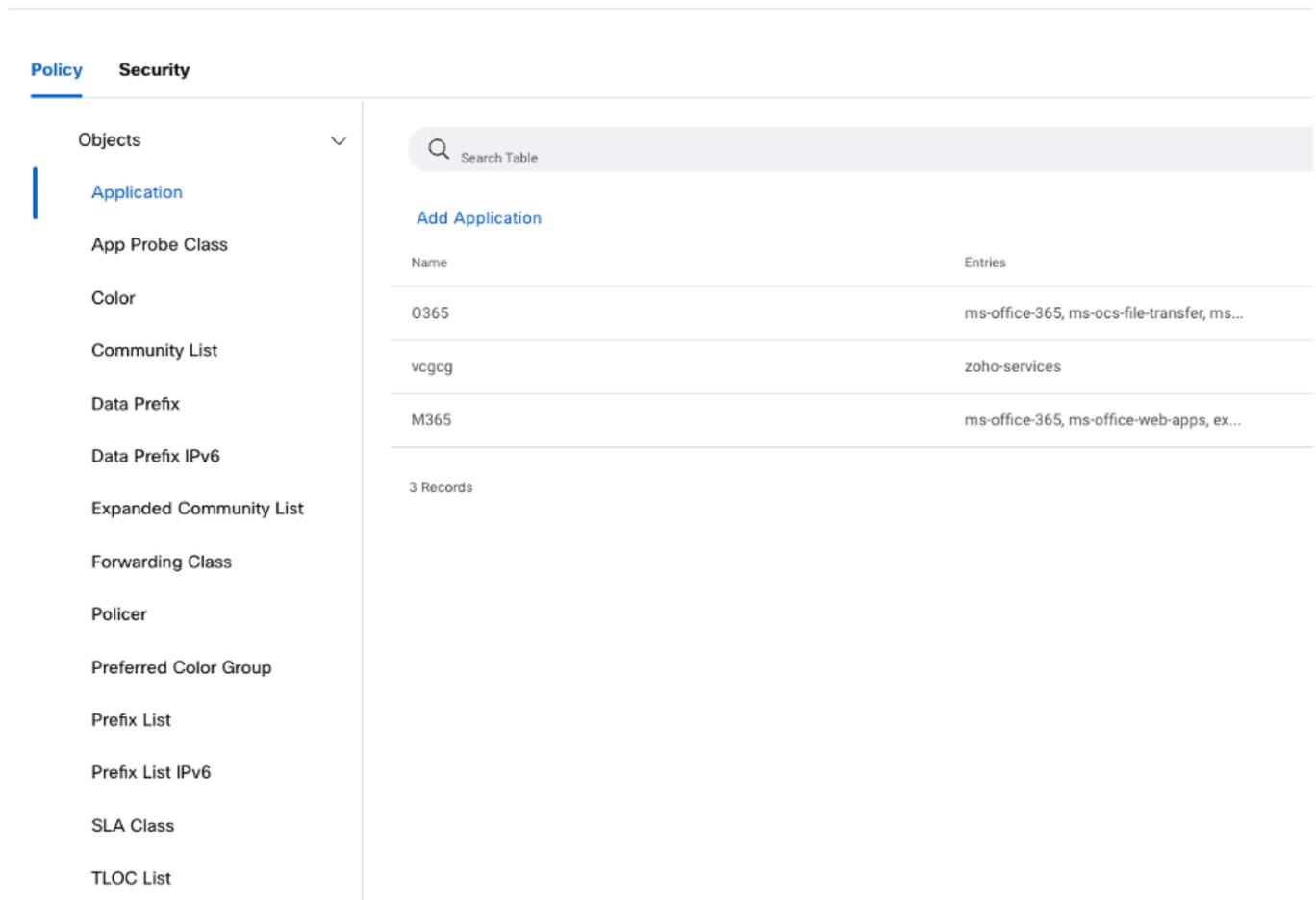
DNS安全

定义允许使用基于云的DNS安全服务进行内容过滤的设置。

利益集团

定义要在策略中使用的对象列表。示例：应用列表、VPN列表、站点列表、前缀列表等。

此外，对于安全策略，请定义高级检查配置文件、SSL解密策略等配置文件。



The screenshot shows a web interface for 'Policy Security'. On the left is a sidebar with a list of objects: Objects, Application (highlighted), App Probe Class, Color, Community List, Data Prefix, Data Prefix IPv6, Expanded Community List, Forwarding Class, Policer, Preferred Color Group, Prefix List, Prefix List IPv6, SLA Class, and TLOC List. The main area has a search bar labeled 'Search Table' and a link 'Add Application'. Below is a table with columns 'Name' and 'Entries'. The table contains three rows of data and a footer indicating '3 Records'.

Name	Entries
0365	ms-office-365, ms-ocs-file-transfer, ms...
vcgcg	zoho-services
M365	ms-office-365, ms-office-web-apps, ex...

策略组-兴趣组

关联和部署

与配置组类似，将设备关联到策略组并进行部署。

本地化策略

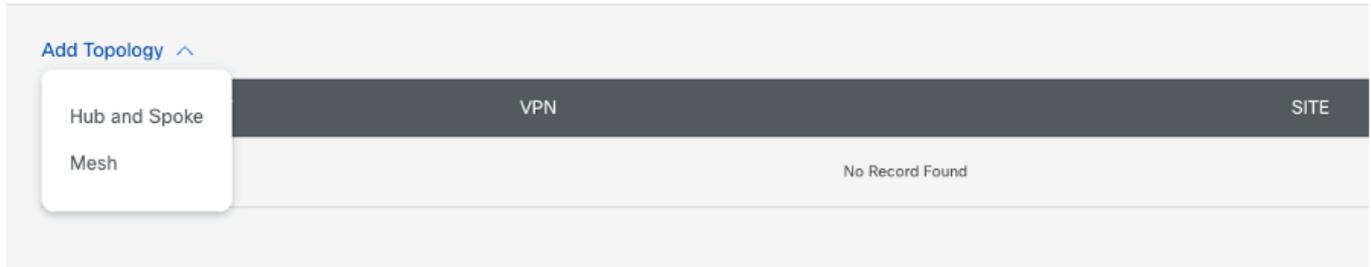
本地化策略（如ACL、路由策略、设备访问策略等）在配置组中定义。

拓扑

定义网络拓扑。

从全网状或星型开始，根据需要进行自定义。

Topology / MyTopology

MyTopology 

Topology菜单

拓扑和VPN

创建拓扑和指定VPN时，请记住这些设计更改。

新设计允许将VPN名称动态映射到VPN ID，而不是1:1映射。

映射到多个VPN ID的VPN名称

插图：

假设在两个不同的配置组中有一个名称为Corporate的VPN。

一个具有VPN ID 10，另一个具有VPN ID 20。

拓扑工作流VPN列表仅显示了Corporate VPN的一个实例。

选择Corporate VPN后，SD-WAN Manager将根据拓扑确定VPN ID。

假设在2个站点中有2台设备：

1. 站点100中的Device1使用Corporate作为VPN 10
2. 站点200中的Device2使用Corporate作为VPN 20

如果站点100和站点200都是拓扑的一部分，则SD-WAN Manager将创建同时具有VPN ID (10和20) 的VPN列表。

如果仅站点100是拓扑的一部分，则SD-WAN Manager将创建一个VPN列表，该列表将仅具有VPN ID 10。

如果仅站点200是拓扑的一部分，则SD-WAN Manager将创建一个VPN列表，该列表将仅具有VPN ID 20。

映射到同一VPN ID的多个VPN名称

可以使用相同的VPN名称配置映射到不同站点中不同VPN ID的多个拓扑策略。

SD-WAN Manager根据与哪些站点关联的拓扑确定实际映射。

插图：

两个用户可以创建两个不同的配置组。

一个将VPN ID 100指定为财务 VPN，另一个将其指定为工程 VPN。

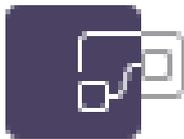
然后，它们可以使用各自的VPN名称创建拓扑。

自注册

要自行激活物理路由器，请使用快速连接 workflow。

使用此工作流程，为要注册的设备预定义主机名、系统IP和站点名称/ID。Manager会自动生成这些日志，但您可以根据需要进行修改。您还可以标记设备，然后使用这些设备将设备自动关联到配置组。

在PnP ZTP自注册过程中，设备会建立到SD-WAN Manager的控制平面隧道连接。SD-WAN Manager现在将预定义交换矩阵配置推送到设备，并且设备加入SD-WAN交换矩阵。



Quick Connect

Onboard your devices.

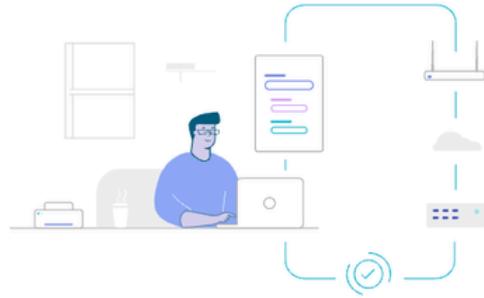
Welcome to Quick Connect

Before getting started, ensure that you have the following configured:

- Organization Name
- Certificate Authorization
- vSmart, vBond, vManage controllers (as applicable)

[Haven't configured them yet? Do it here.](#)

Note : This workflow supports adding up to 25 devices at a time.
For more devices, use device template to configure.



Get Started

Don't show this to me again

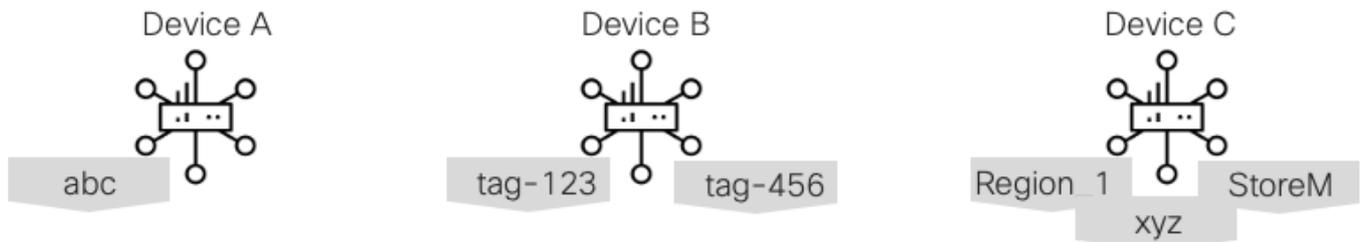
快速连接工作流程说明

标记

设备可以与用户定义的标记相关联。

标记可用于分组、描述、查找或管理设备。

标签允许对设备进行分组，然后将这些设备用于其他功能。



标记示例

示例：配置组与设备的关联。

配置组规则可设置为使具有特定标记的设备自动与该配置组关联。

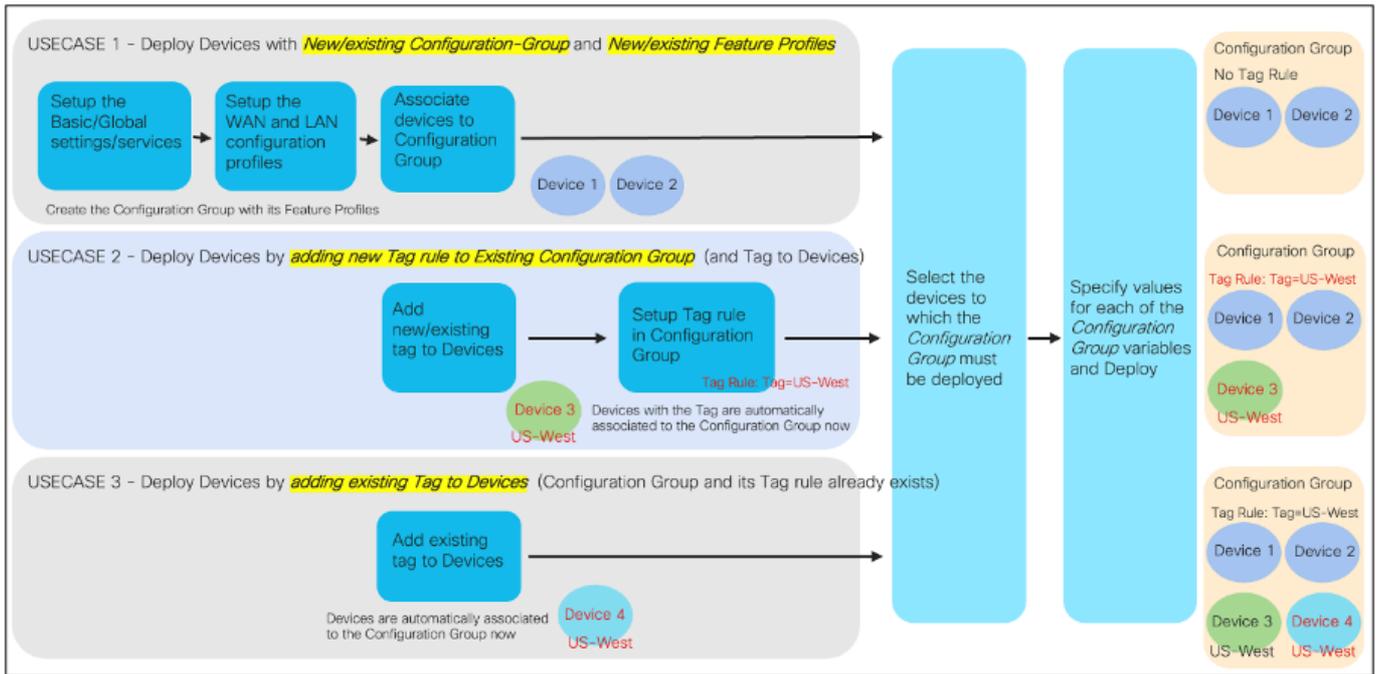
添加标记

在配置(Configuration) ->设备(Devices)中，可以创建/添加/删除设备中的标签。

标记配置组中的规则

在“配置组”(Configuration Group) ->“关联设备”(Associated Devices)页面中，可以添加/编辑标记规则。

插图



标记插图

现有部署

在SD-WAN网络中，使用传统配置和策略的设备可以使用简化配置和策略与设备共存。

本节为想要使用简化配置和策略的客户提供了一些建议，而本节提供了一些建议。

第一步是将设备从设备模板迁移到配置组。完成此操作后，即可部署策略组和/或拓扑。

配置组

设备模板和配置组提供边缘设备配置。因此很容易出现共存。从设备模板迁移到配置组的步骤如下：

第 1 步	从设备模板中提取设备值的副本。这可以从Configuration à Templates中完成，点击设备组右侧的省略号(...)并选择“Export CSV”。
步骤 2	创建配置组（手动或使用转换工具）。
步骤 3	从设备分离设备模板。此时，设备会在连接点维护配置；但不会收到将来对设备模板（或任何组件功能模板）所做的任何更改。
步骤 4	将设备关联到新配置组。

步骤 5	部署与配置组关联的设备。 为了简化此过程，请打开导出的CSV文件，然后更改CSV列标题以匹配配置组中的新变量。
步骤 6	在设备变量输入屏幕之后，您可以预览设备配置。 这可以让您预览配置组的哪些部分与上一个实例不匹配，或者哪些变量已从设备模板更改。

为变量保持一致的命名方案可简化特定于设备的设置。 如果所有设备值都在一个CSV中，则只需重命名列标题一次。

注意：存在一个python脚本，该脚本与设备模板或配置组的CSV文件配合使用，以整合列标题并将其按字母顺序排列。 该脚本可在以下位置找到：
<https://github.com/BradEdgeworth/CSVMerger>

策略组

通过配置组配置的设备可以使用集中式策略或向策略组迁移；但不能对同一应用同时使用这两种策略。 实际上，目标是为边缘设备保持相同的底层策略。 策略组将原始AAR和数据策略合并到单个应用优先级和SLA PG组件中。 实际上，我们只是更改策略配置的构建方式（而不是发送到SD-WAN Manager）。

请务必注意，不能让数据策略或AAR策略引用具有应用优先级和SLA组件的站点的站点列表，因为它们都配置相同的设置。

在集中策略配置集中策略的不同组件时，可以将集中策略与仅使用具有应用优先级和SLA的策略组的控制策略引用到站点。

将设备从集中策略迁移到策略组的步骤包括以下步骤：

第 1 步	创建必要的策略组组件（应用优先级和SLA、嵌入式安全、安全互联网网关/安全服务边缘、DNS安全）。
步骤 2	创建策略组并关联必要的组件。
步骤 3	将站点ID与AAR或数据策略中引用的任何SiteList取消关联。 此时，SD-WAN Manager将更新配置发送到控制器，然后控制器会从边缘设备删除所有活动数据策略说明。 请注意，这可能会导致此时出现意外的流量。

步骤 4	将设备关联到策略组并保存策略组。
步骤 5	将策略组部署到所选设备。此时，SD-WAN Manager会将更新的配置发送到边缘设备（用于QoS/SIG）和控制器；以便控制器可以将更新的数据策略发送到边缘设备。

注意：虽然策略组可以与集中策略共存，但建议将边缘设备转换为配置组时保持集中策略（适用于AAR和数据策略）。然后，开始从集中策略迁移到策略组，以实现 Application Priority & SLA组件中的功能。

这样做纯粹是为了简化操作并降低操作人员的困惑。

NOTE:

Policy Group Engine以不同的格式存储内容。因此，必须在策略组中重新创建集中策略中使用的前缀列表。对于站点列表等其它事物可能会发生这种情况。

拓扑

通过配置组配置的设备可以使用集中策略，也可以向拓扑迁移。实际上，目标是为SD-WAN控制器保持相同的底层控制策略。拓扑是控制策略的最新版本。

请务必注意，不能让控制策略策略引用具有与其关联的拓扑的站点的站点列表，因为它们都配置相同的设置。

当配置不同组件时，可以仅使用数据策略和/或AAR策略的集中策略和拓扑策略。

将设备从集中策略迁移到策略组的步骤：

第 1 步	创建必要的拓扑组件
步骤 2	取消关联集中策略中较旧拓扑列表中的边。
步骤 3	取消站点ID与AAR或数据策略中引用的任何站点列表的关联。 此时，SD-WAN Manager将更新配置发送到控制器，然后控制器删除要迁移的站点的所有活动拓扑配置。 请注意，这可能会导致此时出现意外的流量。
步骤 4	激活拓扑。此时，SD-WAN Manager将更新配置发送到控制器，并修改传输

到边缘设备的所有路由。

注意：虽然拓扑可以与集中策略共存，但建议将边缘设备转换为配置组时保持集中策略（用于拓扑和路由操作）。然后，开始从集中式策略迁移到拓扑，实现修改拓扑和路由控制的功能。

这样做纯粹是为了简化操作并降低操作人员的困惑。

转换工具

范围

“转换工具”可将模板一比一转换为配置组。该工具从SD-WAN Manager实例收集模板，将其转换为配置组（包括功能配置文件和功能包），并将新转换的结构上载到SD-WAN Manager。

* 初步预计2024年10月可在转换工具中将政策转化为政策组。

访问详细信息

该工具的试用版可用。有关详细信息，请访问sdwan-ux-conversion-tool@cisco.com。

操作方法

前提条件

使用该工具之前，请确保SD-WAN Manager正在运行20.12.x。否则，请升级到20.12，然后再继续。

转换工具 workflow

第 1 步	使用思科提供的凭证登录工具。(注意：这些不是CCO凭证。有关详细信息，请访问 sdwan-ux-conversion-tool@cisco.com)。
步骤 2	从主页选择“Conversion Tool”工作流程。 · 如果您以前执行过此工作流程，并且拥有包含已转换配置的JSON文件，则必须选择“从文件上传”工作流程。
步骤 3	登录： 提供SD-WAN Manager IP或URL以及用户凭证。 · 用户必须具有读/写访问权限。

	<ul style="list-style-type: none"> · 端口和子域字段是可选的。
第四步：	<p>导入：</p> <p>点击“Collect”（收集）按钮，从SD-WAN Manager检索所有旧结构（设备模板、功能模板、策略及其相关结构）。</p> <ul style="list-style-type: none"> · 收集完成后，您必须下载包含所有配置的JSON文件。此步骤中必须稍后使用此文件，而不是再次从SD-WAN Manager收集。
第五步：	<p>选择：</p> <p>选择要转换为新等效项的模板和策略。单击“迁移”转换所选结构。</p>
第六步：	<p>转型：</p> <p>此页显示所有新转换的结构。准备就绪后，点击“上传”将这些配置推送到SD-WAN Manager。</p> <ul style="list-style-type: none"> · 如果您尚未准备好推送到SD-WAN Manager，可以将这些转换的配置下载为JSON文件，并在稍后使用“从文件上传”工作流程。
步骤 7.	<p>摘要：</p> <p>此时，在SD-WAN Manager中推送和创建配置。推送配置时，您可以看到进度条。上传完成后，您可以看到上传的配置摘要。</p> <ul style="list-style-type: none"> · 您可以使用“Configuration Groups”、“Feature Profiles”和“Policy Groups”快速链接查看SD-WAN Manager中的新结构。 · 如果发生错误或错误，也可在此步骤中执行回滚。执行回滚操作将删除在此工作流程/会话期间推送到SD-WAN Manager的所有结构。

转换后

您的新构造现在已可以使用。执行“现有部署”(Existing Deployments)部分中的步骤，将设备迁移到新转换的配置组。

考虑事项

- 该工具提供的转换旨在作为指导。在生产环境中部署之前，请进行分析和测试。
- 此工具不考虑配置组的与设备无关的功能。用户可先分析其模板，然后再选择要转换或分析转换的配置组，并相应地关联设备，以从与设备无关的功能中获益。
- 来自旧构造的变量名称和全局值被复制到新转换的构造中。
- 该工具不会将配置推送到设备。执行转换后，用户负责将设备从模板中分离，并将它们关联到

新的配置组。

20.12考虑事项

不能。	项目说明
1	在运行版本低于17.12的边缘上部署配置组时，需要通过CLI加载项配置文件推送DNS配置。
2	创建拓扑需要选择站点，而不是选择在NHM中定义的区域。
3	创建配置组工作流程不会在广域网配置文件中在此VPN中创建VPN512和接口。如果需要，您可以通过编辑Configuration组手动创建此配置。
4	可以复制/复制功能配置文件，策略不受支持。 一组Python脚本可以完成此任务，它们位于： https://github.com/dbrown92700/configGroups/
5	在创建任何与策略配置（本地化策略）相关的功能包之前，策略对象配置文件必须与配置组关联。示例：ACL
6	为接口变量导入CSV会在字符串中插入分号，但失败
7	AppQoE优化（TCP Opt和DRE）和丢失纠正（FEC和Pkt Dup）配置继续使用传统模板/策略。还可以通过配置/策略组中的CLI配置文件进行配置。（20.14用户界面包）
8	适用于SaaS的Cloud OnRamp继续使用传统模板/策略。
9	仅CLI配置文件支持TrustSec/SGT
10	仅CLI配置文件支持UC语音/DSP场/SRST（UI包中从20.13开始）

相关信息

- 思科SD-WAN和云网络YouTube频道

: <https://www.youtube.com/@CiscoSDWANandCloudNetworking>

- UX2.0 -操作简化 : 1.配置单个路由器站点 : <https://www.youtube.com/watch?v=98z-d3knd>
- [思科技术支持和下载](#)

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）。