

Guia de início rápido - Configuração e políticas simplificadas do Catalyst SD-WAN

Contents

[Introdução](#)

[Informações de Apoio](#)

[Summary](#)

[Novas implantações](#)

[Implantações existentes](#)

[Aprimoramentos na experiência do usuário e simplificação operacional](#)

[Defina sua hierarquia de rede e construções de sistema](#)

[Hierarquia de rede](#)

[Construções do sistema](#)

[Fluxos de trabalho](#)

[Grupos de configuração](#)

[Exemplos de Implantação do Grupo de Configuração](#)

[Caso de uso 1: Cliente governamental](#)

[Caso de uso 2: Cliente varejista](#)

[Associado](#)

[Implantar](#)

[Reutilização](#)

[Catálogo de aplicativos](#)

[Grupos de políticas](#)

[Prioridade de aplicativos e SLA](#)

[Modo simples](#)

[Modo Avançado](#)

[Qualidade de Serviço](#)

[Roteamento com reconhecimento de aplicativos](#)

[Política de tráfego](#)

[Segurança incorporada](#)

[Gateway de Internet seguro/Borda de serviço segura](#)

[Segurança de DNS](#)

[Grupos de interesse](#)

[Associar e Implantar](#)

[Políticas localizadas](#)

[Topologia](#)

[Topologia e VPN](#)

[Um mapeamento de nome de VPN para vários IDs de VPN](#)

[Vários nomes de VPN mapeados para o mesmo ID de VPN](#)

[Integração](#)

[Marcação](#)

[Adicionar marca](#)

[Regras de tag no grupo de configuração](#)

[Ilustração](#)

[Implantações existentes](#)

[Grupos de configuração](#)

[Grupos de políticas](#)

[Topologia](#)

[Ferramenta de conversão](#)

[Escopo](#)

[Detalhes de acesso](#)

[How to Use](#)

[Pré-requisito](#)

[Fluxo de Trabalho da Ferramenta de Conversão](#)

[Pós-conversão](#)

[Considerações](#)

[20.12 Considerações](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração e as políticas simplificadas do Catalyst SD-WAN.

Informações de Apoio

Summary

Com o Cisco Catalyst SD-WAN Software Release 20.12/17.12, recomenda-se que os usuários iniciem a migração da configuração tradicional baseada em modelos de dispositivos e recursos para a nova abordagem de configuração baseada em Grupos de Configuração e Grupos de Política. Neste documento, são descritos detalhes importantes para a nova abordagem de configuração.

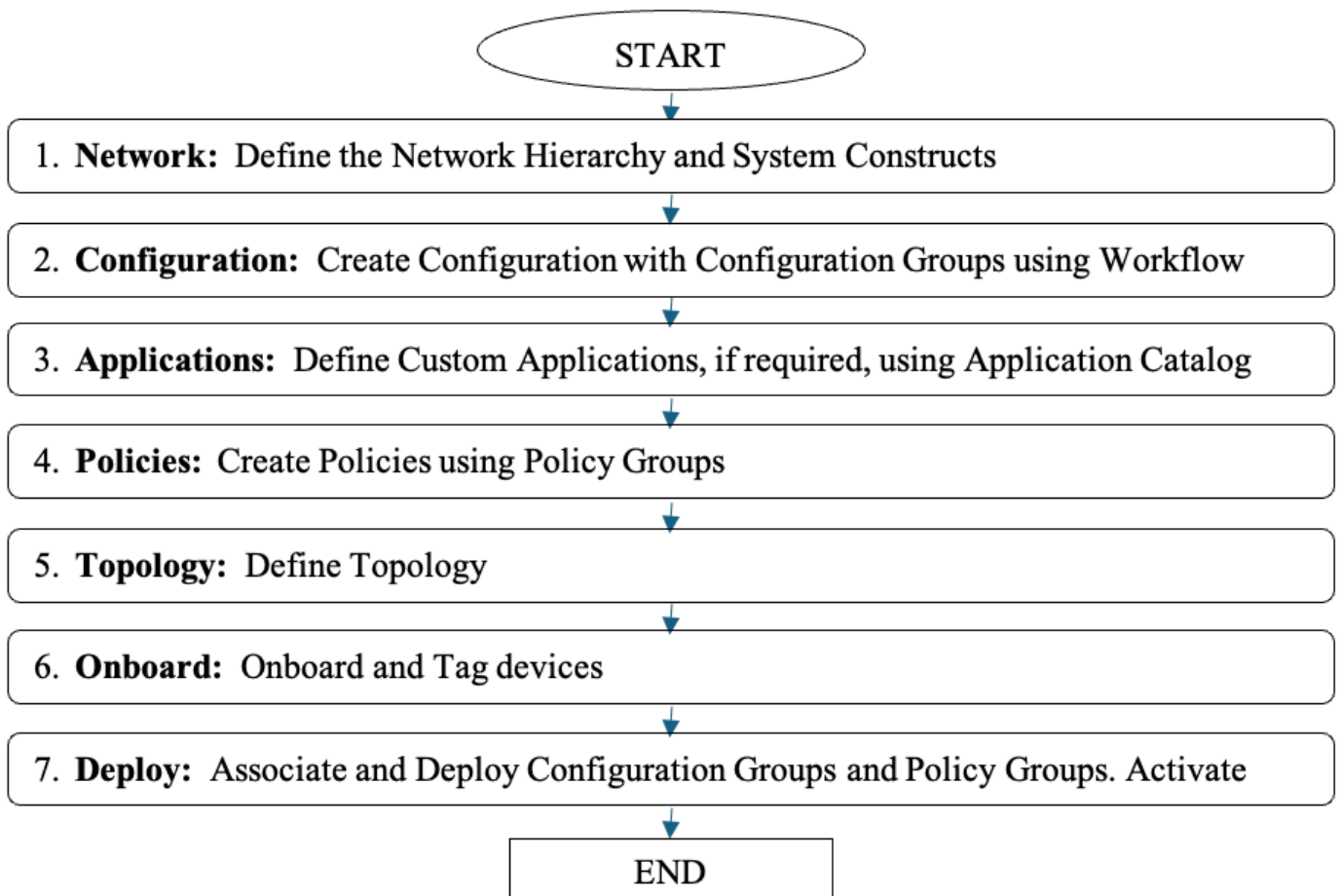
O objetivo principal deste documento é servir como um guia para começar a usar novas construções para configuração, políticas e integração, com a versão 20.12 de ouro. O documento não abrange explicações de características individuais.

Novas implantações

Para utilizar com sucesso a nova abordagem de configuração, você precisa executar estas etapas:

1. Rede: Definir a Hierarquia da Rede e as Construções do Sistema
2. Configuração: criar configuração com grupos de configuração usando o fluxo de trabalho
3. Aplicativos: defina aplicativos personalizados, se necessário, usando o catálogo de aplicativos
4. Políticas: Criar Políticas usando Grupos de Políticas
5. Topologia: Definir Topologia

6. Onboard: dispositivos integrados e de marca
7. Implantar: Associar e Implantar Grupos de Configuração e Grupos de Política. Ative a topologia.



Fluxograma para novas implantações

Implantações existentes

1. Execute as etapas mencionadas na seção [Implantações Existentes](#)
2. Use a [ferramenta de conversão](#) para converter configurações/políticas existentes em novas configurações/políticas

Aprimoramentos na experiência do usuário e simplificação operacional

O Cisco Catalyst SD-WAN oferece uma experiência de usuário aprimorada e simplifica as operações.

- IU comum: uma nova estrutura de UX foi introduzida no Catalyst SD-WAN Manager e em outros produtos da Cisco, para manter a consistência na experiência do usuário e fornecer uma aparência comum entre os produtos.
- Configuração: configuração e criação e implantação de políticas simplificadas com fluxos de trabalho intuitivos baseados em intenção e o uso de padrões inteligentes recomendados pela Cisco.
- Monitoramento: insights detalhados sobre o desempenho e a integridade da rede e dos aplicativos com novos widgets e painéis personalizáveis e aprimorados.

- Solução de problemas: visualizações dinâmicas da topologia de rede e do site, acesso a ferramentas de solução de problemas com base no contexto, relatórios sobre o desempenho da rede e dos aplicativos com base em um agendamento.

Benefícios

Facilidade de uso	Fluxos de trabalho intuitivos e orientados
Subutilização de configuração	Redução da distribuição (agnóstico, reutilização e estrutura do modelo)
Criação de configuração	Mais rápido e fácil com padrões inteligentes
Modificação de configuração	Modificar agora, implantar seletivamente mais tarde
Visibilidade	Novos painéis, aplicativos/sites de monitoramento de desempenho
Orientação para solução de problemas	Topologia do site, orientação sobre ferramentas de solução de problemas

Defina sua hierarquia de rede e construções de sistema

Hierarquia de rede

Fornecer uma noção de "hierarquia", ou seja, Sites, Regiões e Áreas, para a rede. Você pode criar isso com base na sua rede.

Exemplo:



Search



Global (15 of 15 nodes)



AMER



BR1_SanJose



BR2_NewYork



BR6_Dallas



APJC



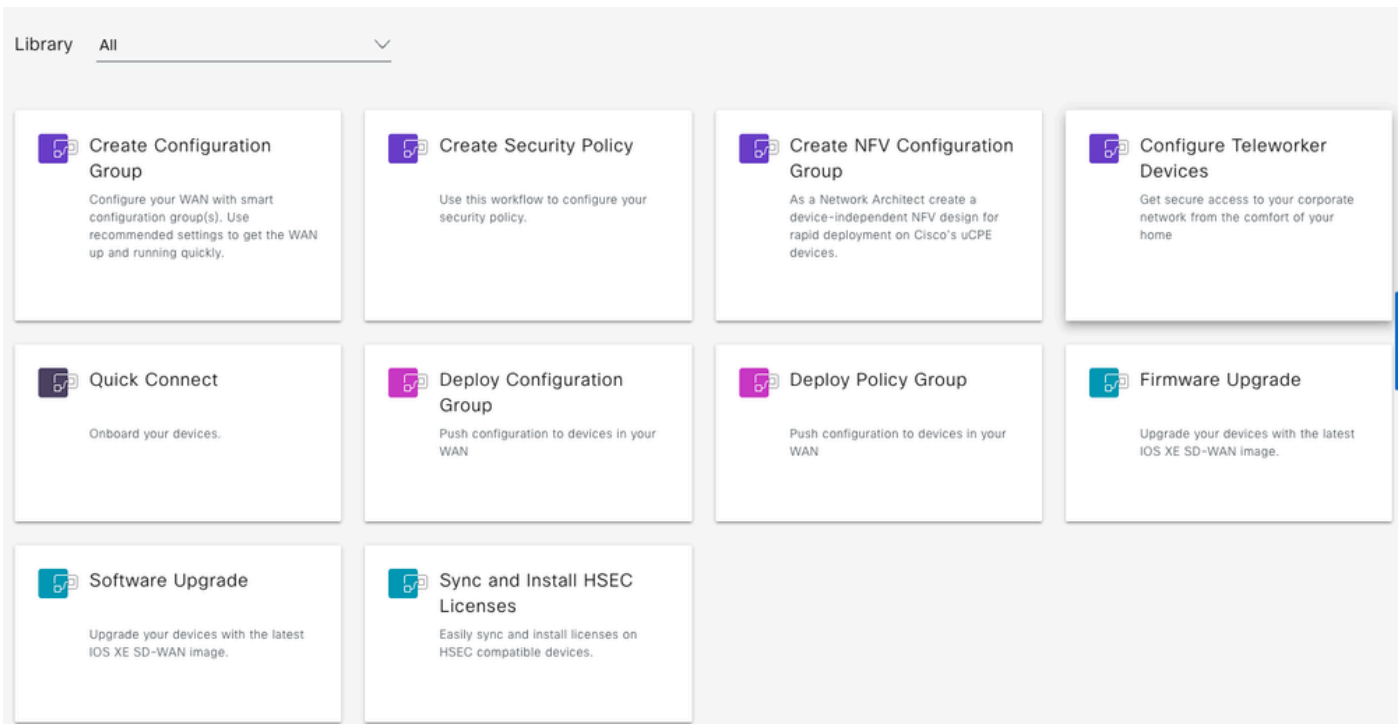
BR3_Mumbai



BR4_Singapore

- A maioria dos botões/configurações está definida com os padrões inteligentes recomendados pela Cisco.
- Os usuários precisam especificar apenas algumas configurações.
- Os botões de configuração avançada estão disponíveis fora do fluxo de trabalho, onde o grupo de configuração pode ser editado manualmente.

Uma Biblioteca de fluxos de trabalho lista todos os fluxos de trabalho disponíveis.

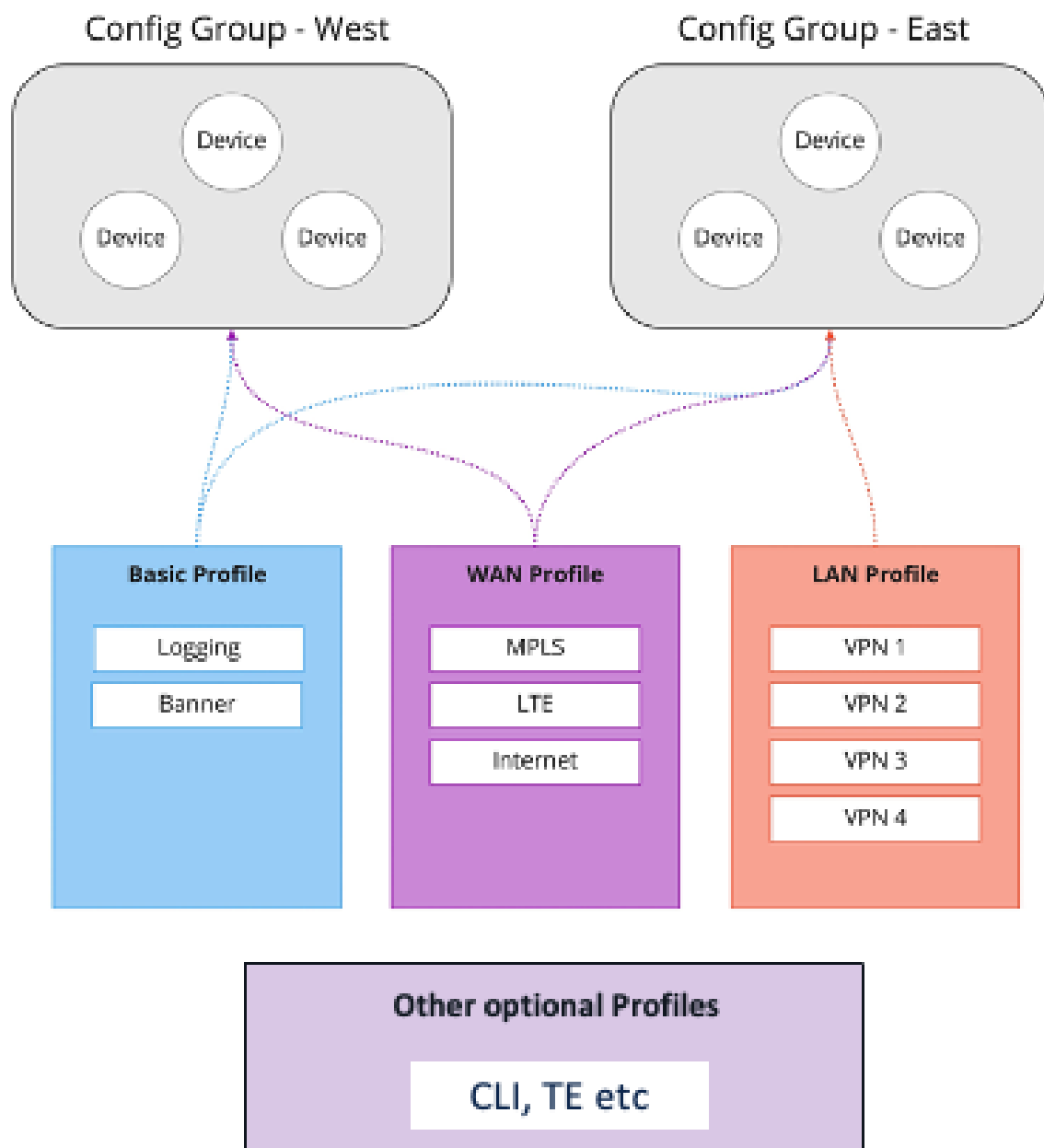


Biblioteca de Fluxos de Trabalho

Grupos de configuração

Os grupos de configuração são uma nova abordagem para a configuração de estrutura que se baseia nos princípios de simplicidade, reutilização e estrutura.

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/config-groups/configuration-group-guide/using-config-groups.html>



Estrutura dos grupos de configuração

Grupos de configuração

- Agrupamento lógico de dispositivos que compartilham uma finalidade comum dentro da WAN.
- O usuário define e pode personalizar esse agrupamento com base em suas necessidades comerciais.

Por exemplo; Leste/Oeste, Américas/APJC/EMEAR, Loja de varejo/Centro de distribuição

Perfis de recurso

- "Baldes" flexíveis de configuração que podem ser compartilhados entre grupos de configuração.
- Crie perfis de recurso com base nos recursos necessários

- Agrupar perfis para concluir a configuração do dispositivo, como blocos de construção
- Construir, salvar e reutilizar

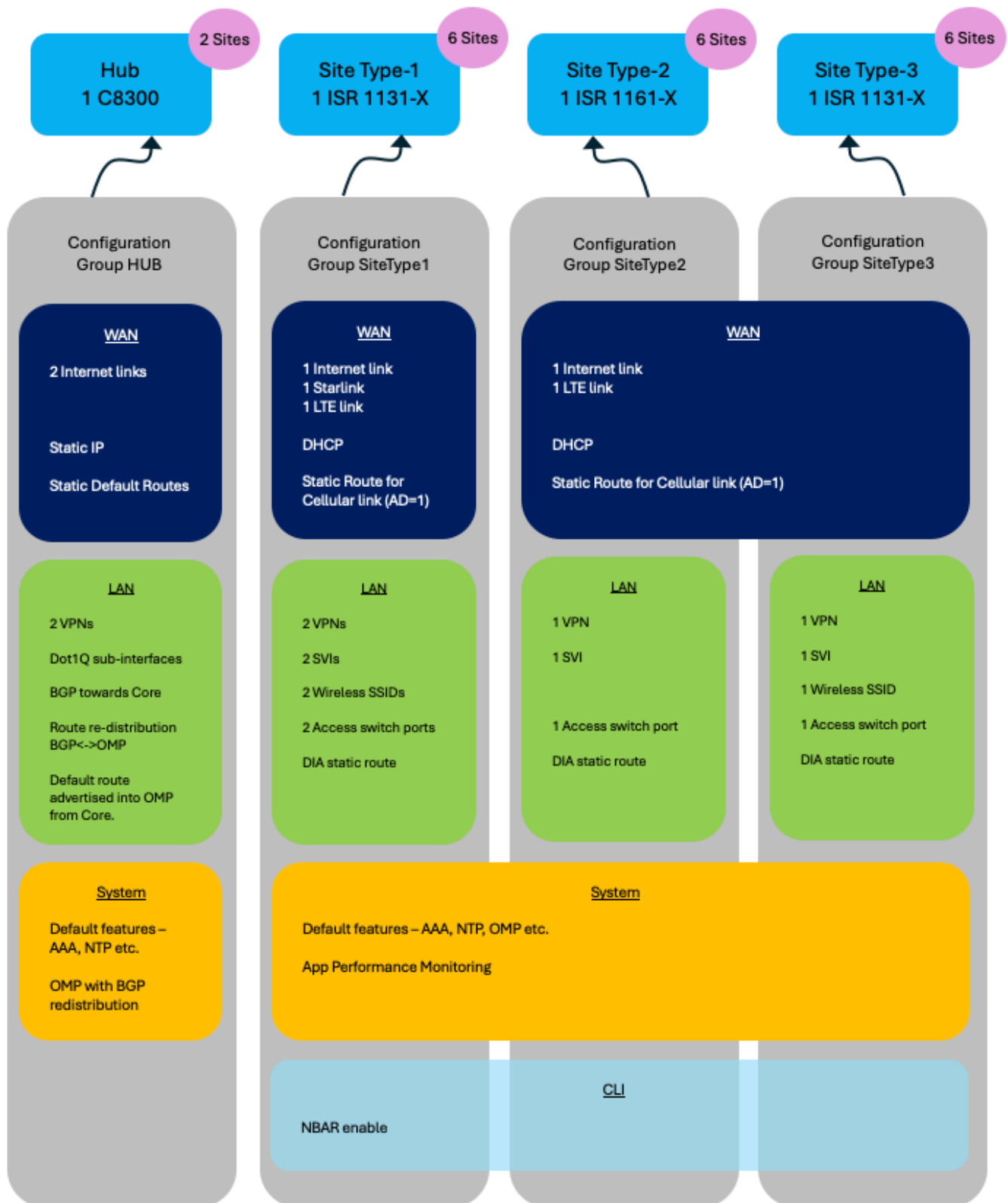
Por exemplo; perfil básico, perfil de WAN, perfil de LAN

Exemplos de Implantação do Grupo de Configuração

Note:

- Os grupos de configuração não dependem do modelo do dispositivo
- Os perfis de recursos podem ser compartilhados entre grupos de configuração

Caso de uso 1: Cliente governamental



Exemplo de caso de uso 1 - Grupos de configuração

HUB do grupo de configuração

Execute o fluxo de trabalho Criar grupo de configuração.



Create Configuration Group

Configure your WAN with smart configuration group(s). Use recommended settings to get the WAN up and running quickly.

Opção Criar Fluxo de Trabalho do Grupo de Configurações

perfil de WAN

2 Internet links

Static IP

Static Default Routes

Exemplo de caso de uso 1 - Perfil de WAN 1

Usando o fluxo de trabalho, a configuração completa do perfil de WAN para este caso de uso pode ser gerada.

Entidades como IP estático real, IP de rota padrão estático/sub-rede/próximo salto e assim por diante, podem ser especificadas como globais ou específicas do dispositivo.

A opção específica do dispositivo pode ser especificada com valores reais durante a implantação do grupo de configuração para os dispositivos.

Perfil de LAN

LAN

2 VPNs

Dot1Q sub-interfaces

BGP towards Core

Route re-distribution

BGP<->OMP

Default route

advertised into OMP

from Core.

pode ser gerada.

- 2 VPNs
- Roteamento BGP em cada uma das VPNs (número AS, prefixos de rede, vizinhos)

Entidades como subinterfaces reais Dot1Q e qualquer outra entidade marcada como específica do dispositivo, podem ser especificadas com valores reais durante a implantação do grupo de configuração para os dispositivos.

NOTE:

A configuração avançada, como redistribuição de rota e anúncio de rota padrão, deve ser configurada após o fluxo de trabalho, editando manualmente o grupo de configuração, assim como as subinterfaces, se forem usadas durante a implantação.

Perfil do sistema

System

Default features –
AAA, NTP etc.

OMP with BGP
redistribution

Usando o fluxo de trabalho, a maior parte da configuração do perfil do sistema para este caso de uso pode ser gerada - OMP, AAA, NTP, Registro e assim por diante.

NOTE:

A configuração avançada, como a redistribuição de OMP-BGP e quaisquer outras alterações nos recursos do sistema, como OMP, AAA, NTP e assim por diante, deve ser configurada após o fluxo de trabalho, editando manualmente o grupo de configuração.

Grupo de Configuração SiteType1

Execute o fluxo de trabalho Criar grupo de configuração.

perfil de WAN

WAN Profile

1 Internet Link

1 Starlink

1 LTE link

DHCP

Static Route for Cellular
link (AD=1)

Exemplo de caso de uso 1 - Perfil de WAN 2

Usando o fluxo de trabalho, a maior parte da configuração do perfil de WAN para este caso de uso pode ser gerada. Interfaces Ethernet para Internet e Starlink. DHCP.

NOTE:

A interface celular do link LTE, incluindo a rota estática, deve ser configurada após o fluxo de trabalho, editando manualmente o grupo de configuração.

LAN Profile

2 VPNs

2 SVIs

2 Wireless SSIDs

2 Access switch ports

DIA static route

Exemplo de caso de uso 1 - perfil de LAN 2

Usando o fluxo de trabalho, algumas das configurações do perfil da LAN para este caso de uso podem ser geradas. 2 VPNs, rota estática DIA.

Entidades como subinterfaces reais Dot1Q e qualquer outra entidade marcada como específica do dispositivo, podem ser especificadas com valores reais durante a implantação do grupo de configuração para os dispositivos.

NOTE:

SVIs, SSIDs sem fio, portas de switch de acesso e assim por diante devem ser configurados após o fluxo de trabalho, editando manualmente o grupo de configuração.

Perfil do sistema

System Profile
**Default features - AAA,
NTP, OMP etc.**
**Application Performance
monitoring**

Exemplo de caso de uso 1 - Perfil de sistema 2

Usando o fluxo de trabalho, a maior parte da configuração do perfil do sistema para este caso de uso pode ser gerada - OMP, AAA, NTP, Registro e assim por diante.

NOTE:

A configuração avançada, como o Monitoramento do desempenho de aplicativos, deve ser configurada após o fluxo de trabalho, editando manualmente o grupo de configuração.

CLI Profile NBAR enable

Exemplo de caso de uso 1 - Perfil CLI 2

Os recursos não suportados via GUI, como a habilitação de App/Flow Visibility (NBAR), podem ser configurados usando um perfil CLI.

Visibilidade de aplicativo/fluxo

Para habilitar a visibilidade de aplicativo e de fluxo, use o perfil/pacote CLI.

(Na versão 20.13 e posterior, ele está disponível em Advanced Settings no Policy Group)

No entanto, na versão 20.12, se uma política de AAR for configurada, a visibilidade de aplicativo/fluxo será habilitada. E configurar isso usando o perfil/pacote CLI, não é necessário.

Grupo de Configuração SiteType2

Execute o fluxo de trabalho Criar grupo de configuração.

perfil de WAN

WAN Profile

1 Internet link
1 LTE link
DHCP
Static Route for Cellular
link (AD=1)

Exemplo de caso de uso 1 - Perfil de WAN 3

Usando o fluxo de trabalho, a maior parte da configuração do perfil de WAN para este caso de uso pode ser gerada. Interface Ethernet para Internet. DHCP.

NOTE:

A interface celular do link LTE, incluindo a rota estática, deve ser configurada após o fluxo de trabalho, editando manualmente o grupo de configuração.

Perfil de LAN

LAN Profile

1 VPN

1 SVI

1 Access switch port

DIA Static route

Exemplo de caso de uso 1 - perfil de LAN 3

Usando o fluxo de trabalho, algumas das configurações do perfil da LAN para este caso de uso podem ser geradas. 1 VPN, rota estática DIA.

Entidades como subinterfaces reais Dot1Q e qualquer outra entidade marcada como específica do dispositivo, podem ser especificadas com valores reais durante a implantação do grupo de configuração para os dispositivos.

NOTE:

O SVI, a porta do switch de acesso e assim por diante devem ser configurados após o fluxo de trabalho, editando manualmente o grupo de configuração.

Perfil do sistema

Igual ao Grupo de Configuração SiteType1

Perfil CLI

Igual ao Grupo de Configuração SiteType1

Grupo de Configuração SiteType3

Execute o fluxo de trabalho Criar grupo de configuração.

Perfil de WAN

Igual ao Grupo de Configuração SiteType2

Perfil de LAN

LAN Profile

1 VPN

1 SVI

1 Wireless SSID

1 Access switch port

DIA Static route

Exemplo de caso de uso 1 - perfil de LAN 4

Usando o fluxo de trabalho, algumas das configurações do perfil da LAN para este caso de uso podem ser geradas. 1 VPN, rota estática DIA.

Entidades como subinterfaces reais Dot1Q e qualquer outra entidade marcada como específica do dispositivo, podem ser especificadas com valores reais durante a implantação do grupo de configuração para os dispositivos.

NOTE:

SVI, SSID sem fio, porta do switch de acesso e assim por diante, devem ser configurados após o fluxo de trabalho, editando manualmente o grupo de configuração.

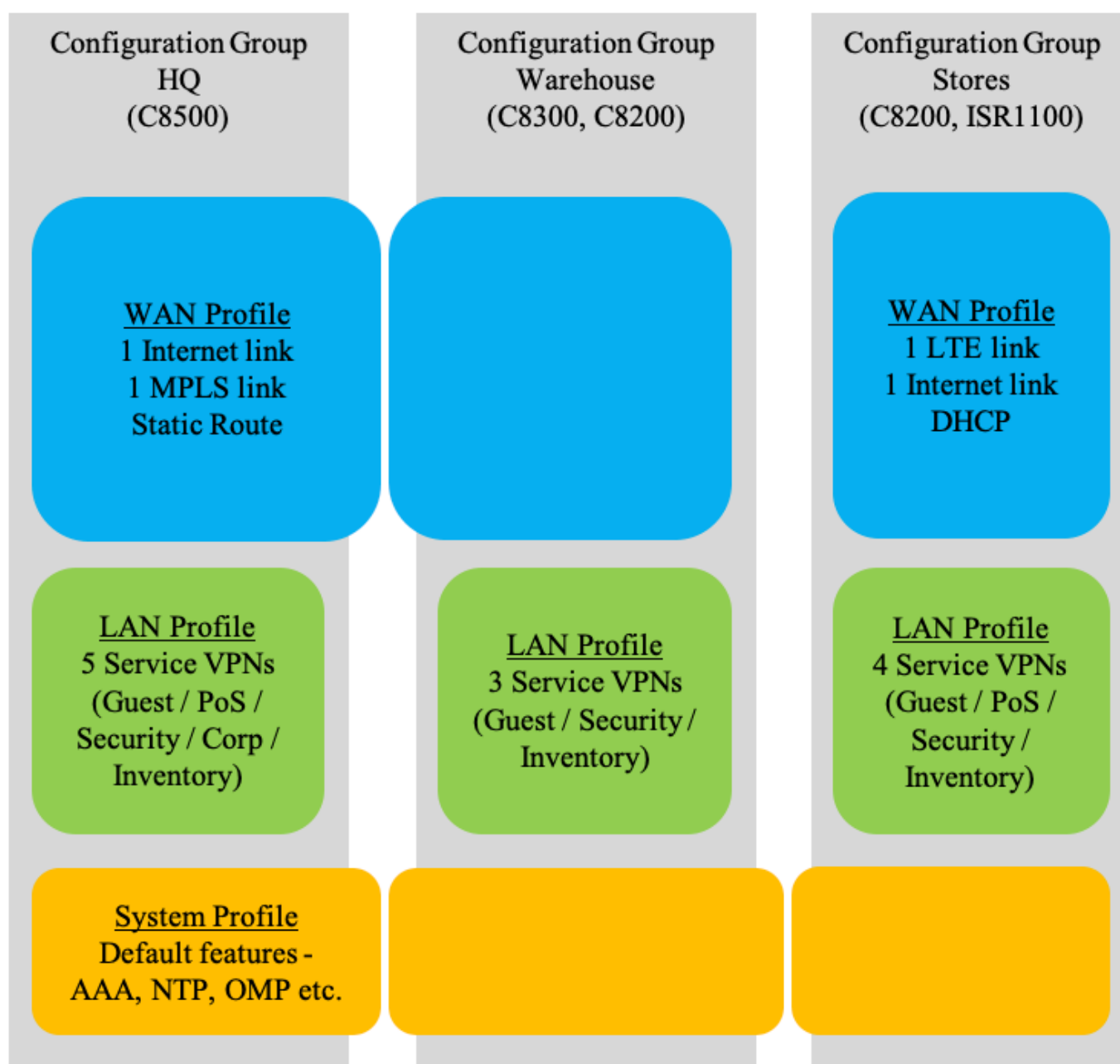
Perfil do sistema

Igual ao Grupo de Configuração SiteType1

Perfil CLI

Igual ao Grupo de Configuração SiteType1

Caso de uso 2: Cliente varejista



Grupo de configuração HQ e Depósito

Execute o fluxo de trabalho Criar grupo de configuração.

perfil de WAN

Usando o fluxo de trabalho, toda a configuração do perfil de WAN para este caso de uso pode ser gerada.

Perfil de LAN

Usando o fluxo de trabalho, toda a configuração do perfil da LAN para este caso de uso pode ser gerada.

Entidades como subinterfaces reais Dot1Q e qualquer outra entidade marcada como específica do dispositivo, podem ser especificadas com valores reais durante a implantação do grupo de configuração para os dispositivos.

Perfil do sistema

Usando o fluxo de trabalho, toda a configuração do perfil do sistema para este caso de uso pode ser gerada.

NOTE:

Se forem necessárias alterações ou se for necessária uma configuração avançada, como o Monitoramento do desempenho dos aplicativos, elas deverão ser configuradas após o fluxo de trabalho, editando manualmente o grupo de configuração.

Armazenamentos de grupos de configuração

Execute o fluxo de trabalho Criar grupo de configuração.

perfil de WAN

Usando o fluxo de trabalho, a maior parte da configuração do perfil de WAN para este caso de uso pode ser gerada.

NOTE:

A interface celular do link LTE, incluindo o roteamento, deve ser configurada após o fluxo de trabalho, editando manualmente o grupo de configuração.

Perfil de LAN

Usando o fluxo de trabalho, toda a configuração do perfil da LAN para este caso de uso pode ser

gerada.

Entidades como subinterfaces reais Dot1Q e qualquer outra entidade marcada como específica do dispositivo, podem ser especificadas com valores reais durante a implantação do grupo de configuração para os dispositivos.

Perfil do sistema

Igual ao Grupo de configuração HQ e Warehouse.

Associado

Na página de edição do grupo de configuração (Configuração -> Grupos de configuração), você pode Associar dispositivos ao grupo de configuração.

Clique em Associar dispositivos e siga as etapas do fluxo de trabalho.

The screenshot shows a web interface for managing configuration groups. At the top, there is a link 'Go Back to Configuration Group list' and the title 'US-WEST-SITES' with an 'Edit' button. Below the title, the description is 'US-WEST-SITES'. There are two tabs: 'Feature Profiles' and 'Associated Devices', with the latter being active. On the left, there is a sidebar with a search bar and a list of items: 'Global', 'SITE_1', and 'SITE_3'. The main content area is titled 'Devices (2)' and contains a table with two rows of device information. The table has columns for Chassis Numbers, Site Name, Hostname, Tags, Config Locked, System IP, Site ID, Device Status, Added by Rule, Last Configured, and Up To Date. The first row shows a device with Site Name 'SITE_1' and System IP '1.1.1.1'. The second row shows a device with Site Name 'SITE_3' and System IP '3.3.3.1'. Above the table, there are buttons for 'Associate Devices', 'Remove Devices', 'Add and Edit Rules', 'Change Device Values', and 'Deploy'. The table is also filtered to show '0 selected' items.

Chassis Numbers	Site Name	Hostname	Tags	Config Locked	System IP	Site ID	Device Status	Added by Rule	Last Configured	Up To Date
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
CBK-01DE1D37-0F1B-F8DF-E71A-9D58D665FD10	SITE_3	Site3-Edge	-	Yes	3.3.3.1	3	In Sync	false	Dec 14, 2023, 6:27:32 AM	True

Associar dispositivo - Grupos de configuração

Implantar

Execute o fluxo de trabalho Implantar grupo de configuração.



Deploy Configuration Group

Push configuration to devices in your WAN

Implantar Fluxo de Trabalho do Grupo de Configuração

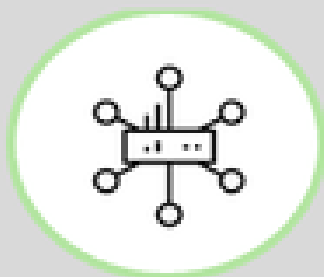
NOTE:

- No Grupo de configuração, a opção Alterar valores do dispositivo altera apenas o valor no banco de dados do Gerenciador e NÃO envia nenhuma alteração para um dispositivo. Se desejar que a alteração ocorra imediatamente, você precisará Implantar as alterações.
- A exportação de valores de variáveis de dispositivo (como um arquivo CSV) pode ser feita no fluxo de trabalho Implantar na etapa Adicionar/revisar configuração de dispositivo.

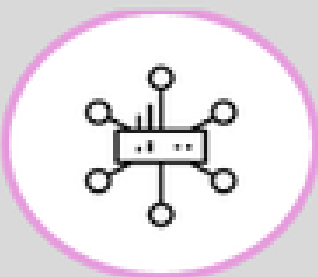
Reutilização

1. Os grupos de configuração não dependem do modelo do dispositivo.

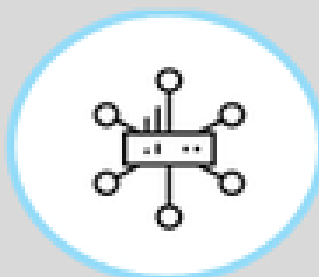
Configuration Group



Device Model 1



Device Model 2



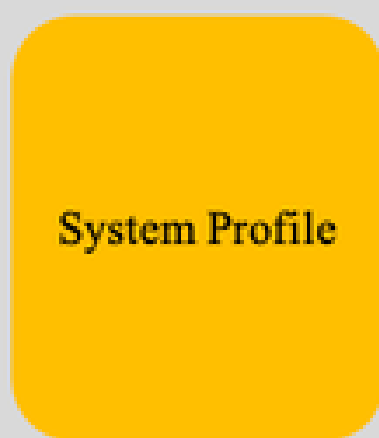
Device Model 3



WAN Profile



LAN Profile



System Profile

Grupo de configuração - Independente do modelo do dispositivo

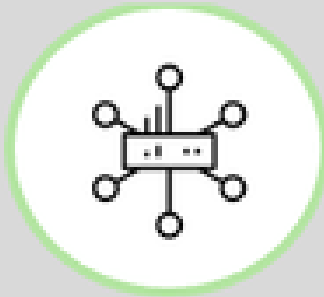
NOTE:

Se uma configuração específica não for suportada em um modelo de dispositivo, o envio do pacote de recursos correspondente não ocorrerá e uma mensagem apropriada será exibida como parte da tarefa de implantação.

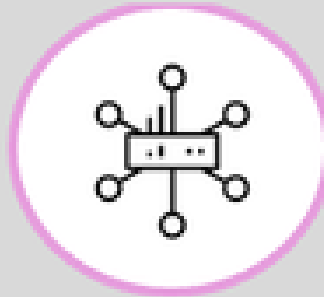
Exemplo: um dispositivo não suporta Wi-Fi, mas o Grupo de configuração contém um pacote Wi-Fi. No momento da implantação, a configuração do pacote Wi-Fi é ignorada e a mensagem da tarefa de implantação informa que o envio da configuração Wi-Fi foi ignorado.

2. Usar variáveis de configuração - valores específicos do dispositivo

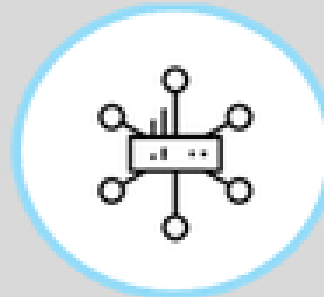
Configuration Group



Device Model 1



Device Model 2



Device Model 3

WAN Profile

LAN Profile

**System
Profile**

Variable 1

Variable 2

Variable 3

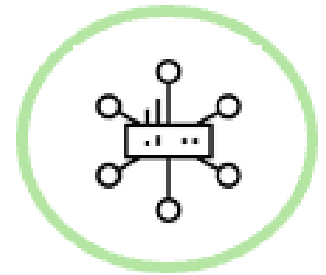
Grupo de Configuração - Variáveis Específicas do Dispositivo

Um perfil de recurso pode ter alguma configuração definida como específica do dispositivo, semelhante às variáveis de modelo.

Exemplo: endereço IP da interface, números de porta, nome da interface e assim por diante.

Esses valores específicos do dispositivo podem ser fornecidos no momento da implantação. E pode ser diferente para dispositivos diferentes.

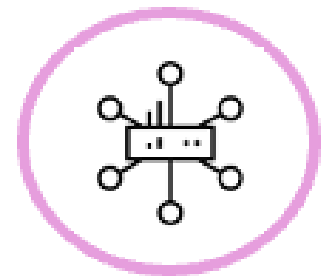
System Profile
Variable 1 = A
Variable 2 = B
Variable 3 = C



Device 1

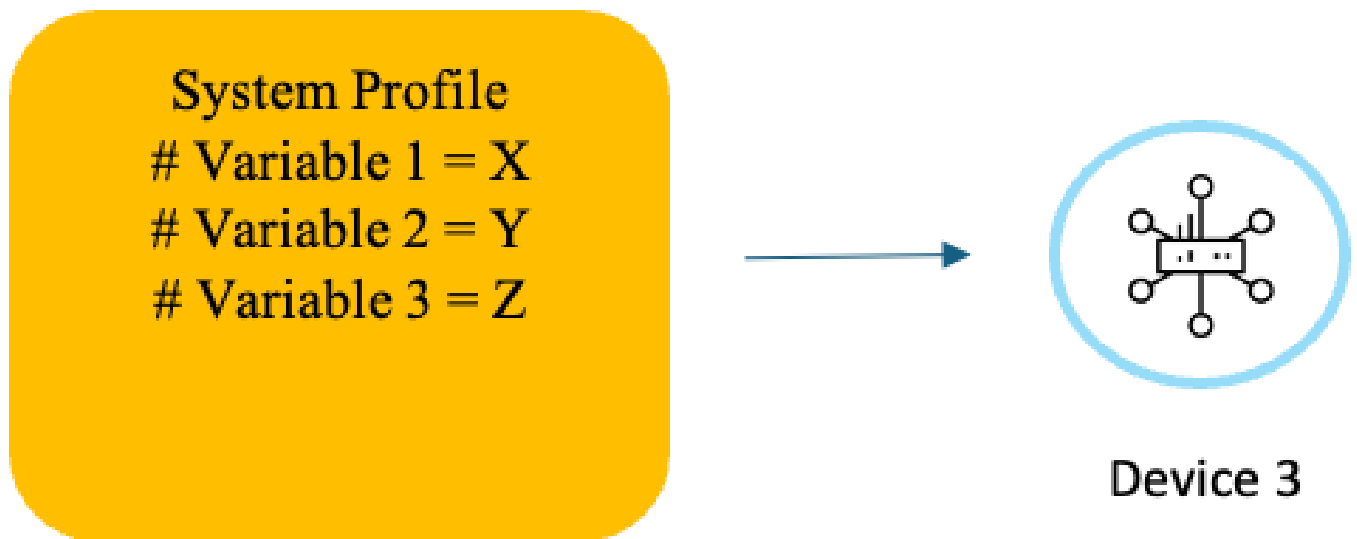
Grupo de Configuração - Variáveis Específicas do Dispositivo Exemplo 1

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



Device 2

Grupo de Configuração - Variáveis Específicas do Dispositivo Exemplo 2



Grupo de Configuração - Variáveis Específicas do Dispositivo Exemplo 3

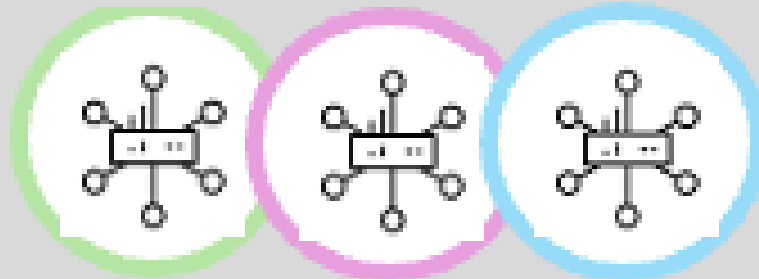
3. Reutilizar perfis de recurso

Os perfis de recurso podem ser reutilizados em todos os grupos de configuração.

Ilustração:

Para vários dispositivos, se as configurações da WAN e do sistema forem as mesmas e diferirem somente na configuração da LAN, por exemplo, os perfis da WAN e do sistema poderão ser reutilizados em seus grupos de configuração enquanto tiverem um perfil de LAN diferente em cada um.

Configuration Group



**WAN
Profile
1**

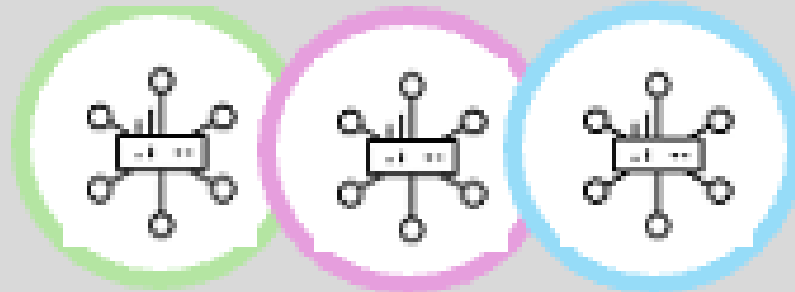
**LAN
Profile
1**

**System
Profile
1**

Reutilizar perfis de recursos - 1

Perfil de LAN 1

Configuration Group



WAN
Profile
1

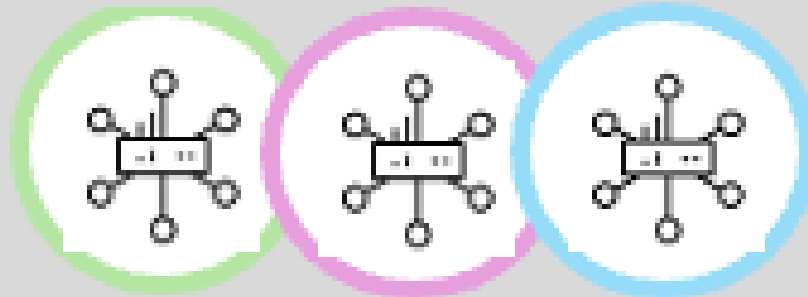
LAN
Profile
2

System
Profile
1

Reutilizar perfis de recursos - 2

Perfil de LAN 2

Configuration Group



**WAN
Profile**

1

**LAN
Profile**

3

**System
Profile**

1

Reutilizar perfis de recursos - 3

Perfil de LAN 3

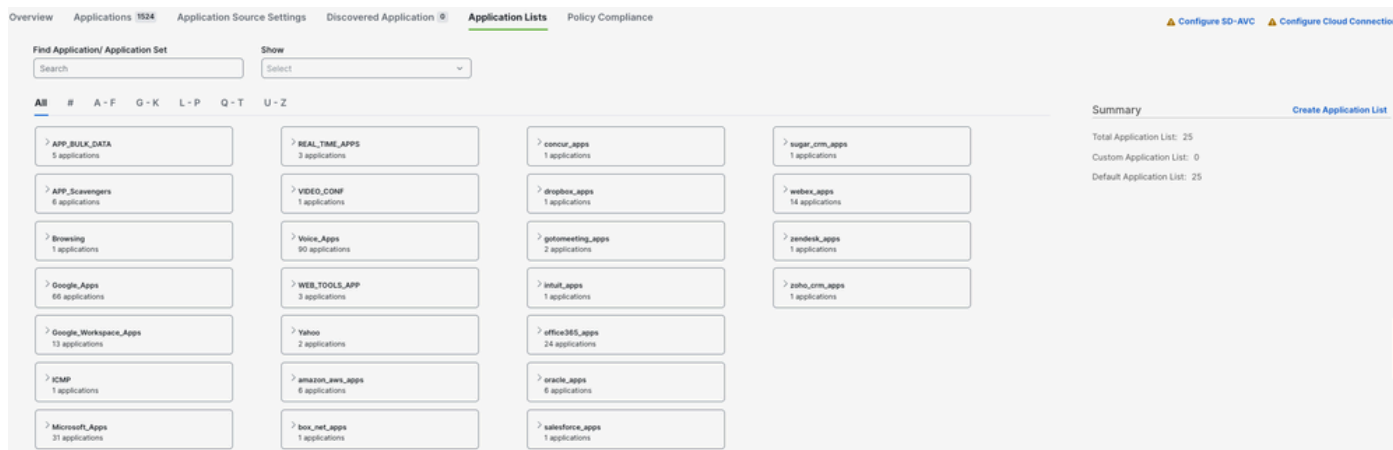
Catálogo de aplicativos

Os dispositivos tradicionais eram capazes de manipular os fluxos de tráfego pela correspondência condicional de endereços IP origem e/ou destino, portas origem/destino e protocolos. À medida que mais e mais aplicativos dependem do DNS ou estão incorporados ao HTTP, é mais difícil identificar com precisão o tráfego de rede no nível do aplicativo.

O mecanismo NBAR (Network Based Application Recognition, reconhecimento de aplicativos baseados em rede) da Cisco tem a capacidade de classificar mais de 1.500 aplicativos, oferecendo aos engenheiros de rede a capacidade de classificar e manipular fluxos de tráfego com mais granularidade. O Catalyst SD-WAN Manager da Cisco tem a capacidade de se conectar a um repositório de aplicativos da Cisco, onde as assinaturas de aplicativos podem ser

atualizadas rapidamente, o que é importante quando os provedores de nuvem mudam de local de hospedagem ou de padrão de tráfego.

O catálogo de aplicativos oferece a capacidade de criar aplicativos personalizados com base na correspondência de nome de servidor, endereço ip, portas ou protocolo. O aplicativo é então definido para uma família de aplicativos, grupo de aplicativos, classe de tráfego e relevância comercial específicos.



Catálogo de aplicativos

Os aplicativos podem ser arrastados e soltos para a relevância comercial e/ou classificação de tráfego apropriada. Após salvar as alterações, as definições são atualizadas no banco de dados.

OBSERVAÇÃO: as classificações de aplicativos são globais, e uma alteração no Catálogo de aplicativos afeta todas as classificações de dispositivos.

Grupos de políticas

Semelhante aos Grupos de configuração, um Grupo de política é um agrupamento de políticas que são implantadas em dispositivos associados ao Grupo de política.

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

O grupo de políticas aborda a criação e a implantação de políticas com base na intenção. Uma interface de usuário e um fluxo de trabalho simplificados tornam a criação de uma política, o agrupamento de políticas e a implantação em dispositivos uma tarefa fácil.

Pré-requisito:

A associação e a implantação do grupo de configuração em um dispositivo é um pré-requisito para a implantação do grupo de política nesse dispositivo.

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

Grupos de políticas

Prioridade de aplicativos e SLA

Com essa intenção de política, você pode especificar:

- Roteamento com reconhecimento de aplicativos e política de SLA
- política de QoS
- Política de dados de tráfego
- política de DIA
- política SIG

Dois modos são fornecidos.

Modo simples

Este é o modo Padrão.

SDWAN Fabric Traffic Policy

Priority	Business Relevance	Preferred Path	When SLA not met	Backup Path
>	Gold	<input type="text" value="Select Preferred Path"/>	<input type="text" value="Default to Best Path"/>	<input type="text" value="Not Applicable"/>
>	Silver	<input type="text" value="Select Preferred Path"/>	<input type="text" value="Default to Best Path"/>	<input type="text" value="Not Applicable"/>
>	Bronze	<input type="text" value="Select Preferred Path"/>	<input type="text" value="Default to Best Path"/>	<input type="text" value="Not Applicable"/>

Internet Offload Traffic

Offload Type	Application List	Fallback to Routing
Secure Internet Gateway	<input type="text" value="Select Application List"/>	<input type="checkbox"/>
Direct Internet Access	<input type="text" value="Select Application List"/>	<input type="checkbox"/>

Apply Policy

Target	Direction	VPN	Interface
<input type="text" value="Enter Direction"/>	<input type="text" value="Select VPN"/>	<input type="text" value="Enter Interfaces"/>	<input type="text" value="Enter Interfaces"/>

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

Modo simples

Isso fornece uma maneira rápida e fácil de definir a prioridade de aplicativos e o SLA para sua rede.

NOTE:

1. A ação de política padrão é DROP
2. Os critérios de correspondência podem ser Aplicativos apenas. Se precisar de prefixos, use o modo Avançado

Modo Avançado

Este é um modo completo e flexível.

Search Traffic Policy [Add Traffic Policy](#)

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 Go to: / 1

SLA Class **QoS Queue**

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

NOTE:

1. A ação de política padrão é DROP

2. Lista de Aplicativos e Classe de Tráfego são essencialmente uma lista de Aplicativos.

Qualquer um deles pode ser usado para corresponder a uma lista de aplicativos. O mapeamento de aplicativos para classe de tráfego pode ser feito no catálogo de aplicativos.

O modo Simples gera regras usando qualquer uma ou ambas, enquanto o modo Avançado fornece apenas a Lista de Aplicativos.

Qualidade de Serviço

Na opção QoS Queue, você pode adicionar uma política de QoS:

Advanced Layout



SLA Class

QoS Queue

[⊕ Add QoS Policy](#)

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

Adicionar política de QoS

Queueing Model

4 Queues ^

Policy Name *

Target Interface *

Value

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)

Bandwidth

Modelos de enfileiramento

Em seguida, você pode definir a política de dados de tráfego (Adicionar política de tráfego).

Adicione regras para corresponder ao tráfego desejado e redirecione para as classes de encaminhamento apropriadas.

Policies > Application Priority & SLA

Basic_4Queue_QoS_Policy (Total Traffic Policy: 1)

Additional Settings Advanced Layout

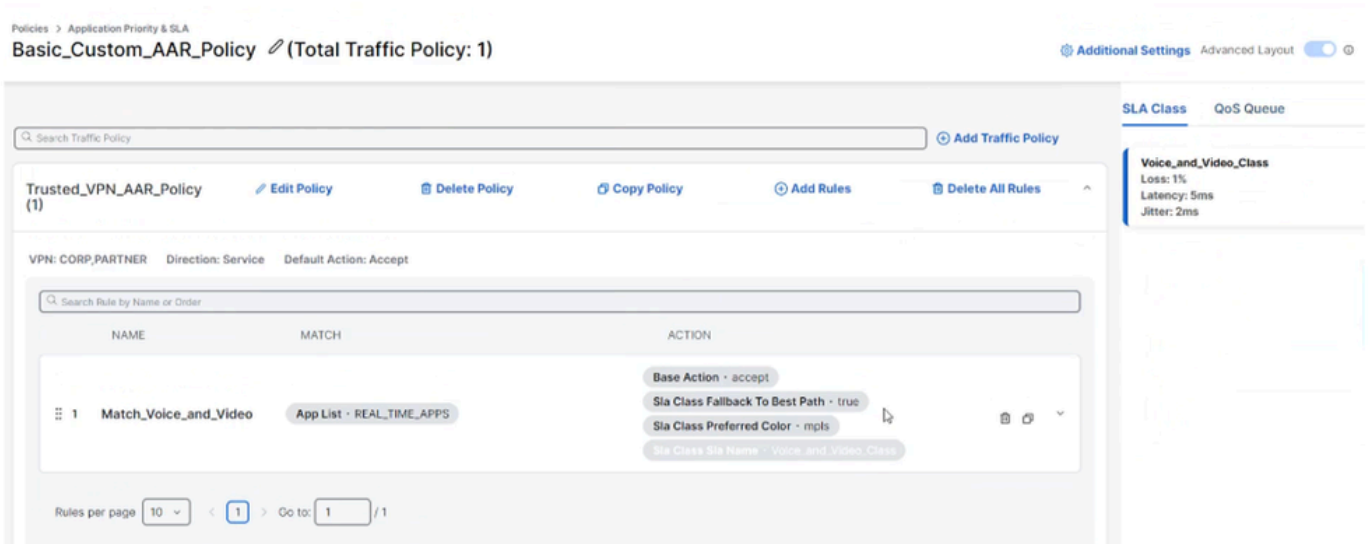
NAME	MATCH	ACTION
1 Match_Voice_Traffic	Dscp - 46	Base Action - accept Count - voice Forwarding Class - VOICE Log - true
2 Match_Critical_Apps	App List - Microsoft_Apps	Base Action - accept Count - critical_apps Forwarding Class - CRITICAL_DATA Log - true
3 Match_Bulk_Data_Traffic	Destination Data Prefix 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%

Política de QoS 2

Roteamento com reconhecimento de aplicativos

Você pode definir classes de SLA e usá-las em uma política de tráfego para realizar a intenção de uma política de AAR.



Política AAR

Visibilidade de aplicativo/fluxo

Para habilitar a visibilidade de aplicativo e a visibilidade de fluxo, use o perfil/pacote CLI no grupo de configuração.

(Na versão 20.13 e posterior, ele está disponível em Advanced Settings no Policy Group)

No entanto, na versão 20.12, se uma política de AAR for configurada, a visibilidade de aplicativo/fluxo será habilitada. E configurar isso usando o perfil/pacote CLI, não é necessário.

Política de tráfego

A política de tráfego também pode ser usada para criar uma política DIA, redirecionamento SIG e assim por diante. Adicione regras conforme necessário.

Search Traffic Policy 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

Search Rule by Name or Order

NAME	MATCH	ACTION
1 Rule1		

Sequence: 1 Name: Rule1 Protocol: IPv4

Match [Add Match](#)

Action [Add Action](#)

Base Action

Accept Drop

Cancel Save Match and Actions

Política de tráfego

NOTE:

Se uma Prioridade de aplicativo e política de SLA for criada no modo simples e depois transferida para o modo Avançado, algumas opções de Correspondência não estarão disponíveis para seleção. Exemplo: o prefixo dos dados de destino está esmaecido. Para disponibilizar essas opções, altere o Protocolo de BOTH para IPv4 ou IPv6, conforme necessário.

Segurança incorporada

Define a política de segurança para NGFW, IPS, malware e filtragem de conteúdo integrados

Gateway de Internet seguro/Borda de serviço segura

Define as configurações necessárias para estabelecer túneis para entidades de segurança e conteúdo baseado em nuvem, como o Cisco Secure Access.

NOTE:

Com a abordagem de configuração herdada, ela estava disponível como um Modelo de recurso.

Segurança de DNS

Defina configurações para permitir o uso de serviços de segurança DNS baseados em nuvem para filtragem de conteúdo.

Grupos de interesse

Defina as listas de objetos a serem usadas em suas políticas. Exemplo: listas de aplicativos, listas de VPN, listas de sites, lista de prefixos e assim por diante.

Além disso, para políticas de segurança, defina seus perfis como perfis de inspeção avançada, política de criptografia SSL e assim por diante.

The screenshot shows the 'Security' tab in the Palo Alto Networks configuration interface. The left sidebar lists various object types under the 'Objects' category, with 'Application' selected. The main content area displays a table of applications with columns for 'Name' and 'Entries'. A search bar is located at the top of the table area.

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

3 Records

Grupos de Políticas - Grupos de Interesse

Associar e Implantar

Semelhante aos Grupos de configuração, associe dispositivos ao Grupo de política e implante.

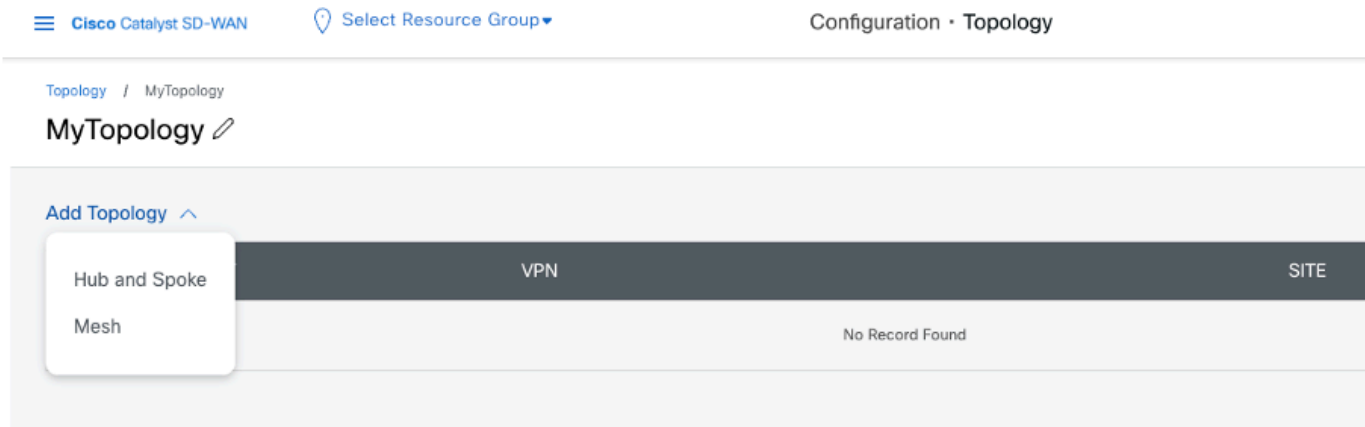
Políticas localizadas

As políticas localizadas, como ACL, política de rota, política de acesso de dispositivo e assim por diante, são definidas nos grupos de configuração.

Topologia

Defina sua topologia de rede.

Comece com uma malha completa ou Hub-n-Spoke e personalize-a, se necessário.



menu Topologia

Topologia e VPN

Lembre-se dessas alterações de design ao criar a topologia e especificar as VPNs.

O novo design permite o mapeamento dinâmico do nome da VPN para o ID da VPN, em vez do mapeamento 1:1.

Um mapeamento de nome de VPN para vários IDs de VPN

Ilustração:

Digamos que haja uma VPN com o nome Corporate em dois grupos de configuração diferentes.

Um tem o ID de VPN 10 e o outro tem o ID de VPN 20.

A lista VPN do fluxo de trabalho da topologia mostra apenas uma instância de VPN corporativa.

Depois de selecionar Corporate VPN, o SD-WAN Manager determina as IDs de VPN com base na topologia.

Digamos que existam 2 dispositivos em 2 locais:

1. Dispositivo1 no local 100 com Empresa como VPN 10
2. Dispositivo2 no local 200 com Empresa como VPN 20

Se o site 100 e o site 200 fizerem parte da topologia, o SD-WAN Manager criará uma lista de VPN que terá IDs de VPN (10 e 20).

Se apenas o site 100 fizer parte da topologia, o SD-WAN Manager criará uma lista de VPN que terá apenas o ID de VPN 10.

Se apenas o site 200 fizer parte da topologia, o SD-WAN Manager criará uma lista de VPN que terá apenas o ID de VPN 20.

Vários nomes de VPN mapeados para o mesmo ID de VPN

Você pode configurar várias políticas de Topologia com o mesmo nome de VPN que são mapeadas para diferentes IDs de VPN em sites diferentes.

O SD-WAN Manager determina o mapeamento real com base em qual topologia está associada a quais sites.

Ilustração:

Dois usuários podem criar dois grupos de configuração diferentes.

Um especifica o ID de VPN 100 como Finance VPN e o outro especifica como Engineering VPN.

Em seguida, eles podem criar a topologia usando seus respectivos nomes de VPN.

Integração

Para integrar seus roteadores físicos, use o Fluxo de trabalho de conexão rápida.

Usando esse fluxo de trabalho, predefina o nome do host, o IP do sistema e o nome/ID do site para os dispositivos a serem integrados. O gerenciador gera automaticamente esses arquivos, mas você pode modificá-los se desejar. Você também pode marcar os dispositivos que podem ser usados para associar automaticamente os dispositivos aos grupos de configuração.

Durante o processo de onboarding do ZTP PnP, os dispositivos estabelecem as conexões de túnel do plano de controle para o gerenciador SD-WAN. O SD-WAN Manager agora envia a configuração de estrutura predefinida para os dispositivos e os dispositivos se juntam à estrutura SD-WAN.



Quick Connect

Onboard your devices.

Fluxo de trabalho de conexão rápida



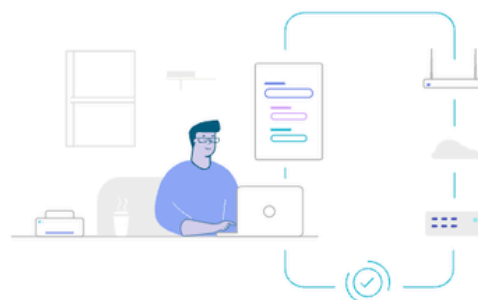
Welcome to Quick Connect

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

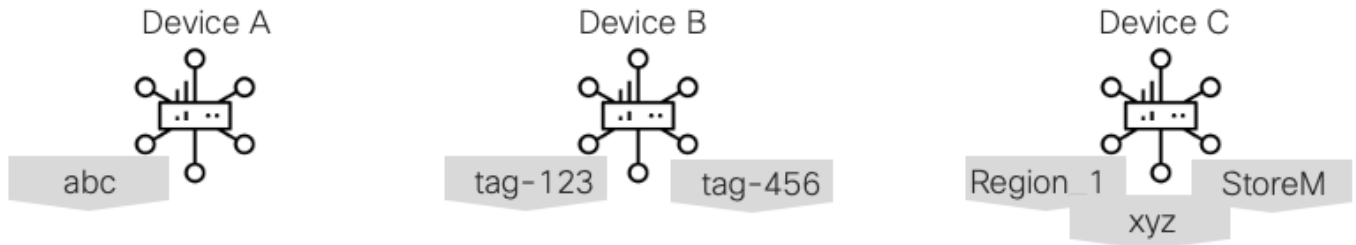
Descrição do fluxo de trabalho de conexão rápida

Marcação

Os dispositivos podem ser associados a marcas definidas pelo usuário.

As marcas podem ser usadas para agrupar, descrever, localizar ou gerenciar dispositivos.

As tags permitem o agrupamento de dispositivos que podem ser usados em outros recursos.



Exemplos de marcação

Exemplo: associação de grupos de configuração a dispositivos.

As regras do grupo de configuração podem ser definidas para permitir que dispositivos com marcas específicas sejam automaticamente associados a esse grupo de configuração.

Adicionar marca

Em Configuration->Devices (Configuração->Dispositivos), as marcas podem ser criadas/adicionadas/removidas dos dispositivos.

Regras de tag no grupo de configuração

Na página Grupo de configuração -> Dispositivos associados, as regras de marcação podem ser adicionadas/editadas.

Ilustração

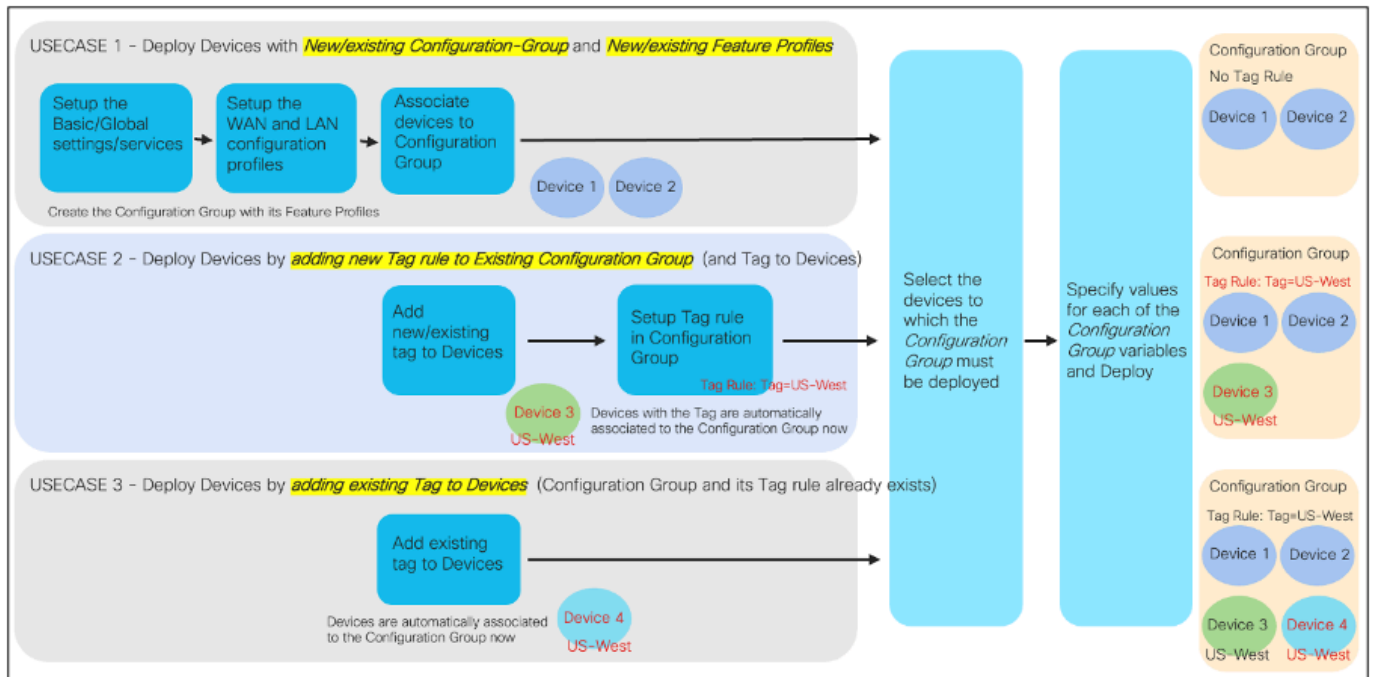


Ilustração de marcação

Implantações existentes

Na rede SD-WAN, os dispositivos que usam a configuração e as políticas herdadas podem coexistir com os dispositivos que usam a configuração e as políticas simplificadas.

Esta seção oferece algumas recomendações para clientes que desejam aproveitar a configuração e as políticas simplificadas. Esta seção oferece algumas recomendações.

A primeira etapa é que os dispositivos precisam ser migrados de Modelos de dispositivo para Grupos de configuração. Depois disso, os grupos de política e/ou a topologia podem ser implantados.

Grupos de configuração

Os modelos de dispositivos e os grupos de configuração fornecem a configuração do dispositivo de borda. Por isso, é fácil que ocorra a coexistência. As etapas para migrar de um modelo de dispositivo para um grupo de configuração são:

Passo 1	Extraia uma cópia dos valores de dispositivo dos modelos de dispositivo. Isso é feito a partir dos Modelos à Configuração, clique nas Elipses (...) à direita do grupo de dispositivos e selecione 'Exportar CSV'.
Passo 2	Crie um grupo de configuração (manualmente ou com a ferramenta de conversão).

Etapa 3	Desanexe o modelo do dispositivo. Nesse momento, o dispositivo mantém a configuração no ponto de conexão, mas não recebe nenhuma alteração futura feita no modelo do dispositivo (ou em qualquer modelo de recurso de componente).
Passo 4	Associe o(s) dispositivo(s) ao novo grupo de configuração.
Etapa 5	Implante os dispositivos associados ao grupo de configuração. Para facilitar esse processo, abra o arquivo CSV exportado e altere os cabeçalhos de coluna CSV para corresponder às novas variáveis do grupo de configuração.
Etapa 6	Após a tela de entrada variável de dispositivo, você pode visualizar a configuração do dispositivo. Isso fornece uma visualização de quais partes do grupo de configuração não correspondem à instância anterior ou de quais variáveis foram alteradas em relação ao Modelo de dispositivo.

A manutenção de um esquema de nomenclatura consistente para variáveis simplifica as configurações específicas do dispositivo. Se todos os valores do dispositivo estiverem em um único CSV, você só terá que renomear os cabeçalhos das colunas uma vez.

OBSERVAÇÃO: existe um script Python que funciona com arquivos CSV para Modelos de Dispositivo ou Grupos de Configuração para consolidar e alfabeticar os cabeçalhos de coluna. O script está disponível aqui:

<https://github.com/BradEdgeworth/CSVMerger>

Grupos de políticas

Os dispositivos configurados por meio de grupos de configuração podem usar uma política centralizada ou migrar para um grupo de política, mas não ambos ao mesmo tempo para o mesmo aplicativo. Em essência, o objetivo é manter a mesma política subjacente para os dispositivos de borda. Os grupos de política combinam as políticas AAR e de dados originais em um único componente de Prioridade de aplicativo e SLA PG. Basicamente, estamos apenas mudando a forma como a configuração das políticas é criada (mas não enviada para o gerenciador SD-WAN).

É importante observar que você não pode ter uma política de dados ou de AAR referindo-se a uma lista de sites com um site que tenha o componente Prioridade de aplicativos e SLA, pois ambos definem a mesma configuração.

É possível ter uma política centralizada com apenas uma política de controle que faça referência a um site que use um grupo de política com prioridade de aplicativo e SLA), à medida que eles

configuram diferentes componentes de uma política centralizada.

As etapas para migrar um dispositivo de uma política centralizada para um grupo de políticas envolvem estas etapas:

Passo 1	Crie os componentes do grupo de políticas necessários (Prioridade de aplicativos e SLA, Segurança incorporada, Gateway de Internet seguro/Borda de serviço seguro, Segurança DNS.
Passo 2	Crie o grupo de políticas e associe os componentes necessários.
Etapa 3	Desassocie a ID do site de quaisquer SiteLists que sejam referências em AAR ou Políticas de dados. Neste momento, o SD-WAN Manager envia a configuração atualizada para os controladores que, em seguida, removem qualquer instrução de política de dados ativa do(s) dispositivo(s) de borda. Observe que isso pode causar fluxos de tráfego não intencionais neste momento.
Passo 4	Associe os dispositivos ao grupo de políticas e salve o grupo de políticas.
Etapa 5	Implante o grupo de políticas nos dispositivos selecionados. Neste momento, o SD-WAN Manager envia configurações atualizadas para os dispositivos de borda (para QoS/SIG) e os controladores; para que os controladores possam enviar políticas de dados atualizadas para os dispositivos de borda.

Observação: embora os grupos de política possam coexistir com uma política centralizada, é recomendável permanecer com uma política centralizada (para AAR e políticas de dados) ao converter dispositivos de borda para grupos de configuração. Em seguida, nesse ponto, inicie a migração da política centralizada para os grupos de política para funcionalidade no componente Prioridade de aplicativo e SLA.

Isso é feito por pura simplicidade e para reduzir a confusão entre a equipe operacional.

NOTE:

O mecanismo de grupo de política armazena itens em um formato diferente. Portanto, uma lista de prefixos usada em uma política centralizada deve ser recriada no grupo de

políticas. Isso pode acontecer com outras coisas, como listas de sites, etc.

Topologia

Os dispositivos configurados por meio de grupos de configuração podem usar uma política centralizada ou migrar para uma topologia. Em essência, o objetivo é manter a mesma política de controle subjacente para os controladores SD-WAN. Topologia é a última iteração das Políticas de Controle.

É importante observar que você não pode ter uma política de controle referenciando uma lista de sites com um site que tenha uma topologia associada a ela, pois ambos definem a mesma configuração.

É possível ter uma política centralizada com apenas uma política de dados e/ou AAR e uma política de topologia à medida que eles configuram componentes diferentes.

Etapas para migrar um dispositivo de uma política centralizada para um grupo de políticas:

Passo 1	Criar os componentes de Topologia necessários
Passo 2	Desassocie os lados da Lista de Topologia mais antiga na Política centralizada.
Etapa 3	Desassocie a ID do site de qualquer Lista de sites referenciada no AAR ou nas Políticas de dados. Neste momento, o SD-WAN Manager envia a configuração atualizada para os controladores, que então removem qualquer configuração de topologia ativa para os locais que estão sendo migrados. Observe que isso pode causar fluxos de tráfego não intencionais neste momento.
Passo 4	Ative a topologia. Neste momento, o SD-WAN Manager envia configurações atualizadas para os controladores e modifica quaisquer rotas que estão sendo transmitidas para dispositivos de borda.

Observação: embora a topologia possa coexistir com uma política centralizada, é recomendável permanecer com uma política centralizada (para topologia e manipulação de rota) ao converter dispositivos de borda para grupos de configuração. Em seguida, nesse ponto, inicie a migração de Política centralizada para Topologia para obter a funcionalidade de modificação de topologias e manipulação de roteamento.

Isso é feito por pura simplicidade e para reduzir a confusão entre a equipe operacional.

Ferramenta de conversão

Escopo

A ferramenta de conversão executa uma conversão de modelos 1 para 1 em grupos de configuração. A ferramenta coleta os modelos de uma instância do SD-WAN Manager, os converte em grupos de configuração (incluindo perfis de recursos e pacotes de recursos) e carrega as construções recém-convertidas no SD-WAN Manager.

* Espera - se que a conversão das políticas em grupos de políticas esteja disponível na ferramenta de conversão em outubro de 2024.

Detalhes de acesso

Uma versão beta da ferramenta está disponível. Entre em contato com sdwan-ux-conversion-tool@cisco.com para obter mais informações.

How to Use

Pré-requisito

Antes de usar a ferramenta, certifique-se de que o seu SD-WAN Manager esteja executando 20.12.x. Caso contrário, atualize para a versão 20.12 antes de continuar.

Fluxo de Trabalho da Ferramenta de Conversão

Passo 1	Entre na ferramenta usando as credenciais fornecidas pela Cisco. (Observação: essas não são credenciais do CCO. Acesse sdwan-ux-conversion-tool@cisco.com para obter mais detalhes).
Passo 2	Selecione o fluxo de trabalho "Ferramenta de conversão" na página inicial. · Se você executou anteriormente esse fluxo de trabalho e tem o arquivo JSON com as configurações convertidas, você deve selecionar o fluxo de trabalho 'Carregar de um arquivo'.
Etapa 3	Login: Forneça seu IP ou URL do SD-WAN Manager junto com as credenciais do

	<p>usuário.</p> <ul style="list-style-type: none"> · O usuário deve ter acesso de leitura/gravação. · Os campos de porta e subdomínio são opcionais.
Etapa 4.	<p>Importar:</p> <p>Clique no botão "Coletar" para recuperar todas as construções legadas (modelos de dispositivos, modelos de recursos, políticas e suas construções associadas) do SD-WAN Manager.</p> <ul style="list-style-type: none"> · Depois de coletado, você deve fazer download do arquivo JSON que contém todas as configurações. Este arquivo deve ser usado durante esta etapa posteriormente, em vez de ser coletado novamente no Gerenciador SD-WAN.
Etapa 5.	<p>Selecione:</p> <p>Selecione os modelos e políticas que deseja converter em seus novos equivalentes. Clique em "Migrar" para converter as construções selecionadas.</p>
Etapa 6.	<p>Transformação:</p> <p>Esta página mostra todas as construções recém-convertidas. Quando estiver pronto, clique em "Upload" para enviar essas configurações para o SD-WAN Manager.</p> <ul style="list-style-type: none"> · Caso ainda não esteja pronto para enviar para o SD-WAN Manager, você poderá baixar essas configurações convertidas como um arquivo JSON e usar o fluxo de trabalho 'Carregar de um arquivo' posteriormente.
Passo 7.	<p>Resumo:</p> <p>No momento, as configurações estão sendo enviadas e criadas no SD-WAN Manager. À medida que as configurações são enviadas, você pode ver a barra de progresso. Quando o carregamento estiver concluído, você poderá ver o resumo das configurações carregadas.</p> <ul style="list-style-type: none"> · Você pode usar os links rápidos "Grupos de configuração", "Perfis de recursos" e "Grupos de políticas" para visualizar as novas construções no seu gerenciador SD-WAN. · Em caso de erro, a reversão também está disponível nesta etapa. A execução de uma reversão remove todas as construções enviadas ao

Gerenciador SD-WAN durante esse fluxo de trabalho/sessão.

Pós-conversão

Seus novos construtores agora estão prontos para uso. Execute as etapas na seção 'Implantações existentes' para migrar seus dispositivos para os grupos de configuração recém-convertidos.

Considerações

- As conversões fornecidas pela ferramenta servem como orientação. Analise e teste antes de implantar em um ambiente de produção.
- A ferramenta não considera a capacidade de grupos de configuração independente de dispositivos. Os usuários podem analisar seus modelos antes de selecionar quais converter ou analisar os grupos de configuração convertidos e associar os dispositivos adequadamente para se beneficiar do recurso independente de dispositivo.
- Nomes de variáveis e valores globais de construções legadas são copiados para as construções recém-convertidas.
- A ferramenta não envia a configuração aos dispositivos. Após realizar as conversões, o usuário é responsável por desconectar dispositivos dos modelos e associá-los aos novos grupos de configuração.

20.12 Considerações

No.	Descrição do Item
1	A configuração DNS precisa ser enviada por meio do Perfil de Complemento CLI ao implantar o Grupo de Configuração na Borda executando uma versão anterior à 17.12.
2	A criação da Topologia requer a seleção de sites em vez de escolher uma área definida no NHM.
3	O fluxo de trabalho Criar grupo de configuração não cria uma VPN512 e uma interface nesta VPN, no perfil da WAN. Se precisar disso, você pode criá-lo manualmente editando o grupo de configuração.
4	Capacidade de copiar/duplicar perfis de recursos, política não suportada. Um conjunto de scripts Python pode realizar essa tarefa e está localizado: https://github.com/dbrown92700/configGroups/

5	Um perfil de Objeto de Política deve ser associado ao Grupo de Configuração antes da criação de qualquer Pacote de recursos relacionado à Configuração de Política (Políticas Localizadas). Exemplo: ACL
6	Importar CSV para variáveis de interface insere ponto-e-vírgula na string e falha
7	A configuração de otimização de AppQoE (TCP Opt e DRE) e correção de perda (FEC e Pkt Dup) continua a usar modelos/políticas herdados. Configurável via perfil CLI em grupos de configuração/política também. (20.14 em Encomenda IU)
8	O Cloud OnRamp para SaaS continua a usar os modelos/políticas herdados.
9	Suporte a TrustSec / SGT apenas com perfil CLI
10	UC Voice / DSP Farm / SRST suportado apenas com perfil CLI (20.13 em diante no pacote UI)

Informações Relacionadas

- Canal da Cisco SD-WAN e Cloud Networking no YouTube:
<https://www.youtube.com/@CiscoSDWANandCloudNetworking>
- UX2.0 - Simplificação operacional: 1. Configure um site de roteador único:
<https://www.youtube.com/watch?v=98z-d3knd>
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.