

Guía de inicio rápido: configuración y políticas simplificadas de Catalyst SD-WAN

Contenido

[Introducción](#)

[Antecedentes](#)

[Summary](#)

[Nuevas implementaciones](#)

[Implementaciones existentes](#)

[Mejoras en la experiencia del usuario y simplificación operativa](#)

[Definir la jerarquía de red y las construcciones del sistema](#)

[Jerarquía de red](#)

[Construcciones del sistema](#)

[Flujos de trabajo](#)

[Grupos de configuración](#)

[Ejemplos de implementación de grupos de configuración](#)

[Caso práctico 1: cliente gubernamental](#)

[Caso práctico 2: cliente minorista](#)

[Asociado](#)

[Implementación](#)

[Reutilización](#)

[Catálogo de aplicaciones](#)

[Grupos de políticas](#)

[Prioridad de aplicaciones y SLA](#)

[Modo sencillo](#)

[Modo avanzado](#)

[Calidad del servicio](#)

[Routing con reconocimiento de aplicaciones](#)

[Política de tráfico](#)

[Seguridad integrada](#)

[Gateway de Internet seguro/Extremo de servicio seguro](#)

[Seguridad DNS](#)

[Grupos de interés](#)

[Asociar e implementar](#)

[Políticas localizadas](#)

[Topología](#)

[Topología y VPN](#)

[Asignación de un nombre VPN a varios ID de VPN](#)

[Asignación de varios nombres de VPN al mismo ID de VPN](#)

[Incorporación](#)

[Etiquetado](#)

[Agregar etiqueta](#)

[Etiquetar reglas en el grupo de configuración](#)

[Ilustración](#)

[Implementaciones existentes](#)

[Grupos de configuración](#)

[Grupos de políticas](#)

[Topología](#)

[Herramienta de conversión](#)

[Alcance](#)

[Detalles de acceso](#)

[Cómo usarla](#)

[Requisito previo](#)

[Flujo de trabajo de herramienta de conversión](#)

[Posterior a la conversión](#)

[Consideraciones](#)

[20.12 Consideraciones](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración simplificada y las políticas de Catalyst SD-WAN.

Antecedentes

Summary

Con la versión 20.12/17.12 del software Cisco Catalyst SD-WAN, se recomienda que los usuarios inicien la migración de la configuración tradicional basada en plantillas de dispositivos y funciones al nuevo enfoque de configuración basado en grupos de configuración y grupos de políticas. En este documento, se describen detalles importantes para el nuevo enfoque de configuración.

El objetivo principal de este documento es servir de guía para comenzar a utilizar nuevas construcciones para la configuración, las políticas y la incorporación, con la versión dorada 20.12. El documento no cubre explicaciones de características individuales.

Nuevas implementaciones

Para utilizar correctamente el nuevo enfoque de configuración, debe realizar estos pasos:

1. Red: Defina la jerarquía de red y las construcciones del sistema
2. Configuración: Crear configuración con grupos de configuración mediante el flujo de trabajo
3. Aplicaciones: defina aplicaciones personalizadas, si es necesario, mediante el catálogo de aplicaciones
4. Políticas: Crear Políticas mediante Grupos de Políticas
5. Topología: Definir Topología
6. Integrado: dispositivos incorporados y etiquetados
7. Desplegar: Asocie e implemente grupos de configuración y grupos de políticas. Activar

topología.

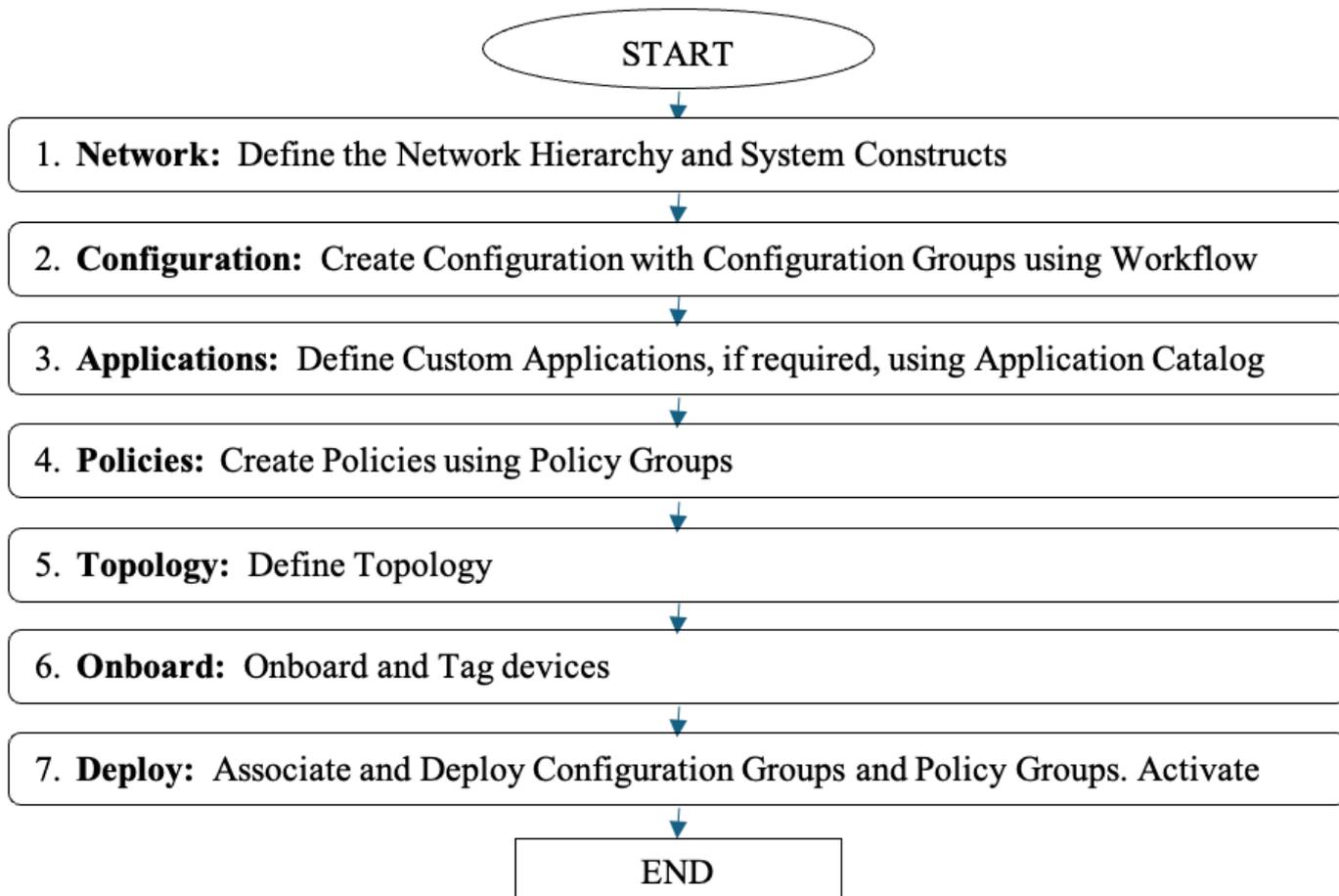


Diagrama de flujo para nuevas implementaciones

Implementaciones existentes

1. Ejecute los pasos mencionados en la sección [Implementaciones existentes](#)
2. Utilice la [herramienta Conversion](#) para convertir la configuración/políticas existentes en nuevas configuraciones/políticas

Mejoras en la experiencia del usuario y simplificación operativa

Cisco Catalyst SD-WAN ofrece una experiencia de usuario mejorada y simplifica las operaciones.

- Interfaz de usuario común: se ha introducido un nuevo marco de UX en Catalyst SD-WAN Manager y otros productos de Cisco, con el fin de lograr la coherencia en la experiencia del usuario y proporcionar un aspecto y una sensación comunes a todos los productos.
- Configuración: configuración simplificada y creación e implementación de políticas con flujos de trabajo intuitivos basados en intención y el uso de los valores predeterminados inteligentes recomendados por Cisco.
- Supervisión: información detallada sobre el estado y el rendimiento de las aplicaciones y la red con nuevos widgets y paneles de control personalizables y mejorados.
- Resolución de problemas: vistas de topología de red y de sitio dinámicas, acceso a herramientas de resolución de problemas basadas en contexto, informes sobre el rendimiento de la red y de las aplicaciones de forma programada.

Beneficios

| | |
|-------------------------------|---|
| Uso sencillo | Flujos de trabajo intuitivos y guiados |
| Expansión de la configuración | Reducción de la expansión (independiente del modelo, reutilización, estructura) |
| Creación de configuración | Predeterminados inteligentes de forma más rápida y sencilla |
| Modificación de configuración | Modificar ahora e implementar selectivamente más tarde |
| Visibilidad | Nuevos paneles, supervisión del rendimiento de aplicaciones/sitios |
| Guía de Troubleshooting | Topología del sitio, guía de herramientas de solución de problemas |

Definir la jerarquía de red y las construcciones del sistema

Jerarquía de red

Proporciona una noción de "jerarquía", es decir, sitios, regiones y áreas, para la red. Puede crearlo en función de su red.

Ejemplo:



Search



Global (15 of 15 nodes)



AMER



BR1_SanJose



BR2_NewYork



BR6_Dallas



APJC



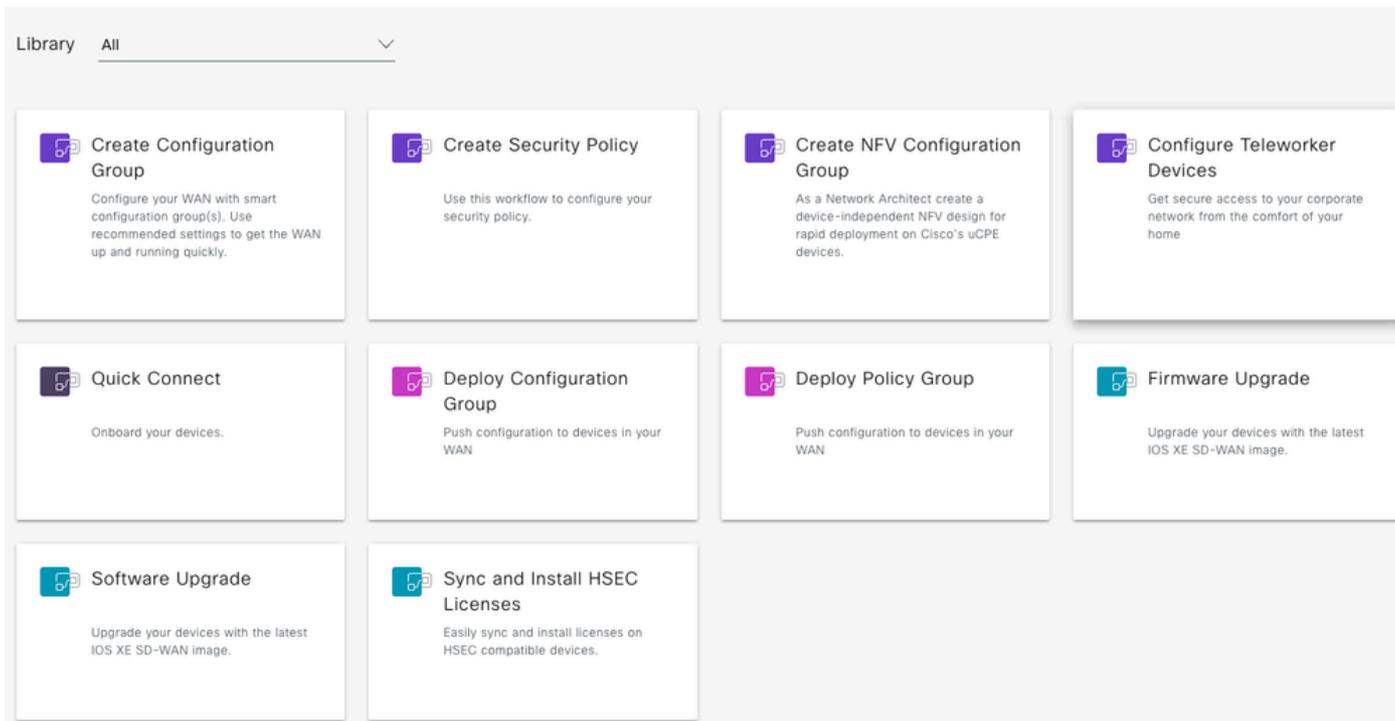
BR3_Mumbai



BR4_Singapore

- La mayoría de los botones/ajustes de configuración se establecen en los valores predeterminados inteligentes recomendados por Cisco.
- Los usuarios solo deben especificar algunas configuraciones.
- Los botones de configuración avanzada están disponibles fuera del flujo de trabajo, donde el grupo de configuración se puede editar manualmente.

Una biblioteca de flujos de trabajo muestra todos los flujos de trabajo disponibles.

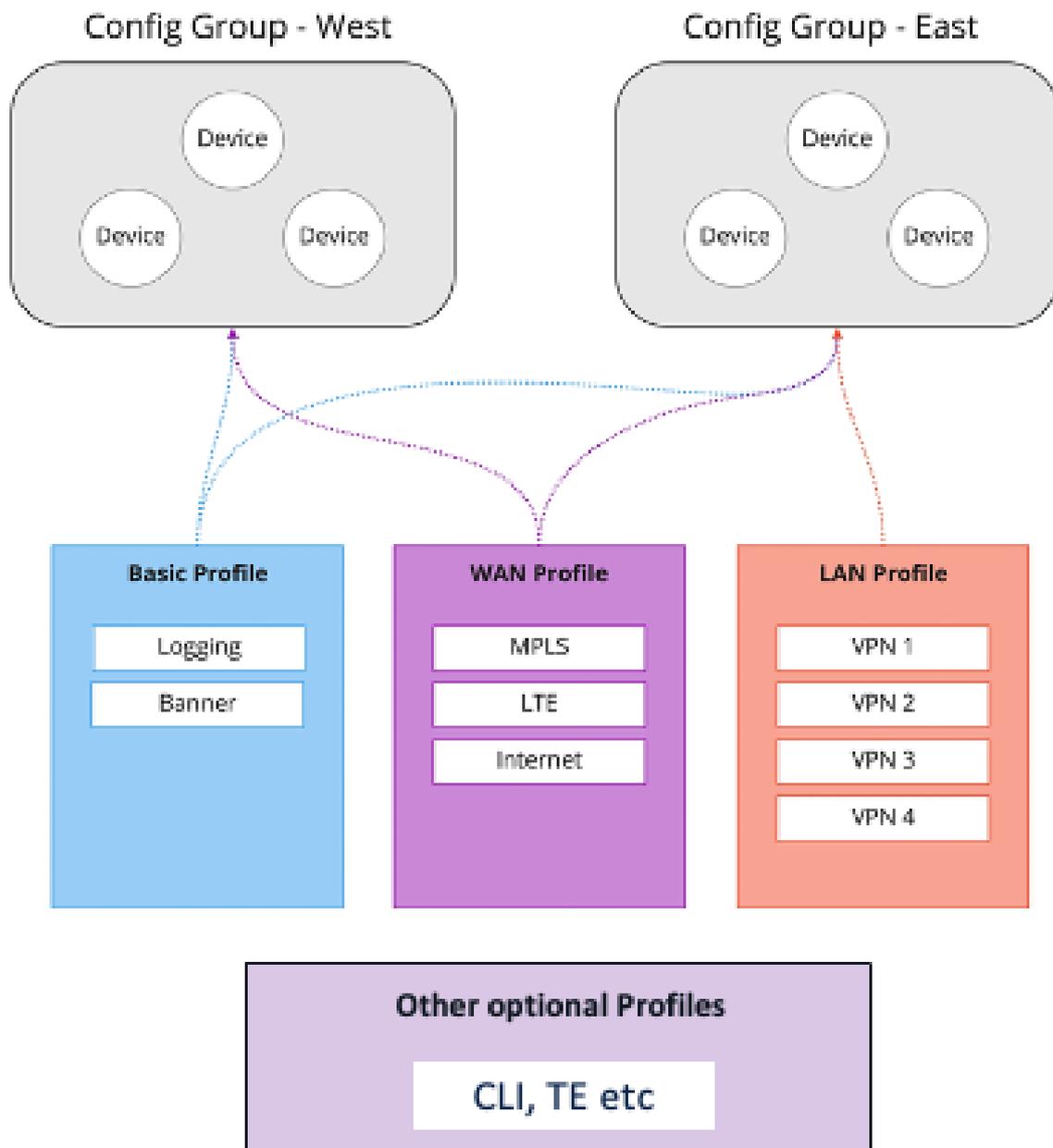


Biblioteca de flujo de trabajo

Grupos de configuración

Los grupos de configuración son un nuevo enfoque de la configuración del fabric que se basa en los principios de simplicidad, reutilización y estructura.

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



Estructura de grupos de configuración

Grupos de configuración

- Agrupación lógica de dispositivos que comparten un propósito común dentro de la WAN.
- El usuario define y puede personalizar esta agrupación en función de sus necesidades empresariales.

Por ejemplo, Este/Oeste, América/APJC/EMEAR, Tienda minorista/Centro de distribución

Perfiles de funciones

- "Bloques" flexibles de configuración que se pueden compartir entre los grupos de configuración.
- Crear perfiles de funciones basados en las funciones necesarias
- Reúna los perfiles para completar la configuración del dispositivo, como bloques de creación

- Creación, almacenamiento y reutilización

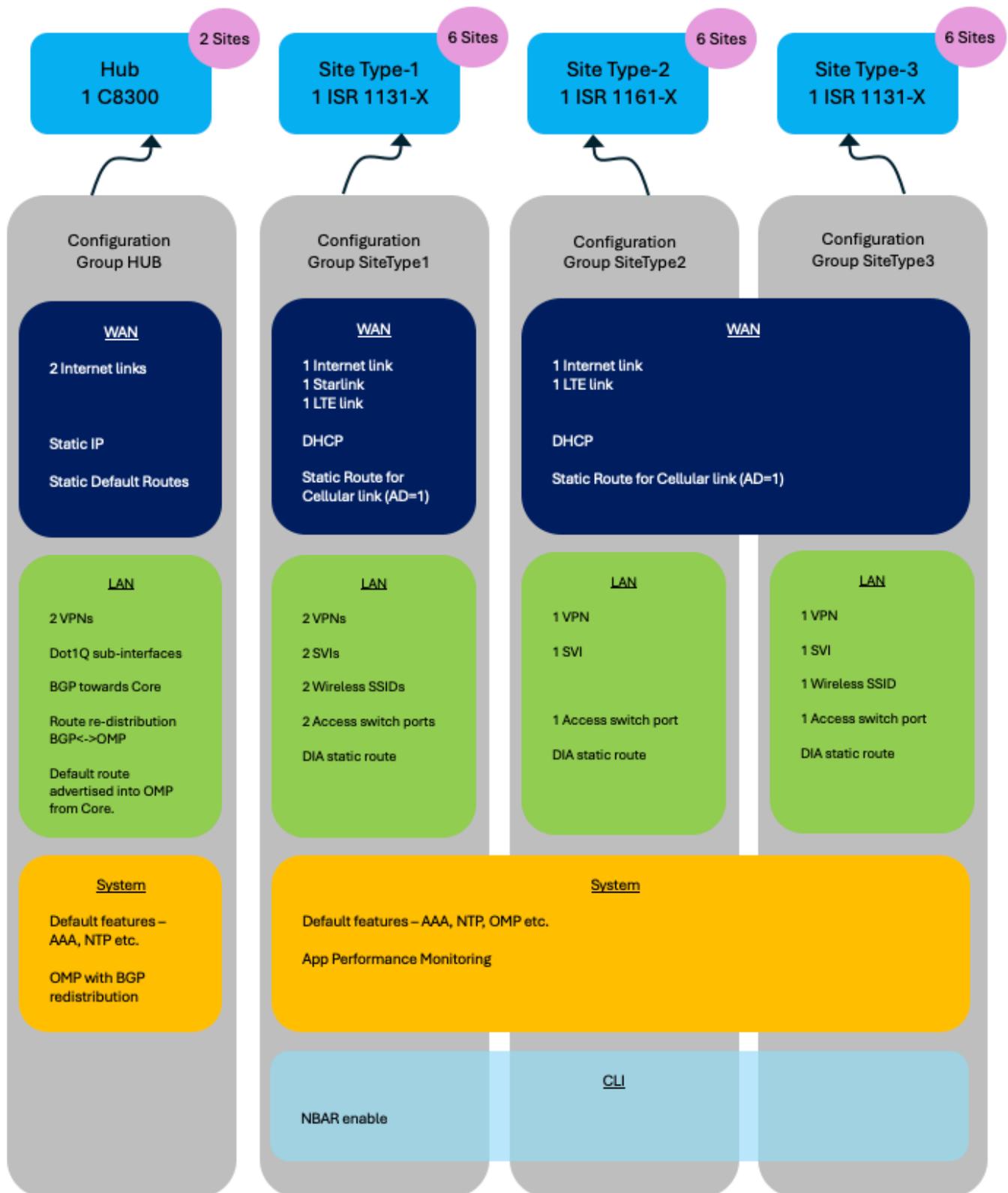
Por ejemplo: perfil básico, perfil WAN, perfil LAN

Ejemplos de implementación de grupos de configuración

Nota:

- Los grupos de configuración son independientes del modelo de dispositivo
- Los perfiles de funciones se pueden compartir entre los grupos de configuración

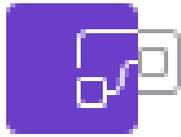
Caso práctico 1: Cliente gubernamental



Ejemplo de uso 1: grupos de configuración

HUB de grupo de configuración

Ejecute el flujo de trabajo Crear grupo de configuración.



Create Configuration Group

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

Opción de flujo de trabajo Crear grupo de configuración

Perfil de WAN

2 Internet links

Static IP

Static Default Routes

Ejemplo de caso práctico 1: perfil WAN 1

Mediante el flujo de trabajo, se puede generar la configuración de perfil WAN completa para este caso práctico.

Las entidades como IP estática real, IP/subred/Next-Hop de ruta estática predeterminada, etc., se pueden especificar como globales o específicas del dispositivo.

La opción específica del dispositivo se puede especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

Perfil LAN

LAN

2 VPNs

Dot1Q sub-interfaces

BGP towards Core

Route re-distribution

BGP<->OMP

Default route

advertised into OMP

from Core.

para este caso práctico.

- 2 VPN
- Routing BGP en cada una de las VPN (número AS, prefijos de red, vecinos)

Las entidades como las subinterfaces Dot1Q reales y cualquier otra entidad marcada como específica del dispositivo se pueden especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

NOTE:

La configuración avanzada, como la redistribución de rutas y el anuncio de rutas predeterminadas, se debe configurar después del flujo de trabajo mediante la edición manual del grupo de configuración, así como de las subinterfaces si se van a utilizar durante la implementación.

Perfil del sistema

System

Default features –
AAA, NTP etc.

OMP with BGP
redistribution

Ejemplo de caso práctico 1: Perfil del sistema 1

Mediante el flujo de trabajo, se puede generar la mayor parte de la configuración del perfil del sistema para este caso práctico: OMP, AAA, NTP, registro, etc.

NOTE:

La configuración avanzada, como la redistribución de OMP-BGP y cualquier otro cambio en las funciones del sistema, como OMP, AAA, NTP, etc., debe configurarse después del flujo de trabajo mediante la edición manual del grupo de configuración.

Tipo de sitio de grupo de configuración 1

Ejecute el flujo de trabajo Create Configuration Group.

Perfil de WAN

WAN Profile

1 Internet Link

1 Starlink

1 LTE link

DHCP

Static Route for Cellular
link (AD=1)

Ejemplo de caso práctico 1: perfil WAN 2

Mediante el flujo de trabajo, se puede generar la mayor parte de la configuración del perfil WAN para este caso práctico. Interfaces Ethernet para Internet y Starlink. DHCP.

NOTE:

La interfaz móvil para el enlace LTE, incluida la ruta estática, debe configurarse después del flujo de trabajo, editando manualmente el grupo de configuración.

LAN Profile

2 VPNs

2 SVIs

2 Wireless SSIDs

2 Access switch ports

DIA static route

Ejemplo de caso práctico 1: perfil LAN 2

Mediante el flujo de trabajo, se puede generar parte de la configuración del perfil de LAN para este caso práctico. 2 VPN, ruta estática DIA.

Las entidades como las subinterfaces Dot1Q reales y cualquier otra entidad marcada como específica del dispositivo se pueden especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

NOTE:

Las SVI, los SSID inalámbricos, los puertos del switch de acceso, etc. deben configurarse después del flujo de trabajo mediante la edición manual del grupo de configuración.

Perfil del sistema

System Profile

Default features - AAA, NTP, OMP etc.

Application Performance monitoring

Ejemplo de caso práctico 1: perfil del sistema 2

Mediante el flujo de trabajo, se puede generar la mayor parte de la configuración del perfil del sistema para este caso práctico: OMP, AAA, NTP, registro, etc.

NOTE:

La configuración avanzada, como la supervisión del rendimiento de la aplicación, se debe configurar después del flujo de trabajo mediante la edición manual del grupo de configuración.

CLI Profile NBAR enable

Ejemplo de uso 1: perfil CLI 2

Las funciones no admitidas mediante la GUI, como la habilitación de la visibilidad de aplicaciones/flujos (NBAR), se pueden configurar mediante un perfil CLI.

Visibilidad de App/Flow

Para habilitar la visibilidad de las aplicaciones y la visibilidad del flujo, utilice el paquete/perfil de CLI.

(En 20.13 y versiones posteriores, está disponible en Configuración avanzada en Grupo de políticas)

Sin embargo, en 20.12, si se configura una política AAR, se habilita App/Flow Visibility. Y no es necesario configurar esto mediante el paquete/perfil de CLI.

Tipo de sitio de grupo de configuración 2

Ejecute el flujo de trabajo Create Configuration Group.

Perfil de WAN

WAN Profile

1 Internet link

1 LTE link

DHCP

Static Route for Cellular link (AD=1)

Ejemplo de caso práctico 1: perfil WAN 3

Mediante el flujo de trabajo, se puede generar la mayor parte de la configuración del perfil WAN para este caso práctico. Interfaz Ethernet para Internet. DHCP.

NOTE:

La interfaz móvil para el enlace LTE, incluida la ruta estática, debe configurarse después del flujo de trabajo, editando manualmente el grupo de configuración.

Perfil LAN

LAN Profile

1 VPN

1 SVI

1 Access switch port

DIA Static route

Ejemplo de caso práctico 1: perfil LAN 3

Mediante el flujo de trabajo, se puede generar parte de la configuración del perfil de LAN para este caso práctico. 1 VPN, ruta estática DIA.

Las entidades como las subinterfaces Dot1Q reales y cualquier otra entidad marcada como específica del dispositivo se pueden especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

NOTE:

SVI, el puerto del switch de acceso, etc., se debe configurar después del flujo de trabajo mediante la edición manual del grupo de configuración.

Perfil del sistema

Igual que Configuration Group SiteType1

Perfil CLI

Igual que Configuration Group SiteType1

Tipo de sitio de grupo de configuración 3

Ejecute el flujo de trabajo Create Configuration Group.

Perfil de WAN

Igual que Configuration Group SiteType2

Perfil LAN

LAN Profile

1 VPN

1 SVI

1 Wireless SSID

1 Access switch port

DIA Static route

Ejemplo de caso práctico 1: perfil LAN 4

Mediante el flujo de trabajo, se puede generar parte de la configuración del perfil de LAN para este caso práctico. 1 VPN, ruta estática DIA.

Las entidades como las subinterfaces Dot1Q reales y cualquier otra entidad marcada como específica del dispositivo se pueden especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

NOTE:

SVI, SSID inalámbrico, puerto del switch de acceso, etc., deben configurarse después del flujo de trabajo mediante la edición manual del grupo de configuración.

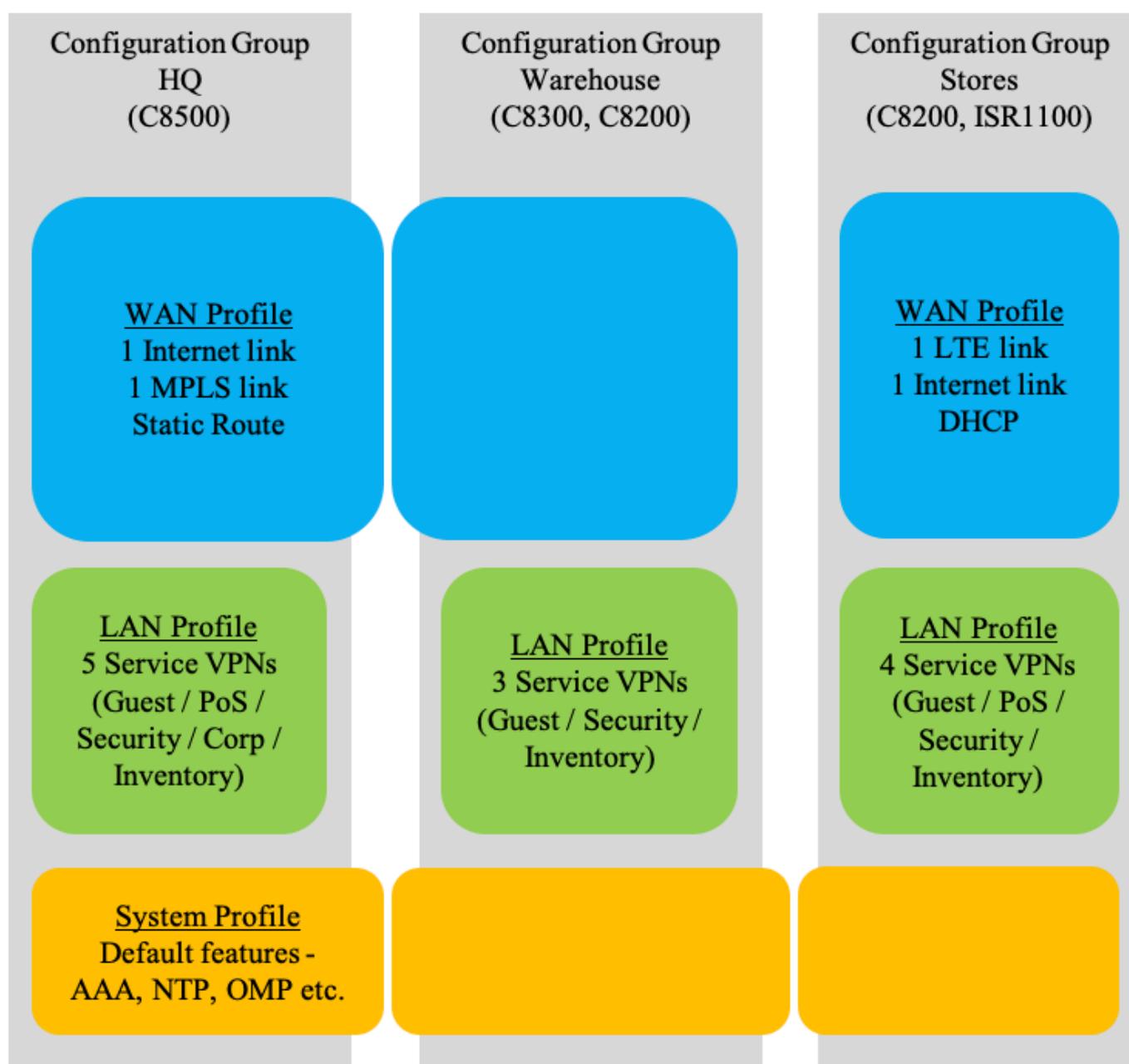
Perfil del sistema

Igual que Configuration Group SiteType1

Perfil CLI

Igual que Configuration Group SiteType1

Caso práctico 2: cliente minorista



Ejemplo de uso 2: grupos de configuración

Sede central y almacén del grupo de configuración

Ejecute el flujo de trabajo Create Configuration Group.

Perfil de WAN

Mediante el flujo de trabajo, se puede generar toda la configuración del perfil de WAN para este caso práctico.

Perfil LAN

Mediante el flujo de trabajo, se puede generar toda la configuración de perfil LAN para este caso práctico.

Las entidades como las subinterfaces Dot1Q reales y cualquier otra entidad marcada como específica del dispositivo se pueden especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

Perfil del sistema

Mediante el flujo de trabajo, se puede generar toda la configuración del perfil del sistema para este caso práctico.

NOTE:

Si se requiere algún cambio o si se requiere una configuración avanzada, como la supervisión del rendimiento de la aplicación, se debe configurar y publicar el flujo de trabajo editando manualmente el grupo de configuración.

Almacenes de grupos de configuración

Ejecute el flujo de trabajo Create Configuration Group.

Perfil de WAN

Mediante el flujo de trabajo, se puede generar la mayor parte de la configuración del perfil WAN para este caso práctico.

NOTE:

La interfaz móvil para el enlace LTE, incluido el enrutamiento, debe configurarse después del flujo de trabajo mediante la edición manual del grupo de configuración.

Perfil LAN

Mediante el flujo de trabajo, se puede generar toda la configuración de perfil LAN para este caso práctico.

Las entidades como las subinterfaces Dot1Q reales y cualquier otra entidad marcada como específica del dispositivo se pueden especificar con valores reales durante la implementación del grupo de configuración en los dispositivos.

Perfil del sistema

Igual que en HQ y Warehouse del grupo de configuración.

Asociado

En la página de edición del grupo de configuración (Configuration -> Configuration Groups), puede asociar dispositivos al grupo de configuración.

Haga clic en Associate Devices y siga los pasos del flujo de trabajo.

Go Back to Configuration Group list

US-WEST-SITES [Edit](#)

Description: US-WEST-SITES

| | | |
|--------------------------|-------------------------|---------------------------------------|
| DEVICE SOLUTION sdwan | MODIFIED BY Chbalaji | LAST UPDATED Dec 14, 2023 06:27:32 |
|--------------------------|-------------------------|---------------------------------------|

Feature Profiles **Associated Devices**

Devices (2) [Export](#)

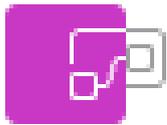
0 selected [Associate Devices](#) [Remove Devices](#) [Add and Edit Rules](#) [Change Device Values](#) [Deploy](#) As of: Jul 15, 2024 10:23 AM

| <input type="checkbox"/> | 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"/> | C8K-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"/> | C8K-01DE1D37-6F1B-F8DF-E71A-9D58D665FD10 | SITE_3 | Site3-Edge | - | Yes | 3.3.3.1 | 3 | In Sync | false | Dec 14, 2023, 6:27:32 AM | True |

Asociar dispositivo - Grupos de configuración

Implementación

Ejecute el flujo de trabajo Deploy Configuration Group.



Deploy Configuration Group

Push configuration to devices in your WAN

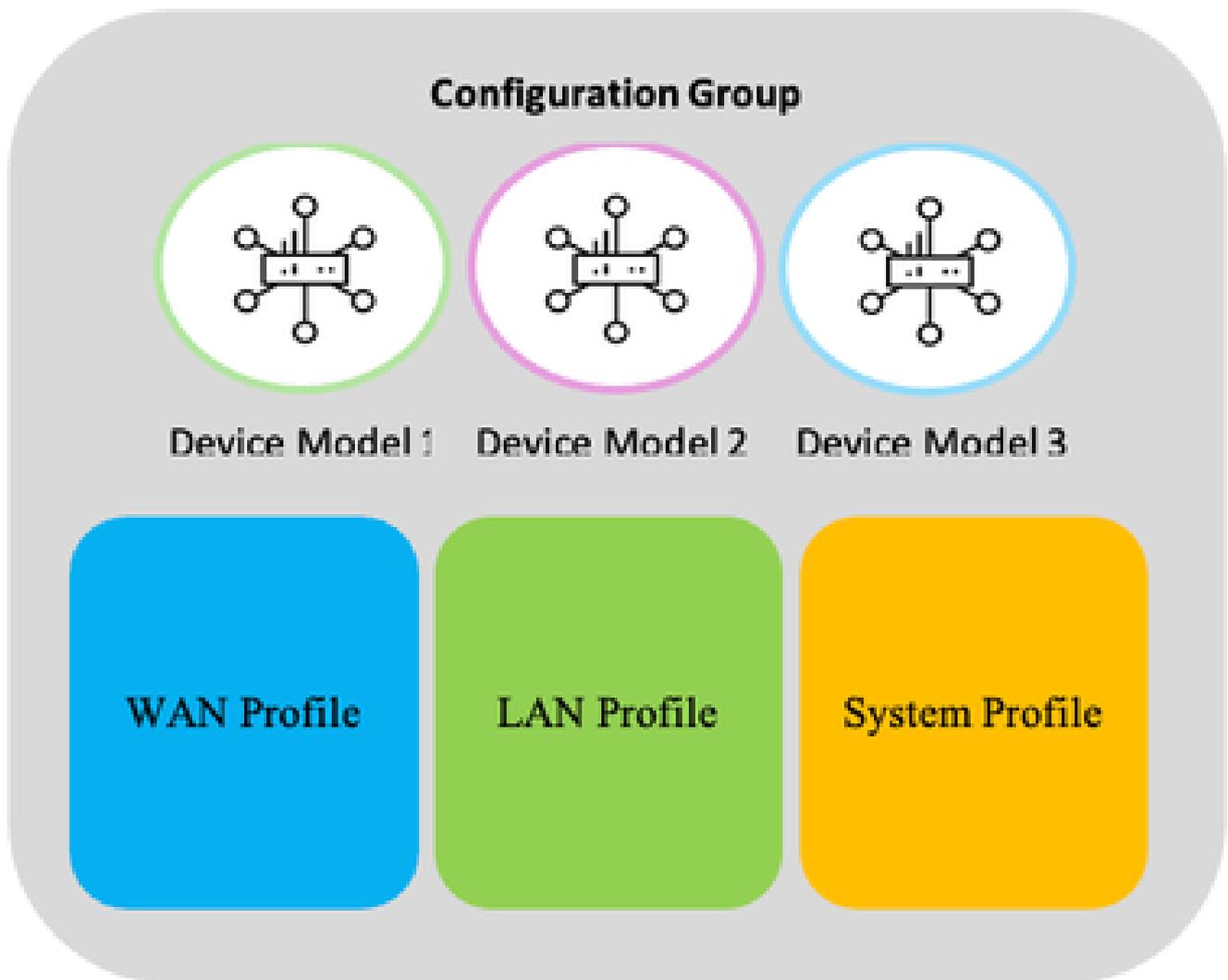
Implementar flujo de trabajo de grupos de configuración

NOTE:

- En el grupo de configuración, el comando Change Device Values sólo cambia el valor de la base de datos del administrador y NO envía ningún cambio a un dispositivo. Si desea que el cambio tenga lugar inmediatamente, debe implementar los cambios.
- La exportación de valores de variables de dispositivo (como un archivo CSV) se puede realizar en el flujo de trabajo de implementación en el paso Agregar/revisar configuración de dispositivo.

Reutilización

1. Los grupos de configuración son independientes del modelo de dispositivo.



Grupo de configuración: independiente del modelo de dispositivo

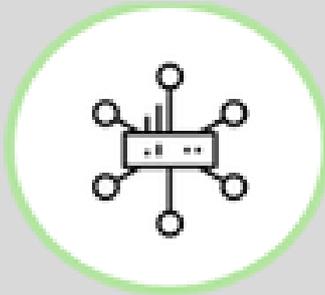
NOTE:

Si una configuración determinada no se admite en un modelo de dispositivo, no se produce la inserción de paquete de funciones correspondiente y se muestra un mensaje adecuado como parte de la tarea de implementación.

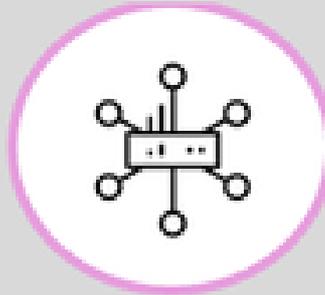
Ejemplo: un dispositivo no admite Wi-Fi, pero el grupo de configuración contiene un paquete Wi-Fi. En el momento de la implementación, se omite la configuración del paquete Wi-Fi y el mensaje de la tarea de implementación informa de que se omitió la inserción de la configuración Wi-Fi.

2. Usar variables de configuración: valores específicos del dispositivo

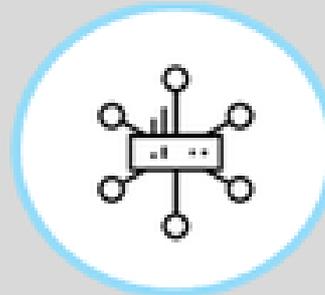
Configuration Group



Device Model 1



Device Model 2



Device Model 3

WAN Profile

LAN Profile

System Profile

Variable 1

Variable 2

Variable 3

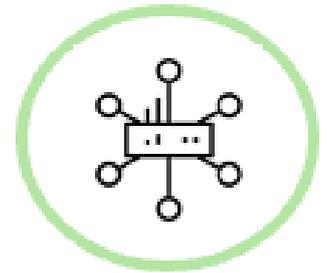
Grupo de configuración: variables específicas del dispositivo

Un perfil de función puede tener una configuración definida como específica del dispositivo, similar a las variables de plantilla.

Ejemplo: dirección IP de la interfaz, números de puerto, nombre de la interfaz, etc.

Estos valores específicos del dispositivo se pueden proporcionar en el momento de la implementación. Y puede ser diferente para diferentes dispositivos.

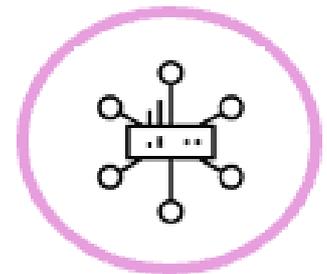
System Profile
Variable 1 = A
Variable 2 = B
Variable 3 = C



Device 1

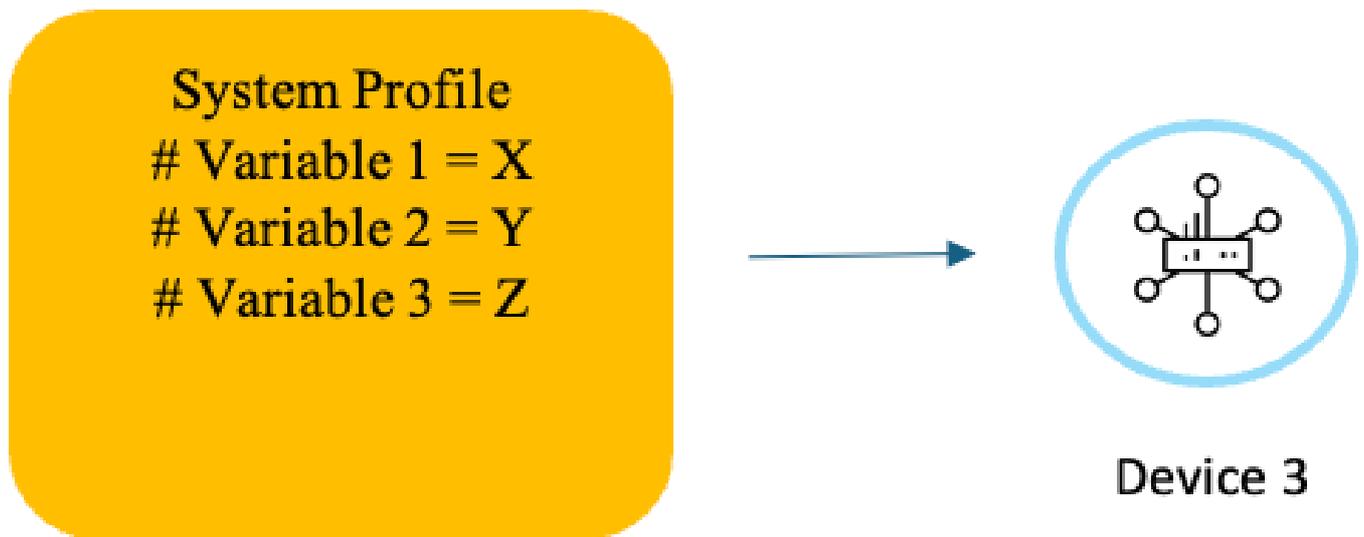
Grupo de configuración - Ejemplo 1 de variables específicas del dispositivo

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



Device 2

Grupo de configuración - Ejemplo 2 de variables específicas del dispositivo



Grupo de configuración - Ejemplo 3 de variables específicas del dispositivo

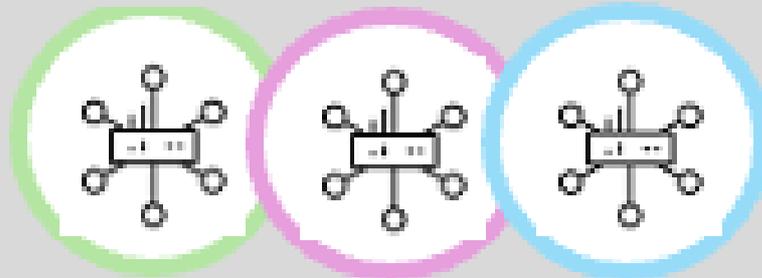
3. Reutilización de perfiles de funciones

Los perfiles de funciones se pueden reutilizar en los grupos de configuración.

Ilustración:

En el caso de varios dispositivos, si las configuraciones de WAN y del sistema son las mismas y solo difieren en la configuración de LAN, por ejemplo, los perfiles de WAN y del sistema se pueden reutilizar en sus grupos de configuración al tiempo que tienen un perfil de LAN diferente en cada uno.

Configuration Group



**WAN
Profile
1**

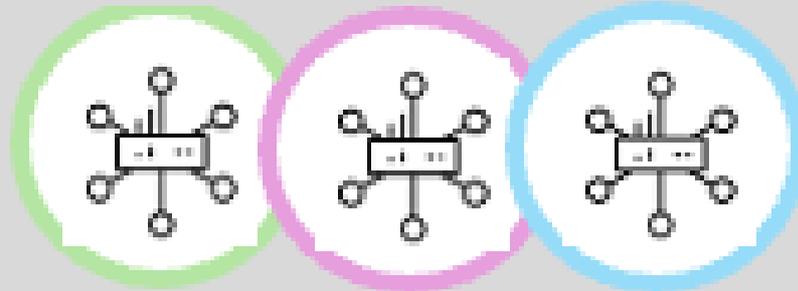
**LAN
Profile
1**

**System
Profile
1**

Reutilización de perfiles de funciones: 1

Perfil LAN 1

Configuration Group



**WAN
Profile
1**

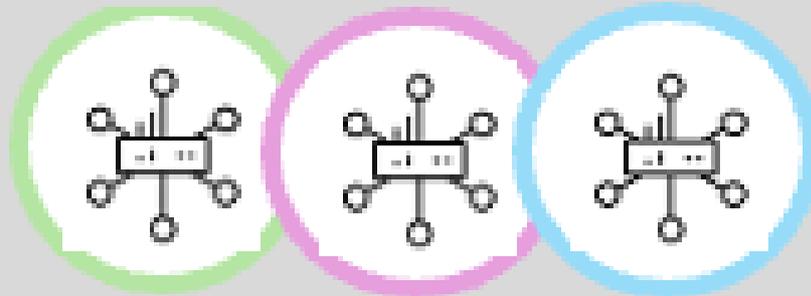
**LAN
Profile
2**

**System
Profile
1**

Reutilización de perfiles de funciones: 2

Perfil de LAN 2

Configuration Group



**WAN
Profile**

1

**LAN
Profile**

3

**System
Profile**

1

Reutilización de perfiles de funciones: 3

Perfil de LAN 3

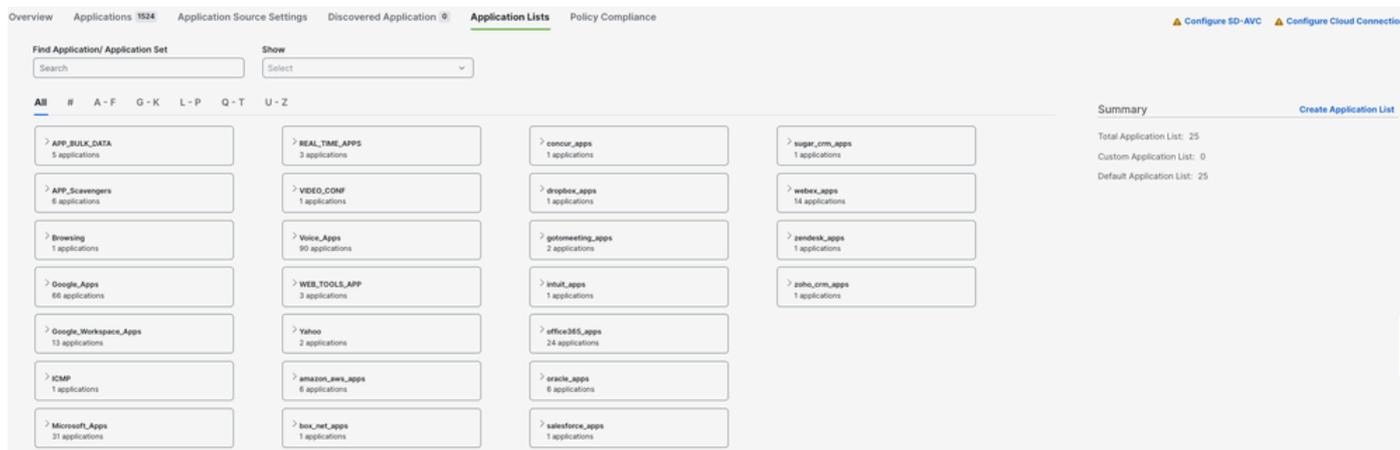
Catálogo de aplicaciones

Los dispositivos tradicionales podían manipular los flujos de tráfico mediante la coincidencia condicional de las direcciones IP de origen o destino, los puertos de origen o destino y los protocolos. A medida que cada vez más aplicaciones dependen de DNS o están integradas en HTTP, es más difícil identificar con precisión el tráfico de red en el nivel de aplicación.

El motor de reconocimiento de aplicaciones basadas en la red (NBAR) de Cisco tiene la capacidad de clasificar más de 1500 aplicaciones, lo que proporciona a los ingenieros de redes la capacidad de clasificar y manipular los flujos de tráfico con mayor granularidad. Cisco Catalyst SD-WAN Manager ofrece la posibilidad de conectarse a un repositorio de aplicaciones de Cisco donde las firmas de las aplicaciones se pueden actualizar rápidamente, lo que es importante

cuando los proveedores de nube cambian las ubicaciones de alojamiento o los patrones de tráfico.

El catálogo de aplicaciones proporciona la capacidad de crear aplicaciones personalizadas basadas en la coincidencia del nombre del servidor, la dirección IP, los puertos o el protocolo. La aplicación se define entonces para una familia de aplicaciones, grupo de aplicaciones, clase de tráfico y relevancia empresarial específicos.



Catálogo de aplicaciones

Las aplicaciones se pueden arrastrar y soltar hasta la relevancia empresarial o clasificación de tráfico adecuada. Al guardar los cambios, las definiciones se actualizan en la base de datos.

NOTA: Las clasificaciones de aplicaciones son globales y un cambio en el catálogo de aplicaciones afecta a todas las clasificaciones de dispositivos.

Grupos de políticas

Al igual que los grupos de configuración, un grupo de políticas es una agrupación de políticas que se implementan en dispositivos asociados al grupo de políticas.

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

El grupo de políticas enfoca la creación e implementación de políticas en función de la intención. Una interfaz de usuario y un flujo de trabajo simplificados facilitan la creación de una política, la agrupación de políticas y la implementación en dispositivos.

Requisito previo:

La asociación del grupo de configuración y la implementación en un dispositivo es un requisito previo para la implementación del grupo de políticas en ese 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

Prioridad de aplicaciones y SLA

Con esta intención de directiva, puede especificar:

- Routing con reconocimiento de aplicaciones y política SLA
- política de QoS
- Política de datos de tráfico
- política DIA
- política SIG

Se proporcionan dos modos.

Modo sencillo

Este es el modo predeterminado.

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 | VPN | Interface |
|--------|-----------------|------------|------------------|
| | Enter Direction | Select VPN | Enter Interfaces |

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

Modo sencillo

Esto proporciona una manera rápida y fácil de definir la prioridad de la aplicación y el SLA para su red.

NOTE:

1. La acción de política predeterminada es DROP
2. Los criterios de coincidencia sólo pueden ser Aplicaciones. Si necesita prefijos, utilice el modo avanzado

Modo avanzado

Se trata de un modo completo y flexible.

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. La acción de política predeterminada es DROP
2. La lista de aplicaciones y la clase de tráfico son básicamente una lista de aplicaciones.

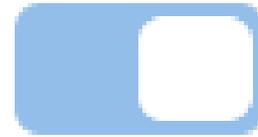
Cualquiera de ellas se puede utilizar para hacer coincidir una lista de aplicaciones. La asignación de aplicaciones a una clase de tráfico se puede realizar en el catálogo de aplicaciones.

El modo simple genera reglas utilizando cualquiera de estas opciones o ambas, mientras que el modo avanzado sólo proporciona la lista de aplicaciones.

Calidad del servicio

En la opción QoS Queue, puede agregar una política de QoS:

Advanced Layout



SLA Class

QoS Queue

[⊕ Add QoS Policy](#)

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

Agregar política de QoS

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) |

Bandwidth

Modelos de colas

A continuación, puede definir la política de datos de tráfico (Agregar política de tráfico).

Agregue reglas para hacer coincidir el tráfico deseado y redirija a las clases de reenvío apropiadas.

Policies > Application Priority & SLA

Basic_4Queue_QoS_Policy (Total Traffic Policy: 1)

Additional Settings Advanced Layout

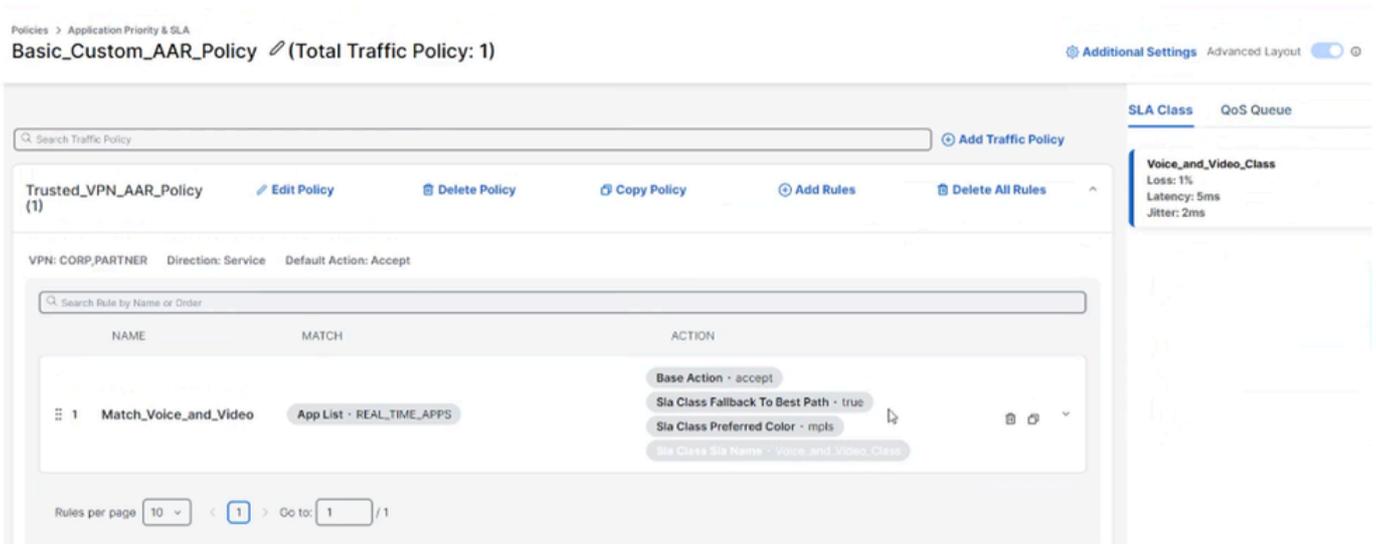
| NAME | MATCH | ACTION |
|---------------------------|---|---|
| 1 Match_Voice_Traffic | Dscp - 46 | Base Action - accept Count - voice Forwarding Class - VOICE Log - true |
| 2 Match_Critical_Apps | App List - Microsoft_Apps | Base Action - accept Count - critical_apps Forwarding Class - CRITICAL_DATA 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

Routing con reconocimiento de aplicaciones

Puede definir clases de SLA y utilizarlas en una política de tráfico para realizar la intención de una política de AAR.



Política AAR

Visibilidad de App/Flow

Para habilitar la visibilidad de las aplicaciones y la visibilidad del flujo, utilice el paquete/perfil de CLI en el grupo de configuración.

(En 20.13 y versiones posteriores, está disponible en Configuración avanzada en Grupo de políticas)

Sin embargo, en 20.12, si se configura una política AAR, se habilita App/Flow Visibility. Y no es necesario configurar esto mediante el paquete/perfil de CLI.

Política de tráfico

La política de tráfico también se puede utilizar para crear una política DIA, redirección SIG, etc. Agregue las reglas que sean necesarias.

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="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 30%;"> <p>Rule1</p> <p>Sequence <input style="width: 100%;" type="text" value="1"/></p> </div> <div style="width: 40%;"> <p>Name <input style="width: 90%;" type="text" value="Rule1"/></p> </div> <div style="width: 30%;"> <p>Protocol <input style="width: 90%;" type="text" value="IPv4"/></p> </div> </div> | | |
| <p>Match Add Match</p> <p>Action Add Action</p> | | |
| <p>Base Action</p> <p><input type="radio"/> Accept <input checked="" type="radio"/> Drop</p> | | |

Cancel
Save Match and Actions

Política de tráfico

NOTE:

Si se crea una política de prioridad de aplicación y SLA en modo simple y, a continuación, se cambia al modo avanzado, algunas opciones de coincidencia no estarán disponibles para su selección. Ejemplo: El prefijo de datos de destino está atenuado.

Para que estas opciones estén disponibles, cambie el Protocolo de BOTH a IPv4 o IPv6 según sea necesario.

Seguridad integrada

Define la política de seguridad para el NGFW integrado, IPS, malware y filtrado de contenido

Gateway de Internet seguro/Extremo de servicio seguro

Define la configuración necesaria para establecer túneles para el contenido basado en la nube y las entidades de seguridad, como Cisco Secure Access.

NOTE:

Con el enfoque de configuración heredado, esto estaba disponible como una plantilla de función.

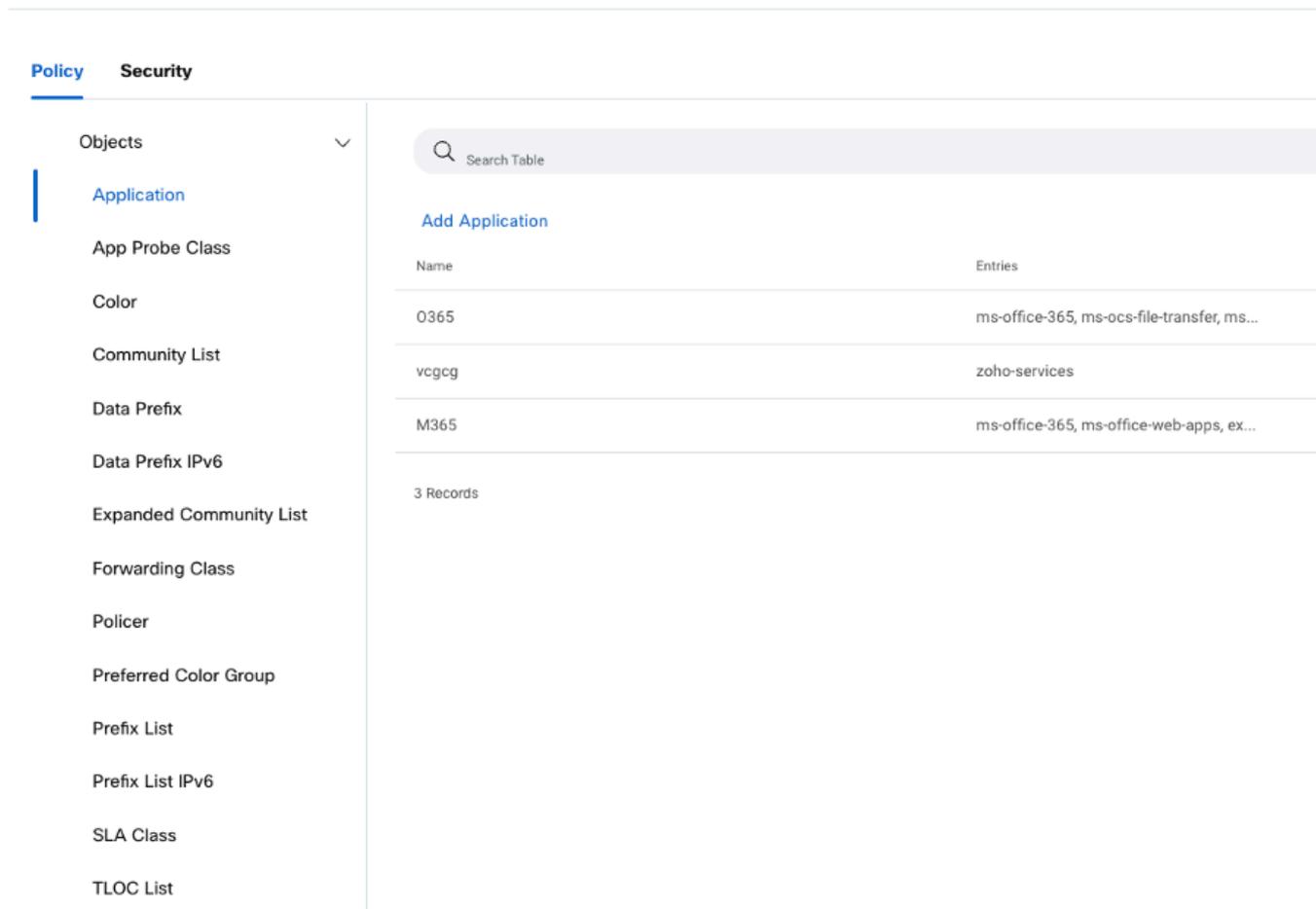
Seguridad DNS

Defina la configuración para permitir el uso de servicios de seguridad DNS basados en la nube para el filtrado de contenido.

Grupos de interés

Defina las listas de objetos que se utilizarán en las directivas. Ejemplo: listas de aplicaciones, listas VPN, listas de sitios, listas de prefijos, etc.

Además, para las políticas de seguridad, defina sus perfiles como perfiles de inspección avanzada, política de descifrado SSL, etc.



The screenshot shows the 'Security' section of a configuration interface. On the left, there is a sidebar with a list of object types under the heading 'Objects'. The 'Application' object type is selected and highlighted in blue. The main area on the right displays a table of applications. At the top of this area is a search bar labeled 'Search Table' and a link 'Add Application'. The table has two columns: 'Name' and 'Entries'. It contains three rows of data. Below the table, it indicates '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... |

Grupos de políticas - Grupos de interés

Asociar e implementar

De forma similar a los grupos de configuración, asocie dispositivos al grupo de políticas e impleméntelo.

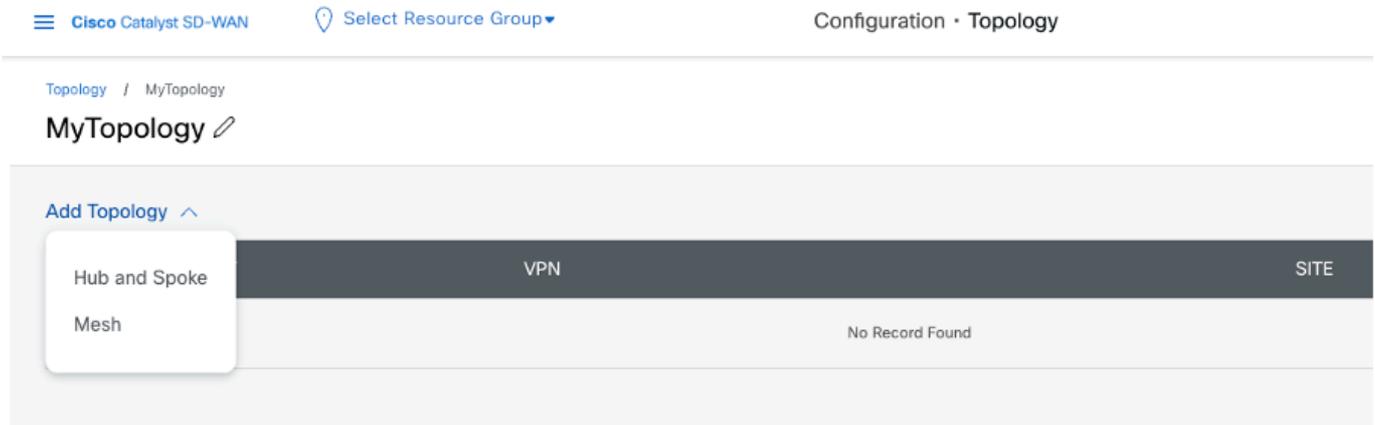
Políticas localizadas

Las políticas localizadas, como ACL, política de ruta, política de acceso del dispositivo, etc., se definen en Grupos de configuración.

Topología

Defina la topología de red.

Comience con una malla completa o Hub-n-Spoke y personalícelo si es necesario.



Menú Topología

Topología y VPN

Tenga en cuenta estos cambios de diseño al crear la topología y especificar las VPN.

El nuevo diseño permite la asignación dinámica del nombre VPN al ID de VPN, en lugar de la asignación 1:1.

Asignación de un nombre VPN a varios ID de VPN

Ilustración:

Digamos que hay una VPN con el nombre Corporate en dos grupos de configuración diferentes.

Uno tiene el ID VPN 10 y el otro tiene el ID VPN 20.

La lista de VPN del flujo de trabajo de topología muestra una instancia de Corporate VPN solamente.

Una vez que selecciona Corporate VPN, el administrador de SD-WAN determina los ID de VPN en función de la topología.

Supongamos que hay 2 dispositivos en 2 sitios:

1. Dispositivo 1 en el sitio 100 con Corporativo como VPN 10
2. Dispositivo2 en el sitio 200 con Corporativo como VPN 20

Si tanto el sitio 100 como el sitio 200 forman parte de la topología, el Administrador de SD-WAN crea una lista de VPN que tendrá los dos ID de VPN (10 y 20).

Si solo el sitio 100 forma parte de la topología, el Administrador de SD-WAN crea una lista de VPN que tendrá solamente el ID de VPN 10.

Si solo el sitio 200 forma parte de la topología, el Administrador de SD-WAN crea una lista de VPN que tendrá solamente el ID de VPN 20.

Asignación de varios nombres de VPN al mismo ID de VPN

Puede configurar varias políticas de topología con el mismo nombre VPN que se asignan a diferentes ID de VPN en diferentes sitios.

El Administrador de SD-WAN determina la asignación real en función de la topología que se asocia a cada sitio.

Ilustración:

Dos usuarios pueden crear dos grupos de configuración diferentes.

Uno especifica VPN ID 100 como Finance VPN y el otro lo especifica como Engineering VPN.

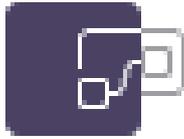
A continuación, pueden crear la topología utilizando sus respectivos nombres de VPN.

Incorporación

Para incorporar los routers físicos, utilice el flujo de trabajo de conexión rápida.

Con este flujo de trabajo, predefina el nombre de host, la IP del sistema y el nombre/ID del sitio para los dispositivos que se van a incorporar. El jefe genera automáticamente estos elementos, pero puede modificarlos si así lo desea. También puede etiquetar los dispositivos que se pueden utilizar para asociar automáticamente los dispositivos a los grupos de configuración.

Durante el proceso de onboarding de PnP ZTP, los dispositivos establecen las conexiones de túnel del plano de control al Administrador de SD-WAN. SD-WAN Manager ahora envía la configuración de fabric predefinida a los dispositivos y estos se unen al fabric SD-WAN.



Quick Connect

Onboard your devices.

Flujo de trabajo de conexión rápida



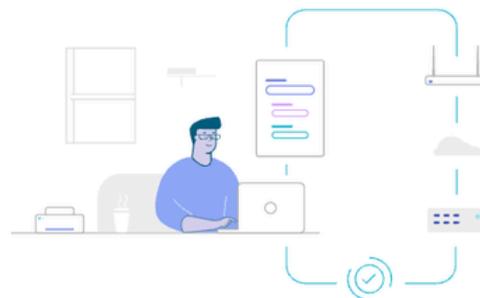
Welcome to Quick Connect

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

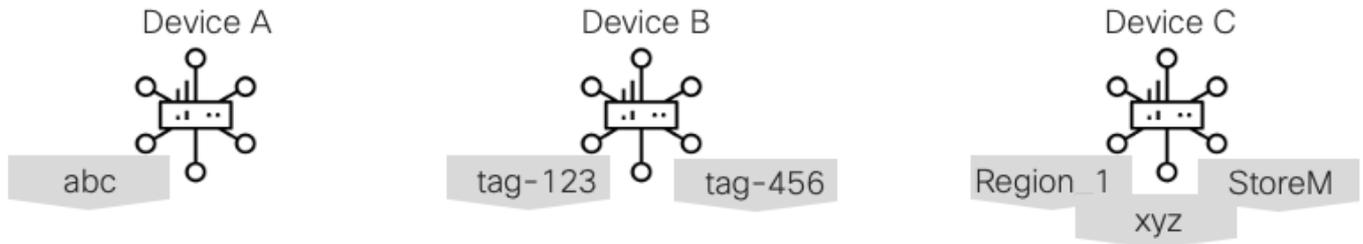
Descripción del flujo de trabajo de conexión rápida

Etiquetado

Los dispositivos se pueden asociar a etiquetas definidas por el usuario.

Las etiquetas se pueden utilizar para agrupar, describir, buscar o administrar dispositivos.

Las etiquetas permiten agrupar los dispositivos que se pueden utilizar en otras funciones.



Ejemplos de Etiquetado

Ejemplo: asociación de grupos de configuración a dispositivos.

Las reglas del grupo de configuración se pueden establecer para permitir que los dispositivos con etiquetas específicas se asocien automáticamente a ese grupo de configuración.

Agregar etiqueta

En Configuración->Dispositivos, se pueden crear/agregar/eliminar etiquetas de los dispositivos.

Etiquetar reglas en el grupo de configuración

En la página Configuration Group -> Associated Devices (Grupo de configuración -> Dispositivos asociados), se pueden agregar/editar reglas de etiquetas.

Ilustración

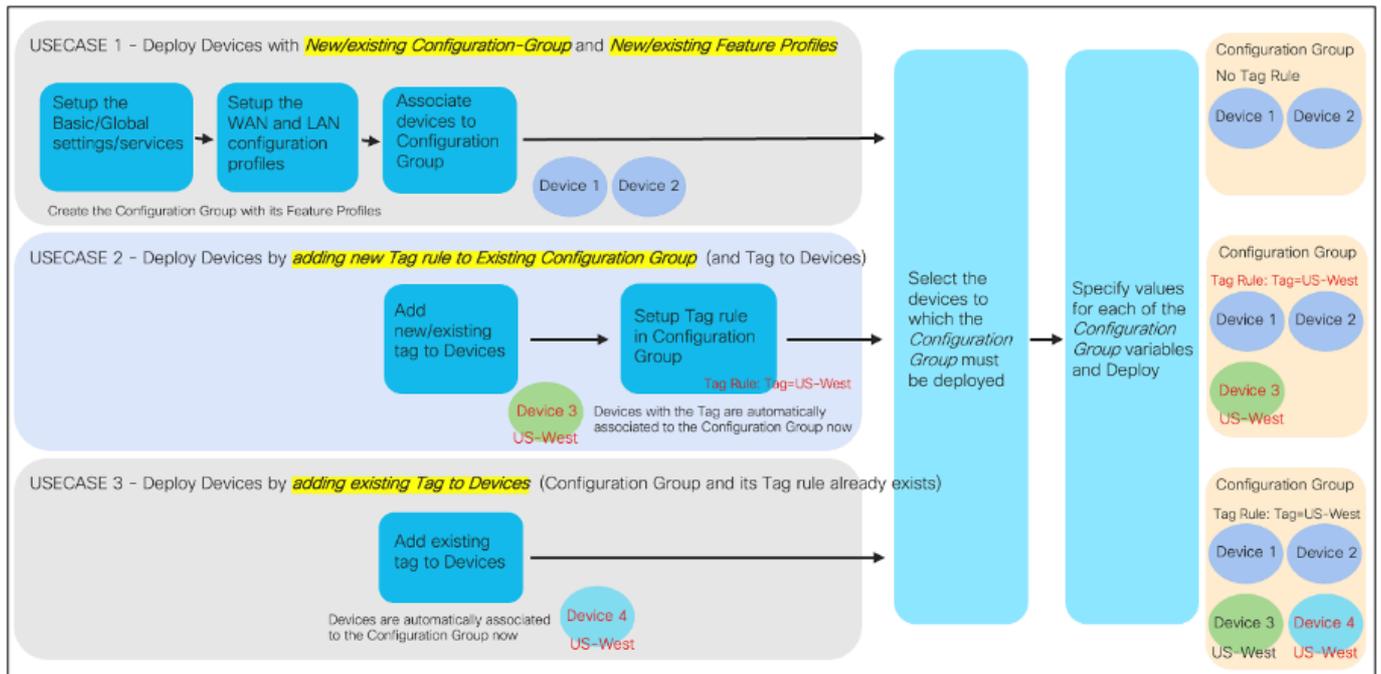


Ilustración de etiquetado

Implementaciones existentes

En la red SD-WAN, los dispositivos que utilizan la configuración y las políticas heredadas pueden coexistir con los dispositivos que utilizan la configuración y las políticas simplificadas.

En esta sección se ofrecen algunas recomendaciones para los clientes que deseen aprovechar la configuración y las políticas simplificadas. En esta sección se ofrecen algunas recomendaciones.

El primer paso consiste en migrar los dispositivos de Plantillas de dispositivos a Grupos de configuración. Una vez hecho esto, se pueden implementar grupos de políticas y/o topologías.

Grupos de configuración

Las plantillas de dispositivos y los grupos de configuración proporcionan la configuración del dispositivo periférico. Así que es fácil que la coexistencia ocurra. Los pasos para migrar de una plantilla de dispositivo a un grupo de configuración son:

| | |
|--------|--|
| Paso 1 | Extraiga una copia de los valores de dispositivo de las plantillas de dispositivo. Esto se logra desde la configuración à Templates, haga clic en los puntos suspensivos (...) a la derecha del grupo de dispositivos y seleccione "Exportar CSV". |
| Paso 2 | Cree un grupo de configuración (manualmente o con la herramienta de conversión). |

| | |
|--------|---|
| Paso 3 | Separe la plantilla de dispositivo del dispositivo. En este momento, el dispositivo mantiene la configuración en el punto de conexión, pero no recibe ningún cambio futuro realizado en la plantilla del dispositivo (ni en ninguna plantilla de funciones de componentes). |
| Paso 4 | Asocie los dispositivos al nuevo grupo de configuración. |
| Paso 5 | Implemente los dispositivos asociados al grupo de configuración. Para facilitar este proceso, abra el archivo CSV exportado y cambie los encabezados de columna CSV para que coincidan con las nuevas variables del grupo de configuración. |
| Paso 6 | Después de la pantalla de entrada variable del dispositivo, puede previsualizar la configuración del dispositivo. Esto le ofrece una vista previa de qué partes del grupo de configuración no coinciden con la instancia anterior o qué variables han cambiado desde la plantilla de dispositivo. |

El mantenimiento de un esquema de nombres coherente para las variables simplifica la configuración específica del dispositivo. Si todos los valores de dispositivo están en un único CSV, solo tendrá que cambiar el nombre de los encabezados de columna una vez.

NOTA: Existe un script de Python que funciona con archivos CSV para plantillas de dispositivo o grupos de configuración para consolidar y ordenar alfabéticamente los encabezados de columna. El guión está disponible aquí:

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

Grupos de políticas

Los dispositivos configurados mediante grupos de configuración pueden utilizar una política centralizada o migrar a un grupo de políticas, pero no ambos al mismo tiempo para la misma aplicación. Básicamente, el objetivo es mantener la misma política subyacente para los dispositivos periféricos. Los grupos de políticas combinan las políticas de datos y AAR originales en un único componente de prioridad de aplicación y PG de SLA. Básicamente, solo estamos cambiando la forma en que se crea la configuración para las políticas (pero no se envía al administrador de SD-WAN).

Es importante tener en cuenta que una política de datos o una política AAR no pueden hacer referencia a una lista de sitios con un sitio que tiene el componente Application Priority y SLA, ya que ambos configuran la misma configuración.

Es posible tener una política centralizada con solo una política de control (referencia a un sitio que

utiliza un grupo de políticas con prioridad de aplicación y SLA) a medida que configuran diferentes componentes de una política centralizada.

Los pasos para migrar un dispositivo desde una política centralizada a un grupo de políticas incluyen los siguientes pasos:

| | |
|--------|---|
| Paso 1 | Cree los componentes de grupo de políticas necesarios (Application Priority y SLA), seguridad integrada, gateway de Internet seguro/Secure Service Edge, seguridad DNS. |
| Paso 2 | Cree el grupo de políticas y asocie los componentes necesarios. |
| Paso 3 | Anule la asociación del identificador del sitio de cualquier lista de sitios que sean referencias en AAR o políticas de datos. En este momento, el administrador de SD-WAN envía la configuración actualizada a los controladores, que eliminan las instrucciones de políticas de datos activas de los dispositivos periféricos. Tenga en cuenta que esto podría provocar flujos de tráfico no deseados en este momento. |
| Paso 4 | Asocie los dispositivos al grupo de políticas y guarde el grupo de políticas. |
| Paso 5 | Implemente el grupo de políticas en los dispositivos seleccionados. En este momento, el administrador de SD-WAN envía configuraciones actualizadas a los dispositivos periféricos (para QoS/SIG) y a los controladores, de modo que los controladores pueden enviar políticas de datos actualizadas a los dispositivos periféricos. |

Nota: aunque los grupos de políticas pueden coexistir con una política centralizada, se recomienda mantener una política centralizada (para políticas de datos y AAR) mientras se convierten los dispositivos periféricos en grupos de configuración. A continuación, en ese momento, inicie la migración de la política centralizada a los grupos de políticas para obtener funcionalidad dentro del componente de prioridad de aplicación y SLA.

Esto se hace por pura simplicidad y para reducir la confusión entre el personal operativo.

NOTE:

El motor de grupos de políticas almacena los elementos en un formato diferente. Por lo

tanto, una lista de prefijos utilizada en una política centralizada se debe volver a crear en el grupo de políticas. Esto puede suceder para otras cosas como las listas de sitios, etc.

Topología

Los dispositivos que se configuran mediante grupos de configuración pueden utilizar una política centralizada o migrar a una topología. En esencia, el objetivo es mantener la misma política de control subyacente para los controladores SD-WAN. La topología es la última iteración de políticas de control.

Es importante tener en cuenta que una directiva de control no puede hacer referencia a una lista de sitios con un sitio que tiene una topología asociada, ya que ambos configuran la misma configuración.

Es posible tener una política centralizada con solo una política de datos y/o AAR, y una política de topología a medida que configuran diferentes componentes.

Pasos para migrar un dispositivo desde una política centralizada a un grupo de políticas:

| | |
|--------|--|
| Paso 1 | Crear los componentes de topología necesarios |
| Paso 2 | Anule la asociación de lados de la lista de topologías más antigua en la política centralizada. |
| Paso 3 | Anule la asociación de la ID del sitio de las listas de sitios a las que se hace referencia en las políticas de datos o AAR. En este momento, el Administrador de SD-WAN envía la configuración actualizada a los Controladores que luego eliminan cualquier configuración de topología activa para los sitios que se están migrando. Tenga en cuenta que esto podría provocar flujos de tráfico no deseados en este momento. |
| Paso 4 | Active la topología. En este momento, el Administrador de SD-WAN envía configuraciones actualizadas a los Controladores y modifica cualquier ruta que se transmita a los dispositivos de borde. |

Nota: Aunque la topología puede coexistir con una política centralizada, se recomienda mantener una política centralizada (para la topología y la manipulación de rutas) mientras se convierten los dispositivos periféricos en grupos de configuración. Entonces, en ese punto, comience la migración de la política

centralizada a la topología para la funcionalidad de modificación de topologías y manipulación de ruteo.

Esto se hace por pura simplicidad y para reducir la confusión entre el personal operativo.

Herramienta de conversión

Alcance

La herramienta de conversión realiza una conversión de 1 a 1 de las plantillas en grupos de configuración. La herramienta recopila las plantillas de una instancia del Administrador de SD-WAN, las convierte en grupos de configuración (incluidos perfiles de funciones y paquetes de funciones) y carga las construcciones recién convertidas en el Administrador de SD-WAN.

* Se espera que la conversión de políticas en grupos de políticas esté disponible en la herramienta de conversión en octubre de 2024.

Detalles de acceso

Hay disponible una versión beta de la herramienta. Para obtener más información, póngase en contacto con sdwan-ux-conversion-tool@cisco.com.

Cómo usarla

Requisito previo

Antes de utilizar la herramienta, asegúrese de que el Administrador de SD-WAN esté ejecutando 20.12.x. Si no es así, actualice a 20.12 antes de continuar.

Flujo de trabajo de herramienta de conversión

| | |
|--------|--|
| Paso 1 | Inicie sesión en la herramienta con las credenciales proporcionadas por Cisco. (Nota: No se trata de credenciales de CCO. Diríjase a sdwan-ux-conversion-tool@cisco.com para obtener más información). |
| Paso 2 | Seleccione el flujo de trabajo de la herramienta de conversión en la página de inicio. · Si ha realizado previamente este flujo de trabajo y tiene el archivo JSON con las configuraciones convertidas, debe seleccionar el flujo de trabajo 'Cargar desde un archivo'. |

| | |
|---------|---|
| Paso 3 | <p>Inicio de sesión:</p> <p>Proporcione la dirección IP o URL del administrador de SD-WAN junto con las credenciales de usuario.</p> <ul style="list-style-type: none"> · El usuario debe tener acceso de lectura y escritura. · Los campos de puerto y subdominio son opcionales. |
| Paso 4. | <p>Importar:</p> <p>Haga clic en el botón "Recopilar" para recuperar todas las construcciones heredadas (plantillas de dispositivos, plantillas de funciones, políticas y sus construcciones asociadas) del Administrador de SD-WAN.</p> <ul style="list-style-type: none"> · Una vez recopilado, debe descargar el archivo JSON que contiene todas las configuraciones. Este archivo se debe utilizar durante este paso más adelante en lugar de volver a recopilarlo desde el Administrador de SD-WAN. |
| Paso 5. | <p>Seleccione:</p> <p>Seleccione las plantillas y directivas que desee convertir en sus equivalentes nuevos. Haga clic en "Migrar" para convertir las construcciones seleccionadas.</p> |
| Paso 6. | <p>Transformación:</p> <p>Esta página muestra todas las construcciones recién convertidas. Cuando esté listo, haga clic en 'Cargar' para enviar estas configuraciones al administrador de SD-WAN.</p> <ul style="list-style-type: none"> · En el caso de que no esté preparado para enviar a SD-WAN Manager todavía, puede descargar estas configuraciones convertidas como un archivo JSON y utilizar el flujo de trabajo 'Cargar desde un archivo' en un momento posterior. |
| Paso 7. | <p>Resumen</p> <p>En este momento, las configuraciones se están introduciendo y creando en el Administrador de SD-WAN. A medida que se introducen las configuraciones, puede ver la barra de progreso. Una vez completada la carga, puede ver el resumen de las configuraciones cargadas.</p> <ul style="list-style-type: none"> · Puede utilizar los enlaces rápidos 'Grupos de configuración', 'Perfiles de funciones' y 'Grupos de políticas' para ver las nuevas construcciones en su |

| | |
|--|---|
| | <p>Administrador de SD-WAN.</p> <ul style="list-style-type: none"> · En el caso de un error o error, la reversión también está disponible en este paso. Al realizar una reversión, se eliminan todas las construcciones que se envían al administrador de SD-WAN durante este flujo de trabajo/sesión. |
|--|---|

Posterior a la conversión

Las nuevas construcciones ya están listas para utilizarse. Ejecute los pasos de la sección "Implementaciones existentes" para migrar los dispositivos a los grupos de configuración recién convertidos.

Consideraciones

- Las conversiones proporcionadas por la herramienta tienen por objeto servir de guía. Analice y pruebe antes de realizar la implementación en un entorno de producción.
- La herramienta no tiene en cuenta la capacidad independiente del dispositivo de los grupos de configuración. Los usuarios pueden analizar sus plantillas antes de seleccionar cuál convertir o analizar los grupos de configuración convertidos y asociar los dispositivos en consecuencia para beneficiarse de la capacidad independiente del dispositivo.
- Los nombres de variables y los valores globales de construcciones heredadas se copian en las construcciones recién convertidas.
- La herramienta no envía la configuración a los dispositivos. Después de realizar las conversiones, el usuario es responsable de separar los dispositivos de las plantillas y asociarlos a los nuevos grupos de configuración.

20.12 Consideraciones

| No. | Descripción del elemento |
|-----|---|
| 1 | La configuración de DNS debe enviarse a través del perfil de complemento de CLI al implementar el grupo de configuración en el perímetro que ejecuta una versión inferior a 17.12. |
| 2 | La creación de Topology requiere la selección de sitios en lugar de elegir un área definida en NHM. |
| 3 | El flujo de trabajo Crear grupo de configuración no crea una VPN512 ni una interfaz en esta VPN, en el perfil WAN. Si lo necesita, puede crearlo manualmente editando el grupo Configuración. |

| | |
|----|---|
| 4 | <p>Posibilidad de copiar/duplicar perfiles de funciones, política no admitida. Un conjunto de scripts Python puede realizar esta tarea y se encuentra:</p> <p>https://github.com/dbrown92700/configGroups/</p> |
| 5 | <p>Un perfil de objeto de directiva debe estar asociado al grupo de configuración antes de crear cualquier paquete de características relacionado con la configuración de directivas (directivas localizadas). Ejemplo: ACL</p> |
| 6 | <p>Importar CSV para variables de interfaz inserta punto y coma en la cadena y falla</p> |
| 7 | <p>La configuración de optimización de AppQoE (TCP Opt y DRE) y corrección de pérdidas (FEC y Pkt Dup) sigue utilizando plantillas y políticas heredadas. También se puede configurar a través del perfil CLI en grupos de configuración/políticas. (20,14 en paquete de interfaz de usuario)</p> |
| 8 | <p>Cloud OnRamp para SaaS sigue utilizando las plantillas/políticas anteriores.</p> |
| 9 | <p>TrustSec/SGT solo compatible con el perfil CLI</p> |
| 10 | <p>Compatibilidad con UC Voice/DSP Farm/SRST solo con el perfil CLI (a partir de 20.13 en paquetes de interfaz de usuario)</p> |

Información Relacionada

- Cisco SD-WAN y Cloud Networking Canal de YouTube:
<https://www.youtube.com/@CiscoSDWANandCloudNetworking>
- UX2.0 - Simplificación operativa: 1. Configuración de un sitio de router único:
<https://www.youtube.com/watch?v=98z-d3knd>
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).