Use IWAN to Improve Application Performance

Overview of Cisco Intelligent WAN (IWAN)

Cisco IWAN is a system that enhances collaboration and cloud application performance while reducing the operating cost of the WAN. This system leverages low-cost, high-bandwidth Internet services to increase bandwidth capacity without compromising the performance, availability, or security of cloud-based applications. Organizations can use IWAN to leverage the Internet as WAN transport, as well as for direct access to Public Cloud applications. See Cisco Intelligent WAN (IWAN) Design Guide, for more information.

positions the IWAN wizard workflow mostly for green field customers where the IWAN services need to be enabled for the first time. The enabled IWAN service cannot be modified for brown field customers. But customers can always overwrite the last-configured service by rewriting any of these services on required sites.

You can use to design, configure, and monitor the IWAN services for an enterprise. Cisco IWAN requires the configuration of DMVPN, PFR, AVC and QOS as part of enabling IWAN services on different devices.

Related Topics

Prerequisites for Enabling IWAN Services, on page 1

Configure IWAN Services Using the IWAN Wizard, on page 4

Prerequisites for Enabling IWAN Services

When designing or deploying IWAN services, configurations need to be decided. A network administrator needs to plan the branches on which the IWAN has to be enabled or reconfigured. In , you can access a set of CVD validated out of the box IWAN templates by navigating to Configuration > Templates > Features & Technologies > Feature Templates. All the templates under this Feature Templates folder are prefixed with "IWAN", and any new template that a user creates will automatically carry the IWAN prefix and will appear in the IWAN workflow.

The tags that are automatically used for the templates are as follows:

- DMVPN: IWAN-DMVPN

- PFR: IWAN-PFR
- QOS: IWAN-QOS
- AVC: IWAN-AVC
- ZBFW: DIA_ZBFW
- CWS: DIA-CWS

Note The Minimum software version required for the templates are as follows:

- IWAN-DMVPN–Cisco IOS Release 15.4 or later
- IWAN-DMVPN–Cisco IOS Release 15.4 or later
- IWAN-QOS–Cisco IOS Release 15.4 or later
- DIA-ZBFW–Cisco IOS Release 15.4 or later
- WAN-AVC– See What is AVC?
- DIA-CWS
  - Cisco Validated Designs (CVD)-Cloud Web Security (CWS) Integrated Services Router-G2 platform from Cisco IOS Release 15.2(1)T1 or later
  - CVD-CWS-Integrated Services Router-4000 platform from Cisco IOS Release 15.5(3)S1 or later

The tags that are used for the IWAN Hub and IWAN Branch Categories based on the Device roles are as follows:

- Hub Category:
  - Primary Controller: IWAN-HUB-Primary-Controller
  - MPLS Hub: IWAN-HUB-MPLS
  - Internet Hub: IWAN-HUB-Internet
- Branch Category:
  - Single Router Branch: IWAN-Branch-Single-Router
  - Dual Router Branch-MPLS: IWAN-Branch-Dual-MPLS
  - Dual Router Branch-Internet: IWAN-Branch-Dual-Internet

Users can create their own templates from the bundle templates or modify the out of the box design templates, which can be recreated from the CVD templates and displayed in the IWAN workflow.

Note If you want to use a user-defined IWAN DMVPN template in the workflow, you must create a template with the following tags:

1. IWAN-DMVPN
2. Device roles tag based on the device role and category
3. DHCP or STATIC depending on whether you want the DHCP option to be enabled/disabled in the IWAN workflow
4. EIGRP or BGP depending on the overlay protocol

Therefore, enabling the complete IWAN services through is done based on two categories, SITE and ROLE. SITE can be HUB or SPOKE, and ROLE can be X, Y, Z, and so on. Depending on this selection, the templates will be organized and displayed in sequence for users to fill in the values. At the end of the workflow, the summary of the configurations to be deployed on the network is displayed. When the Deploy button is clicked, the configurations are pushed to the network.

Important Notes

- Ensure that the interface loopback 0 IP address is configured on all Primary Controllers before deployment.
- The loopback IP of the Primary Controller should be permitted in the DC-LOCAL-ROUTES prefix-list in HUB-Border-MPLS and HUB-Border-Internet routers for Border routers to reach MC.

Example:

```
ip prefix-list DC-LOCAL-ROUTES seq 40 permit <MC loopback0 ip>/32
```

- The DC_Prefix1 field in CVD-DMVPN-MPLS and CVD-DMVPN-Internet templates should match the DC subnet. If there is more than one subnet in DC, then the suffix “le 32” can be used to include all the subnets.

Example:

- - Subnet A–172.29.10.0/30
  - Subnet B–172.29.10.4/30
  - Subnet C–172.29.10.8/30
  - DC_Prefix1(x.x.x.x/x)–172.29.10.0/24 le 32
- In CVD-DMVPN, CVD-DMVPN-Dual-Internet, and CVD-DMVPN-Dual-MPLS templates, the subnet mask of the Loopback interface needs to be entered in the Loopback-Subnet field.
- %IPSEC-3-REPLAY_ERROR: IPSec SA receives an anti-replay error.

If this error message is seen on the HUB-Border-MPLS router, you may be able to resolve this by increasing the window size.

Example:

```
crypto ipsec security-association replay window-size 1024
```

Related Topics

Overview of Cisco Intelligent WAN (IWAN), on page 1
Configure IWAN Services Using the IWAN Wizard, on page 4

Configure IWAN Services Using the IWAN Wizard

provides a wizard to help you design and deploy IWAN services.

Step 1 Select Services > Network Services > IWAN Enablement.

Step 2 Click Next to choose the configuration.

Step 3 Choose the category, device role, overlay protocol and the technologies (DMVPN, PFR, QoS, AVC, DIA-ZBFW, CWS) that will be enabled through this workflow.

The CWS technologies will be enabled only for Single Router Branch and Dual Router Branch-Internet.

Step 4 (Optional) Choose the Post-IWAN template that can be used for pushing the required configuration after IWAN deployment.

Step 5 Click Next to choose the devices on which you want to configure the specified features. To configure IWAN on multiple branches at the same time, select multiple devices and enter the values for each variable.

Step 6 Click Next to choose the input option.

Step 7 Click Work Flow option, the wizard will guide you through entering the necessary values for the selected configuration.

Step 8 Alternately, click Export/Import CSV option, to update all the template properties for the selected devices using CSV export/import mechanism.

a) Uncheck the Do you want Optional Parameters check box, if you want to skip the optional fields while filling the configuration value in the CSV file.
b) Click Export CSV to download the CSV template to your local system.
c) Enter the configuration values in the downloaded CSV template.
d) Click Import CSV to upload the updated CSV file.

Step 9 After entering the necessary configuration values, click Next or click CLI Summary to confirm the device and template configuration values.

Step 10 Schedule the deployment job using Prepare and Schedule tab, if required.

Step 11 Click Next or click Confirmation tab to deploy the template.

Post deployment, ensure that you enable routing between Primary Controllers and Hub Border Routers and include the subnet of the loopback 0 interface as part of the routing domain.

Related Topics

Overview of Cisco Intelligent WAN (IWAN), on page 1
Prerequisites for Enabling IWAN Services, on page 1
Configure PKI Certificate-Based Authentication on Devices Using IWAN (APIC-EM), on page 5

Configure PKI Certificate-Based Authentication on Devices Using IWAN (APIC-EM)

To use PKI certificates (for DMVPN only) in the IWAN workflow, you must first add a valid APIC-EM controller to . See Integrate APIC-EM Policy Information into Plug and Play. The PKI option cannot be enabled if the CNS gateway is selected in the Global PnP/ZTD Settings (Administration > Servers > APIC-EM Controller > Global PnP/ZTD Settings). This is optional when you want to use a pre-shared key for IWAN DMVPN.

In the IWAN work flow, when the PKI option is enabled, in the back-end, the device is added to the APIC-EM Inventory and the PKI service is triggered to install the PKI certification on the device. The device can download the certificate in HTTP.

When the device is in the managed state, it can be used for IWAN provisioning. Here, PKI certificate-based authentication is done instead of using a pre-shared key.

Step 1 Choose Services > Network Services > IWAN Enablement.

Step 2 In the Before You Begin section, click Next.

Step 3 In the Choose Configuration section, select a category, device role from the drop-down lists. DMVPN, PFR, QOS, AVC values are auto-populated once the device role is selected. But these values can be edited. DMVPN is for PKI certificates only.

Step 4 Check the Deploy PKI check box so that the user can enable PKI certificate-based authentication for DMVPN Tunnels. Click Next.

Step 5 In the Select Devices section, select the devices and click Next.

Step 6 In the Demo_DMVPN_TEMP section, enter the values in the fields under Loopback, MPLS Tunnel and EDGRP. Click Apply and then click Next.

Step 7 In the CLI Summary section, the CLI commands in the DMVPN template are displayed along with the values that were entered by the user in the Demo_DMVPN_TEMP section. Click Next.

Step 8 In the Prepare and Schedule section, click Next if you want the job to start now and not recur. If you want the IWAN job to run at a later time in a recurring pattern, then specify the time and recurrence under Schedule. Specify the Job Option, if required.

Step 9 In the Confirmation section, click Deploy to configure the device.

Step 10 The confirmation message appears. Click OK. The User Jobs pane under Administration / Jobs appears. The status of the IWAN DMVNP configuration and PKI certificate provisioning on the device can be tracked in the Job dashboard.

When either of the IWAN DMVPN config or PKI fail, the overall status of the IWAN provisioning will be displayed as “Failed” and the details will display whether the IWAN DMVPN configuration or the PKI failed.

For example, if there is any failure in the PKI IWAN service, an error message “Failed to install PKI certificate on device” will be displayed on the Job page of IWAN. When PKI service fails, all jobs will fail.

Related Topics

Overview of Cisco Intelligent WAN (IWAN), on page 1
Configure IWAN Services Using the IWAN Wizard, on page 4
Integrate APIC-EM Policy Information into Plug and Play