LTRSPG-2518

Configuring and Implementing SD-WAN network using Cisco SD-WAN (Viptela) solution

Sandeep Sharma – Product Manager
Nilesh Khade – Software Engineer

Learning Objectives

Upon completion of this lab, you will be able to:

Build understanding of Cisco-Viptela SDWAN solution capabilities and key functions, this includes Zero touch provisioning, Performance based Application path selection, Regional and Direct Internet Access, Policy based topology creation, and vManage (Management, orchestration) simple GUI interface for provisioning, configuration, policy management, device management, monitoring and troubleshooting.

Scenario

This lab includes the following scenario.

Scenario 1 – An overview of the SD-WAN vManage dashboard and discussion around Zero Touch Provisioning (ZTP) capability. Branch site routers, with design best practices, can easily be provisioned by leveraging automation through zero touch provisioning and centralized configuration. Centralized configuration utilizes the templates that can be pre-configured before device deployment

Scenario 2 – Use the Hybrid WAN connectivity over multiple WAN transport connections. Show connectivity could be established over any kind of transport, application steering over any transport. Use IP as transport to create flexible data plane topologies from full-mesh to Hub-n-Spoke to any arbitrary topologies. Deploy policy to create a strict Hub-n-Spoke topology for Corporate and IOT/PCI VPN segment. For GuestWiFi VPN in branches, only allow DIA.

Scenario 3 – Demonstrate with centralized policy to create different connectivity model/topologies per VPN segment. Corporate VPN – Full Mesh IOT/PCI Segment – Hub-n-Spoke GuestWiFi – Only DIA and no site-to-site communication

Scenario 4 – Demonstrate business defined insertion of services (FW, IPS, IDS, etc) utilizing centralized policies. Cisco SDWAN is a flexible architecture w here services can be deployed in any of the site(s) irrespective of the physical topology. Simple policy activation can make selected applications and sites go through the required service.

Scenario 5 – Application Firewalling using Centralized Policies

In this scenario, implement the policy as a centralized data policy where based on source and destination prefix match, traffic between BR1 and BR2 is dropped in VPN 20. The PCI/IOT segment only requires connectivity to DC from remotes. More granular matches can be done to limit certain applications and allow other applications to flow between the branches.

Scenario 6 - Use the Application aware routing along with arbitrary topology networking to show the business policy driven view of application classification, connectivity and QoS provisioning. Discuss Application Performance settings while highlighting the ability of the network to dynamically switch paths to preserve a consistent application experience

Scenario 7 - The remote offices all utilize a Guest Internet VPN which allows customers to browse the internet via Direct Internet Access. SD-WAN Security policy has been

activated on this guest VPN to protect them. Cisco SD-WAN Security can provide protection against known and unknown malware threats with AMP and Threat Grid.

Challenges

- Focus on Cost and Complexity
- Installing remote site networks is a time consuming, manual and expensive process
- Challenging process to translate application policy to network infrastructure configuration
- Lack visibility into transport health and impact on applications End-to-end WAN configuration is complex
- Lack of centralized configuration management, policy management and monitoring

Benefits

- Reduce Cost and Complexity
- Automated zero touch provisioning to accelerate time to market and reduce costs
- Centralized configuration management of ALL network devices via simple use of Templates
- Business policy definition and activation from centralized vManage
- Visibility into applications and transport health from centralized vManage
- Operational Simplicity

Key Solution Components

- Orchestrator to orchestrate secure communication among all SD-WAN components (vBond)
- Central management and provisioning system (vManage)
- Centralized controller for routing and policy (vSmart)
- Data Plane routers (vEdge)

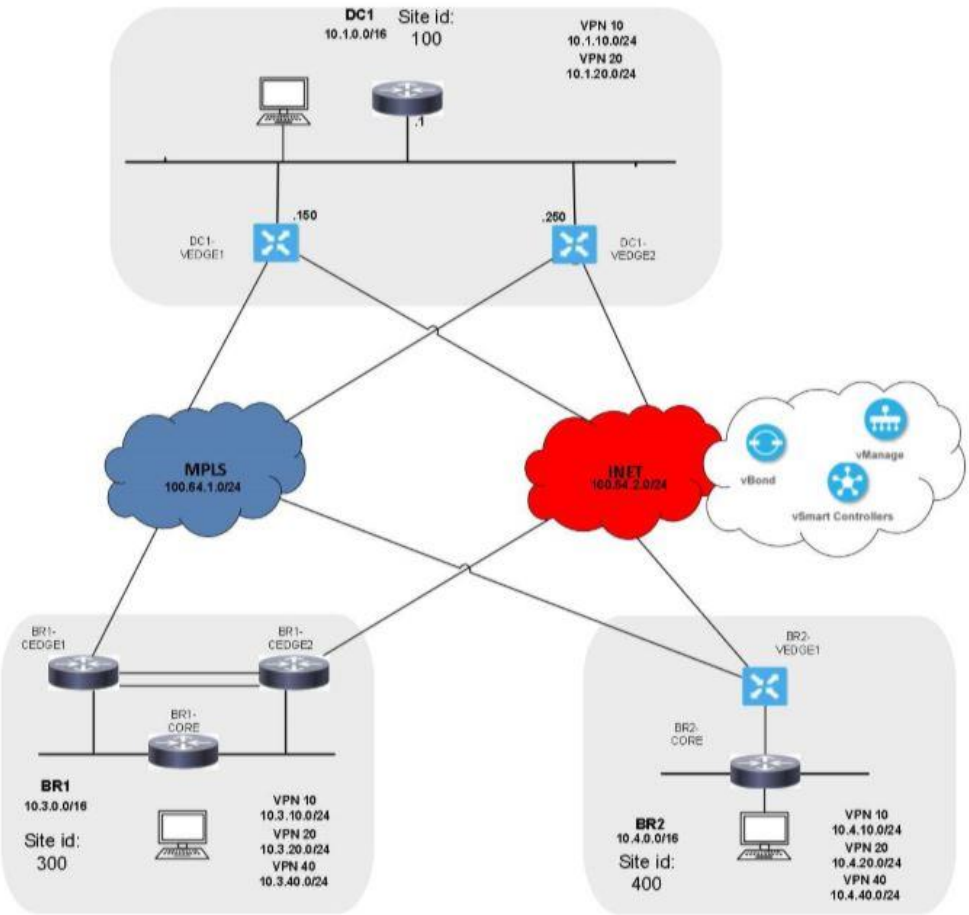
Topology

This content includes preconfigured users and components to illustrate the scripted scenarios and features of the solution. Most components are fully configurable with predefined administrative user accounts. You can see the IP address and user account credentials to use to access a component by clicking the component icon in the Topology menu of your active session and in the scenario steps that require their use.

The topology includes 1 Datacenter and 2 Remote Branches. The topology has 3 different VPN/VRF Segments.

1. Corporate VPN (VPN 10)
   Requires full mesh connectivity across ALL sites.
2. IOT/PCI Segment (VPN 20)
   Requires Hub-n-Spoke between the DC and the Branches.
3. GuestWifi (VPN 40): Not needed in the DC.
   From the branches require DIA. No Site-to-Site communications.

Figure 1. Topology



OSPF is running in the DC and Branch 2 in VPN 10. All other segments are using static routing/VRRP

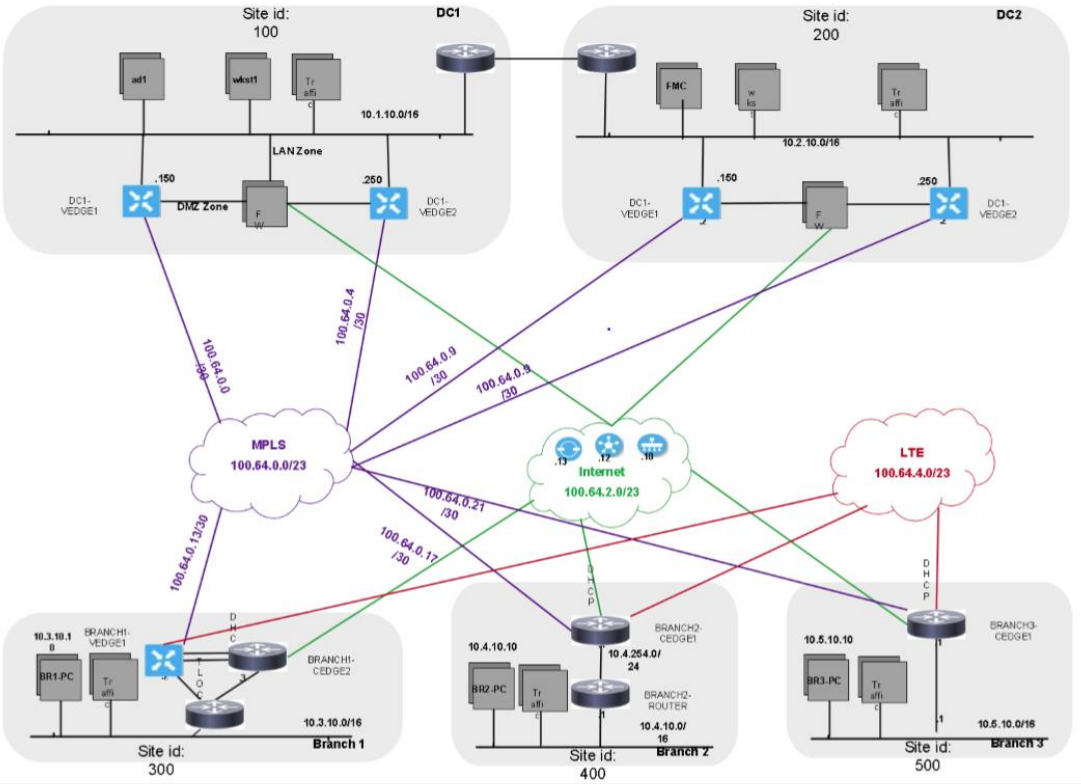
Table 1 : Host IPs for testing data plane connectivity

Site	Site ID	VPN10 (Test IP)	VPN20 (Test IP)	VPN40 (Test IP)
DC1	100	10.1.10.10	10.1.20.10	X
Branch 1	300	10.3.10.10	10.3.20.10	10.3.40.10
Branch 2	400	10.4.10.10	10.4.20.10	10.4.40.10

Table 2: Device Addresses

Device	System IP	Interface IP
vBond1	11.11.11.11	198.18.1.11
vBond2	21.21.21.21	198.18.1.21
vSmart1	12.12.12.12	198.18.1.12
vSmart2	22.22.22.22	198.18.1.22
vManage	10.10.10.10	198.18.1.10

Figure 2: Topology for SDWAN Security Overview (Optional)



Get Started

1. Initiate your session.

NOTE: It may take up to 10 minutes for your session to become active.

NOTE: To display the graphical data properly on vManage Dashboard, please let the dCloud session run for at least 45 minutes before conducting the demo.

2. For best performance, connect to the workstation with Cisco AnyConnect VPN and the local RDP client on your laptop

- Workstation 1: 198.18.133.36, Username: dcloud\administrator, Password: C1sco12345

Scenario 1. Zero Touch Site Bring Up

Management solutions are a crucial part of making Fast IT into a reality. The Cisco-SD Wan solution can effectively be managed on premise, in the cloud or with provider-managed offerings. One should not have to sacrifice critical solution capabilities based on the desire for a simplified control point.

vManage also provides open Northbound REST APIs that drive core network automations solutions and efficient operation.

Additionally, the vEdge routers also support a number of South-bound protocols that will enable your team to extend benefits to both Greenfield and Brownfield environments.

This scenario provides an overview of the Manage Branch Sites component to show the customer how devices are securely detected and provisioned leveraging automation through ZTP

NOTE: vManage periodically polls the statistical data from the devices. In order to display the graphical data properly on vManage Dashboard.
When bringing up the BR2-vEDGE1 for the first time it may take up to 20-30 minutes to display the Flow and DPI graphical data on the Device Dashboard.

Challenge

Provisioning remote sites is a time consuming, manual and expensive process.

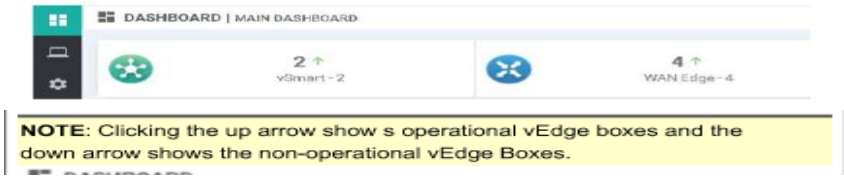
Benefits – Reduce Cost and Complexity

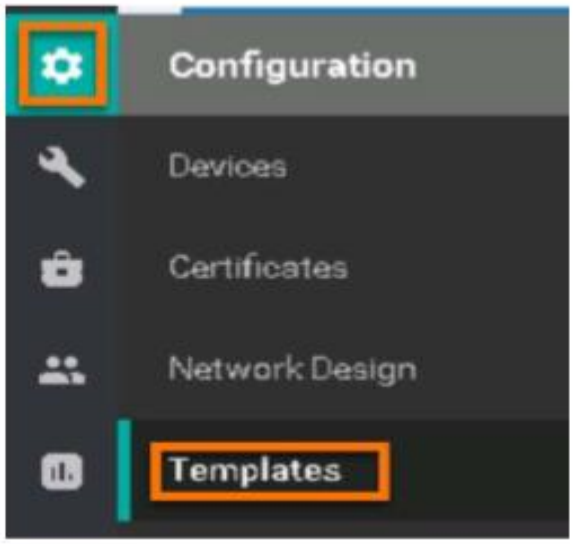
Automated and adaptive provisioning to accelerate time to market and reduce costs

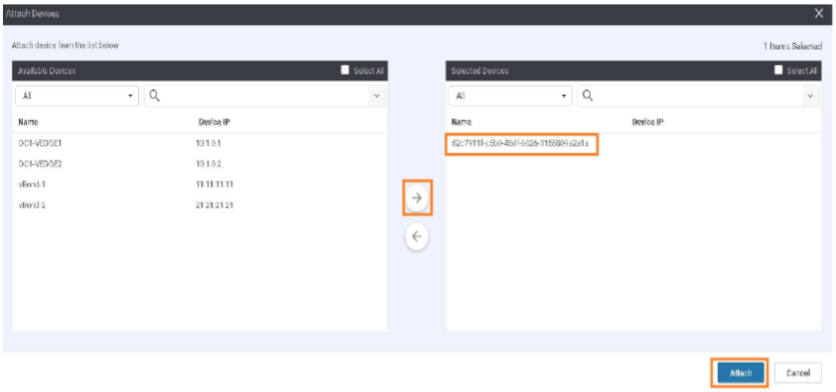
Objective

Bring up a branch on-line utilizing Zero Touch Provisioning (ZTP).

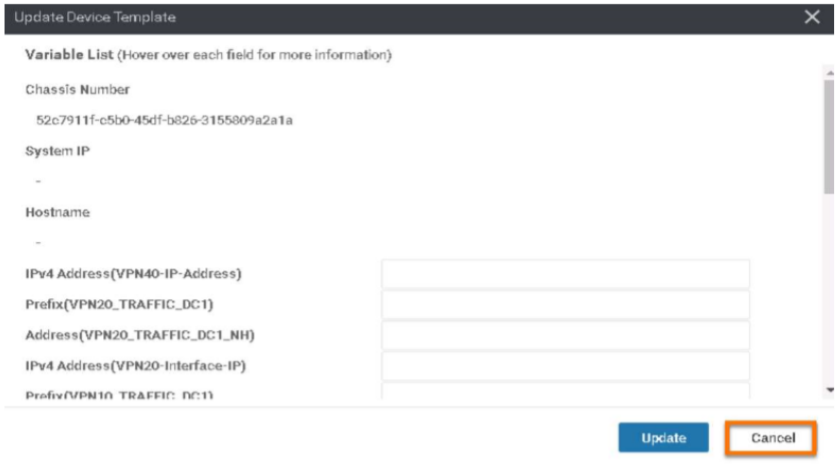
Steps

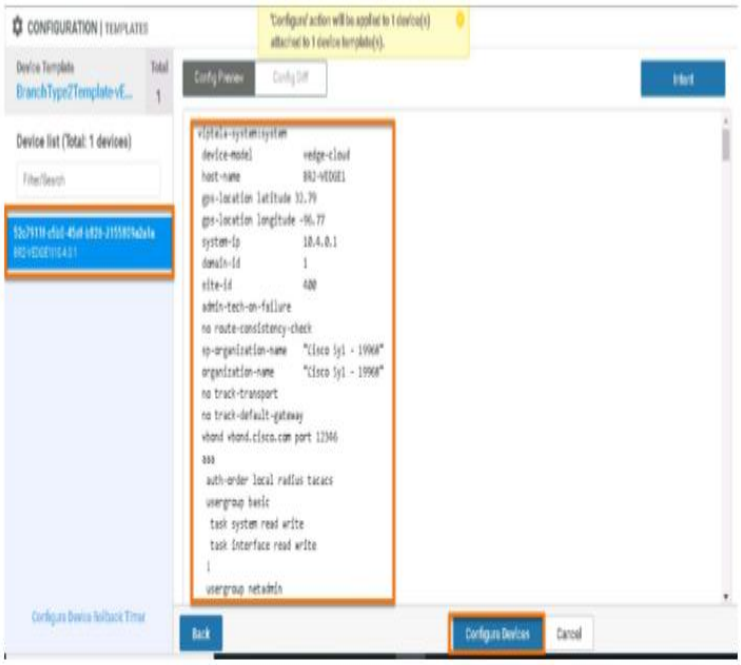
DIALOG	DEMONSTRATION STEPS
Deploy a branch using vManage configuration templates and Viptela's Zero Touch Provisioning (ZTP) service. The ZTP process simulated in this lab, using default configuration from the factory, for the vEdge in Branch 2. The only difference is the out of band VPN 512 configuration. This is configured for the demo user to be able to log in to the vEdge. The ZTP transport (ge0/0) in this case is in shutdown mode. A no shut will be done to simulate connecting vEdge to the transport.	1.Connect to Workstation 1 and launch the Chrome browser. 2.Click the bookmark for Viptela vManage and click through the security warnings to proceed to the vManage service. 3.Log in to vManage using username admin and password admin.  4.The vManage Dashboard displays the controllers that are up. There are four operational vEdges. Branch-2 vEdge is not provisioned yet. 
Configuring Templates Various preconfigured templates will be shown. We will select the preconfigured BranchType2 template to illustrate how a customer can use a template to facilitate and simplify the rollout of a new branch site.	5.Click on Configuration icon and select Templates from the drop-down menu.

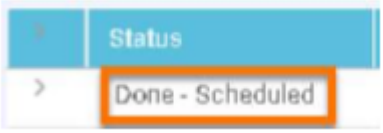
<table>
<tr>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>NOTE: We are selecting this device since it has not been provisioned.</td>
<td>6.Click on the three dots (...) in the right most column for BranchType2Template-vEdge. From the drop-down, select the option Attach Devices.
 

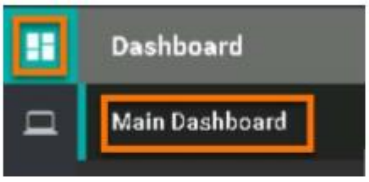
7.From the left pane labeled Available Devices, find the device with chassis-id/UUID of 52c7911f-c5b0-45df-b8263155809a2a1a.
8.Move the selected device to the right pane labeled Selected Devices by clicking on the right arrow.
 

9.Once the device is moved to the right pane, click Attach.
10.Click on the three dots (...) in the right most column and select Edit Device Template.</td>
</tr>
</table>

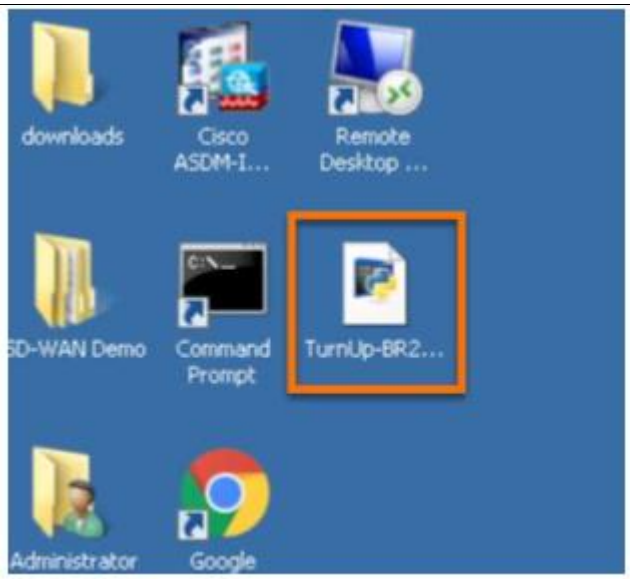
	 11. Click the Cancel button to go back to the previous page.
NOTE: The device values can be updated from the GUI interface, if desired. In this demonstration, we will use a predefined csv file with device values.	12. Click on the upload icon (Up arrow) for uploading the CSV file. 13. Click Choose File. 14. A Prebuilt CSV file named BranchType2Template.csv is in the folder \Desktop\SD-WAN Demo\csvConfigFiles on Workstation 1. 15. Click Open. 16. Click Upload. 17. To populate the values for the variables based on the uploaded CSV file, click Next. 
	18. Click the tab in the left column with BR2-VEDGE1 label to see the full configuration for validation. 19. Click Configure Devices.

<table>
<tr>
<td></td>
<td>


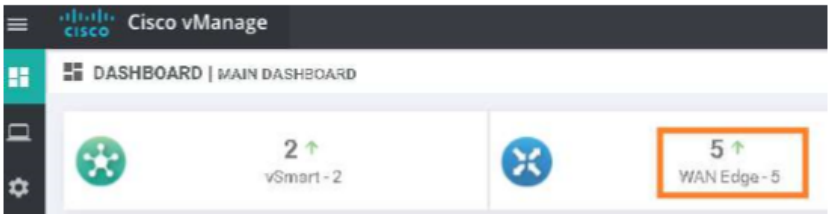
20. Wait for few seconds until the device status changes from In Progress to Done - Scheduled.


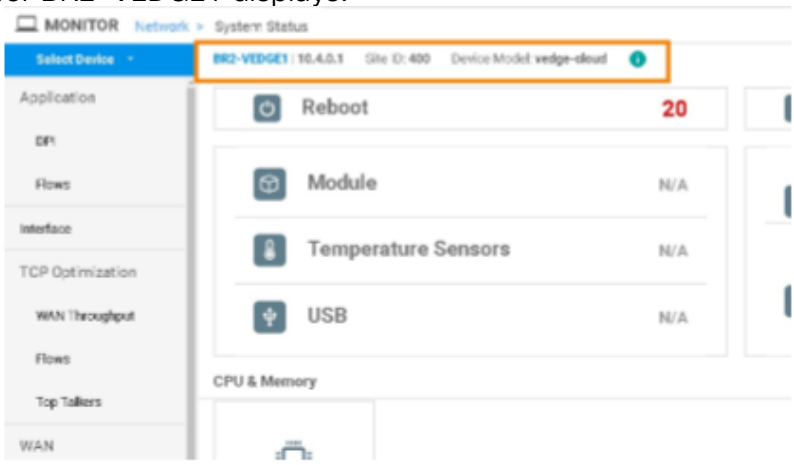
21. Click on the vManage Dashboard icon. The dashboard icon shows that Only 4 vedges are operational.


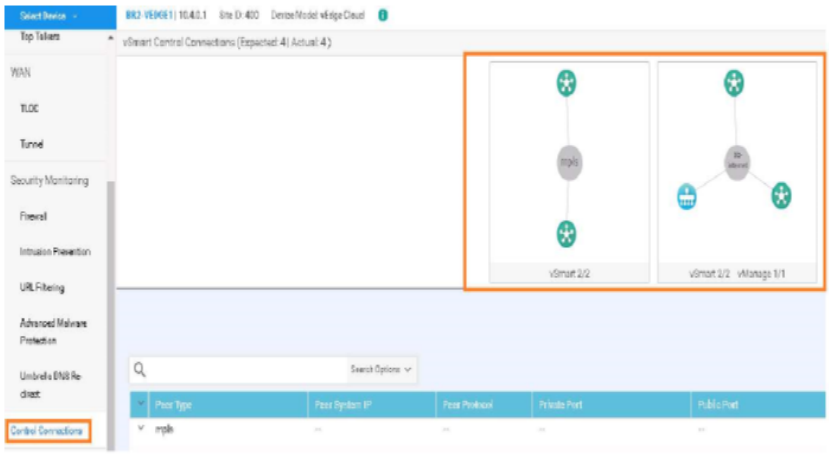
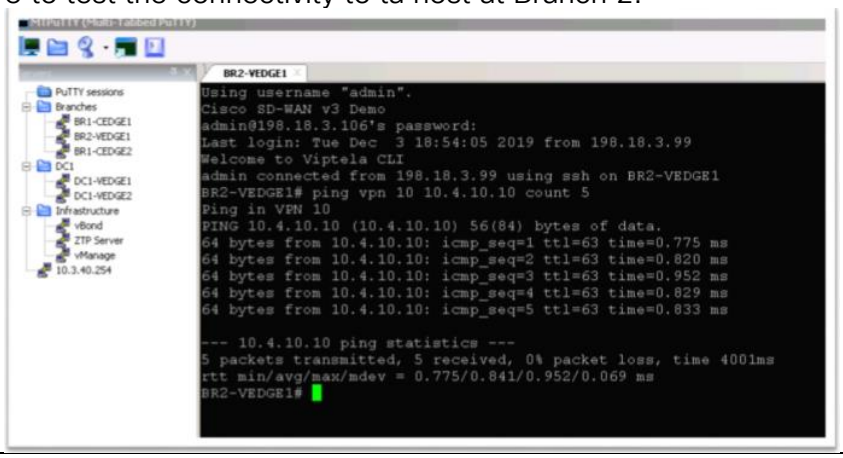
</td>
</tr>
<tr>
<td>NOTE: Accept any MTPutty security alerts to add the key to the Putty cache.</td>
<td>Simulate the Device to be Connected to the Transport for ZTP.
22. To activate the internet connection at Branch2, from the desktop,double-click the Python script named TurnUp-BR2-INET-Connection.py</td>
</tr>
</table>

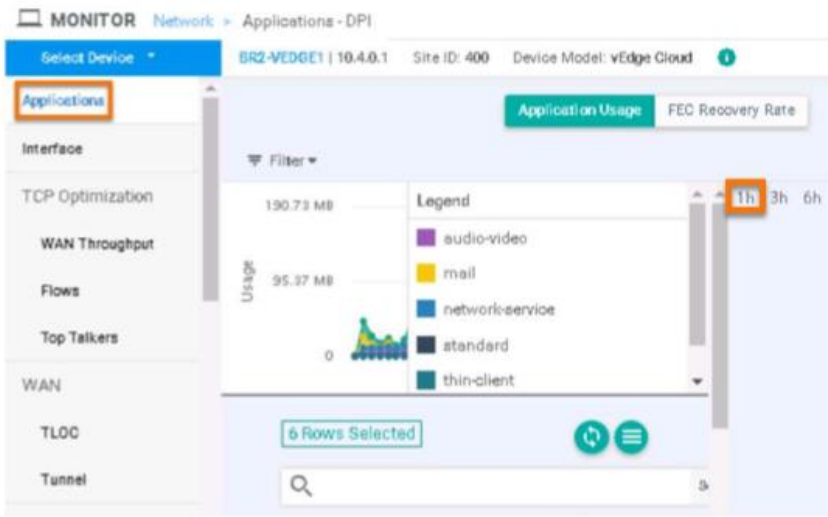
<table>
<tr><td></td><td> 
</td></tr>
<tr><td></td><td>23.Return to the vManage dashboard. The BR2-VEDGE1 will come up and the dashboard will show total of Five (5) Edge devices are operational.

NOTE: This may take a few minutes. Be patient.

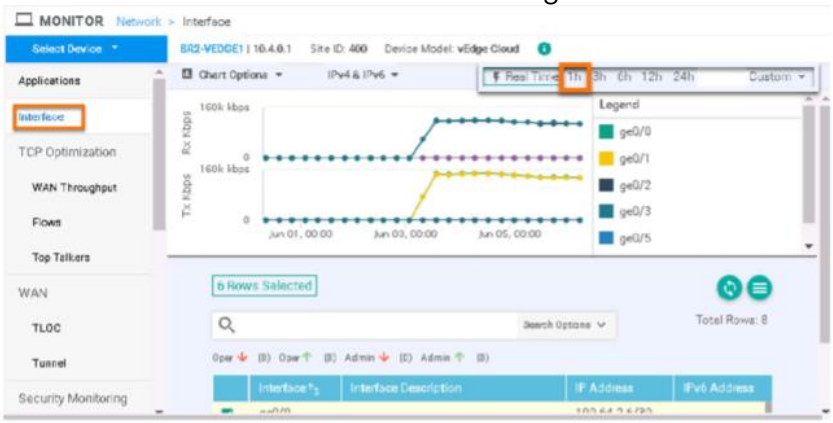
 

24. From the menu,select Monitor > Network
25. Select BR2-VEDGE1 from the list. The device dashboard for BR2-VEDGE1 displays.
 
</td></tr>
<tr><td>NOTE: At this time, there is no policy defined for the overlay and hence we have full-mesh connectivity across all three VPNs (10, 20, 40).</td><td>26. From the Monitor Device menu,Click on Control Connections. Validate that control sessions are established to</td></tr>
</table>

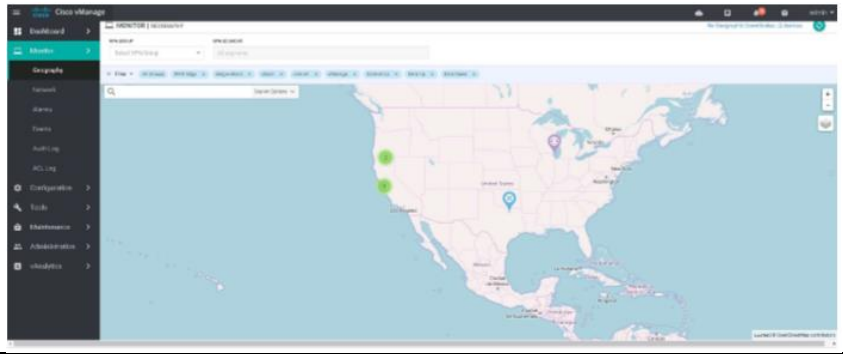
	vSmart and vManage. 
	27. To validate IP reachability within Branch2 VPN10,ping the VPN10 test host at 10.4.10.10. 28. Open the mPutty application.  29. Double click on BR2-VEDGE1. 30. On the command line, type ping vpn10 10.4.10.10 count 5 to test the connectivity to ta host at Branch 2. 
NOTE: If data does not display, adjust the Custom window to a larger date range or select BR1-VEDGE1 from the Select Device drop down at the top of the left column.	31. Return to Monitor > Network and select BR2-VEDGE1 from the list. 32. Click on DPI.



33.Click on Interface in left column menu and then click 1h to see utilization of the interfaces on the edge devices.



34.To View devices/site on map, go to Monitor> Geography. Hover your mouse over devices on the map to see the device details.



Scenario 2. Hub and Spoke Topology

Enterprises may not need a full mesh topology and would like to have a pure Hub-n-SpokeIPSec/BFD topology. This w ill provide the scalability and simplicity for the branches. A simple policy activation will convert full mesh connectivity to Strict Hub-n-Spoke.

In this case, we will create a fabric with IPSec tunnels only getting established between the spokes and the DCs. Based on policy we will not establish any IPSec tunnels between the branches.

For corporate VPN 10, we will only advertise the branch routes to the DCs and not to other Branches. The DCs are advertising default routes and hence when a branch needs to talk to other branches, they will take the default to the DCs. The DC vEdges then route the traffic back to the other remote Branches.

For the PCI/IOT segment (VPN 20), we will advertise the routes between the Branches by setting the next-hop pointing to the DCs TLOCs. This is being done to provide Hub-n-Spoke communication between the Branches through the DCs as there is no default route being advertised from the DCs.

For guest WiFi VPN 40, we don't need any communication between the branches. We will restrict the route exchange between sites for VPN 40. There will be only one static default route in VPN 40 providing direct internet access.

Challenge

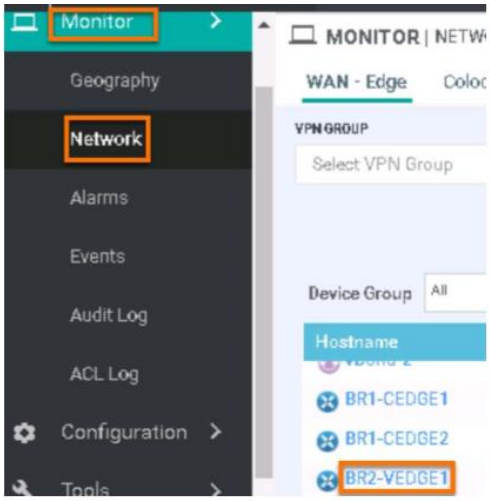
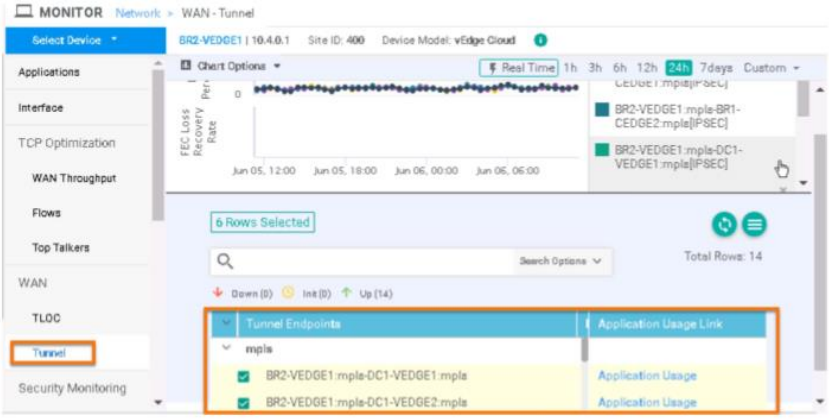
Arbitrary topology creation and management is a complex task and may require touching all the branches and/or the provider involved.

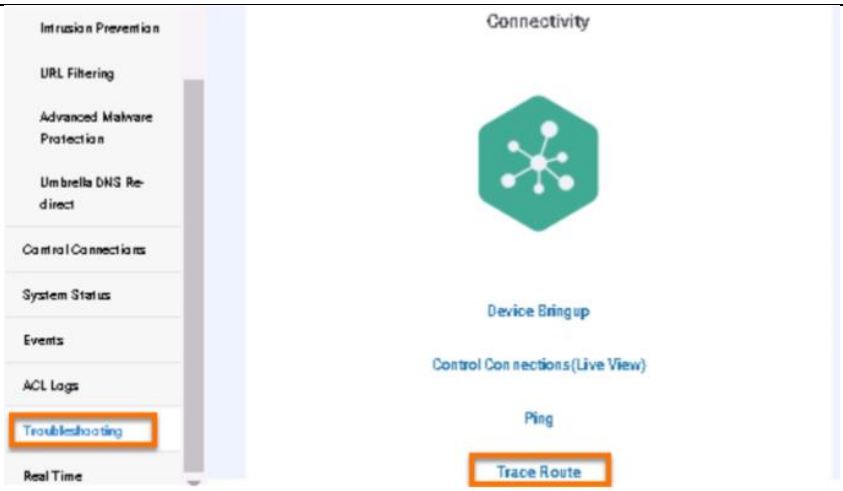
Benefits – Reduce Cost and Complexity

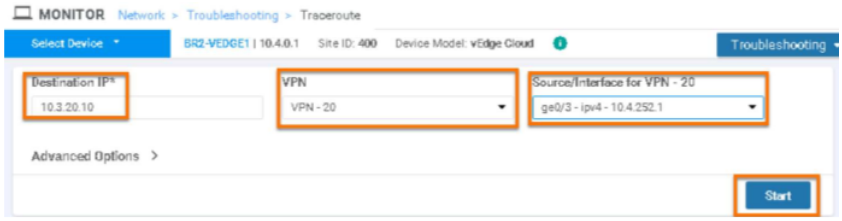
Simple activation of policy from central vManage. Results in simpler operations, reduced cost and reduction in time/effort.

Objective

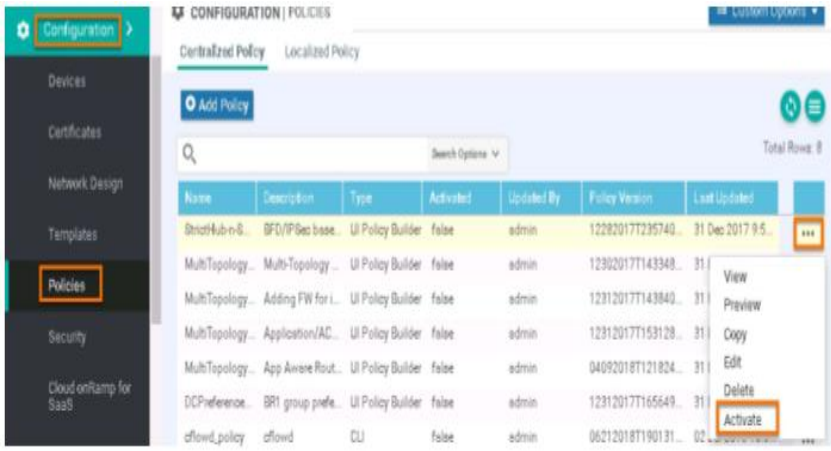
Use centralized control policy to create a Hub-n-Spoke IPSec/BFD topology while maintaining branch-to-branch communication for VPN 10 and VPN 20.

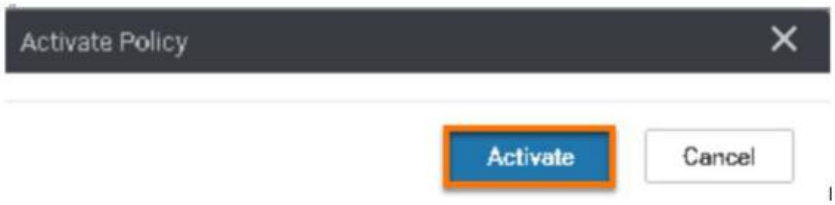
DIALOG	DEMONSTRATION STEPS
	1. Go to vManage. Click on the Monitor > Network. 2. Select BR2-VEDGE1. 
NOTE: The screen displays a subset of the established tunnels. **NOTE:** The tunnels highlighted on your screen may not be exactly like the screen shot shown in the guide.	3. Select Tunnel from the left column. 4. The next screen shows IPSec tunnels are established to the DCs and the remote Branch-1 (Full mesh). 
	5. Select Troubleshooting from the left column. 6. Select Trace Route under Connectivity.

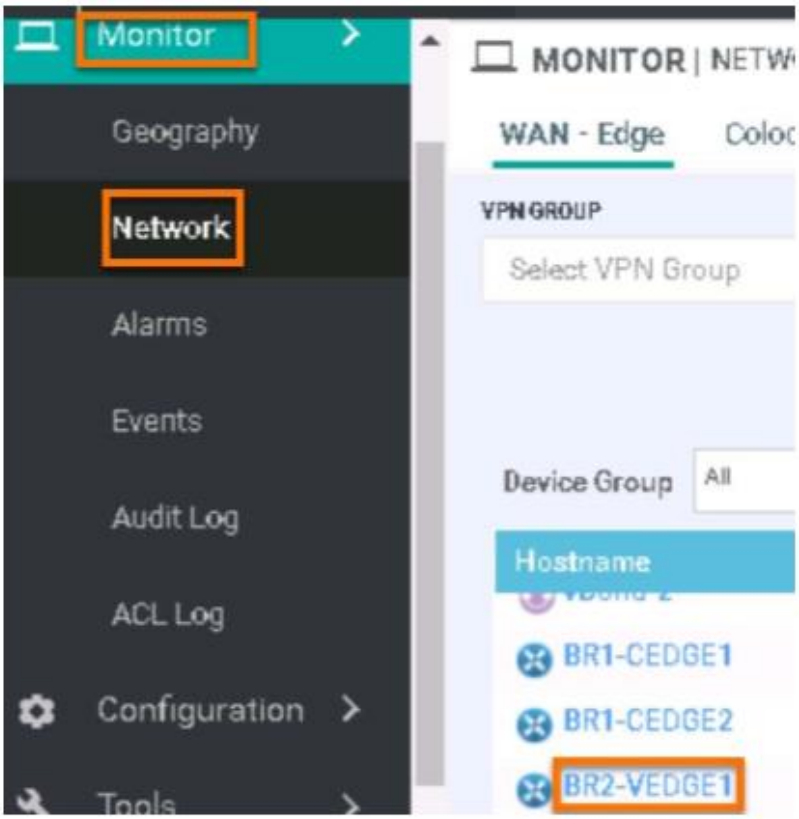
	
	7. In the Destination IP* filed, type 10.3.10.10, from the VPN dropdown,select VPN 10 and from the Source/Interface for VPN10,select the only available option from drop-down menu. 8. Click Start.  **NOTE**: The output on your screen may not be exactly like the screen shot shown in the guide. 
NOTE: The results of the following traceroutes will illustrate a direct (i.e. spoke-to-spoke) path taken from Branch2 to hosts within VPNs 10 and 20 at Branch1.	9. Deselect the current source interface. 10. In the Destination IP* filed, type 10.3.20.10, from the VPN dropdown,select VPN 20 and from the Source/Interface for VPN20,select the only available option from drop-down menu. 11. Click Start.

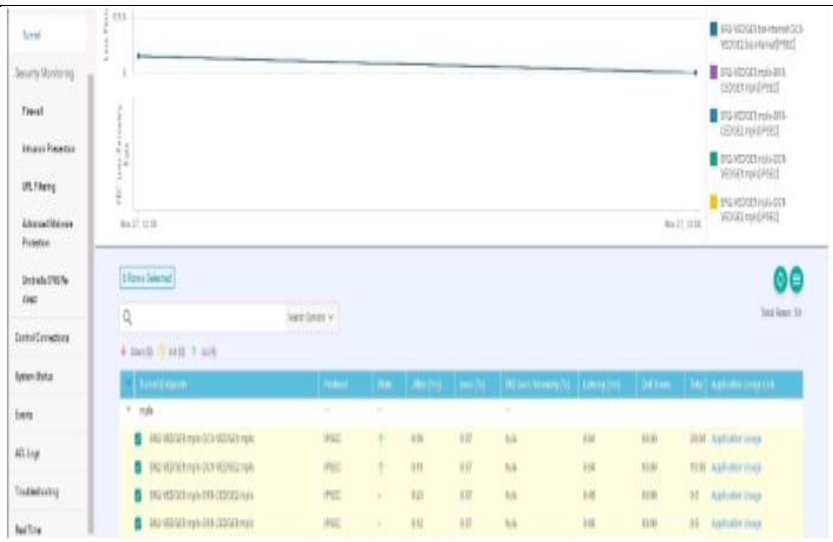
<table>
<tr>
<td></td>
<td> 

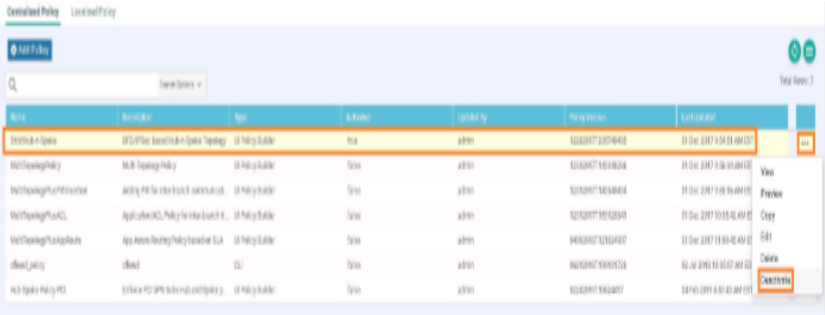
NOTE: The output on your screen may not be exactly like the screen shot shown in the guide.

 </td>
</tr>
<tr>
<td></td>
<td>Configure Policies
12. From the menu, select Configuration > Policies.
13. Click on the three dots (...) for StrictHub-n-Spoke.
14. Select Activate.


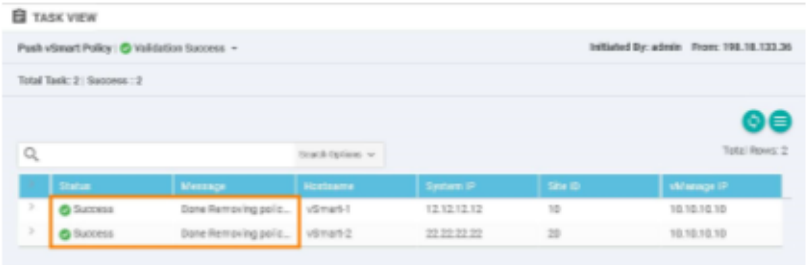
15. Click on Activate button on the pop-up.

</td>
</tr>
<tr>
<td>NOTE: The policy is applied to the vSmart controllers. vSmart will push the policies to the appropriate vEdge routers.</td>
<td>16. Wait until the policy activation Status changes to Success.</td>
</tr>
</table>

	
	17. Validate Strict Hub-n-Spoke topology by selecting Monitor > Network . 18. Select BR2-VEDGE1 
NOTE: Point out that only tunnels to the DC vEdges are in an operational UP state.	19. Select Tunnel from the left column.

	
NOTE: If you have observe now the inter-branch traffic now traverses the DC for VPN20.	20. Select Troubleshooting from the left column. 21. Select Trace Route. 22. Trace the route from BR2 to BR1 by entering 10.3.20.10 and selecting VPN 20. 
NOTE: The output on your screen may not be exactly like the screen shot shown in the guide.	
	23. To de-activate the policy, select Configuration > Policies. 24. Highlight the StrictHub-n-Spoke policy and click the three dots (...) to the right of the policy name.



25. Click Deactivate.
26. The policy status will change from In Progress to Success, and the policy is successfully removed from vSmart-1 and vSmart-2. Full mesh connectivity has been restored.



Scenario 3. Multi-Topology - Different Topologies Per VPN

Enterprises may have multiple VPN segments and may need different connectivity models/topologies. The default in Cisco SD-WAN is to have full mesh for all VPNs. In scenario 2 we demonstrated how you can restrict ALL VPNs to be Hub-n-Spoke.

In this scenario we will demonstrate the following topologies for different VPNs using policies.
Corporate VPN 10 – Full Mesh
PCI/IOT VPN 20 – Hub-n-Spoke
GuestWiFI VPN 40 – DIA ONLY in Branches

Challenge

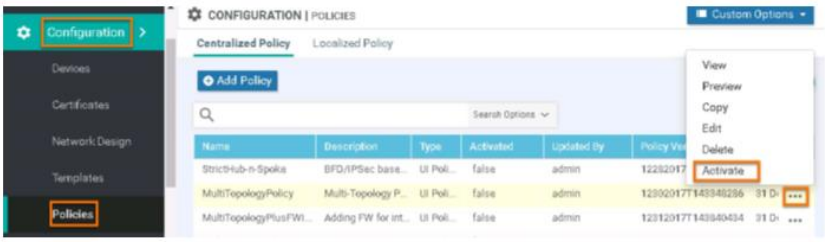
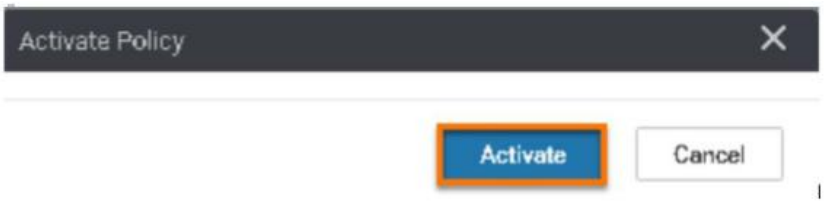
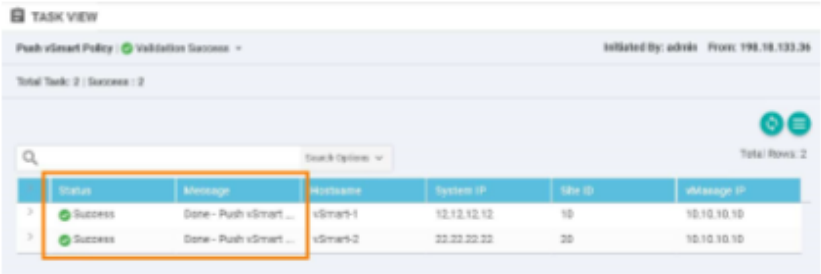
Arbitrary topology creation and management is a complex task and may require touching all the branches and/or involving the provider

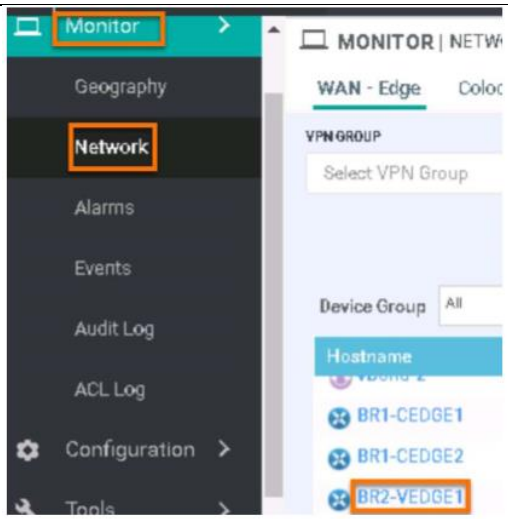
Benefits – Reduce Cost and Complexity

Simple activation of policy from central vManage. Results in simpler operations, reduced cost and reduction in time/effort.

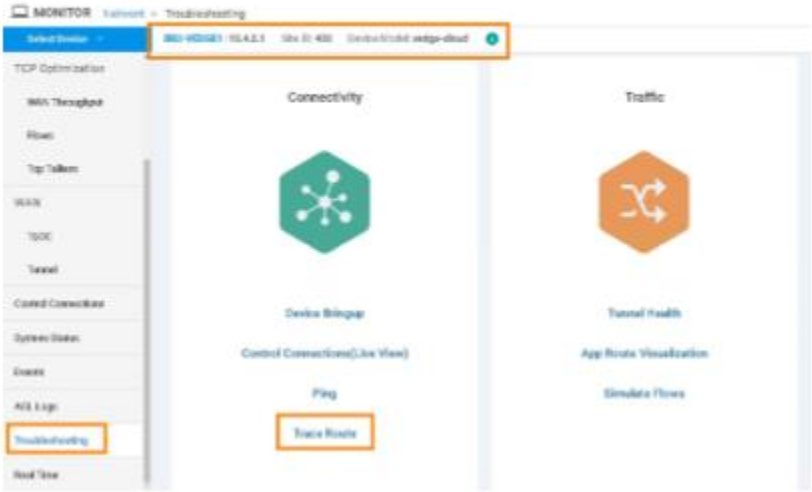
Objective

Create different connectivity topologies per VPN
- Corporate VPN 10 – Full Mesh Topology
- IOT/PCI VPN 20 – Hub-n-Spoke GuestWiFi
- VPN 40 – DIA Only Branches

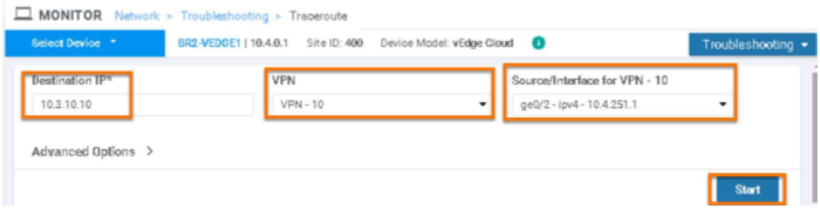
DIALOG	DEMONSTRATION STEPS
Result shows direct path between Branch1 and Branch2 for VPN 10.	1. Go to vManage. Click on the Monitor > Network. 2. Select BR2-VEDGE1. 3. Select Troubleshooting from the left column. 4. Select Trace Route. 5. Enter 10.3.10.10 as the destination IP. 6. Select VPN 10 from drop down menu. 7. Click on Start button.
Result shows direct connectivity between Branch1 and Branch2 for VPN20	8. Do the same for VPN20 using destination IP of 10.3.20.10.
	9. From the menu, select Configuration > Policies . 10. Click on the three dots(...) to the right of MultiTopologyPolicy.  11. Click on Activate. 
	12. When the policy has successfully been pushed to the VSmarts, the activation status changes to Success. 
Validate Full Mesh for VPN 10 and Hub-n-Spoke for VPN 20	13. From the menu, select Monitor > Network. 14. Click BR2-VEDGE1.

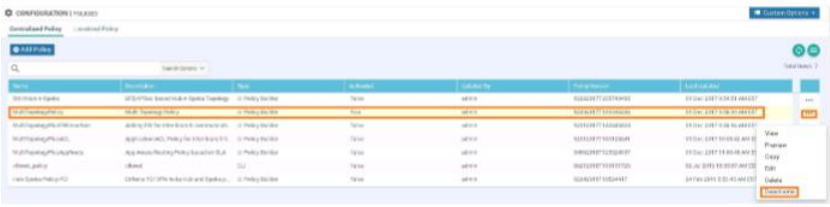


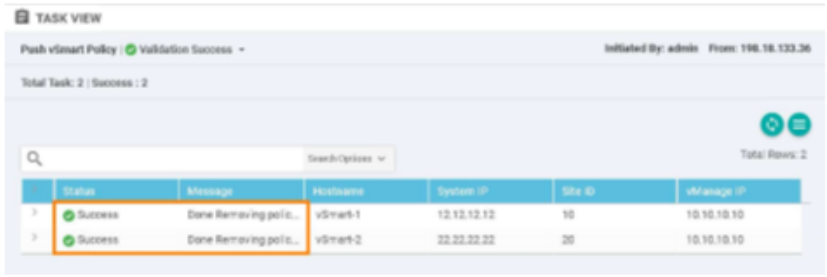
15. Select Troubleshooting from the left column and then click Trace Route.



16. In the Destination IP* field, type 10.3.10.10, from the VPN dropdown, select VPN 10 and from the Source/Interface for VPN 10, select the only available option from drop-down menu.
17. Click Start.



NOTE: If the output yields **n/a** results, click **Start** again or redo the entire trace route steps above. **NOTE**: The output on your screen may not be exactly like the screen shot shown in the guide.	
	18. Deselect the current source interface. 19. In the Destination IP* field, type 10.3.20.10, from the VPN dropdown, select VPN 20 and from the Source/Interface for VPN 20, select the only available option from drop-down menu. 20. Click Start. 
NOTE: If the output yields **n/a** results, click **Start** again or redo the entire trace route steps above. **NOTE**: The output on your screen may not be exactly like the screen shot shown in the guide.	 21. Result display the connectivity between Branch1 and Branch2 through the DC.
	22. To de-activate the policy, select Configuration > Policies. 23. 10. Highlight the MultiTopologyPolicy policy and then click the three dots (...) to the right of the policy name. 24. Select Deactivate. 
	25. Click Deactivate. 26. The policy status will change from In Progress to Success, and the policy is successfully removed.

Scenario 4. Service Insertion – Regional/DC Firewall

When new branches are added from an acquired entity, the enterprise may initially want the direct branch to branch communication to go through the FW in the DC or a Colo/Regional facility hosting FW services.

Using Cisco SD-WAN one can place service anywhere in the network and, based on policies, can make certain flows/sites have traffic go through those services.

Challenge

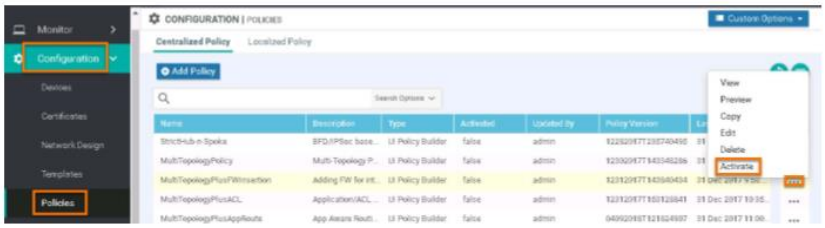
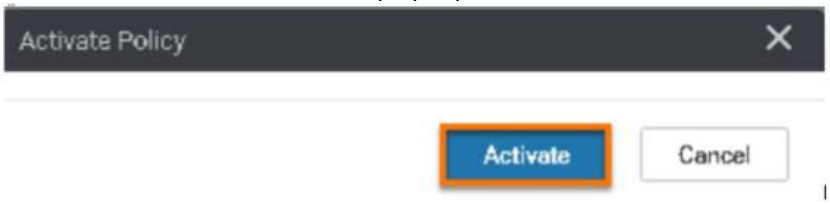
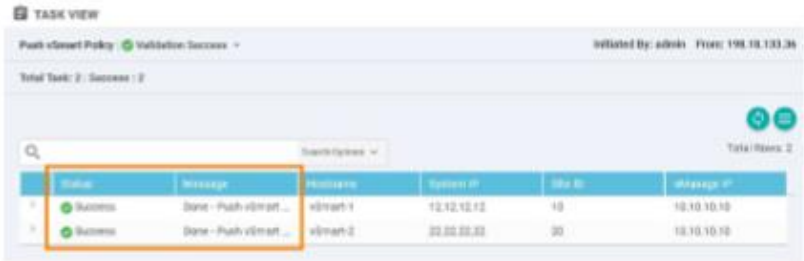
Arbitrary topology creation and management is a complex task and may require touching all the branches and/or involving the provider. Previously, Firewall or any other service had to sit in path but with service insertion the Firewall could sit in any of the enterprise locations.

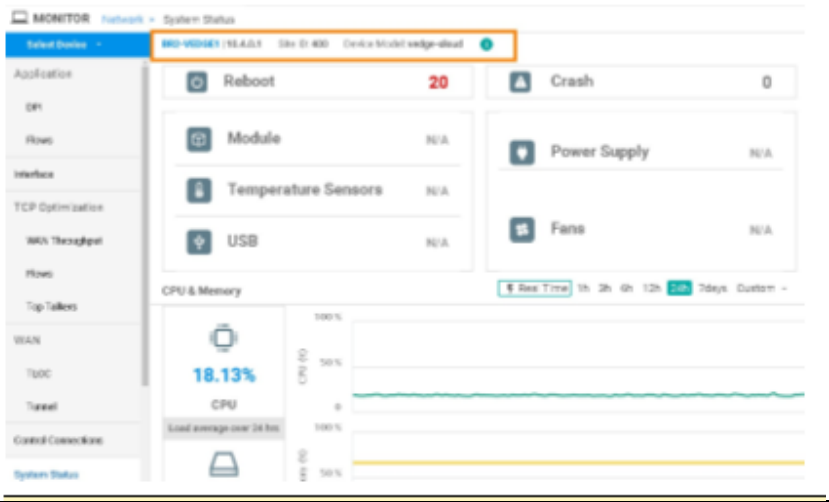
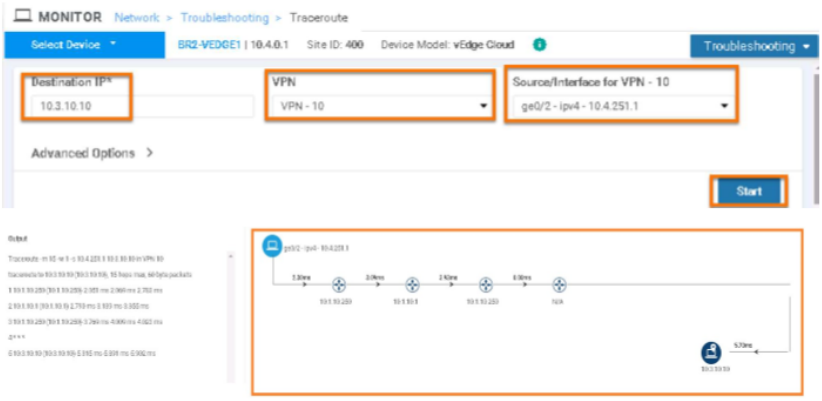
Benefits – Reduce Cost and Complexity

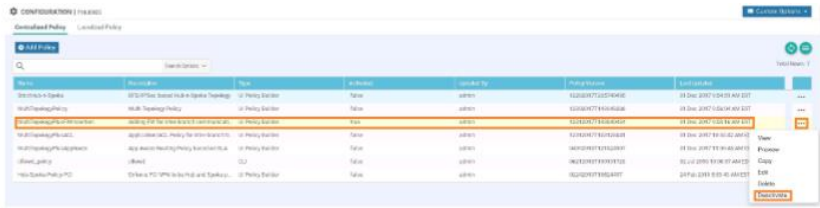
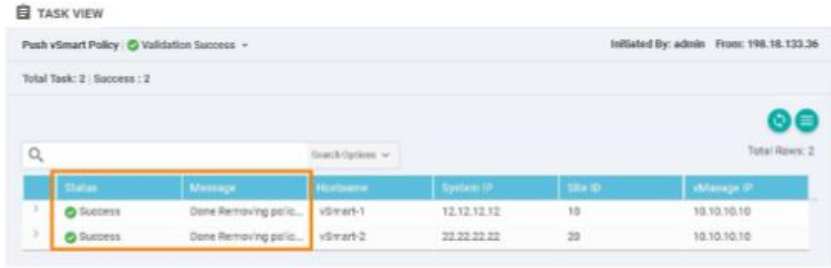
Simple activation of policy from central vManage. Results in simpler operations, reduced cost and reduction in time/effort.
Ubiquitous deployment of security controls via firewall and IPS service insertion policies.

Objective

Have to deploy/define FWs in DC1 and DC2 for corporate VPN 10.
Based on policy have the Branch to Branch traffic go through the Firewall for corporate VPN 10.

DIALOG	DEMONSTRATION STEPS
Result shows direct path between Branch1 and Branch2 for VPN 10.	1. From the menu, select Configuration > Policies. 2. Click the three dots(...) to the right of the policy named MultiTopologyPlusFWInsertion. 3. Select Activate. 
	4. Click Activate on the pop up. 
	5. Wait until the policy is successfully pushed to each vSmart. 
	6. From the menu, select Monitor > Network. 7. Click on BR2-VEDGE1.

	
	8. From the left column, select Troubleshooting. 9. Select Trace Route. 10. In the Destination IP* field, type 10.3.10.10, from the VPN dropdown, select VPN 10 and from the Source/Interface for VPN 10, select the only available option from drop-down menu. 11. Click Start.
NOTE: If the output yields **n/a** results, click **Start** again or redo the entire trace route steps above. **NOTE**: The output on your screen may not be exactly like the screen shot shown in the guide. **NOTE:** You can see that traffic between branches is being rerouted through the data center where a firewall is inspecting traffic.	
	12. Deselect the current source. 13. In the Destination IP* field, type 10.3.20.10, from the VPN dropdown, select VPN 20 and from the Source/Interface for VPN 20, select the only available option from drop-down menu. 14. Click Start.

	
NOTE: If the output yields **n/a** results, click **Start** again or redo the entire trace route steps above. **NOTE**: The output on your screen may not be exactly like the screen shot shown in the guide.	
	15. From the menu, select Monitor > Policies . 16. Click the three dots (...) to the right of the MultiTopologyPlusFWInsertion policy. 17. Select Deactivate. 
	18. The policy status will change from In Progress to Success, and the policy is successfully removed from the vsmarts. 

Scenario 5. Application Firewalling using Centralized Policies

In this scenario, implement the policy as a centralized data policy where based on source and destination prefix match, traffic between BR1 and BR2 is dropped in VPN 20. The PCI/IOT segment only requires connectivity to DC from remotes. More granular matches can be done to limit certain applications and allow other applications to flow between the branches.

Challenge

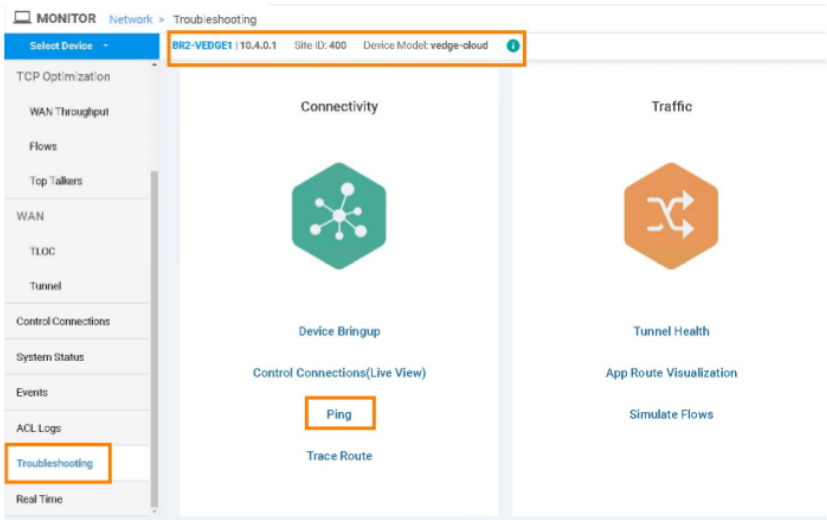
Implementation and maintenance of router-based FW/ACL rules requires touching all the branch routers.
This is a manual and complex task, prone to human errors and may require considerable time and effort.

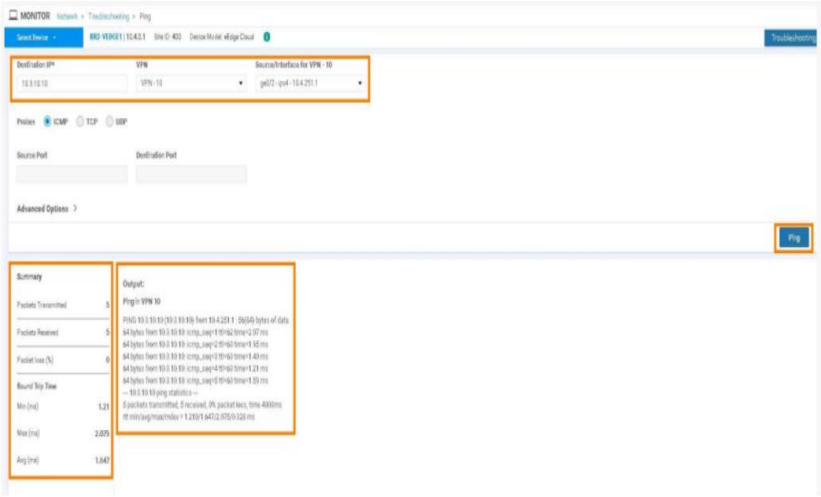
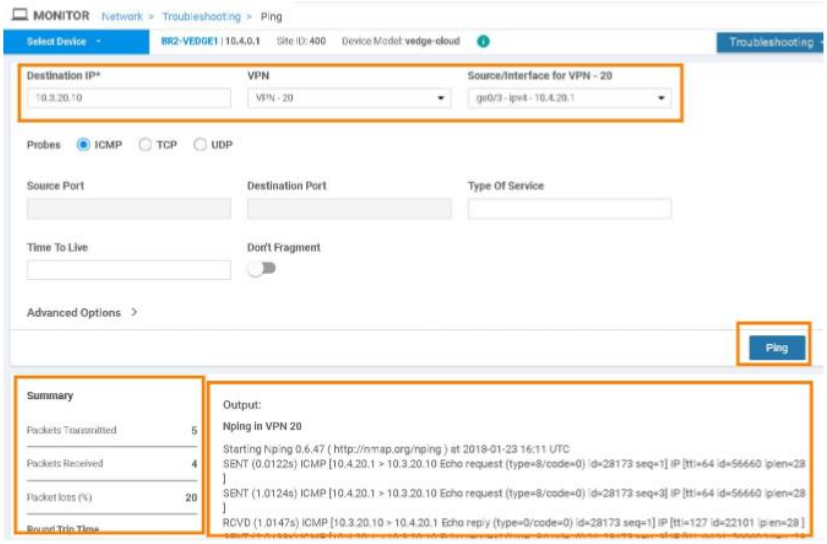
Benefits – Reduce Cost and Complexity

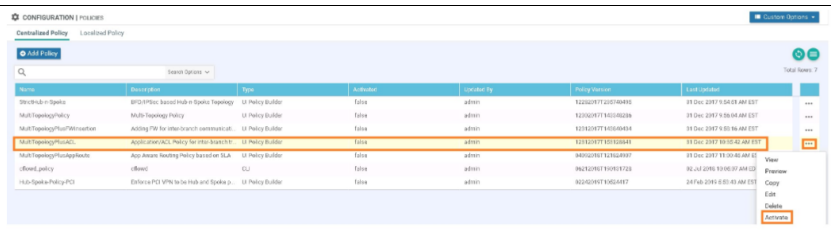
Simple activation of policy from central vManage results in simpler operations, reduced cost, and reduction in time and effort.
Consistent and centralized policy deployment reduces the risk of missed policy application and human error.

Objective

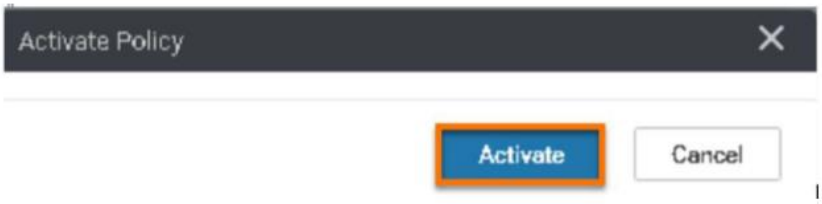
Deploy additional data policy to drop traffic between Branch 1 and Branch
The Multi-Topology control policy must remain in place

DIALOG	DEMONSTRATION STEPS
	1. From the menu, select Monitor > Network. 2. Select BR2-VEDGE1. 3. Click Troubleshooting. 4. Click Ping. 

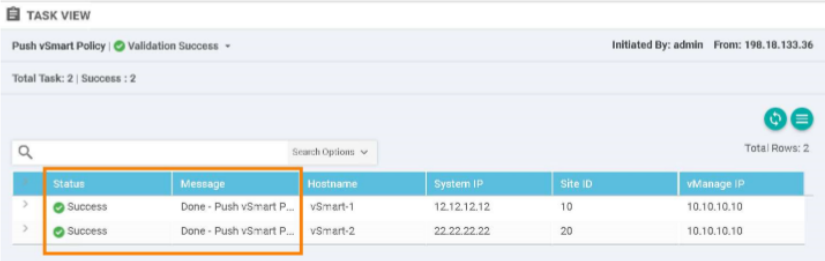
	5. Validate Connectivity from BR2-VEDGE1 to test host in Branch1 in VPN 10 by entering destination ip 10.3.10.10 6. Click Ping. 
	7. Deselect the current source interface. 8. Validate Connectivity from BR2-VEDGE1 to test host in Branch1 in VPN 20 by entering destination ip 10.3.20.10 
	1. From the menu, select Configuration > Policies. 2. Click on the three dots (...) to the right of the MultiTopologyPlusACL policy. 3. Select Activate.

<table>
<tr>
<td></td>
<td>


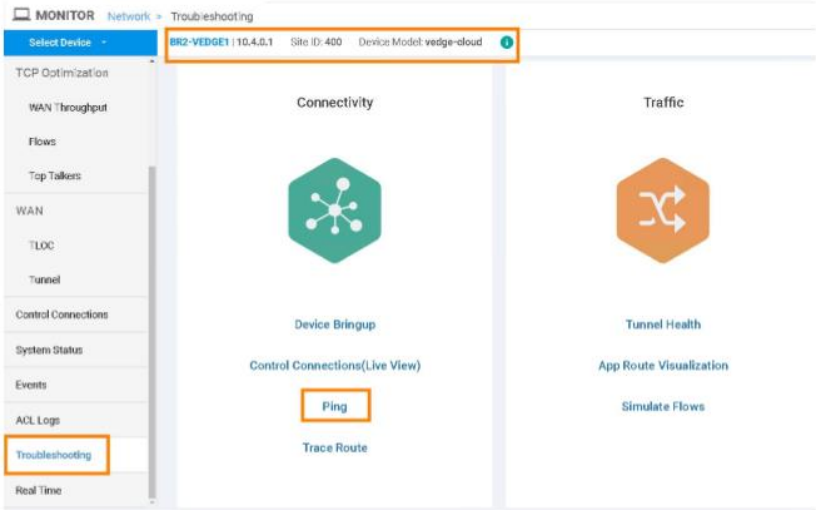
4. Click Activate on the Pop up.



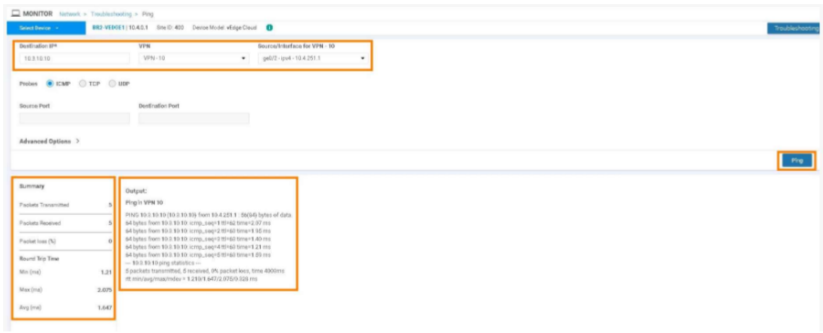
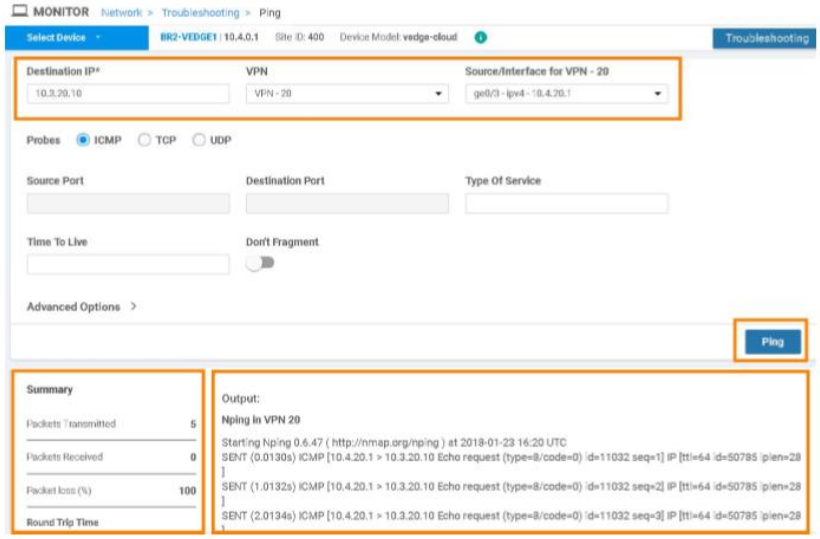
5. Wait until policy is successfully to pushed to each vsmart.

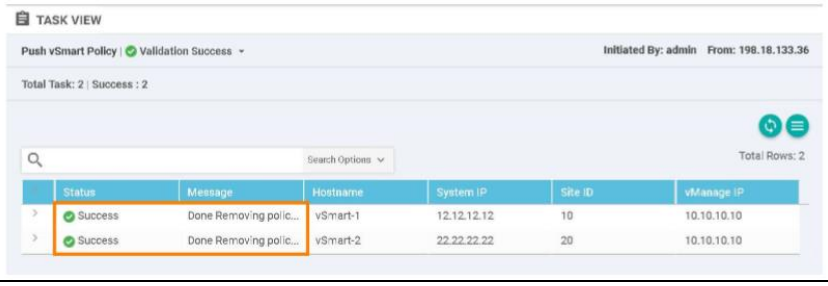


</td>
</tr>
<tr>
<td></td>
<td>
6. From the menu, select Monitor > Network.
7. Select BR2-VEDGE1.
8. Click Troubleshooting.
9. Click Ping.



</td>
</tr>
<tr>
<td></td>
<td>
10. Validate Connectivity from BR2-VEDGE1 to test host in Branch1 in VPN 10 by entering destination ip 10.3.10.10
11. Click Ping.
</td>
</tr>
</table>

	
	12. Deselect the current source interface. 13. Validate there is NO Connectivity from Branch2 in VPN 20 using destination ip 10.3.20.10
NOTE: The ping will fail due to centralized ACL blocking communication between the branches for PCI/IOT segment.	
	14. To De-activate policy select Configuration > Policies. 15. Click on the three dots (...) to the right of the MultiTopologyPlusACL policy. 16. Select Deactivate. 
	17. Click Deactivate. 18. The policy status will change from In Progress to Success, and the policy is successfully removed from the vsmarts.Full mesh connectivity has been restored.

Scenario 6. Application Aware Routing

With fast deployment model and flexible topologies, any type of circuit could be deployed, which provides the ability to direct different types of traffic over different types of links. Video could go over the internet, mission critical applications can go over MPLS. LTE could be circuit of last resort. This provides path diversity and high availability.

In thislab, some of the applications have already had SLAs defined and are pinned to the MPLS. Some applications have been pinned to the internet transport

The policy is applied to ALL sites, so the policy has impact on all the traffic received and sent by BR2-VEDGE1. More traffic is received than sent by the BR2-VEDGE1. Look at the traffic received by BR2-VEDGE1 on the mpls interface and the internet interface. You will observe the traffic received switch from the mpls interface to internet interface after the latency impairment on the MPLS transport.

Challenge

Dynamic path selection based on transport performance is complex to deploy and hard to update policies on demand

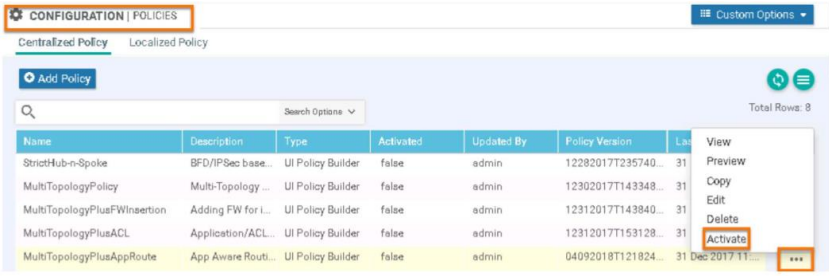
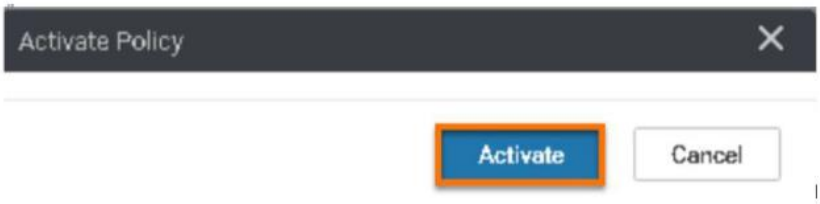
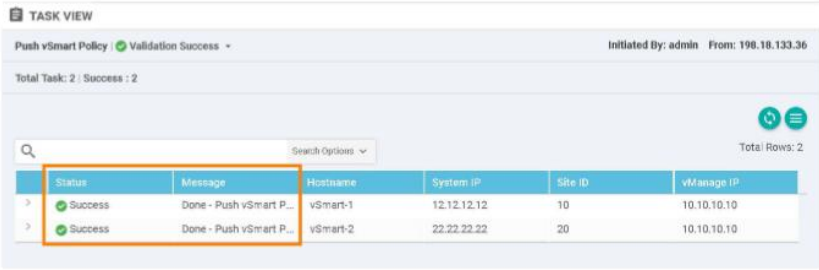
Benefits – Reduce Cost and Complexity

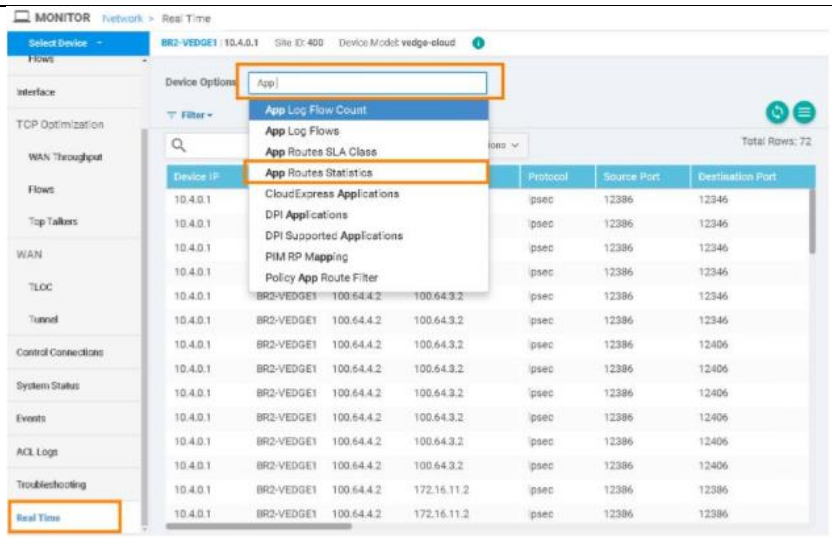
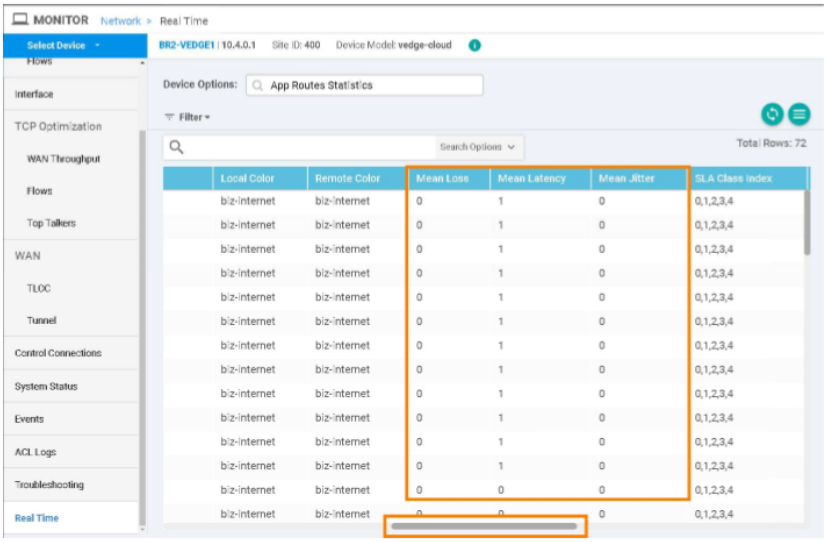
Simple activation of policy from central vManage. Results in simpler operations, reduced cost and reduction in time and effort.

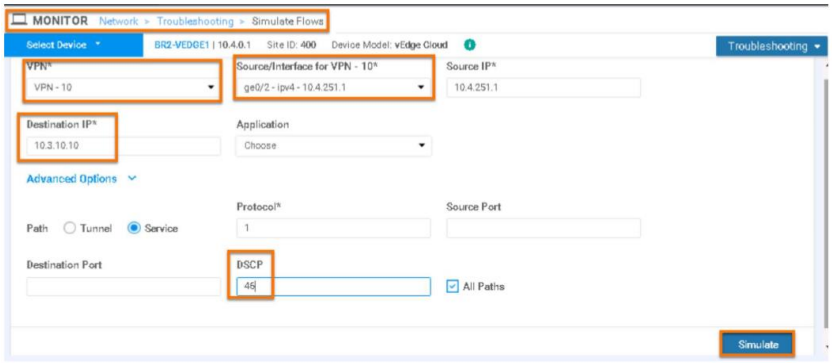
Objective

Define SLA based policies and re-route traffic as the transport network conditions change.

DIALOG	DEMONSTRATION STEPS
	1. From the menu, select Configuration > Policies . Select BR2-VEDGE1. 2. Click the three dots next to the MultiTopologyPlusAppRoute policy.

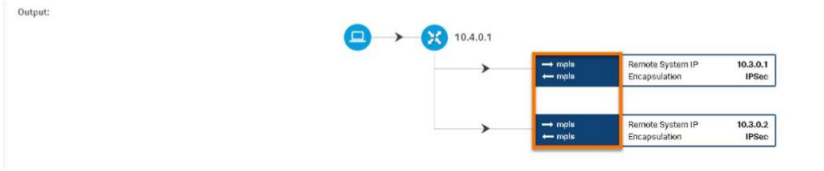
	3. Select Activate.  4. Click Activate on pop-up. 
	5. Wait until the policy is successfully pushed to each vsmart. 
NOTE: The device dashboard for BR2-VEDGE1 displays the current performance measurement on both the transports.	6. From the menu, select Monitor > Network. 7. Select BR2-VEDGE1. 8. Click Real Time. 9. Search for App Route Statistics using Device Option search. 10. Select App Route Statistics and Click Do Not Filter on the pop-up.

	
NOTE: These values are much low er than the SLA definitions defined for the app-route policies.	11. Scroll to the right to see the columns showing (Mean and Average) Latency, Loss and Jitter for each of the tunnels on MPLS and Internet. 
NOTE: Simulate Flow s provides a simulation on what IPSec tunnels will used for the defined flow based on policies and transport performance measurements.	12. Select Troubleshooting. 13. Click Simulate Flows. 14. Select VPN 10. 15. Select the source interface 16. Enter 10.3.10.10 as the destination IP address. 17. Click Advanced Options . 18. Enter the DSCP value of 46.
	19. Click Simulate.



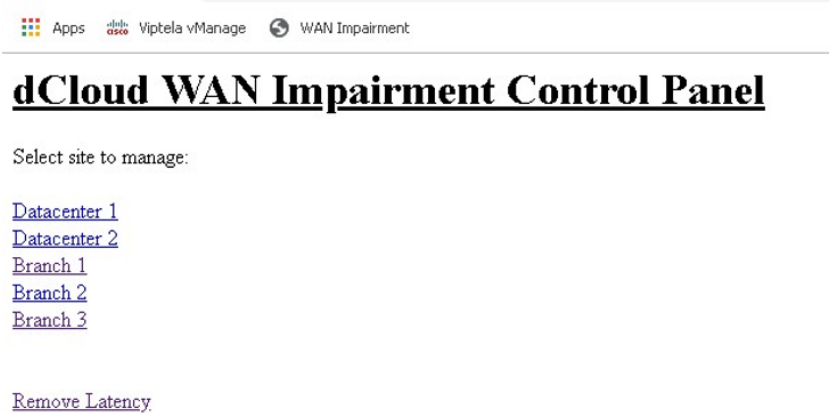
NOTE: This shows that the traffic class with DSCP of 46 will go over MPLS as it meets the SLA (latency <= 50msec) and is the preferred colour.

NOTE: Notice the path uses only mpls.



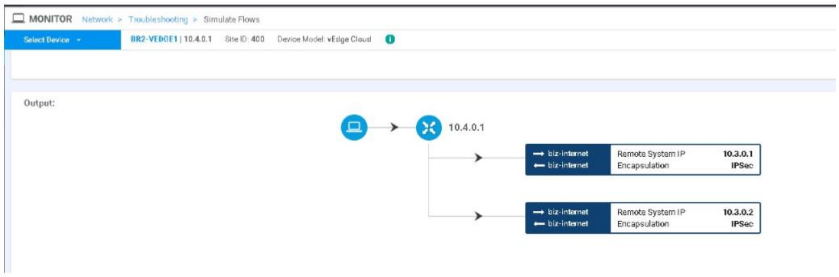
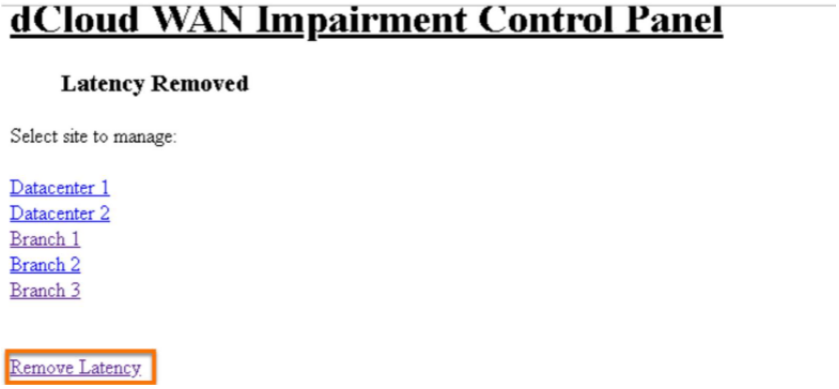
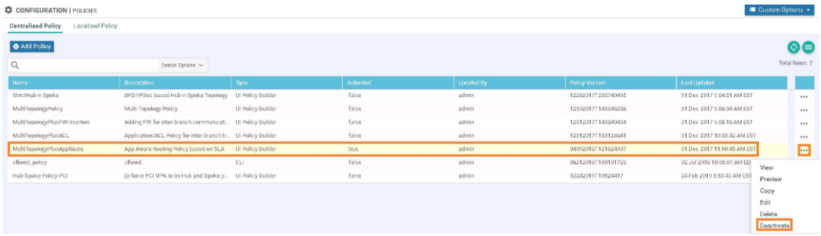
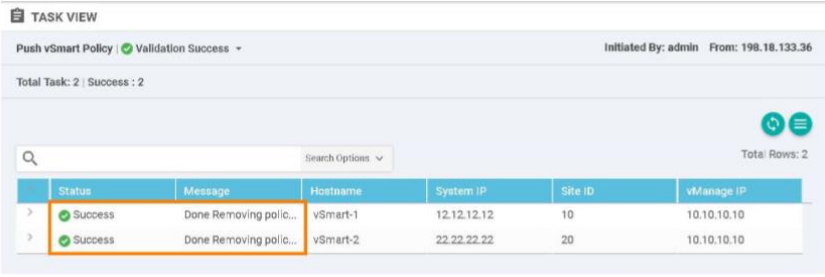
WAN Impairment

20. Open new tab in Chrome and click the WAN Impairment bookmark



21. Click Branch 1 and choose mpls transport and then click Submit.

22. Click back to the open Simulated Flow browser tab.

	23. When latency has been added, to show internet transport, wait 1 minute and then run the test again. 
	24. Return to the WAN Impairment Tool and click Remove Latency. 
	25. From the menu, select Configuration > Policies . 26. Click the three dots (...) to the right of the MultiTopologyPlusAppRoute. 27. Select Deactivate. 
	28. Click Deactivate. 29. The policy status will change from In Progress to Success, and the policy is successfully removed from the vSmarts. 

Scenario 7. SD-WAN Security Overview (Optional)

The remote offices all utilize a Guest Internet VPN which allows customers to browse the internet via Direct Internet Access. SD-WAN Security policy has been activated on this guest VPN to protect them. Cisco SD-WAN Security can provide protection against known and unknown malware threats with AMP and Threat Grid.

Challenge

Backhauled internet-bound traffic on a corporate firewall is a complex problem which requires more appliances.

Benefits – Reduce Cost and Complexity

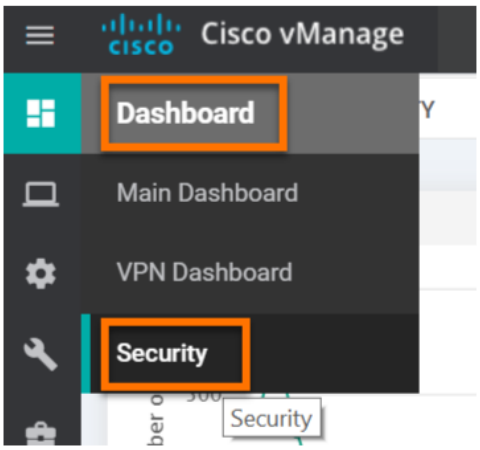
Activation of SD-WAN Security policy from central vManage results in simpler operations, reduced cost, and reduction in time and effort.
Insert a wide range of security offerings at remote locations without needing more appliances

Objective

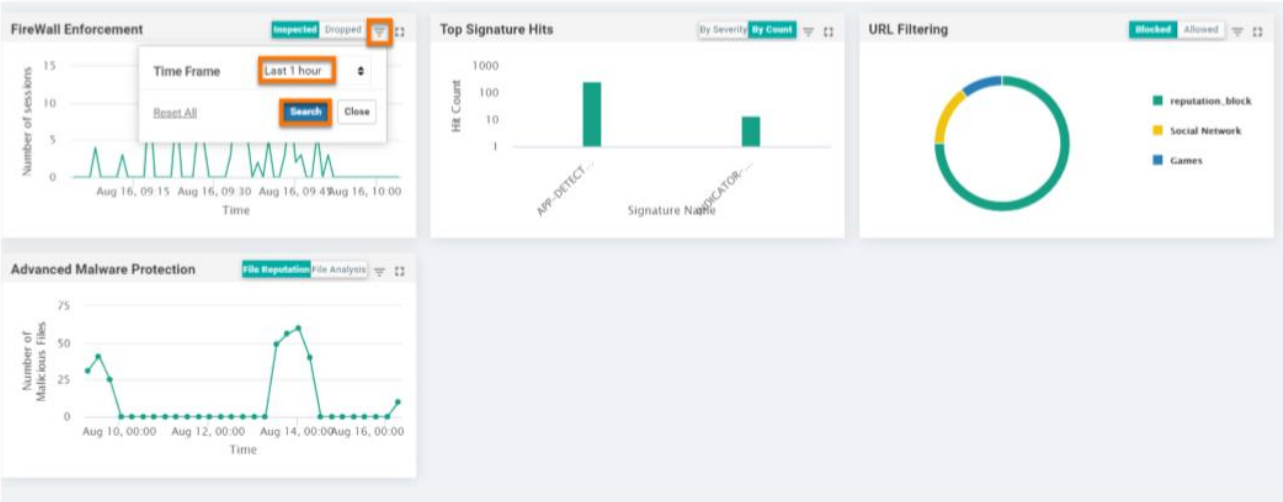
Leverage defense-in-depth security offerings in a combined platform so customers can decide what posture to adopt in distinct locations across the WAN saving on rack space.

Steps

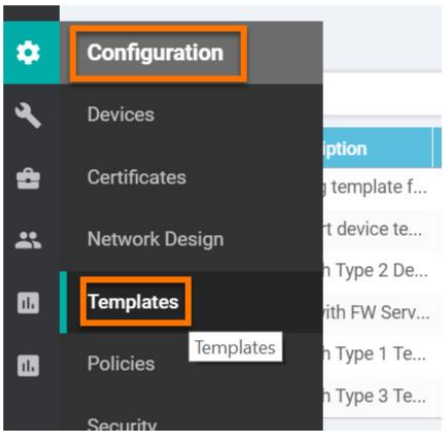
1. Click on the Dashboard button and then Security to view the SD-WAN Security dashboard.



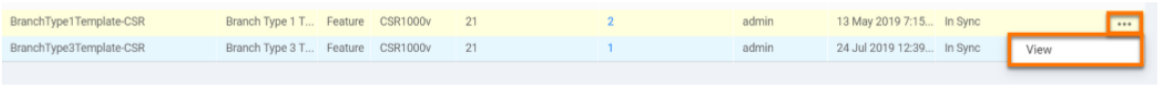
2. Click the small down arrow in the first widget and adjust time frame to 1 hour and click Search.



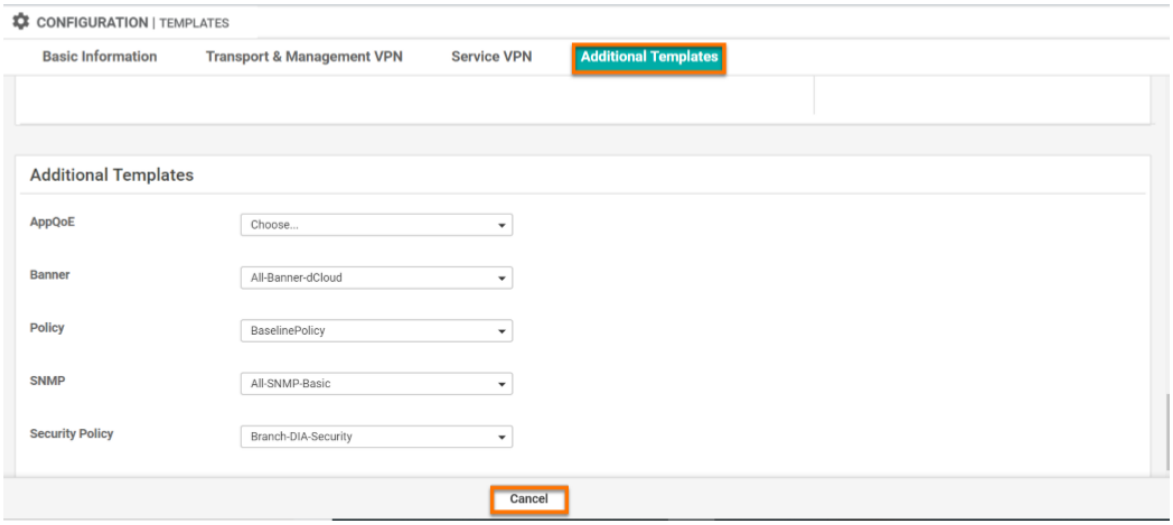
3. Click Configuration > Templates



4. To the right of BranchType1Template-CSR click the three dots (...) and then select View.



5. After the page loads, click Additional Templates which will go to the bottom, where Security Policy is listed.

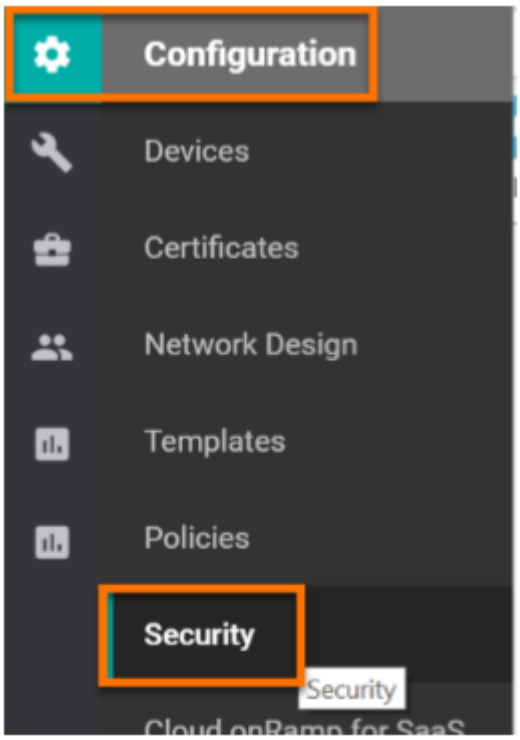


NOTE: Notice the Security Policy and the Container Profile. The Container runs the snort IPS engine.

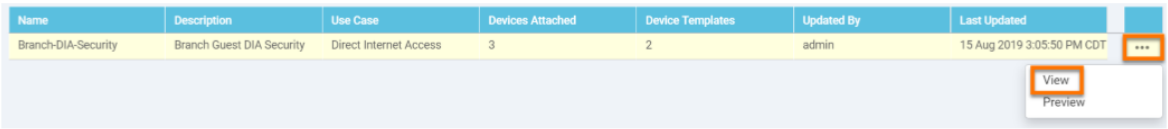
6. Click Cancel.

SD-WAN Security Policies

7. Click Configuration > Security.



8. To the right of Branch-DIA-Security policy, click the three dots (...) and View



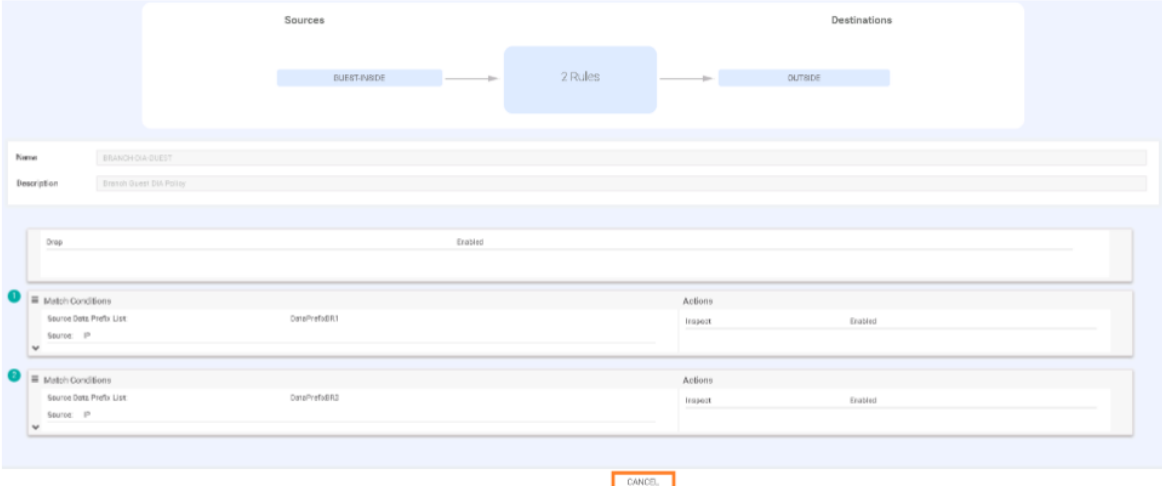
9. Click Firewall on the top.
10. To the right of BRANCH-DIA-GUEST click three dots (...) and View to see the firewall rules in effect.

NOTE: Due to a visual bug in vManage, the implicit deny rule (called Drop) shows above the other rules. It will NOT take effect before the configured rules.

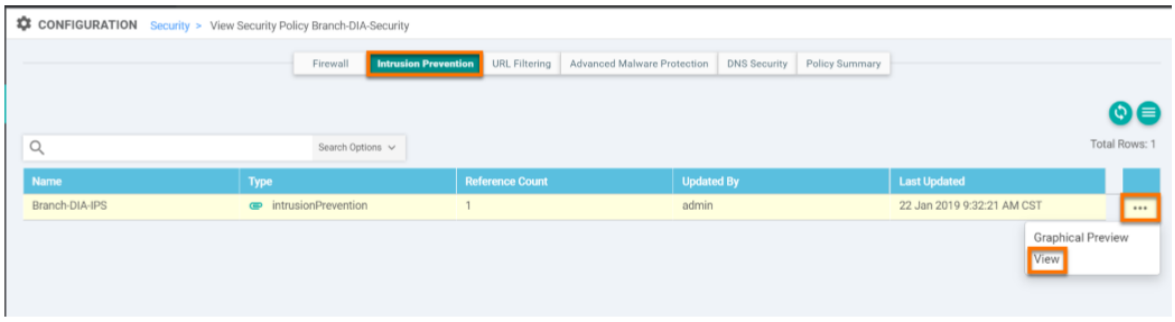
NOTE: Notice that this firewall is zone-based and is configured to inspect traffic from the Guest VPN to the Outside.

NOTE: The rules are allowing traffic from the branch subnets and the traffic is being inspected.

11. Click Cancel to go back to the SD-WAN Security Policy.



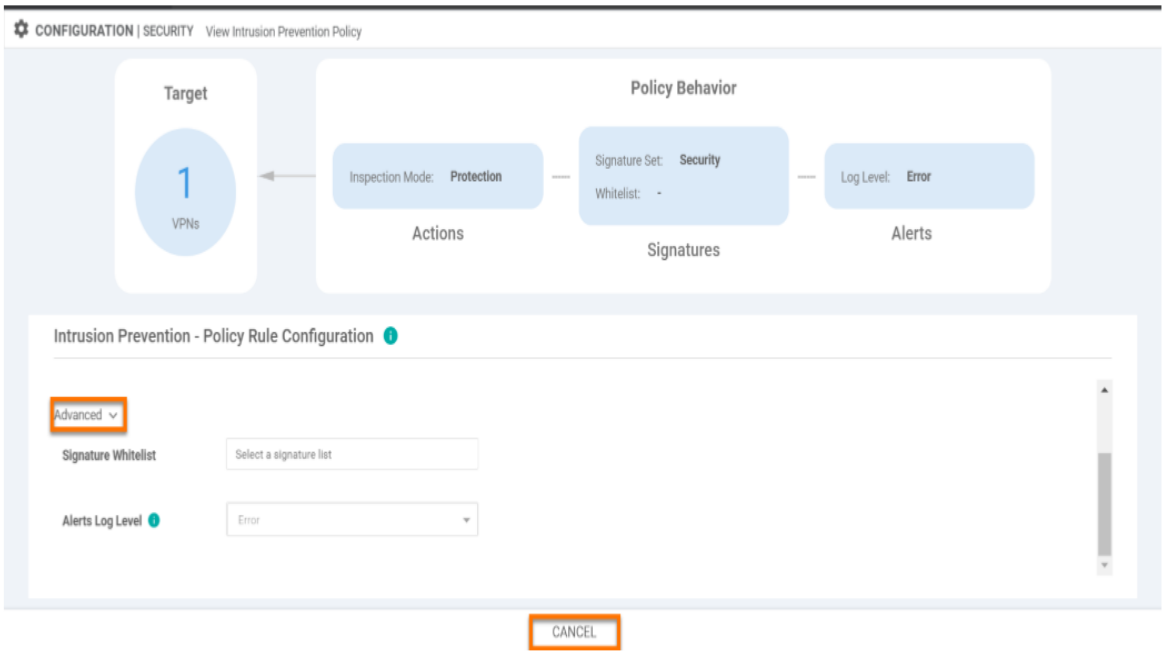
12. Click Intrusion Prevention to see how the IPS rules are set up.
13. Click on the three dots (...) to the right of the Branch-DIA-IPS policy and click View.



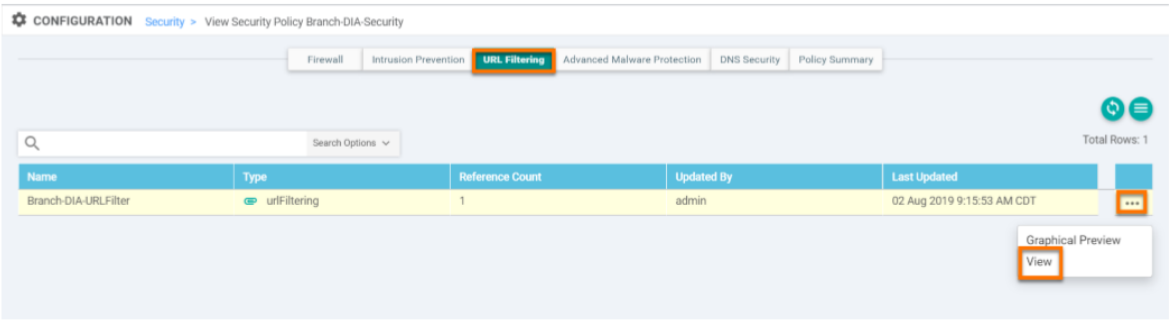
14. Click on Advanced.

NOTE: Notice that we can create a signature whitelist if certain applications are triggering the IPS but should be allowed (common with some corporate home-grown applications).

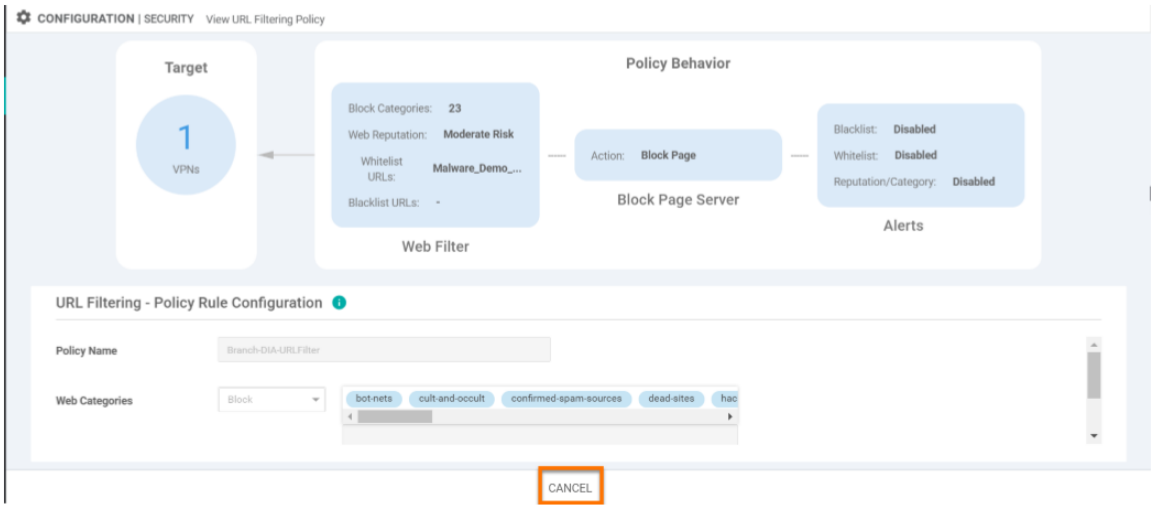
15. Click Cancel.



16. Click on URL Filtering at the top
17. Click the three dots (...) next to the URL Filtering policy and select View.

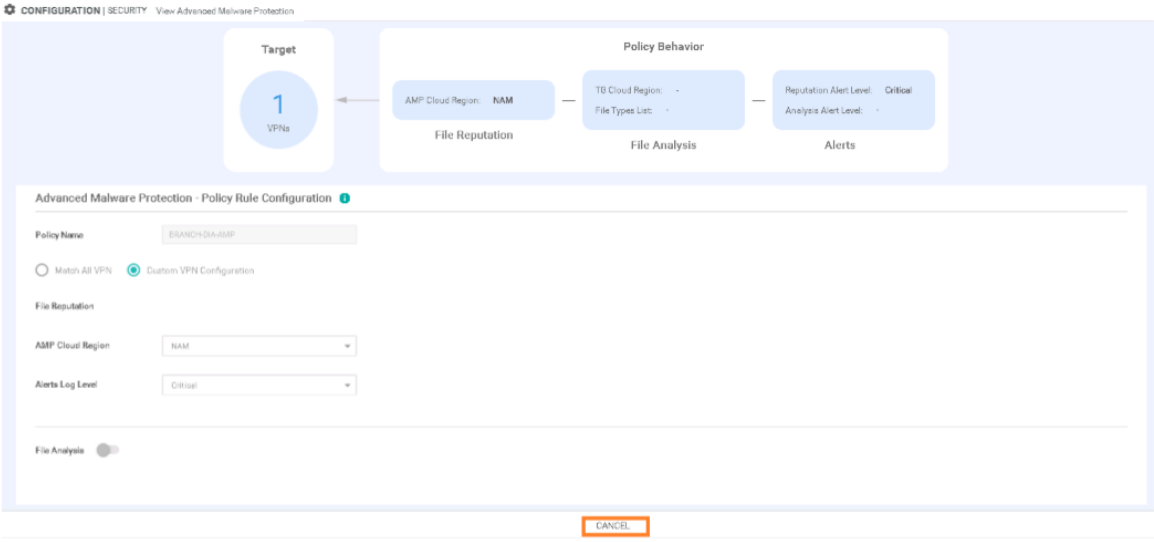


18. Click Cancel.



19. Click Advanced Malware Protection.
20. Click the three dots (...) next to the BRANCH-DIA-AMP and then select View.

21. Click Cancel.



Disclaimer

This training document is to familiarize with Cisco SD-WAN solution Although the lab design and configuration examples could be used as a reference, it's not a real design, thus not all recommended features are used, or enabled optimally. For the design related questions please contact your representative at Cisco, or a Cisco partner.