



# LTRSPG-2518

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

Sandeep Sharma – Product Manager Nilesh Khade – Software Engineer

ılıılı cısco

Copyright © 2019 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.





Learning ObjectiveKey Solution ComponentsTopologyGet StartedScenario 1: Zero Touch Site Bring UpScenario 2: BFD/IPSec based Strict Hub-n-SpokeScenario 3: Multi-Topology/Different Topologies Per VPNScenario 4: Service Insertion FW (Regional/DC Firewall.)Scenario 5: Application Firewalling using Centralized PoliciesScenario 6: Application Aware RoutingScenario 7: SD-WAN Security Overview (Optional)

2





# 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 preconfigured 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 fullmesh 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

3





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
- o Automated zero touch provisioning to accelerate time to market and reduce costs
- Centralized configuration management of ALL network devices via simple use of Templates
- o Business policy definition and activation from centralized vManage
- o 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.

- IOT/PCI Segment (VPN 20) Requires Hub-n-Spoke between the DC and the Branches.
- 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	х
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 providermanaged 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.	<ul> <li>1.Connect to Workstation 1 and launch the Chrome browser.</li> <li>2.Click the bookmark for Viptela vManage and click through the security warnings to proceed to the vManage service.</li> <li>3.Log in to vManage using username admin and password admin.</li> </ul>		
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.	Cisco SD-WAN    Cisco vManage       		
	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.		





	Configuration
	Cevices
	Certificates
	Network Design
	Templates
NOTE: We are selecting this device since it has not been provisioned.	6.Click on the three dots () in the right most column for BranchType2Template-vEdge. From the drop-down, select the option Attach Devices.
	O Citra ato Template •         Edit           Q.         Sarch Options >           Manual         Description:         Type         Description:         Description: <thdescription:< th="">         Description:</thdescription:<>
	<ul> <li>7.From the left pane labeled Available Devices, find the device with chassis-id/UUID of 52c7911f-c5b0-45df-b8263155809a2a1a.</li> <li>8.Move the selected device to the right pane labeled Selected Devices by clicking on the right arrow.</li> </ul>
	Attach date: feen the ist below: Attach
	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.





	Uposte Device remplate
	Variable List (Hover over each field for more information)
	Chassis Number
	52c7911f-c5b0-45df-b826-3155809a2a1a
	System IP
	Hostname
	IPv/ Aridrose(VPN40-IP-Aridrose)
	IPV4 Actress(VPNZO-Interface-IP)
	Profiv(VPN10 TRAFFIC DC11
	Update Cancel
	11. Click the Cancel button to go back to the previous page.
	12. Click on the upload icon (Up arrow) for uploading the
NOTE. The device values can be undated from the GIII interface if desired. In this demonstration, we will use a needefined rev	
HOTE. The device values can be opticed norm the dominientace, in desired, in this demonstration, we will use a predemined (sv	
file with device values.	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
	unloaded CSV file, click Next
	Chassis Number III Iystem III Hostname III Hostname
	S2c7911Fc5b0-45dF-b826-0155809a2a1a 10.4.0.1 BR2-VEDGE1 10.4.254.1/30
	Next Cancel
	18. Click the tab in the left column with BR2-VEDGE1 label to
	see the full configuration for validation
	10 Click Configure Devices
	T9. UICK CONIGULE DEVICES.





	CONFIGURATION   TEMPLATES     Verdgard action will be applied to 1 device(s)     dealing to 1 device(s)
	Device Terrybin Teal DranchType?TemplatevE
	Device list (Total: 1 devices)       Fightla-systemisystem       fightla-systemisystem         Fightla-systemisystem       fightla-systemisystem       fightla-systemisystem         Statistics       setter-and       weige-lowid         Not-wave       SEL-VIDE11       ge-lowid         ge-lowide       setter-isitive       SEL-VIDE11         ge-regelistion-wave       SELSE by1 - 19904*       or track-transport         to track-transport       to track-transport       to track-transport         to track-transport       totack-transport       totack         vetor
	Configure Devices Holtack Timer
	20. Wait for few seconds until the device status changes from
	Status     Done - Scheduled
	21. Click on the vManage Dashboard icon. The dashboard icon shows that Only 4 vedges are operational.
	II DASHBOARD   MAIN DASHBOARD
	vSmart-2
NOTE: Accept any MTPutty security alerts to add the key to the Putty cache.	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



CISCO



	Jownloads       Josephie         Cisco       Remote         Desktop       Desktop         Josephie       Josephie         SD-WAN Demo       Josephie         Command       Prompt         Josephie       Josephie         Josephie       Josephie         Josephie       Josephie         Josephie       Josephie         Josephie       Josephie
	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.
	MONITOR Network > System Status  Sitest Davise   Bit2-VEDGE1   10.4.0.1 Site D: 400 Device Model vedge-sloud  Application
	EPR EPR
	Interface ICO Designation ICO
	WAN Throughput VSB N/A
	Flows CPU & Memory Top Takers
	WAN
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).	26. From the Monitor Device menu, Click on Control Connections. Validate that control sessions are established to





	vSmart and vManage.		
	Seart Device -      BR2 VEIGE1) ID.4.1.1 Bits D-400 Dense Nodel Velge Devid     Top Takes     vSmart Connect Connect and Resected -41 Actual -4.3		
	WAN TLDE Torred		
	Security Monitoring Prienal Intrusion Resention Vorunt 22 Vorunt 2		
	UR Fiteing Advanced Mainex Pretextion Undveds INIS Re Q, Saurch Options v		
	Cardial Connections         V         Peer Type         Peer Typeer Type		
	<ul> <li>27. To validate IP reachability within Branch2 VPN10,ping the VPN10 test host at 10.4.10.10.</li> <li>28. Open the mPutty application.</li> <li>29. Double click on BR2-VEDGE1.</li> <li>30. On the command line, type ping vpn10 10.4.10.10 count 5 to test the connectivity to ta host at Branch 2.</li> </ul>		
<b>NOTE:</b> 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.	<ul><li>31. Return to Monitor &gt; Network and select BR2-VEDGE1</li><li>from the list.</li><li>32. Click on DPI.</li></ul>		



CISCO



MONITOR Network	Applications - DPI	
Select Device -	BR2-VEDGE1   10.4.0.1 Site ID: 400 De	wice Model: vEdge Cloud 🛛 🕕
Applications		polication Usage FEC Recovery Rate
Interface	≂ Filter •	
TCP Optimization	190.73 MB Legend	≏ <b>1h</b> 3h 6h
WAN Throughput	audio-video	
Flows	95.37 MB mail	
Too Talkara	network-ser	vice
top raikers	o standard	
WAN	thin-chent	
TLOC	6 Rows Selected	00
Tunnel	Q	5
Applications TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Turnel Security Monitoring	Cost 1 16.4.6.1 Site 10: 460 Device Model: vEdge Gloud  T Options  I Options	Custom V Custom
Hover your mous details.	se over devices on the r	map to see the device





# Scenario 2. Hub and Spoke Topology

Enterprises may not need a full mesh topology and would like to have a pure Hub-n-SpokelPSec/BFD topology. This will 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 Hubn-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		
	<ol> <li>Go to vManage. Click on the Monitor &gt; Network.</li> <li>Select BR2-VEDGE1.</li> <li>Monitor &gt; <a href="https://www.monitor.inetwork">Monitor</a></li> </ol>		
	Geography WAN - Edge Coloc Network Select VPN Group		
	Alarms Events		
	Audit Log ACL Log BR1-CEDGE1		
	Configuration > BR1-CEDGE2		
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.	<ol> <li>Select Tunnel from the left column.</li> <li>The next screen shows IPSec tunnels are established to the DCs and the remote Branch-1 (Full mesh).</li> </ol>		
	MONITOR Network > WAN - Tunnel         Select Device *       BR2-VEDGE1   10.4.0.1 Site ID: 400 Device Model: vEdge Gloud *         Applications       ID Obset Options *       F Real Time 1h 3h 6h 12h 24h 7days Custom *         Interface       ************************************		
	Flows     6 Rows Selected       Top Talkers     Q       WAN     ↓       TLOC     ✓       Turnel Endpoints     Application Usage Link		
	Turnet          ✓ mpls            Security Monitoring              ØR2-VEDGE1:mple-DC1-VEDGE1:mpla            BR2-VEDGE1:mple-DC1-VEDGE2:mpls               Application Usage		
	<ol> <li>Select Troubleshooting from the left column.</li> <li>Select Trace Route under Connectivity.</li> </ol>		





	Intrusion Prevention	Connectivity
	URL Filtering	
	Advanced Malware	
	Protection	
	Umbrella DNS Re- direct	
	Cantral Cannectians	
	System Status	
	Events	Device Bringup
	ACL Logs	Control Connections(Live View)
	Troubleshooting	Ping
	Real Time	Trace Route
	<ul> <li>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.</li> <li>8. Click Start.</li> </ul>	
	NOTE: The output on your so	reen may not be exactly like the screen shot shown in the guide.
	<b>Rutput</b> Tracewate-in 16-in 1-a 16-4268.8 103.98.99 in VPN 16	x p402-p4-1142011
	tracemente ha 100.10.10.10.10.10.10.10, 12 hope mar, 40 hyte pecke 1 * * *	1894
	2.10.2.10.10 (10.2.10.10) 1.77Fm 1.141Fm 1.141Fm	ηλ
		▲ <sup>inn</sup>
		01D1
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	<ul> <li>9. Deselect the current source interface.</li> <li>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.</li> <li>11. Click Stort</li> </ul>	



CISCO



		Troubleshooting > Traceroute	
	Select Device *	BR2-VEDGE1   10.4.0.1 Site ID: 400 Device I	Vodel: vEdge Cloud 0 Troubleshooting •
	Destination IP*	VPN	Source/Interface for VPN - 20
	10.3.20.10	VPN-2V	gev/a - rpre - rp.e.222.1
	Advanced Options >		
			Start
	NOTE: The output on you	r screen may not be exactly like the scre	en shot shown in the guide.
	Duju.e	gals2-(pd - 184.222.1	
	Tracements -m 15 -m 1 - n 10 4 223, 1 10 0, 20 10 in VPA 20 toconvolutio 10 3 20 10 (10 0 20 10), 16 heps max, 40 byt 1 + + +	Litera	
	2 10 3 20 10 (10 3 20 10) 1 540 no 3 562 no 3 598 no		240m
			10.7.21.33
	Configure Po		- financiana - Daliaina
	12. From	the menu, select Co	) for StrictHub p Spoke
	17 Selec	on the three dots ( t Δctivate	
		CONFIGURATION   POLICIES	🖷 Casteri Optori •
	Construction C	Centralized Policy Localized Policy	
	Devices	O Add Policy	00
	Certificates	0	Total Rows: 8
	Network Design		Manual Decision Processing Land Decision
	Templates	StrictHub-n-8. BFD/IPGec base. UI Policy Builder	false admin 12282017T235740_31 Dec 2017 9.5_
		MultiTopology Multi-Topology UI Policy Builder	felse admin 12302017T143348 31. View
	Poicies	MultiTopology Adding FW for i UI Policy Builder	false admin 123120177143840
	Security	MultiTopology Application/AC UI Policy Builder	falpe admin 12312017715312831 Copy
	Cloud onRamp for	Multi lopology App Avise Rout U Policy Builder	Telse admin 040920181121824 21 Delete
	0000	chowd_polay clowd CU	false admin 06212018T19013102
	15. Click	on Activate button o	on the pop-up.
	Activate Polic	v	×
	Activate Folic	,	
			Activate Cancel
			·
NOTE: The policy is applied to the vSmart	16. Wait u	until the policy active	ation Status changes to
controllers. vSmart will push the policies to the	Succe	355.	
appropriate vEdge routers.			





	C TASK VEW
	Paule vEnuel Policy 🕲 validation Surrans - Helland By advise From 146.18.332.36
	Total Task: 2 (Taxonas ) 2
	00
	Q. Searchipter - Total Royal 2
	Status Printige History Street P Street WatersgelP
	2 Sumer Date Fash (Smart.) (2mart.) 12.12.12.13 10 16.10.16.10
	✓ Otenese Doe-Publishet, sthatt 2222222 22 10.10.10.10
	17 Validata Strict Hub n. Snaka tanalagu bu salasting
	Manitana Natarak
	Monitor > Network .
	18. Select BR2-VEDGE1
	Monitor
	Geography WAN - Edge Coloc
	VPNOROUP
	Network
	Select VPN Group
	Alarms
	Evente
	Events
	Device Group All
	Audit Log
	(Induced)
	Hostname
	ACL Log
	BR1-CEDGE1
	W DAT OLDOLT
	Configuration > BR1-CEDGE2
	BR2-VEDGE1
NOTE: Point out that only tunnels to the DC	19. Select Tunnel from the left column.
vEdges are in an energianal LD state	
vEdges are in an operational UP state.	





	Annel         Annel <th< th=""></th<>
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. MONITOR Network > Troubleshooting > Treceroute Select Device Troubleshooting > Treceroute Select Device Troubleshooting > Treceroute Troubleshooting (VPN - 20) (Select Device Model vEdge Cloud () () () () () () () () () () () () ()
NOTE: The output on your screen may not be exactly like the screen shot shown in the guide.	Stad           Torente et Kin 1 + 134 201 139 203 30 # 94 23           Stadie           Torente et Kin 1 + 134 201 139 203 30 # 94 23           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 201 139 40 an (4 an 120 m)           Torente et Kin 1 + 134 20 m)           Torente
	<ul> <li>23. To de-activate the policy, select Configuration &gt; Policies.</li> <li>24. Highlight the StrictHub-n-Spoke policy and click the three dots () to the right of the policy name.</li> </ul>

```
ılıılı
cısco
```





Controlland Policy Localevel Policy	a.						
O ALL Falley						(	90
Q	tentitries v					Teta	WHIT
16.04	Designe	101	4400	Lipited by	NayTecks	tartipolisi	
Stressub-r-Spala	DFD-075ac based itable-Opeias Topolog	Ul Policy Builder	tu	admin	125120171232740435	11 Dis: 2017 9:54 51 AM CST	
WellawiegPolcy	Md-Toping-Policy	tê Paloy kulder	trim.	admin	121021171100340204	H DAY JOHT R DE DA JAM EST	
Wethpring/Put/Minuston	Adding Pitcher into Branch sommunicati	U NicyBulde	faile	adren	12/12/17/14/54/54/54	11.0 × 2017 9.00 % MM ES Preview	
NiferingPosts	Application IKC, Policy for Handsarch H	. U Nicybalde	1414	admin	121120171101120541	11 Day 2017 10:15 4LAM 21 Copy	
W/SpringPauliplacts	App Anton Tauting Policy based on SLA	Ui Policy Bulder	508	admin	8404284071231234307	11 Dec 2017 11 99-46 AM EL 681	
deal pairs	clout	£L	5/66	admin	842420407430424724	IS IN 2018 10 0517 AN ST	
Hub Tpole Palay PCI	Enlace PD VPN to be Hub and typice p	U Nicy Builder	faite	admin	021420497 10624417	SAFIO SHI'S BACKLAN (ST	_
25.C 26.T S vi	Click Dead The policy Success, Smart-1	ctivate v status and the and vS ored	s will ch e policy Smart-2	ange froi r is succe 2. Full me	n In Prog ssfully re sh conne	ress to moved fror ectivity has	n
25. C 26. T S v! b	Click Dead the policy Success, Smart-1 een rest	ctivate status and the and vS ored.	s will ch e policy Smart-2	ange froi is succe 2. Full me	n In Prog ssfully re sh conne	press to moved from ectivity has	n
25. C 26. T S V b	Click Dead the policy success, Smart-1 een rest	ctivate status and the and vS ored.	e policy Smart-2	ange froi is succe 2. Full me	n In Prog ssfully re sh conne	press to moved from ectivity has	n
25. C 26. T S V b	Click Dead the policy success, Smart-1 een rest	ctivate status and the and vS pred.	s will ch e policy Smart-2	ange froi is succe 2. Full me	m In Prog ssfully re sh conne	press to moved from ectivity has	n
25. C 26. T S V b	Click Dead the policy success, Smart-1 een rest	ctivate status and the and vS ored.	s will ch e policy Smart-2	ange froi is succe 2. Full me	n In Prog ssfully re sh conne	gress to moved from ectivity has	n »
25. C 26. T S V! b	Click Dead The policy Success, Smart-1 een rest	ctivate status and the and vS ored.	s will ch e policy Smart-2	ange froi is succe 2. Full me	n In Prog ssfully re sh conne	gress to moved from ectivity has Brains Press 192, 12, 12 Brains Press 192, 12, 12 Brains Press 192, 12, 12 Brains Press 192, 12, 12 Brains Press 192, 12 Brains 194, 12 Brains 1	n *
25. C 26. T S V b	Click Dear The policy Success, Smart-1 een rest	ctivate status and the and vS ored.	s will ch e policy Smart-2	ange froi is succe 2. Full me	m In Prog ssfully re sh conne	gress to moved from ectivity has Brains Pres 18.11.12 Brains	n *
25. C 26. T S V b Track verse Parts description	Click Dear The policy Success, Smart-1 een rest	ctivate status and the and vS ored.	s will ch e policy Smart-2 Smart-2	ange from r is succe 2. Full me	m In Prog ssfully re sh conne	press to moved from ectivity has brains here 192.12.12 brains bra	n 22





# 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



CISCO



DIALOG	DEMONSTRATION STEPS			
Result shows direct path between Branch1 and Branch2 for VPN 10.	<ol> <li>Go to vManage. Click on the Monitor &gt; Network.</li> <li>Select BR2-VEDGE1.</li> <li>Select Troubleshooting from the left column.</li> <li>Select Trace Route.</li> <li>Enter 10.3.10.10 as the destination IP.</li> <li>Select VPN 10 from drop down menu.</li> <li>Click on Start button.</li> </ol>			
Result shows direct connectivity between Branch1 and Branch2 for VPN20	8. Do the same for VPN20 using destination IP of 10.3 20.10			
	<ul> <li>9. From the menu, select Configuration &gt; Policies .</li> <li>10. Click on the three dots() to the right of MultiTopologyPolicy.</li> <li>Configuration   Policies</li> <li>Configuration   Policies</li></ul>			
	12. When the policy has successfully been pushed to the VSmarts, the activation status changes to Success.			
	Ed TADA VIENT Pueb Vienat Pulky   © Valdation Gaussian - Initiated By: edmin From: 198.18.133.36 Total Tade: 2   Gaussian : 2			
	Col         Exacts Options         Total Rows: 2           1         Statue         Monogor         Hosting         Statue         Statue         Advance IP           2         Statue         Dane- Puph VStratt         VStrath-1         12:12:12:12         N0         N0:10:30           3         Statzess         Dane- Puph VStratt         VStrath-1         12:12:22:22         20         10:10:30			
Validate Full Mesh for VPN 10 and Hub-n- Spoke for VPN 20	13. From the menu, select Monitor > Network. 14. Click BR2-VEDGE1.			

Copyright © 2019 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9–11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



CISCO











NOTE: If the output yields <b>n</b> /a results, click <b>Start</b> again or redo the entire trace route steps above					
NOTE. The output on your screen may not be exactly like the screen shat shown in the quide	0.4pd				
NOTE. The oblight on your screen may not be exactly like the screen shot shown in the golde.	121200001 (1) 121 121 121 121 121 121 121 121 121 1				
	20110104(011010),4770 m: 4700 ms <sup>4</sup> Nik				
	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 Stort				
	MONITOR Network > Troubleshooting > Troperoute				
	Select Device				
	Destination IPs VPN Source/Interface for VPN - 20				
	10.3.20.10 VPN - 20 • ge0/3 - ipv4 - 10.4.252.1 •				
	Advanced Options >				
	Start				
NOTE: If the output yields n/a results, click Start again or redo the entire trace route steps above.	Butjuit politi (p.4. 1942)[2]				
NOTE: The output on your screen may not be exactly like the screen shot shown in the guide.	Toposol m or i i i su cali i no cali i mono do Toposol m la cali i i su cali i mono do Toposol m la cali i i su cali i mono do				
	10122010(0112015)140*m1140*m1170*m 2*** 01120100 Nik				
	2 10 20 10 (00 20 10) 1 MD m + ( ME m +				
	21. Result display the connectivity between Branch1 and				
	Branch2 through the DC				
	Brahonz through the bo.				
	22. To de-activate the policy, select Configuration >				
	Policies.				
	22.10. Highlight the MultiTenelogyDeligy policy and then				
	click the three dots () to the right of the policy name.				
	24. Select Deactivate.				
	C certabulations i muses				
	Q. Sections -				
	Instrum         Instrum <t< th=""></t<>				
	Instrumentation         Address of the first fraction of the sector				
	Valleying/Nu/sylva: Ageno/Nursylva/sale/La ir/Ay/bria Valleying/Nu/sylva: Ageno/Nursylva/sale/La ir/Ay/bria Valleying/Nu/sylva: Becker/stagen/ Ir/ay/bria Valleying/Nu/sylva: Becker/stagen/ Ir/ay/bria Valleying/Nu/sylva: Becker/stagen/ Ir/ay/bria				
	restate-Map PD DAtes 10 PM ediciti-program, 2 Map 2018 The area \$2,000,0110,0407 pm parts 4,000 \$200 (Map 2010)				
	25. Click Deactivate.				
	26. The policy status will change from In Progress to				
	Success, and the policy is successfully removed.				





<b>В</b> ТА	SK VIEW					
Push	rismart Policy   🔿 Validati	on Success -			Initiated By: a	admin From: 198.18.133.36
Total 1	lask: 2   Success : 2					
						00
Q,			Search Options 🗸			Total Rows. 2
1.0	Status	Message	Hostname	System IP	584 10	vManage IP
>	O Success	Done Removing polic	vSmert-1	12.12.12.12	10	10.10.10.10
>	O Success	Done Removing polic	v9mert-2	22.22.22.22	20	10.10.10.10

# 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.



CISCO



DIALOG	DEMONSTRATION STEPS
Result shows direct path between Branch1 and Branch2 for VPN 10.	<ol> <li>From the menu, select Configuration &gt; Policies.</li> <li>Click the three dots() to the right of the policy named</li> </ol>
	MultiTopologyPlusFWInsertion.
	3. Select Activate.
	Monitor > Confidential Policy Located Policy
	Destrees Confidentes Confiden
	Manuel Design         Structure of the spectrum of the spectru
	Templates MultiTepolog/Parky MultiTepolog/P. IJ Pilicy Builder faile admin 12200071110354236 H Achrana MultiTepolog/Pun/Nitraeton Adding PM for III. IJ Pilicy Builder faile admin 1220207111036404 H pilic 20171555.
	Polides         Multifoping/PicsAC,         Application/ACL,         U Policy Builder         fails         admin         Tablication111111111111111111111111111111111111
	4. Click Activate on the pop up.
	Activate Policy ×
	Activate Cancel
	5. Wait until the policy is successfully pushed to each
	vSmart.
	B TASK VIEW
	Pault classed Parky 🌀 Validation Second - Initial Systems - Initia Systems - Initia
	Tetal Taol: 2 Success : 2
	00
	Q Total Room 2
	Color: Neurope Remittere Deriver (Color)     Sector: (Color)
	Dames         Dame-Push vitrant_         vitrant2         22.22.22.23         20         12.10.10.10
	<ol><li>From the menu, select Monitor &gt; Network.</li></ol>
	7. Click on BR2-VEDGE1.

Copyright © 2019 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9–11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.





	MONITOR Network - System Subus
	Selver Dovice
	Reboot 20 Crash 0
	Nues Module NUA Power Supply NUA
	TCP Optimization
	Res Coo Hea
	Top Takes CPU & Memory In 2h (h 12h 2m 2days Duritor -
	TAX O
	Tuoc 18.13% 5 5 5 5
	Tazani CPU n Lind zowage nor 2k htt
	<ol> <li>From the left column, select Troubleshooting.</li> <li>Select Trace Route.</li> <li>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.</li> <li>Click Start.</li> </ol>
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.	MONITOR         Network: > Troubleshooting > Traceroute           Getext Device *         BR2-VEDGE1 (10.4.6.1) Site ID: 400         Device Model: vEdge Cloud         Troubleshooting *           Destination IP*         VPN         Source/Interface for VPN - 10         Image: Cloud
	10.3.10.10 VPN - 10 • ge0/2 - Jpr4 - 10.4.251.1 •
NOTE: You can see that traffic between branches is being rerouted through the data center where a firewall is inspecting traffic	Advanced Options >
	Butk         Image: Constrained with State St
	<ul> <li>12. Deselect the current source.</li> <li>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.</li> <li>14. Click Start</li> </ul>
	14. UIUK Stalt.





	MONITOR Network > Trouble	shooting > Traperoute	
	Select Device * BR2-VED	GE1   10.4.0.1 Site ID: 400 Device Mox	del: vEdge Cloud 0 Trouble shooting
	10.3.20.10	VPN - 20	Source/Interface for VPN - 20 ▼ ge0/3 - ip/4 - 10.4.252.1 ▼
	Advanced Options >		
			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.	0.46A	gth9-1pd-1942021	
	Tracemute -n 15 -e 1 -e 10 4 252 1 10 3 20 50 m VPN 20 tecessete to 10 3 20 10 (10 3 20 10), 16 Feps max, 40 byte packets	Ukr o Din o	
	1 10 1 20 120 (20 1 20 126 1 04 ms 1 512 ms 2 042 ms	1120120 NA	
	2*** 0 40.0.20 40 (00.0.20 40) 40.771 ms 40.972.ms *		
			(A) 1574
			10 1 20 10
	15. From the	menu, select Mo	onitor > Policies .
	16. Click the	three dots () to	o the right of the
	MultiTopo	ologyPlusFWInse	rtion policy.
	17. Select De	eactivate.	🖝 Colonia Indexes -
	Complete Policy Constrait Policy		00
	Q. Institution -	Pas Advert	Treat Rev. 7
	Institution of the second seco	a Pelig Setter Mitos antas a Pelig Setter Tas antas di Pelig Setter Tas	
	matripolog/Acalgobics approximation/Acalgobics     development     development     monocomment     monoco	eritua la Penaytecho Edua DU Edua pelago 2 Penaytecho Nales	Materia         Material         How Destruction         How Destruction
	10 TH "		
	18. The polic	y status will char	nge from In Progress to
	Success,	and the policy is	s successivily removed from
	TASK VIEW	113.	
	Push vSmart Policy 🖉 Validation Succe	* 22	Initiated By: admin From: 198.18.133.36
	Total Task: 2 : Saccess : 2		
			00
	C. Data	BackOption -	System I/2 Site (D - Advance I/2
	> Success Done #	temoving polic VSmart-1	12.12.12.12 10 10.10.10
	Success Done R	terroving policvSmart-2	22.22.22.22 29 10.10.10.10





# 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

111111

**CISCO** 

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

DIALOG		DEMONSTRATION ST	TEPS		
	<ol> <li>From the menu, select Monitor &gt; Network.</li> <li>Select BR2-VEDGE1.</li> <li>Click Troubleshooting.</li> <li>Click Ping.</li> </ol>				
	Select Device -	Troubleshooting     BR2-VEDGE1   10.4.0.1 Site ID: 400 Device Model: vedge-cloud			
	TCP Optimization WAN Throughput Flows	Connectivity	Traffic		
	Top Talkers WAN	*	2¢		
	TLOC Tunnel Control Connections	Desire Bringer	Tunnel Health		
	System Status Events	Control Connections(Live View)	App Route Visualization		
	ACL Logs Troubleshooting Real Time	Ping Trace Route	Simulate Flows		

Copyright © 2019 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9–11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.





<ul> <li>5. Validate Connectivity from BR2-VEDGE1 to test host in Branch1 in VPN 10 by entering destination ip 10.3.10.10</li> <li>6. Click Ping.</li> </ul>
Burnary     Output:       Pasin Summini     1       Pasin Summini S
<ul> <li>7. Deselect the current source interface.</li> <li>8. Validate Connectivity from BR2-VEDGE1 to test host in Branch1 in VPN 20 by entering destination ip 10.3.20.10</li> <li>MONITOR Network &gt; Troubleshooting &gt; Ping</li> <li>Rest-VEDGE1 18.4.0.1 Set U: 400 Device Model weige elocal</li> <li>Troubleshooting &gt; Troubleshooting &gt; Ping</li> <li>Troubleshooting &gt; Ping</li> <li>Troubleshooting &gt; Ping</li> </ul>
10.2.20:10     VPN-20     gx0/2-lyv4-18.4.20.1       Probes     ICMP     TCP       Source Port     Destination Port     Type Of Service       Time To Live     Dorff Fragment       Advanced Options >
Summary         Output:           Packets Transmitted         5           Packets Transmitted         5           Packets Received         4           Packet Statuling Nping 0.6.47 ( http://mmap.org/nping) at 2019-01-23 16:11 UTC           SENT (0.122x) ICMP [10.4.20,1 > 10.3.20,10 Echo request (type=&/code=0) id=28173 seq=1] IP [tti=64 id=56660 pien=28]           SENT (1.0124x) ICMP [10.3.20,10 > 10.4.20,1 Echo request (type=@/code=0) id=28173 seq=1] IP [tti=127 id=22101 pien=28]           RCVD (1.0147s) ICMP [10.3.20,10 > 10.4.20,1 Echo request (type=@/code=0) id=28173 seq=1] IP [tti=127 id=22101 pien=28]
<ol> <li>From the menu, select Configuration &gt; Policies.</li> <li>Click on the three dots () to the right of the MultiTopologyPlusACL policy.</li> <li>Select Activate.</li> </ol>



CISCO



CONFIDURATION (Focuses Controllars Palay Losing Palay	Custow Options •
© AM Folicy	O O
Name         Description         Type         Actualize         Opposition           Non-Works         Benchelm Speke         Units (Min Speke         Units (Min Spekee         Min	East Updated B1 Dec 2017 9:54 61 AM EST ***
Multipologinkurgi Multipologing Multipologin	31 Dec 2017 9.56.04.6M EST
Mathipsophis, a         Application, and an and an and an and an	81 Dec 2017 10:0-42 AM INT  81 Dec 2017 11:00-45 AM IS 92 Jul 2016 10:06:07 AM ID Propriew
Hub-bake-Nicy-PCI Extra PCI VPN to le Hub en Egiste p. U Policy Buller Extra admin 822420811926487	24 Feb 2019 6 50:43 AM EST Copy Edit
	Activate
4. Click Activate on the Pop up.	
Activate Policy	×
Activate Folicy	$\sim$
	0 1
Activate	Cancel
	l,
5. Wait until policy is successfully to pushed	to each
vsmart.	
TASK VIEW	
Push vSmart Policy   🖉 Validation Success 👻 Initiated	By: admin From: 198.18.133.36
Total Task: 2   Success : 2	
	08
Q Search Options 🛩	Total Rows: 2
Status         Message         Hostname         System IP         Site ID	vManage IP
Osuccess     Done - Push vSmart P     vSmart-1     12.12.12.12     10     Osuccess     Done - Push vSmart P     vSmart-2     22.22.22.22     20	10.10.10.10
6. From the menu, select Monitor > Network	
7. Select BR2-VEDGE1.	
8. Click Troubleshooting.	
9 Click Ping	
MONITOR Network > Troubleshooting	
Select Device - BR2-VEDGE1   10.4.0.1 Site (D: 400 Device Model: vedge-aloud	
TCP Optimization	
WAN Throughput Connectivity	Traffic
Flows	
Top Takes	-
WAN	X.,
TLOC	
Turnel	
Control Connections Device Bringup Tun	nel Health
System Status Control Connections(Live View) App Rout	e Visualization
Events Pina Simu	slate Flows
ACL Logs	
Troubleshooting Trace Route	
RealTime	
10 Validato Connectivity from PD2 VEDCE1 +	a tast hast in
Propobl in VDN 10 by optoring docting	
	μh
10.3.10.10	
1 11 Click Ping	





	MONTOR Manual 1 Tableshafing > Pag     Manual Manual 1     Ma
	Budicalise IP*         VPK         Budicalise IV/VE-10           153.1510         VPD-10         gel21-pol-164251.1         +
	Produce 🛞 KSAP 🕓 TOP 🕓 KAP
	Brons Port Beeforder Port
	Advanced bytics: >
	Remark         Multiple           Trainin Trainintian         Figure 1998 109           Paulita Internant         Figure 1998 109           Paulita Internant         Figure 1998 109           Trainin Trainintian         Figure 1998 109           Paulita Internant         Figure 1998 109           Trainin Internant         Figure 1998 109           Traininterit         Figure
	No. (m)         Lan           Soc. (m)         Land Transmittant Consols & By Exclusions, on an exercise           No. (m)         Land           Ang. (m)         Land
	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.	MONITOR Network > Troubleshooting > Ping
	Self-ct Device
	Destination IP* VPN Source/Interface for VPN - 20
	TUCK20110 • Gent/a - Bret/201
	Probes   ICMP  TCP  UDP
	Source Port Destination Port Type Of Service
	Time To Live Dorit Fragment
	Advanced Options >
	Phog
	Summary Output:
	Packets Transmitted 5 Nping in VPN 20 Citations Nation 0.4.47 ( http://organ.com/mices ) at 2019.01.22146-201070
	Packets Received 0 SENT (0.0130s) /CMP [10.42.01 > 10.32.0.10 Echo request (type=8/code=0) id=11032 seq=1] IP [ttl=64 id=50785 iplen=28
	Packet loss (%) 100 SENT (1.0132s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type+8/code+0) id=11032 seq=2] IP [tti=64 id=50785 ipien=28 ]
	Round Trip Time SENT (2.0134s) KCMP (10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=11032 seq=3] IP [ttl=64 id=50785 iplen=28
	14. To De-activate policy select Configuration > Policies.
	15. Click on the three dots () to the right of the
	MultiTopologyPlusACL policy.
	16 Select Deactivate
	C Indiana V Malana V Ma Malana V Malana V Ma
	Instrument         Instrum
	Walf-geloghtack:         Application/SEL help for merborshills. of help builder         East adven
	community         community <thcommunity< th=""> <thcommunity< th=""> <thc< th=""></thc<></thcommunity<></thcommunity<>
	Tele Lacrow
	17. Click Deactivate.
	18 The policy status will change from In Progress to
	Success and the policy is successfully removed from
	the venerate Full meets extract with here been restand
	une vsmartsull mesh connectivity has been restored.





				SK VIEW	🛱 TAS
Initiated By: admin From: 198.18.133.36			idation Success 👻	Smart Policy   😋 Val	Push v
	Total Task: 2   Success : 2				
08					
Total Rows: 2		Search Options 🐱			Q
Site ID vManage IP	System IP	Hostname	Message	Status	
10 10.10.10.10	12.12.12.12	vSmart-1	Done Removing polic	Success	>
20 10.10.10.10	22 22 22 22	vSmart-2	Done Removing polic	Success	>

# 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
	<ol> <li>From the menu, select Configuration &gt; Policies . Select BR2-VEDGE1.</li> </ol>
	2. Click the three dots next to the
	MultiTopologyPlusAppRoute policy.





	3. Select Activate.
	CONFIGURATION   POLICIES
	Centralized Policy Localized Policy
	O Add Policy
	Q Search Options V Total Rowa: 8
	Name Description Type Activated Updated By Policy Version Las View StrietHubroSonike BED/IPSex base UII Policy Builder false admin 1228201177230740 31 Preview
	MultiTopologyPolicy Multi-Topology UI Policy Builder felse admin 12302017T143348 31 Copy
	MultiTopologyPlusFWInsertion Adding FW for I., UI Policy Builder false admin 12312017T143840 31 Delete
	Multi lopologyPlusApRoute App Aware Routi UI Policy Builder false admin 123120171153128 31 Activate MultiTopologyPlusAppRoute App Aware Routi UI Policy Builder false admin 04092018T121824 31 Des 2017115
	4. Click Activate on pop-up.
	Activate Policy
	Activate Cancel
	5 Wait until the policy is successfully pushed to each
	vemort
	vsmart.
	TASK VIEW
	Push vSmart Policy i 🕲 Validation Success * Initiated By: admin From: 198.18.133.36
	TOTAI TABLE Z' SUCCESS Z
	00
	Q Search Options V Total Rows: 2
	Status Message Hotmarre System IP Site ID vManage IP
	O Success         Done - Push vSmart P         vSmart-2         22.22.22.22         20         10.10.10
	6 From the menu select Monitor > Network
NOTE: The device dashboard for BR2-VEDGE1	7 Salaat PD2 VEDCE1
displays the current performance measurement on	7. Select BR2-VEDGET.
both the transports.	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





	MONITOR Network	> Real Time						
	Select Device -	BR2-VEDGE1 10.4	4.0.1 Site E: 4	00 Device Model	t vedge-cloud			
	Flows -	and the second second	-			_		
	interface	Device Options	App]					
		T Filter -	App Log F	Flow Count				00
	TCP Optimization	0	App Log F	Flows		1		Total Govers: 72
	WAN Throughput	Q	App Rout	es SLA Class		1002 -		runni runna, ra
		Device 1P	App Route	es Statistics		Protocol		Destination Port
	Hows	10.4.0.1	CloudExp	ress Applications		psec	12386	12346
	Top Talkers	10.4.0.1	DPI Appli	cations		psec	12386	12346
	WAN	10.4.0.1	DPI Supp	orted Application	s	psec	12386	12346
	man	10.4.0.1	PIM RP M	tapping		DSec	12386	12346
	TLOC	10401	Policy App	p Houte Filter	100.64.9.2	Inser	12396	12246
	Transit	10.4.0.1	000 10000		100.04.0.0	paec	12080	12240
	10000	10.4.0.1	BR2-VEDGE	1 100.04.4.2	100.64.3.2	psec	12386	12340
	Control Connections	10.4.0.1	BR2-VEDGE	1 100.64.4.2	100,64.3.2	psec	12386	12406
	Parters Plates	10.4.0.1	BR2-VEDGE	1 100.64,4.2	100.64.3.2	psec	12386	12406
	aysien aneus	10.4.0.1	BR2-VEDGE	1 100.64.4.2	100.64.3.2	'psec	12386	12406
	Events	10.4.0.1	BR2-VEDGE	1 100.64.4.2	100.64.3.2	psec	12386	12406
	A/3 1	10.4.0.1	BR2-VEDGE	1 100.64.4.2	100.64.3.2	psec	12386	12406
	nu cogs	10.4.0.1	BR2-VEDGE	1 100.64.4.2	100.64.3.2	psec	12386	12406
	Troubleshooting	10.4.0.1	BR2-VEDGE	1 100.64.4.2	172.16.11.2	psec	12386	12386
		10.4.0.1	BP3-VEDGE	1 100 64 4 2	172 16 11 2	inser.	12386	12286
	Real Time	10.4.0.1	BR2-VEDGE	1 100.04.4.2	1/2.10.11.2	paer	12380	12389
definitions defined for the app-route policies.	and tuni	l Avera nels on	ge) La MPL	atency S and	, Loss Intern	and Jit iet.	tter for	each of the
	MONITOR Network	k > Real Time						
	Select Device -	BR2-VEDGE1   10	0.4.0.1 Site ID:	400 Device Mod	el: vedge-cloud	0		
	Hows	-						
	Interface	Device Option	s: 🔍 App Ro	outes Statistics				
		- Filter *						00
	TCP Optimization							Tata Davis 22
	WAN Throughput	Q			Search	Options ~		Total Hows: 72
		Lo	ocal Color	Remote Color	Mean Loss	Mean Latency	y Mean Jitter	SLA Class index
	Flows	bi	z-internet	biz-internet	0	1	0	0,1,2,3,4
	Top Talkers	b	z-internet	biz-internet	0	1	0	0,1,2,3,4
		bi	z-internet	biz-internet	0	1	0	0.1.2.3.4
	WAN	b	z-internet	biz-internet	0	1	0	0.1.2.3.4
	TLOC	h	z-internet	hiz-internet	0	1	0	01234
	Tunnel		a internet	hiz internet	0		0	01224
	Tunnes	D	z-internet	biz-internet		1	0	0,1,2,3,4
	Control Connections	b	z-internet	biz-internet	0	1	0	0,1,2,3,4
	Ounteen Otatus	b	z-internet	biz-internet	0	1	0	0,1,2,3,4
	system status	bi	z-internet	biz-internet	0	1	0	0,1,2,3,4
	Events	bi	z-internet	biz-internet	0	1	0	0,1,2,3,4
	ACI Logs	bi	z-internet	biz-internet	0	1	0	0,1,2,3,4
	ma cop	bi	z-internet	biz-internet	0	1	0	0,1,2,3,4
	Troubleshooting	bi	z-internet	biz-internet	0	0	0	0,1,2,3,4
	Real Time	bi	z-internet	biz-internet	0	0	0	0,1,2,3,4
	New Three	-					-	
<b>NOTE:</b> Simulate Flow s provides a simulation on what IPSec tunnels will used for the defined flow based on policies and transport performance measurements.	12. Sel 13. Clic 14. Sel 15. Sel 16. Ent 17. Clic 18. Ent	ect Tro ect VPf ect the er 10.3 ek Adva er the [	ubles Ilate F N 10. sourc .10.1 inced DSCP	hootin lows. ce inte 0 as th Option value	g. rface ne des ns . of 46.	tination	ı IP adc	Iress.
	19. Clic	k Simu	llate.					



CISCO



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.	MONITOR       Network:       Troubleshooting • Simulate Flows         Gelear Device       Bit2-VEDE(1)10.4.0.1       Site ID: 400       Device Model: vidge Cloud       Image: Cloud       Ima
	WAN Impairment         20. Open new tab in Chrome and click the WAN Impairment bookmark         Impairment bookmark         Impairment with the WAN Impairment <b>dCloud WAN Impairment Control Panel</b> Select site to manage:         Datacenter 1         Datacenter 2         Branch 1         Branch 2         Branch 3
	<ul> <li>21. Click Branch 1 and choose mpls transport and then click Submit.</li> <li>Click Submit.</li> <li>Click Of the open Simulated Flow browser tab.</li> </ul>



CISCO



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. <u>dCloud WAN Impairment Control Panel</u> <u>Latency Removed</u>
Select site to manage: Datacenter 1 Datacenter 2 Branch 1 Branch 2 Branch 3 Remove Latency
25. From the menu, select Configuration > Policies . 26. Click the three dots () to the right of the MultiTopologyPlusAppRoute. 27. Select Deactivate.
<ul> <li>28. Click Deactivate.</li> <li>29. The policy status will change from In Progress to Success, and the policy is successfully removed from the vSmarts.</li> </ul>
Initiated By: admin       From: 198.18.133.36         Total Task: 2   Success : 2       Initiated By: admin         Q       Search Options ∨         Status       Message         Hostname       System IP         Status       Done Removing polic         VSmart-1       12.12.12.12         10       10.10.10.10

Copyright © 2019 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9–11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.





# 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.

BranchType1Template-CSR	Branch Type 1 T	Feature	CSR1000v	21	2	admin	13 May 2019 7:15	In Sync		•••
BranchType3Template-CSR	Branch Type 3 T	Feature	CSR1000v	21	1	admin	24 Jul 2019 12:39	In Sync	View	

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

φ	CONFIGURATION   TEMPLA	ATES		
	<b>Basic Information</b>	Transport & Management VPN	Service VPN	Additional Templates
	Additional Templates			
	AppQoE	Choose	•	
	Banner	All-Banner-dCloud	•	
	Policy	BaselinePolicy	•	
	SNMP	All-SNMP-Basic	•	
	Security Policy	Branch-DIA-Security	•	
			Cancel	
			Guilder	

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

Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated	
Branch-DIA-Security	Branch Guest DIA Security	Direct Internet Access	3	2	admin	15 Aug 2019 3:05:50 PM CDT	•••
						View Preview	

- 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.

	Sources	Destinations	
	BUERT-PARIDE	Rules oursee	
Name BRANCH OLA GUEST Description Dranch Quest DIA Polley			
Drop	Erotled		
Match Conditions     Seurce Data Prets List     Seurce: IP	Cately efabR1	Actions Inspect Gratied	
Match Conditions     Second Data Party	0wx8xdx885	Actions	
Source: IP	Variet Streets	Inspect Evalued	

- 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.

CONFIGURATION Security > V	iew Security Policy Branch-DIA-Security				
	Firewall Intrusion Preven	URL Filtering Advanced Malware Pro	otection DNS Security Policy Summary		
٩	Search Options 🗸			Т	otal Rows: 1
Name	Туре	Reference Count	Updated By	Last Updated	
Branch-DIA-IPS	intrusionPrevention	1	admin	22 Jan 2019 9:32:21 AM CST	
				Graphical Pri View	review

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.

......

CISCO

Copyright © 2019 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.





CONFIGURATION   SECURIT	CONFIGURATION   SECURITY View Intrusion Prevention Policy						
Tar	rget		Policy Behavior				
	1	Inspection Mode: Protection	Signature Set: Security Whitelist: -	Log Level: Error			
VP	PNs	Actions	Signatures	Alerts			
Intrusion Prevention	n - Policy Rule Configur	ration 0					
Advanced 🗸					•		
Signature Whitelist	Select a signature list				- 11		
Alerts Log Level 🌖	Error	Ÿ			×		
			CANCEL				

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

CONFIGURATION Security > View	/ Security Policy Branch-DIA-Security				
	Firewall Intrusion Preven	tion URL Filtering Advanced Malware Pro	otection DNS Security Policy Summary		
					88
Q	Search Options 🗸				Total Rows: 1
Name	Туре	Reference Count	Updated By	Last Updated	
Branch-DIA-URLFilter	urlFiltering	1	admin	02 Aug 2019 9:15:53 AM CDT	
				Graphical View	Preview

18. Click Cancel.





Target		Policy Behavior				
1 VPNs		Block Categories: 23 Web Reputation: Moderate Risk URLs: Malware_Demo Blacklist URLs: - Web Filter	Action: Block Page Block Page Server	Blacklist: Disabled Whitelist: Disabled Reputation/Category: Disabled Alerts		
URL Filtering - Policy Rule C Policy Name	configuration	1 0				
Web Categories Blo	ock 👻	bot-nets cult-and-occult confirm	ned-spam-sources dead-sites had			

19. Click Advanced Malware Protection.

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

CONFIGURATION Security > View Security	nty Policy Branch-DIA-Secur	ity					
		Firewall Intrusio	n Prevention URL Filtering	Advanced Maiware Protection	DNS Security Policy Summary		
							00
Q	Search Options 🗸						Total Rowa: 1
Name	Туре		Reference Count		Updated By	Last Updated	
BRANCH-DIA-AMP	e advancedMalwarePr	rotection	1		admin	03 Sep 2019 3:14:08 PM EDT	
							Graphical Preview View

21. Click Cancel.

CONFIGURATION   SECURITY View Advanced I	Melware Protection				
	Target		Policy Behavior		
	1 -	AMP Cloud Region: NAM	T8 Cloud Region: - File Types List: -	Reputation Alert Level: Critical Analysis Alert Level: -	
	VPNs	File Reputation	File Analysis	Alerts	
Advanced Malware Protection - Poli	icy Rule Configuration 🏮				
Policy Name	MIP				
O Match All VPN ( Custom VPN Confi	iguration				
File Reputation					
AMP Cloud Region NAM	Ψ				
Alerts Log Level Critical	Ψ				
File Analysis					
			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.