Cisco SD-WAN (Viptela) Instant Demo v1

Last Updated: 14-JUNE-2018

About This Demonstration

This guide for the demonstration includes:

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Requirements

Required	Optional
• Laptop	• Cisco AnyConnect®

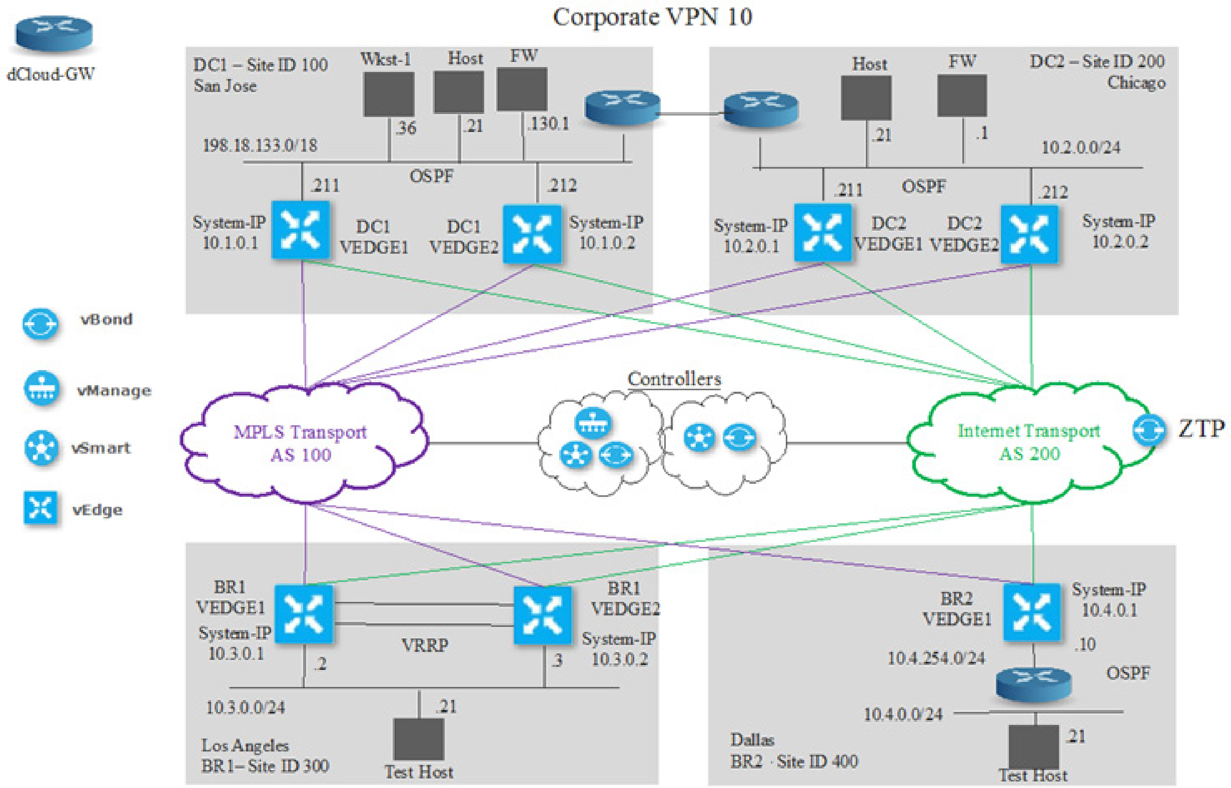
About This Solution

Cisco SD-WAN delivers an uncompromised user experience over any kind of transport, allowing the business to right size their network with operational simplicity while lowering costs. Now, IT can fully utilize their WAN investments with the highest performance, reliability, and security while ensuring that all next generation WAN capability requirements necessary to avoid unexpected expenses, unplanned downtime and unforeseen complications are accounted for.

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.

Figure 1. dCloud Topology



Get Started

BEFORE PRESENTING

Cisco dCloud strongly recommends that you perform the tasks in this document with an active session before presenting in front of a live audience. This will allow you to become familiar with the structure of the document and content.

It may be necessary to schedule a new session after following this guide in order to reset the environment to its original configuration.

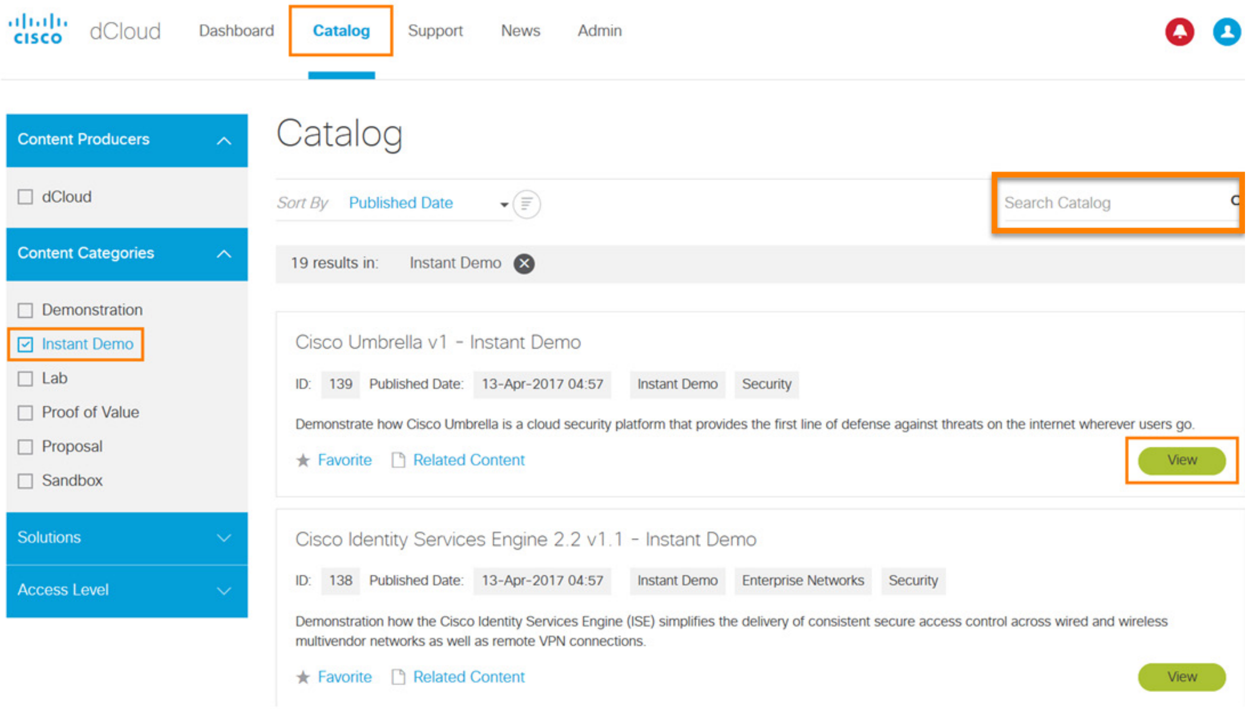
PREPARATION IS KEY TO A SUCCESSFUL PRESENTATION.

Follow the steps to schedule a session of the content and configure your presentation environment.

1. Click **Catalog** and select **Instant Demo** from the side bar. This lists all the dCloud Instant Demos.
2. Click the appropriate **View** button.

NOTE: Alternately, you can use the Search Catalog box to search for the Instant Demo name.

Figure 2. Instant Demo Listing



Cisco Umbrella v1 - Instant Demo

ID: 139 Published Date: 13-Apr-2017 04:57 Instant Demo Security

Demonstrate how Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go.

Cisco Identity Services Engine 2.2 v1.1 - Instant Demo

ID: 138 Published Date: 13-Apr-2017 04:57 Instant Demo Enterprise Networks Security

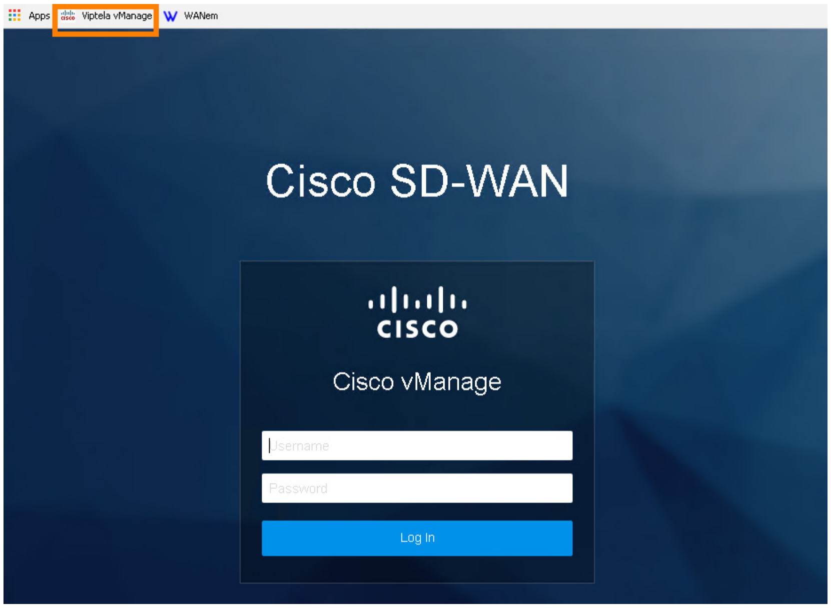
Demonstration how the Cisco Identity Services Engine (ISE) simplifies the delivery of consistent secure access control across wired and wireless multivendor networks as well as remote VPN connections.

Scenario 1. vManage Dashboard

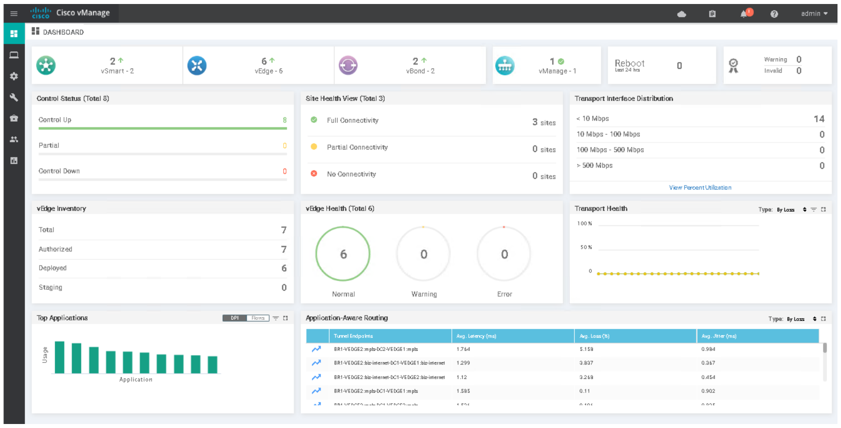
Steps

<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr>
<td>The dashboard provides aggregated visibility into the environment.</td>
<td>

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. Login to vManage using amdemo1/C1sco12345 for username/password.



4. The vManage Dashboard displays aggregated visibility into the environment.



2 vSmart - 2
6 vEdge - 6
2 vBond - 2
1 vManage - 1
Reboot Last 24 hrs 0
Warning 0
Invalid 0

Control Status (Total 8)
Control Up 8
Partial 0
Control Down 0

Site Health View (Total 3)
Full Connectivity 3 sites
Partial Connectivity 0 sites
No Connectivity 0 sites

Transport Interface Distribution
< 10 Mbps 14
10 Mbps - 100 Mbps 0
100 Mbps - 500 Mbps 0
> 500 Mbps 0

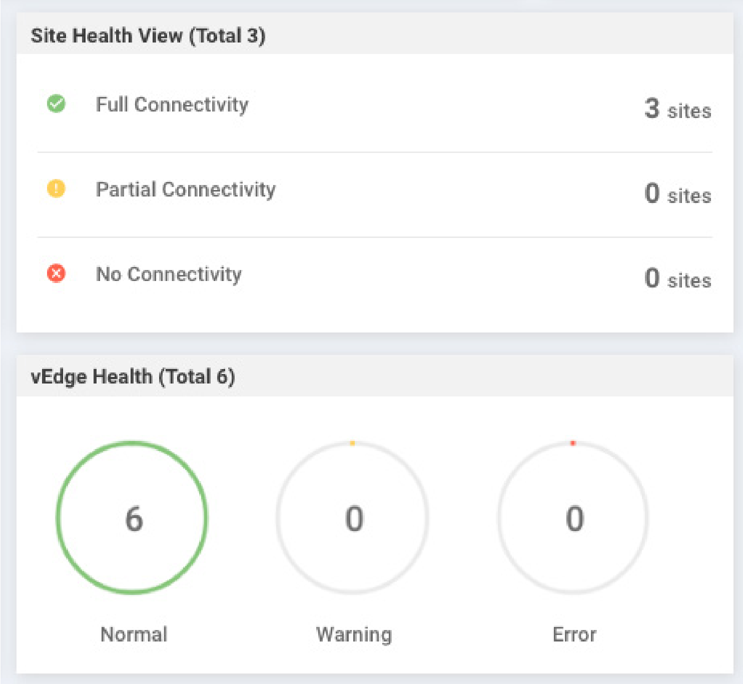
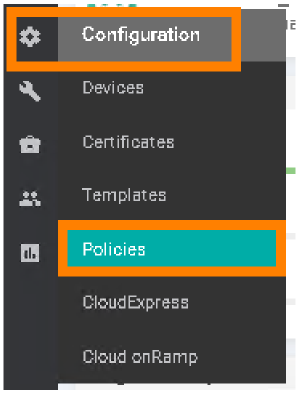
vEdge Inventory
Total 7
Authorized 7
Deployed 6
Staging 0

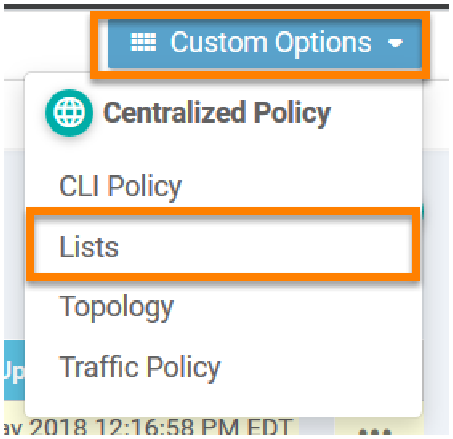
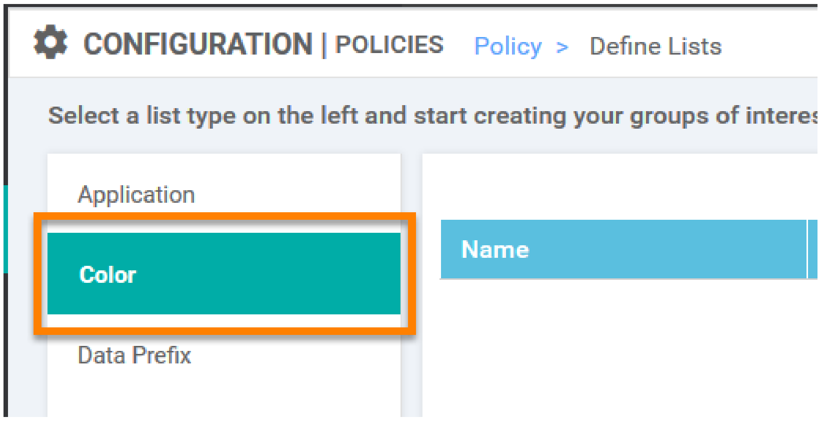
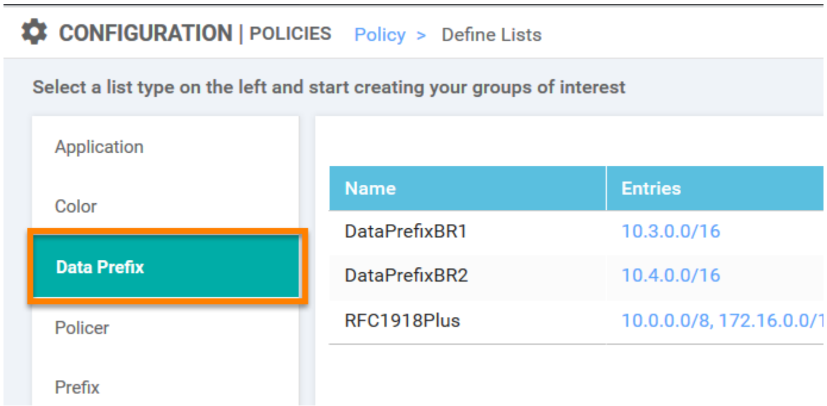
vEdge Health (Total 6)
6 Normal
0 Warning
0 Error

Application-Aware Routing

<table>
<tr><th>Tunnel Endpoints</th><th>Avg. Latency (ms)</th><th>Avg. Loss (%)</th><th>Avg. Jitter (ms)</th></tr>
<tr><td>BR1-VEDGE2:mpls-DC2-VEDGE1:mpls</td><td>1.764</td><td>5.158</td><td>0.984</td></tr>
<tr><td>BR1-VEDGE2:biz-internet-DC1-VEDGE1:biz-internet</td><td>1.299</td><td>3.837</td><td>0.367</td></tr>
<tr><td>BR1-VEDGE2:biz-internet-DC1-VEDGE2:biz-internet</td><td>1.12</td><td>3.268</td><td>0.454</td></tr>
<tr><td>BR1-VEDGE2:mpls-DC1-VEDGE1:mpls</td><td>1.585</td><td>0.11</td><td>0.902</td></tr>
</table>

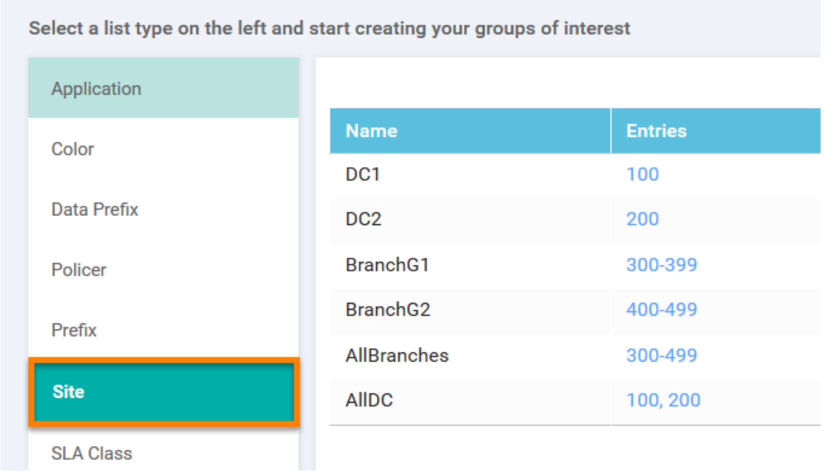
</td>
</tr>
</table>

DIALOG	DEMONSTRATION STEPS
	5. Point out that the dashboard contains vital information, such as the overall health statistics for **Site Health and vEdge Health**.  Site Health View (Total 3) ✓ Full Connectivity 3 sites ! Partial Connectivity 0 sites ✕ No Connectivity 0 sites vEdge Health (Total 6) 6 Normal 0 Warning 0 Error
	6. From the menu, select **Configuration > Policies**.  Configuration Devices Certificates Templates Policies CloudExpress Cloud onRamp

DIALOG	DEMONSTRATION STEPS
	7. In the upper right corner, select **Custom Options > Lists.**  Custom Options Centralized Policy CLI Policy Lists Topology Traffic Policy ay 2018 12:16:58 PM EDT
The color is a tag used to define transports to the environment. Tags are assigned to the circuits being used.	8. From the left panel, click **Color**.  CONFIGURATION | POLICIES Policy > Define Lists Application Color Data Prefix Name Select a list type on the left and start creating your groups of interes
This displays the routing prefixes to change the topology within the routing construct.	9. From the left panel, click **Data Prefix**.  CONFIGURATION | POLICIES Policy > Define Lists Application Color Data Prefix Policer Prefix Select a list type on the left and start creating your groups of interest Name — Entries DataPrefixBR1 — 10.3.0.0/16 DataPrefixBR2 — 10.4.0.0/16 RFC1918Plus — 10.0.0.0/8, 172.16.0.0/1

<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr>
<td>This allows you to specify groupings within the environment based on role, region, or other characteristics to distinguish site types.</td>
<td>

10. From the left panel, click **Site**.

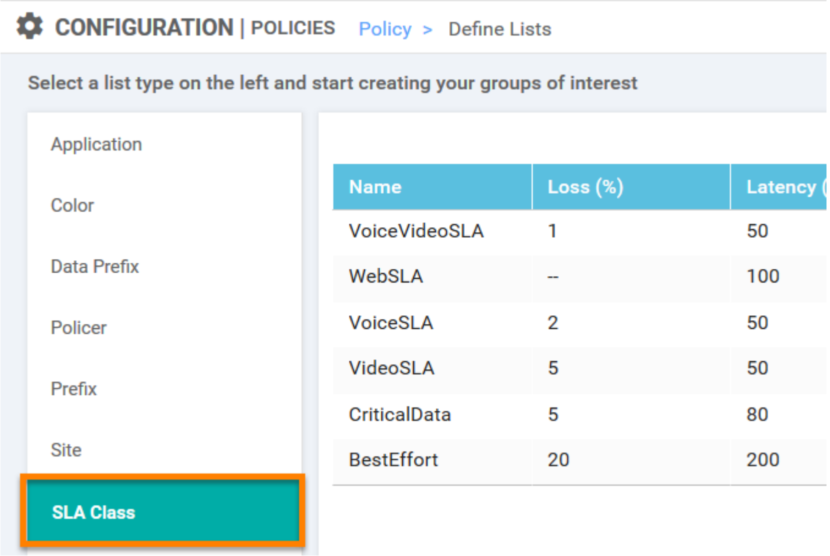


Select a list type on the left and start creating your groups of interest

<table>
<tr><th>Name</th><th>Entries</th></tr>
<tr><td>DC1</td><td>100</td></tr>
<tr><td>DC2</td><td>200</td></tr>
<tr><td>BranchG1</td><td>300-399</td></tr>
<tr><td>BranchG2</td><td>400-499</td></tr>
<tr><td>AllBranches</td><td>300-499</td></tr>
<tr><td>AllDC</td><td>100, 200</td></tr>
</table>

</td>
</tr>
<tr>
<td>This allows you to define classifications at the SLA level to satisfy the required loss and latency characteristics for applications or types of applications.</td>
<td>

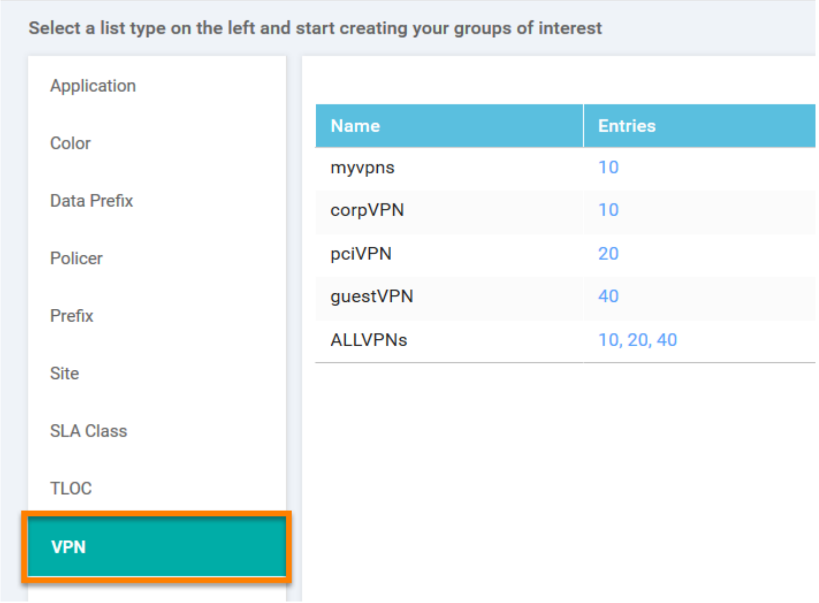
11. From the left panel, click **SLA Class**.

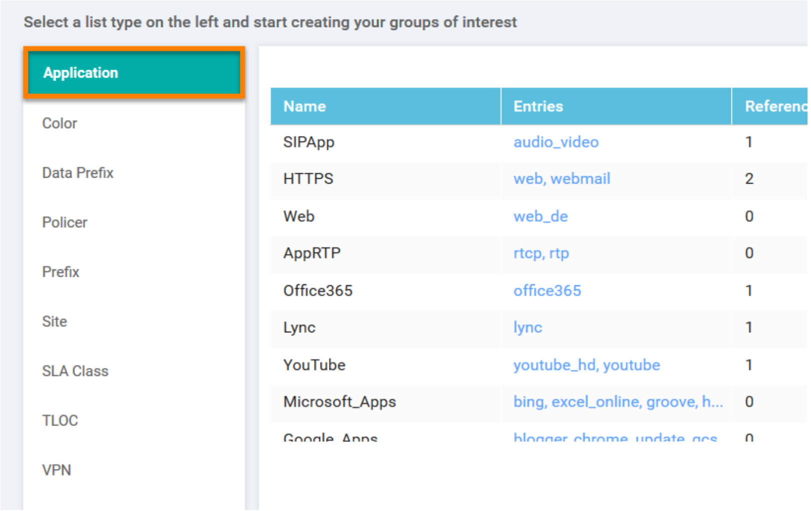


Select a list type on the left and start creating your groups of interest

<table>
<tr><th>Name</th><th>Loss (%)</th><th>Latency (</th></tr>
<tr><td>VoiceVideoSLA</td><td>1</td><td>50</td></tr>
<tr><td>WebSLA</td><td>--</td><td>100</td></tr>
<tr><td>VoiceSLA</td><td>2</td><td>50</td></tr>
<tr><td>VideoSLA</td><td>5</td><td>50</td></tr>
<tr><td>CriticalData</td><td>5</td><td>80</td></tr>
<tr><td>BestEffort</td><td>20</td><td>200</td></tr>
</table>

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

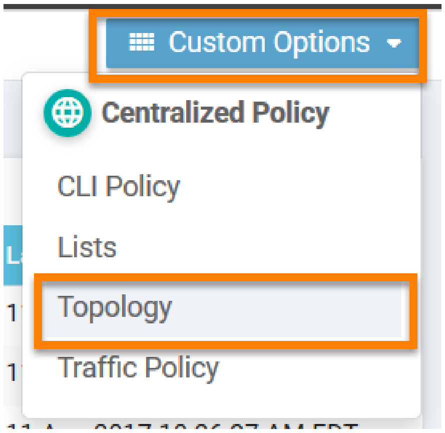
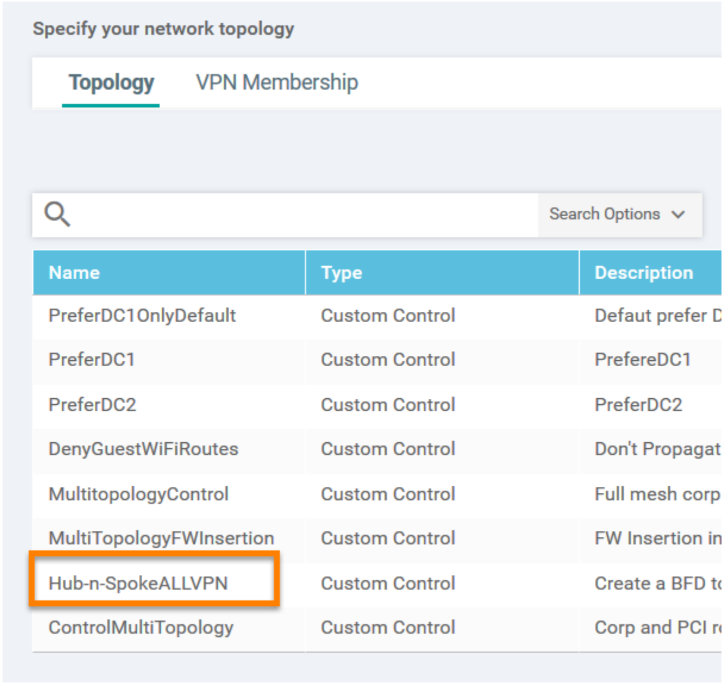
<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr>
<td>
<p>This allows you to define the different segments you will carry inside your network, separating them by purpose, for example, public vpn vs corporate vpn.</p>
<p>Within each vpn construct, you can apply specific policies, leveraging the criteria assigned, for instance, which route is advertised within each VPN, or what to do with the different transports or application on a segment-by-segment basis.</p>
</td>
<td>
<p>12. From the left panel, click <b>VPN</b>.</p>

<p>Select a list type on the left and start creating your groups of interest</p>

<table>
<tr><th>Name</th><th>Entries</th></tr>
<tr><td>myvpns</td><td>10</td></tr>
<tr><td>corpVPN</td><td>10</td></tr>
<tr><td>pciVPN</td><td>20</td></tr>
<tr><td>guestVPN</td><td>40</td></tr>
<tr><td>ALLVPNs</td><td>10, 20, 40</td></tr>
</table>
</td>
</tr>
<tr>
<td>
<p>Once all the objects are defined, you can view and deliver a complete application.</p>
</td>
<td>
<p>13. From the left panel, click <b>Application</b>.</p>

<p>Select a list type on the left and start creating your groups of interest</p>

<table>
<tr><th>Name</th><th>Entries</th><th>Referenc</th></tr>
<tr><td>SIPApp</td><td>audio_video</td><td>1</td></tr>
<tr><td>HTTPS</td><td>web, webmail</td><td>2</td></tr>
<tr><td>Web</td><td>web_de</td><td>0</td></tr>
<tr><td>AppRTP</td><td>rtcp, rtp</td><td>0</td></tr>
<tr><td>Office365</td><td>office365</td><td>1</td></tr>
<tr><td>Lync</td><td>lync</td><td>1</td></tr>
<tr><td>YouTube</td><td>youtube_hd, youtube</td><td>1</td></tr>
<tr><td>Microsoft_Apps</td><td>bing, excel_online, groove, h...</td><td>0</td></tr>
<tr><td>Google_Apps</td><td>blogger, chrome_update, gcs</td><td>0</td></tr>
</table>
</td>
</tr>
</table>

Scenario 2. Topology Creation, Traffic Data, Application Aware Routing, and Monitoring Visibility

Steps

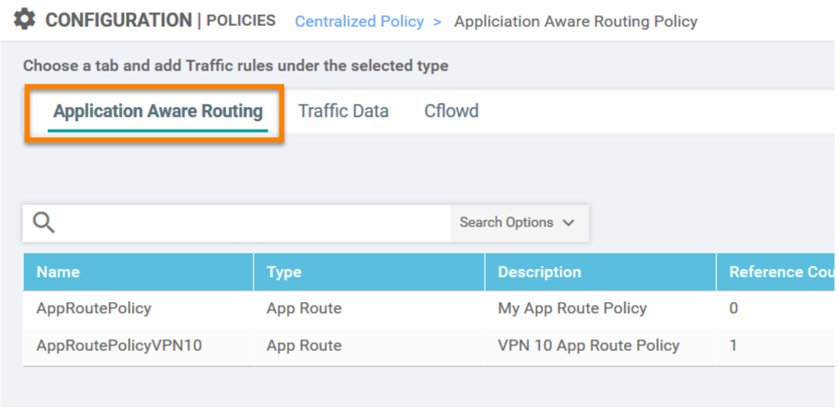
<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr>
<td>The topology helps you define how you control your environment. Can you use a generic Hub and Spoke? Do you need customized setting and mesh type connectivity? Whatever the needs, you can set them using the topology. One single stop helps define everything.</td>
<td>1. In the upper right corner, select <b>Custom Options > Topology.</b>

</td>
</tr>
<tr>
<td>For Hub and Spoke, the wizard is fairly straight-forward, since we’ve taken the time to identify and define all the hub sites.
If the requirements are more complex, for instance for creating a globally distributed network or multiple data centers in multiple geographies, and the branch site in the US must transit through a branch site in Singapore and one in Hong Kong.
This will require you to define much more granularly what data to manipulate.
You can select which routes or transports are used to engineer a transport from end to end, across multiple regions, and have full traffic engineering capabilities.
SD-WAN allows very powerful control over any type of topology.</td>
<td>2. From the existing policies, click the three dots to the right of <b>Hub-n-SpokeALLVPN</b>.
3. Click <b>View</b>.


<table>
<tr><th>Name</th><th>Type</th><th>Description</th></tr>
<tr><td>PreferDC1OnlyDefault</td><td>Custom Control</td><td>Defaut prefer D</td></tr>
<tr><td>PreferDC1</td><td>Custom Control</td><td>PrefereDC1</td></tr>
<tr><td>PreferDC2</td><td>Custom Control</td><td>PreferDC2</td></tr>
<tr><td>DenyGuestWiFiRoutes</td><td>Custom Control</td><td>Don't Propagat</td></tr>
<tr><td>MultitopologyControl</td><td>Custom Control</td><td>Full mesh corp</td></tr>
<tr><td>MultiTopologyFWInsertion</td><td>Custom Control</td><td>FW Insertion in</td></tr>
<tr><td>Hub-n-SpokeALLVPN</td><td>Custom Control</td><td>Create a BFD to</td></tr>
<tr><td>ControlMultiTopology</td><td>Custom Control</td><td>Corp and PCI r</td></tr>
</table>
4. Click <b>Cancel</b>.</td>
</tr>
</table>

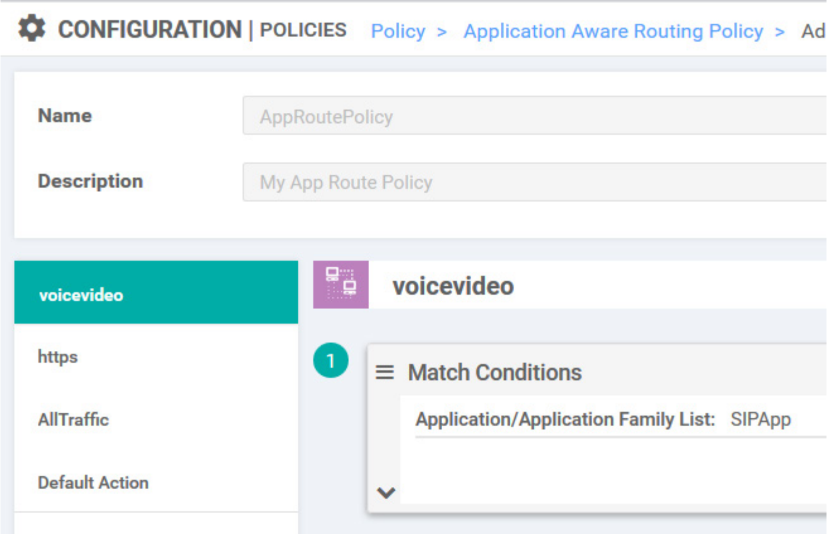
<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr>
<td>
Now that the topology is defined, you can define what happens to each application inside each VPN.

In a centralized fashion, you can define rules for different types of applications.
</td>
<td>
5. In the upper right corner, select <b>Custom Options > Traffic Policy.</b>

6. <b>Application Aware Routing</b> is displayed.

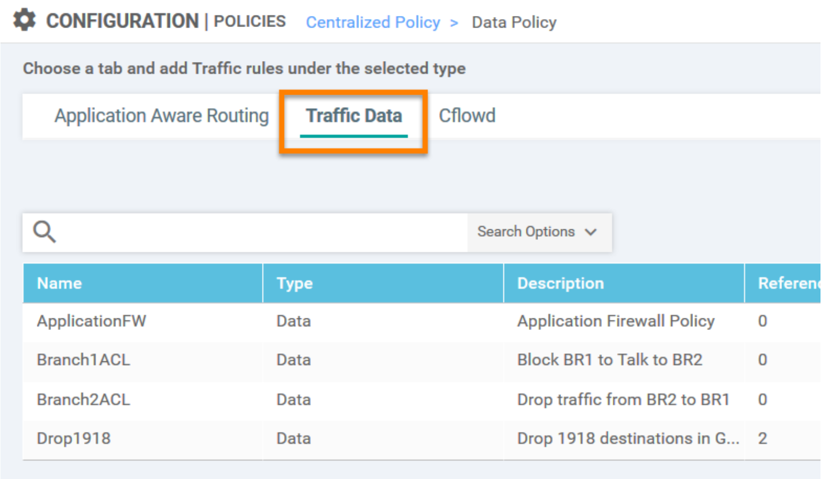

CONFIGURATION | POLICIES Centralized Policy &gt; Appliciation Aware Routing Policy
Choose a tab and add Traffic rules under the selected type
Application Aware Routing Traffic Data Cflowd
Search Options
<table>
<tr><th>Name</th><th>Type</th><th>Description</th><th>Reference Cou</th></tr>
<tr><td>AppRoutePolicy</td><td>App Route</td><td>My App Route Policy</td><td>0</td></tr>
<tr><td>AppRoutePolicyVPN10</td><td>App Route</td><td>VPN 10 App Route Policy</td><td>1</td></tr>
</table>

7. Click the three dots to the right of one of the routing policies and click <b>View</b> to get details.


CONFIGURATION | POLICIES Policy &gt; Application Aware Routing Policy &gt; Ad
Name: AppRoutePolicy
Description: My App Route Policy
voicevideo
https
AllTraffic
Default Action
voicevideo
1 Match Conditions
Application/Application Family List: SIPApp
</td>
</tr>
</table>

<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr><td>You can apply unique SLAs for different types of traffic. You can also specify which transport you prefer to offload traffic from a priority to a non-prioritized circuit in order to preserve bandwidth.</td><td>

8. Click back on your browser and click **Traffic Data**.

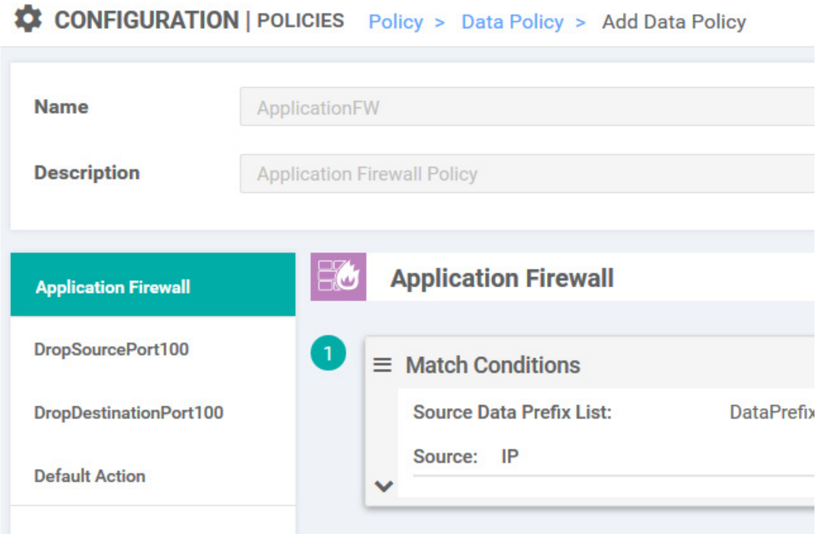


CONFIGURATION | POLICIES Centralized Policy > Data Policy

Choose a tab and add Traffic rules under the selected type

<table>
<tr><th>Name</th><th>Type</th><th>Description</th><th>Referen</th></tr>
<tr><td>ApplicationFW</td><td>Data</td><td>Application Firewall Policy</td><td>0</td></tr>
<tr><td>Branch1ACL</td><td>Data</td><td>Block BR1 to Talk to BR2</td><td>0</td></tr>
<tr><td>Branch2ACL</td><td>Data</td><td>Drop traffic from BR2 to BR1</td><td>0</td></tr>
<tr><td>Drop1918</td><td>Data</td><td>Drop 1918 destinations in G...</td><td>2</td></tr>
</table>

9. Click the three dots to the right of one of the traffic data policies and click **View** to get details.



CONFIGURATION | POLICIES Policy > Data Policy > Add Data Policy

Name: ApplicationFW

Description: Application Firewall Policy

Source Data Prefix List: DataPrefix

Source: IP

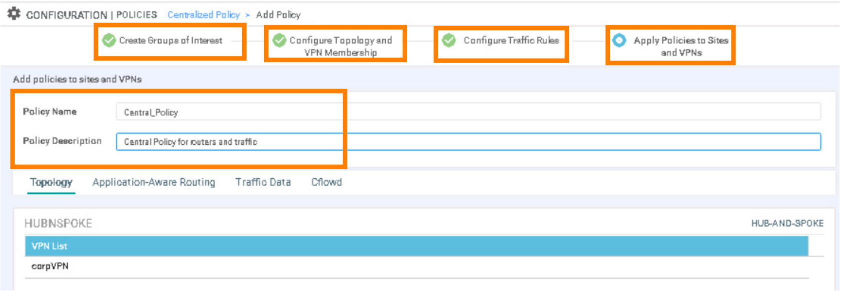
</td></tr>
<tr><td>

Once you define how the applications are treated, you can use the activation mechanism to propagate the policy across the network.

This one page provides the ability to define the entire business objects, your network topology, to control the application traffic, and apply it across the network. This eliminates the need for configuration on any remote endpoints, either physical or virtual, other than IP addressing. All routing or traffic applications are centrally-defined across the network.

</td><td>

10. Click **Cancel**.



CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest
Configure Topology and VPN Membership
Configure Traffic Rules
Apply Policies to Sites and VPNs

Add policies to sites and VPNs

Policy Name: Central_Policy

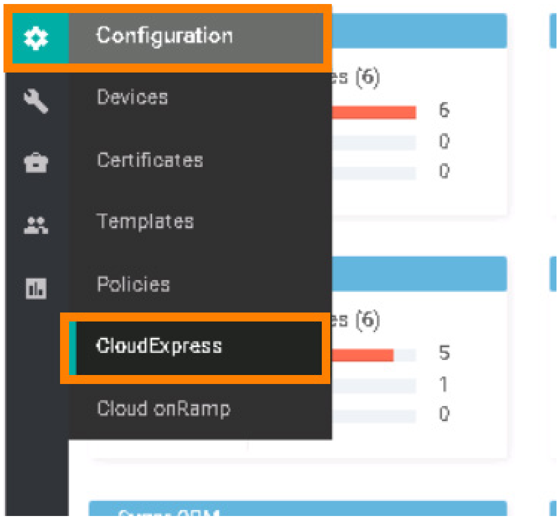
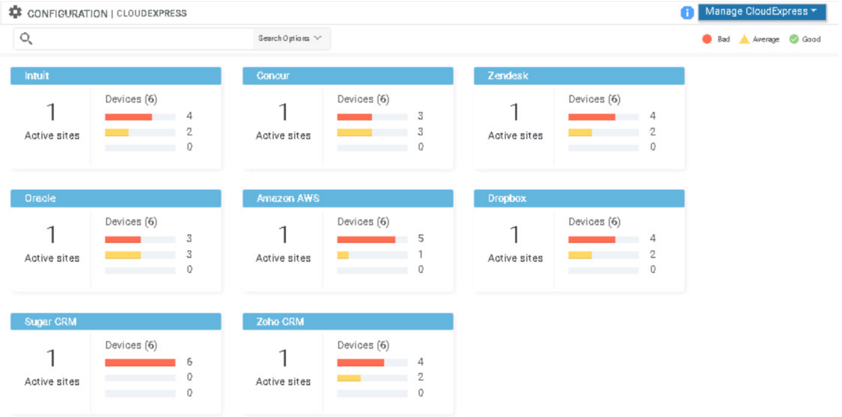
Policy Description: Central Policy for routers and traffic

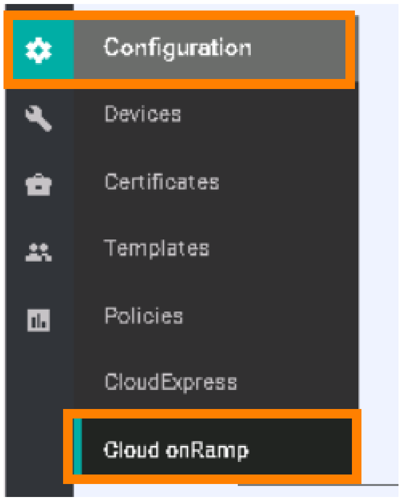
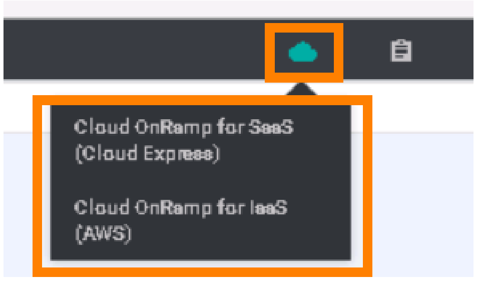
Topology
Application-Aware Routing
Traffic Data
Cflowd
HUBNSPOKE
HUB-AND-SPOKE

VPN List

corpVPN

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

DIALOG	DEMONSTRATION STEPS
So far, we have looked at setting a particular workflow. For setting the wide area network for various lines of business or applications or QOS purposes, we have to consider that so many applications now reside in the Cloud. You want to be able to create optimal pathing for traffic that resides in the cloud. And for this, you will use CloudExpress. This environment provides visibility into a number of applications that reside in the cloud, as well as metrics from the lab environment to the lab instances, including performance metrics.	11. From the menu, click **Configuration > Cloud Express**.  Configuration Devices Certificates Templates Policies CloudExpress Cloud onRamp  CONFIGURATION | CLOUDEXPRESS Manage CloudExpress Search Options Bad Average Good Intuit 1 Active sites Devices (6) 4 2 0 Concur 1 Active sites Devices (6) 3 3 0 Zendesk 1 Active sites Devices (6) 4 2 0 Oracle 1 Active sites Devices (6) 3 3 0 Amazon AWS 1 Active sites Devices (6) 5 1 0 Dropbox 1 Active sites Devices (6) 4 2 0 Sugar CRM 1 Active sites Devices (6) 6 0 0 Zoho CRM 1 Active sites Devices (6) 4 2 0

DIALOG	DEMONSTRATION STEPS
The Cloud onRamp allows you to directly access the cloud and define rules that allow your appliances to directly connect to AWS as your infrastructure. This allows you to deploy appliances directly into other services, like Amazon Web Services and make it natively part of the network. We have the business objectives identified, and the objects of interests to be optimized on the network, as well as the centralized policy activation to deliver the quality experience for these applications.	12. From the menu, click **Configuration > Cloud onRamp.**  Configuration Devices Certificates Templates Policies CloudExpress Cloud onRamp  Cloud OnRamp for SaaS (Cloud Express) Cloud OnRamp for IaaS (AWS)

DIALOG

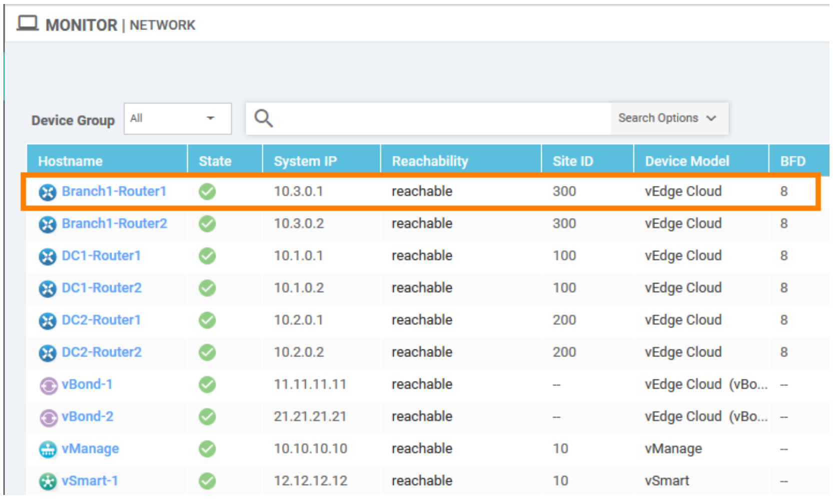
Now, we need assurance and visibility into what is happening in our environment, and to able to get alerts from the environment and trigger improvements.

vManage also has monitoring capabilities, with visibility into any device that is operational, including a direct tunnel path to every device and visibility into the performance, characteristics, and traffic that passes through the device.

vManage gives you visibility into device health, like CTU memory consumption. You can also see the applications traveling through the environment, and flow traffic.

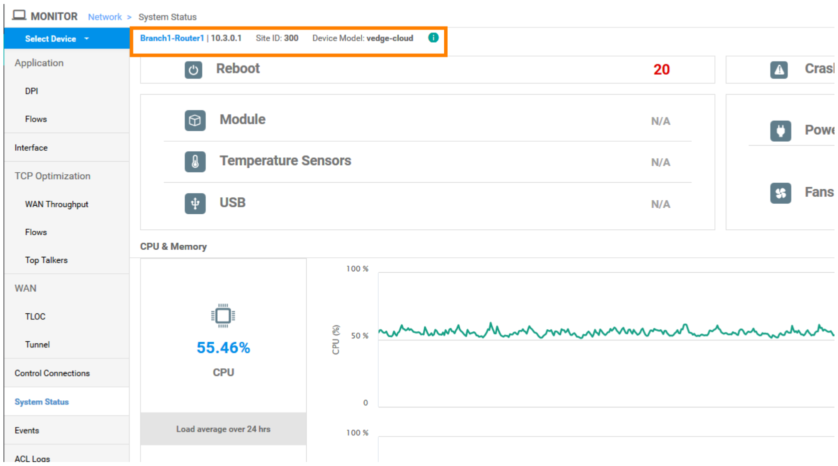
DEMONSTRATION STEPS

13. From the menu, select **Monitor > Network**.
14. Click **Branch1-Router1**.



MONITOR | NETWORK

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD
Branch1-Router1	✓	10.3.0.1	reachable	300	vEdge Cloud	8
Branch1-Router2	✓	10.3.0.2	reachable	300	vEdge Cloud	8
DC1-Router1	✓	10.1.0.1	reachable	100	vEdge Cloud	8
DC1-Router2	✓	10.1.0.2	reachable	100	vEdge Cloud	8
DC2-Router1	✓	10.2.0.1	reachable	200	vEdge Cloud	8
DC2-Router2	✓	10.2.0.2	reachable	200	vEdge Cloud	8
vBond-1	✓	11.11.11.11	reachable	--	vEdge Cloud (vBo...	--
vBond-2	✓	21.21.21.21	reachable	--	vEdge Cloud (vBo...	--
vManage	✓	10.10.10.10	reachable	10	vManage	--
vSmart-1	✓	12.12.12.12	reachable	10	vSmart	--



MONITOR Network > System Status

Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud

Reboot 20

Crasl

Module N/A

Temperature Sensors N/A

USB N/A

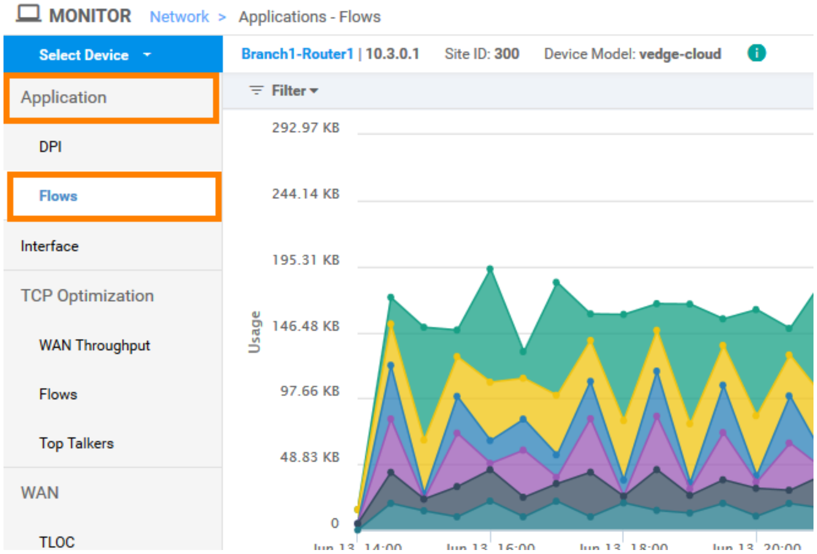
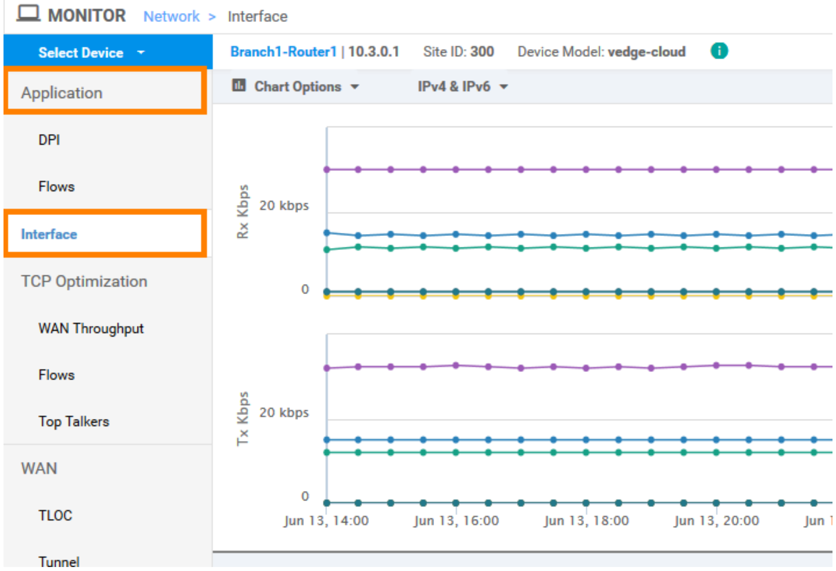
Powe

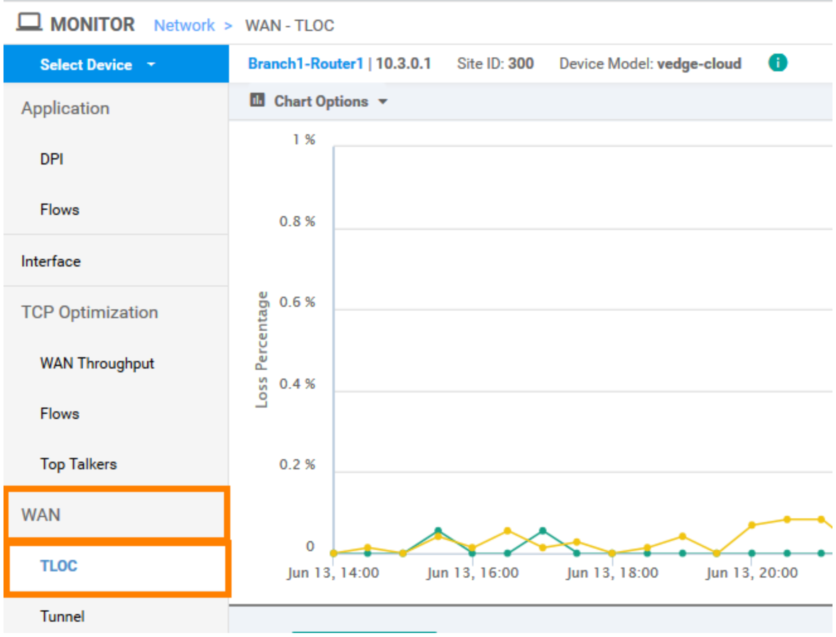
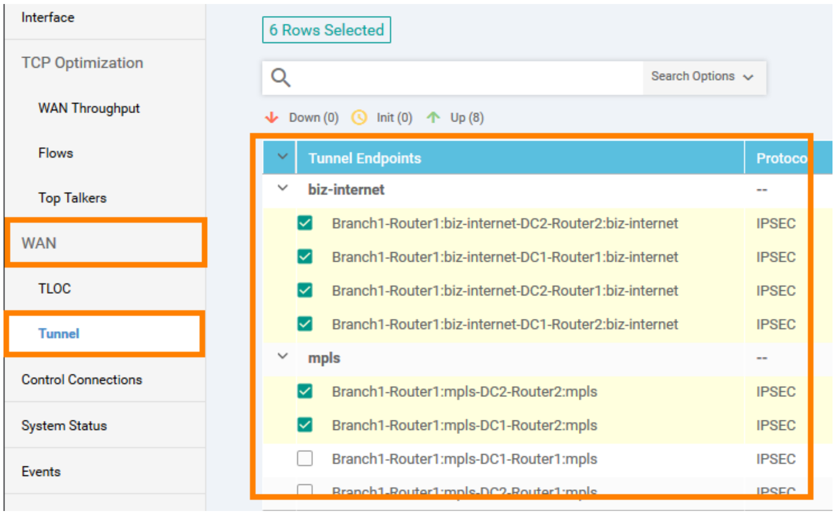
Fans

CPU & Memory

55.46%
CPU

Load average over 24 hrs

DIALOG	DEMONSTRATION STEPS
The traffic generator shows the periodic spikes of traffic, allowing us to see not only the traffic generated, but also the source and destination.	15. Click **Application > Flows**.  MONITOR Network > Applications - Flows Select Device Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud Application DPI Flows Interface TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Filter 292.97 KB 244.14 KB 195.31 KB 146.48 KB 97.66 KB 48.83 KB 0 Usage Jun 13, 14:00 Jun 13, 16:00 Jun 13, 18:00 Jun 13, 20:00
This shows visibility in terms of overall utilization of the different transports and tunnels, and the overall consumption among them.	16. Click on **Application > Interface.**  MONITOR Network > Interface Select Device Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud Application DPI Flows Interface TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Tunnel Chart Options IPv4 & IPv6 Rx Kbps 20 kbps 0 Tx Kbps 20 kbps 0 Jun 13, 14:00 Jun 13, 16:00 Jun 13, 18:00 Jun 13, 20:00 Jun 1

DIALOG	DEMONSTRATION STEPS
The aggregated visualization gives visibility into the transport in question, that is, what are the aggregate characteristics of those transports with regards to loss, latency, and jitter.	17. Click **WAN > TLOC**.  MONITOR Network > WAN - TLOC Select Device Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud Chart Options Application DPI Flows Interface TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Tunnel 1 % 0.8 % 0.6 % 0.4 % 0.2 % 0 Loss Percentage Jun 13, 14:00 Jun 13, 16:00 Jun 13, 18:00 Jun 13, 20:00
You can get a further breakdown into the IPSEC tunnels constructed over the transports to any number of end points. This also supplies metrics for loss, latency and jitter on a tunnel by tunnel basis. When we talk about a meshed environment, we have very detailed information about all the different IPSEC tunnels that get constructed in a meshed environment.	18. Click **WAN > Tunnel**.  Interface TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Tunnel Control Connections System Status Events 6 Rows Selected Search Options Down (0) Init (0) Up (8) Tunnel Endpoints — Protoco biz-internet — -- ☑ Branch1-Router1:biz-internet-DC2-Router2:biz-internet — IPSEC ☑ Branch1-Router1:biz-internet-DC1-Router1:biz-internet — IPSEC ☑ Branch1-Router1:biz-internet-DC2-Router1:biz-internet — IPSEC ☑ Branch1-Router1:biz-internet-DC1-Router2:biz-internet — IPSEC mpls — -- ☑ Branch1-Router1:mpls-DC2-Router2:mpls — IPSEC ☑ Branch1-Router1:mpls-DC1-Router2:mpls — IPSEC ☐ Branch1-Router1:mpls-DC1-Router1:mpls — IPSEC ☐ Branch1-Router1:mpls-DC2-Router1:mpls — IPSEC

<table>
<tr><th>DIALOG</th><th>DEMONSTRATION STEPS</th></tr>
<tr><td>

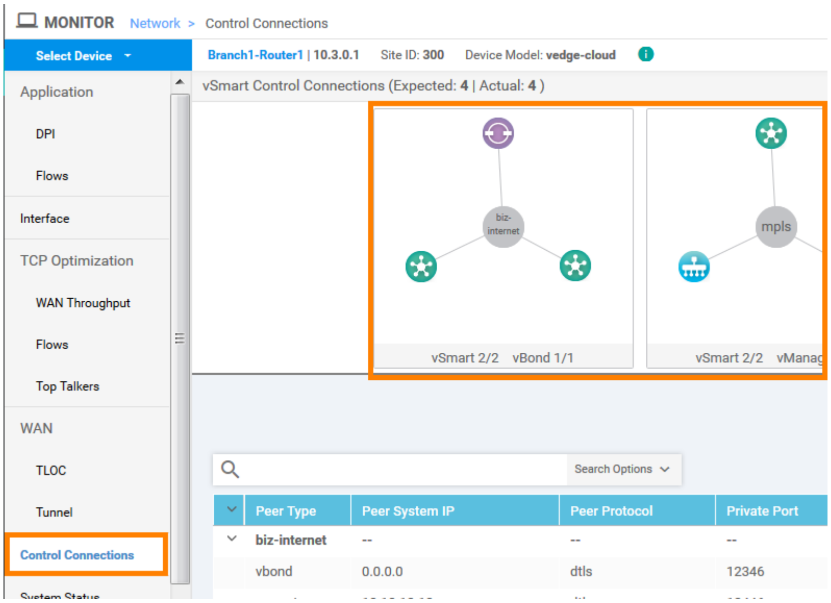
We have visibility into all the different control peers established from an any-edged component.

The number of controlled adjacencies is less than the actual number of IP Sec tunnels because we don't build an adjacency with every other end point. The control plane runs through the edge component and the vSmart controller appliance.

vManage allows you to centrally display all the different connections built across the environment.

</td><td>

19. From the menu, click **Control Connections**.



MONITOR Network > Control Connections

Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud

vSmart Control Connections (Expected: 4 | Actual: 4)

<table>
<tr><th></th><th>Peer Type</th><th>Peer System IP</th><th>Peer Protocol</th><th>Private Port</th></tr>
<tr><td>⌄</td><td>biz-internet</td><td>--</td><td>--</td><td>--</td></tr>
<tr><td></td><td>vbond</td><td>0.0.0.0</td><td>dtls</td><td>12346</td></tr>
</table>

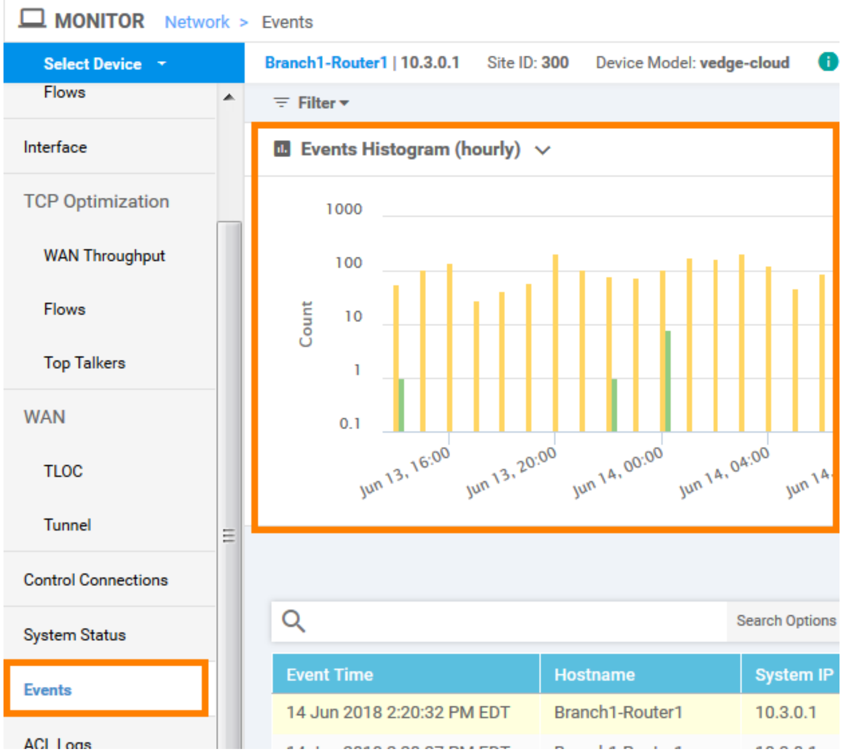
</td></tr>
<tr><td>

We also have full visibility into every real time event.

vManage is an event recipient for every single thing that happens over the network. Changes to tunnels or the quality of tunnels are recorded, as are events where the traffic is redirected to improve the quality of the flow.

</td><td>

20. From the menu, click **Events**.

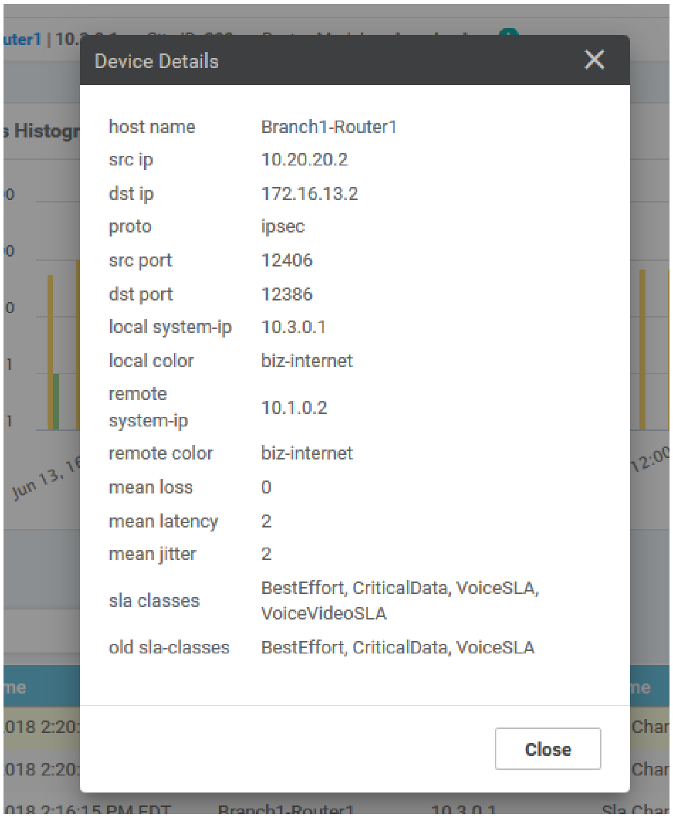
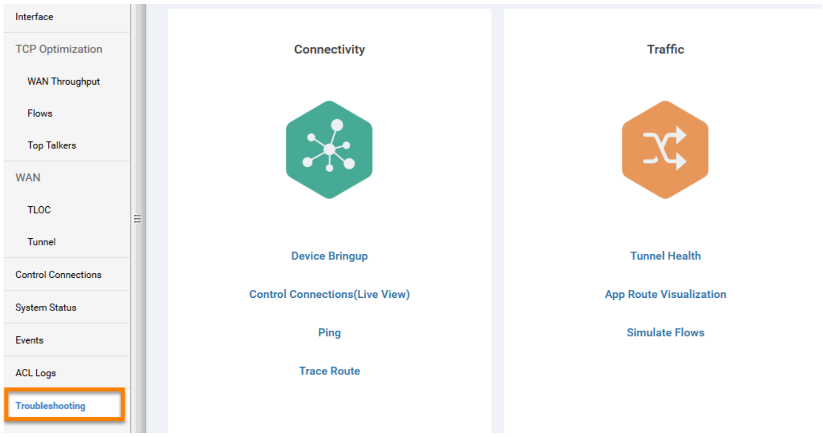


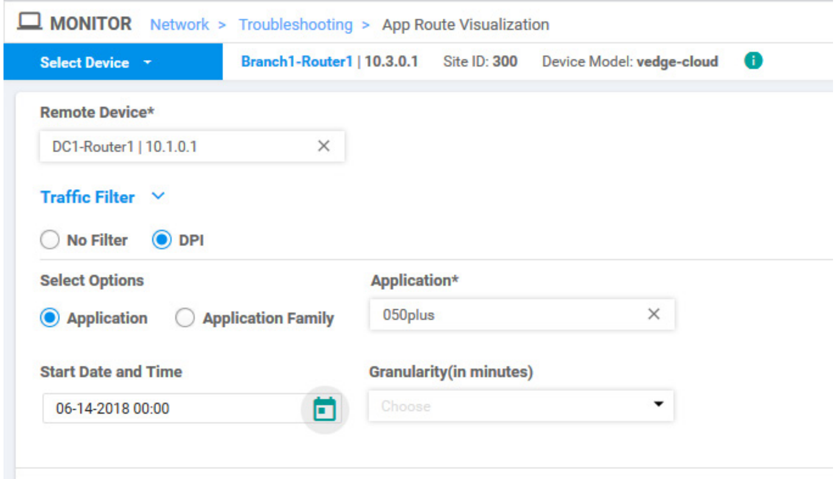
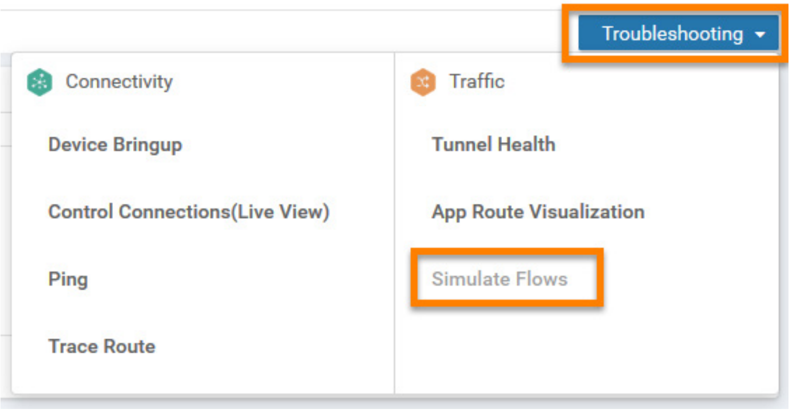
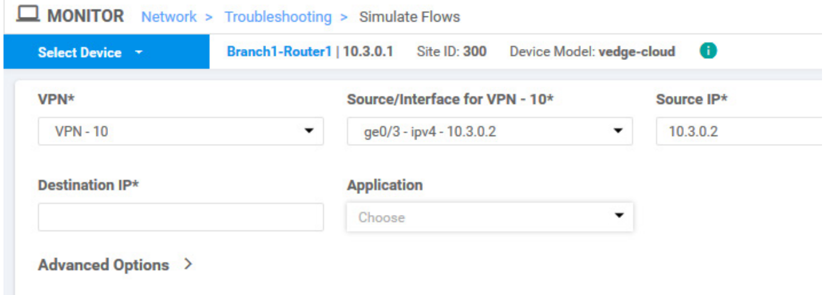
MONITOR Network > Events

Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud

<table>
<tr><th>Event Time</th><th>Hostname</th><th>System IP</th></tr>
<tr><td>14 Jun 2018 2:20:32 PM EDT</td><td>Branch1-Router1</td><td>10.3.0.1</td></tr>
</table>

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

DIALOG	DEMONSTRATION STEPS
	21. Click the three dots next to an **Event Time** and select **Device Details.** 22. Click **Close.**  Device Details host name Branch1-Router1 src ip 10.20.20.2 dst ip 172.16.13.2 proto ipsec src port 12406 dst port 12386 local system-ip 10.3.0.1 local color biz-internet remote system-ip 10.1.0.2 remote color biz-internet mean loss 0 mean latency 2 mean jitter 2 sla classes BestEffort, CriticalData, VoiceSLA, VoiceVideoSLA old sla-classes BestEffort, CriticalData, VoiceSLA
vManage, from an assurance perspective, provides capability to troubleshoot the environment it is managing. It gives you the ability to see what is preventing a device from becoming operational, or diagnosing traffic problems on devices that are operational.	23. From the menu, click **Troubleshooting**.  Interface TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Tunnel Control Connections System Status Events ACL Logs Troubleshooting Connectivity Device Bringup Control Connections(Live View) Ping Trace Route Traffic Tunnel Health App Route Visualization Simulate Flows

DIALOG	DEMONSTRATION STEPS
It allows you to visualize what is occurring for different types of traffic at certain locations. This allows you to get historical data for particular time stamps for the traffic, and the different criteria and transport for the application.	24. Click **App Route Visualization**.  MONITOR Network > Troubleshooting > App Route Visualization Select Device ▾ Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud Remote Device*: DC1-Router1 | 10.1.0.1 Traffic Filter: ○ No Filter ● DPI Select Options: ● Application ○ Application Family Application*: 050plus Start Date and Time: 06-14-2018 00:00 Granularity(in minutes): Choose
To troubleshoot even further, you can simulate particular types of flows in real time, by device or BTN segment.	25. Click **Troubleshooting > Simulate Flows**.  Troubleshooting Connectivity Device Bringup Control Connections(Live View) Ping Trace Route Traffic Tunnel Health App Route Visualization Simulate Flows
This gives you an accurate measurement of what is happening for a type of application, between certain endpoints, over certain ports, with specific types of markings. So from vManage, we get centralized management of all our policies, the ability to monitor and trigger off of all the different things that may be occurring in the environment, and a launch point for detailed analytics.	 MONITOR Network > Troubleshooting > Simulate Flows Select Device ▾ Branch1-Router1 | 10.3.0.1 Site ID: 300 Device Model: vedge-cloud VPN*: VPN - 10 Source/Interface for VPN - 10*: ge0/3 - ipv4 - 10.3.0.2 Source IP*: 10.3.0.2 Destination IP*: Application: Choose Advanced Options >

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**