Pervasive Network Monitoring with DANZ Monitoring Fabric

Table of contents

Introduction

Digital transformation, in today's landscape, is key to an organization's competitive advantage. As organizations have embarked on this digital transformation journey, it has led not only to an exponential growth of their datacenters' size, bandwidth and traffic, but also uncovered a paramount need for pervasive network observability to ensure performance, security and integrity of their datacenters. As security threats continue to increase, ensuring application performance meets the needs of the business is critical.

To gain comprehensive visibility into their network, network and security operators deploy Network Packet Brokers (NPB) as well as tools such as Network Performance Monitoring, Intrusion Detection System, Application Performance Monitoring, Packet Capture Devices, User Experience Monitoring, Compliance Monitoring etc. Traffic from TAP/SPAN ports of production switches and routers is ingested by a set of NPBs, where L2-L4 filters are applied to the traffic and then it is replicated, and/or load balanced to the one or more tools connected to the NPBs.

However, the traditional "box-by-box" management approach, based on expensive, legacy, proprietary NPBs, has proven to be challenging to scale and is operationally complex for today's organization-wide monitoring. Fundamentally, the legacy NPB is still a series of pipes getting packets to tools, without providing any additional insight about the production workloads.

DANZ Monitoring Fabric (DMF) provides a highly differentiated approach to network observability. DMF is a next-generation visibility fabric that provides pervasive organization-wide network observability to enable efficient end-to-end IT troubleshooting workflows for physical, virtual and cloud workloads via a single pane of glass. DMF, in addition to basic NPB functions, such as shipping packets from the production network to performance and security tools, also provides insight into what is happening on the network. With its integration with DMF Recorder Node and DMF Analytics Node, DMF delivers high-performance packet recording, querying and replay functions, and unprecedented real-time/historical contextual visibility to monitor, discover, troubleshoot and predict network and application performance issues as well as accelerate root cause of security breach discovery, respectively. DMF leverages a pair of centralized HA controllers, which treat the entire NPB fabric (using merchant-silicon switches and industry-standard servers) as one. This architecture provides the foundation for a scale-out, cost-effective NPB and lends itself to provide a single point of visibility across the entire environment. With DMF's modern GUI as well as a REST-API powered multi-tenant architecture, different teams, whether DevOps, NetOps or SecOps can simultaneously (and securely) use the DMF's infrastructure (Monitoring-as-a-service) without impacting the other users.

DMF provides the following key benefits:

- Superior Scale-Out Architecture: Pervasive East-West and North-South Visibility for the Datacenter
- Integrated Intelligent Visibility: Enables contextual and Predictive Analytics for the Datacenter workloads
- Simplified Network Time Machine: Faster troubleshooting with integrated packet capture, querying and replay functions
- Optimized CapEx/OpEx: Single SDN-driven operations dashboard and Ethernet price/performance

This solution guides discusses:

- DMF components
- Hardware and Software Options
- Connectivity
- Installation and Bring up
- Zero Touch Fabric
- Policy workflow
- Remote site monitoring
- Managed Services
- Virtual Monitoring

DMF Components

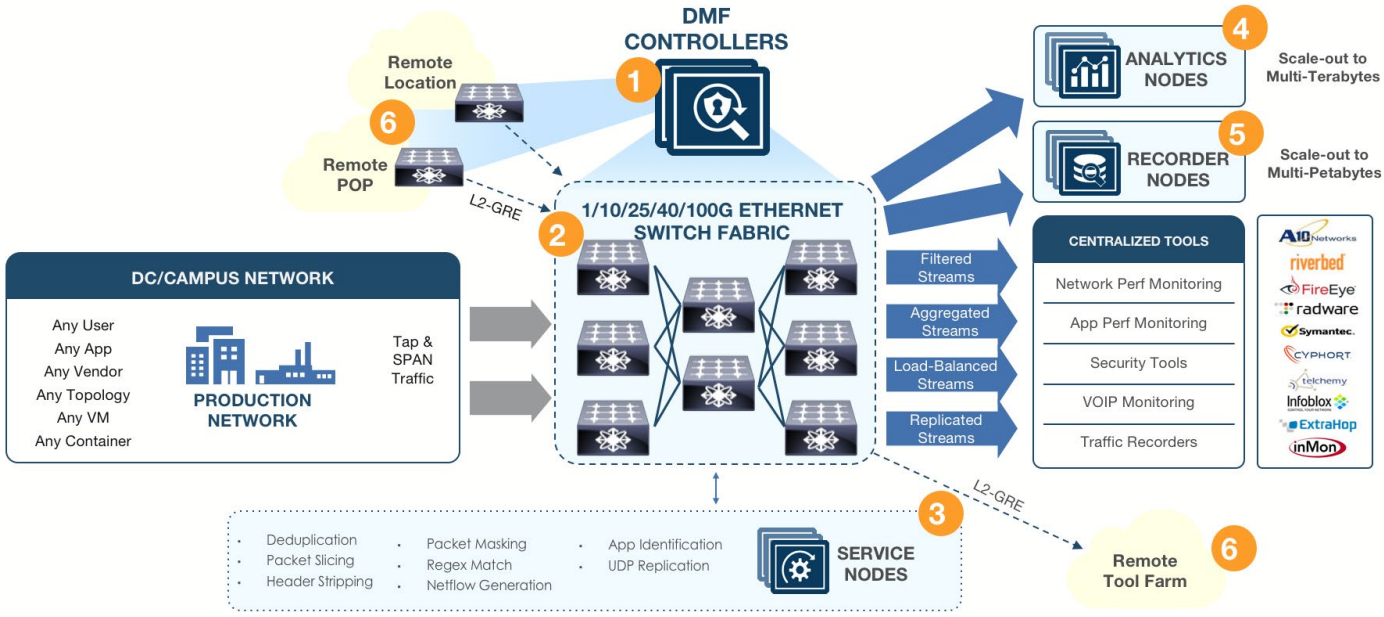

Figure 1: DMF architecture

Hardware and Software Options

Following are the hardware and software components required for this solution:

Component	Hardware/Software
DMF Controller (HA Pair)	Hardware Appliance or Virtual Instance
DMF Switch (es)	Ethernet switches (1G, 10G, 25G, 40G, 100G) with software licenses
Smart Node(s)	
Service Node (s)	Hardware Appliance (40G, 160G, 320G)
Recorder Node (s)	Hardware Appliance (192TB storage)
Analytics Node(s)	Hardware Appliance

Connectivity Diagram

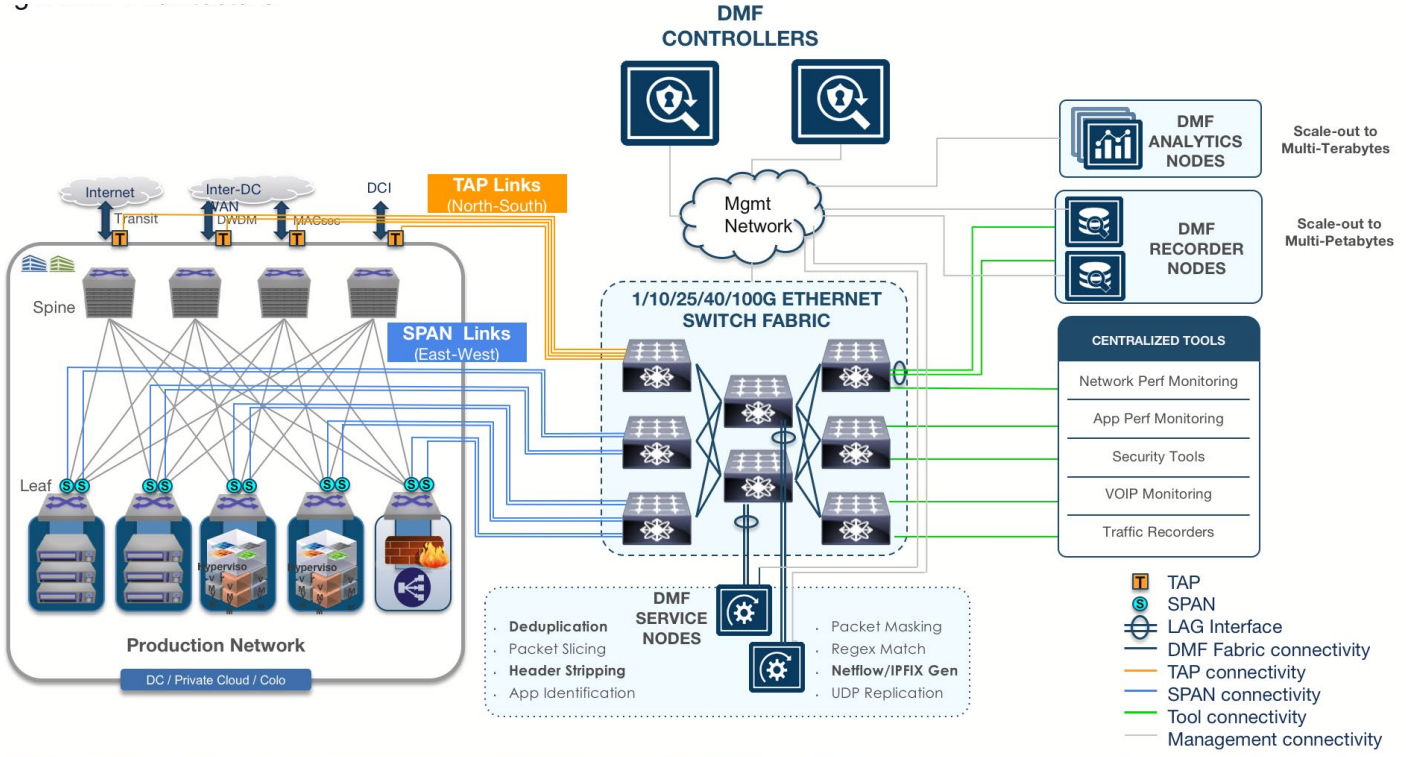

Figure 2: DMF architecture

Installation and Bring up

1. Install the DMF controller software on the appliance or launch a VM instance. (Refer to the DMF Deployment Guide)
2. Configure the IP address for the DMF controller.
3. Connect the data plane ports of the switches together in desired topology ex. Filter-Delivery (Leaf-Spine), Filter-Core-Delivery (Leaf-Spine-Leaf). Switch interconnection links are referred to as core links.
4. Connect Service Node to the Core layer switch.
5. Connect Recorder Node to the Delivery layer switch.
6. From Controller GUI or CLI, select the deployment mode of the fabric.

Zero Touch Fabric

Modern data centers require intelligent, agile, flexible and secure monitoring architecture that provides a single pane of glass management, zero-touch scale and automation. DMF controller achieves these with Zero Touch Networking (ZTN).

DMF controller automatically discovers all switches, Service Nodes, and Recorder Nodes. No user configuration is required on switches or smart nodes.

When all components for DMF fabric, such as Controller, Service Node, Recorder Node and switches are in the same subnet, deployment mode on the controller should be configured as Auto-Discovery. Discovery process for all components is accomplished via L2ZTN process as follows:

1. Once the switches and smart nodes bootup, a discovery message is sent with IPv6 link-local address to IPv6 multicast group.
2. The DMF controller listens on the IPv6 multicast address group.
3. Controller populates the MAC addresses of switches and smart nodes which is then presented to the user as shown in Fig. 3

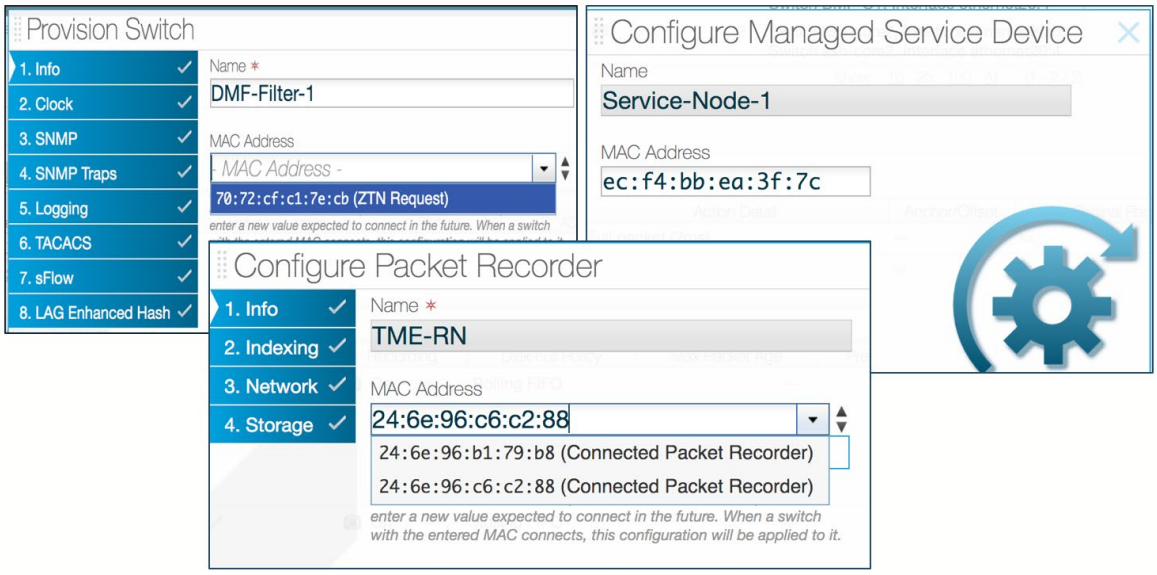

Figure 3: Switch, Service Node, and Recorder Node MAC discovery

Once MAC addresses of switches, Service Nodes and Recorder Nodes are registered in the DMF controller, it pushes the appropriate software image to each node. Configurations, such as SNMP, Logging, Clock etc. are pushed to each node automatically.

Using LLDP message exchange between switches and smart nodes, the controller discovers the datapath, so there is no need for any configuration by the user.

Devices connected to DMF Filter interface via TAP or SPAN ports are also discovered by the controller, if the production devices are exchanging CDP/LLDP messages as displayed in Fig. 4.

Connected Devices

UNIQUE DEVICE NAMES

Click a device name to filter Interfaces table below.

ASH-SN (2) TME-BMF (1) TME-RN2 (1)
bsn-tme-agg (2) TME-PR (1) TME-SN (4)
localhost (5)

SWITCH INTERFACES

Filter table rows FILTER

DMF Switch	DMF Interface	Device Name	Device Description	Chassis ID	Port ID	Port Description	Management Address	Protocol
ash-core2	ethernet20:3	ASH-SN	dmf-service-node	24:6e:96:0c:b2:08	2	sni2	10.111.35.12	LLDP
ash-core2	ethernet20:4	ASH-SN	dmf-service-node	24:6e:96:0c:b2:08	1	sni1	10.111.35.12	LLDP
ash-Sw1-F1	ethernet18	bsn-tme-agg	Arista Networks EOS version 4.13.5F running on an Arista Networ	00:1c:73:10:99:68	Ethernet18	—	10.2.18.8	LLDP
ash-Sw1-F1	ethernet30	localhost	VMware ESX Releasebuild-8169922	vmnic0	44:a8:42:35:02:0c	port 16 on dvSwitch Mgmt-vDS (cswitch)	—	LLDP
BMF-C1	ethernet26:1	TME-SN	dmf-service-node	ec:f4:bb:ea:3f:7c	3	sni3	10.111.35.112	LLDP
BMF-C1	ethernet26:2	TME-SN	dmf-service-node	ec:f4:bb:ea:3f:7c	4	sni4	10.111.35.112	LLDP
BMF-C1	ethernet26:3	TME-SN	dmf-service-node	ec:f4:bb:ea:3f:7c	1	sni1	10.111.35.112	LLDP
BMF-C1	ethernet26:4	TME-SN	dmf-service-node	ec:f4:bb:ea:3f:7c	2	sni2	10.111.35.112	LLDP
BMF-D1	ethernet1	—	—	3c:fd:fe:50:97:63	3c:fd:fe:50:97:63	—	—	LLDP
BMF-D1	ethernet25	localhost	VMware ESX Releasebuild-8169922	vmnic4	a0:36:9f:73:0b:5c	port 13 on dvSwitch Compute-vDS (cswitch)	—	LLDP
BMF-D1	ethernet3	localhost	VMware ESX Releasebuild-8169922	vmnic1	44:a8:42:35:02:0d	port 8 on dvSwitch Compute-vDS (cswitch)	—	LLDP
BMF-D1	ethernet36	localhost	VMware ESX Releasebuild-8169922	vmnic0	44:a8:42:35:02:0c	port 16 on dvSwitch Mgmt-vDS (cswitch)	—	LLDP
BMF-D1	ethernet39	TME-RN2	dmf-recorder-node, SN 132DCP2	24:6e:96:b1:79:b8	f8:f2:1e:1e:15:e0	enp59s0f0	10.111.35.98	LLDP
BMF-D1	ethernet40	TME-BMF	dmf-controller-packet-capture, SN GR58V52	a0:36:9f:78:26:fc	enp5s0f0	—	—	LLDP
BMF-D1	ethernet48	TME-PR	dmf-recorder-node, SN G5HGHQ2	24:6e:96:c6:c2:88	f8:f2:1e:32:81:70	enp59s0f0	10.111.35.99	LLDP
BMF-F1	ethernet17	bsn-tme-agg	Arista Networks EOS version 4.13.5F running on an Arista Networ	00:1c:73:10:99:68	Ethernet17	—	10.2.18.8	LLDP
BMF-F1	ethernet2	localhost	VMware ESX Releasebuild-8169922	vmnic1	44:a8:42:35:02:0d	port 8 on dvSwitch Compute-vDS (cswitch)	—	LLDP
BMF-F1	ethernet25	—	—	3c:fd:fe:a5:62:08	3c:fd:fe:a5:62:08	—	—	LLDP
BMF-F1	ethernet26	—	—	3c:fd:fe:a5:62:09	3c:fd:fe:a5:62:09	—	—	LLDP
BMF-F1	ethernet27	—	—	3c:fd:fe:a5:62:0a	3c:fd:fe:a5:62:0a	—	—	LLDP
BMF-F1	ethernet28	—	—	3c:fd:fe:a5:62:0b	3c:fd:fe:a5:62:0b	—	—	LLDP

Figure 4: Production devices connected to DMF switch fabric

Policy Workflow (Traffic Steering)

Most data centers deploying monitoring and security tools use Network Packet Broker (NPB) to deliver real time visibility into the network. NPBs filter and forward desired traffic to the monitoring and security tools, so tools are only ingesting relevant data.

DANZ Monitoring Fabric helps achieve pervasive network visibility into the network by ingesting traffic from network TAP/SPAN ports, filtering, and delivering the traffic to tools connected anywhere in the fabric via policy workflow.

TAP/SPAN ports which are connected to DMF switch are given the role of Filter interfaces as shown in Fig. 5.

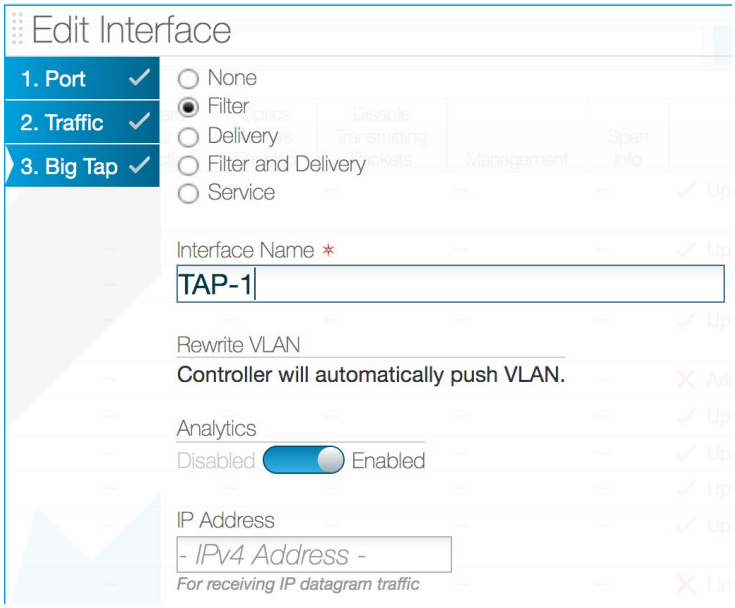

Figure 5: Role assignment to port connected to TAP/SPAN port

Similarly, DMF switch ports which are connected to tools are assigned the role of Delivery interface as shown in Fig. 6.

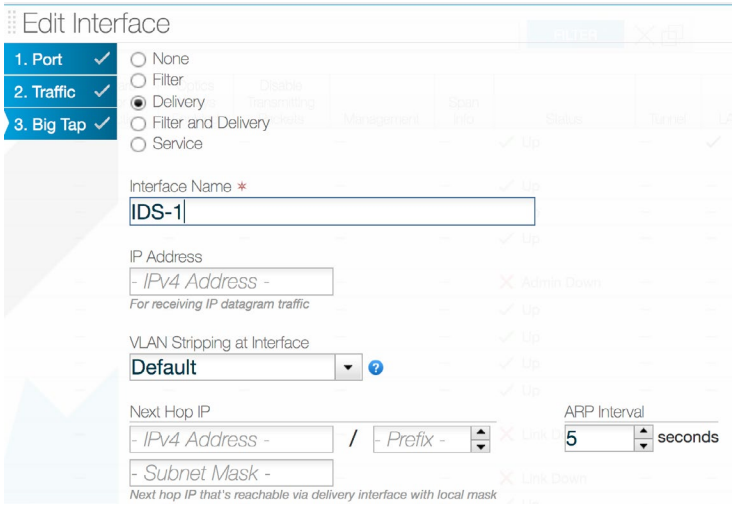

Figure 6: Role assignment to port connected to tools

After roles for the interfaces on DMF switches have been assigned, users can create Policy to forward traffic from Filter interfaces to Delivery interfaces.

Policy workflow:

1. Access the Policies page from the BigTap tab. Big Tap Policies page lists all policies along with the configuration state.
2. The Create Policy window pops up when the user clicks on the + button as shown in Fig 7. Enter the following information on Create Policy --> Info page
   c. Name: Specify alpha-numeric name for policy, which will uniquely identify the policy.
   d. Priority: Specify the policy priority. By default, each policy gets a priority of 100.
   e. Action: Action determines whether traffic is to be forwarded, dropped, or captured. For Packet Capture action, the packet capture interface of the controller must be connected to one of the DMF switch data ports. (Note: Packet Capture is only for quick troubleshooting and not meant for recording packets at line rate or long-term storage.)
   f. Scheduling: Policy Scheduling is used to configure the policy start time. By default, policy starts immediately, but it can be set to start after a delay of specified minutes or at specified date and time.
   g. Run Policy: By default, policy is set to run Always, but the user has the option to configure the policy runtime in minutes.

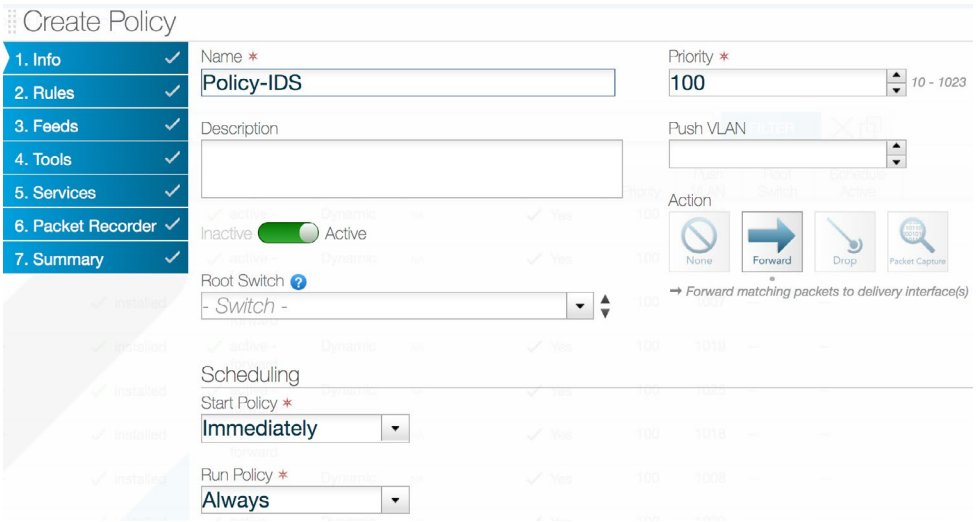

Figure 7: Policy Creation

3. Rules: To filter traffic, rules have to be specified. These rules determine traffic that is to be forwarded or dropped by policies to tools. DMF supports L2-L4 filtering. Shortcuts to most commonly used rules are listed on the Rules tab as shown in Fig. 8.

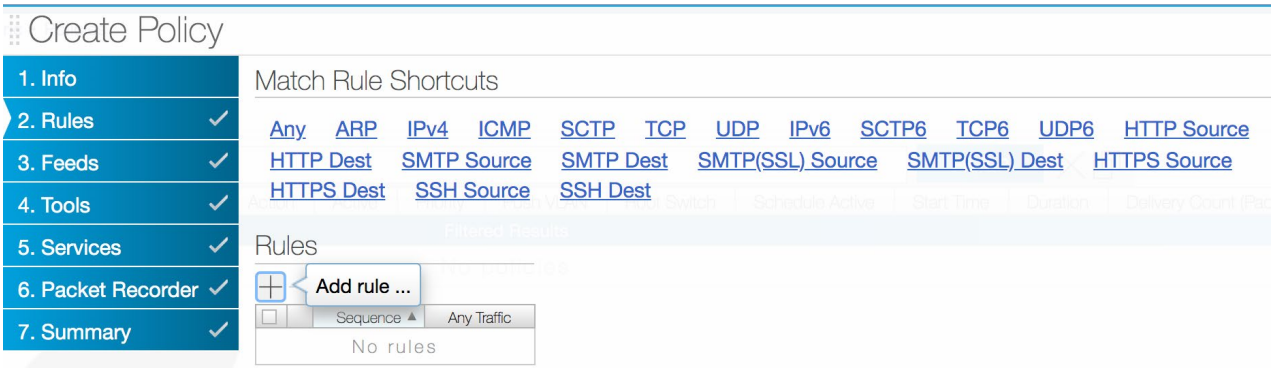

Figure 8: Policy Rules for traffic filtering

4. Feeds: Feeds for the traffic for Policy are the Filter interfaces to which TAP/SPAN ports are connected.
5. Tools: Final step to creating a Policy is to specify the Delivery interfaces where tools are connected.

Policy workflow remains the same whether it is a single tier fabric with 1 switch or 3-tier topology (Filter-Core-Delivery) with 100 switches. DMF controller calculates and establishes the data path from Filter interface to Delivery interface. In case of a link or a device failure between Filter switch and Delivery switch, controller will reroute the traffic for impacted policies to alternate path provided switch fabric has redundancy built in (i.e. Leaf-Spine architecture).

Remote Site Monitoring

To get traffic visibility at remote sites, network operators typically deploy switches at remote sites and tunnel the traffic over to the data center where tools are located. DMF provides remote site visibility via L2GRE tunneling between remote DMF switch and local DC DMF fabric as shown in Fig. 9. Also, traffic from data center DMF fabric can be forwarded to remote tool farms by utilizing L2GRE tunneling.

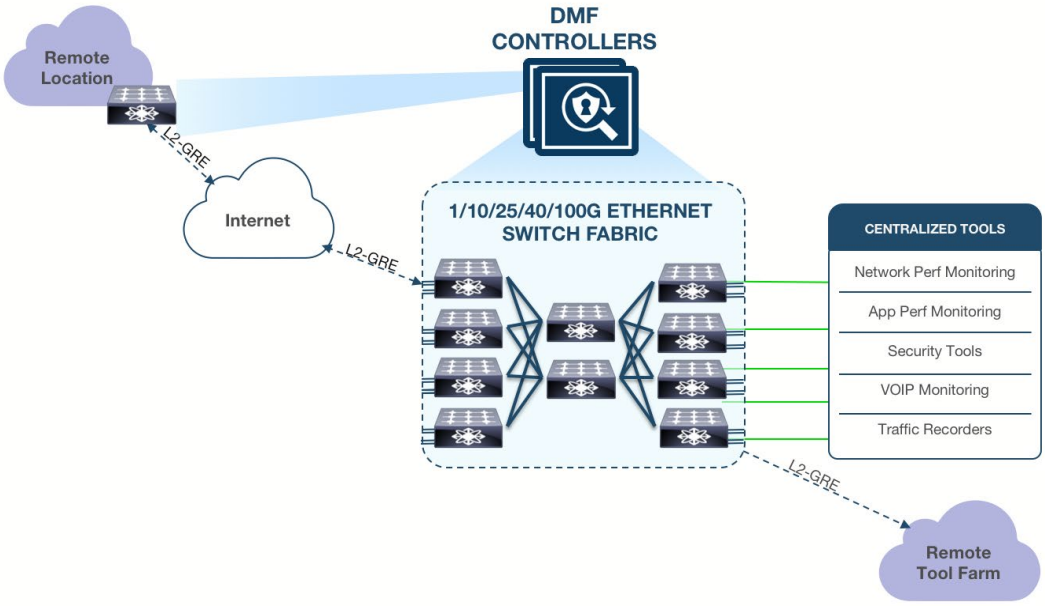

Figure 9: Remote site monitoring

L2GRE tunnel is created on the DMF switch interface which is connected to L3 switch or router. To configure L2GRE tunnel follow the steps:

1. Access the Create Tunnel menu from the Fabric --> Interfaces page.
2. On Configure GRE Tunnel wizard as shown in Fig. 10, populate the required parameters as follows:
   a. Name: Alpha-numeric name to identify the tunnel interface.
   b. Direction: Choose the directionality of the tunnel. If traffic is to be sent to a remote tool farm, select transmit only tunnel. To get traffic from remote sites to data center DMF fabric, use bidirectional tunnel.
   c. Specify the source IP, destination IP and gateway
   d. Select the switch
   e. Select the Parent Interface on which to create a tunnel. This interface should be connected to the L3 switch or router.
   f. Loopback Interface: Select a loopback port. This is required for bidirectional and transmit tunnels. Loopback interface should be any unused physical port on the switch which is configured for MAC loopback.
   g. GRE Decap Keys: Specify the GRE decap key for the tunnel. The key value should be the same for both endpoints of the tunnel.

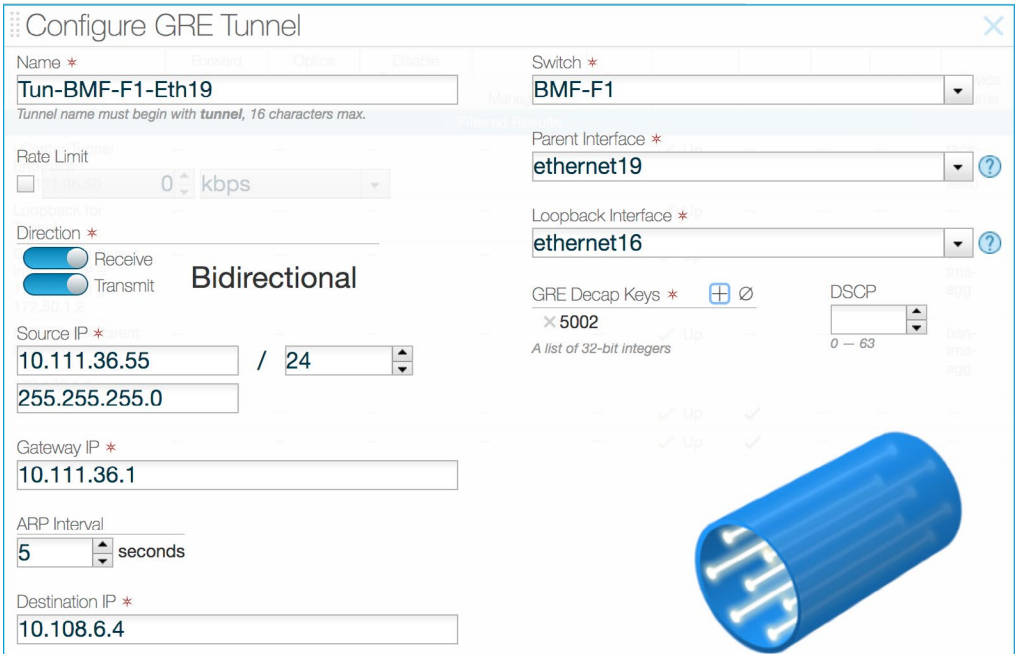

Figure 10: Tunnel creation

For remote site monitoring bidirectional tunnels should be used. After a bidirectional tunnel has been created and the interfaces are up, DMF controller will treat the tunnel as a core-link; hence, making the remote site DMF switch as an extension of the data center fabric as shown in Fig. 11. This reduces the complexity of policy creation, since a single policy can be used to get traffic from Filter interfaces residing on remote DMF switch to Delivery interfaces located in data center. Another advantage to using bidirectional tunnels is that if there are multiple tunnels from remote DMF switch to data center fabric, DMF controller will detect those tunnels as separate core links. This provides path redundancy between remote switch and data center fabric. In case of path failure on one of the core-link tunnels, traffic will be routed to another path by DMF controller.

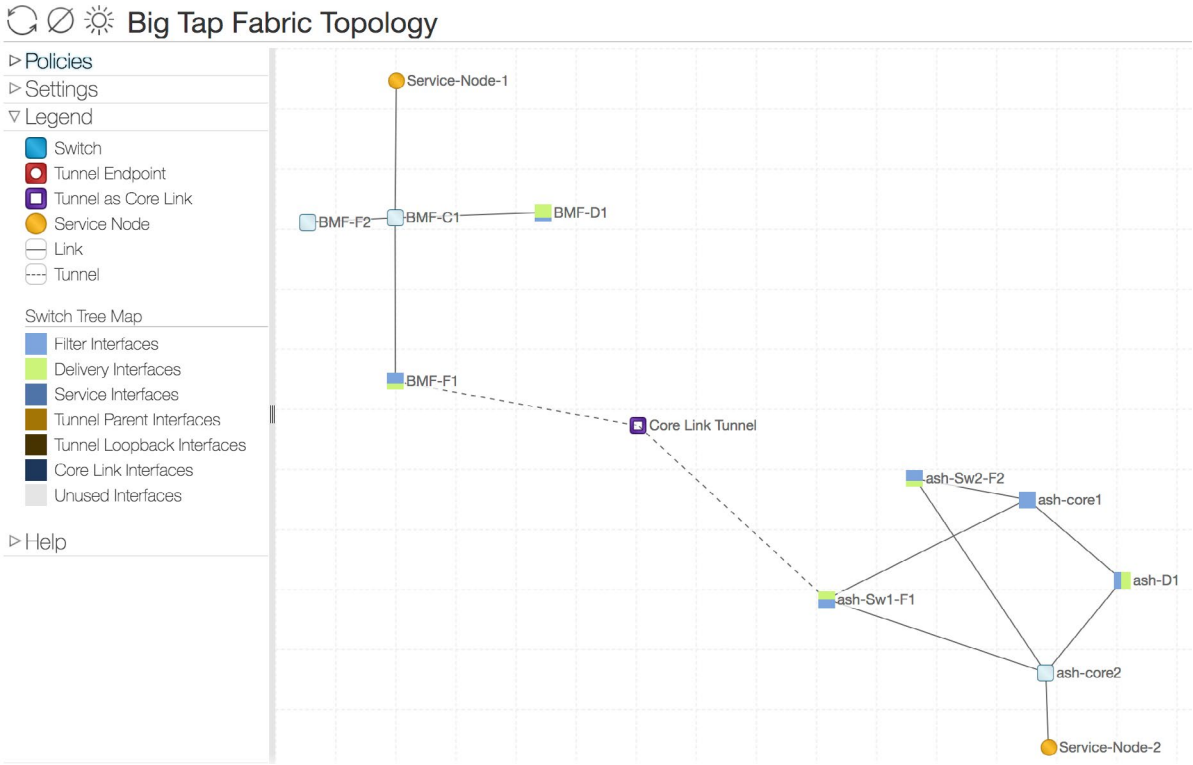

Figure 11: Tunnel as a core link

Managed Services

Packet handling functions, such as traffic aggregation, L2-L4 filtering, packet replication, and tool load balancing are achieved using merchant silicon on DANZ Monitoring Fabric. Advanced packet functions, such as deduplication, slicing, masking, header stripping, etc. are performed on DMF Service Node, since these are not supported on traditional merchant silicon. Service Node is a DPDK-powered, x86-based appliance that connects to the DMF switch fabric (Fig. 12). Service Node comes in 3 form factors:

- Standard 4x10G
- Large: 16X10G
- Extra-Large 16x25G

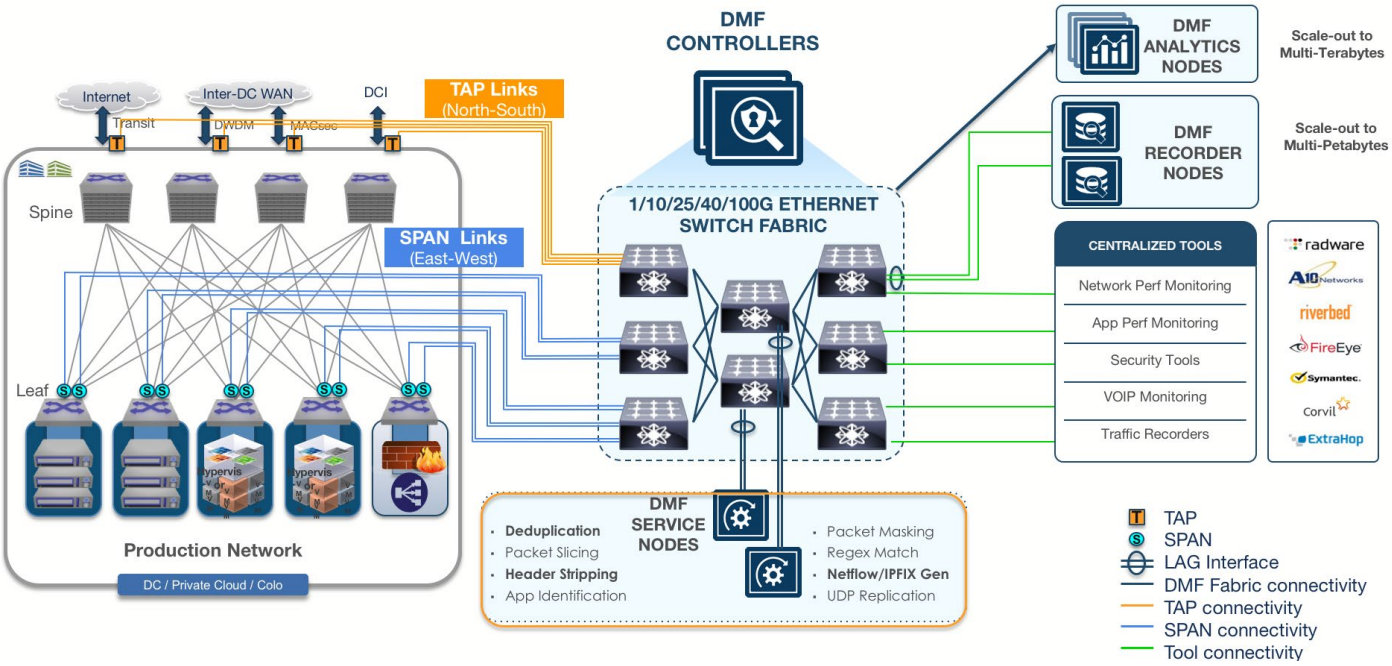

Figure 12: DMF Service Node

Once the Service Node is connected to the DMF switch fabric (Fig. 10) and to the management network, the controller detects the Service Node via LLDP on the data plane. Using ZTN, the controller pushes the correct software image to the Service Node.

- DMF Service Node supports the following services:
- Deduplication
- Packet Slicing
- Header Stripping
- App ID
- Masking
- Pattern Match
- Netflow/IPFIX Generation
- UDP Replication
- GTP Correlation.

One interface of the Service Node can run any one of the services. To achieve scale for any of the services, switch ports to which Service Node interfaces are connected to, can be put in link aggregation group (LAG).

Service on Service Node can be created as follows:

1. From the BigTap menu, access Managed Services page. All the Service Nodes attached to fabric and registered to the controller are displayed here, along with the services which have been created (Fig. 13).

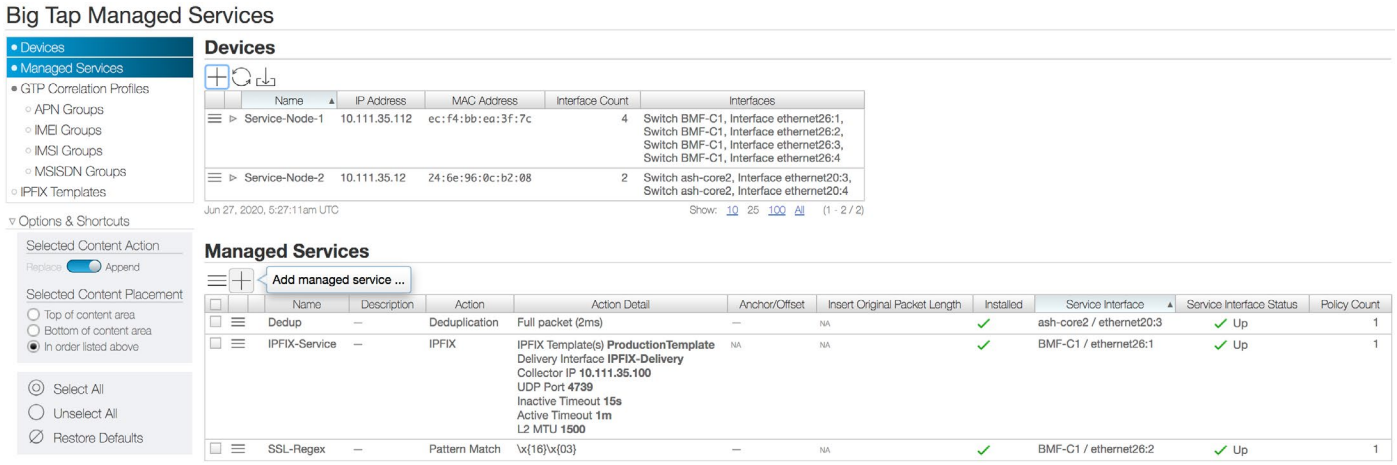

Figure 13: Managed Services page

2. Service can be created from the Managed Services table as shown in Fig. 13.
3. From Create Managed Service page, specify the following as shown in Fig. 14:
   - Alpha-numeric name for the service.
   - DMF switch where Service Node is connected.
   - Interface on which to run the service.
4. Next select the service of interest from the Action drop down menu (Fig. 14) and fill in the required parameters for the service and save the Managed Service.

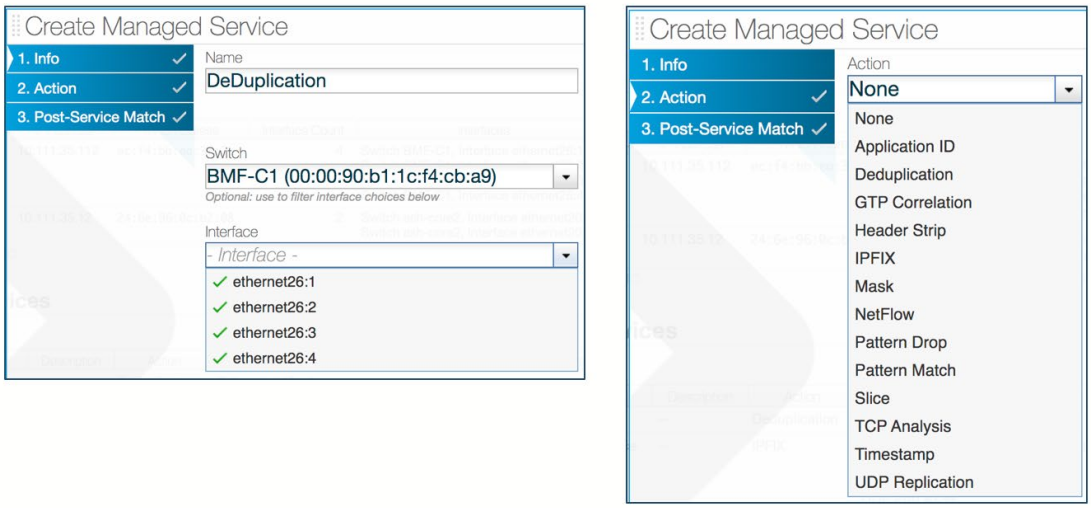

Figure 14: Adding Managed Service

TAP/SPAN traffic, on which service action has to be performed, can be achieved by attaching the configured service to the Policy as shown in Fig. 15.

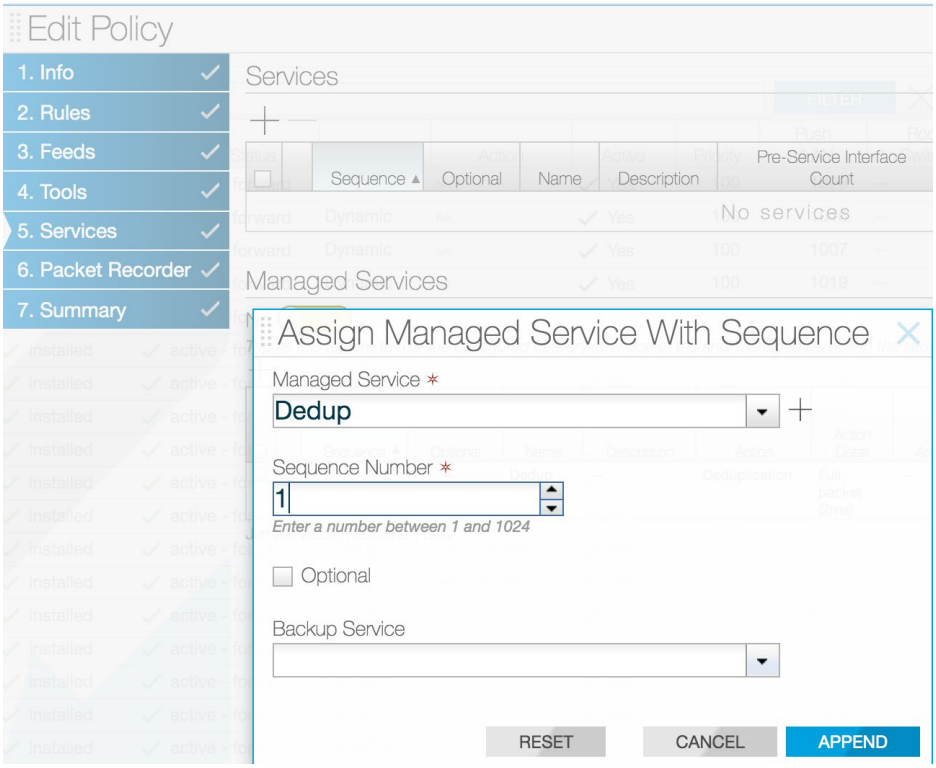

Figure 15: Attach Managed Service to Policy

Once the service is attached to the Policy, traffic from Filter interface is first forwarded to the Service Node, where service action is performed. Data traffic is then forwarded from Service Node to Delivery interface after service action has been performed (Fig. 16).

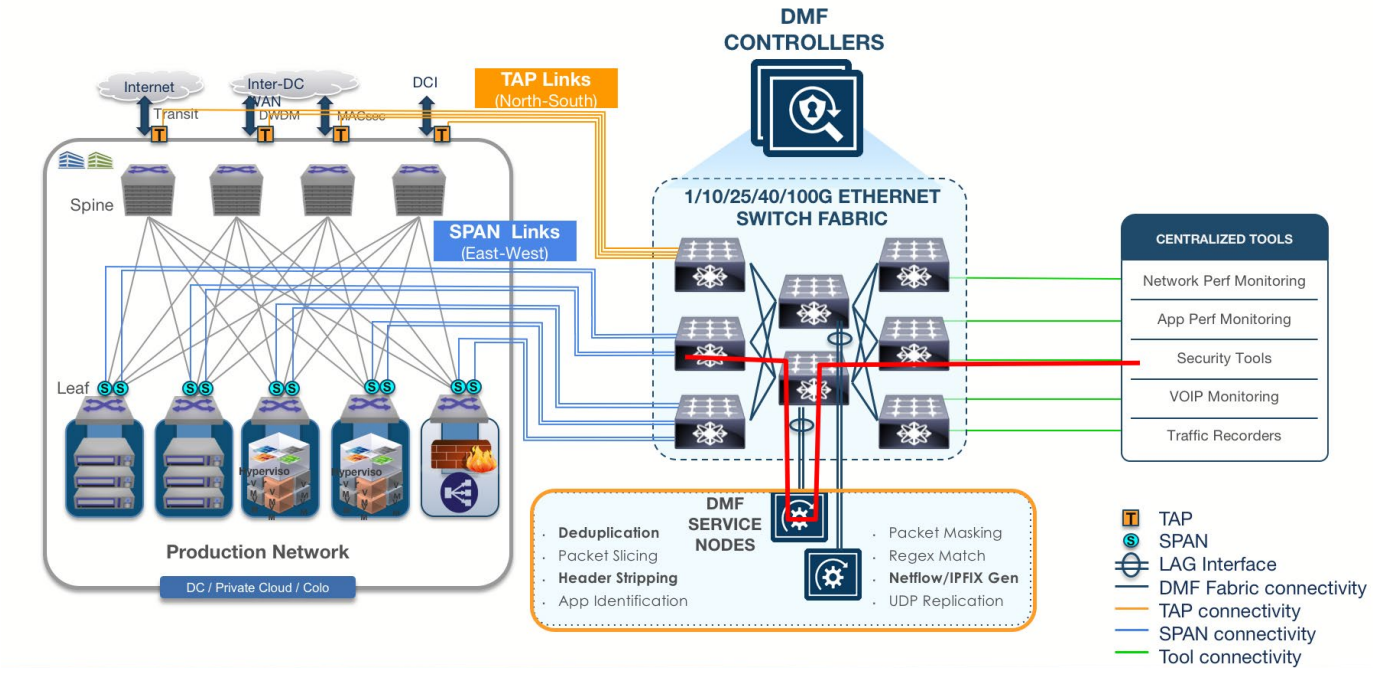

Figure 16: Data path (in red) with service attached to Policy

Virtual Monitoring

Visibility into one's physical network is achieved by monitoring traffic from TAP or SPAN feeds of the production network. So, how does one gain visibility into a virtual environment such as VMware vCenter? Inter host flow visibility between VMs can be achieved by TAP/SPAN of physical switch/router, but what about the intra-host VM to VM communication, where the packet never leaves the ESXi host?

DMF integration with VMware vCenter solves this by providing contextual and flow visibility in VMware virtualized environment. DMF controller provides contextual visibility in VMware virtual environment by leveraging native vSphere APIs. Packet flow visibility is gained by leveraging vDS port mirroring and Encapsulated Remote Mirroring features. For packet flow visibility, DMF provides 2 ways to monitor VM to VM traffic:

1. Option1 SPAN

   With SPAN based monitoring, a port mirror session is created on vDS with a dedicated uplink from host to DMF switch as depicted in Fig. 17.

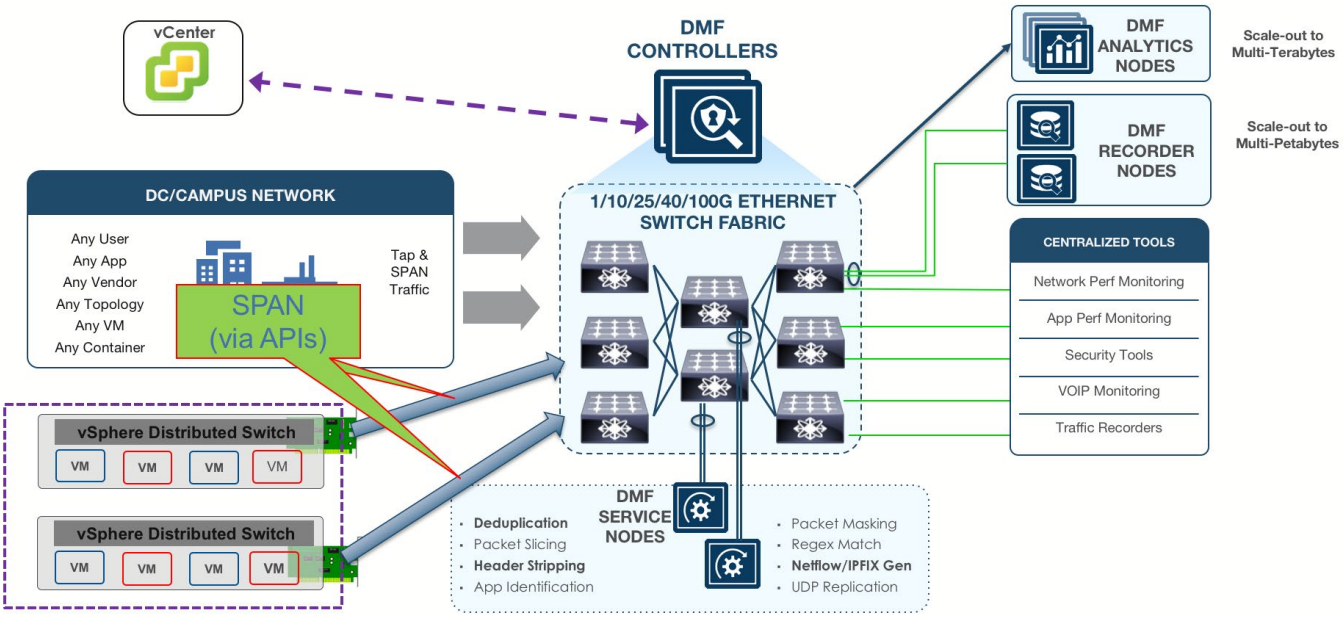

Figure 17: VM traffic visibility with SPAN

2. Option 2 Encapsulated Remote Mirroring.

   With Encapsulated Remote option as mirror type, encapsulated remote mirroring feature on vDS is leveraged to tunnel traffic from VM using L2GRE as shown in Fig 18. Dedicated uplink from ESXi host is not required for this option.

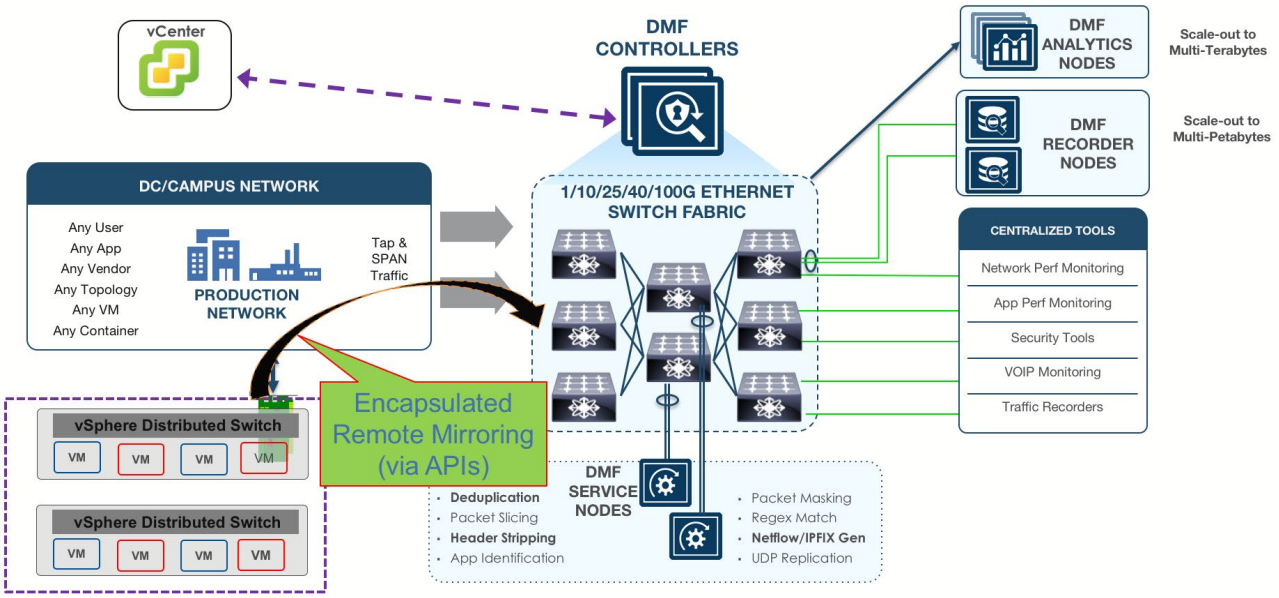

Figure 18 VM traffic visibility with Encapsulated Remote Mirroring

VMware vCenter Integration with SPAN

For continuous monitoring into VMware virtual environment, SPAN monitoring type is recommended. With SPAN monitoring, a dedicated NIC interface from ESXi host is connected to DMF switch interface. Since SPAN monitoring uses a dedicated NIC, production traffic is not impacted.

1. Connect a spare NIC from ESXi host to the DMF switch.
2. LLDP on vDS should be enabled (Fig. 19) with Operation as both. The DMF controller will discover the connected switch interface via LLDP message exchange.

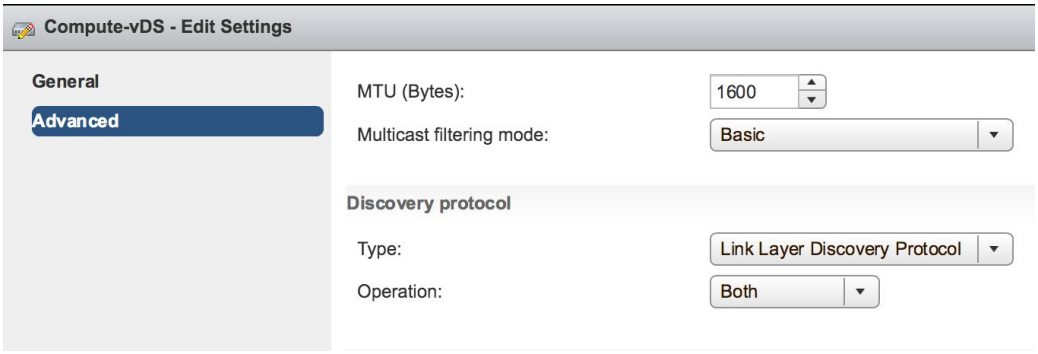

Figure 19: vDS settings to enable LLDP

3. ESXi NIC, which is connected to the DMF switch interface, should not be used for production traffic. To confirm the NIC is not part of active or standby uplinks, access the PortGroup setting from vCenter Networking and move the associated uplink to Unused uplinks as shown in Fig. 20.

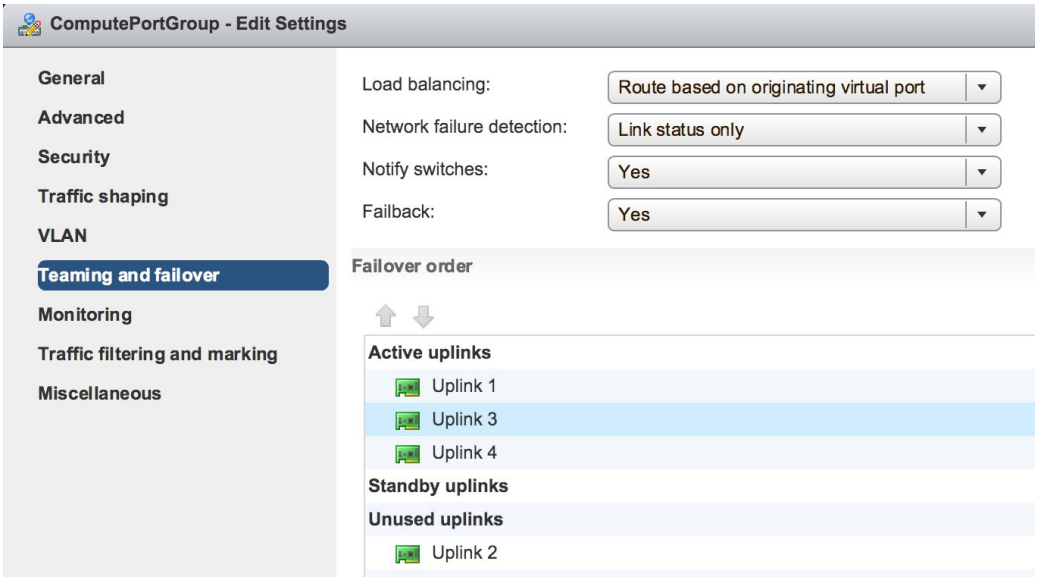

Figure 20: Move uplink used for dedicated SPAN to unused uplinks

4. From DMF controller GUI ,access the VMware vCenter under Integration tab. Add the vCenter and provide the necessary credentials as shown in Fig. 21.

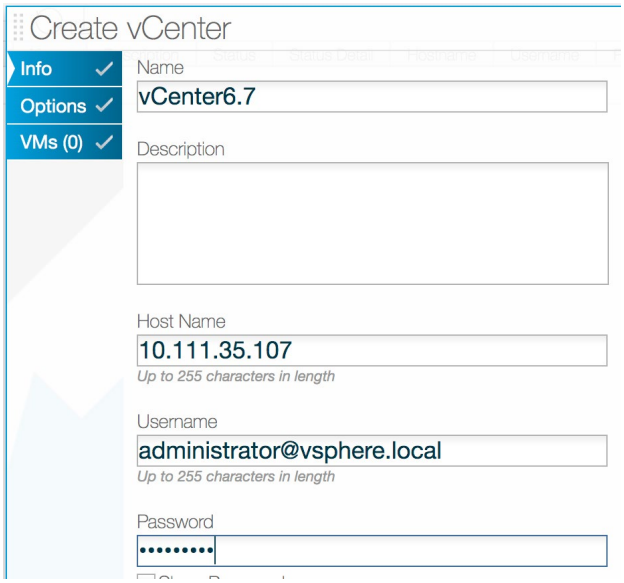

Figure 21: Adding vCenter

5. From the Options tab, select the mirror type, SPAN, and save.

Once the vCenter has been successfully added to the DMF controller, it populates the vCenter inventory via vSphere APIs (Fig. 22).

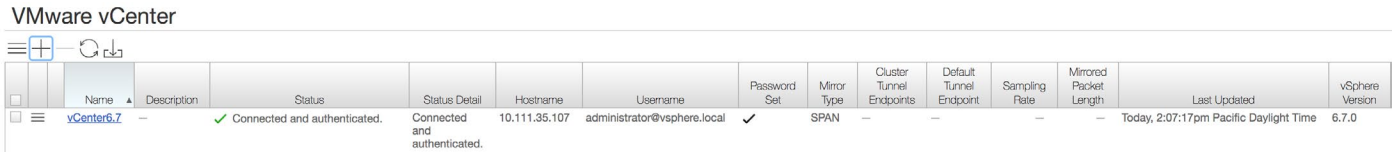

Figure 22: vCenter successfully added to DMF controller

Clicking on the hyperlink of the newly added vCenter takes the user to vCenter inventory page (Fig. 23). vCenter inventory information, such as vCenter version, virtual switches, ESXi hosts, virtual machines etc. are presented to the user.

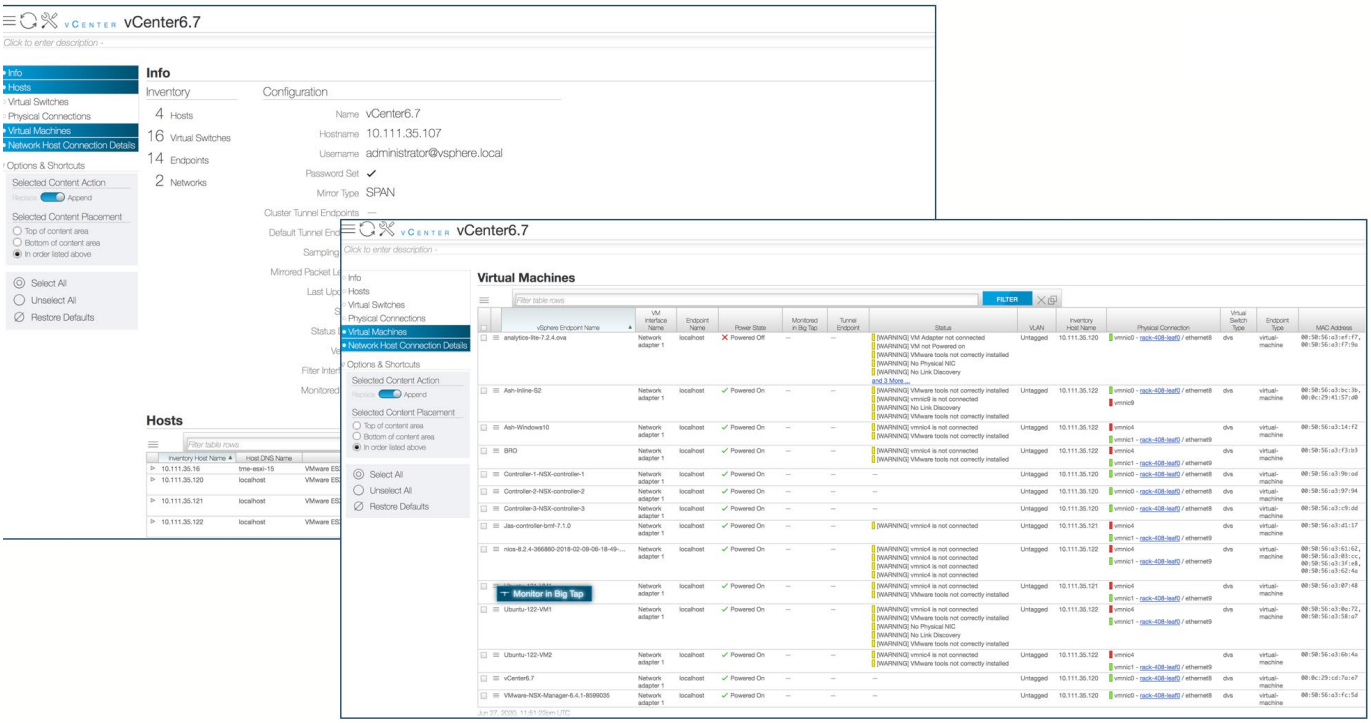

Figure 23: vCenter inventory on DMF controller

To get packet flow visibility for a particular VM, select the VM and start the monitoring session. Once the VM has been selected for monitoring from DMF controller GUI, controller makes an API call to vCenter to create the Remote Mirroring SPAN session on vDS. VM traffic is now spanned from VMware virtual environment to the DMF switch interface (which is connected to ESXi NIC for dedicated monitoring).

Now that packet flow from vCenter vDS is being forwarded to the DMF switch interface Policy can be created. Feed for the Policy would be vCenter (Fig. 24) and Tools would be desired Delivery interfaces to which tools are connected to or remote tool farm.

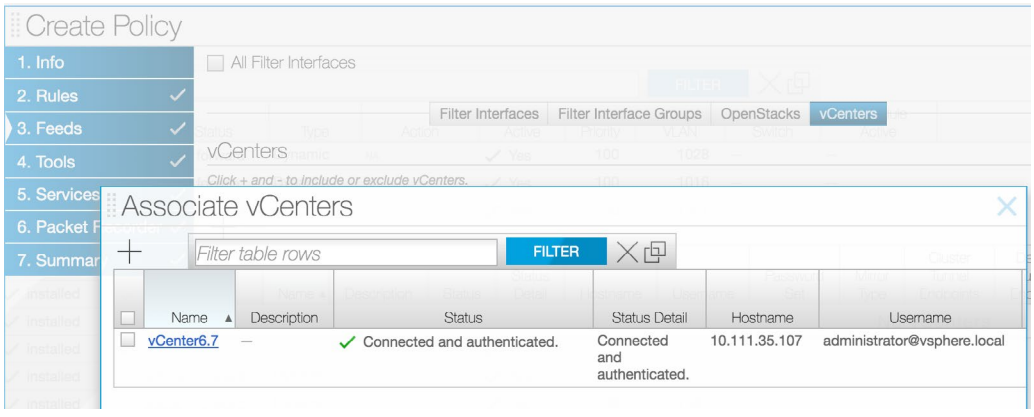

Figure 24: vCenter as Policy feed

VMware vCenter Integration with Encapsulated Remote Mirroring

For dynamic VM monitoring, Encapsulated Remote Mirror type can be used from the DMF controller. Encapsulated Remote Mirroring (ERM) tunnels the packet flow from VMs, which are being monitored over the L2GRE tunnel. L2GRE tunnel is terminated on the DMF switch tunnel endpoint. A DMF switch can terminate a total of 192 receive tunnels.

Create tunnel endpoint as follows:

1. Connect DMF switch interface to a production switch/router that has L3 reachability to vDS on which the VM resides.
2. Tunnel Endpoint is created first by accessing Tunnel Endpoint from the BigTap menu of DMF controller GUI (Fig. 25). Interface for the tunnel endpoint should be a DMF switch interface, which is connected to the production switch/router. Tunnel endpoint interface is where the L2GRE tunnel from vCenter vDS is terminated.

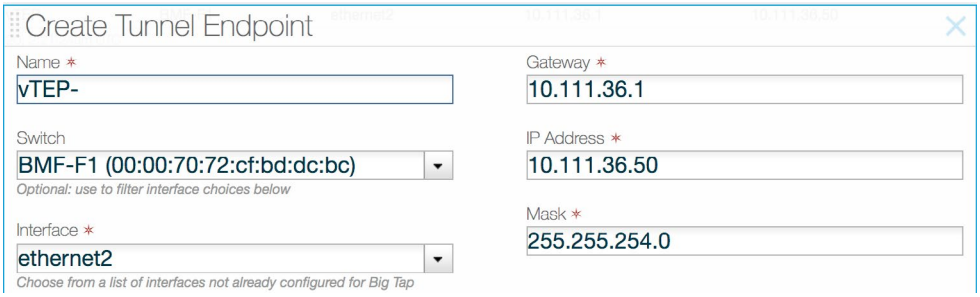

Figure 25: Tunnel Endpoint creation

Register vCenter to DMF controller as follows:

1. From the DMF controller GUI access VMware vCenter under Integration tab. Add the vCenter and provide the necessary credentials as shown in Fig. 21
2. From the Options tab select Encapsulated Remote as Mirror Type (Fig. 26). Select the tunnel endpoint created in step 2 as a Default Tunnel Endpoint or as a Cluster Tunnel Endpoint.
   a. Default Tunnel Endpoint: Receive tunnel interfaces are created for all the ESXi hosts, which are managed by vCenter (Fig 27). Since each DMF switch supports termination of 192 receive tunnels, if vCenter has more than 192 ESXi hosts, then tunnel interfaces for some of the ESXi hosts will not be created. Hence, traffic for those VMs cannot be monitored. Default tunnel endpoint is recommended for vCenters that are managing less than 192 ESXi hosts.

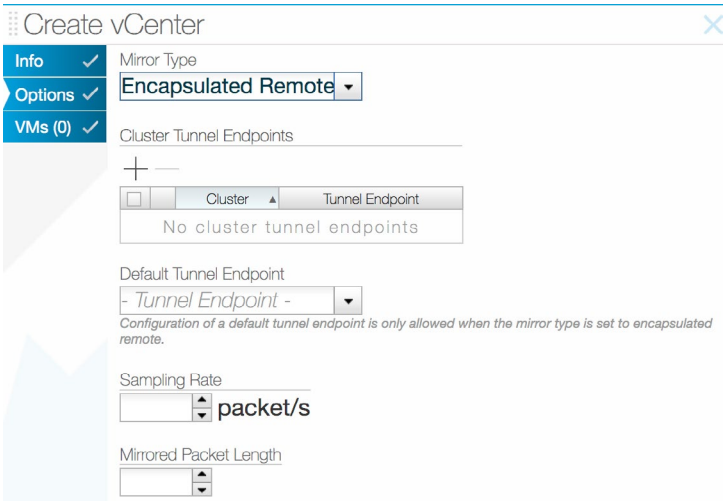

Figure 26: Encapsulated Remote Mirroring options

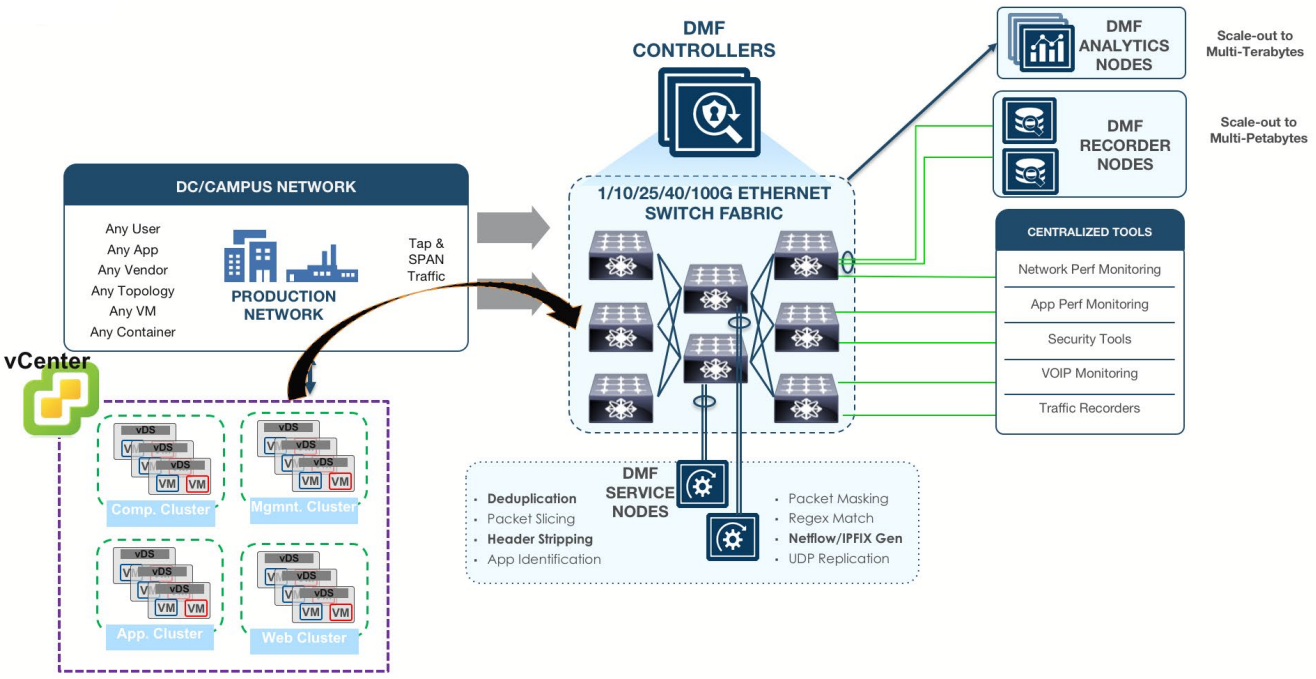

Figure 26: Encapsulated Remote Mirroring options

b. Cluster Tunnel Endpoint: Receive tunnel interfaces are created for each ESXi host which are under the specified vCenter cluster. Tunnels of ESXi hosts from multiple vCenter clusters can terminate on different tunnel endpoints (Fig. 28). These tunnel endpoints can be on different DMF switches. Cluster tunnel endpoint is recommended where vCenter is managing more than 192 ESXi hosts.

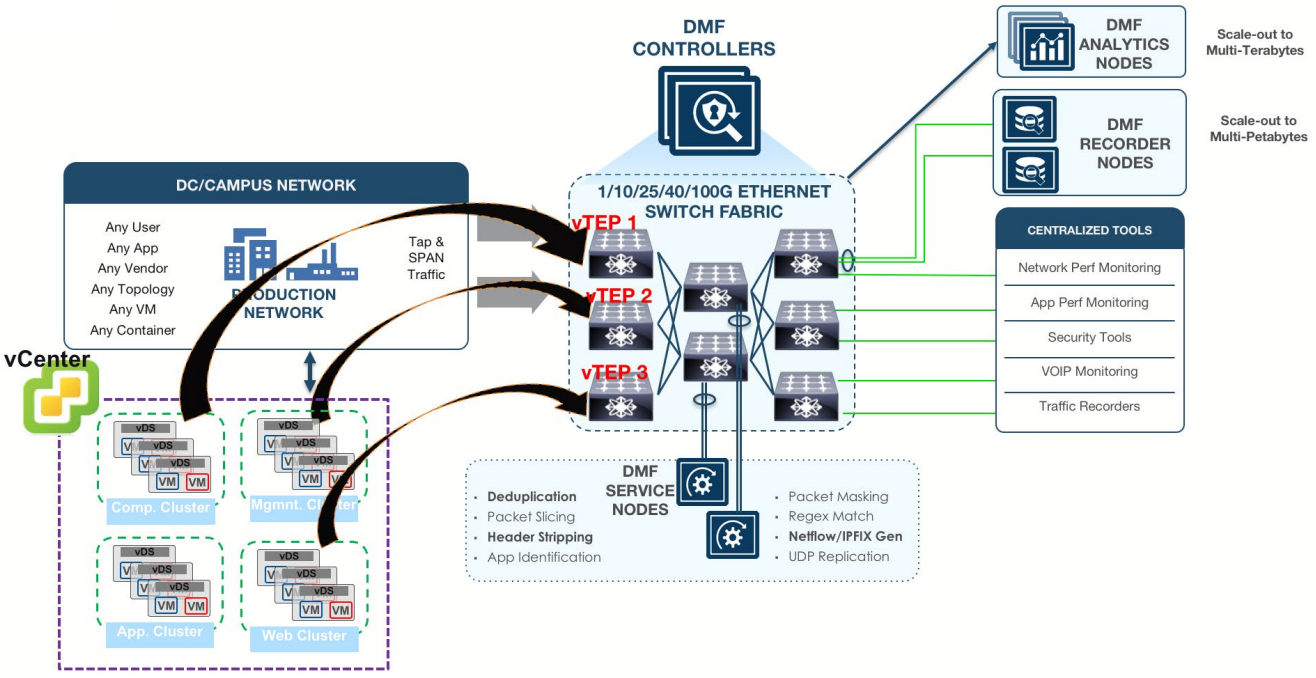

Figure 28: Cluster tunnel endpoint

After vCenter has been successfully added to the DMF controller, virtual Filter Interfaces, which are automatically created by controller, are displayed as shown in Fig. 29. These virtual Filter interfaces are tunnels which correspond to each ESXi host under vCenter or vCenter cluster (depending on the tunnel type selected while adding the vCenter: Cluster Tunnel Endpoint or Default Tunnel Endpoint).

Figure 29: vCenter Integration with Encapsulated Remote Mirror

To get packet flow visibility for a particular VM, user selects the VM and starts the monitoring session. Once the VM has been selected for monitoring from DMF controller GUI, controller makes an API call to vCenter which creates Encapsulated Remote Mirroring session on vDS. Source of the tunnel on vDS is the VM which is being monitored and the destination is the tunnel endpoint. At this point traffic from vDS is tunneled over to the virtual Filter interfaces on the DMF switch.

Now that packet flow from vCenter vDS is being tunneled over to the virtual Filter interface on DMF switch, Policy can be created. Traffic Feed for the Policy is vCenter (Fig. 24), and Tools are desired Delivery interfaces where tools are connected to on DMF fabric or remote tool farm.

By leveraging vSphere APIs, DMF controller provides contextual and packet flow visibility to VMware virtual environment with agentless architecture. Visibility into the virtual environment is maintained even when a VM migrates from one ESXi host to another via vMotion.

Technical Resources

DANZ Monitoring Fabric (DMF) - https://www.arista.com/en/products/danz-monitoring-fabric

Hands on lab: https://dmf-labs.arista.com

Conclusion

Pervasive network observability solution is now easier than ever with DANZ Monitoring Fabric. With its integrated visibility fabric, DMF delivers invaluable network insights at scale -- not just mere plumbing. By enabling a scale-out fabric for enterprise-wide security and monitoring, a single pane of glass for operational simplicity, and multi-tenancy for multiple IT (NetOps, DevOps, SecOps) teams, DMF eliminates the challenges faced by traditional, legacy NPB solutions. Leveraging DMF's contextual and predictive Analytics, Application Dependency Mapping and Network Time Machine features, customers can build custom IT workflows to enable quicker troubleshooting of the network / application issues. With its differentiated, modern architecture, DMF enables enterprises to realize the benefits of simplified productivity, superior scalability, and pervasive security at ethernet economics.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062