White Paper

Extending Your IT Infrastructure Into Amazon Web Services Using Cisco DMVPN and the Cisco Cloud Services Router 1000V Series

Amazon Web Services (AWS) provides a variety of networking features that enable basic connectivity and traffic management to and from applications hosted in the AWS cloud. Enterprise IT departments that specialize in network design and administration may not find all of the networking tools they require in AWS. Additionally, the mechanisms for integrating the AWS cloud with existing enterprise data centers are limited, and they pose a challenge for IT departments seeking a truly transparent and familiar expansion into the cloud.

Unlike other products that offer just cloud gateway functions, or just cloud security features, the Cisco® Cloud Services Router 1000V Series (Cisco CSR 1000V Series) is a complete multiservice cloud networking platform. The Cisco CSR 1000V Series provides networking features including routing, VPN, stateful firewall, application inspection, and even data center interconnect (DCI) and IP mobility. At the core of the Cisco CSR 1000V Series is a modular software architecture that allows for quick and easy integration with additional networking services as cloud networking and customer needs evolve.

Technology Overview

The Cisco CSR 1000V Series

The Cisco CSR 1000V Series is a multitenant-capable router in a virtual form factor that delivers comprehensive WAN gateway functions to multitenant, provider-hosted clouds. Using familiar, industry-leading Cisco IOS® Software networking capabilities, the Cisco CSR 1000V Series enables enterprises to transparently extend their WANs into external provider-hosted clouds and cloud providers to offer enterprise-class networking services to their tenants.

The Cisco CSR 1000V Series addresses these cloud-based networking and security constraints. Built on the same proven Cisco IOS Software platform that is inside the Cisco Integrated Services Router (ISR) and Aggregation Services Router (ASR) product families, the Cisco CSR 1000V Series offers a rich set of features including routing, VPN, firewall, Network Address Translation (NAT), quality of service (QoS), application visibility, failover, and WAN optimization. These functions empower enterprises and cloud providers to build highly secure, optimized, scalable, and consistent hybrid networks.

It also supports flexible and secure WAN design over any transport using Cisco Dynamic Multipoint VPN (DMVPN), firewall, and Cisco Cloud Web Security (CWS) technologies. When combined, these capabilities provide easy multihoming over any carrier service, offering a single routing control plane with minimal peering to the provider; automatic site-to-site IP Security (IPsec) tunnels; and comprehensive threat defense with Cisco Adaptive Security Appliances (ASA), Cisco IOS Firewall, Cisco IOS Intrusion Prevention System (IPS), and Cisco CWS for direct Internet access.

Features

- Cisco Application Visibility and Control (AVC): Cisco AVC provides IT visibility and control at the application level (Layer 7) through Cisco AVC technologies such as Network-Based Application Recognition 2 (NBAR2), Cisco IOS NetFlow, QoS, performance monitoring, medianet, and more. Cisco AVC allows IT to determine what traffic is running across the network, tune the network for business-critical services, and resolve network problems.
- Zone-based firewall (ZBFW): The Cisco CSR 1000V Series includes the advanced security features built into Cisco IOS XE Software such as access control lists (ACLs) and a stateful ZBFW. Configuration of these features is familiar to existing IT staff and allows you to extend existing enterprise security into the AWS cloud. You can apply security policies between virtual networks or applications in the AWS cloud as well as between the AWS cloud and external interconnected locations.

  You can assign the Cisco CSR 1000V Series interfaces to different security zones and specify rules to control the traffic between those zones. The traffic is dynamically inspected as it passes through the zones. ZBFW supports many types of application inspection including HTTP, Secure HTTP (HTTPS), Secure Shell (SSH) Protocol, Simple Mail Transfer Protocol (SMTP), IM applications, and point-to-point file sharing. If no policy is explicitly configured, all traffic moving between zones is blocked.
- Cisco IOS IP Service-Lebel Agreements (IP SLAs): Cisco IOS IP SLAs actively monitor and measure performance between multiple network locations or across multiple network paths. They simulate network data and IP services, and collect network performance information in real time. The information collected includes data about response time, one-way latency, jitter (interpacket delay variance), packet loss, voice-quality scoring, network resource availability, application performance, and server response time. You can use measurement statistics provided by the various Cisco IOS IP SLAs operations for troubleshooting, problem analysis, and designing network topologies.

  Using Cisco IOS IP SLAs, service provider customers can measure and provide SLAs and enterprise customers can verify service levels, verify outsourced SLAs, and understand network performance for new or existing IP services and applications. Cisco IOS IP SLA uses unique service-level assurance metrics and methodology to provide highly accurate, precise service-level assurance measurements.
- Cisco IOS Embedded Event Manager (EEM): Cisco IOS EEM is a powerful and flexible subsystem that provides real-time network event detection and onboard automation. It allows you to adapt the behavior of your network devices to align with your business needs.

Cisco IOS EEM supports more than 20 event detectors that are highly integrated with different Cisco IOS Software components to trigger actions in response to network events. You can inject your business logic into network operations using Cisco IOS EEM policies.

Cisco DMVPN

Cisco DMVPN is a Cisco IOS Software solution for building scalable IPsec VPNs. It uses a centralized architecture to provide easier implementation and management for deployments that require granular access controls for diverse user communities, including mobile workers, telecommuters, and extranet users.

Cisco DMVPN allows branch offices to communicate directly with each other over the public WAN or Internet, for example when using voice over IP (VoIP) between two branch offices, but does not require a permanent VPN connection between sites. It enables zero-touch deployment of IPsec VPNs and improves network performance by reducing latency and jitter while optimizing head-office bandwidth usage.

Cisco DMVPN Benefits

- Lowers capital expenditures (CapEx) and operatimg expenses (OpEx) by reducing costs when integrating voice and video with VPN security
- Simplifies branch-office communications by enabling direct branch office -to-branch office connectivity for business applications such as voice
- Reduces deployment complexity by offering a zero-touch configuration, dramatically reducing the deployment complexity in VPNs
- Improves business resiliency by preventing disruption of business-critical applications and services by incorporating routing with standards-based IPsec

ArcanaNetworks ManageExpress Virtual Office

You can rapidly and securely connect your enterprise network to remote offices, teleworkers, and the cloud with ArcanaNetworks ManageExpress Virtual Office (MEVO), which extends the enterprise securely into the cloud with zero-touch provisioning of Cisco Cloud Services Routers. The zero-touch provisioning is achieved through ArcanaNetworks' cloud service orchestration solution mCloud. You can input the cloud provider's details into MEVO, choose your preferred VPN technology, and let MEVO do the rest. MEVO mCloud transparently interfaces with AWS to provision, deploy, and manage Cisco Cloud Services Routers, connecting them to a private enterprise network. Combined with the Cisco Virtual Office solution, with one touch MEVO will establish a virtual private cloud for your enterprise that encompasses teleworkers, field offices, and cloud datacenters.

The MEVO mCloud feature set further enhances the MEVO solution to securely extend your data center to public or private cloud infrastructures. ArcanaNetworks and Cisco partnered to develop MEVO to specifically address the rapid deployment of Cisco VPN technologies in the enterprise and the cloud. MEVO is part of the Cisco Solutions Plus program and is available on the Cisco Global Price List. For more information, please send an email message to: mevo-interest@external.cisco.com.

ActionPacked Networks LiveAction Software

LiveAction is a sophisticated network performance management and QoS control tool that enables you to optimize end-user experience and business application delivery by effectively managing your application-aware network performance. LiveAction visually controls your enterprise networks by simplifying the complexity of monitoring, analyzing, and configuring technology areas such as QoS, LAN switching, Cisco IOS NetFlow, Flexible NetFlow (FNF), NBAR2, medianet, Cisco AVC, Cisco Performance Routing (PfR), and IP SLA. The latest LiveAction 3.0

release provides improved scalability and guided workflows to quickly resolve business-critical performance problems in your WAN, software as a service (SaaS), and cloud application, Multiprotocol Label Switching (MPLS) or Cisco DMVPN links, converged wired and wireless connections, and video, VoIP, and bring-your-own-device (BYOD) technologies. For more information, visit: https://marketplace.cisco.com/catalog/products/2620.

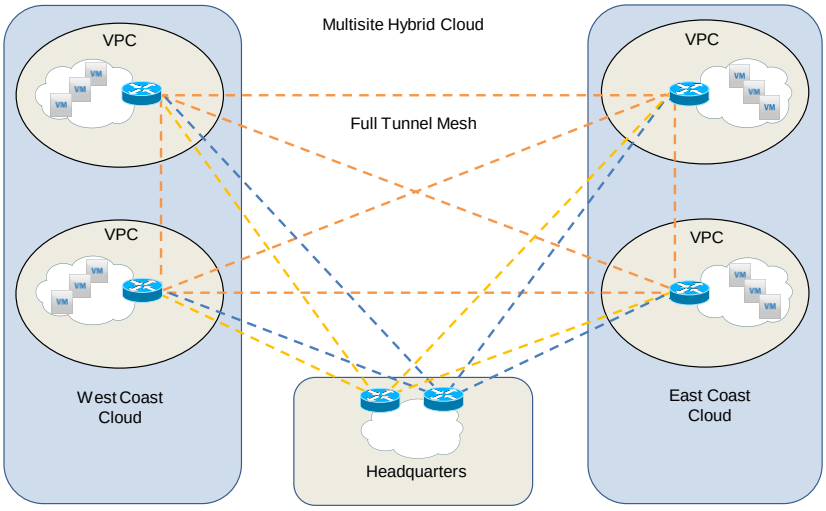
Solution Overview

Organizations typically connect to their applications through a a single VPN tunnel between their data center and AWS. With the Cisco CSR 1000V Series deployed in AWS, every enterprise office and branch-office location can now have direct VPN access into the AWS hosted applications without back-hauling through an existing data center. This approach reduces latency, eliminates the need for expensive private WAN services, avoids per-VPN-tunnel costs that Amazon charges, and even allows AWS to participate in existing route-based VPN topologies.

Fully Connecting All Virtual Private Clouds with Headquarters

Figure 1 illustrates connection of all virtual private clouds (VPCs) with headquarters.

Figure 1. Full Tunnel Mesh Connecting All VPCs with Headquarters

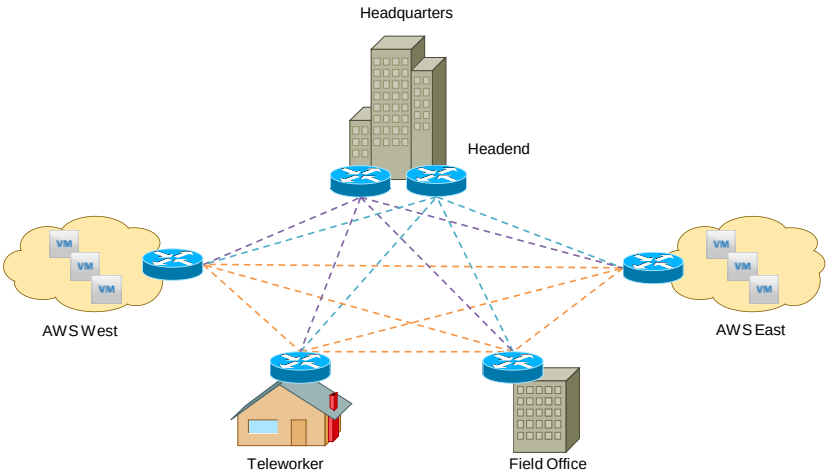


AWS does not provide VPN connectivity between VPCs in discrete AWS regions, making multiregion cloud deployments complex. By deploying a Cisco CSR 1000V Series Router in each region's VPC and interconnecting Cisco CSR 1000V Series Routers through a VPN, you can create a global, secure network topology within the AWS cloud.

Enterprisewide Network Connecting Headquarters, Cloud, Branch Office, and Teleworkers

Figure 2 shows an example of the Cisco CSR 1000V Series connecting multiple locations such as headquarters, cloud, branch office, and teleworkers with enterprisewide networking.

Figure 2. Cisco CSR 1000V Series Connecting Multiple Locations Using Enterprise-Wide Networking

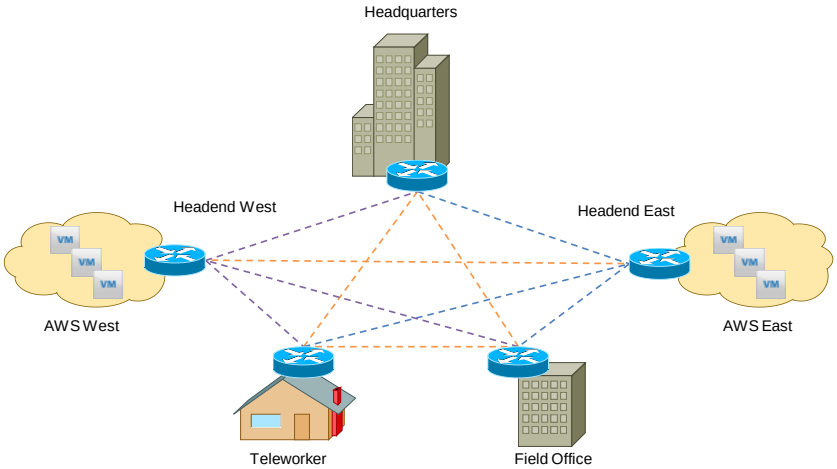


The Cisco CSR 1000V Series is based on the same internetworking operating system that powers the latest edge, branch-office, service, and telecommuting routers, providing the ideal platform on which to build a fully connected enterprise network. Together, these platforms provide easy multihoming over any carrier service offering, a single routing control plane with minimal peering to the provider, automatic site-to-site IPsec tunnels, and comprehensive threat defense.

AWS Hosted, Fully Connected Hybrid Cloud

Figure 3 shows how dynamically created tunnels help avoid bottlenecks by connecting the AWS hosted, fully connected hybrid cloud.

Figure 3. Dynamically Created Tunnels Connect AWS Hosted, Fully Connected Hybrid Cloud to Avoid Bottlenecks

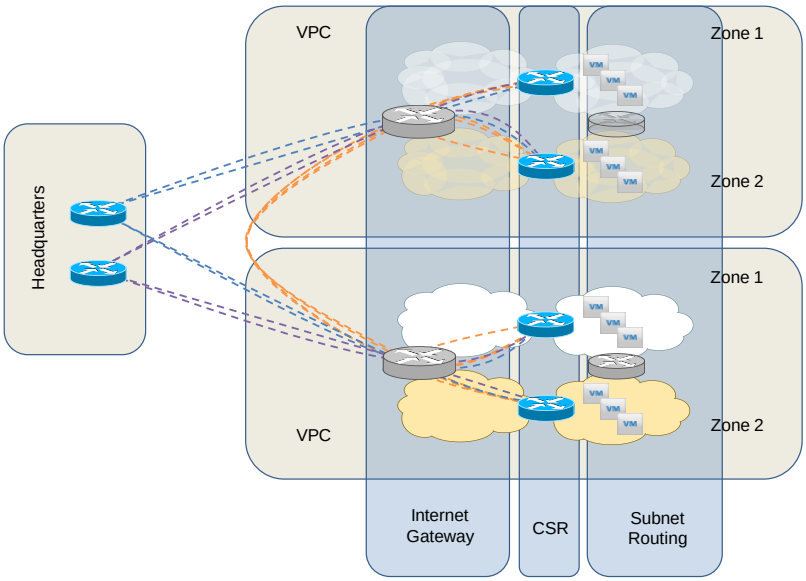


If your organization wants a highly available VPN cloud with geographically disparate headend routers, you can place the headend routers in separate AWS data centers. The full mesh of dynamically created tunnels makes it possible to avoid potential bottlenecks and increased bandwidth costs associated with cloud-based headend routers by allowing spoke-to-spoke traffic. Only traffic destined for the application servers in the cloud flows through the headend routers.

Fully Redundant AWS Cloud Router

Figure 4 shows how you can realize high availability within the fully redundant AWS cloud router with the Cisco CSR 1000V Series.

Figure 4. High Availability Within the Fully Redundant AWS Cloud Router with Cisco CSR 1000V Series



In addition to high availability at the headend, the Cisco CSR 1000V Series can provide high availability within the AWS VPC. You can place multiple Cisco CSR 1000V Series Routers in separate availability zones with a set of routers, using each of them as their default route. When maintenance is required on one of the Cisco CSR 1000V Series Routers, you can route traffic from one availability zone to another Cisco CSR 1000V Series Router in the other availability zone, either manually or automatically through active monitoring. Each of the two Cisco CSR 1000V Series Routers can route to any other spoke in the Cisco DMVPN network as well as other CSR 1000V Routers within AWS.

Benefits

- Single routing plane: The Cisco CSR 1000V Series routing protocol support for Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) allows it to integrate smoothly into the rest of your enterprise network instead of creating islands in the cloud.
- High availability: The dual-hub Cisco DMVPN design provides a fault-tolerant overlay network with no single point of failure. This fault tolerance is increased when the hubs are geographically disparate.

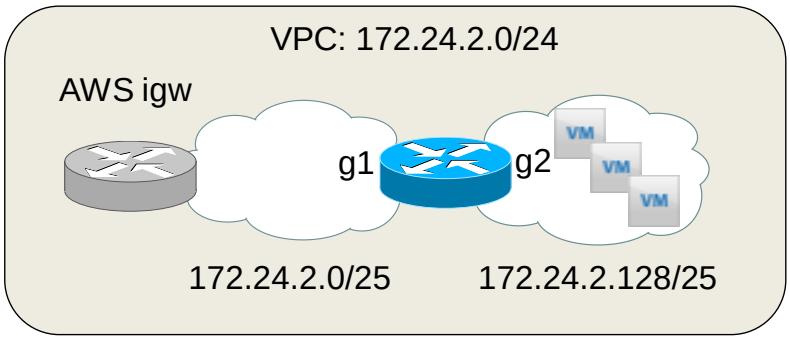
- Defense in depth: The security provided by the overlay network through IPsec tunnels and ZBFWs is disjointed from the underlying AWS infrastructure, providing protection for your corporate network if the AWS account is compromised.
- Unified security policy: Using ZBFWs, your organization can use the Cisco CSR 1000V Series to create a cohesive security policy across your entire network, including branch offices, mobile workers, and public clouds.

Configuration Examples

Dual Subnet Configuration

Figure 5 illustrates a dual subnet configuration.

Figure 5. Dual Subnet Configuration



For best results, the Cisco CSR 1000V Series requires creation of two subnets in the VPC both inside and outside. The outside network provides the address to associate an elastic IP address to allow the Cisco CSR 1000V Series Router to communicate to the headend and other sites. The inside interface connects to the subnet on which the virtual machines reside. Finally, Source/Dest Checking must be disabled on both the inside and outside interfaces of the Cisco CSR 1000V Router.

Next, you should create an Internet gateway and associate it with the VPC. The route table for the outside subnet should contain a default route, for example 0.0.0.0/0, that points to this Internet gateway. The inside subnet should contain a default route that points to the inside interface of the Cisco CSR 1000V Series. You can place routers on either of these subnets. Routers on the inside subnet can reach the routers on the outside subnet, depending on the zone firewall rules specified in the CSR 1000V Routers; hosts outside the VPC also can reach routers on the inside subnet when they are associated with an elastic IP. The configuration follows:

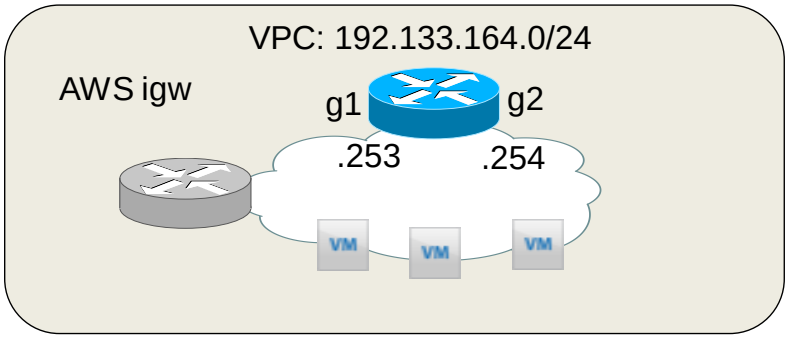
```
interface GigabitEthernet1
 ip address dhcp
 negotiation auto
!
interface GigabitEthernet2
 ip address 172.24.2.254 255.255.255.128
 ip tcp adjust-mss 1360
```

```
 negotiation auto
```

Single Subnet Configuration

Figure 6 shows a single subnet configuration.

Figure 6. Single Subnet Configuration



In some circumstances it is not desirable to create two separate subnets within a virtual device context (VDC) to support the inside and outside interfaces of the Cisco CSR 1000V Series. For example, using two subnets for extending public IP address space into AWS is problematic because part of that address space must be used for the 1:1 NAT address to which the elastic IP address is associated. In this case, you should create the CSR 1000V and put both interfaces in the same subnet. In order to address both interfaces on the same subnet, you should place the inside interface in its own Virtual Route Fowarding (VRF) path. When configuring the Cisco CSR 1000V in this manner, you must configure the instance default router to point to the inside interface of the CSR 1000V in order for it to route traffic. This configuration follows:

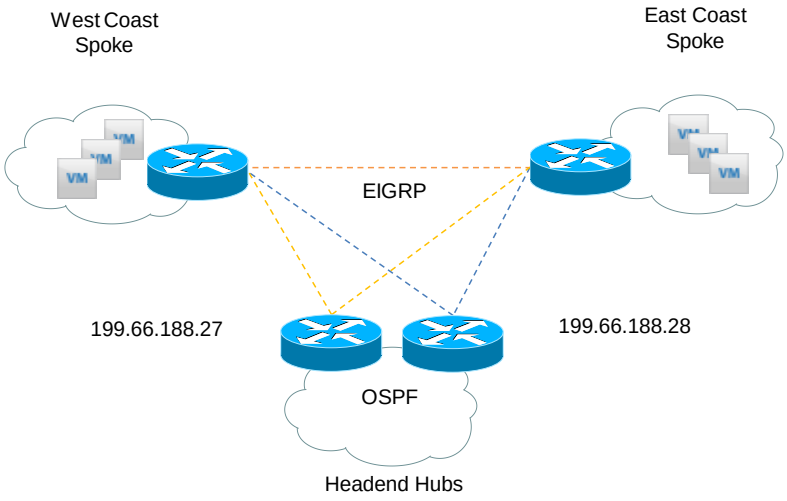
```
ip vrf inside
 rd 1:2
!
interface GigabitEthernet1
 ip address dhcp
 negotiation auto
!
interface GigabitEthernet2
 ip vrf forwarding inside
 ip address 192.133.164.254 255.255.255.0
 ip tcp adjust-mss 1360
 negotiation auto
```

Cisco DMVPN Design Example 1: No Direct Internet Access from Spokes

You can configure Cisco DMVPN to either allow or disallow routers in the AWS network spokes from direct access to the network. This example disallows direct Internet access by placing the outside interface of the AWS Cisco CSR 1000V Series Router in a VRF and then sending a default route from the Cisco DMVPN hub routers. You could use this scenario for private enterprise applications that are hosted on AWS and therefore do not need direct Internet connectivity, or for public applications that should be accessed through the enterprise Internet connections.

Figure 7 shows an example of a Cisco DMVPN configuration.

Figure 7. Cisco DMVPN Example



Configuring a Front Door VRF

Placing the outside interface of the Cisco CSR 1000V Series in a separate VRF path provides greater security and segmentation by separating the routing table that includes corporate routes from the routing table that provides the default route to the Internet. Generally, this separation requires out-of-band management or console access, and AWS provides neither. Fortunately, Cisco EEM provides the flexibility to work around this limitation. The following shows how to configure a Cisco EEM applet to set the outside interface into its own VRF and then reapply the standard Dynamic Host Configuration Protocol (DHCP) configuration that AWS uses:

Create a VRF

```
vrf definition internet-vrf
 rd 1:1
 !
 address-family ipv4
 exit-address-family
```

Create the Cisco EEM Applet

```
event manager applet fvrf
event none
action 1.0 cli command "enable"
action 1.1 cli command "conf t"
action 1.2 cli command "interface gig1"
action 1.3 cli command "vrf forwarding internet-vrf"
action 1.4 cli command "ip address dhcp"
action 2.0 cli command "end"
```

Run the Cisco EEM Applet

```
event manager run fvrf
```

You then can reconnect to the Cisco CSR 1000V Series with SSH to the outside interface.

Final Outside Interface Configuration

```
interface GigabitEthernet1
 vrf forwarding internet-vrf
 ip address dhcp
 negotiation auto
```

Configuring Cisco DMVPN and Routing

This design uses a single DMVPN, dual-hub configuration, EIGRP as the Cisco DMVPN routing protocol, and OSPF as the enterprise routing protocol. The AWS Cisco CSR 1000V Series Routers are configured as DMVPN spokes and EIGRP stub routers. The DMVPN hub routers, typically located in the enterprise headquarters locations, advertise a default route to the Cisco DMVPN spokes and advertise the AWS subnets to the rest of the enterprise. Cisco DMVPN Phase 3 with Next Hop Resolution Protocol (NHRP) redirection is configured to provide spoke-to-spoke tunnel support. This configuration allows AWS application in different Amazon VPCs to communicate directly with each other. Additionally, enterprise branch-office sites can be part of the same Cisco DMVPN, allowing path optimization where the branch office can use secure, direct access to the AWS hosted applications without having to transit the headquarters network. The configuration follows.

Hub Cisco DMVPN and Routing Configuration

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
```

```
crypto isakmp key Cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set xform esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile ipsec-prof
 set transform-set xform
!
!
interface Tunnel0
 ip address 172.24.0.1 255.255.255.0
 no ip redirects
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip nhrp map multicast dynamic
 ip nhrp map 172.24.0.2 199.66.188.28
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile ipsec-prof
  !
router eigrp 1
 network 172.24.0.0
!
router ospf 1
 redistribute static subnets route-map static2ospf
!
ip route 172.24.0.0 255.255.0.0 Null0
!
access-list 1 permit 172.24.0.0 0.0.255.255
!
route-map static2ospf permit 10
 match ip address 1
```

Spoke Cisco DMVPN and Routing Configuration

```
crypto keyring internet-key vrf internet-vrf
  pre-shared-key address 0.0.0.0 0.0.0.0 key Cisco123
!
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
crypto isakmp profile isakmp-prof
   keyring internet-key
   match identity address 0.0.0.0 internet-vrf
!
crypto ipsec transform-set xform esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile ipsec-prof
 set transform-set xform
 set isakmp-profile isakmp-prof
!
interface Tunnel0
 ip address 172.24.0.5 255.255.255.0
 no ip redirects
 ip nhrp network-id 1
 ip nhrp nhs 172.24.0.1 nbma 199.66.188.27 multicast
 ip nhrp nhs 172.24.0.2 nbma 199.66.188.28 multicast
 ip nhrp shortcut
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel key 1
 tunnel vrf internet-vrf
 tunnel protection ipsec profile ipsec-prof
  !
router eigrp 1
 network 172.24.0.0
 eigrp stub connected
```

Cisco DMVPN Design Example 2: Direct Internet Access from AWS Spokes

This example is similar to the previous Cisco DMVPN design. The main difference is that the outside interface of the AWS Cisco CSR 1000V is not placed in a VRF path , but is instead kept in the global table. Instead of receiving a default route from the Cisco DMVPN hub router, the AWS Cisco CSR 1000V uses the default route that the AWS DHCP server provides to send traffic directly to the Internet. At the Cisco DMVPN hub routers, specific OSPF routes are redistributed into the Cisco DMVPN EIGRP process to control which networks are reached through the Cisco DMVPN network. Finally, NAT is used to translate the inside address to the elastic IP address assigned to the Cisco CSR 1000V Series.

Outside Interface Configuration

```
interface GigabitEthernet1
 ip address dhcp
 negotiation auto
```

Hub Cisco DMVPN and Routing Configuration

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
crypto isakmp key Cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set xform esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile ipsec-prof
 set transform-set xform
!
!
interface Tunnel0
 ip address 172.24.0.1 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp map 172.24.0.2 199.66.188.28
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source GigabitEthernet1
```

```
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile ipsec-prof
!
router eigrp 1
 network 172.24.0.0
 redistribute ospf 1 metric 10000 10 255 1 1500 route-map ospf2eigrp
!
router ospf 1
 redistribute static subnets route-map static2ospf
!
ip route 0.0.0.0 0.0.0.0 199.66.188.1
ip route 172.24.0.0 255.255.0.0 Null0
!
access-list 1 permit 172.24.0.0 0.0.255.255
access-list 2 permit 199.66.188.0 0.0.0.255
access-list 2 permit 172.18.0.0 0.0.0.255
!
route-map static2ospf permit 10
 match ip address 1
!
route-map ospf2eigrp permit 10
 match ip address 2
```

Spoke Cisco DMVPN and Routing Configuration

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
crypto isakmp key Cisco123 address 0.0.0.0
crypto isakmp keepalive 30
!
crypto ipsec transform-set xform esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile ipsec-prof
```

```
 set transform-set xform
!
!
interface Tunnel0
 ip address 172.24.0.5 255.255.255.0
 no ip redirects
 ip nhrp network-id 1
 ip nhrp nhs 172.24.0.1 nbma 199.66.188.27 multicast
 ip nhrp nhs 172.24.0.2 nbma 199.66.188.28 multicast
 ip nhrp shortcut
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile ipsec-prof
!
router eigrp 1
 network 172.24.0.0
 eigrp stub connected
```

NAT

You can use NAT to give the inside AWS instances direct access to the Internet using the elastic IP address of the Cisco CSR 1000V Series. Because the outside interface of the CSR 1000V is not assigned the elastic IP address directly, a second NAT is done from the AWS internal address to the actual elastic IP address.

```
interface GigabitEthernet1
 ip nat outside
!
interface GigabitEthernet2
 ip nat inside
 !
ip nat inside source list nat interface GigabitEthernet1 overload
!
ip access-list standard nat
 permit 172.24.2.0 0.0.0.255
```

The Cisco CSR 1000V can also perform NAT port translation to allow direct access of services through protocols such as HTTP. Providing direct access to the AWS-hosted instances allows offloading of bandwidth onto the cloud service provider when central inspection is not required. In the following configuration, 172.24.2.17 is the internal

AWS IP address allocated to the outside interface of the CSR 1000V and 172.24.2.200 is the internal AWS IP address of the router providing service on port 80:

```
ip nat inside source static tcp 172.24.2.200 80 172.24.2.17 80 extendable
```

Zone-Based Firewall Example

When directly accessing services in the cloud service provider or when more granular security is needed, you can configure ZBFWs to extend the enterprise security policy to the Cisco CSR 1000V Series Routers. The following configuration defines three zones: inside, outside, and tunnel. Protocol inspection is used to inspect and allow traffic between zones. An access control list (ACL) is used to define ports for which protocol inspection is not available. Because there is no need for traffic to flow below the tunnel and the outside interface, it is not allowed.

```
class-map type inspect match-any inside-tunnel
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any tunnel-inside
 match protocol icmp
 match protocol http
 match protocol https
 match protocol ssh
 match access-group name tunnel-inside
class-map type inspect match-any inside-outside
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any outside-inside
 match protocol http
 match protocol https
 match access-group name outside-inside
!
policy-map type inspect inside-tunnel
 class type inspect inside-tunnel
  inspect
 class class-default
  drop log
policy-map type inspect outside-inside
 class type inspect outside-inside
  inspect
```

```
 class class-default
  drop log
policy-map type inspect inside-outside
 class type inspect inside-outside
  inspect
 class class-default
  drop log
policy-map type inspect tunnel-inside
 class type inspect tunnel-inside
  inspect
 class class-default
  drop log
!
zone security outside
zone security inside
zone security tunnel
zone-pair security inside-outside source inside destination outside
 service-policy type inspect inside-outside
zone-pair security inside-tunnel source inside destination tunnel
 service-policy type inspect inside-tunnel
zone-pair security outside-inside source outside destination inside
 service-policy type inspect outside-inside
zone-pair security tunnel-inside source tunnel destination inside
 service-policy type inspect tunnel-inside
!
interface Tunnel0
zone-member security tunnel
!
interface GigabitEthernet1
zone-member security outside
!
interface GigabitEthernet2
zone-member security inside
!
ip access-list extended outside-inside
ip access-list extended tunnel-inside
 permit tcp any host 172.24.2.200 eq 3389
```

Secure Public Interfaces

You can use ACLs to protect the router from outside traffic. The following ACL prevents all traffic except what is required to remotely manage the router, create the tunnel, and perform DHCP on the outside interface.

```
ip access-list extended internet
 permit esp any any
 permit udp any eq isakmp any
 permit udp any any eq isakmp
 permit udp any eq non500-isakmp any
 permit udp any any eq non500-isakmp
 permit tcp any any eq 22
 permit tcp any eq 22 any
 permit udp any eq bootps any eq bootpc
 permit udp any eq bootpc any eq bootps

interface GigabitEthernet1
 ip access-group internet in
 ip access-group internet out
```

Note: You can further limit SSH access by applying a vty access class. If the Gig1 interface is in a VRF path, be sure to use the **vrf-also** command option with the **access-class** command (**access-class 34 in vrf-also**).

Note: Policy must be reconciled between interface ACLs and ZBFWs when both are used simultaneously.

AVC

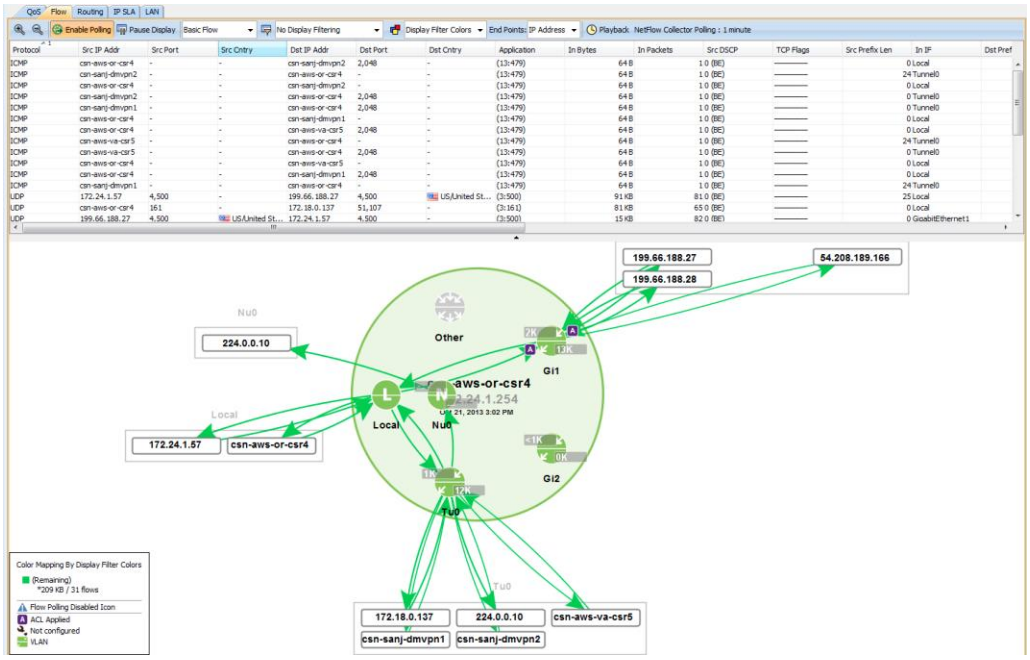
Cisco AVC features, such as Cisco IOS Flexible NetFlow and NBAR2, provide rich application visibility that you can use for application performance monitoring and security applications. You can use LiveAction 3.0 to configure and monitor Cisco AVC on the Cisco CSR 1000V Series Routers. LiveAction generated and applied the following sample Cisco AVC configuration to the Cisco CSR 1000V Routers. In addition, Figure 8 shows a screenshot of the sample Cisco IOS NetFlow data that was collected.

```
flow record LIVEACTION-FLOWRECORD
 description DO NOT MODIFY. USED BY LIVEACTION.
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
```

```
 match flow direction
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect transport tcp flags
 collect interface output
 collect flow sampler
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
!
!
flow exporter LIVEACTION-FLOWEXPORTER
 destination 172.18.0.137
 source GigabitEthernet2
!
!
flow monitor LIVEACTION-FLOWMONITOR
 description DO NOT MODIFY. USED BY LIVEACTION.
 exporter LIVEACTION-FLOWEXPORTER
 cache timeout inactive 10
 cache timeout active 60
 record LIVEACTION-FLOWRECORD
!
interface Tunnel0
 ip nbar protocol-discovery
 ip flow monitor LIVEACTION-FLOWMONITOR input
 ip flow monitor LIVEACTION-FLOWMONITOR output
!
interface GigabitEthernet1
```

```
 ip nbar protocol-discovery
 ip flow monitor LIVEACTION-FLOWMONITOR input
 ip flow monitor LIVEACTION-FLOWMONITOR output
!
interface GigabitEthernet2
 ip nbar protocol-discovery
 ip flow monitor LIVEACTION-FLOWMONITOR input
 ip flow monitor LIVEACTION-FLOWMONITOR output
```

Figure 8. LiveAction AVC Reporting Screenshot



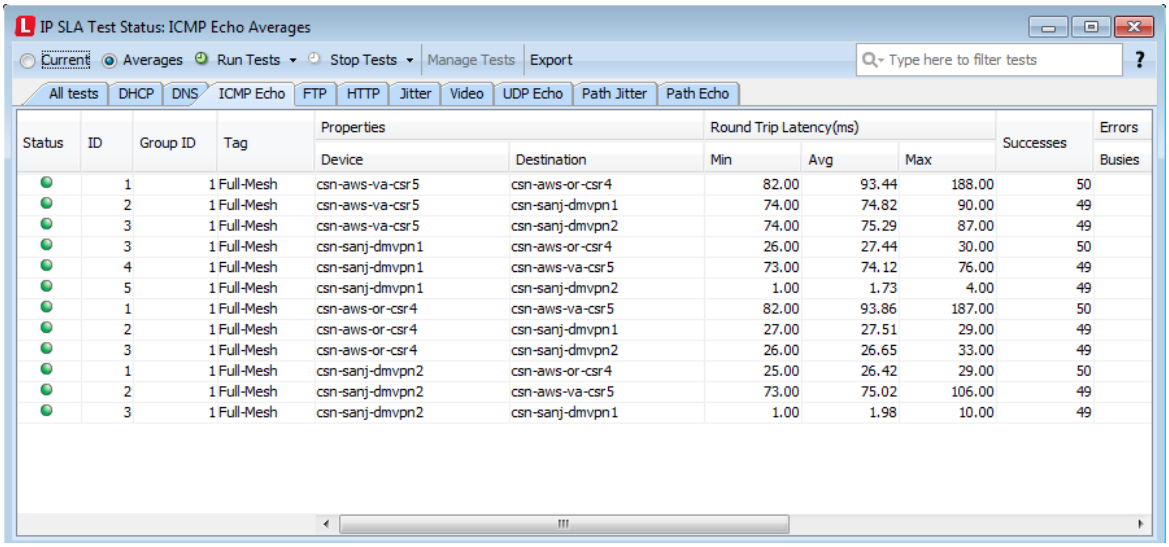
IP SLA

You can use the IP SLA tool to generate synthetic traffic to gather network performance metrics such as delay and loss. LiveAction 3.0 generates IP SLA configuration and provides reporting. The following are sample configurations that were applied; Figure 9 shows a sample screenshot of the capture results.

```
ip sla 1
 icmp-echo 172.24.0.5 source-ip 172.24.0.4
 tag DMVPN_SLA
ip sla 2
 icmp-echo 172.24.0.1 source-ip 172.24.0.4
 tag DMVPN_SLA
ip sla 3
```

```
 icmp-echo 172.24.0.2 source-ip 172.24.0.4
 tag DMVPN_SLA
ip sla group schedule 1 1-3 schedule-period 60 frequency 60 start-time now life
forever
ip sla responder
```

Figure 9. LiveAction IP SLA Statistics Table



Status	ID	Group ID	Tag	Properties		Round Trip Latency(ms)			Successes	Errors
				Device	Destination	Min	Avg	Max		Busies
	1	1	Full-Mesh	csn-aws-va-csr5	csn-aws-or-csr4	82.00	93.44	188.00	50	
	2	1	Full-Mesh	csn-aws-va-csr5	csn-sanj-dmvpn1	74.00	74.82	90.00	49	
	3	1	Full-Mesh	csn-aws-va-csr5	csn-sanj-dmvpn2	74.00	75.29	87.00	49	
	3	1	Full-Mesh	csn-sanj-dmvpn1	csn-aws-or-csr4	26.00	27.44	30.00	50	
	4	1	Full-Mesh	csn-sanj-dmvpn1	csn-aws-va-csr5	73.00	74.12	76.00	49	
	5	1	Full-Mesh	csn-sanj-dmvpn1	csn-sanj-dmvpn2	1.00	1.73	4.00	49	
	1	1	Full-Mesh	csn-aws-or-csr4	csn-aws-va-csr5	82.00	93.86	187.00	50	
	2	1	Full-Mesh	csn-aws-or-csr4	csn-sanj-dmvpn1	27.00	27.51	29.00	49	
	3	1	Full-Mesh	csn-aws-or-csr4	csn-sanj-dmvpn2	26.00	26.65	33.00	49	
	1	1	Full-Mesh	csn-sanj-dmvpn2	csn-aws-or-csr4	25.00	26.42	29.00	50	
	2	1	Full-Mesh	csn-sanj-dmvpn2	csn-aws-va-csr5	73.00	75.02	106.00	49	
	3	1	Full-Mesh	csn-sanj-dmvpn2	csn-sanj-dmvpn1	1.00	1.98	10.00	49	

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.**