Cisco Catalyst SD-WAN Remote Access Design Case Study

American GasCo SD-WAN Remote Access Design

December 2023

Contents

Introduction

Cisco Catalyst SD-WAN design case studies showcase the SD-WAN use cases and solutions that customers have leveraged to achieve their business outcomes. The companies featured in the SD-WAN case studies are fictitious, but the showcased designs are based on customer adoption and best practices learned from actual deployments in the industries represented. The case studies are aligned with the different types of SD-WAN deployments as observed and defined by Gartner in their Magic Quadrant criteria for SD-WAN. The categories include:

- Small Branch
- Global WAN
- Security Sensitive
- Cloud First
- Remote Worker

This case study focuses on the Remote Worker category. To learn more about the other case studies, refer to the Cisco Catalyst SD-WAN Design Case Studies guide.

About This Case Study

This case study builds on the previously published Cisco Catalyst SD-WAN Small Branch Design Case Study which detailed how American GasCo designed their 500+ gas station/convenience stores for Cisco Catalyst SD-WAN. It focuses on how American GasCo deployed the SD-WAN remote access (SDRA) feature to enable secure remote access for technicians and admins responsible for managing and monitoring the store network and its attached computers and IoT devices.

The case study discusses an overview of the SDRA solution, its components, and use cases. Use cases were prototyped in a Cisco lab environment using 20.7 SD-WAN Manager/17.7.2 IOS XE SD-WAN code versions. Detailed configurations and deployment information for the SDRA devices and related components in this testing can be found in the SDRA Deployment Guide, published at https://community.cisco.com/t5/networking-knowledge-base/deploying-sd-wan-remote-access-solution/ta-p/4824064.

Additional supporting documentation can be found in the Cisco SD-WAN Community Resources, which also references other existing SD-WAN documentation.

Audience

The intended audience is for anyone who wants a better understanding of the Cisco Catalyst SD-WAN solution, especially network architects that need to understand the SD-WAN design best practices to make good design choices for their organization.

Background

American GasCo corporation owns and operates approximately 500 gas station convenience stores in the Southeastern region of the US. As part of a modernization initiative, the company deployed SD-WAN to connect employee computers, point-of-sales terminals, and IoT devices to servers and storage hosted in their enterprise data centers. By deploying SD-WAN, the company was able to improve operational efficiency and increase store bandwidth by 200-300% to support a refresh of their forecourt fuel control systems and launch new services such as IP video surveillance and streaming media to the gas pumps.

Sometime after the initial SD-WAN rollout, American GasCo enabled Cisco Catalyst SD-WAN remote access (SDRA) on a subset of their branch routers to provide an agile, secure solution for remote monitoring and troubleshooting of critical devices connected to different service VPNs in the store LANs. This gave technicians the ability to use a soft VPN client to authenticate and establish remote IPsec connections to store WAN Edge routers where they would be logically placed into the VPN(s) they were granted access to, including:

- Forecourt Controller (FCC) system VPN that controls the fuel dispensers, storage tank controllers, outdoor payment terminals, price poles, streaming media servers, and automated car wash devices.
- Convenience store VPN that connects the point-of-sales terminals, back-office computers, and printers.
- Video surveillance VPN that connects the IP video cameras and NVRs to provide local and remote monitoring of the convenience store and forecourt areas.

Cisco Catalyst SD-WAN Remote Access (SDRA) Solution

Overview

A Remote Access (RA) Virtual Private Network (VPN) enables remote users to securely access and use applications that reside in the corporate data center, encrypting all traffic that the remote users send and receive. The Cisco Catalyst SD-WAN Remote Access (SDRA) feature enables Remote Access VPN capability in Cisco IOS XE SD-WAN devices, thus providing seamless integration to all the documented benefits of the Cisco Catalyst SD-WAN Solution.

This solution enables segmentation per user type (Enterprise, Guest, IOT, etc.) and provides support for brownfield deployments. This eliminates the need for two separate solutions, SD-WAN and Remote Access infrastructure, thereby enabling rapid scalability of RA services. In short, the Cisco Catalyst SDRA solution allows the deployment of Remote Access VPNs with users terminated into specific SD-WAN VPNs.

SDRA Components

The SDRA solution leverages the following key components:

- SD-WAN Infrastructure
  - SD-WAN Control Components – Up and functional set of Cisco Catalyst SD-WAN control components deployed either on-premise or in the cloud.
  - SD-WAN Headend Router – An IOS XE SD-WAN router that is configured to terminate the Remote Access VPN into the desired SD-WAN VPN.
- ISE – RADIUS Server for AAA functionality. ISE is required because AnyConnect-EAP is used to provide advanced capabilities, including specifying the target SD-WAN VPN as part of the RADIUS exchange. ISE thus plays an integral role in the entire working of this solution as it authorizes a given remote access user to be seated in preferred SD-WAN VPN, this way a network admin has a better control over which remote user can access what services in their organization.
- Certificate Authority – The Certificate Authority server acts as a trusted entity that provides digital certificates to the SDRA router. These digital certificates are small, verifiable files that contain identity credentials to help the SDRA router represent its authentic online identity (authentic as CA has verified the identity). These digital certificates are thus used to protect information and encrypt and enable secure communication between remote users and SDRA router. This could be a Windows/Linux server or IOS XE router running in Autonomous mode.

- Cisco AnyConnect VPN Client – Cisco AnyConnect VPN software acting as an endpoint client. A Remote Access VPN works by virtue of a virtual tunnel created between an employee's device and the company's network. This tunnel goes through the public internet, but the data sent back and forth through it is protected by encryption and security protocols.

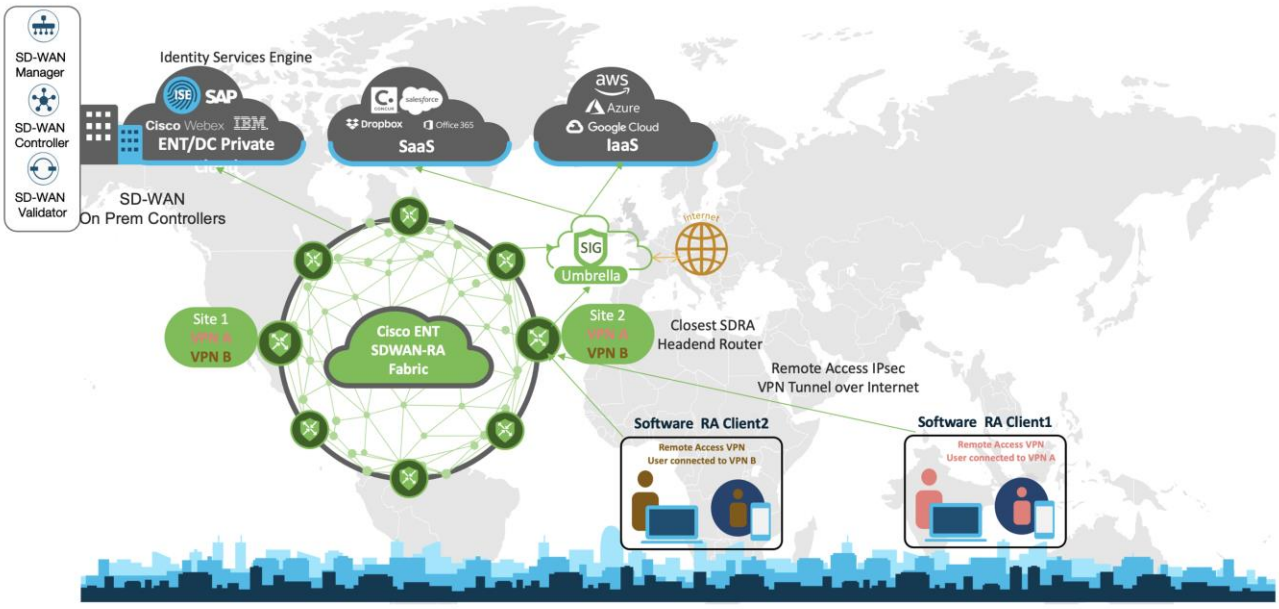
SDRA is similar to any remote user with the only difference being now it behaves as a service VPN LAN user riding on an SD-WAN overlay experiencing the same level of services like Application routing, AppQoE, Umbrella SIG, and DIA. It allows the user to securely connect to the company network, use applications and data, and have a similar experience of working from the office premises.

Listed below are the solution components and minimum recommended software versions required to deploy the SDRA solution.

Table 1. SDRA Components and Minimum Software Versions

Product	Quantity	Role
SD-WAN Manager (20.7)	1	SD-WAN Infrastructure
SD-WAN Validator (20.7)	1	SD-WAN Infrastructure
SD-WAN Controller (20.7)	1	SD-WAN Infrastructure
IOS XE SD-WAN (17.7.2)	1	SDRA Headend Router
Windows/Linux Server/Cisco IOS-XE in Autonomous mode	1	CA Server
Cisco ISE (3.2)	1	AAA Server
Cisco AnyConnect Client	Multiple	AnyConnect Client for Remote Access (Windows/MAC/iOS/Android)

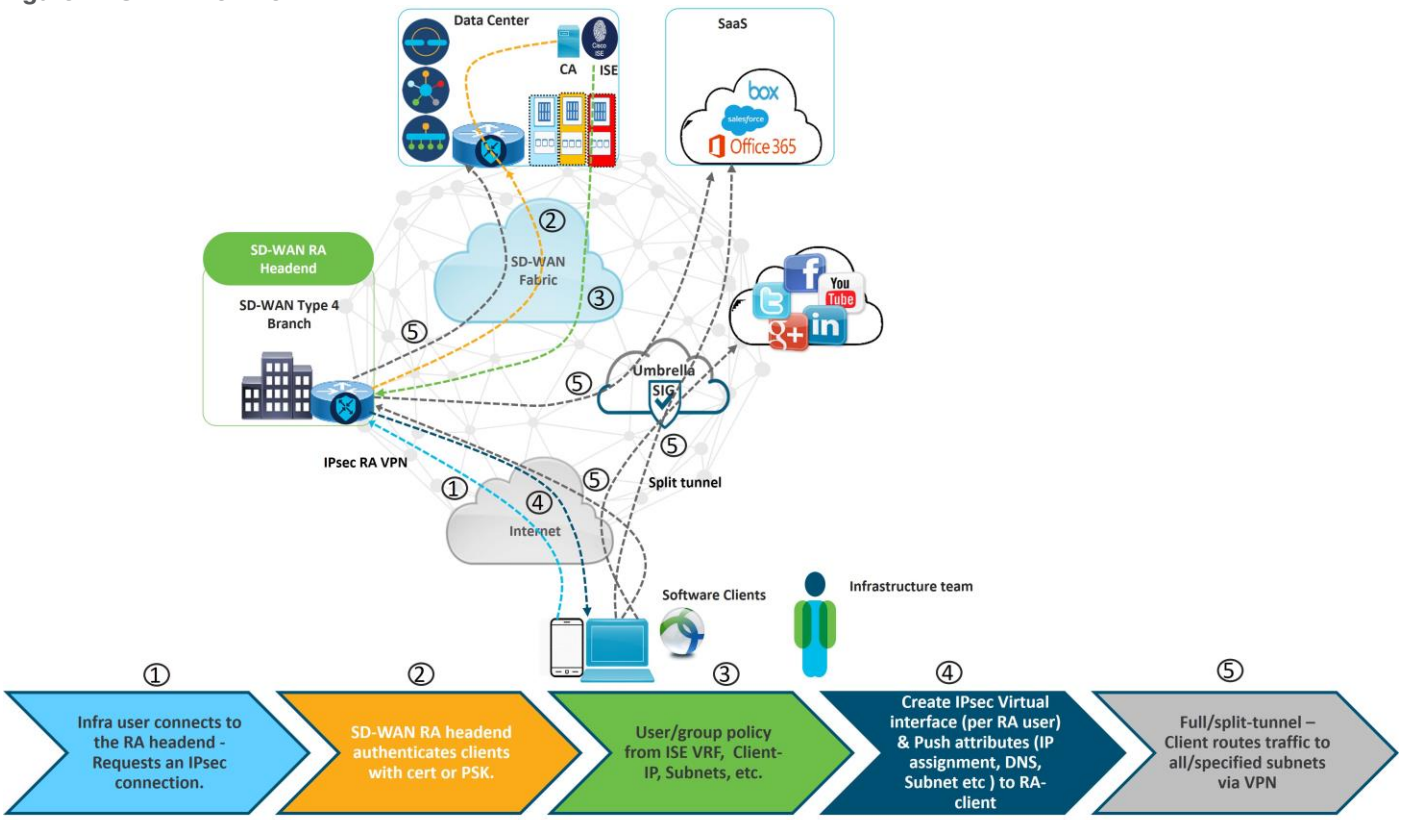
Figure 1. SDRA Components



SDRA Workflow

The following diagram illustrates the SDRA workflow when a remote user attempts to connect to the network:

Figure 2. SDRA Workflow



1. A remote user (ex: bob@americangasco.com) tries to connect to the SDRA headend router.
2. The SDRA headend authenticates the remote user using a certificate issued by the Certificate Authority (CA).
3. ISE already has Bob's AnyConnect credentials in its Identity Database. The moment the authentication succeeds there is a corresponding authorization policy that corresponds to this user. The authorization policy has set of AV attributes that allows this remote user to be seated in a Service VPN of choice. Additional knobs like split tunnel, full tunnel can be configured in this authorization policy to route the traffic accordingly.
4. A Virtual Access Interface per RA client is created on the SDRA headend router which borrows the IP address from the Loopback Interface. All the AV attributes defined in ISE authorization policy are thus passed to this remote client like DNS address, Subnet mask, VPN ID etc. The remote user gets assigned an IP address from the pool defined on both SDRA headend and ISE, and this remote user IP address is successfully seen under the defined VPN routing table as a static route. The Virtual Access interface stays up as long as the secure tunnel connection stays established.
5. If the user is given access to full tunnel, this will cause both the enterprise and Internet traffic to flow via this secure tunnel. For split tunnel, only SD-WAN-specific prefixes will be routed via the tunnel and the rest of the Internet traffic will flow natively from the Remote Access (RA) client.

Design Considerations

The placement of SDRA has been strategically chosen to be at a type 4 branch site within American GasCo's network. This will aid in limiting the network access to just the techs/store/infrastructure team, thereby saving considerable bandwidth as the users won't be backhauling to the DC anymore.

The ISE and CA server must be reachable from SDRA from the preferred SD-WAN VPN. Since the SDRA functionality is supported on the Cisco Catalyst 8000 Edge platform family which includes branch, aggregation, and virtual routers, American GasCo will thus go ahead and replace their existing ISR4k platforms at their type 4 branches with C8500 in the near future, making it as an aggregation point for the remote access users.

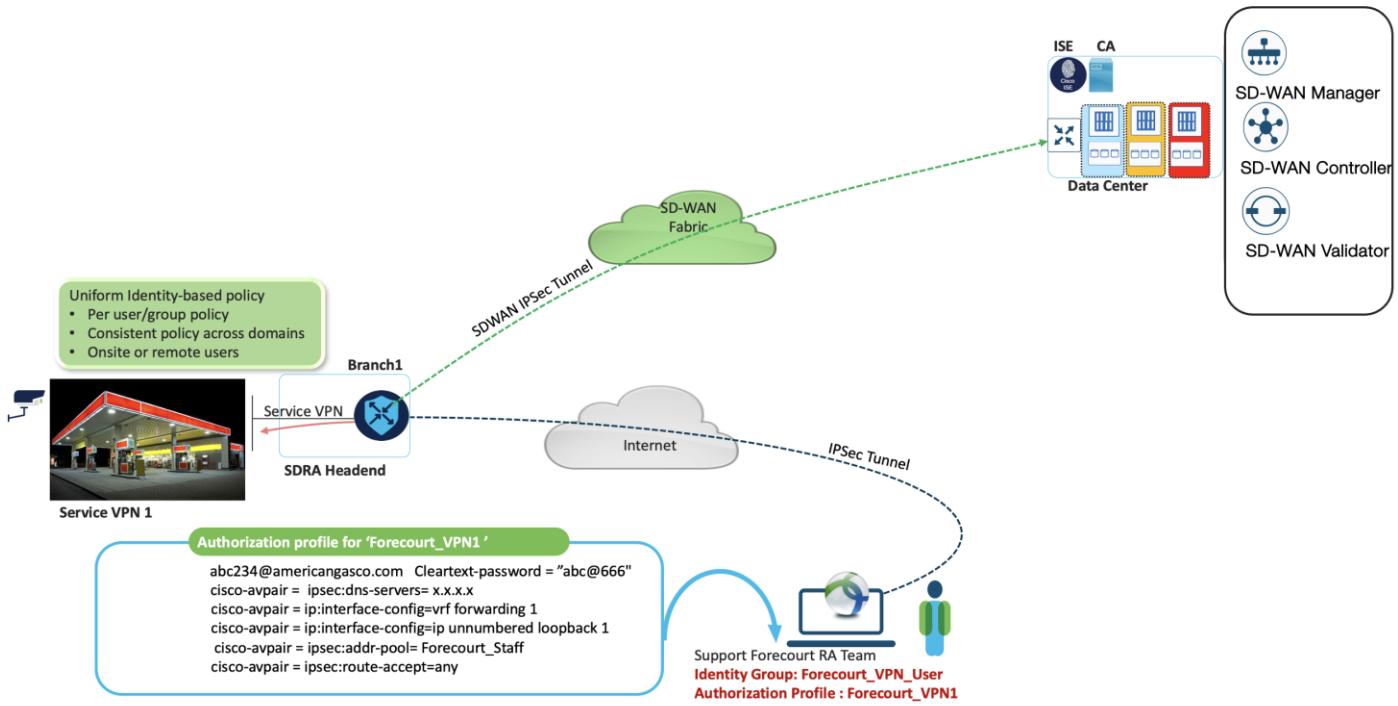
American GasCo SDRA Use Cases

Remote Monitoring of the Forecourt VPN

American GasCo's Infrastructure and Perimeter Security group is responsible for monitoring of the Forecourt controller systems that monitor system status, inventory, credit card transactions, and fuel dispensing at the gas pumps. During work hours, remote monitoring is done by operators at the Atlanta operations center using a custom management system that establishes HTTPS connections to the web interface of each FCC controller using the SD-WAN network. In the event of a system outage or malfunction at a site, the group would typically dispatch a contracted technician for a site visit to diagnose issues and restore system components or connectivity to the LAN.

To reduce the number of truck rolls to a site, American GasCo enabled secure remote access to the FCC VPN so that its infrastructure team and authorized contractors could remotely diagnose and troubleshoot prior to dispatching a technician. The SDRA solution integrates with ISE for authentication to validate credentials and grant access to only the FCC VPN (VPN 1) for these remote technicians. Once connected, the remote technicians are assigned address space from Service VPN 1 where they have direct HTTPS access to the FCC and other devices for monitoring and troubleshooting.

Figure 3. Remote Monitoring of the Forecourt VPN Use Case



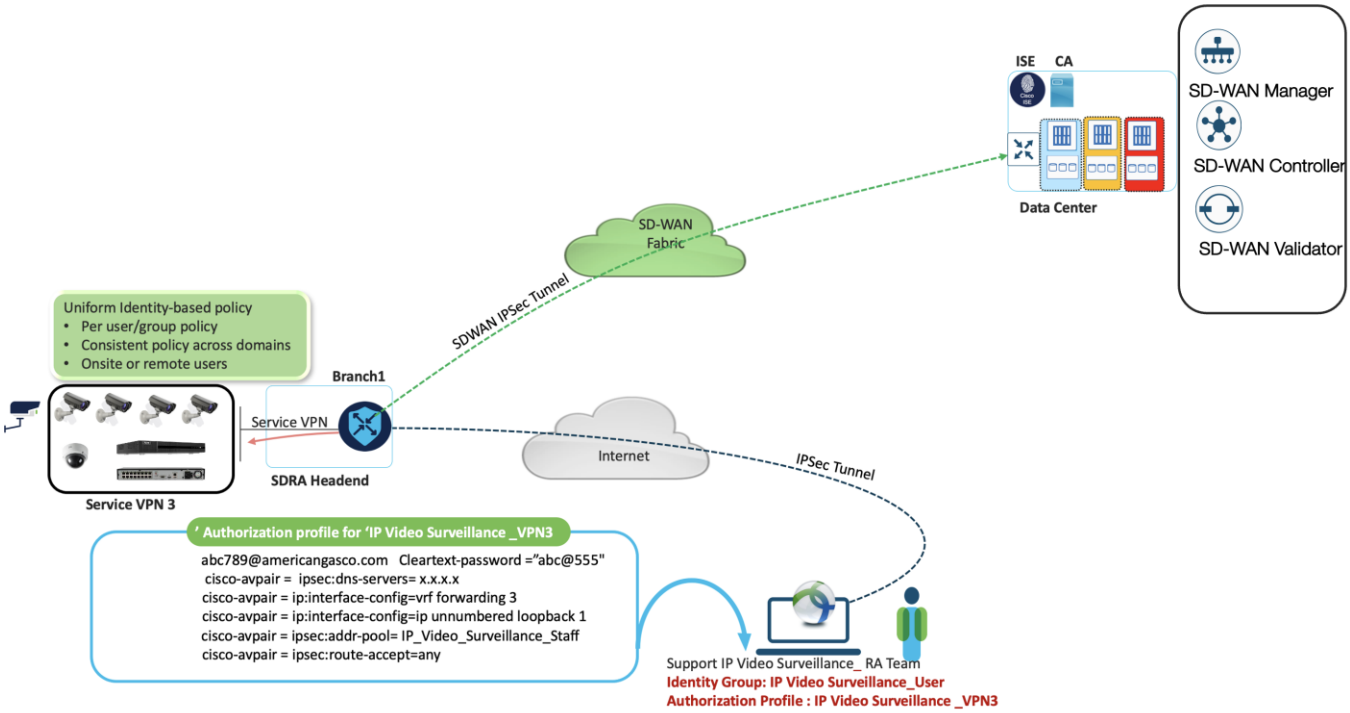
Remote Troubleshooting of IP Surveillance Cameras and NVRs

American GasCo has a dedicated Security Operations Center (SOC) team that manages their IP video surveillance infrastructure and data. This includes realtime monitoring and remote recording of the convenience stores and forecourt areas where cameras are installed.

These feeds get interrupted sometimes and glitches are observed. These systems are imperative for their safety and loss protection and additionally, American GasCo cannot afford degraded service with this compliance monitoring data. As a result, the teams responsible for resolution of these systems are physically dispatched onsite with little or no information about the possible issues. Often, they are required to make multiple trips to first identify and then resolve the issues.

With the deployment of the SDRA solution, an explicit Service VPN has been created only for these teams to troubleshoot remotely and take necessary actions to bring them online in the network. Sitting remotely, they can open target applications, isolate if the problem exists with their cameras/NVR's, their integrated 8-port Ethernet switch, or their network. This led to faster resolutions and a considerable decline in count of Remote Hand dispatches, thus reducing OPEX cost per incident.

Figure 4. Remote Troubleshooting of IP Surveillance Cameras Use Case



Performance Monitoring of the Convenience Stores VPN

American GasCo has a small IT staff responsible for maintaining the SD-WAN network and IT systems at each of their stores. Performance management was traditionally a reactive process, where users called the helpdesk to report outages or network slowdowns. This is unacceptable in a gas station environment since slow performance can translate to lost revenue as frustrated customers cannot process credit card transactions at the pump.

Performance monitoring improved with the deployment of SD-WAN, as the operations teams could use the SD-WAN Manager for centralized monitoring health and tunnel performance between WAN Edge routers. This, however, still did solve the challenge of isolating the root cause of "slow performance problems". Does the problem lie in the network, device, or software?

With Cisco ThousandEyes visibility into SD-WAN health, organizations can deploy agents at remote sites to simulate application transactions to better gauge the application experience. Cisco ThousandEyes has three type of agents:

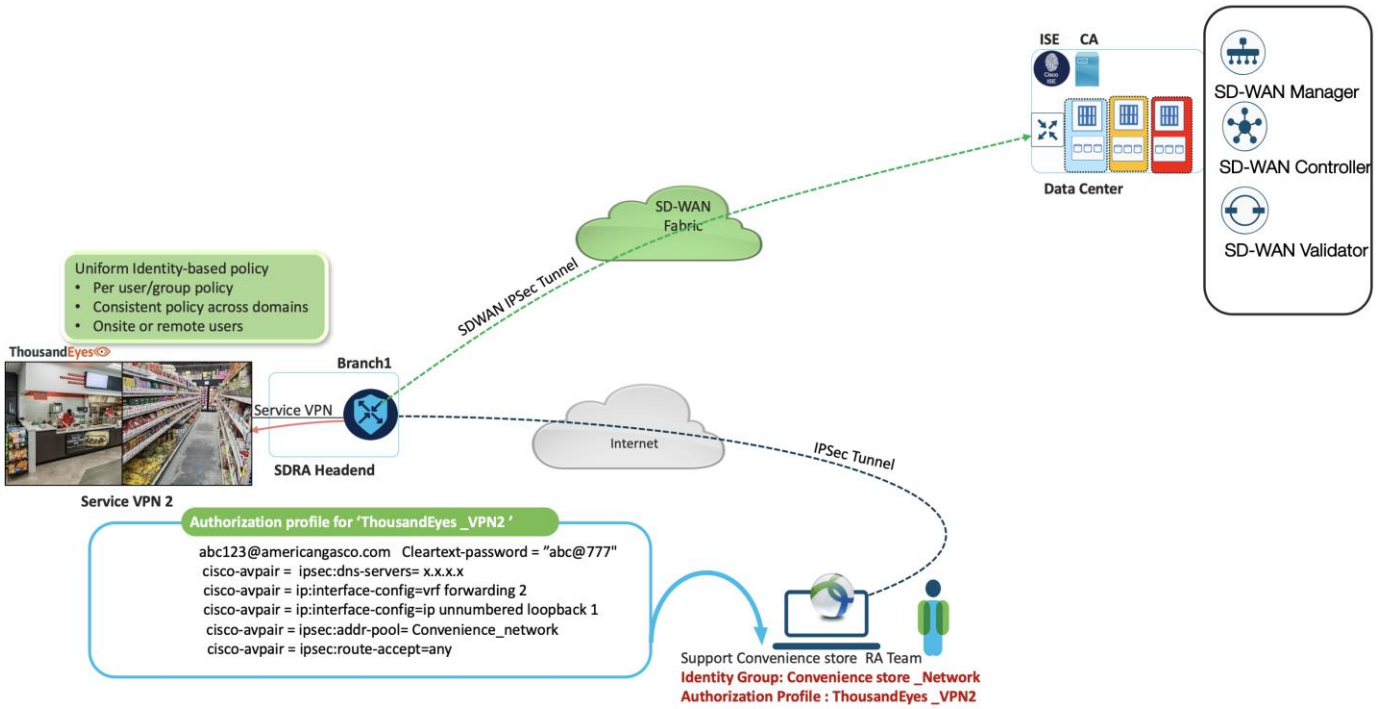
- **Enterprise Agent:** A lightweight software-based agent, easily installed on your own network, that provides visibility within the enterprise campus, data centers, virtual private clouds/virtual networks, and branches. It also supports active monitoring, SNMP-based monitoring, and topological mapping of internal network devices.
- **Cloud Agent:** A globally distributed agent installed and managed by ThousandEyes in 200+ cities to give users access to performance data from local transit providers and last-mile ISPs to simulate end-user performance.
- **Endpoint Agent:** A lightweight service installed on end-user laptops and desktops that provides proactive and real-time monitoring of application experience and network connectivity.

While this was interesting to American GasCo, the ISR 1100 WAN Edge platforms they had deployed at the majority of their sites did not support enterprise agents, and none of the locations had traditional laptops or desktops that could run the endpoint agents. By deploying SDRA, American GasCo was able to create a LAN extension that allowed remote users with agent endpoints deployed to monitor performance.

With the deployment of the SDRA solution, an explicit VPN is created for ThousandEyes to support the network monitoring teams to establish hop-by-hop visibility into the entire network path, including detailed path and performance metrics for internally hosted applications for Service VPN 2.

This enables American GasCo to spot issues quickly and remediate them before they have a major impact on their business.

Figure 5. Performance Monitoring Use Case



Network Merger

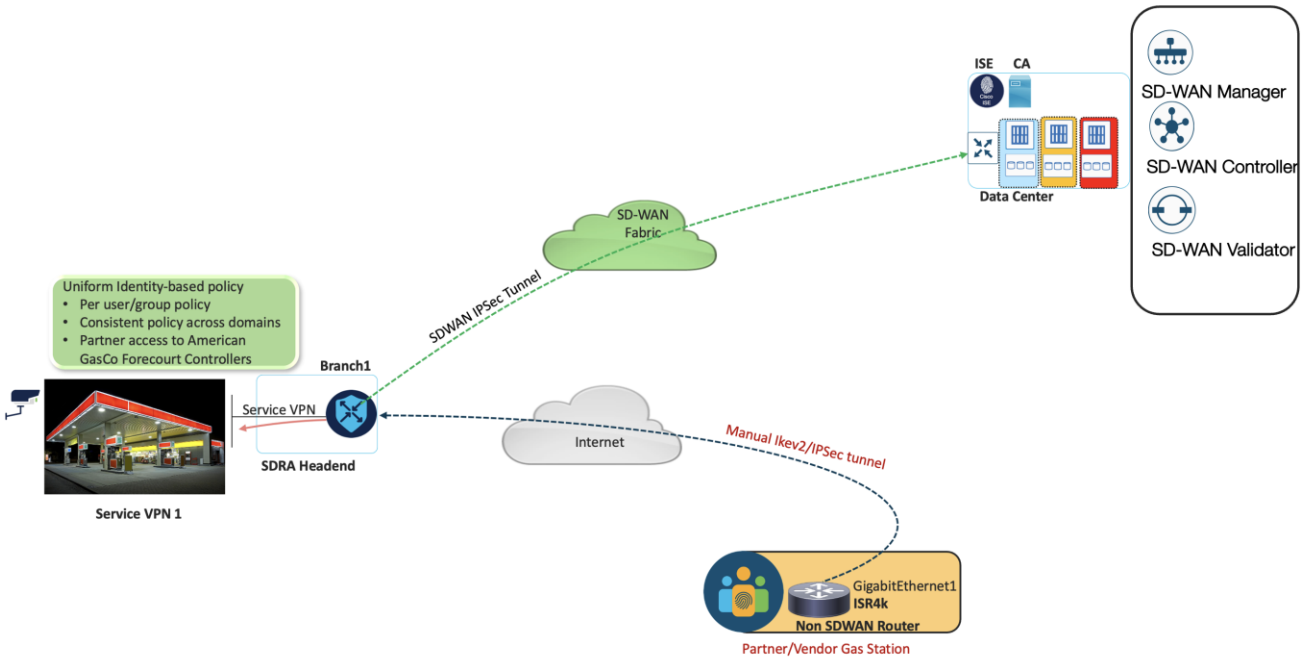
American GasCo recently made an acquisition with another small gas station company called EnergyCo. The EnergyCo infrastructure has Cisco ISR4ks deployed at their sites.

There is a requirement to enable communication between EnergyCo and American GasCo stations so all the infrastructure can be centrally managed by the same team, and all American GasCo services can be made available at EnergyCo stations.

Partner sites can easily provision their ISR4k (non-SD-WAN routers) to connect to SDRA routers using traditional IPsec. ISE will be used to authorize them to provide access to VPN 1 of the American GasCo FCC system. The SDRA solution allows easy and simple accommodation on partner services and makes them a part of the SD-WAN overlay without any front-end CAPEX or OPEX investment.

For the IPsec router configuration at the partner/vendor site, refer to Appendix A.

Figure 6. Network Merger Use Case



Appendix A: IPsec Configuration at Vendor Site

```
crypto ikev2 proposal American_Gasco
 encryption aes-cbc-256
 integrity sha1
 group 14
!
crypto ikev2 policy American_Gasco
 proposal American_Gasco
!
crypto ikev2 keyring keyring1
 peer American_Gasco
  address x.x.x.x (WAN IP address on SDRA Router)
  pre-shared-key Cisco2022
 !
!
!
crypto ikev2 profile American_Gasco
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring1
 no config-exchange request
!

crypto ipsec transform-set American_Gasco esp-aes 256 esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile American_Gasco
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set American_Gasco
 set pfs group16
 set ikev2-profile American_Gasco
!
!
interface Tunnelxx
 ip address 20.20.20.2 255.255.255.252
 ip mtu 1500
 tunnel source a.a.a.a (Local Internet Interface IP address on this Router)
 tunnel mode ipsec ipv4
 tunnel destination x.x.x.x (WAN IP address on SDRA Router)
```

```
tunnel path-mtu-discovery
tunnel protection ipsec profile American_Gasco
```