Cisco Catalyst SD-WAN Security-Sensitive Branch Design Case Study

Tidal Pharmaceuticals SD-WAN Design (Phase 1)

February 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
- Cloud First
- Remote Worker

This case study focuses only on security-sensitive WAN. To learn more about the other case studies, refer to https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/Cisco_SDWAN_Case_Study_Intro.html.

About This Case Study

The security sensitive WAN case study takes a deep dive into a branch SD-WAN connectivity and security design for a fictitious healthcare sector customer, Tidal Pharmaceuticals. The purpose is to provide the reader with an awareness of how security-sensitive customers are leveraging Cisco Catalyst SD-WAN and security to protect remote branch locations connecting to both private and public clouds. Although Tidal Pharmaceuticals is not an actual company, the designs featured in this case study incorporate best practices from security-sensitive SD-WAN deployments in industries where IT security is a top-of-mind priority.

The topics discussed within this case study are organized as follows:

- Cyber Security Threats
  - Internal and External Threats
  - Mitigating Threats
- Cisco Catalyst SD-WAN Secure Architecture
  - Control Plane Security
  - Data Plane Security
  - Management Plane Security
  - Firmware Security
  - Cisco Catalyst SD-WAN Threat Protection for Branch Users and Devices
- Tidal Pharmaceuticals
  - Customer Background
  - Legacy WAN Network
  - Decision to Adopt the SD-WAN Solution
- Tidal's Cisco Catalyst SD-WAN Design
  - High-level Design
- Tidal's Cisco Catalyst SD-WAN Data Center Design
- Tidal's Cisco Catalyst SD-WAN WAN/LAN Branch Design

    - Type 1 – Small Sales Office
    - Type 2 – Medium Shared Sites
    - Type 3 – Large R&D Facilities
- Tidal's Cisco Catalyst SD-WAN Branch Security Design
    - Guest VPN
    - Sales and Clinical VPN
    - R & D VPN
- Case Study Conclusion

This guide is not intended to be a step-by-step "how to" guide for deploying Cisco Catalyst SD-WAN, although enough details are provided for the reader to understand what features and configurations are required on the branch WAN Edge routers. All use cases and feature combinations were prototyped in a Cisco lab environment using 20.6 Manager/17.6 IOS XE SD-WAN code versions. Supporting documentation can be found in the Cisco Catalyst 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 and security architects that need to understand the secure SD-WAN design best practices to make good design choices for an organization's Cisco Catalyst SD-WAN implementation.

Cybersecurity Threats

When making the move to transformative technologies such as SD-WAN and cloud computing, many organizations focus on the business benefits and network innovations without fully considering the security implications of the change. Security teams have historically been excluded from WAN procurement and design conversations as branch applications were typically delivered over private circuits or encrypted VPN tunnels from private data centers protected with an enterprise security stack and considered to be trusted and secure. Internet traffic to and from the branch was typically backhauled over the same secure WAN connections to the data center locations that would forward to enterprise security stacks in DMZs that defined the internal network perimeter. Historically, this "castle-and-moat" approach to security seemed workable, where everyone inside the network perimeter (castle) was considered "good", and everyone outside (the moat) was "bad".

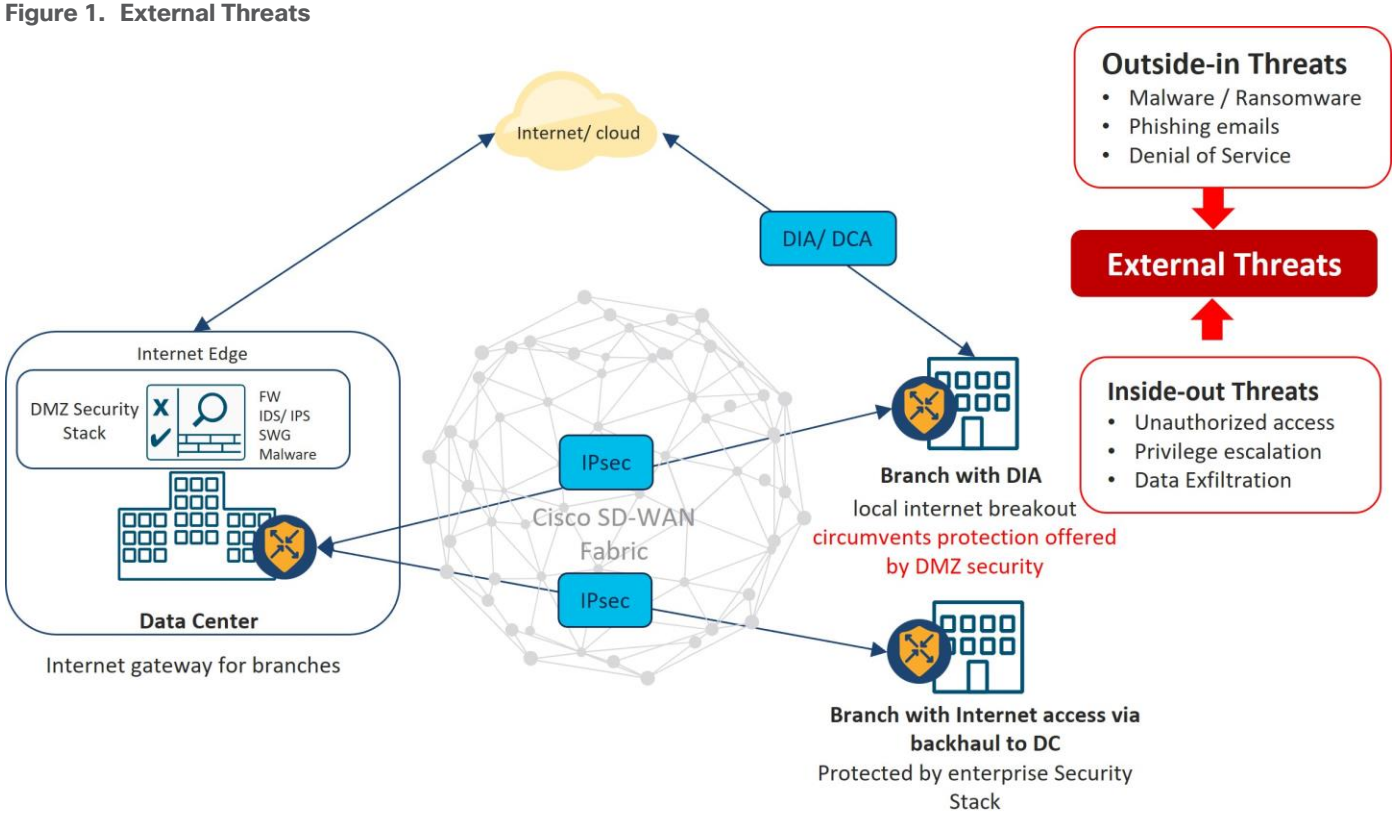
With the advent of SD-WAN and shift to cloud computing, the network perimeter has become more difficult to define and contain. Early adopters of SD-WAN clamored to procure Internet transports for their underlay transport as a cheap, high bandwidth alternative and quickly realized a return on investment. These early adopters were often among the first to leverage SaaS applications and migrate their enterprise applications to cloud data centers, and first to realize that backhauling traffic to centralized data center breakouts and legacy security stacks would not scale or perform to the level of a local Internet breakout at the branch. The enthusiasm of the network teams eager to deploy branch SD-WAN use cases such as Direct Internet Access (DIA) and Direct Cloud Access (DCA) was met with equal dismay by the security teams responsible to protect a greatly expanded network perimeter from external threats on the Internet. It wasn't long before the security teams had a seat at the WAN design table, especially in regulated industries such as financial and healthcare, but also in government and other industries where the crown jewels must be protected not only from bad actors outside the "moat", but also from willing or unwilling users inside the "castle".

All good network engineers know that the first step in network design is gathering a set of business objectives and technical requirements for connectivity. Cybersecurity engineers, on the other hand, are concerned with assessing business risks and understanding cyber security threat trends. While these trends are ever changing,

they can loosely be categorized as being external (outside the moat) threats, or internal (inside the castle) threats.

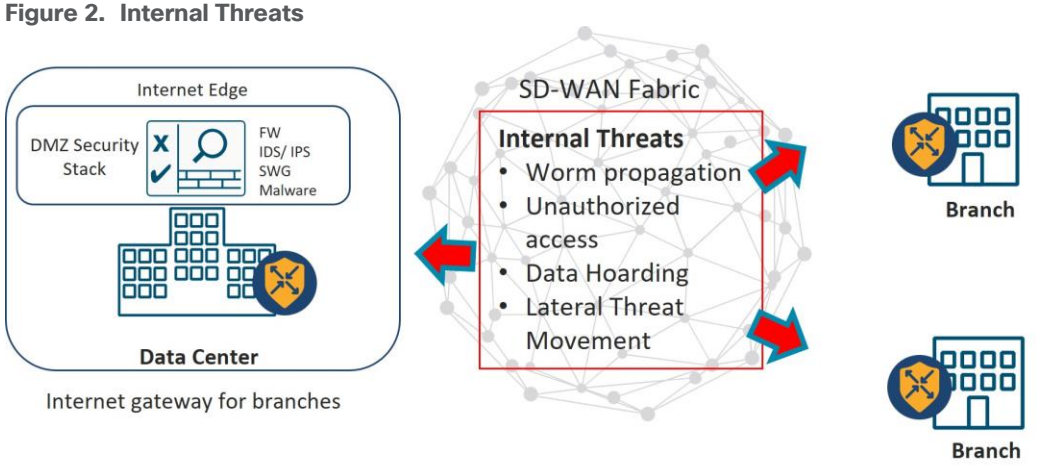
External threats can be further classified as “outside-in” or “inside-out”. Examples of “outside-in” threats include denial of service attacks, phishing emails, and viruses such as trojan horse, malware, ransomware, and crypto mining. Examples of “inside-out” threats include unauthorized access, privilege escalation and data exfiltration. Deploying branch SD-WAN use cases such as DIA/DCA without security mechanisms increases the risk of external threats as they present an opening in the perimeter.

Figure 1. External Threats



Examples of internal threats include virus and worm propagation, unauthorized access, data hoarding, and lateral threat movement. While SD-WAN does not necessarily increase exposure to these threats, the any-to-any connectivity nature of the fabric could potentially accelerate their proliferation once entry has been gained to the inside.

Figure 2. Internal Threats



Mitigating Threats

Effective cybersecurity is an ongoing practice, based on a set of layered defenses. To mitigate these threats from the network, the following technologies and practices are often leveraged, although this is not an exhaustive list:

- Network Segmentation: Network segmentation divides a network into multiple isolated segments or subnets, where each segment can have varying policy and security requirements. This allows you to protect critical assets and helps minimize the number of hosts an attacker can exploit, thus inhibiting the ability for an attacker to spread laterally within an organization if segmentation is done properly.
- Firewalls: Traditional firewalls are used to monitor incoming and outgoing traffic, and permit or block traffic based on policy. Session state can be monitored and ports automatically opened to allow returning outside traffic, while denying other traffic not initiated from the inside network. In addition, deep inspection can be performed to validate legitimate protocol traffic. Firewalls can be either appliance or software-based, and on-premises or cloud-based.
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS): IDS and IPS monitor network traffic and can detect and alert on known threats and suspicious or malicious activity and anomalies. An IPS can monitor and alert as well as block suspicious traffic. These systems can be appliance or software-based and on-premises or cloud-based.
- Advanced Malware Protection (AMP): Malware is malicious software, which includes spyware, adware, ransomware, worms, viruses, and trojans. Malware protection is designed to prevent, detect, and help remove these threats. AMP can be integrated into different network components, including firewalls and network endpoints.
- Secure Web Gateway (SWG): A Secure Web Gateway (SWG) protects users in a network from web-based Internet threats and allows a company to determine what websites employees can visit. Websites can be filtered by URL, domain, or category and web-based applications can be controlled, such as files sharing and cloud storage tools to prevent data loss. The gateway can also inspect files to see if they may pose a risk and block files that contain malicious code.
- DNS/Web-Layer Security: Monitoring and flagging anomalous DNS activity can enhance network protection and stops attacks earlier.
- Cloud-Access Security Broker (CASB): CASB is essential to a security architecture and serves as an intermediary between users and the cloud services that they rely on for day-to-day activities. It allows

security or IT teams to enforce policies that govern users' access to and use of cloud services to prevent data loss, ensure regulatory compliance, and reduce the risk of cyberattacks on the company network.

- URL Filtering: URL filtering compares web traffic against a policy which permits or denies certain websites based on URL.
- Virtual Private Network (VPN) and Encryption: Encryption is the encoding of information which can only be accessed by a user with the correct encryption key. It is used to deter outsiders from accessing sensitive data.
- Zero-Trust Security Controls: The idea of Zero Trust is to prevent unauthorized access to data and systems and where enforcement is as granular as possible. Identity has become more important here due to the disappearance of the traditional network perimeter.
- Network Visibility: Effective risk management requires ongoing monitoring, network visibility, and response. Syslog, SNMP, NetFlow, and auditing logs are important parts of this.
- SSL/TLS Proxy: The SSL/TLS Proxy feature allows an Edge device to decrypt incoming and outgoing SSL-encrypted traffic to facilitate inspection by other Cisco Catalyst SD-WAN security features which can identify risks in the payload that would otherwise be hidden by encryption.

Threat mitigation can be performed by security devices located on-premises or in the cloud. With on-premises deployments, devices can be inserted in strategic locations where all traffic is funneled through them for inspection, offering protection from both internal and external threats. When deployed in the cloud, all Internet and SaaS traffic from a site is redirected to a cloud security provider via tunnels which must pass through a service chain of security checks before it is allowed to be sent to the Internet destination or return to the site. Cloud security does not have visibility to site-to-site traffic and cannot protect against internal threats coming in from other sites on the SD-WAN fabric or backdoor links. With a cloud service, Internet traffic can be protected at much higher rates than on-premises since cloud resources are elastic as opposed to on-site firewalls or UTM appliances where it is fixed.

Cisco Catalyst SD-WAN Secure Architecture

Cisco Catalyst SD-WAN Foundational Security Principles

In a changing world with greater information and cyber security threats, the digital technology industry is adopting stronger standards for compliance. The Cisco Catalyst SD-WAN solution offers exceptional measures for compliance and bases its control plane and data plane design around the following principles in order to secure the overall Cisco Catalyst SD-WAN network infrastructure:

- Authentication: Authentication validates the identity of a user or device. The Cisco Catalyst SD-WAN solution ensures that only authenticated devices are allowed to communicate with each other to form connections and send traffic to one another.
- Authorization: Authorization is the process of verifying what authenticated users or devices can have access to.
- Encryption: Encryption converts data into an encoded, unreadable format. All communication between each pair of devices is encrypted by default, so it is automatically secure and there is no configuration overhead involved in securing the links.
- Integrity: Integrity is protecting data from modification by an unauthorized party.

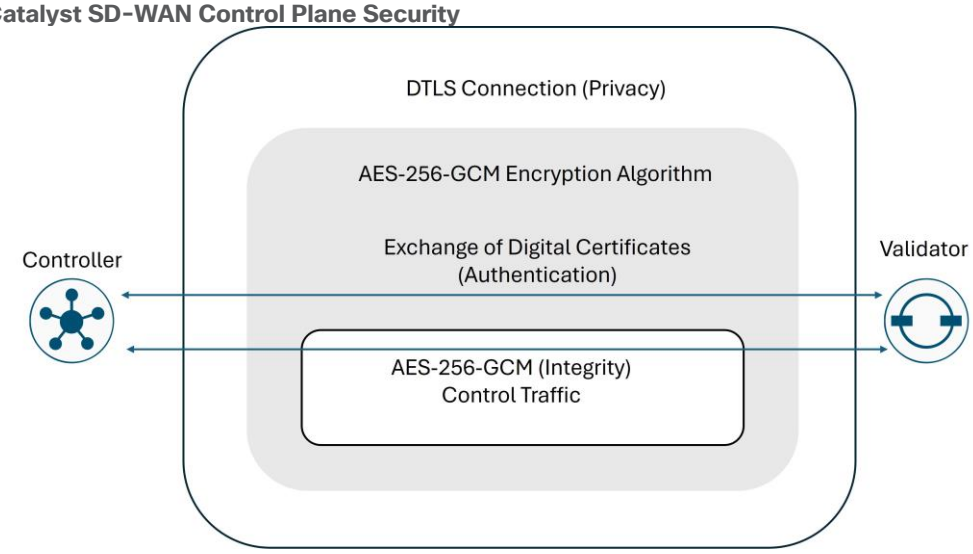
Cisco Catalyst SD-WAN Control Plane Security

While control plane in a network often references the network routing topology which decides where traffic flows, it also includes the control connections between the control components (SD-WAN Validators, Controllers, and Managers) and between the WAN Edge routers and the control components so the necessary control communication can take place. The Cisco Catalyst SD-WAN control plane is designed with network and device security in mind to ensure that all control traffic is confidential, secure, and unable to be manipulated by unauthorized devices or users.

The Cisco Catalyst SD-WAN fabric incorporates a zero-trust security model within its control plane, ensuring that all elements of the fabric are authenticated and authorized prior to admittance to the network. This model is built on the use of digital certificates to establish the identity of each fabric element which is used in authentication. The certificates are used to establish secure Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) control channels between the control components and between the WAN Edge routers and the various control components. TLS and DTLS use Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all control traffic sent over the control connections. AES-256-GCM is also used for integrity, to ensure traffic has not been tampered with.

Within these secure control channels, Overlay Management Protocol (OMP), Network Configuration protocol (NETCONF), and Simple Network Management Protocol (SNMP) can flow, allowing the control components to propagate configuration and networking information. OMP also ensures the secure, automatic propagation and management of encryption keys used by the data plane. In the pairwise keys model, the Controller sends Diffie-Hellman public values to the WAN Edge devices, where they generate their own pairwise IPsec encryption keys.

Figure 3. Cisco Catalyst SD-WAN Control Plane Security



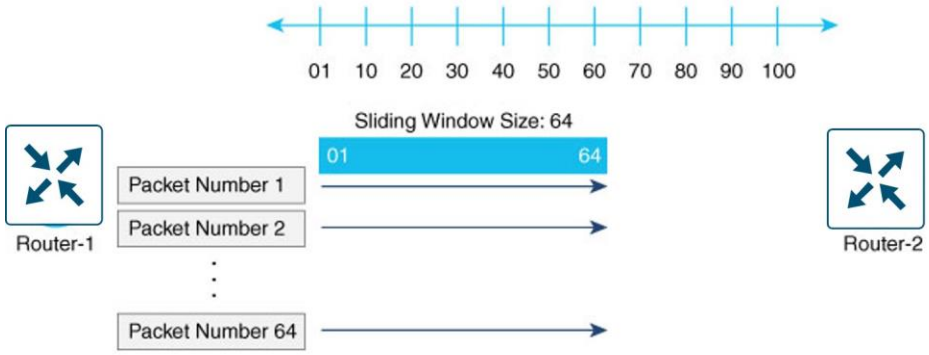
Cisco Catalyst SD-WAN Data Plane Security

The Cisco Catalyst SD-WAN fabric provides data plane communication between its WAN Edge devices that carries user traffic across the WAN network. In typical WAN solutions, data plane security is most recognized in the form of IPsec encryption between routers, though its responsibility does not end there. Many regulatory agencies require both traffic isolation and firewalling in addition to encryption to be compliant.

For the data plane, authentication is enforced by using both a key exchange model and an enhanced version of the Encapsulating Security Payload (ESP) protocol. The enhanced version of ESP also protects the data packet's payload through encryption using the AES-GCM-256 cipher. For integrity, this ESP version uses an AH-like mechanism to check the integrity of the IP and UDP headers, and anti-replay protection is also used. In anti-

replay protection, a sender assigns a set monotonically increasing sequence numbers, and the destination checks these sequence numbers to detect duplicates. Because packets often do not arrive in order, the destination maintains a sliding window of sequence numbers that it will accept.

Figure 4. Anti-Replay for Integrity Checking



As with encryption, traffic isolation is a key element of any compliance strategy – both for its intrinsic benefits as well as the operational benefit it provides when constructing firewall policy based on segmentation. In the Cisco Catalyst SD-WAN solution, segmentation is initiated in the control plane, but it is enforced within the data plane to separate user routing tables using VPNs or VRFs and via zones to create separate security zones.

Cisco Catalyst SD-WAN Management Plane Security

The Cisco Catalyst SD-WAN solution provides a management plane through the SD-WAN Manager Network Management System (NMS) and provides management compliance by controlling who can access, read, and modify configurations and policies. This is achieved through Role-Based Access Control (RBAC) and listing of allowed source IP addresses using Access Control Lists (ACLs) to control which users and devices in the network can access the monitoring and management portal, the SD-WAN Manager NMS.

In addition to all the security features and capabilities listed above, Cisco Catalyst SD-WAN also protects the control plane, data plane, and management plane from unauthorized traffic and threats such as distributed denial of service (DDOS) attacks through control plane policing and implicit access-control policies that drop packets received on WAN transport interfaces from untrusted sources and applications.

Cisco Catalyst SD-WAN Firmware Security

The Cisco IOS-XE routers contain a proprietary, tamper-resistant hardware security chip called the Trust Anchor module (TAm) that is programmed with a signed certificate during manufacturing. It features non-volatile secure storage for generation and storage of key pairs as well as the Secure Unique Device Identifier (SUDI). When the routers join the SD-WAN network, they exchange their certificates with the SD-WAN control components as part of the authentication process. The router's private key is never distributed and cannot be accessed, and any attempt to access it will cause the hardware security chip to fail, thereby disabling all access to the router.

Cisco Catalyst SD-WAN Threat Protection for Branch Users and Devices

The foundational SD-WAN security features described to this point are intended to protect the integrity of the SD-WAN infrastructure from attacks targeted at the control components and WAN Edge routers themselves. Threat protection for branch users and devices refers to features that protect against threats targeted towards branch user computers and other devices from threats such as DDOS, unauthorized access, viruses, malware, and ransomware. Branch security with Cisco Catalyst SD-WAN can be deployed in different ways:

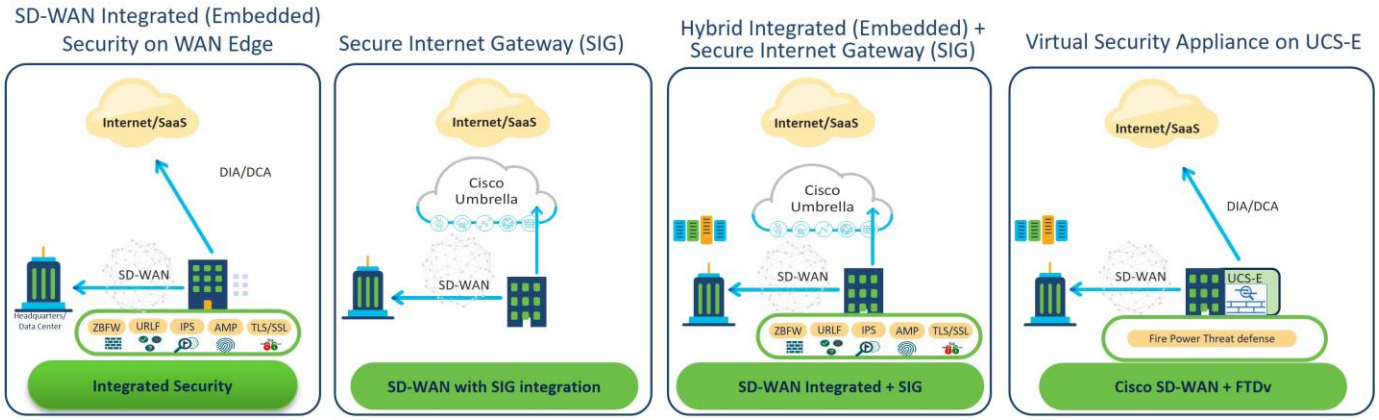
- Integrated (Embedded) Security Features on WAN Edge routers: This refers to the WAN Edge router IOS-XE security features, such as Firewall with Application Awareness (Zone-based FW), Intrusion Prevention Systems with Cisco Talos Signatures (IPS/IDS), URL Filtering (URLF), Advanced Malware Protection (AMP), SSL/TLS proxy, and DNS/Web-layer Security with Umbrella Integration. These features can be configured and monitored by the SD-WAN Manager to facilitate a single pane of glass. Embedded security features on the router can be deployed to inspect some or all traffic leaving or entering from the WAN, protecting sites from internal and external threats. Something to consider when choosing to deploy embedded security features is the impact to WAN Edge router forwarding rates due to resource contention for the fixed CPU resources. Careful planning should be taken when selecting the branch platforms and security features selected to be deployed.

  With the integration of Cisco Umbrella with DNS/Web-Layer Security, an additional layer of protection is added for all branch users, wherein all DNS requests received by the WAN Edge device within a site are redirected to Cisco Umbrella, a cloud-based security service for further inspection. Within Cisco Umbrella, the request is processed and either returned with the IP address of the web service or the client is redirected to a blocked webpage.

  For additional details on integrated security design concepts, see the Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices.

- Secure Internet Gateway (SIG): The Cisco Catalyst SD-WAN router redirects user traffic to a Secure Internet Gateway (SIG) or Cloud Security Provider (CSP) on the Internet, which provides the security features needed to protect the traffic against external threats. The provider can be Cisco Umbrella or another third-party cloud security provider (such as Zscaler) and is connected to the SD-WAN router, typically through a secure IPsec tunnel. This solution offers consistent user and device protection for all branches and allows scaling as needed. Unfortunately, it lacks visibility and control over internal traffic and threats.
- Hybrid Integrated (Embedded) + Security Internet Gateway (SIG): This combination is the best of both worlds, which enables security features on the Cisco Catalyst SD-WAN routers as well as redirects traffic to a Secure Internet Gateway (SIG). Security policy can dictate which security features are applied to which traffic while data policy and/or routing can direct traffic to the SIG. Traffic can be covered by one, both, or neither of the security methods. This is the best balance of security and user experience for Direct Internet Access (DIA).
- Virtual Security Appliance on UCS-E Server Module: With this model, on-premises branch security is delivered by a virtualized security appliance, such as Cisco Secure Threat Defense virtual (FTDv), hosted on a UCS-E module in a SD-WAN Edge router. This branch solution protects against both internal and external threats while affording maximum performance and throughput as the security and routing tasks are handled by different CPUs. This solution also allows customers to deploy preferred virtualized threat defense products offered by 3rd party vendors.

Figure 5. Cisco Catalyst SD-WAN Branch Protection

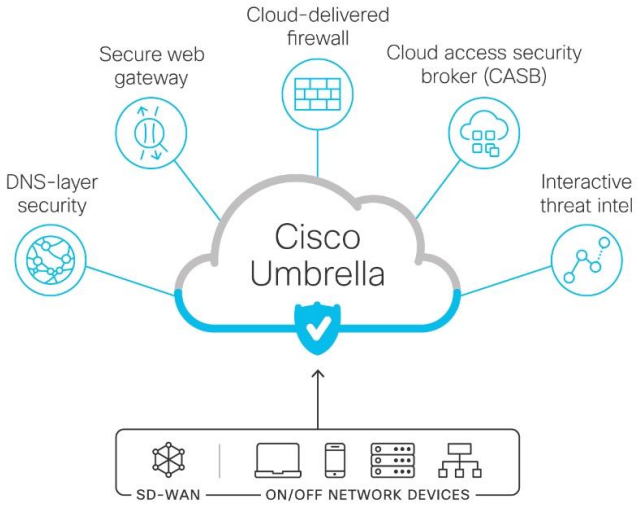


Cisco Umbrella

Cisco Umbrella combines several security functions in a single cloud-delivered service which is easy to manage and deploy. Umbrella can function alone for DNS-layer security, where the WAN Edge router can redirect DNS traffic to Umbrella for further inspection. Umbrella then passes back an IP address of the web service, or it can block the page, depending on the inspection result.

Cisco Umbrella can also function as a Security Internet Gateway (SIG), where it can integrate with a WAN Edge router, which connects to the SIG through an IPsec tunnel and redirects traffic to the SIG either through routing or a data policy. In addition to DNS-layer security, Cisco Umbrella can offer services such as a secure web gateway, cloud-delivered firewall, cloud access security broker (CASB), and interactive threat intelligence.

Figure 6. Cisco Umbrella



Cisco Secure Firewall Threat Defense Virtual (FTDv)

Cisco Secure Firewall Threat Defense Virtual (formerly FTDv/NGFWv) is a virtualized security option that combines Cisco's proven, robust, and Enterprise-class level network firewall by adding capabilities like virtual private network (VPN), application visibility and control (AVC), Next-Generation IPS (NGIPS), URL filtering, and advanced malware protection with consistent security policies across physical, private, and public cloud environments. This virtual firewall portfolio simplifies security management with the ease of configuring, logging, monitoring, and reporting risks using the centralized Cisco Firewall Management Center (FMC). The Cisco FMC

provides visibility into the branch network to quickly detect threat origin and activity and stops attacks before they impact the day-to-day network operations.

Cisco Catalyst SD-WAN Network Visibility

To detect and remediate campus and internet routing problems, ITOps needs total visibility from campus to branch to applications to quickly isolate problem areas whether they reside on the enterprise network side, a service provider's path, or the application hosting side. They need deep observability to rapidly pinpoint the root-cause of performance issues in a multicloud environment before issues impact business revenue and reputation.

Cisco Catalyst SD-WAN offers several network and threat visibility and traffic analytics options:

- Cisco Catalyst SD-WAN Manager GUI/Cisco Catalyst SD-WAN Edge Routers: The monitoring and troubleshooting methods available within the SD-WAN Manager GUI offer visibility into branch traffic flows. Application visibility also gives insight into network traffic flows. When something of interest happens on an individual device in the overlay network, the Edge device reports the alerts and events by sending a notification to the SD-WAN Manager. The SD-WAN Manager then consolidates major and critical events into alarms for visibility into the branch networks.

  In addition, features such as system logging, SNMP, and NetFlow support exporting detailed log messages to an external collector/syslog/SNMP server for analyses, allowing additional insights into network events.
- Cisco Catalyst SD-WAN Manager GUI/Integrated (Embedded) Security on SD-WAN Edge Routers: The security services (ZBFW, IPS/IDS, AMP, etc.) running on the SD-WAN Edge Routers provide statistics and logging of events and alerts to the SD-WAN Manager GUI to provide information into the operation of each system and more visibility to network traffic.
- Cisco vAnalytics: Cisco vAnalytics is a Cisco Catalyst SD-WAN cloud-based analytics service with a graphical interface that offers comprehensive insights into application and network performance.
- Cisco Umbrella SIG and Secure DNS: Integration of Cisco Catalyst SD-WAN with the Cisco Umbrella platform provides the domains for management, visibility, segmentation, secure services, threat defense, and compliance across the Cisco Catalyst SD-WAN network. Cisco Umbrella offers visibility and traffic analytics in the Umbrella dashboard to monitor the traffic redirected from the Cisco Catalyst SD-WAN network for possible threats.
- Cisco ThousandEyes Internet and Cloud Intelligence: The integration of Cisco Catalyst SD-WAN with Cisco ThousandEyes enables IT to gain deep insights from the enterprise campus across Internet, cloud, and SaaS infrastructures. The union of SD-WAN routers and ThousandEyes provides not just underlay and performance visibility for overlay fabrics such as site-to-site tunnels, but also into data center VPC/VPN endpoints, branch-to-cloud proxy tunnel endpoints, and branch to SaaS.
- Cisco Stealthwatch, or Secure Network Analytics: Cisco Catalyst SD-WAN branch traffic flows can also be analyzed using Stealthwatch, or Secure Network Analytics. The platform continuously monitors the network and cloud traffic and pinpoints any hidden threats before they turn into a major incident. It analyzes your network data to help detect threats that may have found a way to bypass your existing controls before they can do serious damage.

Tidal Pharmaceuticals

Customer Background

Tidal Pharmaceuticals is a global pharmaceutical company that leverages science, technology, and people to develop vaccines and specialty medicines that aim to prevent and treat disease. Tidal is a leader in research and development initiatives that focus on scientific innovation to deliver medicines and vaccines to help millions of people around the world. To meet a global market, Tidal maintains and orchestrates a large ecosystem of partners in a few subindustries to develop, produce, market, and sell medicines. Many of the partners in this ecosystem must have access to and control extremely sensitive and valuable information including scientific R&D data, formulas for patented drugs, clinical trials protocols and personal data that includes patient health information. When handling personal data, Tidal must comply with regulations that apply directly to them such as consumer protection and FTC regulations, laws that apply to their customers such as HIPAA, and a growing number of international laws that impose greater restrictions on the use of information such as Europe's forthcoming General Data Protection Regulation (GDPR).

Legacy WAN Architecture

Tidal's legacy WAN fabric was built with a combination of MPLS service provider L3VPN and DMVPN over Internet transports, connecting a national chain of sales, clinical trials, business partner, and R&D offices with enterprise applications in their private data centers. Tidal has been slow to adopt cloud computing, particularly in the heavily regulated R&D and patient outreach arms of the business, where privacy and data integrity is key. Being less regulated, the sales organization began using SaaS applications as part of an IT refresh and migrated to Microsoft Office 365. This was followed with sales adoption of Salesforce, Cisco Webex, and Box secure content management SaaS applications. Internet and SaaS application access for remote sites was provided by backhauling across the MPLS and DMVPN transports to the data center sites which functioned as centralized Internet gateways. Internet traffic to/from remote sites was forwarded through a service chain of enterprise firewalls, web proxies, email security, and IPS appliances to inspect and mitigate against external threats.

Legacy Data Center Design

Tidal Pharmaceuticals owns and operates a pair of on-premises data centers (DCs) that host enterprise applications in local server and storage farms and offer centralized services such as the secure Internet gateways for its remote sites. Each DC functions as a WAN hub where remote site traffic is aggregated onto high-bandwidth transports by WAN routers that forward traffic to its destination by way of a security layer that determines whether it should be filtered or forwarded to its intended destination in the DC or out on the Internet. The data centers are located on each North American coast and interconnected via redundant high speed MPLS circuits that form a data center interconnect (DCI). Each data center site includes redundant Nexus 9K switches, ASR1K routers, UCS servers and storage, and Firepower next generation firewalls to ensure business continuity by eliminating any single point of failure. The data center security architecture is built upon a layered approach of threat prevention, detection and mitigation components following the methodologies and recommendations made in the Cisco SAFE architectural blueprint for a secure data center design.

Legacy Branch Design

Tidal Pharmaceuticals has approximately 60 remote sites with 50% being single-router sites and 50% are dual-router sites, for a total of 90 routers. The remote sites are one of three site types with legacy LAN and WAN connectivity as described below:

- Small Sales offices: These offices (30 single-router sites) typically host 5 to 10 employees, including the sales representatives, managers, executives, and guests that may visit. A typical office layout includes several small rooms and a larger meeting room with a Telepresence conferencing unit. Devices in the

small office include workstations, IP phones, network printers, and video surveillance cameras. The legacy network design consisted of a single workgroup LAN switch, 1-2 WLAN access points, and a Cisco ISR-G2 router connecting to a single MPLS circuit providing 50 Mbps to 100 Mbps of WAN bandwidth. A guest Wi-Fi service was implemented separately from the corporate network, using local provider hotspot services to connect guest Wi-Fi computers and other devices.

- Medium shared sites: These sites (20 dual-router sites) typically host up to 25 people, including Tidal sales representatives, managers, guests, clinical trials specialists, and business partners that work on-site during various phases of clinical trials. The bandwidth and business criticality for medium sites is significantly higher than small sales offices due to the research functions that are conducted at these locations. Large file transfers of medical images and rich media during clinical trials push the site bandwidth requirements from 300 to 500 Mbps, with nightly backups requiring 24x7 WAN availability. To meet these stringent high availability targets, the legacy network design included redundant LAN switches and routers with an ISR4K CE router connected to MPLS for primary WAN connectivity and a second ISR4K DMVPN router connected to Internet for backup. BGP was deployed as the dynamic routing protocol for both MPLS CE-PE routing and DMVPN overly routing over the ISP/Internet transport. Extensive access control lists were deployed to keep the sales and clinical research/business partner traffic separated, and all guest Wi-Fi was provided through local provider hotspots like the small sales offices.
- Large R&D facilities: These facilities (8 dual-router sites) typically host 30 or more employees working in various R&D capacities that are critical to the Tidal business. The R&D department manages highly sensitive data, including patented drug details and patient clinical trial data requiring the highest degree of scrutiny. In addition to the office automation equipment found in small and medium sites, large R&D facilities often include local servers, automated lab equipment, and specialized R&D CAD systems with high-performance microprocessors. High availability is crucial to large R&D facilities that require 24x7 high-speed connectivity to applications in the private data centers. The network design consisted of a pair of dual LAN switches, dual ISR routers with dual MPLS transports ranging from 600 Mbps to 1 Gbps. Internet connectivity for large R&D facilities was backhauled across MPLS regional data center gateway sites where it is subject to security screening and threat protection.

Decision to Adopt the Cisco Catalyst SD-WAN Solution

There were several network and security concerns that prompted Tidal to refresh its WAN infrastructure:

- Branch devices approaching End-of-Life (EOL)/End-of-Sales (EOS): A majority of the branch network and security equipment was reaching end of support, making it subject to security vulnerabilities and defects that presented a risk to the business. As part of the new WAN infrastructure, Tidal decided to refresh their branch routers, switches, and WLAN access points that were nearing EOL milestones.
- Adaptation to Cloud/SaaS: An evaluation of traffic patterns at the small sales and medium offices indicated that 80-90% of traffic was destined to the Internet after the sales organization migrated to Office 365, Salesforce, Webex, and Box. These shifting traffic patterns made it no longer practical to backhaul branch Internet traffic to the data center Internet gateways that were becoming congestion points in the network and affecting performance, prompting Tidal to pursue a solution that would enable local Internet exits at the branch. This service could be extended to guest Wi-Fi so that the costly hotspot solution could be decommissioned.
- Replacement of MPLS with Internet WAN transport at the branch: Tidal decided to replace their existing MPLS transport with high-speed Internet circuits where they were able to get much higher bandwidth at a lower cost. Additionally, these circuits could be used for local breakouts to Internet and Cloud, improving

performance for corporate SaaS connectivity and offering a cheaper alternative for guest WiFi than the provider Hotspot services.

- Increased pressure to improve branch security: Fears of rising cybersecurity threats such as malware and ransomware placed more pressure on Tidal's NetOps team to work with SecOps to build a next generation WAN capable of detecting and defending against attacks. This included threats to the infrastructure such as Denial of Service (DoS), threats to individuals such as phishing, and threats to applications such as Viruses and Malware. Any local Internet exit solution would require threat protection with either on-premises or cloud security. Large, high-bandwidth R&D sites in the new design would be required to have a full stack of threat protection to include Firewall, IPS/IDS, and malware detection to protect from both external and internal threats.

Tidal's Network and Security Requirements

Tidal Pharmaceuticals decided to adopt Cisco Catalyst SD-WAN as a next-generation WAN solution due to its ability to meet all requirements as put forth by the network and security architects and operations teams. The table below summarizes the key requirements of the NetOps and SecOps project stakeholders and the associated Cisco Catalyst SD-WAN strengths to meet these objectives.

Table 1. Tidal Pharmaceutical's NetOps and SecOps Requirements

Stakeholders	Key Requirements	Cisco Catalyst SD-WAN solution strengths
NetOps	Secure automated fabric using only Internet as transport	• Zero touch, Zero Trust Network Architecture (ZTNA) with automated fabric bring-up • Performance-based routing to detect ISP impairments and dynamically select a better path
	Application visibility and granular traffic control	• Deep packet inspection for enhanced visibility from a single pane of glass (SD-WAN Manager). • Enhanced QoS and traffic engineering policies for granular control
	Cost reduction	• Replacement of MPLS circuits with cost-effective Internet transports • Elimination of Wi-Fi Hotspot in favor of DIA • Redirection of SaaS applications from data center Internet gateway to DIA
SecOps	Control components must be deployed On-Premises, in a DMZ with full SecOps threat protection	• Cisco Catalyst SD-WAN supports both on-premises and cloud control component deployments
	Zero trust architecture - authentication	• Cisco WAN Edge Routers have a factory-installed Trusted Platform Module (TPM) chip with a signed certificate. This built-in security helps ensure automated, foolproof authentication of any new Cisco WAN Edge routers joining the network • Communication only between authenticated WAN Edge devices ensure that no untrusted devices join the overlay and access employee devices
	Branch user traffic segmentation (Sales, Guest, Clinical, R&D)	• Highly scalable VPN segmentation
	Encryption	• Communication between each pair of WAN Edge devices is automatically secure via automated bring-up of IPsec tunnels between Edge devices belonging to the SD-WAN fabric

Stakeholders	Key Requirements	Cisco Catalyst SD-WAN solution strengths
	Data Integrity	• Router embedded-security features and integration of cloud security within the SD-WAN fabric guarantee that traffic transmitted across the network and directly from the branch to the internet cloud is not being altered

Tidal's Cisco Catalyst SD-WAN Design

High-level Design (HLD)

Tidal developed a high-level design to scope out the architectural goals and critical aspects of the design at a broad level before diving deep into the low-level design details. The HLD included the planned use cases and features, types and numbers of WAN transport circuits, SD-WAN tunnel topology and transport color scheme, VPN segmentation, threat protection features, control component deployment model, and WAN Edge platform selection.

Planned Use Cases/Features:

For Tidal Pharmaceuticals, Phase 1 of the SD-WAN deployment was scoped to include the following use cases and features:

- Secure Automated WAN
  - Replacement of MPLS transport with a second Internet transport
  - VPN segmentation
  - On-premises control component deployment
- Application Performance Optimization
  - Application visibility
  - Application-Aware Routing
  - Quality of Service (QoS)
- Secure Direct Internet Access
  - Embedded security features (Application-Aware Firewall)
  - Cloud-delivered security (Umbrella SIG, DNS security)
  - On-premises security (FTDv)

For phase 1, application visibility is restricted to the security devices only, with recognition based on deep packet inspection and monitoring through device logging and cflowd record exports to external collectors where it can be parsed into reports for analysis. Application visibility at the SD-WAN Edge routers is planned for a later phase once features such as SD-AVC, Cisco Stealthwatch or ThousandEyes, and Cloud On-ramp for SaaS can be tested in Tidal's lab and piloted at specific test sites.

Transport Circuits

Two Internet circuits (one of each color, biz-internet and public-internet) are the transports for the new SD-WAN design, as well as an LTE transport used for backup. The small branch site type with a single-router deployment will use one Internet transport and LTE as a backup only, while the other sites with dual-router deployments will use dual-Internet transports. Each DC will have a dual WAN-Edge router deployment with dual-Internet transports.

Colors

Due to the traffic pattern where traffic is either Internet-bound, or applications are accessed from the data center, a hub-and-spoke topology will be implemented. In addition, the Internet transport colors will be deployed in non-restrict mode, so each local WAN Edge router will attempt to build site-to-site tunnels from every local Internet TLOC to every remote Internet TLOC at the DC (and vice-versa), regardless of color. This creates additional paths between the remote sites and the DC (the default behavior). There is also a loopback interface for the LTE TLOC deployed on the data center hub routers, so traffic optimizations can be applied to both sides of the tunnel, since LTE is a metered link and bandwidth is more limited compared to the Internet transports. This color will be deployed in restrict mode, so tunnels can only form between TLOC colors that are the same. The LTE TLOC can still use the Internet transports as underlay. See the Cisco Catalyst SD-WAN Small Branch Design Case Study for more information on the LTE configuration and optimizations.

The following table depicts the tunnels built from one branch router to one DC router and the colors associated with each transport. A branch with 2 Internet transport colors in non-restrict mode would result in 4 data tunnels established to every router at each of the 2 DCs:

Table 2. Tidal Pharmaceutical's SD-WAN Transport Color Scheme

Branch Type	Transport Type	Branch Transport Color	Data Center Transport Color	Restrict?
Type 2/3	Internet 1	biz-internet	biz-internet	N
Type 2/3	Internet 1	biz-internet	public-internet	N
Type 2/3	Internet 2	public-internet	biz-internet	N
Type 2/3	Internet 2	public-internet	public-internet	N
Type 1	Internet 1 or 2	biz-internet or public-internet	biz-internet	N
Type 1	Internet 1 or 2	biz-internet or public-internet	public-internet	N
Type 1	Cellular LTE	lte	lte (TLOC is a loopback interface on the DC WAN Edge router)	Y

Overlay Tunnels

Based on this information, the number of overlay tunnels can be calculated for the hub-and-spoke topology. There are 4 total DC SD-WAN routers, 30 site type 1 routers, 40 site type 2 routers, and 16 site type 3 routers, for a total of 90 routers.

- Type 1 routers: When the Internet transport is up, the LTE transport is in backup mode, so tunnels only need to be calculated for the Internet transport. The Internet TLOC on the branch router forms 2 unrestricted tunnels to each DC router, resulting in 8 total tunnels originating from the type 1 branch routers.
- Type 2 routers: Each router has 2 Internet TLOCs and forms 4 unrestricted tunnels to each DC router, resulting in 16 total tunnels originating from the type 2 branch routers.
- Type 3 routers: Each router has 2 Internet TLOCs and forms 4 unrestricted tunnels to each DC router, resulting in 16 total tunnels originating from the type 3 branch routers.

- DC routers: Each DC router forms 2 tunnels to each type 1 router (30), 4 tunnels to each type 2 router (40), and 4 tunnels to each type 3 routers (16), resulting in 60+160+64, or 284 tunnels.

VPN Segmentation

Tidal's security policy mandates that Sales, Guest, Clinical, and R&D operations must be kept separate into different VPNs from end-to-end.

Table 3. Tidal Pharmaceutical's VPN Definitions

VPN	Purpose
1	Research & Development (R&D)
2	Sales
3	Clinical
10	Guest

Control Component Deployment Model

Tidal opted for an on-premises control component deployment model, based on the security requirements dictated by the company's SecOps team. They followed the guidance set forth in the Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources guide for Release 20.6.x (On-Prem Deployment) to calculate the number of SD-WAN Managers needed for the deployment. For the number of SD-WAN devices to manage (90), plus accounting for some future growth (10%), and with SD-WAN Application Intelligence Engine (SAIE) enabled in future phases which should fall in the less than 50Gb/s per day range, one active SD-WAN Manager node and one standby SD-WAN Manager node is adequate for the network. In addition, the number of control connections is relatively small, so only one Controller and one Validator is needed with another one of each for redundancy. This helps derive the server hardware requirements needed for the deployment.

Table 4. On-Premises Control Components Requirement

DC	Manager	Validator	Controller
1	1 (primary)	1	1
2	1 (standby)	1	1

WAN Edge Platform Selection and Site Specifications

Tidal Pharmaceuticals recorded the following new site specifications and outlines their platform selections for each. In the dual-Edge sites, one device should be able to handle the bandwidth of the entire site in case of a failure.

Table 5. Tidal's SD-WAN Platform Selection and Site Specifications

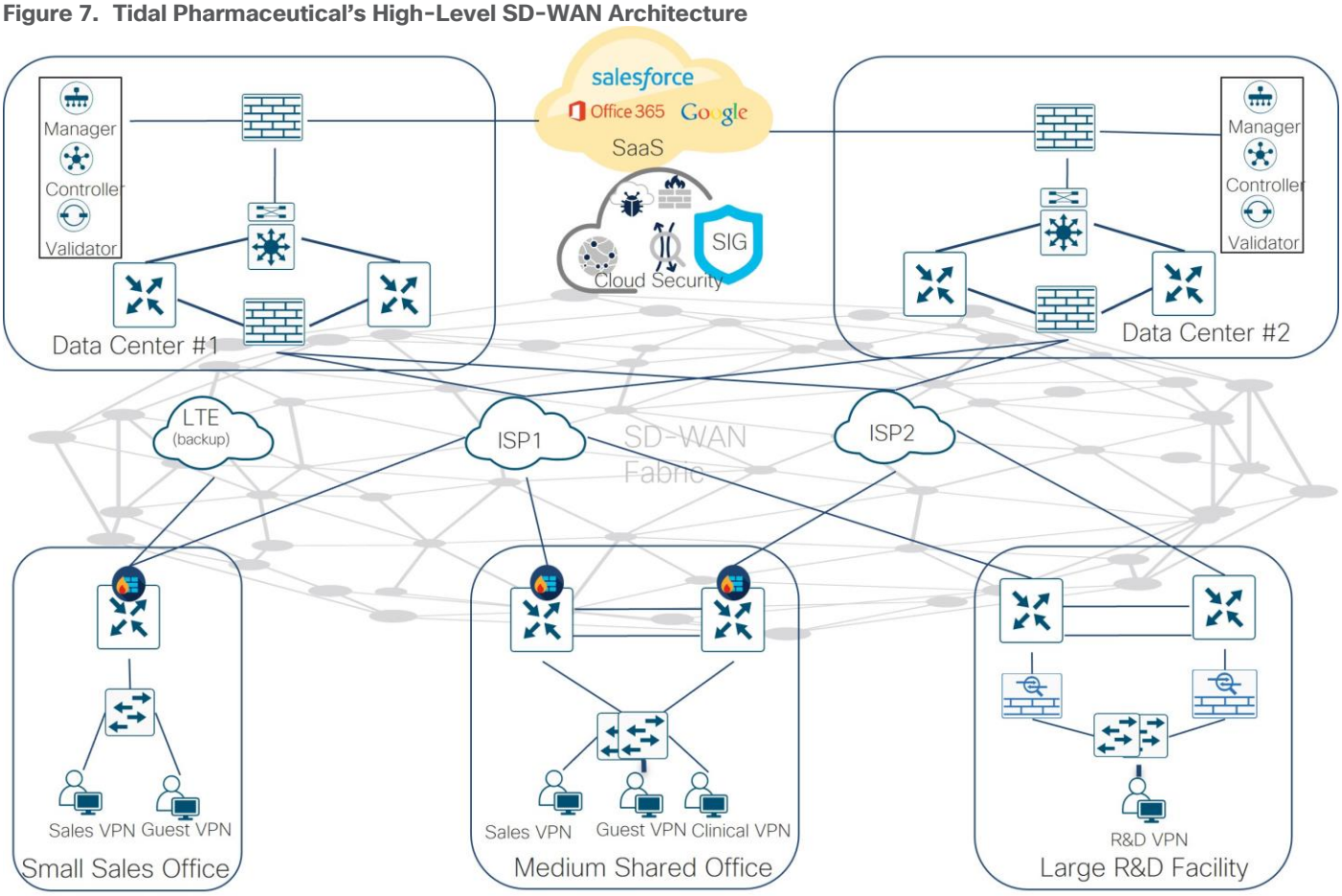
Site Type	Americas Sites	Routers Per Site	Circuits per Site	Bandwidth per Site (Legacy)	Bandwidth per Site (SD-WAN)	Number of Data Plane Tunnels	WAN Edge Router
Small Sales (Branch Type 1)	30	1	2 (Internet and LTE)	50-100 Mbps	100-300 Mbps	8	C1121X-8PLTEPW*
Medium-Sized Shared (Branch Type 2)	20	2	2 (Internet)	300-500 Mbps	600 Mbps-1 Gbps	16	C8200-1N-4T
Large R&D (Branch Type 3)	8	2	2 (Internet)	600 Mbps-1 Gbps	2-6 Gbps	16	C8300-2N2S-4T2X
Data Center	2	2	2 (Internet)	5 Gbps	10 Gbps	284	C8500-12X

*Note that the C1121X (as opposed to C1121) is chosen because it comes with 8 GB of memory and flash to support SD-WAN advanced security features, such as IPS. Tidal has not yet evaluated IPS for integrated/embedded security but wanted to have the option to use it in future phases.

High-level Diagram

The following diagram illustrates Tidal's secure branch connectivity to their private data centers, Internet, and SaaS cloud.

Figure 7. Tidal Pharmaceutical's High-Level SD-WAN Architecture



Tidal's Cisco Catalyst SD-WAN Data Center Design

Tidal deployed Cisco Catalyst SD-WAN control components and Catalyst 8500 Hub WAN Edge routers in its Americas DC 1 and DC 2 data centers. The control component VMs were deployed on VMWare hosted by dedicated Cisco UCS C-series hardware, following the guidance set forth in the Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources for number of VMs, memory, storage, and bandwidth requirements. Due to the relatively small scale of deployment, a single instance of SD-WAN Manager, Validator, and Controller was instantiated in each DC, with the primary SD-WAN Manager in DC 1 and a standby SD-WAN Manager instance in DC 2 for redundancy. The control components were installed in each DC behind a NAT-enabled firewall, with all control components NATed to public, Internet-routable address space. The Controller and Manager were placed in a firewall DMZ while the Validator was placed in a separate DMZ. This, combined with NAT, would minimize exposure to port scanning and other threats, while allowing for Validator NAT address discovery and control connections to remote routers. Tidal followed the guidelines in the Firewall Ports for Viptela Deployments to open the necessary ports for secure inter-control component communications and communications to the WAN Edge routers.

See the Cisco Catalyst SD-WAN Large Global WAN Design Case Study for more information on on-premises control component design.

Tidal's Cisco Catalyst SD-WAN WAN/LAN Branch Design

SD-WAN low-level design standards were developed for each branch type based on specific network connectivity requirements.

Type 1 Branch - Small Sales Office

Tenants at these sites include corporate sales employees and their guests, primarily consuming Internet and SaaS applications across the WAN. SD-WAN connectivity to the data center is offered only to the sales or corporate traffic, and this traffic accounts for less than 10% of the total WAN bandwidth, with the remaining 90% attributed to Internet/SaaS. Tidal chose a converged networking and security “branch in a box” solution, with a single Cisco ISR 1100 series router (C1121X-8PLTEPW) providing wired and wireless LAN access, WAN routing, and security functionality.

WAN-Side

A single Internet circuit serves as the primary WAN transport at these locations with the color being either biz-internet or public-internet, depending on provider availability and cost. An integrated cellular LTE module provides backup connectivity in the event of an ISP failure. Because the LTE has a lower bandwidth than the Internet circuit, sales traffic is prioritized over guest traffic through the use of Per-VPN QoS.

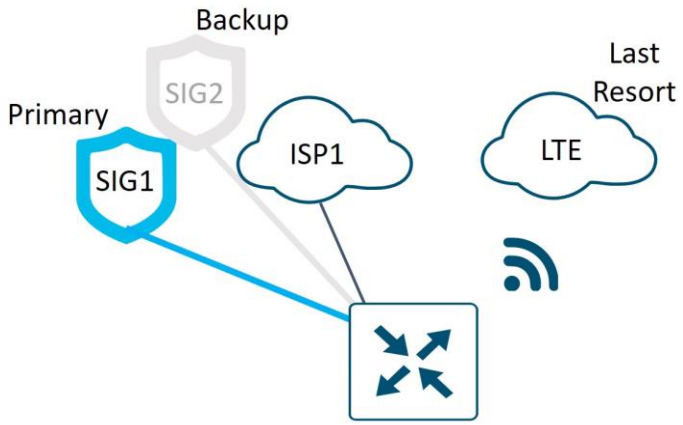
Per-VPN Quality of Service (QoS)

Per-VPN QoS was introduced in SD-WAN Manager release 20.6.1/IOS XE Release 17.6.1a. It allows you to configure a QoS policy to limit the bandwidth that can be used by traffic belonging to each VPN. This becomes especially important in a scenario where the Internet transport fails and the backup LTE must take over since there is typically less bandwidth available on the LTE transport. In this deployment, approximately 80% of the bandwidth is configured for Sales traffic, while approximately 20% of the bandwidth is configured for Guest traffic.

SIG Tunnels

Each small Sales Office WAN Edge router connects to a primary and backup SIG via an IPsec tunnel on the Internet transport. Health checks are run across the SIG tunnels to the SIG Cloud Provider, and if health checks fail, the active tunnel will be brought down and the backup tunnel will be activated. If the Internet transport goes down, the LTE transport will become activated, and primary and backup SIG tunnels will be formed at that time.

Figure 8. SIG Tunnels at a Type 1 Branch - Small Sales Office Site

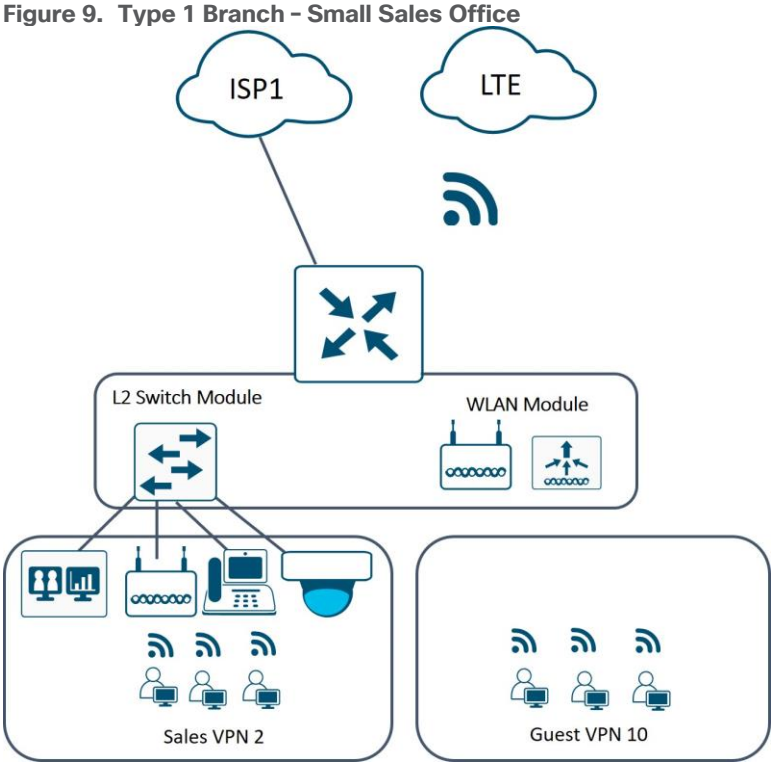


LAN-Side

Ethernet LAN connectivity for up to 8 wired devices in the branch is provided directly wi¬¬¬¬th L2 LAN switch ports, supporting sites with Telepresence units, video surveillance cameras, external Ethernet switches and Wireless LAN access points. ¬¬¬¬A guest WiFi service is implemented using the integrated 802.11ac wireless

LAN module, allowing Tidal to decommission the costly provider “hotspot” service. Sales and Guest traffic are segmented into different VPNs on the LAN, with guest traffic placed into VPN 10 and Sales into VPN 2.

Figure 9. Type 1 Branch – Small Sales Office



Type 2 Branch – Medium Shared Site

These offices support Tidal employees from the Sales and Clinical organizations, in addition to their guests which require Internet access. These offices require more bandwidth and higher availability due to a greater number of users and addition of a clinical department that performs functions critical to Tidal’s business. The branch design for this office type includes a pair of Catalyst 8200 routers and dual Internet transports with up to 1 Gbps aggregate site bandwidth.

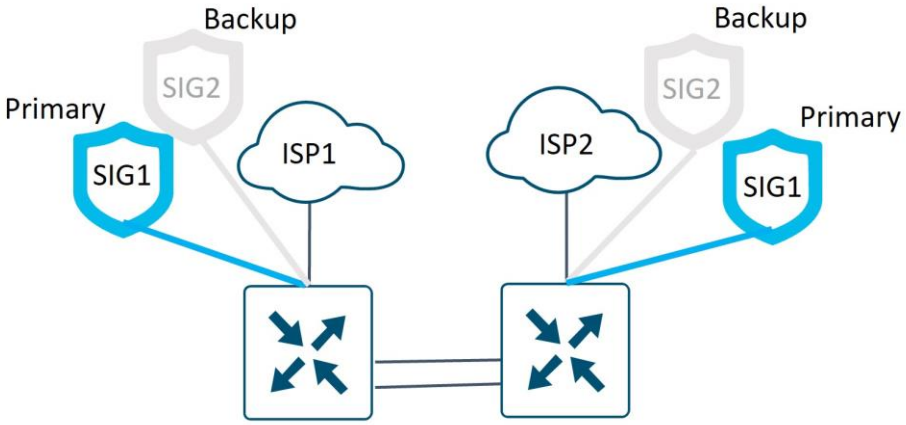
WAN-Side

Dual Internet circuits serve as the WAN transports for these locations, with one transport color labeled “biz-internet” and the other transport color labeled “public-internet”. The link between the two WAN Edge routers is a trunk link with two subinterfaces on each router to serve as TLOC and TLOC extension links.

SIG Tunnels

Each WAN Edge router connects to a primary and backup SIG each through an IPsec tunnel located on the directly connected transport. Tunnels are not built across the TLOC and TLOC extension links because the extra bandwidth is not needed at this time, and it simplifies usage monitoring and troubleshooting. Health checks are run across the SIG tunnels to the SIG Cloud Provider, and if health checks fail, the active tunnel will be brought down and the backup tunnel will be activated.

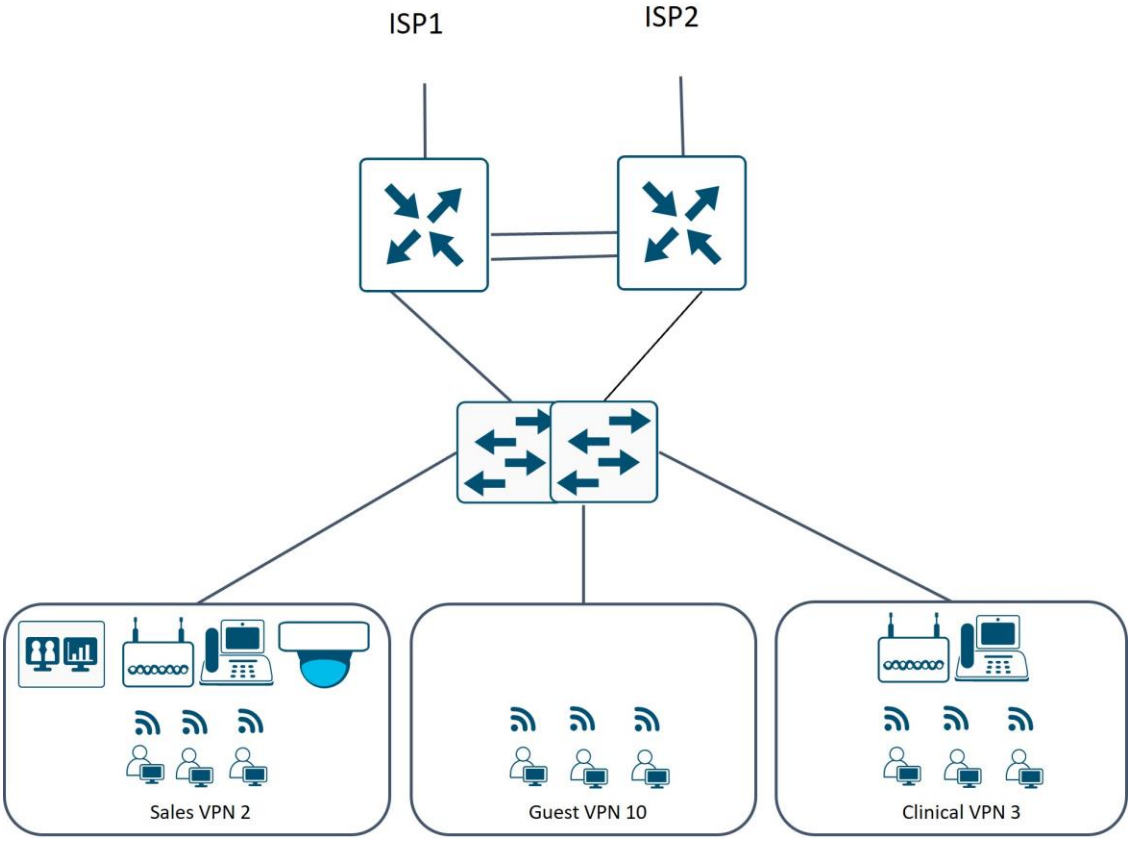
Figure 10. **SIG Tunnels at a Type 2 Branch – Medium Shared Site**



LAN-Side

Ethernet LAN connectivity is provided directly with L2 LAN switch ports, supporting sites with Telepresence units, video surveillance cameras, external Ethernet switches and Wireless LAN access points. Sales, Guest, and Clinical traffic are segmented into different VPNs on the LAN, with guest traffic placed into VPN 10, Sales into VPN 2, and Clinical into VPN 3.

Figure 11. **Type 2 Branch – Medium Shared Site**



High Availability/Redundancy

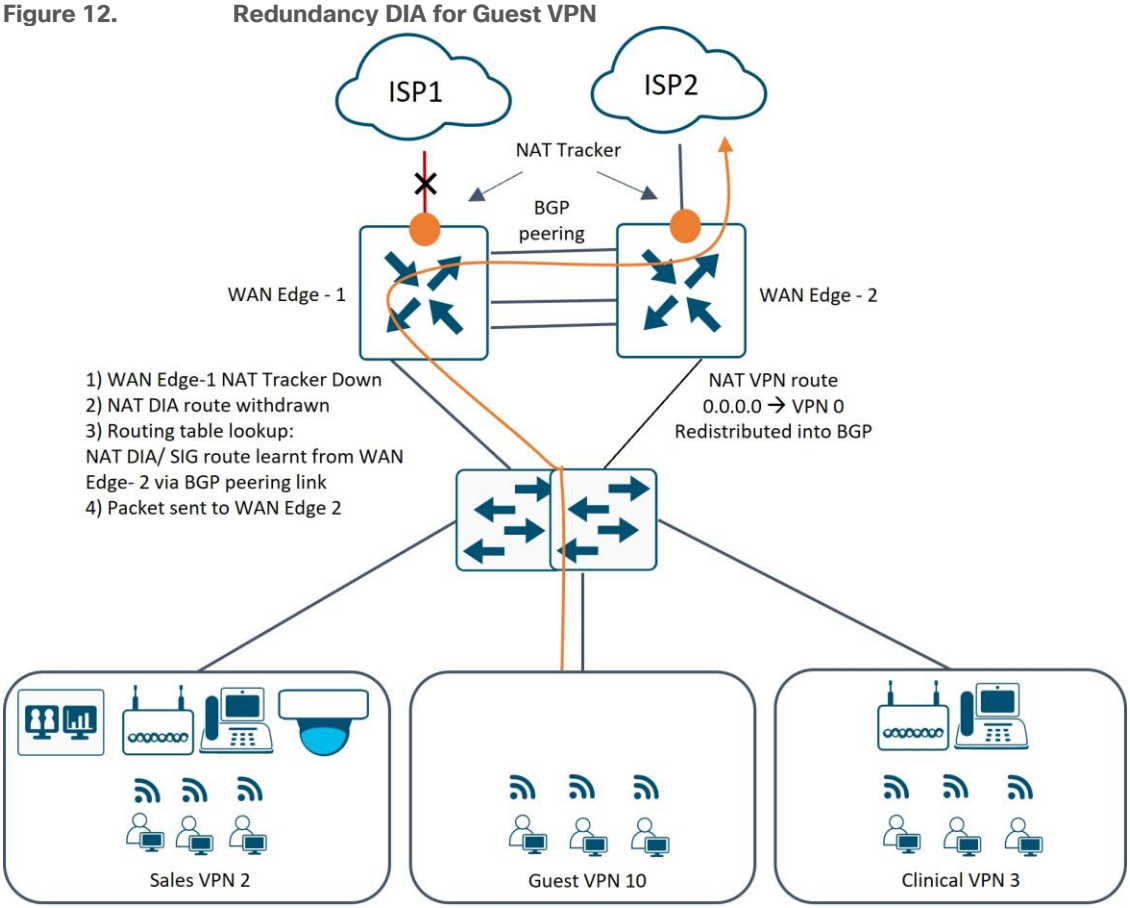
The Guest, Sales, and Clinical VPNs use an L2 topology and utilize VRRP as the next-hop gateways on the WAN Edge routers.

NAT tracker is not supported on subinterfaces (only physical) in 20.6/17.6 and SIG tunnels are not run across the TLOC/TLOC extension interfaces in this use case, so in order to prevent blackholing upon transport failure across the TLOC extension, a subinterface is created for each service VPN on the trunk between the WAN Edge routers. A routing protocol (BGP) is run to redistribute the DIA or SIG default route, so if one Internet transport goes down, traffic will always be drawn to the WAN Edge router advertising a reachable Internet transport.

Guest VPN

The guest VPN uses a NAT VPN route in the service VPN to direct guest traffic to the Internet, and that route is redistributed into BGP between the WAN Edge routers. A NAT tracker runs on the physical interface on a WAN Edge router connected to the local ISP, so if that NAT tracker goes down, the NAT DIA (directly connected) route is withdrawn. The NAT DIA route that is in place for the reachable ISP transport is being redistributed in BGP in the guest VPN between the two WAN Edge routers, so traffic will flow to the reachable ISP transport.

Figure 12. Redundancy DIA for Guest VPN



Sales and Clinical VPN

In the Sales and Clinical VPN, O365 traffic is directed to the Internet via a data policy, internal traffic is directed to the data center through the SD-WAN overlay with OMP routes, or other Internet traffic is directed to the SIG gateway using the default SIG route.

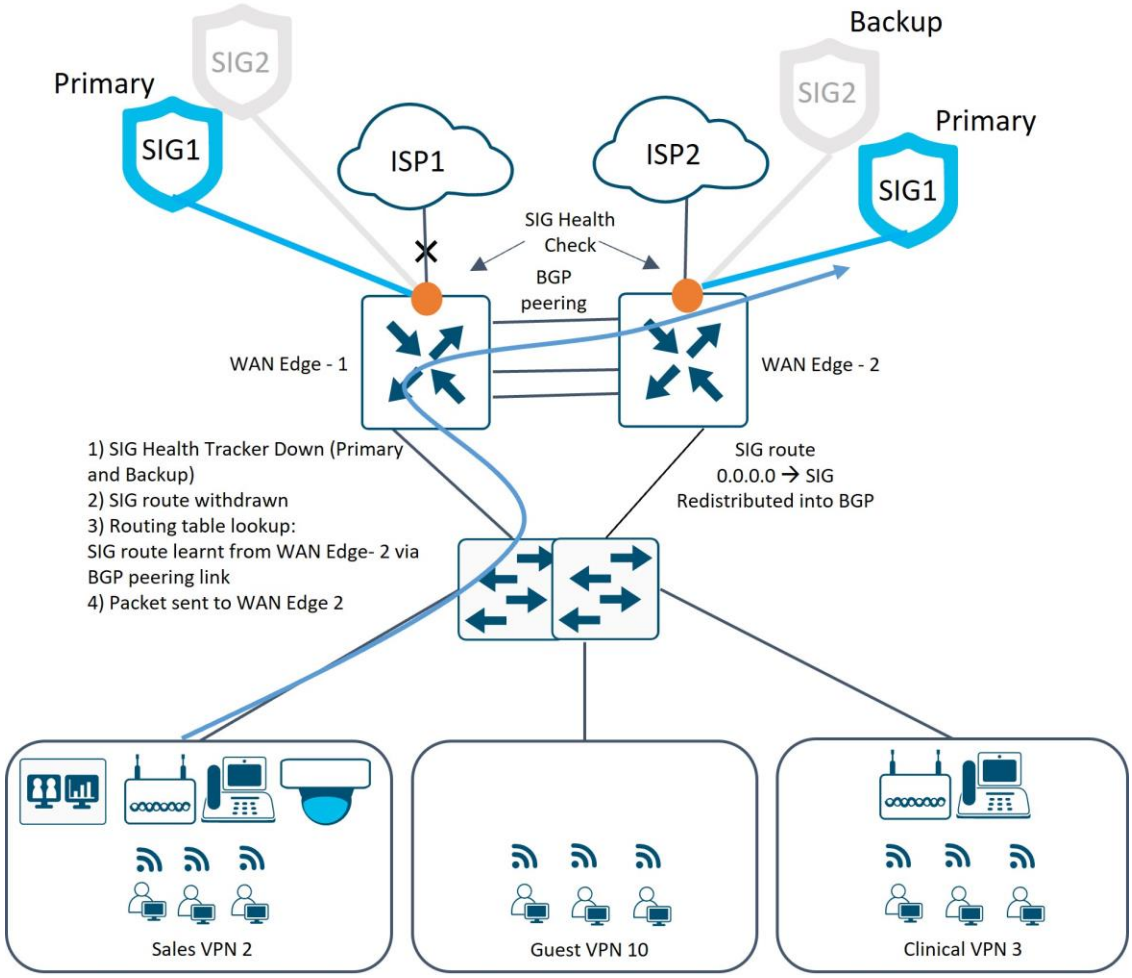
Tech Tip
Note that in 20.6/17.6 SD-WAN Manager/IOS-XE code versions, fallback (to routing) is not supported for traffic redirection to SIG using a centralized data policy. This means that if no SIG tunnel is available, traffic is dropped by the data policy instead of being forwarded using the routing table. The fallback feature is introduced in 20.8/17.8 SD-WAN Manager/IOS-

XE code version. In Tidal's use case, the SIG route was used instead of a centralized data policy to direct traffic to a SIG tunnel, which allows fallback (to routing) to occur when the SIG tunnels are down.

How redundancy works is as follows:

- Internal/Overlay Traffic: Traffic follows the more-specific data center route in OMP that is being advertised to each WAN Edge router over each TLOC. This traffic may traverse the TLOC/TLOC extension link to reach a data center.
- SIG Traffic: SIG traffic is directed to the SIG tunnel using a SIG default route installed in the service VPN, and that route is redistributed into BGP between the WAN Edge routers. A health tracker runs over the SIG tunnels to the SIG Cloud Provider, and if health checks fail, the active tunnel will be brought down and the backup tunnel will be activated. If the backup tunnel cannot be activated, the SIG default route for the directly connected transport is withdrawn. The SIG route that is in place for the reachable SIG tunnel is being redistributed in BGP in the sales and clinical VPNs between the two WAN Edge routers, so traffic will flow to the reachable SIG tunnel. If all SIG tunnels are down, but at least one transport and corresponding overlay SD-WAN tunnel is active, traffic can follow the default route to the data center to reach a security stack and get Internet access.
- O365 Traffic: NAT will be defined only on the directly-connected transport and the data policy will forward traffic out the NAT-enabled interface. A NAT tracker runs on the physical interface on a WAN Edge router connected to the local ISP, so if that NAT tracker goes down, the local Internet interface goes down and routing as a fallback method is used. The SIG default route that is in place for the reachable ISP transport is being redistributed in BGP in the Sales and Clinical VPNs between the two WAN Edge routers, so traffic will flow to the reachable ISP transport.

Figure 13. SIG Redundancy for Sales/Clinical VPN



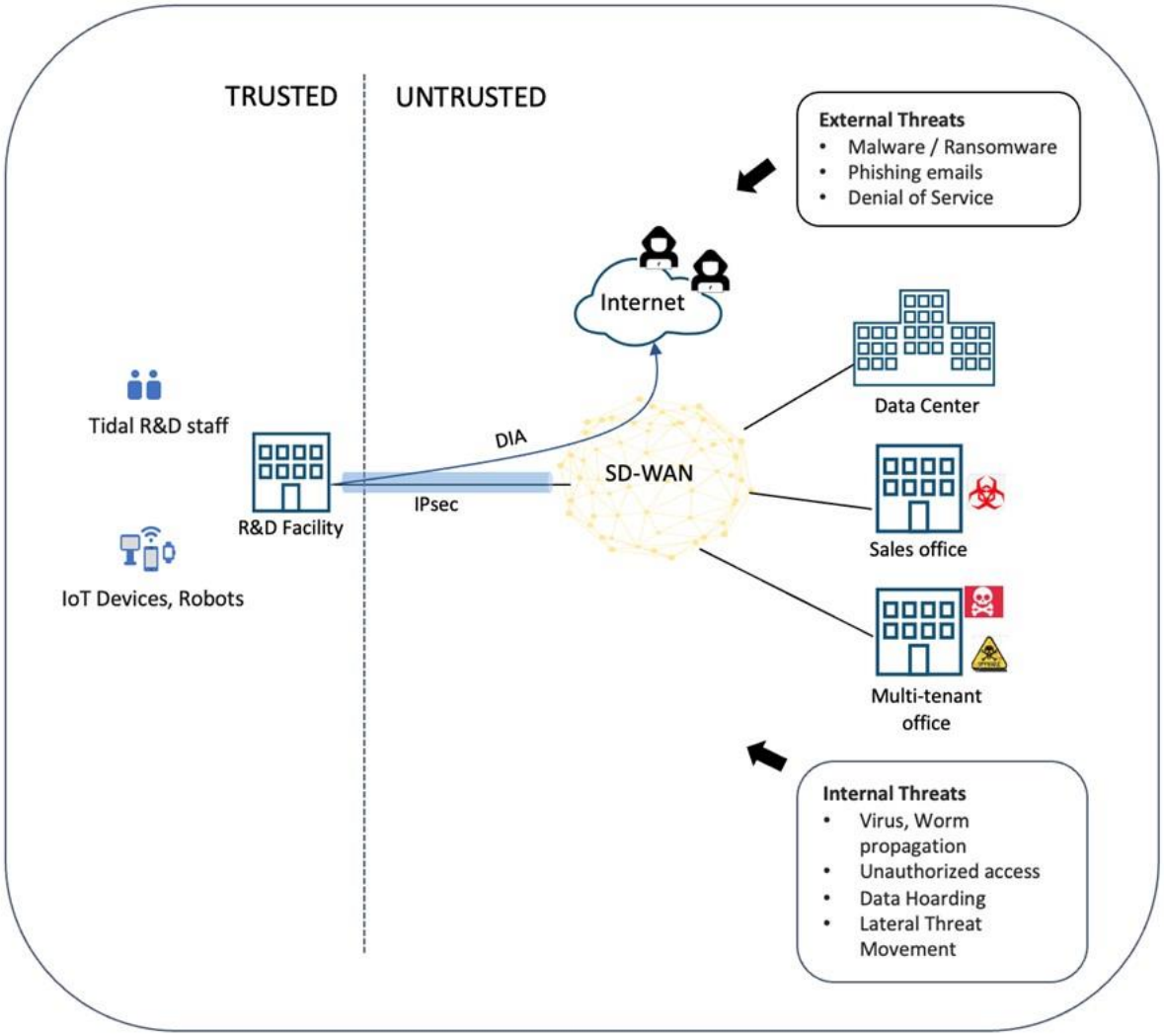
Type 3 Branch – R&D Facility Design

Tidal's R&D facilities are business-critical sites where drug discovery, testing, and prototype production occurs. Tidal workers in R&D facilities include researchers and scientists, project managers, marketing experts, and analysts whose duties are to determine consumer trends and feed this information to researchers. Much of the specialized lab equipment is automated through IoT equipment, with robots performing chemical procedures in "clean rooms" to reduce the risk of health hazard to employees or contamination of prototype drugs in production. These users and devices at R&D facilities utilize both private data center and cloud applications on a daily basis, with a traffic ratio of approximately 80% site-to-DC, and 20% site-to-Cloud. Direct Internet access is enabled to maximize performance for cloud applications, which include pharma-specific SaaS, business/productivity, and general Internet browsing.

Threats

R&D facilities are subject to the highest degree of protection from both external threats coming from the Internet, and internal threats potentially entering the site from compromised hosts or people located at other Tidal sites. It is not enough to simply secure the site's Internet perimeter with on-premises or cloud security; R&D facilities must be fully protected from threats that could potentially enter from other sites on the SD-WAN overlay, defining a site security posture that considers all WAN traffic to be untrusted and subject to on-premises security inspection.

Figure 14. Internal and External Threats



WAN-Side

R&D facilities consume very high WAN bandwidth due to the research activities, file transfers, and nightly database replication that drive requirements up to 6 Gbps at the larger sites. WAN bandwidth is delivered by pairs of Internet service provider circuits that connect to redundant Catalyst 8300 WAN Edge routers configured with TLOC extensions that provide SD-WAN and DIA path redundancy.

LAN-Side

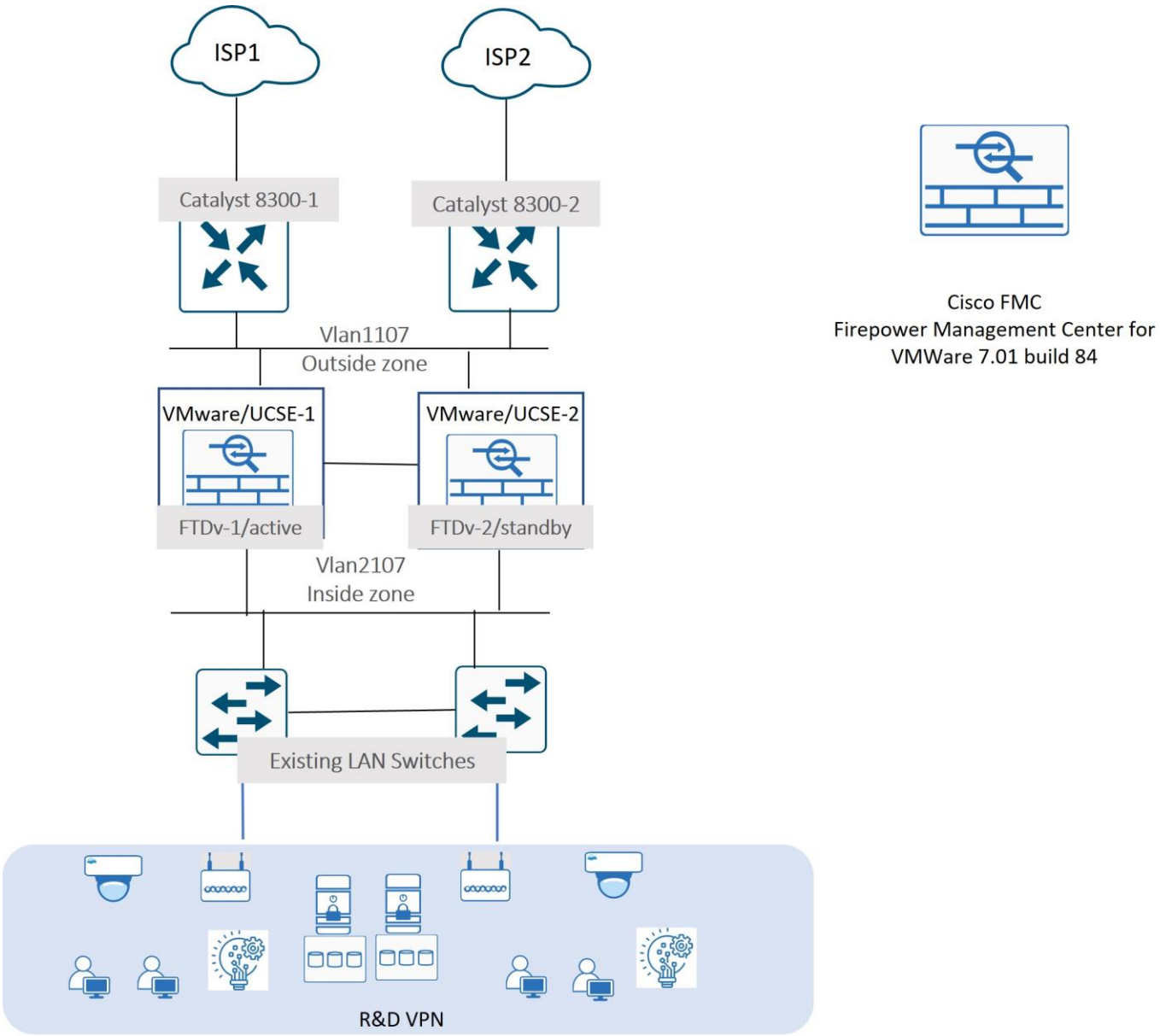
Ethernet LAN connectivity is provided by two separate LAN switches, supporting all R&D activities, including IoT lab equipment, video surveillance cameras, and Wireless LAN access points. R&D traffic is segmented into VPN 1 on the LAN.

Security

For security, Tidal deployed instances of Cisco Secure Firewall Threat Defense virtual (Formerly FTDv NGFW) on VMWare ESXi inside UCS-E server modules in the Catalyst 8300s. Tidal chose FTDv since they required a full-featured, high-throughput threat prevention solution that could integrate with an identity architecture based on Cisco ISE that was planned to be launched as part of the SD-WAN deployment. Deploying FTDv would allow Tidal to perform all the appliance configuration, monitoring, and management functions from a Firewall

Management Center (FMC) instance already deployed in their data centers to manage the Firepower NGFW HA pairs in their Internet DMZs.

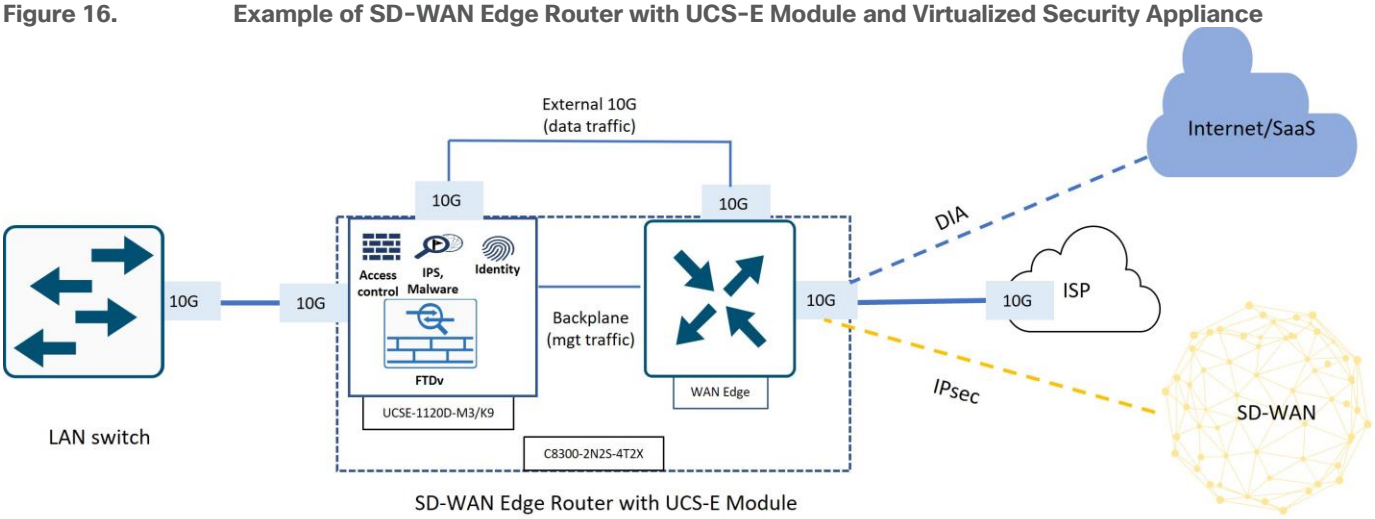
Figure 15. Type 3 Branch – R&D Facility Design



Deploying virtualized network and security services on high capacity UCS-E server modules maximizes WAN Edge routing performance as it frees up router resources so that more CPU can be dedicated to packet

forwarding, which is necessary to meet Tidal's high throughput use case. The diagram below depicts an example of a 10-Gigabit secure branch topology using the external 10 Gigabit interfaces on the UCS-E-1120D server module to insert a virtualized NGFW between the LAN and WAN Edge. Note that even though the UCS-E exists as a module inside the WAN Edge router, the virtualized security appliance acts as an external device since data traffic traverses the external 10 Gigabit port between the UCS-E and WAN Edge router. Only management traffic utilizes the backplane between the UCS-E module and WAN Edge router.

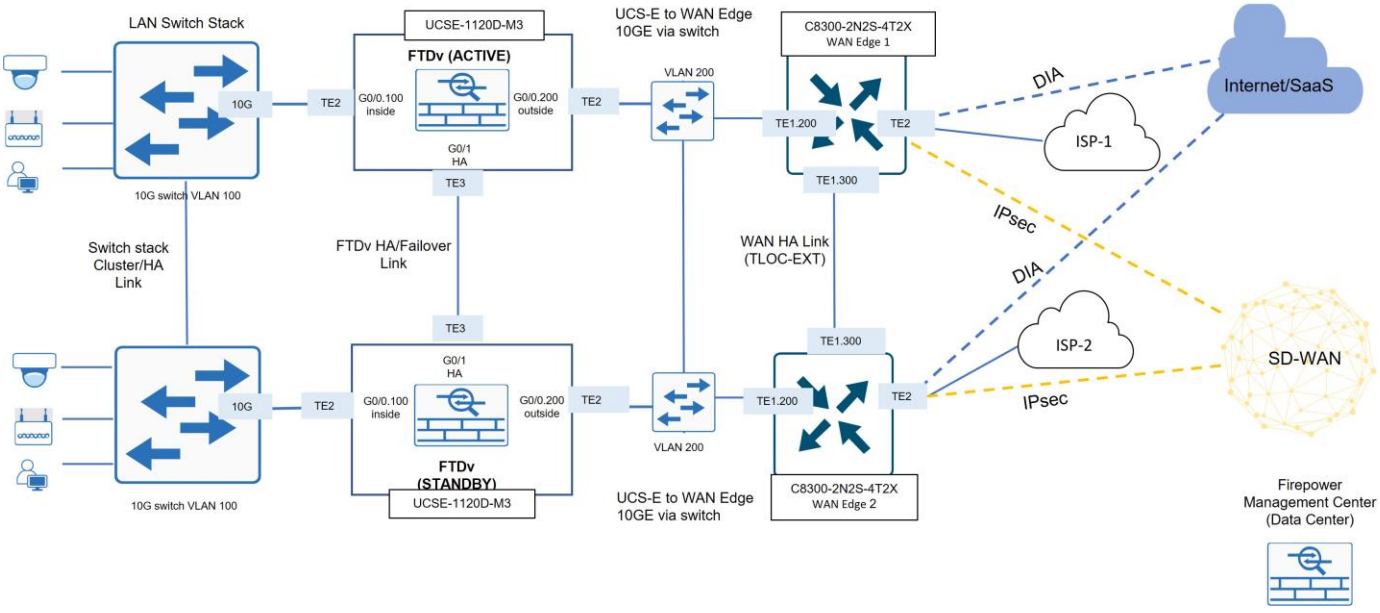
Figure 16. Example of SD-WAN Edge Router with UCS-E Module and Virtualized Security Appliance



High Availability/Redundancy

Tidal deployed redundant LAN, WAN, and security components to meet the high availability SLA for their R&D sites as illustrated in the diagram below.

Figure 17. Tidal Type-3 Branch (R&D Facilities) Low-Level SD-WAN Design



High availability for the R&D facilities/R&D VPN is achieved by enabling various LAN, WAN, and security feature layers as summarized below.

- Active and Standby instances of Cisco Secure Threat Defense Virtual (FTDv) are deployed on UCS-E Server modules in redundant WAN Edge routers.
- End devices connected to the L2 access switches use the FTDv internal interface IP addresses as their default gateways. This address is applied to the active FTDv device in a pair which replies to ARP requests and forwards traffic to the WAN Edge routers. When a switchover occurs, the newly promoted FTDv device assumes the gateway role to seamlessly provide first hop redundancy.
- Each FTDv is configured in routed mode, with a pair of default routes leading to each WAN Edge router. Default routes are conditional, based on probes to destinations on the Internet.
- There are dual WAN Edge routers, each connected to a different ISP circuit, for a total of two ISP circuits to support the site. TLOC extensions provide for SD-WAN path redundancy, so each WAN Edge router has access to both ISP circuits.
- A subinterface in the service VPN runs between the Edge routers, and the default route from each router is redistributed via BGP routing. If an ISP circuit goes down, traffic can follow the default route advertised between the WAN Edge routers and reach an active ISP transport.

Refer to the Cisco Community article Deploying FTDv virtualized security on SD-WAN Cat8K/UCS-E modules for a more detailed description of this design and set of step-by-step deployment instructions.

Tidal's Cisco Catalyst SD-WAN Branch Security Design

Tidal Pharmaceuticals uses a hybrid model of threat protection at their various branch sites, with a combination of embedded features, cloud security, and FTDv on a UCS-E module for protection for guest and corporate users. The following models are used at each branch:

- Type 1 Branch (Small Sales Office):
  - Embedded Security for Guest (Enterprise Firewall and DNS Web Layer Security)
  - Embedded and Cloud Security for Sales (Enterprise Firewall and DNS Web Layer Security and FW/IOS/CASB/Malware on SIG)
- Type 2 Branch (Medium Shared Site)
  - Embedded Security for Guest (Enterprise Firewall and DNS Web Layer Security)
  - Embedded and Cloud Security for Sales and Clinical (Enterprise Firewall and DNS Web Layer Security and FW/IOS/CASB/Malware on SIG)
- Type 3 Branch (R&D Facilities)
  - FTDv on UCS-E for higher throughput security protection

The following table summarizes the traffic paths in each VPN, along with the security method used to protect that traffic.

Table 6. VPN Traffic Paths and Security Methods Used for Protection

VPN	Destination	Path	Security
Guest VPN	Internet	DIA	• Enterprise Firewall with Application Awareness • DNS Web Layer Security
Sales VPN	Enterprise Data Center	Cisco Catalyst SD-WAN	• End-to-end IPsec encryption

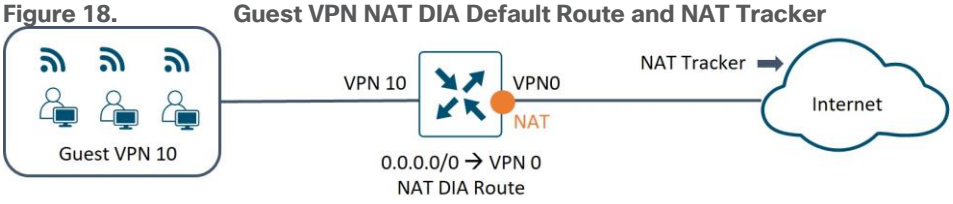
VPN	Destination	Path	Security
and Clinical VPN	Office365 SaaS	DIA	• Enterprise Firewall with Application Awareness • DNS Web Layer Security
	Internet (other than Office365)	IPsec to Umbrella SIG	• Enterprise Firewall with Application Awareness • IPsec Encryption to SIG • FW, IPS, CASB, Malware detection
R&D VPN	Enterprise Data Center	Cisco Catalyst SD-WAN	• End-to-end IPsec encryption • FTDv identity-based access policies • NGFW access control, Snort IPS, Advanced Malware Protection (AMP)
	Internet	DIA	• FTDv identity-based access policies • NGFW access control, Snort IPS, Advanced Malware Protection (AMP), and security intelligence block listing

Guest VPN

Traffic Path

Internet connectivity for guest VPN users is provided through a local breakout, using a NAT-DIA default route in VPN 10. NAT trackers are configured on the VPN 0, physical WAN internet facing interfaces, to detect when the external network becomes unavailable and withdraws the NAT DIA route in the guest VPN.

Figure 18. Guest VPN NAT DIA Default Route and NAT Tracker

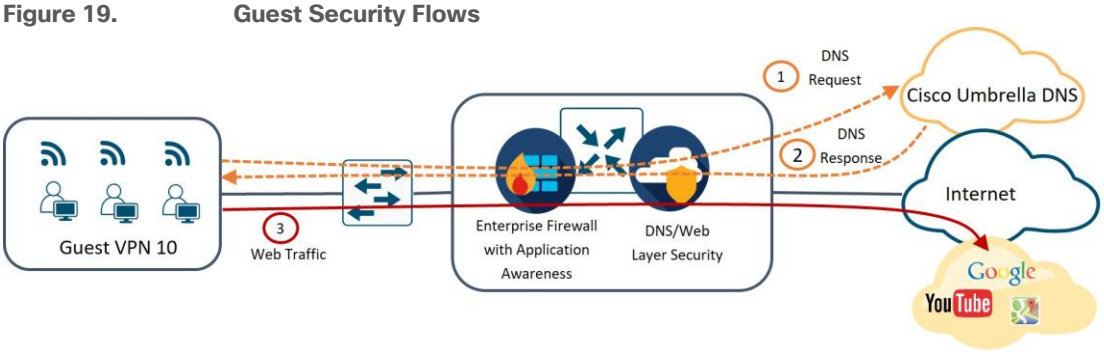


Guest Security

An inter-VPN zone-based firewall between the Guest VPN and VPN 0 is configured which restricts guest users to access only HTTP/ HTTPS web applications. DNS traffic flows from these guest users are also subjected to inspection and redirection to Umbrella DNS resolvers using the DNS/Web-layer security feature. This security feature on the WAN Edge router ensures that DNS queries are authentic, restricting access to web sites that are risky or in violation of Tidal's acceptable use policy.

In addition to the security features maintained to secure guest traffic flows, a VPN membership policy is configured on the Controller. This ensures routes for the guest VPN is kept local to the site, preventing it from using the SD-WAN fabric.

Figure 19. Guest Security Flows

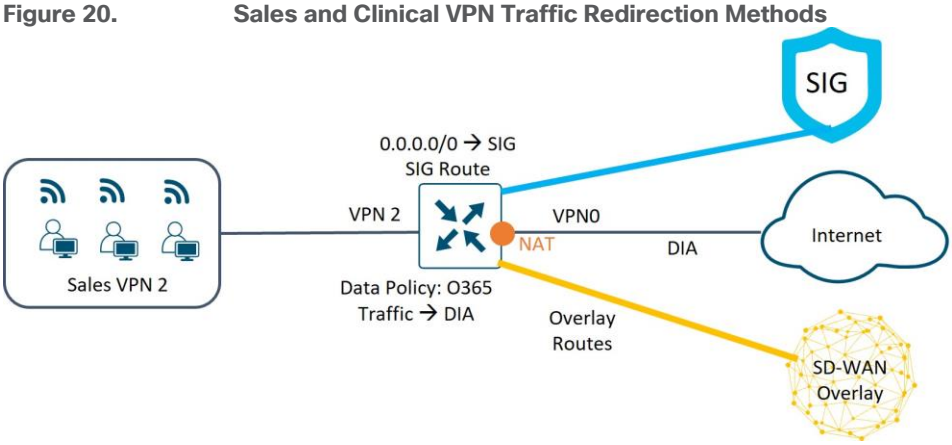


Sales and Clinical VPN

Traffic Paths

In the Sales and Clinical VPN, a combination of data policy and routing is used to steer traffic. In the data policy, traffic with destination prefixes for Office 365 is directed via NAT DIA. All other traffic that doesn't match policy is routed normally. Traffic destined to the data centers is routed over the SD-WAN overlay tunnels, and a default route pointing to SIG exists so the rest of the Internet-bound traffic will be directed over the SIG tunnel.

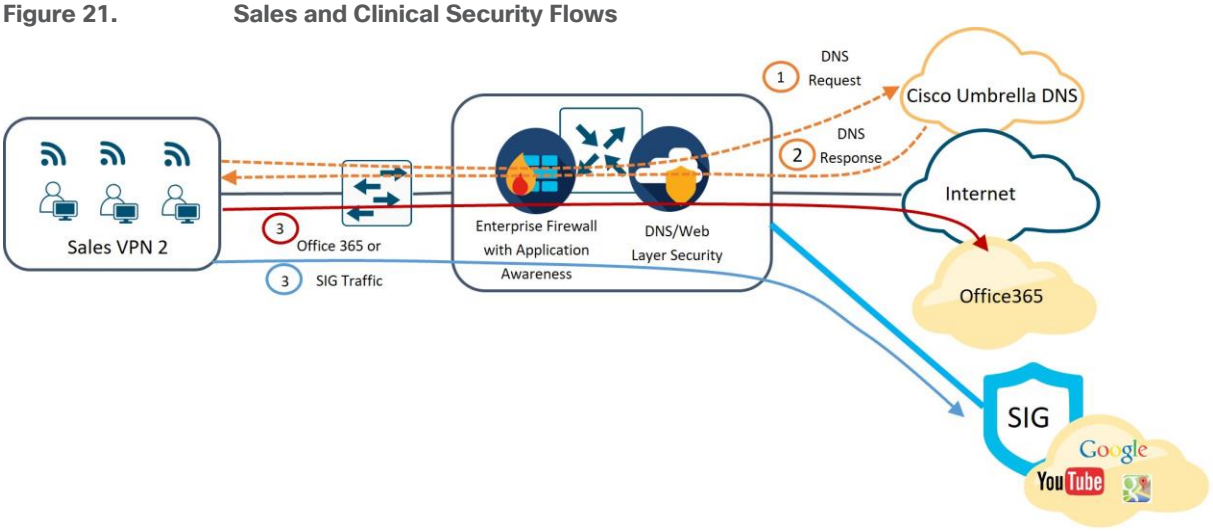
Figure 20. Sales and Clinical VPN Traffic Redirection Methods



Sales and Clinical VPN Security

Sales traffic destined to the Internet must first pass a DNS security check, and once permitted is sent DIA if it is Office365 traffic or forwarded over an IPsec tunnel to an Umbrella SIG gateway. Once received by SIG, traffic is decrypted and forwarded through a cloud security service chain and forwarded to the proper Internet destination before returning by way of the SIG back to the WAN Edge router. Because guest traffic utilizes a zone-based firewall from guest VPN to VPN 0, other service VPNs that utilize VPN 0 for Internet-bound traffic need to use the zone-based firewall for transit traffic.

Figure 21. Sales and Clinical Security Flows



R & D VPN

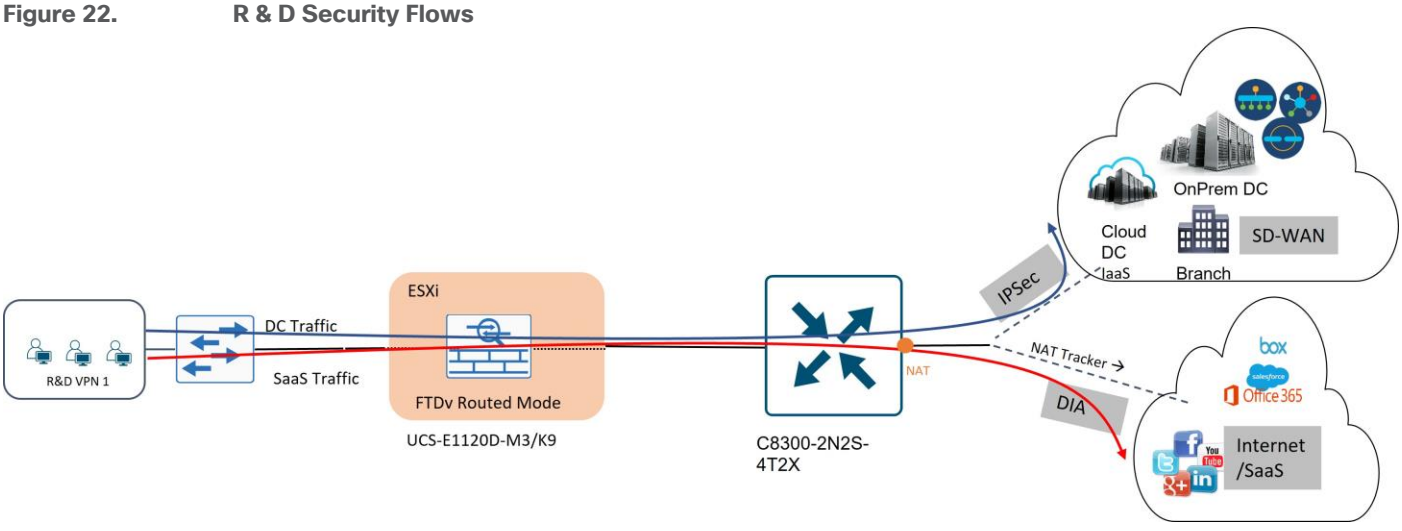
Traffic Path

All traffic originating from the branch passes through FTDv security before reaching the WAN Edge routers. Traffic uses more specific routes to reach devices in the data center over the SD-WAN overlay, and everything that doesn't match uses the Internet path. Internet connectivity for the R & D VPN users is provided through a local breakout, using a NAT-DIA default route in VPN 1. NAT trackers are configured on the VPN 0, physical WAN internet facing interfaces, to detect when the external network becomes unavailable and withdraws the NAT DIA route in the guest VPN.

R & D Security

For the R & D VPN, all traffic must pass through the active FTDv that sits inline and acts as the default gateway for all users. All traffic is subjected to NGFW access control, Snort IPS, and Advanced Malware Protection (AMP). Internet-bound traffic is also subjected to Security Intelligence block listing, which protects traffic from malicious Internet content by using reputation intelligence to quickly block connections to or from URLs, domain names, and IP addresses.

Figure 22. R & D Security Flows



Conclusion

Most enterprises seek similar outcomes with their SD-WAN deployments – better application experience at the branch, increased site availability and employee productivity, more agility to launch new initiatives, greater visibility and control of applications to groom traffic and mitigate threats.

Organizations with a NetOps bias typically focus on simplification and any-to-any connectivity use cases – cloud control components, Direct Internet Access (DIA), multicloud, and colocation deployments that prefer Internet as the WAN transport. NetOps discussions around security are typically limited to traffic encryption, site onboarding, zero-trust, and device hardening aspects of the SD-WAN components to prevent spoofing and denial-of-service attacks from disrupting service. A security-sensitive enterprise like Tidal Pharmaceuticals with a SecOps bias would take a more measured, risk-based approach towards the features they deploy in their SD-WAN designs, starting by evaluating the following questions if a breach were to occur:

- What are the threats?
- Where is the vulnerability?
- What is the probability?
- What would be the impact to the business?

This case study demonstrated how Tidal Pharmaceuticals addressed the specific NetOpS and SecOps challenges and concerns, and how they chose the right combination of products and features to design their three main branch types. The case study highlighted several of the built-in security features of the Cisco Catalyst SD-WAN architecture and dove deep into the products and features they deployed to protect its infrastructure and users from an expanded attack surface created by enabling distributed Internet access at each of their sites.

Appendix A: Configurations

NAT Tracker (All Branch Types)

```
endpoint-tracker diatracker-cisco
endpoint-dns-name www.cisco.com
interval 20
threshold 100
 tracker-type interface
```

NAT DIA Route (VPNs Guest and R & D)

```
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

Interface Configuration (All Branch Types)

```
interface GigabitEthernet0/0/0
 description Internet Transport
ip address x.x.x.x x.x.x.x
 no ip redirects
 ip nat outside
load-interval 30
 negotiation auto
 endpoint-tracker diatracker-cisco
arp timeout 1200
service-policy output shape_GigabitEthernet0/0/0
end
```

Per-VPN QoS (Branch Type 1)

```
policy-map shape_GigabitEthernet0/0/0
 class class-default
 shape average 200000000
service-policy VPN_QoS_Model_200Mbps
service-policy output shape_GigabitEthernet0/0/0


policy-map VPN_QoS_Model_200Mbps
 class Guest_VPN
bandwidth remaining ratio 5
shape average 1000000
service-policy site-qos-map_1Mbps
class Sales_VPN_4
bandwidth remaining ratio 25
shape average 5000000
service-policy site-qos-map_5Mbps
 class class-default
bandwidth remaining ratio 970
```

```
service-policy site-qos-map_194Mbps
service-policy VPN_QoS_Model_200Mbps
```

Traffic Redirection (Centralized Data Policy, VPN Sales/Clinical)

```
viptela-policy:policy
 data-policy Sales_VPN_4_DIA-Policy-1
  vpn-list Sales_VPN_4
    sequence 1
     match
      dns request
      source-ip 0.0.0.0/0
     !
     action accept
      nat use-vpn 0
      nat fallback
     !
    !
    sequence 21
     match
      destination-data-prefix-list o365-prefix
     !
     action accept
      nat use-vpn 0
      nat fallback
     !
    !
  default-action accept
 !
!
 lists
  data-prefix-list o365-prefix**
   ip-prefix x.x.x.x/x
  !
  site-list DIA-dual_site_list
   site-id 8200
  !
  vpn-list Sales_VPN_4
   vpn 4
  !
 !
!
apply-policy
```

```
 site-list DIA-dual_site_list
  data-policy _Guest_VPN_DIA-Policy-1_Sales_VPN_4_DIA-Policy-1 from-service
```

**See Microsoft documents for specific O365 prefixes.

VPN Membership (Centralized Data Policy, VPN Guest)

```
viptela-policy:policy
vpn-membership vpnMembership_635280740
sequence 10
     match
      vpn-list Guest_VPN
     !
     action accept
     !
    !
  default-action reject
 !
 lists
  site-list Guest_VPN_Site_List
site-id 8200
site-id 206202
  !
  vpn-list Guest_VPN
vpn 10
  !
 !
!
apply-policy
 site-list Guest_VPN_Site_List
vpn-membership vpnMembership_635280740
```

Security policy (Branch Types 1 and 2)

```
zone-based-policy ZBFW_inspect_guest_traffic
sequence 1
seq-name Rule_1
match
destination-port 53
protocol 6 17
protocol-name dns
!
action inspect
!
!
```

```
sequence 11
seq-name Rule_2
match
destination-port 80 443
protocol 6 17
protocol-name http https
!
action inspect
!
!
default-action drop
!
zone-based-policy ZBFW_allow_all_sales_traffic
sequence 1
seq-name Rule_1
action inspect
!
!
default-action drop
!
zone GUEST_ZONE
vpn 10
!
zone OUTSIDE
vpn 0
!
zone SALES_ZONE
vpn 4
!
zone-pair ZP_GUEST_ZONE_OUTSID_-1481917054
source-zone GUEST_ZONE
destination-zone OUTSIDE
zone-policy ZBFW_inspect_guest_traffic
!
zone-pair ZP_SALES_ZONE_OUTSIDE__-64344447
source-zone SALES_ZONE
destination-zone OUTSIDE
zone-policy ZBFW_allow_all_sales_traffic
!
!
exit
!
```

```
security
 umbrella
  dnscrypt
```