WAN Services

Design Summary

December 2013

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

This design summary provides information about the use cases covered in a series or set of related CVD guides and summarizes the Cisco products and technologies that solve the challenges presented by the use cases.

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd/wan

Introduction

Data networks are critical to an organization's viability and productivity. Online workforce-enablement tools are beneficial only if the data network provides reliable access to information resources. The number of users and locations in an organization can vary dramatically as an organization grows and adapts to changes in business activity. Providing a consistent user experience when users connect to the network increases their productivity. Whether users are sitting in an office at headquarters or working from a remote site, they require transparent access to the applications and files in order to perform their jobs. Cisco Wide Area Network (WAN) services enable an organization to improve application performance, reduce costs, enhance visibility, and provide greater resiliency.

Cisco WAN services are essential components of the Cisco Intelligent WAN (IWAN). Cisco IWAN delivers an uncompromised user experience over any connection, allowing an organization to right-size their network with operational simplicity and lower costs.

Business Use Cases

For remote-site users to effectively support the business, organizations require that the WAN provide services with sufficient performance and reliability. Because most of the applications and services that the remote-site worker uses are centrally located or hosted in the cloud, the WAN design must provide a common resource access experience to the workforce regardless of location. The following use cases present challenges for many organizations.

Use Case: Data Center Consolidation

Consolidating data centers while growing the remote-site population means that an increasing numbers of remote employees access LAN-based business applications across comparatively low speed WANs. With these applications growing increasingly multimedia-centric and latency-sensitive, Information Technology (IT) and networking staffs are further challenged to keep remote-application response times on par with the experiences of users situated locally to the company's application servers in the data center. Organizations have flat WAN budgets and must handle the new application requirements with the same or less bandwidth then previous years.

Use Case: Application Performance

Many organizations attempt to control costs by acquiring the minimum bandwidth necessary to handle traffic on a circuit. This strategy can lead to congestion and degraded application performance. Organizations need a way to help IT staff verify that quality of service (QoS) is implemented properly, so that latency-sensitive traffic, such as voice, video, and mission critical applications receive priority. They also want continuous security monitoring to detect denial-of-service attacks, network-propagated worms, and other undesirable network events that cause performance to suffer.

Use Case: High-Bandwidth Applications

Organizations want to deploy high-end video solutions, and their underlying networks must be appropriately designed to support the requirements for these solutions. They know traditional IP networks are not well-suited to deal with interactive and real-time requirements, making the delivery of video traffic unpredictable with increasing complexity for network operators and managers. Organizations need an easy way to reduce the complexity and lower the associated costs of deploying video conferencing.

Use Case: Applications in the Cloud

Organizations are looking at the benefits of hosting cloud-based applications at the remote office and allowing access to the public cloud directly. With the emergence of Software-as-a-Service (SaaS) applications such as Cisco WebEx meeting applications, Microsoft 365, and Google Docs, the resulting traffic patterns are limiting visibility and control for IT managers. Organizations want visibility into the network in order to enable resource alignment, ensuring that corporate assets are used appropriately in support of their goals.

Use Case: Efficient Access to Resources from Remote Sites

Although many of the applications and services that the remote-site worker uses are centrally located, there are benefits to providing local Internet access at each remote site location. Offloading Internet browsing and providing direct access to public cloud service providers can greatly reduce traffic on the private WAN, saving costs and improving overall remote site survivability. There is also a growing need for local Internet access from remote sites to improve cloud-based application performance. However, moving perimeter security from the data center to the remote sites, and permitting split tunneling for web access, increases security exposure.

The Value of Cisco WAN Services to an Organization

As organizations consider new business requirements, such as providing video and collaboration applications to its employees, IT departments face challenges associated with supporting all the different applications in the same network. IT needs to manage applications that have very different characteristics and requirements from the network. The IT challenges are exacerbated if you consider shrinking budgets and increasing end-user quality expectations, and as video and diverse applications become pervasive in employees' lives out of the office. Cisco WAN services help your organization minimize and deal with these challenges.

The days of conducting business with information stored locally in files on your computer are disappearing rapidly. The trend is for users to access mission-critical information by connecting to the network and downloading the information or by using a network-enabled application. Users depend upon shared access to common secured storage, web-based applications, and even cloud-based services. Users may start their day at home, in the office, or from a coffee shop, expecting to log on to applications that they need in order to conduct business, update their calendar, or check email—all important tasks that support your business. Connecting to the network to do your work has become as fundamental as turning on a light switch to see your desk; it's expected to work. Taken a step further, the network becomes a means to remain productive whether you are at your desk, roaming over wireless LAN within the facility, or working at a remote site, and you still have the same access to your applications and information.

Now that networks are critical to the operation and innovation of organizations, workforce productivity enhancements are built on the expectation of nonstop access to communications and resources. As networks become more complex in order to meet the needs of any device, any connection type, and any location, they incur an enhanced risk of downtime caused by poor design, complex configurations, increased maintenance, or hardware and software faults. At the same time, organizations seek ways to simplify operations, reduce costs, and improve their return on investment by exploiting their investments as quickly and efficiently as possible.

This design summary discusses how Cisco WAN services will benefit an organization.

Cisco WAN Services

There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for scale, purpose, redundancy, protection from tampering or denial of operation, and the capacity to handle peak loads, the network requires similar consideration. Users depend on the network in order to access the majority of the information they need to do their jobs and to carry their voice or video with reliability, so the network must be able to provide resilient, intelligent transport.

Many businesses have remote locations that depend entirely on applications hosted in a centralized data center or in the cloud. If a WAN outage occurs, these remote locations are essentially offline and they are unable to process transactions, make phone calls or support other types of business services. It is critical to provide reliable connectivity to these locations.

Cisco WAN services allow organizations to smoothly transition from premium WAN connections to less expensive Internet transport without compromising application performance, reliability, and security. With Cisco WAN services, IT can deliver a high level of reliability over any transport: Multiprotocol Label Switching (MPLS), Layer 2, Internet, or hybrid WAN deployments.

Cisco WAN services provide the following benefits to your organization:

Maximize your WAN usage to increase return on investment (ROI)—Help IT fully use its WAN investments and avoid oversubscription. The growth of cloud traffic, guest services, and video can be easily load-balanced across all WAN paths.

Lower costs and service delivery times—Give IT the flexibility to use a variety of providers smoothly, enabling the use of less expensive transport options without compromising performance, reliability, and security.

Help secure remote endpoints—Maintain remote user security by enabling Cisco Cloud Web Security (CWS) to securely and efficiently offload user web traffic.

Deliver application-aware network for optimal performance—Give IT full application-level visibility and control and help tune the network for handling business-critical services and quickly resolving network problems.

Apply advanced compression to minimize the WAN load—Reduce WAN bandwidth consumption by applying advanced compression and avoiding redundant data transfer in order to help applications perform better with the smallest load possible.

Simplify remote-site operations—Deliver rich features on a consolidated platform, providing IT a scalable approach to manage WAN traffic growth remotely from cloud, mobility, and video on a smaller, secure remote-site footprint.

To control operational costs, the WAN must support the convergence of voice, video, and data transport onto a single, centrally managed infrastructure. As organizations move into multinational or global business markets, they require a flexible network design that allows for country-specific access requirements without increased complexity.

The performance, reliable service level, and broad availability of carrier-provided MPLS networks and Layer 2 WAN networks makes these technologies a required consideration for an organization building a WAN.

While the Internet is quickly becoming a more stable platform with better price to performance and improved reliability, it still falls short of meeting standards for many businesses. With Cisco WAN services, IT has the security and application services to deliver the highest levels of resiliency and reliability over their choice of transports.

Introducing Cisco WAN Services

Cisco WAN services allow for the use of the most popular WAN transport technologies, which enables the network architect to choose the appropriate technology based on their business requirements. In some cases, service providers are limited in their coverage, or there is a large cost differential between technologies in certain areas of the world. Cisco WAN services allow an organization the flexibility to consider multiple options while maintaining a consistent user experience.

Some of the unique Cisco WAN services enabled by a Cisco network infrastructure include:

- Application optimization using Cisco WAAS—Allows an organization to apply advanced compression, data de-duplication and application acceleration to minimize WAN load and maximize WAN usage to increase its return on investment.
- Application monitoring using NetFlow—Delivers an application aware network to give an organization the full visibility and control to handle business-critical services and quickly resolve problems.
- Video quality monitoring using Medianet—Provides an organization with the ability to evaluate the videoconferencing and collaboration services running on the network in real-time, with historical data for longer periods.
- Cloud Web Security using Cisco ASA—Allows an organization to directly connect any two locations without backhauling to the data center and to offload traffic onto the Internet while seamlessly scaling security policies in order to protect remote site endpoints.
- Cloud Web Security using Cisco AnyConnect—Helps an organization secure remote user endpoints, which use the Internet to access systems on the internal network.
- Remote site using local Internet—Allows an organization to securely offload Internet browsing and provide direct access to public cloud service providers. This greatly reduces traffics on the private WAN, saving costs and improving overall performance and resiliency.
- Hosted Cloud Connector using Cisco UCS E-Series—Allows an organization to deploy applications at remote-site locations and improve performance by using local Internet access and by reducing traffic transmitted over private WAN links to the primary site. Integrating the application within the existing Cisco ISR router platform at the remote site, without requiring additional standalone platforms, simplifies the operational model.

The following table maps the business use cases to the Cisco WAN services.

Table 1 - Business use cases and Cisco WAN services

	Application optimization	Application monitoring	Video quality monitoring	Cloud Web Security	Local Internet	Hosted Cloud Connector
Data Center Consolidation	X	X			X	
Application Performance	X	X	X		X	X
High-Bandwidth Applications	X	X	X		X	
Applications in the Cloud		X		X	X	X
Efficient Access to Resources from Remote Sites				X	X	X

Each of the Cisco WAN services are discussed in more detail in the following sections of the design summary.

Application Optimization Using Cisco WAAS

The number of remote work sites is increasing, so network administrators need tools to help them ensure solid application performance in remote locations. Recent trends show that a majority of new hires are located at remote sites. These trends are tied to global expansion, employee attraction and retention, mergers and acquisitions, cost savings, and environmental concerns. The enterprise trend toward data-center consolidation also continues.

Consolidating data centers while growing the remote-site population means that increasing numbers of remote employees access LAN-based business applications across comparatively slow WANs. These local users enjoy multimegabit LAN speeds and are not affected by any distance-induced delay, unlike their counterparts at the other end of a WAN connection.

Application optimization can boost network performance along with enhancing security and improving application delivery. Cisco WAN Optimization using Cisco Wide Area Application Services (Cisco WAAS) is an architectural solution comprising a set of tools and techniques that work together in a systems approach to provide best-in-class WAN optimization performance while minimizing its total cost of ownership.

Application optimization using Cisco WAAS enables the following capabilities:

- Enhanced end-user experience increasing effective bandwidth and reducing latency
- Integration into the existing Cisco WAN routers, providing a flexible deployment
- Centralized operation and management of all the organization's application optimization devices

WAAS Nodes

A WAAS node is a Cisco WAAS application accelerator that optimizes and accelerates traffic according to the optimization policies configured on the device. A WAAS node group is a group of WAAS nodes that services a particular set of traffic flows identified by AppNav policies.

Cisco Application Navigator

Cisco Application Navigator (AppNav) technology enables customers to virtualize WAN optimization resources by pooling them into one elastic resource in a manner that is policy based and on demand with the best available scalability and performance. It integrates transparently with Cisco WAAS physical and virtual network infrastructure and supports the capability to expand the WAN optimization service to meet future demands.

The Cisco AppNav solution is comprised of one or more Cisco AppNav Controllers, which intelligently load-share network traffic for optimization to a set of resource pools built with Cisco WAAS nodes. The Cisco AppNav Controllers make intelligent flow distribution decisions based on the state of the WAAS nodes currently providing services.

A Cisco AppNav Controller (ANC) is a Cisco WAVE appliance with a Cisco AppNav Controller Interface Module (IOM) that intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more WNGs for optimization. The ANC function is also available as a component of Cisco IOS-XE running on the Cisco ASR1000 Series routers and the Cisco ISR4451-X router. When the ANC is running as a router software component, it is referred to as AppNav-XE.

A Cisco AppNav Controller group (ANCG) is a group of AppNav Controllers that share a common policy and together provide the necessary intelligence for handling asymmetric flows and providing high availability. The group of all ANC and WAAS node (WN) devices configured together as a system is referred to as an AppNav Cluster.

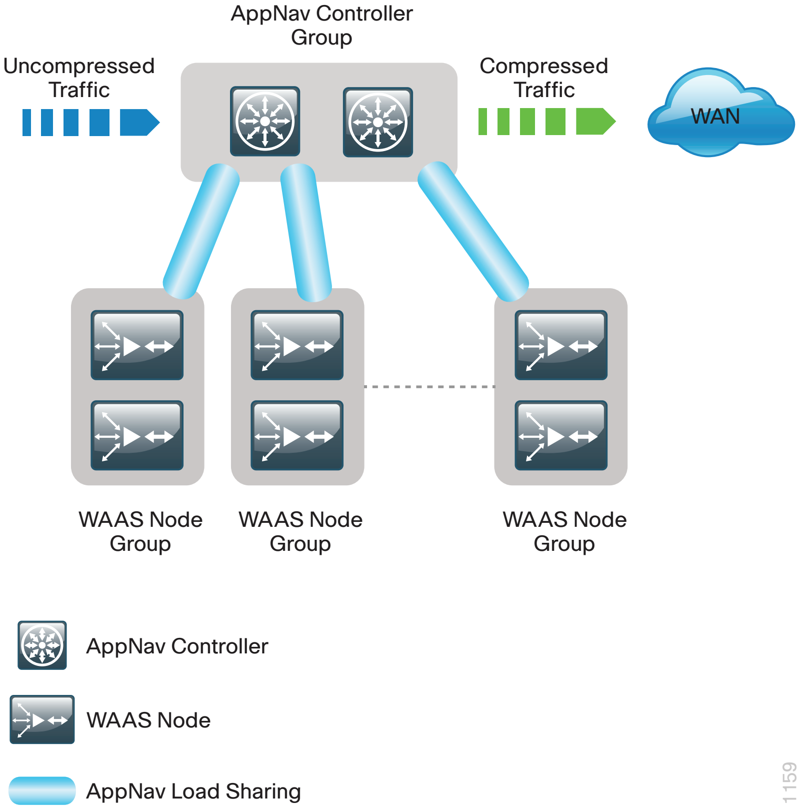
Reader Tip

Some Cisco product documentation may use different terminology. This guide references the most common terminology in use for consistency.

Examples:
WAAS Node (WN) = Service Node (SN)
WAAS Node Group (WNG) = Service Node Group (SNG)

AppNav Controller (ANC) = AppNav Controller (AC)
AppNav Controller Group (ANCG) = AppNav Controller Group (ACG)

Figure 1 - WAAS AppNav components

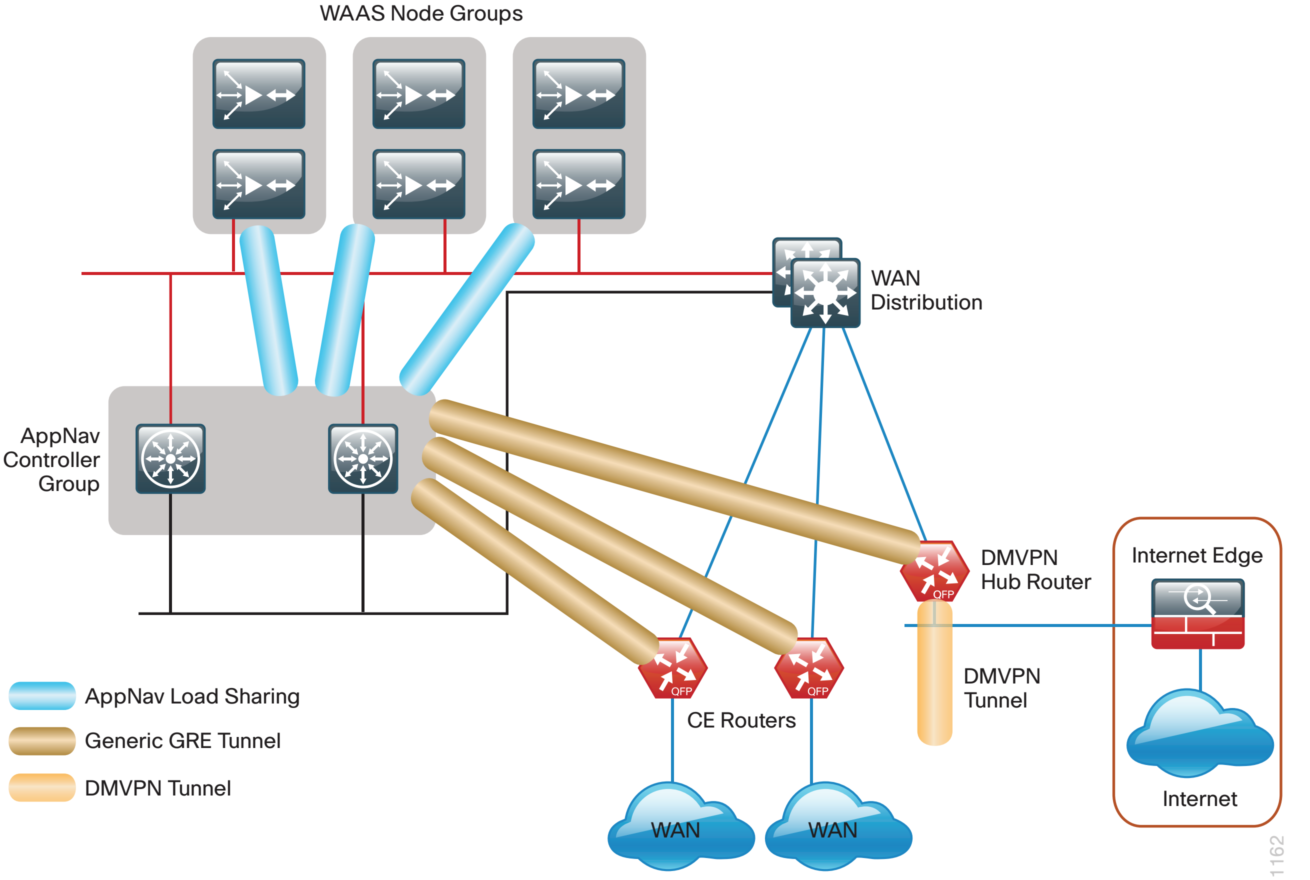


AppNav Off-Path Design Model

The AppNav off-path design is the preferred model for new deployments. This design logically inserts the ANCs between the redirecting routers and the WAAS node group(s). WCCP is still used between the routers and the AppNav controllers, but the WCCP function is strictly limited to redirection and performs no load sharing. AppNav performs the intelligent load sharing.

The connections from the distribution switch to the WAN aggregation routers are routed point-to-point links. This design mandates the use of a generic GRE tunnel between the ANCs and the routers. When a design uses a generic GRE tunnel, it is not required that the ANCs and the WAN aggregation routers are Layer 2 adjacent.

Figure 2 - AppNav off-path deployment model



Remote-Site Design Models

The WAN optimization design for the remote sites can vary somewhat based on site-specific characteristics. Single router sites use a single (non-redundant) Cisco WAVE appliance or vWAAS instance. Dual-router sites use dual WAVE appliances or vWAAS instances. The specifics of the WAAS sizing and form factor primarily depend on the number of end users and bandwidth of the WAN links.

Figure 3 - Cisco WAAS topology—remote-site access-layer design

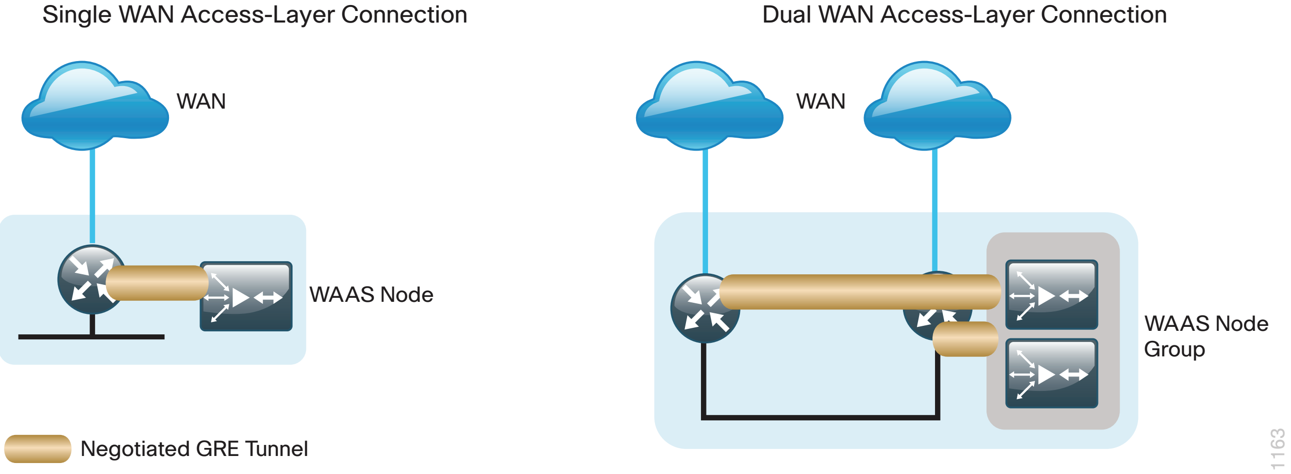
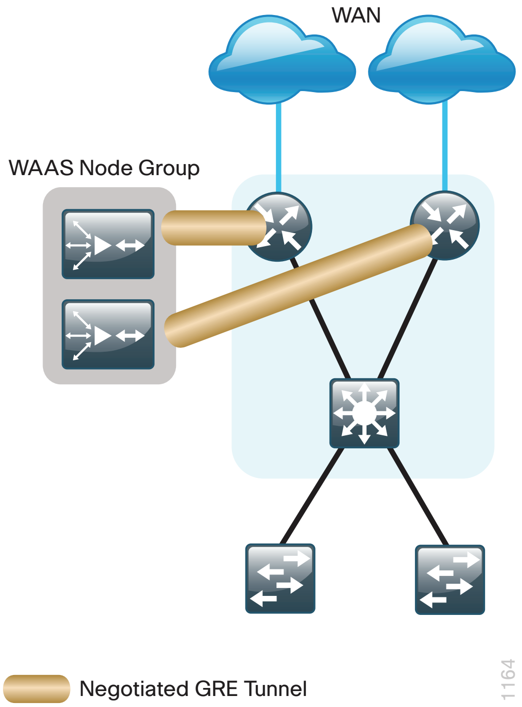

Single WAN Access-Layer Connection
WAN
WAAS Node
Negotiated GRE Tunnel
Dual WAN Access-Layer Connection
WAN
WAAS Node Group
1163

Figure 4 - Cisco WAAS topology—remote-site distribution-layer design



For information about how to deploy this WAN service, see the Application Optimization Using Cisco WAAS Technology Design Guide.

ISR-WAAS

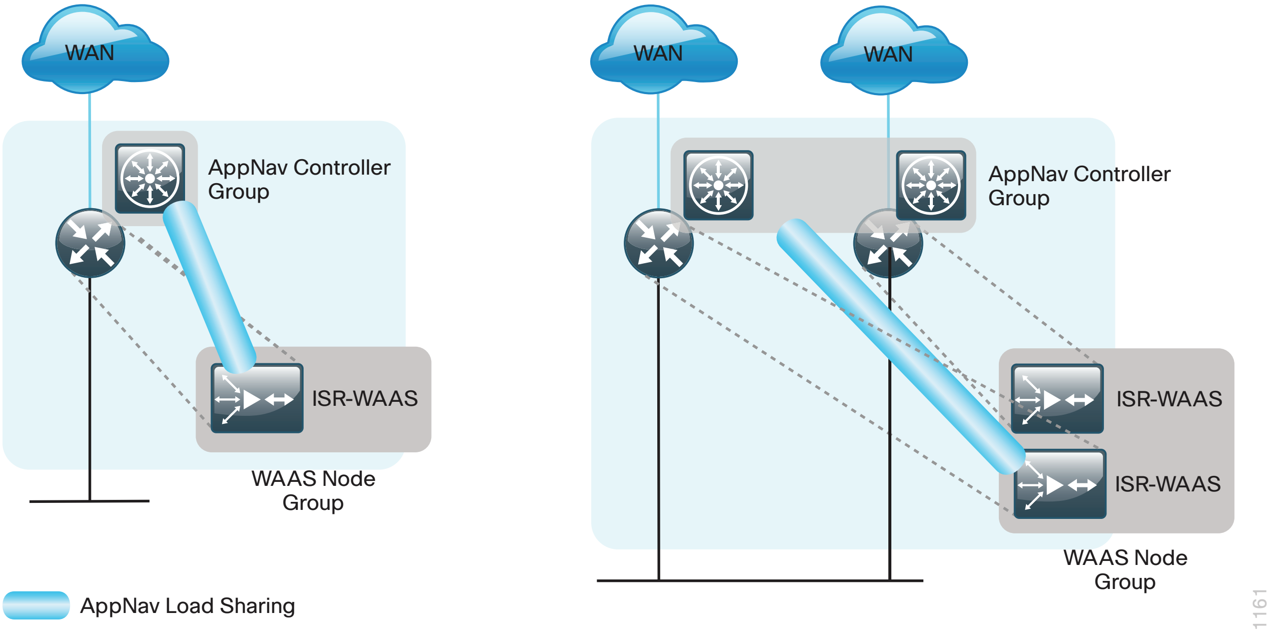
The Cisco ISR4451-X router is the first ISR router to run Cisco IOS-XE Software. The multi-core CPU architecture of the Cisco ISR4451-X supports a built-in services virtualization framework that enables on-demand deployment of services such as a vWAAS instance. The specific implementation of vWAAS running in a Cisco IOS-XE Software container on the Cisco ISR4451-X router is referred to as ISR-WAAS. The term *container* refers to the keyboard, video, and mouse (KVM) hypervisor that runs virtualized applications on the Cisco ISR4451-X router.

In this virtualization framework, the router is the host machine and the virtual-service is a guest OS. The virtual-service shares CPU and memory resources with the host router. Additionally, to deploy a virtual-service, the router requires additional storage beyond the standard bootflash.

ISR-WAAS Remote-Site Design Models

The combination of AppNav-XE and ISR-WAAS on the Cisco ISR4451-X router is entirely self-contained when deployed at a single-router remote-site. Logically, AppNav-XE runs separately on the host OS and ISR-WAAS runs as a guest OS. You configure service insertion on the router and traffic is redirected to ISR-WAAS, but in this case traffic never leaves the router.

Figure 5 - Cisco ISR-WAAS remote-site design models



The dual-router remote-site provides additional resiliency from a hardware and software perspective. Each router runs AppNav-XE and ISR-WAAS. You configure a single ANCG to distribute traffic for optimization to a single WNG that includes the ISR-WAAS instances from both routers. The application traffic load is shared across both ISR-WAAS instances in the WNG depending on the traffic flows and utilization of each ISR-WAAS. Traffic may be sent between the two routers in order to support this resiliency and load sharing.

For information about how to deploy this WAN service, see the Application Optimization Using Cisco ISR-WAAS Technology Design Guide.

Application Monitoring Using NetFlow

There are several trends in the enterprise today driving requirements to build application awareness within the network. The network is the critical infrastructure that enables and supports business processes throughout all the functions of an organization. For the staff responsible for planning, operation, and maintenance of the network and network services, it is indispensable to have visibility into the current health of the network from end-to-end.

Cisco Application Visibility and Control (AVC) combines several key technologies such as NetFlow and Network Based Application Recognition (NBAR) in order to gain deeper insight into application and user traffic flows on the network. Greater visibility helps to quickly isolate and troubleshoot application performance and security related issues.

Organizations need a way to help IT staff verify that quality of service (QoS) is implemented properly, so that latency-sensitive traffic, such as voice or video, receives priority. They also want continuous security monitoring to detect denial-of-service (DoS) attacks, network-propagated worms, and other undesirable network events.

Application monitoring using NetFlow enables the following capabilities:

- Deploy flexible NetFlow (FNF) with NBAR2 to identify application traffic and impacts on the network.
- Reduce peak WAN traffic by using NetFlow statistics to measure WAN traffic changes associated with different application policies, and understand who is utilizing the network and who the network's top talkers are.
- Diagnose slow network performance, bandwidth hogs, and bandwidth utilization in real-time with command-line interface (CLI) or reporting tools.
- Detect and identify unauthorized WAN traffic and avoid costly upgrades by identifying the applications that are causing congestion.
- Detect and monitor security anomalies and other network disruptions and their associated sources.
- Export FNF with NBAR data to Cisco Prime Infrastructure and other third-party collectors by using NetFlow v9 and IP Flow Information Export (IPFIX).
- Validate proper QoS implementation and confirm that appropriate bandwidth has been allocated to each class of service (CoS).

Traditional NetFlow

Cisco IOS NetFlow allows network devices that are forwarding traffic to collect data on individual traffic flows. Traditional NetFlow (TNF) refers to the original implementation of NetFlow, which specifically identified a flow as the unique combination of the following seven key fields:

- IPv4 source IP address
- IPv4 destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type-of-service (ToS) byte
- Input logical interface

These key fields define a unique flow. If a flow has one different field than another flow, then it is considered a new flow.

Flexible NetFlow

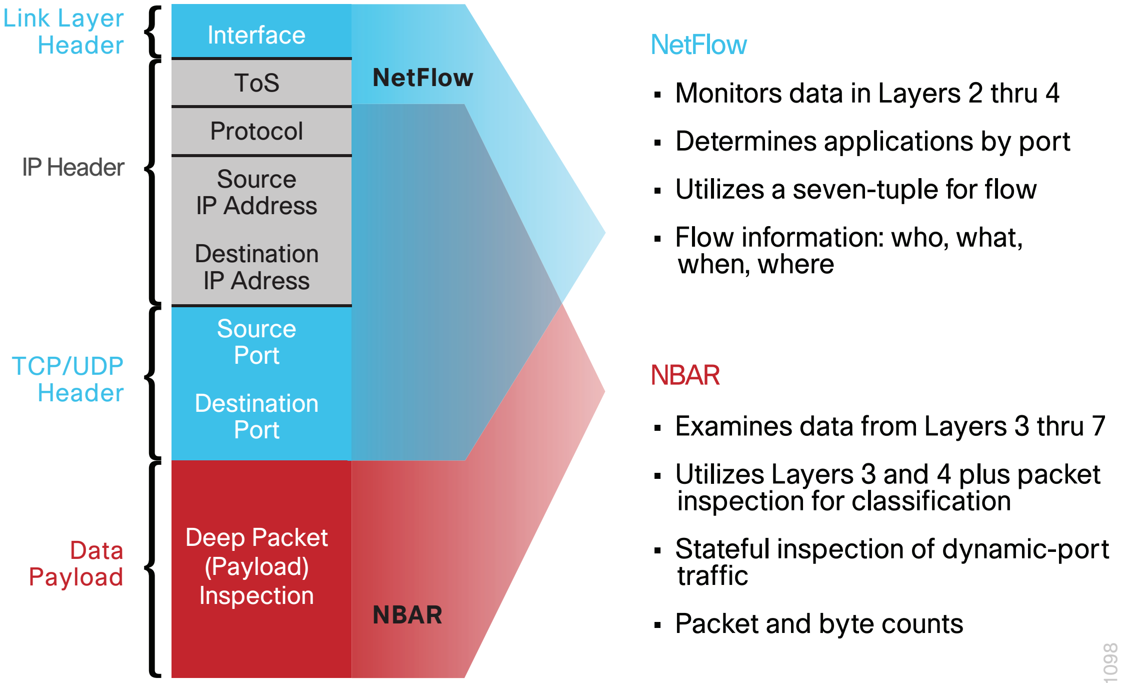
Flexible NetFlow (FNF), unlike TNF, allows you to customize and focus on specific network information. You can use a subset or superset of the traditional seven key fields to define a flow. FNF also has multiple additional fields (both key and non-key). This permits an organization to target more specific information so that the total amount of information and the number of flows being exported is reduced, allowing enhanced scalability and aggregation.

Network-Based Application Recognition

In the past, typical network traffic could be easily identified by using well known port numbers. Today, many applications are carried on the network as HTTP and HTTPS, so identifying applications by their well-known port number is no longer sufficient.

Network Based Application Recognition (NBAR) is an intelligent classification engine in Cisco IOS Software that can recognize a wide variety of applications, including web-based and client/server applications. NBAR uses deep packet inspection to look within the transport layer payload in order to determine the associated application, as shown in the following figure.

Figure 6 - NetFlow and NBAR integration


Link Layer Header
Interface
ToS
Protocol
IP Header
Source IP Address
Destination IP Adress
TCP/UDP Header
Source Port
Destination Port
Data Payload
Deep Packet (Payload) Inspection
NetFlow
NBAR
NetFlow
▪ Monitors data in Layers 2 thru 4
▪ Determines applications by port
▪ Utilizes a seven-tuple for flow
▪ Flow information: who, what, when, where
NBAR
▪ Examines data from Layers 3 thru 7
▪ Utilizes Layers 3 and 4 plus packet inspection for classification
▪ Stateful inspection of dynamic-port traffic
▪ Packet and byte counts
1098

Next Generation NBAR

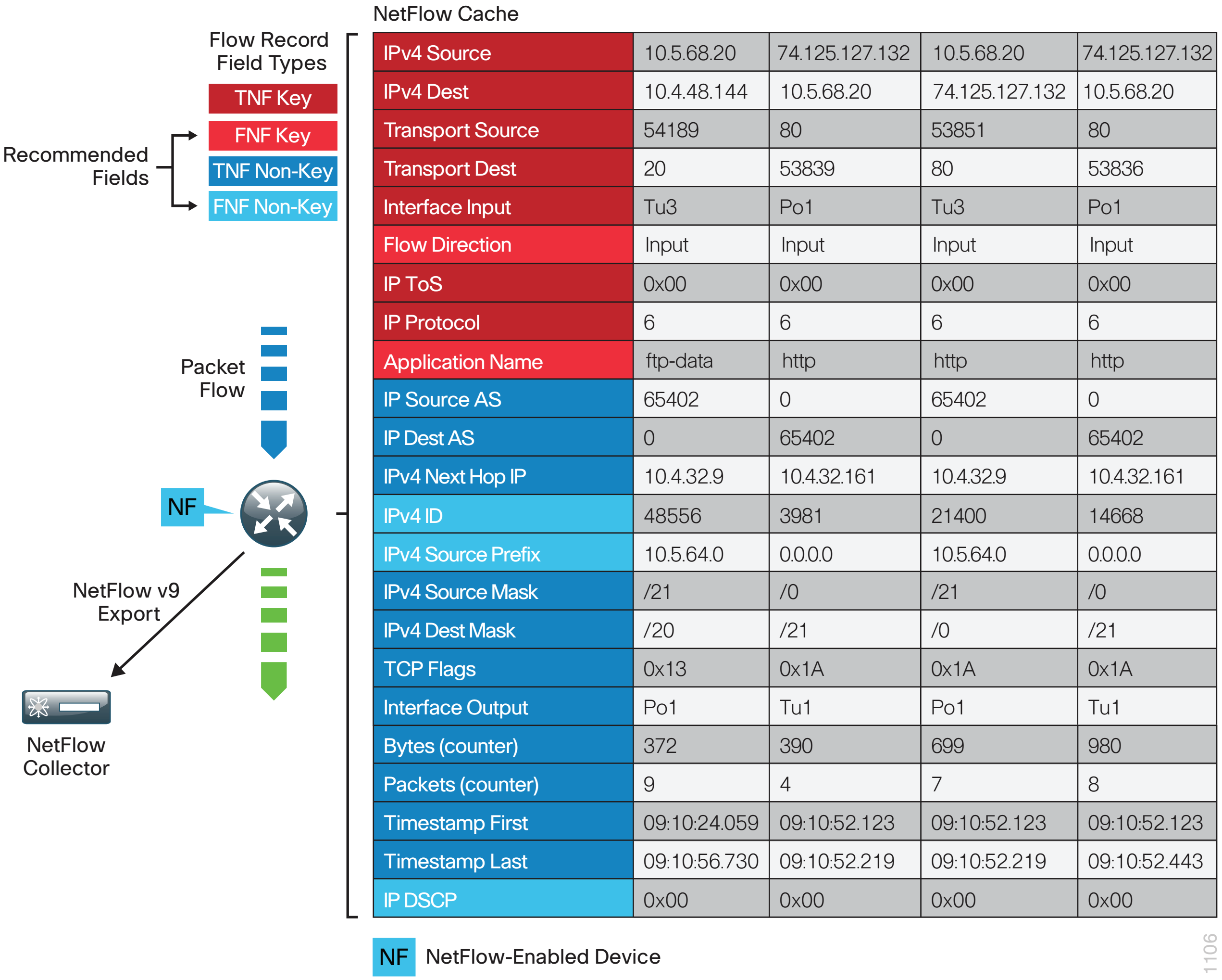
Next Generation NBAR2 (NBAR2) is the next-generation architectural evolution of NBAR. NBAR2 is part of the Cisco AVC solution, which enables greater classification and visibility of network traffic flows. NBAR2 is a stateful, deep packet inspection technology based on the Cisco Service Control Engine with advanced classification techniques, greater accuracy, and many more application signatures supporting over 1000 applications and sub-classifications.

NetFlow Monitoring

The NetFlow data can be viewed directly from the NetFlow-enabled device through the use of CLI **show** commands, but this method is somewhat cumbersome, and it is difficult to correlate the data across multiple devices.

The router exports the flow details to an external device running a flow collector service, as shown in the following figure. The cached flow data is sent periodically, based upon configurable timers. The collector is capable of storing an extensive history of flow information that was switched within the NetFlow device. NetFlow is very efficient; the amount of export data is only a small percentage of the actual traffic in the router or switch. NetFlow accounts for every packet (when in non-sampled mode) and provides a highly condensed and detailed view of all network traffic that entered the router or switch. The NetFlow collector should be located in the server room or data center.

Figure 7 - Flexible NetFlow export to collector



IPv4 Source	10.5.68.20	74.125.127.132	10.5.68.20	74.125.127.132
IPv4 Dest	10.4.48.144	10.5.68.20	74.125.127.132	10.5.68.20
Transport Source	54189	80	53851	80
Transport Dest	20	53839	80	53836
Interface Input	Tu3	Po1	Tu3	Po1
Flow Direction	Input	Input	Input	Input
IP ToS	0x00	0x00	0x00	0x00
IP Protocol	6	6	6	6
Application Name	ftp-data	http	http	http
IP Source AS	65402	0	65402	0
IP Dest AS	0	65402	0	65402
IPv4 Next Hop IP	10.4.32.9	10.4.32.161	10.4.32.9	10.4.32.161
IPv4 ID	48556	3981	21400	14668
IPv4 Source Prefix	10.5.64.0	0.0.0.0	10.5.64.0	0.0.0.0
IPv4 Source Mask	/21	/0	/21	/0
IPv4 Dest Mask	/20	/21	/0	/21
TCP Flags	0x13	0x1A	0x1A	0x1A
Interface Output	Po1	Tu1	Po1	Tu1
Bytes (counter)	372	390	699	980
Packets (counter)	9	4	7	8
Timestamp First	09:10:24.059	09:10:52.123	09:10:52.123	09:10:52.123
Timestamp Last	09:10:56.730	09:10:52.219	09:10:52.219	09:10:52.443
IP DSCP	0x00	0x00	0x00	0x00

The most effective to way to view NetFlow data is through a dedicated analysis application, which is typically paired with the flow-collector service. The various applications are focused on traffic analysis, security (anomaly detection and denial of service), or billing. TNF-monitoring applications expect a standard set of fields to be exported. Each specific FNF-monitoring application will likely have a custom set of NetFlow attributes and a particular export format that must be configured on the NetFlow-enabled device before data can be sent to the collector.

Internet Protocol Flexible Export (IPFIX)

Internet Protocol Flow Information Export (IPFIX) is an IETF–defined, standard protocol for exporting IP flow information. It is based on Cisco Netflow v9 and is sometimes referred to as Netflow v10. The IPFIX export format enables several new capabilities that are not supported with NetFlow v9, such as the ability to put multiple messages into a single datagram, allow vendor unique elements, and allow variable length strings.

Support for variable length fields becomes important when you need to export NBAR2 extracted fields. NBAR2's field extraction capability, such as HTTP URL, Session Initiation Protocol (SIP) domain, and Mail server, allows you to extract information for classification or exporting. When you need this type of information, you are required to use IPFIX.

For information about how to deploy this WAN service, see the Application Monitoring Using Netflow Technology Design Guide.

Video Quality Monitoring Using Medianet

IP-based video conferencing has emerged as the dominant technology in the video-conferencing market. This market includes a broad range of options, ranging from high-definition telepresence systems and room-based solutions at the high-end to dedicated desktop systems at the midrange and PC, desktops, and laptops with web cameras at the low end. The low-end solutions typically rely on best-effort QoS, requiring no specific capabilities from the network. With these lower-end solutions, the video and audio quality may vary significantly depending on what other applications are currently active on the network.

Organizations want to deploy high-end video solutions and their underlying networks must be appropriately designed to support the requirements. They know traditional IP networks are not well-suited to handling interactive and real-time requirements, making the delivery of video conferencing traffic unpredictable with increasing complexity for network operators and managers. Organizations need an easy way to reduce the complexity and lower the associated costs of deploying video conferencing.

Video quality monitoring using medianet enables the following capabilities:

- Video conference quality monitoring
- Simplified installation and management of video endpoints
- Faster troubleshooting for voice, data, and video applications
- Impact assessment of video, voice, and data in your network
- Service-level agreement (SLA) assurance and negotiation
- Collection of key metrics for the service provided
- Faster end-user adoption of rich-media applications through a high-quality, positive user experience

Medianet

Cisco Medianet media monitoring consists of three complementary technologies:

- **Performance Monitor (PerfMon)**—Allows you to analyze the performance of rich-media traffic across the network to provide a holistic view of the network service being delivered. PerfMon can also generate alerts based on defined performance thresholds.
- **Mediatrace**—Discovers Layer 2 and Layer 3 nodes along a flow path. Mediatrace implicitly uses PerfMon in order to provide a dynamic hop-by-hop analysis of media flows in real time to facilitate efficient and targeted diagnostics.

- IP Service-Level Agreement Video Operation (IPSLA VO)—Generates synthetic traffic streams that are very similar to real-media traffic. It can be used in conjunction with Mediatrace in order to perform capacity planning analysis and troubleshooting even before applications are deployed.

You can use PerfMon and Mediatrace to quickly and cost-effectively respond to any video-conferencing quality issues. This capability allows the organization to maintain a reliable and high-quality service for their video-conference attendees. IPSLA VO capabilities allow an organization to plan for future growth in network capacity and provided services.

PerfMon

PerfMon maintains historical data about specific classes of flows traversing routers and switches. The metrics collected by PerfMon can be exported to a network management tool through Flexible NetFlow (FNF) and Netflow version 9 or Simple Network Management Protocol (SNMP). A collector/analysis application can further analyze, summarize, and correlate this information to provide traffic profiling, base-lining, and troubleshooting services for the application and network operations staff.

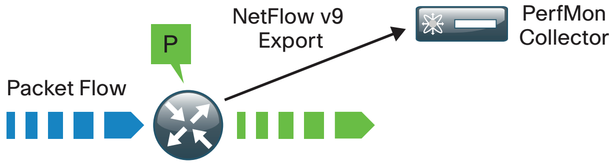
PerfMon uses multiple flow records depending on the protocol being analyzed, either TCP or Real-Time Transport Protocol (RTP), which is commonly used for delivering video and audio that uses User Datagram Protocol (UDP) over IP networks. RTP-specific information such as the Synchronization Source Identifier (SSRC) is essential for tracking and evaluating overall video conferencing performance. The SSRC is a session identifier for every unique audio or video stream, which is required because the source and destination IP addresses (and sometimes the UDP ports) are the same for each of the multiple individual audio or video streams that make-up a high-definition video call.

PerfMon Monitoring

You can view data directly from the PerfMon-enabled device by using CLI **show** commands, but this method is somewhat cumbersome, and it is difficult to correlate the data across multiple devices.

The router exports the PerfMon details to an external device running a flow collector service as shown in the following figure; this is essentially the same operation as a NetFlow export. The collector is capable of storing an extensive history of flow information that was switched within the PerfMon device.

Figure 8 - PerfMon export to collector with predefined RTP flow record



IPv4 Source	10.5.83.40	10.5.4.40	10.4.4.40	10.4.0.40
IPv4 Dest	10.5.3.40	10.5.83.40	10.5.12.40	10.5.12.40
IP Protocol	17	17	17	17
Transport Source	2334	51152	51178	51182
Transport Dest	51150	2336	2350	2352
RTP SSRC	382412038	3578537236	3704889529	1600458234
IPv4 DSCP	34	34	34	34
IPv4 TTL	63	57	57	57
Packets Expected	15007	27671	15009	13262
Packets Lost	0	301	54	81
Packets Lost Rate	0.00%	1.08%	0.35%	0.61%
Event Packet Lost	0	266	58	71
RTP Jitter (mean)	802 usec	7661 usec	6824 usec	6106 usec
RTP Jitter (min)	0 usec	1 usec	0 usec	0 usec
RTP Jitter (max)	6387 usec	137558 usec	74955 usec	75495 usec
Interface Input	Gig0/2.64	Gig0/0	Gig0/0	Gig0/0
Interface Output	Gi0/0	Gi0/2.64	Gi0/2.64	Gi0/2.64
Bytes	3135249	35570174	2766284	11173608
Packets	15007	27370	14955	13181
Bytes Rate	10450 (Bps)	118567 (Bps)	10217 (Bps)	37245 (Bps)
Packets Dropped	0	0	0	0
Application Media Bytes	2835109	35022774	2766284	10909988
Application Media Bytes Rate	9450 (Bps)	116742 (Bps)	9220 (Bps)	36366 (Bps)
Application Media Packets	15007	27370	14955	13181
Application Media Packets Rate	50 (pps)	91 (pps)	49 (pps)	43 (pps)

Key Field
Non-Key Field
Default RTP
Flow Record
Field Types

P PerfMon-Enabled Device

3031

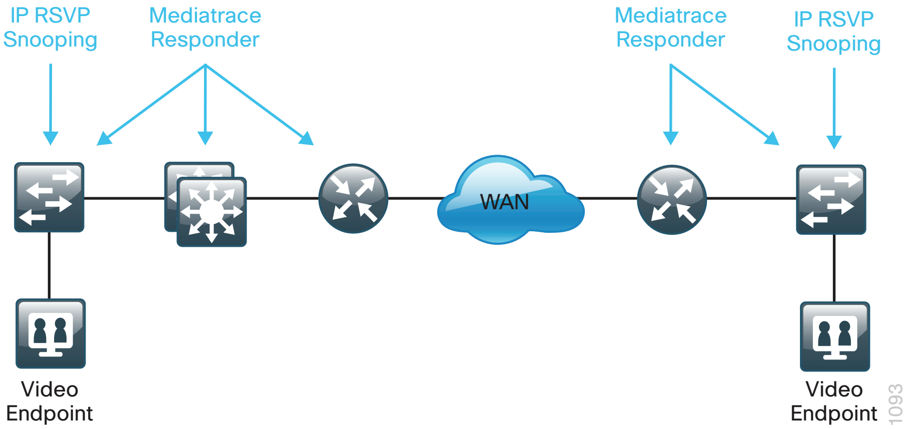
The most effective to way to view PerfMon data is through a dedicated analysis application, which is typically paired with the flow collector service. PerfMon analysis applications are often paired with NetFlow applications, in which case you do not need to install a separate application. Some vendors have added PerfMon analysis to existing video-monitoring applications, without adding full NetFlow analyzer capabilities.

Mediatrace

Cisco Mediatrace is a network diagnostic tool that monitors the state of an audio, video, or data flow across a network path. Mediatrace discovers Layer 2 and Layer 3 devices along the flow path and can collect information from these devices. The types of information include device-specific and interface-specific data, as well as PerfMon data for individual flows.

The IP traceroute tool is a close analog to the Cisco Mediatrace tool; both are capable of determining the intermediate hops of a one-way path between two IP endpoints. Mediatrace extends this capability in several ways. Both Layer 2 and Layer 3 devices can be detected with Mediatrace, but this requires that the devices be configured as Mediatrace responders. An additional requirement for Layer 2 devices is that IP Resource Reservation Protocol (RSVP) snooping be enabled, so that Mediatrace traffic can be properly directed to the Medianet responder on the device. See the following figure for more details.

Figure 9 - Cisco Mediatrace responder and IP RSVP snooping by device



The Cisco Mediatrace initiator device can use either an on-demand or scheduled data collection session to perform a hop-by-hop discovery as well as collect the metrics of interest. Currently, the Mediatrace initiator must be a Cisco router or Cisco switch.

Reader Tip

Although Cisco does not currently have a Mediatrace technology design guide, this guide includes information about Mediatrace in order to present a comprehensive discussion of Cisco Medianet technology.

IPSLA VO

IPSLA Video Operation (IPSLA VO) functions as a valuable tool to assess the readiness of a network to carry rich-media traffic. It has the ability to synthetically generate video profiles that mimic real application traffic, such as Cisco TelePresence activity, IP video surveillance, or IPTV traffic. IPSLA VO can also make use of user-captured packet traces from the customer's existing network, which can then be included in the synthetically generated traffic stream. You can also use this feature to run network readiness tests prior to important collaboration meetings in order to validate that the network will be able to support the expected rich-media traffic.

Reader Tip

Although Cisco does not currently have IPSLA VO technology guide, this guide includes information about IPSLA VO in order to present a comprehensive discussion of Cisco Medianet technology.

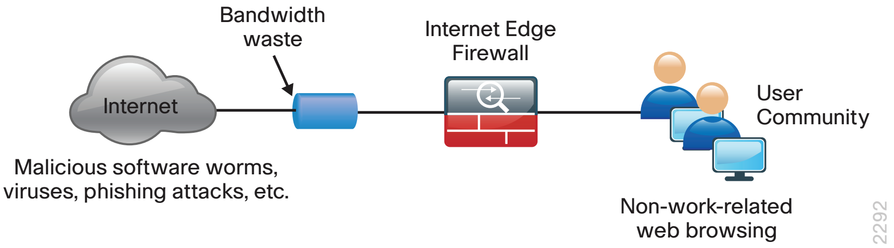
For information about how to deploy this WAN service, see the Video Quality Monitoring Using Medianet Technology Design Guide.

Cloud Web Security

Web access is a requirement for the day-to-day functions of most organizations, but a challenge exists to maintain appropriate web access for everyone in the organization, while minimizing unacceptable or risky use. A solution is needed to control policy-based web access in order to ensure employees work effectively and ensure that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.

Another risk associated with Internet access for the organization is the pervasive threat that exists from accessing sites and content. Other threats include the still popular and very broad threats of viruses and *Trojans*, in which a user receives a file in some manner and is tricked into running it, and the file then executes malicious code. The third variant uses directed attacks over the network. These types of risks are depicted in the figure below.

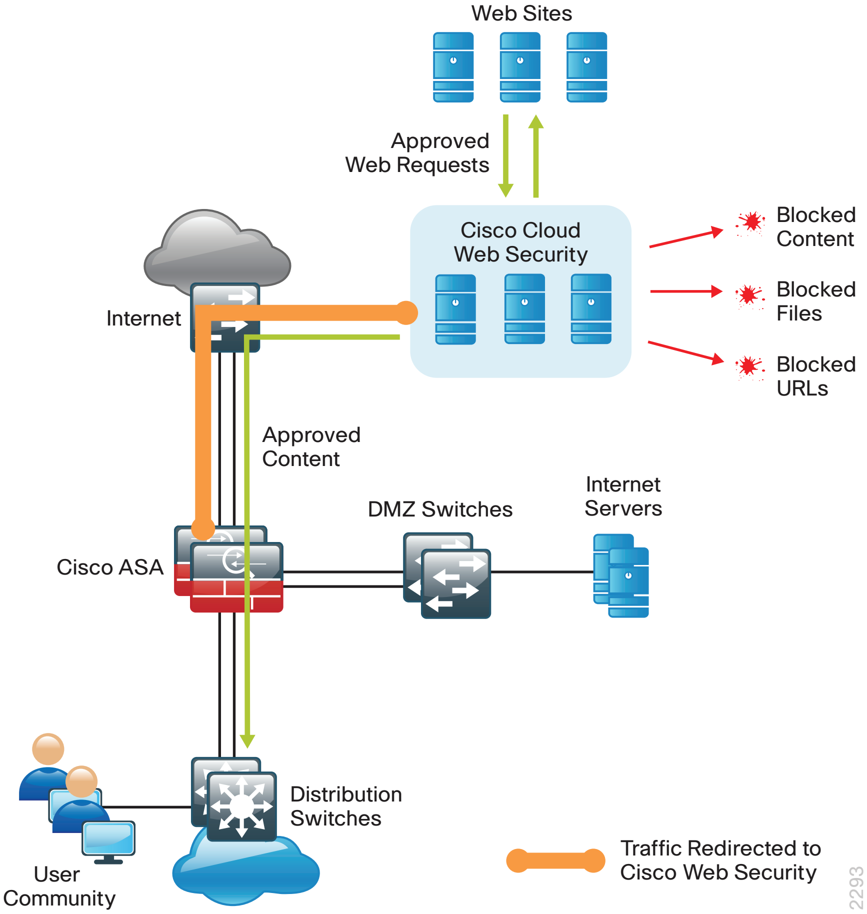
Figure 10 - Business reasons for deploying Cisco Cloud Web Security


Bandwidth waste
Internet Edge Firewall
Internet
User Community
Malicious software worms, viruses, phishing attacks, etc.
Non-work-related web browsing
2292

Cisco Cloud Web Security (CWS) addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection.

Through the use of multiple techniques, Cisco CWS provides granular control over all web content that is accessed. These techniques include real-time dynamic web content classification, a URL-filtering database, and file-type and content filters. The policies enforced by Cisco CWS provide strong web security and control for an organization. Cisco CWS policies apply to all users regardless of their location and device type.

Figure 11 - Cisco CWS Internet edge design



Cisco ASA

Internal users at both the primary site and remote sites access the Internet by using the primary site's Internet-edge Cisco Adaptive Security Appliance (ASA), which provides stateful firewall and intrusion prevention capabilities. It is simple and straightforward to add Cisco CWS to a Cisco ASA appliance that is already configured and operational. This integration uses the Cloud Web Security Connector for Cisco ASA and requires no additional hardware.

Cloud Web Security using Cisco ASA enables the following security capabilities:

- Transparent redirection of user web traffic—Through seamless integration with the Cisco ASA firewall, web traffic is transparently redirected to the Cisco CWS service. No additional hardware or software is required, and no configuration changes are required on user devices.
- Web filtering—Cisco CWS supports filters based on predefined content categories and it also supports more detailed custom filters that can specify application, domain, and content type or file type. The filtering rules can be configured to block or warn based on the specific web-usage policies of an organization.
- Malware protection—Cisco CWS analyzes every web request in order to determine if content is malicious. CWS is powered by the Cisco Security Intelligence Operations (SIO) whose primary role is to help organizations secure business applications and processes through identification, prevention, and remediation of threats.

- **Differentiated policies**—The Cisco CWS web portal applies policies on a per-group basis. Group membership is determined by the group authentication key of the forwarding firewall, source IP address of the web request, or the Microsoft Active Directory user and domain information of the requestor.

The Cisco ASA firewall family sits between the organization's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security. The design uses Cisco ASA to implement a service policy that matches specified traffic and redirects the traffic to the Cisco CWS cloud for inspection. This method is considered a transparent proxy, and no configuration changes are required to web browsers on user devices.

The various traffic flows for each of these user types are shown in the following figures.

Figure 12 - Cisco CWS with internal and guest users

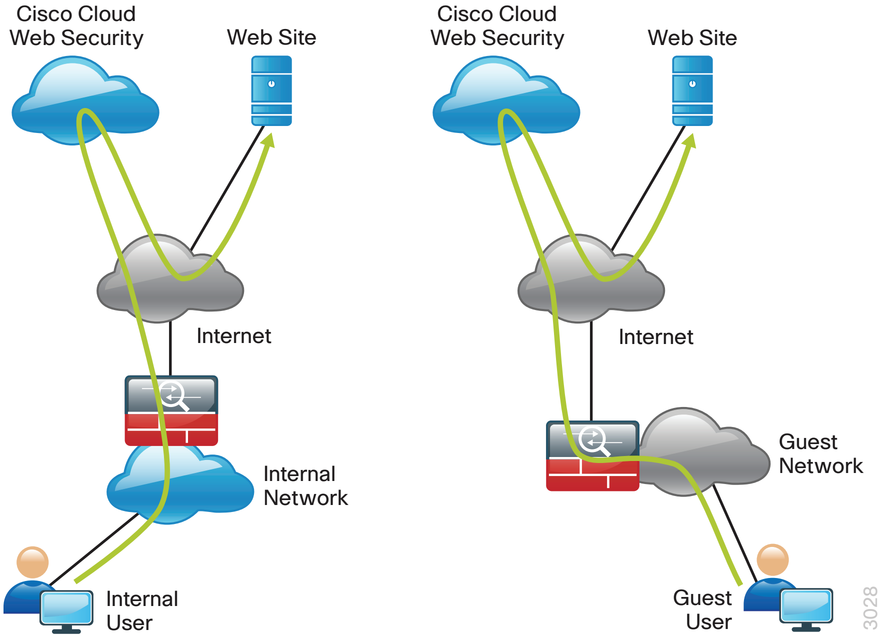
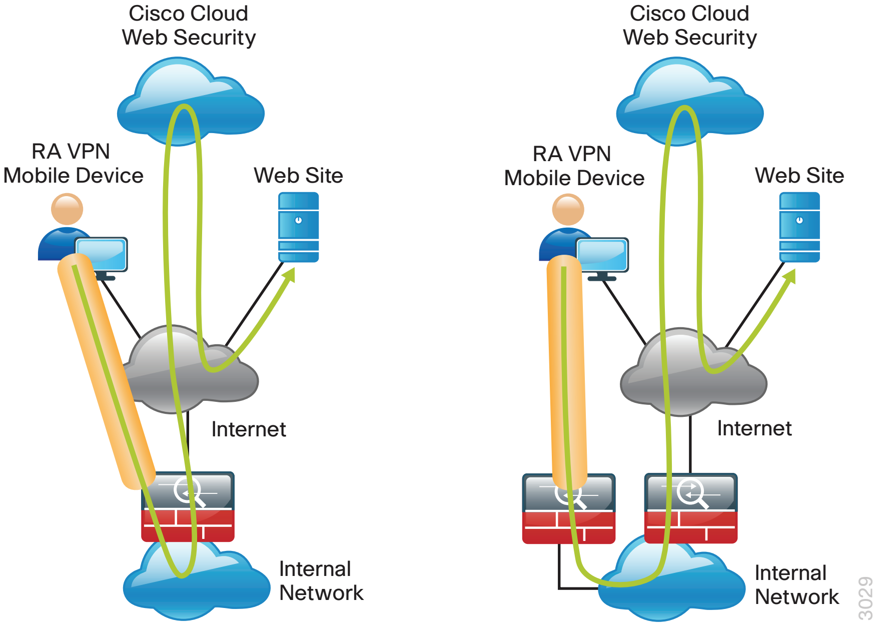


Figure 13 - Cisco CWS for mobile devices using remote-access VPN



Certain source and destination pairs should be exempted from the service policy, such as remote-access VPN users accessing internal networks or internal users accessing demilitarized zone (DMZ) networks.

For information about how to deploy this WAN service, see the Cloud Web Security Using Cisco ASA Technology Design Guide.

Cisco AnyConnect

Mobile remote users connect to their organization's network by using devices that generally fall into two categories: laptops and mobile devices such as smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ. Laptops and other devices that support the Cisco AnyConnect Secure Mobility Client with Cisco CWS are not required to send web traffic to the primary site.

Cloud Web Security using Cisco AnyConnect enables the following security capabilities:

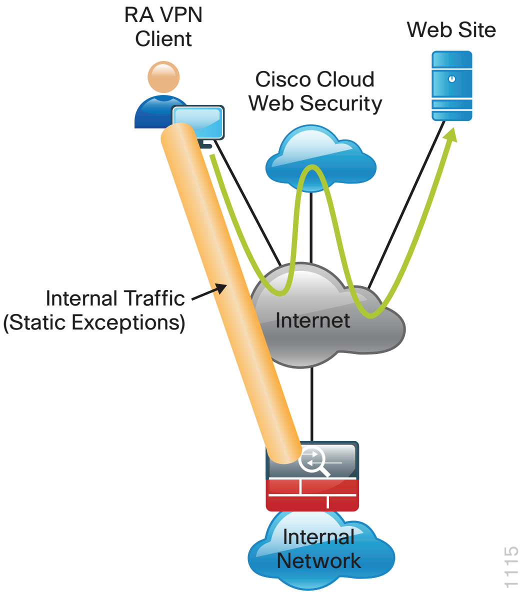
- Redirect web traffic–The Cisco CWS module can be integrated into the Cisco AnyConnect client, allowing web traffic to be transparently redirected to the Cisco CWS service. The CWS module is administered centrally on the RAVPN firewall and requires no additional hardware. Once installed, the CWS module continues to provide web security even when disconnected from the RAVPN firewall.
- Filter web content–Cisco CWS supports filters based on predefined content categories, as well as custom filters that can specify application, domain, content type, or file type. The filtering rules can be configured to block or warn based on the specific web usage policies of an organization.
- Protect against malware–Cisco CWS analyzes every web request to determine if the content is malicious. CWS is powered by the Cisco Security Intelligence Operations, the primary role of which is to help organizations secure business applications and processes through identification, prevention, and remediation of threats.
- Apply differentiated policies–The Cisco CWS web portal applies policies on a per-group basis. Group membership is determined by the group authentication key assigned within the Cisco AnyConnect CWS profile on the RAVPN firewall.

Cloud Web Security using Cisco AnyConnect enables the following network capabilities:

- **Always-on VPN**—The Trusted Network Detection capability of the Cisco AnyConnect client determines if a mobile device is on a trusted internal network or an untrusted external network. If on an untrusted network, the client automatically tries to establish a VPN connection to the primary site. The user needs to provide authentication, but no other intervention is required. If the user disconnects the connection, no other network access is permitted.
- **Mobile data services using Microsoft ActiveSync**—Cisco ASA Firewall and Microsoft Forefront Threat Management Gateway, when deployed in a DMZ network, provide an integrated solution for securing mobile data services. This solution supports a variety of mobile devices that run on Android, iOS, and Windows Mobile operating systems.
- **User authentication**—The AnyConnect client requires all remote access users to authenticate before negotiating a secure connection. Both centralized authentication and local authentication options are supported.
- **Differentiated access**—The remote access VPN is configured to provide different access policies depending on assigned user roles.
- **Strong encryption for data privacy**—The Advanced Encryption Standard cipher with a key length of 256 bits is used for encrypting user data. Additional ciphers are also supported.
- **Hashing for data integrity**—The Secure Hash Standard 1 cryptographic hash function with a 160-bit message digest is used to ensure that data has not been modified during transit.

Mobile remote users connect to their organization's network by using devices that generally fall into two categories: laptops and mobile devices such as smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ.

Figure 14 - Web traffic flow for CWS with Windows and Mac OS X clients



Other capabilities for the Cisco AnyConnect client include features that allow the client to reconnect if the tunnel goes down, to disable the tunnel if the client moves onto the trusted network, or to bring up the tunnel if the client moves from a trusted to an untrusted network. These features make using the client more seamless and friendly because users don't have to manually bring up the VPN tunnel. Users are prompted for credentials when the tunnel is needed, and the tunnel is deactivated when it isn't needed.

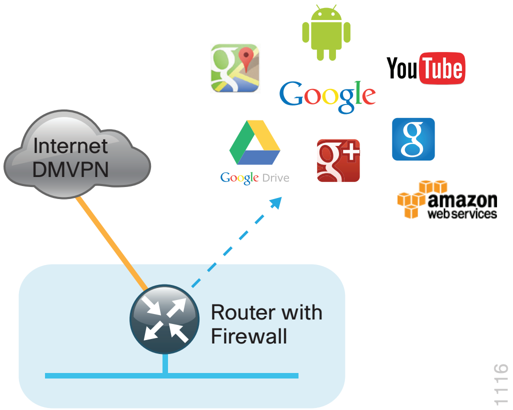
Mobile devices typically use a different deployment model in which basic services, such as mail, calendar, and contacts, are provided over Microsoft ActiveSync, which gives quick access to these commonly used services. For access to other services, including voice, video, internally hosted web servers, file shares, or other network services, a VPN tunnel is required.

For more information about how to deploy this WAN service, see the Cloud Web Security Using Cisco AnyConnect Technology Design Guide.

Remote Site Using Local Internet

Although many of the applications and services that the remote-site worker uses are centrally located, there are benefits in providing local Internet access at each remote-site location. Offloading Internet browsing and providing direct access to public cloud service providers can greatly reduce traffic on the private WAN, saving costs, improving overall survivability and reducing latency. Leveraging the cloud directly from the remote office can increase performance and improve the overall user experience.

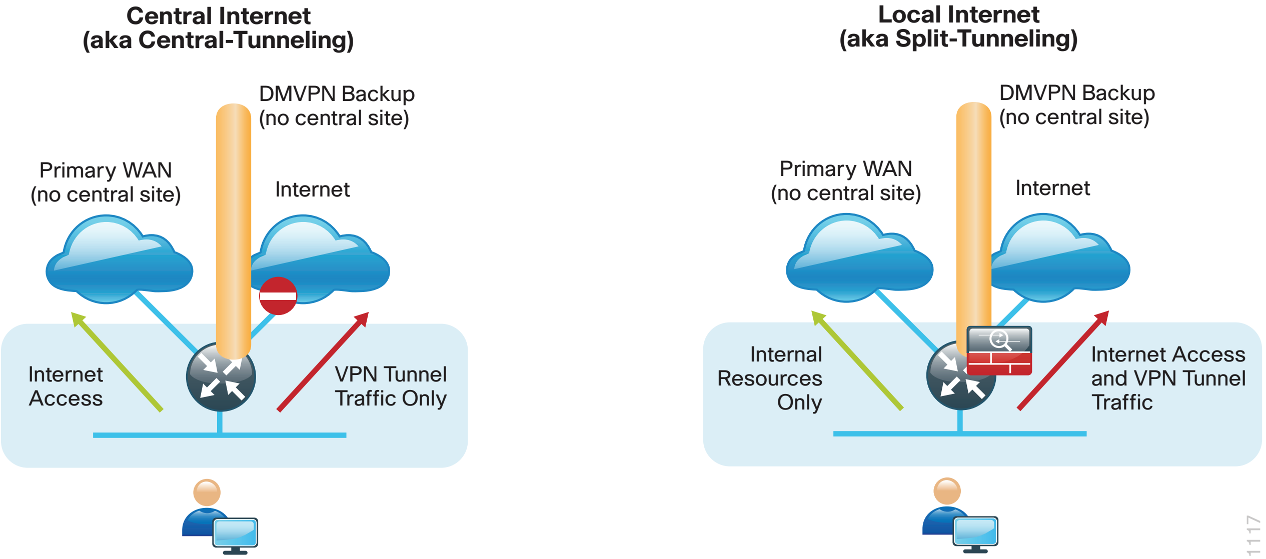
Figure 15 - Single-router, single-link remote site with local Internet access



Remote-Site Design Details

Cloud-enabled, remote-site designs provide remote-office local Internet access solutions for web browsing and cloud services. This is referred to as the local Internet access model. With this model, user web traffic and hosted cloud services traffic is permitted to use the local Internet link in a split-tunneling manner. In this model, a default route is generated locally from each remote site directly to the Internet provider. Private WAN connections using DMVPN over Internet, MPLS, or L2 WAN provide internal routes to the data center and campus. In some configurations backup Internet routing is provided over the private WAN connections.

Figure 16 - Central Internet and local Internet comparison



The primary focus of the design is to allow usage of the following commonly deployed remote-site WAN configurations with local Internet access:

- Single router remote site with Internet and DMVPN WAN connectivity
- Single or dual router remote site with MPLS WAN and local Internet using DMVPN for backup
- Single or dual router remote site with both L2 WAN and local Internet using DMVPN for backup
- Single or dual router remote site with dual-Internet DMVPN for primary and backup connectivity

Figure 17 - Single router, remote-site designs

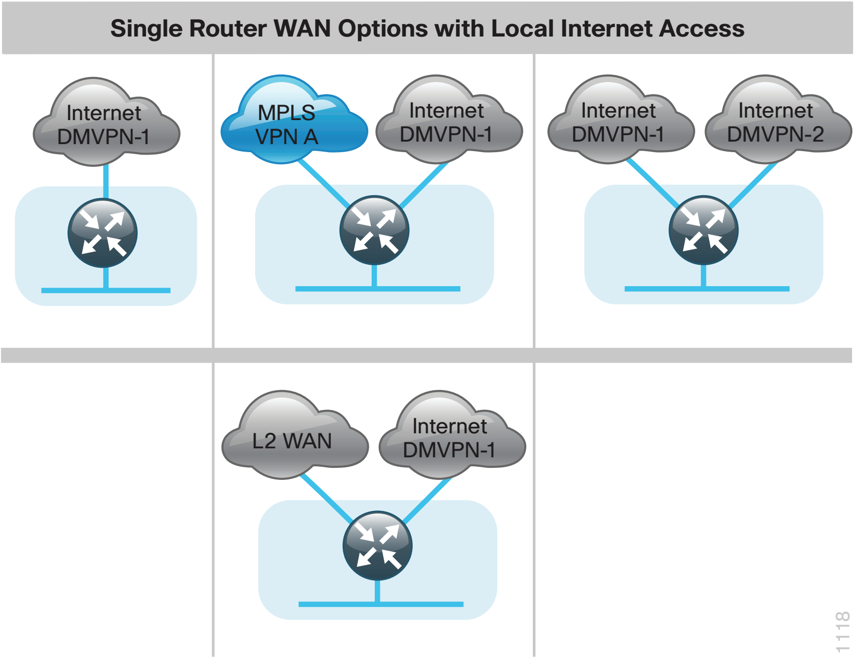
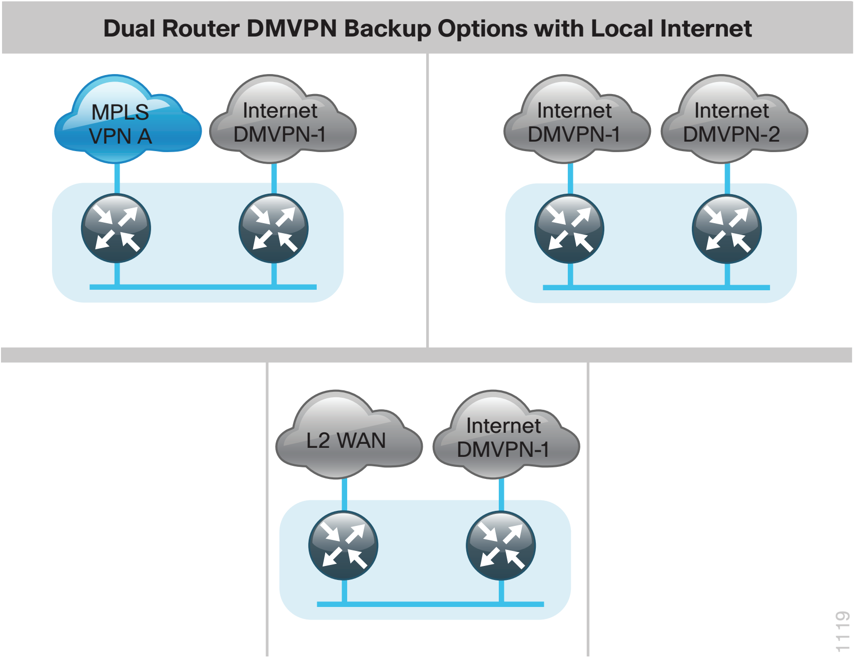


Figure 18 - Dual router, remote-site designs



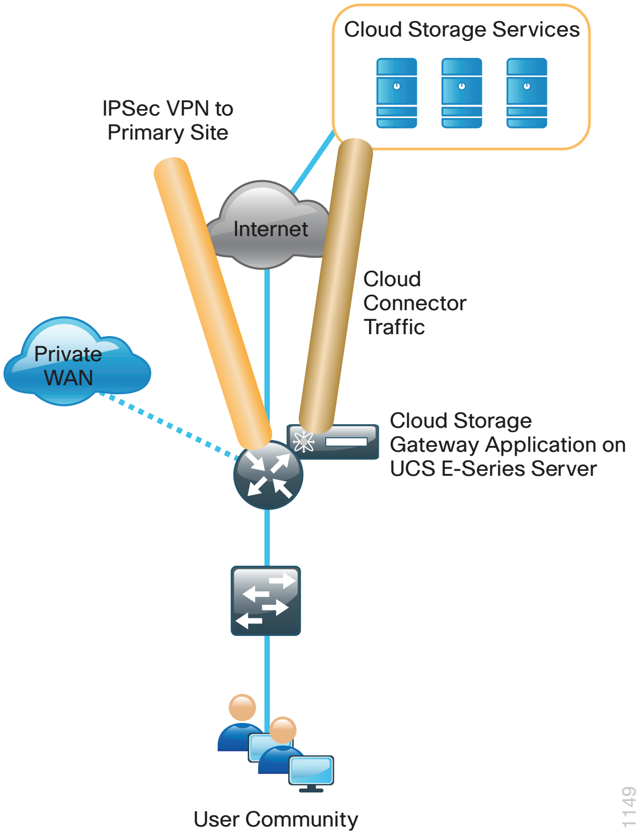
For information about how to deploy this WAN service, see the Remote Site Using Local Internet Access Technology Design Guide.

Hosted Cloud Connector Using Cisco UCS E-Series

Organizations are quickly adopting cloud services to help enable new business models for greater flexibility at lower cost. Organizations are increasingly looking at the benefits of hosting cloud-based applications at the remote office and accessing the public cloud directly. These types of applications are called *cloud connectors* and can be hosted directly on the remote office router using an integrated Cisco Unified Computing System (UCS) server.

A cloud connector is a Cisco or third-party software component embedded in, hosted on, or integrated with enterprise routing platforms. You can use cloud connectors for a variety of applications, including storage, virtualization, document handling, security, collaboration, and provisioning.

Figure 19 - Remote site hosted cloud connector on UCS E-Series Server



When organizations deploy Cisco Cloud Connector applications as part of an integrated platform using the Cisco ISRG2 and UCS E-Series Server module to leverage cloud services in the remote office, the organizations increase network performance by:

- Eliminating WAN backhaul
- Enabling service localization
- Reducing service and support costs

This is all possible while increasing security and visibility through advanced capabilities such as Cisco IOS Zone-Based Firewall (ZBFW) and Cisco Cloud Web Security (CWS), and Cisco AVC.

Cisco Cloud Connector applications deliver business-continuity solutions for voice, data retrieval, cloud storage, and security applications by leveraging local direct Internet access from the remote office location to the cloud-service provider. Additionally, this combined platform eliminates the need for additional remote office footprint and deployment concerns that often arise with multiple component solutions.

Cisco UCS E-Series Integrated Servers

The Cisco Unified Computing System E-Series Servers (UCS E-Series Servers) offer a converged compute, bare metal OS or virtualization ready, networking platform.

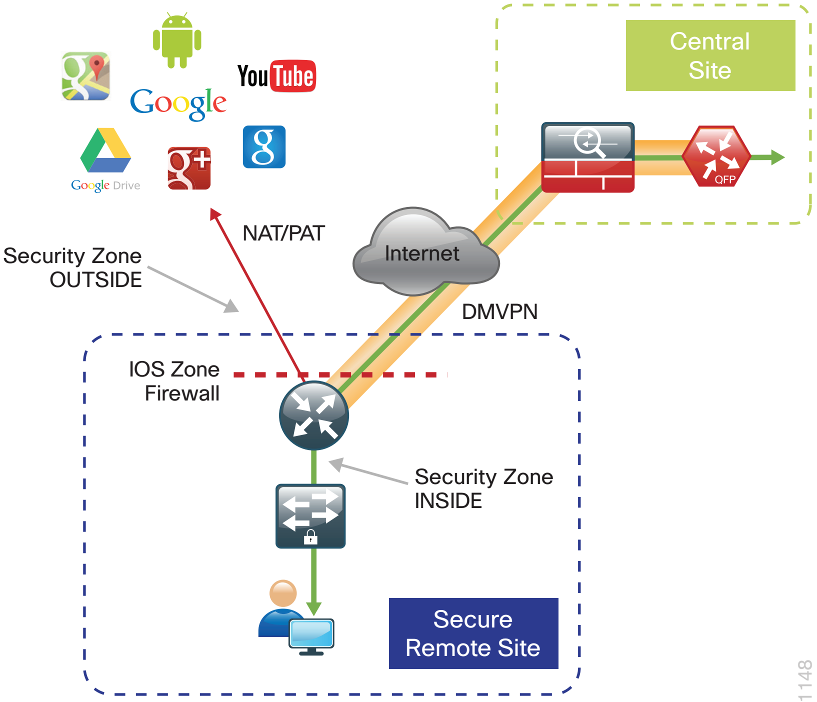
Cisco UCS E-Series server provides an integrated platform for Cisco and third-party Cloud Connector applications to run virtually within the network and is the basis for Cloud Connector Solutions. The hardware capabilities, ease of deployment, and hypervisor support (including VMware, MS hyperV, and Citrix Xen) make the Cisco UCS-E series a viable platform for cloud services deployments.

Cloud Storage Connectors

A Cloud Storage Connector is locally hosted application software that connects an organization via the Internet to cloud-based storage services. Cloud storage promises to deliver great cost savings and business agility for organizations, while also delivering easier ways of storing, sharing, and protecting enterprise data.

To enable distributed cloud storage, organizations must address several key challenges regarding security and overall network impact–specifically, the speed and latency in remote sites. By deploying storage cloud connector solutions, an organization can secure integration of an on-premises storage gateway and the cloud-based storage infrastructure with greatly reduced impact on WAN.

Figure 20 - Cisco secure remote site - cloud storage connector



Cisco has chosen and validated several cloud storage solutions, including the Amazon AWS storage gateway, Asigra Cloud Backup Connector, and the CTERA cloud storage solutions.

For more information about how to deploy this WAN service, see the Hosted Cloud Connector Using Cisco UCS E-Series Technology Design Guide.

Summary

Cisco WAN services are proven solutions that scale to all remote-site sizes over any transport. With rich application and security services on a single platform, IT can scale to hundreds of sites. Also, customers can maintain granular control, from the remote site, to the data center, and out to the public cloud. The traffic is dynamically routed based on application, endpoint, and network conditions to help ensure the best user experience. IT can confidently roll out critical business services such as consolidated data centers, SaaS, IP telephony, and video without overwhelming the WAN.

The Cisco WAN services design guides provide step-by-step guidance for deploying the solutions. With Cisco IWAN and WAN services, IT has the security and application services to deliver the highest levels of resiliency and reliability over any of the most common transports.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

B-0000179-1 12/13