# Next Generation Enterprise WAN Regional WAN Remote Access VPN

## Design Guide

September, 2011

NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE 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 THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R).

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

## Purpose

This document provides an architecture overview of the Cisco® Next Generation Enterprise WAN (NGEW) with an emphasis on the regional WAN (RWAN) implementation of the enterprise edge functions, and takes an architectural approach to designing and deploying routed WAN solutions for Borderless Networks. It describes the architectural components, as well as an overview of the Borderless Networks Services integrated within the architecture.

This document is intended for the reader who wants to:

- Provide for secure access to remote branch offices and mobile users through Internet connectivity
- Incorporate security for privacy and regulatory requirements
- Address the need for mobility of users and machines
- Provide for backup services for remote branch offices primarily connected through a Layer 3 VPN
- Must meet migration requirements for IPv6

## Introduction

## Architecture Overview

## NGEW (High-Level Topology)

The architecture is modular and hierarchical in nature, providing a scalable solution across the enterprise customer segments.

The architecture comprises five core modules:

- The regional WAN (RWAN)
  - Used to connect branch offices and aggregate remote locations
- The in-theater core
  - Used to interconnect RWANs within a country or theater
- The global core
  - Used to interconnect theater cores
- The enterprise edge
  - Used to connect the enterprise network to other networks
- The enterprise interconnect
  - Used as an interconnect and aggregation point for all modules

This modular approach allows for the design of a NGEW that uses basic building blocks and provides the capability to build a RWAN and an in-theater, global, or metropolitan (metro) network and interconnect them as required. Tying these modules together is accomplished by using the enterprise interconnect which, in effect, acts as an enterprise distribution network interconnected by the in-theater level core network. In the largest cases, a top tier of global backbone can interconnect such theaters.

The architecture also focuses on the enterprise edge, encompassing emerging strategies such as connectivity to cloud (private, public, and hybrid) and collaboration services as well as business-to-business rich-media capabilities such as telepresence.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

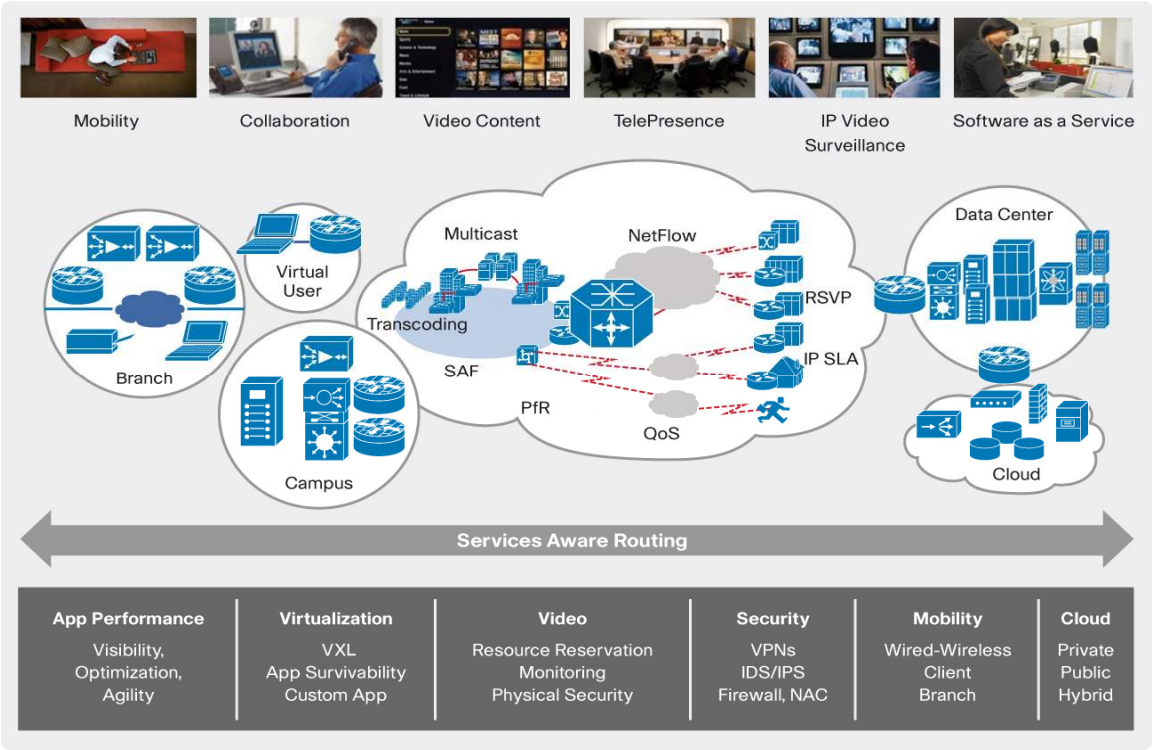
In addition to providing advanced routing functions, another major goal of the architecture is to deliver the applications and services that are relevant and fundamental to the enterprise business along with the routing elements that provide reliable delivery of those services. The incorporation of medianet functions, security services, application velocity, IPv6 transition, and mobility functions within the routing architecture is a clear differentiation and is an important consideration when considering a WAN solution. This approach developed within the architecture allows for incremental additions of services such as these without the need for large-scale replacement of equipment or redesign.

This document brings together two of these modules as it highlights the architecture of the enterprise edge as it relates to supporting the RWAN branch offices. The complete enterprise edge architecture, inclusive of cloud, web, and collaboration services, is detailed more fully in the (NGEW) document “Enterprise Edge Solution Overview”. For this document, note that the edge comprises five service components:

- Web Services: For inbound and outbound Internet access
- Collaboration Services: For connectivity to voice and video hosted services
- Cloud Services: For access to public cloud
- Business-to-Business Services for business-to-business connectivity to partners, etc.
- Mobility Services: Third- and fourth-generation (3G and 4G, respectively) connectivity for remote branch offices and mobile users

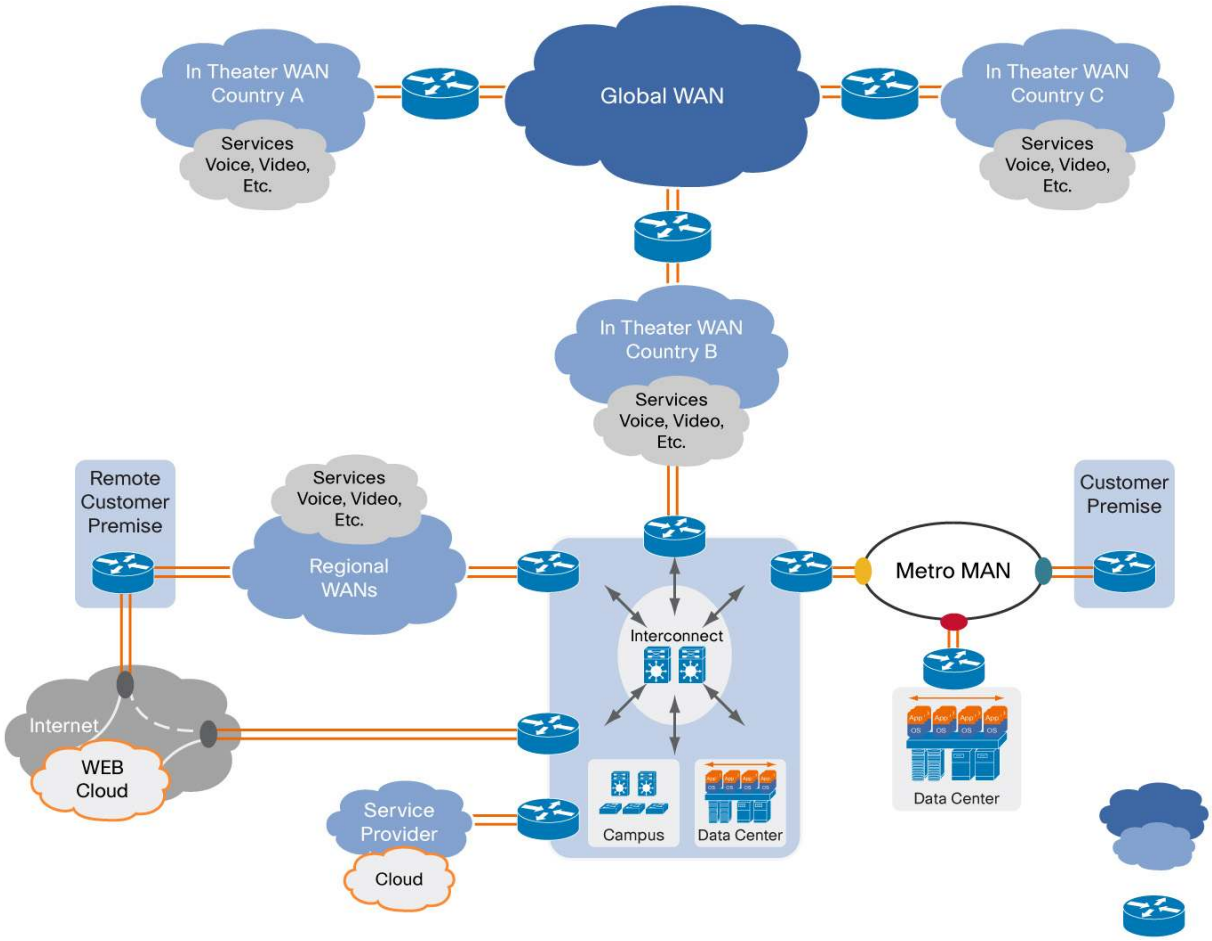
The Web Services component provides the Internet connectivity and services required for the RWAN access as defined within this document, and is the basis for the enterprise edge architecture for RWAN.

**Figure 1.** Enterprise Network Architecture




© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

**Figure 2.** Global Enterprise Archirtecture

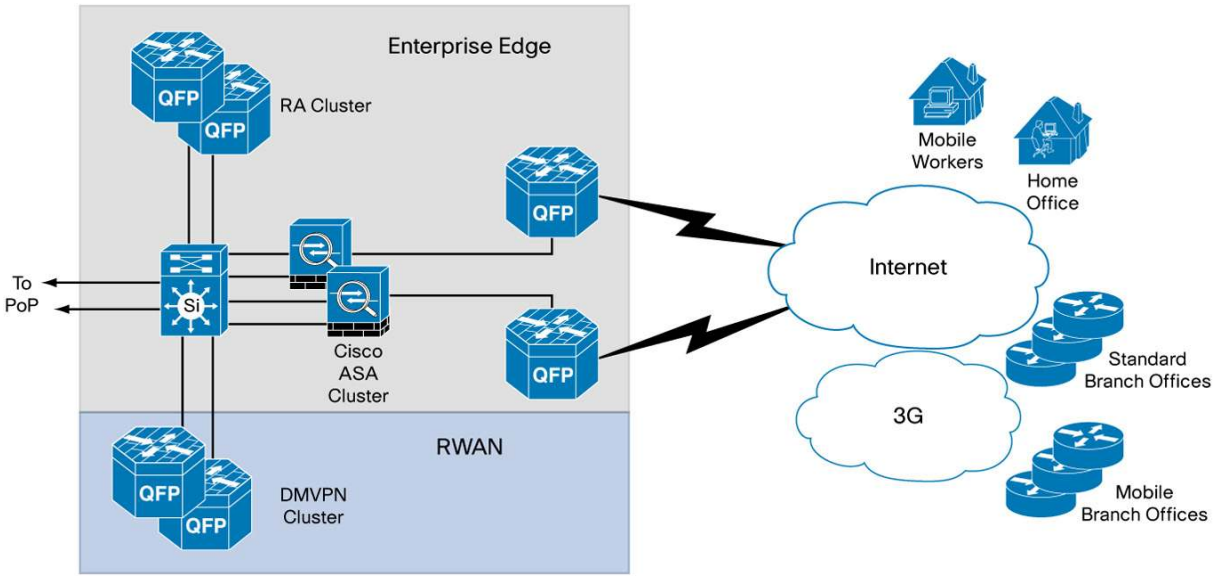



## Enterprise Edge for RWAN

The enterprise edge is the interface between the controlled enterprise network and users or resources that are outside of the enterprise's control or visibility. Users can be employees, partners, or customers. Resources can be Internet access, business-to-business connectivity and collaboration, hosted services, or hosted applications. The enterprise resource edge is also a place where services, such as security, collaboration acceleration, etc., can reside.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

**Figure 3.** Topological View of Enterprise Edge for RWAN Support




The enterprise edge presents a diverse set of requirements because of the variety of user types accessing a variety of resources. This situation is compounded further because users may be located inside or outside of the enterprise network, meaning the enterprise edge can exist in many locations, but every location may not have the same set of requirements.

This document focuses on the enterprise edge functions required to provide for primary branch-office access using Internet, 3G, or 4G connectivity, for backup branch-office access using either remote or mobile user support for enterprise clients.

The architecture is hierarchical in the approach to creating the edge functions. Edge routing, firewall, encryption, and other services are deployed in a layered fashion in order to provide high scalability and availability along with functions.

In the hierarchical enterprise edge module, a pair of Cisco® ASR 1000 Aggregation Services Routers act as the edge routers facing the Internet. Cisco ASA firewalls sit behind the Internet edge routers to provide firewall and Network Address Translation (NAT) functions. The Dynamic Multipoint VPN (DMVPN) and Easy VPN servers are behind firewalls. Two Cisco ASR 1000 Routers are used as DMVPN hubs and two as Easy VPN servers for redundancy with scaling. The DMVPN details are covered in the RWAN deployment guide.

## Enterprise Edge Design Overview

The Internet edge is the part of the network where the enterprise connects to the Internet service provider. The role of the Web Services portion of the enterprise edge is to provide the company a web presence, provide access to the Internet for its users (employees and guests), and to terminate some of the VPNs securely and reliably. In this architecture the Internet-facing routers are two Cisco ASR 1000 Aggregation Services Routers where the network connects to the Internet service providers. Behind the edge routers is the cluster of firewall devices (Cisco Adaptive Security Appliances [ASAs]), firewall devices that act as the NAT device as well providing NAT services while reaching the external network. Cisco ASA firewalls also terminate Cisco AnyConnect™ users and provide the remote users access to the enterprise network. Easy VPN and DMVPN servers are behind the firewall cluster, terminating the secure tunnels and providing access to the remote sites. This design also enables IPv6-only

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

clients to access the Internet. Stateless NAT64 provides the IPv6-to-IPv4 address mapping and is considered a migration and coexistence solution.

### Easy VPN

The Cisco Easy VPN with Dynamic Virtual Tunnel Interface (DVTI) configuration provides a routable interface to selectively send traffic to different destinations, such as an Easy VPN concentrator, a different site-to-site peer, or the Internet. IP Security (IPsec) DVTI configuration does not require a static mapping of IPsec sessions to a physical interface, allowing for the flexibility of sending and receiving encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted when it is forwarded from or to the tunnel interface.

The traffic is forwarded to or from the tunnel interface by virtue of the IP routing table. Routes are dynamically learned during Internet Key Exchange (IKE) mode configuration and inserted into the routing table pointing to the DVTI. Dynamic IP routing can be used to propagate routes across the VPN. Using IP routing to forward the traffic to encryption simplifies the IPsec VPN configuration when compared with using access control lists (ACLs) with the crypto map in native IPsec configuration.

In this design Easy VPN is deployed with two Cisco ASR 1000 Routers acting as Easy VPN servers. The Easy VPN remote clients are Cisco Integrated Services Routers (ISRs). All clients are configured with the two server addresses for redundancy. The Easy VPN servers are placed behind the firewall in this design. The Easy VPN clients are remote workers or home-office users who do not require much configuration on the client side.

### Cisco AnyConnect Security

Cisco AnyConnect security provides secure connection for remote workers connecting to the corporate network. Because these users and locations are an extension of the enterprise network, users have the same expectation of services, that is, data, voice, and video. To meet these expectations, organizations need to control access, provide differentiated services in the areas they control, and have visibility into those controls and differentiated services. Cisco AnyConnect security provides secure connection with enabled policies for the corporate users.

### NAT

#### NAT44

One of the very common enterprise edge features is NAT. In a typical design the private IP addresses are in the enterprise. However, with private IP addresses Internet and public IP addresses cannot be accessed. That is where we use NAT to translate the private IP address to an IP address that can be routed on the Internet. In this design a Cisco ASA is the device that performs the address translation. Generally addresses are translated dynamically from a pool with port overloading. Servers and devices that require static addresses to be accessed from outside are given static translation.

#### NAT64

In this phase of NGEW, Stateless NAT64 provides address family translation services from IPv6 to IPv4. This mechanism addresses scenarios where native IPv6 communication is not possible; for example, when a device on the network does not support dual stack. NAT64 is one of several IPv4-to-IPv6 migration and coexistence technologies available from Cisco. Stateless NAT64 is the mapping algorithm between IPv4 and IPv6 addresses. It is expected that the service provider's IPv4 addresses will be mapped into IPv6 and used by physical IPv6 hosts. The original IPv4 form of these blocks of the service provider's IPv4 addresses is used to represent the physical IPv6 hosts in IPv4. This type of algorithm supports both IPv6 initiated as well as IPv4 initiated communications. Stateless NAT64 does not maintain the bindings or session state like NAT44.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.


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.**



Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)



Printed in USA C07-683917-00 10/11



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.