Application Optimization Using Cisco ISR-WAAS

Technology Design Guide

December 2013

CISCO VALIDATED DESIGN

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.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

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

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Optimization of Traffic Traversing the WAN**—Cisco WAN optimization is an architectural solution comprising a set of tools and techniques that work together in a strategic systems approach to provide best-in-class WAN optimization performance while minimizing its total cost of ownership.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Deployment of Cisco Wide Area Application Services (WAAS) as a virtualized service on the Cisco ISR4451-X router at single-router and dual-router remote sites.
- Native integration of Application Navigator (AppNav) in the Cisco ISR 4451-X router, for intelligent load distribution.
- Integration of Cisco ISR 4451-X remote sites with an existing, deployed Cisco WAAS solution at the primary site and at other remote sites.

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks

Related CVD Guides

MPLS WAN Technology Design Guide

VPN WAN Technology Design Guide

Application Optimization Using Cisco WAAS Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd/wan

Introduction

Application optimization using Cisco Wide Area Application Services (WAAS) is an essential component 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.

This design guide is focused on how to deploy Cisco WAAS using the Cisco ISR4451-X router, which enables new design models. The Cisco IOS Software on the ISR4451-X natively integrates key WAAS features for traffic redirection and can also run the WAAS software as a virtualized service.

The design models in this guide are specific to remote sites that use the Cisco ISR4451-X router. Both single-router and dual-router remote-site topologies are supported. A prerequisite for this guide is the Application Optimization Using Cisco WAAS Technology Design Guide. This guide assumes that Cisco WAAS has already been deployed at the primary WAN-aggregation site.

Technology Use Cases

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. The consolidation efforts move most remote-site assets into data centers, largely to comply with regulatory mandates for centralized security and stronger control over corporate data assets.

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. With these applications growing increasingly multimedia-centric and latency-sensitive, 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. 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.

Use Case: Optimization of Traffic Traversing the WAN

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

This design guide 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

Design Overview

This section includes details that are specific to the Cisco ISR4451-X, including, for completeness, details of the overall Cisco WAAS solution. For more information, see the Application Optimization Using Cisco WAAS Technology Design Guide.

WAAS Nodes

A WAAS node (WN) is a Cisco WAAS application accelerator that optimizes and accelerates traffic according to the optimization policies configured on the device. A WAAS node can be a Cisco WAVE appliance or a virtual WAAS (vWAAS) instance. Cisco ISR-WAAS is a vWAAS instance specifically developed to run natively as a guest OS on the Cisco ISR 4451-X as a host device.

Tech Tip

A Cisco WAAS Express (WAASx) device is not considered to be a WAAS node.

A Cisco WAAS node group (WNG) is a group of WAAS nodes that services a particular set of traffic flows identified by Cisco Application Navigator policies.

Reader Tip

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

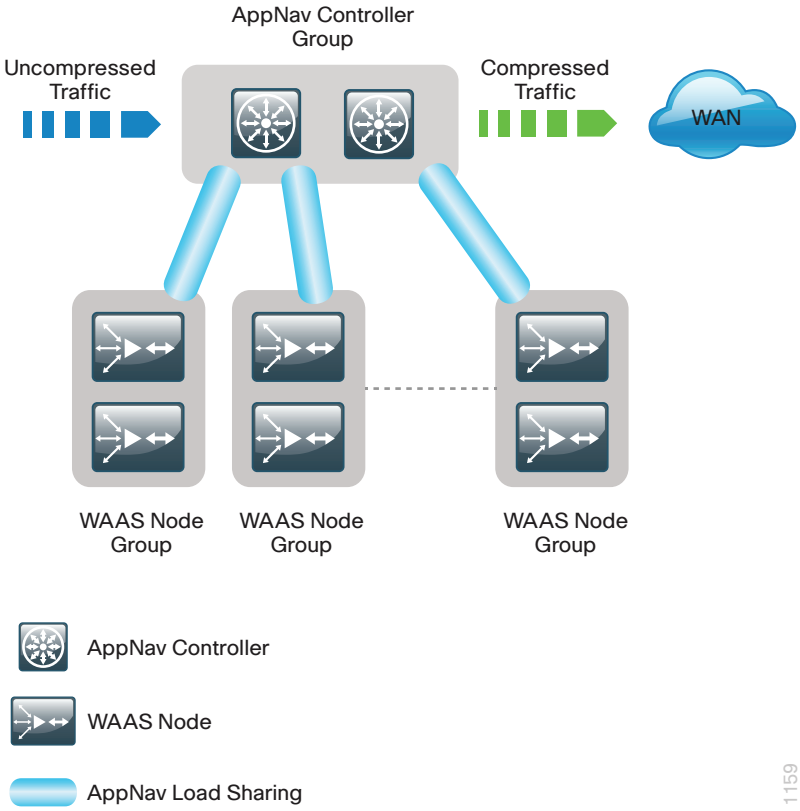
Examples:
WAAS Node (WN) = Service Node (SN)
WAAS Node group (WNG) = Service Node group (SNG)

AppNav

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.

Figure 1 - WAAS AppNav components



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 software running on the Cisco ASR 1000 Series routers and the Cisco ISR 4451-X router. When the AppNav Controller is running as a router software component, it is referred to as AppNav-XE.

Reader Tip

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

Examples:
AppNav Controller (ANC) = AppNav Controller (AC)
AppNav Controller group (ANCG) = AppNav Controller group (ACG)

A Cisco AppNav Controller group (ANCG) is a set 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 WN devices configured together as a system is referred to as an AppNav Cluster.

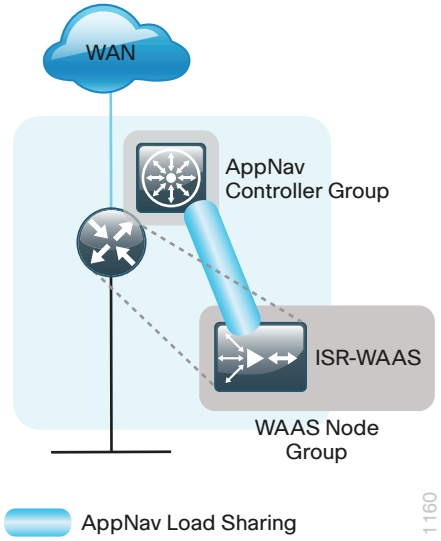
Tech Tip

A Cisco AppNav-XE Controller group must contain only members of the same router product family (Example: only Cisco ASR 1000 routers, or only Cisco ISR 4451-X routers). The ANCG may contain up to four AppNav-XE routers.

The AppNav IOM cannot be used within an AppNav-XE Controller group.

The combination of AppNav-XE and ISR-WAAS on the Cisco ISR 4451-X router delivers the entire application optimization solution on a single hardware platform using resources shared between the router and the vWAAS instance.

Figure 2 - AppNav-XE and ISR-WAAS on the Cisco ISR 4451-X router



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. ISR-WAAS is the specific implementation of vWAAS running in a Cisco IOS-XE Software container on the Cisco ISR4451-X router. The term *container* refers to the Kernel-based Virtual Machine (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, but is allocated dedicated CPU cores to isolate itself from router data plane operations. Additionally, to deploy a virtual service, the router requires additional storage beyond the standard bootflash. The Cisco ISR4451-X router supports a Network Interface Module (NIM) carrier card that can hold one or two 200-GB solid state drives (SSDs) to provide local storage for virtual services. The router requires the **appxk9** package license to run ISR-WAAS.

Table 1 - Cisco ISR-4451X requirements for ISR-WAAS

Profile	Max. optimized TCP connections	Router DRAM (GB)	Number of SSDs (200GB)	Compact flash (GB)
ISR-WAAS-750	750	8	1	16
ISR-WAAS-1300	1300	16	1	32
ISR-WAAS-2500	2500	16	2	32

WAN Aggregation Design Models

There are three different design models for the WAN-aggregation site. All of these design models are supported with Cisco ISR-WAAS. For more information about these design models, see the Application Optimization Using Cisco WAAS Technology Design Guide.

Table 2 - Supported WAN aggregation design models

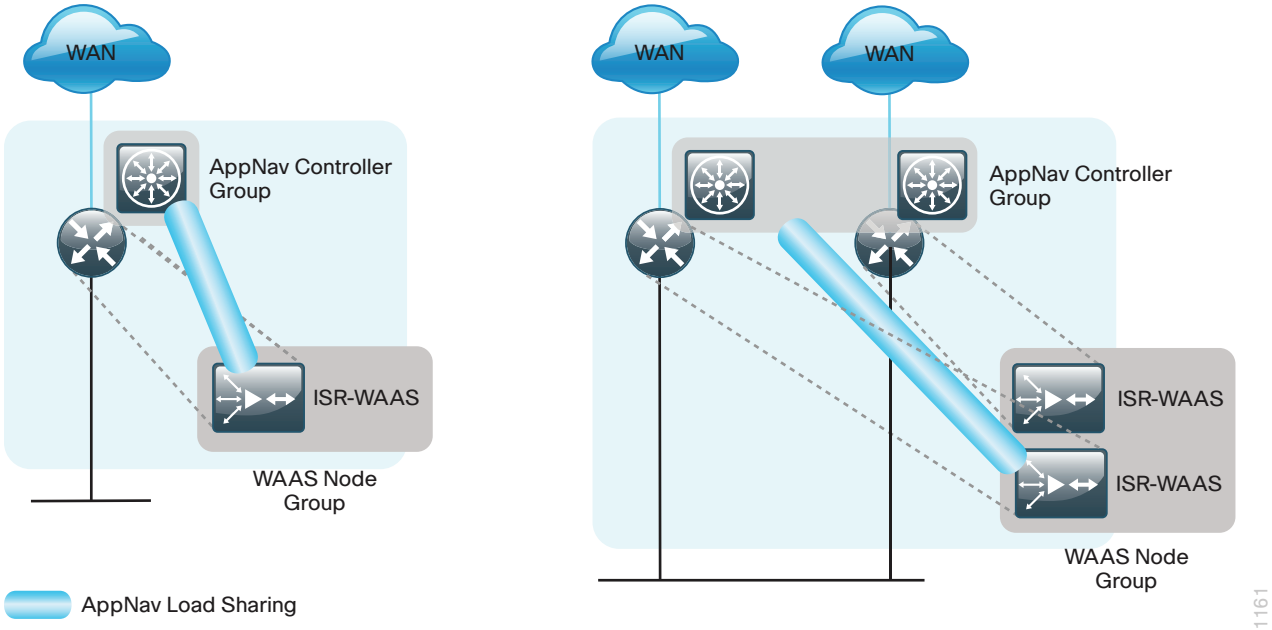
Requirement	WAAS with WCCP design model	AppNav off-path design model	AppNav-XE design model
AppNav IOM	Not needed	Required	Not needed
Mix of different router families	Supported	Supported	All routers must be same product family
Maximum number of ANCs in an ANCG	Not applicable	8	4
Intelligent load sharing	Basic load sharing only	Full AppNav policies	Full AppNav policies

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.

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

Figure 3 - Cisco ISR-WAAS remote-site design models



There are many factors to consider in the selection of the WAN remote-site WAN optimization platform. The primary parameter of interest is the bandwidth of the WAN link. After the bandwidth requirement has been met, the next item under consideration is the maximum number of concurrent, optimized TCP connections. Additional detail on the ISR-WAAS sizing is provided in the following table. The optimized throughput numbers correspond to the apparent bandwidth available after successful optimization by Cisco WAAS.

Table 3 - WAN remote-site Cisco ISR-WAAS on ISR 4451-X

Profile	Max. optimized TCP connections	Max. recommended WAN link [Mbps]	Max. optimized throughput [Mbps]
ISR-WAAS-750	750	75	100
ISR-WAAS-1300	1300	100	150
ISR-WAAS-2500	2500	150	200

For comprehensive sizing and planning, please work with your Cisco account team or Cisco partner.

Deployment Details

This section includes all required steps for deploying Cisco ISR-WAAS on the Cisco ISR4451-X router. This assumes that the Cisco WAAS Central Manager (WCM) is already deployed as recommended in the Application Optimization Using Cisco WAAS Technology Design Guide.

Three different options for installation are provided depending on your requirements. In all options, Cisco WCM may be used to monitor ISR-WAAS performance.

ISR-WAAS at a Single-Router Remote Site—Configured Using EZConfig

This is the simplest installation option and the EZConfig setup script installs Cisco ISR-WAAS and configures AppNav-XE. This option is specific to a single-router deployment and requires manual modification if you need to adapt it to a dual-router deployment.

AppNav-XE Controller Group—Created Using EZConfig

This option assumes that you have already completed a single-router, remote-site deployment using EZConfig and have now decided to add a second router. Rather than restart from the beginning, it is most straightforward to deploy the new router by using EZConfig. After completing EZConfig, you merge the two standalone configurations to use a single common ANCG and single common WNG.

ISR-WAAS at a Dual-Router Remote Site

This is the most flexible option and separates the tasks for installing Cisco ISR-WAAS and configuring AppNav-XE. You add the Cisco ISR4451-X routers to Cisco WCM, and then use the AppNav cluster wizard to configure the ANCG and WNG. In this option, WCM may be used to monitor AppNav-XE as well as ISR-WAAS. EZConfig is not used for this option.

Reader Tip

You may use the dual-router, remote-site procedure for a single-router site if you want to have central management and monitoring of AppNav-XE for these sites. Note that separate monitoring of both Cisco ISR4451-X and Cisco ISR-WAAS consumes additional resources on Cisco WCM.

This design guide uses certain standard design parameters and references various network infrastructure services that are not located within this solution. These parameters are listed in the following table. For your convenience, you can enter your values in the table and refer to it when configuring devices.

Table 4 - Universal design parameters

Network service	CVD values	Site-specific values
Domain name	cisco.local	
Active Directory, DNS server, DHCP server	10.4.48.10	
FTP server	10.4.48.11	
Cisco Secure ACS (Optional)	10.4.48.15	
Network Time Protocol (NTP) server	10.4.48.17	
SNMP read-only community	cisco	
SNMP read-write community	cisco123	

PROCESS

Preparing to Deploy ISR-WAAS

1. Configure DNS settings for Cisco WAAS Central Manager
2. Configure DNS Lookup on the ISR-WAAS host router
3. Verify resources on the ISR-WAAS host router

Procedure 1 Configure DNS settings for Cisco WAAS Central Manager

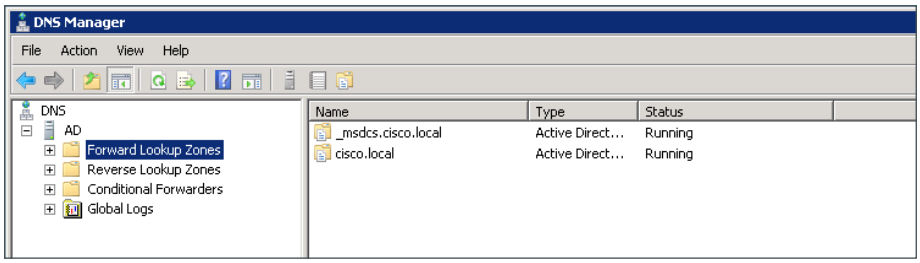
WAAS devices will automatically discover and register with Cisco WCM if a DNS Service Location (SRV) record for _waascms is configured for your domain. You may continue to enter the WCM IP address manually if DNS is not configured with the proper SRV record.

Add a Service Location Record for Cisco WCM.

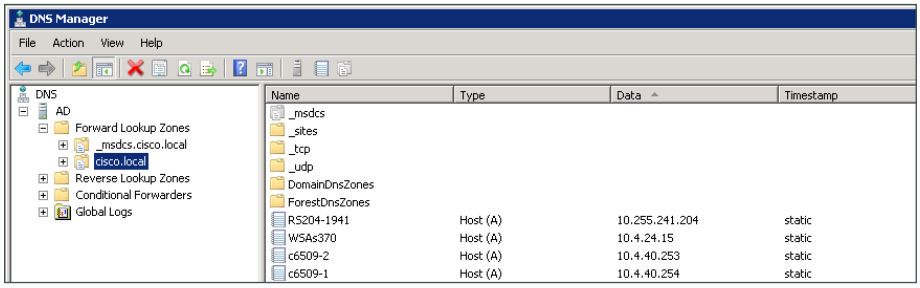
Step 1: On your primary DNS server, launch the DNS Manager.

Reader Tip

This example configuration shows how to create the DNS Service Location Record on a system running Windows Server 2008 R2 Enterprise. Follow a similar procedure for other operating systems.

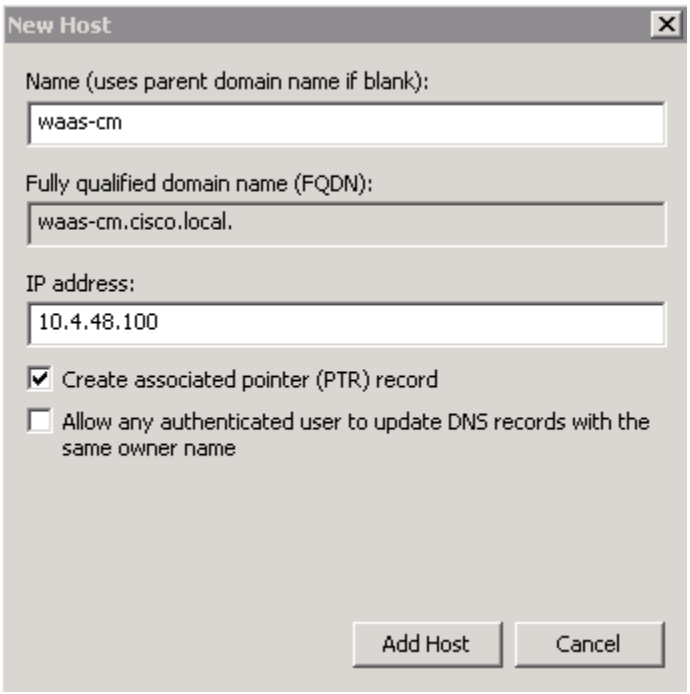


Step 2: Expand Forward Lookup Zone, and then select your forward lookup zone (Example: cisco.local).

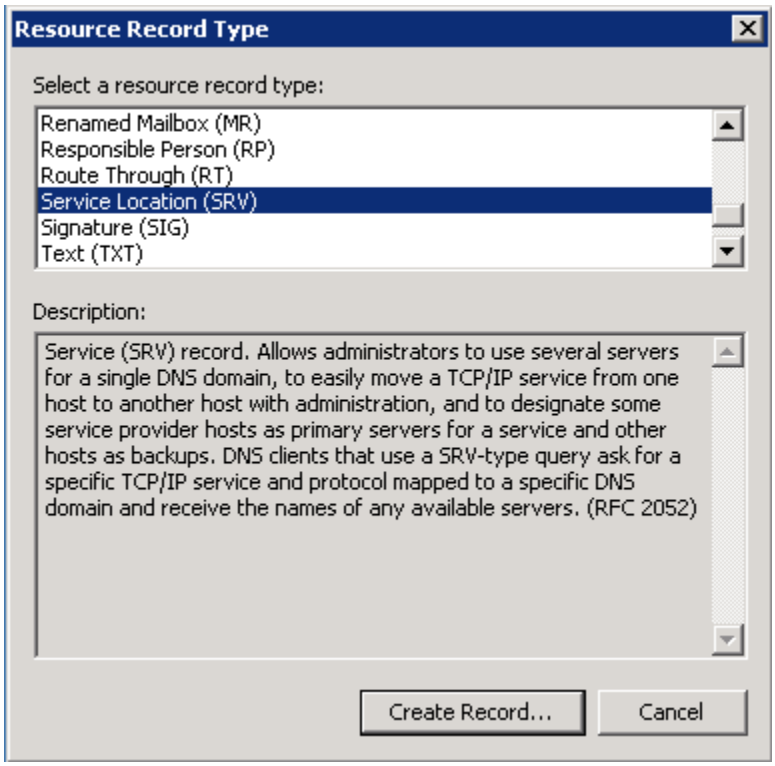


Step 3: If necessary, create a host record for your Cisco WCM by clicking **Action>New Host (A or AAAA)**, entering the following information, and then clicking **Add Host**.

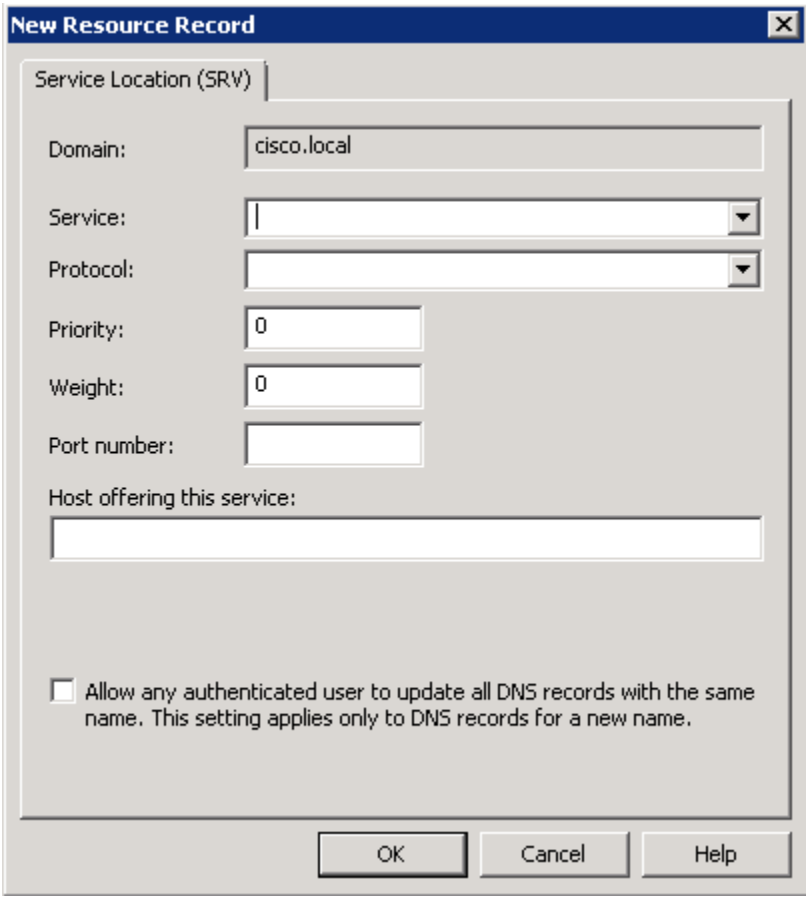
- Name—**waas-cm**
- IP address—**10.4.48.100**



Step 4: Click **Action>Other New Record.**

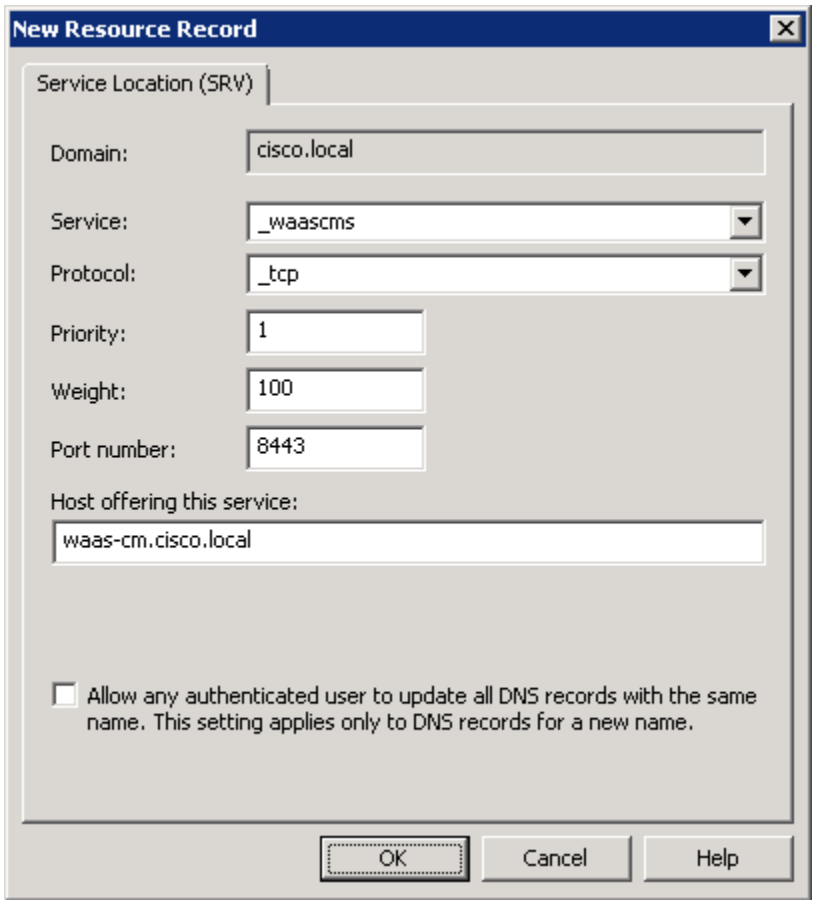


Step 5: Select **Service Location (SRV)**, and then click **Create Record**.



Step 6: In the New Resource Record window, enter the following parameters, and then click **OK**.

- Service–**_waascms**
- Protocol–**_tcp**
- Priority–**1**
- Weight–**100**
- Port number–**8443**
- Host offering this service–**waas-cm.cisco.local**



Step 7: Verify that the SRV record was created correctly by using nslookup from any DNS client.

```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>nslookup
Default Server:  ad.cisco.local
Address:  10.4.48.10

> set type=srv
> _waascms._tcp.cisco.local
Server:  ad.cisco.local
Address:  10.4.48.10

_waascms._tcp.cisco.local       SRV service location:
          priority       = 1
          weight         = 100
          port           = 8443
          svr hostname   = waas-cm.cisco.local
waas-cm.cisco.local     internet address = 10.4.48.100
>
```

Procedure 2 Configure DNS Lookup on the ISR-WAAS host router

The Cisco ISR 4451-X router must be configured to use DNS domain lookup in order to properly autodetect the Cisco WCM.

Step 1: On the Cisco ISR-WAAS host router, if DNS has not already been configured, configure it now.

```
ip domain name cisco.local
ip domain lookup
ip name-server 10.4.48.10
```

Procedure 3 Verify resources on the ISR-WAAS host router

The host router shares storage, memory, and CPU resources with the guest Cisco ISR-WAAS instance. There are three profiles available that correspond to the maximum number of concurrent TCP connections that are supported. Choose the required profile based on the expected number of TCP connections and compare the system requirements with the actual available before starting the installation and configuration.

Table 5 - ISR-WAAS profile resource requirements

Profile	ISR-WAAS-750	ISR-WAAS-1300	ISR-WAAS-2500	Site-specific values
Maximum TCP connections	750	1300	2500	
Disk space (MB)	170271	170288	360879	
Memory (MB)	4096	6144	8192	
CPU	25% system CPU	50% system CPU	75% system CPU	
VCPUs	2	4	6	

Step 1: Verify support for the chosen Cisco ISR-WAAS profile by checking the resources on the router. Compare the available resources with the minimum values listed in Table 5.

```
RS205-4451X#show virtual-service tech-support | inc HDD storage
Maximum HDD storage for virtualization : 381536 MB
RS205-4451X#show virtual-service tech-support | inc Maximum memory
Maximum memory for virtualization : 10240 MB
RS205-4451X#show virtual-service tech-support | inc Maximum system CPU
Maximum system CPU : 75%
RS205-4451X#show virtual-service tech-support | inc Maximum VCPUs
Maximum VCPUs per virtual service : 6
```

Step 2: Configure FTP client on the host router.

```
ip ftp source-interface Loopback0
ip ftp username cvd
ip ftp password c1sco123
```

Step 3: Transfer the Cisco ISR-WAAS OVA file to the host router.

Tech Tip

Multiple filesystems are available on the Cisco ISR-4451X platform. During installation, the filesystem for the guest virtual service is created on harddisk, but you can store the OVA file on either bootflash or harddisk in order to prepare for the installation.

```
RS205-4451X#copy ftp://10.4.48.11/ISR4451X-WAAS-5.3.1.20.ova bootflash:
Destination filename [ISR4451X-WAAS-5.3.1.20.ova]?
Accessing ftp://10.4.48.11/ISR4451X-WAAS-5.3.1.20.ova...
Loading ISR4451X-WAAS-5.3.1.20.ova !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
<content intentionally deleted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 939888640/4096
bytes]

939888640 bytes copied in 2836.528 secs (331352 bytes/sec)
```

PROCESS

Deploying ISR-WAAS at a Single-Router Remote Site

1. Use EZConfig to install ISR-WAAS and configure AppNav-XE

The easiest method to install and configure Cisco ISR-WAAS is to use the EZConfig program. This method is well suited to single router-designs and completes most necessary steps. If you have a dual-router design, Cisco recommends that you use the process, "Deploying ISR-WAAS at a Dual-Router Remote Site," in this guide.

Procedure 1 Use EZConfig to install ISR-WAAS and configure AppNav-XE

This process is for a single-router remote site. The host router does not need to be registered with Cisco WCM for this design because you do the entire configuration by using EZConfig.

Reader Tip

Although you don't use Cisco WCM to configure either the host router or the Cisco ISR-WAAS, you can use it to monitor the status and performance of the ISR-WAAS.

EZConfig does the following:

- Installs the Cisco ISR-WAAS OVA as a guest virtual-service on the host router.
- Creates a WAAS Service Node group and adds Cisco ISR-WAAS as a single member of the group.
- Creates an AppNav Controller group and adds the host router running AppNav-XE as a single member of the group.
- Configures WAAS service insertion on the WAN interfaces.

Table 6 - Cisco ISR-WAAS network parameters

Parameter	CVD values ISR-WAAS	Site-specific values
Router	RS205-4451X	
Virtual service name	AUTOWAAS	
Service node group	AUTOWAAS-SNG	
AppNav Controller group	AUTOWAAS-SCG	
Interception-method	appnav-controller	
Profile	ISR-WAAS-2500	
Data VLAN interface	GigabitEthernet 0/0/3.64	
Data VLAN IP address (AppNav controller IP)	10.5.36.1	
WAAS service IP	10.5.36.8	
WAN interface	GigabitEthernet0/0/0	
WAN interface 2	Tunnel10	
WAAS Central Manager	10.4.48.100	

Tech Tip

This example shows autodiscovery of the Cisco WCM IP address using DNS.

Step 1: Start Cisco ISR-WAAS EZConfig.

```
RS205-4451X# service waas enable
**************************************************************************
****  Entering WAAS service interactive mode.                         ****
****  You will be asked a series of questions, and your answers       ****
****  will be used to modify this device's configuration to           ****
****  enable a WAAS Service on this router.                           ****
**************************************************************************

Continue? [y]:y

At any time: ? for help, CTRL-C to exit.


Only one WAAS image found locally (bootflash:/ISR4451X-WAAS-5.3.1.20.ova) - using as
default

Extracting profiles from bootflash:/ISR4451X-WAAS-5.3.1.20.ova, this may take a couple
of minutes ...
```

```
These are the available profiles
1. ISR-WAAS-2500
2. ISR-WAAS-1300
3. ISR-WAAS-750

Select option  [1]:1
An internal IP interface and subnet is required to deploy a WAAS service on this router.
This internal subnet must contain two usable IP addresses that can route and communicate
with the WAAS Central Manager (WCM).


Enter the IP address to be configured on the WAAS service:  10.5.36.8
The following IP interfaces are currently available on the router:

Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.4.37    YES NVRAM  up                    up
GigabitEthernet0/0/1   172.18.100.34   YES DHCP   up                    up
GigabitEthernet0/0/2   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/3   unassigned      YES NVRAM  up                    up
Gi0/0/3.64             10.5.36.1       YES NVRAM  up                    up
Gi0/0/3.69             10.5.37.1       YES NVRAM  up                    up
GigabitEthernet0       unassigned      YES NVRAM  administratively down down
Loopback0              10.255.252.205  YES NVRAM  up                    up
Tunnel0                10.255.252.205  YES unset  up                    up
Tunnel10               10.4.34.205     YES NVRAM  up                    up

Enter a WAN interface to enable WAAS interception (blank to skip) []:
GigabitEthernet0/0/0

Enter additional WAN interface (blank to finish) []:  Tunnel10

Enter additional WAN interface (blank to finish) []: press enter

****************************
** Configuration Summary: **
****************************

a) WAAS Image and Profile Size:
   bootflash:/ISR4451X-WAAS-5.3.1.20.ova  (939888640) bytes
   ISR-WAAS-2500

b) Router IP/mask:
   Using ip unnumbered from interface GigabitEthernet0/0/3.64

   WAAS Service IP:
   10.5.36.8
```

```
c) WAAS Central Manager:
   10.4.48.100

d) Router WAN Interfaces:
   GigabitEthernet0/0/0
   Tunnel10

Choose one of the letter from 'a-d' to edit, 'v' to view config script, 's' to apply
config [s]:s
```

The Cisco ISR-WAAS OVA is installed and activated. This takes several minutes.

```
The configuration will be applied and the status of the WAAS service will be displayed
after deployment


Installing bootflash:/ISR4451X-WAAS-5.3.1.20.ova

installing!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!

% Activating virtual-service 'AUTOWAAS', this might take a few minutes. Use 'show
virtual-service list' for progress.

System is attempting to deploy and activate WAAS image, this may take up to 10 minutes
activating!!!!


Waiting for WAAS application to be at a stage to accept WCM IP configuration.

Waiting!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
management services enabled

WAAS service activated!
Note:Please issue "copy running-config startup-config" command to save changes!
```

Step 2: Save the configuration on the host router.

```
RS205-4451X# copy running-config startup-config
```

Step 3: Connect to the virtual service console to configure the device management protocols. You can exit from the console by typing **^c^c^c**. It may take a few minutes to receive a login prompt after activation, because ISR-WAAS operating system must boot completely. For all Cisco ISR-WAAS devices, the factory default username is **admin** and the factory default password is **default**.

```
RS205-4451X# virtual-service connect name AUTOWAAS console
Connected to appliance. Exit using ^c^c^c

......

Cisco Wide Area Application Engine Console

Username:
```

Step 4: In the EXEC mode, enable the propagation of local configuration changes to the WCM.

```
cms lcm enable
```

Step 5: Change the default password for the admin account (Example: c1sco123).

```
username admin passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager.  Please use the central manager to configure
user accounts.
New WAAS password: c1sco123
Retype new WAAS password: c1sco123
```

Step 6: Generate the RSA key and enable the sshd service. This enables SSH.

```
ssh-key-generate key-length 2048
sshd enable
no telnet enable
```

Step 7: Enable Simple Network Management Protocol (SNMP). This allows the network infrastructure devices to be managed by a Network Management System (NMS). Configure SNMPv2c for both a read-only and a read-write community string.

```
snmp-server community cisco
snmp-server community cisco123 RW
```

Step 8: If you want to limit access to the appliance, configure management ACLs.

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
interface Virtual 1/0
 ip access-group 155 in
 exit
```

```
!
ip access-list standard  55
 permit 10.4.48.0 0.0.0.255
 exit
snmp-server access-list 55
```

Step 9: If you have a centralized TACACS+ server, enable AAA authentication for access control. This configures secure user authentication as the primary method for user authentication (login) and user authorization (configuration). AAA controls all management access to the Cisco WAAS and Cisco WAVE devices (SSH and HTTPS).

> **Tech Tip**
>
> A factory default local admin user was created on the Cisco WAAS and Cisco WAVE appliances during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or if you do not have a TACACS+ server in your organization.

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 10: After you make configuration changes, in the EXEC mode, save the configuration.

```
copy running-config startup-config
```

Step 11: Disconnect from the virtual service console by typing **^c^c^c**.

PROCESS

Creating an AppNav-XE Controller Group Using EZConfig

1. Convert a standalone ISR-WAAS configuration to a group configuration

If the first router of a dual-router remote site was configured by using EZConfig, you may also configure the second router by using EZConfig. Start this process after completing Procedure 1 in the "Deploying ISR-WAAS at a Single-Router Remote site" process for each router hosting Cisco ISR-WAAS.

Table 7 - Cisco ISR-WAAS network parameters

Parameter	**CVD values ISR-WAAS (Router 1)**	**CVD values ISR-WAAS (Router 2)**	**Site-specific values**
Router	RS215-4451X-1	RS215-4451X-2	
Virtual Service Name	AUTOWAAS	AUTOWAAS	
Service node group	AUTOWAAS-SNG	AUTOWAAS-SNG	
AppNav Controller group	AUTOWAAS-SCG	AUTOWAAS-SCG	
Interception-method	appnav-controller	appnav-controller	
Profile	ISR-WAAS-1300	ISR-WAAS-1300	
Data VLAN interface	Port-channel1.64	Port-channel2.64	
Data VLAN IP address (AppNav controller IP)	10.5.188.2	10.5.188.3	
WAAS service IP	10.5.188.8	10.5.188.9	
WAN interface	GigabitEthernet0/0/0.39	Tunnel10	
WAAS Central Manager	10.4.48.100	10.4.48.100	

Tech Tip

Each of the two standalone Cisco ISR4451-X routers includes a static route to the guest OS. It is not necessary to redistribute this static route into the LAN EIGRP process.

```
ip route 10.5.188.8 255.255.255.255 VirtualPortGroup31
```

This type of static route is known as a *pseudo-static* or *pseudo-connected* route because it meets two conditions:

1) The static route points directly to an interface.
2) The destination IP address is contained within an IP range that is referenced by an EIGRP network statement.

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
```

A pseudo-connected route is treated like a connected route and is automatically advertised within the EIGRP autonomous system as an EIGRP internal route so no redistribution is required.

Although the pseudo-connected routes will be automatically brought into the EIGRP topology and treated similarly to a connected route, EIGRP does not reclassify the route as a connected. Redistribution of static routes, and then applying configuration commands (such as route maps) to the redistributed routes will affect these routes.

Procedure 1 Convert a standalone ISR-WAAS configuration to a group configuration

All AppNav-XE controllers should be in a single ANCG and all WNs should be in a single WNG at a dual-router remote site. The conversion from a pair of standalone ISR-WAAS deployments each created using EZConfig to a single combined deployment requires manual configuration.

This procedure should be performed in parallel on both routers.

Step 1: On the first router, add the WAAS service IP address from the Cisco ISR-WAAS instance on the second router to the Service Node group.

```
service-insertion service-node-group AUTOWAAS-SNG
 service-node 10.5.188.9
```

Step 2: On the second router, add the WAAS service IP address from the Cisco ISR-WAAS instance on the first router to the Service Node group.

```
service-insertion service-node-group AUTOWAAS-SNG
 service-node 10.5.188.8
```

Step 3: On the first router, add the AppNav Controller IP address from the second router to the AppNav Controller group.

```
service-insertion appnav-controller-group AUTOWAAS-SCG
 appnav-controller 10.5.188.3
```

Step 4: On the second router, add the AppNav controller IP address from the first router to the AppNav Controller group.

```
service-insertion appnav-controller-group AUTOWAAS-SCG
 appnav-controller 10.5.188.2
```

Example: RS215-4451X-1

```
service-insertion service-node-group AUTOWAAS-SNG
 service-node 10.5.188.8
 service-node 10.5.188.9
service-insertion appnav-controller-group AUTOWAAS-SCG
 appnav-controller 10.5.188.2
 appnav-controller 10.5.188.3
```

Example: RS215-4451X-2

```
service-insertion service-node-group AUTOWAAS-SNG
 service-node 10.5.188.8
 service-node 10.5.188.9
service-insertion appnav-controller-group AUTOWAAS-SCG
 appnav-controller 10.5.188.2
 appnav-controller 10.5.188.3
```

PROCESS

Deploying ISR-WAAS at a Dual-Router Remote Site

1. Create a WAAS Central Manager user
2. Register the router to the WAAS Central Manager
3. Install the ISR-WAAS OVA as a guest virtual service on the host router
4. Configure the AppNav-XE cluster

This process is for a dual-router remote site. Both routers are registered with Cisco WCM. The Cisco ISR-WAAS virtual service is installed manually and the AppNav-XE cluster is configured using the WCM AppNav Cluster Wizard. EZConfig is not used for this process.

Tech Tip

This process may be used for a single-router remote site. The configuration requires more steps than using EZConfig, but it also allows for centralized management and monitoring of the AppNav-XE controllers.

Procedure 1 Create a WAAS Central Manager user

There are two options when you are creating the Cisco WCM account. If you want to create the account locally on each Cisco AppNav Controller router, complete Option 1. If you want to create it once on the central AAA server, complete Option 2.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized authentication, authorization and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis.

Be aware that if AAA is used for router administration, centralized AAA must also be used for the Cisco WCM user.

Option 1: Create a local user account

Step 1: Create a local user on the remote-site router.

```
username waascm privilege 15 password c1sco123
```

Option 2: Create a centralized AAA account

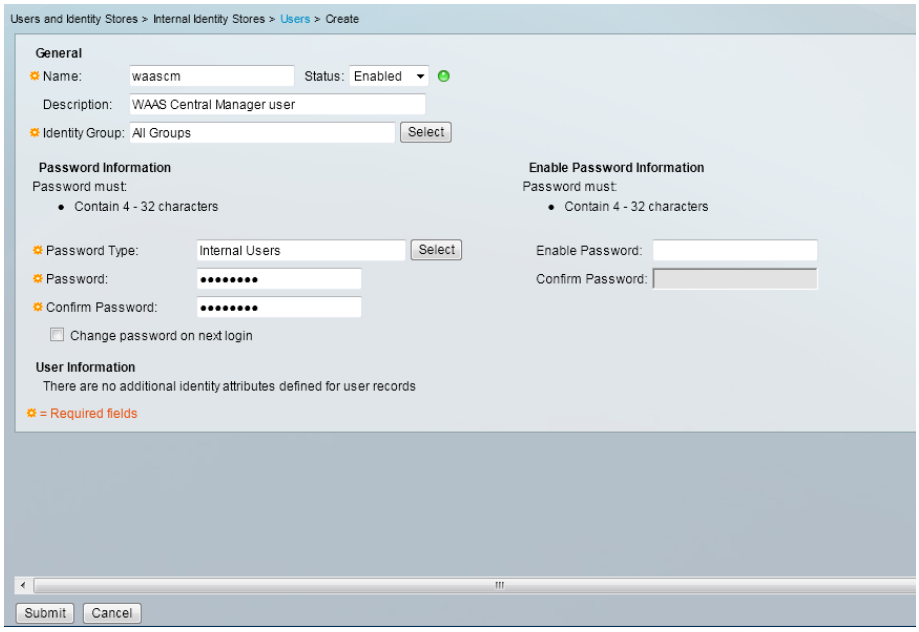
The Cisco Secure ACS internal identity store can contain all the network administrator accounts or just accounts that require a policy exception if an external identity store (such as Microsoft Active Directory) is available. A common example of an account that would require an exception is one associated with a network management system that allows the account to perform automated configuration and monitoring.

Step 1: Navigate and log in to the Cisco Secure ACS Administration page. (Example: https://acs.cisco.local)

Step 2: Navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

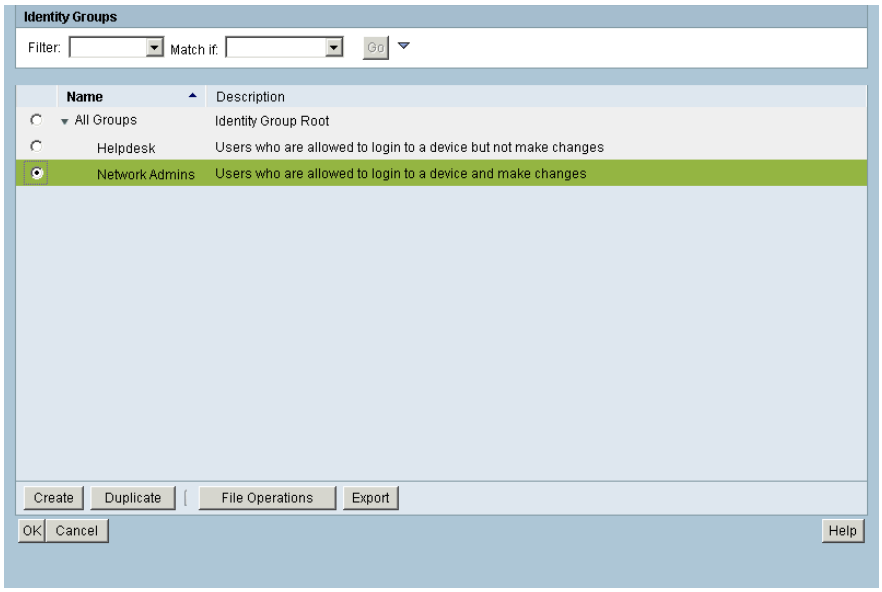
Step 3: Click **Create**.

Step 4: Enter a name, description, and password for the user account. (Example: user name waascm and password c1sco123)



Step 5: To the right of Identity Group, click **Select**.

Step 6: Select **Network Admins**, and then click **OK**.



Step 7: Click **Submit**.

Procedure 2 Register the router to the WAAS Central Manager

Step 1: Verify SSH and HTTPS servers are enabled on the router. If they are not already configured, configure these services now.

Reader Tip

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

Step 2: Specify the transport preferred none on vty lines. This prevents errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

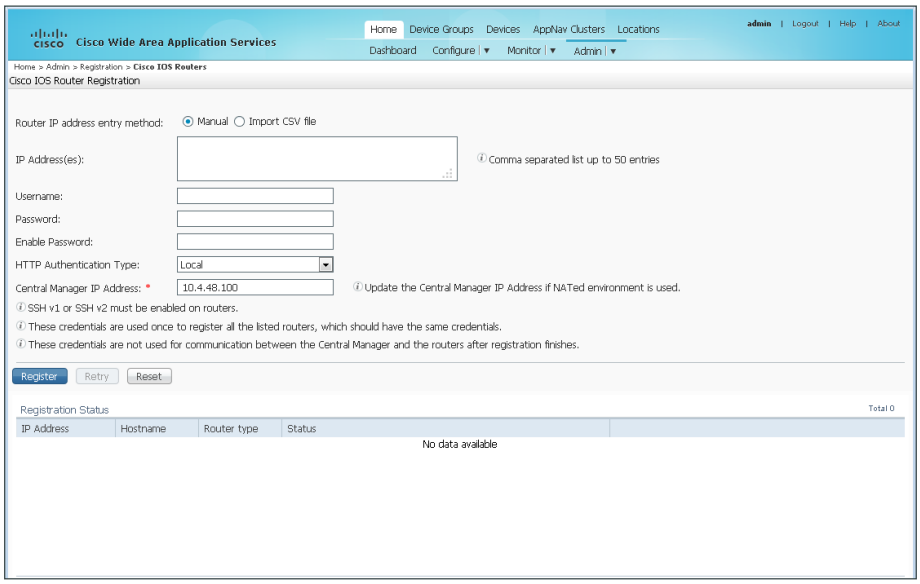
```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

Step 3: If you are using AAA authentication, configure the HTTP server to use AAA.

```
ip http authentication aaa
```

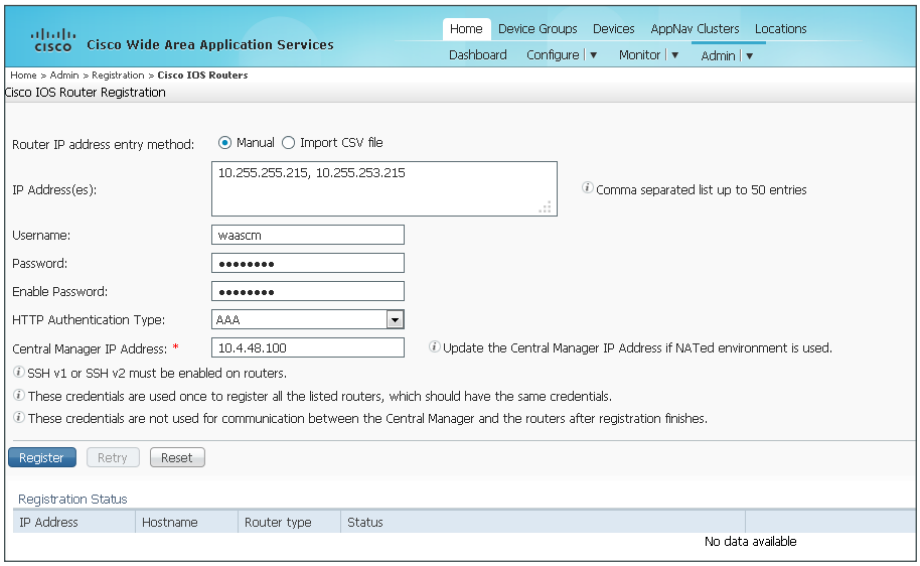
Step 4: Log in to Cisco WCM through the web interface (for example, https://waas-cm.cisco.local:8443).

Step 5: Navigate to **Admin>Registration>Cisco IOS Routers**.



Step 6: Enter the management information of the WAN remote-site routers running Cisco AppNav-XE, and then click **Register**. You may enter the IP addresses of multiple routers (separated by a comma) if they share the same authentication credentials.

- Router IP address entry method–**Manual**
- IP Address(es)–**10.255.255.215, 10.255.253.215**
- Username–**waascm**
- Password–**c1sco123**
- Enable Password–**c1sco123**
- HTTP Authentication Type–AAA
- Central Manager IP Address–**10.4.48.100**



Step 7: Verify successful registration.

Registration Status

IP Address	Hostname	Router type	Status
10.255.255.215	RS215-4451X-1	AppNav-XE Controller	✔ Successfully processed the registration request
10.255.253.215	RS215-4451X-2	AppNav-XE Controller	✔ Successfully processed the registration request

Procedure 3 Install the ISR-WAAS OVA as a guest virtual service on the host router

Table 8 - Cisco ISR-WAAS network parameters

Parameter	CVD values ISR-WAAS (Router 1)	CVD values ISR-WAAS (Router 2)	Site-specific values
Router	RS215-4451X-1	RS215-4451X-2	
Virtual Service Name	RS215_4451X_1_vWAAS	RS215_4451X_2_vWAAS	
Profile	ISR-WAAS-1300	ISR-WAAS-1300	
Data VLAN Interface	Port-channel1.64	Port-channel2.64	
WAAS service IP	10.5.188.8	10.5.188.9	
WAAS Central Manager	10.4.48.100	10.4.48.100	

Step 1: Install the Cisco ISR-WAAS virtual service. Run this command from router exec mode.

Tech Tip

The virtual service name may not include a dash "-".

```
RS215-4451X-1# virtual-service install name RS215_4451X_1_vWAAS package
bootflash:ISR4451X-WAAS-5.3.1.20.ova
```

Step 2: Verify installation of the virtual service.

```
RS215-4451X-1#show virtual-service list
Virtual Service List:

Name                    Status              Package Name
-----------------------------------------------------------------------
RS215_4451X_1_vWAAS     Installed           ISR4451X-WAAS-5.3.1.20.ova
```

Step 3: Configure the virtual port group interface and static route to the WAAS service IP.

```
interface VirtualPortGroup0
 ip unnumbered Port-channel1.64
!
ip route 10.5.188.8 255.255.255.255 VirtualPortGroup0
```

Tech Tip

It is not necessary to redistribute the following static route into the LAN EIGRP process.

```
ip route 10.5.188.8 255.255.255.255 VirtualPortGroup0
```

This type of static route is known as a *pseudo-static* or *pseudo-connected* route because it meets two conditions:

1) The static route points directly to an interface.
2) The destination IP address is contained within an IP range that is referenced by an EIGRP network statement.

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
```

A pseudo-connected route is treated like a connected route and is automatically advertised within the EIGRP autonomous system as an EIGRP internal route so no redistribution is required.

Although the pseudo-connected routes will be automatically brought into the EIGRP topology and treated similarly to a connected route, EIGRP does not reclassify the route as a connected. Redistribution of static routes, and then applying configuration commands (such as route maps) to the redistributed routes will affect these routes.

Step 4: Assign a profile to the virtual service, and then activate it.

```
virtual-service RS215_4451X_1_vWAAS
 profile ISR-WAAS-1300
 vnic gateway VirtualPortGroup0
  guest ip address 10.5.188.8
 activate
```

Step 5: Verify activation of the virtual service.

```
RS215-4451X-1#show virtual-service list
Virtual Service List:

Name                    Status             Package Name
-----------------------------------------------------------------------
RS215_4451X_1_vWAAS     Activated          ISR4451X-WAAS-5.3.1.20.ova
```

Step 6: Connect to the virtual service console to configure the device management protocols. You can exit from the console by typing **^c^c^c**. It may take a few minutes to receive a login prompt after activation, because Cisco ISR-WAAS operating system must boot completely. For all Cisco ISR-WAAS devices, the factory default username is **admin** and the factory default password is **default**.

```
RS215-4451X-1# virtual-service connect name RS215_4451X_1_vWAAS console
Connected to appliance. Exit using ^c^c^c

......

Cisco Wide Area Application Engine Console

Username:
```

Step 7: In the EXEC mode, enable the propagation of local configuration changes to the WCM.

```
cms lcm enable
```

Step 8: Change the default password for the admin account (Example: c1sco123).

```
username admin passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager.  Please use the central manager to configure
user accounts.
New WAAS password: c1sco123
Retype new WAAS password: c1sco123
```

Step 9: Generate the RSA key and enable the sshd service. This enables SSH.

```
ssh-key-generate key-length 2048
sshd enable
no telnet enable
```

Step 10: Enable Simple Network Management Protocol (SNMP). This allows the network infrastructure devices to be managed by a Network Management System (NMS). Configure SNMPv2c for both a read-only and a read-write community string.

```
snmp-server community cisco
snmp-server community cisco123 RW
```

Step 11: If you want to limit access to the appliance, configure management ACLs.

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
interface Virtual 1/0
 ip access-group 155 in
 exit
!
ip access-list standard  55
 permit 10.4.48.0 0.0.0.255
 exit
snmp-server access-list 55
```

Step 12: If you have a centralized TACACS+ server, enable AAA authentication for access control. This configures secure user authentication as the primary method for user authentication (login) and user authorization (configuration). AAA controls all management access to the Cisco WAAS and Cisco WAVE devices (SSH and HTTPS).

Tech Tip

A factory default local admin user was created on the Cisco WAAS and Cisco WAVE appliances during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or if you do not have a TACACS+ server in your organization.

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 13: After you make configuration changes, in the EXEC mode, save the configuration.

```
copy running-config startup-config
```

Step 14: Disconnect from the virtual service console by typing **^c^c^c**.

Step 15: Register Cisco ISR-WAAS to Cisco WCM.

```
RS215-4451X-1# service waas wcm ip address 10.4.48.100
```

Step 16: If this is a dual-router remote site, repeat Step 1 through Step 15 for the second router at the site.

Procedure 4 Configure the AppNav-XE cluster

This procedure is used to create the cluster and assign Cisco ISR-WAAS instances.

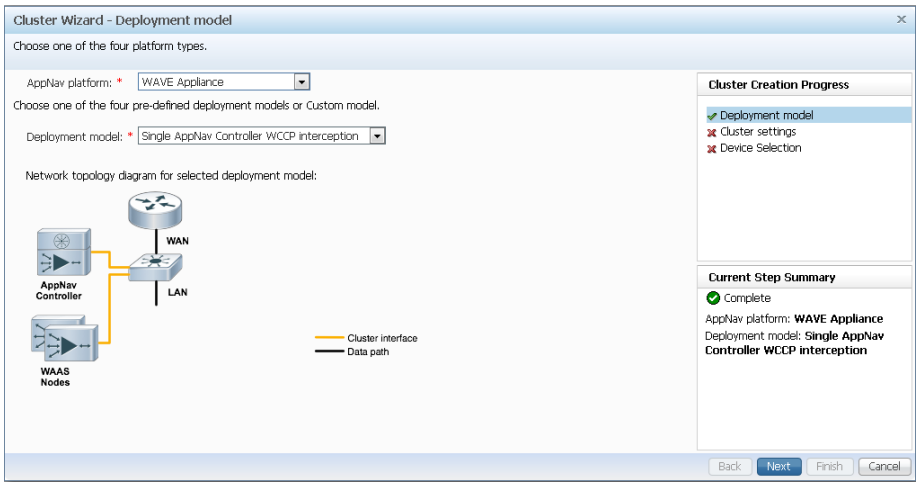
Tech Tip

This procedure assumes that one or more Cisco ISR-WAAS instances have already been configured and are registered to Cisco WCM.

Step 1: Log in to Cisco WCM through the web interface (for example, https://waas-cm.cisco.local:8443).

Step 2: Navigate to **AppNav Clusters > All AppNav Clusters**.

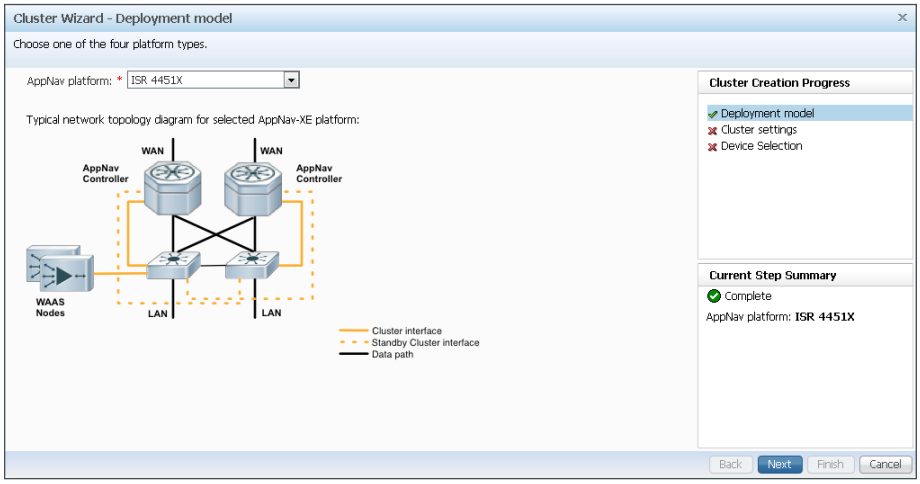
Step 3: Start the configuration by clicking the AppNav Cluster Wizard.



Step 4: Set the Cisco AppNav platform to **ISR 4451X Series**, and then click **Next**.

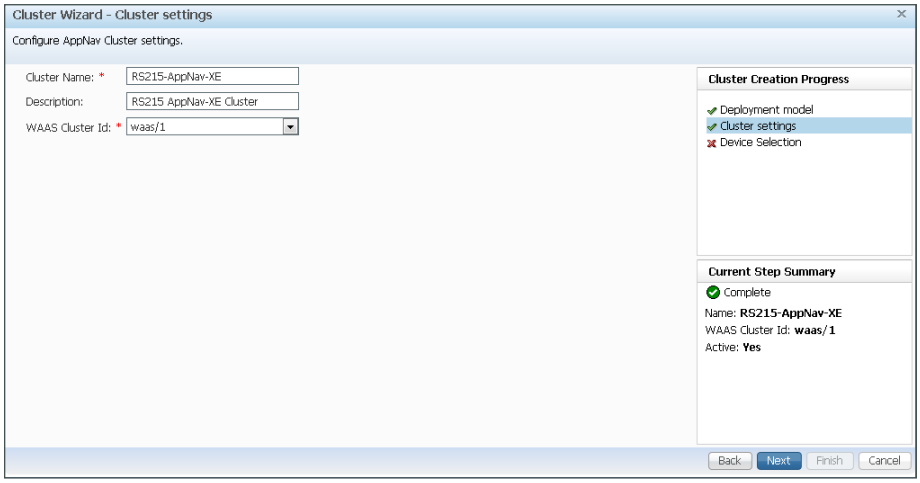
Tech Tip

Cisco AppNav-XE clusters may include routers only within the same product family. You may not mix Cisco ASR 1000 Series routers with Cisco ISR 4451-X routers within the same cluster.



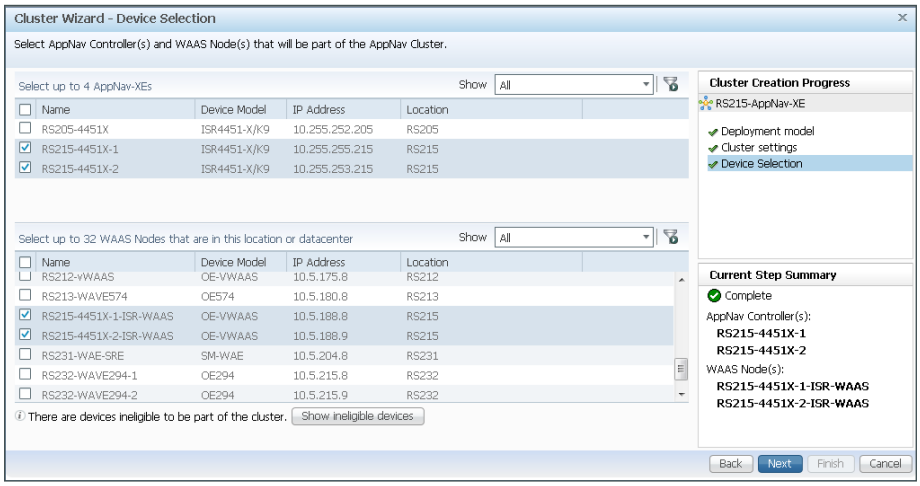
Step 5: In the **Cluster Name** box, enter **RS215-AppNav-XE**, and then, in the **Description** box, enter a description.

Step 6: In the **WAAS Cluster Id** list, choose the default setting of **waas/1**, and then click **Next**.

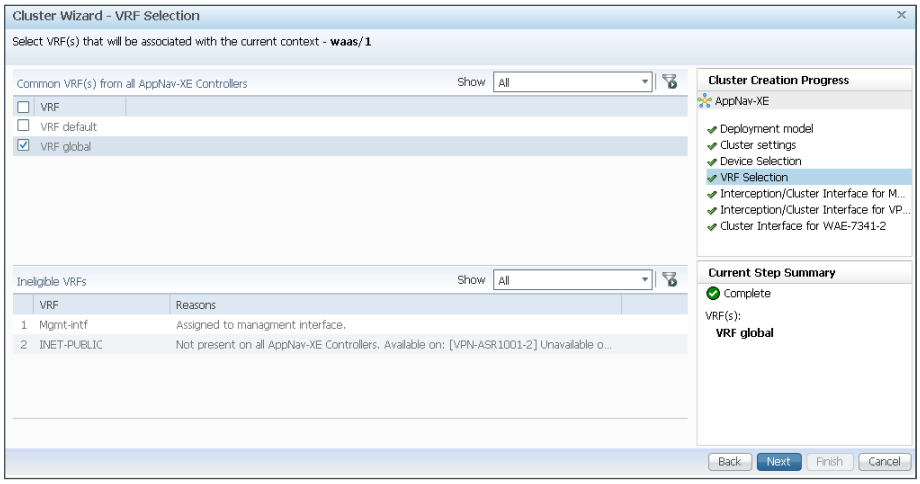


Step 7: Select Cisco AppNav-XE controllers (maximum of 4) that you want to assign to the AppNav cluster under configuration (Example: RS215-4451X-1, RS215-4451X-2).

Step 8: Select the WAAS nodes that you want to assign to the AppNav cluster under configuration (Example: RS215-4451X-1-ISR-WAAS, RS215-4451X-2-ISR-WAAS). After you have selected all devices you want, click **Next**.



Step 9: Clear **VRF default**, select **VRF global**, and then click **Next**.

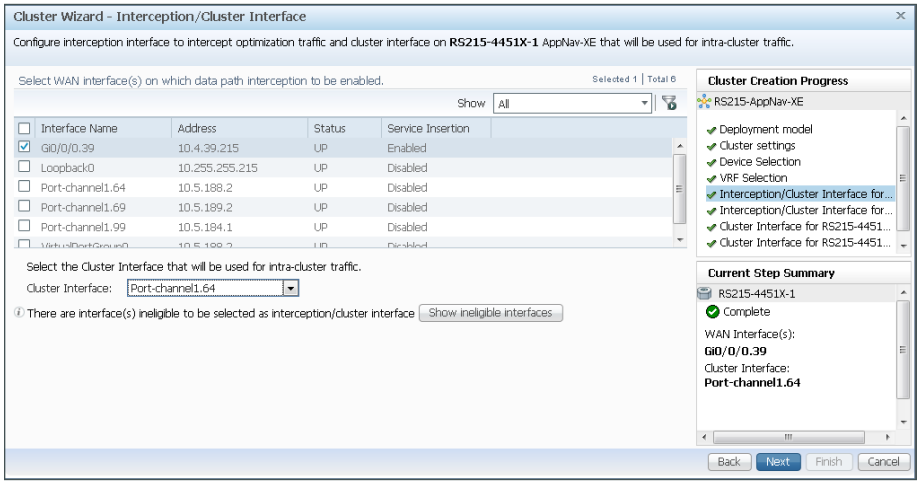


Step 10: Select all WAN-facing interfaces for interception, select the LAN-facing interface as the Cluster Interface for intra-cluster traffic, and then click **Next**. Example settings are shown in the following table.

> **Tech Tip**
>
> An AppNav-XE cluster may contain a maximum of four AppNav Controllers.

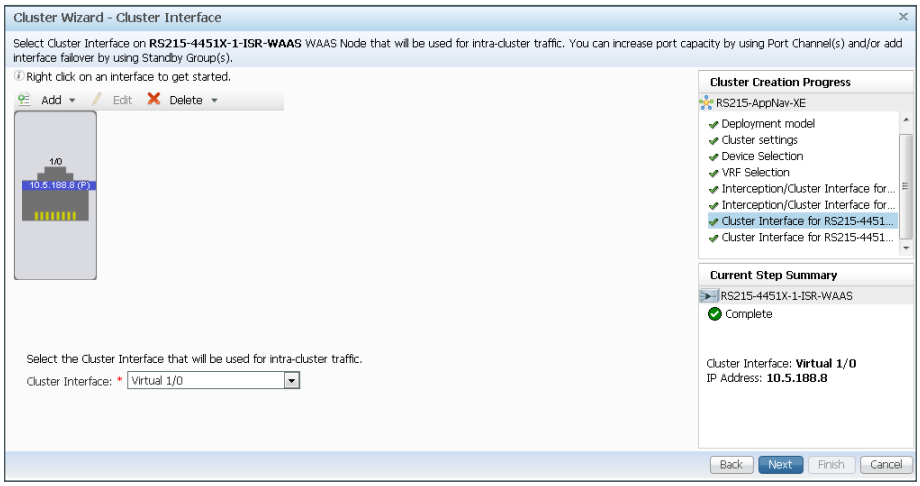
Table 9 - Example settings for interception and cluster interfaces

Router	WAN transport	Interception interface(s)	Cluster Interface
RS215-4451X-1	Layer 2 WAN	Gig0/0/3.39	Port-Channel1.64
RS215-4451X-2	DMVPN-1	Tunnel10	Port-Channel2.64



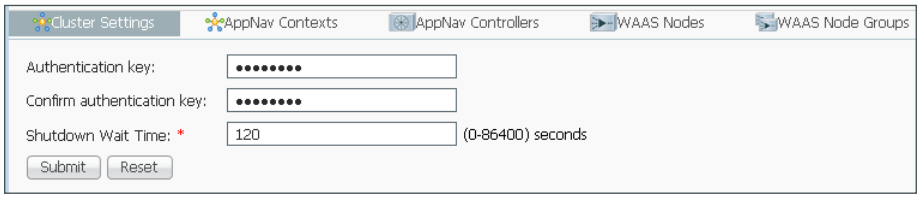
Step 11: If necessary, repeat Step 10 for any additional Cisco AppNav-XE Controller routers.

Step 12: Select the Cluster Interface for the Cisco WAAS node to use for intra-cluster traffic (Example: Virtual1/0). If this is the last WAAS node, click **Finish**, otherwise click **Next**.



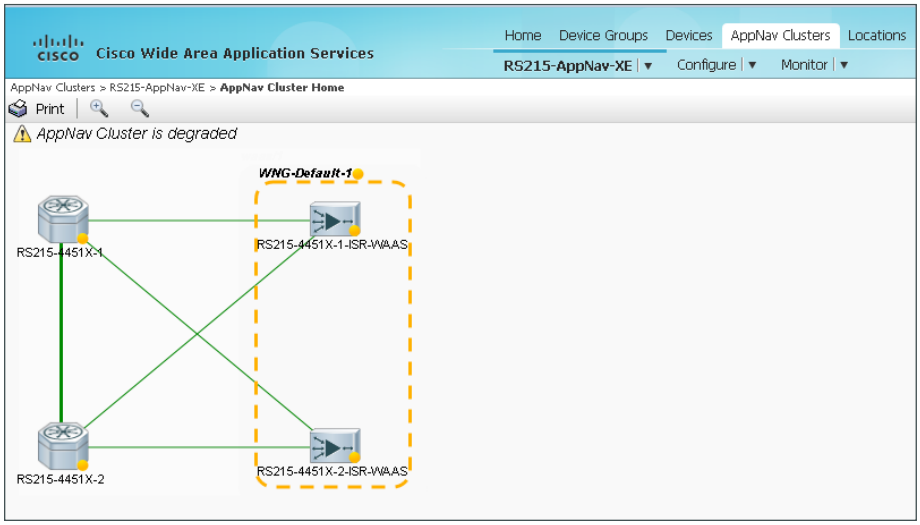
Step 13: If necessary, repeat Step 12 for any additional WAAS nodes.

Step 14: Navigate to **AppNav Clusters > RS215-AppNav-XE**, enter a value for the **Authentication key** and **Confirm authentication key** (Example c1sco123), and then click **Submit**. Authentication with the cluster is configured.



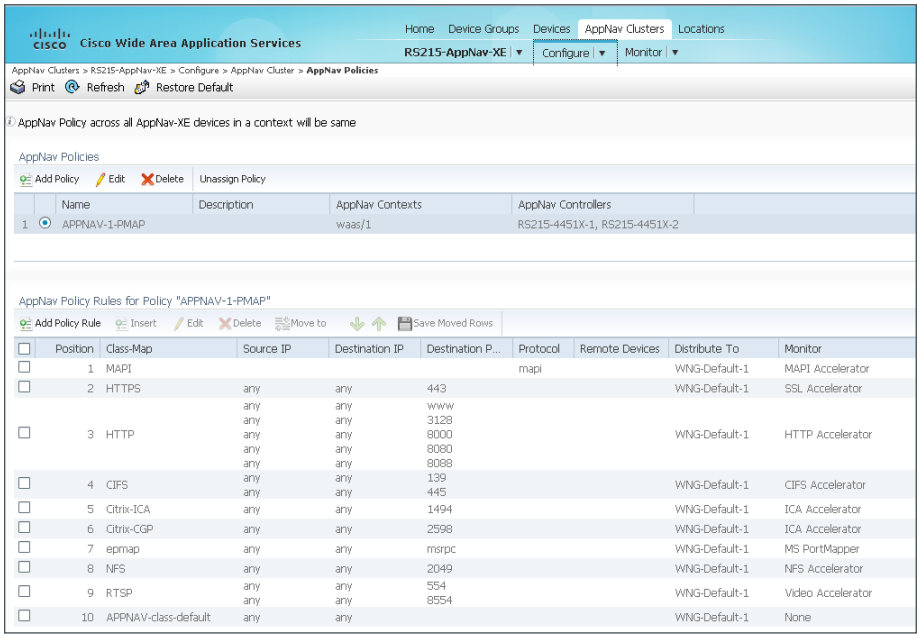
Step 15: Navigate to **AppNav Clusters > AppNav-XE** and verify that the Cisco AppNav cluster is operational.

The default Cisco AppNav policy includes video acceleration. If any of the WAAS nodes do not have a video license, Cisco WCM indicates that the AppNav cluster is degraded.



Step 16: If the Cisco WAAS nodes do not have a video license, disable video acceleration for the Cisco RS215-AppNav-XE cluster by following Step 17 through Step 19.

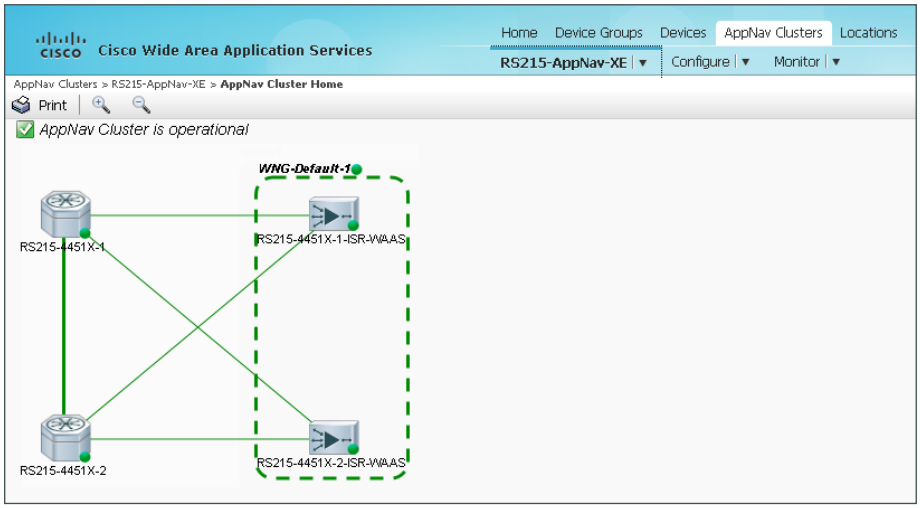
Step 17: If the cluster is not already selected, navigate to **AppNav Cluster > RS215-AppNav-XE**, select the cluster, and then navigate to **Configure>AppNav Policies**.



Step 18: In the lower pane, select the policy rule with the Monitor assigned to Video Accelerator (Example: Position 9 – RTSP), then click **Edit**.

Step 19: Change the setting for Monitor to **None**, click **OK**, and then accept the warning message by clicking **OK** again.

Step 20: Navigate to **AppNav Clusters > RS-215AppNav-XE** and verify that the Cisco AppNav cluster is now operational. Expect a short delay for the new status to be reflected.



Appendix A: Product List

WAAS Central Manager

Functional Area	Product Description	Part Numbers	Software
Central Manager Appliance	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	5.3.1
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	
	Cisco Wide Area Virtualization Engine 294	WAVE-294-K9	
Central Manager Virtual Appliance	Virtual WAAS Central Manager	WAAS-CM-VIRT-K9	5.3.1
	License to manage up to 2000 WAAS Nodes	LIC-VCM-2000N	
	License to manage up to 100 WAAS Nodes	LIC-VCM-100N	

WAAS Remote Site

Functional Area	Product Description	Part Numbers	Software
AppNav-XE Controller	Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU	ISR4451-X-AX/K9	IOS-XE 15.3(3)S securityk9 license appxk9 license
Application Accelerator Virtual Appliance	Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU	ISR4451-X-AX/K9	IOS-XE 15.3(3)S securityk9 license appxk9 license
	NIM Carrier Card for SSD drives	NIM-SSD	
	200 GB, SATA Solid State Disk	SSD-SATA-200G	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU	ISR4451-X-AX/K9	IOS-XE 15.3(3)S securityk9 license appxk9 license

Remote Site 205

Single-Router Configuration Using EZConfig (RS205-4451X)

```
version 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS205-4451X
!
boot-start-marker
boot system flash bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
logging buffered 1000000
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
```

```
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip vrf INET-PUBLIC1
 rd 65512:1
!
ip domain name cisco.local
ip name-server 10.4.48.10
!
!
crypto pki trustpoint TP-self-signed-1895609205
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1895609205
 revocation-check none
 rsakeypair TP-self-signed-1895609205
!
!
crypto pki certificate chain TP-self-signed-1895609205
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101

<content intentionally deleted>

  EA9BBB80 5BDF6E62 3A807C1C 4E7856
   quit
license boot level appxk9
license boot level securityk9
spanning-tree extend system-id
!
username admin password 7 0007421507545A545C
!
redundancy
 mode none
!
!
!
!
!
!
ip ftp source-interface Loopback0
ip ftp username cvd
ip ftp password 7 130646010803557878
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map type appnav match-any RTSP
 match access-group name RTSP
```

```
class-map type appnav match-any AUTOWAAS
 match access-group name AUTOWAAS
class-map match-any DATA
 match dscp af21
class-map type appnav match-any MAPI
 match protocol mapi
class-map type appnav match-any HTTP
 match access-group name HTTP
class-map type appnav match-any CIFS
 match access-group name CIFS
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map type appnav match-any Citrix-CGP
 match access-group name Citrix-CGP
class-map type appnav match-any EPMAP
 match access-group name EPMAP
class-map type appnav match-any HTTPS
 match access-group name HTTPS
class-map match-any VOICE
 match dscp ef
class-map type appnav match-any SN_OR_WCM
 match access-group name SN_OR_WCM
class-map type appnav match-any NFS
 match access-group name NFS
class-map type appnav match-any Citrix-ICA
 match access-group name Citrix-ICA
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
 match access-group name ISAKMP
!
policy-map type appnav AUTOWAAS
 description AUTOWAAS global policy
 class SN_OR_WCM
  pass-through
 class HTTP
  distribute service-node-group AUTOWAAS-SNG
  monitor-load http
 class MAPI
  distribute service-node-group AUTOWAAS-SNG
  monitor-load mapi
 class HTTPS
```

```
  distribute service-node-group AUTOWAAS-SNG
  monitor-load ssl
 class CIFS
  distribute service-node-group AUTOWAAS-SNG
  monitor-load cifs
 class Citrix-ICA
  distribute service-node-group AUTOWAAS-SNG
  monitor-load ica
 class Citrix-CGP
  distribute service-node-group AUTOWAAS-SNG
  monitor-load ica
 class EPMAP
  distribute service-node-group AUTOWAAS-SNG
  monitor-load MS-port-mapper
 class NFS
  distribute service-node-group AUTOWAAS-SNG
  monitor-load nfs
 class RTSP
  distribute service-node-group AUTOWAAS-SNG
  monitor-load video
 class AUTOWAAS
  distribute service-node-group AUTOWAAS-SNG
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
   service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/1
 class class-default
  shape average 5000000
```

```
   service-policy WAN
policy-map WAN-INTERFACE-G0/0/0
 class class-default
  shape average 10000000
   service-policy WAN
!
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server address ipv4 10.4.32.151
 server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
 set group GETVPN-GROUP
!
!
```

```
!
!
!
service-insertion service-node-group AUTOWAAS-SNG
  description "AUTOWAAS"
  service-node 10.5.36.8
  node-discovery enable
!
service-insertion appnav-controller-group AUTOWAAS-SCG
  description "AUTOWAAS"
  appnav-controller 10.5.36.1
!
service-insertion service-context waas/1
  appnav-controller-group AUTOWAAS-SCG
  service-node-group AUTOWAAS-SNG
  service-policy AUTOWAAS
  vrf default
  enable
!
!
interface Loopback0
 ip address 10.255.252.205 255.255.255.255
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 5000
 ip address 10.4.34.205 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-FNF output
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 200 10.5.32.0 255.255.248.0
 ip tcp adjust-mss 1360
```

```
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
 service-insertion waas
!
interface VirtualPortGroup31
 ip unnumbered GigabitEthernet0/0/3.64
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 bandwidth 10000
 ip address 192.168.4.37 255.255.255.252
 ip tcp adjust-mss 1360
 negotiation auto
 no cdp enable
 service-insertion waas
 service-policy output WAN-INTERFACE-G0/0/0
!
interface GigabitEthernet0/0/1
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 negotiation auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0/1
 ip rsvp bandwidth
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3.64
 encapsulation dot1Q 64
 ip address 10.5.36.1 255.255.255.0
 ip helper-address 10.4.48.10
!
interface GigabitEthernet0/0/3.69
 encapsulation dot1Q 69
 ip address 10.5.37.1 255.255.255.0
 ip helper-address 10.4.48.10
!
```

```
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface AppNav-Compress1
 ip unnumbered GigabitEthernet0/0/3.64
 no keepalive
!
interface AppNav-UnCompress1
 ip unnumbered GigabitEthernet0/0/3.64
 no keepalive
!
!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.252.205
 eigrp stub connected summary
!
router bgp 65511
 bgp router-id 10.255.252.205
 bgp log-neighbor-changes
 network 10.5.36.0 mask 255.255.255.0
 network 10.5.37.0 mask 255.255.255.0
 network 10.255.252.205 mask 255.255.255.255
 network 192.168.4.36 mask 255.255.255.252
 aggregate-address 10.5.32.0 255.255.248.0 summary-only
 neighbor 192.168.4.38 remote-as 65402
!
!
virtual-service AUTOWAAS
 profile ISR-WAAS-2500
 vnic gateway VirtualPortGroup31
  guest ip address 10.5.36.8
 activate
!
ip forward-protocol nd
no ip http server
ip http authentication aaa
ip http secure-server
ip http secure-trustpoint TP-self-signed-1895609205
ip http client secure-trustpoint TP-self-signed-1895609205
```

```
ip pim autorp listener
ip pim register-source Loopback0
ip route 10.5.36.8 255.255.255.255 VirtualPortGroup31
ip tacacs source-interface Loopback0
!
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended AUTOWAAS
 permit tcp any any
ip access-list extended CIFS
 permit tcp any any eq 139
 permit tcp any any eq 445
ip access-list extended Citrix-CGP
 permit tcp any any eq 2598
ip access-list extended Citrix-ICA
 permit tcp any any eq 1494
ip access-list extended EPMAP
 permit tcp any any eq msrpc
ip access-list extended HTTP
 permit tcp any any eq www
 permit tcp any any eq 3218
 permit tcp any any eq 8000
 permit tcp any any eq 8080
 permit tcp any any eq 8088
ip access-list extended HTTPS
 permit tcp any any eq 443
ip access-list extended NFS
 permit tcp any any eq 2049
ip access-list extended RTSP
 permit tcp any any eq 554
 permit tcp any any eq 8554
ip access-list extended SN_OR_WCM
 permit tcp host 10.5.36.8 any
 permit tcp any host 10.5.36.8
 permit tcp host 10.4.48.100 any
 permit tcp any host 10.4.48.100
!
!
```

```
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 00371605165E1F2D0A38
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
onep
 transport type tipc
!
end
```

ISR-WAAS Configuration Using EZConfig (RS205-4451X-ISR-WAAS)

```
! waas-universal-k9 version 5.3.1 (build b20 Aug  4 2013)
!
device mode application-accelerator
!
interception-method appnav-controller
!
!
hostname RS205-4451X-ISR-WAAS
!
clock timezone PST -8 0
!
!
```

```
ip domain-name cisco.local
!
!
primary-interface Virtual 1/0
!
interface Virtual 1/0
 ip address 10.5.36.8 255.255.255.0
 ip access-group 155 in
 exit
!
ip default-gateway 10.5.36.1
!
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
!
ip access-list standard 55
 permit 10.4.48.0 0.0.0.255
 exit
!
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
!
!
ntp server 10.4.48.17
!
!
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco123 rw
snmp-server community cisco
snmp-server access-list 55
!
!
!
tacacs key ****
tacacs password ascii
tacacs host 10.4.48.15 primary
!
```

```
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
!
!
no telnet enable
!
sshd enable
!
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
!
accelerator mapi wansecure-mode auto
!
!
!
central-manager address 10.4.48.100
cms enable
!
!
!
stats-collector logging enable
stats-collector logging rate 30
!
service-insertion service-node
  enable
  exit
!
!
! End of WAAS configuration
```

Remote Site 215

Dual-Router Configured Manually and Through WCM (RS215-4451X-1)

```
version 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS215-4451X-1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip domain name cisco.local
ip name-server 10.4.48.10
!
!
```

```
crypto pki trustpoint TP-self-signed-877073049
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-877073049
 revocation-check none
 rsakeypair TP-self-signed-877073049
!
!
crypto pki certificate chain TP-self-signed-877073049
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101

<content intentionally deleted>

  90248651 F830A18B 9A6B9244 05
   quit
license boot level appxk9
license boot level securityk9
spanning-tree extend system-id
!
username admin password 7 06055E324F41584B56
!
redundancy
 mode none
!
!
!
!
!
!
track 50 ip sla 100 reachability
!
ip ftp source-interface Loopback0
ip ftp username bn
ip ftp password 7 121A540411045D5679
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map type appnav match-any RTSP
 match access-group name APPNAV-ACL-RTSP
class-map match-any DATA
 match dscp af21
class-map type appnav match-any MAPI
 match protocol mapi
class-map type appnav match-any HTTP
 match access-group name APPNAV-ACL-HTTP
class-map type appnav match-any APPNAV-class-default
 match access-group name APPNAV-ACL-class-default
```

```
class-map type appnav match-any CIFS
 match access-group name APPNAV-ACL-CIFS
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map type appnav match-any Citrix-CGP
 match access-group name APPNAV-ACL-Citrix-CGP
class-map type appnav match-any HTTPS
 match access-group name APPNAV-ACL-HTTPS
class-map match-any VOICE
 match dscp ef
class-map type appnav match-any Citrix-ICA
 match access-group name APPNAV-ACL-Citrix-ICA
class-map type appnav match-any NFS
 match access-group name APPNAV-ACL-NFS
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map type appnav match-any epmap
 match access-group name APPNAV-ACL-epmap
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
!
policy-map type appnav APPNAV-1-PMAP
 class MAPI
  distribute service-node-group WNG-Default-1
  monitor-load mapi
 class HTTPS
  distribute service-node-group WNG-Default-1
  monitor-load ssl
 class HTTP
  distribute service-node-group WNG-Default-1
  monitor-load http
 class CIFS
  distribute service-node-group WNG-Default-1
  monitor-load cifs
 class Citrix-ICA
  distribute service-node-group WNG-Default-1
  monitor-load ica
 class Citrix-CGP
  distribute service-node-group WNG-Default-1
  monitor-load ica
 class epmap
  distribute service-node-group WNG-Default-1
  monitor-load MS-port-mapper
 class NFS
  distribute service-node-group WNG-Default-1
```

```
  monitor-load nfs
 class RTSP
  distribute service-node-group WNG-Default-1
 class APPNAV-class-default
  distribute service-node-group WNG-Default-1
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
!
!
!
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
!
!
!
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server address ipv4 10.4.32.151
 server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
 set group GETVPN-GROUP
!
```

```
!
!
!
!
service-insertion service-node-group WNG-Default-1
  service-node 10.5.188.8
  service-node 10.5.188.9
!
service-insertion appnav-controller-group scg
  appnav-controller 10.5.188.2
  appnav-controller 10.5.188.3
!
service-insertion service-context waas/1
  authentication sha1 key 7 0205554808095E731F
  appnav-controller-group scg
  service-node-group WNG-Default-1
  service-policy APPNAV-1-PMAP
  vrf global
  enable
!
!
interface Loopback0
 ip address 10.255.255.215 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 description EtherChannel link to RS215-A2960S
 no ip address
 negotiation auto
!
interface Port-channel1.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.188.2 255.255.255.0
 ip helper-address 10.4.48.10
 no ip proxy-arp
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.188.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 141443180F0B7B7977
 standby 1 track 50 decrement 10
!
interface Port-channel1.69
 description Voice
```

```
 encapsulation dot1Q 69
 ip address 10.5.189.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.189.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 0205554808095E731F
 standby 1 track 50 decrement 10
!
interface Port-channel1.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.184.1 255.255.255.252
 ip pim sparse-mode
!
interface VirtualPortGroup0
 ip unnumbered Port-channel1.64
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
 no cdp enable
!
interface GigabitEthernet0/0/0.39
 encapsulation dot1Q 39
 ip address 10.4.39.215 255.255.255.0
 ip pim sparse-mode
 ip summary-address eigrp 300 10.5.184.0 255.255.248.0
 ip tcp adjust-mss 1360
 no cdp enable
 service-insertion waas
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/2
 description RS215-A2960S Gig1/0/24
 no ip address
 negotiation auto
 channel-group 1
```

```
!
interface GigabitEthernet0/0/3
 description RS215-A2960S Gig2/0/24
 no ip address
 negotiation auto
 channel-group 1
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface AppNav-Compress1
 ip unnumbered Port-channel1.64
 no keepalive
!
interface AppNav-UnCompress1
 ip unnumbered Port-channel1.64
 no keepalive
!
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 300
 passive-interface default
 no passive-interface Port-channel1.99
 eigrp router-id 10.255.255.215
!
!
router eigrp 300
 network 10.4.39.0 0.0.0.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 passive-interface default
 no passive-interface GigabitEthernet0/0/0.39
 eigrp router-id 10.255.255.215
 eigrp stub connected summary redistributed
!
!
virtual-service RS215_4451X_1_vWAAS
 profile ISR-WAAS-750
 vnic gateway VirtualPortGroup0
  guest ip address 10.5.188.8
 activate
```

```
!
ip forward-protocol nd
no ip http server
ip http authentication aaa
ip http secure-server
ip http secure-trustpoint TP-self-signed-877073049
ip http client secure-trustpoint TP-self-signed-877073049
ip pim autorp listener
ip pim register-source Loopback0
ip route 10.5.188.8 255.255.255.255 VirtualPortGroup0
ip tacacs source-interface Loopback0
!
!
ip access-list standard R2-LOOPBACK
 permit 10.255.253.215
!
ip access-list extended APPNAV-ACL-CIFS
 permit tcp any any eq 139
 permit tcp any any eq 445
ip access-list extended APPNAV-ACL-Citrix-CGP
 permit tcp any any eq 2598
ip access-list extended APPNAV-ACL-Citrix-ICA
 permit tcp any any eq 1494
ip access-list extended APPNAV-ACL-HTTP
 permit tcp any any eq www
 permit tcp any any eq 3128
 permit tcp any any eq 8000
 permit tcp any any eq 8080
 permit tcp any any eq 8088
ip access-list extended APPNAV-ACL-HTTPS
 permit tcp any any eq 443
ip access-list extended APPNAV-ACL-NFS
 permit tcp any any eq 2049
ip access-list extended APPNAV-ACL-RTSP
 permit tcp any any eq 554
 permit tcp any any eq 8554
ip access-list extended APPNAV-ACL-class-default
 permit tcp any any
ip access-list extended APPNAV-ACL-epmap
 permit tcp any any eq msrpc
!
ip sla 100
 icmp-echo 10.4.39.1 source-interface GigabitEthernet0/0/0.39
 threshold 1000
 timeout 1000
 frequency 15
ip sla schedule 100 life forever start-time now
```

```
!
route-map LOOPBACK-ONLY permit 10
 match ip address R2-LOOPBACK
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 00371605165E1F2D0A38
!
!
!
control-plane
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 transport preferred none
 transport input ssh
line vty 5 15
 exec-timeout 0 0
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
onep
 transport type tipc
!
end
```

Dual-router configured manually and through WCM (RS215-4451X-2)

```
version 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS215-4451X-2
!
boot-start-marker
```

```
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip vrf INET-PUBLIC1
 rd 65512:1
!
!
ip domain name cisco.local
ip name-server 10.4.48.10
!
!
crypto pki trustpoint TP-self-signed-1653662043
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1653662043
 revocation-check none
 rsakeypair TP-self-signed-1653662043
!
!
crypto pki certificate chain TP-self-signed-1653662043
```

```
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101

<content intentionally deleted>

  A1B86605 B7B34F2A 2E9C524C 1F747D
   quit
license boot level appxk9
license boot level securityk9
spanning-tree extend system-id
!
username admin password 7 06055E324F41584B56
!
redundancy
 mode none
!
!
!
!
!
!
ip ftp source-interface Loopback0
ip ftp username bn
ip ftp password 7 110A4816141D5A5E57
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map type appnav match-any RTSP
 match access-group name APPNAV-ACL-RTSP
class-map match-any DATA
 match dscp af21
class-map type appnav match-any MAPI
 match protocol mapi
class-map type appnav match-any HTTP
 match access-group name APPNAV-ACL-HTTP
class-map type appnav match-any APPNAV-class-default
 match access-group name APPNAV-ACL-class-default
class-map type appnav match-any CIFS
 match access-group name APPNAV-ACL-CIFS
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map type appnav match-any Citrix-CGP
 match access-group name APPNAV-ACL-Citrix-CGP
class-map type appnav match-any HTTPS
 match access-group name APPNAV-ACL-HTTPS
```

```
class-map match-any VOICE
 match dscp ef
class-map type appnav match-any Citrix-ICA
 match access-group name APPNAV-ACL-Citrix-ICA
class-map type appnav match-any NFS
 match access-group name APPNAV-ACL-NFS
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map type appnav match-any epmap
 match access-group name APPNAV-ACL-epmap
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
 match access-group name ISAKMP
!
policy-map type appnav APPNAV-1-PMAP
 class MAPI
  distribute service-node-group WNG-Default-1
  monitor-load mapi
 class HTTPS
  distribute service-node-group WNG-Default-1
  monitor-load ssl
 class HTTP
  distribute service-node-group WNG-Default-1
  monitor-load http
 class CIFS
  distribute service-node-group WNG-Default-1
  monitor-load cifs
 class Citrix-ICA
  distribute service-node-group WNG-Default-1
  monitor-load ica
 class Citrix-CGP
  distribute service-node-group WNG-Default-1
  monitor-load ica
 class epmap
  distribute service-node-group WNG-Default-1
  monitor-load MS-port-mapper
 class NFS
  distribute service-node-group WNG-Default-1
  monitor-load nfs
 class RTSP
  distribute service-node-group WNG-Default-1
 class APPNAV-class-default
  distribute service-node-group WNG-Default-1
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
```

```
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
!
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
!
!
service-insertion service-node-group WNG-Default-1
  service-node 10.5.188.8
  service-node 10.5.188.9
!
```

```
service-insertion appnav-controller-group scg
  appnav-controller 10.5.188.2
  appnav-controller 10.5.188.3
!
service-insertion service-context waas/1
  authentication sha1 key 7 130646010803557878
  appnav-controller-group scg
  service-node-group WNG-Default-1
  service-policy APPNAV-1-PMAP
  vrf global
  enable
!
!
interface Loopback0
 ip address 10.255.253.215 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel2
 description EtherChannel link to RS215-A2960S
 no ip address
 no negotiation auto
!
interface Port-channel2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.188.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.188.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string 7 141443180F0B7B7977
!
interface Port-channel2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.189.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.189.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string 7 0205554808095E731F
```

```
!
interface Port-channel2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.184.2 255.255.255.252
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 5000
 ip address 10.4.34.215 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 200 10.5.184.0 255.255.248.0
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
 service-insertion waas
!
interface VirtualPortGroup0
 ip unnumbered Port-channel2.64
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 negotiation auto
 no cdp enable
!
interface GigabitEthernet0/0/1
```

```
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/2
 description RS215-A2960S Gig1/0/23
 no ip address
 negotiation auto
 channel-group 2
!
interface GigabitEthernet0/0/3
 description RS215-A2960S Gig2/0/23
 no ip address
 negotiation auto
 channel-group 2
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface AppNav-Compress1
 ip unnumbered Port-channel2.64
 no keepalive
!
interface AppNav-UnCompress1
 ip unnumbered Port-channel2.64
 no keepalive
!
!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.253.215
 eigrp stub connected summary redistributed
!
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
```

```
 no passive-interface Port-channel2.99
 eigrp router-id 10.255.253.215
!
!
virtual-service RS215_4451X_2_vWAAS
 profile ISR-WAAS-1300
 vnic gateway VirtualPortGroup0
  guest ip address 10.5.188.9
 activate
!
ip forward-protocol nd
no ip http server
ip http authentication aaa
ip http secure-server
ip http secure-trustpoint TP-self-signed-1653662043
ip http client secure-trustpoint TP-self-signed-1653662043
ip pim autorp listener
ip pim register-source Loopback0
ip route 10.5.188.9 255.255.255.255 VirtualPortGroup0
ip tacacs source-interface Loopback0
!
!
ip access-list standard R1-LOOPBACK
 permit 10.255.255.215
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended APPNAV-ACL-CIFS
 permit tcp any any eq 139
 permit tcp any any eq 445
ip access-list extended APPNAV-ACL-Citrix-CGP
 permit tcp any any eq 2598
ip access-list extended APPNAV-ACL-Citrix-ICA
 permit tcp any any eq 1494
ip access-list extended APPNAV-ACL-HTTP
 permit tcp any any eq www
 permit tcp any any eq 3128
 permit tcp any any eq 8000
 permit tcp any any eq 8080
```

```
 permit tcp any any eq 8088
ip access-list extended APPNAV-ACL-HTTPS
 permit tcp any any eq 443
ip access-list extended APPNAV-ACL-NFS
 permit tcp any any eq 2049
ip access-list extended APPNAV-ACL-RTSP
 permit tcp any any eq 554
 permit tcp any any eq 8554
ip access-list extended APPNAV-ACL-class-default
 permit tcp any any
ip access-list extended APPNAV-ACL-epmap
 permit tcp any any eq msrpc
!
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 00371605165E1F2D0A38
!
!
!
control-plane
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 transport preferred none
 transport input ssh
line vty 5 15
 exec-timeout 0 0
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
onep
```

```
 transport type tipc
!
end
```

ISR-WAAS Configuration WCM (RS215-4451X-1-ISR-WAAS)

```
! waas-universal-k9 version 5.3.1 (build b20 Aug  4 2013)
!
device mode application-accelerator
!
interception-method appnav-controller
!
!
hostname RS215-4451X-1-ISR-WAAS
!
clock timezone PST -8 0
!
!
ip domain-name cisco.local
!
!
primary-interface Virtual 1/0
!
interface Virtual 1/0
 ip address 10.5.188.8 255.255.255.0
 ip access-group 155 in
 exit
!
ip default-gateway 10.5.188.1
!
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
!
ip access-list standard 55
 permit 10.4.48.0 0.0.0.255
 exit
!
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
!
```

```
!
ntp server 10.4.48.17
!
!
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco123 rw
snmp-server community cisco
snmp-server access-list 55
!
!
!
tacacs key ****
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
!
!
no telnet enable
!
sshd enable
!
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
!
accelerator mapi wansecure-mode auto
!
!
!
central-manager address 10.4.48.100
cms enable
!
!
!
stats-collector logging enable
stats-collector logging rate 30
!
```

```
service-insertion service-node
  description WN of RS215-AppNav-XE
  authentication sha1 key ****
  enable
  exit
!
!
! End of WAAS configuration
```

ISR-WAAS Configuration WCM (RS215-4451X-2-ISR-WAAS)

```
! waas-universal-k9 version 5.3.1 (build b20 Aug  4 2013)
!
device mode application-accelerator
!
interception-method appnav-controller
!
!
hostname RS215-4451X-2-ISR-WAAS
!
clock timezone PST -8 0
!
!
ip domain-name cisco.local
!
!
primary-interface Virtual 1/0
!
interface Virtual 1/0
 ip address 10.5.188.9 255.255.255.0
 ip access-group 155 in
 exit
!
ip default-gateway 10.5.188.1
!
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
!
ip access-list standard 55
 permit 10.4.48.0 0.0.0.255
 exit
!
ip access-list extended 155
```

```
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
!
!
ntp server 10.4.48.17
!
!
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco123 rw
snmp-server community cisco
snmp-server access-list 55
!
!
!
tacacs key ****
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
!
!
no telnet enable
!
sshd enable
!
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
!
accelerator mapi wansecure-mode auto
!
!
!
central-manager address 10.4.48.100
cms enable
!
```

```
!
!
stats-collector logging enable
stats-collector logging rate 30
!
service-insertion service-node
  description WN of RS215-AppNav-XE
  authentication sha1 key ****
  enable
  exit
!
!
! End of WAAS configuration
```

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.

B-0000120-1 12/13