CISCO VALIDATED PROFILE

Enterprise Routing Internet Edge Profile LAN-WAN

April 2017

Table of Contents

Profile Introduction 1

Network Profile 2

- Topology Diagram 3
- Hardware & Feature Specifications 4
- Test Environment 5

Use-Case Scenarios 7

- Test Methodology 7

Best Practices 8

Appendix A: Output Captures 10

Appendix B: Internet Edge LAN-WAN 15

- Flexible NetFlow 15
- ACL 16
- Box-to-Box Redundancy 17
- HQOS 17
- NAT 20
- ZBFW 20
- AVC Profile A 21
- AVC Profile B 27

Profile Introduction

Cisco is transforming the network edge with the Cisco ASR1K/ISR4K Series Aggregation Services Routers, a new line of midrange routers that establish a new price-to-performance class offering, benefiting both enterprises and service providers. These routers provide a great opportunity for simplifying the WAN edge and significantly decreasing network operating expenses (OpEx). By efficiently integrating a critical set of WAN edge functions such as WAN aggregation, Internet edge services, firewall services, VPN termination, etc. into a single platform, this solution can help enterprises meet their business objectives by facilitating deployment of advanced services in a secure, scalable, and reliable manner while minimizing the total cost of ownership.

Cisco WAN aggregation solutions distinguish themselves from other solutions by offering multiservice routers with the highest performance, availability, and density for concurrent data, as well as security, voice, and application-acceleration services with maximum headroom for growth. The solutions feature embedded security, performance, and memory enhancements. High-performance interfaces featuring the latest WAN technologies can help enterprises meet the needs of the most demanding WAN network.

Enterprise wifi users and devices have been growing exponentially. Customers are demanding large scale Network Address Translation (NAT) deployment for IPv4 address conservation and for IPv6 enabled mobile devices to be able to have Internet access. Cisco Aggregation Services Router (ASR1000) is already the popular platform for Internet Edge platforms, providing 10G connectivities and multiple ISP peerings to download full Internet routing tables, and system resources are still under-utilized. On the other hand, customers are fully aware of the NAT44 and NAT64 rich feature sets on ASR 1000. Additionally, some of the existing platform such as CAT6k FSM module currently in their network performing the NAT function are going end of sale; there are therefore strong requirements to consolidate the border gateway protocol routing and NAT function into single system on ASR 1000. Security is always a priority for customers' Internet Edge deployment, and the ASR 1000 zone-based firewall (ZBFW) provides effective protection against distributed denial of service attacks.

The following table lists the key areas on which the profile focuses.

Table 1 *Profile feature summary*

Deployment areas	Features
Security	ZBFW, ACL
Network services	Hierarchical quality of service (HQOS), control plane policing (CoPP), NAT44
IPV6 migration	V6 to v4 migration via NAT
Network planning & troubleshooting	NetFlow, application visibility
Efficient network management	Cisco Prime Infrastructure,LiveAction
System and network resiliency	EtherChannel, box-to-box high availability (B2BHA)
Routing	EBGP

Network Profile

Cisco ASR 1000 can sustain a high rate of firewall and NAT sessions while maintaining a very high number of concurrent sessions inspected all the way up to layer7 content. B2BHA is a method for achieving high availability of applications such as ZBFW, NAT, VPN, session border controller, etc. between ASR 1000 routers.

The NAT B2BHA support feature enables network-wide protection by making an IP network resilient to potential link and router failures at the NAT border.

The NAT B2BHA support feature also leverages services provided by the redundancy group (RG) infrastructure present on the device to implement the high-availability functionality. The RG infrastructure defines multiple RGs to which applications can subscribe and function in an active-standby mode across different devices. The NAT box-to-box high-availability functionality is achieved when you configure two NAT translators, residing across different devices, to an RG and function as a translation group. One member of the translation group acts as an active translator and the other members of the translation group act as a standby translator. The active translator is responsible for handling traffic that requires address translation. Additionally, the active translator informs the standby translator about packet flows that are being translated. The standby translator uses this information to create a duplicate translation database that equips the standby translator to take over as the active translator in the event of any failures to the active translator. Therefore, the application traffic flow continues unaffected as the translations tables are backed up in a stateful manner across the active and standby translators.

B2BHA deployments could have following three topologies:

- LAN-LAN
- LAN-WAN
- WAN-WAN

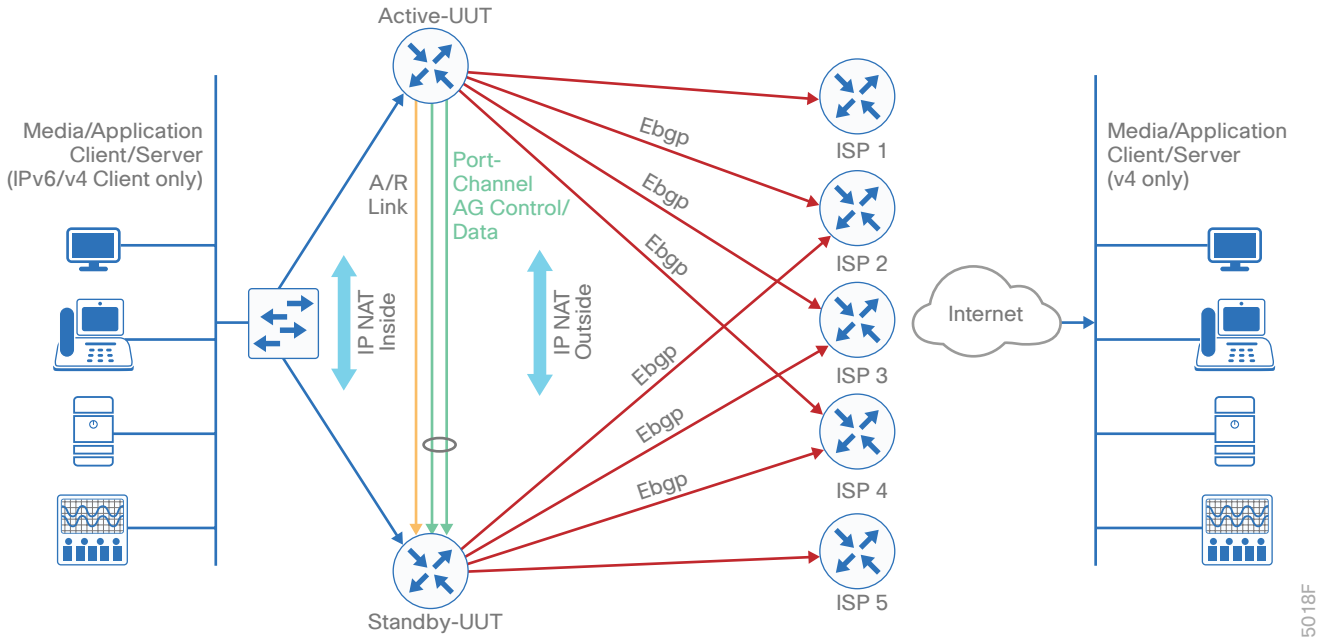
This document focuses on LAN-WAN model.

This is the first time in the Cisco product portfolio that this functionality provided by only an appliance would be offered on a routing platform. B2BHA is supported in the Cisco ASR 1000 family of routers starting RLS3.1.0. ASR 1000 that supports B2BHA offers stateful failover of zone-based firewall and NAT, as well as secure service including session border controller (RLS3.2S). The redundancy framework not only supports a large set of application types but is also built to accommodate any existing or custom redundancy protocol.

Based on the research, customer feedback, and configuration samples, the profile is designed with a deployment topology that is generic and can easily be modified to fit any specific deployment scenario. Refer to the topology for further details.

TOPOLOGY DIAGRAM

Figure 1 *Internet Edge Profile: topology overview*



Disclaimer

The links between the different network layers in the topology are mainly to facilitate this profile validation across different platform combinations, and the actual deployment could vary based on specific requirement

HARDWARE & FEATURE SPECIFICATIONS

This section describes the 3-D feature matrix where the hardware platforms are listed along with their place-in-network and the relevant Government vertical deployment.

Key Vertical Features

The scale of these configured features, the test environment, list of endpoints, and hardware/software versions of the network topology are defined the subsequent sections of this guide.

Disclaimer

Refer to appropriate CCO documentation for release/feature support across different platforms

The following physical topology is used for Internet Edge profile testing. The following devices were used to test the Active and Standby UUT as depicted in topology:

- ASR1001-X (16 GB memory)
- ASR1002-X (16 GB memory)
- ASR1006 with RP2/ESP40 (16 GB memory)

The following device simulates the ISP with which the edge router peers:

- ASR1006 with RP2/ESP40 simulating the ISP

The following device is used as a switch at the LAN end:

- 7606 simulating the Switch

Hardware Profile

Table 2 defines the set of relevant servers, test equipment, and endpoints that are used to complete the end-to-end Government branch vertical profile deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complements the actual physical topology shown in Figure 1.

Table 2 *Hardware profile of servers and endpoints*

VM and HW	Software versions	Description
LiveAction	4.0	For network management
Spirent	Test center 3.95	Generate traffic streams
Ixia	IxNetwork,IxLoad and IxExplorer version 6.40	Generate traffic streams

TEST ENVIRONMENT

This section describes the features and the relevant scales at which the features are deployed across the physical topology. Testing is done with IMIX traffic. Table 3 lists the scale for each feature.

Disclaimer

The table below captures a sample set of scale values used in one of the use cases. Refer to appropriate CCO documentation/datasheets for comprehensive scale data.

Table 3 *Internet Edge Profile: features*

Features	Tested values
Hardware platforms	ASR1002-X(8GB), ASR1001-X(8GB), RP2/ESP40
Routing	Full internet routing table (500k IPv4 routes + 20k IPv6 routes) x5 (learned same routes 5 times via 5 ISP/eBGP Peerings)
Interfaces	SPA-10GE, built-in TenGE, SPA-1GE, port-channel. Internet-facing P2P TenGE/GE links to each ISPs LAN facing TenGE connections to campus VSS switch
ACL	< 1000 ACEs - ACLs applied for class-maps Object Group ACL for NAT/FW
HQOS	QoS Marking on LAN, QoS queueing on Internet link
CoPP	Refer to appropriate CCO documentation for COPP best practice configuration
Flexible NetFlow	Enable NetFlow v9/FNF and Highspeed NetFlow Logging export to an external collector based on traffic being simulated.

Table 3 continued

NAT44/NAT64	Campus traffic could be both IPv4 and IPv6, coming in via same phy/port-channel (sub)interface. Need to be either NAT44 or NAT64 NATed toward Internet. Stateless sessions: ASR1002-X - 1M sessions ASR1001-X - 1M sessions ESP40 - 1M sessions (80%v4; 20%v6) NAT44 ALG: DNS ALG - name entries, PTR record, compress format record, port 21 SIP ALG - vTCP reset storm, tcp retransmition with segments, disable SIP ALG, malformed SIP TCP packets. HTTP ALG - both src/dst ports are well-known RTSP ALG H323 ALG - vTCP need to make adjust in case 10k +h323 resemble packet size received ALG with ip nat max-entries ACL NAT44+ALG+FW+NBAR NAT 64 ALG - FTP64 High Availability: 1) Stateful Inter-box Redundancy 2) Asymmetric routing - A/R (inside Global or VRF) High speed logging (LiveAction) Performance testing for at minimum 10Gbps throughput
ZBFW	IPv4 & IPv6 firewall dual-stack with B2B HA and asymmetric routing support. VRF Support ZBFW B2B A/R. Create 3 FW Zones (inside,outside,DMZ). Inspect all traffic from inside-->outside, DMZ -->outside, allow only http, smtp from outside-->DMZ web & mail server. Allow/inspect SQL/SMTP traffic from web/email server from DMZ-->inside.
AVC	1) AVC Profile A (Application QoS) 2) AVC Profile B (Application QoS + Application Usage)

Use-Case Scenarios

TEST METHODOLOGY

The test cases will be executed using the topology shown in Figure 1, along with the test environment

Images are loaded on the devices under test via the tftp server using the management interface.

To validate a new release, the network topology is upgraded with the new software image with existing configuration composed of the use-cases and relevant traffic profiles. The addition of new use-cases acquired from the field or customer deployments are added on top of the existing configuration.

During each use case execution, syslog would be monitored closely across the devices for any relevant system events, errors, or alarms. With respect to longevity for this profile setup, CPU and memory usage/leaks would be monitored during the validation phase. Furthermore, to test the robustness of the software release and platform under test, typical networks events would be triggered during the use-case execution process.

Best Practices

NAT Configuration Overview

- Change pool size.
- Turn off the traffic by shutting down NAT interfaces
- Clear ip nat translations
- Enter config mode and remove the old pool
- Add new pool/new block
- Turn on the interfaces.
- No need to reload the router

Changing from the default NAT mode to CGN

Use the following steps first on the standby router, then on the active router.

Standby

Step 1: Shutdown redundancy on standby.

Step 2: Enable CGN.

```
ip nat setting mode cgn
ip nat setting pap limit 30 bpa step-size 1
no ip nat inside source route-map rmap-cv pool pool-cv redundancy 1 mapping-id 10
ip nat inside source route-map rmap-cv pool pool-cv redundancy 1 mapping-id 10 overload
```

Step 3: Use **show run | sec ip nat** to verify the results of the configuration changes.

Active

Step 4: Disable NAT on interfaces, and then clear NAT table.

```
interface [inside interface]
 shutdown
interface [outside interface]
 shutdown
clear ip nat translations *
```

Wait until all translations are cleared and all allocated IP addresses are freed.

Step 5: Enable CGN.

```
ip nat setting mode cgn
ip nat setting pap limit 30 bpa step-size 1
no ip nat inside source route-map rmap-cv pool pool-cv redundancy 1 mapping-id 10 forced
ip nat inside source route-map rmap-cv pool pool-cv redundancy 1 mapping-id 10 overload
```

Step 6: Enable interfaces.

```
interface [inside interface]
 no shutdown
interface [outside interface]
 no shutdown
```

Step 7: After translations are created, disable shutdown redundancy on standby, and then wait until the standby comes up and translations are synced.

Tech Tip

Always clear NAT translations the following way:

```
clear ip nat redundancy group [group-id]
```

Tech Tip

NAT64 and NAT44 can exist on the same box but not on the same interface

Appendix A: Output Captures

```
#show ip route  summary
IP routing table name is default (0x0)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           39
0           0
bgp 100         499999      14          0           3744        11232
static          2           36          0           3648        10944
application     0           0           0           0           48001248
144003744
  External: 500013 Internal: 0 Local: 0
internal        21                                              40014888
Total           500022      89          0           48008640    184040808

#show ipv6 route summary
IPv6 routing table name is default(0) global scope - 20022 entries
IPv6 routing table default maximum-paths is 16
Route Source    Networks    Overhead    Memory (bytes)
connected       9           1296        1872
local           12          1728        2496
application     0           0           0
ND              0           0           0
  Default: 0  Prefix: 0  Destination: 0  Redirect: 0
bgp 100         19999       2879856     4159792
  Internal: 0  External: 19999  Local: 0
static          2           288         416
  Static: 2  Per-user static: 0
Total           20022       2883168     4164576

  Number of prefixes:
    /8: 1, /64: 20001, /96: 9, /128: 11
# show nat64 statistics
NAT64 Statistics
Total active translations: 200004 (0 static, 200004 dynamic; 200004 extended)
```

```
Sessions found: 42223
        Sessions created: 200000
        Expired translations: 0
        Global Stats:
           Packets translated (IPv4 -> IPv6)
              Stateless: 0
              Stateful: 1459
              MAP-T: 0
           Packets translated (IPv6 -> IPv4)
              Stateless: 0
              Stateful: 239309
              MAP-T: 0

        Interface Statistics
           TenGigabitEthernet0/2/0.6 (IPv4 not configured, IPv6 configured):
              Packets translated (IPv4 -> IPv6)
                 Stateless: 0
                 Stateful: 0
                 MAP-T: 0
              Packets translated (IPv6 -> IPv4)
            Stateless: 0
                 Stateful: 239309
                 MAP-T: 0
              Packets dropped: 0
           TenGigabitEthernet0/2/0.72 (IPv4 not configured, IPv6 configured):
              Packets translated (IPv4 -> IPv6)
                 Stateless: 0
                 Stateful: 0
                 MAP-T: 0
              Packets translated (IPv6 -> IPv4)
                 Stateless: 0
                 Stateful: 0
                 MAP-T: 0
              Packets dropped: 0
           TenGigabitEthernet0/3/0.6 (IPv4 configured, IPv6 configured):
              Packets translated (IPv4 -> IPv6)
```

```
            Stateless: 0
            Stateful: 1459
            MAP-T: 0
         Packets translated (IPv6 -> IPv4)
Stateless: 0
            Stateful: 0
            MAP-T: 0
         Packets dropped: 0
Dynamic Mapping Statistics
   v6v4
      access-list NAT64_ACL pool POOL_NAT64_1 refcount 0
         pool POOL_NAT64_1:
            start 114.1.1.3 end 114.1.1.254
            total addresses 252, allocated 4 (1%)
            address exhaustion packet count 0
Limit Statistics
#sh ip nat statistics
Total active translations: 834000 (0 static, 834000 dynamic; 834000 extended)
Outside interfaces:
  GigabitEthernet0/0/3, GigabitEthernet0/0/4, TenGigabitEthernet0/3/0.2
  TenGigabitEthernet0/3/0.3, TenGigabitEthernet0/3/0.4
Inside interfaces:
  TenGigabitEthernet0/2/0.2, TenGigabitEthernet0/2/0.3
  TenGigabitEthernet0/2/0.60, TenGigabitEthernet0/2/0.61
  TenGigabitEthernet0/2/0.70, TenGigabitEthernet0/2/0.71
  TenGigabitEthernet0/2/0.72
Hits: 868764  Misses: 834000
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list ACL-IXNETWORK pool POOL-IXNETWORK refcount 834000
 pool POOL-IXNETWORK: id 6, netmask 255.255.0.0
        start 185.0.0.1 end 185.0.254.254
        type generic, total addresses 65278, allocated 1 (0%), misses 0
[Id: 2] access-list ACL-IxNETWORK1 pool POOL-IXNETWORK1 refcount 0
 pool POOL-IXNETWORK1: id 7, netmask 255.255.0.0
```

```
        start 175.0.0.1 end 175.0.254.254
        type generic, total addresses 65278, allocated 0 (0%), misses 0
[Id: 3] access-list spirent pool spirent refcount 0
 pool spirent: id 10, netmask 255.255.0.0
        start 191.0.0.1 end 191.0.254.254
        type generic, total addresses 65278, allocated 0 (0%), misses 0
[Id: 4] access-list spirent1 pool spirent1 refcount 0
 pool spirent1: id 11, netmask 255.255.0.0
        start 141.0.0.1 end 141.0.254.254
        type generic, total addresses 65278, allocated 0 (0%), misses 0
[Id: 5] access-list ACL_VRF pool POOL_VRF refcount 0
 pool POOL_VRF: id 5, netmask 255.255.0.0
        start 71.0.0.1 end 71.0.0.2
        type generic, total addresses 2, allocated 0 (0%), misses 0
[Id: 6] access-list ACL_VRF_STATEFUL pool POOL_VRF_STATEFUL refcount 0
 pool POOL_VRF_STATEFUL: id 2, netmask 255.255.0.0
        start 5.50.0.1 end 5.50.0.2
        type generic, total addresses 2, allocated 0 (0%), misses 0
[Id: 7] access-list ACL_VRF_STATELESS pool POOL_VRF_STATELESS refcount 0
 pool POOL_VRF_STATELESS: id 3, netmask 255.255.0.0
        start 8.80.0.1 end 8.80.0.4
        type generic, total addresses 4, allocated 0 (0%), misses 0
nat-limit statistics:
max entry: max allowed 2000000, used 834000, missed 0
In-to-out drops: 0  Out-to-in drops: 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0

#show flow monitor  my-input-usage-monitor statistics
  Cache type:                               Normal (Platform cache)
  Cache size:                                10000
  Current entries:                            8198
  High Watermark:                            10000
```

```
Flows added:                          814198
Flows not added:                         403
Flows aged:                           806000
  - Emergency aged                    806000
```

Appendix B: Internet Edge LAN-WAN

FLEXIBLE NETFLOW

```
flow record my-input-usage-monitor-record
 match ipv4 version
 match interface input
 match flow direction
 match application name account-on-resolution
 collect routing vrf input
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection new-connections
 collect connection sum-duration
!
!
flow record my-output-usage-monitor-record
 match ipv4 version
 match interface output
 match flow direction
 match application name account-on-resolution
 collect routing vrf input
 collect interface input
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection new-connections
 collect connection sum-duration
!
flow exporter export
 destination [ip address]
 source [interface name]
```

```
transport udp [port number]
        !
        flow monitor my-input-usage-monitor
         exporter export
         cache timeout inactive [value]
         cache timeout active [value]
         cache entries [value]
         record my-input-usage-monitor-record
        !
        flow monitor my-output-usage-monitor
         exporter export
        cache timeout inactive [value]
         cache timeout active [value]
         cache entries [value]
         record my-output-usage-monitor-record
        !
        Interface [interface name]
        ip flow monitor my-input-usage-monitor input
        ip flow monitor my-output-usage-monitor output
```

ACL

```
        ip access-list extended WiFi-Public-RFC1918-protect
         remark Addition of LDAP public space jdigangi
         remark Subscriber DNS
         permit ip any host 10.240.205.161
         permit ip any host 10.240.205.162
         permit ip any host 10.250.255.72
         permit ip any host 10.250.255.73
         permit ip any host 10.243.255.72
         permit ip any host 10.243.255.73
         permit ip any host 10.248.69.86
         permit ip 25.0.0.0 0.255.255.255 167.206.10.144 0.0.0.15
         permit ip 25.0.0.0 0.255.255.255 167.206.211.224 0.0.0.15
         permit ip 25.0.0.0 0.255.255.255 167.206.237.112 0.0.0.15
         remark IPerf
```

BOX-TO-BOX REDUNDANCY

```
redundancy
 application redundancy
  group 1
   name [name]
   preempt
   priority [value] failover threshold [value]
   timers delay [value] reload [value]
   control [interface name]protocol 1
   data [interface name]
   asymmetric-routing interface [interface name]
   asymmetric-routing always-divert enable
   track 1 decrement [value]
  group 2
   name [name]
   preempt
   priority [value]
   control [interface name]protocol 2
   data [interface name]
   asymmetric-routing interface [interface name]
   asymmetric-routing always-divert enable
  protocol 1
   timers hellotime [value] holdtime [value]
   authentication md5 key-string [string]

interface [interface name]
  redundancy rii [value]
redundancy group 1 ip [ip address] exclusive
```

HQOS

```
class-map match-any VOIX
 match dscp ef
class-map match-any ORACLE
 match protocol ora-srv
 match protocol ncube-lm
class-map match-any HTTP
```

```
 match protocol http
class-map match-any CITRIX
 match protocol citrix
class-map match-any DATA1
 match dscp cs4
 match dscp cs2
class-map match-any DATA2
 match dscp af11
class-map match-any DATA3
 match dscp af21
 match dscp af31


class-map match-any HTTPS
 match protocol secure-http
 match protocol ssl
class-map match-any EMAIL
 match protocol attribute category email
class-map match-all cm-epc
 match access-group name acl_epc
class-map match-any VOICE
 match protocol rtp
class-map match-all Undesirable
 match access-group name Undesirable
class-map match-any DNS
 match protocol attribute sub-category naming-services
!
policy-map QOS_WAN
 class VOIX
  priority
  police rate percent 28
 class DATA1
  bandwidth remaining percent 59
  random-detect dscp-based
  fair-queue
 class DATA2
```

```
  bandwidth remaining percent 3
  random-detect dscp-based
  fair-queue
 class DATA3
  bandwidth remaining percent 7
  random-detect dscp-based
  fair-queue
 class class-default
  bandwidth remaining percent 3
  random-detect dscp-based
  fair-queue
policy-map POLICY_WAN
 class class-default
  shape average 10000000000
policy-map QOS_LAN
 class VOICE
  set ip dscp ef
 class HTTP
  set dscp cs4
 class HTTPS
  set dscp cs2
 class ORACLE
  set dscp af11
 class CITRIX
  set ip dscp af21
 class EMAIL
  set ip dscp af31
 class DNS
  set ip dscp default

interface [interface name]
service-policy output POLICY_WAN

interface [interface name]
service-policy output QOS_LAN
```

NAT

```
ip nat settings gatekeeper-size [value]
ip nat switchover replication http
ip nat log translations flow-export v9 udp destination [ip address] [port value] source [interface name]
ip nat translation timeout [value]
ip nat translation tcp-timeout [value]
ip nat translation udp-timeout [value]
ip nat translation dns-timeout [value]
ip nat translation icmp-timeout [value]
ip nat translation max-entries [value]
no ip nat service gatekeeper
ip nat inside source list [access-list name] pool [pool_ name] redundancy 1 mapping-id [value] vrf [vrf_name] overload
nat64 prefix stateful [prefix]
nat64 v4 pool POOL_NAT64 114.1.1.1 114.1.1.2
nat64 v6v4 list NAT64_ACL pool POOL_NAT64 overload redundancy 2 mapping-id [value]

interface [interface name]
 ip nat inside
interface [interface name]
 ip nat outside
interface [interface name]
nat64 enable
```

ZBFW

```
class-map type inspect match-all rtsp
match protocol rtsp
class-map type inspect match-any imap
 match protocol imap
match protocol imaps
match protocol imap3
class-map type inspect match-any http
match protocol http
class-map type inspect match-any CM_External_AntiSpam
match access-group name ACL_External_AntiSpam
```

```
policy-map type inspect (private)_(public)
 class type inspect rtsp
  inspect
 class type inspect imap
  inspect
 class type inspect http
  inspect
 class type inspect CM_External_AntiSpam
  inspect
  class class-default
  pass
zone security private
zone security public
zone-pair security private->public source private destination public
 service-policy type inspect (private)_(public)

interface [interface name]
 zone-member security public
interface [interface name]
 zone-member security private
```

AVC PROFILE A

```
ip access-list extended my-visibility-url_ipv4_tcp
 permit tcp any any
!
class-map match-all my-visibility-conv_ts_ipv4
 match protocol ip
!
class-map match-any my-visibility-url_app
 match protocol napster
 match protocol gotomypc
 match protocol yahoo-messenger
 match protocol tunnel-http
 match protocol baidu-movie
 match protocol flashmyspace
 match protocol directconnect
```

```
 match protocol audio-over-http
 match protocol skype
 match protocol video-over-http
 match protocol pando
 match protocol flashyahoo
 match protocol msn-messenger
 match protocol flash-video
 match protocol webthunder
 match protocol vnc-http
 match protocol activesync
 match protocol irc
 match protocol realmedia
 match protocol gmail
 match protocol google-earth
 match protocol gnutella
 match protocol rtmpt
 match protocol http
 match protocol ms-update
 match protocol rtsp
 match protocol http-alt
 match protocol share-point
 match protocol binary-over-http
 match protocol ms-sms
 match protocol megavideo

class-map match-all my-visibility-url_ipv4
 match access-group name my-visibility-url_ipv4_tcp
 match class-map my-visibility-url_app
!
class-map match-any my-visibility-app_ts
 match protocol dns
 match protocol dht

sampler my-visibility-url_ipv4
 granularity connection
 mode random 1 out-of 50
```

```
!
flow record type performance-monitor my-visibility-conv_ts_ipv4
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match application name account-on-resolution
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect ipv4 ttl
 collect interface input
 collect interface output
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
 collect services waas passthrough-reason
!
flow monitor type performance-monitor my-visibility-conv_ts_ipv4
 record my-visibility-conv_ts_ipv4
 cache entries 625000
 cache timeout synchronized 60
!
flow record type performance-monitor my-visibility-url_ipv4
 description ezPM record
 match connection id
 collect routing vrf input
 collect interface input
```

```
 collect interface output
 collect flow sampler
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect connection initiator
 collect connection new-connections
 collect application http uri statistics
 collect connection delay response to-server sum
 collect connection server counter responses
 collect connection delay response to-server histogram late
 collect connection delay network to-server sum
 collect connection delay network to-client sum
 collect connection client counter packets retransmitted
 collect connection delay network client-to-server sum
 collect connection delay application sum
 collect connection delay application max
 collect connection delay response client-to-server sum
 collect connection transaction duration sum
 collect connection transaction counter complete
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
 collect connection client ipv4 address
 collect connection client transport port
 collect connection server ipv4 address
 collect connection server transport port
 collect services waas segment
 collect services waas passthrough-reason
 collect application http host
!
flow monitor type performance-monitor my-visibility-url_ipv4
 record my-visibility-url_ipv4
 cache type normal
 cache entries 1000000
```

```
 cache timeout event transaction-end
!
flow record type performance-monitor my-visibility-app_ts_in
 description ezPM record
 match routing vrf input
 match ipv4 version
 match ipv4 protocol
 match interface input
 match flow direction
 match application name account-on-resolution
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect routing vrf output
 collect services waas passthrough-reason
!
flow monitor type performance-monitor my-visibility-app_ts_in
 record my-visibility-app_ts_in
 cache entries 1000
 cache timeout synchronized 60
!
flow record type performance-monitor my-visibility-app_ts_out
 description ezPM record
 match ipv4 version
 match ipv4 protocol
 match interface output
 match flow direction
 match application name account-on-resolution
```

```
 match routing vrf output
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect routing vrf input
 collect ipv4 dscp
 collect interface input
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect services waas passthrough-reason
!
flow monitor type performance-monitor my-visibility-app_ts_out
 record my-visibility-app_ts_out
 cache entries 1000
 cache timeout synchronized 60
!

policy-map type performance-monitor my-visibility-in
 parameter default account-on-resolution
 class my-visibility-app_ts
  flow monitor my-visibility-app_ts_in
 class my-visibility-url_ipv4
  flow monitor my-visibility-url_ipv4 sampler my-visibility-url_ipv4
  flow monitor my-visibility-conv_ts_ipv4
 class my-visibility-conv_ts_ipv4
  flow monitor my-visibility-conv_ts_ipv4
!
policy-map type performance-monitor my-visibility-out
 parameter default account-on-resolution
 class my-visibility-app_ts
  flow monitor my-visibility-app_ts_out
 class my-visibility-url_ipv4
```

```
  flow monitor my-visibility-url_ipv4 sampler my-visibility-url_ipv4
  flow monitor my-visibility-conv_ts_ipv4
 class my-visibility-conv_ts_ipv4
  flow monitor my-visibility-conv_ts_ipv4

interface TenGigabitEthernet0/2/0.60
 service-policy type performance-monitor input my-visibility-in
 service-policy type performance-monitor output my-visibility-out
```

AVC PROFILE B

```
ip access-list extended my-visibility-art_ipv4_tcp
 permit tcp any any
!
ip access-list extended my-visibility-url_ipv4_tcp
 permit tcp any any
!
ip access-list extended my-visibility-media_ipv4_udp
 permit udp any any
!
class-map match-all my-visibility-art_ipv4
 match access-group name my-visibility-art_ipv4_tcp
!
class-map match-all my-visibility-conv_ts_ipv4
 match protocol ip
!
class-map match-any my-visibility-url_app
 match protocol napster
 match protocol gotomypc
 match protocol yahoo-messenger
 match protocol tunnel-http
 match protocol baidu-movie
 match protocol flashmyspace
 match protocol directconnect
 match protocol audio-over-http
 match protocol skype
 match protocol video-over-http
```

```
 match protocol pando
 match protocol flashyahoo
 match protocol msn-messenger
 match protocol flash-video
 match protocol webthunder
 match protocol vnc-http
 match protocol activesync
 match protocol irc
 match protocol realmedia
 match protocol gmail
 match protocol google-earth
 match protocol gnutella
 match protocol rtmpt
 match protocol http
 match protocol ms-update
 match protocol rtsp
 match protocol http-alt
 match protocol share-point
 match protocol binary-over-http
 match protocol ms-sms
 match protocol megavideo
!
class-map match-all my-visibility-url_ipv4
 match access-group name my-visibility-url_ipv4_tcp
 match class-map my-visibility-url_app
!
class-map match-all my-visibility-art_url_ipv4
 match class-map my-visibility-art_ipv4
 match class-map my-visibility-url_ipv4
!
class-map match-any my-visibility-media_app
 match protocol telepresence-media
 match protocol rtp
!
class-map match-all my-visibility-media_ipv4_in
 match access-group name my-visibility-media_ipv4_udp
```

```
 match class-map my-visibility-media_app
!
class-map match-all my-visibility-media_ipv4_out
 match access-group name my-visibility-media_ipv4_udp
 match class-map my-visibility-media_app
!
class-map match-any my-visibility-app_ts
 match protocol dns
 match protocol dht
!
sampler my-visibility-url_ipv4
 granularity connection
 mode random 1 out-of 50
!
flow record type performance-monitor my-visibility-art_ipv4
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match application name account-on-resolution
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect ipv4 ttl
 collect interface input
 collect interface output
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect connection delay response to-server sum
 collect connection server counter responses
 collect connection delay response to-server histogram late
```

```
 collect connection delay network to-server sum
 collect connection delay network to-client sum
 collect connection client counter packets retransmitted
 collect connection delay network client-to-server sum
 collect connection delay application sum
 collect connection delay application max
 collect connection delay response client-to-server sum
 collect connection transaction duration sum
 collect connection transaction counter complete
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
 collect services waas passthrough-reason
!
flow monitor type performance-monitor my-visibility-art_ipv4
 record my-visibility-art_ipv4
 cache entries 2000000
 cache timeout synchronized 60
!
flow record type performance-monitor my-visibility-conv_ts_ipv4
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match application name account-on-resolution
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect ipv4 ttl
 collect interface input
 collect interface output
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

```
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
 collect services waas passthrough-reason
!
flow monitor type performance-monitor my-visibility-conv_ts_ipv4
 record my-visibility-conv_ts_ipv4
 cache entries 625000
 cache timeout synchronized 60
!
flow record type performance-monitor my-visibility-url_ipv4
 description ezPM record
 match connection id
 collect routing vrf input
 collect interface input
 collect interface output
 collect flow sampler
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect connection initiator
 collect connection new-connections
 collect application http uri statistics
 collect connection delay response to-server sum
 collect connection server counter responses
 collect connection delay response to-server histogram late
 collect connection delay network to-server sum
 collect connection delay network to-client sum
 collect connection client counter packets retransmitted
 collect connection delay network client-to-server sum
 collect connection delay application sum
 collect connection delay application max
```

```
 collect connection delay response client-to-server sum
 collect connection transaction duration sum
 collect connection transaction counter complete
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
 collect connection client ipv4 address
 collect connection client transport port
 collect connection server ipv4 address
 collect connection server transport port
 collect services waas segment
 collect services waas passthrough-reason
 collect application http host
!
flow monitor type performance-monitor my-visibility-url_ipv4
 record my-visibility-url_ipv4
 cache type normal
 cache entries 1000000
 cache timeout event transaction-end
!
flow record type performance-monitor my-visibility-media_ipv4_in
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match transport rtp ssrc
 match interface input
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect ipv4 ttl
 collect transport packets lost counter
 collect transport rtp jitter maximum
```

```
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect connection initiator
 collect connection new-connections
 collect transport rtp payload-type
 collect transport rtp jitter mean sum
 collect routing vrf output
!
flow monitor type performance-monitor my-visibility-media_ipv4_in
 record my-visibility-media_ipv4_in
 cache entries 8000
 cache timeout synchronized 60
 history size 10
!
flow record type performance-monitor my-visibility-media_ipv4_out
 description ezPM record
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match transport rtp ssrc
 match interface output
 match routing vrf output
 collect datalink source-vlan-id
 collect routing vrf input
 collect ipv4 dscp
 collect ipv4 ttl
 collect transport packets lost counter
 collect transport rtp jitter maximum
 collect interface input
 collect counter bytes long
```

```
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect connection initiator
 collect connection new-connections
 collect transport rtp payload-type
 collect transport rtp jitter mean sum
!
flow monitor type performance-monitor my-visibility-media_ipv4_out
 record my-visibility-media_ipv4_out
 cache entries 8000
 cache timeout synchronized 60
 history size 10
!
flow record type performance-monitor my-visibility-app_ts_in
 description ezPM record
 match routing vrf input
 match ipv4 version
 match ipv4 protocol
 match interface input
 match flow direction
 match application name account-on-resolution
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect routing vrf output
 collect services waas passthrough-reason
```

```
!
flow monitor type performance-monitor my-visibility-app_ts_in
 record my-visibility-app_ts_in
 cache entries 1000
 cache timeout synchronized 60
!
!
flow record type performance-monitor my-visibility-app_ts_out
 description ezPM record
 match ipv4 version
 match ipv4 protocol
 match interface output
 match flow direction
 match application name account-on-resolution
 match routing vrf output
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect routing vrf input
 collect ipv4 dscp
 collect interface input
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect services waas passthrough-reason
!
flow monitor type performance-monitor my-visibility-app_ts_out
 record my-visibility-app_ts_out
 cache entries 1000
 cache timeout synchronized 60
!
policy-map type performance-monitor my-visibility-in
 parameter default account-on-resolution
```

```
 class my-visibility-app_ts
  flow monitor my-visibility-app_ts_in
 class my-visibility-art_url_ipv4
  flow monitor my-visibility-art_ipv4
  flow monitor my-visibility-url_ipv4 sampler my-visibility-url_ipv4
 class my-visibility-art_ipv4
  flow monitor my-visibility-art_ipv4
 class my-visibility-url_ipv4
  flow monitor my-visibility-url_ipv4 sampler my-visibility-url_ipv4
  flow monitor my-visibility-conv_ts_ipv4
 class my-visibility-media_ipv4_in
  flow monitor my-visibility-media_ipv4_in
 class my-visibility-conv_ts_ipv4
  flow monitor my-visibility-conv_ts_ipv4
!
policy-map type performance-monitor my-visibility-out
 parameter default account-on-resolution
 class my-visibility-app_ts
  flow monitor my-visibility-app_ts_out
 class my-visibility-art_url_ipv4
  flow monitor my-visibility-art_ipv4
  flow monitor my-visibility-url_ipv4 sampler my-visibility-url_ipv4
 class my-visibility-art_ipv4
  flow monitor my-visibility-art_ipv4
 class my-visibility-url_ipv4
  flow monitor my-visibility-url_ipv4 sampler my-visibility-url_ipv4
  flow monitor my-visibility-conv_ts_ipv4
 class my-visibility-media_ipv4_out
  flow monitor my-visibility-media_ipv4_out
 class my-visibility-conv_ts_ipv4
  flow monitor my-visibility-conv_ts_ipv4
!
interface TenGigabitEthernet0/2/0.60
 service-policy type performance-monitor input my-visibility-in
 service-policy type performance-monitor output my-visibility-out
```

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.