Application-Aware Path Selection in SRv6 Networks

Path Selection Beyond DSCP Marking on Cisco 8000 Series Secure Routers

July 2026

Executive Summary

Enterprise and service-provider WANs increasingly adopt Segment Routing over IPv6 (SRv6) as a programmable underlay. Meanwhile, application traffic grows more encrypted and dynamic, and AI workloads increasingly dominate this traffic. These AI workloads do not map cleanly to traditional quality of service (QoS) markings.

Routing and steering traffic solely on Differentiated Services Code Point (DSCP) values is a coarse, trust-dependent approach. Application-aware routing identifies traffic at Layer 7 and binds it to transport policies that enforce distinct path service-level agreements (SLAs). Cisco Network-Based Application Recognition (NBAR2) performs this identification on Cisco IOS XE.

The application-aware routing model follows this sequence:

1. NBAR classifies the traffic.
2. Enhanced Policy-Based Routing (ePBR) assigns a Forward Class.
3. A Per-Flow Policy (PFP) applies flow-specific handling.
4. A Per-Destination Policy (PDP) applies destination-specific handling.
5. SRv6 steers the traffic along a path that meets the SLA constraints.

This white paper explains why the application-aware model complements DSCP-only routing. It also describes how NBAR

- recognizes applications on IOS XE
- adds support for AI protocols through recent NBAR protocol-pack updates
- enables you to architect SRv6 PDP and PFP policies that deliver differentiated SLAs for each application.

Finally, this white paper describes how Cisco ThousandEyes closes the assurance loop by correlating application and path visibility.

Introduction

The problem

Wide-area network (WAN) operators traditionally rely on two mechanisms:

- Quality of service (QoS) marking, which uses the Differentiated Services Code Point (DSCP), IP Precedence, or Multiprotocol Label Switching (MPLS) Experimental (EXP) bits.
- Destination-based routing, which uses the prefix, virtual private network (VPN), or Border Gateway Protocol (BGP) next-hop.

Neither mechanism answers two key questions:

- Which application does this flow represent?
- What transport service-level agreement (SLA) does the flow require?

The DSCP indicates how a packet claims to be treated, but it does not identify the application that generated the flow. In modern environments, including encrypted software-as-a-service (SaaS), Quick UDP Internet Connections (QUIC) or Hypertext Transfer Protocol version 3 (HTTP/3), artificial intelligence (AI) application programming interfaces (APIs), and shadow IT, the DSCP alone cannot support intent-based path selection.

Application-aware routing solution

Application-aware routing identifies applications deeply at the network edge and steers flows onto paths that meet application-specific service-level agreements (SLAs). On the Cisco 8000 Series Secure Routers:

Layer	Technology	Role
Application identification	NBAR2 (DPI + signatures)	Classify flows by application/protocol
Ingress marking	MQC + ePBR	Map applications to Forward Classes (FC 0–7)
Per-flow steering	SRv6-TE PFP	Map FC → color (SLA intent)
Per-destination path	SRv6-TE PDP	Compute/steer explicit or dynamic SRv6 paths
SLA enforcement	Flex-Algo, PCE, Performance Measurement	Delay-optimized, affinity-constrained paths
Application identification	NBAR2 (DPI + signatures)	Classify flows by application/protocol
Assurance and validation	Cisco ThousandEyes (Traffic Insights + synthetics)	Correlate NBAR app-ID with path SLA outcomes

Limitations of DSCP-based routing

DSCP is an assertion, not an identity

The DSCP is a 6-bit field that reflects a marking decision. The network cannot independently verify that traffic marked Expedited Forwarding (EF) is real-time collaboration traffic. The network also cannot verify that a bulk backup was not marked EF.

Scenario	DSCP limitation
Default enterprise endpoints	Most traffic arrives as DSCP 0 (Best Effort)
Encrypted SaaS (HTTPS, QUIC)	Port 443 carries thousands of distinct applications
Guest / IoT / unmanaged devices	No consistent marking policy
Cloud egress	Provider rewrites or strips markings at boundary
AI/LLM API traffic	Typically, HTTPS; indistinguishable from generic web at L3/L4

DSCP does not survive semantic boundaries

- Webex meeting media vs. Webex AI transcription
- GitHub Copilot vs. generic GitHub HTTPS
- OpenAI API calls vs. browsing openai.com

Operational fragility

DSCP-based steering requires end-to-end trust across the LAN, the WAN edge, the carrier, and the cloud. Network-Based Application Recognition (NBAR) operates at the first trusted enforcement point: the Secure Router.

Benefits of application-aware routing

True application identity

Network-Based Application Recognition (NBAR2) classifies more than 1,400 applications without client cooperation. To classify these applications, NBAR2 inspects:

- payloads
- flow state
- Domain Name System (DNS) transactions
- Transport Layer Security (TLS) Server Name Indication (SNI)
- Hypertext Transfer Protocol (HTTP) patterns, and
- proprietary signatures.

First-packet and early-flow classification

Network-Based Application Recognition (NBAR) uses these classification techniques:

- **Domain Name System (DNS)-based learning**: NBAR correlates DNS responses with subsequent flows.
- Socket cache: NBAR remembers recently classified server endpoints.
- **Stateful multipacket inspection**: NBAR tracks dynamic ports, such as those used by Session Initiation Protocol (SIP) and File Transfer Protocol (FTP).
- **Deep packet inspection (DPI)**: NBAR performs regular expression matching and field extraction on Hypertext Transfer Protocol (HTTP), Real-time Transport Protocol (RTP), and Citrix traffic.
- **Encrypted traffic analytics**: NBAR matches the Server Name Indication (SNI) and Common Name (CN) without decrypting the traffic.

The SNI is a Transport Layer Security (TLS) extension that the client sends in the ClientHello message. The SNI carries the target hostname in cleartext, such as api.openai.com, so that the server can select the correct certificate before the session is encrypted. NBAR reads the SNI to identify the intended destination application without decrypting the traffic.

The CN is an identity field in the server's X.509 TLS certificate. Servers often use the CN alongside Subject Alternative Name (SAN) entries. NBAR can match the CN or SAN from the server's certificate response when it classifies encrypted flows. This match provides a second signal when the SNI is absent, or it validates the classification.

Together, SNI and CN matching enable NBAR to distinguish applications that share port 443 and encrypted payloads, such as OpenAI API traffic and generic HTTPS browsing.

This capability enables you to enforce policy before enough packets arrive to infer intent from the DSCP alone.

Granular SLA binding

Application (NBAR)	SLA intent	SRv6 color	Path constraint
webex-media	Loss <1%, latency <150ms, jitter <30ms	102	Min-delay, voice-video slice
open-ai / anthropic-ai	Loss <1%, latency <300ms	103	Low-loss path
ftp / ms-update	Latency <500ms, loss <5%	101	High-bandwidth, cost-optimized

Application (NBAR)	SLA intent	SRv6 color	Path constraint
youtube / netflix	Best effort	100	Default IGP / best-cost

NBAR and DSCP: complementary classification for SRv6 steering

NBAR and the DSCP address different parts of the classification problem. Used together, they strengthen Segment Routing over IPv6 (SRv6) Per-Flow Policy (PFP) steering. The same PFP and Per-Destination Policy (PDP) machinery applies whether you set the Forward Class from NBAR, the DSCP, or both.

Aspect	DSCP-based PFP	NBAR-based PFP	Combined (recommended)
Classification input	match dscp ef	match protocol webex-media	match protocol + match dscp
Trust model	Trusts endpoint marking	Independent DPI at edge	NBAR validates; DSCP reinforces QoS
Encrypted SaaS	All appear as DSCP 0	Distinguished by SNI/signature	NBAR identifies; DSCP queues
AI workloads	Invisible (HTTPS)	open-ai, anthropic-ai, etc.	NBAR steers; DSCP queues

Protocol-pack agility

Cisco ships NBAR signatures in Protocol Packs that update independently of Cisco IOS XE images.

Closed-loop visibility

Application-aware routing and Segment Routing over IPv6 (SRv6) steering require you to validate that the policies work as intended. Cisco ThousandEyes on the Secure Router provides this assurance layer. Refer to Cisco ThousandEyes in the application-aware SRv6 solution for a detailed treatment of ThousandEyes in the overall solution.

How NBAR works on Cisco IOS XE

NBAR2 architecture

- Protocol Pack – compiled signature library
- Flow table – stateful per-flow context
- Classification pipeline – DNS-learned → ports → multi-packet → static → encrypted
- MQC integration – match protocol <name> in class-maps

Classification methods

Method	Description	Example
Static port	Well-known TCP/UDP ports	DNS (53), NTP (123)
Stateful inspection	Track negotiations across packets	SIP, FTP, RTSP
Deep packet inspection	Parse headers and payload fields	HTTP URL, RTP payload type
DNS-based learning	Map DNS answer → flow 5-tuple	SaaS first-packet ID
TLS SNI / cert CN	Classify encrypted flows	api.openai.com
Custom protocols	Operator-defined ip nbar custom	Internal app on port 8443
Attribute matching	Group by category, business-relevance	match protocol attribute traffic-class

Procedure 1. Implementation on Cisco 8000 series secure routers

Step 1. Enable NBAR protocol discovery:

```
interface GigabitEthernet0/0/0
 ip nbar protocol-discovery
```

Step 2. Load the latest protocol pack:

```
ip nbar protocol-pack bootflash:PP78-0-0.ppack
show ip nbar protocol-pack active
Router#sh ip nbar protocol-id | i open-ai|anthropic|cursor|webex-ai
```

Note: Protocol Pack upgrades are included in the Routing Advantage license. Refer to the NBAR2 Protocol Pack Library: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Step 3. Define application class-maps (NBAR + DSCP)

NBAR provides application identity for SRv6 path selection; DSCP complements classification for flows already marked by trusted LAN endpoints. The examples use both match protocol and match dscp to illustrate this complementary model.

```
class-map match-all FC-VOICE-VIDEO
 match protocol webex-media
 match dscp ef
```

```
class-map match-all FC-CRITICAL-DATA
 match protocol open-ai
 match protocol anthropic-ai
 match dscp cs6

class-map match-all FC-BULK-DATA
 match protocol ftp
 match protocol ms-update
 match dscp af11

class-map match-all FC-BEST-EFFORT
 match protocol youtube
 match protocol netflix
 match dscp default
```

Step 4. Apply QoS policy

```
policy-map APP-QOS
 class FC-VOICE-VIDEO
  priority percent 30
  set dscp ef
 class FC-CRITICAL-DATA
  bandwidth percent 20
  set dscp cs6
 class FC-BULK-DATA
  bandwidth percent 10
  set dscp af11
 class class-default
  fair-queue
```

Step 5. Verification

```
show policy-map interface GigabitEthernet0/0/0
show ip nbar protocol-discovery stats
```

NBAR updates for AI protocol recognition

Protocol pack 75.0.0

New protocol	Description
open-ai	OpenAI API and services
github-copilot	GitHub Copilot AI assistant
google-ai	Google Gemini and AI services
azure-ai	Microsoft Azure AI services
amazon-sagemaker	AWS SageMaker ML platform
meta	Meta AI services

Protocol pack 76.0.0

New protocol	Description
anthropic-ai	Anthropic Claude models and API
amazon-bedrock	AWS managed foundation-model service
amazon-q	Amazon Q AI assistant
deepseek	DeepSeek AI models
perplexity-ai	Perplexity AI search/assistant
x-ai	xAI (Grok) services

Protocol pack 77.0.0

New protocol	Description
huggingface	Hugging Face model hub and inference

Protocol pack 78.0.0 (April 2026)

New protocol	Description
cursor	Cursor AI-assisted IDE
webex-ai	Webex AI features (transcription, summaries)

Why AI-specific signatures matter

- **Inference APIs (open-ai, anthropic-ai)** – latency-sensitive; low-delay SRv6 paths
- **Model training (amazon-sagemaker, huggingface)** – bulk, throughput-oriented
- **Embedded AI (webex-ai)** – split SLA from webex-media real-time flows
- **Developer tools (cursor, github-copilot)** – distinct security/policy treatment

Leveraging NBAR in SRv6: PDP/PFP SR-TE policies

Cisco IOS XE maps NBAR application signatures to SRv6 transport policies through Forward Class and color.

SRv6 policy model on IOS XE

Application (NBAR)	NBAR class-map	ePBR FC	PFP color	PDP	Path constraint
webex-media	FC-VOICE-VIDEO	2	102	PDP-VOICE-VIDEO	Min-delay, voice-video slice
open-ai / anthropic-ai	FC-CRITICAL-DATA	3	103	PDP-CRITICAL-DATA	Low-loss / min-delay
ftp / ms-update	FC-BULK-DATA	1	101	PDP-BULK-DATA	High-bandwidth, cost-optimized
youtube / netflix	FC-BEST-EFFORT	0	100	PDP-BEST-EFFORT	Default IGP / best-cost

Reference configuration

PDPs – One per SLA plane

```
segment-routing traffic-eng
 policy PDP-VOICE-VIDEO
  color 102 end-point 2001:db8:2::1
  candidate-paths
   preference 100
    constraints
     segments dataplane srv6
     affinity include-all name voice-video
    dynamic
     metric type delay
  performance-measurement
   delay-measurement
    liveness-detection invalidation-action down
```

PFP – Forward class to color mapping

```
segment-routing traffic-eng
 policy PFP-SLA-STEERING
  color 1000 end-point 2001:db8:2::1
  candidate-paths
   preference 100
    per-flow
     forward-class 0 color 100
     forward-class 1 color 101
     forward-class 2 color 102
     forward-class 3 color 103
```

End-to-end configuration – reference applications

Complete chain for all four reference applications: NBAR + DSCP classification, QoS marking, ePBR Forward class, SRv6 PFP, and PDP.

```
! Step A — NBAR + DSCP class-maps
class-map match-all FC-VOICE-VIDEO
 match protocol webex-media
 match dscp ef
class-map match-all FC-CRITICAL-DATA
 match protocol open-ai
 match protocol anthropic-ai
 match dscp cs6
class-map match-all FC-BULK-DATA
 match protocol ftp
 match protocol ms-update
 match dscp af11
class-map match-all FC-BEST-EFFORT
 match protocol youtube
 match protocol netflix
 match dscp default

! Step B — ePBR
policy-map type epbr SRv6-APP-STEERING
 class FC-VOICE-VIDEO
  set forward-class 2
 class FC-CRITICAL-DATA
  set forward-class 3
 class FC-BULK-DATA
  set forward-class 1
 class FC-BEST-EFFORT
  set forward-class 0

! Step C — interface
interface GigabitEthernet0/0/0.100
 service-policy output APP-QOS
 service-policy type epbr input SRv6-APP-STEERING
```

ApplicationClass-map FC Color PDP QoS / DSCP

Application	Class-map	FC	Color	PDP	QoS / DSCP
webex-media	FC-VOICE-VIDEO	2	102	PDP-VOICE-VIDEO	priority, EF (46)

Application	Class-map	FC	Color	PDP	QoS / DSCP
open-ai / anthropic-ai	FC-CRITICAL-DATA	3	103	PDP-CRITICAL-DATA	bandwidth 20%, CS6
ftp / ms-update	FC-BULK-DATA	1	101	PDP-BULK-DATA	bandwidth 10%, AF11
youtube / netflix	FC-BEST-EFFORT	0	100	PDP-BEST-EFFORT	bandwidth 5%, default

SLA validation

Cisco IOS XE 17.18 supports Segment Routing over IPv6 (SRv6) performance measurement on Per-Destination Policies (PDPs). Combined with Cisco ThousandEyes Traffic Insights and synthetic tests, this support enables operators to validate classification, Forward Class (FC) mapping, and path service-level agreement (SLA) delivery. Refer to Cisco ThousandEyes in the application-aware SRv6 solution for more information.

Cisco ThousandEyes in the application-aware SRv6 solution

NBAR and Segment Routing over IPv6 (SRv6) Per-Destination Policy (PDP) and Per-Flow Policy (PFP) answer what the traffic is and where it should go. Cisco ThousandEyes answers whether the application actually performs as expected on the chosen path. On the Cisco 8000 Series Secure Routers, ThousandEyes embeds through the Cisco Application Framework (CAF), which turns each edge router into an observability node.

Role in the end-to-end architecture

Plane	Function	ThousandEyes contribution
Steering	NBAR + SRv6 TE	–
Validation	Confirm SLA delivery	Synthetic probes + SRv6 PM correlation
Troubleshooting	Root-cause analysis	Flow data + path viz at time of incident
Optimization	Policy tuning	QoS audit; bandwidth bottleneck discovery

Traffic insights and NBAR integration

Cisco ThousandEyes Traffic Insights collects Flexible NetFlow and IP Flow Information Export (IPFIX) records from the Secure Router. Traffic Insights then enriches these records with Network-Based Application Recognition (NBAR) application classification, such as open-ai, webex-media, and cursor.

A Traffic Monitor on the LAN and WAN interfaces exports flow records to the ThousandEyes Enterprise Agent, which runs as a Docker container on the Cisco Application Framework (CAF). The Enterprise Agent forwards encrypted data to the cloud, where ThousandEyes correlates the data with synthetic test results.

Synthetic tests detect a problem, and flow data shows which application traffic was on the wire at that moment. Together, they close the loop between policy intent and observed behavior. The policy intent follows this path: NBAR classifies the traffic, maps it to a Forward Class (FC), and assigns the SRv6 color.

Synthetic probing and SLA validation

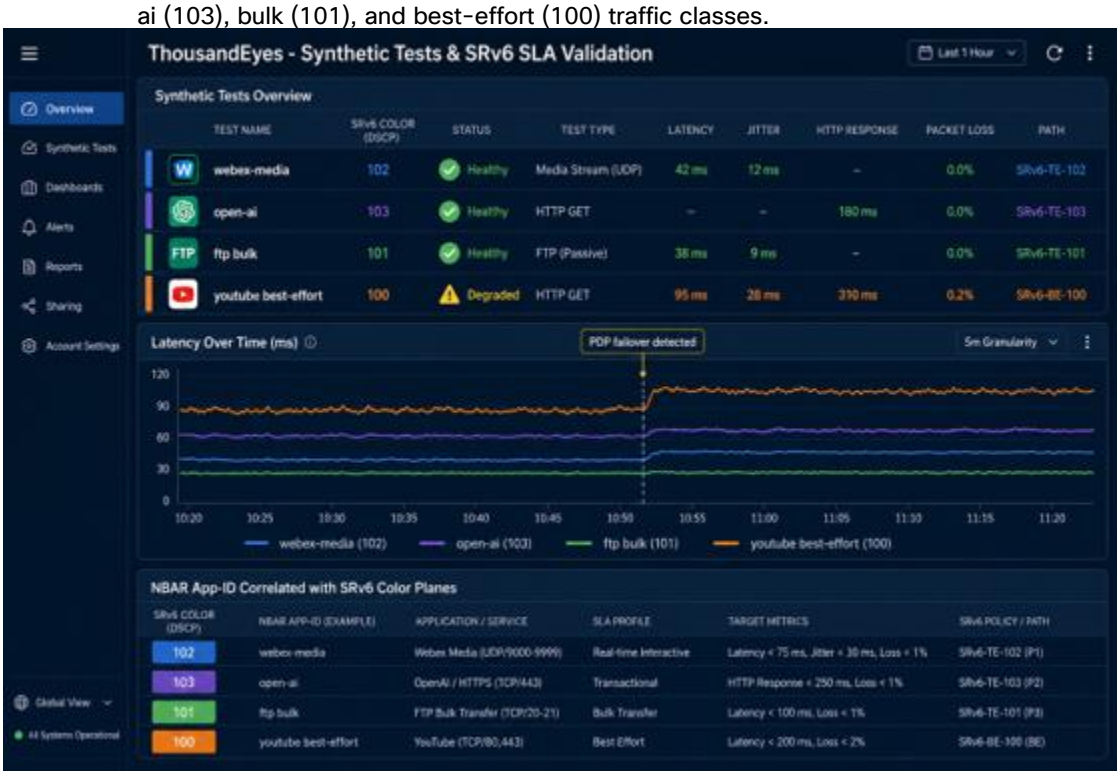
Cisco ThousandEyes Enterprise Agents on the Secure Routers run active synthetic tests to validate Segment Routing over IPv6 (SRv6) service-level agreement (SLA) commitments independently of router-local performance measurement. These tests include:

- network latency, loss, and jitter tests
- Hypertext Transfer Protocol (HTTP) response time tests
- Real-time Transport Protocol (RTP) and Mean Opinion Score (MOS) tests for voice and video, and
- agent-to-agent path tests.

SRv6 / NBAR policy intent	ThousandEyes validation
webex-media → color 102 (min-delay)	RTP stream test; jitter <30 ms threshold
open-ai / anthropic-ai → color 103	HTTP test to API endpoint; response time SLA
ftp / ms-update → color 101 (bulk)	Throughput and loss within bulk SLA
youtube / netflix → color 100	Baseline latency; no premium path expected

SRv6 / NBAR policy intent	ThousandEyes validation
PFP FC mapping correct	Traffic Insights Sankey: app volume by FC/color
PDP failover on liveness-down	Synthetic test detects path change; TE timeline

Table 1. Illustrative ThousandEyes view: synthetic probes validate SRv6 color-plane SLAs for Webex-media (102), open-ai (103), bulk (101), and best-effort (100) traffic classes.



Deployment models on secure routers

The Cisco ThousandEyes Virtual Appliance (TEVA) is a software-based Enterprise Agent that you deploy as a virtual machine at a hub site or data center. TEVA aggregates NetFlow and IP Flow Information Export (IPFIX) records from multiple Cisco 8000 Series Secure Routers at branch sites, and it forwards the enriched flow data to the Cisco ThousandEyes cloud.

TEVA supports a higher flow scale than embedded branch agents. A 32-GB, 16-core appliance supports up to 200,000 flows per second. This scale makes TEVA well suited for regional aggregation, while branch routers retain embedded agents for local synthetic testing.

Model	Description	Best for
Embedded (CAF)	Enterprise Agent on each Secure Router	Branch SRv6 head-end
Centralized (TEVA)	Flows to hub TEVA (200k flows/sec)	Regional aggregation

Operational use cases

- Validate NBAR + SRv6 steering — confirm open-ai flows use the intended color plane
- Troubleshoot SLA breach — Path Visualization isolates underlay vs. ISP vs. overlay

- QoS and policy audit — compare NBAR app mix against queue and FC distribution
- SD-WAN + SRv6 correlation — WAN Insights validates overlay and underlay together

Integration summary

The Cisco ThousandEyes Virtual Appliance (TEVA) is a software-based Enterprise Agent that you deploy as a virtual machine at a hub site or data center. TEVA aggregates NetFlow and IP Flow Information Export (IPFIX) records from multiple Cisco 8000 Series Secure Routers at branch sites, and it forwards the enriched flow data to the Cisco ThousandEyes cloud.

TEVA supports a higher flow scale than embedded branch agents. A 32-GB, 16-core appliance supports up to 200,000 flows per second. This scale makes TEVA well suited for regional aggregation, while branch routers retain embedded agents for local synthetic testing.

Design recommendations

- Classify at the trust boundary — apply NBAR + ePBR on LAN-facing interfaces.
- Separate overlay AAR from underlay SRv6 steering.
- Keep Protocol Packs current for AI application signatures.
- Use PDP performance measurement on latency-sensitive planes.
- Use NBAR and DSCP complementarily — NBAR for SRv6 steering; DSCP for downstream QoS queuing.
- Plan scale: ~200 PFP, ~1000 PDP per Secure Router platform.
- Deploy ThousandEyes Traffic Insights on SRv6 head-ends — export NBAR-enriched NetFlow and correlate with synthetic SLA tests.

Conclusion

DSCP-based routing answers one question: How should the network queue this packet?

Application-aware routing answers two questions: What application is this, and which network path meets its service-level agreement (SLA)?

On the Cisco 8000 Series Secure Routers, Network-Based Application Recognition (NBAR2) chains to Enhanced Policy-Based Routing (ePBR) Forward Classes, Segment Routing over IPv6 (SRv6) Per-Flow Policies (PFPs), and Per-Destination Policies (PDPs) that use delay and affinity constraints. NBAR2 supports AI protocols through Protocol Packs 75 through 78. Cisco ThousandEyes validates that the steering delivers the intended application experience. As a result, you can engineer an intent-based WAN without depending on endpoint markings.

References

- Cisco QoS Configuration Guide — Classifying Network Traffic Using NBAR (IOS XE 17.x)
- Cisco QoS Configuration Guide — Configuring NBAR Using MQC
- NBAR2 Protocol Pack Library — https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html
- Protocol Pack 75.0.0 / 76.0.0 / 77.0.0 / 78.0.0 Release Notes
- Segment Routing over IPv6 — IOS XE 17.x Configuration Guide
- Cisco 8000 Series Secure Routers — ThousandEyes Traffic Insights White Paper
- Cisco Live BRKENT-2520 — Segment Routing Innovations
- Cisco Live BRKXAR-2027 — Cisco 8000 Series Secure Router

This document is intended for network architects and engineers planning application-aware SRv6 deployments on Cisco 8000 Series Secure Routers. Configuration examples are illustrative; validate against your IOS XE release notes and platform scale limits.