Cisco Secure Access Multi-Region Redundancy

Design Guide

February 2026

Contents

In modern distributed enterprise environments, maintaining continuous and reliable connectivity across geographically dispersed sites is a business-critical requirement. Cisco Secure Access provides a robust, secure, and scalable network architecture, however, localized regional outages can still impact service availability.

To mitigate this risk, Multi-Region Backhaul (MRB) offers a strategic approach to multi-region redundancy. By enabling seamless routing and failover between multiple Secure Access regions, MRB allows organizations to connect their BGP fabric to the cloud and advertise identical network prefixes across different geographic points of presence. This ensures that if a specific region becomes unavailable, traffic is dynamically and predictably rerouted to an alternate region, maintaining uninterrupted access to critical applications.

Scope

In Scope

- Regional Redundancy: Utilizing MRB to maintain availability during regional service disruptions.
- Use Cases: Implementation details for Remote Access (VPNaaS), Secure Internet Access (SIA), and Site-to-Site (S2S) connectivity.

Out of Scope

- Data Center Interconnect (DCI) link integration.
- Equal-Cost Multi-Path (ECMP) routing with MRB.
- High Availability (HA) configurations involving multiple CPE devices.
- BGP route redistribution or injection into the local LAN/IGP.
- Configuration on Non-IOS-XE Platforms

Introduction to Multi-Region Backhaul

What is MRB?

Multi-Region Backhaul is a routing feature within Cisco Secure Access. It enables customers to control and optimize traffic flows when advertising the same network prefixes to Secure Access Data Centers (DCs) across different geographic regions. MRB is enabled within Network Tunnel Groups (NTG) in the Secure Access dashboard and relies on BGP to communicate path priority. Its primary objective is to ensure path symmetry, preventing traffic drops caused by stateful security inspections.

Why is MRB Needed?

When a customer site advertises the same route to multiple Secure Access regions, that resource becomes reachable via multiple cloud paths. Because Secure Access DCs are stateful, they must see both sides of a conversation to permit traffic.

- Asymmetric Routing: If a request leaves through Region A but the return traffic attempts to enter through Region B, the security stack in Region B (having no record of the initial connection) will drop the packet.
- Single Region vs. Multi-Region: Within a single region, symmetry is easily managed between the primary and secondary DCs. Across multiple regions, the number of potential paths increases, making manual path control via MRB essential.

How Does MRB Work?

When MRB is enabled on an NTG, Secure Access injects specific BGP attributes into the routes it advertises to the CPE:

- BGP Community String (32644:X): The value of X represents the relative proximity of the Secure Access region to the destination resource. A lower value indicates a "closer" or more preferred path. X is always an even number.
- Multi-Exit Discriminator (MED): This value distinguishes between the Primary (MED 0) and Secondary (MED 1) data centers within a specific region.

By evaluating these tags, the customer's CPE can be configured to prefer the path with the lowest X value, ensuring that traffic always returns through the most direct and symmetric path.

Consider Site A connected to Region A and Region B, while Site B is only connected to Region B. Both sites advertise their local routes. Without MRB, Secure Access advertises Site B's prefix to Site A through both regions without any priority tags.

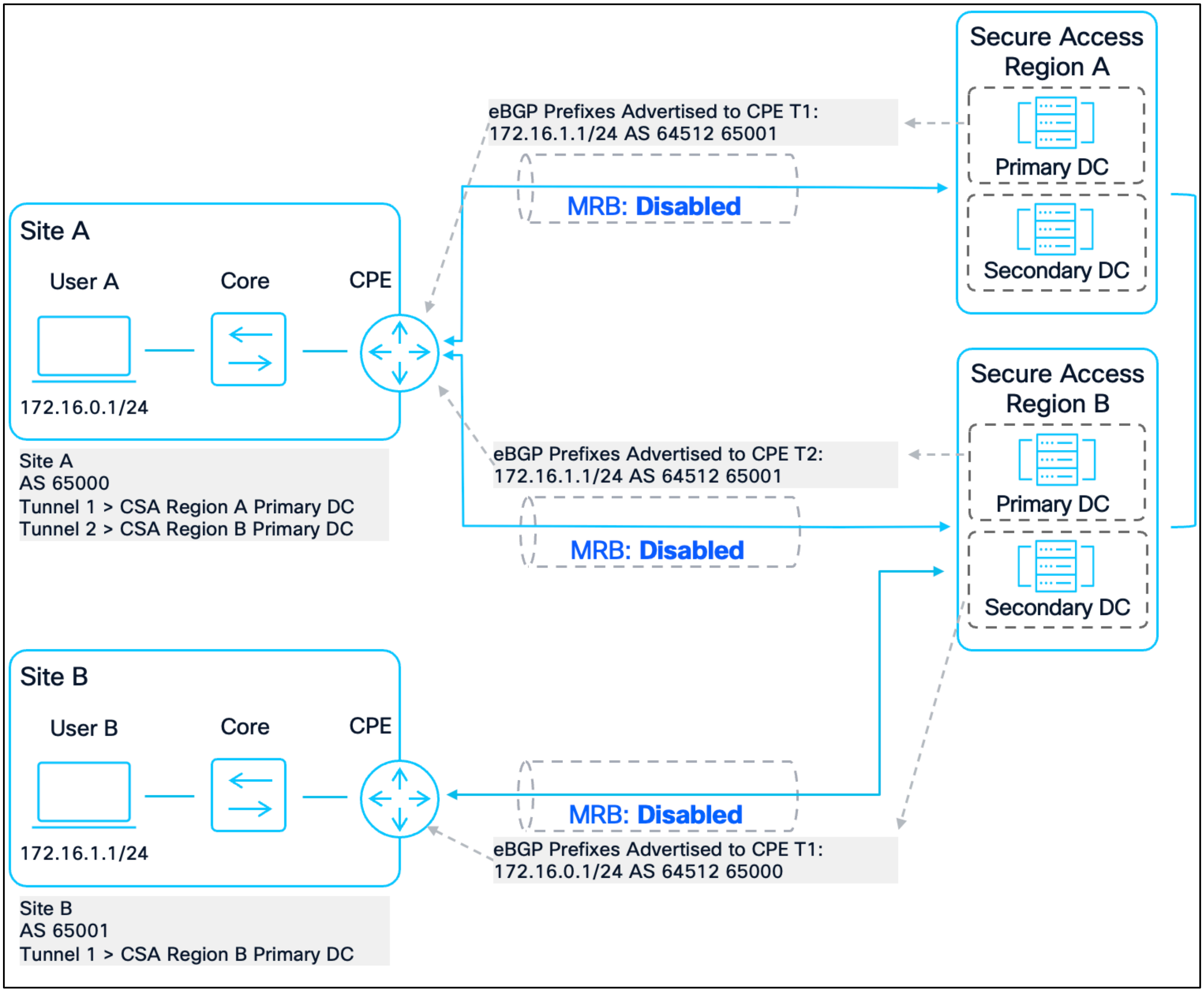

Secure Access
Region A
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
172.16.1.1/24 AS 64512 65001
MRB: Disabled
Site A
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region B Primary DC
Secure Access
Region B
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T2:
172.16.1.1/24 AS 64512 65001
MRB: Disabled
Site B
User B
Core
CPE
172.16.1.1/24
MRB: Disabled
eBGP Prefixes Advertised to CPE T1:
172.16.0.1/24 AS 64512 65000
Site B
AS 65001
Tunnel 1 > CSA Region B Primary DC

Figure 1.
MRB Disabled Scenario

User B (172.16.1.1) at Site B attempts to form a peer-to-peer connection with User A at Site A (172.16.0.1). Secure Access Region B forwards that traffic to Site A and it reaches User A.

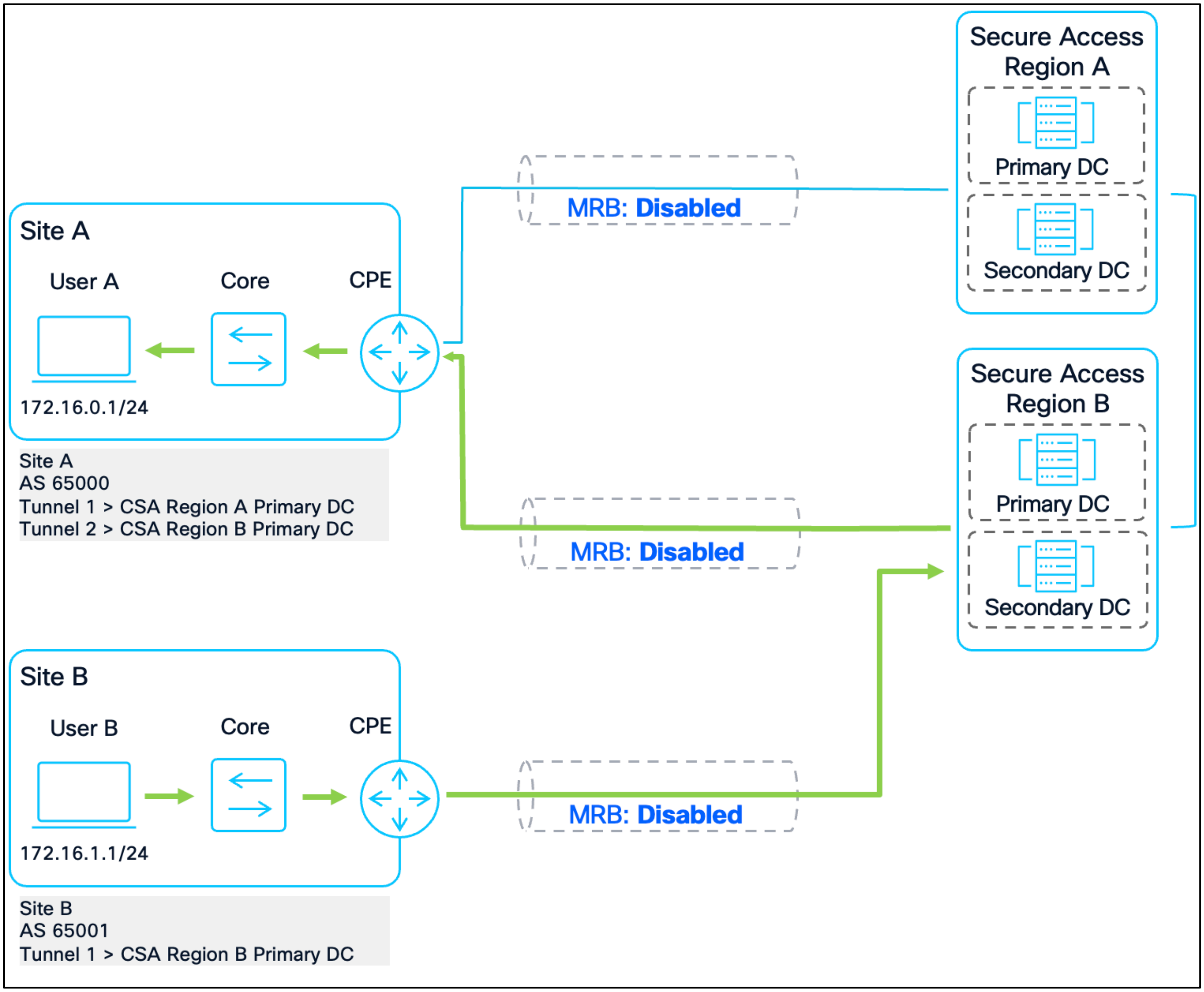


Figure 2.
MRB Disabled User B to User A Routing Logic for Initial Packet

User A responds, but the network's internal routing logic chooses Region A. Because Region A has no state information for this session, it drops the packet.

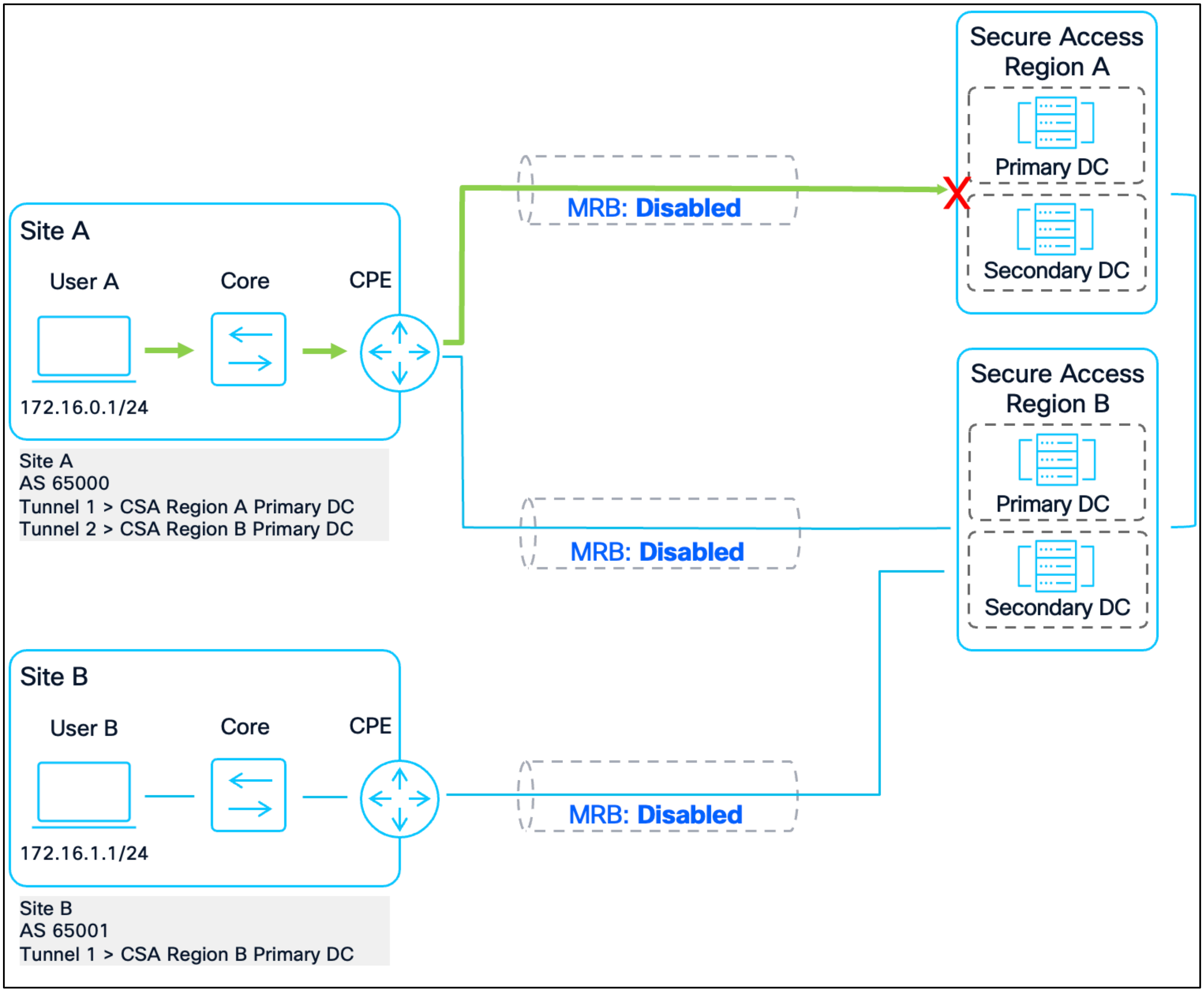


Figure 3.
MRB Disabled User A to User B Routing Logic for Response

With MRB enabled, Secure Access provides the necessary context. This time, Site A is connected to Secure Access Region A and Secure Access Region B using NTGs with MRB **enabled**. Site B has a single connection to Secure Access Region B. MRB is not enabled for Site B's NTG because the routes Site B advertises to Secure Access are only advertised to Region B. Both sites continue to advertise their routes to the connected Secure Access region so that resources at those sites are accessible by the other site. Secure Access advertises Site B's prefixes to Site A through both Region A and Region B.

- Region A tags the prefix with 32644:2 (resource is in the next closest region).
- Region B tags the prefix with 32644:0 (resource is local).

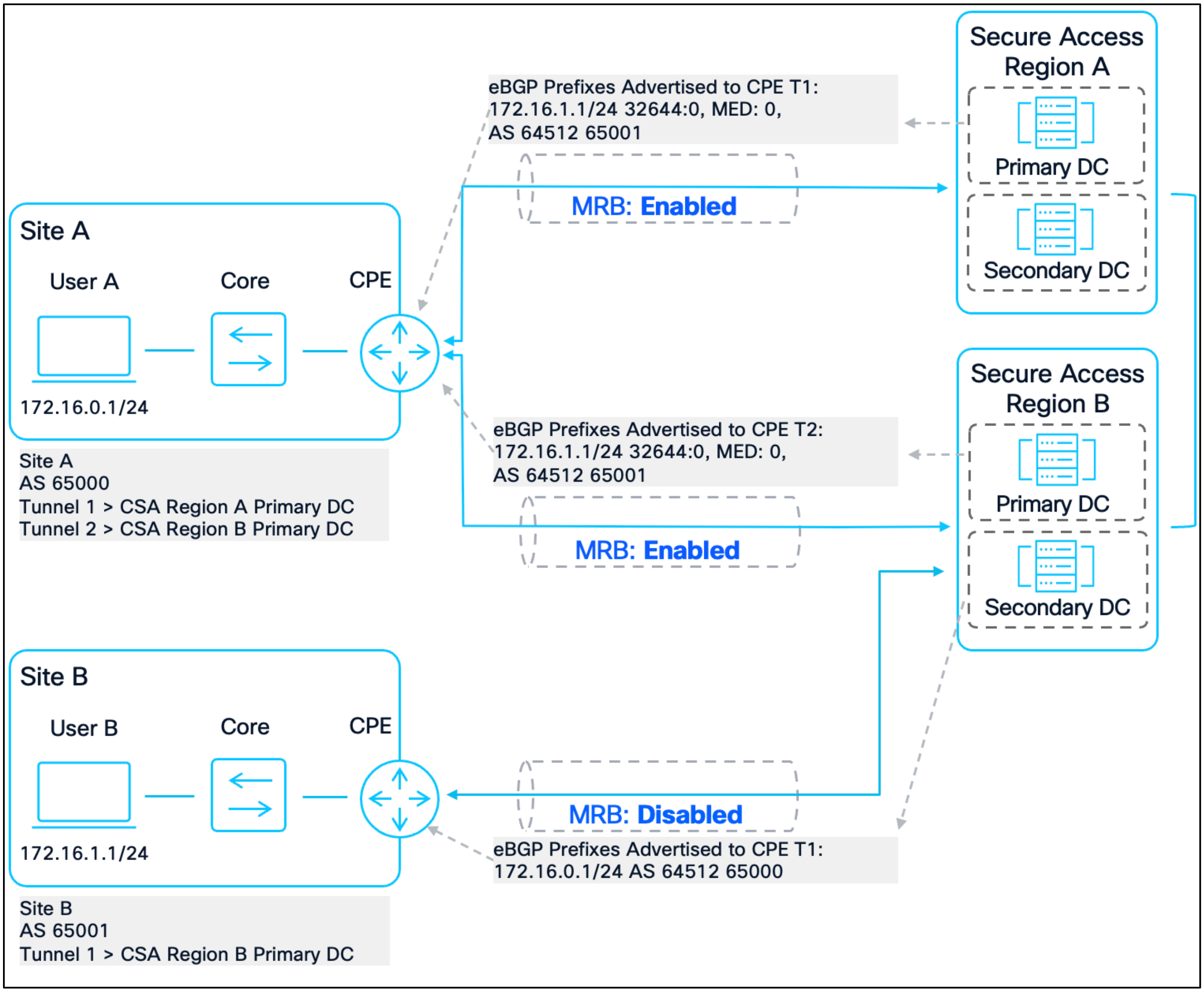

Secure Access
Region A
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
172.16.1.1/24 32644:0, MED: 0,
AS 64512 65001
MRB: Enabled
Site A
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region B Primary DC
Secure Access
Region B
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T2:
172.16.1.1/24 32644:0, MED: 0,
AS 64512 65001
MRB: Enabled
Site B
User B
Core
CPE
172.16.1.1/24
MRB: Disabled
eBGP Prefixes Advertised to CPE T1:
172.16.0.1/24 AS 64512 65000
Site B
AS 65001
Tunnel 1 > CSA Region B Primary DC

Figure 4.
MRB Enabled Scenario

User B (172.16.1.1) at Site B attempts to form a peer-to-peer connection with User A at Site A (172.16.0.1). Like in the previous example, Secure Access Region B forwards that traffic to Site A and it reaches User A. User A responds to the initial packet. The network prefers the route with the lowest X value (32644:0) and uses the community strings to route the traffic to Secure Access Region B ensuring symmetrical routing. Region B has knowledge of this connection and forwards the return packet back to Site B.

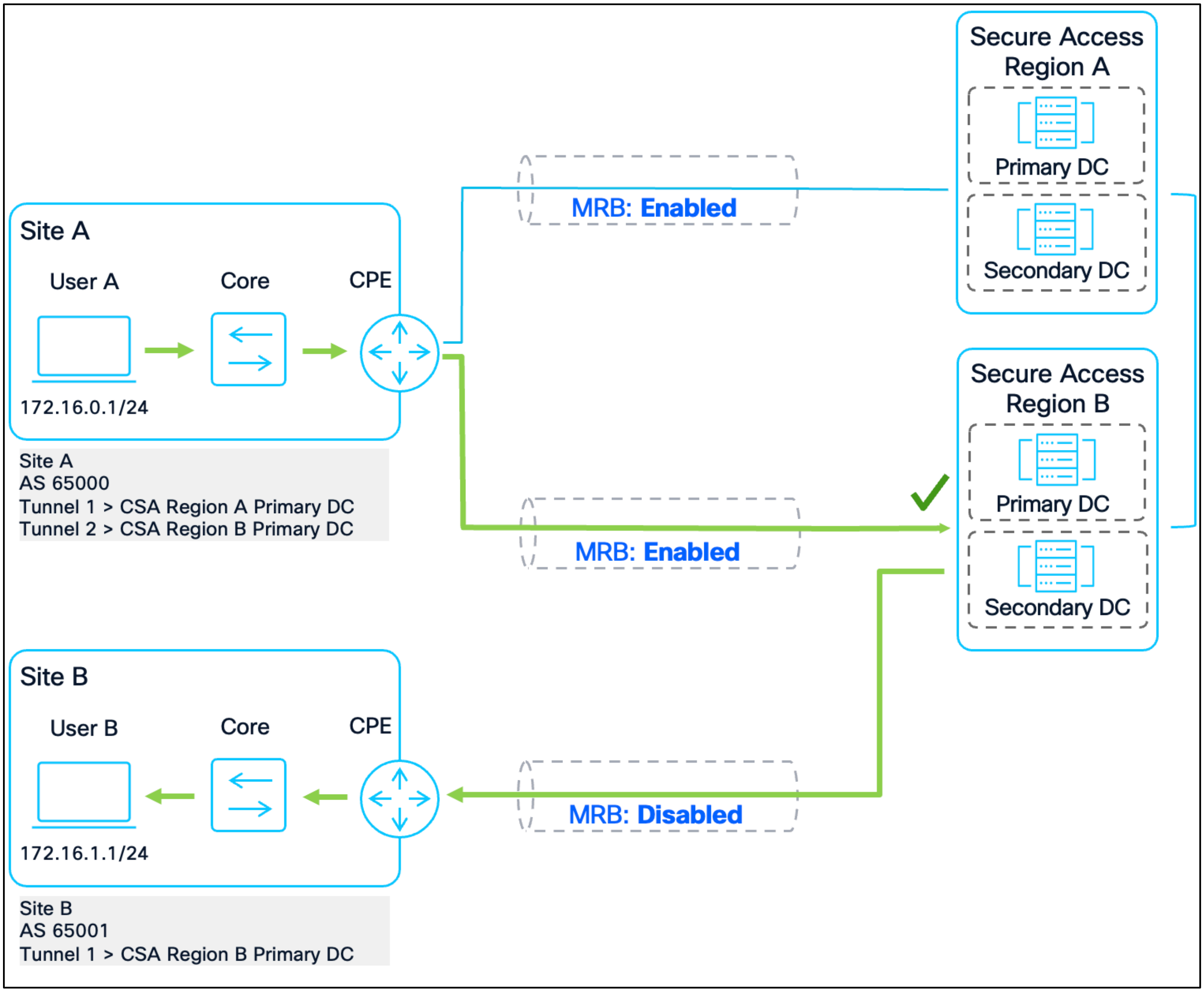


Figure 5.
MRB Enabled User B to User A Routing Logic

Additional Considerations

Understanding Non-Sequential Community Values

The proximity value (X) in the community string 32644:X does not simply count the customer's active connections. Instead, it reflects the global topology of the Secure Access network.

For example, if a customer has a site in the US Pacific Northwest and another in US Virginia:

- When the Virginia region advertises the Pacific Northwest routes, it may use 32644:10 instead of :2.
- This is because Secure Access calculates proximity based on its entire global footprint. From Virginia's perspective, there may be five other regions (e.g., US Ohio, US Central, Mexico, etc.) that are geographically closer than the Pacific Northwest.
- Therefore, 32644:10 indicates that the Pacific Northwest is the 6th closest region globally. **These values may change as Cisco adds more data centers to the Secure Access global fabric.**

Internal Backhaul Forwarding

If traffic enters a Secure Access region that does not have a direct IPsec tunnel to the destination site, the fabric will automatically forward that traffic over its internal high-speed backhaul to the nearest region that does have a direct connection.

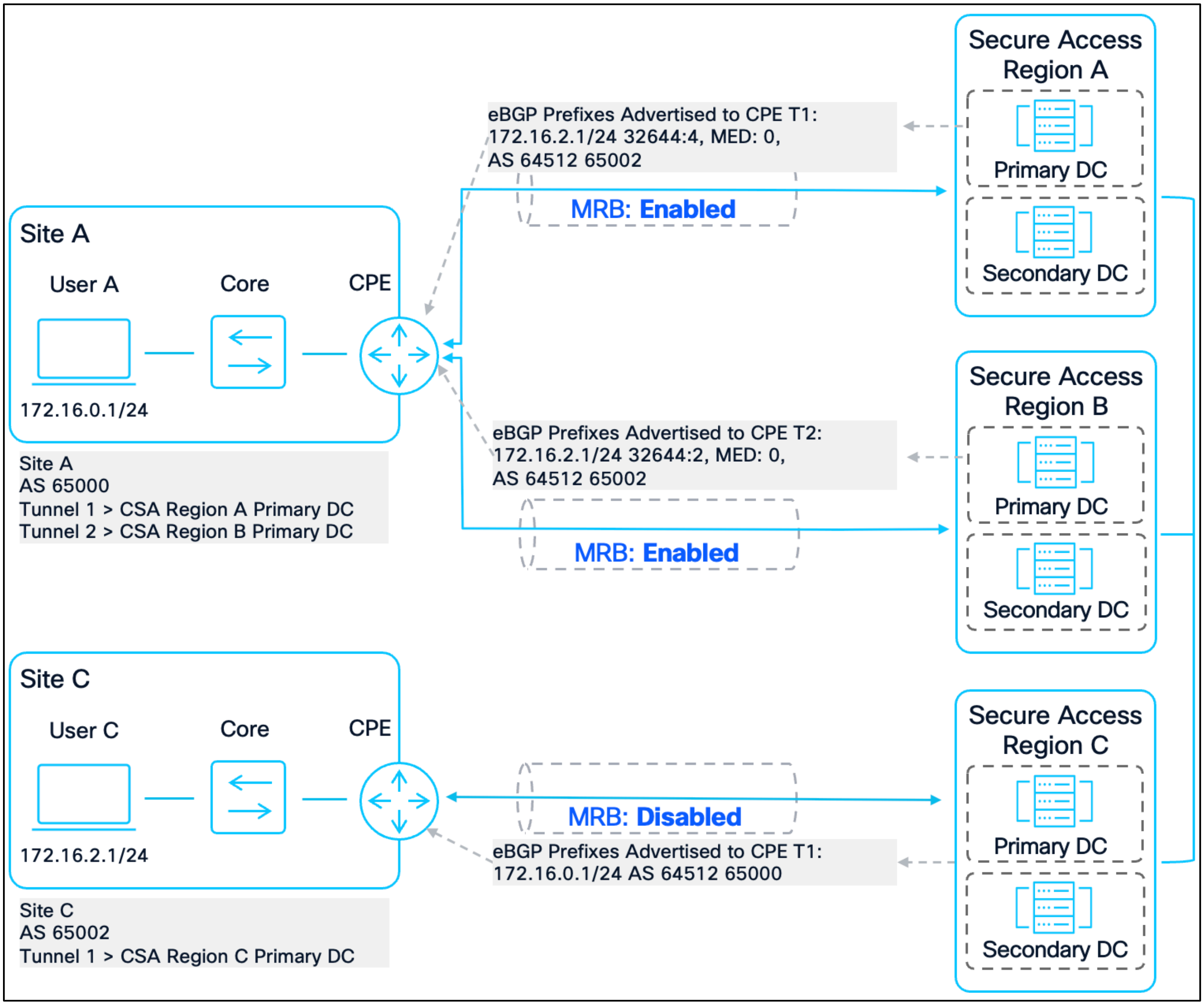

Secure Access Region A
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
172.16.2.1/24 32644:4, MED: 0,
AS 64512 65002
MRB: Enabled
Site A
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region B Primary DC
Secure Access Region B
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T2:
172.16.2.1/24 32644:2, MED: 0,
AS 64512 65002
MRB: Enabled
Site C
User C
Core
CPE
172.16.2.1/24
Site C
AS 65002
Tunnel 1 > CSA Region C Primary DC
Secure Access Region C
Primary DC
Secondary DC
MRB: Disabled
eBGP Prefixes Advertised to CPE T1:
172.16.0.1/24 AS 64512 65000

Figure 6.
Backhaul Forwarding Scenario

In the example above, Site C is connected to Secure Access Region C. User C wants to form a peer-to-peer connection with User A at Site A. Secure Access Region C does not have a direct connection to Site A, which is the site that advertises the route to that resource. Because of this, Region C forwards the traffic to the closest region that has a direct connection to Site A. In this example, that is Region B.

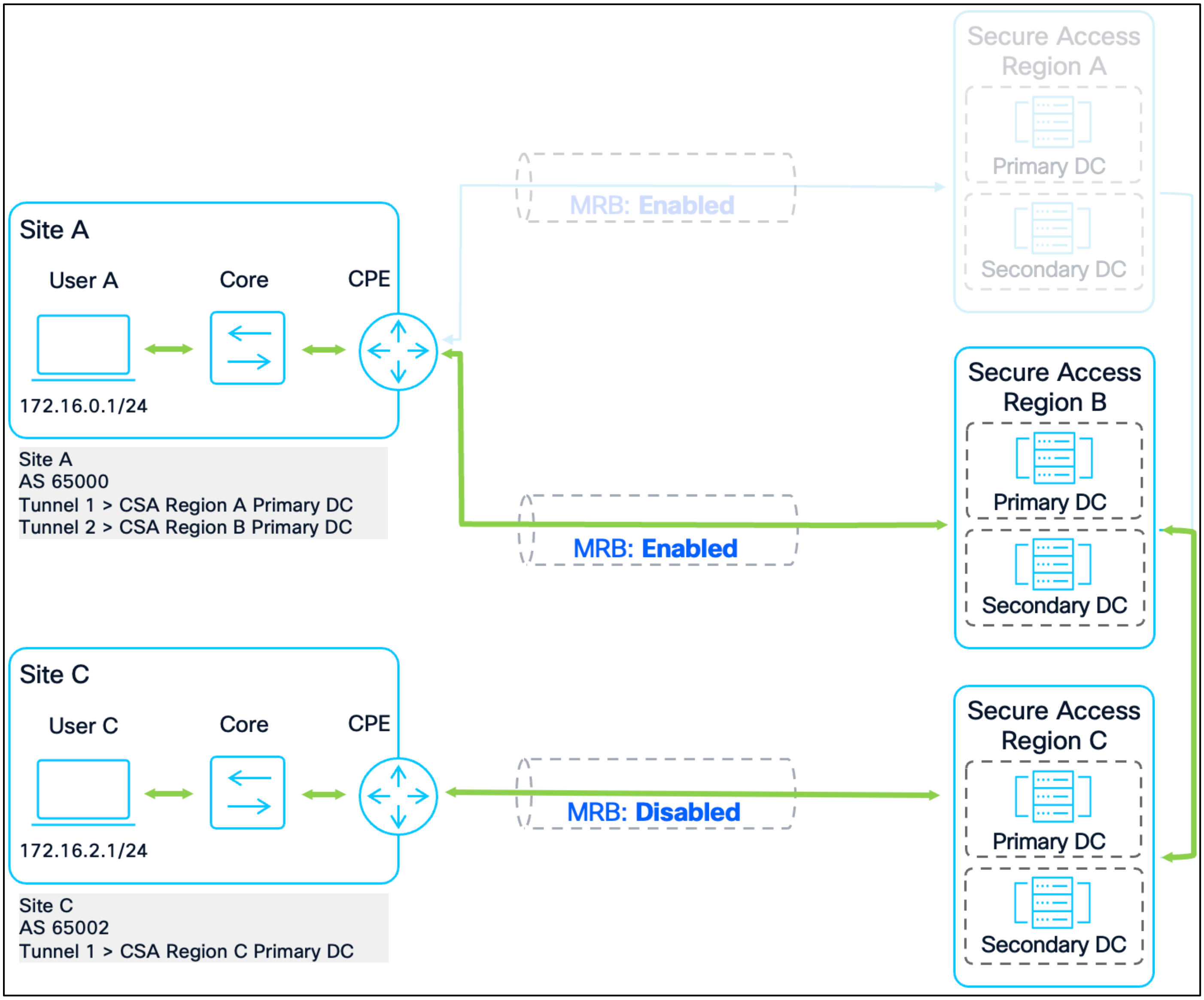


Figure 7.
Backhaul Forwarding Closest Path

Region B receives the packet and forwards it to Site A where it gets to User A. User A sends a return packet to User C. Both Secure Access Regions A and B advertise the return route to User C. Because Region B is closer, the community string value tagged to the User C's prefix is lower (32644:2) compared to the community string value tagged on Region A's prefix (32644:4). Based on the community string, Site A forwards the packet back to Region B and Region B forwards the packet to Region C. Region C then forwards the return packet back to Site C where it reaches User C.

If Site A ignored the community string and forwarded the return packet to Region A, asymmetric routing would have occurred, and the packet would have been dropped.

Only after the Region B connection becomes unavailable, such as if both the Primary and Secondary tunnels go down or the region goes down, will Secure Access direct traffic to the next closest region. In this example, that would be Region A.

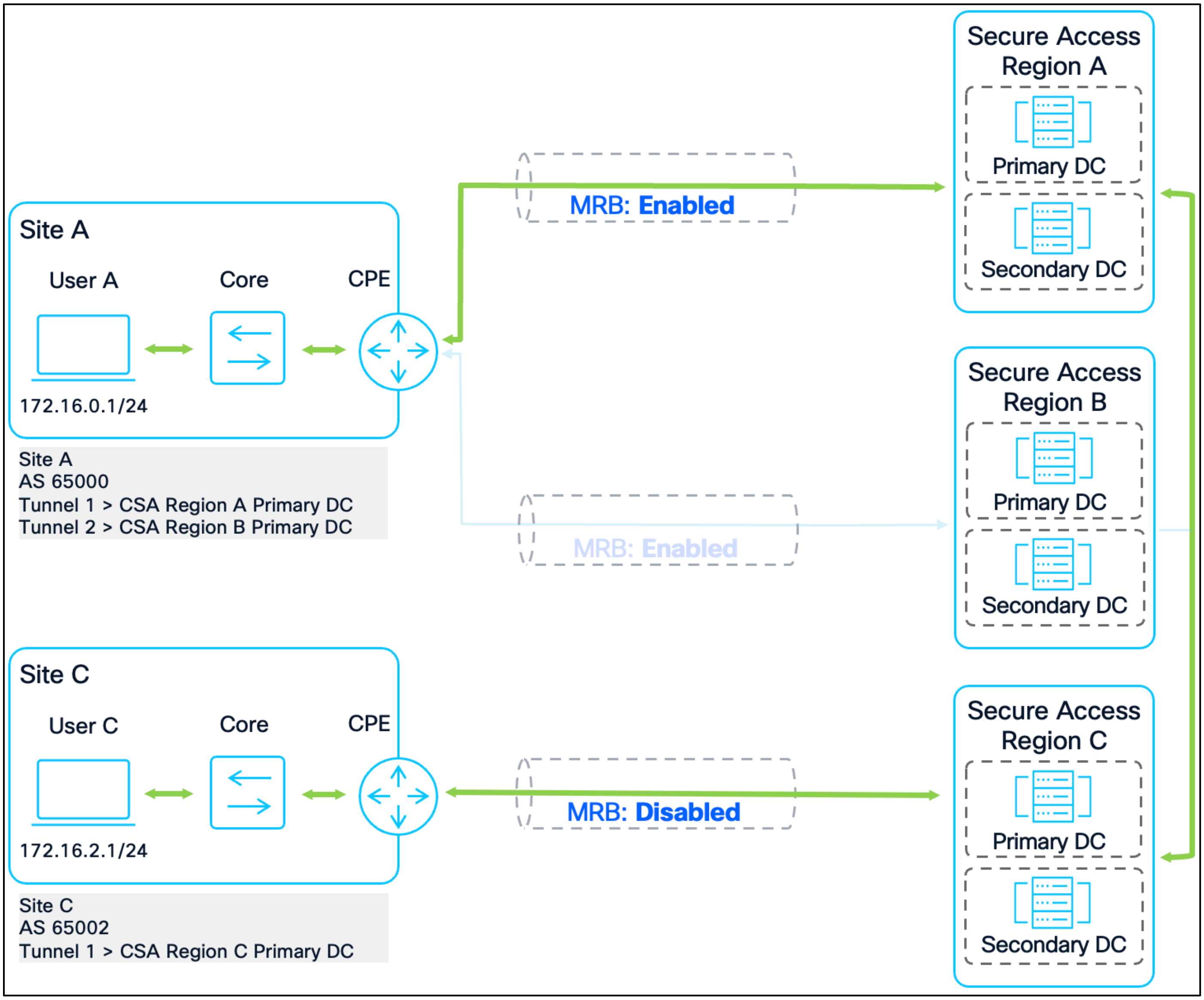


Figure 8.
Backhaul Forwarding second path

Because of this behavior, also known as hot potato routing, it is important that sites route traffic appropriately based on the community string values.

MRB is primarily useful when the same network route is advertised from one or more sites to multiple Secure Access regions. In these situations, traffic can potentially exit through different tunnels, leading to asymmetric routing-where outgoing and return traffic take different paths. Enabling MRB allows sites to select the best exit point, helping to keep traffic paths consistent and avoid asymmetric routing.

There are two common scenarios where the same route is advertised to more than one Secure Access region:

- Data Centers with Dual Connectivity: Customers with data centers that use Data Center Interconnects (DCIs) while also connecting to two different Secure Access regions. This setup makes applications hosted at those datacenters available through both Secure Access paths simultaneously.

- Single Site with Multi-Region Connections: A customer site connected to multiple Secure Access regions for redundancy. If one Secure Access region becomes unavailable, traffic can automatically reroute through another region.

This guide will focus on the Single Site with Multi-Region Connections scenario.

Strategy

Implementing a successful Multi-Region Redundancy architecture requires an ordered approach to configuration and validation. To ensure optimal performance and maintain the path symmetry necessary for stateful security inspections, it is essential to follow the deployment steps outlined below.

Note on Dynamic BGP Community Values and Scalability: The BGP community-string values (32644:X) utilized by Cisco Secure Access represent relative proximity within the global Cisco fabric. As Cisco continues to expand its global infrastructure and introduce new regions, **these proximity indicators (the "X" value) may change to reflect the updated network topology**. For example, a region currently identified as the second closest may shift in priority as new points of presence are integrated into the fabric.

Consequently, customers must prioritize the BGP Attribute Analysis phase to verify the specific community strings currently being advertised to their CPE before finalizing route-map logic. For long-term scalability, **it is recommended to pre-define a comprehensive range of community lists (e.g., 32644:0 through 32644:60)** to ensure the network automatically adapts to future Secure Access expansions without requiring manual configuration updates on every device.

Furthermore, to ensure the configuration remains resilient even when new Secure Access regions are introduced, **a catch-all permit statement should be implemented at the end of each route-map**. This serves as a critical fail-safe, ensuring that any prefix tagged with a new or unidentified community string is still accepted into the routing table with a baseline weight, preventing unintended traffic drops and maintaining continuous connectivity.

Steps to Set Up MRB for Multi-Region Redundancy on a CPE Device:

1. Establish IPsec Tunnels: Create two network tunnel groups (NTGs) with MRB enabled on two different Secure Access regions. Connect your CPE device to the two Secure Access regions using IPsec tunnels. Enable MRB under the Advanced Settings of the Routing section when creating or editing an NTG.

2. Set up BGP neighborships between the CPE and each Secure Access region to facilitate dynamic route exchange and redundancy.

3. Verify BGP Prefix Tags: Examine the community strings and Multi-Exit Discriminators (MEDs) attached to BGP prefixes advertised from each Secure Access region. This step is essential to understand the route preferences being signaled.

4. Design Route-Maps for Traffic Selection: Develop route-maps to prioritize routes based on:

    - **Community String Values:** Prefer routes with the lowest X value, which signifies the closest region.

    - **Tunnel Preference:** Favor the primary tunnel in the Primary region, followed by the secondary tunnel in the same region.

    - **Regional Preference:** Prioritize the nearest region to the site, then the Secondary region. This best practice enhances performance and streamlines routing logic, helping prevent asymmetric routing.

    - **Exceptions:** Define exception handling for specific scenarios, such as site-to-site communication where asymmetric routing could otherwise occur.
    - **Catch-all Logic:** Implement a final sequence to handle unidentified community strings, ensuring no prefixes are dropped.

5. Apply Route-Maps to BGP Peers: Attach the route-maps to the corresponding BGP neighbor configurations to enforce desired routing behavior.
6. Redistribute Routes Internally: Inject the preferred Secure Access routes into your internal routing protocols as required.

This guide will focus on steps 3-5 for a Cisco IOS-XE device. For Establishing IPsec Tunnels, review Manage Network Tunnel Groups and Network Tunnel Configuration. For Configuring BGP Peering, review Dynamic Routing with BGP.

Verify BGP Prefix Tags

Before configuring MRB, you must analyze how Cisco Secure Access advertises routes to your CPE. This data collection phase is critical because it identifies the specific BGP attributes, Community Strings and Multi-Exit Discriminators (MED), that will be used to build your route-map logic.

On IOS-XE, the primary tools for this analysis are **show ip bgp** and **show ip bgp [prefix]**.

Getting a Global View: show ip bgp

The **show ip bgp** command provides a summary of the BGP table. When reviewing this output for Secure Access, focus on the following elements:

- Status Codes (* and >):
    - The asterisk (*) indicates a valid route.
    - The greater-than symbol (>) indicates the best route chosen by the BGP selection algorithm. Only the "best" route is installed in the routing table (RIB) and used for forwarding.
- Path (AS Path): This shows the sequence of Autonomous Systems a route has traversed. Secure Access uses the Private ASN 64512. **Note**: Starting in November 2025, newly created Secure Access organizations will use the public ASN 32644 by default for BGP peering. For these organizations, the command output will return **32644 i** instead. For more information see: Dynamic Routing with BGP.
    - 64512 i: This indicates the prefix is originated directly by Secure Access (e.g., Internet exit points or VPNaaS IP pools).
    - 64512 65001 i: This indicates a Site-to-Site route. In this example, the prefix originated at a remote site (AS 65001), passed through the Secure Access fabric (AS 64512), and was then advertised to your local router. Identifying these paths is essential if you need to create routing exceptions for specific branch offices.
- Next Hop: This identifies the peer’s tunnel interface (IP address) providing the route. On a site setup for redundancy using MRB, you will see four next hops for every prefix (Primary/Secondary DC for the Primary region, and Primary/Secondary DC for the Secondary region).
- Metric (MED): Secure Access uses the Metric (also known as MED) to differentiate between the Primary Tunnel and the Secondary Tunnel within the same region.

  - Metric 0: Represents the Primary Tunnel.
  - Metric 1: Represents the Secondary Tunnel.

```
C8000V-SiteA#show ip bgp
BGP table version is 139, local router ID is 192.168.60.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
 *    192.168.0.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    172.16.1.0/24    169.254.0.5              0             0 64512 65001 i
 *>                    169.254.0.1              0             0 64512 65001 i
 *                     169.254.0.3              1             0 64512 65001 i
 *                     169.254.0.7              1             0 64512 65001 i
```

The Detailed View: show ip bgp [prefix]

While the summary table shows the Metric and AS Path, it does not show BGP Communities or Community Strings. Community Strings are metadata tags applied to routes that Secure Access advertises to communicate "proximity" or "regional distance." To see these, you must look at the specific prefix detail.

- Community String (32644:X): Secure Access uses the format 32644:[Value]. In the example below:
  - 32644:0 indicates a "Local" region. Essentially one of the closest possible regions for the route.
  - 32644:10 indicates a more distant region.

Since the BGP table might show multiple paths with a Metric of 0 (one from the local region and one from a remote region), the Community String is the only way for the router to programmatically distinguish between a Primary region and a Secondary region tunnel.

```
C8000V-SiteA#show ip bgp 192.168.0.0
BGP routing table entry for 192.168.0.0/25, version 127
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
```

Once you've determined the community string values for the prefixes, a route-map can be created to influence routing logic.

Creating Route-Maps for Each BGP Peer

On IOS-XE routers, several attributes can be used to influence routing decisions. In this guide, we'll focus on using the Weight attribute. Weight is a Cisco-specific BGP attribute that only affects route selection on the local router and is not propagated to other BGP peers. Alternatively, the Local Preference attribute could be used, which is a standard BGP attribute shared among peers within the same AS, but for this setup, Weight provides the desired control at the device level.

When traffic from your site is destined for a Secure Access tunnel, the IOS-XE router uses the Weight attribute to decide which tunnel to use. Route-maps are employed to assign weights to different prefixes based on their attributes.

- **Community String-Based Weighting:** Assign higher weights to routes with lower community string values, as these indicate closer proximity.

  For example, a prefix with community string 32644:0 (local region) might be assigned a weight of 503, while 32644:2 could get a weight of 403. Since 503 > 403, the router will prefer the route with 32644:0.

- **Tunnel Preference:** Instead of matching on the MED value tagged on the prefixes advertised by Secure Access, we will simply give prefixes from the secondary tunnel a lower weight. This is done by creating two route-maps: one for primary tunnel and other for secondary tunnel. These route-maps will still match on community strings and apply different weights depending on the community string AND if the route-map is for the primary or secondary DC. Primary tunnels will have some weight value N. For secondary tunnels, the weight is decremented by one (N-1).

  For example, for a prefix tagged with 32644:0, assign a weight of 503 to prefixes from the primary DC and 502 to prefixes from the secondary DC for the same region.

- **Regional Preference:** This builds upon the Primary/Secondary Tunnel Preference mentioned previously. In this design, all sites prioritize the region they are closest to, followed by a Secondary region. Setting the closest Secure Access region as the Primary region follows best practices for performance.

  Two more route-maps will be created: one for primary tunnel to the Secondary region and other for secondary tunnel to the Secondary region. Once again, these route-maps will match on community strings and apply different weights depending on the community string AND if the route-map is for the primary or secondary DC for the Secondary region. For prefixes from the Primary tunnel to the Secondary region, the weight will be decremented by two (N-2). For prefixes from the Secondary tunnel to the Secondary region, the weight will be decremented by three (N-3). To handle prefixes tagged with unidentified community strings or no community strings, it is highly recommended to configure a catch-all at the end. Without a catch-all for prefixes with unidentified community strings, those prefixes will be dropped from the routing table.

An example of what this will look like in practice for two community strings, 32644:0 and 32644:2:

Step 1. Define Community strings

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-2 permit 32644:2
```

Step 2. Create Route-Maps for Each Tunnel/Region Combination

```
route-map Primary-DC-Primary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 203
route-map Primary-DC-Primary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 103
route-map Primary-DC-Primary-Region permit 100
 set weight 53


route-map Secondary-DC-Primary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 202
```

```
route-map Secondary-DC-Primary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 102
route-map Secondary-DC-Primary-Region permit 100
 set weight 52
route-map Primary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 201
route-map Primary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 101
route-map Primary-DC-Secondary-Region permit 100
 set weight 51
route-map Secondary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 200
route-map Secondary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 100
route-map Secondary-DC-Secondary-Region permit 100
 set weight 50
```

These commands do the following:

1. Enable BGP Community String Formatting: ip bgp-community new-format

   Enables the display and use of BGP community strings in the standard "number:number" format, making it easier to match and manage community values.

2. Define Community Lists: ip community-list standard [name] [value]

   Creates named lists to match specific BGP community values. These are used to identify routes tagged with certain Secure Access proximity indicators (the values after the colon).

3. Create Route-Maps to Prioritize Routes

   There are four route-maps, one for each Secure Access region/tunnel group.

   Each route-map matches routes with certain community values and assigns both a local preference and a weight:

   - Higher weights and local preference values are given to routes with lower community string values (closer regions).
   - The route-maps set slightly lower weights for more distant regions or for secondary tunnels.

    - A final catch-all statement gives all other unmatched routes a much lower weight. Without the catch-all, unmatched routes will hit the implicit deny at the end, and the prefix will not be added to the routing table.

Note on Scalability: While this guide focuses on the specific community strings observed during validation (e.g., 32644:0 and 32644:10), a more robust production design involves pre-defining all the community-lists that are sent from Secure Access (32644:0 through 32644:60 at the time of writing this guide). By proactively mapping these values to a descending weight hierarchy, you ensure the network automatically adapts to new Secure Access regions or data centers without requiring manual configuration updates on every CPE. There is also the catch-all statement to handle undefined community strings. The examples in this guide are intentionally condensed to highlight the fundamental mechanics of the MRB logic.

Handling Exceptions

While this approach covers most prefixes, certain conditions may require exceptions to be configured to prevent asymmetric routing. One condition is when two sites have swapped Primary and Secondary regional Priorities – that is Site A’s Primary region is Site B’s Secondary region and Site A’s Secondary region is Site B’s Primary region. Because both sites are connected to the same regions, both Secure Access regions advertise the prefixes as 32644:0. Additionally, because each site prefers different Primary regions, each site will send traffic destined to the other site through a different Secure Access region, rather than the same region, causing asymmetric routing.

To handle this sort of condition, an exception must be made. There are multiple ways to implement an exception, however, in this design guide matching on the AS-Path of the other site was used due to being more scalable. Other methods may include matching on specific prefix lists. For more information, see the section Site to Site (Swapped Primary and Secondary region).

Exception Handling Example:

```
ip as-path access-list 10 permit _(65002)_
route-map Primary-DC-Secondary-Region permit 5
 match as-path 10
 set local-preference 108
 set weight 301
route-map Primary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 201
route-map Primary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 101
route-map Primary-DC-Secondary-Region permit 100
 set weight 51
route-map Secondary-DC-Secondary-Region permit 5
 match as-path 10
 set local-preference 108
 set weight 300
```

```
route-map Secondary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 200
route-map Secondary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 100
route-map Secondary-DC-Secondary-Region permit 100
 set weight 50
```

These commands do the following:

1. Create an AS-Path Access-list: ip as-path access-list [#] permit [value]

   Creates an access-list that matches on specific AS-Path values. In this example, a single AS was used, but multiple AS values can be used by changing the format to **ip as-path access-list [#] permit _(AS1|AS2|…)_.** For example, **ip as-path access-list 10 permit _(65002|65003)_** will match on AS-Path values that have either 65002 or 65003. This can simplify creating exceptions for multiple sites.

2. Add a higher sequence in Route-Maps to match on AS-Path

   Route-maps are evaluated from the lowest sequence to the highest sequence. For the Secondary region Route-maps, a lower sequence is added to the top with the exception. When the AS-Path is found in the prefix, a higher weight is applied. This allows us to send traffic that would normally be forwarded to the Primary/Secondary DC for the Primary region to instead prefer the Primary/Secondary DC for the Secondary region because of a higher weight.

Assign Route-Maps to Appropriate BGP Peers and Validate Result

Finally, the route-maps are applied to the appropriate BGP peers. The peers are associated with the tunnels to the Primary and Secondary Secure Access regions.

```
router bgp 65000
 address-family ipv4
  neighbor 169.254.0.1 route-map Primary-DC-Primary-Region in
  neighbor 169.254.0.3 route-map Secondary-DC-Primary-Region in
  neighbor 169.254.0.5 route-map Primary-DC-Secondary-Region in
  neighbor 169.254.0.7 route-map Secondary-DC-Secondary-Region in
 exit-address-family
```

After the commands have been added to the BGP peers, the routing logic should change within a few moments. To verify the implementation, we use the same show commands from the data collection phase to ensure the attributes are being applied correctly.

Validating with show ip bgp

When reviewing the global BGP table after configuration, focus on how the Weight and LocPrf columns have changed. These values now override the default selection process.

- Weight (The Primary Tie-Breaker): In Cisco IOS-XE, Weight is the first attribute evaluated. Because we assigned the highest weights to the Primary region (e.g., 203/202), the router will now consistently select the Primary region tunnel as "Best" (>), even if the Secondary region has a "better" Metric or a shorter path. If the prefix with weight 203 becomes unavailable, it will then choose the prefix with weight 202.

- LocPrf (Local Preference): While Weight handles the local router, Local Preference ensures that this path is preferred by other iBGP peers within your network.
- The Best Path (>): Confirm that the > symbol has moved to the Primary DC of the Primary region (Next Hop 169.254.0.1).

```
C8000V-SiteA#show ip bgp
[…header omitted…]
 *>   192.168.0.0/25   169.254.0.1               0    106    203 64512 i
 *                     169.254.0.3               1    106    202 64512 i
 *                     169.254.0.5               0    104    101 64512 i
 *                     169.254.0.7               1    104    100 64512 i
```

If your BGP table does not reflect the Weights or Local Preference values defined in your route-maps, use the following steps to identify and resolve the issue.

- The route-map is set up correctly.
  - **show running-configuration | s route-map** can show the configuration of all route-maps on the device. Make sure that the matches follow the expected sequence numbers. Once the route-map finds a match on a sequence; it does not evaluate the remaining sequences.
  - **show running-configuration | s community-list** will show the configured community strings. Ensure that the correct one is being matched in the route-map.
- The prefix is tagged with the same community string value that it should match on in the route-map.
  - Execute the show ip bgp [prefix] command and verify that the Community in the prefix advertised by the peer matches the community-list created and applied in the route-map.
- The route-map is applied to the correct BGP Peer.

Deep Dive

To demonstrate the implementation of Multi-Region Redundancy using MRB, this guide utilizes a reference topology consisting of four distinct sites: Site A, Site B, Site C, and Site D. This specific selection of sites is designed to test every major redundancy permutation, including same-region failover, swapped-region symmetry, and cross-continental distinct-region routing.

Each site is configured with four redundant tunnels, connecting to both a Primary and Secondary Data Center (DC) across two different Secure Access regions, and utilizes BGP to manage prefix advertisements.

Sites A and B: US West Coast (Standard Regional Alignment)

Sites A and B represent a standard dual-region deployment. They prioritize the US West region due to geographic proximity, with US East serving as the designated backup region.

- BGP Configuration: Site A (AS 65000) advertises 172.16.0.0/24; Site B (AS 65001) advertises 172.16.1.0/24.
- Tunnel Architecture:
  - Tunnel 1 & 2: Primary and Secondary DCs in US West (Pacific Northwest).
  - Tunnel 3 & 4: Primary and Secondary DCs in US East (Virginia).

Site C: US East Coast (Swapped Regional Alignment)

Site C serves as the geographic counterpart to the West Coast sites. It utilizes the same two regions but inverts the priority, designating US East as Primary and US West as Secondary. This site is critical for testing symmetry in "swapped" region scenarios.

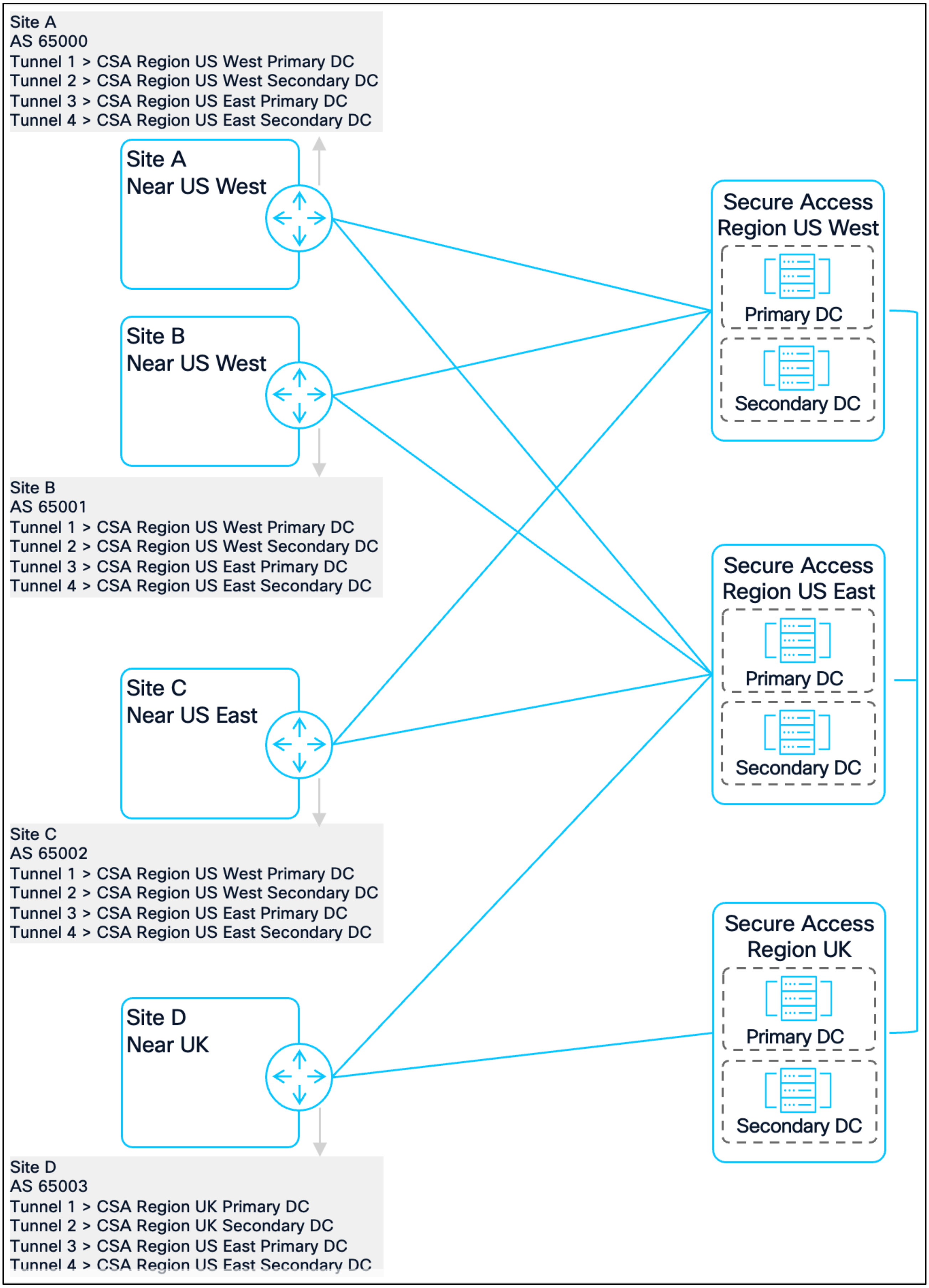
- BGP Configuration: AS 65002; advertising 172.16.2.0/24.
- Tunnel Architecture:
  - Tunnel 1 & 2: Primary and Secondary DCs in US West.
  - Tunnel 3 & 4: Primary and Secondary DCs in US East.

Site D: United Kingdom (Distinct Regional Alignment)

Site D introduces a cross-continental scenario. It is anchored to the UK region as its primary gateway, with US East serving as the Secondary region. This tests how the Secure Access fabric handles traffic between distinct, non-overlapping primary/Secondary regions.

- BGP Configuration: AS 65003; advertising 172.16.3.0/24.
- Tunnel Architecture:
  - Tunnel 1 & 2: Primary and Secondary DCs in UK (United Kingdom).
  - Tunnel 3 & 4: Primary and Secondary DCs in US East.

Note: The final IOS-XE configuration for all four sites is available in Appendix A.



Site A
AS 65000
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC

Site B
AS 65001
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC

Site C
AS 65002
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC

Site D
AS 65003
Tunnel 1 > CSA Region UK Primary DC
Tunnel 2 > CSA Region UK Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC

Figure 9.
Network Topology

Remote Access Redundancy

Multi-Region Remote Access redundancy ensures that Secure Access VPNaaS or ZTNA services remain available during a regional outage. In this design, VPNaaS is deployed in two regions: US West (IP Pool 192.168.0.0/24) and US East (IP Pool 192.168.1.0/24). By analyzing the BGP attributes at the branch router, we can implement a routing policy that ensures traffic returns to the VPN client through the same region it used for ingress.

Data Collection - Remote Access

The IOS-XE command **show ip bgp** is used to check the VPNaaS IP Pools. For brevity, the prefixes not pertaining to the IP Pools (including the system IP Pool) have been removed from the output:

Analyzing the BGP table with show ip bgp reveals that without a route-map, the router defaults to Tunnel 1 (169.254.0.1) for all VPN traffic, regardless of which region the client is connected to. This creates an asymmetric routing issue for clients in the US East pool; while their traffic enters the network via US East (Tunnel 3), the branch router attempts to send return traffic via US West (Tunnel 1).

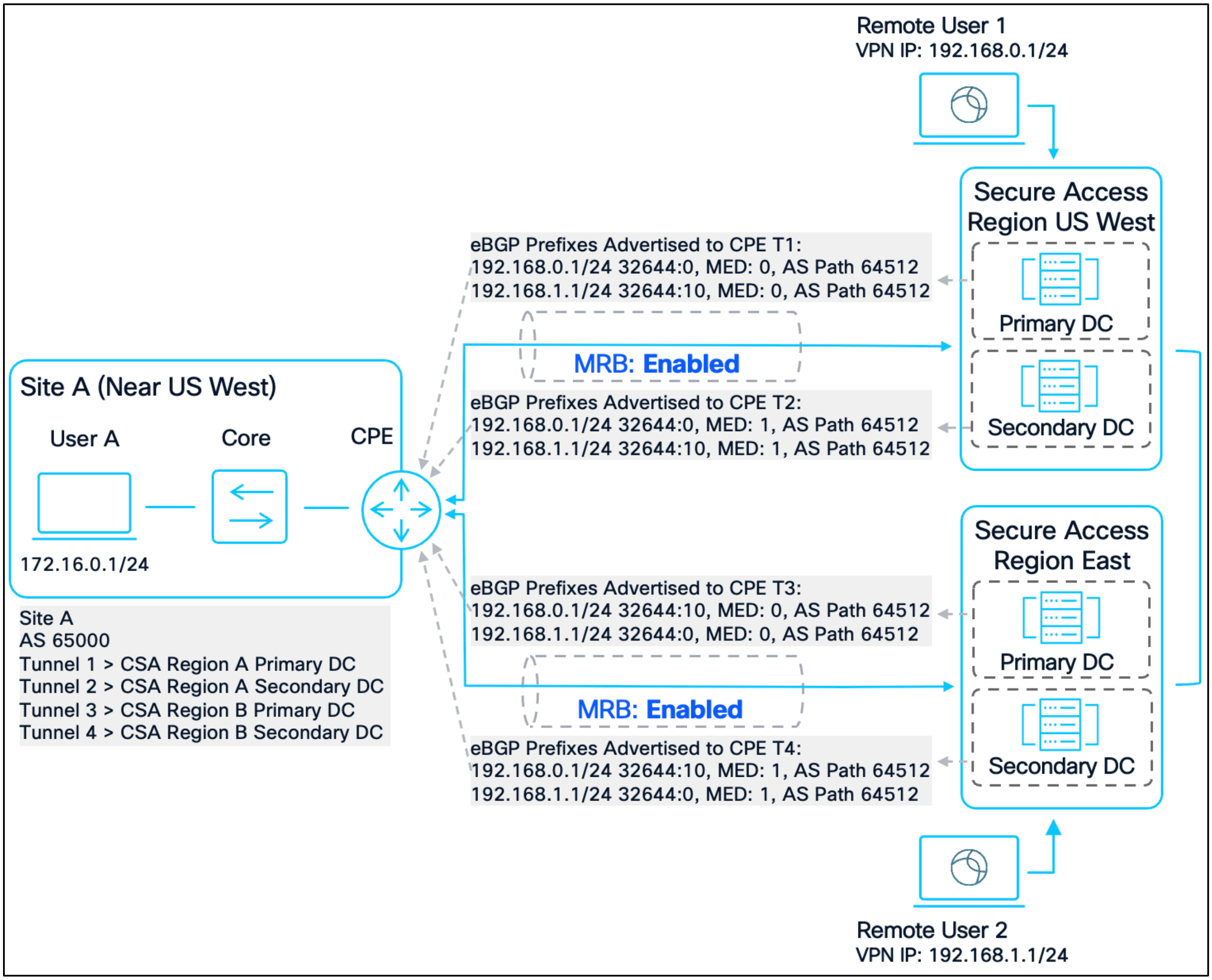

Remote User 1
VPN IP: 192.168.0.1/24
Secure Access Region US West
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
192.168.0.1/24 32644:0, MED: 0, AS Path 64512
192.168.1.1/24 32644:10, MED: 0, AS Path 64512
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
192.168.0.1/24 32644:0, MED: 1, AS Path 64512
192.168.1.1/24 32644:10, MED: 1, AS Path 64512
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
Secure Access Region East
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T3:
192.168.0.1/24 32644:10, MED: 0, AS Path 64512
192.168.1.1/24 32644:0, MED: 0, AS Path 64512
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
192.168.0.1/24 32644:10, MED: 1, AS Path 64512
192.168.1.1/24 32644:0, MED: 1, AS Path 64512
Remote User 2
VPN IP: 192.168.1.1/24

Figure 10.
Remote Access Scenario

```
C8000V-SiteA#show ip bgp
BGP table version is 139, local router ID is 192.168.60.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
[omitted]
 *    192.168.0.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    192.168.0.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    192.168.1.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    192.168.1.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

A detailed inspection using show ip bgp [prefix] confirms that Secure Access uses community strings to identify regional proximity. For the US West pool (192.168.0.0/24), the US West tunnels are tagged with 32644:0 (Local to that region), while the US East tunnels are tagged with 32644:10 (Distant to that region). This logic is inverted for the US East pool. However, because the router currently ignores these tags, it relies on the Metric (MED).

```
C8000V-SiteA#show ip bgp 192.168.0.0
BGP routing table entry for 192.168.0.0/25, version 127
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
```

```
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
C8000V-SiteA#show ip bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/25, version 127
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:10
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
```

Because the MED tag is taken into consideration when determining the best route, if tunnel 1 goes down, the next best path will be the route to the US East Primary DC for both US West and US East VPNaaS Pools.

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.0.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *>   192.168.0.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *>   192.168.1.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *>   192.168.1.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

Configuration – Remote Access

To resolve these issues, the following configuration is applied to Site A. The route-maps use the Weight attribute to override the default BGP selection process. By matching the 32644:0 and 32644:10 community strings and assigning graduated weights, asymmetric routing is prevented while ensuring that:

- The US West primary and secondary DCs are preferred for US West VPN Clients
- The US East primary and secondary DCs are preferred for US East VPN Clients

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
```

```
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

The community-list and route-map configuration will work for both Sites A and B.

While this route-map configuration could work for Remote Access Redundancy on Sites C and D as well, to appropriately handle other scenarios that will be covered later, such as Secure Internet Access redundancy, the route-maps will be modified slightly. For Site C, the route-map will be configured to have a regional preference for US East while Site D has a regional preference for UK. For example, on the Site C Router:

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
```

```
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
address-family ipv4
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

Validation – Remote Access

To make sure that the route-map configuration works, each tunnel will be brought down starting with Tunnel 1. After each tunnel is brought down, the best route will be verified using the **show ip bgp** command.

Failover Test #1

To verify the configuration, a series of failover tests were conducted on Site A. In the baseline state, the router correctly identifies the best path for each pool based on the community tags. Return traffic for the US West pool (192.168.0.0/25) is directed to Tunnel 1 (Weight 203), while return traffic for the US East pool (192.168.1.0/25) is directed to Tunnel 3 (Weight 201). This confirms that asymmetric routing is resolved for clients in both regions.

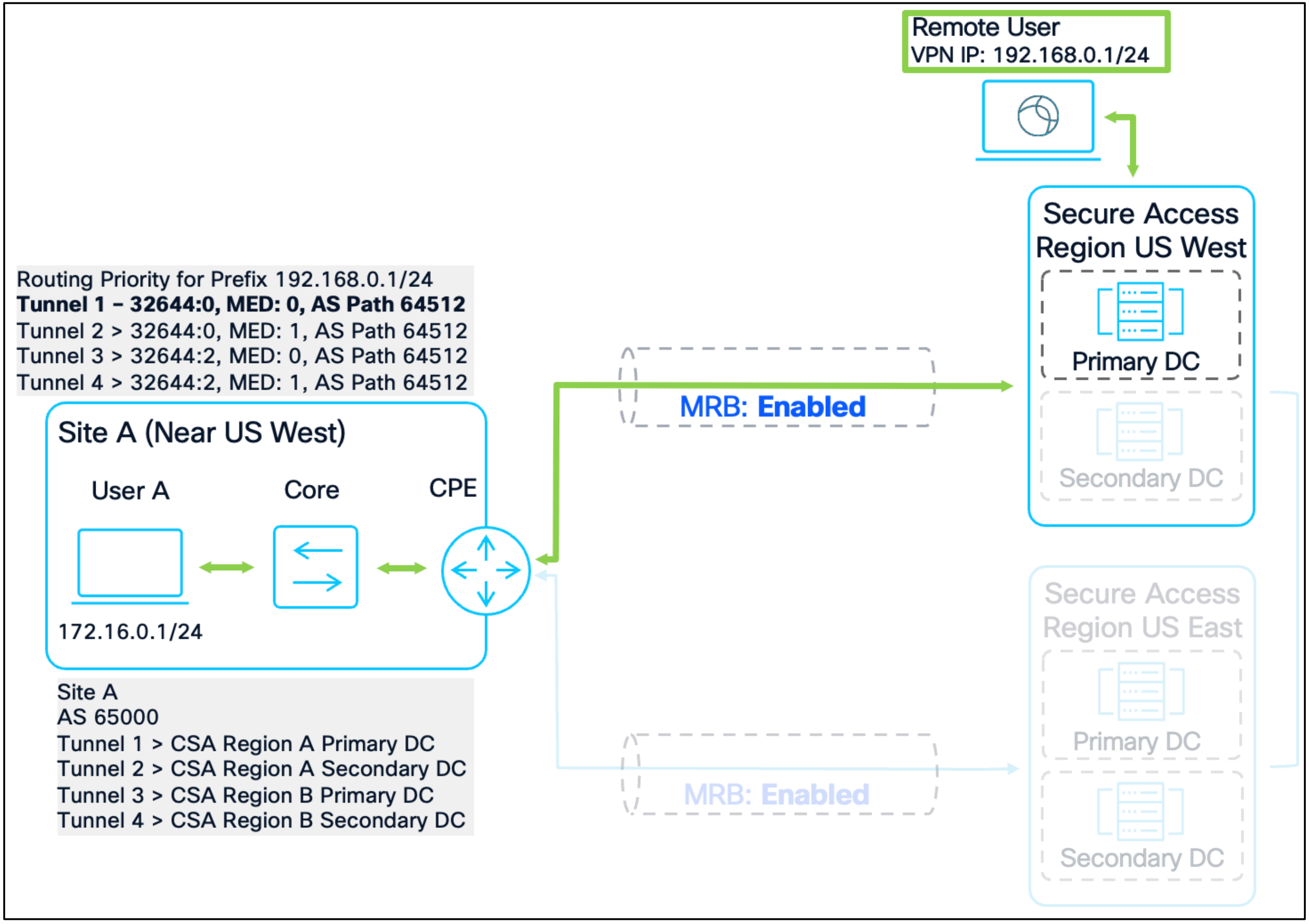

Remote User
VPN IP: 192.168.0.1/24
Secure Access
Region US West
Primary DC
Secondary DC
Routing Priority for Prefix 192.168.0.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512
Tunnel 2 > 32644:0, MED: 1, AS Path 64512
Tunnel 3 > 32644:2, MED: 0, AS Path 64512
Tunnel 4 > 32644:2, MED: 1, AS Path 64512
MRB: Enabled
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
Secure Access
Region US East
Primary DC
Secondary DC
MRB: Enabled

Figure 11.
Remote Access Failover Test #1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.0.0/25   169.254.0.1              0    104    203 64512 i
 *                     169.254.0.5              0    102    101 64512 i
 *                     169.254.0.7              1    102    100 64512 i
 *                     169.254.0.3              1    104    202 64512 i
 *>   192.168.0.128/25 169.254.0.1              0    104    203 64512 i
 *                     169.254.0.5              0    102    101 64512 i
 *                     169.254.0.7              1    102    100 64512 i
 *                     169.254.0.3              1    104    202 64512 i
 *    192.168.1.0/25   169.254.0.1              0    102    103 64512 i
 *>                    169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
 *                     169.254.0.3              1    102    102 64512 i
 *    192.168.1.128/25 169.254.0.1              0     102    103 64512 i
 *>                    169.254.0.5              0     104    201 64512 i
 *                     169.254.0.7              1     104    200 64512 i
 *                     169.254.0.3              1     102    102 64512 i
[omitted]
```

Failover Test #2

When the US West Primary DC (Tunnel 1) is disabled, the router re-evaluates the US West pool. It correctly selects Tunnel 2 (US West Secondary) because its weight of 202 is higher than the backup region's primary tunnel (Weight 101). This maintains regional affinity even though the backup region offers a better Metric.

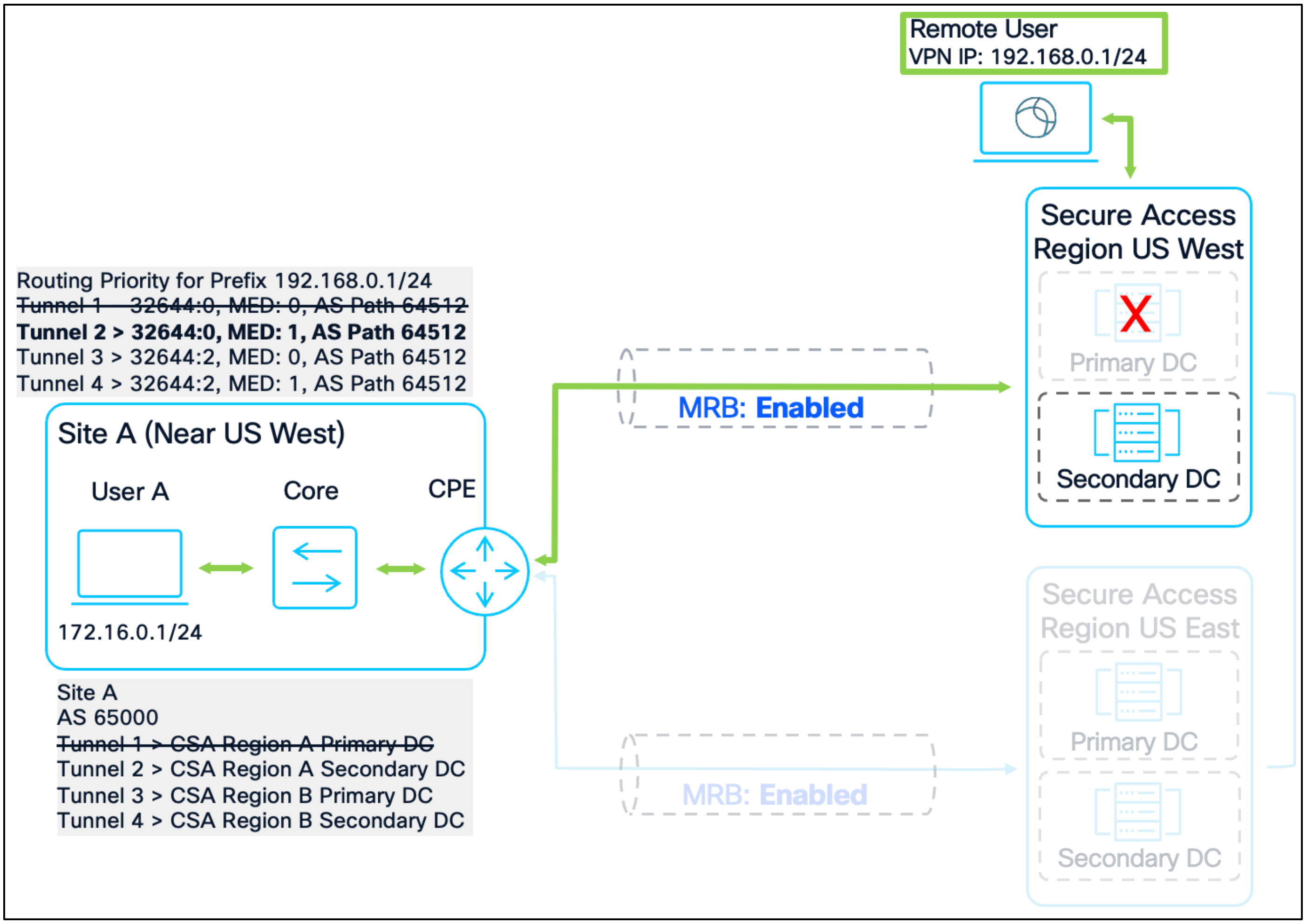
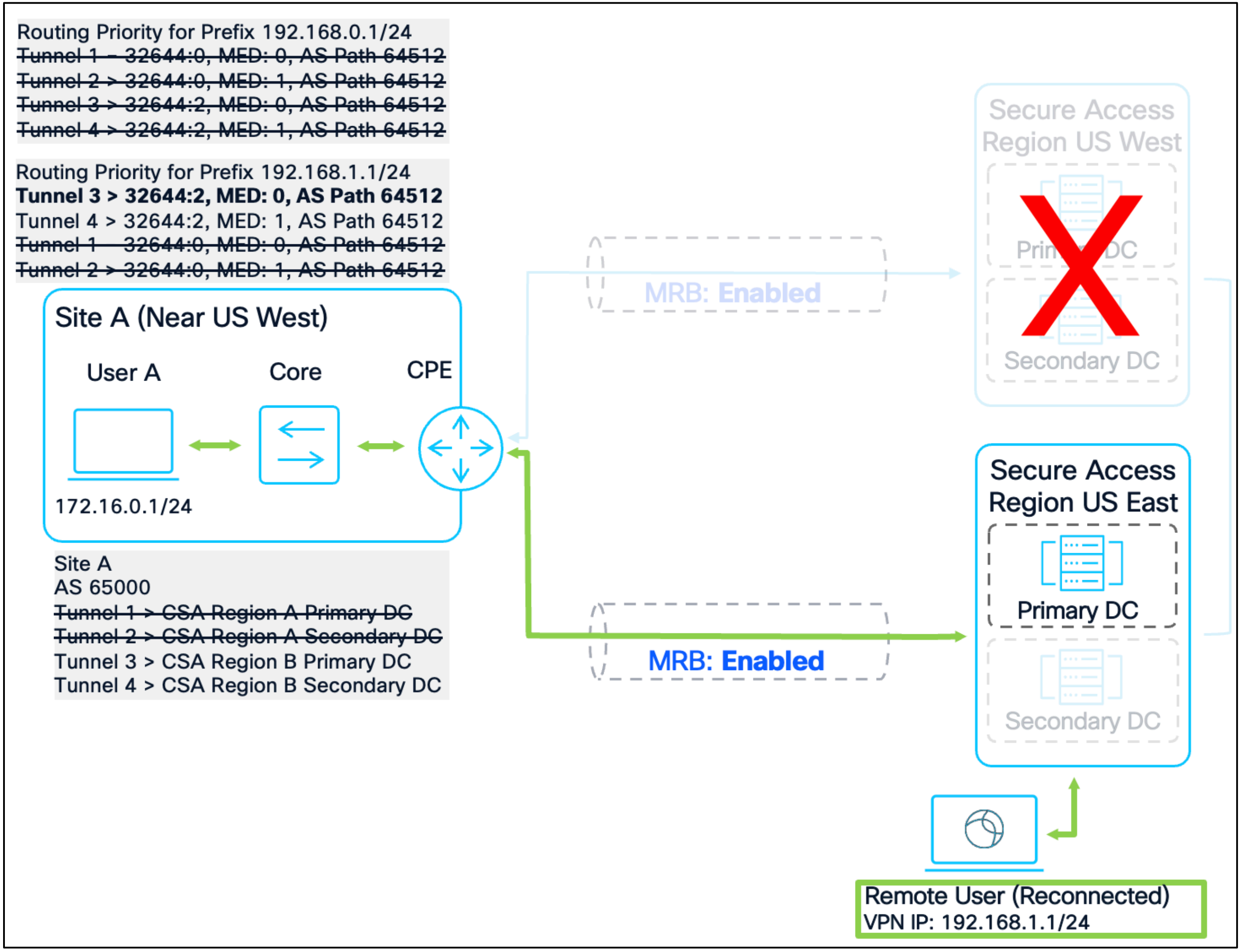

Remote User
VPN IP: 192.168.0.1/24
Secure Access Region US West
X
Primary DC
Secondary DC
Routing Priority for Prefix 192.168.0.1/24
~~Tunnel 1 > 32644:0, MED: 0, AS Path 64512~~
Tunnel 2 > 32644:0, MED: 1, AS Path 64512
Tunnel 3 > 32644:2, MED: 0, AS Path 64512
Tunnel 4 > 32644:2, MED: 1, AS Path 64512
MRB: Enabled
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
Secure Access Region US East
Primary DC
Secondary DC

Figure 12.
Remote Access Failover Test #2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    192.168.0.0/25   169.254.0.5              0     102    101 64512 i
 *                     169.254.0.7              1     102    100 64512 i
 *>                     169.254.0.3             1     104     202  64512  i
 *     192.168.0.128/25 169.254.0.5             0     102     101  64512  i
 *                      169.254.0.7             1     102     100  64512  i
 *>                     169.254.0.3             1     104     202  64512  i
 *>    192.168.1.0/25   169.254.0.5             0     104     201  64512  i
 *                      169.254.0.7             1     104     200  64512  i
 *                      169.254.0.3             1     102     102  64512  i
 *>    192.168.1.128/25 169.254.0.5             0     104     201  64512  i
 *                      169.254.0.7             1     104     200  64512  i
 *                      169.254.0.3             1     102     102  64512  i
[omitted]
```

Failover Test #3

If the entire US West region fails, the US West pool prefixes are no longer advertised. Remote users reconnecting to the US East VPNaaS are assigned addresses from the 192.168.1.0/24 pool. The router identifies Tunnel 3 as the best path for this traffic with a weight of 201, ensuring all return traffic transits the US East primary data center.



Routing Priority for Prefix 192.168.0.1/24
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512~~
~~Tunnel 2 > 32644:0, MED: 1, AS Path 64512~~
~~Tunnel 3 > 32644:2, MED: 0, AS Path 64512~~
~~Tunnel 4 > 32644:2, MED: 1, AS Path 64512~~

Routing Priority for Prefix 192.168.1.1/24
Tunnel 3 > 32644:2, MED: 0, AS Path 64512
Tunnel 4 > 32644:2, MED: 1, AS Path 64512
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512~~
~~Tunnel 2 > 32644:0, MED: 1, AS Path 64512~~

Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Figure 13.
Remote Access Failover Test #3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.1.0/25   169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
 *>   192.168.1.128/25 169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
[omitted]
```

Failover Test #4

In the final failure scenario where only the US East Secondary DC is functional, the router installs Tunnel 4 as the best path with a weight of 200. This confirms that the routing policy is robust enough to maintain a functional connection for remote users as long as a single tunnel to the Secure Access fabric remains active.

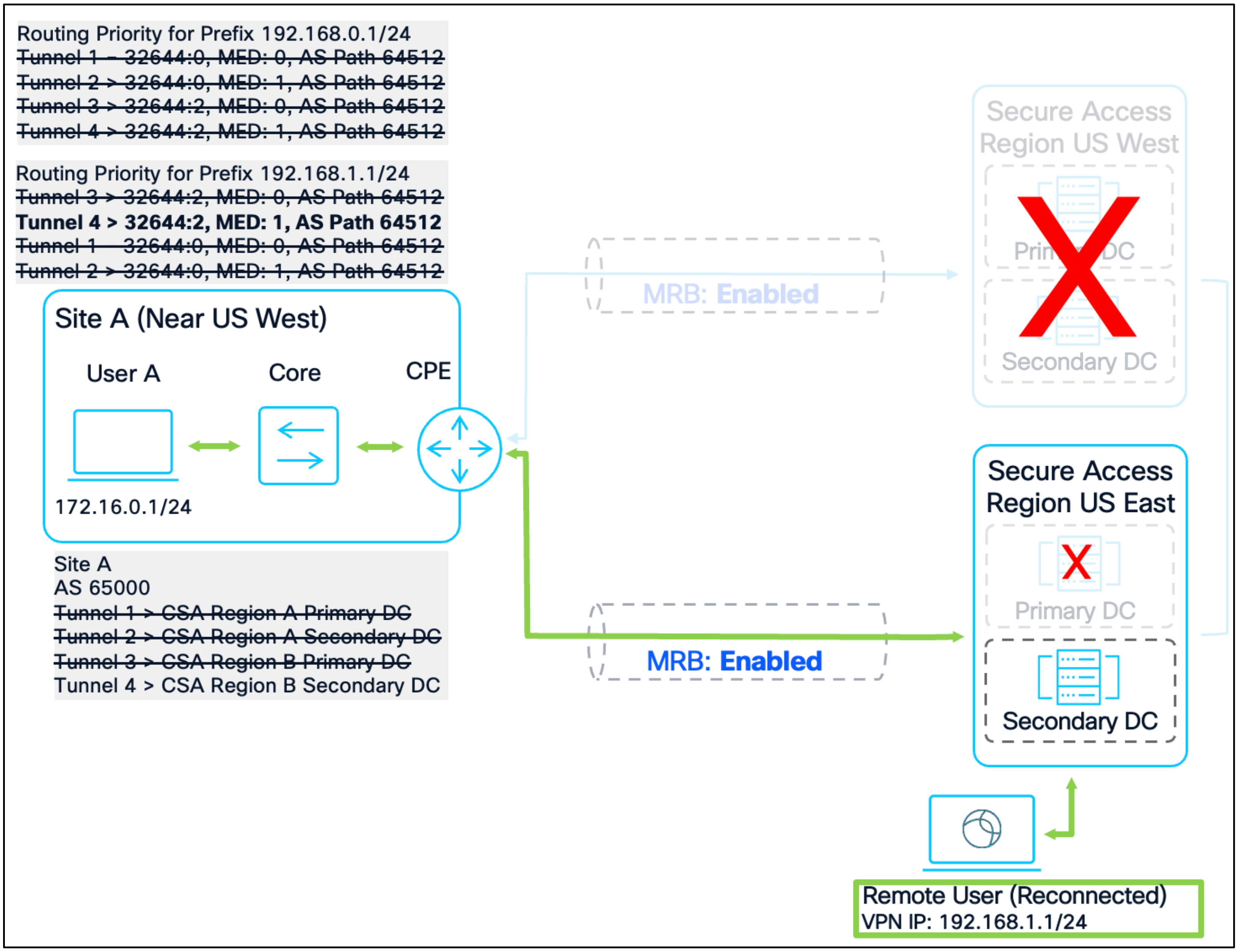

Routing Priority for Prefix 192.168.0.1/24
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512~~
~~Tunnel 2 > 32644:0, MED: 1, AS Path 64512~~
~~Tunnel 3 > 32644:2, MED: 0, AS Path 64512~~
~~Tunnel 4 > 32644:2, MED: 1, AS Path 64512~~
Routing Priority for Prefix 192.168.1.1/24
~~Tunnel 3 > 32644:2, MED: 0, AS Path 64512~~
Tunnel 4 > 32644:2, MED: 1, AS Path 64512
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512~~
~~Tunnel 2 > 32644:0, MED: 1, AS Path 64512~~
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
~~Tunnel 3 > CSA Region B Primary DC~~
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Pri DC
Secondary DC
X
Secure Access Region US East
X
Primary DC
Secondary DC
Remote User (Reconnected)
VPN IP: 192.168.1.1/24

Figure 14.
Remote Access Failover Test #4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.1.0/25   169.254.0.7              1    104    200  64512 i
 *>   192.168.1.128/25 169.254.0.7              1    104    200  64512 i
[omitted]
```

Multi-Region Secure Internet Redundancy

Multi-Region Secure Internet Access (SIA) redundancy ensures that critical security features such as Secure Web Gateway (SWG) and Data Loss Prevention (DLP) remain active even during a regional outage. Because most Secure Access regions provide direct internet egress, they typically tag the default route (0.0.0.0/0) with the "local" community string 32644:0.

Data Collection – Secure Internet Access

To analyze the default routing behavior, we use the show ip bgp command. Without route-maps, the router selects the best path based on the standard BGP tie-breakers.

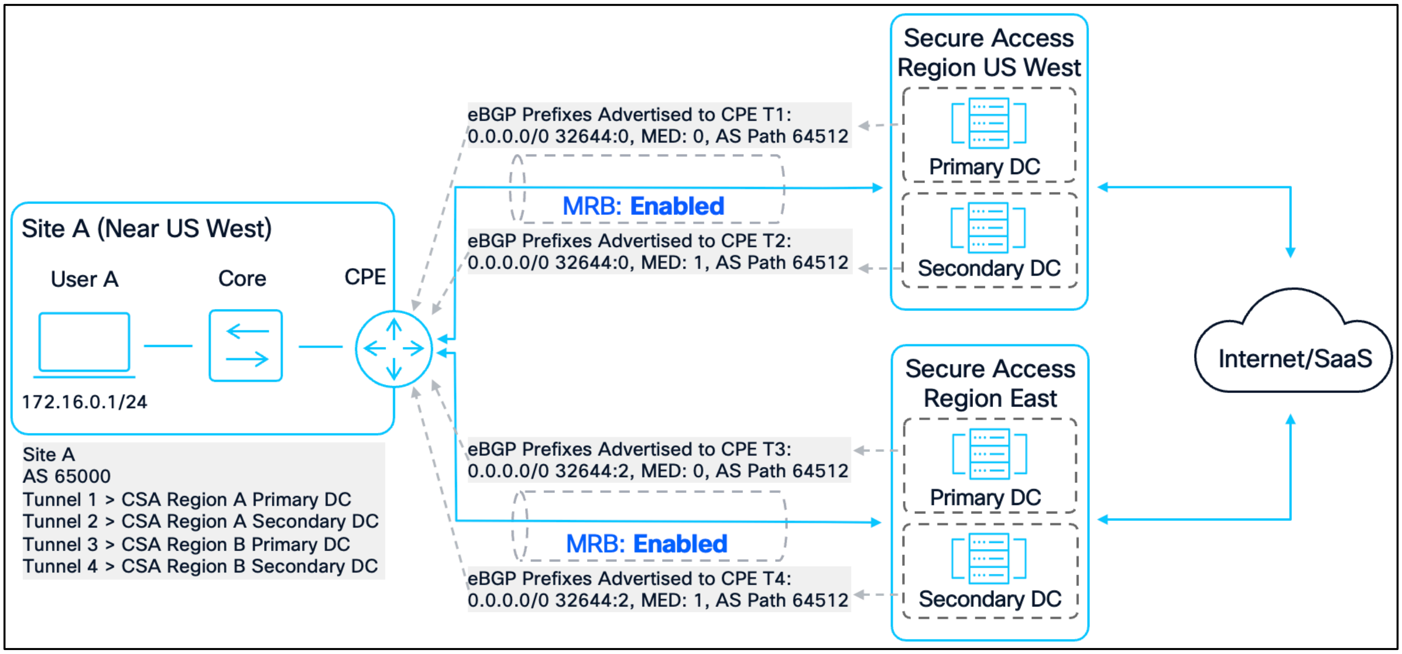

Secure Access Region US West
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
0.0.0.0/0 32644:0, MED: 0, AS Path 64512
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
0.0.0.0/0 32644:0, MED: 1, AS Path 64512
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
Internet/SaaS
Secure Access Region East
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T3:
0.0.0.0/0 32644:2, MED: 0, AS Path 64512
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
0.0.0.0/0 32644:2, MED: 1, AS Path 64512

Figure 15.
Secure Internet Access Scenario

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    0.0.0.0          169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
```

```
[omitted]
```

A detailed look at the prefix using show ip bgp 0.0.0.0 confirms that all four peers advertise the same community tag (32644:0). Because every data center identifies itself as a local exit for internet traffic, community-based weighting alone cannot prioritize one region over another.

```
show ip bgp 0.0.0.0
BGP routing table entry for 0.0.0.0/0, version 373
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 15:02:15 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 15:02:15 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 15:02:15 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 15:02:15 UTC
```

This creates a performance risk: if the primary tunnel in the closest region fails, the router may default to the primary tunnel of a distant region (US East) even if a secondary tunnel in the local region (US West) is still available. To prevent this suboptimal routing, we must ensure that the route-map implements Regional Weighting.

```
C8000V-SiteA#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

Configuration – Secure Internet Access

To correct this, we use the same configuration used for Remote Access Redundancy. The following configuration enforces regional affinity. By assigning unique weights to each tunnel, we ensure the router exhausts all local regional options before failing over to a backup region. The bolded commands are the only ones necessary for Secure Internet Access Redundancy.

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

The community-list and route-map configuration will work for both Sites A and B because they both have a regional preference for US West.

This exact route-map configuration would not be optimal for Sites C and D for Secure Internet Access Redundancy. Because Site C is closest to Secure Access region US East and Site D is closest to Secure Access region United Kingdom, their route-maps should be prioritizing routes to the region they are closest to. For example, on the Site C Router:

```
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
```

```
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
address-family ipv4
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

Validation – Secure Internet Access

To make sure that the route-map configuration works, each tunnel will be brought down starting with Tunnel 1. After each tunnel is brought down, the best route will be verified using the **show ip bgp** command.

Failover Test #1

In the baseline state with all tunnels active, Site A identifies the US West Primary DC as the best path. Site A assigns a weight of 203 to Tunnel 1, ensuring symmetric traffic flow through the Primary regional data center. The BGP table confirms this selection with the best-path symbol (>) indicating the Primary regional next hop.

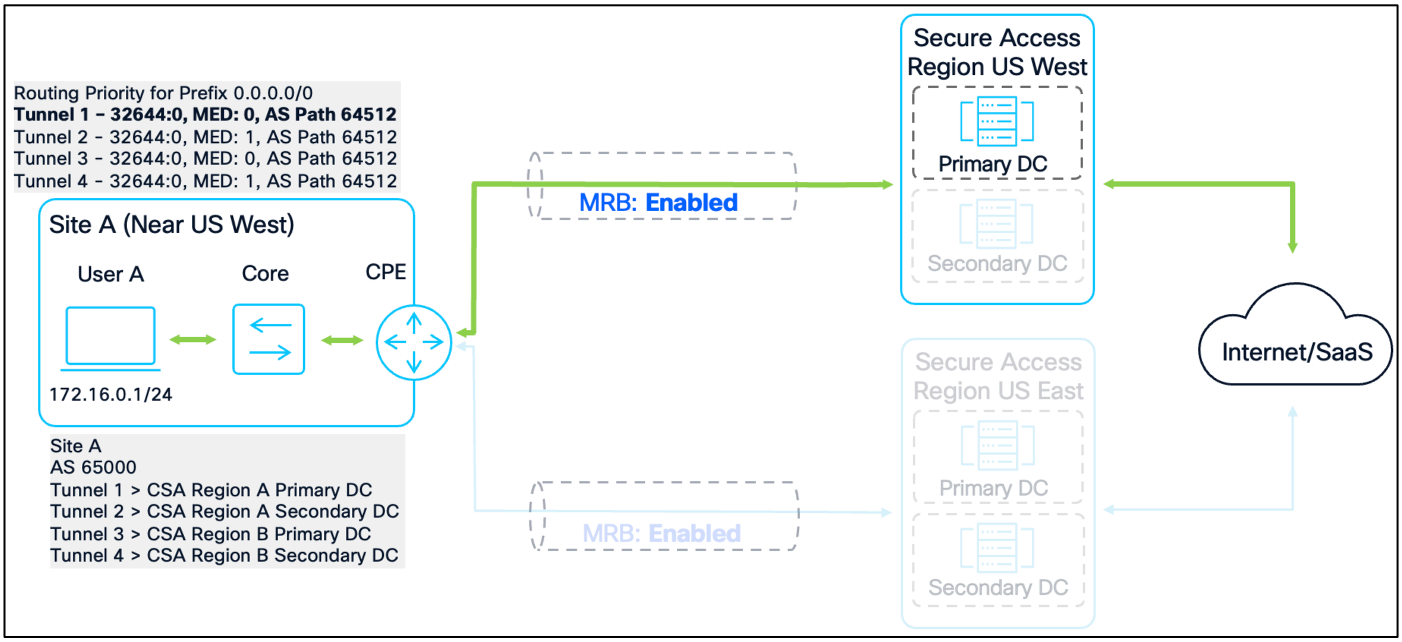
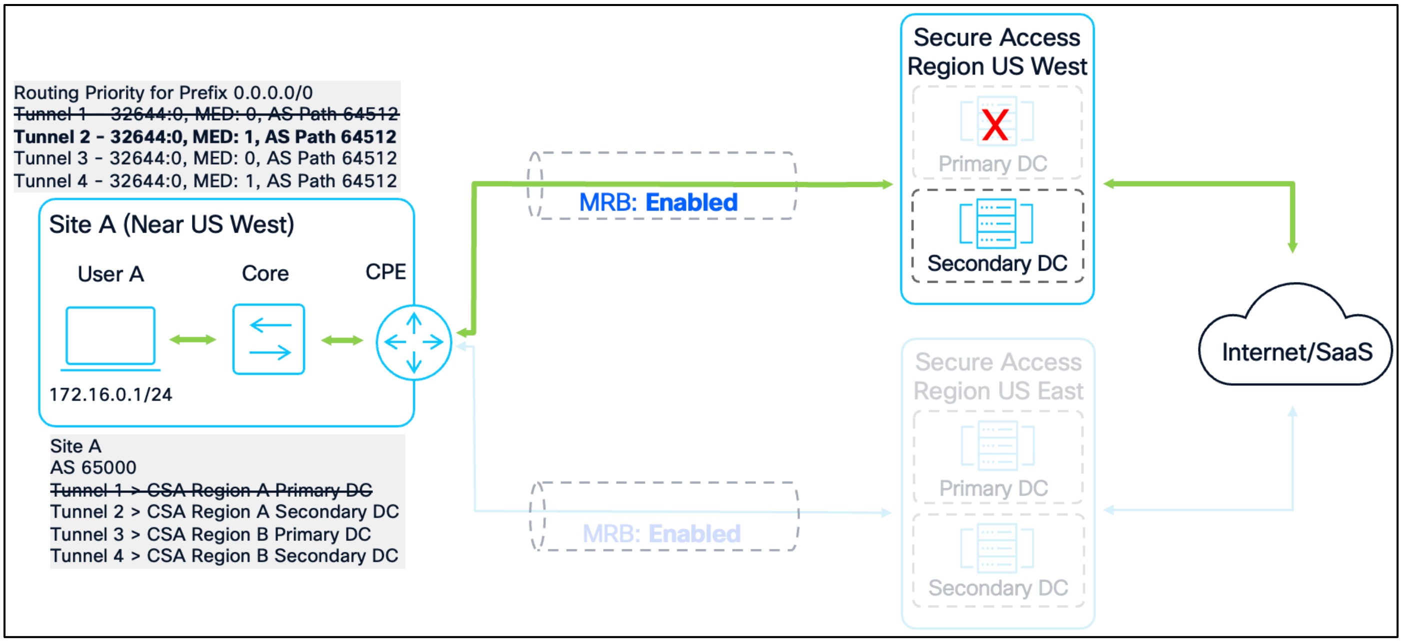

Routing Priority for Prefix 0.0.0.0/0
Tunnel 1 – 32644:0, MED: 0, AS Path 64512
Tunnel 2 – 32644:0, MED: 1, AS Path 64512
Tunnel 3 – 32644:0, MED: 0, AS Path 64512
Tunnel 4 – 32644:0, MED: 1, AS Path 64512
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Internet/SaaS

Figure 16.
Secure Internet Access Failover Test #1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    0.0.0.0          169.254.0.3              1    104    202 64512 i
 *                     169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
 *>                    169.254.0.1              0    104    203 64512 i
[omitted]
```

Failover Test #2

When the US West Primary DC experiences an outage and Tunnel 1 is disabled, the router re-evaluates the remaining paths. Site A now selects Tunnel 2, the US West Secondary DC, because the route-map assigns it a weight of 202. This weight is higher than the 201 assigned to the US East Primary DC, forcing the router to stay within the local region. This successfully overrides the default BGP behavior that would have preferred the distant region due to its lower Metric, thereby avoiding unnecessary latency.



Routing Priority for Prefix 0.0.0.0/0
~~Tunnel 1 - 32644:0, MED: 0, AS Path 64512~~
Tunnel 2 - 32644:0, MED: 1, AS Path 64512
Tunnel 3 - 32644:0, MED: 0, AS Path 64512
Tunnel 4 - 32644:0, MED: 1, AS Path 64512

Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Figure 17.
Secure Internet Access Failover Test #2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.3              1     104    202  64512 i
 *                     169.254.0.5              0     104    201  64512 i
 *                     169.254.0.7              1     104    200  64512 i
[omitted]
```

Failover Test #3

If the entire US West region fails, both routers fail over to the US East Primary DC via Tunnel 3. At this stage, Tunnel 3 carries the highest available weight of 201. The validation shows that these prefixes correctly hit the expected sequences in the route-map.

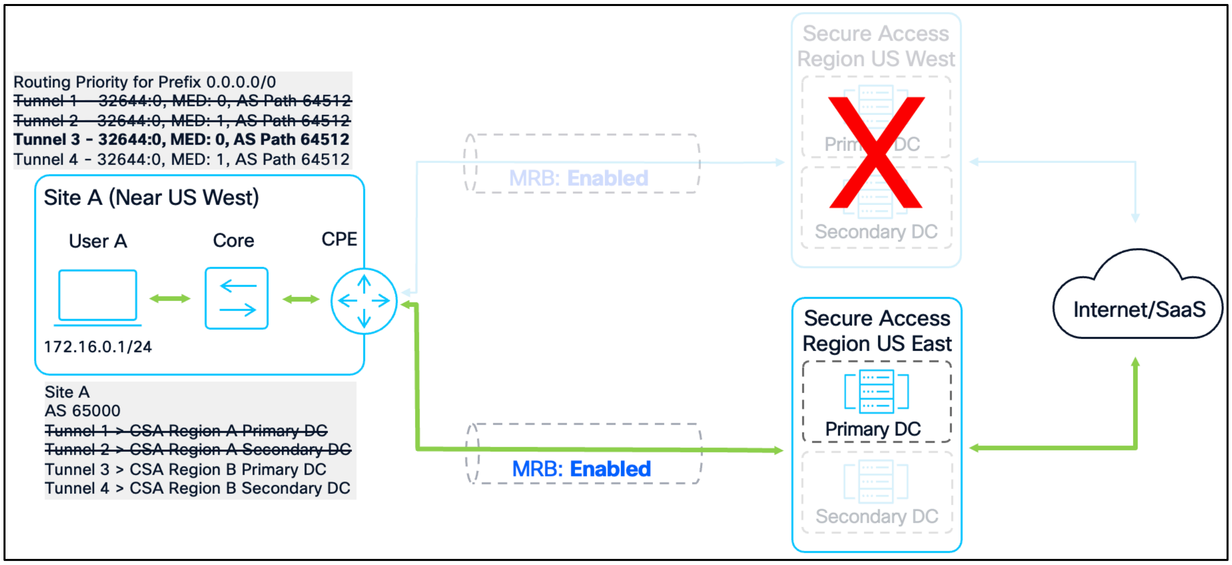

Routing Priority for Prefix 0.0.0.0/0
~~Tunnel 1 - 32644:0, MED: 0, AS Path 64512~~
~~Tunnel 2 - 32644:0, MED: 1, AS Path 64512~~
Tunnel 3 - 32644:0, MED: 0, AS Path 64512
Tunnel 4 - 32644:0, MED: 1, AS Path 64512
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Internet/SaaS

Figure 18.
Secure Internet Failover Test #3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
      Network          Next Hop            Metric LocPrf Weight Path
 *>    0.0.0.0          169.254.0.5              0    104    201  64512 i
 *                      169.254.0.7              1    104    200  64512 i
[omitted]
```

Failover Test #4

In the final failure scenario where only the US East Secondary DC remains functional, the routers install the path to Tunnel 4 with a weight of 200. The BGP table confirms that the routing policy remains robust and maintains a functional connection between sites as long as a single tunnel is established.

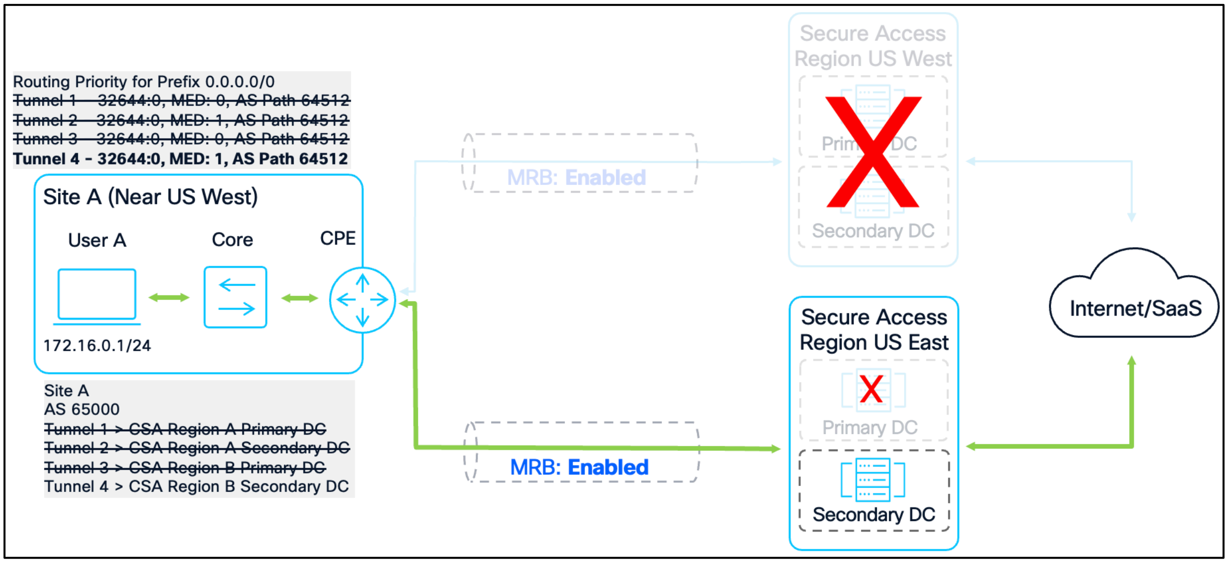

Routing Priority for Prefix 0.0.0.0/0
~~Tunnel 1 - 32644:0, MED: 0, AS Path 64512~~
~~Tunnel 2 - 32644:0, MED: 1, AS Path 64512~~
~~Tunnel 3 - 32644:0, MED: 0, AS Path 64512~~
Tunnel 4 - 32644:0, MED: 1, AS Path 64512
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
~~Tunnel 3 > CSA Region B Primary DC~~
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Internet/SaaS

Figure 19.
Secure Internet Access Failover Test #4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.7              1    104    200  64512 i
[omitted]
```

For Site C, which has US East as its Primary region, using the route-map configuration that prioritizes the US East region allows the router to prioritize prefixes from the US East Primary DC (169.254.0.25) followed by the US East Secondary DC (169.254.0.27). Internet traffic will only be forwarded to US West if both US East DCs go down.

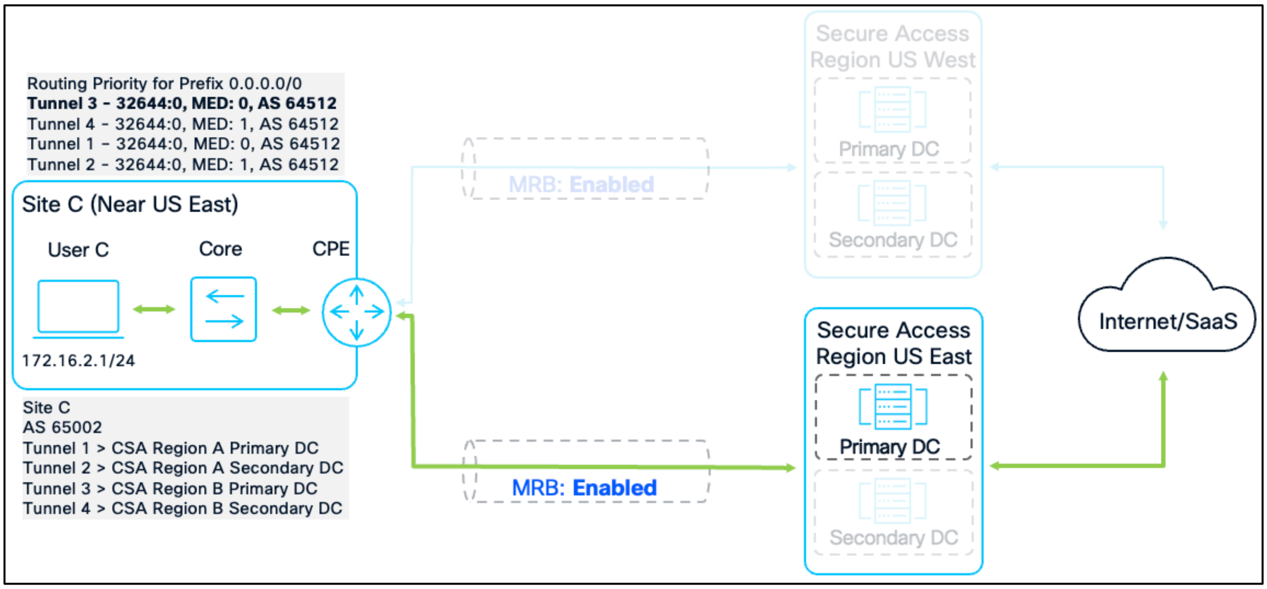

Routing Priority for Prefix 0.0.0.0/0
Tunnel 3 - 32644:0, MED: 0, AS 64512
Tunnel 4 - 32644:0, MED: 1, AS 64512
Tunnel 1 - 32644:0, MED: 0, AS 64512
Tunnel 2 - 32644:0, MED: 1, AS 64512
Site C (Near US East)
User C
Core
CPE
172.16.2.1/24
Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Internet/SaaS

Figure 20.
Site C Secure Internet Access Failover Test

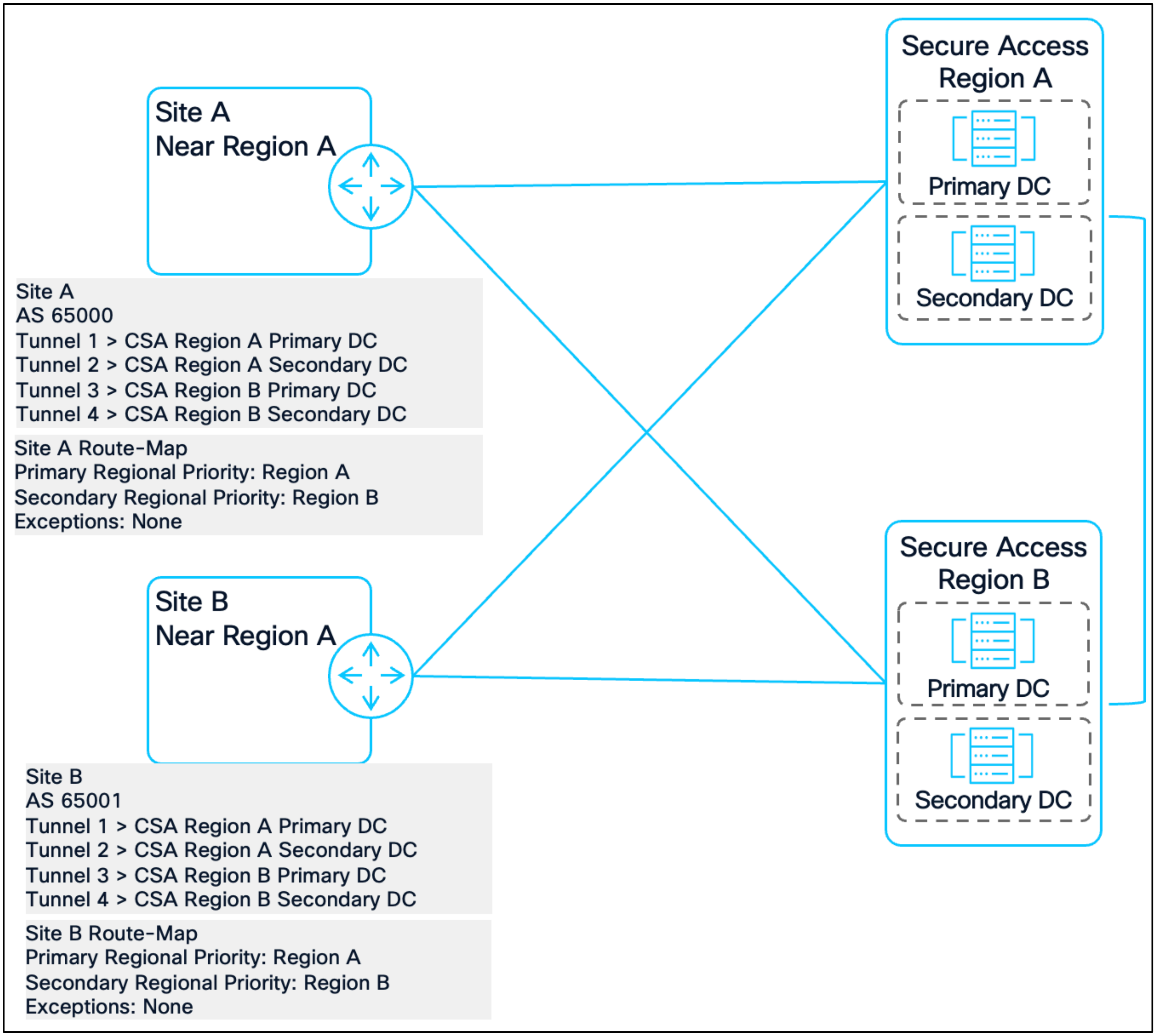
```
C8000V-SiteC# show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    0.0.0.0          169.254.0.23             1    104    200  64512 i
 *                     169.254.0.21             0    104    201  64512 i
 *>                    169.254.0.25             0    104    203  64512 i
 *                     169.254.0.27             1    104    202  64512 i
[omitted]
```

Multi-Region Site to Site Redundancy

The final component of a resilient architecture is Multi-Region Site-to-Site Redundancy. This ensures that users and devices at branch locations maintain persistent access to applications hosted in data centers and private clouds. Site-to-site traffic patterns generally fall into one of three architectural conditions:

Same Primary and Secondary region

This condition occurs when two sites share identical Primary and Secondary Secure Access regions. In this scenario, routers utilize Regional Weighting to manage traffic flow. The configuration prioritizes the Primary region for all inter-site communication, ensuring symmetric paths. Traffic only fails over to the Secondary region if all Primary regional connections are lost.



Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Site A Route-Map
Primary Regional Priority: Region A
Secondary Regional Priority: Region B
Exceptions: None

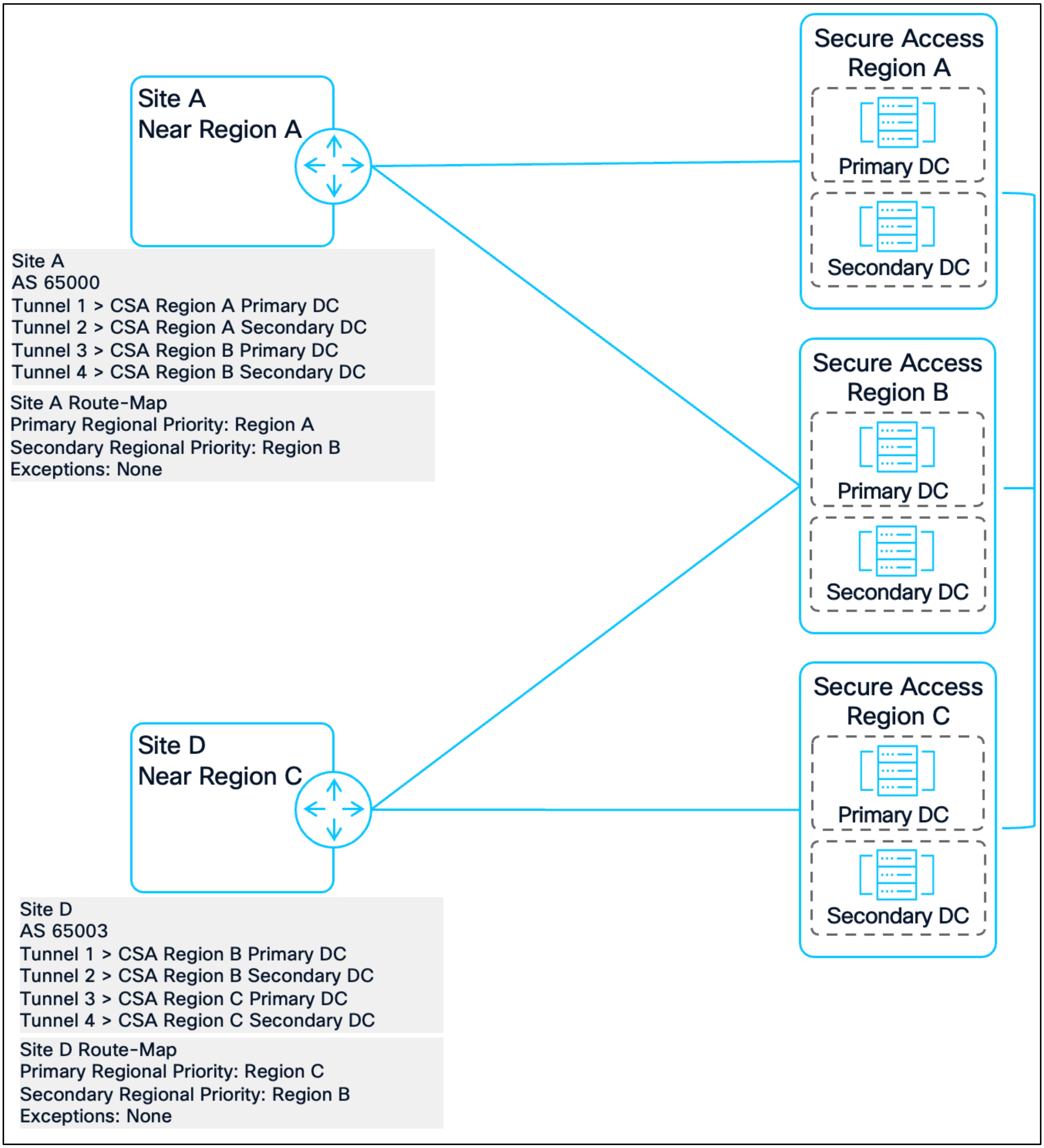
Site B
AS 65001
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Site B Route-Map
Primary Regional Priority: Region A
Secondary Regional Priority: Region B
Exceptions: None

Figure 21.
Same Primary and Secondary region Site to Site Scenario

Distinct Primary or Secondary

This condition applies when sites are assigned to different Primary or Secondary Secure Access regions. Routers leverage Community String Weighting to determine the most efficient regional proximity. By prioritizing the community string with the lowest value, the network prevents asymmetric routing and ensures traffic transits the Secure Access region closest to the source and destination.



Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Site A Route-Map
Primary Regional Priority: Region A
Secondary Regional Priority: Region B
Exceptions: None

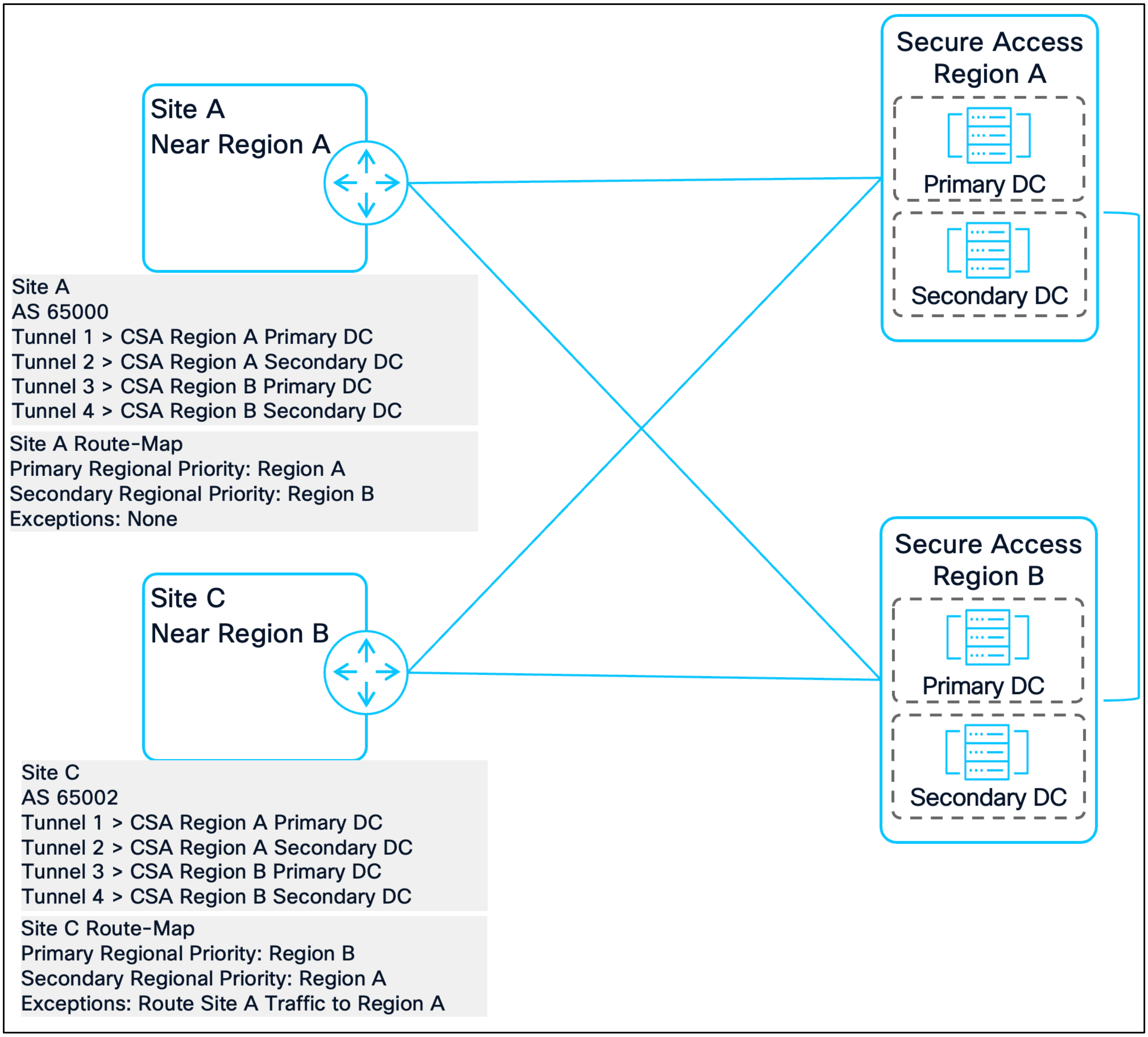
Site D
AS 65003
Tunnel 1 > CSA Region B Primary DC
Tunnel 2 > CSA Region B Secondary DC
Tunnel 3 > CSA Region C Primary DC
Tunnel 4 > CSA Region C Secondary DC

Site D Route-Map
Primary Regional Priority: Region C
Secondary Regional Priority: Region B
Exceptions: None

Figure 22.
Distinct Primary or Secondary region Site to Site Scenario

Swapped Primary and Secondary region

In this scenario, the regional priorities are inverted: Site A's Primary region is Site C's Secondary region, and vice versa. Because Secure Access advertises prefixes to both sites with the same "local" community string (32644:0), standard regional weighting would cause each site to prefer its own local region. This conflict results in asymmetric routing (e.g., Site A sends via Region 1, but Site C responds via Region 2). To maintain path symmetry, a specific routing exception must be implemented to align the sites on a common transit region.



Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Site A Route-Map
Primary Regional Priority: Region A
Secondary Regional Priority: Region B
Exceptions: None

Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Site C Route-Map
Primary Regional Priority: Region B
Secondary Regional Priority: Region A
Exceptions: Route Site A Traffic to Region A

Figure 23.
Swapped Primary and Secondary region Site to Site Scenario

The following sections provide a detailed analysis and configuration for each of these conditions.

Data Collection – Site to Site (Same Primary and Secondary region)

To verify the preferred routes, the IOS-XE command **show ip bgp** is used on both the Site A and Site B router. Here, we are interested in the routes advertised between the two sites. Routes advertised by Site A will have the AS number 65000 in the AS path, while routes advertised by Site B will have the AS number 65001 in the AS path. For brevity, the prefixes not pertaining to traffic between the two sites have been removed from the output.

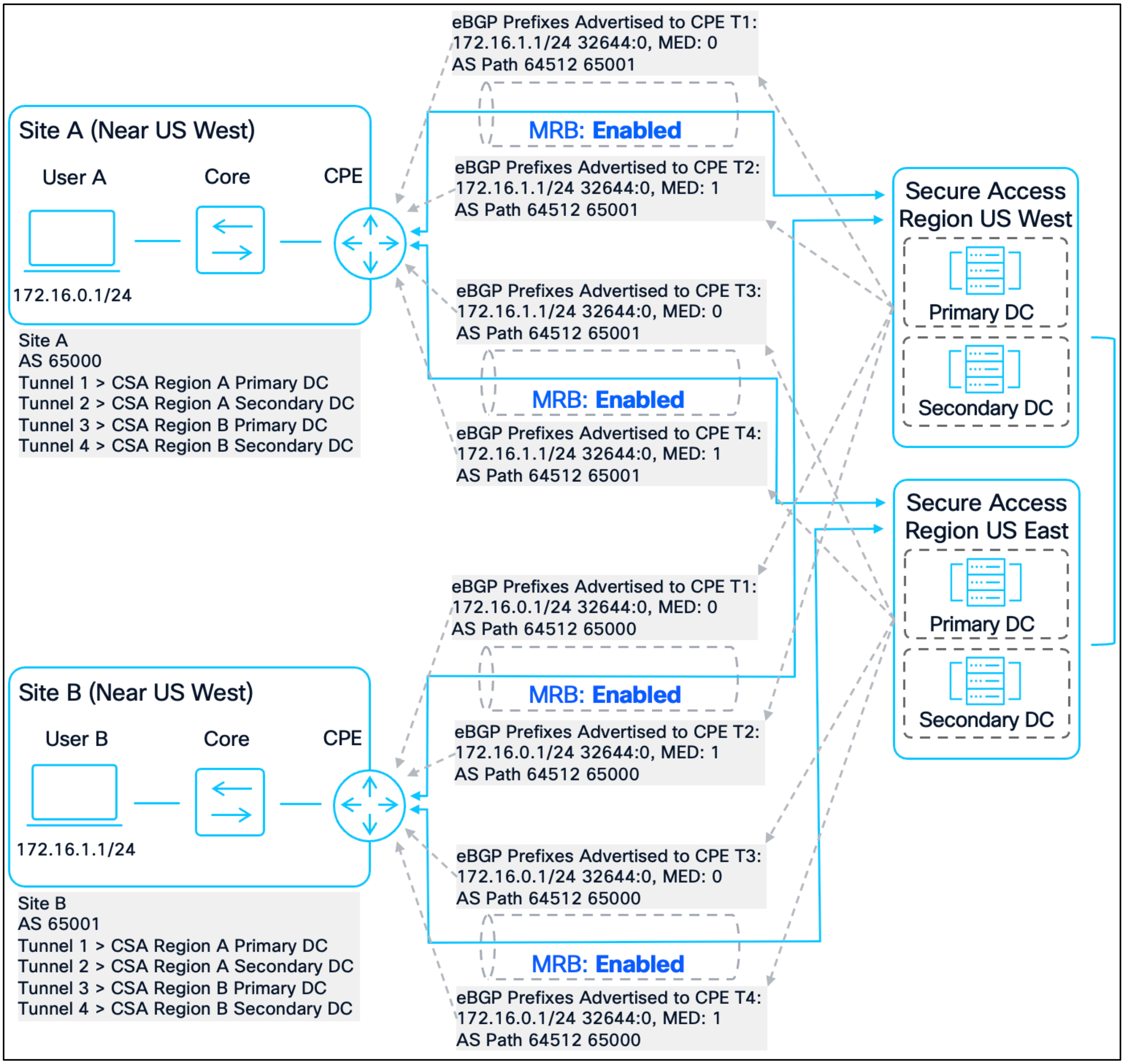

eBGP Prefixes Advertised to CPE T1:
172.16.1.1/24 32644:0, MED: 0
AS Path 64512 65001
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
172.16.1.1/24 32644:0, MED: 1
AS Path 64512 65001
eBGP Prefixes Advertised to CPE T3:
172.16.1.1/24 32644:0, MED: 0
AS Path 64512 65001
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
172.16.1.1/24 32644:0, MED: 1
AS Path 64512 65001
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
172.16.0.1/24 32644:0, MED: 0
AS Path 64512 65000
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
172.16.0.1/24 32644:0, MED: 1
AS Path 64512 65000
eBGP Prefixes Advertised to CPE T3:
172.16.0.1/24 32644:0, MED: 0
AS Path 64512 65000
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
172.16.0.1/24 32644:0, MED: 1
AS Path 64512 65000
Site B (Near US West)
User B
Core
CPE
172.16.1.1/24
Site B
AS 65001
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Figure 24.
Site to Site Same Primary and Secondary region Topology

Without route-map intervention, both routers prefer Tunnel 1 (US West Primary) by default. However, if this primary tunnel fails, the BGP selection algorithm will prefer the US East Primary DC (Metric 0) over the US West Secondary DC (Metric 1). While this maintains symmetry, it results in suboptimal routing by directing traffic to a distant region while a closer regional data center is still available.

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.1.0/24    169.254.0.5              0             0 64512 65001 i
 *>                    169.254.0.1              0             0 64512 65001 i
 *                     169.254.0.3              1             0 64512 65001 i
 *                     169.254.0.7              1             0 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.15             0             0 64512 65000 i
 *                     169.254.0.17             1             0 64512 65000 i
 *>                    169.254.0.11             0             0 64512 65000 i
 *                     169.254.0.13             1             0 64512 65000 i
[omitted]
```

A detailed inspection using show ip bgp [prefix] reveals that Secure Access tags all four paths with the same community string: 32644:0. Because these tags are identical across both the primary and Secondary regions, community-based weighting alone cannot distinguish between them. This necessitates the use of regional weighting to enforce proximity-based failover.

```
C8000V-SiteA#show ip bgp 172.16.1.0
BGP routing table entry for 172.16.1.0/24, version 701
Paths: (4 available, best #1, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  64512 65001
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 17:04:08 UTC
  Refresh Epoch 1
  64512 65001
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:34 UTC
  Refresh Epoch 1
  64512 65001
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:29 UTC
  Refresh Epoch 1
  64512 65001
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:53:37 UTC
C8000V-SiteB#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 258
Paths: (4 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65000
    169.254.0.11 from 169.254.0.11 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 17:04:09 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.15 from 169.254.0.15 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:36 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.17 from 169.254.0.17 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:50:42 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.13 from 169.254.0.13 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:30 UTC
```

Shutting down Tunnel 1 on both sites confirms the suboptimal routing behavior. As shown in the updated BGP tables, both routers select the US East Primary DC as the best path (>), bypassing the geographically closer US West Secondary DC.

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.5             0             0 64512 65001 i
 *                     169.254.0.3             1             0 64512 65001 i
 *                     169.254.0.7             1             0 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.15            0             0 64512 65000 i
 *                     169.254.0.17            1             0 64512 65000 i
 *                     169.254.0.13            1             0 64512 65000 i
[omitted]
```

Configuration – Site to Site (Same Primary and Secondary region)

To correct this, the same configuration used in earlier sections is used. Because both sites have a regional preference for the same Secure Access region (US West) and have the same Secondary region preference (US East), all routes between the two sites will be tagged with 32644:0. Since all inter-site prefixes are tagged with the "local" community string 32644:0, the router relies on Regional Weighting to ensure the Primary region is fully utilized before failing over to the Secondary region. The bolded commands indicate what is relevant for this site-to-site condition.

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
```

```
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

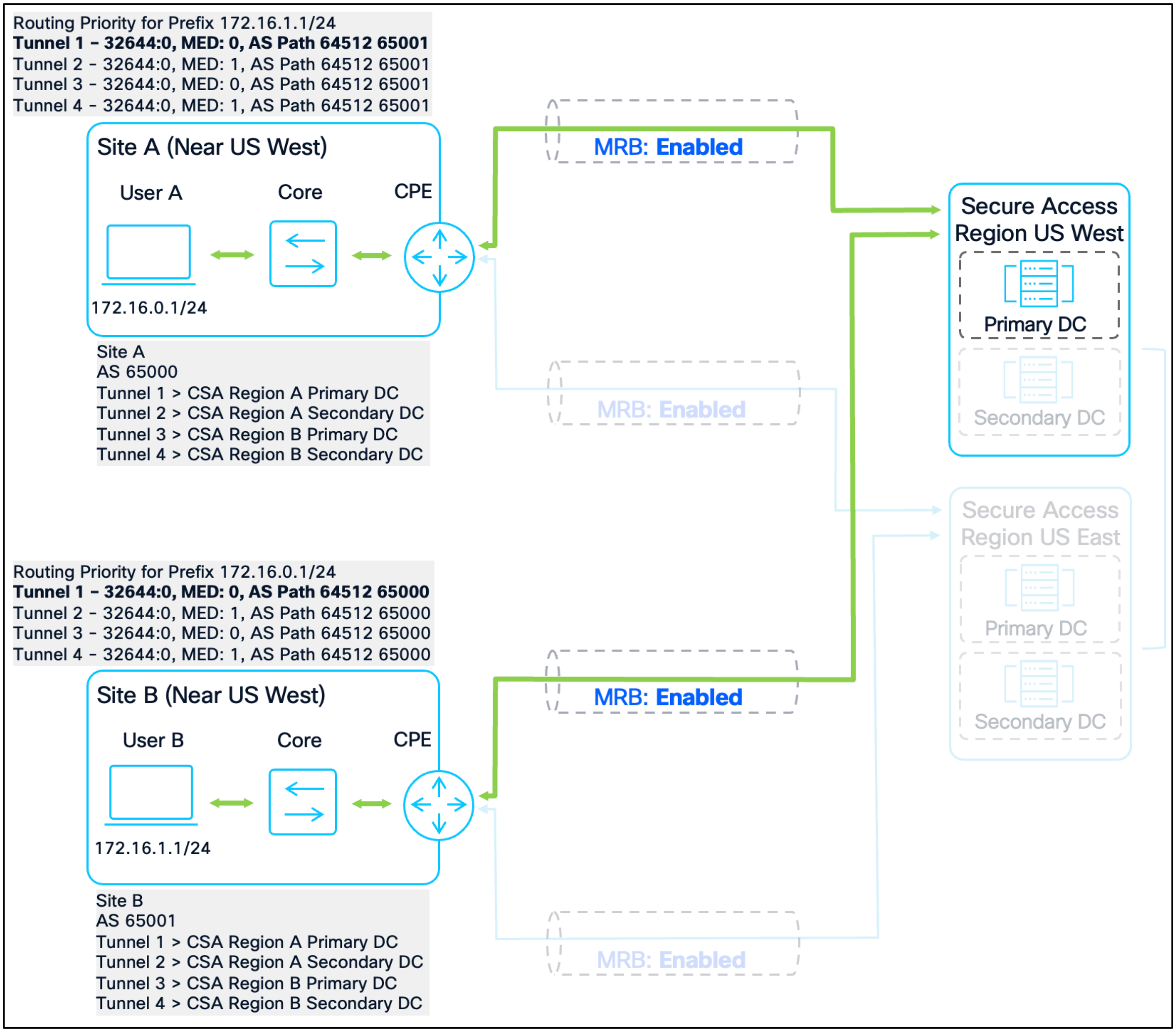
The community-list and route-map configuration will work for both Site A and B because they both have a regional preference for US West and share the same Secondary region US East.

Validation – Site to Site (Same Primary and Secondary region)

To make sure that the route-map configuration works, each tunnel will be brought down starting with Tunnel 1. After each tunnel is brought down, the best route will be verified using the **show ip bgp** command.

Failover Test #1

Under normal operating conditions where all tunnels are active, both routers identify the US West Primary DC as the best path. Site A and Site B both assign a weight of 203 to Tunnel 1, ensuring symmetric traffic flow through the Primary regional data center. The BGP table confirms this selection with the best-path symbol indicating the next hop associated with the Primary region.



Routing Priority for Prefix 172.16.1.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65001
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65001
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65001
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65001
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000
Site B (Near US West)
User B
Core
CPE
172.16.1.1/24
Site B
AS 65001
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled

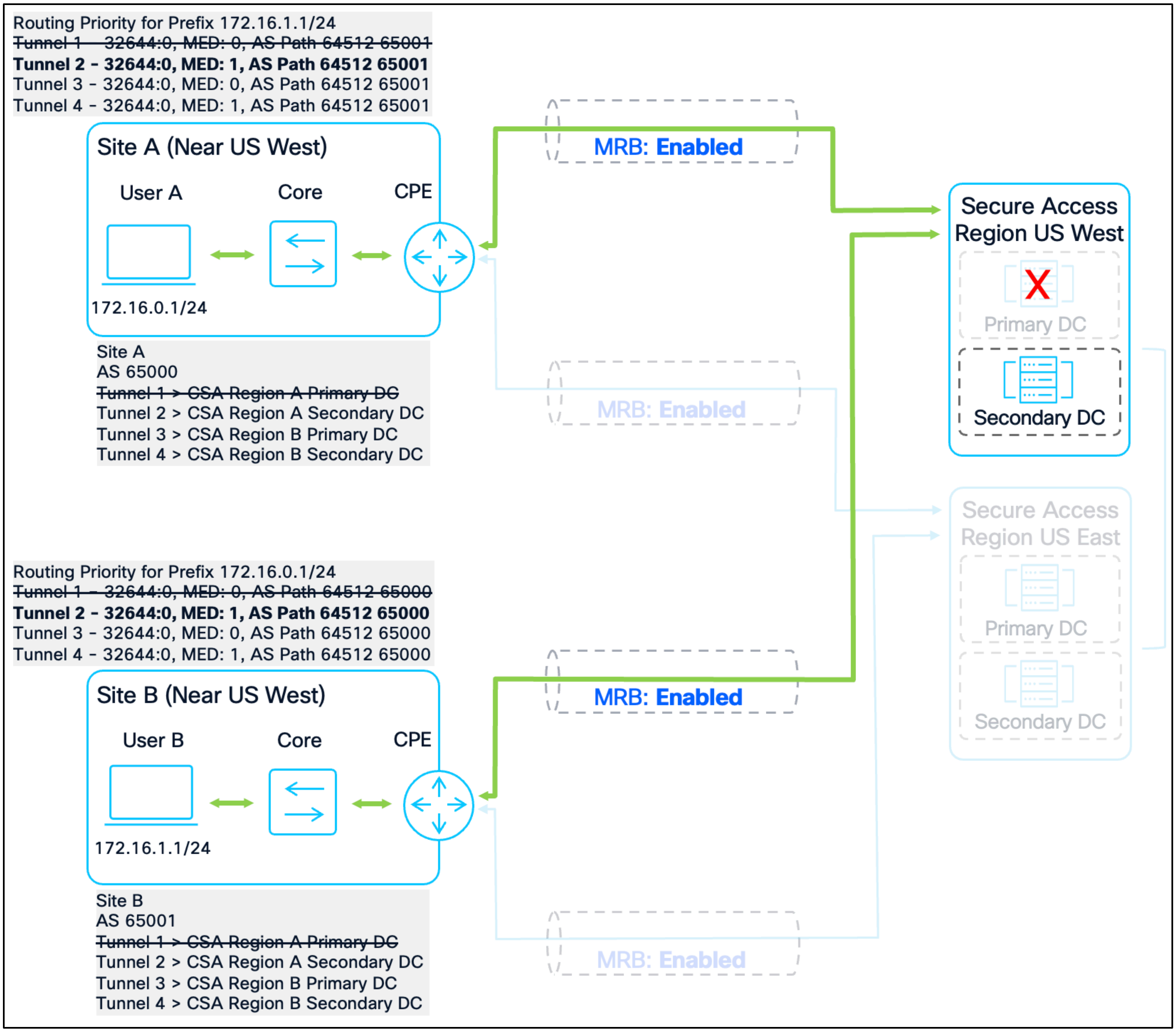
Figure 25.
Site to Site Same Primary and Secondary region Failover Test #1

```
C8000V-SiteA#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.1              0    104    203 64512 65001 i
 *                     169.254.0.5              0    104    201 64512 65001 i
 *                     169.254.0.3              1    104    202 64512 65001 i
 *                     169.254.0.7              1    104    200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.11             0    104    203 64512 65000 i
 *                     169.254.0.15             0    104    201 64512 65000 i
 *                     169.254.0.17             1    104    200 64512 65000 i
 *                     169.254.0.13             1    104    202 64512 65000 i
[omitted]
```

Failover Test #2

In the event of an outage at the US West Primary DC, Tunnel 1 is disabled on both sites. The routers then fail over to the US West Secondary DC via Tunnel 2. Because the route-map assigns a weight of 202 to the secondary tunnel in the Primary region, which is higher than the weight of 201 assigned to the primary tunnel in the Secondary region, the routers maintain regional symmetry. This successfully overrides the default BGP behavior that would have otherwise preferred the US East Primary DC due to its lower Metric (0 vs 1).



Routing Priority for Prefix 172.16.1.1/24
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65001~~
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65001
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65001
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65001

Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Routing Priority for Prefix 172.16.0.1/24
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65000~~
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000

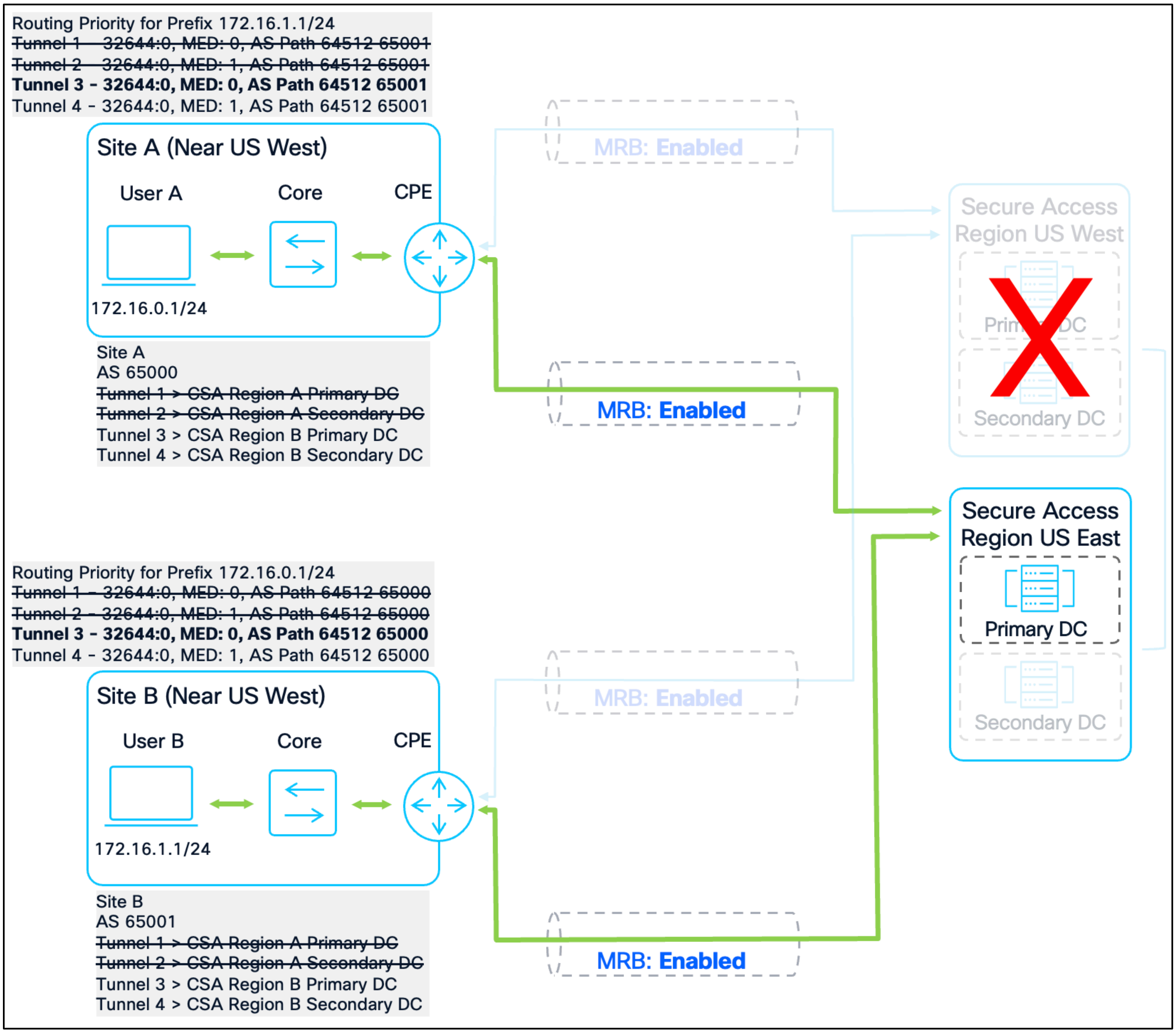
Site B
AS 65001
~~Tunnel 1 > CSA Region A Primary DC~~
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Figure 26.
Site to Site Same Primary and Secondary region Failover Test #2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.1.0/24    169.254.0.5              0     104     201  64512  65001 i
 *>                    169.254.0.3              1     104     202  64512  65001 i
 *                     169.254.0.7              1     104     200  64512  65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.0.0/24     169.254.0.15            0     104     201  64512  65000  i
 *                       169.254.0.17            1     104     200  64512  65000  i
 *>                      169.254.0.13            1     104     202  64512  65000  i
[omitted]
```

Failover Test #3

If the entire US West region experiences an outage, both Tunnel 1 and Tunnel 2 are disabled. The routers then fail over to the US East Primary DC via Tunnel 3. At this stage, Tunnel 3 carries the highest available weight of 201. The BGP table confirms that the best-path selection has moved to the US East path on both routers, maintaining symmetric connectivity through the Secondary region.



Routing Priority for Prefix 172.16.1.1/24
~~Tunnel 1 - 32644:0, MED: 0, AS Path 64512 65001~~
~~Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65001~~
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65001
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65001
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Prim DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
~~Tunnel 1 - 32644:0, MED: 0, AS Path 64512 65000~~
~~Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000~~
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000
Site B (Near US West)
User B
Core
CPE
172.16.1.1/24
Site B
AS 65001
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled

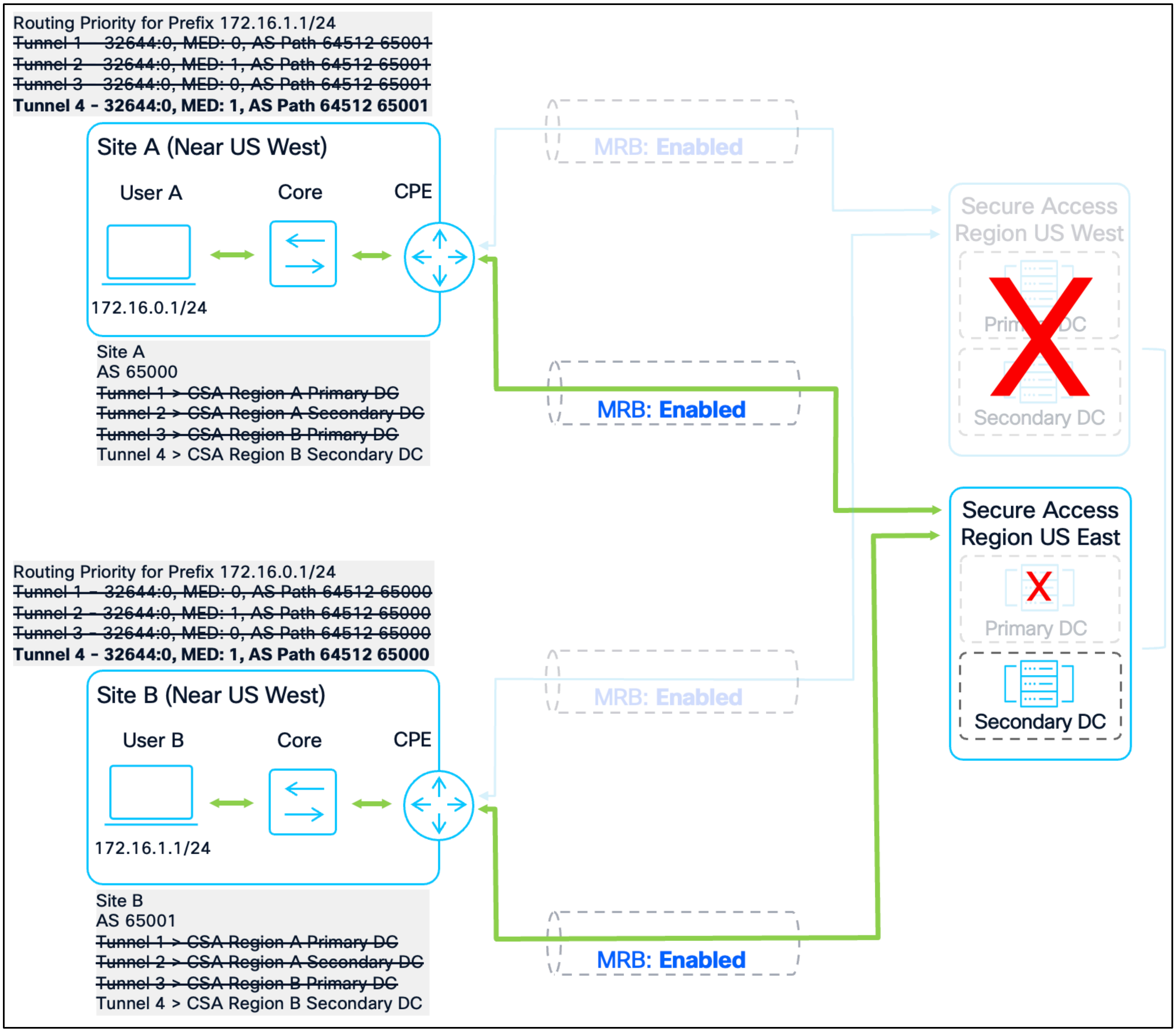
Figure 27.
Site to Site Same Primary and Secondary region Failover Test #3

```
C8000V-SiteA#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.5              0    104    201 64512 65001 i
 *                     169.254.0.7              1    104    200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.15             0    104    201 64512 65000 i
 *                     169.254.0.17             1    104    200 64512 65000 i
[omitted]
```

Failover Test #4

In the final failure scenario where the US West region and the US East Primary DC are both unavailable, only Tunnel 4 remains active. The routers install the path to the US East Secondary DC with a weight of 200. While this represents a total regional failover, the BGP table shows that connectivity is preserved through the last remaining functional tunnel, ensuring that site-to-site traffic continues to flow.



Routing Priority for Prefix 172.16.1.1/24
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65001~~
~~Tunnel 2 – 32644:0, MED: 1, AS Path 64512 65001~~
~~Tunnel 3 – 32644:0, MED: 0, AS Path 64512 65001~~
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65001

Site A
AS 65000
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
~~Tunnel 3 > CSA Region B Primary DC~~
Tunnel 4 > CSA Region B Secondary DC

Routing Priority for Prefix 172.16.0.1/24
~~Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65000~~
~~Tunnel 2 – 32644:0, MED: 1, AS Path 64512 65000~~
~~Tunnel 3 – 32644:0, MED: 0, AS Path 64512 65000~~
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000

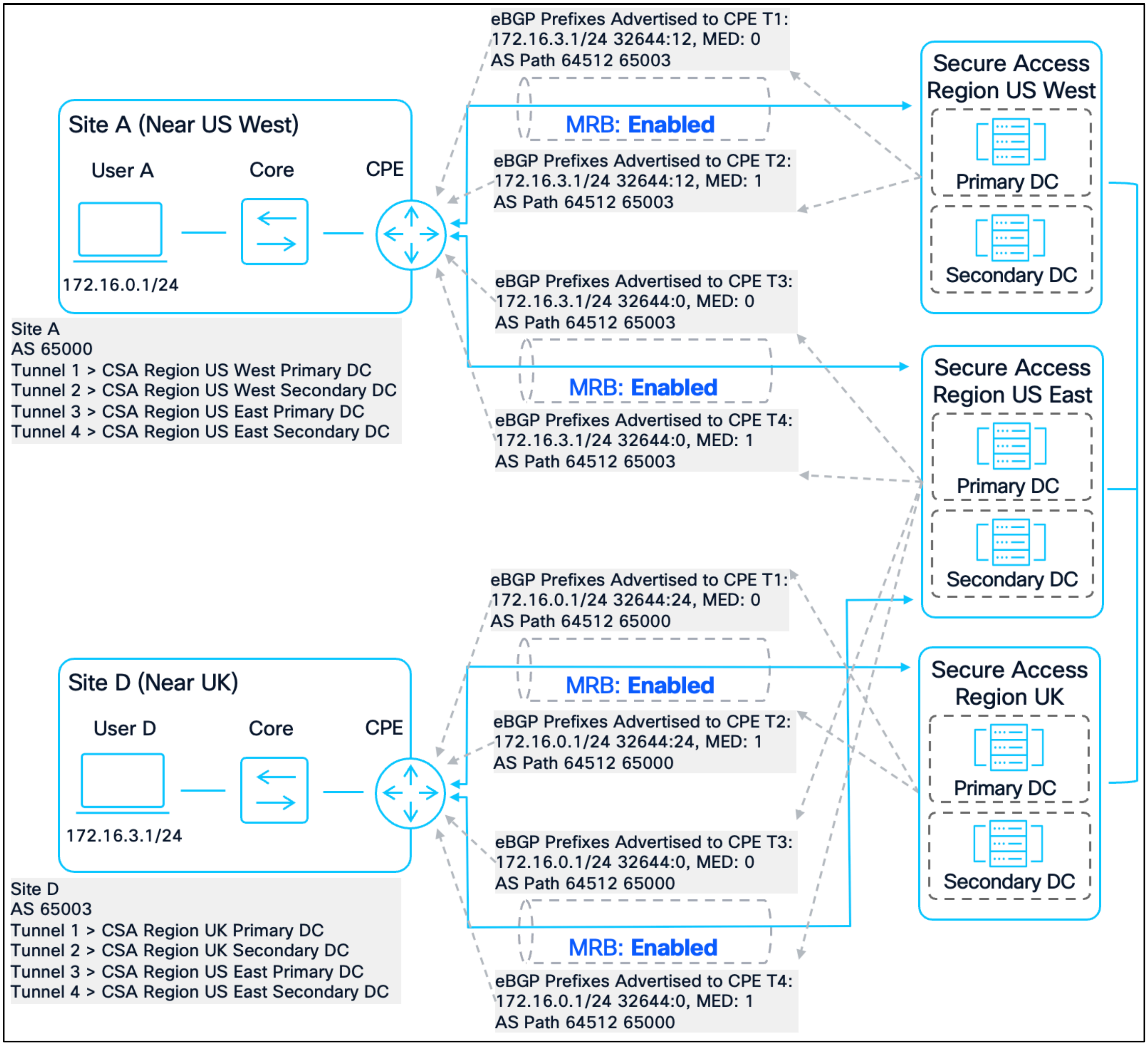
Site B
AS 65001
~~Tunnel 1 > CSA Region A Primary DC~~
~~Tunnel 2 > CSA Region A Secondary DC~~
~~Tunnel 3 > CSA Region B Primary DC~~
Tunnel 4 > CSA Region B Secondary DC

Figure 28.
Site to Site Same Primary and Secondary region Failover Test #4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.7              1     104     200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.17             1     104     200 64512 65000 i
[omitted]
```

Data Collection – Site to Site (Distinct Primary or Secondary region)

To verify the preferred routes, the IOS-XE command **show ip bgp** is used on both the Site A and Site D router. We are interested in the routes advertised between the two sites. Routes advertised by Site A will have the AS number 65000 in the AS path, while routes advertised by Site D will have the AS number 65003 in the AS path. For brevity, the prefixes not pertaining to traffic between the two sites have been removed from the output.



eBGP Prefixes Advertised to CPE T1:
172.16.3.1/24 32644:12, MED: 0
AS Path 64512 65003
Secure Access
Region US West
Primary DC
Secondary DC
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
172.16.3.1/24 32644:12, MED: 1
AS Path 64512 65003
eBGP Prefixes Advertised to CPE T3:
172.16.3.1/24 32644:0, MED: 0
AS Path 64512 65003
Site A
AS 65000
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
172.16.3.1/24 32644:0, MED: 1
AS Path 64512 65003
Secure Access
Region US East
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
172.16.0.1/24 32644:24, MED: 0
AS Path 64512 65000
Site D (Near UK)
User D
Core
CPE
172.16.3.1/24
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
172.16.0.1/24 32644:24, MED: 1
AS Path 64512 65000
Secure Access
Region UK
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T3:
172.16.0.1/24 32644:0, MED: 0
AS Path 64512 65000
Site D
AS 65003
Tunnel 1 > CSA Region UK Primary DC
Tunnel 2 > CSA Region UK Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
172.16.0.1/24 32644:0, MED: 1
AS Path 64512 65000

Figure 29.
Site to Site Distinct Primary or Secondary region Topology

Without route-map intervention, both routers default to Tunnel 1 (their respective local Primary regions). However, Secure Access utilizes "hot potato routing," where traffic is handed off to the destination as quickly as possible within the fabric.

Because both sites are connected to US East, traffic sent from Site A via US West will likely exit the Secure Access fabric at the US East data center to reach Site D. If Site D responds via its own Primary region (UK), the return traffic will exit the fabric at the US East data center to reach Site A. This results in an asymmetric path where the transit regions differ for the forward and return flows.

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.3.0/24    169.254.0.5              0             0 64512 65003 i
 *                     169.254.0.3              1             0 64512 65003 i
 *>                    169.254.0.1              0             0 64512 65003 i
 *                     169.254.0.7              1             0 64512 65003 i
C8000V-SiteD#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.35             0             0 64512 65000 i
 *                     169.254.0.37             1             0 64512 65000 i
 *                     169.254.0.33             1             0 64512 65000 i
 *>                    169.254.0.31             0             0 64512 65000 i
```

A detailed inspection using show ip bgp [prefix] confirms that the shared US East region is closer from the perspective of the Secure Access backbone. On both routers, the prefixes received via US East are tagged with the local community string 32644:0, while the Primary regional tunnels are tagged as more distant.

- Site A: US East is tagged 32644:0 (Local), while US West is tagged 32644:12 (Distant).
- Site D: US East is tagged 32644:0 (Local), while the UK region is tagged 32644:24 (Distant).

```
C8000V-SiteA#show ip bgp 172.16.3.0
BGP routing table entry for 172.16.3.0/24, version 932
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  64512 65003
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:43:28 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:12
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:43:23 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:12
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 05:43:17 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:42:45 UTC
C8000V-SiteD#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 322
Paths: (4 available, best #4, table default)
  Flag: 0x8100
  Not advertised to any peer
  Refresh Epoch 1
  64512 65000
    169.254.0.35 from 169.254.0.35 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:48:27 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.37 from 169.254.0.37 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:48:22 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.33 from 169.254.0.33 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:24
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:48:21 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.31 from 169.254.0.31 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:24
      rx pathid: 0, tx pathid: 0x0
```

To ensure symmetric and optimal routing, the community strings must be weighed appropriately. By prioritizing the 32644:0 tag, both sites will prefer the shared US East region for inter-site traffic, aligning the entry and exit points within the Secure Access fabric.

Configuration – Site to Site (Distinct Primary or Secondary region)

The route-map configuration used for Site A will be modified slightly. The configuration for Site A is updated to include community 32644:12, which represents the regional distance to Site D’s Primary region from US West. This will weigh the prefixes correctly for appropriate routing. The bolded commands are the only ones necessary for this site-to-site condition.

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12

route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

Site D requires a unique configuration tailored to its Primary region in the UK. This site uses community 32644:24 to identify the regional distance to Site A. Like the Site A configuration, Site D is weighted to prefer the shared US East region (32644:0) for inter-site traffic, ensuring that both ends of the connection align on the same transit data center.

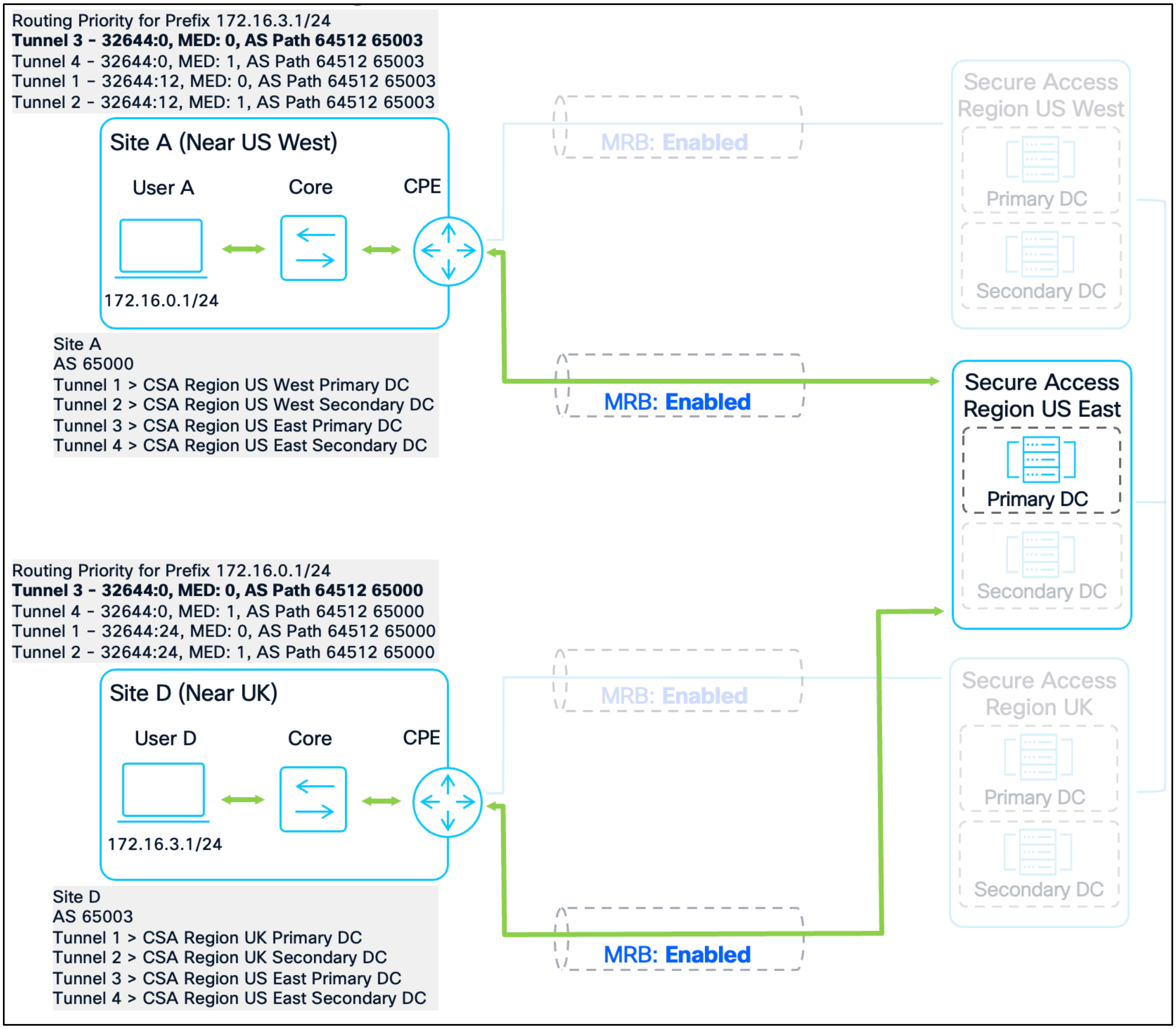
```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-24 permit 32644:24
route-map UK1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map UK1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 103
route-map UK1-INBOUND permit 100
 set weight 53
route-map UK2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map UK2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 102
route-map UK2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65003
address-family ipv4
  neighbor 169.254.0.31 route-map UK1-INBOUND in
  neighbor 169.254.0.33 route-map UK2-INBOUND in
  neighbor 169.254.0.35 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.37 route-map US-EAST2-INBOUND in
 exit-address-family
```

Validation – Site to Site (Distinct Primary or Secondary region)

To verify the effectiveness of the route-map configuration and ensure symmetric traffic flow, a sequential failover test was performed by disabling tunnels one by one. This process confirms that the BGP best-path selection follows the intended weight hierarchy and that the routers correctly prioritize the shared US East region to maintain optimal performance.

Failover Test #1

In the baseline state with all tunnels active, both routers identify the US East Primary DC as the most efficient path. Secure Access tags prefixes via US East with the local community string 32644:0, which receives a higher weight than the more geographically distant Primary regions. Consequently, Site A selects Tunnel 3 with a weight of 301 and Site D selects Tunnel 3 with a weight of 201, resulting in symmetric routing through the shared US East region.



Routing Priority for Prefix 172.16.3.1/24
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65003
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65003
Tunnel 1 - 32644:12, MED: 0, AS Path 64512 65003
Tunnel 2 - 32644:12, MED: 1, AS Path 64512 65003
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 1 - 32644:24, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:24, MED: 1, AS Path 64512 65000
Site D (Near UK)
User D
Core
CPE
172.16.3.1/24
Site D
AS 65003
Tunnel 1 > CSA Region UK Primary DC
Tunnel 2 > CSA Region UK Secondary DC
Tunnel 3 > CSA Region US East Primary DC
Tunnel 4 > CSA Region US East Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region UK
Primary DC
Secondary DC

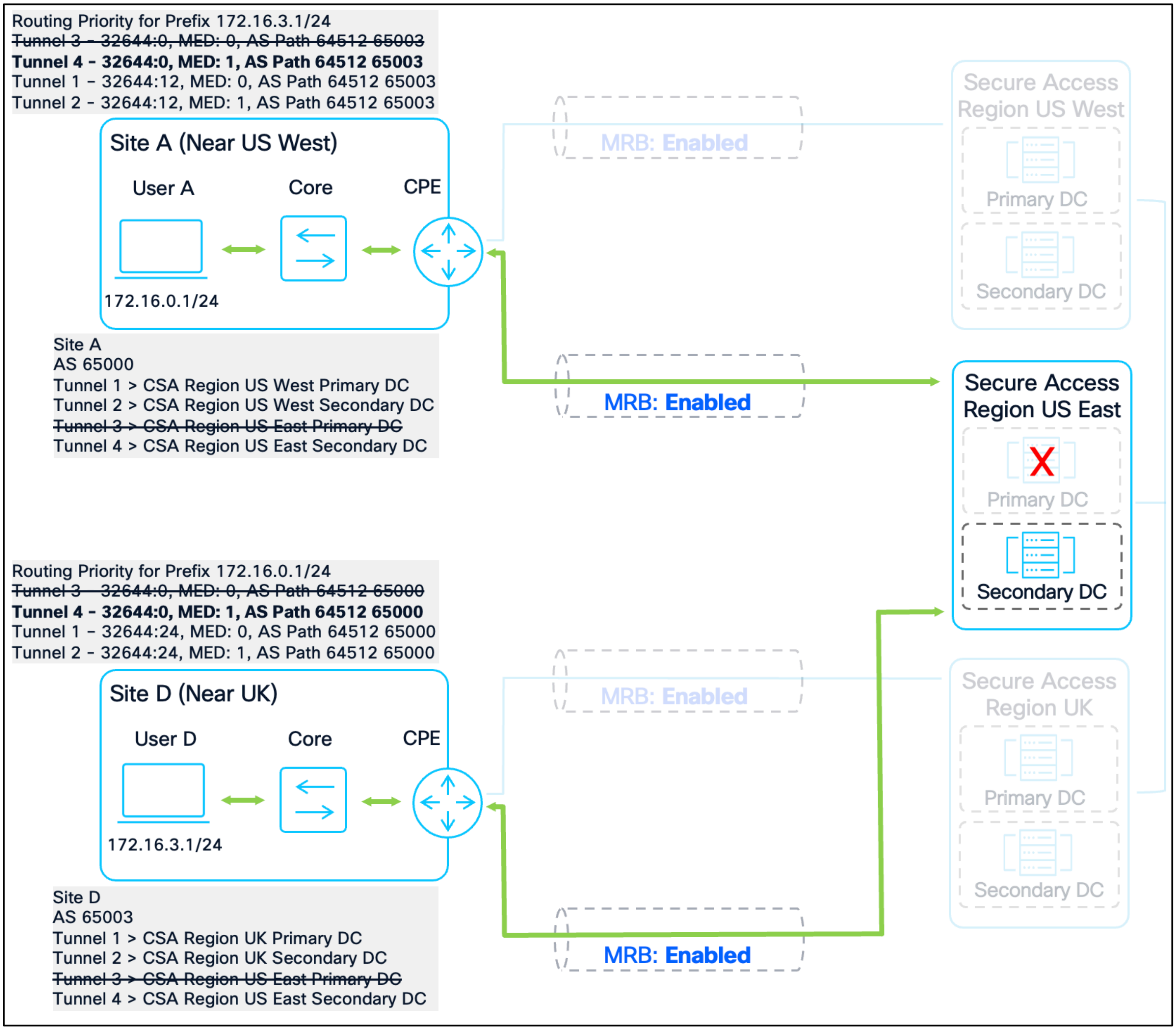
Figure 30.
Site to Site Distinct Primary or Secondary region Failover Test #1

```
C8000V-SiteA#show ip bgp

[…header omitted…]

     Network          Next Hop            Metric LocPrf Weight Path

 *>   172.16.3.0/24    169.254.0.5              0     106     301  64512  65003  i

 *                     169.254.0.3              1     102     102  64512  65003  i

 *                     169.254.0.1              0     102     103  64512  65003  i

 *                     169.254.0.7              1     106     300  64512  65003  i

[omitted]

C8000V-SiteD#show ip bgp

[…header omitted…]
```

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.35             0    104    201 64512 65000 i
 *                     169.254.0.33             1    102    102 64512 65000 i
 *                     169.254.0.31             0    102    103 64512 65000 i
 *                     169.254.0.37             1    104    200 64512 65000 i
[omitted]
```

Failover Test #2

When the US East Primary DC experiences an outage and Tunnel 3 is disabled, both sites automatically fail over to the US East Secondary DC via Tunnel 4. The weight hierarchy ensures that the secondary tunnel within the shared region remains preferred over the distant Primary regions, maintaining symmetric routing through US East.



Routing Priority for Prefix 172.16.3.1/24
~~Tunnel 3 – 32644:0, MED: 0, AS Path 64512 65003~~
Tunnel 4 – 32644:0, MED: 1, AS Path 64512 65003
Tunnel 1 – 32644:12, MED: 0, AS Path 64512 65003
Tunnel 2 – 32644:12, MED: 1, AS Path 64512 65003

Site A
AS 65000
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
~~Tunnel 3 > CSA Region US East Primary DC~~
Tunnel 4 > CSA Region US East Secondary DC

Routing Priority for Prefix 172.16.0.1/24
~~Tunnel 3 – 32644:0, MED: 0, AS Path 64512 65000~~
Tunnel 4 – 32644:0, MED: 1, AS Path 64512 65000
Tunnel 1 – 32644:24, MED: 0, AS Path 64512 65000
Tunnel 2 – 32644:24, MED: 1, AS Path 64512 65000

Site D
AS 65003
Tunnel 1 > CSA Region UK Primary DC
Tunnel 2 > CSA Region UK Secondary DC
~~Tunnel 3 > CSA Region US East Primary DC~~
Tunnel 4 > CSA Region US East Secondary DC

Figure 31.
Site to Site Distinct Primary or Secondary region Failover Test #2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.3.0/24    169.254.0.3              1    102    102 64512 65003 i
 *                     169.254.0.1              0    102    103 64512 65003 i
 *>                    169.254.0.7              1    106    300 64512 65003 i
[omitted]
C8000V-SiteD#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.33             1    102    102 64512 65000 i
 *                     169.254.0.31             0    102    103 64512 65000 i
 *>                    169.254.0.37             1    104    200 64512 65000 i
[omitted]
```

Failover Test #3

If the entire US East region becomes unavailable, both sites fall back to their respective local Primary regions. In this scenario, Site A utilizes US West while Site D utilizes the UK region. A technical observation during this test shows that the community strings shift to values such as 32644:26 and 32644:20. Since these specific tags were not explicitly defined in the route-maps, the prefixes hit the catch-all sequence at the end of the configuration. Site A selects Tunnel 1 and Site D selects Tunnel 1, both with a catch-all weight of 53. This demonstrates how traffic transits the Secure Access backbone between US West and the UK, highlighting the necessity of the catch-all permit statement for maintaining connectivity during major regional outages.

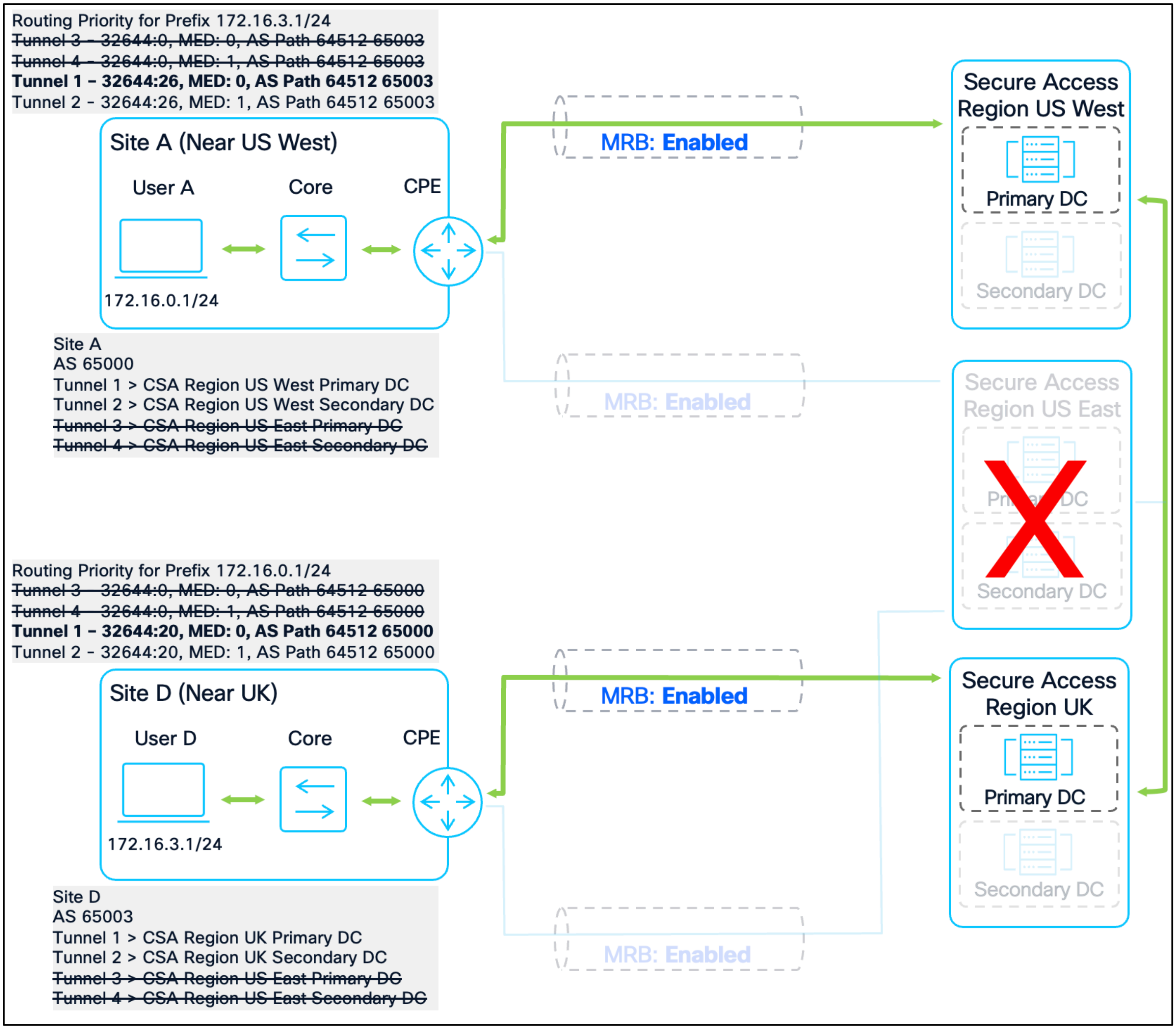

Routing Priority for Prefix 172.16.3.1/24
~~Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65003~~
~~Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65003~~
Tunnel 1 - 32644:26, MED: 0, AS Path 64512 65003
Tunnel 2 - 32644:26, MED: 1, AS Path 64512 65003
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region US West Primary DC
Tunnel 2 > CSA Region US West Secondary DC
~~Tunnel 3 > CSA Region US East Primary DC~~
~~Tunnel 4 > CSA Region US East Secondary DC~~
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
~~Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000~~
~~Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000~~
Tunnel 1 - 32644:20, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:20, MED: 1, AS Path 64512 65000
Site D (Near UK)
User D
Core
CPE
172.16.3.1/24
Site D
AS 65003
Tunnel 1 > CSA Region UK Primary DC
Tunnel 2 > CSA Region UK Secondary DC
~~Tunnel 3 > CSA Region US East Primary DC~~
~~Tunnel 4 > CSA Region US East Secondary DC~~
MRB: Enabled
MRB: Enabled
Secure Access Region UK
Primary DC
Secondary DC

Figure 32.
Site to Site Distinct Primary or Secondary region Failover Test #3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.3.0/24     169.254.0.3            1             52  64512  65003  i
 *>                      169.254.0.1            0             53  64512  65003  i
[omitted]
C8000V-SiteD#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.0.0/24     169.254.0.33           1             52  64512  65000  i
 *>                    169.254.0.31            0            53 64512 65000 i
[omitted]
C8000V-SiteA#show ip bgp 172.16.3.0
BGP routing table entry for 172.16.3.0/24, version 209
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65003
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, weight 52, valid, external
      Community: 32644:26
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 09:07:35 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, weight 53, valid, external, best
      Community: 32644:26
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 09:07:35 UTC
C8000V-SiteD#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 546
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  64512 65000
    169.254.0.33 from 169.254.0.33 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, weight 52, valid, external
      Community: 32644:20
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 09:07:40 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.31 from 169.254.0.31 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, weight 53, valid, external, best
      Community: 32644:20
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 09:07:40 UTC
```

Failover Test #4

During total degradation where only the secondary data centers for the distant regions remain functional, both routers successfully install the final available path. Site A selects the US West Secondary tunnel and Site D selects the UK Secondary tunnel. Connectivity is preserved over the Secure Access backhaul.

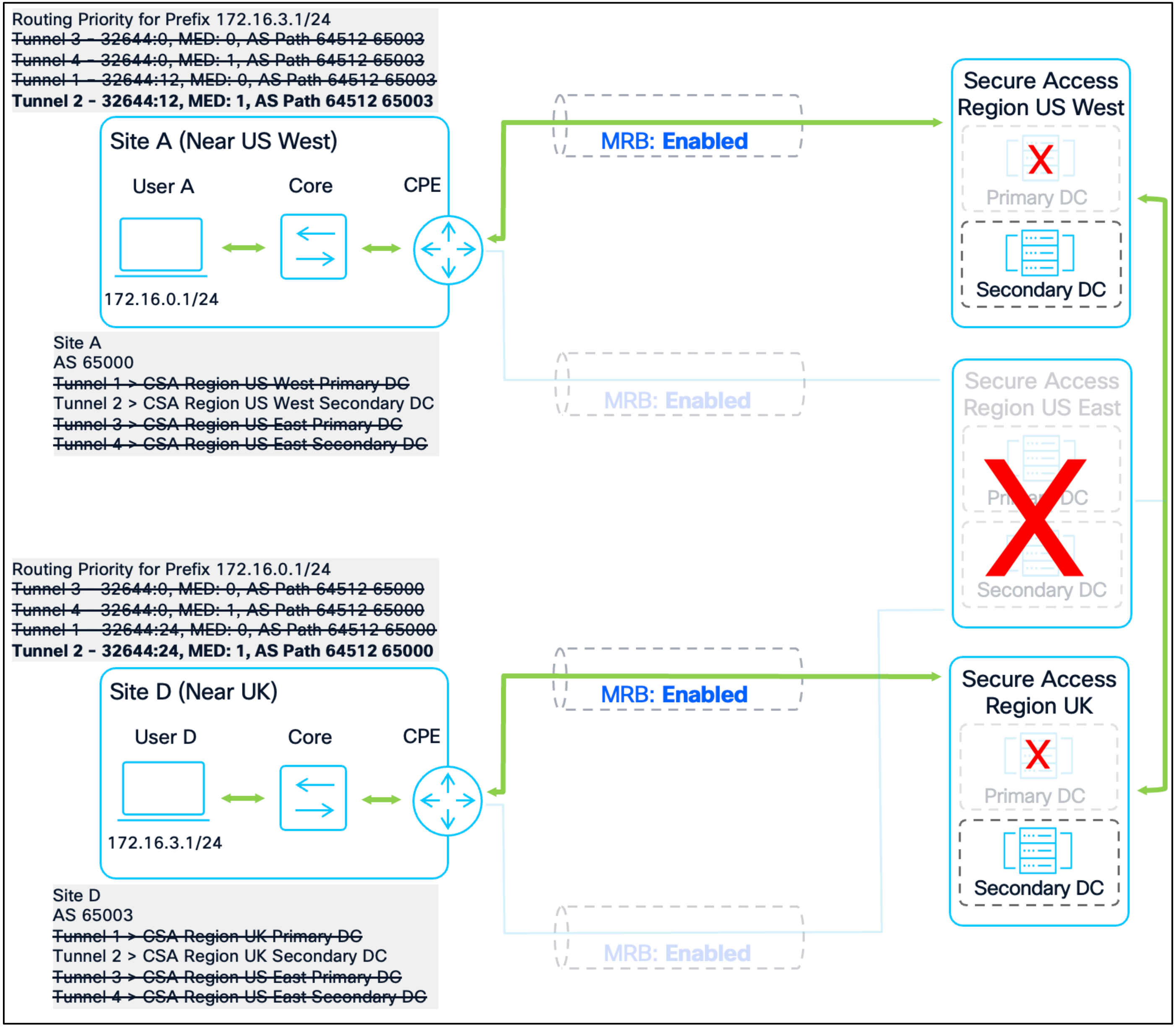

Routing Priority for Prefix 172.16.3.1/24
~~Tunnel 3 – 32644:0, MED: 0, AS Path 64512 65003~~
~~Tunnel 4 – 32644:0, MED: 1, AS Path 64512 65003~~
~~Tunnel 1 – 32644:12, MED: 0, AS Path 64512 65003~~
Tunnel 2 - 32644:12, MED: 1, AS Path 64512 65003
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
~~Tunnel 1 > CSA Region US West Primary DC~~
Tunnel 2 > CSA Region US West Secondary DC
~~Tunnel 3 > CSA Region US East Primary DC~~
~~Tunnel 4 > CSA Region US East Secondary DC~~
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
~~Tunnel 3 – 32644:0, MED: 0, AS Path 64512 65000~~
~~Tunnel 4 – 32644:0, MED: 1, AS Path 64512 65000~~
~~Tunnel 1 – 32644:24, MED: 0, AS Path 64512 65000~~
Tunnel 2 - 32644:24, MED: 1, AS Path 64512 65000
Site D (Near UK)
User D
Core
CPE
172.16.3.1/24
Site D
AS 65003
~~Tunnel 1 > CSA Region UK Primary DC~~
Tunnel 2 > CSA Region UK Secondary DC
~~Tunnel 3 > CSA Region US East Primary DC~~
~~Tunnel 4 > CSA Region US East Secondary DC~~
MRB: Enabled
MRB: Enabled
Secure Access Region UK
Primary DC
Secondary DC

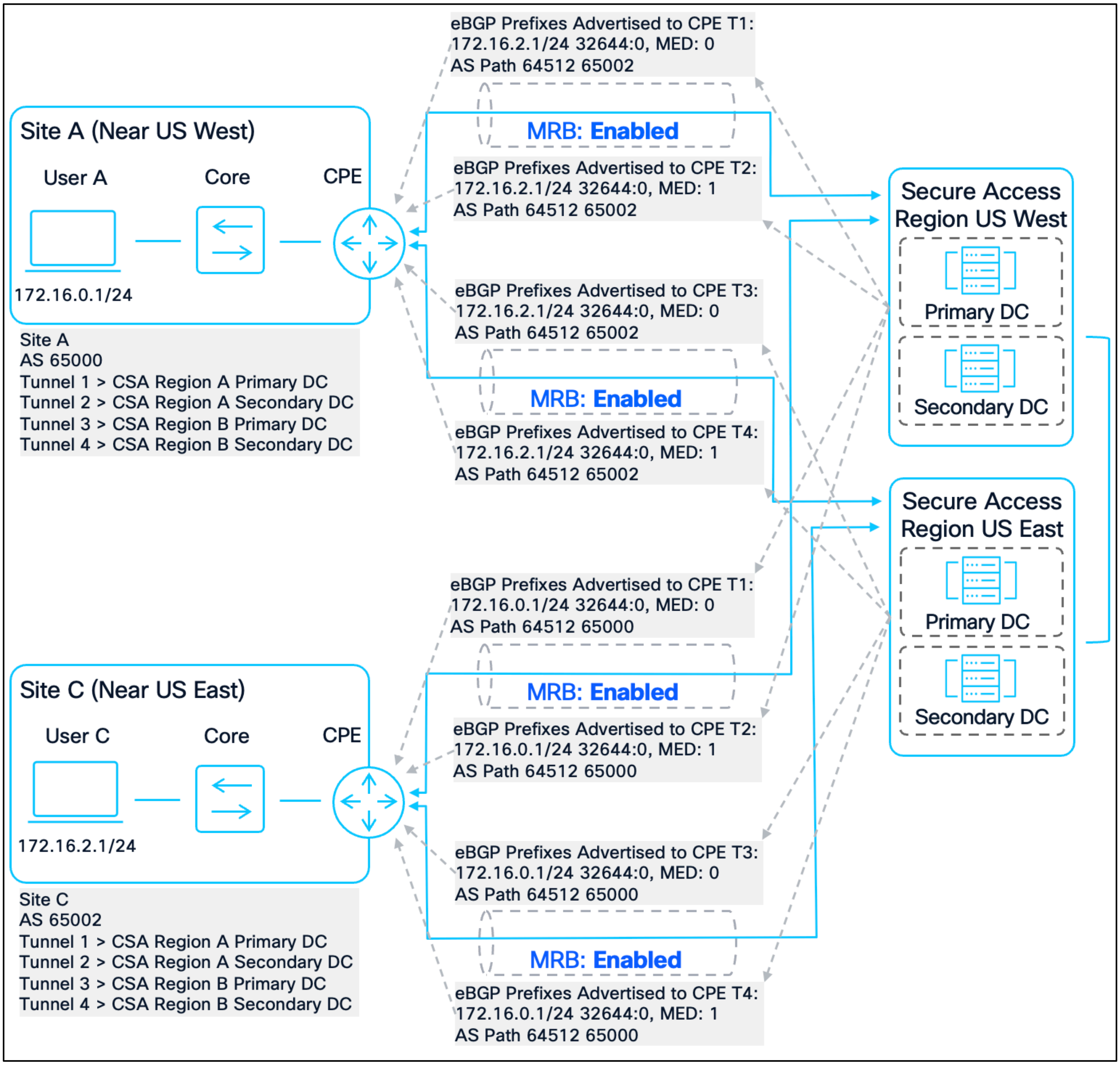
Figure 33.
Site to Site Distinct Primary or Secondary region Failover Test #4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.3.0/24    169.254.0.3              1             52 64512 65003 i
[omitted]
C8000V-SiteD#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.33             1             52 64512 65000 i
[omitted]
```

Data Collection – Site to Site (Swapped Primary and Secondary region)

To verify the preferred routes, the IOS-XE command **show ip bgp** is used on both the Site A and Site C router. We are interested in the routes advertised between the two sites. Routes advertised by Site A have the ASN 65000, while routes advertised by Site C will have the ASN 65002. For brevity, the prefixes not pertaining to traffic between the two sites have been removed from the output.



eBGP Prefixes Advertised to CPE T1:
172.16.2.1/24 32644:0, MED: 0
AS Path 64512 65002
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
172.16.2.1/24 32644:0, MED: 1
AS Path 64512 65002
eBGP Prefixes Advertised to CPE T3:
172.16.2.1/24 32644:0, MED: 0
AS Path 64512 65002
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
172.16.2.1/24 32644:0, MED: 1
AS Path 64512 65002
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
eBGP Prefixes Advertised to CPE T1:
172.16.0.1/24 32644:0, MED: 0
AS Path 64512 65000
MRB: Enabled
eBGP Prefixes Advertised to CPE T2:
172.16.0.1/24 32644:0, MED: 1
AS Path 64512 65000
eBGP Prefixes Advertised to CPE T3:
172.16.0.1/24 32644:0, MED: 0
AS Path 64512 65000
MRB: Enabled
eBGP Prefixes Advertised to CPE T4:
172.16.0.1/24 32644:0, MED: 1
AS Path 64512 65000
Site C (Near US East)
User C
Core
CPE
172.16.2.1/24
Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Figure 34.
Site to Site Swapped Primary and Secondary region Topology

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.2.0/24    169.254.0.1              0             0 64512 65002 i
 *                     169.254.0.5              0             0 64512 65002 i
 *                     169.254.0.7              1             0 64512 65002 i
 *                     169.254.0.3              1             0 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.25             0             0 64512 65000 i
 *                     169.254.0.27             1             0 64512 65000 i
 *>                    169.254.0.21             0             0 64512 65000 i
 *                     169.254.0.23             1             0 64512 65000 i
[omitted]
```

Without route-map intervention, both sites currently prefer Tunnel 1 (US West) because it advertises a Metric of 0. While this provides a symmetric path in the baseline state, the configuration is fragile; a single tunnel failure on either side would immediately trigger asymmetric routing.

A detailed inspection using show ip bgp [prefix] reveals that Secure Access tags all four paths with the local community string 32644:0. This occurs because both US West and US East are considered "local" to the Secure Access backbone for these specific site-to-site connections. Since the tags are identical across both regions, community-based weighting cannot be used to distinguish between the primary and Secondary regions.

```
C8000V-SiteA#show ip bgp 172.16.2.0
BGP routing table entry for 172.16.2.0/24, version 377
Paths: (4 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65002
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 10:15:48 UTC
  Refresh Epoch 1
  64512 65002
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:15:48 UTC
  Refresh Epoch 1
  64512 65002
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:15:48 UTC
  Refresh Epoch 1
  64512 65002
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:15:48 UTC
C8000V-SiteC#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 381
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65000
    169.254.0.25 from 169.254.0.25 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:13:55 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.27 from 169.254.0.27 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:14:01 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.21 from 169.254.0.21 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 10:13:49 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.23 from 169.254.0.23 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 08:56:31 UTC
```

The primary challenge in this scenario is that Site A and Site C have inverted regional preferences. If standard regional preference route-maps are applied:

- Site A will prefer US West (its Primary region).
- Site C will prefer US East (its Primary region).

This creates a deterministic asymmetric routing scenario where traffic from Site A to Site C transits US West but return traffic from Site C to Site A transits US East. To maintain path symmetry, an exception must be implemented to align both sites on a single transit region for their mutual traffic.

Configuration – Site to Site (Swapped Primary and Secondary region)

To resolve the deterministic asymmetry caused by inverted regional priorities, one site must implement a routing exception. In this design, Site C is configured to prefer its Secondary region (US West) specifically for traffic destined to Site A or Site B. This aligns Site C's outbound path with the Primary regional preference of the remote sites, ensuring a symmetric traffic flow across the Secure Access fabric.

For Site A, we will continue to use the route-map configuration used previously. For reference, the Site A route-map and community-list configuration after all the changes so far can be found below. The commands relevant to this specific site to site condition are bolded:

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
```

```
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
```

```
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

Site C will continue to prefer US East as its Primary region; however, configuration is added to include an AS-Path access-list to identify traffic originating from Site A (AS 65000) or Site B (AS 65001). By inserting a high-priority sequence (Sequence 5) into the US West route-maps, Site C will assign a higher weight to these specific prefixes when they are received via its Secondary region. This ensures that for traffic destined to Site A/B, Site C prefers the US West path, matching the preference of the remote sites. The commands relevant to this specific site to site condition are bolded:

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip as-path access-list 10 permit _(65000|65001)_
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 301
route-map US-WEST1-INBOUND permit 10
```

```
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 300
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
address-family ipv4
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

Validation – Site to Site (Swapped Primary and Secondary region)

To validate the route-map configuration and ensure symmetric traffic flow, we performed a sequential failover test by bringing down tunnels one by one. The goal is to verify that the BGP best-path selection (>) follows our weight hierarchy and that Site C's AS-Path exception correctly maintains symmetry with Site A.

Failover Test #1:

In the baseline state, both sites prefer US West for their mutual traffic. Site A uses its default regional preference (Weight 303), while Site C uses its AS-Path exception (Weight 301) to prefer US West instead of its local US East region. This ensures a symmetric path through the US West Primary DC.

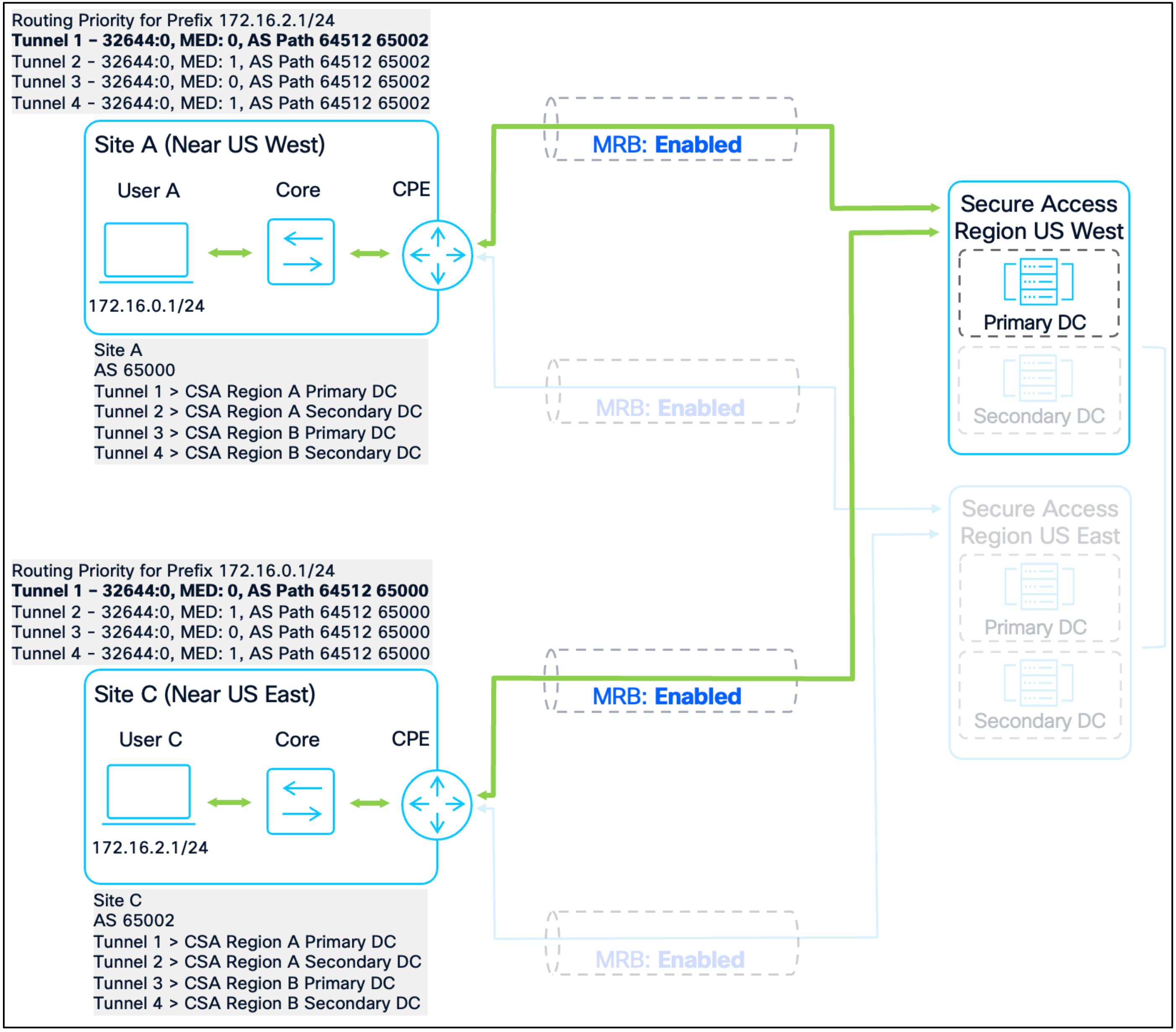

Routing Priority for Prefix 172.16.2.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65002
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65002
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65002
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65002
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000
Site C (Near US East)
User C
Core
CPE
172.16.2.1/24
Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled

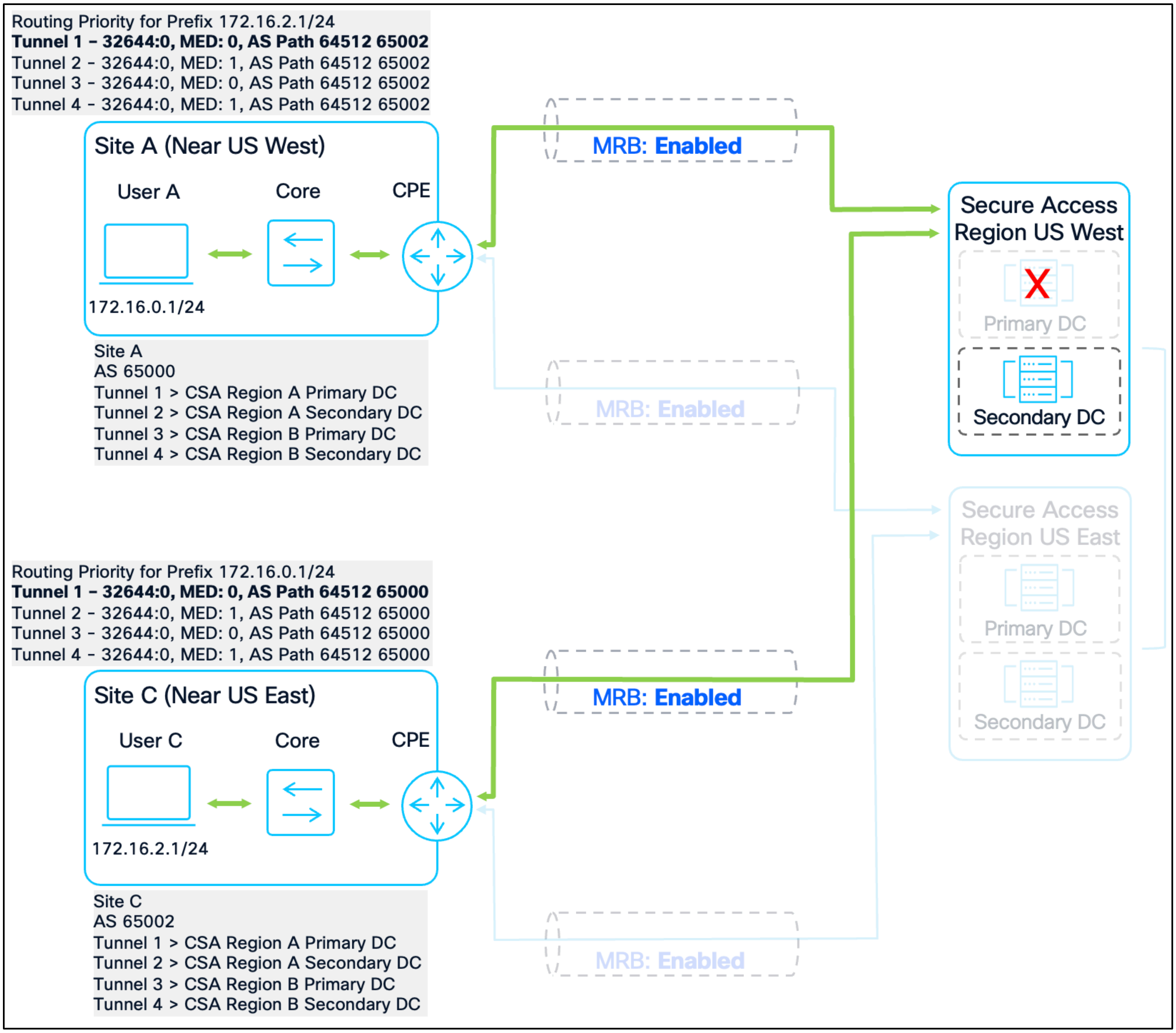
Figure 35.
Site to Site Swapped Primary and Secondary region Failover Test #1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
      Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
 *>                     169.254.0.1              0    106    303 64512 65002 i
 *                      169.254.0.3              1    106    302 64512 65002 i
 *                      169.254.0.5              0    106    301 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
 *                     169.254.0.25             0    104    203 64512 65000 i
 *>                    169.254.0.21             0    106    301 64512 65000 i
 *                     169.254.0.23             1    106    300 64512 65000 i
[omitted]
```

Failover Test #2:

With Tunnel 1 disabled, both routers fail over to the US West Secondary DC. Site A selects Tunnel 2 (Weight 302), and Site C selects Tunnel 2 (Weight 300) via the AS-Path exception. Traffic remains symmetric within the US West region.



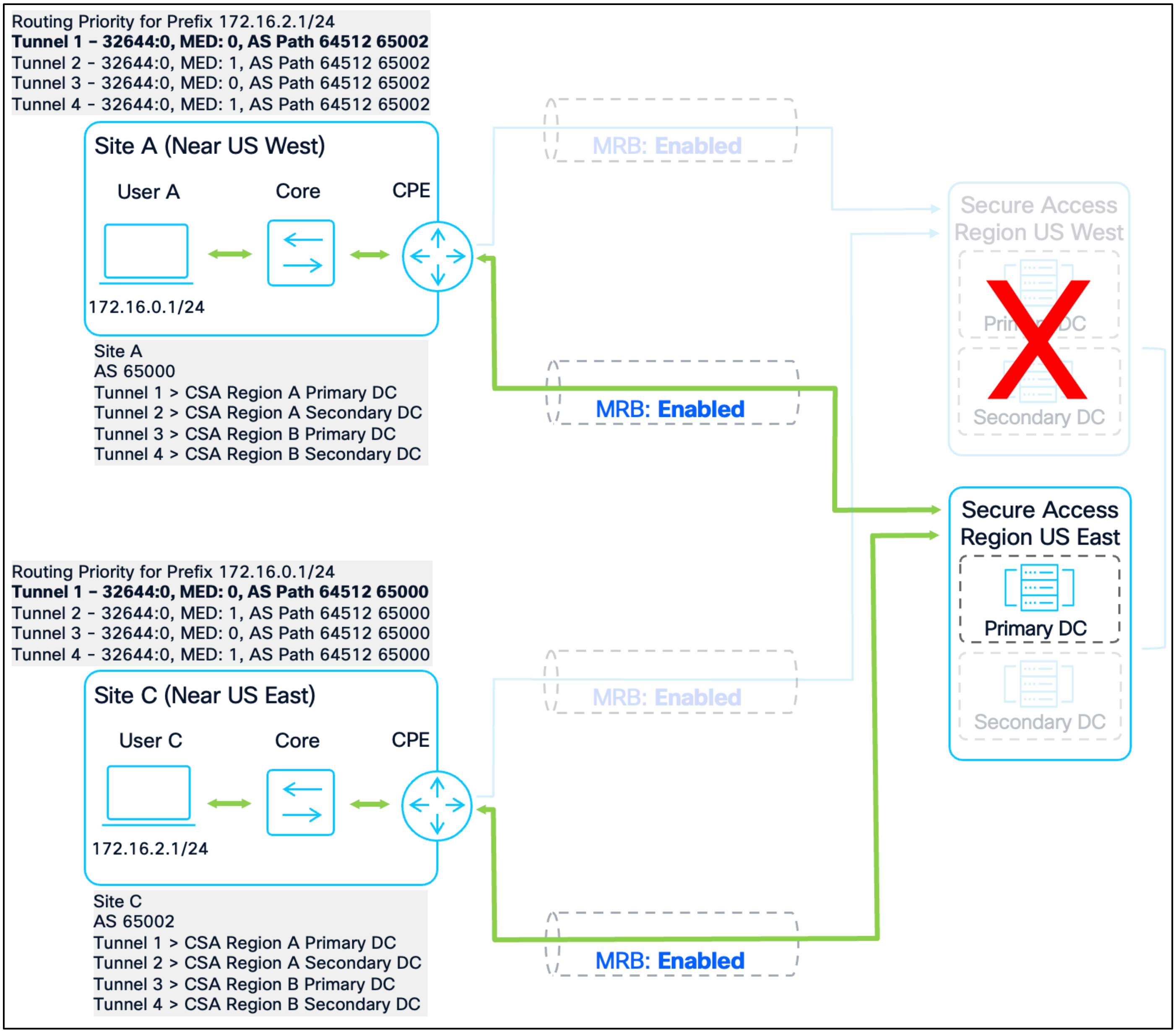
Routing Priority for Prefix 172.16.2.1/24
Tunnel 1 - 32644:0, MED: 0, AS Path 64512 65002
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65002
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65002
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65002
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
X
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
Tunnel 1 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000
Site C (Near US East)
User C
Core
CPE
172.16.2.1/24
Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled

Figure 36.
Site to Site Swapped Primary and Secondary region Failover Test #2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
 *>                    169.254.0.3              1    106    302 64512 65002 i
 *                     169.254.0.5              0    106    301 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
 *                     169.254.0.25             0    104    203 64512 65000 i
 *>                    169.254.0.23             1    106    300 64512 65000 i
[omitted]
```

Failover Test #3:

When the entire US West region is unavailable, both sites fail over to US East. Site A selects the US East Primary DC (Weight 301). Site C now reverts to its standard regional preference for US East (Weight 203) because the AS-Path exception only applied to US West tunnels. Symmetry is maintained via the US East Primary DC.



Routing Priority for Prefix 172.16.2.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65002
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65002
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65002
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65002

Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Routing Priority for Prefix 172.16.0.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000

Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC

Figure 37.
Site to Site Swapped Primary and Secondary region Failover Test #3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.2.0/24    169.254.0.7              1     106     300 64512 65002 i
 *>                     169.254.0.5              0     106     301 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.0.0/24    169.254.0.27             1     104     202 64512 65000 i
 *>                    169.254.0.25             0    104    203 64512 65000 i
[omitted]
```

Failover Test #4:

In this final scenario, only the US East Secondary DC is available. Both routers successfully install the final path (Site A Weight 300, Site C Weight 202). Traffic continues to flow symmetrically over the only remaining functional path.

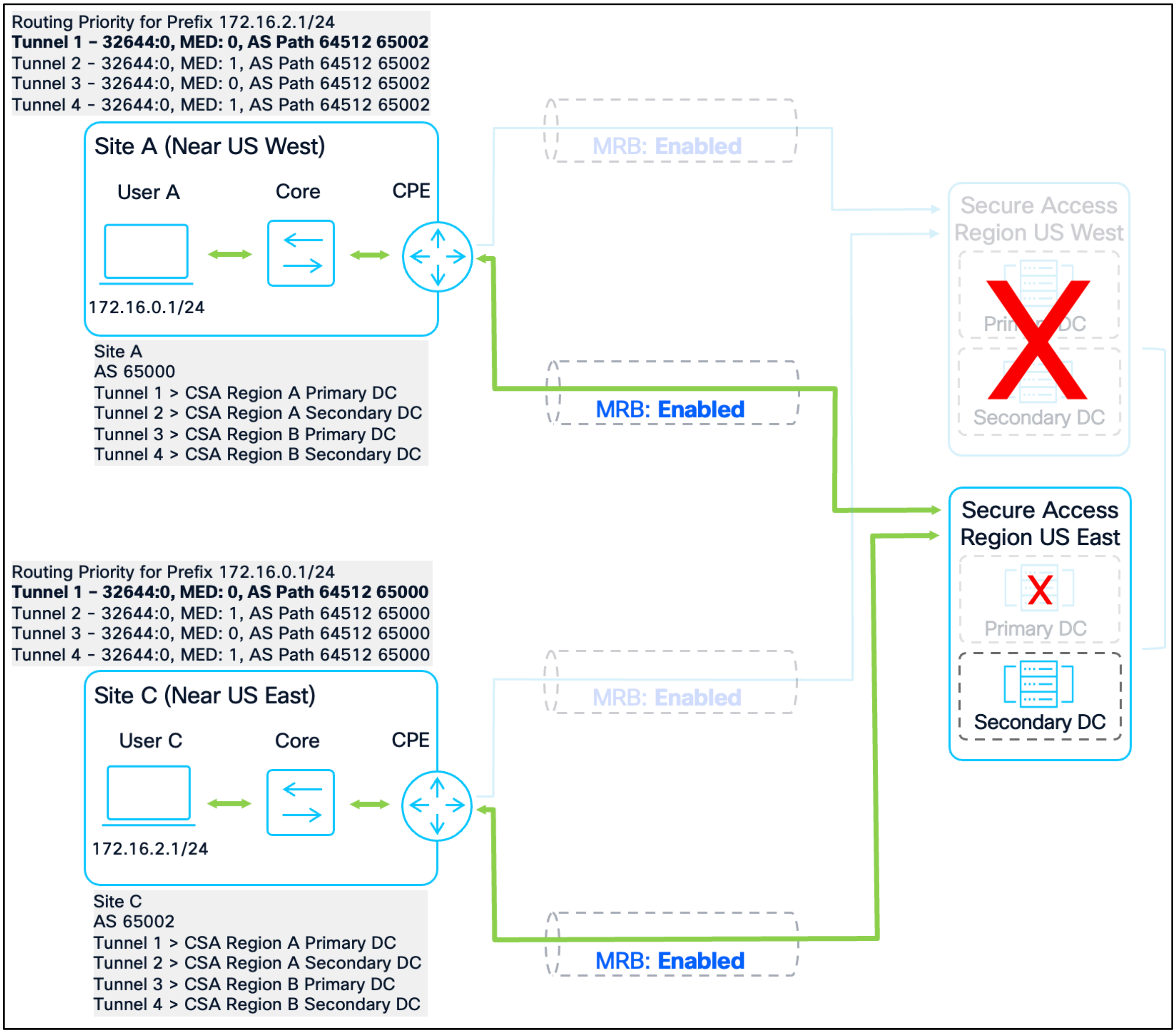

Routing Priority for Prefix 172.16.2.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65002
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65002
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65002
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65002
Site A (Near US West)
User A
Core
CPE
172.16.0.1/24
Site A
AS 65000
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled
Secure Access Region US West
Primary DC
Secondary DC
Secure Access Region US East
Primary DC
Secondary DC
Routing Priority for Prefix 172.16.0.1/24
Tunnel 1 – 32644:0, MED: 0, AS Path 64512 65000
Tunnel 2 - 32644:0, MED: 1, AS Path 64512 65000
Tunnel 3 - 32644:0, MED: 0, AS Path 64512 65000
Tunnel 4 - 32644:0, MED: 1, AS Path 64512 65000
Site C (Near US East)
User C
Core
CPE
172.16.2.1/24
Site C
AS 65002
Tunnel 1 > CSA Region A Primary DC
Tunnel 2 > CSA Region A Secondary DC
Tunnel 3 > CSA Region B Primary DC
Tunnel 4 > CSA Region B Secondary DC
MRB: Enabled
MRB: Enabled

Figure 38.
Site to Site Swapped Primary and Secondary region Failover Test #4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
```

```
 *>   172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
[omitted]
```

Appendix

Appendix A: Site Configurations

The final configuration for the IOS-XE CPE at all sites is listed below. For security purposes, pre-shared keys and Secure Access Org IDs have been removed. The bolded sections indicate the configuration added to supported MRB.

Site A Configuration:

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 44.228.138.150 255.255.255.255
 identity local email SiteA-US-West@XXXXXXX-666363488-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 52.35.201.56 255.255.255.255
 identity local email SiteA-US-West@XXXXXXX-666363490-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteA-US-East@XXXXXXX-666363535-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteA-US-East@XXXXXXX-666363536-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.0 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.228.138.150
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.2 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 52.35.201.56
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.4 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
 ip address 169.254.0.6 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
```

```
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
 bgp log-neighbor-changes
 neighbor 169.254.0.1 remote-as 64512
 neighbor 169.254.0.1 update-source Tunnel1
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 update-source Tunnel2
 neighbor 169.254.0.5 remote-as 64512
 neighbor 169.254.0.5 update-source Tunnel3
 neighbor 169.254.0.7 remote-as 64512
 neighbor 169.254.0.7 update-source Tunnel4
 address-family ipv4
  network 172.16.0.0 mask 255.255.255.0
  neighbor 169.254.0.1 activate
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 activate
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 activate
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 activate
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
exit-address-family
```

Site B Configuration:

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 44.228.138.150 255.255.255.255
 identity local email SiteB-US-West@XXXXXXX-666362793-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 52.35.201.56 255.255.255.255
 identity local email SiteB-US-West@XXXXXXX-666362794-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteB-US-East@XXXXXXX-666362822-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
```

```
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteB-US-East@XXXXXXX-666362824-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.10 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.228.138.150
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.12 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 52.35.201.56
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.14 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
```

```
 ip address 169.254.0.16 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
```

```
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65001
 bgp log-neighbor-changes
 neighbor 169.254.0.11 remote-as 64512
 neighbor 169.254.0.11 update-source Tunnel1
 neighbor 169.254.0.13 remote-as 64512
 neighbor 169.254.0.13 update-source Tunnel2
 neighbor 169.254.0.15 remote-as 64512
 neighbor 169.254.0.15 update-source Tunnel3
 neighbor 169.254.0.17 remote-as 64512
 neighbor 169.254.0.17 update-source Tunnel4
 !
 address-family ipv4
  network 172.16.1.0 mask 255.255.255.0
  neighbor 169.254.0.11 activate
  neighbor 169.254.0.11 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.13 activate
  neighbor 169.254.0.13 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.15 activate
  neighbor 169.254.0.15 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.17 activate
  neighbor 169.254.0.17 route-map US-EAST2-INBOUND in
exit-address-family
```

Site C Configuration:

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 44.228.138.150 255.255.255.255
 identity local email SiteC-US-West@XXXXXXX-666363358-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 52.35.201.56 255.255.255.255
 identity local email SiteC-US-West@XXXXXXX-666363360-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteC-US-East@XXXXXXX-666363390-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteC-US-East@XXXXXXX-666363391-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.20 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.228.138.150
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.22 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 52.35.201.56
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.24 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
 ip address 169.254.0.26 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip as-path access-list 10 permit _(65000|65001)_
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 301
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 300
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
 bgp log-neighbor-changes
 neighbor 169.254.0.21 remote-as 64512
 neighbor 169.254.0.21 update-source Tunnel1
 neighbor 169.254.0.23 remote-as 64512
 neighbor 169.254.0.23 update-source Tunnel2
 neighbor 169.254.0.25 remote-as 64512
 neighbor 169.254.0.25 update-source Tunnel3
 neighbor 169.254.0.27 remote-as 64512
 neighbor 169.254.0.27 update-source Tunnel4
 address-family ipv4
  network 172.16.2.0 mask 255.255.255.0
  neighbor 169.254.0.21 activate
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 activate
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 activate
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 activate
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

Site D Configuration:

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
```

```
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 35.179.86.116 255.255.255.255
 identity local email SiteD-UK@XXXXXXX-666498829-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 35.176.75.117 255.255.255.255
 identity local email SiteD-UK@XXXXXXX-666498830-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteD-US-East@XXXXXXX-666364205-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteD-US-East@XXXXXXX-666364206-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
```

```
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.30 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.179.86.116
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.32 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.176.75.117
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.34 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
 ip address 169.254.0.36 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-24 permit 32644:24
route-map UK1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map UK1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 103
```

```
route-map UK1-INBOUND permit 100
 set weight 53
route-map UK2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map UK2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 102
route-map UK2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65003
 bgp log-neighbor-changes
 neighbor 169.254.0.31 remote-as 64512
 neighbor 169.254.0.31 update-source Tunnel1
 neighbor 169.254.0.33 remote-as 64512
 neighbor 169.254.0.33 update-source Tunnel2
 neighbor 169.254.0.35 remote-as 64512
 neighbor 169.254.0.35 update-source Tunnel3
 neighbor 169.254.0.37 remote-as 64512
 neighbor 169.254.0.37 update-source Tunnel4
```

```
address-family ipv4
 network 172.16.3.0 mask 255.255.255.0
 neighbor 169.254.0.31 activate
 neighbor 169.254.0.31 route-map UK1-INBOUND in
 neighbor 169.254.0.33 activate
 neighbor 169.254.0.33 route-map UK2-INBOUND in
 neighbor 169.254.0.35 activate
 neighbor 169.254.0.35 route-map US-EAST1-INBOUND in
 neighbor 169.254.0.37 activate
 neighbor 169.254.0.37 route-map US-EAST2-INBOUND in
exit-address-family
```

Appendix B: Acronyms Defined

Acronym	Definition
AES	Advanced Encryption Standard
AS	Autonomous System
ASN	Autonomous System Number
BGP	Border Gateway Protocol
CPE	Customer Premises Equipment
DC	Data Center
DCI	Data Center Interconnect
DLP	Data Loss Prevention
DPD	Dead Peer Detection
ECMP	Equal-Cost Multi-Path
EGP	Exterior Gateway Protocol
GCM	Galois/Counter Mode
HA	High Availability
IGP	Interior Gateway Protocol
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LocPrf	Local Preference

Acronym	Definition
MED	Multi-Exit Discriminator
MRB	Multi-Region Backhaul
MSS	Maximum Segment Size
NTG	Network Tunnel Group
PRF	Pseudo-Random Function
RIB	Routing Information Base
S2S	Site-to-Site
SHA	Secure Hash Algorithm
SIA	Secure Internet Access
SSE	Security Service Edge
SWG	Secure Web Gateway
UK	United Kingdom
US	United States
VPN	Virtual Private Network
VPNaaS	Virtual Private Network as a Service
ZTNA	Zero Trust Network Access

Appendix C: Software Versions

Product	Platform	Version
Cisco Catalyst 8000V	IOS-XE	17.18.02
Cisco Secure Access	Cloud Offering	SaaS

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 **https://www.cisco.com/go/offices**.

Printed in USA 02/26