

Misure correttive per in Secure Access Dubai DC interruzione

Sommario

[Introduzione](#)

[Connettori di risorse](#)

[Profili VPN di Accesso remoto](#)

[Gruppi di tunnel di rete](#)

[Secure Web Gateway](#)

[Client di accesso con trust pari a zero](#)

[Informazioni correlate](#)

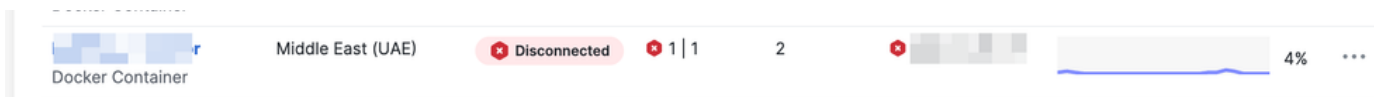
Introduzione

Questo documento contiene le misure correttive per l'incidente del 2 marzo scorso al Secure Access Dubai DC.

<https://status.sse.cisco.com/incidents/7h28mb7mr5zl>

Connettori di risorse

I connettori di risorse già distribuiti verranno visualizzati come disconnessi dal dashboard Accesso sicuro:



I connettori di risorse distribuiti sono associati a una singola area di accesso protetto e non possono essere modificati tramite la modifica della configurazione.

Per risolvere il problema, i clienti interessati devono seguire i passi descritti di seguito:

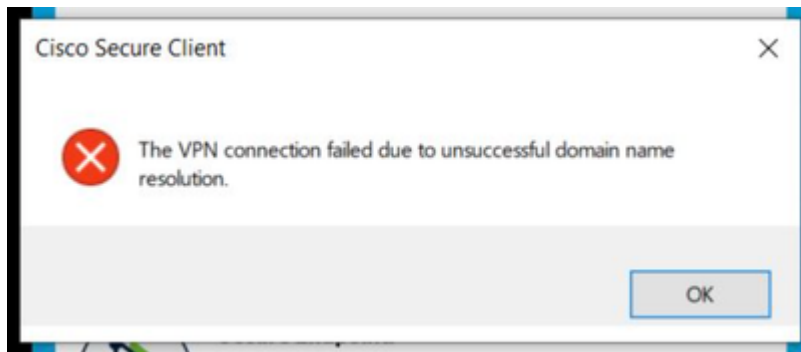
1. Distribuire un nuovo connettore di risorse
2. Creazione di gruppi di connettori in nuove regioni (Mumbai o Hyderabad)
2. Assegnare risorse private ai nuovi gruppi Connector

Per informazioni dettagliate sulla distribuzione di Connettore risorse, vedere la guida alla distribuzione di Connettore risorse:

Profili VPN di Accesso remoto

I client VPN di Accesso remoto possono non riuscire a stabilire la connessione con errori diversi.

Errore di esempio:



Solo per le organizzazioni con profilo VPN ad accesso remoto a Dubai DC:

Attenersi alla procedura seguente:

- Selezionare il data center più vicino disponibile (Mumbai o Hyderabad) come destinazione della migrazione.
- Configurare i pool e i profili IP VPN in modo che corrispondano al carico di sessioni corrente dell'organizzazione, eseguendo il mirroring della configurazione di ME-Central esistente.

Per i passaggi dettagliati sulla configurazione del nuovo profilo VPN, consultare la guida alla distribuzione di VPN ad accesso remoto:

Gruppi di tunnel di rete

Per modificare l'area del gruppo di tunnel di rete, eseguire la procedura seguente:

- Andare alle opzioni NTG come descritto di seguito:
- Modifica il tunnel esistente per la regione del Medio Oriente (EAU).

Network Connections
Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)

Connector Groups **Network Tunnel Groups** FTDs

Network Tunnel Groups 8 total

2 Disconnected ❗ 3 Warning ⚠️ 3 Connected ✅

Network Tunnel Groups
A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Search: mec Region: ▼ Status: ▼ 1 Tunnel Group [+ Add](#)

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
mec Other	⚠️ Warning	Middle East (UAE)	sse-mec-1-1-1	6	sse-mec-1-1-0	1

Actions: Edit, View Details, View Logs, Delete

· Cambiare la regione da Medio Oriente (EAU) a India (Ovest).

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name:

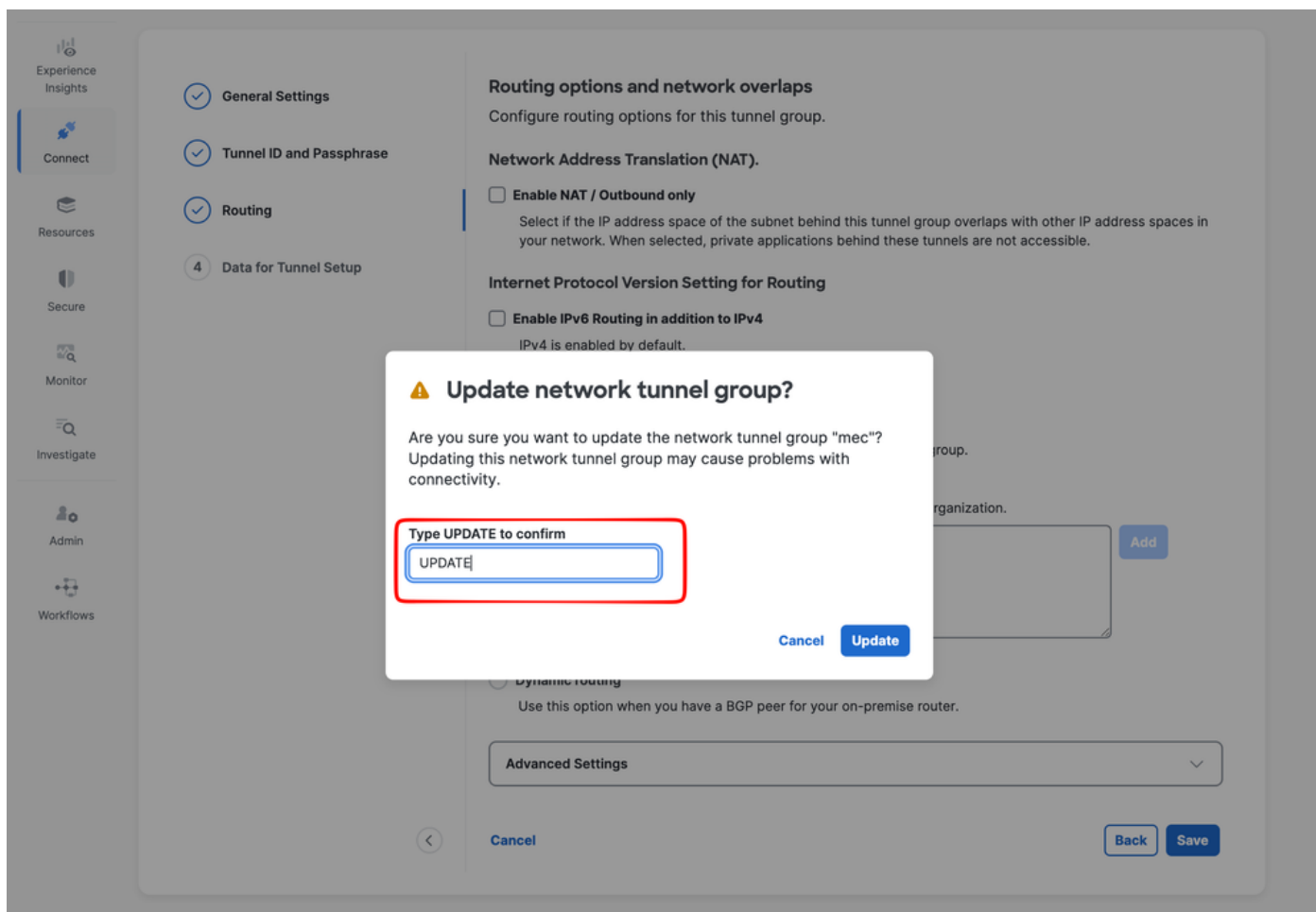
Region: Middle East (UAE) ^

- Africa (South Africa)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Osaka)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Australia (Sydney)
- Brazil
- Canada (Central)
- Canada (West)
- Europe (Germany)
- Europe (Milan)
- Europe (Spain)
- Europe (Stockholm)
- India (South)
- India (West)

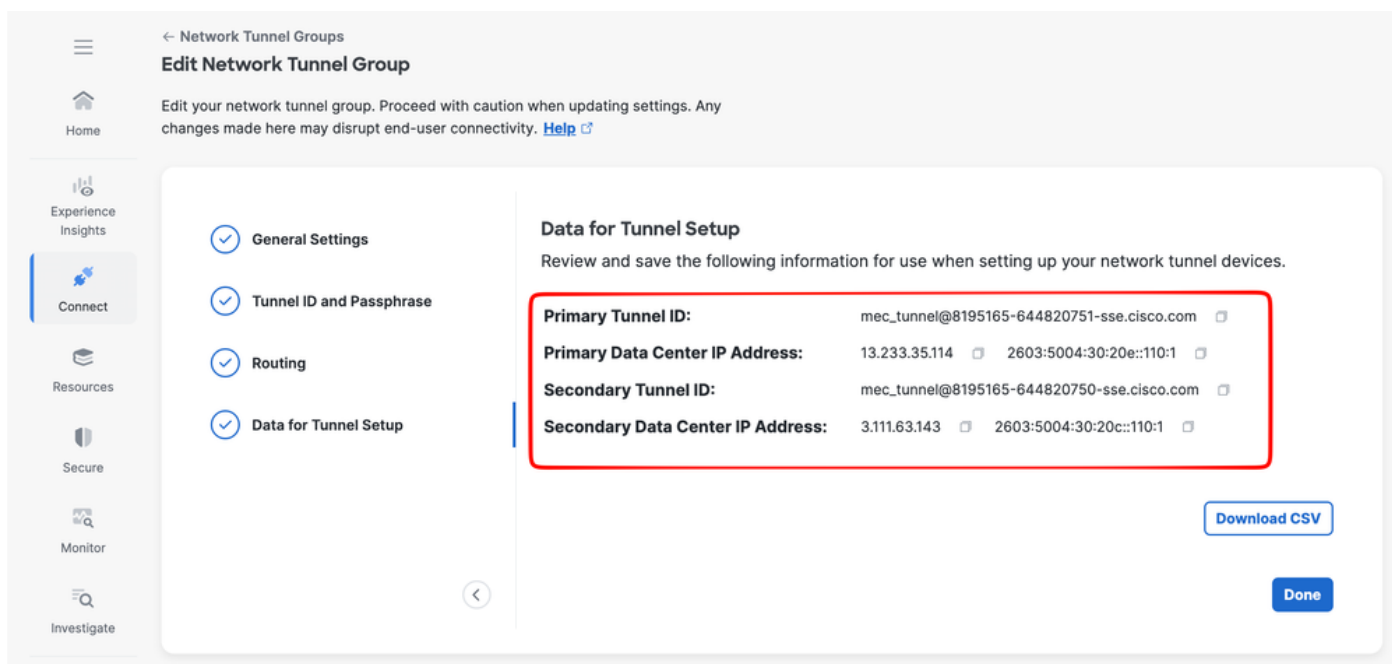
[Next](#)

· Non modificare altre impostazioni; salvare la configurazione.

- Quando richiesto, digitare "UPDATE" e confermare.



- Utilizzare i nuovi indirizzi IP dell'India (occidentale) mostrati per aggiornare il dispositivo IPSEC CPE.



- Se si utilizzano backhaul o route-map a più aree, aggiornare i valori della community BGP in base alle nuove impostazioni di Cisco SSE.

Secure Web Gateway

I client che utilizzano il modulo di sicurezza roaming si connetteranno automaticamente al centro dati ad accesso sicuro più vicino e disponibile.

Al momento non è richiesta alcuna azione da parte dei clienti.

Client di accesso con trust pari a zero

I client che utilizzano il modulo Zero Trust Access si connetteranno automaticamente al centro dati più vicino e disponibile.

Al momento non è richiesta alcuna azione da parte dei clienti.

Informazioni correlate

- [Stato Cisco Secure Access](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).