Connettività da sito a sito con subnet sovrapposte in Cisco Secure Access

Sommario

Introduzione

In questo documento viene descritta la soluzione Cisco Secure Access che si sovrappone alla subnet.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione di Cisco Secure Access.
- Amministrazione di firewall/router.

Cisco raccomanda:

- Accesso amministrativo a Cisco Secure Access.
- Accesso amministrativo al dispositivo headend IPSec (firewall o router)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Operazioni preliminari

Nell'esempio, vi sono due siti di succursale diversi con la stessa subnet IP 192.168.200.0/24, in cui sono connessi a Cisco Secure Access tramite due tunnel IPSec separati.

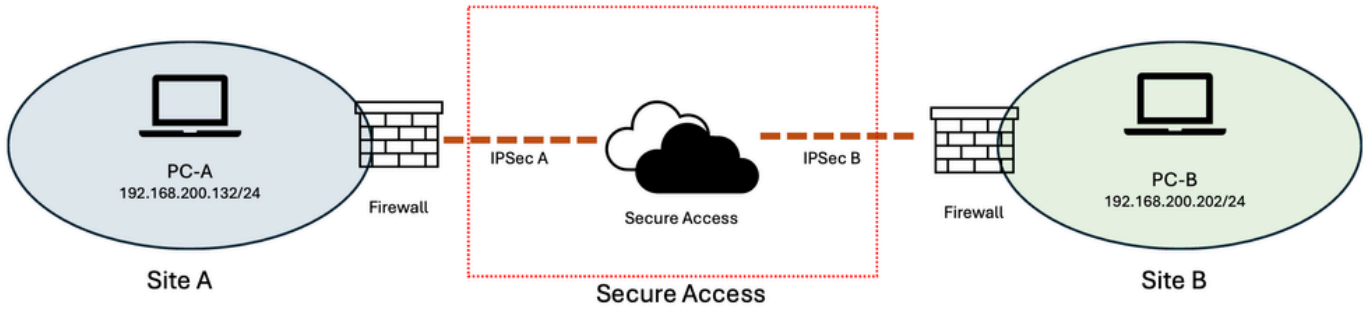


Immagine - Esempio di rete

L'obiettivo è che gli utenti del "Sito A" possano accedere alle risorse del "Sito B" e viceversa.

Preparazione e pianificazione

Poiché entrambi i siti utilizzano la stessa subnet IP (`192.168.200.0/24`), la sovrapposizione dello spazio degli indirizzi impedisce la comunicazione diretta tra i due siti. Per risolvere questa sovrapposizione, vengono assegnate due subnet virtuali non sovrapposte per rappresentare le risorse in ogni sito.

Per questo esempio:

- Sito A: `10.30.30.0/24`

- Sito B: `10.40.40.0/24`
- Subnet effettiva in entrambi i siti: `192.168.200.0/24`

Le subnet virtuali forniscono spazi di indirizzi univoci per ogni sito, mentre le risorse effettive continuano a utilizzare gli indirizzi `192.168.200.0/24` esistenti.

Quando un utente del sito A accede a una risorsa del sito B, accede alla risorsa tramite la subnet virtuale del sito B (**`10.40.40.0/24`**) anziché utilizzando direttamente lo spazio di indirizzi sovrapposto `192.168.200.0/24`.

Cisco Secure Access fornisce una funzionalità NAT (D-NAT) di destinazione uno-a-uno in grado di convertire gli indirizzi virtuali negli indirizzi reali corrispondenti. L'intervallo di indirizzi D-NAT ha le stesse dimensioni della subnet originale. Nell'esempio, le reti virtuali e quelle effettive sono subnet `0/24`, che forniscono una mappatura uno-a-uno tra gli indirizzi IP virtuali e quelli reali.

Ad esempio:

`10.40.40.202` → `192.168.200.202`

Pertanto, una richiesta dal Sito A destinata alla data `10.40.40.202` è tradotta da D-NAT a `192.168.200.202`, consentendo alla richiesta di raggiungere la risorsa corrispondente nel Sito B nonostante entrambi i siti utilizzino la stessa subnet IP sottostante.

Questo approccio crea in modo efficace uno spazio di indirizzi virtuale non sovrapposto per ciascun sito, preservando al contempo l'indirizzo IP esistente delle risorse. Fornisce inoltre una relazione uno-a-uno coerente tra gli indirizzi virtuali e quelli reali, semplificando la comprensione, la gestione e la risoluzione dei problemi della configurazione.

Procedura di configurazione

A causa della progettazione corrente e delle limitazioni di Cisco Secure Access, per ottenere questo scenario è necessaria la configurazione sia sugli headend sui tunnel IPsec che su Cisco Secure Access.

Il dispositivo headend è il firewall o il router che stabilisce il tunnel IPsec per Cisco Secure Access. Oltre a configurare D-NAT in Cisco Secure Access, il firewall dell'headend deve eseguire anche il protocollo NAT di origine (S-NAT) per il traffico di ritorno.

La configurazione è quindi costituita da due sezioni:

1. Configurazione del NAT di destinazione (D-NAT) in Cisco Secure Access per ciascun tunnel di rete separatamente.
2. Configurazione del protocollo NAT di origine (S-NAT) sui firewall per garantire che il traffico di ritorno venga riconvertito nello spazio degli indirizzi virtuali.

Configurazione di Cisco Secure Access

Passaggio 1: Dal portale di gestione Cisco Secure Access, selezionare Connect > Network Connections e selezionare la scheda Network Tunnel Groups (Gruppi di tunnel di rete).

Passaggio 2: Modificare il gruppo di tunnel di rete associato al tunnel IPsec per il sito che utilizza la subnet sovrapposta.

In questo esempio:

- IPSec-A = Gruppo tunnel di rete per il sito A
- IPSec-B = Gruppo tunnel di rete per il sito B

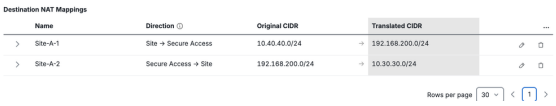
Passaggio 3: Fare clic sul menu a tre punti accanto al gruppo di tunnel di rete desiderato e selezionare Modifica.

Passaggio 4: Dal menu a sinistra, selezionare la scheda Routing e abilitare Network Address Translation (NAT), se non è già abilitato.

Passaggio 5: In Mapping NAT di destinazione fare clic su Aggiungi mapping.

Passaggio 6: Utilizzare questa tabella per configurare i mapping D-NAT per ciascun gruppo di tunnel di rete:

	Sito A - Tunnel IPSec	Sito B - Tunnel IPSec
NAT-1 di destinazione	Sito → Accesso sicuro CIDR originale: 10.40.40.0/24 CIDR tradotto: 192.168.200.0/24	Sito → Accesso sicuro CIDR originale: 10.30.30.0/24 CIDR tradotto: 192.168.200.0/24

NAT-2 di destinazione	Accesso sicuro → Sito CIDR originale: 192.168.200.0/24 CIDR tradotto: 10.30.30.0/24	Accesso sicuro → Sito CIDR originale: 192.168.200.0/24 CIDR tradotto: 10.40.40.0/24
	 Sito tunnel IPsec A - Configurazione D-NAT	 Sito tunnel IPsec B - Configurazione D-NAT

Nota: Dopo aver configurato le impostazioni per ciascun gruppo di tunnel di rete, fare clic su Salva. Quando viene visualizzata la finestra di conferma, immettere UPDATE per confermare la modifica. Ripetere la stessa procedura per l'altro gruppo di tunnel di rete

Configurazione del firewall

La configurazione del firewall è richiesta a causa di un limite corrente nella gestione delle subnet IP sovrapposte dietro i gruppi di tunnel di rete.

Quando Cisco Secure Access esegue il protocollo D-NAT su un pacchetto in arrivo, l'indirizzo di destinazione tradotto viene utilizzato per consegnare il pacchetto alla risorsa di destinazione. Tuttavia, la traduzione inversa corrispondente non viene eseguita automaticamente per il traffico di ritorno in questo scenario subnet sovrapposta.

Di conseguenza, il traffico di ritorno deve essere terminato manualmente con un NAT di origine sul firewall.

Il requisito chiave è che il server di destinazione visualizzi il traffico di ritorno utilizzando l'indirizzo IP virtuale a cui il client ha effettuato l'accesso in origine, anziché l'indirizzo IP effettivo del server.

Esempio

Si supponga quanto segue:

- Client del sito A: `192.168.200.132`
- Server Web sito B: `192.168.200.202`
- Subnet virtuale sito B: `10.40.40.0/24`
- Indirizzo virtuale del server Web: `10.40.40.202`

Il client nel sito A accede al server Web del sito B utilizzando https://10.40.40.202

Cisco Secure Access esegue D-NAT `10.40.40.202 → 192.168.200.202`

Il pacchetto raggiunge quindi il server Web al numero `192.168.200.202`.

Il problema si verifica con il traffico di ritorno. Senza ulteriori NAT sul firewall, il server Web genera la risposta con Source: `192.168.200.202`

Tuttavia, il client ha avviato la connessione alla destinazione: `10.40.40.202`

Pertanto, il traffico di ritorno deve essere tradotto in modo che l'indirizzo di origine presentato al client corrisponda all'indirizzo virtuale `192.168.200.202 → 10.40.40.202`

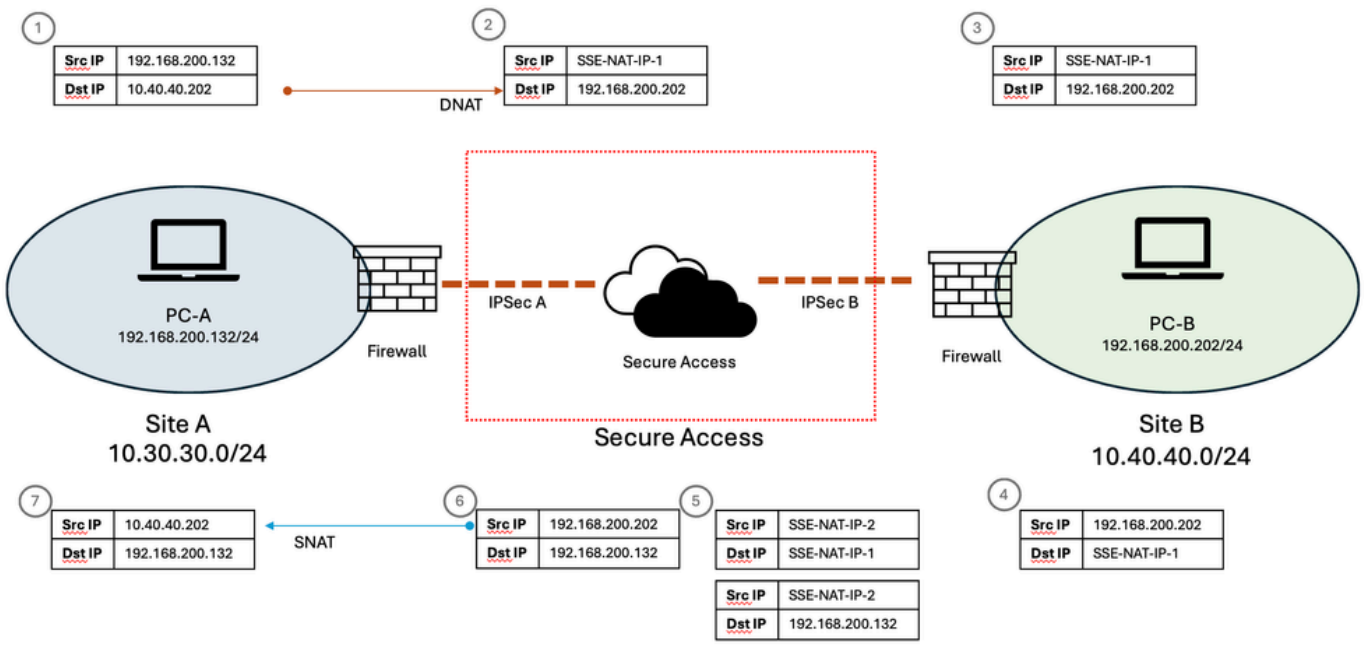


Immagine - Flusso di rete

A tale scopo, il firewall esegue il NAT di origine sul traffico in uscita verso il Network Tunnel Group.

Per questo esempio, la mappatura richiesta è`192.168.200.0/24 → 10.40.40.0/24`

In questo modo viene creata una relazione uno-a-uno inversa tra gli indirizzi reali e gli indirizzi virtuali corrispondenti.

SNAT uno-a-uno

Se il firewall supporta il protocollo NAT di origine uno-a-uno per l'intera subnet, una singola regola NAT può rappresentare l'intervallo di indirizzi completo `/24`.

Ad esempio:

Origine reale	Origine tradotta
`192.168.200.0/24`	`10.40.40.0/24`

Ne risultano mappature come `192.168.200.202 → 10.40.202` e `192.168.200.203 → 10.40.40.203`

La stessa relazione uno-a-uno viene applicata all'intera subnet.

Firewall senza SNAT "uno a uno"

Se il firewall non supporta il protocollo NAT di origine uno-a-uno per l'intera subnet, è necessario configurare singolarmente ogni mapping richiesto.

Ad esempio, per il server Web:

- IP di origine: `192.168.200.202`
- Source interface (interfaccia di origine): Gruppo tunnel di rete
- Direzione traffico: In entrata
- IP origine convertita: `10.40.40.202`

La traduzione risultante è `192.168.200.202 → 10.40.40.202`

È possibile applicare lo stesso approccio a ogni risorsa che richiede l'accesso tramite la subnet virtuale.

In questo modo viene garantito che entrambe le direzioni della comunicazione mantengano lo schema di indirizzamento virtuale e che il client riceva la risposta dallo stesso indirizzo IP virtuale utilizzato per stabilire la connessione.

Informazioni correlate

Configurazione mapping NAT/Network Tunnel Group di Cisco Secure Access:
https://securitydocs.cisco.com/docs/csa/olh/168842.dita

Riferimento alla configurazione e al routing di Cisco Secure Access Network Tunnel Group:
https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Guida alla risoluzione dei problemi e alla raccolta di dati di base di Cisco Secure Access:
https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

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).