Configurazione dei criteri SIG per l'accesso remoto per gli utenti di Secure Connect

Sommario

Introduzione

In questo documento viene descritto come creare criteri SIG per l'accesso remoto per utenti Secure Connect.

Panoramica

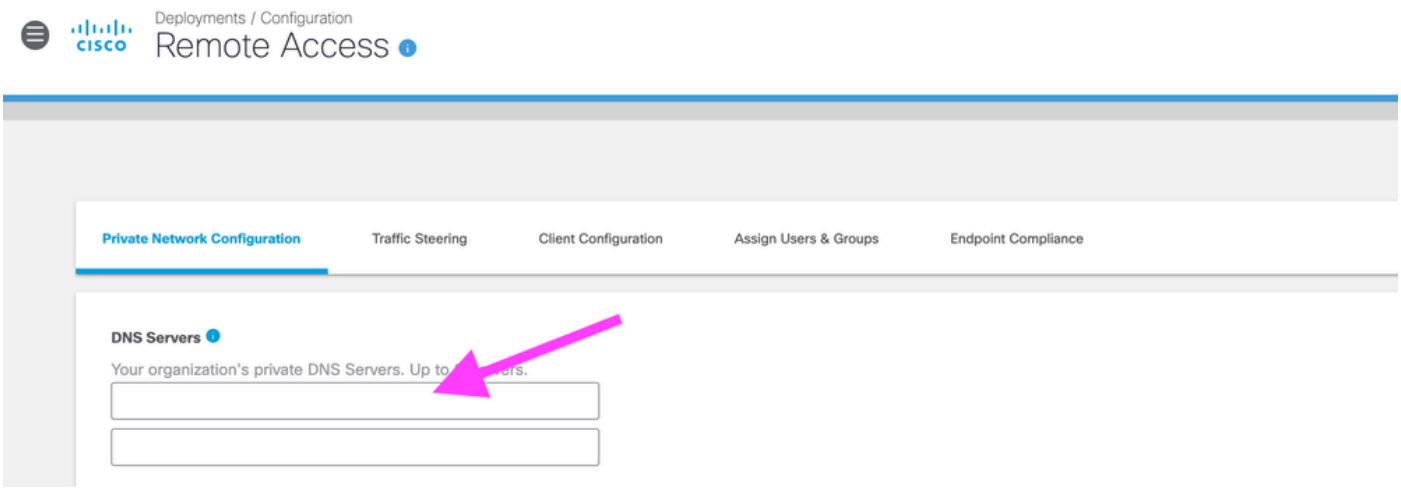
Questo articolo della Knowledge Base si applica ai clienti che utilizzano il pacchetto Secure Connect che include la funzionalità di accesso remoto (VPNaaS) in Umbrella.

Gli amministratori possono configurare le policy Umbrella Firewall, Web e Data Loss da applicare agli utenti in roaming connessi all'accesso remoto tramite AnyConnect.

Criteri DNS

È possibile inviare query DNS ai resolver Umbrella (ad esempio 208.67.222.22) tramite la connessione VPN ad accesso remoto AnyConnect. Tuttavia, questa operazione non consente l'identificazione, i criteri o la segnalazione del traffico DNS nel dashboard Umbrella.

- Questa opzione fornisce solo la risoluzione DNS e pertanto non è consigliata.
- L'utilizzo di resolver DNS esterni nella configurazione VPN DNS impedisce la risoluzione delle zone DNS interne.

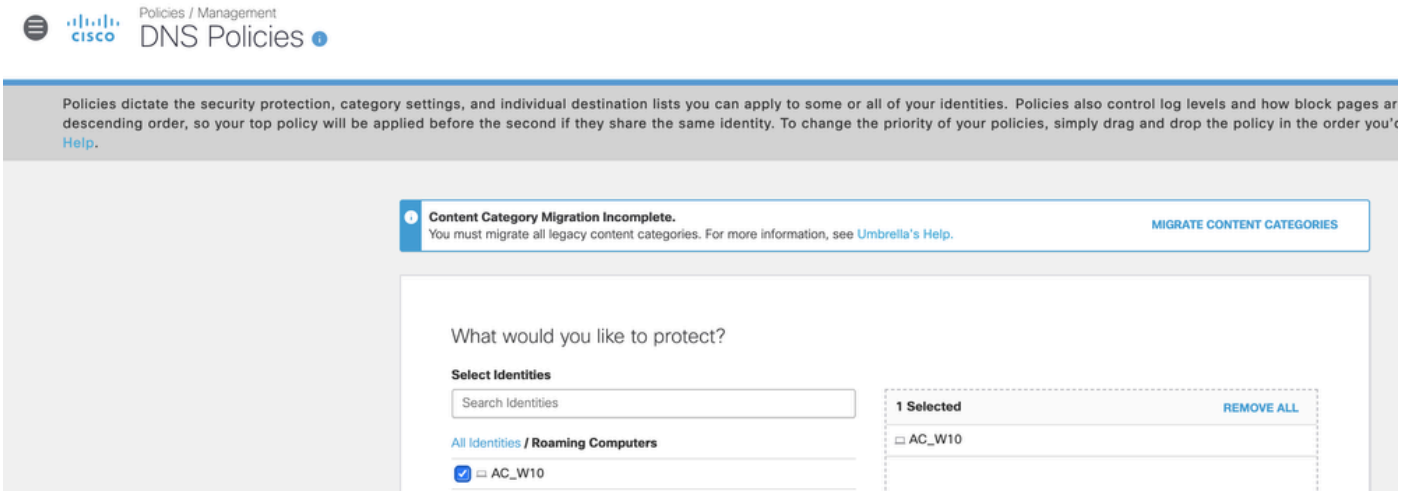


4410210378004

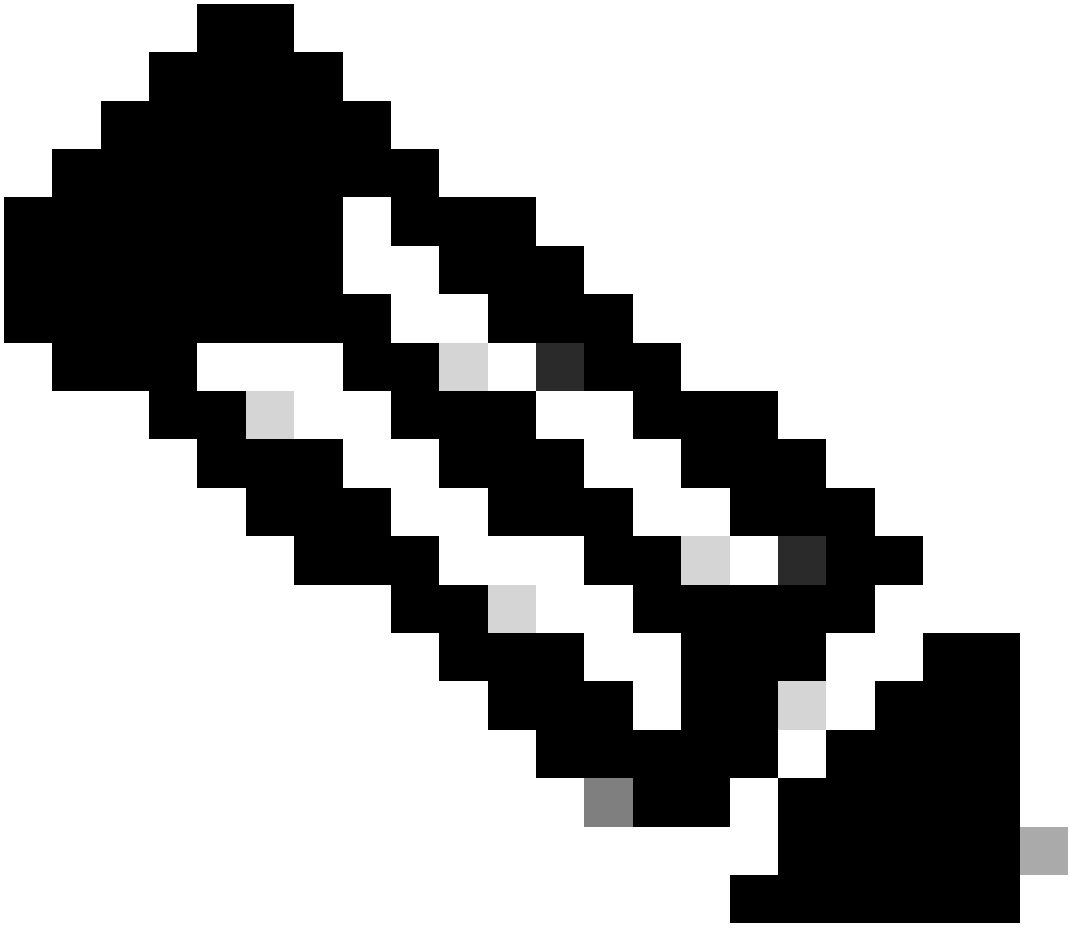
Per aggiungere identità, criteri e report per le query DNS, è necessario considerare uno dei tre metodi seguenti:

- (Consigliato) - Distribuire il modulo Umbrella AnyConnect Roaming (da Distribuzioni > Computer mobili). Il traffico DNS esterno viene inviato direttamente a Umbrella con l'identità di "computer in roaming" applicata. Questo modulo supporta inoltre l'identificazione utente facoltativa di Active Directory.
- Inoltra il traffico dal server DNS locale a Umbrella e identifica il traffico utilizzando un'identità di rete. Tutti gli utenti ricevono lo stesso criterio/identità e non è presente alcun report granulare per gli utenti.
- Per inoltrare il traffico a Umbrella, utilizzare un'appliance virtuale Umbrella sulla rete locale. Le query DNS possono essere identificate dal relativo indirizzo IP interno (pool VPN). È possibile aggiungere l'integrazione di Active Directory. È necessaria l'installazione di componenti locali aggiuntivi.

Nell'esempio viene mostrato come configurare un criterio DNS (Criteri > Criteri DNS) per un singolo client AnyConnect - ciò è possibile solo quando viene distribuito il modulo di roaming Umbrella AnyConnect:



4410210455444



Nota: Quando si usa il modulo Umbrella per AnyConnect, il traffico DNS può essere inviato facoltativamente all'interno o all'esterno del tunnel a seconda della configurazione del tunneling suddiviso.

Criteri firewall

I criteri firewall si applicano al traffico tra i client di Accesso remoto (AnyConnect) e Internet. Configurare le regole in 'Distribuzioni > Criteri firewall' come indicato nella documentazione disponibile qui: Gestire il firewall.

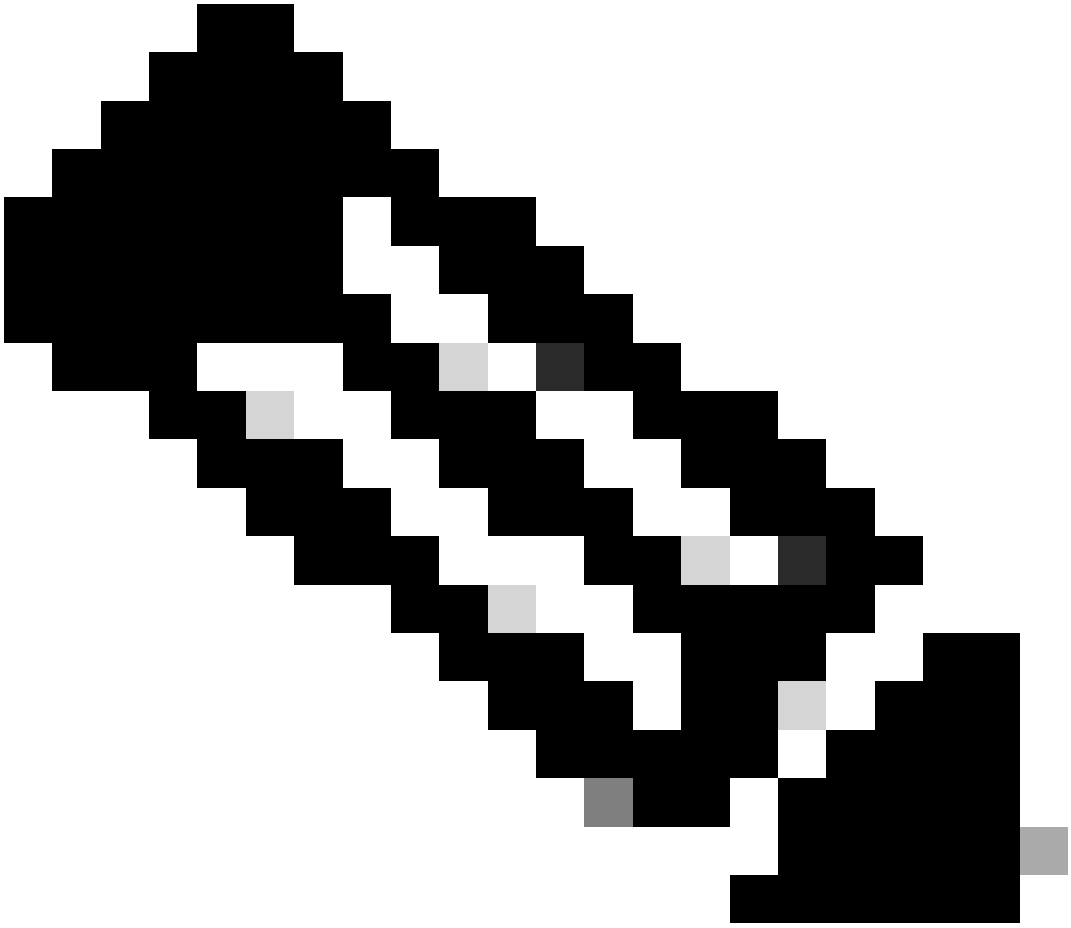
La regola predefinita del firewall viene applicata ai client di Accesso remoto. Se si sta creando un criterio specifico per gli utenti di Accesso remoto, è possibile scegliere di creare un nuovo criterio firewall e selezionare "Orgid di Accesso remoto:<ID>" come identità del tunnel di origine.
Lo stesso criterio firewall si applica a tutti gli utenti di accesso remoto.

- I criteri firewall non vengono utilizzati per controllare l'accesso tra i client di Autorità registrazione integrità e le reti private/di succursale. Questo deve essere controllato con

firewall locali.

- Come tutte le regole del firewall Umbrella, queste regole controllano le connessioni in uscita per i client di Accesso remoto. Le connessioni in entrata non sono mai consentite.
- L'indirizzo IP di origine per i client di Accesso remoto viene sempre assegnato dinamicamente dal pool VPN.
    - Non è consigliabile creare regole per un computer specifico utilizzando l'indirizzo IP di origine, in quanto l'indirizzo IP viene riassegnato dinamicamente
    - La creazione di regole che interessano gli utenti di uno specifico centro dati di Accesso remoto è possibile utilizzando un intervallo "CIDR di origine". Ogni centro dati fornisce un intervallo di pool VPN diverso configurato nella pagina 'Distribuzioni > Accesso remoto'.

4409322341524



Nota: L'identificazione per utente non è disponibile per i criteri firewall.

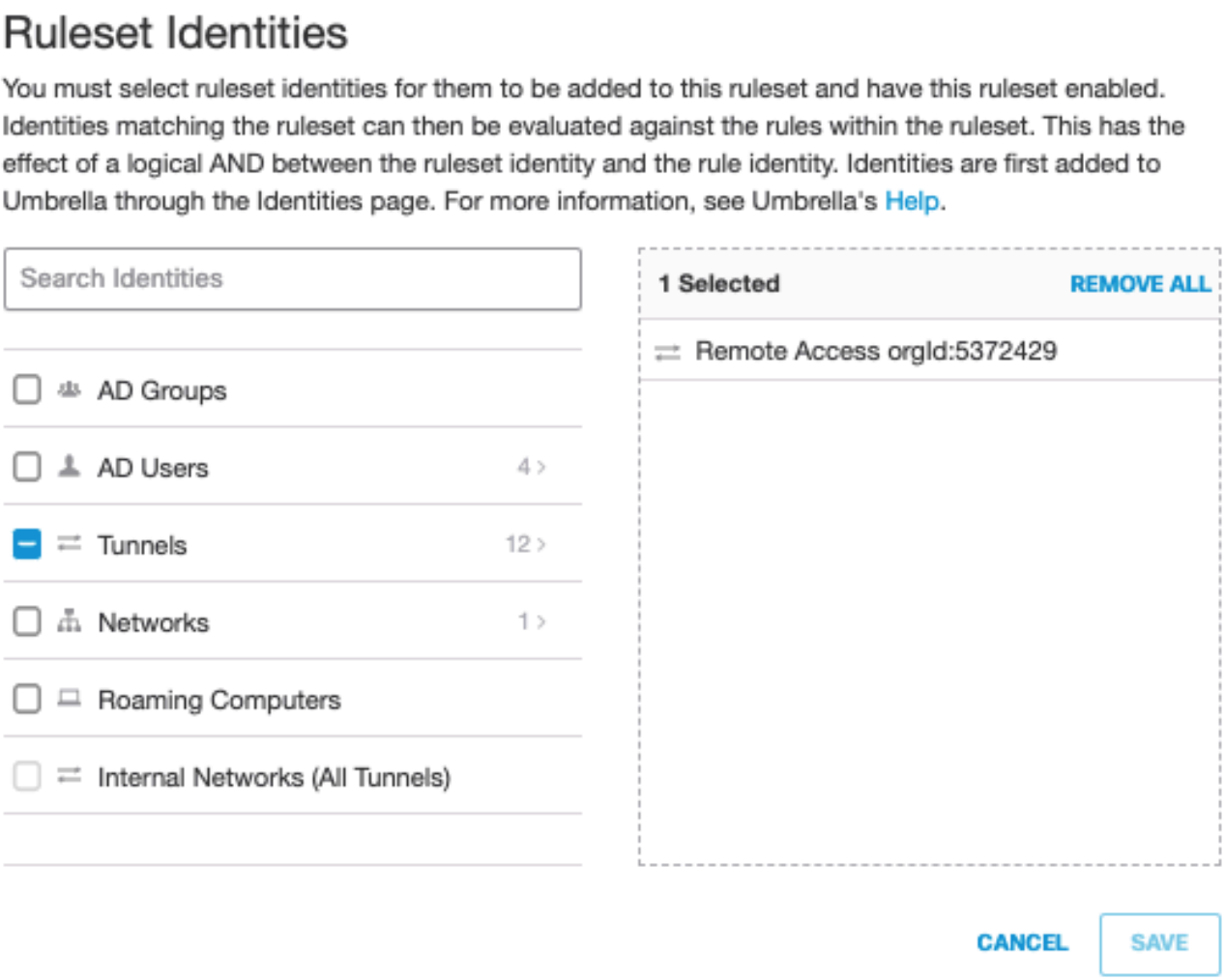
Criteri Web

I criteri Web si applicano al traffico tra i client di Accesso remoto (AnyConnect) e Internet. Configurare le regole in 'Distribuzioni > Criteri Web' come indicato nella documentazione disponibile qui: Gestire i criteri Web.

- I criteri Web non vengono utilizzati per controllare l'accesso tra i client di Autorità registrazione integrità e i server Web Private/Branch. I criteri Web si applicano solo ai siti Web esterni.

Il criterio Web predefinito si applica ai client di Accesso remoto. È tuttavia consigliabile creare un nuovo set di regole per definire impostazioni di protezione specifiche per i client di Accesso remoto. Quando si definiscono le identità del set di regole, scegliere ID orgid di Accesso remoto:<ID> dall'elenco dei tunnel. Lo stesso criterio Web si applica a tutti gli utenti di Accesso remoto.

Dopo aver creato un set di regole, è possibile aggiungere una regola Web a cui definire le impostazioni di applicazione e filtro delle categorie di contenuti.

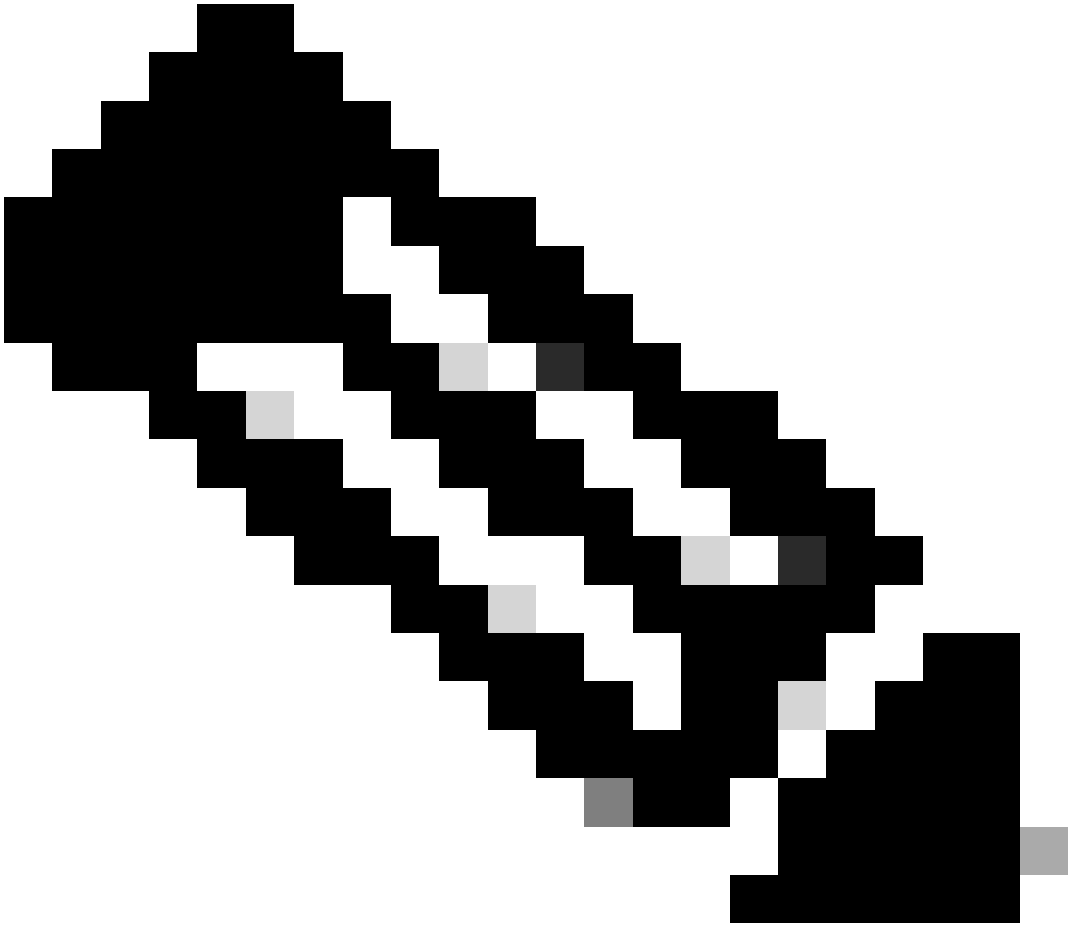


4409322363924

Identificazione utente Web

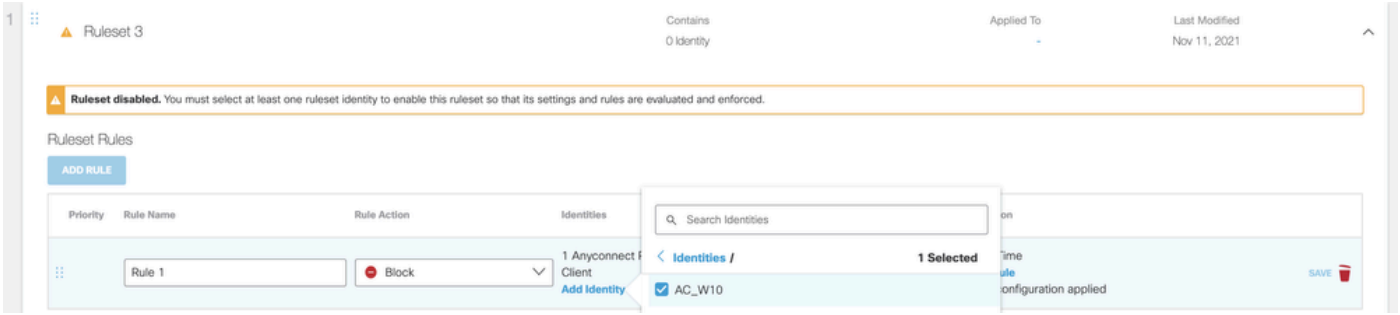
Per impostazione predefinita, il traffico di Accesso remoto non può essere controllato per singoli utenti o gruppi. Lo stesso criterio si applica a tutto il traffico RA in base all'identità "ID dell'orge di Accesso remoto". Per aggiungere l'identificazione utente/gruppo, sono disponibili due opzioni:

- Installare il modulo AnyConnect Umbrella Roaming Security e abilitare la funzione dell'agente SWG. L'agente invia il traffico Web direttamente a Umbrella SWG con l'identità di "computer in roaming" applicata. Questo modulo supporta inoltre l'identificazione utente facoltativa di Active Directory.
- Abilitare SAML nel set di regole Web che influisce sull'identità dell'ID di accesso remoto. Dopo la connessione all'accesso remoto, agli utenti RA viene richiesto di eseguire una seconda autenticazione tramite SAML durante la generazione del traffico del browser Web.



Nota: Quando si usa il modulo Umbrella per AnyConnect, il traffico SWG può essere inviato facoltativamente all'interno o all'esterno del tunnel a seconda della configurazione del tunneling suddiviso.

Nell'esempio viene mostrato come configurare un criterio DNS (Criteri > Criteri DNS) per un singolo client AnyConnect - ciò è possibile solo quando viene distribuito il modulo di roaming Umbrella AnyConnect:

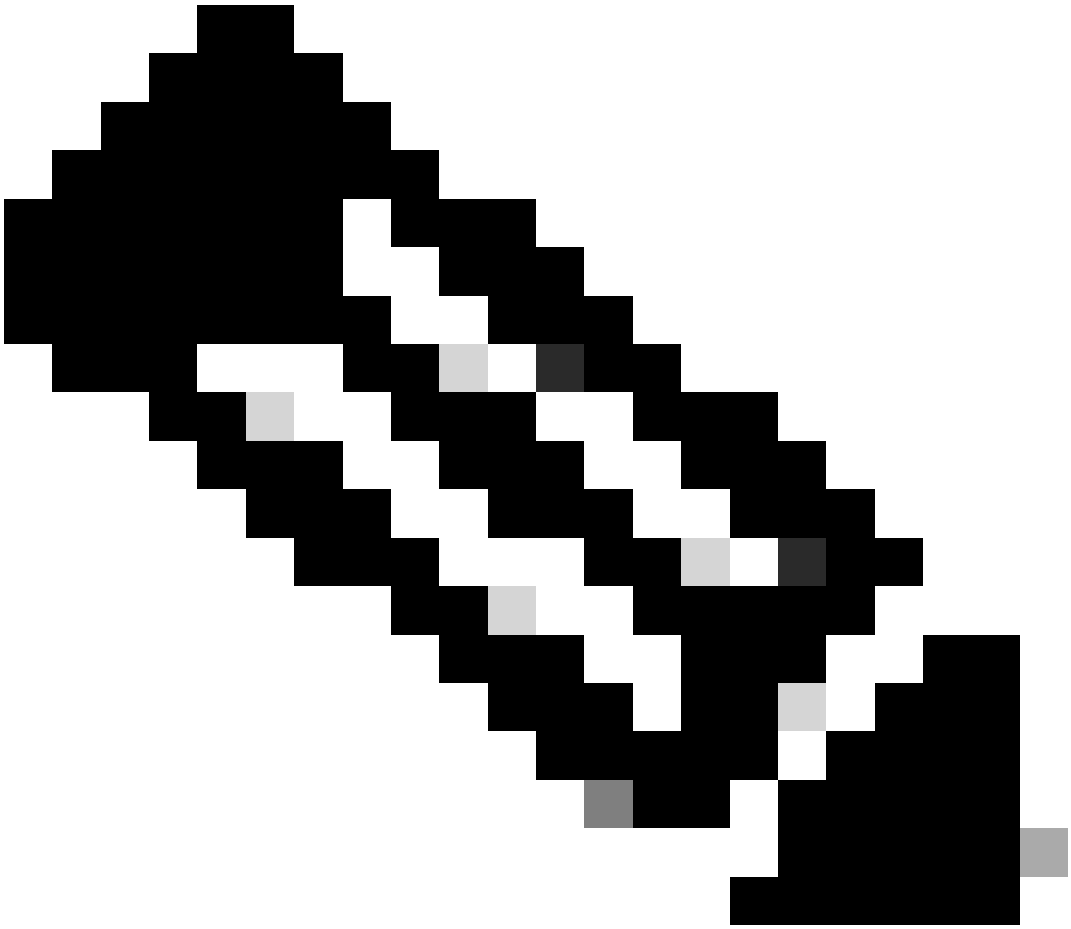


4410210499476

Criteri di prevenzione della perdita dei dati

Le policy sulla perdita di dati si applicano al traffico tra i client di accesso remoto (AnyConnect) e Internet. Configurare le regole in 'Distribuzioni > Criteri di prevenzione della perdita di dati' come indicato nella documentazione disponibile qui: Gestire i criteri di protezione dei dati.

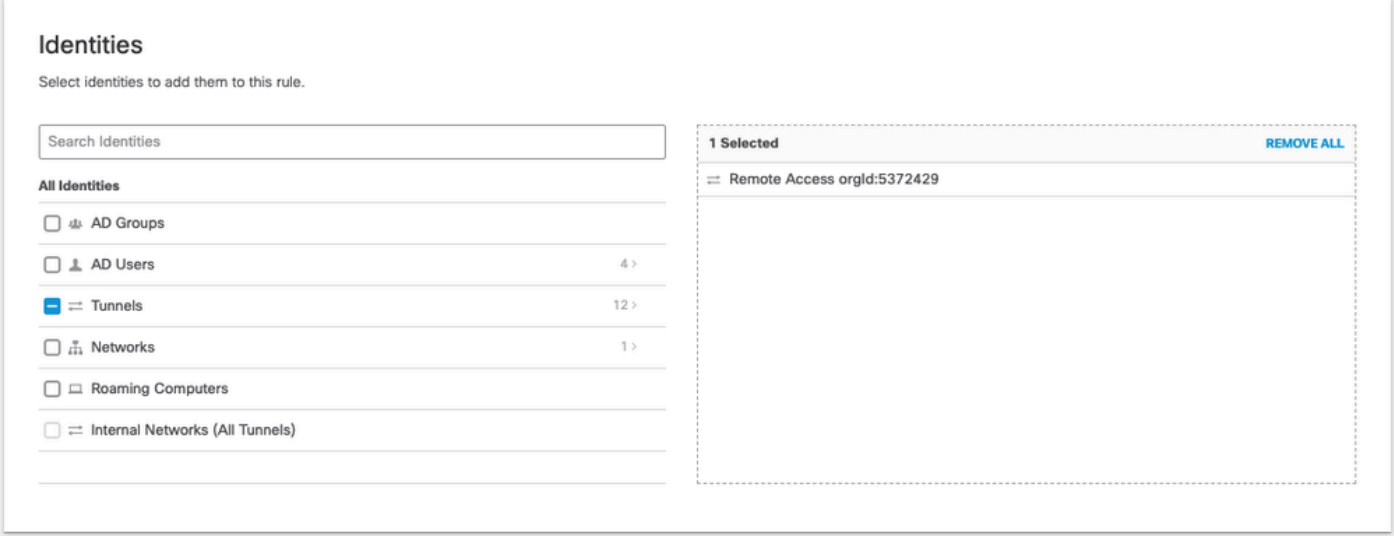
- I criteri di prevenzione della perdita dei dati non vengono utilizzati per controllare l'accesso tra i client di Autorità registrazione integrità e i server Web Private/Branch. I criteri di prevenzione della perdita dei dati si applicano solo al traffico di siti Web esterni.



Nota: Per applicare i criteri di prevenzione della perdita dei dati, è necessario aver creato un set di regole Web per gli utenti di Accesso remoto. Il set di regole Web deve avere la decrittografia HTTPS abilitata.

Quando si selezionano le identità per una regola di protezione dei dati, scegliere l'ID di accesso remoto:<ID>. Lo stesso criterio di protezione dei dati si applica a tutti gli utenti. Per completare la regola di prevenzione della perdita dei dati è inoltre necessario selezionare o definire i

classificatori di prevenzione della perdita dei dati.



4409322428820

Identificazione utente DLP

DLP ottiene l'identità utente dal gateway Web sicuro (criteri Web). Per istruzioni su come aggiungere l'identificazione utente, consultare la sezione Criteri Web.

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).