Configurare il client Umbrella Roaming su una rete aziendale

Sommario

Introduzione

Questo documento descrive la configurazione del client di roaming Umbrella sulla rete aziendale.

Panoramica

Il client di roaming Umbrella è un ottimo strumento per la protezione degli utenti remoti, ma può anche proteggere gli utenti sulla rete aziendale, aggiungendo un altro livello di sicurezza. A seconda delle esigenze dell'azienda alcuni amministratori desiderano la protezione continua del client di roaming Umbrella sulla rete aziendale, mentre altri amministratori preferiscono che il client di roaming Umbrella "si ritorni" a favore di altre politiche Umbrella.

Umbrella offre flessibilità su come il client di roaming Umbrella funziona quando entra nella rete. In questo articolo vengono delineati questi diversi approcci.

Obiettivi

D). Perché disattivare il client di roaming Umbrella sulla rete aziendale?

In genere non è necessario disabilitare il client di roaming Umbrella per il funzionamento del DNS interno ed esterno. Il client di roaming Umbrella utilizza la funzionalità di gestione dei domini per indirizzare il traffico DNS interno ai normali server DNS. Ciò consente di mantenere la protezione e la connettività mentre il client di roaming Umbrella viene eseguito sugli endpoint della rete.

Tuttavia, a volte vi sono motivi per prendere in considerazione la disabilitazione della protezione del client in roaming...

- Fornire un criterio "*in rete*" e "*fuori rete*" diverso agli utenti in roaming che lasciano la rete.
- L'utilizzo di un server DNS interno in una rete aziendale offre alcuni vantaggi in termini di memorizzazione nella cache e riduzione del traffico DNS in uscita.
- Il client di roaming Umbrella invia periodicamente messaggi di richiesta per verificare la connessione con Umbrella. Questo traffico aggiuntivo può essere indesiderato quando si dispone di un numero elevato di client.

D) Perché dovrei voler mantenere abilitato il client di roaming Umbrella sulla mia rete aziendale?

D'altro canto, ci sono ottime ragioni per mantenere sempre abilitato il client di roaming:

- Verificare che il computer client Umbrella mobile utilizzi sempre lo stesso criterio.
- Sempre identificabile nei report (anziché nell'identità di rete) il nome host del client di roaming Umbrella per la creazione di report granulari.
- Il client in roaming utilizza il traffico 'Encrypted DNS' per migliorare la privacy
- Per gli utenti gateway Web sicuri (che usano AnyConnect), il client deve rimanere abilitato per fornire il filtro Web SWG.

Modalità operative

Sempre attivo

Il client di roaming Umbrella può rimanere attivo anche quando viene utilizzato sulla rete aziendale. In questa modalità i criteri vengono configurati utilizzando l'identità del client mobile Umbrella e tale identità viene visualizzata nei report.

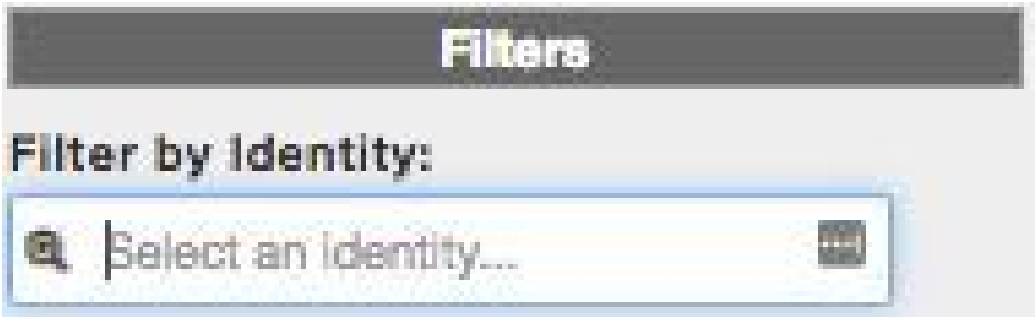
Policy	L'identità del client mobile Umbrella viene utilizzata sempre.
Creazione di report	L'identità del client mobile Umbrella viene sempre visualizzata nei report che offrono granularità per computer
Traffico DNS	• Il client di roaming Umbrella continua a inviare query DNS direttamente a Umbrella, anche quando si trova su una rete aziendale. • Le query inviate a Umbrella sono crittografate, fornendo ulteriore protezione. • Le query per 'Domini interni' vengono instradate ai normali server DNS e non inviate a Umbrella.

Messaggi probe	Il client di roaming Umbrella continua a inviare messaggi di prova per determinare la disponibilità di Umbrella.

Come configurare la modalità 'Always ON':

1. Passare a Identità > Computer mobili.
2. Fare clic sull'icona (Impostazioni client mobili).
3. Deselezionare Disabilita reindirizzamento DNS in una rete protetta da Umbrella e fare clic su Salva.
4. Crea un criterio separato per i tuoi client di roaming Umbrella e assicurati che sia la priorità più alta (in cima all'elenco). I criteri per i client mobili Umbrella devono avere una priorità più alta rispetto ai criteri basati sulle identità di rete.

Usa criteri di rete regolari
Il client di roaming Umbrella è abilitato e continua a parlare direttamente con Umbrella, tuttavia, l'identità di rete viene utilizzata sia per la policy che per la creazione di report. Questa modalità viene attivata semplicemente inserendo il criterio di rete con una precedenza maggiore rispetto al criterio del client di roaming Umbrella.

Policy	Il criterio di rete viene utilizzato quando ci si trova nella rete protetta. Ciò consente l'applicazione di criteri di rete di attivazione/disattivazione diversi.
Creazione di report	• La creazione di rapporti è associata all'identità di rete come identità primaria. • La creazione di rapporti consente comunque di eseguire ricerche tramite il nome host del client mobile Umbrella per filtrare i risultati solo per quel client. 
Traffico DNS	• Il client di roaming Umbrella continua a inviare query DNS direttamente

	a Umbrella, anche quando si trova su una rete aziendale. • Le query inviate a Umbrella sono crittografate, fornendo ulteriore protezione. • Le query per 'Domini interni' vengono instradate ai normali server DNS e non inviate a Umbrella.
Messaggi probe	Il client di roaming Umbrella continua a inviare messaggi di prova per determinare la disponibilità di Umbrella.

Come utilizzare i criteri di rete normali:

1. Passare a Identità > Computer mobili.
2. Fare clic sull'icona (Impostazioni client mobili).
3. Deselezionare Disabilita reindirizzamento DNS in una rete protetta da Umbrella e fare clic su Salva.
4. Creare un criterio separato per le reti. Verificare che i criteri per le reti abbiano la precedenza su tutti i criteri basati sul client di roaming.

Disabilitazione dietro reti protette (ideale per reti più piccole)
Il client di roaming Umbrella può 'interrompersi' quando rileva che si trova su una rete protetta. Ciò significa che l'identità di rete viene utilizzata sia per la definizione dei criteri che per la creazione dei rapporti.

Questa modalità è simile alla modalità 'Usa criteri di rete regolari', con la differenza che il client di roaming Umbrella si disattiva effettivamente e non interferisce con il traffico DNS.

Policy	Il criterio di rete viene utilizzato quando ci si trova nella rete protetta. Ciò consente l'applicazione di criteri di rete di attivazione/disattivazione diversi.
Creazione di report	Quando nella rete protetta non è presente alcuna granularità per singolo computer per il report. La creazione di rapporti è associata solo all'identità di rete.
Traffico DNS	Quando si trova nella rete protetta, il client di roaming Umbrella non interferisce con le query DNS e passa al normale server DNS interno.

Messaggi probe	Il client di roaming Umbrella continua a inviare messaggi di prova per determinare che si trova in una rete protetta.

Come configurare Disabilita dietro reti protette:

1. Passare a Identità > Computer mobili.
2. Fare clic sull'icona (Impostazioni client mobili).
3. Selezionare Disabilita reindirizzamento DNS in una rete protetta da Umbrella e fare clic su Salva.
4. Passare a Criteri > Elenco criteri.
5. Creare un criterio separato per le reti. Verificare che i criteri per le reti abbiano la precedenza su tutti i criteri basati sul client di roaming Umbrella.
6. I server DNS locali devono essere inoltrati ai resolver Umbrella e devono essere registrati correttamente nel dashboard Umbrella.
7. Affinché questa funzionalità funzioni, l'indirizzo IP in uscita utilizzato dalla workstation client deve essere registrato con la stessa identità di rete dell'indirizzo IP in uscita utilizzato dai server DNS interni. Per ulteriori informazioni, vedere questo articolo.

Disabilita dietro dominio di rete trusted (ideale per reti di grandi dimensioni)

È ora possibile scegliere un 'Dominio di rete trusted' configurato dal cliente. Il client tenta di risolvere questo dominio DNS (record A) e di disabilitare la protezione quando il dominio viene risolto correttamente. Questo record deve essere un record DNS solo interno che viene risolto solo quando il client si trova nella rete aziendale.

Policy	Il client si interrompe ogni volta che viene rilevato il dominio trusted e non riceve necessariamente criteri Umbrella o filtri. Si consiglia di aggiungere altre funzionalità Umbrella (ad es. protezione della rete) per garantire che i criteri siano ancora applicati alla rete aziendale.
Creazione di report	Il client si interrompe ogni volta che viene rilevato il dominio trusted e non riceve necessariamente criteri Umbrella o filtri. Se la rete è protetta da altre funzionalità Umbrella (ad esempio Network Protection), il traffico viene visualizzato nei report sotto l'identità di rete.
Traffico DNS	Quando il client di roaming Umbrella si trova sulla rete attendibile, non interferisce con le query DNS e passa al normale server DNS interno.

Messaggi probe	Il client di roaming Umbrella disabilita la maggior parte dei test 'probe' DNS in questo stato, riducendo notevolmente la quantità di traffico generato dai client di roaming.

Come configurare il dominio di rete trusted:

1. Creare un record A DNS nei server DNS interni (ad esempio Magic.mydomain.tld).
    1. Il record deve essere un "sottodominio" (almeno 3 etichette DNS)
    2. Il record deve essere risolto in un indirizzo interno RFC-1918
    3. Fai attenzione a non far sì che il documento esista pubblicamente
2. Passare a Identità > Computer mobili.
3. Fare clic sull'icona (Impostazioni client mobili).
4. Selezionare l'opzione Dominio di rete trusted e immettere il nome di dominio, ad esempio Magic.mydomain.tld). Fare clic su Save (Salva).

Uso del client di roaming Umbrella con un'appliance virtuale Umbrella

Come parte del prodotto 'Insights' Umbrella (nei pacchetti Platform and Insights) forniamo una Virtual Appliance (VA) che agisce come server d'inoltro DNS all'interno della vostra rete. Questa VA è la chiave per ottenere visibilità sull'origine delle richieste DNS nella rete ed è necessaria anche per l'integrazione di Active Directory.

Per impostazione predefinita, il client di roaming Umbrella si disattiva se rileva che è in uso un VA per l'inoltro DNS. Se la VA è stata assegnata come server DNS (tramite le impostazioni DHCP o statiche), il client di roaming Umbrella lo rileva e lo disattiva.

Ritorno VA

Policy	Con il backoff VA abilitato, l'identità VA viene utilizzata per decidere il criterio scelto. È possibile creare criteri in base alle seguenti identità: • Utente AD (solo se l'integrazione AD è abilitata) • Computer AD (solo se l'integrazione AD è abilitata) • Rete interna • Nome sito ombrello. Fare clic qui per ulteriori informazioni sulla precedenza dei criteri.
Creazione di report	Con il backoff VA abilitato, il client di roaming Umbrella è disabilitato quando è dietro un VA e non viene visualizzato nei report. Il report viene registrato come:

	• Utente AD (solo se l'integrazione AD è abilitata) • Computer AD (solo se l'integrazione AD è abilitata) • Rete interna • Nome sito ombrello. Inoltre, per ogni richiesta viene registrato l'indirizzo IP del client interno. 
Traffico DNS	• Il client di roaming Umbrella non interferisce con le query DNS e passa all'appliance virtuale. • Il VSA inoltra le query DNS esterne a Umbrella (crittografata). • Il VSA instrada le query DNS interne in modo appropriato e le inoltra ai server DNS interni configurati.
Messaggi probe	Il client di roaming Umbrella invia ancora messaggi di richiesta a Umbrella, ma a un tasso ridotto.

Come configurare il backoff VA:

1. Questa funzione è abilitata per impostazione predefinita, ma è possibile controllarne lo stato (ed eventualmente disabilitarla)
2. Passare a Identità > Computer mobili.
3. Fare clic sull'icona (Impostazioni client mobili).
4. Selezionare l'opzione Backoff VA

Cisco Umbrella AnyConnect Roaming Security Module

Il modulo Umbrella per Cisco AnyConnect supporta tutte le modalità operative descritte sopra. Sono inoltre disponibili due modalità AnyConnect aggiuntive specifiche. Entrambe queste modalità possono essere abilitate in Umbrella Dashboard nella pagina Identità > Computer mobili, tuttavia, è necessaria un'ulteriore configurazione all'interno del profilo VPN di AnyConnect.

- Rispetta AnyConnect Trusted Network Detection.
  Questa funzione determina la disabilitazione del modulo Umbrella Security quando Cisco AnyConnect determina che si trova su una rete attendibile. Per identificare la rete, usare la funzionalità di rilevamento di reti attendibili di AnyConnect. È possibile utilizzare domini, server DNS e URL attendibili per identificare la rete aziendale. Per ulteriori informazioni, consultare la documentazione di AnyConnect.
- Disabilita client mobile mentre sono attive sessioni VPN full-tunnel
  Con questa funzione abilitata, il modulo Umbrella viene disabilitato quando AnyConnect è connesso a una VPN con tunnel completo (o Tunnel All DNS).

Quando è disattivato, il client di roaming non filtra il traffico DNS, quindi è importante assicurarsi che la rete sia protetta da altre misure di sicurezza, come la funzionalità Protezione rete.

Ulteriori informazioni

Se si desidera disabilitare il client di roaming sulla rete aziendale ma è necessario un maggiore controllo o discutere di altre opzioni, contattare il supporto Cisco Umbrella.

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).