Konfiguration eines Umbrella-Roaming-Clients in einem Unternehmensnetzwerk

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des Umbrella-Roaming-Clients in Ihrem Unternehmensnetzwerk beschrieben.

Überblick

Der Umbrella-Roaming-Client ist ein hervorragendes Tool zum Schutz von Remote-Benutzern. Er kann jedoch auch die Benutzer in Ihrem Unternehmensnetzwerk schützen und eine weitere Sicherheitsebene hinzufügen. Je nach den Anforderungen des Unternehmens wünschen einige Administratoren einen kontinuierlichen Schutz des Umbrella-Roaming-Clients im Unternehmensnetzwerk, während andere Administratoren es vorziehen, den Umbrella-Roaming-Client zugunsten anderer Umbrella-Richtlinien "zurückzustellen".

Umbrella bietet Flexibilität bei der Funktionsweise des Umbrella-Roaming-Clients, wenn dieser in Ihr Netzwerk eintritt. In diesem Artikel werden diese verschiedenen Ansätze erläutert.

Ziele

F). Warum sollte ich den Umbrella-Roaming-Client in meinem Firmennetzwerk deaktivieren?

Normalerweise muss der Umbrella-Roaming-Client nicht deaktiviert werden, damit interne und externe DNS-Dienste funktionieren. Der Umbrella-Roaming-Client verwendet die Domänenmanagement-Funktion, um den internen DNS-Datenverkehr an die normalen DNS-Server weiterzuleiten. Auf diese Weise können Sie sowohl den Schutz als auch die Konnektivität aufrechterhalten, während der Umbrella-Roaming-Client auf Ihren Endgeräten im Netzwerk

ausgeführt wird.

Manchmal gibt es jedoch Gründe, den Schutz des Roaming-Clients zu deaktivieren...

- Bereitstellung einer anderen "*netzinternen*" und "*netzexternen*" Richtlinie für Roaming-Benutzer, die das Netzwerk verlassen.
- Die Verwendung eines internen DNS-Servers in einem Unternehmensnetzwerk bietet einige Vorteile im Hinblick auf Caching und die Reduzierung des ausgehenden DNS-Datenverkehrs.
- Der Umbrella-Roaming-Client sendet regelmäßig Testnachrichten, um die Verbindung zu Umbrella zu überprüfen. Dieser zusätzliche Datenverkehr kann unerwünscht sein, wenn Sie eine sehr große Anzahl von Clients haben.

F) Warum sollte der Umbrella-Roaming-Client in meinem Firmennetzwerk aktiviert bleiben?

Andererseits gibt es einige gute Gründe, den Roaming-Client immer aktiviert zu lassen:

- Stellen Sie sicher, dass der Umbrella-Roaming-Client-Computer stets die gleiche Richtlinie verwendet.
- Immer den Hostnamen des Umbrella-Roaming-Clients in Berichten identifizierbar (anstelle der Netzwerkidentität) - für detaillierte Berichte.
- Der Roaming-Client verwendet 'Encrypted DNS'-Datenverkehr, um den Datenschutz zu verbessern
- Für Benutzer des sicheren Web-Gateways (mit AnyConnect) muss der Client aktiviert bleiben, um SWG-Webfilterung bereitzustellen.

Betriebsmodi

Immer EIN

Der Umbrella-Roaming-Client kann selbst dann aktiv bleiben, wenn er im Firmennetzwerk verwendet wird. In diesem Modus werden Richtlinien mithilfe der Umbrella-Roaming-Client-Identität konfiguriert, und diese Identität wird in Berichten angezeigt.

Richtlinie	Die Umbrella-Roaming-Client-Identität wird immer verwendet.
Berichterstellung	Die Umbrella-Roaming-Client-Identität wird immer in Berichten mit gerätespezifischer Detailgenauigkeit angezeigt.
DNS-	• Der Umbrella-Roaming-Client sendet weiterhin DNS-Anfragen direkt

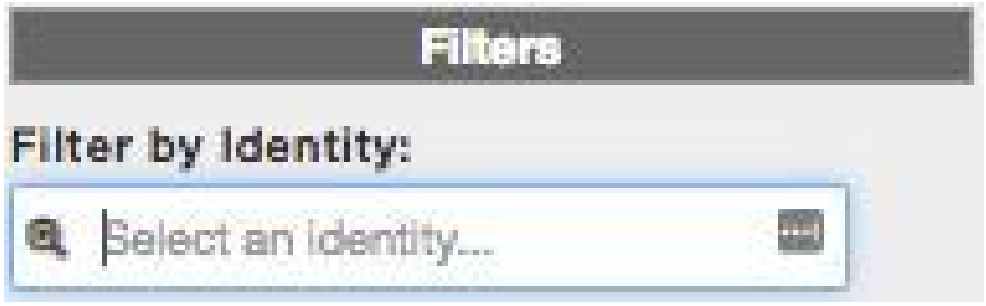
Datenverkehr	an Umbrella, selbst wenn er sich in einem Firmennetzwerk befindet. • An Umbrella gesendete Abfragen werden verschlüsselt, um zusätzliche Sicherheit zu gewährleisten. • Abfragen für 'interne Domänen' werden an Ihre normalen DNS-Server weitergeleitet und nicht an Umbrella gesendet.
Testnachrichten	Der Umbrella-Roaming-Client sendet weiterhin Testnachrichten, um die Verfügbarkeit von Umbrella zu ermitteln.

So konfigurieren Sie den Always ON-Modus:

1. Navigieren Sie zu Identitäten > Roaming Computers.
2. Klicken Sie auf das Symbol (Roaming-Client-Einstellungen).
3. Deaktivieren Sie die DNS-Umleitung in einem Umbrella Protected Network, und klicken Sie auf Speichern.
4. Erstellen Sie eine separate Richtlinie für Ihre Umbrella-Roaming-Clients, und stellen Sie sicher, dass dies die höchste Priorität hat (ganz oben in der Liste). Ihre Umbrella-Richtlinie für Roaming-Clients muss eine höhere Priorität haben als alle Richtlinien, die auf Netzwerkidentitäten basieren.

Verwendung regulärer Netzwerkrichtlinien
Der Umbrella-Roaming-Client ist aktiviert und kommuniziert weiterhin direkt mit Umbrella. Die Netzwerkidentität wird jedoch sowohl für Richtlinien- als auch für Berichtszwecke verwendet. Dieser Modus wird einfach aktiviert, indem die Netzwerkrichtlinie eine höhere Priorität erhält als die Umbrella-Richtlinie für Roaming-Clients.

Richtlinie	Die Netzwerkrichtlinie wird im geschützten Netzwerk verwendet. Dies ermöglicht unterschiedliche Netzwerkrichtlinien für die An- und Abschaltung.
Berichterstellung	• Die Berichterstellung ist mit der Netzwerkidentität als primärer Identität verknüpft. • Die Berichterstellung ermöglicht es Ihnen weiterhin, über den Umbrella-Roaming-Client-Hostnamen nach Ergebnissen zu suchen, die nur für diesen Client bestimmt sind.

	
DNS-Datenverkehr	• Der Umbrella-Roaming-Client sendet weiterhin DNS-Anfragen direkt an Umbrella, selbst wenn er sich in einem Firmennetzwerk befindet. • An Umbrella gesendete Abfragen werden verschlüsselt, um zusätzliche Sicherheit zu gewährleisten. • Abfragen für 'interne Domänen' werden an Ihre normalen DNS-Server weitergeleitet und nicht an Umbrella gesendet.
Testnachrichten	Der Umbrella-Roaming-Client sendet weiterhin Testnachrichten, um die Verfügbarkeit von Umbrella zu ermitteln.

So verwenden Sie die reguläre Netzwerkrichtlinie:

1. Navigieren Sie zu Identitäten > Roaming Computers.
2. Klicken Sie auf das Symbol (Roaming-Client-Einstellungen).
3. Deaktivieren Sie die DNS-Umleitung in einem Umbrella Protected Network, und klicken Sie auf Speichern.
4. Erstellen Sie eine separate Richtlinie für Ihre Netzwerke. Stellen Sie sicher, dass die Richtlinie für Ihre Netzwerke eine höhere Priorität hat als alle Richtlinien, die auf dem Roaming-Client basieren.

Deaktivieren Sie Protected Networks (Ideal für kleinere Netzwerke)
Der Umbrella-Roaming-Client kann sich zurückziehen, wenn er erkennt, dass er sich in einem geschützten Netzwerk befindet. Das bedeutet, dass die Netzwerkidentität sowohl für Richtlinien- als auch für Berichterstellungszwecke verwendet wird.

Dieser Modus ähnelt dem Modus "Use Regular Network Policy" (Reguläre Netzwerkrichtlinie verwenden), mit der Ausnahme, dass der Umbrella-Roaming-Client sich selbst deaktiviert und den DNS-Datenverkehr nicht beeinträchtigt.

Richtlinie	Die Netzwerkrichtlinie wird im geschützten Netzwerk verwendet. Dies ermöglicht unterschiedliche Netzwerkrichtlinien für die An- und Abschaltung.

Berichterstellung	Wenn sich das geschützte Netzwerk befindet, ist die Berichterstellung nicht auf einzelne Systeme zugeschnitten. Die Berichterstellung ist nur mit der Netzwerkidentität verknüpft.
DNS-Datenverkehr	Wenn sich der Umbrella-Roaming-Client im geschützten Netzwerk befindet, beeinträchtigt er nicht die DNS-Abfragen und geht zum normalen internen DNS-Server.
Testnachrichten	Der Umbrella-Roaming-Client sendet weiterhin Testnachrichten, um festzustellen, dass er sich in einem geschützten Netzwerk befindet.

So konfigurieren Sie Disable hinter geschützten Netzwerken:

1. Navigieren Sie zu Identitäten > Roaming Computers.
2. Klicken Sie auf das Symbol (Roaming-Client-Einstellungen).
3. Wählen Sie DNS-Umleitung deaktivieren, während Sie sich in einem Umbrella Protected Network befinden, und klicken Sie auf Speichern.
4. Navigieren Sie zu Richtlinien > Richtlinienliste.
5. Erstellen Sie eine separate Richtlinie für Ihre Netzwerke. Stellen Sie sicher, dass die Richtlinie für Ihre Netzwerke eine höhere Priorität hat als alle Richtlinien, die auf dem Umbrella Roaming Client basieren.
6. Ihre lokalen DNS-Server müssen an Umbrella-Resolver weitergeleitet und im Umbrella-Dashboard richtig registriert werden.
7. Damit diese Funktion funktioniert, muss die von der Client-Workstation verwendete Ausgangs-IP in derselben Netzwerkidentität registriert sein wie die Ausgangs-IP, die von den internen DNS-Servern verwendet wird. Ausführliche Informationen finden Sie in diesem Artikel.

Deaktivierung hinter vertrauenswürdiger Netzwerkdomäne (ideal für größere Netzwerke)

Sie können jetzt eine vom Kunden konfigurierte vertrauenswürdige Netzwerkdomäne auswählen. Der Client versucht, diese DNS-Domäne (A-Eintrag) aufzulösen und den Schutz zu deaktivieren, wenn die Domäne erfolgreich aufgelöst wird. Hierbei handelt es sich um einen rein internen DNS-Eintrag, der nur aufgelöst wird, wenn sich der Client im Unternehmensnetzwerk befindet.

Richtlinie	Der Client gibt ein Backup ab, wenn die vertrauenswürdige Domäne erkannt wird und nicht unbedingt die Umbrella-Richtlinie oder -Filterung erhält. Wir empfehlen, weitere Umbrella-Funktionen (z. B. Netzwerkschutz), um sicherzustellen, dass die Richtlinien im

	Unternehmensnetzwerk weiterhin angewendet werden.
Berichterstellung	Der Client gibt ein Backup ab, wenn die vertrauenswürdige Domäne erkannt wird und nicht unbedingt die Umbrella-Richtlinie oder -Filterung erhält. Wenn das Netzwerk durch andere Umbrella-Funktionen (z. B. Netzwerkschutz), dann wird der Datenverkehr in Berichten unter der Netzwerkidentität angezeigt.
DNS-Datenverkehr	Wenn sich der Umbrella-Roaming-Client im vertrauenswürdigen Netzwerk befindet, beeinträchtigt er die DNS-Abfragen nicht und wird an den normalen internen DNS-Server weitergeleitet.
Testnachrichten	Der Umbrella-Roaming-Client deaktiviert den Großteil seiner DNS-Tests in diesem Zustand, wodurch der von Roaming-Clients generierte Datenverkehr erheblich reduziert wird.

So konfigurieren Sie eine vertrauenswürdige Netzwerkdomäne:

1. Erstellen Sie einen DNS-A-Eintrag auf Ihren internen DNS-Servern (z. B. magic.mydomain.tld).
    1. Der Datensatz muss eine "Sub-Domäne" sein (mindestens 3 DNS-Labels).
    2. Der Datensatz muss zu einer internen RFC-1918-Adresse aufgelöst werden.
    3. Achten Sie darauf, dass der Datensatz nicht öffentlich vorhanden ist.
2. Navigieren Sie zu Identitäten > Roaming Computers.
3. Klicken Sie auf das Symbol (Roaming-Client-Einstellungen).
4. Wählen Sie die Option Trusted Network Domain (Vertrauenswürdige Netzwerkdomäne) aus, und geben Sie den Domänennamen ein (z. B. magic.mydomain.tld). Klicken Sie auf Speichern.

Verwendung des Umbrella Roaming Client mit einer Umbrella Virtual Appliance

Als Teil des Umbrella 'Insights'-Produkts (im Platform and Insights-Paket) stellen wir eine virtuelle Appliance (VA) bereit, die als DNS-Forwarder innerhalb Ihres Netzwerks fungiert. Diese VA ist der Schlüssel zur Transparenz der Quelle von DNS-Anfragen in Ihrem Netzwerk und auch für unsere Active Directory-Integration erforderlich.

Standardmäßig deaktiviert sich der Umbrella-Roaming-Client selbst, wenn er erkennt, dass eine VA für die DNS-Weiterleitung verwendet wird. Wenn die VA als DNS-Server zugewiesen wurde

(entweder über DHCP oder statische Einstellungen), erkennt der Umbrella-Roaming-Client dies und deaktiviert sich selbst.

VA-Backoff

Richtlinie	Bei aktiviertem VA-Backoff wird die VA-Identität verwendet, um die gewählte Richtlinie zu bestimmen. Richtlinien können auf Grundlage der folgenden Identitäten erstellt werden: • AD-Benutzer (nur bei aktivierter AD-Integration) • AD-Computer (nur bei aktivierter AD-Integration) • Internes Netzwerk • Umbrella-Standortname. Klicken Sie hier, um weitere Informationen zur Priorität von Richtlinien zu erhalten.
Berichterstellung	Wenn VA-Backoff aktiviert ist, wird der Umbrella-Roaming-Client hinter einer VA deaktiviert und nicht in Berichten angezeigt. Die Berichterstellung wird protokolliert als: • AD-Benutzer (nur bei aktivierter AD-Integration) • AD-Computer (nur bei aktivierter AD-Integration) • Internes Netzwerk • Umbrella-Standortname. Außerdem wird für jede Anforderung die interne Client-IP-Adresse protokolliert. 
DNS-Datenverkehr	• Der Umbrella-Roaming-Client beeinträchtigt die DNS-Abfragen nicht und leitet sie an die virtuelle Appliance weiter. • Die VA leitet externe DNS-Abfragen an Umbrella (verschlüsselt) weiter. • Die VA leitet interne DNS-Abfragen nach Bedarf weiter und leitet sie an die konfigurierten internen DNS-Server weiter.
Testnachrichten	Der Umbrella-Roaming-Client sendet weiterhin Testnachrichten an Umbrella, jedoch mit einer reduzierten Rate.

So konfigurieren Sie VA Backoff:

1. Diese Funktion ist standardmäßig aktiviert, Sie können jedoch ihren Status überprüfen (und sie optional deaktivieren).
2. Navigieren Sie zu Identitäten > Roaming Computers.
3. Klicken Sie auf das Symbol (Roaming-Client-Einstellungen).
4. Option VA Backoff auswählen

Cisco Umbrella AnyConnect Roaming-Sicherheitsmodul

Das Umbrella-Modul für Cisco AnyConnect unterstützt alle oben beschriebenen Betriebsmodi. Zwei weitere AnyConnect-spezifische Modi stehen ebenfalls zur Verfügung. Beide Modi können in Ihrem Umbrella Dashboard auf der Seite Identitäten > Roaming-Computer aktiviert werden. Im AnyConnect VPN-Profil ist jedoch eine zusätzliche Konfiguration erforderlich.

- Respektieren Sie die AnyConnect Trusted Network Detection.
  Diese Funktion bewirkt, dass das Umbrella Security-Modul deaktiviert wird, wenn Cisco AnyConnect feststellt, dass es sich in einem vertrauenswürdigen Netzwerk befindet. Dies beruht auf der AnyConnect-Funktion zur Erkennung vertrauenswürdiger Netzwerke zur Identifizierung des Netzwerks. Sie können vertrauenswürdige Domänen, DNS-Server und URLs verwenden, um Ihr Unternehmensnetzwerk zu identifizieren. Weitere Informationen finden Sie in der AnyConnect-Dokumentation.
- Deaktivieren des Roaming-Clients, während VPN-Sitzungen im gesamten Tunnel aktiv sind
  Wenn diese Funktion aktiviert ist, wird das Umbrella-Modul deaktiviert, wenn AnyConnect mit einem Full Tunnel (oder Tunnel All DNS) VPN verbunden ist.

Wenn der Roaming-Client deaktiviert ist, wird der DNS-Verkehr nicht gefiltert. Daher ist es wichtig, sicherzustellen, dass Ihr Netzwerk durch andere Sicherheitsmaßnahmen wie die Netzwerkschutzfunktion abgedeckt ist.

Weitere Informationen

Wenn Sie den Roaming-Client in Ihrem Unternehmensnetzwerk deaktivieren möchten, aber mehr Kontrolle benötigen oder andere Optionen besprechen möchten, wenden Sie sich an den Cisco Umbrella Support.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.