Konfigurieren von SIG-Richtlinien für den Remote-Zugriff für Secure Connect-Benutzer

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie SIG-Richtlinien für den Remote-Zugriff für Secure Connect-Benutzer erstellen.

Überblick

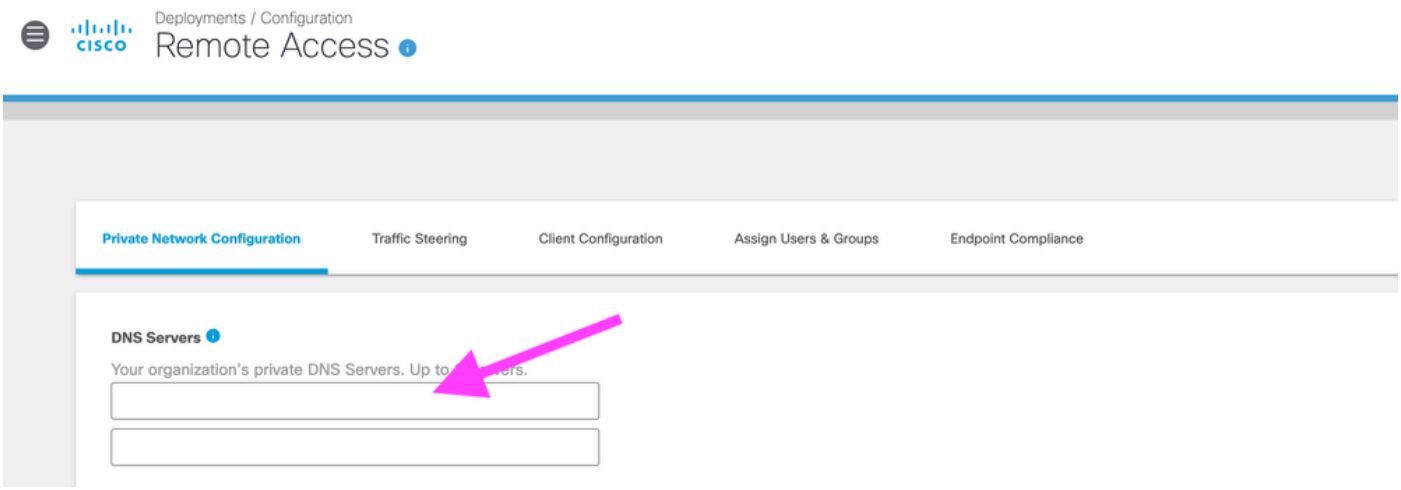
Dieser Knowledgebase-Artikel bezieht sich auf Kunden, die ein Secure Connect-Paket verwenden, das Remote Access (VPNaaS)-Funktionen in Umbrella beinhaltet.

Administratoren können Umbrella Firewall-, Web- und Data Loss-Richtlinien so konfigurieren, dass sie auf Roaming-Benutzer angewendet werden, die über AnyConnect mit Remote Access verbunden sind.

DNS-Richtlinien

Es ist möglich, DNS-Abfragen an Umbrella-Resolver (z.B. 208.67.222.222) über die AnyConnect Remote Access VPN-Verbindung. Dies ermöglicht jedoch keine Identifizierung, Richtlinien oder Berichterstellung für DNS-Datenverkehr auf dem Umbrella Dashboard.

- Dies bietet nur die DNS-Auflösung und wird daher in der Regel nicht empfohlen.
- Die Verwendung externer DNS-Resolver in der VPN-DNS-Konfiguration verhindert die Auflösung interner DNS-Zonen.

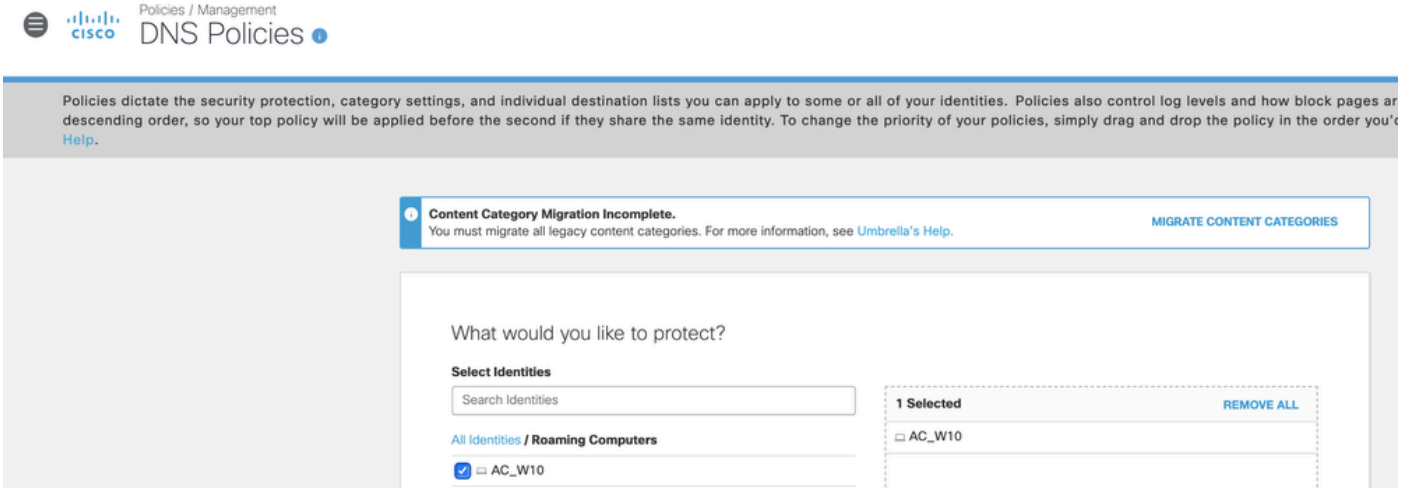


4410210378004

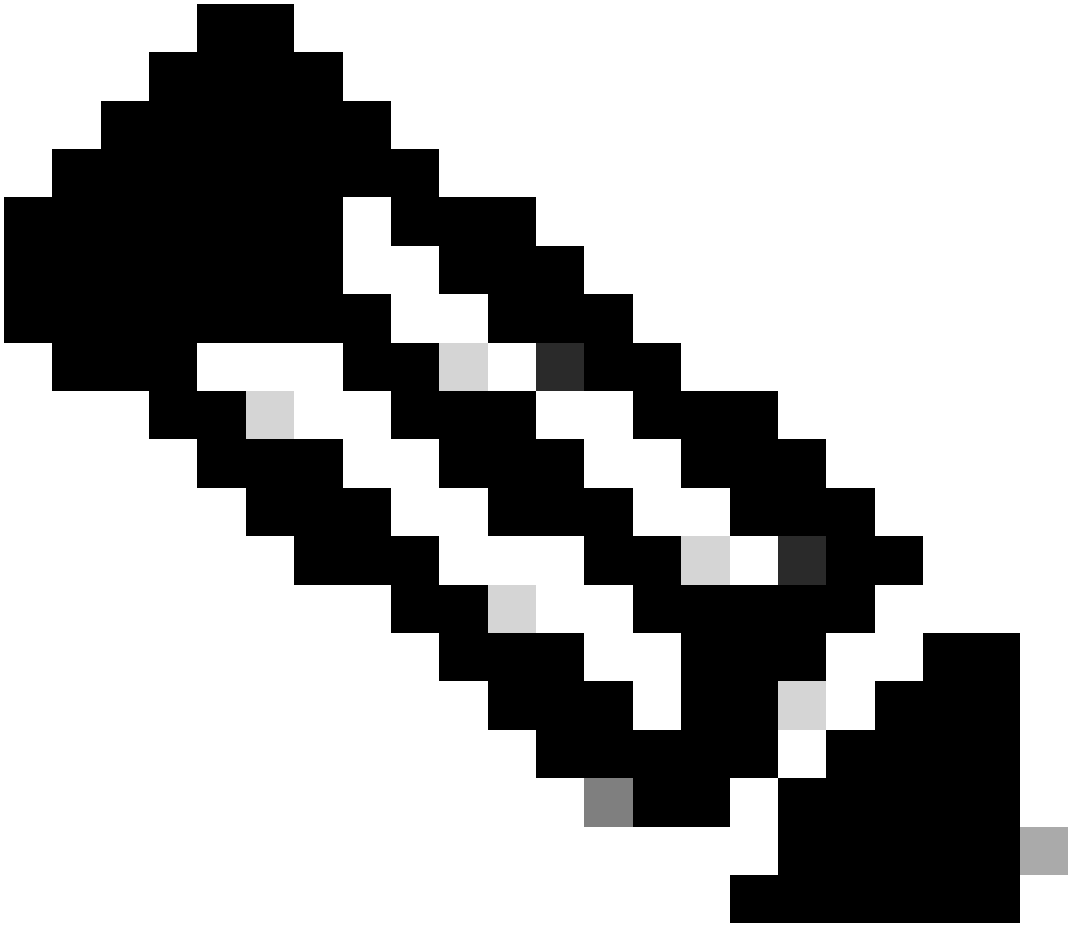
Um Identität, Richtlinien und Reporting für DNS-Abfragen hinzuzufügen, muss eine von drei Methoden berücksichtigt werden:

- (Empfohlen) - Stellen Sie das Umbrella AnyConnect Roaming-Modul bereit (aus Deployments > Roaming Computers). Externer DNS-Datenverkehr wird direkt an Umbrella mit angewandter "Roaming-Computer"-Identität gesendet. Dieses Modul unterstützt auch die optionale AD-Benutzeridentifizierung.
- Leiten Sie Datenverkehr von Ihrem DNS-Server vor Ort an Umbrella weiter, und identifizieren Sie den Datenverkehr mithilfe einer Netzwerk-Identität. Alle Benutzer erhalten die gleiche Richtlinie/Identität, und es gibt keine detaillierten Benutzerberichte.
- Verwenden Sie eine Umbrella Virtual Appliance in Ihrem lokalen Netzwerk, um Datenverkehr an Umbrella weiterzuleiten. DNS-Abfragen können anhand ihrer internen IP-Adresse (VPN-Pool-IP-Adresse) identifiziert werden. Die AD-Integration kann hinzugefügt werden. Dies erfordert die Installation zusätzlicher Komponenten vor Ort.

Dieses Beispiel zeigt, wie eine DNS-Richtlinie (Richtlinien > DNS-Richtlinien) für einen einzelnen AnyConnect-Client konfiguriert werden kann. Dies ist nur möglich, wenn das Umbrella AnyConnect Roaming Module bereitgestellt wird:



4410210455444



Anmerkung: Bei Verwendung des Umbrella-Moduls für AnyConnect kann DNS-Datenverkehr je nach Split-Tunneling-Konfiguration wahlweise innerhalb oder außerhalb des Tunnels gesendet werden.

Firewall-Richtlinien

Firewall-Richtlinien gelten für den Datenverkehr zwischen den Remote Access-Clients (AnyConnect) und dem Internet. Konfigurieren Sie die Regeln in "Deployments > Firewall Policy" wie in der folgenden Dokumentation beschrieben: Firewall verwalten.

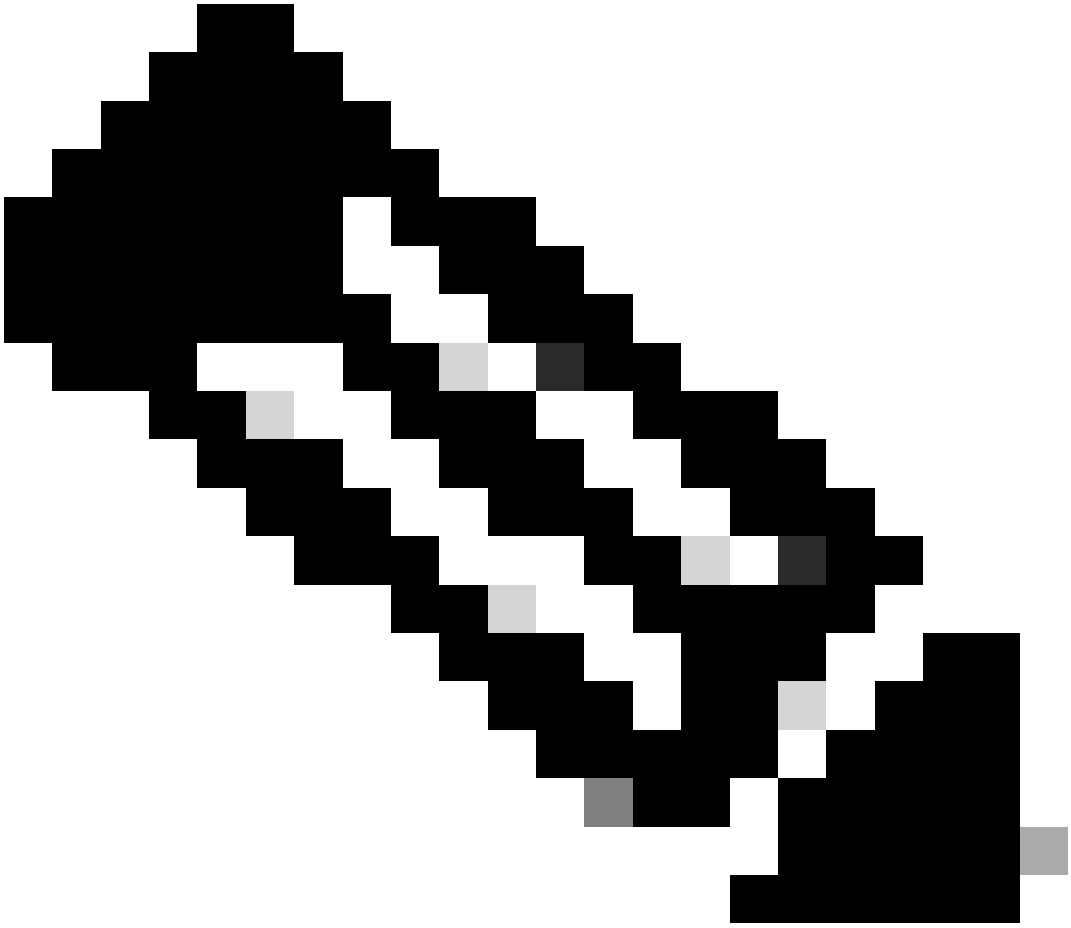
Die Standard-Firewall-Regel gilt für RAS-Clients. Wenn Sie eine bestimmte Richtlinie für Remote-Zugriffs-Benutzer erstellen, können Sie optional eine neue Firewall-Richtlinie erstellen und "Remote Access-Orgid:<ID>" als Quell-Tunnelidentität auswählen.
Die gleiche Firewall-Richtlinie gilt für alle Remote-Benutzer.

- Firewall-Richtlinien werden nicht verwendet, um den Zugriff zwischen RA-Clients und Privat-/Zweigstellennetzwerken zu steuern. Dies muss mithilfe von Firewalls vor Ort gesteuert

werden.

- Wie alle Umbrella-Firewall-Regeln steuern diese Regeln ausgehende Verbindungen für RAS-Clients. Eingehende Verbindungen sind niemals zulässig.
- Die Quell-IP-Adresse für RAS-Clients wird immer dynamisch aus dem VPN-Pool zugewiesen.
    - Das Erstellen von Regeln für einen bestimmten Computer mithilfe von "Quell-IP" wird nicht empfohlen, da die IP dynamisch neu zugewiesen wird
    - Das Erstellen von Regeln, die Benutzer eines bestimmten Remote Access-Rechenzentrums betreffen, ist über einen "Source CIDR"-Bereich möglich. Jedes Rechenzentrum stellt einen anderen VPN-Pool-Bereich bereit, der auf der Seite "Deployments > Remote Access" (Bereitstellungen > Remote-Zugriff) konfiguriert wird.

4409322341524



Anmerkung: Die Benutzeridentifizierung für Firewall-Richtlinien ist nicht verfügbar.

Webrichtlinien

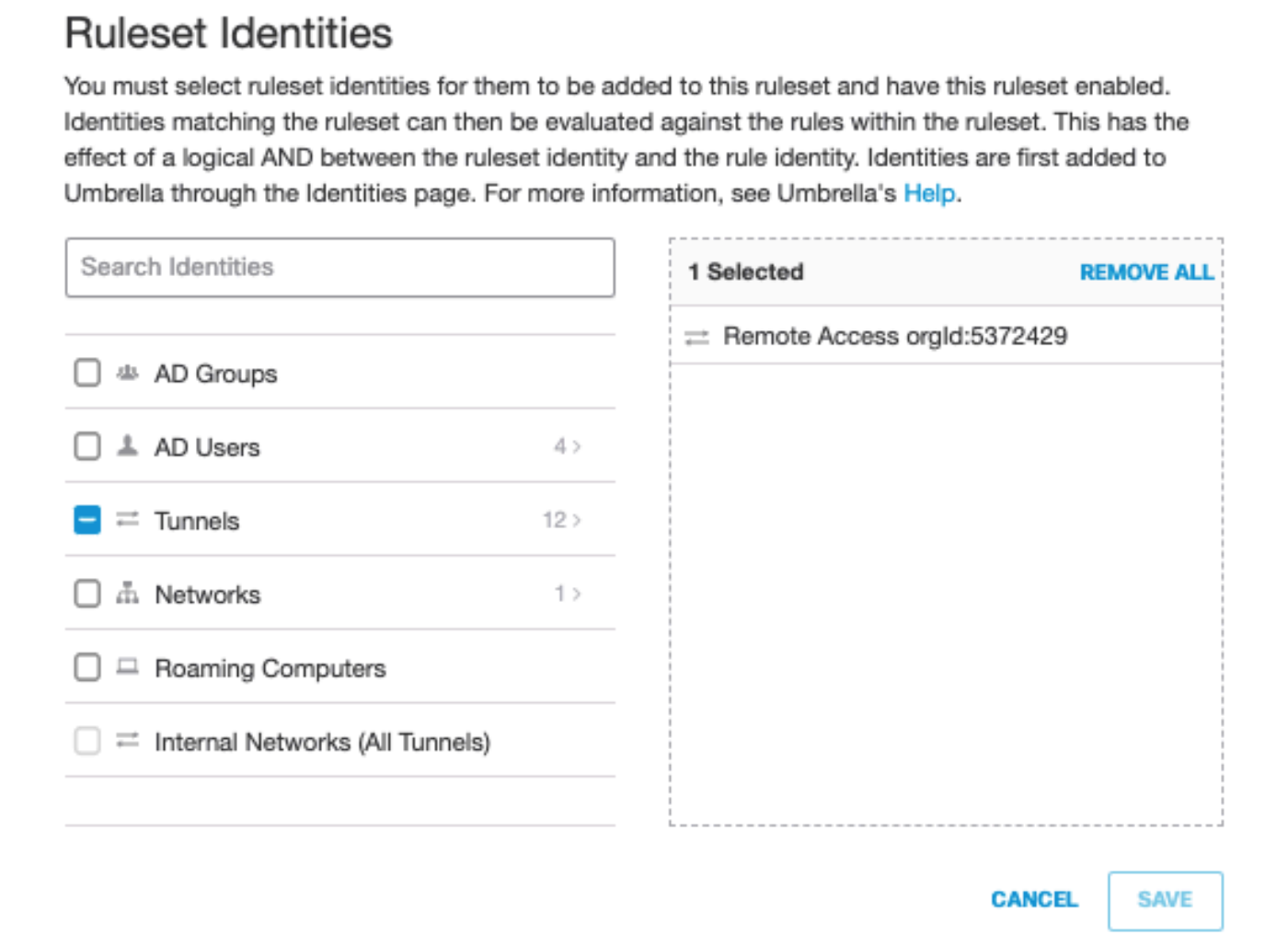
Webrichtlinien gelten für den Datenverkehr zwischen den Remote Access-Clients (AnyConnect) und dem Internet. Konfigurieren Sie die Regeln in "Deployments > Web Policies" wie in der folgenden Dokumentation beschrieben: Webrichtlinien verwalten.

- Webrichtlinien werden nicht verwendet, um den Zugriff zwischen RA-Clients und Private/Branch-Webservern zu steuern. Webrichtlinien gelten nur für externe Websites.

Die Standard-Webrichtlinie gilt für RAS-Clients. Es wird jedoch empfohlen, einen neuen Regelsatz zu erstellen, um die Sicherheitseinstellungen speziell für RAS-Clients zu definieren. Wählen Sie bei der Definition der Regelsatz-Identitäten in der Tunnelliste die Option RAS-Orgid:<ID>. Die gleiche Webrichtlinie gilt für alle RAS-Benutzer.

Nachdem Sie einen Regelsatz erstellt haben, können Sie eine Webregel hinzufügen, die die

Inhaltskategoriefilterung und Anwendungseinstellungen definiert.

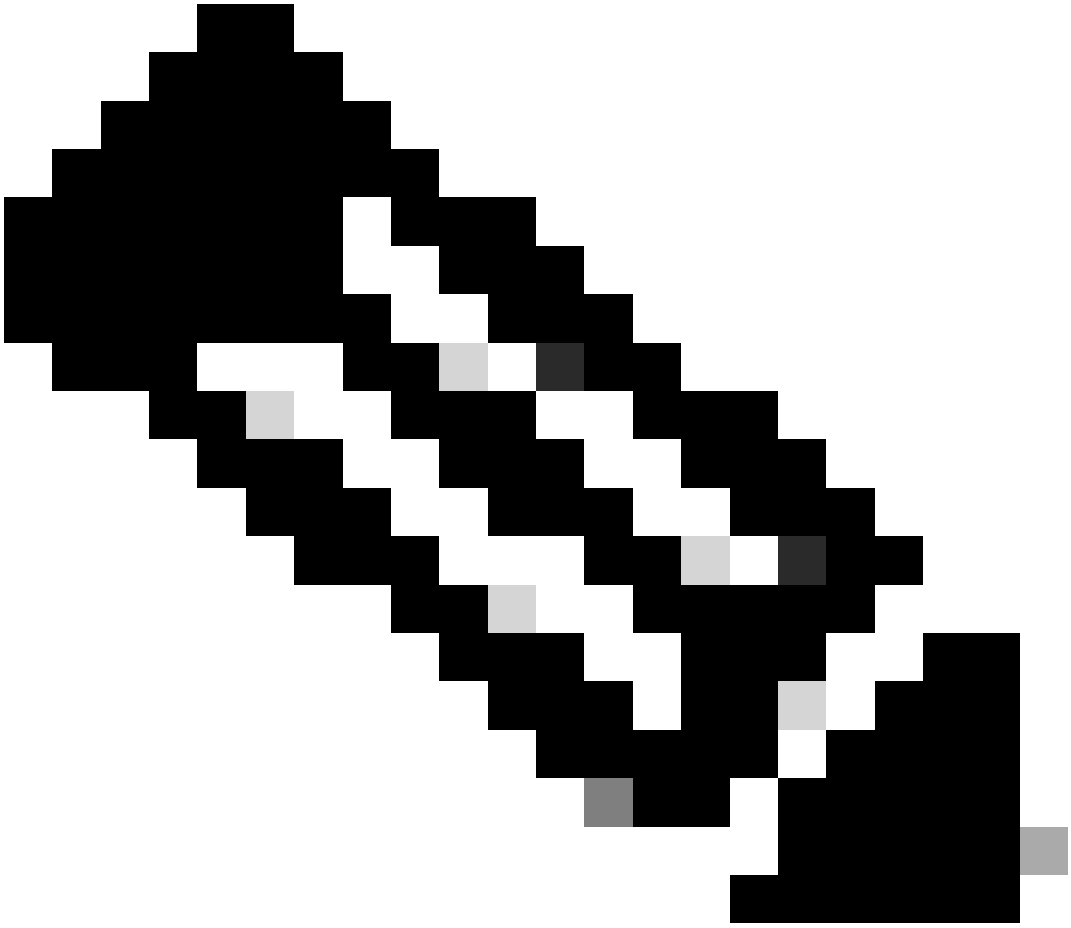


4409322363924

Web-Benutzeridentifizierung

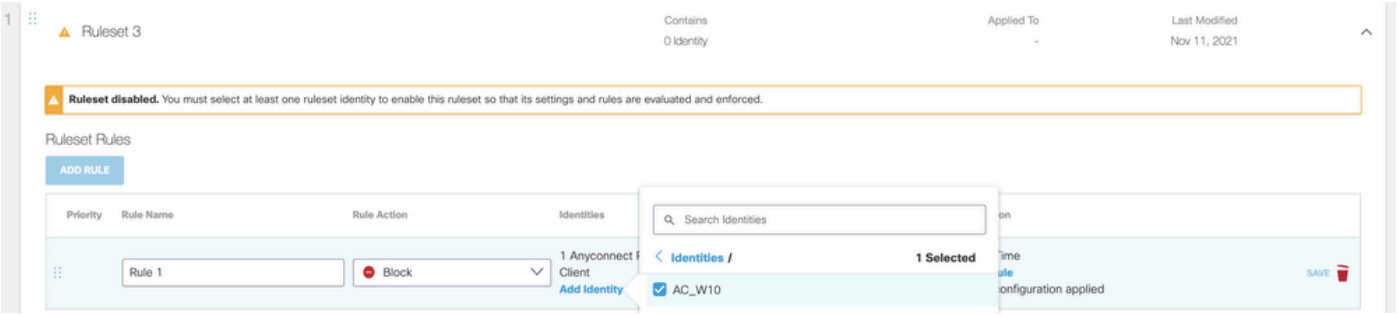
Standardmäßig kann der RAS-Datenverkehr nicht auf Benutzer- oder Gruppenbasis gesteuert werden. Dieselbe Richtlinie gilt für den gesamten RA-Datenverkehr, der auf der Identität der Remote-Zugriffs-ID basiert. Um Benutzer-/Gruppen-ID hinzuzufügen, haben Sie zwei Möglichkeiten:

- Installieren Sie unser AnyConnect Umbrella Roaming Security-Modul, und aktivieren Sie die SWG-Agent-Funktion. Der Agent sendet den Web-Datenverkehr direkt an die Umbrella SWG, wobei die Identität "Roaming-Computer" übernommen wird. Dieses Modul unterstützt auch die optionale AD-Benutzeridentifizierung.
- Aktivieren Sie SAML im Webregelsatz, der sich auf Ihre Identität "Remote Access Orgid" auswirkt. Nach dem Herstellen der Verbindung mit dem Remote-Zugriff werden RA-Benutzer bei der Generierung von Webbrowser-Datenverkehr ein zweites Mal aufgefordert, sich über SAML zu authentifizieren.



Anmerkung: Bei Verwendung des Umbrella-Moduls für AnyConnect kann SWG-Datenverkehr je nach Split-Tunneling-Konfiguration wahlweise innerhalb oder außerhalb des Tunnels gesendet werden.

Dieses Beispiel zeigt, wie eine DNS-Richtlinie (Richtlinien > DNS-Richtlinien) für einen einzelnen AnyConnect-Client konfiguriert werden kann. Dies ist nur möglich, wenn das Umbrella AnyConnect Roaming Module bereitgestellt wird:

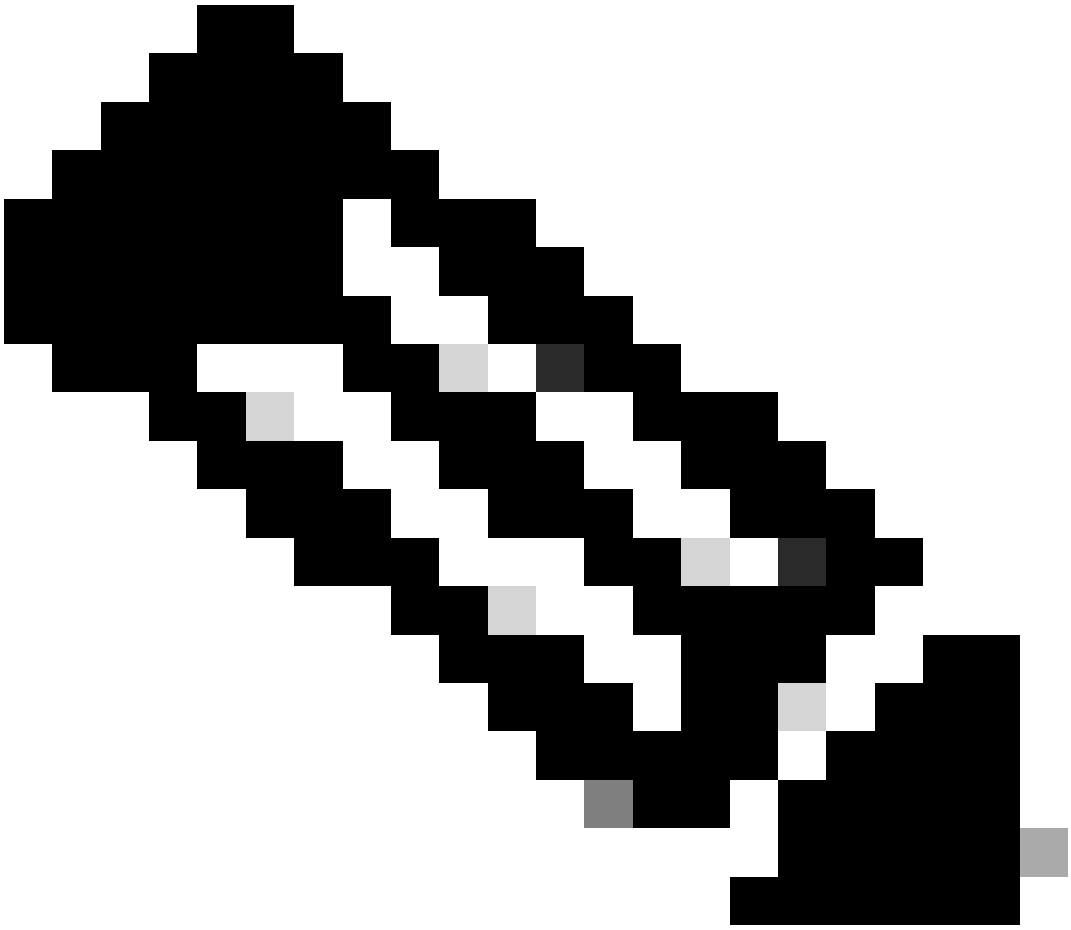


4410210499476

SvD-Richtlinien

Richtlinien für Datenverluste gelten für den Datenverkehr zwischen den Remote Access-Clients (AnyConnect) und dem Internet. Konfigurieren Sie die Regeln in "Deployments > Data Loss Prevention Policies" (Bereitstellungen > Richtlinien zum Schutz vor Datenverlust) wie in der folgenden Dokumentation beschrieben: Datenschutzrichtlinien verwalten.

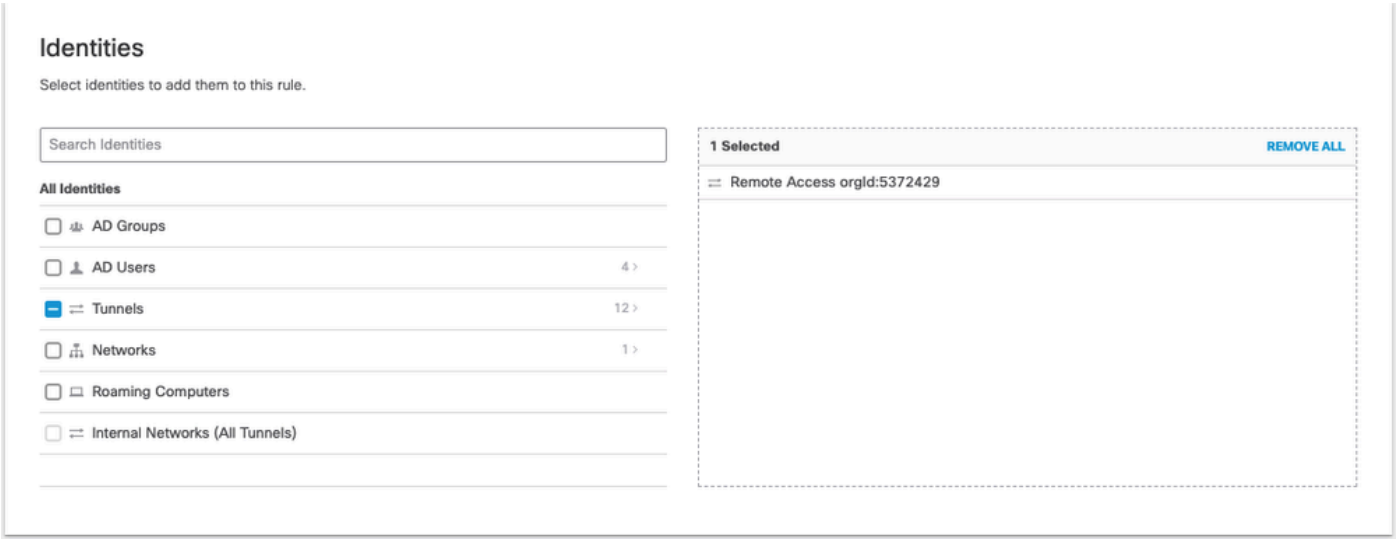
- SvD-Policys werden nicht verwendet, um den Zugriff zwischen RA-Clients und Webservern für Privat-/Zweigstellen zu steuern. SvD-Richtlinien gelten nur für den Datenverkehr externer Websites.



Anmerkung: Damit SvD-Policys angewendet werden, müssen Sie zuerst einen Webregelsatz für RAS-Benutzer erstellt haben. Für den Webregelsatz muss die HTTPS-Entschlüsselung aktiviert sein.

Wenn Sie Identitäten für eine Datenschutzregel auswählen, wählen Sie Remotezugriffsorgid:<ID>. Die gleiche Datenschutzrichtlinie gilt für alle Benutzer. Zum Abschließen der SvD-Regel müssen

Sie außerdem SvD-Klassifizierungen auswählen oder definieren.



4409322428820

SvD-Benutzererkennung

DLP ruft die Benutzeridentität vom sicheren Web-Gateway ab (Webrichtlinien). Anweisungen zum Hinzufügen der Benutzeridentifizierung finden Sie im Abschnitt zu Webrichtlinien.

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.