Configure SIG Policies for Remote Access for Secure Connect Users

Contents

Introduction

This document describes how to create SIG policies for Remote Access for Secure Connect users.

Overview

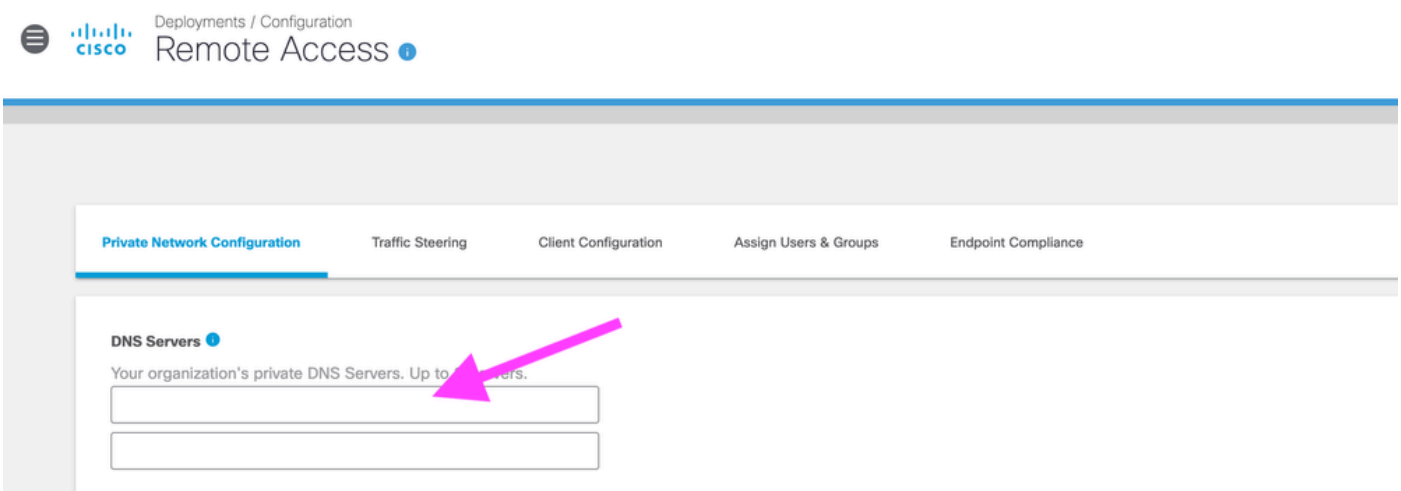
This Knowledgebase article applies to customers using Secure Connect package which includes Remote Access (VPNaaS) functionality in Umbrella.

Administrators can configure Umbrella Firewall, Web, and Data Loss policies to apply to roaming users connected to Remote Access via AnyConnect.

DNS Policies

It is possible to send DNS queries to Umbrella resolvers (eg. 208.67.222.222) via the AnyConnect Remote Access VPN connection. However, this does not enable identification, policy, or reporting of DNS traffic on the Umbrella dashboard.

- This provides DNS resolution only and therefore is not typically recommended.
- Using external DNS resolvers in your VPN DNS configuration prevents resolution of internal DNS Zones.



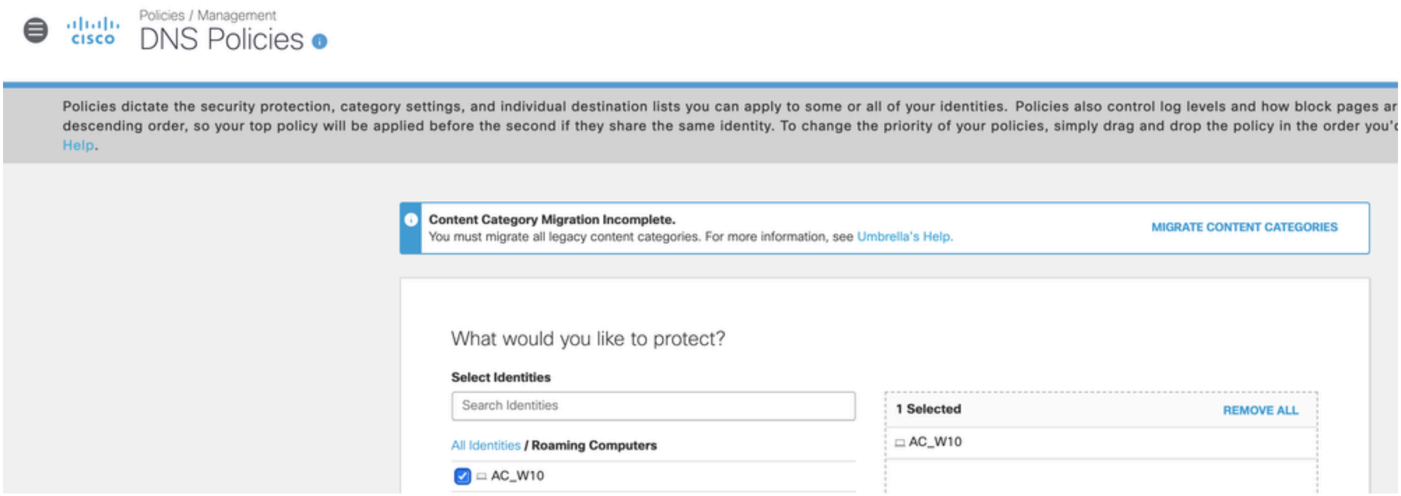
Your organization's private DNS Servers. Up to ers.

4410210378004

To add identity, policy, and reorting for DNS queries, one of three methods must be considered:

- **(Recommended)** - Deploy the Umbrella AnyConnect Roaming module (from Deployments > Roaming Computers). External DNS traffic is sent directly to Umbrella with "Roaming Computer" identity applied. This module also supports optional AD user identification.
- Forward traffic from your on-premise DNS server to Umbrella and identify traffic using a Network identity. All users receive the same policy/identity and there is no granular user reporting.
- Use an Umbrella Virtual Appliance on your on-premise network to forward traffic to Umbrella. DNS queries can be identified by their internal (VPN pool IP address). AD integration can be added - requires installation of additional on-premise components.

This example shows how a DNS Policy can be configured (*Policies > DNS Policies*) for an individual AnyConnect client - this is only possible when the Umbrella AnyConnect Roaming Module is deployed:



Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages ar descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'c Help.

Content Category Migration Incomplete.
You must migrate all legacy content categories. For more information, see Umbrella's Help.

4410210455444

Note: When using the Umbrella module for AnyConnect, DNS traffic can optionally be sent inside or outside the tunnel depending on your split tunneling configuration.

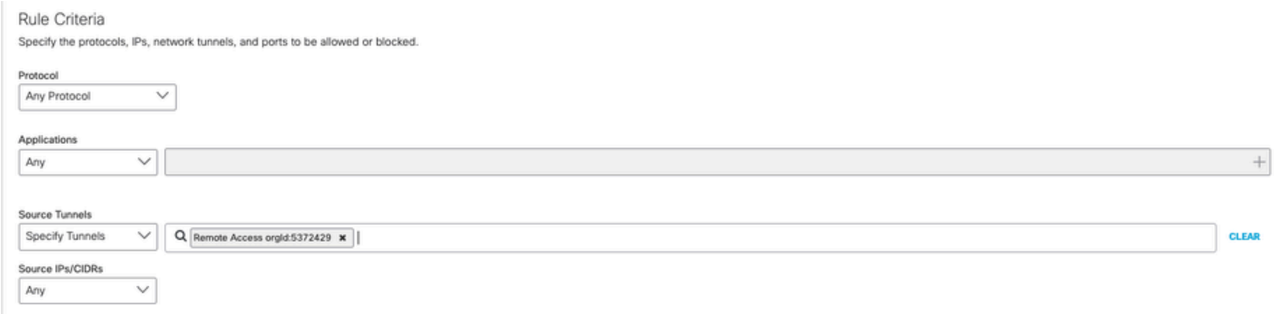
Firewall Policies

Firewall policies apply to traffic between the Remote Access (AnyConnect) clients and the internet. Configure rules in '*Deployments > Firewall Policy*' as per documentation found here: Manage Firewall.

The default firewall rule applies to Remote Access clients. If you are creating a specific policy for Remote Access users, you can optionally choose to create a new firewall policy and select "**Remote Access orgid:<ID>"** as the source tunnel identity.
The same Firewall Policy applies to all remote access users.

- Firewall policies are not used to control access between RA clients and Private/Branch networks. This must be controlled with on-premise firewalls.
- Like all Umbrella firewall rules, these rules control *outbound* connections for Remote Access clients. Inbound connections are never allowed.
- The source IP address for Remote Access clients is always dynamically assigned from the VPN pool.
    - Creating rules for a specific computer using "Source IP" is not recommended as the IP is

    dynamically re-assigned
  - Creating rules affecting users of a specific Remote Access data center is possible by using a "Source CIDR" range. Each data center provides a different VPN pool range which is configured on the '*Deployments > Remote Access*' page.



Rule Criteria

Specify the protocols, IPs, network tunnels, and ports to be allowed or blocked.

Protocol: Any Protocol

Applications: Any

Source Tunnels: Specify Tunnels — Remote Access orgId:5372429 ×

Source IPs/CIDRs: Any

4409322341524

Note: Per User identification is not available for firewall policies.

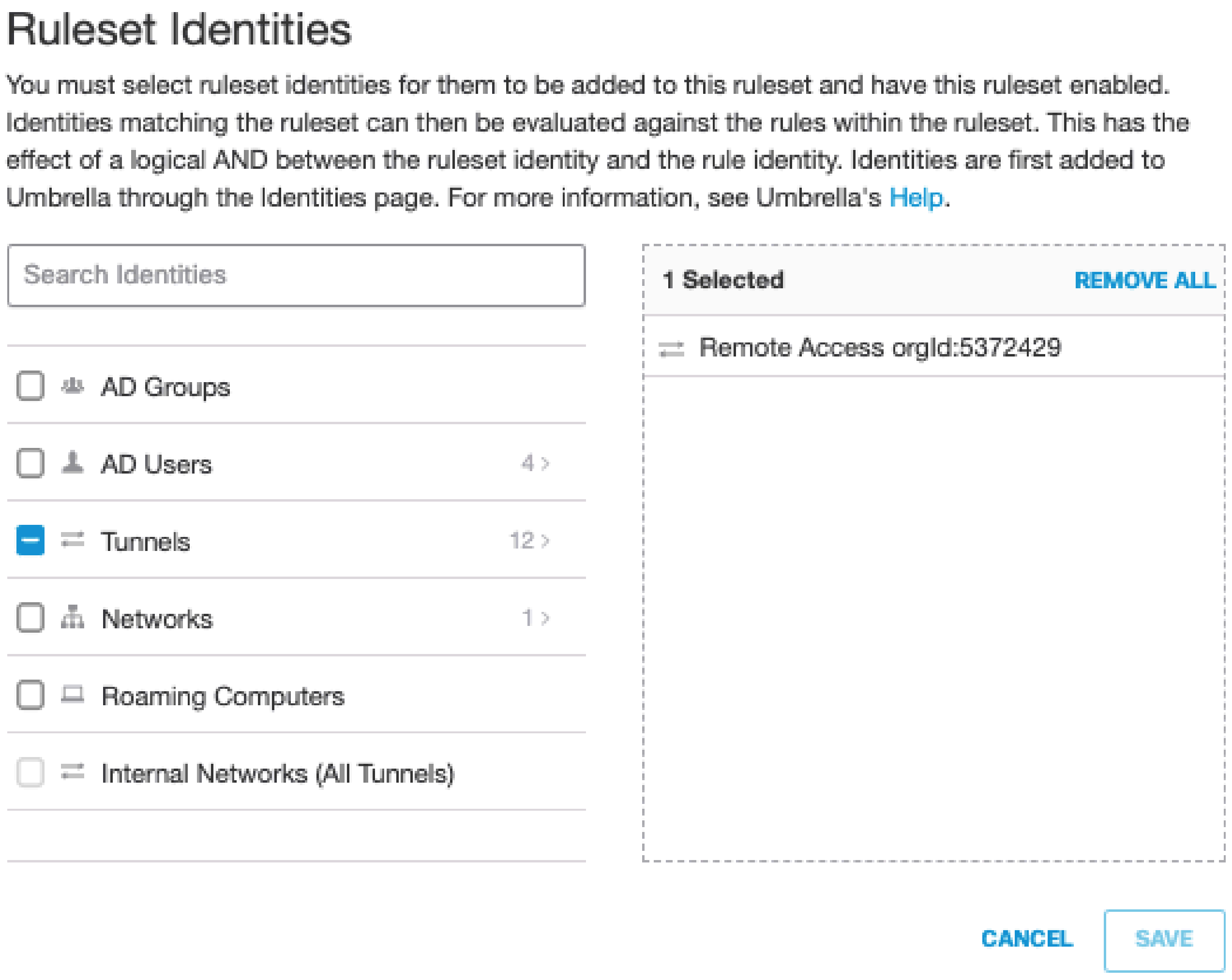
Web Policies

Web policies apply to traffic between the Remote Access (AnyConnect) clients and the internet. Configure rules in '*Deployments > Web Policies*' as per documentation found here: Manage Web Policies.

- Web policies are not used to control access between RA clients and Private/Branch webservers. Web policies only apply to external websites.

The default web policy applies to Remote Access clients. However, we recommend creating a new ruleset to define security settings specifically for Remote Access clients. When defining the Ruleset identities choose **Remote Access orgid:<ID>** from the list of tunnels. The same Web Policy applies to all remote access users.

After creating a ruleset it is possible to add a web rule to which defines Content Category Filtering and application settings.



Ruleset Identities

You must select ruleset identities for them to be added to this ruleset and have this ruleset enabled. Identities matching the ruleset can then be evaluated against the rules within the ruleset. This has the effect of a logical AND between the ruleset identity and the rule identity. Identities are first added to Umbrella through the Identities page. For more information, see Umbrella's Help.

Search Identities

□ AD Groups

□ AD Users 4 >

⊟ Tunnels 12 >

□ Networks 1 >

□ Roaming Computers

□ Internal Networks (All Tunnels)

1 Selected REMOVE ALL

Remote Access orgId:5372429

CANCEL SAVE

4409322363924

Web User Identification

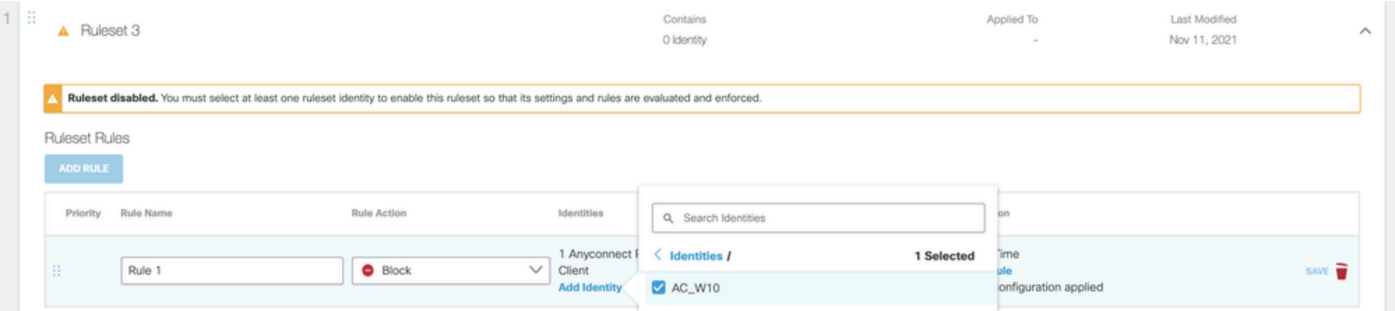
By default, Remote Access traffic cannot be controlled on a per-user or group basis. The same policy applies to all RA traffic based on the "Remote Access orgid" identity. To add user/group identification you have two options:

- Install our AnyConnect Umbrella Roaming Security module and enable the SWG agent feature. The agent sends web traffic directly to Umbrella SWG with "Roaming Computer" identity applied. This module also supports optional AD user identification.

- Enable SAML in the web ruleset that affects your "Remote Access orgid" identity. After connecting to remote access, RA users are prompted to authenticate via SAML a second time when generating web browser traffic.

Note: When using the Umbrella module for AnyConnect, SWG traffic can optionally be sent inside or outside the tunnel depending on your split tunneling configuration.

This example shows how a DNS Policy can be configured (Policies > DNS Policies) for an individual AnyConnect client - this is only possible when the Umbrella AnyConnect Roaming Module is deployed:



Contains	Applied To	Last Modified
0 Identity	-	Nov 11, 2021

Ruleset disabled. You must select at least one ruleset identity to enable this ruleset so that its settings and rules are evaluated and enforced.

Ruleset Rules

Priority	Rule Name	Rule Action	Identities	on
	Rule 1	Block	1 Anyconnect F Client Add Identity	'ime ule onfiguration applied

Search Identities

Identities / 1 Selected

☑ AC_W10

4410210499476

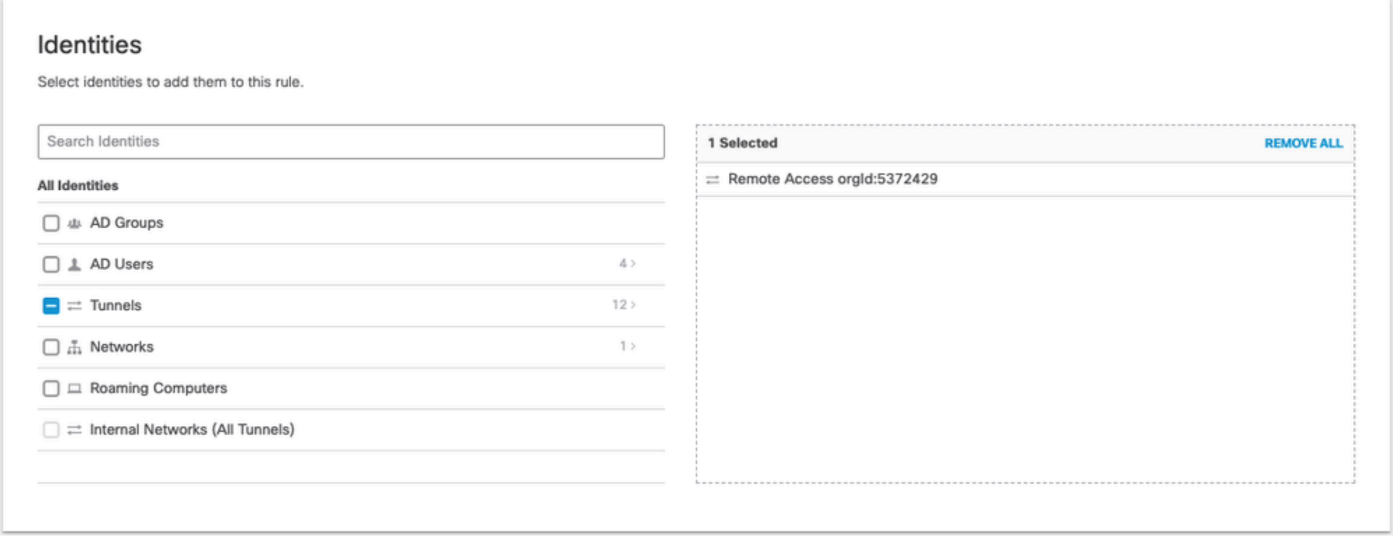
DLP Policies

Data Loss policies apply to traffic between the Remote Access (AnyConnect) clients and the internet. Configure rules in 'Deployments > Data Loss Prevention Policies' as per documentation found here: Manage Data Protection Policies.

- DLP policies are not used to control access between RA clients and Private/Branch webservers. DLP policies only apply to traffic external websites.

Note: In order for DLP policies to apply you first must have created a Web Ruleset for Remote Access users. The web ruleset must have HTTPS Decryption Enabled.

When selecting identities for a Data protection rule, choose **Remote Access orgid:<ID>.** The same data protection policy applies to all users. To complete the DLP rule you also need to select or define DLP Classifiers.



Identities

Select identities to add them to this rule.

Search Identities

All Identities

- ☐ AD Groups
- ☐ AD Users 4 >
- ⊟ Tunnels 12 >
- ☐ Networks 1 >
- ☐ Roaming Computers
- ☐ Internal Networks (All Tunnels)

1 Selected REMOVE ALL

Remote Access orgId:5372429

4409322428820

DLP User Identification

DLP gets user identity from the secure web gateway (Web policies). Refer to the Web policies section for instructions on how to add user identification.