

Secure Connect 사용자를 위한 원격 액세스를 위한 SIG 정책 구성

목차

[소개](#)

[개요](#)

[DNS 정책](#)

[방화벽 정책](#)

[웹 정책](#)

[웹 사용자 ID](#)

[DLP 정책](#)

[DLP 사용자 식별](#)

소개

이 문서에서는 Secure Connect 사용자를 위한 원격 액세스에 대한 SIG 정책을 생성하는 방법에 대해 설명합니다.

개요

이 Knowledgebase 문서는 Umbrella의 VPNaaS(Remote Access) 기능이 포함된 Secure Connect 패키지를 사용하는 고객에게 적용됩니다.

관리자는 AnyConnect를 통해 원격 액세스에 연결된 로밍 사용자에게 적용할 Umbrella 방화벽, 웹 및 데이터 손실 정책을 구성할 수 있습니다.

DNS 정책

DNS 쿼리를 Umbrella 확인자(예: 208.67.222.222). 그러나 Umbrella 대시보드에서 DNS 트래픽의 식별, 정책 또는 보고는 활성화되지 않습니다.

- 이는 DNS 확인만 제공하므로 일반적으로 권장되지 않습니다.
- VPN DNS 컨피그레이션에서 외부 DNS 리졸버를 사용하면 내부 DNS 영역을 확인할 수 없습니다.

Private Network Configuration

Traffic Steering

Client Configuration

Assign Users & Groups

Endpoint Compliance

DNS Servers

Your organization's private DNS Servers. Up to 10 servers.

4410210378004

DNS 쿼리에 ID, 정책 및 보고를 추가하려면 다음 세 가지 방법 중 하나를 고려해야 합니다.

- (권장) - Umbrella AnyConnect [로밍 모듈을 구축합니다](#)(Deployments(구축) > Roaming Computers(로밍 컴퓨터)에서). 외부 DNS 트래픽은 "로밍 컴퓨터" ID가 적용된 Umbrella로 직접 전송됩니다. 이 모듈은 선택적인 [AD 사용자 식별도 지원합니다](#).
- 온프레미스 DNS 서버에서 Umbrella로 트래픽을 전달하고 [네트워크](#) ID를 사용하여 트래픽을 식별합니다. 모든 사용자는 동일한 정책/ID를 받으며 세분화된 사용자 보고가 없습니다.
- 온프레미스 네트워크에서 [Umbrella Virtual](#) Appliance를 사용하여 트래픽을 Umbrella로 전달합니다. DNS 쿼리는 내부(VPN 풀 IP 주소)로 식별할 수 있습니다. [AD 통합](#)을 추가할 수 있습니다. 추가 온-프레미스 구성 요소를 설치해야 합니다.

이 예에서는 개별 AnyConnect 클라이언트에 대해 DNS 정책을 구성하는 방법(Policies(정책) > DNS Policies(DNS 정책))을 보여줍니다. 이 방법은 Umbrella AnyConnect 로밍 모듈이 구축된 경우에만 가능합니다.

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 are displayed in 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 want. [Help](#).

Content Category Migration Incomplete.

You must migrate all legacy content categories. For more information, see [Umbrella's Help](#).

[MIGRATE CONTENT CATEGORIES](#)

What would you like to protect?

Select Identities

Search Identities

All Identities / Roaming Computers

☒ AC_W10

1 Selected

[REMOVE ALL](#)

☐ AC_W10

4410210455444



참고: AnyConnect용 Umbrella 모듈을 사용할 경우 스플릿 터널링 컨피그레이션에 따라 DNS 트래픽을 터널 내부 또는 외부로 전송할 수 있습니다.

방화벽 정책

방화벽 정책은 원격 액세스(AnyConnect) 클라이언트와 인터넷 간의 트래픽에 적용됩니다. 다음 설명서에 따라 'Deployments(구축) > Firewall Policy(방화벽 정책)'에서 규칙을 구성합니다. [방화벽 관리](#).

기본 방화벽 규칙은 원격 액세스 클라이언트에 적용됩니다. 원격 액세스 사용자에게 특정 정책을 생성하는 경우 선택적으로 새 방화벽 정책을 생성하고 소스 터널 ID로 "Remote Access orgid:<ID>"를 선택할 수 있습니다.

동일한 방화벽 정책이 모든 원격 액세스 사용자에게 적용됩니다.

- RA 클라이언트와 프라이빗/브랜치 네트워크 간의 액세스를 제어하는 데 방화벽 정책을 사용하지 않습니다. 이는 온프레미스 방화벽으로 제어해야 합니다.
- 모든 Umbrella 방화벽 규칙과 마찬가지로, 이러한 규칙은 원격 액세스 클라이언트에 대한 아

아웃바운드 연결을 제어합니다. 인바운드 연결은 허용되지 않습니다.

- 원격 액세스 클라이언트의 소스 IP 주소는 항상 VPN 풀에서 동적으로 할당됩니다.
 - IP가 동적으로 다시 할당되므로 "소스 IP"를 사용하여 특정 컴퓨터에 대한 규칙을 만들지 않는 것이 좋습니다
 - "소스 CIDR" 범위를 사용하면 특정 원격 액세스 데이터 센터의 사용자에게 영향을 주는 규칙을 만들 수 있습니다. 각 데이터 센터는 'Deployments(구축) > Remote Access(원격 액세스)' 페이지에 구성된 다른 VPN 풀 범위를 제공합니다.

Rule Criteria

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

Protocol

Any Protocol

Applications

Any

Source Tunnels

Specify Tunnels

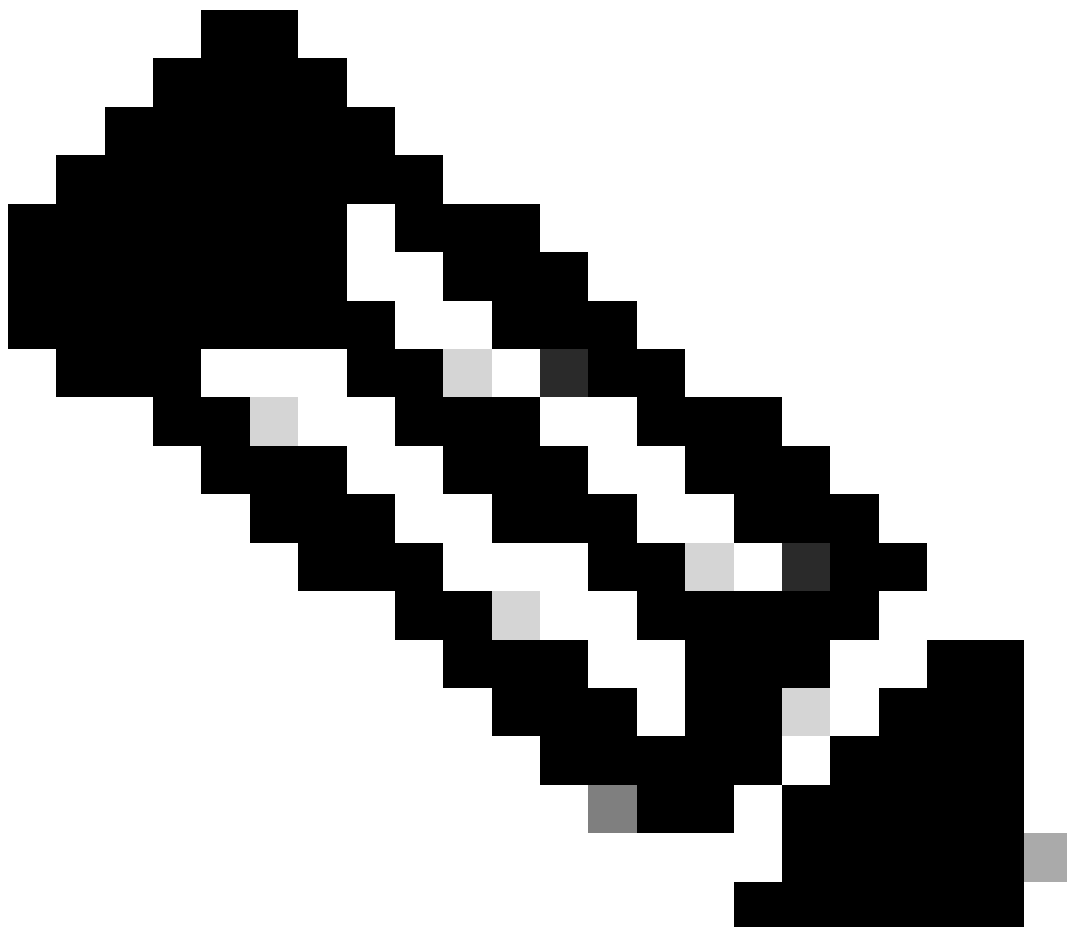
Remote Access orgId:5372429

CLEAR

Source IPs/CIDRs

Any

4409322341524



참고: 사용자별 ID는 방화벽 정책에 사용할 수 없습니다.

웹 정책

웹 정책은 원격 액세스(AnyConnect) 클라이언트와 인터넷 간의 트래픽에 적용됩니다. 다음 문서에 따라 'Deployments(구축) > Web Policies(웹 정책)'에서 규칙을 구성합니다. [웹 정책을 관리합니다.](#)

- 웹 정책은 RA 클라이언트와 사설/지사 웹 서버 간의 액세스를 제어하는 데 사용되지 않습니다.
• 웹 정책은 외부 웹 사이트에만 적용됩니다.

기본 웹 정책은 원격 액세스 클라이언트에 적용됩니다. 그러나 원격 액세스 클라이언트 [에](#) 대한 보안 [설정을](#) 정의하기 위해 [새 규칙](#) 세트를 만드는 것이 좋습니다. 규칙 세트 ID를 정의할 때 터널 목록에서 원격 액세스 orgid:<ID>를 선택합니다. 모든 원격 액세스 사용자에게 동일한 웹 정책이 적용됩니다.

규칙 세트를 만든 후 콘텐츠 카테고리 필터링 및 응용 프로그램 [설정을](#) 정의하는 [웹](#) 규칙을 [추가할](#) 수 있습니다.

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

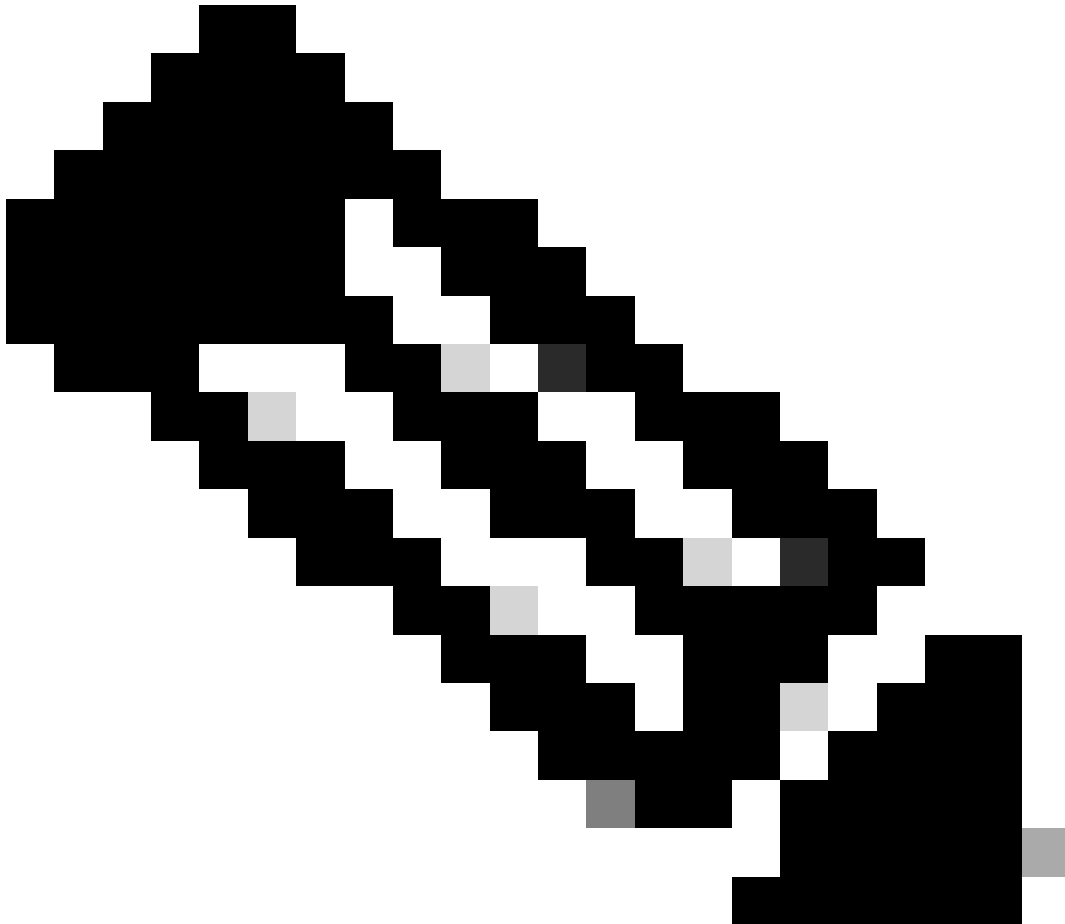
CANCEL

SAVE

웹 사용자 ID

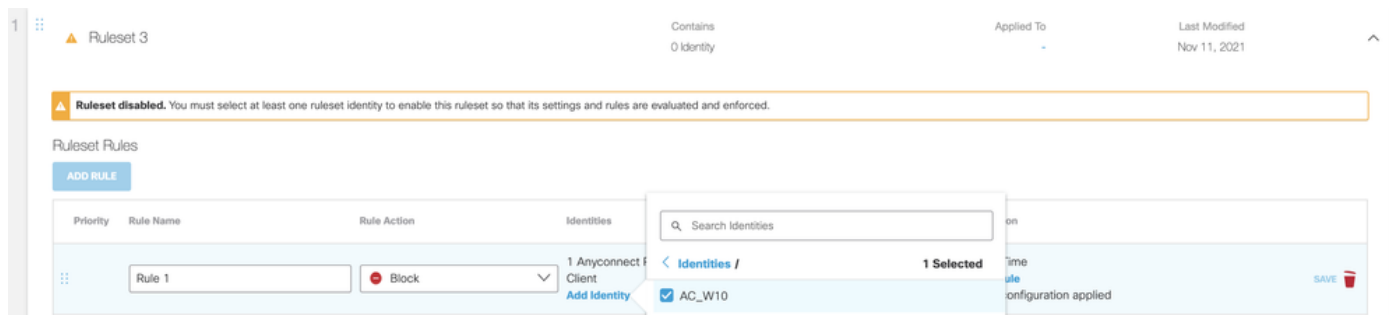
기본적으로 원격 액세스 트래픽은 사용자 또는 그룹 단위로 제어할 수 없습니다. 동일한 정책이 "원격 액세스 orgid" ID를 기반으로 모든 RA 트래픽에 적용됩니다. 사용자/그룹 ID를 추가하려면 두 가지 옵션이 있습니다.

- AnyConnect Umbrella [Roaming Security 모듈](#)을 설치하고 SWG [에이전트](#) 기능을 [활성화합니다](#). 에이전트는 "로밍 컴퓨터" ID가 적용된 웹 트래픽을 Umbrella SWG로 직접 전송합니다. 이 모듈은 선택적인 [AD 사용자 식별도 지원합니다](#).
- "[원격](#) 액세스 orgid" ID에 영향을 주는 웹 규칙 세트에서 SAML을 활성화합니다. 원격 액세스에 연결한 후 RA 사용자는 웹 브라우저 트래픽을 생성할 때 SAML을 통해 두 번째로 인증하라는 프롬프트를 받습니다.



참고: AnyConnect용 Umbrella 모듈을 사용할 경우 스플릿 터널링 컨피그레이션에 따라 SWG 트래픽을 터널 내부 또는 외부로 선택적으로 전송할 수 있습니다.

이 예에서는 개별 AnyConnect 클라이언트에 대해 DNS 정책을 구성하는 방법(Policies(정책) > DNS Policies(DNS 정책))을 보여줍니다. 이는 Umbrella AnyConnect 로밍 모듈이 구축된 경우에만 가능합니다.

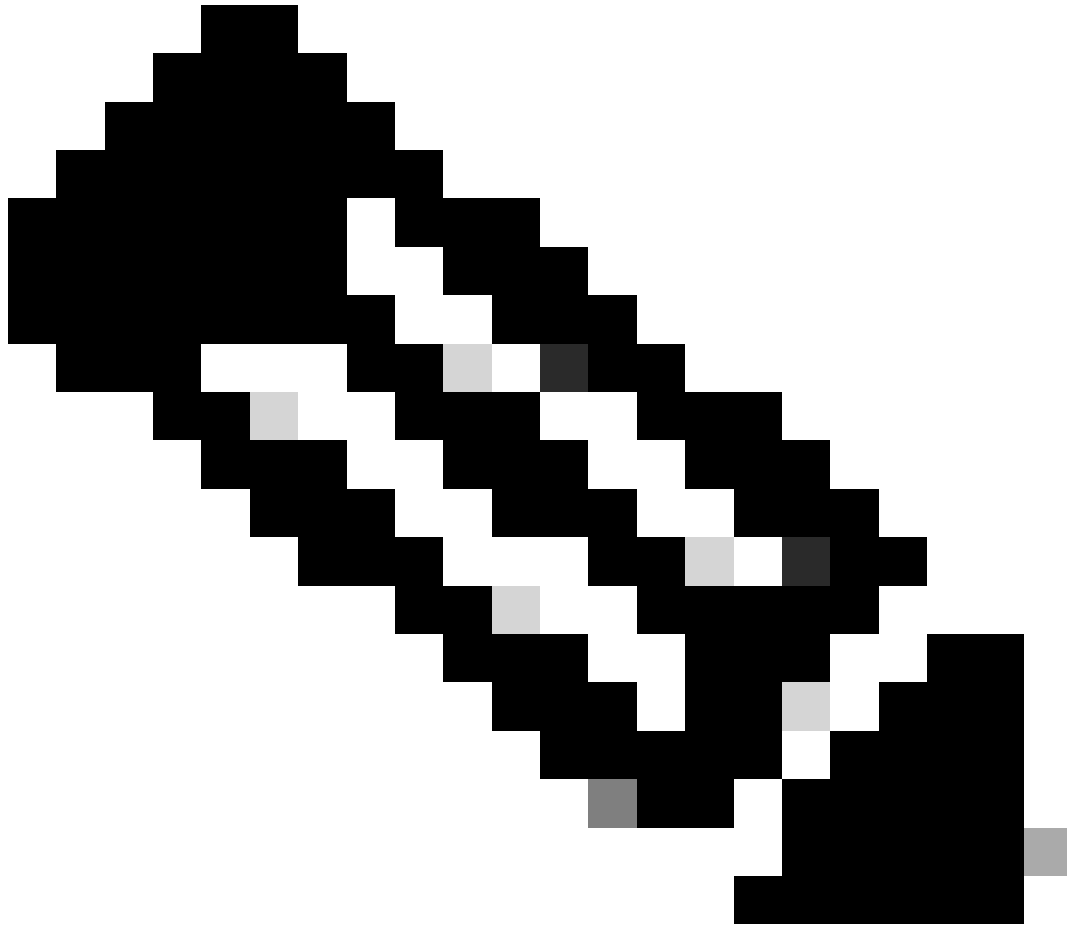


4410210499476

DLP 정책

데이터 손실 정책은 원격 액세스(AnyConnect) 클라이언트와 인터넷 간의 트래픽에 적용됩니다. 다음 문서에 따라 'Deployments(구축) > Data Loss Prevention Policies(데이터 유출 방지 정책)'에서 규칙을 구성합니다. [데이터 보호 정책을 관리합니다.](#)

- DLP 정책은 RA 클라이언트와 사설/지사 웹 서버 간의 액세스를 제어하는 데 사용되지 않습니다. DLP 정책은 트래픽 외부 웹 사이트에만 적용됩니다.



참고: DLP 정책을 먼저 적용하려면 원격 액세스 사용자를 위한 웹 규칙 세트를 생성해야 합니다. 웹 규칙 집합에 HTTPS 암호 해독이 활성화되어 있어야 합니다.

데이터 보호 규칙에 대한 ID를 선택할 때 원격 액세스 orgid:<ID>를 선택합니다. 모든 사용자에게 동일한 데이터 보호 정책이 적용됩니다. DLP 규칙을 완료하려면 DLP 분류자를 선택하거나 정의해야 [합니다](#).

Identities

Select identities to add them to this rule.

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 사용자 식별

DLP는 보안 웹 게이트웨이(웹 정책)에서 사용자 ID를 가져옵니다. 사용자 ID를 추가하는 방법에 대한 지침은 웹 정책 섹션을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.