

신뢰할 수 있는 네트워크 탐지를 통해 제로 트러스트 네트워크 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계: 트러스트된 네트워크 프로파일 생성 - DNS 서버 및 도메인](#)

[2단계: 개인 또는 인터넷 액세스를 위한 TND 활성화](#)

[3단계: 클라이언트측 컨피그레이션](#)

[다음을 확인합니다.](#)

[보안 클라이언트에서](#)

[DART 번들 -ZTA 로그에서](#)

[관련 정보](#)

소개

이 문서에서는 ZTNA Trusted Network Detection을 구성하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

- Secure Client 최소 버전 5.1.10
- 지원되는 플랫폼 - Windows 및 MacOS
- Windows용 TPM(Trusted Platform Module)
- Apple 디바이스용 Secure Enclave 코프로세서
- 신뢰할 수 있는 네트워크 프로파일에 구성된 '신뢰할 수 있는 서버'는 ZTA 가로채기에서 암시적으로 제외됩니다. 이러한 서버는 ZTA 프라이빗 리소스로 액세스할 수도 없습니다.
- TND 컨피그레이션은 조직에 등록된 모든 클라이언트에 영향을 미칩
- 관리자는 다음 단계를 사용하여 신뢰할 수 있는 서버에 대한 '인증서 공개 키 해시'를 생성할 수 있습니다
 - 신뢰할 수 있는 서버 퍼블릭 인증서 다운로드
 - 이 셸 명령을 실행하여 다음을 generate the hash 수행합니다.

```
openssl x509 -in
```

```
-pubkey -noout | openssl pkey -pubin -outform DER | openssl dgst -sha256
```

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 액세스
- SAML 또는 인증서 기반 인증을 사용하여 제로 트러스트 액세스에 디바이스를 등록합니다.

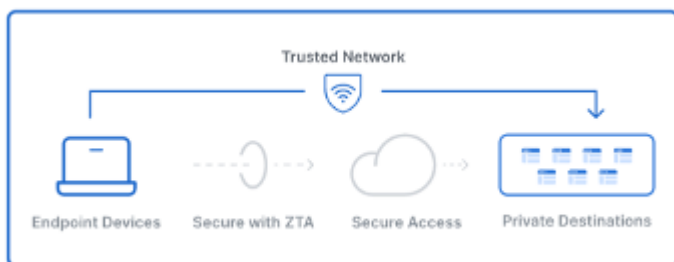
사용되는 구성 요소

- Secure Client 버전 5.1.13
- TPM
- 보안 액세스 테넌트
- Windows 장치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

- TND를 통해 관리자는 보안 클라이언트를 구성하여 신뢰할 수 있는 네트워크에서 ZTA 트래픽 조정 및 시행을 일시적으로 일시 중지할 수 있습니다.
- 보안 클라이언트는 엔드포인트가 신뢰할 수 있는 네트워크에서 나갈 때 ZTA 시행을 다시 시작합니다.
- 이 기능에는 최종 사용자 상호 작용이 필요하지 않습니다.
- ZTA TND 구성은 프라이빗 및 인터넷 ZTA 대상에 대해 독립적으로 관리할 수 있습니다.



주요 이점

- 향상된 네트워크 성능과 짧은 레이턴시로 더 원활한 사용자 환경을 제공합니다.
- 신뢰할 수 있는 네트워크의 로컬 보안 시행은 유연하고 최적화된 리소스 활용을 제공합니다.
- 최종 사용자는 어떠한 프롬프트나 조치 없이도 이점을 활용할 수 있습니다.
- 프라이빗 액세스 및 인터넷 액세스를 위한 TND의 독립적인 제어를 통해 관리자는 다양한 운영 및 보안 문제를 유연하게 처리할 수 있습니다.

구성

1단계: 트러스트된 네트워크 프로파일 생성 - DNS 서버 및 도메인

Secure [Access Dashboard\(보안 액세스 대시보드\)](#)로 이동합니다.

- 클릭Connect>End User Connectivity>Manage Trusted Networks> +Add

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust Access Virtual Private Network Internet Security

Enrollment methods [Manage](#)

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: [SSO Authentication](#) [Certificates](#)

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles [Manage Trusted Networks](#) [+ ZTA Profile](#)

Manage Zero Trust Access (ZTA) profiles, which allow you to add users and groups to unique traffic steering configurations for client-based ZTA connections. [Help](#)

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	Test1	3 Destinations Trusted Networks Enabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Enabled	1 Users 0 Groups	Dec 17, 2025

Default Profile

If there is no profile match, the default profile is applied. This profile includes private resources that are enabled for client-based Zero Trust Access.

Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
Default ZTA Profile	24 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	All Users All Groups	Dec 17, 2025

- 신뢰할 수 있는 네트워크 프로파일의 이름을 제공하고 다음 조건 중 하나 이상을 구성합니다.
 - DNS Servers - 클라이언트가 신뢰할 수 있는 네트워크에 있는 경우 네트워크 인터페이스에 있어야 하는 모든 DNS 서버 주소의 쉼표로 구분된 값입니다. 입력한 모든 서버를 사용하여 이 프로파일을 일치시킬 수 있습니다. TND가 일치하려면 DNS 서버 주소 중 하나가 로컬 인터페이스와 일치해야 합니다.
 - DNS Domains - 클라이언트가 신뢰할 수 있는 네트워크에 있는 경우 네트워크 인터페이스에 포함해야 하는 DNS 접미사의 쉼표로 구분된 값입니다.
 - Trusted Server- 제공한 해시와 일치하는 해시가 있는 TLS 인증서를 제시하는 네트워크에 하나 이상의 서버를 추가합니다. 443 이외의 포트를 지정하려면 표준 표기법을 사용하여 포트를 추가합니다. 최대 10개의 신뢰할 수 있는 서버를 추가할 수 있으며, 이 중 하나만 검증을 통과해야 합니다.
 - Certificate Public Key Hash: 인증서 해시를 [생성하는 방법](#)을 알아보려면 단계 사전 요구 사항 및 [시스템](#) 제한을 선택합니다.

단계를 반복하여 신뢰할 수 있는 네트워크 프로파일을 더 추가합니다.



참고: 동일한 조건 내의 여러 옵션은 OR 연산자입니다. 정의된 다른 기준은 AND 연산자입니다.

☰

Home

Experience Insights

Connect

Resources

Secure

Monitor

Investigate

Admin

Workflows

🔧 Step 2, Task 2: Defined a trusted network

2/4 tasks

← Trusted Networks

Edit Trusted Networks

Include as many criteria as required to define a trusted network or network segment. [Help](#)

Trusted Network Name

TestDNSServer

☐ Set as default Trusted Network for UZTA ⓘ

Inspect

☒ Physical adapters

☐ Physical and virtual adapters Beta

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

CriterionDNS Domains ⓘ

DNS Domains

amitlab.com

— Remove Criterion

AND

CriterionDNS Servers ⓘ

DNS Servers

192.168.52.2

— Remove Criterion

+ Add Criterion

2단계: 프라이빗 또는 인터넷 액세스를 위한 TND 활성화

- Connect> 로 이동합니다. End User Connectivity
- ZTA 프로필 수정
- 어느Secure Private Destinations쪽에 Secure Internet Access

보안 프라이빗 액세스

1 Secure Private Access
1 Destination

2 Secure Internet Access

3 Users and Groups

Secure Private Access

Add the private destinations and private resources to

Traffic Steering

Options

보안 인터넷 액세스

✓ Secure Private Access
1 Destination

2 Secure Internet Access

3 Users and Groups

Secure Internet Access


Add the Internet and SaaS destinations to

Traffic Steering

Options

- 클릭 Options
 - 전에 Use trusted networks to secure private destinations 선택한 옵션 Use trusted networks to secure internet destinations 을 클릭하거나 종속합니다.
 - 클릭 + Trusted Network

Name	Inspector Adapters	DNS Domains	DNS Servers	Trusted Servers
------	--------------------	-------------	-------------	-----------------



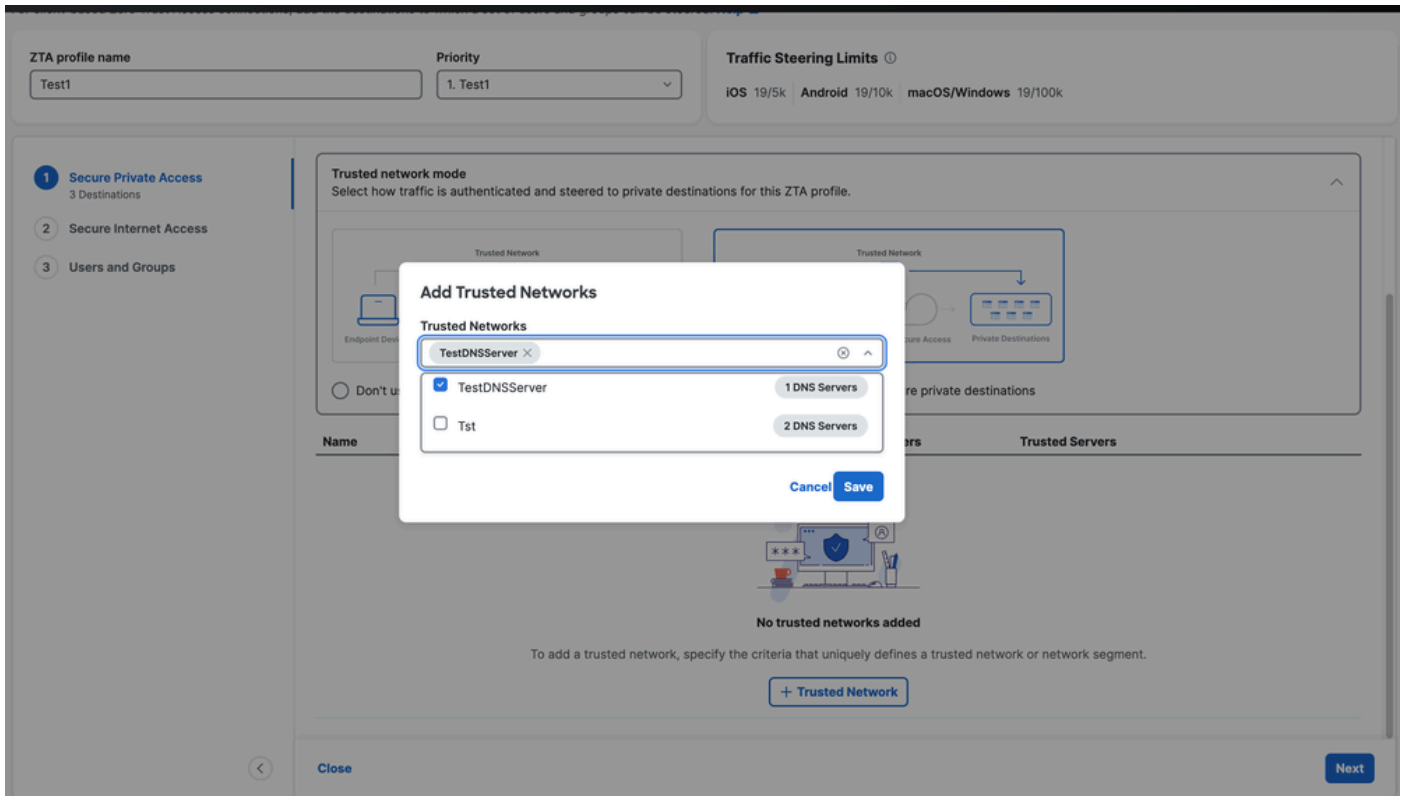
No trusted networks added

To add a trusted network, specify the criteria that uniquely defines a trusted network or network segment.

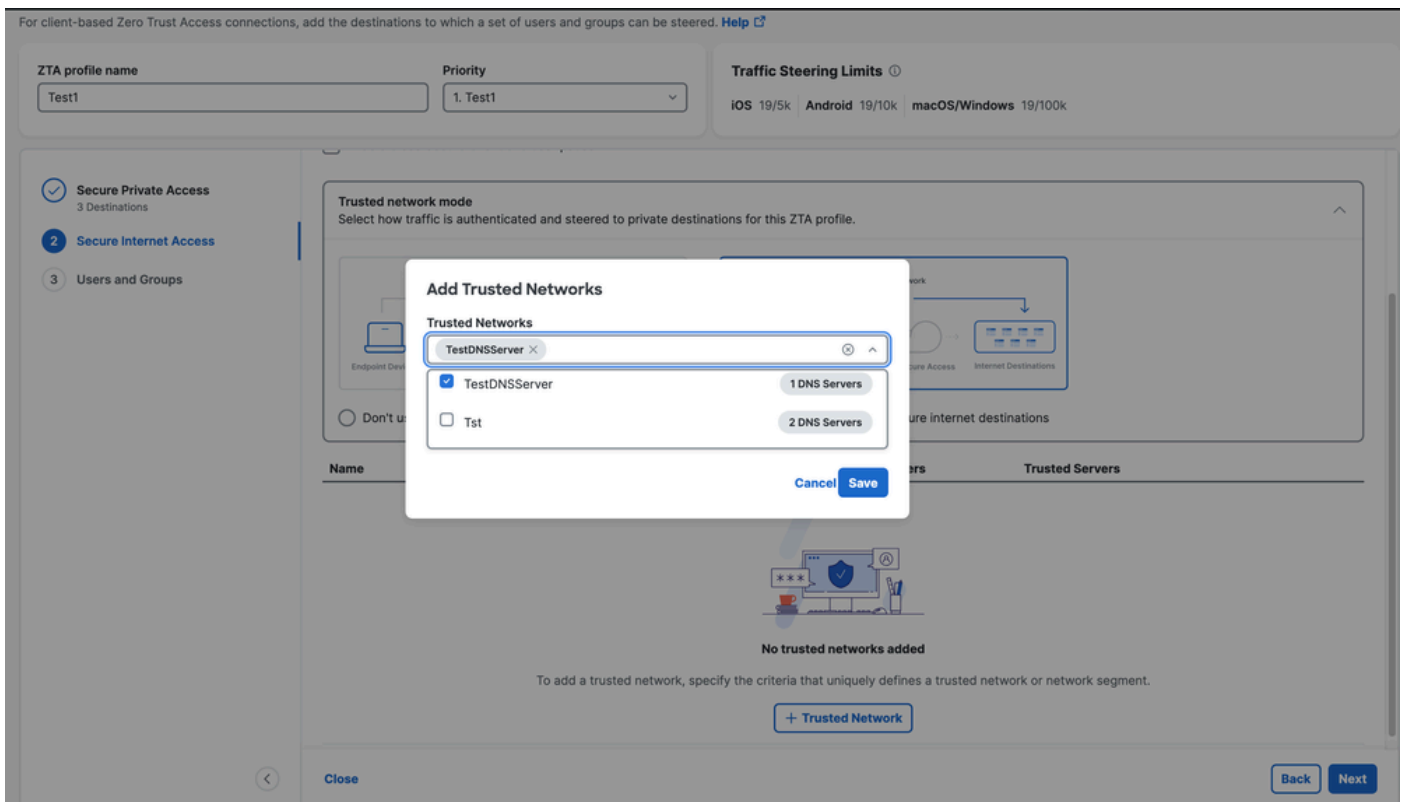
+ Trusted Network

- 이전 페이지에서 구성한 신뢰할 수 있는 네트워크 프로필을 선택하고 Save

보안 프라이빗 액세스



보안 인터넷 액세스



- 를 Users/Groups ZTA Profile에 할당하고 을 클릭합니다 Close.

ZTA profile name

Test1

Priority

1. Test1

Traffic Steering Limits ⓘ

iOS 19/5k

Android 19/10k

macOS/Windows 19/100k

Secure Private Access

3 Destinations

Secure Internet Access

Users and Groups

Users and Groups

Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users 1

Groups 0

Q Search

+ Users and Groups

Name	Email	Type	Users
amara2_saf@cxsecurity.com		User	-

Rows per page 10 < >

Back

Close

3단계: 클라이언트측 컨피그레이션

1. Physical Adaptor(물리적 어댑터)를 기준으로 선택한 대로 Ethernet Adaptor(이더넷 어댑터) 아래에 올바른 DNS 서버가 정의되어 있는지 확인합니다
2. 연결별 DNS 접미사가 정의되어 있는지 확인합니다.

```

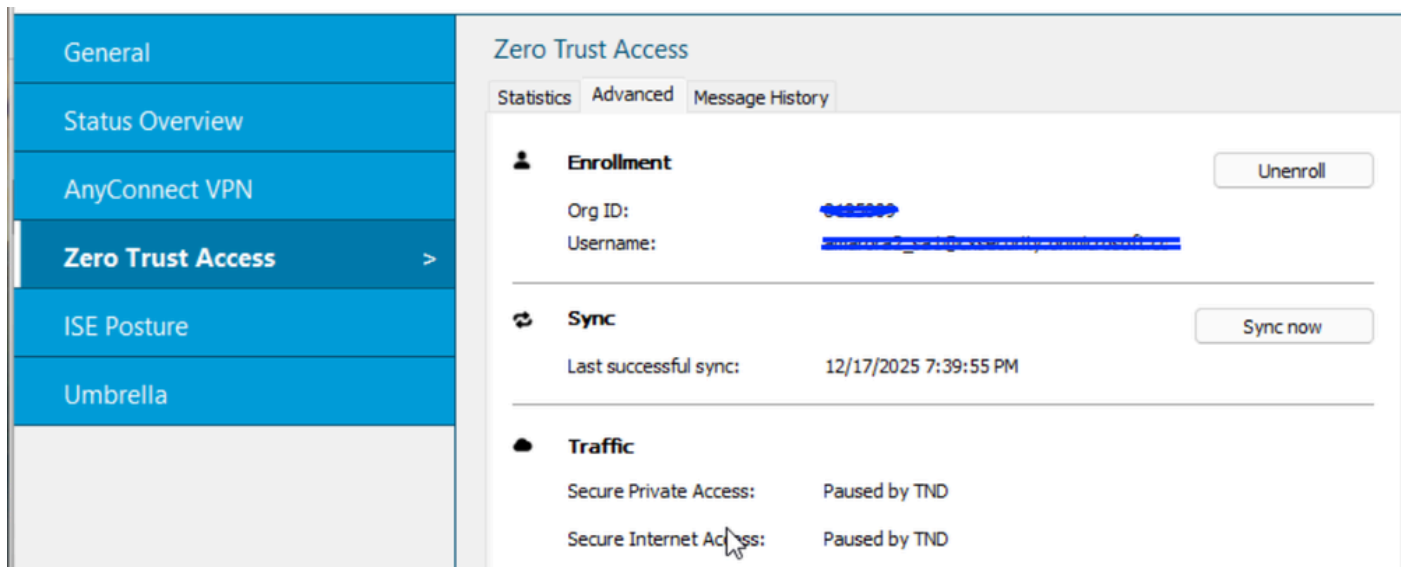
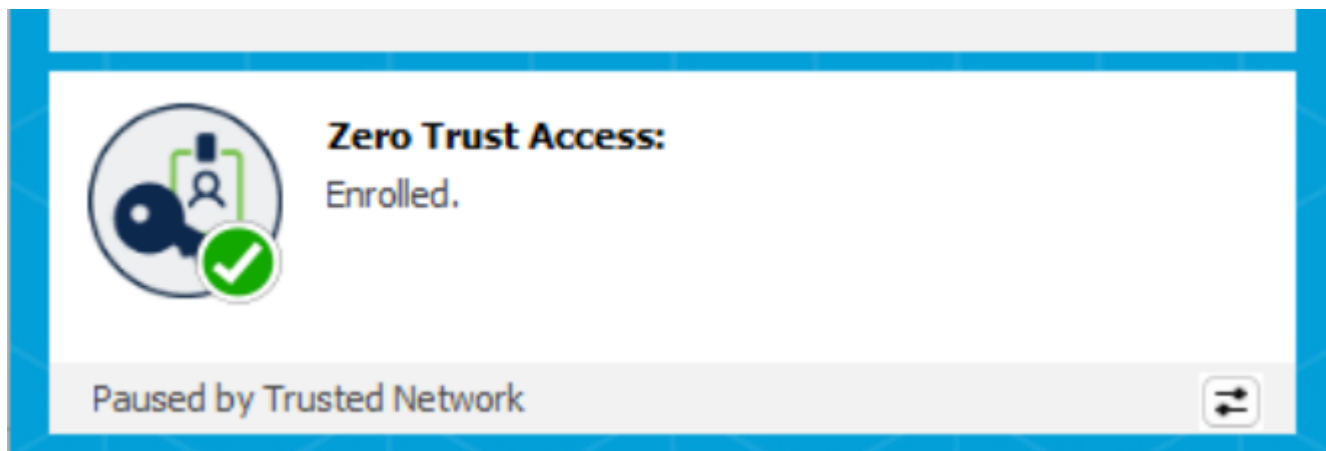
Ethernet adapter Ethernet0:

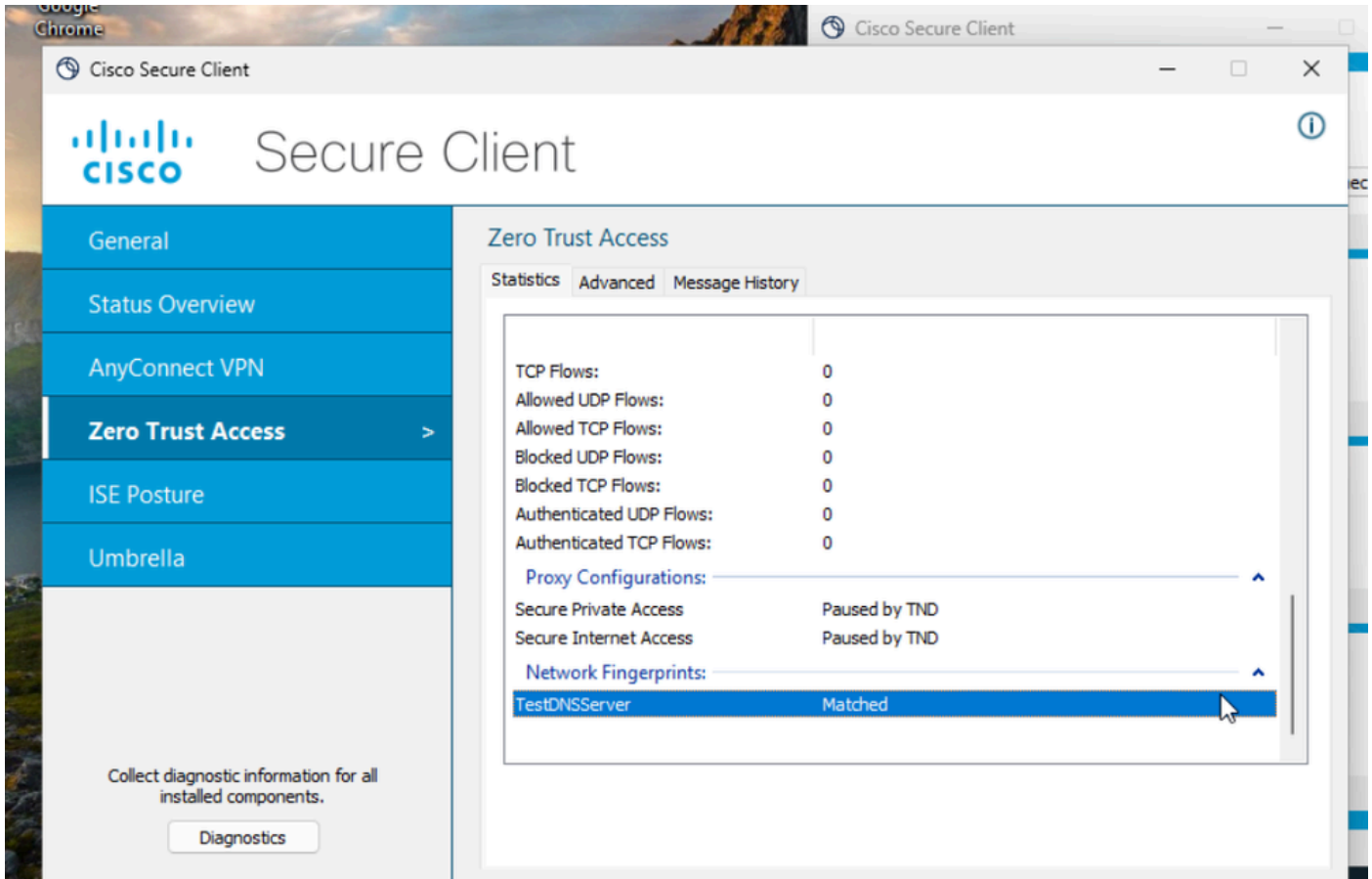
Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-4F-E6-BD
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.52.213(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, December 17, 2025 8:04:46 PM
Lease Expires . . . . . : Wednesday, December 17, 2025 9:02:07 PM
Default Gateway . . . . . : 192.168.52.2
DHCP Server . . . . . : 192.168.52.254
DNS Servers . . . . . : 192.168.52.2
Primary WINS Server . . . . . : 192.168.52.2
NetBIOS over Tcpip. . . . . : Enabled
  
```

다음 ZTA 컨피그레이션이 Secure Client에 몇 분 후에 동기화되면 ZTA 모듈이 구성된 Trusted Networks 중 하나에 있음을 감지하면 자동으로 일시 중지됩니다.

다음에 확인합니다.

- 보안 클라이언트에서





• DART 번들에서 - ZTA 로그

구성된 TND 규칙이 없습니다.

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:316
ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND는 ProxyConfig 'default_spa_config'(규칙 없음)에 연결합니다.

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:316
ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND는 ProxyConfig 'default_tia_config'(규칙 없음)에 연결합니다.

구성된 TND 규칙 - DNS 서버 - 클라이언트 수신 컨피그레이션

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4] W/ CaptivePortalDetectionService.cpp:308
CaptivePortalDetectionService::getProbeUrl() 마지막 네트워크 스냅샷 없음, 첫 번째 프로브 url 사용

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] // NetworkChangeService.cpp:144 NetworkChangeService::Start() 초기 네트워크 스냅샷:

이더넷0: subnets=192.168.52.213/24 dns_servers=192.168.52.2 dns_domain=amitlab.com dns_suffixes=amitlab.com isPhysical=true
default_gateways=192.168.52.2
captivePortalState=알 수 없음

conditional_actions": [{"action": "disconnect"}]는 TND가 ZTA 프로필에 구성되었음을 알려줍니다.

2025-12-17 17:55:36.430233 csc_zta_agent[0x00000c90/config_service, 0x0000343c] // ConfigSync.cpp:309
ConfigSync::HandleRequestComplete()에서 새 구성을 받았습니다.

{"ztnaConfig":{"global_settings":{"exclude_local_ip":true},"network_fingerprints":[{"id":"28f629ee-7618-44cd-852d-6ae1674e3cac","label":"TestDNSServer","match_dns_domains":["amitlab.com"],"match_dns_servers":

["192.168.52.2"],"retry_interval":300}],proxy_configs":[{"conditional_actions":[{"action":"disconnect","check_type":"on_network","match_network_fingerprint":"28f629ee-7618-44cd-852d-6ae1674e3cac"}],{"action":"connect"},"id":"default_spa_config","label":"Secure Private 액세스

","match_resource_config":["spa_steering_config"],"proxy_server":"spa_proxy_server"},"conditional_actions":[{"action":"disconnect","check_type":"on_network"}, {"action":"connect"}],{"id": "7618-44cd-852d-6ae1674e3cac"}]

2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main, 0x0000343c] // NetworkFingerprintService.cpp:196
NetworkFingerprintService::handleStatusUpdate() 브로드캐스트 네트워크 핑거프린트 상태: 지문: 28f629ee-7618-44cd-852d-6ae1674e3cac 인터페이스: 이더넷0

DNS 조건에서 TND 연결 끊기

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:378
ActiveSteeringPolicy::UpdateActiveProxyConfigs() 활성 프록시 컨피그레이션 업데이트

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:287
ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND는 조건으로 인해 ProxyConfig "Secure Internet Access"의 연결을 끊습니다.
네트워크(_n): 28f629ee-7618-44cd-852d-6ae1674e3cac 작업 = 연결 끊기

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:366
ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Private Access'의 연결이 끊어졌습니다. 이유: 비활성Tnd
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:366
ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Internet Access'의 연결이 끊어졌습니다. 이유: 비활성Tnd
규칙 유형 DNS 일치

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main, 0x0000343c] // ZtnaTransportManager.cpp:1251
ZtnaTransportManager::closeObsoleteAppFlows() 오래된 ProxyConfig enrollmentId=7b35249c-64e1-4f55-b12b-58875a806969
proxyConfigId=default_tia_config TCP destination [safebrowsing.googleapis.com]:443 srcPort=61049 realDestDestDest ipAddr=172.253.122.95
process=<chrome.exe|PID 11904|user amit\amita> parentProcess=<chrome.exe|PID 5220|user amit\amita> matchRuleType=DNS

관련 정보

- [Cisco 기술 지원 및 다운로드](#)
- [Cisco Secure Access Help Center](#)
- [Cisco ISE 설계 가이드](#)

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.