Cisco Secure Access 릴리스 노트

최초 게시일: 2023년 10월 27일
마지막 수정일: 2023년 12월 15일

알림: Cisco Secure Access - 브라우저 Zero Trust 액세스 URL 변경

2023 년 12 월 5 일 화요일부터 Cisco Secure Access 에서 브라우저 기반 Zero Trust 액세스 URL(브라우저 기반 전용)이 .com 도메인에서 .io 도메인으로 변경됩니다. 브라우저 기반 URL 은 최종 사용자가 브라우저 기반 Zero Trust 액세스를 사용하여 프라이빗 리소스에 안전하게 연결하기 위해 기업에서 설정하는 맞춤형 주소입니다.

원활한 전환을 위해, 12 월 5 일부터 15 일까지 현재 .com URL 과 새 .io URL 을 함께 사용하게 되며, 이후 .com URL 의 사용은 중지됩니다. 사용자 측에서는 각 리소스를 고유하게 식별하는 URL 접두사를 변경할 필요가 없습니다. Secure Access 가 자동으로 *<your organization's tenant ID>-ztna.sse.cisco.io* 접두사를 조인하여 새 공용 URL 주소를 구성합니다.

이렇게 하려면 **애플리케이션 소유자 및 엔드 유저에게 업데이트된 URL 을 알려야 합니다**. 엔드 유저는 새 URL 을 즐겨찾기에 추가하는 것이 좋습니다.

알려진 문제 - 2023년 12월 15일 릴리스

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
리소스 커넥터 구축	리소스 커넥터 VM 은 복제할 수 없으며 독립적으로 구축해야 합니다.	리소스 커넥터가 복제된 경우, 원본 인스턴스와 복제된 인스턴스가 제대로 작동하지 않습니다.	IT 관리자
리소스 커넥터에 대한 IPv6 지원	리소스 커넥터에서는 IPv4 주소만 지원됩니다. IPv6 은 아직 지원되지 않습니다.	리소스 커넥터는 IPv4 로만 구성할 수 있습니다.	IT 관리자

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
리소스 커넥터를 통한 브라우저 기반/클라이언트 기반 ZTNA 액세스	네트워크 서브넷이 CGNAT 범위 100.64.0.0/10 과 중복되지 않아야 합니다.	중복 네트워크를 구성하면 트래픽을 프라이빗 리소스로 라우팅하는 데 문제가 발생합니다.	IT 관리자
대시보드에서 로깅	리소스 커넥터를 통과하는 ZTNA 트래픽의 경우 기록되는 방화벽 이벤트의 IP 주소가 부정확할 수 있습니다.	로깅 이벤트가 부정확할 수 있습니다.	IT 관리자
리소스 커넥터 인터페이스	리소스 커넥터는 단일 인터페이스에서만 실행할 수 있습니다.	여러 인터페이스로 구성된 리소스 커넥터는 지원되지 않습니다.	IT 관리자
리소스 커넥터 그룹 프로비저닝 키	프로비저닝 키는 관리 대시보드의 API 키 페이지에 표시됩니다.	관리자가 프로비저닝 키를 삭제하면 삭제된 프로비저닝 키를 사용하여 새 리소스 커넥터를 등록할 수 없게 됩니다.	IT 관리자
리소스 커넥터 그룹 영역 변경	관리자는 생성된 후 리소스 커넥터 그룹과 연결된 영역을 편집할 수 없습니다.	리소스 커넥터 그룹을 생성한 후에는 영역을 변경할 수 없습니다. 이 그룹을 기존 영역에서 삭제하고 새 영역에서 다시 생성해야 합니다.	IT 관리자

알려진 문제 - 2023년 10월 27일 릴리스

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
클라이언트 기반 ZTNA	Secure Client ZTA 모듈은 Windows 10 및 11 과 MacOS 버전 11, 12, 13, 14 에서만 사용 가능합니다.	다른 플랫폼은 지원되지 않습니다.	엔드 유저

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
동기화 간격	조정 구성, 클라이언트에서의 포스처 업데이트, 터널 설정 등 특정 구성 변경 사항을 모든 시스템 구성 요소에 적용하려면 최대 5 분이 걸립니다.		
외부 API	외부 API 는 문서화되지 않고 지원되지 않습니다.	현재 보안 액세스와 SDWAN 통합을 지원하는 외부 API 는 두 가지뿐입니다. Umbrella 의 기존 API 중 일부는 문서화되지 않거나 지원되지 않는 API 로 사용할 수 있습니다.	IT 관리자/개발자 커뮤니티
데이터 보존	데이터 보존은 DNS 쿼리의 경우 1 년, FW, SWG 및 DNS 의 경우 30 일입니다.	없음	IT 관리자
액세스 정책 지원	SWG 및 DNS 는 액세스 정책에서 인라인 IP 를 적용하지 않습니다.	소스 또는 대상의 인라인 IP 에 대해 고객이 생성한 규칙은 방화벽에서만 지원됩니다.	IT 관리자
정책 규칙 관리	지원되는 규칙 제한은 5K 입니다. 액세스 규칙의 수가 5K 를 초과하면 정책 UI 및 정책 시행의 성능이 영향을 받습니다.	고객은 큰 성능 영향 없이 인터넷 액세스 및 프라이빗 액세스 규칙을 포함하여 최대 5K 의 규칙을 생성할 수 있습니다.	IT 관리자
브랜치 연결에 대한 ECMP 지원	ECMP 기반 로드 밸런싱은 지원되지 않습니다.	브랜치 연결은 ECMP 를 활용하여 여러 터널에 로드 밸런싱할 수 없습니다.	IT 관리자

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
RAVPN	원격 액세스 VPN 서비스로 업그레이드하면 현재 세션의 연결이 끊어집니다.	사용자는 세션을 다시 설정해야 합니다. 이는 지속적인 VPN 연결을 제공하는 기존 ASA 설계입니다.	엔드 유저
RAVPN	중복 SAML 구성이 있는 여러 원격 액세스 VPN 프로파일이 제대로 작동하지 않습니다.	VPN 프로파일마다 다른 SAML 구성을 사용해야 합니다.	IT 관리자
중복 서브넷은 지원되지 않음	동일한 조직 내의 각 브랜치는 서로 다른 중첩되지 않은 서브넷을 사용해야 합니다. 예를 들어 동일한 조직의 두 브랜치는 서브넷 192.168.10.0/24 를 사용할 수 없습니다.	고객은 각 브랜치에 서로 다른 서브넷이 있는지 확인해야 합니다. 또는 자신의 측에서 브랜치 트래픽을 NAT 처리하고 CNHE 에 대해 NAT 주소만 구성해야 합니다.	IT 관리자
SAML + IP 서로게이트	IP 서로게이트가 활성화된 조직의 경우 SAML 을 활성화했다가 비활성화하면 SAML 이 비활성화된 후 최대 12 시간 동안에는 사용자 ID 가 인증된 사용자에게 계속 적용될 수 있습니다.	고객은 이전에 인증된 사용자에게 적용되는 사용자 기반 정책을 확인할 수 있습니다. 인증되지 않은 사용자에게는 영향을 주지 않습니다.	엔드 유저
Mac 의 클라이언트 기반 ZTA	현재 macOS 에서는 여러 사용자를 지원할 수 없습니다. 등록하는 첫 번째 사용자만 ZTA 를 활용할 수 있습니다. 또한 동일한 디바이스에 여러 사용자를 등록할 수 없습니다. 이는 macOS 의 Secure Enclave 에서 보안이 기본적으로 작동하는 방식 때문입니다. Cisco 에서는 이 문제와 관련된 사용자 환경을 개선할 수 있는 방법을 조사하고 있으며 앞으로 몇 주 동안 추가 정보를 제공할 예정입니다.	한 명의 사용자만 macOS 디바이스에서 ZTA 등록을 성공적으로 수행할 수 있습니다.	여러 사용자가 단일 macOS 디바이스를 사용하는 고객

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
엔드포인트 포스처 관리	조직당 포스처 프로파일 제한은 100 개입니다.	조직 내에서 생성된 포스처 프로파일의 수가 100 을 초과하는 경우 사용되지 않는 포스처 프로파일을 삭제하거나 기존 프로파일을 편집하라는 오류 메시지가 고객에게 표시됩니다.	IT 관리자
AD 용 자동 업그레이드 구성	고객은 AD 컨트롤러용 업그레이드 기간을 구성할 수 있어야 합니다. 그러나 현재는 이 기능을 사용할 수 없습니다.	업그레이드는 매일 오전 2 시~오전 6 시 사이에 이루어집니다.	IT 관리자
BGP 에서 학습한 라우팅 정보가 사용자 인터페이스에 표시되지 않음	BGP 네트워크 터널 - 원격 위치에서 학습된 경로/접두사가 아직 표시되지 않습니다.		IT 관리자
클라이언트 기반 및 클라이언트리스 ZTA	ZTNA 로부터의 프라이빗 트래픽의 경우, IPS 이벤트의 소스 IP 는 (100.64.0.0/10) 범위이며 클라이언트 IP 는 포함되지 않습니다.	고객은 이벤트를 식별하기 위해 로그에서 사용자 ID 를 대신 입력해야 합니다.	IT 관리자
클라이언트리스 ZTA	클라이언트리스 ZTA 는 "TLS 1.3 전용" 애플리케이션을 지원하지 않습니다.	고객은 애플리케이션 측에서 TLS 1.2 도 활성화해야 합니다.	IT 관리자
FWaaS	대상이 모두인 액세스 정책의 경우 애플리케이션 정보가 방화벽 이벤트에 표시되지 않습니다.	기능에는 영향이 없습니다.	IT 관리자
FWaaS	연결에 우선하는 보안 또는 최대 탐지 IPS 프로파일이 구성된 경우 SAML 인증이 방화벽(IPS)에서 차단될 수 있습니다. 이는 브랜치-인터넷 트래픽에만 적용됩니다.	SAML 인증 로그인 페이지는 인증을 위해 제공되지 않습니다.	엔드 유저

기능	주의 사항 설명	고객에게 미치는 영향은 무엇입니까?	어떤 사용자가 영향을 받습니까?
사용자 및 그룹	'모든 사용자 및 그룹 동기화'에서 '할당된 사용자 및 그룹만 동기화'로 Azure AD 범위를 변경하면 비활성화 이벤트가 전송되지 않습니다.	정의된 범위를 벗어난 사용자 및 그룹은 대시보드에 나열됩니다.	IT 관리자
보안 인터넷	이스라엘에서 Umbrella 로밍 모듈 또는 PAC 파일에 연결하는 사용자는 이스라엘 보안 액세스 PoP 에 도달하지 않습니다. 대신 트래픽이 프랑크푸르트 또는 런던으로 이동합니다. 해결 방법: IPsec 터널 또는 RAVPN 을 사용하여 이스라엘 PoP 에 연결합니다.	레이턴시 증가, 히브리어 대신 영어로 렌더링된 페이지, 지리위치, 데이터 주권.	엔드 유저