일반 운영 기능

시작하기

표 *1:* 시작하기

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
구성용 **ASA CLI**	구성용 제한된 **Threat Defense CLI,** 전체 **GUI** 구성 참조: 시작 가이드(콘솔 액세스), 명령 참조, 디바이스 구성 가이드	threat defense CLI에는 초기 구성 전용 및 일부 특수 작업에 대한 제한된 명령이 포함되어 있습니다. 디바이스 구성 검색이 제한된 management center에서 구성을 수행해야 합니다.
모니터링용 **ASA CLI**	모니터링용 **Threat Defense CLI** UI 경로: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**> **Advanced Troubleshooting(**고급 문제 해결**)** > **Threat Defense CLI(**위협 방어 **CLI)** 참조: 시작 가이드(콘솔 액세스), 명령 참조, 웹 인터페이스에서 Threat Defense CLI 사용	ASA에서 사용할 수 있는 동일한 **show** 명령을 사용할 수 있습니다. SSH를 사용하여 콘솔에서 CLI에 액세스하거나 CLI 웹 툴을 사용할 수 있습니다.
초기 구성	초기 구성 참조: 시작 가이드(콘솔 액세스)	CLI 또는 device manager를 사용하여 네트워크 설정을 지정하고 management center에 등록합니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
구성 변경	구성 구축 UI 경로: 구축 참조: 구성 구축	management center에서 변경 사항을 구축해야 합니다.
스마트 라이선스	스마트 라이선스 UI 경로: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 참조: 라이선스 방법: Cisco Smart Account에 Management Center 등록	라이선스는 management center에서 사용 및 할당됩니다.
투명한 또는 라우팅된 방화벽 모드	투명한 또는 라우팅된 방화벽 모드 참조: 투명한 또는 라우팅된 방화벽 모드	ASA와 마찬가지로 디바이스를 management center에 등록하기 전에 CLI를 사용하여 방화벽 모드를 변경해야 합니다.

고가용성 및 확장성

표 *2:* 고가용성 및 확장성

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
다중 상황 모드	다중 인스턴스 모드 또는 가상 라우터 UI 경로: • Firepower 4100/9300 다중 인스턴스: **Logical Devices(**논리적 디바이스**)** > **Add(**추가**)** (섀시 관리자) • 가상 라우터: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)** 참조: Firepower 4100/9300에서 다중 인스턴스 기능 사용, 가상 라우터 방법: 가상 라우터 생성, 가상 라우터에 인터페이스 할당, 가상 라우터에 대한 NAT 구성, 중복 주소 공간으로 인터넷 액세스 제공, 라우팅 정책 구성	대부분의 경우 고객은 전체 분리가 아닌 별도의 라우팅 테이블만 필요할 수 있습니다. 이 경우 가상 라우터를 사용할 수 있습니다. 완전한 구성 분리를 위해 지원되는 플랫폼에서 다중 인스턴스 모드를 사용합니다. 이 구현은 ASA 다중 상황 모드와 다르지만 기능은 유사합니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
액티브/스탠바이 장애 조치	고가용성 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **High Availability(**고가용성**)** 참조: 고가용성 방법: 고가용성(HA) 쌍 생성	
클러스터링	클러스터링 UI 경로: • Firepower 4100/9300: **Logical Devices(**논리적 디바이스**)** > **Add(**추가**)** (섀시 관리자) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **Device(**디바이스**)**(management center) • 퍼블릭 클라우드용 Threat Defense Virtual **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **Device(**디바이스**)** • Secure Firewall 3100: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **Cluster(**클러스터**)** • 프라이빗 클라우드용 Threat Defense Virtual: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **Cluster(**클러스터**)** 참조: Secure Firewall 3100에서 위협 방어용 클러스터 구축, Firepower 4100/9300에서 위협 방어용 클러스터 구축, 퍼블릭 클라우드에서 가상 위협 방어용 클러스터 구축, 프라이빗 클라우드에서 가상 위협 방어용 클러스터 구축 방법: 클러스터 생성, 기존 클러스터 수정, 기존 클러스터에 노드 추가, 클러스터에서 데이터 노드 제거, 클러스터 분리, 클러스터 삭제, 클러스터링에서 노드 분리, 클러스터링에서 데이터 노드 삭제	사이트 간 클러스터링 및 분산 사이트 간 VPN은 지원되지 않습니다.

인터페이스

threat defense의 경우 인터페이스는 디바이스별로 구성됩니다. 그러나 대부분의 기능은 보안 영역에 인터페이스를 할당한 다음 인터페이스에 직접 정책을 적용하는 것이 아니라 영역에 정책을 적용합니다. 보안 정책 자체와 마찬가지로 영역은 여러 디바이스에서 공유할 수 있는 개체로 구성됩니다.

참고 threat defense는 ASA와 같은 일반 방화벽 인터페이스를 지원하지만 다른 유형의 IPS 전용 인터페이스도 지원합니다.

표 *3: Interfaces*

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
관리 인터페이스	관리 인터페이스 UI 경로: **Device**(디바이스) > **Device Management**(디바이스 관리) > **Edit**(편집) > **Devices**(디바이스) > **Management**(관리) 참조: Threat Defense 초기 구성 완료	ASA에는 자체 라우팅 테이블이 있는 관리 전용 인터페이스가 있지만 대부분 데이터 인터페이스와 유사하게 작동합니다. threat defense에는 데이터 인터페이스와 별도로 관리 인터페이스가 있습니다. 이 인터페이스는 디바이스를 관리 센터에 설치하고 등록하는 데 사용됩니다. 고유 IP 주소 및 정적 라우팅을 사용합니다.
물리적 인터페이스	물리적 인터페이스 UI 경로: **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Edit**(편집) > **Interfaces**(인터페이스) 참조: 인터페이스 개요 방법: 인터페이스 설정 구성	
Firepower 1010 스위치 포트	**Firepower 1010** 스위치 포트 UI 경로: **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Edit**(편집) > **Interfaces**(인터페이스) 참조: Firepower 1010 스위치 포트 구성	
EtherChannel	**EtherChannel** UI 경로: **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Edit**(편집) > **Interfaces**(인터페이스) 참조: EtherChannel 인터페이스 구성	
루프백 인터페이스	루프백 인터페이스 UI 경로: **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Edit**(편집) > **Interfaces**(인터페이스) 참조: 루프백 인터페이스 구성	

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
VLAN 하위 인터페이스	**VLAN** 하위 인터페이스 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Interfaces(**인터페이스**)** 참조: VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성	
VXLAN 인터페이스	**VXLAN** 인터페이스 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Interfaces(**인터페이스**)** 참조: VXLAN 인터페이스 구성	
라우팅 및 투명 모드 인터페이스	라우팅 및 투명 모드 인터페이스 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Interfaces(**인터페이스**)** 참조: 라우팅 및 투명 모드 인터페이스 구성	
고급 인터페이스 구성	고급 인터페이스 구성 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Interfaces(**인터페이스**)** 참조: 고급 인터페이스 설정 구성	
트래픽 영역	**ECMP** UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **ECMP** 참조: ECMP	

기본 설정

표 *4:* 기본 설정

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
DNS 서버	**DNS** 서버 UI 경로: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **DNS Server Group(DNS** 서버 그룹**)** • **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS** 참조: DNS Server Group(DNS 서버 그룹), Configure DNS(DNS 구성), FlexConfig Policies(FlexConfig 정책)	DNS 서버는 여러 디바이스에 적용할 수 있는 플랫폼 설정의 일부입니다. 참고 threat defense 전용 관리 인터페이스에 대한 DNS 서버는 **configure network dns servers** 및 **configure network dns searchdomains** 명령을 사용하여 CLI에서 구성됩니다.
ISA 3000 하드웨어 우회	**ISA 3000** 하드웨어 우회 UI 경로: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** • **Devices(**디바이스**)** > **FlexConfig** 참고: 정전(ISA 3000)에 대한 자동 하드웨어 우회를 구성하는 방법	이 기능은 FlexConfig를 사용하여 구성할 수 있습니다.
ISA 3000 정밀 시간 프로토콜	**ISA 3000** 정밀 시간 프로토콜 UI 경로: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** • **Devices(**디바이스**)** > **FlexConfig** 참조: Precision Time Protocol을 구성하는 방법(ISA 3000)	이 기능은 FlexConfig를 사용하여 구성할 수 있습니다.
ISA 3000 듀얼 전원 공급장치	**ISA 3000** 정밀 듀얼 전원 공급 장치 UI 경로: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** • **Devices(**디바이스**)** > **FlexConfig** 참조: FlexConfig 정책	이 기능은 FlexConfig를 사용하여 구성할 수 있습니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
DHCP 서버	**DHCP** 서버 UI 경로: • IPv4: **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **DHCP** > **DHCP Server(DHCP** 서버**)** • IPv6: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Interfaces(**인터페이스**)** > **IPv6** > **DHCP** 참조: DHCPv4 서버 구성, DHCPv6 스테이트리스 서버 구성	
DHCP 릴레이 에이전트	**DHCP** 릴레이 에이전트 UI 경로: **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **DHCP** > **DHCP Relay(DHCP** 릴레이**)** 참조: DHCP 릴레이 에이전트 구성	
DDNS	**DDNS** UI 경로: **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **DHCP** > **DDNS** 참조: 동적 DNS 구성	
디지털 인증서	인증서**, PKI** UI 경로: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** • **Devices(**디바이스**)** > **Certificates(**인증서**)** 참조: PKI, 인증서 방법: • RA(원격 액세스) VPN에 대한 인증서 인증 - RA VPN에서 인증서 인증을 위한 인증서 맵 생성, 인증서 맵을 연결 프로파일에 연결 • 원격 액세스 VPN 구성을 위해 디바이스에 ID 인증서 생성 및 설치 - PKCS12 인증서 등록 개체, 수동 인증서 등록 개체, 자체 서명 인증서 등록 개체, SCEP 인증서 등록 개체, 수동 인증서 설치, PKCS12 설치, SCEP 또는 자체 서명 인증서 , 원격 액세스 VPN 구성 • VPN 구성 - 수동 재등록을 사용하여 인증서 갱신, 자체 서명, SCEP 또는 EST 등록을 사용하여 인증서 갱신	재사용 가능한 인증서 개체를 생성한 다음 디바이스별로 적용합니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
ARP 검사 및 **MAC** 주소 테이블	**ARP** 검사 및 **MAC** 주소 테이블 UI 경로: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Interfaces(**인터페이스**)** > **Advanced(**고급**)** > **ARP and MAC(ARP** 및 **MAC)** • **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **ARP Inspection(ARP** 검사**)** 참조: 고급 인터페이스 설정, ARP 검사 구성	ARP 검사는 여러 디바이스에 적용할 수 있는 플랫폼 설정의 일부입니다.
WCCP	**WCCP** UI 경로: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** • **Devices(**디바이스**)** > **FlexConfig** 참조: FlexConfig 정책	이 기능은 FlexConfig를 사용하여 구성할 수 있습니다.

라우팅

라우팅은 디바이스별로 구성됩니다.

표 *5:* 라우팅

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
데이터 및 관리 라우팅 테이블	데이터 및 관리 라우팅 테이블 참조: 라우팅을 위한 참조 방법: 라우팅 정책 구성	ASA 및 threat defense에는 관리 라우팅 테이블과 데이터 라우팅 테이블에 대한 트래픽의 기본값이 서로 다릅니다. 참고 전용 관리 인터페이스에는 CLI에서 구성할 수 있는 별도의 Linux 라우팅 테이블이 있습니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
고정 경로 및 기본 경로	고정 경로 및 기본 경로 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **Static Route(**정적 경로**)** 참조: 고정 경로 및 기본 경로 방법: VTI에 대한 고정 경로 구성	
정책 기반 라우팅	정책 기반 라우팅 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **Policy Based Routing(**정책 기반 라우팅**)** 참조: 정책 기반 라우팅	
경로 맵	경로 맵 UI 경로: **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Route Map(**경로 맵**)** 참조: 경로 맵	
Bidirectional Forwarding Detection 라우팅	**Bidirectional Forwarding Detection** 라우팅 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **BFD** 참조: Bidirectional Forwarding Detection 라우팅	
BGP	**BGP** UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **BGP** 참조: BGP 방법: VTI에 대한 BGP 라우팅 구성	
OSPF	**OSPF** UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**편집**)** > **Routing(**라우팅**)** > **OSPF** 참조: OSPF	

ASA 기능	Secure Firewall Management Center의 Threat Defense 기능	참고
ISIS	**ISIS** UI 경로: • **Objects(개체)** > **Object Management(개체 관리)** > **FlexConfig** > **FlexConfig Object(FlexConfig 개체)** • **Devices(디바이스)** > **FlexConfig** 참조: FlexConfig 정책	이 기능은 FlexConfig를 사용하여 구성할 수 있습니다.
EIGRP	**EIGRP** UI 경로: **Devices(디바이스)** > **Device Management(디바이스 관리)** > **Edit(편집)** > **Routing(라우팅)** > **EIGRP** 참조: EIGRP	
멀티캐스트 라우팅	멀티캐스트 라우팅 UI 경로: **Devices(디바이스)** > **Device Management(디바이스 관리)** > **Edit(편집)** > **Routing(라우팅)** > **Multicast Routing(멀티캐스트 라우팅)** 참조: 멀티캐스트	
RIP	**RIP** UI 경로: **Devices(디바이스)** > **Device Management(디바이스 관리)** > **Edit(편집)** > **Routing(라우팅)** > **RIP** 참조: RIP	

AAA 서버

threat defense에서는 VPN 액세스에 AAA 서버를 사용할 수 있습니다. 관리 액세스를 위한 AAA 서버 및 로컬 데이터베이스에 대해서는 시스템 관리, 11 페이지의 내용을 참조하십시오.

표 *6: AAA* 서버

ASA 기능	Secure Firewall Management Center의 Threat Defense 기능	참고
VPN용 RADIUS	**VPN용 RADIUS** UI 경로: **Object(개체)** > **Object Management(개체 관리)** > **AAA Server(AAA 서버)** > **RADIUS Server Group(RADIUS 서버 그룹)**. 참조: RADIUS 서버 그룹 추가	

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
VPN용 **LDAP**	**VPN**용 **LDAP** UI 경로: **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 참조: Active Directory 영역 및 영역 디렉터리 생성 방법: 원격 액세스 VPN에 대한 LDAP 속성 맵 구성	
VPN용 **SAML Single Sign-On**	**VPN**용 **SAML Single Sign-On** UI 경로: **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **Single Sign-on Server(SSO(Single Sign-On)** 서버**)** 참조: SSO(Single Sign-On) 서버 추가 방법: SAML SSO(Single Sign-On) 서버 개체 추가	

시스템 관리

표 *7:* 시스템 관리

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
디바이스 관리용 로컬 데이터베이스	내부 사용자**(management center)** UI 경로: 시스템 (⚙) > **Users(**사용자**)** 참조: 내부 사용자 추가 사용자**(threat defense)** 참조: CLI에서 내부 사용자 추가	management center 및 threat defense는 별도의 사용자 데이터베이스를 유지합니다. 웹 액세스 및 CLI 액세스를 위한 management center 사용자를 구성할 수 있습니다. threat defense 사용자를 추가하려면 CLI를 사용해야 합니다. threat defense 사용자는 SSH 액세스 권한을 갖습니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
디바이스 관리용 **RADIUS**	**RADIUS(management center)** UI 경로: 시스템 (⚙) > **Users(**사용자**)** > **External Authentication(**외부 인증**)** 참조: Management Center에 대한 RADIUS 외부 인증 개체 추가 **RADIUS(threat defense)** UI 경로: • 시스템 (⚙) > **Users(**사용자**)** > **External Authentication(**외부 인증**)** • **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Edit(**편집**)** > **External Authentication(**외부 인증**)** 참조: SSH에 대한 외부 인증 구성	threat defense 사용자의 경우 플랫폼 설정의 일부로 RADIUS 인증 개체를 활성화합니다.
디바이스 관리용 **LDAP**	**LDAP(management center)** UI 경로: 시스템 (⚙) > **Users(**사용자**)** > **External Authentication(**외부 인증**)** 참조: Management Center에 대한 LDAP 외부 인증 개체 추가 **LDAP(threat defense)** UI 경로: • 시스템 (⚙) > **Users(**사용자**)** > **External Authentication(**외부 인증**)** • **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Edit(**편집**)** > **External Authentication(**외부 인증**)** 참조: SSH에 대한 외부 인증 구성	threat defense 사용자의 경우 플랫폼 설정의 일부로 LDAP 인증 개체를 활성화합니다.
SSH	액세스 목록**(management center)** UI 경로: 시스템 (⚙) > **Configuration(**구성**)** > **Access List(**액세스 목록**)** 참조: 액세스 목록 보안 셸**(threat defense)** UI 경로: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Secure Shell(**보안 셸**)** 참조: 보안 셸 구성	management center의 경우 SSH는 기본적으로 활성화되어 있습니다. 시스템 구성에서 액세스를 제한할 수 있습니다. threat defense의 경우 SSH는 전용 관리 인터페이스에 대해 기본적으로 활성화됩니다. **configure ssh-access-list** 명령을 사용하여 액세스를 제한할 수 있습니다. 데이터 인터페이스에 대한 SSH의 경우 플랫폼 설정에서 활성화합니다. 플랫폼 설정은 여러 디바이스에 적용할 수 있습니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
HTTPS	액세스 목록 UI 경로: 시스템 (⚙) > **Configuration(**구성**)** > **Access List(**액세스 목록**)** 참조: 액세스 목록	시스템 구성에서 management center에 대한 HTTPS 액세스를 제어할 수 있습니다. management center에서 관리하는 경우 threat defense는 HTTPS 액세스를 지원하지 않습니다.
소프트웨어 업그레이드	소프트웨어 업그레이드 UI 경로: 시스템 (⚙) > **Updates(**업데이트**)** 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 설명서 방법: Secure Firewall Threat Defense 업그레이드	management center를 사용하여 모든 업그레이드를 수행합니다.
다운그레이드	되돌리기 UI 경로: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **More(**추가**)** > **Revert Upgrade(**업그레이드 되돌리기**)** 참조: 업그레이드 되돌리기	
백업 및 복구	백업 및 복구 UI 경로: 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)** 참조: 백업 및 복원	
SSD 핫스왑**(Secure Firewall 3100)**	**SSD** 핫스왑**(Secure Firewall 3100)** 참조: Secure Firewall 3100에서 SSD 핫스왑	CLI를 사용하여 핫스왑을 수행합니다.
디버깅 메시지	디버깅 메시지 참조: 명령 참조의 debug 명령	
패킷 캡처	패킷 캡처 UI 경로: **Devices(**디바이스**)** > **Packet Capture(**패킷 캡처**)** 참조: 캡처 추적 사용 방법: 위협 방어 디바이스에 대한 패킷 캡처 수집	
Packet Tracer	**Packet Tracer** UI 경로: **Devices(**디바이스**)** > **Packet Tracer(**패킷 트레이서**)** 참조: 패킷 트레이서 사용 방법: 위협 방어 디바이스 문제 해결을 위한 패킷 추적 수집	

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
Ping	**Ping** UI 경로: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**> **Advanced Troubleshooting(**고급 문제 해결**)** > **Threat Defense CLI(**위협 방어 **CLI)** 참조: 명령 참조의 debug 명령	
Traceroute	**Traceroute** UI 경로: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**> **Advanced Troubleshooting(**고급 문제 해결**)** > **Threat Defense CLI(**위협 방어 **CLI)** 참조: 명령 참조의 traceroute 명령	
연결 모니터링	연결 모니터링 UI 경로: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**> **Advanced Troubleshooting(**고급 문제 해결**)** > **Threat Defense CLI(**위협 방어 **CLI)** 참조: 명령 참조의 show conn 명령	
show asp drop	**ASP** 삭제 UI 경로: 시스템 (⚙) > **Health(**상태**)** > **Policy(**정책**)** 참조: 상태 모듈	

모니터링

표 *8:* 모니터링

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
로깅	**Syslog** UI 경로: • ASA-style syslogs(ASA 스타일 시스템 로그): **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Syslog(**시스템 로그**)** • 파일 및 악성코드, 연결, 보안 인텔리전스 및 침입 이벤트에 대한 알림: **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Edit(**편집**)** > **Logging(**로깅**)** • 액세스 제어 규칙, 침입 규칙 및 기타 고급 서비스에 대한 알림: **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)** 참조: 시스템 로그 구성, 보안 이벤트에 대한 시스템 로그 메시지 전송 정보, 시스템 로그 알림 응답 생성	threat defense는 ASA와 동일한 시스템 로그 기능을 지원합니다. 그러나 threat defense에서만 지원하는 차세대 IPS 지원에 의해 생성된 로깅 및 알림도 지원합니다. 시스템 로그 설정은 여러 디바이스에 적용할 수 있는 플랫폼 설정의 일부입니다.
SNMP	**SNMP** UI 경로: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SNMP** 참조: SNMP 구성	SNMP 설정은 여러 디바이스에 적용할 수 있는 플랫폼 설정의 일부입니다.
Cisco Success Network	**Cisco Success Network** UI 경로: **Integration(**통합**)** > **SecureX** > **Cisco Cloud Support(Cisco Cloud** 지원**)** 참조: Cisco Success Network 등록 구성	
ISA 3000에 대한 알람	**ISA 3000**에 대한 알람 UI 경로: **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** 참조: Cisco ISA 3000에 대한 알람	이 기능은 FlexConfig를 사용하여 구성할 수 있습니다.