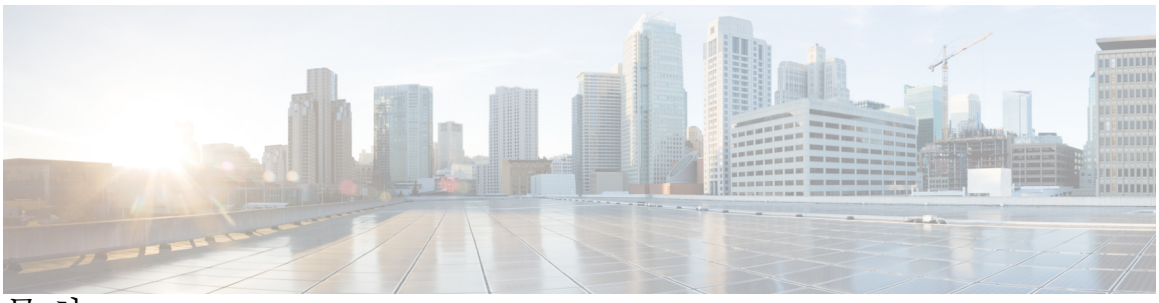
Cisco Secure Firewall ASA에서 위협 방어 기능으로 매핑

초판: 2023년 2월 21일

최종 변경: 2023년 7월 27일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

가이드 정보

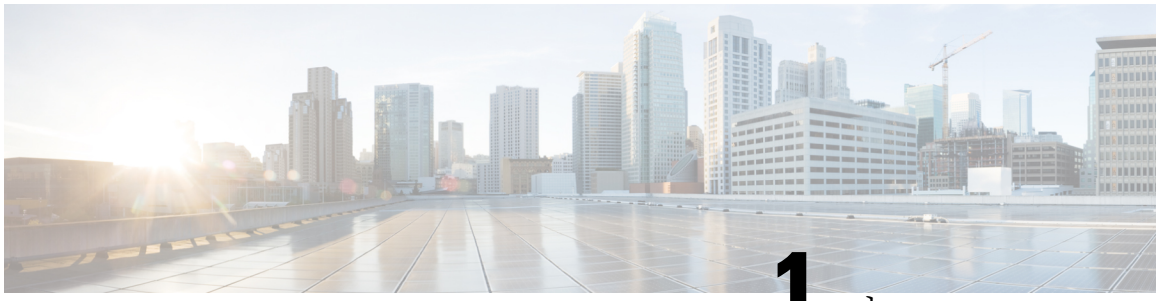
이 문서에서는 일반적으로 사용되는 ASA 기능 및 threat defense의 해당 기능에 대해 설명합니다. 각 ASA 기능(ASA 구성 가이드 장 또는 섹션과 관련이 있음)에 대해 Secure Firewall Management Center 또는 CDO(Cisco Defense Orchestrator) 클라우드 제공 방화벽 관리 센터에서 기능을 구성할 수 있는 UI 경로와 함께 threat defense에 해당하는 기능이 나열되어 있습니다. 기능 구현에 대해 자세히 알아볼 수 있도록 management center 설명서 링크도 제공됩니다. 각 기능에 대해 알려진 제한 사항 또는 차이점(있는 경우)이 제공됩니다.

management center는 여러 디바이스에 보안 정책을 적용할 수 있는 다중 디바이스 관리자입니다.

threat defense에는 ASA에 없는 여러 가지 유용한 보안 기능뿐만 아니라 ASA 관리 방법에서 사용할 수 없는 management center에서 제공하는 관리 기능이 포함되어 있습니다. 이 가이드에서는 ASA에서 사용할 수 없는 threat defense 기능을 나열하지 않습니다.

참고 management center는 FlexConfig라는 CLI 툴을 사용하여 일부 ASA 기능을 지원합니다.

가이드 정보



1 장

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.

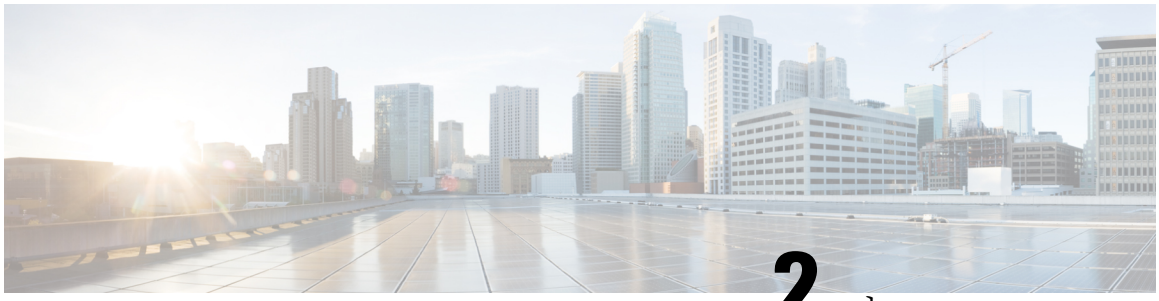
ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
HTTPS	액세스 목록 UI 경로: 시스템 (⚙) > **Configuration(**구성**)** > **Access List(**액세스 목록**)** 참조: 액세스 목록	시스템 구성에서 management center에 대한 HTTPS 액세스를 제어할 수 있습니다. management center에서 관리하는 경우 threat defense는 HTTPS 액세스를 지원하지 않습니다.
소프트웨어 업그레이드	소프트웨어 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.



2 장

방화벽 기능

다음 주제에서는 Secure Firewall Management Center 또는 클라우드 제공 Firewall Management Center를 사용하여 Secure Firewall Threat Defense에서 ASA 방화벽 기능 또는 해당 기능을 구성하는 방법을 설명합니다. 기능은 *CLI/ASDM* 설명서 *2: Cisco Secure Firewall ASA* 시리즈 방화벽 *CLI/ASDM* 구성 가이드 문서에 설명된 방식에 따라 느슨하게 구성되어 있습니다.

액세스 제어

ASA CLI 또는 ADSM을 사용하여 ASA를 구성할 때는 항상 한 번에 하나의 디바이스만 구성합니다.

이에 비해 Secure Firewall Management Center의 액세스 제어 정책은 항상 공유 정책입니다. 정책을 생성한 다음 하나 이상의 디바이스에 할당합니다.

일반적으로 여러 디바이스에 대한 액세스 제어 정책을 생성합니다. 예를 들어 모든 원격 위치 방화벽(원격 사이트를 기본 기업 네트워크에 연결)에 동일한 정책을 할당할 수 있습니다. 그런 다음 코어 데이터 센터에 상주하는 방화벽에 대해 다른 정책을 가질 수 있습니다. 물론 각 디바이스에 대해 별도의 정책을 생성할 수는 있지만 여러 디바이스 관리자를 효율적으로 사용하는 것은 아닙니다.

지정된 액세스 제어 규칙이 디바이스에 적용되는지 여부는 규칙에 지정된 인터페이스에 의해 제어됩니다.

- 인터페이스를 지정하지 않으면 정책이 할당된 모든 디바이스에 규칙이 적용됩니다.
- 특정 디바이스 인터페이스의 목록인 개체인 보안 영역을 지정하면 지정된 영역에 인터페이스가 있는 디바이스에만 규칙이 적용되고 구축됩니다. 보안 영역은 단순히 인터페이스 이름을 포함하는 것이 아니라 "디바이스의 인터페이스" 쌍을 포함합니다. 예를 들어, "inside on device1"은 "inside on device2"를 포함하지 않는 영역에 있을 수 있습니다.

다음 표에는 ASA의 기본 액세스 제어 기능 및 Secure Firewall Threat Defense 디바이스에서 해당 기능을 구성할 수 있는 위치가 나와 있습니다.

표 *9:* 액세스 제어 기능

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
액세스 제어용 개체.	개체 UI 경로: **Objects(**개체**)** > **Object Management(**개체 관리**)**. 참조: 개체 관리. 방법: 동적 개체 구성	또한 액세스 제어 정책을 편집할 때 네트워크 및 포트(서비스) 개체를 생성할 수 있습니다. 보안 그룹 태그 및 시간 범위도 지원됩니다. 네트워크 서비스 및 로컬 사용자 그룹은 지원되지 않거나 필요하지 않습니다. 액세스 제어 규칙에서 사용할 수 있는 추가 개체: 애플리케이션 필터, 지리위치, 인터페이스 보안 영역, URL 및 VLAN 태그 이러한 개체는 ASA에서 사용할 수 없는 기능에 적용됩니다.
비 액세스 제어 그룹/규칙에 대한 **ACL(Access Control List)**	**ACL(**액세스 제어 목록**)** UI 경로: 표준 및 확장 ACL: **Objects(**개체**)** > **Object Management(**개체 관리**)**. Ethertype ACL: **Devices(**디바이스**)** > **FlexConfig**. 참조: 개체 관리 및 FlexConfig 정책. 방법: • RA(원격 액세스) VPN 연결을 위한 트래픽 필터링 구성 - RA VPN 연결에서 트래픽 필터링을 위한 확장 액세스 목록 생성, RA VPN 연결에서 트래픽 필터링을 위한 그룹 정책에 확장 액세스 목록 추가	표준 또는 확장 ACL에 대한 개체를 생성한 다음 ACL이 필요한 라우팅 또는 기타 기능을 구성할 때 해당 개체를 사용합니다.
Access Control Rules(액세스 제어 규칙**)** - 기본(네트워크, 포트, 프로토콜, ICMP)	액세스 컨트롤 규칙 UI 경로: **Policies(**정책**)** > **Access Control(**액세스 제어**)**. 참조: 액세스 제어 규칙. 방법: • 디바이스 설정 - 액세스 제어 규칙 추가 - 기능 연습, 액세스 제어 정책 생성 • VTI 터널 구성 - VTI를 통한 암호화된 트래픽을 허용하도록 액세스 제어 규칙을 구성합니다. • 새 액세스 제어 정책 UI - 기능 연습 - 새 AC 정책 UI 액세스, 새 AC 정책 UI - 규칙 테이블, 새 AC 정책 UI - 규칙 생성, 새 AC 정책 UI - 규칙 수정	액세스 제어 정책은 기본 5-튜플 및 VLAN 액세스 제어 규칙을 지원합니다. 또한 지리위치 개체를 사용하여 특정 지리적 위치와 연결된 IP 주소를 대상으로 지정할 수 있습니다. 또한 사전 필터 정책을 사용하여 터널링된 트래픽(예: GRE) 및 기타 5-튜플 트래픽을 제어할 수 있습니다. 사전 필터 규칙은 액세스 제어 규칙보다 먼저 처리되며 ASA에서 사용할 수 없습니다. **Policies(**정책**)** > **Prefilter(**사전 필터**)**를 참조하십시오.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
액세스 제어 규칙 - 사용자 기반 제어	액세스 컨트롤 규칙 UI 경로: 사용자 이름 및 그룹 매핑을 가져오기 위한 규칙을 구성하려면 **Policies(**정책**)** > **Identity(ID)**로 이동합니다. 그런 다음 액세스 제어 규칙에서 사용자 이름 및 그룹을 선택할 수 있습니다. **Policies(**정책**)** > **Access Control(**액세스 제어**)**. 참조: 액세스 제어 규칙 및 사용자 ID 정책. 방법: 동적 개체에 대한 액세스 제어 정책 규칙 구성	ASA에 비해 사용자/그룹 멤버십을 획득할 수 있는 옵션이 더 많습니다.
액세스 제어 규칙 - 보안 그룹 및 Trustsec	액세스 컨트롤 규칙 UI 경로: ID 서비스 엔진을 설정하려면 **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Identity Sources(ID** 소스**)**로 이동합니다. 그런 다음 액세스 제어 규칙에서 보안 그룹 태그를 선택할 수 있습니다. **Policies(**정책**)** > **Access Control(**액세스 제어**)**. 참조: 액세스 제어 규칙 및 ISE/ISE-PIC를 사용하여 사용자 제어.	Identity Services Engine을 사용하여 사용자 기반 제어를 위한 사용자 이름/사용자 그룹 정보를 수집할 수도 있습니다.
(ASA에서는 사용할 수 없음) 액세스 제어 규칙—레이어 7 애플리케이션 제어.	액세스 컨트롤 규칙 UI 경로: **Policies(**정책**)** > **Access Control(**액세스 제어**)**. 참조: 액세스 제어 규칙.	예를 들어, 동일한 프로토콜 및 포트를 사용하는 애플리케이션에 대한 액세스 제어 규칙을 작성할 수 있습니다. 이를 통해 서로 다른 유형의 HTTP/HTTPS 트래픽을 구분할 수 있습니다. 애플리케이션 필터링을 사용하면 ASA에서 사용 가능한 것보다 더 세부적인 제어를 적용할 수 있습니다.
액세스 제어 규칙 - URL 필터링.	액세스 컨트롤 규칙 UI 경로: **Policies(**정책**)** > **Access Control(**액세스 제어**)**. 참조: URL 필터링.	URL 범주 및 평판을 기반으로 액세스를 제어하려면 URL 필터링 라이선스가 필요합니다. 또한 액세스 제어 정책 내에 정의된 보안 인텔리전스 정책을 사용하여 URL 또는 네트워크 개체를 기반으로 초기 필터링을 수행할 수 있습니다. DNS 정책은 DNS 조회 요청에 대해 동일한 작업을 수행할 수 있습니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
디바이스 간 트래픽에 대한 **ICMP** 액세스 규칙(**icmp permit/deny** 및 **ipv6 icmp permit/deny** 명령)	**ICMP** 액세스 규칙 UI 경로: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**, **ICMP Access(ICMP** 액세스**)** 페이지. . 참조: 플랫폼 설정	액세스 제어 정책과 마찬가지로 플랫폼 설정 정책도 공유되며 여러 디바이스에 정책을 적용할 수 있습니다.
Cisco Umbrella	**Cisco Umbrella** UI 경로: **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Cloud Services(**클라우드 서비스**)** **Policies(**정책**)** > **DNS** **Devices(**디바이스**)** > **VPN: Site-to-Site(VPN:** 사이트 간**)** > **SASE Topology(SASE** 토폴로지**)**. 참조: DNS 정책 및 Secure Firewall Threat Defense용 사이트 간 VPN.	Umbrella DNS 정책 및 Umbrella SASE VPN 토폴로지를 생성할 수 있습니다.

네트워크 주소 변환

액세스 제어 정책과 마찬가지로 NAT(Network Address Translation) 정책도 공유됩니다. NAT 정책을 생성한 다음 하나 이상의 디바이스에 할당합니다. FlexConfig 정책도 공유됩니다.

지정된 NAT 규칙이 디바이스에 구축되는지 여부는 규칙을 인터페이스별로 제한하는지 아니면 모든 인터페이스에 규칙을 적용하는지에 따라 달라집니다.

- 인터페이스를 지정하지 않으면 정책이 할당된 모든 디바이스에 규칙이 적용됩니다.
- 인터페이스 개체를 지정하면 지정된 개체에 인터페이스가 있는 디바이스에만 규칙이 적용되고 구축됩니다.

다음 표에는 ASA의 기본 네트워크 주소 변환 기능 및 Secure Firewall Threat Defense 디바이스에서 구성할 위치 또는 해당 기능이 나와 있습니다.

표 *10: NAT(Network Address Translation)* 기능

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
NAT(Network Address Translation) — 동적 NAT/PAT, 정적 NAT, ID NAT.	**NAT(**네트워크 주소 변환**)** UI 경로: **Devices(**디바이스**)** > **NAT**. 참조: NAT(네트워크 주소 변환). 방법: • 디바이스 설정 - NAT 정책 생성 - 기능 워크스루 • 가상 라우팅 구성 - 주소 공간이 겹치는 인터넷 액세스 제공, 가상 라우터용 NAT 구성	개체 및 2회 NAT를 모두 구성할 수 있습니다. 그러나 Secure Firewall Threat Defense에서는 이를 자동 NAT 및 수동 NAT라고 합니다.
포트 블록 할당을 사용하는 **PAT(Port Address Translation)**.	포트 블록 할당을 사용하는 **PAT(Port Address Translation)**. UI 경로: 전역 PAT 포트 블록 할당 설정(명령)을 구성하려면(**xlate block-allocation** 명령), **Devices(**디바이스**)** > **FlexConfig**를 사용합니다. 그런 다음 **Devices(**디바이스**)** > **NAT**를 사용하여 PAT 규칙을 구성할 수 있습니다. 참조: Network Address Translation(NAT) 및 FlexConfig 정책.	이 기능은 통신사급 또는 대규모 PAT에 사용됩니다.
세션당 **PAT** 또는 다중 세션 **PAT(xlate per-session** 명령).	세션당 **PAT** 또는 다중 세션 **PAT** UI 경로: **Devices(**디바이스**)** > **FlexConfig**. 참조: FlexConfig 정책.	Secure Firewall Threat Defense 기본 구성에는 ASA와 동일한 사전 정의된 세션별 규칙이 포함되어 있습니다. 구성은 기본이 아닌 동작을 원하는 경우에만 필요합니다.
주소 및 포트 매핑 **(MAP)**	주소 및 포트 매핑**(MAP)** UI 경로: **Devices(**디바이스**)** > **FlexConfig**. 참조: FlexConfig 정책.	MAP(주소 및 포트 매핑)은 IPv4 주소를 IPv6로 변환하기 위한 통신사급 기능입니다.

애플리케이션 검사

Snort는 Secure Firewall Threat Defense 디바이스의 기본 검사 엔진입니다. 그러나 ASA 검사는 계속 실행되며 Snort 검사 전에 적용됩니다.

Snort는 많은 HTTP 검사를 수행하므로 ASA HTTP 검사 엔진은 전혀 지원되지 않으며 구성할 수도 없습니다.

대부분의 ASA 검사 엔진은 기본 설정으로 기본적으로 활성화되어 있습니다. ASA 검사 엔진이 추가 구성을 지원하는 경우 FlexConfig(공유 정책)를 사용하여 설정을 구성해야 합니다. 둘 이상의 디바이

스에 동일한 설정을 사용하는 경우 검사 설정에 대한 단일 FlexConfig 정책을 생성하고 모든 해당 디바이스에 적용할 수 있습니다.

검사를 해제(또는 설정)해야 하는 경우 FlexConfig 대신 각 디바이스에 대해 디바이스 CLI의 **configure inspection** 명령을 사용할 수 있습니다. 그러나 가능한 모든 프로토콜 검사를 명령에서 사용할 수 있는 것은 아닙니다.

다음 표에는 다양한 ASA 검사 엔진이 나열되어 있으며, Secure Firewall Threat Defense 디바이스에서 기본적으로 활성화되어 있는 엔진이 나와 있습니다.

표 *11:* 애플리케이션 검사 기능

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
기본 인터넷 프로토콜 검사	인스펙션 UI 경로: **Devices(**디바이스**)** > **FlexConfig**. 참조: FlexConfig 정책.	다음은 지원되는 검사입니다. 굵은 텍스트는 검사가 기본 구성에서 활성화되어 있음을 나타냅니다. • DCERPC • **DNS** • **FTP** • **ICMP** • **ICMP Error** • ILS • **IP Options** • IPsec Pass Through • IPv6 • Lisp • **NetBIOS** • PPTP • **RSH** • SMTP/ESMTP • **SNMP** • **SQL*Net** • **Sun RPC** • **TFTP** • WAAS • XDMCP • VXLAN 지원되지 않음(Snort에서 수행): HTTP, IM(인스턴트 메시징)

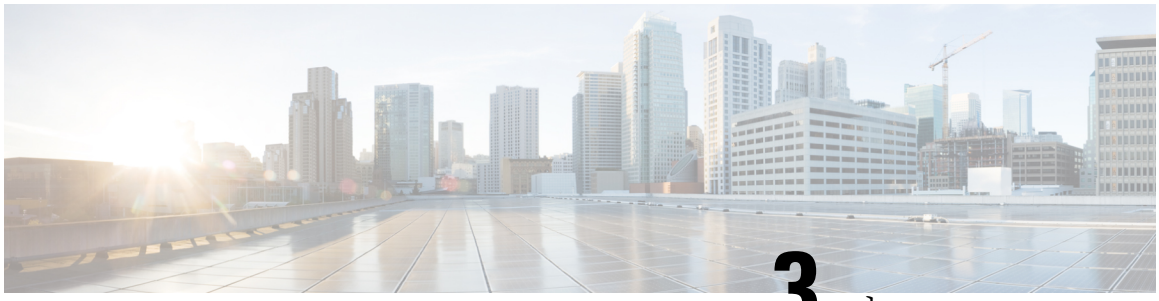
ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
음성 및 비디오 프로토콜에 대한 검사	인스펙션 UI 경로: **Devices(**디바이스**)** > **FlexConfig**. 참조: FlexConfig 정책.	다음은 지원되는 검사입니다. 굵은 텍스트는 검사가 기본 구성에서 활성화되어 있음을 나타냅니다. • CTIQBE • **H.323 H.225** • **H.323 RAS** • MGCP • **RTSP** • **SIP** • **Skinny** • STUN
모바일 네트워크 검사.	인스펙션 UI 경로: **Devices(**디바이스**)** > **FlexConfig**. 참조: FlexConfig 정책.	다음은 지원되는 검사입니다. 이러한 검사에는 통신 사업자 라이선스가 필요합니다. 기본적으로 활성화되지 않습니다. • 배율 • GTP/GPRS • M3UA • SCTP • RADIUS 계정 관리(이 검사에는 통신 사업자 라이선스가 필요하지 않음)

서비스 정책, 연결 설정, 위협 탐지

다음 표에는 디바이스를 통과하는 연결의 일부 측면을 제어하는 느슨하게 관련된 기능이 나와 있습니다. 이러한 설정의 대부분에는 대부분의 경우 작동하는 기본값이 있습니다.

표 *12:* 서비스 정책, 연결 설정, 위협 탐지 기능

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
전역 시간 초과	전역 시간 초과 UI 경로: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**, **Timeouts(**시간 초과**)** 페이지. 참조: 플랫폼 설정	플랫폼 설정은 공유 정책입니다. 이러한 설정은 정책이 할당된 각 디바이스에 적용됩니다.
연결 설정에 대한 서비스 정책	위협 방어 서비스 정책 UI path(UI 경로): **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 정책을 수정하는 동안 **Advanced Settings(**고급 설정**)** 아래에서 **Threat Defense Service Policy(**위협 방어 서비스 정책**)**를 찾습니다. 참조: 서비스 정책.	이러한 설정에는 **TCP** 상태 우회, **TCP** 시퀀스 임의 설정, **TCP** 가로채기**, DCD(Dead Connection Detection)**, **TCP** 표준화, 트래픽 클래스당 일반 연결 제한 및 시간 초과가 포함됩니다. 위협 방어 서비스 정책은 하나 이상의 디바이스에 할당하는 공유 정책인 액세스 제어 정책의 일부로 정의됩니다. 특정 인터페이스로 제한하는 모든 규칙은 해당 인터페이스를 포함하는 디바이스에서만 구성됩니다. 전역 규칙은 액세스 제어 정책에 할당된 모든 디바이스에 적용됩니다.
QoS(Quality of Service)	**QoS(Quality of Service)** UI 경로: **Devices(**디바이스**)** > **QoS**. See: Quality of Service(서비스 품질).	QoS 정책은 공유되지만 정책의 각 규칙은 하나 이상의 인터페이스를 지정해야 합니다. 규칙이 디바이스의 인터페이스를 포함하는 경우에만 디바이스에 규칙이 구성됩니다.
위협 탐지 (**threat-detection** 명령).	위협 탐지 UI path(UI 경로): **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 정책을 수정하는 동안 **Advanced Settings(**고급 설정**)** 아래에서 **Threat Detection(**위협 탐지**)**을 찾습니다. 참조: 위협 탐지.	Secure Firewall Threat Defense 기능은 ASA 기능과 정확히 중복되지 않지만 새로운 기능을 포함합니다. FlexConfig를 사용하여 ASA 명령 버전을 배포할 수도 있습니다.



3 장

가상 프라이빗 네트워크 기능

이 장에서는 Secure Firewall Management Center를 사용하여 Secure Firewall Threat Defense에서 ASA Virtual Private Network 기능을 구성하기 위한 개괄적인 정보를 제공합니다.

사이트 대 사이트 VPN

표 *13:* 사이트 대 사이트 *VPN*

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
LAN-to-LAN IPsec	정책 기반 **VPN** UI 경로: **Devices(**디바이스**)** > **Site To Site(**사이트 간**)** > **Policy Based(**정책 기반**) (Crypto Map)**. 참조: 정책 기반 사이트 간 VPN 구성. 방법: 정책 기반 사이트 간 VPN 구성, 기존 사이트 간 VPN 구축에 대한 IKE 옵션 사용자 지정, 기존 사이트 간 VPN 구축에 대한 IPsec 옵션 사용자 지정, 기존 사이트 간 VPN에 대한 고급 설정 사용자 지정 사이트 간 VPN 구축	management center는 피어에서 VPN을 구성할 수 있는 단일 마법사를 제공합니다.
Virtual tunnel interface(VTI)	경로 기반 **VPN** UI 경로: **Devices(**디바이스**)** > **Site To Site(**사이트 간**)** > **Route Based (VTI)(**경로 기반**(VTI))** 참조: 라우트 기반 사이트 간 VPN 생성. 방법: 경로 기반 VPN(VTI) 생성, VTI에 대한 고정 경로 구성, VTI에 대한 BGP 라우팅 구성, VTI를 통한 암호화된 트래픽을 허용하는 액세스 제어 규칙 구성	동적 VTI를 사용하는 허브와 고정 VTI를 사용하는 스포크 간에 VPN을 생성하는 것은 마법사를 사용하는 management center에서 훨씬 쉽습니다. ASDM에는 마법사가 없습니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
Umbrella SASE	**Umbrella**에서 **SASE** 터널 구축 UI 경로: **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)** > +**SASE Topology(SASE** 토폴로지**)**. 참조: Umbrella에서 SASE 터널 구축.	
사이트 간 **VPN** 모니터링	사이트 간 **VPN** 모니터링 UI 경로: **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Site to Site VPN(**사이트 간 **VPN)** 참조: Monitor the Site-to-Site VPN(사이트 간 VPN 모니터링).	

원격 액세스 VPN

표 *14:* 원격 액세스 *VPN*

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
원격 액세스 **IPsec(IKEv2) VPN**	원격 액세스 **VPN** 정책 UI 경로: **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)** > **Policy Assignment(**정책 할당**)** > **VPN Protocols(VPN** 프로토콜**)** > **IPsec-IKEv2**. 참조 원격 액세스 VPN 연결 구성. 사용 방법: • RA(원격 액세스) VPN 연결을 위한 트래픽 필터링 구성 - RA VPN 연결에서 트래픽 필터링을 위한 확장 액세스 목록 생성, RA VPN 연결에서 트래픽 필터링을 위한 그룹 정책에 확장 액세스 목록 추가 • 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, 원격 액세스 VPN에 대한 LDAP 특성 맵 구성, SAML 단일 로그인 서버 개체 추가, 원격 액세스 VPN에 대한 Dynamic Access Policy 구성 VPN 액세스	management center에서 연결 프로파일 및 그룹 정책 개체를 구성하는 방법은 ASA에서와 동일하게 유지됩니다. 로컬 사용자 및 Active Directory/LDAP를 생성하려면 영역 개체를 생성해야 합니다. 영역은 management center와 사용자가 서버의 사용자 계정 간 연결을 의미합니다.
원격 액세스 **SSL VPN**	원격 액세스 **VPN** 정책 UI 경로: **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)** > **Policy Assignment(**정책 할당**)** > **SSL**. 참조 원격 액세스 VPN 연결 구성. 방법: 원격 액세스 VPN 구성	
VPN 로드 밸런싱	**VPN** 로드 밸런싱 UI 경로: 원격 액세스 VPN 정책을 편집합니다. **Advanced(**고급**)** > **Load Balancing(**로드 밸런싱**)**. 참조: VPN 로드 밸런싱 구성.	VPN 로드 밸런싱은 VPN 로드 밸런싱 그룹의 디바이스 간에 원격 액세스 VPN 트래픽을 균등하게 분산시키는 메커니즘입니다.

ASA 기능	**Secure Firewall Management Center**의 **Threat Defense** 기능	참고
Dynamic Access Policy	**Dynamic Access Policy** UI 경로: **Devices(**디바이스**)** > **Dynamic Access Policy**. 참조: Dynamic Access Policy. 방법: 원격 액세스 VPN에 대한 Dynamic Access Policy 구성.	VPN 환경의 역동성을 해결하는 권한 부여를 구성할 수 있습니다.
VPN 모니터링	원격 액세스 **VPN** 대시보드 UI 경로: **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Remote Access VPN(**원격 액세스 **VPN)** 참조: 원격 액세스 VPN 모니터링.	
Secure Client Hostscan	**VPN** 파일 개체 UI 경로: **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Secure Client File(**보안 클라이언트 파일**)** 참조: 파일 개체.	
Secure Client 사용자 지정 속성	**Secure Client** 사용자 지정 속성 개체 UI 경로: **Objects** > **Object Management(**개체 관리**)** > **VPN** > **Custom Attribute(**사용자 지정 속성**)**. 보안 클라이언트 사용자 지정 속성 개체	