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 *1:* 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 *2: 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 *3:* 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 4: 서비스 정책, 연결 설정, 위협 탐지 기능

ASA 기능	Secure Firewall Management Center의 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.