Radware DefensePro 서비스 체인 빠른 시작 설명서

최초 게시일: 2016년 1월 27일

최종 업데이트: 2016년 3월 4일

1. Firepower 9300의 Radware DefensePro 서비스 체인 정보

Cisco FXOS 섀시에서는 단일 블레이드에서 여러 서비스(예: ASA 방화벽 및 서드파티 DDoS 애플리케이션)를 지원할 수 있습니다. 이러한 애플리케이션은 서비스 체인을 구성하기 위해 함께 연결될 수 있습니다. Firepower 9300의 FXOS(Firepower eXtensible Operating System) 1.1.4 이상에서는 서드파티 Radware DefensePro 가상 플랫폼을 ASA 방화벽 앞에서 실행하도록 설치할 수 있습니다. Radware DefensePro는 FXOS 섀시에서 DDoS(Distributed Denial-of-Service) 탐지 및 차단 기능을 제공하는 KVM 기반 가상 플랫폼입니다. 서비스 체인이 FXOS 섀시에서 사용되도록 설정된 경우, 네트워크의 인그레스 트래픽은 ASA 방화벽에 도달하기 전에 먼저 DefensePro 가상 플랫폼을 통과해야 합니다.

참고:

- Radware DefensePro 서비스 체인은 독립형 컨피그레이션 또는 ASA 방화벽이 있는 내장 섀시 클러스터링 컨피그레이션에서 활성화할 수 있습니다.
- DefensePro 애플리케이션은 최대 3개의 보안 모듈에서 별도의 인스턴스로 실행될 수 있습니다.
- Radware DefensePro 가상 플랫폼은 Radware vDP(가상 DefensePro) 또는 간단하게 vDP라고도 합니다.
- Radware DefensePro 애플리케이션은 경우에 따라 ASA 방화벽을 위한 링크 데코레이터라고도 합니다.

Firepower 9300의 Radware DefensePro 서비스 체인을 위한 라이센싱 요건

Firepower 9300의 Radware Virtual DefensePro 애플리케이션을 위한 라이센싱은 Radware APSolute Vision Manager를 통해 처리합니다. 디바이스에 맞는 처리량 라이센스를 주문하려면 CCW(Cisco Commerce Workspace)로 이동하십시오. 이 요청을 제출하고 나면 Radware Portal에 대한 로그인과 링크를 받게 됩니다. 여기에서 라이센스를 요청할 수 있습니다.

Radware의 APSolute Vision Manager 및 처리량 라이센싱 요건에 대한 자세한 정보는 Radware 사이트 (https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision)의 문서를 참조하십시오. 이 포털에 액세스하려면 Radware에 등록해야 합니다.

시간대 동기화 요건

Firepower 보안 어플라이언스에 Radware vDP를 구축하기 전에 etc/UTC 시간대와 함께 NTP 서버를 사용하도록 Chassis Manager를 설정해야 합니다.

절차

1. Firepower Chassis Manager에서 **Platform Settings(플랫폼 설정)**를 선택하여 **Platform Settings(플랫폼 설정)** 페이지에서 **NTP** 영역을 엽니다.
2. **Time Zone(시간대)** 드롭다운 목록에서 **etc/UTC**를 선택합니다.
3. **Set Time Source(시간 소스 설정)**에서 **Use NTP Server(NTP 서버 사용)**를 선택합니다.
4. **NTP Server(NTP 서버)** 필드에서 사용할 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다.
5. **Save(저장)**를 클릭합니다.

Firepower 섀시에서 날짜와 시간을 설정하는 데 대한 자세한 정보는 *Cisco FXOS CLI 환경 설정 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 환경 설정 가이드*(http://www.cisco.com/go/firepower9300-config)의 "날짜 및 시간 설정" 주제를 참조하십시오.

APSolute Vision Manager 버전 요건

Radware APSolute Vision은 vDP의 기본 관리 인터페이스입니다. APSolute Vision 관리자가 vDP와 Firepower 9300 서비스 체인 통합에서 제공하는 전체 기능을 지원하려면 APSolute Vision 버전 R3.40 이상이어야 합니다.

2. 서비스 체인에 Radware vDP 구축 및 구성

Firepower Chassis Manager를 사용하여 독립형 ASA 또는 ASA 클러스터에 Radware DefensePro 서비스 체인을 구축할 수 있습니다. 전체 CLI 절차에 대한 내용은 FXOS CLI 컨피그레이션 가이드를 참조하십시오.

시작하기 전에

Cisco.com에서 vDP 이미지를 다운로드한 다음 FXOS 섀시에 해당 이미지를 업로드합니다.

관리 인터페이스와 데이터 인터페이스를 구성합니다.

ASA 및 vDP 데코레이터의 구축 컨피그레이션에 포함할 수 있는 관리 프로그램의 관리 유형 인터페이스를 구성합니다. 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다.

절차

1. Firepower Chassis Manager에서 **Interface(인터페이스)**를 선택하여 인터페이스 페이지를 엽니다.
2. EtherChannel을 추가하려면 다음을 수행합니다.
   a. **Add Port Channel(포트 채널 추가)**를 클릭합니다.
   b. Port Channel ID(포트 채널 ID)에 1~47 사이의 값을 입력합니다.
   c. **Enable(사용)** 확인란이 선택된 상태로 둡니다.
   d. Type(유형)은 **Management(관리)** 또는 **Data(데이터)**를 선택합니다. 논리적 디바이스당 1개의 관리 인터페이스만 포함할 수 있습니다. **Cluster(클러스터)**는 선택하지 마십시오.

e. 원하는 멤버 인터페이스를 추가합니다.

f. **OK(확인)**를 클릭합니다.

3. 단일 인터페이스의 경우:

a. 인터페이스 행에서 **Edit(수정)** 아이콘을 클릭하여 Edit Interface(인터페이스 수정) 대화 상자를 엽니다.

b. **Enable(사용)** 확인란을 선택합니다.

c. Type(유형)은 **Management(관리)** 또는 **Data(데이터)**를 클릭합니다. 논리적 디바이스당 1개의 관리 인터페이스만 포함할 수 있습니다.

d. **OK(확인)**를 클릭합니다.

Radware DefensePro Service Chain으로 독립형 ASA 구축

절차

1. **Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
2. **Add Device(디바이스 추가)**를 클릭하여 Add Device(디바이스 추가) 대화 상자를 엽니다.
3. **Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다.
4. **Template(템플릿)**은 **asa**를 선택합니다.
5. **Image Version(이미지 버전)**은 ASA 소프트웨어 버전을 선택합니다.
6. **Device Mode(디바이스 모드)**는 **Standalone(독립형)** 라디오 버튼을 클릭합니다.
7. **OK(확인)**를 클릭합니다. Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.
8. **Data Ports(데이터 포트)** 영역을 확장하고 ASA에 할당할 각 인터페이스를 클릭합니다.
9. 화면 중앙의 디바이스 아이콘을 클릭합니다. **ASA Configuration(ASA 컨피그레이션)** 대화 상자가 나타납니다.
10. 프롬프트에 따라 구축 옵션을 구성합니다.
11. **OK(확인)**를 클릭하여 ASA Configuration(ASA 컨피그레이션) 대화 상자를 닫습니다.
12. Decorators(데코레이터) 영역에서 vDP를 선택합니다. **Radware: Virtual DefensePro - Configuration(Radware: 가상 DefensePro - 컨피그레이션)** 대화 상자가 나타납니다. **General Information(일반 정보)** 탭 아래에서 다음 필드를 구성합니다.
13. 하나 이상의 vDP 버전을 FXOS 섀시에 업로드한 경우, **Version(버전)** 드롭다운에서 사용할 버전을 선택합니다.
14. **Management Interface(관리 인터페이스)** 드롭다운에서 이 절차의 앞 부분에서 생성한 관리 인터페이스를 선택합니다.
15. 사용할 **Address Type(주소 유형)**을 IPv4 전용, IPv6 전용 또는 IPv4 및 IPv6 중에서 선택합니다.
16. 이전 단계의 **Address Type(주소 유형)** 선택에 따라 다음 필드를 구성합니다.
    a. **Management IP(관리 IP)** 필드에서 로컬 IP 주소를 구성합니다.
    b. IPv4 전용: **Network Mask(네트워크 마스크)**를 입력합니다.

       IPv6 전용: **Prefix Length(접두사 길이)**를 입력합니다.
    c. **Network Gateway(네트워크 게이트웨이)** 주소를 입력합니다.
17. vDP 데코레이터에 할당할 각 데이터 포트 옆에 있는 확인란을 클릭합니다. 선택하는 각 데이터 포트에서 모든 인그레스 트래픽이 ASA에 도달하기 전에 vDP 데코레이터를 먼저 통과합니다. 모든 이그레스 트래픽은 먼저 ASA를 통해 전송된 다음 vDP로 전송됩니다.

18. **OK(확인)**를 클릭합니다.
19. **Save(저장)**를 클릭합니다.

    FXOS 섀시에서는 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈로 푸시하여 논리적 디바이스 및 vDP 데코레이터를 구축합니다.

Radware DefensePro Service Chain으로 ASA 클러스터 구축

절차

1. **Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
2. **Add Device(디바이스 추가)**를 클릭하여 Add Device(디바이스 추가) 대화 상자를 엽니다.
3. **Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다.
4. **Template(템플릿)**은 **asa**를 선택합니다.
5. **Image Version(이미지 버전)**은 ASA 소프트웨어 버전을 선택합니다.
6. **Device Mode(디바이스 모드)**는 **Cluster(클러스터)** 라디오 버튼을 클릭합니다.
7. **Create New Cluster(새 클러스터 생성)** 라디오 버튼을 클릭합니다.
8. **OK(확인)**를 클릭합니다. Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.
9. **Data Ports(데이터 포트)** 영역을 확장하고 ASA에 할당할 각 인터페이스를 클릭합니다.
10. 화면 중앙의 디바이스 아이콘을 클릭합니다. **ASA Configuration(ASA 컨피그레이션)** 대화 상자가 나타납니다.
11. 프롬프트에 따라 구축 옵션을 구성합니다.
12. **OK(확인)**를 클릭하여 ASA Configuration(ASA 컨피그레이션) 대화 상자를 닫습니다.

    참고: **Management IP Pool(관리 IP 풀)** 필드에서 로컬 IP 주소의 풀을 구성합니다. 이 주소 중 하나는 하이픈으로 구분되는 시작 및 종료 주소를 입력하여 인터페이스의 각 클러스터 통합에 할당됩니다. 최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 기본 유닛에 속하는 **가상 IP 주소**(기본 클러스터 IP 주소라고 함)는 이러한 풀에 속하지 않습니다. 따라서 동일한 네트워크에서 가상 IP 주소에 대한 IP 주소를 예약해 두어야 합니다. IPv4 및/또는 IPv6 주소를 사용할 수 있습니다.
13. Decorators(데코레이터) 영역에서 **vDP**를 선택합니다. **Radware: Virtual DefensePro - Configuration(Radware: 가상 DefensePro - 컨피그레이션)** 대화 상자가 나타납니다. **General Information(일반 정보)** 탭 아래에서 다음 필드를 구성합니다.
14. 하나 이상의 vDP 버전을 FXOS 섀시에 업로드한 경우, **Version(버전)** 드롭다운에서 사용할 vDP 버전을 선택합니다.
15. **Management Interface(관리 인터페이스)** 드롭다운에서 관리 인터페이스를 선택합니다.
16. vDP 데코레이터에 할당할 각 데이터 포트 옆에 있는 확인란을 클릭합니다. 선택하는 각 데이터 포트에서 모든 인그레스 트래픽이 ASA에 도달하기 전에 vDP 데코레이터를 먼저 통과합니다. 모든 이그레스 트래픽은 먼저 ASA를 통해 전송된 다음 vDP로 전송됩니다.
17. **Interface Information(인터페이스 정보)** 탭을 클릭합니다.
18. 사용할 **Address Type(주소 유형)**을 IPv4 전용, IPv6 전용 또는 IPv4 및 IPv6 중에서 선택합니다.
19. 각 보안 모듈에 대해 다음 필드를 구성합니다. 표시되는 필드는 이전 단계의 **Address Type(주소 유형)** 선택에 따라 결정됩니다.
    a. **Management IP(관리 IP)** 필드에서 로컬 IP 주소를 구성합니다.
    b. IPv4 전용: **Network Mask(네트워크 마스크)**를 입력합니다.

       IPv6 전용: **Prefix Length(접두사 길이)**를 입력합니다.
    c. **Network Gateway(네트워크 게이트웨이)** 주소를 입력합니다.

20. **OK(확인)**를 클릭합니다.
21. **Save(저장)**를 클릭합니다.

    FXOS 섀시에서는 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈로 푸시하여 논리적 디바이스 및 vDP 데코레이터를 구축합니다.

DefensePro 인스턴스가 클러스터에 구성되었는지 확인

ASA 클러스터에 vDP 애플리케이션 인스턴스를 설치한 후 DefensePro 인스턴스가 클러스터에 구성되었는지 확인해야 합니다.

절차

1. **Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
2. 구성된 논리적 디바이스 목록을 vDP에 대한 항목으로 스크롤합니다. 해당 특성이 **Management IP(관리 IP)** 열에 나열되어 있는지 확인합니다.
   - **CLUSTER-ROLE** 요소가 DefensePro 인스턴스에 대해 unknown으로 표시되는 경우, DefensePro 애플리케이션을 시작하고 vDP 클러스터 생성을 완료하도록 마스터 IP 주소를 구성합니다. 이 작업을 수행하려면 아래 **Cluster the vDP Application Instances(vDP 애플리케이션 인스턴스 클러스터링)**에 자세히 설명된 절차를 따르십시오.
   - **CLUSTER-ROLE** 요소가 DefensePro 인스턴스에 대해 primary 또는 secondary로 표시되는 경우, 애플리케이션이 온라인 상태로 클러스터에서 형성됩니다.

vDP 애플리케이션 인스턴스 클러스터링

ASA 클러스터에 vDP 인스턴스를 설치한 후 vDP 인스턴스를 클러스터링할 vDP CLI를 입력해야 합니다. 독립형 컨피그레이션에서 vDP 서비스 체인을 설정한 경우 이 단계를 수행하지 않아도 됩니다.

절차

1. FXOS CLI에 연결합니다.
2. vDP 애플리케이션 인스턴스에 연결합니다.

   ```
   connect module slot console
   connect vdp
   ```

3. 지정된 사용자 이름과 비밀번호(radware/radware)를 사용하여 DefensePro 애플리케이션 인스턴스에 로그인합니다.
4. FXOS 플랫폼에서 vDP 인스턴스에 할당한 클러스터 IP를 표시합니다.

   ```
   device clustering management-channel ip
   ```

5. 할당된 이 IP에 마스터 IP를 설정합니다.

   ```
   device clustering set master ip
   ```

6. 클러스터 상태를 사용하도록 설정합니다.

   ```
   device clustering state set enable
   ```

7. vDP 애플리케이션을 종료하고 FXOS CLI로 돌아갑니다.

   ```
   Ctrl ]
   ```

8. 다음 vDP 애플리케이션 인스턴스에 연결합니다.

   ```
   connect module slot_2 console
   connect vdp
   ```

9. 이 절차의 4단계와 5단계에서 찾아 할당한 클러스터 IP로 마스터 IP를 설정합니다.

   device clustering set *master ip*

10. 클러스터 상태를 사용하도록 설정합니다.

    device clustering state set enable

11. vDP 애플리케이션을 종료하고 FXOS CLI로 돌아갑니다.

    Ctrl]

12. 세 번째 vDP 애플리케이션 인스턴스에서 8~11단계를 반복합니다(적용 가능한 경우). 세 개의 vDP 인스턴스 모두에 대한 마스터 IP를 구성하고 나면 첫 번째 인스턴스에 기본이 지정되고 나머지 두 인스턴스에 클러스터의 보조 클러스터 역할이 할당됩니다.

13. 클러스터가 구성되었는지 확인합니다.

    device clustering show

14. vDP 애플리케이션 콘솔을 종료하고 FXOS 모듈 CLI로 돌아갑니다.

    Ctrl]

3. vDP 웹 서비스 사용

APSolute Vision에서 FXOS 섀시에 구축된 가상 DefensePro 애플리케이션을 관리하려면 vDP 웹 인터페이스를 사용하도록 설정해야 합니다.

절차

1. FXOS CLI에서 vDP 애플리케이션 인스턴스에 연결합니다.

   connect module *slot* **console**
   connect vdp

2. 지정된 사용자 이름과 비밀번호(radware/radware)를 사용하여 DefensePro 애플리케이션 인스턴스에 로그인합니다.

3. vDP 웹 서비스 사용

   manage secure-web status set enable

4. vDP 애플리케이션 콘솔을 종료하고 FXOS 모듈 CLI로 돌아갑니다.

   Ctrl]

4. UDP/TCP 포트 열기

Radware APSolute Vision Manager 인터페이스는 다양한 UDP/TCP 포트를 사용하여 Radware vDP 애플리케이션과 통신합니다. vDP 애플리케이션이 APSolute Vision Manager와 통신하려면 이러한 포트에 액세스 가능하며 방화벽으로 인해 차단되지 않는지 확인해야 합니다. 열려는 특정 포트에 대한 자세한 내용은 APSolute Vision 사용 설명서의 다음 표를 참조하십시오.

- **APSolute Vision Server-WBM 통신 및 운영 체제에 대한 포트**
- **Radware 디바이스를 사용하는 APSolute Vision Server의 통신 포트**

5. 다음으로 살펴볼 내용

- 모든 Firepower 9300 설명서를 참조해 주십시오.
- 모든 ASA/ASDM 설명서에 대한 링크는 Navigating the Cisco ASA Series Documentation에 있습니다.
- **DefensePro for Firepower 9300 사용 설명서** (http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html) 다운로드
- Radware의 APSolute Vision Manager에 대한 자세한 내용과 문서는 Radware 사이트의 문서 포털 (https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision)을 참조하십시오. 이 포털에 액세스하려면 Radware에 등록해야 합니다.

5. 다음으로 살펴볼 내용