SMB용 Cisco ASA with FirePOWER 통합 위협 방어 v1

최종 업데이트: 2015년 10월 28일

이 솔루션에 대한 정보

ATP(Advanced Threat Protection)가 필요한 중소기업, 중견기업 및 분산형 대기업은 지금까지 충분한 서비스를 제공받지 못했습니다. 이러한 조직은 기존 차세대 방화벽 또는 보안 기능이 떨어지는 UTM(Unified Threat Management) 솔루션 등 비용이 많이 들고 관리자에게 비실용적인 포인트 솔루션에 만족해야 했습니다.

새로운 Cisco ASA with FirePOWER Services인 5506-X, 5508-X 및 5516-X는 중소기업 및 중견기업을 위해 특별히 만들어진 NGFW 솔루션입니다. 이 솔루션은 방화벽, 애플리케이션 제어, NGIPS, URL 필터링, AMP(Advanced Malware Protection) 및 VPN을 비롯한 최고의 업계 선도적인 위협 차단 기능을 제공합니다. 탁월한 가시성과 제어력, 자동 위협 우선순위 지정으로, 다른 방식이었다면 직원들에게 큰 부담이 될 수 있는 시간을 효율적으로 관리할 수 있는 오탐(false-positive) 알림을 제공합니다. 또한 이 솔루션은 향상된 사고 대응 기능을 제공합니다. 이를 통해 치료 시간이 수 주에서 몇 시간으로 단축되었다는 고객 사례를 많이 듣습니다.

중소기업, 중견기업 및 지사도 이제 대기업에서만 가능했던 수준과 동일한 ATP(Advanced Threat Protection) 능력을 갖추게 되었습니다.

이러한 Cisco NGFW 모델은 중소기업과 중견기업을 위해 특별히 설계되었음은 물론, NSS Labs 2014 Next-Generation Firewall Security Value Map에서 최고의 보안 등급을 받은 5525-X와 5585-X를 포함한 기타 5500-X 제품군과 동일한 수준의 탁월한 위협 차단 기술을 제공합니다. 이러한 Cisco NGFW에는 싱글 인스턴스 구축을 위한 통합 온박스(on-box) 관리를 포함하며 필요할 경우 중앙 집중식 관리도 지원됩니다. 또한 통합 무선 액세스 포인트를 포함하는 5506W-X를 비롯해 산업 통제 및 핵심 인프라 환경을 지원하는 러기다이즈드(내구성 강화) 5506H-X 등을 갖추고 있습니다.

데모 정보

사전 구성된 본 데모에는 다음이 포함됩니다.

- 시나리오 1: 통합 위협 방어 심층 분석

요구 사항

아래의 표에는 사전 구성된 데모의 요구 사항이 요약되어 있습니다.

표 1. 요구 사항

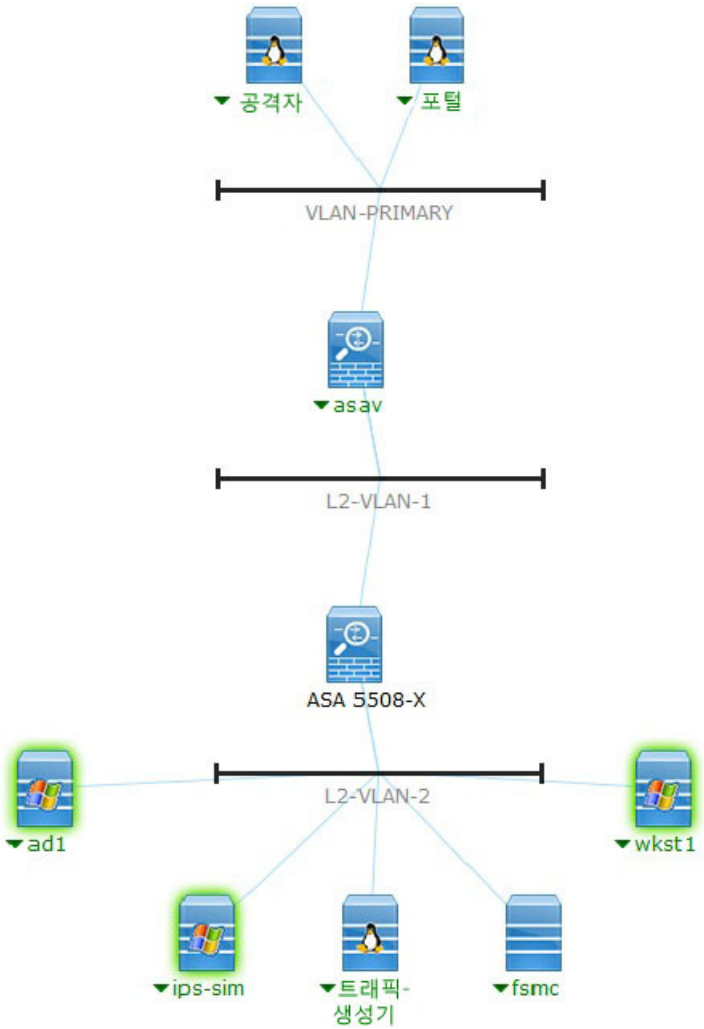
필수	선택 사항
• 랩톱	• Cisco AnyConnect

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

토폴로지

이 콘텐츠에는 사전 구성된 사용자 및 구성 요소가 포함되어 스크립팅된 시나리오와 솔루션의 기능을 보여줍니다. 대부분의 구성 요소는 사전 구성된 관리자 계정을 사용해 완전하게 구성할 수 있습니다. 액티브 세션 중 또는 이 작업이 필요한 시나리오 단계에서 **Topology(토폴로지)** 메뉴의 구성 요소 아이콘을 클릭해 구성 요소에 액세스하는 데 사용하는 IP 주소 및 사용자 계정 접속 정보를 볼 수 있습니다.

그림 1. 토폴로지



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

시작하기

프레젠테이션 전

실제 청중 앞에서 프레젠테이션하기 전에 이 문서를 검토하고 액티브 세션을 확인하는 것이 좋습니다. 이를 통해 문서 및 콘텐츠의 구조에 더욱 익숙해질 수 있습니다.

준비는 성공적인 프레젠테이션의 핵심입니다.

아래의 단계를 따라 콘텐츠의 세션을 예약하고 프레젠테이션 환경을 구성합니다.

1. dcloud.cisco.com으로 이동해 가장 가까운 위치를 선택한 후 Cisco.com접속 정보를 사용하여 로그인합니다.
2. 세션을 예약합니다. [방법 보기]
3. dCloud가 있는 라우터를 처음 사용한다면 이 라우터를 등록하고 구성합니다. [방법 보기]
4. 연결을 테스트합니다. [방법 보기]
5. 세션의 상태가 **My Dashboard(내 대시보드) > My Sessions(내 세션)**에서 **Active(액티브)** 상태인지 확인합니다.

참고: 세션이 액티브 상태로 설정되는 데에는 최대 15분 정도가 소요될 수 있습니다.

6. **View(보기)**를 클릭하여 액티브 세션을 엽니다.
7. 최상의 성능을 위해서 **Cisco AnyConnect VPN**[방법 보기] 및 랩톱의 **로컬 RDP 클라이언트**[방법 보기]를 통해 워크스테이션에 연결합니다.
    - 워크스테이션 1: **198.19.10.36**, 사용자 이름: **administrator**, 비밀번호: **C1sco12345**

참고: Cisco dCloud Remote Desktop 클라이언트를 사용해서도 워크스테이션에 연결할 수 있습니다[방법 보기]. dCloud Remote Desktop 클라이언트는 최소한의 상호 작용을 통해 액티브 세션 액세스할 때 최상의 성능을 제공합니다. 그러나 수많은 사용자가 이 방법을 사용할 때 연결 및 성능 문제를 경험하고 있습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

시나리오 1. 통합 위협 방어 심층 분석

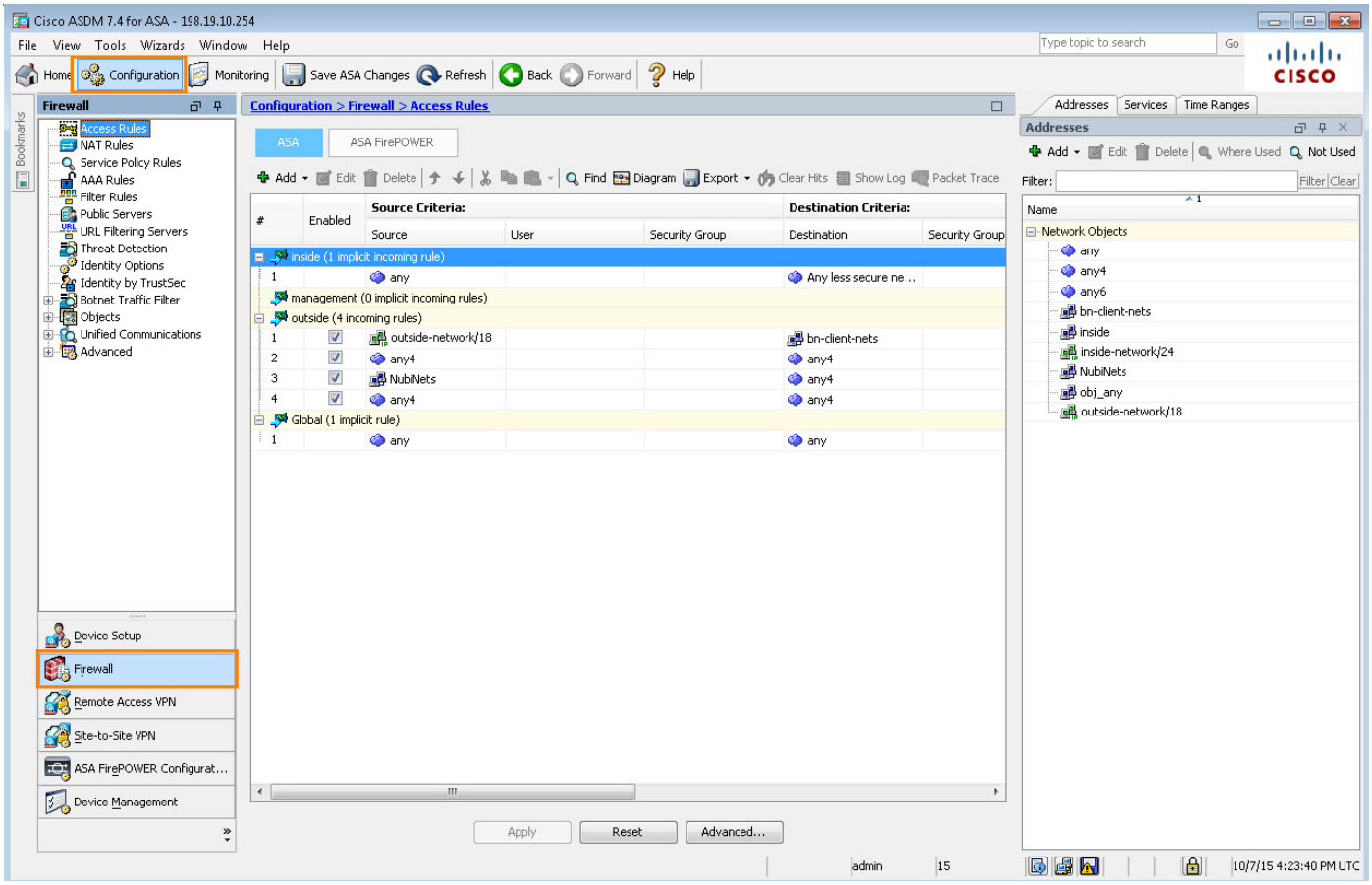
단계

서비스 정책 규칙

ASA 전역 검사 정책에 특정 서비스 정책 규칙을 적용하면 ASA에서 어떤 트래픽을 SFR 모듈로 전송할지 지정할 수 있습니다. 이 데모에서는 ASA를 통과하는 모든 트래픽을 추가 처리를 위해 SFR 모듈로 전송하는 ASA 컨피그레이션에 대해 알아봅니다.

1. RDP의 wkst1에 연결하고 사용자 ID **dcloud\administrator** 및 비밀번호 **C1sco12345**를 사용해 로그인합니다.
2. **Cisco ASDM-IDM Launcher** 아이콘을 선택합니다. 사용자 ID **admin** 및 비밀번호 **C1sco12345**를 사용해 로그인합니다.
3. **Configuration(컨피그레이션)**을 선택합니다.
4. 왼쪽 메뉴에서 **Firewall(방화벽)**을 선택합니다.

그림 2. 컨피그레이션 > 방화벽

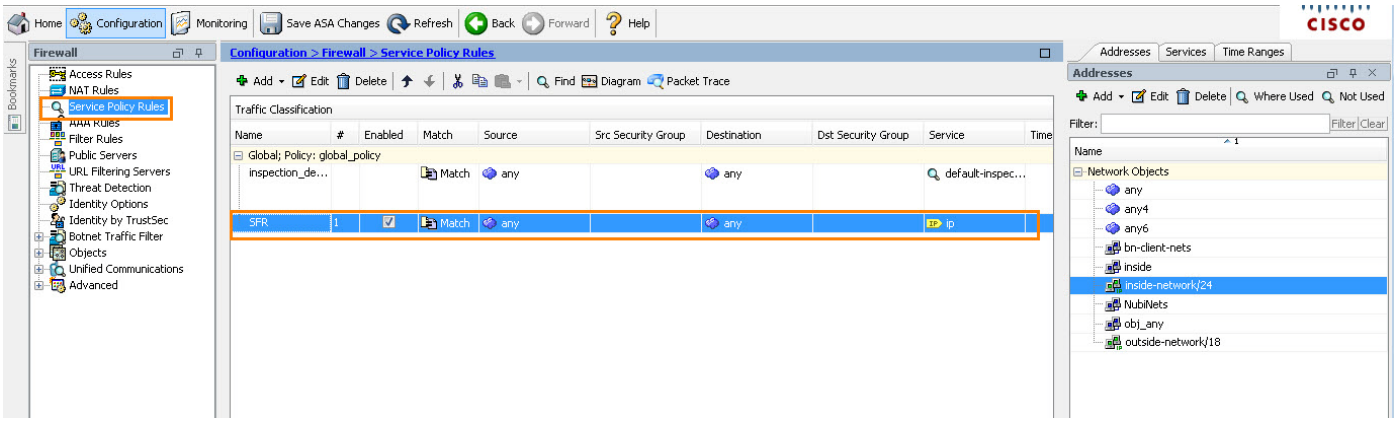


5. 왼쪽 메뉴에서 **Service Policy Rules(서비스 정책 규칙)**를 선택합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

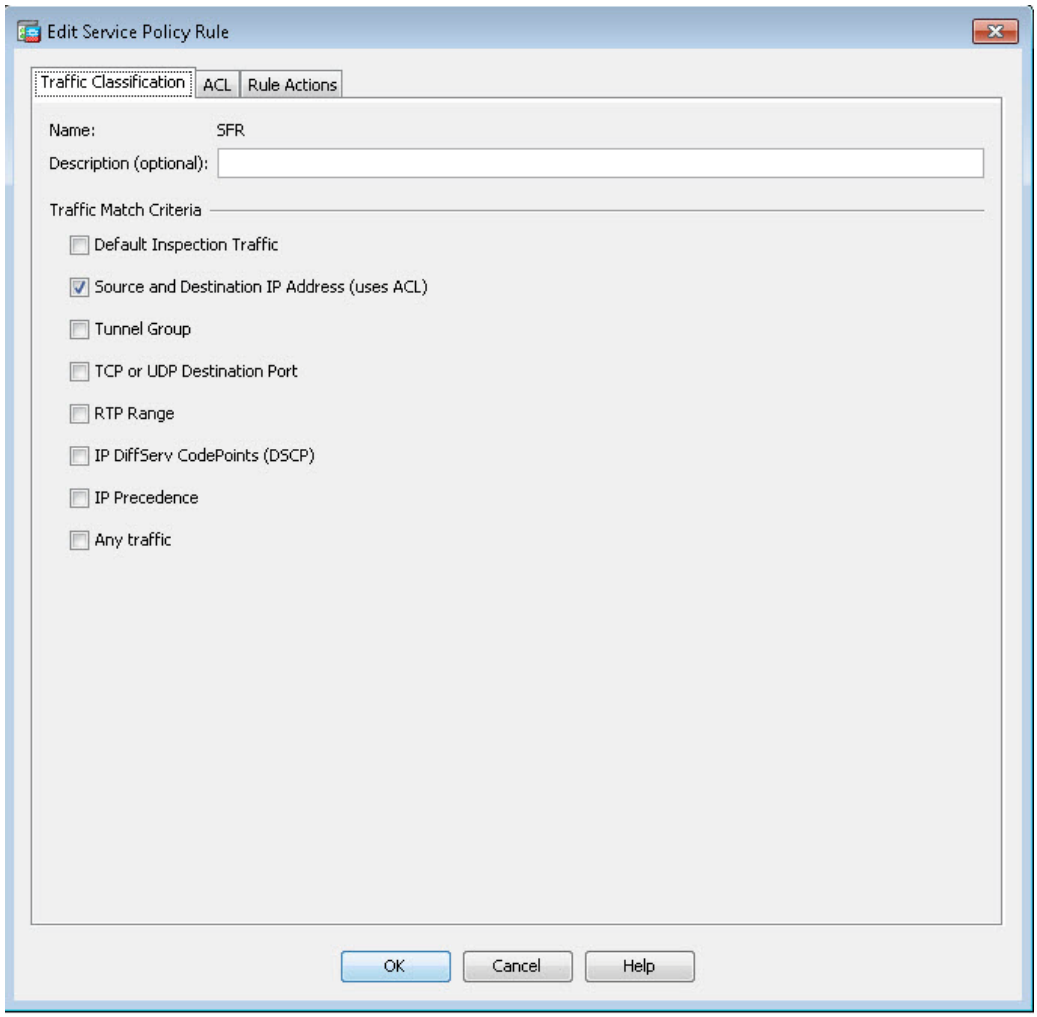
6. 목록에서 **SFR** 규칙을 더블 클릭합니다.

그림 3. 서비스 정책 규칙 > SFR



7. SFR 규칙은 ASA를 통과하는 트래픽을 추가 처리를 위해 SFR 모듈로 리디렉션하는 방법을 정의합니다.

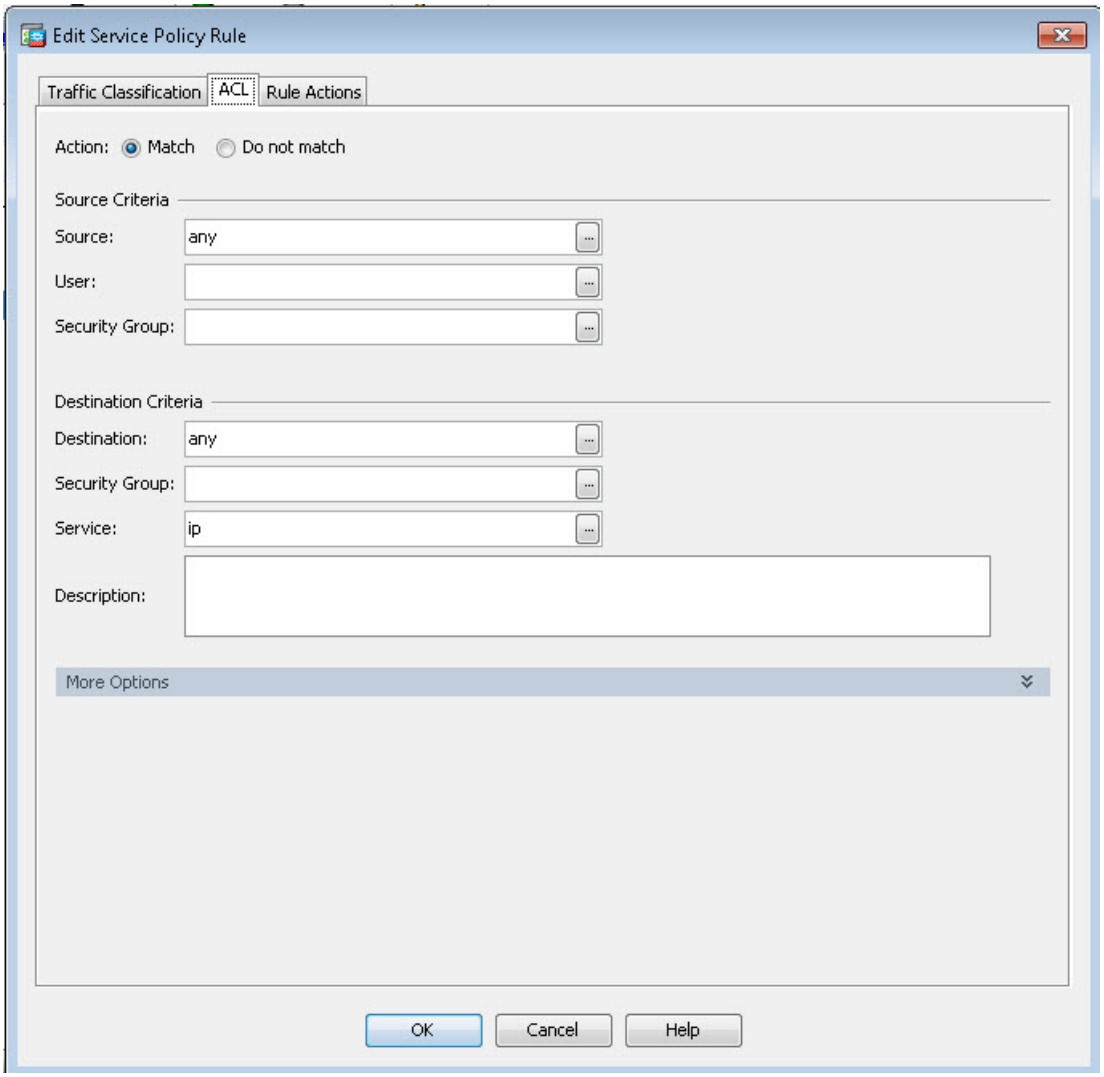
그림 4. SFR 규칙



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

8. **ACL 탭**을 클릭합니다. 이렇게 하면 액세스 제어 목록 옵션이 나열됩니다.

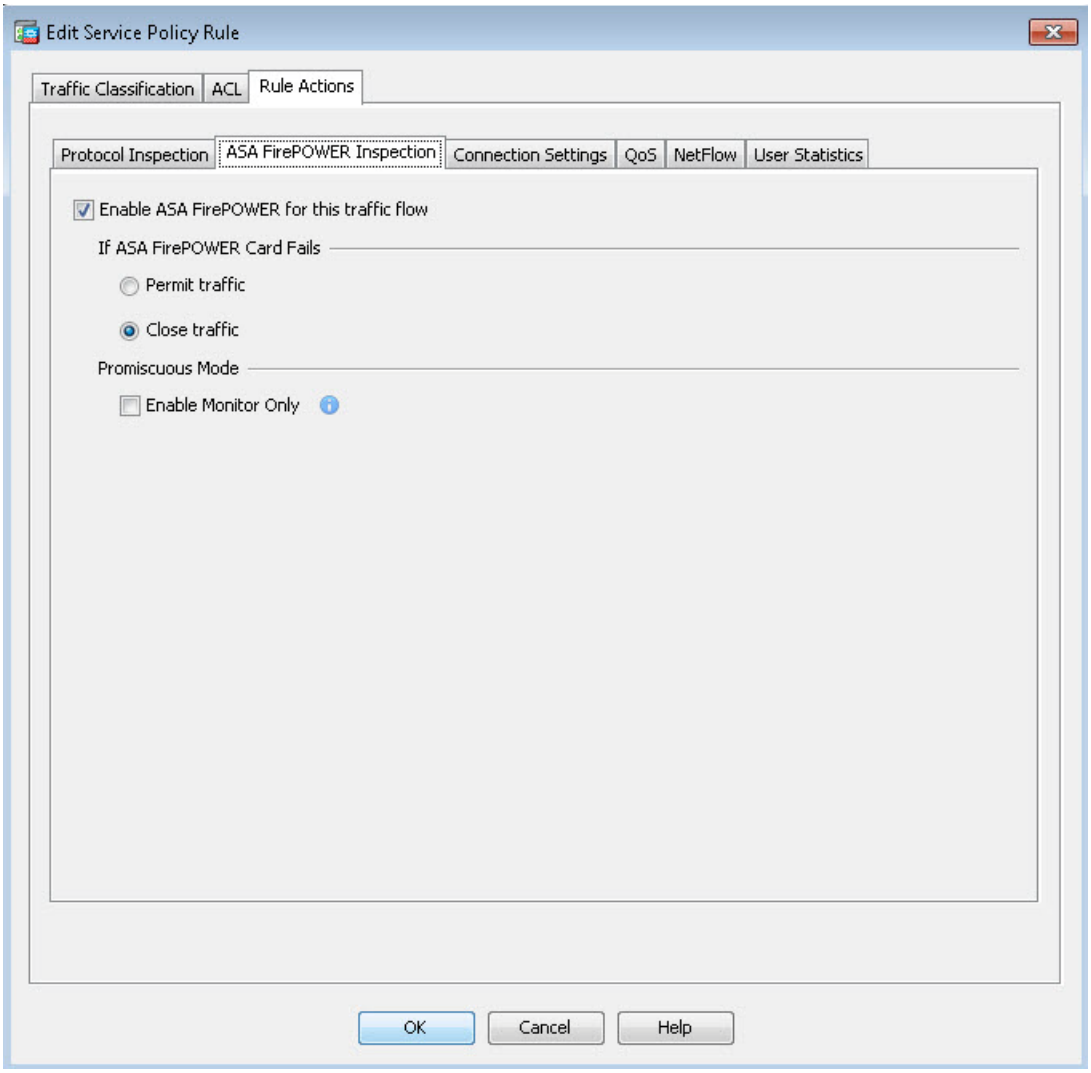
그림 5. ACL 탭



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

9. **Rule Actions(규칙 동작) 탭**을 클릭하고 **ASA FirePOWER Inspection(ASA FirePOWER 검사) 탭**을 클릭합니다.

그림 6. 규칙 동작 > ASA FirePOWER 검사



10. **Cancel(취소)**을 클릭하고 **ASDM** 창을 최소화합니다.

참고: 표시된 SFR 규칙은 ASA 전역 검사 정책의 일부입니다. 허용 IP와 매칭되는 모든 트래픽과 이 규칙에서 호출한 모든 ACL은 추가 처리를 위해 SFR 모듈로 리디렉션됩니다. 그다음 SFR 모듈은 해당 트래픽을 액세스 제어 정책, 침입 정책 또는 파일 정책 등에 통과시킵니다.

SFR 모듈은 FC(Fail Close) 상태로 구성됩니다. 이는 SFR 모듈이 응답하지 않게 되면 ASA가 어떤 트래픽도 전달하지 않는다는 것을 의미합니다. 조직에서 SFR 모듈 장애 시 어떠한 트래픽도 전달하지 않으므로 강화된 보안을 제공합니다. FO(Fail Open)는 이 모듈을 구성하는 대안 방식으로 같은 상황에서도 SFR 모듈이 없는 것처럼 ASA가 트래픽을 계속 전달하게 됩니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

위협 탐지

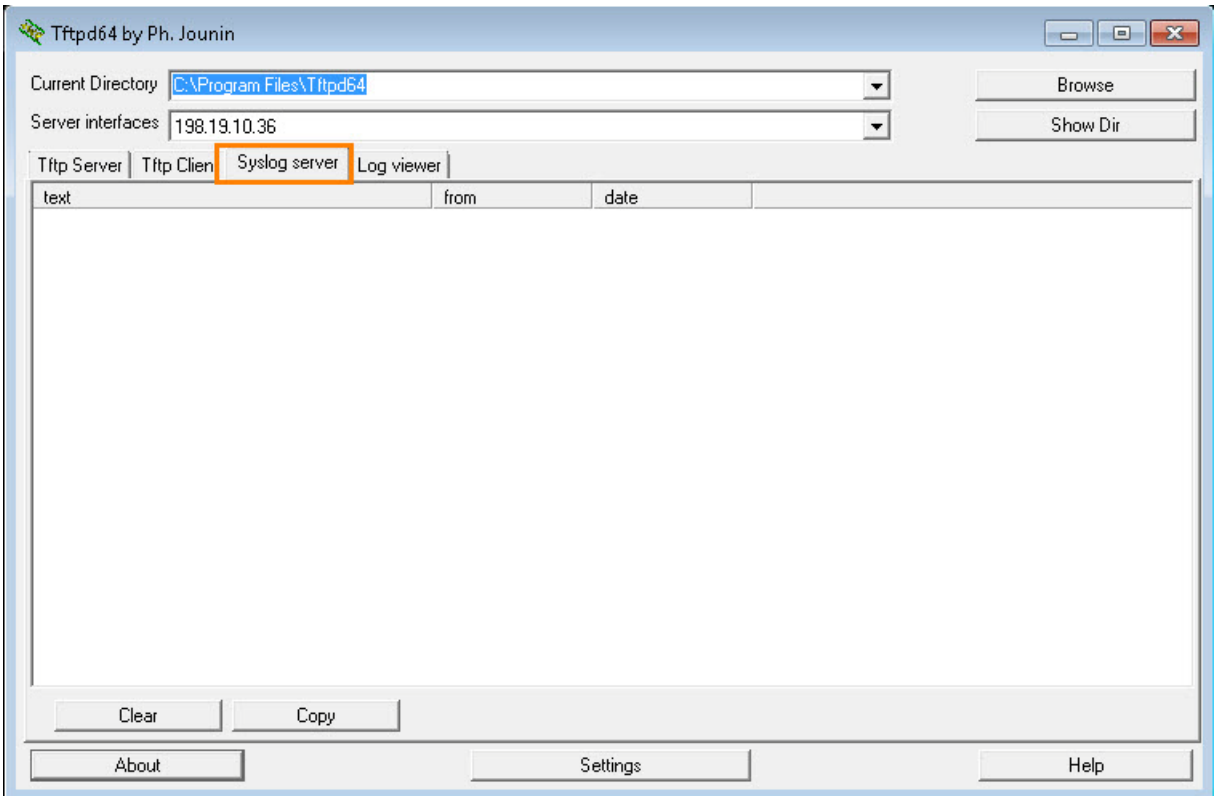
이 시나리오에서는 Microsoft Internet Explorer의 취약성을 악용하는 공격자 시스템에 서버 측 익스플로잇을 실행합니다. 익스플로잇을 쉽게 실행하려면, 데스크톱에서 스크립트를 실행하고 간단한 명령어를 입력합니다. 스크립트는 공격자 VM에 SSH 세션을 열고 익스플로잇 코드를 시작합니다. ips-sim VM은 공격자 웹 서버에 지속적으로 액세스를 시도하는 Windows 서버 설정이며 취약성을 공략하기 위해 계속 실행됩니다. ips-sim Internet Explorer 프로세스가 공격자에 연결되면, 공격자는 취약성을 악용합니다. 침입 이벤트는 SFR 모듈에서 탐지되며 syslog 메시지가 네트워크 관리자에게 전송됩니다.

1. 데스크톱에서 **Tftpd64** 아이콘을 더블 클릭합니다.

그림 7. Tftpd64

2. **Syslog Server(Syslog 서버)** 탭을 클릭합니다. 이 창에는 수신 이벤트가 표시됩니다. 이 창을 보이는 상태로 놔둡니다.

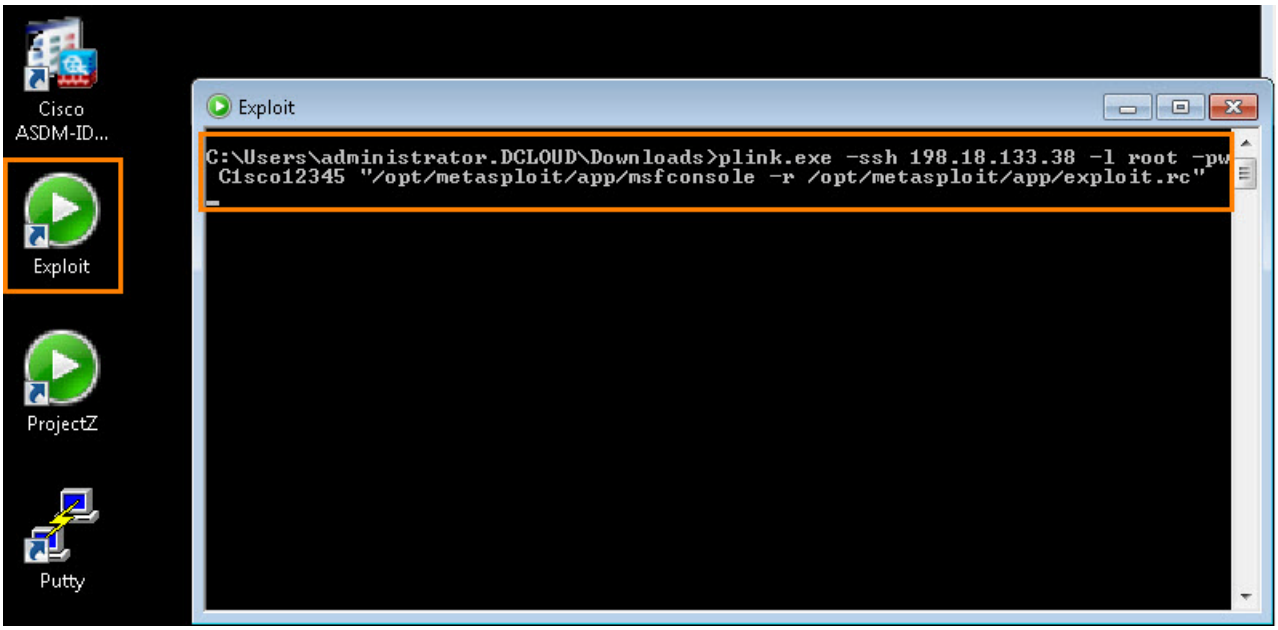
그림 8. Syslog 서버



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

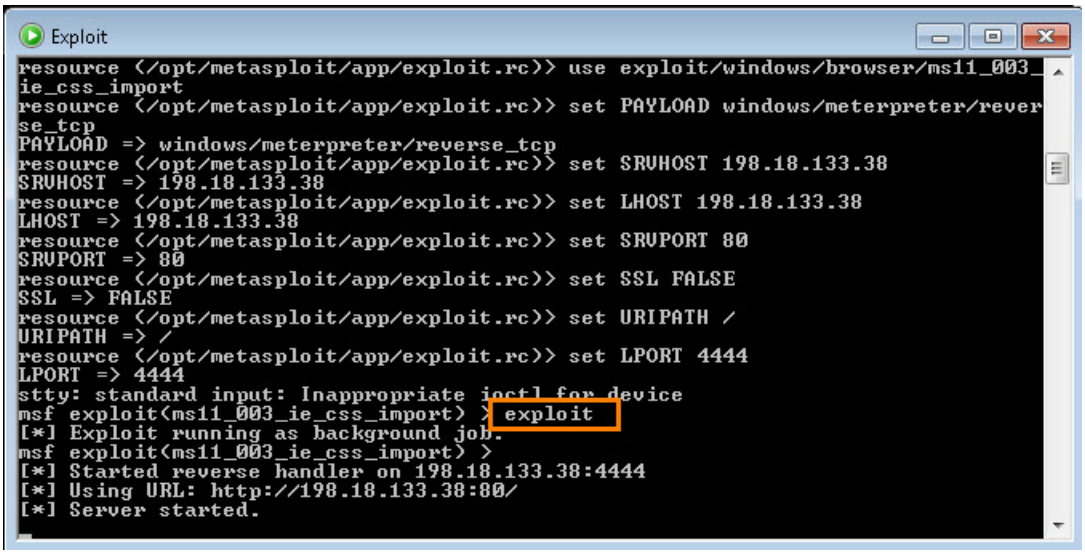
3. 데스크톱에서 Exploit(익스플로잇) 아이콘을 더블 클릭합니다. 공격자 Linux 상자로 연결되어 서버 측 익스플로잇이 실행되고, 방화벽에 경고가 트리거되고 해킹 이벤트를 시뮬레이션합니다. 스크립트가 완료될 때까지 잠시 기다린 후 프롬프트로 돌아옵니다.

그림 9. 익스플로잇



4. Exploit(익스플로잇) 창에 **exploit**을 입력하고 **Enter 키를 눌러** 서버 측 익스플로잇을 실행합니다.

그림 10. 익스플로잇 명령



5. **Syslog server(Syslog 서버) 탭**에 경고가 표시될 때까지 익스플로잇 창이 실행되게 합니다.

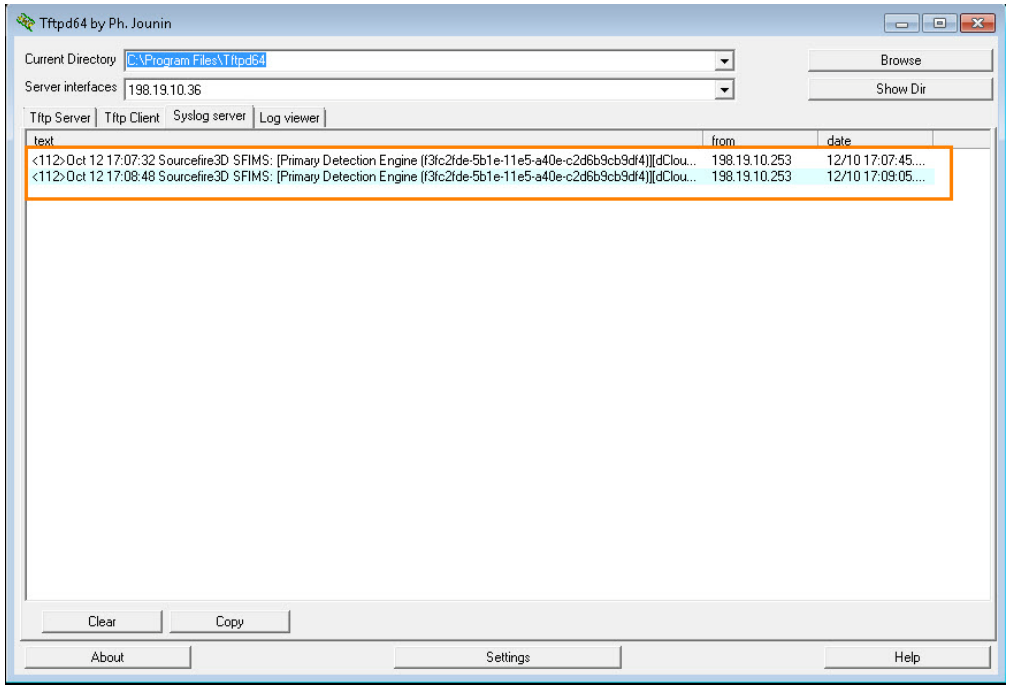
© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

6. SFR 모듈이 익스플로잇을 탐지하면 **syslog 메시지**를 전송하여 네트워크 관리자에게 경고합니다.

참고: 익스플로잇은 탐지되었으나 SFR 컨피그레이션의 IPS 규칙에는 현재 차단이 아닌 경고로 설정되어 있으므로 이 시점에서는 차단되지 않습니다. SFR 컨피그레이션을 인라인에서 익스플로잇을 차단하도록 변경합니다.

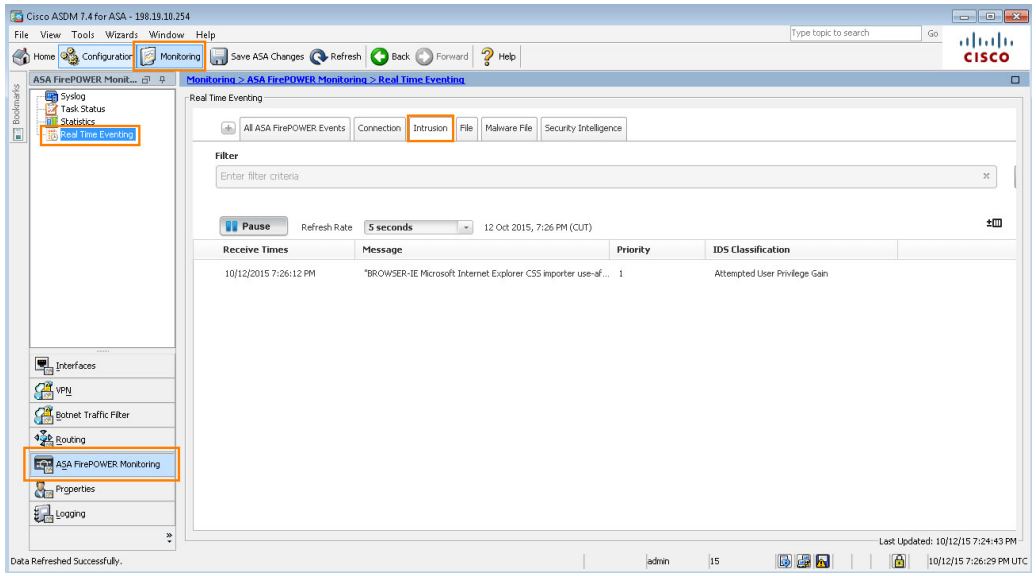
ASA는 예시로 syslog를 TFTPD64에 전송합니다. ASA는 내역 정보를 저장할 수 없으므로 외부 syslog 서버가 경고 및 보고에 사용될 수 있습니다.

그림 11. Syslog 서버와 탐지된 위협



7. **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Real Time Eventing(실시간 이벤트)**을 클릭하고 **Intrusion(침입) 탭**을 클릭합니다.

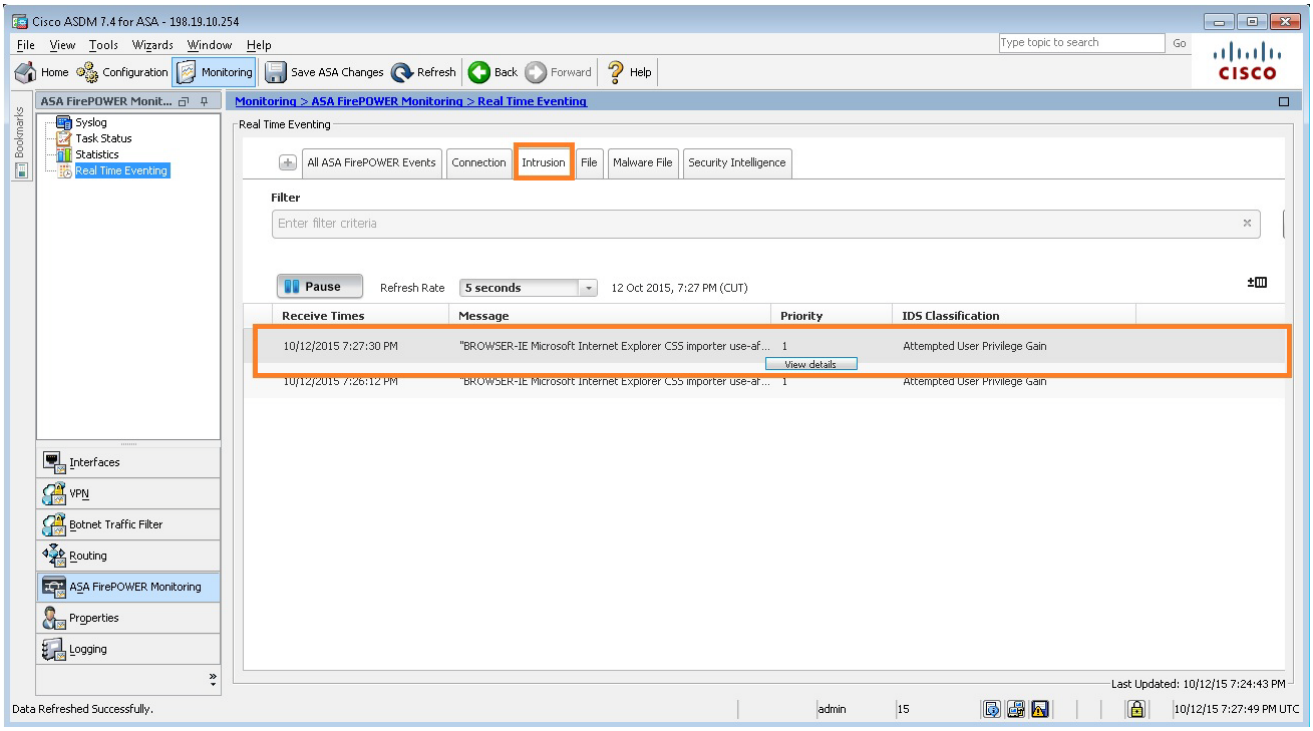
그림 12. 침입 탭



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

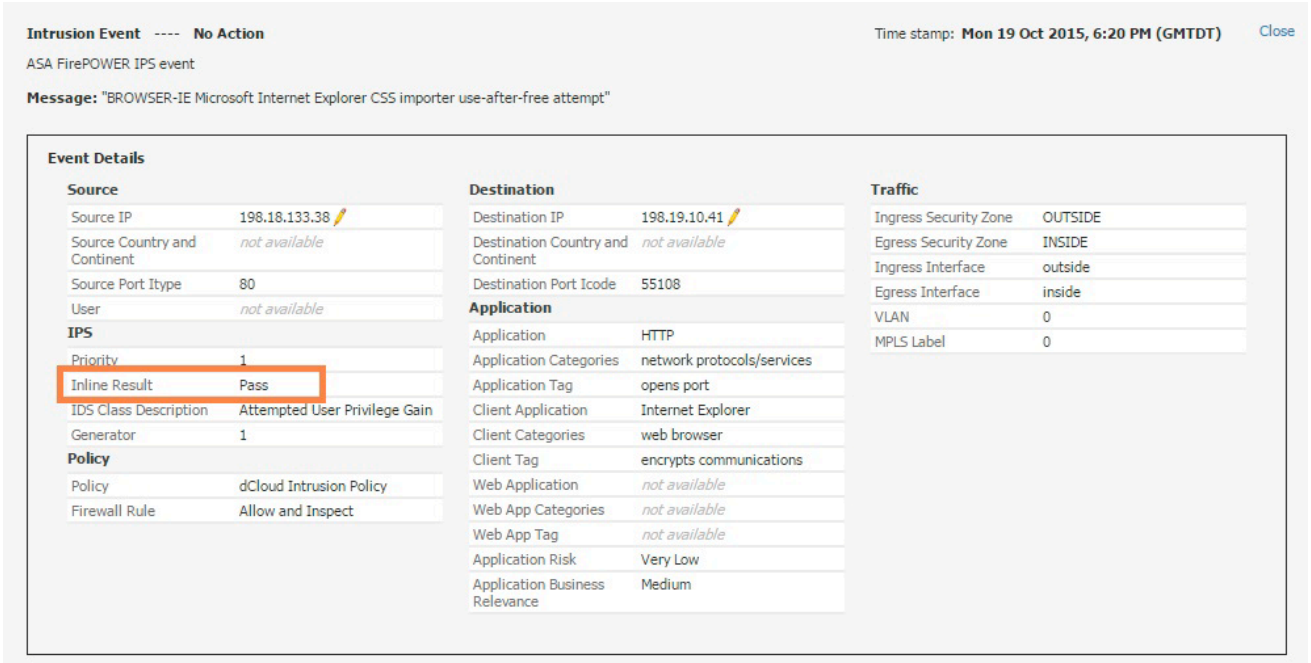
8. 최근 경고를 선택하고 **View Details(세부사항 보기)**를 클릭합니다.

그림 13. 침입 세부사항



9. **Inline Result(인라인 결과)**에 Pass(통과)라고 나타납니다.

그림 14. 인라인 결과 – 통과



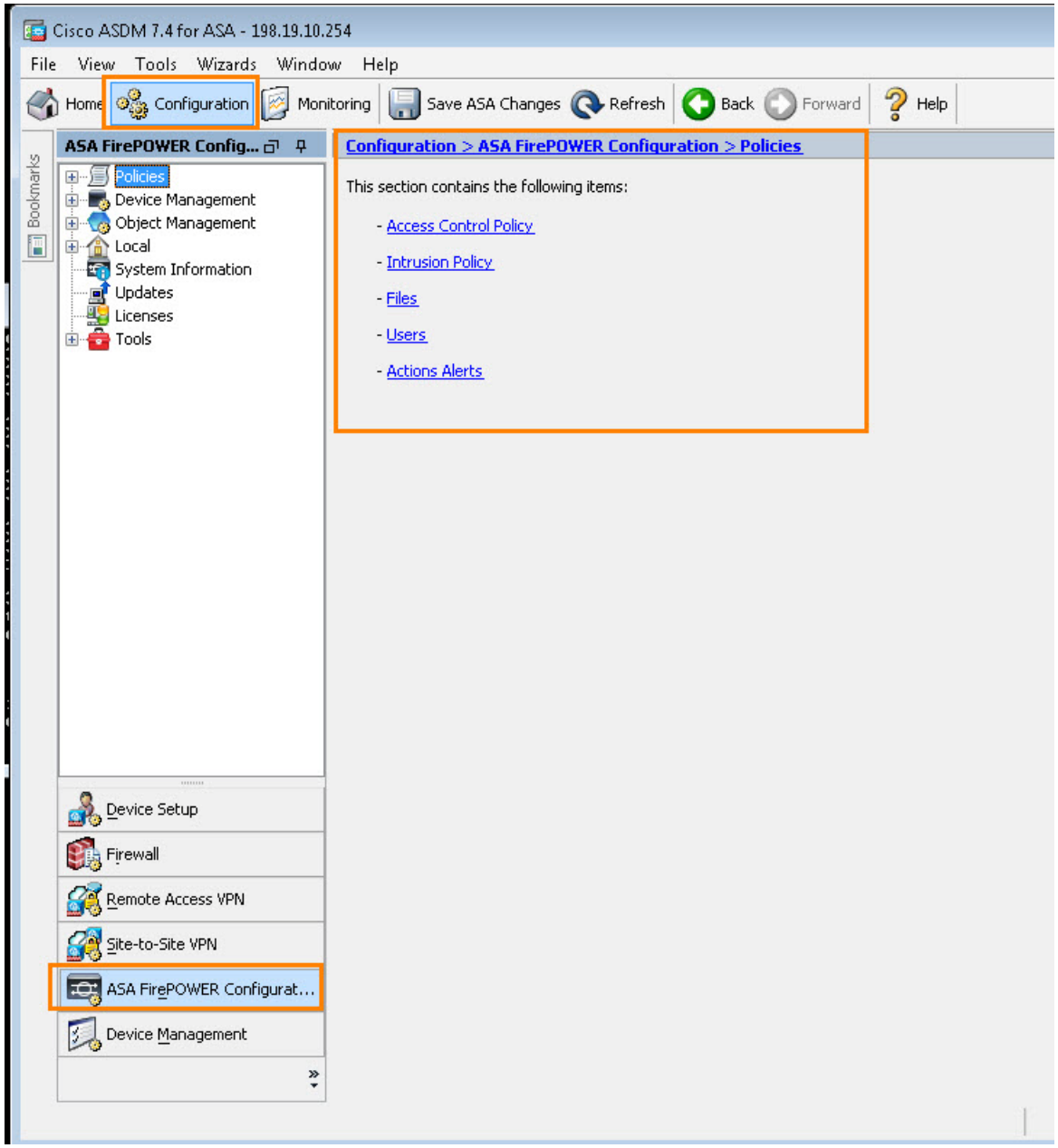
© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

위협 차단

마지막 섹션에서 익스플로잇은 탐지되었지만 아직 차단되지는 않았습니다. 이 섹션에서는 이 특정 익스플로잇으로 트리거되는 트래픽을 차단할 수 있도록 SFR IPS 정책을 수정합니다.

1. **ASDM** 창을 최대화합니다.
2. **Configuration(컨피그레이션)**을 클릭하고 **ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션)**을 클릭합니다.

그림 15. 컨피그레이션 > ASA FirePOWER 컨피그레이션

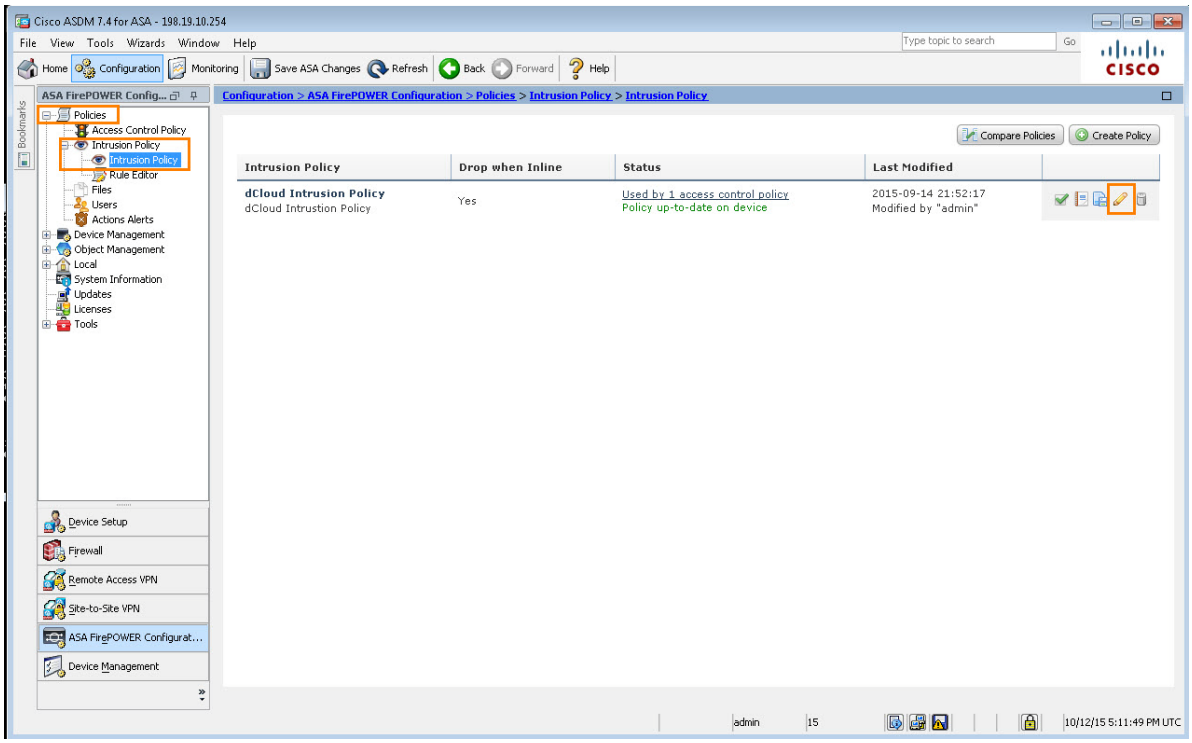


3. **Policies(정책) > Intrusion Policy(침입 정책) > Intrusion Policy(침입 정책)**를 클릭합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

4. **편집 아이콘(연필)**을 클릭합니다. 이렇게 하면 침입 정책을 변경할 수 있습니다.

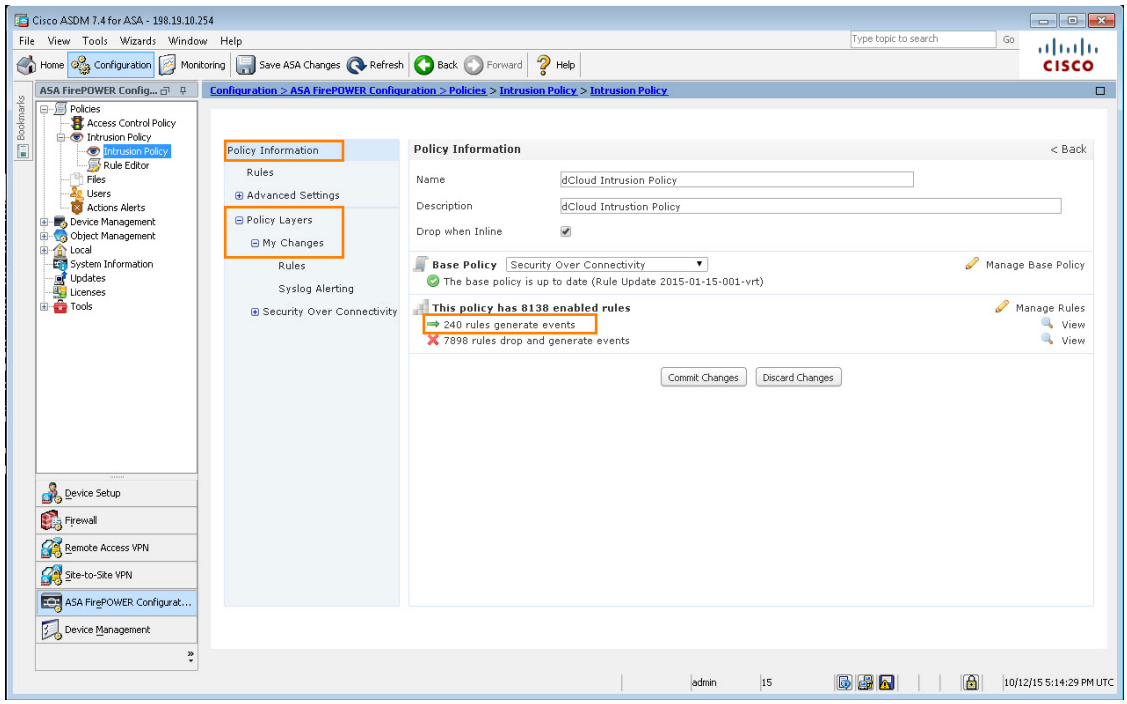
그림 16. 침입 정책 편집



5. **Policy Layers(정책 레이어) > My Changes(내 변경 사항)**를 클릭합니다.

6. 규칙 목록에서 녹색 화살표 옆에 있는 **xxx rules generate events(xxx 규칙 생성 이벤트)**를 클릭합니다.

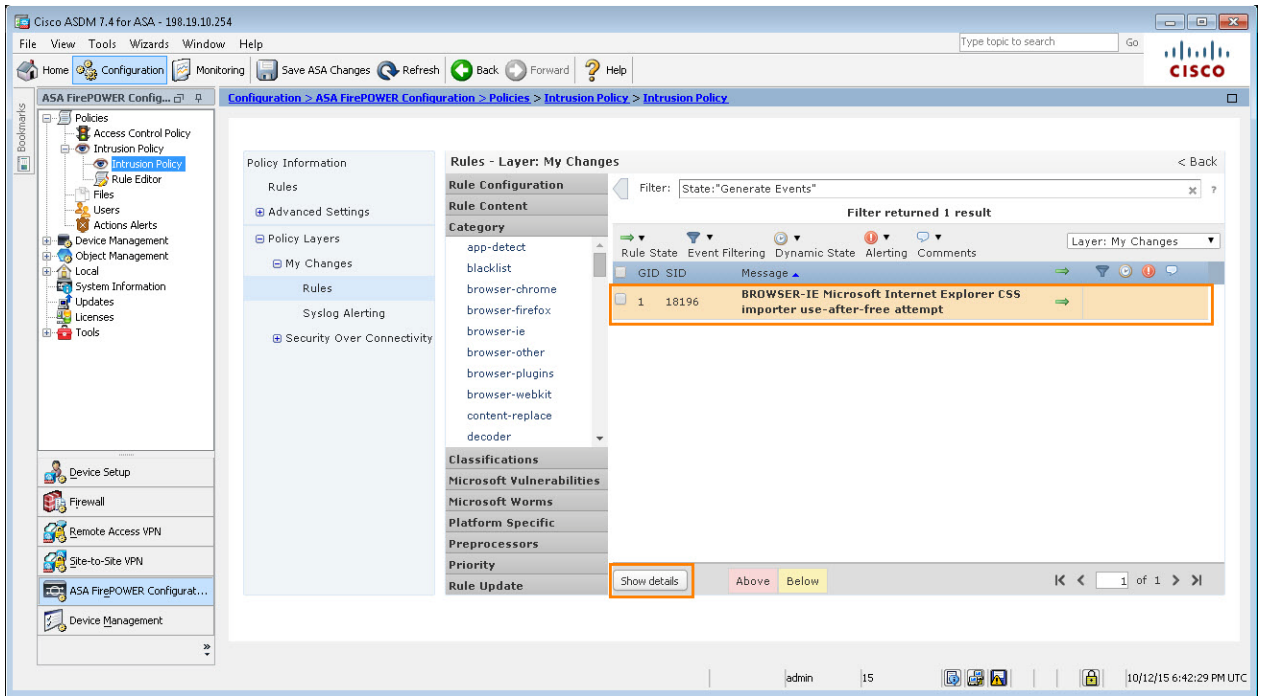
그림 17. 정책 레이어 > 내 변경 사항



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

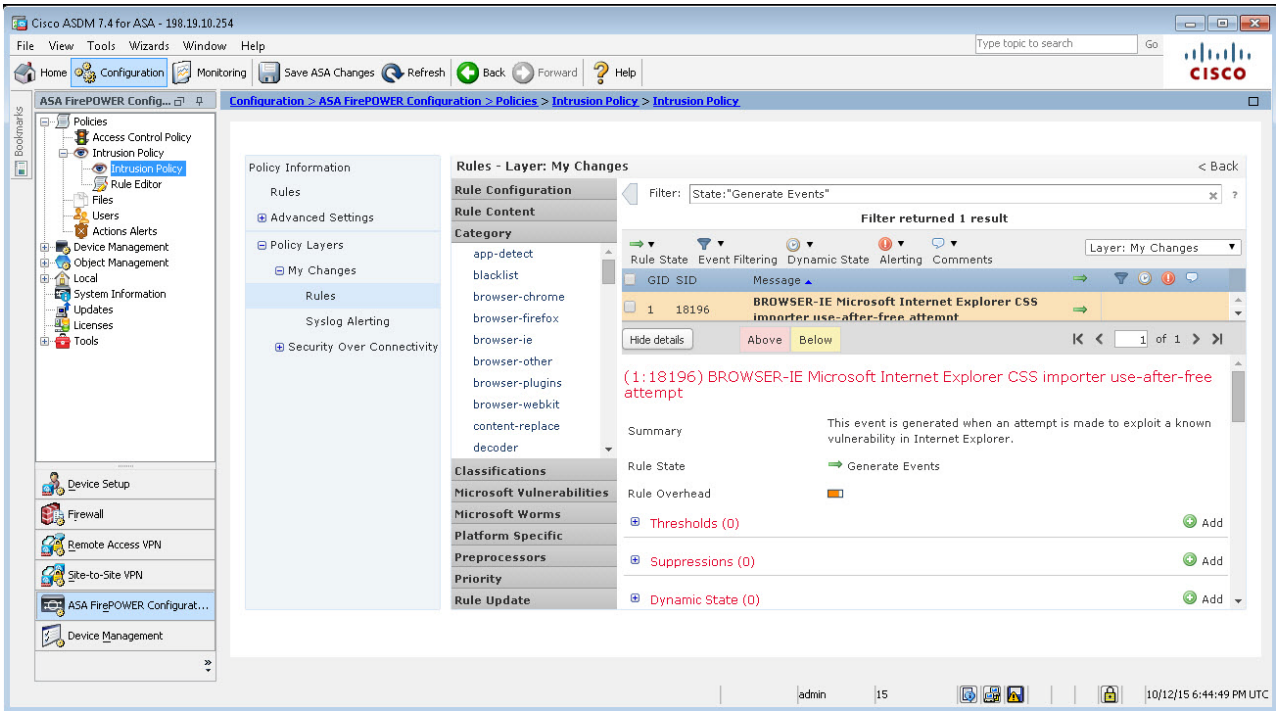
7. **BROWSER-IE Microsoft Internet Explorer CSS importer use-after-free attempt** 규칙을 클릭합니다.

그림 18. 규칙 레이어



8. 목록에서 규칙을 선택하고 **View Details(세부사항 보기)**를 클릭합니다.

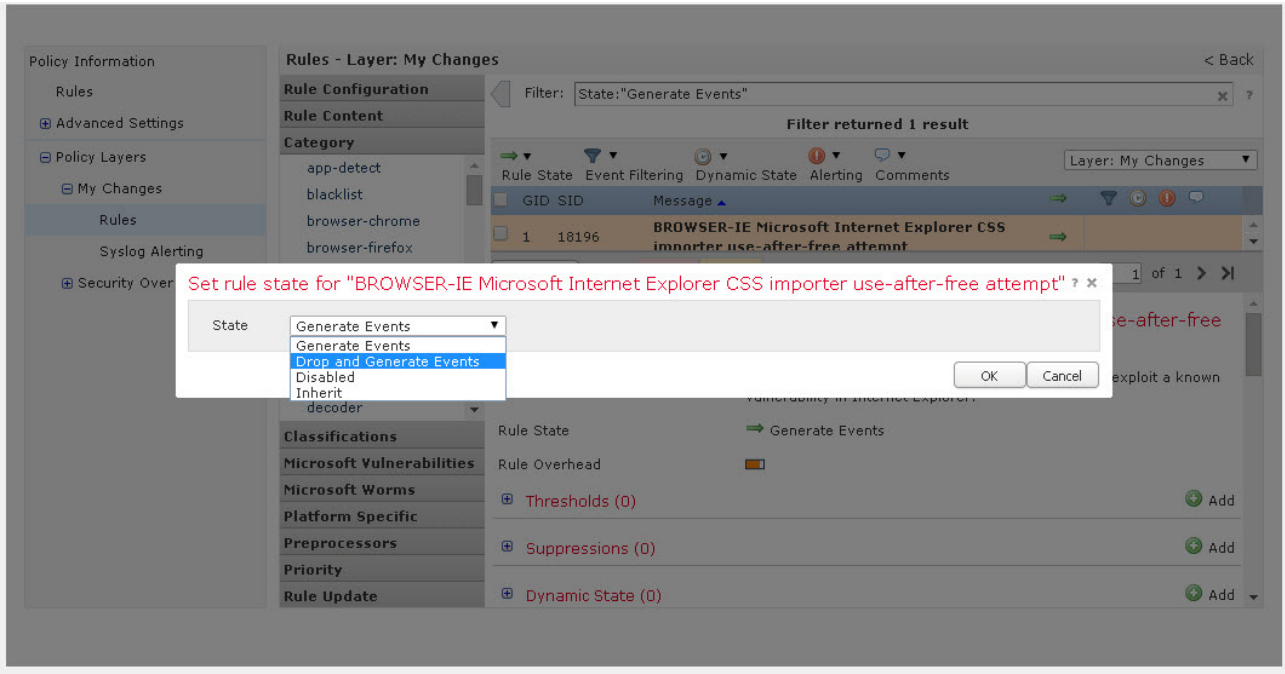
그림 19. 세부사항 보기



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

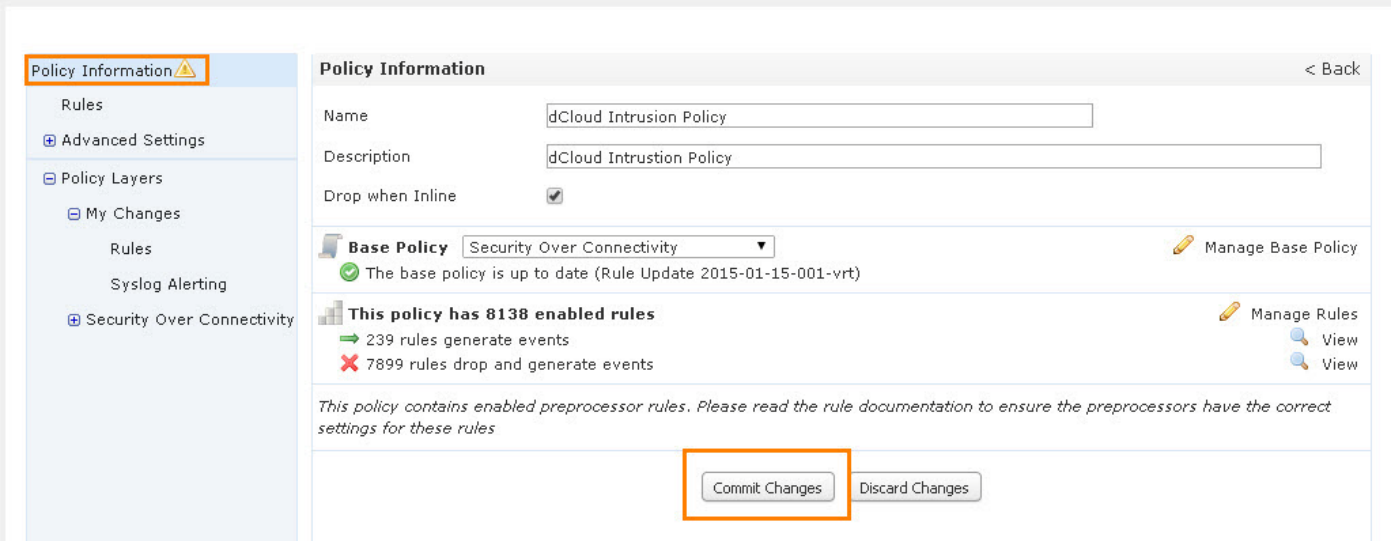
9. 규칙 동작이 이벤트 차단이 아닌 이벤트 생성으로 설정되었다고 나타납니다. 차단을 설정하려면 **Generate Events(이벤트 생성)**를 클릭합니다. Set Rule State(규칙 상태 설정) 창이 나타납니다.

그림 20. 규칙 상태 설정



10. 드롭다운 목록에서 **Drop and Generate Events(이벤트 삭제 및 생성)**를 선택합니다.
11. **OK(확인)**를 클릭합니다.
12. **OK(확인)**를 다시 클릭합니다.
13. **Policy Information(정책 정보)** 및 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

그림 21. 변경 사항 커밋



14. **OK(확인)**를 클릭해 저장을 확인합니다. 이렇게 하면 업데이트된 컨피그레이션이 저장됩니다.

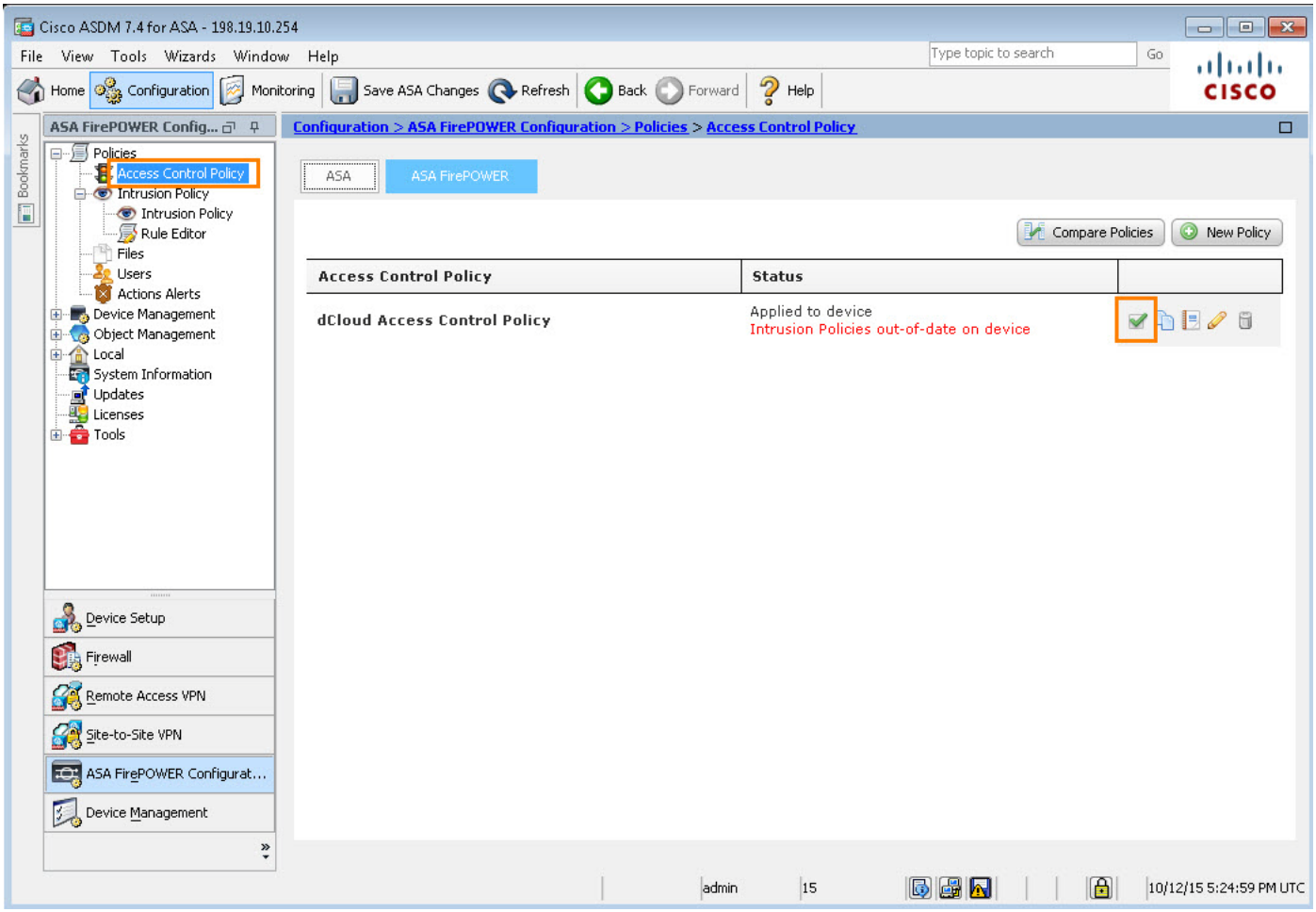
© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

정책 재적용

1. 왼쪽 메뉴에서 **Access Control Policy(액세스 제어 정책)**를 선택합니다.
2. Access Control Policy(액세스 제어 정책) 창에서, **녹색 확인 표시**를 클릭하고 **Apply All(모두 적용)**을 클릭해 정책을 적용합니다.

참고: 정책 상태가 만료에서 최신 상태로 적용 중으로 변경됩니다. 상태가 applied to device(디바이스에 적용됨)/Policy Up-to-date on device(디바이스에 최신 정책 적용됨)로 변경될 때까지 기다립니다. 이 작업에는 최대 5분이 소요될 수 있습니다.

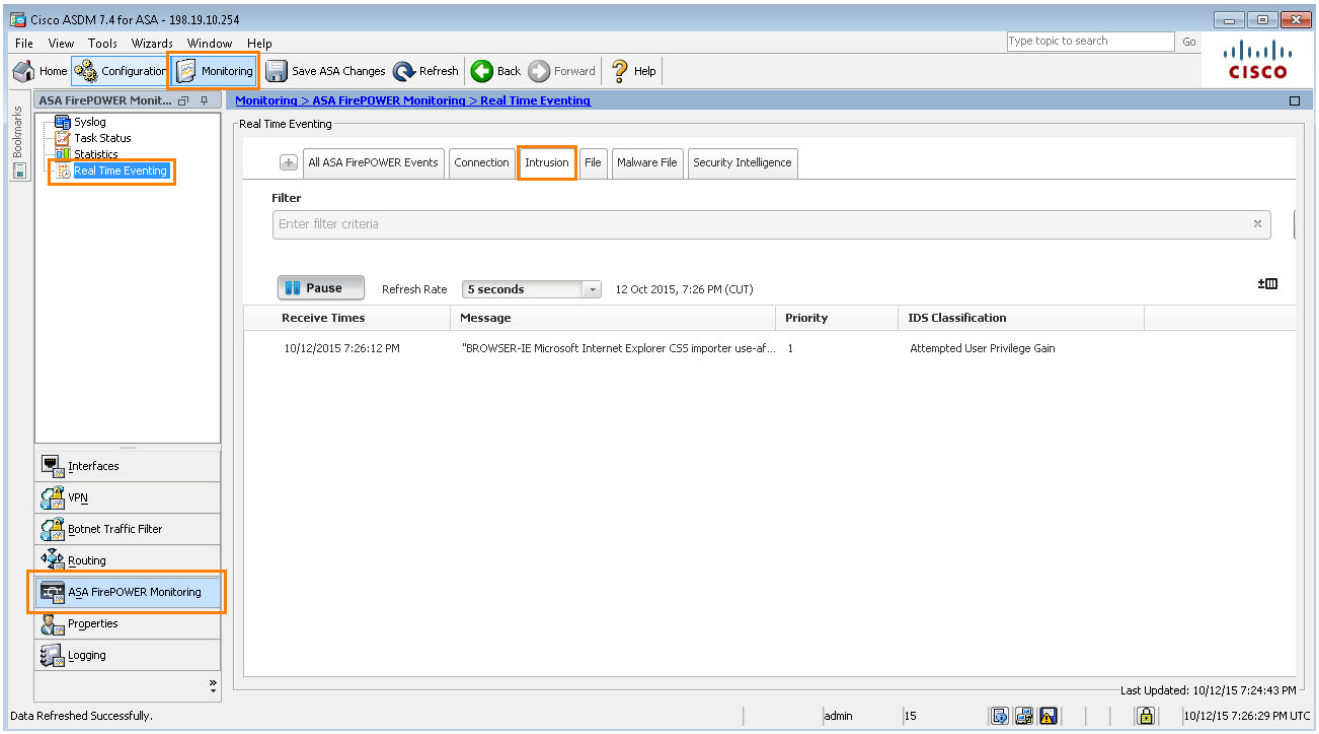
그림 22. 액세스 제어 정책



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

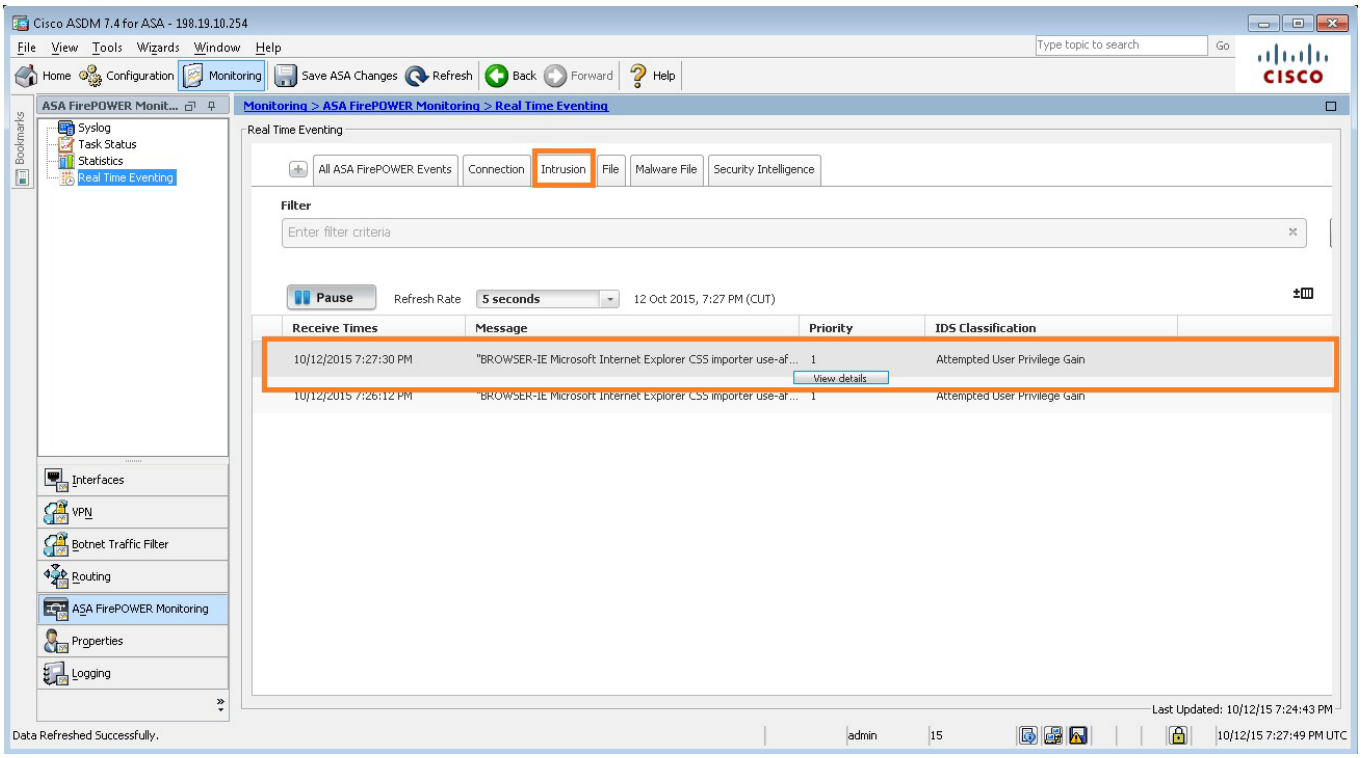
3. **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Real Time Eventing(실시간 이벤트)**을 클릭하고 **Intrusion(침입) 탭**을 클릭합니다.

그림 23. 침입 탭



4. 최근 경고를 선택하고 **View Details(세부사항 보기)**를 클릭합니다.

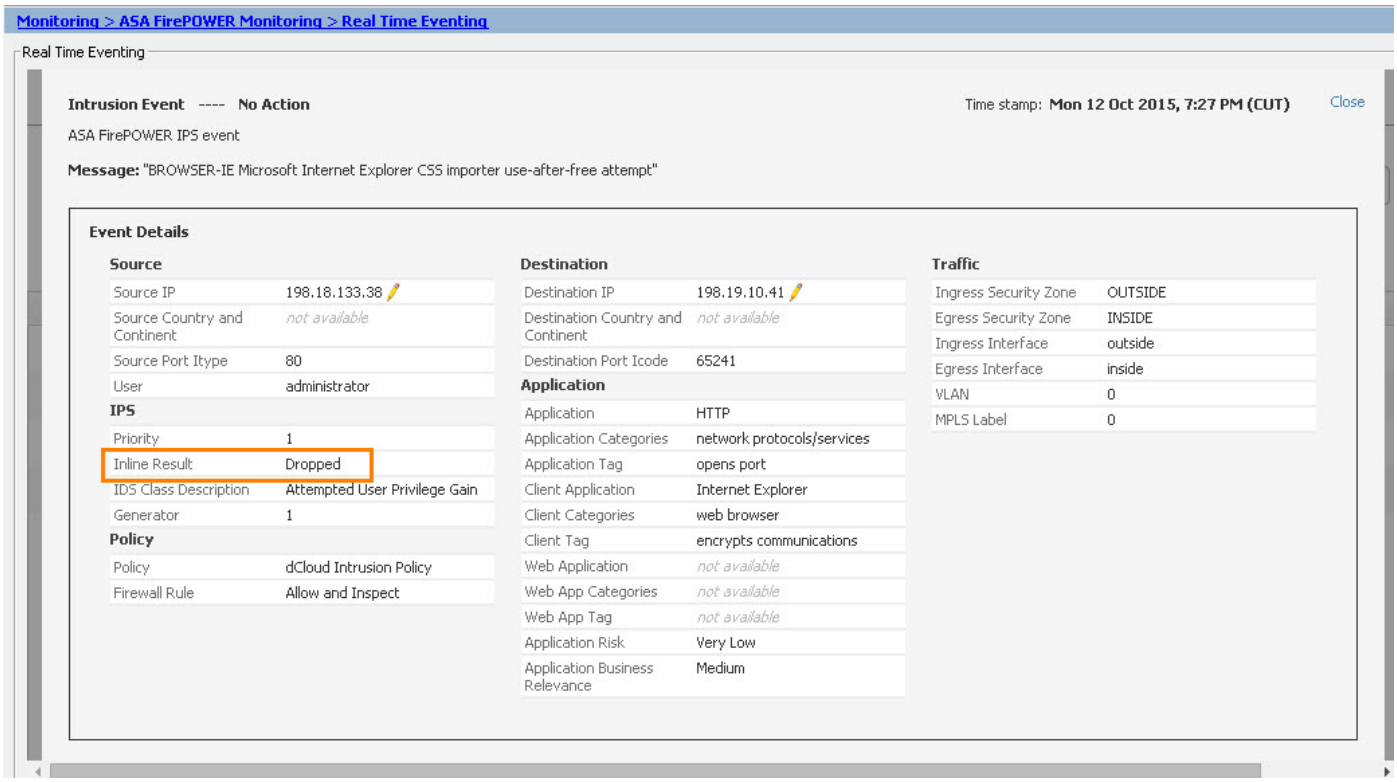
그림 24. 침입 세부사항



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

5. **Inline Result(인라인 결과)**에는 현재 Dropped(삭제됨)라고 나타나며 해당 정책에서 이제 침입을 차단하고 있음을 보여줍니다.

그림 25. 인라인 결과 - 삭제됨



6. **Exploit(익스플로잇)** 창과 **Syslog 서버**를 닫습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

오프박스 관리

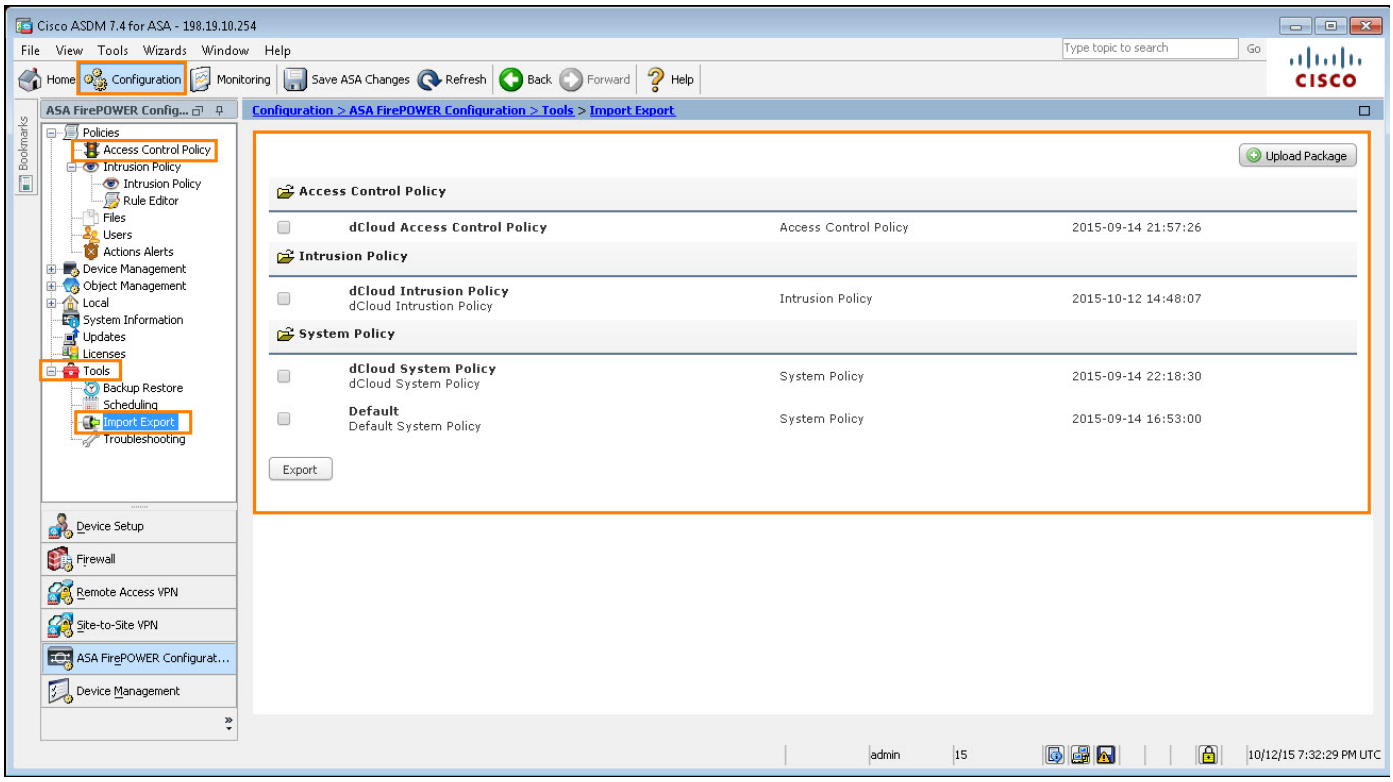
FireSIGHT Management Center는 ASDM을 사용해 다음과 같은 많은 장점을 제공합니다.

- **이벤트.** 초당 이벤트 기능이 향상되고 이벤트 스토리지가 추가되었습니다. IPS 이벤트, 연결 및 악성코드 이벤트, 이벤트 자동화 및 우선순위 지정 간의 상관 관계를 나타냅니다.
- **정책.** ASDM 기능 이외에 17개 이상의 액세스 제어, 로깅 및 알림 기능 제어를 포함합니다. 각 단일 어플라이언스별로 다를 수 있는 시스템 설정과 달리, 이러한 정책은 구축 전체에서 일반적으로 비슷합니다.
- **보고.** 고급 기능으로 세부적인 보고 기능을 제공합니다.
- **상황 인식.** 구축 규모가 클수록 호스트 추적 과정에 더 많은 문제가 발생할 수 있습니다. FSMC는 영향 분석을 포함한 폭넓은 상황 정보를 제공하여 IPS 이벤트 및 교정 기능에 대한 우선순위를 지정합니다.
- **대시보드.** 애플리케이션, 연결, 위협, 파일 및 URL 등의 기타 정보를 제공하는 세부적인 사용자 지정 대시보드입니다.
- **디바이스 관리.** 2개 이상의 디바이스에 더욱 향상된 관리 기능을 제공합니다.

1. **ASDM** 창을 최대화합니다.
2. **Configuration(컨피그레이션) > Access Control Policy(액세스 제어 정책) > Tools(도구) > Import/Export(가져오기/내보내기)**를 클릭합니다.

참고: Import Export(가져오기 내보내기) 화면을 통해 온박스 정책을 내보내고 나중에 FSMC(FireSIGHT Management Center)로 가져올 수 있습니다. 또한, FSMC에서 내보낸 정책도 가져올 수 있습니다. 이 데모에서는 필요한 모든 정책이 FSMC에 이미 로드되어 있으므로 실제로 정책을 내보낼 필요가 없습니다.

그림 26. 컨피그레이션 > 액세스 제어 정책 > 도구 > 가져오기/내보내기

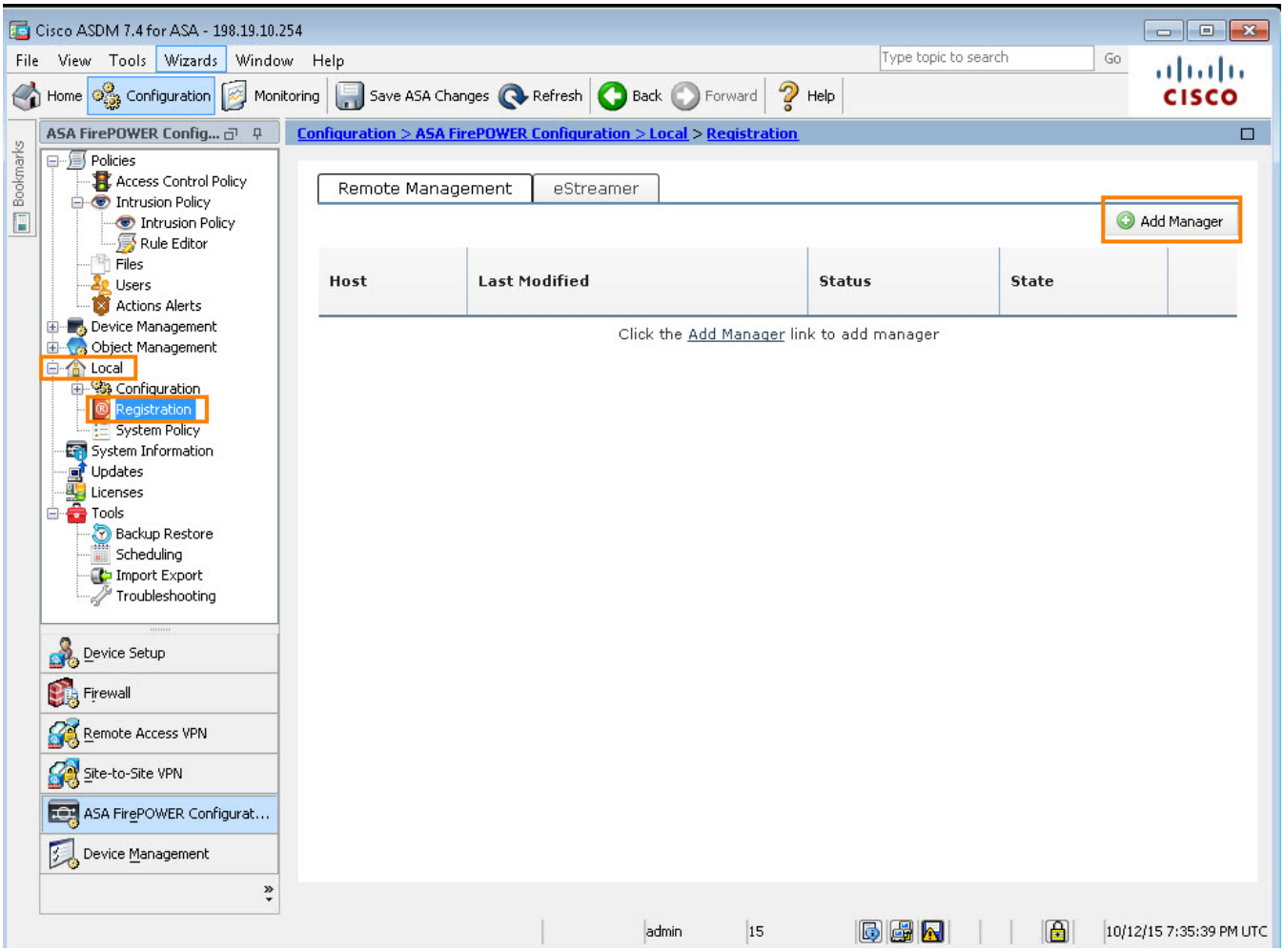


© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

3. **Local(로컬) > Registration(등록)**을 클릭합니다. 이를 통해 ASDM 온박스 관리에서 전체 FireSIGHT Management Center로 FirePOWER 모듈 관리를 재할당할 수 있습니다.

4. 오른쪽 상단에서 **Add Manager(관리자 추가)**를 클릭합니다.

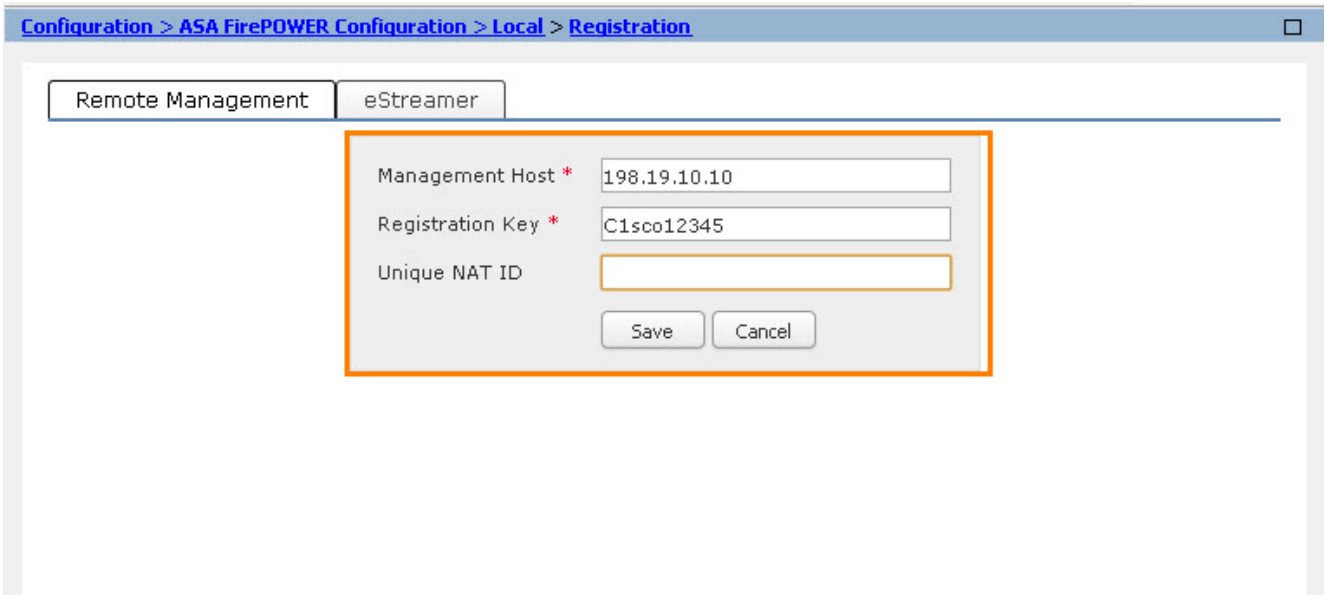
그림 27. 로컬 > 등록 - 관리자 추가



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

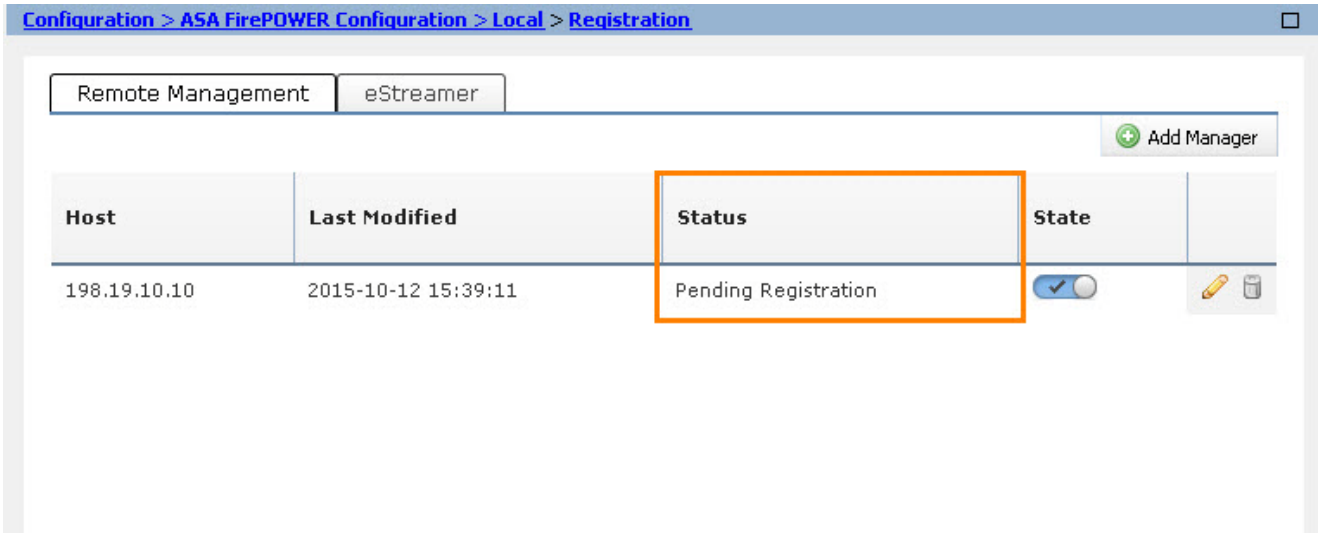
5. 다음 정보를 입력합니다.
   - 관리 호스트: 198.19.10.10
   - 등록 키: C1sco12345
   - 고유한 ID NAT: 빈칸

그림 28. 관리자 정보 추가



6. **Save(저장)**를 클릭합니다. IP 주소의 상태가 Pending Registration(등록 대기 중)입니다.

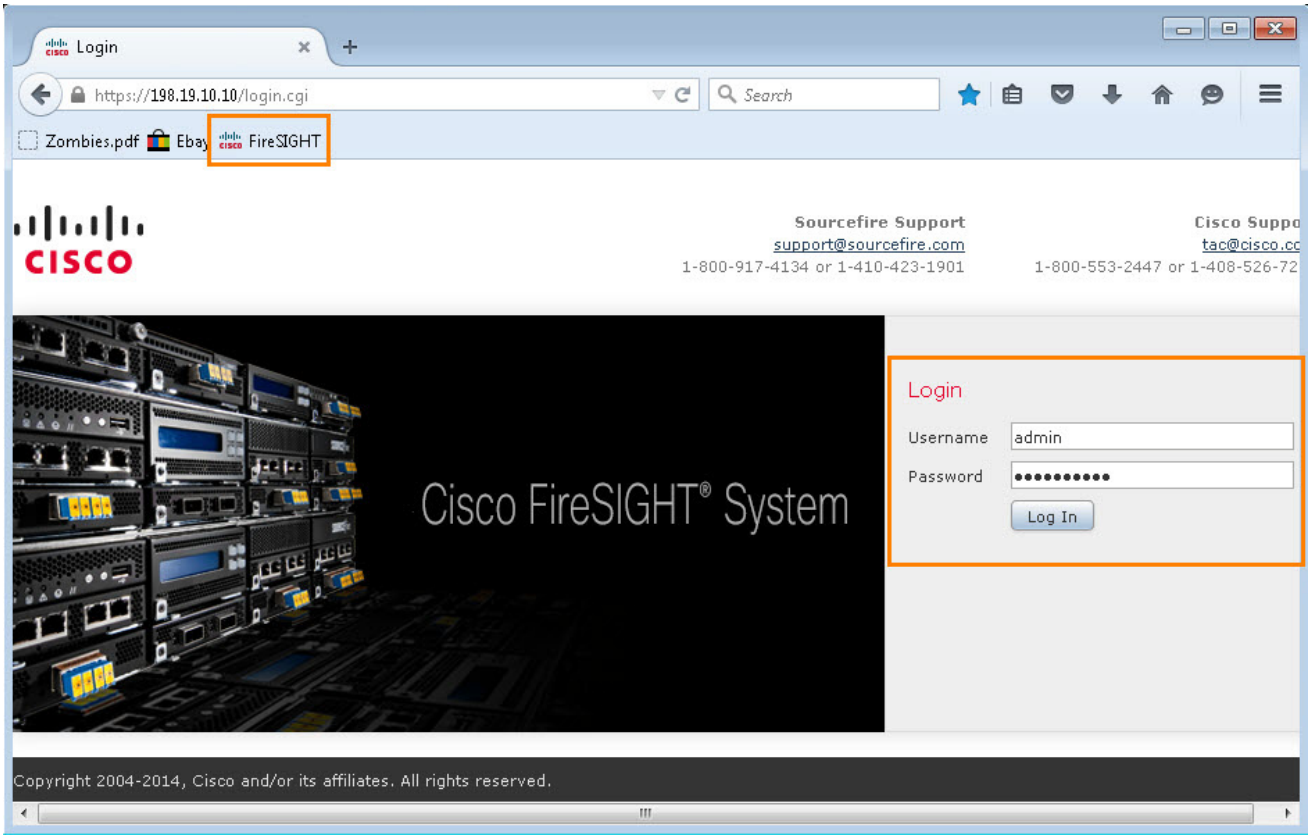
그림 29. 등록 대기 중



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

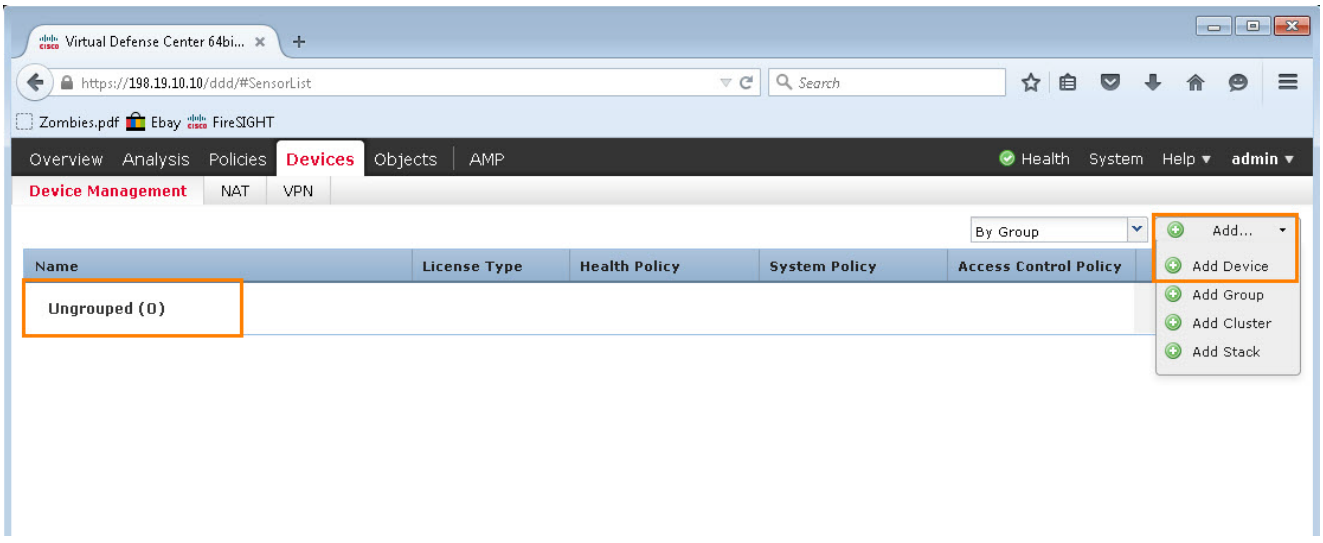
7. **ASDM** 창을 닫습니다.
8. **Firefox**를 열고 메뉴 모음의 아이콘을 클릭하고 캐시된 자격 증명을 사용하여 **FireSIGHT Management Center**에 로그인합니다.

그림 30. FireSIGHT Management Center에 로그인



9. 주 화면에서, **Devices(디바이스) > Device Management(디바이스 관리)**를 클릭합니다. 현재 추가된 디바이스가 없습니다.
10. 오른쪽 상단에서 **Add(추가) > Add Device(디바이스 추가)**를 클릭합니다.

그림 31. 추가 > 디바이스 추가

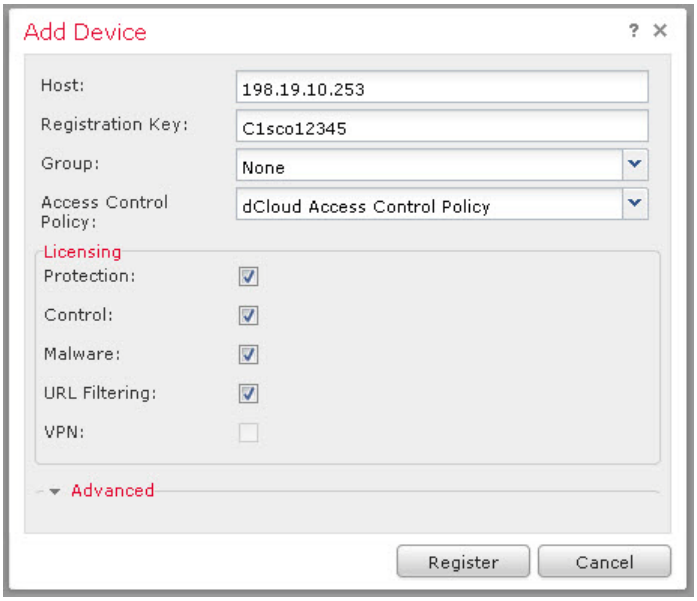


© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

11. **Add Device(디바이스 추가) 창**에 다음 정보를 입력합니다.

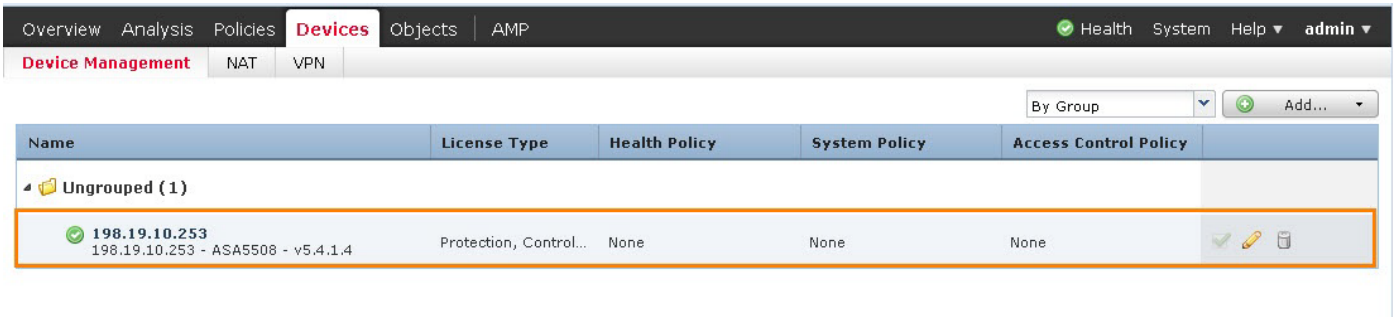
- 호스트: 198.19.10.253
- 등록 키: C1sco12345
- 그룹: 없음
- 액세스 제어 정책: dCloud 액세스 제어 정책
- 라이센스: 모든 상자를 선택

그림 32. 디바이스 추가



12. **Register(등록)**를 클릭합니다. 이 작업에는 2~3분이 소요될 수 있습니다.

그림 33. 등록된 디바이스

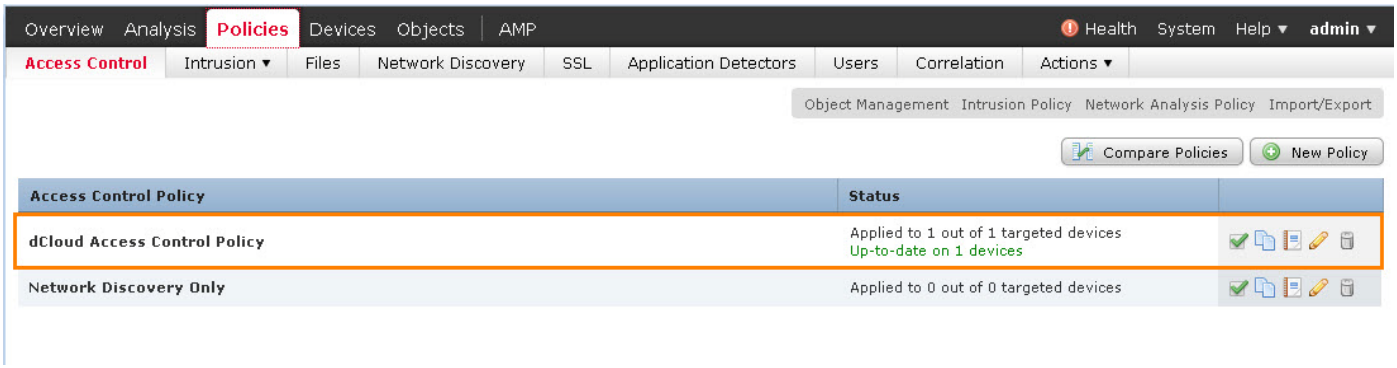


© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

13. 디바이스가 성공적으로 추가되면, 액세스 제어 정책 및 기타 정책이 SFR 모듈에 자동으로 적용됩니다. **Policies(정책) > Access Control(액세스 제어)**로 이동합니다. 정책은 디바이스에 적용되며 완전히 적용되는 데에는 약간의 시간이 소요될 수 있습니다. 상태가 **Up-to-date on 1 devices(디바이스 1개 최신 상태)**로 변경될 때까지 기다립니다.

참고: 보고 기능은 디바이스가 추가되고 정책이 완전히 적용될 때까지 업데이트되지 않습니다. 이 작업에는 최대 5분이 소요될 수 있습니다. 잠시만 기다려 주십시오.

그림 34. 정책 > 액세스 제어



14. **Policies(정책) > Network Discovery(네트워크 검색)**로 이동합니다. **Apply(적용)**를 클릭한 다음 **Yes(예)**를 클릭하여 확인합니다. 네트워크 검색 정책이 SFR 모듈에 적용되기를 기다립니다. 정책이 성공적으로 적용되면 상태가 **Up to date on all targeted devices(모든 대상 디바이스 최신 상태)**로 변경됩니다.

참고: 실제 환경에서 상태 및 시스템 정책도 적용됩니다. 이 데모에서는 이 정책은 적용하지 않습니다.

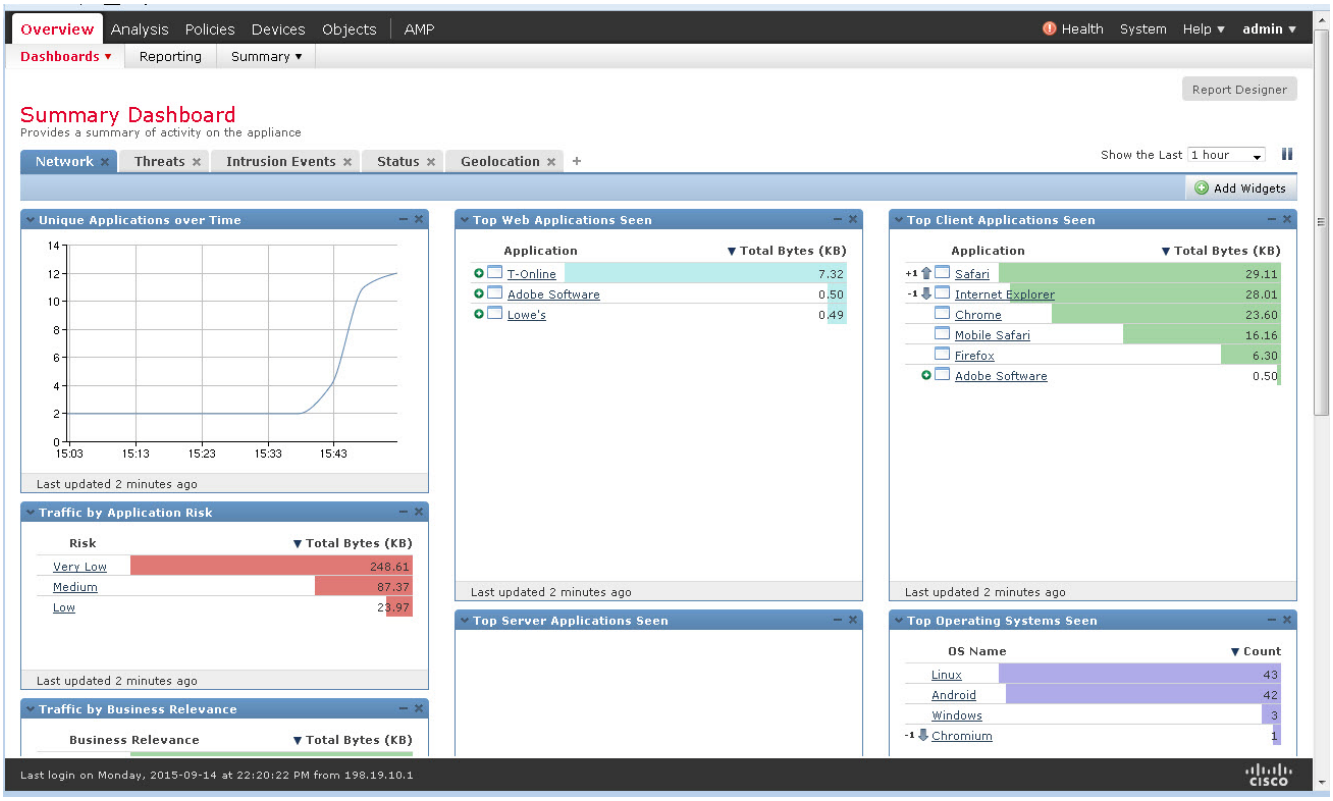
© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

고급 오프박스 기능

1. **Overview(개요) > Dashboards(대시보드) > Summary Dashboard(요약 대시보드)**를 클릭합니다. 이러한 보고서에는 다음 정보가 표시됩니다.
   - Unique Applications Over Time
   - Top Web Applications Seen
   - Top Client Applications Seen
   - Traffic by Application Risk
   - Top Server Applications Seen
   - Top Operating Systems Seen
   - Traffic by Business Relevance
   - Traffic by Application Category
   - Risky Applications with Low Business Relevance
   - Traffic by Initiator User
   - Connections by URL Reputation
   - Connections by URL Category

참고: 이 보고서가 완전히 작성되는 데에는 약간의 시간이 소요될 수 있습니다. 일부 보고서에서 데이터를 확인할 수 없다면 시스템이 정보를 입력할 수 있도록 몇 분 정도 기다렸다가 다시 확인해 보십시오.

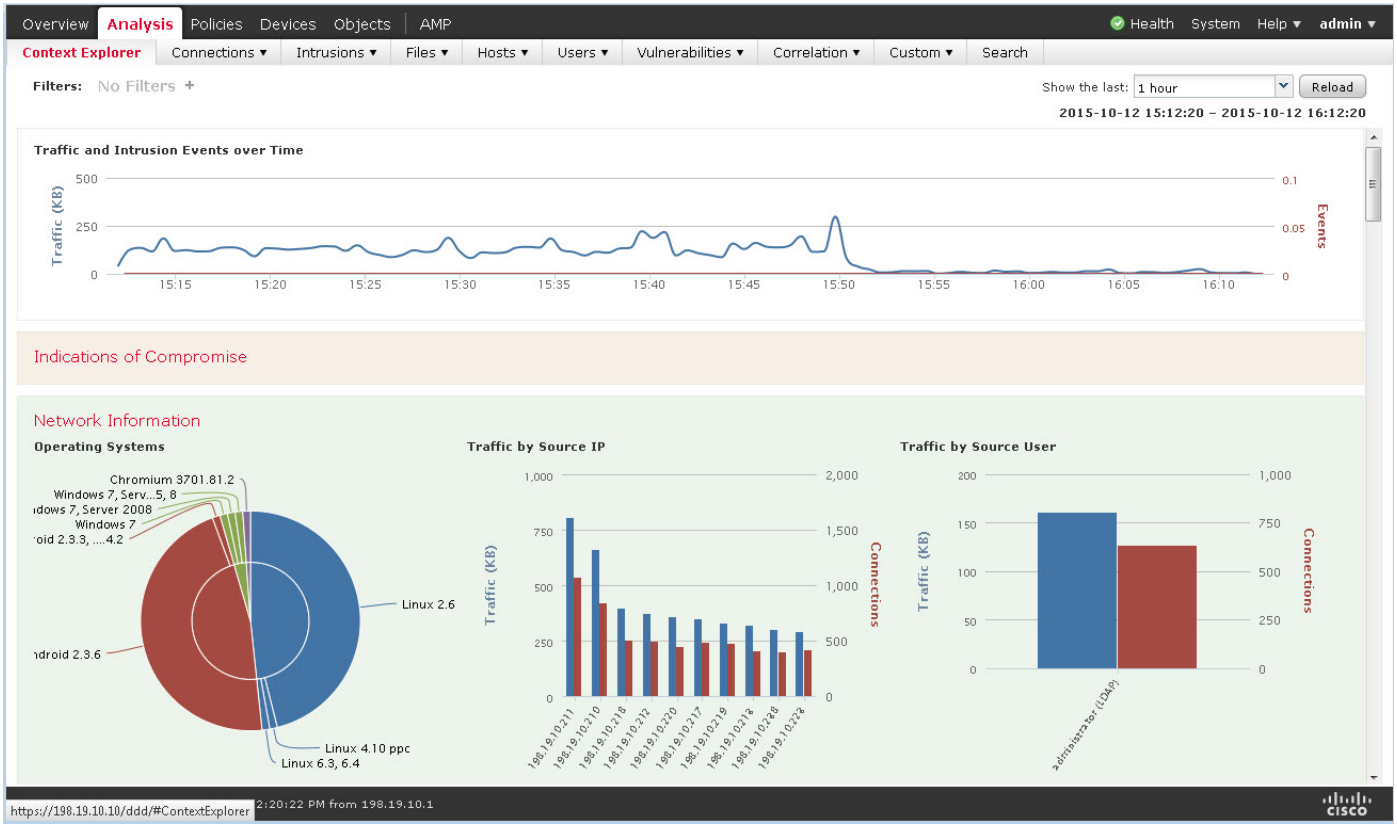
그림 35. 요약 대시보드



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

2. **Analysis(분석) > Context Explorer(컨텍스트 탐색기)**를 클릭합니다. 이 페이지에는 다음 정보가 표시됩니다.
   - 시간 경과에 따른 트래픽 및 침입 이벤트
   - 감염 지표
   - 네트워크 정보
   - 애플리케이션 프로토콜 정보
   - 보안 인텔리전스
   - 침입 정보
   - 파일 정보
   - 위치 정보
   - URL 정보

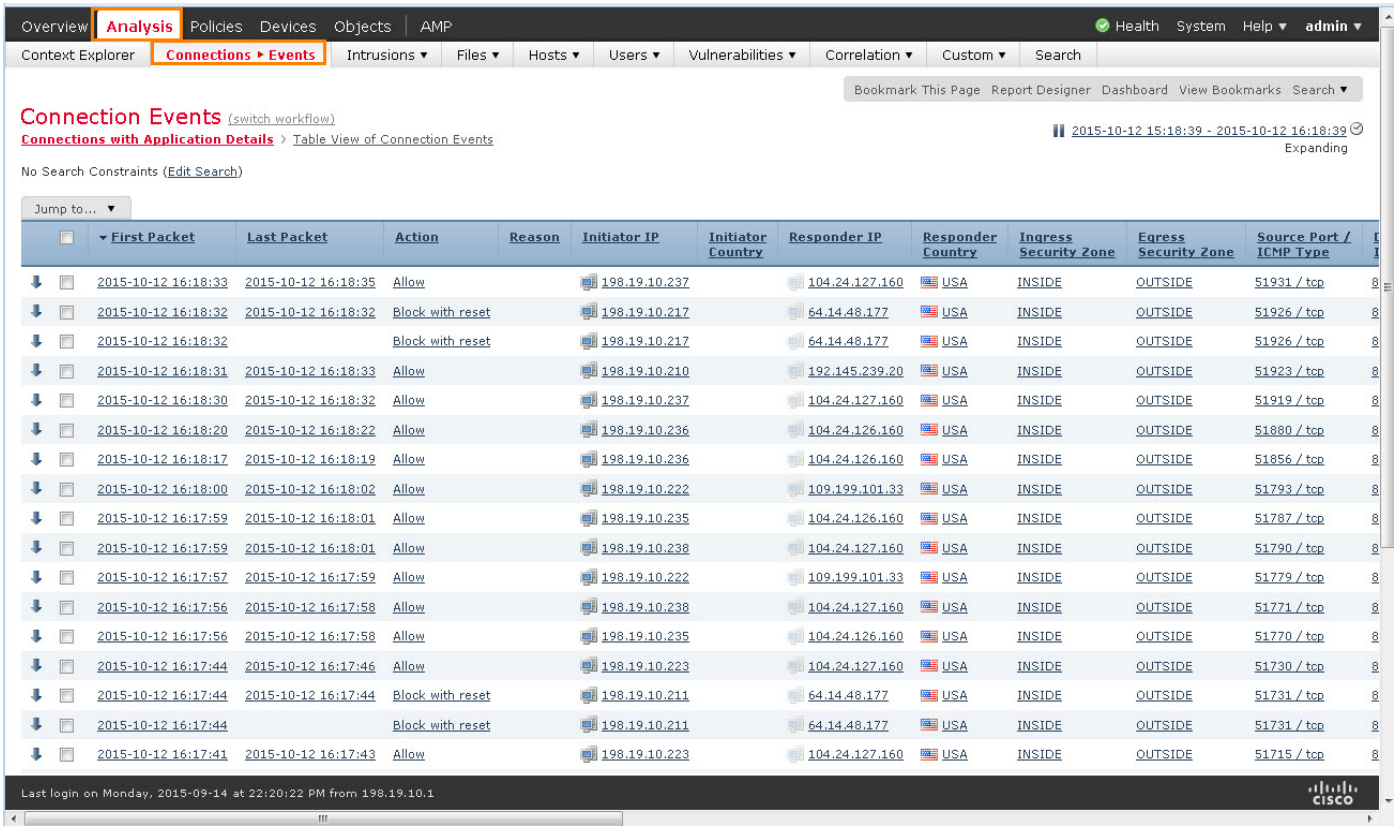
그림 36. 분석 > 컨텍스트 탐색기



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

3. **Analysis(분석) > Connections(연결) > Events(이벤트)**를 클릭합니다. 트래픽 생성 정보가 나타납니다.

그림 37. 분석 > 연결 > 이벤트



미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.