Stealthwatch® Management Console

사용 설명서

(Stealthwatch System v6.9용)

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 UCB(University of Berkeley)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

모든 인쇄 사본 및 소프트 카피 복제본은 비통제 사본으로 간주되며 원본 온라인 버전을 최신 버전으로 참조해야 합니다.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트(www.cisco.com/go/offices)에서 확인하십시오.

목차

1-설명서 정보 11
개요 11
대상 독자 12
SMC 정보 13
SMC 사용자 인터페이스 13
이 설명서 사용 방법 14
문서 아이콘 15
약어 16
기타 리소스 18
관련 문서 18
NetFlow Ninjas 블로그 18
Stealthwatch 비디오 라이브러리 18
지원 팀에 문의 18

2-STEALTHWATCH 어플라이언스 라이선싱 19
개요 19
라이선스 활성화 20
다운로드 및 라이선스 센터 21
관리되는 어플라이언스와 관리되지 않는 어플라이언스 비교 21
라이선스 활성화 22
라이선스 활성화 - 온라인 방식 23
라이선스 활성화 - 오프라인 방식 24
라이선스 상태 정보 28
플로우 수집 29
기능 라이선스 상태 30

3-SMC 클라이언트 인터페이스 탐색 33
개요 33
클라이언트 메모리 할당 34
관점 35
엔터프라이즈 트리 및 툴팁 36
트리를 통한 검색 36
트리 브랜치 37
알람 심각도 레벨 38
엔터프라이즈 트리 표시기 39
툴팁 40

SMC 문서 열기 42
메인 메뉴 42
파일 메뉴 43
편집 메뉴 43
보기 메뉴 44
최상위 메뉴 44
상태 메뉴 44
보안 메뉴 45
호스트 메뉴 45
트래픽 메뉴 45
보고서 메뉴 46
플로우 메뉴 46
컨피그레이션 메뉴 47
도움말 메뉴 47
문서 작업 48
라이브 데이터와 정적 데이터 표시 비교 48
탭과 한 문서에서 다른 문서로 이동 49
문서 방향 변경 51
문서 헤더 52
문서로 이동 버튼 52
문서 헤더에서 52
문서 툴바에서 53
빠른 탐색을 위한 마우스 오른쪽 버튼으로 클릭 54
선택한 문서에 대한 더블 클릭 기능 56
문서 검색 57
문서 닫기 60
테이블 작업 61
열 정렬 61
열 이동 및 크기 조정 62
열 숨기기 및 표시 63
데이터 내보내기 64
멀티섹션 팝업 메뉴 66
빠른 보기 67
차트 작업 68
문서 데이터 필터링 71
날짜/시간 72
호스트 72
인터페이스 73
서비스 및 애플리케이션 73
기타 필터 옵션 74
대시보드 필터 75

문서 인쇄 79
인쇄 미리보기 79
인쇄 설정 80
인쇄 81
문서 저장 82
나중에 사용할 수 있도록 문서 레이아웃 저장 82
문서를 PDF 파일로 저장 85
온라인 도움말 86
목차 87
색인 87
검색 87
용어집 88
즐겨찾기 89
빠른 검색 89
키보드 바로가기 91

4-호스트 관리 97
개요 97
호스트 그룹 98
Catch All(모두 탐지) 호스트 그룹 99
SLIC Threat Feed 호스트 그룹 101
정보 보고서 위로 이동 102
호스트 그룹 만들기 전략 102
호스트 그룹 만들기 103
IP 주소 104
호스트 그룹 멤버십 106
관계형 플로우 맵 107

5-보기 및 대시보드 109
개요 109
SMC의 기본 대시보드 110
호스트 그룹 대시보드 113
호스트 그룹 대시보드 - 네트워크 페이지 114
호스트 그룹 대시보드 - 보안 페이지 115
호스트 그룹 대시보드 - 알람 요약 페이지 116
고유한 대시보드 구축 117

6-지표: 행동 변경 순위 지정 123
개요 123
관심 지표(CI) 125
대상 지표(TI) 128
파일 공유 지수 130

7-트래픽 및 네트워크 성능 모니터링. 133
개요 133
트래픽 모니터링 134
인터넷 트래픽 개요 134
회사 네트워크 개요 137
엑스포터/네트워크 디바이스 139
가상 머신 143
네트워크 성능 147
왕복 시간. 148
서버 응답 시간 149
TCP 재전송 비율. 150
테이블 151

8-플로우 분석 153
개요 153
플로우 필터 154
플로우 쿼리 입력 154
플로우 테이블 탭 168
테이블 탭 168
짧은 리스트 탭 169
빠른 보기 171
플로우 분석 시나리오 172
상위 관심 지표 호스트 172
워크플로 개요 172
보안 이벤트 활동(호스트 스냅샷) 검토 173
사용자 ID 정보(호스트 스냅샷) 검토 175
애플리케이션 트래픽 급증 176
워크플로 개요 177
트래픽 방향 식별. 178
관련 호스트 식별. 179
관련 사용자 식별. 180
오버로드된 인터페이스 181
워크플로 개요 181
오버로드된 인터페이스(인터페이스 상태) 식별 183

느린 네트워크 184
워크플로 개요 184
Stealthwatch IDentity를 사용하여 IP 주소 찾기 186
과도하게 사용된 인터페이스(호스트 스냅샷) 확인 188
높은 대역폭 호스트(인터페이스 요약 대시보드) 찾기 189
높은 대역폭 호스트에 로그인한 사용자 식별 190
상위 활성 플로우 검토 191
외부 조회 193
외부 조회 구성 194
외부 조회 수행 199

9-SLIC THREAT FEED 서비스 203
개요 203
SLIC Threat Feed 정보 204
사전 요구 사항 205
SLIC Threat Feed 작동 방식 207
SLIC Threat Feed 호스트 그룹 208
SLIC Threat Feed 활성화 209
SLIC Threat Feed 비활성화 211
SLIC 보안 이벤트 212

10-문제 원인 찾기 215
개요 215
식별 프로세스 216
알람 요약 217
알람 테이블 219
전체 검색 221
호스트 스냅샷에서 세부사항 가져오기 223
호스트가 다른 알람을 유발했나요? 225
위협이 얼마나 광범위한가? 226
정상적인 행동인가요? 230
어떤 호스트가 동일한 특징을 공유하나요? 231

11-알람 대응 233
개요 233
알람에 대응하는 방법 235
알람 확인 235
알람 확인 취소 237

알람 닫기 237
닫힌 알람 다시 열기 240
Stealthwatch 완화 기능 241
완화 디바이스 구성 242
정책에 대한 완화 기능 활성화 245
알람에 대한 완화 작업 정의 247
완화 및 알람 테이블 249
권한 부여(수동) 모드. 249
자동 모드. 250
완화 작업 문서 251

12-불필요한 알람 줄이기. 253
개요 253
베이스라인 설정 254
호스트 정책 관리 259
내부 호스트/외부 호스트의 기본 정책 편집 261
유효한 호스트 정책 262
알람 카테고리 265
호스트 정책에서 알람 카테고리 구성 266
보안 이벤트 269
호스트 정책에서 보안 이벤트 구성 270
정책 생성 및 편집 273
사전 정의된 그룹에 호스트 할당 274
역할 정책 생성 275
역할 정책 편집 281
호스트 정책 생성 283
호스트 정책 편집 287
알람 289
차이 기반 알람과 설정/해제 알람 비교 289
차이 기반 알람에 대한 설정 292
권장사항 295
상위 관심 지표(CI) 295
상위 파일 공유 지수 296
높은 총 트래픽 296
높은 트래픽 297
ICMP 플러드 297
낮은 트래픽 298
메일 릴레이 298
최대 플로우 시작됨 299
최대 플로우 제공됨 299
새 플로우 시작됨 300
새 플로우 제공됨 300
스팸 소스 301

의심스러운 데이터 손실 301
의심스러운 긴 플로우 302
의심스러운 UDP 활동 303
SYN 플러드 303
SYN 수신됨 304
UDP 플러드 304
웜 활동 305

13-문서 작업 307
개요 307
문서 저장 308
로그인 문서 310
문서 공유 313
DAR 파일 313
DAR 파일 내보내기 313
DAR 파일 가져오기 314
공용 문서 314
문서 일정 지정 316
새 일정 추가 316
기존 일정 편집 319
일정에 문서 추가 320
예약된 문서 이메일로 보내기 321
SMC에 이메일 서버 추가 321
일정에 사용자 이메일 주소 추가 323
공유 문서 사전 필터링 323
아카이브 문서 검색 326

14-사용자 관리 329
개요 329
프로세스 개요 330
인증 서비스 추가 331
사용자가 보고 구성할 수 있는 항목 제어(데이터 역할) 335
이중화된 Flow Collector 데이터를 숨기기 위한 데이터 역할 추가 338
기본 Flow Collector의 데이터 역할 추가 338
이중화된 Flow Collector의 데이터 역할 추가 340
사용자가 수행할 수 있는 작업 제어(기능 역할) 342
사용자 계정 추가 344
사용자 계정 편집 346
예약된 문서를 사용자 계정에 연결하기 349
새 일정 추가 350
기존 일정 편집 353

일정에 문서 추가 355
일정에 사용자 이메일 주소 추가 356
로그인 문서 358

색인 361

1

설명서 정보

개요

이 설명서는 SMC(Stealthwatch Management Console) 소프트웨어를 사용하여 네트워크 성능 문제 및 보안 위험을 최소화하기 위한 "모범 사례"를 담은 지침을 제공합니다. 복잡하고 다양한 많은 네트워크가 존재하므로 이 설명서가 종합 사용 설명서를 의미하지는 않습니다. 대신 이 설명서의 목적은 SMC 소프트웨어를 사용하여 네트워크 성능 문제 또는 네트워크에 대한 위협을 처리 및/또는 방지하기 위한 최선의 방법을 다루는 지침을 제공하는 것입니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 대상 독자
- SMC 정보
- 이 설명서 사용 방법
- 문서 아이콘
- 약어
- 기타 리소스

참고:

*SMC 클라이언트 온라인 도움말*은 SMC 소프트웨어의 다양한 구성 요소 사용에 대한 유용한 정보를 담고 있습니다.

대상 독자

이 설명서의 기본 대상 독자는 SMC 소프트웨어를 매일 사용하는 사용자부터 관리자에 이르는 모든 사용자입니다. 여기서는 사용자가 이미 네트워킹 개념뿐만 아니라 다음과 같은 Stealthwatch System 개념의 일반적인 내용을 이해하고 있다고 가정합니다.

- 호스트
- 플로우
- 서비스
- 애플리케이션
- 지표
- SMC 문서 및 탐색

SMC 정보

SMC(Stealthwatch Management Console)는 네트워크 관리자가 단일 지점에서 분산된 여러 Stealthwatch Flow Collector를 정의, 구성 및 모니터링할 수 있게 지원하는 엔터프라이즈 레벨 보안 관리 시스템입니다. 이 시스템은 물리적 환경 및 가상 환경 전반에서 플로우 기반 보안, 네트워크 및 애플리케이션 성능 모니터링을 제공합니다. 네트워크 운영 및 보안 팀은 Stealthwatch를 통해 누가 네트워크를 사용하고 있는지, 어떤 애플리케이션과 서비스가 사용되고 있는지와 작업을 얼마나 잘 수행하는지를 확인할 수 있습니다.

관리자는 테이블, 파이 차트, 그래프 및 보고서를 사용하여 보안 위협을 빠르게 탐지하고 우선 순위를 정하며 네트워크 오용 및 최적화되지 않은 성능을 정확하게 찾아내고 엔터프라이즈 전반 즉, 모든 단일 컨트롤 센터에서 이벤트 응답을 관리할 수 있습니다. Stealthwatch는 비정상적인 행동을 빠르고 자세하게 살펴보고 상황별 정보와 함께 SMC에 즉시 알람을 보내 보안 담당자가 신속하고 단호한 조치를 취하여 잠재적인 피해를 줄일 수 있게 합니다.

SMC 사용자 인터페이스

Stealthwatch System은 v6.5.0부터 센서의 데이터를 표시하고 관리 기능(예: 정책 정의)을 제공하기 위해 일정 기간 동안 두 개의 사용자 인터페이스(예: 관리 콘솔)를 사용하게 됩니다. 기존 인터페이스를 계속해서 사용할 수 있지만 점차적으로 중단될 예정입니다. 기존 기능은 새로운 Stealthwatch 웹 애플리케이션 인터페이스로 이전되고 있습니다. 이 전환 기간 동안에는 두 가지 UI를 모두 사용해야 합니다. 각 UI에 대한 온라인 도움말에서 필요시 한 UI에서 다른 UI로 전환해야 하는 이유를 설명해 드리겠습니다.

SMC: SMC는 그래프, 테이블 및 필터 정보를 제공합니다. 필터는 경우에 따라 여러 페이지 또는 대화 상자로 구성됩니다.

웹 애플리케이션: 새로운 형식은 상업용 웹 사이트에서 찾을 수 있는 요소(예: 쿼리의 초점 범위를 줄이는 데 사용하는 필터 창)를 포함하여 더 시각적인 접근 방식을 사용합니다. 이 UI는 Stealthwatch System을 실행할 때 열립니다. 원하는 경우 이 UI에서 SMC 클라이언트 인터페이스에 액세스할 수 있습니다.

이 설명서 사용 방법

이 소개 내용 외에도 이 가이드는 다음과 같은 장으로 분류되어 있습니다.

해당하는 장	다음을 수행하는 방법 설명
2 - Stealthwatch 어플라이언스 라이선싱	Stealthwatch 어플라이언스 라이선스를 획득합니다.
3 - SMC 클라이언트 인터페이스 탐색	SMC 내에서 공통 탐색 요소를 사용합니다.
4 - 호스트 관리	정책을 사용하여 행동을 제어할 수 있도록 호스트를 그룹화합니다.
5 - 보기 및 대시보드	SMC 내에서 가장 중요한 활동을 나타내는 데이터의 다양한 테이블 형식 및 그래픽 표시를 봅니다.
6 - 지표: 행동 변경 순위 지정	지표를 사용하여 비정상적인 행동을 추적합니다.
7 - 트래픽 및 네트워크 성능 모니터링	서버와 네트워크 응답 시간뿐만 아니라 트래픽을 모니터링합니다.
8 - 플로우 분석	트렌드를 결정하기 위해 호스트를 오고 가는 플로우를 분석합니다.
9 - SLIC Threat Feed 서비스	Stealthwatch의 온라인 위협 인텔리전스 서비스를 사용합니다.
10 - 문제 원인 찾기	알람을 확인하고 닫으며 자동 완화 기능을 사용하고 소스를 수동으로 차단합니다.
11 - 알람 대응	표시되는 불필요한 알람 수를 줄이기 위해 정책을 조정합니다.
12 - 불필요한 알람 줄이기	알람을 유발한 첫 번째 호스트와 이 알람이 영향을 미치는 호스트를 찾습니다.
13 - 문서 작업	지정한 구성 요소를 포함하는 맞춤형 문서를 저장 및 공유하고 문서의 일정을 지정합니다.
14 - 사용자 관리	사용자 액세스 및 사용자와 연결된 역할을 관리합니다.

문서 아이콘

이 문서에서는 중요한 정보를 표시하기 위해 다음과 같은 아이콘을 사용합니다.

아이콘	의미	포함되는 정보
	팁:	바로가기 또는 특정 작업을 수행하는 간편한 방법 등을 나타냅니다.
	참고	이 문서 또는 Stealthwatch System에서 사용 시 유용한 내용입니다.
	중요	소프트웨어 오작동 등의 중대한 결과를 방지하기 위해 준수해야 하는 내용입니다.
	주의	데이터 손실 또는 하드웨어 손상을 방지하기 위해 준수해야 하는 내용입니다.

약어

이 설명서에는 다음 약어가 나와 있습니다.

약어	정의
AS(번호)	Autonomous System(자동 시스템)
CI	Concern Index(관심 지표)
CIDR	Classless Inter-Domain Routing
CSV	Comma-Separated-Value(쉼표로 구분된 값)
DAR	Disk Archive(디스크 아카이브)
DHCP	Dynamic Host Configuration Protocol(동적 호스트 구성 프로토콜)
DNS	Domain Name System(서비스 또는 서버)
DoS	Denial of Service(서비스 거부)
DSCP	Differentiated Services Code Point
FSI	File Sharing Index(파일 공유 지수)
IANA	Internet Assigned Numbers Authority
ID	Identifier(식별자)
IM	Instant Messaging(인스턴트 메시징)
IP	Internet Protocol(인터넷 프로토콜)
MAC	Media Access Control(미디어 액세스 제어)
MPLS	Multiprotocol Label Switching
PDF	Portable Document Format
P2P	Peer-to-Peer
RADIUS	Remote Authentication Dial-in User Service
RFC	Request for Comment
RTT	Round Trip Time(왕복 시간)
SMC	Stealthwatch Management Console
SNMP	Simple Network Management Protocol
SRT	Server Response Time(서버 응답 시간)
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol(전송 제어 프로토콜)

약어	정의
TI	Target Index(대상 지표)
UDP	User Datagram Protocol
UI	User Interface(사용자 인터페이스)
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine(가상 머신)
VPN	Virtual Private Network(가상 프라이빗 네트워크)

기타 리소스

이 가이드 외에도 다음과 같은 문서 및 온라인 자료를 유용하게 사용할 수 있습니다.

관련 문서

Stealthwatch 제품에 대한 추가 정보는 Stealthwatch 사용자 커뮤니티 웹 사이트(community.lancope.com)에서 확인할 수 있습니다.

NetFlow Ninjas 블로그

Lancope의 *NetFlow Ninjas* 블로그(http://www.lancope.com/blog)에서는 NetFlow, NetFlow 업계, 새로운 Stealthwatch 기능에 대한 다양한 정보와 더불어 Stealthwatch 사용에 관한 유용한 정보를 제공합니다.

Stealthwatch 비디오 라이브러리

Stealthwatch 온라인 비디오 라이브러리(http://www.lancope.com/resource-center/videos)는 네트워크 성능 및 보안 관리를 위한 Stealthwatch의 이점을 보여줍니다.

지원 팀에 문의

기술 지원이 필요한 경우 다음 중 하나를 수행하십시오.

- 현지 Lancope 파트너에 문의하십시오.
- 이메일 지원을 받으려면 Lancope 고객 커뮤니티(community.lancope.com)를 방문하십시오.
- 전화: +1 800-838-6574
- Lancope 고객 커뮤니티 웹 사이트(community.lancope.com)에서 지원 양식을 사용하여 사례를 제출하십시오.

이 경우 다음 정보를 입력해야 합니다.

- 사용자 이름
- 회사 이름
- 위치

2

STEALTHWATCH 어플라이언스 라이선싱

개요

v6.3부터 Stealthwatch 제품에 대한 라이선싱 요건이 변경되었습니다. Lancope에서 직접 제품을 구매하든 Lancope의 파트너 중 한 곳을 통해 구매하든 관계없이 Stealthwatch System의 모든 새로운 설치 및 업그레이드 시 유효한 라이선스가 필요합니다.

라이선싱 요구 사항을 확인하는 데 유용한 Inventory Report(인벤토리 보고서)를 확인할 수도 있습니다. 이 보고서는 시스템에 설치되어 있는 Lancope 제품에 대한 자세한 정보를 제공합니다.

참고:

인벤토리 보고서에 대한 자세한 내용은 30페이지의 "기능 라이선스 상태" 및 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

이 장은 다음 항목으로 구성되어 있습니다.

- 라이선스 활성화
- 라이선스 상태 정보

라이선스 활성화

다음의 Stealthwatch 어플라이언스에는 라이선스가 있어야 합니다.

- SMC
- Flow Collector
- FlowSensor
- UDP Director(FlowReplicator라고도 함)

각 라이선스는 어플라이언스 시리얼 번호와 연결되어 있습니다. 동일한 유형의 어플라이언스를 여러 개 사용하는 경우, 물리적 어플라이언스인지 가상 어플라이언스인지 관계없이 각 어플라이언스에 라이선스가 있어야 합니다.

다음 Stealthwatch 기능에도 라이선스가 있어야 합니다.

- Stealthwatch 모듈
- DDoS 모듈
- 초당 플로우 수(FPS)
- SLIC(Stealthwatch Labs Intelligence Center) 위협 피드
- ID 서비스

신규 구축을 위한 초기 라이선싱에 대한 지침은 *Stealthwatch 제품 다운로드 및 라이선싱* 문서를 참조하십시오. 이 섹션의 절차를 사용하여 현재 구축에 새 라이선스를 추가하거나 기존 라이선스를 업데이트하십시오.

어플라이언스 또는 기능을 위한 새 라이선스를 구입하거나 기존 라이선스를 갱신하려면 다음 중 하나를 수행하십시오.

- 현지 Lancope 파트너에 문의하십시오.
- +1 888-419-1462로 문의하십시오.
- sales@lancope.com으로 이메일을 전송하십시오.

다운로드 및 라이선스 센터

Lancope Download and License Center(Lancope 다운로드 및 라이선스 센터)는 온라인 소프트웨어 전송 서비스로, 사용자 계정을 관리하고 라이선스를 포함한 Stealthwatch 제품을 최신 상태로 유지하는 데 도움이 됩니다. 어플라이언스, 기능 또는 라이선스를 구매할 경우, 다음 섹션에 설명된 대로 Lancope Download and License Center(다운로드 및 라이선스 센터)로 이동됩니다. 다운로드 및 라이선스 센터를 주기적으로 확인하여 새로운 소프트웨어 릴리스에 대한 소식을 얻는 것이 좋습니다. https://lancope.flexnetoperations.com으로 이동하여 언제든지 계정에 액세스할 수 있습니다. 로그인 ID는 사용자의 이메일 주소입니다.

참고:

Lancope에서 물리적 Stealthwatch 어플라이언스를 직접 구매하고 SMC에서 인터넷 액세스가 가능한 경우, Download and License Center(다운로드 및 라이선스 센터)에 액세스하여 라이선스를 활성화할 필요가 없습니다.

질문이 있거나 다운로드 및 라이선스 센터에 문제가 있는 경우, lancope@flexnetoperations.com으로 문의하거나 1-888-715-4687(미국 내 지역) 또는 1-408-642-3965(미국 외 지역)로 전화하십시오.

관리되는 어플라이언스와 관리되지 않는 어플라이언스 비교

관리되는 어플라이언스는 SMC와 직접 통신하는 반면 관리되지 않는(독립형) 어플라이언스는 SMC와 직접 통신하지 않습니다. 다음 리스트는 어떤 Stealthwatch 어플라이언스가 관리되는지 또는 독립형인지 나타냅니다.

- Flow Collector는 항상 관리됩니다.
- FlowSensor는 관리되거나 독립형일 수 있습니다.
- UDP Director(FlowReplicator라고도 함)는 항상 독립형입니다.

참고:

어플라이언스 관리(관리자) 인터페이스를 사용하여 독립형 어플라이언스에 대한 라이선스를 활성화하십시오. 어플라이언스 관리 인터페이스를 사용하여 관리되지 않는 어플라이언스에 대한 라이선스를 활성화하는 방법에 대한 정보는 *어플라이언스 관리 온라인 도움말*을 참조하십시오.

라이선스 활성화

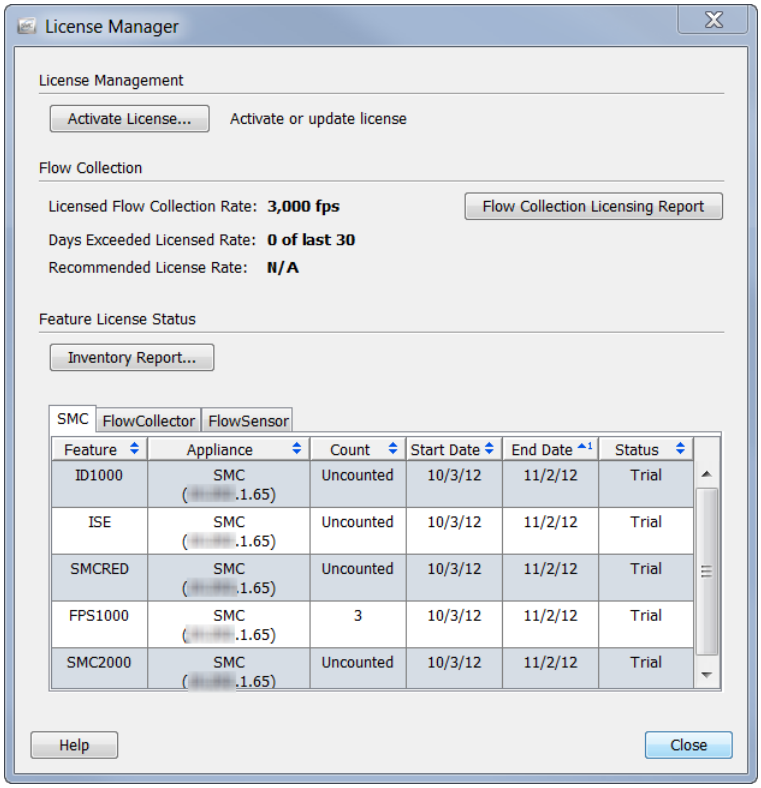
기능 또는 관리되는 어플라이언스를 위해 새 라이선스를 활성화하거나 기존 라이선스를 업데이트하려면 다음 단계를 수행하십시오.

1. 어플라이언스 또는 기능에 대한 모든 라이선스 토큰을 받았습니까?
   - 대답이 예인 경우 2단계로 이동합니다.
   - 대답이 아니요인 경우 3단계로 이동합니다.
2. 라이선스 토큰을 수신한 경우, Download and License Center(다운로드 및 라이선스 센터)에 액세스하여 라이선스 토큰을 계정에 추가하고 해당하는 제품을 등록합니다. 관련 지침은 웹 사이트의 라이선싱 문서 섹션을 참조하십시오.
3. 가상 어플라이언스입니까?
   - 대답이 예인 경우 4단계로 이동합니다.
   - 대답이 아니요인 경우 5단계로 이동합니다.
4. 가상 어플라이언스인 경우, *Stealthwatch VE 설치 및 환경 설정 가이드*에 설명된 대로 어플라이언스를 설치 및 구성합니다.
5. 이 SMC가 인터넷에 연결되어 있습니까?
   - 대답이 예인 경우 23페이지의 "라이선스 활성화 - 온라인 방식"으로 이동합니다.
   - 대답이 아니요인 경우 24페이지의 "라이선스 활성화 - 오프라인 방식"으로 이동합니다.

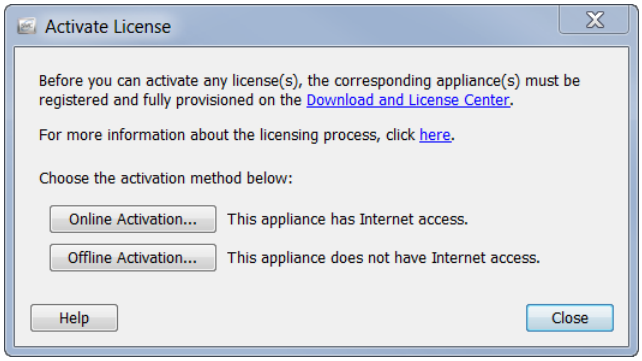
라이선스 활성화 - 온라인 방식

SMC가 인터넷에 연결되어 있을 때 기능 또는 관리되는 어플라이언스를 위해 라이선스를 활성화하려면 다음 단계를 수행하십시오.

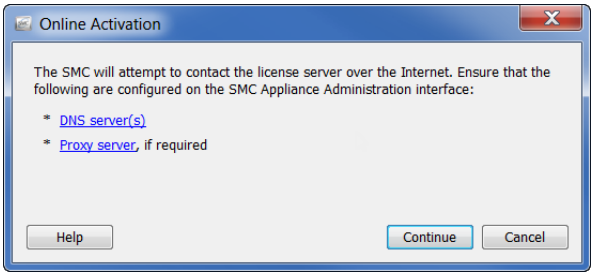
1. SMC 클라이언트 인터페이스에 액세스합니다.
2. 메인 메뉴에서 **Help(도움말) > License Management(라이선스 관리)**를 선택합니다. 다음과 같은 License Manager 대화 상자가 열립니다.



3. **Activate License(라이선스 활성화)**를 클릭합니다. 다음과 같은 Activate License(라이선스 활성화) 대화 상자가 열립니다.

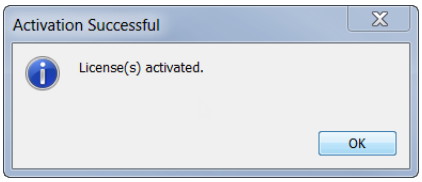


4. **Online Activation(온라인 활성화)**을 클릭합니다. Online Activation(온라인 활성화) 대화 상자가 열립니다.

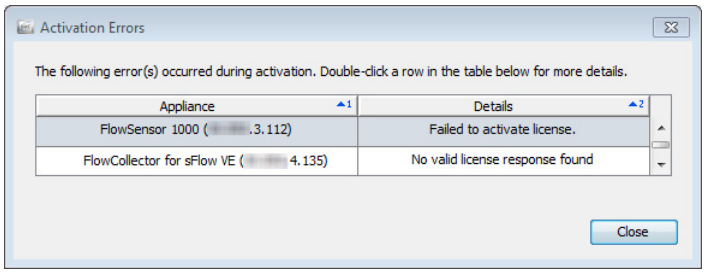


5. **Continue(계속)**를 클릭합니다.

   - 프로세스가 정상적으로 완료되면 확인 대화 상자가 열립니다. **OK(확인)**를 클릭하여 대화 상자를 닫습니다.



   - 활성화에 실패하면 오류 대화 상자가 열리고 프로세스가 실패한 각 어플라이언스가 나열됩니다. 자세한 내용을 확인하려면 테이블에서 행을 더블 클릭하십시오. **Close(닫기)**를 클릭하여 대화 상자를 종료합니다.



라이선스 활성화 - 오프라인 방식

SMC가 인터넷에 연결되어 있지 않을 때 기능 또는 관리되는 어플라이언스를 위해 라이선스를 활성화하려면 다음 단계를 수행하십시오.

1. 인터넷 액세스가 가능한 컴퓨터로 이동합니다.
2. Download and License Center(다운로드 및 라이선스 센터) (https://lancope.flexnetoperations.com)에 액세스하고 My Appliances(내 어플라이언스) 페이지로 이동합니다.

3. 해당하는 어플라이언스를 선택하고 라이선스를 로컬 하드 드라이브, 네트워크 위치 또는 플래시 드라이브와 같은 휴대용 디바이스에 다운로드합니다.

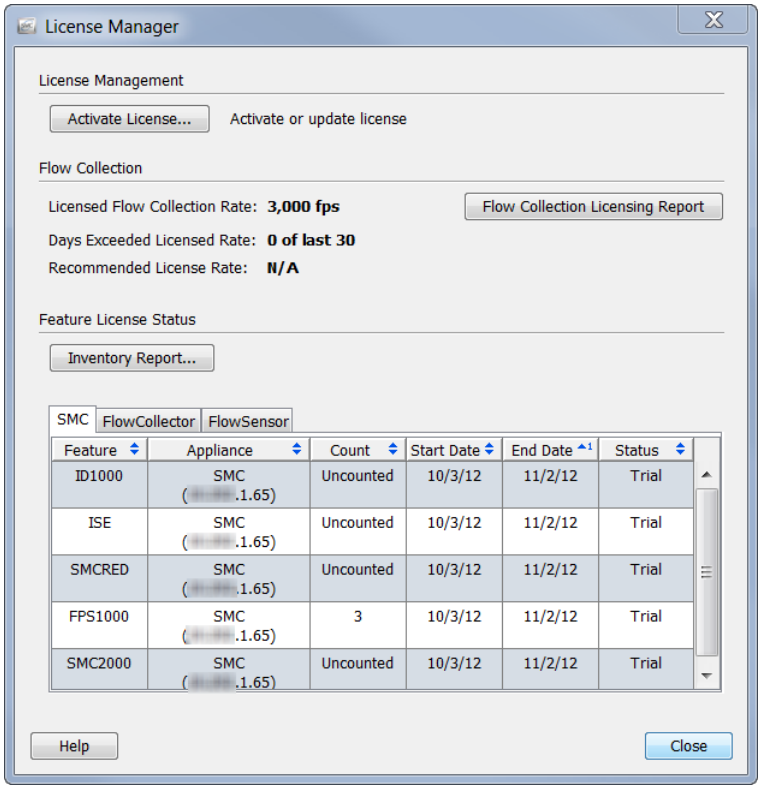
   단일 라이선스(BIN) 파일 또는 여러 개의 라이선스를 다운로드할 수 있습니다. 여러 개의 라이선스를 다운로드하는 경우, 단일 디렉토리 또는 ZIP 파일에 모든 BIN 파일을 저장할 수 있습니다.

4. SMC 클라이언트 인터페이스에 액세스하는 데 사용한 컴퓨터로 이동합니다.

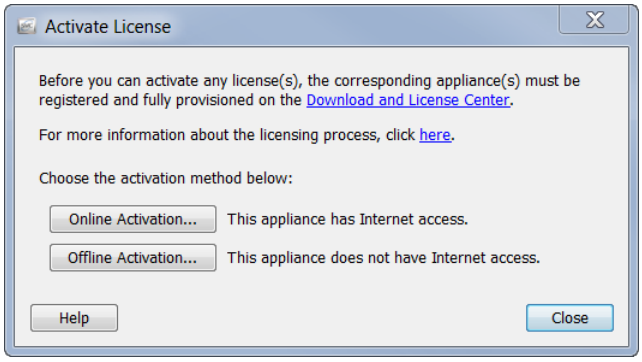
5. SMC 클라이언트 인터페이스에 액세스합니다.

6. 메인 메뉴에서 **Help(도움말) > License Management(라이선스 관리)**를 선택합니다.

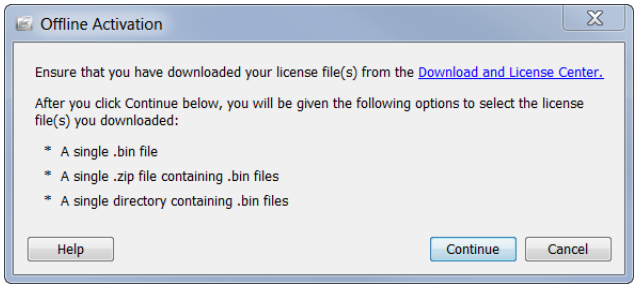
   다음과 같은 License Manager 대화 상자가 열립니다.



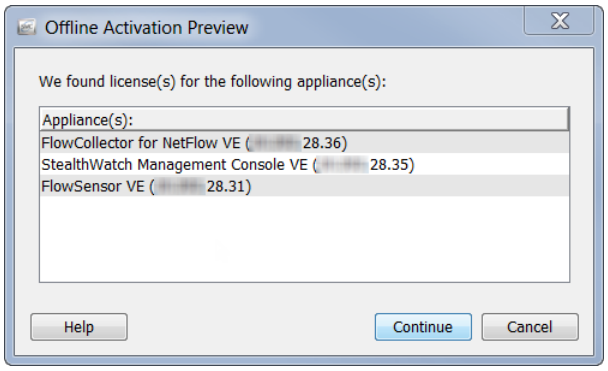
7. **Activate License(라이선스 활성화)**를 클릭합니다. 다음과 같은 Activate License(라이선스 활성화) 대화 상자가 열립니다.



8. **Offline Activation(오프라인 활성화)**을 클릭합니다. Offline Activation(오프라인 활성화) 대화 상자가 열립니다.

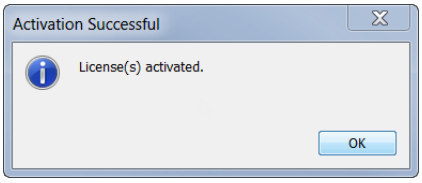


9. **Continue(계속)**를 클릭합니다. 파일을 선택할 수 있는 대화 상자가 열립니다.
10. 3단계에서 라이선스 파일을 다운로드한 위치로 이동합니다.
11. BIN 파일, 여러 개의 BIN 파일이 포함된 디렉토리 또는 라이선스가 필요한 기능이나 어플라이언스를 위한 라이선스가 포함된 ZIP 파일을 선택합니다. 현재 사용 가능한 라이선스의 어플라이언스를 표시하는 Offline Activation Preview(오프라인 활성화 미리보기) 대화 상자가 열립니다.

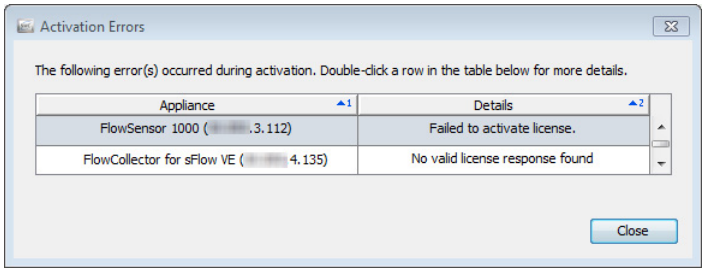


12. **Continue(계속)**를 클릭합니다.

- 프로세스가 정상적으로 완료되면 확인 대화 상자가 열립니다. **OK(확인)**를 클릭하여 대화 상자를 닫습니다.



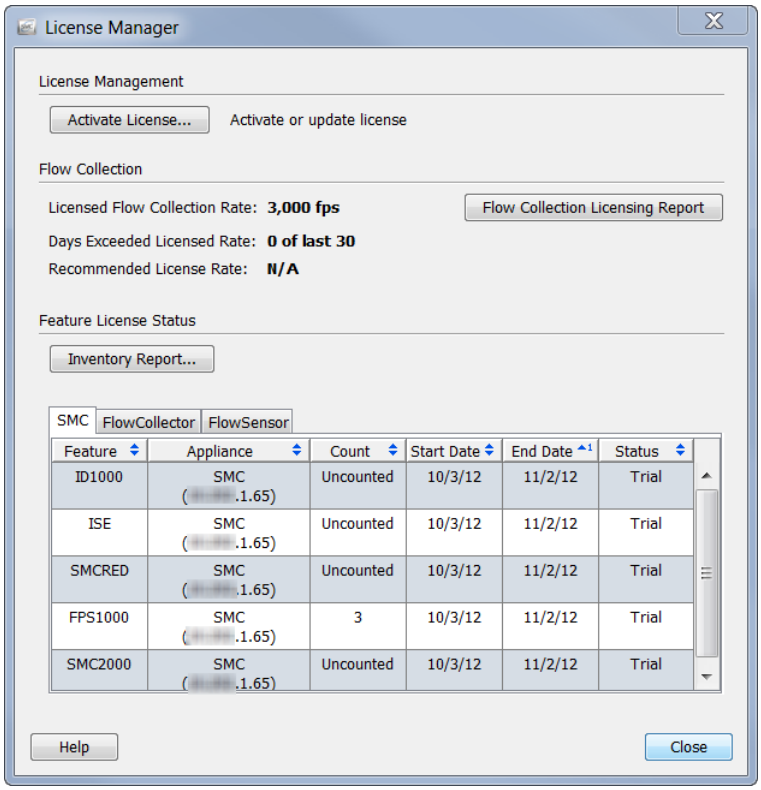
- 활성화에 실패하면 오류 대화 상자가 열리고 프로세스가 실패한 각 어플라이언스가 나열됩니다. 자세한 내용을 확인하려면 테이블에서 행을 더블 클릭하십시오. **Close(닫기)**를 클릭하여 대화 상자를 종료합니다.



라이선스 상태 정보

SMC, 관리되는 어플라이언스 및 기능에 대한 라이선스 정보를 확인하려는 경우, 다음 단계를 수행하십시오.

1. SMC 클라이언트 인터페이스에 액세스합니다.
2. 메인 메뉴에서 **Help(도움말) > License Management(라이선스 관리)**를 선택합니다. 다음과 같은 License Manager 대화 상자가 열립니다.



이 대화 상자는 다음의 3가지 섹션으로 나뉩니다.

- License Management(라이선스 관리) - 이 섹션에서는 라이선스를 활성화할 수 있습니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 22페이지의 "라이선스 활성화"를 참조하십시오.
- Flow Collection(플로우 수집) - 이 섹션에서는 초당 플로우 수(FPS) 라이선스에 대한 정보를 제공합니다. 추가 정보는 29페이지의 "플로우 수집"을 참조하십시오.
- Feature License Status(기능 라이선스 상태) - 이 섹션에서는 SMC와 관리되는 어플라이언스 및 기능에 대한 정보를 제공합니다. 추가 정보는 30페이지의 "기능 라이선스 상태"를 참조하십시오.

플로우 수집

License Manager 대화 상자의 Flow Collection(플로우 수집) 섹션에서는 다음 테이블에서와 같이 FPS 라이선스에 대한 정보를 제공합니다.

항목	설명
Licensed Flow Collection Rate(라이선스 플로우 수집 비율)	라이선스에서 허용하는 모든 Flow Collector의 초당 최대 플로우 수(95번째 백분위 수)입니다. 이 비율이 초과되는 경우, Stealthwatch Flow License Exceeded(Stealthwatch 플로우 라이선스 초과됨) 알람이 생성됩니다.
Days Exceeded Licensed Rate(라이선스 날짜가 초과된 비율)	시스템이 라이선스에서 허용하는 초당 최대 플로우 수를 초과한 마지막 30일간의 일수입니다. **참고:** 시스템에서 이 라이선스 비율이 10일 이상 초과된 경우, 이 값은 빨간색이 됩니다. 시스템에서 이 라이선스 비율이 10일 미만으로 초과된 경우, 이 값은 노란색이 됩니다.
Recommended License Rate(권장 라이선스 비율)	실제 플로우 수집 비율이 지난 30일 동안의 라이선스 제한을 초과한 횟수를 기준으로 시스템이 라이선스를 얻어야 하는 기간의 FPS 수(Lancope에서 권장)입니다.
Flow Collection Licensing Report(플로우 수집 라이선싱 보고서)	Stealthwatch System이 매일 관찰하는 시스템 전반의 트래픽 속도(FPS 단위)에 대한 그래픽과 테이블 형식 데이터를 보려면 Flow Collection Licensing Report(플로우 수집 라이선싱 보고서) 버튼을 클릭합니다. 이 정보를 사용하여 실제 사용량을 라이선스에서 허용하는 한도와 비교하는 방법을 결정할 수 있습니다.

기능 라이선스 상태

License Manager 대화 상자의 Feature License Status(기능 라이선스 상태) 섹션은 기능, SMC 및 관리되는 어플라이언스에 대한 정보를 제공합니다. 이 테이블에는 라이선스가 있는 각 어플라이언스의 탭이 나와 있습니다. 다음 정보는 이러한 각각의 탭에 대한 내용입니다.

항목	설명
Inventory Report(인벤토리 보고서)	라이선스에 대한 세부사항을 보려면 Inventory Report(인벤토리 보고서) 버튼을 클릭합니다. 이 보고서는 실제 라이선싱 요구 사항을 결정하는 데 도움을 줄 수 있습니다.
Feature(기능)	해당하는 경우 모델 번호를 포함하여 라이선스가 있는 Stealthwatch 제품의 유형입니다.
Appliance(어플라이언스)	라이선스와 연결되어 있는 어플라이언스의 이름 및 IP 주소입니다.
Count(개수)	라이선스가 허용하는 기능의 수입니다. 항목 *Uncounted(무수한)*는 "무제한"을 의미합니다.
Start Date(시작일)	이 값은 다음과 같이 다양한 요인에 따라 달라집니다. ▶ 영구, 평가 또는 서브스크립션 라이선스인 경우 이 날짜는 라이선스가 Download and License Center(다운로드 및 라이선스 센터)에서 프로비저닝된 날짜입니다. ▶ *Not Applicable(적용할 수 없음)* 값이 나타나는 경우, 이 기능이 시스템에 존재하지만 라이선스가 활성화되지 않은 것입니다. ▶ (물리적 어플라이언스에만 해당) 평가판 라이선스인 경우, 사용자가 어플라이언스를 처음으로 시작한 날짜입니다.
End Date(종료일)	라이선스가 만료되는 날짜입니다.
-계속-	

항목	설명
Status(상태)	각 라이선스의 상태입니다. 가능한 값은 다음과 같습니다. ▶ Installed(설치됨) - 이 기능이 시스템에 설치되었으며 라이선스가 활성화 상태입니다. ▶ Not Installed(설치되지 않음) - 이 기능이 시스템에 존재하지만 라이선스가 활성화되지 않았습니다. (시작일은 *Not Applicable(적용할 수 없음)* 상태를 표시합니다.) ▶ Expired(만료됨) - 다음 라이선스 중 하나가 만료되었습니다. • 평가판 라이선스 • 서브스크립션 라이선스 • 30일 평가판 라이선스 ▶ Trial(평가판) - (물리적 어플라이언스에만 해당) 라이선스가 30일 평가판 기간이 만료되기 전입니다.

3

SMC 클라이언트 인터페이스 탐색

개요

SMC 클라이언트 인터페이스는 네트워크 모니터링, 보호 및 분석을 지원하기 위해 방대한 규모로 수집되는 문서를 포함합니다. 일반적으로 이 문서 및 인터페이스의 일반 탐색 요소를 숙지하면 Stealthwatch를 더욱 능숙하게 사용할 수 있고 네트워크에서 이벤트를 보다 효율적으로 분석하는 데 도움이 됩니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 클라이언트 메모리 할당
- 관점
- 엔터프라이즈 트리 및 툴팁
- SMC 문서 열기
- 문서 작업
- 테이블 작업
- 차트 작업
- 문서 데이터 필터링
- 문서 인쇄
- 문서 저장
- 온라인 도움말
- 키보드 바로가기

클라이언트 메모리 할당

Client Memory Allocation(클라이언트 메모리 할당) 드롭다운 상자를 사용하여 클라이언트 컴퓨터에서 SMC Java 클라이언트 소프트웨어를 실행하도록 RAM(Random Access Memory)을 얼마나 할당할지 설정할 수 있습니다. 열려 있는 많은 문서 또는 대량의 데이터 집합(예: 100k 레코드 이상을 사용하는 플로우 쿼리)으로 작업하는 경우 메모리 할당을 늘려 보십시오.

컴퓨터는 선택한 메모리 할당의 최소 2배에 해당하는 RAM을 포함해야 합니다. 예를 들어 1024MB 컴퓨터의 경우 최대 512MB를 선택하고, 4GB 컴퓨터의 경우 2GB까지 선택할 수 있습니다.

최대 2048MB까지 할당할 수 있습니다. 최대 할당량을 선택하는 경우, 64비트 Java 기능을 사용하고 단일 버전의 Java만 설치되어 있어야 합니다.

팁:

- SMC 클라이언트 인터페이스가 자주 "중단" 상태로 나타나는 경우, 이 값을 늘려 보십시오.
- Java와 관련된 오류 메시지가 표시되면 메모리 할당을 줄여 보십시오.

관점

SMC 클라이언트 인터페이스에 로그인한 후 사용자에게 표시되는 보기는 로그인 권한(즉, 관점)에 따라 달라집니다. 이러한 이유로, 사무실에 있을 때 SMC 클라이언트 인터페이스에 표시되는 항목은 이 설명서에 표시되는 항목과 약간 다를 수 있습니다.

Stealthwatch 관리자는 로그인 권한을 User & Role Management(사용자 및 역할 관리) 대화 상자에서 정의합니다. 자세한 내용은 14장, "사용자 관리"를 참조해 주십시오.

직접 맞춤형 대시보드를 만들고 로그인 문서를 작성하거나 SMC 내에서 이미 설정되어 있는 대시보드를 선택할 수도 있습니다. 원하는 만큼 많은 맞춤형 대시보드를 생성할 수 있습니다. 대시보드는 표시하려는 데이터와 함께 SMC 구성 요소를 포함하는 다양한 보고서의 집합입니다. 대시보드를 통해 사용자가 보려는 주요 정보에 중점을 둘 수 있습니다.

참고:

- 로그인 문서 설정에 대한 자세한 내용은 310페이지의 "로그인 문서"(13장, "문서 작업"에 포함)를 참조하십시오.
- 대시보드 구축에 대한 자세한 내용은 5장, "보기 및 대시보드"를 참조하십시오.

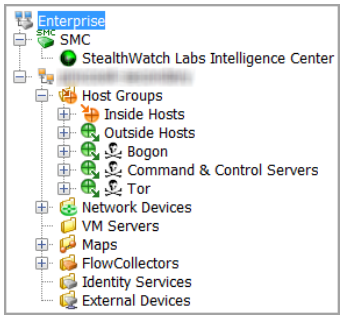
도메인 대시보드는 도메인에서 중요한 활동에 대한 그래픽 및 테이블 형식 데이터를 제공하므로 로그인 문서로 사용하도록 할 수 있는 문서의 예입니다. 이 데이터는 SMC에서 5분 간격으로 수집됩니다. 기본적으로 도메인 대시보드는 관리 사용자를 위한 로그인 문서로 사용하도록 자동으로 구성됩니다. 또한 새로운 사용자를 위해 예약된 문서로 바로 사용할 수 있습니다. 문서로 사용하려면 Stealthwatch 일일 보고서 일정을 활성화하고 이 문서를 포함시키면 됩니다.

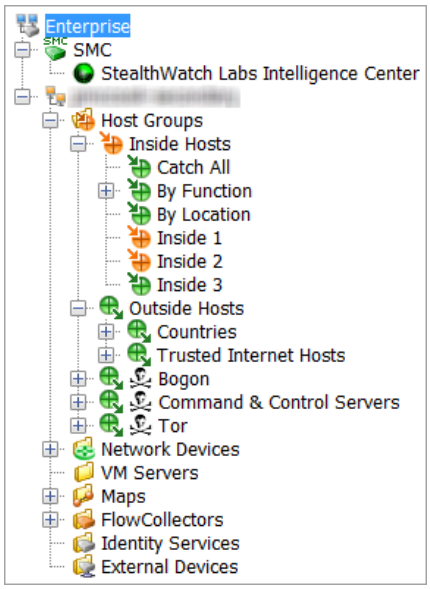
참고:

문서 활성화 및 일정 지정에 대한 자세한 내용은 349페이지의 "예약된 문서를 사용자 계정에 연결하기"(14장, "사용자 관리"에 포함)를 참조하십시오.

엔터프라이즈 트리 및 툴팁

SMC 클라이언트 인터페이스의 왼쪽 탐색 창에 있는 항목 리스트는 흔히 엔터프라이즈 트리라고 합니다. 또한 엔터프라이즈 페이지 또는 호스트 그룹 트리라고도 합니다. 이 트리는 기본적으로 모니터링되고 있는 네트워크의 구조를 표시합니다.





기본적으로 엔터프라이즈 트리의 옵션은 축소되어 있습니다. 트리에서 모든 옵션을 동시에 확장하려면 트리에서 항목을 마우스 오른쪽 버튼으로 클릭하고 **Expand All(모두 확장)**을 선택합니다. 모든 항목을 동시에 축소하려면 항목을 마우스 오른쪽 버튼으로 클릭하고 **Collapse All(모두 축소)**을 선택합니다. 엔터프라이즈 트리를 완전히 숨기려면 메인 메뉴로 이동하여 **View(보기) > Hide Tree(트리 숨기기)**를 클릭하거나 키보드에서 **Ctrl+T**를 누릅니다. SMC는 확장 및 축소된 폴더 설정을 저장합니다. 이렇게 하면 다음에 로그인할 때 엔터프라이즈 트리가 저장해둔 대로 나타납니다.

트리를 통한 검색

엔터프라이즈 트리에서 항목을 검색하려면 엔터프라이즈 트리의 맨 아래에 있는 Find(찾기) 필드(

)에 원하는 텍스트를 입력합니다.

참고:

Find(찾기) 필드는 기본적으로 숨겨져 있습니다. 이 필드를 처음에 열 때 **CTRL+F**를 클릭해야 다음에 SMC를 열 때마다 이 필드가 표시됩니다.

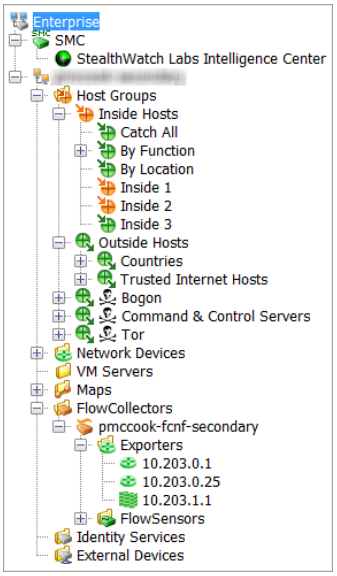
다음 방법 중 하나를 사용하여 원하는 텍스트의 추가 인스턴스에 대한 트리를 통해 앞뒤로 검색할 수 있습니다.

- Find(찾기) 필드의 오른쪽에서 아래로() 및 위로() 버튼을 클릭합니다.
- 키보드에서 아래쪽( ) 및 위쪽( ) 화살표 키를 누릅니다.

팁:

검색이 처리되는 동안 SMC에서 다른 작업을 계속해서 수행할 수 있습니다.

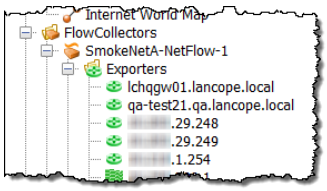
트리 브랜치



이 예에 나와 있는 엔터프라이즈 트리 브랜치는 엔터프라이즈 트리에 항상 있습니다. 이 브랜치는 SMC에서 모니터링되는 모든 도메인을 포함하는 모든 SMC 관리 옵션에 대한 최상위 수집 지점을 나타냅니다.

관점에 따라 SMC 브랜치가 있거나 없을 수 있습니다. 이 브랜치는 SMC 어플라이언스 자체를 나타냅니다. 시스템에서 페일 오버 SMC를 사용 중인 경우, 기본 및 보조 SMC 브랜치가 모두 표시됩니다.

다른 트리 브랜치는 연결된 호스트 그룹, Stealthwatch Flow Collector, Stealthwatch FlowSensor, VM(Virtual Machine) 서버(예: ESX 호스트), VM, 맵, 주변 디바이스 및 외부 디바이스와 함께 SMC 어플라이언스가 모니터링하는 도메인을 나타냅니다.



브랜치를 확장하려면 관련 더하기 기호()를 클릭합니다. 표시되는 브랜치 중 하나가 Flow Collector 브랜치입니다. 선택한 도메인에서 SMC 어플라이언스에 정보를 전송 중인 Flow Collector의 리스트를 보려면 관련 더하기 기호를 클릭하여 Flow Collector 브랜치를 확장합니다. 특정 Flow Collector에 대한 브랜치를 확장하는 경우, 관련 FlowSensor 어플라이언스, 엑스포터 및 방화벽을 볼 수 있습니다.

참고:

FlowSensor VE는 FlowSensor 브랜치와 VM 서버 브랜치 아래에 나타납니다.

알람 심각도 레벨

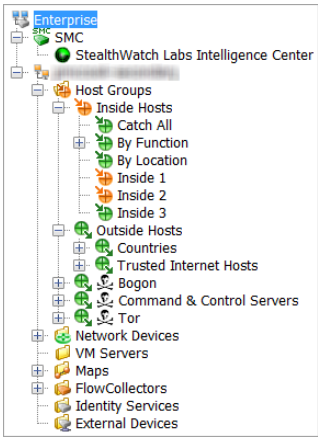
엔터프라이즈 트리 브랜치를 사용하면 표시된 알람 심각도 레벨의 정도에 따라 아이콘 색상이 변경되므로 네트워크의 어느 위치에 알람 조건이 있는지 즉시 확인할 수 있습니다. SMC를 보면 각 알람에 이미 기본적인 알람 레벨이 할당되어 있습니다. 그러나, 로그인 권한에 따라 Alarm Configuration(알람 컨피그레이션) 대화 상자를 사용하여 네트워크 환경의 요구 사항에 맞게 이러한 심각도 레벨 할당을 변경할 수 있습니다. 다음 테이블에는 특정 색상별로 표시되는 다양한 유형의 심각도 레벨이 나와 있습니다.

심각도 레벨	관련 색상
Critical(위험)	빨간색
Major(심각)	주황색
Minor(경미)	노란색
Trivial(단순)	파란색
Informational(정보)	하늘색
No Alarm Exists(알람 없음)	녹색

참고:

최상위 레벨 브랜치 아이콘은 낮은 레벨의 브랜치에서 발생하는 가장 높은 심각도 알람의 색상을 표시합니다.

메뉴를 보면서 스스로에게 다음 질문을 해 보십시오.



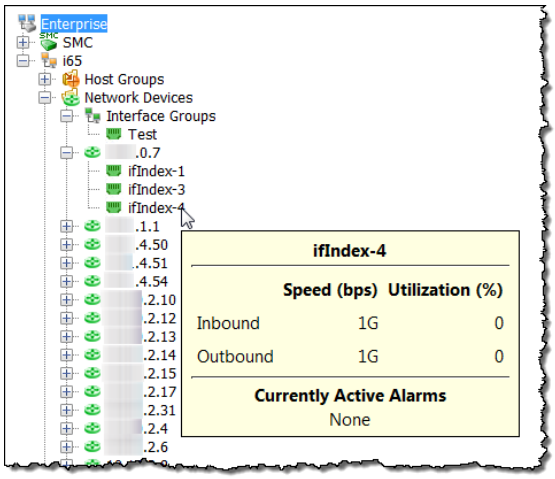
- 아이콘이 빨간색 또는 주황색인가요? 해당하는 경우, 위험 또는 심각 알람 조건이 있다는 것을 알 수 있습니다.
- 이 아이콘이 표시되나요? 해당하는 경우, 이 아이콘 옆에 있는 디바이스에 대한 연결이 손실되었습니다.
  - 내부 호스트 하위 트리를 확장하여 알람이 가장 중요하거나 가장 민감한 호스트 그룹에 존재하는지 확인할 수 있습니다.
  - 호스트 그룹 하위 트리에서 호스트 그룹 대시보드 문서(이 장 뒷부분에서 설명) 중 하나를 열어 자세한 내용을 확인할 수 있습니다.

- SMC 아이콘이 어떤 색상인가요? 녹색 또는 회색을 제외한 모든 색상은 SMC 어플라이언스에 시스템 알람이 있다는 것을 나타냅니다.

참고:

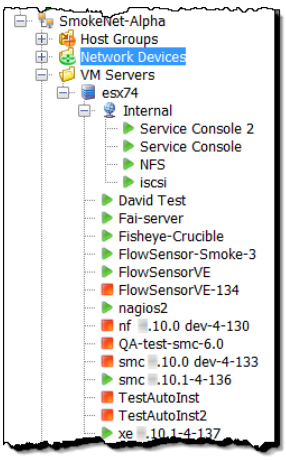
시스템은 1분에 한 번씩 엔터프라이즈 트리를 업데이트합니다. 그러나, 가장 최신 정보를 확인하려면 메인 메뉴로 이동하여 **View(보기) > Refresh Tree(트리 새로 고침)**를 클릭하여 언제든지 트리를 새로 고칠 수 있습니다. 또한 엔터프라이즈 트리에서 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 **Refresh Tree(트리 새로 고침)**를 선택할 수 있습니다.

엔터프라이즈 트리 표시기



브랜치 위에 커서를 올려 놓으면, 해당 개체에 발생한 총 알람 수와 각각에 대한 심각도 레벨을 표시하는 툴팁이 나타납니다. Flow Collector 브랜치의 경우 Stealthwatch 어플라이언스의 알람 정보 및 ID가 표시됩니다. 또한, SMC가 어플라이언스와 마지막으로 통신을 시도한 시기, SMC가 응답을 수신한 시기, 어플라이언스가 마지막으로 이벤트를 보고한 시기를 확인할 수 있습니다.

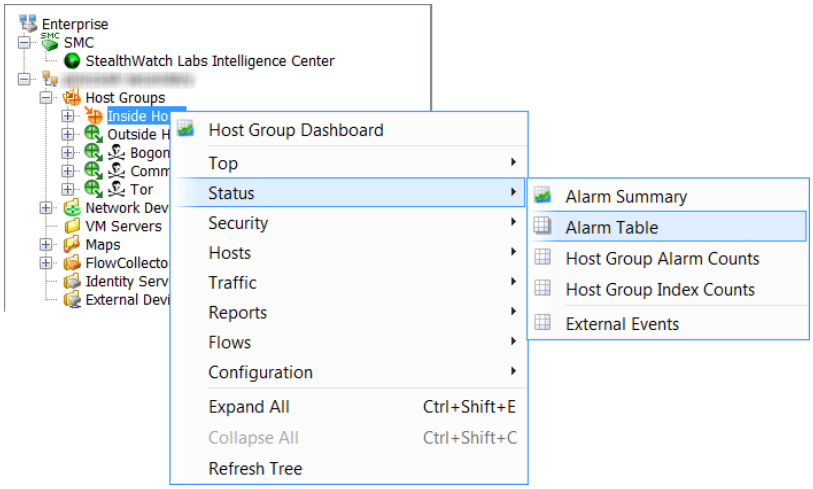
엔터프라이즈 트리에서는 알람 조건뿐만 아니라 VM의 상태도 확인할 수 있습니다. 다음 아이콘은 VM의 전원이 켜져 있는지 아니면 꺼져 있는지 또는 일시 중단 상태인지를 나타냅니다.



- – 전원이 켜져 있음
- – 전원이 꺼져 있음
- – 일시 중단됨

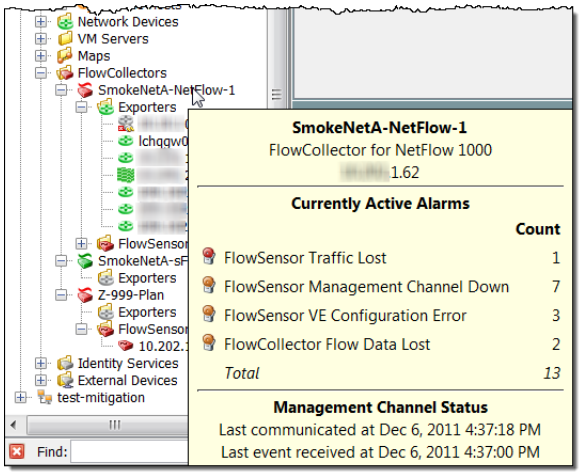
원형 아이콘()은 VM 서버 리소스 그룹을 나타냅니다. 지구 모양 아이콘()은 VM 서버 내부의 관리 요소를 나타냅니다.

브랜치를 마우스 오른쪽 버튼으로 클릭하고 **Status(상태) > Alarm Table(알람 테이블)**을 선택하면 해당 항목에 대한 알람 정보를 자세히 확인할 수 있습니다.

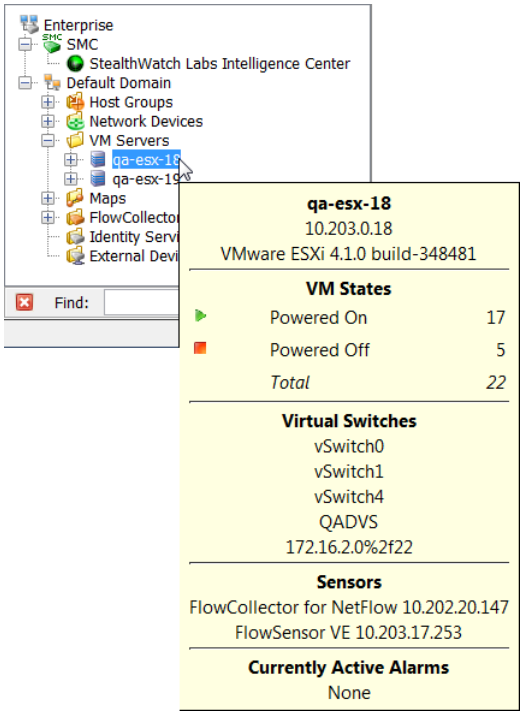


툴팁

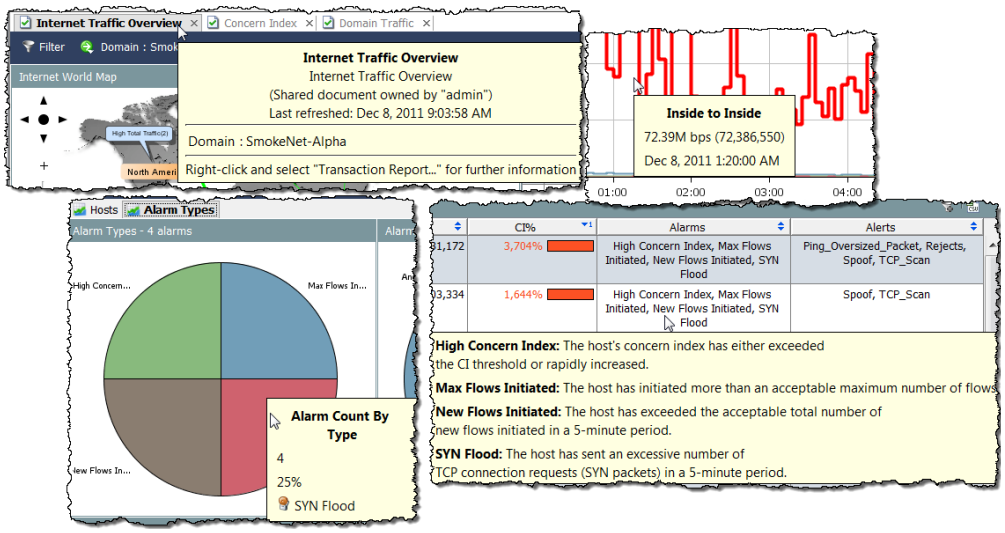
SMC 클라이언트 인터페이스의 다양한 요소 위에 커서를 올려 놓으면 툴팁에 해당 요소에 대한 요약 정보가 표시됩니다. 예를 들어 엔터프라이즈 트리에서 Flow Collector 이름 위에 커서를 올려 놓으면 Flow Collector가 트리거한 모든 알람 및 통신 상태와 함께 식별 정보를 확인할 수 있습니다.



마찬가지로, 시스템에서 VM 서버(즉, ESX 호스트)를 사용하는 경우, 엔터프라이즈 트리에서 VM 서버 이름 위에 커서를 올려 놓으면 이름, IP 주소 및 VM 서버에 관한 기타 정보와 함께 툴팁이 표시됩니다.



툴팁은 사실상 SMC 클라이언트 인터페이스의 모든 곳에 있습니다. 해당하는 툴팁을 확인하려면 요소(예: 탭, 그래프, 차트 또는 테이블 셀) 위에 커서를 올려 놓습니다.



SMC 문서 열기

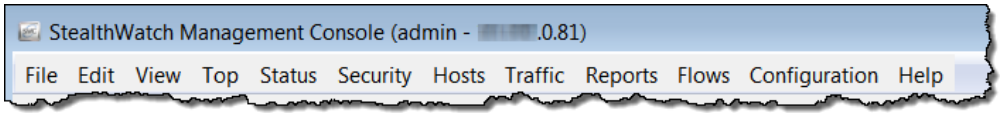
SMC 클라이언트 인터페이스를 통해 메인 메뉴를 사용하고 마우스 오른쪽 버튼으로 클릭 기능 등의 여러 가지 방법으로 문서를 열 수 있습니다.

참고:

문서는 보고서라고도 합니다. 이러한 용어가 동일한 의미로 사용되는 예가 이 사용 설명서에 나와 있습니다.

메인 메뉴

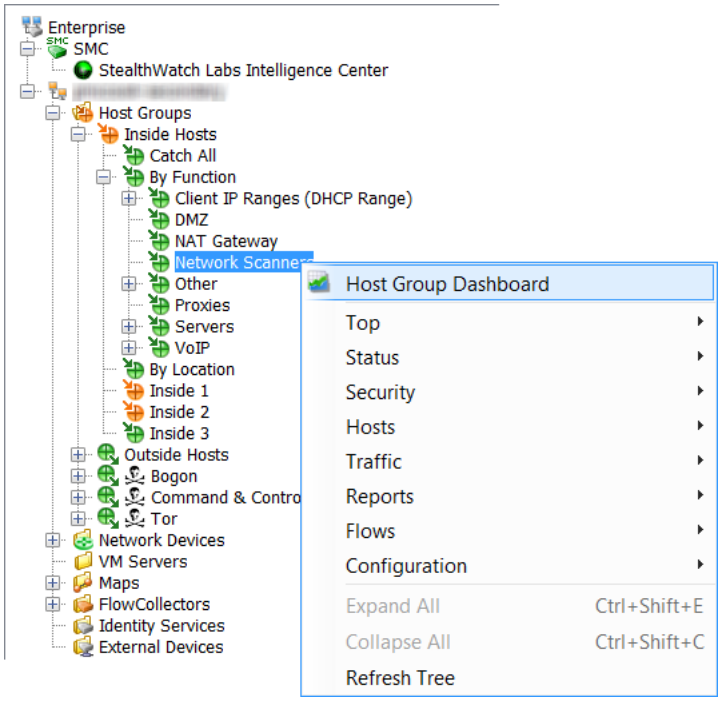
메인 메뉴에서 메뉴 항목을 클릭하여 문서를 열 수 있습니다.



사용할 수 있는 옵션은 다음의 세 가지 기본 요소에 따라 다릅니다.

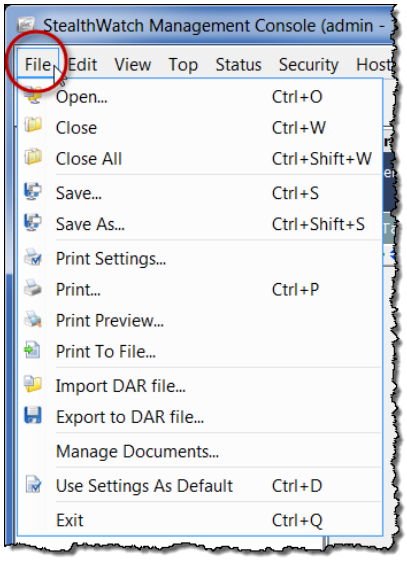
- 엔터프라이즈 트리에서 클릭한 항목
- 특정 SMC 문서에서 클릭한 항목
- 로그인 권한

예를 들어, 엔터프라이즈 트리에서 호스트 그룹을 클릭한 다음 **Host Group Dashboard(호스트 그룹 대시보드)**를 마우스 오른쪽 버튼으로 클릭하면 해당 호스트 그룹에 대한 데이터만 표시됩니다.



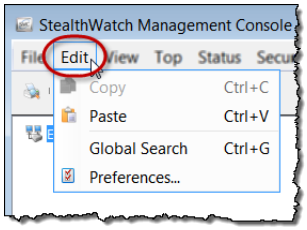
파일 메뉴

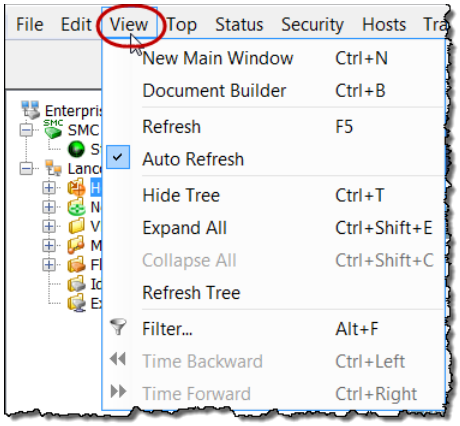
File(파일) 메뉴는 문서 열기, 닫기, 저장, 인쇄 및 다른 사용자와 공유와 같은 SMC 문서 작업을 위한 옵션을 제공합니다.



편집 메뉴

Edit(편집) 메뉴는 복사, 붙여넣기 및 데이터 검색뿐만 아니라 특정 디스플레이 기본 설정에 대한 정의 옵션을 제공합니다.



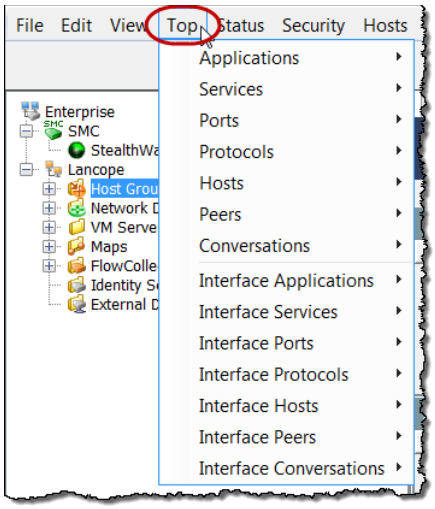


보기 메뉴

View(보기) 메뉴를 사용하여 SMC 사용자 인터페이스의 새 인스턴스를 열고 맞춤형 대시보드를 구축하고 자동 새로 고침 기능을 중지하거나 시작하고 데이터를 수동으로 새로 고치고 다양한 방식으로 엔터프라이즈 트리를 표시하거나 모두 숨기고 데이터를 필터링하거나 이전 기간 또는 이후 기간에 해당하는 데이터를 표시할 수 있습니다.

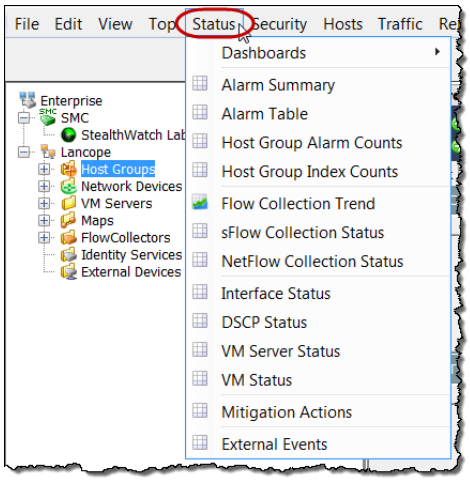
최상위 메뉴

Top(최상위) 메뉴를 사용하여 가장 자주 사용되는 애플리케이션, 가장 자주 사용되는 서비스, 가장 자주 사용되는 포트, 가장 활성화된 호스트 등의 특정한 기준에 기초하여 가장 자주 사용되는 데이터를 표시할 수 있습니다. 이러한 데이터를 전체 네트워크에서 보거나 인바운드 트래픽, 아웃바운드 트래픽, 도메인이나 호스트 그룹 내부 트래픽 또는 특정 인터페이스를 이동하는 트래픽에 따라 세분화할 수 있습니다.



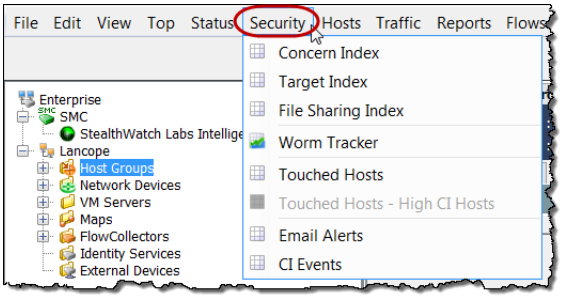
상태 메뉴

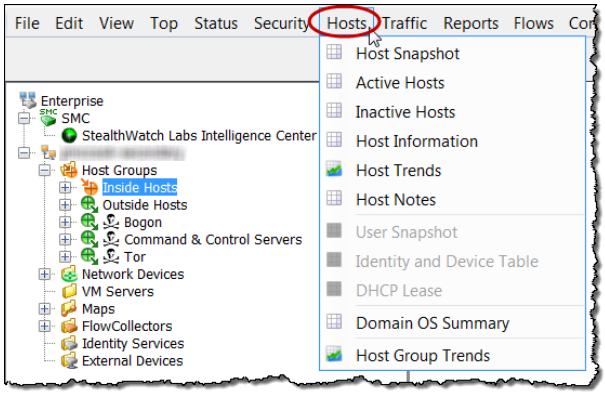
Status(상태) 메뉴는 알람, 트래픽, 가능한 데이터 손실, 인터페이스, VM, 외부 이벤트 등의 특정한 조건에 기초하여 네트워크의 여러 부분에 대한 상태를 표시하기 위한 옵션을 제공합니다.



보안 메뉴

Security(보안) 메뉴를 사용하여 상위 관심도 호스트, 표적이 되는 호스트, 파일 공유 활동, 웜 활동과 비정상적인 이메일 트래픽과 같은 보안 문제와 관련된 데이터를 확인합니다.



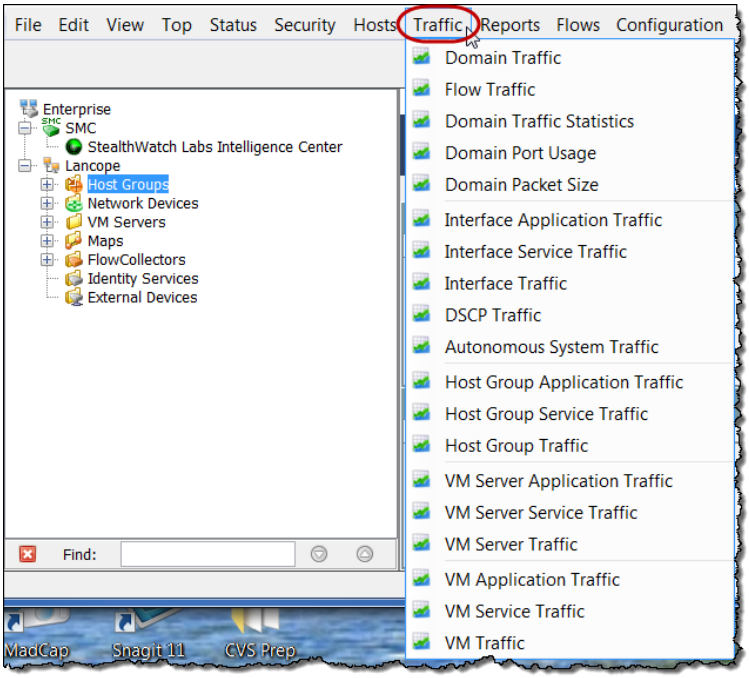


호스트 메뉴

Host(호스트) 메뉴는 개별 호스트 활동, 호스트 행동의 트렌드, 활성 또는 비활성 호스트, 호스트 사용자 ID 등 호스트와 관련된 데이터를 표시하기 위한 옵션을 제공합니다.

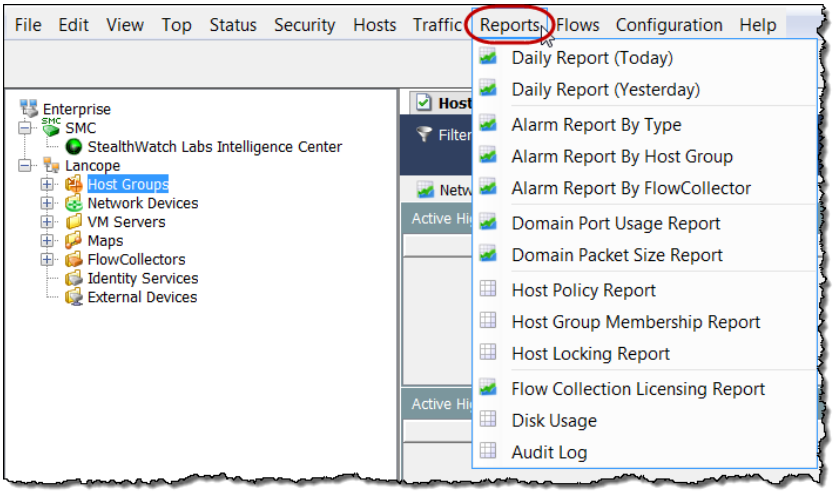
트래픽 메뉴

Traffic(트래픽) 메뉴를 사용하면 도메인, 인터페이스, 호스트 그룹, 애플리케이션, 서비스, 포트, VM 등의 다양한 방법으로 세분화된 트래픽 정보를 확인할 수 있습니다.



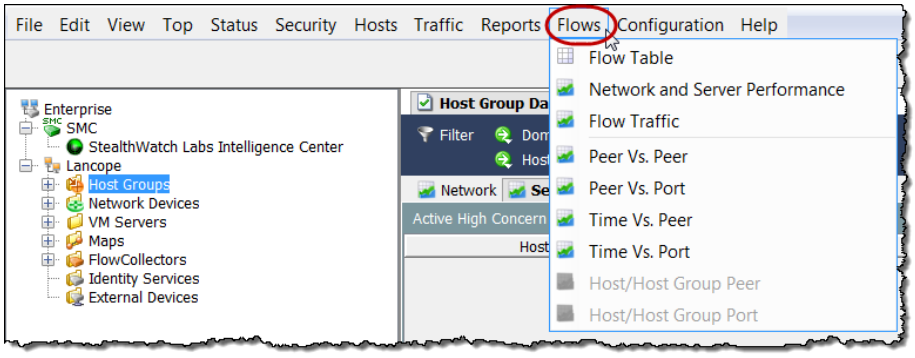
보고서 메뉴

Reports(보고서) 메뉴를 사용하면 도메인 활동에 대한 일일 요약, 또는 유형, 호스트 그룹 또는 Flow Collector에 따라 발생한 알람에 대한 보고서와 같은 Stealthwatch 데이터베이스에 대해 쿼리를 실행할 수 있습니다.



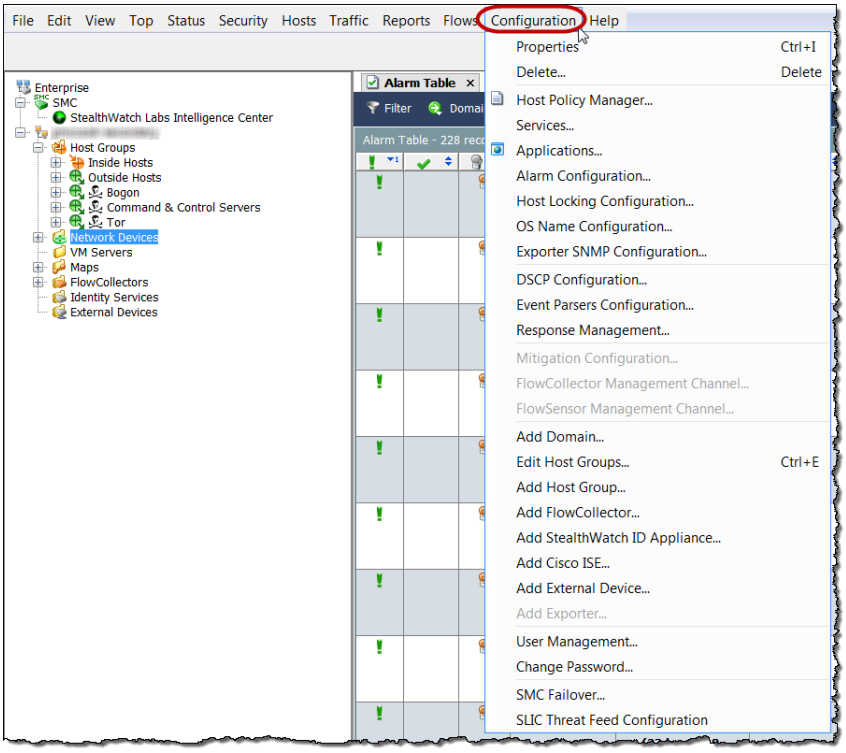
플로우 메뉴

이름이 의미하는 바와 같이 Flow(플로우) 메뉴는 네트워크 및 서버 성능 플로우 데이터를 포함하여 플로우를 분석하는 다양한 방법을 제공합니다.



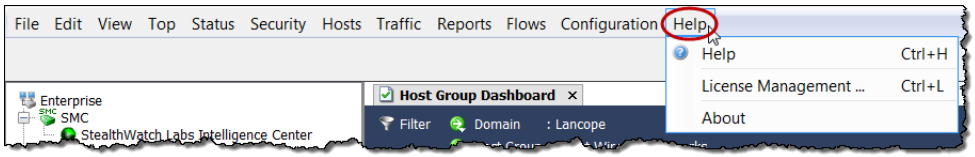
컨피그레이션 메뉴

Configuration(컨피그레이션) 메뉴에는 Stealthwatch에서 사용할 수 있는 대부분의 컨피그레이션 옵션이 포함되어 있습니다. 도메인, 어플라이언스, 호스트 그룹, 정책, 애플리케이션 또는 서비스 정의를 추가, 편집 또는 삭제하여 원하는 대로 모니터링되는 네트워크를 구성하거나 세분화할 수 있습니다. 사용자 및 사용자의 로그인 권한을 추가, 편집 또는 삭제하여 액세스를 제한할 수도 있습니다. Stealthwatch System은 알람 심각도 레벨의 기본 집합을 사용합니다. 원하는 경우, 조직의 요구에 따라 이 집합을 변경할 수 있습니다.



도움말 메뉴

Help(도움말) 메뉴에는 *SMC 클라이언트 온라인 도움말*과 SMC 클라이언트 소프트웨어의 버전, 라이선스 및 설명과 관련된 정보가 포함되어 있습니다. 온라인 도움말 사용 시 이점에 대해서는 곧 자세히 다룰 것입니다.

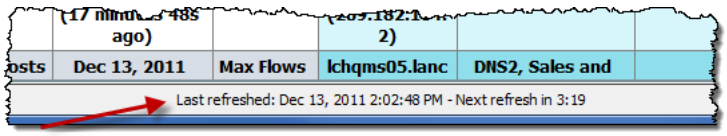


문서 작업

SMC 문서에 나타나는 몇 가지 공통 탐색 요소에 대해 살펴보겠습니다.

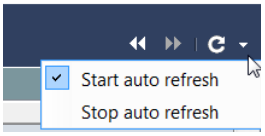
라이브 데이터와 정적 데이터 표시 비교

SMC 어플라이언스는 Stealthwatch Flow Collector에서 데이터를 수집하며 대부분의 SMC 문서에서 데이터를 자동으로 새로 고칩니다. 따라서 항상 비교적 최신 정보를 확인할 수 있습니다. 창의 맨 아래에 있는 카운터를 보고 다음 번 자동 새로 고침이 언제 수행되는지 확인할 수 있습니다.



Refresh(새로 고침) 버튼( )은 문서 헤더의 맨 오른쪽에 위치해 있습니다. 이 버튼을 클릭하면 활성 문서가 새로 고쳐지고 최신 데이터로 라이브 상태가 되며 자동 새로 고침 기능이 다시 설정됩니다.

장기간 정보를 확인하려는 경우, 문서를 정적으로 설정할 수 있습니다.

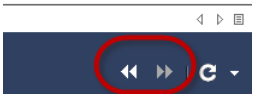


드롭다운 메뉴에서 다음 옵션 중 하나를 클릭하여 문서를 정적 또는 라이브로 설정할 수 있습니다.

- 자동 새로 고침 시작 - 이 문서는 현재 라이브(활성) 상태입니다. 자동 새로 고침 간격이 만료되면 SMC 소프트웨어는 문서를 새 데이터로 업데이트합니다.
- 자동 새로 고침 중지 - 이 문서는 현재 정적(비활성) 상태입니다.

팁:

언제든지 **Refresh(새로 고침)** 버튼을 클릭하여 데이터 업데이트를 트리거할 수 있습니다.



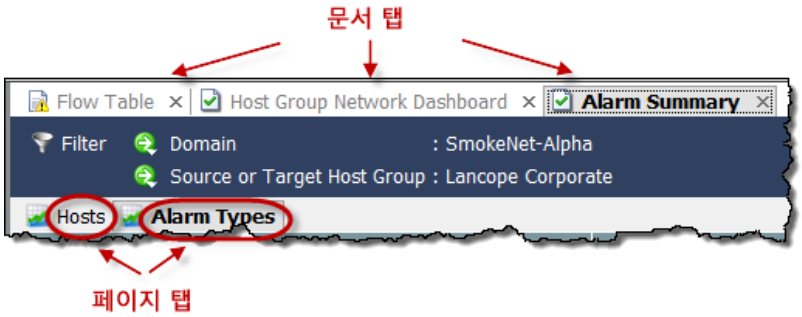
문서 헤더의 맨 오른쪽에는 View Earlier Data(이전 데이터 보기) 버튼( )과 View Later Data(이후 데이터 보기) 버튼( )도 위치해 있습니다. 이러한 버튼을 클릭하면 Filter(필터) 대화 상자에 설정된 시간 증가 값에 따라 데이터를 각각 뒤로 또는 앞으로 이동할 수 있습니다.

팁:

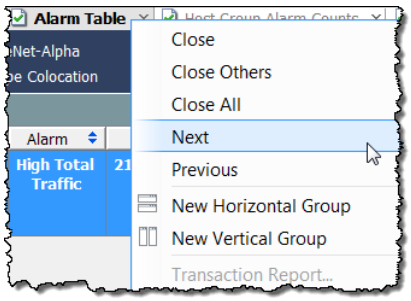
- 데이터 전체에서 시간을 빠르게 뒤로 이동시키려면 **Ctrl+좌측 화살표**를 누릅니다.
- 데이터 전체에서 시간을 빠르게 앞으로 이동시키려면 **Ctrl+우측 화살표**를 누릅니다.

탭과 한 문서에서 다른 문서로 이동

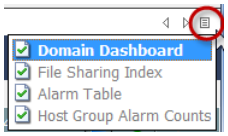
SMC 클라이언트 인터페이스에서 여러 문서를 동시에 열 수 있습니다. 각 문서는 다른 문서와 탭으로 분리됩니다. 다음 예에 표시된 Alarm Summary(알람 요약)와 같이 일부 문서에는 여러 페이지가 있으며, 이 페이지 또한 탭으로 분리됩니다.



여러 가지 방법으로 한 문서에서 다음 문서로 이동할 수 있습니다. 원하는 문서 탭을 클릭하고 문서 탭을 마우스 오른쪽 버튼으로 클릭한 후 **Next(다음)** 또는 **Previous(이전)**를 선택하거나 **Alt** 키와 키보드에 있는 왼쪽 ← 또는 오른쪽 → 화살표 키 중 하나를 동시에 누릅니다.

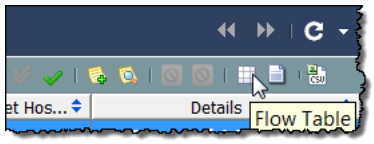


열려 있는 문서가 너무 많아 일부 탭을 볼 수 없는 경우, 탭의 오른쪽에 있는 오른쪽 ▶ 또는 왼쪽 ◀ 화살표를 클릭하여 한 문서를 다른 위치로 이동할 수 있습니다. 또한 List(리스트) 버튼 ☰을 클릭하여 드롭다운 리스트에서 열려 있는 문서를 클릭할 수 있습니다.



활성 문서는 현재 사용자가 보고 있는 문서입니다. 활성 문서의 제목은 항상 검은색이며 굵게 표시됩니다. 활성 문서는 해당하는 새로 고침 간격에 따라 자동으로 새로 고쳐집니다. 비활성 문서는 자동으로 새로 고쳐지지 않습니다. 비활성 문서를 활성으로 설정한 다음 수동으로 새로 고쳐야 합니다. 새로 고침이 시작되면 새로 고침이 완료될 때까지 기다릴 필요 없이 다른 문서를 탐색할 수 있습니다.

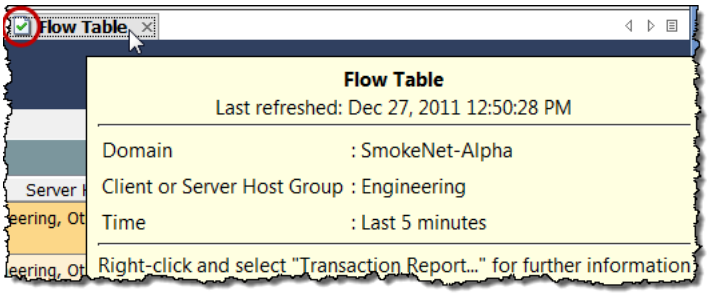
많은 문서에는 문서의 특정 기능을 지닌 버튼이 있는 고유한 툴바가 있습니다. 버튼 위에 커서를 올려 놓으면 버튼을 설명하는 툴팁을 확인할 수 있습니다.



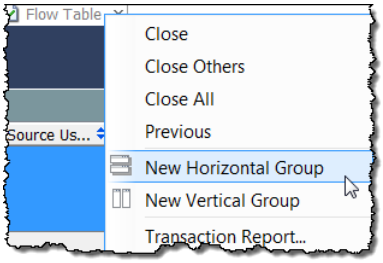
각 문서 탭에는 문서의 새로 고침 상태를 나타내는 아이콘이 있습니다(다음 예에서 동그라미로 표시된 영역 참조). 비활성 문서가 새로 고침을 완료하면 탭 텍스트의 색상이 새로 고침 상태를 나타내도록 변경됩니다. 다음 아이콘은 사용할 수 있는 다른 새로 고침 상태를 나타냅니다.

- 작업 중 - 문서를 새로 고치는 중이거나 다른 작업을 수행하는 중입니다.
- 새로 고침 완료 - 마지막 새로 고침이 성공적으로 완료되었으며 비활성 탭 텍스트가 녹색입니다.
- 새로 고침 완료(오류 포함) - 마지막 새로 고침이 성공적으로 완료되었지만 오류가 발생했거나 더 많은 정보를 사용할 수 있으며 비활성 탭 텍스트가 노란색입니다.
- 오류 - 마지막 새로 고침을 완료하는 데 실패했으며 비활성 탭 텍스트가 빨간색입니다.

문서 탭 위에 커서를 올려 놓으면 해당 문서에 대한 요약 정보를 제공하는 툴팁이 표시됩니다.



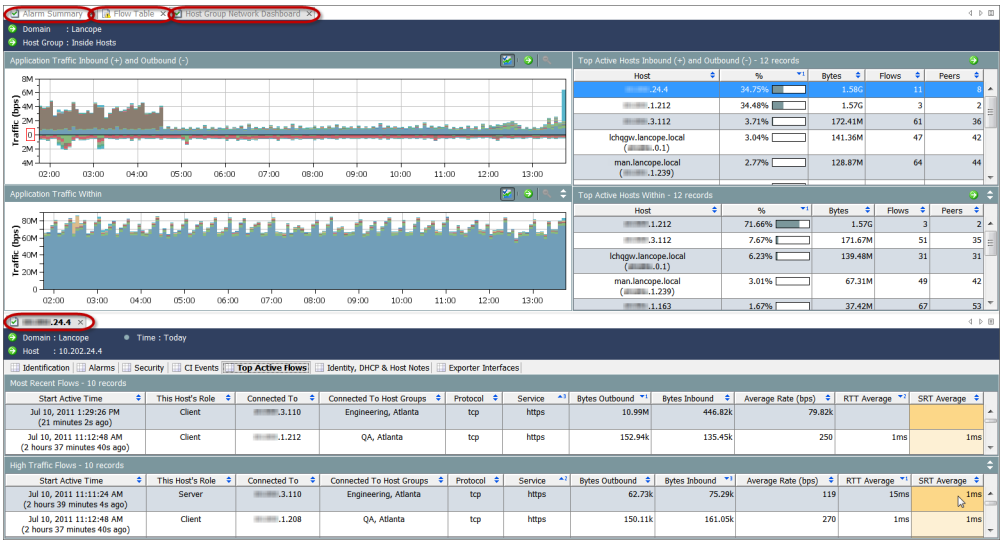
문서 방향 변경



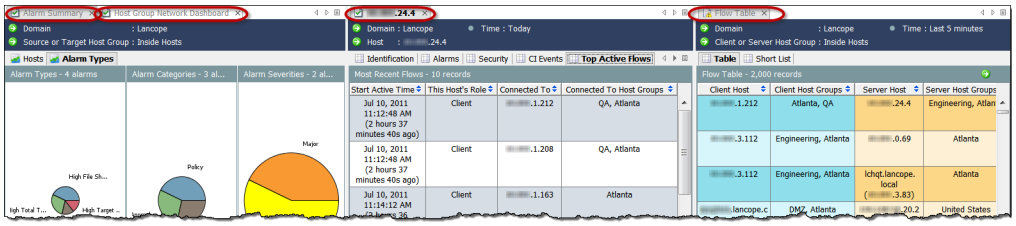
기본적으로 여러 문서를 열면 탭별로 간격이 띄워진 상태로 문서가 다른 문서 뒤에 하나씩 표시됩니다. 원하는 경우 서로 아래에(수평) 또는 서로 옆에(수직) 표시되도록 이 방향을 변경할 수 있습니다. 문서 탭을 마우스 오른쪽 버튼으로 클릭하고 **New Horizontal Group(새 수평 그룹)** 또는 **New Vertical Group(새 수직 그룹)** 중 하나를 클릭하여 원하는 방향을 선택합니다.

원하는 방향에 따라 나타나는 결과는 다음 예 중에서 하나와 유사합니다.

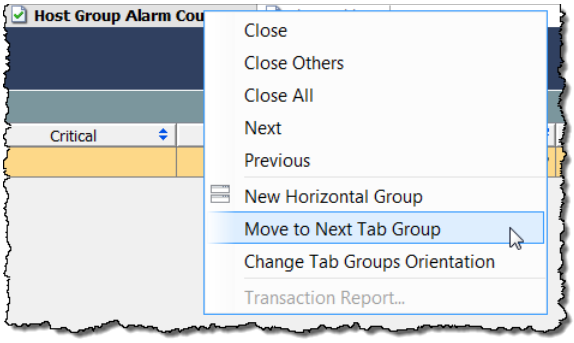
수평 그룹



수직 그룹



현재 방향에 따라 원하는 배열을 얻을 때까지 문서 탭을 마우스 오른쪽 버튼으로 클릭하고 **Move to Next Tab Group(다음 탭 그룹으로 이동)**, **Move to Previous Tab Group(이전 탭 그룹으로 이동)** 또는 **Change Tab Groups Orientation(탭 그룹 방향 변경)**을 선택하여 문서를 한 탭 그룹에서 다른 탭 그룹으로 이동할 수 있습니다. 또한 열려 있는 문서 중에서 문서 탭을 클릭하고 한 위치에서 다른 위치로 끌어올 수 있습니다.



문서 헤더

문서 헤더에는 문서가 제공하는 데이터에 대한 정보가 포함되어 있습니다.

플로우 테이블 헤더는 이전 예에 나와 있습니다. 헤더는 관련된 호스트가 위치한 도메인뿐만 아니라 호스트 그룹 이름도 나열합니다. 또한 제공되는 데이터가 언제 캡처되었는지 확인할 수 있습니다.

따라서 이 예에 나와 있는 데이터가 SmokeNet-Alpha 도메인의 내부 호스트라는 호스트 그룹에서 발생하고 있는 플로우에 대한 것임을 알 수 있습니다. 문서에 표시된 데이터는 지난 12시간 동안 캡처되었습니다. 필터를 사용하여 이러한 파라미터를 변경할 수 있습니다. 이 내용에 대해서는 곧 살펴볼 것입니다.

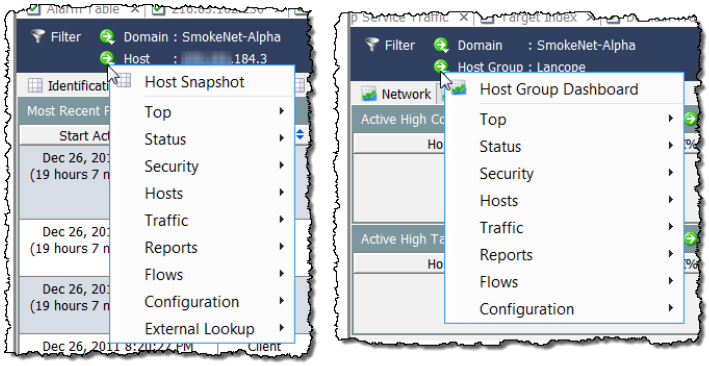
문서로 이동 버튼

Go to Document(문서로 이동) 버튼 은 문서 헤더와 SMC 클라이언트 인터페이스 전체의 툴바에 표시됩니다. 이 버튼을 클릭할 때 표시되는 항목은 버튼과 연결된 개체에 따라 다릅니다.

문서 헤더에서

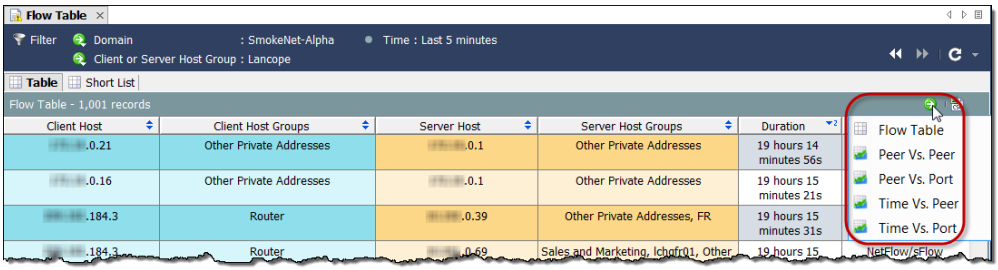
예를 들어, 문서 헤더에서 호스트 IP 주소 옆에 있는 **Go to Document(문서로 이동)** 버튼을 클릭할 경우, 호스트와 관련된 문서 옵션의 리스트가 표시됩니다. 이러한 옵션 중 하나를 클릭할 경우, 표시되는 데이터는 특정 호스트에만 관련이 있습니다.

마찬가지로, 헤더에서 호스트 그룹 이름 옆에 있는 **Go to Document(문서로 이동)** 버튼을 클릭할 경우, 해당 호스트 그룹과 관련된 문서 옵션의 리스트가 표시됩니다. 이러한 옵션 중 하나를 클릭할 경우, 표시되는 데이터는 특정 호스트 그룹에만 관련이 있습니다.

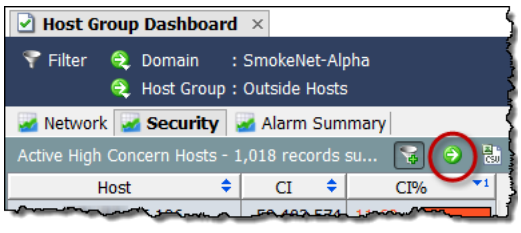


문서 툴바에서

문서 툴바에 나타나는 Go to Document(문서로 이동) 버튼을 사용하면 다양한 방식으로 표시한 데이터를 볼 수 있습니다. 예를 들어, 특정 호스트 그룹에 대한 플로우 테이블을 보고 있다고 가정하겠습니다. 플로우 테이블 툴바에 나타나는 **Go to Document(문서로 이동)** 버튼을 클릭할 경우, 해당 플로우와 관련된 문서 옵션의 리스트가 표시됩니다. 이러한 옵션 중 하나를 클릭할 경우, 이 플로우 정보는 다양한 형식으로 표시됩니다.

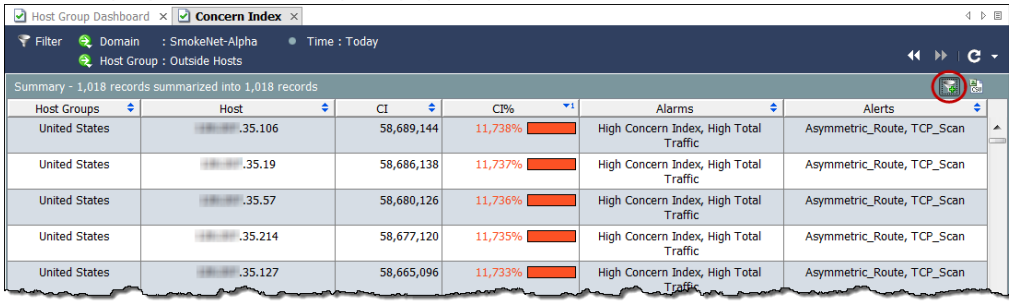


경우에 따라 보고 있는 데이터와 관련된 문서가 하나만 있습니다. 이 경우, **Go to Document(문서로 이동)** 버튼을 클릭하면 해당 문서가 즉시 열립니다.



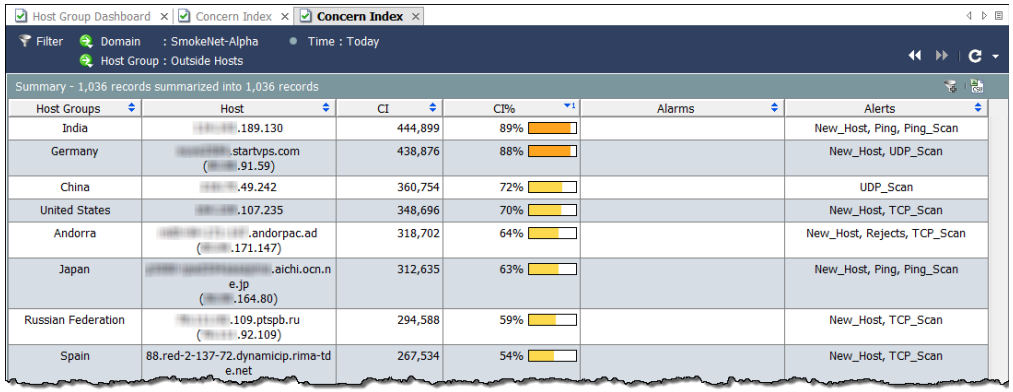
예를 들어 호스트 그룹 대시보드에 있는 각 구성 요소에는 Go to Document(문서로 이동) 버튼이 있는 고유한 툴바가 포함되어 있습니다. 활성 상위 관심도 호스트 구성 요소의 버튼을 클릭할 경우, 호스트 그룹 대시보드의 해당 구성 요소에서 표시되는 정보에만 관련된 데이터를 표시하도록 SMC는 즉시 사전 필터링된 관심 지표(CI) 문서를 엽니다.

관심 지표(CI) 문서는 마지막 아카이브 시간 이후에 가장 높은 CI 점수를 지닌 호스트에 대한 정보를 표시합니다.



관심 지표(CI) 문서를 열 경우, 기본적으로 Concern Index(관심 지표) 필터 버튼(문서의 오른쪽 상단 모서리에 있음)이 활성화되고 관심 지표는 활성 상위 관심 지표 알람(즉, 100보다 높은 CI 퍼센트를 지닌 알람)을 지닌 호스트만 보여줍니다. CI 퍼센트가 50을 초과하는 호스트만 보려면 **Concern Index(관심 지표) 필터** 버튼을 클릭합니다.

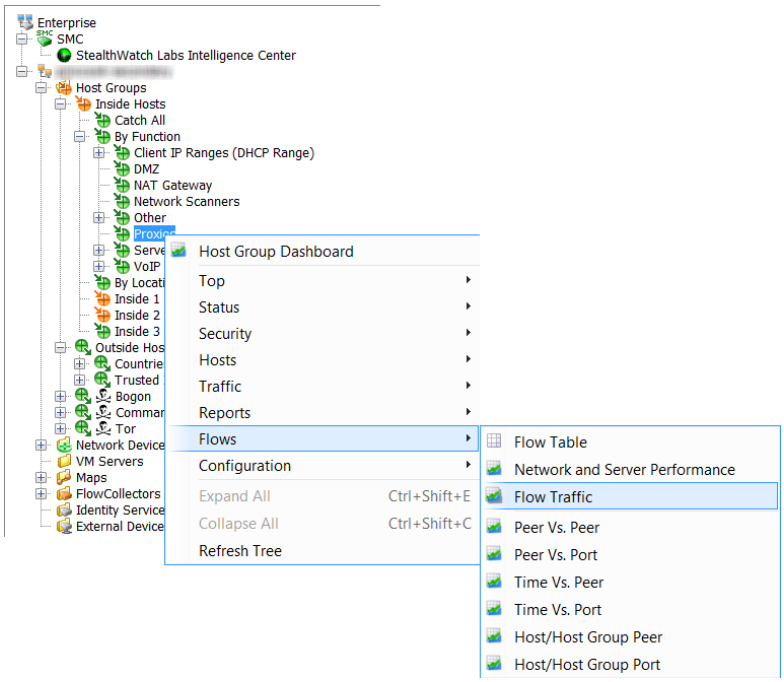
Concern Index(관심 지표) 필터 버튼의 더하기 기호가 회색()으로 변하고 CI 퍼센트가 50을 초과하는 호스트만 나타납니다.



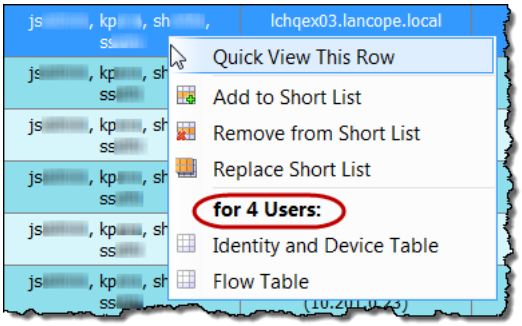
빠른 탐색을 위한 마우스 오른쪽 버튼으로 클릭

SMC 클라이언트 인터페이스를 통해 제공되는 마우스 오른쪽 버튼으로 클릭 기능은 문서 열기를 위한 대안을 제공합니다. 오른쪽 버튼으로 클릭 메뉴는 보통 메인 메뉴에서 작업을 수행하는 것보다 더 빠르게 가장 구체적인 데이터를 찾는 데 도움이 됩니다.

엔터프라이즈 트리에서 요소를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 원하는 문서를 선택합니다. 이 시점에 표시되는 데이터는 클릭하는 요소와 구체적으로 관련이 있습니다. 예를 들어, 엔터프라이즈 트리에서 호스트 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Flows(플로우) > Flow Traffic(플로우 트래픽)**을 선택할 경우, 표시되는 플로우 트래픽 데이터는 해당 호스트 그룹과 구체적으로 관련이 있습니다.



문서를 여는 또 다른 방법은 문서 내에서 마우스 오른쪽 버튼으로 클릭하고 나타나는 팝업 메뉴에서 원하는 항목을 선택하는 것입니다. 예를 들어 문서의 열 내에서 사용자 이름(하나 또는 여러 개)을 마우스 오른쪽 버튼으로 클릭할 경우, 다음과 같은 팝업 메뉴가 나타납니다.



팝업 메뉴(이전 이미지에서 동그라미로 표시된 부분)에서 레이블은 해당 레이블 아래에 나열된 문서를 필터링하는 데 사용할 수 있는 사용자의 수를 나타냅니다. 이름을 하나만 클릭할 경우 해당 레이블은 사용자 이름을 나타냅니다.

참고:

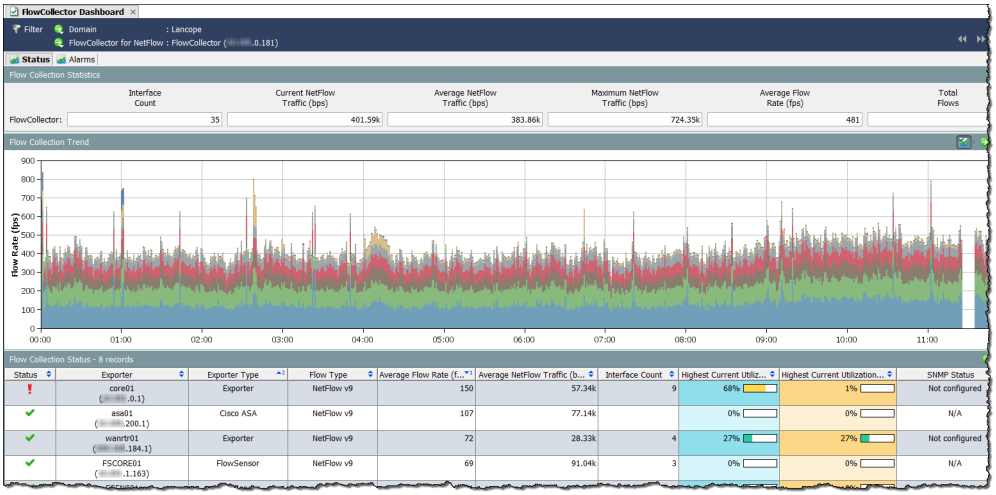
- 또한 테이블 셀에서 항목을 더블 클릭하고 **Go to Document(문서로 이동)** 버튼을 클릭하여 문서를 열 수 있습니다.

선택한 문서에 대한 더블 클릭 기능

더블 클릭 기능은 선택한 문서를 열기 위한 대안을 제공합니다. 엔터프라이즈 트리에서 브랜치를 더블 클릭하여 열 수 있는 문서에 대해서는 다음 테이블을 참조하십시오.

엔터프라이즈 트리에서 이 브랜치를 더블 클릭할 경우...	열리는 문서
SMC 폴더	SMC 대시보드
특정 호스트 그룹	호스트 그룹 대시보드
내부/외부 호스트 폴더	호스트 그룹 대시보드
네트워크 디바이스 폴더 또는 특정 네트워크 디바이스	인터페이스 상태
엑스포터 폴더 또는 특정 엑스포터	인터페이스 상태
특정 인터페이스	인터페이스 요약 대시보드
Flow Sensor 폴더	인터페이스 상태
VM 서버 폴더	VM 서버 상태
특정 VM	VM 트래픽
특정 맵	특정 맵
특정 Cisco ASA 엑스포터	ASA에서 필터링된 마지막 5분 동안의 플로우 테이블
Cisco ASA 방화벽(예: Palo Alto 방화벽)이 아닌 모든 방화벽	인터페이스 상태
방화벽 인터페이스	인터페이스 요약 대시보드
특정 Flow Collector	Flow Collector 대시보드
특정 Cisco ISE	ID 및 디바이스 테이블
특정 ID	사용자 ID 필터 대화 상자
특정 외부 디바이스	외부 이벤트

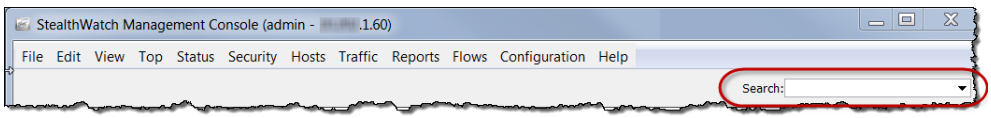
예를 들어 Flow Collector를 더블 클릭할 경우, 해당 Flow Collector에 대한 Flow Collector 대시보드가 열립니다.



문서 검색

SMC를 사용하여 엔터프라이즈 트리의 항목 검색 외에 특정 항목에 대한 모든 문서(모든 도메인에서)를 검색할 수 있습니다. 기본 툴바의 Search(검색) 필드에서 전체 문자열, 부분 문자열 또는 와일드카드(*)가 포함된 부분 문자열을 사용하여 다음 항목을 검색할 수 있습니다.

- 알람 ID
- 호스트 또는 엑스포터 IP 주소
- 다음 이름을 사용합니다.
  - 엑스포터
  - 호스트 그룹
  - 서버
  - 사용자
  - VM
  - VM 서버

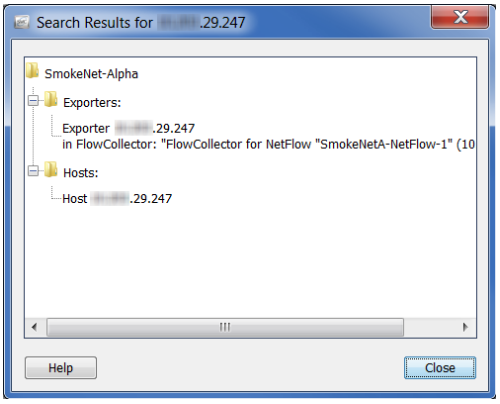


참고:

- 검색 결과는 사용자 이름과 관련된 데이터 역할 및 기능 역할에 따라 제한됩니다.

팁:

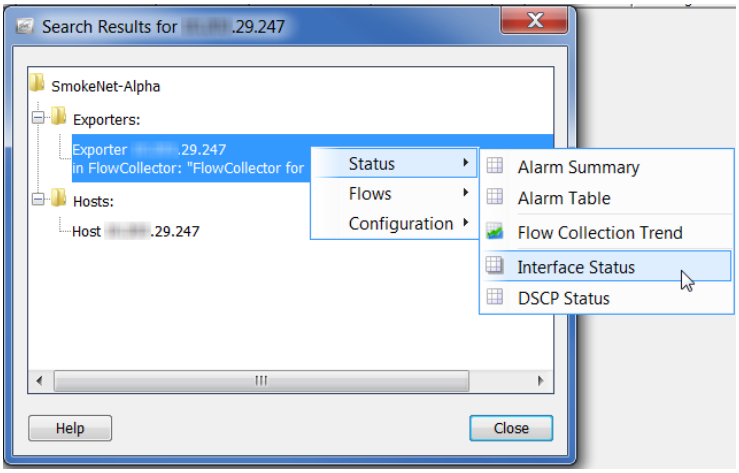
Search(검색) 드롭다운 리스트 상자를 사용하여 이전에 검색한 항목을 선택한 다음 **Enter** 키를 눌러 검색을 실행할 수 있습니다.



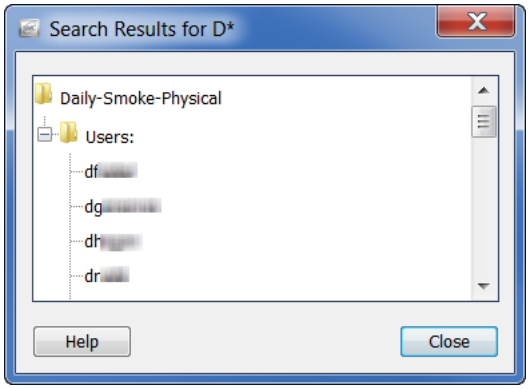
예를 들어 Search(검색) 필드에 엑스포터의 IP 주소를 입력한 다음 키보드에서 **Enter** 키를 누르면 Search Results(검색 결과) 대화 상자가 SMC에서 해당 IP 주소가 나타나는 위치 리스트를 표시합니다.

대부분의 경우, 리스트에서 IP 주소를 더블 클릭하여 해당 항목에 대한 특정 문서를 표시할 수 있습니다. 예를 들어, Host(호스트) 항목 아래에서 IP 주소를 더블 클릭하면 해당 IP 주소에 대한 호스트 스냅샷이 표시됩니다.

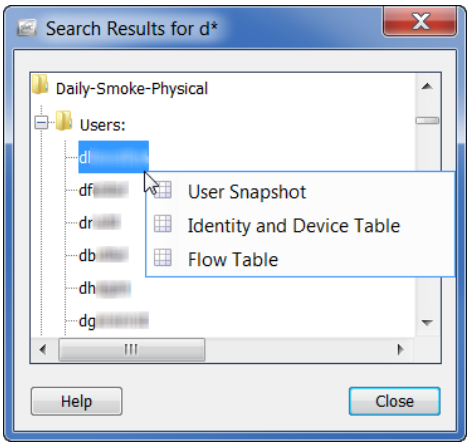
또한 해당 IP 주소와 관련이 있으며 사용자가 액세스할 수 있는 기타 정보 문서의 리스트를 보려면 IP 주소를 마우스 오른쪽 버튼으로 클릭하면 됩니다.



사용자 이름을 검색할 때 각 사용자 이름이 Search Results(검색 결과) 대화 상자에서 "Users(사용자)" 폴더 안에 개별 항목으로 나타납니다.



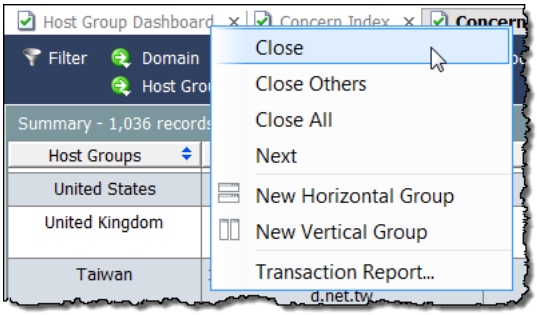
사용자 이름을 더블 클릭할 경우, Identity and Device Table(ID 및 디바이스 테이블)이 사용자에 대해 사전 필터링된 상태로 열립니다. 사용자 이름을 마우스 오른쪽 버튼으로 클릭하면 다음 팝업 메뉴가 나타나며, 이 메뉴에서 해당하는 사용자에 대해 사전 필터링할 문서를 선택할 수 있습니다.



문서 닫기

SMC 문서를 여는 방법과 마찬가지로 닫는 방법에도 여러 가지가 있습니다. 문서를 하나 닫으려면 문서 탭의 오른쪽 모서리에서 **X**를 클릭합니다. 또는 메인 메뉴에서 키보드에 있는 **File(파일) > Close(닫기)**를 클릭하거나 **Ctrl+W**를 누릅니다.

모든 문서를 닫으려면 메인 메뉴에서 **File(파일) > Close All(모두 닫기)**을 클릭합니다. 문서 탭을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 해당하는 옵션을 선택할 수도 있습니다.

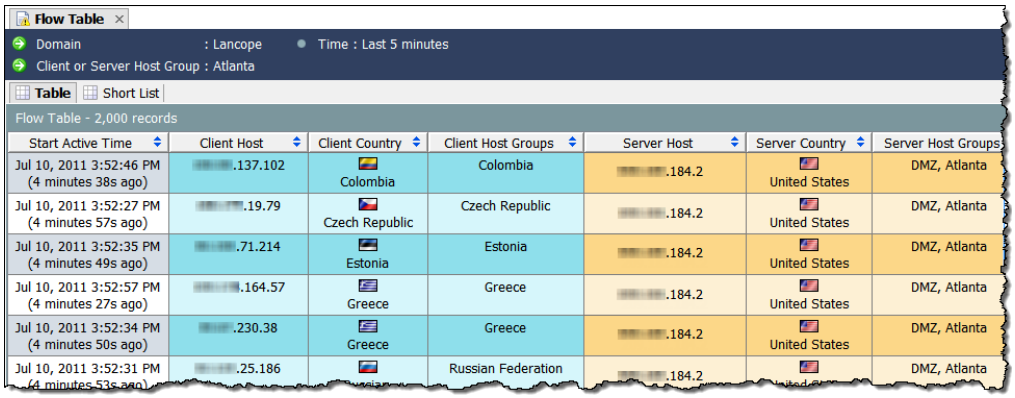


참고:

SMC에서 사용할 수 있는 키보드 바로가기의 전체 리스트는 91페이지의 "키보드 바로가기"를 참조하십시오.

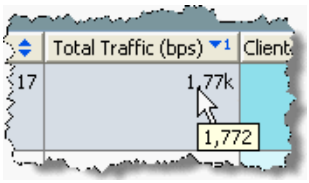
테이블 작업

테이블이 포함되어 있는 문서는 추가 탐색 요소를 제공합니다. 하나의 주요 그래픽 큐는 다음 플로우 테이블에 표시된 것과 같이 테이블 행에서 색상을 사용하는 것입니다.



- 파란색은 클라이언트 측 데이터를 나타냅니다.
- 노란색-주황색은 서버 측 데이터를 나타냅니다.

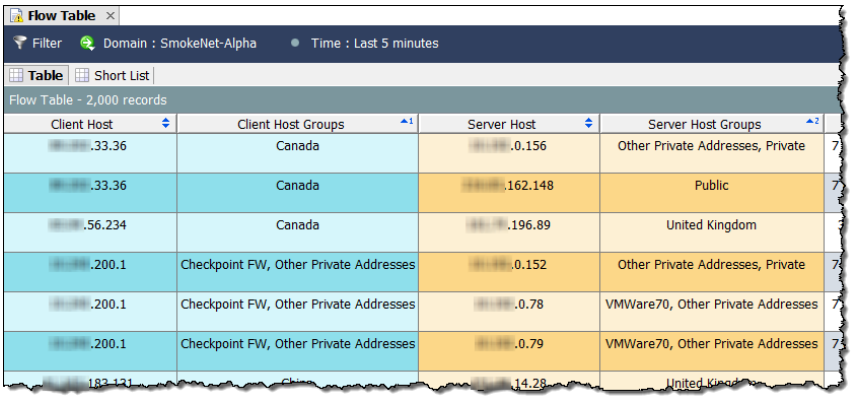
측정 단위는 *bps*(초당 비트 수)와 같이 열 머리글에 표시됩니다. 해당하는 셀의 숫자 값은 반올림됩니다. 그러나, 툴팁에서 반올림 값 위에 커서를 올려 놓으면 정확한 값을 표시할 수 있습니다.



열 정렬

오름차순 또는 내림차순으로 열을 정렬하려면 열 헤딩에서 **Up/Down(위로/아래로)** 버튼을 클릭합니다. (이 버튼은 오름차순 또는 내림차순을 표시하도록 전환됩니다.) 3가지 특정 열로 테이블을 정렬할 수 있습니다. 단일 열을 정렬할 경우, 전체 테이블이 해당 열을 기준으로 정렬됩니다. 두 번째 열을 정렬할 경우, 전체 테이블이 두 번째 열을 기준으로 먼저 정렬된 다음 정렬한 첫 번째 열을 기준으로 정렬됩니다.

다음 예에서 정렬된 첫 번째 열은 영숫자를 오름차순으로 정렬한 Server Host Groups(서버 호스트 그룹) 열입니다. 그 다음으로 Client Host Groups(클라이언트 호스트 그룹) 열이 영숫자 기준으로 오름차순으로 정렬되었을 때 이 열이 첫 번째 열로 정렬되었으며 Server Host Groups(서버 호스트 그룹) 열이 두 번째 열로 정렬되었습니다.

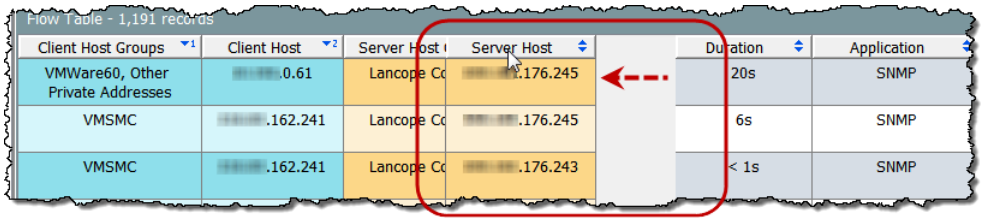


참고:

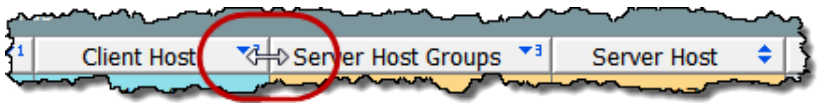
열에서 정렬 행동을 제거하려면 열 헤더를 클릭한 상태로 키보드에서 **Ctrl** 키를 누릅니다.

열 이동 및 크기 조정

열을 왼쪽 또는 오른쪽으로 이동하려면 열 헤딩을 클릭하고 열을 원하는 위치로 끌어오면 됩니다.

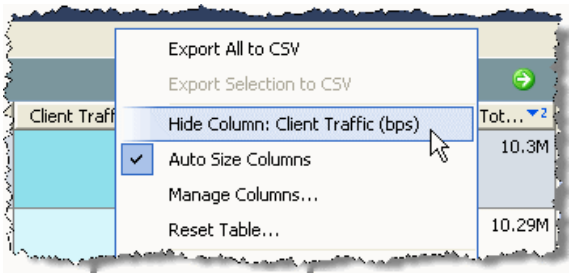


기본적으로 열 너비는 자동으로 조정되며 모든 열이 가능한 최대 범위로 화면에 표시됩니다. 열의 폭을 수동으로 넓히거나 줄이려면 열 헤딩 경계를 클릭하여 원하는 폭으로 왼쪽이나 오른쪽으로 끌어옵니다.

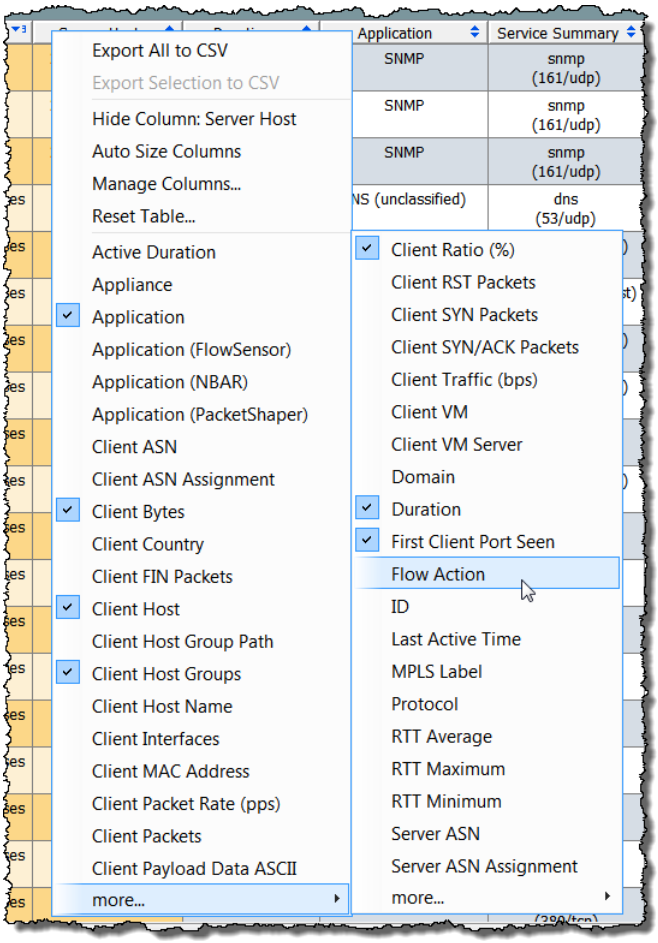


열 숨기기 및 표시

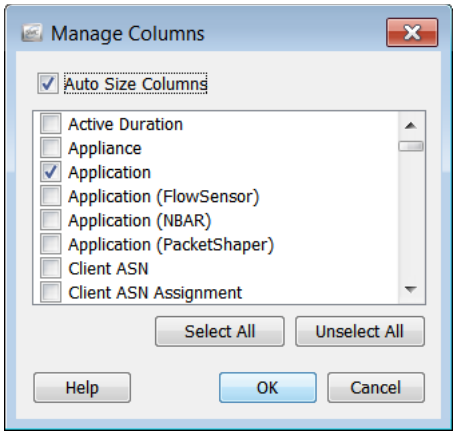
열을 숨기려면 열 헤딩을 마우스 오른쪽 버튼으로 클릭하고 **Hide Column: <Name>(열 숨기기: <이름>)**을 선택합니다.



더 많은 열을 표시하려면 열 헤딩을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 보려는 열을 선택합니다.



또는 Manage Columns(열 관리) 대화 상자로 이동하여 특정 열을 숨기거나 표시할 수 있습니다. 열 헤딩을 마우스 오른쪽 버튼으로 클릭하고 **Manage Columns(열 관리)**를 선택합니다. 해당하는 문서에서 열을 표시하려는 경우, 확인란을 클릭하여 체크 마크를 추가합니다(체크 마크가 아직 추가되지 않은 경우). 해당하는 문서에서 열을 표시하지 않으려는 경우, 확인란을 클릭하여 체크 마크를 제거합니다(체크 마크가 계속 표시되는 경우).



SMC에서 열의 크기가 자동으로 조정되도록 설정하려면 대화 상자 상단에서 **Auto Size Columns(열 크기 자동 조정)** 확인란에 체크 마크가 있는지 확인합니다. SMC는 가로 스크롤 바 없이 모든 열이 가능한 최대 범위로 화면에 표시되도록 열 크기를 자동으로 조정합니다. 모든 열의 크기를 수동으로 조정하려면 **Auto Size Columns(열 크기 자동 조정)** 확인란에 체크 마크가 없는지 확인합니다.

변경을 모두 완료하면 **OK(확인)**를 클릭하여 변경 사항을 적용하고 Manage Columns(열 관리) 대화 상자를 닫습니다.

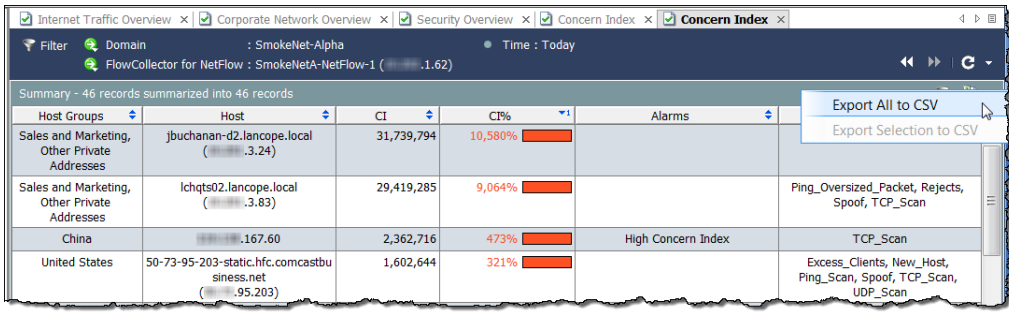
팁:

테이블 기본 설정으로 돌아가려면 열 헤딩을 마우스 오른쪽 버튼으로 클릭하고 **Reset Table(테이블 재설정)**을 선택합니다.

데이터 내보내기

SMC 테이블에 나타나는 데이터를 CSV(쉼표로 구분된 값) 파일에 저장할 수 있습니다. 그런 다음 나중에 CSV 파일을 Microsoft Excel과 같은 대부분의 스프레드시트 프로그램으로 가져와서 확인할 수 있습니다. 테이블의 모든 정보를 내보내거나 특정 선택 영역만 내보낼 수 있습니다.

테이블의 모든 정보를 내보내려면 문서의 오른쪽 상단 모서리에서 **Export to CSV(CSV로 내보내기)** 버튼을 클릭한 다음 **Export All to CSV(모두 CSV로 내보내기)**를 클릭합니다.



참고:

테이블에서 한 행의 정보만 내보내려면 내보내려는 데이터 행을 클릭합니다. 둘 이상의 행을 선택하려면 선택할 때 **Shift** 또는 **Ctrl** 키를 누르거나 원하는 선택 항목을 강조 표시하도록 커서를 끌어옵니다. 문서의 오른쪽 상단 모서리에서 **Export to CSV(CSV로 내보내기)** 버튼을 클릭한 다음 **Export Selection to CSV(CSV로 선택 항목 내보내기)**를 클릭합니다.

Save(저장) 대화 상자가 열리면 정보를 저장할 디렉토리로 이동한 다음 파일 이름을 입력합니다. (파일을 이 형식으로 저장하려면 파일 이름 끝에서 **.csv**를 입력해야 합니다.) **Save(저장)**를 클릭합니다. 이제 선택한 스프레드시트 프로그램에서 해당 정보를 열고 확인할 수 있습니다.

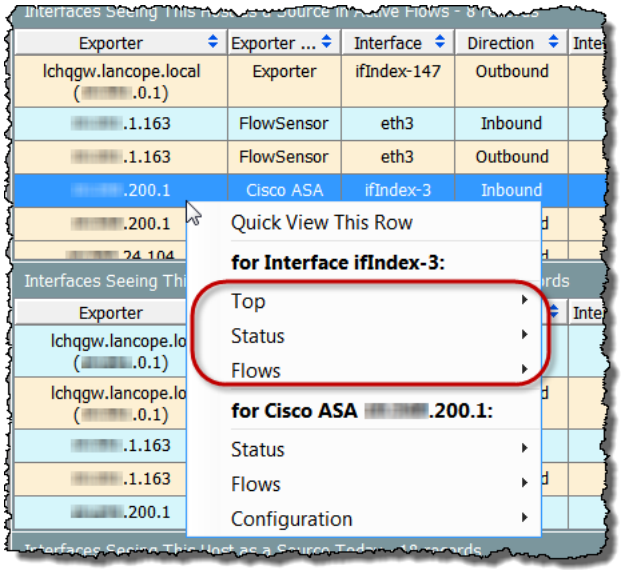
팁:

테이블에서 헤더를 마우스 오른쪽 버튼으로 클릭하여 Export to CSV(CSV로 내보내기) 옵션에 액세스할 수 있습니다. (옵션이 팝업 메뉴에 나타납니다.)

멀티섹션 팝업 메뉴

지금까지 다루었던 테이블의 팝업 메뉴는 매우 단순했으며 옵션에 섹션이 하나였습니다. 그러나, 일부 팝업 메뉴에는 선택한 행 처리 방법에 따라 여러 개의 섹션이 있습니다.

예를 들어, 다음 예에 표시된 팝업 메뉴를 보려면 호스트 스냅샷의 엑스포터 인터페이스 탭에서 엑스포터를 클릭한 다음 마우스 오른쪽 버튼으로 클릭해야 합니다.

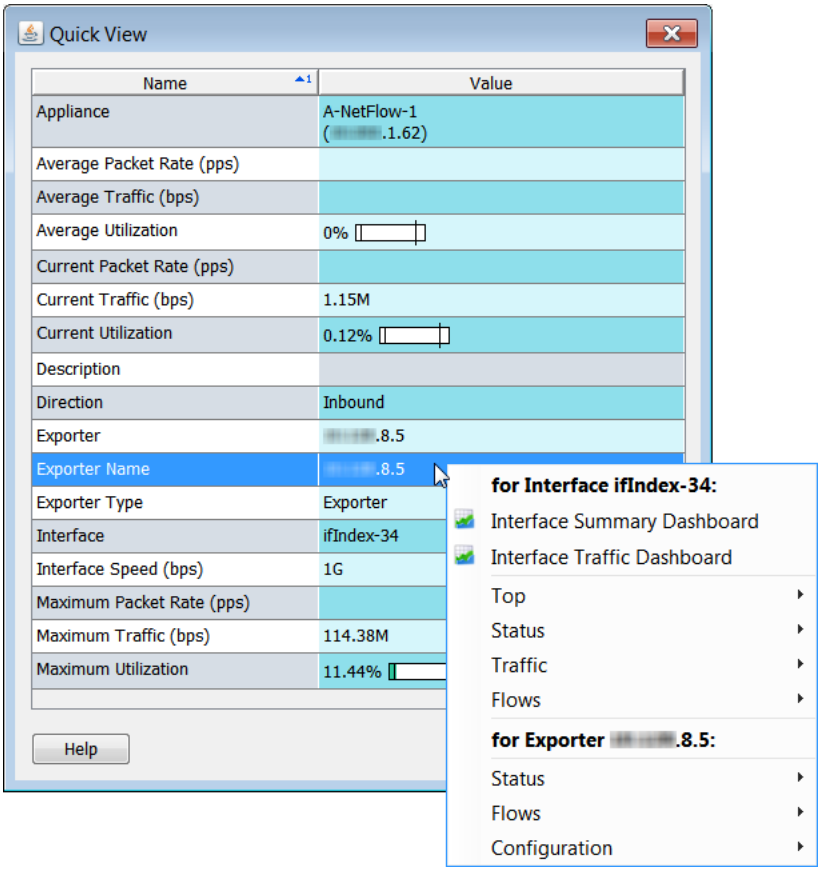


팝업 메뉴의 맨 위에 나타나는 옵션은 행 전체에 적용됩니다. 팝업 메뉴에서 다음으로 표시되는 섹션은 해당 행의 특정 셀에 적용됩니다. 이전 예에서 다음과 같은 유형의 문서를 볼 수 있습니다.

- ifIndex-3 인터페이스와 구체적으로 관련이 있는 문서(이전 예에서 동그라미로 표시된 옵션 클릭).
- Cisco ASA xxx.xxx.200.1 엑스포터와 구체적으로 관련이 있는 문서(팝업 메뉴에서 마지막 3개 옵션)

빠른 보기

Quick View(빠른 보기) 대화 상자에서는 테이블의 특정 행에 나타나는 데이터를 빠르고 쉽게 볼 수 있는 방법을 제공합니다. 원하는 행을 클릭하고 키보드에서 스페이스바를 누릅니다. 또한 행을 마우스 오른쪽 버튼으로 클릭하고 **Quick View This Row(이 행 빠른 보기)**를 선택합니다.



경우에 따라 빠른 보기는 다른 문서의 필터링된 보기에 대한 탐색 기능을 제공합니다. 해당 행에 있는 데이터에 대한 자세한 내용을 확인하기 위해 관련된 문서와 함께 팝업 메뉴를 보려면 행 내에서 마우스 오른쪽 버튼을 클릭합니다.

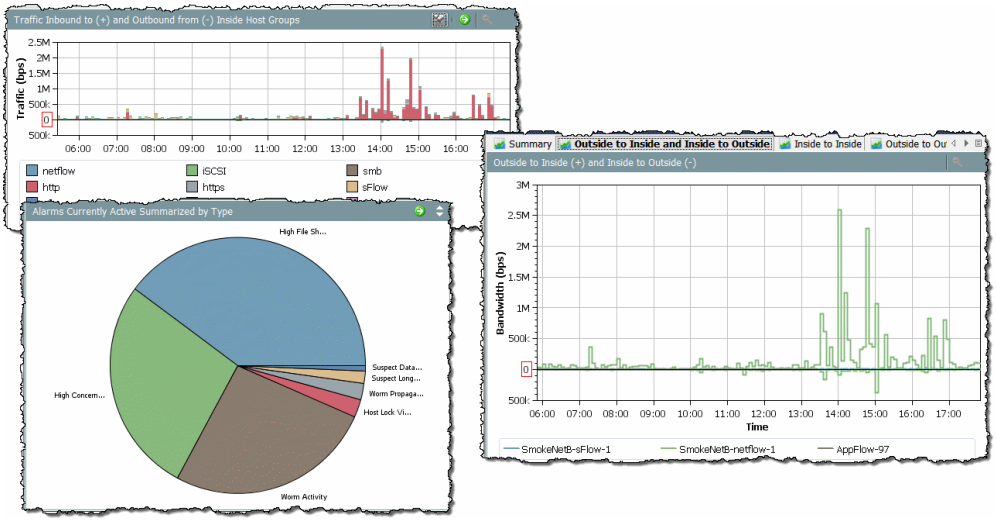
키보드에서 **Alt** 키를 위로 또는 아래로 키와 동시에 눌러 빠른 보기를 닫지 않고 관련 문서에서 행 사이를 탐색할 수 있습니다.

빠른 보기 대화 상자를 닫으려면 다음 중 하나를 수행하십시오.

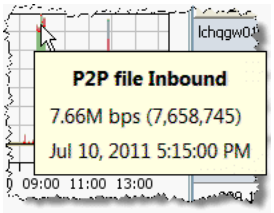
- 키보드에서 스페이스바를 누릅니다.
- 키보드에서 **Esc** 키를 누릅니다.
- 오른쪽 상단 모서리에 있는 ❎ 버튼을 클릭합니다.

차트 작업

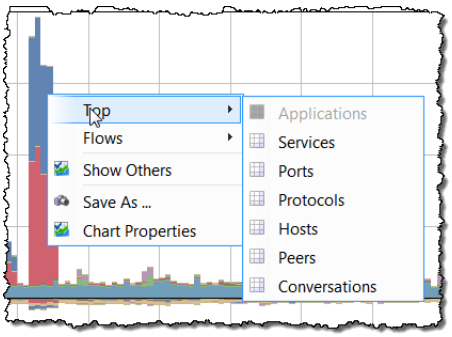
SMC 클라이언트 인터페이스의 일부 문서에는 다음 예에서와 같이 막대, 선 또는 파이 차트가 포함되어 있습니다.



차트의 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 **Save As(다른 이름으로 저장)**를 선택하여 차트를 JPG 또는 PNG 파일로 저장할 수 있습니다. 그런 다음 분석, 보고 또는 아카이브용으로 필요한 경우 다른 문서로 그래픽을 가져올 수 있습니다.



차트의 각 색상은 보고 있는 차트에 따라 특정한 애플리케이션, 서비스, 알람 유형 또는 어플라이언스를 나타냅니다. 차트에서 특정 항목에 대한 세부사항을 보려면 색상이 있는 영역 위에 커서를 올려 놓아 툴팁을 통해 더 많은 정보를 확인하십시오.



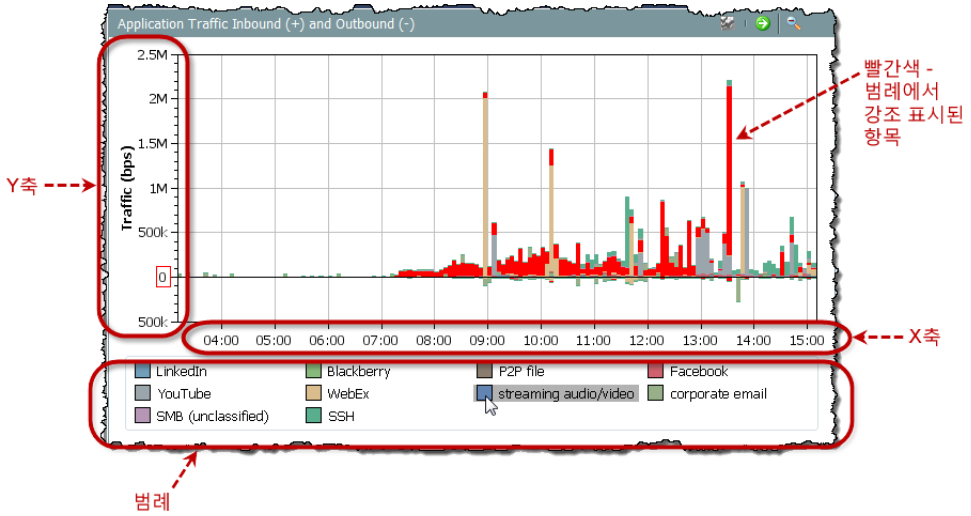
또한 색상이 있는 영역을 마우스 오른쪽 버튼으로 클릭하고 나타나는 팝업 메뉴에서 옵션을 클릭할 수 있습니다. 열리는 문서에는 차트에서 클릭한 항목과 구체적으로 관련이 있는 데이터가 포함되어 있습니다.

관심 있는 영역 전체에서 커서를 누른 상태에서 끌어다 놓아 막대 또는 선형 차트 영역을 확대할 수 있습니다. 영역을 확대하면 키보드의 화살표 키를 사용하여 차트에서 위, 아래, 옆으로 이동하여 다른 영역을 볼 수 있습니다. 정상 배율로 돌아가려면 키보드에서 **F** 키를 누르거나 차트의 오른쪽 상단 모서리에서 **Zoom-out(축소)** 버튼 을 클릭합니다.

참고:

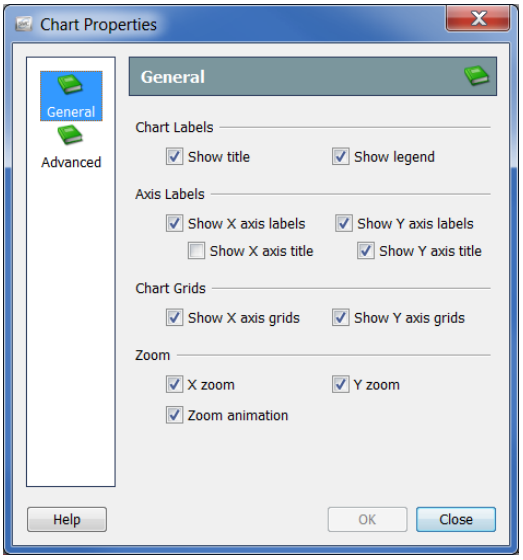
서비스 트래픽 데이터를 보여 주는 차트의 오른쪽 상단 모서리에는 Show/Hide(표시/숨기기) 버튼이 있으며, 이 버튼을 통해 일반적으로 *Others(기타)*로 레이블이 지정된 서비스 트래픽을 표시하거나 숨길 수 있습니다.

막대 및 선형 차트는 다양한 색상과 표시하는 항목을 나열하는 범례와 함께 제공됩니다. 범례에서 항목 위에 커서를 올려 놓으면 해당 차트에서 관련 데이터 포인트가 빨간색으로 강조 표시됩니다.

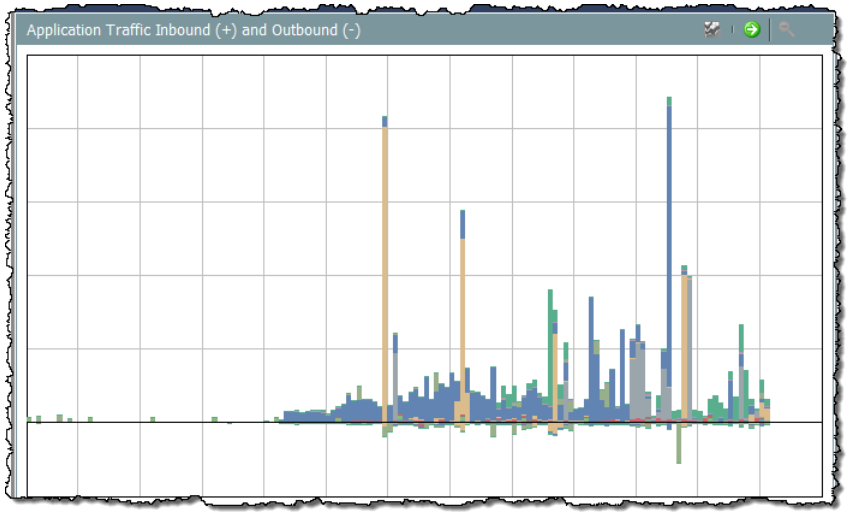


그림에 나와 있는 것처럼 이러한 요소는 문서에서 많은 공간을 차지할 수 있습니다. 데이터 포인트 위에 커서를 올려 툴팁을 확인하는 방법으로 대부분의 해당 정보를 확인할 수 있으므로 범례 및 축을 확인할 필요성을 결정할 수 있습니다.

범례 또는 축을 숨기려면 차트에서 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 **Chart Properties(차트 속성)**를 선택하여 Chart Properties(차트 속성) 대화 상자를 엽니다. Chart Properties(차트 속성) 대화 상자에서 표시하지 않으려는 요소가 있으면 해당하는 확인란을 클릭하여 체크 마크를 제거합니다.

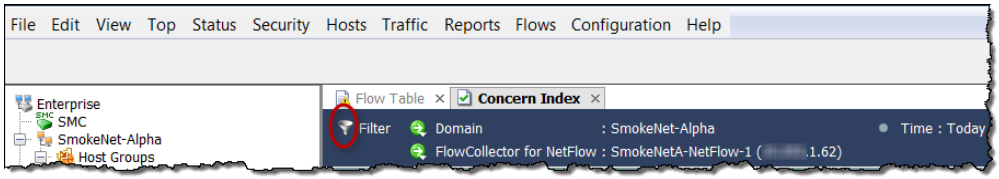


예를 들어 호스트 그룹 네트워크 대시보드에 있는 애플리케이션 트래픽 인바운드 및 아웃바운드 차트에서 범례와 축 레이블을 숨기는 경우, 다음 예와 유사한 결과가 표시됩니다.

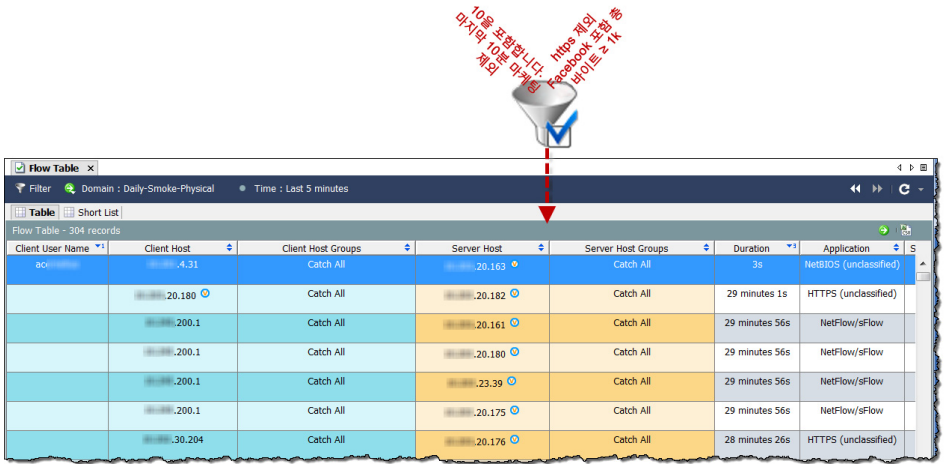


문서 데이터 필터링

이 설명서에서 기억할 수 있는 내용이 없는 경우 *필터는 사용하기 아주 쉽다*는 점을 기억하십시오. 활성 SMC 문서의 필터를 열려면 문서 헤더에서 **Filter(필터)** 버튼만 클릭하면 됩니다.



Stealthwatch System에서 사용할 수 있는 방대한 양의 데이터에서 원하는 정보만 정확하게 추출하려면 필터를 깔때기로 사용하십시오.



사실상 모든 SMC 문서를 필터링할 수 있습니다. 필터링을 통해 포렌식 관점에서 매우 도움이 될 수 있는 기록 데이터를 볼 수도 있습니다.

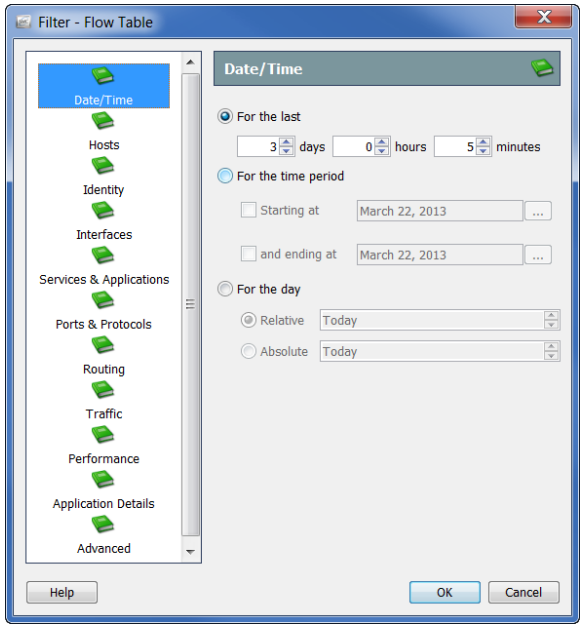
참고:

문서를 공유 문서로 저장할 때 필터 설정도 저장됩니다. 이에 관한 자세한 내용은 82페이지의 "문서 저장"을 참조하십시오.

모든 SMC 문서에는 거의 동일한 방식으로 동작하는 필터가 있습니다. 플로우 테이블에서 볼 수 있는 정보 필터링에 대해 살펴보겠습니다.

날짜/시간

Date/Time(날짜/시간) 페이지에서는 특정 날짜와 시간 동안 마지막까지 발생한 플로우 정보를 표시하도록 플로우 테이블을 필터링할 수 있습니다.



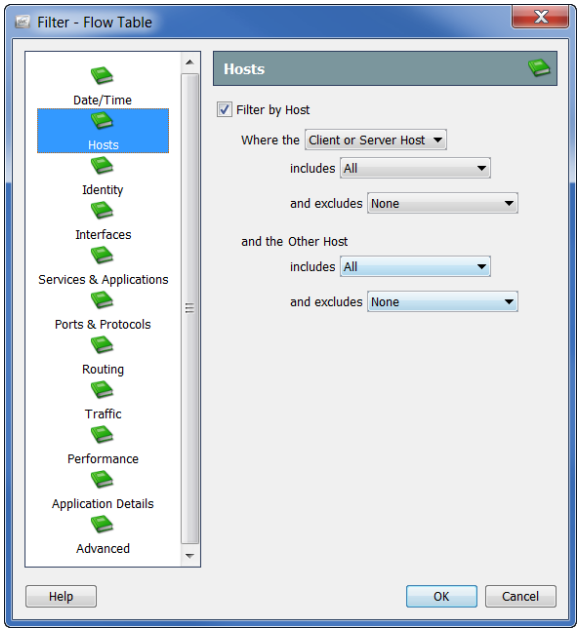
팁:

여러 날짜 동안의 플로우를 조사하려면 빠른 응답을 위해 플로우 테이블 대신 플로우 트래픽 문서를 사용하십시오.

호스트

플로우 테이블 필터의 Hosts(호스트) 페이지에서는 특정 호스트에만 관련이 있는 플로우에 대한 정보를 표시할 수 있습니다.

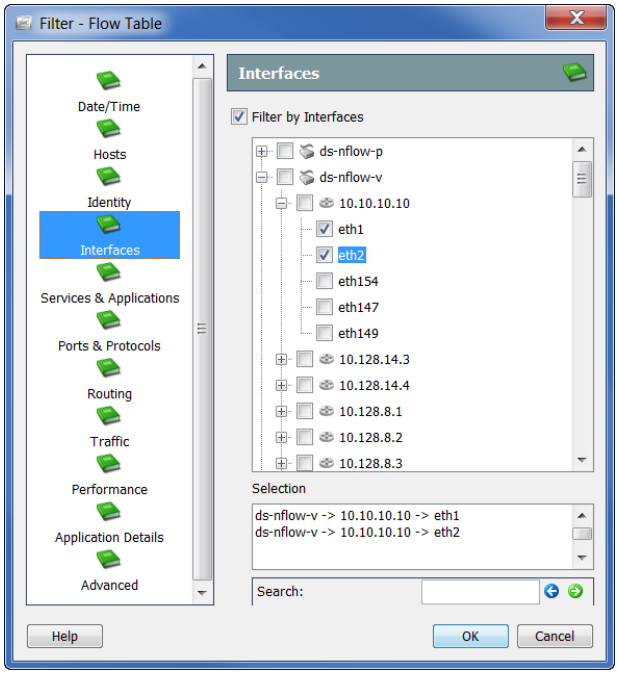
서버 호스트, 클라이언트 호스트 또는 둘 다에 대한 필터링을 수행할 수 있습니다. 특정 호스트 그룹, IP 주소 범위 또는 특정 IP 주소로 초점의 범위를 좁힐 수 있습니다. VM을 포함하거나 이러한 요소 중 하나를 제외할 수 있습니다.



팁:

NATed 플로우를 표시하지 않고 임의의 내부 호스트와 관련된 플로우를 찾아보려면 Flow Table Filter: Hosts(플로우 테이블 필터: 호스트) 페이지로 이동하여 네트워크에서 사용하는 광범위한 내부 IP 주소 범위(예: 10.0.0.0/8)가 필터링 프로세스에 포함되도록 지정하십시오.

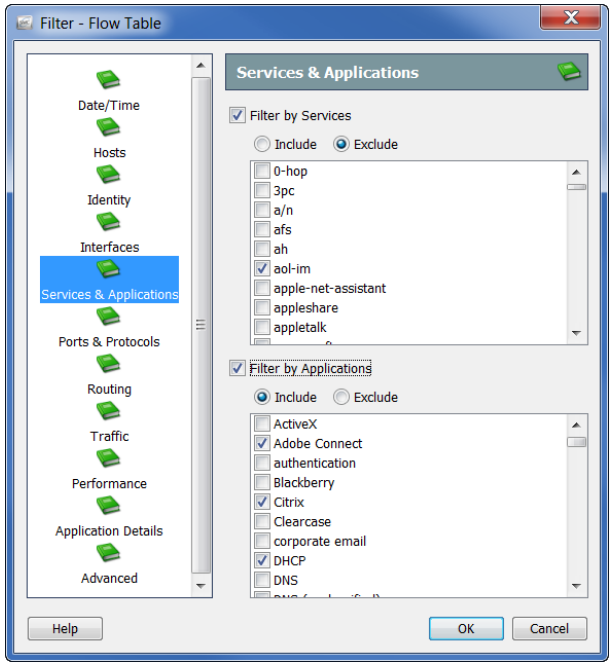
인터페이스



플로우 테이블 필터의 Interfaces(인터페이스) 페이지에서는 특정 Flow Collector, 엑스포터 및/또는 인터페이스와 관련이 있는 플로우에 대한 정보를 표시할 수 있습니다. Flow Collector의 모든 엑스포터를 선택하려면 Flow Collector의 해당하는 확인란을 클릭하여 체크 마크를 추가합니다. 이렇게 하면 해당 엑스포터에 대해 모든 인터페이스를 선택하게 됩니다.

선택한 항목은 필터의 Selection(선택) 필드에 나타납니다. 또한 항목 이름의 일부를 알고 있는 경우 맨 아래에 있는 Search(검색) 필드에 이 이름을 입력하여 인터페이스 리스트에서 위치를 찾을 수 있습니다.

서비스 및 애플리케이션



플로우 테이블 필터의 Services & Applications(서비스 및 애플리케이션) 페이지에서는 특정 서비스 및/또는 애플리케이션을 사용한 플로우에 대한 정보를 표시할 수 있습니다. 또한 특정 서비스 및/또는 애플리케이션을 사용한 플로우를 제외할 수 있습니다.

기타 필터 옵션

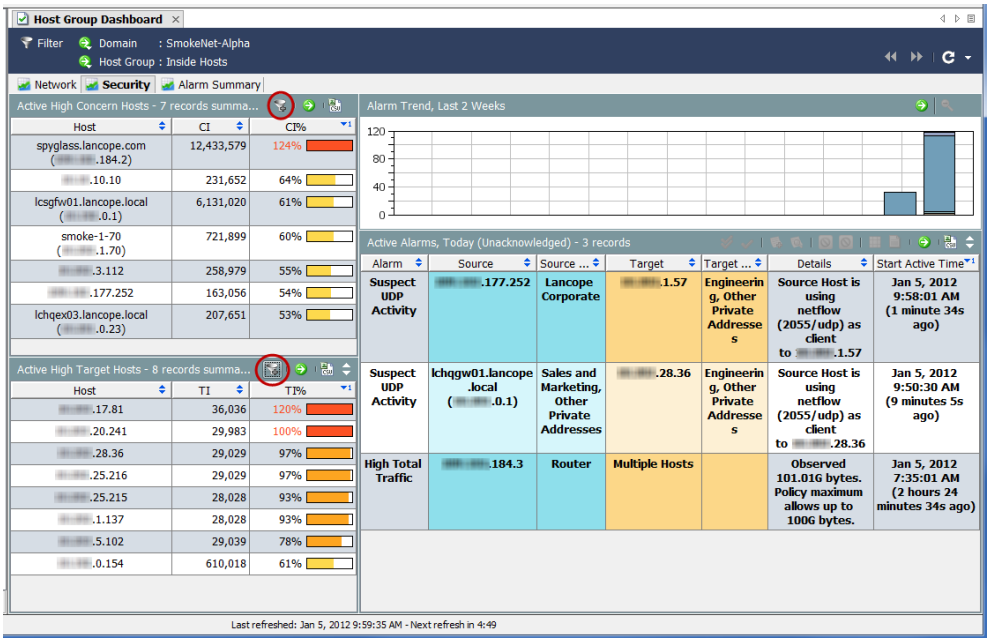
플로우 테이블 필터의 다른 페이지는 방금 다루었던 필터 페이지와 유사하게 동작합니다. 다음 테이블은 나머지 Flow Table Filter(플로우 테이블 필터) 페이지 각각에 대한 간략한 설명을 제공합니다.

해당 페이지...	플로우 필터링 기준...
Identity(ID)	사용자 이름
포트 및 프로토콜	특정 IANA 정의 프로토콜, TCP/UDP 포트 및/또는 클라이언트에서만 사용하는 포트
라우팅	DSCP 포인트, 자율 시스템 번호, VLAN ID 및/또는 MPLS 레이블
트래픽	원하는 경우에 특정 값 범위를 포함하는 총 바이트, 총 패킷, 클라이언트 바이트, 클라이언트 패킷, 서버 바이트 및/또는 서버 패킷 참고: 플로우 테이블은 원시 트래픽 데이터를 보여줍니다.
성능	총 TCP 연결, 총 TCP 재전송, 최소/최대/평균 RTT 및/또는 최소/최대/평균 SRT(원하는 경우 특정 값 범위 포함)
애플리케이션 세부사항	특정 애플리케이션 세부사항 문자열(포함 또는 제외)
고급	레코드의 최대 수, 특정 플로우 레코드 필드의 가장 높은 값 또는 가장 낮은 값(예: 총 바이트, 클라이언트 바이트 등), 방화벽에서 허용/거부된 플로우 작업, 포함되거나 제외된 중복 플로우 및/또는 포함되거나 제외된 인터페이스 데이터와 신속한 쿼리(정렬 또는 그룹화 없음).

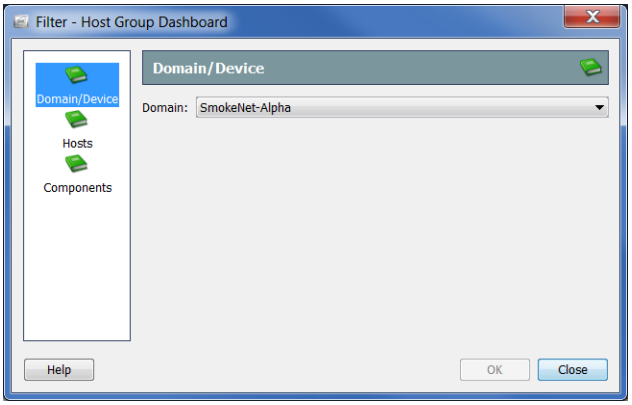
문서, 대화 상자 또는 필터에 대한 질문이 있는 경우, 언제든지 *SMC 클라이언트 온라인 도움말*을 참조할 수 있습니다.

대시보드 필터

대부분의 SMC 문서 필터는 플로우 테이블 필터와 매우 유사하게 동작합니다. 그러나, 대시보드 필터는 약간 다릅니다. 대시보드 필터를 사용하면 연결된 대시보드에서 각 구성 요소를 필터링할 수 있습니다. 예를 들어, 호스트 그룹 대시보드에서 정보를 필터링할 수 있는 방법을 살펴보겠습니다.



호스트 그룹 대시보드의 문서 헤더에서 **Dashboard Filter(대시보드 필터)** 버튼을 클릭하여 필터를 엽니다. 일반적으로, 대시보드 필터에는 다음 3가지 화면에 표시된 것과 같이 세 페이지가 포함되어 있습니다.

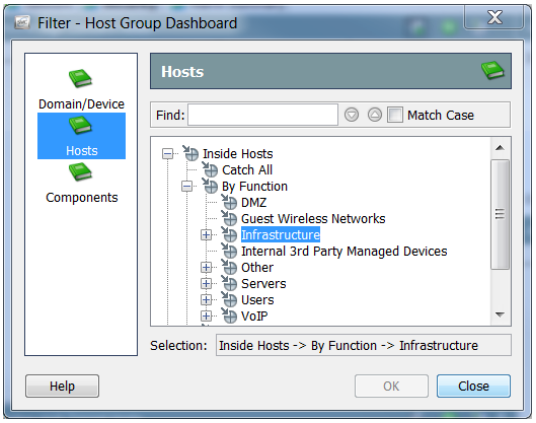


이 예에서 필터의 Domain/Device(도메인/디바이스) 페이지를 사용하면 데이터를 보고 있는 도메인만 변경할 수 있습니다. 이전 예에서 SmokeNet-Alpha 도메인을 선택했습니다. 대시보드에 따라 특정 Flow Collector, 엑스포터 및/또는 인터페이스를 선택할 수도 있습니다.

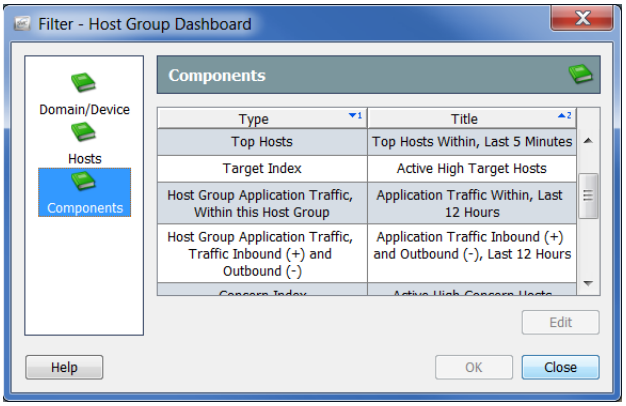
참고:

필터의 세 페이지에서 어떤 항목을 지정하든 구성 요소 필터에서 선택사항이 재정의되며 이 내용은 곧 살펴보겠습니다.

다른 호스트 그룹에 대한 데이터를 표시하기 위해 대시보드를 필터링하려면 Hosts(호스트) 페이지를 엽니다. 호스트 그룹 리스트 전체를 스크롤하여 선택할 수 있습니다. 또는 Find(찾기) 필드에서 호스트 그룹 이름의 일부 또는 이름 전체를 입력하여 리스트 전체를 자동으로 검색하고 원하는 호스트 그룹을 찾을 수 있습니다. 클릭하는 호스트 그룹은 화면 맨 아래에 있는 Selection(선택) 필드에 나타납니다. 이 예에서는 By Function(기능별) 호스트 그룹 아래에서 Infrastructure(인프라) 호스트 그룹을 클릭했습니다.



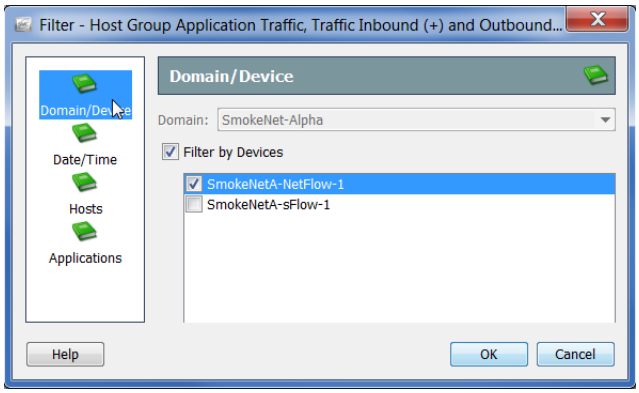
필터의 Components(구성 요소) 페이지를 열면 대시보드의 개별 구성 요소를 필터링할 수 있습니다.



참고:

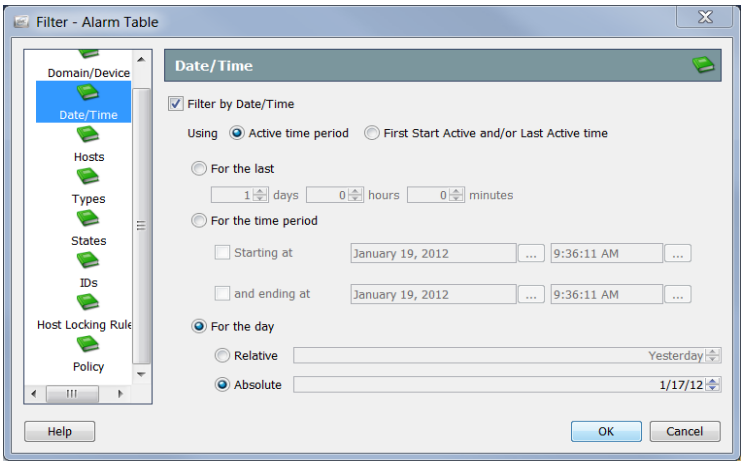
대시보드에 나타나는 대로 이름을 변경하려면 구성 요소 제목을 더블 클릭하십시오.

예를 들어, 특정 기간 동안 특정 Flow Collector에서 관찰한 대로 개인 주소 호스트 그룹에서 모든 Facebook 활동을 보려고 한다고 가정해 보겠습니다. 이 경우 Type(유형) 열에서 **Host Group Application Traffic, Traffic Inbound (+) and Outbound (-)(호스트 그룹 애플리케이션 트래픽, 트래픽 인바운드(+) 및 아웃바운드(-))**를 클릭한 다음 **Edit(편집)**을 클릭합니다.



해당 구성 요소에 대한 Filter(필터) 대화 상자가 열립니다. 대시보드 필터에서 SmokeNet-Alpha 도메인을 이미 클릭했으므로 여기에서 변경할 수 없습니다. 그러나, 데이터를 확인하려는 Flow Collector를 선택할 수 있습니다.

확인할 기간을 지정하려면 필터의 Date/Time(날짜/시간) 페이지를 엽니다.

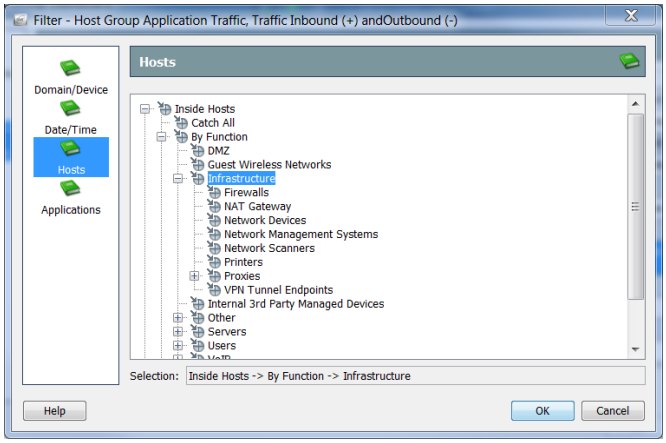


For the day(날짜)의 Relative(상대) 및 Absolute(절대) 설정은 특정 레이아웃 및/또는 필터를 저장한 상태에서 나중에 보기 위해 저장하려는 문서에 유용할 수 있습니다.

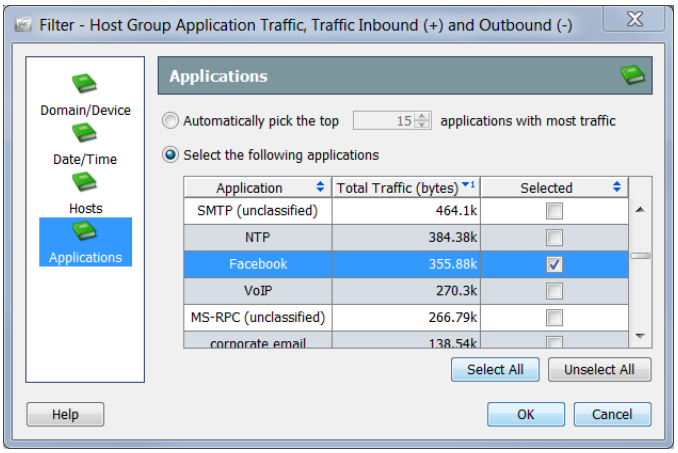
"For the day(날짜)" 섹션 아래에서 **Relative(상대)**를 클릭한 다음 리스트 상자에서 **Yesterday(어제)**를 선택한다고 가정해 보겠습니다. 그런 다음 문서를 공유 상태로 저장합니다. 문서를 여는 시기와 관계없이 선택한 *Yesterday(어제)*로 남아 있습니다. 따라서, 문서는 항상 오늘 하루 전날에 대한 데이터를 보여줍니다.

이제는 대신 "For the day(날짜)" 섹션 아래에서 **Absolute(절대)**를 클릭한 다음 리스트 상자에서 **1/17/12**를 선택한다고 가정해 보겠습니다. 그런 다음 문서를 공유 상태로 저장합니다. 문서를 여는 시기와 관계없이 선택한 *1/17/12*로 남아 있습니다. 따라서, 문서는 항상 해당 날짜의 데이터를 보여줍니다.

대시보드 필터에서 Infrastructure(인프라) 호스트 그룹을 이미 클릭했으므로 구성 요소 필터의 Hosts(호스트) 페이지에서 변경할 수 없습니다. 선택 사항만 볼 수 있습니다.



Facebook을 제외하고 모든 애플리케이션을 필터링하려면 구성 요소 필터의 Applications(애플리케이션) 페이지를 엽니다. 기본적으로 이 필터는 대부분의 트래픽을 유발하는 상위 10개 애플리케이션을 자동으로 선택합니다. **Select the following applications(다음 애플리케이션 선택)** 옵션을 클릭한 다음 오른쪽 하단 모서리에서 **Unselect All(모두 선택 취소)**을 클릭하여 선택한 모든 애플리케이션을 지웁니다. 마지막으로 **Facebook** 확인란을 클릭하여 체크 마크를 추가합니다.



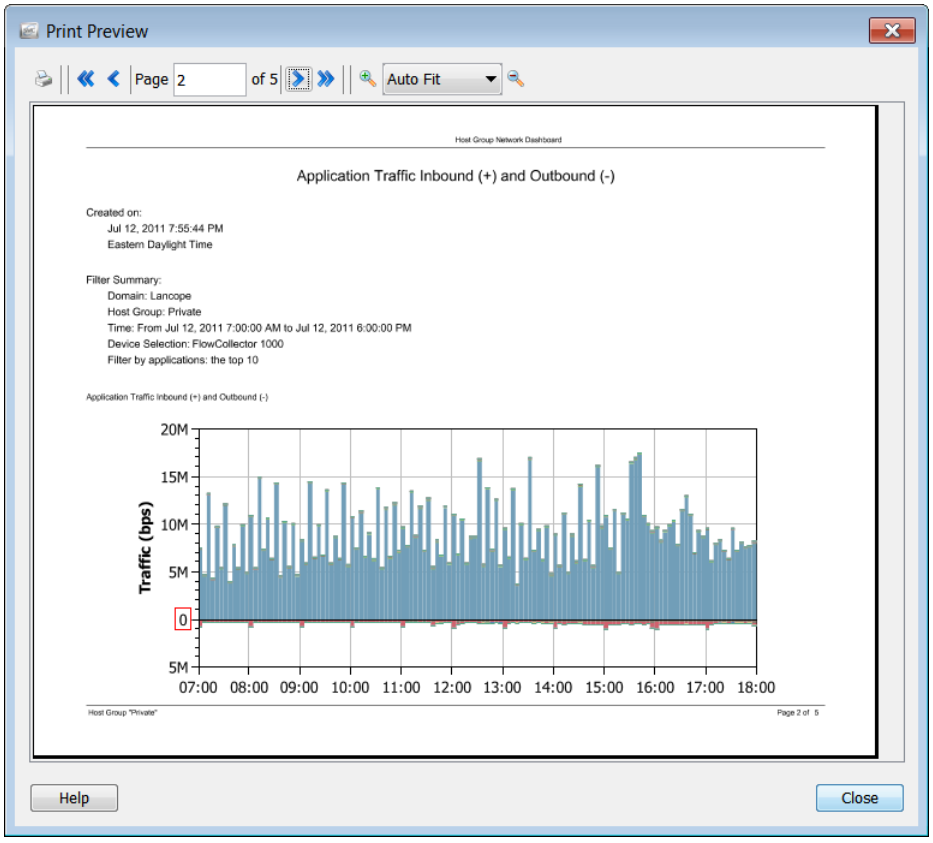
작업을 완료하면 **OK(확인)**를 클릭하여 구성 요소 필터를 닫고 대시보드 필터로 돌아갑니다. 대시보드 필터에서 변경 사항이 있는 경우 변경을 완료하면 **OK(확인)**를 클릭하여 선택한 데이터 집합으로 대시보드를 새로 고칩니다.

문서 인쇄

아카이브 또는 보고용으로 나중에 검토하거나 동료에게 보내기 위해 SMC 문서를 인쇄할 수 있습니다. SMC를 사용하면 문서를 미리 보거나, 인쇄 설정을 맞춤화할 수 있으며, 문서를 PDF 파일로 인쇄 및 저장할 수 있습니다.

인쇄 미리보기

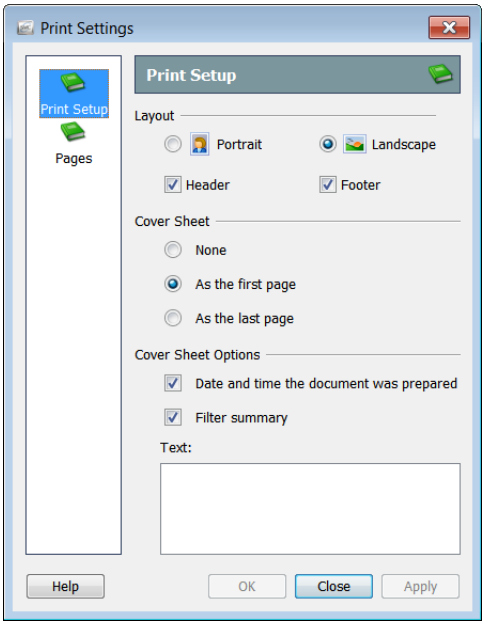
문서를 인쇄하기 전에 문서가 표시되는 방식을 미리 보려면 메인 메뉴에서 **File(파일) > Print Preview(인쇄 미리보기)**를 선택합니다. Print Preview(인쇄 미리보기) 대화 상자가 열립니다.



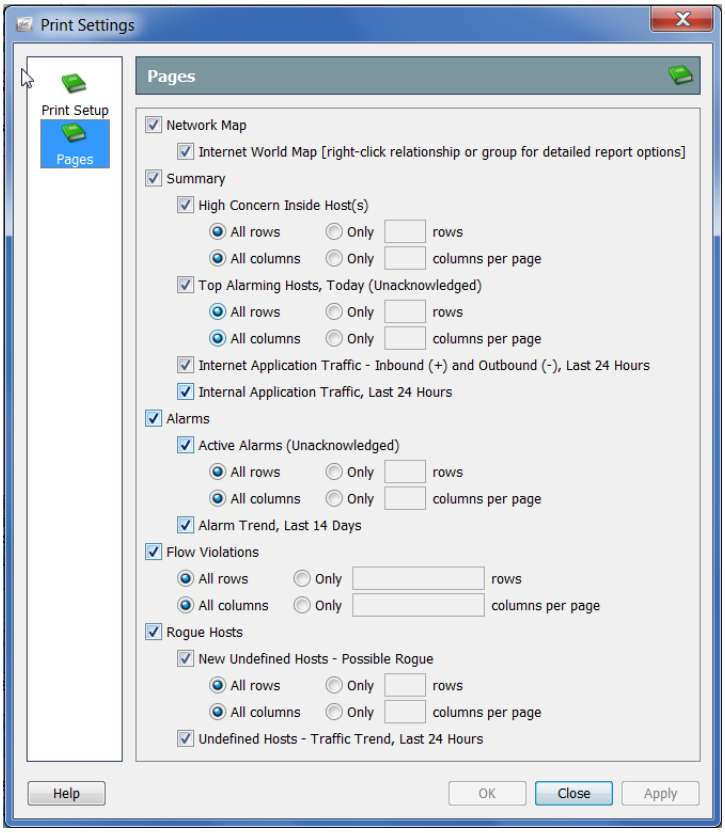
인쇄 설정

문서를 인쇄하기 전에 문서의 인쇄 모양을 맞춤화하려면 Print Settings(인쇄 설정) 기능을 사용합니다. 메인 메뉴에서 **File(파일) > Print Settings(인쇄 설정)**를 선택하여 Print Settings(인쇄 설정) 대화 상자를 엽니다.

Print Setup(인쇄 설정) 페이지에서 페이지 레이아웃을 세로 또는 가로 방향으로 정의할 수 있습니다. 원하는 경우 헤더, 바닥글 및 표지까지 추가할 수 있습니다.

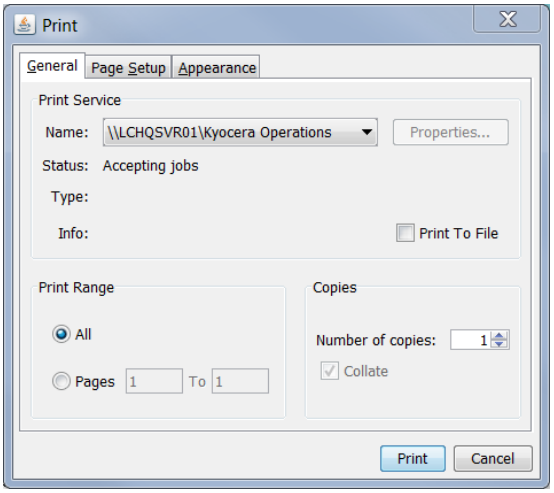


Pages(페이지) 페이지에서 인쇄하려는 문서의 페이지뿐만 아니라 열 및/또는 행을 선택할 수 있습니다.



인쇄

문서를 인쇄하려면 메인 메뉴에서 **File(파일) > Print(인쇄)**를 선택합니다. Print(인쇄) 대화 상자가 열립니다.



참고:

고품질의 글꼴을 원하는 경우, Preferences: PDF Viewer(기본 설정: PDF 뷰어) 대화 상자에서 외부 PDF 뷰어(Adobe Acrobat Reader 등)에 대한 경로를 설정합니다. 이 대화 상자에는 메인 메뉴의 **Edit(편집) > Preferences(기본 설정)**를 선택하여 액세스할 수 있습니다.

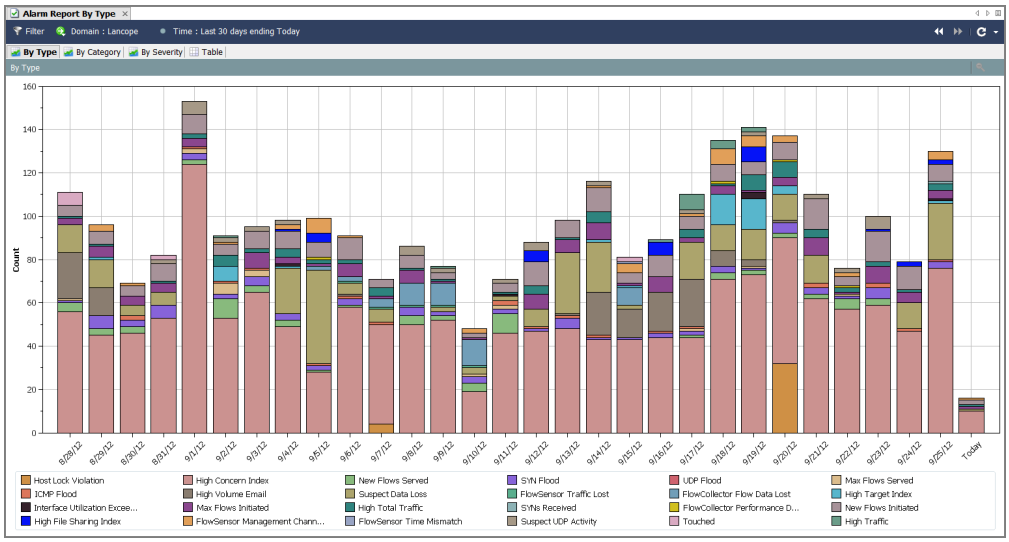
문서 저장

나중에 사용할 수 있도록 문서 레이아웃 저장

SMC 문서의 레이아웃을 재정렬한 뒤 나중에 사용하기 위해 해당 레이아웃을 저장하려는 경우, 문서를 저장하십시오. 문서를 저장할 경우 언제든지 검색할 수 있도록 SMC 어플라이언스에 저장됩니다.

문서를 저장하려면 다음 단계를 수행하십시오.

1. 저장할 문서를 엽니다. 예에서와 같이 Alarm Report By Type(유형별 알람 보고서) 문서가 열립니다.



2. 원하는 대로 레이아웃 또는 필터 설정을 변경합니다.
3. (선택사항) SMC 메인 메뉴에서 **File(파일) > Print Settings(인쇄 설정)**를 선택하고 열리는 대화 상자에서 문서를 인쇄할 때마다 어떻게 표시할지 구성합니다. **OK(확인)**를 클릭하여 변경 사항을 저장합니다.
4. (선택사항) 문서가 PDF로 표시되는 방식을 확인하려면 **File(파일) > Print Preview(인쇄 미리보기)**를 선택합니다.

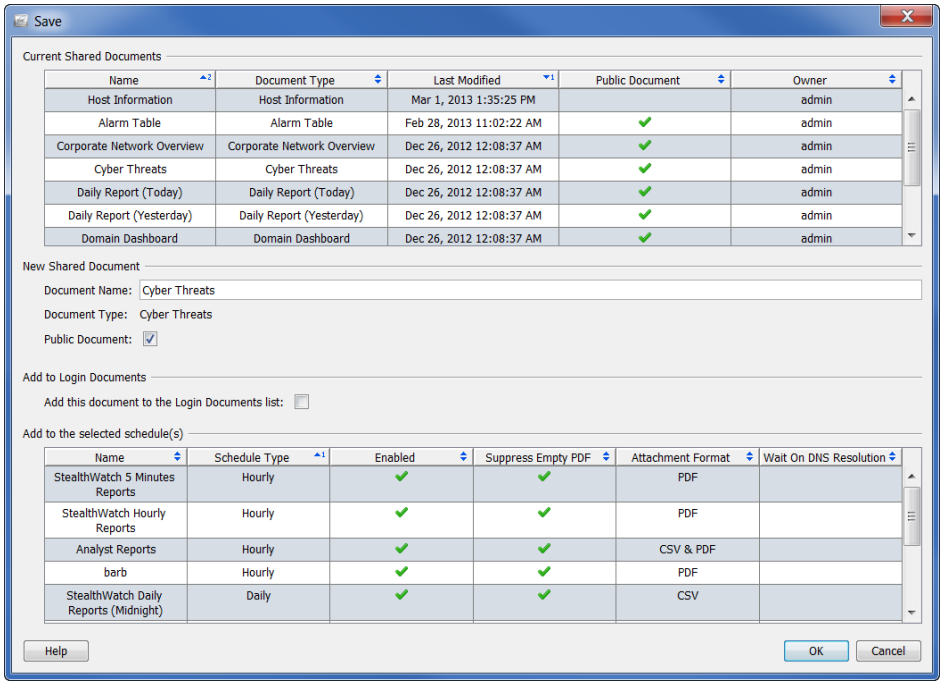
참고:

문서 레이아웃을 변경하고 변경 사항을 유지하려면(예: 열 위치 변경 또는 표시되는 열 변경) **File(파일) > Use Settings as Default(설정을 기본값으로 사용)**를 선택합니다. 이러한 변경 사항은 다음에 문서를 열 때 적용됩니다.

5. 다음 중 하나를 수행합니다.

   - 동일한 이름을 사용하여 이전 버전을 바꾸려는 경우 SMC 메인 메뉴에서 **File(파일) > Save(저장)**를 선택합니다.
   - 다음과 같은 경우, SMC 메인 메뉴에서 **File(파일) > Save As(다른 이름으로 저장)**를 선택합니다.
     - 문서의 사본을 새 이름으로 저장하려는 경우
     - 새 문서를 만든 다음 이 문서를 처음으로 저장하는 경우

     Save(저장) 대화 상자가 열립니다.



6. Name(이름) 필드에 쉽게 알아볼 수 있는 문서 이름을 입력합니다. (사용자 본인 이름을 사용하는 것을 권장합니다.)
7. (선택사항) 다른 사용자가 자신의 이름으로 이 문서를 열 수 있도록 설정하려는 경우, **Public(공용)** 확인란을 선택합니다.

참고:

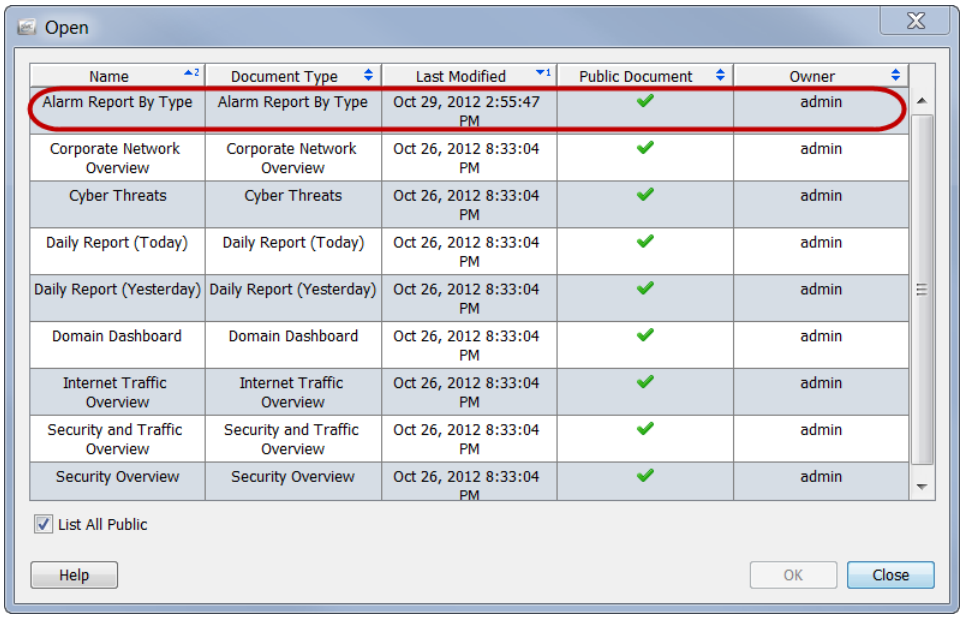
공용 문서에 대한 자세한 내용은 13장, "문서 작업"의 314페이지의 "공용 문서"를 참조하십시오.

8. (선택사항) 사용자 이름으로 SMC 클라이언트 인터페이스에 로그인할 때마다 자동으로 문서가 열리도록 설정하려면 "Add this document to the Login Documents list(로그인 문서 리스트에 이 문서 추가)" 확인란을 선택합니다.

참고:

로그인 문서에 대한 자세한 내용은 13장, "문서 작업"의 310페이지의 " 로그인 문서"를 참조하십시오.

9. **OK(확인)**를 클릭합니다. 문서가 SMC 어플라이언스에 저장됩니다. 이제 SMC 액세스가 가능한 모든 컴퓨터에서 지정한 레이아웃 및/또는 필터 설정으로 사용자 이름 아래에서 이 문서를 열 수 있습니다.
10. 이 문서를 열려면 SMC 메인 메뉴에서 **File(파일) > Open(열기)**을 선택합니다. Open(열기) 대화 상자가 열립니다.



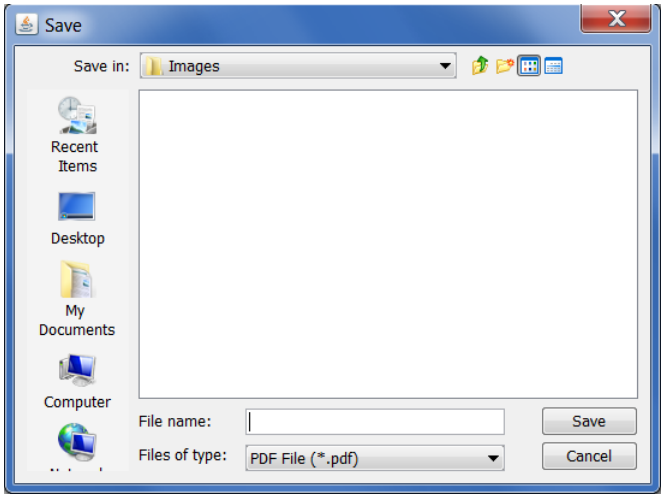
11. 문서를 선택하고 **OK(확인)**를 클릭합니다.

참고:

기본적으로 사용자 이름 아래에 저장한 문서만 나타납니다. 다른 사용자가 만든 문서를 포함하여 모든 문서를 나열하려면 **List All Public(모든 공용 문서 나열)** 확인란을 선택합니다.

문서를 PDF 파일로 저장

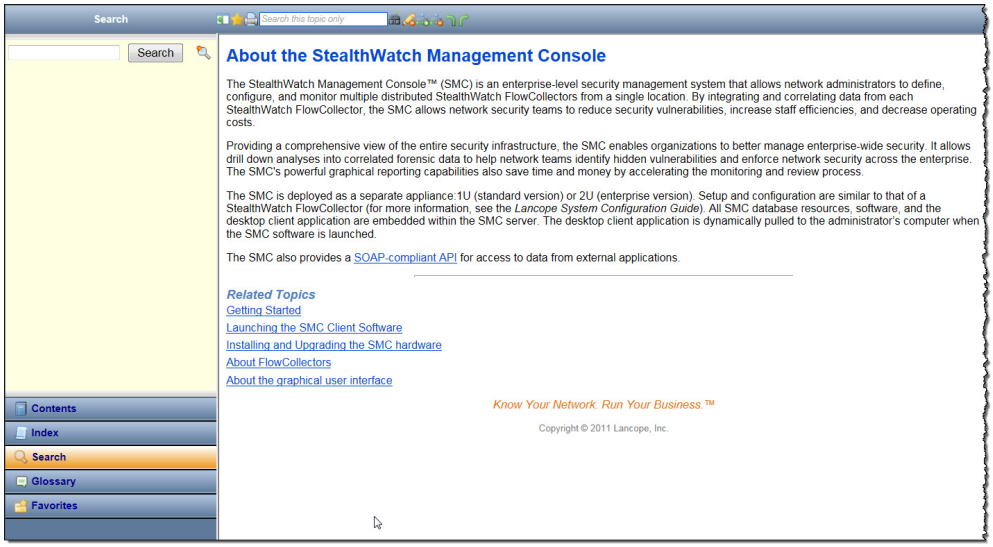
활성 SMC 문서를 PDF 파일로 저장하려면 메인 메뉴에서 **File(파일) > Print to File(파일로 인쇄)**을 선택합니다. Save(저장) 대화 상자가 열립니다.



Save(저장) 대화 상자가 열리면 문서를 저장할 디렉토리 및 파일 이름으로 이동한 다음 **Save(저장)**를 클릭합니다. 그런 다음 PDF 파일을 읽을 수 있는 툴을 사용하여 문서를 열 수 있습니다.

온라인 도움말

SMC 문서에 대한 자세한 정보가 필요한 경우, 키보드에서 **F1** 키 또는 **Ctrl+H** 키를 눌러 *SMC 클라이언트 온라인 도움말*을 확인합니다. 또한 메인 메뉴로 이동하여 **Help(도움말) > Help(도움말)**를 선택할 수 있습니다.



문서가 활성화되어 있는 동안 온라인 도움말에 액세스하면 해당 문서와 관련된 도움말 항목이 표시됩니다. 문서가 열려 있지 않으면 소개 도움말 항목인 "Stealthwatch Management Console 정보"가 표시됩니다.

참고:

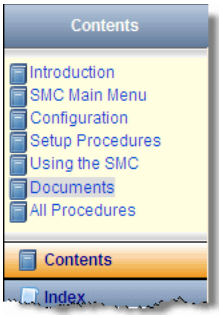
SMC 클라이언트 인터페이스에 로그인했을 때 사용한 동일한 자격 증명을 사용하여 로그인해야 할 수 있습니다. 활성 문서에 대한 정보가 표시되지 않으면 SMC 클라이언트 인터페이스로 다시 이동하여 **F1**을 다시 누르십시오.

*SMC 클라이언트 온라인 도움말*에 액세스한 후에 왼쪽 탐색 창의 맨 아래에 있는 다음 버튼을 사용하여 정보를 찾는 여러 가지 방법이 있습니다.

- 목차
- 색인
- 검색
- 용어집
- 즐겨찾기

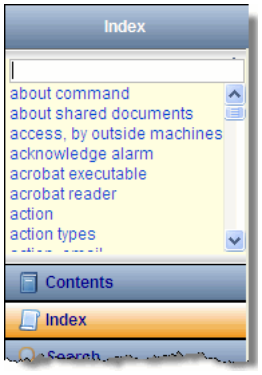
열려 있는 항목을 검색하려면 항목 영역의 맨 위에서 빠른 검색 기능을 사용할 수도 있습니다.

목차



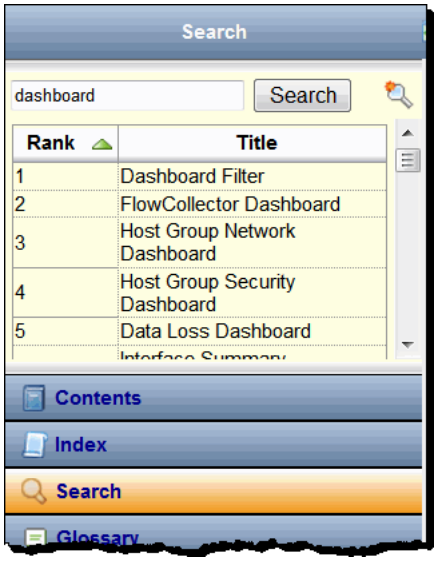
Contents(목차) 창은 이 가이드의 목차와 매우 유사하게 구성되어 있는 온라인 도움말의 목차를 제공합니다. 목차를 보려면 왼쪽 탐색 창의 맨 아래에서 **Contents(목차)**를 클릭합니다. 해당 도움말 항목을 보려면 리스트에서 항목을 클릭합니다.

색인



Index(색인) 창은 관련 항목을 찾을 수 있도록 전체 검색을 수행할 수 있는 단어 리스트를 제공합니다. 색인을 보려면 왼쪽 탐색 창의 맨 아래에서 **Index(색인)**를 클릭합니다. 해당 도움말 항목을 보려면 리스트에서 항목을 클릭합니다. 리스트 전체를 스크롤하여 선택하거나 맨 위에 있는 필드에 텍스트를 입력하여 리스트에 있는 해당 텍스트로 바로 이동할 수 있습니다. 그런 다음, 원하는 항목을 보려면 선택합니다.

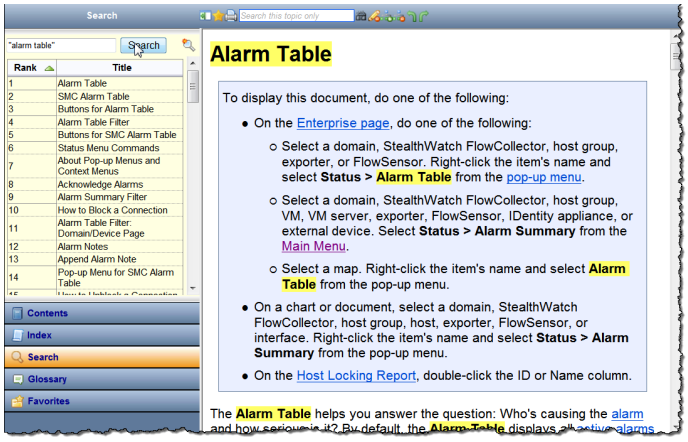
검색



온라인 도움말에 액세스할 때 문서가 열려 있지 않은 경우, Search(검색) 창이 기본적으로 열립니다. 상단에 있는 필드에 찾으려는 텍스트를 입력한 다음 왼쪽 탐색 창의 맨 아래에서 **Search(검색)**를 클릭하거나 키보드에서 **Enter**를 누릅니다. 입력한 텍스트와의 관련성에 따라 순위가 지정된 항목의 리스트가 나타납니다. 항목을 보려면 해당 항목을 클릭합니다.

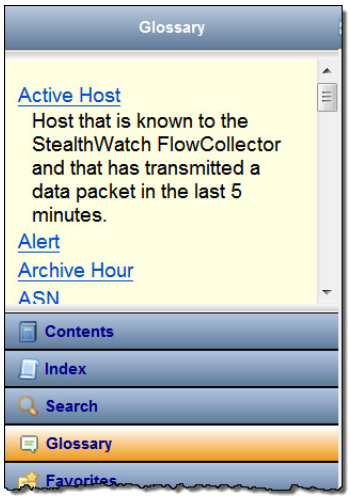
일반적인 정보 찾기 외에 이 기능은 특정 SMC 문서를 여는 방법을 알아야 하는 경우에 유용할 수 있습니다. 특정 문서와 관련된 모든 도움말 항목은 해당 문서에 액세스하는 방법에 관한 첫 번째 단락에서 지침을 제공합니다.

예를 들어 알람 테이블을 열어야 하지만 방법을 모르거나 기억할 수 없다고 가정해 보겠습니다. 검색 필드에 간단하게 "알람 테이블"을 입력한 다음 **Enter** 키를 누릅니다. 알람 테이블 도움말 항목이 검색 결과에 나타나면 항목 이름을 클릭합니다. 도움말 항목이 나타나면 알람 테이블에 액세스하기 위한 지침을 볼 수 있습니다.



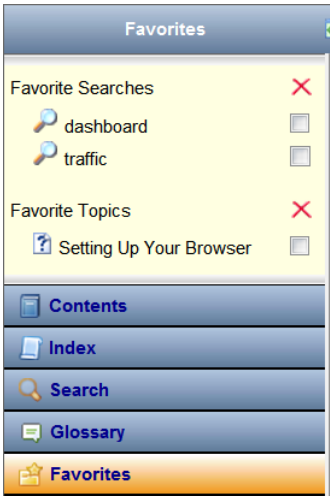
온라인 도움말에서 자주 찾는 항목이 있는 경우, 검색 텍스트를 즐겨찾기 리스트에 추가할 수 있습니다. Search(검색) 필드에 간단하게 텍스트를 입력한 다음 **Search Favorite(즐겨찾기 검색)** 버튼을 클릭합니다. 다음 번에 해당 텍스트를 검색할 때 즐겨찾기 리스트로 간단하게 이동하여 클릭할 수 있습니다.

용어집



Glossary(용어집) 창은 Stealthwatch System 전체에서 공통적으로 사용되는 단어에 대한 정의를 제공합니다. 용어집을 보려면 왼쪽 탐색 창의 맨 아래에서 **Glossary(용어집)**를 클릭합니다. 정의를 보려면 리스트에서 단어를 클릭합니다.

즐겨찾기



Favorites(즐겨찾기) 창에는 즐겨찾기로 표시한 모든 검색 항목이 포함되어 있습니다. 즐겨찾기를 보려면 왼쪽 탐색 창의 맨 아래에서 **Favorites(즐겨찾기)**를 클릭합니다.

즐겨찾기 리스트에 검색 텍스트를 추가하는 방법에 대해서는 이미 설명해 드렸습니다. 또한 리스트에 항목을 추가할 수 있습니다. 이 기능은 특정 항목을 자주 참조하고 찾아야 하는 경우 유용할 수 있습니다. 즐겨찾기 리스트에 추가할 항목 위에 있는 도움말 툴바에서 **Topic Favorite(항목 즐겨찾기)** ⭐ 버튼을 클릭합니다. 다음 번에 해당 항목을 살펴봐야 할 때 즐겨찾기 리스트로 간단하게 이동하여 클릭할 수 있습니다.

Favorite Searches(즐겨찾기 검색) 항목을 클릭하면 검색 창이 열려 해당 항목과 관련된 항목이 나열됩니다. 해당 도움말 항목을 보려면 리스트에서 항목을 클릭합니다.

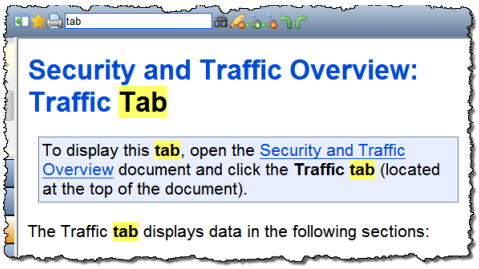
Favorite Topics(즐겨찾기 항목) 항목을 클릭하면 해당 도움말 항목이 열립니다.

즐겨찾기 리스트에서 항목을 제거하려면 해당하는 확인란(☑)을 클릭하고 체크 마크를 추가한 다음 ✕ 버튼을 클릭합니다.

빠른 검색

Quick Search(빠른 검색) 필드는 도움말 툴바에서 도움말 항목 위에 있습니다.

이 필드를 사용하면 보고 있는 도움말 항목 내에서 텍스트를 검색할 수 있습니다. Quick Search(빠른 검색) 필드에 텍스트를 간단하게 입력한 다음 **Search(검색)** 버튼을 클릭하거나 키보드에서 **Enter** 키를 누릅니다. 입력한 텍스트가 항목에 나타나는 경우, 노란색으로 강조 표시되며 다음 예에서와 같이 표시됩니다. 강조 표시를 제거하려면 **Highlighter(형광펜)** 버튼을 클릭합니다.



참고:

도움말 툴바에서 버튼에 대한 자세한 내용을 보려면 버튼 위에 커서를 올려 툴팁을 확인합니다.

키보드 바로가기

다음 테이블은 SMC 클라이언트 인터페이스에서 다양한 기능을 수행하는 데 사용할 수 있는 여러 가지 키보드 바로가기 리스트를 제공합니다. 이러한 여러 가지 바로가기는 메인 메뉴에서의 선택 항목과 같습니다.

참고:

이 리스트에서 언급한 모든 문서에 대해 다루지는 않았지만 SMC에 더 익숙해지는 데 유용한 참조 자료로 사용할 수 있습니다.

사용할 키	목적
←	차트에서: 확대 영역에서 뒤로(왼쪽) 이동합니다.
→	차트에서: 확대 영역에서 앞으로(오른쪽) 이동합니다.
↑	차트에서: 확대 영역에서 위로 이동합니다. 트리에서 Find(찾기) 필드 사용 시: Find(찾기) 필드에 있는 것과 같은 텍스트의 이전 항목을 트리에서 찾습니다.
↓	차트에서: 확대 영역에서 아래로 이동합니다. 트리에서 Find(찾기) 필드 사용 시: Find(찾기) 필드에 있는 것과 같은 텍스트의 다음 항목을 트리에서 찾습니다.
Alt + ←	여러 문서가 열려 있을 때 활성 문서의 왼쪽에 있는 문서를 봅니다. Quick View for Flow(플로우 빠른 보기) 대화 상자에서: 탭과 탭 사이를 왼쪽으로 이동합니다.
Alt + →	여러 문서가 열려 있을 때 활성 문서의 오른쪽에 있는 문서를 봅니다. Quick View for Flow(플로우 빠른 보기) 대화 상자에서: 탭과 탭 사이를 오른쪽으로 이동합니다.
Alt + ↑	Quick View(빠른 보기) 대화 상자에서: 해당 문서 테이블에서 위 행으로 이동합니다.
Alt + ↓	Quick View(빠른 보기) 대화 상자에서: 해당 문서 테이블에서 아래 행으로 이동합니다.

-계속-

사용할 키	목적
Alt + F	엔터프라이즈 트리의 Find(찾기) 필드가 숨겨져 있는 경우: Find(찾기) 필드를 표시합니다. 엔터프라이즈 트리의 Find(찾기) 필드가 표시되는 경우: Find(찾기) 필드에 커서를 둡니다.
Ctrl	테이블에서 이 키를 누르고 열 헤딩을 클릭하면 해당 열의 정렬 순서가 제거됩니다.
Ctrl + ←	활성 문서에 이전 기간의 데이터를 표시합니다. 이 바로가기는 메인 메뉴에서 **View(보기) > Time Backward(이전 시간으로 이동)**를 선택하는 것과 동일합니다. 또한 기본 툴바에서 **Time Backward(이전 시간으로 이동)** 버튼  을 클릭할 수 있습니다.
Ctrl + →	활성 문서에 이후 기간의 데이터를 표시합니다. 이 바로가기는 메인 메뉴에서 **View(보기) > Time Forward(이후 시간으로 이동)**를 선택하는 것과 동일합니다. 또한 기본 툴바에서 **Time Forward(이후 시간으로 이동)** 버튼  을 클릭할 수 있습니다.
Ctrl + B	맞춤형 문서 및 레이아웃을 작성할 수 있는 문서 작성기를 엽니다. 이 바로가기는 메인 메뉴에서 **View(보기) > Document Builder(문서 작성기)**를 선택하는 것과 동일합니다. 문서 작성기에서 이 바로가기는 **View(보기) > New Document Builder(새 문서 작성기)**를 선택하는 것과 동일합니다.
Ctrl + C	선택한 텍스트를 복사합니다. 이 바로가기는 메인 메뉴에서 **Edit(편집) > Copy(복사)**를 선택하는 것과 동일합니다.
Ctrl + D	특정 SMC 문서를 열 때마다 동일한 레이아웃 설정을 사용합니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Use Settings as Default(설정을 기본값으로 사용)**를 선택하는 것과 동일합니다.
Ctrl + E	호스트 그룹 편집기를 엽니다. 이 바로가기는 메인 메뉴에서 **Configuration(컨피그레이션) > Edit Host Groups(호스트 그룹 편집)**를 선택하는 것과 동일합니다.

-계속-

사용할 키	목적
Ctrl + F	엔터프라이즈 트리의 Find(찾기) 필드가 숨겨져 있는 경우: Find(찾기) 필드를 표시합니다.
Ctrl + G	IP 주소, 알람 ID, VM 또는 VM 서버에 대한 모든 SMC 문서를 검색할 수 있도록 Global Search(전체 검색) 필드에 커서를 둡니다. 이 바로가기는 메인 메뉴에서 **Edit(편집) > Global Search(전체 검색)**를 선택하는 것과 동일합니다.
Ctrl + H	활성 대화 상자 또는 문서와 관련된 온라인 도움말을 표시합니다. (먼저 로그인해야 할 수 있습니다.) 이 바로가기는 메인 메뉴 또는 Document Builder(문서 작성기) 메인 메뉴에서 **Help(도움말) > Help(도움말)**를 선택하는 것과 동일합니다.
Ctrl + I	선택한 개체의 속성을 표시합니다. 이 바로가기는 메인 메뉴에서 **Configuration(컨피그레이션) > Properties(속성)**를 선택하는 것과 동일합니다.
Ctrl + L	License Manager를 봅니다. 이 바로가기는 메인 메뉴에서 **Help(도움말) > License Management(라이선스 관리)**를 선택하는 것과 동일합니다.
Ctrl + N	SMC 클라이언트 인터페이스의 새 인스턴스를 엽니다. 이 바로가기는 메인 메뉴에서 **View(보기) > New Main Window(새 기본 창)**를 선택하는 것과 동일합니다.
Ctrl + O	DAR 파일로 저장된 문서를 엽니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Open(열기)**을 선택하는 것과 동일합니다.
Ctrl + P	활성 문서를 인쇄합니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Print(인쇄)**를 선택하는 것과 동일합니다.
Ctrl + Q	SMC 클라이언트 인터페이스를 닫습니다(즉, 끝내기 또는 종료). 이 바로가기는 메인 메뉴에서 **File(파일) > Exit(종료)**를 선택하는 것과 동일합니다.
-계속-	

사용할 키	목적
Ctrl + S	활성 문서를 특정 레이아웃 및 필터 설정 세트와 함께 DAR 파일로 저장합니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Save As(다른 이름으로 저장)**를 선택하는 것과 동일합니다.
Ctrl + T	엔터프라이즈 트리를 숨기거나 표시합니다. 이 바로가기는 메인 메뉴에서 **View(보기) > Hide/Show Tree(트리 숨기기/표시)**를 선택하는 것과 동일합니다.
Ctrl + V	복사한 텍스트를 수정 가능한 필드에 삽입(붙여넣기)합니다. 이 바로가기는 메인 메뉴에서 **Edit(편집) > Paste(붙여넣기)**를 선택하는 것과 동일합니다.
Ctrl + W	활성 문서를 닫습니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Close(닫기)**를 선택하는 것과 동일합니다.
Ctrl + Shift + C	트리에서 선택한 브랜치를 축소하거나 선택한 브랜치가 없을 경우 트리의 모든 항목을 축소합니다. 이 바로가기는 메인 메뉴 또는 Document Builder(문서 작성기) 메인 메뉴에서 **View(보기) > Collapse All(모두 축소)**을 선택하는 것과 동일합니다.
Ctrl + Shift + E	트리에서 선택한 브랜치를 확장하거나, 선택한 브랜치가 없을 경우 트리의 모든 항목을 확장합니다. 이 바로가기는 메인 메뉴 또는 Document Builder(문서 작성기) 메인 메뉴에서 **View(보기) > Expand All(모두 확장)**을 선택하는 것과 동일합니다.
Ctrl + Shift + S	활성 문서를 특정 레이아웃 및 필터 설정 세트와 함께 새 이름의 DAR 파일로 저장합니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Save As(다른 이름으로 저장)**를 선택하는 것과 동일합니다.
Ctrl + Shift + W	열린 문서를 모두 닫습니다. 이 바로가기는 메인 메뉴에서 **File(파일) > Close All(모두 닫기)**을 선택하는 것과 동일합니다.
Delete	선택한 항목을 삭제합니다. 이 바로가기는 메인 메뉴에서 **Configuration(컨피그레이션) > Delete(삭제)**를 선택하는 것과 동일합니다.

-계속-

사용할 키	목적
Esc	대화 상자 창을 닫습니다.
F	차트에서: 원래 확대/축소 레벨로 돌아갑니다.
F1	활성 대화 상자 또는 문서와 관련된 온라인 도움말을 확인합니다. (먼저 로그인해야 할 수 있습니다.)
F3	문서 작성기에서: Search(검색) 필드에 있는 것과 같은 텍스트의 다음 항목을 검색 트리에서 찾습니다. 이 바로가기는 Document Builder(문서 작성기) 메인 메뉴에서 **Edit(편집) > Find Next in Tree(트리에서 다음 항목 찾기)**를 선택하는 것과 동일합니다.
F5	활성 문서의 데이터를 새로 고칩니다. 이 바로가기는 메인 메뉴에서 **View(보기) > Refresh(새로 고침)**를 선택하는 것과 동일합니다. 또한 기본 툴바에서 **Refresh(새로 고침)** 버튼( )을 클릭할 수 있습니다.
Alt + ←	열린 문서에 여러 탭이 있는 경우, 활성 탭의 왼쪽에 있는 탭을 표시합니다.
Alt + →	열린 문서에 여러 탭이 있는 경우, 활성 탭의 오른쪽에 있는 탭을 표시합니다.
Shift + F3	문서 작성기에서: Search(검색) 필드에 있는 것과 같은 텍스트의 이전 항목을 검색 트리에서 찾습니다. 이 바로가기는 Document Builder(문서 작성기) 메인 메뉴에서 **Edit(편집) > Find Previous in Tree(트리에서 이전 항목 찾기)**를 선택하는 것과 동일합니다.
Spacebar	일부 테이블에서: 행을 클릭하고 스페이스바를 누르면 선택한 항목에 대한 Quick View(빠른 보기) 대화 상자가 표시됩니다. Quick View(빠른 보기) 대화 상자가 열렸을 때 스페이스바를 누르면 대화 상자가 닫힙니다.
Z	차트에서: X축에서 확대합니다.

4

호스트 관리

개요

네트워크에서 모든 호스트를 개별적으로 관리하는 일은 아주 힘든 작업입니다. 그러나, Stealthwatch는 호스트를 호스트 그룹으로 구성하도록 지원하는 방법으로 많은 양의 업무를 줄이는 데 도움을 줍니다.

호스트 그룹은 호스트를 유연하게 구성하는 방법을 제공합니다. 일반적으로 호스트는 여러 그룹에 속할 수 있습니다. 또한 호스트 그룹 및/또는 호스트별로 정책을 정의할 수 있습니다.

이 장에서는 호스트를 호스트 그룹으로 논리적으로 구성하여 네트워크의 다양한 영역을 모니터링하고 호스트 행동을 보다 효율적으로 관리할 수 있는 방법을 알아보겠습니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 호스트 그룹
- 관계형 플로우 맵

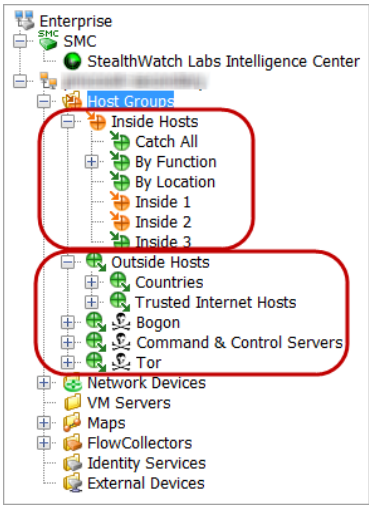
호스트 그룹

호스트 그룹은 기본적으로 위치, 기능 또는 토폴로지 등의 비슷한 속성을 지닌 여러 호스트 IP 주소 또는 IP 주소 범위의 가상 컨테이너입니다. 호스트를 호스트 그룹으로 그룹화함으로써 Stealthwatch Flow Collector가 개별 호스트가 아닌 그룹인 해당 호스트의 행동을 모니터링하고 이에 대응하는 방식을 제어할 수 있습니다.

관리자는 조직에 적합한 어떤 방법으로든 호스트를 구성할 수 있습니다. 이렇게 자유롭게 구성할 수 있어 보고 및 트래픽 관리가 제한 없이 유연할 수 있습니다. 또한 정책 관리가 훨씬 쉬우므로 관리자가 네트워크에서의 호스트 역할에 기초하여 호스트에 대한 정책을 설정할 수 있습니다.

SMC 클라이언트 인터페이스는 다음 예에서와 같이 Enterprise(엔터프라이즈) 트리에서 호스트 그룹 구조뿐만 아니라 네트워크 구조를 표시합니다. 기본적으로 각 도메인에는 하위 호스트 그룹을 추가할 수 있는 다음과 같은 최상위 호스트 그룹이 포함되어 있습니다.

- **내부 호스트** - 호스트가 네트워크의 일부로 구체적으로 정의되어 있는 모든 호스트 그룹을 포함합니다.
- **외부 호스트** - 호스트가 네트워크의 일부로 구체적으로 정의되어 있지 않은 모든 호스트 그룹을 포함합니다.



참고:

사용자의 로그인 권한에 따라 Enterprise(엔터프라이즈) 트리에서 모든 호스트 그룹의 표시 여부가 결정됩니다.

로그인 권한에 따라 최상위 호스트 그룹을 원하는 만큼 추가할 수 있으며, 각 그룹에는 하위 호스트 그룹이 원하는 개수만큼 포함됩니다. 여기에도 하위 호스트 그룹 등을 포함할 수 있습니다. 특정 호스트 그룹에 정의되지 않은 모든 IP 주소는 Outside Hosts(외부 호스트) 호스트 그룹의 Countries(국가) 하위 호스트 그룹에 자동으로 속하게 됩니다. 중복 호스트 그룹 이름을 사용할 수 있지만 동일한 호스트 그룹 레벨(즉, 동일한 상위 호스트 그룹 아래)에서는 사용할 수 없습니다.

참고:

Enterprise(엔터프라이즈) 트리의 Host Groups(호스트 그룹) 브랜치 아래의 모든 레벨에서 호스트 그룹을 만들 수 있지만 Inside Hosts(내부 호스트) 또는 Outside Hosts(외부 호스트) 브랜치 아래에서 추가하는 것이 좋습니다.

기본적으로 Stealthwatch System은 네트워크 외부에 있는 호스트에 대해서는 정책을 만들지 않습니다. 그러나, 정기적으로 네트워크에서 트래픽을 유발하는 외부 호스트를 추적해야 하는 경우, 이 호스트를 외부 호스트 그룹에 배치하고 해당 그룹에 대한 정책을 설정할 수 있습니다. 그런 다음 내부 호스트에서와 마찬가지로 설정을 조정할 수 있습니다.

참고:

또한 특별한 보고를 위해 필요한 경우 최상위 레벨 호스트 그룹(즉, 내부 호스트 또는 외부 호스트와 동일한 레벨)을 만들 수 있습니다

다음은 특정한 외부 호스트의 행동을 추적해야 하는 몇 가지 상황입니다.

- 외부 DNS 서버를 사용 중일 때
- 사용자 네트워크에 정기적으로 액세스하는 서드파티 컨설턴트 또는 벤더가 있는 경우
- 사용자 네트워크에 정기적으로 액세스하는 파트너 회사가 있는 경우

Catch All(모두 탐지) 호스트 그룹

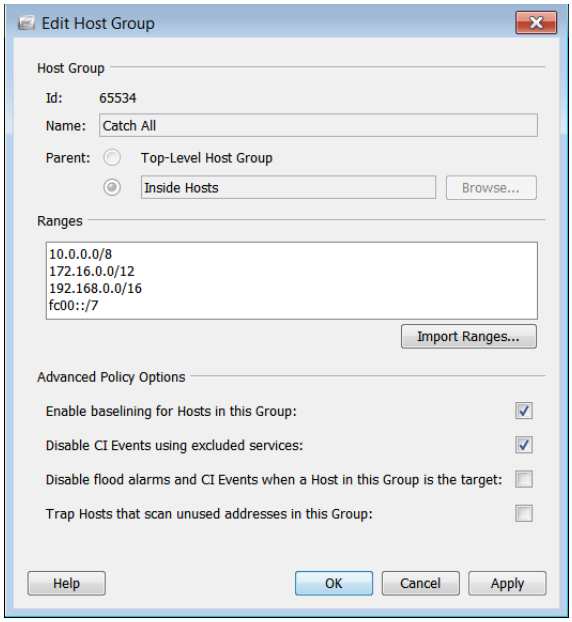
Inside Hosts(내부 호스트) 호스트 그룹에는 기본 Catch All(모두 탐지) 하위 호스트 그룹이 포함되어 있습니다. 관리자는 Catch All(모두 탐지) 호스트 그룹을 사용하여 호스트 그룹 구조를 개선할 수 있습니다.

네트워크에 대응하는 모든 대규모 IP 범위는 처음에 Catch All(모두 탐지) 호스트 그룹에 넣는 것이 좋습니다. 그런 다음 IP 범위가 보다 제한적으로 정의되거나 특정 IP 주소가 있는 다른 호스트 그룹을 생성하면, 이러한 범위/주소는 Catch All(모두 탐지) 호스트 그룹 밖으로 자동으로 이동됩니다.

Stealthwatch System v6에 대한 새로운 SMC 설치는 기본적으로 다음 IP 범위(RFC 1918 및 RFC 4193)를 Catch All(모두 탐지) 호스트 그룹에 배치합니다.

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- fc00::/7

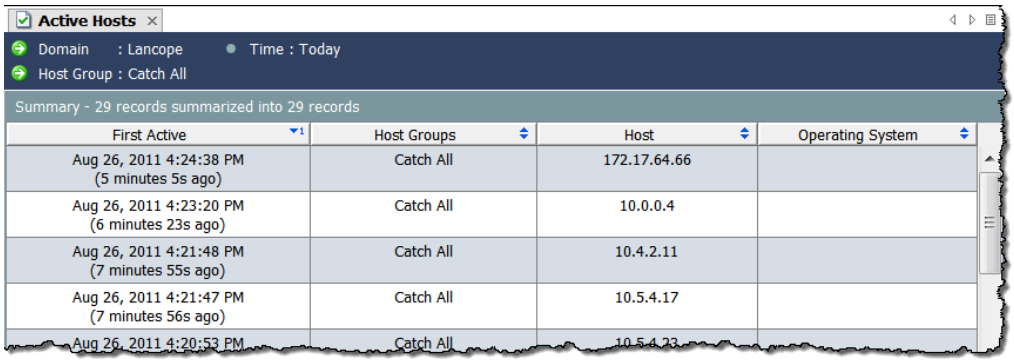
공용 IP 주소를 등록한 경우, 이 주소의 범위를 Catch All(모두 탐지) 호스트 그룹에 수동으로 넣는 것이 좋습니다. 로그인 권한에 따라, Enterprise(엔터프라이즈) 트리에서 마우스 오른쪽 버튼으로 **Catch All(모두 탐지)** 호스트 그룹을 클릭하고 **Configuration(컨피그레이션) > Host Group Properties(호스트 그룹 속성)**를 선택하면 Catch All(모두 탐지) 호스트 그룹에 어떤 IP 범위/주소가 정의되어 있는지 볼 수 있습니다.



참고:

- 호스트 그룹을 편집하려면 Enterprise(엔터프라이즈) 트리에서 해당 호스트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > Host Group Properties(호스트 그룹 속성)**를 선택합니다.
- 호스트 이름은 다음과 같은 특수 문자를 포함하는 영숫자 문자를 사용할 수 있습니다. < , > . ? ” ‘ : ; | { [}] + = _ - ( ) * & ^ % $ # @ ! ~ ‘ 및 “공백”

원칙적으로 호스트 그룹 구조 정의가 완료되면 Catch All(모두 탐지) 호스트 그룹에 활성 IP 주소가 더 이상 없어야 합니다. 비인가 호스트 IP 주소의 경우 Active Hosts(활성 호스트) 문서의 Catch All(모두 탐지) 호스트 그룹에서 확인할 수 있습니다. Enterprise(엔터프라이즈) 트리에서 **Catch All(모두 탐지)** 호스트 그룹을 마우스 오른쪽 버튼으로 클릭한 다음 **Hosts(호스트) > Active Hosts(활성 호스트)**를 선택하면 됩니다.

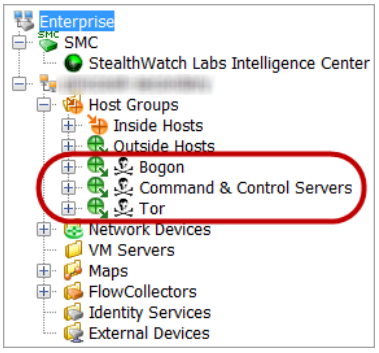


모든 네트워크는 서로 다르지만 Catch All(모두 탐지) 호스트 그룹에 호스트를 할당할 경우 고려해야 할 몇 가지 사항이 있습니다.

- 네트워크 내에서 어떤 영역이 다른 영역보다 더 민감합니까?
- 어떤 네트워크 영역이 자주 변화하고 있으며 어떤 네트워크 영역이 꽤 안정적입니까?
- 중요 자산이 어디에 있습니까?
- 어떤 호스트가 유사한 기능을 수행합니까?
- 사용자의 호스트가 수행하는 다른 기능은 무엇입니까?
- 간단히 말해 특이하고 주기적으로 "이상한" 행동을 하는 호스트가 있습니까?

SLIC Threat Feed 호스트 그룹

SLIC Threat Feed에는 악의적인 활동에 사용되는 것으로 알려진 IP 주소, 포트 번호, 프로토콜, 호스트 이름 및 URL이 포함되어 있습니다. SLIC Threat Feed에 포함되어 있는 호스트 그룹은 다음과 같습니다.



- Bogon - Bogon은 공용 인터넷에서 공식적으로 할당되지 않은 IP 주소입니다.
- C&C(Command & Control) 서버 - C&C 서버는 봇넷에 명령을 실행하고 가로채기된 컴퓨터에서 보고서를 다시 수신하는 중앙 집중식 컴퓨터입니다.
- Tor - Tor는 인터넷 익명화 서비스입니다.

참고:

사용자 호스트에 연결되어 있을 수 있는 SLIC Server Feed에서 URL을 탐지하려면 IPFIX를 내보내도록 구성되어 있는 FlowSensor 또는 라우터를 설치해야 합니다 (NetFlow와 비교). (기본적으로, FlowSensor는 IPFIX를 내보내도록 구성되어 있습니다.)

이전에 언급한 호스트 그룹 중 하나에서 악성 호스트와 통신했던 호스트를 조사하려고 할 때 악성 호스트가 관련 호스트 그룹에 더 이상 나타나지 않는 경우, Alarm Table(알람 테이블)로 이동하여 다음 구성 요소에서 필터링을 수행하십시오.

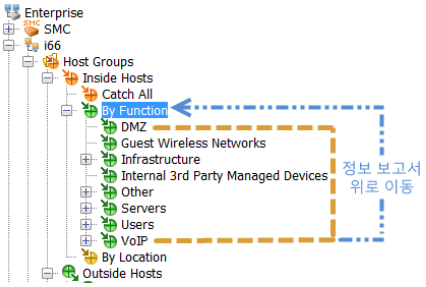
- 유형 - 필터링할 악성 호스트 유형에 따라 해당하는 bogon, C&C(Command & Control) 또는 Tor 알람을 선택합니다.
- 날짜/시간 - 조사하려는 기간에 따라 필터링합니다.

참고:

SLIC Threat Feed 호스트 그룹 브랜치는 이름을 바꾸거나 변경, 이동 또는 삭제할 수 없습니다.

정보 보고서 위로 이동

호스트 그룹에 대한 모든 SMC 문서에는 하위 호스트 그룹 내의 모든 호스트에 대한 정보가 포함되어 있습니다. 예를 들어, 필터 설정을 변경하지 않고 By Function(기능별) 호스트 그룹에 대한 호스트 정보 문서를 열 경우, 이 호스트 그룹 아래에 있는 모든 하위 호스트 그룹의 모든 호스트에 대한 정보뿐만 아니라 By Function(기능별) 호스트 그룹의 바로 아래에 정의되어 있는 모든 호스트에 대한 정보도 볼 수 있습니다.



호스트 그룹 만들기 전략

이 단계에서 호스트 그룹은 이미 정의되어 있을 가능성이 높습니다. 하지만 호스트 그룹이 작동하는 방식에 대한 이해를 돕기 위해 그룹을 만드는 몇 가지 추천 전략에 대해 잠시 살펴보겠습니다.

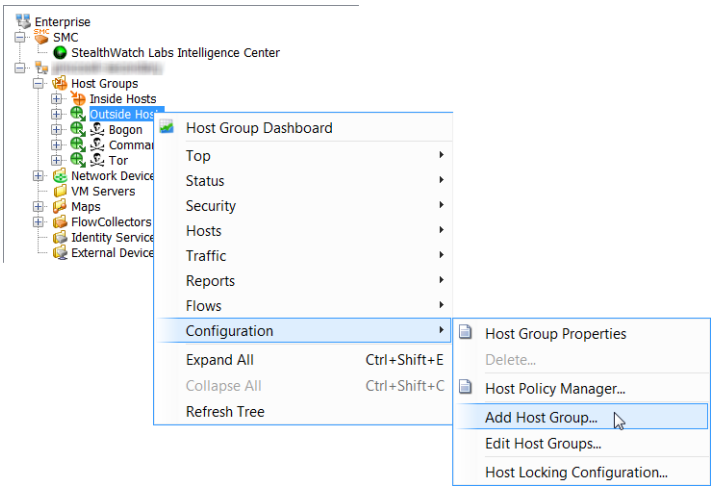
모든 Stealthwatch Flow Collector는 기본 호스트 그룹 구조와 함께 제공됩니다. 로그인 권한에 따라 네트워크 요구 사항에 맞게 기본 호스트 그룹을 수정할 수 있습니다. 추가 호스트 그룹을 만들 뿐만 아니라 Inside Hosts(내부 호스트), Catch All(모두 탐지), Outside Hosts(외부 호스트), Countries(국가), 그리고 Command & Control Servers(C&C 서버)를 제외한 기본 호스트 그룹을 삭제할 수 있습니다.

앞에서 Catch All(모두 탐지) 호스트 그룹에서 처음에 호스트를 배치하는 권장 사항에 대해 살펴보았습니다. 또한 서로 유사하게 행동하는 호스트를 호스트 그룹에 함께 배치하는 것이 좋습니다. 그러나, 네트워크 내의 각 부서, 지리적 지역, IP 세그먼트 또는 조직에 적합한 기타 카테고리별로 다른 호스트 그룹을 만들 수 있습니다.

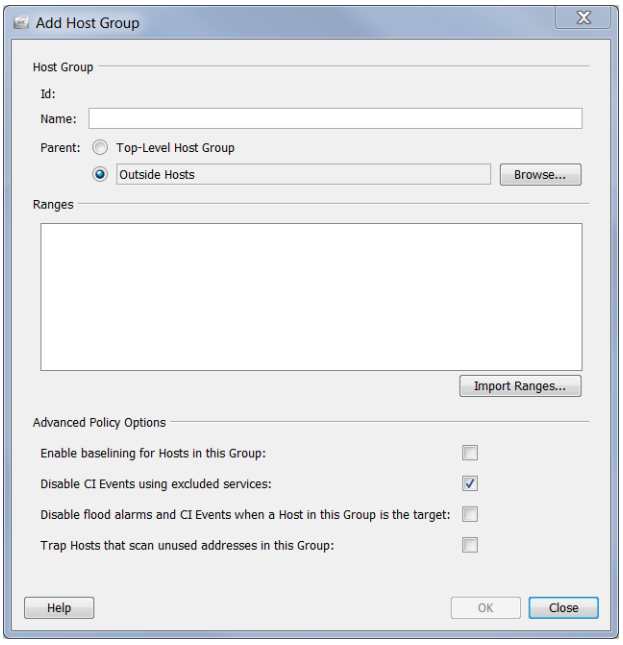
호스트 그룹 만들기

호스트 그룹을 만들려면 다음 단계를 수행하십시오.

1. Enterprise(엔터프라이즈) 페이지의 트리 메뉴에서 **Inside Hosts(내부 호스트)** 또는 **Outside Hosts(외부 호스트)** 폴더(다른 호스트 그룹을 추가하는 대상 호스트) 중 하나를 클릭합니다.
2. **Inside Hosts(내부 호스트)** 또는 **Outside Hosts(외부 호스트)** 호스트 그룹(적용 가능한 경우) 중 하나를 마우스 오른쪽 버튼으로 클릭한 다음 **Configuration(컨피그레이션) > Add Host Group(호스트 그룹 추가)**을 선택합니다.



Add Host Group(호스트 그룹 추가) 대화 상자가 열립니다.



3. Name(이름) 필드에 추가하려는 호스트 그룹의 이름(예: *파트너*)을 입력합니다.
4. Parent(상위) 필드에서 기본값이 올바르지 않은 경우 새 호스트 그룹의 상위 필드를 클릭합니다.
5. Range(범위) 필드에서 원하는 IP 주소 범위를 입력합니다. 이 호스트 그룹의 IP 주소를 포함하는 기존 파일이 있는 경우 **Import Ranges(범위 가져오기)**를 클릭합니다.
6. **Advanced Policy Options(고급 정책 옵션)** 섹션에서 새 호스트 그룹에 적용할 옵션을 클릭합니다.
7. **OK(확인)**를 클릭하여 Add Host Group(호스트 그룹 추가) 대화 상자를 닫습니다. Enterprise(엔터프라이즈) 페이지의 트리 메뉴가 새 호스트 그룹을 포함하도록 자동으로 업데이트됩니다.

IP 주소

각 호스트 그룹에 포함할 IPv4 또는 IPv6 IP 주소 중 하나를 사용할 수 있습니다. IPv4 IP 주소를 입력하는 경우 다음 테이블에 설명된 표기법 형식을 사용해야 합니다.

표기법	예
단일 IP 주소	**10.52.1.55** 10.52.1.55의 호스트만 포함
후행 점 서브넷	**10.52.** 10.52.0.0~10.52.255.255 사이의 모든 IP 주소 포함 **참고:** 끝에 후행 마침표(.)를 포함해야 합니다.
CIDR(Classless Inter-Domain Routing) 표기법("/"를 사용하여 마스크 비트 표시)	**10.52.1.0/24** 10.52.1.0~10.52.1.255 사이의 모든 IP 주소 포함 **참고:** "마스크"를 사용하는 IP 주소를 입력하려면 이 표기법을 사용하십시오. *SMC 클라이언트 온라인 도움말*은 CIDR 표기법 사용에 대한 자세한 정보를 제공합니다. **Search(검색)** 기능을 사용하여 **CIDR**에 대한 참조를 찾습니다.

표기법	예
네트워크 범위	**10-11.** 10.0.0.0~11.255.255.255 사이의 모든 IP 주소 포함 **10.52-53.** 10.52.0.0~10.52.255.255와 10.53.0.0~10.53.255.255 사이의 모든 IP 주소 포함 **10.52-55.3.** 10.52.3.0~10.52.3.255, 10.53.3.0~10.53.3.255, 10.54.3.0~10.54.3.255, 10.55.3.0~10.55.3.255 사이의 모든 IP 주소 포함 **참고:** 끝에 후행 마침표(.)를 포함하십시오.
호스트 범위	**10.52.1.0-10** 10.52.1.0~10.52.1.10 사이의 모든 IP 주소 포함 **10.52.0.0-10.52.255.255** 10.52.0.0~10.52.255.255 사이의 모든 IP 주소 포함 **참고:** IPv4 주소 범위(예: 10.52.100-255.15-255)에서 최대 2개의 옥텟을 바꿀 수 있습니다.
여러 범위	**10.52.100-255.15-255** **10.52.100-255.15-255.3** **1-2.3-4.5-6.7-8**
쉼표로 구분된 리스트	**10.52.1.10,10.52.1.50,10.100.1.20** 이 3개의 호스트만 포함

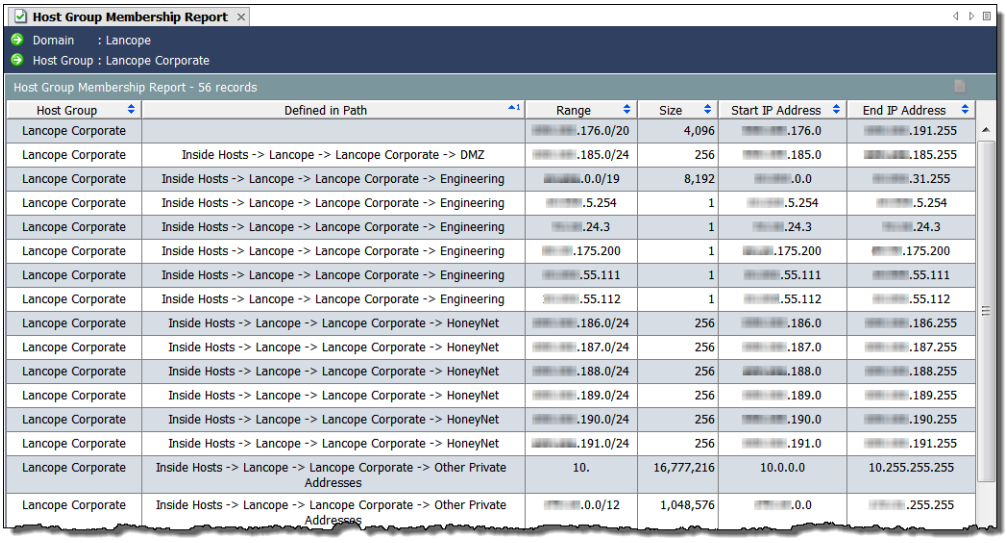
IPv6 IP 주소를 입력하는 경우 다음 테이블에 설명된 표기법 형식을 사용해야 합니다.

표기법	예
단일 IP 주소	**2001:0DB8:0000:0056:0000:ABCD:EF12:3456** **2001:DB8:0:56:0:ABCD:EF12:3456** **2001:DB8::56:0:ABCD:EF12:3456** **2001:DB80:0:56::ABCD:EF12:3456** **2001:DB80:0:56::ABCD:239.18.52.86**
글로벌 라우팅 접두사 서브넷	**2001:DB8:0:56::/64**
네트워크 범위	**2001:DB8:0:56-58::/64**

표기법	예
호스트 범위	**2001:DB8:0:56:ABCD:EF12:3456:1-10** **2001:DB8:0:56:ABCD:EF12:3456:1-** **2001:DB8:0:56:ABCD:EF12:3456:10**
여러 범위	**2001:DB8:0:56-58:ABCD:EF12:3456:1-10** **2001:DB8:0:56-58:ABCD-ABCF:EF12:3456:1-10**

호스트 그룹 멤버십

호스트 그룹 구조를 보려면 Host Group Membership Report(호스트 그룹 멤버십 보고서)를 엽니다. 일반적으로 Enterprise(엔터프라이즈) 트리에서 아무 요소나 마우스 오른쪽 버튼으로 클릭한 다음 **Reports(보고서) > Host Group Membership Report(호스트 그룹 멤버십 보고서)**를 선택하여 이 보고서에 액세스할 수 있습니다.


Host Group Membership Report

Domain : Lancope

Host Group : Lancope Corporate

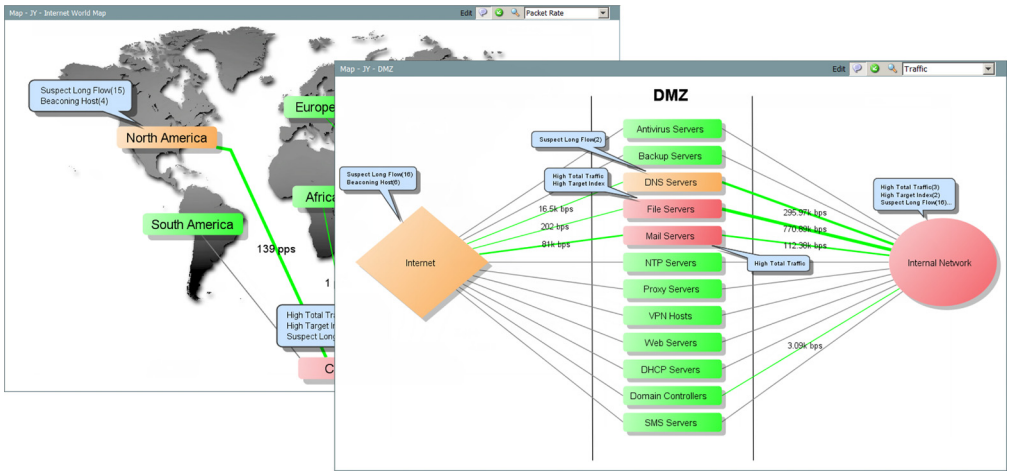
Host Group Membership Report - 56 records

Host Group	Defined in Path	Range	Size	Start IP Address	End IP Address
Lancope Corporate		.176.0/20	4,096	.176.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> DMZ	.185.0/24	256	.185.0	.185.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.0.0/19	8,192	.0.0	.31.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.5.254	1	.5.254	.5.254
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.24.3	1	.24.3	.24.3
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.175.200	1	.175.200	.175.200
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.111	1	.55.111	.55.111
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.112	1	.55.112	.55.112
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.186.0/24	256	.186.0	.186.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.187.0/24	256	.187.0	.187.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.188.0/24	256	.188.0	.188.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.189.0/24	256	.189.0	.189.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.190.0/24	256	.190.0	.190.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.191.0/24	256	.191.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	10.	16,777,216	10.0.0.0	10.255.255.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	.0.0/12	1,048,576	.0.0	.255.255

관계형 플로우 맵

관계형 플로우 맵은 네트워크 전체에서 호스트 그룹 간 트래픽의 현재 상태에 대한 그래픽 보기를 제공합니다. 따라서 어디에 초점을 두어야 하는지 즉시 확인할 수 있습니다. Stealthwatch에는 필요에 따라 관리자가 맞춤 설정할 수 있는 몇 가지 기본 맵이 제공됩니다.

또한 관리자는 다음 예에 표시된 것과 같이 위치, 기능 또는 가상 환경 같은 기준을 바탕으로 새로운 관계 맵을 쉽게 구성할 수 있습니다.



맵을 사용하면 주요 질문에 대한 해답을 찾을 수 있습니다. 2개의 호스트 그룹 간에 관계를 생성하면 이러한 그룹을 이동하는 트래픽을 분석할 수 있습니다. 맵에서 호스트 그룹을 더블 클릭하여 어떤 문제가 있는지 세분화하고 심층적으로 파악할 수 있습니다. 관계를 만들 때 관계(호스트 그룹 사이의 선)를 마우스 오른쪽 버튼으로 클릭한 다음 **Relationship(관계) > Policy(정책)**를 선택하여 호스트 그룹 간의 베이스라인 설정 및 알람 기능을 활성화할 수 있습니다.

5

보기 및 대시보드

개요

기본적으로 SMC의 문서는 네트워크에서 발생하는 모든 단일 활동에 대한 정보를 표시합니다. 하지만 사용자가 특정 유형의 트래픽 또는 알람에만 관심이 있다면 어떨까요? 또는 해당 문서에 있는 모든 내용보다 문서의 특정 부분만 보고 싶다면 어떨까요? SMC를 활용하면 고유한 대시보드를 구축할 수 있어 관심 있는 주요 정보에만 초점을 둘 수 있습니다.

이 장은 다음 항목으로 구성되어 있습니다.

- SMC의 기본 대시보드
- 호스트 그룹 대시보드
- 고유한 대시보드 구축

SMC의 기본 대시보드

SMC 콘솔에는 많은 수의 기본 대시보드가 포함되어 있으므로 한 문서에서 다양한 유형의 정보를 쉽게 볼 수 있습니다. Main Menu(메인 메뉴)에서 이 대시보드에 액세스하려면 **Status(상태) > Dashboard(대시보드) > [기본 대시보드 이름]**을 선택합니다.

다음은 SMC 콘솔의 기본 대시보드 리스트(알파벳 순서)와 각 대시보드에 대한 설명입니다.

대시보드 이름	설명
Alarm Dashboard(알람 대시보드)	이 대시보드는 선택한 도메인에 대한 알람 데이터를 표시합니다. 데이터는 다음 섹션에 표시됩니다. ▶ 새로운 알람 ▶ 확인된 알람
Cyber Threats Dashboard	이 대시보드는 도메인에 영향을 주는 사이버 위협에 대한 그래픽과 테이블 형식 데이터를 제공합니다. 데이터는 다음 탭에 표시됩니다. ▶ 평판 ▶ 정찰 ▶ 데이터 유출 ▶ 악성코드 ▶ 봇넷
Data Loss Dashboard(데이터 유출 대시보드)	이 대시보드는 선택한 도메인에서의 데이터 전송 활동에 대한 디스플레이를 제공합니다. 데이터는 다음 섹션에 표시됩니다. ▶ 데이터 유출 알람(오늘) ▶ 활성 데이터 유출 알람에 대한 호스트 정보 ▶ 데이터 유출 알람의 트렌드 ▶ 상위 20개 업로드(오늘)
DDoS Alarm Dashboard(DDoS 알람 대시보드)	이 대시보드는 다음 정보를 제공합니다. ▶ 발생하기 시작하면서 DDoS 위협 또는 DDoS 공격을 나타낼 수 있는 활동 ▶ 네트워크에서 발생한 알람에 대한 자세한 정보
DDoS Traffic Dashboard(DDoS 트래픽 대시보드)	이 대시보드는 DDoS 공격을 나타낼 수 있는 네트워크에서의 트래픽 패턴의 급증과 변화에 대한 정보를 제공합니다.

대시보드 이름	설명
Flow Collector Dashboard(Flow Collector 대시보드)	이 대시보드는 Stealthwatch Flow Collector에서 가장 중요한 활동을 그래픽으로 나타냅니다. 데이터는 다음 섹션에 표시됩니다. ▶ 상태 탭 • 플로우 수집 통계 • 플로우 수집 트렌드 • 플로우 수집 상태 ▶ 알람 탭 • Flow Collector 알람 트렌드, 이전 30일 • Flow Collector 알람, 이전 30일
Host Group Dashboard(호스트 그룹 대시보드)	호스트 그룹 대시보드에 대한 자세한 내용은 113페이지의 "호스트 그룹 대시보드"를 참조하십시오.
Interface Summary Dashboard(인터페이스 요약 대시보드)	이 대시보드는 선택한 인터페이스에 대한 트래픽을 다양한 그래픽 및 테이블 형식 데이터로 제공합니다. 데이터는 다음 섹션에 표시됩니다. ▶ 트래픽 통계, 지난 6시간 ▶ 인바운드 및 아웃바운드 사용률, 지난 6시간 ▶ 인바운드 및 아웃바운드 애플리케이션 트래픽, 지난 6시간 ▶ 상위 활성 대화, 인바운드 ▶ 상위 활성 대화, 아웃바운드
Interface Traffic Dashboard(인터페이스 트래픽 대시보드)	이 대시보드는 선택한 인터페이스에 대한 트래픽을 다양한 그래픽 및 테이블 형식 데이터로 제공합니다. 데이터는 다음 섹션에 표시됩니다. ▶ 인터페이스 서비스 트래픽 ▶ 인터페이스 애플리케이션 트래픽 ▶ 인터페이스 통계 ▶ 인터페이스 사용률 ▶ DSCP 트래픽
Security Overview(보안 개요)	이 대시보드는 시스템 보안과 관련된 그래픽 및 테이블 형식 데이터를 제공합니다. 데이터는 다음 섹션에 표시됩니다. ▶ 내부 관심도 호스트 ▶ 외부 관심도 호스트 ▶ 상위 알람 호스트 ▶ 유형별로 요약된 현재 활성 상태 알람

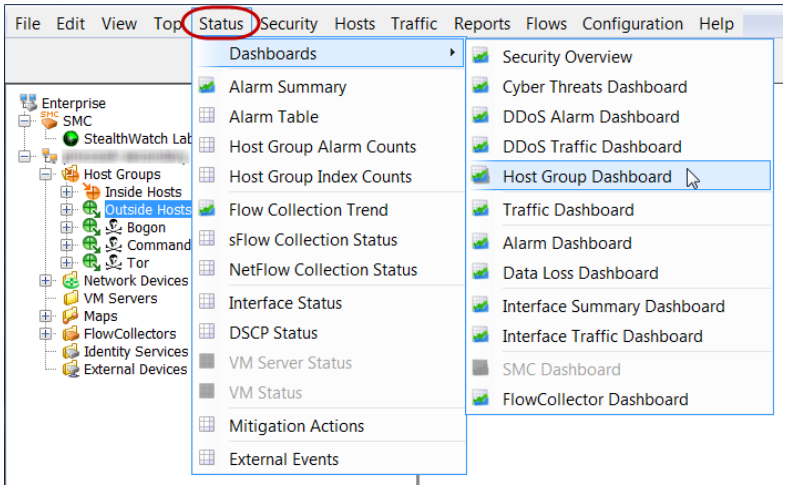
대시보드 이름	설명
SMC Dashboard(SMC 대시보드)	이 대시보드는 SMC 콘솔에서 가장 중요한 활동을 그래픽으로 나타냅니다. 데이터는 다음 섹션에 표시됩니다. ▶ SMC 성능 ▶ SMC 알람 ▶ SMC 이벤트 처리됨
Traffic Dashboard(트래픽 대시보드)	이 대시보드는 선택한 도메인에 대한 트래픽 통계를 그래픽으로 나타냅니다. 데이터는 다음 섹션에 표시됩니다. ▶ 프로토콜, 내부 및 외부 호스트의 패킷 ▶ TCP 플래그, 내부 및 외부 호스트의 패킷 ▶ 내부 및 외부 호스트에서 시작된 활성 플로우 ▶ 내부 및 외부 활성 호스트

참고:

이러한 대시보드에 대한 자세한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

호스트 그룹 대시보드

Host Group Dashboard(호스트 그룹 대시보드)는 선택된 호스트 그룹에 대한 중요한 네트워크, 보안, 알람 활동의 그래픽 및 테이블 형식 데이터를 제공합니다. 이 데이터는 SMC에서 5분 간격으로 수집됩니다. 이 문서를 표시하려면 먼저 Enterprise(엔터프라이즈) 트리에서 데이터를 확인할 호스트를 클릭한 다음 SMC 메인 메뉴에서 **Status(상태) > Dashboard(대시보드) > Host Group Dashboard(호스트 그룹 대시보드)**를 선택합니다.

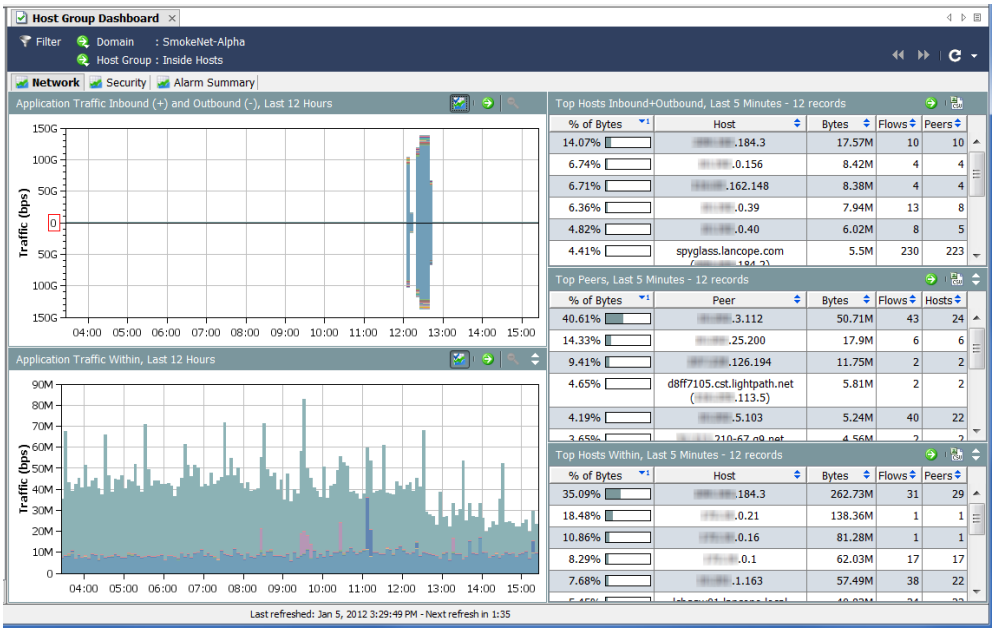


Host Group Dashboard(호스트 그룹 대시보드) 내에서 다음 페이지를 확인하는 방법에 대한 내용을 보려면 이 장의 나머지 부분에서 해당 섹션으로 이동하십시오.

- 네트워크 페이지
- 보안 페이지
- 알람 요약 페이지

호스트 그룹 대시보드 - 네트워크 페이지

Host Group Dashboard(호스트 그룹 대시보드): Network(네트워크) 페이지는 선택된 호스트 그룹에 대한 중요한 네트워크 관련 활동의 그래픽 및 테이블 형식 데이터를 제공합니다. 이 대시보드를 보려면 **Network(네트워크)** 탭을 클릭합니다.

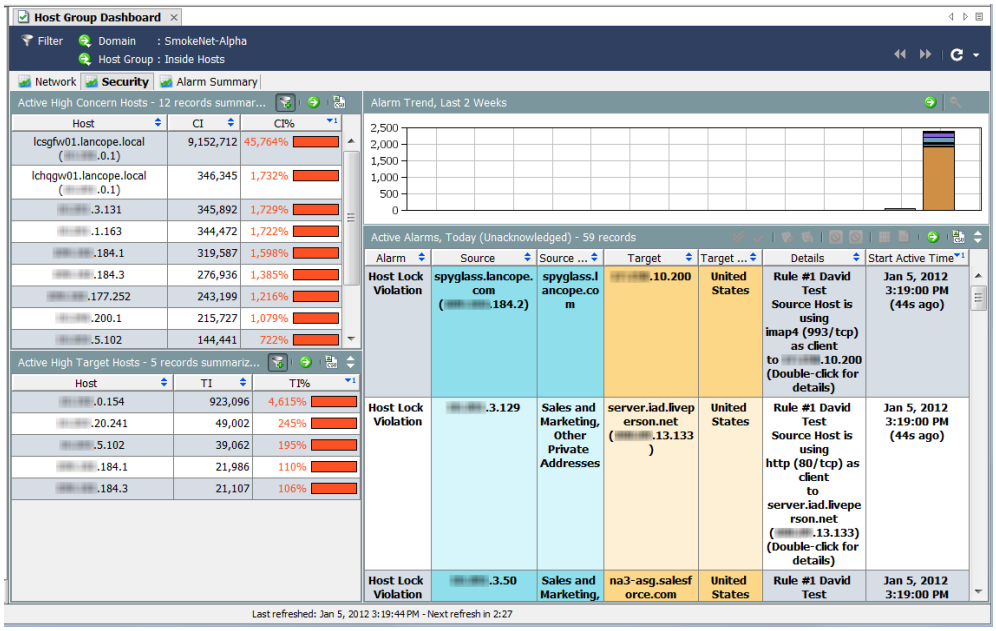


Network(네트워크) 페이지를 보면서 스스로에게 다음 질문을 해 보십시오.

- Application(애플리케이션) 그래프에 조직에서 일반적으로 사용하지 않는 애플리케이션에 대한 많은 양의 트래픽이 표시됩니까?
- 애플리케이션 그래프에 하루 중 특정 시간(예: 일반 근무 시간 이후)에 일반적으로 사용하지 않는 애플리케이션에 대한 많은 양의 트래픽이 표시됩니까?
- 애플리케이션 그래프에 Undefined(정의되지 않은) 애플리케이션 또는 Others(기타) 애플리케이션에 대한 상당한 양의 트래픽이 표시됩니까? 그렇다면 더 많은 애플리케이션 정의를 구성해야 합니다.
- Top Active Hosts(상위 활성 호스트) 테이블에 일반적으로 상위 활성 호스트 리스트에 있어서는 안 되는 호스트가 포함되어 있습니까?
- 상위 활성 호스트 테이블에 적은 수의 호스트가 매우 높은 비율의 트래픽을 차지하고 있는 것으로 나타납니까?

호스트 그룹 대시보드 - 보안 페이지

Host Group Dashboard(호스트 그룹 대시보드): Security(보안) 페이지는 첫 번째로 표시되는 대시보드입니다. 이 문서는 선택된 호스트 그룹에 대한 중요한 보안 관련 활동의 그래픽 및 테이블 형식 데이터를 제공합니다.



참고:

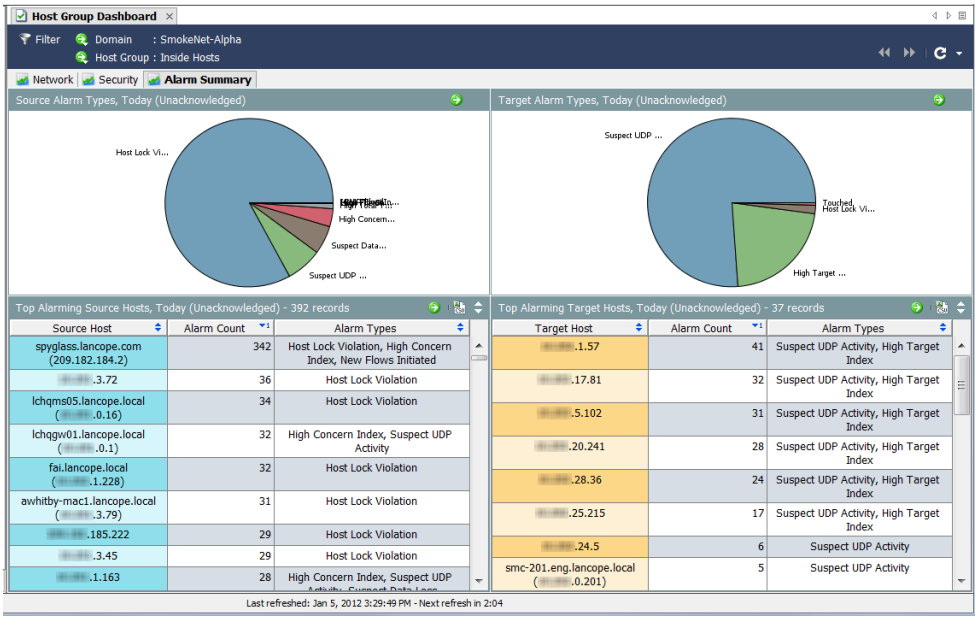
각 문서 헤더에서 **Go to Document(문서로 이동)** 버튼( )을 클릭하여 각 구성 요소를 개별 문서로 열 수 있습니다.

Security(보안) 페이지를 보면서 스스로에게 다음 질문을 해보십시오.

- High CI Hosts(상위 CI 호스트) 테이블에 조직에 중요한 호스트에 대한 상위 관심 지표가 표시됩니까?
- Alarm Report by Host Group(호스트 그룹별 알람 보고서) 테이블에 민감한 호스트 그룹에 대한 상위 관심 지표 알람이 표시됩니까?
- 호스트 그룹별 알람 보고서 테이블에 특정한 날에 상위 관심 지표 알람이 급증한 것으로 나타납니까?
- 상위 알람 호스트 테이블에 조직에 중요한 호스트에 대한 많은 수의 알람이 표시됩니까?
- 상위 알람 호스트 테이블에 특히 우려하는 알람 유형이 표시됩니까?
- Top Scans(상위 스캔) 테이블에 조직에 중요한 소스 호스트 또는 대상 호스트에 대한 많은 수의 TCP/UDP 주소 스캔이 표시됩니까?

호스트 그룹 대시보드 - 알람 요약 페이지

Host Group Dashboard(호스트 그룹 대시보드): Alarm Summary(알람 요약) 페이지는 선택된 호스트 그룹에 대한 알람 활동의 그래픽 요약 및 자세한 테이블 데이터를 제공합니다. 이 대시보드를 보려면 **Alarm Summary(알람 요약)** 탭을 클릭합니다.



Alarm(알람) 페이지를 보면서 스스로에게 다음 질문을 해보십시오.

- 테이블에 조직에 중요한 호스트 또는 호스트 그룹에 대한 많은 수의 알람이 표시됩니까?
- 테이블에 특히 우려하는 알람 유형이 표시됩니까?

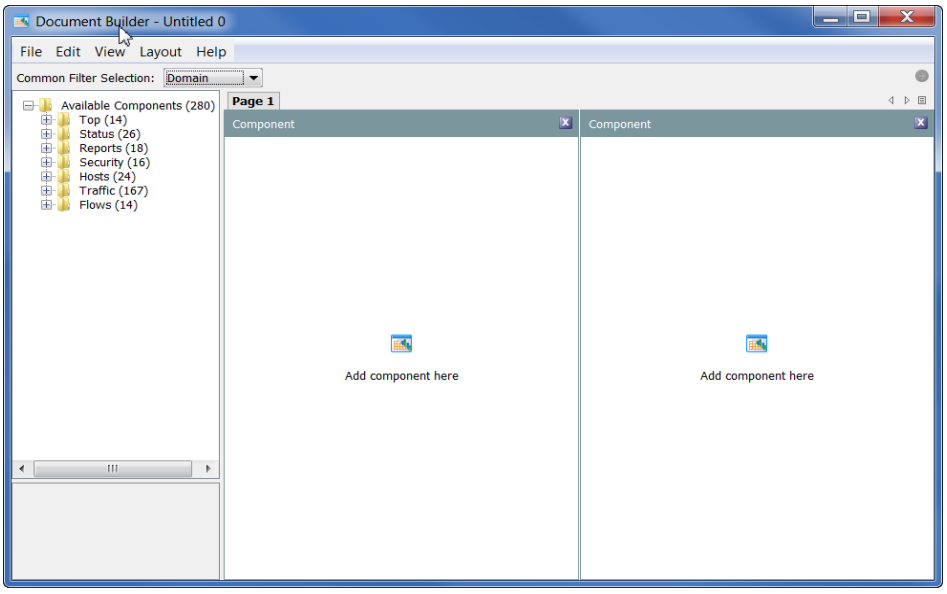
고유한 대시보드 구축

Document Builder(문서 작성기)를 사용하면 확인하려는 데이터와 함께 SMC 구성 요소를 포함하는 맞춤형 대시보드(다양한 보고서의 집합인 대시보드)를 만들 수 있습니다. 자신에게 적합한 텍스트로 이 구성 요소의 이름을 변경할 수도 있습니다.

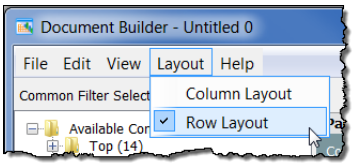
실례를 들기 위해 보안 알람에만 초점을 둔 Security Report(보안 보고서) 대시보드를 구축해 보겠습니다. 이 예에서 여러 구성 요소를 지닌 여러 탭을 사용할 것입니다. 그러나, 사용자가 필요한 대시보드 유형을 구축할 때 동일한 원칙을 사용할 수 있습니다.

고유한 맞춤형 대시보드를 구축하려면 다음 단계를 수행하십시오.

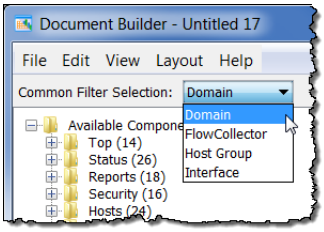
1. SMC 메인 메뉴에서 **View(보기) > Document Builder(문서 작성기)**를 선택합니다. Document Builder(문서 작성기) 대화 상자가 열립니다.



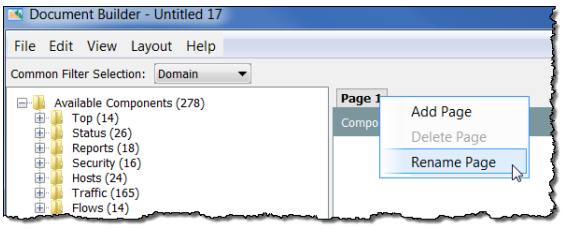
2. 열 형식(기본값) 대신 행 형식을 사용하는 문서가 필요한 경우, 문서 작성기 메인 메뉴에서 **Layout(레이아웃) > Row Layout(행 레이아웃)**을 선택합니다.

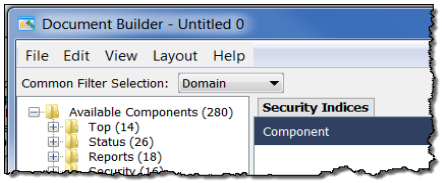


3. Common Filter Selection(공통 필터 선택 사항) 드롭다운 리스트에서 화살표를 클릭하고 이 문서를 기본적으로 필터링할 기준 옵션을 클릭합니다. 오른쪽 예에서 문서는 Domain(도메인)을 기준으로 필터링됩니다.



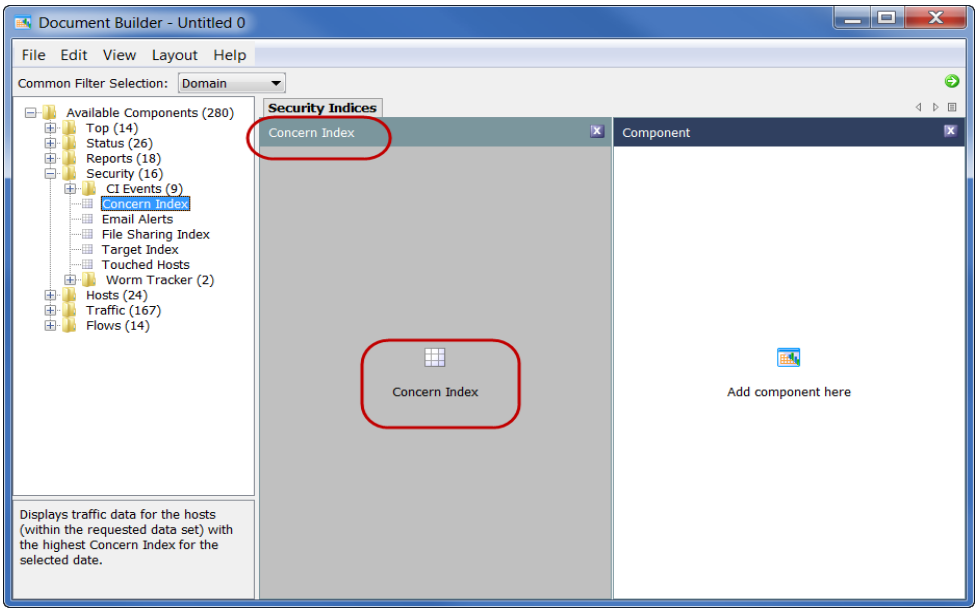
4. 페이지 이름을 변경하려면 페이지 탭을 마우스 오른쪽 버튼으로 클릭하고 **Rename Page(페이지 이름 변경)**를 선택합니다. (또한 탭을 더블 클릭하여 탭에 새 페이지 이름을 직접 입력할 수도 있습니다.)





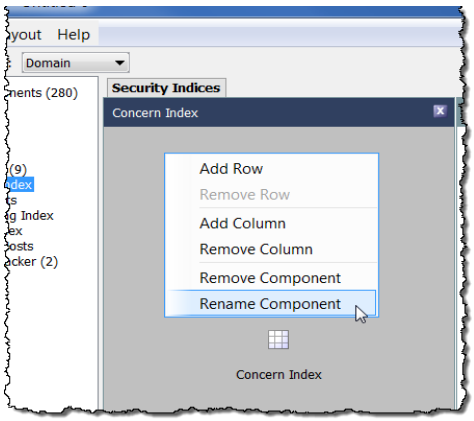
왼쪽 예에서는 페이지 탭에서 이름을 *Page 1(1페이지)*에서 *Security Indices(보안 지표)*로 변경했습니다.

5. 왼쪽 트리 메뉴에서 추가할 구성 요소를 클릭하고 원하는 페이지 영역으로 끌어옵니다. 다음 예에서는 Concern Index(관심 지표) 구성 요소를 왼쪽 열로 끌어왔습니다.

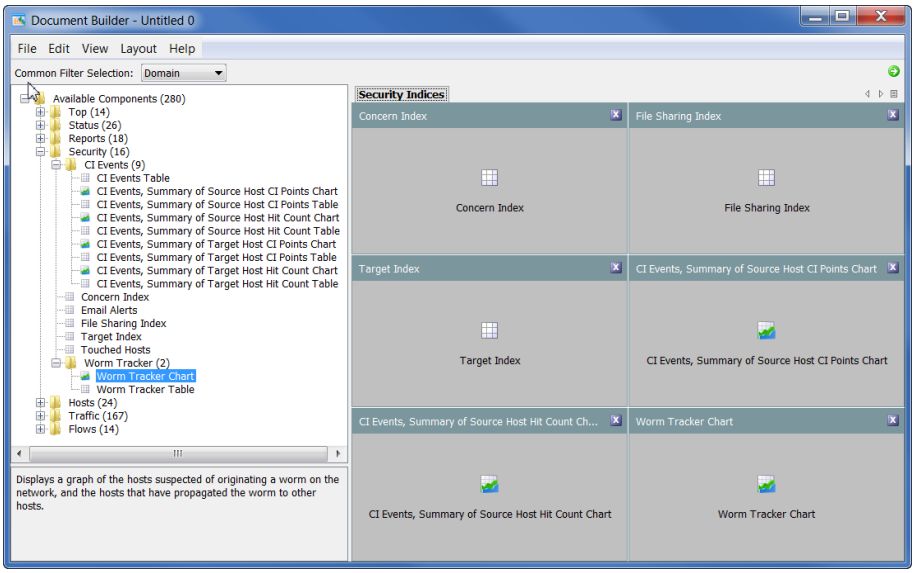


구성 요소 이름이 *Component(구성 요소)*에서 방금 추가한 구성 요소 이름인 *Concern Index(관심 지표)*로 변경된 방법을 확인하십시오. 또한 열 중간에서 아이콘 이름이 방금 추가한 구성 요소의 이름으로 변경되었는지 확인하십시오.

6. 구성 요소 이름을 변경하려면 구성 요소의 본문을 마우스 오른쪽 버튼으로 클릭하고 **Rename Component(구성 요소 이름 변경)**를 선택합니다.



7. 완료할 때까지 이 페이지에 구성 요소를 계속해서 추가합니다. 기본 페이지에는 구성 요소에 대해 두 개의 영역만 표시됩니다. 그러나, 3개 이상의 영역을 추가하는 경우 설정을 조정할 수 있습니다. 다음 예에서는 6개의 구성 요소가 있습니다. 열에 새 구성 요소를 추가할 때마다 해당 열의 마지막 항목 아래에 표시됩니다. 필요할 경우 언제든지 레이아웃을 변경할 수 있습니다.

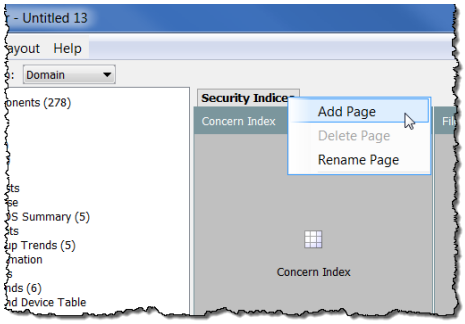


참고:

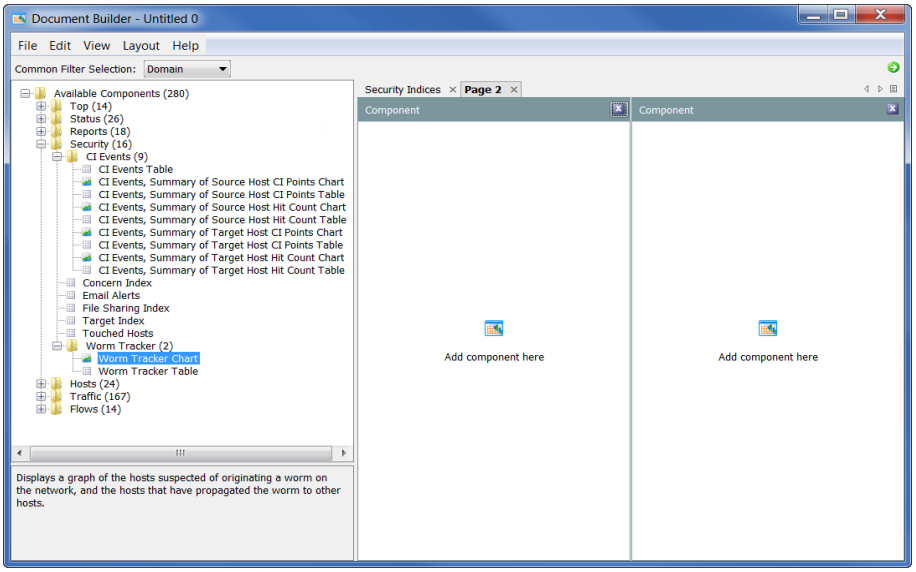
구성 요소 영역을 비우려면  버튼을 한 번 클릭합니다.

구성 요소 영역을 완전히 삭제하려면  버튼을 두 번 클릭합니다.

8. 다른 페이지(탭)를 문서에 추가하려면 기존 탭을 마우스 오른쪽 버튼으로 클릭하고 **Add Page(페이지 추가)**를 선택합니다.



새로운 빈 페이지가 열립니다.



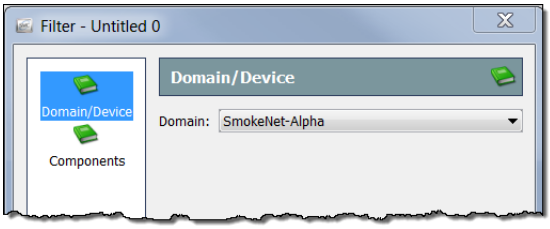
9. 첫 번째 페이지에서와 마찬가지로 구성 요소를 이 페이지에서 배치하려는 위치로 끌어옵니다.

10. 문서 작성을 완료하면 **File(파일) > Save As(다른 이름으로 저장)**를 클릭하여 하드 드라이브에 XML 템플릿으로 저장합니다.

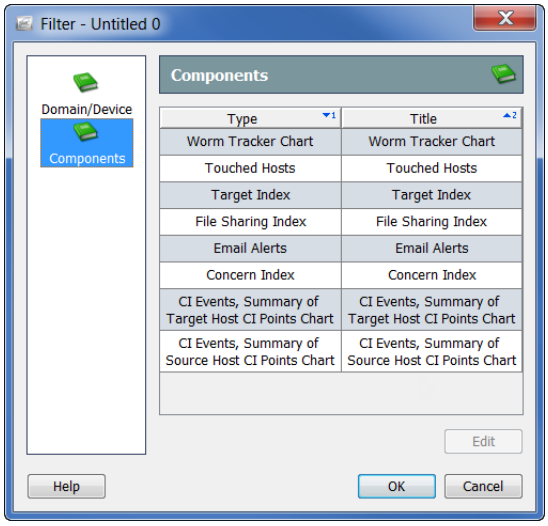
참고:

파일 이름이 문서 이름으로 사용됩니다. 예를 들어 파일 이름을 *1234*로 저장한 경우, 문서 제목이 *1234*가 됩니다. 따라서 문서에 의미 있는 파일 이름(예: *보안 보고서*)을 지정하십시오.

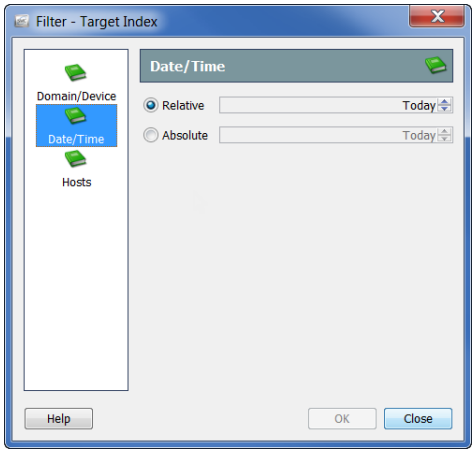
11. Document Builder(문서 작성기) 대화 상자의 오른쪽 상단 모서리에서 **Go to Document(문서로 이동)** 버튼()을 클릭하여 SMC 클라이언트 인터페이스에서 문서를 실행합니다. 문서의 Filter(필터) 대화 상자가 열립니다. 아직 강조 표시되지 않은 경우 **Domain/Device(도메인/디바이스)** 버튼을 클릭합니다. 필터링하려는 도메인이 선택되었는지 확인합니다.



12. **Component(구성 요소)** 버튼을 클릭합니다. 문서에 포함되어 있는 모든 구성 요소가 나열됩니다.

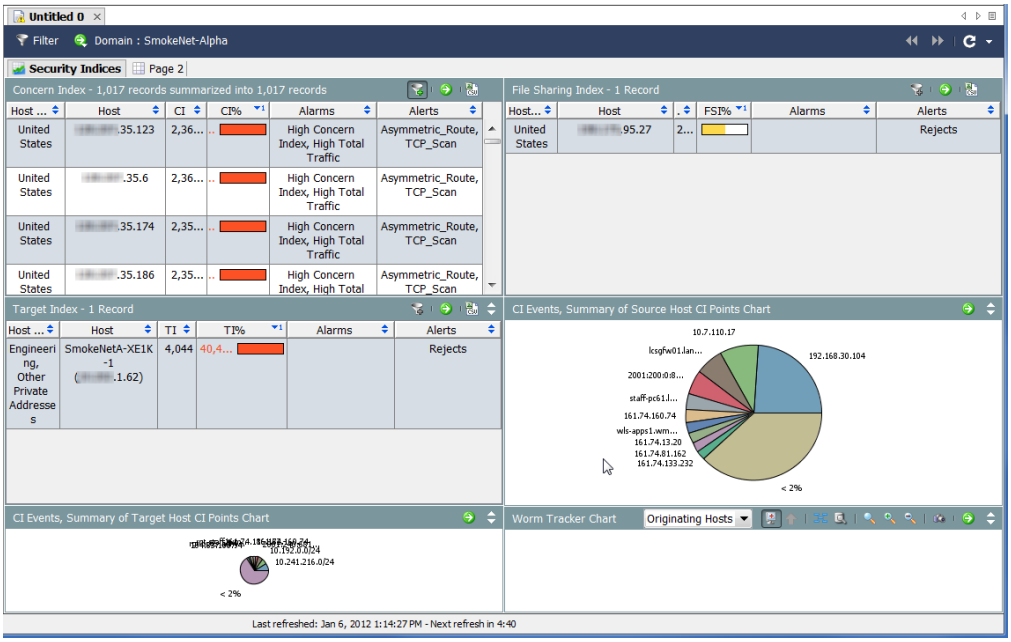


13. 필터링할 구성 요소를 클릭하고 **Edit(편집)**을 클릭합니다. 해당 구성 요소에 대한 Filter(필터) 대화 상자가 열립니다. (필터링할 수 있는 옵션은 대화 상자의 왼쪽에서 클릭하는 버튼에 따라 다릅니다.)



14. 선택한 후에 **OK(확인)**를 클릭합니다.

15. SMC GUI에서 새 문서가 열리면 다음 예와 유사하게 표시됩니다. 원하는 대로 열과 구성 요소의 크기를 조정합니다.



16. SMC Main Menu(메인 메뉴)에서 작업을 완료하면 **File(파일)> Save As(다른 이름으로 저장)**를 선택하고 문서를 SMC 서버에 저장하여 SMC에서 열 수 있도록 설정합니다.

참고:

파일 이름이 문서 이름으로 사용됩니다. 예를 들어 파일 이름을 *1234*로 저장한 경우, 문서 제목이 *1234*가 됩니다. 따라서 문서에 의미 있는 파일 이름(예: *보안 보고서*)을 지정하십시오.

17. Document Builder(문서 작성기)를 닫습니다.

참고:

Document Builder(문서 작성기)에서 이전에 저장한 XML 및 DAR 파일을 열어 필요할 때마다 편집할 수 있습니다.

6

지표: 행동 변경 순위 지정

개요

Stealthwatch에서는 지표를 사용하여 네트워크에서 호스트 이상 징후를 탐지할 수 있습니다. Stealthwatch Flow Collector는 전용 휴리스틱스(heuristics) 및 알고리즘을 사용하여 사용자 환경에서 정상 행동의 기준을 설정하여 관심 지표(CI) 포인트를 허용되지 않는 다양한 호스트 행동의 대상 호스트에 추가합니다. 누적된 지표 포인트가 허용 가능한 임계값을 초과할 경우, Flow Collector는 알람을 발생시킵니다.

지표는 비정상적인 행동이 어떠한지와 신뢰할 수 있는 Stealthwatch가 비정상적인 활동과 어떤 관련이 있는지를 나타내는 데 유용합니다. 즉, 지표는 조사의 우선 순위를 지정하는 데 도움이 됩니다.

예를 들어 낯선 사람이 현관 문 앞에서 잘못된 주소를 찾아 왔다고 하는 경우 경찰을 부를 이유가 없다고 생각할 것입니다. 관심 지표가 비교적 낮은 것입니다. 그러나, 낯선 사람이 계속해서 거리를 다니면서 이웃의 현관 앞에서 동일한 행동을 한다면 이 사람의 행동은 점점 더 의심스러워집니다.

낯선 사람이 이웃의 현관 앞에 접근할 때마다 관심 지표의 포인트가 높아집니다. 낯선 사람이 세 번째 문 앞에 접근할 때 경찰을 부를 정도의 관심이 생기게 됩니다. 이 경우, 이 행동에 대해 걱정할 필요가 없는 임계값은 두 번째 문 앞에서 하는 행동일 경우입니다. 세 번째 문에서는 임계값이 초과되고 무언가 조치를 취해야 할 것으로 생각하게 됩니다.

Stealthwatch 지표는 네트워크를 보호하기 위해 동일한 방식으로 많은 작업을 수행하며 비정상적인 활동이 허용되지 않는 레벨에 도달할 경우에만 알람을 발생시킵니다. 기본적으로, 이 지표에 빨간색으로 표시된 항목이 있으면 중대한 행동 변화가 발생했음을 의미합니다.

예를 들어 Stealthwatch가 CI 포인트를 할당하는 경우에도 단일 TCP 재설정이 알람을 유발하지 않습니다. 그러나, 시스템에서 허용으로 정의된 레벨을 기준으로 수많은 TCP 재설정이 알람을 유발할 수 있습니다.

Stealthwatch는 다음 지표를 사용하여 비정상적인 행동을 추적합니다.

- 관심 지표(CI) – 네트워크 무결성을 손상시킬 수 있는 활동을 수행하는 것으로 보이는 호스트를 추적합니다.
- 대상 지표(TI) – 다른 호스트의 의심스러운 행동으로 인한 희생자로 보이는 호스트를 추적합니다.
- 파일 공유 지수(FSI) – 피어-투-피어(P2P) 활동의 지표가 되는 행동을 추적합니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 관심 지표(CI)
- 대상 지표(TI)
- 파일 공유 지수

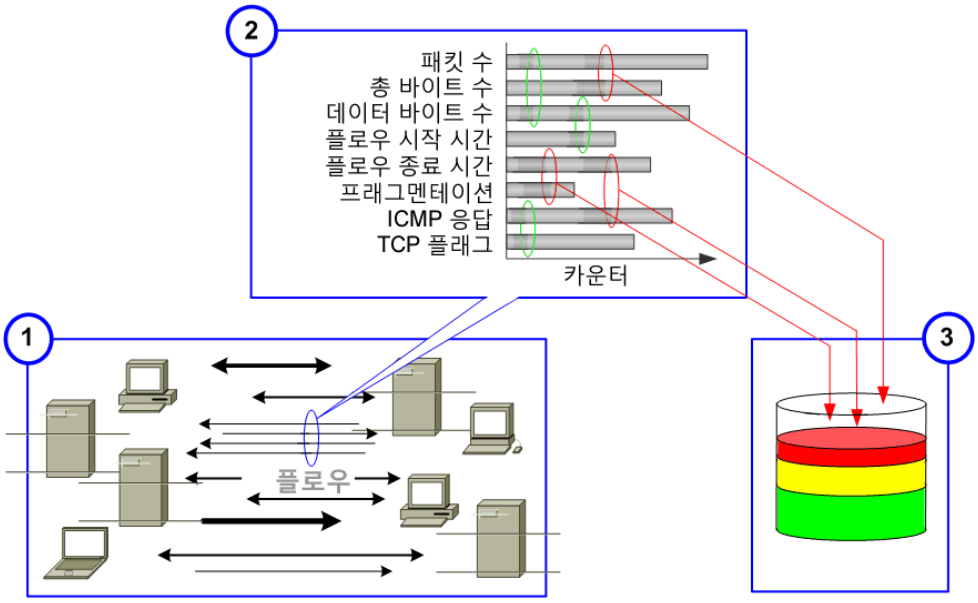
관심 지표(CI)

Concern Index(관심 지표, CI)는 Stealthwatch가 의심스러운 플로우 활동(예: 서비스 거부(DoS) 또는 스캐닝 활동 중에 네트워크 호스트로부터 응답을 호출하기 위해 의도적으로 전송되는 패킷)을 사용자에게 알려줄 때 사용하는 기본 수단입니다. Stealthwatch는 이렇게 발생한 활동을 Security Events(보안 이벤트)로 레이블을 지정합니다.

Security Event(보안 이벤트)는 보안 침해, 잘못 구성된 디바이스, 제대로 동작하지 않는 서버 또는 네트워킹 문제의 다른 원인을 나타낼 수 있습니다. Stealthwatch는 이 이벤트와 연관된 정보를 계속해서 추적하며 해당 호스트의 CI 점수를 높입니다. CI가 클수록 해당 행동에 대한 관심도 레벨이 높아집니다.

포인트 점수가 설정된 임계값을 초과하면 Stealthwatch는 활동 소스인 호스트를 대상으로 상위 CI 알람을 발생시킵니다. CI 값의 범위는 0포인트에서 수십만 포인트에 이를 수 있습니다.

다음 다이어그램은 증가하는 CI와 관련된 세 가지 기본 단계를 보여줍니다.



1. Stealthwatch Flow Collector는 호스트가 관련된 플로우를 관찰합니다.
2. Flow Collector는 이 행동을 허용 가능한 행동으로 구성된 활동과 비교합니다.
3. Flow Collector는 허용할 수 없는 호스트 활동의 일부를 찾아낸 다음 CI를 높입니다.

상위 관심 지표 알람을 지닌 내부 호스트는 일반적으로 호스트가 비정상적인 행동을 보여주고 있음을 나타내며 가능한 보안 침해, 오용 또는 정책 위반에 대해 검사를 받아야 합니다.

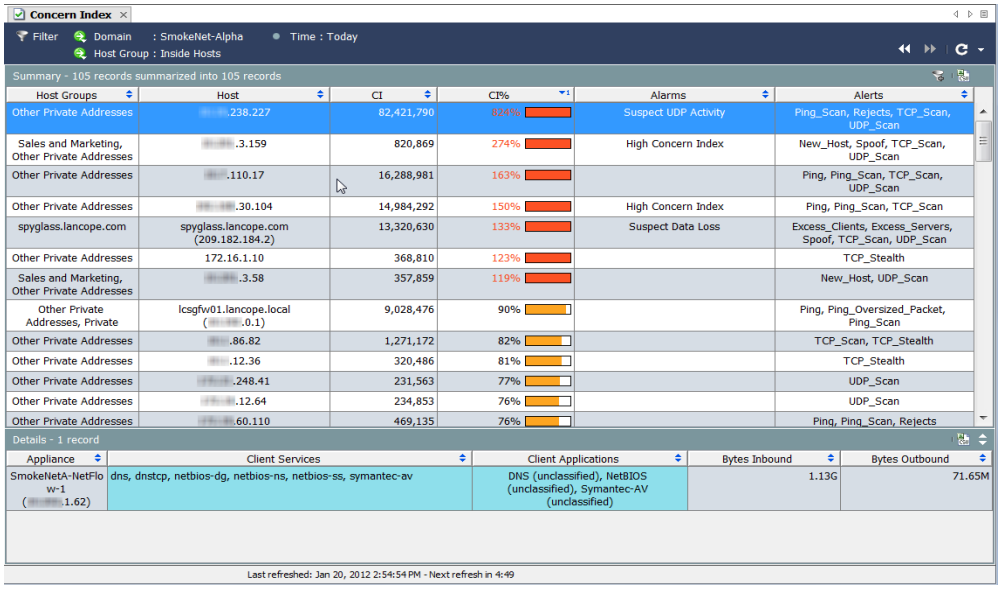
상위 관심 지표 알람을 지닌 외부 호스트는 네트워크 무결성을 위반하려는 시도 중에 "비정상적인 행동"을 하는 경우가 자주 있습니다. 두 경우 모두 관심 지표 문서는 네트워크를 공격하고 있는 호스트뿐만 아니라 어떤 호스트가 공격을 당하고 있는지를 식별하는 데 도움이 됩니다.

참고:

호스트 활동이 CI 임계값을 초과하고 연결된 호스트 그룹에 대한 상위 관심 지표 알람이 억제된 경우, Flow Collector는 해당 호스트에 대해 상위 관심 지표 알람을 발생시키지 않습니다.

Stealthwatch Flow Collector는 사용자가 정의한 *아카이브 시간*에 24시간마다 모든 지표 수를 지웁니다. 이때 Flow Collector는 이전 24시간 동안 수집한 로그 파일 및 웹 파일을 저장한 다음, 데이터를 수집하는 새로운 하루를 시작합니다.

관심 지표(CI) 문서는 마지막 아카이브 시간 이후에 가장 높은 CI 점수를 지닌 호스트에 대한 정보를 표시합니다.



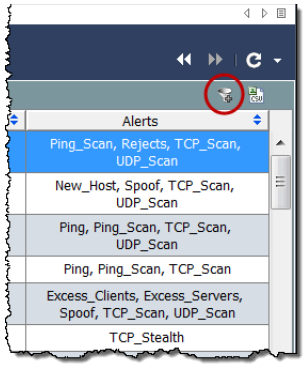
관심 지표 문서를 표시하려면 도메인 또는 호스트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Security(보안) > Concern Index(관심 지표)**를 선택합니다.

관심 지표 문서는 위협의 우선 순위를 정하고 실제로 중요한 이벤트에 집중하는 데 도움이 됩니다. 매일 수 천 개의 알람을 확인하는 대신 Stealthwatch는 가장 높은 심각도에서 가장 낮은 심각도 순으로 소수의 실행 가능한 항목을 제공합니다.

참고:

알림은 비정상적인 네트워크 활동에 대한 정보를 요약한 것이지만 알람과 달리, 통보되지 않습니다.

기본적으로 Concern Index(관심 지표) 필터 버튼()(문서의 오른쪽 상단 모서리에 있음)이 활성화되고 관심 지표는 활성 관심 지표 알람(즉, CI 퍼센트가 100 이상인 알람)을 지닌 호스트만 보여줍니다. CI 퍼센트가 50을 초과하는 호스트를 보려면 **Concern Index(관심 지표) 필터** 버튼을 클릭합니다. 활성 상위 관심 지표 알람이 존재하는지 여부에 관계없이 Concern Index(관심 지표) 필터 버튼의 더하기 기호가 회색()으로 변하고 CI 퍼센트가 50을 초과하는 호스트가 표시됩니다.



참고:

호스트에 대해 누적된 CI는 아카이브 시간에 지워집니다.

Concern Index(관심 지표)의 맨 위에는 Summary(요약) 섹션이 있으며 맨 아래에는 Details(세부사항) 섹션이 있습니다. Details(세부사항) 섹션에서 행에 대한 추가 정보를 보려면 Summary(요약) 섹션에서 행을 선택합니다.

이전 예에서 최고 위협 레벨을 지닌 호스트는 xxx.xxx.238.227입니다. 이 예에서는 이 호스트가 내부 호스트라고 가정하겠습니다. 이 호스트에 대한 다음 정보를 쉽게 확인할 수 있습니다.

- 마지막 아카이브 시간 이후에 이 호스트는 약 824%의 CI 퍼센트를 누적했습니다.
- 이 호스트는 2개의 알림인 Ping_Scan, Rejects(거부), TCP_Scan 및 UDP_Scan을 유발시켰습니다.
- 1.13G의 데이터를 수신했습니다.
- 71.65M의 데이터를 전송했습니다.

이 호스트는 CI 퍼센트, 알람, 알림 및 데이터 전송을 조합하여 보안 침해 가능성이 있는 것처럼 보이므로 보안 침해, 오용 또는 정책 위반 가능성을 검사 받아야 합니다.

Security Event(보안 이벤트)의 소스인 호스트에 대한 Host Snapshot(호스트 스냅샷)을 열려면 호스트 IP 주소를 더블 클릭합니다.

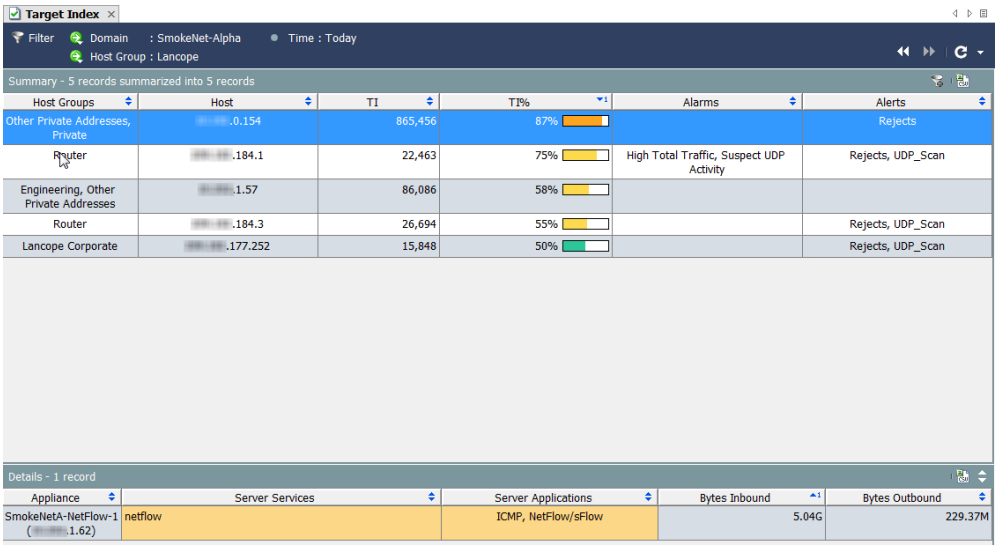
참고:

관심 지표 문서에서 확인할 수 있는 다양한 열에 대한 설명은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

대상 지표(TI)

대상 지표(TI)는 마지막 Stealthwatch Flow Collector 아카이브 시간 이후에 가장 높은 대상 지표를 지녔던 호스트(요청된 데이터 집합 내부에 있음)를 표시합니다. Stealthwatch Flow Collector는 대상 IP 주소가 많은 수의 보안 이벤트 또는 기타 악의적인 공격을 ***수신했거나*** 임계값을 초과한 경우 High Target Index(상위 대상 지표) 알람을 트리거합니다. 대상 지표의 목적은 많은 호스트가 단일 내부 호스트에서 직접 수행하는 분산된 공격 가능성을 알리는 것입니다.

보안이 침해된 호스트와 연결된 서비스 및 포트를 식별하면 방화벽에서 금지된 포트를 차단할 수 있으며 장비 및 소프트웨어에 따라 호스트 자체에서도 차단할 수 있습니다. 또한 네트워크에서 호스트의 연결을 끊고 연결을 취소할 수 있습니다.

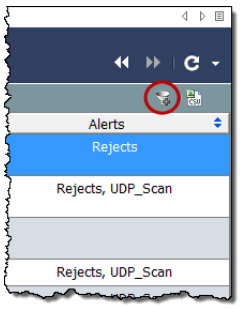


Target Index(대상 지표)를 표시하려면 도메인 또는 호스트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Security(보안) > Target Index(대상 지표)**를 선택합니다.

대상 지표 값의 범위는 0포인트에서 수십만 포인트에 이를 수 있습니다. 대상 지표(TI) 포인트는 각 호스트에 대해 누적되며 TI 알람을 유발할 수 있습니다. 기본적으로 데이터는 TI 퍼센트를 기준으로 내림차순으로 정렬됩니다. 이 데이터는 마지막 아카이브 시간 이후에 도메인에서 관찰된 가장 높은 데이터 값을 나타냅니다. 예를 들어 TI 퍼센트가 158인 호스트가 58%까지 자신의 TI 임계값을 초과했으며 추가 조사를 받을 수 있습니다. 다음 테이블에서 설명한 것과 같이 백분율 뒤에는 TI 임계값에 가까워지면 색상이 변하는 그래프가 나옵니다.

구성된 임계값의백분율	텍스트 색상
구성된 임계값의 0%	빈 그래픽
구성된 임계값의 0%~50%	녹색
구성된 임계값의 51%~75%	노란색
구성된 임계값의 76%~99%	주황색
구성된 임계값의 100% 이상	빨간색

기본적으로 Target Index Filter(대상 지표 필터) 버튼()(문서의 오른쪽 상단 모서리에 있음)이 활성화되고 Target Index(대상 지표)는 활성 대상 지표 알람(즉, 100보다 높은 TI 퍼센트를 지닌 알람)을 지닌 호스트만 보여줍니다. TI 퍼센트가 50을 초과하는 호스트를 보려면 **Target Index Filter(대상 지표 필터)** 버튼을 클릭합니다. Target Index(대상 지표) 필터 버튼의 더하기 기호가 회색()으로 변하고 TI 퍼센트가 50을 초과하는 호스트가 표시됩니다.

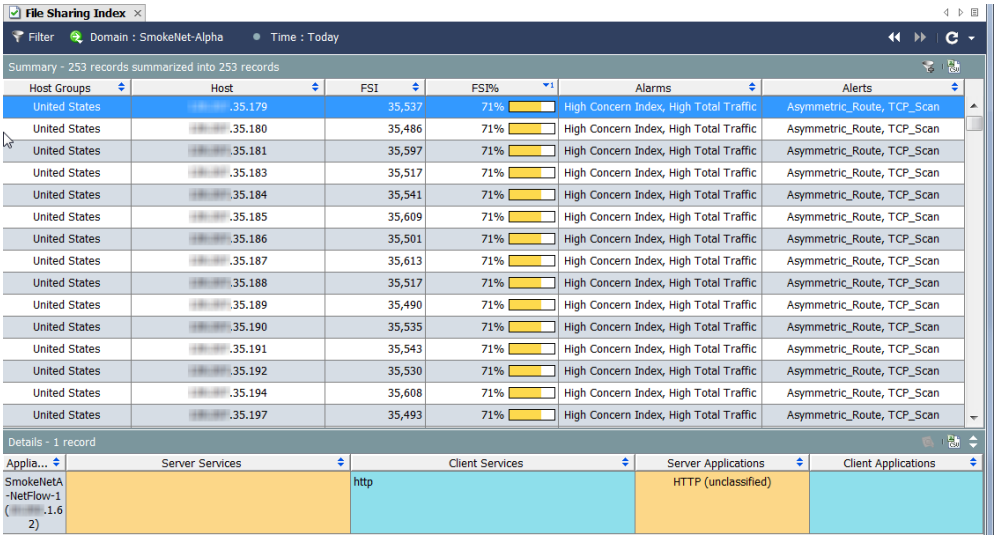


파일 공유 지수

File Sharing Index(파일 공유 지수, FSI)의 목표는 의심스러운 파일 공유 애플리케이션을 탐지하는 것으로, 특히 조직을 위험에 처하게 하는 피어-투-피어(P2P) 통신을 탐지합니다. 이것은 네트워크의 다른 내부 또는 외부와 저작권이 있는 자료를 공유함으로써 민감한 정보 전송 또는 조직 네트워크의 남용으로 인해 발생할 수 있습니다.

Stealthwatch Flow Collector는 네트워크에 있는 모든 호스트에서 수행하는 연결에 대한 다양한 정보를 수집합니다. 특정 통계의 상관서을 분석하여, File Sharing Index(파일 공유 지수)는 P2P 활동을 나타낼 수 있는 파일 전송과 관련된 것처럼 보이는 호스트를 식별하여 얻습니다.

이 지수는 상관 관계 분석 기법을 사용하여 포인트를 추가함으로써 파일 공유 활동과 가장 일반적으로 연관이 있는 센서 조합을 발생시켰거나 가장 활성 상태인 호스트를 표시합니다. 이 기술은 Stealthwatch Flow Collector가 스캔 활동을 표시하기 위해 사용하는 Concern Index(관심 지표) 값을 결정하는 기술과 유사합니다. File Sharing Index(파일 공유 지수) 문서는 조사할 호스트의 우선순위가 지정된 리스트와 선택적인 호스트 레벨 알람을 제공합니다.



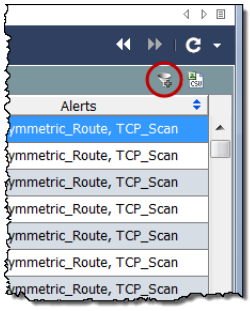
파일 공유 지수를 표시하려면 도메인 또는 호스트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Security(보안) > File Sharing Index(파일 공유 지수)**를 선택합니다.

파일 공유 지수 값의 범위는 0포인트에서 수십만 포인트에 이를 수 있습니다. 파일 공유 지수 포인트는 각 호스트에 대해 누적되며 File Sharing Index(파일 공유 지수) 알람을 유발할 수 있습니다. 기본적으로 데이터는 FSI 퍼센트를 기준으로 내림차순으로 정렬됩니다. 이 데이터는 마지막 아카이브 시간 이후에 도메인에서 관찰된 가장 높은 데이터 값을 나타냅니다. 예를 들어 FSI 퍼센트가 158인 호스트가 58%만큼 자신의 FSI 임계값을 초과했으며 추가 조사를 받을 수 있습니다.

다음 테이블에서 설명한 것과 같이 백분율 뒤에는 FSI 임계값에 가까워지면 색상이 변하는 그래프가 나옵니다.

구성된 임계값의백분율	텍스트 색상
구성된 임계값의 0%	빈 그래픽
구성된 임계값의 0%~50%	녹색
구성된 임계값의 51%~75%	노란색
구성된 임계값의 76%~99%	주황색
구성된 임계값의 100% 이상	빨간색

기본적으로 File Sharing Index(파일 공유 지수) 필터 버튼()(문서의 오른쪽 상단 모서리에 있음)이 활성화되고 File Sharing Index(파일 공유 지수)는 활성 파일 공유 지수 알람(즉, 100보다 높은 FSI 퍼센트를 지닌 알람)을 지닌 호스트만 보여줍니다. FSI 퍼센트가 50을 초과하는 호스트를 보려면 **File Sharing Index(파일 공유 지수) 필터** 버튼을 클릭합니다. File Sharing Index(파일 공유 지수) 필터 버튼의 더하기 기호가 회색()으로 변하고 FSI 퍼센트가 50을 초과하는 호스트가 표시됩니다.



7

트래픽 및 네트워크 성능 모니터링

개요

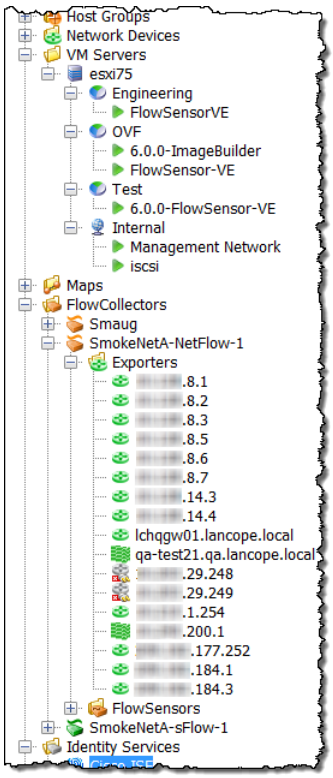
Stealthwatch는 네트워크 행동 분석을 사용하여 네트워크를 모니터링하고 잠재적인 문제를 나타낼 수 있는 변경 사항이 발생할 때 알려줍니다. 시스템은 호스트가 활성 상태인 시기, 호스트 간의 데이터 전송량, 관련 있는 트래픽 유형과 같은 행동을 기록하면서 네트워크에 있는 모든 호스트를 지속적으로 관찰합니다.

이 장에서는 호스트 및 네트워크 행동의 변경 사항을 확인할 수 있도록 네트워크에서 트래픽을 나타내는 그래픽과 테이블 형식 데이터에 액세스하는 방법에 대해 설명합니다. 따라서 잠재적인 위협이 존재하는 경우, 네트워크에 손해를 입히기 전에 이러한 위협을 해결할 수 있습니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 트래픽 모니터링
- 엑스포터/네트워크 디바이스
- 가상 머신

트래픽 모니터링



Enterprise(엔터프라이즈) 트리는 SMC 그래픽 사용자 인터페이스의 왼쪽에 있는 프레임입니다. 이 프레임은 트리 메뉴를 사용하여 시스템 상태를 확인하고 문서를 요청하기 위한 신속하고 쉬운 방법을 제공합니다.

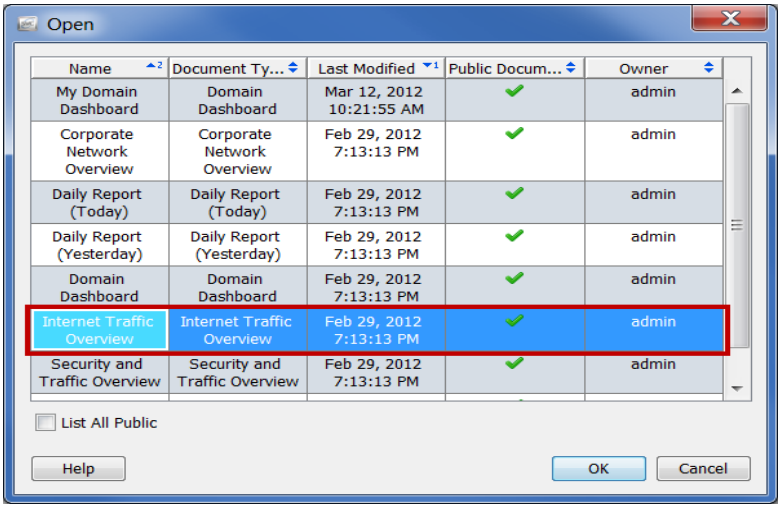
트래픽 모니터링을 위해 관심을 가져야 할 두 가지 주요 영역은 다음과 같습니다.

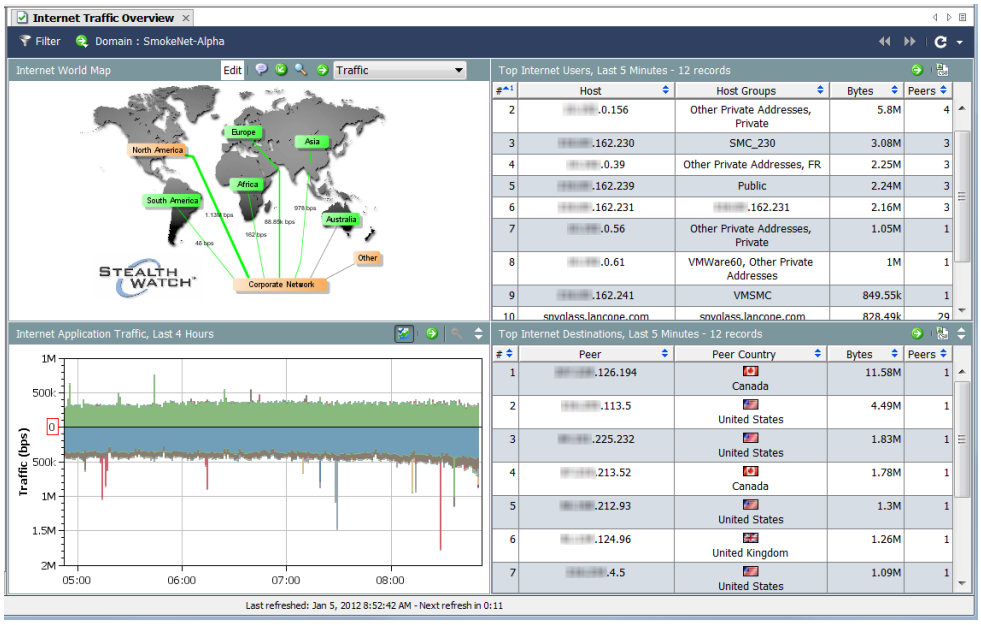
- 엑스포터 – Stealthwatch Flow Collector에 데이터를 전송하기 위해 구성된 라우터 또는 스위치입니다.
- VM – Stealthwatch FlowSensor에서 모니터링되는 가상 머신입니다.

왼쪽의 예는 엔터프라이즈 트리에서 엑스포터 및 VM을 찾을 수 있는 위치를 보여줍니다.

인터넷 트래픽 개요

Internet Traffic Overview(인터넷 트래픽 개요)는 인터넷과 연결된 도메인 트래픽의 그래픽과 테이블 형식 데이터를 제공합니다. 이 문서를 표시하려면 메인 메뉴에서 **File(파일) > Open(열기)**을 선택합니다. 다음 대화 상자가 열립니다. Internet Traffic Overview(인터넷 트래픽 개요) 문서를 선택하고 **OK(확인)**를 클릭합니다.





Internet World Map(인터넷 세계 지도)을 보면서 스스로에게 다음 질문을 해보십시오.

- 호스트 그룹 또는 호스트 그룹 관계가 위험 알람 또는 중대 알람을 표시하나요? 색상 및 설명선이 판단하는 데 도움이 됩니다.

  해당하는 경우, 호스트 그룹 또는 호스트 그룹 관계 알람 제공을 마우스 오른쪽 버튼으로 클릭한 다음 **Alarm Table(알람 테이블)**을 선택하여 더 많은 정보를 얻습니다.

- 문서 헤더의 드롭다운 리스트에서 화살표를 클릭하여 나타나는 데이터 유형을 변경합니다. 호스트 그룹 관계가 비정상적인 양의 정보를 표시하나요? 선의 두께와 선의 상태 텍스트가 판단하는 데 도움이 됩니다.

  해당하는 경우, 호스트 그룹 관계를 마우스 오른쪽 버튼으로 클릭한 다음 **Host Group Relationship Dashboard(호스트 그룹 관계 대시보드)**를 선택하여 더 많은 정보를 얻습니다.

Internet Application Traffic(인터넷 애플리케이션 트래픽)을 보면서 스스로에게 다음 질문을 해보십시오.

- 그래프가 조직에서 사용 중인 애플리케이션의 비정상적인 급증 현상을 보여줍니까?

팁:

Hide Others(기타 항목 숨기기) 버튼()을 클릭하여 가장 많이 사용되는 애플리케이션이 아닌 애플리케이션의 트래픽을 숨길 수 있습니다. 이 버튼은 데이터를 숨기거나 표시하도록 전환됩니다.

- 그래프가 조직에서 일반적으로 사용하지 않는 애플리케이션의 상당한 양의 트래픽을 보여줍니까?
- 그래프가 정의되지 않은 애플리케이션 또는 기타 애플리케이션의 상당한 양의 트래픽을 보여줍니까?

그렇다면 더 많은 애플리케이션 정의를 구성해야 합니다.

Top Internet Users(상위 인터넷 사용자)를 보면서 스스로에게 다음 질문을 해보십시오.

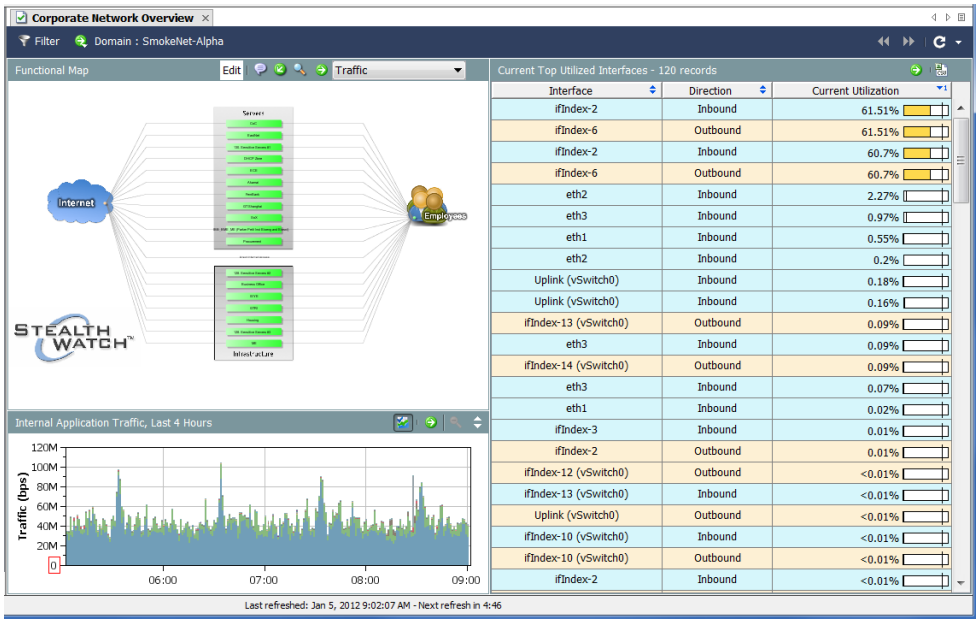
- 조직에서 상위 인터넷 사용자 중에 있어서는 안 되는 호스트에 대한 많은 양의 트래픽이 테이블에 표시됩니까?
- 서버 역할을 수행하고 있으며 많은 양의 트래픽을 전송하고 있는 조직의 호스트가 테이블에 표시됩니까?
- 많은 수의 피어에 트래픽을 전송하거나 피어에서 트래픽을 수신하는 조직의 호스트가 테이블에 표시됩니까?

Top Internet Destinations(상위 인터넷 대상)을 보면서 스스로에게 다음 질문을 해보십시오.

- 조직과 통신해서는 안 되는 피어의 많은 양의 트래픽이 테이블에 표시됩니까?
- 클라이언트 역할을 수행하고 있으며 조직에서 호스트로부터 많은 양의 트래픽을 수신하고 있는 피어가 테이블에 표시됩니까?
- 조직에서 많은 수의 호스트에 트래픽을 전송하거나 호스트로부터 트래픽을 수신하는 피어가 테이블에 표시됩니까?

회사 네트워크 개요

Corporate Network Overview(회사 네트워크 개요)는 회사 네트워크 전체와 연결된 도메인 트래픽의 그래픽과 테이블 형식 데이터를 제공합니다. 이 문서를 표시하려면 메인 메뉴에서 **File(파일) > Open(열기)**을 선택합니다. Open(열기) 대화 상자가 열립니다. Corporate Network Overview(회사 네트워크 개요) 문서를 선택하고 **OK(확인)**를 클릭합니다.



Functional Map(기능 맵)을 보면서 스스로에게 다음 질문을 해보십시오.

- 호스트 그룹 또는 호스트 그룹 관계가 위험 알람 또는 중대 알람을 표시하나요? 색상 및 설명선이 판단하는 데 도움이 됩니다.

  해당하는 경우, 호스트 그룹 또는 호스트 그룹 관계 알람 제공을 마우스 오른쪽 버튼으로 클릭한 다음 **Alarm Table(알람 테이블)**을 선택하여 더 많은 정보를 얻습니다.

- 문서 헤더의 드롭다운 리스트에서 화살표를 클릭하여 나타나는 데이터 유형을 변경합니다. 호스트 그룹 관계가 비정상적인 양의 정보를 표시하나요? 선의 두께와 선의 상태 텍스트가 판단하는 데 도움이 됩니다.

  해당하는 경우, 호스트 그룹 관계를 마우스 오른쪽 버튼으로 클릭한 다음 **Host Group Dashboard(호스트 그룹 대시보드)**를 선택하여 더 많은 정보를 얻습니다.

Internal Application Traffic(내부 애플리케이션 트래픽)을 보면서 스스로에게 다음 질문을 해보십시오.

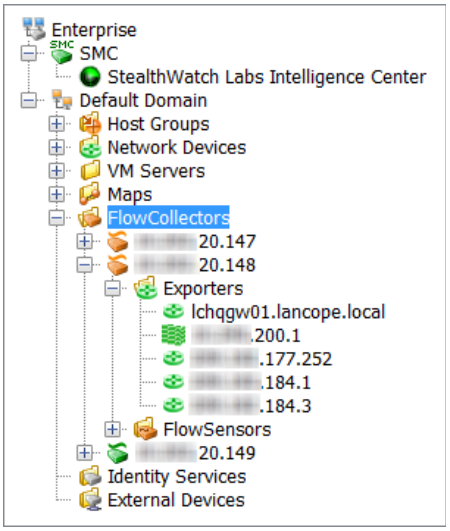
- 그래프가 조직에서 사용 중인 애플리케이션의 비정상적인 급증 현상을 보여줍니까?
- 그래프가 조직에서 일반적으로 사용하지 않는 애플리케이션의 상당한 양의 트래픽을 보여줍니까?
- 그래프가 정의되지 않은 애플리케이션 또는 기타 애플리케이션의 상당한 양의 트래픽을 보여줍니까? 그렇다면 더 많은 애플리케이션 정의를 구성해야 합니다.

Current Top Utilized Interface(현재 상위 활용 인터페이스)를 보면서 스스로에게 다음 질문을 해보십시오.

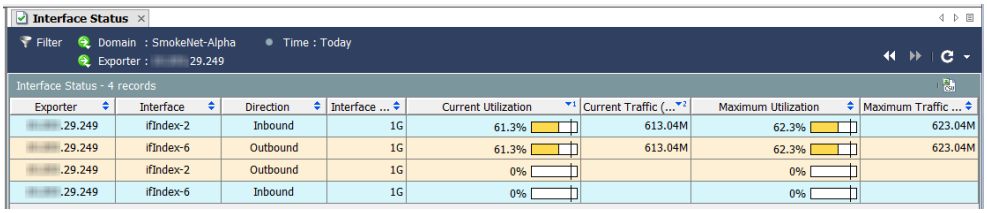
- 테이블이 포화된(즉, 비정상적으로 높은 비율의 사용률을 나타냄) 인터페이스가 테이블에 표시됩니까?
- 상위 사용자에 포함되어서는 안 되는 인터페이스가 테이블에 표시됩니까?

엑스포터/네트워크 디바이스

엑스포터는 오른쪽 예에서와 같이 데이터를 수신하는 Stealthwatch Flow Collector 아래에 있는 트리에 있습니다.



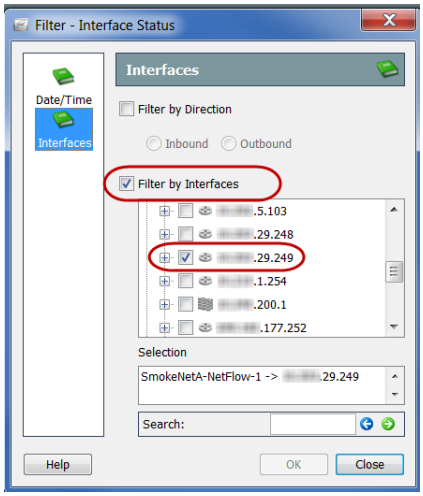
엑스포터에 대한 문서를 직접 탐색하려면 Enterprise(엔터프라이즈) 트리에서 적절한 호스트 아래에 있는 Network Devices(네트워크 디바이스) 옵션을 확장한 다음 엑스포터를 더블 클릭합니다. Interface Status(인터페이스 상태) 문서가 열립니다. 이 문서는 sFlow용 Stealthwatch Flow Collector 또는 NetFlow용 Stealthwatch Flow Collector에 데이터를 전송하는 라우터 또는 스위치(즉, 엑스포터)에서 인터페이스에 대한 통계를 표시합니다.



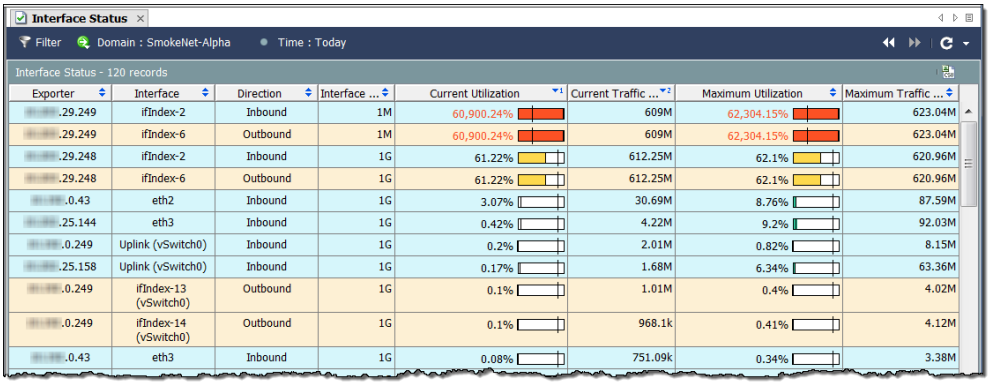
참고:

Interface Status(인터페이스 상태) 문서는 Cisco ASA 엑스포터 유형에 사용할 수 없습니다.

Interface Status(인터페이스 상태) 문서의 좌측 상단에서 **Filter(필터)** 버튼( )을 클릭합니다. 열리는 Filter - Interface Status(필터 - 인터페이스 상태) 대화 상자에서 아직 강조 표시되지 않은 경우, **Interfaces(인터페이스)** 버튼을 클릭합니다.

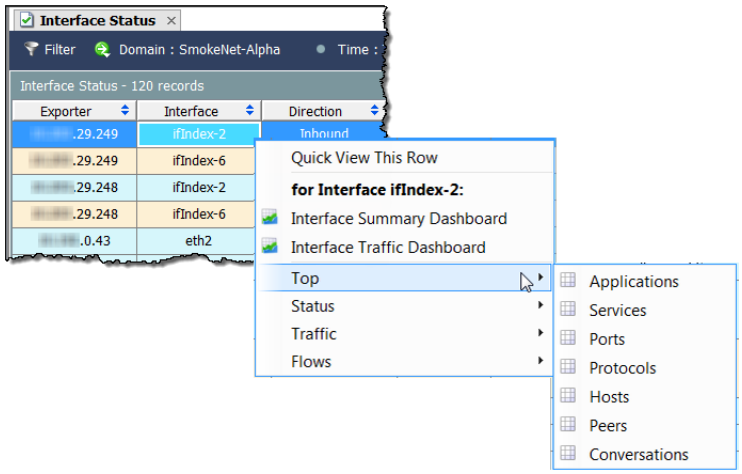


Filter by Interfaces(필터링 기준: 인터페이스) 확인란을 클릭하여 체크 마크를 제거합니다. 다음으로, 문서를 현재 필터링하고 있는 엑스포터를 찾습니다(체크 마크가 있는 유일한 엑스포터). 이 엑스포터의 확인란을 클릭하여 체크 마크를 제거한 다음 **OK(확인)**를 클릭합니다. 다음 예에서와 같이 Interface Status(인터페이스 상태) 문서는 이제 전체 도메인에 대한 트래픽 통계를 보여줍니다.

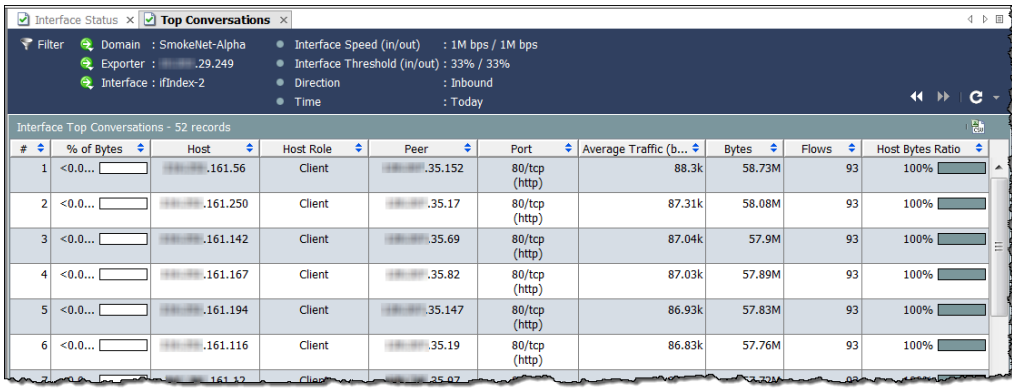


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

Interface(인터페이스) 열에서 인터페이스를 마우스 오른쪽 버튼으로 클릭하고 **Top(상위)**을 선택합니다. 여러 가지 옵션을 선택할 수 있는 팝업 메뉴가 나타납니다.



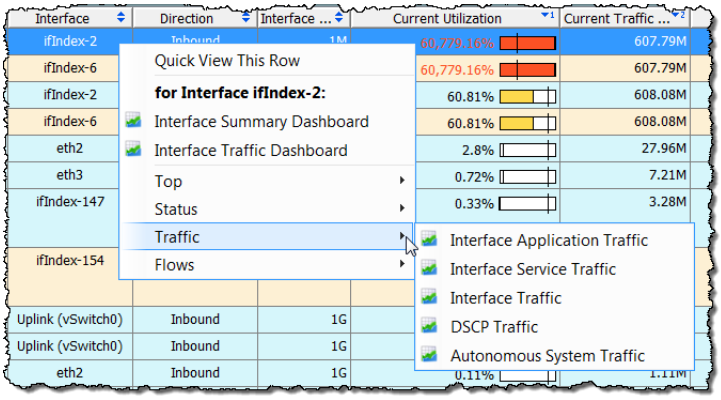
예를 들어, **Top(상위) > Conversations(대화)**을 선택한 경우, 다음 예에서와 같이 Top Conversations(상위 대화) 문서가 표시됩니다. Top Conversations(상위 대화) 문서는 상위 대화에 따라 플로우 데이터를 나열합니다. 방향(필터에서 변경 가능)은 데이터가 모든 트래픽(즉, 전체), 선택한 항목에 대한 트래픽 인바운드, 선택한 항목에서의 트래픽 아웃바운드 또는 선택한 항목 내에서의 트래픽을 포함하는지 여부를 나타냅니다.



팁:

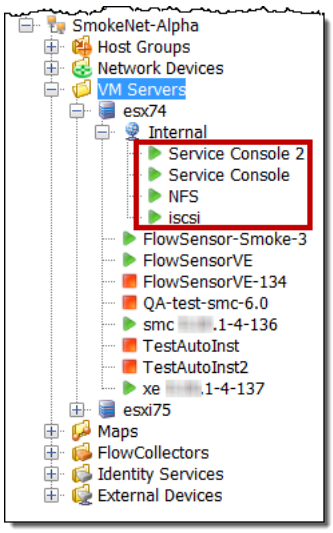
인터페이스를 더블 클릭하여 Summary Report(요약 보고서)를 열 수 있습니다.

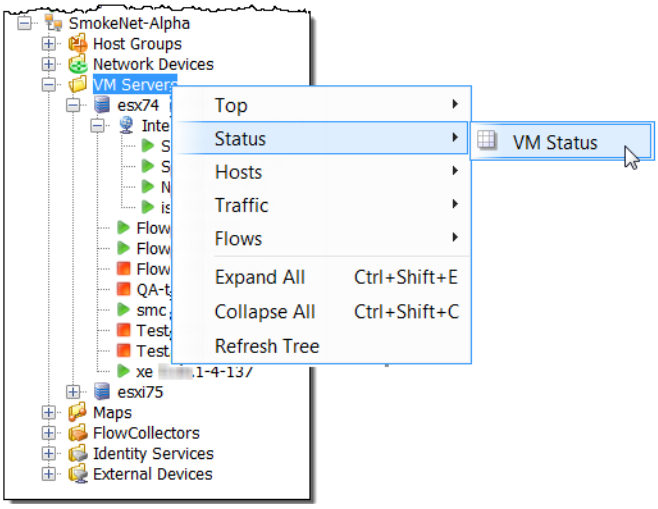
열 내에서 마우스 오른쪽 버튼으로 클릭한 다음 첫 번째 팝업 메뉴에서 **Traffic(트래픽)**을 선택하여 트래픽을 모니터링하는 데 유용한 다른 여러 문서를 찾을 수 있습니다.



가상 머신

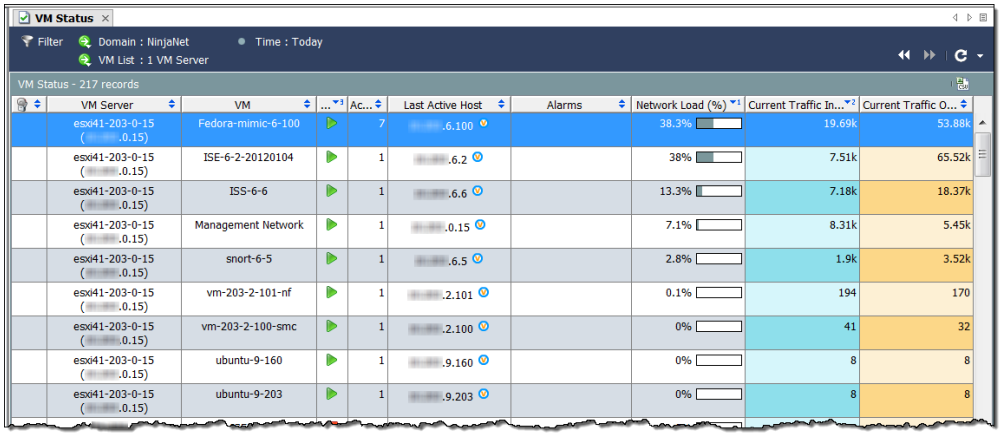
VM은 오른쪽 예에서와 같이 연결된 VM 서버(및 존재하는 경우 리소스 그룹) 아래에 있는 Enterprise(엔터프라이즈) 트리에 있습니다.





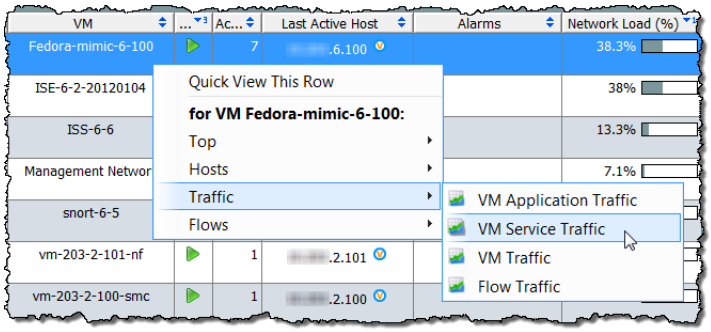
특정 VM 서버에서 VM의 상태를 확인해 보도록 하겠습니다. 이렇게 하려면 VM 서버를 마우스 오른쪽 버튼으로 클릭하고 **Status(상태) > VM Status(VM 상태)**를 선택합니다.

VM Status(VM 상태) 문서가 열립니다. 이 문서는 동일한 VM 서버에 있는 VM에 대한 유용한 통계를 보여줍니다.

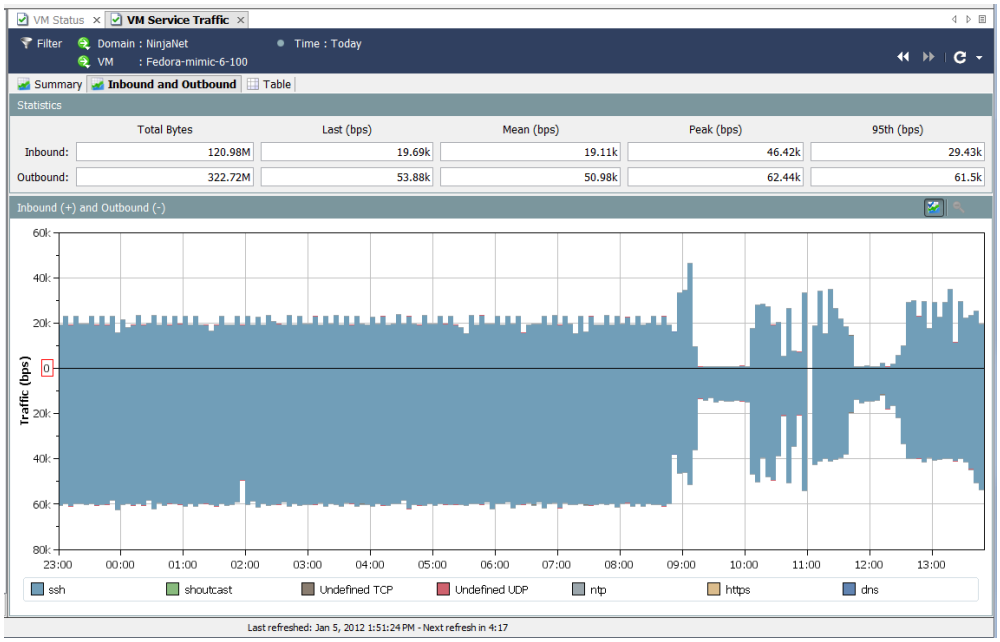


참고:

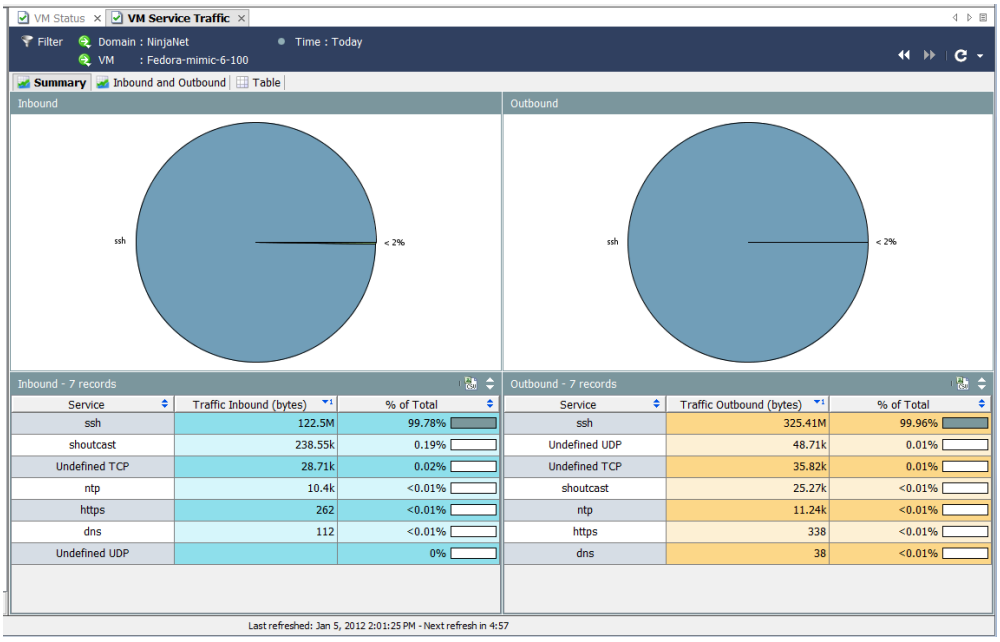
이 문서를 사용하여 시스템에서 가장 많이 사용된 VM에 대한 자세한 정보를 찾을 수 있습니다. 예를 들어 VM을 마우스 오른쪽 버튼으로 클릭하여 해당 VM에 맞게 필터링된 다른 유용한 문서를 볼 수 있습니다.



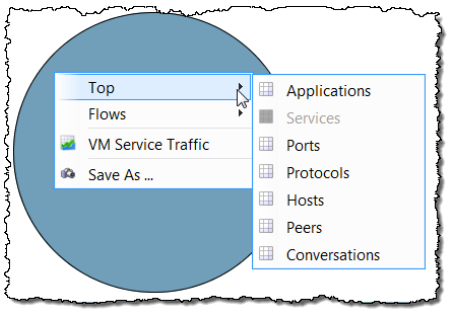
VM을 마우스 오른쪽 버튼으로 클릭하고 **Traffic(트래픽) > VM Service Traffic(VM 서비스 트래픽)**을 선택합니다. 다음 예에서와 같이 VM Service Traffic(VM 서비스 트래픽) 문서가 열립니다. 이 문서는 사용했던 상위 10개의 서비스에 따라 선택한 VM에 대해 전송 및 수신된 트래픽 데이터를 모두 보여줍니다.



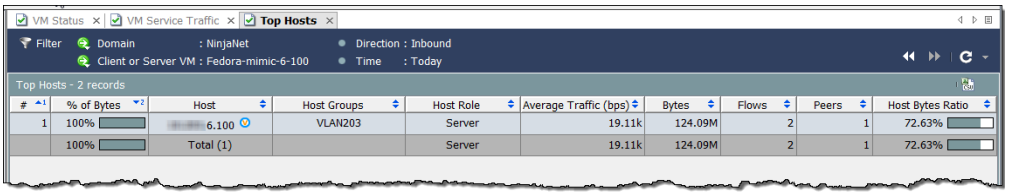
Summary(요약) 탭을 클릭하여 파이 차트에 요약된 데이터를 확인합니다.



VM Service Traffic(VM 서비스 트래픽) 문서에서 추가로 세분화할 수 있습니다. 예를 들어 특정 서비스에 대해 너무 많은 트래픽이 표시되는 경우, 차트 또는 테이블에 있는 항목을 마우스 오른쪽 버튼으로 클릭하고 **Top(상위)**을 선택합니다. 여러 가지 옵션을 선택할 수 있는 팝업 메뉴가 나타납니다.

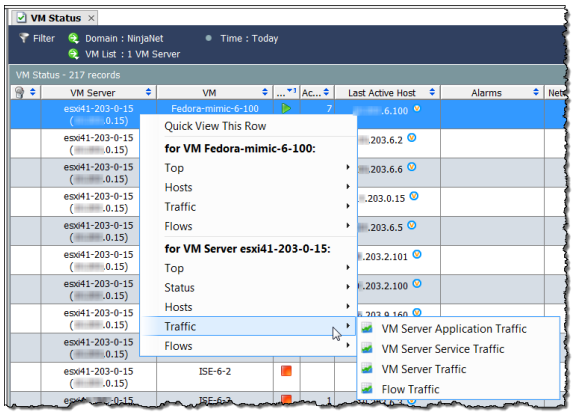


예를 들어, **Top(상위) > Hosts(호스트)**를 선택한 경우, Top Hosts(상위 호스트) 문서가 표시됩니다.



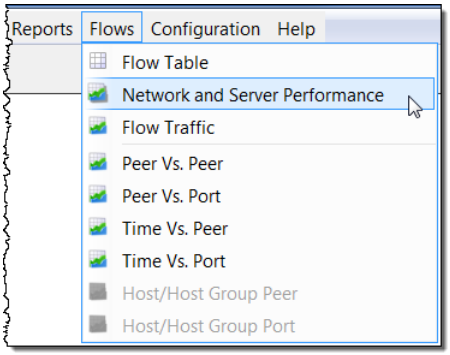
Top Hosts(상위 호스트) 문서는 상위 호스트에 따라 플로우 데이터를 나열합니다. 방향(필터에서 변경 가능)은 데이터가 모든 트래픽(즉, 전체), 선택한 항목에 대한 트래픽 인바운드, 선택한 항목에서의 트래픽 아웃바운드 또는 선택한 항목 내에서의 트래픽을 포함하는지 여부를 나타냅니다.

열 내에서 마우스 오른쪽 버튼으로 클릭한 다음 첫 번째 팝업 메뉴에서 **Traffic(트래픽)**을 선택하여 트래픽을 모니터링하는 데 유용한 다른 여러 문서를 찾을 수 있습니다.



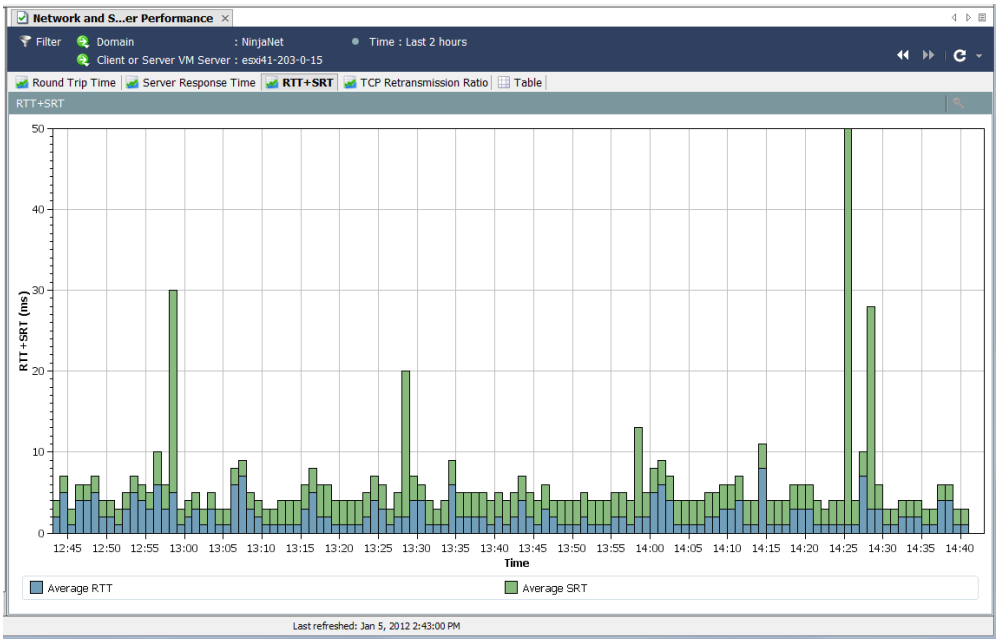
네트워크 성능

"느린 인터넷"에 대해 불평하는 직원이 있다고 가정해 보겠습니다. 이러한 유형의 문제를 조사하기 위해 Network and Server Performance(네트워크 및 서버 성능) 문서를 사용할 수 있습니다. 메인 메뉴에서 이 문서에 액세스하려면 **Flows(플로우) > Network and Server Performance(네트워크 및 서버 성능)**를 선택합니다.



참고:

이 보고서에는 이 보고서를 채우는 특정 값을 수집하기 위해 Stealthwatch FlowSensor가 필요합니다.



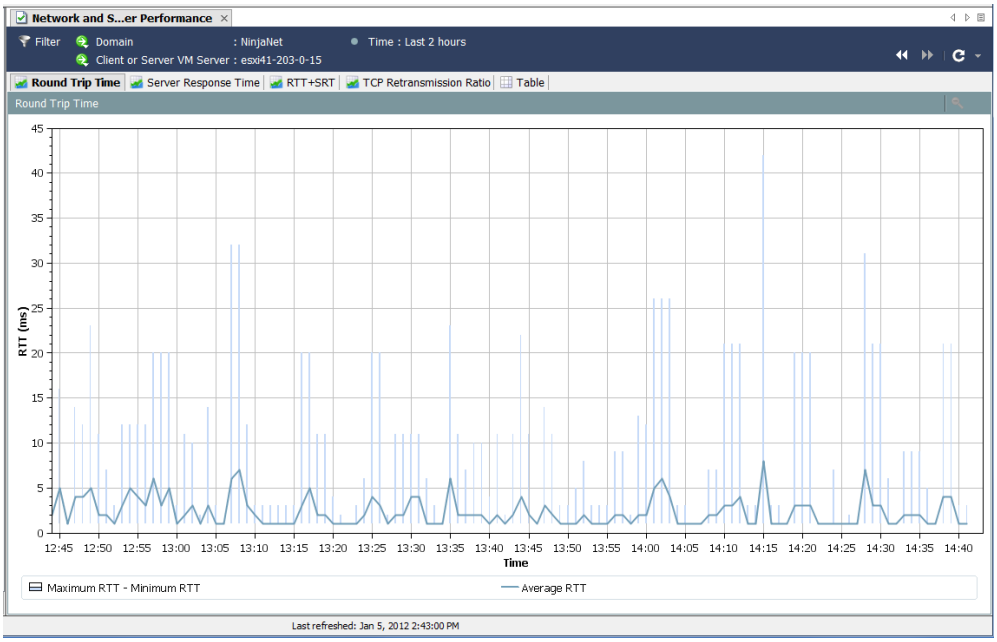
Network and Server Performance(네트워크 및 서버 성능) 문서는 데이터베이스에 저장된 플로우에 대한 다양한 성능 데이터를 표시합니다. 이 데이터를 보려면 문서 상단에 위치한 다음 탭에 액세스하십시오.

- 왕복 시간
- 서버 응답 시간
- RTT+SRT

- TCP 재전송 비율
- 테이블

왕복 시간

Round Trip Time(왕복 시간) 탭은 플로우의 왕복 시간에 대한 통계를 그래픽으로 표시합니다.

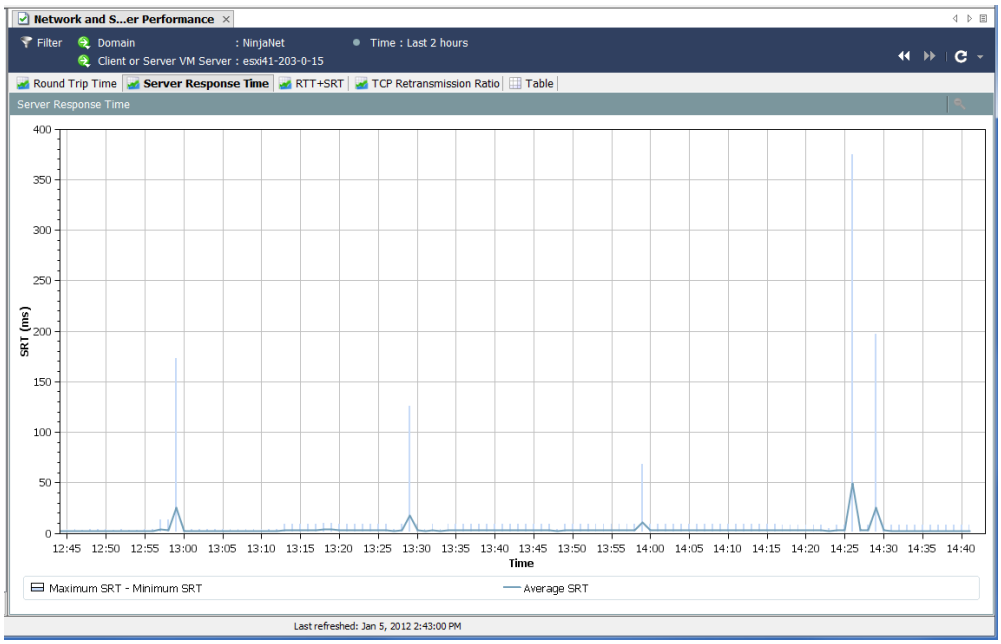


이 기능은 멀리 떨어져 있는 호스트 그룹 간에 플로우를 완료하는 데 필요한 시간을 측정하는 데 유용합니다. Filter(필터)에서 Hosts(호스트) 페이지를 사용하여 설정할 수 있습니다.

그래프의 맨 아래에 있는 어두운 선은 계산된 평균 RTT를 나타내며 길고 얇은 선은 매분 계산된 최소 및 최대 RTT 사이의 분포를 나타냅니다.

서버 응답 시간

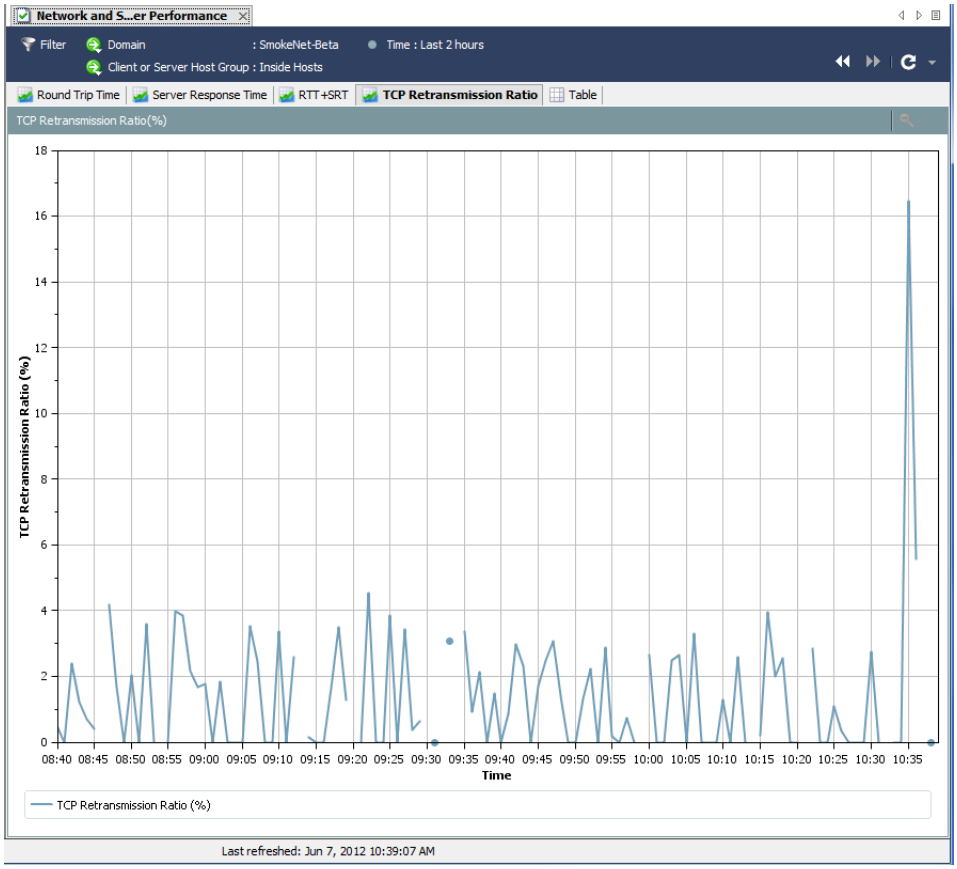
Server Response Time(서버 응답 시간) 탭은 플로우의 서버 응답 시간(SRT)에 대한 통계를 그래픽으로 표시합니다.



이 기능은 서버가 요청에 응답하는 데 필요한 시간을 측정하는 데 유용합니다. 예를 들어 화면이 "내용을 채우는 데 매우 오래 걸리기" 때문에 사용자가 웹 기반 애플리케이션의 성능이 불량하다고 불평합니다. 이 문서를 사용하여 서버의 SRT를 관찰하고 평균 SRT를 서버에서 사용자의 평균 SRT와 비교할 수 있습니다.

TCP 재전송 비율

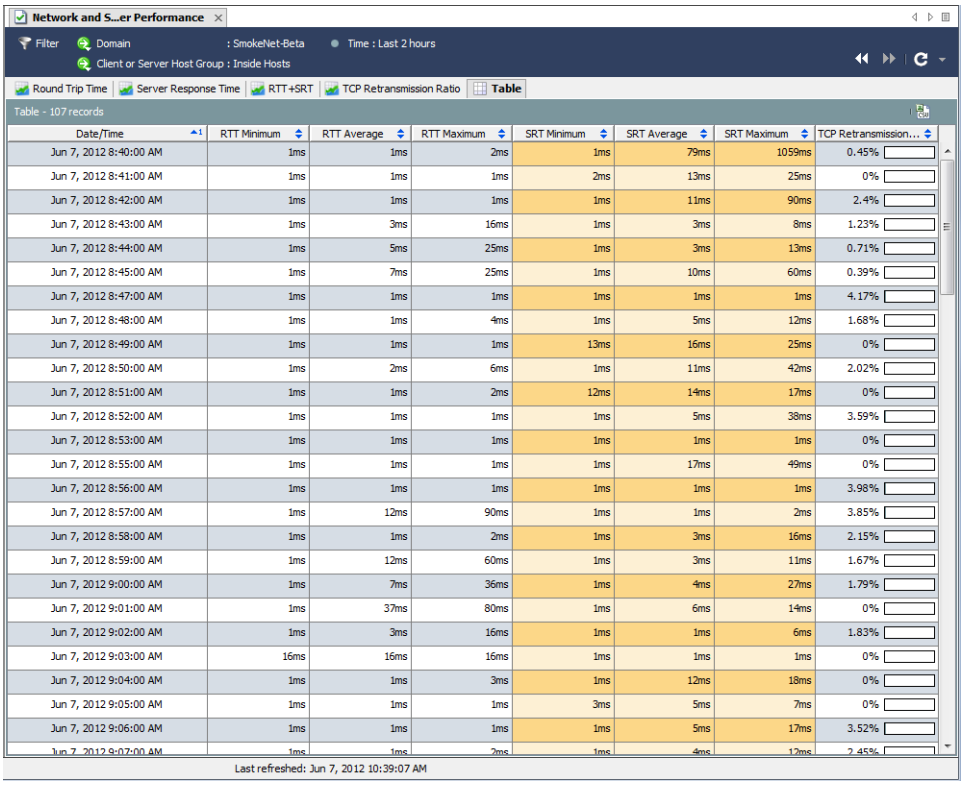
Network and Server Performance(네트워크 및 서버 성능) 문서의 TCP Retransmission Ratio(TCP 재전송 비율) 탭은 재전송된 패킷의 백분율을 그래픽으로 표시합니다. 데이터는 데이터 레코드 사이에서 1분 간격이며 기본적으로 2시간 동안 다뤄집니다. 재전송은 일반적으로 패킷이 손상되거나 손실되기 때문에 발생합니다.



참고:
이 문서는 Stealthwatch FlowSensor에서 데이터를 수신 중인 NetFlow용 Stealthwatch Flow Collector가 있는 도메인에서만 사용 가능합니다.

테이블

Network and Server Performance(네트워크 및 서버 성능) 문서의 Table(테이블) 탭은 플로우에 대한 성능 데이터를 나열합니다. 데이터는 데이터 레코드 사이에서 1분 간격이며 기본적으로 2시간 동안 다뤄집니다.



Date/Time	RTT Minimum	RTT Average	RTT Maximum	SRT Minimum	SRT Average	SRT Maximum	TCP Retransmission...
Jun 7, 2012 8:40:00 AM	1ms	1ms	2ms	1ms	79ms	1059ms	0.45%
Jun 7, 2012 8:41:00 AM	1ms	1ms	1ms	2ms	13ms	25ms	0%
Jun 7, 2012 8:42:00 AM	1ms	1ms	1ms	1ms	11ms	90ms	2.4%
Jun 7, 2012 8:43:00 AM	1ms	3ms	16ms	1ms	3ms	8ms	1.23%
Jun 7, 2012 8:44:00 AM	1ms	5ms	25ms	1ms	3ms	13ms	0.71%
Jun 7, 2012 8:45:00 AM	1ms	7ms	25ms	1ms	10ms	60ms	0.39%
Jun 7, 2012 8:47:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	4.17%
Jun 7, 2012 8:48:00 AM	1ms	1ms	4ms	1ms	5ms	12ms	1.68%
Jun 7, 2012 8:49:00 AM	1ms	1ms	1ms	13ms	16ms	25ms	0%
Jun 7, 2012 8:50:00 AM	1ms	2ms	6ms	1ms	11ms	42ms	2.02%
Jun 7, 2012 8:51:00 AM	1ms	1ms	2ms	12ms	14ms	17ms	0%
Jun 7, 2012 8:52:00 AM	1ms	1ms	1ms	1ms	5ms	38ms	3.59%
Jun 7, 2012 8:53:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	0%
Jun 7, 2012 8:55:00 AM	1ms	1ms	1ms	1ms	17ms	49ms	0%
Jun 7, 2012 8:56:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	3.98%
Jun 7, 2012 8:57:00 AM	1ms	12ms	90ms	1ms	1ms	2ms	3.85%
Jun 7, 2012 8:58:00 AM	1ms	1ms	2ms	1ms	3ms	16ms	2.15%
Jun 7, 2012 8:59:00 AM	1ms	12ms	60ms	1ms	3ms	11ms	1.67%
Jun 7, 2012 9:00:00 AM	1ms	7ms	36ms	1ms	4ms	27ms	1.79%
Jun 7, 2012 9:01:00 AM	1ms	37ms	80ms	1ms	6ms	14ms	0%
Jun 7, 2012 9:02:00 AM	1ms	3ms	16ms	1ms	1ms	6ms	1.83%
Jun 7, 2012 9:03:00 AM	16ms	16ms	16ms	1ms	1ms	1ms	0%
Jun 7, 2012 9:04:00 AM	1ms	1ms	3ms	1ms	12ms	18ms	0%
Jun 7, 2012 9:05:00 AM	1ms	1ms	1ms	3ms	5ms	7ms	0%
Jun 7, 2012 9:06:00 AM	1ms	1ms	1ms	1ms	5ms	17ms	3.52%
Jun 7, 2012 9:07:00 AM	1ms	1ms	2ms	1ms	4ms	12ms	2.45%

참고:

이 문서는 Stealthwatch FlowSensor에서 데이터를 수신 중인 NetFlow용 Stealthwatch Flow Collector가 있는 도메인에서만 사용 가능합니다.

8

플로우 분석

개요

여러분은 특정 호스트가 손상되었다고 판단되면 보안 침해를 유발한 것으로 의심되는 호스트를 식별하기 위해 호스트를 오고 가는 대화를 "취소"하려고 합니다. 또는 트래픽이 급격히 증가하면 데이터를 분석하여 급증의 원인을 알아내려 합니다. 알람이 트리거되면 네트워크 위협에 해당하는지 판단해야 하는 경우도 있습니다.

플로우 분석 프로세스를 사용하면 네트워크 보안을 위해 이러한 사항을 판단할 수 있습니다. 이 장에서는 플로우 분석 프로세스의 개요를 제공하고 가장 일반적인 사용의 몇 가지 시나리오에 대해 설명합니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 플로우 필터
- 플로우 테이블 탭
- 빠른 보기
- 플로우 분석 시나리오
- 외부 조회

플로우 필터

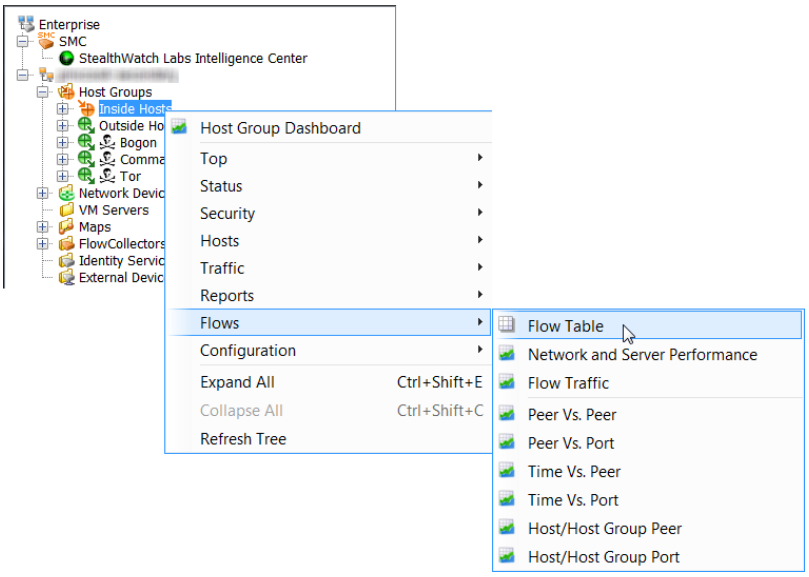
Flow Filter(플로우 필터) 대화 상자를 사용하여 원하는 결과를 얻기 위해 다양한 레벨의 필터링을 설정하고 검토하려는 플로우 데이터를 선택할 수 있습니다.

플로우 쿼리 입력

플로우 데이터를 쿼리하려면 다음 단계를 수행하십시오.

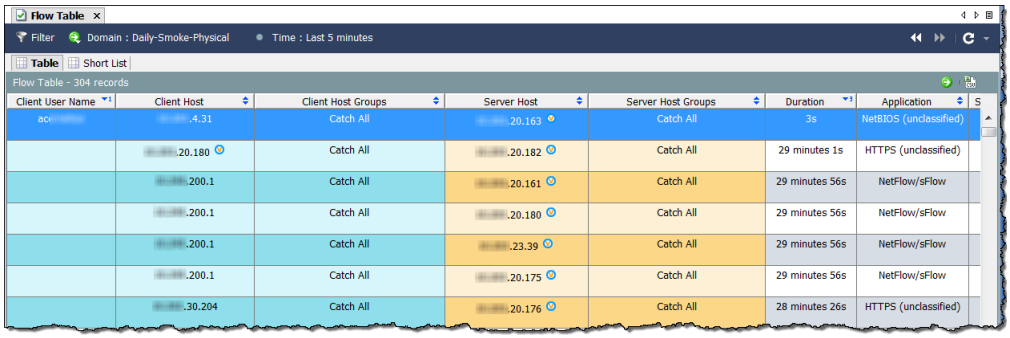
참고:
다음 단계에서 설명한 모든 설정을 사용할 필요는 없습니다.

1. 도메인, 어플라이언스, 호스트 그룹 또는 호스트 IP 주소를 마우스 오른쪽 버튼으로 클릭한 다음 **Flows(플로우) > Flow Table(플로우 테이블)**을 선택합니다.

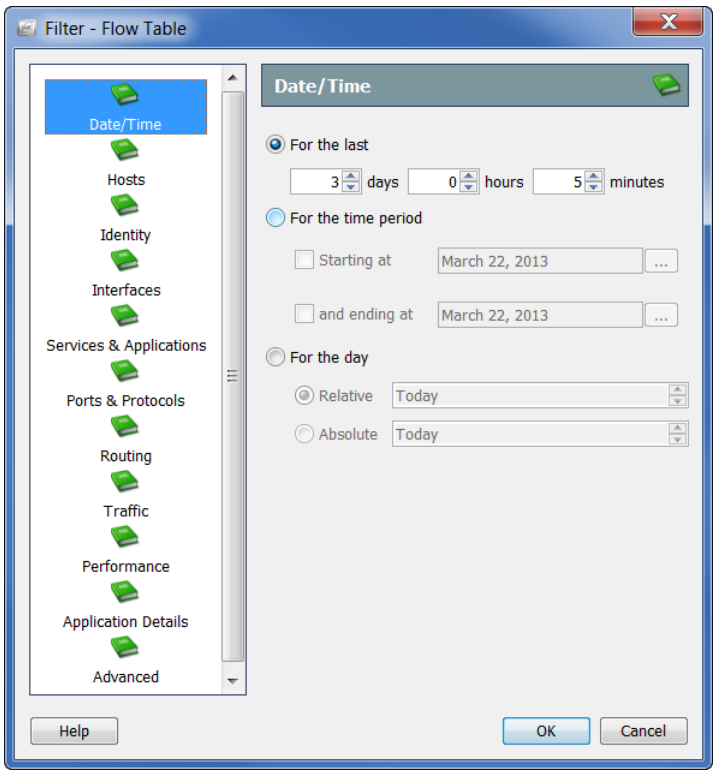


팁:
팝업 메뉴에서 **Flow Table(플로우 테이블)**을 클릭할 때 키보드에서 **Ctrl**을 누르면 검색 조건을 구체화할 수 있도록 필터가 먼저 표시됩니다. **OK(확인)**를 클릭하고 나면 플로우 테이블이 사용자가 입력한 검색 기준을 사용하여 표시됩니다.

플로우 테이블이 열립니다.



2. 플로우 테이블의 좌측 상단 모서리에서 **Filter(필터)** 버튼( )을 클릭하여 Filter(필터) 대화 상자를 연 다음 아직 강조 표시되지 않은 경우, **Date/Time(날짜/시간)** 아이콘을 클릭합니다. Date/Time(날짜/시간) 페이지가 열립니다.

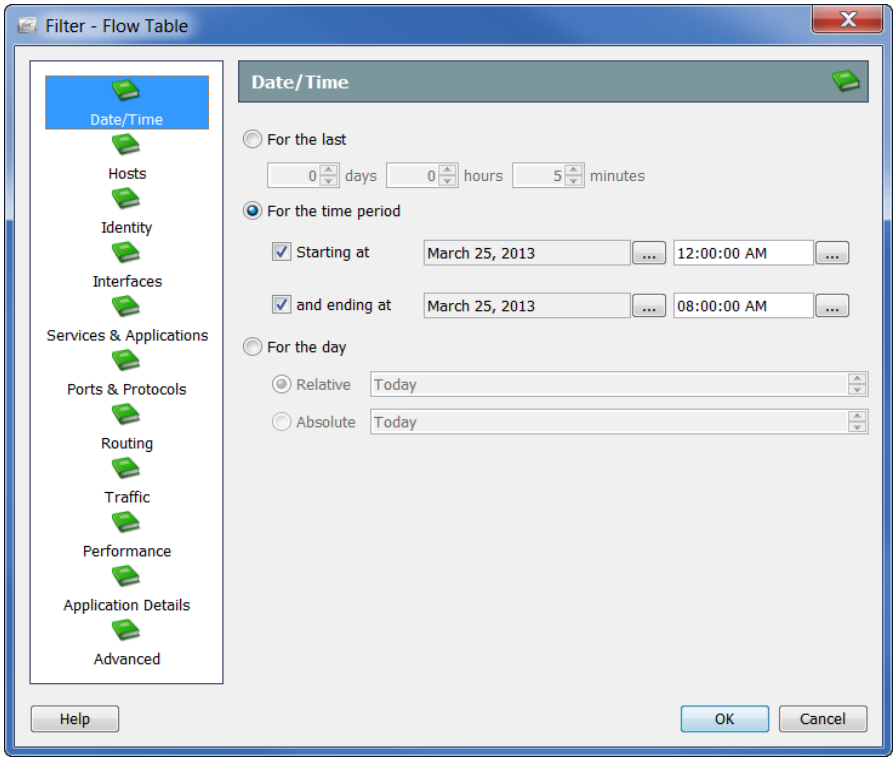


3. 정확한 날짜/시간, 범위 또는 플로우 데이터를 필터링하는 기준이 되는 관련 설정을 지정합니다. 예를 들어, 특정일에 자정과 오전 8시 사이의 모든 플로우를 표시하려는 경우, 다음 단계를 수행하십시오.

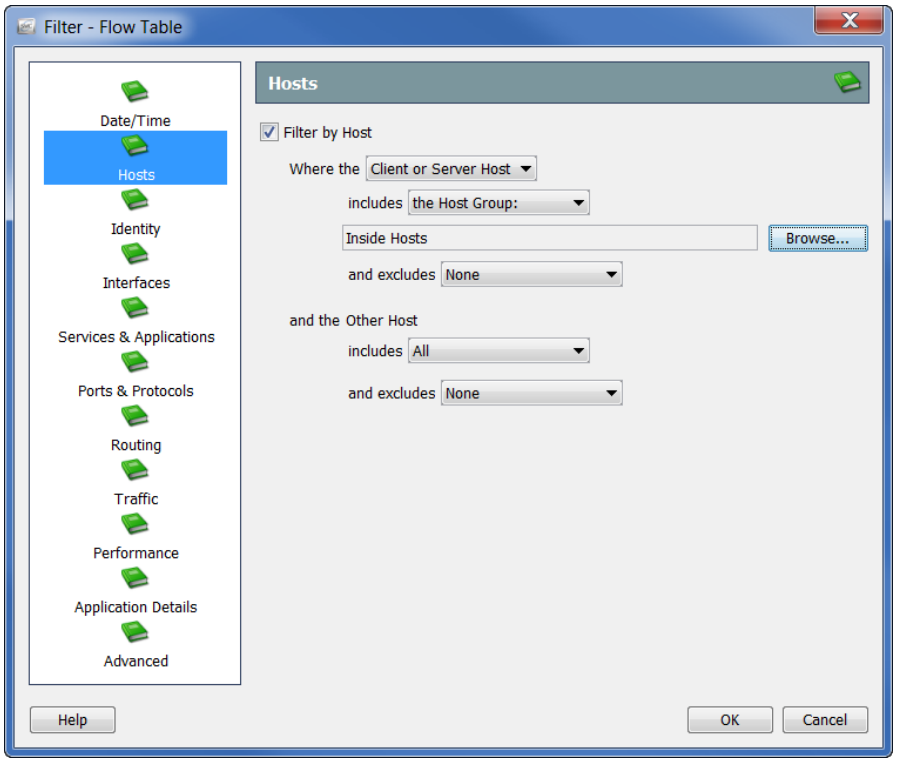
   a. **For the time period(기간)** 옵션을 클릭합니다.

   b. **Starting at(시작 시간)** 옵션을 클릭하고 필터링하려는 날짜를 입력한 다음 시간 필드에 ***12:00:00***을 입력합니다.

c. **and ending at(종료 시간)** 옵션을 클릭하고 필터링하려는 날짜를 입력한 다음 해당 옵션의 시간 필드에 ***08:00:00***을 입력합니다.

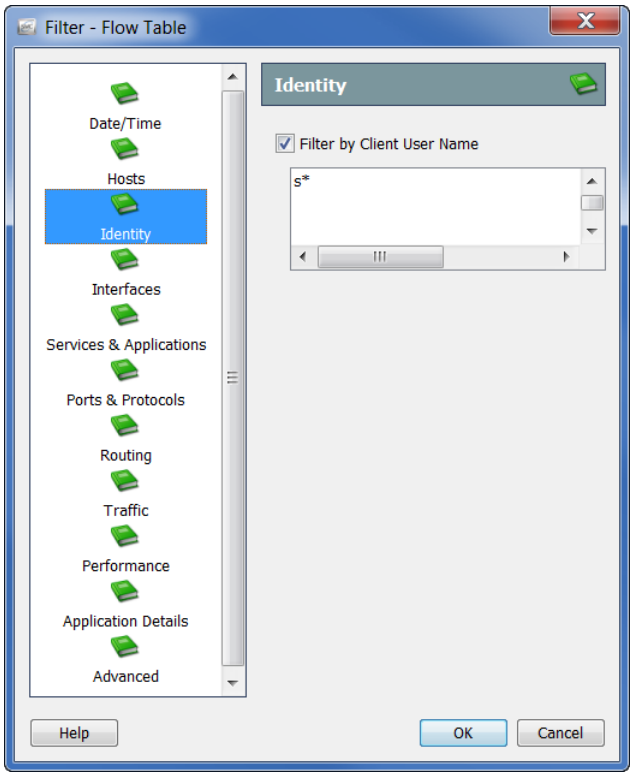


4. **Host(호스트)** 아이콘을 클릭합니다. Host(호스트) 페이지가 열립니다.



플로우 데이터를 필터링하는 데 사용할 호스트를 지정합니다. 호스트 그룹, 하나 이상의 VM, IP 주소 범위(CIDR 형식 사용) 또는 IP 주소 리스트(쉼표로 구분된 형식)를 포함/제외할 수 있습니다.

5. Identity(ID) 아이콘을 클릭합니다. Identity(ID) 페이지가 열립니다.



다음 단계를 완료하여 플로우 데이터를 필터링하는 데 사용할 사용자 이름을 지정합니다.

1. Client User Name(클라이언트 사용자 이름) 확인란을 클릭하여 체크 마크를 삽입합니다.
2. 텍스트 필드에 다음과 같은 콘텐츠를 입력합니다.
   - 단일 사용자 이름(예: jdoe)
   - 여러 사용자 이름(예: jdoe, jalpha, jbeta). 각 이름을 쉼표로 구분하거나 각 이름 다음에 **Enter** 키를 눌러 이름을 입력할 수 있습니다(라인당 하나의 이름 입력). 이름의 쉼표로 구분된 값(CSV) 리스트에서 복사하여 붙여 넣을 수도 있습니다.
   - 와일드 카드가 있는 부분 이름. 와일드 카드는 어떤 위치에든 있을 수 있습니다(예: srh*, *doe). 각 이름에 둘 이상의 와일드 카드를 사용할 수 있습니다.

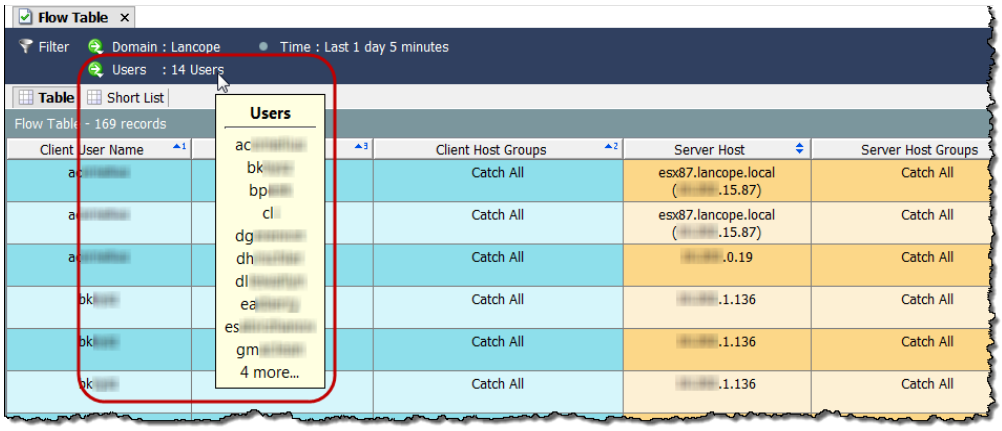
참고:

- 이 필드는 대/소문자를 구분하지 않습니다.
- 사용자 이름에는 | + = ? “ < > ( ) : ; 문자를 포함할 수 없습니다.

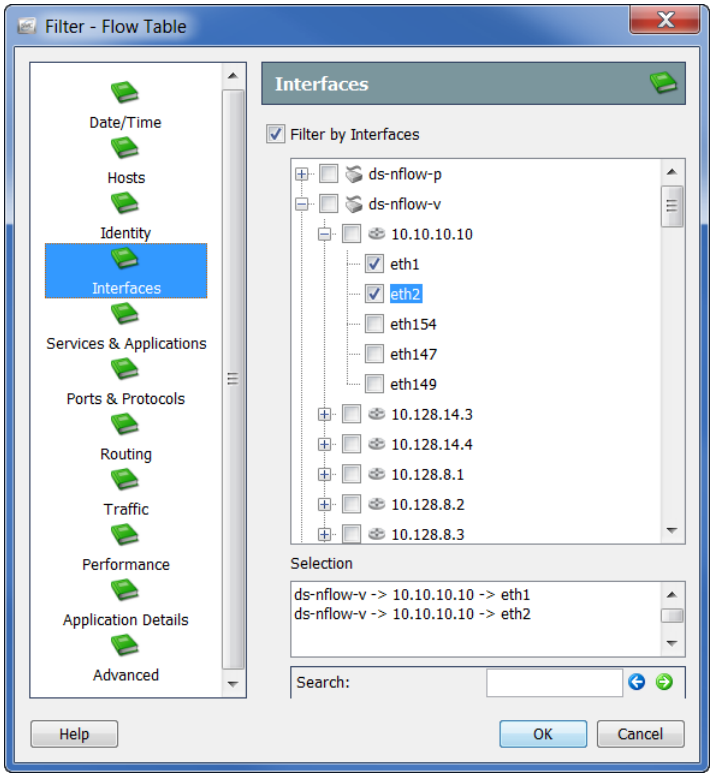
3. **OK(확인)**를 클릭합니다.

결과는 Client User Name(클라이언트 사용자 이름) 열에 표시됩니다. 한 명의 사용자만 필터링하는 경우, 사용자 이름이 헤더에 표시됩니다. 둘 이상의 사용자를 필터링하는 경우, 헤더는 필터링하는 사용자 이름의 수를 표시합니다. 이 항목 위에 커서를 올려 놓으면 쿼리한 처음 10명의 사용자 이름이 팝업 창에 나열됩니다(아래 화면 참조).

첫 번째 10명의 사용자 외에 필터링한 사용자 이름의 수가 팝업 창 맨 아래에 표시됩니다. 아래 예에서 14명의 사용자 이름이 필터링되었으므로 팝업 창 맨 아래에 항목 *4 more...(추가 4명)*가 나타납니다.

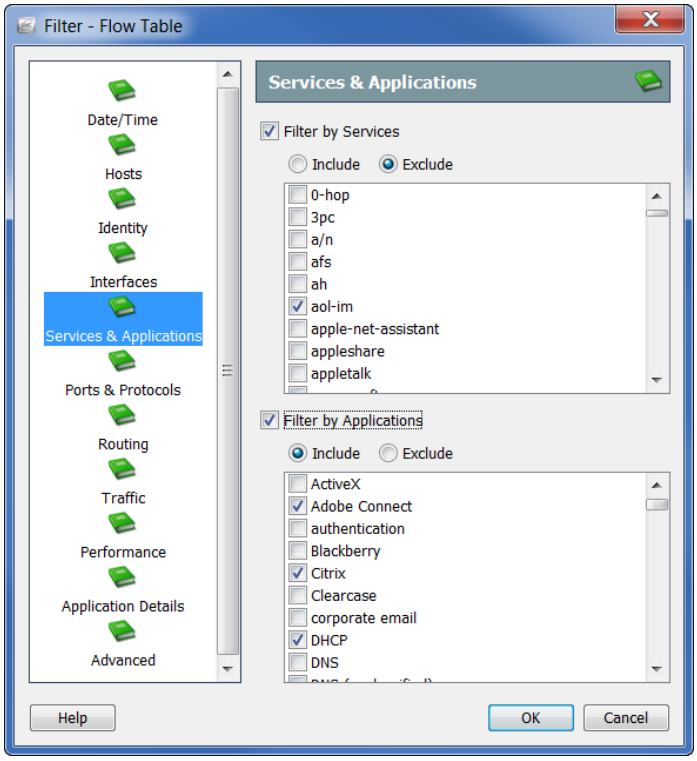


4. **Interfaces(인터페이스)** 아이콘을 클릭합니다. Interfaces(인터페이스) 페이지가 열립니다.



플로우 데이터를 필터링하는 데 사용할 인터페이스를 지정합니다. 개별 인터페이스, 전체 엑스포터 또는 Stealthwatch 어플라이언스를 클릭할 수 있습니다.

5. **Services & Applications(서비스 및 애플리케이션)** 아이콘을 클릭합니다. Services & Applications(서비스 및 애플리케이션) 페이지가 열립니다.

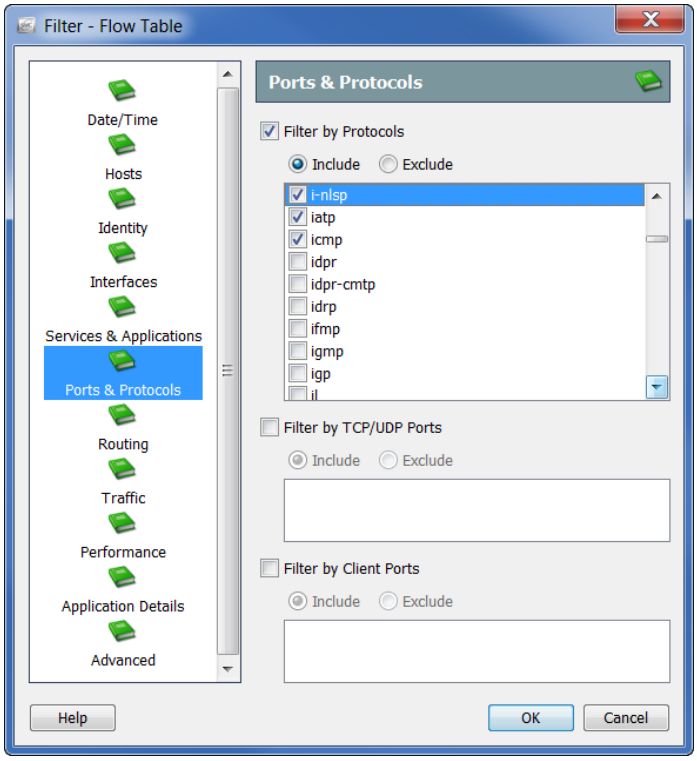


체크 마크를 추가하려면 다음 확인란 중 하나 또는 둘 다를 클릭하여 플로우 데이터를 필터링하는 데 사용할 서비스 또는 애플리케이션을 지정합니다.

- 필터링 기준: 서비스
- 필터링 기준: 애플리케이션

Include(포함) 또는 **Exclude(제외)** 옵션 중 하나를 클릭합니다. 예를 들어 Facebook을 제외하고 모든 항목에 대한 쿼리를 제한할 수도 있습니다. 이 경우, 체크 마크를 추가하려면 **Filter by Applications(필터링 기준: 애플리케이션)** 확인란을 클릭하고 **Exclude(제외)** 옵션을 클릭한 다음 **Facebook** 확인란을 클릭하여 체크 마크를 추가합니다.

6. **Ports & Protocols(포트 및 프로토콜)** 아이콘을 클릭합니다. Ports & Protocols(포트 및 프로토콜) 페이지가 열립니다.

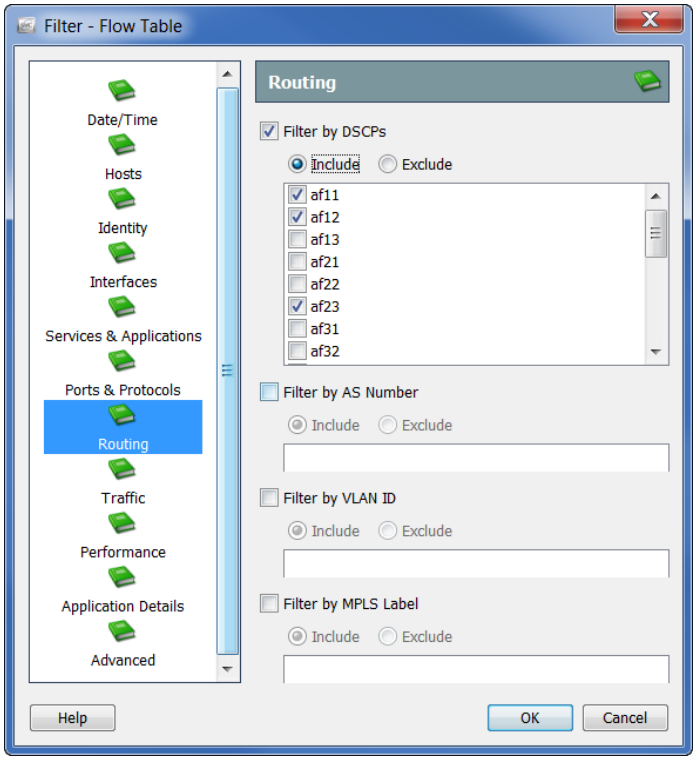


체크 마크를 추가하려면 다음 확인란 중 하나 또는 모두를 클릭하여 플로우 데이터를 필터링하는 데 사용할 포트 및 프로토콜을 지정합니다.

- 필터링 기준: 프로토콜
- 필터링 기준: TCP/UDP 포트
- 필터링 기준: 클라이언트 포트

쿼리를 추가로 맞춤 설정하려면 **Include(포함)** 또는 **Exclude(제외)** 옵션 중 하나를 클릭합니다.

7. **Routing(라우팅)** 아이콘을 클릭합니다. Routing(라우팅) 페이지가 열립니다.

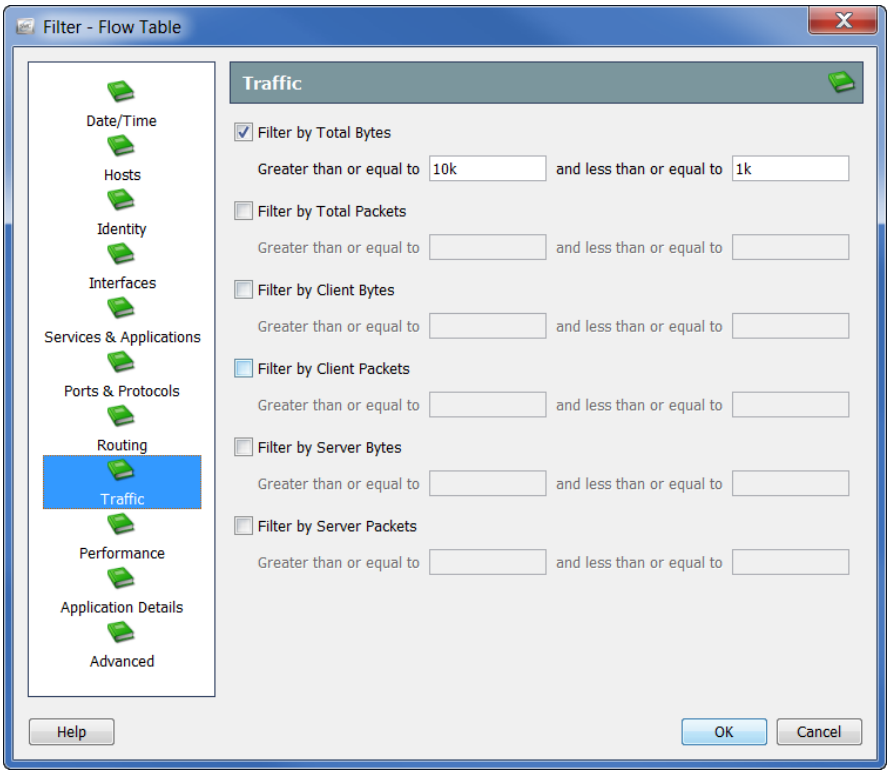


체크 마크를 추가하려면 다음 확인란 중 하나 또는 모두를 클릭하여 플로우 데이터를 필터링하는 데 사용할 파라미터를 지정합니다.

- 필터링 기준: DSCP
- 필터링 기준: AS 번호
- 필터링 기준: VLAN ID
- 필터링 기준: MPLS 레이블

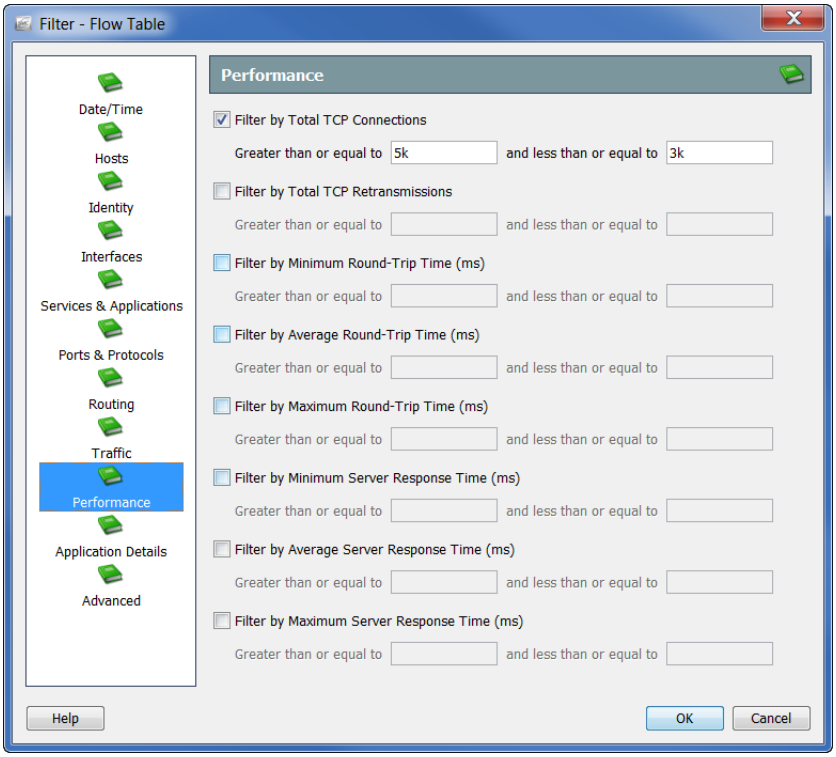
쿼리를 추가로 맞춤 설정하려면 **Include(포함)** 또는 **Exclude(제외)** 옵션 중 하나를 클릭합니다.

8. **Traffic(트래픽)** 아이콘을 클릭합니다. Traffic(트래픽) 페이지가 열립니다.



플로우 데이터를 필터링하는 데 사용할 트래픽 데이터의 유형 및 크기를 지정합니다.

9. **Performance(성능)** 아이콘을 클릭합니다. Performance(성능) 페이지가 열립니다.

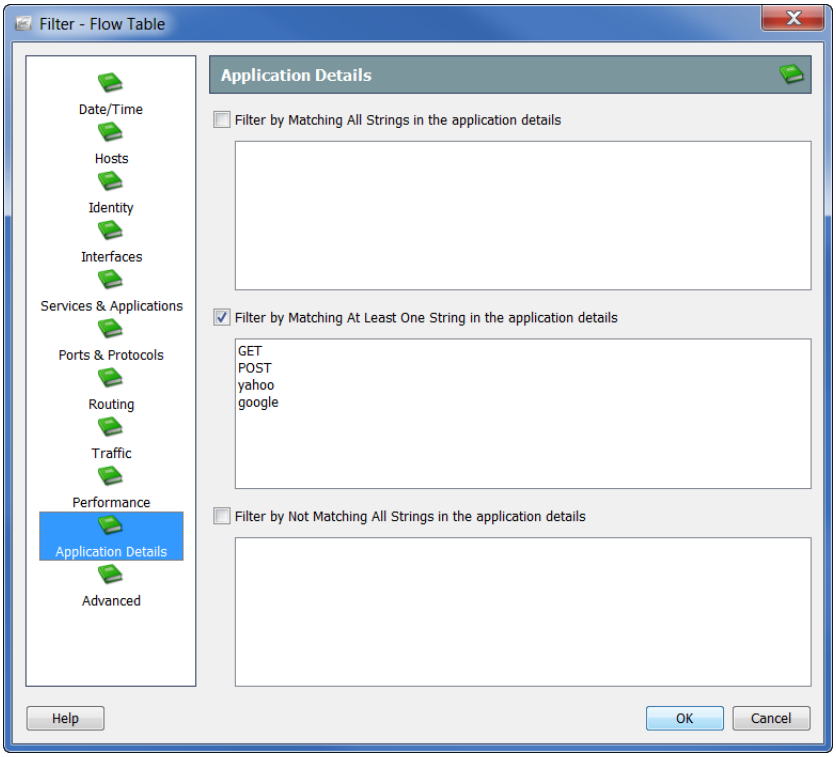


플로우 데이터를 필터링하는 데 사용할 성능 데이터의 유형 및 크기를 지정합니다.

참고:

Performance(성능) 페이지의 모든 값의 경우 Stealthwatch FlowSensor가 이 정보를 수집하고 저장해야 합니다.

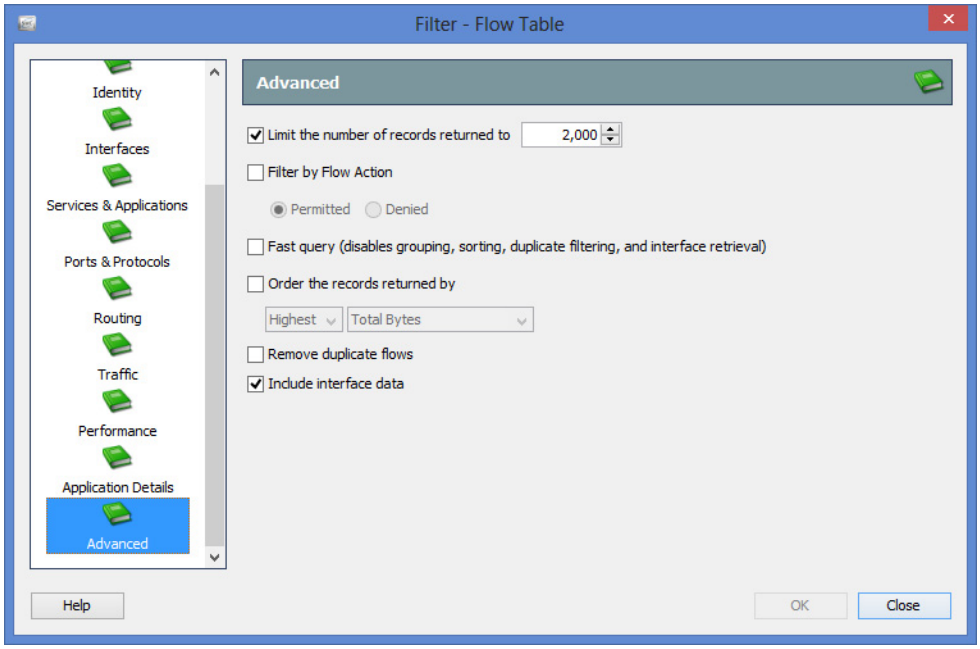
10. **Application Details(애플리케이션 세부사항)** 아이콘을 클릭합니다. Application Details(애플리케이션 세부사항) 페이지가 열립니다.



플로우 데이터를 필터링하는 데 사용할 페이로드 정보를 지정합니다.

Application Details(애플리케이션 세부사항) 페이지의 모든 값에는 FlowSensor가 필요하며 이 정보를 수집하고 저장하려면 Flexible NetFlow 내에서 페이로드 내보내기 작업을 수행해야 합니다.

11. **Advanced(고급)** 아이콘을 클릭합니다. Advanced(고급) 페이지가 열립니다.



플로우 레코드의 최대 수로 쿼리를 제한할 수 있습니다. 또한 데이터가 저장되는 방식(예: 데이터를 가져오기 전에 서버에 저장)과 중복 플로우가 결과에서 제거되는지 여부를 지정할 수 있습니다.

참고:

- **Remove duplicate flows(중복 플로우 제거)** 옵션은 Flow Collector가 여러 개인 경우에만 관련이 있습니다. 단일 Flow Collector는 자동으로 중복이 제거됩니다.
- 인터페이스 데이터를 볼 필요가 없는 경우, **Include interface data(인터페이스 데이터 포함)** 확인란을 클릭하여 체크 마크를 제거합니다. 이렇게 하면 데이터 검색이 빨라집니다.

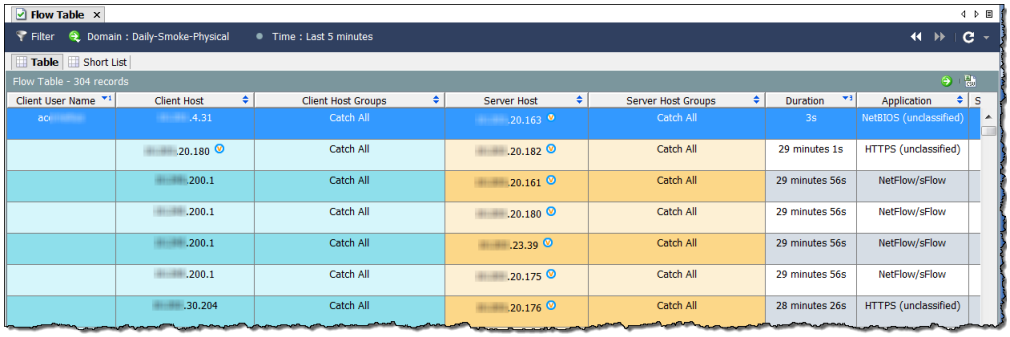
12. 필터링을 수행할 준비가 되면 **OK(확인)**를 클릭합니다. 플로우 쿼리가 전송되고 검색된 데이터가 플로우 테이블 문서에 나타납니다.

다음 번에 플로우 테이블에 액세스할 때 Advanced(고급) 페이지에 지정한 필터 설정만 계속해서 적용됩니다. 플로우 테이블 필터의 다른 페이지에 있는 필터 설정은 유지되지 않습니다.

플로우 테이블 탭

테이블 탭

Flow Table(플로우 테이블) 문서의 Table(테이블) 탭은 플로우 테이블 필터에 지정한 옵션을 기준으로 플로우에 대한 데이터를 표시합니다.



참고:

문서의 오른쪽 상단 모서리에서 **Go to Document(문서로 이동)** 버튼( )을 클릭하여 동일한 플로우 데이터를 사용하는 다른 문서를 표시할 수 있습니다.

가져온 플로우 파일이 원래 어플라이언스/도메인 정보를 포함하지 않기 때문에 이 정보를 필요로 하는 팝업 메뉴 옵션을 가져온 플로우 파일에 사용할 수 없습니다(회색으로 비활성화됨).

참고:

플로우 파일 가져오기에 대한 자세한 내용은 *SMC 클라이언트 온라인 도움말*의 "플로우 파일을 가져오는 방법" 항목을 참조하십시오.

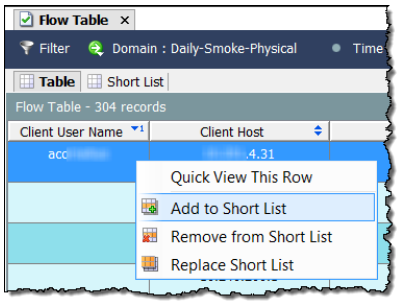
테이블에 표시되는 열을 변경하려면 헤딩을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 원하는 열을 선택합니다. 이름 옆에 체크 마크가 있는 헤딩은 이 헤딩이 문서에 표시된다는 것을 나타냅니다.

짧은 리스트 탭

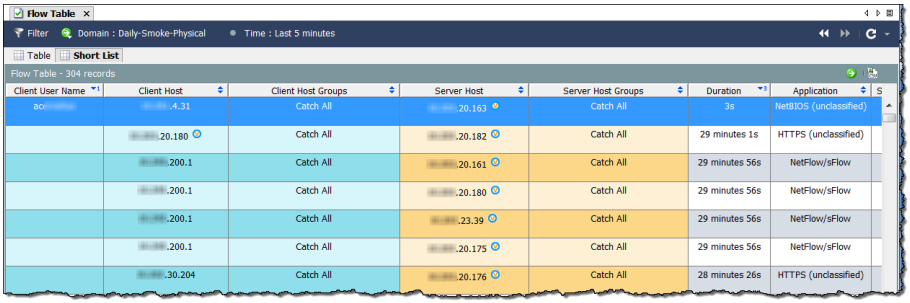
Short List(짧은 리스트) 탭은 Table(테이블) 탭과 동일한 컨피그레이션을 공유합니다. 한 탭에서 내용을 변경하면 자동으로 다른 탭에 반영됩니다.

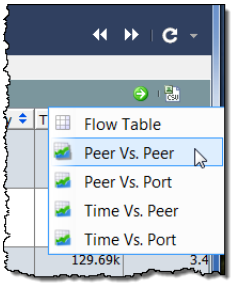
Flow Table(플로우 테이블) 문서의 Short List(짧은 리스트) 탭을 사용하면 Flow Table: Table(플로우 테이블: 테이블) 페이지에 나타나는 플로우 데이터의 하위 집합을 표시할 수 있습니다. 예를 들어, Table(테이블) 탭은 수 천 개의 플로우 레코드를 표시할 수 있지만 보다 자세한 분석을 위해 적은 수의 행만 볼 수도 있습니다. Short List(짧은 리스트) 기능을 사용하면 쉽게 볼 수 있도록 특정 행을 선택할 수 있습니다.

오른쪽 예에서와 같이 Table(테이블) 탭에서 행을 마우스 오른쪽 버튼으로 클릭하고 **Add to Shortlist(짧은 리스트에 추가)**를 선택합니다.



플로우를 보려면 **Short List(짧은 리스트)** 탭을 클릭하여 플로우의 짧은 리스트를 엽니다. 선택한 행이 이 문서에 표시됩니다.





데이터의 하위 집합을 그래픽으로 보려면 **Go to Document(문서로 이동)** 버튼( )을 클릭하고 팝업 메뉴에서 원하는 분석 유형(예: 피어-투-피어)을 클릭합니다.

짧은 리스트에는 플로우 테이블 필터에 의해 검색된 모든 데이터 대신 호스트의 데이터만 나타납니다.

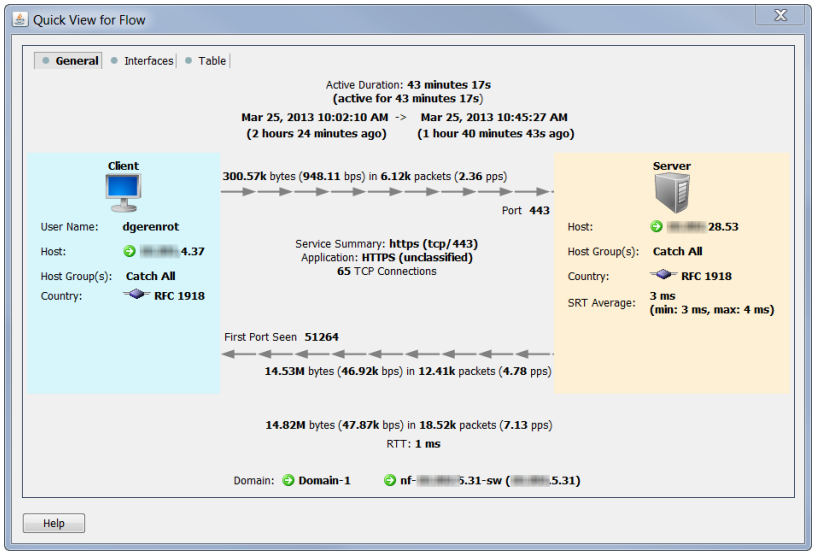
빠른 보기

Quick View(빠른 보기) 대화 상자에서는 테이블 형식 데이터를 그래픽으로 볼 수 있는 빠르고 쉬운 방법을 제공합니다. 또한 다른 문서의 필터링된 보기에 대한 빠른 탐색을 제공합니다.

Quick View(빠른 보기) 대화 상자를 보려면 테이블 셀을 클릭한 다음 스페이스바를 누릅니다. 대화 상자를 보이지 않게 하려면 스페이스바를 다시 누르거나 Esc 키를 누릅니다.

아래 예에서와 같이 Quick View(빠른 보기) 대화 상자는 다음 탭에서 데이터를 보여줍니다.

- 일반
- 인터페이스
- 테이블



키보드에서 Alt 키를 ← 또는 → 키와 함께 눌러 탭 사이를 이동할 수 있습니다.

키보드에서 Alt 키를 ↑ 또는 ↓ 키와 함께 눌러 플로우 사이(빠른 보기 대화 상자를 연 상태에서)를 이동할 수 있습니다.

팁:

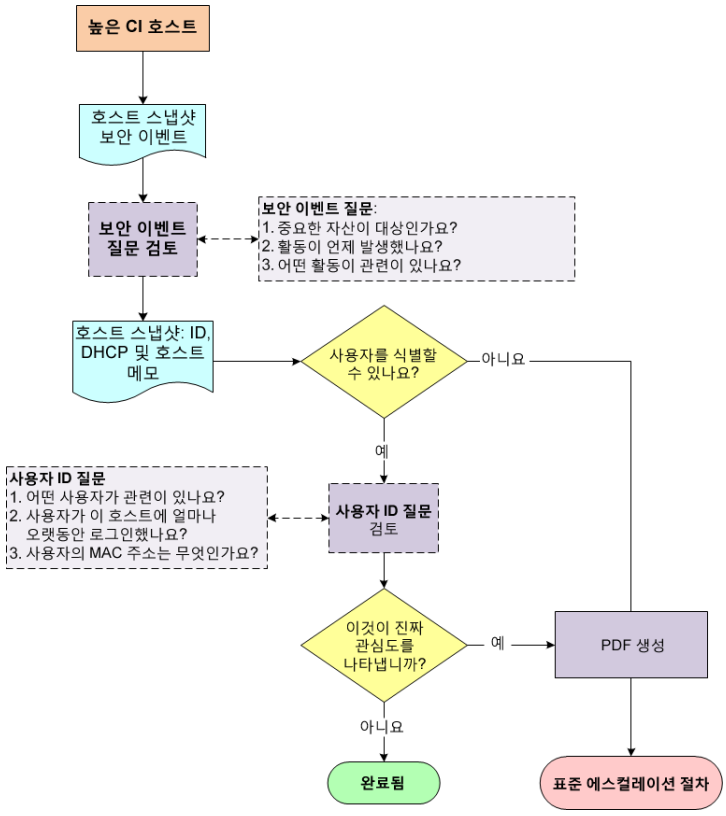
다른 테이블에 적용되는 동일한 탐색 기능(예: 다른 문서로 드릴다운)이 이 테이블에도 적용됩니다.

플로우 분석 시나리오

지금까지 플로우 분석 프로세스에 대해 알아보았습니다. 이제 몇 가지 공통된 시나리오에 대해 살펴보겠습니다.

상위 관심 지표 호스트

상위 CI 호스트는 의심스러운 플로우 활동(보안 이벤트)의 소스인 호스트입니다. 다음 다이어그램은 위협의 진위 여부를 판단하는 데 사용할 수 있는 워크플로를 보여줍니다.



워크플로 개요

다음 단계에서는 앞에 나온 워크플로 다이어그램에 설명되어 있는 절차에 대한 개요를 제공합니다.

1. 소스 호스트의 Host Snapshot: Security Events(호스트 스냅샷: 보안 이벤트) 페이지를 열고 세부사항을 검토합니다. 다음 섹션인 "보안 이벤트 활동(호스트 스냅샷) 검토" 섹션을 참조하십시오.
2. **Identity, DHCP & Host Notes(ID, DHCP 및 호스트 메모)** 탭을 클릭합니다.

3. 사용자를 식별할 수 있나요?
   - 그렇다면, 4단계로 이동합니다.
   - 그렇지 않다면 6단계로 이동합니다.
4. 소스 호스트에 로그인한 사용자의 정보를 검토합니다. 175페이지의 "사용자 ID 정보(호스트 스냅샷) 검토"를 참조하십시오.
5. 수집한 정보를 기준으로 할 때 이 활동이 진짜 관심도를 나타냅니까?
   - 대답이 예이거나 잘 모르는 경우, 6단계로 이동합니다.
   - 대답이 아니요인 경우 이 단계에서 중지합니다.
6. 호스트 스냅샷의 PDF를 만들고 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

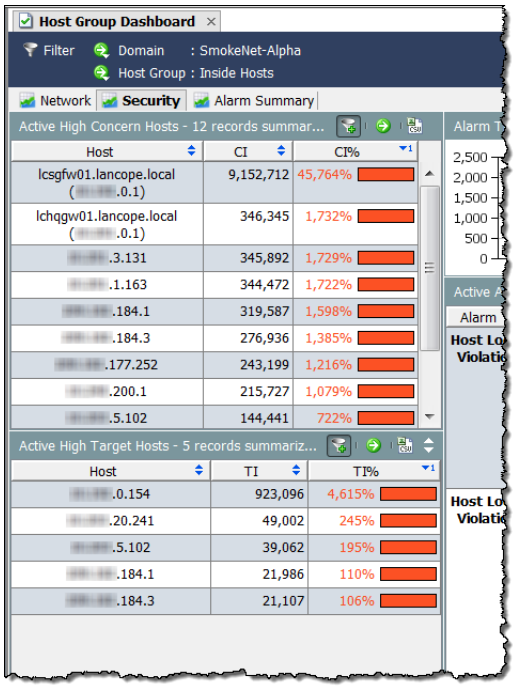
보안 이벤트 활동(호스트 스냅샷) 검토

상위 CI 호스트는 악성코드에 감염되거나 다른 방식으로 보안이 침해될 수 있습니다. SMC는 다음을 포함하여 상위 CI 호스트를 쉽게 식별할 수 있는 여러 위치를 제공합니다.

- 관심 지표(CI)
- 알람 테이블(알람이 트리거된 경우)
- Host Group Dashboard: Security(호스트 그룹 대시보드: 보안) 페이지

이 워크플로는 Host Group Dashboard: Security(호스트 그룹 대시보드: 보안) 페이지에서 조사를 시작합니다. 상위 CI 호스트의 보안 이벤트 활동을 검토하려면 다음 단계를 수행하십시오.

1. Host Group Dashboard(호스트 그룹 대시보드)에서 **Security(보안)** 탭을 클릭합니다. **Active High Concern Hosts(활성 상위 관심도 호스트)** 및 **Active High Target Hosts(활성 상위 대상 호스트)** 섹션에서 상위 CI 호스트 및 상위 TI 호스트가 특정 호스트 그룹 대시보드와 연결된 호스트 그룹에 대해 나열됩니다.

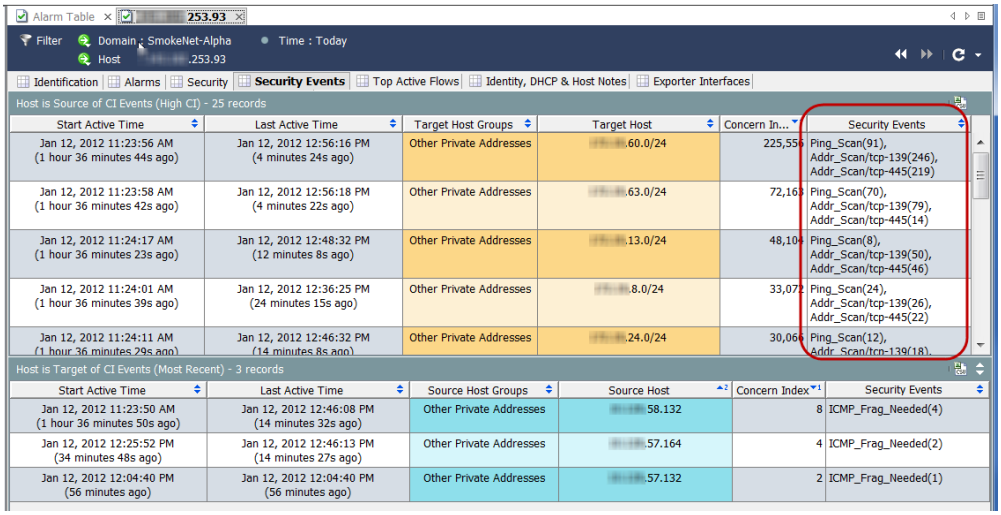


2. 해당하는 호스트 IP 주소를 더블 클릭하여 호스트 스냅샷을 엽니다.

팁:

IP 주소를 알고 있는 경우 전체 검색 기능을 사용하여 호스트 스냅샷을 찾을 수도 있습니다.

3. **Security Events(보안 이벤트)** 탭을 클릭합니다.
4. **Host is Source of Security Events (High CI)(호스트가 보안 이벤트의 소스임(상위 CI))** 섹션에서 Security Events(보안 이벤트) 열의 항목을 검토합니다(다음 예 참조). 다음 질문을 스스로에게 해보십시오.
   - 중요한 자산이 표적이 되고 있나요?
   - 활동이 언제 발생했나요?
   - 어떤 활동이 관련이 있나요?



참고:

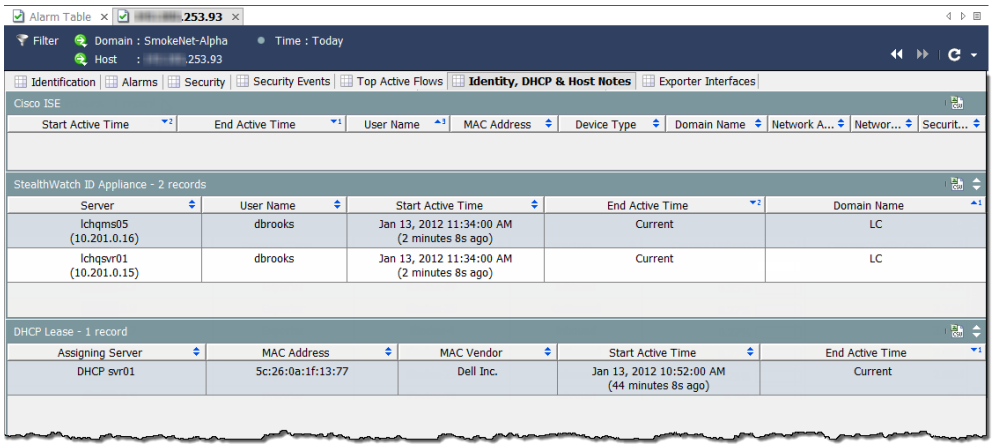
특정 보안 이벤트에 대한 자세한 설명은 *SMC 클라이언트 온라인 도움말*의 "보안 이벤트" 항목을 참조하십시오.

5. 다음 섹션에 설명된 대로 사용자 ID 정보를 검토합니다.

사용자 ID 정보(호스트 스냅샷) 검토

상위 CI 호스트의 보안 이벤트 활동을 파악한 경우, 해당 호스트에 로그인한 사용자의 ID를 검토하려면 다음 단계를 수행하십시오.

1. 호스트 스냅샷에서 **Identity, DHCP & Host Notes(ID, DHCP 및 호스트 메모)** 탭을 클릭합니다.

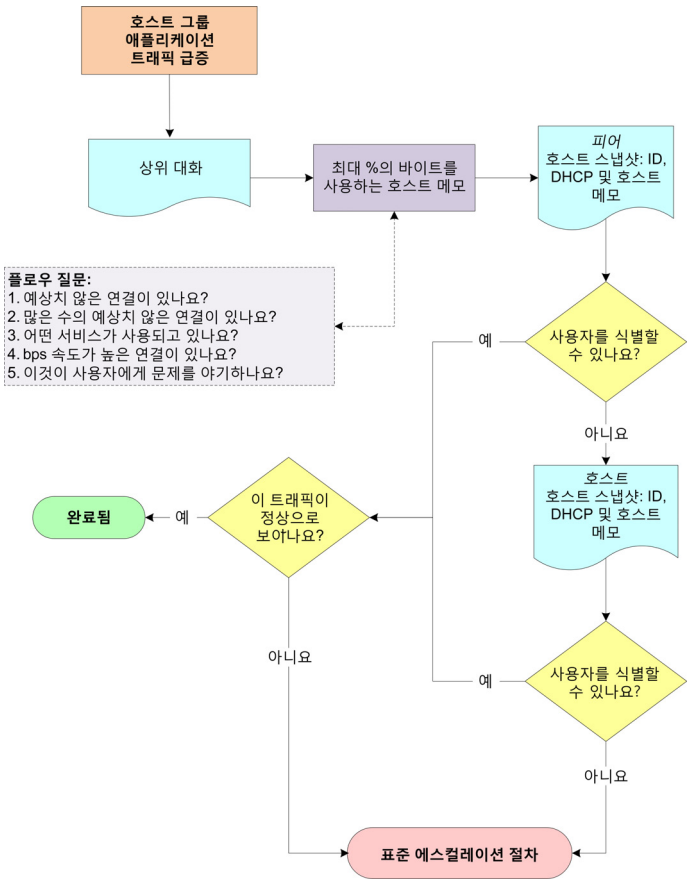


2. 사용자 정보를 확인할 수 있나요?
   - 그렇다면, 3단계로 이동합니다.
   - 그렇지 않다면 5단계로 이동합니다.

3. 다음 질문을 마음 속으로 생각하면서 사용자 정보를 검토합니다.
   - 어떤 사용자가 이 호스트에 로그인했나요?
   - 이 사용자가 얼마나 오래 로그인했나요?
   - 사용자의 MAC 주소는 무엇인가요?
4. 이 호스트에 대해 수집한 정보를 기준으로 할 때 이 활동이 진짜 관심도를 나타냅니까?
   - 대답이 예이거나 잘 모르는 경우, 5단계로 이동합니다.
   - 대답이 아니요인 경우 이 단계에서 중지합니다.
5. 호스트 스냅샷의 PDF를 만들고 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

애플리케이션 트래픽 급증

네트워크의 한 영역에서 트래픽이 갑자기 증가한 경우, 트래픽이 갑자기 증가한 원인과 관심을 가져야 할지 여부를 판단하는 데 도움이 되는 다음 다이어그램에 나와 있는 워크플로를 사용하십시오.



워크플로 개요

SMC는 다음과 같은 트래픽 급증을 확인할 수 있는 여러 위치를 제공합니다.

- 트래픽 메뉴를 통해 액세스 가능한 모든 트래픽 그래프.
- 호스트 그룹 대시보드: 네트워크 페이지

이 워크플로는 네트워크 페이지에서 조사를 시작합니다. 다음 단계에서는 앞에 나온 워크플로 다이어그램에 설명되어 있는 절차에 대한 개요를 제공합니다.

1. Network(네트워크) 페이지에서 어느 방향으로 트래픽 급증이 진행되는지 판단합니다. 179페이지의 "관련 호스트 식별"을 참조하십시오.
2. 트래픽 급증 부분을 더블 클릭하여 Top Conversations(상위 대화) 문서를 연 다음 어떤 호스트 쌍이 발견된 방향에서 대부분의 대역폭을 사용하는지 식별합니다. 179페이지의 "관련 호스트 식별"을 참조하십시오.
3. 위에서 식별한 호스트 쌍과 관련하여 다음 질문을 검토합니다.
   - 예상치 않은 연결(예: 권한 없는 호스트 그룹 또는 서버)이 있나요?
   - 많은 수의 예상치 않은 연결이 있나요?
   - 어떤 포트가 사용되고 있나요?
   - 발신 및/또는 수신 중인 많은 양의 트래픽이 있나요?
   - bps 속도가 높은 연결이 있나요?
   - 이 급증 현상이 네트워크에 관한 사용자 불만사항과 연관이 있나요?
4. 피어에 대해 Host Snapshot: Identity, DHCP & Host Notes(호스트 스냅샷: ID, DHCP 및 호스트 메모) 페이지를 엽니다. 180페이지의 "관련 사용자 식별"을 참조하십시오.
5. 관련된 사용자를 식별할 수 있나요?
   - 그렇다면, 8단계로 이동합니다.
   - 그렇지 않다면 6단계로 이동합니다.
6. 호스트에 대해 Host Snapshot: Identity, DHCP & Host Notes(호스트 스냅샷: ID, DHCP 및 호스트 메모) 페이지를 엽니다. 180페이지의 "관련 사용자 식별"을 참조하십시오.
7. 관련된 사용자를 식별할 수 있나요?
   - 그렇다면, 8단계로 이동합니다.
   - 그렇지 않다면 9단계로 이동합니다.
8. 이 트래픽이 합법적인 활동처럼 보이나요?
   - 대답이 예이거나 잘 모르는 경우, 9단계로 이동합니다.
   - 대답이 아니요인 경우, 트래픽 급증을 무시할 수 있습니다.
9. 지금까지 수집한 정보를 취합하여 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

트래픽 방향 식별

Host Group Dashboard(호스트 그룹 대시보드)는 Network(네트워크) 탭에서 호스트 그룹 애플리케이션 트래픽의 가장 종합적인 보기를 제공합니다.

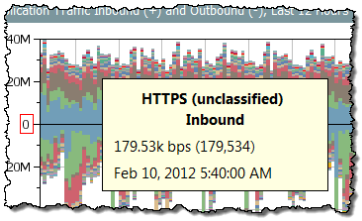
Application Traffic Inbound (+) and Outbound (-)(애플리케이션 트래픽 인바운드(+) 및 아웃바운드(-)) 및 **Application Traffic Within(애플리케이션 트래픽 내부)** 차트를 살펴보고 트래픽에 급증이 있는지 즉시 확인하고 트래픽이 어떤 방향으로 이동하는지 판단합니다.

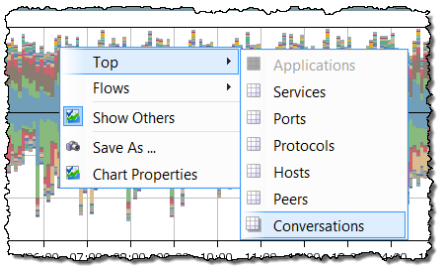
Application Traffic Inbound (+) and Outbound (-)(애플리케이션 트래픽 인바운드(+) 및 아웃바운드(-)) 차트는 외부 호스트 그룹에서 내부 호스트 그룹으로의 트래픽 이동과 그 반대의 경우를 보여줍니다. 인바운드 트래픽은 값이 0인 라인 위에 나타납니다. 아웃바운드 트래픽은 값이 0인 라인 아래에 나타납니다.

Application Traffic Within(애플리케이션 트래픽 내부) 차트는 네트워크 내부(내부 호스트 그룹)의 하위호스트 그룹 사이에서만 이동하는 트래픽을 보여줍니다.

각 차트는 필터에 설정된 기간 동안 사용된 상위 15개의 애플리케이션을 표시합니다. 각기 다른 색상은 각 애플리케이션을 나타냅니다. 각 차트의 범례는 가장 많이 사용된 서비스부터 가장 적게 사용된 서비스 순으로 서비스를 나열합니다. 범례에서 애플리케이션 위에 커서를 올려 놓으면 차트에서 강조 표시된 애플리케이션을 확인할 수 있습니다.

오른쪽 예에서와 같이 차트 위의 데이터 포인트 위에 커서를 올려 놓으면 해당 트래픽에 대한 세부사항을 제공하는 툴팁이 표시됩니다.



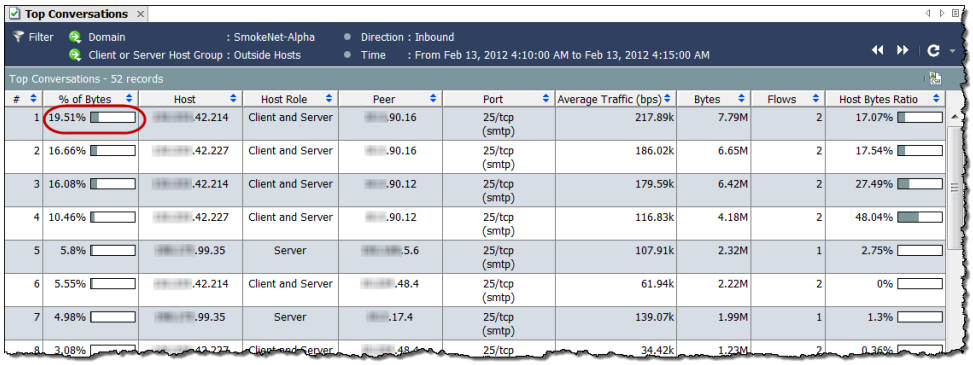


왼쪽 예에서와 같이 데이터 포인트를 더블 클릭하면 해당 트래픽에 대한 자세한 내용을 볼 수 있도록 여러 옵션 중에서 선택할 수 있는 팝업 메뉴가 표시됩니다.

관련 호스트 식별

트래픽이 어느 방향으로 이동하는지 파악한 경우, 다음 단계를 완료하여 어떤 호스트 쌍이 관련이 있는지 판단하십시오.

1. Network(네트워크) 탭에서 트래픽 급증 부분을 더블 클릭하여 Top Conversations(상위 대화) 문서를 엽니다.

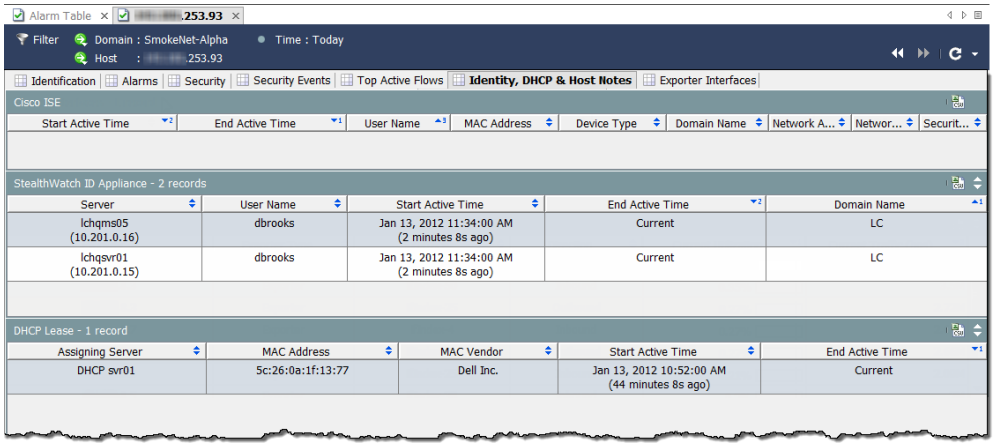


2. 가장 높은 바이트 비율을 사용 중인 호스트와 피어를 식별합니다. (기본적으로, 백분율은 숫자 **1**(**#** 열)로 표시됩니다.)
3. 위에서 식별한 호스트 쌍과 관련하여 다음 질문을 검토합니다.
   - 예상치 않은 연결(예: 권한 없는 호스트 그룹 또는 서버)이 있나요?
   - 많은 수의 예상치 않은 연결이 있나요?
   - 어떤 포트가 사용되고 있나요?
   - 발신 및/또는 수신 중인 많은 양의 트래픽이 있나요?
   - bps 속도가 높은 연결이 있나요?
   - 이 급증 현상이 네트워크에 관한 사용자 불만사항과 연관이 있나요?

관련 사용자 식별

트래픽 급증과 관련된 호스트 쌍의 IP 주소를 파악한 경우, 다음 단계를 완료하여 어떤 사용자가 관련이 있으며 이 활동이 관심도에 해당하는지를 식별할 수 있는지 확인하십시오.

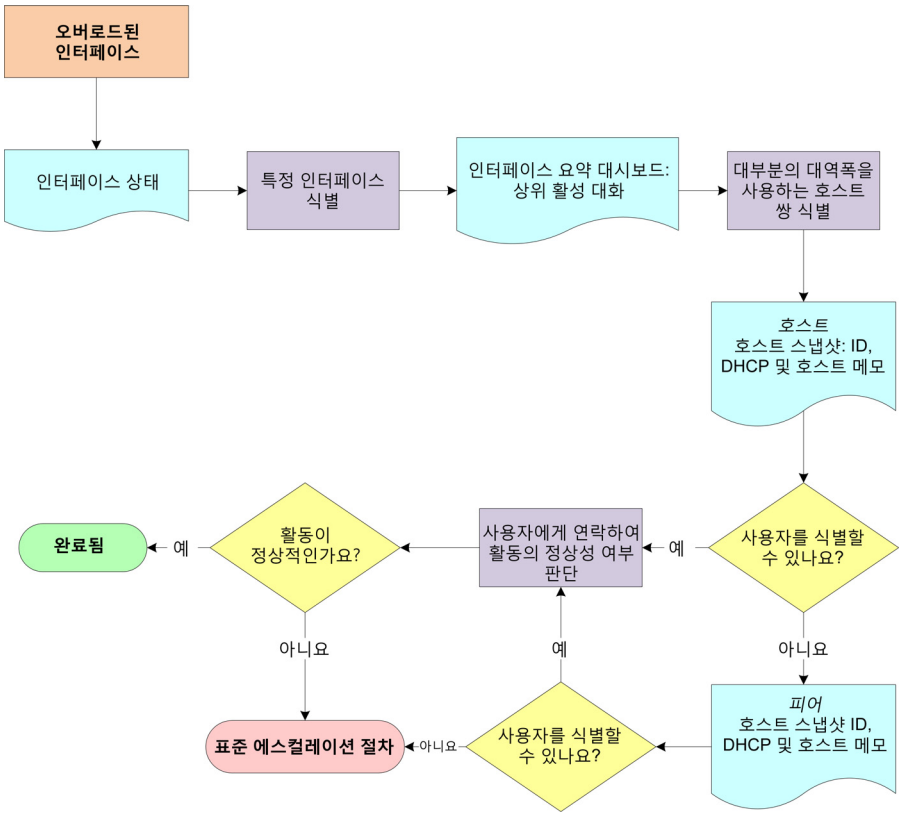
1. 해당하는 호스트 IP 주소를 더블 클릭하여 호스트 스냅샷을 엽니다.
2. **Identity, DHCP & Host Notes(ID, DHCP 및 호스트 메모)** 탭을 클릭합니다.



3. 사용자 정보를 확인할 수 있나요?
   - 그렇다면, 6단계로 이동합니다.
   - 그렇지 않다면 4단계로 이동합니다.
4. 해당하는 피어 IP 주소를 더블 클릭하여 호스트 스냅샷을 엽니다.
5. **Identity, DHCP & Host Notes(ID, DHCP 및 호스트 메모)** 탭을 클릭합니다.
6. 사용자 정보를 확인할 수 있나요?
   - 그렇다면, 6단계로 이동합니다.
   - 그렇지 않다면 7단계로 이동합니다.
7. 이 활동이 관심도에 해당하는 것으로 나타납니까?
   - 대답이 예이거나 잘 모르는 경우, 7단계로 이동합니다.
   - 대답이 아니요인 경우 이 단계에서 중지합니다.
8. 지금까지 수집한 정보를 취합하여 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

오버로드된 인터페이스

인터페이스가 오버로드되었거나 용량에 거의 도달한 것으로 알고 있는 경우 또는 그렇게 의심되는 경우, 다음 다이어그램에 표시된 워크플로를 사용하여 문제의 원인을 파악할 수 있습니다.



워크플로 개요

SMC는 다음을 포함하여 인터페이스 사용률을 쉽게 파악할 수 있는 여러 위치를 제공합니다.

- 엔터프라이즈 트리 내 네트워크 디바이스
- 인터페이스 상태
- 알람 테이블(인터페이스 사용률 초과됨 알람이 트리거된 경우)

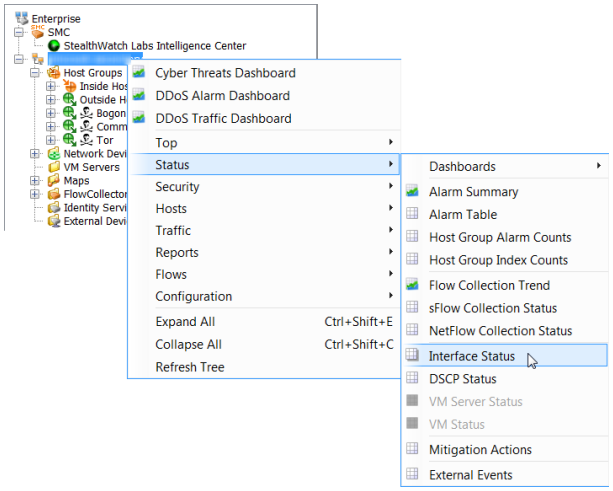
이 워크플로는 인터페이스 상태 문서에서 조사를 시작합니다. 다음 단계에서는 앞에 나온 워크플로 다이어그램에 설명되어 있는 절차에 대한 개요를 제공합니다.

1. 도메인에 대한 Interface Status(인터페이스 상태) 문서를 열어 오버로드된 인터페이스를 식별합니다. 다음 섹션인 "오버로드된 인터페이스(인터페이스 상태) 식별" 섹션을 참조하십시오.
2. 과도하게 사용된 인터페이스에 대한 Interface Summary Dashboard(인터페이스 요약 대시보드)를 열고 Top Active Conversations(상위 활성 대화)를 살펴봅니다.
3. 호스트 쌍(호스트 및 피어)의 IP 주소가 대부분의 대역폭을 사용하고 있는 점을 참고합니다.
4. 호스트에 대해 Host Snapshot: Identity, DHCP & Host Notes(호스트 스냅샷: ID, DHCP 및 호스트 메모) 페이지를 엽니다. 190페이지의 "높은 대역폭 호스트에 로그인한 사용자 식별"을 참조하십시오.
5. 사용자를 식별할 수 있나요?
   - 그렇다면, 8단계로 이동합니다.
   - 그렇지 않다면 6단계로 이동합니다.
6. 피어에 대해 Host Snapshot: Identity, DHCP & Host Notes(호스트 스냅샷: ID, DHCP 및 호스트 메모) 페이지를 엽니다. 190페이지의 "높은 대역폭 호스트에 로그인한 사용자 식별"을 참조하십시오.
7. 사용자를 식별할 수 있나요?
   - 그렇다면, 8단계로 이동합니다.
   - 그렇지 않다면 10단계로 이동합니다.
8. 사용자에게 연락하여 사용자와 관련된 활동이 정상적인지 여부를 판단합니다.
9. 활동이 정상적인가요?
   - 그렇다면 이 단계에서 중지합니다.
   - 그렇지 않다면 10단계로 이동합니다.
10. 지금까지 수집한 정보를 취합하여 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

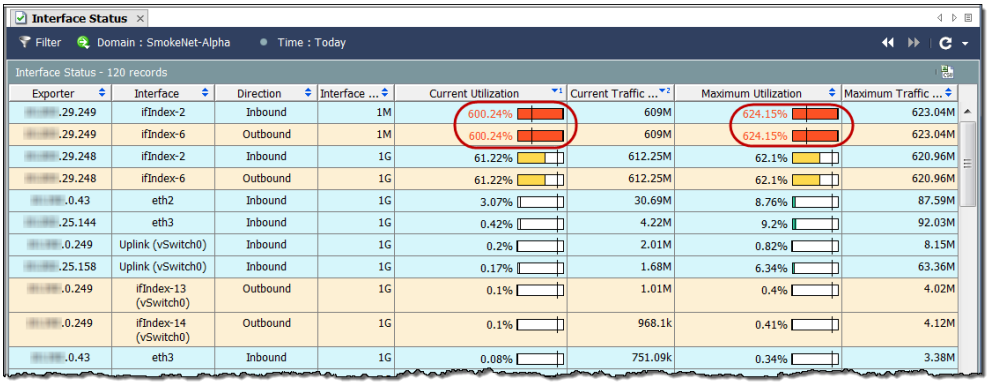
오버로드된 인터페이스(인터페이스 상태) 식별

Interface Status(인터페이스 상태) 문서를 열어 오버로드되었거나 용량에 거의 도달한 특정 인터페이스를 식별하려면 다음 단계를 수행하십시오.

1. 도메인 이름을 마우스 오른쪽 버튼으로 클릭하고 **Status(상태) > Interface Status(인터페이스 상태)**를 선택합니다.



2. Interface Status(인터페이스 상태) 문서가 열리면 다음 예에서와 같이 오버로드되었거나 용량에 거의 도달한 인터페이스를 식별합니다. (**힌트:** Current Utilization(현재 사용률) 및 Maximum Utilization(최대 사용률) 열에 있는 빨간색, 주황색 또는 노란색 막대를 살펴보십시오.)

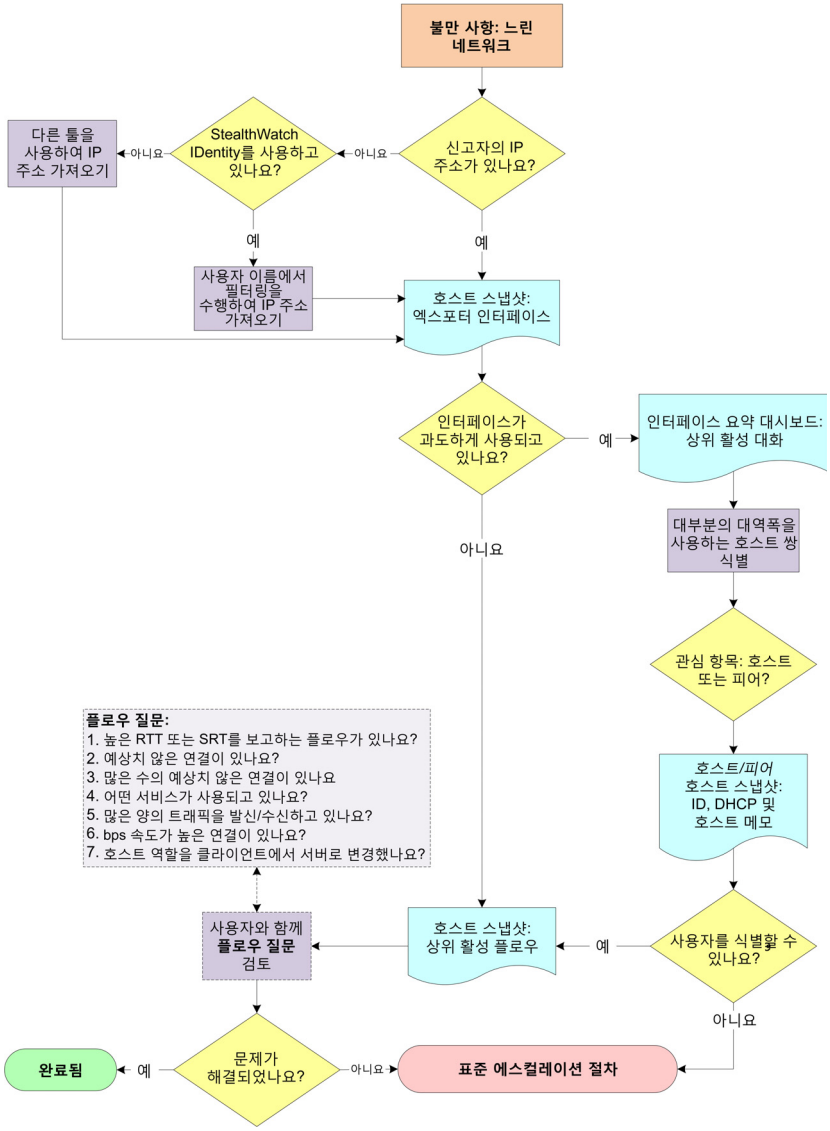


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	600.24%	609M	624.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	600.24%	609M	624.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

3. 해당하는 Interface(인터페이스) 셀을 더블 클릭하여 식별된 인터페이스에 대한 Interface Summary Dashboard(인터페이스 요약 대시보드)를 열어 트래픽이 높은 이유를 알아봅니다. 189페이지의 "높은 대역폭 호스트(인터페이스 요약 대시보드) 찾기"를 참조하십시오.

느린 네트워크

가장 일반적인 사용자 불만 중 하나는 네트워크가 느리다는 것입니다. 다음 다이어그램은 문제의 원인을 찾아내는 데 도움이 되는 워크플로를 보여줍니다.



워크플로 개요

다음 단계에서는 앞에 나온 워크플로 다이어그램에 설명되어 있는 절차에 대한 개요를 제공합니다.

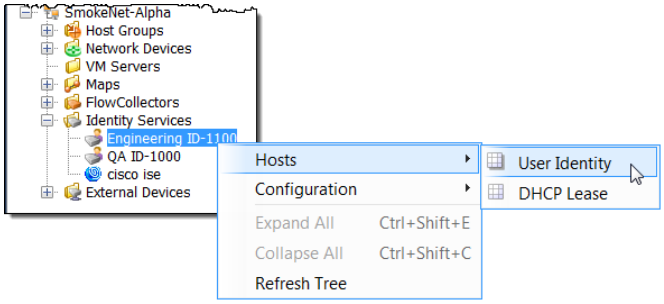
1. 불만 사항이 있는 사용자의 IP 주소가 있나요?
   - 그렇다면 3단계로 이동합니다.
   - 그렇지 않다면 2단계로 이동합니다.

2. Stealthwatch IDentity 어플라이언스가 있나요?
   - 대답이 예인 경우, 사용자 ID 필터를 사용하여 사용자의 IP 주소를 검색하십시오. 다음 섹션인 "Stealthwatch IDentity를 사용하여 IP 주소 찾기" 섹션을 참조하십시오.
   - 대답이 아니요인 경우, 사용자의 IP 주소를 얻을 수 있는 모든 툴(예: ipconfig)을 사용하십시오.
3. 사용자 IP 주소의 Host Snapshot: Exporter Interfaces(호스트 스냅샷: 엑스포터 인터페이스) 페이지를 엽니다. 188페이지의 "과도하게 사용된 인터페이스(호스트 스냅샷) 확인"을 참조하십시오.
4. 과도하게 사용되거나 용량에 거의 도달한 인터페이스가 있나요?
   - 대답이 예인 경우, 과도하게 사용된 인터페이스에 대한 Interface Summary Dashboard(인터페이스 요약 대시보드)를 열고 Top Active Conversations(상위 활성 대화)를 살펴봅니다. 189페이지의 "높은 대역폭 호스트(인터페이스 요약 대시보드) 찾기"를 참조하십시오.
   - 대답이 아니요인 경우 8단계로 이동합니다.
5. 호스트 쌍(호스트 및 피어)의 IP 주소가 대부분의 대역폭을 사용하고 있는 점을 참고합니다.
6. 가장 관심 있는 호스트 쌍에 기초하여 해당 IP 주소에 로그인한 사용자를 식별하기 위해 시도하는 호스트 또는 피어 중 하나의 Host Snapshot: Identity, DHCP & Host Notes(호스트 스냅샷: ID, DHCP 및 호스트 메모) 페이지를 엽니다. 190페이지의 "높은 대역폭 호스트에 로그인한 사용자 식별"을 참조하십시오.
7. 사용자를 식별할 수 있나요?
   - 대답이 예인 경우 사용자의 IP 주소를 얻고 8단계로 이동합니다.
   - 대답이 아니요인 경우 10단계로 이동합니다.
8. 연결된 Host Snapshot: Top Active Flows(호스트 스냅샷: 상위 활성 플로우) 페이지를 열고 사용자와 연결된 플로우 세부사항을 검토하여 문제의 잠재적인 원인을 판단합니다. 191페이지의 "상위 활성 플로우 검토"를 참조하십시오.
9. 문제를 해결할 수 있었나요?
   - 대답이 예인 경우 이 단계에서 중지합니다.
   - 대답이 아니요인 경우 10단계로 이동합니다.
10. 지금까지 수집한 정보를 취합하여 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

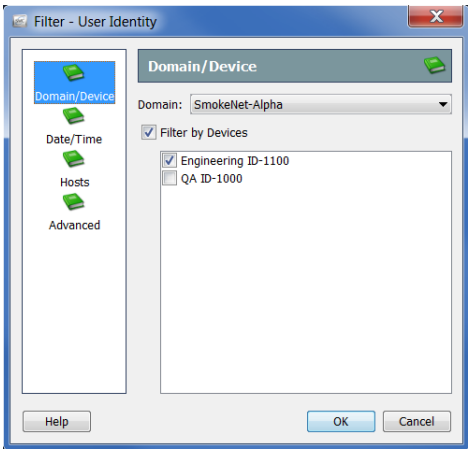
Stealthwatch IDentity를 사용하여 IP 주소 찾기

Stealthwatch Identity 어플라이언스를 사용하는 경우, 특정 사용자가 현재 사용 중이거나 사용했던 IP 주소를 신속하게 찾으려면 다음 단계를 수행하십시오.

1. 엔터프라이즈 트리에서 Identity Services(ID 서비스) 브랜치를 확장하고 사용하려는 Identity 어플라이언스를 찾습니다.
2. Identity 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Hosts(호스트) > User Identity(사용자 ID)**를 선택합니다.



Filter(필터) 대화 상자의 User Identity(사용자 ID) 페이지가 열립니다. 선택한 도메인과 디바이스가 Domain/Device(도메인/디바이스) 페이지에서 자동으로 선택됩니다.

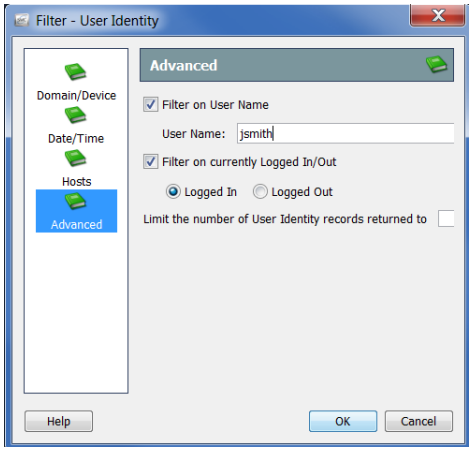


참고:

- 필터를 마지막으로 닫을 때 확인한 마지막 페이지에 필터가 열립니다. 필터를 한 번도 열지 않은 경우, Domain/Device(도메인/디바이스) 페이지에 열립니다.
- 사용자의 IP 주소에 대한 모든 Identity 어플라이언스를 살펴보려면 Domain/Device(도메인/디바이스) 페이지에서 **Filter by Devices(필터링 기준: 디바이스)** 확인란을 클릭하여 체크 마크를 제거합니다.

3. **Advanced(고급)** 버튼을 클릭합니다. Advanced(고급) 페이지가 열립니다.

4. **Filter on User Name(사용자 이름 필터링)** 확인란을 클릭하여 체크 마크를 추가한 다음 User Name(사용자 이름) 필드에 사용자 로그인 이름을 입력합니다.



5. 선택한 **Filter on currently Logged In/Out(현재 로그인/로그아웃한 사용자 필터링)** 옵션에 표시된 것과 같이 기본적으로 필터는 쿼리 당시 로그인한 사용자의 IP 주소만 찾습니다.

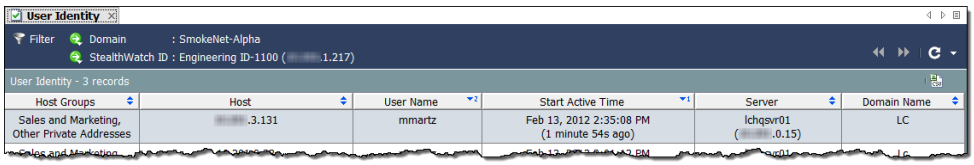
   사용자가 로그인한 다른 시기의 IP 주소를 검색하려면 **Filter on currently Logged In/Out(현재 로그인/로그아웃한 사용자 필터링)** 확인란을 클릭하여 체크 마크를 지운 다음에서 필터의 Date/Time(날짜/시간) 페이지로 이동하여 확인하려는 시간대를 지정합니다.

6. 원하는 경우, **Limit the number of User Identity records returned to(반환되는 사용자 ID 레코드 수 제한)** 필드에 값을 입력하여 표시되는 레코드 수를 변경합니다.

참고:

이 섹션에서 설명한 문제 유형을 해결하려면 일반적으로 필터에서 다른 파라미터를 정의할 필요가 없습니다. 추가 지원이 필요한 경우 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

7. **OK(확인)**를 클릭합니다. 지정된 사용자 이름과 연결된 IP 주소를 표시하는 User Identity(사용자 ID) 문서가 열립니다.



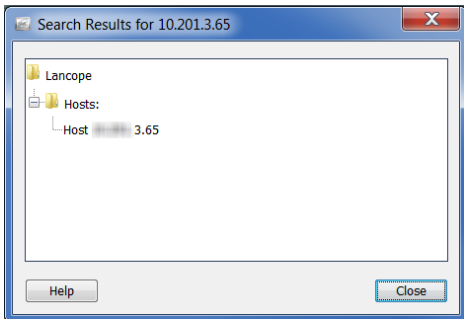
팁:

연결된 호스트 스냅샷을 열려면 IP 주소를 더블 클릭하십시오.

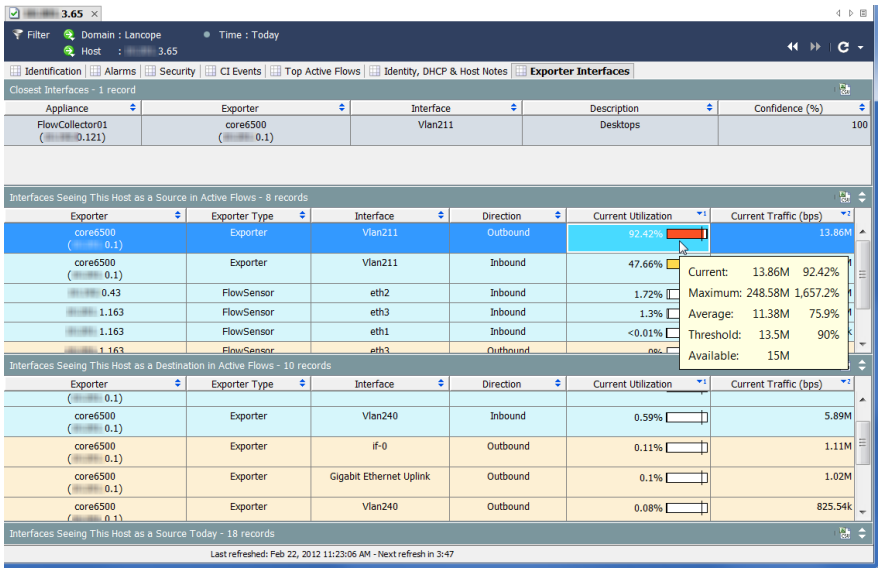
과도하게 사용된 인터페이스(호스트 스냅샷) 확인

특정 IP 주소의 Host Snapshot: Exporter Interfaces(호스트 스냅샷: 엑스포터 인터페이스) 탭을 열어 인터페이스가 오버로드되었는지 확인하려면 다음 단계를 수행하십시오.

1. IP 주소를 찾기 위해 사용자 ID 문서를 사용했나요?
   - 대답이 예인 경우 해당 IP 주소를 더블 클릭하여 호스트 스냅샷을 연 다음 4단계로 이동합니다.
   - 대답이 아니요인 경우 2단계로 이동합니다.
2. SMC 툴바에서 Global Search(전체 검색) 필드에 IP 주소를 입력한 다음 **Enter** 키를 누릅니다. 오른쪽 예에서와 같이 Search Results(검색 결과) 대화 상자에 해당 주소가 SMC에 나타난 각 위치의 리스트가 표시됩니다.



3. 호스트 IP 주소 항목을 더블 클릭합니다.
4. 호스트 스냅샷이 열리면 **Exporter Interfaces(엑스포터 인터페이스)** 탭을 클릭합니다.



팁:

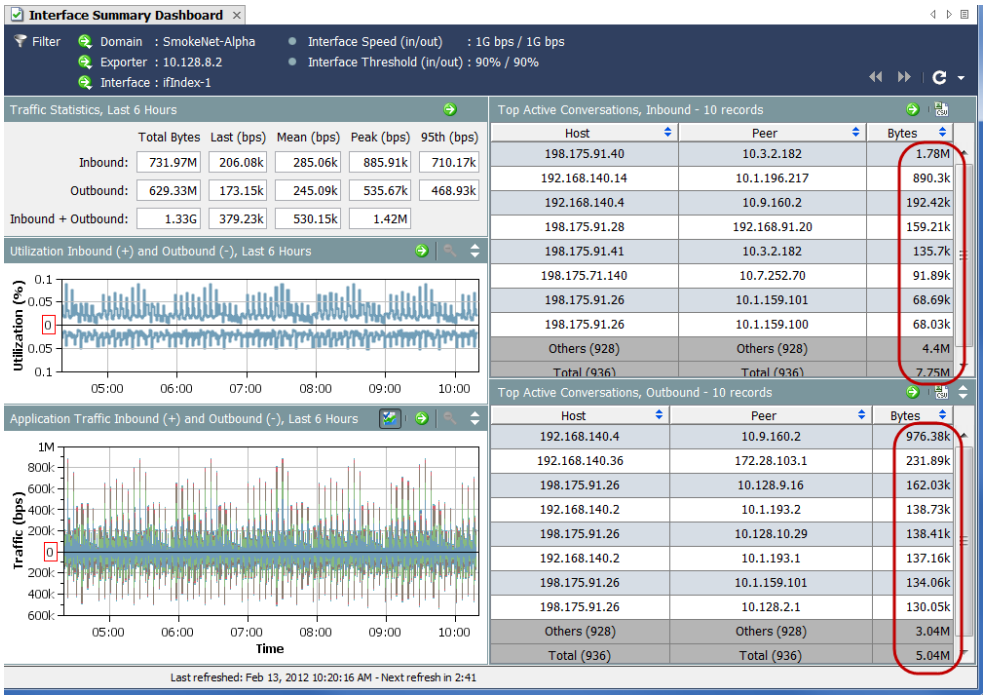
Current Utilization(현재 사용률) 열에 있는 값 위로 커서를 올려 놓으면 연결된 인터페이스에 대한 용량 가용성과 사용 정보를 확인할 수 있습니다.

5. 오버로드되었거나 용량에 거의 도달한 인터페이스가 있나요? (**힌트:** Current Utilization(현재 사용률) 열에 있는 빨간색, 주황색 또는 노란색 막대를 살펴보십시오.)

   - 대답이 예인 경우, 오버로드된 인터페이스의 Interface Summary Dashboard(인터페이스 요약 대시보드)를 열어 트래픽이 높은 이유를 알아봅니다. 다음 섹션인 "높은 대역폭 호스트(인터페이스 요약 대시보드) 찾기" 섹션을 참조하십시오.
   - 대답이 아니요인 경우, 호스트 스냅샷에서 **Top Active Flows(상위 활성 플로우)** 탭을 클릭하고 사용자와 연결된 플로우 세부사항을 검토하여 문제의 잠재적인 원인을 알아봅니다. 191페이지의 "상위 활성 플로우 검토"를 참조하십시오.

높은 대역폭 호스트(인터페이스 요약 대시보드) 찾기

Interface Summary(인터페이스 요약)에서 Exporter Interfaces(엑스포터 인터페이스) 탭을 살펴보다가 Interface(인터페이스) 열에서 오버로드되었거나 용량에 거의 도달한 인터페이스를 확인할 경우, 연결된 Interface Summary Dashboard(인터페이스 요약 대시보드)를 열려면 더블 클릭합니다.



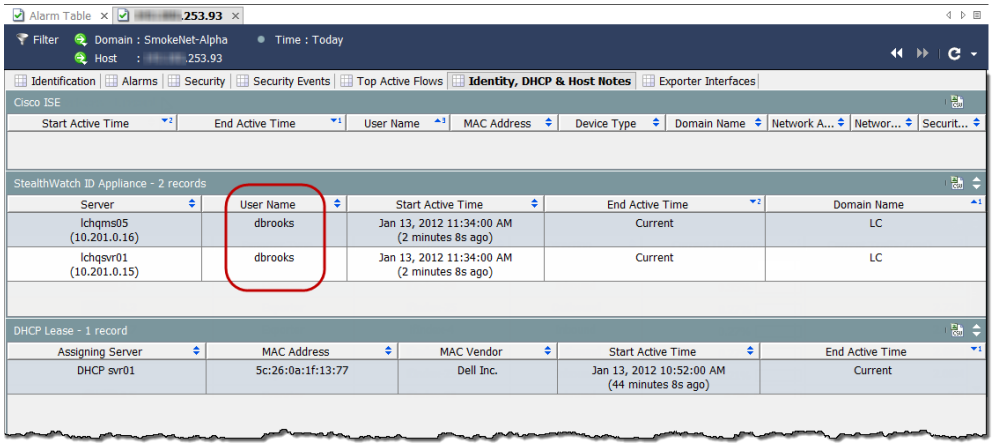
대시보드의 오른쪽에서 Top Active Conversations(상위 활성 대화) Inbound(인바운드) 및 Outbound(아웃바운드)를 확인합니다. 두 가지 방향에서 대역폭을 가장 많이 사용하고 있는(Bytes(바이트) 열 참조) 호스트 쌍(호스트 및 피어)을 식별합니다.

이 IP 주소 각각에 로그인한 사용자를 식별하기 위해 각 IP 주소에 대한 Host Snapshot: Identity, DHCP & Host Notes(호스트 스냅샷: ID, DHCP 및 호스트 메모) 탭을 엽니다. 190페이지의 "높은 대역폭 호스트에 로그인한 사용자 식별"을 참조하십시오.

높은 대역폭 호스트에 로그인한 사용자 식별

과도한 대역폭을 사용 중인 호스트 및/또는 피어의 IP 주소가 있는 경우, 해당 주소에 대한 호스트 스냅샷을 연 다음 **Identity, DHCP & Host Notes(ID, DHCP 및 호스트 메모)** 탭을 클릭합니다.

로그인 정보를 사용할 수 있으면 해당 IP 주소에 로그인한 사용자의 사용자 이름을 볼 수 있습니다.



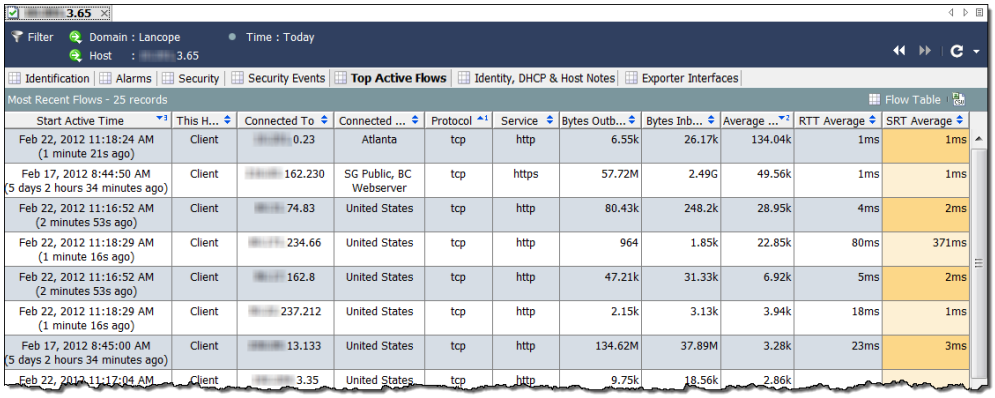
사용자 정보를 사용할 수 없는 경우, 지금까지 수집한 정보를 취합하여 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

팁:

Stealthwatch Identity 어플라이언스를 사용하는 경우, 사용자 이름을 더블 클릭하여 사용자 ID 문서를 열고 해당 사용자와 연결된 IP 주소를 확인할 수 있습니다.

상위 활성 플로우 검토

호스트 스냅샷의 Top Active Flows(상위 활성 플로우) 탭은 Stealthwatch 어플라이언스별로 25개의 가장 최신 플로우와 어플라이언스별로 트래픽이 가장 높은 25개의 플로우에 대한 자세한 정보를 제공합니다.



Start Active Time	This H...	Connected To	Connected ...	Protocol	Service	Bytes Outb...	Bytes Inb...	Average ...	RTT Average	SRT Average
Feb 22, 2012 11:18:24 AM (1 minute 21s ago)	Client	0.23	Atlanta	tcp	http	6.55k	26.17k	134.04k	1ms	1ms
Feb 17, 2012 8:44:50 AM (5 days 2 hours 34 minutes ago)	Client	162.230	SG Public, BC Webserver	tcp	https	57.72M	2.49G	49.56k	1ms	1ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	74.83	United States	tcp	http	80.43k	248.2k	28.95k	4ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	234.66	United States	tcp	http	964	1.85k	22.85k	80ms	371ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	162.8	United States	tcp	http	47.21k	31.33k	6.92k	5ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	237.212	United States	tcp	http	2.15k	3.13k	3.94k	18ms	1ms
Feb 17, 2012 8:45:00 AM (5 days 2 hours 34 minutes ago)	Client	13.133	United States	tcp	http	134.62M	37.89M	3.28k	23ms	3ms
Feb 22, 2012 11:17:04 AM	Client	3.35	United States	tcp	http	9.75k	18.56k	2.86k		

우선, RTT와 SRT 값을 살펴보십시오. SRT가 허용할 수 없을 정도로 높은 경우, 서버에 문제가 있는 것을 알 수 있으므로 문제를 해결하기 위해 서버 팀에 문의할 수 있습니다.

SRT 값이 적당한 경우, 네트워크의 다른 위치에 문제가 있으며 호스트 자체에 문제가 있을 가능성이 가장 높습니다. Top Active Flows(상위 활성 플로우) 탭을 살펴보면서 다음 질문을 검토하십시오. 질문에 답하면 호스트가 가로채기 되었거나 악성코드에 감염되었는지 여부를 판단하거나 사용자가 권한이 없는 활동에 참여하고 있는지 판단하는 데 도움이 됩니다.

1. 예상치 않은 연결(예: 권한 없는 호스트 그룹 또는 서버)이 있나요?
2. 많은 수의 예상치 않은 연결이 있나요?
3. 어떤 서비스가 사용되고 있나요?
4. 발신 및/또는 수신 중인 많은 양의 트래픽이 있나요?
5. bps 속도가 높은 연결이 있나요?
6. 호스트의 역할이 클라이언트에서 서버로 변경되었나요? 워크스테이션이 갑자기 서버 역할로 실행되는 경우, 악성코드에 감염되었거나 가로채기 되었을 가능성이 가장 높습니다.

이전 질문에 대한 답변에 기초하여 문제를 해결할 수 없는 경우 다음 단계를 수행하십시오.

1. 호스트의 안티 바이러스 프로그램 또는 방화벽이 문제가 되는 서버로의 액세스를 차단하고 있지 않은지 확인하십시오.
2. 호스트의 안티 바이러스 프로그램이 악성코드를 탐지하지 못했거나 보안이 침해되었을 수 있기 때문에 다른 안티 바이러스 프로그램(예: Malwarebytes의 Anti-Malware)을 사용하여 호스트에서 바이러스 스캔을 실행하십시오.
3. 어떤 새로운 애플리케이션이 호스트에서 설치되었거나 업데이트되었는지 확인하십시오. 설치 또는 업데이트된 경우, 애플리케이션이 제대로 구성되었는지 확인하십시오. 애플리케이션을 제거한 다음 다시 설치해야 할 수도 있습니다.

이러한 제안사항대로 문제를 해결할 수 없는 경우, 지금까지 수집한 정보를 취합하여 조직의 표준 에스컬레이션 절차에 따라 에스컬레이션합니다.

외부 조회

External Lookup(외부 조회) 기능을 사용하면 웹 애플리케이션(또는 내부 자산 데이터베이스)을 실행하여 IP 주소에 대한 추가 정보를 확인할 수 있습니다. 이 웹 애플리케이션 또는 데이터베이스를 SMC(Stealthwatch Management Console) 클라이언트 인터페이스 또는 SMC 웹 애플리케이션 인터페이스에서 직접 실행할 수 있습니다.

또한 외부 조회 기능을 사용하여 SMC 클라이언트 인터페이스에서 SMC 웹 애플리케이션 인터페이스로 신속하게 이동할 수 있게 해주는 바로가기를 만들 수 있습니다.

Stealthwatch System은 외부 조회 기능을 사용하기 위해 다음과 같은 기본 웹 애플리케이션(조회 옵션)을 포함합니다. 이 옵션은 Stealthwatch System에 추가할 필요가 없습니다.

- Cisco SenderBase
- DShield
- 호스트 보고서

Stealthwatch System 관리자가 IP 주소에 대한 추가 정보를 확인하기 위해 추가할 수 있는 웹 애플리케이션의 몇 가지 예는 다음과 같습니다.

- BigFix
- CiscoWorks
- Cisco ISE(Identity Services Engine)
- Splunk
- Tripwire
- Ziften

중요:

기본으로 제공되는 것 외의 조회 옵션을 추가하려면 SMC 웹 애플리케이션 인터페이스에서 External Lookup Configuration(외부 조회 컨피그레이션) 툴을 사용해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "외부 조회 구성"을 참조하십시오.

외부 조회 구성

앞에서 언급한 것과 같이 Cisco SenderBase, Dshield 및 호스트 이름은 외부 조회 기능에 사용하도록 기본적으로 포함되어 있으므로 Stealthwatch System에 추가할 필요가 없습니다. 이 기능에 다른 웹 애플리케이션을 사용하려면 해당 애플리케이션을 Stealthwatch System에 추가해야 합니다. 이렇게 추가하려면 SMC 웹 애플리케이션 인터페이스에서 외부 조회 컨피그레이션 툴을 사용하십시오.

참고:

이전에 추가한 각 외부 조회 옵션에 대해 v6.7로 업그레이드할 경우 v.6.7에서 항목이 2개가 됩니다.

Stealthwatch System은 외부 조회 컨피그레이션을 관리하기 위해 더 이상 webLinks.xml 파일을 사용하지 않습니다.

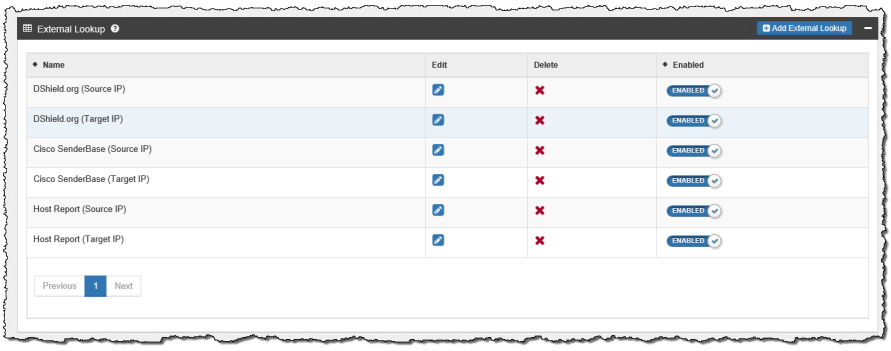
이 툴을 사용하여 웹 애플리케이션에 보낼 특정 파라미터를 구성할 수도 있습니다. 구성하는 파라미터는 조회를 수행 중인 IP 주소에서 사용할 수 있는 경우에만 전송됩니다.

조회 옵션을 추가하고 웹 애플리케이션에 보낼 파라미터를 구성하려면 다음 단계를 수행하십시오.

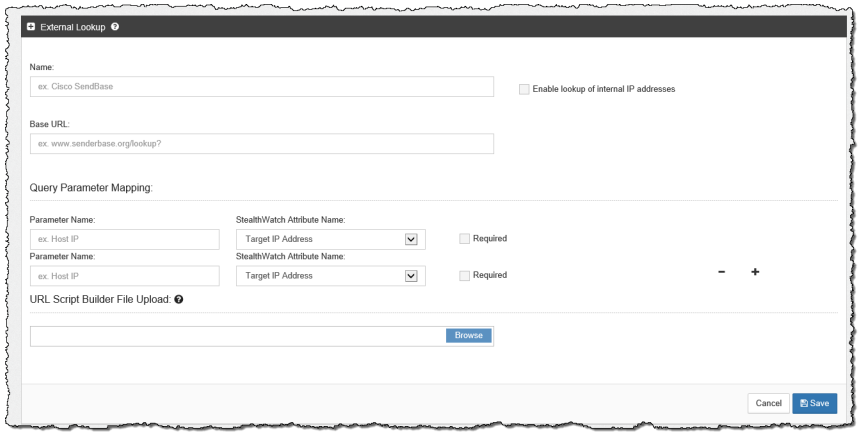
1. SMC 웹 애플리케이션 인터페이스의 왼쪽 탐색 창에서 **Tools(툴) > Settings(설정) > External Lookup Configuration(외부 조회 컨피그레이션)**을 클릭합니다. External Lookup Configuration(외부 조회 컨피그레이션) 페이지가 열립니다.

   외부 조회 기능에서 사용하지 않도록 조회 옵션을 비활성화하려면(하지만 나중에 사용하기 위해 컨피그레이션은 유지), 해당하는 행에서 **Enabled(활성화됨)**를 클릭합니다. 이 버튼은 *Disabled(비활성화됨)* 상태 표시를 설정/해제합니다.

   나중에 이 조회 옵션을 활성화하려면 **Disabled(비활성화됨)**를 클릭합니다. 이 버튼은 *Enabled(활성화됨)* 상태 표시를 설정/해제합니다.



2. **Add External Lookup(외부 조회 추가)**을 클릭합니다. External Lookup(외부 조회) 섹션이 열립니다.



3. 이 섹션의 상단 부분에서 다음 필드에 해당하는 항목을 입력합니다.
   - 이름
   - 기본 URL
4. 웹 애플리케이션에서 내부 IP주소에 대한 정보를 확인하려면 "Enable lookup of internal IP addresses(내부 IP 주소 조회 활성화)" 확인란을 선택하십시오.
5. Query Parameter Mapping(쿼리 파라미터 매핑) 섹션의 첫 번째 Stealthwatch Attribute Name(특성 이름) 필드에서 **Source IP Address(소스 IP 주소)** 또는 **Target IP Address(대상 IP 주소)**를 선택합니다.

중요:

추가한 조회 옵션에 대해 소스 IP 주소 또는 대상 IP 주소 중 하나를 구성해야 합니다.

6. 해당하는 Parameter Name(파라미터 이름) 필드에서 이전 단계에서 선택한 IP 주소를 지정하는 데 사용한 웹 애플리케이션의 파라미터 이름을 입력합니다.
7. 원하는 경우 조회를 수행 중인 IP 주소에 대해 웹 애플리케이션에 전송할 추가 파라미터 중 하나를 구성하십시오.
   - 대상 IP 주소
   - 대상 포트 번호
   - 소스 IP 주소
   - 소스 포트 번호
   - 호스트 이름
   - 타임스탬프(UTC)

- 전송 프로토콜
- 사용자

추가 파라미터를 추가하려면 첫 번째로 구성된 행의 끝에 있는 더하기(+) 기호를 클릭합니다. 구성된 행을 삭제하려면 해당하는 행에서 빼기(-) 기호를 클릭합니다.

참고:
각 조회 옵션에 대해 최대 20개의 쿼리 파라미터를 매핑할 수 있습니다.

8. 특정 웹 애플리케이션을 사용하여 조회를 수행할 때 파라미터를 필수로 설정하려면, Required(필수) 확인란을 선택합니다. 특정 웹 애플리케이션에 대해 필수로 지정하는 모든 파라미터는 조회를 수행 중인 IP 주소에 사용할 수 있어야 합니다. 필수 파라미터 중 하나 이상을 관련 IP 주소에 사용할 수 없는 경우, 해당 조회 옵션이 팝업 메뉴에서 활성화되지 않습니다.
9. 쿼리 파라미터가 표준 쿼리 파라미터와 일치하지 않는 경우, 맞춤화된 스크립트 빌더 컨피그레이션을 URL 스크립트 빌더 파일 업로드 필드에 업로드해야 합니다.

참고:
다음 스크립트 예에서 강조 표시된 변수를 사용하십시오.

스크립트 빌더 파일에는 쿼리 파라미터를 웹 애플리케이션이 쿼리를 실행하는 데 필요로 하는 URL 형식으로 구성하는 스크립트가 포함됩니다.

스크립트 빌더 파일을 업로드하지 않는 경우, Stealthwatch System은 아래에 표시된 기본 표준 쿼리 파라미터를 사용합니다.

```
BaseURL?[ParameterName1]=[ParameterValue1]&
ParameterName2]=[ParameterValue2]&
ParameterName3]=[ParameterValue3](등등, 추가한 각 파라미터에 대해)
```

URL 및 스크립트 예

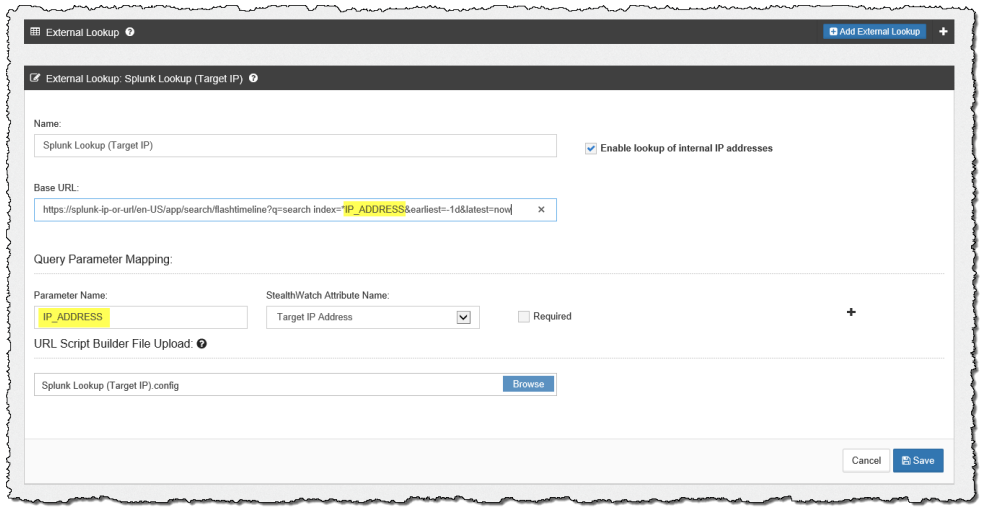
예 1

다음 URL 및 스크립트 예는 파라미터 이름(예: Splunk) 없이 값을 사용하는 웹 애플리케이션에 사용됩니다.

```
https://splunk-ip-or-url/en-US/app/search/flash-timeline
?q=search index=* 192.10.20.43 &earliest=-1d&lastest=now
```

```
def String query = baseUrl;
def String url = baseUrl;

vendorValues.each { valueOperand ->

    if (url.indexOf(valueOperand.getName()) != -1) {
        def String convertedStr = "";
        if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
            convertedStr = valueOperand.getFromValue().toString();
        } else if (valueOperand.getFromValue() instanceof Date) {
            convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
        }
        if (query.indexOf(valueOperand.getName()) != -1) {
            String[] parts = query.split(valueOperand.getName());
            query = "";
            def int i = 0;

            parts.each { part ->
                if (i + 1 < parts.length) {
                    query = query + part + URLEncoder.encode(convertedStr,"UTF-8");
                } else {
                    query = query + part;
                }

                i += 1;
            }

            if (url.endsWith(valueOperand.getName())) {
                query += URLEncoder.encode(convertedStr,"UTF-8");
            }
            url = query;
        }
    }
};

return query;
```

이 예에서 이전에 표시된 URL 형식으로 쿼리 파라미터를 구성하는 스크립트를 작성하려면 아래 이미지에서 강조 표시된 Parameter Name(파라미터 이름) 필드 항목을 사용하십시오.



참고:

필요한 만큼 많은 특성을 구성할 수 있지만, 동일한 수의 파라미터를 구성해야 합니다.

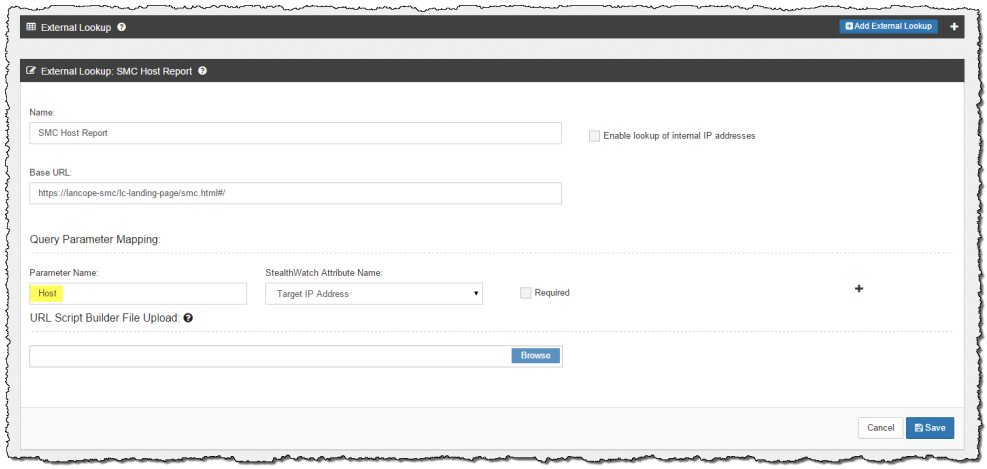
예 2

다음 URL 및 스크립트 예는 나머지 유사한 경로 파라미터(예: Stealthwatch 호스트 보고서)를 사용하는 웹 애플리케이션에 사용됩니다.

```
https://lancope-smc/lc-landing-page/smc.html#/host
/172.21.114.17
```

```
def String query = "";

vendorValues.each { valueOperand ->


    query += valueOperand.getName() + "/";
    def String convertedStr = "";
    if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
        convertedStr = valueOperand.getFromValue().toString();
    } else if (valueOperand.getFromValue() instanceof Date) {
        convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
    }
    String.valueOf('java.lang.Integer');
    query += URLEncoder.encode(convertedStr,"UTF-8");
};

def char lastChar = baseUrl.charAt(baseUrl.length() - 1);
if (lastChar != '?' && lastChar != '/' && lastChar != '&') {
    baseUrl = baseUrl + "?";
};

query = baseUrl + query;
return query;
```

이 예에서 이전에 표시된 URL 형식으로 쿼리 파라미터를 구성하는 스크립트를 작성하려면 아래 이미지에서 강조 표시된 Parameter Name(파라미터 이름) 필드 항목을 사용하십시오.

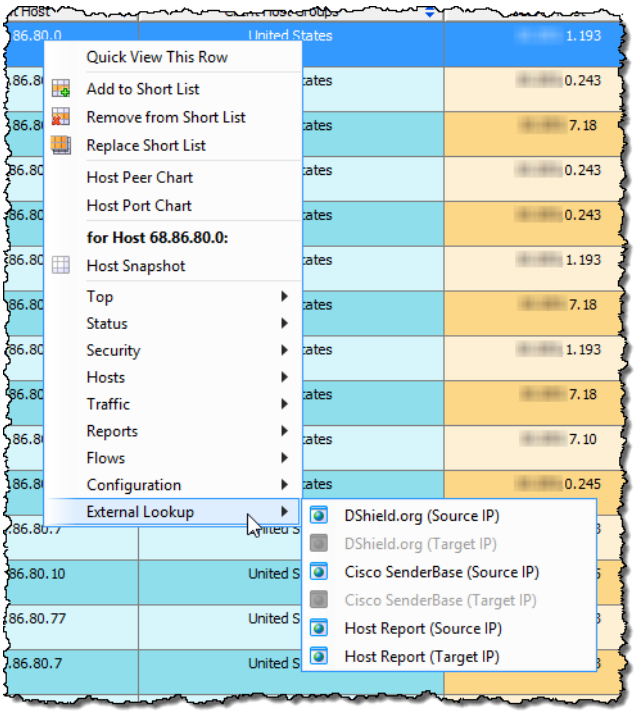


10. 완료하면 **Save(저장)**를 클릭합니다. External Lookup(외부 조회) 섹션으로 돌아갑니다. 이제 방금 추가한 조회 옵션이 리스트에 표시되며 기본적으로 활성화됩니다(외부 조회 기능에 사용 가능).

외부 조회 수행

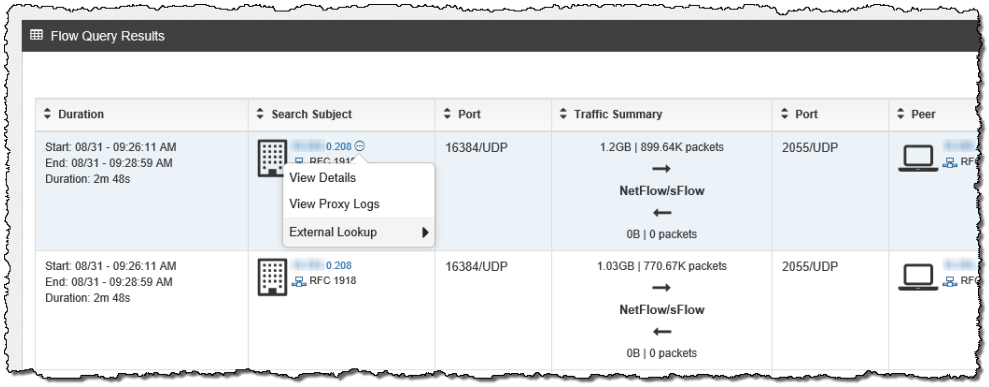
IP 주소에 대한 추가 정보를 확인하기 위해 웹 애플리케이션을 쿼리하려면 다음 단계를 수행하십시오.

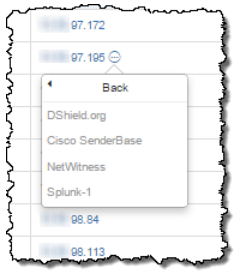
1. 다음 중 하나를 수행합니다.
   - SMC 클라이언트 인터페이스에 있는 경우 2단계로 이동합니다.
   - SMC 웹 애플리케이션 인터페이스에 있는 경우에는 3단계로 이동합니다.
2. 다음 단계를 완료합니다.
   a. SMC 클라이언트 인터페이스에서 관련 IP 주소를 포함하는 문서를 엽니다.
   b. IP 주소를 마우스 오른쪽 버튼으로 클릭합니다.
   c. 표시되는 팝업 메뉴에서 **External Lookup(외부 조회)**을 클릭합니다. 보조 팝업 메뉴가 나타납니다.



3. 다음 단계를 완료합니다.
   a. SMC 웹 애플리케이션 인터페이스에서 Standard Flow Query Results(표준 플로우 쿼리 결과) 페이지 또는 Advanced Flow Query Results (고급 플로우 쿼리 결과) 페이지를 엽니다.
   b. Search Subject(검색 주제) 열 또는 Peer(피어) 열에서 IP 주소 위에 마우스를 올려 놓고 줄임표를 클릭합니다.

c. 표시되는 팝업 메뉴에서 **External Lookup(외부 조회)**을 클릭합니다. 보조 팝업 메뉴가 나타납니다.

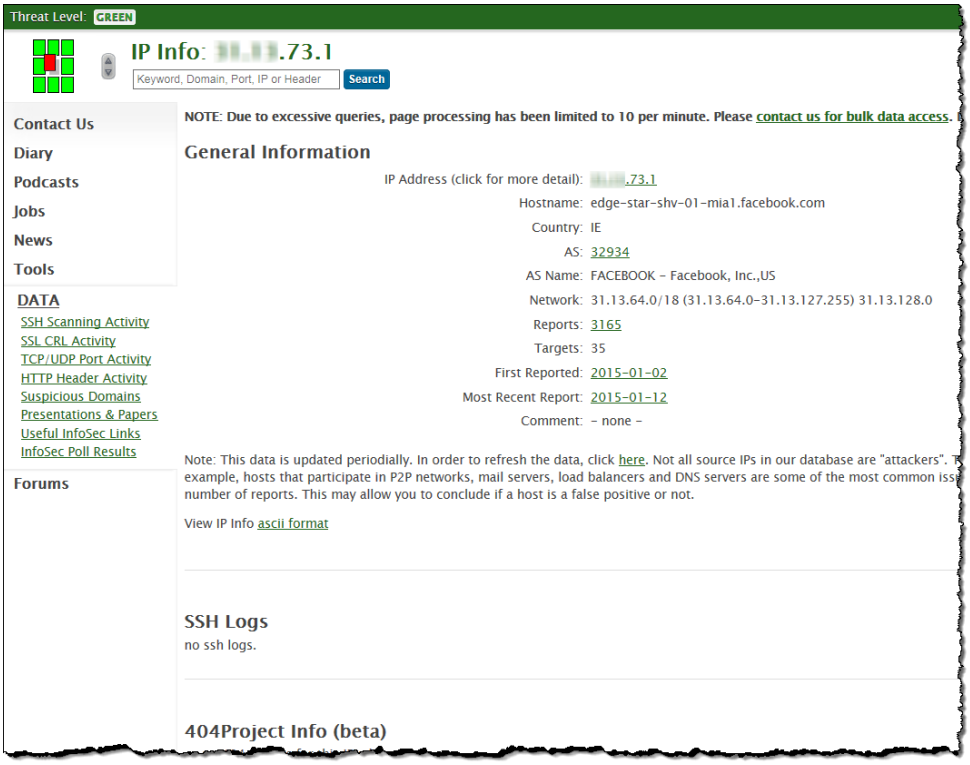




4. 3단계에 표시된 보조 팝업 메뉴에서 원하는 조회 옵션을 클릭합니다. 선택한 조회 옵션에 해당하는 웹 애플리케이션이 열리고(웹 애플리케이션에 로그인하라는 메시지가 표시될 수 있음) 조회를 수행 중인 IP 주소에 대한 쿼리 결과가 표시됩니다.

특정 웹 애플리케이션에 대해 필수로 지정하는 모든 파라미터는 조회를 수행 중인 IP 주소에 사용할 수 있어야 합니다. 필수 파라미터 중 하나 이상을 관련 IP 주소에 사용할 수 없는 경우, 해당 조회 옵션이 팝업 메뉴에서 활성화되지 않습니다. 자세한 내용은 194페이지의 "벤더 구성"을 참조하십시오.

다음은 DShield 웹 애플리케이션을 사용하는 쿼리에 대해 반환되는 정보의 예입니다.



9

SLIC Threat Feed 서비스

개요

SLIC(Stealthwatch Labs Intelligence Center) Threat Feed는 Lancope에서 제공하는 서비스로, 네트워크 위협에 대한 정보를 자주 업데이트하여 제공합니다. SLIC Threat Feed는 Stealthwatch가 유해한 네트워크 활동을 신속하고 정확하게 식별할 때 사용하는 악성코드 C&C(Command and Control) 서버와 기타 관심 있는 호스트(예: bogons, Tor)에 대한 데이터를 제공합니다.

이 장은 다음 항목으로 구성되어 있습니다.

- SLIC Threat Feed 정보
- 사전 요구 사항
- SLIC Threat Feed 작동 방식
- SLIC Threat Feed 활성화
- SLIC Threat Feed 비활성화
- SLIC 보안 이벤트

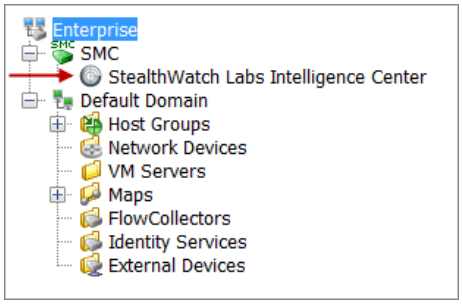
SLIC Threat Feed 정보

SLIC Threat Feed는 Lancope의 연구 이니셔티브로, 이를 통해 고객과 일반 대중에게 인터넷의 주요 위협에 대한 글로벌 인텔리전스를 제공할 수 있습니다. StealthLabs로 알려져 있는 Lancope의 연구 그룹은 사내 연구를 수행하고 서드 파티 전문가와 파트너로 구성된 광범위한 커뮤니티를 활용하여 전 세계에서 새로 등장하고 있는 위협 정보를 집계하고 있습니다.

StealthLabs 연구 팀의 구성원은 제품 개발자, 보안 연구원, 저자 및 연설가로서 컴퓨터 보안의 최전선에서 수십 년 간 축적된 다양한 경험을 보유하고 있습니다. SLIC Threat Feed는 연구 팀 구성원의 프레젠테이션과 웹 세미나 뿐만 아니라 컴퓨터 보안 위협 전망에서 논의 및 분석되었던 최신 개발을 담은 공개 블로그에 대한 링크를 제공합니다. 또한 C&C, 스캐닝 및 DDoS 활동 맵을 볼 수 있으며 Lancope 담당자와의 실시간 채팅도 가능합니다.

SLIC 웹 사이트에 액세스하여 SLIC Threat Feed에 대한 더 자세한 정보를 확인할 수 있습니다. 이 웹 사이트에 액세스하려면 다음 중 하나를 수행하십시오.

- 브라우저에 http://www.lancope.com/slic를 입력합니다.
- Enterprise(엔터프라이즈) 트리에서 StealthLabs Intelligence Center 브랜치를 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > StealthLabs Intelligence Center**를 선택합니다.



Enterprise(엔터프라이즈) 트리에서 (오른쪽에 있는 이미지에서 화살표로 표시된) SLIC 아이콘은 SLIC Threat Feed 활성화 여부 및 활성 알람이 존재하는지 여부에 따라 색상이 변경됩니다. 지침은 다음 리스트를 참조하십시오.

- SLIC Threat Feed가 비활성화된 경우, 아이콘은 회색입니다. (오른쪽에 있는 이미지에서 아이콘은 비활성화된 모드로 표시되었습니다.)
- SLIC Threat Feed가 활성화 상태이고 활성 알람이 없는 경우, 아이콘은 녹색입니다.
- SLIC Threat Feed가 활성화 상태이고 SLIC 채널 다운 알람이 있는 경우, 아이콘은 맨 아래에 X 표시가 있는 회색입니다. 다른 활성 알람이 없는 경우, SMC 아이콘의 색상이 주황색으로 변경됩니다. 현재 다른 알람이 존재하는 경우, 아이콘 색상은 최고 심각도 알람의 색상으로 변경됩니다.

사전 요구 사항

SLIC Threat Feed가 작동하려면 먼저 다음 조건을 충족해야 합니다.

- SMC 어플라이언스가 인터넷 액세스가 가능하며 SLIC 서버와 통신할 수 있어야 합니다.
- SMC 어플라이언스에서 DNS 서버를 구성해야 합니다.
- 네트워크에서 인터넷 프록시를 사용하는 경우 SMC 어플라이언스에서 프록시 서버를 구성해야 합니다.

참고:

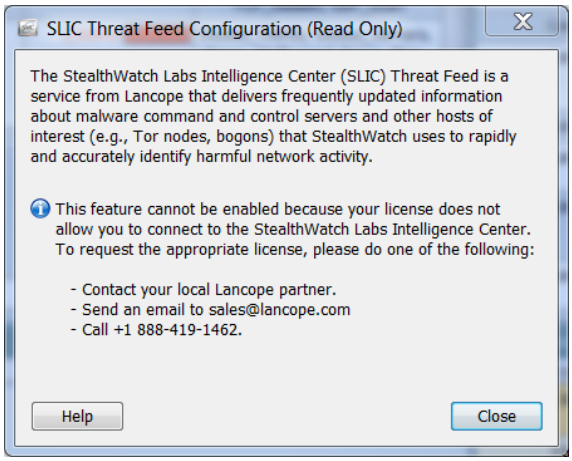
Threat Feed는 프록시 서버를 통해 인터넷에 연결될 수 있습니다. 프록시 서버에서 인터넷에 액세스해야 하는 경우, 어플라이언스 관리(관리자) 인터페이스를 연 다음 **Configuration(컨피그레이션) > Services(서비스)**를 클릭하여 프록시 서버를 구성하십시오. 자세한 내용은 *Stealthwatch System 하드웨어 환경 설정 가이드*, 해당하는 어플라이언스에 대한 환경 설정 가이드 또는 어플라이언스 관리 온라인 도움말을 참조하십시오.

- SLIC Threat Feed는 SMC 클라이언트 인터페이스에서 활성화되어야 합니다.
- SMC 라이선스는 SLIC Threat Feed를 포함해야 합니다.

라이선스 만료일까지 15일 미만이 남은 경우, 경고 대화 상자가 표시됩니다. 라이선스가 만료된 후에 다음 상황이 발생합니다.

- SMC가 SLIC Threat Feed를 비활성화합니다.
- Enterprise(엔터프라이즈) 트리에서 Bogon, C&C(Command & Control) 서버, Tor 호스트 그룹 브랜치 색상이 흐려지고 SLIC Threat Feed가 더 이상 동적 정보(피드)를 제공하지 않습니다.

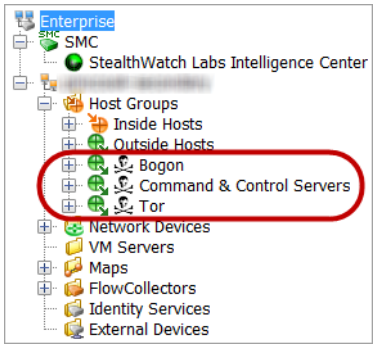
- SMC 클라이언트 인터페이스는 라이선스가 SLIC Threat Feed에 대한 연결을 허용하지 않기 때문에 이 기능을 활성화할 수 없다고 알려주는 메시지를 표시합니다.



SLIC THREAT FEED 작동 방식

다음은 SLIC Threat Feed를 활성화할 경우 발생하는 이벤트의 순서입니다.

1. SLIC Threat Feed는 SMC에 식별된 위협 리스트를 다운로드합니다. 이 리스트는 오른쪽 이미지에서와 같이 Enterprise(엔터프라이즈) 트리에서 각 호스트 그룹 브랜치 내부에 표시됩니다.



2. SMC는 시스템의 각 Flow Collector에 이 리스트를 배포합니다.
3. Flow Collector는 네트워크에 있는 호스트를 모니터링할 때 이 정보를 사용합니다.
4. Flow Collector가 SLIC Threat Feed에서 위협 호스트와 통신하고 있는 네트워크의 호스트를 탐지할 경우, 보안 이벤트가 트리거됩니다.

참고:

이러한 보안 이벤트가 트리거할 수 있는 알람(트리거하도록 구성된 경우)과 각 알람이 발생하기 전에 필요한 조건에 대한 자세한 내용은 212페이지의 "SLIC 보안 이벤트"를 참조하십시오.

5. SMC에서 SLIC Threat Feed가 활성화되었지만 SMC 서버가 SLIC Threat Feed에서 데이터를 검색할 수 없는 경우, SLIC Channel Down(SLIC 채널 다운) 알람이 트리거됩니다. Enterprise(엔터프라이즈) 트리에서 SLIC 아이콘이 회색으로 바뀌고 아이콘 맨 아래에 X가 나타납니다.

   다음 두 가지 조건 중 하나가 참인 경우, 이 알람이 지워집니다.

   - SMC 서버가 SLIC Threat Feed에서 데이터를 다시 검색하기 시작합니다.
   - SLIC Threat Feed를 비활성화합니다.

SLIC Threat Feed 호스트 그룹

참고:

SLIC Threat Feed 호스트 그룹 브랜치는 이름을 바꾸거나 변경, 이동 또는 삭제할 수 없습니다.

SLIC Threat Feed에는 악의적인 활동에 사용되는 것으로 알려진 IP 주소, 포트 번호, 프로토콜, 호스트 이름 및 URL이 포함되어 있습니다. SLIC Threat Feed에 포함되어 있는 호스트 그룹은 다음과 같습니다.

- Bogon - Bogon은 공용 인터넷에서 공식적으로 할당되지 않은 IP 주소입니다.
- C&C(Command & Control) 서버 - C&C 서버는 봇넷에 명령을 실행하고 가로채기된 컴퓨터에서 보고서를 다시 수신하는 중앙 집중식 컴퓨터입니다.
- Tor - Tor는 인터넷 익명화 서비스입니다.

참고:

사용자 호스트에 연결되어 있을 수 있는 SLIC Server Feed에서 URL을 탐지하려면 IPFIX를 내보내도록 구성되어 있는 FlowSensor 또는 라우터를 설치해야 합니다(NetFlow와 비교). (기본적으로, FlowSensor는 IPFIX를 내보내도록 구성되어 있습니다.)

이전에 언급한 호스트 그룹 중 하나에서 악성 호스트와 통신했던 호스트를 조사하려고 할 때 악성 호스트가 관련 호스트 그룹에 더 이상 나타나지 않는 경우, Alarm Table(알람 테이블)로 이동하여 다음 구성 요소에서 필터링을 수행하십시오.

- 유형 - 필터링할 악성 호스트 유형에 따라 해당하는 bogon, C&C(Command & Control) 또는 Tor 알람을 선택합니다.
- 날짜/시간 - 조사하려는 기간에 따라 필터링합니다.

SLIC THREAT FEED 활성화

SLIC Threat Feed를 사용하려면 먼저 Download and License Center(다운로드 및 라이선스 센터)에 액세스하여 SLIC Threat Feed 라이선스를 활성화해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 2장, "Stealthwatch 어플라이언스 라이선싱"을 참조하십시오.

SLIC Threat Feed를 처음으로 활성화하는 경우, SLIC Threat Feed 키를 입력해야 합니다. Lancope는 고객이 SLIC Threat Feed 기능을 구매하면 SLIC Threat Feed 키를 이메일로 보냅니다. 관리자 권한이 있는 사용자만 SLIC Threat Feed 키를 입력하고 SLIC Threat Feed를 활성화하거나 비활성화할 수 있습니다.

SLIC Threat Feed를 활성화하려면 다음 단계를 수행하십시오.

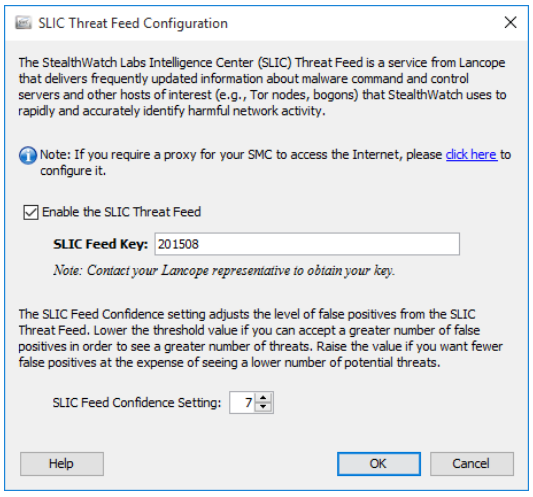
1. SMC에서 인터넷에 액세스하기 위한 프록시가 필요한가요?
   - 대답이 예인 경우 SMC 어플라이언스 관리 인터페이스로 이동하여 프록시를 구성합니다(**Configuration(컨피그레이션) > Services(서비스)**).
   - 대답이 아니요인 경우 2단계로 이동합니다.

참고:

자세한 내용은 *Stealthwatch System 하드웨어 환경 설정 가이드*, 해당하는 어플라이언스에 대한 환경 설정 가이드 또는 *어플라이언스 관리 온라인 도움말*을 참조하십시오.

2. Enterprise(엔터프라이즈) 트리의 SMC 클라이언트 인터페이스에서 StealthLabs Intelligence Center 브랜치를 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > SLIC Threat Feed Configuration(SLIC Threat Feed 컨피그레이션)**을 선택합니다.

   SLIC Threat Feed 컨피그레이션 대화 상자가 열립니다.

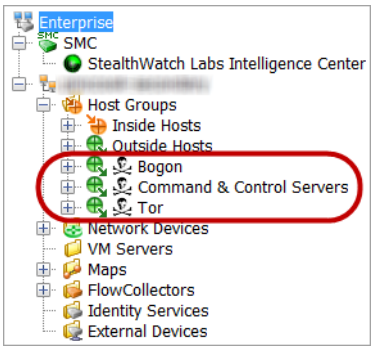


참고:

SLIC Threat Feed 기능에 대한 라이선스가 없는 경우, SLIC Threat Feed 컨피그레이션 대화 상자가 표시되지 않습니다. 대신 이 기능에 대한 라이선스가 없음을 알리는 메시지를 받게 됩니다.

3. "Enable the SLIC Threat Feed(SLIC Threat Feed 활성화)" 확인란을 선택합니다.
4. SLIC Threat Feed를 처음으로 활성화하고 있나요?
   - 대답이 예인 경우 SLIC Threat Feed 키를 SLIC Threat Feed Key 필드에 입력합니다.
   - 대답이 아니요인 경우 5단계로 이동합니다.
5. 원하는 경우 SLIC Feed Confidence Setting(SLIC Feed 신뢰도 설정)을 변경합니다. SLIC Feed Confidence Setting(SLIC Feed 신뢰도 설정)을 조정하여 Stealthwatch가 SLIC Threat Feed의 호스트와 일치할 경우 필요한 신뢰도 임계값을 선택할 수 있습니다.

   더 많은 수의 위협(숫자가 낮을수록 낮은 신뢰도 등급을 의미)을 보기 위해 더 많은 수의 오탐을 수락할 수 있는 경우 임계값의 값을 낮춥니다. 더 적은 수의 잠재적인 위협을 확인하는 대신 더 적은 수의 오탐을 원하는 경우 값을 늘립니다. 기본적으로 이 값은 7로 설정됩니다.
6. **OK(확인)**를 클릭합니다. 다음 호스트 그룹 브랜치가 Enterprise(엔터프라이즈) 트리에 표시됩니다.
   - Bogon
   - C&C(Command & Control) 서버
   - Tor



참고:

OK(확인)를 클릭한 다음에 이 리스트가 트리에 표시되는 데 최대 1분이 소요될 수 있습니다.

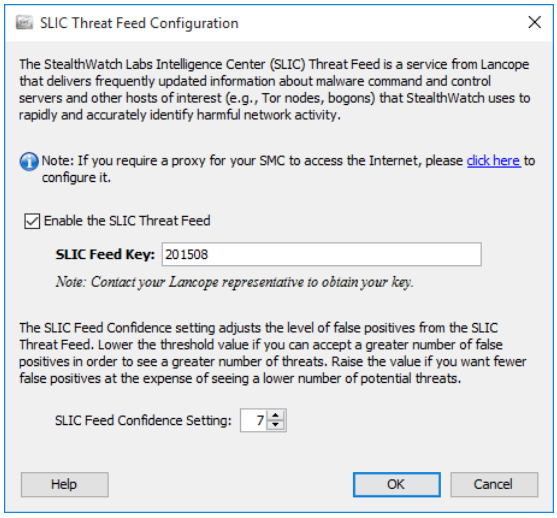
SLIC THREAT FEED 비활성화

관리자 권한이 있는 사용자만 SLIC Threat Feed를 비활성화할 수 있습니다.

SLIC Threat Feed를 비활성화하려면 다음 단계를 수행하십시오.

1. Enterprise(엔터프라이즈) 트리에서 StealthwatchLabs Intelligence Center 브랜치를 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > SLIC Threat Feed Configuration(SLIC Threat Feed 컨피그레이션)**을 선택합니다.

   SLIC Threat Feed 컨피그레이션 대화 상자가 표시됩니다.



2. "Enable the SLIC Threat Feed(SLIC Threat Feed 활성화)" 확인란을 선택하여 선택을 지웁니다. SLIC Threat Feed Key 필드의 항목이 흐려집니다.

참고:

나중에 SLIC Threat Feed를 활성화하도록 선택하려면 "Enable the SLIC Threat Feed(SLIC Threat Feed 활성화)" 확인란을 클릭하여 체크 마크를 추가하면 됩니다. SLIC Threat Feed 키를 다시 입력할 필요가 없습니다.

3. **OK(확인)**를 클릭합니다.

SLIC 보안 이벤트

이 섹션에서는 SLIC Threat Feed에 있는 위협 호스트에 의해 트리거될 수 있는 보안 이벤트에 대해 설명합니다. 이러한 보안 이벤트는 알람을 트리거하도록 구성된 경우, 각각 SMC 클라이언트 인터페이스에서 알람을 트리거합니다. (이 설정은 SMC 클라이언트 인터페이스의 Host Policy Manager(호스트 정책 관리자)에서 구성될 수 있습니다.) 알람이 트리거되면 SMC 클라이언트 인터페이스의 Alarm Table(알람 테이블)에 표시됩니다.

Flow Collector가 탐지하는 항목과 SMC 컨피그레이션에 따라 다음과 같이 보안 이벤트가 알람을 트리거할 수 있습니다.

보안 이벤트	설명
Bot Infected Host – Attempted C&C Activity(봇에 감염된 호스트 - C&C 활동 시도됨)	이 알람은 네트워크의 호스트가 C&C 서버 리스트에 나타나는 C&C 서버와 통신을 시도했으므로 이제는 봇넷의 멤버라는 것을 나타냅니다. 통신은 단방향만 가능합니다. 내부 호스트는 이니시에이터(initiator)로서 관심 지표(CI) 포인트를 누적합니다. 소스 호스트가 연결을 시도하는 C&C 서버가 내부 호스트이기도 한 경우 해당 C&C 서버는 대상 지표(TI) 포인트를 누적합니다. 이 색인에 대한 자세한 내용은 6장 "색인: 행동 변경 순위 지정"을 참조하십시오.
Bot Infected Host – Successful C&C Activity(봇에 감염된 호스트 - C&C 활동 성공)	이 알람은 네트워크의 호스트가 C&C 서버 리스트에 나타나는 C&C 서버와 통신하고 응답을 수신했으므로 이제는 봇넷의 멤버라는 것을 나타냅니다. C&C 서버는 네트워크의 내부 또는 외부에 있을 수 있습니다. 통신은 양방향입니다. 내부 호스트는 이니시에이터(initiator)로서 CI 포인트를 누적합니다. 소스 호스트가 연결하는 C&C 서버가 내부 호스트이기도 한 경우 해당 C&C 서버는 TI 포인트를 누적합니다.
Bot Command & Control Server(봇 C&C 서버)	이 알람은 네트워크 내부의 호스트가 봇넷의 C&C 서버로 작동하고 있음을 나타냅니다. 이 알람은 네트워크의 내부 호스트가 SLIC Threat Feed에서 C&C 서버로 식별한 IP 주소와 일치하는 경우 트리거됩니다. 이 알람은 소스 IP 주소만 식별합니다. 대상은 식별되지 않습니다.
Connection from Bogon Address Attempted(Bogon 주소에서 연결 시도됨)	네트워크 내부에 있는 호스트 서버와의 통신 시도에 실패한 외부 Bogon 호스트 인스턴스를 찾습니다. Bogon 접두사는 인터넷 라우팅 테이블에 표시되지 않아야 하는 경로입니다.
Connection From Bogon Address Successful(Bogon 주소에서 연결 성공)	클라이언트 역할을 하며 네트워크 내부에 있는 호스트 서버와의 통신에 성공한 외부 Bogon 호스트 인스턴스를 찾습니다. Bogon 접두사는 인터넷 라우팅 테이블에 표시되지 않아야 하는 경로입니다.

보안 이벤트	설명
Connection from Tor Attempted(Tor에서 연결 시도됨)	누군가가 현재 Tor 네트워크 종료 노드에서 사용자에게 연결을 시도했으나 실패했습니다. Tor는 인터넷 익명화 서비스입니다.
Connection from Tor Successful(Tor에서 연결 성공)	네트워크에 있는 하나 이상의 호스트가 현재 Tor 네트워크 종료 노드에서 트래픽을 수신하고 있습니다. Tor는 인터넷 익명화 서비스입니다.
Connection To Bogon Address Attempted(Bogon 주소로 연결 시도됨)	외부 Bogon 호스트와의 통신 시도에 실패한 네트워크 내부의 호스트 인스턴스를 찾습니다. Bogon 접두사는 인터넷 라우팅 테이블에 표시되지 않아야 하는 경로입니다.
Connection To Bogon Address Successful(Bogon 주소로 연결 성공)	네트워크 내부의 호스트와 외부 Bogon IP 주소 간의 양방향 트래픽 인스턴스를 찾습니다. 여기서 Bogon IP 주소란 공개 인터넷에서 할당되지 않았으며 통신이 수행되었음을 알려 주는 주소입니다. Bogon 접두사는 인터넷 라우팅 테이블에 표시되지 않아야 하는 경로입니다.
Connection to Tor Attempted(Tor로 연결 시도됨)	활성 내부 호스트 중 하나가 현재 Tor 네트워크 시작 노드에 연결을 시도했으나 실패했습니다. Tor는 인터넷 익명화 서비스입니다.
Connection to Tor Attempted(Tor로 연결 성공)	네트워크에 있는 하나 이상의 호스트가 Tor 네트워크에 트래픽을 전송하고 있습니다. Tor는 인터넷 익명화 서비스입니다.
Inside Tor Entry Detected(내부 Tor 엔트리 탐지됨)	활성 내부 호스트 중 하나가 Tor 시작 노드 역할을 수행하고 있습니다. Tor는 인터넷 익명화 서비스입니다.
Inside Tor Exit Detected(내부 Tor 종료 탐지됨)	활성 내부 호스트 중 하나가 Tor 종료 노드 역할을 수행하고 있습니다. Tor는 인터넷 익명화 서비스입니다.

참고:

이러한 알람에 대한 자세한 내용은 *SMC 클라이언트 온라인 도움말*의 "알람 리스트" 항목을 참조하십시오.

10

문제 원인 찾기

개요

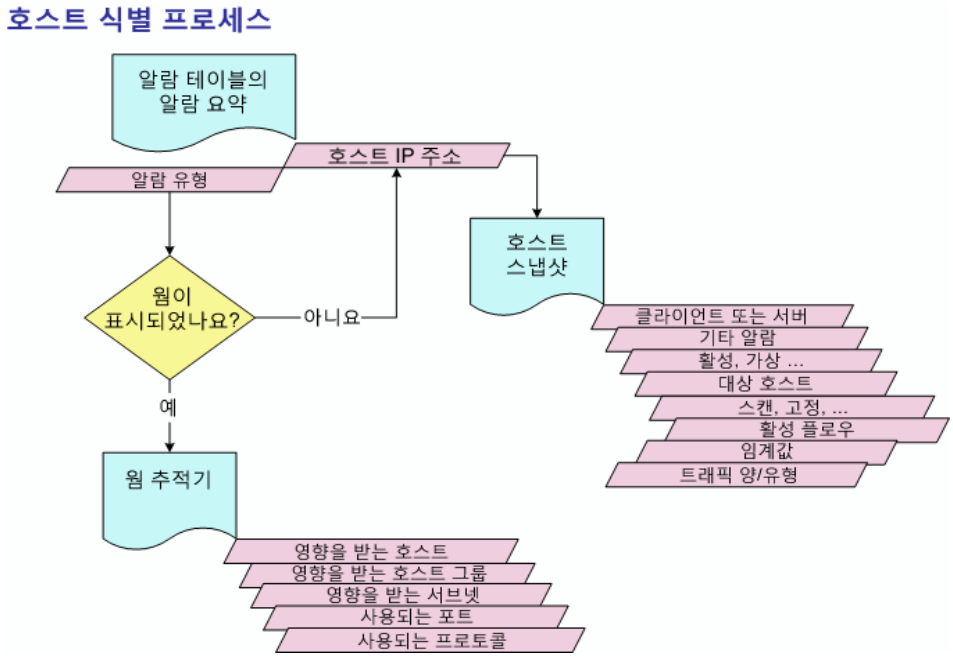
앞에서 살펴본 것처럼, 위협을 처리하는 첫 번째 단계는 어떤 호스트가 알람을 유발하고 있는지(즉 "소스 호스트") 찾아내는 것입니다. 이 장에서는 SMC를 사용하여 소스 호스트에 대한 정보를 수집함으로써 위협을 처리하는 방법에 대해 올바른 결정을 내릴 수 있는 방법에 대해 설명합니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 식별 프로세스
- 알람 요약
- 알람 테이블
- 전체 검색
- 호스트 스냅샷에서 세부사항 가져오기
- 정상적인 행동인가요?
- 어떤 호스트가 동일한 특징을 공유하나요?

식별 프로세스

어떤 경우에는 알람 조건과 관련하여 수행할 작업을 평가하는 것이 소스 호스트의 IP 주소 위치 찾기와 같이 간단합니다. 그러나, 어떤 때에는 호스트와 알람에 대한 자세한 정보도 필요합니다. 어느 경우든 간에, Alarm Summary(알람 요약)와 Alarm Table(알람 테이블)이 평가 도구로 활용됩니다. 다음 다이어그램은 의심스러운 호스트를 식별하려고 할 때 따라야 할 프로세스를 보여줍니다.



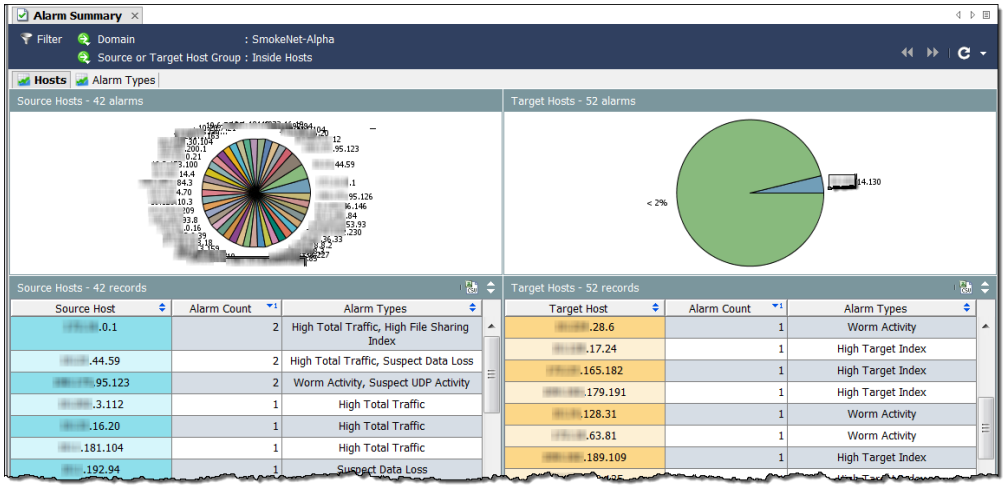
참고:

네트워크에서 문제를 일으킨 호스트의 레코드를 보관하면 "반복적인 위반자"가 있는지 쉽게 판단할 수 있습니다.

알람 요약

호스트를 식별하는 가장 간단한 방법은 Alarm Summary(알람 요약)를 사용하는 것입니다. 이 문서를 열려면 도메인, 엑스포터 또는 FlowSensor를 마우스 오른쪽 버튼으로 클릭한 다음 팝업 메뉴에서 **Status(상태) > Alarm Summary(알람 요약)**를 선택합니다.

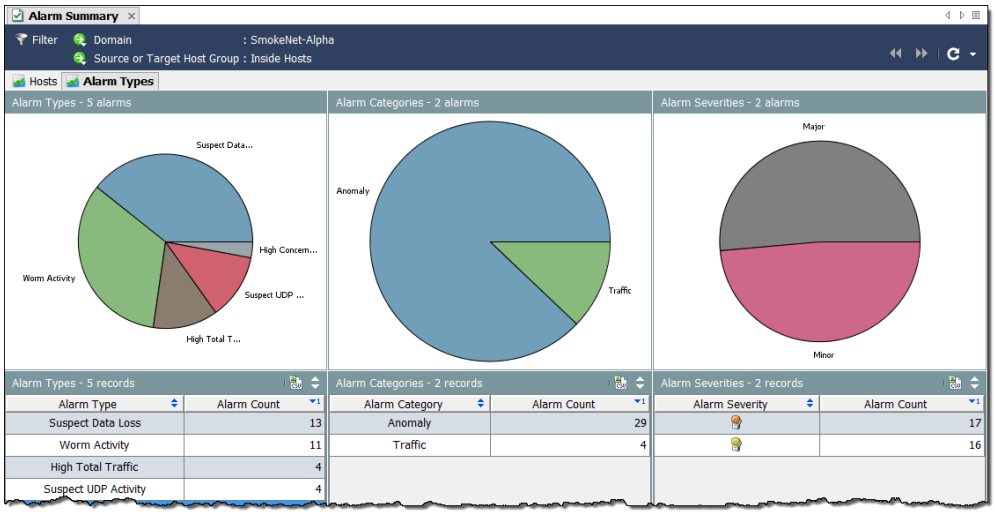
여기에서 유형, 카테고리, 심각도 레벨, 소스 호스트 IP 주소 및 대상 호스트 IP 주소별로 세분화된 네트워크 상의 모든 알람에 대한 그래픽 표시를 볼 수 있습니다. 다음 예에서는 Hosts(호스트) 탭에서 소스 호스트 IP 주소를 쉽게 볼 수 있습니다.



이 문서의 내용을 탐색하기 위해 다음 작업 중 하나를 수행할 수 있습니다.

- 호스트 스냅샷을 보려면 Hosts(호스트) 탭에서 호스트 IP 주소를 더블 클릭합니다.
- 알람 테이블의 필터링된 보기를 보려면 **Alarm Count(알람 수)** 또는 **Alarm Types(알람 유형)** 열을 더블 클릭합니다.

다른 보기를 보려면 **Alarm Types(알람 유형)** 탭을 클릭합니다.



이 문서의 내용을 탐색하기 위해 다음 작업 중 하나를 수행할 수 있습니다.

- 알람 테이블의 필터링된 보기를 보려면 Alarm Types(알람 유형) 탭에서 차트 또는 테이블 항목을 더블 클릭합니다.
- 해당 항목과 연결된 알람만 표시하기 위해 사전 필터링된 알람 테이블을 표시하려면 열 중 하나의 항목 또는 파이 차트를 더블 클릭합니다.

  예를 들어, Alarm Types(알람 유형) 열에서 **High Concern Index(상위 관심 지표)** 알람을 더블 클릭하는 경우, 알람 테이블이 상위 관심 지표(CI) 알람만 표시합니다.

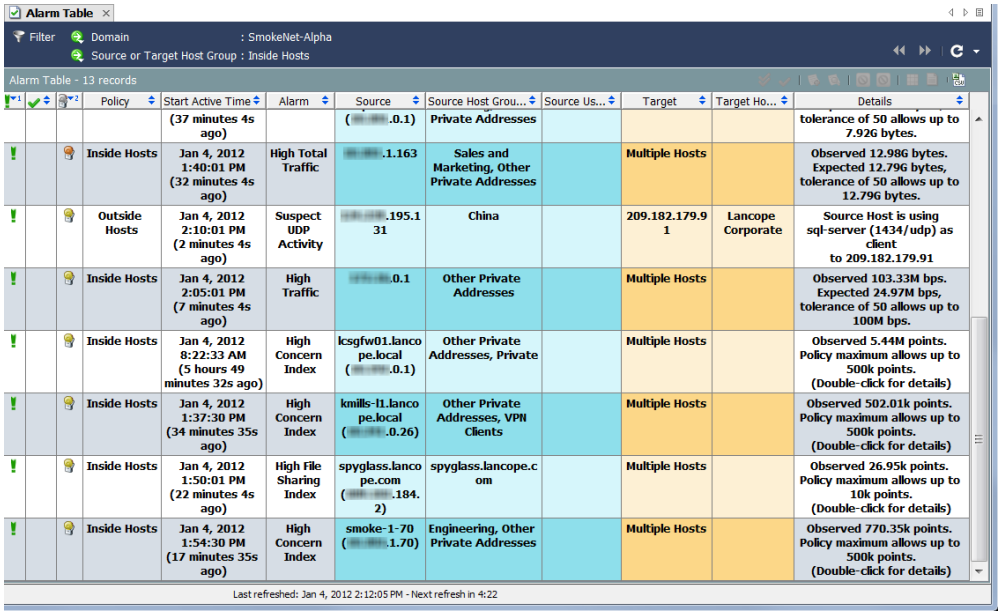
참고:

각 알람에 대한 설명은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

알람 테이블

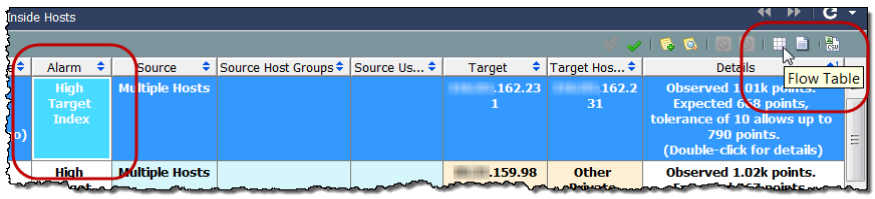
알람에 대한 자세한 정보가 필요한 경우, Alarm Table(알람 테이블)로 이동하십시오. 이 문서를 열려면 도메인, Stealthwatch Flow Collector, 호스트 그룹, 엑스포터 또는 FlowSensor를 마우스 오른쪽 버튼으로 클릭한 다음 팝업 메뉴에서 **Status(상태) > Alarm Table(알람 테이블)**을 선택합니다.

알람 테이블을 사용하면 "알람의 원인이 무엇인가?"와 "알람이 얼마나 심각한가?"와 같은 질문에 대한 해답을 찾는 데 도움이 됩니다. 기본적으로 알람 테이블은 알람을 생성한 Stealthwatch Flow Collector의 마지막 아카이브 시간 이후에 발생한 모든 활성 알람을 표시합니다.



대부분의 SMC 문서와 마찬가지로 알람 테이블은 문서를 여는 레벨과 일치하는 데이터를 표시합니다. 예를 들어 도메인 레벨에서 알람 테이블을 열 경우, 표시되는 알람이 해당 도메인 전체와 관련이 있습니다. 호스트 그룹 레벨에서 알람 테이블을 열 경우, 표시되는 알람이 해당 호스트 그룹과 해당 하위 호스트 그룹에만 관련이 있습니다.

알람을 보는 것 외에도 알람 테이블을 사용하면 로그인 권한에 따라 알람을 확인하고 닫거나 알람에 메모를 추가할 수 있습니다. 알람을 클릭한 다음 **Flow Table(플로우 테이블)** 버튼을 클릭하면 플로우 테이블이 해당 알람와 연결된 모든 플로우와 함께 표시됩니다.

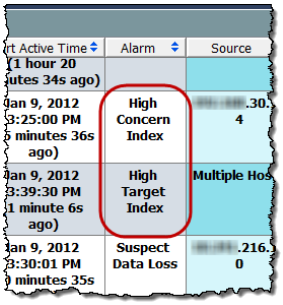


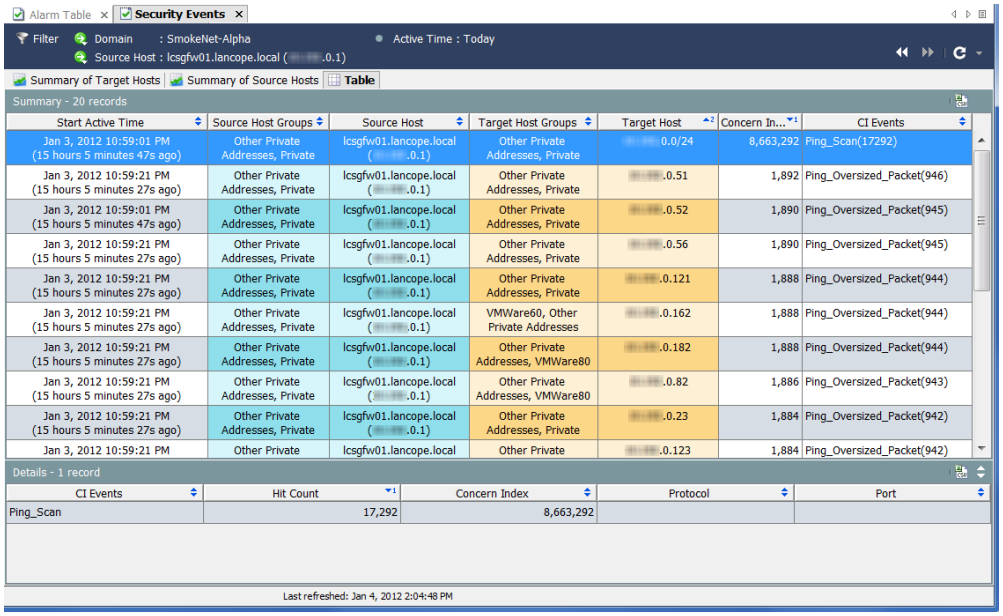
알람은 알람을 발생시킨 조건이 더 이상 존재하지 않을 때까지 활성 상태를 유지합니다. 알람 조건이 존재하지 않을 때 알람은 비활성 상태가 되고 이 시점에 원하는 경우 알람을 닫을 수 있습니다. 활성 알람을 확인할 수 있지만 닫을 수는 없습니다. 비활성 알람만 닫을 수 있습니다.

알람 테이블의 또 다른 이점은 이를 활용하여 다음 작업을 수행할 수 있다는 것입니다.

- 알람 확인/확인 취소
- 알람 메모 추가/보기
- 호스트 차단 또는 차단 해제(즉, 알람 완화)

알람 테이블 내에서 High Concern Index(상위 관심 지표) 알람 또는 High Target Index(상위 대상 지표) 알람을 더블 클릭할 경우, 다음 예에서와 같이 보안 이벤트 문서가 표시됩니다. 이 문서는 알람을 유발한 보안 이벤트에 대한 데이터를 표시합니다.





참고:

알람에 대한 응답 관련 정보는 11장, "알람 대응"을 참조하십시오.

전체 검색

Global Search(전체 검색) 기능을 사용하면 특정 항목에 대한 모든 문서를 도메인 전체에서 검색할 수 있습니다. 기본 툴바의 Search(검색) 필드에서 전체 문자열, 부분 문자열 또는 와일드카드(*)가 포함된 부분 문자열을 사용하여 다음 항목을 검색할 수 있습니다.

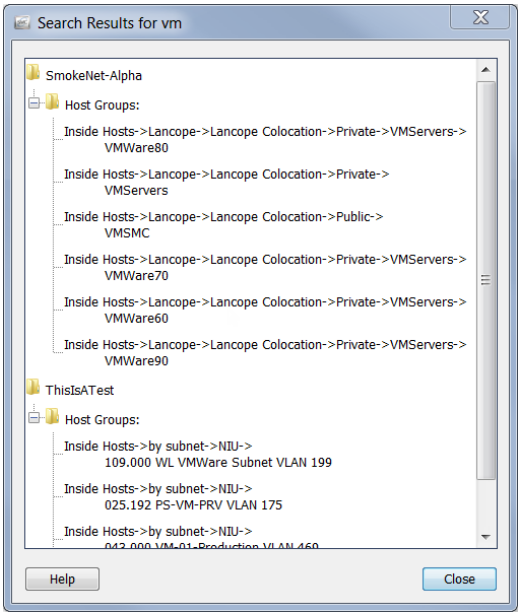
- 알람 ID
- 호스트 또는 엑스포터 IP 주소
- 다음 이름을 사용합니다.
  - 엑스포터
  - 호스트 그룹
  - 서버
  - 사용자
  - VM
  - VM 서버

참고:
검색 결과는 사용자 이름과 관련된 데이터 역할 및 기능 역할에 따라 제한됩니다.

팁:
Search(검색) 드롭다운 리스트 상자를 사용하여 이전에 검색한 항목을 선택한 다음 **Enter** 키를 눌러 검색을 실행할 수 있습니다.

검색을 수행하려면 툴바에서 Global Search(전체 검색) 상자 안을 클릭합니다.

검색 항목을 입력하고 **Enter** 키를 누릅니다. Search Results(검색 결과) 대화 상자가 열립니다.

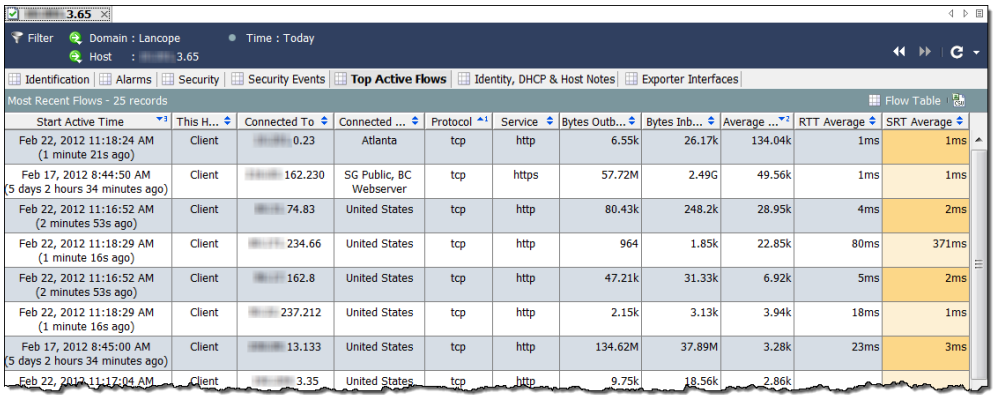


다음 중 하나를 수행합니다.

- 검색 결과를 더블 클릭합니다.
- 검색 결과를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 원하는 항목을 선택합니다.

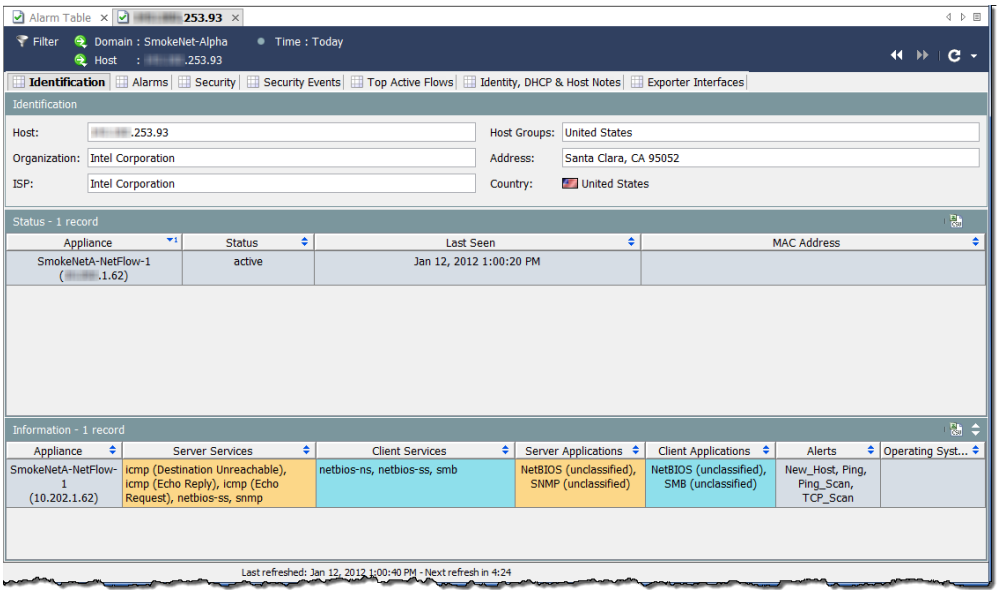
호스트 스냅샷에서 세부사항 가져오기

호스트 행동의 변화를 조사하는 경우 주로 호스트 스냅샷 문서를 제일 먼저 확인하게 됩니다. 이 문서는 네트워크의 각 호스트에 대해 가장 포괄적인 정보를 제공합니다.



대부분의 경우, SMC 클라이언트 인터페이스의 아무 곳에서나 호스트 IP 주소를 더블 클릭하면 해당 호스트에 대한 호스트 스냅샷을 확인할 수 있습니다. 호스트 스냅샷에는 다음 정보가 포함되어 있습니다.

- 가장 최근에 호스트와 연결된 플로우.
- 지금까지 가장 많은 양의 트래픽이 있는 플로우.
- 호스트에 로그인한 사용자 이름.
- 호스트와 연결된 모든 알람.
- 플로우를 전송 중인 엑스포터 인터페이스.
- 호스트 IP 주소가 할당된 조직과 해당하는 경우 이 호스트 IP 주소 및 ISP(Internet Service Provider).
- 호스트의 상태와 네트워크에서 마지막으로 통신한 것으로 확인된 시점.
- 호스트의 서버/클라이언트 프로파일과 운영 체제(OS), 호스트와 연결된 모든 알림.

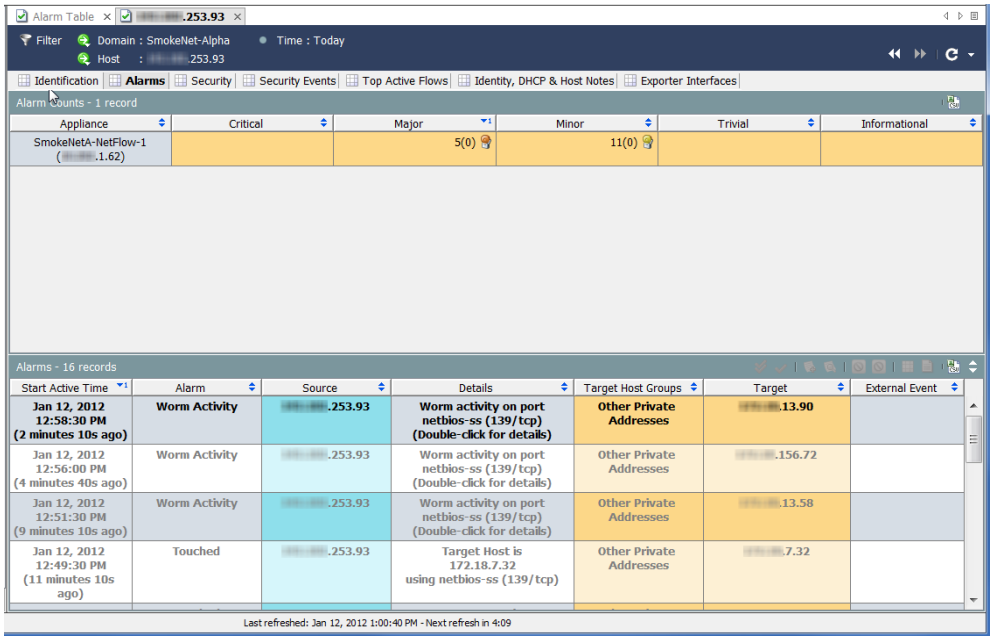


위의 예에서는 Identification(식별) 탭에서 선택한 호스트에 대해 다음 정보를 확인할 수 있습니다.

- 호스트에 개인 IP 주소가 있습니다.
- 이 호스트에 대해 시스템에서 마지막으로 확인한 활동은 2012년 1월 12일입니다.
- 시스템에서 다른 많은 서비스 중에 netbios 트래픽이 서버와 클라이언트 모두에서 호스트에 대해 발생했음을 보고했습니다.

호스트가 다른 알람을 유발했나요?

Host Snapshot(호스트 스냅샷)의 Alarms(알람) 탭은 해당 호스트가 다른 알람을 생성했는지와 만약 생성했다면 그 개수와 해당 유형을 나타냅니다.



호스트로 인해 더 많은 알람이 발생할수록 관심도가 높아져야 합니다. 심각도 레벨은 특정 상황에 맞게 조정할 수 있도록 구성 가능합니다.

앞의 예에서 선택한 호스트에 대해 다음 정보를 확인할 수 있습니다.

- Alarm Counts(알람 수) 테이블에 해당하는 Stealthwatch 어플라이언스에서 보고한 대로 알람 유형 및 카테고리에 기초하여 선택한 호스트에 의해 발생한 알람 수가 표시됩니다. 이 예에서 Stealthwatch 어플라이언스는 11개의 경미한 알람 조건과 5개의 중대한 알람 조건을 보고했습니다.

참고:

열 헤딩을 마우스 오른쪽 버튼으로 클릭하고 테이블에 표시할 특정 알람 유형의 열을 선택할 수 있습니다.

- 알람 테이블에 마지막 아카이브 시간 이후에 선택한 호스트에서 생성한 개별 알람에 대한 자세한 데이터가 표시됩니다. 이 경우, 이 호스트가 여러 웜 활동 알람을 생성했음을 알 수 있습니다.

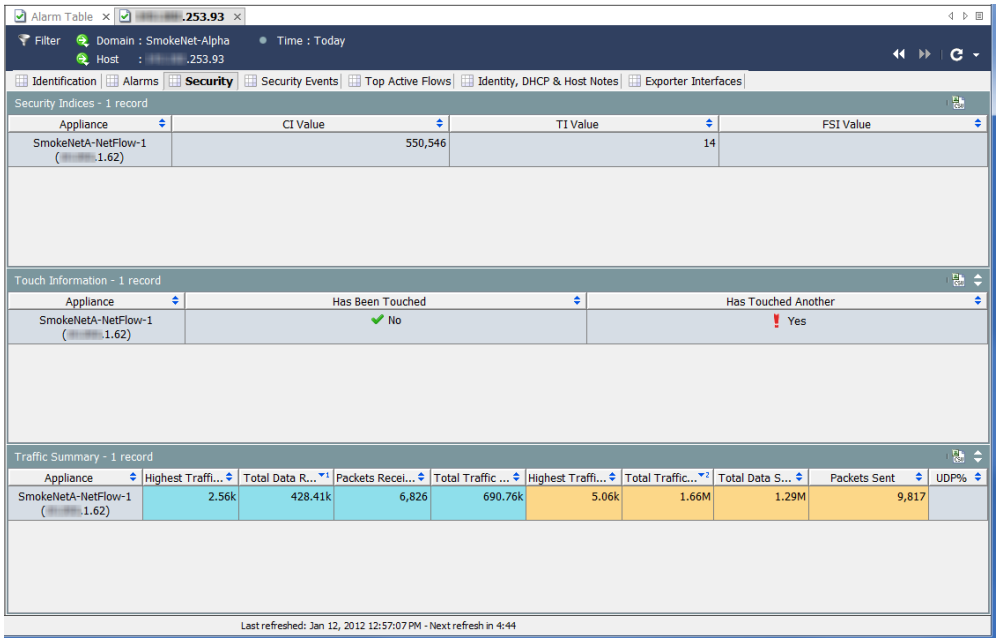
참고:

Host Policy Manager(호스트 정책 관리자)를 열어 이러한 값에 대해 설정된 정책 설정을 확인 및/또는 조정할 수 있습니다.

이 호스트가 감염되었을 것으로 의심되기 때문에 다음 단계는 감염 소스와 얼마나 많은 호스트가 영향을 받는지를 식별하는 것입니다.

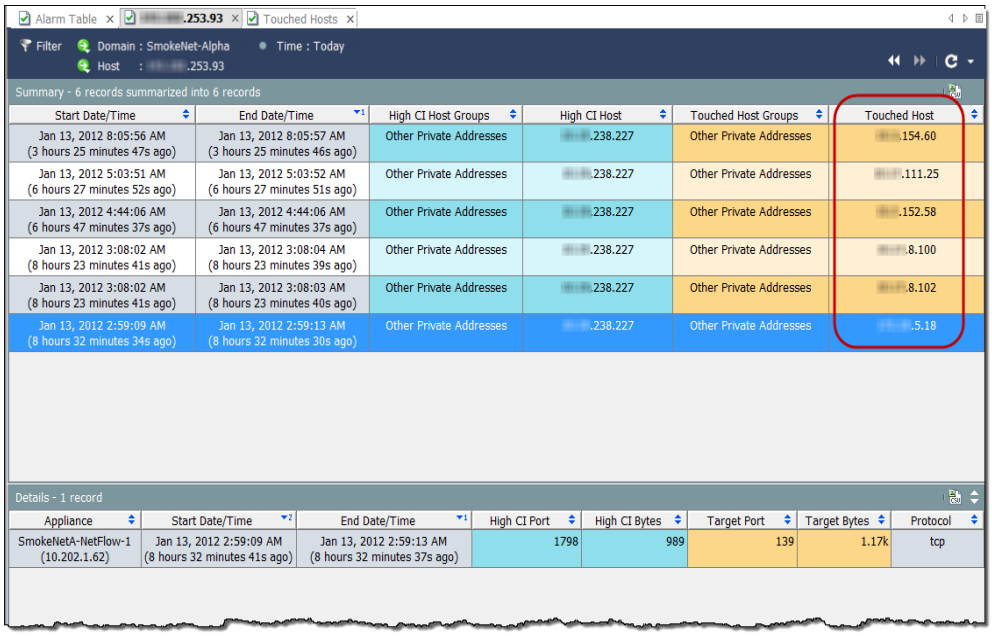
위협이 얼마나 광범위한가?

웜이 표시되는지 여부와 관계없이 다음 예에서와 같이 Host Snapshot(호스트 스냅샷)에서 Security(보안) 탭으로 이동하여 해당 호스트가 다른 호스트에 접근했는지 또는 다른 호스트에 의해 접근되었는지 확인할 수 있습니다. Touch Information(접근 정보) 테이블을 사용하면 이 호스트에 대한 위협이 다른 곳에서 발생했는지와 이 호스트가 다른 호스트에 위협을 확산시켰는지 판단하는 데 도움이 됩니다.



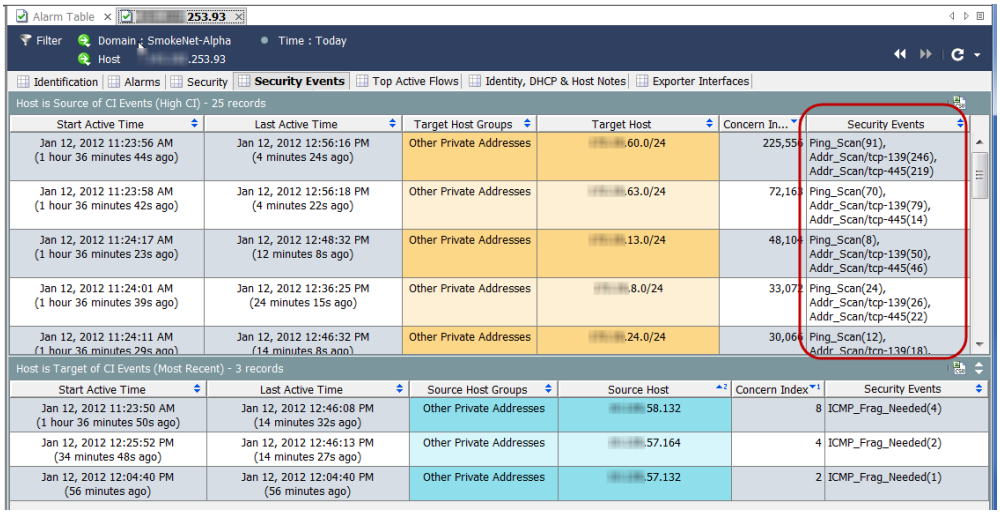
또한 Security Indices(보안 지표) 테이블은 이 호스트가 Stealthwatch 어플라이언스별로 다양한 지표의 제한을 얼마나 초과했는지 보여줍니다. Traffic Summary(트래픽 요약) 테이블은 이 호스트가 얼마나 많은 트래픽을 전송 및/또는 수신하고 있는지 보여주므로 파일 공유 활동을 판단하는 데 유용합니다.

앞의 예에서 이 호스트가 접근한 다른 호스트가 얼마나 되는지 확인해야 합니다. 이렇게 하려면 **Has Touched Another(다른 항목에 접근함)** 열로 이동하여 **Yes(예)**를 더블 클릭합니다. 접근된 호스트 문서가 열립니다. Touched Host(접근된 호스트) 열에서 상위 CI 호스트가 대상 호스트에 최소 6회 이상 접근했음을 확인할 수 있습니다.

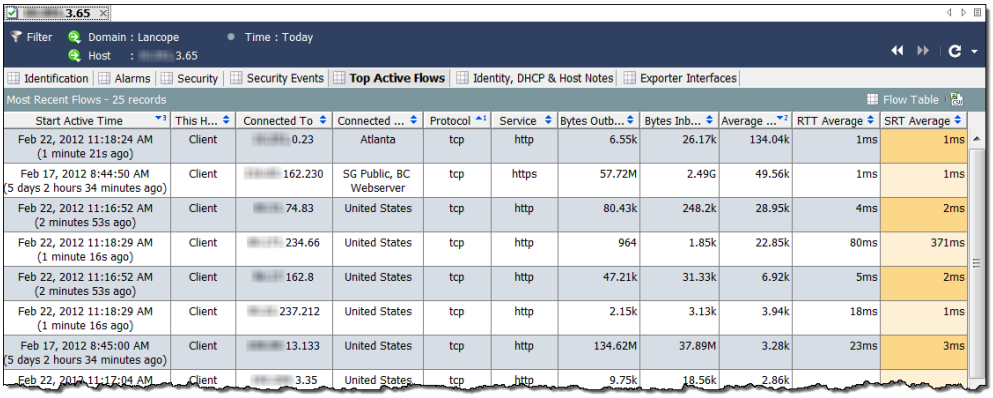


이전 테이블의 행 중에서 하나를 선택하여 맨 아래에 있는 Details(세부사항) 섹션에서 상위 CI 포트 및 바이트, 대상 포트 및 바이트, 영향을 받는 호스트에 사용되는 프로토콜과 같은 보다 자세한 정보를 확인할 수 있습니다.

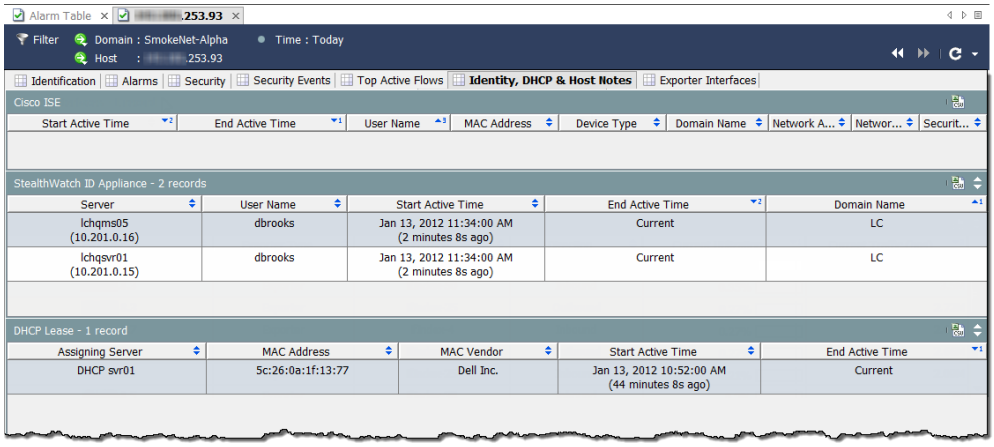
보안 이벤트 유형을 보려면 호스트 스냅샷에서 **Security Events(보안 이벤트)** 탭을 클릭합니다. 이 예에서 보안 이벤트 유형은 Address Scan(주소 스캔)과 Ping Scan(Ping 스캔)입니다.



이 호스트에 대한 상위 활성 플로우를 보려는 경우 **Top Active Flows(상위 활성 플로우)** 탭을 클릭합니다.



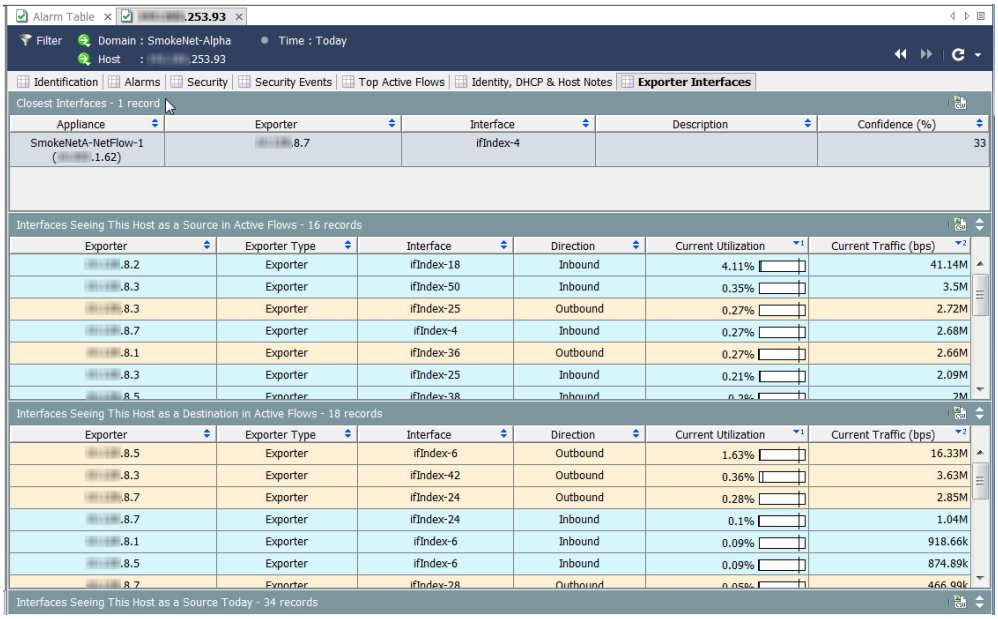
도메인의 어떤 사용자가 IP 주소와 연결되어 있는지 알아보려면 **Identity, DHCP & Host Notes(ID, DHCP 및 호스트 메모)** 탭을 클릭합니다.



참고:

사용자 ID 데이터를 얻으려면 Stealthwatch Identity 어플라이언스 또는 Cisco ISE 어플라이언스가 있어야 합니다.

가장 가까운 엑스포터에 대한 추가 정보를 확인하고 호스트가 활성 플로우의 소스 또는 대상인지 여부를 판단하려면 **Exporter Interfaces(엑스포터 인터페이스)** 탭을 클릭합니다.



이때 소스 호스트와 대상 호스트를 구분하려면 충분한 정보가 필요합니다. 이제 조직의 정책에 따라 정리 프로세스를 시작할 수 있습니다. 예를 들어, 다음 작업 중 하나를 수행할 수 있습니다.

- 각 호스트에서 안티 바이러스 소프트웨어를 실행합니다.
- 모든 호스트가 같은 호스트 그룹에 있다면, 전체 호스트 그룹을 차단하거나 격리할 수 있습니다.
- 데이터를 교환 중인 포트를 차단합니다.

정상적인 행동인가요?

지금까지는 알람 조건이 위협의 결과라고 가정했습니다. 하지만, 알람을 유발한 행동이 해당 호스트에서 완벽하게 정상이라면 어떻게 해야 하나요?

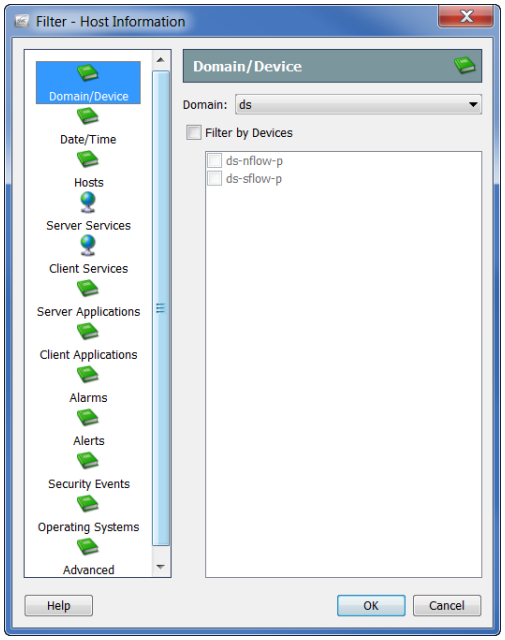
예를 들어 이메일 서버에 트래픽, 특히 이메일 트래픽이 많이 있습니다. 그러나, 파라미터가 해당 서버에서 너무 낮게 설정된 경우, 이 서버에 대해 다수의 메일 및/또는 트래픽 알람이 표시됩니다. 이 경우 해결책은 파라미터의 한계를 현실적인 수준으로 더 높게 설정하는 것입니다. 따라서 불필요하게 보게 되는 알람 수가 감소합니다. 다른 경우에는 정책을 편집해야 할 수 있습니다.

참고:

파라미터 조정 및 정책 편집에 대한 자세한 내용은 11장, "알람 대응"을 참조하십시오.

어떤 호스트가 동일한 특징을 공유하나요?

특정 알람을 유발하고 특정 서비스를 사용하거나 다른 공통적인 특징을 공유하는 호스트를 모두 보려는 경우, Host Information(호스트 정보) 필터를 사용할 수 있습니다. 이 필터에 액세스하려면 메인 메뉴에서 **Hosts(호스트) > Host Information(호스트 정보)**을 선택합니다.

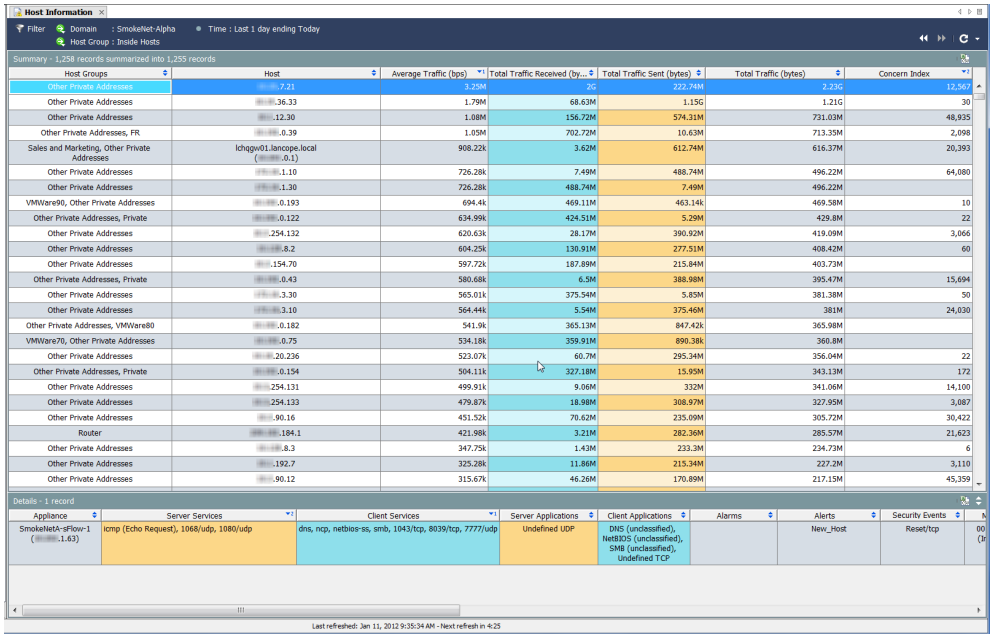


Filter - Host Information(필터 - 호스트 정보) 대화 상자를 사용하면 특정 파라미터를 선택하여 해당 파라미터 범위에서 적합한 모든 호스트를 대상으로 쿼리를 수행할 수 있습니다. 예를 들어 허용되지 않는 서비스 또는 애플리케이션을 사용하거나 Worm Activity(웜 활동) 알람을 유발하는 특정 호스트 그룹에서 모든 호스트를 대상으로 필터링할 수 있습니다.

참고:

정보 쿼리(IQ)를 수행 중이므로 경우에 따라 이 프로세스를 "호스트 IQ 수행 중"이라고 합니다.

원하는 파라미터를 지정한 후 **OK(확인)**를 클릭하여 Host Information(호스트 정보) 문서(즉, 호스트 IQ)를 요청된 데이터와 함께 표시합니다.



참고:

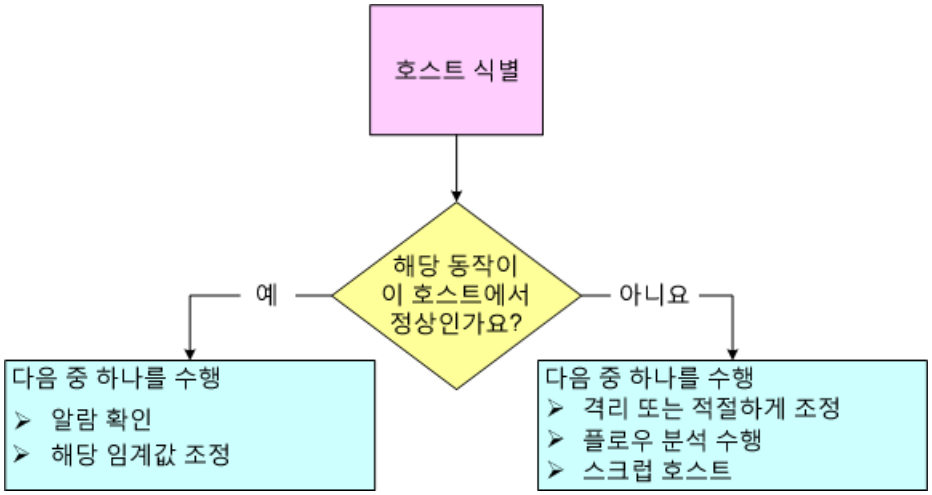
상위 관심 지표(CI) 알람뿐만 아니라 TCP_Scan 알림을 유발하는 모든 호스트를 대상으로 필터링하는 경우, 어떤 방식으로든 감염되었을 가능성이 가장 높은 호스트 리스트가 결과에 포함됩니다.

11

알람 대응

개요

다음 다이어그램은 네트워크에 대한 위협을 해결할 때 따라야 할 기본 단계를 보여줍니다.



그림에 나와 있는 것처럼 알람에 대해 조치를 취하기 전에 다음의 3가지 질문에 대답해야 합니다.

- 어떤 호스트가 처음으로 알람을 유발했나요?
- 알람을 유발한 행동이 이 호스트에서 정상인가요?
- 영향을 받은 다른 호스트가 있다면 해당 호스트는 무엇인가요?

참고:

정상이라고 알고 있는 활동에 대해서도 불필요한 알람이 많이 표시되는 경우를 볼 수 있습니다. 표시되는 불필요한 알람 수를 줄이는 방법에 대한 자세한 내용은 12장, "불필요한 알람 줄이기"를 참조하십시오.

위의 질문에 대답한 후에 SMC 소프트웨어를 사용하여 알람에 대응하는 방법을 결정할 수 있습니다. 이 장에는 알람에 대응할 때 취해야 할 가장 공통적인 조치에 대한 내용이 포함되어 있습니다.

참고:

알람에 대응할 때 수행할 수 있는 다른 절차에 대한 자세한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

이 장은 다음 항목으로 구성되어 있습니다.

- 알람에 대응하는 방법
- Stealthwatch 완화 기능

알람에 대응하는 방법

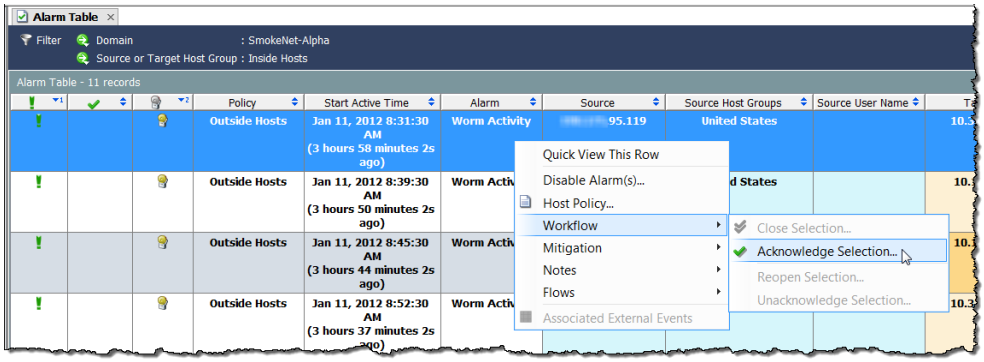
알람에 대응하는 방법에는 여러 가지가 있습니다. 알람 확인, 알람 확인 취소, 알람 닫기, 닫힌 알람 다시 열기를 수행할 수 있습니다. 이 특정한 절차에 대해 읽어보려면 다음 섹션을 참조하십시오.

알람 확인

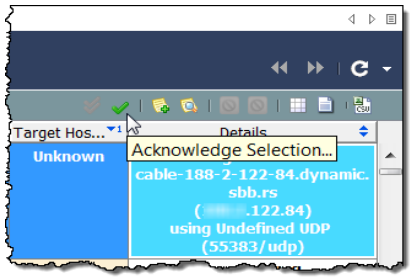
알람을 확인할 때 이것은 알람이 조사중임을 나타냅니다. 이 방법은 워크플로와 다른 팀 구성원에게 알람이 조사중임을 알리는 데 유용합니다. 알람을 확인하기 전에 필요한 경우 알람 확인을 취소할 수 있다는 점을 기억하십시오.

알람은 알람이 활성 또는 비활성 상태인지 여부에 관계없이 확인 또는 확인 취소될 수 있습니다. SMC를 사용하여 알람을 확인하려면 다음 단계를 완료하십시오.

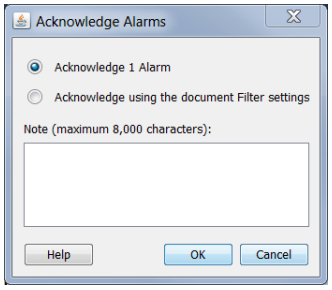
1. Alarm Table(알람 테이블)에서 알람을 마우스 오른쪽 버튼으로 클릭하고 **Workflow(워크플로) > Acknowledge Selection(선택 항목 확인)**을 선택합니다.



또한 알람을 클릭한 다음 알람 테이블 툴바에서 **Acknowledge Selection(선택 항목 확인)** 버튼을 클릭할 수 있습니다.



알람이 닫히는 이유를 설명하는 메모를 입력하도록 요청하는 Acknowledge Alarms(알람 확인) 대화 상자가 열립니다.



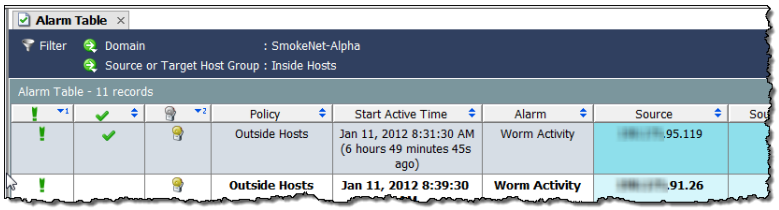
2. 알람을 확인하거나 문서 필터에서 설정을 사용하여 확인하도록 지정합니다. 알람 확인의 의미를 파악하려면 사용 가능한 옵션에 대한 다음 설명을 참조하십시오.

   - **Acknowledge [x] Alarm(s)([x]개의 알람 확인)** - 알람 테이블에 현재 표시되는 알람만 확인합니다. 여기서 [x]는 선택한 알람의 총 수와 일치합니다. 이 옵션을 클릭하는 경우 시스템에서 각 알람을 하나씩 확인합니다. 따라서 많은 수의 알람이 있는 경우(예: 1000개 이상) 시스템에서 이 프로세스를 완료하는 데 상당한 시간이 소요됩니다.
   - **Acknowledge using the document Filter settings(문서 필터 설정을 사용하여 확인)** - 확인 프로세스 동안 *발생할 수 있는 모든 새로운 알람을 포함하여* 알람을 하나씩 확인하는 대신 대량으로 현재 필터 설정에 포함된 모든 알람을 확인합니다. 예를 들어, 알람 테이블 필터가 경미한 알람 유형만 표시하도록 설정된 경우, 이 설정에 기초하여 모든 알람을 확인하도록 선택하는 것입니다. 시스템에서는 알람 테이블에 현재 표시되는 경미한 알람뿐만 아니라 확인 프로세스가 진행되는 동안 생성되었을 수 있지만 표시되지 않은 경미한 알람도 확인합니다.

참고:

Acknowledge using the document Filter settings(문서 필터 설정을 사용하여 확인) 옵션이 대량으로 알람을 확인하기 때문에 특히, 1000개 이상의 알람이 있는 경우 다른 옵션보다 작업이 훨씬 더 신속하게 수행됩니다. 그러나 이 옵션을 선택하면 표시된 적이 없는 알람을 확인할 수 있다는 점을 인지해야 합니다.

3. 텍스트 입력 필드를 클릭하고 알람을 확인하는 이유에 관한 설명을 입력한 다음 **OK(확인)**를 클릭합니다. 체크 마크( )가 Acknowledged(확인됨) 열에 나타나고 Last Note(마지막 메모) 열을 표시하도록 선택한 경우 이 열에 메모가 나타납니다. 해당 알람에 대한 테이블 열의 텍스트는 굵은 글씨체가 해제됩니다.



참고:

Acknowledged(확인됨) 및/또는 Last Note(마지막 메모) 열을 확인하려면 열 헤더를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 해당하는 옵션을 선택합니다.

알람 확인 취소

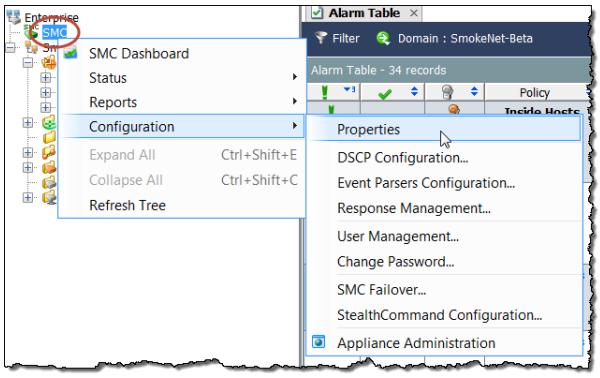
SMC를 사용하면 하나 이상의 확인된 알람을 확인 취소할 수 있습니다. 예를 들어, 실수로 알람을 확인한 경우, 다음 단계를 완료해야 할 수 있습니다.

1. Alarm Table(알람 테이블)에 확인된 알람 중에서 확인을 취소하려는 알람을 표시합니다. 필요한 경우 알람 필터를 사용합니다.
2. 확인을 취소하려는 알람을 마우스 오른쪽 버튼으로 클릭하고 **Workflow(워크플로) > Unacknowledge Selection(선택 항목 확인 취소)**을 선택합니다. Unacknowledge Alarms(알람 확인 취소) 대화 상자가 열립니다.
3. 알람 메모를 입력하고 **OK(확인)**를 클릭합니다.
4. 확인할 각 알람에 대해 2단계와 3단계를 반복합니다.

알람 닫기

알람이 원하는 대로 해결되었음을 표시하려는 경우, 알람을 닫을 수 있습니다. 참고로, 알람은 수동으로 닫을 필요가 없습니다.

알람이 비활성 상태가 되면 SMC Properties(SMC 속성)의 Data Retention(데이터 보존) 페이지에서 알람 테이블에 지정된 일수보다 알람이 오래될 경우 데이터베이스에서 자동으로 제거됩니다. 이 페이지에 액세스하려면 엔터프라이즈 트리에서 SMC 아이콘을 마우스 오른쪽 버튼으로 클릭한 다음 **Configuration(컨피그레이션) > Properties(속성)**를 클릭합니다.

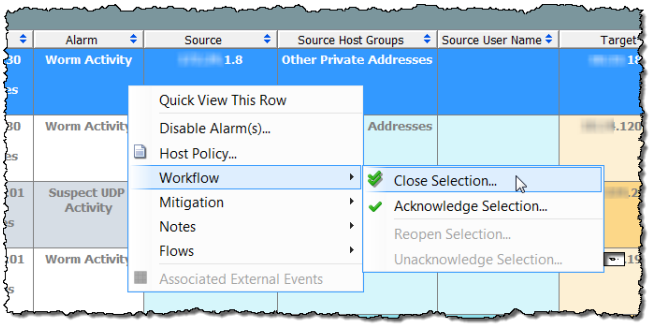


알람을 닫기 전에 다음 사항에 유의해야 합니다.

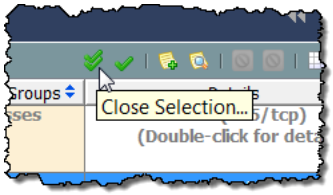
- 활성 알람은 닫을 수 없습니다.
- 특정 호스트에 대한 알람을 닫을 때 호스트는 다음 아카이브 시간 이전에 다시 해당 알람을 생성할 수 있습니다.
- 필요한 경우 알람 닫기를 취소할 수 있습니다.

SMC를 사용하여 알람을 닫으려면 다음 단계를 완료하십시오.

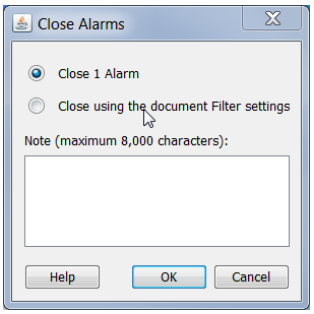
1. 비활성 알람이 표시되도록 Alarm Table(알람 테이블) 필터를 변경합니다. 이렇게 하려면 Alarm Table(알람 테이블) 필터 대화 상자의 States(상태) 페이지에서 **Filter on currently Active(현재 활성 상태인 알람 필터링)** 확인란을 클릭하여 체크 마크를 추가한 다음 **Inactive(비활성)** 옵션을 클릭합니다.
2. Alarm Table(알람 테이블)에서 알람을 마우스 오른쪽 버튼으로 클릭하고 **Workflow(워크플로) > Close Selection(선택 항목 닫기)**을 선택합니다.



또한 알람을 클릭한 다음 알람 테이블 툴바에서 **Close Selection(선택 항목 닫기)** 버튼을 클릭할 수 있습니다.



알람이 닫히는 이유를 설명하는 메모를 입력하도록 요청하는 Close Alarms(알람 닫기) 창이 열립니다.



3. 알람을 닫거나 문서 필터에서 설정을 사용하여 닫도록 지정합니다. 알람 닫기의 의미를 파악하려면 사용 가능한 옵션에 대한 다음 설명을 참조하십시오.

   - **Close [x] Alarms([x]개의 알람 닫기)** - 알람 테이블에 현재 표시되는 알람만 확인하고 닫습니다. 여기서 [x]는 알람 테이블에 표시된 알람의 총 수와 일치합니다. 이 옵션을 클릭하는 경우 시스템이 각 알람을 하나씩 확인하고 닫습니다. 따라서 많은 수의 알람이 있는 경우(예: 1000개 이상) 시스템에서 이 옵션을 사용하여 해당 프로세스를 완료하는 데 상당한 시간이 소요됩니다.
   - **Close using the document Filter settings(문서 필터 설정을 사용하여 닫기)** - 닫기 프로세스가 진행되는 동안 *발생할 수 있는 모든 새로운 알람을 포함하여* 알람을 하나씩 확인하고 닫는 대신 대량으로 현재 필터 설정에 포함된 모든 알람을 확인하고 닫습니다. 예를 들어, 알람 테이블 필터가 경미한 알람 유형만 표시하도록 설정된 경우, 이 설정에 기초하여 모든 알람을 닫도록 선택하는 것입니다. 시스템에서는 알람 테이블에 현재 표시되는 경미한 알람뿐만 아니라 닫기 프로세스가 진행되는 동안 생성되었을 수 있지만 표시되지 않은 경미한 알람도 닫습니다.

참고:

"Close using the document Filter settings(문서 필터 설정을 사용하여 닫기)" 옵션이 대량으로 알람을 닫기 때문에 특히, 1000개 이상의 알람이 있는 경우 다른 옵션보다 작업이 훨씬 더 신속하게 수행됩니다. 그러나 이 옵션을 선택하면 표시된 적이 없는 알람을 닫을 수 있다는 점을 인지해야 합니다.

4. 텍스트 입력 필드를 클릭하고 알람을 닫는 이유에 관한 설명을 입력한 다음 **OK(확인)**를 클릭합니다. 체크 마크( )가 Closed(닫힘) 열에 나타나고, Last Note(마지막 메모) 열을 표시하도록 선택한 경우 이 열에 메모가 나타납니다.

참고:

Acknowledged(확인됨) 및/또는 Last Note(마지막 메모) 열을 확인하려면 열 헤더를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 해당하는 옵션을 선택합니다.

닫힌 알람 다시 열기

SMC를 사용하면 하나 이상의 닫힌 알람을 다시 열 수 있습니다. 예를 들어, 실수로 알람을 닫은 경우, 다음 단계를 완료해야 할 수 있습니다.

1. Alarm Table(알람 테이블)에 닫힌 알람 중에서 다시 열려는 알람을 표시합니다. 필요한 경우 알람 필터를 사용합니다.
2. 다시 열려는 알람을 마우스 오른쪽 버튼으로 클릭하고 **Workflow(워크플로) > Reopen Selection(선택 항목 다시 열기)**을 선택합니다.
3. 알람 메모를 입력한 다음 **OK(확인)**를 클릭합니다.
4. 확인할 각 알람에 대해 2단계와 3단계를 반복합니다.

STEALTHWATCH 완화 기능

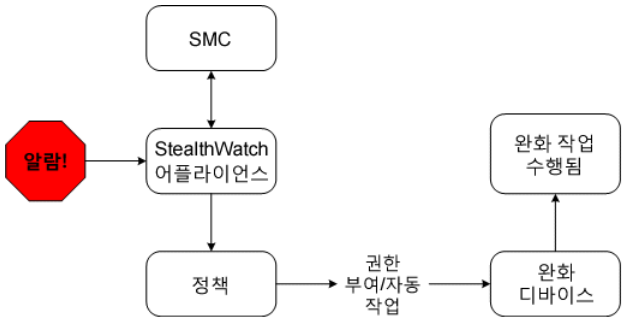
Stealthwatch 소프트웨어는 다양한 위협에 대한 시스템의 대응을 자동화하는 데 사용할 수 있는 위협 완화 기능을 제공합니다. 이 기능을 사용하여 특정 알람에 대응하는 방식과 관련한 의사 결정을 내리는 데 필요한 시간을 줄일 수 있습니다. 시스템은 알람이 발생하는 즉시 가능한 한 빨리 이 기능을 수행합니다.

Stealthwatch 완화 기능은 몇 초 이내에 문제를 해결하는 데 도움이 됩니다. 원하는 경우, 완화 기능을 즉시 수행하도록(자동 모드) 설정하거나 권한 부여를 먼저 요청하도록(권한 부여 또는 수동 모드) 설정할 수 있습니다.

Stealthwatch 완화 기능은 기본적으로 비활성화되어 있습니다. 이 기능을 활성화하려면 다음 단계를 완료해야 합니다. 이 단계에 대해서는 이 섹션의 후반부에 자세히 설명되어 있습니다.

1. 완화 기능(예: 방화벽 정의)을 사용하려는 각 어플라이언스에 대해 완화 디바이스를 구성합니다.
2. 완화 기능을 사용하려는 정책에 대해 완화 기능을 활성화합니다.
3. 개별 알람에 대해 원하는 완화 작업을 정의합니다.

다음 그림은 Stealthwatch 완화 기능이 작동하는 방법에 대한 일반적인 개요를 제공합니다.



이 기능을 활성화한 경우 지정된 알람이 발생하면 Stealthwatch System은 디바이스에 구성되어 있는 완화 작업을 수행하도록 요청하면서 완화 디바이스에 신호를 보냅니다. 디바이스는 해당 알람에 대해 지정한 정책 설정에 기초하여 요청된 작업을 수행합니다.

참고:

시스템에서는 브로드캐스트 리스트 또는 완화 화이트리스트에 있는 호스트를 대상으로 완화 작업을 수행하지 않습니다. 이 리스트에 대한 자세한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.

완화 디바이스 구성

Stealthwatch System 및 완화 디바이스 간의 통신을 설정하도록 SMC를 구성해야 합니다. 여러 어플라이언스에서 동일한 완화 디바이스를 사용하도록 하려면, 해당 디바이스에 대해 개별적으로 각 어플라이언스를 구성해야 합니다.

참고:

Stealthwatch 디바이스에서 정보를 수신하도록 완화 디바이스를 구성해야 할 수도 있습니다. 자세한 내용은 *완화 디바이스 환경 설정* 가이드를 참조하십시오. Stealthwatch 사용자 커뮤니티 웹 사이트(https://community.lancope.com)에서 이 문서를 확인할 수 있습니다.

다음과 같이 어플라이언스당 최대 5개의 완화 디바이스 유형을 구성할 수 있습니다.

- Brocade INM
- Cisco ASA
- Cisco Guard
- Cisco Router(Internetworking Operating System 11.3 이상)
- 맞춤형
- Radware DefensePro
- Stealthwatch SNMP 완화 인터페이스

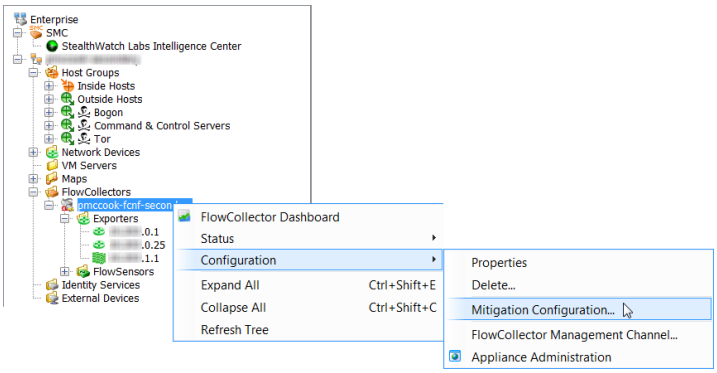
참고:

- 이 모든 완화 디바이스 유형(Radware DefensePro 제외)은 Stealthwatch 모듈에서만 사용할 수 있습니다. Radware DefensePro는 DDoS 모듈에서만 사용할 수 있습니다.
- 완화 작업을 맞춤화하기 위해 예상 스크립트를 사용하려는 경우 맞춤화 옵션을 선택하십시오. 그러나, 예상 스크립트를 사용하기 전에 Lancope 고객 지원팀에 문의하는 것이 좋습니다.

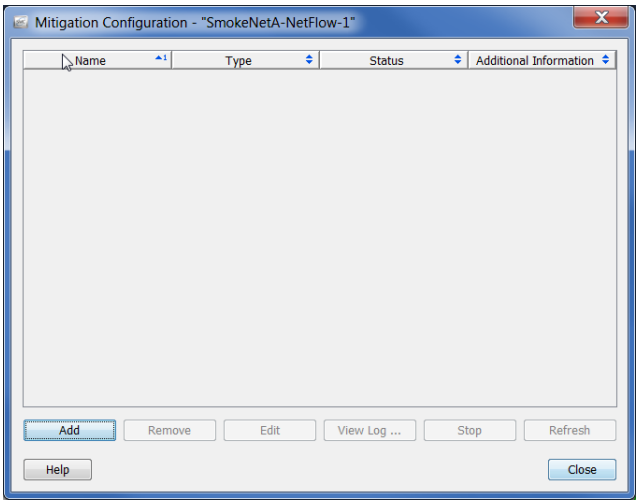
선택하는 완화 디바이스 유형에 따라 시스템에서 수행할 수 있는 완화 작업 유형이 결정됩니다. 예를 들어 특정 디바이스는 소스 IP 주소에서 오는 트래픽 차단만 지원할 수 있습니다.

SMC에서 완화 디바이스를 구성하려면 다음 단계를 수행하십시오.

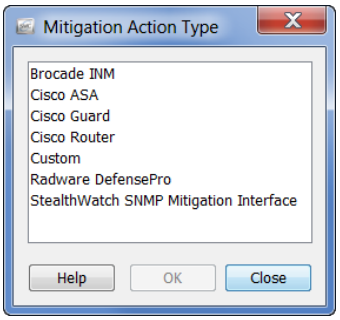
1. 어플라이언스 이름을 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > Mitigation Configuration(완화 컨피그레이션)**을 선택합니다.



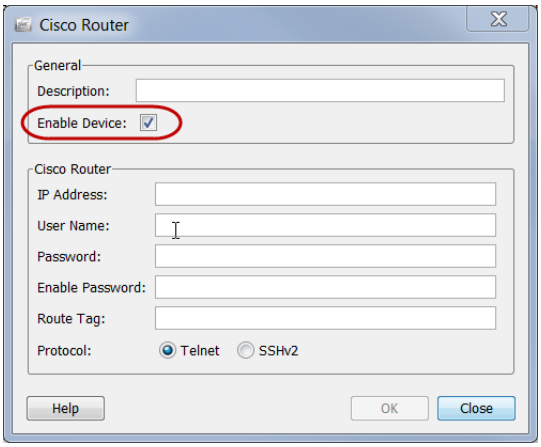
Mitigation Configuration(완화 컨피그레이션) 대화 상자가 열립니다.



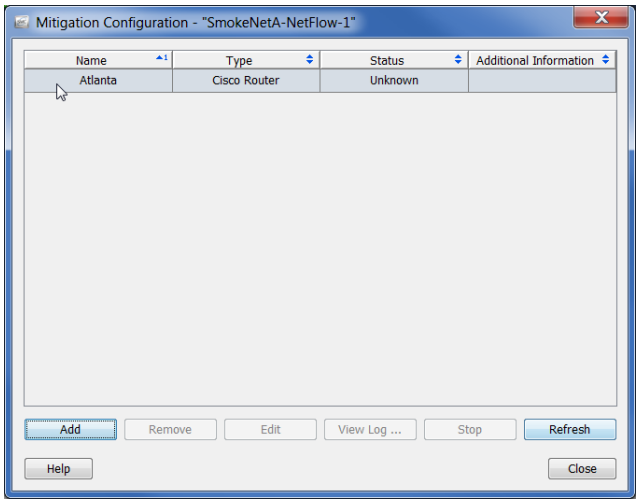
2. **Add(추가)**를 클릭합니다. Mitigation Action Type(완화 작업 유형) 대화 상자가 열립니다.



3. 사용하려는 완화 디바이스 유형을 클릭한 다음 **OK(확인)**를 클릭합니다. 선택한 디바이스 유형에 대해 디바이스 정보 대화 상자가 열립니다. 예를 들어, **Cisco Router(Cisco 라우터)**를 클릭하면 Cisco 라우터 정보 대화 상자가 열립니다.



4. 이전 예에서와 같이 **Enable Device(디바이스 활성화)** 확인란에 체크 마크가 있는지 확인합니다. 이 확인란을 선택하지 않으면 디바이스가 Stealthwatch System에서 정보를 수신하지 않으며 완화 기능이 작동하지 않습니다.
5. 선택된 디바이스에 대한 특정한 식별 정보를 모두 입력한 다음 **OK(확인)**를 클릭합니다. 디바이스 정보 대화 상자가 닫히고 추가한 디바이스가 이제 Mitigation Configuration(완화 컨피그레이션) 대화 상자에 포함됩니다.



6. 이 어플라이언스를 대상으로 추가해야 하는 완화 디바이스를 모두 추가할 때까지 2~5단계를 반복합니다.
7. 작업이 완료되면 **Close(닫기)**를 클릭하여 Mitigation Configuration(완화 컨피그레이션) 대화 상자를 닫습니다.

이제 다음 섹션에 설명된 호스트 그룹별 완화 기능 활성화를 수행할 수 있습니다.

참고:

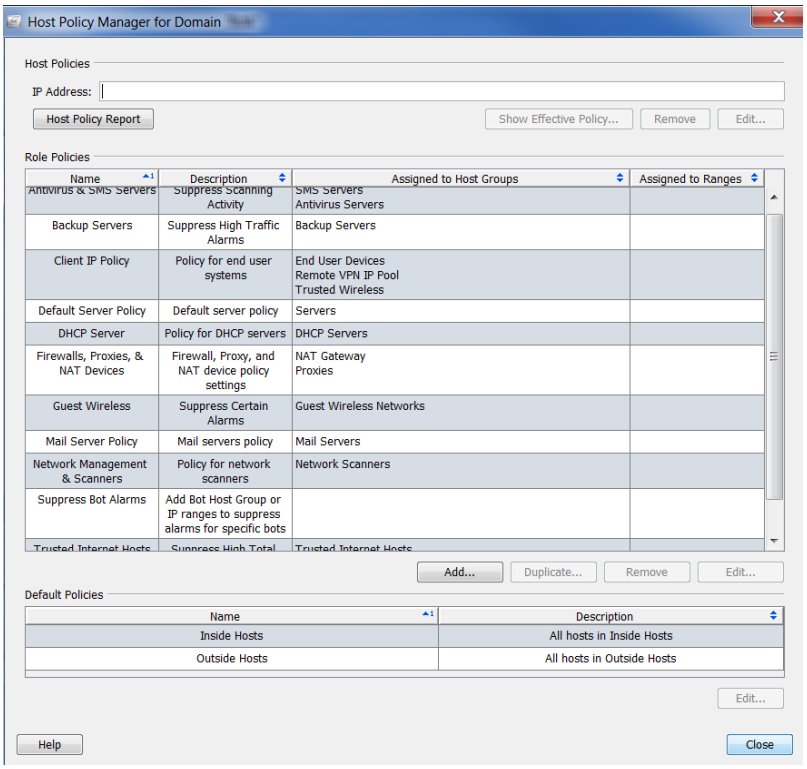
완화 기능이 작동하려면 완화 디바이스가 실행되어야 합니다.

정책에 대한 완화 기능 활성화

완화 디바이스를 구성한 경우 하나 이상의 호스트 그룹에 할당 가능한 특정 정책에 대해 Stealthwatch 완화 기능을 활성화할 수 있습니다. 예를 들어 내부 호스트 기본 정책에 대해 완화 기능을 활성화할 수 있습니다. 또한 몇 가지 호스트 그룹 또는 특정 호스트 IP 주소에서도 이 기능을 사용할 수 있습니다.

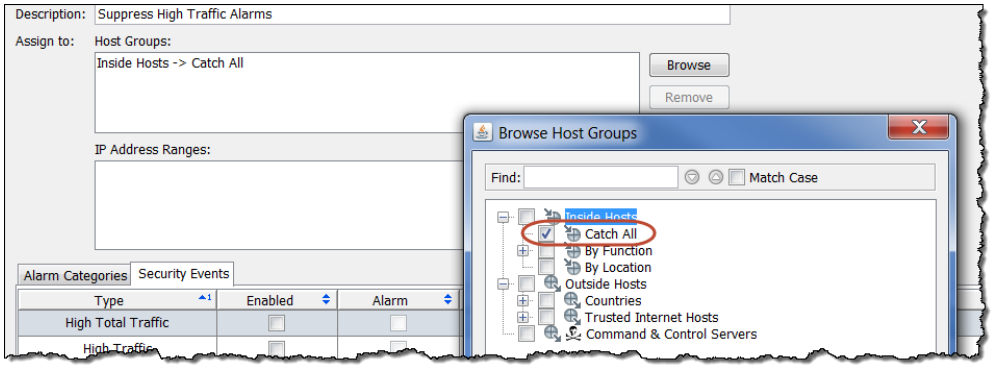
다음 예에서 특정 역할 정책에 대해 완화 기능을 활성화하는 상황을 가정해 보겠습니다. 이렇게 하려면 다음 단계를 수행하십시오.

1. 메인 메뉴에서 **Configuration(컨피그레이션) > Host Policy Manager(호스트 정책 관리자)**를 선택합니다. Host Policy Manager(호스트 정책 관리자) 대화 상자가 열립니다.

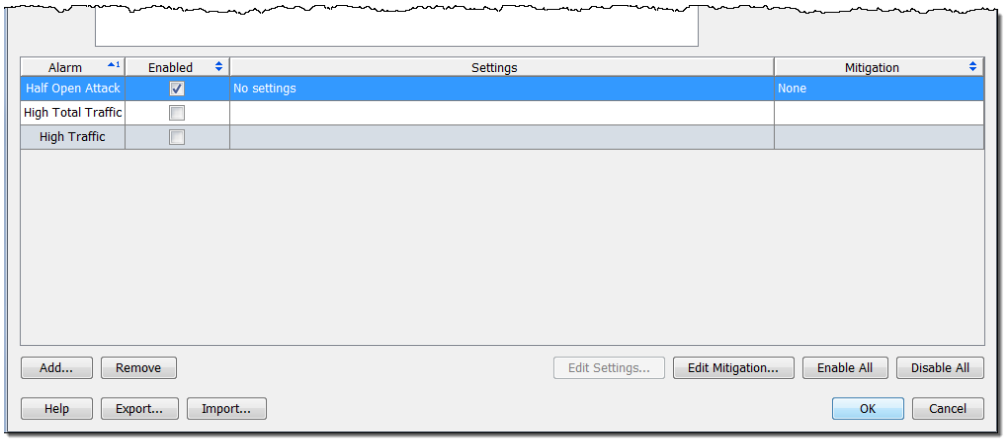


2. **Role Policies(역할 정책)** 섹션에서 원하는 역할 정책을 클릭한 다음 **Edit(편집)**을 클릭합니다. Edit Role Policy(역할 정책 편집) 대화 상자가 열립니다.

3. **Assign to: Host Groups:(할당 대상: 호스트 그룹)** 섹션에서 **Browse(찾아보기)**를 클릭하여 정책이 적용되는 호스트 그룹을 선택한 다음 **OK(확인)**를 클릭하여 Edit Role Policy(역할 정책 편집) 대화 상자로 돌아갑니다. (또한 IP Address Ranges(IP 주소 범위) 필드에서 특정 호스트 IP 주소 또는 범위를 지정할 수 있습니다.)



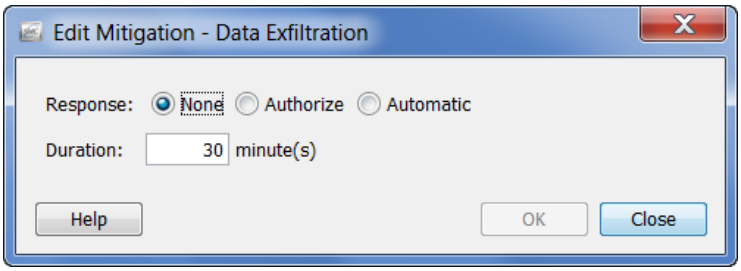
4. Edit Role Policy(역할 정책 편집) 대화 상자에서 확인란을 클릭하여 완화 기능을 활성화하려는 각 알람의 Enabled(활성화됨) 열에서 체크 마크를 추가합니다. (원하는 알람이 나열되지 않은 경우 추가하려면 **Add(추가)**를 클릭합니다.)



알람에 대한 완화 작업 정의

이제 원하는 개별 알람에 대해 완화 작업을 정의할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

1. 이전 섹션의 4단계에 이어서 지금 열려 있는 Edit Role Policy(역할 정책 편집) 대화 상자에서 완화 기능을 활성화하려는 알람을 포함하는 열을 선택한 다음 **Edit Mitigation(완화 편집)**을 클릭합니다. Edit Mitigation(완화 편집) 대화 상자가 열립니다(내용은 알람에 따라 다를 수 있음).



참고:

Lancope는 각 완화 작업에 대해 권장되는 기본 설정을 제공합니다. 원하는 경우 네트워크 요구 사항에 맞게 설정을 변경할 수 있습니다.

2. 다음 설명에 따라 팝업 메뉴에서 원하는 완화 대응을 클릭합니다.

대응	설명
없음	알람에 대한 모든 완화 작업을 비활성화하려면 **None(없음)**을 클릭합니다.
권한 부여	알람이 발생했을 때 시스템에서 선택한 완화 작업을 수행하기 전에 권한 부여를 요청하도록 하려면 **Authorize(권한 부여)**를 클릭합니다. 시스템에서 연결을 자동으로 차단하도록 허용하는 것보다는 수동으로 연결을 차단하도록 하려면 이 설정을 사용하십시오.
자동	알람이 발생했을 때 시스템에서 즉시 자동으로 선택한 완화 작업을 수행하도록 하려면 **Automatic(자동)**을 클릭합니다.

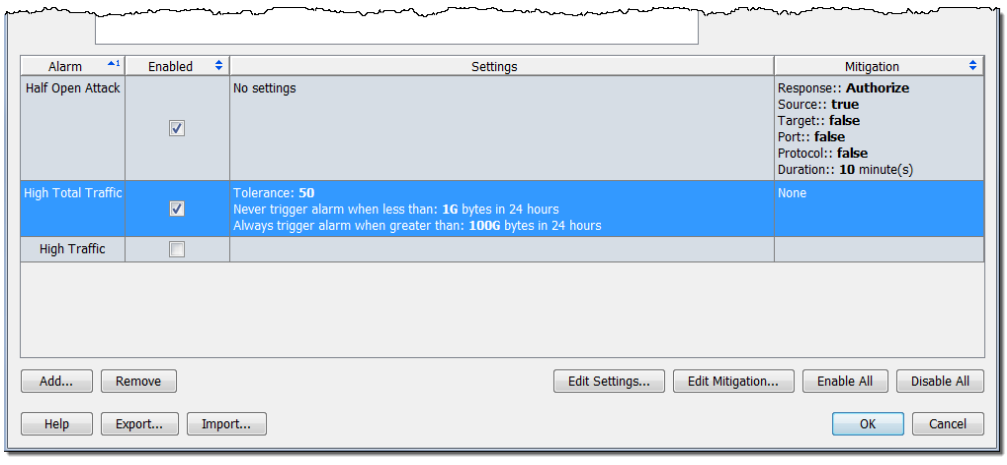
3. 다음 테이블에 표시된 대로 기타 완화 설정을 지정하십시오. 소스 또는 대상 IP 주소, 프로토콜 및/또는 포트 번호의 조합에 따라 각 알람에 대한 완화 작업을 맞춤화할 수 있습니다. 완화 작업이 실행되는 기간도 지정할 수 있습니다.

완화 옵션	목적
Source(소스)	의심스러운 활동을 유발한 호스트에서 들어오는 트래픽을 차단합니다.
Target(대상)	의심스러운 활동의 대상인 호스트로 이동하는 트래픽을 차단합니다.
Port(포트)	의심스러운 트래픽이 이동하는 수단이 되는 인터페이스를 차단합니다.
Protocol(프로토콜)	의심스러운 트래픽을 전송하는 데 사용되는 프로토콜을 차단합니다.
Duration(소요 시간)	차단 작업을 적용할 시간(분)입니다. 이 기간이 만료되면 완화 프로세스가 종료됩니다. **참고:** 소요 시간이 0인 경우 무한을 나타냅니다. 즉, 완화 프로세스가 수동으로 종료될 때까지 완화 작업이 적용됩니다.

참고:

- Cisco 라우터는 포트 또는 프로토콜 완화 작업을 지원하지 않습니다.
- OPSEC 디바이스의 경우 소스와 대상 완화 작업을 모두 활성화해야 합니다. 그렇지 않으면, 이 디바이스는 연결을 차단할 수 없습니다.

4. 알람에 대한 완화 설정을 지정한 경우, **OK(확인)**를 클릭합니다. 설정은 Edit Role Policy(역할 정책 편집) 대화 상자에 표시됩니다.



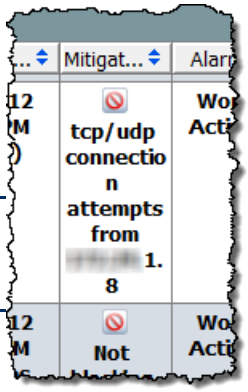
5. 완화 설정을 구성할 각 알람에서 1~4단계를 반복합니다.
6. 작업이 완료되면 **OK(확인)**를 클릭한 다음 **Close(닫기)**를 클릭하여 Host Policy Manager(호스트 정책 관리자)를 닫습니다.

완화 및 알람 테이블

완화 조치를 Authorize(권한 부여) 또는 Automatic(자동) 모드에서 활성화했는지에 따라 해당 알람이 발생하면 Alarm Table(알람 테이블)은 차단 작업이 수행되는지 여부를 표시합니다.

권한 부여(수동) 모드

Authorize(권한 부여) 모드로 완화 작업을 설정한 알람이 발생하면 Alarm Table(알람 테이블)의 Mitigation(완화) 열에 빨간색의 "Not Blocking(차단 안 함)" 아이콘이 표시됩니다.



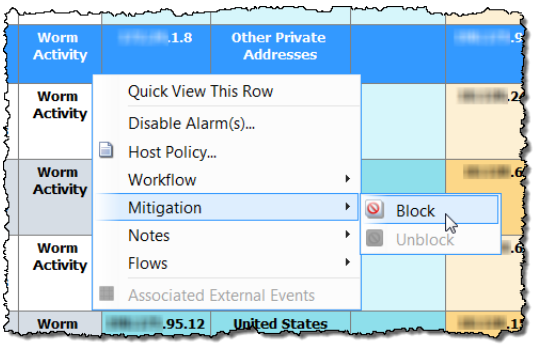
참고:

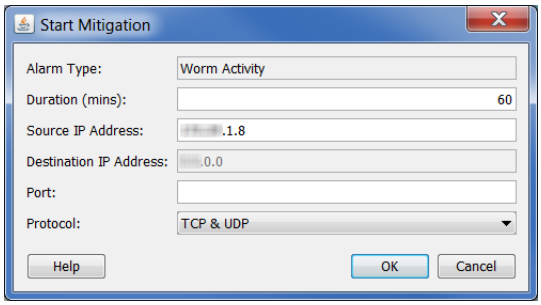
Mitigation(완화) 열을 표시하려면 열 헤더를 마우스 오른쪽 버튼으로 클릭하고 **Mitigation(완화)**을 선택합니다.

완화 작업이 Authorize(권한 부여) 모드인 경우 Alarm Table(알람 테이블)에서 특정 알람을 대상으로 한 완화 작업을 수동으로 수행하려면 다음 단계를 수행하십시오.

1. 알람을 마우스 오른쪽 버튼으로 클릭하고 **Mitigation(완화) > Block(차단)**을 선택합니다.

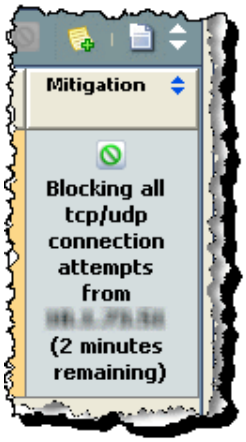
   Start Mitigation(완화 시작) 대화 상자가 열립니다.





2. 원하는 경우, 완화 작업 파라미터를 변경한 다음 **OK(확인)**를 클릭합니다. Start Mitigation(완화 시작) 대화 상자가 닫히고 Alarm Table(알람 테이블)이 새로 고쳐집니다.

3. 알람 조건을 찾습니다. 빨간색의 "Not Blocking(차단 안 함)" 아이콘이 이제 녹색의 "Blocking(차단)" 아이콘으로 바뀝니다.



참고:

완화 작업이 만료되기 전에 연결의 차단을 해제하려는 경우, 알람을 마우스 오른쪽 버튼으로 클릭하고 **Mitigation(완화) > Unblock(차단 해제)**을 선택하면 됩니다.

자동 모드

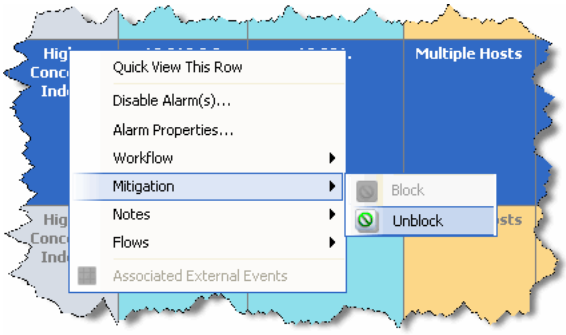
Automatic(자동) 모드로 완화 작업을 설정한 상태에서 알람이 발생하면 이전 예에서와 같이 Alarm Table(알람 테이블)의 Mitigation(완화) 열에 녹색의 "Blocking(차단)" 아이콘이 표시됩니다.

참고:

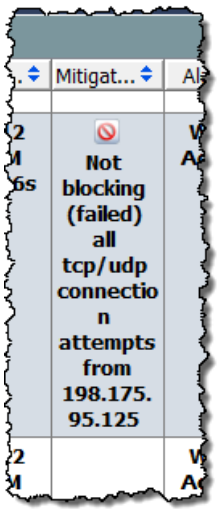
Mitigation(완화) 열을 표시하려면 열 헤더를 마우스 오른쪽 버튼으로 클릭하고 **Mitigation(완화)**을 선택합니다.

완화 작업이 Automatic(자동) 모드이므로 알람이 발생했을 때 아무 조치를 취할 필요가 없습니다. 그러나, 완화 작업을 중지하려는 경우 다음 단계를 수행하십시오.

1. Alarm Table(알람 테이블)에서 알람을 마우스 오른쪽 버튼으로 클릭하고 **Mitigation(완화) > Unblock(차단 해제)**을 선택합니다. 알람 테이블이 새로 고쳐집니다.

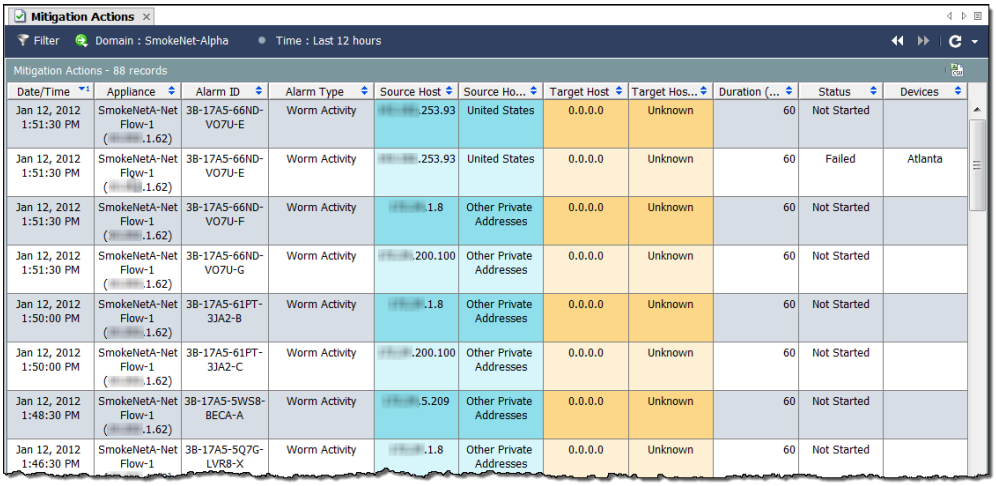


2. 문서를 다시 새로 고친 후 알람 조건을 다시 선택합니다. 녹색의 "Blocking(차단)" 아이콘이 이제 빨간색의 "Not Blocking(차단 안 함)" 아이콘으로 바뀝니다.



완화 작업 문서

Mitigation Actions(완화 작업) 문서를 사용하면 마지막 아카이브 시간 이후에 도메인에서 발생한 모든 완화 작업의 상태를 볼 수 있습니다. 완화 작업 문서에 액세스하려면 해당 도메인을 마우스 오른쪽 버튼으로 클릭한 다음 **Status(상태) > Mitigation Actions(완화 작업)**를 선택합니다. Mitigation(완화) 문서가 열립니다.



Date/Time	Appliance	Alarm ID	Alarm Type	Source Host	Source Ho...	Target Host	Target Hos...	Duration (...	Status	Devices
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-E	Worm Activity	.253.93	United States	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-E	Worm Activity	.253.93	United States	0.0.0.0	Unknown	60	Failed	Atlanta
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-F	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-G	Worm Activity	.200.100	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:50:00 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-61PT-3JA2-B	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:50:00 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-61PT-3JA2-C	Worm Activity	.200.100	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:48:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-5WS8-BECA-A	Worm Activity	5.209	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:46:30 PM	SmokeNetA-Net Flow-1	3B-17A5-5Q7G-LVR8-X	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	

12

불필요한 알람 줄이기

개요

특정한 정책 설정을 너무 낮게 설정했거나 문제가 없는 것으로 식별된 서비스 또는 애플리케이션이 실수로 특정 호스트 그룹을 대상으로 허용되지 않은 경우, 실제로는 행동이 정상이지만 의심스럽게 보이는 행동 때문에 알람이 발생할 수 있습니다. 이 장에서는 표시되는 불필요한 알람 수를 줄이는 방법에 대해 설명합니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 베이스라인 설정
- 호스트 정책 관리
- 정책 생성 및 편집
- 알람
- 권장사항

베이스라인 설정

베이스라인 설정은 네트워크에서 정상적인 행동으로 간주되는 항목의 프로파일을 구축하기 때문에 네트워크 모니터링에서 중요합니다. 이 설정을 통해 Stealthwatch가 비정상적인 행동을 관찰할 경우 알람을 트리거할 수 있습니다.

Stealthwatch는 네트워크에 설치되는 즉시 네트워크의 모든 호스트를 식별하기 시작합니다. 처음 7일 동안 Stealthwatch는 다음과 같은 약 90가지 특성에 기초하여 정상적인 행동으로 보이는 항목의 베이스라인을 설정합니다.

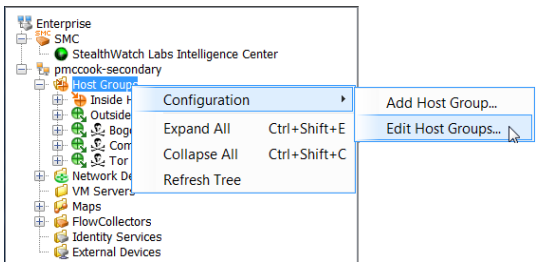
- 일반 대역폭 사용량
- 다른 호스트와의 통신
- 동시 플로우 수
- 초당 패킷(pps)

이 베이스라인은 하루 동안의 예상 행동을 나타냅니다. 베이스라인은 하루 동안에 사용할 임계값을 계산하기 위해 허용 수준과 함께 사용됩니다.

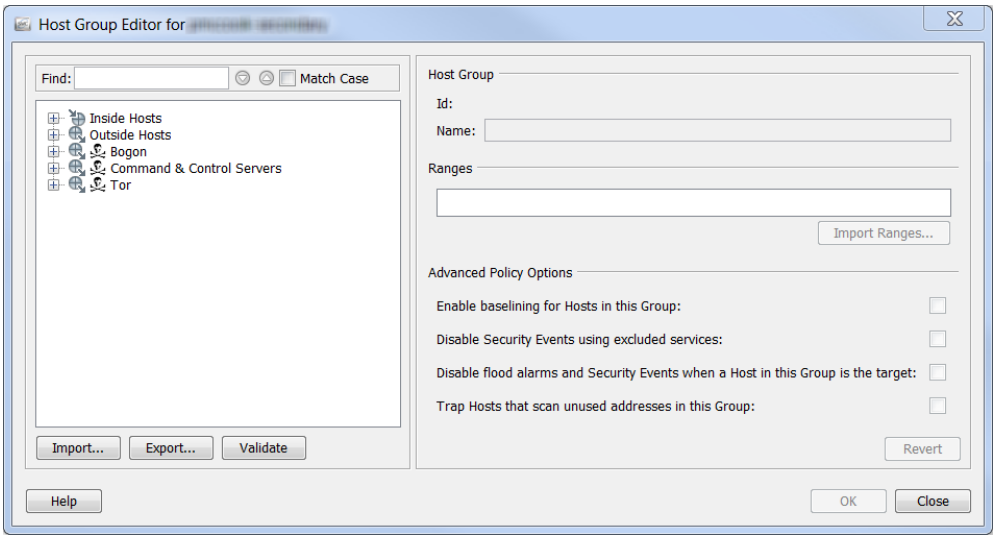
참고:

알람과 관련된 허용 수준의 개념에 대한 자세한 내용은 289페이지의 "알람"을 참조하십시오.

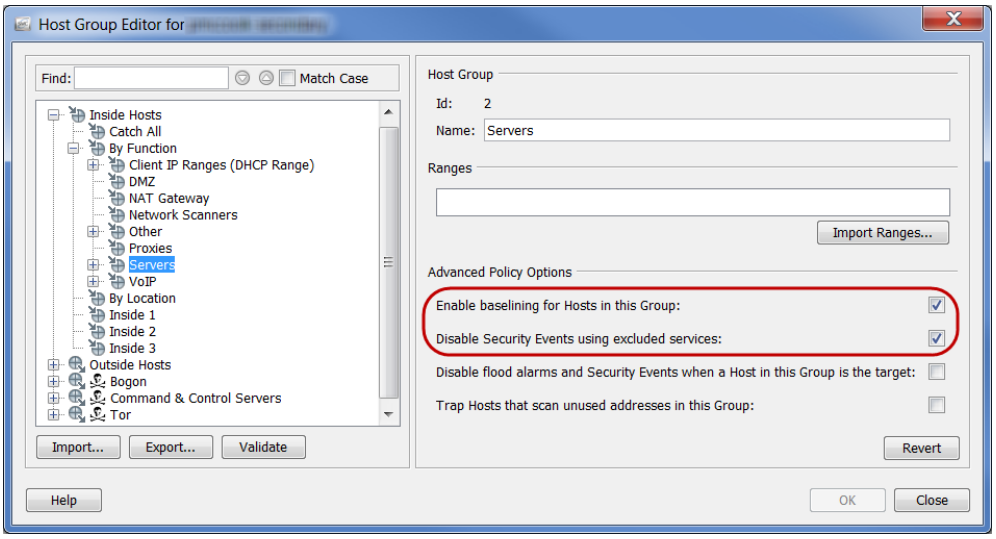
이러한 90가지 특성은 앞에서 언급한 호스트 프로파일의 일부가 됩니다. 기본적으로, Stealthwatch 베이스라인은 내부 호스트 그룹 내에 있는 모든 호스트를 대상으로 합니다. 그러나, 외부 호스트 호스트 그룹의 경우 Stealthwatch 베이스라인은 호스트 그룹 레벨에서 호스트 행동만 집계합니다. Host Group Editor(호스트 그룹 편집기) 대화 상자에서 언제든지 베이스라인 설정 방법을 변경할 수 있습니다.



이 대화 상자에 액세스하려면 엔터프라이즈 트리에서 **Host Group(호스트 그룹)**을 마우스 오른쪽 버튼으로 클릭한 다음 **Configuration(컨피그레이션) > Edit Host Groups(호스트 그룹 편집)**를 선택합니다.



대화 상자 왼쪽에 있는 엔터프라이즈 트리에서 베이스라인 설정 방법을 변경할 대상 호스트를 클릭합니다. Advanced Policy Options(고급 정책 옵션) 섹션에서 클릭한 호스트에 대한 현재 설정을 나타내도록 확인란의 체크 마크가 자동으로 채워집니다.



고유한 호스트 레벨 베이스라인은 **Enable baselining for Hosts in this Group(이 그룹에서 호스트에 대한 베이스라인 설정 활성화)** 확인란에 체크 마크가 있는 *경우에만* 호스트 그룹에 있는 각 호스트에 대해 설정됩니다. 그렇지 않으면 Stealthwatch 베이스라인은 호스트 그룹 레벨에서 호스트 행동을 집계합니다.

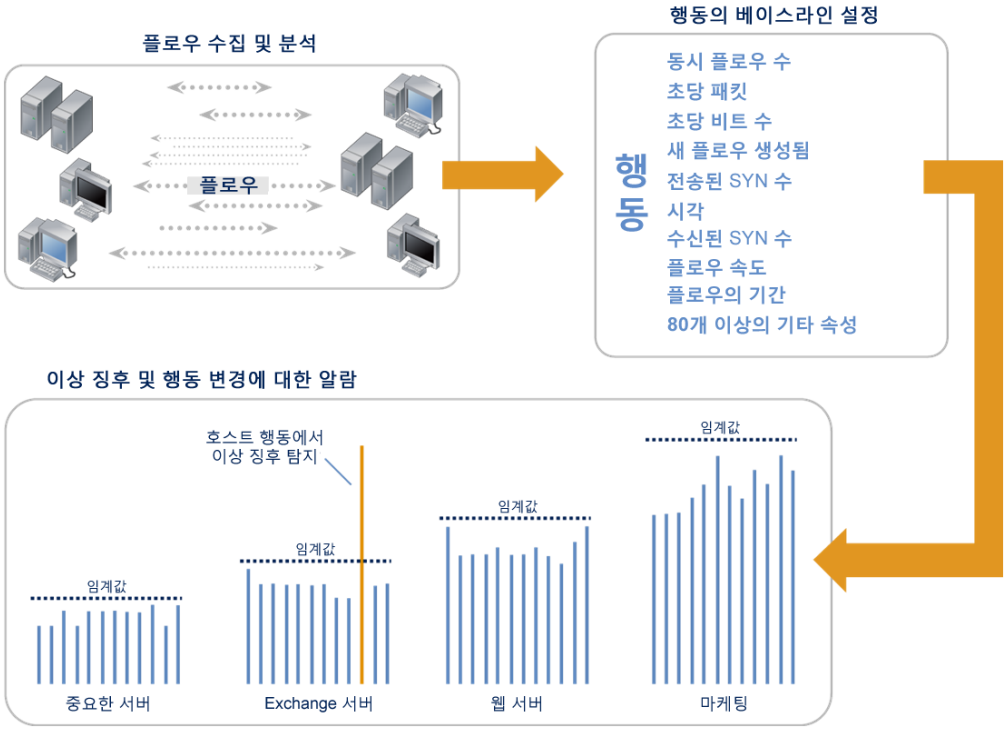
앞에서 설명한 대로 Stealthwatch 베이스라인은 기본적으로 내부 호스트 그룹 내에 있는 모든 호스트를 대상으로 합니다. 따라서 기본적으로 이 옵션은 내부 호스트에 대해 활성화됩니다(이전 예에서 동그라미로 표시된 영역 참조).

참고:

IP가 자주 변경되는 매우 동적인 환경(예: DHCP 범위)의 경우 이 기능을 비활성화할 수 있습니다. 비활성화할 경우, 이로 인해 모든 DHCP 호스트의 예상된 행동에 대한 베이스라인이 모든 DHCP 호스트처럼 행동하게 됩니다.

그러나, 기본적으로 Stealthwatch 베이스라인은 외부 호스트 그룹에 대해 호스트 그룹 레벨에서 호스트 행동만 집계합니다. 따라서 기본적으로 이 옵션은 외부 호스트에 대해 비활성화됩니다.

다음 다이어그램은 베이스라인 설정 프로세스를 보여줍니다.



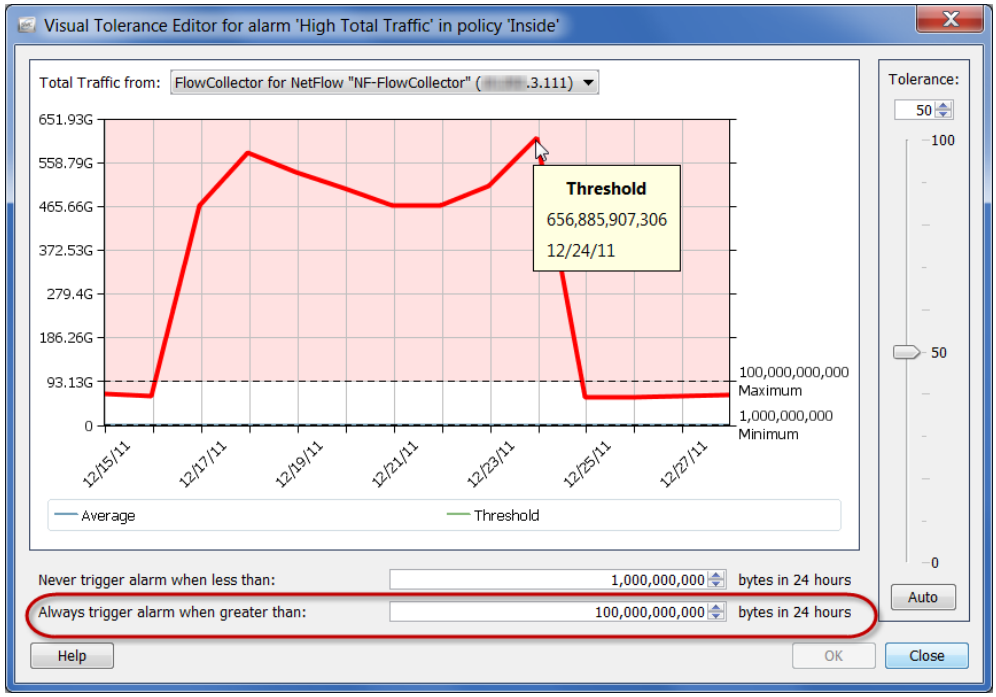
처음 7일이 지난 후 Stealthwatch는 규칙적인 단계로 이뤄진 28일 베이스라인을 생성하기 위해 14가지 주요 특성을 추적합니다. 이 베이스라인은 지난 28일 동안의 일일 특성 값의 평균으로, 마지막 7일에 높은 가중치가 적용됩니다. 베이스라인이 마지막 7일을 통합하므로 이것은 주간 값을 나타내는 데 사용됩니다. 따라서, 베이스라인은 이전 월의 값을 포함하지만 가장 최근 주에 높은 가중치가 적용됩니다.

참고:

이 14가지 주요 특성의 소스인 14가지 알람의 리스트를 보려면 289페이지의 "차이 기반 알람과 설정/해제 알람 비교"의 표를 참조하십시오.

Stealthwatch는 베이스라인을 설정할 때 다음 지침을 사용합니다.

- 호스트 베이스라인 설정의 경우 Stealthwatch는 활성화된 각 알람에 대해 표시되는 호스트의 일일 최대 값을 저장합니다(예: 높은 총 트래픽 알람).
- 호스트 그룹 베이스라인 설정의 경우 Stealthwatch는 그룹에 있는 모든 호스트에 대한 최대값의 평균을 저장합니다(예: 모든 호스트의 총 트래픽 최대값의 평균).
- 호스트에 일일 값이 없는 경우, 호스트는 자신이 소속되어 있으며 호스트의 수가 가장 적은 그룹의 베이스라인을 사용합니다. 예를 들어 호스트가 두 개의 그룹(10.201.0.0/16으로 정의된 그룹 A와 10.201.3.0/24로 정의된 그룹 B)에 속하는 경우, 베이스라인은 호스트의 수가 더 적은 그룹 B를 상속받습니다.
- 호스트 그룹 베이스라인이 0인 경우, 최대값이 사용됩니다(예: 24시간 기준으로 총 트래픽의 최대 바이트).
- 새로 설치하는 경우, 모든 호스트는 베이스라인이 설정될 때까지 첫 번째 날의 컨피그레이션 정책 최대값을 사용합니다. 호스트는 최대값을 초과하지 않으면 알람을 보내지 않습니다(다음 예에서 동그라미로 표시된 옵션 참조).



앞으로 Stealthwatch는 다음과 같은 행동에서의 변화를 찾아 강조 표시합니다.

- 하나의 호스트가 짧은 기간 동안에 많은 수의 다른 호스트와 접촉(예: 피어-투-피어 애플리케이션, 웜)
- 긴 플로우 기간(예: 은닉 채널, VPN)
- 무단 포트의 사용(예: 비인가 서버/애플리케이션)
- 대역폭 이상 징후(예: Warezserver, 서비스 거부)
- 무단 통신(예: 회계 서버와 통신하는 VPN 호스트)

Stealthwatch는 호스트가 Stealthwatch에서 "정상적인" 행동으로 베이스라인을 설정한 항목의 임계값을 초과할 때마다 알람을 트리거합니다. Stealthwatch는 행동이 발생할 때 호스트의 행동을 관찰하고 여러 독점 알고리즘을 사용하여 서명 기반 솔루션을 통해 자주 생성되는 알람과 같은 오탐 알람의 생성을 방지합니다.

호스트 정책 관리

로그인 권한에 따라 사용자는 정책을 사용하여 Stealthwatch에서 호스트 행동을 모니터링하고 이에 대응하는 방법을 제어할 수 있습니다. 정책에는 특정 행동이 관찰될 때 Stealthwatch가 반응하는 방식을 결정하는 설정이 포함되어 있습니다. Stealthwatch는 다음 세 가지 유형의 정책을 사용하며 이 정책은 필요 시 수정할 수 있습니다.

- *기본 정책* - 모든 내부 호스트 및 모든 외부 호스트와 관련이 있습니다.
- *역할 정책* - 일반적인 목적으로 사용되는 호스트 수집(IP 주소)과 관련이 있습니다(예: 웹 서버, 방화벽, 신뢰할 수 있는 인터넷 호스트 등).
- *호스트 정책* - 특정 IP 주소와 관련이 있습니다.

호스트 정책은 다른 모든 정책보다 우선적으로 적용됩니다. 따라서, 호스트 정책이 역할 정책보다 더 구체적이며 역할 정책은 기본 정책보다 구체적입니다. 호스트에 대한 가장 구체적인 정책 설정만 알람을 트리거합니다.

참고:

호스트는 둘 이상의 호스트 정책에 할당될 수 없습니다.

예를 들어, 알람이 역할 정책에 추가된 경우, 알람이 비활성화, 활성화 상태이든 알람 설정이 변경되었든 간에 기본 정책의 동일한 알람이 재정의됩니다.

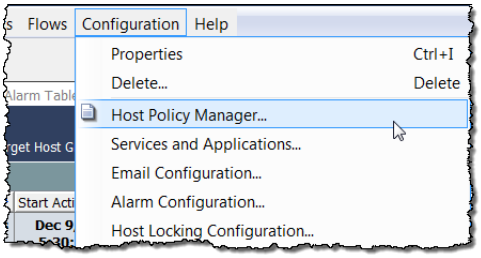
마찬가지로, 알람이 특정 호스트의 호스트 정책에 추가된 경우, 알람이 비활성화, 활성화 상태이든 알람 설정이 변경되었든 간에 해당 호스트에 적용될 수 있는 모든 역할 정책 또는 기본 정책의 동일한 알람이 재정의됩니다.

호스트가 호스트 정책에 할당되지 않았지만 두 개 이상의 역할 정책에 할당된 경우, Stealthwatch System은 각 알람에 대해 어떤 정책 설정이 호스트의 유효한 정책에서 사용되는지 결정합니다. 유효한 정책을 결정하는 방법에 대한 자세한 내용은 262페이지의 "유효한 호스트 정책"을 참조하십시오.

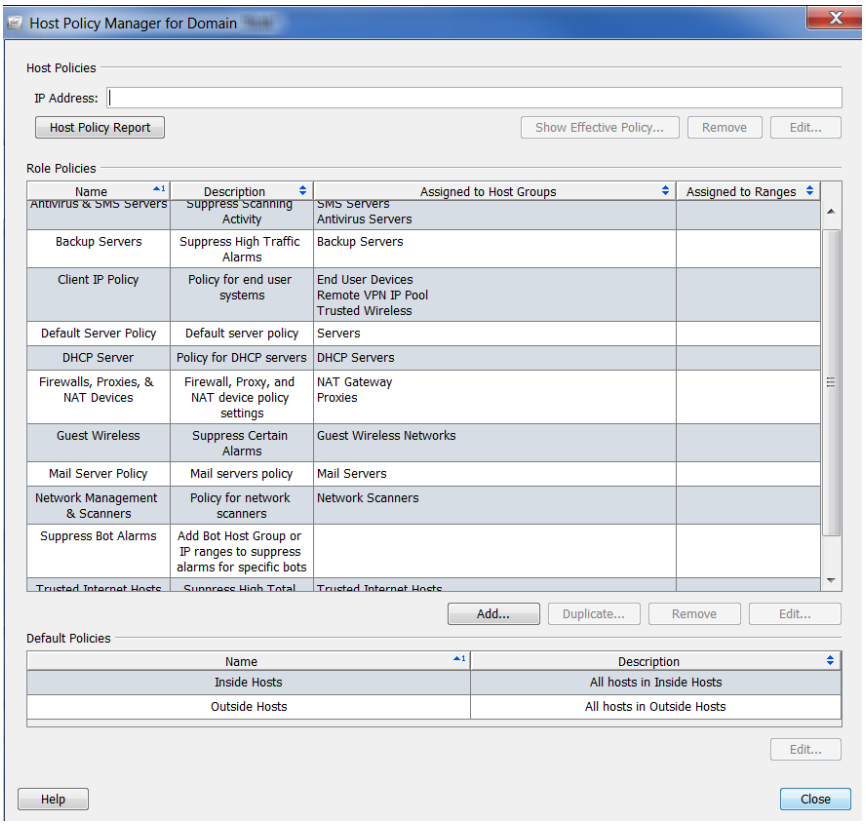
도메인, 호스트 그룹 또는 특정 호스트에 대해 허용되는 행동의 임계값을 변경하려면 적용할 호스트 그룹 또는 호스트의 수에 따라 적절한 유형의 정책을 생성하거나 편집해야 합니다.

Stealthwatch System에 있는 두 가지 기본 정책: 내부 호스트 기본 정책과 외부 호스트 기본 정책. 이러한 설정은 역할 정책 또는 호스트 정책을 생성하지 않은 경우 적용됩니다.

이러한 그룹 중 하나 또는 모두의 기본 정책을 편집해야 하는지 결정할 수 있습니다. 이렇게 하려면 호스트 정책 관리자에 액세스해야 합니다. 이 대화 상자에 액세스하려면 메인 메뉴에서 **Configuration(컨피그레이션) > Host Policy Manager(호스트 정책 관리자)**를 선택합니다.



Host Policy Manager(호스트 정책 관리자) 대화 상자가 열립니다.



이 대화 상자에서 다음 섹션을 사용하여 정책을 구성할 수 있습니다.

- 호스트 정책 - 단일 호스트에 대한 정책을 관리할 수 있습니다.
- 역할 정책 - 시스템에서 수행하는 역할에 따라 호스트에 대한 정책을 관리할 수 있습니다.
- 기본 정책 - 내부 호스트 또는 외부 호스트에 대한 기본 정책을 관리할 수 있습니다.

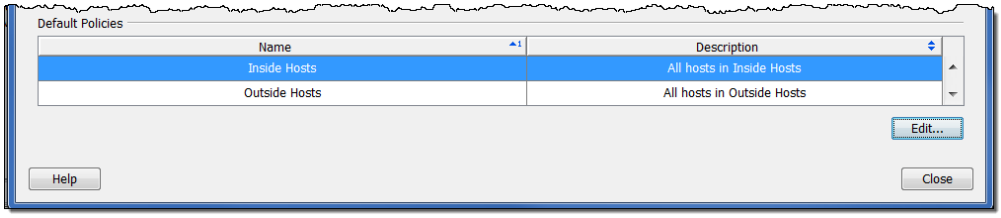
참고:

역할 정책 및 호스트 정책의 생성 및 편집에 대한 자세한 내용은 273페이지의 "정책 생성 및 편집"을 참조하십시오.

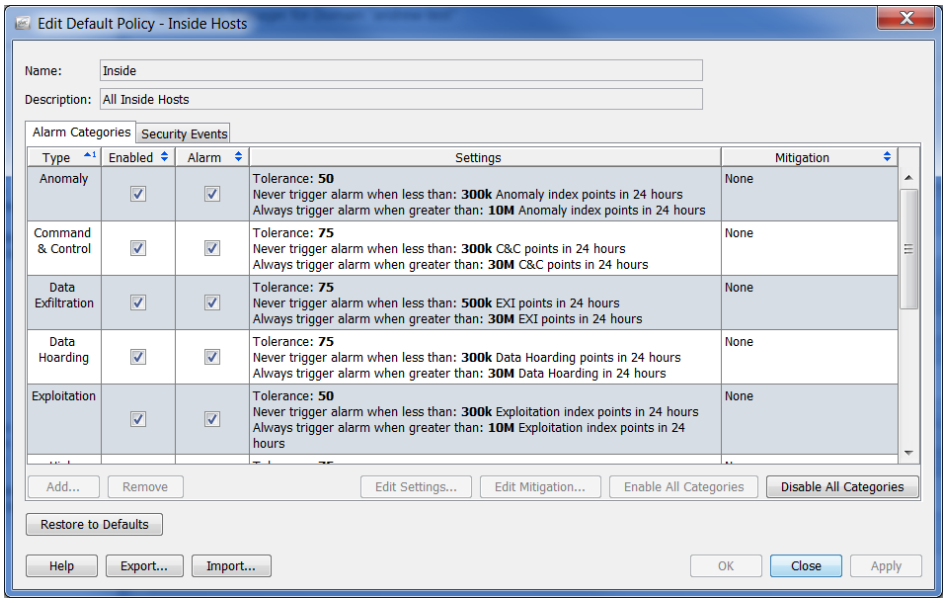
내부 호스트/외부 호스트의 기본 정책 편집

내부 호스트 기본 정책 또는 외부 호스트 기본 정책을 편집하려면 다음 단계를 수행하십시오.

1. 메인 메뉴에서 **Configuration(컨피그레이션) > Host Policy Manager(호스트 정책 관리자)**를 선택합니다. 이전 화면에서와 같이 Host Policy Manager(호스트 정책 관리자) 대화 상자가 열립니다.
2. **Default Polices(기본 정책)** 섹션에서 편집할 기본 정책의 호스트 이름을 선택한 다음 **Edit(편집)**을 클릭합니다.



Edit Default Policy(기본 정책 편집) 대화 상자가 열립니다.



주의:

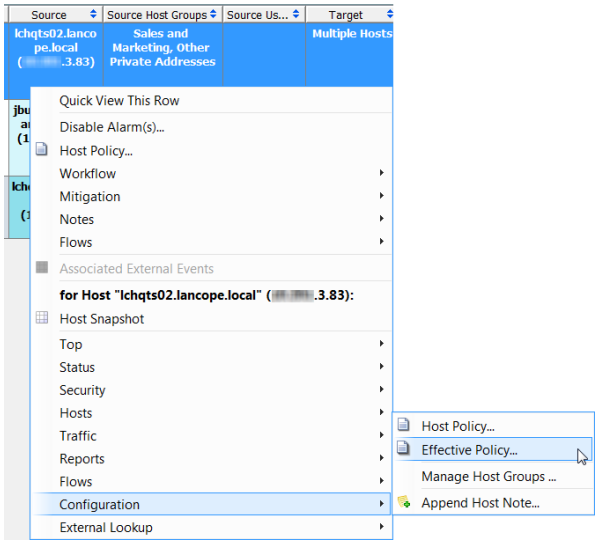
Restore to Defaults(기본값으로 복원)를 클릭하면 현재 정책이 공장 기본 정책 설정으로 재정의되므로 이 기능을 사용할 때는 특히 주의하십시오.

3. 알람 카테고리를 정책에 추가하고 이 알람 카테고리와 연결된 알람의 설정 또는 완화 기능을 편집하고 알람 카테고리를 활성화 또는 비활성화하려는 경우, 266페이지의 "호스트 정책에서 알람 카테고리 구성"으로 이동합니다.
4. 정책에서 사용되는 보안 이벤트를 구성하고 CI와 연결된 알람의 설정 또는 완화 기능을 편집하고 보안 이벤트를 활성화 또는 비활성화하려는 경우, 270페이지의 "호스트 정책에서 보안 이벤트 구성"으로 이동합니다.

유효한 호스트 정책

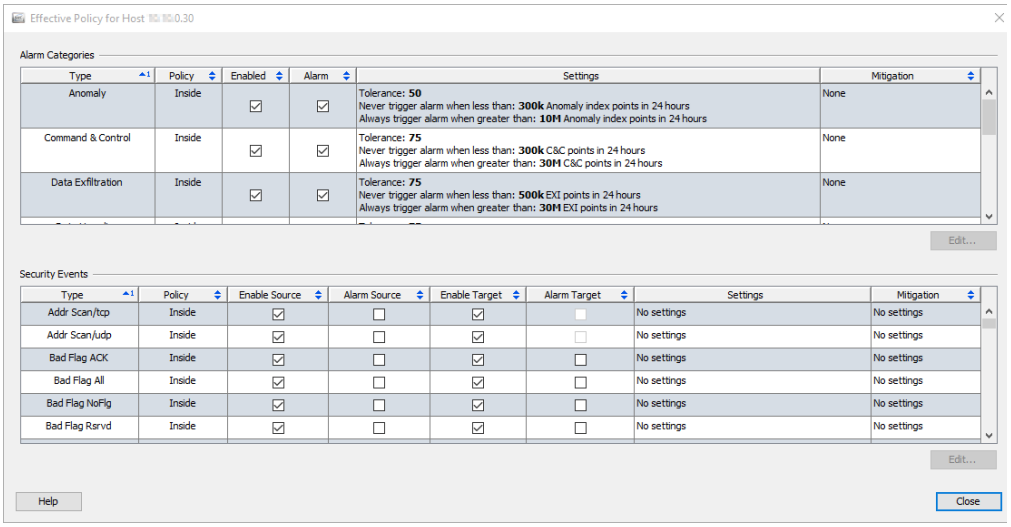
알람에 대응하는 경우 먼저 어떤 정책이 해당하는 특정 알람을 트리거했는지 판단해야 합니다. IP 주소를 볼 수 있는 경우, 이 IP 주소를 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > Effective Policy(유효한 정책)**를 선택합니다.

다음 예에 나와 있는 것처럼 Effective Host(유효한 호스트) 대화 상자가 열립니다.



팁:

알람 테이블에 있는 경우 제어 정책을 찾을 수 있는 빠른 방법은 헤더 내에서 마우스 오른쪽 버튼을 클릭하고 팝업 메뉴에서 **Policy(정책)**를 선택하여 Policy(정책) 열이 표시되도록 활성화하는 것입니다. 이 열을 확인하여 어떤 정책에 따라 알람이 제어되는지 판단할 수 있습니다. 이 시점에서 특정 정책에 대한 정책 설정을 참조하려면 **Policy(정책)** 열에서 정책 이름을 더블 클릭합니다.



이전 예에서와 같이 상위 파일 공유 지수 알람은 서버 역할 정책에 따라 제어되며 높은 트래픽 알람은 내부 호스트 정책에 따라 제어됩니다.

호스트가 호스트 정책에 할당되지 않았지만 두 개 이상의 다르게 구성된 역할 정책에 할당된 상황이 있을 수 있습니다. 이 경우, Stealthwatch System은 먼저 다음 4개의 열이 호스트가 할당된 역할 정책 중 하나에서 선택 취소되었는지 확인합니다.

- 소스 활성화
- 알람 소스
- 대상 활성화
- 알람 대상

이전 글머리 기호 리스트에서 명명된 4개의 열 중 하나만 정책 중 하나에서 선택 취소된 경우에도 해당 열이 유효한 정책에서 선택 취소됩니다. 즉, 선택이 취소된 모든 열("false" 설정과 동일)은 호스트가 할당된 기타 역할 정책에서 동일한 열을 재정의합니다. 해당 열이 선택된 경우("true" 설정과 동일) 즉, False 설정이 true 설정을 재정의합니다.

할당된 모든 역할 정책에서 선택된 모든 열이 유효한 정책에서 선택된 상태로 유지됩니다.

예 1

역할 정책 1의 상태			
소스 활성화	알람 소스	대상 활성화	알람 대상
True	True	False	False
역할 정책 2의 상태역할 정책 1의 상태			
소스 활성화	알람 소스	대상 활성화	알람 대상
False	False	True	True
유효한 정책의 상태유효한 정책의 상태			
소스 활성화	알람 소스	대상 활성화	알람 대상
False	False	False	False

예 2

역할 정책 1의 상태			
소스 활성화	알람 소스	대상 활성화	알람 대상
True	True	True	False
역할 정책 2의 상태역할 정책 1의 상태			
소스 활성화	알람 소스	대상 활성화	알람 대상
True	False	True	True
유효한 정책의 상태유효한 정책의 상태			
소스 활성화	알람 소스	대상 활성화	알람 대상
True	False	True	False

호스트에 대한 유효한 정책은 Policy(정책) 열에 유효한 모든 정책의 이름을 표시합니다. 보안 이벤트에 대해 소스 정책 및 대상 정책이 모두 있는 경우, Policy(정책) 열은 소스 정책을 먼저 나열한 다음 대상 정책을 두 번째로 나열합니다.

참고:

알람에 대응하는 방법에 대한 다음 단계에 대해서는 273페이지의 "정책 생성 및 편집"을 참조하십시오.

알람 카테고리

이 섹션을 사용하여 이 역할 정책과 함께 사용되는 알람 카테고리를 구성하십시오. 카테고리는 특정 유형의 보안 이벤트를 그룹화하는 방법을 제공합니다. 각 알람 카테고리는 발생하는 이벤트 수와 유형에 따라 알람을 생성할 수 있습니다.

다음을 수행할 수 있습니다.

- 알람 카테고리 설정 추가 또는 편집
- 알람 카테고리와 관련된 알람의 완화 기능 편집
- 알람 카테고리 활성화 또는 비활성화

다음 유형의 알람 카테고리를 사용할 수 있습니다.

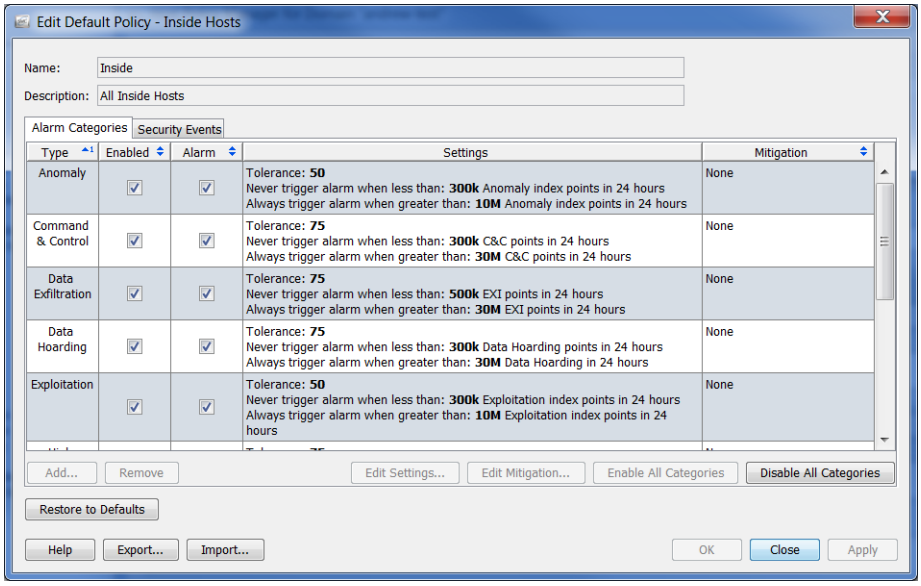
항목	설명
이상 징후	호스트가 비정상으로 동작하고 있거나 비정상적인 트래픽을 생성하고 있음을 나타내지만 다른 활동 카테고리와 일치하지 않는 이벤트를 추적합니다.
C&C(Command & Control)	네트워크 내에서 C&C 서버와의 접속을 시도하는 봇에 감염된 서버 또는 호스트의 유무를 나타냅니다.
데이터 유출	비정상적인 양의 데이터가 전송된 내부 및 외부 호스트를 추적합니다. 호스트가 구성된 임계값을 초과하는 이러한 이벤트를 다수 트리거할 경우 상위 유출 알람이 발효됩니다.
데이터 호딩	네트워크의 소스나 대상 호스트가 하나 이상의 호스트에서 비정상적인 양의 데이터를 다운로드했습니다.
공격	웜 전파, 무차별 대입 비밀번호 크래킹 등 호스트 간의 직접적인 보안 침해 시도를 추적합니다.
상위 관심 지표(CI)	관심 지표(CI)가 CI 임계값을 초과했거나 빠르게 증가한 호스트를 추적합니다. 상위 관심 지표(CI) 및 상위 대상 지표(TI) 카테고리는 동일한 이벤트를 사용합니다. 이벤트가 소스 호스트에서 트리거된 경우, 상위 CI 카테고리 알람이 발생합니다. 이벤트가 대상 호스트에서 트리거된 경우, 상위 TI 알람이 발생합니다.
상위 DDoS 소스 지표	호스트가 DDoS 공격의 소스로 식별되었음을 나타냅니다.
상위 DDoS 대상 지표	호스트가 DDoS 공격의 대상으로 식별되었음을 나타냅니다.

항목	설명
상위 대상 지표(TI)	허용 가능한 수보다 많은 스캔 또는 기타 악의적인 공격을 받은 내부 호스트를 추적합니다. 상위 관심 지표(CI) 및 상위 대상 지표(TI) 카테고리는 동일한 이벤트를 사용합니다. 이벤트가 소스 호스트에서 트리거된 경우, 상위 CI 카테고리 알람이 발생합니다. 이벤트가 대상 호스트에서 트리거된 경우, 상위 TI 알람이 발생합니다.
정책 위반	정상적인 네트워크 정책을 위반하는 행동이 주체에 표시됩니다.
정찰	TCP 또는 UDP를 사용 중이며 조직의 호스트에 대해 실행 중인 악성일 수 있는 무단 스캔 유무를 나타냅니다. "정찰"이라고 부르는 이러한 스캔은 네트워크에 대한 공격을 예고하는 초기 지표이며, 스캔의 출처가 조직의 외부 또는 내부일 수 있습니다.

호스트 정책에서 알람 카테고리 구성

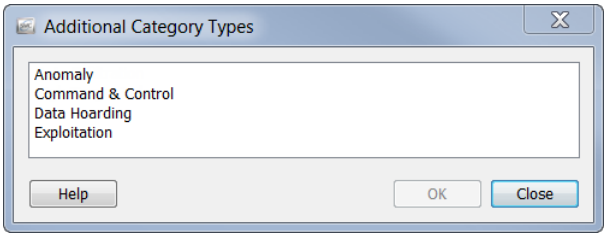
알람 카테고리를 구성하려면 다음 단계를 수행하십시오.

1. Edit Policy(정책 편집) 대화 상자에서 **Alarm Categories(알람 카테고리)** 탭을 클릭합니다.



2. 다음 중 하나를 수행합니다.
   - 알람 카테고리를 추가해야 하는 경우 3단계로 이동합니다.
   - 알람 카테고리를 편집해야 하는 경우 5단계로 이동합니다.

3. 알람 카테고리를 추가하려면 **Add(추가)**를 클릭합니다. Alarm Categories(알람 카테고리) 대화 상자가 열립니다.

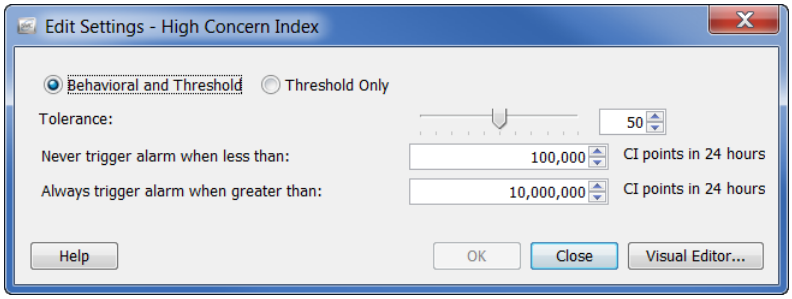


4. 하나 이상의 알람 카테고리를 선택하고 **OK(확인)**를 클릭합니다.

   Edit Policy(정책 편집) 대화 상자로 돌아갑니다.

5. 알람 카테고리에 대한 임계값 설정, 행동 또는 허용 수준을 편집하려면 편집할 알람 카테고리를 선택합니다.

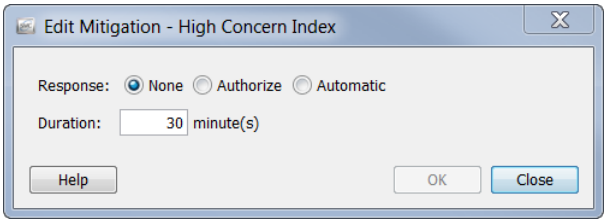
6. **Edit Settings(설정 편집)**를 클릭합니다. Edit Settings(설정 편집) 대화 상자가 열립니다.



7. 필요에 따라 설정을 변경하고 작업을 완료하면 **OK(확인)**를 클릭합니다. Edit Policy(정책 편집) 대화 상자로 돌아갑니다.

8. 완화 발생 시기 및 방법을 지정하려면 편집할 알람 카테고리를 선택합니다.

9. **Edit Mitigation(완화 편집)**을 클릭합니다. Edit Mitigation(완화 편집) 대화 상자가 열립니다.



10. 필요에 따라 설정을 변경하고 작업을 완료하면 **OK(확인)**를 클릭합니다. Edit Policy(정책 편집) 대화 상자로 돌아갑니다.

참고:

- 설정이 알람 카테고리에 대해 구성되어 있지 않은 경우, Settings(설정) 열에 *No Settings(설정 없음)*가 나타납니다.
- 완화 설정이 알람 카테고리에 대해 구성되어 있지 않은 경우, Mitigation(완화) 열에 *None(없음)*이 나타납니다.

11. 알람 카테고리를 활성화하려면 Enabled(활성화됨) 열에서 알람 카테고리 확인란을 선택합니다.

팁:

한 번에 모든 알람 카테고리에 적용하려면 Enable All Categories(모든 카테고리 활성화) 또는 Disable All Categories(모든 카테고리 비활성화) 버튼을 사용하십시오.

12. 보안 이벤트에 대한 알람을 발효하려면 Alarm(알람) 열에 있는 확인란을 선택합니다.
13. 다음 중 하나를 수행합니다.
    - Edit Policy(정책 편집) 대화 상자를 종료하지 않고 설정을 적용하려면 **Apply(적용) > Close(닫기)**를 클릭합니다.
    - 설정을 적용하고 Edit Policy(정책 편집) 대화 상자를 종료하려면 **OK(확인)**를 클릭합니다.

참고:

- 다양한 유형의 알람 설정에 대한 자세한 내용은 289페이지의 "알람"을 참조하십시오.
- 특정 알람의 권장 설정에 대한 내용은 295페이지의 "권장사항"을 참조하십시오.

보안 이벤트

이 섹션을 사용하여 정책에서 사용되는 보안 이벤트를 구성하고 CI와 연결된 알람의 설정 또는 완화 기능을 편집하고 보안 이벤트를 활성화 또는 비활성화 하십시오. Security Events(보안 이벤트) 탭의 확인란에 대한 설명은 다음 표를 참조하십시오.

이 확인란 선택...	다음 작업 수행...
소스 정책에 적용	호스트 정책 또는 역할 정책이 기존의 유효한 정책에 정의되어 있는 소스 설정을 대체하도록 지정하려는 경우입니다. **참고:** 이 열은 호스트 정책 또는 역할 정책을 편집하는 경우에만 적용할 수 있습니다.
소스 활성화	소스에 대해 활성화된 보안 이벤트가 해당하는 모든 알람 카테고리의 포인트에 영향을 주도록 지정하려는 경우입니다.
알람 소스	소스에 대해 활성화된 보안 이벤트가 연결된 알람을 트리거하도록 지정하려는 경우입니다.
소스 대상에 적용	호스트 정책 또는 역할 정책이 기존의 유효한 정책에 정의되어 있는 소스 설정을 대체하도록 지정하려는 경우입니다. **참고:** 이 열은 호스트 정책 또는 역할 정책을 편집하는 경우에만 적용할 수 있습니다.
대상 활성화	대상에 대해 활성화된 보안 이벤트가 해당하는 모든 알람 카테고리의 포인트에 영향을 주도록 지정하려는 경우입니다.
알람 대상	대상에 대해 활성화된 보안 이벤트가 연결된 알람을 트리거하도록 지정하려는 경우입니다.

특정 유형의 보안 이벤트가 알람을 생성하지 않는 상황에 대해서는 다음 내용을 참조하십시오.

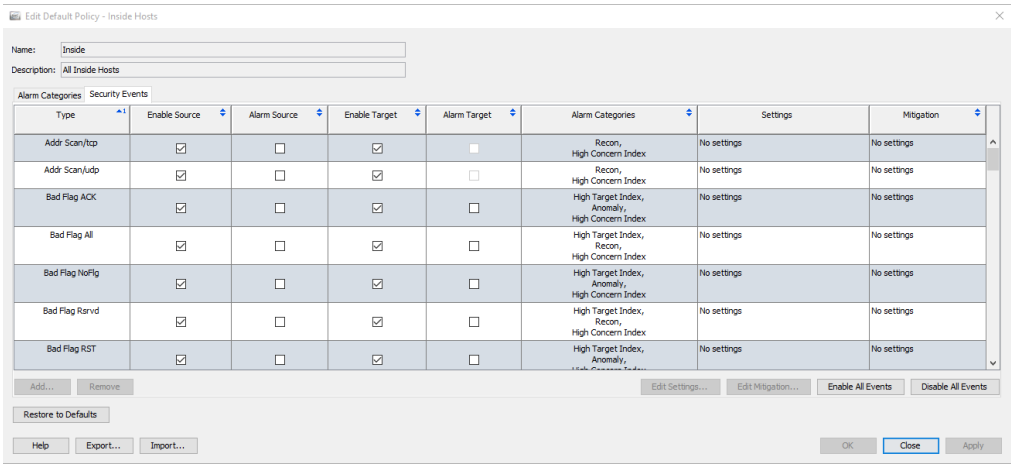
- 일대다(예: 최대 플로우 시작됨) - 이 유형의 보안 이벤트는 대상에서 알람을 생성할 수 없으므로 이 보안 이벤트에 대해 Alarm Target(알람 대상) 확인란을 선택할 수 없습니다.
- 다대일(예: SYN 수신됨) - 이 유형의 보안 이벤트는 소스에서 알람을 생성할 수 없으므로 이 보안 이벤트에 대해 Alarm Source(알람 소스) 확인란을 선택할 수 없습니다.

마우스 오른쪽 버튼을 클릭하고 Disable Alarm(알람 비활성화)을 선택하여 Alarm Table(알람 테이블)에서 알람을 비활성화할 수 있습니다. 이렇게 하면 해당하는 보안 이벤트에 대한 Alarm Source(알람 소스) 및 Alarm Target(알람 대상) 확인란의 선택이 취소됩니다. Enable Source(소스 활성화) 및 Enable Target(대상 활성화) 확인란은 선택된 상태로 유지됩니다. 그 결과 Enable Source(소스 활성화) 및 Enable Target(대상 활성화) 열은 선택된 상태로, Alarm Source(알람 소스) 및 Alarm Target(알람 대상) 열은 선택 취소된 상태로 새 호스트 정책이 생성됩니다.

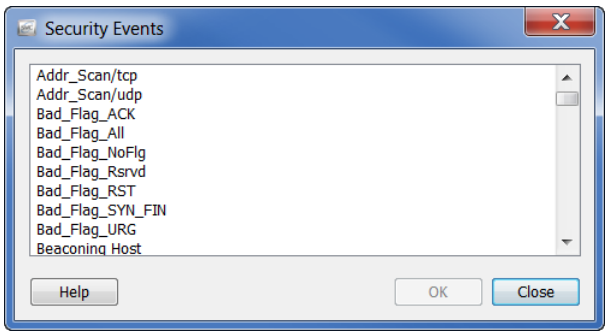
호스트 정책에서 보안 이벤트 구성

보안 이벤트를 구성하려면 다음 단계를 수행하십시오.

1. Edit Policy(정책 편집) 대화 상자에서 **Security Events(보안 이벤트)** 탭을 클릭합니다.



2. 다음 중 하나를 수행합니다.
   - 보안 이벤트를 추가해야 하는 경우 3단계로 이동합니다.
   - 보안 이벤트를 편집해야 하는 경우 5단계로 이동합니다.
3. 보안 이벤트를 추가하려면 **Add(추가)**를 클릭합니다. Security Events(보안 이벤트) 대화 상자가 열립니다.



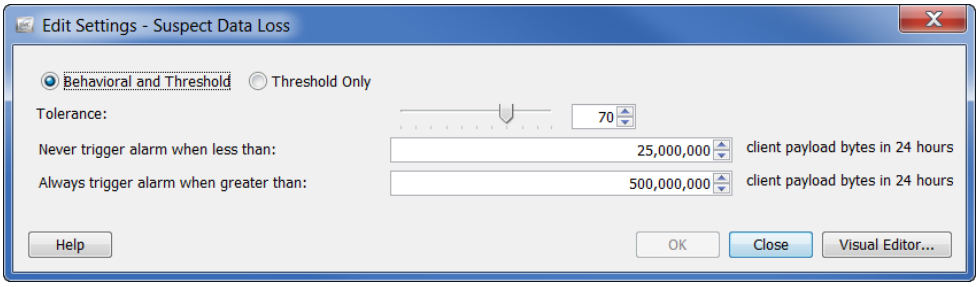
4. 다음 중 하나를 수행합니다.

   - 보안 이벤트를 하나 추가하려면 이벤트를 선택하고 **OK(확인)**를 클릭합니다.
   - 순서대로 나열된 여러 개의 이벤트를 추가하려면 첫 번째 이벤트를 선택하고 **Shift** 키를 누른 후 순서에서 마지막 이벤트를 선택하고 **OK(확인)**를 클릭합니다.
   - 순서대로 나열되지 않은 여러 개의 이벤트를 추가하려면 **Ctrl** 키를 누르고 각 이벤트를 선택한 후 **OK(확인)**를 클릭합니다.

   Security Events(보안 이벤트) 탭으로 돌아갑니다.

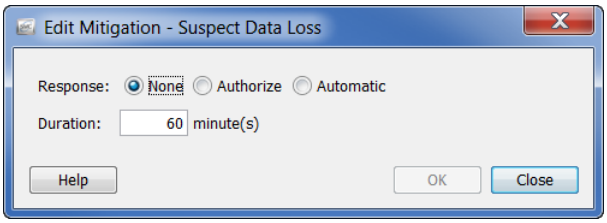
5. 보안 이벤트에 대한 임계값 설정, 행동 또는 허용 수준을 편집하려면 편집할 보안 이벤트를 선택합니다.
6. **Edit Settings(설정 편집)**를 클릭합니다.

   Edit Settings(설정 편집) 대화 상자가 열립니다.



7. 필요에 따라 설정을 변경하고 작업을 완료하면 **OK(확인)**를 클릭합니다. Edit Policy(정책 편집) 대화 상자로 돌아갑니다.
8. 완화 발생 시기 및 방법을 지정하려면 편집할 보안 이벤트를 선택합니다.
9. **Edit Mitigation(완화 편집)**을 클릭합니다.

   Edit Mitigation(완화 편집) 대화 상자가 열립니다.



10. 필요에 따라 설정을 변경하고 작업을 완료하면 **OK(확인)**를 클릭합니다. Edit Policy(정책 편집) 대화 상자로 돌아갑니다.

참고:

- 설정이 알람 카테고리에 대해 구성되어 있지 않은 경우, Settings(설정) 열에 *No Settings(설정 없음)*가 나타납니다.
- 완화 설정이 알람 카테고리에 대해 구성되어 있지 않은 경우, Mitigation(완화) 열에 *None(없음)*이 나타납니다.

11. 소스 보안 이벤트, 대상 보안 이벤트 또는 두 가지 모두를 활성화할지 여부에 따라 해당하는 모든 알람 카테고리의 포인트에 영향을 주려면 해당하는 Enable(활성화) 확인란을 클릭합니다.

팁:

한 번에 모든 이벤트에 적용하려면 Enable All Events(모든 이벤트 활성화) 또는 Disable All Events(모든 이벤트 비활성화) 버튼을 사용하십시오.

12. 소스 보안 이벤트, 대상 보안 이벤트 또는 두 가지 모두에 대해 알람을 발효할지 여부에 따라 해당하는 Alarm(알람) 확인란을 클릭합니다.
13. 다음 중 하나를 수행합니다.
    - Edit Policy(정책 편집) 대화 상자를 종료하지 않고 설정을 적용하려면 **Apply(적용) > Close(닫기)**를 클릭합니다.
    - 설정을 적용하고 Edit Policy(정책 편집) 대화 상자를 종료하려면 **OK(확인)**를 클릭합니다.

참고:

- 다양한 유형의 알람 설정에 대한 자세한 내용은 289페이지의 "알람"을 참조하십시오.
- 특정 알람의 권장 설정에 대한 내용은 295페이지의 "권장사항"을 참조하십시오.

정책 생성 및 편집

이전 섹션에서 설명한 것처럼 알람에 대응할 때는 어떤 정책이 특정 알람을 트리거했는지 판단해야 합니다. 알람을 편집하거나 비활성화할 준비가 된 경우 호스트 스냅샷의 Alarm Table(알람 테이블) 또는 **Alarm(알람)** 섹션에 있을 가능성이 매우 높습니다. 따라서 다음 예에서는 사용자가 Alarm Table(알람 테이블)에서 알람을 편집하거나 비활성화할 준비가 된 시나리오를 사용하겠습니다.

알람에 대응할 경우, 다음 단계를 수행하십시오.

1. 트리거 호스트가 무엇인지를 판단합니다. 예를 들어, 호스트가 서버 또는 데스크톱, 또는 기타입니까? 또한, 행동이 정상인지 판단합니다. 행동이 정상인 경우 다음 단계를 진행합니다. 행동이 정상이 아닌 경우, 알람의 원인을 조사하기 위해 표준 에스컬레이션 절차를 따르십시오.
2. 트리거 호스트가 이미 생성된 기본 역할 정책이 있는 사전 정의된 그룹(예: 백업 서버, 방화벽, 프록시)의 멤버는 아니지만 논리적으로 한 그룹에 소속될 수 있는 경우, 이 호스트를 논리적으로 적합한 사전 정의된 그룹에 할당하십시오. (274페이지의 "사전 정의된 그룹에 호스트 할당"을 참조하십시오.)

   예를 들어 트리거 호스트가 백업 서버인 경우 "백업 서버"라는 사전 정의된 그룹이 있으므로 이 그룹에는 기본 역할 정책이 이미 생성되어 있습니다. 따라서, 이 트리거 호스트를 백업 서버 그룹에 할당할 수 있습니다. 그런 다음 이 호스트는 백업 서버에 대한 기본 역할 정책에 자동으로 할당됩니다.
3. 트리거 호스트가 사전 정의된 그룹의 멤버가 아니며 논리적으로 한 그룹에 적합하지 않지만 다른 역할 정책에 속하는 경우, 이 호스트가 속한 역할 정책을 편집하십시오. (281페이지의 "역할 정책 편집"을 참조하십시오.)

   트리거 호스트가 사전 정의된 그룹의 멤버가 아니며 논리적으로 한 그룹에 적합하지 않지만 호스트 정책에 속하는 경우, 이 호스트가 속한 호스트 정책을 편집하십시오. (287페이지의 "호스트 정책 편집"을 참조하십시오.)
4. 트리거 호스트가 역할 정책 또는 호스트 정책에 속하지 않는 경우 다음 중 하나를 수행할 수 있습니다.

   - 이 호스트를 관리하는 외부 호스트 기본 정책 또는 내부 호스트 기본 정책 중 하나를 편집합니다(둘 중 하나 적용). (261페이지의 "내부 호스트/외부 호스트의 기본 정책 편집"을 참조하십시오.)

주의:

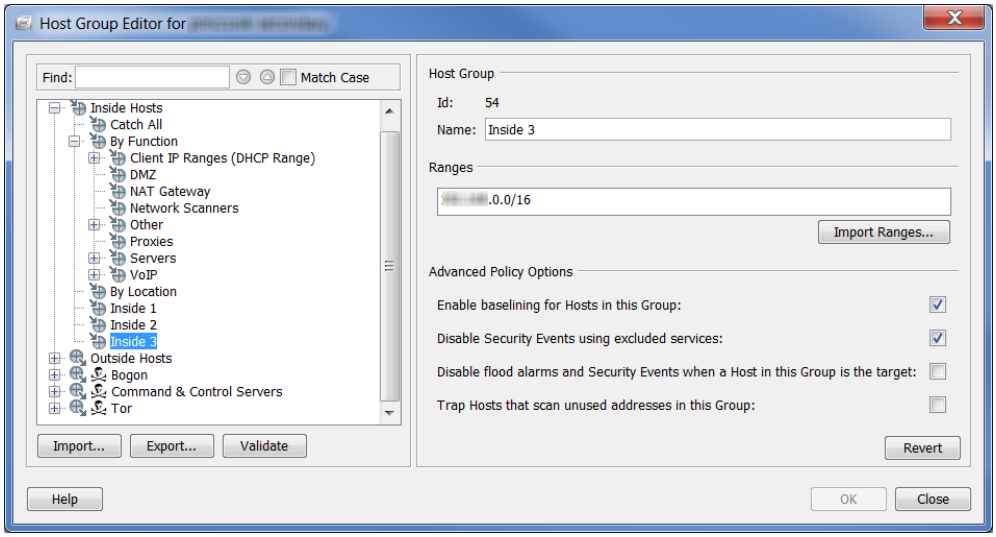
내부 호스트 기본 정책 또는 외부 호스트 기본 정책을 편집하면 글로벌 설정에 영향을 미친다는 점을 기억하십시오.

- 이 호스트에 대한 역할 정책을 생성합니다. (275페이지의 "역할 정책 생성"을 참조하십시오.)
- 이 호스트에 대한 호스트 정책을 생성합니다. (283페이지의 "호스트 정책 생성"을 참조하십시오.)

사전 정의된 그룹에 호스트 할당

호스트를 사전 정의된 그룹에 할당하려면 다음 단계를 수행하십시오.

1. Enterprise(엔터프라이즈) 페이지의 트리 메뉴에서 트리거 호스트가 속한 도메인을 클릭합니다.
2. 메인 메뉴에서 **Configuration(컨피그레이션) > Edit Host Groups(호스트 그룹 편집)**를 선택합니다. 엔터프라이즈 트리에서 클릭한 도메인에 대한 Host Group Editor(호스트 그룹 편집기) 대화 상자가 열립니다.
3. 왼쪽 창에서 트리거 호스트를 할당할 그룹을 클릭합니다. 이미 이 그룹의 멤버인 호스트의 IP 주소가 대화 상자의 오른쪽에 있는 Ranges(범위) 필드에 표시됩니다.



팁:

단일 호스트를 그룹으로 신속하게 이동하려면 문서 내에서 호스트를 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > Manage Host Groups(호스트 그룹 관리)**를 선택합니다. 해당 호스트에 대한 Host Groups(호스트 그룹) 대화 상자가 열리면, 대화 상자의 맨 위 섹션에서 원하는 그룹을 선택한 다음 **OK(확인)**를 클릭합니다.

4. 3단계에서 지정한 그룹에 IP 주소를 추가하려면 다음 단계를 완료합니다.
   - Ranges(범위) 필드에 트리거 호스트의 IP 주소를 입력합니다.
   - 둘 이상의 호스트를 추가하려고 하며 호스트가 범위 내에 있는 경우 Ranges(범위) 필드에서 트리거 호스트의 원하는 IP 주소 범위를 입력합니다.
   - 둘 이상의 호스트를 추가하려고 하며 트리거 호스트의 IP 주소가 포함된 기존 파일이 있는 경우 IP 주소를 가져오려면 **Import Ranges(범위 가져오기)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다. Enterprise(엔터프라이즈) 페이지의 트리 메뉴가 새로 추가된 모든 IP 주소를 3단계에서 지정한 그룹에 포함하도록 자동으로 업데이트됩니다.

역할 정책 생성

공통 기능 또는 유사한 특성을 공유하는 호스트 그룹에 동일한 알람 임계값이 할당되게 하려면 역할 정책을 생성하십시오.

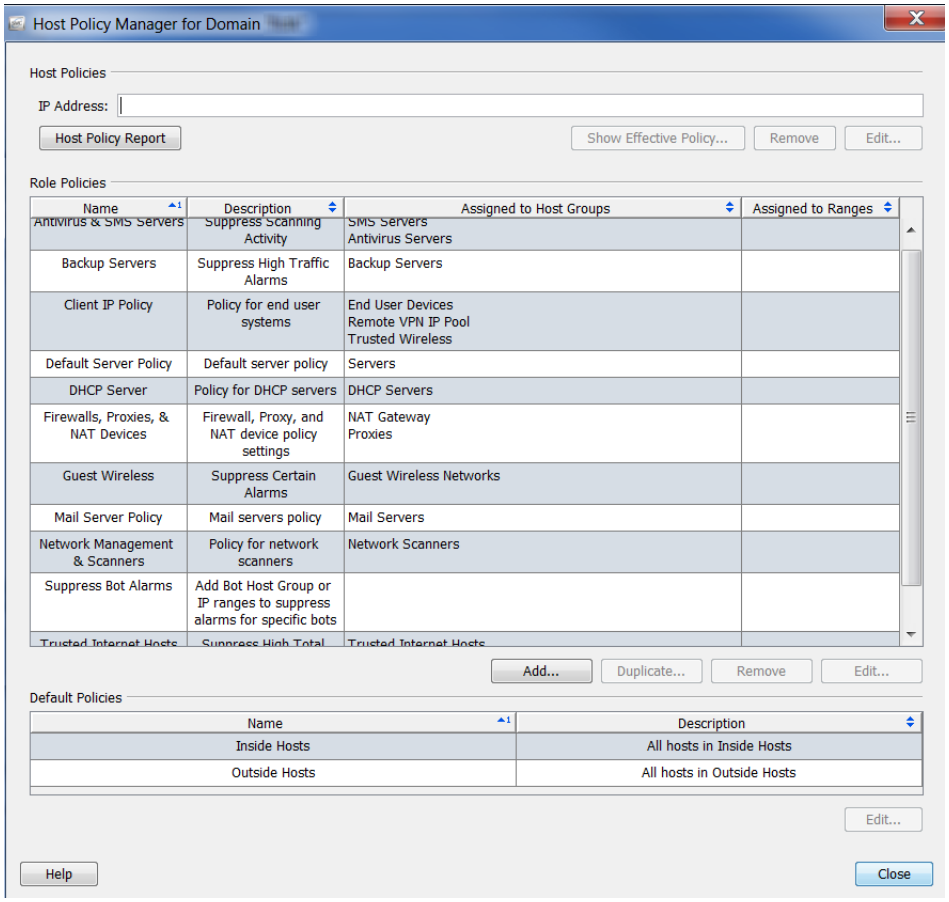
IP 주소에 대한 호스트 정책이 없으면 Stealthwatch는 해당 호스트를 관리하는 역할 정책의 해당 알람 설정을 사용합니다. 호스트는 여러 역할 정책에 존재하고 역할 정책의 **모든** 설정을 상속받을 수 있습니다. 따라서 둘 이상의 역할 정책을 특정 호스트에 적용할 수 있고 각 정책에 대한 임계값 설정이 다를 수 있으므로 호스트 행동이 각 역할 정책 내에서 정의된 값을 초과하는 경우, 여러 개의 알람이 트리거될 수 있습니다.

참고:

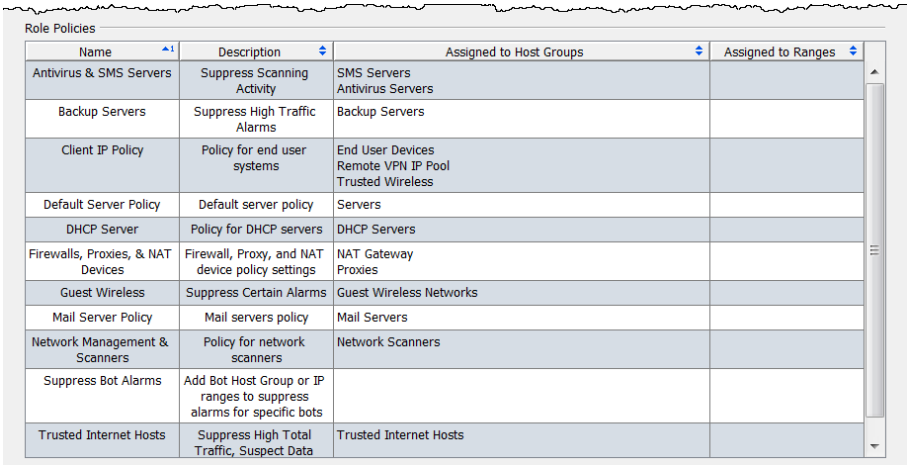
혼란을 방지하기 위해 다른 값(예: 다른 팀 대상 값)을 기준으로 알람을 트리거해야 하는 경우를 제외하고 동일한 알람을 사용하는 여러 역할 정책을 사용하지 않는 것이 가장 좋습니다.

역할 정책을 추가하려면 다음 단계를 수행하십시오.

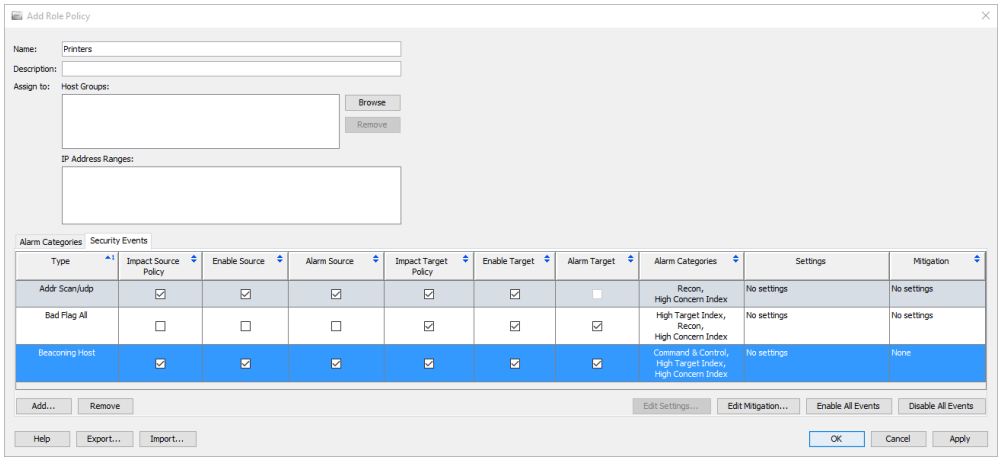
1. 메인 메뉴에서 **Configuration(컨피그레이션) > Host Policy Manager(호스트 정책 관리자)**를 선택합니다. Host Policy Manager(호스트 정책 관리자) 대화 상자가 열립니다.



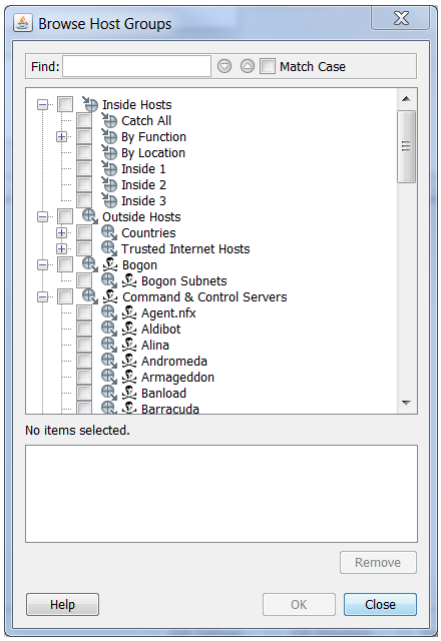
2. Host Policy Manager(호스트 정책 관리자) 대화 상자의 **Role Policies(역할 정책)** 섹션에서 **Add(추가)**를 클릭합니다.



Add Role Policy(역할 정책 추가) 대화 상자가 열립니다.



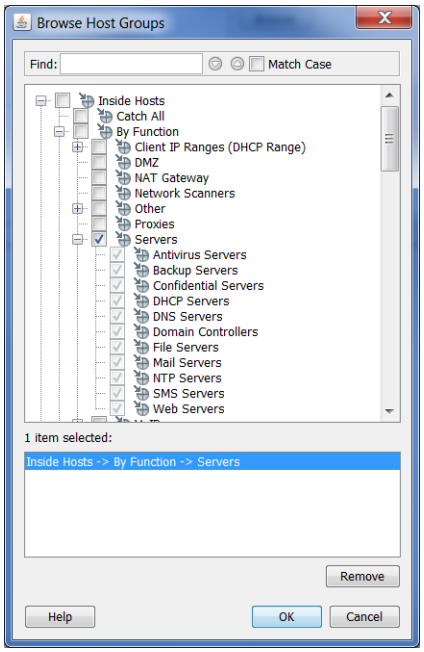
3. Name(이름) 필드에 추가하려는 정책의 이름(예: 회계 부서)을 입력합니다.
4. Description(설명) 필드에 설명을 입력합니다(선택사항).
5. 다음 단계 중 하나를 완료합니다.
   - IP Address Ranges(IP 주소 범위) 필드에서 특정 호스트 IP 주소 또는 범위를 입력합니다.
   - "Assign to: Host Groups(할당 대상: 호스트 그룹)" 필드에서 **Browse(찾아보기)**를 클릭합니다. Browse Host Groups(호스트 그룹 찾아보기) 대화 상자가 열립니다.



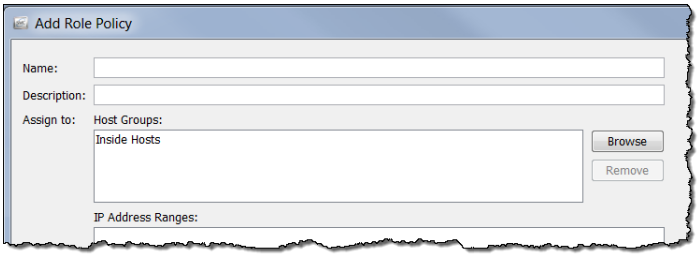
참고:

각 호스트 그룹에는 특정 알람을 방지할 수 있는 속성 설정이 있습니다. 이러한 설정을 보려면 엔터프라이즈 트리 메뉴에서 호스트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > Host Group Properties(호스트 그룹 속성)**를 선택합니다. Edit Host Group(호스트 그룹 편집) 대화 상자가 열립니다. Advanced Policy Options(고급 정책 옵션)가 맨 아래에 나열됩니다.

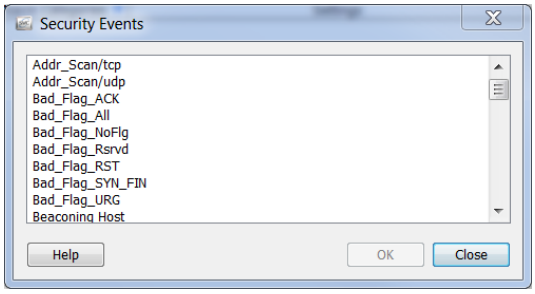
6. 정책을 적용할 호스트 그룹을 클릭합니다. 상위 호스트를 클릭하면 이 호스트에 속하는 모든 호스트가 자동으로 선택됩니다.



7. **OK(확인)**를 클릭합니다. 이제 그룹이 Add Role Policy(역할 정책 추가) 대화 상자의 **Assign to: Host Groups:(할당 대상: 호스트 그룹:)** 섹션에 표시됩니다.



8. Add Role Policy(역할 정책 추가) 대화 상자의 맨 아래에서 **Add(추가)**를 클릭합니다. Security Events(보안 이벤트) 대화 상자가 열립니다.

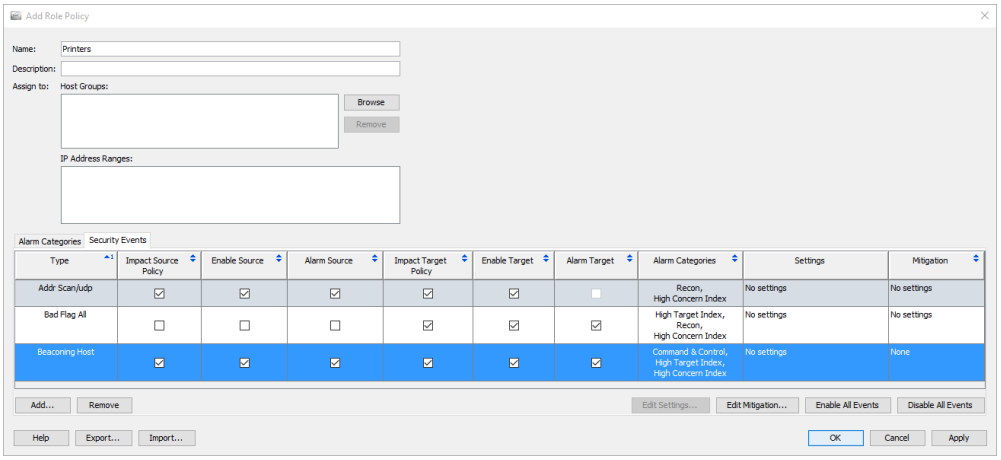


9. 편집할 알람을 클릭하고 **OK(확인)**를 클릭합니다.

참고:

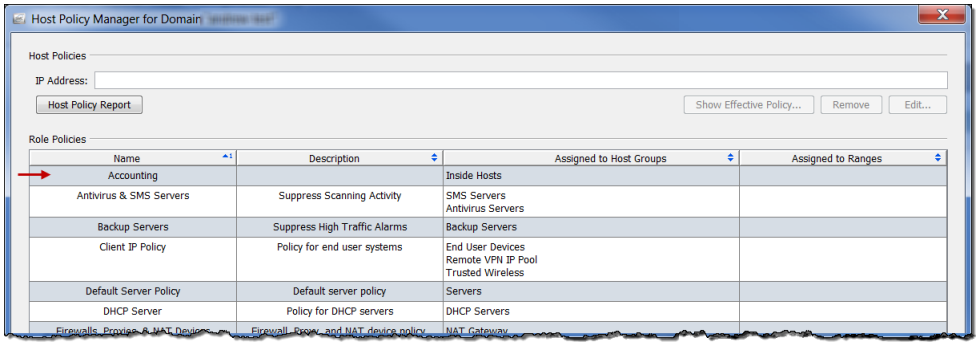
둘 이상의 알람을 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 알람을 클릭합니다. 알람의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 알람을 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 알람을 클릭합니다.

알람이 Add Role Policy(역할 정책 추가) 대화 상자에 표시됩니다.



10. 이 정책에서 트리거할 각 알람에 대한 확인란을 선택합니다.

11. **Apply(적용) > Close(닫기)**를 클릭합니다. Host Policy Manager(호스트 정책 관리자) 대화 상자의 Role Policies(역할 정책) 섹션에 정책이 나타납니다.



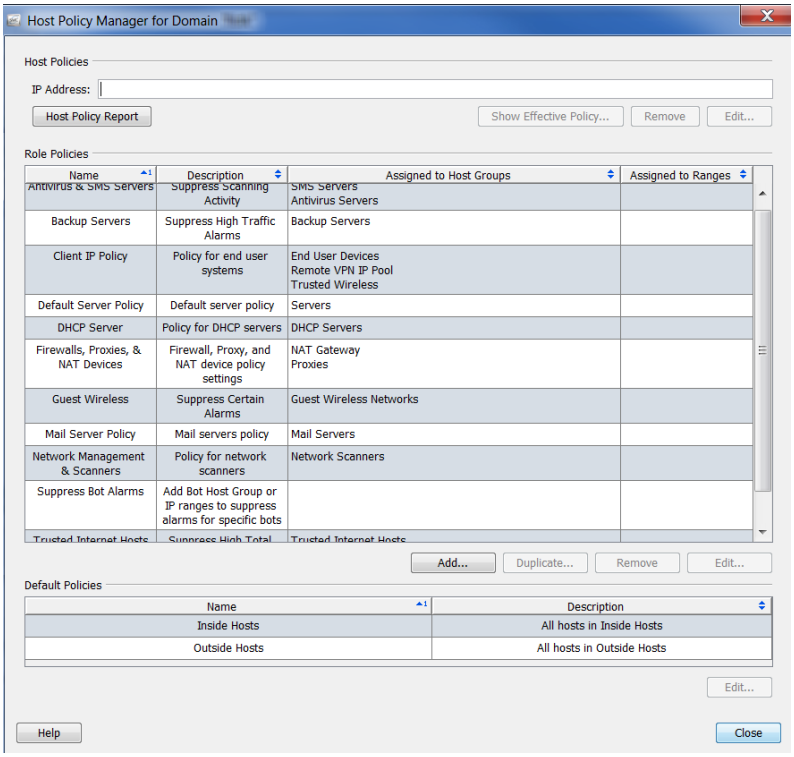
팁:

IP 주소의 한 범위 또는 IP 주소의 여러 범위에 역할 정책을 할당하려는 경우, 해당 IP 주소에 대해 호스트 그룹을 생성한 다음 이 호스트 그룹에 역할 정책을 할당하십시오.

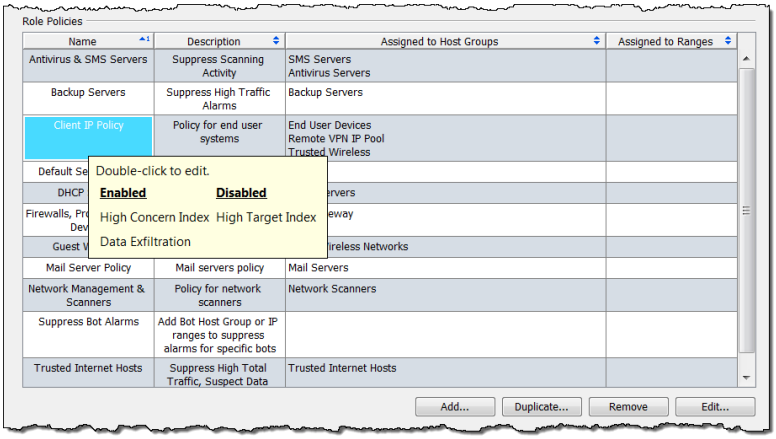
역할 정책 편집

역할 정책을 편집하려면 다음 단계를 수행하십시오.

1. 메인 메뉴에서 **Configuration(컨피그레이션) > Host Policy Manager(호스트 정책 관리자)**를 선택합니다. Host Policy Manager(호스트 정책 관리자) 대화 상자가 열립니다.



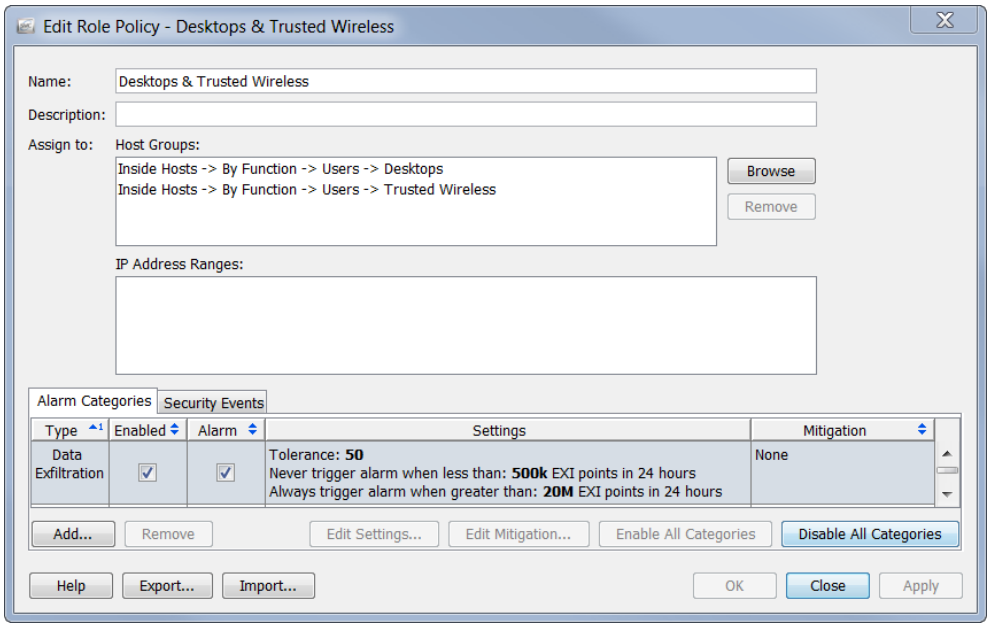
2. Host Policy Manager(호스트 정책 관리자) 대화 상자의 **Role Policies(역할 정책)** 섹션에서 편집할 역할 정책의 이름을 클릭한 다음 **Edit(편집)**을 클릭합니다.



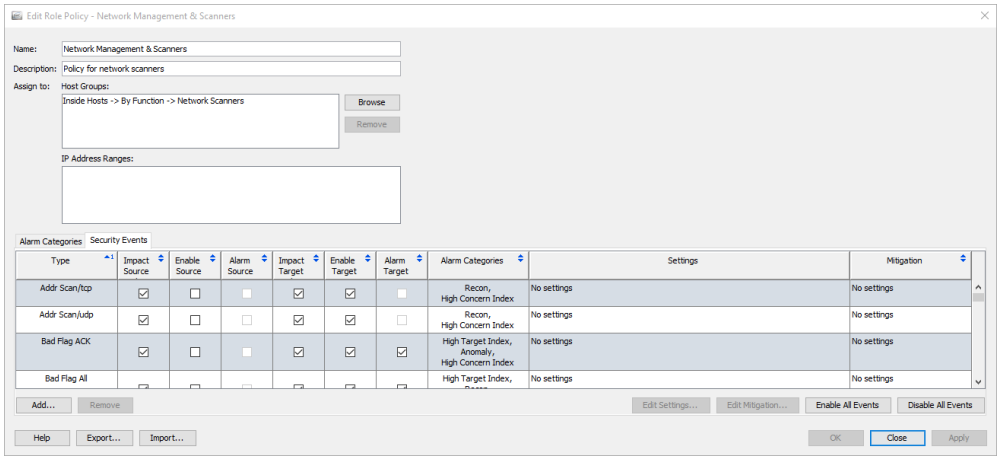
참고:

항목 위에 커서를 올려 놓으면 모든 활성화 및 비활성화된 알람 리스트가 나타납니다. 이전 예에서 알람을 비활성화하지 않았으므로 비활성화된 알람 리스트가 없습니다.

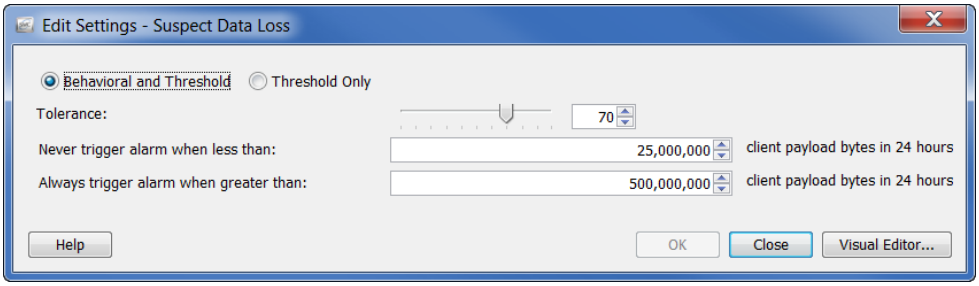
Edit Role Policy(역할 정책 편집) 대화 상자가 열립니다. 기본적으로 Alarm Categories(알람 카테고리) 탭이 열립니다.



편집할 알람에 따라 Security Events(보안 이벤트) 탭을 클릭해야 할 수 있습니다.



3. 편집할 알람을 더블 클릭합니다(Settings(설정) 열에서 클릭). 해당 알람에 대한 Edit Settings(설정 편집) 대화 상자가 열립니다.



4. 편집을 완료하면 **Close(닫기)**를 클릭합니다.

참고:

- 다양한 유형의 알람 설정에 대한 자세한 내용은 289페이지의 "알람"을 참조하십시오.
- 특정 알람의 권장 설정에 대한 내용은 295페이지의 "권장사항"을 참조하십시오.

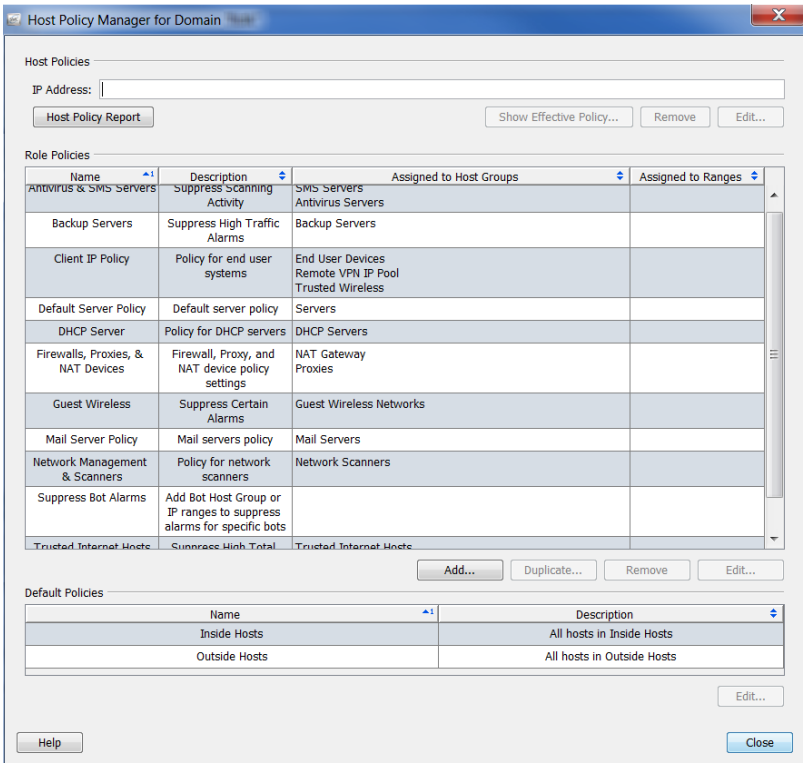
호스트 정책 생성

앞에서 설명했듯이 IP 주소가 역할 또는 기본 정책 레벨에서 다른 알람에 할당되었는지 여부와 관계없이 IP 주소에 대한 호스트 정책이 있는 경우, Stealthwatch는 이 호스트 정책에서 해당하는 알람 카테고리 설정을 사용하여 해당 호스트에 대해 알람을 트리거할 시기를 판단합니다. 호스트 정책이 항상 역할 정책과 기본 정책을 재정의한다는 점을 기억하십시오.

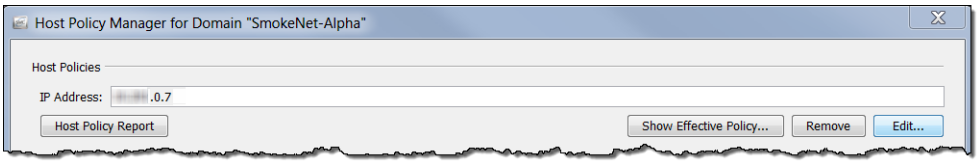
개별 호스트에 대해 호스트 정책을 편집할 수 있습니다(역할 정책 또는 기본 정책 편집과 반대). 개별 호스트를 찾고 있으며 예를 들어 알람 테이블에서 특정 호스트에 대해 트리거되서는 안되거나 다른 임계값에서 트리거되어야 하는 특정 알람이 트리거된 것을 발견하는 경우, 해당 특정 호스트에 대해 유효한 호스트 정책을 수정할 수 있습니다.

호스트 정책을 추가하려면 다음 단계를 수행하십시오.

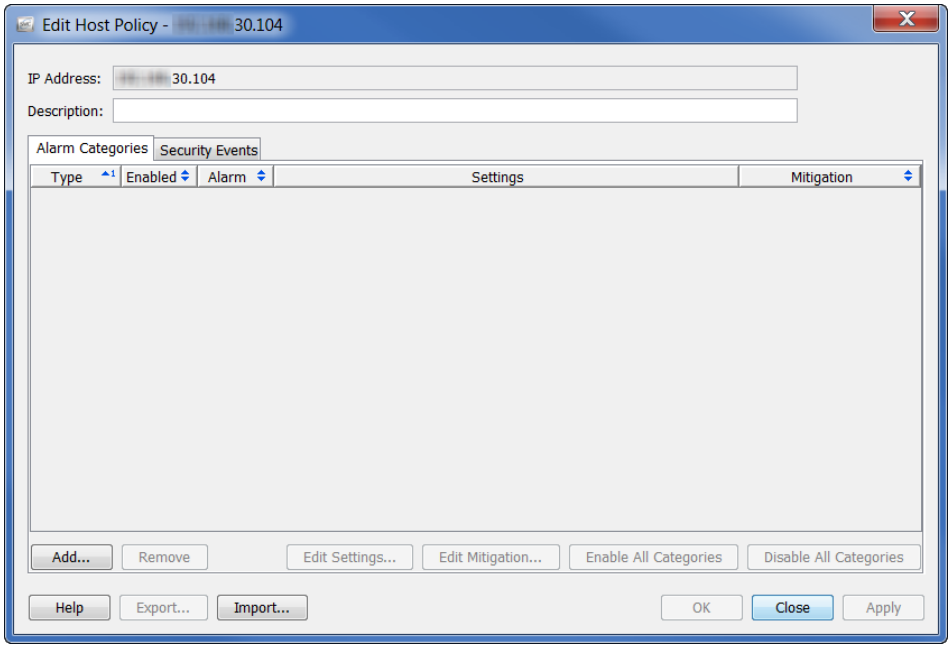
1. 메인 메뉴에서 **Configuration(컨피그레이션) > Host Policy Manager(호스트 정책 관리자)**를 선택합니다. Host Policy Manager(호스트 정책 관리자) 대화 상자가 열립니다.



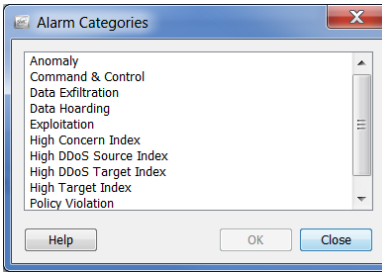
2. **Host Policies(호스트 정책)** 섹션에서 호스트 정책을 추가할 대상 호스트의 IP 주소를 입력합니다.
3. **Edit(편집)**을 클릭합니다.



Edit Host Policy(호스트 정책 편집) 대화 상자가 열립니다. 기본적으로 Alarm Categories(알람 카테고리) 탭이 열립니다.



4. **Add(추가)**를 클릭합니다. Alarm Categories(알람 카테고리) 대화 상자가 열립니다.

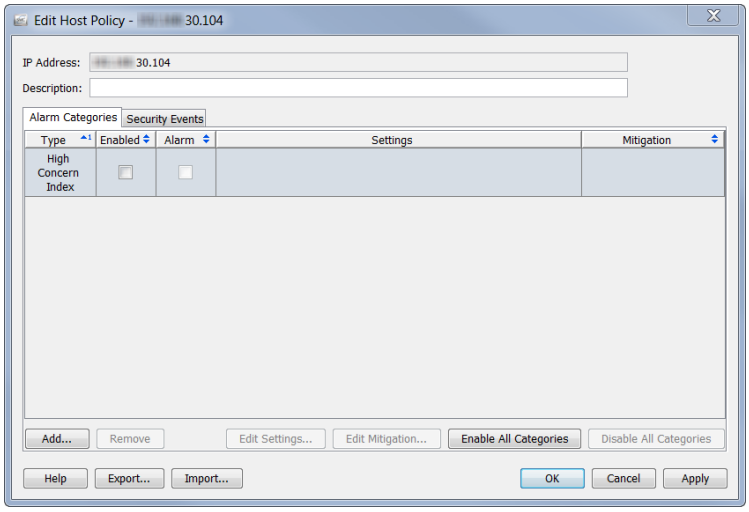


5. 이 호스트 정책에 추가할 알람 카테고리를 클릭한 다음 **OK(확인)**를 클릭합니다.

참고:

둘 이상의 알람을 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 알람을 클릭합니다. 알람의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 알람을 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 알람을 클릭합니다.

알람 카테고리가 Edit Host Policy(호스트 정책 편집) 대화 상자에 표시됩니다.



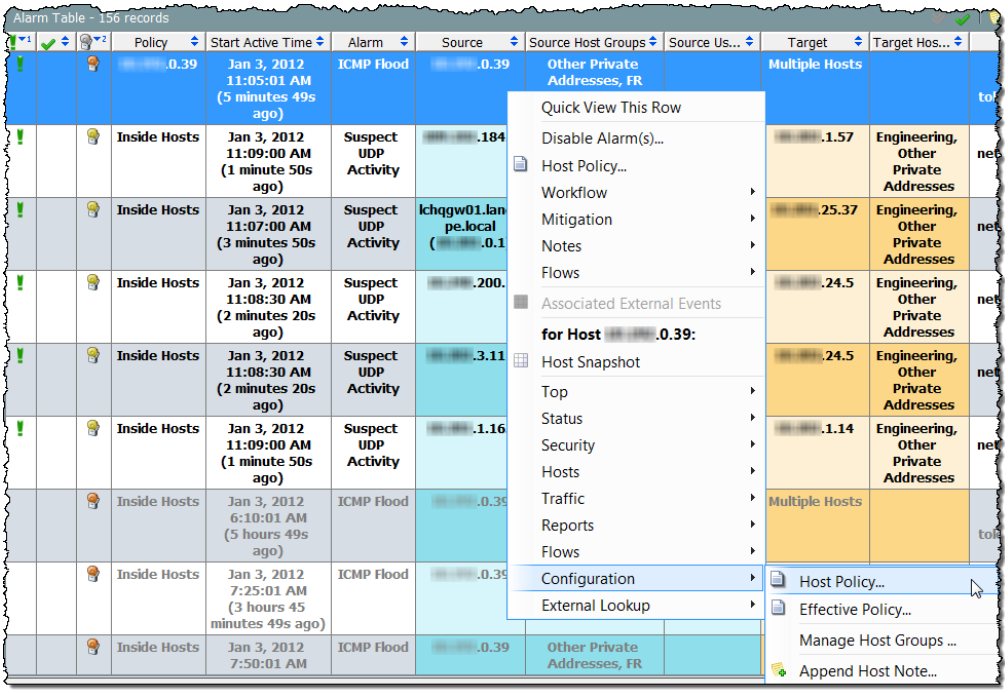
참고:

Enabled(활성화됨) 열에 이 정책에서 트리거할 모든 알람에 대한 체크 마크가 있는지 확인하십시오.

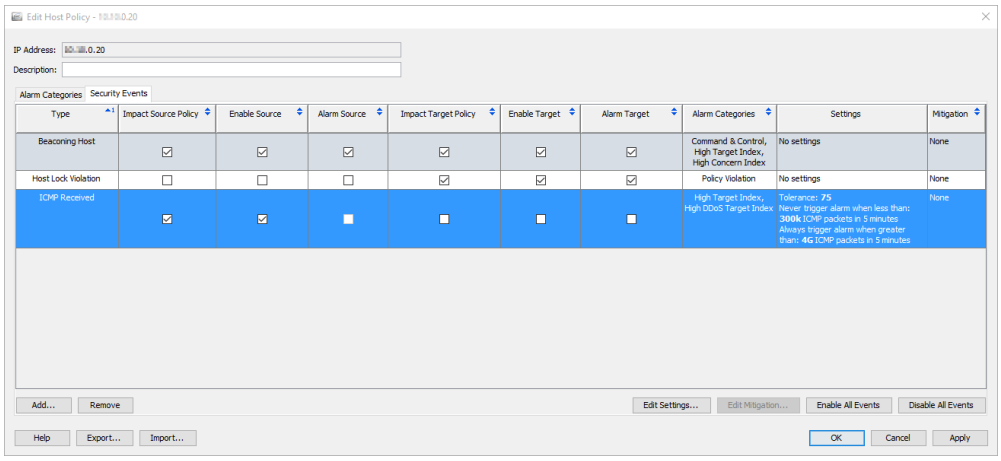
호스트 정책 편집

호스트 정책을 편집하려면 다음 단계를 수행하십시오.

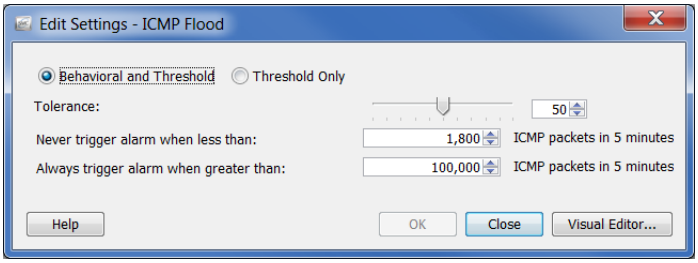
1. 호스트 IP 주소를 마우스 오른쪽 버튼으로 클릭하고 **Configuration(컨피그레이션) > Host Policy(호스트 정책)**를 선택합니다.



해당 호스트에 대한 Host Policy(호스트 정책) 대화 상자가 열립니다.



2. 수정할 알람을 더블 클릭합니다. 해당 알람에 대한 Edit Settings(설정 편집) 대화 상자가 열립니다.



3. 변경하고 **Close(닫기)**를 클릭합니다.

참고:

- 다양한 유형의 알람 설정에 대한 자세한 내용은 289페이지의 "알람"을 참조하십시오.
- 특정 알람의 권장 설정에 대한 내용은 295페이지의 "권장사항"을 참조하십시오.

알람

차이 기반 알람과 설정/해제 알람 비교

알람은 호스트 활동이 과거 행동에서 상당한 변화를 겪을 때 트리거됩니다. 이러한 유형의 알람에 대한 허용 수준(즉, 민감도)은 호스트 정책 관리자를 사용하여 변경할 수 있습니다. 이러한 알람을 차이 기반 알람이라고 합니다. 다음 테이블에는 차이 기반 알람이 나와 있습니다.

참고:

알람 카테고리 또한 차이 기반입니다.

차이 기반 알람	
이상 징후	포트 스캔
무차별 암호 대입 로그인	관계형의 높은 총 트래픽
명령 및 제어	관계형의 높은 트래픽
데이터 유출	관계형 ICMP 플러드
데이터 호딩	관계형의 낮은 트래픽
공격	관계형의 최대 플로우 시작됨
상위 관심 지표(CI)	관계형의 최대 플로우 제공됨
상위 DDoS 소스 지표(SI)	관계형의 SYN 플러드
상위 DDoS 대상 지표(TI)	관계형의 UDP 플러드
상위 파일 공유 지수(FSI)	관계형의 왕복 시간
높은 SMC 피어	관계형의 서버 응답 시간
상위 대상 지표(TI)	관계형의 TCP 재전송 비율
높은 트래픽	관계형의 높은 총 트래픽
대량의 이메일	느린 연결 플러드
ICMP 플러드	SPAN 소스
ICMP 수신됨	SSH 역방향 셸
메일 거부	의심스러운 데이터 호딩
메일 릴레이	의심스러운 데이터 손실
최대 플로우 시작됨	SYN 플러드

차이 기반 알람	
최대 플로우 제공됨	SYN 수신됨
패킷 플러드	표적 데이터 호딩
새 플로우 시작됨	연결됨
새 플로우 제공됨	트랩된 호스트
정책 위반	UDP 플러드
정찰	수신된 UDP

이 접근 방식의 주요 이점은 시스템을 조정하여 발생하는 알람 수를 조직의 요구 사항에 맞출 수 있다는 점입니다. 즉, 많은 수의 알람을 선호하는 경우(즉, 예상되는 행동에서 약간의 변화만 허용 가능) 연관된 정책에서 허용 수준 설정을 낮출 수 있습니다. 반대로, 적은 수의 알람을 선호하는 경우(즉, 예상되는 행동에서 상당한 변화 허용 가능) 허용 수준 설정을 높일 수 있습니다. 기본적으로, 차이 기반 알람에 대한 각 설정은 숫자 값에 연결되며 이 값은 위 또는 아래로 조정할 수 있습니다.

차이 기반 알람에서 사용되는 임계값은 최근 활동 및 구성된 허용 수준을 기준으로 베이스라인에서 생성됩니다. 그 결과 행동이 지나치게 많이 변경된 경우 알람을 생성하는 기능을 그대로 유지하면서 시간이 지남에 따라 행동을 변경하는 기능이 호스트에 제공됩니다. 허용 수준을 설정하여 허용 가능한 변화 수준을 제어할 수 있습니다. 기본적으로, 알람 임계값 레벨의 민감도를 조정하는 기능이 있습니다(즉, 원하는 레벨에 맞게 "소음 줄이기").

차이 기반 알람을 사용할 경우 호스트가 특정 레벨의 편차에 도달해야 알람이 트리거됩니다. 예를 들어, 상위 총 트래픽 알람에 대한 허용 수준이 50으로 설정된 경우 시스템은 예상값(호스트 베이스라인)을 넘는 값의 최저 50%는 무시하지만 이 값보다 높은 경우 알람을 생성합니다.

참고:

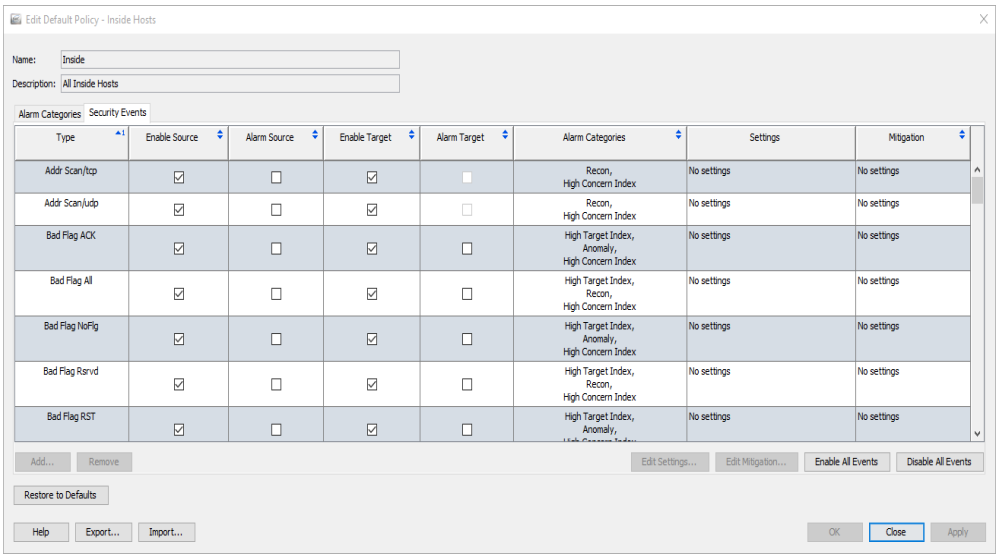
알람 설정에 대한 자세한 내용은 292페이지의 "차이 기반 알람에 대한 설정"을 참조하십시오.

두 번째 유형의 알람은 설정하거나 해제할 수 있는 알람입니다. 이 유형의 알람을 트리거하는 기준은 차이 기반 알람의 트리거 기준과 다릅니다. 간단한 설정/해제 설정을 지닌 알람의 경우, 이 유형의 알람이 트리거되기 전에 호스트 행동이 상호 간에 모두 일치해야 하는 특정 조건에 부합해야 합니다. 이러한 조건에 모두 해당하지 않는 경우 알람이 트리거되지 않습니다. 예를 들어, 웜 활동 알람을 트리거하려면 **모든** 다음 행동이 발생해야 합니다.

- 소스 호스트가 여러 하위 네트워크에서 스캔되었습니다.
- 최소 하나 이상의 대상 호스트가 소스 호스트에 연결되었습니다.
- 이 대상 호스트가 소스 호스트에 정보를 전송했습니다.

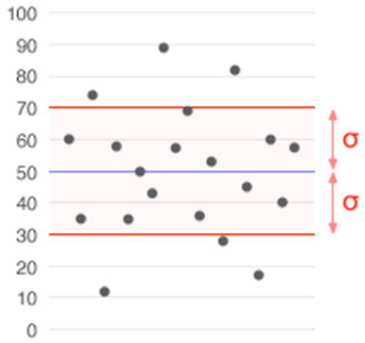
이러한 조건 중 하나라도 해당하지 않는 경우 알람이 트리거되지 않습니다.

Edit Default Policy(기본 정책 편집) 대화 상자의 Settings(설정) 열에서 어떤 알람이 차이 기반 알람이며 어떤 알람이 설정/해제 알람인지 판단할 수 있습니다. 알람이 차이 기반 알람인 경우, 해당 알람에 대해 표시되었던 허용 수준 값이 표시됩니다. 알람이 설정/해제 알람인 경우, "No Settings(설정 없음)" 항목이 표시됩니다.



차이 기반 알람에 대한 설정

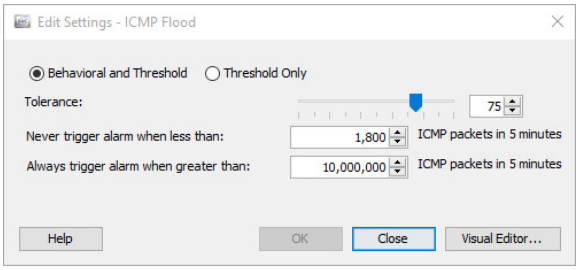
이전 섹션에서 설명한 것처럼 차이 기반 알람에서 사용되는 임계값은 최근 활동 및 구성된 허용 수준 기준으로 베이스라인에서 생성됩니다. 허용 수준은 "규정된 기준치로부터 표준 편차의 수"로 정의되며 이를 통해 알람의 임계값 레벨의 민감도를 조정할 수 있습니다.



평균이 50(파란색으로 표시됨)이고 표준 편차(σ)가 20인 데이터 집합

표준 편차는 통계에서 널리 사용되는 가변성 또는 다양성을 측정하는 방법입니다. 표준 편차는 평균(즉, 중간값 또는 예상 값)과 얼마나 차이가 있는지 보여줍니다. 낮은 표준 편차는 데이터 포인트가 평균과 매우 가까운 것을 나타내는 반면, 높은 표준 편차는 데이터 포인트가 넓은 범위의 값에 분포되어 있는 것을 나타냅니다.

다음 예는 차이 기반 알람에 대한 Edit Settings(설정 편집) 대화 상자를 보여 줍니다.



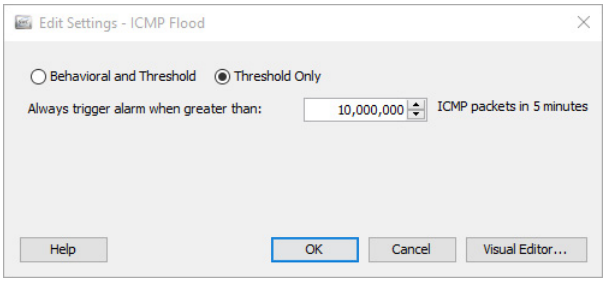
차이 기반 알람에는 다음과 같은 조정 가능한 설정이 포함되어 있습니다.

- 행동 및 임계값 - 이 옵션을 선택하면 대화 상자에 허용 수준 설정, 최소 임계값, 최대 임계값이 표시됩니다.
  - 허용 수준- 알람을 생성하기 전에 예상 행동을 초과하는 실제 행동을 얼마나 허용할지 나타내는 0과 100 사이의 상대적인 숫자입니다. 이 옵션을 사용하여 "매우 다른" 것을 정의할 수 있습니다.
    - 허용 수준이 0이면 예상 값을 초과한 모든 값에 대해 알람을 생성한다는 의미로, 매우 민감한 설정이므로 많은 알람이 발생합니다.

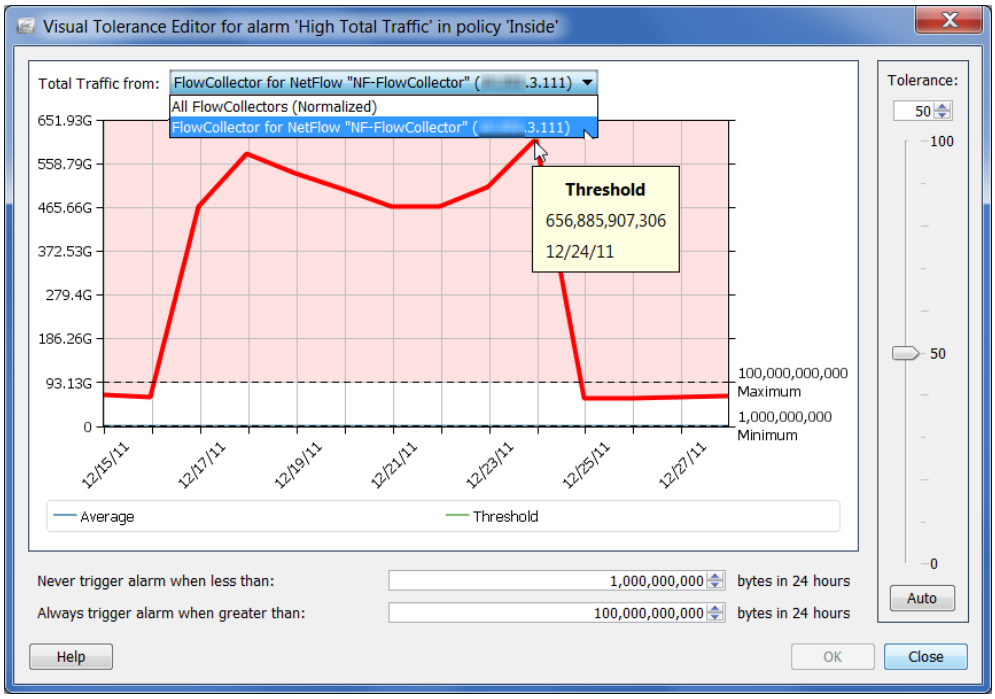
- 허용 수준 100은 알람을 허용할 수 있는 최고 레벨을 의미합니다. 이 옵션은 알람이 트리거되는 횟수를 상당히 줄여주지만 알람이 트리거되지 않게 하려면 알람을 비활성화해야 합니다.
- 허용 수준이 50이면 호스트가 예상값을 넘는 값의 최저 50%는 무시하지만 이 값보다 높은 경우 알람을 생성합니다.

- *다음 값 미만일 경우 알람을 트리거하지 않음: 최소 임계값*이라고도 하는 이 옵션은 알람 트리거를 허용하는 최소값을 나타내는 정적 값입니다. 알람은 관찰된 값이 이 설정보다 작을 경우 트리거되지 않습니다. 즉, 호스트가 예상 값을 훨씬 초과하지만, 이 대화 상자에 나와 있는 최소값보다 크지 않은 경우, 알람을 트리거하지 않습니다.
- *다음 값보다 클 경우 항상 알람 트리거: 최대 임계값*이라고도 하는 이 옵션은 알람을 트리거하지 않도록 하는 가장 높은 값을 나타내는 정적 값입니다. 알람은 관찰된 값이 이 설정을 초과하는 경우 트리거됩니다. 즉, 호스트가 이 대화 상자에 나와 있는 최대값을 초과하는 경우, 해당 호스트에 대해 예상되는 값인 경우에도 알람을 트리거합니다.

▶ 임계값만 - 이 옵션을 선택하면 대화 상자에 최대 임계값 설정만 표시됩니다.



Visual Editor(시각적 편집기)를 클릭하여 Visual Editor(시각적 편집기) 대화 상자에 액세스합니다. 다음 예에서와 같이 Visual Tolerance Editor(시각적 허용 수준 편집기)는 특정 알람에 대한 호스트 또는 호스트 그룹 정책의 설정을 조정하기 위한 그래픽 방식입니다.



참고:

Flow Collector를 하나만 사용 중인 경우 화면 상단의 **Total Traffic from(다음 위치의 총 트래픽)** 드롭다운 리스트에서 **Flow Collector** 옵션을 클릭하여 관련 알람의 실제 값을 확인하십시오. Flow Collector를 여러 개 사용 중인 경우 **Normalized(표준화됨)** 옵션을 클릭하여 값을 표준화합니다.

권장사항

이 섹션에서는 지나치게 많은 수의 불필요한 알람을 수신하는 이벤트에서 네트워크를 미세조정하는 방법에 대한 권장사항을 제공합니다. 이 섹션에서 권장사항은 알파벳 순서로 나열된 가장 일반적인 알람 유형에 따라 분류되었습니다.

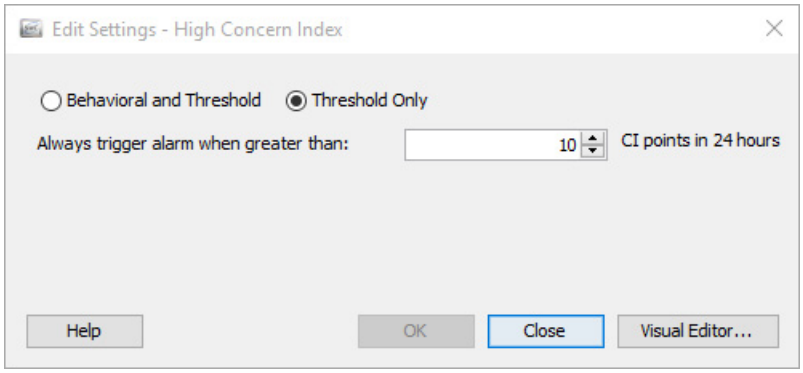
참고:

- 이러한 알람 및 기타 알람에 대한 자세한 설명을 읽으려면 *SMC 클라이언트 온라인 도움말*의 "알람 리스트" 항목을 참조하십시오.
- 아래에 나열된 알람 설정을 조정하는 방법에 대한 자세한 내용은 292페이지의 "차이 기반 알람에 대한 설정"을 참조하십시오.

상위 관심 지표(CI)

High Concern Index(상위 관심 지표(CI))는 마지막 아카이브 시간 이후에 CI 포인트가 가장 높은 호스트에 대한 정보를 표시합니다. 따라서 위협의 우선 순위를 정하고 실제로 중요한 이벤트에 중점을 두는 데 도움이 됩니다. 매일 수 천 개의 알람을 확인하는 대신 Stealthwatch는 가장 높은 심각도에서 가장 낮은 심각도 순으로 소수의 실행 가능한 항목을 제공합니다.

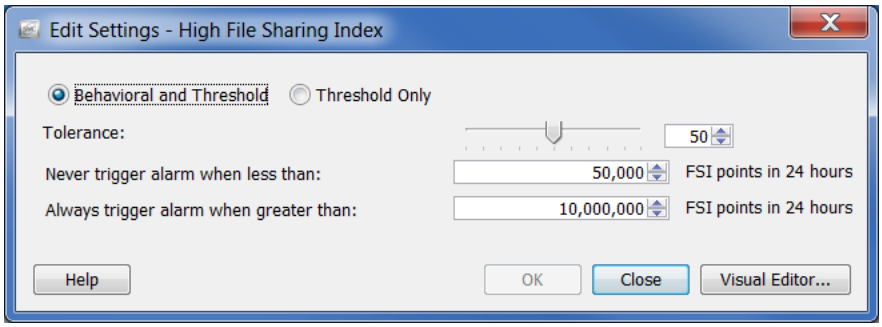
일반적으로 내부 호스트로 인해 상위 관심 지표(CI) 알람이 발생할 경우, 호스트가 더 이상 정상적으로 동작하지 않는 것을 나타냅니다. 표시되는 상위 CI 알람이 보안 침해 또는 오용의 결과가 아닌 것으로 충분히 판단되는 경우 Host Policy Manager(호스트 정책 관리자)에서 설정을 조정합니다. 또한 알람을 트리거하는 보안 이벤트를 지정할 수 있습니다.



상위 파일 공유 지수

High File Sharing Index(상위 파일 공유 지수(FSI)) 알람은 Host Policy Manager(호스트 정책 관리자)에서 정의된 대로 파일 공유 활동이 FSI 임계값을 초과했음을 나타냅니다. 호스트가 파일 공유에 사용된 상위 FSI 알람을 유발하는 경우, 다음 단계 중 하나를 완료하여 표시되는 불필요한 알람 수를 줄일 수 있습니다.

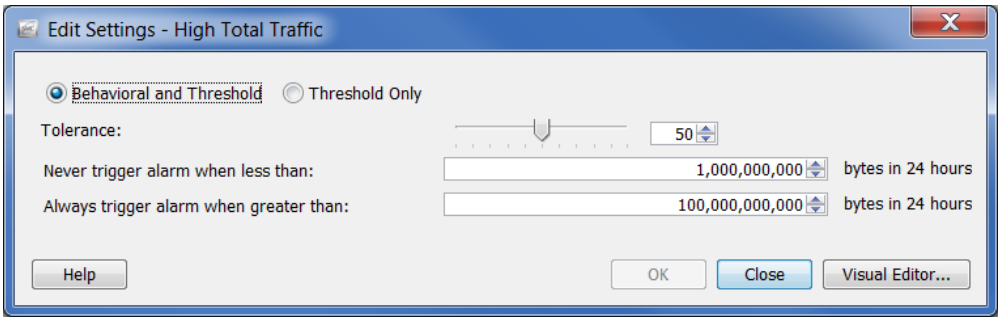
- 체크 마크를 제거하기 위해 해당하는 정책에서 **Enabled(활성화됨)** 확인란을 클릭하여 해당 호스트/호스트 그룹에 영향을 미치는 정책에 대해 상위 파일 공유 지수 알람을 비활성화합니다.
- 해당 호스트/호스트 그룹에 영향을 미치는 정책에 대해 상위 파일 공유 지수 알람 임계값 또는 허용 수준 설정을 높입니다.



높은 총 트래픽

High Total Traffic(높은 총 트래픽) 알람은 총 트래픽 인바운드와 총 트래픽 아웃바운드를 더한 값이 호스트에 대한 정책 설정을 초과하는 경우를 나타냅니다. 표시되는 높은 총 트래픽 알람의 양이 마음에 들지 않으면 해당하는 정책에서 설정을 조정합니다.

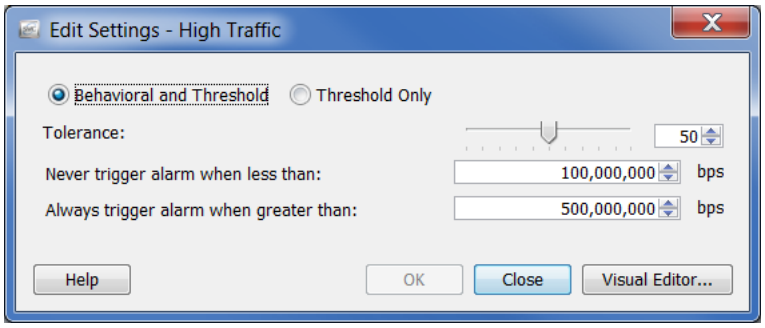
보고되고 있는 평균 바이트 수 이상의 의심스러운 호스트 또는 호스트 그룹에 대한 정책 설정을 적용합니다.



높은 트래픽

High Traffic(높은 트래픽) 알람은 평균 5분이 넘는 호스트 트래픽 속도가 허용되는 트래픽 값 제한을 초과한 경우를 나타냅니다. 표시되는 높은 트래픽 알람의 양이 마음에 들지 않으면 해당하는 정책에서 설정을 조정합니다.

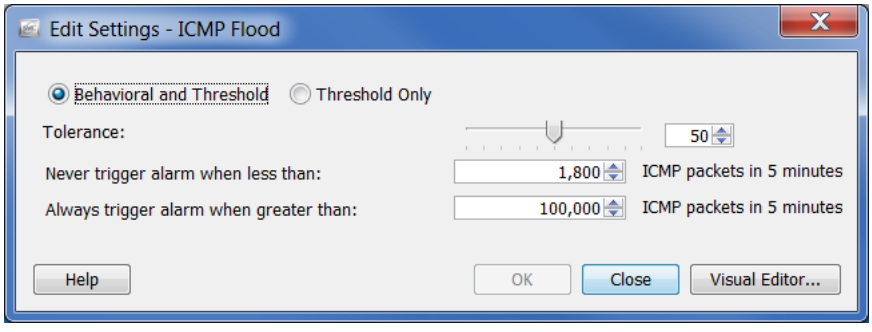
보고되고 있는 평균 바이트 수 이상의 의심스러운 호스트 또는 호스트 그룹에 대한 정책 설정을 적용합니다.



ICMP 플러드

ICMP Flood(ICMP 플러드) 알람은 소스 호스트가 지난 5분 동안 지나치게 많은 수의 ICMP 패킷을 전송했음을 나타냅니다. 이 알람은 DoS(Denial of Service) 공격 또는 공개적인 스캔 활동을 나타낼 수 있습니다. 이 상황을 해결하려면 어떤 호스트에서 알람이 발생하는지 알아보십시오. 네트워크에서 호스트로 다수의 ping을 전송 중인 관리 서버일 수 있습니다.

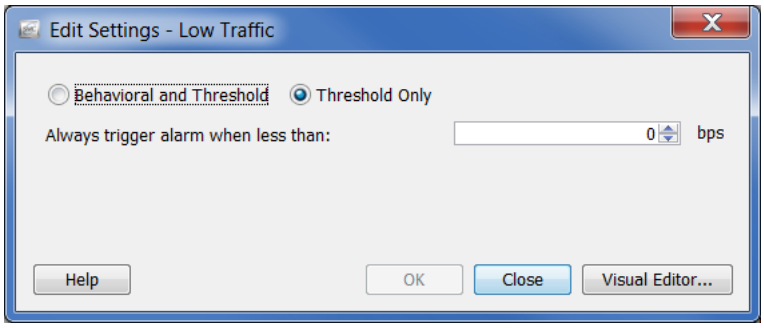
알람을 중지하려면 해당하는 정책에서 **Enabled(활성화됨)** 확인란을 클릭하여 해당 호스트/호스트 그룹에 대한 ICMP 플러드 알람을 비활성화하여 체크 마크를 제거합니다.



낮은 트래픽

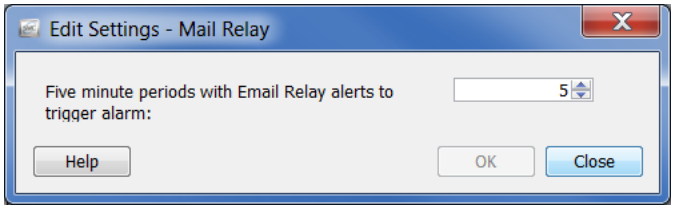
Low Traffic(낮은 트래픽) 알람은 평균 5분이 넘는 호스트 트래픽 속도가 허용되는 최소 트래픽 값 미만으로 떨어진 경우를 나타냅니다. 표시되는 낮은 트래픽 알람의 양이 마음에 들지 않으면 해당하는 정책에서 설정을 조정합니다.

보고되고 있는 평균 바이트 수 이상의 의심스러운 호스트 또는 호스트 그룹에 대한 정책 설정을 적용합니다.



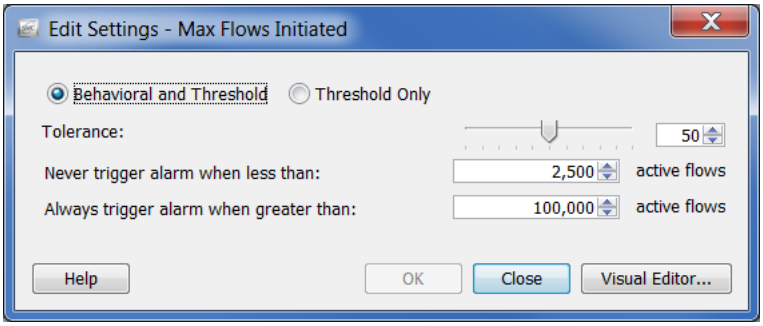
메일 릴레이

Mail Relay(메일 릴레이) 알람은 대상 호스트가 이메일 릴레이로 동작할 수 있음을 나타냅니다. 실제 메일 서버인 경우, 체크 마크를 제거하기 위해 해당하는 정책에서 **Enabled(활성화됨)** 확인란을 클릭하여 해당 호스트/호스트 그룹에 대한 메일 릴레이 알람을 비활성화하여 체크 마크를 제거합니다.



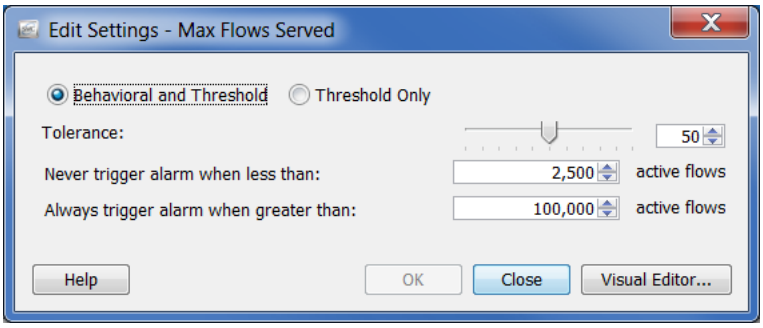
최대 플로우 시작됨

Max Flows Initiated(최대 플로우 시작됨) 알람은 호스트가 허용되는 설정보다 더 많은 플로우를 시작했음을 나타내며 이 숫자는 해당하는 *Always trigger alarm when greater than(다음 값보다 클 경우 항상 알람 트리거)* 정책 설정에 지정되어 있습니다. 특히 도메인 컨트롤러인 경우 이 설정을 적용합니다.



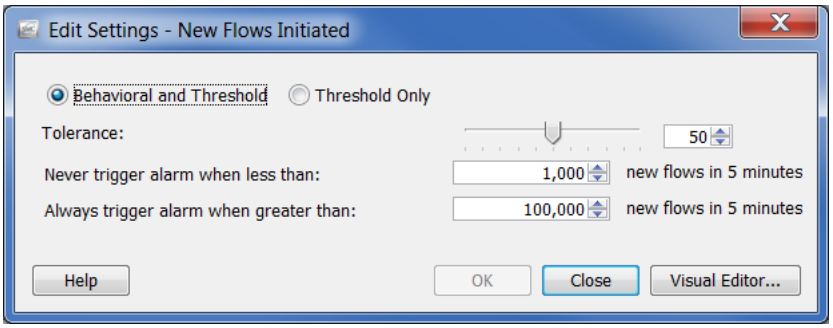
최대 플로우 제공됨

Max Flows Served(최대 플로우 제공됨) 알람은 호스트가 허용되는 설정보다 더 많은 플로우를 제공했음을 나타내며 이 숫자는 해당하는 *Always trigger alarm when greater than(다음 값보다 클 경우 항상 알람 트리거)* 정책 설정에 지정되어 있습니다. 특히 도메인 컨트롤러인 경우 이 설정을 적용합니다.



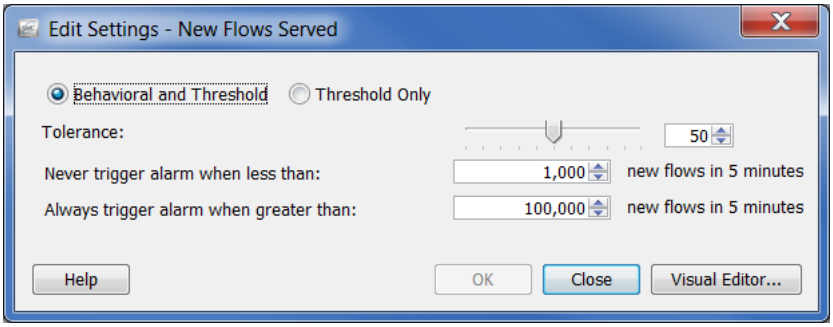
새 플로우 시작됨

New Flows Initiated(새 플로우 시작됨) 알람은 호스트가 5분 동안 시작된 새 플로우의 총 수에 대한 정책 설정을 초과한 것을 나타냅니다. 특히 도메인 컨트롤러인 경우 이 설정을 적용합니다.



새 플로우 제공됨

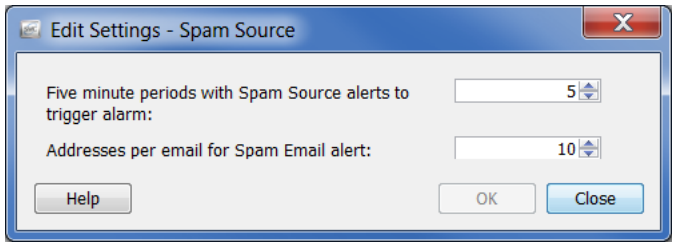
New Flows Served(새 플로우 제공됨) 알람은 호스트가 5분 동안 제공된 새 플로우의 총 수에 대한 정책 설정을 초과한 것을 나타냅니다. 특히 도메인 컨트롤러인 경우 이 설정을 적용합니다.



스팸 소스

Spam Source(스팸 소스) 알람은 소스 호스트가 이메일 스팸을 전송하고 있을 가능성을 나타냅니다. 호스트가 메일 서버인 경우, 해당하는 정책의 **Enabled(활성화됨)** 확인란을 클릭하여 해당 호스트/호스트 그룹에 대한 스팸 소스 알람을 비활성화하여 체크 마크를 제거합니다.

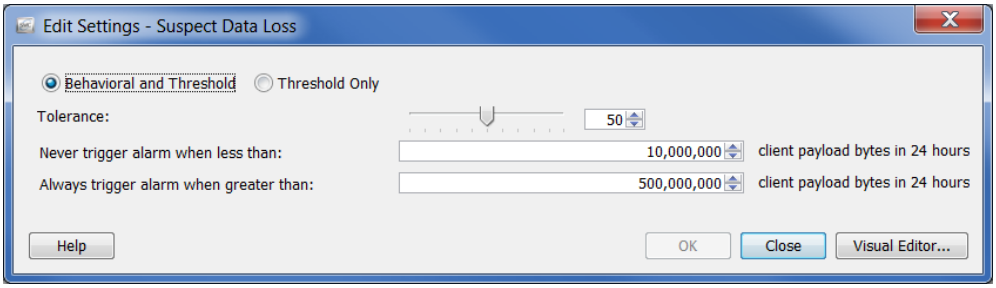
호스트가 메일 서버가 아닌 경우 감염될 수 있습니다.



의심스러운 데이터 손실

Suspect Data Loss(의심스러운 데이터 손실) 알람은 외부 호스트 그룹에 대한 총 TCP 및 UDP 페이로드 데이터가 정책 설정을 초과한 것을 나타냅니다. 표시되는 의심스러운 데이터 손실 알람의 수가 마음에 들지 않으면 알려진 높은 트래픽 외부 호스트 그룹(예: YouTube, Facebook, 비즈니스 파트너)에 대해 이 알람을 비활성화합니다.

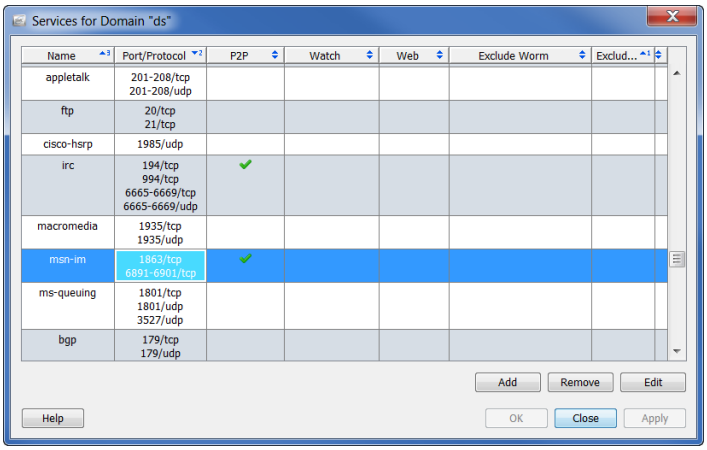
그런 다음 중요한 호스트 또는 호스트 그룹에 대한 정책의 설정을 조정합니다. 보고되고 있는 평균 바이트 수 이상으로 임계값을 올립니다.

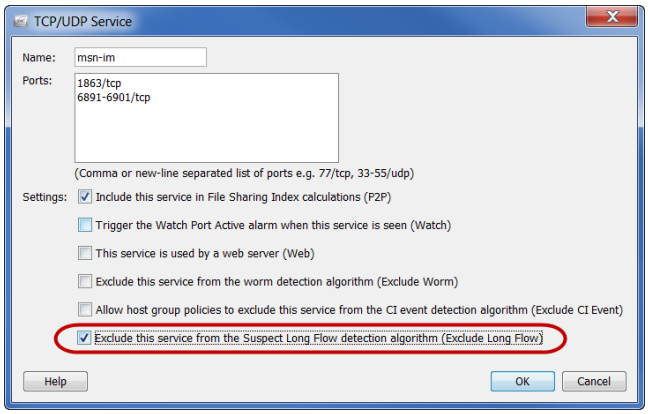


의심스러운 긴 플로우

Suspect Long Flow(의심스러운 긴 플로우) 알람은 내부 호스트와 외부 호스트 간의 IP 통신 시간이 "플로우를 수명이 긴 것으로 지정하는 데 필요한 시간(초)"의 설정을 초과하는 것을 나타냅니다. 이 알람은 스파이웨어, 원격 데스크톱 기술(예: gotomypc.com), VPN, IRC 봇넷 및 기타 기밀 통신 수단과 같은 의심스러운 통신 채널을 탐지합니다. IM 기술을 사용하는 내부 호스트는 플로우가 허용되는 최대값보다 오래 지속되기 때문에 이러한 유형의 알람을 유발하는 경향이 있습니다(기본 = 9시간).

구성된 서비스를 수정하여 Suspect Long Flow(의심스러운 긴 플로우) 알람을 생성하여 AOL AIM(포트 5190), Yahoo IM(TCP 포트 5050) 및 MSN Messenger(TCP 포트 1863) 등의 IM 기술을 제외할 수 있습니다. 메인 메뉴에서 **Configuration(컨피그레이션) > Services(서비스)**를 선택합니다. 해당 도메인에 대한 Services(서비스) 대화 상자가 열립니다.





편집 중인 서비스의 이름을 포함하는 행을 선택한 다음 화면 맨 아래에서 **Edit(편집)**을 클릭합니다. **Exclude this service from the Suspect Long Flow detection algorithm (Exclude Long Flow)(의심스러운 긴 플로우 탐지 알고리즘에서 이 서비스 제외(긴 플로우 제외))** 확인란을 클릭하여 체크 마크를 추가합니다.

또는 비즈니스 파트너 등 권한이 있는 네트워크에 대한 외부 호스트 그룹을 생성한 다음 해당하는 정책에서 Suspect Long Flow(의심스러운 긴 플로우) 알람을 비활성화할 수 있습니다.

참고:

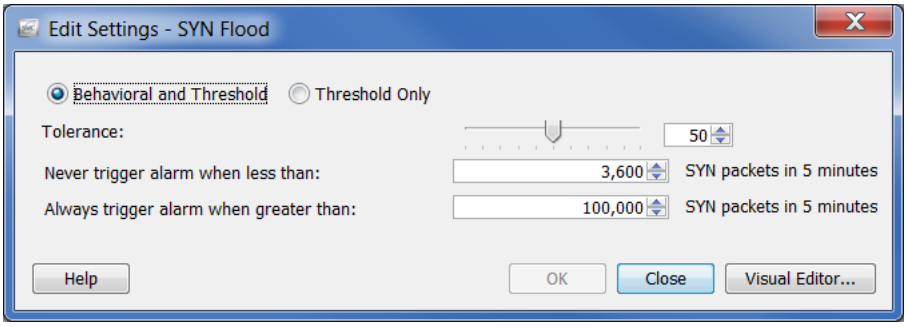
의심스러운 긴 플로우 알람은 클라이언트/서버 관계에 상관없이 항상 내부 호스트에서 발생합니다. 이 알람이 외부 호스트에 대해 비활성화되어 있는 경우, 해당 외부 호스트에 연결된 모든 내부 호스트가 이 알람에서 제외됩니다.

의심스러운 UDP 활동

Suspect UDP Activity(의심스러운 UDP 활동) 알람은 UDP 포트에서 여러 개의 호스트를 스캔하고 있는 호스트가 단일한 대형 패킷을 다른 호스트에 성공적으로 전송했음을 나타냅니다. 이러한 유형의 행동은 SQL Slammer 및 Witty와 같은 대다수 단일 패킷 UDP 기반 웜에서 일관되게 나타납니다. 즉시 이 알람을 조사합니다.

SYN 플러드

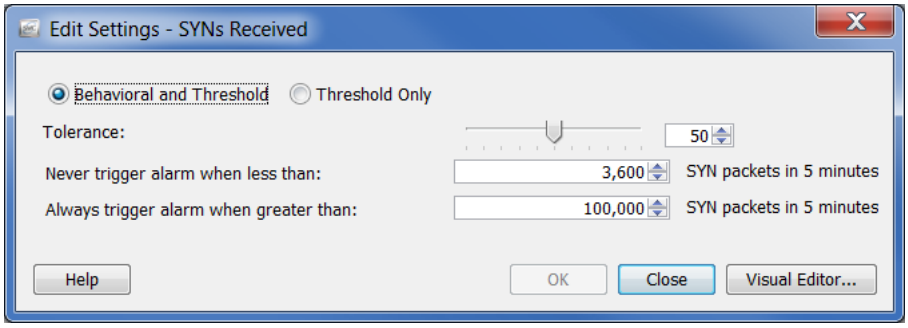
SYN Flood(SYN 플러드) 알람은 호스트가 5분 동안 지나치게 많은 수의 TCP 연결 요청(SYN 패킷)을 전송했음을 나타냅니다. DOS 공격 또는 공개적인 스캔 활동이 진행 중인지 여부를 확인하려면 이 알람을 조사합니다.



SYN 수신됨

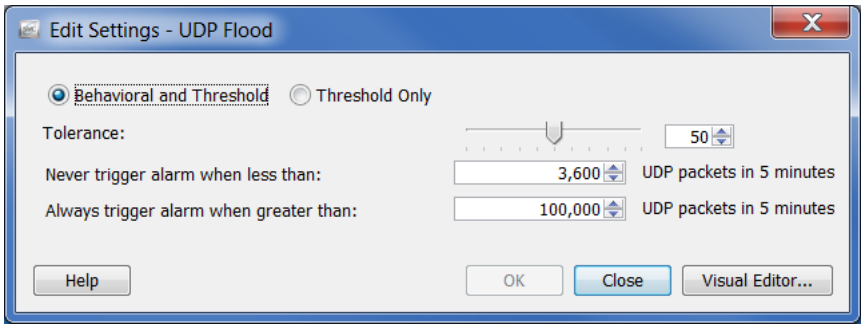
SYNs Received(SYN 수신됨) 알람은 호스트가 5분 동안 지나치게 많은 수의 응답되지 않은 TCP 연결 요청(SYN 패킷)을 수신했음을 나타냅니다. 이 알람은 분산된(다대일) DoS 공격을 나타낼 수 있습니다.

그러나, 서버에서 많은 수의 SYN 패킷을 수신하는 것은 일반적입니다. 이 경우 *Never trigger alarm when less than(다음 값 미만일 경우 알람을 트리거하지 않음)* 설정을 표시되는 알람의 평균 수 이상으로 높입니다. 다른 서버보다 SYN 패킷을 더 많이 수신하는 서버를 개별 호스트 그룹(웹 서버와 애플리케이션 서버 비교)으로 분리할 수 있습니다.



UDP 플러드

UDP Flood(UDP 플러드) 알람은 소스 IP가 지난 5분 동안 지나치게 많은 수의 UDP 패킷을 전송했음을 나타냅니다. DOS 공격 또는 공개적인 스캔 활동이 진행 중인지 여부를 확인하려면 이 알람을 조사합니다.



웜 활동

Worm Activity(웜 활동) 알람은 호스트가 스캔되었으며 둘 이상의 서브넷 전체에서 특정 포트에 연결되었음을 나타냅니다. 이 알람의 세부사항 섹션에서는 활동이 관찰된 대상 포트를 지정합니다.

도메인 컨트롤러가 UDP 포트와 ping 스캔에서 주소 스캔을 수행하는 것은 일반적입니다. Worm Activity(웜 활동) 알람이 도메인 컨트롤러를 사용하는 호스트 그룹에서 발생할 경우, 해당하는 정책의 상위 관심 지표(CI) 알람에 대한 Security Events(보안 이벤트) 탭에서 **Addr_Scan/udp** 및 **Ping** 확인란의 체크마크를 제거하여 이 알람이 발생하는 것을 방지할 수 있습니다.

13

문서 작업

개요

이 장에서는 SMC 문서를 특정 레이아웃 및 필터 설정 세트와 함께 저장하고 문서를 로그인 문서 리스트에 추가하며 DAR 파일을 생성하고 문서를 공유하며 정기적으로 문서를 생성하는 방법과 문서를 다른 사용자에게 이메일로 전송하는 방법 등의 프로세스에 대해 설명합니다.

이 장은 다음 항목으로 구성되어 있습니다.

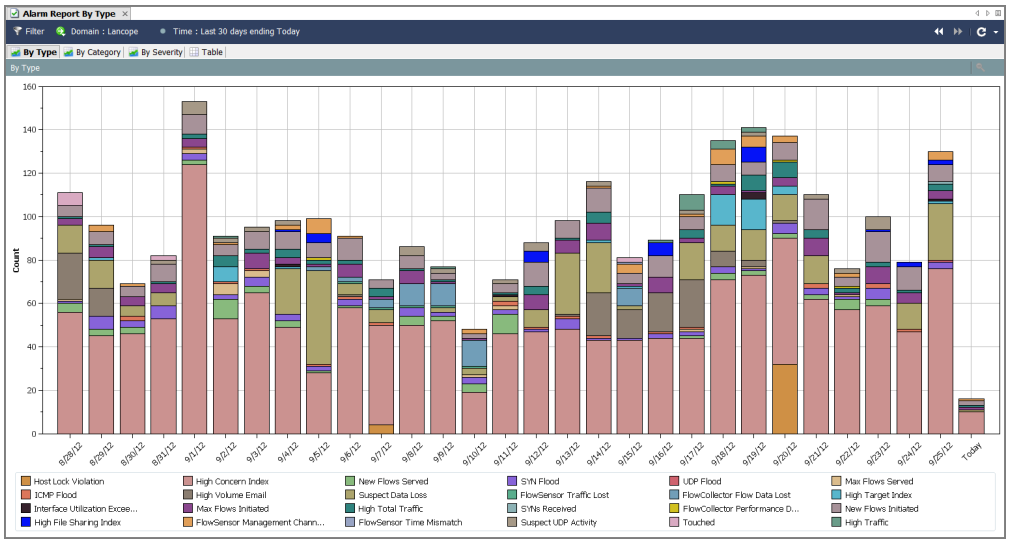
- 문서 저장
- 문서 공유
- 문서 일정 지정

문서 저장

SMC 문서의 레이아웃을 재정렬한 뒤 나중에 사용하기 위해 해당 레이아웃을 저장하려는 경우, 문서를 저장하십시오. 문서를 저장할 경우 언제든지 검색할 수 있도록 SMC 어플라이언스에 저장됩니다.

문서를 저장하려면 다음 단계를 수행하십시오.

1. 저장할 문서를 엽니다. 예에서와 같이 Alarm Report By Type(유형별 알람 보고서) 문서가 열립니다.



2. 원하는 대로 레이아웃 또는 필터 설정을 변경합니다.
3. (선택사항) SMC 메인 메뉴에서 **File(파일) > Print Settings(인쇄 설정)**를 선택하고 열리는 대화 상자에서 문서를 인쇄할 때마다 어떻게 표시할지 구성합니다. **OK(확인)**를 클릭하여 변경 사항을 저장합니다.
4. (선택사항) 문서가 PDF로 표시되는 방식을 확인하려면 **File(파일) > Print Preview(인쇄 미리보기)**를 선택합니다.

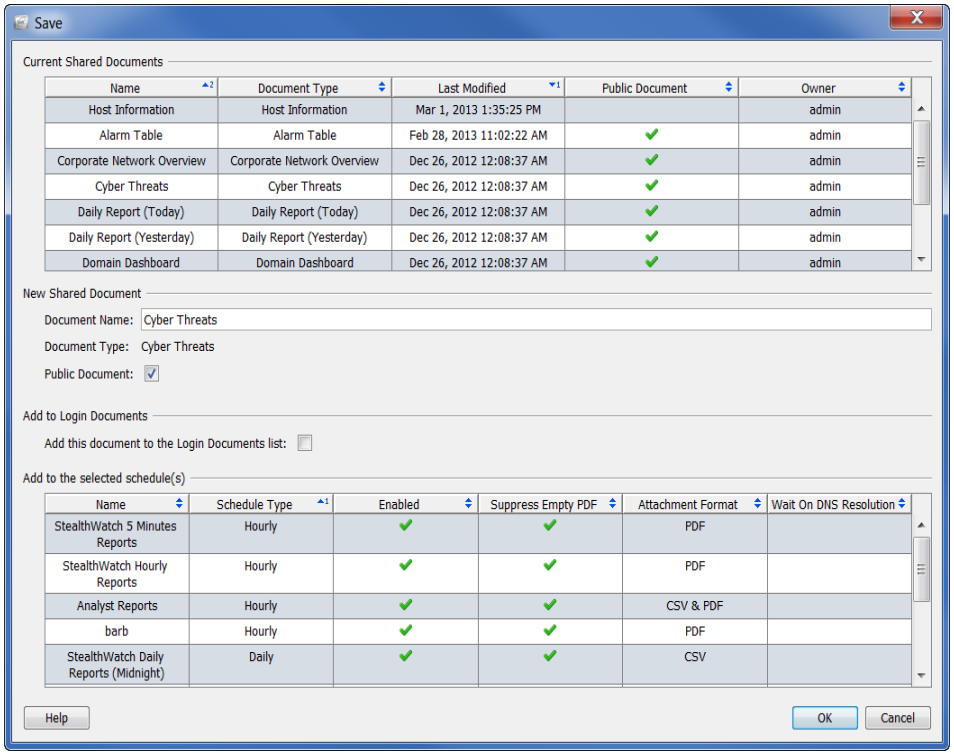
참고:

문서 레이아웃을 변경하고 변경 사항을 유지하려면(예: 열 위치 변경 또는 표시되는 열 변경) File(파일) > Use Settings as Default(설정을 기본값으로 사용)를 선택합니다. 이러한 변경 사항은 다음에 문서를 열 때 적용됩니다.

5. 다음 중 하나를 수행합니다.
   - 동일한 이름을 사용하여 이전 버전을 바꾸려는 경우 SMC 메인 메뉴에서 **File(파일) > Save(저장)**를 선택합니다.
   - 다음과 같은 경우, SMC 메인 메뉴에서 **File(파일) > Save As(다른 이름으로 저장)**를 선택합니다.

- 문서의 사본을 새 이름으로 저장하려는 경우
- 새 문서를 만든 다음 이 문서를 처음으로 저장하는 경우

Save(저장) 대화 상자가 열립니다.



6. Name(이름) 필드에 쉽게 알아볼 수 있는 문서 이름을 입력합니다. (사용자 본인 이름을 사용하는 것을 권장합니다.)
7. (선택사항) 다른 사용자가 자신의 이름으로 이 문서를 열 수 있도록 설정하려는 경우, **Public(공용)** 확인란을 선택합니다.

참고:

공용 문서에 대한 자세한 내용은 314페이지의 "공용 문서"를 참조하십시오.

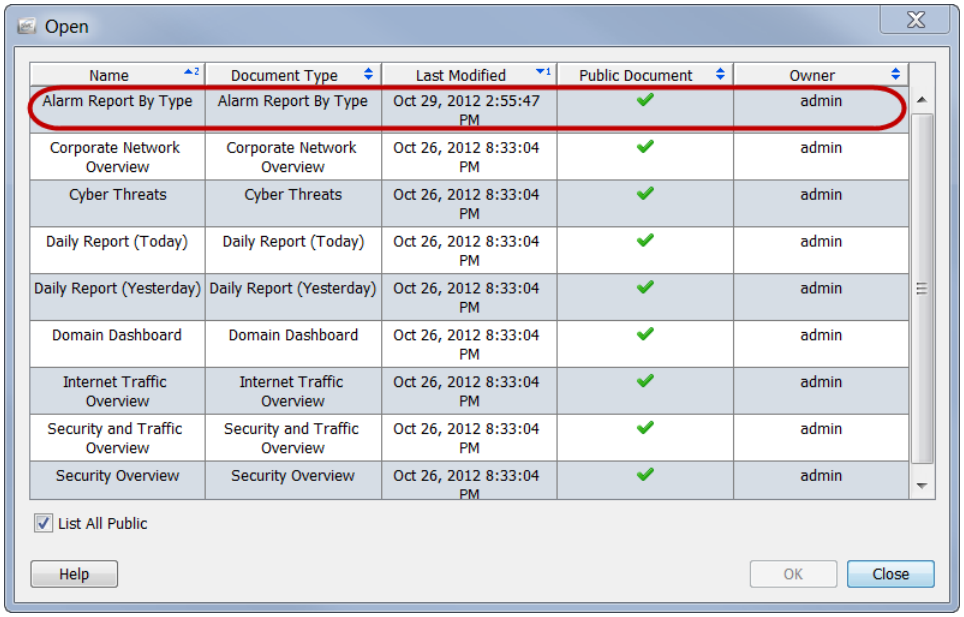
8. (선택사항) 사용자 이름으로 SMC 클라이언트 인터페이스에 로그인할 때마다 자동으로 문서가 열리도록 설정하려면 “Add this document to the Login Documents list(로그인 문서 리스트에 이 문서 추가)” 확인란을 선택합니다.

참고:

로그인 문서에 대한 자세한 내용은 310페이지의 "로그인 문서"를 참조하십시오.

9. **OK(확인)**를 클릭합니다. 문서가 SMC 어플라이언스에 저장됩니다. 이제 SMC 액세스가 가능한 모든 컴퓨터에서 지정한 레이아웃 및/또는 필터 설정으로 사용자 이름 아래에서 이 문서를 열 수 있습니다.

10. 이 문서를 열려면 SMC 메인 메뉴에서 **File(파일) > Open(열기)**을 선택합니다. Open(열기) 대화 상자가 열립니다.



11. 문서를 선택하고 **OK(확인)**를 클릭합니다.

참고:

기본적으로 사용자 이름 아래에 저장한 문서만 나타납니다. 다른 사용자가 만든 문서를 포함하여 모든 문서를 나열하려면 List All Public(모든 공용 문서 나열) 확인란을 선택합니다.

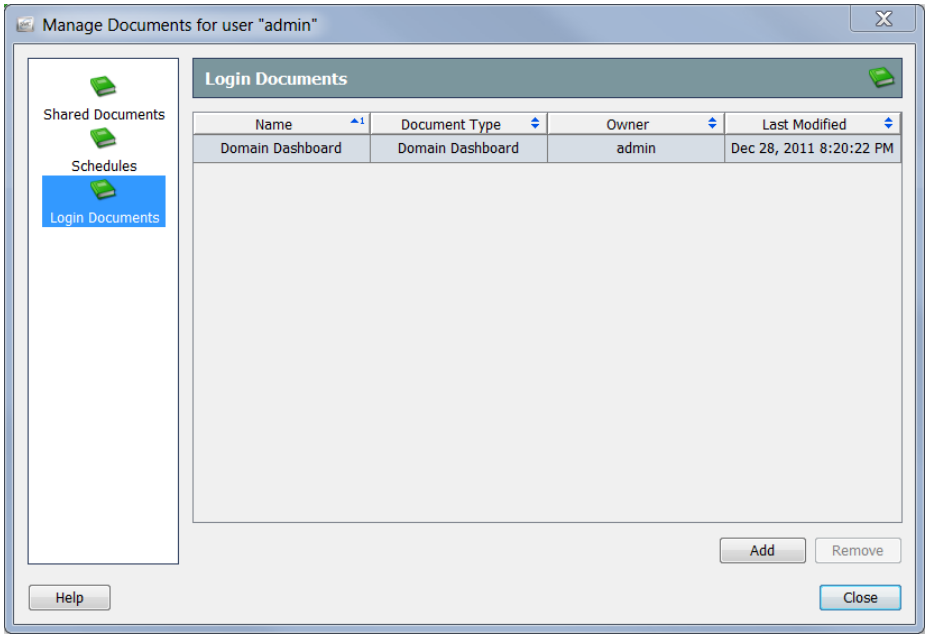
로그인 문서

어떤 문서든 로그인 문서 리스트에 추가할 수 있습니다. 로그인 문서는 SMC 클라이언트 인터페이스에 로그인할 때마다 자동으로 열립니다. 이 기능을 사용하지 않으면 정기적으로 문서를 수동으로 열어야 하므로 이 기능은 문서를 확인하는 데 유용합니다.

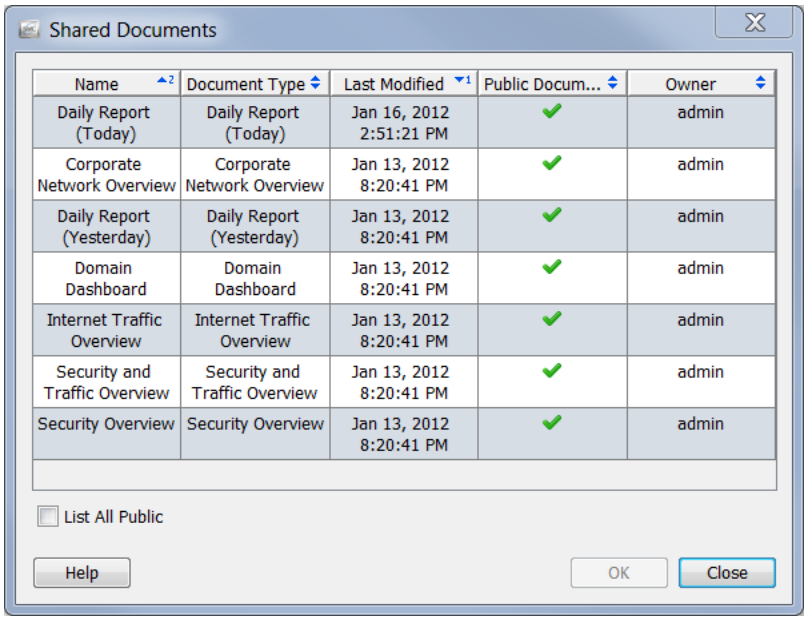
문서를 로그인 문서로 설정하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **File(파일) > Manage Documents(문서 관리)**를 선택합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.

2. **Login Documents(로그인 문서)** 아이콘을 클릭합니다. Login Documents(로그인 문서) 페이지가 열립니다.



3. **Add(추가)**를 클릭합니다. Shared Documents(공유 문서) 대화 상자가 열립니다.



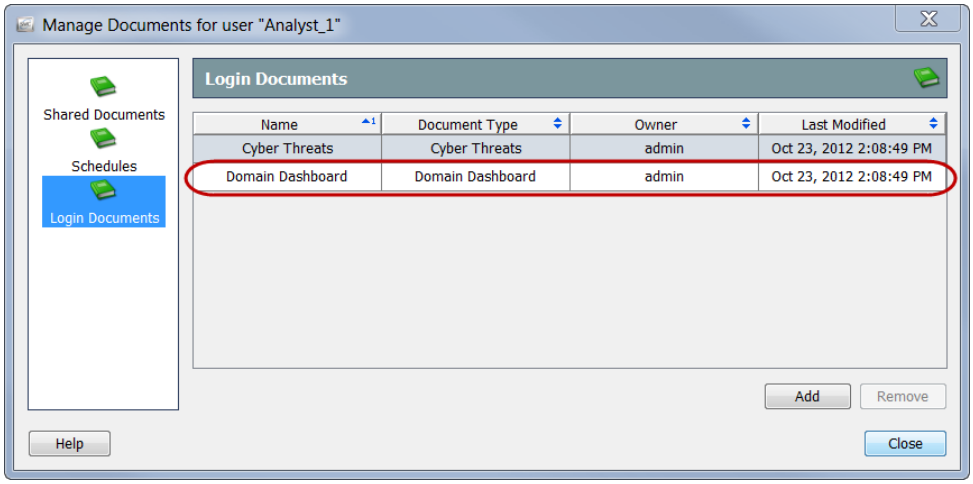
4. 다른 사용자가 저장한 모든 공용 문서를 보려면 "List All Public(모든 공용 문서 나열)" 확인란을 선택합니다.

5. 사용자의 로그인 문서 리스트에 추가할 문서를 선택합니다. 이 예에서는 Domain Dashboard(도메인 대시보드) 문서를 선택합니다.

참고:

둘 이상의 문서를 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 문서를 클릭합니다. 문서의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 문서를 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 문서를 클릭합니다.

6. **OK(확인)**를 클릭합니다. Shared Documents(공유 문서) 대화 상자가 닫힙니다. 선택한 문서가 사용자의 로그인 문서 리스트에 나타납니다.



7. **Close(닫기)**를 클릭하여 Manage Documents(문서 관리) 대화 상자를 종료합니다.

문서 공유

다른 사용자와 문서를 공유하는 방법에는 다음과 같은 두 가지 방법이 있습니다.

- DAR 파일로 내보내기
- 공용으로 설정

DAR 파일

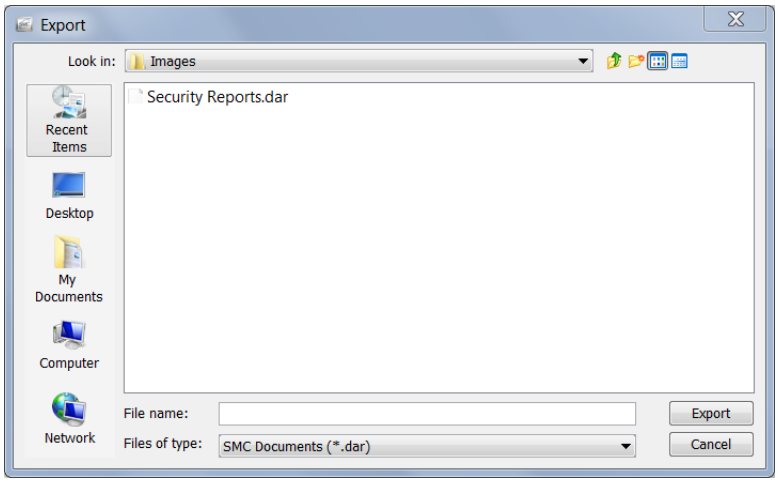
DAR 파일로 문서를 내보내면 문서로 다음과 같은 작업을 수행할 수 있습니다.

- 컴퓨터의 하드 드라이브에 문서 복사
- SMC 어플라이언스에 대한 액세스 권한이 있는 다른 컴퓨터에서 사용하기 위해 문서를 플래시 드라이브에 복사
- 다른 사람과 문서 공유

DAR 파일 내보내기

문서를 DAR 파일로 내보내려면 다음 단계를 수행하십시오.

1. 내보낼 문서를 엽니다.
2. 원하는 대로 레이아웃 또는 필터 설정을 변경합니다.
3. SMC 메인 메뉴에서 **File(파일) > Export to DAR file(DAR 파일로 내보내기)**을 선택합니다. Export(내보내기) 대화 상자가 열립니다.



4. 문서를 내보낼 위치로 이동합니다.
5. File name(파일 이름) 필드에 파일 이름을 입력합니다.

6. **Export(내보내기)**를 클릭합니다. 문서는 선택한 위치에 DAR 파일로 저장됩니다. 또한, 문서 탭의 이름이 새로 지정됩니다.

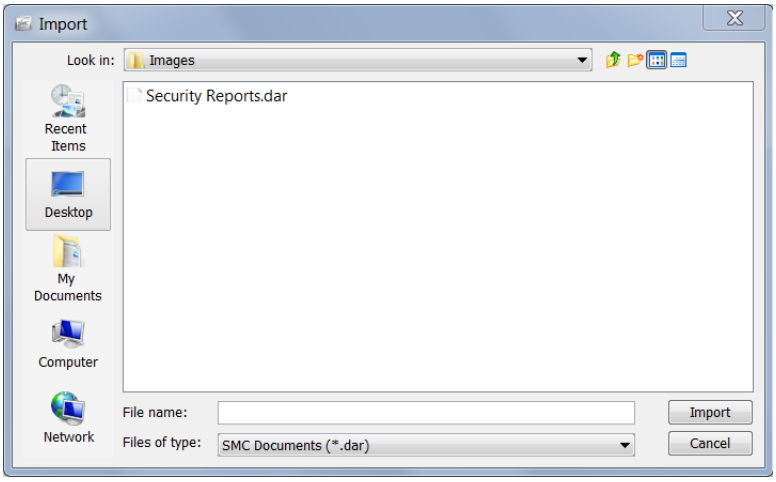
참고:

문서 탭 위에 커서를 올려 놓으면 툴팁이 나타나 원본 문서 이름과 생성한 사람("소유한 사람") 등 문서에 대한 세부사항이 표시됩니다.

DAR 파일 가져오기

누군가가 문서를 DAR 파일로 내보낸 후 사용자에게 제공한 경우, 사용자는 이 문서를 가져와 SMC 클라이언트 인터페이스에서 언제든지 열 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **File(파일) > Import DAR file(DAR 파일 가져오기)**을 선택합니다. Import(가져오기) 대화 상자가 열립니다.



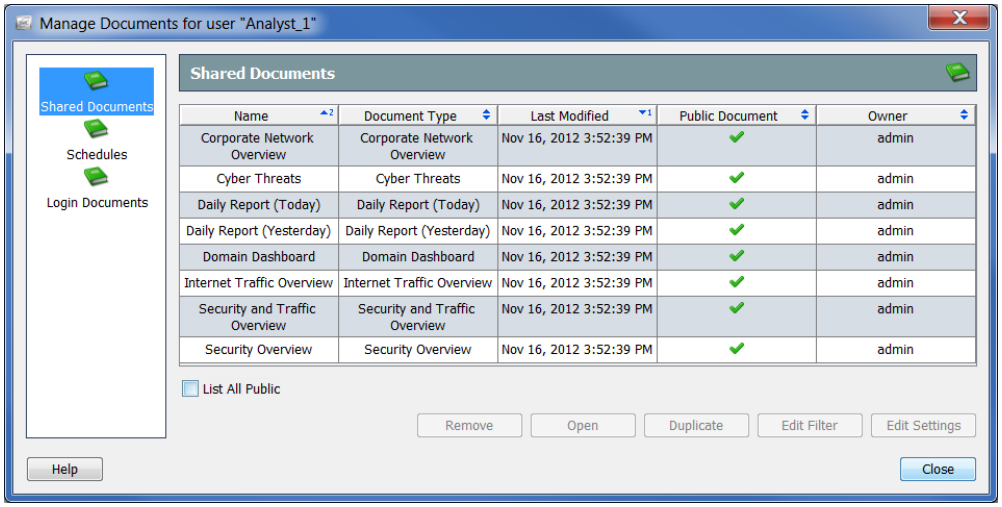
2. DAR 파일이 있는 위치로 이동합니다.
3. DAR 파일을 선택합니다.
4. **Import(가져오기)**를 클릭합니다. SMC 클라이언트 인터페이스에서 문서가 열립니다.

공용 문서

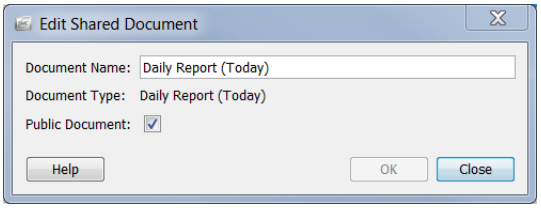
공용 문서를 만들 경우, SMC 어플라이언스에 대한 액세스 권한이 있는 다른 사용자가 사용자 이름 아래에서 문서를 볼 수 있도록 합니다.

308페이지의 "문서 저장"에 설명된 대로 문서를 저장할 때 문서를 공용으로 설정할 수 있습니다. 다음 단계를 완료하여 이전에 저장한 문서를 공용으로 설정할 수 있습니다.

1. 메인 메뉴에서 **File(파일) > Manage Documents(문서 관리)**를 선택합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.



2. **Shared Documents(공유 문서)** 아이콘을 클릭합니다. Shared Documents(공유 문서) 페이지가 열립니다.
3. 원하는 문서를 선택합니다.
4. **Edit Settings(설정 편집)**를 클릭합니다. Edit Settings(설정 편집) 대화 상자가 열립니다.



5. **Public Document(공용 문서)** 확인란을 선택합니다.
6. **OK(확인)**를 클릭하여 Edit(편집) 대화 상자를 종료합니다.
7. **Close(닫기)**를 클릭하여 Manage Documents(문서 관리) 대화 상자를 종료합니다.

SMC 클라이언트 인터페이스에 대한 액세스 권한이 있는 사용자는 공용으로 설정된 이 문서 및 기타 다른 문서를 볼 수 있습니다.

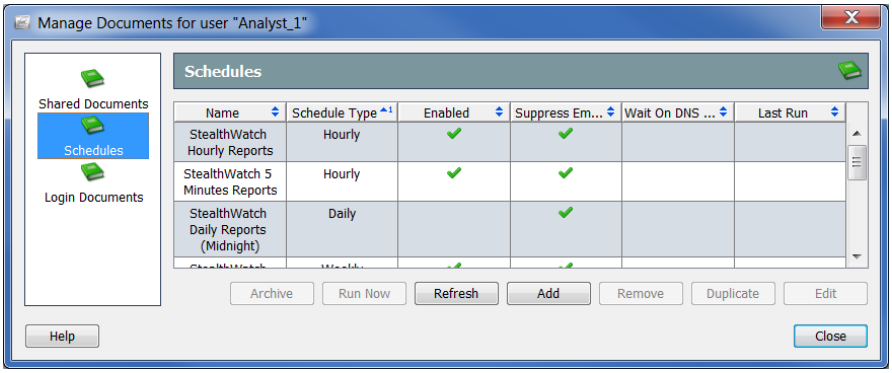
문서 일정 지정

항상 동일한 설정(예: 필터, 레이아웃, 시간 간격)을 사용하여 문서를 자동으로 생성하려는 경우가 있을 수 있습니다. 이를 위해 원하는 설정을 포함하는 일정에 문서를 추가해야 합니다.

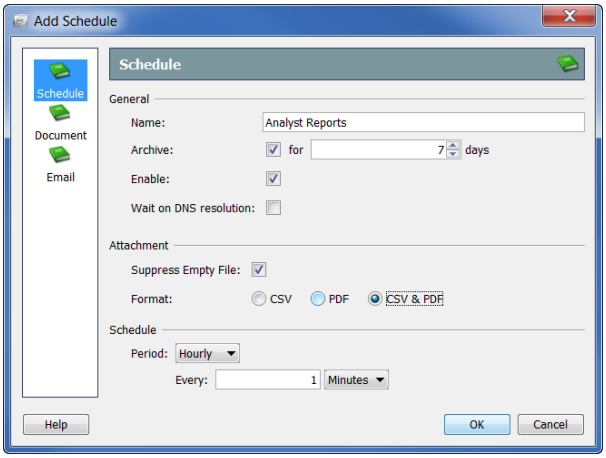
새 일정 추가

계정에 새 일정을 추가하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **File(파일) > Manage Documents(문서 관리)**를 선택합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.



2. **Schedules(일정)** 아이콘을 클릭합니다. Schedules(일정) 페이지가 열립니다.
3. **Add(추가)**를 클릭합니다. Add Schedule(일정 추가) 대화 상자가 열립니다.



4. **Schedule(일정)** 아이콘을 클릭합니다. Schedule(일정) 페이지가 열립니다.

5. Name(이름) 필드에 일정 이름을 입력합니다. 이 예에서는 일정을 "Analyst Reports(분석가 보고서)"라고 하겠습니다.

6. 다음 테이블에서와 같이 General(일반) 섹션에서 파라미터를 정의합니다.

원하는 작업	다음을 선택
SMC 데이터베이스에서 이 일정에 따라 생성된 문서 저장	**Archive(아카이브)** 확인란. 그런 다음 해당하는 드롭다운 리스트를 클릭하고 문서를 저장하려는 일수를 선택합니다.
이 일정을 만드는 즉시 활성화	**Enable(활성화)** 확인란.
문서에서 참조된 IP 주소가 이름으로 확인될 때까지 시스템이 예약한 문서의 생성을 대기하도록 설정	"Wait on DNS resolution(DNS 확인에서 대기)" 확인란. **참고:** 이 기능을 활성화하면 문서 생성이 지연될 수 있습니다. 각 IP 주소는 확인하는 데 최대 2초가 걸릴 수 있습니다. IP 주소가 2초 이내에 확인되지 않는 경우, 해당 IP 주소는 DNS 이름 없이 표시됩니다.
SMC가 데이터 없이 생성된 문서를 아카이브하거나 이메일로 발송하는 것을 방지	"Suppress Empty File(빈 파일 표시 안 함)" 확인란.
인쇄할 문서 유형 지정	▶ CSV(쉼표로 구분된 값) - 생성된 문서에 포함된 테이블 데이터만 인쇄하려는 경우 이 옵션을 선택합니다. • 각 테이블은 CSV 파일에 포함됩니다. • 다른 모든 데이터 유형(예: 지도, 그래프, 차트)은 인쇄하지 않습니다. • 각 문서의 모든 CSV 파일은 한 파일로 압축됩니다(즉, 문서당 하나의 압축된 파일). • 모든 압축된 파일은 선택한 일정에 따라 생성된 문서 사본을 이메일로 수신하도록 지정되어 있는 각 사용자에게 이메일로 발송됩니다.
	▶ PDF - 생성된 문서에 포함된 모든 데이터를 인쇄하려는 경우 이 옵션을 선택합니다. • 생성된 각 문서는 PDF 파일에 포함됩니다. • 각 PDF 파일은 한 파일로 압축됩니다. • 모든 압축된 파일은 선택한 일정에 따라 생성된 문서 사본을 이메일로 수신하도록 지정되어 있는 각 사용자에게 이메일로 발송됩니다.
-계속-	

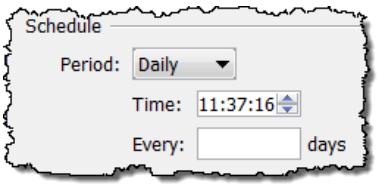
원하는 작업	다음을 선택
인쇄할 문서 유형 지정	▶ CSV 및 PDF - CSV 형식으로 테이블 데이터를 인쇄하고 PDF 형식으로 기타 모든 데이터를 인쇄하려는 경우 이 옵션을 선택합니다. • 각 테이블은 CSV 파일에 포함됩니다. • 생성된 각 문서의 모든 기타 데이터 유형은 한 PDF 파일에 포함됩니다(즉, 문서당 하나의 PDF 파일). • 문서에 포함된 모든 파일은 한 파일로 압축됩니다(즉, 문서당 하나의 압축된 파일). • 모든 압축된 파일은 선택한 일정에 따라 생성된 문서 사본을 이메일로 수신하도록 지정되어 있는 각 사용자에게 이메일로 발송됩니다.

참고:

- Print Settings(인쇄 설정) 대화 상자의 Pages(페이지) 페이지에서 테이블을 활성화하지 않으면, 일정이 CSV 파일을 만들도록 구성된 경우에도 일정에서 해당 테이블에 대한 CSV 파일을 만들지 않습니다.
- Print Settings(인쇄 설정) 대화 상자의 Print Setup(인쇄 설정) 페이지에서 필터 요약 옵션을 지정할 경우 필터 요약이 생성된 문서에 포함됩니다. 참고로, "As the first page(첫 번째 페이지로)" 옵션 또는 "As the last page(마지막 페이지로)" 옵션(Cover Sheet(표지) 섹션) 중 하나를 선택하여 Filter summary(필터 요약) 확인란(Cover Sheet Options(표지 옵션) 섹션)을 활성화해야 옵션을 선택할 수 있습니다.

7. Period(기간) 드롭다운 리스트를 클릭하고 SMC에서 이 일정과 연결된 문서를 생성하는 빈도를 선택합니다. 예약된 문서를 매시간, 매일, 매주 또는 매월 생성하도록 선택할 수 있습니다. 선택하는 옵션에 따라 세부사항을 지정할 수 있는 다양한 필드가 나타납니다.

   예를 들어, **Daily(매일)**를 선택하면 일정을 실행하려는 날짜의 시간과 일정을 매일, 2일에 한 번, 3일에 한 번 등으로 실행할지 여부를 지정할 수 있는 2개의 필드가 나타납니다.

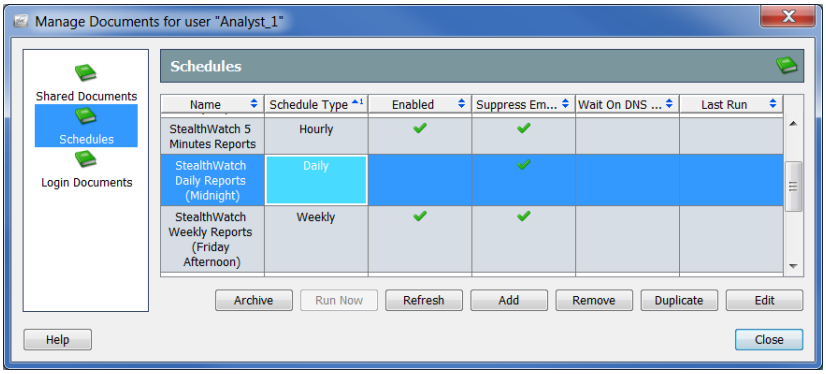


8. 320페이지의 "일정에 문서 추가"를 진행합니다.

기존 일정 편집

계정에 연결하려는 일정이 이미 있는 경우 다음 단계를 완료하여 일정을 편집합니다.

1. SMC 메인 메뉴에서 **File(파일) > Manage Documents(문서 관리)**를 선택합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.

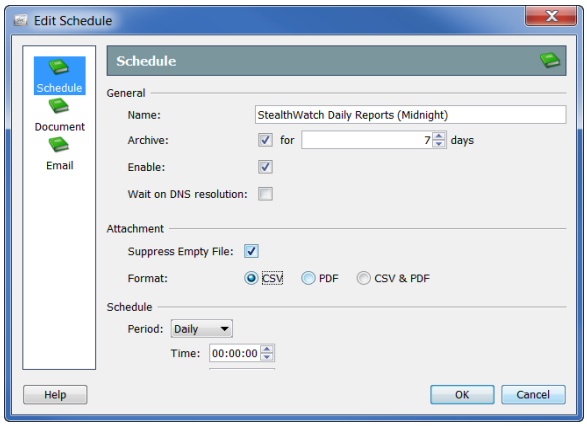


2. **Schedules(일정)** 아이콘을 클릭합니다. Schedules(일정) 페이지가 열립니다.
3. 편집하려는 일정을 선택합니다.

참고:

위의 예에서는 Stealthwatch Daily Report(Midnight)(Stealthwatch 일일 보고서(자정)) 일정을 선택했습니다. Enabled(활성화됨) 열에 체크 마크가 없으면 이 일정이 사용자 계정에 대해 활성화되지 않았음을 의미합니다. 일정이 활성화되지 않으면 이 일정에 포함된 문서가 생성되지 않습니다.

4. **Edit(편집)**을 클릭합니다. Edit Schedule(일정 편집) 대화 상자가 열립니다.

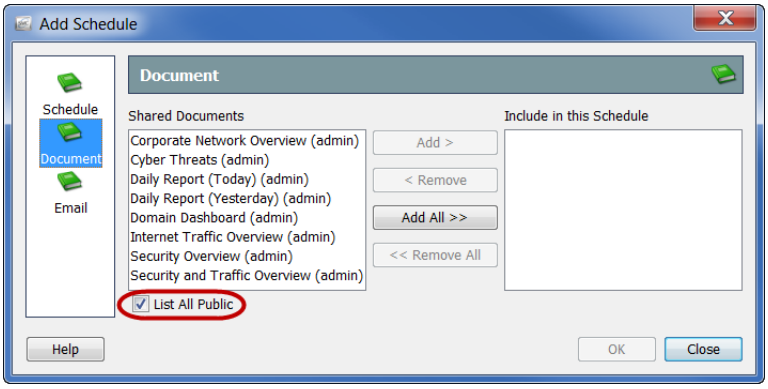


5. **Schedule(일정)** 아이콘을 클릭합니다. Schedule(일정) 페이지가 열립니다.
6. 원하는 대로 설정을 변경합니다. 옵션에 대한 자세한 내용을 확인하려면 **Help(도움말)**를 클릭하십시오.
7. 이 장의 다음 내용인 "일정에 문서 추가"를 계속 진행합니다.

일정에 문서 추가

하나 이상의 문서를 일정에 추가하려면 다음 단계를 수행하십시오.

1. Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자에서 **Document(문서)** 아이콘을 클릭합니다. Document(문서) 페이지가 열립니다.

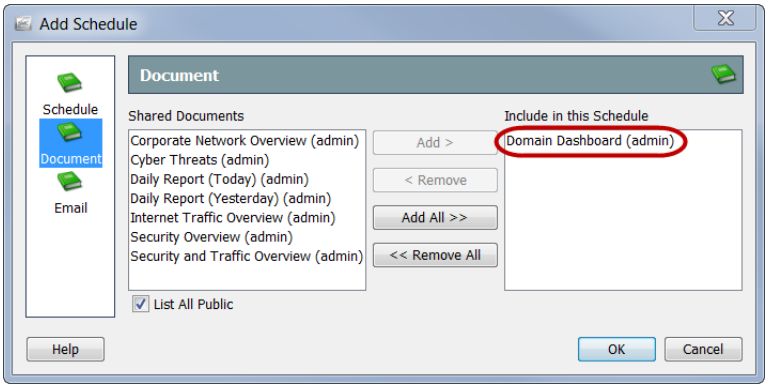


2. 아직 선택하지 않은 경우 **List All Public(모든 공용 문서 나열)** 확인란을 선택합니다. (자세한 내용은 314페이지의 "공용 문서"를 참조하십시오.)
3. 일정에 추가할 문서를 선택합니다. 이 예에서는 Domain Dashboard(도메인 대시보드) 문서를 선택합니다.

참고:

둘 이상의 문서를 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 문서를 클릭합니다. 문서의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 문서를 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 문서를 클릭합니다.

4. **Add(추가)**를 클릭합니다. 문서가 Include in This Schedule(이 일정에 포함) 필드에 나타납니다.



5. SMC가 예약된 문서를 자동으로 이메일로 보내도록 설정하시겠습니까?
   - 대답이 예인 경우 323페이지의 "일정에 사용자 이메일 주소 추가"를 계속 진행합니다.
   - 대답이 아니요인 경우 **OK(확인)**를 클릭하여 정보를 저장하고 Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자를 종료한 다음 Manage Documents(문서 관리) 대화 상자로 돌아갑니다.
6. 나머지 대화 상자를 닫습니다.

예약된 문서 이메일로 보내기

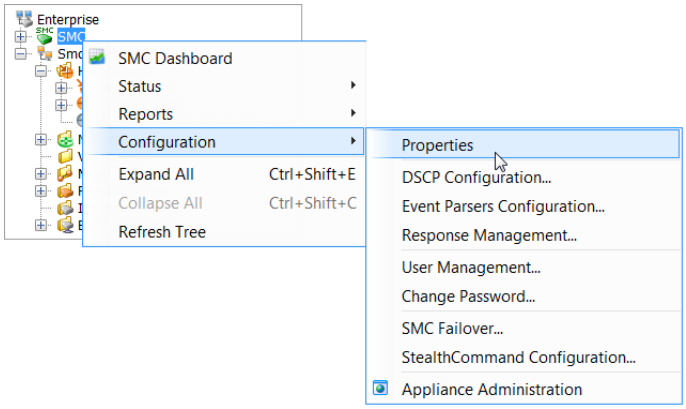
SMC가 예약된 문서를 사용자에게 자동으로 이메일로 보내도록 설정하려는 경우 다음 2가지 절차를 완료하십시오.

1. SMC에 이메일 서버의 IP 주소를 추가합니다. (다음 섹션인, "SMC에 이메일 서버 추가" 섹션을 참조하십시오.)
2. 일정에 사용자 이메일 주소를 추가합니다. (323페이지의 "일정에 사용자 이메일 주소 추가"를 참조하십시오.)

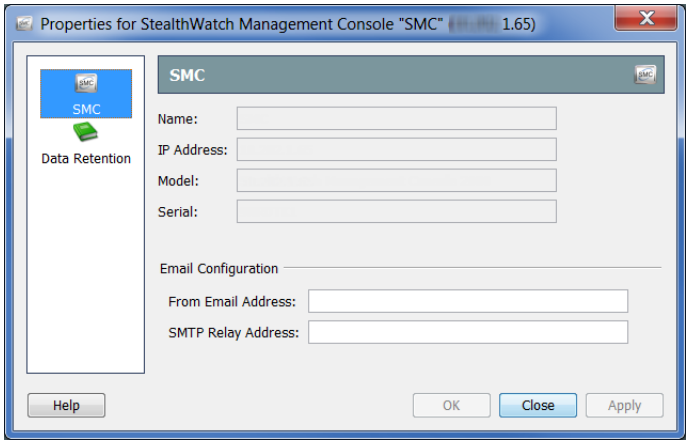
SMC에 이메일 서버 추가

이전에 SMC에 이메일 서버의 IP 주소를 추가하지 않은 경우 먼저 이 작업을 수행해야 SMC에서 예약된 문서를 이메일로 보낼 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

1. Enterprise(엔터프라이즈) 트리에서 **SMC** 브랜치를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **Configuration(컨피그레이션) > Properties(속성)**를 선택합니다. Properties(속성) 대화 상자가 열립니다.



2. **SMC** 아이콘을 클릭합니다. SMC 페이지가 열립니다.



3. (선택사항) From Email Address(보내는 사람 이메일 주소) 필드에서 다음 형식을 사용하여 주소를 입력합니다.

   [FromUser]@[hostname].[domain]

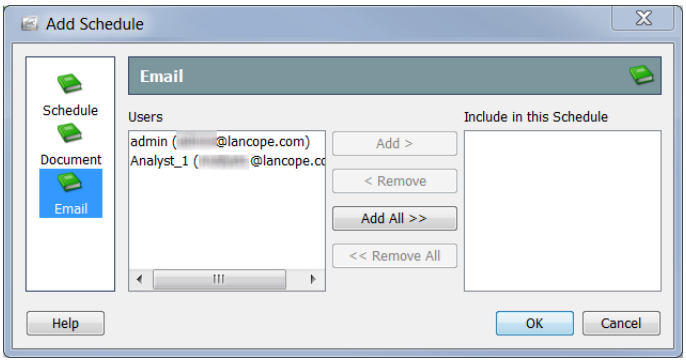
4. SMTP Relay Address(SMTP 릴레이 주소) 필드에서 이메일 서버의 IP 주소를 입력합니다.

5. **OK(확인)**를 클릭하여 정보를 저장하고 Properties(속성) 대화 상자를 닫습니다.

일정에 사용자 이메일 주소 추가

SMC에서 예약된 문서를 사용자에게 자동으로 이메일로 보내도록 설정하려는 경우 다음 단계를 완료하여 일정에 이메일 주소를 추가해야 합니다.

1. Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자에서 **Email(이메일)** 아이콘을 클릭합니다. Email(이메일) 페이지가 열립니다.



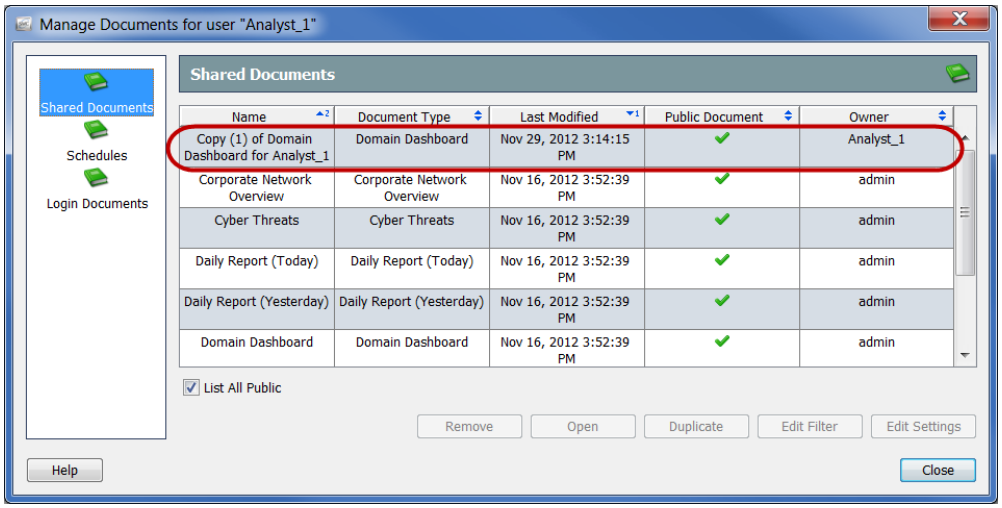
2. Users(사용자) 필드에서 이메일 주소를 선택합니다.
3. **Add(추가)**를 클릭합니다. 이메일 주소가 Include in This Schedule(이 일정에 포함) 필드에 나타납니다.
4. **OK(확인)**를 클릭하여 정보를 저장하고 Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자를 종료한 다음 Manage Documents(문서 관리) 대화 상자로 돌아갑니다.
5. 나머지 대화 상자를 닫습니다.

공유 문서 사전 필터링

예약별로 공유 문서가 생성될 때 해당 필터 설정을 자동으로 사용하도록 모든 공유 문서의 필터 설정을 편집할 수 있습니다.

편집 내용은 다음 방법 중 하나로 저장됩니다.

- 문서 소유자가 아닌 경우, 원본 문서는 수정되지 않은 상태로 유지되며 중복 문서가 새 필터 설정으로 생성됩니다. 중복 문서에만 새 필터 설정이 포함됩니다.



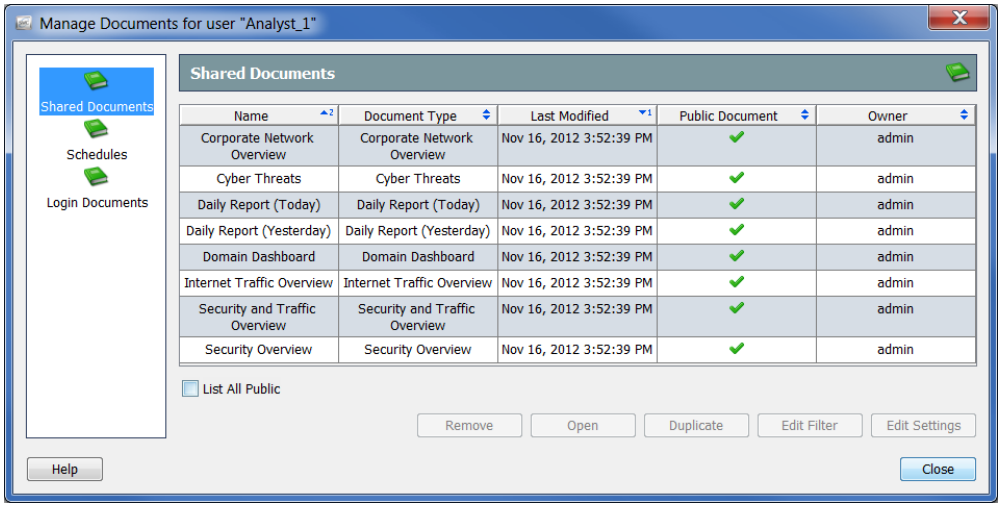
- 문서의 소유자인 경우 새 필터 설정이 원본 문서에서 적용됩니다. 이때부터 이 문서에 대한 액세스 권한을 가진 누구나 언제든지 이 문서를 생성하고 열 수 있으며 문서에는 새 필터 설정이 적용됩니다.

예약별로 공유 문서가 생성될 때 해당 필터 설정을 자동으로 사용하도록 공유 문서의 필터 설정을 편집할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

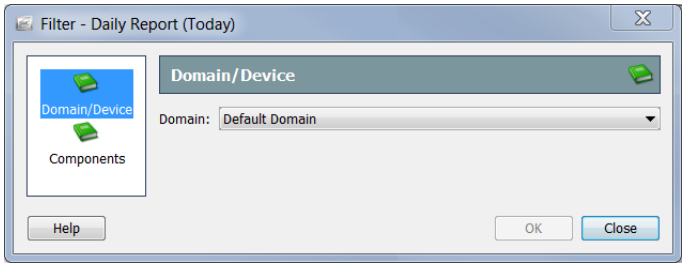
참고:

문서 필터링에 대한 자세한 내용은 3장, "SMC 클라이언트 인터페이스 탐색"의 "문서 데이터 필터링"을 참조하십시오.

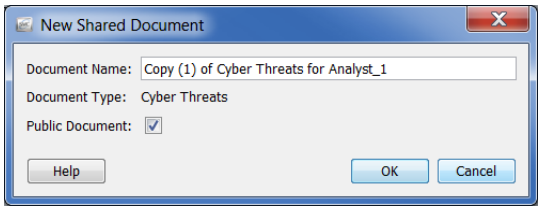
1. 메인 메뉴에서 **File(파일) > Manage Documents(문서 관리)**를 선택합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.



2. **Shared Documents(공유 문서)** 아이콘을 클릭합니다. Shared Documents(공유 문서) 페이지가 열립니다.
3. 원하는 문서를 선택합니다.
4. **Edit Filter(필터 편집)**를 클릭합니다. Filter(필터) 대화 상자가 열립니다.



5. 원하는 대로 필터 설정을 변경합니다. 다른 사용자가 소유한 문서의 필터 설정을 편집하는 경우, 아래 예에서와 같이 New Shared Document(새 공유 문서) 대화 상자가 열립니다.



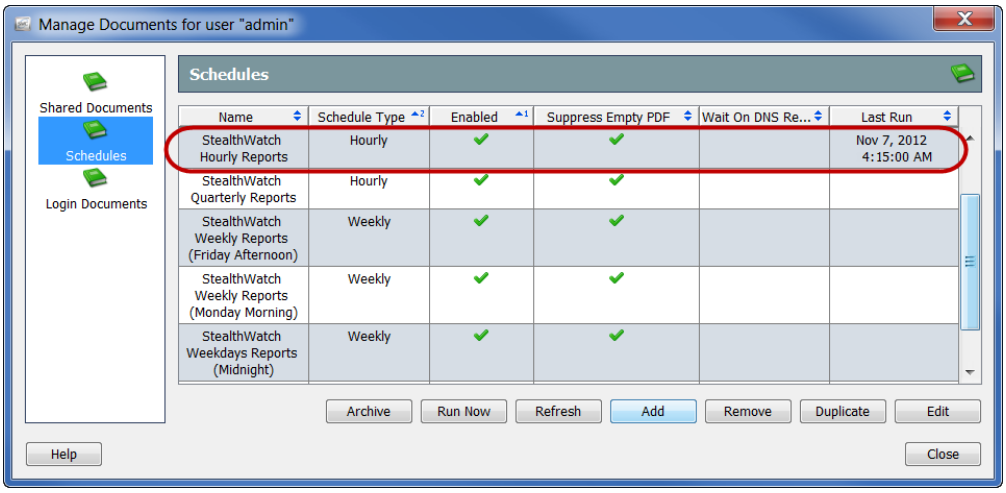
6. 다음 중 하나를 수행합니다.
   - Document Name(문서 이름) 필드에서 기본 이름을 수락하려면 **OK(확인)**를 클릭하고 New Shared Document(새 공유 문서) 대화 상자를 종료합니다.
   - Document Name(문서 이름) 필드에서 이름을 변경하고 **OK(확인)**를 클릭하여 New Shared Document(새 공유 문서) 대화 상자를 종료합니다.
7. **OK(확인)**를 클릭하여 Managed Documents(관리되는 문서) 대화 상자를 종료합니다.

아카이브 문서 검색

SMC에서 예약된 문서를 사용자에게 자동으로 이메일로 보내도록 설정하지 않으려는 경우 또는 SMC에서 이메일을 수신하는 기능을 사용하지 않는 경우, 예약된 문서를 편리한 시간에 검색하도록 선택할 수 있습니다.

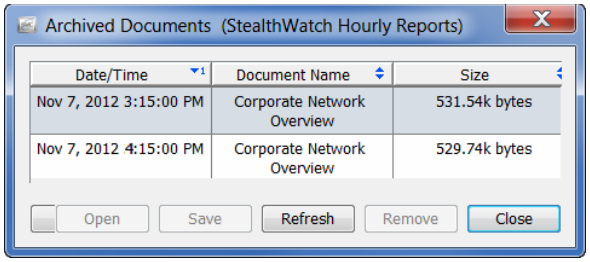
생성된 문서를 검색하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **File(파일) > Manage Documents(문서 관리)**를 선택합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.

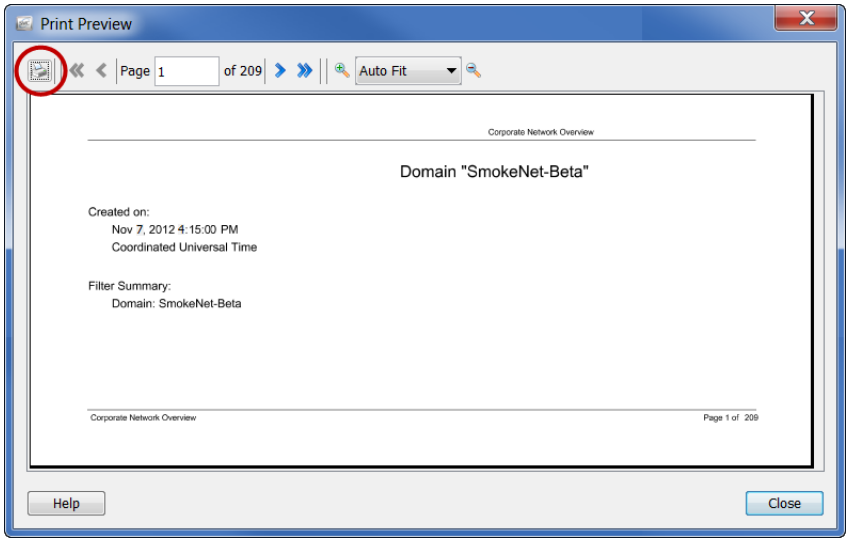


2. **Schedules(일정)** 아이콘을 클릭합니다. Schedules(일정) 페이지가 열립니다.
3. 생성된 문서가 포함된 일정을 보려면 클릭합니다. 참고로, Last Run(마지막 실행) 열에는 일정이 마지막으로 실행된 날짜와 시간이 나와 있습니다.

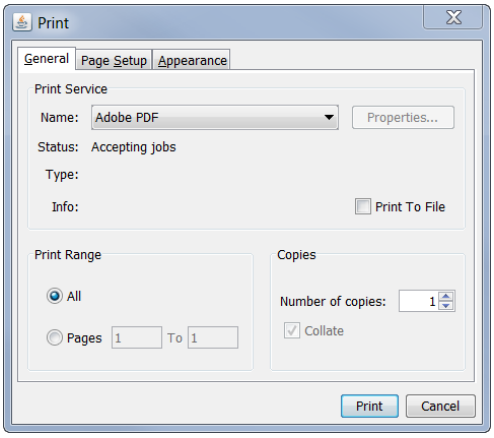
4. **Archive(아카이브)**를 클릭합니다. 오른쪽에 표시된 것과 같이 Archived Documents(아카이브 문서) 대화 상자가 열립니다.



5. 보려는 문서를 클릭합니다.
6. **Open(열기)**을 클릭합니다. Print Preview(인쇄 미리보기) 대화 상자가 열립니다.



7. **Print(인쇄)** 아이콘(이전 이미지에서 원으로 표시됨)을 클릭합니다. Print(인쇄) 대화 상자가 열립니다.



문서의 하드 카피를 인쇄하거나 로컬 하드 드라이브에 다운로드할 수 있습니다.

14

사용자 관리

개요

참고:

관리자 권한이 있는 사용자만 이 장의 절차를 수행할 수 있습니다.

SMC는 매우 유연하므로 다양한 권한 레벨의 사용자를 설정할 수 있습니다. 예를 들어 한 사용자가 네트워크의 모든 영역을 보고 수정하도록 허용할 수 있습니다. 또는 특정 사용자가 다른 기능을 수행하지 않고 네트워크의 특정 영역만 볼 수 있도록 권한을 제한할 수 있습니다.

이 장은 다음 항목으로 구성되어 있습니다.

- 프로세스 개요
- 인증 서비스 추가
- 사용자가 보고 구성할 수 있는 항목 제어(데이터 역할)
- 사용자가 수행할 수 있는 작업 제어(기능 역할)
- 사용자 계정 추가
- 예약된 문서를 사용자 계정에 연결하기
- 로그인 문서

프로세스 개요

일반적으로 SMC에서 사용자를 관리하기 위한 프로세스에는 이 장에 자세히 나와 있는 다음 절차를 완료하는 과정이 포함됩니다.

1. SMC에서 예약된 문서를 사용자에게 자동으로 이메일로 보내도록 설정하려는 경우 13장, "문서 작업"의 321페이지의 "SMC에 이메일 서버 추가"에 설명된 대로 이메일 서버 정보를 SMC에 추가하십시오.
2. 네트워크에서 사용하는 인증 서비스를 추가합니다.
3. 각 사용자가 보고 구성할 수 있게 하려는 데이터를 결정합니다.
4. 사용자의 데이터 역할을 추가합니다.
5. 각 사용자가 액세스할 수 있게 하려는 SMC 기능(즉, 메뉴 옵션)을 결정합니다.
6. 사용자의 기능 역할을 추가합니다.
7. 적용 가능한 데이터 및 기능 역할을 가진 사용자를 추가합니다.

참고:

관리자 권한을 지닌 사용자는 모든 SMC 기능에 액세스할 뿐만 아니라 모든 데이터를 보고 구성할 수 있습니다.

8. 원하는 경우, 예약된 문서를 사용자 계정에 연결합니다.

참고:

사용자가 로그인할 때까지 변경 사항이 적용되지 않습니다. 따라서 영향을 받는 사용자가 로그인한 상태에서 이러한 요소를 수정하는 경우, 로그아웃한 다음에 다시 로그인할 때까지 이러한 변경 사항이 표시되지 않습니다.

인증 서비스 추가

참고:

- 로컬 인증을 사용하도록 선택하는 경우, 이 절차를 수행할 필요가 없습니다.
- 네트워크에서 RADIUS 또는 TACACS 서버를 사용하지 않는 경우 로컬로 인증해야 합니다.

사용자 관리의 첫 번째 단계는 로컬(내부)에서 인증할지 인증 서비스(외부)를 사용할지를 결정하는 것입니다. 기본적으로 Stealthwatch System은 로컬 인증을 사용합니다.

인증은 클라이언트 또는 사용자의 ID를 서버 또는 호스트에서 확인할 때 사용하는 프로세스입니다. 이 프로세스에는 여러 가지 형식을 사용할 수 있지만 일반적으로 액세스 권한을 얻기 위한 검증에서 클라이언트가 서버에 비밀번호를 제공하는 과정이 포함되어 있습니다.

다음 인증 서비스 중 하나를 사용하는 경우 시스템 액세스를 위해 이러한 서비스 중 하나를 활용하도록 SMC를 구성할 수 있습니다. Stealthwatch에서는 다음 인증 서비스를 지원합니다.

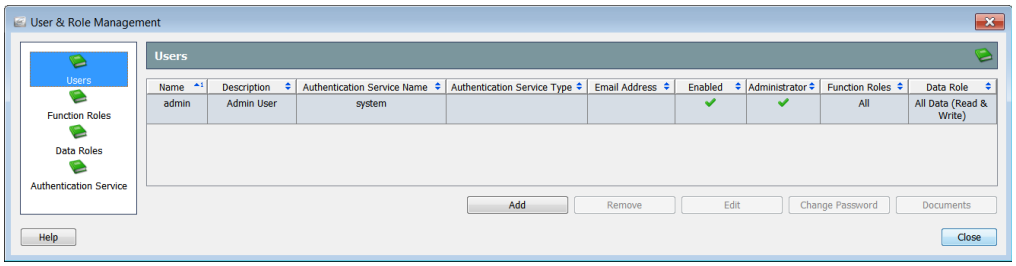
- RADIUS(Remote Authentication Dial-in User Service)
- TACACS+(Terminal Access Controller Access Control System

중요:

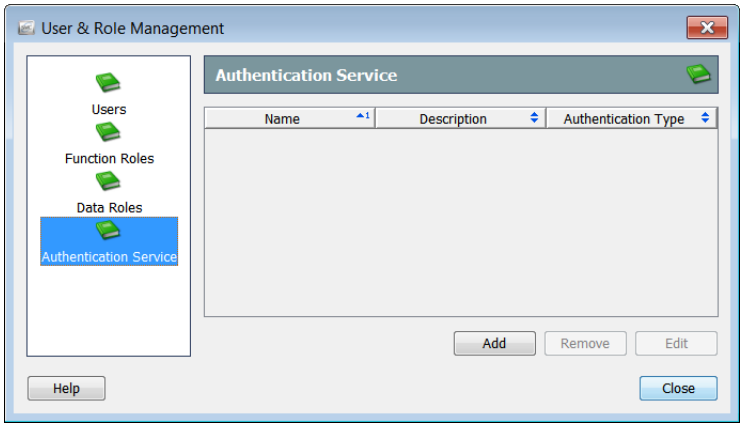
시스템에서 RADIUS 인증 서버로 Windows 인터넷 인증 서비스를 사용하는 경우, 사용자의 Active Directory 사용자 계정에서 "Dial-in(전화 접속)" 액세스가 활성화되어 있어야 합니다. 그렇지 않으면, 사용자는 SMC에 로그인할 수 없습니다.

인증 서비스를 추가하려는 경우 다음 단계를 수행하십시오.

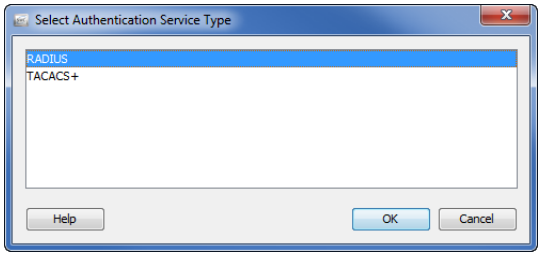
1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.



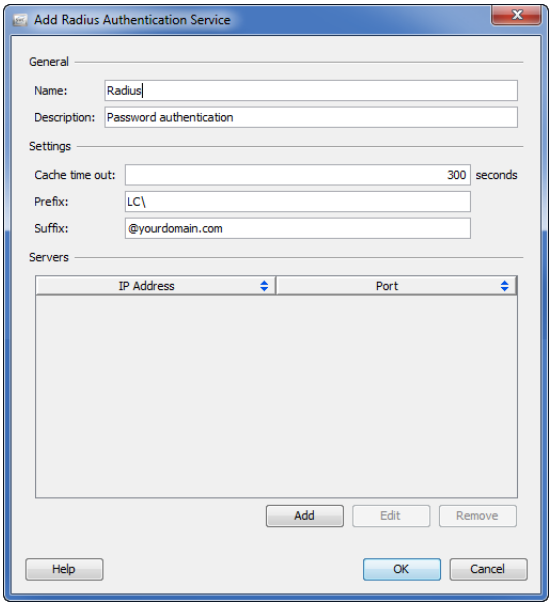
2. **Authentication Service(인증 서비스)** 아이콘을 클릭합니다. Authentication Service(인증 서비스) 페이지가 열립니다.



3. **Add(추가)**를 클릭합니다. Select Authentication Service Type(인증 서비스 유형 선택) 대화 상자가 열립니다.



4. 원하는 서비스를 선택한 다음 **OK(확인)**를 클릭합니다. Add Authentication Service(인증 서비스 추가) 대화 상자가 열립니다.



5. 해당하는 필드에서 다음 정보를 입력합니다.

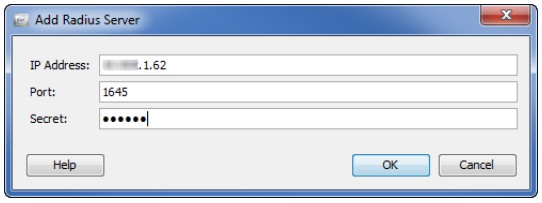
   - 인증 서비스 이름
   - 서비스 설명(선택사항)
   - 캐시 시간이 초과되고 시스템에서 인증 서버를 필요로 할 때까지 사용자/비밀번호가 유효한 시간(초).

참고:

각 SMC 문서 및 SMC 문서의 각 셀에는 사용자에 대한 검증과 할당된 역할이 필요합니다. SMC는 사용자가 각 SMC 문서에 로그인할 필요가 없도록 캐시 시간 초과(초)에 대한 인증을 캐시합니다.

   - 서비스에 필요한 모든 접두사(예: `rowspan="1" colspan="1"` 또는 `[domain]\`)
   - 서비스에 필요한 모든 접미사(예: `@yourdomain.com`)

6. **Add(추가)**를 클릭하여 인증 서버 정보를 추가합니다. Add [Service Name] Server([서비스 이름] 서버 추가) 대화 상자가 열립니다.

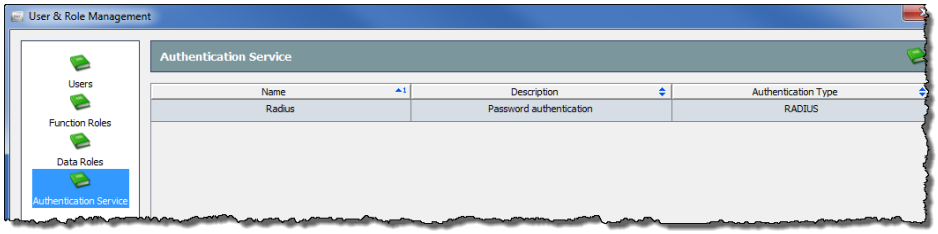


7. 해당하는 필드에 인증 서버에 대한 다음 정보를 입력합니다.

   - IP 주소
   - 인증 서비스 관련 포트 번호
     - RADIUS 기본값 = 1645
     - TACACS+ 기본값 = 49
   - 도메인 관리자가 사용자에게 제공한 암호(RADIUS) 또는 키(TACACS +)

8. **OK(확인)**를 클릭합니다. Add Server(서버 추가) 대화 상자가 닫힙니다. Add Authentication Service(인증 서비스 추가) 대화 상자의 Servers(서버) 테이블이 새 서버로 업데이트됩니다.

9. **OK(확인)**를 클릭합니다. Add Authentication Service(인증 서비스 추가) 대화 상자가 닫힙니다. 새 서비스가 Authentication Service(인증 서비스) 페이지에 나타납니다.



10. **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 닫거나 다음 섹션으로 계속 진행합니다.

사용자가 보고 구성할 수 있는 항목 제어(데이터 역할)

SMC를 사용하면 사용자의 *data roles(데이터 역할)*를 정의할 수 있습니다. 데이터 역할은 다음을 포함하여 어떤 사용자 정보를 보고(읽기) 구성(쓰기)할 수 있는지 제어합니다.

- 도메인
- 호스트 그룹
- VM 서버
- VM
- Flow Collector
- 엑스포터
- FlowSensors
- 외부 디바이스
- Identity 디바이스

데이터 역할은 사용자에게 표시하지 않을 데이터를 효과적으로 숨기는 방법도 제공합니다. 예를 들어, 시스템에서 이중화된(페일오버) Flow Collector를 사용하는 경우, 기본 Flow Collector의 데이터와 페일오버의 동일한 데이터인 중복 데이터가 SMC에 보고됩니다. 그러나, 페일오버 Flow Collector에서 데이터를 숨기는 데이터 역할을 생성할 수 있습니다. 그러면 이 데이터 역할에 할당된 사용자에게 기본 Flow Collector의 데이터만 표시됩니다.

참고:

이전 시나리오에 대한 자세한 내용은 338페이지의 "이중화된 Flow Collector 데이터를 숨기기 위한 데이터 역할 추가"를 참조하십시오.

SMC에는 다음과 같은 기본 데이터 역할이 제공됩니다.

- 모든 데이터(읽기 및 쓰기) - 이 데이터 역할을 가진 사용자는 모든 Stealthwatch 데이터를 보고 구성할 수 있습니다.
- 모든 데이터(읽기 전용) - 이 데이터 역할을 가진 사용자는 모든 Stealthwatch 데이터를 볼 수 있지만 구성할 수는 없습니다.

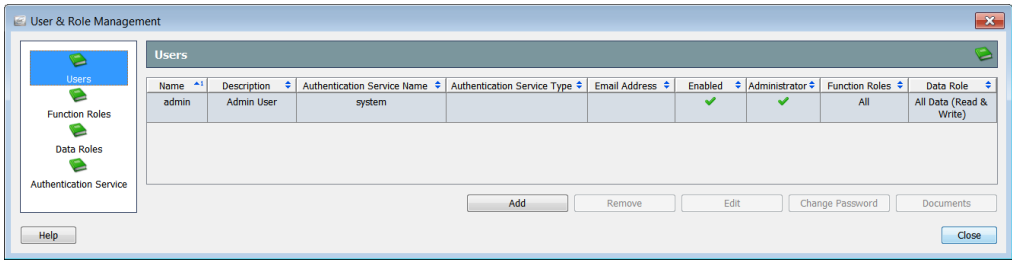
참고:

추가하는 각 사용자에게 데이터 역할을 할당해야 합니다.

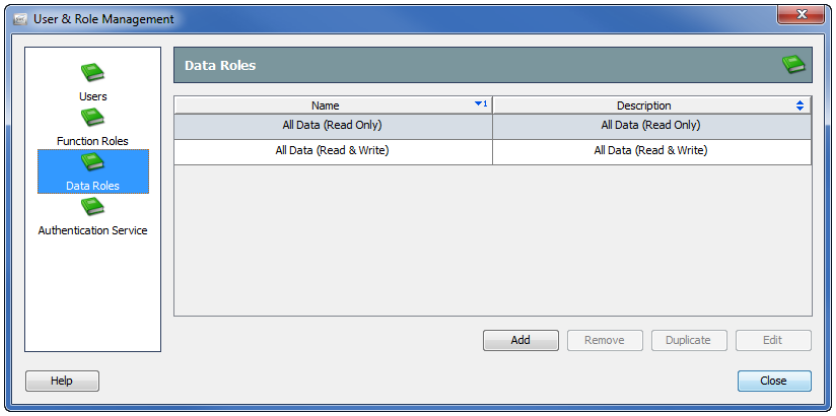
필요에 따라 새 데이터 역할을 생성할 수 있습니다. 생성하는 모든 데이터 역할을 수정 또는 삭제할 수 있습니다. 그러나, 기본 데이터 역할은 수정하거나 삭제할 수 없습니다.

데이터 역할을 추가하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.

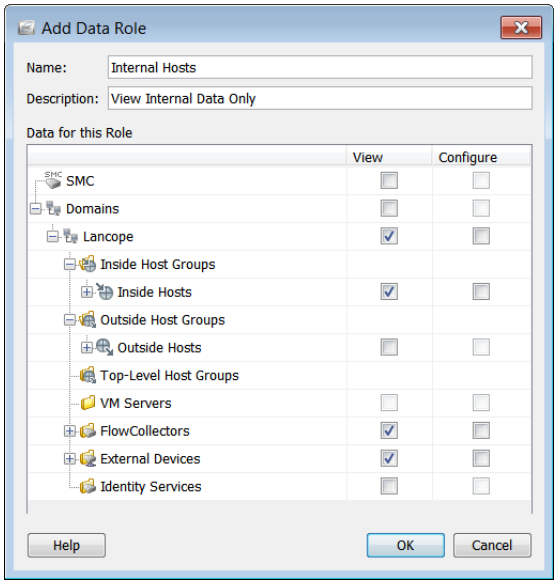


2. **Data Roles(데이터 역할)** 아이콘을 클릭합니다. Data Roles(데이터 역할) 페이지가 열립니다.



3. **Add(추가)**를 클릭합니다.

   Add Data Role(데이터 역할 추가) 대화 상자가 열립니다.

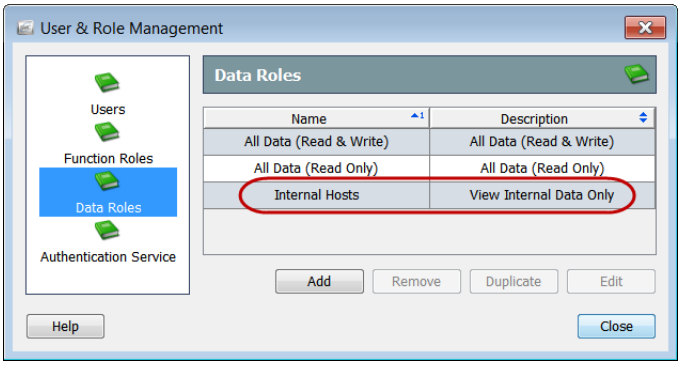


4. Name(이름) 필드에 데이터 역할의 이름을 입력합니다.
5. (선택사항) Description(설명) 필드에 데이터 역할의 설명을 입력합니다.
6. 이 데이터 역할을 지닌 사용자가 보거나 구성하거나 이 두 가지를 모두 수행할 수 있게 하려는 항목의 확인란을 선택합니다.

참고:

사용자에게 데이터를 숨기려면 해당 데이터와 연결된 항목의 View(보기) 확인란을 선택하지 마십시오(예: 이중화된 Flow Collector).

7. **OK(확인)**를 클릭합니다. Add Data Role(데이터 역할 추가) 대화 상자가 닫힙니다. 새 데이터 역할이 Data Roles(데이터 역할) 페이지에 나타납니다.



8. **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 닫거나 다음 섹션으로 계속 진행합니다.

이중화된 Flow Collector 데이터를 숨기기 위한 데이터 역할 추가

이중화된 Flow Collector를 사용 중이며 사용자가 기본 Flow Collector에서 가져온 데이터만 보도록 설정하려면 다음 순서대로 이 섹션에서 다음의 4가지 절차를 완료하십시오.

1. 기본 Flow Collector의 데이터 역할을 추가합니다. (338페이지 참조)
2. 이중화된 Flow Collector의 데이터 역할을 추가합니다. (340페이지 참조)
3. 사용자 계정을 추가하고 기본 Flow Collector 데이터 역할을 계정에 할당합니다. (344페이지 참조)
4. 필요한 경우 사용자 계정을 편집하고 이중화된 Flow Collector 데이터 역할을 계정에 할당합니다. (346페이지 참조)

중요:

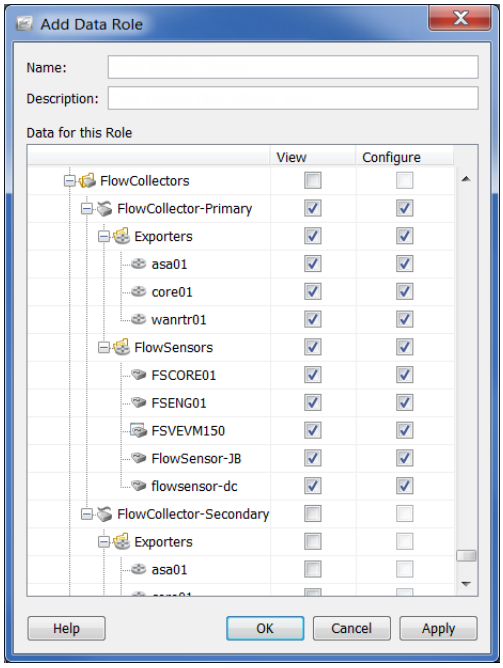
기본 Flow Collector에 장애가 발생하고 사용자의 데이터 역할에서 이중화된 Flow Collector를 숨기는 경우 사용자에게 데이터가 표시되지 않습니다. 이 문제를 해결하려면 이중화된 Flow Collector를 보여 주는 데이터 역할을 할당하도록 사용자 계정을 편집하십시오.

기본 Flow Collector의 데이터 역할 추가

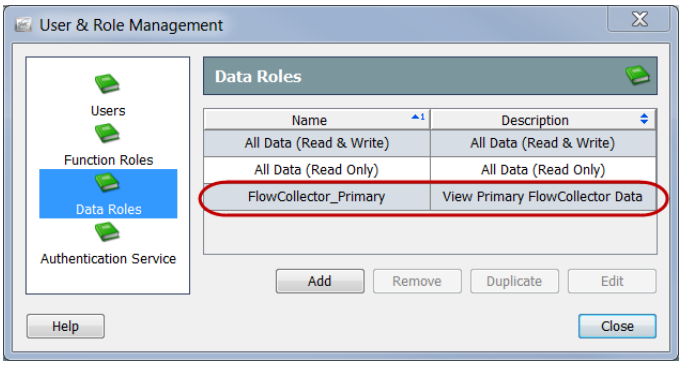
기본 Flow Collector의 데이터 역할을 추가하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.
2. **Data Roles(데이터 역할)** 아이콘을 클릭합니다. Data Roles(데이터 역할) 페이지가 열립니다.

3. **Add(추가)**를 클릭합니다. Add Data Role(데이터 역할 추가) 대화 상자가 열립니다.



4. Name(이름) 필드에 데이터 역할의 이름(예: Flow Collector_Primary)을 입력합니다.
5. (선택사항) Description(설명) 필드에 데이터 역할의 설명을 입력합니다.
6. 아래로 스크롤하여 기본 Flow Collector로 이동하여 이 데이터 역할을 지닌 사용자가 보거나 구성하거나 이 두 가지를 모두 수행할 수 있도록 하려는 항목의 확인란을 선택합니다.
7. **OK(확인)**를 클릭합니다. Add Data Role(데이터 역할 추가) 대화 상자가 닫힙니다. 새 데이터 역할이 Data Roles(데이터 역할) 페이지에 나타납니다.

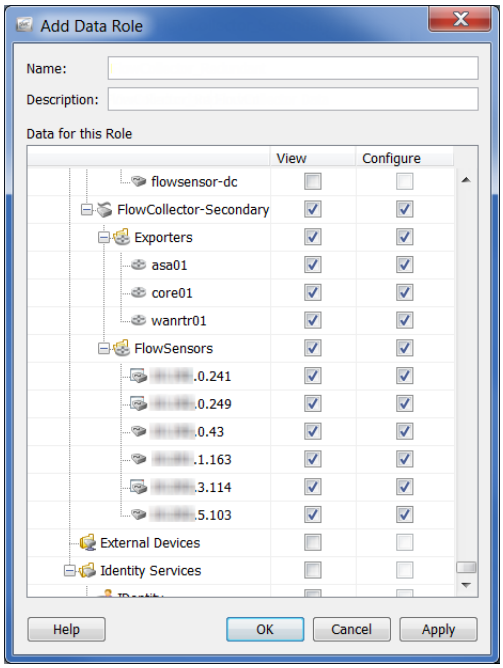


8. 다음 섹션으로 계속 진행합니다.

이중화된 Flow Collector의 데이터 역할 추가

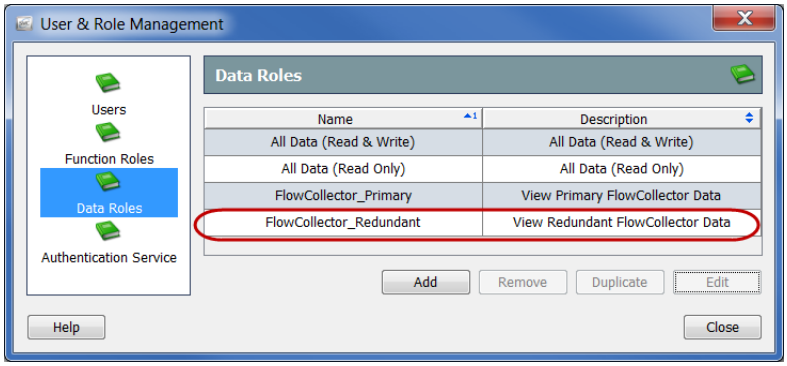
이중화된 Flow Collector의 데이터 역할을 추가하려면 다음 단계를 수행하십시오.

1. User & Role Management(사용자 및 역할 관리) 대화 상자의 Data Roles(데이터 역할) 페이지에서 **Add(추가)**를 클릭합니다. Add Data Role(데이터 역할 추가) 대화 상자가 열립니다.



2. Name(이름) 필드에 데이터 역할의 이름(예: Flow Collector _Secondary)을 입력합니다.
3. (선택사항) Description(설명) 필드에 데이터 역할의 설명을 입력합니다.
4. 아래로 스크롤하여 이중화된 Flow Collector로 이동하여 이 데이터 역할을 지닌 사용자가 보거나 구성하거나 이 두 가지를 모두 수행할 수 있도록 하려는 항목의 확인란을 선택합니다.

5. **OK(확인)**를 클릭합니다. Add Data Role(데이터 역할 추가) 대화 상자가 닫힙니다. 새 데이터 역할이 Data Roles(데이터 역할) 페이지에 나타납니다.



이제 기본 및 이중화된 Flow Collector 모두의 데이터 역할을 사용하므로 344페이지의 "사용자 계정 추가"에 설명된 대로 이 역할을 사용자에게 할당할 수 있습니다.

6. **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 닫거나 다음 섹션으로 계속 진행합니다.

사용자가 수행할 수 있는 작업 제어(기능 역할)

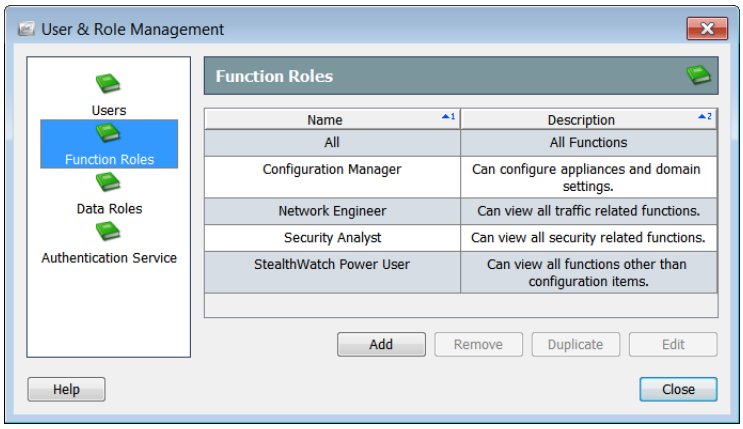
원하는 데이터 역할을 생성한 후에 사용자를 정의하는 다음 단계는 *기능 역할*을 생성하는 것입니다. 기능 역할은 사용자가 액세스할 수 있는 SMC 메뉴 항목과 사용자가 수행할 수 있는 작업을 제어합니다. SMC에는 다음과 같은 기본 기능 역할이 제공됩니다.

- 모두 - 사용자가 모든 메뉴 항목을 보고 SMC 클라이언트 인터페이스 내에서 어떤 항목이든 변경할 수 있도록 허용합니다.
- 컨피그레이션 관리자 - 사용자가 모든 메뉴 항목을 보고 모든 어플라이언스와 도메인 설정을 구성할 수 있도록 허용합니다.
- 네트워크 엔지니어 - 사용자가 SMC 클라이언트 인터페이스 내에서 모든 트래픽 관련 메뉴 항목을 보고 알람 및 호스트 메모를 추가하며 완화를 제외한 모든 알람 작업을 수행할 수 있도록 허용합니다.
- 보안 분석가 - 사용자가 모든 보안 관련 메뉴 항목을 보고 알람 및 호스트 메모를 추가하며 완화를 포함한 모든 알람 작업을 수행할 수 있도록 허용합니다.
- Stealthwatch 고급 사용자 - 사용자가 모든 메뉴 항목을 보고 알람을 확인하며 알람 및 호스트 메모를 추가할 수 있도록 허용합니다(단, 변경 기능 없이).

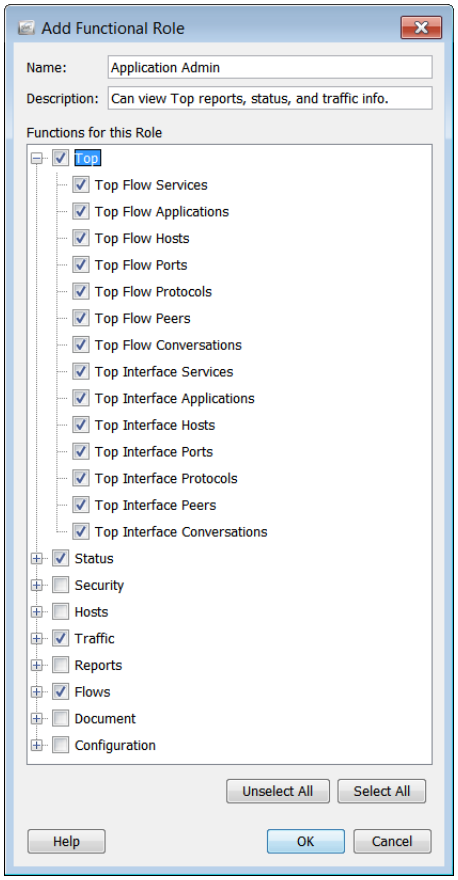
필요에 따라 추가 기능 역할을 생성할 수 있습니다. 또한 기본값을 포함하여 모든 기능 역할을 수정 또는 삭제할 수 있습니다.

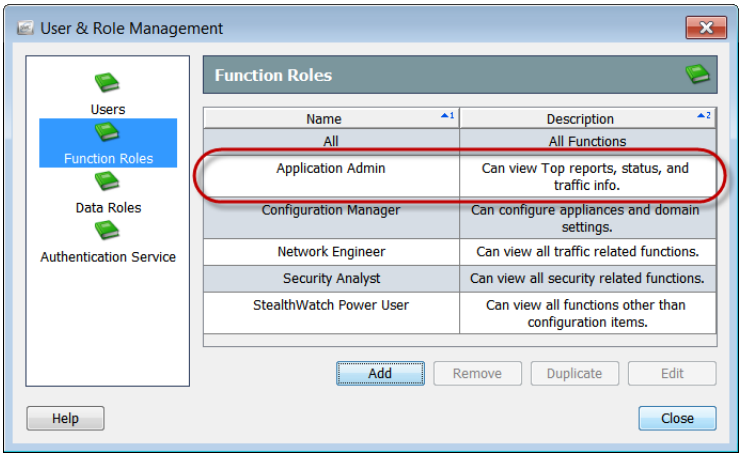
기능 역할을 추가하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.
2. **Function Role(기능 역할)** 아이콘을 클릭합니다. Function Role(기능 역할) 페이지가 열립니다.



3. **Add(추가)**를 클릭합니다. Add Functional Role(기능 역할 추가) 대화 상자가 열립니다.
4. Name(이름) 필드에 기능 역할의 이름을 입력합니다.
5. (선택사항) Description(설명) 필드에 기능 역할의 설명을 입력합니다.
6. 이 기능 역할을 지닌 사용자가 보거나 수행할 수 있도록 하려는 항목의 확인란을 선택합니다.
7. **OK(확인)**를 클릭합니다. Add Functional Role(기능 역할 추가) 대화 상자가 닫힙니다. 새 기능 역할이 Functional Roles(기능 역할) 페이지에 나타납니다.





8. **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 닫거나 다음 섹션으로 계속 진행합니다.

사용자 계정 추가

원하는 데이터 역할 및 기능 역할을 추가한 후에는 사용자를 추가하고 적절한 역할을 할당할 수 있습니다. SMC에는 이미 관리 사용자가 정의되어 있습니다. 기본 관리 사용자를 포함하여 모든 사용자를 수정할 수 있으며, 관리 사용자를 *제외*하고 모든 사용자를 삭제할 수 있습니다.

참고:

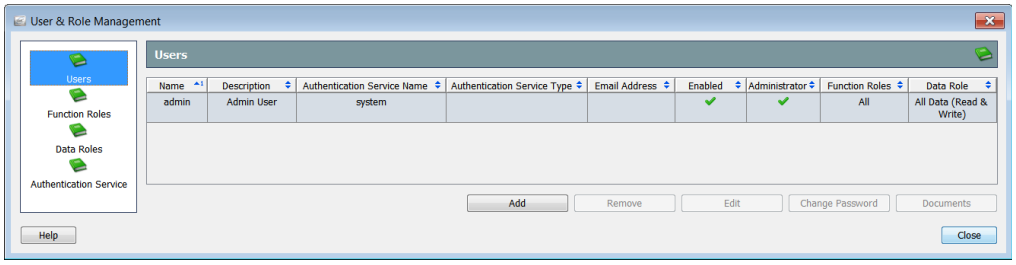
SMC에서 예약된 문서를 자동으로 이메일로 전송하도록 설정할 사용자 계정을 추가해야 합니다.

사용자를 추가할 때 다음 지침을 고려하십시오.

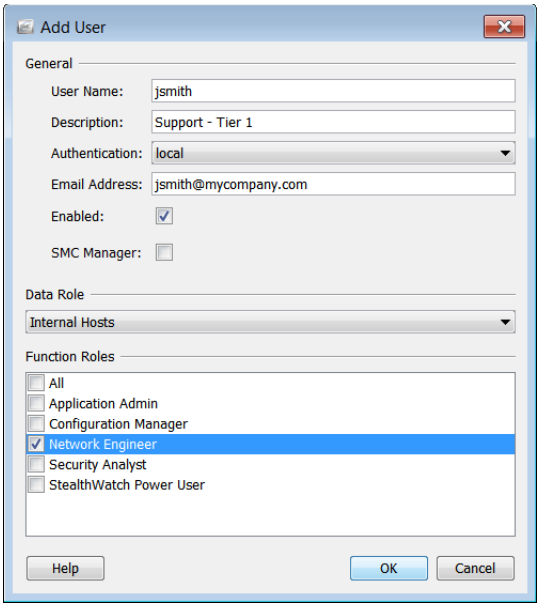
- 다른 모든 사용자에게 *admin(관리자)* 이름을 지정할 수 없습니다.
- 관리 사용자만 어플라이언스 관리 웹 인터페이스에 로그인할 수 있습니다.
- **Administrator(관리자)** 확인란(9단계)을 선택한 경우, 추가 중인 사용자가 관리자 권한을 지니게 되어 사용자가 다음 작업을 수행하도록 할 수 있습니다.
  - 모든 데이터 보기 및 구성
  - 모든 메뉴 항목에 액세스 및 모든 기능 수행
  - 기타 사용자 생성 및 관리

새 사용자를 추가하려면 다음 단계를 수행하십시오.

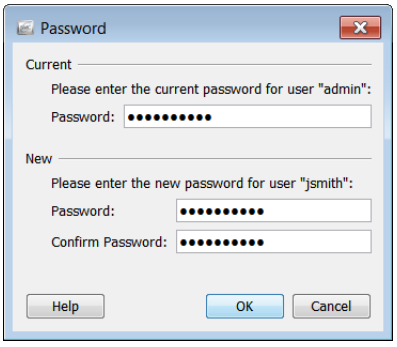
1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.
2. **Users(사용자)** 아이콘을 클릭합니다. Users(사용자) 페이지가 열립니다.



3. **Add(추가)**를 클릭합니다. Add User(사용자 추가) 대화 상자가 열립니다.

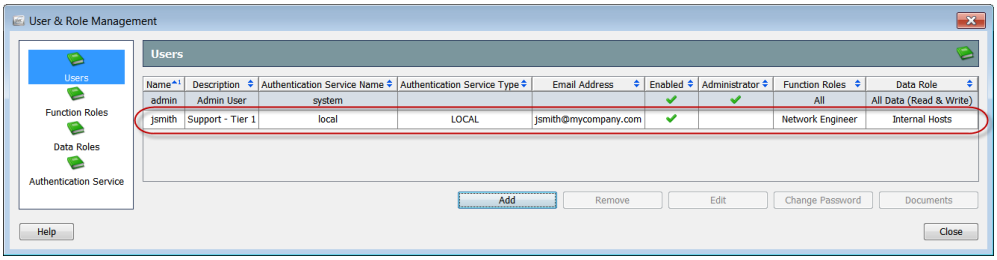


4. Name(이름) 필드에 사용자의 로그인 이름(대/소문자 구분)을 입력합니다.
5. (선택사항) Description(설명) 필드에 사용자에 대한 설명을 입력합니다.
6. 사용자의 ID를 인증하는 데 사용할 인증 서비스를 선택합니다.
7. SMC에서 이메일 보고서 및 알람을 이 사용자에게 보내도록 설정하려면 사용자의 이메일 주소를 입력합니다.
8. 이 사용자가 SMC 클라이언트 인터페이스에 로그인하여 이메일을 통해 예약된 문서를 수신하도록 설정하려면 **Enabled(활성화됨)** 확인란을 선택합니다.
9. 사용자에게 관리자 권한이 필요한가요?
   - 대답이 예인 경우 **SMC Manager(SMC 관리자)** 확인란을 선택합니다. 대답이 아니요인 경우 12단계로 이동합니다.
   - 대답이 아니요인 경우 다음 단계로 계속 진행합니다.
10. Data Role(데이터 역할) 섹션에서 드롭다운 상자를 클릭하고 이 사용자에게 할당할 데이터 역할을 선택합니다(예: Flow Collector_Primary).
11. Function Role(기능 역할) 섹션에서 이 사용자에게 할당할 기능 역할을 선택합니다.
12. **OK(확인)**를 클릭합니다. Add User(사용자 추가) 대화 상자가 닫히고 Password(비밀번호) 대화 상자가 열립니다.



13. 현재 섹션에서 관리 사용자의 비밀번호를 입력합니다.
14. 해당하는 경우, 다음 작업을 수행합니다.
   - New(새로 만들기) 섹션에서 새 사용자의 비밀번호(대/소문자 구분)를 입력합니다.
   - Confirm Password(비밀번호 확인) 필드에서 비밀번호를 다시 입력합니다.

15. **OK(확인)**를 클릭합니다. Password(비밀번호) 대화 상자가 닫힙니다. 새 사용자가 Users(사용자) 페이지에 나타납니다.



16. 예약된 문서를 이 사용자의 계정과 연결하시겠습니까?
    - 대답이 예인 경우 349페이지의 "예약된 문서를 사용자 계정에 연결하기"를 계속 진행합니다.
    - 대답이 아니요인 경우 17단계로 이동합니다.
17. 로그인 문서를 이 사용자의 계정과 연결하시겠습니까?
    - 대답이 예인 경우 358페이지의 "로그인 문서"로 이동합니다.
    - 대답이 아니요인 경우 **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 종료합니다.

사용자 계정 편집

사용자의 계정 정보를 변경해야 하는 경우 이 섹션의 단계를 완료하십시오. 예를 들어 사용자에게 이중화된 Flow Collector를 숨기는 데이터 역할을 할당한 경우, 기본 Flow Collector에 장애가 발생하면 이 절차를 사용하여 이중화된 Flow Collector를 보여 주는 데이터 역할을 사용자에게 할당할 수 있습니다.

중요:

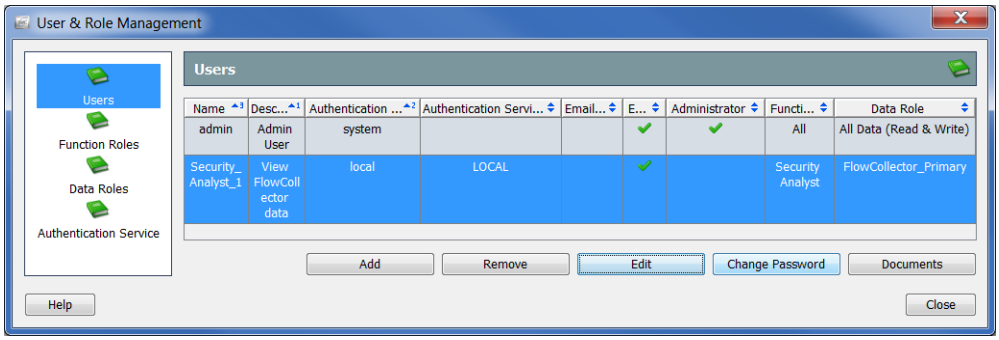
기본 Flow Collector에 장애가 발생하고 사용자의 데이터 역할에서 이중화된 Flow Collector를 숨기는 경우 사용자에게 데이터가 표시되지 않습니다.

참고:

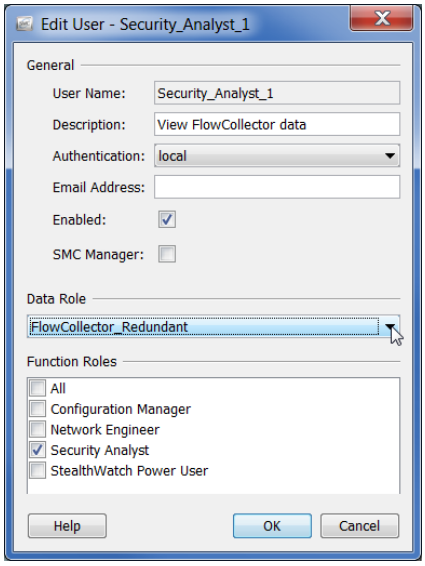
사용자가 로그인할 때까지 변경 사항이 적용되지 않습니다. 따라서 영향을 받는 사용자가 로그인한 상태에서 이러한 요소를 수정하는 경우, 로그아웃한 다음에 다시 로그인할 때까지 이러한 변경 사항이 표시되지 않습니다.

1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.
2. Users(사용자) 아이콘을 클릭합니다. Users(사용자) 페이지가 열립니다.

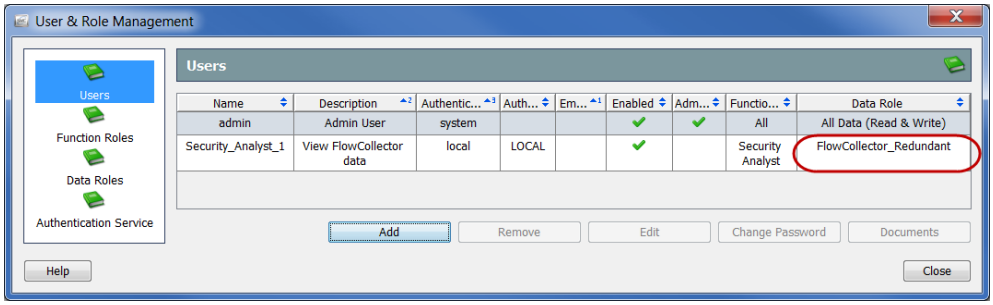
3. 편집하려는 사용자 계정을 선택합니다.



4. **Edit(편집)**을 클릭합니다. 해당 사용자에 대한 Edit User(사용자 편집) 대화 상자가 열립니다.



5. Data Role(데이터 역할) 섹션에서 데이터 역할을 변경하려면 드롭다운 상자를 클릭하고 데이터 역할(예: 이중화된 Flow Collector를 보여 주는 데이터 역할)을 선택합니다.
6. 이 계정의 기타 설정을 적절하게 변경합니다.
7. **OK(확인)**를 클릭합니다. Edit User(사용자 편집) 대화 상자가 닫힙니다. 사용자의 새로운 정보가 Users(사용자) 페이지에 나타납니다. 이러한 변경 사항은 사용자가 다음에 로그인할 때 적용됩니다.



8. 예약된 문서를 이 사용자의 계정과 연결하시겠습니까?
   - 대답이 예인 경우 349페이지의 "예약된 문서를 사용자 계정에 연결하기"를 계속 진행합니다.
   - 대답이 아니요인 경우 9단계로 이동합니다.
9. 로그인 문서를 이 사용자의 계정과 연결하시겠습니까?
   - 대답이 예인 경우 358페이지의 "로그인 문서"로 이동합니다.
   - 대답이 아니요인 경우 **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 종료합니다.

예약된 문서를 사용자 계정에 연결하기

항상 동일한 설정(예: 필터, 레이아웃, 시간 간격)을 사용하여 문서를 자동으로 생성하려는 경우가 있을 수 있습니다. 이를 위해 원하는 설정을 포함하는 일정에 문서를 추가해야 합니다.

Stealthwatch는 예약된 문서를 사용자 계정과 연결하는 두 가지 방법을 제공합니다. 관리 사용자인 경우 이 섹션에서 설명한 대로 사용자 계정을 생성/편집할 때 User & Role Management(사용자 및 역할 관리) 대화 상자를 사용할 수 있습니다.

개별 사용자는 13장, "문서 작업"에 설명된 대로 Manage Documents(문서 관리) 대화 상자를 사용하여 고유한 계정에 대해 작업을 완료할 수 있습니다.

참고:

이 섹션에서는 원하는 문서가 이미 SMC 어플라이언스에 저장되어 있다고 가정합니다. 문서 저장에 대한 자세한 내용은 13장, "문서 작업"을 참조하십시오.

문서 일정은 단순히 하나 이상의 문서를 얼마나 자주 실행하고 얼마나 오랫동안 아카이브할지에 대한 파라미터를 설정합니다. SMC는 자동으로 모든 사용자 계정과 연결되어 있는 기본 일정 집합과 함께 제공됩니다. 모든 기본 일정이 활성화되어 있지는 않습니다. 그러나, 각 사용자에 대해 모두 사용할 수 있습니다.

또한, 사용자는 직접 맞춤형 일정을 생성할 수 있습니다. 마지막으로, 관리 사용자인 경우, 이 섹션에서 설명한 대로 계정을 생성할 때 사용자 계정에 맞춤형 일정을 연결할 수 있습니다.

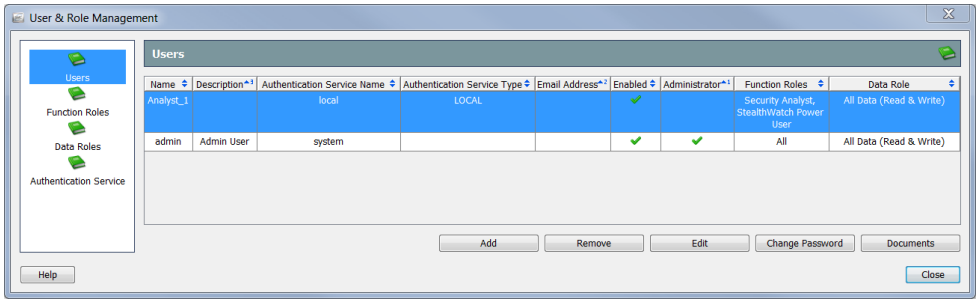
일정을 사용자 계정과 연결하는 프로세스에는 다음 절차를 완료하는 과정이 포함됩니다.

1. 새 일정을 추가하거나 기존 일정을 편집합니다.
2. 일정에 하나 이상의 문서를 추가합니다.
3. (선택사항) 예약된 문서를 생성할 때 SMC에서 예약된 문서를 사용자에게 자동으로 이메일로 보내도록 설정하려면 사용자 이메일 주소를 일정에 추가합니다.

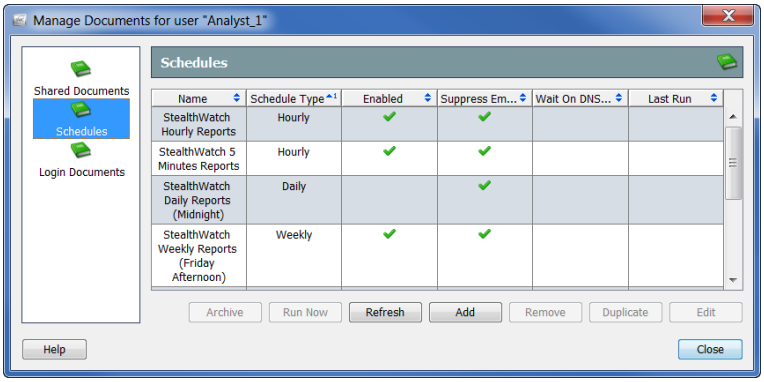
새 일정 추가

새 일정을 사용자 계정에 추가하려면 다음 단계를 완료하십시오.

1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.

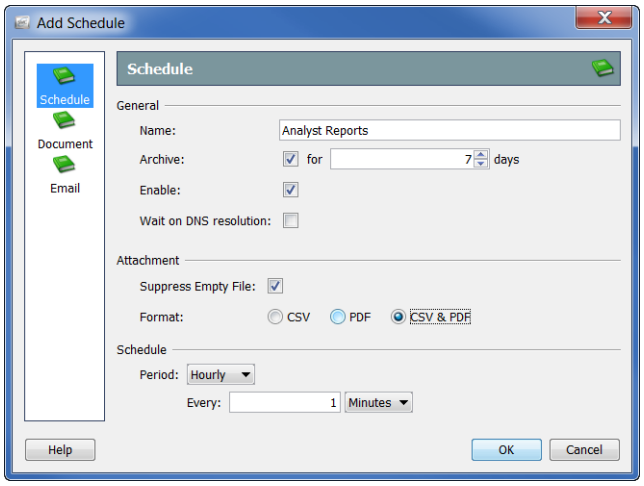


2. **Users(사용자)** 아이콘을 클릭합니다. Users(사용자) 페이지가 열립니다.
3. 원하는 사용자를 선택합니다.
4. **Documents(문서)**를 클릭합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.



5. **Schedules(일정)** 아이콘을 클릭합니다. Schedules(일정) 페이지가 열립니다.

6. **Add(추가)**를 클릭합니다. Add Schedule(일정 추가) 대화 상자가 열립니다.



7. **Schedule(일정)** 아이콘을 클릭합니다. Schedule(일정) 페이지가 열립니다.
8. Name(이름) 필드에 일정 이름을 입력합니다. 이 예에서는 일정을 "Analyst Reports(분석가 보고서)"라고 하겠습니다.
9. 다음 테이블에서와 같이 General(일반) 섹션에서 파라미터를 정의합니다.

원하는 작업	수행할 작업
SMC 데이터베이스에서 이 일정에 따라 생성된 문서 저장	**Archive(아카이브)** 확인란을 선택합니다. 그런 다음 해당하는 드롭다운 리스트를 클릭하고 문서를 저장하려는 일수를 선택합니다.
이 일정을 만드는 즉시 활성화	**Enable(활성화)** 확인란을 선택합니다.
문서에서 참조된 IP 주소가 이름으로 확인될 때까지 시스템이 예약한 문서의 생성을 대기하도록 설정	"Wait on DNS resolution(DNS 확인에서 대기)" 확인란을 선택합니다. **참고:** 이 기능을 활성화하면 문서 생성이 지연될 수 있습니다. 각 IP 주소는 확인하는 데 최대 2초가 걸릴 수 있습니다. IP 주소가 2초 이내에 확인되지 않는 경우, 해당 IP 주소는 DNS 이름 없이 표시됩니다.
SMC가 데이터 없이 생성된 문서를 아카이브하거나 이메일로 발송하는 것을 방지	"Suppress Empty File(빈 파일 표시 안 함)" 확인란을 선택합니다.
-계속-	

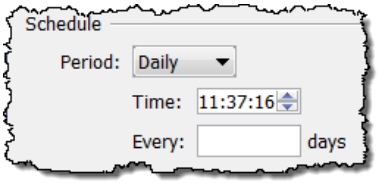
원하는 작업	수행할 작업
인쇄할 문서 유형 지정	▶ CSV(쉼표로 구분된 값) - 생성된 문서에 포함된 테이블 데이터만 인쇄하려는 경우 이 옵션을 선택합니다. • 각 테이블은 CSV 파일에 포함됩니다. • 다른 모든 데이터 유형(예: 지도, 그래프, 차트)은 인쇄하지 않습니다. • 각 문서의 모든 CSV 파일은 한 파일로 압축됩니다(즉, 문서당 하나의 압축된 파일). • 모든 압축된 파일은 선택한 일정에 따라 생성된 문서 사본을 이메일로 수신하도록 지정되어 있는 각 사용자에게 이메일로 발송됩니다. ▶ PDF - 생성된 문서에 포함된 모든 데이터를 인쇄하려는 경우 이 옵션을 선택합니다. • 생성된 각 문서는 PDF 파일에 포함됩니다. • 각 PDF 파일은 한 파일로 압축됩니다. • 모든 압축된 파일은 선택한 일정에 따라 생성된 문서 사본을 이메일로 수신하도록 지정되어 있는 각 사용자에게 이메일로 발송됩니다. ▶ CSV 및 PDF - CSV 형식으로 테이블 데이터를 인쇄하고 PDF 형식으로 기타 모든 데이터를 인쇄하려는 경우 이 옵션을 선택합니다. • 각 테이블은 CSV 파일에 포함됩니다. • 생성된 각 문서의 모든 기타 데이터 유형은 한 PDF 파일에 포함됩니다(즉, 문서당 하나의 PDF 파일). • 문서에 포함된 모든 파일은 한 파일로 압축됩니다(즉, 문서당 하나의 압축된 파일). • 모든 압축된 파일은 선택한 일정에 따라 생성된 문서 사본을 이메일로 수신하도록 지정되어 있는 각 사용자에게 이메일로 발송됩니다.

참고:

- Print Settings(인쇄 설정) 대화 상자의 Pages(페이지) 페이지에서 테이블을 활성화하지 않으면, 일정이 CSV 파일을 만들도록 구성된 경우에도 일정에서 해당 테이블에 대한 CSV 파일을 만들지 않습니다.
- Print Settings(인쇄 설정) 대화 상자의 Print Setup(인쇄 설정) 페이지에서 필터 요약 옵션을 지정할 경우 필터 요약이 생성된 문서에 포함됩니다. 참고로, "As the first page(첫 번째 페이지로)" 옵션 또는 "As the last page(마지막 페이지로)" 옵션(Cover Sheet(표지) 섹션) 중 하나를 선택하여 Filter summary(필터 요약) 확인란(Cover Sheet Options(표지 옵션) 섹션)을 활성화해야 옵션을 선택할 수 있습니다.

10. Period(기간) 드롭다운 리스트를 클릭하고 SMC에서 이 일정과 연결된 문서를 생성하는 빈도를 선택합니다. 예약된 문서를 매시간, 매일, 매주 또는 매월 생성하도록 선택할 수 있습니다. 선택하는 옵션에 따라 세부사항을 지정할 수 있는 다양한 필드가 나타납니다.

    예를 들어, **Daily(매일)**를 선택하면 일정을 실행하려는 날짜의 시간과 일정을 매일, 2일에 한 번, 3일에 한 번 등으로 실행할지 여부를 지정할 수 있는 2개의 필드가 나타납니다.

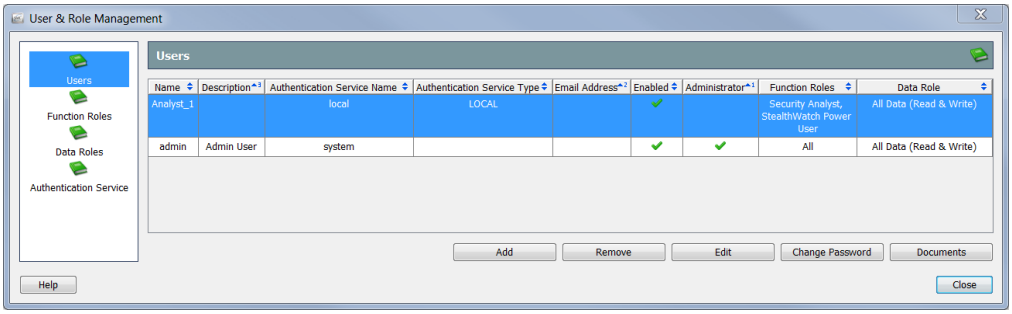


11. 355페이지의 "일정에 문서 추가"를 진행합니다.

기존 일정 편집

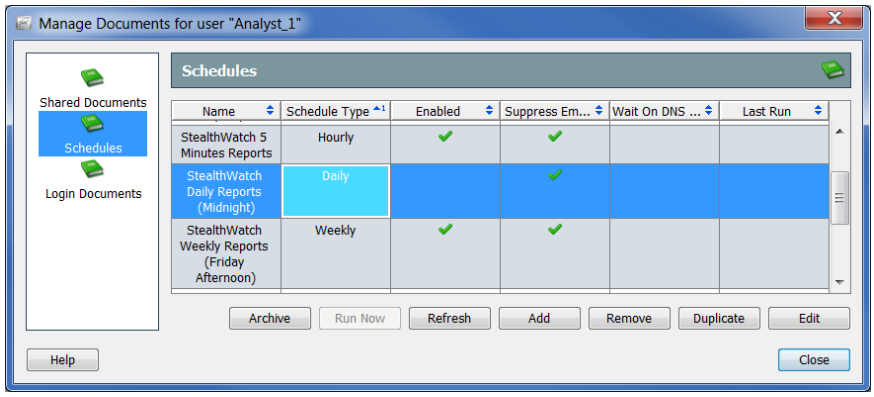
사용자 계정에 연결하려는 일정이 이미 있는 경우 다음 단계를 완료하여 그에 따라 일정을 편집하십시오.

1. 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.



2. **Users(사용자)** 아이콘을 클릭합니다. Users(사용자) 페이지가 열립니다.

3. 원하는 사용자를 선택합니다.
4. **Documents(문서)**를 클릭합니다. Manage Documents(문서 관리) 대화 상자가 열립니다.

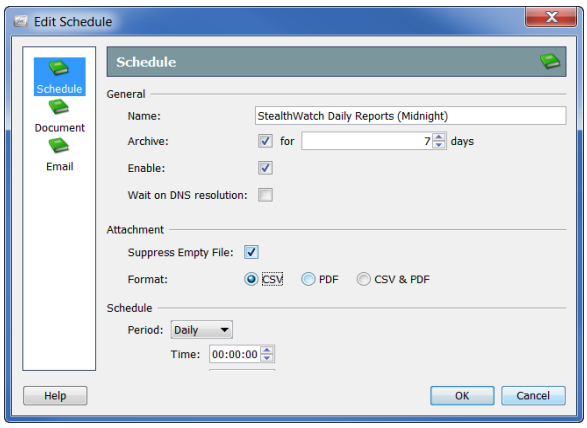


5. **Schedules(일정)** 아이콘을 클릭합니다. Schedules(일정) 페이지가 열립니다.
6. 편집하려는 일정을 선택합니다.

참고:

위의 예에서는 Stealthwatch Daily Report(Midnight)(Stealthwatch 일일 보고서(자정)) 일정을 선택했습니다. 참고로, Enabled(활성화됨) 열에 체크 마크가 없으면 이 일정이 사용자 계정에 대해 활성화되지 않았음을 의미합니다. 일정이 활성화되지 않으면 이 일정에 포함된 문서가 생성되지 않습니다.

7. **Edit(편집)**을 클릭합니다. Edit Schedule(일정 편집) 대화 상자가 열립니다.



8. **Schedule(일정)** 아이콘을 클릭합니다. Schedule(일정) 페이지가 열립니다.

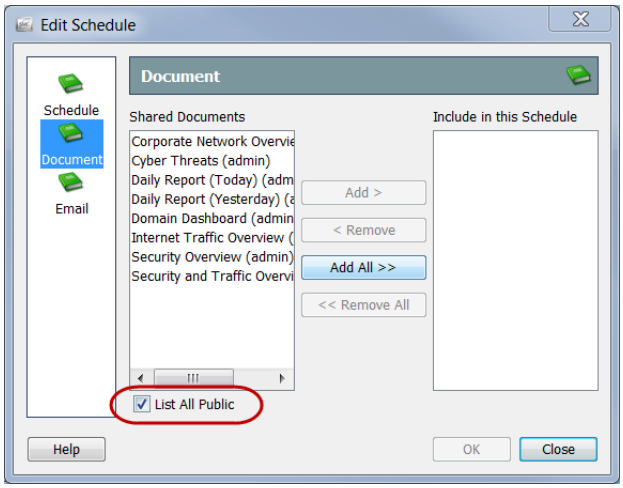
9. 원하는 대로 설정을 변경합니다. 옵션에 대한 자세한 내용을 확인하려면 **Help(도움말)**를 클릭하십시오.

10. 이 장의 다음 내용인 "일정에 문서 추가"를 계속 진행합니다.

일정에 문서 추가

하나 이상의 문서를 일정에 추가하려면 다음 단계를 수행하십시오.

1. Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자에서 **Document(문서)** 아이콘을 클릭합니다. Document(문서) 페이지가 열립니다.



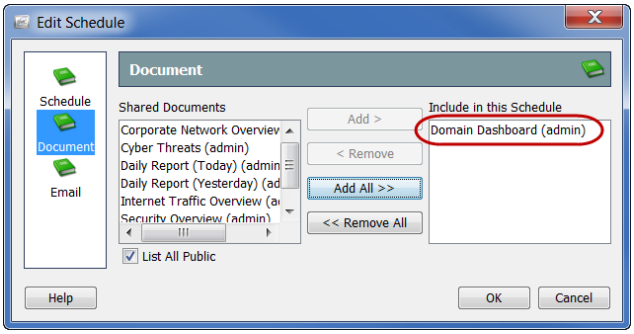
2. 아직 선택하지 않은 경우 **List All Public(모든 공용 문서 나열)** 확인란을 선택합니다. (자세한 내용은 13장, "문서 작업"에서 314페이지의 "공용 문서"를 참조하십시오.)

3. 일정에 추가할 문서를 선택합니다. 이 예에서는 Domain Dashboard(도메인 대시보드) 문서를 선택합니다.

참고:

둘 이상의 문서를 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 문서를 클릭합니다. 문서의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 문서를 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 문서를 클릭합니다.

4. **Add(추가)**를 클릭합니다. 문서가 Include in This Schedule(이 일정에 포함) 필드에 나타납니다.



5. SMC에서 예약된 문서를 자동으로 이 사용자에게 이메일로 보내도록 설정하시겠습니까?
   - 대답이 예인 경우 이 장의 다음 내용인 "일정에 사용자 이메일 주소 추가"를 계속 진행합니다.
   - 대답이 아니요인 경우 **OK(확인)**를 클릭하여 정보를 저장하고 Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자를 종료한 다음 Manage Documents(문서 관리) 대화 상자로 돌아갑니다.
6. 나머지 대화 상자를 닫습니다.

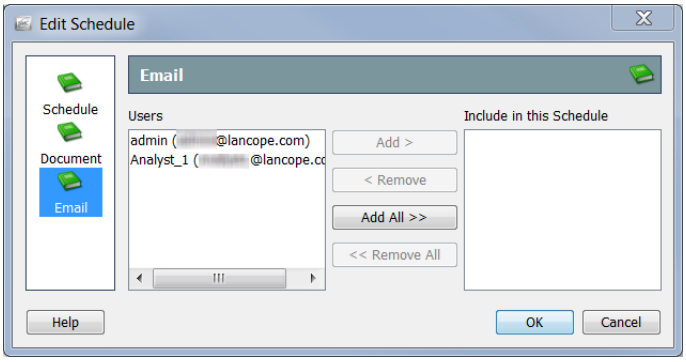
일정에 사용자 이메일 주소 추가

참고:

SMC에 이메일 서버의 IP 주소를 추가하지 않은 경우 먼저 이 작업을 수행해야 SMC에서 예약된 문서를 이메일로 보내도록 설정할 수 있습니다. (자세한 내용은 13장, "문서 작업"에서 321페이지의 "SMC에 이메일 서버 추가"를 참조하십시오.)

SMC에서 예약된 문서를 누군가에게 자동으로 이메일로 보내도록 설정하려는 경우 다음 단계를 완료하여 일정에 이메일 주소를 추가해야 합니다.

1. Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자에서 **Email(이메일)** 아이콘을 클릭합니다. Email(이메일) 페이지가 열립니다.



2. Users(사용자) 필드에서 사용자의 이메일 주소를 선택합니다.
3. **Add(추가)**를 클릭합니다. 이메일 주소가 Include in This Schedule(이 일정에 포함) 필드에 나타납니다.

참고:

둘 이상의 이메일 주소를 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 이메일 주소를 클릭합니다. 이메일 주소의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 이메일 주소를 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 이메일 주소를 클릭합니다.

4. **OK(확인)**를 클릭하여 정보를 저장하고 Add (or Edit) Schedule(일정 추가 또는 편집) 대화 상자를 종료한 다음 Manage Documents(문서 관리) 대화 상자로 돌아갑니다.
5. 로그인 문서를 이 섹션에 추가하시겠습니까?
   - 대답이 예인 경우 이 장의 다음 내용인 "로그인 문서"를 계속 진행합니다.
   - 대답이 아니요인 경우, 나머지 대화 상자를 닫습니다.

로그인 문서

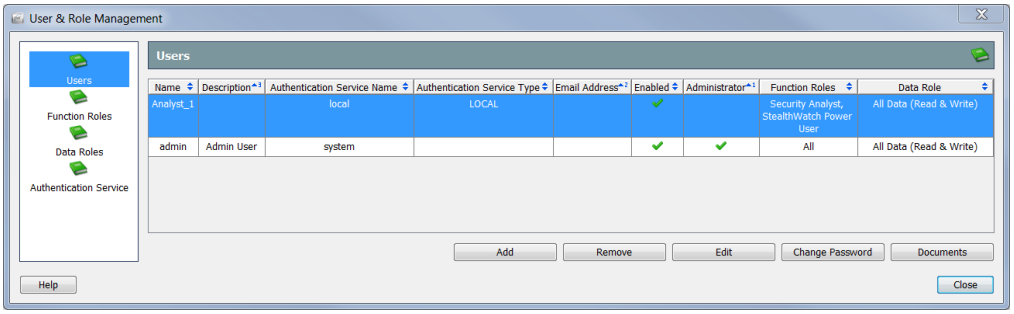
어떤 문서든 로그인 문서 리스트에 추가할 수 있습니다. 로그인 문서는 SMC 클라이언트 인터페이스에 로그인할 때마다 자동으로 열립니다. 이 기능을 사용하지 않으면 정기적으로 문서를 수동으로 열어야 하므로 이 기능은 문서를 확인하는 데 유용합니다.

참고:

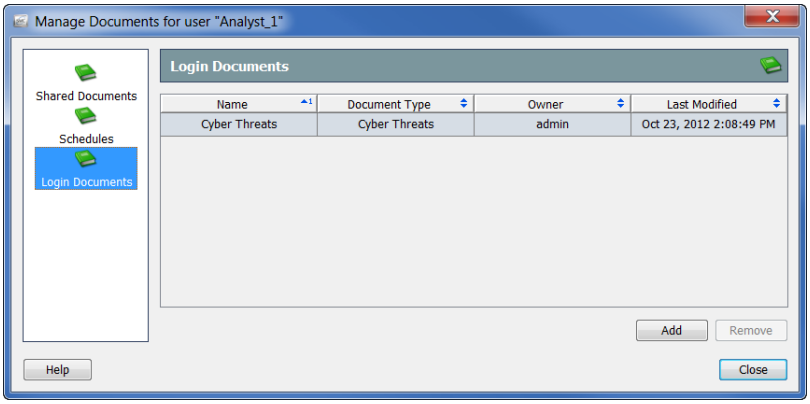
이 섹션에서는 원하는 공유 문서가 이미 생성되어 있는 것으로 가정합니다. 공유 문서 생성에 대한 자세한 내용은 13장, "문서 작업"을 참조하십시오.

문서를 사용자 계정의 로그인 문서로 설정하려면 다음 단계를 수행하십시오.

1. SMC 메인 메뉴에서 **Configuration(컨피그레이션) > User Management(사용자 관리)**를 선택합니다. User & Role Management(사용자 및 역할 관리) 대화 상자가 열립니다.

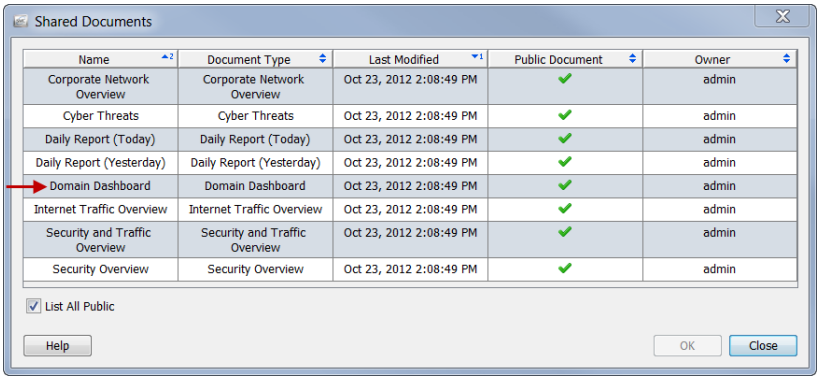


2. **Users(사용자)** 아이콘을 클릭합니다. Users(사용자) 페이지가 열립니다.
3. 로그인 문서를 추가할 사용자 계정을 선택합니다.
4. **Documents(문서)**를 클릭합니다. 선택한 사용자에 대한 Manage Documents(문서 관리) 대화 상자가 열립니다.



5. **Login Documents(로그인 문서)** 아이콘을 클릭합니다. Login Documents(로그인 문서) 페이지가 열립니다.

6. **Add(추가)**를 클릭합니다. 저장한 모든 문서를 보여주는 Shared Documents(공유 문서) 대화 상자가 열립니다.

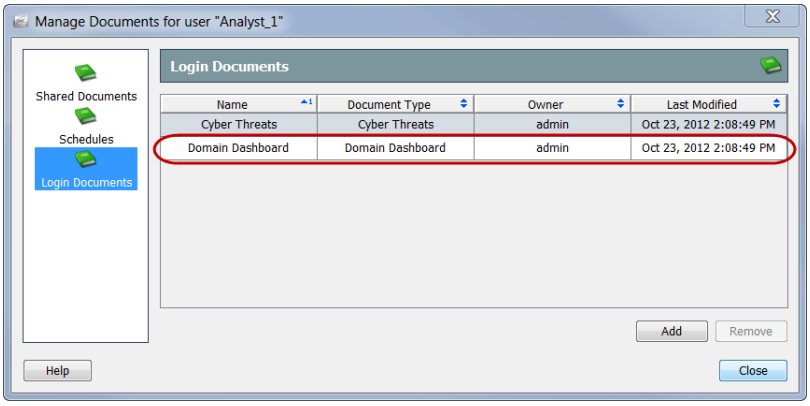


7. 다른 사용자가 저장한 모든 공용 문서를 보려면 **List All Public(모든 공용 문서 나열)** 확인란을 선택합니다.
8. 사용자의 로그인 문서 리스트에 추가할 문서를 선택합니다. 이 예에서는 Domain Dashboard(도메인 대시보드) 문서를 선택합니다.

참고:

둘 이상의 문서를 선택하려면 **Ctrl** 키를 누른 상태에서 추가하려는 각 문서를 클릭합니다. 문서의 범위를 선택하려면 선택하려는 범위 맨 위에 있는 문서를 클릭하고 **Shift** 키를 누른 상태에서 선택하려는 범위 맨 아래에 있는 문서를 클릭합니다.

9. **OK(확인)**를 클릭합니다. Shared Documents(공유 문서) 대화 상자가 닫힙니다. 선택한 문서가 사용자의 로그인 문서 리스트에 나타납니다.



10. **Close(닫기)**를 클릭하여 Manage Documents(문서 관리) 대화 상자를 종료합니다.
11. **Close(닫기)**를 클릭하여 User & Role Management(사용자 및 역할 관리) 대화 상자를 종료합니다.

색인

C

CIDR 형식 157
CSV 파일 64

D

DAR 파일 313
  가져오기 314
  내보내기 313
DAR 파일 가져오기 314
DAR 파일 내보내기 313

I

ICMP 플러드 알람 297
IP 주소
  찾기 186
  호스트 그룹용 104

N

NATed 플로우 72
NetFlow Ninjas 블로그 18

P

P2P 활동 124

R

RADIUS 331

S

SLIC
  C&C 서버 호스트 그룹 208
  봇넷 알람 212
  비활성화 211
  사전 요구 사항 205
  프로세스 207
  활성화 209
SYN 수신됨 알람 304
SYN 플러드 알람 303

T

TACACS 331

U

UDP 플러드 알람 304

V

VM 서버 상태 아이콘 39

ㄱ

개요 19
검색
  문서에서 57, 221
  엔터프라이즈 트리에서 36
고객 지원 18
관계형 플로우 맵 107
관련 문서 18
관심 지표
  증가 125
  퍼센트 127
  포인트 123
  필터 버튼 54, 127
관심 지표 증가 125
관심 지표(CI) 124, 125
구성된 임계값
  대상 지표 129
  파일 공유 지수 130
기능 역할 342
기본 설정, 디스플레이 43
기본 정책 259
기본 정책 편집
  내부 호스트 261
  외부 호스트 261
기본 정책 편집 대화 상자 261
기술 지원 18

ㄴ

낮은 트래픽 알람 298
내보내기
    데이터 65
네트워크
    미세조정 295
    성능 147
네트워크 미세조정 295
네트워크 및 서버 성능 문서 147
네트워크 행동 분석 133
높은 대역폭 호스트, 찾기 189
높은 총 트래픽 알람 296
높은 트래픽 알람 297
느린 인터넷 147

ㄷ

다이어그램
    베이스라인 설정 프로세스 256
    증가하는 CI 단계 125
    호스트 식별 프로세스 216
닫기
    문서 60
    알람 237
닫힌 알람 다시 열기 240
대상 지표 128
    구성된 임계값 129
    퍼센트 128
    필터 버튼 129
대상 지표(TI) 124
대시보드
    호스트 그룹 113
    호스트 그룹 네트워크 114
    호스트 그룹 보안 115
    호스트 그룹 알람 요약 116
더블 클릭 기능 55
데이터 역할 335
    데이터 숨기기 335, 337
    이중화된 FlowCollector 데이터 숨기기 338
도움말
    메뉴 47
    온라인 87
디스플레이 기본 설정 43

ㄹ

라이브 데이터 48
라이선스 활성화 22
라이선싱
    관리되는 어플라이언스 활성화 ... 22
    오프라인 방식, 관리되는 어플라이언스 24
    온라인 방식, 관리되는 어플라이언스 23
로그인
    권한 35
로그인 문서 310, 358

ㅁ

마우스 오른쪽 버튼으로 클릭 기능 . 54, 58
맞춤형 대시보드 35, 44, 117
맞춤형 대시보드 구축 117
메뉴
    도움말 47
    보고서 46
    보기 44
    보안 45
    상태 44
    최상위 44
    컨피그레이션 47
    트래픽 45
    파일 43
    팝업 66
    편집 43
    플로우 46
    호스트 45
메인 메뉴 42
메일 릴레이 알람 298
모두 축소 명령 36
모두 확장 명령 36
문서
    PDF 파일로 저장 86
    공용 314
    공유 313
    닫기 60
    로그인 310, 358
    방향 51
    비활성 50
    새로 고침 48
    아카이브됨 326
    여러 문서 간 이동 49

열기 42
인쇄 80, 82
인쇄 미리보기 80
인쇄 설정 맞춤화 81
일정 지정 316
저장 83, 308
탭 49
툴바 50
헤더 52
활성 50
문서 새로 고침 상태 아이콘 50
문서 아이콘, 설명 15
문서 작성기 117

ㅂ

바로가기, 키보드 92
반복적인 위반자 216
버전 정보 47
버튼
문서로 이동 52, 115, 121
검색 91
관심 지표 필터 54, 127
기타 항목 숨기기 136
대상 지표 필터 129
대시보드 필터 76
리스트 49
새로 고침 48
선택 항목 닫기 239
선택 항목 확인 235
위로/아래로 61
이후 데이터 보기 48
즐겨찾기 검색 89
축소 68
툴바 50
파일 공유 지수 필터 131
표시/숨기기 69
플로우 테이블 219
필터 71
항목 즐겨찾기 90
형광펜 91
베이스라인 설정 254
보고서 메뉴 46
보기 메뉴 44
보안 메뉴 45
불필요한 알람 230
블로그, NetFlow Ninjas 18
비디오 라이브러리 18
비인가 호스트 100
비정상적인 행동 123
비활성 문서 50
빠른 보기 67, 171

ㅅ

사용자 관리 330
기능 역할 추가 342
데이터 숨기기 335, 337
데이터 역할 추가 335
사용자 계정 추가 344
사용자 계정 편집 346
사전 정의된 그룹에 호스트 할당 274
사전 정의된 호스트 그룹 274
삭제
기능 역할 342
데이터 역할 336
사용자 344
상대 시간 설정 78
상위 관심 지표 알람 125, 295
상위 파일 공유 지수 알람 296
상태 메뉴 44
새 플로우 시작됨 알람 300
새 플로우 제공됨 알람 300
새로 고침
문서 48
엔터프라이즈 트리 39
생성
역할 정책 275
호스트 정책 283
서버 응답 시간(SRT) 149
서버, 성능 147
설정 편집 대화 상자 288
설정/해제 알람 289
소스 호스트 215
수정
기능 역할 342
데이터 역할 336
사용자 344
스팸 소스 알람 301
시각적 편집기 대화 상자 293

o

아이콘
VM 서버 상태 39
문서 새로 고침 상태 50
아카이브 문서 326
아카이브 시간 126
알람
닫기 237
닫힌 알람 다시 열기 240
대응 273
봇넷 알람 212
설정/해제 289
심각도 레벨 38
완화, 권한 부여 모드 249
완화, 자동 모드 250
임계값 설정 292
차이 기반 289
차이 기반 설정 292
트리거 258
표시기 39
행동 설정 292
허용 수준설정 292
확인 235
확인 취소 237
알람 요약 217
알람 테이블 219
알람 확인 235
알람 확인 취소 237
알람에 대응 273
알람에 대한 임계값 설정 292
알람에 대한 행동 설정 292
알람에 대한 허용 수준설정 292
약어 16
어플라이언스에 대한 라이선스 정보
기능 라이선스 상태 정보 30
플로우 수집 정보 29
엔터프라이즈 트리 36, 39
브랜치 37
역할 정책 259
역할 정책 추가 대화 상자 277
역할 정책 편집 대화 상자 282
열
숨기기 63
이동 62
정렬 61
크기 조정 62
표시 63
열기
문서 42
예약된 문서
SMC에 이메일 서버 추가 321
기존 일정 활성화 319, 353
문서 추가 320, 355
사용자 계정과 연결 349
사용자 이메일 주소 추가 ... 323, 356
새 일정 추가 316, 350
이메일 보내기 321
온라인 도움말 47, 87
검색 옵션 88
목차 옵션 88
빠른 검색 옵션 90
색인 옵션 88
용어집 옵션 89
즐겨찾기 리스트 89
즐겨찾기 옵션 90
완화 기능
권한 부여 모드 241, 247
대응 유형 247
비활성화 모드 247
수동 모드 241
자동 모드 241, 247
프로세스 241
완화 디바이스
구성 243
유형 242
활성화 245
완화 옵션, 유형 248
완화 작업 문서 251
완화 작업, 정의 247
완화, 해당 알람
자동 모드 250
완화, 해당하는 알람
권한 부여 모드 249
왕복 시간(RTT) 148
외부 조회 193
웜 활동 알람 305
유효한 호스트 대화 상자 262
유효한 호스트 정책 262
의심스러운 UDP 활동 알람 303
의심스러운 긴 플로우 알람 302

의심스러운 데이터 손실 알람 301
이중화된 FlowCollector 335, 337
인쇄
문서 80, 82
인쇄 설정 맞춤화 81
인쇄 미리보기 80
인증 서비스 331
인터넷 트래픽 개요 134
인터넷, 느림 147
일반 알람
ICMP 플러드 297
SYN 수신됨 304
SYN 플러드 303
UDP 플러드 304
낮은 트래픽 298
높은 총 트래픽 296
높은 트래픽 297
메일 릴레이 298
상위 관심도 295
상위 파일 공유 지수 296
새 플로우 시작됨 300
새 플로우 제공됨 300
스팸 소스 301
웜 활동 305
의심스러운 UDP 활동 303
의심스러운 긴 플로우 302
의심스러운 데이터 손실 301
최대 플로우 시작됨 299
최대 플로우 제공됨 299

ㅈ

저장
PDF 파일로 문서 저장 86
문서 83, 308
전체 검색 57, 221
절대 시간 설정 78
접근된 호스트 226
접근된 호스트 문서 226
정상적인 행동 230
정적 데이터 48
정책
기본 259
내부 호스트 편집 261
역할 259
역할 생성 275
역할 편집 281
외부 호스트 편집 261
유효한 호스트 262
호스트 259
호스트 생성 283
호스트 편집 287
지표 123

ㅊ

차이 기반 알람 289
설정 292
차트
X축, Y축 69
범례 69
확대 및 축소 68
차트 속성 대화 상자 69
최대 플로우 시작됨 알람 299
최대 플로우 제공됨 알람 299
최상위 메뉴 44
추가
기능 역할 342
데이터 역할 336
사용자 344

ㅋ

컨피그레이션 메뉴 47
키보드 바로가기 92

ㅌ

탭
문서 49
배열 52
탭 그룹 콘텐츠 변경 52
페이지 49
테이블
기본값 복원 64
행 색상 61
테이블 기본값 복원 64
통신 상태 40
툴바 50
툴팁 40
트래픽
모니터링 134
방향 식별 178
인터넷 트래픽 개요 134
회사 네트워크 개요 137

트래픽 메뉴 45
트래픽 모니터링 134
트리 브랜치 37
트리 숨기기 명령 36

ㅍ

파일 공유 226
파일 공유 지수 124, 129
  구성된 임계값 130
  퍼센트 130
  필터 버튼 131
파일 메뉴 43
팝업 메뉴 66
페이지 탭 49
편집
  역할 정책 281
  호스트 정책 287
편집 메뉴 43
폰트, 변경 82
플로우 메뉴 46
플로우 분석 시나리오 워크플로
  느린 네트워크 184
  상위 관심 지표 호스트 172
  서비스 트래픽 급증 176
  오버로드된 인터페이스 181
플로우 시나리오 워크플로
  느린 네트워크 184
  상위 관심 지표 호스트 172
  애플리케이션 트래픽 급증 176
  오버로드된 인터페이스 181
플로우 조사 53
플로우 쿼리 154
플로우 테이블 53, 155
  버튼 219
  짧은 리스트 탭 169
  테이블 탭 168
플로우 테이블 필터
  고급 페이지 75, 167
  날짜/시간 페이지 72, 155
  라우팅 페이지 74, 163
  서비스 및 애플리케이션 페이지 74, 161
  성능 페이지 74, 165
  애플리케이션 세부사항 페이지 74, 166
  인터페이스 페이지 73, 160
  트래픽 페이지 74, 164
  포트 및 프로토콜 페이지 74, 162
  호스트 페이지 72, 157

ㅎ

호스트
  공통적인 특징 공유 231
  동작 45
  베이스라인 설정 254
  접근됨 226
호스트 IQ 232
  수행 231
호스트 그룹 98
  C&C 서버 101, 208
  IP 주소 104
  모두 탐지 99
  사전 정의됨 274
호스트 그룹 네트워크 대시보드 114
호스트 그룹 대시보드 113
호스트 그룹 멤버십 보고서 106
호스트 그룹 보안 대시보드 53, 115
호스트 그룹 알람 요약 대시보드 116
호스트 그룹 편집기 대화 상자 274
호스트 메뉴 45
호스트 스냅샷 217, 223
  ID, DHCP 및 호스트 메모 탭 228
  보안 이벤트 탭 227
  보안 탭 226
  상위 활성 플로우 탭 228
  식별 탭 224
  알람 탭 225
  엑스포터 인터페이스 탭 229
호스트 식별 프로세스 216
호스트 정보
  문서 232
  필터 231
호스트 정책 259
호스트 정책 관리 259
호스트 정책 관리자 대화 상자 260
호스트 정책 편집 대화 상자 285
활성 문서 50
회사 네트워크 개요 137