

ASA 및 FTD용 SNMP Syslog 트랩 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[ASA 컨피그레이션](#)

[FDM에서 관리하는 FTD 구성](#)

[FMC에서 관리하는 FTD 컨피그레이션](#)

[다음을 확인합니다.](#)

[snmp-server 통계 표시](#)

[로깅 설정 표시](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 및 FTD(Firepower Threat Defense)에서 Syslog 메시지를 전송하도록 SNMP(Simple Network Management Protocol) 트랩을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA에 대한 기본 지식
- Cisco FTD에 대한 기본 지식
- SNMP 프로토콜에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Firepower Threat Defense for AWS 6.6.0
- Firepower Management Center 버전 6.6.0
- Cisco Adaptive Security Appliance Software 버전 9.12(3)9

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Cisco ASA 및 FTD에는 로깅 정보를 제공하는 여러 기능이 있습니다. 그러나 Syslog 서버가 옵션이 아닌 특정 위치가 있습니다. 사용 가능한 SNMP 서버가 있는 경우 SNMP 트랩을 사용할 수 있습니다.

이 도구는 문제 해결 또는 모니터링을 위해 특정 메시지를 보내는 데 유용합니다. 예를 들어, 장애 조치 시나리오 중에 추적해야 하는 관련 문제가 있는 경우 FTD 및 ASA의 클래스 ha에 대한 SNMP 트랩을 사용하여 이러한 메시지에만 집중할 수 있습니다.

Syslog 클래스와 관련된 자세한 내용은 [이 문서](#)에서 확인할 수 있습니다.

이 문서의 목적은 CLI(Command Line Interface), FMC에서 관리하는 FTD 및 FDM(Firepower Device Manager)에서 관리하는 FTD를 사용하는 ASA에 대한 구성 예를 제공하는 것입니다.

FTD에 Cisco CDO(Defense Orchestrator)를 사용하는 경우 이 컨피그레이션을 FDM 인터페이스에 추가해야 합니다.

주의: 높은 syslog 속도의 경우 다른 작업에 영향을 미치지 않도록 syslog 메시지에 속도 제한을 구성하는 것이 좋습니다.

이 문서의 모든 예제에 사용되는 정보입니다.

SNMP 버전: **SNMPv3**

SNMPv3 그룹: **그룹 이름**

SNMPv3 사용자: 인증을 위한 HMAC SHA 알고리즘을 사용하는 **admin-user**

SNMP 서버 IP 주소: **10.20.15.12**

SNMP 서버와 통신하는 데 사용할 ASA/FTD 인터페이스: **외부**

Syslog 메시지 ID: **111009**

구성

ASA 컨피그레이션

이 단계는 아래 정보를 따라 ASA에서 SNMP 트랩을 구성하는 데 사용할 수 있습니다.

1단계. Syslog 목록에 추가할 메시지를 구성합니다.

```
logging list syslog-list message 111009
```

2단계. SNMPv3 서버 매개변수를 구성합니다.

```
snmp-server enable
```

```
snmp-server group group-name v3 auth
```

```
snmp-server user admin-user group-name v3 auth sha cisco123
```

3단계. SNMP 트랩을 활성화합니다.

```
snmp-server enable traps syslog
```

4단계. SNMP 트랩을 로깅 대상으로 추가합니다.

```
logging history syslog-list
```

FDM에서 관리하는 FTD 구성

FDM에서 FTD를 관리할 때 SNMP 서버에 전송할 특정 Syslog 목록을 구성하는 데 이 단계를 사용할 수 있습니다.

1단계. Objects(개체) > Event List Filters(이벤트 목록 필터)로 이동하고 +버튼에서 선택합니다.

2단계. 짝수 목록의 이름을 지정하고 관련 클래스 또는 메시지 ID를 포함합니다.그런 다음 확인을 선택합니다.

Edit Event List Filter

Name

Description

Severity and Log Class

Syslog Range / Message ID

100000 - 999999

[Add Another Syslog Range / Message ID](#)

CANCEL OK

3단계. FDM 홈 화면에서 [고급 구성] > [FlexConfig] > [FlexConfig 객체]로 이동하고 + 단추를 선택합니다.

다음 정보를 사용하여 다음 FlexConfig 개체를 만듭니다.

Name(이름): **SNMP-Server**

설명(선택 사항):**SNMP 서버 정보**

템플릿:

```
snmp-server enable
snmp-server group group-name v3 auth
snmp-server user admin-user group-name v3 auth sha cisco123
snmp-server host outside 10.20.15.12 version 3 admin-user
```

템플릿 무효화:

```
no snmp-server host outside 10.20.15.12 version 3 admin-user
no snmp-server user admin-user group-name v3 auth sha cisco123
no snmp-server group group-name v3 auth
no snmp-server enable
```

Edit FlexConfig Object



Name

SNMP-Server

Description

SNMP Server Information

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 snmp-server enable
2 snmp-server group group-name v3 auth
3 snmp-server user admin-user group-name v3 auth sha cisco123
4 snmp-server host outside 10.20.15.12 version 3 admin-user
```

Negate Template ⚠

Expand | Reset

```
1 no snmp-server host outside 10.20.15.12 version 3 admin-user
2 no snmp-server user admin-user group-name v3 auth sha cisco123
3 no snmp-server group group-name v3 auth
4 no snmp-server enable
```

CANCEL

OK

Name(이름): **SNMP-Traps**

설명(선택 사항): **SNMP 트랩 사용**

템플릿:

snmp-server enable traps syslog

템플릿 무효화:

no snmp-server enable traps syslog

Edit FlexConfig Object



Name

SNMP-Traps

Description

Enable SNMP traps

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 snmp-server enable traps syslog
```

Negate Template

Expand | Reset

```
1 no snmp-server enable traps syslog
```

CANCEL

OK

이름: 로깅 기록

설명(선택 사항): SNMP 트랩 syslog 메시지를 설정하는 개체입니다.

템플릿:

```
logging history logging-list
```

템플릿 무효화:

```
no logging history logging-list
```

Create FlexConfig Object



Name

Logging-List

Description

Syslog list to send through SNMP traps



Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 logging list syslog-list message 111009
2 logging trap syslog-list
```

Negate Template

Expand | Reset

```
1 no logging trap syslog-list
2 no logging list syslog-list message 111009
```

CANCEL

OK

4단계. Advanced Configuration(고급 컨피그레이션) > FlexConfig > FlexConfig Policy(FlexConfig 정책)로 이동하고 이전 단계에서 생성된 모든 객체를 추가합니다.중속 명령이 동일한 객체(SNMP-Server)에 포함되어 있으므로 순서는 관련이 없습니다. 세 개의 객체가 있고 Preview 섹션에 명령 목록이 표시되면 Save를 선택합니다.

Successfully saved.

Group List

- 1. Logging-history
- 2. SNMP-Server
- 3. SNMP-Traps

Preview

```
1 logging history logging-list
2 snmp-server enable
3 snmp-server group group-name v3 auth
4 snmp-server user admin-user group-name v3 auth sha cisco123
5 snmp-server host outside 10.20.15.12 version 3 admin-user
6 snmp-server enable traps syslog
```

SAVE

5단계. 배치 아이콘을 선택하여 변경사항을 적용합니다.

FMC에서 관리하는 FTD 컨피그레이션

위의 예에서는 이전 시나리오와 유사한 시나리오를 보여 주지만 이러한 변경 사항은 FMC에서 구성한 다음 FTD에서 관리하는 FTD에 구축됩니다. SNMPv2도 사용할 수 있습니다. [이 문서에서는](#) FMC 관리를 사용하여 FTD에서 이 버전의 SNMP 서버를 설정하는 방법을 설명합니다.

1단계. Devices(디바이스) > Platform Settings(플랫폼 설정)로 이동하고 관리되는 디바이스에 할당된 정책에서 Edit(수정)를 선택하여 컨피그레이션을 적용합니다.

2단계. SNMP로 이동하고 Enable SNMP Servers 옵션을 선택합니다.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help

Device Management NAT VPN QoS **Platform Settings** FlexConfig Certificates

FTD-PS You have unsaved changes Save

Enter Description Policy A

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP
ICMP
Secure Shell
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
Time Zone
UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

Hosts Users **SNMP Traps**

Interface	Network	SNMP Version	Poll/Trap	Trap Port	Username
No records to display					

3단계. 사용자 탭을 선택하고 추가 버튼을 선택합니다. 사용자 정보를 입력합니다.

Add Username ? X

Security Level	Auth
Username*	user-admin
Encryption Password Type	Clear Text
Auth Algorithm Type	SHA
Authentication Password*	••••••••
Confirm*	••••••••
Encryption Type	
Encryption Password	
Confirm	

OK Cancel

4단계. Hosts(호스트) 탭에서 Add(추가)를 선택합니다. SNMP 서버와 관련된 정보를 입력합니다. 영역 대신 인터페이스를 사용하는 경우 오른쪽 코너 섹션에 인터페이스 이름을 수동으로 추가해야 합니다. 필요한 정보가 모두 포함되면 확인을 선택합니다.

Add SNMP Management Hosts

IP Address* +

SNMP Version

Username

Community String

Confirm

Poll

Trap

Trap Port (1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface


Available Zones ↻


Selected Zones/Interfaces

outside	✕
---------	---

5단계. **SNMP Traps(SNMP 트랩)** 탭을 선택하고 Syslog(Syslog) 상자를 선택합니다. 다른 트랩 확인 표시가 필요하지 않은 경우 해당 표시를 모두 제거해야 합니다.

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

FTD-PS You have unsaved changes 

Enter Description  Policy A

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

Hosts **Users** **SNMP Traps**

Enable Traps All SNMP Syslog

Standard

Authentication

Link up

Link Down

Cold Start

Warm Start

Entity MIB

6단계. Syslog로 이동하고 **Event Lists** 탭을 선택합니다. 추가 버튼을 선택합니다. 목록에 포함할 이름과 메시지를 추가합니다. 계속하려면 **확인**을 선택합니다.



Add Event List ? X

Name*

Severity/EventClass

Message ID

+ Add

Message IDs
111009  

OK

Cancel

7단계. Logging **Destinations**(로깅 대상) 탭을 선택하고 Add(추가) 버튼을 선택합니다.

Logging Destination(로깅 대상)을 **SNMP Trap**(SNMP 트랩)으로 변경합니다.

User Event List(사용자 이벤트 목록)를 선택하고 옆에 있는 6단계에서 생성한 이벤트 목록을 선택합니다.

확인을 선택하여 이 섹션 편집을 완료합니다.

Add Logging Filter ? X

Logging Destination: SNMP Trap

Event Class: Use Event List logging-list

+ Add

Event Class	Syslog Severity
No records to display	

OK Cancel

8단계. Save(저장) 버튼을 선택하고 **Deploy** the changes to the managed device(관리되는 디바이스에 변경 사항 배포)를 선택합니다.

다음을 확인합니다.

아래 명령은 FTD CLISH 및 ASA CLI에서 모두 사용할 수 있습니다.

snmp-server 통계 표시

"**show snmp-server statistics**" 명령은 트랩이 전송된 횟수에 대한 정보를 제공합니다.이 카운터는 다른 트랩을 포함할 수 있습니다.

```
# show snmp-server statistics
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
```

```
0 Get-next PDUs
0 Get-bulk PDUs
0 Set-request PDUs (Not supported)
2 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
```

2 Trap PDUs

이 예에서 사용되는 메시지 ID는 사용자가 명령을 실행할 때마다 트리거됩니다."show" 명령을 실행할 때마다 카운터가 증가합니다.

로깅 설정 표시

"show logging setting"은 각 대상에서 보낸 메시지에 대한 정보를 제공합니다.기록 로깅은 SNMP 트랩에 대한 카운터를 나타냅니다.트랩 로깅 통계는 Syslog 호스트 카운터와 관련되어 있습니다.

```
# show logging setting
Syslog logging: enabled
Facility: 20
Timestamp logging: enabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 30 messages logged
Trap logging: level debugging, facility 20, 30 messages logged
Global TCP syslog stats::
NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
PARTIAL_REWRITE_CNT: 0
Permit-hostdown logging: disabled
History logging: list syslog-list, 14 messages logged
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

"show logging queue" 명령을 실행하여 메시지를 삭제하지 않도록 합니다.

```
# show logging queue

Logging Queue length limit : 512 msg(s)
0 msg (s) discarded due to queue overflow
0 msg (s) discarded due to memory allocation failure
Current 0 msg on queue, 231 msgs most on queue
```

관련 정보

- [Cisco ASA Series Syslog 메시지](#)
- [CLI Book 1: Cisco ASA Series General Operations CLI 컨피그레이션 가이드, 9.12](#)
- [Firepower NGFW 어플라이언스에서 SNMP 구성](#)