SDWAN용 컨피그레이션 그룹을 사용하여 보안 기능 활성화

목차

소개

이 문서에서는 컨피그레이션 그룹을 통한 NGFW, URL 필터링, AMP 및 IPS/IDS 구성에 대해 설명하며, 여기에는 통합 로깅에 대한 지침이 포함되어 있습니다.

사전 요구 사항

플로우 가시성 및 앱 가시성 활성화

정책 그룹을 사용하여 정책을 정의하는 경우

- Policy group(정책 그룹)을 선택한 다음 Application priority and SLA(애플리케이션 우선순위 및 SLA)를 선택합니다.
- Add new(새로 추가)를 선택합니다.
- Additional settings(추가 설정)를 클릭하고 Application visibility and Flow visibility(애플리케이션 가시성 및 플로우 가시성)를 활성화합니다

레거시 정책을 사용하는 경우

- 컨피그레이션 그룹에서 Cli 애드온 프로필을 선택하고 다음 명령을 추가합니다

```
policy
app-visibility
flow-visibility
```

기능에 대한 전제 조건을 준수해야 합니다 (https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/url-filtering.html).

```
Note: If you are using the legacy policy along with Configuration groups :

Select Configuration and Click Security
Click Custom Options and select Policies/Profiles and then access these features to enable
```

이 문서에서는 정책 그룹을 사용하여 활성화할 기능에 대해 중점적으로 설명합니다

차세대 방화벽(NGFW)

NGFW를 활성화하려면 다음 단계를 수행합니다.

- Policy group(정책 그룹)을 선택하고 NGFW를 클릭한 다음 Add NGFW Policy(NGFW 정책 추가)를 클릭합니다
- 정책 이름을 지정하고 Next(다음)를 클릭합니다.
- NGFW 정책과 연결할 컨피그레이션 그룹을 선택합니다
- 규칙을 추가하고 Next를 클릭합니다
- NGFW 정책 생성

업로깅을 활성화하려면 NGFW 정책을 수정한 다음 Additional Settings(추가 설정)를 선택하고 Unified Logging(통합 로깅)을 켭니다

URL 필터링

20.18 이전 릴리스에 대해 URL 필터링을 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Groups of Interest(관심 그룹)를 클릭합니다
- Security(보안)를 선택한 다음 Profiles(프로파일)를 확장합니다.

릴리스 20.18 이상에 대해 url 필터링을 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Objects and Profiles(개체 및 프로필)를 클릭합니다
- 보안 프로필 선택

Add url filtering(URL 필터링 추가)을 선택하고 세부 정보를 입력한 다음 save(저장)를 클릭합니다.

AMP(Advanced Malware Protection)

20.18 이전 릴리스용 AMP를 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Groups of Interest(관심 그룹)를 클릭합니다
- Security(보안)를 선택한 다음 Profiles(프로파일)를 확장합니다.

AMP for Releases 20.18 이상을 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Objects and Profiles(개체 및 프로필)를 클릭합니다
- 보안 프로필 선택

Advanced Malware Protection을 선택하고 Add Advanced Malware Protection을 클릭합니다

세부 정보를 추가하고 저장을 클릭합니다.

IPS(Intrusion Prevention System)/IDS(Intrusion Prevention Detection)

20.18 이전 릴리스에 대해 IPS/IDS를 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Groups of Interest(관심 그룹)를 클릭합니다
- Security(보안)를 선택한 다음 Profiles(프로파일)를 확장합니다.

릴리스 20.18 이상에 대해 IPS/IDS를 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Objects and Profiles(개체 및 프로필)를 클릭합니다
- 보안 프로필 선택

Intrusion Prevention을 선택하고 Add Intrusion Prevention을 클릭합니다

세부 정보를 추가하고 저장을 클릭합니다.

AIP(Advanced Inspection Profile) 생성

20.18 이전 릴리스에 대해 AIP를 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Groups of Interest(관심 그룹)를 클릭합니다
- Security(보안)를 선택한 다음 Profiles(프로파일)를 확장합니다.

릴리스 20.18 이상에 대해 AIP를 활성화하려면

- UI에서 Configuration(컨피그레이션)을 선택한 다음 Policy group(정책 그룹)을 선택하고 Objects and Profiles(개체 및 프로필)를 클릭합니다
- 보안 프로필 선택

Advanced Inspection Profile을 선택하고 Add Advanced Inspection Profile을 클릭합니다

- 이전 단계에서 생성한 AMP/IPS/Url 필터링 이름을 입력하고 save를 클릭합니다

AIP와 NGFW의 연계

- Configuration(컨피그레이션)을 선택한 다음 Policy groups(정책 그룹)를 선택하고 NGFW를 클릭합니다
- 이전에 생성한 NGFW 정책 수정
- 이전에 생성한 NGFW 규칙의 경우 이전에 생성한 AIP 프로필을 수정 및 연결한 후 save(저장)를 클릭합니다

로깅

ulogging의 경우 cli add on을 사용하여 컨피그레이션 그룹을 통해 라우터에서 기능을 활성화합니다

```
policy
ip visibility features
ulogging enable

parameter-map type inspect-global
log dropped-packets
log flow-export fnf
log flow
!
utd engine standard unified-policy
utd global
flow-logging all
```

확인

```
show  flow monitor sdwan-flow-monitor cache

IPV4 SOURCE ADDRESS:                              10.100.10.75
IPV4 DESTINATION ADDRESS:                         10.10.10.25
TRNS SOURCE PORT:                                 53
TRNS DESTINATION PORT:                            34796
IP VPN ID:                                        10
IP PROTOCOL:                                      17
tcp flags:                                        0x00
interface input:                                  Gi2
interface output:                                 Gi3
flow cts source group tag:                        0
flow cts destination group tag:                   0
counter bytes long:                               125
counter packets long:                             1
timestamp abs first:                              14:59:47.613
timestamp abs last:                               14:59:47.613
flow end reason:                                  Not determined
connection initiator:                             Reverse initiator
interface overlay session id input:               10
interface overlay session id output:              0
connection connection id long:                    0x000000000050D9CC
drop cause id:                                    0
counter bytes drop long:                          0
sdwan sla not met :                               0
sdwan preferred color not met :                   0
sdwan queue id :                                  2
counter packets drop long:                        0
ulogging fw zp id:                                4
ulogging fw zone id array:                        3 3
ulogging fw class id:                             12544961
ulogging fw policy id:                            5559936
ulogging fw proto id:                             25
ulogging fw action:                               2
ulogging fw drop reason id:                       0
ulogging fw source ipv4 address translated:       0.0.0.0
ulogging fw destination ipv4 address translated:  0.0.0.0
ulogging fw source port translated:               0
ulogging fw destination port translated:          0
ulogging utd ips pri:                             1
```

```
ulogging utd ips sid:                              57756
ulogging utd ips gid:                              1
ulogging utd ips cid:                              21
ulogging utd urlf url hash:                        00000000000000000000000000000000
ulogging utd urlf url category:                    0
ulogging utd urlf url reputation:                  0
ulogging utd urlf application name:
ulogging utd amp dispos:                           0
ulogging utd amp filename hash:                    00000000000000000000000000000000
ulogging utd amp file type:                        0
ulogging utd amp file hash:                        0000000000000000000000000000000000000000000000000000000000000000
ulogging utd amp malname hash:                     00000000000000000000000000000000
ulogging utd drop reason id:                       0
ulogging sdvt drop reason id:                      0
ulogging utd ips policy id:                        1
ulogging utd ips action id:                        1
ulogging utd urlf policy id:                       N/A
ulogging utd urlf action id:                       N/A
ulogging utd amp policy id:                        N/A
ulogging utd amp action id:                        N/A
ulogging utd urlf reason id:                       0
ulogging ulogging flow direction:                  Reverse initiator
ulogging fw user name:
ulogging fw source ipv6 address translated:        ::
ulogging fw destination ipv6 address translated:   ::
ip dscp:                                           0x00
application name:                                  port dns
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.