보안 인증서 컴플라이언스

보안 인증서 컴플라이언스

미국 연방 정부 기관은 미 국방성 및 글로벌 인증 기관에서 마련한 보안 표준을 준수하는 장비 및 소프트웨어만 사용해야 할 경우가 있습니다. Firepower 4100/9300 섀시는 이러한 보안 인증 표준의 컴플라이언스를 지원합니다.

이러한 표준의 컴플라이언스를 지원하는 기능을 활성하하는 단계는 다음 항목을 참조하십시오.

- FIPS 모드 활성화
- Common Criteria 모드 활성화
- IPSec 보안 채널 구성, 3 페이지
- 트러스트 포인트에 대한 정적 CRL 구성, 9 페이지
- 인증서 해지 목록 확인 정보, 10 페이지
- CRL 주기적 다운로드 구성, 15 페이지
- NTP를 사용하여 날짜 및 시간 설정
- LDAP 키 링 인증서 설정, 16 페이지
- IP 액세스 목록 구성
- 클라이언트 인증서 인증 활성화, 17 페이지

- 최소 비밀번호 길이 확인 구성
- 최대 로그인 시도 횟수 설정

참고 이러한 항목은 Firepower 4100/9300 섀시에서 인증 컴플라이언스를 활성화하는 방법에 대해서만 설명합니다. Firepower 4100/9300 섀시에서 인증 컴플라이언스를 활성화한다고 해서 연결된 논리적 디바이스로 컴플라이언스가 자동으로 전파되지는 않습니다.

SSH 호스트 키 생성

FXOS 릴리스 2.0.1 이전에는, 디바이스의 초기 설정 중 생성된 SSH 호스트 키가 1024비트로 하드 코딩되었습니다. FIPS 및 Common Criteria 인증을 준수하려면 이러한 과거의 호스트 키를 삭제하고 새 호스트 키를 생성해야 합니다. 자세한 내용은 FIPS 모드 활성화 또는 Common Criteria 모드 활성화를 참조하십시오.

과거의 SSH 호스트 키를 삭제하고 인증을 준수하는 새 호스트 키를 생성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** FXOS CLI에서 서비스 모드로 들어갑니다.

scope system

scope services

단계 **2** SSH 호스트 키를 삭제합니다.

delete ssh-server host-key

단계 **3** 구성을 커밋합니다.

commit-buffer

단계 **4** SSH 호스트 키 크기를 2048비트로 설정합니다.

set ssh-server host-key rsa 2048

단계 **5** 구성을 커밋합니다.

commit-buffer

단계 **6** 새 SSH 호스트 키를 생성합니다.

create ssh-server host-key

commit-buffer

단계 **7** 새 호스트 키 크기를 확인합니다.

show ssh-server host-key

호스트 키 크기: 2048

IPSec 보안 채널 구성

IPSec은 IETF(Internet Engineering Task Force)에서 개발한 개방형 표준 프레임워크입니다. IP 네트워크를 통해 안전하고 인증되고 믿을 수 있는 통신을 생성합니다. IPSec 보안 서비스는 다음을 제공합니다.

- Connectionless Integrity(연결없는 무결성) – 수신된 트래픽이 수정되지 않았다는 보장.
- 데이터 원본 인증 – 합법적인 당사자가 트래픽을 전송한다는 보장.
- Confidentiality (encryption)(기밀성(암호화)) – 인증되지 않은 당사자가 사용자의 트래픽을 검사하지 않음을 보장.
- 액세스 제어 – 리소스의 무단 사용 방지.

IPSec 보안 채널은 다음 알고리즘을 지원합니다.

- 1단계

  ```
  aes128gcm16-prfsha384-prfsha512-prfsha256-prfsha1-ecp256-ecp384-ecp521-modp2048-modp3072-modp4096
  aes128-aes192-aes256-sha256-sha384-sha1_160-sha1-sha512-prfsha384-prfsha512-prfsha256-prfsha1-ecp256-ecp384-ecp521
  aes128-aes192-aes256-sha256-sha384-sha1_160-sha1-sha512-prfsha384-prfsha512-prfsha256-prfsha1-modp2048-modp3072-modp4096
  ```

- 2단계
  - AES SHA 기반 암호화 알고리즘만 지원됩니다. (DES 및 MD5는 지원되지 않음)
  - 지원되는 DH 그룹은 14, 15, 16, 19, 20 및 21입니다.

참고 IPSec 연결은 FXOS에서만 시작할 수 있습니다. FXOS는 수신 IPSec 연결 요청을 수락하지 않습니다.

IPsec 터널은 FXOS가 피어 간에 설정하는 SA 집합입니다. SA는 프로토콜과 알고리즘을 지정하여 민감한 데이터에 지정하고 피어가 사용하는 키 요소도 지정합니다. IPsec SA는 사용자 트래픽의 실제 전송을 제어합니다. SA는 단방향이지만 일반적으로 쌍(인바운드 및 아웃바운드)으로 설정됩니다.

새시 관리자의 IPSec에는 두 가지 모드가 있습니다.

전송 모드
: IP 헤더, IPSec 헤더, TCP 헤더, 데이터

터널 모드
: 새 IP 헤더, IPSec 헤더, 원래 IP 헤더, TCP 헤더, 데이터

IPSec의 작업은 5 가지 주요 단계로 나눌 수 있습니다.

1. 트래픽 선택 – IPSec 정책과 일치하는 트래픽이 IKE 프로세스를 시작합니다. 예를 들어 src/dst 호스트 IP 또는 서브넷을 사용하여 트래픽을 선택할 수 있습니다. 또는 사용자가 admin 명령을 통해 IKE 프로세스를 트리거할 수 있습니다.
2. IKE 1 단계 – IPSec 피어를 인증하고 IKE 교환을 활성화하는 보안 채널을 설정합니다.
3. IKE 2 단계 – IPSec 터널을 설정하기 위해 SA를 협상합니다. SA는 Security Association(보안 연결)을 나타내며, 데이터 트래픽을 보호하는 데 사용되는 보안 서비스를 설명하는 IPSec 엔드포인트 간의 관계입니다.
4. 데이터 전송 – 데이터 패킷은 SA에 저장된 매개변수 및 키를 사용하여 IPSec 헤더에서 암호화되고 캡슐화 됩니다.
5. IPSec 터널 종료 – IPSec SA는 삭제를 통해 또는 시간 초과로 종료됩니다.

공용 네트워크를 통과하는 데이터 패킷에 대해 엔드 투 엔드 암호화 및 인증 서비스를 제공하기 위해 Firepower 4100/9300 섀시에서 IPSec를 구성할 수 있습니다. 이 옵션은 시스템에서 Common Criteria 인증 컴플라이언스를 얻기 위해 제공되는 숫자 중 하나입니다. 자세한 내용은 보안 인증서 컴플라이언스, 1 페이지를 참고하십시오.

참고

- FIPS 모드에서 IPSec 보안 채널을 사용하는 경우 IPSec 피어가 RFC 7427을 지원해야 합니다.
- IKE 및 SA 연결 간에 암호화 키 강도 매칭의 적용을 구성하도록 선택한 경우(아래의 절차에서 sa-strength-enforcement를 yes로 설정):

SA 적용이 활성화된 경우	IKE 협상 키 크기가 ESP 협상 키 크기보다 작은 경우 연결이 실패합니다. IKE 협상 키 크기가 ESP 협상 키 크기보다 크거나 같은 경우 SA 적용 확인이 통과하고 연결이 성공합니다.
SA 적용이 비활성화된 경우	SA 적용 확인이 통과하고 연결이 성공합니다.

IPSec 보안 채널을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** 키 링을 생성합니다.

enter keyring ssp

! create certreq subject-name *subject-name* **ip** *ip*

단계 **3** 연결된 인증서 요청 정보를 입력합니다.

enter certreq

단계 **4** 국가를 설정합니다.

set country *country*

단계 **5** DNS를 설정합니다.

set dns *dns*

단계 **6** 이메일을 설정합니다.

set e-mail *email*

단계 **7** IP 정보를 설정합니다.

set ip *ip-address*

set ipv6 *ipv6*

단계 **8** 지역 정보를 설정합니다.

set locality *locality*

단계 **9** 조직 이름을 설정합니다.

set org-name *org-name*

단계 **10** 조직 단위 이름을 설정합니다.

set org-unit-name *org-unit-name*

단계 **11** 비밀번호를 설정합니다.

! set password

단계 **12** 상태를 설정합니다.

set state *state*

단계 **13** certreq의 주체 이름을 설정합니다.

set subject-name *subject-name*

단계 **14** 종료합니다.

exit

단계 **15** 모듈러스를 설정합니다.

set modulus *modulus*

단계 **16** 인증서 요청의 재생성을 설정합니다.

setregenerate *{yes | no}*

단계 **17** 트러스트 포인트를 설정합니다.

set trustpoint interca

단계 **18** 종료합니다.

exit

단계 **19** 새로 만든 트러스트 포인트를 입력합니다.

enter trustpoint interca

단계 **20** 인증서 서명 요청을 생성합니다.

set certchain

예제**:**

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMAsG
A1UECwwEU1RCVTELMAkGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWC3NzcEBzc3Au
bmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690Vl8/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FlRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QIiGYSctlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMOdWbdeMG3EihxEEOUPD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVl/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZlO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhzYxVZ10DHKIzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpBQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJCggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/fluJ+s/VJSVZWK4tAWvR7wl
QngCKRJW6FYpzeyNBctiJ07wO+Wt4e3KhIjJDYvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBjN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
```

```
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazaIT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
```

단계 **21** 인증서 서명 요청을 표시합니다.

show certreq

예제**:**

```
Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
□□:
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQwwCgYDVQQH
DANTSkMxDjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3t0laoxPbfE
p/lTKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClK/tsIxsPkV0
```

```
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPlX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAlBgkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEARtRBoInxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZl03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMl9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----
```

단계 **22** IPSec 모드로 들어갑니다.

scope ipsec

단계 **23** 로그 자세한 정보 레벨을 설정합니다.

set log-level *log_level*

단계 **24** IPSec 연결을 만들고 입력합니다.

enter connection *connection_name*

단계 **25** IPSec 모드를 tunnel 또는 transport로 설정합니다.

set mode *tunnel_or_transport*

단계 **26** 로컬 IP 주소를 설정합니다.

set local-addr *ip_address*

단계 **27** 원격 IP 주소를 설정합니다.

set remote-addr *ip_address*

단계 **28** 터널 모드를 사용하는 경우 원격 서브넷을 설정합니다.

set remote-subnet *ip/mask*

단계 **29** (선택 사항) 원격 ID를 설정합니다.

set remote-ike-ident *remote_identity_name*

단계 **30** 키 링 이름을 설정합니다.

set keyring-name *name*

단계 **31** (선택 사항) 키 링 비밀번호를 설정합니다.

set keyring-passwd *passphrase*

단계 **32** (선택 사항) IKE-SA 수명을 분 단위로 설정합니다.

set ike-rekey-time *minutes*

minutes 값은 60~1440의 정수일 수 있습니다.

단계 **33** (선택 사항) Child SA 수명을 분 단위로 설정합니다(30-480).

set esp-rekey-time *minutes*

minutes 값은 30~480의 정수일 수 있습니다.

단계 **34** (선택 사항) 초기 연결 중에 수행할 재전송 시퀀스의 수를 설정합니다.

set keyringtries *retry_number*

retry_number 값은 1~5의 정수일 수 있습니다.

단계 **35** (선택 사항) 인증서 해지 목록 확인을 활성화 또는 비활성화합니다.

set revoke-policy *{relaxed | strict}*

단계 **36** 연결을 활성화합니다.

set admin-state enable

단계 **37** 모든 연결을 다시 로드합니다.

reload-conns

시스템이 모든 연결을 중지한 다음 다시 로드합니다. 모든 연결이 재설정을 시도합니다.

단계 **38** (선택 사항) 기존 트러스트 포인트 이름을 IPsec에 추가합니다.

create authority *trustpoint_name*

단계 **39** IKE 및 SA 연결 간 암호화 키 강도 매칭의 적용을 구성합니다.

set sa-strength-enforcement *yes_or_no*

트러스트 포인트에 대한 정적 CRL 구성

해지된 인증서는 CRL(Certification Revocation List)에 유지됩니다. 클라이언트 애플리케이션은 CRL을 사용하여 서버의 인증을 확인합니다. 서버 애플리케이션은 CRL을 사용하여, 더 이상 신뢰할 수 없는 클라이언트 애플리케이션의 액세스 요청을 허용 또는 거부합니다.

CRL(Certification Revocation List) 정보를 사용하여 피어 인증서를 검증하도록 Firepower 4100/9300 섀시를 구성할 수 있습니다. 이 옵션은 시스템에서 Common Criteria 인증 컴플라이언스를 얻기 위해 제공되는 숫자 중 하나입니다. 자세한 내용은 보안 인증서 컴플라이언스, 1 페이지를 참고하십시오.

CRL 정보를 사용하여 피어 인증서를 검증하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** 트러스트 포인트 모드로 들어갑니다.

scopetrustpoint *trustname*

단계 **3** 해지 모드로 들어갑니다.

scope revoke

단계 **4** CRL 파일을 다운로드합니다.

import crl *protocol*://*user_id@CA_or_CRL_issuer_IP*/tmp/*DoDCA1CRL1.crl*

참고 DER 형식 정적 CRL은 FXOS에서 지원되지 않습니다. 다음 명령을 사용하여 DER 형식 CRL 파일을 PEM 형식으로 변환해야 합니다.

```
openssl crl -in filename.crl -inform DER -outform PEM -out crl.pem
```

단계 **5** (선택 사항) CRL 정보 가져오기 프로세스의 상태를 표시합니다.

show import-task detail

단계 **6** 인증서 해지 메서드를 CRL-only로 설정합니다.

set certrevokemethod {crl}

인증서 해지 목록 확인 정보

IPSec, HTTPS 및 안전한 LDAP 연결에서 CRL(Certificate Revocation List) 확인 모드를 엄격하게 또는 엄격하지 않게 구성할 수 있습니다.

FXOS는 동적(정적이 아님) CRL 정보를 동적 CRL 정보를 나타내는 X.509 인증서의 CDP 정보에서 수집합니다. 시스템 관리가 FXOS 시스템에서 로컬 CRL 정보를 나타내는 정적 CRL 정보를 수동으로 다운로드합니다. FXOS는 인증서 체인에서 현재 처리 중인 인증서에 대해 동적 CRL 정보를 처리합니다. 정적 CRL은 전체 피어 인증서 체인에 적용됩니다.

안전한 IPSec, LDAP 및 HTTPS 연결을 위한 인증서 해지 확인을 활성화 또는 비활성화하는 단계에 대해서는 IPSec 안전한 채널 구성, LDAP 제공자 생성 및 HTTPS 구성 섹션을 참조하십시오.

참고

- Certificate Revocation Check Mode(인증서 해지 확인 모드)를 Strict(엄격)로 설정하는 경우 피어 인증서 체인의 레벨이 1 이상일 때만 정적 CRL이 적용됩니다. (예를 들어, 피어 인증서 체인이 루트 CA 인증서 및 루트 CA에서 서명한 피어 인증서만 포함한 경우)
- IPSec에 대해 정적 CRL을 구성할 때는 가져온 CRL 파일에 Authority Key Identifier(기관 키 식별자)(authkey) 필드가 있어야 합니다. 이 필드가 없으면 IPSec에서는 해당 파일이 유효하지 않은 것으로 간주합니다.
- 정적 CRL은 동일한 발급자의 동적 CRL보다 먼저 사용됩니다. FXOS가 피어 인증서를 검증할 때, 동일 발급자의 유효한(확인된) 정적 CRL이 있는 경우, FXOS는 피어 인증서의 CDP를 무시합니다.
- 다음 시나리오에서는 엄격한 CRL 확인이 기본적으로 활성화됩니다.
  - 새로 생성된 보안 LDAP 제공자 연결, IPSec 연결 또는 클라이언트 인증서 항목
  - 새로 구축한 FXOS 섀시 관리자(FXOS 2.3.1.x 이상의 초기 시작 버전으로 구축됨)

다음 표에서는 인증서 해지 목록 확인 설정 및 인증서 검증에 따라 연결 결과를 설명합니다.

표 *1:* 로컬 정적 ***CRL*** 없이 정적으로 설정된 인증서 해제 확인 모드

로컬 정적 **CRL** 없음	**LDAP** 연결	**IPSec** 연결	클라이언트 인증서 인증
피어 인증서 체인 확인	전체 인증서 체인 필요	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인에서 CDP 확인	전체 인증서 체인 필요	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음	예
피어 인증서 체인에서 인증서 유효성 검사 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 해지된 인증서	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락	syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 장애	syslog 메시지와 함께 연결 실패

로컬 정적 **CRL** 없음	**LDAP** 연결	**IPSec** 연결	클라이언트 인증서 인증
유효한 서명이 있는 피어 인증서 체인에서 하나의 CDP CRL이 비어 있음	연결 성공	연결 성공	syslog 메시지와 함께 연결 실패
피어 인증서 체인의 CDP 중 다운로드할 수 없는 것이 있음	syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 장애	syslog 메시지와 함께 연결 실패
인증서에 CDP가 있지만 CDP 서버가 다운됨	syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 장애	syslog 메시지와 함께 연결 실패
인증서에 CDP가 있고 서버가 가동 중이고 CRL이 CDP에 있지만, CRL에 유효하지 않은 서명이 있음	syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 장애	syslog 메시지와 함께 연결 실패

표 ***2:*** 로컬 정적 ***CRL***과 함께 ***Strict***로 설정된 인증서 해제 확인 모드

로컬 정적 **CRL** 있음	**LDAP** 연결	**IPSec** 연결
피어 인증서 체인 확인	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인에서 CDP 확인	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음
피어 인증서 체인에서 인증서 유효성 검사 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 해지된 인증서	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락(인증서 체인 레벨 1)	연결 성공	연결 성공
피어 인증서 체인에서 하나의 CDP CRL이 비어 있음(인증서 체인 레벨 1)	연결 성공	연결 성공
피어 인증서 체인의 CDP 중 다운로드할 수 없는 것이 있음(인증서 체인 레벨 1)	연결 성공	연결 성공

로컬 정적 **CRL** 있음	**LDAP** 연결	**IPSec** 연결
인증서에 CDP가 있지만 CDP 서버가 다운됨(인증서 체인 레벨 1)	연결 성공	연결 성공
인증서에 CDP가 있고 서버가 가동 중이고 CRL이 CDP에 있지만, CRL에 유효하지 않은 서명이 있음(인증서 체인 레벨 1)	연결 성공	연결 성공
피어 인증서 체인 레벨이 1보다 높음	syslog 메시지와 함께 연결 실패	CDP와 결합하는 경우 연결이 성공함 CDP가 없으면 연결에서 장애가 발생하며 syslog 메시지가 제공됨

표 ***3:*** 로컬 정적 ***CRL*** 없이 ***Relaxed***로 설정된 인증서 해제 확인 모드

로컬 정적 **CRL** 없음	**LDAP** 연결	**IPSec** 연결	클라이언트 인증서 인증
피어 인증서 체인 확인	전체 인증서 체인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인에서 CDP 확인	전체 인증서 체인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음	예
피어 인증서 체인에서 인증서 유효성 검사 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 해지된 인증서	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락	연결 성공	연결 성공	syslog 메시지와 함께 연결 실패
유효한 서명이 있는 피어 인증서 체인에서 하나의 CDP CRL이 비어 있음	연결 성공	연결 성공	연결 성공
피어 인증서 체인의 CDP 중 다운로드할 수 없는 것이 있음	연결 성공	연결 성공	연결 성공

로컬 정적 **CRL** 없음	**LDAP** 연결	**IPSec** 연결	클라이언트 인증서 인증
인증서에 CDP가 있지만 CDP 서버가 다운됨	연결 성공	연결 성공	연결 성공
인증서에 CDP가 있고 서버가 가동 중이고 CRL이 CDP에 있지만, CRL에 유효하지 않은 서명이 있음	연결 성공	연결 성공	연결 성공

표 ***4:*** 로컬 정적 ***CRL***과 함께 ***Relaxed***로 설정된 인증서 해제 확인 모드

로컬 정적 **CRL** 있음	**LDAP** 연결	**IPSec** 연결
피어 인증서 체인 확인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인에서 CDP 확인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음
피어 인증서 체인에서 인증서 유효성 검사 실패	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 해지된 인증서	syslog 메시지와 함께 연결 실패	syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락(인증서 체인 레벨 1)	연결 성공	연결 성공
피어 인증서 체인에서 하나의 CDP CRL이 비어 있음(인증서 체인 레벨 1)	연결 성공	연결 성공
피어 인증서 체인의 CDP 중 다운로드할 수 없는 것이 있음(인증서 체인 레벨 1)	연결 성공	연결 성공
인증서에 CDP가 있지만 CDP 서버가 다운됨(인증서 체인 레벨 1)	연결 성공	연결 성공
인증서에 CDP가 있고 서버가 가동 중이고 CRL이 CDP에 있지만, CRL에 유효하지 않은 서명이 있음(인증서 체인 레벨 1)	연결 성공	연결 성공

로컬 정적 **CRL** 있음	**LDAP** 연결	**IPSec** 연결
피어 인증서 체인 레벨이 1보다 높음	syslog 메시지와 함께 연결 실패	CDP와 결합하는 경우 연결이 성공함 CDP가 없으면 연결에서 장애가 발생하며 syslog 메시지가 제공됨

CRL 주기적 다운로드 구성

CRL을 주기적으로 다운로드하도록 시스템을 구성하여 1~24시간마다 새 CRL을 사용하여 인증서를 검증할 수 있습니다.

이 기능과 함께 다음 프로토콜 및 인터페이스를 사용할 수 있습니다.

- FTP
- SCP
- SFTP
- TFTP
- USB

참고

- SCEP 및 OCSP는 지원되지 않습니다.
- 주기적 다운로드는 CRL당 하나만 구성할 수 있습니다.
- 트러스트 포인트당 하나의 CRL이 지원됩니다.

참고 기간은 1시간 간격으로만 구성할 수 있습니다.

CRL 주기적 다운로드를 구성하려면 다음 단계를 수행하십시오.

시작하기 전에

CRL 정보를 사용하여 피어 인증서를 검증하도록 Firepower 4100/9300 섀시를 이미 구성했는지 확인하십시오. 자세한 내용은 트러스트 포인트에 대한 정적 CRL 구성, 9 페이지를 참고하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** 트러스트 포인트 모드로 들어갑니다.

scope trustpoint

단계 **3** 해지 모드로 들어갑니다.

scope revoke

단계 **4** 해지 구성을 수정합니다.

sh config

단계 **5** 원하는 구성을 설정합니다.

예제**:**

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

단계 **6** 구성 파일을 종료합니다.

exit

단계 **7** (선택 사항) 새 CRL을 다운로드하여 새로운 구성을 테스트합니다.

예제**:**

```
Firepower-chassis /security/trustpoint/revoke # sh import-task

□□□□ □□:
□□ □□ □□□□□ □□          Port(□□)     Userid        □/□
--------- -------- ---------------- ---------- --------------- -----
rootCA.crl Scp     182.23.33.113   0          myname        Downloading
```

LDAP 키 링 인증서 설정

Firepower 4100/9300 섀시에서 TLS 연결을 지원하기 위해 안전한 LDAP 클라이언트 키 링 인증서를 구성할 수 있습니다. 이 옵션은 시스템에서 Common Criteria 인증 컴플라이언스를 얻기 위해 제공되는 숫자 중 하나입니다. 자세한 내용은 보안 인증서 컴플라이언스, 1 페이지를 참고하십시오.

참고 Common Criteria 모드가 활성화되면 SSL을 활성화하고, 서버 DNS 정보를 사용하여 키 링 인증서를 생성해야 합니다.

LDAP 서버 항목에 대해 SSL이 활성화되면 연결을 설정할 때 키 링 정보를 참조하고 확인해야 합니다.

안전한 LDAP 연결(SSL 활성화)을 위해 LDAP 서버 정보는 CC 모드에서 DNS 정보여야 합니다.

안전한 LDAP 클라이언트 키 링 인증서를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** LDAP 모드로 들어갑니다.

scope ldap

단계 **3** LDAP 서버 모드로 들어갑니다.

enter server *{server_ip|server_dns}*

단계 **4** LDAP 키 링을 설정합니다.

set keyring *keyring_name*

단계 **5** 구성을 커밋합니다.

commit-buffer

클라이언트 인증서 인증 활성화

LDAP와 함께 클라이언트 인증서를 사용하여 사용자의 HTTPS 액세스를 인증하도록 시스템을 설정할 수 있습니다. Firepower 4100/9300 섀시의 기본 인증 구성은 자격 증명 기반입니다.

참고 인증서 인증이 활성화된 경우, 이것이 HTTPS에 대해 허용되는 유일한 인증 형식입니다.

클라이언트 인증서 인증 기능의 FXOS 2.1.1 릴리스에서는 인증서 해지 확인이 지원되지 않습니다.

이 기능을 사용하려면 클라이언트 인증서에서 다음 요구 사항을 충족해야 합니다.

- X509 특성 Subject Alternative Name - Email(주체 대체 이름 - 이메일)에 사용자 이름을 포함해야 합니다.
- Supervisor의 트러스트 포인트로 인증서를 가져온 루트 CA가 클라이언트 인증서에 서명해야 합니다.

프로시저

단계 **1** FXOS CLI에서 서비스 모드로 들어갑니다.

scope system

scope services

단계 **2** (선택 사항) HTTPS 인증에 대한 옵션을 확인합니다.

set https auth-type

예제**:**

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

단계 **3** HTTPS 인증을 클라이언트 기반으로 설정합니다.

set https auth-type cert-auth

단계 **4** 구성을 커밋합니다.

commit-buffer