セキュリティ認定準拠

セキュリティ認定コンプライアンス

米国連邦政府機関は、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower 4100/9300 シャーシ は、これらのセキュリティ認証基準のいくつかに準拠しています。

これらの基準に準拠する機能を有効にするステップについては、次のトピックを参照してください。

- FIPS モードの有効化，（2 ページ）
- コモン クライテリア モードの有効化，（3 ページ）
- IPSec セキュア チャネルの設定，（4 ページ）

（注） これらのトピックは Firepower 4100/9300 シャーシ における認定準拠の有効化についてのみ説明していることに注意してください。Firepower 4100/9300 シャーシ で認定準拠を有効にしても、接続された論理デバイスにまでそのコンプライアンスは自動的には伝搬されません。

FIPS モードの有効化

Firepower 4100/9300 シャーシで FIPS モードを有効にするには、次の手順を実行します。

手順

ステップ 1 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。

ステップ 2 [プラットフォーム設定（Platform Settings）]**Platform Settings**を選択して、[プラットフォーム設定（Platform Settings）] ウィンドウを開きます。

ステップ 3 [FIPS/CC モード（FIPS/CC mode）]**FIPS/CC mode**を選択して、[FIPS および共通基準（FIPS and Common Criteria）] ウィンドウを開きます。

ステップ 4 FIPS の [有効化（Enable）]**Enable**チェックボックスをオンにします。

ステップ 5 [保存（Save）]**Save**をクリックして、設定を保存します。

ステップ 6 プロンプトに従ってシステムをリブートします。

次の作業

FXOS リリース 2.0.1 より以前は、デバイスの最初の設定時に作成した SSH ホスト キーが 1024 ビットにハード コードされていました。FIPS およびコモン クライテリア認定要件に準拠するには、この古いホスト キーを破棄し、SSH ホスト キーの生成，（3 ページ） で詳細を説明する手

順を使用して新しいホスト キーを生成する必要があります。これらの追加手順を実行しないと、FIPS モードを有効にしてデバイスをリブートした後に、SSH を使用してスーパバイザに接続できなくなります。FXOS 2.0.1 以降を使用して初期設定を行った場合は、新しいホスト キーを生成する必要はありません。

コモン クライテリア モードの有効化

Firepower 4100/9300 シャーシ上でコモン クライテリア モードを有効にするには、次の手順を実行します。

手順

ステップ 1 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。

ステップ 2 [プラットフォーム設定（Platform Settings）]**Platform Settings**を選択して、[プラットフォーム設定（Platform Settings）] ウィンドウを開きます。

ステップ 3 [FIPS/CC モード（FIPS/CC mode）]**FIPS/CC mode**を選択して、[FIPS および共通基準（FIPS and Common Criteria）] ウィンドウを開きます。

ステップ 4 コモン クライテリアの [有効化（Enable）]**Enable**チェックボックスをオンにします。

ステップ 5 [保存（Save）]**Save**をクリックして、設定を保存します。

ステップ 6 プロンプトに従ってシステムをリブートします。

次の作業

FXOS リリース 2.0.1 より以前は、デバイスの最初の設定時に作成した SSH ホスト キーが 1024 ビットにハード コードされていました。FIPS およびコモン クライテリア認定要件に準拠するには、この古いホスト キーを破棄し、**SSH ホスト キーの生成，（3 ページ）** で詳細を説明する手順を使用して新しいホスト キーを生成する必要があります。これらの追加手順を実行しないと、コモンクライテリア モードを有効にしてデバイスをリブートした後に、SSH を使用してスーパバイザに接続できなくなります。FXOS 2.0.1 以降を使用して初期設定を行った場合は、新しいホスト キーを生成する必要はありません。

SSH ホスト キーの生成

FXOS リリース 2.0.1 より以前は、デバイスの初期設定時に作成した既存の SSH ホスト キーが 1024 ビットにハードコードされていました。FIPS およびコモン クライテリア認定に準拠するには、この古いホスト キーを破棄して新しいホスト キーを生成する必要があります。詳細については、FIPS モードの有効化，（2 ページ） または コモン クライテリア モードの有効化，（3 ページ） を参照してください。

古いSSHホストキーを破壊し、新しい証明書準拠キーを生成するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、サービス モードに入ります。
scopesystem

scopeservices

ステップ 2 SSH ホスト キーを削除します。
deletessh-serverhost-key

ステップ 3 設定を確定します。
commit-buffer

ステップ 4 SSH ホスト キーのサイズを 2048 ビットに設定します。
setssh-serverhost-keyrsa 2048

ステップ 5 設定を確定します。
commit-buffer

ステップ 6 新しい SSH ホスト キーを作成します。
createssh-serverhost-key

commit-buffer

ステップ 7 新しいホスト キーのサイズを確認します。
showssh-serverhost-key

ホスト キー サイズ：2048

IPSec セキュア チャネルの設定

Firepower 4100/9300 シャーシ上で IPSec を設定して、エンドツーエンドのデータ暗号化や、パブリック ネットワーク内を移動するデータ パケットに対する認証サービスを提供できます。このオプションは、システムのコモン クライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定コンプライアンス，（1 ページ）を参照してください。

（注） IKE 接続と SA 接続の間で一致する暗号キー強度の適用を設定する場合は、次のようにします（次の手順で sa-strength-enforcement を yes に設定します）。

SA の適用を有効にする場合	IKE によりネゴシエートされたキー サイズが、ESP によりネゴシエートされたキー サイズより小さい場合、接続は失敗します。 IKE によりネゴシエートされたキー サイズが、ESP によりネゴシエートされたキー サイズより大きいか等しい場合、SA 適用検査にパスして、接続は成功します。
SA の適用を無効にした場合	SA 適用検査にパスし、接続は成功します。

IPSec セキュア チャネルを設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。
scopesystem

scopesecurity

ステップ 2 キー リングを作成します。
enterkeyringssp

!createcertreqsubject-name *subject-name***ip** *ip*

ステップ 3 関連する証明書要求情報を入力します。
entercertreq

ステップ 4 国を設定します。
setcountry *country*

ステップ 5 DNS を設定します。
setdns *dns*

ステップ 6 電子メールを設定します。
sete-mail *email*

ステップ 7 IP 情報を設定します。
setfi-a-ip *fi-a-ip*

setfi-a-ipv6 *fi-a-ipv6*

setfi-b-ip *fi-b-ip*

setfi-b-ipv6 *fi-b-ipv6*

setipv6 *ipv6*

ステップ 8 ローカリティを設定します。
setlocality *locality*

ステップ 9 組織名を設定します。
setorg-name *org-name*

ステップ 10 組織ユニット名を設定します。
setorg-unit-name *org-unit-name*

ステップ 11 パスワードを設定します。
!setpassword

ステップ 12 状態を設定します。
setstate *state*

ステップ 13 certreq のサブジェクト名を設定します。
setsubject-name *subject-name*

ステップ 14 終了します。
exit

ステップ 15 モジュラスを設定します。
setmodulus *modulus*

ステップ 16 証明書要求の再生成を設定します。
setregenerate *{ yes | no }*

ステップ 17 トラストポイントを設定します。
settrustpointinterca

ステップ 18 終了します。
exit

ステップ 19 新しく作成されたトラストポイントを入力します。
entertrustpointinterca

ステップ 20 証明書署名要求を作成します。
setcertchain

例：

```
-----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
MRMwEQYDVQQDDApbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
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+YRazalT9xj9KH
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
```

ステップ 21 証明書署名要求を表示します。

showcertreq

例：

```
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):
Request:
-----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-----
```

ステップ 22 IPSec モードに入ります。
scopeipsec

ステップ 23 ログ冗長レベルを設定します。
setlog-level *log_level*

ステップ 24 IPSec 接続を作成し、入力します。
enterconnection *connection_name*

ステップ 25 IPsec モードをトンネリングまたは伝送のために設定します。
setmode *tunnel_or_transport*

ステップ 26 ローカル IP アドレスを設定します。
setlocal-addr *ip_address*

ステップ 27 リモート IP アドレスを設定します。
setremote-addr *ip_address*

ステップ 28 トンネル モードを使用している場合、リモート サブネットを設定します。
setremote-subnet *ip/mask*

ステップ 29 （任意）リモート ID を設定します。
setremote-ike-ident *remote_identity_name*

ステップ 30 キーリング名を設定します。
setkeyring-name 名前

ステップ 31 （任意）キーリング パスワードを設定します。
setkeyring-passwd *passphrase*

ステップ 32 （任意）IKE-SA の有効期間を分単位で設定します。
setike-rekey-time 分

minutes 値には、60 ～ 1440 の範囲内の任意の整数を設定できます。

ステップ 33 （任意）子の SA の有効期間を分単位（30 ～ 480 分）で設定します。
setesp-rekey-time 分

minutes 値には、30 ～ 480 の範囲内の任意の整数を設定できます。

ステップ 34 （任意）初期接続中に実行する再送信シーケンスの番号を設定します。
setkeyringtries *retry_number*

retry_number 値には、1 ～ 5 の範囲の任意の整数を指定できます。

ステップ 35 （任意）証明書失効リスト検査を、有効または無効にします。
setrevoke-policy *{ relaxed | strict }*

ステップ 36 接続を有効にします。
setadmin-stateenable

ステップ 37 すべての接続をリロードします。
reload-conns

ステップ 38 （任意）既存のトラストポイント名を IPsec に追加します。
createauthority *trustpoint_name*

ステップ 39 IKE 接続と SA 接続との間の、対応する暗号キー強度の適用を設定します。
setsa-strength-enforcement *yes_or_no*

トラストポイントのスタティック CRL の設定

失効した証明書は、証明書失効リスト（CRL）で保持されます。クライアント アプリケーションは、CRL を使用してサーバの認証を確認します。サーバ アプリケーションは CRL を使用して、信頼されなくなったクライアント アプリケーションからのアクセス要求を許可または拒否します。

証明書失効リスト（CRL）情報を使用して、Firepower 4100/9300 シャーシがピア証明書を検証するように設定できます。このオプションは、システムのコモン クライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定コンプライアンス, （1 ページ）を参照してください。

CRL 情報を使用してピア証明書を検証するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。
scopesecurity

ステップ 2 トラストポイント モードに入ります。
scopetrustpoint *trustname*

ステップ 3 取り消しモードに入ります。
scoperevoke

ステップ 4 CRL ファイルをダウンロードします。
importcrl *protocol*://*user_id*@*CA_or_CRL_issuer_IP*/tmp/*DoDCA1CRL1.crl*

ステップ 5 （任意）CRL 情報のインポート プロセスのステータスを表示します。
showimport-taskdetail

ステップ 6 CRL 専用の、証明書取り消し方法を設定します。
setcertrevokemethod{crl}

証明書失効リストのチェックについて

証明書失効リスト（CRL）チェック モードを、IPSec、HTTPS およびセキュアな LDAP 接続で厳格または緩和に設定できます。

ダイナミック（非スタティック）CRL 情報は、X.509 証明書の CDP 情報から収集され、動的な CRL 情報を示します。スタティック CRL 情報は、システム管理によって手動でダウンロードされ、FXOS システムのローカルな CRL 情報を示します。ダイナミック CRL 情報は、証明書チェーンの現在処理中の証明書に対してのみ処理されます。スタティック CRL は、ピアの証明書チェーン全体に適用されます。

セキュアな IPSec、LDAP および HTTPS 接続の証明書失効のチェックを有効または無効にするステップについては、IPSec セキュア チャネルの設定, （4 ページ）、LDAP プロバイダーの作成およびHTTPS の設定を参照してください。

（注）
- 証明書失効のチェック モードが厳格に設定されている場合、スタティック CRL はピア証明書チェーンのレベルが 1 以上のときにのみ適用されます。（たとえば、ピア証明書チェーンにルート CA 証明書およびルート CA によって署名されたピア証明書のみが含まれているとき。）
- IPSec にスタティック CRL を設定するときには、インポートされた CRL ファイルに [Authority Key Identifier (authkey)] フィールドが存在している必要があります。そうでない場合、IPSec はそれを無効と見なします。
- スタティック CRL は、同じ発行元からのダイナミック CRL より優先されます。ピア証明書を検証するときに、同じ発行者の有効な（決定済みの）スタティック CRL があれば、ピア証明書の CDP は無視されます。

次の表は、証明書失効リストのチェックの設定と証明書の検証に応じた接続の結果を示しています。

表 *1*：厳格（ローカル スタティック *CRL* なし）に設定した証明書失効のチェック モード

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A	○
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
1 つの CDP でピア証明書チェーンが欠落しています	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
有効な署名付きピア証明書チェーンの 1 つの CDP CRL が空です	接続に成功	接続に成功	接続に失敗（syslog メッセージあり）
ピア証明書チェーンの CDP がダウンロードできません	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）
証明書に CDP はありますが、CDP サーバがダウンしています	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）
証明書に CDP があり、サーバはアップしており、CRL は CDP にありますが、CRL に無効な署名があります	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）

表 *2*：厳格（ローカル スタティック *CRL* あり）に設定した証明書失効のチェック モード

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
1 つの CDP でピア証明書チェーンが欠落しています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの CDP をダウンロードできません（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP がありますが、CDP サーバがダウンしています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗（syslog メッセージあり）	CDP と組み合わせて使用すると、接続に成功します CDP がなければ、接続に失敗し、syslog メッセージが表示されます

表 *3*：緩和（ローカル スタティック *CRL* なし）に設定した証明書失効のチェック モード

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンの CDP のチェック	完全な証明書チェーン	完全な証明書チェーン	完全な証明書チェーン

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A	○
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
1 つの CDP でピア証明書チェーンが欠落しています	接続に成功	接続に成功	接続に失敗（syslog メッセージあり）
有効な署名付きピア証明書チェーンの 1 つの CDP CRL が空です	接続に成功	接続に成功	接続に成功
ピア証明書チェーンの CDP がダウンロードできません	接続に成功	接続に成功	接続に成功
証明書に CDP はありますが、CDP サーバがダウンしています	接続に成功	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります	接続に成功	接続に成功	接続に成功

表 *4*：緩和（ローカル スタティック *CRL* あり）に設定した証明書失効のチェック モード

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンの CDP のチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
1 つの CDP でピア証明書チェーンが欠落しています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの CDP をダウンロードできません（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP がありますが、CDP サーバがダウンしています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗（syslog メッセージあり）	CDP と組み合わせて使用すると、接続に成功します CDP がなければ、接続に失敗し、syslog メッセージが表示されます

CRL 定期ダウンロードの設定

システムを、CRL を定期的にダウンロードして、証明書の検証に新しい CRL を 1 ～ 24 時間ごとに使用するように設定できます。

この機能とともに、次のプロトコルとインターフェイスを使用できます。

- FTP
- SCP
- SFTP
- TFTP
- USB

（注）
- SCEP および OCSP はサポートされません。
- CRL ごとに設定できるのは 1 つの定期ダウンロードのみです。
- トラストポイントごとにサポートされるのは 1 つの CRL です。

（注） 期間は 1 時間間隔でのみ設定できます。

CRL 定期ダウンロードを設定するには、次の手順を実行します。

はじめる前に

Firepower 4100/9300 シャーシが、ピア証明書を（CRL）情報を使用して検証するように設定されていることを確認します。詳細については、トラストポイントのスタティック CRL の設定，（9 ページ）を参照してください。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。
scopesecurity

ステップ 2 トラストポイント モードに入ります。
scopetrustpoint

ステップ 3 取り消しモードに入ります。
scoperevoke

ステップ 4 取り消し設定を編集します。
shconfig

ステップ 5 優先設定を設定します。

例：

```
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
```

ステップ 6 設定ファイルを終了します。
exit

ステップ 7 （任意）新しい CRL をダウンロードして、新しい設定をテストします。

例：

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

Import task:
File Name Protocol Server          Port      Userid        State
--------- -------- --------------- ---------- -------------- -----
rootCA.crl Scp     182.23.33.113   0          myname        Downloading
```

NTP サーバ認証の有効化

NTP サーバ認証を有効にするには、Firepower 4100/9300 シャーシで次の手順を実行します。

（注）
- 有効にすると、NTP 認証機能は設定済みのすべてのサーバでグローバルに機能します。
- NTP サーバ認証では SHA1 のみがサポートされます。
- サーバを認証するには、キー ID とキー値が必要です。キー ID は、メッセージ ダイジェストのコンピューティング時に、使用するキー値をクライアントとサーバの両方に指示するために使用されます。キー値は、ntp-keygen を使用して導出される固定値です。

手順

ステップ 1 ntp 4.2.8p8 をダウンロードします。

ステップ 2 NTP サーバを、**ntpd openssl** を有効にしてインストールします。

ステップ 3 NTP キー ID とキー値を生成します。
ntp-keygen-M

これらの生成されたキーは、次の手順に使用します。

ステップ 4 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。

ステップ 5 [プラットフォーム設定（Platform Settings）]**Platform Settings**を選択して、[プラットフォーム設定（Platform Settings）] ウィンドウを開きます。

ステップ 6 [時刻源を設定（Set Time Source）] 領域で、[NTP サーバの使用（Use NTP server）]**Use NTP server** ラジオ ボタンをクリックします。

ステップ 7 生成された SHA1 文字列とキーで NTP サーバを追加します。

ステップ 8 [保存（Save）]**Save**をクリックして、NTP サーバ設定を保存します。

ステップ 9 [ntp 認証の有効化（Enable ntp-authentication）]**Enable ntp-authentication**チェックボックスをオンにします。

ステップ 10 [保存（Save）]**Save**をクリックします。

LDAP キー リング証明書の設定

Firepower 4100/9300 シャーシ上で TLS 接続をサポートする、セキュアな LDAP クライアント キー リング証明書を設定できます。このオプションは、システムのコモン クライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定コンプライアンス，（1 ページ）を参照してください。

（注） コモン クライテリア モードを有効にする場合は、SSL が有効になっている必要があります。さらにキー リング証明書を作成するために、サーバ DNS 情報を使用する必要があります。

SSL を LDAP サーバ エントリに対して有効にすると、接続の形成時にキー リング情報が参照されて確認されます。

LDAP サーバ情報は、セキュア LDAP 接続（SSL 使用可能）用の、CC モードの DNS 情報である必要があります。

セキュア LDAP クライアントのキー リング証明書を設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。
scopesecurity

ステップ 2 LDAP モードに入ります。
scopeldap

ステップ 3 LDAP サーバ モードに入ります。
enterserver *{server_ip|server_dns}*

ステップ 4 LDAP キー リングを設定します。
setkeyring *keyring_name*

ステップ 5 設定を確定します。
commit-buffer

IP アクセス リストの設定

デフォルトでは、Firepower 4100/9300 シャーシはローカル Web サーバへのすべてのアクセスを拒否します。IP アクセス リストを、各 IP ブロックの許可されるサービスのリストを使用して設定する必要があります。

IP アクセス リストは、次のプロトコルをサポートします。

- HTTPS
- SNMP
- SSH

IP アドレス（v4 または v6）の各ブロックで、最大 25 個の異なるサブネットを各サービスに対して設定できます。サブネットを 0、プレフィックスを 0 と指定すると、サービスに無制限にアクセスできるようになります。

手順

ステップ 1 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。

ステップ 2 [プラットフォーム設定（Platform Settings）]**Platform Settings**を選択して、[プラットフォーム設定（Platform Settings）] ページを開きます。

ステップ 3 [アクセス リスト（Access List）]**Access List**を選択して、[アクセス リスト（Access List）] 領域を開きます。

ステップ 4 この領域で、[IP アクセス リスト（IP Access List）] にリストされている IPv4 および IPv6 アドレスを表示、追加、削除できます。

IPv4 ブロックを追加するには、有効な IPv4 IP アドレスとプレフィックスの長さ（0 ～ 32）を入力し、プロトコルを選択する必要があります。

IPv6 ブロックを追加するには、有効な IPv6 IP アドレスとプレフィックスの長さ（0 ～ 128）を入力し、プロトコルを選択する必要があります。

クライアント証明書認証の有効化

HTTPS アクセスのユーザを認証するために、システムにクライアント証明書を LDAP と一緒に使用させることができます。Firepower 4100/9300 シャーシ上でのデフォルトの認証設定は、認証ベースです。

（注） 証明書認証が有効である場合、これは HTTPS に許可されている唯一の認証形式です。

証明書失効検査は、FXOS 2.1.1 リリースのクライアント証明書認証機能ではサポートされていません。

この機能を使用するには、クライアント証明書が次の要件を満たしている必要があります。

- ユーザ名が X509 属性 [サブジェクト代替名：電子メール（Subject Alternative Name - Email）] に含まれている必要があります。
- クライアント証明書は、その証明書をスーパバイザ上のトラストポイントにインポートしているルート CA により署名されている必要があります。

手順

ステップ 1 FXOS CLI から、サービス モードに入ります。
scopesystem

scopesecurity

ステップ 2 （任意）HTTPS 認証のオプションを表示します。
sethttpsauth-type

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

ステップ 3 HTTPS 認証をクライアントベースに設定します。
sethttpsauth-typecert-auth

ステップ 4 設定を確定します。
commit-buffer