



Secure Sockets Layer Virtual Private Network (SSL VPN)

Secure Sockets Layer Virtual Private Network (SSL VPN) 機能は Cisco IOS ソフトウェアでサポートされています。この機能を使用することにより、リモートユーザーはインターネット上のどこからでも企業ネットワークにアクセスできるようになります。リモートアクセスは、Secure Socket Layer 対応 (SSL 対応) の SSL VPN ゲートウェイを介して提供されます。SSL VPN ゲートウェイによりリモートユーザーはセキュアな VPN トンネルを確立できます。SSL VPN 機能は、フルトンネルクライアントが初めから備えている HTTP over SSL (HTTPS) ブラウザサポートを使用して、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできる包括的なソリューションを実現します。

- [SSL VPN の前提条件 \(1 ページ\)](#)
- [SSL VPN の制約事項 \(2 ページ\)](#)
- [SSL VPN に関する情報 \(2 ページ\)](#)
- [SSL VPN の設定方法 \(5 ページ\)](#)
- [SSL VPN の設定例 \(19 ページ\)](#)
- [SSL VPN のその他の関連資料 \(22 ページ\)](#)
- [SSL VPN の機能情報 \(22 ページ\)](#)

SSL VPN の前提条件

SSL VPN サービスのリモートユーザーが、SSL VPN ゲートウェイ背後にあるプライベートネットワーク上のリソースに安全にアクセスするには、次が必要です。

- アカウント (ログイン名とパスワード)
- Cisco AnyConnect Client を使用したフルトンネルモードのサポート
- Cisco AnyConnect Client をインストールするための管理者権限

SSL VPN の制約事項

- ACL は DENY ステートメントをサポートしていません。
- Cisco AnyConnect VPN を使用して、高い起動レートでトンネルを作成すると、障害が発生する可能性があります。多数の VPN SSL セッション（1000 など）を作成する場合は、15 TPS 以下の起動レートを使用してください。より高い TPS レートを使用すると、障害が発生する可能性があります。
- SSL VPN ピア検出（PD）は、AnyConnect クライアントバージョン 3.x 以降でのみサポートされています。

SSL VPN に関する情報

SSL VPN の概要

Cisco IOS XE SSL VPN は、データ、音声、およびワイヤレス向け統合型プラットフォームに備わる業界最先端のセキュリティ機能およびルーティング機能に SSL VPN リモートアクセス接続機能を統合して提供するルータベースのソリューションです。セキュリティはエンドユーザーの介入を必要とせず、簡単に管理できます。エンドユーザーは Cisco IOS XE SSL VPN を使用して、自宅やワイヤレスホットスポットなど、インターネットに接続されている任意の場所から安全にアクセスすることができます。また、Cisco IOS XE SSL VPN は、機密データを保護したまま、企業ネットワークへのアクセスを海外のパートナーやコンサルタントに拡張する場合にも使用できます。Cisco IOS XE SSL VPN と動的にダウンロードされる Cisco AnyConnect VPN Client を組み合わせて使用することにより、ほぼすべての企業アプリケーションへの完全なネットワークアクセスをリモートユーザーに提供することができます。

SSL VPN には次の 3 つのアクセスモードがありますが、Cisco IOS XE ソフトウェアでサポートされているのはトンネルモードのみです。

- クライアントレス：クライアントレスモードでは、プライベート Web リソースおよび Web コンテンツへのセキュアなアクセスが可能です。このモードは、インターネットアクセス、データベース、Web インターフェイスを使用するオンラインツールなど、Web ブラウザでアクセスするようなほとんどのコンテンツにアクセスする場合に便利です。
- シンククライアント（ポートフォワーディング Java アプレット）：シンククライアントモードでは、Web ブラウザの暗号化機能が拡張され、Post Office Protocol バージョン 3（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、Telnet、セキュアシェル（SSH）などの TCP ベースアプリケーションにリモートアクセスできます。
- フルトンネルモード：フルトンネルクライアントモードでは、動的にダウンロードされる SSL VPN 用 Cisco AnyConnect VPN Client（次世代の SSL VPN Client）を介して幅広いアプリケーションがサポートされます。フルトンネルクライアントモードでは、どのアプ

リケーションにも仮想的にネットワーク層アクセスできる、軽量で中央集約的な設定の、サポートが簡単な SSL VPN トンネリングクライアントが提供されます。



(注) **ip http secure-server** が有効になっている場合、SSL VPN は機能しません。

この機能は、次のプラットフォームでサポートされます。

プラットフォーム	サポートされている Cisco IOS XE リリース
Cisco Cloud Services Router 1000V シリーズ	Cisco IOS XE リリース 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 サービス統合型ルータ Cisco 4451 サービス統合型ルータ Cisco 4431 サービス統合型ルータ	Cisco IOS XE Cupertino 17.7.1a

リモートアクセスのモード

通常のクライアントレスリモートアクセスシナリオでは、リモートユーザーは SSL トンネルを確立してアプリケーション層 (Web および Eメールなど) の内部ネットワーク間のデータを移動します。トンネルモードでは、リモートユーザーは SSL トンネルを使用してネットワーク (IP) レイヤでデータを移動します。したがって、トンネルモードではほとんどの IP ベースアプリケーションがサポートされます。トンネルモードでは多くの一般的な企業アプリケーション (Microsoft Outlook、Microsoft Exchange、Lotus Notes E-mail、Telnet など) がサポートされています。

フルトンネルモードでサポートされる SSL VPN の機能と利点は次のとおりです。

- クライアントレス IPsec VPN に似た動作
- Java または ActiveX を使用して読み込まれるトンネルクライアント
- アプリケーションにとらわれない：すべての IP ベースアプリケーションのサポート
- スケーラブル
- インストールに必要なローカル管理許可

フルトンネルクライアントモードでは、動的にダウンロードされる SSL VPN 用 Cisco AnyConnect VPN Client (次世代の SSL VPN Client) を介して幅広いアプリケーションがサポートされます。フルトンネルクライアントモードでは、どのアプリケーションにも仮想的にネットワーク層アクセスできる、軽量で中央集約的な設定の、サポートが簡単な SSL VPN トンネリングクライアントが提供されます。SSL VPN の利点は、追加デスクトップソフトウェアをインストール

することなく、ほとんどのインターネット接続されたシステムからもアクセスできる点です。Cisco SSL AnyConnect VPN を使用すると、リモートユーザーが SSL VPN ゲートウェイ経由でインターネットから企業ネットワークにアクセスできるようになります。ゲートウェイとの間で SSL VPN 接続を確立する際に、リモートユーザーの機器（ラップトップ、モバイル端末、PDA など）に Cisco AnyConnect VPN Client がダウンロードされてインストールされます。リモートユーザーが SSL VPN ゲートウェイにログインすると、トンネル接続が確立されます。トンネル接続は、グループポリシー設定によって指定されます。デフォルトでは、接続が閉じると Cisco AnyConnect VPN Client はクライアント PC から削除されます。ただし、Cisco AnyConnect VPN Client をクライアント機器にインストールしたままにしておくこともできます。

Cisco SSL AnyConnect VPN を使用すると会社のネットワーク内のサービスに簡単にアクセスすることができます。また、SSL VPN ゲートウェイでの VPN 設定も簡素化されます。それにより、システム管理者の負荷が軽減されます。

SSL VPN CLI の構成要素

SSL プロポーザル

SSL プロポーザルでは、サポートする暗号スイートが指定されています。各暗号スイートでは、キー交換アルゴリズム、一括暗号化アルゴリズム、および MAC アルゴリズムが定義されています。SSL ネゴシエーション時に、設定されている暗号スイートのいずれかがクライアントのプロポーザルから選択されます。クライアントのプロポーザルに含まれるスイートと設定されているスイートがまったく一致しない場合は、ネゴシエーションが終了します。現在のところ、暗号方式はクライアントの優先順位に基づいて選択されます。

SSL プロポーザルは、SSL ハンドシェイクプロトコルによる暗号化と復号のネゴシエーションで使用されます。ユーザが定義したプロポーザルが存在しない場合は、デフォルトの SSL プロポーザルが SSL ポリシーで使用されます。デフォルトのプロポーザルでは、次の順序で暗号方式が指定されています。

```
protection rsa-aes256-sha1 rsa-aes128-sha1 rsa-3des-ede-sha1 rsa-3des-ede-sha1
```

SSL ポリシー

SSL ポリシーでは、サポートする暗号スイートと、SSL ネゴシエーションで使用するトラストポイントが定義されています。SSL ポリシーは SSL ネゴシエーションで使用されるすべてのパラメータのコンテナです。ポリシーの選択は、ポリシーで設定されているパラメータに対してセッションのパラメータを照合することによって行われます。デフォルトのポリシーはありません。各ポリシーには、プロポーザルとトラストポイントが関連付けられています。

SSL プロファイル

SSL VPN プロファイルでは、認証およびアカウントリングのリストが定義されています。プロファイルの選択は、ポリシーと URL 値によって決定されます。プロファイルには、デフォルトの認可ポリシーを関連付けることもできます。

次のルールが適用されます。

- ポリシーおよび URL は SSL VPN プロファイルごとに一意である必要があります。
- セッションを起動するためには、1 つ以上の認可方式が指定されている必要があります。
- 3 つの認可タイプ（ユーザー、グループ、およびキャッシュ）を同時に使用することもできます。
- デフォルトの認可タイプはありません。
- 認可の優先順位は、ユーザ認可、キャッシュ認可、グループ認可の順になります。グループ認可を優先するように設定されている場合の優先順位は、グループ許可、ユーザー認可、キャッシュ認可の順になります。

SSL 認可ポリシー

SSL 認可ポリシーはリモートクライアントにプッシュされる認可パラメータのコンテナです。プッシュされた認可パラメータは仮想アクセスインターフェイスでローカルに、またはデバイス上でグローバルに適用されます。認可ポリシーは SSL VPN プロファイルから参照されます。

SSL VPN MIB

SSL VPN MIB は、SSL VPN を実装するシスコのエンティティに関し、シスコの実装に固有の属性を表します。この MIB は、SSL VPN、トラップ制御、および通知グループを管理することにより、シスコの SSL VPN 実装における運用情報を提供します。たとえば、SSL VPN MIB は、デバイス上でアクティブな SSL トンネルの数などの情報を提供します。

SSL VPN の設定方法

ここでは、SSL VPN の設定に関連するさまざまなタスクについて説明します。

SSL プロポーザルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl proposal *proposal-name***
4. **protection**
5. **end**
6. **show crypto ssl proposal [*proposal name*]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto ssl proposal <i>proposal-name</i> 例： Device(config)# crypto ssl proposal proposal1	SSL プロポーザル名を定義し、SSL プロポーザル コンフィギュレーション モードを開始します。
ステップ 4	protection 例： Device(config-crypto-ssl-proposal)# protection rsa-3des-ede-sha1 rsa-aes128-sha1	次の暗号スイートの中から 1 つまたは複数を選択します。 <ul style="list-style-type: none"> • rsa-3des-ede-sha1 • rsa-aes128-sha1 • rsa-aes256-sha1 • rsa-rc4128-md5
ステップ 5	end 例： Device(config-crypto-ssl-proposal)# end	SSL プロポーザル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show crypto ssl proposal [<i>proposal name</i>] 例： Device# show crypto ssl proposal	(任意) SSL プロポーザルを表示します。

SSL ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl policy *policy-name***
4. **ip address local *ip-address* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*]**
5. **ip interface local *interface-name* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*]**
6. **pki trustpoint *trustpoint-name* sign**
7. **ssl proposal *proposal-name***
8. **no shut**

9. **end**
10. **show crypto ssl policy** [*policy-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto ssl policy <i>policy-name</i> 例： Device(config)# crypto ssl policy policy1	SSL ポリシー名を定義し、SSL ポリシー コンフィギュレーション モードを開始します。
ステップ 4	ip address local <i>ip-address</i> [vrf <i>vrf-name</i>] [port <i>port-number</i>] [standby <i>redundancy-name</i>] 例： Device(config-crypto-ssl-policy)# ip address local 10.0.0.1 port 446	TCP リスナーを開始するためのローカル IP アドレスを指定します。 (注) このコマンドまたは ip interface local コマンドの実行は必須です。
ステップ 5	ip interface local <i>interface-name</i> [vrf <i>vrf-name</i>] [port <i>port-number</i>] [standby <i>redundancy-name</i>] 例： Device(config-crypto-ssl-policy)# ip interface local FastEthernet redundancy1	TCP リスナーを開始するためのローカル インターフェイスを指定します。 (注) このコマンドまたは ip address local コマンドの実行は必須です。
ステップ 6	pki trustpoint <i>trustpoint-name</i> sign 例： Device(config-crypto-ssl-policy)# pki trustpoint tpl sign	(任意) SSL ハンドシェイク中にサーバー証明書を送信するトラストポイントを指定します。 (注) このコマンドが指定されていない場合は、デフォルトの自己署名トラストポイントが使用されます。デフォルトの自己署名トラストポイントが存在しない場合は、システムによりデフォルトの自己署名証明書が作成されます。
ステップ 7	ssl proposal <i>proposal-name</i> 例： Device(config-crypto-ssl-policy)# ssl proposal pr1	(任意) SSL ハンドシェイク中に選択する暗号スイートを指定します。 (注) プロポーザルが指定されていない場合は、デフォルトのプロポーザルが使用されます。

	コマンドまたはアクション	目的
ステップ 8	no shut 例： Device(config-crypto-ssl-policy)# no shut	設定に基づいて TCP リスナーを開始します。
ステップ 9	end 例： Device(config-crypto-ssl-policy)# end	SSL ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	show crypto ssl policy [policy-name] 例： Device# show crypto ssl policy	(任意) SSL ポリシーを表示します。

SSL プロファイルの設定

始める前に

AAA 設定の詳細については、『[Authentication Authorization and Accounting Configuration Guide](#)』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl profile profile-name**
4. **aaa accounting user-pass list list-name**
5. **aaa authentication user-pass list list-name**
6. **aaa authorization group [override] user-pass list aaa-listname aaa-username**
7. **aaa authorization user user-pass {cached | list aaa-listname aaa-username}**
8. **match policy policy-name**
9. **match url url-name**
10. **no shut**
11. **end**
12. **show crypto ssl profile [profile-name]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto ssl profile profile-name 例： Device(config)# crypto ssl profile profile1	SSL プロファイルを定義し、SSL プロファイル コンフィギュレーション モードを開始します。
ステップ 4	aaa accounting user-pass list list-name 例： Device(config-crypto-ssl-profile)# aaa accounting user-pass list list1	認証、認可、およびアカウントリング (AAA) 方式リストを指定します。
ステップ 5	aaa authentication user-pass list list-name 例： Device(config-crypto-ssl-profile)# aaa authentication user-pass list list2	AAA 方式リストを指定します。
ステップ 6	aaa authorization group [override] user-pass list aaa-listname aaa-username 例： Device(config-crypto-ssl-profile)# aaa authorization group override user-pass list list1 user1	グループ認可用の AAA 方式リストとユーザー名を指定します。 <ul style="list-style-type: none"> • group : グループ認可を指定します。 • override : (任意) 属性のマージ中はグループ認可からの属性を優先する必要があることを指定します。デフォルトでは、ユーザー属性が優先されます。 • user-pass : ユーザーパスワードに基づく認可を指定します。 • aaa-listname : AAA 方式リスト名。 • aaa-username : AAA 要求で使用する必要があるユーザー名。デバイスで定義されている SSL 認可ポリシー名を参照します。
ステップ 7	aaa authorization user user-pass {cached list aaa-listname aaa-username} 例： Device(config-crypto-ssl-profile)# aaa authorization user user-pass list list1 user1	ユーザー認可用の AAA 方式リストとユーザー名を指定します。 <ul style="list-style-type: none"> • user : ユーザー認可を指定します。 • user-pass : ユーザーパスワードに基づく認可を指定します。 • cached : EAP 認証中に受信した属性または AAA 事前共有キーから取得した属性をキャッシュする必要があることを指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>aaa-listname</i> : AAA 方式リスト名。 • <i>aaa-username</i> : AAA 認可要求で使用する必要があるユーザー名。
ステップ 8	match policy <i>policy-name</i> 例 : Device(config-crypto-ssl-profile)# match policy policy1	match 文を使用し、SSL ポリシー名に基づいてピアの SSL プロファイルを選択します。
ステップ 9	match url <i>url-name</i> 例 : Device(config-crypto-ssl-profile)# match url www.abc.com	match 文を使用し、URL に基づいてピアの SSL プロファイルを選択します。
ステップ 10	no shut 例 : Device(config-crypto-ssl-profile)# no shut	match policy コマンドで指定されているポリシーが使用されるまでそのプロファイルを閉じないように指定します。
ステップ 11	end 例 : Device(config-crypto-ssl-profile)# end	SSL プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	show crypto ssl profile [<i>profile-name</i>] 例 : Device# show crypto ssl profile	(任意) SSL プロファイルを表示します。

SSL 認可ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl authorization policy** *policy-name*
4. **banner** *banner-text*
5. **client profile** *profile-name*
6. **def-domain** *domain-name*
7. 次のコマンドの 1 つを実行します。
 - **dns** *primary-server* [*secondary-server*]
 - または
 - **ipv6 dns** *primary-server* [*secondary-server*]
8. **dpd-interval** {*client* | *server*} *interval*

9. **homepage** *homepage-text*
10. **include-local-lan**
11. **ipv6 prefix** *prefix*
12. **keepalive** *seconds*
13. **module** *module-name*
14. **msie-proxy exception** *exception-name*
15. **msie-proxy option** {*auto* | *bypass* | *none*}
16. **msie-proxy server** {*ip-address* | *dns-name*}
17. **mtu** *bytes*
18. **netmask** *mask*
19. 次のコマンドの 1 つを実行します。
 - **pool** *name*
 - または
 - **ipv6 pool** *name*
20. **rekey time** *seconds*
21. 次のコマンドの 1 つを実行します。
 - **route set access-list** *acl-name*
 - または
 - **ipv6 route set access-list** *access-list-name*
22. **smartcard-removal-disconnect**
23. **split-dns** *string*
24. **timeout** {*disconnect seconds* | *idle seconds* | *session seconds*}
25. **wins** *primary-server* [*secondary-server*]
26. **end**
27. **show crypto ssl authorization policy** [*policy-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto ssl authorization policy <i>policy-name</i> 例： Device(config)# crypto ssl authorization policy policy1	SSL 認可ポリシーを指定し、SSL 認可ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	banner <i>banner-text</i> 例 : <pre>Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel. NOTE: DO NOT dial emergency response numbers (e.g. 911,112) from software telephony clients. Your exact location and the appropriate emergency response agency may not be easily identified.</pre>	バナーを指定します。バナーはトンネルが正常に確立されると表示されます。
ステップ 5	client profile <i>profile-name</i> 例 : <pre>Device(config-crypto-ssl-auth-policy)# client profile Employee</pre>	AnyConnect クライアントプロファイルを指定します。 crypto vpn anyconnect profile コマンドを使用してすでに指定されているプロファイルを使用する必要があります。AnyConnect イメージおよびプロファイルの設定例については、例： AnyConnect イメージおよびプロファイルの指定 (20 ページ) のセクションを参照してください。 AnyConnect の設定の詳細については、『 Cisco AnyConnect Secure Mobility Client Administrator Guide 』を参照してください。
ステップ 6	def-domain <i>domain-name</i> 例 : <pre>Device(config-crypto-ssl-auth-policy)# def-domain example.com</pre>	デフォルト ドメインを指定します。このパラメータでは、クライアントが使用できるデフォルト ドメインを指定します。
ステップ 7	次のコマンドの 1 つを実行します。 <ul style="list-style-type: none"> • dns <i>primary-server</i> [<i>secondary-server</i>] • または • ipv6 dns <i>primary-server</i> [<i>secondary-server</i>] 例 : <pre>Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100</pre> 例 : <pre>Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2</pre>	プライマリおよびセカンダリ Domain Name Service (DNS) サーバーの IPv4 アドレスまたは IPv6 アドレスを指定します。 <ul style="list-style-type: none"> • <i>primary-server</i> : プライマリ DNS サーバーの IP アドレス。 • <i>secondary-server</i> : (任意) セカンダリ DNS サーバーの IP アドレス。
ステップ 8	dpd-interval { <i>client</i> <i>server</i> } <i>interval</i> 例 : <pre>Device(config-crypto-ssl-auth-policy)# dpd-interval client 1000</pre>	クライアントまたはサーバーの Dead Peer Detection (DPD; デッドピア検出) をグローバルに設定します。 <ul style="list-style-type: none"> • client : クライアントモードの DPD。デフォルト値は 300 (5 分) です。 • server : サーバーモードの DPD。デフォルト値は 300 (5 分) です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>interval</i> : 間隔 (秒単位)。範囲は 5 ~ 3600 です。
ステップ 9	homepage <i>homepage-text</i> 例 : Device (config-crypto-ssl-auth-policy) # homepage http://www.abc.com	SSL VPN ホーム ページの URL を指定します。
ステップ 10	include-local-lan 例 : Device (config-crypto-ssl-auth-policy) # include-local-lan	このキーワードを指定すると、ローカル LAN のリソース (ネットワーク プリンタなど) にリモート ユーザがアクセスできるようになります。
ステップ 11	ipv6 prefix <i>prefix</i> 例 : Device (config-crypto-ssl-auth-policy) # ipv6 prefix 64	IPv6 アドレスの IPv6 プレフィックスを定義します。 <ul style="list-style-type: none"> • <i>prefix</i> : プレフィックス長。有効な範囲は 1 ~ 128 です。
ステップ 12	keepalive <i>seconds</i> 例 : Device (config-crypto-ssl-auth-policy) # keepalive 500	キープアライブの最小値、最大値、およびデフォルト値を秒単位で設定します。
ステップ 13	module <i>module-name</i> 例 : Device (config-crypto-ssl-auth-policy) # module gina	VPN を特定のグループに接続するために必要なモジュールをサーバ ゲートウェイにダウンロードします。 <ul style="list-style-type: none"> • dart : AnyConnect Diagnostics and Reporting Tool (DART) モジュールをダウンロードします。 • gina : Start Before Logon (SBL) モジュールをダウンロードします。
ステップ 14	msie-proxy exception <i>exception-name</i> 例 : Device (config-crypto-ssl-auth-policy) # msie-proxy exception 198.51.100.2	<i>exception-name</i> 引数で指定された DNS 名または IP アドレスにはプロキシ経由で送信が行われなくなります。
ステップ 15	msie-proxy option { <i>auto</i> <i>bypass</i> <i>none</i> } 例 : Device (config-crypto-ssl-auth-policy) # msie-proxy option bypass	Microsoft Internet Explorer ブラウザのプロキシ設定を指定します。内部のプロキシサーバを指定して、企業ネットワークへの接続時にブラウザのトラフィックがプロキシサーバを経由するように設定する場合は、プロキシ設定が必要です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • auto : プロキシサーバー設定を自動検出するようにブラウザを設定します。 • bypass : ローカルアドレスの場合はプロキシサーバーを経由しません。 • none : プロキシサーバーを使用しないようにブラウザを設定します。
ステップ 16	msie-proxy server { <i>ip-address</i> <i>dns-name</i> } 例 : Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2	プロキシサーバーの IP アドレスまたは DNS 名（後にポート番号を付けることもできます）。 (注) msie-proxy option bypass コマンドが指定されている場合、このコマンドは必須です。
ステップ 17	mtu bytes 例 : Device(config-crypto-ssl-auth-policy)# mtu 1000	(任意) MTU の最小値、最大値、およびデフォルト値を設定します。 (注) このコマンドで指定された値は、Cisco AnyConnect Secure クライアントの設定で指定されているデフォルトの MTU 値よりも優先されます。このコマンドを指定しない場合は、Cisco AnyConnect Secure クライアントの設定で指定されている値が MTU 値として使用されます。計算された MTU がこのコマンドで指定されている MTU を下回っている場合、このコマンドは無視されます。
ステップ 18	netmask mask 例 : Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0	クライアントに IP アドレスを割り当てるサブネットのネットマスクを指定します。 <ul style="list-style-type: none"> • mask : サブネット マスク アドレス。
ステップ 19	次のコマンドの 1 つを実行します。 <ul style="list-style-type: none"> • pool name • または • ipv6 pool name 例 : Device(config-crypto-ssl-auth-policy)# pool abc 例 : Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool	リモートアクセスクライアントに IP アドレスを割り当てるためのローカル IPv4 アドレスプールまたはローカル IPv6 アドレスプールを定義します。 <ul style="list-style-type: none"> • name : ローカル IP アドレスプールの名前。 (注) ip local pool コマンドを使用してすでに定義されているローカル IP アドレスプールを使用する必要があります。

	コマンドまたはアクション	目的
ステップ 20	rekey time seconds 例 : Device(config-crypto-ssl-auth-policy)# rekey time 1110	キー再生成の間隔を秒単位で指定します。デフォルト値は 3600 です。
ステップ 21	次のコマンドの 1 つを実行します。 <ul style="list-style-type: none"> • route set access-list acl-name • または • ipv6 route set access-list access-list-name 例 : Device(config-crypto-ssl-auth-policy)# route set access-list acl1 例 : Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1	アクセスリストを使用して、トンネルを介してセキュリティで保護する必要がある IPv4 または IPv6 ルートを確立します。 <ul style="list-style-type: none"> • <i>acl-name</i> : アクセス リスト名。
ステップ 22	smartcard-removal-disconnect 例 : Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect	スマートカードの削除による接続解除を有効にし、スマート カードが削除されたときにクライアント側でセッションを終了するよう指定します。
ステップ 23	split-dns string 例 : Device(config-crypto-ssl-auth-policy)# split-dns example.com example.net	クライアント側でプライベート ネットワーク用に使用するドメイン名を 10 個まで指定できます。
ステップ 24	timeout {disconnect seconds idle seconds session seconds} 例 : Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000	タイムアウトを秒単位で指定します。 <ul style="list-style-type: none"> • disconnect seconds : Cisco AnyConnect クライアントからゲートウェイサーバーへの接続を再試行する期間を秒単位で指定します。デフォルト値は 0 です • idle seconds : アイドルタイムアウトを秒単位で指定します。デフォルト値は 1800 (30 分) です。 • session seconds : セッションタイムアウトを秒単位で指定します。デフォルト値は 43200 (12 時間) です。
ステップ 25	wins primary-server [secondary-server] 例 : Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115	内部の Windows Internet Naming Service (WINS) サーバのアドレスを指定します。 <ul style="list-style-type: none"> • <i>primary-server</i> : プライマリ WINS サーバーの IP アドレス。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>secondary-server</i> : (任意) セカンダリ WINS サーバーの IP アドレス。
ステップ 26	end 例 : Device(config-crypto-ssl-auth-policy)# end	SSL 認可ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 27	show crypto ssl authorization policy [<i>policy-name</i>] 例 : Device(config-crypto-ssl-auth-policy)# show crypto ssl authorization policy	(任意) SSL 認可ポリシーを表示します。

SSL VPN 設定の確認

このセクションでは、**show** コマンドを使用して SSL VPN の設定を確認する方法について説明します。

手順の概要

1. **enable**
2. **show crypto ssl proposal** [*name*]
3. **show crypto ssl policy** [*name*]
4. **show crypto ssl profile** [*name*]
5. **show crypto ssl authorization policy** [*name*]
6. **show crypto ssl session** {**user** *user-name* | **profile** *profile-name*}
7. **show crypto ssl stats** [**profile** *profile-name*] [**tunnel**] [**detail**]
8. **clear crypto ssl session** {**profile** *profile-name*| **user** *user-name*}

手順の詳細

ステップ 1 enable

例 :

```
Device> enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

ステップ 2 show crypto ssl proposal [*name*]

例 :

```
Device# show crypto ssl proposal
```

```
SSL Proposal: sslprop
Protection: 3DES-SHA1
```


SSL プロポーザルを表示します。

ステップ 3 show crypto ssl policy [name]

例：

```
Device# show crypto ssl policy

SSL Policy: sslpolicy
Status      : ACTIVE
Proposal    : sslprop
IP Address  : 10.78.106.23
Port        : 443
fvrf        : 0
Trust Point: TP-self-signed-1183786860
Redundancy  : none
```

SSL ポリシーを表示します。

ステップ 4 show crypto ssl profile [name]

例：

```
Device# show crypto ssl profile

SSL Profile: sslprofile
Status: ACTIVE
Match Criteria:
  URL: none
  Policy:
    sslpolicy
AAA accounting List      : local
AAA authentication List  :none
AAA authorization cached :true
AAA authorization user List :default
AAA authorization user name: sslauth
AAA authorization group List :none
AAA authorization group name: none
Authentication Mode      : user credentials
Interface                 : SSLVPN-VIF1
  Status: ENABLE
```

SSL プロファイルを表示します。

ステップ 5 show crypto ssl authorization policy [name]

例：

```
Device# show crypto ssl authorization policy

SSL Auth Policy: sslauth
V4 Parameter:
  Address Pool: SVC_POOL
  Netmask: 255.255.255.0
  Route ACL : split-include
Banner                : none
Home Page              : none
Idle timeout          : 300
Disconnect Timeout    : 0
Session Timeout       : 43200
Keepalive Interval    : 0
DPD Interval          : 300
Rekey
  Interval: 0
```

```

Method : none
Split DNS : none
Default domain : none
Proxy Settings
  Server: none
  Option: NULL
  Exception(s): none
Anyconnect Profile Name :
SBL Enabled : NO
MAX MTU : 1406
Smart Card
Removal Disconnect : NO

```

SSL 認可ポリシーを表示します。

ステップ6 show crypto ssl session {user user-name | profile profile-name}

例 :

```
Device# show crypto ssl session user LAB
```

```

Session Type : Full Tunnel
Client User-Agent : AnyConnect Windows 3.0.08057

Username : LAB Num Connection : 1
Public IP : 10.163.209.245
Profile : sslprofile Policy Group : sslauth
Last-Used : 00:00:02 Created : *00:58:44.219 PDT Thu Jul 25 2013
Session Timeout : 43200 Idle Timeout : 300
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : sslvpn-pool MTU Size : 1406
Rekey Time : 0 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.1.1.2 Netmask : 255.255.255.0
Rx IP Packets : 0 Tx IP Packets : 125
CSTP Started : 00:01:12 Last-Received : 00:00:02
CSTP DPD-Req sent : 0 Virtual Access : 0
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 34552

```

```
Device# show crypto ssl session profile sslprofile
```

```

SSL profile name: sslprofile
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
LAB 10.163.209.245 1 00:00:33 00:00:00
Error receiving show session info from remote cores

```

SSL VPN セッション情報を表示します。

ステップ7 show crypto ssl stats [profile profile-name] [tunnel] [detail]

例 :

```
Device# show crypto ssl stats
```

```

SSLVPN Global statistics:
Active connections : 0 AAA pending reqs : 0
Peak connections : 1 Peak time : 1w6d
Authentication failures : 21
VPN session timeout : 1 VPN idle timeout : 0
User cleared VPN sessions: 0 Login Denied : 0
Connect succeed : 1 Connect failed : 0
Reconnect succeed : 0 Reconnect failed : 0

```

```

IP Addr Alloc Failed      : 0          VA creation failed      : 0
Route Insertion Failed   : 0
IPV6 Addr Alloc Failed   : 0
IPV6 Route Insert Failed : 0
IPV6 Hash Insert Failed  : 0
IPV6 STC Alloc Failed    : 0
in  CSTP control         : 5          out CSTP control        : 3
in  CSTP data            : 21         out CSTP data           : 8

Device# show crypto ssl stats tunnel profile prfl
SSLVPN Profile name : prfl
Tunnel Statistics:
  Active connections      : 0
  Peak connections       : 0          Peak time                : never
  Connect succeed        : 0          Connect failed           : 0
  Reconnect succeed      : 0          Reconnect failed        : 0
  DPD timeout            : 0
Client
  in  CSTP frames        : 0          in  CSTP control         : 0
  in  CSTP data          : 0          in  CSTP bytes           : 0
  out CSTP frames        : 0          out CSTP control         : 0
  out CSTP data          : 0          out CSTP bytes           : 0
  cef in  CSTP data frames : 0        cef in  CSTP data bytes  : 0
  cef out CSTP data frames : 0        cef out CSTP data bytes  : 0
Server
  In  IP pkts           : 0          In  IP bytes             : 0
  Out IP pkts           : 0          Out IP bytes             : 0

```

SSL VPN の統計情報を表示します。

ステップ 8 clear crypto ssl session {profile profile-name| user user-name}

例 :

```
Device# clear crypto ssl session sslprofile
```

SSL VPN セッションをクリアします。

SSL VPN の設定例

例 : SSL VPN の仮想テンプレートの作成

次の例では、SSL VPN のテンプレートを作成する方法を示します。

```

Device> enable
Device# configure terminal
Device(config)# interface virtual-template 1 type vpn
Device(config-if)# ip unnumbered Te0/0/4
Device(config-if)# ip tcp adjust-mss 1300
Device(config-if)# end

```

例：AnyConnect イメージおよびプロファイルの指定

次の例は、Cisco AnyConnect イメージおよびプロファイルの指定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto vpn anyconnect bootflash:/webvpn/anyconnect-win-3.1.04072-k9.pkg
sequence 1
Device(config)# crypto vpn anyconnect profile Employee bootflash:/Employee.xml
Device(config)# end
```

例：SSL プロポーザルの設定

次の例は、SSL プロポーザルの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl proposal proposal1
Device(config-crypto-ssl-proposal)# protection rsa-3des-ede-sha1 rsa-aes128-sha1
Device(config-crypto-ssl-proposal)# end
```

例：SSL ポリシーの設定

次の例は、SSL ポリシーの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl policy policy1
Device(config-crypto-ssl-policy)# ip address local 10.0.0.1 port 443
Device(config-crypto-ssl-policy)# pki trustpoint tp1 sign
Device(config-crypto-ssl-policy)# ssl proposal proposal1
Device(config-crypto-ssl-policy)# no shut
Device(config-crypto-ssl-policy)# end
```

例：SSL プロファイルの設定

次の例は、SSL プロファイルの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl profile profile1
Device(config-crypto-ssl-profile)# aaa accounting user-pass list list1
Device(config-crypto-ssl-profile)# aaa authentication user-pass list list2
Device(config-crypto-ssl-profile)# aaa authorization group override user-pass list list1
user1
Device(config-crypto-ssl-profile)# aaa authorization user user-pass list list1 user1
Device(config-crypto-ssl-profile)# match policy policy1
Device(config-crypto-ssl-profile)# match url www.abc.com
Device(config-crypto-ssl-profile)# virtual-template 1
Device(config-crypto-ssl-profile)# no shut
Device(config-crypto-ssl-profile)# end
```

例：SSL 認可ポリシーの設定

次の例は、SSL 認可ポリシーの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile Employee
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0
Device(config-crypto-ssl-auth-policy)# pool abc
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

次の例は、SSL VPN の IPv6 サポート機能をイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile profile1
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# ipv6 prefix 64
Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

SSL VPN のその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	<ul style="list-style-type: none"> 『Cisco IOS Security Command Reference: Commands A to C』 『Cisco IOS Security Command Reference: Commands D to L』 『Cisco IOS Security Command Reference: Commands M to R』 『Cisco IOS Security Command Reference: Commands S to Z』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	http://www.cisco.com/cisco/web/support/index.html

SSL VPN の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りが無い限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: SSL VPN の機能情報

機能名	リリース	機能情報
SSL VPN	Cisco IOS XE リリース 17.7.1a	SSL VPN 機能が導入されました。この機能は Cisco IOS XE ソフトウェアでサポートされています。この機能を使用することにより、リモートユーザーはインターネット上のどこからでも企業ネットワークにアクセスできるようになります。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。